

# StorageTek Tape Analytics

## User's Guide



Version 2.4

F33184-03

March 2022

The Oracle logo, consisting of a solid red square with the word "ORACLE" in white, uppercase, sans-serif font centered within it.

ORACLE®

Copyright © 2021, 2022, Oracle and/or its affiliates.

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

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

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

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software" or "commercial computer software documentation" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

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

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

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

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

# Contents

## Preface

---

Documentation Accessibility	xvi
Diversity and Inclusion	xvi
Related Documentation	xvi

## 1 Getting Started

---

About StorageTek Tape Analytics (STA)	1-1
Display STA Software Version Information	1-2
Log in to STA	1-2
User Account Lockout	1-2
Best Practices for STA Login Sessions	1-3
Familiarize Yourself With STA	1-3
Log Out of STA	1-4

## 2 Users and Preferences

---

Configure Your User Preferences and Settings	2-1
Change Your Password	2-1
Username and Password Requirements	2-1
Set Accessibility Options	2-2
Set the Screen Refresh Interval	2-2
Set the Time Zone	2-3
Set the Login Session Timeout Period	2-3
Show or Hide Removed Drives and Media	2-3
Modify Confirmation Dialog Box Preferences	2-4
Manage Other Users	2-5
Add, Modify, or Delete a User	2-5
User Roles and Privileges	2-5

## 3 Screen Layout and Navigation

---

General Screen Layout	3-2
-----------------------	-----

Navigate Using the Left Menu	3-2
Navigate Using Quick Links	3-3
Navigate Using Text Links	3-4
View Tooltips	3-5
Adjust the Zoom	3-5
Resize or Collapse Areas of the Screen	3-5

## 4 Graphs

---

Types of Graphs	4-1
Line Graphs	4-1
Area Charts	4-2
Bar Graphs	4-2
Pie Graphs	4-2
Spark Charts	4-3
Best Practices for Using Graphs	4-3
Modify the Appearance and Arrangement of Graphs	4-5
Restore the Graph Area	4-5
Detach a Graph Pane	4-5
Move Graph Panes on an Overview Screen	4-6
Add or Remove a Graph Pane on an Overview Screen	4-6
Switch Between Narrow and Wide View Graphs	4-7
Print Graphs	4-8
Modify the Data Displayed By Graphs	4-8
Change the Graphed Attribute	4-8
Set the Date Range of a Graph	4-9
Synchronize a Date Range Across All Graphs	4-9
Add Library Resources to Graphs	4-10
Switch Between Actual and Percentage Values	4-10
Graph Data for a Pivot Table Attribute	4-11
Graph Data for a Pivot Table Layer	4-11

## 5 Tables

---

Modify a Table	5-1
Detach a Table	5-1
Reorder Columns	5-2
Resize Column Width	5-3
Sort by a Single Column	5-4
Sort by Multiple Columns	5-5
Hide and Reveal Columns	5-5

Display a Specific Table Page	5-6
Display Details for One or More Resources	5-6
Annotate a Table Row	5-7
Print a Table	5-7
Refresh the Table Display	5-7
Modify a Pivot Table	5-8
What Are Pivot Tables?	5-8
View the Name of a Pivot Table Layer	5-9
Resize a Column or Row of a Pivot Table	5-9
Display Details for a Pivot Table Value	5-10
Move Pivot Table Layers	5-10
Change Pivot Table Attributes and Nesting Order	5-11
Add Table Data to Graphs	5-11
Export Table Data to a Spreadsheet or Document	5-12
Select Multiple Rows in a Table or List	5-13

## 6 Dashboard

---

View the Dashboard	6-1
Dashboard Layout	6-1
Link to Details from a Dashboard Pane	6-2
Detach a Pane to View More Detail	6-3
View the Dashboard on a Mobile Device	6-3
Why is the dashboard taking a long time to load?	6-3
Customize the Dashboard	6-4
Change the Size of Dashboard Panes	6-4
Add a Dashboard Pane	6-5
Move a Dashboard Pane	6-5
Remove a Dashboard Pane	6-6
Annotate a Dashboard Pane	6-6
Filter a Dashboard Pane	6-6
Save the Dashboard Layout	6-7
Dashboard Pane Types	6-7
Graph Panes	6-7
Table Panes	6-10
Report Panes	6-12

## 7 Templates

---

Template Types	7-1
Apply a Template	7-2

Set the Default Template for a Screen	7-3
Customize a Template	7-4
Save a Template	7-4
Modify a Template	7-5
Rename a Template	7-5
Set a the Visibility of a Template to Public or Private	7-6
Template Ownership and Visibility	7-7
Delete a Template	7-7
Share a Template	7-7
Export a Template	7-8
Import a Template	7-8
Restore the Predefined Templates	7-9
User Roles for Template Activities	7-9
Descriptions of Predefined Templates	7-10
Dashboard Predefined Templates	7-11
Complexes Overview Predefined Templates	7-12
Libraries – Overview Predefined Templates	7-12
Libraries – Messages Predefined Template	7-13
Drives – Overview Predefined Templates	7-13
Drives – Analysis Predefined Templates	7-14
Drives – Messages Predefined Template	7-14
Media – Overview Predefined Templates	7-14
Media – Analysis Predefined Templates	7-15
Media – Messages Predefined Template	7-16
Robots Overview Predefined Templates	7-16
CAPs Overview Predefined Templates	7-16
PTPs Overview Predefined Templates	7-16
Elevators Overview Predefined Templates	7-17
Alerts Overview Predefined Templates	7-17
Exchanges Overview Predefined Templates	7-17
Drive Cleanings Overview Predefined Templates	7-18
Media Validation Overview Predefined Templates	7-18
All Messages – Overview Predefined Templates	7-18
All Messages – Analysis Predefined Template	7-19

## 8 Filters

---

View the Filter Applied to the Current Screen	8-1
Do Filters Apply to Multiple Screens?	8-1
Apply a Filter	8-1
Filter Using the Dialog Box	8-2

Filter Operators by Attribute Type	8-3
Filter by Applying a Template	8-4
Filter Using Dashboard Graphics	8-5
Filter Using Pivot Links	8-6
Clear the Current Filter	8-7

## 9 Alerts

---

How Alerts Work	9-1
Best Practices for Alert Policies	9-2
Define Alert Policies	9-3
View a List of Alert Policies	9-3
Create, Copy, or Modify an Alert Policy	9-4
Alert Policy Wizard	9-4
Modify Email Recipients for an Alert Policy	9-5
Enable or Disable an Alert Policy	9-6
View Alerts	9-6
View a List of Generated Alerts	9-7
Display Details for an Alert	9-7
Show or Hide Dismissed Alerts	9-8
Change the State of an Alert	9-8
Alerts Workflow	9-8
User Roles for Alerts Management	9-9
Alert Entities	9-9
Alert Severities	9-10
Alert Policy Examples	9-10
"Warning" Policy for Drives Example	9-11
"Informative" Policy for Drives Example	9-11
"Severe" Policy for Media Example	9-12
"Severe" Policy for CAPs Example	9-13
Policy for Exchanges Using "Media Health Indicator" Example	9-14
"Warning" Policy for Media Using "Media Health Indicator" Example	9-14
Sample Alert Emails	9-15

## 10 Executive Reports

---

Best Practices for Executive Reports	10-1
View, Download, or Delete Executive Report Files	10-2
View a List of Executive Reports	10-2
Download an Executive Report File	10-2
Delete an Executive Report File	10-3

Run an Executive Report On Demand	10-3
Manage Executive Report Policies	10-4
View a List of Executive Report Policies	10-4
Define an Executive Report Policy	10-4
Delete an Executive Report Policy	10-5
User Roles for Executive Reports and Policies	10-5
Sample Executive Report	10-6

## 11 Logical Groups

---

Types of Logical Groups	11-1
Best Practices for Logical Groups	11-1
Why Use Logical Groups?	11-2
Configure Logical Groups	11-2
Create a Manual Logical Group	11-3
Logical Group Ownership	11-3
Add Drives and Media to a Manual Logical Group	11-3
Remove Drives and Media From a Manual Logical Group	11-4
Create and Define a Dynamic Logical Group	11-5
Dynamic Group Selection Criteria	11-5
Change the Selection Criteria for a Dynamic Logical Group	11-6
Force a Dynamic Logical Group Update	11-7
View Logical Group Assignments for Selected Drives or Media	11-7
List All Drives and Media Assigned to a Logical Group	11-7
Rename a Logical Group	11-8
Delete a Logical Group	11-9
Filter by Logical Group	11-9
How Changes to Logical Group Definitions Affect Filters	11-10
Where Can I Use Logical Group Filtering?	11-11

## 12 Media Validation

---

Features and Benefits of Media Validation	12-2
Media Validation Feature Comparison for STA and the Library Interface	12-3
Configure the Media Validation Drive Pool	12-4
Identify Drives for the Media Validation Pool	12-4
Add Drives to the Media Validation Pool	12-5
Verify there are Valid Validation Drives	12-5
Automate Media Validation Using Policies	12-6
Create, Copy, or Modify a Media Validation Policy	12-6
Media Validation Policy Wizard	12-7



Enable or Disable a Media Validation Policy	12-9
Identify Media Eligible for Validation	12-9
Configure Drive Calibration and Qualification	12-10
Create the Calibration Media Logical Group	12-10
How to Choose Calibration Media	12-12
Enable Drive Calibration and Qualification	12-13
Disable Drive Calibration and Qualification	12-13
Verify Drive Calibration Status	12-14
Benefits of Calibration and Qualification	12-14
How Calibration and Qualification Work	12-15
Enable or Disable STA-driven Media Validation	12-17
Submit Manual Media Validation Requests	12-18
Resubmit a Completed Media Validation	12-20
Resume Validations on T10000 T2 Media	12-21
Manage the Media Validation Requests Queue	12-22
Display the Media Validation Request Queue	12-22
Reorder Pending Media Validation Requests	12-22
Cancel In-Progress or Pending Media Validation Requests	12-23
User Roles for Media Validation Activities	12-24
Types of Media Validation Tests	12-24
How STA Tracks and Reports Media Validation	12-25
Why Aren't SL150 Media Validation Drives Showing in STA?	12-28

## 13 Email Recipients

---

Define the SMTP Email Server	13-1
Add, Modify, or Delete an Email Recipient	13-2
Test the Email Server and Recipient Definitions	13-3

## 14 Service Log Bundles

---

About Log Bundles	14-1
Log Bundle Types	14-1
Log Bundle Naming	14-2
Log Bundle Retention	14-2
Log Bundle Directories	14-3
Create and Submit a Log Bundle to Oracle Support	14-3
Create a Library Component Log Bundle	14-3
Create a Database Bundle	14-4
Create an RDA Log Bundle from the STA Application	14-4
Create an RDA Log Bundle from the System Command Line	14-5

Download a Log Bundle	14-6
Manually Forward a Log Bundle to My Oracle Support	14-6
Delete a Log Bundle	14-6
View a List of Log Bundles	14-7
Display Log Run Information	14-7

## 15 Automatic Log Bundles and SDP

---

How Automatic Bundle Creation Works	15-1
How the Service Delivery Platform (SDP) Handles a Bundle	15-2
How Automatic Bundle Alerts Work	15-2
Enable or Disable Automatic Bundle Creation	15-2
Best Practices When Enabling Automatic Bundle Creation	15-3
Define the SDP Host to STA	15-4
Test STA to SDP Communication	15-5
Define Email Recipients for Automatic Log Bundle Alerts	15-6
Display Automatic Bundle Creation Policies	15-7
Display Automatic Bundle Alerts	15-7
Display Library Components With Automatic Bundles	15-8

## 16 Library Connection (SNMP or SCI)

---

Configure SNMP (for SL150, SL500, SL3000, SL8500)	16-1
Configure SNMP on the Libraries	16-2
Retrieve the Library IP Address	16-2
Enable SNMP on the Library	16-4
Create an SNMP v3 User	16-5
Retrieve the Library SNMP Engine ID (SL500, SL3000, SL8500)	16-6
Create the STA SNMP v3 Trap Recipient	16-7
Configure SNMP on the STA Server	16-8
Sign In to the STA GUI	16-8
Verify SNMP Communication with a Library (optional)	16-9
Configure SNMP Client Attributes for STA	16-10
Configure the SNMP Connection to a Library	16-11
Update the SNMP Configuration After a Library or STA Change	16-12
Update SNMP After a Redundant Electronics Switch (SL3000, SL8500)	16-12
Update SNMP After a Library Firmware Upgrade (SL500, SL3000, SL8500)	16-13
Update SNMP After Changing the STA Server IP Address	16-14
Remove a Library Connection from STA	16-14
Delete or Modify the STA Trap Recipient	16-14
Configure SNMP v2c Mode	16-15

When to Use v2c Mode	16-15
Create an SNMP v2c User	16-15
Create the STA SNMP v2c Trap Recipient	16-16
Enable SNMP v2c Mode for STA	16-17
Configure SCI (for SL4000)	16-18
Add the SL4000 as a Monitored Library	16-18
Test the Library Connection	16-20
When to Test the Library Connection	16-21
Manually Collect Library Data	16-21
When to Manually Collect Data	16-22
About Library Data Collection	16-22
About the Monitored Libraries Table	16-23
About the Library Engine ID	16-24
Troubleshoot the Library Connection	16-25
Verify the Library is Operational	16-26
Verify the Firewall Settings	16-27
Enable and Test the SCI Destination on the SL4000	16-27
Manually Configure the SL4000 to Send Outbound SCI to STA	16-28
Export SNMP Connection Settings to a Text File	16-29
Display All SNMP Trap Recipients	16-30
Troubleshoot a Failed MIB Walk Channel Test	16-30
Troubleshoot a Failed Trap Channel Test	16-32
Troubleshoot a Failed Media Validation Support Test	16-33
Troubleshoot Unsuccessful Trap Processing	16-33

## 17 Understanding STA Data

---

Understand How STA Handles Changes to the Tape Environment	17-1
Understand Data Retention and the Tracking Timestamp	17-1
How Incomplete Exchanges Affect STA	17-2
Why Some Values May Be Dimmed	17-2
What Happens to Data When Drives and Media Are Removed	17-3
What Happens to Data When Libraries Are Removed	17-4
What Happens to Data When an SL8500 Library is Moved to a New Complex	17-4
How STA Handles "Missing" Media	17-5
How STA Handles Duplicate Volume Serial Numbers	17-5
How to Map Host and STA Drive Identifiers	17-6
Use STA to Answer Common Tape Environment Questions	17-7
Best Practices for Investigating Tape Environment Issues	17-7
General Error Trend Analysis	17-8
View Error Messages From a Specific Time	17-9

View Trends in Critical Drive and Media Errors	17-9
View Trends in Exchange Errors	17-10
Library System Analysis	17-11
Identify Media and Drives Involved with Job Errors	17-11
Display Correlations Between the Drives and Media with the Most Errors	17-12
Determine Number of Libraries, Drives, or Media in the System	17-13
Report Library Activity Levels	17-14
Drive Analysis	17-16
Identify Drives With the Most Errors	17-16
Analyze Drive Failure Trends	17-17
Identify Drives that Had a Health State Change	17-18
Analyze Drive Efficiency	17-18
Analyze Drive Utilization	17-19
Report Drive Firmware Levels	17-21
Media Analysis	17-23
Identify Media With the Most Errors	17-23
Identify Failed Mount Exchanges	17-24
Identify Shortages or Surpluses of Media	17-25
Analyze Media Utilization	17-27
Identify Media for a Migration	17-28
Identify Older Media	17-29
Identify Media that is Approaching Capacity	17-29

## A Quick Start Guide

---

Log in to STA	A-1
Apply a Dashboard Template	A-3
Explore the Dashboard	A-4
Navigate Using the Left Menu	A-7
Navigate Using Text Links	A-8
Understand the General Screen Layout	A-10
Display Media Exchanges for a Library	A-12
Reset a Screen Filter	A-13
Display Full Details for Selected Exchanges	A-14
Display Aggregated Drive Data	A-17
Export Data to a Spreadsheet	A-19
Access the Online Help	A-19
Log Out	A-21
Next Steps After Finishing the Quick Start	A-21

## B Data Reference

---

Attribute Definitions	B-1
Symbols	B-2
A	B-2
B	B-9
C	B-9
D	B-11
E	B-17
F	B-20
H	B-20
I	B-20
L	B-21
M	B-25
MV	B-33
N	B-38
P	B-38
R	B-41
S	B-43
T	B-44
U	B-45
W	B-45
Data Reference: Complexes Overview	B-46
Data Reference: Libraries Overview	B-48
Data Reference: Drives Overview	B-50
Data Reference: Media Overview	B-57
Data Reference: Robots Overview	B-63
Data Reference: CAPs Overview	B-64
Data Reference: PTPs Overview	B-66
Data Reference: Elevators Overview	B-67
Data Reference: Alerts Overview	B-68
Data Reference: Exchanges Overview	B-70
Data Reference: Drive Cleanings Overview	B-78
Data Reference: Media Validation Overview	B-80
Data Reference: Messages Screens	B-82

## C Troubleshoot Issues

---

ISSUE: Cannot Access the STA GUI	C-1
ISSUE: GUI Elements Do Not Render Correctly	C-2
ISSUE: Exchanges Not Showing Up in STA	C-3
ISSUE: T1000D Drives Are Not Showing Quality Index After Media Validation	C-4

ISSUE: Database Communication Link Failure (IMPORTANT)	C-5
ISSUE: OSCI Library Connection Test Fails	C-5
ISSUE: SNMP Library Connection Test Fails	C-6
ISSUE: SNMP Trap Status Not Updating After Connection Test	C-6
ISSUE: Cannot Connect to SDP	C-7
ISSUE: STA Fails to Restart Properly After Reboot	C-7
ISSUE: Weblogic Server Processes Not Starting	C-7
ISSUE: Authentication Prompts During STA start Command	C-8
ISSUE: Backup Service or Resource Monitor Fails	C-8
ISSUE: MySQL Installation Fails	C-9
ISSUE: STA Does Not Completely Deinstall	C-9

## Index

---

## List of Tables

---

2-1	User Role Privileges, Organized by Screen	2-6
9-1	Alert Privileges for User Roles	9-9
10-1	Executive Report User Roles	10-6

# Preface

This guide provides procedures for using the StorageTek Tape Analytics (STA) user interface.

## Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

### Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> or visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> if you are hearing impaired.

## Diversity and Inclusion

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

## Related Documentation

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



# 1

## Getting Started

Learn how to log into the GUI and use key features of the interface to discover the powerful data analysis of STA.

- [About StorageTek Tape Analytics \(STA\)](#)
- [Log in to STA](#)
- [Familiarize Yourself With STA](#)
- [Log Out of STA](#)

**See Also:**

- [Quick Start Guide](#)

## About StorageTek Tape Analytics (STA)

Oracle's StorageTek Tape Analytics (STA) is an intelligent monitoring application that collects and analyzes data about your tape library environment.

STA is available exclusively for Oracle's StorageTek Modular Tape Libraries. It simplifies tape storage management and helps you make informed decisions about future tape storage investments based on the current health of your environment. STA allows you to monitor globally dispersed libraries from a single, browser-based user interface. You can manage open systems and mainframe mixed-media, and mixed-drive environments across multiple library platforms.

STA's detailed analysis allows you to increase the utilization and performance of your tape investments. A continually updated database of library operations provides the basis for the analytics. STA captures and retains data from your tape library environment and uses this data to calculate the health status of your library resources (drives and media). STA compiles data according to a variety of criteria and displays it in tabular and graphical formats, allowing you to quickly assess tape environment activity, health, and capacity.

### Devices Supported by STA

#### Tape Libraries

- SL8500
- SL4000
- SL3000
- SL500
- SL150

#### Drive and Media Types

- StorageTek T10000A, B, C, and D drives (with T10000 T1 and T2 media)
- StorageTek 9840C and 9840D
- HP LTO generations 3, 4, 5, and 6

- IBM LTO generations 3, 4, 5, 6, 7, 8 and 9
- LTO M8 media is only supported by STA 2.3.1 and above

See the *STA Installation and Configuration Guide* for complete details about the device support, minimum firmware levels, and other requirements

## Display STA Software Version Information

Display version information about the STA application and supporting software. This information is useful whenever you contact your Oracle support representative.

1. Within the GUI, click **About** in the bottom-right of the screen.
2. The About dialog box displays:
  - STA software version and build information
  - Weblogic server version and patch level
  - Database server version and driver level
  - Database schema version and size information
  - Oracle ADF and SDP information
  - Linux operating system and Java release

## Log in to STA

Use a compatible browser to log in to the web GUI of STA.

1. Obtain the following from your STA administrator:
  - URL of the STA application
  - Your STA username and password
2. Verify your computer and browser are configured correctly. See the *STA Installation and Configuration Guide* for minimum requirements.
3. Go to: `https://<host_name>:<port>/STA`
  - `<host_name>` is the name of the STA server
  - `<port>` is the port defined during STA installation
4. Enter your username and password, and then click **Login**.
5. Depending on your preference settings, you may be prompted to [Set Accessibility Options](#).

## User Account Lockout

After five unsuccessful login attempts within a five-minute period, you will be locked out of your user account for 30 minutes.

For security reasons, your account cannot be reset during the lockout period, even by the STA administrator. You must wait the full 30-minutes before attempting to log in again.

## Best Practices for STA Login Sessions

Follow these best practices when logged in to STA.

### **Do Not Use the Browser Forward and Back Buttons**

Do not use your browser's **Forward** and **Back** (or **Next** and **Previous**) buttons for navigating through the STA screens. Using these buttons could have unpredictable results, as the data you see may be stale or out of sync with the data on the STA server. To navigate, you should always use the methods provided by STA: the Navigation Bar and text links.

### **Always log out to end a session**

When you are ready to finish a login session, always explicitly log out, rather than simply closing the browser window. Logging out releases the session memory on the STA server for other processes. If you simply close the browser window, the session memory is not freed until the defined session timeout period is exceeded, possibly impacting STA performance, especially if your session timeout period is long.

### **One Login Session Per Browser**

For each browser you can have only one login session at a time open to a particular STA instance. If you have multiple sessions open to the same STA instance in the same browser, you may notice navigation and display issues, such as a frozen navigation bar (where the tabs on the navigation bar cannot be selected or expanded). You may also notice the **Logout** link or the **Setup & Administration** link in the Navigation Bar disappear from the screen display. If you notice any of these conditions, you should close or log out of all but one session to an STA instance in the browser.

## Familiarize Yourself With STA

Learn about key features and discover the powerful data analysis that STA can provide.

If you are new to STA, you should complete the steps in the [Quick Start Guide](#). Additionally, you may want to review the following:

- [Navigate Using the Left Menu](#)
- [Navigate Using Text Links](#)
- [Apply a Template](#)
- [Customize the Dashboard](#)
- [Apply a Filter](#)
- [Modify the Appearance and Arrangement of Graphs](#)
- [Modify the Data Displayed By Graphs](#)
- [Modify a Table](#)
- [Modify a Pivot Table](#)
- [Export Table Data to a Spreadsheet or Document](#)

## Log Out of STA

Always end your STA session by logging out rather than closing the browser. This releases session memory on the STA server for other processes.

From any STA screen, click **Logout** in the upper-right of the main toolbar.

# 2

## Users and Preferences

Each user can modify preferences for their username. The administrator can add, modify, or delete other users.

- [Configure Your User Preferences and Settings](#)
- [Manage Other Users](#)

### Configure Your User Preferences and Settings

Each user can modify preferences and settings for their login session. The settings remain in effect for future login sessions.

- [Change Your Password](#)
- [Set Accessibility Options](#)
- [Set the Screen Refresh Interval](#)
- [Set the Login Session Timeout Period](#)
- [Set the Time Zone](#)
- [Show or Hide Removed Drives and Media](#)
- [Modify Confirmation Dialog Box Preferences](#)

### Change Your Password

Regularly change the password for your STA username to maximize security.

1. From the **Preferences** drop-down in the upper-right, select **General**.
2. In the **Change Password** field, enter the new password.
3. Enter the password again in the **Verify Password** field.
4. Click **OK**.

### Username and Password Requirements

Each username and password must meet minimum requirements.

Username requirements:

- Must be 1–16 characters in length
- All usernames must be unique, but are not case sensitive

Password requirements:

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

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

## Set Accessibility Options

The first time you log in to the GUI, it will prompt you to set the accessibility options (this prompt remains each time you login until you select "Do not show"). You can change the settings at anytime.

1. From the **Preferences** drop-down in the upper-right, select **Accessibility**.
2. Select accessibility settings:
  - **Screen reader** - If you are using a screen reader (such as JAWS) to interface with the GUI, select this option. The GUI generates components that have rich user interface interaction and allows you to perform all screen actions with the keyboard instead of a mouse, and alternate text is provided for all screen icons, buttons, and graphic images.
  - **High contrast** - The GUI generates high-contrast-friendly visual content. High-contrast mode is designed for use with operating systems or browsers that have high-contrast features enabled.
  - **Large-fonts** - The GUI generates browser zoom-friendly content.
  - **Do not show these options again** – Indicates that you do not want this dialog box to be displayed automatically when you log in. If you apply this option, this dialog box will be skipped for all future times that you log in to STA. You can use this procedure to reset this option at any time.
3. Click **OK**.

STA modifies the screen display immediately according to your selections. These settings remain in effect for future login sessions, until you explicitly change them.

## Set the Screen Refresh Interval

The screen display refreshes at the frequency you specify. The default is 480 seconds (8 minutes).

1. From the **Preferences** drop-down in the upper-right, select **General**.
2. In the field, enter the new refresh rate (60 to 720), and then click **OK**.
3. The settings take effect immediately and only applies to your username. They remain in effect for this and future login sessions, until you change them again using this procedure.

## Set the Time Zone

By default, STA displays times adjusted to your computer's system clock. You can change the time zone for your username to see data displayed according to a different location.

### Note:

These settings do not affect the Dashboard display. Dashboard data is always shown in UTC time, regardless of your time zone preference settings.

1. From the **Preferences** drop-down in the upper-right, select **General**.
2. Select a from the drop-down, and then click **OK**.

To have STA automatically detect your local time zone based on your computer's system clock, select `<Auto-detect Time Zone>`.

3. Data in all STA screens is immediately displayed in the new time zone. The time zone setting remains in effect for future login sessions, until you change it again using this procedure.

## Set the Login Session Timeout Period

If your login session is idle for longer than the timeout period, your session ends. The default is 30 minutes.

1. From the **Preferences** drop-down in the upper-right, select **General**.
2. In the field, enter the timeout period (10 to 1440).

Increasing the session timeout will likely increase STA server memory utilization, which may impact STA performance.

3. Click **OK**.

The settings take effect immediately. They remain in effect for future login sessions, until you change them again using this procedure.

## Show or Hide Removed Drives and Media

Choose whether to show or hide removed drives and media within STA screens. By default, removed drives and media are not included on their respective Overview and Analysis screens.

1. From the **Preferences** drop-down in the upper-right, select **Data Handling**.
2. Select the appropriate check boxes:
  - Show Removed Drives
  - Show Removed Media
3. Verify your selections and then click **OK**.

The settings take effect immediately. They remain in effect for this and future login sessions, until you change them again using this procedure.

### How the "Show Removed" Settings Affect STA Screens

Option	If Selected	If Deselected
Show Removed Drives	<p>The Drives–Overview screen shows removed drives.</p> <p>The Drives–Analysis screen includes data for removed drives.</p> <p>On all screens, the removed drive serial number becomes an active link to the Drives–Overview, Detail View screen.</p>	<p>The Drives–Overview screen hides removed drives.</p> <p>The Drives–Analysis screen does not include removed drives.</p> <p>On all screens, the removed drive serial number becomes dimmed and is not a link.</p>
Show Removed Media	<p>The Media–Overview screen shows removed media.</p> <p>The Media–Analysis screen includes data for removed media.</p> <p>On all screens, the removed volume serial numbers (VSNs or volsers) becomes an active link to the Media–Overview, Detail View screen.</p>	<p>The Media–Overview screen hides removed media.</p> <p>The Media–Analysis screen does not include data for removed media.</p> <p>On all screens, the removed volume serial numbers (VSNs or volsers) becomes dimmed and is not a link.</p>

**See Also:** [What Happens to Data When Drives and Media Are Removed](#)

## Modify Confirmation Dialog Box Preferences

Choose whether to display or suppress confirmation dialog boxes that appear when performing various tasks.

- From the **Preferences** drop-down in the upper-right, select **Confirmations**.
- For each option listed, select the check box to display the dialog box or deselect the check box to suppress the dialog box. Options are:
  - Graph Time Sync** – Select to have a confirmation appear before you synchronize all graphs on a screen to the same date range. Clear the checkbox to suppress the confirmation and synchronize graphs as soon as you click Synchronize Date Range in the Graph Pane Toolbar.
  - Template Overwrite** – Select to have a confirmation appear before you save changes to an existing template. Clear the checkbox to suppress the confirmation and immediately overwrite templates as soon as you click Save in the Save Template dialog box.
  - Template Default** – Select to have a confirmation appear when you change the default template for a screen. Clear the checkbox to suppress the confirmation and set a new default template set as soon as you click Default Template in the Templates toolbar.
  - Template Delete** – Select to have a confirmation appear before you delete an existing template. Clear the checkbox to suppress the confirmation and delete a template as soon as you click Delete in the Delete Template dialog box.
- Verify your selections and then click **OK**.

The settings take effect immediately. They remain in effect for future login sessions, until you change them again using this procedure.



## Manage Other Users




Administrator users can manage other users. This includes adding, modifying, or deleting a user.

- [Add, Modify, or Delete a User](#)
- [User Roles and Privileges](#)

### Add, Modify, or Delete a User

An administrator can add, modify, or remove other users through the STA user interface.

If you need to configure Open LDAP or IBM RACF user authentication, see the instructions for configuring an access control service provider in the *STA Installation and Configuration Guide*.

1. You must have Administrator privileges.
2. In the left navigation, expand **Setup & Administration**, then select **Users**.
3. Click **Create User** . Or select a user and click **Modify User**  or **Delete User** .
4. If creating or modifying a user, complete the dialog box, and then click **Save**.
  - *User Name*—Enter the name of the user.
  - *Description*—Enter a description of the new user, if desired.
  - *Role*—In the menu, select Administrator, Operator, or Viewer.
  - *Enter Password*—Enter the login password for the new user. It must be at least eight characters long and contain a mix of letters and numbers.
  - *Verify Password*—Reenter the password.
5. If deleting a user, select what to do with the templates and logical groups they owned:
  - **Leave them in place, make them public**—Retain all templates and logical groups owned by this username. Make them public and available to all users.
  - **Delete them**—Delete all templates and logical groups owned by this username. Note that deleting a logical group may invalidate any filters, templates, and executive reports using that logical group.

### User Roles and Privileges

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

The user role is displayed in the Main Toolbar, next to your STA username. The primary administrator user was created during STA installation and can create and maintain any number of additional users.



- **Viewer** – Has viewing access to screens on the Home, Tape System Hardware, and Tape System Activity tabs. Can only modify the appearance of screens for the current login session, filter screens, and apply templates created by users with higher privileges. Can download executive reports created by users with higher privileges.
- **Operator** – Has all privileges of the Viewer role. Also has editing privileges for some Setup & Administration screens and view-only privileges on Configuration screens. Cannot create policies or perform configuration tasks.
- **Administrator** – Has all privileges of the Operator role, plus full editing privileges for all Setup & Administration screens. Can create STA policies, define configuration settings, and create STA usernames.

Procedures in this documentation identify the user role required to access screens and perform activities. If no role is identified, then the activity can be performed by all users.

Each role comes with a set of privileges, which determine the screens and activities available to that user. Privileges are predefined and cannot be modified. The Viewer role provides the fewest privileges, while the Administrator role provides the most.

In the table below, X denotes that the user can perform the activity.

**Table 2-1 User Role Privileges, Organized by Screen**

Screen	Activity	View	Op	Adm
Preferences menu	Configure preferences for your STA username. Change the password for your STA username.	X	X	X
Templates toolbar	Apply a template to the current screen. Set the current template as the screen default for your STA username.	X	X	X
Templates toolbar	Create a template. Modify the appearance of a custom template. Save a template to a new name. Change the public or private visibility settings of a custom template owned by your STA username.	-	X	X
Home > Dashboard	Modify the screen display for this session only by adding and changing dashboard panes.	X	X	X
Home > Quick Links	Display a list of all templates available to your STA username. Navigate to a screen with the selected template applied.	X	X	X
Home > Executive Reports	Display a list of public report files run automatically or on demand. Export and view a report file.	X	X	X
Home > Executive Reports	Delete a public report file.	-	X	X

**Table 2-1 (Cont.) User Role Privileges, Organized by Screen**

Screen	Activity	View	Op	Adm
Tape System Hardware	Modify the screen display for this session only by adding and changing graphs and table attributes.	X	X	X
Tape System Hardware > Drives – Overview	Display drives assigned to the media validation drive pools.	X	X	X
Tape System Hardware > Drives – Overview	Add selected drives to a manual logical group. View logical group assignments for selected drives.	-	X	X
Tape System Hardware > Media – Overview	Add selected media to a manual logical group. View logical group assignments for selected media. Submit manual media validation requests. Resume interrupted validations of T10000T2 media.	-	X	X
Tape System Activity	Modify the screen display for this session only by adding and changing graphs and table attributes.	X	X	X
Tape System Activity > Alerts Overview	Display a list of all generated alerts. Export the alerts list to a spreadsheet or document. View detail for an alert. Change the state of an alert. Show or hide dismissed alerts.	X	X	X
Tape System Activity > Alerts Overview	Annotate an alert.	-	X	X
Tape System Activity > Media Validation Overview	Submit manual media validation requests one at a time. Reorder pending media validation requests. Cancel selected pending or in-progress media validation requests. Resume an interrupted validation of a T10000T2 media.	X	X	X
Tape System Activity > All Messages	Display a list of all SNMP traps received by STA. Export selected SNMP traps to a spreadsheet or document. View detail for a selected SNMP trap.	X	X	X

**Table 2-1 (Cont.) User Role Privileges, Organized by Screen**

Screen	Activity	View	Op	Adm
Setup & Admin > Logical Groups	Create a manual or dynamic logical group. List all drives and media assigned to a logical group. Add and remove drives and media from a manual logical group. Change the selection criteria for a dynamic logical group. Force a dynamic logical group update. Rename or delete a logical group.	-	X	X
Setup & Admin > Alerts Policies	Display a list of defined alert policies.	-	X	X
Setup & Admin > Alerts Policies	Define, copy, rename, and delete an alert policy. Change the criteria for a selected policy. Change the list of email recipients for a policy. Enable or disable an alert policy.	-	-	X
Setup & Admin > Executive Reports Policies	Display a list of public executive report policies. Run a public report on demand.	-	X	X
Setup & Admin > Executive Reports Policies	Create, modify, and delete a public report policy or a private policy created by your STA username. Display a list of public policies and private policies created by your STA username. Define a regular schedule for a report. Assign public or private ownership to a policy. Designate email addresses to receive report files. Change the dashboard template on which a report is based.	-	-	X
Setup & Admin > Templates Management	Display a list of all templates available to your STA username. Change the default screen template for your STA username. Change the public or private visibility settings of a template owned by your STA username. Rename, export, import, or delete a template. Restore the STA predefined templates.	-	X	X

Table 2-1 (Cont.) User Role Privileges, Organized by Screen

Screen	Activity	View	Op	Adm
Setup & Admin > Media Validation	Display media validation configuration settings. Display drives in the media validation drive pools. Display the list of media validation policies.	-	X	X
Setup & Admin > Media Validation	Enable or disable media validation on STA. Enable or disable drive calibration. Define, copy, rename, and delete a media validation policy. Change the criteria for a media validation policy. Enable or disable a media validation policy.	-	-	X
Setup & Admin > Service – Logs	Display a list of all available service log bundles. Create or delete a log bundle. Display run information for a log bundle. Download a log bundle to your local computer.	-	X	X
Setup & Admin > Configuration – SNMP Connections	Display SNMP client settings for STA. Display SNMP connection settings for all monitored libraries. Export SNMP connection settings for all monitored libraries to a text file.	-	X	X
Setup & Admin > Configuration – SNMP Connections	Configure SNMP client settings for STA. Configure the SNMP connection to a library. Test a library SNMP connection. Perform a manual data collection for a monitored library. Remove a library connection from STA.	-	-	X
Setup & Admin > Configuration – Users	Display a list of all STA usernames and their roles.	-	X	X
Setup & Admin > Configuration – Users	Create and modify an STA username. Change the password for an STA username. Delete an STA username.	-	-	X
Setup & Admin > Configuration – Email	Display configuration settings for the STA SMTP server. Display a list of all available email recipients and their location information.	-	X	X

**Table 2-1 (Cont.) User Role Privileges, Organized by Screen**

Screen	Activity	View	Op	Adm
Setup & Admin > Configuration – Email	Configure the STA SMTP server. Configure an available email recipient. Send a test email to an available recipient. Delete an available email recipient.	-	-	X

To see the roles required for various GUI activities, see the following:

- [User Roles for Template Activities](#)
- [User Roles for Alerts Management](#)
- [User Roles for Executive Reports and Policies](#)
- [User Roles for Media Validation Activities](#)

# 3

## Screen Layout and Navigation

Familiarize yourself with the general STA screen layout. Learn to navigate STA and modify the screen appearance.



### Note:

Do not use the browser forward and back buttons. Data may become stale or out of sync with the server. Use the left navigation tree or text links instead.

- [General Screen Layout](#)
- [Navigate Using the Left Menu](#)
- [Navigate Using Quick Links](#)
- [Navigate Using Text Links](#)
- [View Tooltips](#)
- [Adjust the Zoom](#)
- [Resize or Collapse Areas of the Screen](#)

## General Screen Layout

Most STA screens follow the same general structure and layout.

The screenshot shows the Oracle StorageTek Tape Analytics interface. The main window (3) displays a bar chart titled "Library Complex Name Total" with a Y-axis labeled "Count" ranging from 0 to 2,400. The chart shows data for various library complexes, with the highest count for SL150\_464970G+1243S. Below the chart is a table with columns for ACTION, EVALUATE, MONITOR, USE, UNKNOWN, and Total. The table data is as follows:

		ACTION	EVALUATE	MONITOR	USE	UNKNOWN	Total
SL150_464970G+1243S	1	0	0	0	0	154	154
	Media Library Number Total	0	0	0	0	154	154
SL3000_571000200056	1	0	0	0	15	9	24
	Media Library Number Total	0	0	0	15	9	24
SL3000_571000201755	1	0	0	0	0	40	40
	Media Library Number Total	0	0	0	0	40	40
SL8500 1	1	1	6	37	976	296	1316

- 1. Main Toolbar** — Provides access to user preferences, online help, and logging out. Indicates the current user.
- 2. Navigation Menu** — Primary navigation that provides direct access to all STA screens.
- 3. Main Window** — Main area of the screen where the STA content is displayed.
- 4. Templates Toolbar** — Shows the currently applied template. Allows the user to select a template, save a template, or set the default template.
- 5. Collapse Pane icon** — Indicates that the pane can be collapsed or resized, either vertically or horizontally.
- 6. Resize control bar** — Click and drag this bar to resize the screen area. The bar appears when you hover over the space between two resizable screen areas.

## Navigate Using the Left Menu

Navigate to specific screens by expanding sections of the left navigation menu and selecting a link.

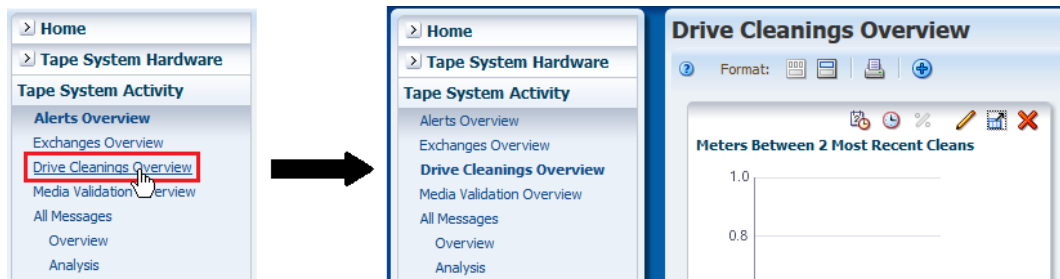
The left navigation menu has four main tabs: Home, Tape System Hardware, Tape System Activity, and Setup & Administration. Expand a tab and click a link to navigate to a screen.



1. Click a collapsed section in the left navigation menu.



2. Click a link within the currently expanded tab to display that screen.



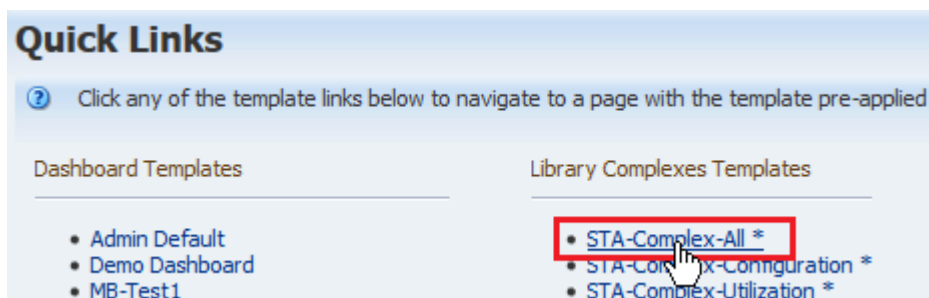
## Navigate Using Quick Links

The Quick Links page contains links to templates for the main screens of STA. Click a link to apply a template and navigate to a specific screen.

1. In the left navigation menu, expand **Home**, and then select **Quick Links**.
2. Predefined templates are identified with an asterisk (\*). Click a template in the list to navigate to that screen and load the template.

### Note:

The Quick Links page does not show STA-Default templates.



## Navigate Using Text Links

Click text links to view detailed information about the corresponding resources.

Links appear on the screen in underlined blue text for resource IDs or pivot table values. Clicking a link will apply filter criteria and take you to a corresponding screen with more information. The filter criteria remains active as you navigate to other screens. See [Filters](#) for more information.

### Resource ID Link

Click a resource ID link to go to the detail view for that resource.

The screenshot shows a table with columns: Drive Serial Number, Drive Type, and Library Complex Name. The value '576004007613' in the Drive Serial Number column is highlighted with a red box. A black arrow points from this cell to a detailed view titled 'Details for Drive 576004007613'. The details view shows the following information:

- Drive Serial Number: 576004007613
- Drive Tray Serial Number: 0729COL+1550E60125
- Drive WWNN: 50:01:04:F0:00:8A:AE:69
- Drive Type: T10000c
- Drive Health: USE
- Drive Health Trend: UNCHANGED

### Pivot Table Value Link

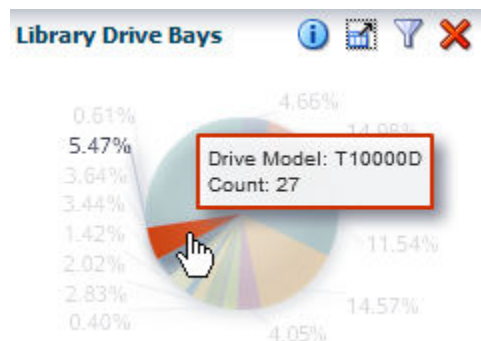
Click a value within a pivot table to go to the overview screen with a corresponding filter applied.

The screenshot shows a pivot table with columns: ACTION and EVALUATE. The value '4' in the ACTION column is highlighted with a red box. A black arrow points from this cell to an overview screen titled 'Drives - Overview'. The overview screen shows a table of drives with columns: Drive Serial Number, Drive Type, Library Complex Name, and Drive Library Name. The 'Applied Filter' is 'Drive Health: SL3000\_571000200060'. The table contains the following data:

Drive Serial Number	Drive Type	Library Complex Name	Drive Library Name
576004000904	T10000c	SL3000_57100C	crimson11
579001000173	T10000d	SL3000_57100C	crimson11
579001000247	T10000d	SL3000_57100C	crimson11
579001000314	T10000d	SL3000_57100C	crimson11

## View Tooltips

Hover over items within STA to view a tooltip with more detail about text, icons, and graphs.



## Adjust the Zoom

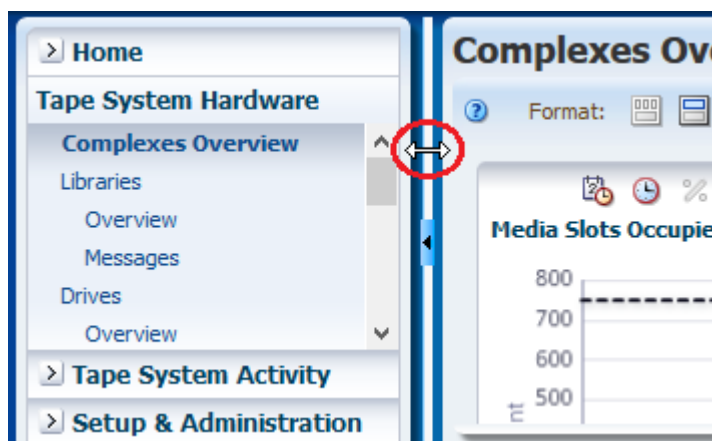
STA supports browser zoom, but zooming in too far may cause screen elements to be truncated. Avoid zooming in too far.

You can zoom in so far that the **Logout** link is truncated from the Main Toolbar. If you notice items being truncated, try to increase the size of the browser window, reduce the browser zoom, or close the browser session and log in again. This will restore the default zoom.

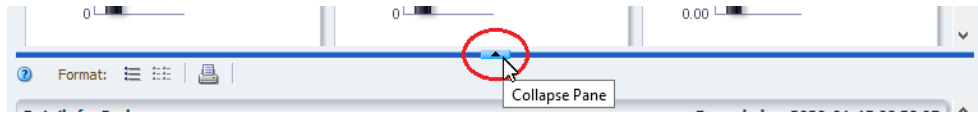
## Resize or Collapse Areas of the Screen

Resize the navigation menu, main window, tables, or graphs to fit your specific needs.

1. Move the mouse over the space between areas of the screen, until the resize control bar appears. Click and drag the bar to resize the area.



2. Toggle the **Collapse Pane** icon to collapse or restore an area of the screen.



# 4

## Graphs

Graphs display on the Dashboard, Overview, and Analysis screens. Modify how the graphs display and what data they display to better analyze your library system.

- [Types of Graphs](#)
- [Best Practices for Using Graphs](#)
- [Modify the Appearance and Arrangement of Graphs](#)
- [Modify the Data Displayed By Graphs](#)

### Types of Graphs

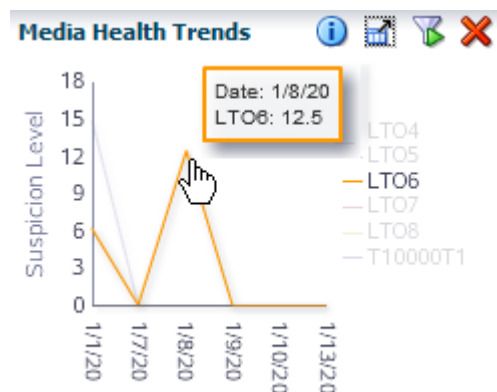
STA uses multiple graph types to display data.

- [Line Graphs](#)
- [Area Charts](#)
- [Bar Graphs](#)
- [Pie Graphs](#)
- [Spark Charts](#)

### Line Graphs

Line graphs display actual values for one or more resources over a period of time.

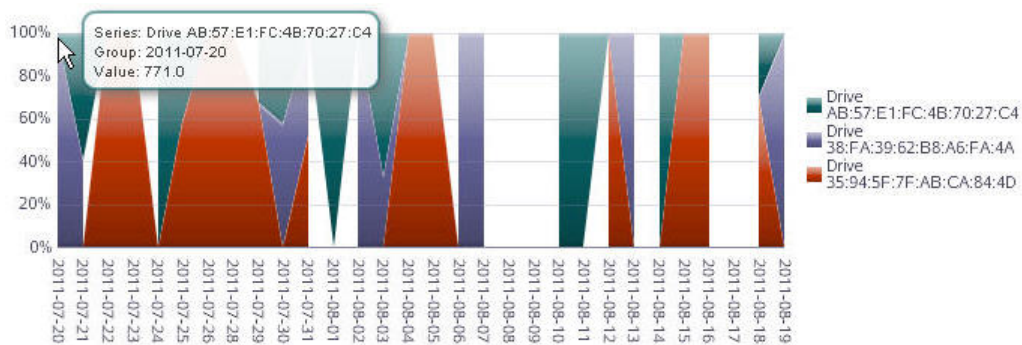
Each line represents a resource (drive or media) or other category of data. Time is always shown on the horizontal axis. Each point on the line represents an actual value at a point in time. There must be at least two data points available for a line graph. If there is only one data point, the graph will display as a bar chart. The default date range for most STA line graphs (libraries, complexes, drives, and media) is the last 30 days. For exchanges, the default is one day—the current date.



## Area Charts

Area charts show percentage values for two or more resources over a period of time.

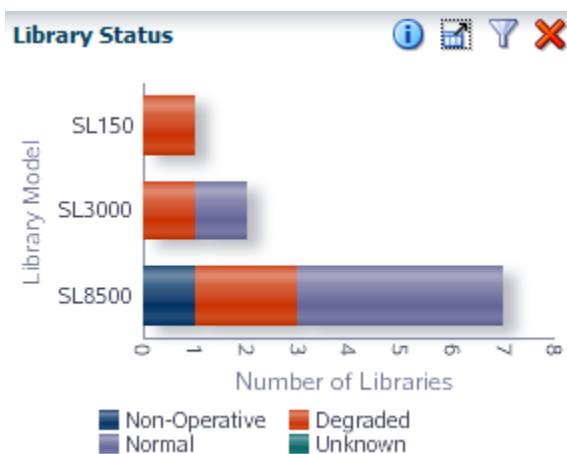
An area chart is similar to a line graph, but the area under the line is filled in with a color or pattern. Each line represents a resource or other category of data, and the size of the area under the line represents the resource's percentage of the total. Time is always displayed on the horizontal axis. Each point on the line represents an actual data value at a point in time. The default date range for most STA area charts (libraries, complexes, drives, and media) is the last 30 days. For exchanges, the default is one day—the current date.



## Bar Graphs

Bar graphs display actual values for one or more resources at a point in time.

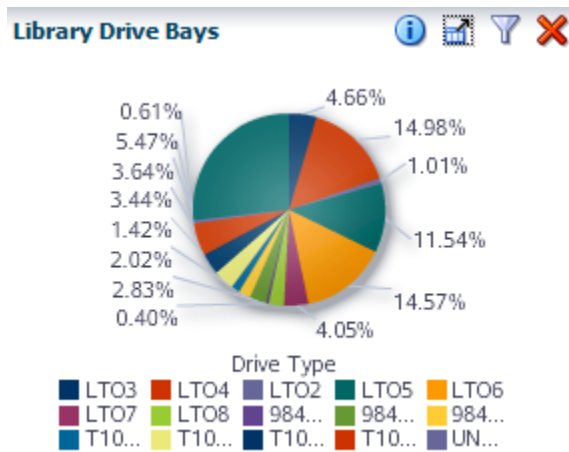
Each bar represents a resource (drive, media, library) or other category of data, and the size of the bar represents the resource's actual value.



## Pie Graphs

Pie graphs show the percentage of a resource compared to the total.

Each section of the pie represents a resource or other category of data. The size of the section represents the resource's percentage of the total. To be meaningful, pie charts require graphing at least two resources.



## Spark Charts

A spark chart is a small line graph that plots up to four key values—Start, End, High, and Low—for a date range. Spark charts can help you to see patterns in data values over time.

Some dashboard panes contain embedded spark charts. Depending on the date range selected and the variation among the key values, a given chart may have only two or three dots plotted, rather than four. This is because the dot for one value may hide the other if two key values are close in date and value. Filtering for a shorter date range may reveal more detail.

Type	Start Value	Trend Data	End Value	High Value	Low Value
Media Slots Installed	15,781		15,781	15,781	15,781
Media Slots Activated	9,910		9,910	9,910	9,910
Media Slots Occupied	5,590		6,361	6,361	5,580
Media Removed	0		469	469	0
Media Utilized (> 0.0)	273		279	281	273
Media Blank (< 0.0)	29		32	32	29
Media Unknown/None	5,288		6,050	6,050	5,269

## Best Practices for Using Graphs

Follow best practices when working with graphs in STA to maximize their usefulness.

### Hide graphs to make space for the table

Collapse the graphs area of the screen to provide more space to view a table. You can save this view as a default template if the table details are more useful in your environment than the graphical overview.

See [Resize or Collapse Areas of the Screen](#).

See [Save a Template](#) and [Set the Default Template for a Screen](#).

### Compare to the system average

The dotted black line shown by default in all graphs shows a summary or average across your tape library system. This provides a good comparative baseline.

### Add individual resources to graphs

Add specific resources (drives, media, and so on) to the graphs. This is a powerful tool for comparing resources within your tape library system.

See [Add Library Resources to Graphs](#).

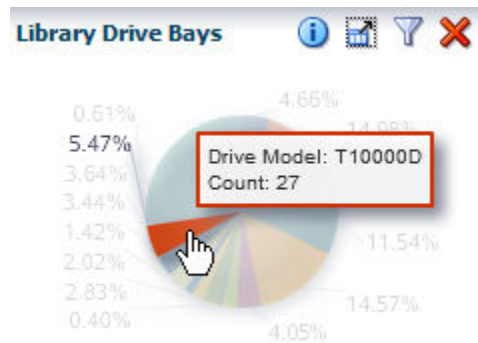
### Synchronize the date and time range on graphs

Synchronize date and time ranges on the Overview screen graphs to provide a good way to compare resources across multiple data ranges. Change the date and time range in one graph and then synchronize the other graphs to it.

See [Synchronize a Date Range Across All Graphs](#).

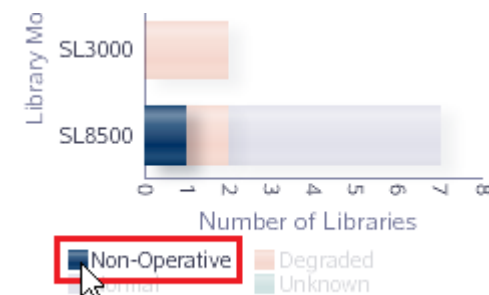
### Display Detailed Values

Move the mouse over a areas of a graph to display the value in a tooltip. Other items within the graph are dimmed.



### Highlight Values

Move the mouse over an area of the legend to highlight that entry in the graph. All other entries remain on the graph but are dimmed.






# Modify the Appearance and Arrangement of Graphs

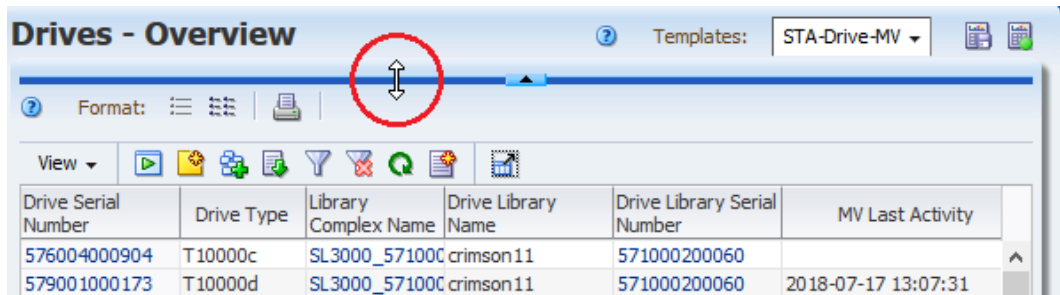
Adjust how graphs display within STA to help analyze data.

- [Restore the Graph Area](#)
- [Detach a Graph Pane](#)
- [Move Graph Panes on an Overview Screen](#)
- [Add or Remove a Graph Pane on an Overview Screen](#)
- [Switch Between Narrow and Wide View Graphs](#)
- [Print Graphs](#)

## Restore the Graph Area

Some templates and pages do not automatically display the graph area. If clicking the collapse pane icon has no effect, you must manually unhide the graph area.

1. Toggle the collapse pane icon so that it is up .
2. Hover the cursor to the left or right of the icon, then click and drag the bar down.



**See also:**

- [Resize or Collapse Areas of the Screen](#)

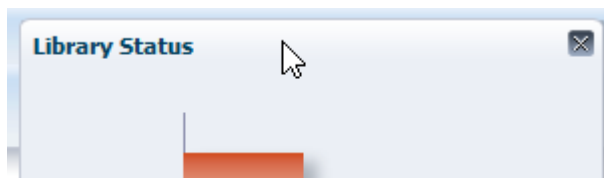
## Detach a Graph Pane

Detach a pane to view the graph in closer detail.

1. Click **Detach Pane**  in the graph's toolbar.



2. To move the detached pane, click and drag the top border.



3. To resize the detached pane, click and drag an edge or corner.



4. To restore the graph pane to its normal position, click **Close**. If you navigate to another screen, the pane is automatically closed.

## Move Graph Panes on an Overview Screen

Rearrange graph panes on an Overview screen to change the order of the graphs.


1. Hover over the top of the graph. The **Move Object** cursor appears.

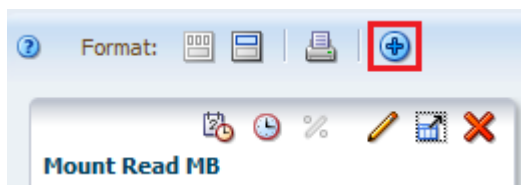


2. Click and drag the pane to its new location.
3. Once the pane is near the position you want, release the cursor. The pane snaps into place. You do not need to position it exactly.


## Add or Remove a Graph Pane on an Overview Screen

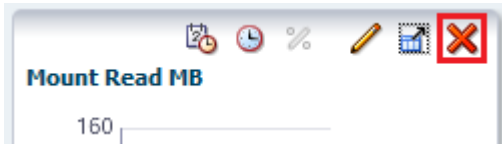
Add or remove graphs in the graph area of an Overview screen.

1. Click **Add Graph**  near the top of an Overview screen.



2. STA adds a graph with the default attribute and places it at the end of the graph area. You may need to scroll down to locate it.
3. To adjust the graph, see:
  - [Move Graph Panes on an Overview Screen](#).

- Change the Graphed Attribute.
4. To remove the graph, click **Remove Pane**  on the graph's toolbar.




### How a Newly Added Graph Displays Data

- The graph displays the default attribute for the resource type. You can change the attribute to any available attribute for the resource.
- If the existing graph panes have all been synchronized to the same date range, the new graph uses the synchronized range. Otherwise, the graph uses the system default date range of the previous 30 days.
- The new graph displays actual values, even if all the existing graphs display percentages.
- If individual resources have been applied to the existing graphs, the new graph displays the those resources as well.

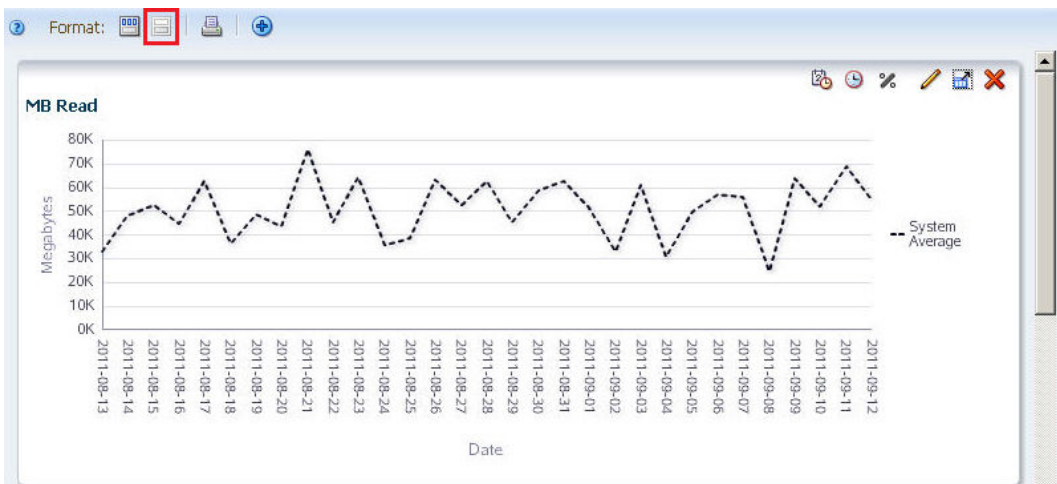
## Switch Between Narrow and Wide View Graphs


On Overview or Analysis screens, you can display graphs in narrow or wide format.

Narrow view is the default, and it allows side-by-side comparisons. Wide view allows you to see each graph in greater detail.

1. Click **Wide View**  on the graphics area toolbar.

The graphs display individually across the width of the screen. Scroll down to view the graphs.




2. To switch back to narrow view, click **Narrow View**  in the graphics area toolbar. The graphs display side-by-side.



## Print Graphs

Print all graphs currently displayed.

1. For best results, you might want to display the graphs in Wide View mode. This will allow you to see more detail in the printed graphs.  
 See [Switch Between Narrow and Wide View Graphs](#).
2. Click **Printable Graphs**  on the graphics area toolbar.
3. A new tab is created in your browser window, showing all graphs in a printable format. Use the browser's print function to send this display to a printer.

## Modify the Data Displayed By Graphs

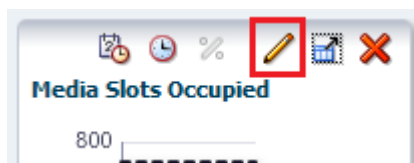
Modify the data displayed on one or more graph panes to help with analysis.

- [Change the Graphed Attribute](#)
- [Set the Date Range of a Graph](#)
- [Synchronize a Date Range Across All Graphs](#)
- [Add Library Resources to Graphs](#)
- [Switch Between Actual and Percentage Values](#)
- [Graph Data for a Pivot Table Attribute](#)
- [Graph Data for a Pivot Table Layer](#)
- [Add Table Data to Graphs](#)

## Change the Graphed Attribute

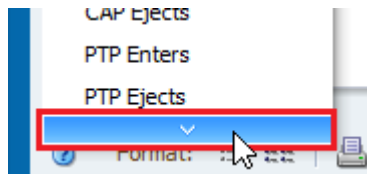
Change the resource attribute displayed in a graph on an Overview screen.

1. Click **Change Graphed Attribute**  in the graph's toolbar.



2. From the drop-down, select the attribute to display.

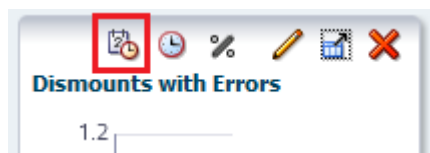
The menu lists all available attributes for this resource type. You may need to scroll down within the list.





## Set the Date Range of a Graph

Change the date range of a graph on an Overview screen. You can specify a new range or a point in time (single day).

1. Click **Choose Date Range**  in the graph's toolbar.



2. Complete the dialog box, specifying either:


- **Single Date** — Either type the date manually or click **Select Date**  and choose the date. The date format is `yyyy-mm-dd`.
- **Date Range** — In the and fields, enter the first and last dates of the range. Type the dates manually or click **Select Date**  and choose the dates. The date format is `yyyy-mm-dd`.

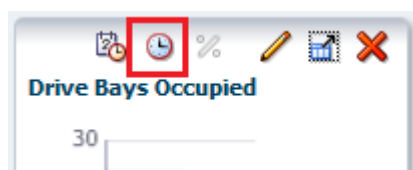
3. Click **OK**.

Single date graphs are displayed as bar charts. Date range graphs are displayed as line graphs

## Synchronize a Date Range Across All Graphs

Synchronize all graphs to the same date range on an Overview screen. This can help compare data.

1. In one of the graphs, set the date range.
2. Click **Synchronize Date Range**  in the graph's toolbar.



3. Confirm you want to synchronize all graphs.


The page reloads with all graph panes synchronized to display the same date range. All other data characteristics (graphed attribute, actual versus percentage values, added resources) remain unchanged.

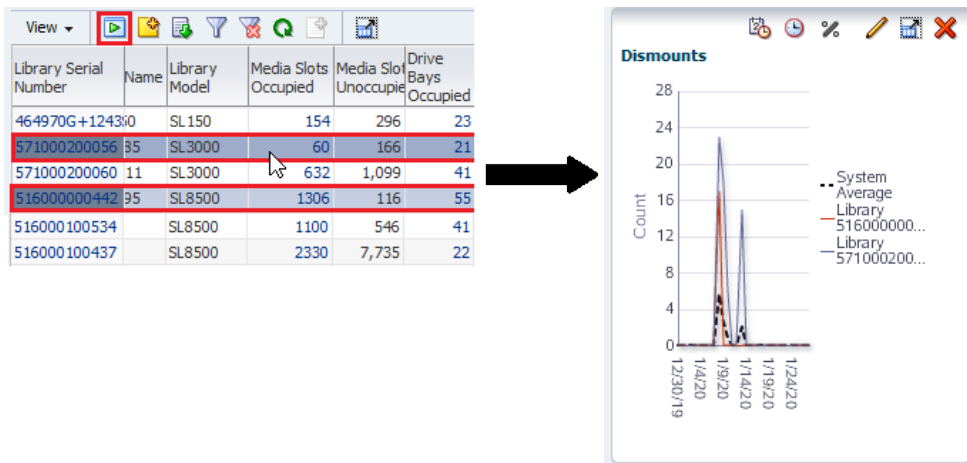
**See Also:**

- [Set the Date Range of a Graph](#)

## Add Library Resources to Graphs

Initially graphs only show the system average. Add library resources (such as libraries, drives, or media) to all graphs on an Overview screen to view trends.

1. In the table, select a row (or use shift-click/ctrl-click to select multiple rows).
2. Click **Apply Selection**  in the table toolbar. The graphs update with the selected resources.




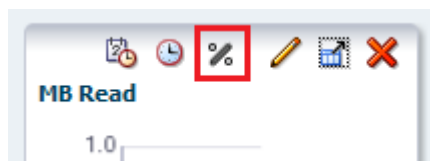
3. To remove all resources from the graphs and display only the System Average, deselect all the selected resources in the table and click **Apply Selection** again.

## Switch Between Actual and Percentage Values

Switch between actual and percentage values on the graphs of an Overview or Analysis screen.

Actual values are displayed by default. Percentage values compare resources, therefore you should have at least two resources added to the graph when displaying percentage values.

1. Add two or more resources to the graph.
2. Click **Show Percentages**  on the graph's toolbar.



3. Click **Show Percentages**  again to switch back to actual values.

**See Also:**

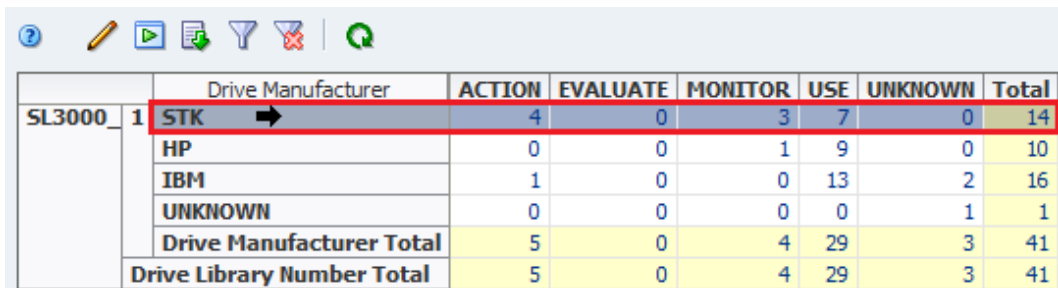
- [Add Library Resources to Graphs](#)

## Graph Data for a Pivot Table Attribute

Graph detail data for a pivot table attribute.

1. Navigate to an **Analysis** screen (such as Drives Analysis).
2. In the pivot table, select a row (in the example below, the "STK" value for the Drive Manufacturer attribute is selected).

If you select a column edge attribute, or if you select multiple rows, you will see the error, "Please select one and only one row."



	Drive Manufacturer	ACTION	EVALUATE	MONITOR	USE	UNKNOWN	Total
SL3000_1	<b>STK</b> →	4	0	3	7	0	14
	HP	0	0	1	9	0	10
	IBM	1	0	0	13	2	16
	UNKNOWN	0	0	0	0	1	1
	<b>Drive Manufacturer Total</b>	5	0	4	29	3	41
	<b>Drive Library Number Total</b>	5	0	4	29	3	41

3. Click **Apply Selection**  in the Pivot Table Toolbar.

The selected attribute value is displayed in a single graph pane.

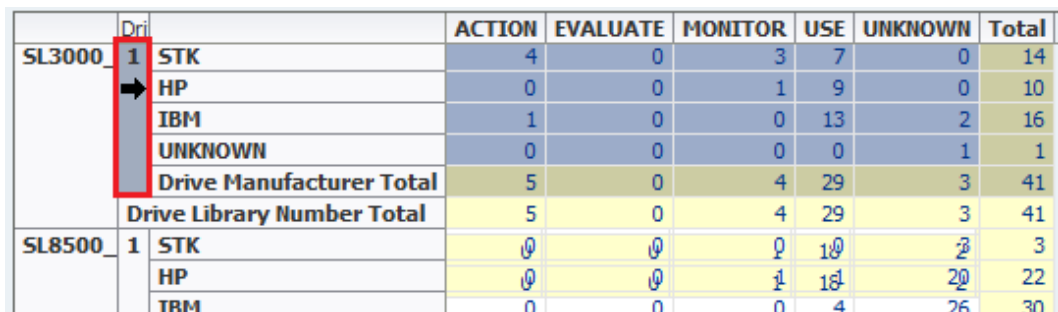
**See Also:**

- [Modify a Pivot Table](#)

## Graph Data for a Pivot Table Layer

Graph data for an entire pivot table layer to view multiple graph panes: one for the cumulative totals and one for each of the attribute values included in the totals.

1. Navigate to an **Analysis** screen (such as Drives Analysis).
2. In the pivot table, select a layer that contains multiple values (in this example below, the nesting layer "Library Number" is selected, which contains data for multiple drive manufacturers).

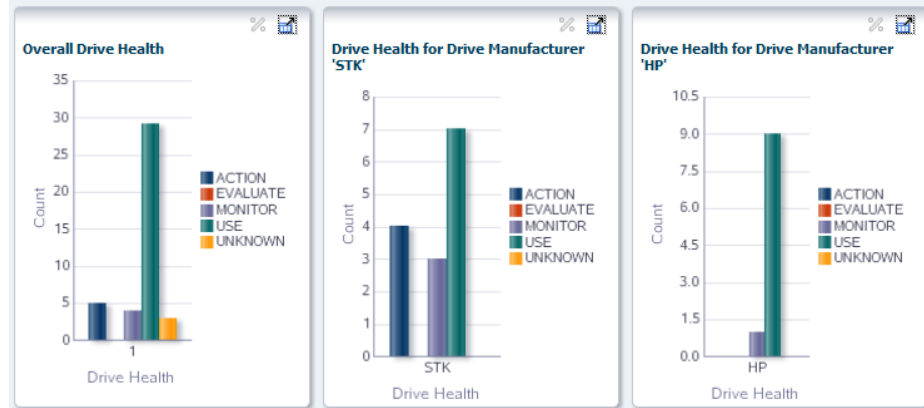


	Drive Manufacturer	ACTION	EVALUATE	MONITOR	USE	UNKNOWN	Total
SL3000_1	<b>STK</b> →	4	0	3	7	0	14
	HP	0	0	1	9	0	10
	IBM	1	0	0	13	2	16
	UNKNOWN	0	0	0	0	1	1
	<b>Drive Manufacturer Total</b>	5	0	4	29	3	41
	<b>Drive Library Number Total</b>	5	0	4	29	3	41
SL8500_1	STK	0	0	0	10	2	3
	HP	0	0	1	18	20	22
	IBM	0	0	0	4	26	30

3. Click **Apply Selection**  above the table.

The Graphics Area is updated as follows:

- The left-most pane shows the summary data for the attribute.
- The panes to the right show detail for each attribute (in this case: STK and HP).



**See Also:**

- [Modify a Pivot Table](#)



# 5

## Tables

Tables appear on Overview and Analysis screens. You can sort, rearrange columns, and export table data to better analyze your library system. STA uses both standard tables and pivot tables to display data.

- [Modify a Table](#)
- [Modify a Pivot Table](#)
- [Add Table Data to Graphs](#)
- [Export Table Data to a Spreadsheet or Document](#)
- [Select Multiple Rows in a Table or List](#)

### Modify a Table

Modify the display of the table to help analyze your library system.

- [Detach a Table](#)
- [Reorder Columns](#)
- [Resize Column Width](#)
- [Sort by a Single Column](#)
- [Sort by Multiple Columns](#)
- [Hide and Reveal Columns](#)
- [Display a Specific Table Page](#)
- [Display Details for One or More Resources](#)
- [Annotate a Table Row](#)
- [Print a Table](#)
- [Refresh the Table Display](#)

### Detach a Table

Detach a table to display it in a separate window so that you can resize and move it within the browser window. You can detach one table at a time.

1. Click the **Detach**  icon in the table toolbar.



2. To restore the table to its normal position, click **Close** within the detached window.

## Reorder Columns

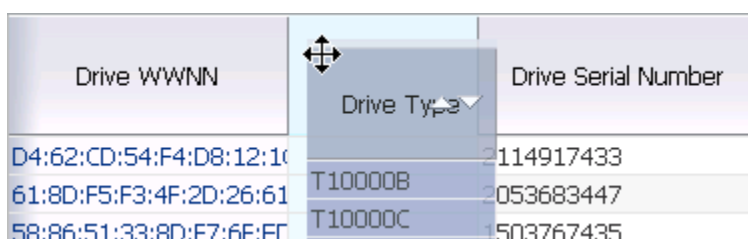
Move table columns into an order that helps you best see the data.

### By Mouse

1. Click and drag the column heading. The cursor changes to the Move object cursor.

#### Note:

The column on the far-left is fixed and cannot be moved.

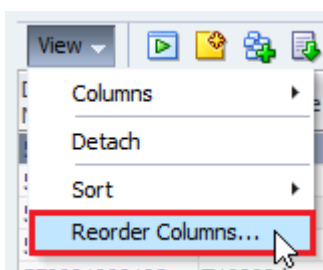


Drive WWNN	Drive Type	Drive Serial Number
D4:62:CD:54:F4:D8:12:10	T10000B	114917433
61:8D:F5:F3:4F:2D:26:61	T10000C	053683447
58:86:51:33:8D:F7:6F:FF	T10000C	503767435

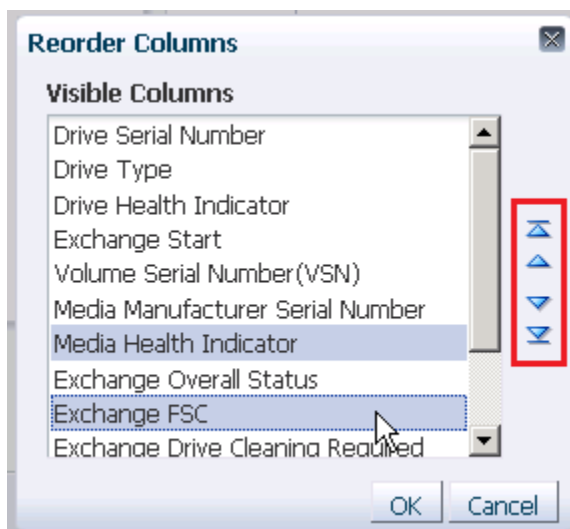
2. Once the column is close to the position you want, release the cursor. The column snaps into place. You do not need to position it exactly.

### By Menu

1. From the **View** drop-down in the table toolbar, select **Reorder Columns...**



2. In the list, select the columns you want to move.



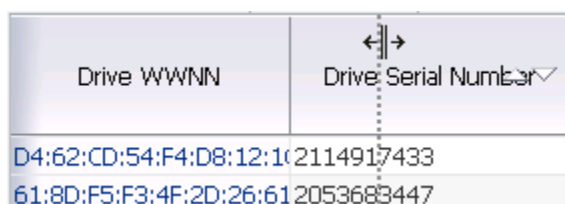
3. Click the **up** and **down** arrows on the right of the dialog to reorder the items. Moving items up in the list moves the column left in the table.
4. Repeat this process until the list is arranged the way you want, and then click **OK**.

## Resize Column Width

Adjust the width of a table column to better view the data.

### By Mouse

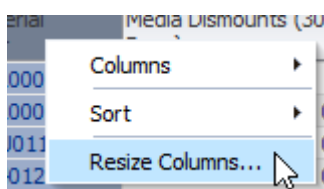
1. Hover over the right-hand border of the column heading.
2. Click and drag the border. A dotted vertical line appears to indicate the pending width.



3. When the column is the width you want, release the cursor. The column is resized. All other columns retain their original widths.

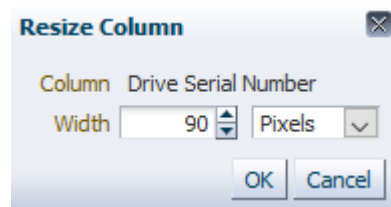
### By Menu

1. Right-click the heading of the column, and select **Resize Columns...**



2. Adjust the width using either **Pixels** or **Percent**.

If adjusting by percentage, the current width is multiplied by the percentage to calculate the new width. For example: an entry of 200 doubles the current width. An entry of 25 reduces the current width to one-quarter of what it is now.



3. Click **OK**.

## Sort by a Single Column

Sort the table by a single column to help breakdown the data.

For screens that include a `Page Number` field (Exchanges, Drive Cleanings, and Messages), the sort applies only to the records displayed on the current page.

### By Mouse

Hover over a column heading, then click either **Ascending** ▲ or **Descending** ▼.

Drive WWNN	Drive Serial Number	Drive Type
D4:62:CD:54:F4:D8:12:10	2114917433	
61:8D:F5:F3:4F:2D:26:61	2053683447	T10000C

### Note:

You cannot sort the first column with the mouse. Use the menu method instead.

### By Menu

Right-click the heading of the column. Select **Sort**, then **Ascending** or **Descending**.

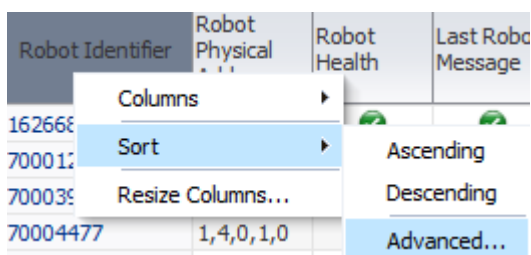
Drive Serial Number	Drive Type	Library Complex Name	Drive Library Name
576004000119			elih 1R
576004007613			
579001000352			
579004005210	T10000d	SL8500_2	

## Sort by Multiple Columns

Sort the table using up to three columns to help breakdown the data.

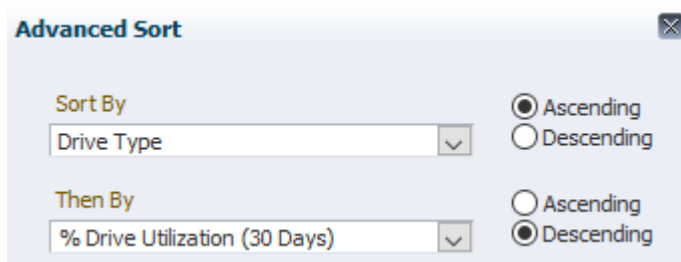
For screens that include a `Page Number` field (Exchanges, Drive Cleanings, and Messages), the sort applies only to the records displayed on the current page.

1. Right-click a column heading, then select **Sort**, then **Advanced...**



Robot Identifier	Robot Physical	Robot Health	Last Robot Message
162668			
700012			
700039			
70004477	1,4,0,1,0		

2. In the Sort By menu, select the column for the primary sort. Select either the **Ascending** or **Descending** options.



**Advanced Sort**

Sort By: Drive Type  Ascending  Descending

Then By: % Drive Utilization (30 Days)  Ascending  Descending

3. Repeat for up to three sorting criteria. Click **OK**.

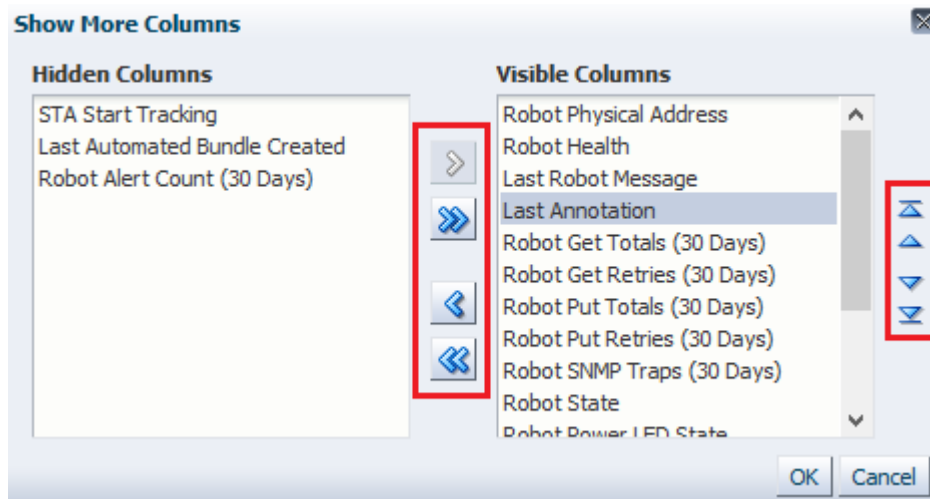
The table data is sorted according to your selections, and the column headers indicate the sort criteria.

Drive Serial Number	Drive Type	% Drive Utilization (30 Days)
576004007613	T10000c	0.00
576004000119	T10000c	0.00

## Hide and Reveal Columns

Select which columns appear in the table. Hiding columns can help to see critical data.

1. From the **View** drop-down `View`, select **Columns**, then **Show More Columns...**
2. Use the **left** and **right** arrows to move the columns between the Hidden and Visible lists. Use the **up** and **down** arrows to re-order the Visible columns.



## Display a Specific Table Page

Messages, Alerts, Exchanges, and Drive Clearings screens display records grouped into pages each with 1,000 records.

Use the **Page Number** field in the toolbar to select the page to display.

Page Number:  of 4

Note that sorting only applies to the currently displayed page.

## Display Details for One or More Resources

Display detailed information for one or more resources (such as media, libraries, drives, and so on).

1. In the table, select a row (or use shift-click/ctrl-click to select multiple rows).

Exchange Start	Drive Serial Number	Drive Model	Drive Health	Volume Serial Number
2019-03-08 15:45:16	10WT000134	LTO8	✓	SF8486
2019-03-08 15:41:38	10WT000134	LTO8	✓	SF8486
2019-03-08 15:38:01	10WT000134	LTO8	✓	SF8486
2019-03-08 15:34:21	10WT000134	LTO8	✓	SF8486
2019-03-08 15:30:43	10WT000134	LTO8	✓	SF8486

2. Click **Detail View** in the table toolbar.



- If you have selected multiple resources, they are displayed in order of ID. Scroll down to see all records.




- To return to the table, click **List View** in the toolbar.



## Annotate a Table Row


Annotations allow the Operator or Administrator to attach a 250 character comment to selected records. Users with Viewer privileges can display annotations but cannot create or modify them.

- Select a table row (or use shift-click/ctrl-click to select multiple rows).  
If you do not select any records, the annotation will apply to all records currently displayed.
- Click **Add/Edit Annotation**  in the table toolbar.
- Type up to 250 characters in the text field. There are no formatting options, such as boldface, color, or line feeds.
- Click **Save Annotation**.

## Print a Table

Print the currently displayed table data.

This does not print all data in the table, only the data currently on the screen. To print all the table data, export the table data to a file and then print it. See [Export Table Data to a Spreadsheet or Document](#).

- Scroll to the area of the table that you want to print.
- Click **Printable Table**  on the table toolbar.
- Use the browser's standard Print function to send this display to a printer.

## Refresh the Table Display

Do not use the browser refresh button. Update the table data using the refresh icon in the table toolbar.

Click **Refresh Table**  in the table toolbar.

## Modify a Pivot Table

Analysis screens contain pivot tables to help breakdown data. Modify the layout of pivot tables to compile data in different ways.

- [What Are Pivot Tables?](#)
- [View the Name of a Pivot Table Layer](#)
- [Resize a Column or Row of a Pivot Table](#)
- [Display Details for a Pivot Table Value](#)
- [Move Pivot Table Layers](#)
- [Change Pivot Table Attributes and Nesting Order](#)

## What Are Pivot Tables?

Pivot tables show data compiled into different layers to help breakdown data without the need to open multiple windows or export data to a spreadsheet.

Each layer in a pivot table represents filter criteria. Pivot tables can display from two to seven filter criteria. Two is the minimum because there must be one for each table edge. For example, you can use pivot tables to look at the health of drives, not just by library location, but also by drive type, firmware level, and many other attributes.

The format of a pivot table is dynamic in that you can change the way the data is organized simply by dragging and dropping (also known as pivoting) the layers from one area to another. Moving a layer within the same edge changes the nesting order. Moving a layer to the opposite edge (moving a layer from row to column edge, for example) adds the layer there.

Below is a sample pivot table:

			ACTION	EVALUATE	MONITOR	USE	UNKNOWN	Total
SL8500_2	1	STK	0	0	0	4	0	4
		<b>Drive Manufacturer Total</b>	0	0	0	4	0	4
		<b>Drive Library Number Total</b>	0	0	0	4	0	4
<b>Library Complex Name Total</b>			0	0	0	4	0	4

- There is one column layer on the top edge of the table: Drive Health Indicator with Action, Evaluate, Monitor, Use, Unknown, and Total.
- There are three row layers on the left edge of the table: Library Complex Name, Library Number, and Drive Manufacturer. The layers are nested from left (outer) to right (inner). In this example, Library Complex Name is the outermost layer, and Drive Manufacturer is the innermost.

The values in each table cell are the result of the filter criteria intrinsic to each table layer, joined by "AND" statements. For example, in the table above the cell at the intersection of the SL8500\_1, STK row and USE column has the value "4". This value is the result of the following filter criteria:

- Library Complex Is SL8500\_2, AND



- Library Number Is 1, AND
- Library Manufacturer Is STK, AND
- Drive Health Indicator Is USE

The values in each pivot table cell are active links. These links provide access to additional details about the items included in the count.

See [Navigate Using Text Links](#).

## View the Name of a Pivot Table Layer

Display the attribute name for a pivot table layer.

- Hover over a row or column to view the corresponding attribute name. The attribute name displays at the top (for columns) or to the left (for rows).

		Drive Health	ACTION	EVALUATE	MONITOR
SL150_4	1	HP	0	0	0
		IBM	0	0	0
		Drive Manufacturer Total	0	0	0
		Drive Library Number Total	0	0	0

## Resize a Column or Row of a Pivot Table

Adjust the width and height of the columns or rows to better view the data.

### By Mouse

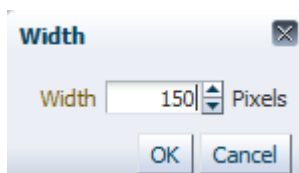
1. Hover over the heading border.
2. Click and drag the border. A dotted line appears to indicate the pending size.

			ACT
SL150_464970G+1243SY0226	1	HP	
		IBM	
		Drive Manufacturer Total	
		Drive Library Number Total	
SL3000_571000200056	1	IBM	

3. When the cell is properly sized, release the cursor.

### By Menu

1. Right-click a heading, and then select **Height...** or **Width...**
2. Set the new **Pixel** size.

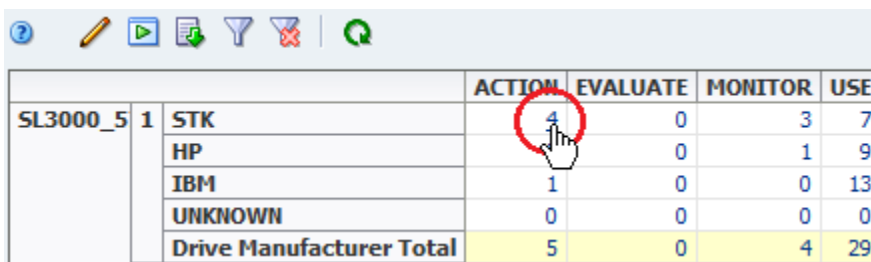


3. Click **OK**.

## Display Details for a Pivot Table Value

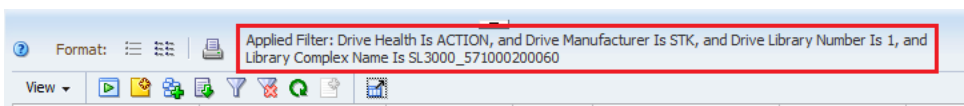
Click a value within a pivot table to view more details about the associated resources.

1. Click the active link of the pivot table value.



			ACTION	EVALUATE	MONITOR	USE
SL3000_5	1	STK	4	0	3	7
		HP		0	1	9
		IBM	1	0	0	13
		UNKNOWN	0	0	0	0
		<b>Drive Manufacturer Total</b>	5	0	4	29

The associated Overview screen displays with a filter applied that corresponds to the value.



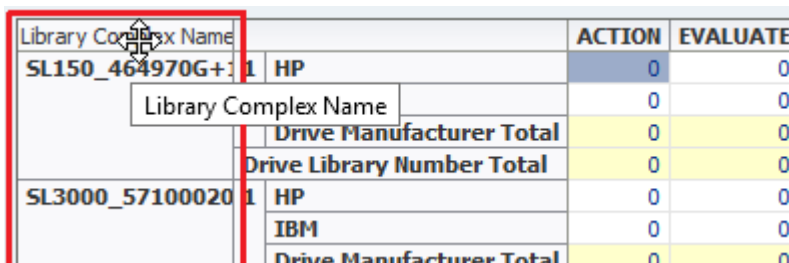
			ACTION	EVALUATE	MONITOR	USE
SL150_464970G+	1	HP	0	0		
		Library Complex Name		0	0	
		<b>Drive Manufacturer Total</b>	0	0		
		<b>Drive Library Number Total</b>	0	0		
SL3000_57100020	1	HP	0	0		
		IBM	0	0		
		<b>Drive Manufacturer Total</b>	0	0		

2. Click any active links on this screen to get to additional information.

## Move Pivot Table Layers

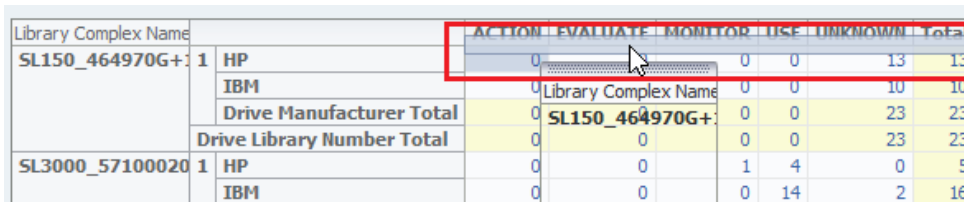
Rearrange pivot table layers to better analyze data.

1. Hover over a heading, until the layer's name appears.



Library Complex Name			ACTION	EVALUATE
SL150_464970G+	1	HP	0	0
		Library Complex Name		0
		<b>Drive Manufacturer Total</b>	0	0
		<b>Drive Library Number Total</b>	0	0
SL3000_57100020	1	HP	0	0
		IBM	0	0
		<b>Drive Manufacturer Total</b>	0	0

2. Click and drag the layer to a new location.




Library Complex Name			ACTION	EVALUATE	MONITOR	USE	UNKNOWN	Total
SL150_464970G+	1	HP	0	0	0	0	13	13
		IBM	0	0	0	0	10	10
		<b>Drive Manufacturer Total</b>	0	0	0	0	23	23
		<b>Drive Library Number Total</b>	0	0	0	0	23	23
SL3000_57100020	1	HP	0	0	1	4	0	5
		IBM	0	0	0	14	2	16

When you release the cursor, the table is reorganized and the aggregate counts in the data cells are re-calculated.

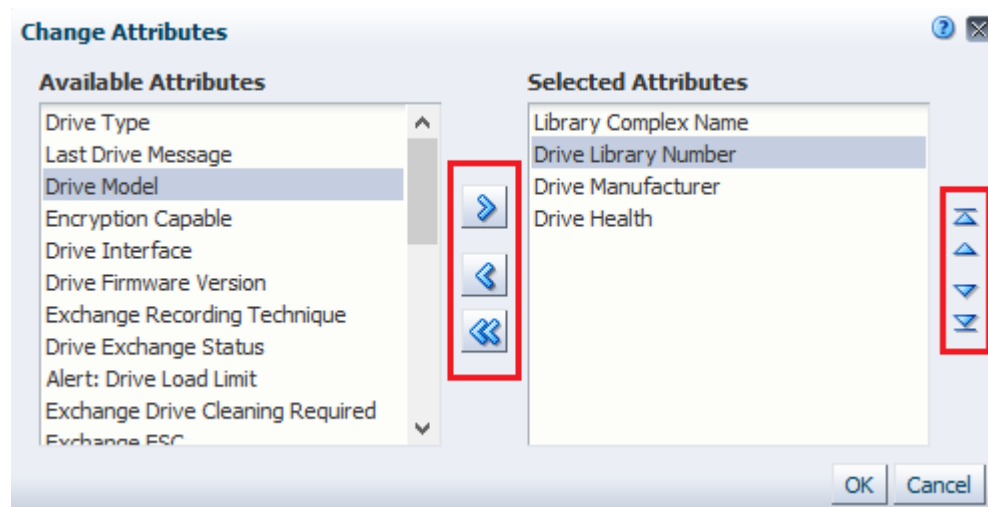
## Change Pivot Table Attributes and Nesting Order

Choose which attributes to display in the pivot table. Change the order in which they are nested.

1. Click **Change Attributes**  in the pivot table toolbar.
2. Select an attribute (shift- or ctrl-click to select multiples).

Use the **left** and **right** arrows to move the attributes between the *Available* and *Selected* lists. Use the **up** and **down** arrows to order the selected attributes.


Pivot tables can have between two and seven attributes.

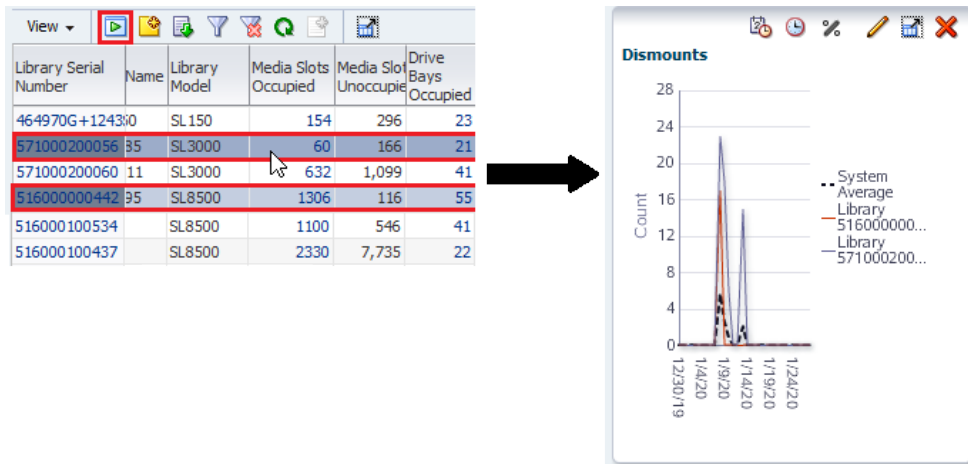


3. Verify the attributes you want are in the **Selected Attributes** list and in the proper order. Click **OK**.

## Add Table Data to Graphs

Select rows of a table and apply the selection to add data to the graphs.


1. In the table, select a row (or use shift-click/ctrl-click to select multiple rows).
2. Click **Apply Selection**  in the table toolbar. The graphs update with the selected resources.

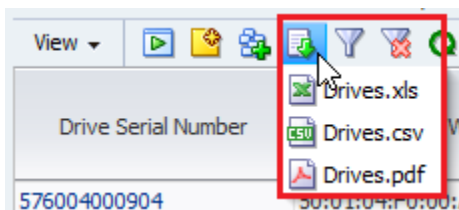


- To remove all resources from the graphs and display only the System Average, deselect all the selected resources in the table and click **Apply Selection** again.

## Export Table Data to a Spreadsheet or Document

Export a table to a file for further analysis using an third party software application.

- Set up the table so it contains all the data you want to export.
  - If you have applied a filter to the table, the spreadsheet includes only the records that match the criteria you have specified.
  - Data records and attributes currently scrolled off the visible portion of the screen are included.
  - Hidden attributes are not included.
- Click **Export**  in the toolbar, and then select the format.



- XLS** – The file is given a `.xls` extension, but the data is actually saved in HTML format. The file can be opened with either a browser or a spreadsheet application, such as Microsoft Excel.
  - CSV** – Comma Separated Values file, which can be opened with a variety of spreadsheet applications.
  - PDF** – Portable Document Format file, which can be opened with Adobe Reader.
- Save the file to a location on your local system.

For large amounts of data, it may take several minutes to create the file. You may not receive any screen feedback while the file is being created.

4. Open the .xls or .csv file in a spreadsheet application (such as Microsoft Excel).

 **Note:**

For .xls files, the extension of the file is .xls, but the format is html. When opening the file in a spreadsheet program, you may be required to verify that the file is not corrupt and from a trusted source.

You can also open the file in a browser, but the content will be view only.

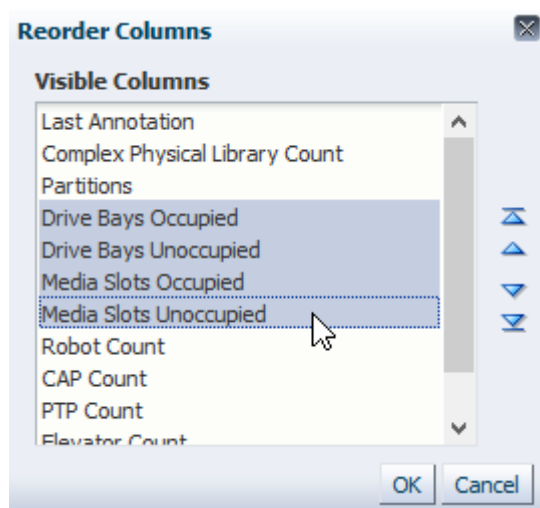
5. You may need to change the cell format of some columns to properly view the data.  
For example, Drive Serial Numbers may display in scientific format and will need to be changed to Number format with 0 decimals.

## Select Multiple Rows in a Table or List

Select multiple items in a table or list using shift-click and ctrl-click. This can be useful to add multiple resources to a graph or modify multiple items at a time.

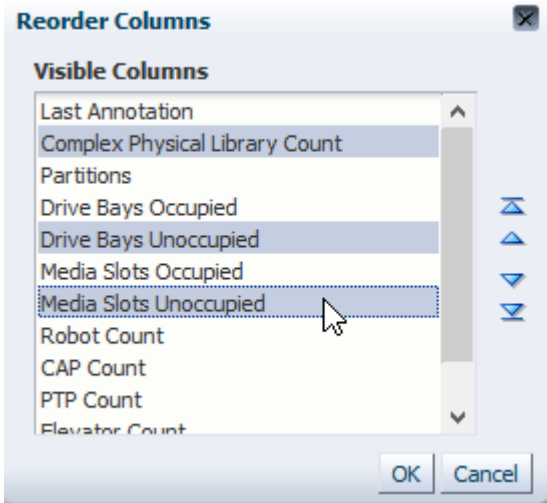
### Shift+click

To select a range of items, hold down the shift key and then click on the top item followed by the bottom item.



### Ctrl+click

To select multiple items that are not in a range, hold down the ctrl key and then click on each item.



# 6

## Dashboard

The dashboard is the first screen you see after logging in. It consists of multiple panes, each showing different data for your tape library system. You can save the dashboard layout as a template.

- [View the Dashboard](#)
- [Customize the Dashboard](#)
- [Dashboard Pane Types](#)

**See Also:**

- [Customize a Template](#)

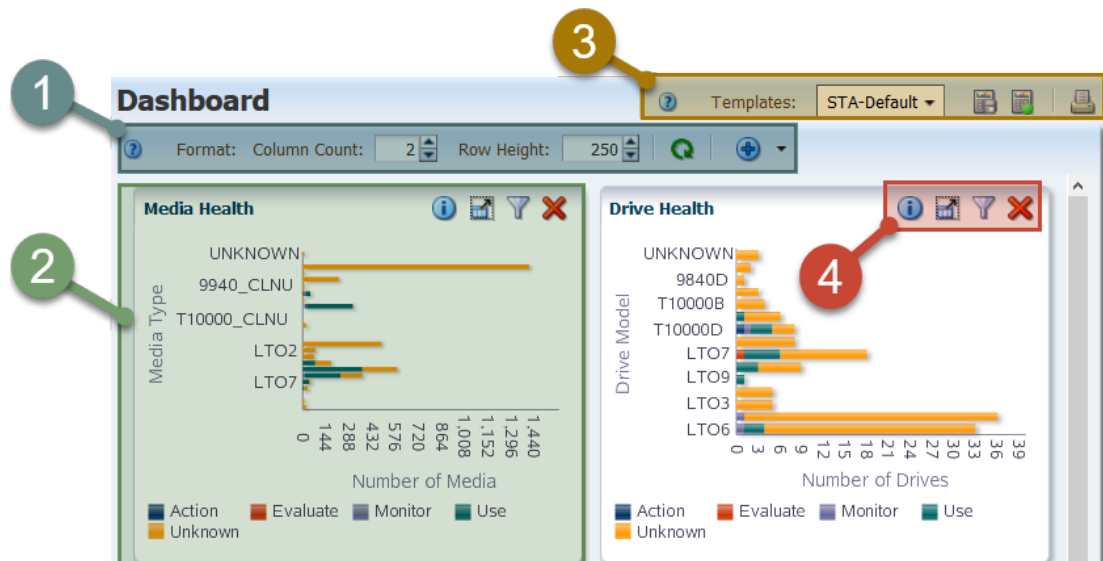
### View the Dashboard

View data on the dashboard to get a high-level view of your tape library system.

- [Dashboard Layout](#)
- [Link to Details from a Dashboard Pane](#)
- [Detach a Pane to View More Detail](#)
- [View the Dashboard on a Mobile Device](#)
- [Why is the dashboard taking a long time to load?](#)

### Dashboard Layout

The dashboard consists of the dashboard toolbar, template toolbar, and dashboard pane area.



1. **Dashboard Toolbar** — Add a pane or change the number and size of the dashboard panes displayed.
2. **Dashboard Pane** — Dashboard panes are arranged in columns and rows. Each pane shows a different high-level view of your tape library system.
3. **Template Toolbar** — Select a template, save a template, or set the default template for the screen.
4. **Pane Toolbar** — Annotate the dashboard pane, detach the pane, or filter the data.

#### Times Displayed on the Dashboard

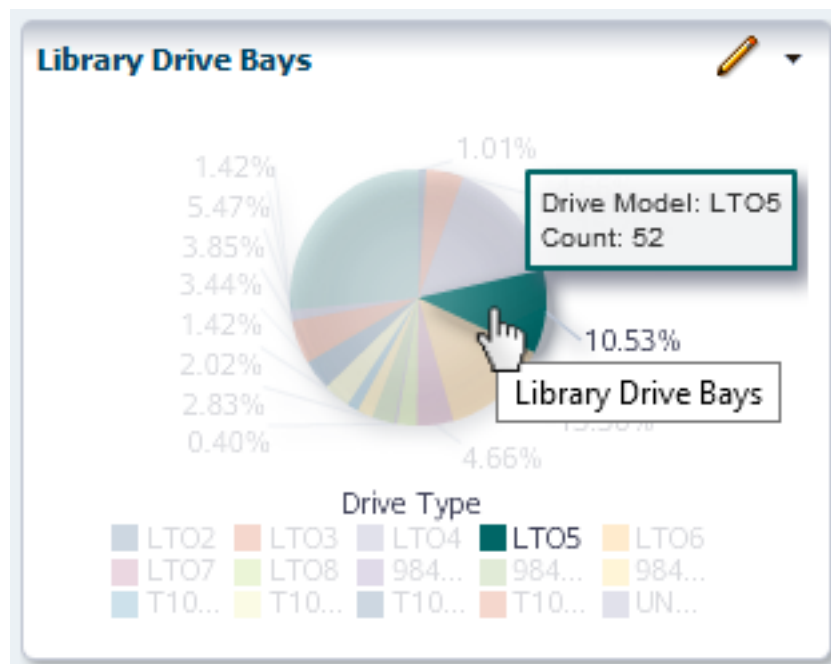
Dashboard data is reported in UTC time, while all other STA screens report times adjusted for your local time zone (as specified in the time zone preferences for your username).

## Link to Details from a Dashboard Pane

Click links within dashboard panes to access more detail about the selected resources.

#### Graph Links

When you click a portion of a graph you apply an associated filter. For more information, see [Filter Using Dashboard Graphics](#).



#### Text Links

When you click the text link within table panes, it displays the detail view for the selected resource.


For example, clicking the drive serial number within the Drives Watch List will display the Drives - Overview page showing details for drive with that serial number.



Drive Serial Number	Drive Model	Drive Health	Drive Health Trend
576004000904	T10000C	✖	↓
579001000173	T10000D	✖	▬
579001000000	T10000D	✖	▬

## Detach a Pane to View More Detail

Open a separate window to view the pane data in closer detail.

1. In the left navigation bar, select **Home**, then select **Dashboard**.
2. In the pane's toolbar, click **Detach Pane** .



## View the Dashboard on a Mobile Device

Display a read-only version of the dashboard on a mobile device.

You cannot link to other screens from the dashboard nor rearrange panes or save templates. Therefore, you must first create dashboard templates through a desktop STA connection before accessing them on a mobile device.

1. Obtain access to the network on which STA is running. If the network is protected by a firewall or virtual private network (VPN), see your system administrator for access instructions.
2. From a browser on your mobile device, log in to STA.
3. To change the display, select a template from the **Templates** drop-down menu at the top of the screen.
4. To log out, click the **Logout** link at the bottom of the screen.

## Why is the dashboard taking a long time to load?

It may take some time for a complex dashboard to load.

Applying filters to panes can also impact the load time. If you experience long load times, you may want to break up a complex dashboard into multiple, smaller templates.

## Customize the Dashboard

You can select up to 30 panes to display on a single dashboard. There are over 50 different panes to choose from, each one showing a different set of analytic and summary data collected by STA.

- [Change the Size of Dashboard Panes](#)
- [Add a Dashboard Pane](#)
- [Move a Dashboard Pane](#)
- [Remove a Dashboard Pane](#)
- [Annotate a Dashboard Pane](#)
- [Filter a Dashboard Pane](#)
- [Save the Dashboard Layout](#)
- [Dashboard Pane Types](#)

## Change the Size of Dashboard Panes

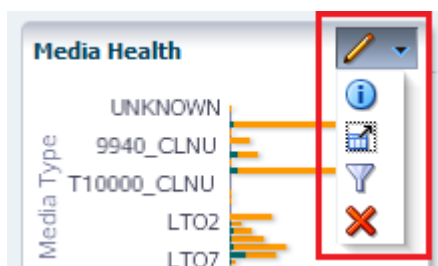
Modify the column count and row height of the dashboard layout to change the size of the panes.

1. In the left navigation bar, select **Home**, then select **Dashboard**.
2. In the dashboard toolbar, adjust the **Column Count** (1 to 5) and **Row Height** (100 to 600).



Changes take effect as soon as you press **Enter** or move the cursor.

3. Having numerous columns may truncate the pane toolbar. Click the drop-down in the top-right of the pane to view the hidden icons.




## Add a Dashboard Pane

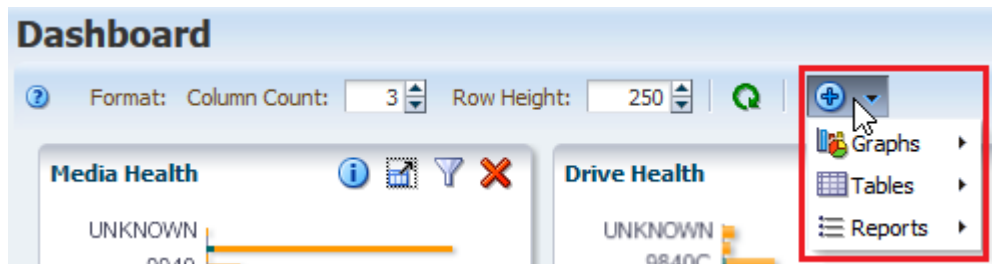
Add a maximum of 30 panes to the dashboard. Newly added panes appear at the bottom of the dashboard.

You can add more than one instance of the same type of pane, and you can filter each instance differently so you can focus on different data. For example, you may want to add two separate Media Health panes: one for big libraries (SL3000 and SL8500) and one for small (SL150 and SL500).

### Note:

Adding a large number of dashboard panes may result in the pane legends being truncated or not displayed at all. If this occurs, you may want to remove some panes to restore the legends.

1. In the left navigation bar, select **Home**, then select **Dashboard**.
2. In the dashboard toolbar, click **Add a Dashboard Portlet** .



3. From the one of the submenus (**Graphs**, **Tables**, or **Reports**), select the specific pane to add.
4. The pane appears at the end of the dashboard display. To reorder the panes, see [Move a Dashboard Pane](#).
5. To retain the newly added pane for future logins, save the dashboard as a template. See [Save a Template](#).

## Move a Dashboard Pane

Drag and drop panes within the dashboard to reorder them.

1. In the left navigation bar, select **Home**, then select **Dashboard**.
2. Hover over the top of the pane (near the title). Until you see the move icon.




3. Drag and drop the pane to a new location.

4. To retain the order for future logins, save the dashboard as a template. See [Save a Template](#).

## Remove a Dashboard Pane

Remove a pane to no longer have it display in the dashboard.

1. In the left navigation bar, select **Home**, then select **Dashboard**.
2. On the pane's toolbar, click **Remove Pane** .




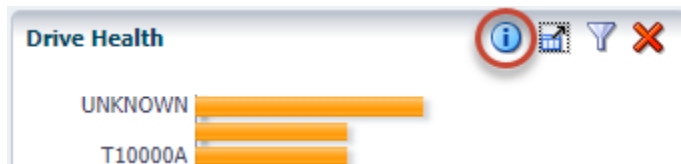
3. To retain the current dashboard view for future logins, save the dashboard as a template. See [Save a Template](#).

## Annotate a Dashboard Pane

Annotations appear on executive reports. Use them to clarify information or draw attention to specific data.

Annotation text is specific to the current dashboard template and your username. For example, if the Drive Health pane appears in several dashboard templates, each instance of the Drive Health pane can have a different annotation associated with it. Annotations entered by one user on the Drive Health pane do not appear to a user logged in with a different username.

1. In the left navigation bar, select **Home**, then select **Dashboard**.
2. Click **Panel Information**  in the pane's toolbar.



3. Enter the annotation text (up to 1000 characters) for this instance of the pane, and then click **Save Annotation**.
4. For the updated annotation to appear on an executive report, you must save the current dashboard template. See [Save a Template](#) and [Modify a Template](#). If you log out of this session without saving the template, the annotation will be lost for future login sessions when the executive report runs.

## Filter a Dashboard Pane


Apply a filter to a pane to alter the data displayed.

1. In the left navigation bar, select **Home**, then select **Dashboard**.

2. On the pane's toolbar, click **Filter Data**  or the **Applied Filter**  icon.



 **Note:**

If a pane already has a filter, it will have the **Applied Filter**  icon. Hover over the icon to display a description of the filter.

3. For details on how to filter data, see [Filter Using the Dialog Box](#).
4. To clear all filter criteria, click **Reset** within the Filter Data dialog.

## Save the Dashboard Layout

Create a template of the dashboard to save the layout for future use.

Operator or Administrator users can arrange the dashboard and save it as a custom template. The order and size of the panes and any applied filters are saved as part of the template.

See [Save a Template](#).

## Dashboard Pane Types

The dashboard has three types of panes: Graphs, Tables, and Reports.

- [Graph Panes](#)
- [Table Panes](#)
- [Report Panes](#)

## Graph Panes

Graph panes can be bar, pie, and line graphs. You can graph numerous attributes related to alerts, drives, media, and libraries.

### Alerts

Bar chart showing the total number of STA alerts for drives, media, libraries, CAPs, and PTPs generated over a selected date range.

Alerts are generated based on user-defined alert policies. Because the number of alert policies and their criteria and severity are entirely user-defined, this graph does not necessarily indicate issues with your tape library system environment.

### Alert Trends

Line graph showing the total number and severity of STA alerts each day over a selected date range.

Alerts are generated based on user-defined alert policies. Because the number of alert policies and their criteria and severity are entirely user-defined, this graph does not necessarily indicate issues with your tape library system environment.

**Cumulative Data Read and Written**

Line graph showing the total amount of data read and written over a selected date range.

**Drive Activity Trends**

Area chart showing, by drive model, the total number of dismounts each day over a selected date range.

**Drive Health**

Bar chart showing, by drive model, the total number of drives with each Drive Health Indicator as computed by STA.

**Drive Health Trends**

Line graph showing, by drive model, the average Drive Suspicion Level each day over a selected date range.

To compute the daily value for a given model, STA averages the suspicion levels of *all* installed drives of that model, regardless of how many were actually used that day. If a drive was not used on a given day, its suspicion level is carried forward from the day before.

**Drive Utilization (Hourly, Daily, Weekly, or Monthly)**

Line graph showing the average percentage of time the drives were occupied each hour, day, week, or month. You can filter by drive location (complex, library, or rail, for example) and by date range.

Values shown in this pane are updated at the end of each hour, so are not real-time.

**I/O Throughput (Hourly, Daily, Weekly, or Monthly)**

Line graph showing the total amount of data read and written each hour, day, week, or month over a selected date range.

**Library Component Health Trends**

Line graph showing, by library component type (robots, CAPs, elevators, and pass-through ports), the average daily condition over a selected date range.

The conditions are as reported by the library, not by STA.

**Library Component Status**

Bar chart showing, by library component type (robots, CAPs, elevators and pass-through ports), the current total number of components with each reported condition.

The conditions are as reported by the library, not by STA.

**Library Drive Bays**

Pie chart showing the current distribution of installed drives by type and empty drive slots.

**Library Media Slots**

Pie chart showing the current distribution of occupied media slots by media type and empty slots.

**Library Status**

Bar chart showing, by library model, the current total number of libraries with each Top-Level Indicator as reported by the library.

**Maximum Mount Times (Hourly, Daily, Weekly, or Monthly)**

Line graph showing, for each hour, day, week, or month over a selected date range, the total time-to-mount of the single exchange that took the longest time to mount. The value plotted is the total time from the start of the exchange to the start of the mount.

**Media – Least Recently Mounted (Hourly, Daily, Weekly, or Monthly)**

Line graph showing, for each hour, day, week, or month over a selected date range, the piece of media with the longest time since the last exchange. The value plotted is the total time since the last exchange. Only media that have had exchange activity are included. Values shown in this pane are updated at the end of each hour, so are not real-time.

**Media Health**

Bar chart showing, by media type, the total number of media with each Media Health Indicator as computed by STA.

**Media Health Trends**

Line graph showing, by media type, the average Media Suspicion Level each day over a selected date range.

To compute the daily value for a given media type, STA averages the suspicion levels of all available media of that type, regardless of how many were actually used that day. If a media was not used on a given day, its suspicion level is carried forward from the day before.

**Media Movements (Hourly, Daily, Weekly, or Monthly)**

Line graph showing the total times media were entered, ejected, or otherwise moved each hour, day, week, or month over a selected date range. "Other" movements include moves by robots, elevators, or PTPs.

Values shown in this pane are updated at the end of each hour, so are not real-time.

**Media Slots Available (Hourly, Daily, Weekly, or Monthly)**

Line graph showing the minimum and maximum media slots available each hour, day, week, or month over a selected date range

**Media Utilization (Hourly, Daily, Weekly, or Monthly)**

Line graph showing an estimate of average media utilization each hour, day, week, or month over a selected date range. Media utilization is the percentage of the total media capacity that has been used by data—that is, the "fullness" of the media. Only media that have had exchange activity are included.

Values shown in this pane are updated at the end of each hour, so are not real-time.

**Media Utilization Bands (Hourly, Daily, Weekly, or Monthly)**

Line graph showing an estimate of the number of media *bands*, or utilization ranges, used each hour, day, week, or month over a selected date range. A band appears on the graph only if there are media with utilization values in that range.

The <0001% band includes both media that is literally blank and media that is effectively blank because it has an internal label but no real data.

Values shown in this pane are updated at the end of each hour, so are not real-time.

**Media Validation**

Line graph showing the total number of media validations, and the total passed, failed, and unknown for the selected time period.

**Mounts (Hourly, Daily, Weekly, or Monthly)**

Line graph showing the total number of mounts each hour, day, week, or month over a selected date range. The value plotted is the number of mounts, not dismounts.

**Robot Health**

Bar chart showing the current number of robots by Robot Health as computed by STA.

**SL8500 Dismount Efficiency (moves)**

Bar chart summarizing the total number of rails on which a media travels to complete a dismount request as part of an exchange. This includes movements by robots, elevators, and PTPs. If a media crosses a rail without stopping, the rail is not included in the count. For example:

- For a media moved from a drive to a media slot on the same rail, the count is "1."
- For a media moved from a drive on rail #4 to a media slot on rail #1, the count is "2."
- For a media moved from a drive on rail #4, to a PTP on rail #3, to a drive on rail #1 in a different library, the count is "3."

For libraries managed by StorageTek ACSLS, if the media *float* option is enabled, dismount move efficiency will be "1" whenever media slots are available within the same LSM as the drive.

**SL8500 Mount Efficiency (moves)**

Bar chart summarizing the total number of rails on which a media travels to complete a mount request as part of an exchange. This includes movements by robots, elevators, and PTPs. If a media crosses a rail without stopping, the rail is not included in the count. For example:

- For a media moved from a media slot to a drive on the same rail, the count is "1."
- For a media moved from a media slot on rail #1 to a drive on rail #4, the count is "2."
- For a media moved from a drive on rail #1, to a PTP on rail #3, to a drive on rail #4 in a different library, the count is "3."

## Table Panes

Dashboard table panes include point-in-time reports and spark charts.

**Data Read/Written Trends**

Summarizes the amount of data read and written, and average data compression ratio over a selected date range.

The Total Data Stored values are the total amount of data stored on all media in the selected libraries as of the indicated dates.

The Data Compression values displayed in the table are rounded to the nearest whole number; the table cell tooltips display decimal value detail.

This pane displays values for dates within the 60 days only. If you filter for a date range extending past the previous six months, the pane displays values only for dates that fall within the allowed range. Following are examples:

- Filtering for "Number of Days More Than 25" shows values for the period from 60 to 25 days ago.
- Filtering for "Number of Days Less Than 75" shows values for the period 60 days ago to current.
- Filtering for "Number of Days More Than 200" shows no data.



**Drive Capacity Planning (30 Days)**

Summarizes installed drive slots, installed drives, removed drives, and drive utilization statistics over the last 30 days.

The Drives Under-utilized count includes unknown drives (drives for which STA has received no data), as well as drives that have never been used.

**Drives Fewest Meters Between Recent Cleanings**

Lists drives that have run the fewest meters of tape between the two most recent cleanings.

The table only includes drives for which STA has recorded at least two cleaning actions. This is as of the current point in time.

**Drives Watch List**

Summarizes drives with Action or Evaluate drive health. Lists the drive serial number, model, Drive Health Indicator, Drive Health Trend, and most recent annotation. This is as of the current point in time.

**Media Capacity Planning (30 Days)**

Summarizes installed, activated, and occupied media slots, media removed, and media utilization statistics over the last 30 days.

The following values are updated each day at 00:00 UTC time, so are not real-time.

- Media Utilized
- Media Blank
- Media Unknown/Never Mounted

All other values are real-time.

**Media Exceptions**

Lists media that have been removed from the tape library system through some means other than a cartridge access port (CAP) or mailslot. This is as of the current point in time.

**Media Validation**

Summarizes media validation results by verification test type. By default, this pane shows data for the last 14 days. The counts in the Pass, Fail, and Unknown columns are based on the MV Result attribute, as follows:

- Pass – MV Result Passed
- Fail – MV Result is Failed or Degraded
- Unknown – MV Result is Unknown

This table reports completed validations only; pending or in-process validations are not included. It includes validations initiated by all sources, including host applications, SL Console, and the library CLI, as well as STA.

**Media Watch List**

Summarizes media with Action or Evaluate media health. Lists the volume serial number (volser), type, Media Health Indicator, Media Health Trend, and most recent annotation. This is as of the current point in time.

**Monitored Device Trends**

Summarizes the number of resources in your tape library system over a selected date range. Information includes the total number of libraries, robots, CAPs, pass-through ports (PTPs), elevators, drives, media, and media removed through a CAP, SL3000 AEM, or SL150 mailslot.

## Report Panes

Report panes are text-only summaries of current information about your tape library system.

### **Data Read Report**

Summarizes total data read from media, including the daily average, daily high and low marks, and average compression ratio.

### **Data Written Report**

Summarizes total data written to media, including the daily average, daily high and low marks, and average compression ratio.

### **Drives Health Report**

Summarizes the number of drives by Drive Health Indicator as computed by STA.

### **Library Status Report**

Summarizes the number of libraries by Library Top-Level Indicator reported by the library.

### **Media Health Report**

Summarizes the number of media by Media Health Indicator as computed by STA. The "Unknown" category includes media for which STA has not received sufficient data to calculate health; this may occur for the following reasons:

- The media has not been mounted in a drive during the time STA has been monitoring it.
- The STA Supported attribute for the media has a value of False. This indicates the media has a type does not meet the minimum requirements for STA analytics—for example, SDLT and LTO-2 media. See the *STA Installation and Configuration Guide* for details about supported media types.

### **Media Validation Report**

Summarizes media validation activity, including a breakdown of validations performed, number of media validated, number of drives used, and validation elapsed times.

### **Monitored Device Counts**

Summarizes total devices monitored in your tape library system, including libraries, robots, CAPs, pass-through ports (PTPs), elevators, drives, media, and media removed through a CAP, SL3000 AEM, or SL150 mailslot. By default, this report includes all devices as of the current date.

# 7

## Templates

Templates provide a way to save, reuse, and share a particular screen layout.

Templates are screen specific and available for the Dashboard, all Tape System Hardware screens, and all Tape System Activity screens. Templates are not available for the Setup & Administration tab.

- [Template Types](#)
- [Apply a Template](#)
- [Set the Default Template for a Screen](#)
- [Customize a Template](#)
- [Share a Template](#)
- [Restore the Predefined Templates](#)
- [User Roles for Template Activities](#)
- [Descriptions of Predefined Templates](#)

## Template Types

Templates can be pre-defined or user created.

### Pre-defined Templates

STA comes with a set of predefined templates that provide frequently used information about library resources (such as libraries, drives, media) and events (such as exchanges and cleaning activities). Predefined templates are prefixed with "STA-".

Predefined templates are available to all users. They cannot be modified directly. Instead, you must save any changes to a new, custom template. You can, however, delete predefined templates that you don't need and then later restore them.

See [Descriptions of Predefined Templates](#) for a description of each template.

### Custom Templates

An Operator or Administrator can create a custom template by modifying the current screen—such as changing graphed attributes, re-ordering columns in a list view table, or applying filter criteria—and then saving the new display as a template. Any number of custom templates can be created for each screen. When you save a template you assign it a name and designate its visibility setting (public or private). Once you have saved a custom template, it is immediately available for the current and future login sessions.

See [Save a Template](#).

# Apply a Template

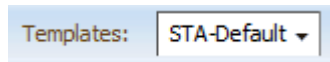
Applying a template to a screen will load a previously saved layout.

When you initially navigate to a screen, STA applies the default template for your username. There are several ways that you can apply a template for a screen: the toolbar, quick links, or the template management page.

Templates exhibit sticky behavior, meaning once you apply a template to a screen, STA will continue to display that template whenever you access that screen. The template will remain in effect for the rest of the current login session, until you explicitly apply a different template, or logout.

## Use the Toolbar to Apply a Template

1. Navigate to the screen that you want to apply the template to.
2. In the upper-right, select a template from the **Templates** drop-down menu.



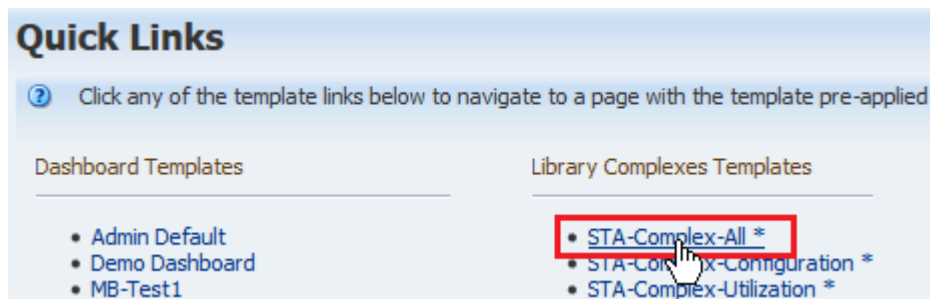
## Use Quick Links to Apply a Template

Quick Links provide quick access to templates available to your STA username.

1. In the left navigation, expand **Home**, and then select **Quick Links**.
2. The templates are grouped by screen name. Predefined templates are identified with an asterisk (\*). Click a template in the list to load the template.

### Note:

STA-Default" is not shown in the Quick Links list.



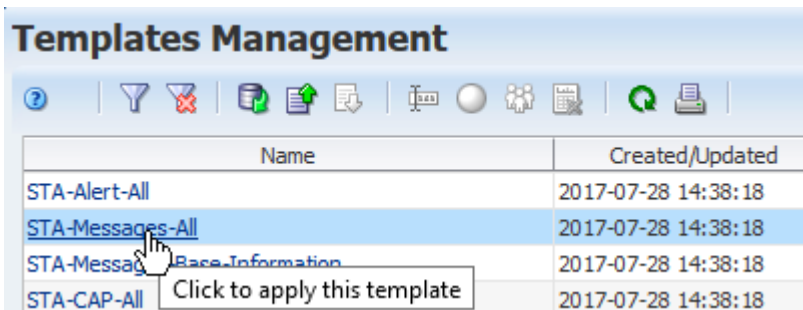
## Use Templates Management to Apply a Template

1. You must have Operator or Administrator privileges.
2. In the left navigation, expand **Setup & Administration**, then select **Templates Management**.

- In the table, click the name of the template you want to load.

 **Note:**

The "STA-Default" templates are not shown in the list.

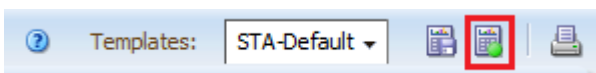


## Set the Default Template for a Screen


The default template initially displays when you first view a screen after logging in. You can set the default template using the toolbar or using templates management.

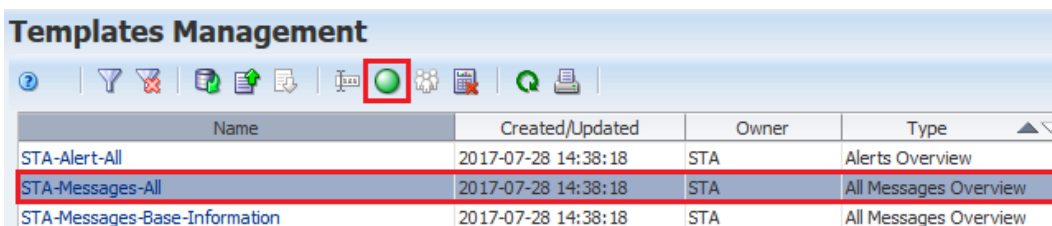
### Use the Templates Toolbar

- In the current screen, verify the template you want to set as the default is selected in the **Templates** drop-down menu.
- Click **Default Template**.



### Use the Templates Management Screen

- In the left navigation bar, select **Setup & Administration**, then select **Templates Management**.
- The Type column displays which screen the template applies to. Select a template for the given screen type. Click **Set Default** .



- This update does not take effect until your next login session. Log out and then log back in to see the change.

## Customize a Template


Create a new template or modify an existing template to fit your needs.

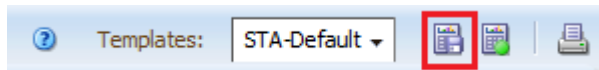
- [Save a Template](#)
- [Modify a Template](#)
- [Rename a Template](#)
- [Set a the Visibility of a Template to Public or Private](#)
- [Delete a Template](#)

## Save a Template

Save the current screen layout and filters as a template to use in the future.

Use custom templates to address the top three tape operation concerns at your site. This will help make the data more understandable and manageable. To create templates that are as flexible as possible, use general, rather than specific, filtering criteria. For example, when creating a template that filters by a time period, use "Number of Days" attributes instead of "Date" attributes.

1. You must have Operator or Administrator privileges.
2. On the screen you want to save, click **Save Template**  in the upper-right corner.



3. Enter a **Template Name**.

### **Tip:**

Do not start the name with "STA-". This prefix is used for all predefined templates.

Include the first part of the template type consistently as part of the name. This makes it easier to know the purpose of imported or exported XML files. For example, if the template type is "Media Overview", then a good template name would be "Media-Exception".

4. Select a **Shared** option. See [Template Ownership and Visibility](#) for more info.
  - *Private* – The template will be available to the current STA username only.
  - *Public* – The template will be available to all STA usernames.
5. Click **Save**.

### Screen Characteristics INCLUDED in the Template Definition

- Graph display details, such as:
  - Wide versus narrow view

- Graphed attributes
- Percent versus actual value display
- Date range
- Whether the Graphics Area is visible or collapsed
- Table display details, such as:
  - Hidden and visible columns
  - Column order
  - Column width
- Filter criteria

#### Screen Characteristics NOT INCLUDED in the Template Definition

- Table resource selections applied to graphs
- Table sort criteria
- Specific data content

## Modify a Template

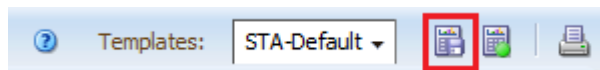
Modify an existing template to save changes for future use.

When creating custom templates, it is often easier to modify an existing template rather than starting from scratch. You can modify any template that you own. To modify an STA predefined template or public template owned by another username, you must save the modifications as a new template. See [Save a Template](#).

1. You must have Operator or Administrator privileges.
2. Navigate to the screen you wish to modify.
3. From the **Templates** drop-down menu, select a template.
4. Modify the screen.

See [Screen Characteristics INCLUDED in the Template Definition](#) for more info on what changes will be saved.

5. Click **Save Template**  in the upper-right corner of the screen.




6. Verify the Name and Shared settings, and then click **Save**.

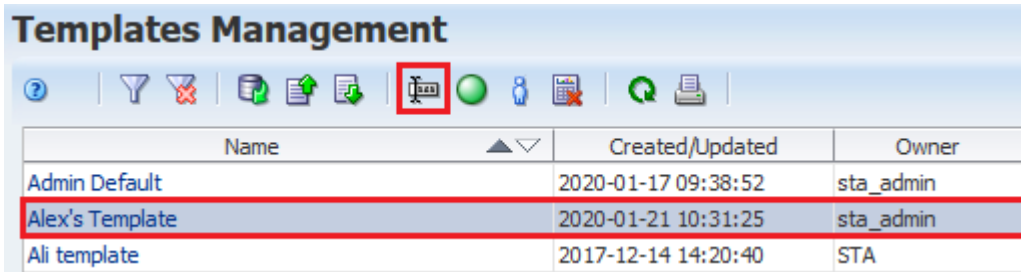
## Rename a Template

Rename any custom template available to your username. You cannot rename STA predefined templates.

1. You must have Operator or Administrator privileges.
2. In the left navigation bar, select **Setup & Administration**, then select **Templates Management**.

3. Select a custom template, and then click **Rename** .

**Templates Management**



Name	Created/Updated	Owner
Admin Default	2020-01-17 09:38:52	sta_admin
Alex's Template	2020-01-21 10:31:25	sta_admin
Ali template	2017-12-14 14:20:40	STA

 **Tip:**



When naming templates, do not start the name with "STA-". This prefix is used for all predefined templates. Include the first part of the template type consistently as part of the name. This makes it easier to know the purpose of imported or exported XML files. For example, if the template type is "Media Overview", then a good template name would be "Media-Exception".

4. Enter the new name, and then click **OK**.

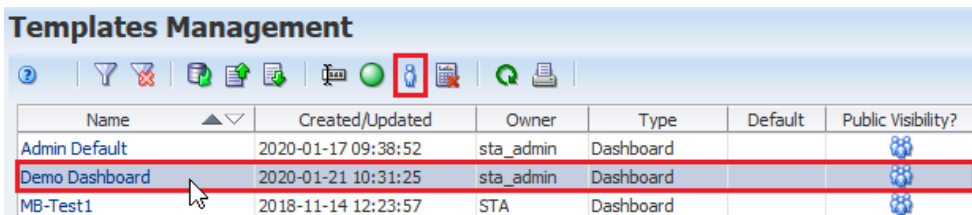
## Set a the Visibility of a Template to Public or Private




Assign public or private visibility to a template you own. A public template can be used by other users. A private template can only be used by your username.

To share templates by importing and exporting, see [Share a Template](#).

1. You must have Operator or Administrator privileges.
2. In the left navigation bar, select **Setup & Administration**, then select **Templates Management**.
3. Select a template that you own (your username must be listed in the Owner column).
4. Click **Make Template Private**  or **Make Template Public** .

**Templates Management**



Name	Created/Updated	Owner	Type	Default	Public Visibility?
Admin Default	2020-01-17 09:38:52	sta_admin	Dashboard		
Demo Dashboard	2020-01-21 10:31:25	sta_admin	Dashboard		
MB-Test1	2018-11-14 12:23:57	STA	Dashboard		

5. Note that the icon in the *Public Visibility?* has changed.



## Template Ownership and Visibility

The Templates Management screen displays ownership and visibility for available templates.

### Ownership

The template owner is the STA username that created the template. You cannot change the ownership. For predefined templates, the owner is always "STA". Operators or Administrators can modify, rename, delete, and assign default status to any templates they own.

### Visibility


A template's visibility determines who can see and use the template. The template owner can change visibility to either public or private:

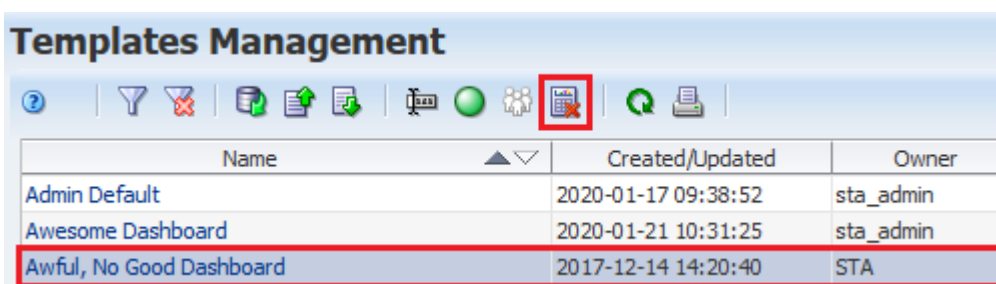
- *Public* – All STA usernames can use the template. STA predefined templates are always public. Operators or Administrators can use, modify, and delete any templates that have public visibility, even if they are owned by another STA username.
- *Private* – Only the STA username that own the template can use it.

## Delete a Template

Delete a custom or predefined template to remove it from STA.

If you delete a template that was the default for any STA usernames, then the "STA-Default" template becomes their new default.

1. You must have Operator or Administrator privileges.
2. In the left navigation, select **Setup & Administration**, then select **Templates Management**.
3. Select a template in the list, and then click **Delete** .



Name	Created/Updated	Owner
Admin Default	2020-01-17 09:38:52	sta_admin
Awesome Dashboard	2020-01-21 10:31:25	sta_admin
Awful, No Good Dashboard	2017-12-14 14:20:40	STA

### See Also:

- [Restore the Predefined Templates](#)

## Share a Template

Share custom templates with other users by exporting and importing the template.

For example, you can save a custom template, export it as an XML file to your local computer, and then email the XML file to another user. The other user can then log in to STA with their username, import the XML file, and begin using the template immediately.

**Note:**


Sharing by importing and exporting is different than sharing by adjusting the visibility setting. See [Template Ownership and Visibility](#) for more info.

- [Export a Template](#)
- [Import a Template](#)

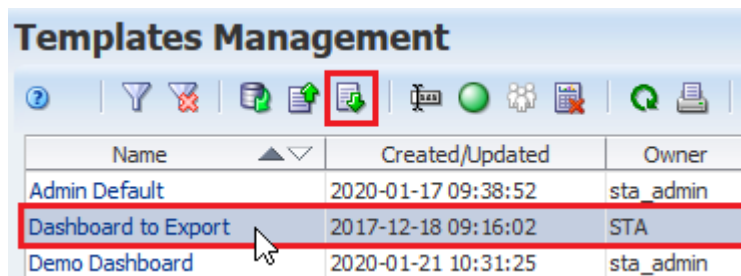
## Export a Template

Export a custom template in XML format to share the template with another user.

After you have created a significant set of templates, be sure to export them to XML file format and save them outside of STA. Exporting and importing templates can also be a useful way of circulating and exchanging templates both on- and off-site.

1. In the left navigation bar, select **Setup & Administration**, then select **Templates Management**.
2. Select a template in the list, and then click Click **Export** .


You can export any custom template available to your username, even if you are not the owner. You cannot export STA predefined templates.



3. Save the file to an accessible location.

## Import a Template

Import a template received from another user so that it is available to your username.

1. Verify the template is saved to a location accessible to your browser.
2. You must have Operator or Administrator privileges.
3. In the left navigation bar, expand **Setup & Administration**, then select **Templates Management**.
4. Click **Import Template** .



5. Click **Browse** and navigate to the location of the template file. The file must have a `.xml` extension. Click **Ok**.
6. The template is added to the list. The assigned Owner is your STA username, and the Visibility is set to Private.

Name ▲▼	Created/Updated	Owner	Type	Default	Public Visibility?
Admin Default	2020-01-17 09:38:52	sta_admin	Dashboard		
Dashboard Worth Sharing	2020-01-21 10:31:25	sta_admin	Dashboard		
Demo Dashboard	2017-12-18 09:16:02	STA	Dashboard		

## Restore the Predefined Templates

Restore the STA predefined templates after deleting them. This does not affect custom templates.

1. You must have Operator or Administrator privileges.
2. In the left navigation, select **Setup & Administration**, then select **Templates Management**.
3. Click **Restore Predefined Templates**



## User Roles for Template Activities

Some template activities can be performed by all user roles, while others are available only to users with Administrator or Operator privileges.

Regardless of user role, you have access to all public templates and private templates owned by your current STA username. You cannot use private templates owned by another STA username. The following table provides a summary of activities available to each role.

User Roles	Template Activity	Screen or Toolbar
Viewer and above	Apply a template to the current screen Set the current template as the screen default for your STA username	Template toolbar
Viewer and above	Display a list of all templates available to your STA username Navigate to a screen with the selected template applied	Select <b>Home</b> , then select <b>Quick Links</b> .
Operator and above	Display a list of all templates available to your STA username Change the default screen template for your STA username	Select <b>Setup &amp; Administration</b> , then select <b>Template Management</b> .

User Roles	Template Activity	Screen or Toolbar
Operator and above	Create a template Modify the appearance of a template—custom templates only Save a template to a new name—custom templates only Change the public or private visibility settings of a template—custom templates owned by your STA username only	Template toolbar
Operator and above	Rename a template—custom templates only Change the public or private visibility settings of a template—templates owned by your STA username only Export a template—custom templates only Import a template Delete a template Restore the STA predefined templates	Select <b>Setup &amp; Administration</b> , then select <b>Templates Management</b>

## Descriptions of Predefined Templates

The predefined templates come standard with the STA application. STA predefined templates are always prefixed "STA-".

This section includes short descriptions of the predefined templates for each Overview, Analysis, and Messages screen.

### Home Tab

- [Dashboard Predefined Templates](#)

### Tape System Hardware Tab

- [Complexes Overview Predefined Templates](#)
- [Libraries – Overview Predefined Templates](#)
- [Libraries – Messages Predefined Template](#)
- [Drives – Overview Predefined Templates](#)
- [Drives – Analysis Predefined Templates](#)
- [Drives – Messages Predefined Template](#)
- [Media – Overview Predefined Templates](#)
- [Media – Analysis Predefined Templates](#)
- [Media – Messages Predefined Template](#)
- [Robots Overview Predefined Templates](#)
- [CAPs Overview Predefined Templates](#)
- [PTPs Overview Predefined Templates](#)
- [Elevators Overview Predefined Templates](#)

### Tape System Activity Tab

- [Alerts Overview Predefined Templates](#)

- [Exchanges Overview Predefined Templates](#)
- [Drive Cleanings Overview Predefined Templates](#)
- [Media Validation Overview Predefined Templates](#)
- [All Messages – Overview Predefined Templates](#)
- [All Messages – Analysis Predefined Template](#)

## Dashboard Predefined Templates

The dashboard predefined templates are meant to provide an overall look at your library system.

### **STA-Default**

Provides a comprehensive summary of the condition, configuration, and daily performance of your tape library system.

### **STA-Dashboard-All-Graphs**

Displays all available graph panes in alphabetical order. This template is useful for selecting panes to include in dashboard templates and executive reports. Only the Daily version is displayed for graphs that include Monthly, Weekly, Daily, and Hourly versions.

### **STA-Dashboard-All-Reports**

Displays all available report panes in alphabetical order. This template is useful for selecting panes to include in dashboard templates and executive reports.

### **STA-Dashboard-All-Tables**

Displays all available table panes in alphabetical order. This template is useful for selecting panes to include in dashboard templates and executive reports.

### **STA-Dashboard-Nearline-Daily**

Displays daily summary information for drive and media activity in your tape library system over the last 30 days. The displayed panes summarize mount activity, I/O throughput, drive and media utilization, and drive and media slot availability. Data displayed in this template is updated at the end of each day. For bar charts, at least one full day's worth of data must have been collected by STA in order for data to be displayed. For line graphs, at least two data points are required, so at least two days' worth of data are required.

### **STA-Dashboard-Nearline-Hourly**

Displays hourly summary information for drive and media activity in your tape library system over the last four days. The displayed panes summarize mount activity, I/O throughput, drive and media utilization, and drive and media slot availability. Data displayed in this template is updated at the end of each hour. For bar charts, at least one full hour's worth of data must have been collected by STA in order for data to be displayed. For line graphs, at least two data points are required, so at least two hours' worth of data are required.

### **STA-Dashboard-Nearline-Monthly**

Displays monthly summary information for drive and media activity in your tape library system over the last 365 days. The displayed panes summarize mount activity, I/O throughput, drive and media utilization, and drive and media slot availability. Data displayed in this template is updated at the end of each month. For bar charts, at least one full month's worth of data must have been collected by STA in order for data to be displayed. For line graphs, at least two data points are required, so at least two months' worth of data are required.

**STA-Dashboard-Nearline-Weekly**

Displays daily summary information for drive and media activity in your tape library system over the last 100 days. The displayed panes summarize mount activity, I/O throughput, drive and media utilization, and drive and media slot availability. Data displayed in this template is updated at the end of each week. For bar charts, at least one full week's worth of data must have been collected by STA in order for data to be displayed. For line graphs, at least two data points are required, so at least two weeks' worth of data are required.

**STA-Dashboard-Quick-Start**

Displays information about the overall configuration and condition of the tape library system. Used with the [Quick Start Guide](#).

## Complexes Overview Predefined Templates

The Complexes Overview predefined templates provide information about the library complexes such as configuration and utilization.

**STA-Default**

Displays basic library complex configuration.

**STA-Complex-All**

Displays all library complex graphs and table attributes.

**STA-Complex-Configuration**

Displays information about the library complex physical and partition configuration.

**STA-Complex-Utilization**

Displays the physical configuration of the library complex and summarizes activity in the complex, including enters and ejects, mounts and dismounts, and drive utilization.

## Libraries – Overview Predefined Templates

The Libraries - Overview predefined templates provide information about the tape libraries such as configuration, health, and utilization.

**STA-Default**

Displays basic library properties and configuration information.

**STA-Lib-All**

Displays all library table attributes.

**STA-Lib-Base-Information**

Displays the base library configuration and relatively static data; useful for library description and inventory listings.

**STA-Lib-Configuration**

Displays information about the library physical and partition configuration. Also includes connection information useful for troubleshooting connection issues.

**STA-Lib-Health**

Displays information about library health, firmware, and SNMP connection with STA.

**STA-Lib-Quick-Start**

Displays information about the overall configuration and condition of the library; used with the *STA Quick Start Guide*.

**STA-Lib-Utilization**

Displays summary information about the amount and rates of library activity and drive utilization.

## Libraries – Messages Predefined Template

The Libraries - Messages predefined template provides information about the SNMP traps sent by the libraries.

**STA-Default**

Displays SNMP traps, including detail about the library and device involved. Includes messages with the following Trap Types: CAP, Heartbeat, Library Environment Check, Library Log, Library Status, and PTP. Some messages may also appear in the Drives – Messages and Media – Messages screens.

## Drives – Overview Predefined Templates

The Drives - Overview predefined templates provide information about the tape drives such as performance, health, and utilization.

**STA-Default**

Displays drive configuration information and the status of the most recent exchange that occurred on the drive.

**STA-Drive-All**

Displays all drive graphs and table attributes.

**STA-Drive-Base-Information**

Displays the base drive configuration and relatively static data; useful for drive description and inventory listings.

**STA-Drive-Health**

Displays current and summary health and activity information for all drives.

**STA-Drive-LTO-Performance**

Displays performance data for LTO drives only.

**STA-Drive-LTO-Utilization**

Displays utilization statistics for LTO drives only.

**STA-Drive-Last-Exchange**

Displays information for the last exchange that occurred on each drive.

**STA-Drive-MV**

Displays drives that meet the criteria for performing STA media validation. The displayed attributes provide detail that is useful for selecting and monitoring the performance of drives that may be assigned to the validation drive pools.

**STA-Drive-Performance-30-Days**

Displays summary performance data for all drives over the last 30 days.

**STA-Drive-T10000-Performance**

Displays performance data for T10000 drives only.

**STA-Drive-T10000-Utilization**

Displays utilization statistics for T10000 drives only.

**STA-Drive-Utilization**

Displays utilization statistics for all drives.

## Drives – Analysis Predefined Templates

The Drives - Analysis predefined templates provide information about tape drive health and firmware.

**STA-Default**

Summarizes current drive health by library complex.

**STA-Drive-Firmware-Levels**

Summarizes current drive firmware levels by drive type.

**STA-Drive-Read-Marginal**

Summarizes the "Exchange Read Marginal" status for applicable drives, by library complex name. Applicable to StorageTek T10000 drives only.

## Drives – Messages Predefined Template

The Drives - Messages predefined template provides information about drive-related SNMP traps sent by the libraries.

**STA-Default**

Displays SNMP traps, including detail about the drive involved. Includes drive-related messages with the following Trap Types: Drive, Library Environment Check, and Library Log. Some messages may also appear in the Libraries – Messages and Media – Messages screens.

## Media – Overview Predefined Templates

The Media - Overview predefined templates provide information about media such as media validation status, health, cleaning status, utilization, and performance.

**STA-Default**

Displays base information about the media, its most recent exchange, and the drive involved.

**STA-Media-All**

Displays all media graphs and table attributes.

**STA- Media-Base-Information**

Displays the base media information and relatively static data; useful for media description and inventory listing.

**STA-Media-Cleaning**

Displays base information about cleaning media only. Also displays the status of the cleaning media's most recent exchange and the drive involved.



**STA-Media-Expired**

Displays information about expired media. Your Oracle support representative may ask you to use this template before submitting error log information.

**STA-Media-Health**

Displays current and summary health and activity information for all media.

**STA-Media-LTO-Performance**

Displays summary performance information for LTO media only.

**STA-Media-LTO-Utilization**

Displays summary utilization information for LTO media only.

**STA-Media-Last-Exchange**

Displays information about the last exchange for each piece of media.

**STA-Media-MIR-Stats**

Displays data from the media information record (MIR).

**STA-Media-MV-Calibration**

Displays detail about media assigned to the calibration media logical group, including information about the last calibration performed by the media.

**STA-Media-MV-Performed**

Displays media that have been validated within the last 30 days. The displayed attributes provide detail about media validation operations performed on these media.

**STA-Media-Stats-Last-Exchange**

Displays throughput and efficiency information for the last exchange for each piece of media. Your Oracle support representative may ask you to use this template before submitting error log information.

**STA-Media-T10000-Performance**

Displays summary performance information for T10000 media only.

**STA-Media-T10000-Utilization**

Displays summary utilization information for T10000 media only.

**STA-Media-Utilization**

Displays summary utilization information for all media.

## Media – Analysis Predefined Templates

The Media - Analysis predefined templates provide information about media health.

**STA-Default**

Summarizes current media health by library complex.

**STA-Media-HealthByMediaType**

Summarizes current media health by media type.

## Media – Messages Predefined Template

The Media - Messages predefined template provides information about media related SNMP traps sent by the libraries.

### **STA-Default**

Displays SNMP traps, including detail about the media involved. Includes media-related messages with the following Trap Types: Library Environment Check and Library Log. Some messages may also appear in the Libraries – Messages and Drives – Messages screens.

## Robots Overview Predefined Templates

The Robots Overview predefined templates provide information about the robots within the libraries.

### **STA-Default**

Displays properties and activities for all library robots.

### **STA-Robot-All**

Displays all available data attributes for all library robots.

## CAPs Overview Predefined Templates

The CAPs Overview predefined templates provide information about the CAPs within the libraries.

### **STA-Default**

Displays properties and activities for all library cartridge access ports (CAPs), SL3000 Access Expansion Modules (AEMs), and SL150 mailslots.

### **STA-CAP-All**

Displays all available data attributes for all library CAPs, SL3000 AEMs, and SL150 mailslots.

## PTPs Overview Predefined Templates

The PTPs Overview predefined templates provide information about the PTP (pass through ports) within the SL8500 libraries.

### **STA-Default**

Displays properties and activities for all SL8500 library pass-thru ports (PTPs).

### **STA-PTP-All**

Displays all available data attributes for all SL8500 library PTPs.

## Elevators Overview Predefined Templates

The Elevators Overview predefined templates provide information about the elevators with the SL8500 libraries.

### **STA-Default**

Displays properties and activities for all SL8500 library elevators.

### **STA-Elevator-All**

Displays all available data attributes for all SL8500 library elevators.

## Alerts Overview Predefined Templates

The Alerts Overview predefined templates provide information about STA alerts.

### **STA-Default**

Displays summary information for all STA alerts. The displayed attributes identify the alert policy, severity, criteria, and the tape library system resource or event for which the alert was generated.

### **STA-Alert-All**

Displays all available attributes for all STA alerts.

## Exchanges Overview Predefined Templates

The Exchanges Overview predefined templates provide information about exchanges such as which drive, media, and library was involved as well as alerts.

### **STA-Default**

Displays identification and status information for the drive, media, and library involved in each exchange.

### **STA-Exchange-Alerts-All**

Displays information about alerts that occurred during exchanges; exchanges that have not generated an alert are not included.

### **STA-Exchange-Alerts-Errors**

Displays all exchanges that resulted in at least one severe or warning tape alert. The displayed attributes provide detail about the types of errors that occurred. Severe tape alerts indicate an error on the exchange that may put your data at risk. Warning tape alerts indicate an error that may be associated with a hardware failure.

Your Oracle support representative may ask you to use this template before submitting error log information.

### **STA-Exchange-Alerts-Informational**

Displays all exchanges that resulted in at least one informational tape alert. The displayed attributes provide detail about the types of alerts that occurred. Informational tape alerts do not indicate an error on the exchange—cleaning alerts are an example.

### **STA-Exchange-Alerts-Severe**

Displays all exchanges that resulted in at least one severe tape alert. The displayed attributes provide detail about the types of errors that occurred. Severe tape alerts indicate an error on the exchange that may put your data at risk.

**STA-Exchange-Alerts-Warning**

Displays all exchanges that resulted in at least one warning tape alert. The displayed attributes provide detail about the types of errors that occurred. Warning tape alerts indicate an error on the exchange that may be associated with a hardware failure.

**STA-Exchange-Base Information**

Displays base information for all exchanges, such as drive and volume serial number, drive and media health, drive and media exchange status, MB read and written, and times.

**STA-Exchange-MIR-Alerts**

Displays all exchanges that resulted in alerts related to the media information record (MIR). Your Oracle support representative may ask you to use this template before submitting error log information.

## Drive Cleanings Overview Predefined Templates

The Drive Cleanings Overview predefined templates provide information about drives that have been cleaned within the libraries.

**STA-Default**

Displays identification and status information for the drive, media, and library involved in each cleaning exchange.

**STA-Cleaning-All**

Displays all cleaning exchange attributes.

**STA-Cleaning-Base-Information**

Displays base information for all cleaning exchanges, such as drive and volume serial number, drive lifetime cleans, and current and maximum cleaning uses.

## Media Validation Overview Predefined Templates

The Media Validation Overview predefined templates provide information about media validation requests.

**STA-Default**

Displays summary information for all media validation requests. The displayed attributes identify the request state, verification test, initiator, and policy name, if applicable. Validation results for completed validations are shown, including recommended action for requests with issues.

**STA-MediaValidation-All**

Displays all available attributes for all media validations.

## All Messages – Overview Predefined Templates

The All Messages - Overview predefined templates provide information about all SNMP traps sent by the libraries.

**STA-Default**

Displays SNMP traps, including detail about the library and device involved.

**STA-Messages-All**

Displays all attributes available for SNMP traps (no graphs are available for this screen).

**STA- Messages-Base-Information**

Displays base data for SNMP traps; useful for an overview, description, and listing of STA messages.

## All Messages – Analysis Predefined Template

The All Messages - Analysis predefined template provides information about all STA messages.

**STA-Default**

Summarizes STA message severity levels by library complex.

# 8

## Filters

Filters reduce the amount of data displayed by a graph or table. Use filters to focus on a subset of information.

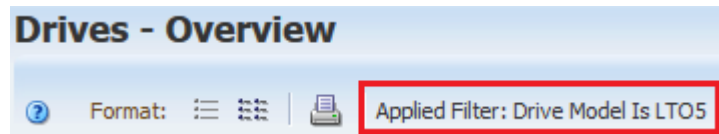
- [View the Filter Applied to the Current Screen](#)
- [Apply a Filter](#)
- [Clear the Current Filter](#)

**See Also:**

- [Filter by Logical Group](#)

### View the Filter Applied to the Current Screen

Once you apply a filter, the criteria displays in the "Applied Filter" area of the table. Use this area to verify which filter criteria has been applied to the current table view. If there is no filter applied, this area is blank.



Filter descriptions longer than 250 characters are truncated. You can hover the cursor over the text to display a tooltip containing the full description.

### Do Filters Apply to Multiple Screens?

A filter applies only to the screen on which you initially create it, except for a few screens on the Drives and Media tab that are paired. For these pairings, any filter applied on one screen is automatically applied to its partner.

The screen pairings are:

- Drives–Overview and Drives–Analysis
- Media–Overview and Media–Analysis
- All Messages–Overview and All Messages–Analysis

### Apply a Filter


Apply a filter by using the filter dialog, applying a template, clicking graph data, or clicking data in a pivot table.

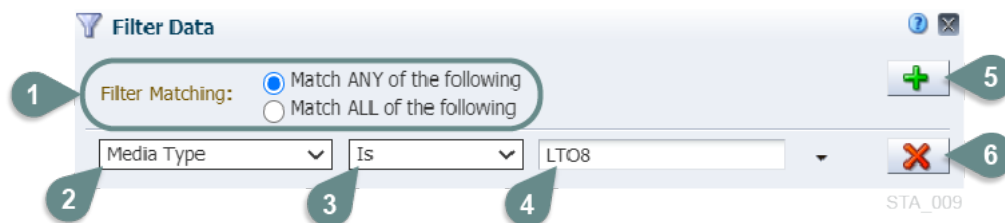
Once you apply a filter to a screen, it remains in effect for the duration of your login session. If you navigate away from the screen and then return, the filter will still be in effect. To change

or remove a filter, you must apply a new filter, remove the filter, apply a template, or log out of STA.

- [Filter Using the Dialog Box](#)
- [Filter by Applying a Template](#)
- [Filter Using Dashboard Graphics](#)
- [Filter Using Pivot Links](#)

## Filter Using the Dialog Box



The filter dialog box appears when you click the **Filter Data** icon  or when you create dynamic logical groups.



1. Select the type of match:
  - **Match ANY of the following** – Selects records that meet any of the criteria you specify. This is the default.
  - **Match ALL of the following** – Selects only records that meet all of the criteria you specify
2. Select an **Attribute**.

### Tip:

Type the first few letters to quickly move to a menu item.

3. Select an **Operator**. See [Filter Operators by Attribute Type](#).
4. Select a **Value**. Text entries are not case sensitive.
5. To add a filter criteria, click **Add** .
6. To remove a filter criteria, click **Remove**  next to the filter.

## Filter Operators by Attribute Type

Operators define how an attribute is used to filter data. The available operators vary depending on the type of attribute.

### Text attribute operators

Examples of text attributes include Drive Health Indicator, Volume Serial Number and Drive WWNN. Some criteria values are free-form and some must be chosen from the drop-down list.

- **Is** – Selects records with attribute values that match the specified string exactly.
- **Isn't** – Selects records with attribute values that do not match the specified string exactly.
- **Is Blank** – Selects records with blank or null attribute values. This is useful for selecting records that have not had a particular attribute value set in STA. For example, the criteria "% Drive Utilization (30 Days) Is Blank" would select all drives that have not been used in the last 30 days.
- **Starts With** – Selects records with attribute values that start with the specified string.
- **Contains** – Selects records that contain the specified string anywhere within the attribute value.
- **Doesn't Contain** – Selects records that do not contain the specified string anywhere within the attribute value.
- **Ends With** – Selects records with attribute values that end with the specified string.

### Logical group operators

Generally, you should use the "Contains" and "Doesn't Contain" operators. The "Is" and "Isn't" operators require an exclusive match and therefore may select no records when the drives or media belong to multiple groups.

- **Is** – Selects drives and media assigned only to the specified logical group and not assigned to any others.
- **Isn't** – Selects all drives and media, except those assigned only to the specified logical group and not assigned to any others.
- **Contains** – Selects drives and media assigned to the specified logical group and any others.
- **Doesn't Contain** – Selects drives and media not assigned to the specified group but assigned to others.

See [Filter by Logical Group](#) for more details.

### Date and time stamp operators

Examples of time stamp attributes include STA Start Tracking (Dates) and Last Exchange Start (Dates).

- **Equals** – Selects entries with attribute dates and times equal to the one you specify.
- **Isn't** – Selects entries with attribute dates and times not equal to the one you specify.
- **Is Before** – Selects entries with attribute dates and times before the one you specify.
- **Is After** – Selects entries with attribute dates and times after the one you specify.



### "Number of days" operators

Examples of "number of days" attributes include STA Start Tracking (No. Days) and Last Exchange Start (No. Days)

- **Less than # days ago** – Selects entries that occurred less than (<) the specified number of days ago.
- **More than # days ago** – Selects entries that occurred more than (>) the specified number of days ago.

Type the value in the associated text entry field.

These operators are especially useful if you want to include a time-related filter in a saved template. By selecting records based on age rather than a specific date and time stamp, the filter is useful now and in the future.

### Numeric operators

Examples of numeric attributes include Media Length in Meters and Exchange Elapsed Time.

- **Is** – Selects records with attribute values equal to the specified value.
- **Isn't** – Selects records with attribute values not equal to the specified value.
- **Less Than** – Selects records with attribute values less than (<) the specified value.
- **Greater Than** – Selects records with attribute values greater than (>) the specified value.

Type the value in the associated text entry field. Do not include units of measure, such as MB, in your entry. Decimals are allowed.

### Boolean operators

Examples of Boolean attributes include Cleaning Media and Exchange Write Inefficient

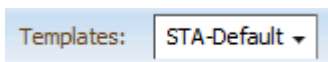
- **True** – Selects records for which the condition is true.
- **False** – Selects records for which the condition is not true.

## Filter by Applying a Template

Applying a template automatically applies any filter criteria included in the template definition. The template filter criteria overrides any filter that may already be in effect.

### Use the Toolbar to Apply a Template

1. Navigate to the screen that you want to apply the template to.
2. In the upper-right, select a template from the **Templates** drop-down menu.



### Use Quick Links to Apply a Template

Quick Links provide quick access to templates available to your STA username.

1. In the left navigation, expand **Home**, and then select **Quick Links**.
2. The templates are grouped by screen name. Predefined templates are identified with an asterisk (\*). Click a template in the list to load the template.

 **Note:**

STA-Default" is not shown in the Quick Links list.

### Quick Links

Click any of the template links below to navigate to a page with the template pre-applied

Dashboard Templates	Library Complexes Templates
<ul style="list-style-type: none"> <li>Admin Default</li> <li>Demo Dashboard</li> <li>MB-Test1</li> </ul>	<ul style="list-style-type: none"> <li><b>STA-Complex-All *</b></li> <li>STA-Complex-Configuration *</li> <li>STA-Complex-Utilization *</li> </ul>

### Use Templates Management to Apply a Template

1. You must have Operator or Administrator privileges.
2. In the left navigation, expand **Setup & Administration**, then select **Templates Management**.
3. In the table, click the name of the template you want to load.

 **Note:**

The "STA-Default" templates are not shown in the list.

### Templates Management

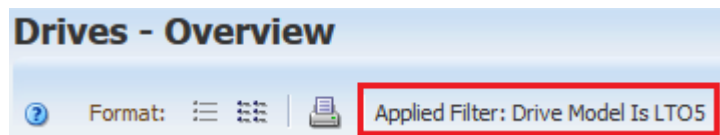
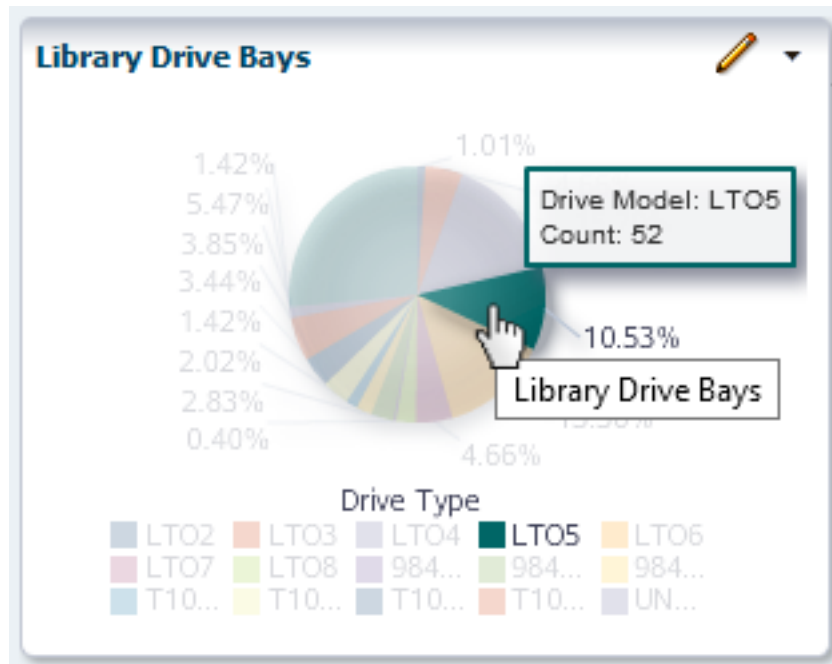
Name	Created/Updated
STA-Alert-All	2017-07-28 14:38:18
<a href="#">STA-Messages-All</a>	2017-07-28 14:38:18
STA-Messages-Base-Information	2017-07-28 14:38:18
STA-CAP-All	2017-07-28 14:38:18

Click to apply this template

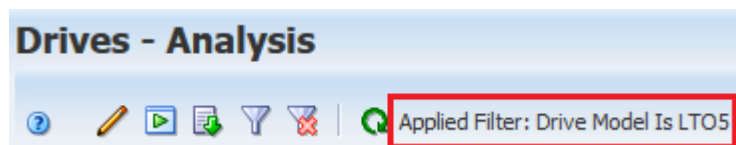
## Filter Using Dashboard Graphics

Click a component of a bar, pie, or area chart to bring up a list for the selected resource with a corresponding filter applied.

For example, if you click the LTO5 portion of the Library Drive Bays pane, it will display the Drives-Overview screen with the filter "Drive Model Is LTO5" applied.



Clicking the paired screen "Drives - Analysis" will display data with this same filter.



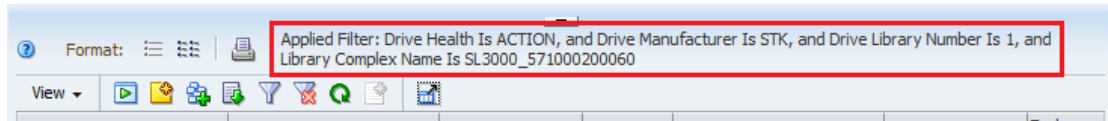
Some graph sections may not have associated detailed information to display. Therefore, clicking some graph sections may not link anywhere (such as unallocated media slots).

## Filter Using Pivot Links

The cells within pivot tables contain counts of resources or events that meet specific criteria. Click a value within the pivot table to apply a filter corresponding to that cell.


For example, in the following Drives – Analysis pivot table, the "4" in the ACTION column indicates that there are a total of four STK drives with a health status of "Action" in the SL3000\_5 library. Clicking on this link takes you to the Drives – Overview screen and applies a filter for drives.

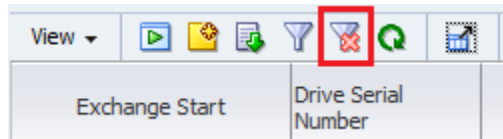
	ACTION	EVALUATE	MONITOR	USE
SL3000_5 1	STK	4	0	3 7
	HP	0	0	1 9
	IBM	1	0	0 13
	UNKNOWN	0	0	0 0
	<b>Drive Manufacturer Total</b>	<b>5</b>	<b>0</b>	<b>4 29</b>





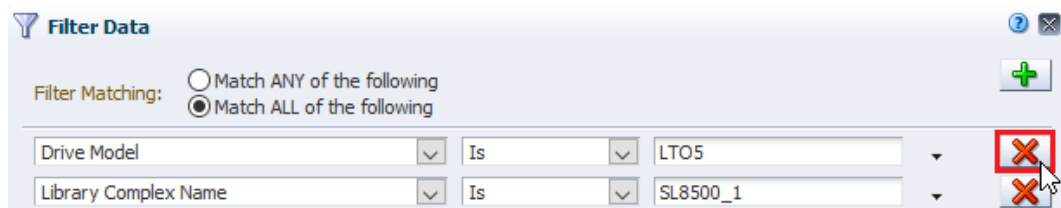
## Clear the Current Filter

Remove filter criteria from a table to increase the number of items displayed.

1. To clear all filter criteria, click **Reset Filter**  in the toolbar.



2. To remove a single criteria from the filter, click **Filter Data**  in the toolbar.  
Then, in the Filter Data dialog, click **Remove**  next to the filter. Click **Apply**.



### Don't See the Filter Icons?

If you don't see the Reset Filter or Filter Data icons in the toolbar, you may be in Detail View format. Toggle to List View.



# 9

## Alerts

Alerts notify you of events and conditions in your tape library system based on user-defined policies.

You can create as many alert policies as you want. Each policy identifies the alert frequency as well as the types of conditions and events that trigger the alert. Optionally, STA can send alerts to email addresses.

- [How Alerts Work](#)
- [Best Practices for Alert Policies](#)
- [Define Alert Policies](#)
- [View Alerts](#)
- [Change the State of an Alert](#)
- [User Roles for Alerts Management](#)
- [Alert Entities](#)
- [Alert Severities](#)
- [Alert Policy Examples](#)
- [Sample Alert Emails](#)

### How Alerts Work

Administrator users can define and enable multiple alert policies. STA continuously evaluates any enabled alert policies and sends alerts when corresponding events occur.

Alert policies are evaluated when:

- An enabled alert policy is created or modified in any way.
- A drive/media exchange or media validation occurs.
- An SNMP trap is received from a monitored library.
- A library data collection occurs.
- An STA application or server event occurs.
- An automated log bundle is created for a library component or the STA database. This applies only if automatic bundle creation is enabled.

STA generates alerts based on the alert policy criteria and severity. An alert is generated if the policy criteria are matched and enough time has passed since the last alert for the same library resource and event. The time period is determined by the policy severity. If the alert policy includes email addresses, an email containing details about the alert is sent to the designated addresses.

Any STA user can monitor alerts from the **Alerts Overview** screen on the **Tape System Activity** tab. The screen displays a list of generated alerts, and you can sort, filter, export,

and print this list according to your needs. Users with Operator privileges can also annotate selected alerts.

If you are using an alerts workflow at your site, you can update the state of selected alerts to reflect current progress. Alerts workflow management is an optional manual process.

**See Also:**

- [Create, Copy, or Modify an Alert Policy](#)
- [Alert Severities](#)
- [Alert Policy Examples](#)
- [Sample Alert Emails](#)
- [Alerts Workflow](#)

## Best Practices for Alert Policies

Follow best practices when creating and managing alert policies to maximize their effectiveness.

### **Create custom alert policies**

Create custom alert policies to address site-specific concerns. This is a parallel practice to creating custom templates. Do not use the "STA" prefix when naming your customized versions. This prefix is used for the sample STA alert policies.

### **Copy the STA sample alert policies**

Unlike the predefined templates delivered with STA, the sample alert policies are not write-protected, and you can modify them directly. However, if you modify or delete the sample policies, you cannot restore them to their original state. For any modifications, it is recommended that you copy the sample policy and modify the copy while leaving the original unchanged.

See [Create, Copy, or Modify an Alert Policy](#).

It is also recommended that you print a record of the sample policies as delivered, so you can re-create them manually if necessary. The sample alert policies are not write-protected and cannot be restored. You should keep copies of the sample policies even if you do not use them.

See [View a List of Alert Policies](#).

### **Avoid too many alerts**

You should define alert policies using criteria specific to the policy entity type. For exchange and media validation alert policies, use criteria unique to exchanges and validations and not available for drives and media. Otherwise, you may create overlapping alert policies that result in multiple alerts and emails for the same event or resource attribute.

For example, you could create and enable all three of the following policies:

- Warning policy for Media: Drive Health Indicator is MONITOR or Media Health Indicator is MONITOR
- Warning policy for Drives: Drive Health Indicator is MONITOR or Media Health Indicator is MONITOR

- Policy for Exchanges: Drive Health Indicator is MONITOR or Media Health Indicator is MONITOR

The Media and Drive alert policies would each generate an alert every 24 hours for each drive and media with MONITOR health. In addition, the Exchanges alert policy would generate an alert every time a drive or media with MONITOR health is involved in an exchange. You could potentially get scores of alerts from a single drive or media with MONITOR health.

A better approach would be to create and enable the following policies:

- Warning policy for Media: Media Health Indicator is MONITOR
- Warning policy for Drives: Drive Health Indicator is MONITOR
- Policy for Exchanges: Alert: Drive Dump Available Is True

#### **Use the "Contains" operator for alerts relating to logical groups**

When defining alert policies for drives or media, you can use logical groups in the selection criteria. Because drives and media can belong to more than one logical group at a time, it is usually appropriate to use the "Contains" and "Doesn't Contain" operators when specifying the criteria, rather than the "Is" and "Isn't" operators.

See [Filter by Logical Group](#).

#### **Create an alert for duplicate volsers**

It may be useful to define alert policies to notify you of duplicate volume serial numbers (volsers).

See [How STA Handles Duplicate Volume Serial Numbers](#).

## Define Alert Policies

An administrator user can define and enable alert policies.

- [View a List of Alert Policies](#)
- [Create, Copy, or Modify an Alert Policy](#)
- [Modify Email Recipients for an Alert Policy](#)
- [Enable or Disable an Alert Policy](#)

## View a List of Alert Policies

The Alerts Policies screen shows all policies created for the STA system.

1. You must have Operator or Administrator privileges.
2. In the left navigation, expand **Setup & Administration**, then select **Alerts Policies**.
3. Optionally, you can apply filters to the table.





See [Filter Using the Dialog Box](#).

## Create, Copy, or Modify an Alert Policy

Use the Alert Policies Wizard to create, copy, or modify an alert policy.

### ▲ Caution:

The STA sample policies are not write-protected. You cannot restore the original versions once they are modified. Copy the original version before making modifications.

1. You must have Administrator privileges.
2. In the left navigation, expand **Setup & Administration**, then select **Alerts Policies**.
3. Use the toolbar to:
  - *Create a new policy:* Click **New Alert Policy** .
  - *Copy a policy:* Select a policy in the list, and then click **Copy Alert Policy** .
  - *Modify a policy:* Select a policy in the list, and then click **Edit Alert Policy** .
  - *Delete a policy:* Select a policy in the list, and then click **Delete Alert Policy** .
4. Use the wizard to configure the policy. Proceed to [Alert Policy Wizard](#).

## Alert Policy Wizard

The policy wizard appears whenever you create, modify, or copy an alert policy.

Within the wizard, you can select the breadcrumb links to go directly to any screen you have already visited.




1. On the *Policy Name* screen of the wizard, enter:
  - *Policy Name* — a unique name using any alphanumeric characters up to 250 characters in length. All sample alert policies beginning with "STA," so you should not start with this prefix.
  - *Policy Description* (optional) — This information is included in alert emails. You may want to use this field to specify recommended corrective actions for alerts generated by this policy.
2. On the *Policy Type* screen of the wizard, select:



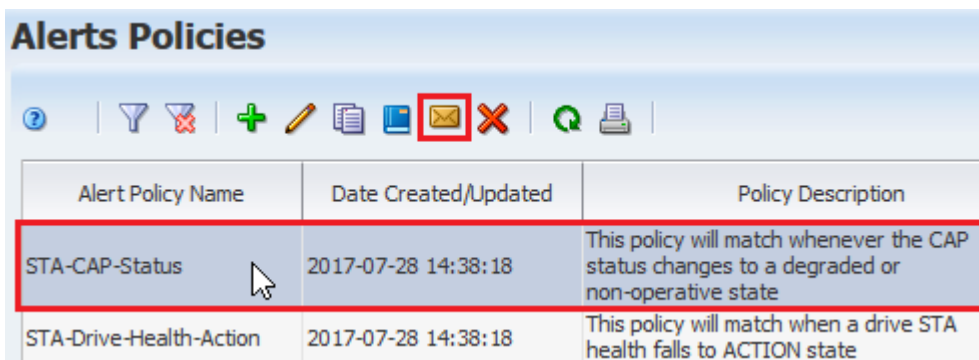
- **Entity Type** — The type of library system component for which this policy may generate alerts. Options include libraries, drives, media, exchanges, and media validations. See [Alert Entities](#) for a complete list.
  - **Severity** — The severity level of the alert policy. Determines the frequency with which alerts may be generated whenever the criteria defined by this policy are met. See [Alert Severities](#) for information about severity levels.
3. On the *Alert Criteria* screen of the wizard, specify filters you wish to apply.  
See [Filter Using the Dialog Box](#).  
  
You can define alerts based on any attribute available for the selected alert Entity. However, not all attributes create events that will actually trigger an alert. In addition, for Media Validation alert policies, alerts are triggered by final validation results only, not intermediate results.
  4. On the *Recipients* screen of the wizard, select the `Email Recipients`.
  5. On the *Review* screen:
    - Verify that all the policy information is correct.
    - Use the `Enable Alert Policy` checkbox as follows:
      - Select the check box to create the policy and enable it immediately.
      - Deselect the check box to create the policy but leave it disabled for now.

## Modify Email Recipients for an Alert Policy

Add or remove email recipients for an alert policy. Recipients receive a notification for all alerts generated by the policy.

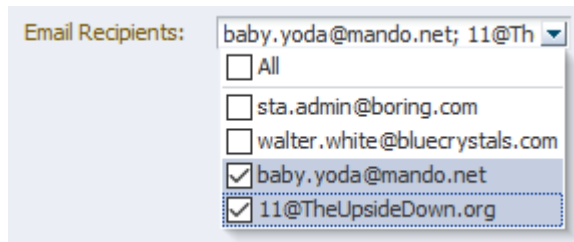
1. You must have Administrator privileges.
2. In the left navigation, expand **Setup & Administration**, then select **Alerts Policies**.
3. Select a policy in the list, and then click **Edit Email Recipients** .

**Alerts Policies**



Alert Policy Name	Date Created/Updated	Policy Description
STA-CAP-Status	2017-07-28 14:38:18	This policy will match whenever the CAP status changes to a degraded or non-operative state
STA-Drive-Health-Action	2017-07-28 14:38:18	This policy will match when a drive STA health falls to ACTION state

4. From the **Email Recipients** drop-down, select addresses that you want to receive alerts. Deselect the addresses you do not want to receive alerts.



5. Click **OK**.

**See Also:**



- [Sample Alert Emails](#)

## Enable or Disable an Alert Policy

Choose to enable or disable an alert policy. Only enabled policies generate alerts.

1. To ensure email recipients are notified of all alerts generated by a particular policy, you should add the recipients to the policy before enabling it.

See [Modify Email Recipients for an Alert Policy](#).

2. You must have Administrator privileges.
3. In the left navigation, expand **Setup & Administration**, then select **Alerts Policies**.
4. Select the policy in the list, and then click **Enable Alert Policy**  or **Disable Alert Policy** .
  - If enabled, the corresponding tape library resources or events are immediately evaluated against the policy criteria, and alerts are generated.
  - If disabled, alerts are no longer generated for the policy.

Alerts Policies		
Alert Policy Name	Date Created/Updated	Policy Description
STA-CAP-Status	2017-07-28 14:38:18	This policy will match whenever the CAP status changes to a degraded or non-operative state
STA-Drive-Health-Action	2017-07-28 14:38:18	This policy will match when a drive STA health falls to ACTION state

## View Alerts

View the alerts created for STA.

- [View a List of Generated Alerts](#)
- [Display Details for an Alert](#)
- [Show or Hide Dismissed Alerts](#)

## View a List of Generated Alerts

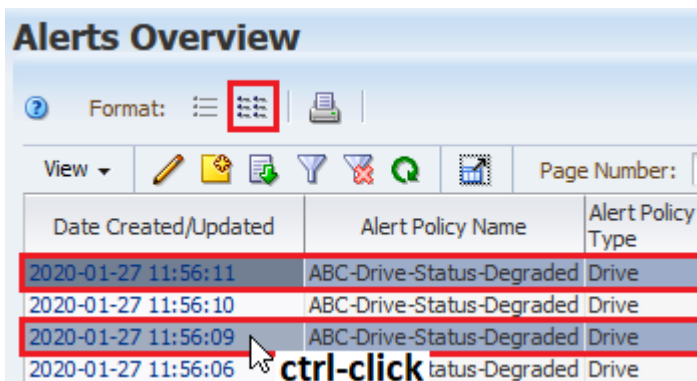
The Alerts Overview screen shows all active (not dismissed) alerts that have been generated to-date.

1. In the left navigation, expand **Tape System Activity**, then select **Alerts Overview**.
2. Optionally, you can apply filters to the list.  
See [Filter Using the Dialog Box](#).
3. To annotate an alert, see [Annotate a Table Row](#). Annotating requires Operator privileges.

## Display Details for an Alert

Display details about an alert to identify the tape library system event or condition that triggered it.

1. In the left navigation, expand **Tape System Activity**, then select **Alerts Overview**.
2. Select the alerts you want to view (shift- or ctrl-click to select multiple alerts). Click **Detail View**.



**Alerts Overview**

Format: [Format Icon] [Print Icon]

View [View Icon] [Edit Icon] [Add Icon] [Refresh Icon] [Filter Icon] [Refresh Icon] [Print Icon] Page Number: [Page Number Input]

Date Created/Updated	Alert Policy Name	Alert Policy Type
2020-01-27 11:56:11	ABC-Drive-Status-Degraded	Drive
2020-01-27 11:56:10	ABC-Drive-Status-Degraded	Drive
2020-01-27 11:56:09	ABC-Drive-Status-Degraded	Drive
2020-01-27 11:56:06	ABC-Drive-Status-Degraded	Drive

ctrl-click

3. The detail view contains links to other screens containing related information. Click the links to gather information on what triggered the alert.

For example, you might click the Alert Event Type link to trace the cause of the alert and determine whether you need to take any action.



**Other Details**

Alert Policy Type: [Drive](#)

Component ID: [MXP1124CFM](#)

Alert State: [New](#)

Alert Event Type: [Trap](#)

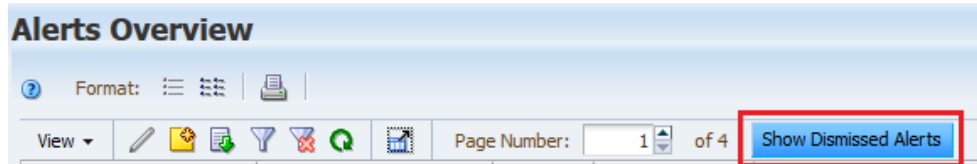
Alert Reason: [Last Drive Message=DEGRADED](#)

## Show or Hide Dismissed Alerts

Choose whether to hide or display dismissed alerts on the Alerts Overview screen. By default, all dismissed alerts are hidden from view.

See [Change the State of an Alert](#) for details on how alerts are dismissed.

1. In the left navigation, expand **Tape System Activity**, then select **Alerts Overview**.
2. Click **Show Dismissed Alerts**.




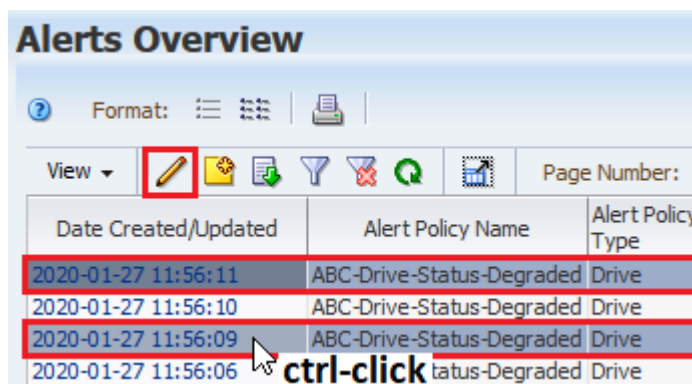
3. To hide the dismissed alerts again, click **Hide Dismissed Alerts**.

## Change the State of an Alert

Change the state of alerts according to the alerts workflow process implemented at your site.

See [Alerts Workflow](#) for an example workflow.

1. In the left navigation, expand **Tape System Activity**, then select **Alerts Overview**.
2. Select the alerts you want to modify (shift- or ctrl-click to select multiple). Click **Change Alert State** .



3. From the drop-down, select the state you want to assign, and then click **OK**.
4. If you changed the selected alerts to "Dismissed," and the Alerts Overview screen is set to hide dismissed alerts, the alerts are removed from the display. See [Show or Hide Dismissed Alerts](#).

## Alerts Workflow

You can set alerts on the Overview screen to several predefined states. The progression of an alert through various states is called a workflow.

Change the alert state depending on the current action being taken for the alert. You can implement the alerts workflow in whatever manner best suites your site, but a suggested progression of alert states is:

1. New – STA assigns this state to all alerts when they are created.
2. Acknowledged – The alert has been noted.
3. In Progress – The alert has been assigned to a responsible party and is being evaluated.
4. Dismissed – The responsible party has completed all activity on the alert. By default, all dismissed alerts are hidden on the Alerts Overview screen, but you can optionally display them. See [Show or Hide Dismissed Alerts](#).

See [Change the State of an Alert](#) for details on using alert states to implement a manual workflow.

## User Roles for Alerts Management

A user's access to alerts is determined by their role.

**Table 9-1 Alert Privileges for User Roles**

User Role	Activity	Screen
Operator and above	Display, filter, and print a list of defined alert policies.	<b>Setup &amp; Administration</b> , then select <b>Alerts Policies</b> .
Administrator only	Define, copy, rename, delete, enable, or disable an alert policy. Change the policy criteria. Change the list of email recipients.	<b>Setup &amp; Administration</b> , then select <b>Alerts Policies</b> .
Viewer and above	Display, filter, and print a list of all generated alerts. Export the alerts list to a spreadsheet or document.View detail for a selected alert. Change the state of a selected alert. Show or hide dismissed alerts.	<b>Tape System Activity</b> , then select <b>Alerts Overview</b> .
Operator and above	Annotate an alert.	<b>Tape System Activity</b> , then select <b>Alerts Overview</b> .

## Alert Entities

Alert entities correspond to a particular type of tape library resources and events.

The supported entities are:

- Library complex
- Library
- Drive
- Media
- Robot
- CAP
- PTP – Relevant only to SL8500 libraries.

- Elevator – Relevant only to SL8500 libraries.
- Exchange – See [Alert Severities](#) for information about how Exchange alert policies are processed differently from other policy types.
- Media validation – Applies only if media validation is enabled in STA. Alerts are triggered by final validation results only, not intermediate results.
- STA application itself – Notifies whenever the STA application restarts.

## Alert Severities

The policy severity determines the frequency with which alerts are generated.

The severity levels are:

- Severe – An alert may be generated once an hour.
- Warning – An alert may be generated once every 24 hours.
- Informative – Only one alert is generated; no additional alerts are generated, even if the policy criteria continue to be met.

See [Alert Policy Examples](#) for examples detailing the effects of the assigned severity levels.

### Alert Severities for Exchange and Media Validation are Irrelevant

Because exchanges and media validations are events, not resources, they generate alerts whenever a new exchange or validation is processed and the policy criteria are matched, regardless of time frames.

Therefore, the severity levels you assign to these alert policies are irrelevant. See [Policy for Exchanges Using "Media Health Indicator" Example](#) and ["Warning" Policy for Media Using "Media Health Indicator" Example](#) below for details.

Additionally with exchange and media validation alert policies, you must take care not to create overlapping policies that might generate multiple alerts from the same exchange or validation. See [Best Practices for Alert Policies](#) for details.

## Alert Policy Examples

Alert policy examples illustrate how and when STA generates alerts based on specific policy criteria and severities.

These examples show how a policy's severity level influences the frequency of alert generation. You can use this information to decide which severity levels to assign to your alert policies.

- ["Warning" Policy for Drives Example](#)
- ["Informative" Policy for Drives Example](#)
- ["Severe" Policy for Media Example](#)
- ["Severe" Policy for CAPs Example](#)
- [Policy for Exchanges Using "Media Health Indicator" Example](#)
- ["Warning" Policy for Media Using "Media Health Indicator" Example](#)

## "Warning" Policy for Drives Example

This example policy generates alerts for drives that require attention because they have ACTION or EVALUATE health.

**Policy entity:** Drives

**Policy severity:** Warning – alerts may be generated every 24 hours.

**Policy criteria:** Drive Health Indicator is ACTION, or Drive Health Indicator is EVALUATE.

Time/Events	Evaluation	Result
05:00:17, Day 1 The policy is created and enabled. Drive 1 health is EVALUATE. Drive 2 health is MONITOR.	The policy is evaluated for all drives and matched for Drive 1 but not Drive 2.	An alert is generated for Drive 1 and emails sent to the defined recipients. No alert for Drive 2.
08:12:24, Day 1 Drive 1 health goes to ACTION. Drive 2 health is still MONITOR.	The policy is evaluated for all drives and matched for Drive 1 but not Drive 2.	Since it has been less than 24 hours since the last alert for Drive 1, no new alert is generated. No alert for Drive 2.
13:37:01, Day 1 Drive 1 health is still ACTION. Drive 2 health goes to EVALUATE.	The policy is evaluated for all drives and matched for both Drive 1 and Drive 2.	No alert for Drive 1. An alert is generated for Drive 2 and emails sent to the defined recipients.
05:01:03, Day 2 Drive 1 health is still ACTION. Drive 2 health is still EVALUATE.	The policy is evaluated for all drives and matched for both Drive 1 and Drive 2.	Since it has been more than 24 hours since the previous alert for Drive 1, a new alert is generated and emails sent to the defined recipients. No new alert for Drive 2 since it has been less than 24 hours since the last alert for Drive 2.
17:08:43, Day 2 A new email recipient is added to the policy. Drive 1 health is still ACTION. Drive 2 health is still EVALUATE.	The policy is evaluated for all drives and matched for both Drive 1 and Drive 2.	No new alert for Drive 1. Since it has been more than 24 hours since the previous alert for Drive 2, a new alert is generated and emails sent to the defined recipients.

## "Informative" Policy for Drives Example

This example policy generates alerts for drives that require attention because they have ACTION or EVALUATE health, but with the Informative severity.

**Policy entity:** Drives

**Policy severity:** Informative – alerts are generated only once.

**Policy criteria:** Drive Health Indicator is ACTION, or Drive Health Indicator is EVALUATE.

Time/Events	Evaluation	Result
05:00:171 The policy is created and enabled. Drive 1 health is EVALUATE. Drive 2 health is MONITOR.	The policy is evaluated for all drives and matched for Drive 1 but not Drive 2.	An alert is generated for Drive 1 and emails sent to the defined recipients. No additional alerts will be generated by this policy for this drive. No alert for Drive 2.
08:12:24 Drive 1 health goes to ACTION. Drive 2 health is still MONITOR.	The policy is evaluated for all drives and matched for Drive 1 but not Drive 2.	No new alert for Drive 1. No alert for Drive 2.
13:37:01 Drive 1 health is still ACTION. Drive 2 health goes to EVALUATE.	The policy is evaluated for all drives and matched for both Drive 1 and Drive 2.	No new alert for Drive 1. An alert is generated for Drive 2 and emails sent to the defined recipients. No additional alerts will be generated by this policy for this drive.
05:01:03 Drive 1 health is still ACTION. Drive 2 health goes to USE.	The policy is evaluated for all drives and matched for Drive 1 but not Drive 2.	No new alerts for Drive 1 nor Drive 2.

## "Severe" Policy for Media Example

This example policy generates alerts for exchanges resulting in a 5135 FSC. This FSC indicates issues with the tape leader, and the media should be ejected from the library and examined as soon as possible.

**Policy entity:** Media

**Policy severity:** Severe – Alerts may be generated every hour depending on exchange activity.

**Policy criteria:** Exchange FSC is 5135.

Time/Events	Evaluation	Result
08:00:53 The policy is created and enabled.	The policy is evaluated as new exchanges are processed and no match is found.	No alerts are generated.



Time/Events	Evaluation	Result
08:05:09 A 5135 FSC occurs on an exchange for Media A.	The policy is evaluated as new exchanges are processed and matched for Media A.	An alert is generated for Media A and emails sent to the defined recipients.  No additional alerts will be generated by this policy for this exchange. Media A will have no more alerts from this policy until it is involved in a new exchange (assuming future exchanges also result in a 5135 FSC).
09:13:17 A 5135 FSC occurs on an exchange for Media B.	The policy is evaluated for new exchanges and matched for Media B.	An alert is generated for Media B and emails sent to the defined recipients.  No additional alerts will be generated by this policy for this exchange.
10:35:22 A 5135 FSC occurs on a new exchange for Media A.	The policy is evaluated for new exchanges and matched for Media A.	An alert is generated for Media A and emails sent to the defined recipients.  No additional alerts will be generated by this policy for this exchange.

## "Severe" Policy for CAPs Example

This example policy generates alerts for CAPs that require attention.

**Policy entity:** CAPs

**Policy severity:** Severe – Alerts may be generated every hour.

**Policy criteria:** CAP Library Health is NOTOPERATIVE or CAP Library Health is DEGRADED.

Time/Events	Evaluation	Result
14:05:10 The policy is created and enabled. CAP 1A is in a DEGRADED state.	The policy is evaluated for all CAPs and matched for CAP 1A.	An alert is generated for CAP 1A and emails sent to the defined recipients.
15:01:12 CAP 2B goes into a NOTOPERATIVE state.	The policy is evaluated for all CAPs and matched for both CAP 1A and CAP 2B.	No new alert for CAP 1A. An alert is generated for CAP 2B and emails sent to the defined recipients.
15:05:20 CAP 1A is still DEGRADED and CAP 2B is still NOTOPERATIVE.	The policy is evaluated for all CAPs and matched for both CAP 1A and CAP 2B.	A new alert is generated for CAP 1A and emails sent to the defined recipients. No new alert for CAP 2B.

Time/Events	Evaluation	Result
16:01:27 CAP 1A is still DEGRADED and CAP 2B is still NOTOPERATIVE.	The policy is evaluated for all CAPs and matched for both CAP 1A and CAP 2B.	No new alert for CAP 1A. An new alert is generated for CAP 2B and emails sent to the defined recipients.

## Policy for Exchanges Using "Media Health Indicator" Example

This example policy generates alerts for exchanges where the media health indicator is Evaluate.

Exchange alert policies differ from policies for other library system components in that the severity of the policy is irrelevant. Because exchanges are discrete events, exchange alert policies always generate alerts when the policy criteria are met, regardless of policy severity.

**Policy entity:** Exchanges

**Policy severity:** Because this is an exchange alert, the policy severity is irrelevant. In this case, the severity is "Informative," but the results would be the same for all severity levels: alerts are generated for all exchanges involving media with EVALUATE health.

**Policy criteria:** Media Health Indicator is EVALUATE.

Time/Events	Evaluation	Result
13:13:17, Day 1 The policy is created and enabled. Media Z health is EVALUATE.	The policy is evaluated for all exchanges and no match is found.	No alert is generated.
14:43:09, Day 1 An exchange occurs for Media Z, whose health is EVALUATE.	The policy is evaluated for all exchanges and matched for Media Z.	An alert is generated for Media Z and emails sent to the defined recipients.
07:20:24, Day 1 Another exchange occurs for Media Z, whose health is still EVALUATE.	The policy is evaluated for all exchanges and matched for Media Z.	A new alert is generated for Media Z and emails sent to the defined recipients.
15:05:19, Day 2 Another exchange occurs for Media Z, whose health is still EVALUATE.	The policy is evaluated for all exchanges and matched for Media Z.	A new alert is generated for Media Z and emails sent to the defined recipients.

## "Warning" Policy for Media Using "Media Health Indicator" Example

This example policy generates alerts for media with EVALUATE health.

This example is similar to [Policy for Exchanges Using "Media Health Indicator" Example](#), but because it is a Media alert policy, it results in fewer alerts.

**Policy entity:** Media

**Policy severity:** Warning – alerts may be generated every 24 hours.

**Policy criteria:** Media Health Indicator is EVALUATE.

Time/Events	Evaluation	Result
13:13:17, Day 1 The policy is created and enabled. Media Z health is EVALUATE.	The policy is evaluated for all media and matched for Media Z.	An alert is generated for Media Z and emails sent to the defined recipients.
14:43:09, Day 1 An exchange occurs for Media Z, whose health is still EVALUATE.	The policy is evaluated for all media and matched for Media Z.	Since it has been less than 24 hours since the last alert for Media Z, no new alert is generated.
07:20:24, Day 2 Another exchange occurs for Media Z, whose health is still EVALUATE.	The policy is evaluated for all media and matched for Media Z.	No new alert is generated for Media Z since it has still been less than 24 hours since the last one.
15:05:19, Day 2 Another exchange occurs for Media Z, whose health is still EVALUATE.	The policy is evaluated for all media and matched for Media Z.	Since it has been more than 24 hours since the previous alert for Media Z, a new alert is generated and emails sent to the defined recipients.

## Sample Alert Emails

These examples show sample alert emails generated when an alert policy is triggered by an event.

### Example 9-1 Sample Exchange Alert Email

Exchange Started at December 13, 2013 5:52:05 AM MDT and Ended at December 13, 2013 7:15:41 AM MDT

STA Drive Alert - 2013-12-13 07:20:46 (Drive HU1233210W)

Alert Summary:

Policy Desc: Generates an alert when the Drive Health Indicator is Evaluate and Drive Health Trend is Worse.

Criteria Met: Drive Health Indicator=EVALUATE and Drive Health Trend=WORSE

STA Server: sysbiz

DRIVE

Serial Number: HU1233210W

Tray Serial Number: UNKNOWN

Model: HpUltrium6

Last Annotation:

Health Indicator: Evaluate

Health Trend: Worse

Suspicion Level: 90.0

Exchange Status: GOOD

Exchange Tape Alerts - Warning: 0

Exchange Tape Alerts - Critical: 0

Alerts (30 days): 3

### **Example 9-2 Sample STA Application Alert Email**

STA STA Server Alert 2013-12-15 22:39:21 (STA Server bizsys)

Alert Summary:

Policy Desc: This policy will match when the STA software is restarted.  
Criteria Met: staEngine: Server in an UNKNOWN State - Restarting.  
STA Server: bizsys

# 10

## Executive Reports

Executive reports provide high-level information about your tape library system. STA runs reports based on the report policies that you define.

The reports include information from a specific dashboard template, including any annotations. You can run executive reports on a regular schedule and on demand.

- [Best Practices for Executive Reports](#)
- [View, Download, or Delete Executive Report Files](#)
- [Run an Executive Report On Demand](#)
- [Manage Executive Report Policies](#)
- [User Roles for Executive Reports and Policies](#)
- [Sample Executive Report](#)

### Best Practices for Executive Reports

Follow best practices when using executive reports to maximize their usefulness.

#### **Identify and create templates specifically for executive report**

Identify a set of existing templates—or create some new ones—that show the specific areas of interest at your site. Use these templates to generate a set of executive reports for various periods: hourly, daily, weekly, and monthly.

#### **Have executive reports emailed to you**

Have the reports emailed to you automatically for a minimum 30-day period of normal operation. Do this for all tape system resources, particularly for a large tape system: robots, CAPS, drives, media, and so on.

#### **Create a Site Operational Summary**

Use the reports to create a *Site Operational Summary* document that calls out both general and specific aspects of normal operation at your site. By understanding your site's operational profile and having a summary that can be shared, you can more easily identify anomalies in operations.

For example:

- Every Thursday at 16:00: Spike in usage of drives in A-01, up to 60 percent, due to the weekly scientific data import
- Data compression range: 1 to 3.5
- Drive efficiency: approximately 97 percent
- Typical number of monthly cleans: 4

## View, Download, or Delete Executive Report Files

The Executive Reports screen lists all executive reports created by STA. You can download or delete any public reports or those owned by your username.

- [View a List of Executive Reports](#)
- [Download an Executive Report File](#)
- [Delete an Executive Report File](#)

### View a List of Executive Reports

The Executive Reports screen shows a list of all executive reports currently stored on the STA server.

1. In the left navigation, expand **Home**, then select **Executive Reports**.
2. Optionally, you can filter the list to reduce the number of entries displayed.  
See [Filter Using the Dialog Box](#).
3. If you do not see a recent executive report and want to create one, you can run a report on demand.  
See [Run an Executive Report On Demand](#).


### Download an Executive Report File

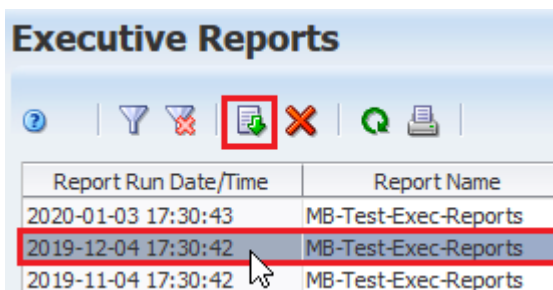
Export an executive report as a PDF file to view its contents.



#### Note:

You only have access to public reports and private ones owned by your username. You cannot perform these tasks on reports privately owned by another user.


1. In the left navigation, expand **Home**, then select **Executive Reports**.
2. Optionally, you can filter the list to reduce the number of entries displayed.  
See [Filter Using the Dialog Box](#).
3. Select a report in the list, and then click **Export** .

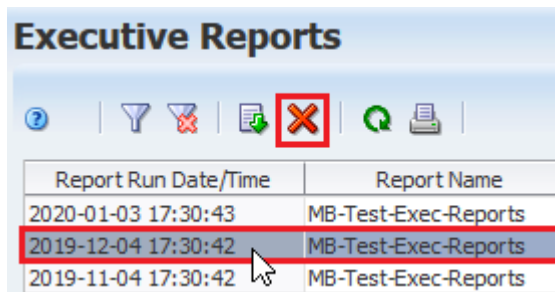


4. Download the file, and then open it with a pdf reader or the browser.

## Delete an Executive Report File

Delete specific report files that you no longer need. This does not affect other report files, nor the report policy definition.


1. In the left navigation, expand **Home**, then select **Executive Reports**.
2. Select the report file from the list, and then click **Delete** . You can select only one report file at a time to delete.



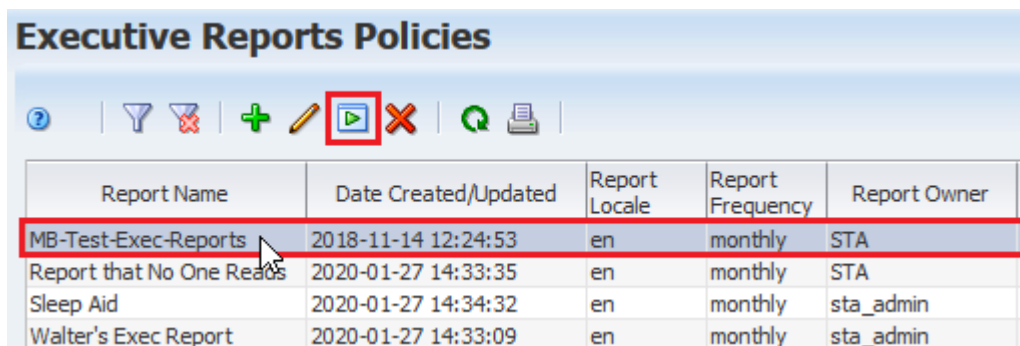
3. Verify and click **Yes**.

## Run an Executive Report On Demand

Run an executive report right away. Creating an on-demand report does not affect the report's schedule. It will also run at its regularly scheduled time.

1. You must have Operator and Administrator privileges.
2. In the left navigation, expand **Setup & Administration**, then select **Executive Reports Policies**.
3. Select the report policy in the list, and then click **Run** .

STA runs the report at the first available opportunity, which could take up to two minutes.



4. In the Reports pop-up, verify the information and click **OK** to run the report.  
See [Download an Executive Report File](#) for instructions on displaying the output.

## Manage Executive Report Policies

Executive report policies define when STA should generate an executive report. The policy is based on a dashboard template and runs automatically at the interval you define.

- [View a List of Executive Report Policies](#)
- [Define an Executive Report Policy](#)
- [Delete an Executive Report Policy](#)



### View a List of Executive Report Policies

View a list of existing executive report policies to identify which you may want to use.

1. You must have Administrator privileges.
2. In the left navigation, expand **Setup & Administration**, then select **Executive Reports Policies**.
3. Optionally, you can filter the list to reduce the number of entries.  
See [Filter Using the Dialog Box](#).

### Define an Executive Report Policy

Create an executive report policy or modify an existing policy. STA regularly runs executive reports based on the policies defined for the system.


1. You must have Administrator privileges.
2. Verify the dashboard template is configured how you want it.
3. In the left navigation, expand **Setup & Administration**, then select **Executive Reports Policies**.
4. Click **Add** , or select a report in the list and then click **Edit** .
5. Enter the following:
  - **Report Name** — a unique name using any alphanumeric characters up to 250 characters in length.
  - **Source Dashboard Template** — Select the template you want to use as the basis of the executive report. The menu lists all dashboard templates available to your STA username.
  - **Locale** — English is the only option at this time.
  - **Start Date** — Specify the date for scheduled runs of the report to begin. Reports run shortly after 00:30 UTC, starting on this date.
  - **Run Frequency** — Select a frequency to run the report.
  - **Shared**
    - *Public* makes the report available to all users.



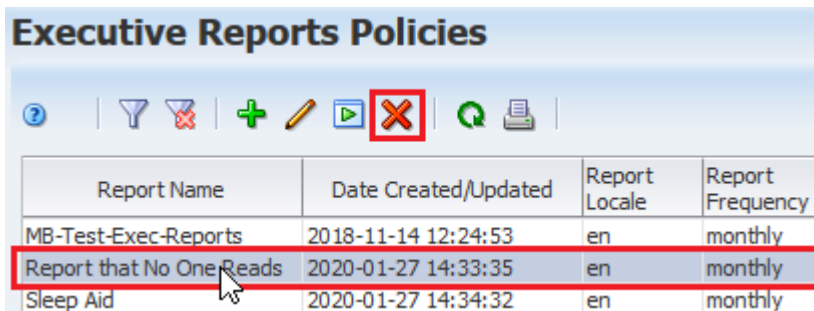
- *Private* makes the report available to only the current STA user. This does not affect the email recipients list. You can have copies of the report sent to other users even if the report is private.
  - **Email Recipients** — Select the email addresses to which you want copies of the report sent after each report run. The report is sent as a PDF attachment as soon as it runs. The menu lists all email addresses that have been defined to STA.
6. Verify the information is correct, and then click either:
- **Save** to save the report policy and have it run for the first time on the designated Start Date.
  - **Save and Run** to save the report policy and run it immediately. This does not affect the schedule you have define. It will also run at its regularly scheduled time, starting on the designated Start Date.

## Delete an Executive Report Policy

Delete public or private policies that have been created by your STA username. Deleting a policy does not delete generated report files. You can still view the reports on the Executive Reports screen.

1. You must have Administrator privileges.
2. In the left navigation, expand **Setup & Administration**, then select **Executive Reports Policies**.
3. Select the report policy from the list, and then click **Delete** .

**Executive Reports Policies**



Report Name	Date Created/Updated	Report Locale	Report Frequency
MB-Test-Exec-Reports	2018-11-14 12:24:53	en	monthly
Report that No One Reads	2020-01-27 14:33:35	en	monthly
Sleep Aid	2020-01-27 14:34:32	en	monthly

4. Verify and click **Yes**.

## User Roles for Executive Reports and Policies

A user's access to executive reports and policies depends on their role.

**Table 10-1 Executive Report User Roles**

User Role	Report Activity	Screen
Administrator only	Create a public or private report policy. Display a list of report policies, including public policies and private policies created by the current STA username. Delete or modify a report policy, including public policies or private policies created by the current STA username, scheduled run, email recipients, and dashboard template.	Select <b>Setup &amp; Administration</b> , then select <b>Executive Reports Policies</b> .
Operator and above	Display, filter, or print a list of public report policies. Run a public report on demand.	Select <b>Setup &amp; Administration</b> , then select <b>Executive Reports Policies</b> .
Operator and above	Delete a public report file run automatically or on demand.	Select <b>Home</b> , then select <b>Executive Reports</b> .
Viewer and above	Display a list of public report files run automatically or on demand, as follows: <ul style="list-style-type: none"> <li>• Export and view a report file.</li> <li>• Filter the report file list.</li> <li>• Print the report file list.</li> </ul>	Select <b>Home</b> , then select <b>Executive Reports</b> .

## Sample Executive Report

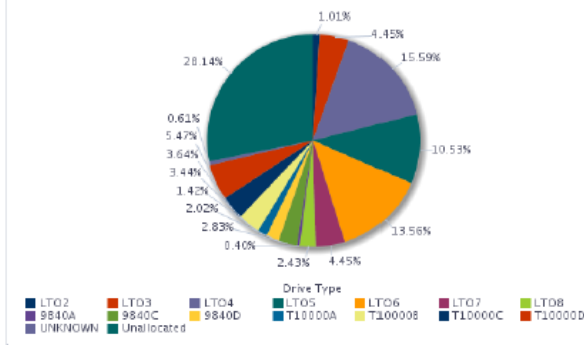
Executive reports help summarize data about your library system. The report is often a series of graphs each with corresponding annotations.

This is a sample page from an executive report.

STA Report: MB-Test-Exec-Reports

2019-12-05 00:30:41

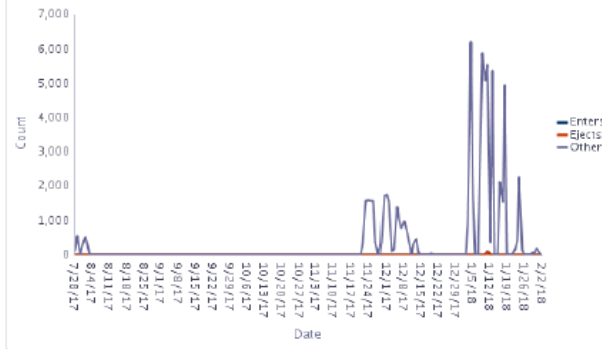
Library Drive Bays



The Library Drive Bays pie chart shows the distribution and types of drives installed within the selected libraries. It also shows unoccupied drive bays in which additional drives could be installed.

As of Dec 5, 2019, there were 139 unallocated drive bays out of 494 total slots (28 percent unoccupied)

Media Movements (Daily)



The Media Movements (Daily) displays the total number of media that were entered, ejected, or otherwise moved across all the libraries STA is monitoring. Other moves are comprised of elevator, PTP, and robotic moves for mounting and dismounting media. Each data point is a daily summary of all movements observed by STA.

# 11

## Logical Groups

Logical groups can help organize data by grouping together specific drives and media.

Logical groups can contain any combination of drives, media, or both. Individual drives and media can belong to more than one logical group at a time.

- [Types of Logical Groups](#)
- [Best Practices for Logical Groups](#)
- [Configure Logical Groups](#)
- [Filter by Logical Group](#)

### Types of Logical Groups

There are two types of logical groups: manual and dynamic.

- **Manual** — The user manually selects the drives and media assigned to the group. See [Create a Manual Logical Group](#).
- **Dynamic** — The user defines a set of filter criteria that STA uses to automatically assign drives and media to the group. Dynamic groups update automatically every hour. When drives and media meet the selection criteria for a group, they are automatically added to the group, and when they no longer meet the criteria, they are automatically removed. See [Create and Define a Dynamic Logical Group](#).

### Best Practices for Logical Groups

Follow these tips when creating and managing logical groups.

#### **Create an example to see how logical groups could be used**

Practice using logical groups, even if you don't see why you need them. Often, in just setting up your first one, you'll recognize how they can be used to simplify your work in STA.

#### **Use meaningful logical group names**

Make logical group names meaningful and easy to distinguish so you can remember the purpose of the group.

#### **Use the "Contains" operator when filtering logical groups**

Drives and media can belong to more than one logical group at a time; therefore, when you filter by logical group, it is usually appropriate to use the "Contains" and "Doesn't Contain" operators, which perform non-exclusive matches, rather than the "Is" and "Isn't" operators, which perform exclusive matches.

See [Filter by Logical Group](#).

## Why Use Logical Groups?

Use logical groups to focus STA data on a particular subset of drives and media.

Logical groups allow you to:

- Filter data on the Drives Overview/Analysis screens, Media Overview/Analysis screens, or dashboard panes using logical groups.
- Save screen layouts that have been filtered by logical group as templates. The filters are saved as part of the templates.
- Create executive reports based on dashboard templates that are filtered by logical group.

### Logical Group Usage Examples

#### Media Validation

If your site has enabled media validation, you can use logical groups when defining automated media validation policies.

#### Library Partitions

A library has eight partitions, and users would like to produce STA reports for drives and media in each partition. To do so, you could create one logical group for each library partition.

#### Libraries in Different Geographic Locations

Two library operators manage libraries at one site and three other operators manage another site. The operators would like to see STA data that apply to drives and media at their site only. To do so, you could create one logical group for each site.

#### Archival Media

An archival site creates two copies of each archived media. To help manage the two sets of media, you could create one logical group for all copy #1 media and another logical group for copy #2 media.

#### Calibration Media

If you choose to enable drive calibration and qualification, which is part of the STA media validation feature, you must define a logical group of media to be used for this purpose. All drive calibration and qualification activities will be done exclusively with these media, and the media should not be used for production data.

## Configure Logical Groups

Some configuration tasks only apply to manual groups, some apply only to logical groups, and some apply to both.

Configuring logical groups requires Operator or Administrator privileges.

- [View Logical Group Assignments for Selected Drives or Media](#)
- [List All Drives and Media Assigned to a Logical Group](#)
- [Rename a Logical Group](#)
- [Delete a Logical Group](#)

### Manual Logical Groups


- [Create a Manual Logical Group](#)
- [Add Drives and Media to a Manual Logical Group](#)
- [Remove Drives and Media From a Manual Logical Group](#)

#### Dynamic Logical Groups

- [Create and Define a Dynamic Logical Group](#)
- [Change the Selection Criteria for a Dynamic Logical Group](#)
- [Force a Dynamic Logical Group Update](#)

## Create a Manual Logical Group

Create a logical group and manually assign drives and media to it. Resources included in the group do not change unless you manually add or remove them.

1. In the left navigation, expand **Setup & Administration**, select **Logical Groups**.
2. Click **Add Logical Group** .
3. Complete the Create Logical Group screen:
  - **Logical Group Name** — a unique name using a maximum of 249 alphanumeric characters.
  - **Logical Group Type** — Select **Manual**
4. Click **Save**.
5. Initially the group will be empty, showing a drive and media count of 0. You must add drives and media to it.

Proceed to [Add Drives and Media to a Manual Logical Group](#) or if creating a group for media validation drive calibration, see [Create the Calibration Media Logical Group](#).

## Logical Group Ownership


The STA username that created the logical group also owns that group. The ownership cannot be changed except when the owner is deleted. The logical group owner is displayed on the Logical Groups screen.

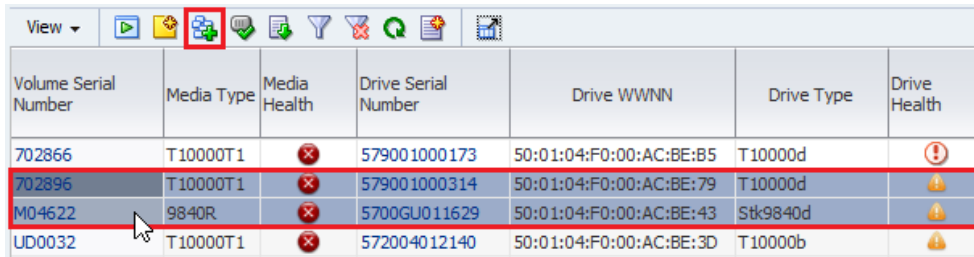
When the administrator deletes an STA username, all logical groups owned by that username are automatically deleted or made public, according to the selection made by the administrator (see [Add, Modify, or Delete a User](#)).









## Add Drives and Media to a Manual Logical Group

When you first create a manual logical group it will be empty. You must manually add drives and media to the group.

1. The logical group must already exist.  
See [Create a Manual Logical Group](#).
2. In the left navigation, expand **Tape System Hardware**. Select either:
  - **Drives – Overview** to add drives
  - **Media – Overview** to add media

3. Within the table, select drives or media to add (shift- or ctrl-click to select multiple). Click **Logical Groups** .



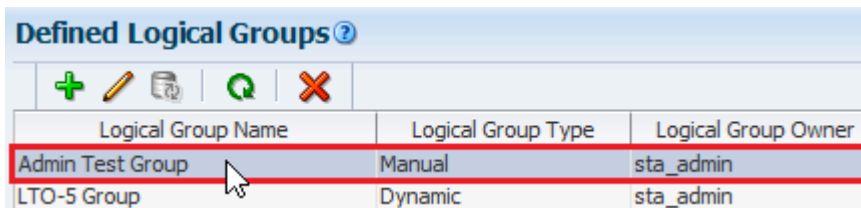
Volume Serial Number	Media Type	Media Health	Drive Serial Number	Drive WWNN	Drive Type	Drive Health
702866	T10000T1		579001000173	50:01:04:F0:00:AC:BE:B5	T10000d	
702896	T10000T1		579001000314	50:01:04:F0:00:AC:BE:79	T10000d	
M04622	9840R		5700GU011629	50:01:04:F0:00:AC:BE:43	Stk9840d	
UD0032	T10000T1		572004012140	50:01:04:F0:00:AC:BE:3D	T10000b	

4. Select the group from the drop-down. Only manual groups appear in the list. You cannot manually add drives and media to a dynamic group.
5. Click **OK**.


## Remove Drives and Media From a Manual Logical Group

Remove selected drives and media from a manual logical group.

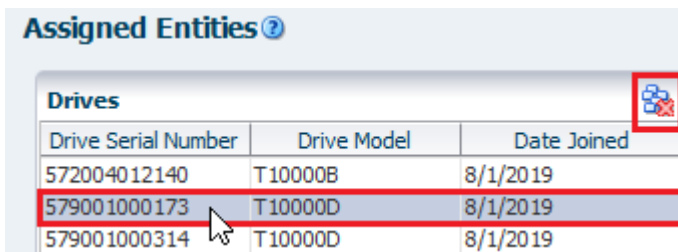
1. In the left navigation, expand **Setup & Administration**, select **Logical Groups**.
2. Within the Defined Logical Groups table, select the manual group to modify.



Logical Group Name	Logical Group Type	Logical Group Owner
Admin Test Group	Manual	sta_admin
LTO-5 Group	Dynamic	sta_admin

3. Within the **Assigned Entities** section, select the drives or media you want to remove from the group, and then click **Unassign Entities** .

You can select multiple records at once, but they must all be from the same table (either Drives or Media).




Drive Serial Number	Drive Model	Date Joined
572004012140	T10000B	8/1/2019
579001000173	T10000D	8/1/2019
579001000314	T10000D	8/1/2019

4. Verify and click **Yes**.

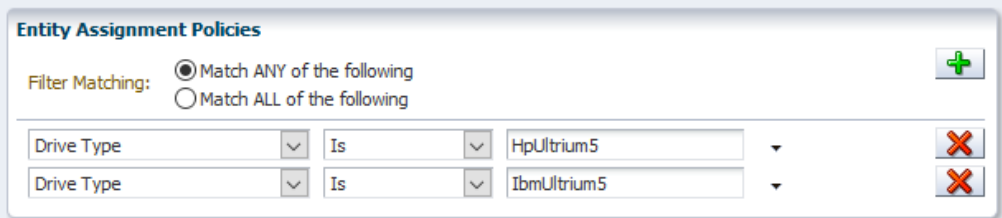
## Create and Define a Dynamic Logical Group


A dynamic group uses selection criteria (filters) to automatically determine which drives and media to include in the group.

When drives and media meet the selection criteria for a group, they are automatically added to the group, and when they no longer meet the criteria, they are automatically removed. Dynamic groups update automatically every hour.

1. In the left navigation, expand **Setup & Administration**, select **Logical Groups**.
2. Click **Add Logical Group** .
3. Complete the Create Logical Groups dialog:
  - **Logical Group Name** — Enter a unique name for the group using up to 250 alphanumeric characters (for example "LTO5- Drives").
  - **Logical Group Type** — Select **Dynamic**.
  - **Entity Assignment Rules** — Select filter criteria for the group ([Dynamic Group Selection Criteria](#)). See [Filter Using the Dialog Box](#) on how to define a filter.

For example, if you wanted all LTO5 drives, you would create this filter:



4. Verify that your criteria are correct and click **Save**.
5. Initially, the media and drive counts for the group are 0. Click **Refresh Table**  to update the drive and media counts.

Depending on the size of your tape library system and the complexity of the selection criteria, it may take several minutes to add all drives and media to the group. Leaving the Logical Groups screen does not interrupt this process.

## Dynamic Group Selection Criteria

A variety of drive and media attributes are available for creating selection criteria. Some attributes apply only to drives, some only to media, and some to both.

The following table identifies the available criteria and whether it applies to drives, media, or both.


Selection Criteria Attribute	Applies to:
Cleaning Media	Media
Drive Firmware Version	Drives
Drive Health Indicator	Drives

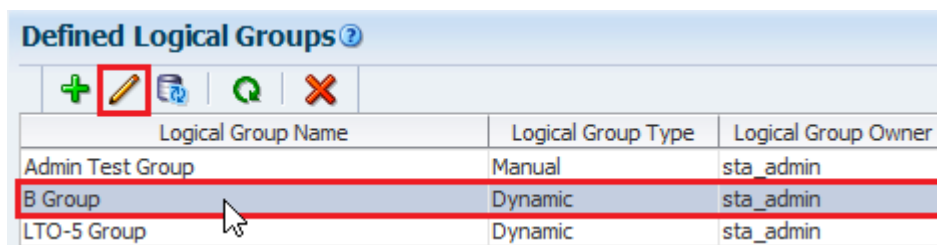


Selection Criteria Attribute	Applies to:
Drive Serial Number	Drives
Drive Type	Drives
Drive Suspicion Level	Drives
HLL Address	Both
Library Complex Name	Both
Library Model	Both
Library Name	Both
Library Number	Both
Library Serial Number	Both
Media Health Indicator	Media
Media Suspicion Level	Media
Media Type	Media
Partition Name	Both
Partition Number	Both
Partition Type	Both
Physical Address	Both
Rail Number	Both
SCSI Element ID	Both
STA Start Tracking (Number of Fays)	Both
STA Start Tracking (Date)	Both
Volume Serial Number	Media

## Change the Selection Criteria for a Dynamic Logical Group

Change the selection criteria for an existing dynamic logical group to modify the drives and media included to the group.


1. In the left navigation, expand **Setup & Administration**, select **Logical Groups**.
2. Select a dynamic group from the list, and then click **Edit Logical Group** .

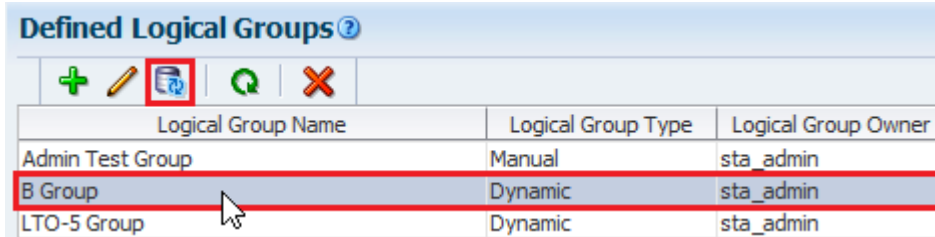


3. Add, delete, and modify selection criteria as necessary.  
See [Filter Using the Dialog Box](#) for instructions.


## Force a Dynamic Logical Group Update

Dynamic groups update automatically every hour, but you can force an update between cycles to reflect any changes to the library contents.

1. In the left navigation, expand **Setup & Administration**, select **Logical Groups**.
2. Select a dynamic group from the list, and then click **Refresh Dynamic Group** .



Logical Group Name	Logical Group Type	Logical Group Owner
Admin Test Group	Manual	sta_admin
B Group	Dynamic	sta_admin
LTO-5 Group	Dynamic	sta_admin

3. STA begins updating the group in the background. Click **Refresh Table**  to update the in-progress drive and media counts.

Depending on the size of your tape library system and the complexity of the selection criteria, it may take several minutes to add all drives and media to the group. Leaving the Logical Groups screen does not interrupt this process.

## View Logical Group Assignments for Selected Drives or Media

View the drive and media assignments for logical groups.

1. In the left navigation, expand **Tape System Hardware**. Select either:
  - **Drives – Overview**
  - **Media – Overview**
2. Select the records you want to display, and click **Detail View**.



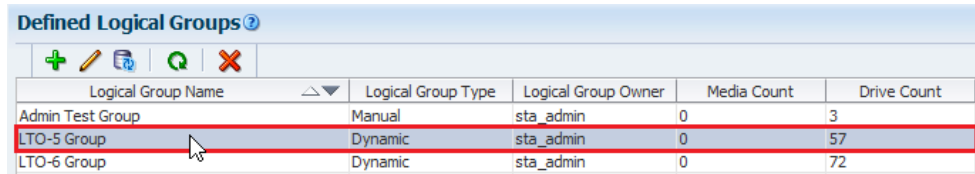
3. Near the bottom of the details view, the **User-Provided Information** section lists all logical group assignments.

## List All Drives and Media Assigned to a Logical Group

Display a list of all drives and media assigned to a selected logical group.

1. In the left navigation, expand **Setup & Administration**, select **Logical Groups**.
2. Within the **Defined Logical Groups** table, select the group.

**Defined Logical Groups** ?



Logical Group Name	Logical Group Type	Logical Group Owner	Media Count	Drive Count
Admin Test Group	Manual	sta_admin	0	3
LTO-5 Group	Dynamic	sta_admin	0	57
LTO-6 Group	Dynamic	sta_admin	0	72

- All assigned drives and media display within the **Assigned Entities** section.


**Assigned Entities** ?

**Drives**

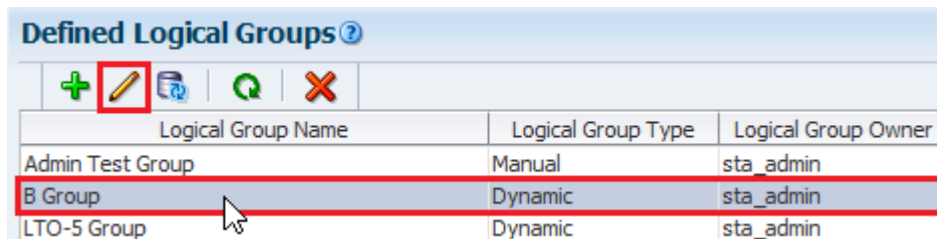
Drive Serial Number	Drive Model	Date Joined
1068001130	LTO5	8/1/2019
1068001274	LTO5	8/1/2019
1068001295	LTO5	8/1/2019

## Rename a Logical Group

Change the name of an existing manual or dynamic logical group.

- In the Navigation Bar, select **Setup & Administration**, then select **Logical Groups**.
- Select the group from the list, and then click **Edit Logical Group** .

**Defined Logical Groups** ?




Logical Group Name	Logical Group Type	Logical Group Owner
Admin Test Group	Manual	sta_admin
B Group	Dynamic	sta_admin
LTO-5 Group	Dynamic	sta_admin

- Enter the new **Logical Group Name**, and then click **Save**.
- The Assigned Entities table indicates the group contains no drives nor media. This is just lag in the table display.

**Assigned Entities** ?

**Drives**


Drive Serial Number	Drive Model	Date Joined
The selected logical group contains no drives.		

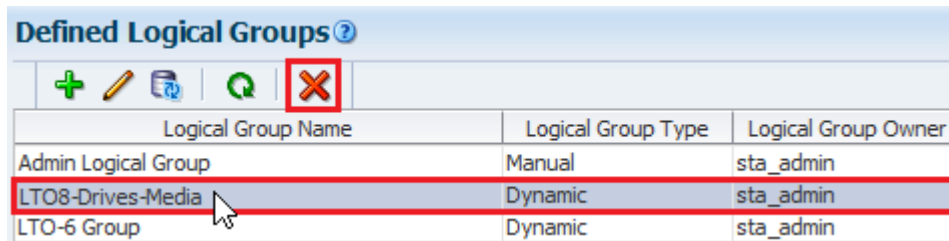
To update the Assigned Entities table display, click refresh  and then re-select the logical group again. The display updates with the assigned drives and media.

## Delete a Logical Group

Delete a manual or dynamic logical group to remove the group from STA.

This procedure deletes the entire logical group. To remove just selected drives or media from a manual group, see [Remove Drives and Media From a Manual Logical Group](#).

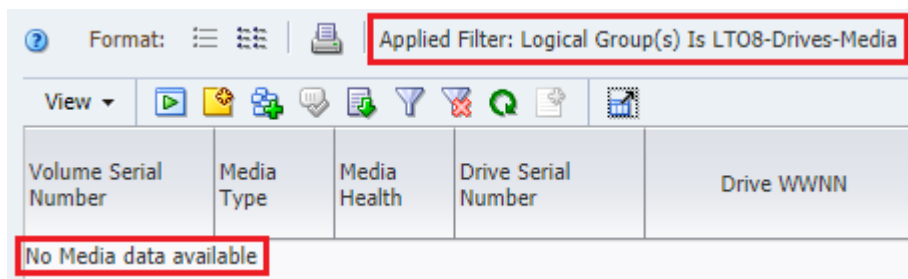
1. In the left navigation, expand **Setup & Administration**, select **Logical Groups**.
2. Select the group from the list, and then click **Delete Logical Group** .



Logical Group Name	Logical Group Type	Logical Group Owner
Admin Logical Group	Manual	sta_admin
LTO8-Drives-Media	Dynamic	sta_admin
LTO-6 Group	Dynamic	sta_admin

3. Verify that you have selected the correct logical group, and then click **Yes**.

Any screens, dashboard panes, or templates filtered by the group now show "No data to display" or "No data available."



Volume Serial Number	Media Type	Media Health	Drive Serial Number	Drive WWNN
No Media data available				

## Filter by Logical Group

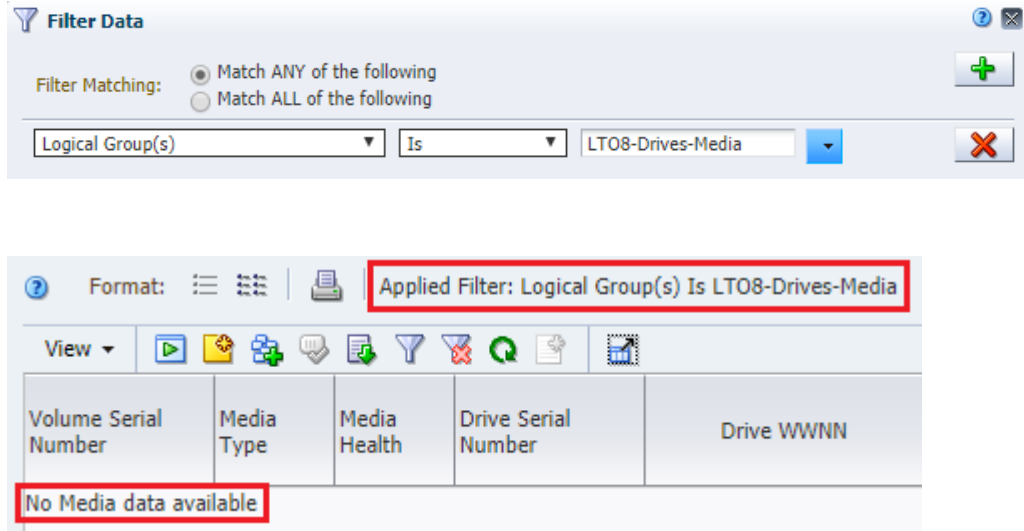
Filter screens by a logical group to focus data on a screen to just the drives and media included in that group.

Use the "Contains" and "Doesn't Contain" operators rather than "Is" and "Isn't" because drives and media can belong to more than one logical group at a time. The "Is" and "Isn't" operators require an exclusive match and therefore may select no records at all when the drives or media belong to multiple groups.

### Example of using the "Is" operator when filtering by logical group

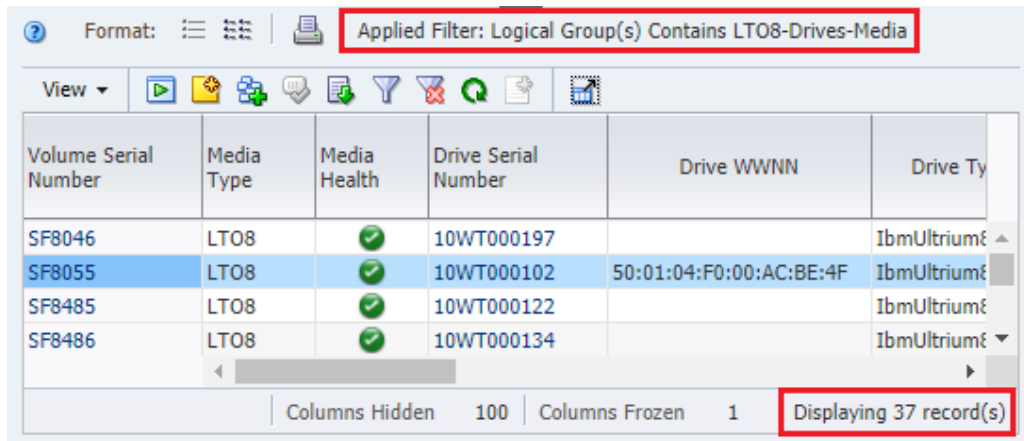
On the Media – Overview screen, using the filter "Logical Group(s) Is LTO8-Drives-Media" selects no records because all the drives and media in the group also belong to at least one other group.

The "Is" operator selects only drives and media that belong exclusively to the specified logical groups. If the drives and media belong to any other groups as well, they are not selected by the filter.



### Example of using the "Contains" Operator when Filtering by Logical Group

Using the filter operator "Contains" instead of "Is" selects all media records in the logical group (this case 37). The "Contains" operator selects drives and media that belong to the specified logical groups, as well as any number of other groups.



## How Changes to Logical Group Definitions Affect Filters

If a filter uses a logical group, modifications to the definition of the logical group affect the behavior of the filter.

For example, if you make the policies of a dynamic group more restricted, such as selecting only T10K cleaning media vs all T10K media. The number of results produced by the logical group filter will be reduced. If you change the name of the logical group, the filter will select no results because the old logical group name is still used in the filter. You must update the filter to use the new name.

## Where Can I Use Logical Group Filtering?

You can only use logical group filtering for some screens, policies, and dashboard panes.

Filter by logical group on the following screens:

- Drives Overview and Drive Analysis
- Media Overview and Media Analysis

Use logical groups in the selection criteria for the following types of policies:

- Alert policies
- Media validation policies

Filter the following dashboard panes by logical group.

### Graph Panes

- Drive Health
- Drive Utilization
- I/O Throughput
- Library Drive Bays
- Library Media Slots
- Maximum Mount Times
- Media Health
- Mounts

### Table Panes

- Drives Requiring the Most Cleanings Per Meter
- Drives Watch List
- Media Watch List
- Monitored Device Trends

### Report Panes

- Data Read Report
- Data Written Report
- Drives Health Report
- Media Health Report
- Monitored Device Counts

# 12

## Media Validation

Media validation is an optional STA feature that uses policies to automate validation tests on media within the library system.

Media validation helps ensure long-term preservation of the data in your tape library system. It provides automated, policy-driven validation of media in the tape libraries, using the data integrity checking capabilities of the tape drives. STA analyzes the validation results and makes recommendations for preserving your data.

### Note:

For the SL150, SL3000, and SL8500, media validation requires SNMP v3 and is supported only for tape library system configurations that meet minimum requirements. See the *STA Installation and Configuration Guide* Requirements for STA section for a list of STA, library, drive, and media requirements.

### About

- [Features and Benefits of Media Validation](#)
- [User Roles for Media Validation Activities](#)
- [Types of Media Validation Tests](#)
- [How STA Tracks and Reports Media Validation](#)
- [Why Aren't SL150 Media Validation Drives Showing in STA?](#)

### Configure Media Validation

- [Configure the Media Validation Drive Pool](#)
- [Configure Drive Calibration and Qualification](#)
- [Enable or Disable STA-driven Media Validation](#)

### Define Media Validation Policies

- [Create, Copy, or Modify a Media Validation Policy](#)
- [Enable or Disable a Media Validation Policy](#)
- [Identify Media Eligible for Validation](#)

### Manage Media Validation

- [Submit Manual Media Validation Requests](#)
- [Resubmit a Completed Media Validation](#)
- [Resume Validations on T10000 T2 Media](#)
- [Manage the Media Validation Requests Queue](#)

## Features and Benefits of Media Validation

STA allows you to automate and manage media validation across all libraries in your system. STA-driven media validation has distinct advantages over validation done through the library interface.

### Supported Media Types

The library models support media validation for the following media types:

- SL150 - LTO media validation only
- SL3000 - T10000 media validation only
- SL8500 - LTO and T10000 media validation

### Increased Security with Reduced Cost and Complexity

Media validation is done internally by the drives themselves, providing several advantages over validation methods offered by other vendors. Data in your tape library system is kept secure because there is no need to send it across a network to a separate application. Costs are reduced because there is no need for a dedicated host server or additional host software to read information from the media and drives, and there is no need for additional Fibre Channel data connections to the drives.

### No Disruption to Library Production Operations

Validation drives are not available for use by host applications, but if a host requires media that is being validated, the host request takes priority. The library interrupts the validation, dismounts the media from the drive, and makes the media available to the application. This is done transparently to the application.

### Assurance of Valid Test Results

To confirm the validity of all media validation tests, STA provides optional drive calibration and qualification features. Calibration ensures that validation drives are in good working order, and qualification ensures that the validation drives remain calibrated and failed validations are the result of problems with the media, not the drive. These features operate without user intervention once they are configured and enabled.

### Automated Validation Operations

With STA, you can define policies for automatically selecting media for validation. For example, you could define policies to initiate validations whenever media health falls to Action or whenever a drive detects a bad media information record (MIR). STA automatically queues the media for validation on a compatible drive. STA can initiate and process multiple validations simultaneously, depending on the number of drives you have set aside for validation activities.

### User Management of Validation Requests

You can use STA to manage the validation request queue. You can reprioritize pending validation requests, cancel in-progress requests, and initiate validations manually.



### Limit to Validation Frequency

To prevent the overuse of data media, STA does not allow a piece of media to be validated more than once in a 24-hour period. This applies to both manual and automated validation requests.

### Comprehensive Reporting of Validation Results

STA displays the results of all validation activities performed in your tape library system. This includes validations initiated by other applications, such as Oracle's StorageTek SLC and Oracle's StorageTek Storage Archive Manager (SAM). STA analyzes validation results and makes recommendations for action you should take.

When a media validation is in process, the drive is reserved to the initiating application and not available to any others. Oracle recommends performing media validations through one application at a time to avoid potential drive reservation conflicts.

## Media Validation Feature Comparison for STA and the Library Interface

STA provide significantly more media validation features than the library interface.

An X indicates the feature is supported by that product.

Feature	STA	Library Interface
Configure the validation drive pool.	-	X
Support all verification test types.	X	X
Automatically mitigate false-positive validation results.	X	-
Calibrate validation drives.	X	-
Automatically perform ongoing qualification of validation drives.	X	-
Perform one validation at a time.	X	X
Perform multiple validations at a time.	X	-
Perform validations in multiple libraries or complexes at once.	X	-
Perform automated, policy-driven validations.	X	-
Submit multiple validation requests to a user-managed request queue.	X	-
Reprioritize pending validation requests.	X	-
Display progress indicators for in-progress validations.	X	X
Display validation results one at a time.	X	X
Display multiple validation results at one time.	X	-
Display validation results in table and graph form.	X	-
Display validation history over a selected date range.	X	-
Display detailed validation failure and disposition information.	X	-
Report indications of marginal tape quality (on selected drive firmware versions only).	X	-
Receive alerts about validation results.	X	-

Feature	STA	Library Interface
Display dashboard summaries of validation activity.	X	-
Receive emailed executive reports summaries of validation activity.	X	-


## Configure the Media Validation Drive Pool

Use the library's interface to define a reserved pool of drives. Use STA to identify and verify your tape library system contains media validation drives.

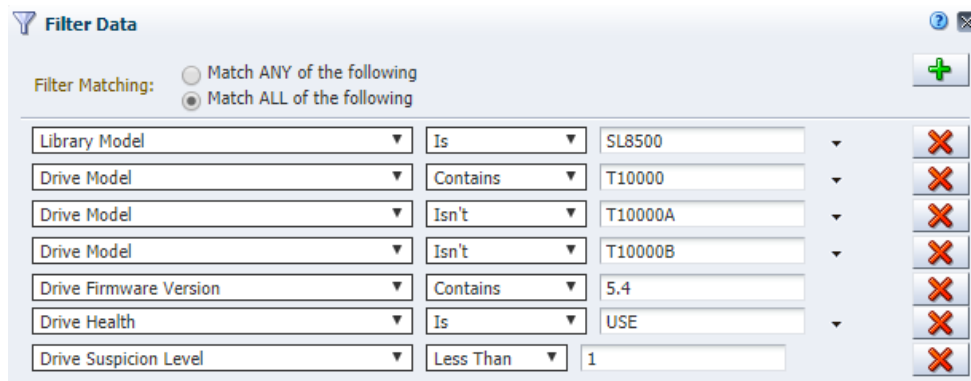
- [Identify Drives for the Media Validation Pool](#)
- [Add Drives to the Media Validation Pool](#)
- [Verify there are Valid Validation Drives](#)

## Identify Drives for the Media Validation Pool

Use STA filtering to identify high-quality, compatible drives for media validation.








1. Review [Which Drives are Best for Media Validation?](#)
2. In the left navigation, expand **Tape System Hardware**, then select **Drives Overview**.
3. In the table toolbar, click **Filter Data** .
4. Add criteria based on the requirements and recommendations for valid drives.

Below is a sample filter you might use to identify T10000 drives within an SL85000.



**Filter Data**

Filter Matching:  Match ANY of the following  Match ALL of the following

Library Model	Is	SL8500	
Drive Model	Contains	T10000	
Drive Model	Isn't	T10000A	
Drive Model	Isn't	T10000B	
Drive Firmware Version	Contains	5.4	
Drive Health	Is	USE	
Drive Suspicion Level	Less Than	1	

5. Add potential drives to the Drives - Overview graphs to get a visual representation of the drive characteristics and confirm your selections.

See [Add Library Resources to Graphs](#).

### Which Drives are Best for Media Validation?

The drives must meet the following minimum requirements:

- T10000C or D drives with firmware version ending in 5.40 or higher (this indicates the firmware supports TTI 5.4+).

- T10000D drives must have *Level 3 Media Validation* and *Level 3 RQI Margin Report* enabled within VOP to provide Quality Index values. See [ISSUE: T10000D Drives Are Not Showing Quality Index After Media Validation](#).
- IBM LTO 6+ drives (for SL150), IBM LTO 6+ drives in ADI mode (for SL8500)
- Drive Health Indicator is Use.
- Drive Suspicion Level is 0.

Select high-quality drives, with recent activity and few or no errors. Drives with the following characteristics may be good candidates for the validation pools:

- Activity in the last 30 days. See the Drive Dismounts (30 Days) attribute.
- No drive errors. See the Drive Errors (30 Days) attribute.
- No excessive drive cleans. See the Cleans (30 Days) attribute.
- No excessive alerts or SNMP traps. If there are alerts and traps, you may want to investigate to determine whether they indicate a potential problem with the drive. See the Drive SNMP Trap Count (30 Days) and Alert Count (30 Days) attributes.
- Relatively fast. See the Mount R/W MB/sec (30 Days) attribute.

## Add Drives to the Media Validation Pool

Add media validation drives to a reserved pool using the library's interface. These drives are not accessible by host applications.

After using STA to identify candidate drives, use the library's interface to configure the media drive pool. See the product's *Library Guide* for instructions. See <https://docs.oracle.com/en/storage/tape-storage/index.html> to access the documentation.


Host applications cannot access validation drives. Each complex or standalone library can have a validation drive pool with up to ten drives. You must assign at least one drive per complex or standalone library. If you will be validating encrypted media, you must assign at least one drive that has been enabled for encryption and connected to Oracle Key Manager (OKM). STA automatically detects any changes to the media validation pool.

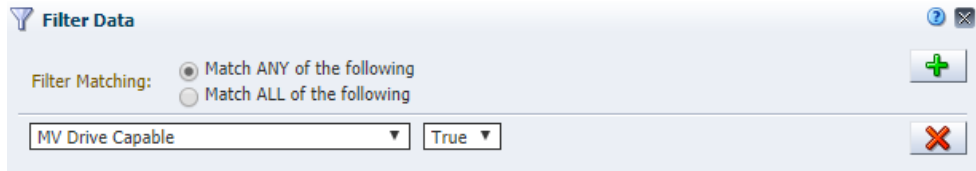
### See Also:

- [Identify Drives for the Media Validation Pool](#)

## Verify there are Valid Validation Drives

The library's interface does not check that drives meet STA requirements. Therefore, some drives in the pool may not be compatible with STA policy-driven validation. Use STA to display validation drives that meet the minimum STA requirements.

1. In the left navigation, expand **Tape System Hardware**, then select **Drives Overview**.
2. In the table toolbar, click **Filter Data** .
3. Select **MV Drive Capable** and **True**, and then click **Apply**.



- The table displays only drives that have been assigned to the validation pools and that meet minimum requirements for STA media validation.

Drive Serial Number	Drive Type	Library Complex Name	Drive Library Serial Number	MV Drive Allocated	MV Drive Capable	MV Drive Available
576004000119	T10000c	SL8500_2	516000100437	✓	✓	✓
576004007613	T10000c	SL8500_2	516000100437	✓	✓	✓
579001000352	T10000d	SL8500_2	516000100437	✓	✓	✓

- Make sure there are valid drives in each library that will be performing media validation.

## Automate Media Validation Using Policies

Media validation policies automate validation by defining how STA selects the media to test.

Based on the user-defined criteria for the policy, STA identifies media within the tape library system that should be validated. For each media selected, STA generates a validation request, which is submitted to the validation queue. As soon as a compatible drive becomes available, the validation starts. STA manages this activity automatically.





Depending on the number of media validation policies and how they are defined, validation could occur several times a day on a single piece of media. To prevent this, STA limits automated validations to one per day for each media. Once a validation request has been generated for a piece of media, STA will not generate any additional validation requests for it that day.

- [Create, Copy, or Modify a Media Validation Policy](#)
- [Media Validation Policy Wizard](#)
- [Enable or Disable a Media Validation Policy](#)
- [Identify Media Eligible for Validation](#)

## Create, Copy, or Modify a Media Validation Policy

Use the Media Validation Policy wizard to configure a policy for automating media validation.

- You must have Administrator privileges to create or modify policies. You must have Operator or Administrator privileges to view the list of policies.
- In the left navigation, expand **Setup & Administration**, then select **Media Validation**.

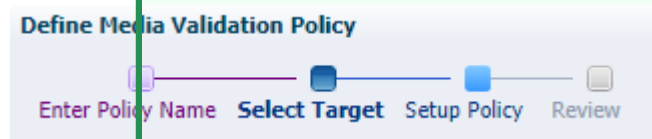
3. The defined policies are listed in the Media Validation Policies section.
4. Use the toolbar to:
  - Create a new policy: click **New Media Validation Policy** .
  - Copy a policy: select a policy in the list, and then click **Copy Policy** .
  - Modify a policy: select a policy in the list, and then click **Edit Policy** .
  - Delete a policy: select a policy in the list, and then click **Delete Policy** . You do not need to disable a media validation policy before deleting it.
5. Use the wizard to configure the policy. Proceed to [Media Validation Policy Wizard](#).

## Media Validation Policy Wizard

The Media Validation Policy wizard steps you through policy configuration. The wizard appears whenever you create, modify, or copy a media validation policy.

### Tip:

On any screen of the wizard, select the breadcrumb links to go to any screen you have already visited.



1. To access the wizard, complete the steps in [Create, Copy, or Modify a Media Validation Policy](#).
2. On the *Policy Name* screen of the wizard, enter:
  - **Policy Name** — A unique name using any alphanumeric characters up to 250 characters in length, such as "MV-Lib2-Complete-Verify". All sample alert policies beginning with "STA," so you should not start with this prefix.
  - **Policy Description** (optional) — Use this information to describe what the policy does, such as "Selects T10K media that have Action health and performs a Complete Verify".
3. On the *Select Target* screen of the wizard, select either:
  - **Select media format and optional library complex** — Select this if you want this policy to validate media using a specific recording format. Then select:
    - **Media Format** — The media recording formats you want this policy to validate. Select as many formats as you want.
    - **Library Complex** — If you select **None**, the policy will validate the specified media types across all complexes. If you select a library complex, the policy will validate only media within that complex.

- **Select logical group** — Select this if you want this policy to validate media in a specific predefined logical group.
  - `Logical Groups` — Select a logical group that includes media libraries that contain validation drives. STA does not verify this for you. If you select a logical group that includes both media and drives, the policy applies to the media only and does not affect the drives.
- 4. On the *Setup Policy* screen of the wizard, select:
  - **Policy Criteria** — Select an option from the drop-down menu:
    - `Random Selection` – Randomly selects media for validation whenever a validation drive in the standalone library or library complex is available.
    - `Media Health = Action` – Selects media that have had a specified number of successive exchanges resulting in an Exchange Media Health of Action. You can specify from one to five exchanges.
    - `Media Health = Evaluate` – Selects media that have had a specified number of successive exchanges resulting in an Exchange Media Health of Evaluate. You can specify from one to five exchanges.
    - `Media Health = Monitor` – Selects media that have had a specified number of successive exchanges resulting in an Exchange Media Health of Monitor. You can specify from one to five exchanges.
    - `Extended period of non-use` – Selects media that have not had an exchange for a specified number of days. You can specify from 365 to 1,095 days (one to three years).
    - `Newly Entered` – Selects media that have recently been entered into the library.
    - `Bad MIR Detected (T10000 only)` – Selects media with an exchange resulting in a Bad MIR Detected error. A bad media information record (MIR) indicates degraded high-speed access on the media.
    - `Days since last validation` – Selects media that have not been validated for the specified number of days. You can specify from 365 to 1,095 days.
  - **Validation Test Type** — select the type of verification test you want the drive to perform. See [Types of Media Validation Tests](#). If you select Complete Verify Plus or Verify and Rebuild MIR, but have LTO media as part of the policy, the library will not perform media validation on the LTO media. You should select a type that applies to media in the policy. If you select *Complete Verify* or *Complete Verify Plus*, you must also select one of the following options.
    - `Perform validations from beginning of tape` – Starts testing of all media from the beginning of tape (BOT), even if the media has already been partially validated.
    - `Continue validations from last known validated data point` – Resumes partially validated T10000T2 media, if the drive can determine this from the media RFID chip. Otherwise, it will start from the beginning of tape (BOT).



See [Resume Validations on T10000 T2 Media](#) for details on these options.

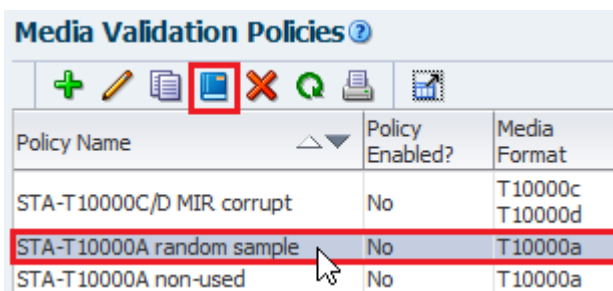
- 5. On the *Review* screen:

- Verify that all the policy information is correct.
  - Use the **Enable Alert Policy** checkbox as follows:
    - Select the check box to create the policy and enable it immediately.
    - Deselect the check box to create the policy but leave it disabled for now.
6. Click **Save**.

## Enable or Disable a Media Validation Policy

Control the generation of automated media validation requests by enabling or disabling media validation policies.

1. You must have Administrator privileges.
2. In the left navigation, expand **Setup & Administration**, select **Media Validation**.
3. Select the policy you want to modify. Click **Enable Media Validation Policy**  or **Disable Media Validation Policy** , as applicable.



Policy Name	Policy Enabled?	Media Format
STA-T10000C/D MIR corrupt	No	T10000c T10000d
STA-T10000A random sample	No	T10000a
STA-T10000A non-used	No	T10000a

4. The policy updates according to your selection.
  - If enabled, STA immediately begins evaluating media against the policy criteria and generating media validation requests.
  - If disabled, STA no longer generates media validation requests for the policy. STA completes any pending or in-progress media validation unless you cancel them. See [Cancel In-Progress or Pending Media Validation Requests](#).

## Identify Media Eligible for Validation

Media must have a minimum history to be used for policy-driven validation.



### Note:

If you have enabled drive calibration, STA will exclude any media in the calibration media logical group from all validation policies.

A minimum history means that the media must have values for the following:

- Exchange Recording Technique
- Media Suspicion Level

- [MB Written](#)

If you want STA to validate media that does not have this history, you should manually initiate a Basic Verify. See [Submit Manual Media Validation Requests](#).

#### **Not All Media May Be Validated by a Policy**

With the addition of LTO media validation starting with STA 2.4.0, it is now possible to define a policy using a test type that does not apply to all the media identified by the policy. For example, you may create a policy that uses a logical group which contains both LTO and T10000 media, and select Complete Verify Plus as the test type. In this case, the LTO media would not be tested by the policy.

## Configure Drive Calibration and Qualification

Drive calibration and qualification confirms the validity of media validation tests. When these features are enabled, STA uses calibrated and qualified drives to perform media validation activities.

Calibration and qualification are optional but recommended to improve the quality of media validation data. Calibration, which is a one-time setup process which helps to ensure validation drives are in good working order before they are used for media validation. Qualification is an ongoing, automated process performed on drives that have been calibrated. It verifies that failed validations are the result of problems with the media, not the drive.

Calibration and qualification ensure that the results of each and every media validation reflect the true quality of the tested media and are not caused by issues with the validation drives.

#### **About Calibration and Qualification**

- [Benefits of Calibration and Qualification](#)
- [How Calibration and Qualification Work](#)

#### **How to Configure Calibration and Qualification**

- [Create the Calibration Media Logical Group](#)
- [How to Choose Calibration Media](#)
- [Enable Drive Calibration and Qualification](#)
- [Disable Drive Calibration and Qualification](#)
- [Verify Drive Calibration Status](#)

## Create the Calibration Media Logical Group



Assign media for drive calibration and qualification to a dedicated calibration media logical group. Media in this group should not be used for host operations or in regular media validation operations.

There is only one calibration media logical group for your entire tape library system. You must assign at least two media for each drive in the validation drive pool. There is no maximum number of media you can assign to the group. Only assign media to the group, not drives.



 **Note:**

For best results, you should not use production media for calibration. The media that you select should be dedicated solely for calibration to assure that the media is of the highest quality.

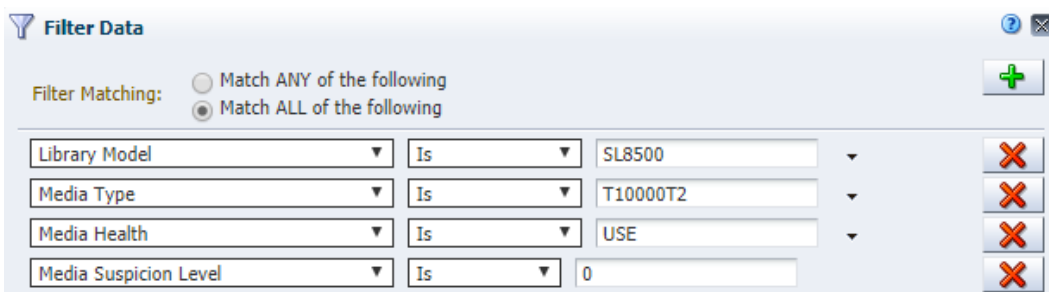
1. You must have Operator or Administrator privileges.
2. In the left navigation, expand **Setup & Administration**, select **Logical Groups**.
3. Click **Add Logical Group** .
4. Complete the Create Logical Group screen:
  - Logical Group Name — a unique name using a maximum of 249 alphanumeric characters. Name the group so that you can easily identify it (such as "Calibration Media").
  - Logical Group Type — Select **Manual**
5. Click **Save**. Initially the group is empty, use the following steps to add media to it.
6. In the left navigation, expand **Tape System Hardware**, select **Media Overview**.
7. In the table toolbar, click **Filter Data** .
8. Enter selection criteria that will provide appropriate media for calibrations. Then click **Apply**.

See [How to Choose Calibration Media](#) .

 **Note:**





STA does not check the media you add to the calibration logical group, so it is possible to assign media that cannot be used for calibration and qualification.

The following is an example of selection criteria for calibration media.



**Filter Data**


Filter Matching:  Match ANY of the following  Match ALL of the following

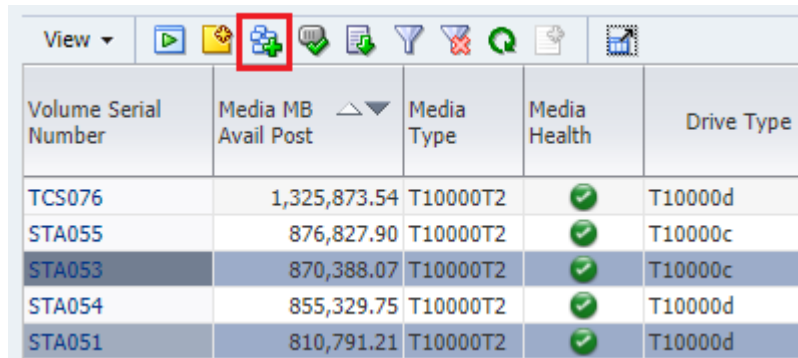
Library Model	Is	SL8500	
Media Type	Is	T10000T2	
Media Health	Is	USE	
Media Suspicion Level	Is	0	






9. Sort the results by the **Media MB Avail Post** column to locate media with at least two wraps of written data (see the table below for minimum values).

Media Type	MB Written for Two Wraps
T10000D Standard	119,000 MB
T10000D Sport	23,800 MB

Media Type	MB Written for Two Wraps
T10000TC Standard	97,000 MB
T10000TC Sport	19,400 MB
LTO-9	128,000 MB
LTO-8	114,000 MB
LTO-7 or M8	106,000 MB
LTO-6	36,000 MB
LTO-5	18,000 MB

10. From the list, select the media to use for calibration and qualification. Then from the table toolbar, click **Logical Groups** .



Volume Serial Number	Media MB Avail Post	Media Type	Media Health	Drive Type
TCS076	1,325,873.54	T10000T2		T10000d
STA055	876,827.90	T10000T2		T10000c
STA053	870,388.07	T10000T2		T10000c
STA054	855,329.75	T10000T2		T10000d
STA051	810,791.21	T10000T2		T10000d

11. From the drop-down menu, select the logical group you created for the calibration media, and click **OK**.

 **Note:**

If any media assigned to the calibration logical group do not have the minimum required history, STA automatically initiates a Basic Verify before attempting to use them for drive calibration.

## How to Choose Calibration Media

You should dedicate calibration media exclusively for drive calibration and qualification, and not use them for production data. This helps to ensure that the quality of the media is not compromised by production operations.

The following may be good candidates for calibration media:

- Media that has been in use but has data you no longer need. For example, expired backup media in good condition.
- New or unused media in good condition to which you have written dummy data. The data may be encrypted or not, depending on your needs.

The calibration media must meet the following criteria:

- For T10000, Media Type is T10000T2 or T10000T2 Sport
- For LTO, Media Type is the same generation or previous generation as the LTO drive within the pool. For LTO8 drives, the media can be LTO8, M8, or LTO7.

- Media Health Indicator is USE.
- Media Suspicion Level is 0.
- At least two wraps of data have been written to the media.

## Enable Drive Calibration and Qualification

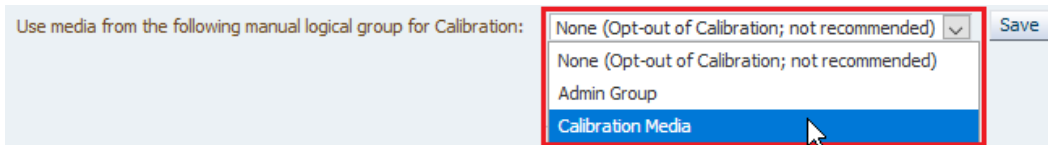
Oracle highly recommends enabling drive calibration and qualification if you are using STA media validation, as it helps ensure both the validity of validation results and the health of the drives.

### Prerequisites:

- The calibration media logical group must already exist and has media assigned to it. See [Create the Calibration Media Logical Group](#).

### Procedures:

1. You must have Administrator privileges.
2. In the left navigation, expand **Setup & Administration**, select **Media Validation**.
3. In the **Use Media From the Following Manual Logical Group for Calibration** drop-down menu, select the logical group you created for calibration.



4. Verify your selection, and click **Save**.
5. STA begins calibrating drives in the media validation drive pool. If calibration is successful, the screen displays the message, "Drive and Media Pool Setup Success--calibration has been successful."

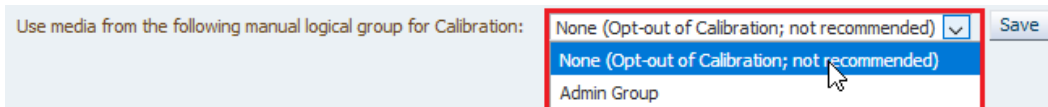
### See Also:

- [How Calibration and Qualification Work](#)
- [Benefits of Calibration and Qualification](#)

## Disable Drive Calibration and Qualification

It is highly recommended that you enable drive calibration and qualification if you are using STA media validation. However, you can disable the feature at anytime.

1. You must have Administrator privileges.
2. In the left navigation, expand **Setup & Administration**, select **Media Validation**.
3. In the "Use Media From the Following Manual Logical Group for Calibration" drop-down menu, select **None (Opt out of calibration; not recommended)**.



4. Verify your selection, and click **Save**.
5. Review and click **Yes** to confirm that want to disable calibration and qualification.
6. STA finishes any in-progress calibration or qualification activities, but does not begin any new calibration or qualification operations.


**See Also:**

- [How Calibration and Qualification Work](#)
- [Benefits of Calibration and Qualification](#)

## Verify Drive Calibration Status

STA may be unable to calibrate all drives within the media validation pool due to a lack of calibration media or drive issues. Verify the status of the validation drives and address any issues by adding media or removing the drive from the pool.

1. In the left navigation, expand **Tape System Hardware** and select **Drives Overview**.
2. From the **Templates** drop-down, select **STA-Drive-MV**.
3. Within the table, review the **MV Calibration State** for each drive.



Drive Serial Number	Drive Type	Drive Health	T10000 MV Calibration Quality Index	LTO MV Calibration RQ	MV Recommendation	MV Drive In Use	MV Drive Allocated	MV Drive Capable	MV Drive Reserved	MV Drive Available	MV Calibration State	MV Calibration Information
57901000421	T10000d	🔴	31.24		Corrupted MIR: Verify and Rebuild MIR.		✓	✓		✓	Not Suitable	Drive is not configured for Media Validation.
57601000495	T10000c	🟢	87.48			✓	✓	✓	✓	✓	Calibrated	Drive is Calibrated.
57604001123	T10000c	🟢	87.49		Media OK: Continue using tape.	✓	✓	✓	✓	✓	Calibrated	Drive is Calibrated.
57604005754	T10000c	🟢	100.00		Media OK: Continue using tape.	✓	✓	✓	✓	✓	Calibrated	Drive is Calibrated.
57904004338	T10000d	🟢	99.88		Media OK: Continue using tape.	✓	✓	✓	✓	✓	Calibrated	Drive is Calibrated.
1013001279	IbmUltrium7	🟢		90.00	Media OK: Continue using tape.		✓	✓		✓	Offline	Taking Drive Offline.
10WT005571	IbmUltrium7	🟢			Blank Media: Continue using tape.		✓	✓		✓	Drive Calibration Needs Media	No More Free Media Available in Media Pool.
10WT000103	IbmUltrium8	🟢		90.00	Media OK: Continue using tape.		✓	✓		✓	Calibrated	Drive is Calibrated.
10WT000106	IbmUltrium8	🟢		90.00	Media OK: Continue using tape.		✓	✓		✓	Calibrated	Drive is Calibrated.

4. If the drive is "Not Suitable" you should remove the drive from the media validation pool.
5. If no calibration media is available, you should add compatible media to the calibration media logical group.

**See also:**

- [Create the Calibration Media Logical Group](#)
- [How Calibration and Qualification Work](#)

## Benefits of Calibration and Qualification

Oracle highly recommends that you enable calibration and qualification if using media validation, as it can ensure the results, verify drive health, and increase efficiency.

### Validity of Validation Results

When an exchange failure occurs, there can be uncertainty whether the problem is with the drive, the media, or both. The STA drive calibration and qualification features directly address these uncertainties, providing you with assurance the failed validation is a result of the media, not the drive.

### Ensure Health of Validation Drives

Because validation drives have a higher-than-normal number of exchanges with problem media, they may become degraded at a faster rate than production drives. Through drive qualification, STA continuously verifies the health of validation drives. STA identifies drive problems early so you can service or replace the validation drives before they begin to cause problems with production media.

### Automatic Verification of the Validation Drive

When a media validation fails, and if drive calibration and qualification is disabled, you must manually verify why the media validation failed. If drive calibration and qualification is enabled, STA verifies all failed validations through the process of drive qualification. Qualification is done automatically with no user intervention. Because STA uses pre-qualified media, it is only necessary to do a Standard Verify for the qualification, which takes significantly less time than a Complete Verify.

## How Calibration and Qualification Work

Calibration is a one-time setup process. Qualification is an ongoing process that runs in the background. Together they ensure that the results of media validation test are accurate.

### Calibration Process

Drive calibration is a one-time setup that begins as soon as you enable drive calibration. During calibration STA tests all drives in the validation pool using a Standard Verify. If you add a new drive to the media validation pool, STA automatically begins calibrating the drive. STA also automatically re-calibrates drives after a firmware update. However, STA may not be able to calibrate all drives in the pool due to a lack of calibration media or other drive factors. You should check the calibration status of the drives and address any drives that STA is unable to calibrate.

Calibration uses the following basic process for each validation drive:

1. STA performs two Standard Verify validations on the drive, each time using a different media from the calibration media logical group.
2. STA analyzes the Quality Index values for T10K drive and Read Quality (RQ) values for LTO drives. For a drive to be qualified, the following criteria must be met:
  - One media must have quality  $\geq 75$ . This is assigned to the drive as the *primary* calibration media.
  - One media must have quality  $\geq 50$ . This is assigned to the drive as the *secondary* calibration media.
3. Depending on the quality results, STA proceeds as follows:
  - If both criteria are met after two validations, the drive is calibrated. A third validation is not necessary for this drive.
  - If only one of these criteria is met after two validations, a third validation is performed using a different media from the calibration media logical group.
  - If both these criteria are not met after three validations, the drive is considered *not suitable*.

### Calibration Results

If a drive passes calibration, STA dedicates a primary and secondary calibration media to the drive, which STA uses for all qualification on the drive.

If a drive fails calibration, STA disqualifies the drive and assigns it the Calibration State of "Not Suitable". STA will not use disqualified drives for validation as long as drive calibration remains enabled. The disqualified drives will remain in the media validation drive pool until you explicitly remove them through the library interface. If drive calibration is disabled, STA ignores the "Not Suitable" Calibration State and uses the drives for validation. This may happen if calibration was enabled on STA at one point and has since been disabled.

After STA calibrates all drives, the Media Validation Configuration screen displays, "Drive and Media Pool Setup Success--calibration has been successful." Detailed results about individual drives are displayed on the Drives – Overview screen, and you can review the results and take appropriate action.

### Qualification Process and Results

Qualification is an ongoing process that runs automatically in the background whenever a media validation results in a Degraded or Failed status. During qualification, the validation drive is tested using a Standard Verify. The test are performed using the primary and secondary calibration media assigned to the drive.

Upon completion of qualification, STA makes one of the following recommendations about the quality of the drive and the media:

- The drive is disqualified.
- The data media is bad.
- The data media is bad, and the secondary calibration media is disqualified.

Qualification results are displayed on the Media Validation Overview screen in the MV Calibration and Qualification attributes. You can review the results and take appropriate action. Disqualified media are not used for drive calibration or qualification. They remain in the calibration media logical group until you explicitly remove them.

### Drive Calibration and Qualification Terms

These terms are useful in understanding the concepts of drive calibration and qualification and are used throughout this section.

#### Validation exchange

A media and drive exchange in which the drive performs a specified validation test on the media and its data.

#### Failed validation

A media validation exchange that ends with a "Degraded" or "Failed" status.

#### False positive result

A failed validation that is the result of problems with the validation drive, not the media. STA uses drive calibration and qualification processes to reduce the possibility of false positive results and ensure that failed validations are the result of problems with the media.

**Drive calibration**

Optional STA media validation feature whose purpose is to ensure that validation drives are performing optimally. If drive calibration is enabled, validation drives must be calibrated before STA can use them for media validation.

**Calibrated drive**

Validation drive that has successfully passed the STA drive calibration process. A drive that fails calibration is considered disqualified and is not used by STA. If the STA drive calibration feature is disabled, all validation drives are considered uncalibrated, but they are used by STA.

**Uncalibrated drive**

A drive that has not yet been calibrated; or a validation drive in a system in which the STA calibration feature has not been enabled.

**Drive qualification**

Optional STA media validation feature that ensures validation drives remain calibrated and helps to ensure failed validations are the result of problems with the media, not the drive. STA automatically initiates a drive qualification process whenever there is a failed validation. Drive qualification is enabled as part of drive calibration. Drive calibration is essentially a one-time process, whereas drive qualification is ongoing.

**Qualified drive**

Calibrated drive that has successfully passed the STA drive qualification process.

**Disqualified drive**

A drive that has failed STA calibration or qualification.

**Calibration media**

Media that has been set aside specifically for drive calibration and qualification. You assign calibration media to a manual logical group through STA. It is highly recommended that you dedicate calibration media exclusively to drive calibration and not use them for production data. Calibration media should be of high quality.

**LTO Read Quality (RQ)**

Measure of the amount of error correction left on the media. This value is calculated by STA based on information provided by the drive. Read quality applies to the exchange as a whole and includes contributions from both the media and the drive involved in the exchange. This term is specific to media validation and differs from Read Margin. Read quality is reported as a percentage. A high value is desirable.

**T10K Quality Index**

Measure of the amount of error correction left on the media. This value is provided by the drive. During drive calibration and qualification, STA uses the quality index to determine whether the drive is qualified or disqualified. Quality is reported as a percentage. A high value is desirable.

## Enable or Disable STA-driven Media Validation

Media validation is disabled by default, you must enable it within the STA interface.

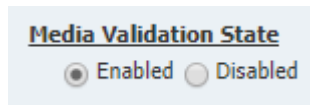
Once enabled, STA media validation is available for all eligible libraries in your tape library system. If you disable media validation after it has already been enabled, STA does not accept new validation requests. However, any pending or in-progress requests remain in the validation queue and are processed to completion. If you want to cancel these requests, see [Cancel In-Progress or Pending Media Validation Requests](#).

**Prerequisites:**

- Before enabling, verify that you have properly configured media validation and defined media validation policies.

**Procedures:**

1. You must have Administrator privileges.
2. In the left navigation, expand **Setup & Administration**, then select **Media Validation**.
3. Select either **Enable** or **Disable**.



4. Verify your selection, and click **Yes** to confirm.
5. The Status area updates (see below for common messages).

**Possible Status Messages WITHOUT Drive Calibration and Qualification**

- Media Validation is DISABLED.
- Media Validation successfully enabled.
- Media Validation Enabled; Opted-out of Drive Calibration.

**Possible Status Messages WITH Drive Calibration and Qualification**

If you enabled the drive calibration and qualification feature, it may take time to. You may see the following messages while this process is underway.

- Media Calibration Process in Progress.
- Media Operation to Create History in Progress.
- Drive Qualification Type Pool Pre-Calibration SUCCESS.
- Calibration Success. Drive Qualification is Now Active.

**Possible Error Status Message**

- No Available Drives, Not Suitable for Media Validation Use.
- No Available Media, Not Suitable for Calibration Use.
- Warning: Insufficient Media in MV Media Pool for Number Of Drives in MV Partition.

## Submit Manual Media Validation Requests

Manually submit media validation requests to the validation queue. You can start new validations or to resume validations that were previously interrupted.

1. In the left navigation, expand **Tape System Hardware**, select **Media Overview**.
2. Apply appropriate filter criteria to narrow down the list of media.  
For example, **Media Type | Contains | T10000**.



- Highlight the media to validate (shift-click or ctrl-click to select multiples). You cannot select media that belongs to the calibration media logical group.

Click **Media Validation** .

**Media - Overview**

Format: [Icons]

View [Icons]

Volume Serial Number	Media Manufacturer Serial Number	Media Type	Cleaning Media	Media Physical Address	Media Library Name
702866	708026010304	T10000T1		1,1,9,1,46	crimson11
702896	708019020274	T10000T1		1,1,-6,2,12	crimson11
M04622		9840R		1,1,-8,1,3	crimson11
UD0032	710232040132	T10000T1		1,1,-12,1,44	crimson11
UG0004	710239050084	T10000T1		1,1,-9,2,37	crimson11
CLNU22		LTO1		1,1,-11,2,17	crimson11

- Review the Validation screen.

**+ Validation Activities** ✕

WARNING: Only 3 media out of 4 media are eligible to be added for media validation. i

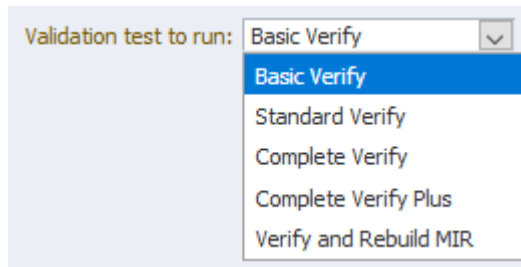
Volume Serial Number	Media Type	Library Complex Name
LAB005	T10000T2	SL8500_1
TEE999	T10000T2	SL8500_1
LAB011	T10000T2	SL8500_1

Validation test to run:

Drive:

Media may be ineligible if:

- The media are cleaning media.
  - The media are in library or complex that does not contain a media validation pool.
  - Drives in the media validation pool are not compatible with the media.
  - Drives in the validation drive pool do not meet minimum requirements for STA media validation.
- In the **Validation test to run** drop-down menu, select the test type (see [Types of Media Validation Tests](#)).

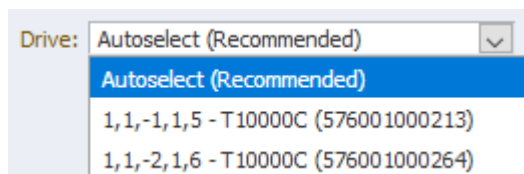


If you select *Complete Verify* or *Complete Verify Plus*, you may also be required to select one of the following options:

- **Perform validations from beginning of tape** – Indicates you want T10000T2 media to be validated from the beginning of tape (BOT).
- **Continue validations from last known validated data point** – Indicates you want testing of T10000T2 media that has been partially validated to resume where the previous validation left off, if the drive can determine this from the media RFID chip. If the drive cannot determine where the previous validation left off, it will start from the beginning of tape.

See [Resume Validations on T10000 T2 Media](#).

6. In the **Drive** drop-down menu, select the drive to use for the validations. This option is available only if the media you have selected all reside within the same library complex or standalone library.




**IMPORTANT:** It is recommended that you choose **Autoselect**, which causes STA to automatically select a compatible validation drive for each media. If the drive you manually select is not compatible with some of the media—for example, some of the media is encrypted but the drive is not encryption capable—the validation requests will be added to the request queue, but they will remain in a pending state.

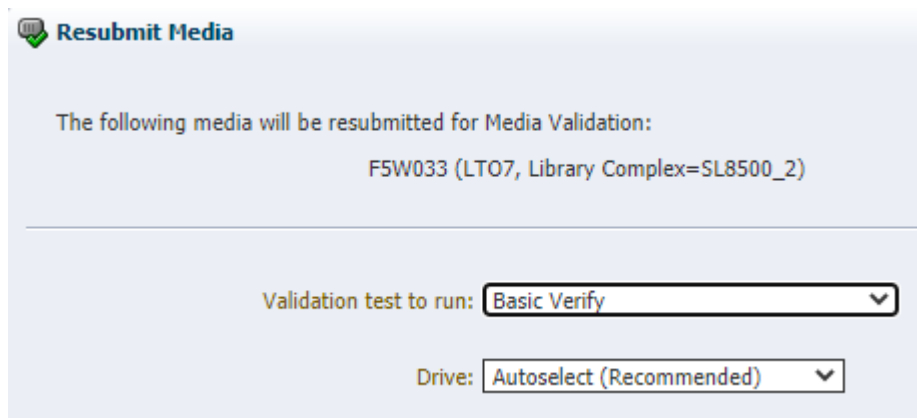
7. Click **Create**.
8. View the requests on the Media Validation Overview screen (see [Display the Media Validation Request Queue](#)).

## Resubmit a Completed Media Validation

Resubmit completed media validations to retest the media. This can be useful when you want to verify a suspected piece of media.

1. In the left navigation, expand **Tape System Activity**, select **Media Validation Overview**.
2. Within the table, highlight the row for the media validation you want to resubmit. You can only resubmit completed validations.

3. Click **Resubmit Media Validation** .
4. Select the [media validation test type](#) and drive from the drop-down lists.



**Resubmit Media**

The following media will be resubmitted for Media Validation:  
F5W033 (LT07, Library Complex=SL8500\_2)

Validation test to run:

Drive:

5. Click **OK**.

## Resume Validations on T10000 T2 Media

For T10000 T2 media, you can resume Complete Verify and Complete Verify Plus validations that have been interrupted or canceled.

You can either restart at the beginning of tape (BOT) or resume where the validation left off. You cannot resume validations for LTO or T1 media.

1. Manually start a validation, selecting the T10000 T2 media that you want to resume and selecting the Complete Verify or Complete Verify Plus validation type.  
See [Submit Manual Media Validation Requests](#) for details on how to start the validation.
2. After selecting the validation type, select one of the following options:
  - **Perform validations from beginning of tape** – Starts the validation at the beginning of tape (BOT). Depending on the read/write operations that have occurred on the media since the most recent validation was interrupted, the validation may no longer be valid, and you may want to select this option.
  - **Continue validations from last known validated data point** – Resumes the validation where the previous one left off, if the drive can determine this from the media RFID chip. If the drive cannot determine where the previous validation left off, it will start from the beginning of tape.

### When Can I Resume a Validation?

You can only resume interrupted validations if certain conditions are true.

*All* of the following conditions must be true to resume a validation:

- You have selected T10000T2 media for validation (T10000T1 and LTO media validations always start at the beginning of tape).
- The validation test type is Complete Verify or Complete Verify Plus (other test types always start at the beginning of tape).

- The most recent validation for the media was not completed (previously completed validations always re-validated from the beginning of tape).

## Manage the Media Validation Requests Queue

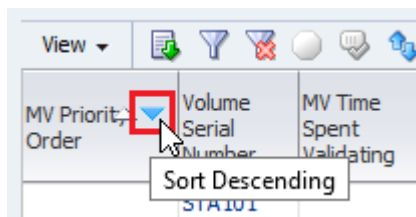
STA places pending media validation requests within a queue. Manage the queue to re-prioritize or cancel requests.

- [Display the Media Validation Request Queue](#)
- [Reorder Pending Media Validation Requests](#)
- [Cancel In-Progress or Pending Media Validation Requests](#)

## Display the Media Validation Request Queue

Display information about pending, in-progress, and completed media validation requests.


1. From the left navigation, expand **Tape System Activity**, select **Media Validation Overview**.
2. The table displays all validation requests. By default, the requests are sorted in Priority Order, starting with "1," which means the oldest requests are at the top of the screen. To view the most recent requests, select **Sort Descending** ▼ on the column.



3. From this screen, you can manage the validation request queue by performing any of the following tasks:
  - [Reorder Pending Media Validation Requests](#)
  - [Cancel In-Progress or Pending Media Validation Requests](#)

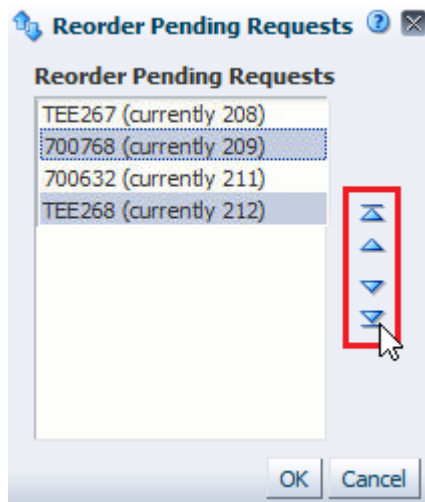
## Reorder Pending Media Validation Requests

Re-prioritize pending requests to change the order in which the libraries will handle the media validation.

1. In the left navigation, expand **Tape System Activity**, select **Media Validation Overview**.
2. In the table toolbar, click **Reorder Pending Requests** .




3. Select the requests you want to reprioritize, and click the up or down arrows to move them in the list. Click **OK**.



## Cancel In-Progress or Pending Media Validation Requests

Cancel requests to remove them from the validation request queue. Cancel in-progress requests to stop the media validation.

You can cancel any pending validation, but you can only cancel in-progress Complete Verify or Complete Verify Plus media validations. You cannot cancel other in-progress validation types.

1. In the left navigation, expand **Tape System Activity**, select **Media Validation Overview**.
2. Select the requests to cancel, and click **Cancel** .

The **Cancel** button does not activate if you select completed validations. As shown below.

MV Priority Order	Volume Serial Number	MV Time Spent Validating	MV Estimated Time Remaining	Exchange Start	MV Test Type	MV Request State
	STA101				Complete Verify Plu	Completed
	DCB019	0:18:58.5		2018-07-17 13:07:31	Standard Verify	Completed
	BCB011	0:40:30.7		2018-07-17 13:08:54	Complete Verify	Completed

3. Verify the list of volume serial numbers, and click **Yes** to confirm.
4. Pending requests are canceled and removed from request queue.

In-progress requests may take several minutes for the drive to receive the request and unload and dismount the media. Once the media has been returned to a media slot, the validation request is removed from the validation request queue. You can later resume or repeat the validation. See [Resume Validations on T10000 T2 Media](#) for details.

## User Roles for Media Validation Activities

A user's access to media validation functionality depends on their role.

User Role and Screen	Media Validation Action
Viewer and above Screen: Tape System Hardware > Drives Overview	Display drives in the media validation drive pools.
Viewer and above Screen: Tape System Activity > Media Validation Overview	Display, filter, and print a list of all media validation requests. Export the media validation requests list to a spreadsheet or document. View detail for a selected media validation request. Manually submit media validation requests one at a time. Reorder or cancel pending media validation requests. Resume an interrupted validation of a T10000T2 media.
Operator and above Screen: Tape System Hardware > Media Overview	Manually submit multiple media validation requests. Resume multiple interrupted validations of T10000T2 media.
Operator and above Screen: Setup & Admin > Media Validation	Display and print the list of media validation policies.
Administrator only Screen: Setup & Admin > Media Validation	Display drives in the media validation drive pools. Enable or disable media validation and validation policies. Enable or disable drive calibration by selecting the designated logical group of media. Define, copy, edit, or delete a media validation policy.

## Types of Media Validation Tests

The media validation test type determines the level of verification performed on the tape. The test type affects both the duration of the test and the information returned by the test.

You select the type of test to perform when you define a media validation policy or initiate a manual media validation.

Type	Description	Duration	Media Type
Basic Verify	Verifies the tape can be mounted and validates the media information record (MIR). Detects if the MIR is unreadable or out of sync and updates the following data attributes for the media: <ul style="list-style-type: none"> <li>Exchange Recording Technique</li> <li>Media Suspicion Level</li> <li>MB Written</li> </ul>	~ 2 minutes - 2 hours LTO tapes may require <b>2 hours</b> to complete if tape is un-initialized and must be calibrated. (T10K tapes not affected.)	LTO, T10000

Type	Description	Duration	Media Type
Standard Verify	Verifies that the highest-priority areas of the media are readable: the beginning of tape (BOT), end of data (EOD), and the outer-most wraps of data written on the top and bottom edges of the tape. This test is not valid for blank tapes.	< 30 minutes - 2 hours LTO tapes may require <b>2 hours</b> to complete if tape is un-initialized and must be calibrated. (T10K tapes not affected.)	LTO, T10000
Complete Verify or Resume Complete Verify	Verifies readability of all data records. The drive does a record-by-record verification with no decompression nor decryption. The drive validates data at maximum tape velocity, regardless of the compression ratio used on the media. By default, the validation starts at the beginning of tape (BOT). For T10000T2 media, you can choose to resume validation from the last verified location. This test is not valid for blank tapes.	5 - 24+ hours Depends on the starting point, the amount of data on the media, and the drive type. LTO tapes require 24 hours or more to complete verification. T10000 tapes may require 13 hours or more to complete verification. Resume Complete verify is available only for T10K tapes, not LTO tapes.	LTO, T10000
Complete Verify Plus or Resume Complete Verify Plus	Verifies readability of all data records, including StorageTek Data Integrity Validation (DIV) checking. If the data records are compressed and encrypted, the test requires the validation drive to be encryption capable and connected to an Oracle Key Manager (OKM). This test is not valid for FICON drives. By default, the validation starts at the beginning of tape (BOT). For T10000T2 media, you can choose to resume validation from the last verified location. This test is not valid for blank tapes.	5 - 9 hours Depends on the starting point, the amount of data on the media, and the drive type.	T10000
Verify and Rebuild MIR	Verifies the MIR and rebuilds it if necessary. If there are errors, the drive finds the last known-good spot on the MIR, then does a record-by-record verification with no decompression nor decryption. If the MIR is invalid or out of sync, the drive reads all records, starting from the beginning of tape (BOT), to rebuild the MIR. Records are not decompressed nor decrypted. The drive reads the data at maximum tape velocity. You should use this method if there is a corrupt MIR on an exchange. This is significantly faster than using Virtual Operator Panel (VOP) to rebuild the MIR.	5 - 9 hours Depends on the starting point, the amount of data on the media, and the drive type.	T10000

## How STA Tracks and Reports Media Validation

STA uses a queue to track media validation requests. STA reports the current state, initiator, and results of the test.

### Media Validation Request Queue

Based on the policies enabled, STA automatically selects media to validate and places it on the media validation queue. Once compatible media validation drive becomes available, STA initiates validation for the media.

If you remove drives, media, or library connections from your tape library system, any associated pending STA validation requests remain in the request queue until you explicitly cancel them.

See [Manage the Media Validation Requests Queue](#).

### Media Validation Request States

As STA processes the validation request, it updates the media's state. Requests are typically processed through the following sequence:

- Pending – The request has been submitted and is waiting for a compatible validation drive to come available. The MV Status Information attribute may display additional details.
- Starting – The drive has been reserved for the validation operation.
- In-Progress – The validation is in progress. The MV Time Spent Validating and MV Estimated Time Remaining attributes are continually updated as the operation proceeds.
- Completed – The validation has completed.

In addition, the following Request States may occur at any time:

- Error – An error has occurred with the request. The Request Status Information attribute may display additional details.
- Stopping, or Stop Requested – The request has been stopped, either manually or by a media request from a host application.

### Media Validation Initiators

Media validation can be started by other applications. The Initiator attribute indicates the source of the media validation. Options are as follows:

- BUI - Indicates the validation was initiated by the SL150 Browser User Interface.
- Drive – Indicates the validation was initiated directly on the validation drive.
- Host – Indicates an external host application, such as Oracle's StorageTek Storage Archive Manager (SAM).
- Library – Indicates the library command-line interface (CLI). Only Oracle support representatives are authorized to initiate media validations through the CLI. However, library administrators can use the CLI to cancel pending or in-progress validations. See the applicable *Library Guide* for details.
- SLC – Indicates SL Console.
- STA – Indicates STA.

### Media Validation Results

When a validation completes, the media is returned to a media slot, and STA displays the results and recommendations for user action. Following are attributes on the Media Validation Overview screen that you may find useful for interpreting validation results, particularly for validations that result in errors.

#### MV Result

STA assigns one of the following values to each completed validation:



- Use – The media passed validation.
- Degraded – Migrate the data and scratch the media.
- Failed – Migrate the data and disposition the media according to your site's policies.
- Unknown – May occur in the following situations:
  - The validation was canceled by STA or interrupted by a host request for the media.
  - An error occurred during the validation.
  - Communication between STA and the library was interrupted during the validation.
  - The media information record (MIR) is corrupted.
  - The validation was initiated by an application other than STA and STA has not received sufficient information from the library to determine the result.

### **MV Quality Index**

The quality index is a measure of the amount of error correction left on the media, computed by STA based on the results of the validation. This value is expressed as a percentage, with a higher value indicating a better result. This attribute is blank in the following cases:

- The validation is a Basic Verify.
- The validation resulted in an media validation Perm Status of True.
- The validation resulted in an Invalid MIR error.

### **MV Recommendation**

This attribute includes recommendations from STA for user action. Following are some messages you may see.

- Media OK: continue using.
- Media Degraded--Perform Qualification.
- Corrupted MIR: Rebuild MIR and Re-run Media Validation.
- Disposition Drive.
- Permanent error encountered: Perform drive qualification.
- Not enough data to determine MV results. Rerun media validation.
- Degraded Media: Rerun Media Validation Using a Different Drive.
- Media Validation Interrupted.

### **MV Status Information**

This attribute is usually blank but may contain information about issues that occurred with the validation request. It may explain the problem or suggest corrective action to take. Following are some messages you may see:

- Drive Timeout; MDV manager cancel – Indicates STA requested the library to return the media to a media slot because the validation took longer than it should have and timed out. This is usually the result of a library operational error. If the Read Percentage attribute for the validation exchange is less than 100 percent, then the validation did not complete. If this status recurs for the media, there is probably an issue with the media; if it recurs for the drive, there is probably an issue with the drive.
- Library returned error code – Indicates an error code returned by the library while processing the validation request. The error code is also listed in the Library Error attribute.

## Why Aren't SL150 Media Validation Drives Showing in STA?

If the SL150's Drive Element Addressing mode is set incorrectly, the media validation drives will not appear in the STA application.

You must set the SL150 to Address All Drive Slots mode if using STA and media validation. If the mode is Address Only Installed Drives, the media validation drives will not show within STA.

See Set Label Format and Element Addressing Mode (SL150 only) to change the Drive Element Addressing mode.

# 13

## Email Recipients

Define email recipients to receive STA alerts and executive reports.

- [Define the SMTP Email Server](#)
- [Add, Modify, or Delete an Email Recipient](#)
- [Test the Email Server and Recipient Definitions](#)

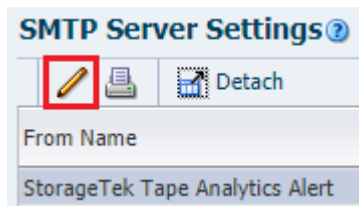
**See Also:**

- [Alerts](#)
- [Executive Reports](#)

### Define the SMTP Email Server

Define the server to use for sending recipients alert and executive report. These procedures assume an email server has already been configured at your site.

1. You must have Administrator privileges.
2. Contact your IT administrator to determine the host address and authentication requirements for the email server you want to use for sending STA emails.
3. In the left navigation, expand **Setup & Administration** and select **Email**.
4. In the SMTP Server Settings table, highlight StorageTek Tape Analytics Alerts, and then click **Edit Selected SMTP Server**.






5. Complete the dialog box as follows:
  - **SMTP Host Address**—Enter the fully qualified name of the outgoing SMTP server to be used for STA emails. This must be a valid email server. If the email server does not require authentication, you may need to specify `localhost` for the SMTP Host Address.
  - **SMTP Port**—Enter the port number for outgoing mail transport. Typically, this is port 25, but check with your IT administrator to verify this is the port used at your site.
  - **From Name**—Enter the name you want to appear in the **From** line of the emails. Oracle recommends you use text that identifies the STA server.
  - **From Email Address**—Enter the email address from which STA email is sent. This must be a valid address on the email server. Since recipients cannot reply to this

address, you may want to use an address that indicates this, such as `DoNotReply@YourCompany.com`.

- **Enabled?**—Select the check box to enable the email server.
  - **Use Secure Connection Protocol**—To use a secure connection protocol, select the check box, and then select the protocol by clicking either **TLS** or **SSL**.
  - **Requires Authentication**—This check box is available only if you have selected the **Use Secure Connection Protocol** check box. If the SMTP server requires authentication, select the check box and then complete the remaining username and password fields.
6. Click **Save**.

## Add, Modify, or Delete an Email Recipient

Update the list of email recipients available to receive STA emails. A user does not need an STA username to receive STA emails.

1. You must have Administrator privileges.
2. In the left navigation, expand **Setup & Administration**, and then select **Email**.
3. In the Email Addresses table, click **Add** . Or select a recipient and then click **Edit**  or **Delete** .

### **Caution:**

There is no confirmation dialog box for deleting. The email address is deleted as soon as you click **Delete Selected Email(s)**. If the address is used in any alert or Executive Report policies, it is also deleted from them. You can delete only one address at a time.


4. If adding or modifying, complete the dialog box, and then click **Save**.
  - **Address:** Enter a valid email address (for example, `yourname@yourcompany.com`).
  - **Language-Locale:** Select the preferred language for emails sent to this address (English is currently the only selection).
  - **Time Zone:** Select the recipient's time zone.

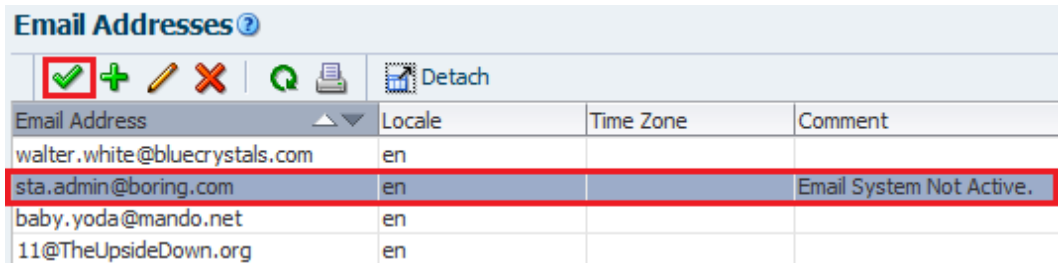
### **Note:**

The Comment field in the Email Addresses table is reserved for system-generated comments about email activity directed to each email address. This field cannot be edited by the user.


## Test the Email Server and Recipient Definitions

Verify the STA email server and recipient definitions by sending a test email to a selected recipient. You can test only one recipient at a time.

1. You must have Administrator privileges.
2. In the left navigation, expand **Setup & Administration**, then select **Email**.
3. Select an email address, then click the **Test SMTP and Email Address Setup** .



Email Address	Locale	Time Zone	Comment
walter.white@bluecrystals.com	en		
sta.admin@boring.com	en		Email System Not Active.
baby.yoda@mando.net	en		
11@TheUpsideDown.org	en		

4. The STA email server sends a test email to the selected address and updates the Comment field with details about the test. You may need to click the **Refresh Table**  button to see the comment.

5. Check the recipient's email to confirm receipt. Below is a sample of the test email contents.

```
From: stasmtptest@example.com
Date: 10/20/2014 2:24 PM
Subject: STA Test Email Alert - 2014-10-20 14:23:54 (Test Email sta_server)
STA Test Email Alert - 2014-10-20 14:23:54 (Test Email sta_server)
```

6. If the email does not arrive within a few minutes, verify that the STA email server and recipient have been defined correctly. You can also check the following STA log for additional information. Contact your IT administrator for assistance, if necessary.

```
/Oracle_storage_home/Middleware/user_projects/domains/TBI/servers/staEngine/logs/
staEngine.log
```

# 14

## Service Log Bundles

Create log bundles to collect information that can help troubleshoot STA issues.

You should create log bundles as soon as possible after an issue occurs, as this makes it easier for Oracle support or STA development to find details leading up to the issue.

- [About Log Bundles](#)
- [Create and Submit a Log Bundle to Oracle Support](#)
- [Delete a Log Bundle](#)
- [View a List of Log Bundles](#)
- [Display Log Run Information](#)

**See Also:**

- [Automatic Log Bundles and SDP](#)

### About Log Bundles

Log bundles are a set of logs saved to a compressed zip file. Oracle support can use these log bundles to troubleshoot issues with STA.

- [Log Bundle Types](#)
- [Log Bundle Naming](#)
- [Log Bundle Retention](#)
- [Log Bundle Directories](#)

### Log Bundle Types

There are three main log bundle types: RDA, STA database, and library component. Each collects a different set of information.

**Remote Diagnostics Agent (RDA) log bundles**

Collect information about the STA server environment, the operating system, and the STA application. You can create RDA logs automatically or manually. STA generates an RDA bundle when STA is restarted or when the password or port change utility is unable to roll back to a previous value.

Oracle support can use RDA log bundles to troubleshoot issues with STA installation and configuration, and server system performance and security. You may want to create an RDA log bundle when:

- The STA user interface displays a message indicating you should take a snapshot.
- Oracle Service requests that you take a snapshot.
- An unexpected STA application event occurs and it appears to be a bug.

### STA database log bundles

A full dump of the STA MySQL database. You can only create these manually. Oracle Service can use database bundles to troubleshoot issues with the database itself or with the STA application. You can use them to back up the database before an upgrade or to transfer it to another server. Although the dump file is compressed, it can be quite large, depending on the size of your STA database.

### Library component log bundles

Logs for libraries, drives, media, robots, CAPs, PTPs, or elevators. Media bundles can only be created manually. All other library component bundles can be created manually or automatically.

The log bundles include information about component configuration and current top-level condition and health, if available. Also, for drives and media, the bundles include recent exchange history. Oracle support can use these log bundles to troubleshoot issues with individual components monitored by STA.

## Log Bundle Naming

STA appends log information to a user-assigned prefix name to ensure each bundle has a unique name.

The filename is:

```
user-assigned_prefix--logtype_component_type-serial_number_timestamp.zip
```

Where:

- *user-assigned\_prefix* — maximum 210 alphanumeric characters or underscores. Multiple consecutive underscores are not valid. Spaces are automatically replaced with underscores. Cannot begin with AUX, CON, NUL, or PRN.
- *log\_type* — identifies the type of log bundle. For example, CAP, STA\_DBSnapshot.
- *component\_type*— identifies the specific type of component, such as ROTATIONAL\_CAP, HP\_LTO5.
- *identifier*—unique serial number of the hardware component. Does not apply to RDA log bundles.
- *timestamp*—date and time when the log bundle was created.

For example:

```
NSDB--STA_DBSnapshot-14.4.2017.53.03.26.zip  
NSCAP--Cap_CAP-516000100437+1643197981+4_-07.4.2017.51.08.09.zip
```

## Log Bundle Retention

STA retains log bundles for 10 days, based on their creation date, then automatically purges them.

You can create any number of log bundles. The size and number are limited only by the available disk space on the STA server. Once purged, log bundles no longer appear on the Service–Logs screen. If you want to retain selected bundles for a longer time, you can download them to your local computer within the 10-day period. You can also delete log bundles manually at any time.

**See Also:**

- [Download a Log Bundle](#)
- [Delete a Log Bundle](#)

## Log Bundle Directories

The location of log bundles depends on the log type and creation method.

Log bundle and database dump creation log directory:

```
/var/log/tbi/get_sta_db_bundle.log
```

Application generated RDA and library component log bundle directory:

```
/Oracle_storage_home/Middleware/rda/snapshots
```

Command line generated RDA log bundle directory:

```
/Oracle_storage_home/Middleware/rda/output
```

Where `/Oracle_storage_home` is the Oracle storage home location defined during STA installation. See the *STA Installation and Configuration Guide* for details.

## Create and Submit a Log Bundle to Oracle Support

Manually create a log bundle and the submit it to My Oracle Support.

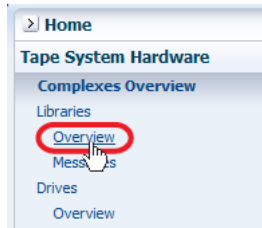
1. Manually create a log bundle using one of the following procedures:
  - [Create a Library Component Log Bundle](#)
  - [Create a Database Bundle](#)
  - [Create an RDA Log Bundle from the STA Application](#)
  - [Create an RDA Log Bundle from the System Command Line](#)
2. Download the log bundle zip file to your local computer.  
See [Download a Log Bundle](#).
3. Forward the log bundle zip file to My Oracle Support (MOS).  
See [Manually Forward a Log Bundle to My Oracle Support](#).


## Create a Library Component Log Bundle

Create a log bundle with a current snapshot of service information for a library component type: libraries, drives, media, robots, CAPs, PTPs, or elevators.

1. In the left navigation, expand **Tape System Hardware** and then select the Overview screen of a component type (such as **Libraries — Overview**).





2. Select a single table row and click **Create New Log Bundle** .

Library Serial Number	Library Complex Name	Library Name	Library Model
464970G+1243SY0	SL150_464970G+1243SY02	sta-sl150	SL150
571000200056	SL3000_571000200056	sl8500-85	SL3000
571000200060	SL3000_571000200060	crimson11	SL3000

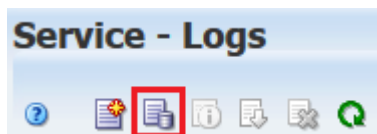
You can create log bundles for only one record at a time. If you select multiple records, **Create New Log Bundle** is greyed-out.


3. Enter the user-assigned prefix in the `Log Bundle Name` field. Click **Save**.  
See [Log Bundle Naming](#) for more information.
4. It may take several minutes for STA to create and save the bundle. If you leave the current screen, the process continues in the background.

## Create a Database Bundle

Create a database bundle, which is a full MySQL dump of the STA database.

1. In the left navigation, expand **Setup & Administration**, then select **Logs**.
2. Click **Create New Database Bundle** .

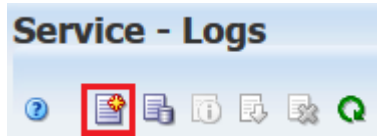



3. Enter the user-assigned prefix in the `Database Bundle Name` field. Click **Save**.  
See [Log Bundle Naming](#) for more information.
4. It may take several minutes for STA to create the bundle. You may need to click **Refresh Table**  for the log to appear on the screen. If you leave the screen, the process continues in the background.

## Create an RDA Log Bundle from the STA Application

Create an RDA log bundle, which contains a current snapshot of service information for the STA server and application.

1. In the left navigation, expand **Setup & Administration**, then select **Logs**.
2. Click **Create New Log Bundle** .



3. Enter the user-assigned prefix in the `Log Bundle Name` field. Click **Save**.  
See [Log Bundle Naming](#) for how this value is used.
4. It may take several minutes for STA to create the bundle. You may need to click **Refresh Table**  for the log to appear on the screen. If you leave the screen, the process continues in the background.

## Create an RDA Log Bundle from the System Command Line

Collect service information manually from the system command line.

1. Log on to the STA server as the Oracle user.
2. Change to the RDA directory. For example:  

```
# cd /Oracle/Middleware/rda
```
3. Verify that the RDA `output.cfg` file is present.  

```
$ ls -la output.cfg
-rw-r----- 1 oracle oinstall 23550 Mar 29 12:47 output.cfg
```
4. Enter the following command to generate the log bundle.  

```
$ ./rda.sh -f -v
```

Where:

- `-v`—Displays the progress of the data collection; this parameter is optional.
- `-f`—Forces a current data collection.

The utility generates an RDA log bundle with the default name `RDA_ouput_us.zip`. This may take several minutes.

5. Use any of the following commands to display information about the `rda.sh` utility:
  - `./rda.sh -M`—Displays the complete man page for the utility.
  - `./rda.sh -M STA`—Displays a summary of the log files generated by the utility for STA.
  - `./rda.sh -h`—Displays help information for all utility options.
6. Rename the RDA zip file to a unique name. For example:  


```
# mv RDA_output_us.zip RDA.STA_myserver_170223.zip
```
7. Optionally, use one of the following methods to display a listing of the files.
  - Open a browser window on the STA server and navigate to the URL: `file:///Oracle/Middleware/rda/output/RDA__start.htm`

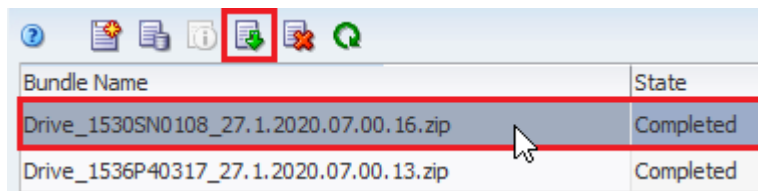
- Download the zip file to your local computer, unzip the bundle, and access the log files through the URL above.

## Download a Log Bundle

Download a completed log bundle to your local computer saved as a zip file. Then email the log bundle to Oracle support or attach it to an Oracle Service Request.

This procedure applies only to log bundles created from the STA user interface. To download RDA log bundles created from the system command line, see [Create an RDA Log Bundle from the System Command Line](#).

1. In the left navigation, expand **Setup & Administration**, then select **Logs**.
2. Select a log bundle in the list, and then click **Download Selected Bundle** .



Bundle Name	State
Drive_1530SN0108_27.1.2020.07.00.16.zip	Completed
Drive_1536P40317_27.1.2020.07.00.13.zip	Completed

3. Save the file to the location of your choice.

## Manually Forward a Log Bundle to My Oracle Support


Email a log bundle to you service representative or attach it to an Oracle Service Request (SR).

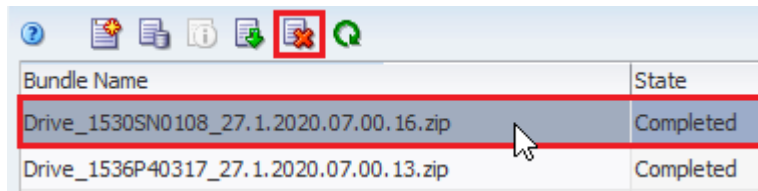
If you are using SDP, log bundles are automatically send to Oracle. See [How Automatic Bundle Alerts Work](#).

1. Access the My Oracle Support website at the following URL:  
<https://support.oracle.com/CSP/ui/flash.html>
2. Click **Sign In** and enter your username and password.
3. Select the **Service Requests** tab.
4. In the top menu, select **Help**, then **How do I create an SR?**
5. Follow the instructions to provide the necessary information, upload the log bundle, and submit the SR.

## Delete a Log Bundle

Delete a log bundle to remove it from the system and clear space.

1. In the left navigation, expand **Setup & Administration**, then select **Logs**.
2. Select a log bundle in the list, and then click **Delete Selected Bundle** .



Bundle Name	State
Drive_1530SN0108_27.1.2020.07.00.16.zip	Completed
Drive_1536P40317_27.1.2020.07.00.13.zip	Completed

## View a List of Log Bundles

Display information for log bundles created through the STA application.

1. In the left navigation, expand **Setup & Administration**, then select **Logs**.
2. The Service Logs screen displays the following information for each log bundle:
  - Bundle Name—Unique name assigned to the log snapshot, including a user-defined prefix.
  - State—Running state of the log bundle (Running or Completed)
  - Date Created—Date and time the log run was started
  - File Size (KB)—Size of the log bundle file

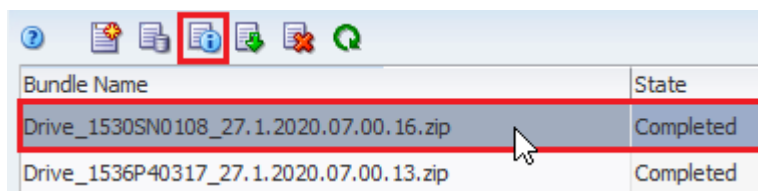
See [Log Bundle Types](#) for descriptions of the types of log bundles.

## Display Log Run Information

Display detailed information about a manually created log bundle.

You can perform this procedure while the log is running or after it completes. You cannot view information for manual RDA bundles created from the system command line.

1. In the left navigation, expand **Setup & Administration**, then select **Logs**.
2. Select a log bundle in the list. Click **Bundle Run Info** .



Bundle Name	State
Drive_1530SN0108_27.1.2020.07.00.16.zip	Completed
Drive_1536P40317_27.1.2020.07.00.13.zip	Completed

3. Review the information, and then click **Close**.

# 15

## Automatic Log Bundles and SDP

You can enable STA to create automatic log bundles based on a set of pre-defined policies. If you have Service Delivery Platform (SDP) installed at your site, you can configure STA to forward automatic bundles to SDP.

Depending on SDP and Oracle's Auto Service Request (ASR) configuration, SDP may automatically create a Service Request and forward the log bundles to My Oracle Support (MOS).

- [How Automatic Bundle Creation Works](#)
- [Enable or Disable Automatic Bundle Creation](#)
- [Define the SDP Host to STA](#)
- [Test STA to SDP Communication](#)
- [Define Email Recipients for Automatic Log Bundle Alerts](#)
- [Display Automatic Bundle Creation Policies](#)
- [Display Automatic Bundle Alerts](#)
- [Display Library Components With Automatic Bundles](#)

### How Automatic Bundle Creation Works

After you configure automatic bundle generation, STA creates bundles when certain events occur within the library system.

By default, automatic bundle generation is disabled. Once enabled, STA creates automatic RDA or library component log bundles according to the predefined policies. STA automatically generates an alert when a log bundle is created and sends email notifications to the designated recipients.

If you have enabled forwarding to SDP, STA automatically sends the log bundles to the SDP host. SDP only receives log bundles for hardware and products that are registered for service under the connected SDP server. However, you can manually download all log bundles from STA (whether sent to SDP or not) through the STA interface. STA purges automatic bundles when they are 10 days old, based on their creation date.

Some examples of events that may cause STA to generate an automatic bundle are:

- A library is in a not-operative state.
- A library drive has "Action" health.
- A library robot is in a degraded state.
- STA has been restarted.
- The STA password change utility is unable to roll back to the previous password.

**See Also:**

- [Display Automatic Bundle Creation Policies](#)

- [How the Service Delivery Platform \(SDP\) Handles a Bundle](#)
- [How Automatic Bundle Alerts Work](#)

## How the Service Delivery Platform (SDP) Handles a Bundle

After receiving an automatic log bundle, SDP processes the bundle according to the policies configured for your site.

- If Oracle's Auto Service Request (ASR) is configured at your site, a Service Request (SR) may be automatically generated and the log bundle attached. ASR is a feature of Oracle hardware warranty, Oracle Premier Support for Systems, and Oracle Platinum Services.
- If Remote Request is configured at your site, your Oracle Service Representative may request that SDP collect additional log bundles, if necessary.

See the following documentation on My Oracle Support (MOS):

<https://support.oracle.com>.

- *StorageTek Service Delivery Platform User's Guide*—describes installation and configuration of StorageTek SDP.
- *ASR Manager User's Guide*—describes installation and configuration of ASR.

## How Automatic Bundle Alerts Work

STA creates an alert whenever it creates an automatic log bundle. These automatic bundle creation alerts behave similarly to other STA alerts, but their criteria are not user-modifiable.

Optionally, you can define email recipients for automatic bundle creation alerts. Whenever STA generates an alert, it also sends emails to the designated addresses. Through emailed alerts, users can be notified of automatic bundle activity without the need to log in to the STA application. Alert emails can even be sent to employees who do not have STA login privileges.

### See Also:

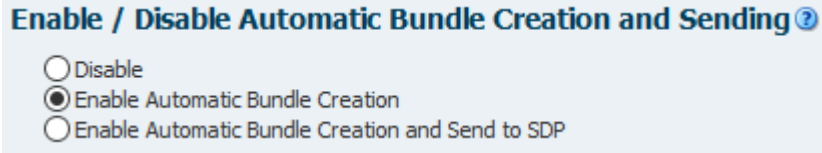
- [How Alerts Work](#)
- [Define Email Recipients for Automatic Log Bundle Alerts](#)

## Enable or Disable Automatic Bundle Creation

Choose to enable or disable automatic log bundle creation. Choose to send the bundles to SDP or have them remain only on the STA server. Changes take effect immediately.

1. Review [Best Practices When Enabling Automatic Bundle Creation](#).
2. If using SDP, complete the following before enabling automatic bundles:
  - [Define the SDP Host to STA](#)
  - [Test STA to SDP Communication](#)
3. In the left navigation, expand **Setup & Administration**, then select **Automatic Bundles & SDP**.

4. Near the top of the screen, select an option:
  - **Disable**
  - **Enable Automatic Bundle Creation**
  - **Enable Automatic Bundle Creation and Send to SDP**



5. Click **OK** to dismiss the dialog box.
6. The *Last Enable/Disable Result* column of the SDP Host Settings and Status table shows the status of your configuration change.

**SDP Host Settings and Status**

SDP Host IP Address	SDP Host Port	Connection Status	Registration Status	Last SDP Test Result	Last Enable/Disable Result
10.80.40.113	15000			SUCCESS: Connection Test	SUCCESS: Automatic Bundle Creation Only is enabled.

## Best Practices When Enabling Automatic Bundle Creation

Follow these tips when configuring and managing automatic bundle creation.

### Ensure library data collections are complete before enabling forwarding to SDP

Before enabling forwarding to SDP, ensure that data collections for all STA-monitored libraries have completed successfully. Specifically, the *Last Connection Status* column for all libraries must say *SUCCESS*. Wait for any in-process data collections to complete successfully, and troubleshoot and repeat any failed data collections.

### Disable forwarding to SDP before making library changes

Disable forwarding to SDP before making any of the following library configuration changes:

- Add or remove a library from STA monitoring.
- Modify SNMP connection settings in STA or the library.
- Upgrade library firmware.
- Add, remove, or swap a drive.
- Add, remove, or swap a library component, such as a robot, pass-thru port (PTP), or storage cells.


## Define the SDP Host to STA





Identify the SDP host so that STA can send automatic log bundles. This procedure applies only if you want to use automatic bundle creation and forwarding to SDP.

### Note:

SDP-to-STA connectivity is a 1-to-1 relation. Do not configure multiple STA servers to a single SDP server, or vice versa. Only connect one STA server to one SDP server.

STA can only connect to supported versions of SDP. See the requirements in the *STA Installation and Configuration Guide* or contact your Oracle support representative for supported versions.

1. Verify the IP address and hostname of the SDP server are defined on the network. You may need to add an entry in the `/etc/hosts` file of the STA server. For example "10.20.30.40 sdp2host".
2. Obtain the following information:
  - IP address of the SDP host.
  - Port number for outbound communication from STA to the SDP host. The same port must be assigned on both the STA server and the SDP host. See the *StorageTek Service Delivery Platform User's Guide* for complete instructions on configuring the SDP host.
3. In the left navigation, expand **Setup & Administration**, then select **Automatic Bundles & SDP**.
4. In the SDP Host Settings and Status table, click **Edit SDP Host Details** .



SDP Host Settings and Status 		
		
SDP Host IP Address	SDP Host Port	Connection Status
10.80.40.113	15000	

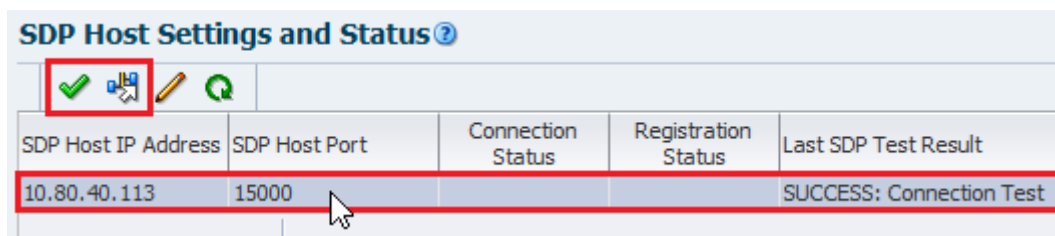
5. Complete the **Configure SDP Host** dialog:
  - **SDP Host IP Address**—IP address of the SDP host. This must be the IP address of a valid SDP host on the network.
  - **SDP Host Port**—Port number on the STA server to be used for outbound communication to the SDP host. The same port number must be configured on the SDP host to receive messages from STA. Default is 15000.
6. Click **OK**. You can now test the SDP host connection.  
See [Test STA to SDP Communication](#).



## Test STA to SDP Communication

Test the communication between STA, the SDP host, and My Oracle Support. This procedure applies only if you want to use automatic bundle creation and forwarding to SDP.

1. Before testing the connection, you must define the SDP host. See [Define the SDP Host to STA](#).
2. In the left navigation, expand **Setup & Administration**, then select **Automatic Bundles & SDP**.
3. Highlight the SDP host in the *SDP Host Settings and Status* table, and click either:
  - **Connection Test to SDP Host**  — Verifies STA can communicate with the SDP server.
  - **Service Request Test to SDP Host**  — Verifies SDP can receive requests from STA and that the SDP host has been registered and can communicate with My Oracle Support. You should run the connection test first before running this test.




SDP Host IP Address	SDP Host Port	Connection Status	Registration Status	Last SDP Test Result
10.80.40.113	15000			SUCCESS: Connection Test

4. Click **OK** to dismiss the dialog box.
5. View the *Last SDP Test Result* column of the SDP Host Settings and Status table. You may need to refresh the table.

For connection tests, that status might be "SUCCESS: Connection test" or "FAILURE: Failure to register STA with SDP".

For service request tests, the status might be "SUCCESS: Service Request test" or "FAILURE: Service Request test. STA unable to connect to SDP".

6. If you are unable to connect to SDP, verify that you have added the SDP server to the `/etc/hosts` file of the STA server. For example "10.20.30.40 sdp2host". See the Troubleshooting appendix of the *STA Administration Guide* for more information.
7. If the Service Request test fails, but the Connection Test succeeds, verify the SDP server is connected and communicating with its ASR/My Oracle Support server. The Service Request test is an end-to-end test that requires all server connections be operational.
8. Verify successful data collection for all monitored libraries. This ensures that SNMP communication is established and STA has current configuration information for all monitored libraries.
  - a. In the left navigation, expand **Setup & Administration**, select **SNMP Connections**.
  - b. Verify that the `Last Connection Status` for all monitored libraries indicates SUCCESS.

Monitored Libraries 			
Library Name	Library Complex	Library IP Address(es)	Last Connection Status
crimson11	SL3000_571000200060	10.80.104.51	FAILED
elib18	SL8500_2	10.80.104.98 10.80.105.98	SUCCESS
elib6	SL8500_8	10.80.104.86	FAILED

- If any libraries indicate `IN PROGRESS`, wait for data collection to complete.
- If any indicate `FAILED`, troubleshoot the problem (see the *STA Installation and Configuration Guide*) and then initiate a new data collection (see [Manually Collect Library Data](#)).


### When to Test the STA to SDP Communication

Oracle recommends you test the connection at the following times:

- Before enabling forwarding to SDP
- After modifying connection settings in STA or the SDP host
- After rebooting either STA or the SDP host
- Any time you suspect the connection between STA, the SDP host, and My Oracle Support has been lost or interrupted

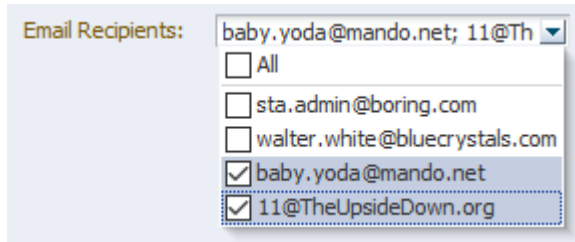
## Define Email Recipients for Automatic Log Bundle Alerts

Add or remove email recipients for a selected automatic bundle policy. Any number of addresses can receive emails.

1. You must have Administrator privileges.
2. Define the email recipients with in the **Setup & Administration Email** tab before adding them to an alert policy.
3. In the left navigation, select **Setup & Administration**, then select **Automatic Bundles & SDP**.
4. Select a policy in the Automatic Bundle Creation Policies table, click **Edit Email Recipients** .

Automatic Bundle Creation Policies 		
Policy Name	Date Created/Updated	Policy Description
ABC-CAP-Status-Degraded	2017-07-28 14:38:18	This policy will match whenever the CAP top level condition changes to DEGRADED state.
ABC-CAP-Status-Notoperativ	2017-07-28 14:38:18	This policy will match whenever the CAP top level condition changes to NOT-OPERATIVE

5. From the drop-down menu, select the **Email Recipients**. Click **OK**.



6. STA sends alerts to the recipients according to the alert generation requirements.  
 See [Modify Email Recipients for an Alert Policy](#).

## Display Automatic Bundle Creation Policies

View a list of pre-defined policies for creating automatic bundles. There is one policy for each type of library component. An alert is triggered when an automatic log bundle for that library component type is created.

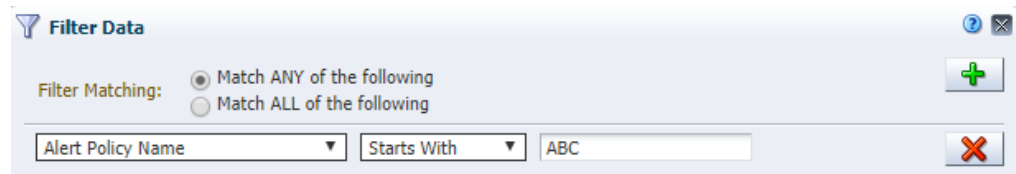
1. In the left navigation, expand **Setup & Administration**, then select **Automatic Bundles & SDP**.
2. The policies are listed in the Automatic Bundle Creation Policies table.

Automatic Bundle Creation Policies	
Policy Name	Date Created/Updated
ABC-CAP-Status-Degraded	2020-03-17 10:56:22
ABC-CAP-Status-Notopera...	2020-03-17 10:56:22

## Display Automatic Bundle Alerts

Filter the Alerts Overview screen to show automatic bundle alerts. Automatic bundle alerts have an Alert Policy Name prefixed by "ABC".

1. In the left navigation, expand **Tape System Activity**, then select **Alerts Overview**.
2. Filter for alerts starting with "ABC":
  - a. Click **Filter Data** in the table toolbar.
  - b. Select **Match ALL of the following** and specify **Alert Policy Name | Starts With | ABC**.



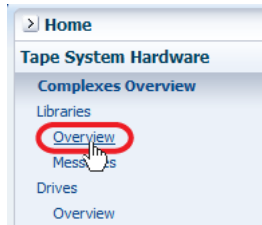
- c. Click **Apply**.



3. See [Filters](#) to apply additional filtering criteria.

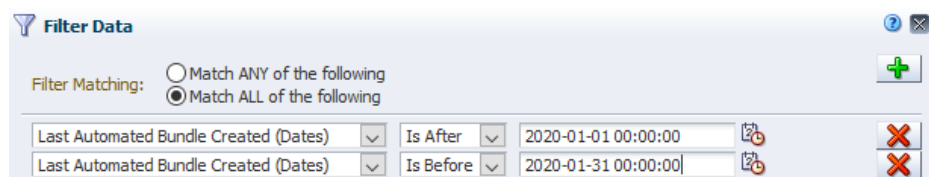
## Display Library Components With Automatic Bundles

Display all library components that have an automatic log bundle within a specified time period.

1. In the left navigation, expand **Tape System Hardware** and then select the **Overview** screen of a component type (such as Libraries—Overview).



2. Verify that the *Last Automatic Bundle Created* column is in the table. If not, add the column to the table:
  - a. From the **View** drop-down , select **Columns**, then **Show More Columns...**
  - b. Move **Last Automatic Bundle Created** to the Visible Columns list. Click **OK**.
3. Filter for bundles created during specified time period:
  - a. Click **Filter Data**  in the table toolbar.
  - b. In the filter matching field, select **Match ALL of the following**.
  - c. Specify criteria using the **Last Automatic Bundle Created** attributes.  
 For example: Last Automated Bundle Created (Dates) | Is After | a date.
  - d. Click **Apply**.



**See Also:**

- [Filters](#)
- [Hide and Reveal Columns](#)

# 16

## Library Connection (SNMP or SCI)

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

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

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

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

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

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

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



#### Note:

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

- [Configure SNMP on the Libraries](#)
- [Configure SNMP on the STA Server](#)
- [Update the SNMP Configuration After a Library or STA Change](#)
- [Troubleshoot the Library Connection](#)
- [Configure SNMP v2c Mode](#)

## Configure SNMP on the Libraries

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

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

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

### Retrieve the Library IP Address


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

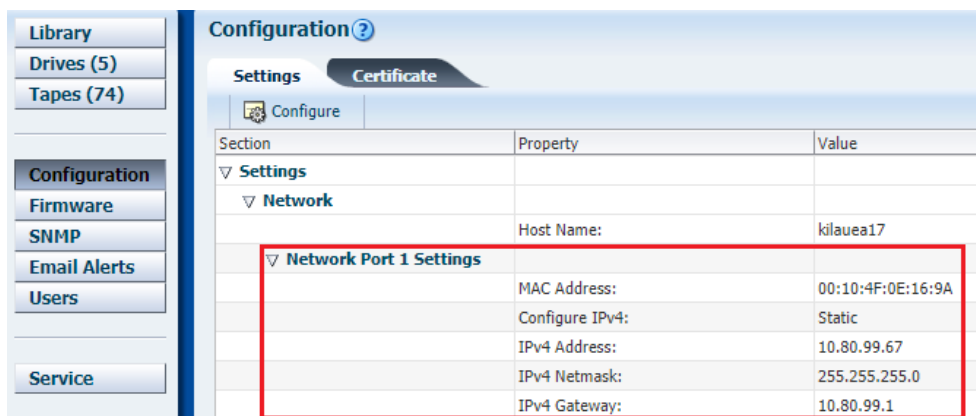
For SL3000 and SL8500 libraries, choose the method that corresponds to the library's configuration, either: Redundant Electronics, Dual TCP/IP, or neither.

#### SL150

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

 **Note:**

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



The screenshot shows the Configuration interface with a navigation tree on the left and a main configuration area on the right. The navigation tree includes Library, Drives (5), Tapes (74), Configuration (selected), Firmware, SNMP, Email Alerts, Users, and Service. The main area is titled 'Configuration' and has tabs for Settings and Certificate. Under the Settings tab, there is a 'Configure' button and a table with columns for Section, Property, and Value. The table is expanded to show 'Network Port 1 Settings' with the following properties:

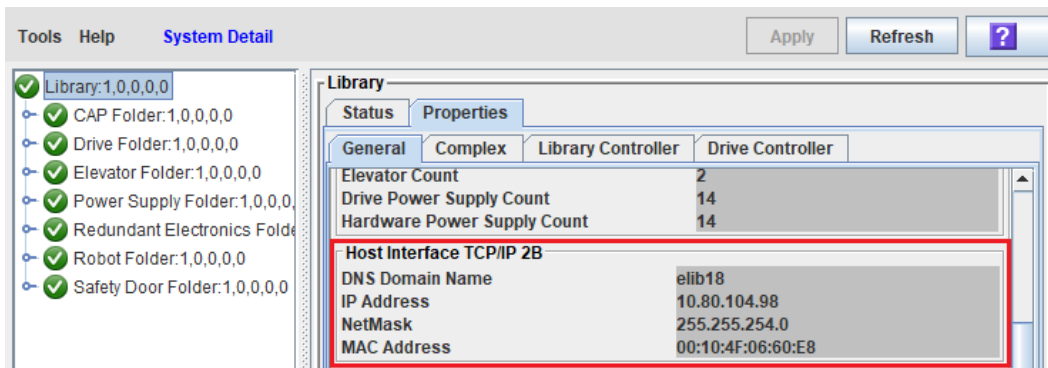
Section	Property	Value
Settings		
Network		
	Host Name:	kilauea17
Network Port 1 Settings		
	MAC Address:	00:10:4F:0E:16:9A
	Configure IPv4:	Static
	IPv4 Address:	10.80.99.67
	IPv4 Netmask:	255.255.255.0
	IPv4 Gateway:	10.80.99.1

**SL500**

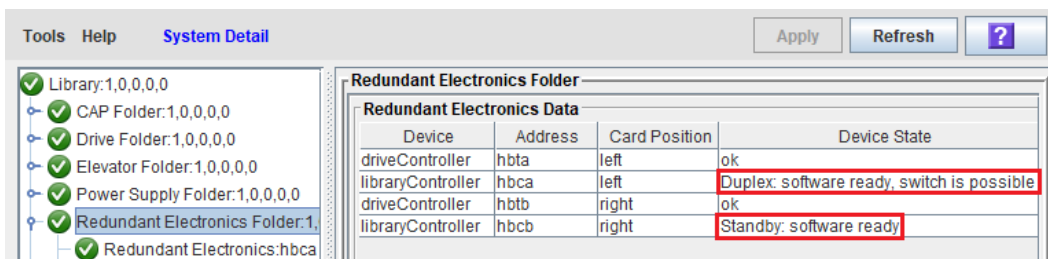
1. Using SLC, from the **Tools** menu, select **System Detail**.
2. In the navigation tree, select **Library**.
3. Select the **Properties** tab, then select the **General** tab.  
The library IP address is listed under the Library Interface TCP/IP section.
4. Record the library IP address as the primary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

**SL3000 or SL8500 - Neither Dual TCP/IP nor RE**

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

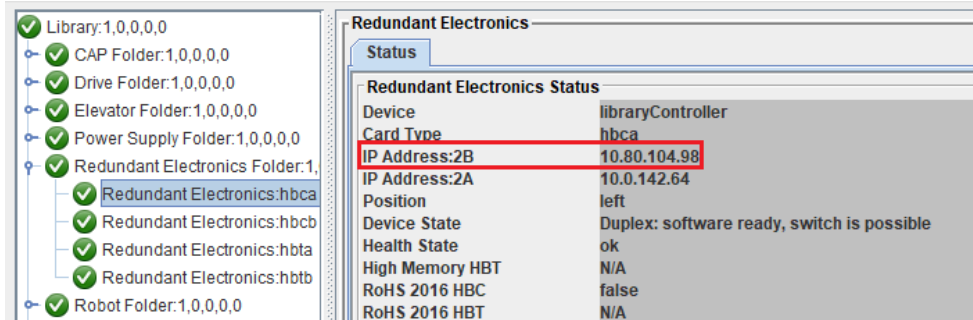
**SL3000 or SL8500 - Redundant Electronics Support**

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



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

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



Redundant Electronics Status	
Device	libraryController
Card Type	hbca
IP Address:2B	10.80.104.98
IP Address:2A	10.0.142.64
Position	left
Device State	Duplex: software ready, switch is possible
Health State	ok
High Memory HBT	N/A
RoHS 2016 HBC	false
RoHS 2016 HBT	N/A

- Repeat for the alternate (standby) controller card.

### SL3000 or SL8500 - Dual TCP/IP Support

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

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

#### Note:

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

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

## Enable SNMP on the Library

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

### SL3000 and SL8500

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

```
> snmp enable port2b
```

### SL500

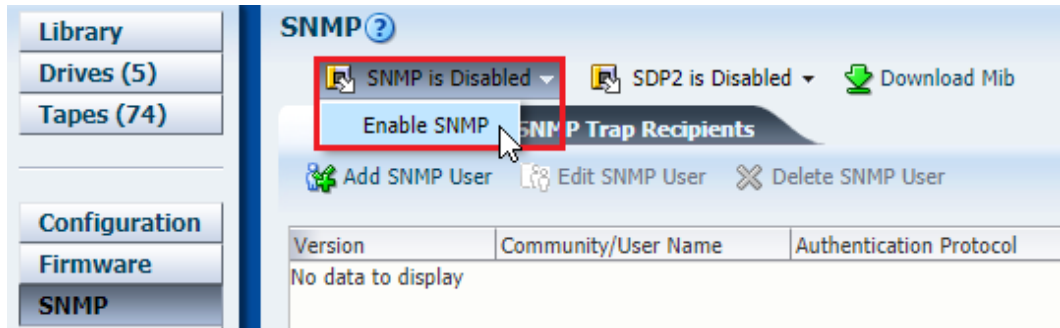
Enable SNMP on port 1B using the CLI.

```
> snmp enable port1b
```



## SL150

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



## Create an SNMP v3 User

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

### Requirements

- The authorization method must be `SHA` (Secure Hash Algorithm), and the privacy method must be `DES` (Data Encryption Standard).
- All SNMP libraries must use the same SNMP v3 credentials. Define a unique SNMP v3 user for this purpose and then define this same user on all monitored libraries.
- Do *not* use the values "public" or "private" for the SNMP v3 username, as these values are well known and present a security risk. Use values that are not as easily discovered. The username can only contain alphanumeric characters (a–z, A–Z, 0–9). Special characters are not allowed.
- Authorization and privacy passwords must be at least eight characters in length, and cannot contain commas, semicolons, or equal signs.

### SL500, SL3000, and SL8500

#### Note:

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

1. Using CLI, create an SNMP v3 user:

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

Where:

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

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

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

For SL500, do not use quotes. For example:


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

2. List the SNMP users to verify that the SNMP v3 user has been added correctly.
  - > `snmp listUsers`

## SL150

### Note:

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

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

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

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

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

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

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

## Create the STA SNMP v3 Trap Recipient

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

Note the following configuration requirements:

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

### SL500, SL3000, SL8500

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

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

Where:

- STA\_server\_IP is the IP address of the STA server.
- recipient\_name is the SNMP username you created in for the SNMPv3 user.
- auth\_password and priv\_password are the authorization and privacy passwords you created in for the SNMPv3 user.
- library\_engineID is the library engine ID you displayed in [Retrieve the Library SNMP Engine ID \(SL500, SL3000, SL8500\)](#), including the 0x prefix.

For SL3000 and SL8500 libraries, enclose recipient\_name, auth\_password, and priv\_password in single quotes. For example:

```
SL3000> snmp addTrapRecipient trapLevel
1,2,3,4,11,13,14,21,25,27,41,45,61,63,65,81,85,100 host 192.0.2.20 version v3 name
'STAsnmp' auth SHA authPass 'authpwd1' priv DES privPass 'privpwd1' engineId
0x00abcdef00000000000000000000
```


For SL500, do not use quotes. For example:

```
SL500> snmp addTrapRecipient trapLevel
1,2,3,4,11,13,14,21,25,27,41,45,61,63,65,81,85,100 host 192.0.2.20 version v3 name
STAsnmp auth SHA authPass authpwd1 priv DES privPass privpwd1 engineId
0x00abcdef00000000000000000000
```

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

```
> snmp listTrapRecipients
```

### SL150

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

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

## Configure SNMP on the STA Server

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

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

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

## Sign In to the STA GUI

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

1. Go to: **http(s)://<host\_name>:<port>/STA/**

Where:

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

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

2. Enter the STA administrator username and password.

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

## Verify SNMP Communication with a Library (optional)

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

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

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

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

Where:

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

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

Successful snmpget command:

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

Failed snmpget commands:

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

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

4. Test the SNMP v2c connection.

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

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

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

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

- a. Log in as the system root user.

```
$ su root
```

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

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


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

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

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

## Configure SNMP Client Attributes for STA

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

1. In the STA GUI, expand the **Setup & Administration** tab, and then select **Library Connections**.
2. Select the row in the Client Attributes table, and then click **Edit** .



SNMP Username	Password Encryption	Privacy Encryption
jep1	SHA	DES

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

### Note:

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

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

- **Enter Privacy Encryption Password (Privacy)**—Type the privacy encryption password.
  - **User Community**—Type the SNMP v2c community string specified on the library. This field is required for the SNMP handshake with the library.
  - **Trap Community** —Type the SNMP v2c community string specified on the library. This field is used only if SNMP v2c is used for communication with the library.
4. Click **Save**.
  5. Click **OK** to dismiss the message. You will perform the connection test later.


## Configure the SNMP Connection to a Library


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











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

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

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

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

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

Monitored Libraries 		
		
		
		
Library Name	Library Complex	Library IP Address(es)
crimson11	SL3000_571000200060	10.80.104.51
elib18	SL8500_2	10.80.104.98 10.80.105.98
elib6	SL8500_8	10.80.104.86

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

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

 **Caution:**

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

- **Library Time Zone**—Select the library's local time zone.
5. Click **Save**. Click **OK** to dismiss the Library Connection Test message. You will perform the test after adding all libraries.
  6. Repeat for each library monitored by STA.
  7. After adding all the libraries, proceed to [Test the Library Connection](#).

## Update the SNMP Configuration After a Library or STA Change

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

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

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

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

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



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

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

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

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

### Update the SNMP Settings in STA

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

In the Define Library Connection Details dialog box, clear the Library Engine ID field and click **Save**. This forces STA to update the engine ID to the new value when it reconnects to the library.

3. Re-establish the SNMP connection with the library. See [Test the Library Connection](#).
4. Record the new SNMP engine ID displayed on the SNMP connections table. You will use this value in the next part of the procedure.

### Verify SNMP Settings on the Library

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

## Update SNMP After Changing the STA Server IP Address

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

### Confirm Network and SNMP Connectivity

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

### Update SNMP Settings on the Library


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

### Update SNMP Settings in STA

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

## Remove a Library Connection from STA

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

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

## Delete or Modify the STA Trap Recipient

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

### SL150

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

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

#### SL500, SL3000, and SL8500

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

```
snmp deleteTrapRecipient id index
```

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

For example: ADMIN> snmp deleteTrapRecipient id 1

3. Re-add the trap recipient, as necessary (see [Create the STA SNMP v3 Trap Recipient](#)).

## Configure SNMP v2c Mode

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

To configure the libraries and STA to use SNMP v2c:

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

## When to Use v2c Mode

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

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

## Create an SNMP v2c User

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

### Requirements

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

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

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

### SL500, SL3000, and SL8500

1. Using CLI, add the SNMP v2c user.

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


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

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

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

```
> snmp listUsers
```

### SL150

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

## Create the STA SNMP v2c Trap Recipient

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

Note the following configuration requirements:

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

### SL500, SL3000, and SL8500

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

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

Where:

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

For example:

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

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

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

### SL150

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

## Enable SNMP v2c Mode for STA

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

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

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

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

4. Edit the SNMP version properties file.
5. Change the SNMP v2c parameter to `true`.

```
V2c=true
```

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

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

## Configure SCI (for SL4000)

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

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

- [Add the SL4000 as a Monitored Library](#)
- [Test the Library Connection](#)
- [Manually Collect Library Data](#)

## Add the SL4000 as a Monitored Library


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


### Prerequisites before connecting STA to an SL4000

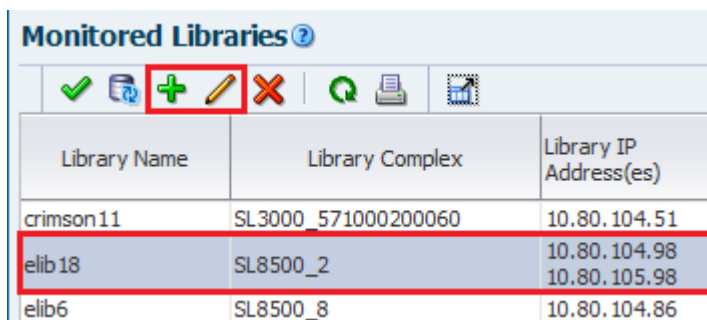
- Obtain the credential information for an SL4000 user with the "User" role to be used by STA to communicate using SCI.
- Obtain the credential information for an STA account to be used by the SL4000 to communicate to STA using outbound SCI.
- Configure the STA server firewall settings for the following: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

### Procedures

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

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

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




Library Name	Library Complex	Library IP Address(es)
crimson11	SL3000_571000200060	10.80.104.51
elib18	SL8500_2	10.80.104.98 10.80.105.98
elib6	SL8500_8	10.80.104.86

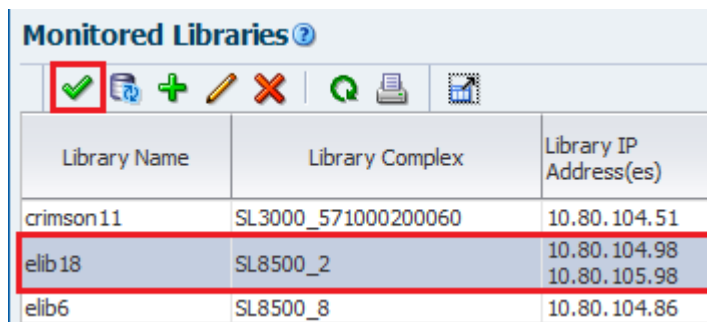
4. Select **Library API** for the connection type.
5. Complete the dialog box:
  - **Library Name**—A name to identify the library throughout the STA user interface screens (for example, the library host name).
  - **Library Primary IP Address**—The IP address of the primary public port on the library.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

## Test the Library Connection

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

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

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



Library Name	Library Complex	Library IP Address(es)
crimson11	SL3000_571000200060	10.80.104.51
elib18	SL8500_2	10.80.104.98 10.80.105.98
elib6	SL8500_8	10.80.104.86

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

For SNMP, the message indicates results for the following:

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

For SCI, the message indicates results for the following:

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



- If the OSCI test fails, see [Enable and Test the SCI Destination on the SL4000](#).
  - If the test fails for other reasons, see [Troubleshoot the Library Connection](#).
7. After successfully testing the connection, proceed to [Manually Collect Library Data](#).

## When to Test the Library Connection

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

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


## Manually Collect Library Data


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




### Note:

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

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

Monitored Libraries 		
Library Name	Library Complex	Library IP Address(es)
crimson11	SL3000_571000200060	10.80.104.51
elib18	SL8500_2	10.80.104.98 10.80.105.98
elib6	SL8500_8	10.80.104.86

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

## When to Manually Collect Data

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

### Data collection is **REQUIRED** when:

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

### Data collection is **RECOMMENDED** when:

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

## About Library Data Collection

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

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

### What is Collected During the Initial Data Collection

- Locations of activated storage cells
- Partition information

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

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

#### How Data Collections Are Initiated

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

#### Affect of Data Collections on Library Performance

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

#### What Data is Collected from the Library

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

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

## About the Monitored Libraries Table

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

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

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

Table Field	Description	Applies to:
Library IP Address	The IP address of the monitored library.	SNMP, SCI
STA IP Address	IP address of the STA server.	SNMP, SCI
Library Engine ID	The unique SNMP engine ID for the library (see <a href="#">About the Library Engine ID</a> ).	SNMP only
Connection Type	Either SNMP or Library API (which is also known as SCI).	SNMP, SCI
Library API User ID	ID of the SL4000 user account to be used for SCI communication.	SCI only
Library API HTTP port	Port used for SCI HTTP communication. The default is 7102.	SCI only
Library API HTTPS port	Port used for SCI HTTPS communication. The default is 7103.	SCI only
Recent Communication Status	Indicates the latest status of information from the library over the outbound SCI channel or SNMP trap channel. This may intermittently indicate MISSED HEARTBEAT. This is normal.	SNMP, SCI
Library Time Zone	The time zone of the library.	SNMP, SCI
Last Successful Connection	Date and time when the test or data collection was completed, if successful.	SNMP, SCI
Last Connection Attempt	Date and time when the connection test or data collection was initiated.	SNMP, SCI
Last Connection Status	Results of the test or data collection. <ul style="list-style-type: none"> <li>• IN PROGRESS – A data collection is underway.</li> <li>• SUCCESS – The connection test or data collection completed successfully.</li> <li>• FAILED – The connection test or data collection failed. Possible reasons are listed in the Last Connection Failure Detail field.</li> <li>• REJECTED – The data collection request was rejected, possibly because the library is busy or unavailable.</li> <li>• DUPLICATE – The data collection request was rejected because another one is already in progress.</li> </ul>	SNMP, SCI
Last Connection Failure Details	If the test or collection fails, STA provides information on the cause of failure.	SNMP, SCI

## About the Library Engine ID

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

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

**The Library Engine ID field may be blank if:**

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

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

**When to manually clear the Library Engine ID field:**

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

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

## Troubleshoot the Library Connection

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

### General Troubleshooting

- [Verify the Library is Operational](#)

### SCI Troubleshooting

- [Verify the Firewall Settings](#)
- [Enable and Test the SCI Destination on the SL4000](#)
- [Manually Configure the SL4000 to Send Outbound SCI to STA](#)

### SNMP Troubleshooting

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

## Verify the Library is Operational

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

### Note:

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

### SL150 or SL4000

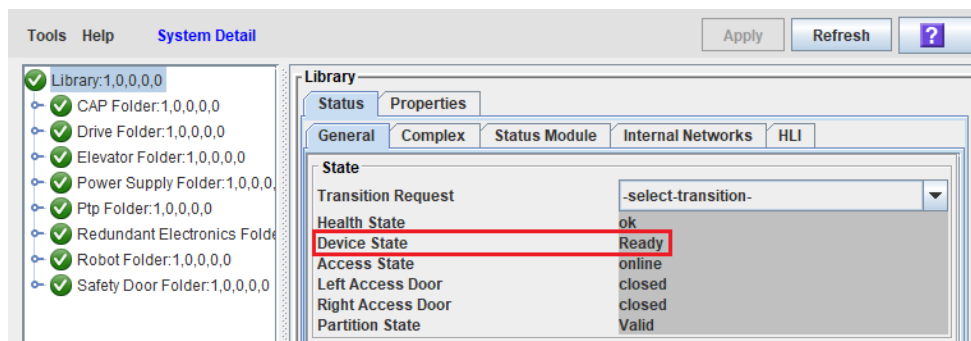
1. Log in to the browser-based user interface.
2. At the top of the screen, verify that the Health field indicates "Operational".

### SL500

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

### SL3000 and SL8500

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



## Verify the Firewall Settings

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

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

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

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

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

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

### WARNING:

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

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

```
# service iptables save
```

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

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

## Enable and Test the SCI Destination on the SL4000

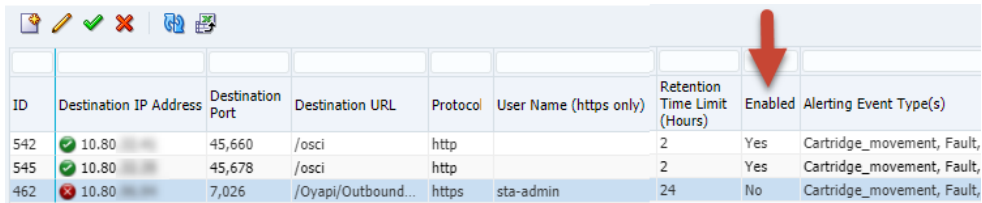
Verify the SCI destination is enabled and run a test to validate the configuration to the STA server is properly defined. The test sends a "test" event message to the destination.

### Access the SL4000 GUI Notifications Page


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

### Verify the Destination is Enabled


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



ID	Destination IP Address	Destination Port	Destination URL	Protocol	User Name (https only)	Retention Time Limit (Hours)	Enabled	Alerting Event Type(s)
542	10.80	45,660	/osci	http		2	Yes	Cartridge_movement, Fault,
545	10.80	45,678	/osci	http		2	Yes	Cartridge_movement, Fault,
462	10.80	7,026	/Oyapi/Outbound...	https	sta-admin	24	No	Cartridge_movement, Fault,


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

### Test the Destination

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

## Manually Configure the SL4000 to Send Outbound SCI to STA

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

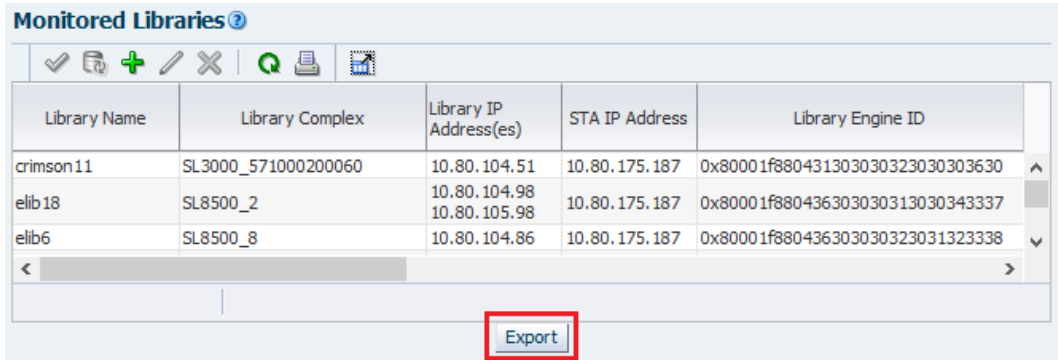
1. STA automatically configures OSCI when you add the SL4000 to the Monitored Libraries table within the STA interface. Only perform this procedure if you are troubleshooting a connection issue.
2. Sign in to the SL4000 GUI.
3. Click **Notifications** in the left navigation area.
4. Click the **SCI**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



## Export SNMP Connection Settings to a Text File

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

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



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

### Example 16-1 Sample SNMP Configuration File

```
Define SNMP Client Settings
```

```
Client Attributes
```

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

```
Monitored Libraries
```

```
STA IP Address = 10.80.145.78
Library Name = SL3000A
Library Complex = SL3000_5720123200089
Library Primary IP Address = 10.80.104.51
Library Secondary IP Address = Not Specified
Library Engine ID = 0x80001f880431303030123123303000
Requested MIB Walk Time = 00:00:00
Library Serial Number = 5720123200089
Library Time Zone = UTC
```

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

## Display All SNMP Trap Recipients

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

### SL150

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

### SL500, SL3000, and SL8500

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

```
snmp listTrapRecipients
```

For example:

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

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

## Troubleshoot a Failed MIB Walk Channel Test

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

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

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

### Steps to Perform on the Library

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

```
traceRoute <IP address of STA server public port>
```
  - SL500:

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

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

### Steps to Perform on the STA Server

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

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

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

## Troubleshoot a Failed Trap Channel Test

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

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

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

Use this procedure to diagnose and resolve the issues.

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

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

## Troubleshoot a Failed Media Validation Support Test

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

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

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

Use the following procedure to diagnose and resolve the issues.

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

## Troubleshoot Unsuccessful Trap Processing

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

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

```
# tcpdump -v host <IP address of library public port> > /var/tmp/<output file name> &
```
4. In the output, look for `.snmptrap` and `SNMPv3`. Network traffic for data collection requests contain `.snmp`.

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

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

If necessary, troubleshoot communications over this port:

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

```
"SEVERE: SNMP Trap/Inform Listener Port 162 is NOT bindable. Stop the application currently bound to that port."
```
- b. If port 162 is already in use, determine what process is using it.

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

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

```
# chkconfig --list
```

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

- a. Deconfigure SNMP services.

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

- b. Stop SNMP services.

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

- c. Stop and restart STA services.

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

7. If some traps are being reported in the STA Notifications screen, verify that all trap levels were specified when creating a trap recipient on the library. See the [SNMP v3 trap recipient creation procedure](#) in the [Create the STA SNMP v3 Trap Recipient](#) for the list of supported trap levels.
8. For the SL500, verify that you configured the library with a supported version of SL Console. Earlier versions of SL Console restrict the number of trap level characters that can be entered.
9. For SL500 and SL150 libraries, verify that the Volume Label Format is set properly.

# 17

## Understanding STA Data

Interpret STA data to address common questions about your tape library system. Understand how STA handles changes to the library system to better analyze and use the data provided by STA.

- [Understand How STA Handles Changes to the Tape Environment](#)
- [Use STA to Answer Common Tape Environment Questions](#)
- [General Error Trend Analysis](#)
- [Library System Analysis](#)
- [Drive Analysis](#)
- [Media Analysis](#)

## Understand How STA Handles Changes to the Tape Environment

Changes or anomalies in the tape system environment (such as removed drives or media, removed libraries, duplicate or missing media, and so on) can affect STA data.

- [Understand Data Retention and the Tracking Timestamp](#)
- [How Incomplete Exchanges Affect STA](#)
- [Why Some Values May Be Dimmed](#)
- [What Happens to Data When Drives and Media Are Removed](#)
- [What Happens to Data When Libraries Are Removed](#)
- [What Happens to Data When an SL8500 Library is Moved to a New Complex](#)
- [How STA Handles "Missing" Media](#)
- [How STA Handles Duplicate Volume Serial Numbers](#)
- [How to Map Host and STA Drive Identifiers](#)

## Understand Data Retention and the Tracking Timestamp

STA retains data indefinitely as a historical record and never deletes data. It uses a start tracking timestamp and stop tracking timestamp to track resources within the system.

When STA begins tracking a resource (library, drive, or media), STA assigns the resource an `STA Start Tracking` timestamp. If you remove the resource from the library environment, STA assigns it an `STA Stop Tracking` timestamp. If you re-add the resource later, the `STA Start Tracking` attribute reflects the original timestamp assigned when STA first began tracking the resource.

Data for removed resources may be hidden from the STA data screens depending on the Data Handling settings for your username. The data has not be removed from the database, only hidden within the STA interface.

Although STA never deletes data, periodically the MySQL Event Scheduler purges processed SNMP records from the database to minimize database growth.

**See Also:**

- [What Happens to Data When Drives and Media Are Removed](#)
- [What Happens to Data When Libraries Are Removed](#)

## How Incomplete Exchanges Affect STA

If STA loses connection to a library during in-process exchanges, you may notice incomplete exchanges on the Exchanges Overview screen. When STA reconnects with the library, it processes all new exchanges normally.

A library connection may be dropped when:

- You manually delete a library connection through the STA user interface.
- You stop STA to perform server maintenance or an STA upgrade.
- There is a power or network outage affecting the STA server.

While the connection is down:

- STA receives no record of exchanges that start and finish completely during the connection downtime. STA does not show these exchanges and does not use them in calculating drive or media health.
- STA receives only partial information for exchanges that either start or finish while the connection is down and does not have enough information to perform a full analysis so exchange status is set to "Unknown". STA does not use these exchanges in calculating drive or media health.

## Why Some Values May Be Dimmed

STA will dim (gray-out) some data elements or resource identifies to reflect a particular status within the library environment.

Elements may be dimmed because:

- The drive or media was removed from the library system.
- The exchange has not yet completed. Once the exchange completes, the identifier is no longer dimmed, and the link is active.
- The alert event types for which a corresponding element does not exist.
- An upgrade is in process.



## What Happens to Data When Drives and Media Are Removed

By default, STA hides data for drives and media that have been removed from your tape library environment. You can change the display preference to show removed resources at any time.

### How Removed Drives/Media Display With "Show Removed Drives" Setting On

- The STA Stop Tracking date indicates the date and time when STA determined the drive or media no longer exists in any of the monitored libraries.
- Some attributes are set to "REMOVED". These include: Library Complex Name, Drive Library Name, Media Library Name, Library Model, Partition Type, Partition Name, Physical Address.

On the Drives Overview screen, you may see:

Drive Serial Number	Drive Tray Serial Number	Library Complex Name	Drive Library Name	STA Stop Tracking
576001000264	Unknown	SL3000_571000200	crimson11	
579004005595	464970G+1608J91	REMOVED	REMOVED	2019-05-09 15:19:41
HU1803169U	Unknown	SL3000_571000200	crimson11	

On the Drives Analysis screen, you may see:

		ACTION	EVALUATE	MONITOR	USE	UNKNOWN	Total
<b>REMOVED</b>	<b>-1 STK</b>	0	0	1	24	16	41
	HP	0	0	0	7	53	60
	IBM	0	0	0	12	81	93
	UNKNOWN	0	0	0	0	60	60
	<b>Drive Manufacturer Total</b>	0	0	1	43	210	254
	<b>Drive Library Number Total</b>	0	0	1	43	210	254
<b>Library Complex Name Total</b>		5	0	7	123	481	616

### Impact of Removed Drives and Media on Calculated Totals

STA provides both current information about your tape library system and historical information collected over time.

- Historical summaries—Rolling 30-day and daily summaries and averages are always calculated based on the number of drives and media in the system during the reporting period. The "show removed drives/media" setting has no effect on these calculations.
- Currently Displayed Values—Totals and aggregations displayed on Overview and Analysis screens are calculated based on the number of records currently displayed. The totals will change based on the "show removed drives/media" settings.

#### See Also:

- To change the removed resources show/hide setting, see [Show or Hide Removed Drives and Media](#).

## What Happens to Data When Libraries Are Removed

If you remove a library from the tape library environment, STA hides any data related to the library and hides resources within the library.

Once you remove a library:

- STA no longer collects data from the library, and you can delete the STA server trap recipient from the library SNMP configuration.
- The Libraries Overview and Complexes Overview screens no longer display the library.
- The Drives and Media screens no longer show drives and media that were in the library.
- The Exchanges Overview and Drive Cleanings Overview screens no longer display exchanges and cleaning activities that have occurred in the library.
- The Drives Messages, Media Messages, and All Messages Overview screens no longer show messages for the library and its drives and media.
- Pending STA media validation requests remain in the validation request queue until you explicitly cancel them. See [Cancel In-Progress or Pending Media Validation Requests](#) for details

Although the library data is removed from the user interface screens, it is never removed from the STA data store. If you later restore a connection to the library, all existing library data is made available on the STA screens again.

## What Happens to Data When an SL8500 Library is Moved to a New Complex

Moving an SL8500 library from one complex to another affects the way data is displayed, sorted, and filtered on all STA screens.

STA rolls up data for the entire library complex, so moving one library to another will affect the data for the complexes. STA uses a unique Library Complex Name to identify each complex (such as SL8500\_1 where 1 is the complex ID). If you move a library from one complex to another, the Library Complex Name associated with it changes. As a result, data for the moved library will be associated with two different library complexes within the historical data of STA.

For example, consider the following scenario:

1. An SL8500 library, "BigLibraryA", is assigned to a complex with two other libraries. Oracle Service assigns ID 1 to the complex.
2. In STA, you create a connection to BigLibraryA. The Library Complex Name for BigLibraryA is SL8500\_1.
3. STA monitors BigLibraryA, and all data for the library is rolled up to Library Complex Name SL8500\_1.
4. After three months, you decide to move BigLibraryA to a new complex. You remove the STA connection to BigLibraryA, and all data for the library is retired, as described in [What Happens to Data When Libraries Are Removed](#).
5. Oracle Service moves BigLibraryA to the new complex, which has complex ID 2.

6. You reestablish the STA connection to BigLibraryA. This has the following effects on new and historical data for the library:
  - Because BigLibraryA is now in complex ID 2, the STA Library Complex Name for the library is SL8500\_2, and all data collected by STA from this point forward is rolled up to that Library Complex Name.
  - All historical data, from the first three-month period, is still rolled up to Library Complex Name SL8500\_1.
  - When you sort or filter data by Library Complex Name, the data for BigLibraryA is associated to two different complexes, depending on the time period.

## How STA Handles "Missing" Media

STA only detects media in a library storage cell or drive at the time of a data collection. STA does not detect media in a robot hand, elevator, PTP, or drive when the library initializes.

STA keeps media that has unexpectedly "disappeared" on the STA screens for a short period of time in anticipation of detecting it. Although this occurrence is rare, it happens most often in an SL8500 complex, where the libraries frequently transfer media from one library to another through pass-thru ports (PTPs).

If you cannot find a volume serial number (VSN or volser) within STA, you should:

1. Verify that you have the correct volser.
2. Filter the Media – Overview screen for that volser, to verify it is really missing.
3. If the volser appears on the Media – Overview screen, check the Start Tracking, End Tracking, and Ejected Date attributes.
4. If the media has an End Tracking date but no Ejected Date, the media may have been removed from the library by an unsupported method, such as through an open library door. On the Dashboard, check the Media Exception Report pane. This report lists media that has left the library through a means other than a CAP, AEM, or mailslot.
5. Initiate a manual data collection on the library in which you expect the media to be located.

### See Also:

- [Manually Collect Library Data](#)

## How STA Handles Duplicate Volume Serial Numbers

In STA, all history for a particular piece of media is tied to its volume serial number (volser). Volsers should be unique across all monitored libraries. Duplicate volsers will result in co-mingling of data for different pieces of media.

Volsers are considered duplicates if the media has the same volser, domain, and media type. Domain identifies the media format, and type identifies the version, as illustrated in the following examples:

- LTO6 – "LTO" is the domain and "6" is the type.
- T1000T1 – "T1000" is the domain and "T1" is the type.

The Duplicate Detected flag appears on the Exchanges Overview screen and indicates that the volser involved in the exchange is a duplicate — the media has the same volser as another media of the same domain and type but with a different media serial number (MSN).

If you find exchanges with this flag, you should investigate and determine whether to assign a different volsr to one of the media, as the data for the two will be co-mingled.



#### Note:

Only some drive types and firmware levels report MSNs; therefore, with some drive types, STA may not receive all the information necessary to detect duplicate volsers.

## How to Map Host and STA Drive Identifiers

STA does not know the host's logical device ID for a drive. To identify a drive, you must manually map the host drive identifiers to the STA identifiers such as drive serial number, World Wide Name (WWN), or physical location.

### Mainframe Identifiers

Mainframe hosts use a four-digit hexadecimal drive ID (0000–FFFF) to identify a drive. To map the host identifiers to the STA identifiers, you can use Oracle's Enterprise Library Software (ELS) `Display DDrives` command on the mainframe host. The `IDEntity` option lists the mainframe hexadecimal ID, serial number, and WWN for each drive. Following is an example of the command output.

### Sample ELS Display DDrives Command Output

```
DISPLAY DRIVES IDENTITY
.SLS4633I Display Drives Command 994
DRIVE LOCATION MODEL WORLD WIDE NAME SERIAL NUMBER
0A10 00:02:01:08 T9840D 50:01:04:F0:00:79:18:CD 5700GU008737
0A11 00:02:01:09 T9840D 50:01:04:F0:00:79:18:C1 5700GU006080
0B04 01:01:01:14 T9940B 50:01:04:F0:00:89:A7:74 479000025047
0B05 01:02:01:14 T9940B 50:01:04:F0:00:89:A7:44 479000026693
0B06 01:02:01:15 T1B35 50:01:04:F0:00:89:A7:68 572004003720
0B07 01:02:01:11 T1B35 50:01:04:F0:00:89:A7:68 572004003720
```

You can issue this command from a variety of locations on the mainframe host, including the operator console or an `SMCUUUI` utility batch job. Optionally, you can save the output of the command to a `.csv` or `.xml` file. See the *ELS Command, Control Statement, and Utility Reference* manual for complete details about usage, syntax, and options.

### Open Systems Identifiers

On open systems hosts (Linux and Solaris), logical device names for tape drives are found in the `/dev/rmt` directory. To map the host logical names to the STA identifiers, you can do a long listing (`ls -l`) of this directory. The command output shows the logical device name and the pointer to the raw device file, which includes the WWN for the drive. Following is an example of the output on Linux; the logical device name and WWN for each drive are highlighted in **bold** type.

### Sample Linux /dev/rmt Directory Listing

```
# ls -l /dev/rmt
lrwxrwxrwx 1 root root 86 Jan 31 16:31 /dev/rmt/0cbn ->../../devices/pci@79,0/pci10de,377@a/pci1077,171@0/fp@0,0/tape@w500104f000b8050e,0:cbn
```

```
lrwxrwxrwx 1 root root 86 Jan 31 16:31 /dev/rmt/1cbn ->../../devices/pci@79,0/
pci10de,377@a/pci1077,171@0/fp@0,0/tape@w500104f000b80511,0:cbn
#
```

## Use STA to Answer Common Tape Environment Questions

Use STA to help answer common questions about the performance of the library system and the state of drives and media.

Typical Question	Task
Which drives and media have had the most errors in the last 30 days? Are there any correlations between the two?	<a href="#">Identify Drives With the Most Errors</a>
Which drives have had the most errors this week? Have their error rates gone up?	<a href="#">Analyze Drive Failure Trends</a>
Which drives have had significantly declining efficiency over time?	<a href="#">Analyze Drive Efficiency</a>
Is the drive that failed twice today the same one that caused problems two months ago?	<a href="#">Analyze Drive Failure Trends</a>
At 9:00 am today, one of our tape jobs experienced an error. Which drive and media were involved? Have they also experienced other errors?	<a href="#">Identify Media and Drives Involved with Job Errors</a>
What critical errors were reported to STA last month? Is the total number trending up, down, or staying stable?	<a href="#">View Trends in Critical Drive and Media Errors</a>
How many libraries, drives, or media are in my tape system environment? How many drives or media of a particular type are in my tape system environment?	<a href="#">Determine Number of Libraries, Drives, or Media in the System</a>
Which are the top three drives in terms of utilization?	<a href="#">Analyze Drive Utilization</a>
Which types of media are in short supply? Do I have an oversupply of any type?	<a href="#">Identify Shortages or Surpluses of Media</a> <a href="#">Analyze Media Utilization</a> <a href="#">Analyze Drive Utilization</a>
Am I likely to need more media, drives, or storage cells next year? If so, how many?	<a href="#">Identify Shortages or Surpluses of Media</a>
Which types of drives or media are used the most in my tape system?	<a href="#">Analyze Drive Utilization</a>
Which library in my tape environment is the busiest? Which is the least busy?	<a href="#">Report Library Activity Levels</a>
Which media are over 90 percent full? How do I generate a list that can be used to create a script to eject them from the library?	<a href="#">Identify Media that is Approaching Capacity</a>
Have all my drives been upgraded to the latest firmware?	<a href="#">Report Drive Firmware Levels</a>

## Best Practices for Investigating Tape Environment Issues

Follow best practices when investigating issues with drives and media.

### Tape alert detail

Tape alert counts for the last exchange are available on the Drive, Media, and Exchange Overview screens. To determine the nature of a tape alert, go to the Exchanges Overview Detail View and review the following sections:

- Exchange Alerts – Severe
- Exchange Alerts – Warning
- Exchange Alerts – Informational

#### Transient media

Media must be in a library storage cell or a drive at the time of a data collection for it to be detected. Media in a transient location is not detected by a data collection and therefore may not appear on the STA screens.

If media is unexpectedly missing, see [How STA Handles "Missing" Media](#) for some troubleshooting steps.

#### Collect drive details

If you suspect a problem with a drive, save details of its recent activity to a PDF file. You can include this file in any inquiries to Oracle Service.

1. On the Drives Overview screen, select the **Drive Serial Number** active link to display the Detail View.
2. Save the resulting display as a PDF file.

#### Export and review recent exchanges for a drive

Exchange detail may provide valuable information about a drive issue.

1. On the Drives Overview screen, select **View**, then **Columns**. then **Show More Columns**.
2. Move `Drive Dismounts (30 days)` into the Visible Columns column, then click **OK**.
3. Select the **Drive Dismounts (30 days)** aggregate count link for the drive. You are taken to the Exchanges Overview screen, filtered to show all the exchanges included in the count.
4. On the Exchanges Overview List View, select **Columns**, then **Show All**.
5. Select **Export**, then **Exchange.xls** to export the data to Excel format.
6. A fixable condition may stand out to you as you scroll through the worksheet columns. For example, you may notice that the "Media Directory Invalid" error appears on multiple media.

#### Create a site-specific STA task *cheat sheet*

For each area of concern or activity you have accomplished in STA, document the quick steps to do it. For example:

- Determining which drives have been cleaned over the last month
- Determining which drives have been idle more than a week
- Determining if some media need to be retired
- How to do year-end planning and new media purchase estimates

Use the procedures in the preceding sections as starting points.

## General Error Trend Analysis


Find trends in errors to better analyze your library system.

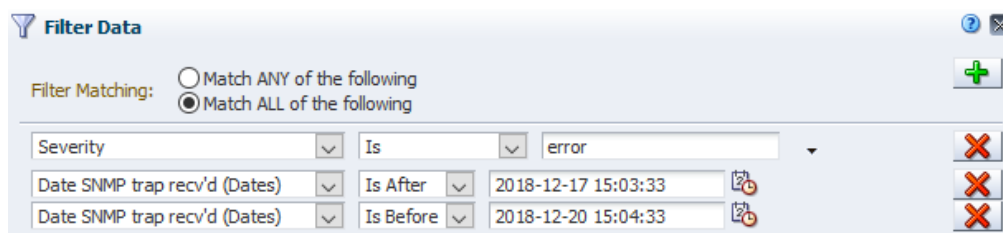
- [View Error Messages From a Specific Time](#)

- [View Trends in Critical Drive and Media Errors](#)
- [View Trends in Exchange Errors](#)

## View Error Messages From a Specific Time

Check for error messages during a specific time period to help you answer questions such as "What critical errors were reported to STA last month?".

1. In the left navigation, expand **Tape System Activity**, select **All Messages Overview**.
2. Add a filter to narrow down the data to just traps that involved errors:
  - a. Click **Filter Data** .
  - b. Select **Match ALL entered criteria**.
  - c. Add the following criteria:
    - Severity | Is | Error
    - Date SNMP trap recv'd (Dates) | Is After | select starting date
    - Date SNMP trap recv'd (Dates) | Is Before | select ending date
  - d. Click **Apply**.




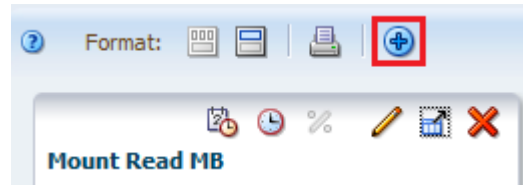
Field	Operator	Value
Severity	Is	error
Date SNMP trap recv'd (Dates)	Is After	2018-12-17 15:03:33
Date SNMP trap recv'd (Dates)	Is Before	2018-12-20 15:04:33

3. Review the errors during the time period.

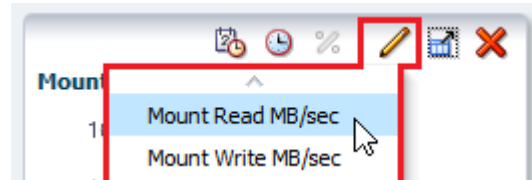
## View Trends in Critical Drive and Media Errors


Drive and media errors result from exchanges. Therefore, use the Exchanges Overview screen for a consolidated view of errors to answer the question "Is the total number of errors trending up, down, or staying stable?".

1. In the left navigation, select **Tape System Activity**, select **Exchanges Overview**.
2. In the **Templates** menu, select the "STA-Exchanges-Alerts-All" (or "STA-Exchanges-Alerts-Errors" for a smaller subset).
3. The template includes several columns that indicate different types of errors. Review the errors listed.
4. If there are enough errors to indicate possible trends, add graphs of interest to the Graph Area:
  - a. [Restore the Graph Area](#).
  - b. Click **Add Graph** . STA displays a new graph with the attribute MB Read.



- c. Within the graph's toolbar, click **Change Graphed Attribute**  and select an attribute of interest.




- d. Repeat to add multiple graphs (such as Write Efficiency, Read Margin, and R/W Rate MB/sec).
- 5. Use an external spreadsheet application to calculate total errors by error type.
  - a. Click the **Export**  and select **Exchange.xls** (see [Export Table Data to a Spreadsheet or Document](#) for more information).
  - b. Save the file to a location on your local computer.
  - c. Use a spreadsheet application to open the file and summarize the data.

## View Trends in Exchange Errors

View exchange errors for the last week to address the questions: "Which drives have had the most errors this week? Have their error rates gone up?".

1. In the left navigation, expand **Tape System Activity**, select **Exchanges Overview**.
2. In the **Templates** menu, apply the "STA-Exchange-Alerts-Errors" template.
3. In the Drive Serial Number column, click **Sort Ascending** or **Sort Descending**.

Exchange Start	Drive Serial Number	Volume Serial Number	Media Manufacturer Serial Number
2020-01-13 09:39:57	1536P40317	SF7148	MG7XWLJUHA
2020-01-13 08:44:10	1536P40317	SF7148	MG7XWLJUHA

4. To focus on specific errors, move columns around and remove empty columns (see [Reorder Columns](#) and [Hide and Reveal Columns](#)).
5. Add a filter to display just this week's data:
  - a. Click **Filter Data** .
  - b. In the Filter Matching field, select **Match ALL entered criteria**.



- c. Add the criteria: **Exchange Start (No. Days) |Less than # days ago | 7**
- d. Click **Apply**.

The screenshot shows a 'Filter Data' dialog box with the following configuration:

- Filter Matching:**  Match ALL of the following
- Criteria 1: Exchange Tape Alerts - Severe, Greater Than, 0
- Criteria 2: Exchange Tape Alerts - Warning, Greater Than, 0
- Criteria 3: Exchange Start (No. Days), Less than # days ago, 7 (highlighted with a red box)

## Library System Analysis

Analyze resource errors, trends, and identify total types of resources within your system.



- [Identify Media and Drives Involved with Job Errors](#)
- [Display Correlations Between the Drives and Media with the Most Errors](#)
- [Determine Number of Libraries, Drives, or Media in the System](#)
- [Report Library Activity Levels](#)

### Identify Media and Drives Involved with Job Errors

Add a filter to the Exchanges Overview screen to identify drives and media involved with an error.

This procedure can help address the questions such as, "At 9:00 am today, one of our tape jobs experienced an error. Which drive and media were involved? Have they also experienced other errors?"

In cases where each "job" is an independent exchange (that is, mount, read/write data, dismount), you can use this method to access information about tape job failures.

1. In the left navigation, expand **Tape System Activity**, select **Exchanges Overview**.
2. To view more of the table, click **Collapse Pane**  in the middle of the screen (see [Resize or Collapse Areas of the Screen](#)).
3. Add a filter to narrow down the data to just exchanges that experienced errors:
  - a. Click **Filter Data** .
  - b. In the Filter Matching field, select **Match ANY entered criteria**.
  - c. Add selection criteria:
    - Drive Exchange Status, Contains, ERROR
    - Media Exchange Status, Contains, ERROR

Entries are not case-sensitive, so "ERROR" will match "error" or "Error".
  - d. Click **Apply**.

**Filter Data**

Filter Matching:  Match ANY of the following  
 Match ALL of the following

Drive Exchange Status	Contains	ERROR	<input type="checkbox"/>
Media Exchange Status	Contains	ERROR	<input type="checkbox"/>

4. Scroll to the exchanges that occurred during the time in questions, and review the information in the Drive Exchange Status, Media Exchange Status, and Exchange FSC columns for details about the errors.

Drive Model	Media Type	Drive Exchange Status	Media Exchange Status	Exchange FSC
T10000C	T10000T1	DRIVE_ERROR	MEDIA_ERROR	
T10000A	T10000T1	NON_DRV_ERRO	NON_DRV_ERROR	3613
T10000B	T10000T1	DRIVE_ERROR	MEDIA_ERROR	

**Note:**

The Drive Health Indicator and Media Health Indicator columns may indicate Use even after an error. This is because the values of these attributes are aggregated over time. The specific values depend on the frequency and severity of errors, and whether there have been subsequent exchanges with no problems. Recent exchanges with no problems move the aggregated value toward a "Use" status.

5. Optionally, to display detail about a drive or media involved in an error, select the text link in either the Drive Serial Number or Volume Serial Number column.


Drive Serial Number	Volume Serial Number
576004000904	<a href="#">UG0004</a>
531004002822	UG0005

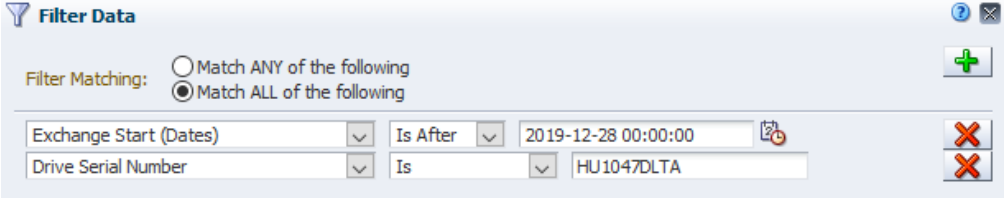
## Display Correlations Between the Drives and Media with the Most Errors

Determine if there is a correlation between the drives and media with the most errors. This may help identify problematic drives and media.

Identify drives and media with the most errors to address the questions, "Which drives and media have had the most errors in the last 30 days? Are there any correlations between the two?"



1. In the left navigation, expand **Tape System Activity**, select **Exchanges Overview**.
2. Filter the data to display only those exchanges within the last 30 days and that involve the drive with the most errors (identified in [Identify Drives With the Most Errors](#)).

- a. Click **Filter Data** .
- b. Select **Match ALL** entered criteria.
- c. Add the filter criteria:
  - Exchange Start (Dates), Is After, a date 30 days ago
  - Drive Serial Number, Is, serial number of the drive with the most errors
- d. Click **Apply**.

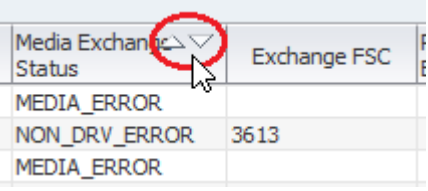


**Filter Data**


Filter Matching:  Match ANY of the following  
 Match ALL of the following

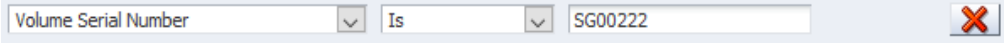
Exchange Start (Dates)	Is After	2019-12-28 00:00:00	
Drive Serial Number	Is	HU1047DLTA	


3. To focus on the media involved in the errors, sort the table by a related column (such as Media Exchange Status, Exchange FSC, or Media Health Indicator).



Media Exchange Status	Exchange FSC
MEDIA_ERROR	
NON_DRV_ERROR	3613
MEDIA_ERROR	

4. Look at the Volume Serial Number column to see if there are any correlations between drive errors and specific media.
5. If you do find a potential correlation, filter the data further to display just the exchanges that involve both the faulty drive and the suspect media.
  - a. Click **Filter Data** .
  - b. Leave the current criteria rows as is, but add:
    - Volume Serial Number | Is | volser of the suspect media



Volume Serial Number	Is	SG00222	
----------------------	----	---------	---

- c. Click **Apply**.

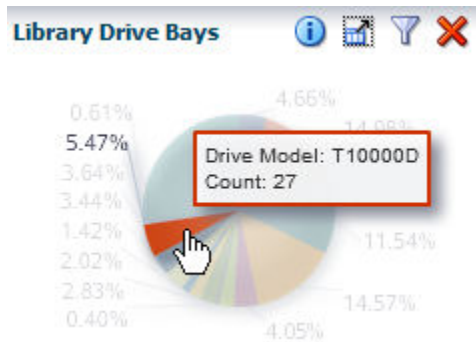
## Determine Number of Libraries, Drives, or Media in the System

Use the Dashboard, Overview, or Analysis screens to determine how many libraries, drives, or media are in your tape system environment.

### Hover Over Dashboard Items to View Resource Totals


1. In the left navigation, expand **Home**, then select **Dashboard**.
2. Use the Library Status, Library Media Slots, and Library Drive Bays to view total for various types of resources.

3. Hover over an item to get a count for the particular resource.




4. Optionally, click a section of the chart to link to the Overview screen for that resource.

#### Use Record Totals within Overview Tables to Get Total Resources

1. In the left navigation, expand **Tape System Hardware**, select an overview (such as Drives Overview).
2. Click Reset Filter  to removal all filtering and view totals for the entire system.
3. In the lower-right of the table, the number of records indicates the total number of resources (such as drives).

Displaying 362 record(s)

#### Use the Analysis Screen to View an Aggregated Total

1. In the left navigation, expand **Tape System Hardware**, select an analysis screen (such as Drives Analysis).
2. Click Reset Filter  to removal all filtering and view totals for the entire system.
3. The value in the bottom-right of the pivot table shows the total for the system.

		ACTION	EVALUATE	MONITOR	USE	UNKNOWN	Total
	HP	0	0	0	0	39	39
	IBM	0	0	0	0	14	14
	<b>Drive Manufacturer Total</b>	0	0	0	0	54	54
	<b>Drive Library Number Total</b>	0	0	0	15	144	159
<b>Library Complex Name Total</b>		5	0	6	80	271	362

## Report Library Activity Levels



Identify which library in your environment is the busiest. This may be helpful to determine how to reallocate resources.

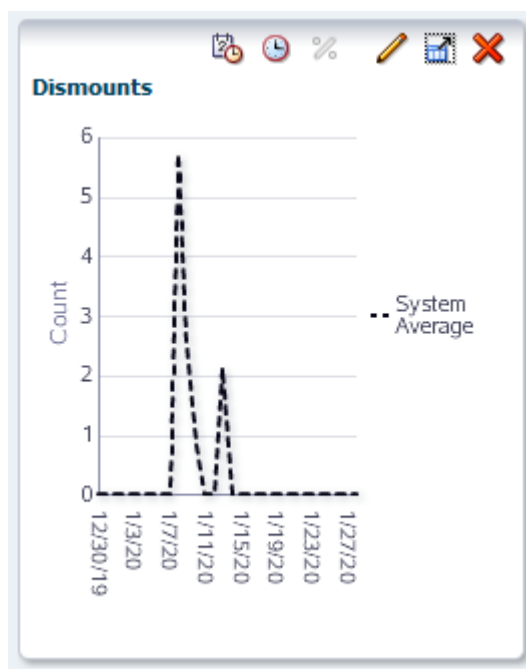
This procedure addresses the questions, "Which library in my tape environment is the busiest? Which is the least busy?" The definition of *busy* varies by site; common definitions include the number of exchanges, mounts, or dismounts. This procedure


uses the number of mounts. In addition, it provides instructions for graphing the data so you can compare the libraries to one another and to the system average.

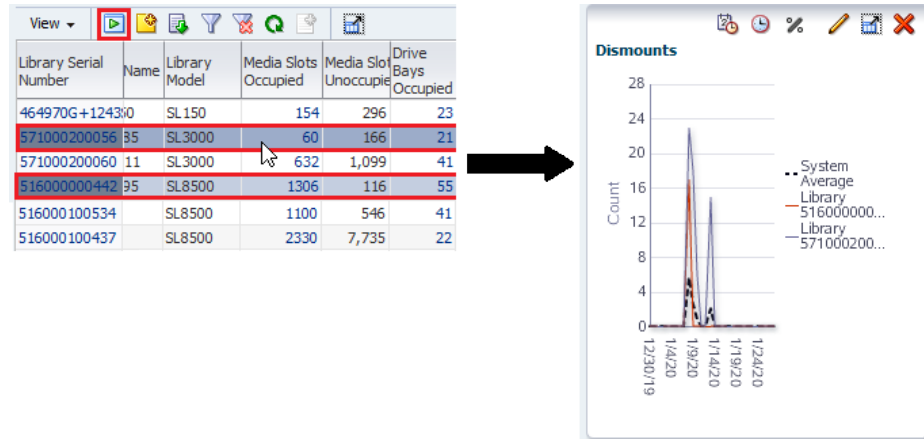
1. In the left navigation, expand **Tape System Hardware**, select **Libraries Overview**.
2. In the **Templates** menu, select "STA-Lib-Utilization".
3. Click **Sort Ascending** or **Sort Descending** for one of the following columns: Mounts (30 Days), CAP Enters (30 Days), CAP Ejects (30 Days), Occupied Storage Cells, or MB R/W (30 Days).

% Drive Utilization (30 Days)	MB R/W (30 Days)
3.26	13,403.69
0.00	0.00

4. Add a graph pane showing dismounts.
  - a. Click **Add Graph** .
  - b. Within the graph's toolbar, click **Change Graphed Attribute**  and select **Dismounts**.
  - c. The graph is updated to display the system average for dismount data.



5. Add selected libraries to the graph to compare to the system average.
  - a. In the table, select the libraries you want to add to the graphs.
  - b. Click the **Apply Selection** .



## Drive Analysis

Identify problematic drives, analyze error and efficiency trends, and check drive firmware levels.

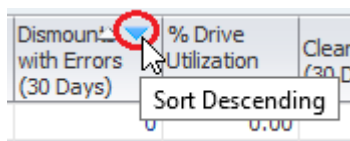
- Identify Drives With the Most Errors
- Analyze Drive Failure Trends
- Identify Drives that Had a Health State Change
- Analyze Drive Efficiency
- Analyze Drive Utilization
- Report Drive Firmware Levels

### Identify Drives With the Most Errors

A high number of errors may indicate a problematic drive.

Identify the drives that have had the most errors recently to see if their error rates have changed to answer questions such as, "Which drives have had the most errors this week? Have their error rates gone up?"

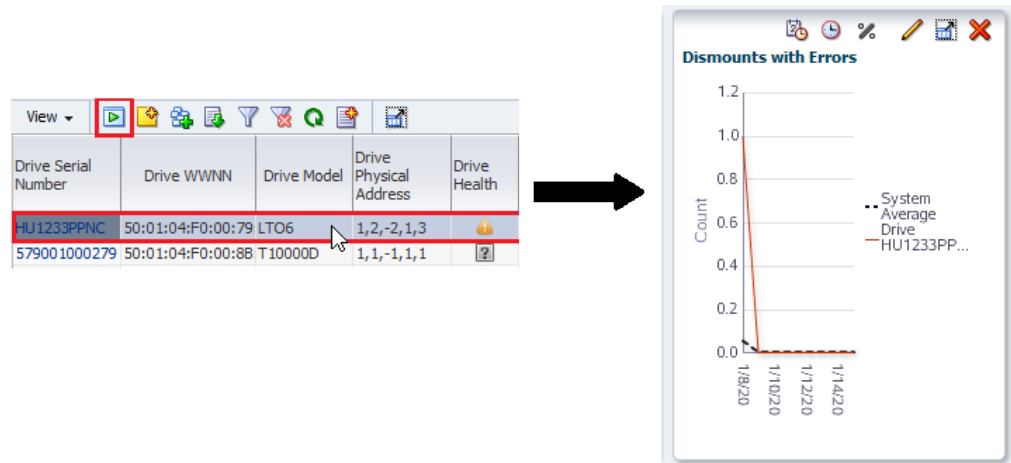
1. In the left navigation, expand **Tape System Hardware**, then select **Drives Overview**.
2. In the **Templates** drop-down, select "STA-Drive-Health".
3. In the Dismounts with Errors (30 Days) column, click the **Sort Descending** arrow. The drives with the most errors are brought to the top of the list.




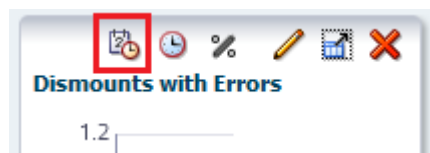
4. Add drives to the graphs to compare their attributes against the system average.
  - a. Select the drives you want to add to the graphs (shift- or ctrl-click to select multiples).

- b. Click **Apply Selection** .

The graphs are updated with the drive data. In the example below, one of the drives shows a high level of errors when compared with the system average.



5. Narrow down the date range on the Drive Errors graph pane.
- a. Click **Choose Date Range**  on the graph's toolbar.





- b. Complete the Choose Date Range dialog box as follows:
- Select **Time Range**.
  - In the **Starting Date** and **Ending Date** fields, enter the start and end dates of the current week.
- c. Click **OK**.

The graph will update with the new time period. Variations in the graph lines should show increases and decreases in error rates during the week.

## Analyze Drive Failure Trends

Look at drive failure trends to addresses questions such as, "Is the drive that failed twice today the same one that caused problems two months ago?"

1. In the left navigation, expand **Tape System Activity**, select **Exchanges Overview**.
2. To view more of the table, click **Collapse Pane**  in the middle of the screen (see [Resize or Collapse Areas of the Screen](#)).
3. Add a filter to narrow down the data to exchanges from four and five months ago involving the suspect drive.
  - a. Click **Filter Data** .

- b. Select **Match ALL entered criteria**.
- c. Add the following selection criteria:
  - Exchange Start (Dates), Is After, a date three months ago
  - Exchange End (Dates), Is Before, a date two months ago
  - Drive Serial Number, Is, the serial number of the drive with errors

If your site has exchanges that last more than a day, you may need to adjust your date settings to encompass complete exchanges involving the drive in question.

- d. Click **Apply**.

4. Visually scan the data to determine whether the drive experienced exchanges with errors during this period.

## Identify Drives that Had a Health State Change

Get a snapshot of drives whose health state have changed.

1. In the left navigation, expand **Tape System Hardware**, select **Drives Messages**.
2. In the Device Serial Number column, click the **Sort Ascending** or **Sort Descending** arrow. Errors and statuses are grouped by drive.

Device Serial Number	Device State
MXP1124CFM	DEGRADED
MXP1124CFM	NORMAL
MXP1124CFM	
MXP1124CFM	DEGRADED

3. Visually scan the list for changes in the device state of individual drives.




## Analyze Drive Efficiency

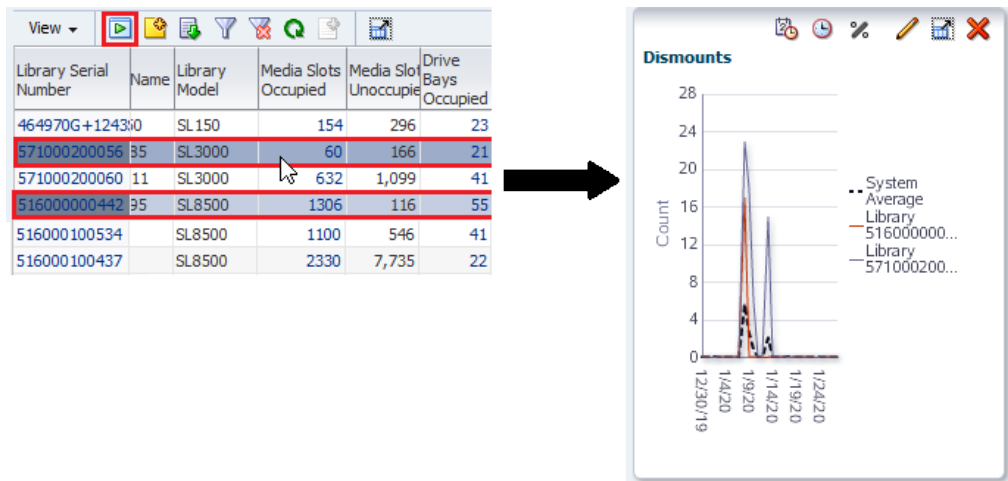
STA collects read and write rates per exchange and then summarizes them into daily and 30-day time periods to help answer the question, "Which drives have had significantly change in efficiency over time?"

1. In the left navigation, expand **Tape System Hardware**, select **Drives Overview**.
2. In the **Templates** menu, apply the "STA-Drive-Performance-30-Days".

This does not include any graph panes. Some values may be null if STA has not been monitoring a drive long enough to gather data.



3. Add graphs to see changes in efficiency over time.
  - a. Restore the Graph Area.
  - b. Click **Add Graph** . STA displays a new graph with the attribute MB Read.
  - c. Within the graph's toolbar, click **Change Graphed Attribute**  and select an attribute of interest (such as Avg Mount Read MB/sec).
  - d. Repeat to add multiple graphs.
4. Add specific drives to the graphs to compare them against the system average.
  - a. Select specific drives in the table (shift- or ctrl-click to select multiples).
  - b. Click **Apply Selection** . The graphs update with the drive specific data.




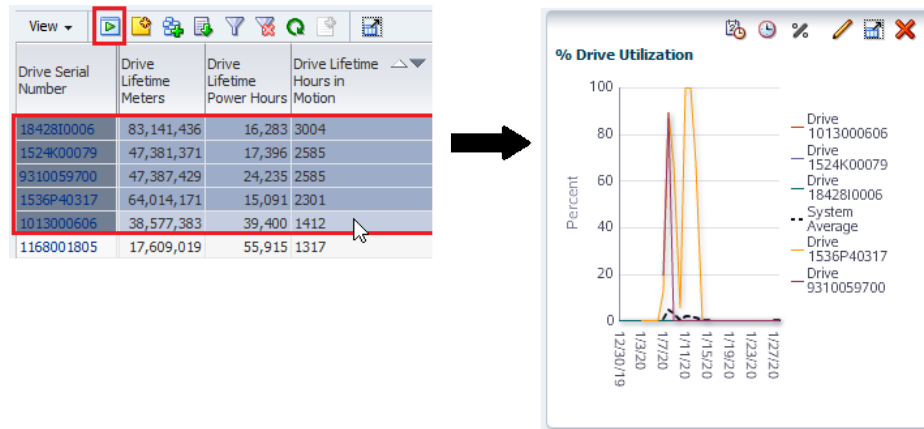
## Analyze Drive Utilization


Analyze drive utilization to address the question, "Which drives are used the most?" Utilization can be defined in several ways, including lifetime hours in use, amount of data passed, and total number of mounts.

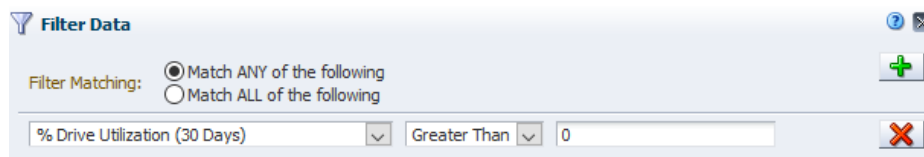
1. In the left navigation, select **Tape System Hardware**, select **Drives Overview**.
2. In the **Templates** menu, select "STA-Drive-Utilization".
3. Use either of these columns to analyze drive use:
  - Drive Lifetime Hours in Motion (enterprise drives only)
  - % Drive Utilization (30 Days)
4. In the corresponding column, click the **Sort Descending** arrow. The most used drives are brought to the top of the table.

Drive Lifetime Hours in Motion	Time Spent Reading	Time Spent Writing
	Sort Descending	

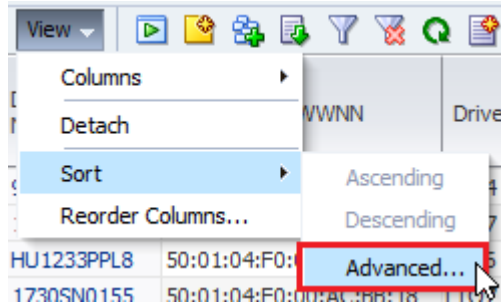
5. Add the top five drives to the graph to compare their attribute values against the system average.
  - a. In the table, select the top five drives.
  - b. Click the **Apply Selection**  to add the drives to the graphs.



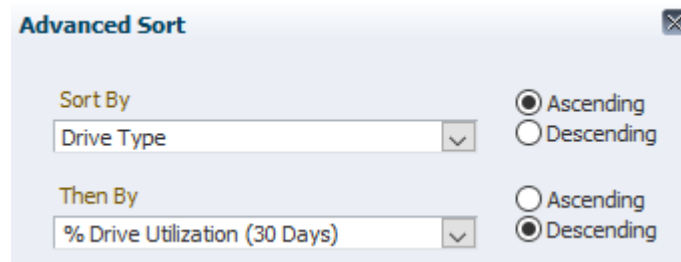
6. Filter the data to hide drives for which STA has no utilization data.
  - a. Click **Filter Data** .
  - b. Add one of the following criteria that represents a utilization measure of interest to you.
    - To identify drives with the highest utilization rates, use: % Utilization (30 Days) | Greater Than | 0.
    - To identify drives that have recorded the most new data, use: MB Write (30 Days) or MB Received (30 Days) | Greater Than | 0.
    - To identify drives that have passed the most data at the drive head, use: MB R/W (30 Days) | Greater Than | 0.
    - For drives that have been in the library for their entire periods of use: Drive Lifetime Loads or Drive Lifetime Hours in Motion | Greater Than | 0.
  - c. Click **Apply**.




7. Sort the data by drive type and then utilization. From the **View** drop-down, select **Sort**, and then **Advanced...**




- a. In the "Sort By" field, select **Drive Type**.
- b. In the "Then By" field, select the attribute that you used in Step b above, and **Descending**.
- c. Click **OK**.

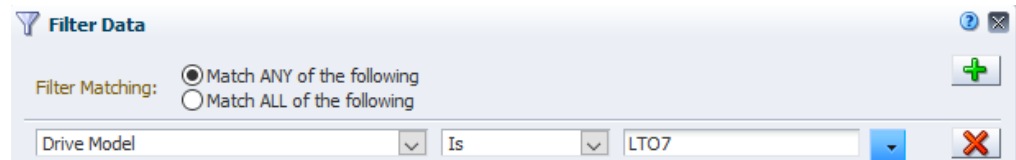



8. Use an external spreadsheet application to calculate the total capacity and space available for each media type.
  - a. Click **Export**  and select **Drives.xls** (see [Export Table Data to a Spreadsheet or Document](#) for more information).
  - b. Save the file to a location on your local computer.
  - c. Open the file in a spreadsheet application and summarize the data. For example, you may want to calculate totals, percentages used, or averages by media type.

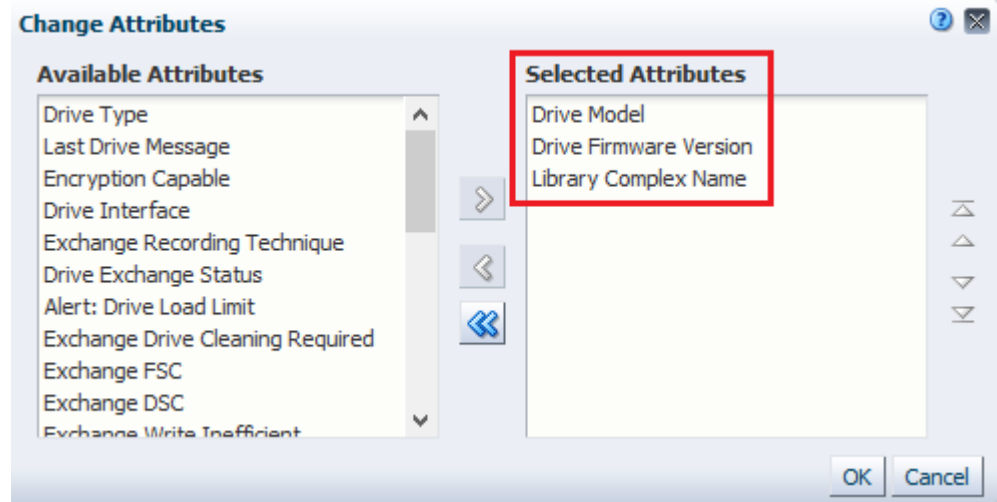
## Report Drive Firmware Levels

Identify drive firmware levels to address the question, "Have all my drives been upgraded to the latest firmware?"

1. In the left navigation, expand **Tape System Hardware**, select **Drives Analysis**.
2. Filter the table to display firmware levels for a specific drive model.
  - a. Click **Filter Data** .
  - b. Add the criteria: Drive Model | Is | select the drive model
  - c. Click **Apply**.



3. Reorganize the pivot table to aggregate firmware levels by drive model.
  - a. Above the table, click **Change Attribute** .
  - b. Rearrange the attributes so the Selected Attributes list is as follows:
    - Drive Model
    - Drive Firmware Version
    - Library Complex Name
  - c. Click **OK**.



4. To display a detailed listing of any of the subtotals, click the text link in a cell.

		SL8500_14	SL8500_2	SL8500_51	SL8500_8	Total
LTO7	F980	0	0	0	0	2
	FA11	0	0	0	0	1
	FA14	2	0	0	0	4
	G9Q2	0	0	0	0	19
	H5B4	0	0	0	0	0
	H9E2	0	0	0	4	7

You are taken to the Drives – Overview screen, which displays additional detail for the drives included in the selected subtotal.

Drive Serial Number	Drive WWNN	Drive Model
<a href="#">10WT005546</a>	50:01:04:F0:00:A0:E5:20	LTO7
<a href="#">10WT010279</a>	50:01:04:F0:00:A0:E5:23	LTO7
<a href="#">10WT010272</a>	50:01:04:F0:00:A0:E5:02	LTO7

## Media Analysis

Identify problematic media, analyze utilization, identify older media, and identify media approaching capacity.

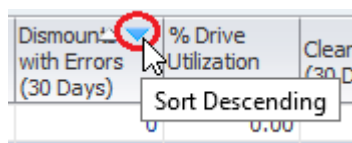
- Identify Media With the Most Errors
- Identify Failed Mount Exchanges
- Identify Shortages or Surpluses of Media
- Analyze Media Utilization
- Identify Older Media
- Identify Media that is Approaching Capacity


### Identify Media With the Most Errors

A high number of errors may indicate problematic media.

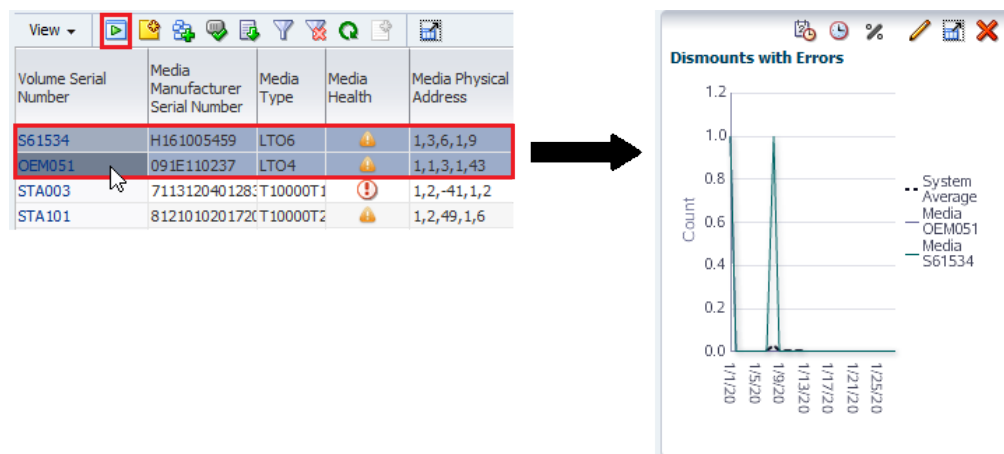
1. In the left navigation, expand **Tape System Hardware**, then select **Media Overview**.
2. In the **Templates** drop-down menu, apply the "STA-Media-Health" template.
3. In the Dismounts With Errors (30 Days) column, click **Sort Descending** ▼.

The media with the most errors are brought to the top of the list.



4. Add selected media to the graphs to compare their attribute values against the system average.
  - a. Select the media you want to add to the graphs.
  - b. Click **Apply Selection** .


The graphs are updated with the media data. In the example below, both media show high numbers of errors when compared with the system average.

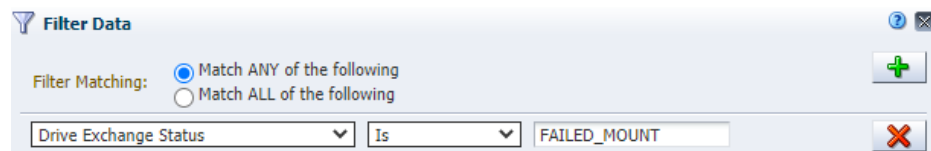


## Identify Failed Mount Exchanges

Use the Exchanges Overview and SNMP messages to identify failed mount exchanges. A failed mount could indicate an issue with the media or drive.

Use a filter on the Exchanges Overview page to identify failed mounts. STA identifies the first failed mount exchange and filters out any repeat mount failures to prevent reporting multiple repeat errors caused by clients retrying. As a result, you must look at the SNMP messages to identify repeat mount failures.

1. In the left navigation, expand **Tape System Activity**, select **Exchanges Overview**.
2. Add a filter to identify failed mount exchanges.
  - a. Click **Filter Data** .
  - b. Add the following selection criteria: Drive Exchange Status, Is, FAILED\_MOUNT
  - c. Click **Apply**.




**Filter Data** ? ✕


Filter Matching:  Match ANY of the following +  
 Match ALL of the following

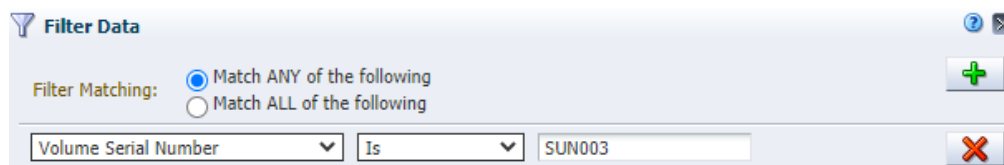
Drive Exchange Status v Is v FAILED\_MOUNT ✕

3. Note the volume serial number for the media that had a failed mount exchange.



Exchange Start	Drive Serial Number	Drive Model	Drive Health	Volume Serial Number	Media Type	Media Health	Drive Exchange Status	Media Exchange Status
2021-04-08 19:48:26	10WT005568	LTO7	<span>?</span>	SUN003	LT05	<span>?</span>	FAILED_MOUNT	FAILED_MOUNT
2021-04-08 00:28:33	1013001473	LTO7	<span>?</span>	SUN004	LT05	<span>?</span>	FAILED_MOUNT	FAILED_MOUNT
2021-04-08 00:21:52	1013001473	LTO7	<span>?</span>	SUN003	LT05	<span>?</span>	FAILED_MOUNT	FAILED_MOUNT

4. Navigate to the **All Messages - Overview** page.
5. From the **Templates** drop-down, select **STA-Messages-All**.
6. Use the volume serial number to filter the SNMP messages and identify multiple failed mount exchanges.
  - a. Click **Filter Data** .
  - b. Add the following selection criteria: Volume Serial Number, Is, *volser of problematic media*
  - c. Click **Apply**.




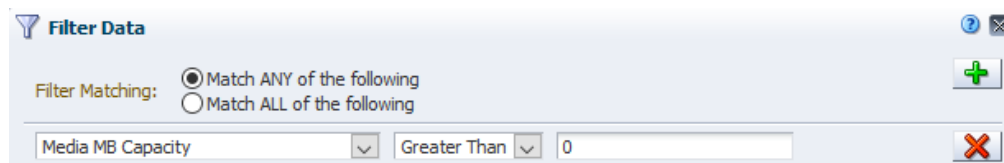
7. Look through the results for "Drive load failed due to media error" to identify the number of times the mount failed.

## Identify Shortages or Surpluses of Media

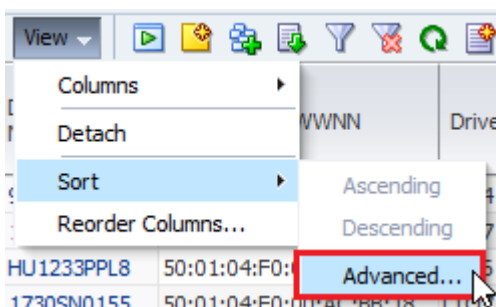
Use media utilization data to address the questions, "Which type of media am I the shortest on? Do I have an oversupply of any type?"

The definition of media available for writing varies by site. For example, a site that does not reuse media may simply compare total versus available capacity for each type of media; another site that does reuse media may look at some media life measure instead. Both of these measures, and others, are available within STA. This procedure uses total versus available capacity.

1. In the left navigation, expand **Tape System Hardware**, select **Media Overview**.
2. In the **Templates** menu, select "STA-Media-Utilization".
3. Note the total number of records in the table (displayed in the lower-right corner of the table).
4. Filter out media for which capacity or availability information is not available.
  - a. Click **Filter Data** .
  - b. Add the criteria: Media MB Capacity | Greater Than | 0
  - c. Click **Apply**.



5. Note the number of records eliminated (by comparing the total number of records displayed in the lower right corner of the table), since it reflects the level of uncertainty.
6. Sort the table to display the capacity and space available for each piece of media. From the **View** drop-down, then select **Sort**, then select **Advanced...**

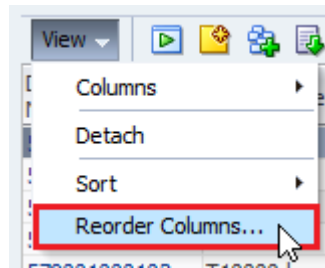


- a. In the Sort By menu, select **Media Type, Ascending**.
- b. In the first Then By menu, select **Media MB Avail Pre, Ascending**
- c. In the next Then By menu, select **Media MB Avail Post, Ascending**

LTO drives report the Media MB Avail Pre attribute, and StorageTek enterprise drives report Media MB Avail Post. Including both attributes in the sort criteria ensures you will include all media types.

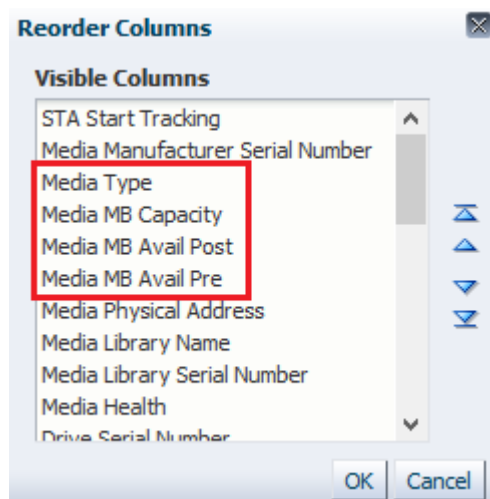
The image shows a configuration window for sorting data. It has three sections, each with a dropdown menu and two radio buttons for 'Ascending' and 'Descending'.  
 - Section 1: 'Sort By' dropdown is 'Media Type', 'Ascending' radio button is selected.  
 - Section 2: 'Then By' dropdown is 'Media MB Avail Pre', 'Ascending' radio button is selected.  
 - Section 3: 'Then By' dropdown is 'Media MB Avail Post', 'Ascending' radio button is selected.


- d. Click **OK**.
7. Reorder the columns to better view the capacity data together on the screen.
    - a. From the **View** drop-down, select **Reorder Columns...**



- b. Arrange the following attributes so they are listed together.
  - Media Type
  - Media MB Capacity
  - Media MB Avail Pre
  - Media MB Avail Post
- c. Click **OK**.






8. Use an external spreadsheet application to calculate the total capacity and space available for each media type.
  - a. Click **Export**  and select **Media.xls** (see [Export Table Data to a Spreadsheet or Document](#) for more information).
  - b. Save the file to a location on your local computer.
  - c. Open the file in a spreadsheet application and summarize the data. For example, you may want to calculate totals, percentages used, or averages by media type.

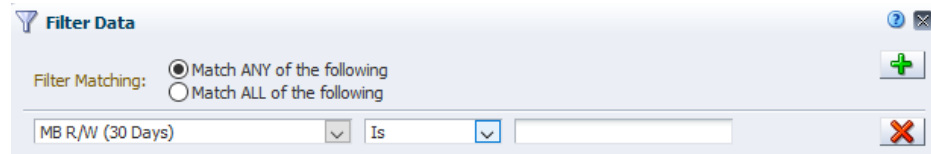
## Analyze Media Utilization

Look at media utilization to addresses the question, "Which types of drives or media are used the most in my tape system?"

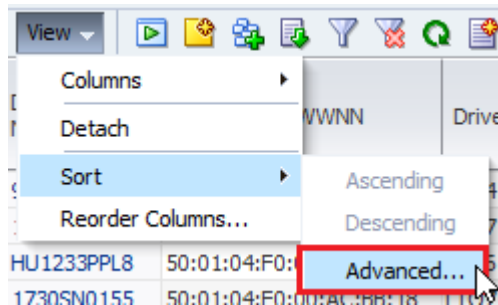
The drives and media that make up the majority of the system are not necessarily subject to the most use. Utilization is affected by your client configuration and the types of drives and media requested by these clients. This procedure addresses some of the most common ways of defining *most used*.

1. In the left navigation, expand **Tape System Hardware**, select **Media Overview**.
2. In the **Templates** menu, select "STA-Media-Utilization".
3. Filter out media for which STA has no utilization data.
  - a. Click **Filter Data** .
  - b. Add one of the following criteria that represents the utilization measure of interest to you.
    - To identify media with the greatest amount of movement, use: Time spent reading or writing | Greater Than | 0.
    - To identify media below a specific threshold of available space, use: Media MB Avail Pre/Post | Greater Than | 0.
    - To identify media with the highest number of mounts and dismounts, use: Media Dismounts (30 days) | Greater Than | 0.
    - To identify media with the greatest amount of data read or written, use: MB R/W (30 days) | Greater Than | 0.

- c. Click **Apply**.




4. Sort multiple columns to group the records by media type and then utilization. From the **View** drop-down, then select **Sort**, then **Advanced...**



- a. In the Sort By field, select **Media Type, Ascending**.
- b. In the Then By field, select the attribute that you used in step above, and **Descending**.

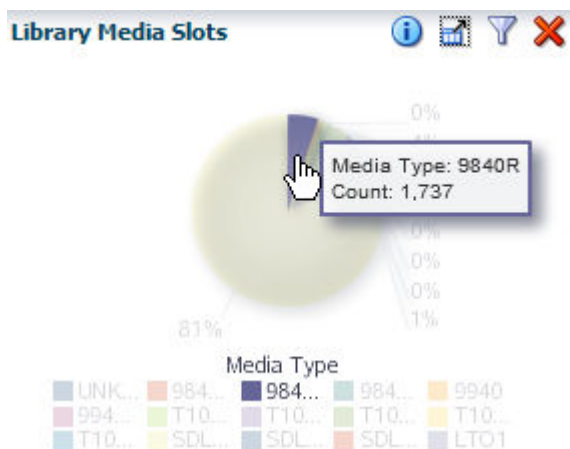


- c. Click **OK**.
5. Use an external spreadsheet application to calculate the total capacity and space available for each media type.
  - a. Click **Export**  and select **Media.xls** (see [Export Table Data to a Spreadsheet or Document](#) for more information).
  - b. Save the file to a location on your local computer.
  - c. Open the file in a spreadsheet application and summarize the data.

## Identify Media for a Migration

If your site is migrating off one type of media and you need to replace it with another, use STA to identify older media.

1. In the left navigation, expand **Home**, then select **Dashboard**.
2. In the Library Media Slots graph, hover over areas of the pie chart to display detail for a type of media.



3. Click a section of the pie chart to go to the Media – Overview screen filtered for that type of media.
4. Organize the media records by remaining capacity, physical location, or other attributes pertinent to the migration process.

## Identify Older Media

Identify existing media that is aging or showing errors beyond your site-defined reasonable threshold.

1. In the left navigation, expand **Tape System Hardware**, select **Media Overview**.
2. In the **Templates** menu, select "STA-Media-Expired".

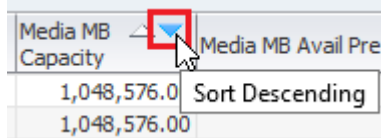
This template shows media that have expired and should be retired from service.

Volume Serial Number	Media Library Serial Number	Cleaning Media	Alert: Media Clean Expired	Media Suspicion Level	Media Health	Media Life Indicator	Drive Serial Number	Alert: Media Load Limit
CLNU22	571000200060			100.00	⊗	⊗	1210140782	✓
CLNU44	571000200060	✓		100.00	⊗	⊗	HU19477NHO	


## Identify Media that is Approaching Capacity

Identify media approaching capacity to address questions such as, "Which media are over 90 percent full? Which media should I eject from the library?"

1. In the left navigation, expand **Tape System Hardware**, select **Media Overview**.
2. In the **Templates** menu, select "STA-Media-Utilization".
3. In the Media MB Capacity column, click **Sort Descending**.



Media MB Capacity	Media MB Avail Pre
1,048,576.0	Sort Descending
1,048,576.00	

4. Use an external spreadsheet application to calculate percent of capacity used.
  - a. Click the **Export**  and select **Media.xls** (see [Export Table Data to a Spreadsheet or Document](#) for more information).
  - b. Save the file to a location on your local computer.
  - c. Use a spreadsheet application to open the file and summarize the data.

# A

## Quick Start Guide

Jump-start your knowledge of STA with a step-by-step tutorial through the interface.

This guide will step you through a series of tasks, providing samples of commonly used screens and explaining key features of the interface.

- [Log in to STA](#)
- [Apply a Dashboard Template](#)
- [Explore the Dashboard](#)
- [Navigate Using the Left Menu](#)
- [Navigate Using Text Links](#)
- [Understand the General Screen Layout](#)
- [Display Media Exchanges for a Library](#)
- [Reset a Screen Filter](#)
- [Display Full Details for Selected Exchanges](#)
- [Display Aggregated Drive Data](#)
- [Export Data to a Spreadsheet](#)
- [Access the Online Help](#)
- [Log Out](#)

## Log in to STA

Sign in to STA to access the user interface.

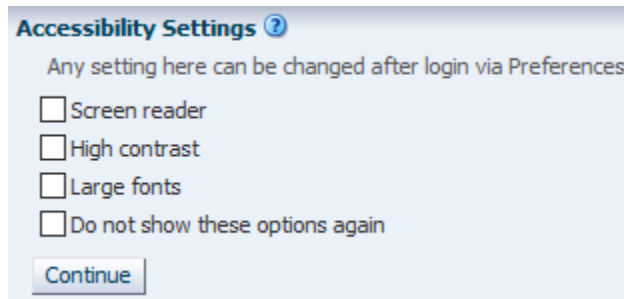


### Note:

When using STA, do not navigate with the browser's **Forward** or **Back** buttons. The data may become out of sync with the STA server.

1. Obtain the following from your STA administrator:
  - URL of the STA application
  - Your STA username and password
2. Using a supported browser, enter the URL and port number given to you by your STA administrator (typically something like `http://hostname:7021/STA`).
3. On the login screen, enter your STA username and password. Click **Login**.
4. Depending on the preference settings for your username, the Accessibility Settings dialog may appear. STA offers a variety of accessibility features for users with low vision,

blindness, color blindness, or other visual impairments. See [Set Accessibility Options](#) for more information.



For now, click **Continue**.

- The Dashboard is always the first screen that STA displays after you log in. You will see data specific to your company, but the screen layout should be similar to the following example.

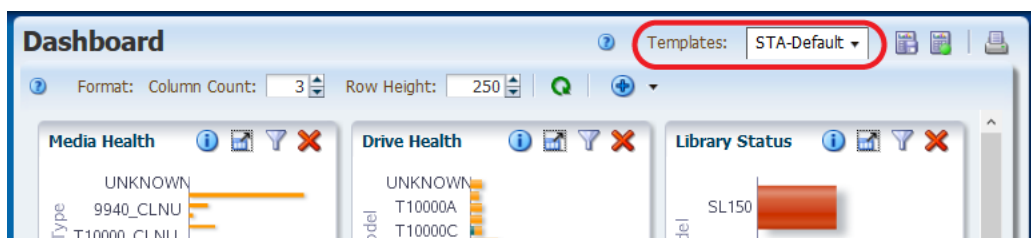


## Apply a Dashboard Template

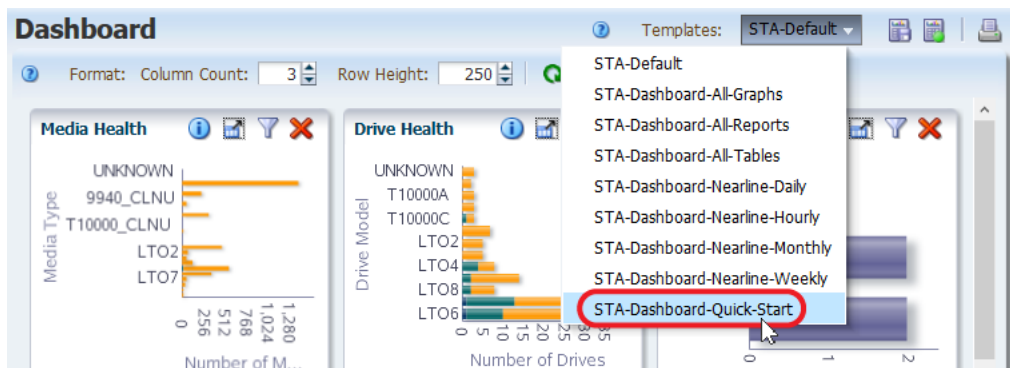
You can control the appearance of most STA screens, including the Dashboard, by applying a template. Templates define a variety of screen characteristics, including graph layouts, table layouts, and filter criteria.

In the example below, the initially applied template is "STA-Default," which is the default dashboard template delivered with the STA application. If your username has a different template assigned as the default, then a different template will display initially. STA comes with several predefined templates that provide you with frequently used information about library components and activity. See [Descriptions of Predefined Templates](#).

1. Determine the currently applied template by looking at the **Templates** menu.



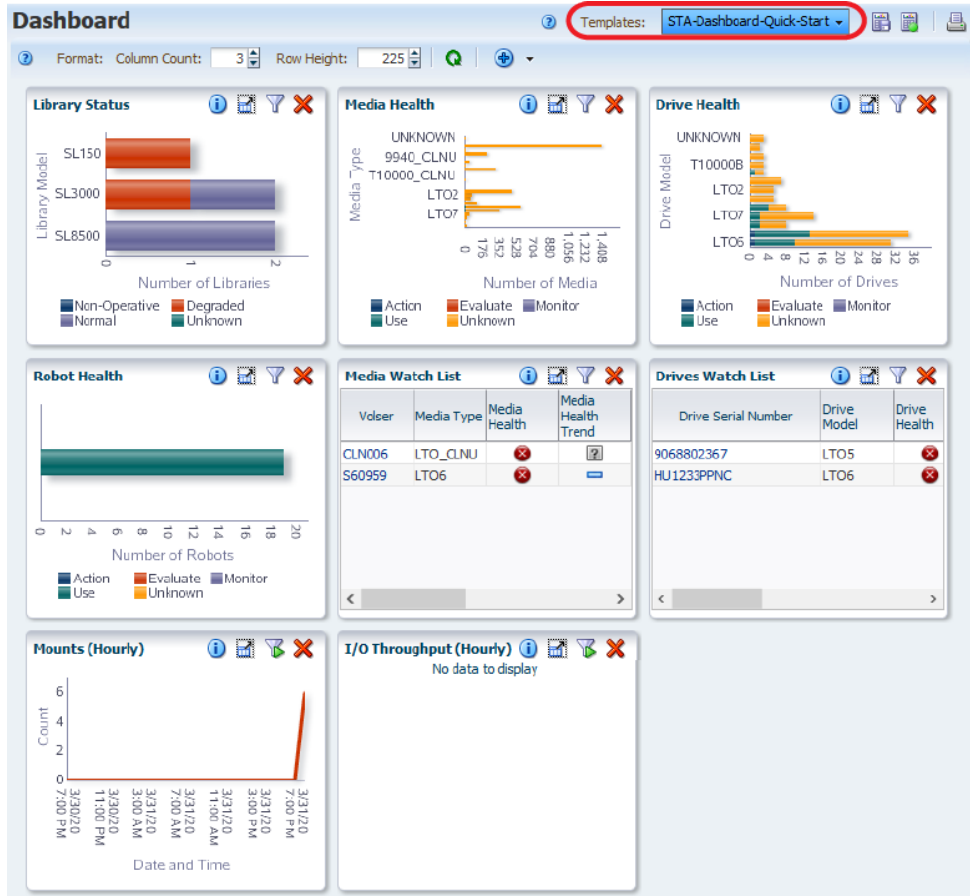
2. Apply a new template by selecting one from the Templates drop-down menu, such as **STA-Dashboard-Quick-Start**.



3. The Dashboard will update with a new template layout.

The STA-Dashboard-Quick-Start template provides you with a high-level view of your tape library system. It includes:

- Panes that summarize the current condition of your library system components (Library Status, Media Health, Drive Health, and Robot Health panes).
- Panes that alert you to drives and media that may need attention (Media Watch List and Drives Watch List panes)
- Panes that show line graphs of library activity over the last few hours (Mounts and I/O Throughput panes).



## Explore the Dashboard

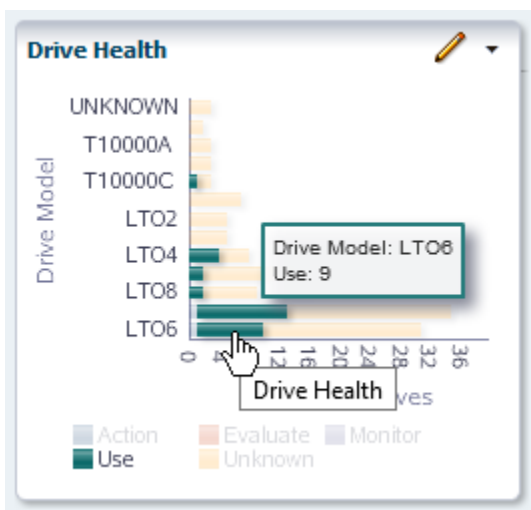
Use the Dashboard to view high-level information about your library system.

The Dashboard contains multiple panes, each showing a different aspect of your library environment. You can hover your mouse over areas of graphical panes to display detailed information. You can click links within some panes to navigate to other screens to view corresponding data.

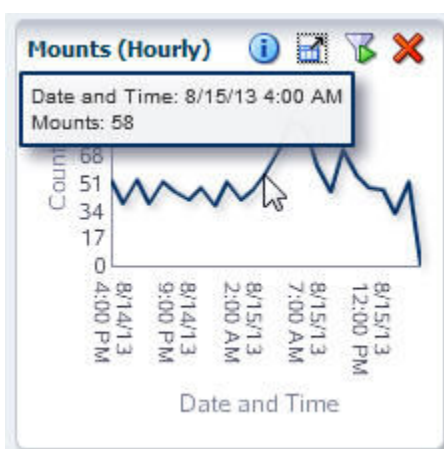
1. Choose any bar chart on the Dashboard and move your mouse over the graph to display detailed values for the bar chart segments.

In the example below, hovering over the LTO6 bar of the Drive Health pane reveals there are nine LTO6 drives in the Use state.



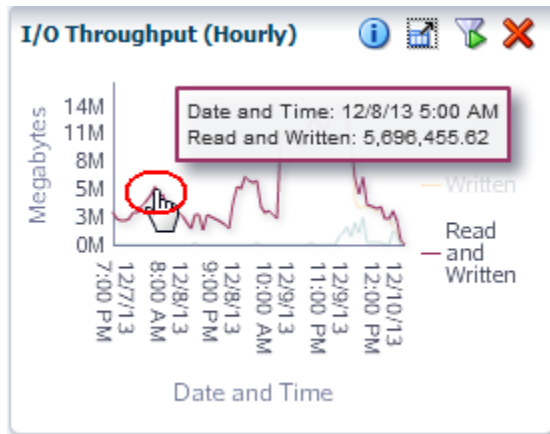


2. Move your mouse over any line graph, such as the Mounts (Hourly) pane, to display detail for each of the data points on the line.

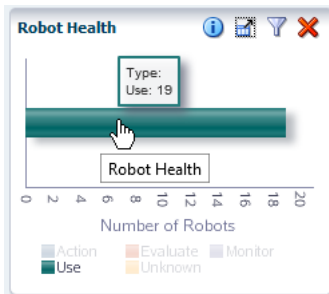


3. The units of measure and scaling of the graphs vary from pane to pane. Check the labels on each axis. STA adjusts the scaling according to the actual data displayed to show as much detail as possible.

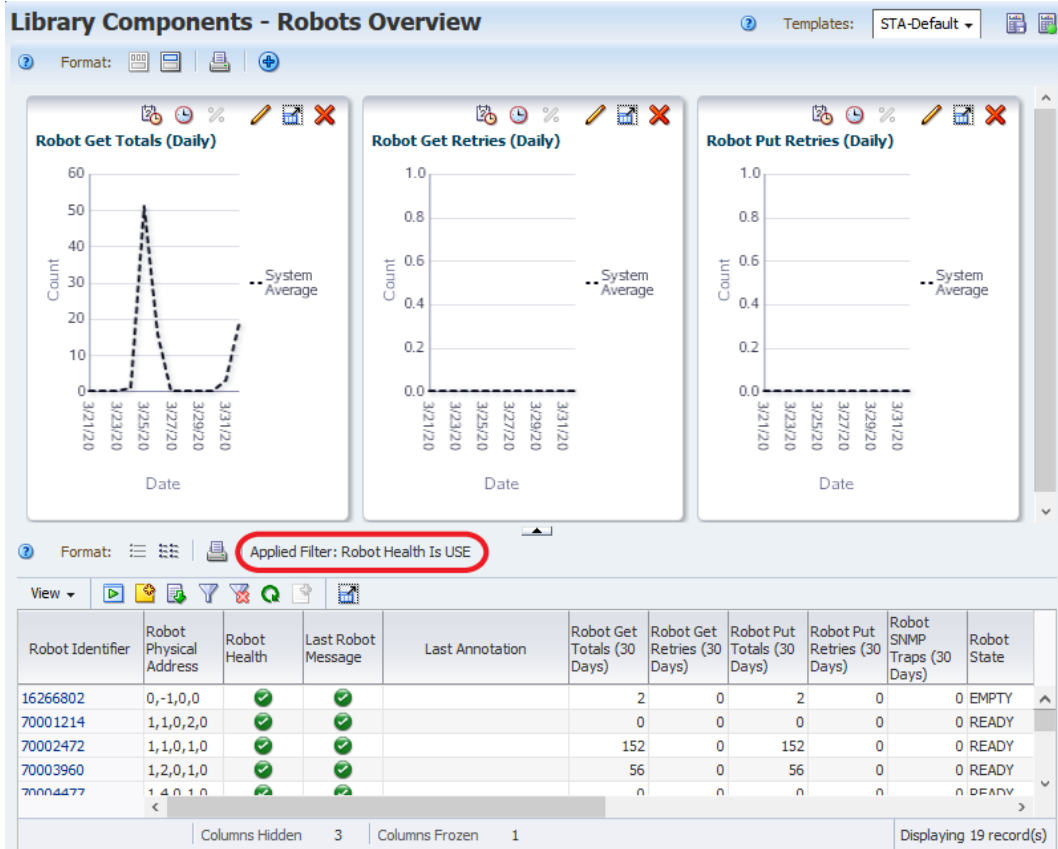
For example, in the following I/O Throughput (Hourly) pane, the vertical axis is labeled "Megabytes," with markers every 3M (three million), from 0M to 14M. Each data point on the line graph, therefore, represents *millions of megabytes*, which converts to terabytes (TB). The hover text for the selected data point indicates 5,696,455.62 MB Read and Written, which converts to roughly 5.69 TB.



4. Bar chart, pie chart, and area chart segments are also active links.  
In the Robot Health pane, click a bar chart segment.



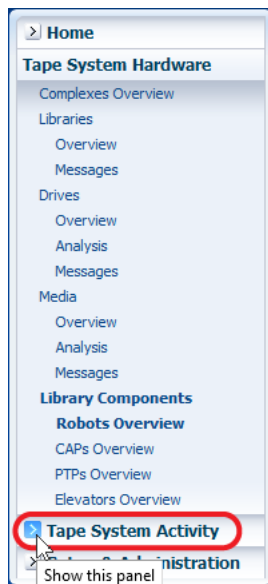
The link displays the Library Components – Robots Overview screen. It shows detailed information about the robots included in the bar segment that you clicked. In this example, the filter shows all robots with a "Use" health.



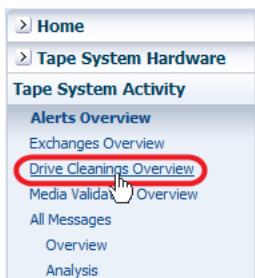
## Navigate Using the Left Menu

The left navigation menu is the primary method for accessing STA screens. It is a series of vertical accordion tabs that you can expand and collapse to access various screens.

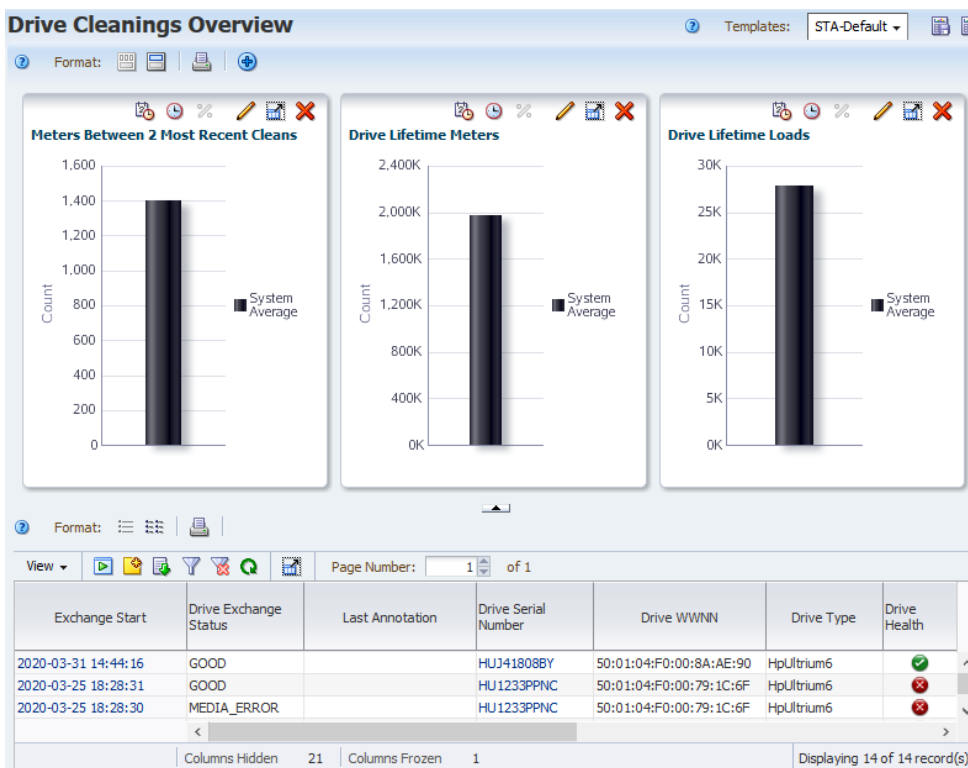
1. Click a collapsed section in the left navigation menu, such as **Tape System Activity**.



- Click a link within the currently expanded tab. Such as **Drive Cleanings Overview**.



The link takes you to the Drive Cleanings Overview page. Below is an example that has the STA-Default template applied. As with the Dashboard, the screen appearance may vary if your STA username has a different template assigned as the default.



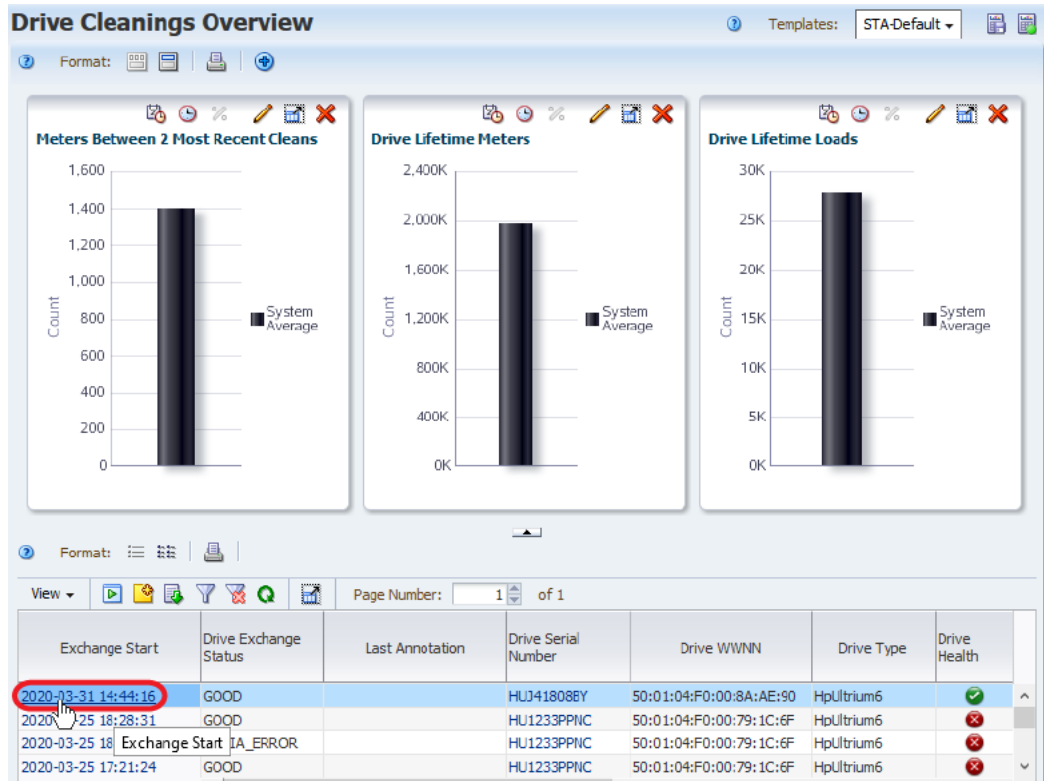
## Navigate Using Text Links

Although the Navigation Bar is the primary method of navigation, you can also navigate by using active links that occur throughout the STA screens.

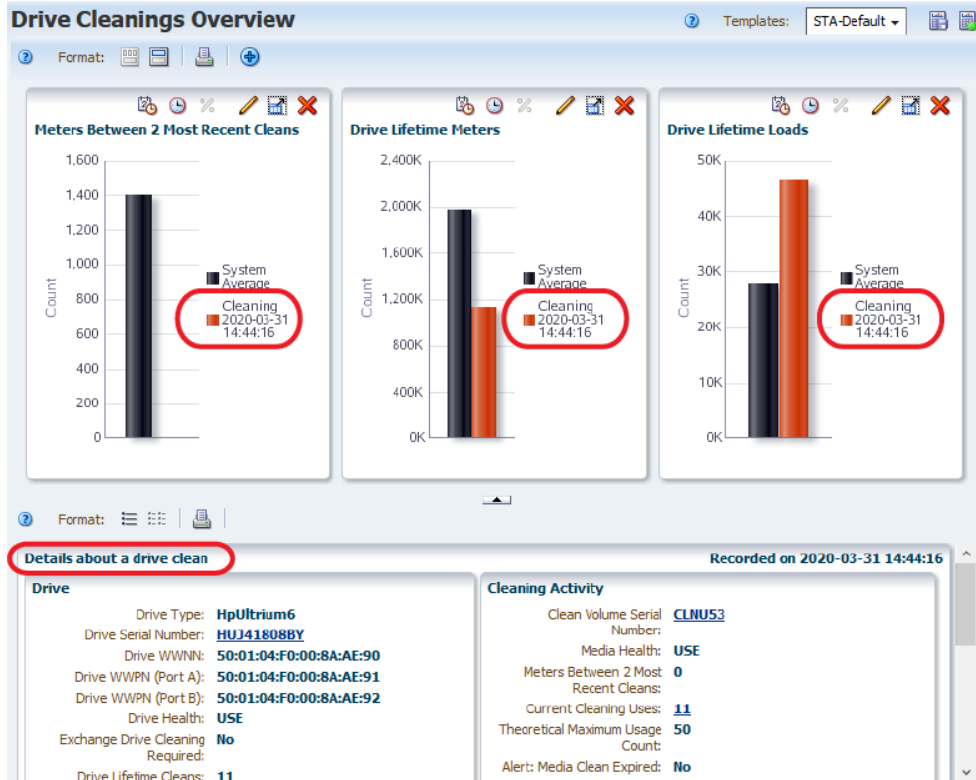
Fields with blue text are active links that allow you to navigate to other screens to see related data.

The example below uses the Drive Cleanings Overview page.

1. Click on an active link within the table area of the screen. For example, the first entry within the Exchange Start column.



2. The Drives Cleanings Overview page refreshes with the selected drive cleaning exchange added to the graph and the details displayed below the graph area.



## Understand the General Screen Layout

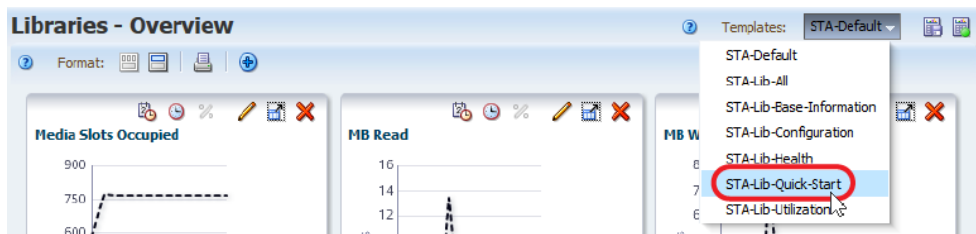
STA "Overview" screens have three main areas: Graph, Table, and Status Line. Understanding this general STA screen layout can help you better interpret the data that STA provides.

In the example below, we will use the Libraries Overview page to see an example of a common STA screen layout.

1. In the left navigation, under **Tape System Hardware**, select the **Libraries Overview** link.



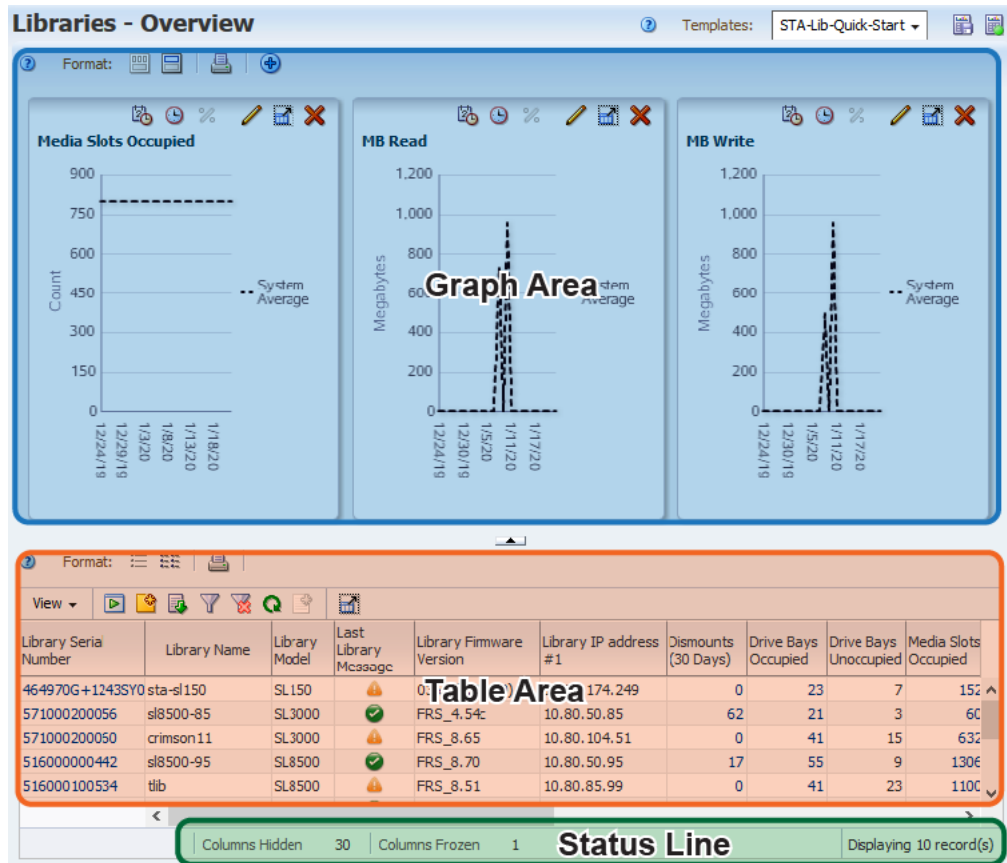
2. From the Templates drop-down menu, select **STA-Lib-Quick-Start**.



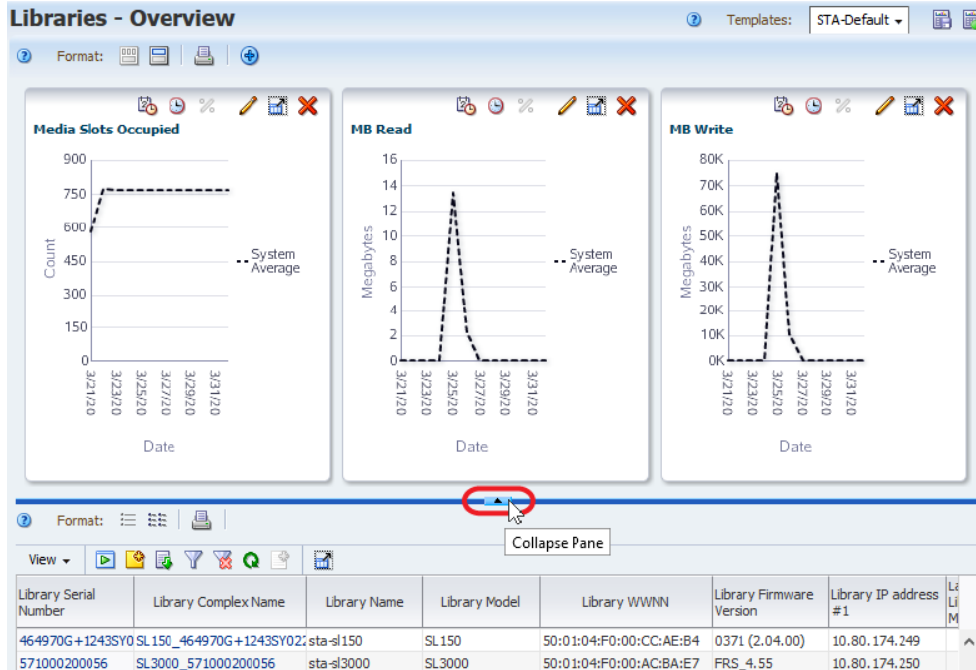
- Note that the screen contains a **Graphics Area** and a **Table Area**. STA "Overview" screens include these two sections.

Also note the **Status Line** at the bottom of the screen, which indicates:

- Columns Hidden* – It is normal for table columns to be hidden. STA collects hundreds of data attributes and most screen templates display only a subset. You can selectively show or hide any of the available attributes.
- Columns Frozen* – The first table column is always frozen in position as you scroll to the right on the screen.
- Number of records displayed* – In this example, the value displayed indicates that STA is monitoring a tape library system that includes 10 libraries.



- Click the collapse pane icon to hide the graph area of the screen.



## Display Media Exchanges for a Library

The tape libraries send detailed data to STA for each move, mount, and dismount that occurs. These are referred to as exchanges. You can use exchange data to better understand the media activity of your library system.

The Dismounts attribute for a library indicates the total number of dismounts that have occurred within the library. Each dismount marks the end of an exchange, in which the drive mounted the media, potentially performed read/write activity, and then dismounted the media. Use this dismount data to analyze exchange activity for a specific library.

1. On the **Library Overview** page with the **STA-Lib-Quick-Start** template applied, locate a library for which the value in the *Dismounts (30 Days)* column is greater than zero (this indicates that the library has had some media exchange activity).

Click the active link in the Dismounts column.

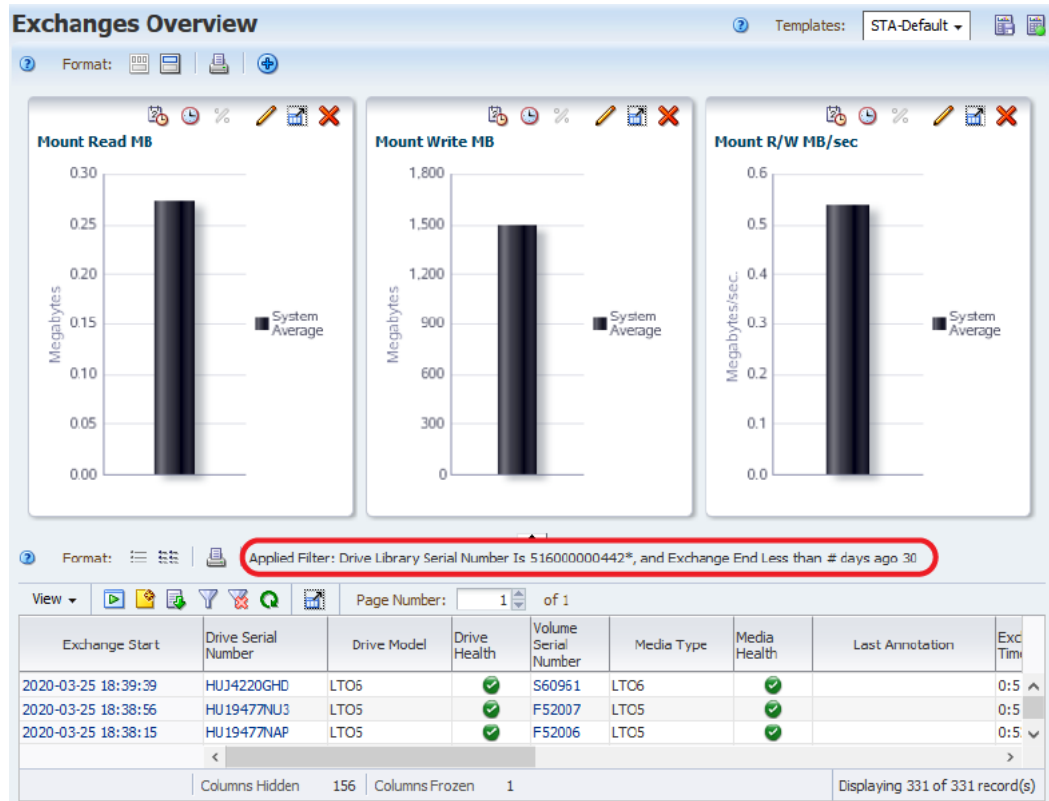
The screenshot shows the 'Libraries - Overview' dashboard with a table of library details. A red circle highlights the 'Dismounts (30 Days)' value of 330 for the library with ID 51600000442.

Library Serial Number	Library Name	Library Model	Last Library Message	Library Firmware Version	Library IP address #1	Dismounts (30 Days)	Drive Bays Occupied	Drive Bays Unoccupied	Media Slots Occupied	Media Slot Unoccupied
464970G+1243SY0	sta-sl150	SL150	🚫	0371 (2.04.00)	10.80.174.249	1	22	0	154	29
571000200056	sta-sl3000	SL3000	🟢	FRS_4.55	10.80.174.250	0	11	13	23	19
571000201755	sl8500-85	SL3000	🟢	FRS_4.55	10.80.50.85	0	17	7	38	19
51600000442	sl8500-95	SL8500	🟢	FRS_8.70	10.80.50.95	330	55	9	1309	11
516000100437	elib18	SL8500	🟢	FRS_8.70	10.80.104.98		22	42	2330	7,73

2. The link takes you to the Exchanges Overview screen, showing details for media exchanges for the selected library. The most recent exchanges are at the top of the table.



Note the "Applied Filter" area at the top of the table, which identifies the filter criteria applied to the screen. Whenever you navigate to a screen using a link, STA automatically applies a filter based on the originating link.

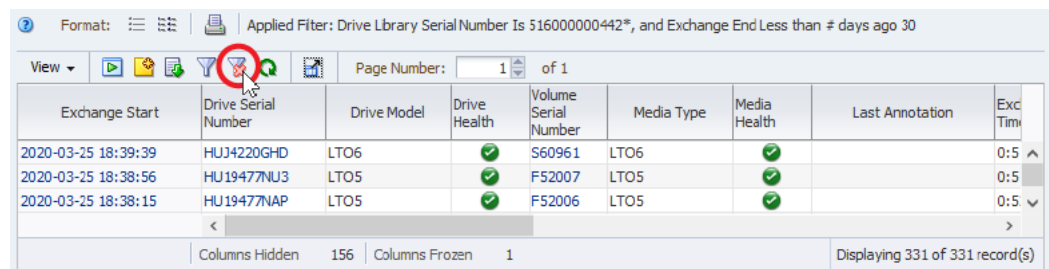


## Reset a Screen Filter

Filters allow you to focus on a subset of information. However, there are times when you may want to clear a filter to see more data.

In the example below, the applied filter indicates that the screen displays data only for the selected library serial number and only for exchanges that have occurred in the last 30 days. In addition, the Status Line shows the total number of records displayed (331). You can clear the filter to display all available records.

1. Click **Reset Filter**  in the table toolbar to remove the filter criteria.



2. Note that the applied filter area is blank and the Status Line now shows more records.

Exchange Start	Drive Serial Number	Drive Model	Drive Health	Volume Serial Number	Media Type	Media Health	Last Annotation	Exc Tim
2020-03-31 14:51:44	HU14040WCD	LTO6	✓	ENG011	LTO4	✓		0:0
2020-03-31 14:49:41	1310091204	LTO4	?	000125	LTO2	?		0:0
2020-03-31 14:48:16	576004007613	T10000C	✓	STA117	T10000T2	✓		0:0

## Display Full Details for Selected Exchanges

Most STA screens display the list view by default. You can use the detail view to display full details for a selected set of data.

For example, you can use the following steps to view full details of the three most recent exchanges.

1. Within the table of the **Exchanges Overview** screen, shift-click to select the first three table rows. Be careful to click in the white space of each row and not on an active link.

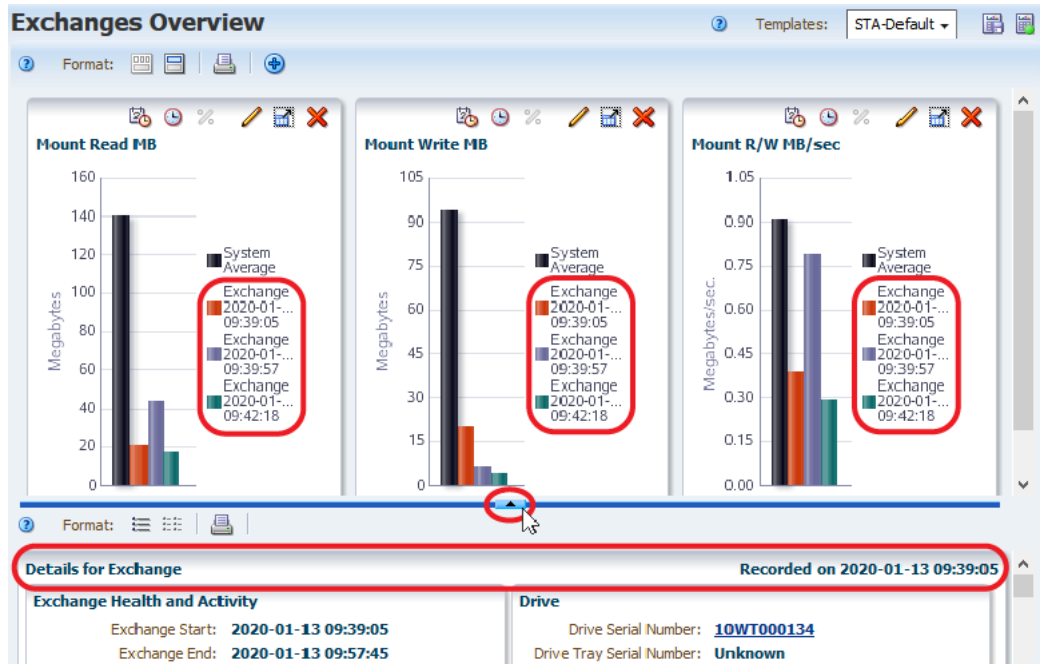
Click **Detail View** in the table toolbar.

**Exchanges Overview** Templates: STA-Default

Exchange Start	Drive Serial Number	Drive Model	Drive Health	Volume Serial Number	Media Type	Media Health	Last Annotation	Exc Tim
2020-03-31 14:51:44	HU14040WCD	LTO6	✓	ENG011	LTO4	✓		0:0
2020-03-31 14:49:41	1310091204	LTO4	?	000125	LTO2	?		0:0
2020-03-31 14:48:16	576004007613	T10000C	✓	STA117	T10000T2	✓		0:0
2020-03-31 14:46:52	1310003864	LTO4	?	A00057	LTO3	?		0:0
2020-03-31 14:46:05	1210036542	LTO3	?	A00058	LTO3	?		0:0

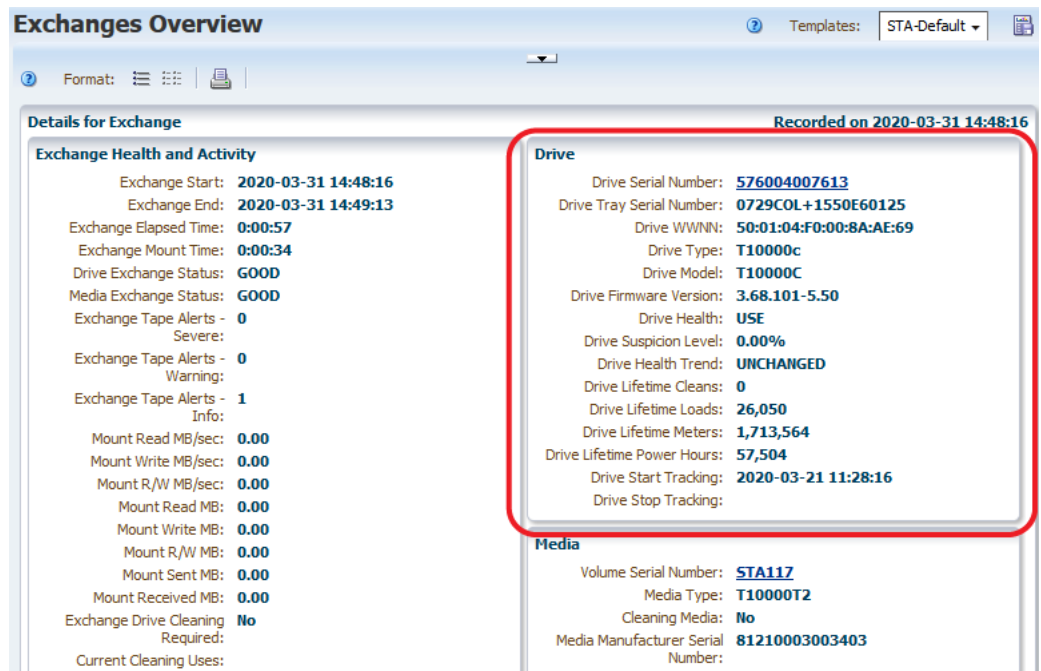
2. Note that the graphs update to show the three exchanges. The bottom of the screen displays full details in text form for the exchanges.

Click **Collapse Pane** to hide the graph area of the screen.



3. Scroll through the Detail View section to see information for each record.

STA organizes attributes for each record into related information sets. For example, the "Drive" section contains data about the drive used in the exchange.



4. Some attribute values are active links (blue underlined values). Clicking an active link takes you to the associated screen with a filter applied.

Click the **Drive Serial Number** link.

**Drive**

Drive Serial Number: **576004007613**

Drive Tray Serial Number: **0729COL+1550E60125**

Drive WWNN: **50:01:04:F0:00:8A:AE:69**

Drive Type: **T10000c**

- The link takes you to the Drives - Overview screen, where the graphs display only the data for the selected drive. The bottom of the screen remains in the Detail View mode and the graphs update with data for the selected drive.

**Drives - Overview** Templates: STA-Default

Format: [Icons]

**Details for Drive 576004007613** Monitored since 2020-03-21 11:28:16

Drive	Media
Drive Serial Number: <b>576004007613</b> Drive Tray Serial Number: <b>0729COL+1550E60125</b> Drive WWNN: <b>50:01:04:F0:00:8A:AE:69</b> Drive Type: <b>T10000c</b> Drive Health: <b>USE</b> Drive Health Trend: <b>UNCHANGED</b> Last Drive Message: <b>UNKNOWN</b>	Volume Serial Number: <b>STA117</b> Media Manufacturer Serial Number: <b>81210003003403</b> Media Health: <b>USE</b> WORM/VolSafe Media: <b>No</b> Cleaning Media: <b>No</b>

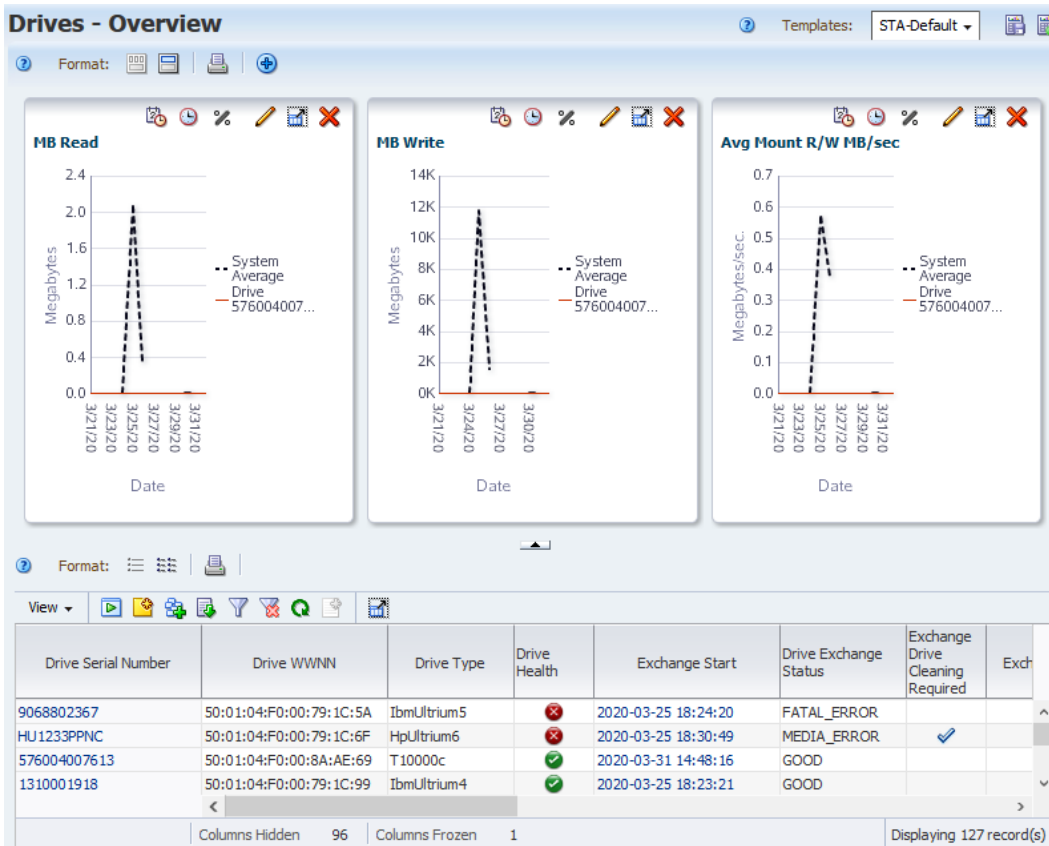
- Click **List View** to display data in a table instead of the detailed view.

Format: [List View Icon]

**Details for Drive 576004007613** Monitored since 2020-03-21 11:28:16

Drive	Media
Drive Serial Number: <b>576004007613</b>	Volume Serial Number: <b>STA117</b>

The screen updates with the table displayed below the graph area. The example below shows the STA-Default template for the Drives – Overview screen. Your display may look different if you have a different template assigned as the default.

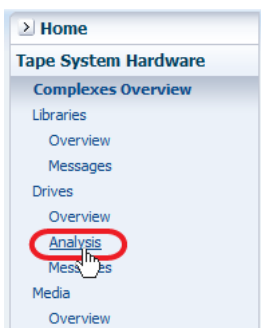


## Display Aggregated Drive Data

Analysis screens show aggregated data for library components or events using a pivot table. You can modify the table to organize data into categories of your choice.

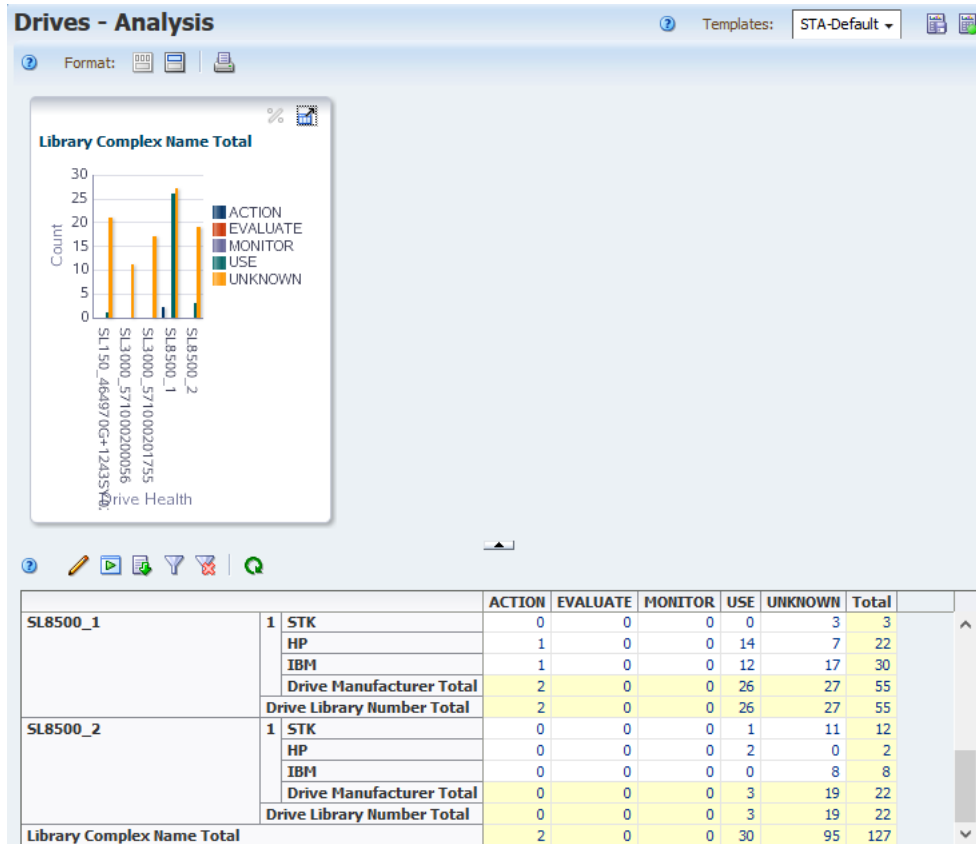
Pivot tables can help you see patterns and trends that you otherwise might not see in a standard table. Use the following steps to display aggregated drive data and the underlying details.

1. In the left navigation, select **Drives Analysis**.

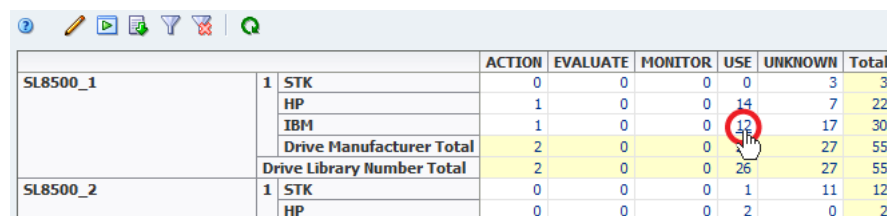


The Drives – Analysis screen has a graph area at the top and a pivot table at the bottom. The example below shows the STA-Default template for the Drives – Analysis screen.

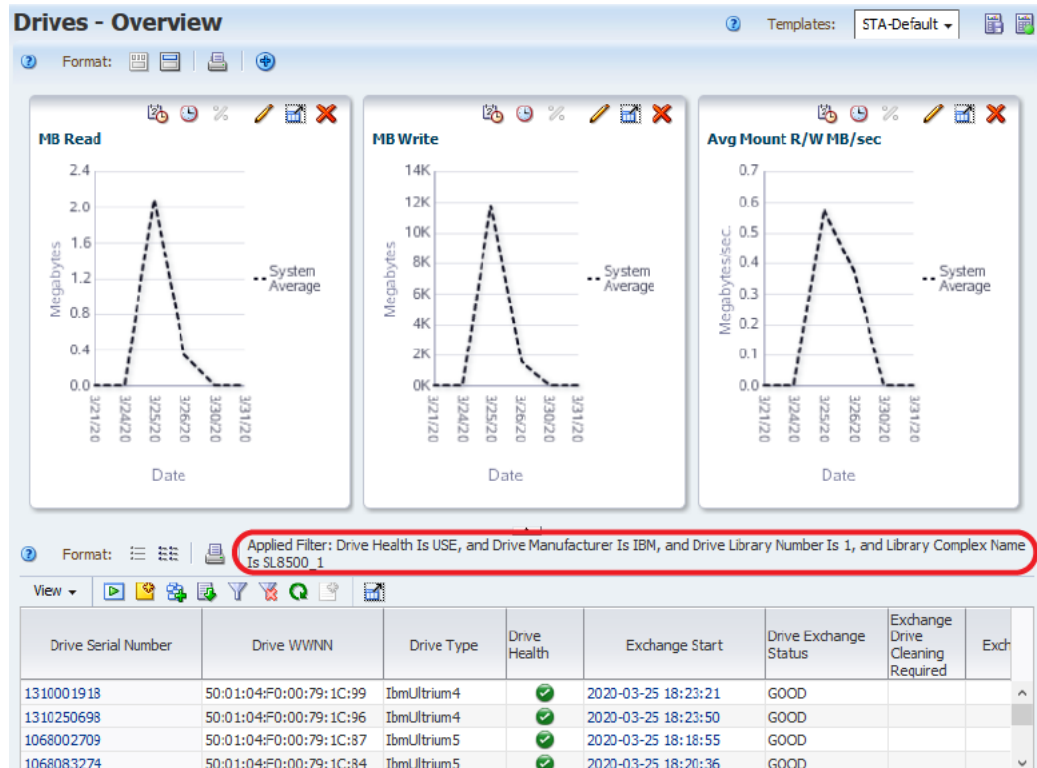
The pivot table aggregates drive health data by library complex, library ID, and drive manufacturer.



- The values in the pivot table are active links. Click a link to see details for the aggregated number.



The link takes you to the Drive-Overview page with a filter applied that shows the selected values from the pivot table.

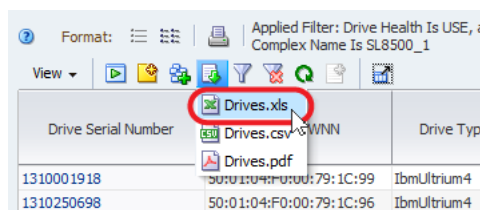


## Export Data to a Spreadsheet

You can export data from tables and pivot tables to transfer the data to other applications for further analysis.

1. Select the **Export** icon in the table toolbar.

The drop-down shows available formats. Select **Drives.xls**.



2. Save the file to an accessible location, and then open the file in a spreadsheet application.

## Access the Online Help

You can access the help from any screen of the GUI. The help provides context sensitive information for the currently displayed screen.

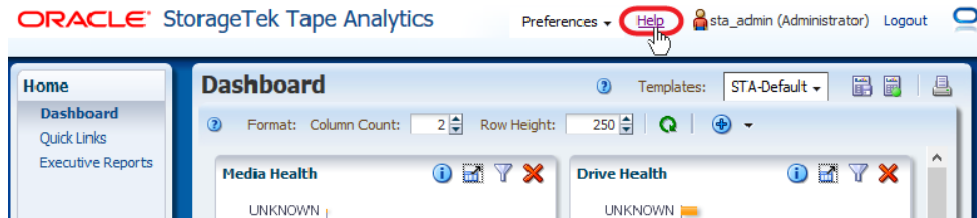
There are two main ways to access the help:

- Click the Help link in main toolbar at the top-right of the GUI.

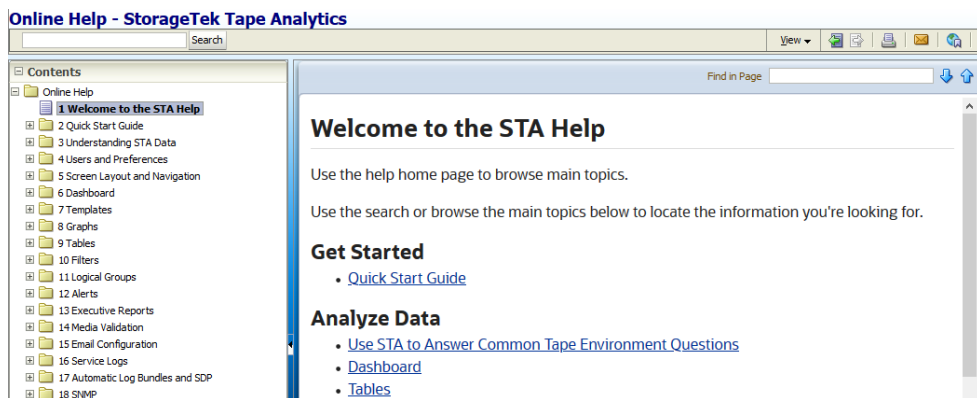
- Click a (?) help icon found throughout various GUI screens.

The example below accesses the help from the Dashboard screen.

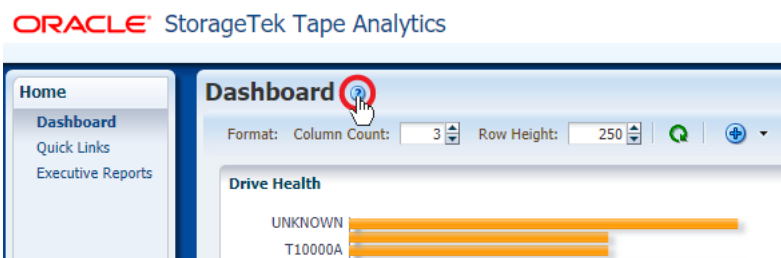
1. Click the **Help** link in the main toolbar.



2. The help opens in a new browser tab with the help homepage displayed. Click any active link to navigate to other help topics.

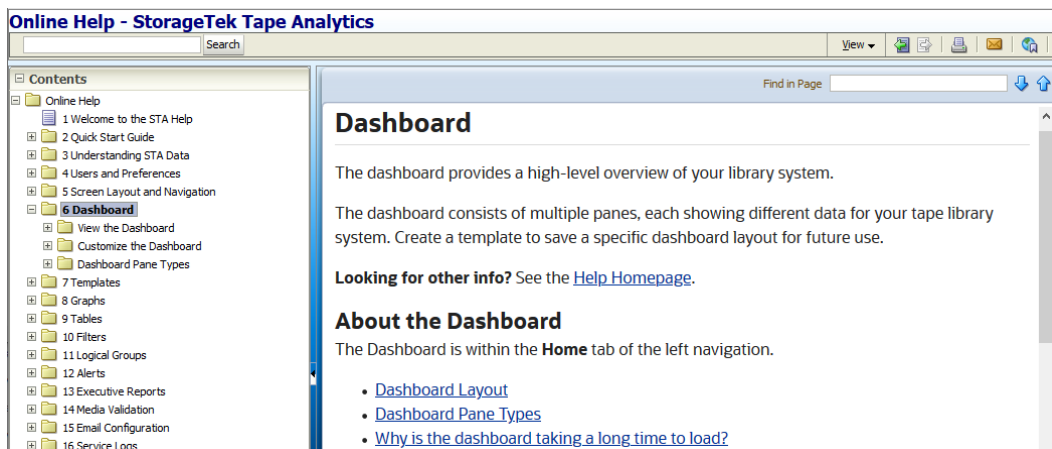


3. Return to the tab running the Dashboard. Click on a (?) help icon.



This time, the Help displays information for the Dashboard.

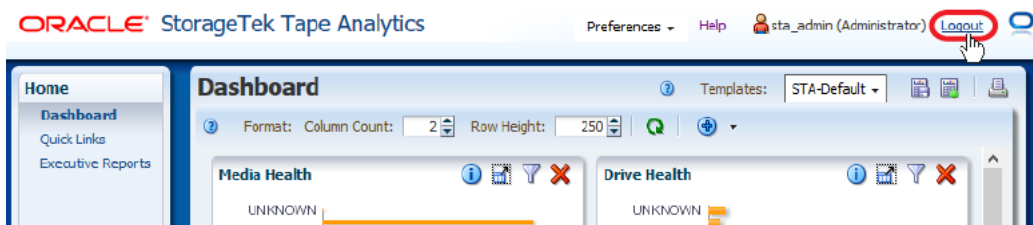




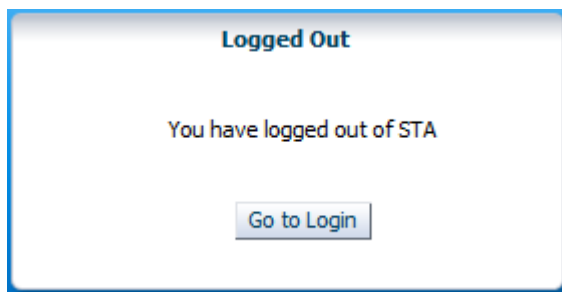
## Log Out

You should always explicitly log out of STA, rather than simply closing the browser window or tab. Logging out releases application memory immediately, rather than waiting until after your session times out.

1. From any STA screen, click **Logout** in the upper-right of the main toolbar.



2. The Logged Out dialog box appears. Click **Go to Login** to return to the login screen.



## Next Steps After Finishing the Quick Start

As you gain experience with STA and the data that it collects, you may want to explore how you can use STA to better manage your tape library system.

Use the following sections within this guide to learn more about what you can do with STA.

- [Users and Preferences](#)

- [Screen Layout and Navigation](#)
- [Graphs](#)
- [Tables](#)
- [Dashboard](#)
- [Templates](#)
- [Filters](#)
- [Alerts](#)
- [Executive Reports](#)
- [Logical Groups](#)
- [Media Validation](#)
- [Email Recipients](#)
- [Service Log Bundles](#)
- [Automatic Log Bundles and SDP](#)
- [Library Connection \(SNMP or SCI\)](#)
- [Understanding STA Data](#)
- [Data Reference](#)

# B

## Data Reference

The data reference provides descriptions of all data fields and identifies the attributes listed on each detail view screen. Use it to determine where data is displayed within the various screens of STA and look up the meaning of attributes.

For a description of all attributes and data fields in STA see:

- [Attribute Definitions](#)

For a list of all attributes on each Detail View screen see:

- [Complexes Overview](#)
- [Libraries Overview](#)
- [Drives Overview](#)
- [Media Overview](#)
- [Robots Overview](#)
- [CAPs Overview](#)
- [PTP Overview](#)
- [Elevators Overview](#)
- [Alerts Overview](#)
- [Exchanges Overview](#)
- [Drive Cleanings Overview](#)
- [Media Validation Overview](#)
- [All Messages Screens](#)

## Attribute Definitions

Attribute definitions provide a description of all data fields displayed by STA. Use this section when you need to know the definition of a table column heading, graph attribute, and so on.

The definitions are listed alphabetically, click a link below to go directly to a letter:

- [Symbols](#)
- [A](#)
- [B](#)
- [C](#)
- [D](#)
- [E](#)
- [F](#)
- [H](#)

- I
- L
- M
- MV
- N
- P
- R
- S
- T
- U
- W

## Symbols

### **% Drive Utilization**

Percentage of time all drives in the library were occupied. Does not include time drives are not available because of application reservation or library positioning.

## A

### **Action Taken**

Applies to automatic log bundle alerts only. Action taken by STA in response to the alert. If automatic bundle creation is enabled, STA attempts to create an automatic log bundle, and if forwarding to StorageTek Service Delivery Platform (SDP) is enabled, STA attempts to send the bundle to the SDP host. This message indicates whether these actions are successful. In this message, the term *ABC* refers to *automatic bundle creation*.

### **Agent Boot Date/Time**

Date and time the SNMP agent was started, in the library's local time.

### **Alert Event Type**

Type of event or activity that was in process when the alert was triggered.

Options are as follows:

- AppMonitor – The alert was triggered during a restart of the STA application. This event type is not a selectable link.
- Exchange – The alert was triggered during an exchange. Click the link to navigate to the Exchanges Overview screen displaying detail about the exchange.
- MIB Walk – The alert was triggered during a Get Latest Data performed from the Configuration – SNMP Connections screen. This event type is not a selectable link.
- Robot Analytic – The alert was triggered by a change in robot health. This event type is not a selectable link.
- Trap – The alert was triggered by an SNMP trap from the library. Click the link to navigate to the All Messages – Overview screen displaying detail about the trap.

- blank – Either the alert was triggered by an internal STA calculation, or the triggering event is unknown. In either case, there is no detail to display.

**Alert Policy Name**

User-defined name assigned to the alert policy.

**Alert Policy Type**

Type of alert policy. Examples are: STA, Complex, MDV, Media, Move, Robot.

**Alert Reason**

Criteria of the alert policy that generated this alert.

**Alert Severity**

Severity level of the alert policy that generated this alert. Options are: Severe, Warning, Informative. The severity level of a policy determines how often alerts are triggered.

**Alert State**

Current state of the alert. Options are: New, Acknowledged, In-progress, Dismissed, Unknown. "New" and "Unknown" states are assigned by STA. All other states are user-assigned according to the optional alerts workflow implemented at your site.

**Alert: Cleaning Media**

LTO only.

Cleaning media has been loaded in the drive.

**Alert: Drive Automated Interface**

LTO only.

The drive has experienced an Automation Interface fault.

**Alert: Drive Clean Now**

Both enterprise and LTO.

A media error has caused a cleaning request.

**Alert: Drive Clean Periodic Requested**

Both enterprise and LTO.

A clean threshold has been exceeded. Set when a StorageTek enterprise or IBM LTO drive detects that it needs routine cleaning.

**Alert: Drive Cooling Fan**

LTO only.

The drive has detected that a cooling fan is not operating within manufacturer-specified limits.

**Alert: Drive Diagnostics Required**

LTO only.

A failure requiring diagnostics has occurred. Triggered by a tape alert 39. This alert is reset after diagnostics are run.

**Alert: Drive Dual-Port Interface**

LTO only.

A redundant interface port on the drive has failed.

**Alert: Drive Dump Available**

Enterprise only.

A drive dump created earlier is available. This alert is reset after the dump is downloaded.

If you see this alert, Oracle recommends you collect a drive dump and drive logs as soon as possible. This will assist Oracle Support with drive fault analysis.

**Alert: Drive Event Log Near Full**

Enterprise only.

The drive event log is 75 percent or more full. This is an expected state, as the log is circular. Events may be overwritten unless they are collected. If Oracle Service Delivery Platform (SDP) is installed, the logs are cleared.

**Alert: Drive Failure Predicted**

Both enterprise and LTO.

The drive firmware has predicted a drive hardware failure.

**Alert: Drive FW Download**

LTO only.

A drive firmware download has failed because an invalid firmware file was used for this drive type.

**Alert: Drive FW Failure**

Both enterprise and LTO.

The drive has detected a firmware fault and has reset itself. This alert remains active until all dumps are retrieved from the drive.

Retrieve the drive dumps.

**Alert: Drive Hard Error**

LTO only.

Indicates an unrecoverable read, write, or positioning error. This alert is cleared internally when the media is ejected.

Check the following alerts for additional detail: Media Error, Read Failure, Write Failure.

**Alert: Drive Hardware A**

LTO only.

The drive has experienced a hardware fault from which it can recover through a reset.

**Alert: Drive Hardware B**

LTO only.

The drive has experienced a hardware fault from which it can recover through a power cycle. This alert is set if the tape drive fails its internal power-on self-tests and is cleared internally when the drive is powered off.

**Alert: Drive Interface Fault**

LTO only.

The drive has experienced a problem with the host interface. Check cables and connections and restart the operation.

**Alert: Drive Load Limit**

Both enterprise and LTO.

Indicates whether the drive exceeded its lifetime limit of media loads at the time of the exchange.

**Alert: Drive Model Incompatible**

Enterprise only.

The drive is down-level for the media attempting to be loaded.

**Alert: Drive Temperature**

Both enterprise and LTO.

The drive has experienced a cooling problem. This could impact media integrity.

**Alert: Drive Voltage**

LTO only.

Drive voltage limit has been exceeded

**Alert: Forced Eject Attempted**

LTO only.

A manual or forced eject occurred while the drive was reading or writing.

**Alert: Invalid Cleaning**

LTO only.

The cleaning media is incompatible with the drive.

**Alert: Media Cart Memory Failure**

Indicates the cartridge memory failed during the exchange. This results in reduced performance.

**Alert: Media Clean Expired**

Both Enterprise and LTO.

The drive firmware has determined that the cleaning media has already been used the maximum number of times and cannot be used for this cleaning exchange.

**Alert: Media Diminished Capacity**

LTO only.

The volume state has been set not to allow partition 0 to use the full native capacity of the volume. For example, the volume is partitioned, or the available medium for use has been reduced by a SET CAPACITY command.

**Alert: Media Directory Corrupt**

Both Enterprise and LTO.

The media directory on the tape media is corrupted, leading to degraded file search performance until the directory is rebuilt. This has occurred because the drive was powered down with media loaded, or a permanent error prevented the media directory from being updated.

**Alert: Media Directory Invalid**

Both Enterprise and LTO.

The media directory has been corrupted. No data was lost, but media performance could be impacted.

The media directory can be rebuilt by reading all the data.

**Alert: Media Eject Failed**

LTO only.

The eject operation has failed.

Eject the media, reload, and restart the operation.

**Alert: Media End of Warranty**

Enterprise only.

The media has reached the end of its warranty period, and further use is not covered by warranty.

**Alert: Media Error**

Both enterprise and LTO.

Media performance is severely degraded, or the media can no longer be read or written. This alert is set for any unrecoverable read, write, or positioning error caused by faulty media and is cleared internally when the media is ejected.

**Alert: Media Life Exceeded**

Both enterprise and LTO.

The media has exceeded its expected useful life. Available for IBM LTO-4 and above drives only. HP drives report the Nearing Media Life Alert attribute instead.

**Alert: Media Load Failure**

Both Enterprise and LTO.

The drive was unable to load the media and thread the tape.

**Alert: Media Load Limit**

Both Enterprise and LTO.

The media has exceeded the recommended number of drive loads.

**Alert: Media Lost Statistics**

Both Enterprise and LTO.

Some previously existing media statistics have been lost due to a drive or library being powered down with media loaded.

**Alert: Media Maintenance**

Enterprise only.

Media in the drive requires physical maintenance, which must be corrected before the media can be loaded successfully. For example, the leader may be pulled into the cartridge.

**Alert: Media Nearing End of Life**

The media is approaching the end of its expected useful life. Available for HP drives only.

**Alert: Media No Start of Data**

Both Enterprise and LTO.

Start of customer data could not be found

**Alert: Media Not Data Grade**

LTO only.

The drive has not been able to read the media recognition system stripes, indicating the media is not data-grade. Any data you write to the media is at risk.

**Alert: Media Recoverable Mechanical**

LTO only.

The tape has snapped or suffered a mechanical failure in the drive, but the media can still be ejected.

**Alert: Media RFID Warning**

Enterprise only.

The media RFID was found to be open at load time, indicating the drive was powered off before the media was unloaded on the previous mount. Results in degraded media performance. Writing is not allowed until End of Data is found.

**Alert: Media System Read Failure**

Both Enterprise and LTO.

The system area on the media could not be read from at load time. No data was lost, but media performance could be impacted.



**Alert: Media System Write Failure**

Both Enterprise and LTO.

The system area on the media could not be written to at unload. No data was lost, but media performance could be impacted.

Monitor the drive and media. If this error persists across multiple media, service the drive.

**Alert: Media Unrecoverable Mechanical**

LTO only.

The tape has snapped or suffered a mechanical failure in the drive and cannot be extracted.

Do not attempt to eject the media.

**Alert: Media Unrecoverable Snapped**

Enterprise only.

The tape has snapped in the drive and cannot be extracted. Do not attempt to eject the media.

**Alert: MIR Invalid**

Enterprise only.

The media information record (MIR) was not updated sometime in the past, resulting in degraded file search performance.

The MIR can be rebuilt by reading all the data.

**Alert: Permanent Error**

Enterprise only.

A permanent media error occurred while the media was mounted. Check the exchange FSC or DSC for more information.

**Alert: Read Failure**

LTO only.

Read has failed. The media is damaged or the drive is faulty.

**Alert: Read Only**

LTO only.

Media of this type is read-only in this drive. The media appears as write-protected.

**Alert: Read Warning**

Both Enterprise and LTO.

The drive has experienced severe trouble reading from the media.

The media or drive require attention.

**Alert: Unload Prevented**

LTO only.

The media cannot be ejected because the drive is in use.

Wait until the operation has completed before ejecting the media.

**Alert: Unrecoverable Unload**

LTO only.

The drive reached the maximum number of unload retries and was unable to unload the media.

**Alert: Unsupported Format**

LTO only.

Media of this type is not supported in this drive.

**Alert: WORM Integrity Failure**

LTO only.

The drive has detected an inconsistency during the WORM volume integrity checks. The media may have been tampered with.

**Alert: WORM Overwrite Attempted**

LTO only.

An attempt was made to overwrite user data on a WORM volume.

**Alert: Write Failure**

LTO only.

The drive was unable to write data to the media. This alert is set for any unrecoverable write/positioning error, due to either faulty media or faulty drive hardware. The alert is cleared internally when the tape is ejected.

**Alert: Write Protect**

LTO only.

A write command was attempted to write-protected media.

**Alert: Write Warning**

Both Enterprise and LTO.

The drive has experienced severe trouble writing to the media.

The media or drive require attention.

**Annotation History**

User-defined annotation assigned to the library resource or activity. List View shows the most recent annotation. Detail View shows full annotation history, in reverse chronological order.

**Avg Mount R/W MB**

Average megabytes read and written by the drive per exchange. Calculated as:

```
total MB (read +written) /total completed exchanges
```

**Avg Mount R/W MB/sec**

Average throughput rate for the drive, in megabytes per second. Calculated as:

```
total MB (read +written) /total seconds mount time
```

This value may be affected by a variety of factors external to the drive, such as robot speed or application behavior—for example, some applications do not dismount media immediately upon completion of read/write operations, causing the drive to be idle for much of the mount. As a result, this value is not likely to represent the drive's maximum potential throughput rate.

**Avg Mount Read MB**

Average megabytes read by the drive per exchange. Calculated as:

```
total MB read /total completed exchanges
```

**Avg Mount Read MB/sec**

Average read rate for the drive, in megabytes per second. Calculated as:

```
total MB read /total seconds mount time
```

This value may be affected by a variety of factors external to the drive, such as robot speed or application behavior—for example, some applications do not dismount media immediately upon completion of read/write operations, causing the drive to be idle for much of the mount. As a result, this value is not likely to represent the drive's maximum potential read rate.

**Avg Mount Write MB**

Average megabytes written by the drive per exchange. Calculated as:

```
total MB written /total completed exchanges
```

**Avg Mount Write MB/sec**

Average write rate for the drive, in megabytes per second. Calculated as:

```
total MB written /total seconds mount time
```

This value may be affected by a variety of factors external to the drive, such as robot speed or application behavior. For example, some applications do not dismount media immediately upon completion of read/write operations, causing the drive to be idle for much of the mount. As a result, this value is not likely to represent the drive's maximum potential write rate.

**B****Base Model**

Library model.

**Bundle Name**

Applies to automatic log bundle alerts only. Unique name assigned by STA to the automatic log bundle. This includes the component type, serial number (does not apply to RDA log bundles), and date and time stamp when the bundle was created.

For example:

```
Cap_CAP-516000100437+1643197981+4_-07.4.2017.51.08.09.zip  
Drive_572001000232_-07.4.2017.48.08.00.zip  
Elevator_ELEVATOR-74029666+754889920_-07.4.2017.59.09.56.zip  
Ptp_74028986_-07.4.2017.51.09.05.zip
```

**C****CAP**

Serial number of the CAP

**CAP Accessibility**

Current CAP accessibility state, as reported by the library. Options are: ALLOW, CLOSED ALLOW, PREVENT, CLOSED PREVENT.

**CAP Alert Count**

Total alerts generated for this CAP, AEM, or mailslot, based on defined STA alert policies. This field links to the Alerts Overview screen, list view, which lists alerts for this CAP.

**CAP Count**

Total CAPs, AEMs (SL3000 only), and mailslots (SL150 only)

**CAP Ejects**

For Complexes Overview and Libraries Overview: Total media ejected from the library or complex through all CAPs, AEMs (SL3000 only), and mailslots (SL150 only).

For CAPs Overview: Total media ejected through the CAP

**CAP Enters**

For Complexes Overview and Libraries Overview: Total media entered into the complex through all CAPs, AEMs (SL3000 only), and mailslots (SL150 only)

For CAPs Overview: Total media entered through the CAP

**CAP Identifier**

Unique identifier for the CAP.

**CAP Physical Address**

Library internal address. See [Physical Address](#).

**CAP SNMP Traps**

Total CAP messages received from the library. A sudden increase in this number indicates a condition that should be investigated.

**CAP State**

Current CAP state, as reported by the library. STA updates this value hourly. Additionally for SL3000 and SL8500 libraries, the value is updated as SNMP traps for the CAP are received from the library.

Options are:

- OPEN—CAP is open.
- CLOSED—CAP is closed.
- AUDITING—CAP is undergoing an audit by the robot.

**CAP Type**

Type of CAP. Options are:

- ROTATIONAL—Rotational CAP. Applies to SL8500 and SL3000 libraries only.
- BULK—Bulk-load CAP. Applies to SL8500 libraries only. SL8500 libraries can have eight bulk-load CAPs, and each is reported separately.
- SL500\_CAP—Standard SL500 CAP.
- AEM—Access Expansion Module. Applies to SL3000 libraries only.

**Clean Volume Serial Number**

Volume serial number (VSN or volser) assigned to the media by its external label. If the library does not supply the volser, STA provides one composed of `Library Serial Number:Physical Address`. Not all cleaning media have a volser starting with "CLN". This field links to the Media – Overview screen, detail view, which displays all available detail for this media.

**Cleaning Media**

For Drives Overview: Indicates whether cleaning media has been loaded in the drive. For Media Overview and Exchanges Overview: Indicates whether this is a cleaning media, as determined by the media domain and type. Possible values: True or False.

**Note:**

Not all cleaning media have a volser starting with "CLN".

**Cleans**

Total exchanges involving cleaning media. This count includes both successful and unsuccessful cleaning operations; therefore it is not necessarily an indicator of the number of times the drive has been cleaned. This field links to the Drive Cleanings Overview screen, list view, which lists cleaning exchanges for this drive.

**Complex Physical Library Count**

Total libraries in the complex (always "1" for non-SL8500 libraries). This field links to the Libraries – Overview screen, list view, which lists all libraries in this complex.

**Component ID**

Unique identifier for the resource involved in the alert. The type of ID depends on the alert. For example, a volume serial number (for media), drive serial number (for drives), library serial number (for libraries).

**Cumulative Library Uptime**

Total time the library has been running since the last reboot. Displayed as hh:mm:ss.

**Current CAP Slots**

Total slots currently present in the CAP. This is less than the [Maximum CAP Slots](#) if magazines have been removed for loading or unloading,

**Current Cleaning Uses**

Total times the cleaning media has been mounted in a drive. Some media types track this count, in which case, this value is as reported by the media itself. Other media types do not track this count, in which case, this value is as recorded by STA. Since the cleaning media may have been used before the start of STA monitoring, STA may not have exchange records for all drive cleanings done with the media.

## D

**Data Compression Ratio**

Compression ratio for the exchange. Displayed as ratio, calculated as:

```
(Total uncompressed data sent or received by the drive / Total compressed data read or written to the media) :1
```

**Date Created/Updated**

Date and time when the alert was triggered.

**Device Activity**

Internal library functionality that is producing the message. For example, "AuditDaemon" indicates logging information from the library audit function. Values come directly from the library and vary by library model, firmware level, and hardware configuration. The values may reflect significant library events or configuration changes, such as "reboot" or "setPartition." To troubleshoot library issues, it may be useful to sort or filter the All Messages – Overview screen by this attribute.

**Device Address**

Library internal address of the device associated with the SNMP trap. See [Physical Address](#).

**Device ID**

FRU ID of the device associated with the event.

**Device Serial Number**

Serial number or other unique identifier of the device associated with the event.

**Device State**

State of the device at the time the trap was sent. Varies by device type, as in the following examples:

- Drives – EMPTY, LOADED, NEEDS\_CLEANING
- CAPs – OPEN, CLOSE, UNKNOWN
- Pass-thru ports (PTPs) – OK, ERROR, WARNING, INFO, TRACE

#### **Device Time**

Date and time of the event, in UTC standard format.

#### **Dismounts**

Total dismounts for all drives. This field links to the Exchanges Overview screen, which lists exchanges for this library.

#### **Dismounts With Errors**

Total dismounts for this drive or media in which an error occurred during the exchange. The error could be due to issues with the drive, the media, or both. This field links to the Exchanges Overview screen, which lists the exchanges with errors.

#### **Drive**

Electronic serial number of the drive. \*NO-SERIAL\* indicates it is not known. This field links to the Drives – Overview screen, detail view, which displays all available details for this drive.

#### **Drive Alert Count**

Total alerts generated for this drive, based on defined STA alert policies. This field links to the Alerts Overview screen, list view, which lists alerts for this drive.

#### **Drive Bays Installed**

Total drive slots installed but not necessarily activated for use. Calculated as:

`Drive Slots Occupied + Drives Slots Unoccupied.`

#### **Drive Bays Occupied**

Total drive slots with drives installed. This field links to the Drives – Overview screen, list view, which lists all drives for this complex.

#### **Drive Bays Unoccupied**

Total drive slots with no drives installed.

#### **Drive Cleans**

Total exchanges involving cleaning media. This is not necessarily an indicator of the number of cleans actually performed, as this count includes both successful and unsuccessful cleaning operations. This field links to the Drive Cleanings Overview screen, list view, which lists cleaning exchanges for this library or complex.

#### **Drive Dismounts**

Total times media have been unloaded from this drive. This field links to the Exchanges Overview screen, list view, which lists this drive's exchanges.

#### **Drive Exchange Status**

Status of the drive upon completion of the exchange, as derived from a variety of factors, including drive errors, write efficiency, and read margin. Possible values:

- CART\_MEM\_FAILURE – An error has occurred with the cartridge memory; this results in reduced performance.
- CLEAN\_REQ – The drive is due for cleaning.

- DRIVE\_ERROR – The drive has experienced a hardware or microcode error.
- ENCRYPT\_ERROR – An error has occurred with the encryption key management system. This is neither a drive nor media problem, so there is no effect on the suspicion of the drive or media.  
  
Possible causes for this status include the following: compromised network connectivity to the encryption key server; the encryption key server is down; the drive key enrollment has expired and the drive must be re-enrolled; either the drive or the media is not encryption-capable. It may be possible for the drive to read unencrypted media until the encryption issue is resolved.
- EXPIRED\_CLEAN\_TAPE – The cleaning media has expired.
- FAILED\_MOUNT
- FATAL\_ERROR – The media cannot be mounted or is stuck. Possible reasons include a problem with the drive hardware or the media cartridge.
- FW\_DOWN\_LEVEL – The drive firmware is downlevel.
- GOOD – The exchange completed with no issues.
- INCOMPLETE\_UNLOAD – The application requested that the media be unloaded. The drive has detected data still in its buffer and has asked for confirmation from the application.
- INVALID\_OPERATION – The host has requested an invalid operation, such as any of the following: mounting media in an incompatible drive; reading from media that is blank; writing on media that is write-protected; attempting to locate a position beyond the beginning or end of the tape.
- LOAD\_ERROR – An issue with the media prevented it from being loaded. Possible causes include: a problem with the drive hardware or microcode; a problem with the cartridge leader.
- LTO\_NON\_ADI\_MODE –ADI mode has not been enabled on either the library, the drive, or both.
- MEDIA\_ERROR – The media cannot be read or written. Possible causes include a problem with the tape medium or the MIR.
- NON\_DRV\_ERROR – This is neither a drive nor media problem, so there is no effect on the suspicion of the drive or media. For additional information, check the following: for Enterprise drives, check the exchange fault symptom code (FSC); for LTO drives, check recent tape alerts.

Possible causes for this status are as follows:

\* A Media Write Protect Tape Alert must be set. The host application is attempting to write to media that has been write protected.

\* FSC has been set to 3627, 3629, 362A, or 362B. These FSC codes are set during a "normal operation," which checks that a piece of media is truly blank before labeling it. The host application will perform the following sequence: 1) mount new tape; 2) attempt to check for no label; 3) label the new tape.

- OTHER\_DRV\_ERROR
- OTHER\_ERROR
- PERM\_ERROR – A permanent error occurred on the exchange. This may be the result of a media format error, possibly from a previous exchange.

- **READ\_ERROR** – The media could not be read. Possible causes include: a problem with the drive hardware or microcode; a problem with the media MIR; the media may have been corrupted during a previous mount; the drive and media may be incompatible
- **UNKNOWN** – STA has not received enough exchange data from the library to calculate drive health. It may be that the drive is not supported (LTO-2, for example) or the library firmware is downlevel.
- **UNLOAD\_ERROR** – An error occurred during the unload operation. Possible causes include: a problem writing to the media RFID or MIR; the drive and media may be incompatible.
- **WRITE\_ERROR** – An error occurred during the write operation. Possible causes include: a problem with the drive hardware or microcode; the media may have been corrupted during a previous exchange; the drive and media may be incompatible.

#### **Drive Firmware Version**

Drive firmware and host interface level. See the requirement in the *STA Installation and Configuration Guide* for details on whether this firmware version supports rich data for STA.

#### **Drive Health**

Drive health as computed by STA analytics. This is a point-in-time value based on data gathered from the drive during current and past exchanges. It reflects a variety of factors, such as the drive's error history, read margin, and write efficiency.

This value includes all data up to and including the last completed exchange. It is updated immediately after each completed exchange involving the drive.

STA only receives information about errors detected by a drive while performing read/write activity to a media. STA does not receive information about errors that may occur in the data path or the host application.

Cleaning exchanges have a neutral impact on drive health.

This attribute is not to be confused with the drive status reported by the library; see [Last Drive Message](#) for comparison.

Possible values, in order of degrading health:

- **USE** – The drive has had no failures or degradation in the last ten exchanges
- **MONITOR** – The drive has had multiple errors; there is a less than 80 percent chance that it needs service.
- **EVALUATE** – The drive has had multiple errors; there is a greater than 80 percent chance that it needs service.
- **ACTION** – The drive has had an error that requires attention. The drive may require service. You should investigate and determine a proper course of action.
- **UNKNOWN** – STA has not received enough data to compute health for the drive. This may be due to a variety of factors, including an unsupported drive model, downlevel drive firmware, or ADI mode not enabled for an LTO drive.

#### **Drive Health Trend**

Trend of drive health between the last two exchanges, as computed by STA analytics. Options are: BETTER, UNCHANGED, WORSE.

#### **Drive HLI Address**

Host Library Interface (HLI) address of the location. Applies only to drives or media slots in HLI partitions or libraries. This address is assigned by the ACSLS or ELS host



software. This value is available only for SL8500 libraries with firmware FRS\_7.80 or higher or SL3000 libraries with firmware FRS\_4.0 or higher. For all others, the value is left blank. See [HLI Address](#).

**Drive Interface**

Host interface type for the drive. Possible values:

- ESCON – IBM Enterprise Systems Connection
- FIBRE – Fibre channel
- FICON – IBM Fibre Channel
- SAS – Serial Attached SCSI
- SCSI – Small Computer System Interface
- UNKNOWN – The library did not report the interface type.

**Drive Library Name**

User-assigned name for the library. Assigned in the Settings – SNMP Connections screen.

**Drive Library Number**

Unique ID assigned to the library.

**Drive Library Serial Number**

Library frame serial number. This field links to the Libraries – Overview screen, detail view, which displays all available details for this library.

**Drive Lifetime Cleans**

Total cleans performed on the drive over its life. The drive life may be longer than the time it has been monitored by STA.

**Drive Lifetime Hours in Motion**

Total hours the drive heads have been in motion over the life of the drive. The drive life may be longer than the time it has been monitored by STA.

**Drive Lifetime Loads**

Total media loads for the drive over its life. Available for all drive types but LTO-3. The drive life may be longer than the amount of time it has been monitored by STA.

**Drive Lifetime Meters**

Total meters of tape that have passed through the drive heads over the drive's life. Available for all drive types but LTO-3. The drive life may be longer than the amount of time it has been monitored by STA.

**Drive Lifetime Meters of Head Contact**

Total meters of media passed through the drive heads over the life of the drive.

**Drive Lifetime Meters Positioning**

Total positioning meters of media passed at high speed through the drive heads over the life of the drive. Positioning meters occur during locate, rewind, and spacing operations.

**Drive Lifetime Power Hours**

Total hours the drive has been powered on over its life. The drive life may be longer than the amount of time it has been monitored by STA.

**Drive Manufacturer**

Drive manufacturer.

For example, STK, IBM, QUANTUM, and so on.

**Drive Model**

Drive model short description. For example, T10000C, LTO4, and so on. UNKNOWN indicates a broken drive or a drive for which STA cannot determine the type. Type is UNKNOWN for all DLT and SDLT drives, for which STA does not compute health.

**Drive Physical Address**

Library internal address for the drive. See [Physical Address](#).

**Drive Properties Updated**

Date and time when the drive properties were last updated. Initially set to the date and time when STA first recognized the drive, and updated whenever subsequent updates occur, such as updating the drive firmware.

**Drive Rail Number**

Rail number. For SL150, SL500, and SL3000 libraries, this value is always 1. For SL8500 libraries, possible values are 1, 2, 3, or 4.

Drives used: [Drives Overview](#), [Exchanges Overview](#)

**Drive SCSI Element ID**

SCSI element ID of the drive location. Applies only to drives in SCSI partitions or libraries. See the product's *Library Guide* for details on how SCSI IDs are assigned. A value of "-1" indicates the drive is not in a SCSI slot. For example, it may be in a SL8500 library, an HLI partition in a SL3000 library, or a slot not allocated to a partition in a partitioned library.

**Drive Serial Number**

Electronic serial number of the drive. \*NO-SERIAL\* indicates it is not known. This field links to the [Drives – Overview](#) screen, detail view, which displays all available details for this drive.

**Drive SNMP Trap Count**

Total drive messages received from the library over the last 30 days. A sudden increase in this number indicates a condition that should be investigated. This field links to the [Drives – Messages](#) screen, list view, which lists SNMP traps for this drive.

**Drive Start Tracking**

Date and time when STA first began tracking this drive serial number.

**Drive Stop Tracking**

Date and time when STA stopped tracking this drive serial number. This is when STA determined the drive serial number no longer exists in any of the monitored libraries and updated the drive status from "missing" to "removed".

**Drive Suspicion Level**

Calculated suspicion level for the drive. Possible values: 0–100. Lower numbers are desirable. The higher the number, the higher the probability the drive needs attention.

**Drive Tray Serial Number**

Serial number of the drive tray, which must be entered manually by an Oracle support representative. Valid entries include alphanumeric characters only; no special characters are allowed. If the entry has not yet been entered, the value is "unknown." This entry is referenced when a [Service Request](#) is submitted.

**Drive Type**

Drive type long description sent by the library. For example, T10000c-Enc, HpUltrium4, and so on. UNKNOWN indicates a broken drive or a drive for which STA cannot determine the type. Type is UNKNOWN for all DLT and SDLT drives, for which STA does not compute health.

**Drive Vendor**

Drive manufacturer

**Drive WWNN**

World Wide Node Name for the drive slot.

**Drive WWPN (Port A)**

World Wide Port Name for drive port A. This is automatically generated by the library controller during library initialization.

**Drive WWPN (Port B)**

World Wide Port Name for drive port B. This is automatically generated by the library controller during library initialization.

**Duplicate Detected**

STA has detected that the volume serial number (VSN or volser) of the media used in the exchange is a duplicate. This alert appears only on the exchange in which the duplicate is detected.

Duplicate volsers occur when two pieces of media with the same media type have the same volser and two different manufacturer serial numbers. If this alert appears multiple times for the same volser, it is likely there is more than one physical media with the same media type and volser label in the tape environment. If it only appears once for the volser, it may be that the volser label from a retired media has been re-used on a new media.

**E****Elevator**

Serial number of the elevator

**Elevator Alert Count**

Total alerts generated for this elevator, based on defined STA alert policies. This field links to the Alerts Overview screen, list view, which lists alerts for this elevator.

**Elevator Count**

Total elevators. Applies to SL8500 libraries only.

**Elevator Identifier**

Unique identifier for the elevator

**Elevator Physical Address**

Library internal address. See [Physical Address](#).

**Elevator Power LED State**

Current state of the elevator power LED. Normal condition is ON. Options are: ON, OFF, or UNKNOWN.

**Elevator SNMP Traps**

Total elevator messages received from the library. A sudden increase in this number indicates a condition that should be investigated.

**Elevator State**

Current elevator state, as reported by the library. Examples are: READY. STA updates this value hourly and as SNMP traps for the elevator are received from the library.

**Encryption Capable**

This field indicates whether the drive is capable of supporting encryption. It does not indicate that the drive has encryption enabled. Additional hardware or software components and configuration on the library or drive may be necessary to actually enable encryption. For example, LTO drives may require an encryption card and must either be enrolled using Library Managed Encryption using the library interface or drive-enrolled encryption using VOP. Refer to the library documentation for more details on enabling encryption.

**Exchange Drive Cleaning Required**

Indicates whether the drive needed cleaning at the time of the exchange. Possible values: Yes or No. Additional detail may be available through the Clean Periodic Alert and Clean Now Alert attributes.

**Exchange Elapsed Time**

Total time the media is involved in the exchange, including transit time immediately before and after the mount. Starts at the beginning of the move to retrieve the media from a media slot and ends when the media is placed in the first available location after removal from the drive. For SL8500 libraries, the first available location after removal from the drive could be an elevator, but for all other libraries, it is always a media slot. Displayed in `hh:mm:ss` format.

**Exchange Encryption Used**

Encryption method used by the drive for the exchange. Available for StorageTek enterprise drives only. Possible values:

- `Encrypted_ANSI_10` – ANSI encryption.
- `Encrypted_Sun_KMS` – Oracle Key Manager (OKM) encryption.
- `Not_Encrypted` – Not encrypted.
- `Unknown` – The drive did not report encryption information.
- Blank (no value displayed) – STA did not receive any encryption information; the value is always blank for ADI/LTO exchanges.

**Exchange End**

Date and time when the exchange completed

**Exchange Library Name**

User-assigned name for the library where the most recent exchange occurred. If the media has been ejected, you can use this value to determine the library from which the media was ejected. Enables reporting of library information if the media has been ejected.

**Exchange Mount Time**

Total time the media is mounted in the drive. Includes the total time between the start of the mount and the start of the dismount. Does not include transit time before and after the mount. Displayed in `hh:mm:ss` format.

If this attribute is blank, then it is likely that STA did not receive all the exchange data from the library.

**Exchange Read Margin**

Amount of error correction code (ECC) read margin remaining on the media, as reported by the drive during the last mount. Reported as a percentage. A high value is desirable. Available only for StorageTek T10000C and T10000D drives.

If STA determines that this value has gone below a threshold for this drive type, the Exchange Read Marginal attribute is set to True.

The Exchange Read Margin graph on the Drives – Overview and Media – Overview screens shows a system average over time for all drives. Because not all drive types report read margin, the system average may vary significantly over time, depending on which drives had exchange activity during the reported period. If there are no exchanges for T10000C and T10000D drives on a given date, the value is set to zero for that day.

**Exchange Read Marginal**

Indicates whether the drive met the read margin standard for the drive type. Possible values: True or False. Available only for StorageTek T10000C and T10000D drives.

**Exchange Recording Technique**

Recording format used by the drive during the exchange or media validation. For Exchanges Overview, options include: T10000D, LTO5, and 9840B.

For Media Validation Overview, options are: T10000A, T10000B, T10000C, and T10000D only. T10000A and T10000B drives can write to T10000T1 media; T10000C and T10000D drives can write to T10000T2 media.

**Exchange Start**

Date and time when the drive was reserved for the exchange, cleaning activity, or media validation activity. This field links to the Exchanges Overview screen, detail view, which displays all available detail for this exchange.

**Exchange Tape Alerts – Info**

Number of Informational tape alerts received in the exchange.

**Exchange Tape Alerts – Severe**

Number of Severe tape alerts received in the exchange.

**Exchange Tape Alerts – Warning**

Number of Warning tape alerts received in the exchange.

**Exchange Write Efficiency**

Write efficiency for the exchange, based on capacity over distance. Reported as a percentage. A high value is desirable. Available only for StorageTek T10000C and T10000D drives.

If STA determines that this value has gone below a threshold for this drive type, the Exchange Write Inefficient attribute is set to True.

The Exchange Write Efficiency graph on the Drives – Overview and Media – Overview screens shows a system average over time for all drives. Because not all drive types report write efficiency, the system average may vary significantly over time, depending on which drives had exchange activity during the reported period. If there are no exchanges for T10000C and T10000D drives on a given date, the value is set to zero for that day.

**Exchange Write Inefficient**

Indicates whether the drive failed to meet the write efficiency standard for the drive type. Possible values: True or False. Available only for StorageTek T10000C and T10000D drives.

## F

**Formatted Density Code**

Supported density for the drive, as reported by the SCSI Report Density Support command.

## H

**HLI Address**

For media slots, format is *l, p, w, c*, where:

- *l* =logical storage manager (LSM) number. Possible values are 0, 1, 2, or 3.
- *p* =panel number.
- *r* =row number.
- *c* =column number.

For drives, format is *l, p, t*, where:

- *l* =logical storage manager (LSM) number. Possible values are 0, 1, 2, or 3.
- *p* =panel number
- *t* =transport number

**Host DB Sync Errors**

Total host database synchronization errors.

**Host Request Timeouts**

Total host requests that ended in timeouts.

**HP Device Status**

Four-byte hexadecimal code indicating the status of the drive. Available for HP drives only.

**HP Media Status**

Four-byte hexadecimal code indicating the status of the media. Available for HP media only.

## I

**IBM Drive Efficiency (Hex)**

Three-byte hexadecimal code indicating the drive's efficiency over its life. Possible values are 01h (best) to FFh (worst); 00h indicates the efficiency is unknown. Available for IBM LTO-4 and above drives only.

**IBM Media Efficiency (Hex)**

Three-byte hexadecimal code indicating the media's efficiency over its life. Possible values are 01h (best) to FFh (worst); 00h indicates the efficiency is unknown. Available for IBM LTO-4 and above drives only.

**Interface Name**

Interface type of the device associated with the event.

## L

**Last Automated Bundle Created**

Date and time when the most recent automatic log bundle was created for this library component. This attribute is updated only if Automatic Bundle Creation is enabled in STA.

**Last Auto Bundle Sent to SDP**

Date and time when the most recent automatic log bundle for this library component was sent to StorageTek Service Delivery Platform (SDP). This attribute is updated only if Automatic Bundle Creation and Send to SDP are both enabled in STA.

**Last CAP Message**

Current condition of the CAP as reported directly by the library. Options are: DEGRADED, NORMAL, NOTOPERATIVE, UNKNOWN.

**Last Drive Message**

Current condition of the drive as reported directly by the library. Updated whenever messages for the drive are received by STA from the library. This attribute is not to be confused with the drive health calculated by STA; see [Drive Health](#) for comparison.

Possible values:

- DEGRADED – The drive has experienced an error.
- NORMAL – The drive is functioning normally.
- NOTOPERATIVE – The library has lost communication with the drive, or the drive has experienced an error or mechanical failure.
- UNKNOWN – STA has not received any messages for the drive. This is the default value until the first message is received for the drive.

**Last Elevator Message**

Current condition of the elevator as reported directly by the library. Options are: DEGRADED, NORMAL, NOTOPERATIVE, UNKNOWN.

**Last Exchange Start**

Date and time when the drive was reserved for the most recent exchange. This field links to the Exchanges Overview screen, detail view, which displays all available details for this exchange.

**Last Library Message**

Current condition of the library as reported directly by the library. Updated whenever messages for the library top-level state are received by STA from the library. Possible values:

- DEGRADED – The library has experienced an error.
- NORMAL – The library is functioning normally.
- NOTOPERATIVE – The library is not operating.
- Null (no value displayed) – STA has not received any messages from the library. This is the default value until the first message is received for the library.

**Last T10000 MV Qualification Quality Index**

Quality Index is calculated during the most recent drive qualification in which this media was used. The quality index is a measure of the amount of error correction left on the media. A higher value is desirable.

Provided only for T1000T2 media that has been assigned as the primary or secondary calibration media for a validation drive and the drive firmware supports TTI 5.4.

**Last LTO MV Qualification RQ**

The read quality from the last qualification done as a result of an LTO media validation.

**Last PTP Message**

Current condition of the pass-through port (PTP) as reported directly by the library. Applies to SL8500 libraries only. Options are: DEGRADED, NORMAL, NOTOPERATIVE, UNKNOWN.

**Last Robot Message**

Current health of the robot as reported by the library. Options are: DEGRADED, NORMAL, NOTOPERATIVE, UNKNOWN. This attribute is not to be confused with the robot health computed by STA; see [Robot Health](#) for comparison. This attribute is updated only on completion of a library data collection. Regular data collections are done automatically, or you may initiate a manual data collection at any time.

**Library**

Library frame serial number. This field links to the Libraries – Overview screen, detail view, which displays all available details for this library.

**Library Alert Count**

Total alerts generated for this library, based on defined STA alert policies. This field links to the Alerts Overview screen, list view, which lists alerts for this library.

**Library Complex**

Name assigned to the complex by STA.

- For SL150, SL500, and SL3000 libraries, this value is formatted as `library_model_library_serial_number`. Examples: SL150\_262960B+1234BA0018, SL500\_522000001839, SL3000\_571000020075
- For SL8500 libraries, this value is formatted as `library_model_complex_ID`. Examples: SL8500\_1, SL8500\_4

This field links to the Libraries – Complexes Overview screen, detail view, which displays all available details about this complex. See "Library Complexes Screen".

**Library Complex Alert Count**

Total alerts generated for this library complex, based on defined STA alert policies. This field links to the Alerts Overview screen, list view, which lists alerts for this complex.

**Library Complex Name**

Name assigned to the complex by STA. This field links to the Libraries – Complexes Overview screen, detail view, which displays all available details about this complex.

- For SL150, SL500, and SL3000 libraries, this value is formatted as `library_model_library_serial_number`. Examples: SL150\_262960B+1234BA0018, SL500\_522000001839, SL3000\_571000020075



For these library models, because the attribute value includes the library serial number and there can be only one library per complex, the Library Complex Name for each library is always unique and does not change.

- For SL8500 libraries, this value is formatted as *library\_model\_complex\_ID*.  
Examples: SL8500\_1, SL8500\_4

For SL8500 libraries, the attribute value is unique for each complex, but because a complex can include multiple libraries, multiple libraries can share the same Library Complex Name. The value assigned to a library changes if the library is moved from one complex to another.

### **Library Complex Number**

Library complex ID, as configured on the library. For SL150, SL500, and SL3000 libraries, the value is always "1". For SL8500 libraries, the value is set by your Oracle support representative and must be unique for each complex.

### **Library Firmware Updated**

Date and time of last library firmware update.

### **Library Firmware Version**

Current library firmware version.

### **Library IP address #1**

IP address of the public port on the library. The attribute value is specified by the user or administrator when the library connection is configured. For SL150 libraries, it is the Network Port 1 port; for SL500 libraries, it is the 1B port; for SL3000 and SL8500 libraries, it is the 2B port. For SL3000 and SL8500 libraries using the Redundant Electronics feature, this should be the 2B port on the active controller card.

### **Library IP address #2**

The attribute value is specified by the user or administrator when the library connection is configured. For and SL150 and SL500 libraries, this attribute is always blank. For SL3000 and SL8500 libraries, this entry enables STA to maintain uninterrupted SNMP communications with the library if either a Redundant Electronics switch or a Dual TCP/IP failover occurs, and it may be any of the following:

- For libraries with the Redundant Electronics feature, it is the IP address of the 2B port on the alternate (standby) controller card.
- For libraries with the Dual TCP/IP feature, it is the IP address of the 2A port on the active controller card.
- For libraries with both features, it may be either of the above, depending on what the user or administrator has specified. See the *STA Installation and Configuration Guide* for detailed instructions on configuring the libraries for STA.
- For libraries with neither of these features, this attribute is blank.

### **Library Last Booted**

Date and time the library was last rebooted. Provided only for SL150 and SL500 libraries.

### **Library Messaging Health**

Indicates whether STA is receiving SNMP traps from the library. Possible values: GOOD, EVALUATE, ACTION.

### **Library Model**

Library model number. Possible values: SL150, SL500, SL3000, or SL8500.

**Library Name**

User-assigned name for the library. Assigned in the Settings – SNMP Connections screen.

**Library-native Address**

The addressing scheme used internal to each library and in each library's user interface. This will be the same as the physical address for the SL3000 and SL8500, but will be different than the physical address for the SL150 and SL4000. Refer to the Library Guide for the library model for more information on addressing schemes. Examples for the SL150 and SL4000:

- 2,B,1 (base, 3)
- -2,B,1 (left 1, 2)
- Module 12 Top Drive
- ROTATIONAL Base

**Library Number**

Unique ID assigned to the library.

**Library Scan Completed**

Date and time when the most recent successful library configuration data collection was completed.

**Library Serial Number**

Library frame serial number. This field links to the Libraries – Overview screen, detail view, which displays all available details for this library.

**Library SNMP Traps**

Total SNMP traps received by STA from the library. Includes traps for any of the following: library, drive, CAP or mailslot, and pass-thru port (PTP) status, library environment checks, library logs, library connection tests, and library configuration data collections. This field links to the Libraries – Messages screen, list view, which lists SNMP traps for this library.

**Library WWNN**

Library World Wide Node Name.

**Lifetime Hours Incompatible**

Total head-motion hours during which incompatible media was loaded over the life of the drive.

**Logical Group(s)**

Logical groups to which the drive or media is assigned

**LTO MV Calibration RQ**

The read quality from the last LTO media validation calibration process.

**LTO MV RQ**

Read Quality (RQ) is a measure of how much error correction is left on the media, as calculated from the last exchange or media validation. This value is specific to the exchange, with contributions from both the drive and the media. Read quality is reported as a percentage. A high value is desirable. The value may be blank if: the media validation was interrupted or incomplete, the test was a basic verify, or the media type doesn't apply (for example, the media is T10K).

**LTO Sense Code (Hex)**

The sense code is a hex value provided by the drive to indicate status of an exchange. The drive uses a combination of three values to reflect status: Sense Key, Sense Code (ASC), and Sense Code Qualifier (ASCQ). Refer to the IBM LTO SCSI Reference documentation for definitions of the sense data.

**LTO Sense Code Qualifier (Hex)**

The sense code qualifier is a hex value provided by the drive to indicate status of an exchange. The drive uses a combination of three values to reflect status: Sense Key, Sense Code (ASC), and Sense Code Qualifier (ASCQ). Refer to the IBM LTO SCSI Reference documentation for definitions of the sense data.

**LTO Sense Key (Hex)**

The sense key is a hex value provided by the drive to indicate status of an exchange. The drive uses a combination of three values to reflect status: Sense Key, Sense Code (ASC), and Sense Code Qualifier (ASCQ). Refer to the IBM LTO SCSI Reference documentation for definitions of the sense data.

**M****Maximum CAP Slots**

Total slot capacity of the CAP. For the total slots currently present in the CAP, reflecting any magazines that may have been removed for loading or unloading, see [Current CAP Slots](#).

**MB R/W**

For Complexes Overview and Libraries Overview: Total megabytes read and written by all drives in the library or complex.

For Drives Overview: Total megabytes read and written by the drive.

For Media Overview: Total megabytes read from and written to the media

**MB Read**

For Complexes Overview and Libraries Overview: Total megabytes read by all drives in the library or complex.

For Drives Overview: Total megabytes read by the drive.

For Media Overview: Total megabytes read from the media

**MB Received**

For Complexes Overview and Libraries Overview: Total megabytes uncompressed data received from hosts by all drives in the library or complex.

For Drives Overview: Total megabytes received by the drive from hosts during write operations. This could be compressed or uncompressed megabytes, depending on the host application.

For Media Overview: Total megabytes written to the media from hosts. The data could be compressed or uncompressed megabytes, depending on the host application.

**MB Sent**

For Complexes Overview or Libraries Overview: Total megabytes uncompressed data sent to hosts by all drives in the library or complex.

For Drives Overview: Total megabytes sent by the drive to hosts during read operations. This could be compressed or uncompressed megabytes, depending on whether compression has been enabled on the drive.

For Media Overview: Total megabytes sent from the media to hosts. This could be compressed or uncompressed megabytes, depending on whether compression has been enabled on the drive.

**MB Write**

For Complexes Overview or Libraries Overview: Total megabytes written by all drives in the library or complex.

For Drives Overview: Total megabytes written by the drive.

For Media Overview: Total megabytes written to the media

**Media**

Volume serial number (VSN or volser) assigned to the media by its external label. If the library does not supply the volser, STA provides one composed of Library Serial Number:Physical Address. This field links to the Media – Overview screen, detail view, which displays all available detail for this media.

**Media Alert Count**

Total alerts generated for this media, based on defined STA alert policies. This field links to the Alerts Overview screen, list view, which lists alerts for this media.

**Media Auxiliary Memory Capacity**

Media's total auxiliary memory at the time of manufacture, in bytes

**Media Blank**

Indicates the media has never had data written to it.

**Media Capacity Utilization**

Percentage of the total media capacity that has been used by data. Calculated as:

`Media MB Avail Pre / Media MB Capacity`

**Media Destination HLI Address**

Host Library Interface (HLI) address of the location. Applies only to drives or media slots in HLI partitions or libraries. This address is assigned by the ACSLS or ELS host software. This value is available only for SL8500 libraries with firmware FRS\_7.80 or higher or SL3000 libraries with firmware FRS\_4.0 or higher. For all others, the value is left blank. See [HLI Address](#).

**Media Destination Library Number**

Unique ID assigned to the library.

**Media Destination Physical Address**

Library internal address. See [Physical Address](#).

**Media Destination Rail Number**

Rail number. For SL150, SL500, and SL3000 libraries, this value is always 1. For SL8500 libraries, possible values are 1, 2, 3, or 4.

**Media Destination SCSI Element ID**

SCSI element ID of the destination location. Applies only to drives and media slots in SCSI partitions or libraries. See the product's *Library Guide* for details on how SCSI IDs are assigned.

A value of "-1" indicates the location is not a SCSI slot. For example, it may be in a SL8500 library, an HLI partition in a SL3000 library, or a slot not allocated to a partition in a partitioned library.

**Media Dismounts**

Total dismounts for this media. This field links to the Exchanges Overview screen, which lists this media's exchanges.

**Media Ejected from Library**

Date and time when the media was last ejected from the library through a CAP

**Media Entered Library**

Date and time when the media was last entered into the library through a CAP

**Media EOL Percentage**

Percentage of the media's expected useful life that has elapsed

**Media Exchange Status**

Status of the media upon completion of the exchange, as derived from a variety of factors, including media errors, write efficiency, and read margin. Possible values:

- **CART\_MEM\_FAILURE** – An error has occurred with the cartridge memory; this results in reduced performance.
- **CLEAN\_REQ** – The drive is due for cleaning.
- **DRIVE\_ERROR** – The drive has experienced a hardware or microcode error.
- **ENCRYPT\_ERROR** – An error has occurred with the encryption key management system. This is neither a drive nor media problem, so there is no effect on the suspicion of the drive or media.

Possible causes for this status include the following: compromised network connectivity to the encryption key server; the encryption key server is down; the drive key enrollment has expired and the drive must be re-enrolled; either the drive or the media is not encryption-capable. It may be possible for the drive to read unencrypted media until the encryption issue is resolved.

- **EXPIRED\_CLEAN\_TAPE** – The cleaning media has expired.
- **FAILED\_MOUNT**
- **FATAL\_ERROR** – The media cannot be mounted or is stuck. Possible reasons include a problem with the drive hardware or the media cartridge.
- **FW\_DOWN\_LEVEL** – The drive firmware is downlevel.
- **GOOD** – The exchange completed with no issues.
- **INCOMPLETE\_UNLOAD** – The application requested that the media be unloaded. The drive has detected data still in its buffer and has asked for confirmation from the application.
- **INVALID\_OPERATION** – The host has requested an invalid operation, such as any of the following: mounting media in an incompatible drive; reading from media that is blank; writing on media that is write-protected; attempting to locate a position beyond the beginning or end of the tape.
- **LOAD\_ERROR** – An issue with the media prevented it from being loaded. Possible causes include: a problem with the drive hardware or microcode; a problem with the cartridge leader.
- **LTO\_NON\_ADI\_MODE** –ADI mode has not been enabled on either the library, the drive, or both.
- **MEDIA\_ERROR** – The media cannot be read or written. Possible causes include a problem with the tape medium or the MIR.

- **NON\_DRV\_ERROR** – This is neither a drive nor media problem, so there is no effect on the suspicion of the drive or media. For additional information, check the following: for Enterprise drives, check the exchange fault symptom code (FSC); for LTO drives, check recent tape alerts.

Possible causes for this status are as follows:

\* A Media Write Protect Tape Alert must be set. The host application is attempting to write to media that has been write protected.

\* FSC has been set to 3627, 3629, 362A, or 362B. These FSC codes are set during a "normal operation," which checks that a piece of media is truly blank before labeling it. The host application will perform the following sequence: 1) mount new tape; 2) attempt to check for no label; 3) label the new tape.

- **OTHER\_DRV\_ERROR**
- **OTHER\_ERROR**
- **PERM\_ERROR** – A permanent error occurred on the exchange. This may be the result of a media format error, possibly from a previous exchange.
- **READ\_ERROR** – The media could not be read. Possible causes include: a problem with the drive hardware or microcode; a problem with the media MIR; the media may have been corrupted during a previous mount; the drive and media may be incompatible
- **UNKNOWN** – STA has not received enough exchange data from the library to calculate drive health. It may be that the drive is not supported (LTO-2, for example) or the library firmware is downlevel.
- **UNLOAD\_ERROR** – An error occurred during the unload operation. Possible causes include: a problem writing to the media RFID or MIR; the drive and media may be incompatible.
- **WRITE\_ERROR** – An error occurred during the write operation. Possible causes include: a problem with the drive hardware or microcode; the media may have been corrupted during a previous exchange; the drive and media may be incompatible.

### Media Health

Media health as computed by STA analytics. This value reflects a variety of factors, such as the media's error history, read margin, and write efficiency. It includes all data up to and including the last completed exchange and is updated immediately upon completion of the exchange. STA only receives information about errors detected by a drive while performing read/write activity to the media. STA does not receive information about errors that may occur in the data path or host applications.

Possible values, in order of degrading health:

- **USE** – The media has had no failures or degradation in the last ten exchanges.
- **MONITOR** – The media has had multiple errors; there is a less than 80 percent chance that it needs service.
- **EVALUATE** – The media has had multiple errors; there is a greater than 80 percent chance that it needs service.
- **ACTION** – The media has had an error that requires service.

- UNKNOWN – STA has not received enough data to compute health for the media. This may be due to a variety of factors, including exchanges on unsupported drive models, drives with downlevel firmware, or LTO drives with ADI mode not enabled.

**Media Health Trend**

Trend of media health between the last two exchanges, as computed by STA analytics. Options are: BETTER, UNCHANGED, WORSE.

**Media HLI Address**

Host Library Interface (HLI) address of the location. Applies only to drives or media slots in HLI partitions or libraries. This address is assigned by the ACSLS or ELS host software. This value is available only for SL8500 libraries with firmware FRS\_7.80 or higher or SL3000 libraries with firmware FRS\_4.0 or higher. For all others, the value is left blank. See [HLI Address](#).

**Media Length in Meters**

Length of the media, in meters

**Media Library Name**

User-assigned name for the library. Assigned in the Settings – SNMP Connections screen.

**Media Library Number**

Unique ID assigned to the library.

**Media Library Serial Number**

Library frame serial number. This field links to the Libraries – Overview screen, detail view, which displays all available details for this library.

**Media Life Indicator**

Indicates whether the media has reached the end of its expected useful life. Possible values: EOL, GOOD, UNKNOWN.

**Media Long Type**

Detailed media type as reported by the library. Examples include LtoGen5\_1500GB, LtoGen6\_2.5TB, T10000, T10000T2\_Sport, and T10kUniv\_Cleaning. UNKNOWN indicates media with a missing or unreadable external volume serial number (VSN or volser) label.

**Media Manufacturer**

Media manufacturer. Possible values are "STK" for StorageTek enterprise media, or "LTO" for LTO media.

**Media Manufacturer Date**

Date when the media was manufactured, in `yyyymmdd` format. This date is converted from UTC time to the time zone specified in the user's Preferences settings.

**Media Manufacturer Serial Number**

Media serial number assigned by the manufacturer. STA does not have this information until the media has been mounted in a drive.

**Media MB Avail Post**

Unused media capacity, in megabytes; this value is provided after the exchange completes. Available for StorageTek enterprise drives only. Reported value varies by drive vendor and other factors.

**Media MB Avail Pre**

Unused media capacity, in megabytes; this value is provided before the beginning of the exchange. Available for LTO drives only. Reported value varies by drive vendor and other factors.

**Media MB Capacity**

Maximum media capacity, in megabytes. Reported value varies by drive vendor and other factors.

**Media Physical Address**

Library internal address. See [Physical Address](#).

**Media Rail Number**

Rail number. For SL150, SL500, and SL3000 libraries, this value is always 1. For SL8500 libraries, possible values are 1, 2, 3, or 4.

**Media Slot SCSI Element ID**

SCSI element ID of the slot where the media is located. Applies only to media slots in SCSI partitions or libraries. See the product's *Library Guide* for details on how SCSI IDs are assigned.

A value of "-1" indicates the media is not in a SCSI slot. For example, it may be in a SL8500 library, an HLI partition in a SL3000 library, or a slot not allocated to a partition in a partitioned library.

**Media Slots Activated**

Total media slots activated through hardware activation.

**Media Slots Installed**

Total media slots installed but not necessarily activated for use.

**Media Slots Occupied**

Total slots occupied by media. This count includes media in both activated storage slots and system slots. This field links to the Media – Overview screen, list view, which lists all media for this library.

Although system slots are not intended for long-term storage of data media, they may temporarily contain data media in certain situations. The following are examples of when media monitored by STA may reside in system slots (see the product's *Library Guide* for complete details on the use of system slots).

- Data media may be moved to system slots during a library diagnostic self-test.
- Data media in transit at the time of a Redundant Electronics failover may be moved to system slots.
- Cleaning media may be stored in system slots if a library is using automatic cleaning.

STA updates this attribute only after completing a library data collection. For example, if you enter media through a CAP, you may need to perform a manual data collection or wait for a scheduled collection to complete before this attribute reflects the new media count.

**Media Slots Unoccupied**

Total storage slots with no media. This count only includes activated storage slots.

**Media Source HLI Address**

Host Library Interface (HLI) address of the location. Applies only to drives or media slots in HLI partitions or libraries. This address is assigned by the ACSLS or ELS host



software. This value is available only for SL8500 libraries with firmware FRS\_7.80 or higher or SL3000 libraries with firmware FRS\_4.0 or higher. For all others, the value is left blank. See [HLI Address](#).

**Media Source Library Number**

Unique ID assigned to the library.

**Media Source Physical Address**

Library internal address. See [Physical Address](#).

**Media Source Rail Number**

Rail number. For SL150, SL500, and SL3000 libraries, this value is always 1. For SL8500 libraries, possible values are 1, 2, 3, or 4.

**Media Source SCSI Element ID**

SCSI element ID of the source location. Applies only to drives and media slots in SCSI partitions or libraries. See the product's *Library Guide* for details on how SCSI IDs are assigned.

A value of "-1" indicates the location is not a SCSI slot. For example, it may be in a SL8500 library, an HLI partition in a SL3000 library, or a slot not allocated to a partition in a partitioned library.

**Media Start Tracking**

Date and time when STA first began tracking this volume serial number (VSN or volser). If the volser is used on more than one media, this field reflects the earliest start date available.

**Media Stop Tracking**

Date and time when STA stopped tracking this volume serial number (VSN or volser). This is when STA determined the volser no longer exists in any of the monitored libraries and updated the volser status from "missing" to "removed".

**Media Suspicion Level**

Calculated suspicion level for the media. Possible values: 0–100. Lower numbers are desirable. The higher the number, the higher the probability the media needs attention. The Media Suspicion Level graph on the Media – Overview screen shows the daily system average media suspicion level, which is calculated daily at midnight, STA server time.

**Media Type**

Media type short description. Examples include LTO4, LTO\_CLNU, T10000T1, and T10000T2\_CLN. UNKNOWN indicates media with a missing or unreadable external volume serial number (VSN or volser) label. Type is UNKNOWN for all DLT and SDLT media, for which STA does not compute health.

**Media Write Efficiency**

Write efficiency for all the data on the media, based on capacity over distance. Expressed as a percentage. Computed by comparing how many blocks it took to write the data compared to what it should take.

Available only if the drive firmware supports TTI 5.4.

This attribute is useful in selecting media to be used for drive calibration and qualification.

**Meters Between 2 Most Recent Cleans**

Total megabytes read and written by the drive between the two most recent cleanings.

**Meters since Last Clean**

Total megabytes read and written by the drive since its last cleaning.

**Monitored since**

Date and time when STA started tracking this resource (library, complex, drive, or media).

**Mount R/W MB**

Total megabytes read or written by the drive during the mount

**Mount R/W MB/sec**

Average throughput rate for the drive, in megabytes per second. Calculated as:

```
total MB (read +written) /total seconds mount time
```

This value may be affected by a variety of factors external to the drive, such as robot speed or application behavior—for example, some applications do not dismount media immediately upon completion of read/write operations, causing the drive to be idle for much of the mount. As a result, this value is not likely to represent the drive's maximum potential throughput rate.

**Mount Read MB**

Total megabytes read by the drive during the mount. Some media transactions involve a very small amount of I/O. All values greater than 0.0 and less than 0.1 are displayed as 0.01. A value of 0.0 indicates no I/O.

**Mount Read MB/sec**

Average read rate for the drive, in megabytes per second. Calculated as:

```
total MB read /total seconds mount time
```

This value may be affected by a variety of factors external to the drive, such as robot speed or application behavior—for example, some applications do not dismount media immediately upon completion of read/write operations, causing the drive to be idle for much of the mount. As a result, this value is not likely to represent the drive's maximum potential read rate.

**Mount Received MB**

Total uncompressed megabytes received by the application from the drive during the mount.

**Mount Sent MB**

Total uncompressed megabytes sent from the application to the drive during the mount.

**Mount Write MB**

Total megabytes written by the drive during the mount

**Mount Write MB/sec**

Average write rate for the drive, in megabytes per second. Calculated as:

```
total MB written /total seconds mount time
```

This value may be affected by a variety of factors external to the drive, such as robot speed or application behavior—for example, some applications do not dismount media immediately upon completion of read/write operations, causing the drive to be idle for much of the mount. As a result, this value is not likely to represent the drive's maximum potential write rate.

## MV

**MV Calibration Attempts**

Number of calibrations attempted on the drive during the most recent calibration or qualification cycle. A minimum of two attempts are required for a successful calibration or qualification. Possible values: 0, 1, 2, 3.

**MV Calibration Current State**

Current state of the media relating to drive calibration and qualification. Applies only if the media is assigned to a validation drive as the primary or secondary calibration media. Options include: Assigned, Available, Calibrated, Not Suitable, Media in Calibration, Media in Qualification.

**MV Calibration Date**

Date and time when the media was last used for drive calibration. Available only if the media has been assigned to the calibration media logical group.

**MV Calibration Drive SN**

Serial number of the validation drive that was most recently calibrated or qualified with this media.

**MV Calibration Drive Type**

Drive type of the validation drive that was most recently calibrated or qualified with this media.

**MV Calibration Information**

Information about the most recent calibration or qualification of the drive. Options include: Calibration in progress, Completed.

**MV Calibration Suspicion**

Media Suspicion Level of the most recent drive calibration in which this media was used. Possible values: 0–100. Lower numbers are desirable. The higher the number, the higher the probability the media needs attention. Provided only if the media has been assigned as the primary or secondary calibration media for a validation drive.

**MV Calibration Library Complex**

Name of the library complex in which the most recent drive calibration or qualification was performed using this media.

**MV Calibration Library Model**

Model of the library in which the most recent drive calibration or qualification was performed using this media.

**MV Calibration Library SN**

Serial number of the library complex in which the most recent drive calibration or qualification was performed using this media.

**MV Calibration Number of Wraps**

Total wraps of data present on the media. Calculated based on the Media Type and the MV Calibration MB Used. Used to determine whether the media has enough data to be used for drive calibration and qualification.

**MV Calibration Request**

Indicates the exchange was initiated by STA to fulfill one of the following processes:

- A drive calibration
- A drive qualification
- A Basic Verify performed on calibration media that has no STA history

**MV Calibration Starting Suspicion**

Drive suspicion level reported at the start of the most recent calibration of the drive. Possible values: 0–100. Lower numbers are desirable. The higher the number, the higher the probability the drive needs attention.

**MV Calibration State**

State of the most recent drive calibration or qualification performed on the drive.

Options are:

- For both drives and media – Calibrated, Not calibrated, Not Suitable, Offline, Drive Calibration Needs Media, Media Make History.
- For drives only – Drive In Calibration 1, Drive In Calibration 2, Drive In Qualification 1, Drive In Qualification 2.
- For media only – Media In Calibration, Media In Qualification.

**MV Calibration Status Information**

Information about the current validation status of the media. Available only if the media has been assigned to the calibration media logical group.

**MV Count**

Total validations performed on the media.

**MV Days Since Last Validation**

Number of days since the media was last validated based on the last validation time. Null if the media has not yet been validated.

**MV Quality Index (for T10000)**

The quality index is computed by STA based on the results of the media validation. The quality index is a measure of the amount of error correction left on the media. This value is specific to the media and, by factoring out the drive's contribution. Provided only for validations involving T10000T2 media and validation drives with firmware supporting TTI 5.4.

The Quality Index is reported as a percentage, and a higher value is desirable. It is not computed in the following situations:

- The validation is a Basic Verify.
- The Media Type of the validated media is T10000T1.
- The validation results in an media validation Perm Status of True.
- The validation results in an Invalid MIR error.

**MV Drive Allocated**

Indicates the drive has been assigned to the media validation drive pool through SL Console.

**MV Drive Available**

Indicates the drive is currently available to perform media validation exchanges, as determined by STA analytics. If this attribute is blank, the drive does not meet minimum requirements for STA media validation.

**MV Drive Calibrated**

Date and time when the drive was most recently calibrated.

**MV Drive Capable**

Indicates STA can use this drive for validation activities. The drive has been assigned to a media validation drive pool through SL Console and has a Drive Type and Drive Firmware Version that support STA media validation.

**MV Drive In Use**

Indicates the validation drive is currently in use by STA, another application, or diagnostics operations.

**MV Drive Reserved**

Indicates the validation drive is reserved by STA for use in a media validation.

**MV Estimated Time Remaining**

Estimated time remaining on the media validation as reported by the drive. The value is updated periodically. Available only for in-progress validations.

**MV Incomplete**

Indicates the validation has not completed. The validation may be pending or in-process. Options are True or False.

**MV Initiator**

Software application or device used to initiate the media validation activity. Options are: DRIVE, HOST, LIBRAY, SLC, STA.

**MV Interrupted**

The media validation operation could not begin or has been interrupted. See the [MV Status Information](#) and [MV Recommendation](#) attributes for additional information.

Options are True or False. A True status may occur in the following situations:

- The validation was interrupted by a host request for the media or manually canceled while in process.
- The validation could not begin. Possible reasons include: the drive and media types do not match; the media is encrypted, but the validation drive is not encryption capable; the drive has timed out because of a network or other system error.

You may need to restart or resume the media validation request depending on the situation.

**MV Last Activity**

Start date and time of the most recent media validation. For Drives – Overview, this is the most recent validation performed by the drive. For Media – Overview, this is the most recent validation performed on the media.

**MV Last Calibration Quality Index**

The Quality Index reported upon completion of the most recent drive calibration. The Quality Index is a measure of the amount of error correction left on the media. A higher value is desirable.

Provided only for validations involving T10000T2 media and validation drives with firmware supporting TTI 5.4.

**MV Last Qualification Start**

Start date and time of the most recent qualification of the drive.

**MV Last Recommendation**

Recommended user action for the most recently completed media validation. Determined by STA analytics, based on the results of the validation. Examples include: "Media OK: Continue using"; "Corrupted MIR: Rebuild MIR and Re-run Media Validation"; "Migrate the data and scratch the tape".

**MV Last Recording Technique**

Exchange Recording Technique used by the drive during the most recent calibration or qualification performed with this media.

**MV Last State Update**

Date and time when the status of this media validation was last updated. Updated whenever there is a change to the MV Request State.

**MV Last Test Type**

Type of verification test performed during the most recent validation on this media.

**MV Library Error**

Library event code for a library error that occurred during the media validation. A value indicates an operational issue with the media validation that prevented the test from completing; it does not imply there are issues with the media itself. You can display the library event codes through the SL Console; see the *SL8500 Library Guide* for details.

**MV MB Tape Used**

Total amount of data that has been written to the media as determined by the drive during drive calibration. Used with the Media Type to calculate the MV Calibration Number of Wraps for the media.

**MV Policy Name**

User-defined name assigned to the media validation policy.

**MV Pool End Date**

Date the media was no longer eligible for use in calibration. Possible reasons are as follows; see the [Configure Drive Calibration and Qualification](#) for additional details about calibration media qualifications.

- The media was removed from the calibration media logical group.
- The media has been disqualified from calibration.
- New data has been written to the media, invalidating any prior calibration information.
- The media was removed from the tape library system.

**MV Pool Start Date**

Date the media was added to the calibration media logical group.

**MV Primary Calibration Media**

Indicates this media is assigned to a validation drive as the primary calibration media. Possible values: True or False (blank).

- For primary calibration media, this attribute is True and the MV Calibration Drive SN attribute indicates the drive it is assigned to.
- For secondary calibration media, this attribute is False and the MV Calibration Drive SN attribute indicates the drive it is assigned to.
- For media not used for drive calibration, this attribute is False and there is no MV Calibration Drive SN entry.

**MV Primary Qualification Start**

Start date and time of the most recent qualification of the drive using the primary calibration media.

**MV Priority Order**

Order in which media validation requests are processed in the queue. Applies only to pending and in-process requests. This value is blank for completed validations.

**MV Recommendation**

Recommended user action determined by STA analytics based on the results of the media validation. Provided only for completed validations. Examples include: "Media OK: Continue using"; "Corrupted MIR: Rebuild MIR and Re-run Media Validation"; "Migrate the data and scratch the tape"; "Disposition Drive".

**MV Request Start**

Date and time when the media validation request was placed in the MV queue. Depending on the source of the request, this is either the time the MV request was initiated by STA, or the time STA recognized the request initiated by another application.

**MV Request State**

Status of the media validation request. Examples are: Completed, Error, In-Progress - Stop Requested, Interrupted, Pending, Starting, Unknown.

See [MV Interrupted](#), [MV Recommendation](#), [MV Status Information](#) for additional information about validations with issues.

**MV Result**

Final result of the media validation as determined by STA analytics upon successful completion of the verification test. This attribute applies to the quality of the data on the media.

Options are: DEGRADED, FAILED, USE, UNKNOWN. The value is UNKNOWN if the validation was interrupted or did not complete successfully.

**MV Secondary Qualification Start**

Start date and time of the most recent qualification of the drive using the secondary calibration media.

**MV Status Information**

Provides information about issues with the media validation request. The information may explain the problem or suggest corrective action to take. This attribute is usually blank.

Examples include: "Waiting for drive; all drives in use." and "Incompatible tape format for drive."

A value of "Drive Timeout; MDV manager cancel" indicates STA requested the library to return the media to a media slot because the validation took longer than it should have and timed out. This is usually the result of a library operational error. If the Read Percentage attribute for the validation exchange is less than 100 percent, then the validation did not complete. If this status recurs for the media, there is probably an issue with the media; if it recurs for the drive, there is probably an issue with the drive.

**MV Test Percentage**

Percentage of the verification test that has been completed during this media validation. The value is updated periodically for in-progress validations. A value of 100 indicates the test completed successfully. If the test was interrupted, the value remains less than 100.

**MV Test Type**

Indicates the type of verification test performed during the media validation. Examples are: Basic Verify, Cancel Validation, Complete Verify Plus, Standard Verify, Verify and Rebuild MIR.

**MV Time Spent Validating**

Total time the media validation has taken, as reported by the drive. The time starts when the validation test begins on the drive and ends when the test is complete. For in-progress validations, the value is updated periodically. For pending validation requests, the value is null.

## N

**New Property Effective**

Date and time when the new property value is effective.

**New Property Value**

New value assigned to the property.

## P

**Partition Name**

Unique name assigned to the partition by STA. Includes the library-assigned partition number. Formatted as:

```
Library Complex Name:Partition Type:Partition Number
```

**Partition Number**

Unique partition ID assigned on the library. For nonpartitioned libraries, the value is always "0". For partitioned libraries, possible values are 1–8.

**Partition Type**

Type of host-partition connection. Possible values:

- HLI – HLI (Host Library Interface) protocol
- OTHER – System cells, used for storage of diagnostic media.
- SCSI – SCSI protocol

**Partitions**

Total number of user-defined partitions in the complex or library. The maximum number of partitions per library is eight, and per complex, it is 16.

This count does *not* include the following:

- System partitions—for storage of cleaning and diagnostic media.
- Empty partitions—partitions with no storage slots, drive bays, or CAPs. SL Console allows you to create empty partitions to reserve the partition number for later use.



Partitions for SL8500 complexes can extend across libraries. In such cases, the libraries in the same complex must all have the same partition count. For example, complex SL8500\_1 includes 10 libraries and 4 partitions. On the Complexes Overview screen, the Partitions value for complex SL8500\_1 is "4," and on the Libraries Overview screen, the Partition count for each of the 10 libraries in the complex is also "4."

**Perm Read Errors**

Number of permanent read errors

**Perm Write Errors**

Number of permanent write errors

**Permanent Error**

Indicates the exchange resulted in a permanent error. Available only if the drive firmware supports TTI 5.4. Options are True or False.

This status could be the result of an operational error, a bad drive, or bad media. For media validation exchanges, in most cases when this value is True, the MV Result is Unknown.

**Port Speed (Port A)**

Connection speed of Drive Port A as reported by the library. Possible values are as follows:

- A specific value (for example, FC-8Gb or SAS-3Gb)—Indicates the port has been initialized and the speed has been assigned.
- Auto—Indicates the speed is auto-negotiated between the drive and the switch.
- Unknown—Indicates the library does not have enough information, possibly because the port is not configured or does not exist.
- Null—Indicates the port does not exist. For example, if the drive has only one port, the value for Port B is null.

**Port Speed (Port B)**

Connection speed of Drive Port B as reported by the library. Possible values are as follows:

- A specific value (for example, FC-8Gb or SAS-3Gb)—Indicates the port has been initialized and the speed has been assigned.
- Auto—Indicates the speed is auto-negotiated between the drive and the switch.
- Unknown—Indicates the library does not have enough information, possibly because the port is not configured or does not exist.
- Null—Indicates the port does not exist. For example, if the drive has only one port, the value for Port B is null.

**Property Name**

Device property being changed.

**PTP**

Unique identifier of the pass-through port (PTP). Applies to SL8500 libraries only.

**PTP Alert Count**

Total alerts generated for this PTP, based on defined STA alert policies. This field links to the Alerts Overview screen, list view, which lists alerts for this PTP.

**PTP Count**

Total pass-through ports (PTPs). Applies to SL8500 libraries only.

**PTP Ejects**

Total media ejected through all pass-through ports (PTPs) over the last 30 days. Applies to SL8500 libraries only; all other libraries show 0.

**PTP Enters**

Total media entered through all pass-through ports (PTPs) over the last 30 days. Applies to SL8500 libraries only; all other libraries show 0.

**PTP Identifier**

Unique identifier for the pass-through port (PTP)

**PTP Physical Address**

Library internal address of the pass-through port (PTP). Applies to SL8500 libraries only. The format is  $l, r, c, s, w$  (for example,  $1, 1, -6, 1, 0$ ), where:

- $l$  =library number. For nonpartitioned libraries, this is the library ID; for partitioned libraries, this is the partition ID (1–8).
- $r$  =rail number. For SL8500 libraries, possible values are 1, 2, 3, or 4.
- $c$  =column number. For PTPs, this value is always -6.
- $s$  =side number. For PTPs, this value is always 1.
- $w$  =row number. For PTPs, this value is always 0.

**PTP Power LED State**

Current state of the pass-through port (PTP) power LED. Normal condition is ON. Options are: ON, OFF, or UNKNOWN.

**PTP SNMP Traps**

Total pass-through port (PTP) messages received from the library. A sudden increase in this number indicates a condition that should be investigated.

**PTP State**

Current pass-through port (PTP) state, as reported by the library. Applies to SL8500 libraries only. Examples are: READY. STA updates this value hourly and as SNMP traps for the PTP are received from the library.

**Physical Address**

For SL150 libraries, the format is  $m, s, w, c$  (for example,  $1, Left, 1, 2$ ), where:

- $m$  =module number; 1–10, from top (base module) to bottom
- $s$  =side; Left or Right
- $w$  =row number; 1–3, from top to bottom
- $c$  =column number; 1–5, from front to back

For SL500 libraries, the format is  $l, m, r, c$  (for example,  $0, 2, 2, 3$ ), where:

- $l$  =for nonpartitioned libraries, this is the library ID (always 0); for partitioned libraries, this is the partition ID (1–8).
- $m$  =module number; 1–5, from top to bottom of the rack
- $r$  =drive row number; 1–2 (Base Module) or 1–4 (Drive Expansion Module), from top to bottom of the module

- `c` =column number; always 9 for drives

For SL3000 and SL8500 libraries, the format is `l, r, c, s, w` (for example, `1, 1, 2, 2, 3`), where:

- `l` =library number. For nonpartitioned libraries, this is the library ID; for partitioned libraries, this is the partition ID (1–8).
- `r` =rail number. For SL3000 libraries, this value is always 1. For SL8500 libraries, possible values are 1, 2, 3, or 4.
- `c` =column number.
- `s` =side number.
- `w` =row number.

## R

### **R/W MB/sec**

Throughput rate for the time spent actively reading and writing; idle time is excluded. Expressed in megabytes per second. Available for StorageTek enterprise drives only. Calculated as:

```
(compressed MB read +compressed MB written) / (read time +write time)
```

### **R/W Mount Ratio**

Ratio of read and write time to total mount time. Displayed as a percentage. A value close to 1.0 indicates the drive is active over the entire mount. Available for StorageTek enterprise drives only.

Calculated as:

```
(read time +write time) /total mount time
```

### **Read Margin**

Amount of error correction code (ECC) read margin remaining on the media, as reported by the drive during the last mount. Reported as a percentage. A high value is desirable. Available only for StorageTek T10000C and T10000D drives.

If STA determines that this value has gone below a threshold for this drive type, the Exchange Read Marginal attribute is set to True.

### **Read MB/sec**

Read rate for the time spent actively reading; idle time is excluded. Expressed in megabytes per second. Available for StorageTek enterprise drives only.

Calculated as:

```
compressed MB read /total read time
```

### **Read Mount Ratio**

Ratio of read time to total mount time. Calculated as:

```
read time /total mount time
```

### **Read Quality (RQ)**

Measure of how much error correction is left on the media, as calculated from the last exchange or media validation. This value is specific to the exchange, with contributions from both the drive and the media. Read quality is reported as a percentage. A high value is desirable.

**Received on**

Date and time when the STA server received the SNMP trap from the library.

**Recorded on**

Date and time when the exchange started.

**Repositioning Cycles**

Total times the media was repositioned for any reason

**Repositioning Cycles Non ERP**

Total times the media was repositioned due to non-ERP (error recovery process) reasons, such as data overrun or underrun.

**Request ID**

Unique ID for the SNMP request.

**Result Code**

Device result code for the event.

**Robot**

Serial number of the robot

**Robot Alert Count**

Total alerts generated for this robot, based on defined STA alert policies. This field links to the Alerts Overview screen, list view, which lists alerts for this robot.

**Robot Count**

Total number of robots

**Robot Get Retries**

Total robot *get* retries

**Robot Get Totals**

Total robot media *get* actions

**Robot Health**

Current health of the robot as calculated by STA. Options are: ACTION, ERROR, EVALUATE, MONITOR, USE, UNKNOWN. This attribute is not to be confused with the robot status reported by the library; see [Last Robot Message](#) for comparison. This attribute is updated only on completion of a library data collection. Regular data collections are done automatically, or you may initiate a manual data collection at any time.

**Robot Identifier**

Unique identifier for the robot

**Robot Physical Address**

Library internal address. See [Physical Address](#).

**Robot Power LED State**

Current state of the robot power LED. Normal condition is ON. Options are: ON, OFF, or UNKNOWN.

**Robot Put Retries**

Total robot media *put* retries

**Robot Put Totals**

Total robot media *put* actions

**Robot SNMP Traps**

Total robot messages received from the library. A sudden increase in this number indicates a condition that should be investigated.

**Robot State**

Current robot state, as reported by the library. Options are: EMPTY, ERROR, INOPERATIVE, NOT POWERED, NOT INSTALLED, or READY. STA updates this value hourly. Additionally for SL3000 and SL8500 libraries, the value is updated as SNMP traps for the robot are received from the library.

**S****Severity**

Severity of the event.

**Servo Perm Errors**

Number of permanent servo errors

**SNMP Trap**

Type of SNMP trap. Options are:

- CAP
- Drive
- Heartbeat
- Library Environment Check
- Library Log
- Library Status
- PTP
- SNMP Agent Start

**STA Start Tracking**

For Drives Overview: Date and time when STA first began tracking this drive serial number.  
For Media Overview: Date and time when STA first began tracking this volume serial number (VSN or volser). If the volser is used on more than one media, this field reflects the earliest start date available.

**STA Stop Tracking**

For Drives Overview: Date and time when STA stopped tracking this drive serial number. This is when STA determined the drive serial number no longer exists in any of the monitored libraries and updated the drive status from "missing" to "removed".  
For Media Overview: Date and time when STA stopped tracking this volume serial number (VSN or volser). This is when STA determined the volser no longer exists in any of the monitored libraries and updated the volser status from "missing" to "removed".

**STA Supported**

Indicates the media meets the minimum requirements for STA analytics. Possible values: True or False. The following media types usually have a value of True.

- StorageTek T1000T1 and higher
- StorageTek 9840
- LTO-3 and higher

STA tracks media for which this value is False, but it is not able to perform full analytics on them because it receives only minimal data about them. See the requirements in the *STA Installation and Configuration Guide* for details about supported media.

## T

### **T10000 Exchange DSC (Hex)**

Data status code (DSC) for the exchange. Available only for drives whose firmware supports TTI 5.40+.

### **T10000 Exchange FSC (Hex)**

Four-byte hexadecimal fault symptom code (FSC). For example, FD55, S053, and so on. Reported only if an error occurred during the exchange.

### **T10000 MV Calibration Quality Index**

The Calibration Quality Index calculated during most recent drive calibration in which this media was used. Data quality is a measure of the amount of error correction left on the media. A higher value is desirable.

Provided only for T10000T2 media assigned to the calibration media logical group and the validation drive firmware supports TTI 5.4.

### **T10000 MV Quality Index**

The Quality Index is a measure of how much error correction is left on the media, as calculated from the last exchange or media validation. This value is specific to the exchange, with contributions from both the drive and the media. Read quality is reported as a percentage. A high value is desirable. The value may be blank if: the media validation was interrupted or incomplete, the test was a basic verify, or the media type doesn't apply (for example, the media is LTO).

### **Text**

Additional text regarding the event, sent by the subsystem.

### **Theoretical Maximum Usage Count**

Manufacturer's recommended usage limit for the cleaning media. Not available for all media and drive types. This value may show as "0" or blank, which should be interpreted as not available or unknown.

### **Time Spent Loaded**

Total time during this exchange that the drive has tension on the media. Does not include the time required to thread the media.

### **Time Spent Mounting**

Total time during this exchange that the media was mounted in the drive. Does not include time spent loading and unloading the media.

### **Time Spent R/W**

Total time the drive spent reading and writing data during the exchange

**Time Spent Reading**

Total time the drive spent reading data during the exchange

**Time Spent Writing**

Total time the drive spent writing data during the exchange

**Total Host Requests**

Total host requests received by this library or complex.

**Trap Type**

Entity type to which the trap pertains. One of the following:

- CAP – CAP, AEM, or mailslot status
- Drive – Drive status
- Heartbeat
- Library Environment Check
- Library Log
- Library Status

## U

**Unload Errors**

Number of permanent unload errors

**Usage Perm Errors**

Number of unknown usage errors

**Username**

STA username associated with the event.

**Volume Serial Number**

Volume serial number (VSN or volser) assigned to the media by its external label. If the library does not supply the volser, STA provides one composed of `Library Serial Number:Physical Address`. This field links to the Media – Overview screen, detail view, which displays all available detail for this media.

## W

**WORM/VolSafe Media**

Indicates whether the media uses StorageTek VolSafe technology. STA does not know the status until the media has been mounted. Possible values: Yes or No. Blank indicates unknown.

**Write Efficiency**

Write efficiency for the exchange, based on capacity over distance. Reported as a percentage. A high value is desirable. Available only for StorageTek T10000C and T10000D drives.

If STA determines that this value has gone below a threshold for this drive type, the Exchange Write Inefficient attribute is set to True.

The Exchange Write Efficiency graph on the Drives – Overview and Media – Overview screens shows a system average over time for all drives. Because not all drive types report write efficiency, the system average may vary significantly over time, depending on which

drives had exchange activity during the reported period. If there are no exchanges for T10000C and T10000D drives on a given date, the value is set to zero for that day.

**Write MB/sec**

Write rate for the time spent actively writing; idle time is excluded. Expressed in megabytes per second. Calculated as:

compressed MB written /total write time

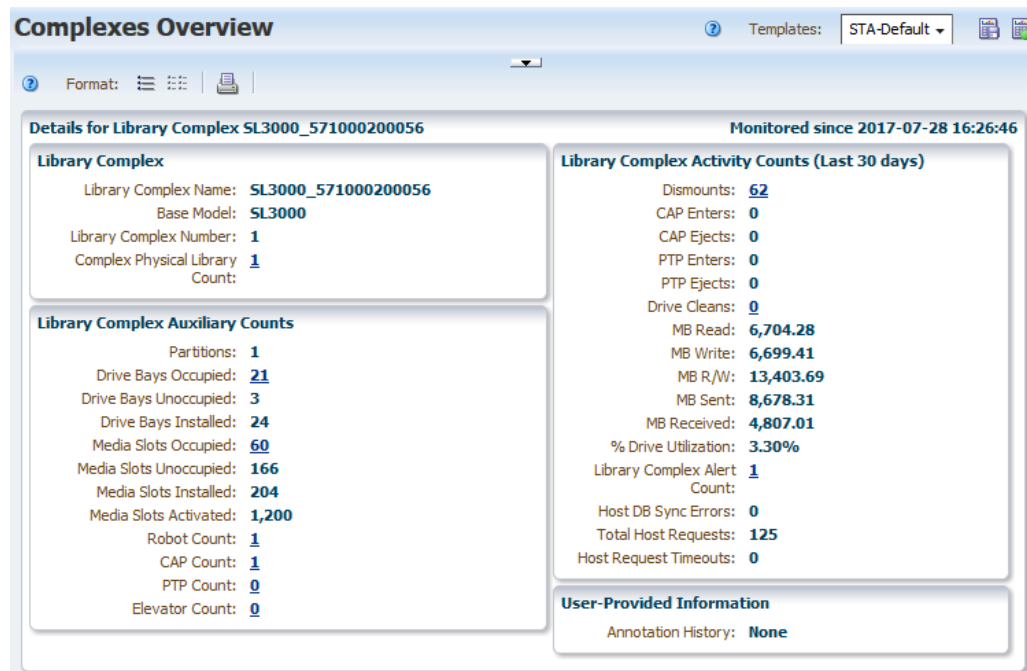
**Write Mount Ratio**

Ratio of write time to total mount time. Calculated as:

write time /total mount time

## Data Reference: Complexes Overview

The Complexes Overview screen shows attributes related to one or more selected library complexes.



**Title**

STA assigns values for these attributes when it first starts tracking the library complex.

- [Library Complex](#)
- [Monitored since](#)

**Library Complex**

These attributes are rolled up for all libraries that share the same complex ID. These attributes come directly from the libraries and are updated with each library configuration data collection.



- Library Complex Name
- Base Model
- Library Complex Number
- Complex Physical Library Count

#### **Library Complex Activity Counts (Last 30 days)**

Activity totals for all libraries in the complex over the last 30 days. These are updated with each completed exchange.

- Dismounts
- CAP Enters
- CAP Ejects
- PTP Enters
- PTP Ejects
- Drive Cleans
- MB Read
- MB Write
- MB R/W
- MB Sent
- MB Received
- % Drive Utilization
- Library Complex Alert Count
- Host DB Sync Errors
- Total Host Requests
- Host Request Timeouts

#### **Library Complex Auxiliary Counts**

Total resource counts for all libraries in the complex. The summary fields are updated with each completed exchange. The asset fields are updated with each library data collection.

- Partitions
- Drive Bays Occupied
- Drive Bays Unoccupied
- Drive Bays Installed
- Media Slots Occupied
- Media Slots Unoccupied
- Media Slots Installed
- Media Slots Activated
- Robot Count
- CAP Count

- [PTP Count](#)
- [Elevator Count](#)

**User-Provided Information**

- [Annotation History](#)

## Data Reference: Libraries Overview

The Libraries - Overview screen shows attributes related to one or more selected libraries.

The screenshot displays the 'Libraries - Overview' interface for Library 571000200056. The interface is divided into several sections:

- Details for Library 571000200056** (Monitored since 2017-07-28 16:26:46):
  - Library**:
    - Library Complex Name: [SL3000\\_571000200056](#)
    - Library Name: [s18500-85](#)
    - Library Number: [1](#)
    - Library Model: [SL3000](#)
    - Library Serial Number: [571000200056](#)
    - Library WWNN: [50:01:04:F0:00:AC:BA:E7](#)
    - Last Library Message: [DEGRADED](#)
    - Last Automated Bundle Created: [2020-01-13 08:32:45](#)
    - Library Messaging Health: [1](#)
    - Library Last Booted: [2019-12-03 14:00:09](#)
    - Library Firmware Updated: [FRS\\_4.54c](#)
    - Library Firmware Version: [FRS\\_4.54c](#)
    - Library IP address #1: [10.80.50.85](#)
    - Library IP address #2: [2020-01-29 14:09:31](#)
    - Library Scan Completed: [2020-01-29 14:09:31](#)
    - Cumulative Library Uptime: [2020-01-29 14:09:31](#)
  - Library Activity Counts (Last 30 days)**:
    - Library SNMP Traps: [1,958](#)
    - Library Alert Count: [1](#)
    - Dismounts: [62](#)
    - CAP Enters: [0](#)
    - CAP Ejects: [0](#)
    - PTP Enters: [0](#)
    - PTP Ejects: [0](#)
    - Drive Cleans: [0](#)
    - MB Read: [6,704.28](#)
    - MB Write: [6,699.41](#)
    - MB R/W: [13,403.69](#)
    - MB Sent: [8,678.31](#)
    - MB Received: [4,807.01](#)
    - % Drive Utilization: [3.27%](#)
    - Host DB Sync Errors: [0](#)
    - Total Host Requests: [125](#)
    - Host Request Timeouts: [0](#)
  - Library Auxiliary Counts**:
    - Drive Bays Occupied: [21](#)
    - Drive Bays Unoccupied: [3](#)
    - Drive Bays Installed: [24](#)
    - Media Slots Occupied: [60](#)
    - Media Slots Unoccupied: [166](#)
    - Media Slots Installed: [204](#)
    - Media Slots Activated: [1,200](#)
    - Robot Count: [1](#)
    - CAP Count: [1](#)
    - PTP Count: [0](#)
    - Elevator Count: [0](#)
  - User-Provided Information**:
    - Annotation History: [None](#)

**Title**

Values for these attributes are assigned when STA first starts tracking the library.

- [Library](#)
- [Monitored since](#)

**Library**

Details about the library. These attributes come directly from the library and are updated with each library configuration data collection.

- Library Complex Name
- Library Name
- Library Number
- Library Model
- Library Serial Number
- Library WWNN
- Last Library Message
- Last Automated Bundle Created
- Library Messaging Health
- Library Last Booted
- Library Firmware Updated
- Library Firmware Version
- Library IP address #1
- Library IP address #2
- Library Scan Completed
- Cumulative Library Uptime

#### **Library Activity Counts (Last 30 days)**

Activity totals for the library over the last 30 days. These are updated with each completed exchange.

- Library SNMP Traps
- Library Alert Count
- Dismounts
- CAP Enters
- CAP Ejects
- PTP Enters
- PTP Ejects
- Drive Cleans
- MB Read
- MB Write
- MB R/W
- MB Sent
- MB Received
- % Drive Utilization
- Host DB Sync Errors
- Total Host Requests
- Host Request Timeouts

### Library Auxiliary Counts

Library resource counts. The summary fields are updated with each completed exchange. The asset fields are updated with each library data collection.

- [Drive Bays Occupied](#)
- [Drive Bays Unoccupied](#)
- [Drive Bays Installed](#)
- [Media Slots Occupied](#)
- [Media Slots Unoccupied](#)
- [Media Slots Installed](#)
- [Media Slots Activated](#)
- [Robot Count](#)
- [CAP Count](#)
- [PTP Count](#)
- [Elevator Count](#)

### User-Provided Information

- [Annotation History](#)

## Data Reference: Drives Overview

The Drives - Overview screen shows attributes for one or more selected drives.

### What does the Encryption-Cable field mean?

This field indicates whether the drive is capable of supporting encryption. It does not indicate that the drive has encryption enabled. Additional hardware or software components and configuration on the library or drive may be necessary to actually enable encryption. For example, LTO drives may require an encryption card and must either be enrolled using Library Managed Encryption using the library interface or drive-enrolled encryption using VOP. Refer to the library documentation for more details on enabling encryption.

### Sample Screen for an Enterprise Drive

**Drives - Overview**
Templates: STA-Default

Format: [Icons] Applied Filter: MV Drive Allocated True

**Details for Drive 576004003943**

**Drive**

Drive Serial Number: **576004003943**  
 Drive Tray Serial Number: **323232323232**  
 Drive WWNN: **50:01:04:F0:00:8A:AE:30**  
 Drive Type: **T10000c**  
 Drive Health: **MONITOR**  
 Drive Health Trend: **WORSE**  
 Last Drive Message: **UNKNOWN**  
 Last Automated Bundle Created:  
 Drive WWPN (Port A): **50:01:04:F0:00:8A:AE:31**  
 Port Speed (Port A): **Auto**  
 Drive WWPN (Port B): **50:01:04:F0:00:8A:AE:32**  
 Port Speed (Port B): **Auto**  
 Drive Model: **T10000C**  
 Drive Manufacturer: **STK**  
 Encryption Capable: **Yes**  
 Drive Interface: **FIBRE**  
 Drive Properties Updated: **2021-04-06 18:01:38**  
 Drive Firmware Version: **3.69.103-5.50**  
 STA Start Tracking: **2021-04-06 18:01:38**  
 STA Stop Tracking:

**Drive Activity Counts (Last 30 Days)**

% Drive Utilization: **1.00%**  
 Drive Dismounts: **29**  
 Drive SNMP Trap Count: **0**  
 Drive Alert Count: **0**  
 Dismounts with Errors: **2**  
 Cleans: **0**  
 MB Read: **0.00**  
 MB Write: **0.00**  
 MB R/W: **0.00**  
 MB Sent: **0.00**  
 MB Received: **0.00**  
 Avg Mount Read MB/sec: **0.00**  
 Avg Mount Write MB/sec: **0.00**  
 Avg Mount R/W MB/sec: **0.00**  
 Avg Mount Read MB: **0.00**  
 Avg Mount Write MB: **0.00**  
 Avg Mount R/W MB: **0.00**

**Drive Location**

Drive Library Name: **elib18**  
 Drive Library Serial Number: **516000100437**  
 Drive Library Number: **1**  
 Drive Rail Number: **3**  
 Drive Physical Address: **1,3,-2,1,1**  
 Drive Library-native Address: **1,3,-2,1,1**  
 Drive HLI Address:  
 Drive SCSI Element ID: **-1**

**Library Complex**

Library Complex Name: **SL8500\_2**  
 Library Model: **SL8500**  
 Partition Type: **NONE**  
 Partition Name: **SL8500\_2:NONE**  
 Partition Number: **-1**

**Monitored since 2021-04-06 18:01:38**

**Media**

Volume Serial Number: **STA005**  
 Media Manufacturer Serial Number: **71131205012734**  
 Media Health: **MONITOR**  
 WORM/VolSafe Media: **No**  
 Cleaning Media: **No**

**Most Recent Exchange**

Exchange Start: **2021-04-08 03:14:14**  
 Exchange Elapsed Time: **2:20:46**  
 Exchange Mount Time: **2:10:48**  
 Mount R/W MB/sec: **0.00**  
 Exchange Recording Technique: **T10000B**  
 Drive Exchange Status: **DRIVE\_ERROR**  
 Exchange Tape Alerts - Severe: **1**  
 Exchange Tape Alerts - Warning: **4**  
 Exchange Tape Alerts - Info: **1**  
 Data Compression Ratio:  
 Alert: Drive Load Limit: **No**  
 Drive Suspicion Level: **25.00%**  
 Exchange Drive Cleaning Required: **No**  
 Meters Between 2 Most Recent Cleans:  
 Meters since Last Clean: **0**  
 Drive Lifetime Cleans: **0**  
 Drive Lifetime Loads: **46,765**  
 Drive Lifetime Meters: **6,752,419**  
 Drive Lifetime Power Hours: **73,720**

**Additional Exchange Information for Enterprise Drives**

T10000 Exchange FSC (Hex):  
 T10000 Exchange DSC (Hex):  
 Exchange Write Inefficient: **No**  
 Exchange Read Marginal: **No**  
 Exchange Write Efficiency: **100.00%**  
 Exchange Read Margin:  
 Time Spent Reading: **0:00:00**  
 Time Spent Writing: **0:00:00**  
 Time Spent R/W: **0:00:00**  
 Read MB/sec:  
 Write MB/sec:  
 R/W MB/sec:  
 Read Mount Ratio: **0.00%**  
 Write Mount Ratio: **0.00%**  
 R/W Mount Ratio: **0.00%**  
 Exchange Encryption Used: **Not Encrypted**

**Media Validation Information for Enterprise Drives**

MV Calibration Attempts:  
 MV Calibration State:  
 MV Calibration Information:  
 T10000 MV Calibration Quality Index:  
 MV Calibration Starting Suspicion:  
 MV Drive Calibrated:  
 MV Last Activity: **2021-04-08 02:46:14**  
 MV Recommendation: **Media OK: Continue using tape.**  
 MV Drive Allocated: **Yes**  
 MV Drive Capable: **Yes**  
 MV Drive Available: **Yes**  
 MV Drive In Use: **No**  
 MV Drive Reserved: **No**  
 MV Last Qualification Start:  
 MV Primary Qualification Start:  
 MV Secondary Qualification Start:

**User-Provided Information**

Logical Group(s): **None**  
 Annotation History: **None**

## Sample Screen for an LTO Drive

**Drives - Overview** Templates: STA-Default

Format: Applied Filter: MV Drive Allocated True

**Details for Drive 10WT000197** Monitored since 2021-04-06 18:01:38

**Drive**

- Drive Serial Number: **10WT000197**
- Drive Tray Serial Number: **464970G+1730VS0024**
- Drive WWNN: **50:01:04:F0:00:8A:AE:1B**
- Drive Type: **IbmUltrium8**
- Drive Health: **USE**
- Drive Health Trend: **UNCHANGED**
- Last Drive Message: **UNKNOWN**
- Last Automated Bundle Created:
- Drive WWPN (Port A): **50:01:04:F0:00:8A:AE:1C**
- Port Speed (Port A): **Auto**
- Drive WWPN (Port B): **50:01:04:F0:00:8A:AE:1D**
- Port Speed (Port B): **Auto**
- Drive Model: **LTO8**
- Drive Manufacturer: **IBM**
- Encryption Capable: **Yes**
- Drive Interface: **FIBRE**
- Drive Properties Updated: **2021-04-06 18:01:38**
- Drive Firmware Version: **MA70**
- STA Start Tracking: **2021-04-06 18:01:38**
- STA Stop Tracking:

**Media**

- Volume Serial Number: **FM8201**
- Media Manufacturer Serial Number: **EX42XVRFWE**
- Media Health: **USE**
- WORM/VolSafe Media: **No**
- Cleaning Media: **No**

**Most Recent Exchange**

- Exchange Start: **2021-04-08 00:27:00**
- Exchange Elapsed Time: **0:02:49**
- Exchange Mount Time: **0:02:04**
- Mount R/W MB/sec: **0.00**
- Exchange Recording Technique: **LTO8**
- Drive Exchange Status: **GOOD**
- Exchange Tape Alerts - Severe: **0**
- Exchange Tape Alerts - Warning: **0**
- Exchange Tape Alerts - Info: **0**
- Data Compression Ratio:
- Alert: Drive Load Limit: **No**
- Drive Suspicion Level: **0.00%**
- Exchange Drive Cleaning Required: **No**
- Meters Between 2 Most Recent Cleans:
- Meters since Last Clean:
- Drive Lifetime Cleans: **0**
- Drive Lifetime Loads: **620**
- Drive Lifetime Meters: **1,207,607**
- Drive Lifetime Power Hours: **30,930**

**Drive Activity Counts (Last 30 Days)**

- % Drive Utilization: **0.08%**
- Drive Dismounts: **12**
- Drive SNMP Trap Count: **0**
- Drive Alert Count: **0**
- Dismounts with Errors: **0**
- Cleans: **0**
- MB Read: **0.00**
- MB Write: **0.00**
- MB R/W: **0.00**
- MB Sent: **0.00**
- MB Received: **0.00**
- Avg Mount Read MB/sec: **0.00**
- Avg Mount Write MB/sec: **0.00**
- Avg Mount R/W MB/sec: **0.00**
- Avg Mount Read MB: **0.00**
- Avg Mount Write MB: **0.00**
- Avg Mount R/W MB: **0.00**

**Drive Location**

- Drive Library Name: **elib18**
- Drive Library Serial Number: **516000100437**
- Drive Library Number: **1**
- Drive Rail Number: **3**
- Drive Physical Address: **1,3,2,1,2**
- Drive Library-native Address: **1,3,2,1,2**
- Drive HLI Address:
- Drive SCSI Element ID: **-1**

**Library Complex**

- Library Complex Name: **SL8500\_2**
- Library Model: **SL8500**
- Partition Type: **NONE**
- Partition Name: **SL8500\_2:NONE**
- Partition Number: **-1**

**Additional Exchange Information for LTO Drives**

- Alert: Drive Diagnostics Required: **No**
- Drive Lifetime Hours in Motion: **63**
- IBM Drive Efficiency (Hex): **0x27**
- IBM Media Efficiency (Hex): **0x17**
- HP Device Status:

**Media Validation Information for LTO Drives**

- MV Calibration Attempts:
- MV Calibration State:
- MV Calibration Information:
- LTO MV Calibration RQ:
- MV Calibration Starting Suspicion:
- MV Drive Calibrated:
- MV Last Activity: **2021-04-08 00:27:00**
- MV Recommendation: **Blank Media: Continue using tape.**
- MV Drive Allocated: **Yes**
- MV Drive Capable: **Yes**
- MV Drive Available: **Yes**
- MV Drive In Use: **No**
- MV Drive Reserved: **No**
- MV Last Qualification Start:
- MV Primary Qualification Start:
- MV Secondary Qualification Start:

**User-Provided Information**

- Logical Group(s): **None**
- Annotation History: **None**

### Title

Values for these attributes are assigned when STA first starts tracking the drive.

- [Drive](#)
- [Monitored since](#)

### **Drive**

Information about the drive properties.

- [Drive Serial Number](#)
- [Drive Tray Serial Number](#)
- [Drive WWNN](#)
- [Drive Type](#)
- [Drive Health](#)
- [Drive Health Trend](#)
- [Last Drive Message](#)
- [Last Automated Bundle Created](#)
- [Drive WWPN \(Port A\)](#)
- [Port Speed \(Port A\)](#)
- [Drive WWPN \(Port B\)](#)
- [Port Speed \(Port B\)](#)
- [Drive Model](#)
- [Drive Manufacturer](#)
- [Encryption Capable](#)
- [Drive Interface](#)
- [Drive Properties Updated](#)
- [Drive Firmware Version](#)
- [STA Start Tracking](#)
- [STA Stop Tracking](#)

### **Media**

Details about the media used in the drive's most recent exchange that occurred during or before this aggregation period.

- [Volume Serial Number](#)
- [Media Manufacturer Serial Number](#)
- [Media Health](#)
- [WORM/VolSafe Media](#)
- [Cleaning Media](#)

### **Most Recent Exchange**

Details about the drive's most recent exchange that occurred during or before this aggregation period.

- [Exchange Start](#)

- Exchange Elapsed Time
- Exchange Mount Time
- Mount R/W MB/sec
- Exchange Recording Technique
- Drive Exchange Status
- Exchange Tape Alerts – Severe
- Exchange Tape Alerts – Warning
- Exchange Tape Alerts – Info
- Data Compression Ratio
- Alert: Drive Load Limit
- Drive Suspicion Level
- Exchange Drive Cleaning Required
- Meters Between 2 Most Recent Cleans
- Meters since Last Clean
- Drive Lifetime Cleans
- Drive Lifetime Loads
- Drive Lifetime Meters
- Drive Lifetime Power Hours

#### **Drive Activity Counts (Last 30 Days)**

Total activity counts for the drive over the last 30 days. These values are updated with each completed exchange involving the drive.

- % Drive Utilization
- Drive Dismounts
- Drive SNMP Trap Count
- Drive Alert Count
- Dismounts With Errors
- Cleans
- MB Read
- MB Write
- MB R/W
- MB Sent
- MB Received
- Avg Mount Read MB/sec
- Avg Mount Write MB/sec
- Avg Mount R/W MB/sec
- Avg Mount Read MB
- Avg Mount Write MB



- [Avg Mount R/W MB](#)

#### **Additional Exchange Information for Enterprise Drives**

Additional details about the drive's most recent exchange. This section appears only for StorageTek enterprise drives, such as 9840D or T10000C.

- [T10000 Exchange DSC \(Hex\)](#)
- [T10000 Exchange FSC \(Hex\)](#)
- [Exchange Write Inefficient](#)
- [Exchange Read Marginal](#)
- [Exchange Write Efficiency](#)
- [Exchange Read Margin](#)
- [Time Spent Reading](#)
- [Time Spent Writing](#)
- [Time Spent R/W](#)
- [Read MB/sec](#)
- [Write MB/sec](#)
- [R/W MB/sec](#)
- [Read Mount Ratio](#)
- [Write Mount Ratio](#)
- [R/W Mount Ratio](#)
- [Exchange Encryption Used](#)

#### **Additional Exchange Information for LTO Drives**

Additional details about the drive's most recent exchange. This section appears only for LTO drives.

- [Alert: Drive Diagnostics Required](#)
- [Drive Lifetime Hours in Motion](#)
- [IBM Media Efficiency \(Hex\)](#)
- [IBM Drive Efficiency \(Hex\)](#)
- [HP Device Status](#)

#### **Drive Location**

Details about the location of the drive within the library. These attributes are updated whenever a library data collection is performed.

- [Drive Library Name](#)
- [Drive Library Serial Number](#)
- [Drive Library Number](#)
- [Drive Rail Number](#)
- [Drive Physical Address](#)

- [Drive Library-native Address](#)
- [Drive HLI Address](#)
- [Drive SCSI Element ID](#)

### **Library Complex**

Information about the library complex where the drive is located, as of the last completed library data collection.

- [Library Complex Name](#)
- [Library Model](#)
- [Partition Type](#)
- [Partition Name](#)
- [Partition Number](#)

### **Media Validation Information**

Information about media validation and drive calibration and qualification operations for this drive. This section appears only for drives that have been assigned to the media validation drive pool through the library interface.

- [MV Calibration Attempts](#)
- [MV Calibration State](#)
- [MV Calibration Information](#)
- [LTO MV Calibration RQ](#)
- [T10000 MV Calibration Quality Index](#)
- [MV Calibration Starting Suspicion](#)
- [MV Drive Calibrated](#)
- [MV Last Activity](#)
- [MV Recommendation](#)
- [MV Drive Allocated](#)
- [MV Drive Capable](#)
- [MV Drive Available](#)
- [MV Drive In Use](#)
- [MV Drive Reserved](#)
- [MV Last Qualification Start](#)
- [MV Primary Qualification Start](#)
- [MV Secondary Qualification Start](#)

### **User-Provided Information**

- [Logical Group\(s\)](#)
- [Annotation History](#)

# Data Reference: Media Overview

The Media - Overview screen shows attributes for one or more pieces of selected media.

## Sample Screen for Enterprise Media

**Media - Overview** Templates: STA-Default

Format: Applied Filter: MV Last Test Type Is Standard Verify

**Details for Media STA110** Monitored since 2021-04-06 18:01:16

**Media Details**

Volume Serial Number: **STA110**  
 Media Type: **T10000T2**  
 Media Long Type: **T10000T2**  
 STA Supported: **Yes**  
 Media Health: **USE**  
 Media Health Trend: **UNCHANGED**  
 WORM/VolSafe Media: **No**  
 Media Manufacturer Serial Number: **81210202018503**  
 STA Start Tracking: **2021-04-06 18:01:16**  
 STA Stop Tracking:  
 Media Entered Library:  
 Media Ejected from Library:

**Media DATA Activity Counts (Last 30 Days)**

Media Dismounts: **2**  
 Dismounts with Errors: **0**  
 MV Count: **4**  
 Media Alert Count: **0**  
 MB Read: **0.00**  
 MB Write: **0.00**  
 MB R/W: **0.00**  
 MB Sent: **0.00**  
 MB Received: **0.00**  
 Avg Mount Read MB/sec: **0.00**  
 Avg Mount Write MB/sec: **0.00**  
 Avg Mount R/W MB/sec: **0.00**

**Current Home Media Location**

Media Library Name: **elib18**  
 Media Library Serial Number: **516000100437**  
 Media Library Number: **1**  
 Media Rail Number: **3**  
 Media Physical Address: **1,3,-1,2,8**  
 Media Library-native Address: **1,3,-1,2,8**  
 Media HLI Address: **2,2,20,0**  
 Media Slot SCSI Element ID: **-1**

**Drive**

Drive Serial Number: **579004001992**  
 Drive WWNN: **50:01:04:F0:00:8A:AE:18**  
 Drive Type: **T10000d**  
 Drive Health: **USE**

**Library Complex**

Library Complex Name: **SL8500\_2**  
 Library Model: **SL8500**  
 Partition Type: **HLI**  
 Partition Name: **SL8500\_2:HLI:0**  
 Partition Number: **0**

**Media Validation Information for Enterprise Media**

Media Write Efficiency: **100.00**  
 T10000 MV Quality Index: **68.74%**  
 MV Days Since Last Validation: **0**  
 MV Last Activity: **2021-04-08 00:51:36**  
 MV Last Test Type: **Standard Verify**  
 MV Recommendation: **Media OK: Continue using tape.**

**Calibration Information for Enterprise Media**

MV Calibration Library Complex:  
 MV Calibration Library SN:  
 MV Calibration Library Model:  
 MV Calibration Drive Type:  
 MV Calibration Drive SN:  
 MV Pool Start Date:

**Most Recent Exchange**

Last Exchange Start: **2021-04-08 00:34:04**  
 Exchange Elapsed Time: **0:17:32**  
 Exchange Mount Time: **0:16:48**  
 Exchange Library Name: **elib18**  
 Exchange Recording Technique: **T10000C**  
 Media Exchange Status: **GOOD**  
 Exchange Tape Alerts - Severe: **0**  
 Exchange Tape Alerts - Warning: **0**  
 Exchange Tape Alerts - Info: **1**  
 Media Suspicion Level: **0.00%**  
 Exchange Drive Cleaning Required: **No**  
 Media Life Indicator: **GOOD**  
 Media EOL Percentage: **11**  
 Mount R/W MB/sec: **0.00**  
 Data Compression Ratio:  
 Duplicate Detected: **No**  
 Alert: Media Cart Memory Failure: **No**  
 Alert: Media Load Limit: **No**

**Additional Exchange Information for Enterprise Media**

Media MB Capacity: **5,242,880.00**  
 Media MB Avail Post:  
 Media Capacity Utilization: **9.05%**  
 Exchange Encryption Used: **Not Encrypted**  
 T10000 Exchange FSC (Hex):  
 T10000 Exchange DSC (Hex):  
 Permanent Error: **No**  
 Media Blank: **No**  
 Exchange Write Inefficient: **No**  
 Exchange Read Marginal: **No**  
 Exchange Write Efficiency: **100.00%**  
 Exchange Read Margin: **68.74%**  
 Time Spent Reading: **0:00:00**  
 Time Spent Writing: **0:00:00**  
 Time Spent R/W: **0:00:00**  
 Read MB/sec:  
 Write MB/sec:  
 R/W MB/sec: **0.00**  
 Read Mount Ratio: **0.00%**  
 Write Mount Ratio: **0.00%**  
 R/W Mount Ratio: **0.00%**

**Cleaning Usage**

Cleaning Media: **No**

**User-Provided Information**

Logical Group(s): **None**  
 Annotation History: **None**

### Sample Screen for LTO Media

**Media - Overview** ?
Templates: STA-Default v
?

Format: ☰ ☰ ☰ ☰ | Applied Filter: MV Last Test Type Is Standard Verify

**Details for Media SF8090** Monitored since 2021-04-06 18:01:16

**Media Details**

Volume Serial Number: **SF8090**  
 Media Type: **LTO8**  
 Media Long Type: **LtoGen8\_12.8TB**  
 STA Supported: **Yes**  
 Media Health: **USE**  
 Media Health Trend: **UNCHANGED**  
 WORM/VolSafe Media: **No**  
 Media Manufacturer Serial Number: **MJ64Y68LE0**  
 STA Start Tracking: **2021-04-06 18:01:16**  
 STA Stop Tracking:  
 Media Entered Library:  
 Media Ejected from Library:

**Media DATA Activity Counts (Last 30 Days)**

Media Dismounts: **2**  
 Dismounts with Errors: **0**  
 MV Count: **0**  
 Media Alert Count: **0**  
 MB Read: **0.00**  
 MB Write: **0.00**  
 MB R/W: **0.00**  
 MB Sent: **0.00**  
 MB Received: **0.00**  
 Avg Mount Read MB/sec: **0.00**  
 Avg Mount Write MB/sec: **0.00**  
 Avg Mount R/W MB/sec: **0.00**

**Current Home Media Location**

Media Library Name: **elib18**  
 Media Library Serial Number: **516000100437**  
 Media Library Number: **1**  
 Media Rail Number: **2**  
 Media Physical Address: **1,2,50,2,6**  
 Media Library-native Address: **1,2,50,2,6**  
 Media HLI Address: **1,49,18,1**  
 Media Slot SCSI Element ID: **-1**

**Drive**

Drive Serial Number: **10WT000197**  
 Drive WWNN: **50:01:04:F0:00:8A:AE:1B**  
 Drive Type: **IbmUltrium8**  
 Drive Health: **USE**

**Library Complex**

Library Complex Name: **SL8500\_2**  
 Library Model: **SL8500**  
 Partition Type: **HLI**  
 Partition Name: **SL8500\_2:HLI:0**  
 Partition Number: **0**

**Media Validation Information for LTO Media**

Media Write Efficiency:  
 LTO MV RQ: **100.00%**  
 MV Days Since Last Validation:  
 MV Last Activity:  
 MV Last Test Type: **Standard Verify**  
 MV Recommendation: **Blank Media: Continue using tape.**

**Calibration Information for LTO Media**

MV Calibration Library Complex:  
 MV Calibration Library SN:  
 MV Calibration Library Model:  
 MV Calibration Drive Type:  
 MV Calibration Drive SN:  
 MV Pool Start Date:  
 MV Pool End Date:  
 MV Calibration Date:  
 LTO MV Calibration RQ:  
 MV Calibration Suspicion:  
 Last LTO MV Qualification RQ:  
 MV Last Recording Technique:  
 MV MB Tape Used:  
 MV-Calibration-Number-of Wraps:  
 MV Primary Calibration Media:  
 MV Calibration Current State:  
 MV Calibration Status Information:

**Most Recent Exchange**

Last Exchange Start: **2021-04-07 23:51:32**  
 Exchange Elapsed Time: **0:03:32**  
 Exchange Mount Time: **0:02:11**  
 Exchange Library Name: **elib18**  
 Exchange Recording Technique: **LTO8**  
 Media Exchange Status: **GOOD**  
 Exchange Tape Alerts - Severe: **0**  
 Exchange Tape Alerts - Warning: **0**  
 Exchange Tape Alerts - Info: **0**  
 Media Suspicion Level: **0.00%**  
 Exchange Drive Cleaning Required: **No**  
 Media Life Indicator: **GOOD**  
 Media EOL Percentage:  
 Mount R/W MB/sec: **0.00**  
 Data Compression Ratio:  
 Duplicate Detected: **No**  
 Alert: Media Cart Memory Failure: **No**  
 Alert: Media Load Limit: **No**

**Additional Exchange Information for LTO Media**

Media MB Capacity: **11,444,091.00**  
 Media MB Avail Pre: **11,444,091.00**  
 Media Capacity Utilization: **0.00%**  
 IBM Media Efficiency (Hex): **0x17**  
 HP Media Status:  
 Media Length in Meters: **960**  
 Media Manufacturer Date: **2017-07-03**  
 Media Auxiliary Memory Capacity:  
 Alert: Media Directory Corrupt: **No**  
 Alert: Media Nearing End of Life:

**Cleaning Usage**

Cleaning Media: **No**

**User-Provided Information**

Logical Group(s): **None**  
 Annotation History: **None**

**Title**

Values for these attributes are assigned when STA first starts tracking the media.

- [Media](#)
- [Monitored since](#)

**Media Details**

Details about a data or cleaning media.

- [Volume Serial Number](#)
- [Media Type](#)
- [Media Long Type](#)
- [STA Supported](#)
- [Media Health](#)
- [Media Health Trend](#)
- [WORM/VolSafe Media](#)
- [Media Manufacturer Serial Number](#)
- [STA Start Tracking](#)
- [STA Stop Tracking](#)
- [Media Entered Library](#)
- [Media Ejected from Library](#)

**Most Recent Exchange**

Details about the most recent exchange for the media.

- [Last Exchange Start](#)
- [Exchange Elapsed Time](#)
- [Exchange Mount Time](#)
- [Exchange Library Name](#)
- [Exchange Recording Technique](#)
- [Media Exchange Status](#)
- [Exchange Tape Alerts – Severe](#)
- [Exchange Tape Alerts – Warning](#)
- [Exchange Tape Alerts – Info](#)
- [Media Suspicion Level](#)
- [Exchange Drive Cleaning Required](#)
- [Media Life Indicator](#)
- [Media EOL Percentage](#)
- [Mount R/W MB/sec](#)
- [Data Compression Ratio](#)

- Duplicate Detected
- Alert: Media Cart Memory Failure
- Alert: Media Load Limit

#### **Media Data Activity Counts (Last 30 Days)**

Total activity counts for the media over the last 30 days. This section appears only for data media.

- Media Dismounts
- Dismounts With Errors
- MV Count
- Media Alert Count
- MB Read
- MB Write
- MB R/W
- MB Sent
- MB Received
- Avg Mount Read MB/sec
- Avg Mount Write MB
- Avg Mount R/W MB/sec

#### **Current Home Media Location**

Details about the media's current location, as of the last completed exchange.

- Media Library Name
- Media Library Serial Number
- Media Library Number
- Media Rail Number
- Media Physical Address
- Media Library-native Address
- Media HLI Address
- Media Slot SCSI Element ID

#### **Drive**

Details about the drive involved in the latest exchange.

- Drive Serial Number
- Drive WWNN
- Drive Type
- Drive Health

### **Additional Exchange Information for Enterprise Media**

Appears for StorageTek enterprise media only.

- Media MB Capacity
- Media MB Avail Post
- Media Capacity Utilization
- Exchange Encryption Used
- T10000 Exchange DSC (Hex)
- T10000 Exchange FSC (Hex)
- Permanent Error
- Media Blank
- Exchange Write Inefficient
- Exchange Read Marginal
- Exchange Write Efficiency
- Exchange Read Margin
- Time Spent Reading
- Time Spent Writing
- Time Spent R/W
- Read MB/sec
- Write MB/sec
- R/W MB/sec
- Read Mount Ratio
- Write Mount Ratio
- R/W Mount Ratio

### **Additional Exchange Information for LTO Media**

Appears for LTO media only.

- Media MB Capacity
- Media MB Avail Pre
- Media Capacity Utilization
- IBM Media Efficiency (Hex)
- HP Media Status
- Media Length in Meters
- Media Manufacturer Date
- Media Auxiliary Memory Capacity
- Alert: Media Directory Corrupt
- Alert: Media Nearing End of Life

### **Library Complex**

Details about the library complex where the media is located.

- [Library Complex Name](#)
- [Library Model](#)
- [Partition Type](#)
- [Partition Name](#)
- [Partition Number](#)

### **Cleaning Usage**

- [Cleaning Media](#)

### **User-Provided Information**

- [Logical Group\(s\)](#)
- [Annotation History](#)

### **Media Validation Information**

Details about the most recent media validation for the media.

- [Media Write Efficiency](#)
- [T10000 MV Quality Index](#) or [LTO MV RQ](#)
- [MV Days Since Last Validation](#)
- [MV Last Activity](#)
- [MV Last Test Type](#)
- [MV Recommendation](#)

### **Calibration Information**

- [MV Calibration Library Complex](#)
- [MV Calibration Library SN](#)
- [MV Calibration Library Model](#)
- [MV Calibration Drive Type](#)
- [MV Calibration Drive SN](#)
- [MV Pool Start Date](#)
- [MV Pool End Date](#)
- [MV Calibration Date](#)
- [T10000 MV Calibration Quality Index](#) or [LTO MV Calibration RQ](#)
- [MV Calibration Suspicion](#)
- [Last T10000 MV Qualification Quality Index](#) or [Last LTO MV Qualification RQ](#)
- [MV Last Recording Technique](#)
- [MV MB Tape Used](#)



- [MV Calibration Number of Wraps](#)
- [MV Primary Calibration Media](#)
- [MV Calibration Current State](#)
- [MV Calibration Status Information](#)

## Data Reference: Robots Overview

The Robots Overview screen shows attributes for one or more selected robots within the library system.

**Library Components - Robots Overview** Templates: STA-Default

Format: [Icons]

**Details for Robot 465769T+15393E004D** Monitored since 2021-04-07 00:15:34

Robot	Robot Activity Counts (Last 30 Days)
Robot Identifier: <b>465769T+15393E004D</b>	Robot Get Totals: <b>0</b>
Robot Physical Address: <b>1,1,0,0,0</b>	Robot Get Retries: <b>0</b>
Robot Library-native Address: <b>right</b>	Robot Put Totals: <b>0</b>
Robot Health: <b>USE</b>	Robot Put Retries: <b>0</b>
Last Robot Message: <b>NORMAL</b>	Robot Alert Count: <b>0</b>
Last Automated Bundle Created:	Robot SNMP Traps: <b>0</b>
Robot State: <b>INACTIVE</b>	
Robot Power LED State: <b>ON</b>	

Library Complex	User-Provided Information
Library Complex Name: <b>SL4000 464970G+1611BU0016</b>	Annotation History: <b>None</b>
Library Name: <b>Maalox</b>	
Library Serial Number: <b>464970G+1611BU0016</b>	
Library Model: <b>SL4000</b>	

### Title

Values for these attributes are assigned when the SNMP trap is received from the library.

- [Robot](#)
- [Monitored since](#)

### Robot

Details about the robot. With the exception of Robot STA Health, these attributes come directly from the library and are updated with each library configuration data collection. Robot STA Health is an analytic calculated by STA.

- [Robot Identifier](#)
- [Robot Physical Address](#)
- [Robot Library-native Address](#)
- [Robot Health](#)
- [Last Robot Message](#)
- [Last Automated Bundle Created](#)
- [Robot State](#)
- [Robot Power LED State](#)

### Robot Activity Counts (Last 30 Days)

Activity totals for the robot over the last 30 days. These are updated as each associated activity is completed.

- [Robot Get Totals](#)
- [Robot Get Retries](#)
- [Robot Put Totals](#)
- [Robot Put Retries](#)
- [Robot Alert Count](#)
- [Robot SNMP Traps](#)

### User-Provided Information

- [Annotation History](#)

### Library Complex

Information about the library complex where the robot is located, as of the last completed library data collection.

- [Library Complex Name](#)
- [Library Name](#)
- [Library Serial Number](#)
- [Library Model](#)

## Data Reference: CAPs Overview

The CAPs Overview screen shows attributes related to one or more library CAPs, Access Expansion Modules (AEMs – SL3000 libraries only), or mailslots (SL150 libraries only).

**Library Components - CAPs Overview** Templates: STA-Default

Format: [Icons]

---

**Details for CAP CAP-465769T+15233G0034+124** Monitored since 2021-04-06 18:57:19

CAP		CAP Activity Counts (Last 30 Days)	
CAP Identifier:	CAP-465769T+15233G0034+124	CAP Ejects:	0
CAP Physical Address:	1,1,5,2,0	CAP Enters:	0
CAP Library-native Address:	ROTATIONAL Base	CAP SNMP Traps:	0
CAP Type:	ROTATIONAL	CAP Alert Count:	0
Maximum CAP Slots:	39	<b>User-Provided Information</b>	
Current CAP Slots:	26	Annotation History: None	
Last CAP Message:	NORMAL		
Last Automated Bundle Created:			
CAP State:	UNLOCKED		
CAP Accessibility:			

Library Complex	
Library Complex Name:	<a href="#">SL4000_464970G+1536BU00K1</a>
Library Name:	keystone13
Library Serial Number:	<a href="#">464970G+1536BU00K1</a>
Library Model:	SL4000

**Title**

Values for these attributes are assigned when the SNMP trap is received from the library.

- [CAP](#)
- [Monitored since](#)

**CAP**

Details about the CAP. These attributes come directly from the library and are updated with each library configuration data collection.

- [CAP Identifier](#)
- [CAP Physical Address](#)
- [CAP Library-native Address](#)
- [CAP Type](#)
- [Maximum CAP Slots](#)
- [Current CAP Slots](#)
- [Last CAP Message](#)
- [Last Automated Bundle Created](#)
- [CAP State](#)
- [CAP Accessibility](#)

**CAP Activity Counts (Last 30 Days)**

Activity totals for the CAP over the last 30 days. These are updated as each associated activity is completed.

- [CAP Ejects](#)
- [CAP Enters](#)
- [CAP SNMP Traps](#)
- [CAP Alert Count](#)

**User-Provided Information**

- [Annotation History](#)

**Library Complex**

Information about the library complex where the CAP is located, as of the last completed library data collection.

- [Library Complex Name](#)
- [Library Name](#)
- [Library Serial Number](#)
- [Library Model](#)

## Data Reference: PTPs Overview

The PTPs Overview screen shows attributes related to one or more library pass-through ports (PTPs).

PTPs are only used in SL8500 libraries. They allow media to pass between SL8500s within a library complex.

**Library Components - PTPs Overview** Templates: STA-Default

Format: [Icons]

**Details for PTP 66004837** Monitored since 2021-04-06 17:54:10

**PTP**

- PTP Identifier: **66004837**
- PTP Physical Address: **4,4,-6,1,0**
- PTP Library-native Address: **4,4,-6,1,0**
- Last PTP Message: **NORMAL**
- Last Automated Bundle Created:
- PTP State: **READY**
- PTP Power LED State: **ON**

**PTP Activity Counts (Last 30 Days)**

- PTP Alert Count: **0**
- PTP SNMP Traps: **0**

**User-Provided Information**

- Annotation History: **None**

**Library Complex**

- Library Complex Name: **SL8500\_8**
- Library Name: **tenstr04**
- Library Serial Number: **516000100217**
- Library Model: **SL8500**

### Title

Values for these attributes are assigned when the SNMP trap is received from the library.

- [PTP](#)
- [Monitored since](#)

### PTP

Details about the PTP. These attributes come directly from the library and are updated with each library configuration data collection.

- [PTP Identifier](#)
- [PTP Physical Address](#)
- [PTP Library-native Address](#)
- [Last PTP Message](#)
- [Last Automated Bundle Created](#)
- [PTP State](#)
- [PTP Power LED State](#)

### PTP Activity Counts (Last 30 Days)

Activity totals for the PTP over the last 30 days. These are updated as alerts are generated and SNMP messages are received from the library.

- [PTP Alert Count](#)

- [PTP SNMP Traps](#)

### User-Provided Information

- [Annotation History](#)

### Library Complex

Information about the library complex where the PTP is located, as of the last completed library data collection.

- [Library Complex Name](#)
- [Library Name](#)
- [Library Serial Number](#)
- [Library Model](#)

## Data Reference: Elevators Overview

The Elevators Overview screen shows attributes related to one or more library elevators. It is applicable to SL8500 libraries only.

Elevators transfer media between rails with an SL8500 library.

**Library Components - Elevators Overview** ? Templates: STA-Default

Format: [Icons]

**Details for Elevator ELEVATOR-66003392+50832801** Monitored since 2021-04-06 17:54:08

**Elevator**

Elevator Identifier: **ELEVATOR-66003392+50832801**  
 Elevator Physical Address: **4,0,14,2,0**  
 Elevator Library-native Address: **4,0,14,2,0**  
 Last Elevator Message: **NORMAL**  
 Last Automated Bundle Created:  
 Elevator State: **READY**  
 Elevator Power LED State: **ON**

**Elevator Activity Counts (Last 30 Days)**

Elevator Alert Count: **0**  
 Elevator SNMP Traps: **0**

**User-Provided Information**

Annotation History: **None**

**Library Complex**

Library Complex Name: **SL8500 8**  
 Library Name: **tenstr04**  
 Library Serial Number: **516000100217**  
 Library Model: **SL8500**

### Title

Values for these attributes are assigned when the SNMP trap is received from the library.

- [Elevator](#)
- [Monitored since](#)

### Elevator

Details about the elevator. These attributes come directly from the library and are updated with each library configuration data collection.

- [Elevator Identifier](#)

- [Elevator Physical Address](#)
- [Elevator Library-native Address](#)
- [Last Elevator Message](#)
- [Last Automated Bundle Created](#)
- [Elevator State](#)
- [Elevator Power LED State](#)

### Elevator Activity Counts (Last 30 Days)

Activity totals for the elevator over the last 30 days. These are updated as alerts are generated and SNMP messages are received from the library.

- [Elevator Alert Count](#)
- [Elevator SNMP Traps](#)

### User-Provided Information

- [Annotation History](#)

### Library Complex

Information about the library complex where the elevator is located, as of the last completed library data collection.

- [Library Complex Name](#)
- [Library Name](#)
- [Library Serial Number](#)
- [Library Model](#)

## Data Reference: Alerts Overview

The Alerts Overview screen shows attributes related to one or more alerts.

The screenshot shows the 'Alerts Overview' interface. At the top, there's a title bar with 'Alerts Overview', a help icon, and a 'Templates: STA-Default' dropdown. Below the title bar is a 'Format' section with icons for help, list, grid, and print. The main content area is divided into several sections:

- Alert Detail** (Alert Date 2020-01-16 10:58:57):
  - Alert Details:** Date Created/Updated: 2020-01-16 10:58:57, Alert Policy Name: ABC-Drive-Status-Degraded, Alert Severity: Warning.
  - Alert Location Information:** Library Serial Number: 571000200056, Library Name: sl8500-85, Library Complex Name: SL3000\_571000200056.
- Other Details:** Alert Policy Type: Drive, Component ID: 9310059700, Alert State: New, Alert Event Type: Trap, Alert Reason: Last Drive Message=DEGRADED, Drive Serial Number: (blank), Volume Serial Number: (blank).
- User-Provided Information:** Annotation History: None.

### Alert Details

Details about an alert that was triggered.

- [Date Created/Updated](#)
- [Alert Policy Name](#)
- [Alert Severity](#)

**Other Details**

- [Alert Policy Type](#)
- [Component ID](#)
- [Alert State](#)
- [Alert Event Type](#)
- [Alert Reason](#)
- [Drive Serial Number](#) (for drive or media alerts only)
- [Volume Serial Number](#) (for drive or media alerts only)
- [Bundle Name](#)
- [Alert State](#)

**Alert Location Information**

- [Library Serial Number](#)
- [Library Name](#)
- [Library Complex Name](#)

**User-Provided Information**

- [Annotation History](#)

# Data Reference: Exchanges Overview

The Exchanges Overview screen shows attributes related to one or more exchanges. There is one view for enterprise media and a slightly different view for LTO media.

## Sample Screen for Enterprise Media

**Exchanges Overview** [?] Templates: STA-Default [v]

Format: [icon] [icon] [icon]

**Details for Exchange** Recorded on 2021-04-08 03:07:16

**Exchange Health and Activity**

- Exchange Start: 2021-04-08 03:07:16
- Exchange End: 2021-04-08 03:19:16
- Exchange Elapsed Time: 0:12:00
- Exchange Mount Time: 0:11:24
- Drive Exchange Status: GOOD
- Media Exchange Status: GOOD
- Exchange Tape Alerts - Severe: 0
- Exchange Tape Alerts - Warning: 0
- Exchange Tape Alerts - Info: 1
- Mount Read MB/sec: 0.00
- Mount Write MB/sec: 0.00
- Mount R/W MB/sec: 0.00
- Mount Read MB: 0.00
- Mount Write MB: 0.00
- Mount R/W MB: 0.00
- Mount Sent MB: 0.00
- Mount Received MB: 0.00
- Exchange Drive Cleaning Required: No
- Current Cleaning Uses:

**Enterprise Specific Information**

- Media MB Capacity: 8,388,608.00
- Media MB Avail Post: 7,529,606.30
- Exchange Write Inefficient: No
- Exchange Read Marginal: No
- Write Efficiency: 100.00%
- Read Margin: 81.21%
- Time Spent Loaded: 0:09:09
- Time Spent Reading: 0:00:00
- Time Spent Writing: 0:00:00
- Time Spent R/W: 0:00:00
- Read MB/sec:
- Write MB/sec:
- I/O MB/sec:
- Read Mount Ratio: 0.00%
- Write Mount Ratio: 0.00%
- R/W Mount Ratio: 0.00%
- Repositioning Cycles: 12
- Repositioning Cycles Non ERP: 0

**Additional Enterprise Exchange Information**

- T10000 Exchange FSC (Hex):
- T10000 Exchange DSC (Hex):
- Media Blank: No
- Media Write Efficiency: 100
- T10000 MV Quality Index: 81.21%
- Permanent Error: No
- MV Test Type: Standard Verify
- MV Test Percentage: 100
- Perm Read Errors: 0
- Perm Write Errors: 0
- Servo Perm Errors: 0
- Unload Errors: 0
- Usage Perm Errors: 0
- Drive Lifetime Meters Positioning: 205,871
- Drive Lifetime Meters of Head Contact: 1,173,163

**Enterprise Exchange Alerts - Severe**

- Alert: Drive Clean Now: No
- Alert: Drive Failure Predicted: No
- Alert: Drive Temperature: No
- Alert: Media Clean Expired: No
- Alert: Media Error: No
- Alert: Media Loading Failure: No
- Alert: Media Maintenance: No
- Alert: Media No Start of Data: No

**Drive**

- Drive Serial Number: 579004005210
- Drive Tray Serial Number: 464970G+1551J91412
- Drive WWNN: 50:01:04:F0:00:8A:AE:1E
- Drive Type: T10000d
- Drive Model: T10000D
- Drive Firmware Version: 4.18.103-5.60
- Drive Health: USE
- Drive Suspicion Level: 0.00%
- Drive Health Trend: UNCHANGED
- Drive Lifetime Cleans: 2
- Drive Lifetime Loads: 20,435
- Drive Lifetime Meters: 4,797,594
- Drive Lifetime Power Hours: 44,147
- Drive Start Tracking: 2021-04-06 18:01:38
- Drive Stop Tracking:

**Media**

- Volume Serial Number: STA114
- Media Type: T10000T2
- Cleaning Media: No
- Media Manufacturer Serial Number: 81210202018903
- Media Health: USE
- Media Suspicion Level: 0.00%
- Media Health Trend: UNCHANGED
- Data Compression Ratio:
- Exchange Recording Technique: T10000D
- Exchange Encryption Used: Not Encrypted
- Duplicate Detected: No
- Media Start Tracking: 2021-04-06 18:01:16
- Media Stop Tracking:

**Library Complex**

- Library Complex Name: SL8500\_2
- Library Model: SL8500
- Partition Type: NONE
- Partition Name: SL8500\_2;NONE
- Partition Number: -1

**Drive Bay Location**

- Drive Library Name: elib18
- Drive Library Serial Number: 516000100437
- Drive Library Number: 1
- Drive Rail Number: 3
- Drive Physical Address: 1,3,1,1,2
- Drive HLI Address:
- Drive SCSI Element ID: -1

**Media Source Location**

- Media Source Library Number: 1
- Media Source Rail Number: 2
- Media Source Physical Address: 1,2,38,2,13
- Media Source HLI Address: 1,37,25,1
- Media Source SCSI Element ID: -1

**Media Destination Location**

- Media Destination Library Number: 1
- Media Destination Rail Number: 2
- Media Destination Physical Address: 1,2,38,2,13
- Media Destination HLI Address: 1,37,25,1
- Media Destination SCSI Element ID: -1

**Enterprise Exchange Alerts - Informational**

- Alert: Drive Dump Available: No



### Sample Screen for LTO Media

**Exchanges Overview** ?
Templates: STA-Default

Format: [Icons]

**Details for Exchange** Recorded on 2021-04-07 23:58:50

**Exchange Health and Activity**

Exchange Start: **2021-04-07 23:58:50**  
Exchange End: **2021-04-08 00:02:19**  
Exchange Elapsed Time: **0:03:29**  
Exchange Mount Time: **0:02:10**  
Drive Exchange Status: **GOOD**  
Media Exchange Status: **GOOD**  
Exchange Tape Alerts - Severe: **0**  
Exchange Tape Alerts - Warning: **0**  
Exchange Tape Alerts - Info: **0**  
Mount Read MB/sec: **0.00**  
Mount Write MB/sec: **0.00**  
Mount R/W MB/sec: **0.00**  
Mount Read MB: **0.00**  
Mount Write MB: **0.00**  
Mount R/W MB: **0.00**  
Mount Sent MB: **0.00**  
Mount Received MB: **0.00**  
Exchange Drive Cleaning Required: **No**  
Current Cleaning Uses:

**LTO Specific Information**

Media MB Capacity: **5,722,045.00**  
Media MB Avail Pre: **5,722,045.00**  
Media Length in Meters: **960**  
Media Manufacturer Date: **2018-05-01 18:00:00**  
Media Auxiliary Memory Capacity: **16,352**  
Formatted Density Code: **92**  
Lifetime Hours Incompatible: **0**  
Drive Lifetime Hours in Motion: **63**  
IBM Drive Efficiency (Hex): **0x26**  
IBM Media Efficiency (Hex): **0x17**  
HP Device Status:  
HP Media Status:

**Additional LTO Exchange Information**

Media Blank: **Yes**  
Media Write Efficiency: **100.00%**  
LTO MV RQ: **100.00%**  
Permanent Error: **No**  
MV Test Type: **Standard Verify**  
MV Test Percentage: **100**  
Perm Read Errors:  
Perm Write Errors:  
Servo Perm Errors:  
Unload Errors:  
Usage Perm Errors:  
Drive Lifetime Meters Positioning:  
Drive Lifetime Meters of Head Contact:

**LTO Exchange Alerts - Severe**

Alert: Drive Automated Interface: **No**  
Alert: Drive Clean Now: **No**  
Alert: Drive Cooling Fan: **No**  
Alert: Drive Failure Predicted: **No**  
Alert: Drive Hardware A: **No**  
Alert: Drive Hardware B: **No**  
Alert: Drive Interface Fault: **No**  
Alert: Drive Temperature: **No**  
Alert: Media Clean Expired: **No**  
Alert: Media Eject Failed: **No**  
Alert: Media Error: **No**  
Alert: Media Loading Failure: **No**  
Alert: Media No Start of Data: **No**  
Alert: Media Recoverable Mechanical: **No**  
Alert: Media System Read Failure: **No**  
Alert: Media System Write Failure: **No**

**Drive**

Drive Serial Number: **10WT000197**  
Drive Tray Serial Number: **464970G+1730VS0024**  
Drive WWNN: **50:01:04:F0:00:8A:AE:1B**  
Drive Type: **IbmUltrium8**  
Drive Model: **LTO8**  
Drive Firmware Version: **MA70**  
Drive Health: **USE**  
Drive Suspicion Level: **0.00%**  
Drive Health Trend: **UNCHANGED**  
Drive Lifetime Cleans: **0**  
Drive Lifetime Loads: **616**  
Drive Lifetime Meters: **1,207,451**  
Drive Lifetime Power Hours: **30,930**  
Drive Start Tracking: **2021-04-06 18:01:38**  
Drive Stop Tracking:

**Media**

Volume Serial Number: **FM8200**  
Media Type: **LTO8**  
Cleaning Media: **No**  
Media Manufacturer Serial Number: **EX42XVYVTL**  
Media Health: **USE**  
Media Suspicion Level: **0.00%**  
Media Health Trend: **UNCHANGED**  
Data Compression Ratio:  
Exchange Recording Technique: **LTO8**  
Duplicate Detected: **No**  
Media Start Tracking: **2021-04-06 18:01:16**  
Media Stop Tracking:

**Library Complex**

Library Complex Name: **SL8500\_2**  
Library Model: **SL8500**  
Partition Type: **NONE**  
Partition Name: **SL8500\_2:NONE**  
Partition Number: **-1**

**Drive Bay Location**

Drive Library Name: **elib18**  
Drive Library Serial Number: **516000100437**  
Drive Library Number: **1**  
Drive Rail Number: **3**  
Drive Physical Address: **1,3,2,1,2**  
Drive HLI Address:  
Drive SCSI Element ID: **-1**

**Media Source Location**

Media Source Library Number: **1**  
Media Source Rail Number: **2**  
Media Source Physical Address: **1,2,47,1,9**  
Media Source HLI Address: **1,46,8,1**  
Media Source SCSI Element ID: **-1**

**Media Destination Location**

Media Destination Library Number: **1**  
Media Destination Rail Number: **2**  
Media Destination Physical Address: **1,2,47,1,9**  
Media Destination HLI Address: **1,46,8,1**  
Media Destination SCSI Element ID: **-1**

**LTO Exchange Alerts - Informational**

Alert: Cleaning Media: **No**  
Alert: Drive FW Download: **No**  
Alert: Drive Load Limit: **No**  
Alert: Forced Eject: **No**

### **Title**

Values for these attributes are assigned at the start of the exchange.

- [Recorded on](#)

### **Exchange Health and Activity**

Details about the media and drive health during the exchange

- [Exchange Start](#)
- [Exchange End](#)
- [Exchange Elapsed Time](#)
- [Exchange Mount Time](#)
- [Drive Exchange Status](#)
- [Media Exchange Status](#)
- [Exchange Tape Alerts – Severe](#)
- [Exchange Tape Alerts – Warning](#)
- [Exchange Tape Alerts – Info](#)
- [Mount Read MB/sec](#)
- [Mount Write MB/sec](#)
- [Mount R/W MB/sec](#)
- [Mount Read MB](#)
- [Mount Write MB](#)
- [Mount R/W MB](#)
- [Mount Sent MB](#)
- [Mount Received MB](#)
- [Exchange Drive Cleaning Required](#)
- [Current Cleaning Uses](#)

### **Drive**

Details about the drive involved in the exchange.

- [Drive Serial Number](#)
- [Drive Tray Serial Number](#)
- [Drive WWNN](#)
- [Drive Type](#)
- [Drive Model](#)
- [Drive Firmware Version](#)
- [Drive Health](#)
- [Drive Suspicion Level](#)
- [Drive Health Trend](#)

- [Drive Lifetime Cleans](#)
- [Drive Lifetime Loads](#)
- [Drive Lifetime Meters](#)
- [Drive Lifetime Power Hours](#)
- [Drive Start Tracking](#)
- [Drive Stop Tracking](#)

### **Media**

Details about the media involved in the exchange.

- [Volume Serial Number](#)
- [Media Type](#)
- [Cleaning Media](#)
- [Media Manufacturer Serial Number](#)
- [Media Health](#)
- [Media Suspicion Level](#)
- [Media Health Trend](#)
- [Data Compression Ratio](#)
- [Exchange Recording Technique](#)
- [Exchange Encryption Used](#) (enterprise exchanges only)
- [Duplicate Detected](#)
- [Media Start Tracking](#)
- [Media Stop Tracking](#)

### **Library Complex**

Information about the library complex where the exchange occurred. The information is current as of the last completed library data collection.

- [Library Complex Name](#)
- [Library Model](#)
- [Partition Type](#)
- [Partition Name](#)
- [Partition Number](#)

### **Enterprise Specific Information**

Information specific to the StorageTek enterprise drive involved in the exchange. Appears only if the exchange involved an enterprise drive.

- [Media MB Capacity](#)
- [Media MB Avail Post](#)
- [Exchange Write Inefficient](#)
- [Exchange Read Marginal](#)

- Write Efficiency
- Read Margin
- Time Spent Loaded
- Time Spent Reading
- Time Spent Writing
- Time Spent R/W
- Read MB/sec
- Write MB/sec
- R/W MB/sec
- Read Mount Ratio
- Write Mount Ratio
- R/W Mount Ratio
- Repositioning Cycles
- Repositioning Cycles Non ERP

#### **Additional Exchange Information**

Information about errors that occurred during the exchange.

- T10000 Exchange DSC (Hex)
- T10000 Exchange FSC (Hex)
- Media Blank
- Media Write Efficiency
- T10000 MV Quality Index or LTO MV RQ
- Permanent Error
- MV Test Type
- MV Test Percentage
- Perm Read Errors
- Perm Write Errors
- Servo Perm Errors
- Unload Errors
- Usage Perm Errors
- Drive Lifetime Meters Positioning
- Drive Lifetime Meters of Head Contact

#### **LTO Specific Information**

Information specific to the LTO drive involved in the exchange. Appears only if the exchange involved an LTO drive.

- Media MB Capacity
- Media MB Avail Pre

- [Media Length in Meters](#)
- [Media Manufacturer Date](#)
- [Media Auxiliary Memory Capacity](#)
- [Formatted Density Code](#)
- [Lifetime Hours Incompatible](#)
- [Drive Lifetime Hours in Motion](#)
- [IBM Drive Efficiency \(Hex\)](#)
- [IBM Media Efficiency \(Hex\)](#)
- [HP Device Status](#)
- [HP Media Status](#)

### **Drive Bay Location**

Location of the drive involved in the exchange.

- [Drive Library Name](#)
- [Drive Library Serial Number](#)
- [Drive Library Number](#)
- [Drive Rail Number](#)
- [Drive Physical Address](#)
- [Drive HLI Address](#)
- [Drive SCSI Element ID](#)

### **Media Source Location**

Location of the media at the start of the exchange; the location immediately before the mount. Can be a media slot or drive.

- [Media Source Library Number](#)
- [Media Source Rail Number](#)
- [Media Source Physical Address](#)
- [Media Source HLI Address](#)
- [Media Source SCSI Element ID](#)

### **Media Destination Location**

Location of the media at the completion of the exchange. This is the first location immediately after the dismount from the drive, therefore it is always in the same library where the exchange occurred. The location can be a media slot or drive.

- [Media Destination Library Number](#)
- [Media Destination Rail Number](#)
- [Media Destination Physical Address](#)
- [Media Destination HLI Address](#)
- [Media Destination SCSI Element ID](#)

### **Enterprise Exchange Alerts – Severe**

Information about severe errors that occurred during the exchange. This section appears for enterprise drives only.

- [Alert: Drive Clean Now](#)
- [Alert: Drive Failure Predicted](#)
- [Alert: Drive Temperature](#)
- [Alert: Media Clean Expired](#)
- [Alert: Media Error](#)
- [Alert: Media Load Failure](#)
- [Alert: Media Maintenance](#)
- [Alert: Media No Start of Data](#)
- [Alert: Media System Read Failure](#)
- [Alert: Media System Write Failure](#)
- [Alert: Media Unrecoverable Snapped](#)
- [Alert: Permanent Error](#)

### **Enterprise Exchange Alerts – Warning**

Information about warning errors that occurred during the exchange. This section appears for enterprise drives only.

- [Alert: Drive Clean Periodic Requested](#)
- [Alert: Drive FW Failure](#)
- [Alert: Drive Hard Error](#)
- [Alert: Media Load Failure](#)
- [Alert: Media Cart Memory Failure](#)
- [Alert: Media Directory Invalid](#)
- [Alert: Media Lost Statistics](#)
- [Alert: MIR Invalid](#)
- [Alert: Media RFID Warning](#)
- [Alert: Read Warning](#)
- [Alert: Write Warning](#)

### **Enterprise Exchange Alerts – Informational**

Information about informational errors that occurred during the exchange. This section appears for enterprise drives only.

- [Alert: Drive Dump Available](#)
- [Alert: Drive Event Log Near Full](#)
- [Alert: Drive Load Limit](#)
- [Alert: Drive Model Incompatible](#)

- [Alert: Media End of Warranty](#)
- [Alert: Media Life Exceeded](#)
- [Alert: Media Load Limit](#)

#### **LTO Exchange Alerts – Severe**

Information about severe errors that occurred during the exchange. This section appears for LTO drives only.

- [Alert: Drive Automated Interface](#)
- [Alert: Drive Clean Now](#)
- [Alert: Drive Cooling Fan](#)
- [Alert: Drive Failure Predicted](#)
- [Alert: Drive Hardware A](#)
- [Alert: Drive Hardware B](#)
- [Alert: Drive Interface Fault](#)
- [Alert: Drive Temperature](#)
- [Alert: Media Clean Expired](#)
- [Alert: Media Eject Failed](#)
- [Alert: Media Error](#)
- [Alert: Media Load Failure](#)
- [Alert: Media No Start of Data](#)
- [Alert: Media Recoverable Mechanical](#)
- [Alert: Media System Read Failure](#)
- [Alert: Media System Write Failure](#)
- [Alert: Media Unrecoverable Mechanical](#)
- [Alert: Read Failure](#)
- [Alert: Unrecoverable Unload](#)
- [Alert: Write Failure](#)

#### **LTO Exchange Alerts – Warning**

Information about informational errors that occurred during the exchange. This section appears for LTO drives only.

- [Alert: Drive Clean Periodic Requested](#)
- [Alert: Drive Diagnostics Required](#)
- [Alert: Drive Dual-Port Interface](#)
- [Alert: Drive FW Failure](#)
- [Alert: Drive Voltage](#)
- [Alert: Drive Hard Error](#)
- [Alert: Media Cart Memory Failure](#)

- [Alert: Media Directory Corrupt](#)
- [Alert: Media Directory Invalid](#)
- [Alert: Media Lost Statistics](#)
- [Alert: Media Not Data Grade](#)
- [Alert: Read Warning](#)
- [Alert: WORM Integrity Failure](#)
- [Alert: WORM Overwrite Attempted](#)
- [Alert: Write Warning](#)

#### **LTO Exchange Alerts – Informational**

Information about informational errors that occurred during the exchange. This section appears for LTO drives only.

- [Alert: Cleaning Media](#)
- [Alert: Drive FW Download](#)
- [Alert: Drive Load Limit](#)
- [Alert: Forced Eject Attempted](#)
- [Alert: Invalid Cleaning](#)
- [Alert: Media Diminished Capacity](#)
- [Alert: Media Life Exceeded](#)
- [Alert: Media Load Limit](#)
- [Alert: Media Nearing End of Life](#)
- [Alert: Read Only](#)
- [Alert: Unload Prevented](#)
- [Alert: Unsupported Format](#)
- [Alert: Write Protect](#)

#### **User-Provided Information**

- [Annotation History](#)

## Data Reference: Drive Cleanings Overview

The Drive Cleanings Overview screen shows attributes related to drive cleaning exchanges. This screen reports all cleaning activity, including successful and unsuccessful cleaning exchanges.



#### **Note:**

Cleaning media are not required to have a volser starting with "CLN".



### Title

Values for these attributes are assigned when the cleaning action starts.

- [Recorded on](#)

### Drive

Details about the drive involved in the cleaning action.

- [Drive Type](#)
- [Drive Serial Number](#)
- [Drive WWNN](#)
- [Drive WWPN \(Port A\)](#)
- [Drive WWPN \(Port B\)](#)
- [Drive Health](#)
- [Exchange Drive Cleaning Required](#)
- [Drive Lifetime Cleans](#)
- [Drive Lifetime Loads](#)
- [Drive Lifetime Meters](#)
- [Drive Start Tracking](#)
- [Drive Stop Tracking](#)

### Cleaning Activity

Details about the drive clean exchange.

- [Clean Volume Serial Number](#)

- [Media Health](#)
- [Meters Between 2 Most Recent Cleans](#)
- [Current Cleaning Uses](#)
- [Theoretical Maximum Usage Count](#)
- [Alert: Media Clean Expired](#)
- [Exchange Start](#)
- [Exchange End](#)
- [Exchange Elapsed Time](#)
- [Exchange Mount Time](#)
- [Drive Exchange Status](#)
- [Media Exchange Status](#)
- [T10000 Exchange FSC \(Hex\)](#)

### Library

Details about the library where the drive clean took place.

- [Library Complex Name](#)
- [Library Name](#)
- [Library Model](#)
- [Library Serial Number](#)
- [Library WWNN](#)

### User-Provided Information

- [Annotation History](#)

## Data Reference: Media Validation Overview

The Media Validation Overview screen shows details about media validation activity. This screen does not have a detail view.

MV Priority Order	Volume Serial Number	Media Type	Exchange Recording Technique	MV Request Start	MV Test Percentage	MV Time Spent Validating	MV Estimated Time Remaining	Exchange Start	MV Last State
	STA114	T10000T2	T10000D		100.00	0:09:03.4		2021-04-08 03:07:16	2021-04-08 03:1
	STA117	T10000T2	T10000C		100.00	0:07:39.5		2021-04-08 03:07:15	2021-04-08 03:1
	STA100	T10000T2	T10000C		100.00	0:01:30.2		2021-04-08 03:00:23	2021-04-08 03:0
	TCD201	T10000T2	T10000D		100.00	0:09:02.9		2021-04-08 03:00:18	2021-04-08 03:1
	STA103	T10000T2	T10000D		100.00	0:00:25.5		2021-04-08 02:53:20	2021-04-08 02:5
	STA118	T10000T2	T10000C		100.00	0:12:44.9		2021-04-08 02:46:14	2021-04-08 03:0

### Media Validation Attribute Definitions

Attributes are listed in the order they appear when you show all columns.

- MV Priority Order
- Volume Serial Number
- Media Type
- Exchange Recording Technique
- MV Request Start
- MV Test Percentage
- MV Time Spent Validating
- MV Estimated Time Remaining
- Exchange Start
- MV Last State Update
- MV Test Type
- MV Request State
- MV Result
- MV Interrupted
- MV Incomplete
- T10000 Exchange FSC (Hex)
- T10000 Exchange DSC (Hex)
- MV Library Error
- T10000 MV Quality Index
- LTO MV RQ
- Permanent Error
- LTO Sense Key (Hex)
- LTO Sense Code (Hex)
- LTO Sense Code Qualifier (Hex)
- MV Initiator
- MV Policy Name
- Drive Serial Number
- Drive Model
- MV Calibration Request
- Library Complex Name
- Media Library Name
- Library Model
- Media Library Serial Number
- MV Status Information
- MV Recommendation

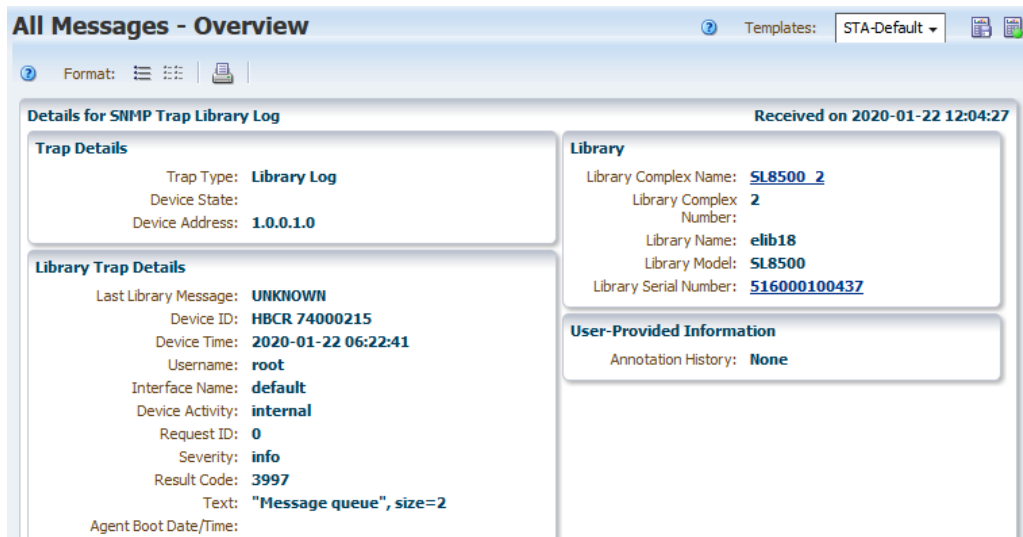
## Data Reference: Messages Screens

The Messages screens show attributes relating to SNMP traps received by STA from the libraries.

There are multiple messages screens within STA:

- Libraries – Messages
- Drives – Messages
- Media – Messages
- All Messages – Overview
- All Messages – Analysis

These screens share many of the same attributes as listed below:



### Title

Values for these attributes are assigned when the SNMP trap is received from the library.

- [SNMP Trap](#)
- [Received on](#)

### Trap Details

Provides information about the type of SNMP trap and the device involved.

- [Trap Type](#)
- [Device State](#)
- [Device Address](#)

### **Drive Trap Details**

Provides detailed information from the drive trap.

- [Drive Type](#)
- [Drive Vendor](#)
- [Device Serial Number](#)

### **Library Trap Details**

Provides detailed information from the library trap.

- [Last Library Message](#)
- [Device ID](#)
- [Device Time](#)
- [Username](#)
- [Interface Name](#)
- [Device Activity](#)
- [Request ID](#)
- [Severity](#)
- [Result Code](#)
- [Text](#)
- [Agent Boot Date/Time](#)

### **Library**

Provides information about the library that sent the SNMP trap.

- [Library Complex Name](#)
- [Library Complex Number](#)
- [Library Name](#)
- [Library Model](#)
- [Library Serial Number](#)

### **Library Configuration Details**

Provides detailed information about library hardware configuration update traps.

- [Property Name](#)
- [New Property Value](#)
- [New Property Effective](#)

### **User-Provided Information**

- [Annotation History](#)

# C

## Troubleshoot Issues

Many issues you may encounter have a workaround or simple resolution.

### GUI Issues

- [ISSUE: Cannot Access the STA GUI](#)
- [ISSUE: GUI Elements Do Not Render Correctly](#)

### Data Issues

- [ISSUE: Exchanges Not Showing Up in STA](#)
- [ISSUE: T1000D Drives Are Not Showing Quality Index After Media Validation](#)

### Connection Issues

- [ISSUE: Database Communication Link Failure \(IMPORTANT\)](#)
- [ISSUE: OSCI Library Connection Test Fails](#)
- [ISSUE: SNMP Library Connection Test Fails](#)
- [ISSUE: SNMP Trap Status Not Updating After Connection Test](#)
- [ISSUE: Cannot Connect to SDP](#)

### Server Process and Installation Issues

- [ISSUE: STA Fails to Restart Properly After Reboot](#)
- [ISSUE: Weblogic Server Processes Not Starting](#)
- [ISSUE: Authentication Prompts During STA start Command](#)
- [ISSUE: Backup Service or Resource Monitor Fails](#)
- [ISSUE: MySQL Installation Fails](#)
- [ISSUE: STA Does Not Completely Deinstall](#)

## ISSUE: Cannot Access the STA GUI

If you cannot access the STA GUI, first verify STA is running. Then, verify the firewall settings and iptables.

### Resolution

1. Verify STA is running by using the command:

```
# STA status all
```

2. Verify you are using the correct URL:

```
http://<server name or IP address>:7021/STA
```

OR

```
https://<server name or IP address>:7022/STA
```

Ports 7021 and 7022 are the default installer port numbers. If you customized or changed the port numbers, use the corresponding custom port numbers instead.

3. If STA is running and you still cannot access the GUI, verify the following firewall settings:

- Firewall is running
- Check `hosts.allow` and `hosts.deny` files if using those OS services
- REJECT rules are not interfering with the GUI ports (such as 162 and 7029)

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

```
# systemctl status iptables
# iptables -L
```

4. If needed, use the `iptables` command to remove or modify the firewall rules to allow access to the STA GUI. For example:

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

#### WARNING:

Removing or modifying firewall rules can create security risks and must be done by qualified security administrator.

5. If the GUI was inaccessible after a server reboot occurred, verify the `iptables`:
  - a. Verify `iptables` rules were been saved correctly using the service `iptables save` command.

```
# service iptables save
```

- b. Verify the `iptables` server is enabled. For example

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

## ISSUE: GUI Elements Do Not Render Correctly

When using a browser tab that you previously used for a now expired STA session, various elements may not work as expected. Logging out or terminating the browser session can correct this issue.

An improperly closed-out and expired STA session may cause the UI infrastructure to apply stale information which it cannot render. This behavior is not browser-specific. It can occur on various browser platforms.

### Symptoms

- Navigation bar may not contain all normal entries
- Pages may render, but without all expected elements
- User customizations (like custom templates and defaults) may not appear
- Dialog boxes may fail to launch or may not respond to input
- Interface may fail to respond to input or appear frozen

The staUi log will contain `RESTORE_VIEW` errors. These errors are usually followed by another more specific indicator like “null windowId”, “page has expired”, “Could not find saved view state”, and so on.

### Workaround

This error is non-destructive. There are several options to work around it:

- Always click **Logout** to terminate your STA sessions. If you do so, the error will not occur.
- If you forgot to logout of the previous session, click **Logout** on the current session. This will clean out the UI state. Then, you can log back into STA.
- Terminate the browser tab and open a new tab to log into STA.

## ISSUE: Exchanges Not Showing Up in STA

If exchanges are not showing up within STA, the SNMP traps from the library may not be reaching STA. You should verify the SNMP configuration and verify the iptables.

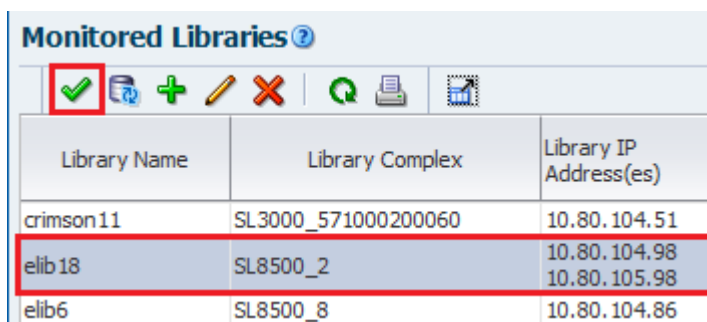
### Verify STA is Running

1. Open a terminal session on the STA server, and login in as the Oracle user.
2. Verify STA is running by using the command:

```
$ STA status all
```

### Test the SNMP Connection

1. Sign in to the STA GUI. In the left navigation, expand **Setup & Administration**, then click **Library Connections**.
2. Within the Monitored Libraries table, select the library in question and click **Test Connection** ✓.



Library Name	Library Complex	Library IP Address(es)
crimson11	SL3000_571000200060	10.80.104.51
elib18	SL8500_2	10.80.104.98 10.80.105.98
elib6	SL8500_8	10.80.104.86

If the MIB Walk or Trap Channel tests **FAIL**, see the following sections in the Installation and Configuration Guide "Configure SNMP" chapter:

- "Troubleshoot a Failed MIB Walk Channel Test"
- "Troubleshoot a Failed Trap Channel Test"
- If these do not correct the issue, proceed to [Verify Network Configuration](#).

If the tests **PASS**, proceed to [Verify iptables Configuration](#).



### Verify Network Configuration

1. If STA is running but the connection test fails, verify the following:
  - Firewall is running (also known as iptables)
  - hosts.allow and hosts.deny files (if using those services). You may need to add the library IP address to hosts.allow.
  - REJECT rules do not interfere with the GUI ports (for example 162 and 7029)
  - Port forwarding from 162 to 7029 (port 7029 may be different if you have customized it)
  - Network router configuration between the STA server and library. Some routers may drop UDP or SNMP packets.

To verify STA server settings, login as the root user and use the following commands:

```
# systemctl status iptables
# more /etc/hosts.allow
# iptables -L
# iptables -L -t nat
Chain PREROUTING (policy ACCEPT)
target    prot opt source      destination
REDIRECT  udp  --  anywhere   anywhere    udp dpt:snmptrap redir ports 7027
```

2. If needed, use the iptables command to add port forwarding or remove and modify the rules to all SNMP traps.

### Verify iptables Configuration

A server reboot can cause an issue with the iptable configuration. If the issue occurred following a reboot, verify the iptables are correct.

1. Use service iptables save command to verify the iptables rules are saved correctly.

```
# service iptables save
```

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

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

## ISSUE: T10000D Drives Are Not Showing Quality Index After Media Validation

The T10000D drives must have both *Level 3 Media Validation* and *Level 3 RQI Margin Report* enabled within VOP to report Quality Index values.

### Verify the VOP Settings

1. Within VOP, under the **Retrieve** menu, select **View Drive Data**.
2. Select the **Maintenance** tab.
3. Check that both *Level 3 Media Validation* and *Level 3 RQI Margin Report* are enabled.

- If not, follow the steps below to enable both of these settings.

#### Enable the Settings

- Set the drive offline. Within the **Drive Operations** menu, select **Set Offline**.
- Within the **Configuration** menu, select **Drive Data**.
- Select the **Maintenance** tab.
- Enable *Level 3 Media Validation* and *Level 3 RQI Margin Report*.
- Click **Commit**. The drive will IPL.
- Retry the media validation.

## ISSUE: Database Communication Link Failure (IMPORTANT)

Database communication link failures can occur if there are duplicate iptable rules.

The following exceptions in the Weblogic logs indicate a database communication issue:  
com.mysql.jdbc.exceptions.jdbc4.CommunicationsException: Communications link failure.

To correct the issue:

- Have the network administrator review the iptable rules.
- Remove duplicate or overlapping iptable rules.
- Stop and restart STA:

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

## ISSUE: OSCI Library Connection Test Fails

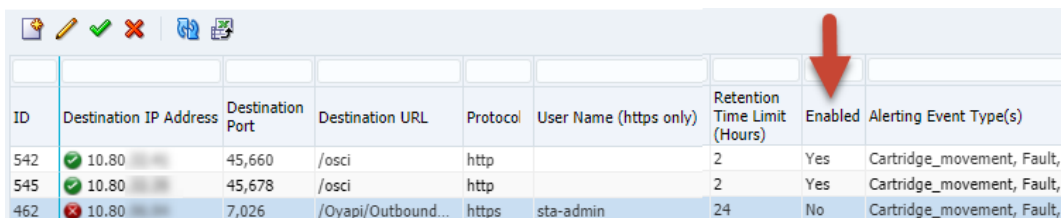
The OSCI connection test may fail if the destination is not enabled within the SL4000 user interface.

#### Access the SL4000 GUI Notifications Page


- Log into the SL4000 GUI.
- Click **Notifications** in the left navigation area.
- Click the **SCI** tab.

#### Verify the Destination is Enabled

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



ID	Destination IP Address	Destination Port	Destination URL	Protocol	User Name (https only)	Retention Time Limit (Hours)	Enabled	Alerting Event Type(s)
542	10.80	45,660	/osci	http		2	Yes	Cartridge_movement, Fault,
545	10.80	45,678	/osci	http		2	Yes	Cartridge_movement, Fault,
462	10.80	7,026	/Oyapi/Outbound...	https	sta-admin	24	No	Cartridge_movement, Fault,

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

## ISSUE: SNMP Library Connection Test Fails

The SNMP library connection test may fail for multiple reasons such as iptables configuration.


If the connection test failure is occurring with an SL150 library, be sure to verify firewall rules.

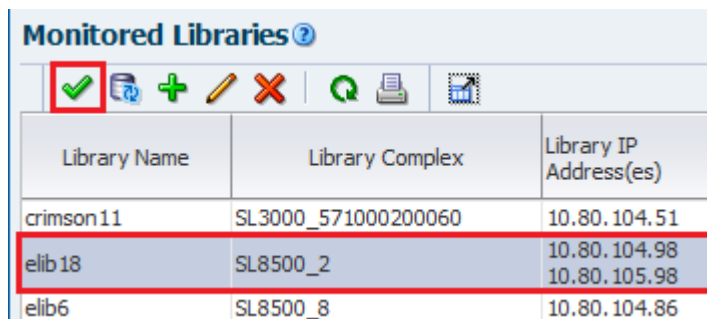
Refer to [ISSUE: Exchanges Not Showing Up in STA](#) for details on how to troubleshoot this issue.

## ISSUE: SNMP Trap Status Not Updating After Connection Test

The SNMP configuration screen may not update immediately after a connection test, even after a refresh, but you can run the connection test again and use the values provided by the Test Connection dialog to confirm the status.

### Workaround

1. Sign in to the STA GUI. In the left navigation, expand **Setup & Administration**, then click **Library Connections**.
2. Within the Monitored Libraries table, select the library in question and click **Test Connection** .



Library Name	Library Complex	Library IP Address(es)
crimson11	SL3000_571000200060	10.80.104.51
elib18	SL8500_2	10.80.104.98 10.80.105.98
elib6	SL8500_8	10.80.104.86

3. Use the values reported by the test to verify the status.

Such as:

- MIB Walk Channel :: Good (SNMP V3)
- Trap Channel :: Good (SNMP V3)
- Media Validation Support :: Good

## ISSUE: Cannot Connect to SDP

STA may not be able to connect to SDP due to a hostname mismatch. Adding an entry to the `/etc/hosts` file on the STA server can resolve this issue.

### Symptom

SDP status within the STA GUI indicates "Unable to contact or connect to SDP host".

This can occur if the SDP server hostname defined on the public name servers does not match the hostname sent within the ASR packets. For example, the SDP server sends an ASR packet with its name as "sdp2host" but the name defined on the public name servers is "sdp2server.mycompany.com".

### Resolution

Define the SDP host in the `/etc/hosts` file on the STA server. Add an entry with the IP address of the SDP server and the hostname that the SDP server provides in the ASR packets. For example, "10.20.30.40 sdp2host".

## ISSUE: STA Fails to Restart Properly After Reboot

Sometimes STA fails to restart properly after the system reboots on Linux 7 systems using systemd services. Stopping and starting STA should resolve this issue.

1. Open a terminal session on the STA server.
2. Stop and restart STA.

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

## ISSUE: Weblogic Server Processes Not Starting

After a server reboot or non-graceful shutdown of STA, one of the Weblogic server processes like (staAdapter, staEngine, staUi, AdminServer) may not start. This can be caused by a Weblogic lock file (.lck) that was not properly removed during shutdown.

### Resolution

1. Open a terminal session on the STA server and login as the Oracle user.
2. Examine the Weblogic log files for the services that have not started. Look for errors or the presence of a .lck file.

The log files are located in:

```
TBI/servers/AdminServer/logs/weblogic.log
TBI/servers/staAdapter/logs/weblogic_staAdapter.log
TBI/servers/staUi/logs/weblogic_staUi.log
TBI/servers/staEngine/logs/weblogic_staEngine.log
```

3. Use the `rm -f` command to remove the lock file for the STA server process that has not started.
4. Restart STA using the command:

```
$ STA start all
```

## ISSUE: Authentication Prompts During STA start Command

When using Linux 7 or 8, you may see an authentication message after using the STA start command. The message should time out and the STA service should start. Or the server administrator can add polkit rules to remove the authentication requests.

### Symptom

While using the STA start command the following authentication messages appear:

```
Starting staweblologic Service.==== AUTHENTICATING FOR
org.freedesktop.systemd1.manage-units ===
Authentication is required to manage system services or units.
Authenticating as: root
```

### Resolution

The OS polkit service running on the server generates this message. Depending on the server configuration this authentication prompt (password prompt) will time out and STA services will start normally.

If the authenticate does interfere with STA service starting, then contact your server administrator. The administrator can add polkit rules to remove the authentication requests in the following location:

```
/usr/share/polkit-1/rules.d/org.freedesktop.systemd1.manage-units.rules
```

#### WARNING:

Modifying polkit rules can create security risks and must be done by qualified security administrator.

## ISSUE: Backup Service or Resource Monitor Fails

The Backup Service or Resource Monitor may fail if the Oracle user does not have write access to `/etc/.java` or `staservd` does not have write access to `/etc/.java/.systemPrefs`.

### Symptom

The service fails with the following:

```
Error: java.util.prefs.BackingStoreException: Couldn't get file lock.
```

### Resolution

1. Open a terminal session on the STA server and login as the root user.
2. Provide write access to the `/etc/.java` and `/etc/.java/.systemPrefs` directories. For example:

```
# chmod 777 /etc/.java
# chmod 777 /etc/.java/.systemPrefs
```

3. Switch to the Oracle user.
4. Stop the services daemon:

```
$ STA stop staservd  
$ STA status staservd
```

You should see: staservd service is shutdown

5. Start the services daemon:

```
$ STA start staservd
```

## ISSUE: MySQL Installation Fails

If the installation fails to install MySQL, you may need to restart the server and retry the installation.

### Symptom

You may encounter 'ERROR 2002 (HY000): Can't connect to local MySQL server through socket'.

### Workaround

Keep retrying the install until the installation does not hit the timing window which is causing this issue.

1. Reboot the server, then retry the installation.
2. Retry the installation using the other installer type (meaning try the silent installer if you previously used the GUI installer or vice versa).

## ISSUE: STA Does Not Completely Deinstall

If the deinstallation of STA fails or fails to uninstall everything, you may need to manually remove components of STA.

The following steps assume that the Storage Home is `/Oracle` and the Oracle Inventory Home is `/Oracle`. If these values differ for your system, adjust the steps below.

Some of the steps may fail because the component may already be uninstalled.

1. Start a terminal session as the 'root' super user.
2. Stop the WebLogic processes:

```
# STA stop all
```

3. Stop MySQL:

```
# service mysql stop
```

4. Stop any remaining oracle processes (this assumes the oracle user was used to install STA, otherwise adjust appropriately).

```
# ps -eaf | grep oracle  
# kill -9 <pids>
```

Repeat until all oracle processes have been killed.

5. Remove the following directories:

```
# rm -rf /Oracle/Middleware
# rm -rf /Oracle/StorageTek_Tape_Analytics/
```

6. Identify any installed MySQL packages:

```
# yum list MySQL*
```

7. Remove the MySQL packages:

```
# yum remove MySQL*
```

8. Remove the following directories:

```
# rm -rf /usr/bin/STA
# rm -rf /Oracle/oraInventory
# rm -f /etc/oraInst.loc
```

# Index

## Symbols

---

'About' link, [1-2](#)  
"missing" media, [17-5](#)

## A

---

accessibility settings, [2-2](#)  
administrator  
    manage users, [2-5](#)  
aggregated count, [3-4](#), [4-11](#), [5-10](#)  
alerts, [9-1](#)  
    auto log bundles, [15-7](#)  
    best practices, [9-2](#)  
    changing the state, [9-8](#)  
    displaying detail, [9-7](#)  
    emails, [9-5](#), [9-15](#)  
    entities, [9-9](#)  
    how they work, [9-1](#)  
    policies, [9-3](#)  
    policy examples, [9-10](#)  
    severities, [9-10](#)  
    show/hide dismissed, [9-8](#)  
    user roles, [9-9](#)  
    viewing, [9-6](#)  
    workflow, [9-8](#)  
annotations, [5-7](#), [6-6](#)  
apply  
    filters, [8-1](#)  
    template, [7-2](#)  
area charts, [4-2](#)

## B

---

bar graphs, [4-2](#)  
best practices  
    alerts, [9-2](#)  
    auto bundle creation, [15-3](#)  
    executive reports, [10-1](#)  
    graphs, [4-3](#)  
    investigate issues, [17-7](#)  
    logical groups, [11-1](#)

## C

---

chart: see graphs, [4-1](#)  
collapse  
    areas of screen, [3-5](#)  
confirmation dialog settings, [2-4](#)  
create  
    alert policies, [9-3](#)  
    template, [7-4](#)  
    user, [2-5](#)  
ctrl-click, [5-13](#)

## D

---

dashboard, [6-1](#)  
    adding panes, [6-5](#)  
    annotations, [6-6](#)  
    change layout, [6-4](#)  
    customizing, [6-4](#)  
    detach pane, [6-3](#)  
    filtering, [6-6](#)  
    filtering using graphics, [8-5](#)  
    graph panes, [6-7](#)  
    layout, [6-1](#)  
    linking to details, [6-2](#)  
    loading time, [6-3](#)  
    mobile device support, [6-3](#)  
    pane size, [6-4](#)  
    pane types, [6-7](#)  
    removing panes, [6-6](#)  
    report panes, [6-12](#)  
    save layout, [6-7](#)  
    table panes, [6-10](#)  
    templates, [7-11](#)  
    time, [6-1](#)  
data collection, [16-21](#), [16-22](#)  
database  
    log bundle, [14-4](#)  
date range  
    changing on graphs, [4-9](#)  
    synchronizing across graphs, [4-9](#)  
default  
    template, [7-3](#)  
delete  
    log bundle, [14-6](#)



delete (*continued*)

- logical group, [11-9](#)
- template, [7-7](#)
- user, [2-5](#)

detach

- dashboard pane, [6-3](#)
- graphs, [4-5](#)
- tables, [5-1](#)

display settings, [2-3](#)

- confirmation dialog, [2-4](#)

download

- log bundles, [14-6](#)

drives

- analysis, [17-16](#)
- calibration and qualification, [12-10](#)
- efficiency trends, [17-18](#)
- error rates, [17-16](#), [17-17](#)
- error trends, [17-9](#)
- errors, [17-12](#)
- firmware levels, [17-21](#)
- identifiers, [17-6](#)
- logical groups, [11-3](#), [11-4](#)
- media validation, [12-4](#)
- removed, [17-3](#)
- utilization, [17-19](#)
- viewing logical group membership, [11-7](#)

duplicate volume serial numbers, [17-5](#)

## E

---

email

- addresses, [13-2](#)
- auto log recipients, [15-6](#)
- define server, [13-1](#)
- recipients, [13-1](#)
- testing, [13-3](#)

email recipient, [9-5](#)

engine ID, [16-24](#)

errors

- drives and media, [17-11](#)

executive reports, [10-1](#), [10-2](#)

- best practices, [10-1](#)
- deleting, [10-3](#)
- download, [10-2](#)
- policies, [10-4](#)
- running on demand, [10-3](#)
- sample, [10-6](#)
- user privileges, [10-5](#)

export table data, [5-12](#)

## F

---

filters, [8-1](#)

- applying, [8-1](#)
- applying a template, [8-4](#)

filters (*continued*)

- clearing, [8-7](#)
- dashboard graphics, [8-5](#)
- dashboard pane, [6-6](#)
- dialog box, [8-2](#)
- logical group, [11-9](#)
- pivot table links, [8-6](#)
- removing, [8-7](#)
- screen pairings, [8-1](#)
- view applied filter, [8-1](#)

## G

---

graphs, [4-1](#)

- adding, [4-6](#)
- area, [4-2](#)
- bar, [4-2](#)
- best practices, [4-3](#)
- changing the attribute, [4-8](#)
- changing the date range, [4-9](#)
- dashboard panes, [6-7](#)
- detaching, [4-5](#)
- line, [4-1](#)
- modifying, [4-5](#), [4-8](#)
- moving, [4-6](#)
- narrow and wide views, [4-7](#)
- pie, [4-2](#)
- pivot table attributes, [4-11](#)
- pivot table layer, [4-11](#)
- plotting library resources, [4-10](#)
- print, [4-8](#)
- removing, [4-6](#)
- restore graph area, [4-5](#)
- spark, [4-3](#)
- switching between actual and percentage values, [4-10](#)
- synchronizing date range, [4-9](#)
- types, [4-1](#)

## H

---

high contrast setting, [2-2](#)

## L

---

large fonts setting, [2-2](#)

line graphs, [4-1](#)

log bundles, [14-1](#)

- about, [14-1](#)
- automatic, [15-1](#)
- best practices, [15-3](#)
- creation process, [14-3](#)
- database, [14-4](#)
- deleting, [14-6](#)

log bundles (*continued*)  
 directories, [14-3](#)  
 download, [14-6](#)  
 forward to Oracle Support, [14-6](#)  
 library log, [14-3](#)  
 naming, [14-2](#)  
 RDA, [14-4](#), [14-5](#)  
 retention, [14-2](#)  
 run information, [14-7](#)  
 types, [14-1](#)  
 viewing, [14-7](#)

log out of STA, [1-4](#)

logical groups, [11-1](#)  
 best practices, [11-1](#)  
 calibration media, [12-10](#)  
 configuring, [11-2](#)  
 deleting, [11-9](#)  
 dynamic  
   creating and defining, [11-5](#)  
   forcing an update, [11-7](#)  
   selection criteria, [11-5](#), [11-6](#)  
 filtering, [11-9](#)  
 manual  
   adding drives and media, [11-3](#)  
   creating, [11-3](#)  
   removing drives and media, [11-4](#)  
 ownership, [11-3](#)  
 renaming, [11-8](#)  
 types, [11-1](#)  
 uses, [11-2](#)  
 view drive/media assignment, [11-7](#)

## M

---

media  
 analysis, [17-23](#)  
 approaching capacity, [17-29](#)  
 calibration, [12-12](#)  
 error rates, [17-23](#)  
 error trends, [17-9](#)  
 errors, [17-12](#)  
 identify older media, [17-29](#)  
 logical groups, [11-3](#), [11-4](#)  
 migration, [17-28](#)  
 missing, [17-5](#)  
 removed, [17-3](#)  
 shortages and surpluses, [17-25](#)  
 utilization, [17-27](#)  
 viewing logical group membership, [11-7](#)

media validation  
 about, [12-1](#), [12-25](#)  
 benefits, [12-2](#)  
 calibration media, [12-12](#)  
 disabling, [12-17](#)

media validation (*continued*)  
 drive calibration and qualification, [12-10](#),  
   [12-15](#)  
   benefits, [12-14](#)  
 drive pool, [12-4](#)  
 eligible media, [12-9](#)  
 enabling, [12-17](#)  
 features, [12-2](#)  
 manual request, [12-18](#)  
 policies, [12-6](#)  
 queue, [12-22](#)  
 resume request, [12-21](#)  
 types, [12-24](#)  
 user privileges, [12-24](#)  
 wizard, [12-7](#)

mobile device support, [6-3](#)

modify  
 template, [7-5](#)  
 user, [2-5](#)

monitored libraries table, [16-23](#)

move  
 column, [5-2](#)  
 graph panes, [4-6](#)  
 pivot table layers, [5-10](#)

My Oracle Support, [14-6](#)

## N

---

narrow view, [4-7](#)

navigation  
 collapsing and restoring, [3-5](#)  
 left navigation menu, [3-2](#)  
 quick links, [3-3](#)  
 text links, [3-4](#)

navigation menu  
 using, [3-2](#)

## P

---

page number field, [5-4–5-6](#)

pane types, [6-7](#)

pie charts, [4-2](#)

pivot tables  
 changing attributes and nesting order, [5-11](#)  
 description, [5-8](#)  
 displaying the layer name, [5-9](#)  
 displaying value details, [5-10](#)  
 exporting data, [5-12](#)  
 filtering, [8-6](#)  
 graphing a layer, [4-11](#)  
 graphing an attribute, [4-11](#)  
 modify, [5-8](#)  
 moving layers, [5-10](#)  
 resize column or row, [5-9](#)

policies  
 media validation, [12-6](#)  
 predefined templates, [7-10](#)  
 print  
 graphs, [4-8](#)  
 tables, [5-7](#)  
 private template, [7-6](#)  
 privileges, [2-5](#)  
 media validation, [12-24](#)  
 public template, [7-6](#)

## Q

---

quick links screen, [3-3](#), [7-2](#)  
 quick start guide, [A-1](#)

## R

---

RDA log bundle, [14-4](#), [14-5](#)  
 refresh  
 tables, [5-7](#)  
 refresh screen rate, [2-2](#)  
 Refresh Settings dialog, [2-3](#)  
 remove filter, [8-7](#)  
 removed  
 drives, [17-3](#)  
 media, [17-3](#)  
 removed drives and media display settings, [2-3](#)  
 removed libraries, [17-4](#)  
 rename  
 logical group, [11-8](#)  
 template, [7-5](#)  
 reorder  
 column, [5-2](#)  
 reports  
 dashboard panes, [6-12](#)  
 resize  
 areas of screen, [3-5](#)  
 column, [5-3](#)  
 dashboard panes, [6-4](#)  
 pivot tables, [5-9](#)  
 resource ID, [3-4](#)  
 restore  
 predefined templates, [7-9](#)  
 roles, [2-5](#)

## S

---

save  
 template, [7-2](#), [7-4](#)  
 SCI, [16-1](#), [16-18](#)  
 data collection, [16-21](#)  
 troubleshooting, [16-25](#)

screen layout  
 description, [3-2](#)  
 resizing, [3-5](#)  
 restore graph area, [4-5](#)  
 screen reader setting, [2-2](#)  
 screen refresh interval, [2-2](#)  
 SDP, [15-1](#)  
 define host, [15-4](#)  
 test connection, [15-5](#)  
 select multiple rows, [5-13](#)  
 session timeout period, [2-3](#)  
 modifying, [2-3](#)  
 severities, [9-10](#)  
 share template, [7-6](#), [7-7](#)  
 shift-click, [5-13](#)  
 SNMP, [16-1](#)  
 data collection, [16-21](#)  
 troubleshooting, [16-25](#)  
 software version information, [1-2](#)  
 sort  
 table columns, [5-4](#), [5-5](#)  
 using filters, [8-1](#)  
 spark charts, [4-3](#)

## T

---

tables, [5-1](#)  
 annotations, [5-7](#)  
 dashboard panes, [6-10](#)  
 detaching, [5-1](#)  
 displaying a specific page, [5-6](#)  
 displaying detail for resources, [5-6](#)  
 exporting data, [5-12](#)  
 hiding and revealing columns, [5-5](#)  
 modify, [5-1](#)  
 moving a column, [5-2](#)  
 pivot, [5-8](#)  
 print, [5-7](#)  
 refresh, [5-7](#)  
 resize column, [5-3](#)  
 sorting by column, [5-4](#), [5-5](#)  
 templates  
 applying, [7-2](#)  
 creating, [7-4](#)  
 deleting, [7-7](#)  
 description, [7-1](#)  
 exporting, [7-8](#)  
 importing, [7-8](#)  
 modifying, [7-5](#)  
 ownership, [7-6](#)  
 predefined, [7-9](#), [7-10](#)  
 public and private, [7-6](#)  
 renaming, [7-5](#)  
 saving, [7-4](#)  
 screen characteristics, [7-4](#)

templates (*continued*)

- set default, [7-3](#)
- sharing, [7-6](#), [7-7](#)
- types, [7-1](#)
- user roles, [7-9](#)
- visibility, [7-6](#)

## test

- SDP connection, [15-5](#)

text links, [3-4](#)tooltip, [3-5](#)transient library locations, [17-5](#)

## troubleshooting

- firewall, [16-27](#)
- SCI, [16-25](#)
- SNMP, [16-25](#)

---

**U**

---

## users

- add, modify, delete, [2-5](#)

users (*continued*)

- alerts privileges, [9-9](#)
- media validation privileges, [12-24](#)
- privileges, [2-5](#)
- roles, [2-5](#)
- template privileges, [7-9](#)

---

**V**

---

volsers, [17-5](#)volume serial numbers, [17-5](#)

---

**W**

---

wide view, [4-7](#)

---

**Z**

---

zoom adjustment, [3-5](#)