StorageTek Tape Analytics

User's Guide

Version 2.2.0

E68627-01

February 2016

ORACLE

StorageTek Tape Analytics User's Guide, Version 2.2.0

E68627-01

Copyright © 2013, 2016, Oracle and/or its affiliates. All rights reserved.

Primary Author: Nancy Stevens

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

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

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

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

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

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

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

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

This documentation is in preproduction status and is intended for demonstration and preliminary use only. It may not be specific to the hardware on which you are using the software. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to this documentation and will not be responsible for any loss, costs, or damages incurred due to the use of this documentation.

The information contained in this document is for informational sharing purposes only and should be considered in your capacity as a customer advisory board member or pursuant to your beta trial agreement only. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle.

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle Master Agreement, Oracle License and Services Agreement, Oracle PartnerNetwork Agreement, Oracle distribution agreement, or other license agreement which has been executed by you and Oracle and with which you agree to comply. This document and information contained herein may not be disclosed, copied, reproduced, or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

Contents

Preface xiii

Audience xiii
Documentation Accessibility xiii
Related Documents xiii
Conventions xiv

What's New xv

STA 2.2.0 February 2016 xv

1 Getting Started

STA Overview 1-1
Supported Devices 1-1
StorageTek Modular Tape Libraries 1-2
Drive and Media Types 1-2
STA Login Sessions 1-2
Username and Password Requirements 1-2
User Account Lockout 1-2
User Roles 1-3
Best Practices for Login Sessions 1-3
Login Tasks 1-4
Log In to STA 1-4
Enable HTTPS in Your Browser (optional) 1-5
Log Out of STA 1-8
Display STA Software Version Information 1-9
Change Your Password 1-9
Help 1-11
Help Window Layout 1-12
Help Toolbar 1-12
Help Contents Tab 1-13
Help Index Tab 1-14
Help Search Tab 1-15

2 Dashboard

Using the Dashboard 2-1
Customizing the Dashboard 2-3

Dashboard Templates ... 2-3
Times Displayed on the Dashboard ... 2-3
Linking to Detail Screens ... 2-4
Dashboard Layout ... 2-6
Dashboard Toolbar ... 2-7
Dashboard Portlet Toolbar ... 2-8
Portlet Types ... 2-8
Graph Portlets ... 2-9
Table Portlets ... 2-10
Report Portlets ... 2-11
Mobile Dashboard Display ... 2-11
Mobile Display Requirements ... 2-12
Accessing STA From Your Mobile Device ... 2-13
Dashboard Tasks ... 2-13
Change the Dashboard Column and Row Layout ... 2-14
Add a Dashboard Portlet ... 2-15
Add or Change a Dashboard Portlet Annotation ... 2-17
Apply or Change a Dashboard Portlet Filter ... 2-18
Clear a Dashboard Portlet Filter ... 2-20
Display the Dashboard on a Mobile Device ... 2-22

3 Templates

Using Templates ... 3-1
Template Defaults ... 3-1
Predefined Templates ... 3-2
Custom Templates ... 3-2
User Roles for Template Usage Activities ... 3-2
Defining and Managing Templates ... 3-3
Screen Characteristics Included in the Template Definition ... 3-3
Screen Characteristics Not Included in the Template Definition ... 3-3
Template Ownership and Visibility ... 3-3
Sharing Templates ... 3-4
User Roles for Template Management Activities ... 3-4
Template Toolbars and Screens ... 3-5
Templates Toolbar ... 3-5
Template Quick Links Screen ... 3-5
Templates Management Screen ... 3-7
Best Practices for Templates ... 3-7
Template Usage Tasks ... 3-8
Apply a Template ... 3-8
Set the Default Template for a Screen ... 3-11
Clear the Default Template for a Screen ... 3-12
Template Management Tasks ... 3-13
Create a Template ... 3-13
Modify a Template ... 3-15
Rename a Template ... 3-18
Change the Visibility (Public or Private) Settings for a Template ... 3-18

Export a Template 3-19
Import a Template 3-19
Delete a Template 3-21
Restore the STA Predefined Templates 3-22

4 Filtering Data

About Filters 4-1
Filter Application 4-1
Filter Duration 4-2
Applying a Filter 4-2
Filter Data Dialog Box 4-2
Filter Operators by Attribute Type 4-3
Filtering Using Aggregate Count Links 4-6
Filtering by Applying a Template 4-7
Filtering Using Dashboard Graphics 4-8
Filtering Tasks 4-9
Use the Filter Data Dialog Box to Change a Table Filter 4-9
Clear the Current Filter 4-12
Use an Aggregate Count Link to Apply a Filter 4-13
Apply a Filter From the Dashboard 4-16

5 STA Alerts

How Alerts Work 5-1
Defining Alert Policies 5-1
Alert Generation 5-2
Monitoring Generated Alerts 5-2
User Roles for Alerts Management 5-3
Details on Defining Alert Policies 5-3
Alert Policy Entities 5-3
Alert Policy Severities 5-4
Alert Policy Criteria 5-8
STA Sample Alert Policies 5-8
Best Practices for Alert Policies 5-9
Alert Emails 5-10
Alerts Workflow 5-11
Alert Management Tasks 5-11
Manage the List of Alert Policies 5-12
Create an Alert Policy 5-12
Copy an Alert Policy 5-18
Modify an Alert Policy 5-19
Modify Email Recipients for an Alert Policy 5-21
Enable or Disable an Alert Policy 5-22
Delete an Alert Policy 5-23
Manage the List of Generated Alerts 5-25
Display Detail For an Alert 5-25
Change the State of an Alert 5-27

Show or Hide Dismissed Alerts 5-28

6 Executive Reports

Executive Report Creation Process 6-1
Using Executive Reports 6-2
Displaying Executive Reports 6-2
Running Executive Reports 6-3
User Roles for Executive Report Files 6-4
Executive Report Policies 6-5
Defining Executive Report Policies 6-5
Emailing Executive Reports 6-6
User Roles for Executive Report Policies 6-6
Best Practices for Executive Reports 6-6
Executive Report File Tasks 6-7
Run an Executive Report On Demand 6-7
View an Executive Report 6-8
Delete an Executive Report File 6-9
Manage the List of Executive Report Files 6-10
Executive Report Policy Tasks 6-11
Create or Modify an Executive Report Policy 6-11
Delete an Executive Report Policy 6-14
Manage the List of Executive Report Policies 6-15

7 Logical Groups

Using Logical Groups 7-1
Logical Group Examples 7-2
Logical Group Creation Process 7-2
Logical Group Ownership 7-2
Types of Logical Groups 7-3
Manual Logical Groups 7-3
Dynamic Logical Groups 7-3
Filtering by Logical Group 7-4
Constructing Filters Using Logical Groups 7-5
How Changes to Logical Group Definitions Can Affect Filters 7-6
Dashboard Portlets With Filtering by Logical Group 7-10
Best Practices for Logical Groups 7-11
Logical Group Creation and Management Tasks 7-11
Create a Manual Logical Group 7-11
Add Drives and Media to a Manual Logical Group 7-13
Remove Drives and Media From a Manual Logical Group 7-15
Create and Define a Dynamic Logical Group 7-17
Change the Selection Criteria for a Dynamic Logical Group 7-21
Force a Dynamic Logical Group Update 7-22
View Logical Group Assignments for Selected Drives or Media 7-23
List All Drives and Media Assigned to a Logical Group 7-24
Rename a Logical Group 7-25
Delete a Logical Group 7-27

8 STA Media Validation

Overview of STA Media Validation 8-1
Features and Benefits of STA Media Validation 8-2
Feature Comparison for STA and SL Console 8-3
Types of Verification Tests 8-3
Configuring STA Media Validation 8-5
Preparing for STA Media Validation 8-5
Validation Drive Pools 8-6
Enabling Media Validation 8-8
Disabling Media Validation 8-10
Drive Calibration and Qualification 8-10
Drive Calibration and Qualification Terms 8-11
Benefits of Calibration and Qualification 8-12
How Calibration and Qualification Work 8-13
Preparing for Calibration and Qualification 8-14
Submitting Manual Validation Requests 8-17
Manual Verify and Rebuild MIR Requests for Incompatible Media and Drives 8-19
Using Automated Media Validation 8-19
Media Eligible for Automated Validation 8-20
Defining Validation Policies 8-20
Managing the STA Media Validation Request Queue 8-21
Displaying the Status of Validation Requests 8-21
Canceling Pending or In-Progress Validation Requests 8-24
Resuming Interrupted "Complete Verify" Tests on T10000T2 Media 8-24
User Roles for Media Validation 8-25
Best Practices for Media Validation 8-26
Media Validation Tasks 8-26
Display Validation Drives for STA Media Validation 8-27
Enable or Disable Media Validation on STA 8-30
Create the Calibration Media Logical Group 8-31
Enable Drive Calibration and Qualification 8-34
Disable Drive Calibration and Qualification 8-36
Display the Media Validation Request Queue 8-37
Submit Manual Media Validation Requests 8-39
Reorder Pending Media Validation Requests 8-46
Cancel Pending Media Validation Requests 8-49
Cancel In-Progress "Complete Verify" Validations 8-51
Create a Media Validation Policy 8-53
Display the List of Media Validation Policies 8-58
Enable or Disable a Media Validation Policy 8-59
Copy a Media Validation Policy 8-61
Modify a Media Validation Policy 8-62
Delete a Media Validation Policy 8-64

9 STA Usernames and Email

STA Usernames 9-1

Username and Password Requirements 9-1
STA User Roles 9-1
STA User Management Tasks 9-5
Add an STA Username 9-5
Modify an STA Username 9-6
Delete an STA Username 9-7
Email Configuration Tasks 9-8
Define the STA SMTP Server 9-8
Add an Available Email Recipient 9-10
Display Email Configuration Information 9-11
Test the Email Server and Recipient Definitions 9-12
Modify an Available Email Recipient 9-13
Delete an Available Email Recipient 9-13

10 STA Service Logs

Service Log Overview 10-1
Reasons for Generating a Log Bundle 10-1
Taking a Log Snapshot 10-2
Log Bundle Process 10-2
Service Log Tasks 10-2
Create a Service Log Bundle From the STA User Interface 10-3
Create a Service Log Bundle From the System Command Line 10-3
List Generated Log Bundles 10-5
Display Log Run Information 10-5
Download a Log Bundle 10-6
Delete a Log Bundle 10-7
Forward a Log Snapshot to Oracle Support 10-7

11 Managing SNMP Connections in STA

SNMP Configuration for STA 11-1
STA Data Store 11-1
Maintaining SNMP Connections and the STA Data Store 11-2
Library Connection Status Information 11-2
Understanding the Library Engine ID 11-2
Testing Library SNMP Connections 11-3
Collecting Library Configuration Data 11-5
SNMP Maintenance Tasks Performed in STA 11-7
Verify SNMP Communication With a Library 11-7
Configure SNMP Client Settings for STA 11-9
Configure the SNMP Connection to a Library 11-11
Test a Library SNMP Connection 11-13
Perform a Manual Data Collection 11-15
Export SNMP Connection Settings to a Text File 11-16
Remove a Library Connection From STA 11-17
Supporting SNMP Maintenance Tasks Performed on the Library 11-18
Verify the Library is Operational 11-18
Display All SNMP Trap Recipients 11-19

Delete or Modify the STA Trap Recipient 11-20
Special SNMP Connection Update Tasks 11-20
Update the SNMP Connection After a Library Redundant Electronics Switch 11-21
Update the SNMP Connection After a Library Firmware Upgrade 11-21
Update the SNMP Connection After a Change to the STA Server IP Address 11-22
SNMP Connection Troubleshooting Tasks 11-23
Troubleshoot a Failed MIB Walk Channel Test 11-23
Troubleshoot a Failed Trap Channel Test 11-25
Troubleshoot a Failed Media Validation Support Test 11-26
Troubleshoot Unsuccessful Trap Processing 11-26

12 Understanding STA Analytics

Data Retention 12-1
Incomplete Exchanges 12-1
Dimmed Values on STA Screens 12-2
Removed Drives and Media 12-2
Identifying Removed Drives and Media 12-3
Impact of Removed Drives and Media on Calculated Totals 12-3
How Removed Drives and Media Affect Calculated Summaries 12-4
How Removed Drives and Media Affect Overview and Analysis Screens 12-4
Removed Libraries 12-8
What Happens to Data When an SL8500 Library is Moved to a New Complex 12-9
"Missing" Media 12-10
Duplicate Volume Serial Numbers 12-10
"Duplicate Detected" Flag on Exchanges 12-11
Mapping Host and STA Drive Identifiers 12-11
Mainframe Identifiers 12-11
Open Systems Identifiers 12-12

13 Using STA to Answer Tape Environment Questions

Drive and Media Health Questions 13-1
Report the Media and Drive With the Most Errors 13-1
Report Trends in Drive Error Rates 13-8
Report Drive Efficiency Trends 13-14
Report Trends in Drive Failures 13-17
Report Information to Help Troubleshoot Tape Job Errors 13-19
Report Trends in Critical Errors 13-23
Capacity and Resource Management Questions 13-28
Report Total Libraries, Drives, or Media 13-29
Report Drive and Media Types 13-31
Report Drives With the Highest Utilization 13-33
Report Shortages or Surpluses of Media 13-36
Project Future Media, Drive, or Storage Cell Requirements 13-40
Report Resources With the Highest Utilization 13-46
Report Library Relative Activity Levels 13-51
Report Media Approaching Capacity 13-54

Report Drive Firmware Levels 13-56
Best Practices for Investigating Tape Environment Issues 13-63

A Dashboard Portlets

Graph Portlets A-1
Table Portlets A-4
Report Portlets A-6

B STA Predefined Templates

Dashboard Templates B-2
Complexes Overview Templates B-3
Libraries – Overview Templates B-4
Libraries – Messages Templates B-4
Drives – Overview Templates B-5
Drives – Analysis Templates B-6
Drives – Messages Templates B-6
Media – Overview Templates B-6
Media – Analysis Templates B-8
Media – Messages Templates B-8
Robots Overview Templates B-8
CAPs Overview Templates B-8
PTPs Overview Templates B-9
Elevators Overview Templates B-9
Alerts Overview Templates B-9
Exchanges Overview Templates B-10
Drive Cleanings Overview Templates B-11
Media Validation Overview Templates B-11
All Messages – Overview Templates B-11
All Messages – Analysis Templates B-12

C STA Dialog Box Reference

Login Dialog Box C-1
Login C-1
Dashboard Dialog Box C-2
Annotate C-3
Filter Dialog Box C-4
Filter Data C-4
Media Validation Overview Dialog Boxes C-5
Cancel Requests C-5
Resubmit Media C-6
Reorder Pending Requests C-7
Logical Groups Dialog Boxes C-8
Logical Groups C-8
Create or Edit Logical Group C-9
Delete Logical Group C-11
Unassign Entities C-11

Alerts Policies Dialog Boxes C-12
Alert Policy Wizard C-12
Executive Reports Policies Dialog Boxes C-14
Add/Edit Executive Reports Policy C-14
Reports C-16
Delete C-16
Templates Management Dialog Boxes C-17
Reset (Templates) C-17
Import Template C-18
Rename Template C-19
Delete Template C-20
Save Template C-21
Save Template (Overwrite) C-22
Default Template C-22
Media Validation Policy Wizard and Dialog Boxes C-23
Media Validation Configuration Confirmation C-23
Media Validation Policy Wizard C-24
Service Log Dialog Boxes C-26
Create New Log Bundle C-26
Log Bundle Run Info C-27
Delete Selected Log Bundle C-28
SNMP Connections Dialog Boxes C-28
Define SNMP Client Settings C-29
Define Library Connection Details C-31
Confirmation (Delete Library Connection) C-33
User Management Dialog Boxes C-34
User Configuration C-34
Delete User C-35
Email Configuration Dialog Boxes C-36
Define SMTP Server Details C-36
Define Email Details C-38

Index

Preface

This guide provides concepts and procedures for using Oracle's StorageTek Tape Analytics (STA).

Audience

This document is intended for new and experienced users of STA.

Documentation Accessibility

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

Access to Oracle Support

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

Related Documents

The STA documentation set consists of the following documents.

For users of the STA application

- *STA Quick Start Guide*—Use this guide to introduce yourself to the STA application and some features of the user interface.
- *STA User's Guide*—Use this guide for instructions on using all STA application features, including the Dashboard, templates, filters, alerts, Executive Reports, logical groups, and STA media validation. This guide also provides instructions for administering and managing STA usernames, email addresses, service logs, and SNMP connections with the monitored libraries.
- *STA Screen Basics Guide*—Use this guide for full details about the STA user interface. It describes the screen navigation and layout, and the use of graphs and tables.
- *STA Data Reference Guide*—Use this guide to look up definitions for all STA tape library system screens and data attributes.

For installers and administrators of the STA server and application

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

Conventions

The following text conventions are used in this document:

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

What's New

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

STA 2.2.0 February 2016

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

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

1

Getting Started

This chapter includes the following topics:

- STA Overview
- Supported Devices
- STA Login Sessions
- Best Practices for Login Sessions
- Login Tasks
- Help

STA Overview

Oracle's StorageTek Tape Analytics (STA) is an intelligent monitoring application available exclusively for Oracle's StorageTek Modular Tape Libraries. It simplifies tape storage management and allows you to 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 performance trending analyses allow you to increase the utilization and performance of your tape investments. These analyses are based on a continually updated database of library operations. 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 aggregates data according to a variety of criteria and displays it in tabular and graphical formats, allowing you to quickly assess environment activity, health, and capacity.

Supported Devices

This section identifies the devices supported by STA. See the *STA Requirements Guide* for complete details about minimum firmware levels and other requirements.

In general, the newer the drive model and the more up-to-date the drive and library firmware, the richer the data that STA receives and the more in-depth the analysis it can perform. For best results, it is recommended that you update your drive and library firmware to the most current versions.

StorageTek Modular Tape Libraries

- SL8500 standalone libraries and complexes
- SL3000
- SL500
- SL150

Drive and Media Types

- StorageTek T10000A, T10000B, T10000C, and T10000D drives
- StorageTek T10000T1 and T10000T2 media
- StorageTek 9840C and 9840D
- HP LTO-3, LTO-4, LTO-5, and LTO-6, full Automation Drive Interface (ADI) support
- IBM LTO-3 and LTO-4, full ADI support
- IBM LTO-5 and LTO-6, basic support—Library Drive Interface (LDI) mode—only

> **Note:** For LTO drives, the ADI protocol must be enabled on both the drives and the library for STA to receive rich data about these drives. LTO 2 and SDLT drives do not support ADI, and therefore STA receives only minimal data about them.

STA Login Sessions

Your STA administrator will provide you with an STA username and password for logging into STA. Once you are logged in, you have access to all STA screens and features. See "Log In to STA" on page 1-4 for instructions.

Username and Password Requirements

Username requirements are as follows:

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

Password requirements are as follows:

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

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

You can change your password at any time. See "Change Your Password" on page 1-9 for details.

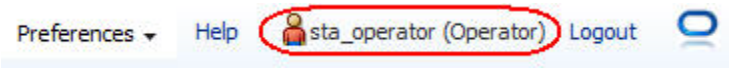
User Account Lockout

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, so you must wait the full 30-minutes before attempting to log in again.

User Roles

Each STA username is assigned a user role, which determines the screens and activities the user can access. Your user role is displayed in the Main Toolbar, next to your STA username.



The user roles are as follows:

- **Viewer** – Can access all screens from the Home, Tape System Hardware, and Tape System Activity menus.
- **Operator** – Has all privileges of the Viewer role. Also has editing privileges for some Setup & Administration screens and view-only privileges on Configuration screens.
- **Administrator** – Has all privileges of the Operator role, plus has full editing privileges for all Setup & Administration screens.

For a complete description of the screens and activities available to each role, see "STA User Roles" on page 9-1.

The STA documentation identifies the user role required to access screens and perform activities. If no role is identified, then the activity can be performed by all users.

Best Practices for Login Sessions

This section provides tips for your STA login sessions. See the *STA Screen Basics Guide* for related screen display tips.

Using the STA Navigation Bar

The Navigation Bar provides perspectives focused on hardware components (for example, Libraries, Drives, and Robots) and activities involving those components (for example, Exchanges, Drive Cleanings, and Alerts). Choose the perspective and views that achieve your goals most easily.

Navigating forward and backward

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

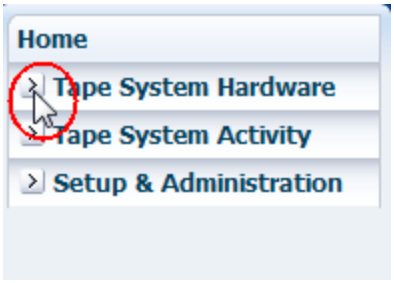
When you are ready to finish a login session, always explicitly log, rather than simply closing the browser window. Logging out releases the session memory on the STA server for other processes. If you simply close the browser window, the session memory is not freed until the defined session timeout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

See "Log Out of STA" on page 1-8.

Number of STA login sessions

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 the locked Navigation Bar shown in the example below—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.



Loss of VPN connection

If you are connected to STA through a virtual private network (VPN) and the VPN connection goes down, you may see an error message similar to the following:

```
null windowId
ADF_FACES-60097: For more information, please see the server's error log for an
entry beginning with: ADF_FACES-60096:Server Exception during PPR, #1
```

After reconnecting to VPN, you should initiate a new STA login session, either by forcing a reload of the current STA browser page or by closing the current STA page and then opening a new one.

If you simply reconnect to VPN without initiating a new login session, you will appear to be logged in, but the **Logout** link in the Main Toolbar at the top of the page will be missing.

Login Tasks

- "Log In to STA" on page 1-4
- "Enable HTTPS in Your Browser (optional)" on page 1-5
- "Log Out of STA" on page 1-8
- "Display STA Software Version Information" on page 1-9
- "Change Your Password" on page 1-9

Log In to STA

Use this procedure to start an STA session. Before using this procedure, you must verify that your computer and browser are configured correctly. See the *STA Requirements Guide* for minimum requirements.

In addition, you must get the following information from your STA administrator:

- URL of the STA application
- Your STA username and password

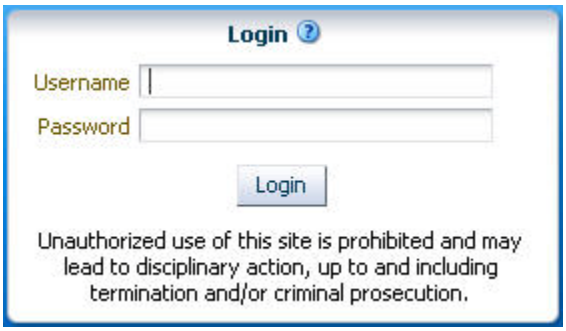
1. Start a supported Web browser on your computer.
2. In the **Location Bar** or **Address** field, enter the URL of the STA application. The URL uses one of the following formats:

   http://local_host_name:port_number/STA

   https://local_host_name:port_number/STA

   where local_host_name and port_number are the name and port number of the STA server given to you by your STA administrator. Typically, STA runs on port 7021.

   The Login screen appears.



3. Enter the STA username and password you have been assigned, and then click **Login**.

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

4. Complete the Accessibility Settings dialog box, if applicable, and then click **OK**. See the *STA Screen Basics Guide* for details on completing this dialog box.

   The Dashboard appears.

Enable HTTPS in Your Browser (optional)

Use this procedure to explicitly enable the HTTPS protocol in your browser so you can use a secure connection to log in to STA.

Note: Use this procedure only if STA is accessed at your site with the HTTPS protocol (that is, the STA URL starts with https:// rather than http://). You can skip this procedure if the STA URL starts with http://

Background: When accessed through HTTPS, the STA user interface requires the TLS 1.0 protocol. Recent browser versions have enabled TLS 1.2 or TLS 1.3 and disabled TLS 1.0 by default. If TLS 1.0 is disabled in your browser, the HTTPS connection to STA fails with a warning, such as "Secure Connection Failed".

Use the procedure for the browser you use to access STA. After you complete the procedure, the TLS 1.0 protocol remains enabled in the browser for future sessions on the computer you are using.

- "Firefox 38 on Windows 7" on page 1-6
- "Internet Explorer 10 on Windows 7" on page 1-7
- "Chrome 46 on Windows 7" on page 1-7
- "Safari 8 on OS X" on page 1-8

Note: These procedures provide sample instructions for selected recent-version browsers, and the steps may vary slightly if you are running a different version browser or operating system than the ones listed here. See the *STA Requirements Guide* for supported browser versions.

Firefox 38 on Windows 7

1. Open a new tab in the browser.
2. In the address bar, enter about:config.
3. If the "This might void your warranty" screen is displayed, click **I'll be careful, I promise!**
4. In the Search bar, enter security.tls.version.fallback-limit.
5. If the displayed value is not 1, double-click the entry to change it.
6. Enter 1 and click **OK**.
7. Restart the browser.
8. The first time you use HTTPS to log in to STA after using this procedure, you may see a message that the connection is untrusted. Perform the following steps to permanently add the security exception to your browser:
   a. On the This Connection is Untrusted screen, select **I Understand the Risks** and click **Add Exception**.
   b. In the Add Security Exception dialog box, select the **Permanently store this exception** check box and click **Confirm Security Exception**.

      The browser continues to the STA login screen.

Internet Explorer 10 on Windows 7

> **Note:** You cannot access STA in Internet Explorer 11; you must use a different version of Internet Explorer.

1. In the **Tools** menu, select **Internet Options**.
2. Select the **Advanced** tab.
3. Scroll to the Security heading and select the **Use TLS 1.0** check box. Click **OK**.
4. The first time you use HTTPS to log in to STA after using this procedure, you may see a message indicating a problem with the website's security certificate. To permanently add the security exception to your browser, select the **Continue to this website (not recommended)** link.

   The browser continues to the STA login screen.

Chrome 46 on Windows 7

1. Open a new tab in the browser.
2. In the address bar, type chrome://settings.
3. Select the **Show advanced settings** link at the bottom of the page.
4. In the Network heading, click **Change proxy settings**.
5. In the Internet Properties dialog, select the **Advanced** tab.

> **Note:** Chrome shares the Windows Internet Properties dialog box with Internet Explorer, so you may see "Internet Explorer" referenced in the dialog box.

6. Scroll to the Security heading and select the **Use TLS 1.0** check box. Click **OK**.
7. Restart your computer.

> **Note:** You must restart your computer, not just the browser.

8. Right-click the Google Chrome shortcut on your desktop, and select Properties.
9. Select the **Shortcut** tab in the Google Chrome Properties dialog box.
10. In the **Target** field, add a space and the following parameter to the end of the text that is already there (after the closing quote mark). This parameter enforces the use of TLS1 as the minimum fallback protocol.

    --ssl-version-fallback-min=tls1

    The contents of the **Target** field should now be similar to the following:

    "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --ssl-version-fallback-min=tls1

11. Click **OK**.
12. The first time you use HTTPS to log in to STA after using this procedure, you may see a message that the connection is not private. Perform the following steps to permanently add the security exception to your browser:

a. On the Your connection is not private screen, select the **Advanced** link.

b. Select the **Proceed to *server_name* (unsafe)** link.

The browser continues to the STA login screen.

Safari 8 on OS X

On OS X, Apple Security Update 2014-005 is all that is needed to allow HTTPS access to STA. Use the following procedure to verify this update has been installed on your computer. See the following website for details about the update.

https://support.apple.com/en-us/HT203107

1. In the Apple menu, click the **Option** button and select **System Information**.
2. Scroll to the **Software** heading and select **Installations**.
3. Verify that Security Update 2014-005 is included in the displayed list (by default, software updates are listed in alphabetical order).

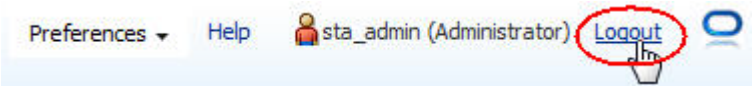
Log Out of STA

Use this procedure to terminate your STA session. You can terminate your session at any time.

Note: It is recommended that you log out of STA rather than simply closing the browser window. Logging out releases the session memory on the STA server for other processes. It is especially important to log out if your defined login session timeout period is long. See the *STA Screen Basics Guide* for related information.

---

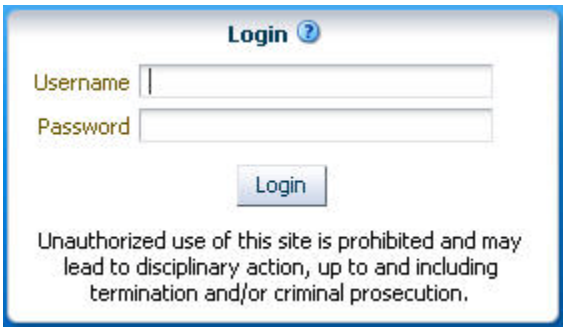
1. From any STA screen, click **Logout** in the Main Toolbar.



Your login session is terminated and the Logged Out dialog box appears.

2. Click **Go to Login**.

The Login screen appears. See "Log In to STA" on page 1-4 for instructions on logging in.



Display STA Software Version Information

Use this procedure to display version information about the STA application and supporting software. This information is useful whenever you contact your Oracle support representative.

1. Click **About** in the Status Line.

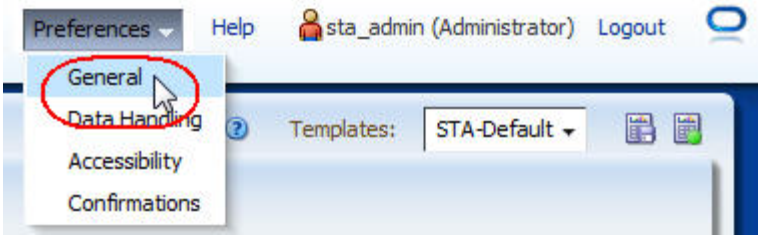
The version information dialog box is displayed.

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

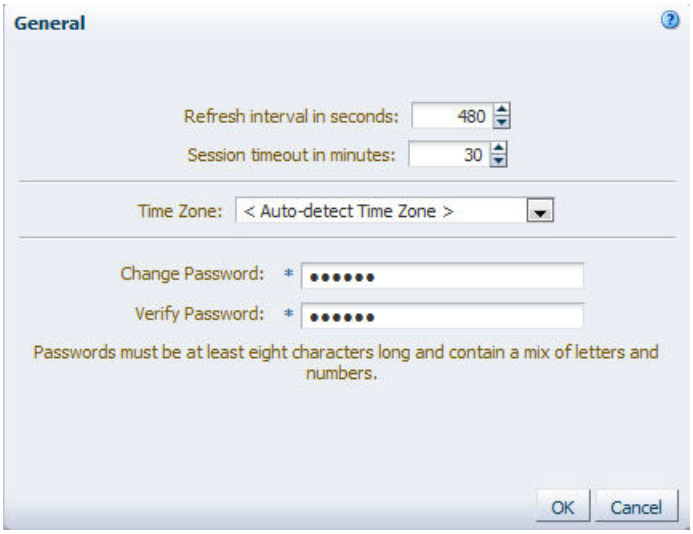
Change Your Password

Use this procedure to change the password for your STA username. See "Username and Password Requirements" on page 1-2 for details on valid password assignments.

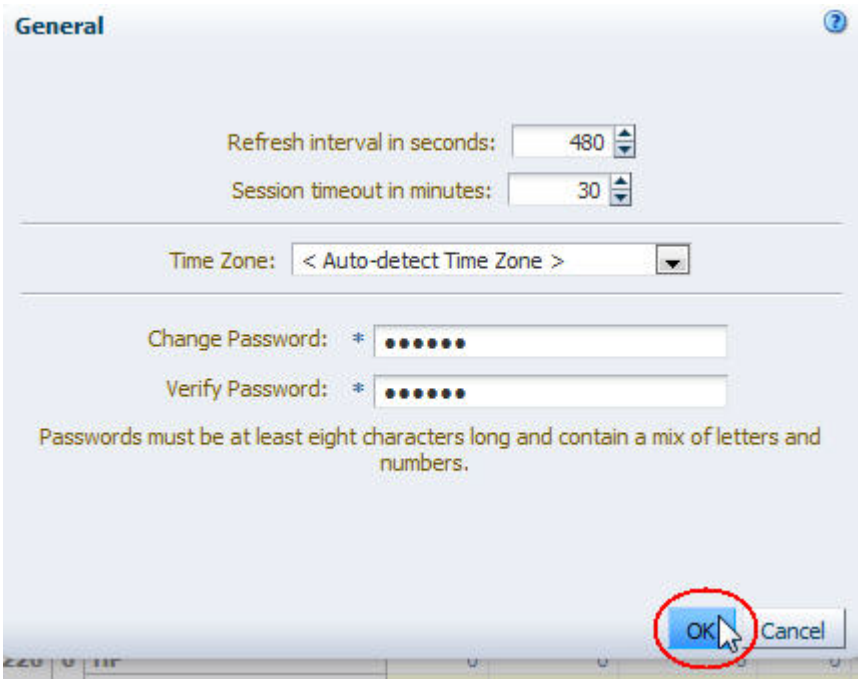
1. In the Main Toolbar, select **Preferences**, then select **General**.



The General dialog box appears.



2. In the **Change Password** field, enter the new password you want to assign. The entry is masked as you type.
3. Enter the password again in the **Verify Password** field.
4. Click **OK**.

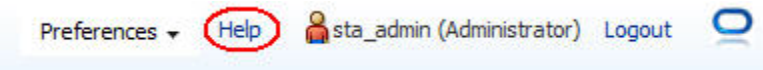


Your password is updated, and the next time you log in, you must use the new one.

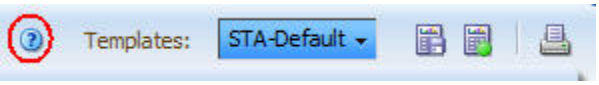
Help

STA provides context-sensitive Help for all screens. Help buttons are located on the following toolbars:

- Main Toolbar



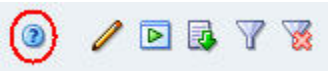
- Template Toolbar



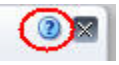
- Graphics Area Toolbar

- List View Table Toolbar (Overview screens only)

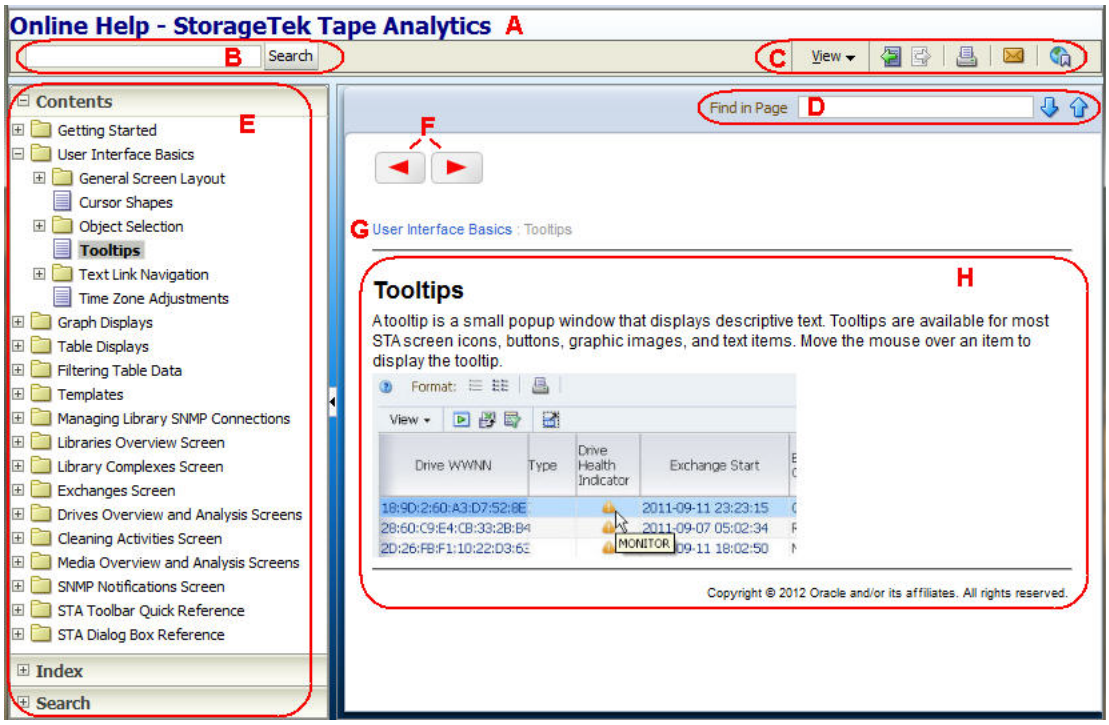
- Pivot Table Toolbar (Analysis screens only)



- Dialog boxes



Help Window Layout



Item	Name	Description
A	Title	Displays the title of the help system.
B	Helpset Quick Search	Allows you to perform a quick search throughout the helpset.
C	Help Toolbar	Provides direct access to commands for interacting with the helpset. See "Help Toolbar" on page 1-12 for details.
D	Topic Quick Search	Allows you to perform a quick search within the currently displayed topic.
E	Help Navigation Bar	Provides three navigation tabs: Contents, Index, and Search. See the following topics for details: ■ "Help Contents Tab" on page 1-13 ■ "Help Index Tab" on page 1-14 ■ "Help Search Tab" on page 1-15
F	Browse Buttons	Allows you to browse sequentially through the help topics, forward and backward.
G	Topic Breadcrumbs	Shows the current topic within the topic hierarchy. Click a parent heading to display that topic.
H	Topic Area	Displays the contents of the help topic.

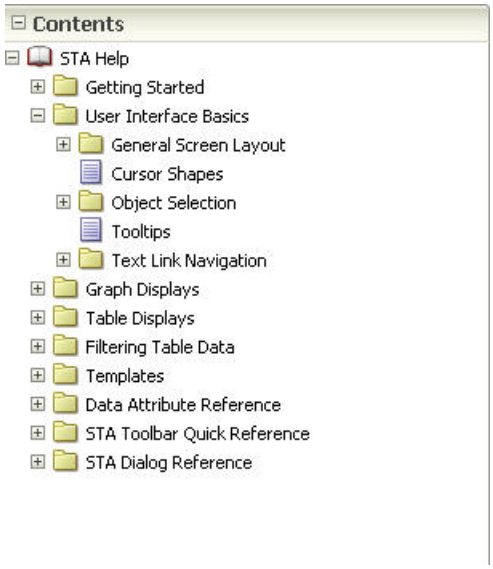
Help Toolbar

The Help Toolbar provides direct access to frequently used commands for displaying and using the help system.

Icon	Name	Description
View	View menu	Provides the following selections: ■ **Maximize Reading Pane** – Toggles the expansion or collapse of the navigator pane. ■ **Restore Default Window Layout** – Rearranges the panes according to the default layout. ■ **Contents** – Expands the Contents tab in the Help Navigation Bar. ■ **Index** – Expands the Index tab in the Help Navigation Bar. ■ **Search** – Expands the Search tab in the Help Navigation Bar. ■ **Show permanent link for this topic page** – Allows you to save a link to the current topic in your browser bookmarks.
	Go back/forward one page	Allows you to retrace your steps backward and forward through previously displayed topics.
	Print this topic page	Opens your computer's print dialog box so you can print the current topic.
	Email this topic page	Opens your computer's default email application so you can email the link to the current topic.
	Link to this topic page	Allows you to save the link to the current topic in your browser bookmarks.

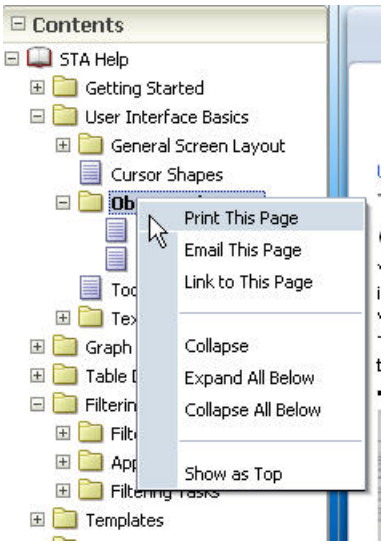
Help Contents Tab

The Contents tab displays the table of contents for the helpset. Topics are listed in a hierarchical tree, with higher-level headings shown as folders. You can expand or collapse folders to list or hide the headings within. Click a heading to display the topic in the Topic Area.



Context Menu

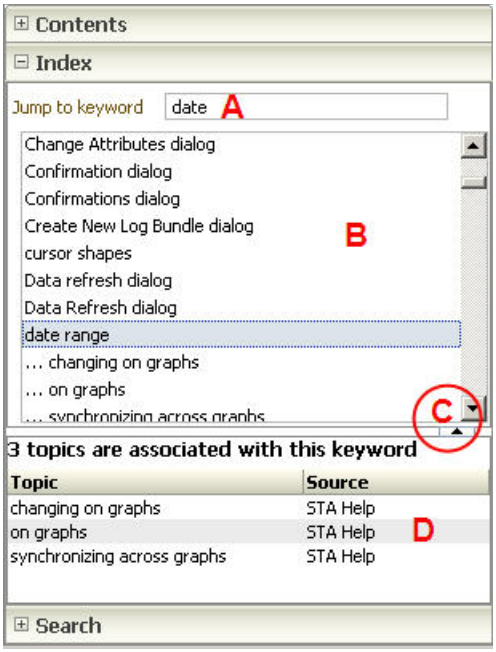
Right-click within the **Contents** Tab to bring up the Context menu.



Menu Selection	Action
Print This Page	Opens your computer's print dialog box so you can print the current topic. Also available through the Help Toolbar.
Email This Page	Opens your computer's default email application so you can email the link to this topic. Also available through the Help Toolbar.
Link to This Page	Allows you save a link to the current topic in your browser bookmarks. Also available through the Help Toolbar.
Expand	Expands the selected heading.
Collapse	Collapses the table of contents to hide the headings within the selected heading.
Expand All Below	Expands the selected heading and all sub-headings within it.
Collapse All Below	Collapses the selected heading and all sub-headings within it.
Show As Top	Displays the current heading at the top of the Contents tab.

Help Index Tab

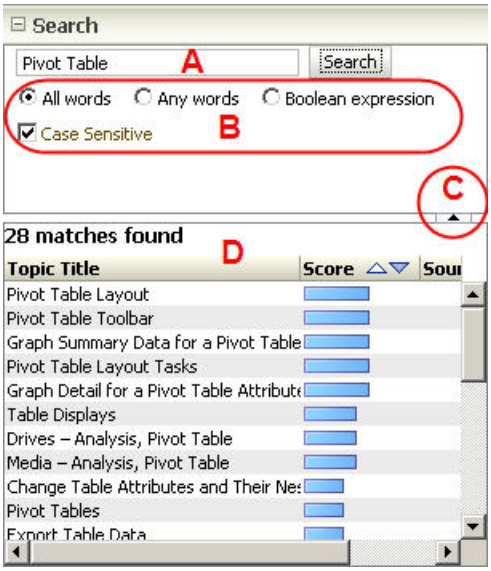
The Index tab displays a sorted index of keywords in a two-level hierarchy. A keyword can be associated with multiple topics.



Item	Name	Description
A	Jump to keyword	Enter one or more words in the text field. As you type, the first keyword in the list that matches the typed letters is selected. As more letters are typed, a more accurate selection is made.
B	Keyword list	Two-level list of keywords, sorted alphabetically. Select a keyword to display the associated topic in the Topic list.
C	Expand/Collapse Pane	Click to expand or collapse the Topic list.
D	Topic list	List of keywords. Click a keyword link to display the associated topic in the Topic Area. Click a column heading (Topic or Source) to sort by that column.

Help Search Tab

The Search tab allows you to construct a full-text query that searches throughout the helpset.



Item	Name	Description
A	Search text	Enter one or more words in the text field. As you type, the first keyword in the list that matches the typed letters is selected. As more letters are typed, a more accurate selection is made.
B	Selection criteria	Allows you to specify selection criteria for the search.
C	Expand/Collapse Pane	Click to expand or collapse the Topic list.
D	Topic list	List of search results. Includes the topic title, score, and source of each. Click a topic link to display it in the Topic Area. The Score column indicates the ranking of the topics according to how well they match the search criteria. By default, all topics are sorted by Score. Click a column heading (Topic Title, Score, or Source) to sort by that column.

2

Dashboard

The Dashboard is the first screen you see when you log in. It consists of multiple *portlets*, each showing a different view of your tape library system.

This chapter includes the following sections:

- Using the Dashboard
- Dashboard Layout
- Portlet Types
- Mobile Dashboard Display
- Dashboard Tasks

Using the Dashboard

Following is an example of the default Dashboard delivered with STA. Your display may differ if another Dashboard template has been assigned as the default for your STA username.

Dashboard
Format:
Column Count:
3
Row Height:
250
Media Health
LTO2
LTO3
LTO4
LTO5
LTO_CLNU
Media Type
0
3
6
9
12
15
18
21
24
27
30
Number of Media
Action
Evaluate
Monitor
Use
Unknown
Drive Health
Drive Model
LTO5
0
1
2
Number of Drives
Action
Evaluate
Monitor
Use
Unknown
Library He
Library Model
SL500
Action Media
Volser
Media Type
Action Date
CLNU61
LTO_CLNU
2013-06-14 04:02:59
Action Drives
Drive Serial Number
Drive Model
Acti
No drives currently in ACTION state
Cum. Data
14M
13M
11M
10M
8M
7M
6M
4M
3M
1M
0M
Megabytes
6/14/13
Library Media Cells
1.92%
25.00%
3.85%
7.69%
46.15%
15.38%
Media Type
LTO2
LTO3
LTO4
LTO5
LTO_CLNU
Unallocated
Library Drive Bays
100.00%
Drive Type
LTO5
Unallocated
Cart Move
2
1
0
Count
6/14/13

Customizing the Dashboard

The Dashboard is fully customizable. There are over 50 different portlets to display, each one showing a different set of analytic and summary data collected by STA. You can include a maximum of 30 portlets at one time. See "Portlet Types" on page 2-8 for descriptions of the available portlets.

You can rearrange portlets, change their sizes, and filter the data that is shown on each portlet. See "Dashboard Tasks" on page 2-13 for instructions.

Dashboard Templates

If you have Operator or Administrator privileges, once you have arranged a Dashboard the way you like, you can save the display as a customized Dashboard template. The order and size of the portlets and any applied filters are saved as part of the template.

Dashboard templates are the basis of Executive Reports. See "Executive Reports" on page 6-1 for details.

Note: It may take some time for a complex Dashboard arrangement to load on your screen. Applying filters to Dashboard portlets can also impact the screen loading time. If you experience long load times, you may want to break up a complex Dashboard into multiple, smaller Dashboards.

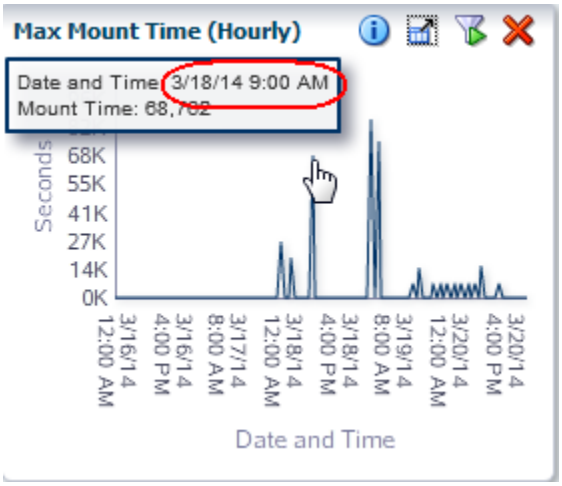
Default Dashboard

Your default Dashboard view is determined by your STA username, not your user role. There may be a different default Dashboard template for each STA username.

Times Displayed on the Dashboard

Because the Dashboard reports high-level summaries for your entire tape library system, all data is reported in UTC time. In contrast, all other STA screens report times adjusted for your local time zone (as specified in the time zone preferences for your STA username; see the*STA User's Guide* for details).

In the sample Maximum Mount Time (Hourly) graph below, the selected mount shows a date and time of 3/18/14 9:00 AM. However, if you were to view this mount on the Exchanges Overview screen, the date and time would be adjusted to your time zone preference. For example, if your preference setting were UTC-5, the selected mount would show a date and time of 3/18/14 4:00 AM.on the Exchanges Overview screen.

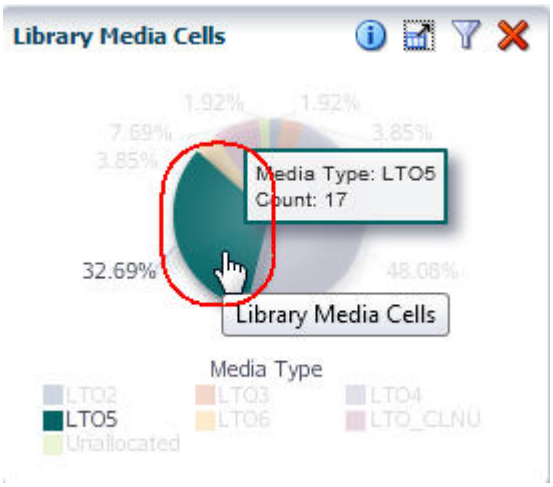


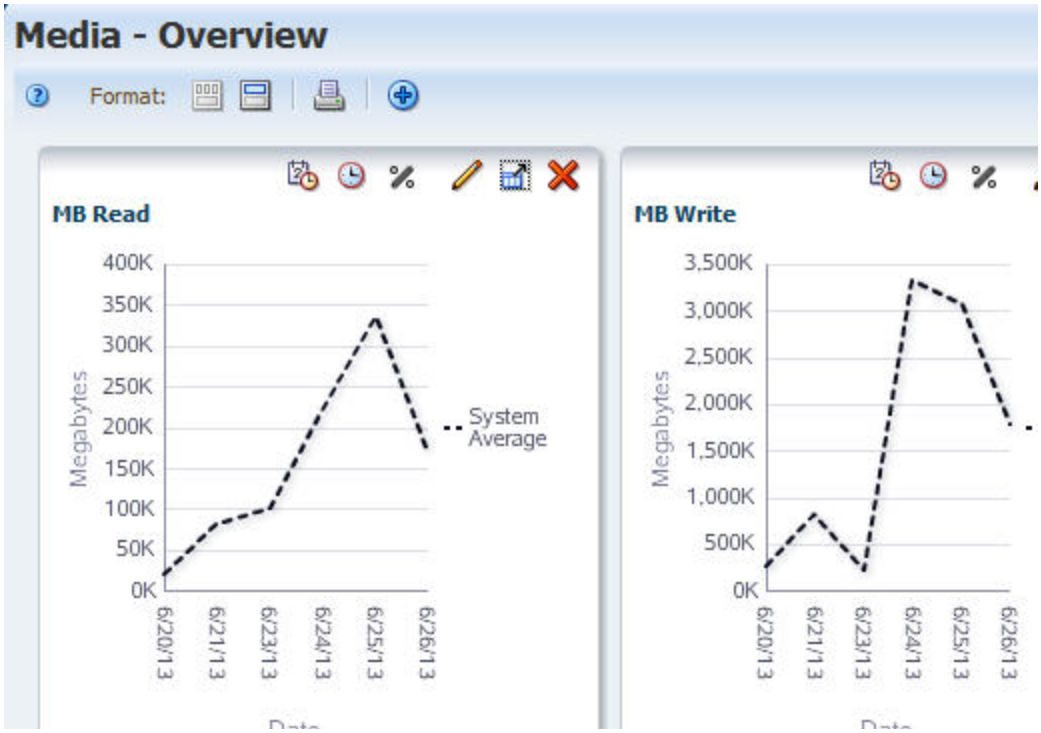
Linking to Detail Screens

Some Dashboard portlets provide links to other STA screens, allowing you to *drill down* to more detail about the selected resources. See "Filtering Using Dashboard Graphics" on page 4-8 and "Apply a Filter From the Dashboard" on page 4-16 for additional information.

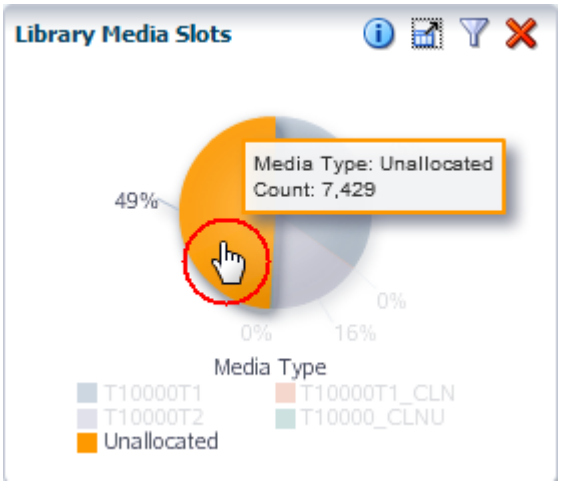
Graph Links

Bar charts, pie charts, and area charts bring up the List View for the selected resource, with a filter applied to the screen display. The following screens show how clicking on a pie chart section brings up the Media – Overview screen List View, filtered to show only the selected media type.



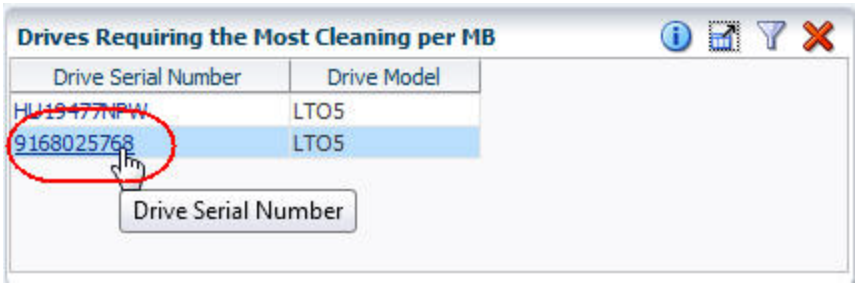


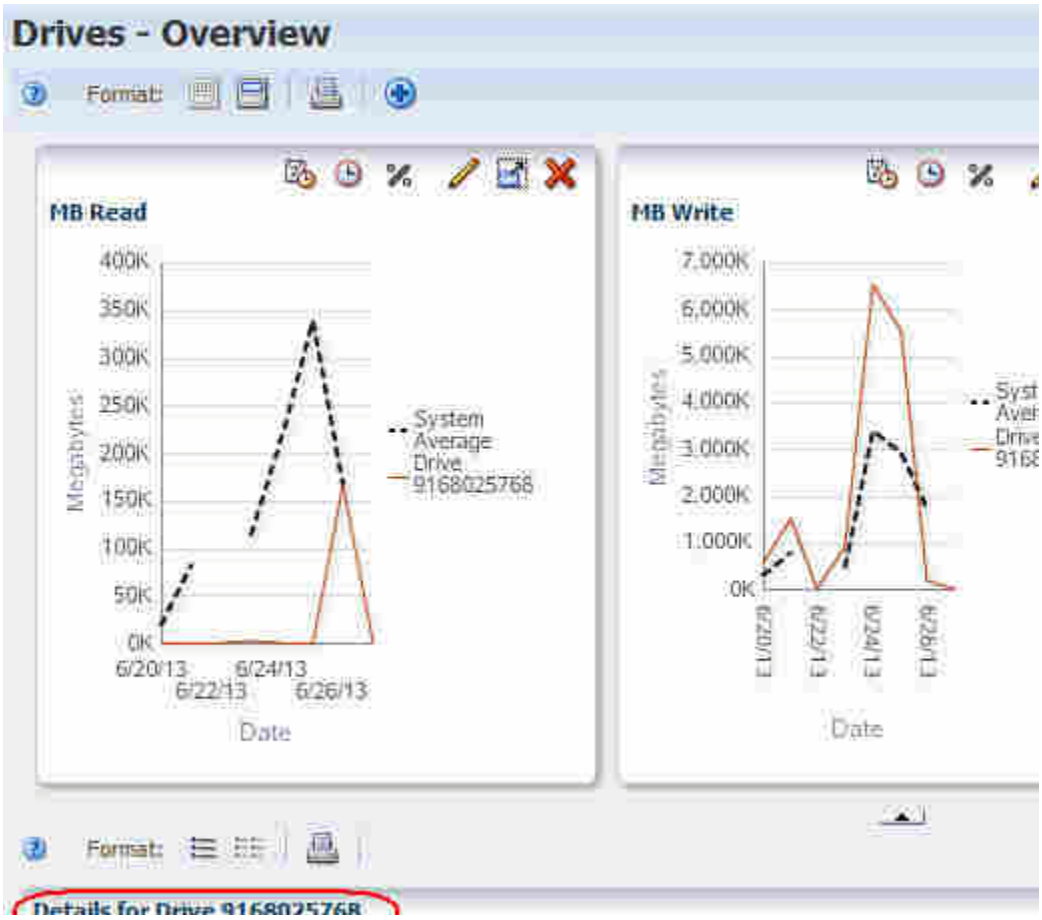
Some graph sections may not have associated Overview screen information to display. For example, in the Library Media Slots portlet below, there is no media detail available for the Unallocated category, which represents media slots that are empty or not activated. Therefore, clicking on this section of the pie has no effect.



Text Links

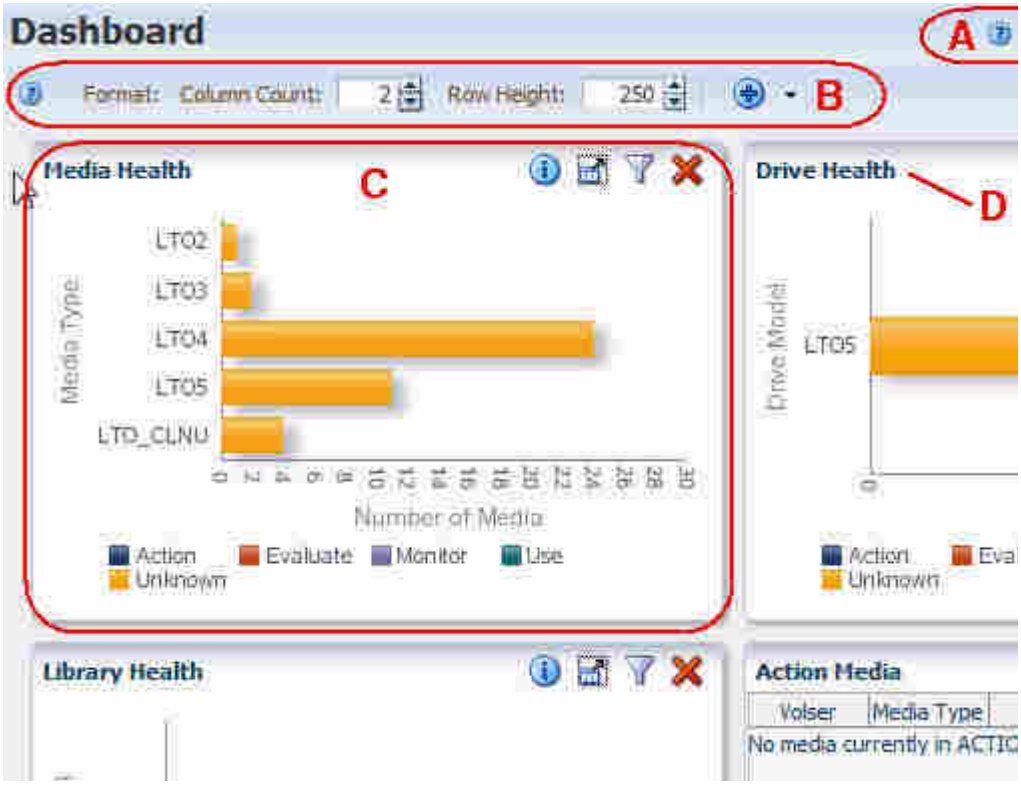
Some table portlets include text links, which bring up the Detail View for the selected resource. The following screens show how the drive serial number link on a Dashboard portlet brings up the Drives – Overview screen Detail View for the selected drive. See the *STA Screen Basics Guide* for additional information on text links.





Dashboard Layout

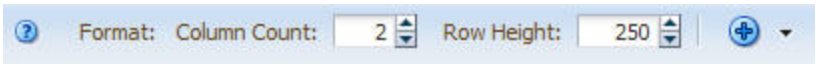
The Dashboard is divided into equal-sized portlets that are arranged in columns and rows. There can be from one to five columns, and any number of rows. Rows can be 100 to 600 pixels in height.

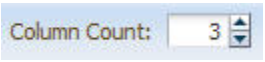
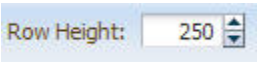
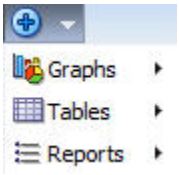


Item	Name	Description
A	Template Toolbar	Provides direct access to commands for applying and managing templates. This toolbar appears on most STA screens. See "Templates Toolbar" on page 3-5 for details.
B	Dashboard Toolbar	Provides direct access to commands for managing the Dashboard display. See "Dashboard Toolbar" on page 2-7 for descriptions of each icon.
C	Dashboard portlet	Dashboard portlets are arranged in columns and rows. Each portlet shows a different high-level view of your tape library system. See "Dashboard Portlets" on page A-1 for details.
D	Dashboard portlet title	Identifies the type of data in the portlet. See "Dashboard Portlets" on page A-1 for details.
E	Dashboard portlet toolbar	Provides direct access to commands for manipulating the display of this Dashboard portlet. See "Dashboard Portlet Toolbar" on page 2-8 for details.
F	Dashboard portlet border	Shaded area at the top of the Dashboard portlet. Allows you to grab the portlet and move it. See the *STA Screen Basics Guide* for details.
G	Vertical scrollbar	Appears only if there are additional rows below the bottom of the screen.

Dashboard Toolbar

The Dashboard Toolbar appears at the top of the Dashboard. It provides direct access to frequently used commands for controlling the overall display of the Dashboard.



Icon	Name	Description
	Help	Displays help for the Dashboard. **Related Topic:** "Help" on page 1-11
	Column Count	Displays the number of columns in the Dashboard display and allows you to change it. **Related Topic:** "Change the Dashboard Column and Row Layout" on page 2-14
	Row Height	Displays the height of each Dashboard row, in pixels, and allows you to change it. **Related Topic:** "Change the Dashboard Column and Row Layout" on page 2-14
	Add Portlet menu	Menu provides options for you to add selected graph, table, or report portlets to the Dashboard display. **Related Topic:** "Add a Dashboard Portlet" on page 2-15

Dashboard Portlet Toolbar

The Dashboard Portlet toolbar appears at the top of each Dashboard portlet. It provides direct access to frequently used commands for modifying the portlet.

Icon	Name	Description
	Panel Information	Displays a description of the portlet and allows you to add an annotation, which appears on Executive Reports. **Related Task** "Add or Change a Dashboard Portlet Annotation" on page 2-17
	Detach Pane	Detaches the portlet from the screen and displays it in a separate window in the browser foreground. **Related Topic:** the *STA Screen Basics Guide*
 	Filter Data	Displays a dialog box that allows you to define, modify, or reset filter criteria and apply them to the portlet. The first icon indicates there is no filter in effect; the second icon indicates a filter has been applied. **Related Topic:** "Apply or Change a Dashboard Portlet Filter" on page 2-18 and "Clear a Dashboard Portlet Filter" on page 2-20
	Remove Pane	Deletes the portlet from the Dashboard display. **Related Topic:** the *STA Screen Basics Guide*

Portlet Types

The following portlet types are available:

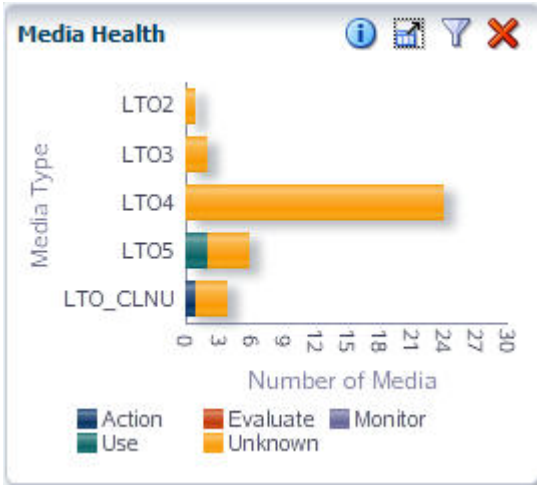
- "Graph Portlets" on page 2-9
- "Table Portlets" on page 2-10
- "Report Portlets" on page 2-11

See "Dashboard Portlets" on page A-1 for descriptions of the available portlets.

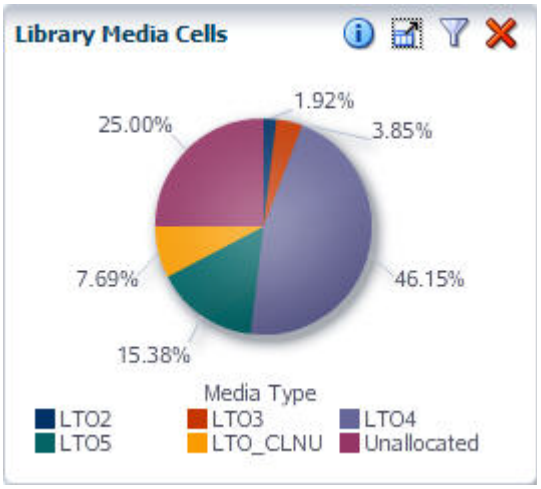
Graph Portlets

The following types of graph portlets are available. See "Graph Portlets" on page A-1 for descriptions of individual portlets. See the *STA Screen Basics Guide* for additional details about the display and uses of the various graph types.

- Bar chart—Used for point-in-time data.



- Pie charts—Used for point-in-time data.



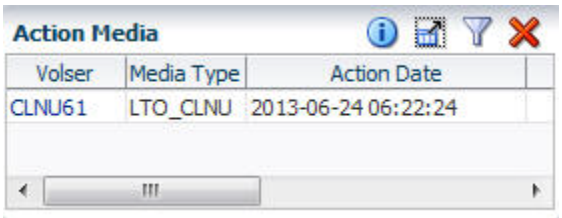
- Line graphs—Used for date and time range data.

For line graphs where there is only a single point of data—for example, a monthly graph where only a single month's data exists—a bar graph is displayed instead. Following is an example.

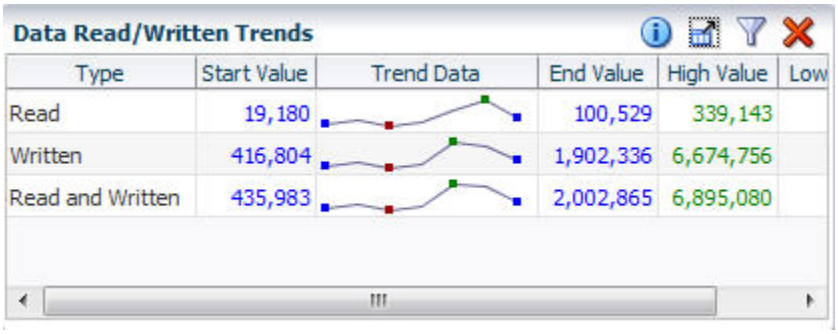
Table Portlets

The following types of table portlets are available. See "Table Portlets" on page A-4 for descriptions of individual portlets.

- List table—Displays data in a traditional list table.



- Trend report—Includes an embedded *spark chart* showing start, end, high, and low values over the range. See the *STA Screen Basics Guide* for additional information about spark charts.



Report Portlets

Report portlets are text-only windows showing current information. See "Report Portlets" on page A-6 for descriptions of individual portlets.

Mobile Dashboard Display

STA supports the Dashboard display on mobile devices. You can display any Dashboard template available to your STA username. Regardless of your user role, however, the mobile display is read-only. You cannot link to other screens from the Dashboard nor can you rearrange portlets and save templates. Therefore, Dashboard templates accessed from a mobile device must first be created through a desktop STA connection.

The Dashboard display is automatically optimized for your mobile device. For example, a three-column template may display in single column on a mobile phone but two columns on a tablet. Device rotation is also supported. See Figure 2–1 and Figure 2–2 for sample Dashboard displays.

Figure 2–1 Sample Mobile Dashboard Display on a Tablet

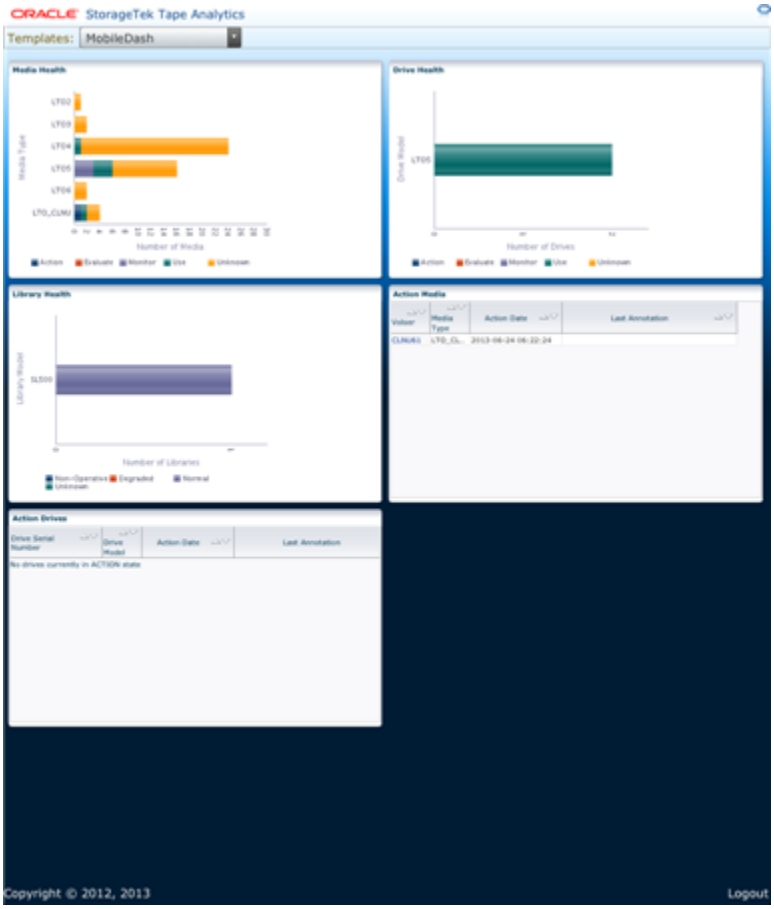


Figure 2–2 Sample Mobile Dashboard Display on a Mobile Phone

Mobile Display Requirements

The following table lists the device operating system requirements for mobile display. In addition, all devices must run the default browser version provided with the device operating system.

Device Type	Operating System
Apple iPhone and iPad	iOS 5.0 and above ■ iPhone 4S runs iOS 5.0 ■ iPhone 5 runs iOS 6.0 ■ iPad3 supports iOS 5.1.1 ■ iPads 4 and 5 support iOS 6.13
Google Android	Android 2.3 and above ■ Samsung and Amazon tablets run Android version 4.0 ■ Google tablets run Android version 4.1
Blackberry	Blackberry 7 OS and above
Windows tablets	Latest version

Accessing STA From Your Mobile Device

Your mobile device must have access to the network on which STA is running.

- If the network is publicly accessible, you can simply open a browser window on your mobile device, enter the URL of the STA application, and then log in with your STA username and password. See "Log In to STA" on page 1-4 for instructions.
- If the network is protected by a firewall or virtual private network (VPN), see your system administrator for access instructions.

Dashboard Tasks

These procedures allow you to modify the appearance and arrangement of the Dashboard. If you have Operator or Administrator privileges, once you have modified the Dashboard display, you can save the arrangement as a Dashboard template.

- "Change the Dashboard Column and Row Layout" on page 2-14
- "Add a Dashboard Portlet" on page 2-15
- "Add or Change a Dashboard Portlet Annotation" on page 2-17
- "Apply or Change a Dashboard Portlet Filter" on page 2-18
- "Clear a Dashboard Portlet Filter" on page 2-20
- "Display the Dashboard on a Mobile Device" on page 2-22

You can also perform the following procedures with the Dashboard, and the instructions are the same as for other STA display areas.

- Detach a Dashboard portlet. See the *STA Screen Basics Guide*
- Remove a Dashboard portlet. See the *STA Screen Basics Guide*.
- Save the current Dashboard display as a new or modified template (Operator and Administrator users only). See "Create a Template" on page 3-13 or "Modify a Template" on page 3-15 for detailed instructions.

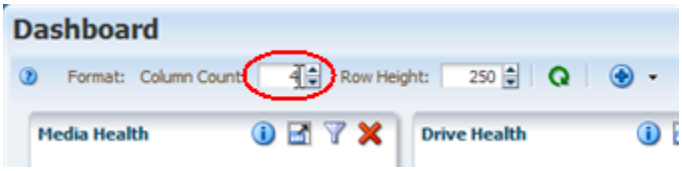
Change the Dashboard Column and Row Layout

You can change the size of the individual Dashboard portlets by modifying the column count and row height. Resizing portlets in this way can help to clarify the data.

1. In the Navigation Bar, select **Home**, then select **Dashboard**.

The default Dashboard for your STA username is displayed.

2. To change the number of portlet columns, and therefore the width of each portlet, enter a number in the **Column Count** field in the Dashboard toolbar. You can also use the spinbox control arrows to change the field value. Valid entries are 1 to 5.

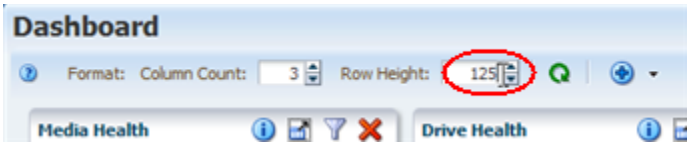


The change takes effect as soon as you press **Enter** or move the cursor to another area of the screen.

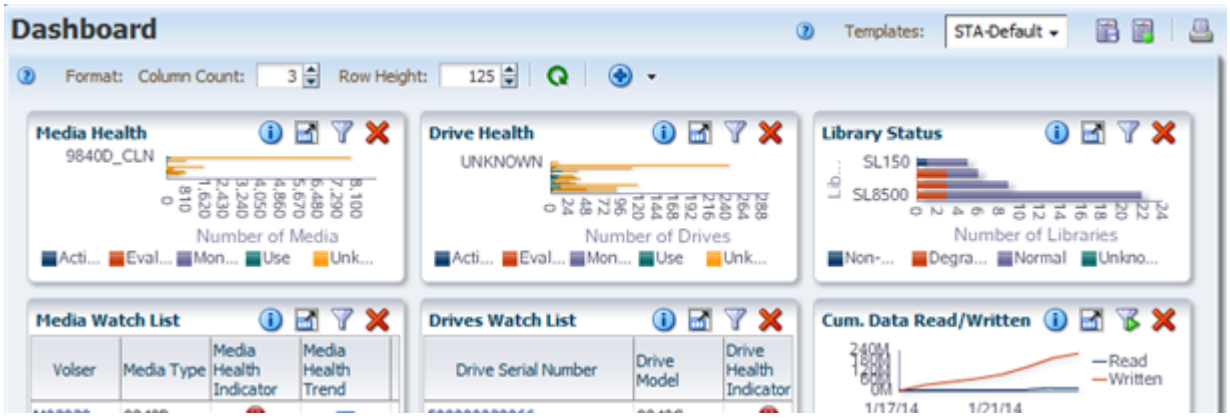
Note: If you increase the number of columns, the Dashboard Portlet toolbars may be truncated due to lack of space. Any hidden icons are available from the menu at the far-right of the toolbar.

---

3. To change the height of each portlet, enter a number in the **Row Height** field in the Dashboard toolbar. You can also use the spinbox control arrows to change the field value. Valid entries are 100 to 600.



The change takes effect as soon as you press **Enter** or move the cursor to another area of the screen.



Add a Dashboard Portlet

Use this procedure to add a portlet to the Dashboard display. You can include a maximum of 30 portlets.

You can add more than one instance of the same type of portlet, 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 portlets: one for big libraries (SL3000 and SL8500) and one for small (SL150 and SL500).

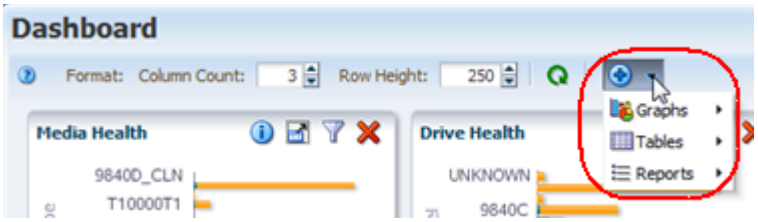
Note: Adding a large number of Dashboard portlets may result in the portlet legends being truncated or not displayed at all. If this occurs, you may want to remove some portlets to restore the legends.

---

1. In the Navigation Bar, select **Home**, then select **Dashboard**.

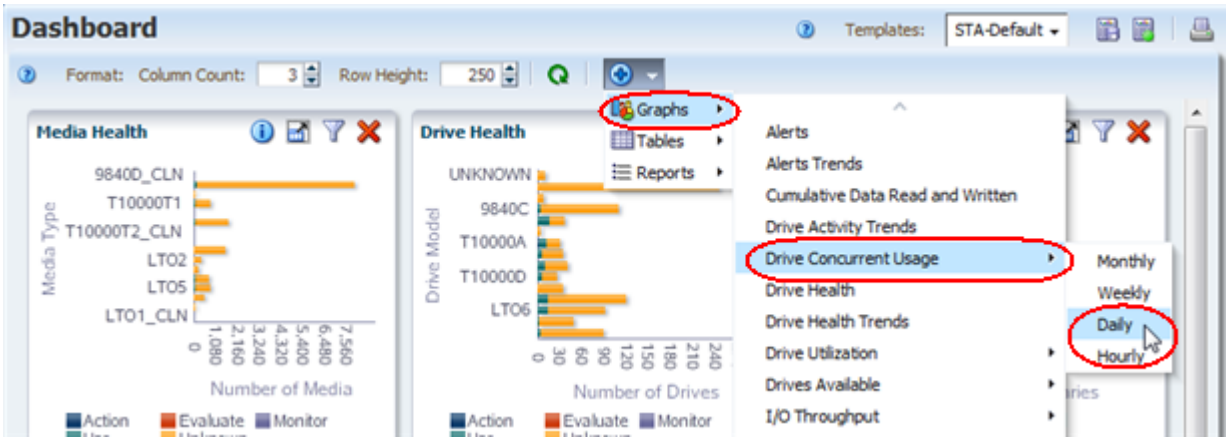
The default Dashboard for your STA username is displayed.

2. In the Dashboard toolbar, select the **Add Portlet** menu.

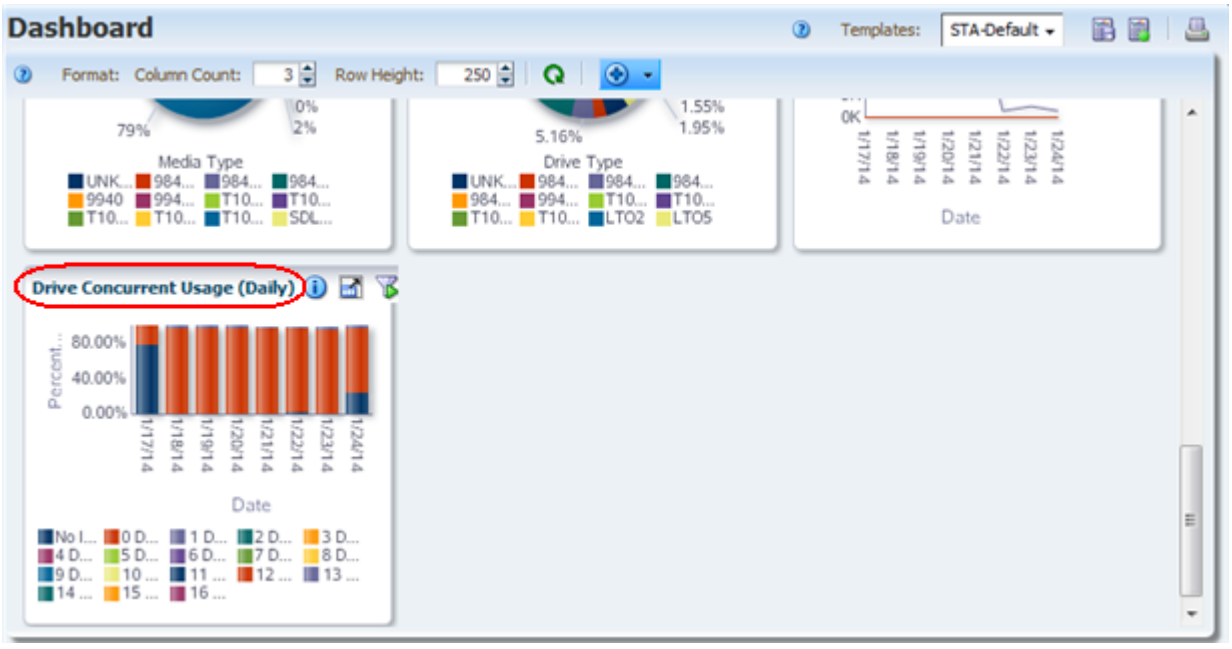


Submenus are listed for the portlet types—Graphs, Tables, or Reports.

3. From the appropriate portlet submenu, select the specific portlet you want to add. Time-related portlets provide you with options for Monthly, Weekly, Daily, or Hourly time increments.



The portlet is added to the end of the Dashboard display. You may need to use the vertical scrollbar to view it. To move the portlet to a new position, see the *STA Screen Basics Guide*.



Add or Change a Dashboard Portlet Annotation

Use this procedure to add or modify a user-defined text annotation for the current portlet. The annotation appears on Executive Reports and can be used for a variety of purposes, such as clarifying the information displayed or drawing attention to specific data.

Note: The text you enter is specific to the current Dashboard template. For example, if the Drive Health portlet appears in several Dashboard templates, each instance of the Drive Health portlet can have a different annotation associated with it.

Note: Annotation text is specific to your STA username. For example, annotations entered by one user on the Drive Health portlet do not appear to a user logged in with a different STA username.

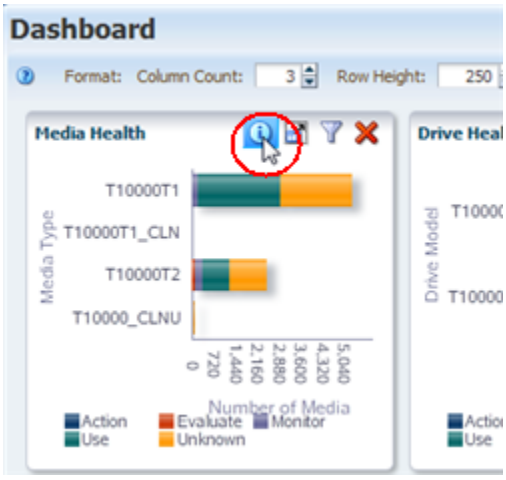
Annotations can be up to 1,000 ASCII characters in length. There are no formatting options, such as boldface or color. Also, spacing options, such as forced line feeds, are not preserved on the Executive Reports.

For an annotation to appear on an Executive Report, the current Dashboard view must be saved as a template. Additionally, if you modify a portlet annotation, any existing Dashboard templates using that portlet must be re-saved in order for the updated annotation to appear on Executive Reports. See "Create a Template" on page 3-13 and "Modify a Template" on page 3-15 for detailed instructions.

1. In the Navigation Bar, select **Home**, then select **Dashboard**.

The default Dashboard for your STA username is displayed.

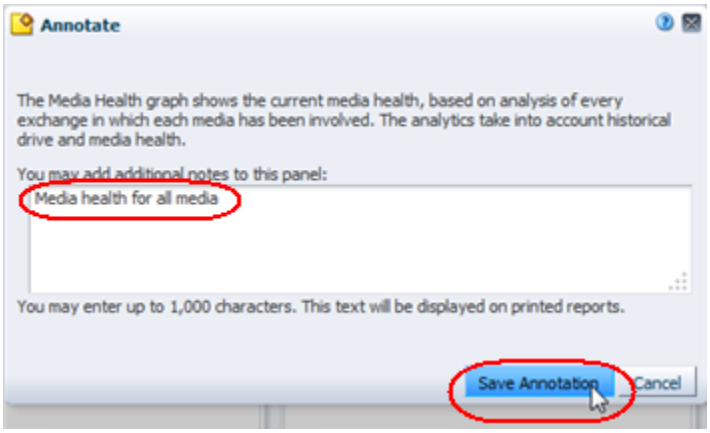
2. Click **Panel Information** in the Portlet Toolbar of the Dashboard portlet you want to annotate.



The Annotate dialog box appears.

3. Enter the annotation text you want to appear in this instance of the portlet, and click **Save Annotation** to save the information. Annotations can be up to 1,000 characters in length.

> **Note:** To better view the text, you can resize the dialog box by grabbing the lower-right corner of the text area and stretching it.



Once saved, the annotation is not visible on the Dashboard portlet itself, but can be viewed by clicking **Panel Information** again. To have the annotation appear on an Executive Report based on this Dashboard display, you must save the display as a new template or an update to an existing template.

> **Caution:** To retain this annotation for future login sessions, you must save the current display as a template or an update to an existing template. If you log out of this session without saving the template, the annotation will be lost for future login sessions and Executive Report runs.

Apply or Change a Dashboard Portlet Filter

Use this procedure to change the data displayed on a Dashboard portlet by applying a new filter or modifying an existing one.

> **Note:** To remove all filter criteria from a Dashboard portlet, see "Clear a Dashboard Portlet Filter" on page 2-20.

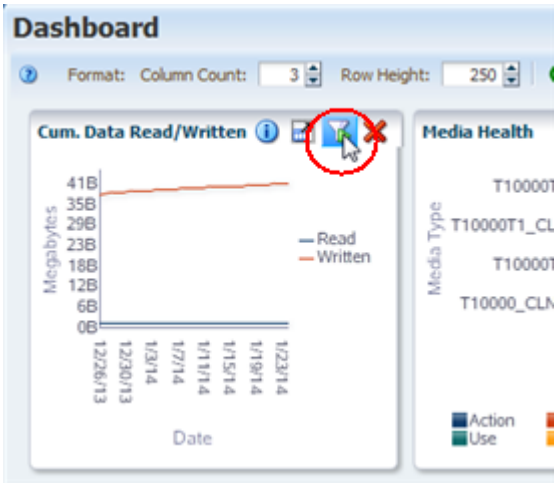
If a filter has been applied to a portlet, the **Applied Filter** icon is displayed. Some portlets are filtered by default, so they include this icon already. Hover the mouse over the icon to display a description of the applied filter.

The criteria for filtering Dashboard portlets varies by portlet type. For example, you can filter most line graphs by a date range, but you cannot do so for a pie chart.

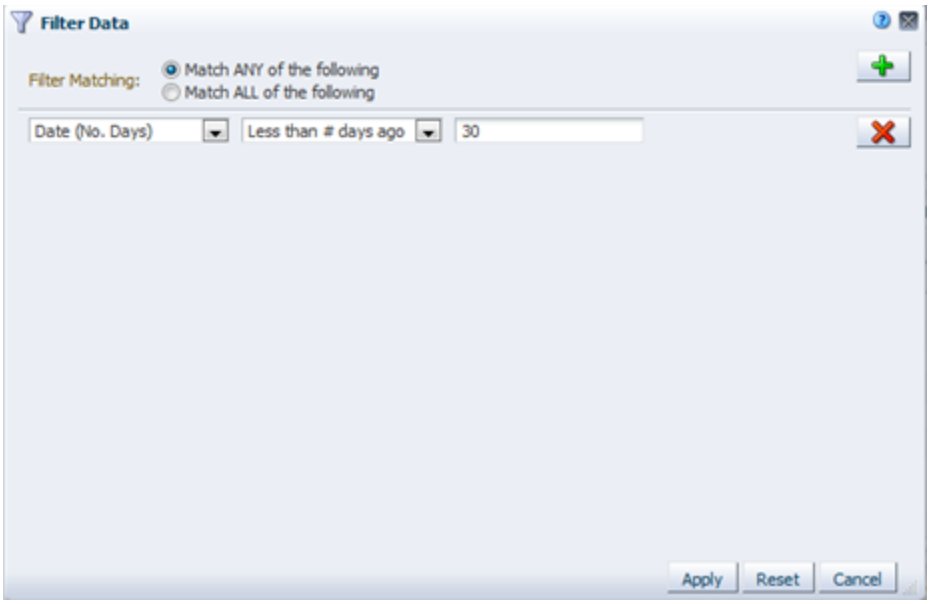
1. In the Navigation Bar, select **Home**, then select **Dashboard**.

The default Dashboard for your STA username is displayed.

2. On the Dashboard Portlet toolbar of the portlet you want to modify, click **Filter**. If the portlet already has a filter applied, click **Applied Filter**.



The Filter Data dialog box appears. If no filter has been applied, the dialog box displays the default settings. If a filter is already in effect, the criteria are displayed in the dialog box.



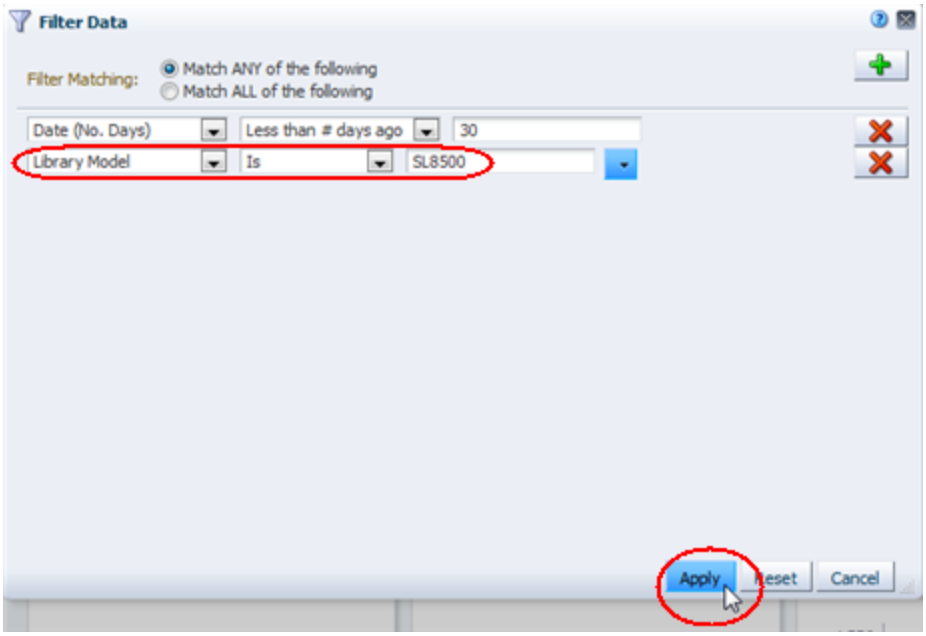
3. Specify the filter criteria in the dialog box, as follows:

   a. In the **Filter Matching** field, select one of the options to indicate whether you want to match any or all of the criteria you specify. See "Filter Data Dialog Box" on page 4-2 for details.

b. Indicate the filter criteria for as many portlet attributes as you want. Click **Add new filter criteria row** to add more criteria.

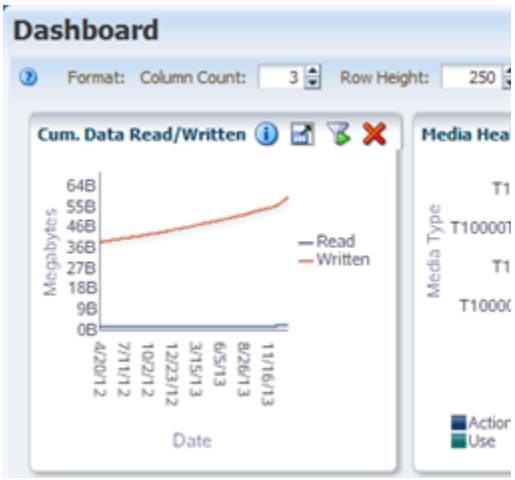
c. To remove filter criteria, click **Remove this filter criteria row**.

4. Verify that your specifications are correct, and then click **Apply**.



The following updates are made to the Dashboard portlet:

- The portlet displays a summary or analysis of only the records that match the criteria you have specified.
- The Dashboard Portlet Toolbar displays the **Applied Filter** icon.



Clear a Dashboard Portlet Filter

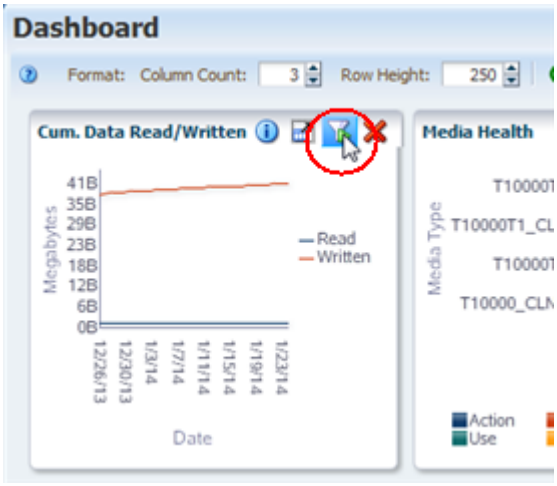
Use this procedure to remove all filter criteria from a Dashboard portlet. Unlike graph portlets on other screens, there is no **Reset Filter** icon available on Dashboard portlets.

Note: To remove selected (not all) filter criteria from a Dashboard portlet, see "Apply or Change a Dashboard Portlet Filter" on page 2-18.

1. In the Navigation Bar, select **Home**, then select **Dashboard**.

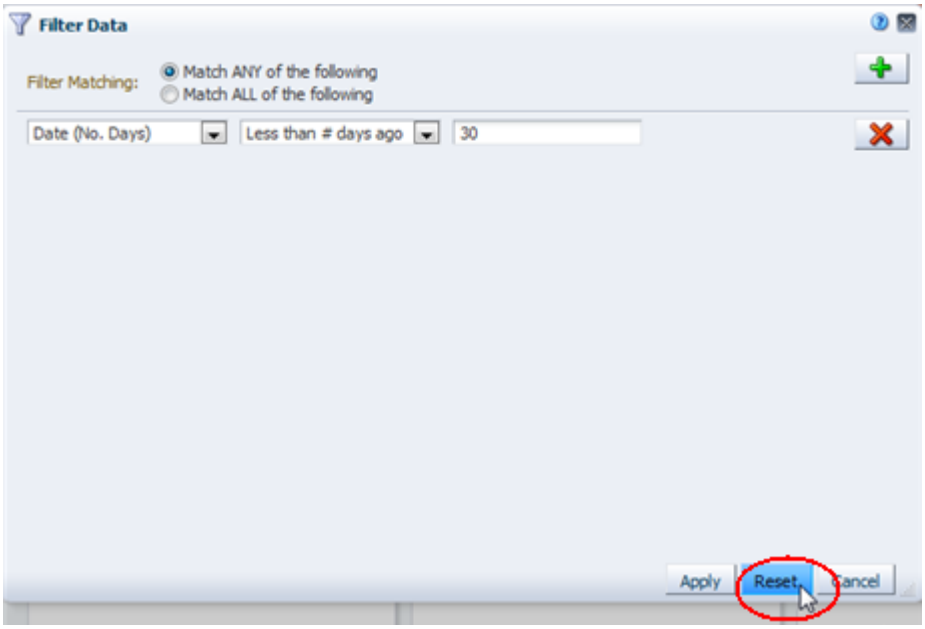
The default Dashboard for your STA username is displayed.

2. Click **Filter Data** in the Dashboard Portlet Toolbar.



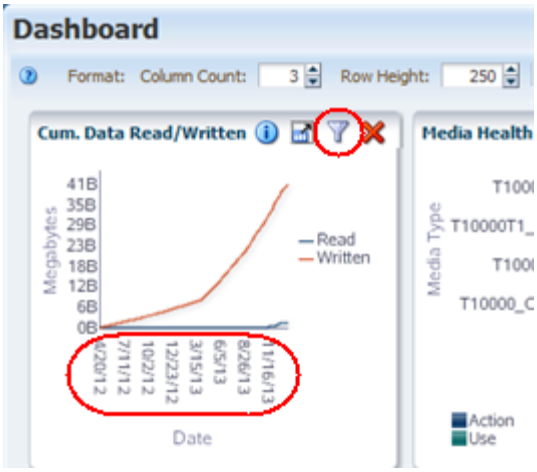
The Filter Data dialog box appears, and all selection criteria currently in effect are indicated.

3. Click **Reset**.



The following updates are made to the Dashboard Portlet:

- All filter criteria are removed from the portlet so it displays all available records.
- The Dashboard Portlet Toolbar displays the **Filter** icon.



Display the Dashboard on a Mobile Device

Use this procedure to display a read-only version of the Dashboard on a mobile device, such as a mobile phone or tablet. See "Mobile Display Requirements" on page 2-12 to verify that your device is supported.

Note: Before performing this procedure, you must obtain access to the network on which STA is running. See "Accessing STA From Your Mobile Device" on page 2-13 for details.

Note: The examples in this procedure are from a mobile phone display.

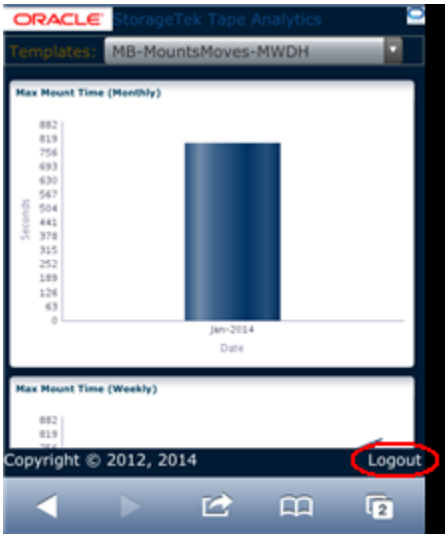
---

1. Start a browser window on your mobile device and log in to STA. See "Log In to STA" on page 1-4 for details.

   The default Dashboard template for your STA username is displayed.

2. To change the display, select the template you want to view from the **Templates** menu.

3. To log out, click the **Logout** link at the bottom of the screen.


ORACLE StorageTek Tape Analytics
Templates:
MB-MountsMoves-MWDH
Max Mount Time (Monthly)
Seconds
Jan-2014
Date
Max Mount Time (Weekly)
Copyright © 2012, 2014
Logout

3

Templates

Templates provide modified STA screen views that can be saved, reused, and shared with other users. This chapter describes the concepts and detailed procedures for creating, using, and managing templates.

This chapter includes the following sections:

- Using Templates
- Defining and Managing Templates
- Template Toolbars and Screens
- Best Practices for Templates
- Template Usage Tasks
- Template Management Tasks

Using Templates

Templates are available for the Dashboard and all screens on the **Tape System Hardware** and **Tape System Activity** tabs. They are not available for screens on the **Setup & Administration** tab.

Templates are screen-specific; a template for the Drives – Overview screen can be applied to that screen only and cannot be applied to the Drives – Analysis screen, for example. Each screen has a default template, which is the one that is automatically applied when you first navigate to that screen in a login session.

To apply a different template to a screen, you simply select the template you want to use from the **Templates** menu in the Templates toolbar. If you leave the screen and later return, the last-used template remains applied.

Template Defaults

In any given login session, the first time you navigate to a screen, the screen is displayed using the default template. Each screen has its own default, which you can designate. The default templates for each screen are user-specific, so each STA username may have its own set of assigned defaults. Each screen can have only one default.

You can assign defaults for your current STA username only. See "Set the Default Template for a Screen" on page 3-11 and "Clear the Default Template for a Screen" on page 3-12 for instructions.

The predefined templates provided with STA include a set of initial screen defaults. These templates are all named "STA-Default," one for each screen.

Predefined Templates

STA is delivered 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). To make predefined templates easy to identify, their names are prefixed "STA-".

Predefined templates are available to all users, but only users with Operator or Administrator privileges can make changes to them. You cannot modify the predefined templates directly; instead, you must save any changes to a new, custom template. You can, however, delete predefined templates that you do not use and then later restore them.

Custom Templates

Any number of custom templates can be created for each screen. Only users with Operator or Administrator privileges can create or modify custom templates.

You 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. When you save a template you assign it a name and designate its visibility (public or private) setting.

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

Once you have saved a custom template, it is immediately available for the current and future login sessions.

User Roles for Template Usage Activities

Some template activities can be performed by all user roles, whereas others are available only to users with Administrator or Operator privileges. The following table provides a summary of activities available to each role.

Note: 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.

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 **Home**, then select **Quick Links.**
Operator and above	Display a list of all templates available to your STA username Change the default screen template for your STA username	Select **Setup & Administration**, then select **Template Management**.

Defining and Managing Templates

Templates include a variety of screen display characteristics, such as graph and table layouts and filter criteria. Applying a template to a screen updates the screen display so it matches the characteristics defined in the template.

STA provides a default template for each screen, as well as a set of predefined templates, which are available to all STA usernames. You can also create your own custom templates tailored to your needs and optionally share them with other users.

STA templates exhibit *sticky* behavior, in that once a template is applied to a screen, that template continues to be displayed whenever you access that screen during the remainder of the current login session, until you explicitly apply a different template.

Screen Characteristics Included in the Template Definition

Changes to the following screen characteristics are saved as part of 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 (See the *STA Screen Basics Guide* for details.)
- Table display details, such as:
  - Hidden and visible columns
  - Column order
  - Column width
- Filter criteria

Screen Characteristics Not Included in the Template Definition

Changes to the following screen characteristics are not saved as part of the template definition:

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

Template Ownership and Visibility

Ownership and visibility for available templates are displayed on the Templates Management screen, which is available to all users with Operator or Administrator privileges. The two concepts are explained below.

Ownership

A template is owned by the STA username that created it, and the ownership cannot be changed. In the case of STA predefined templates, the owner is always "STA". If you

have Operator or Administrator privileges, you can use, modify, rename, delete, and assign default status to any templates you own.

Visibility

A template's visibility determines who can see and use the template. A template's visibility can be changed only by the owner. Visibility is either public or private, as follows:

- Public – The template is available to all STA usernames. STA predefined templates are always public. If you have Operator or Administrator privileges, you can use, modify, and delete any templates that have public visibility, even if they are owned by another STA username.
- Private – The template is available only to the STA username that owns it.

Note: When an STA username is deleted, all private templates owned by that username are automatically deleted or made public, according to the selection made by the Administrator user performing the deletion. See "Delete an STA Username" on page 9-7 for details.

Sharing Templates

You can share custom templates with other users through the STA import and export functions. 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 STA username, import the XML file, and begin using the template immediately.

See "Export a Template" on page 3-19 and "Import a Template" on page 3-19 for instructions. These activities require Operator or Administrator privileges.

User Roles for Template Management Activities

Template management template activities are available only to users with Administrator or Operator privileges. The following table provides a summary of activities available to each role.

Note: You can manage public templates and private templates owned by your current STA username. You cannot manage private templates that are owned by another STA username.

User Roles	Template Activity	Screen or Toolbar
Operator and above	Create a template	Template toolbar
	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	

User Roles	Template Activity	Screen or 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 **Setup & Administration**, then select **Templates Management**

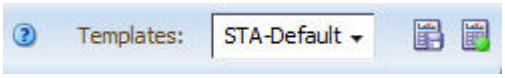
Template Toolbars and Screens

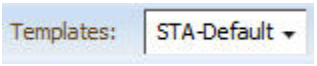
This section describes the following toolbars and screens, which allow you to use and manage templates:

- "Templates Toolbar" on page 3-5
- "Template Quick Links Screen" on page 3-5
- "Templates Management Screen" on page 3-7

Templates Toolbar

For screens that have templates, the Templates Toolbar appears at the top of the main window area. It provides direct access to frequently used commands for applying and managing templates.

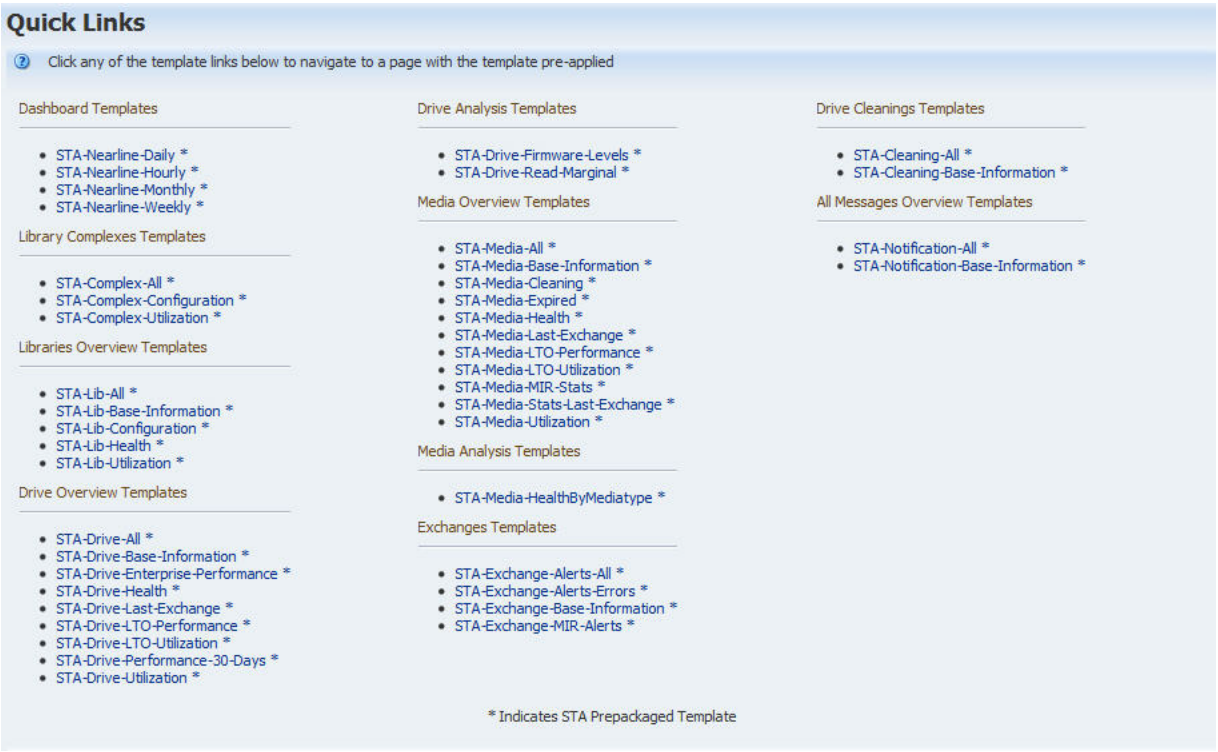


Icon	Name	Description
	Help	Displays help for template functions. **Related Topic:** "Help" on page 1-11
	Templates menu	Menu lists all available templates for this screen. The first entry is always "STA-Default". The list includes all predefined and custom templates available to the current user. Select a template to apply it to the current screen. **Related Topic:** "Apply a Template" on page 3-8
	Save Template	Allows you to save the current screen configuration, either as a new template or as a modification of an existing template (if you are the owner). **Note:** This icon is available only for Operator and Administrator users. **Related Topic:** "Create a Template" on page 3-13 and "Modify a Template" on page 3-15
	Default Template	Allows you to set the current template as the screen default for the current STA username. **Related Topic:** "Set the Default Template for a Screen" on page 3-11

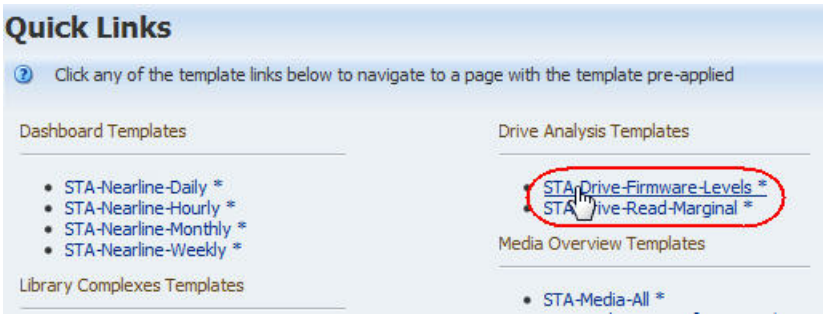
Template Quick Links Screen

The Quick Lists screen provides links to templates available to your STA username. Following is a sample of the default Quick Links screen provided with STA. Because

the list is specific to the current STA username, your display may differ if other templates are available to your STA username.



As shown in the following screen sample, each template name is a hot link, which you can click to navigate to that screen with the selected template automatically applied.



The templates are grouped by screen, such as Libraries Overview Templates, Drive Analysis Templates, Exchanges Templates, and so on. Within each screen group, the templates are listed in alphabetical order. The list is automatically updated with new templates or template name changes.

Quick links are available for the following template types:

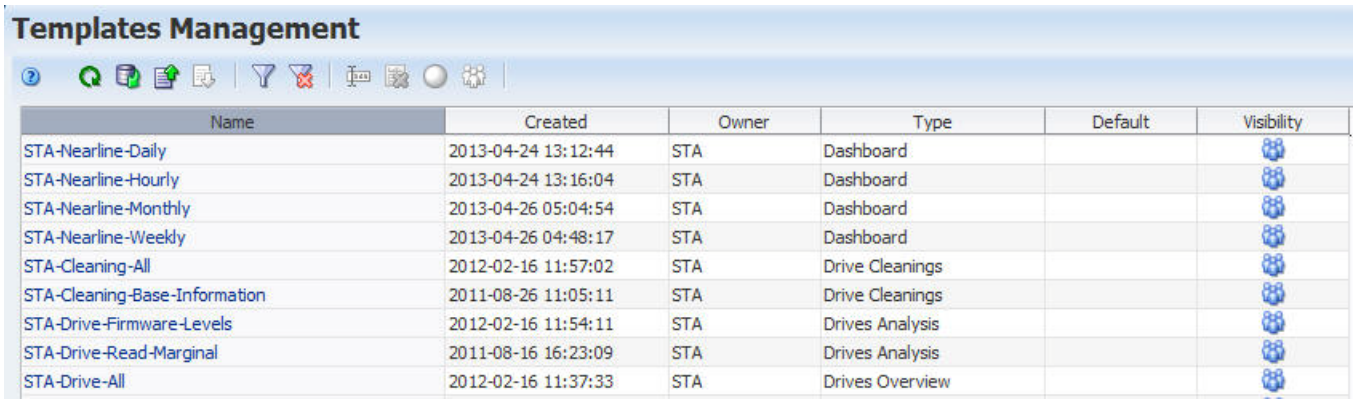
- All predefined templates – These are identified with an asterisk (*) after the name
- All custom public templates
- All custom private templates owned by the current STA username

Note: The Quick Links screen does not include the templates named "STA-Default" for each screen group. Therefore, if the only template available to your STA username for a particular screen is the one named "STA-Default," that group is not listed. It is added to the screen as soon as an available custom template is added.

Templates Management Screen

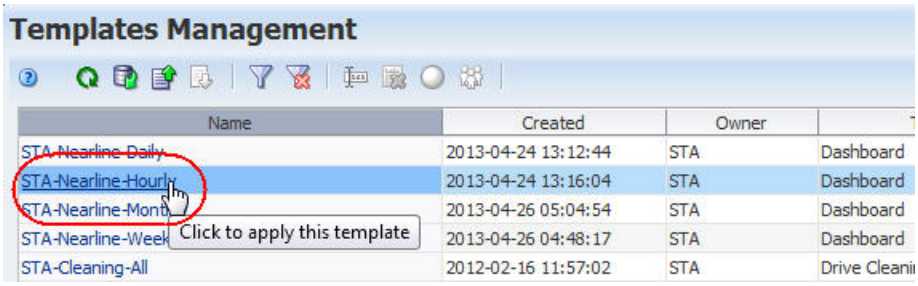
The Templates Management screen, which is found on the **Setup & Administration** tab, is available only to Operator and Administrator users.

Following is a sample of the default Templates Management screen provided with STA. Because the list is specific to the current STA username, you may see different templates listed on your display.



Name	Created	Owner	Type	Default	Visibility
STA-Nearline-Daily	2013-04-24 13:12:44	STA	Dashboard		
STA-Nearline-Hourly	2013-04-24 13:16:04	STA	Dashboard		
STA-Nearline-Monthly	2013-04-26 05:04:54	STA	Dashboard		
STA-Nearline-Weekly	2013-04-26 04:48:17	STA	Dashboard		
STA-Cleaning-All	2012-02-16 11:57:02	STA	Drive Cleanings		
STA-Cleaning-Base-Information	2011-08-26 11:05:11	STA	Drive Cleanings		
STA-Drive-Firmware-Levels	2012-02-16 11:54:11	STA	Drives Analysis		
STA-Drive-Read-Marginal	2011-08-16 16:23:09	STA	Drives Analysis		
STA-Drive-All	2012-02-16 11:37:33	STA	Drives Overview		

As shown in the following screen sample, each template name is a hot link, which you can click to navigate to that screen with the selected template automatically applied.



Best Practices for Templates

This section provides tips for defining and using custom templates.

Predefined template reserved names

When naming templates, do not start the name with "STA-". This prefix is used by STA for all predefined templates distributed with the STA package.

See "Custom Templates" on page 3-2.

Use consistent template names and prefixes

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".

Create custom templates
Create custom templates that can be used to address the top three tape operation concerns at your site. Identifying your top uses for STA gives you a smaller, more understandable and manageable focus within its vast data mine.

See "Create a Template" on page 3-13.

Specific views and data
Using templates to create specific views that show only the items that interest you will speed up your use and navigation in the user interface by many times.

See "Template Usage Tasks" on page 3-8.

Modify existing templates
When creating custom templates, there are probably already templates very close to what you need; modify existing ones rather than starting from scratch.

See "Modify a Template" on page 3-15.

Templates and filters
Remember to use filters to separate different parts of your operations. A Dashboard that allows you to compare and contrast the same attributes but in different parts of your library environment is invaluable. You must create them yourself onsite.

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.

Exporting templates
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.

See the following sections:

- "Export a Template" on page 3-19
- "Import a Template" on page 3-19

Template Usage Tasks

- "Apply a Template" on page 3-8
- "Set the Default Template for a Screen" on page 3-11
- "Clear the Default Template for a Screen" on page 3-12

Apply a Template

Use this procedure to apply a template to the current screen. When you initially navigate to a screen in a login session, the default template for your STA username is applied automatically.

You can perform this procedure with any of the following methods:

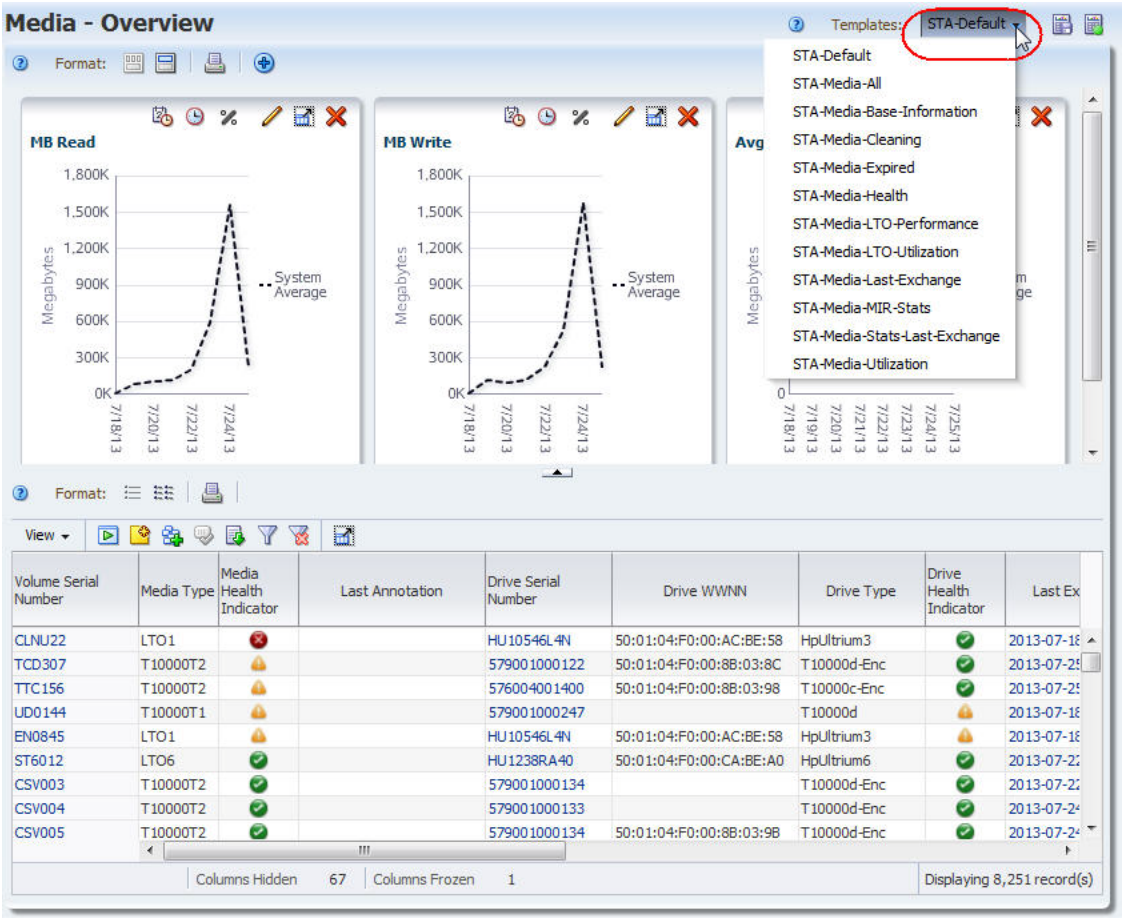
- "Using the Templates Toolbar" on page 3-9
- "From the Quick Links Screen" on page 3-10
- "From the Templates Management Screen" on page 3-11

Using the Templates Toolbar

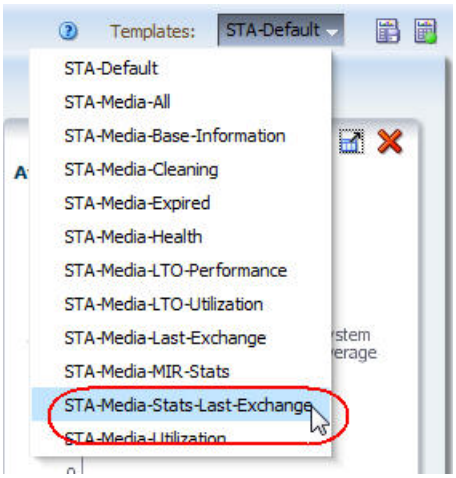
Note: This option can be performed by any user.

1. In the current screen, select the **Templates** menu.

   The menu displays all templates that are available to your STA username. The currently displayed template is identified in the dark area of the **Templates** field.

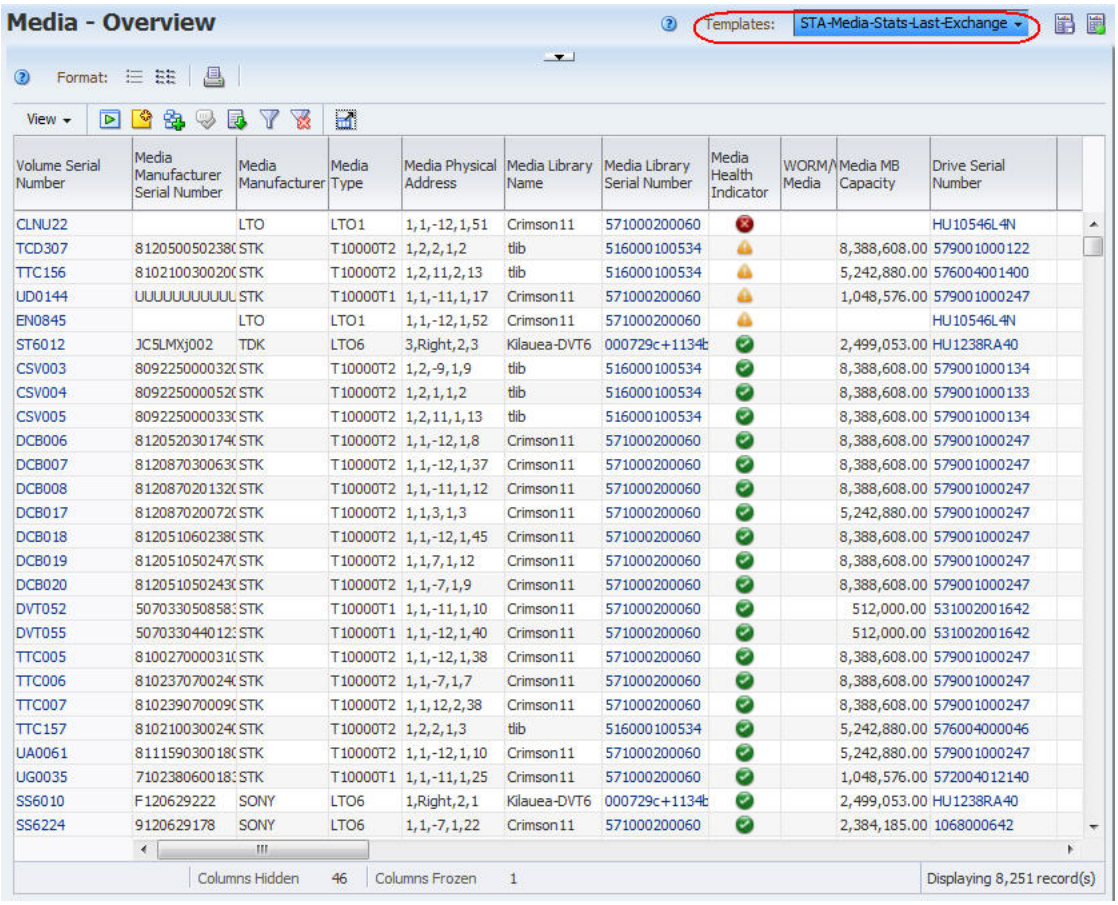


2. In the **Templates** menu, select the template you want to apply.



The new template is applied.

Note: You can always verify the currently applied template by viewing the name displayed in the **Templates** field.



From the Quick Links Screen

Note: This option can be performed by any user.

1. In the Navigation Bar, select **Home**, then select **Quick Links**

The screen displays templates available to your STA username.

Note: The templates named "STA-Default" are not included in the list.

2. Select the text link of the template you want to use.
3. You are taken to the screen with the selected template applied.

From the Templates Management Screen

> **Note:** This option requires Operator or Administrator privileges.

1. In the Navigation Bar, select **Setup & Administration**, then select **Templates Management**.

The screen displays all templates available to your STA username.

> **Note:** The templates named "STA-Default" are not included in the list.

2. Select the text link of the template you want to use.
3. You are taken to the screen with the selected template applied.

Set the Default Template for a Screen

Use this procedure to assign a template as the screen default for your STA username. You can set only one default per screen, although each STA username can have its own set of defaults.

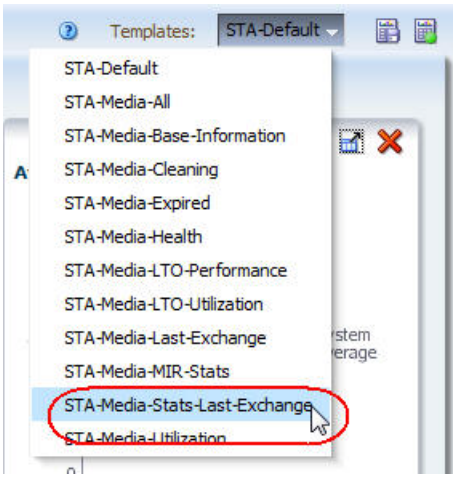
> **Note:** You cannot assign default templates for other STA usernames.

You can perform this procedure with either of the following methods:

- "From the Templates Toolbar" on page 3-12
- "From the Templates Management Screen" on page 3-12

From the Templates Toolbar

1. In the current screen, from the **Templates** menu select the template you want to be the default.



   The template is applied.

2. In the **Templates** menu, click **Default Template**.

   The template is updated to be your default for this screen.

From the Templates Management Screen

> **Note:** This option requires Operator or Administrator privileges.

1. In the Navigation Bar, select **Setup & Administration**, then select **Templates Management**.
2. Select the template you want to be the default for the selected screen.
3. Click **Set Default** in the Templates Management toolbar.

   The template is updated to be your default for the selected screen. This update does not take effect until your next login session.

Clear the Default Template for a Screen

Use this procedure to clear the default template setting for a screen and re-assign the "STA-Default" template as the screen default for your STA username.

> **Note:** You cannot clear default templates for other STA usernames.

> **Note:** This procedure requires Operator or Administrator privileges.

1. In the Navigation Bar, select **Setup & Administration**, then select **Templates Management**.
2. Select the template you want to be the default for the indicated screen type.
3. Click **Clear Default** in the Templates Management toolbar.

The "STA-Default" template is re-assigned as your default template for the selected screen.

Template Management Tasks

- "Create a Template" on page 3-13
- "Modify a Template" on page 3-15
- "Rename a Template" on page 3-18
- "Change the Visibility (Public or Private) Settings for a Template" on page 3-18
- "Export a Template" on page 3-19
- "Import a Template" on page 3-19
- "Delete a Template" on page 3-21
- "Restore the STA Predefined Templates" on page 3-22

Create a Template

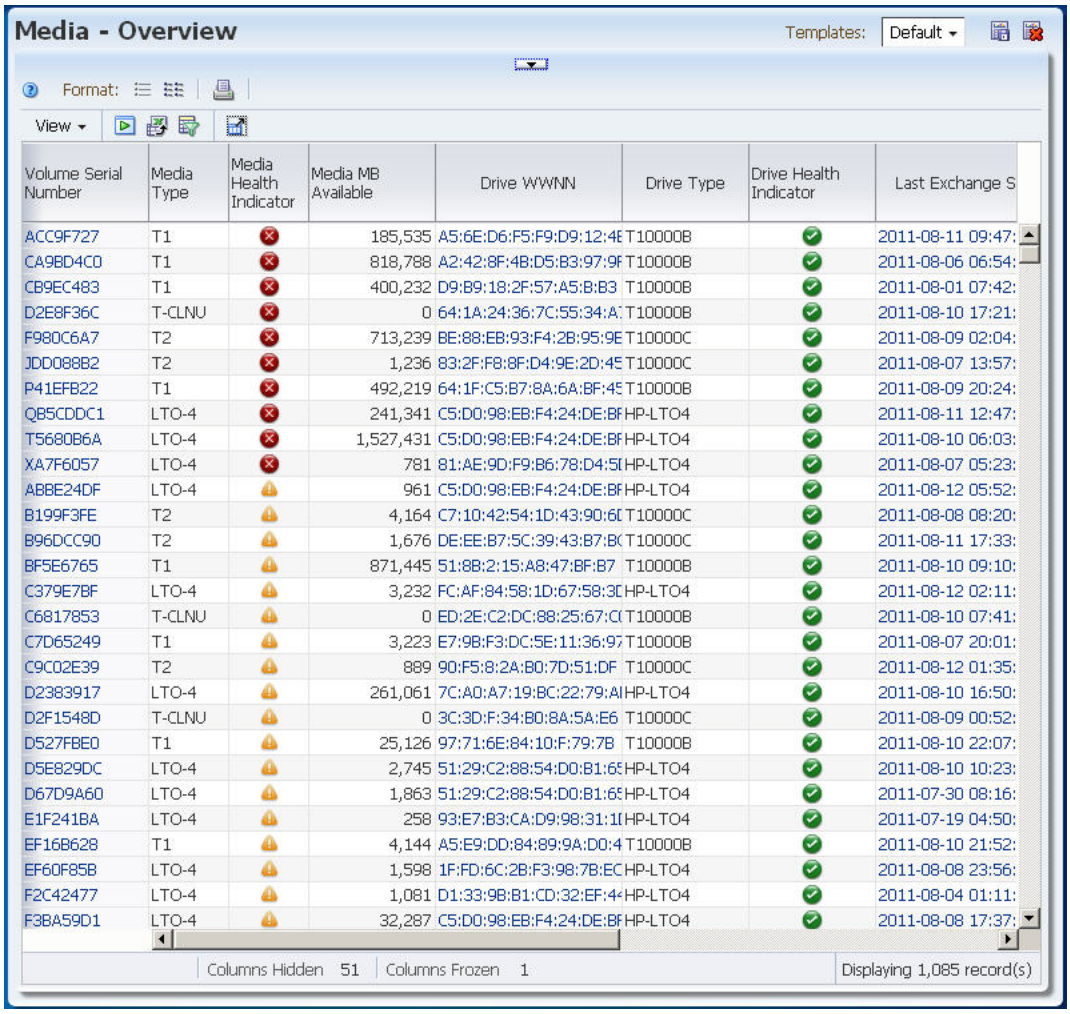
Use this procedure to create and save a new template for the current screen. You can designate whether the template will be available to your STA username only or to all.

Note: This procedure requires Operator or Administrator privileges.

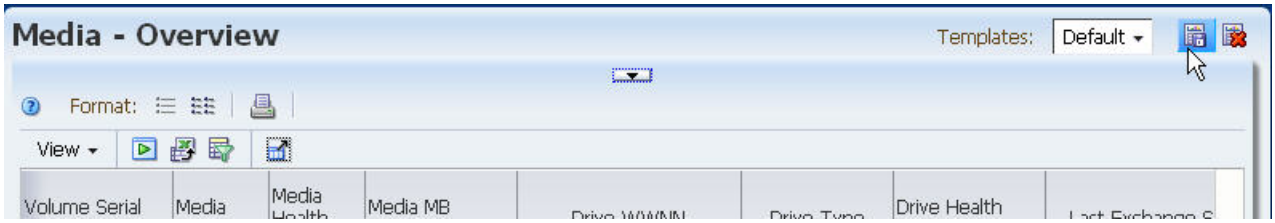
1. Apply the desired changes to the current screen.

   Note: See "Screen Characteristics Included in the Template Definition" on page 3-3 for the types of screen changes that can be included in a template.

   In the following example, the Media – Overview screen has been modified by collapsing the graphics pane so that only the tables area is visible.



2. When you have made all the modifications you want, click **Save Template**.



The Save Template dialog box appears.

3. Complete the Save Template dialog box, as follows:
   a. In the **Template Name** field, type a new, unique name.

Note: If the name already exists, when you click **Save**, depending on your user Confirmations preferences, you may be asked to confirm whether you want to overwrite the existing template. See "Modify a Template" on page 3-15 for instructions.

b. In the **Shared** field, select a visibility option. See "Template Ownership and Visibility" on page 3-3 for additional information.

* Private – The template will be available to the current STA username only.
* Public – The template will be available to all STA usernames.

4. Click **Save**.

The template is saved and the name is displayed in the **Templates** menu.

Modify a Template

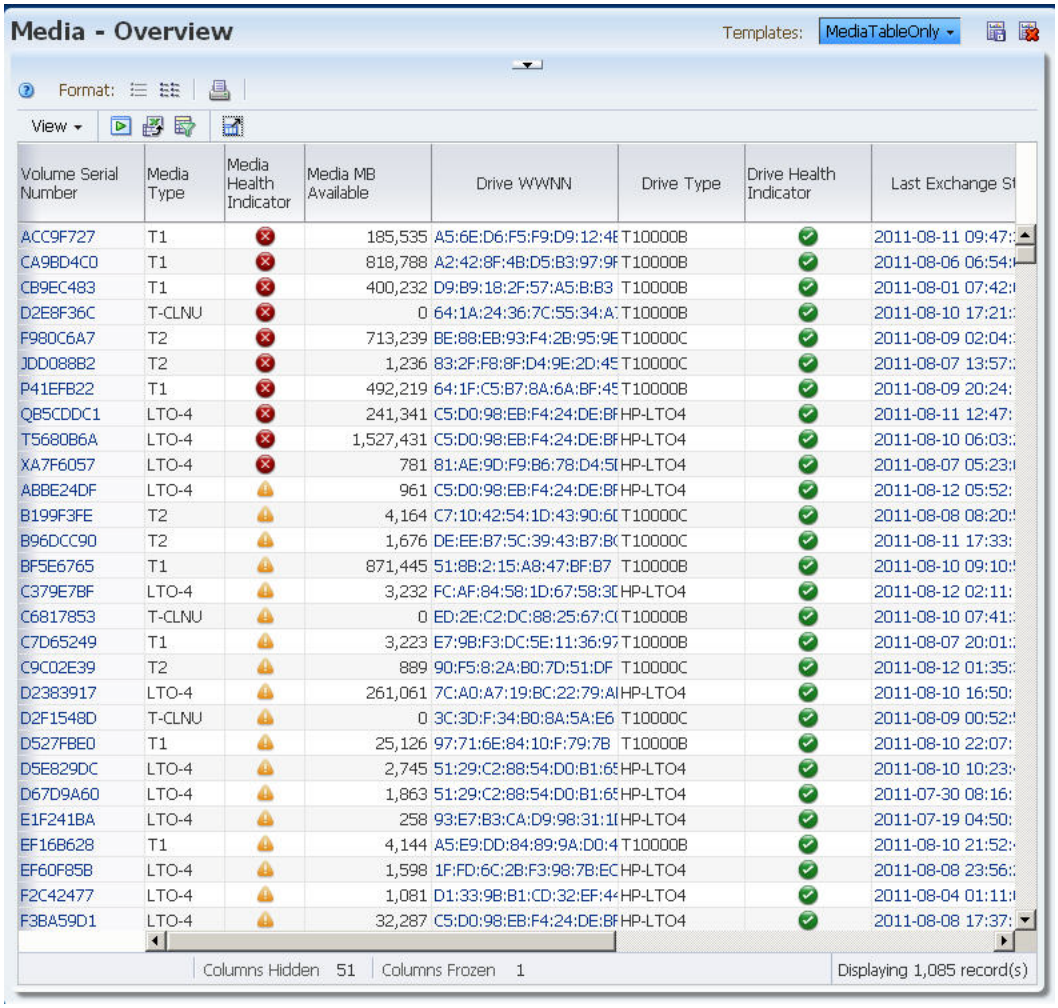
Use this procedure to modify an existing template for the current screen. You can modify any custom template owned by your STA username.

You must be the owner of the template to modify it directly. To modify an STA predefined template or public template owned by another STA username, you must save the modifications to a new name. See "Create a Template" on page 3-13 for instructions.

Note: This procedure requires Operator or Administrator privileges.

1. In the **Templates** menu, select the template you want to modify.

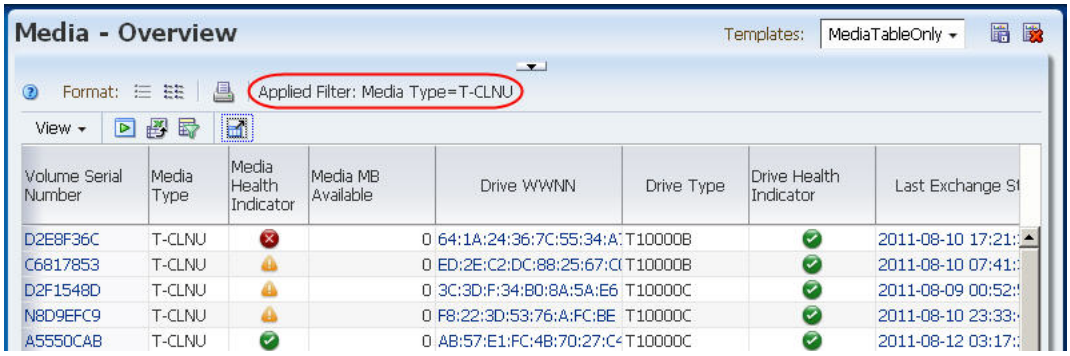
The template is applied to the screen.



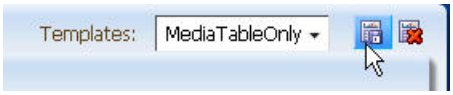
2. Make the screen changes you want to include in the template.

Note: See "Screen Characteristics Included in the Template Definition" on page 3-3 for the types of screen changes that can be included in a template.

In this example, the screen is modified by applying the filter, "Media Type=TCLNU".

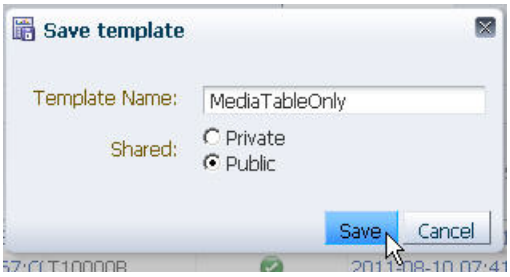


3. Verify your changes, and then click **Save Template** in the Templates Toolbar.



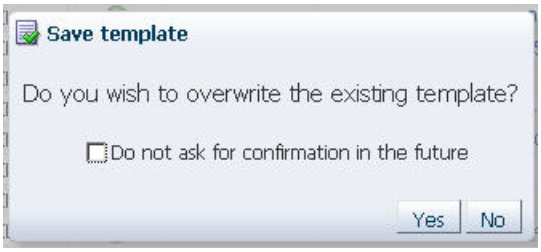
The Save Template dialog box appears, and the current template name is supplied in the **Template Name** field.

4. Complete the Save Template dialog box, as follows:
   a. Leave the **Template Name** field as is.
   b. Depending on whether you want to modify the visibility of the template, either select an option in the **Shared** field or leave the field as is:
      * 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**.

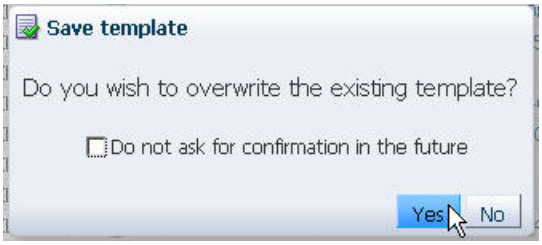


The Template Overwrite Confirmation dialog box appears.

> **Note:** This dialog box does not appear if it has been turned off. See the *STA Screen Basics Guide* for details.



6. Click **Yes** to confirm the modification.



The template is updated with the changes you have specified.

Rename a Template

Use this procedure to rename an existing custom template. You can rename any custom template available to your STA username, even if you are not the owner. You cannot rename STA predefined templates.

Note: This procedure requires Operator or Administrator privileges.

1. In the Navigation Bar, select **Setup & Administration**, then select **Templates Management**.
2. Select the custom template you want to rename.
3. Click **Rename** in the Templates Management toolbar.

   The Rename Template dialog box appears.
4. In the **New Name** field, type the name you want to assign. Your entry must be unique; you cannot enter a name that has already been assigned.
5. Click **OK**.

   The name is updated.

Change the Visibility (Public or Private) Settings for a Template

Use this procedure to assign public or private visibility to a template owned by your STA username.

Note: This procedure requires Operator or Administrator privileges. In addition, your STA username must be the owner of the template.

1. In the Navigation Bar, select **Setup & Administration**, then select **Templates Management**.
2. Select the template you want to modify.

   If the template is currently private, the **Make Template Public** icon in the Templates Management toolbar becomes active. If the template is currently public, the **Make Template Private** icon becomes active.
3. Click **Make Template public/ private**.

   The template is updated to according to your selection.

Export a Template

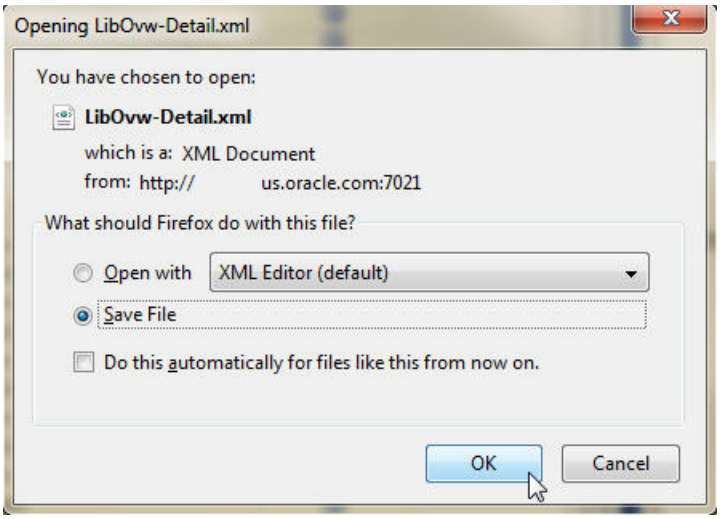
Use this procedure to export a custom template from the STA application to your computer in XML format. This allows you to share custom templates with other users.

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

> **Note:** This procedure requires Operator or Administrator privileges.

1. In the Navigation Bar, select **Setup & Administration**, then select **Templates Management**.
2. Select the custom template you want to export.
3. Click **Export** in the Templates Management toolbar.

   The file is downloaded to your computer according to your browser settings. See your browser documentation for details. Following is a sample dialog box you might see on a computer running Windows. Note that the file will be saved with a .xml extension.



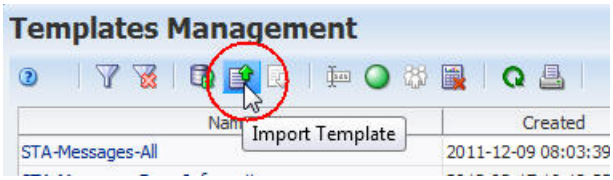
Import a Template

Use this procedure to import an STA template received from another source so it is available to your STA username. This allows another user to export and email a custom template to you for your use. See "Sharing Templates" on page 3-4 for additional information.

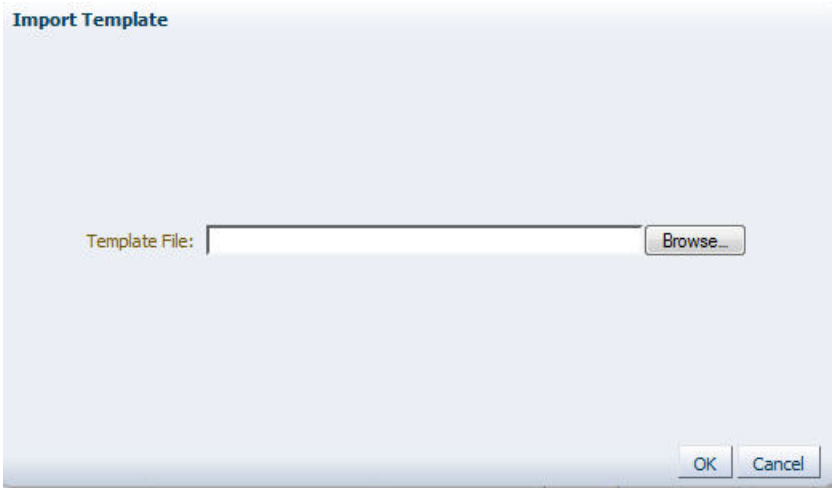
> **Note:** This procedure requires Operator or Administrator privileges.

The template you want to import must be located on a drive accessible to your computer, such as a local drive, network drive to which you are connected, or a flash drive mounted on your computer.

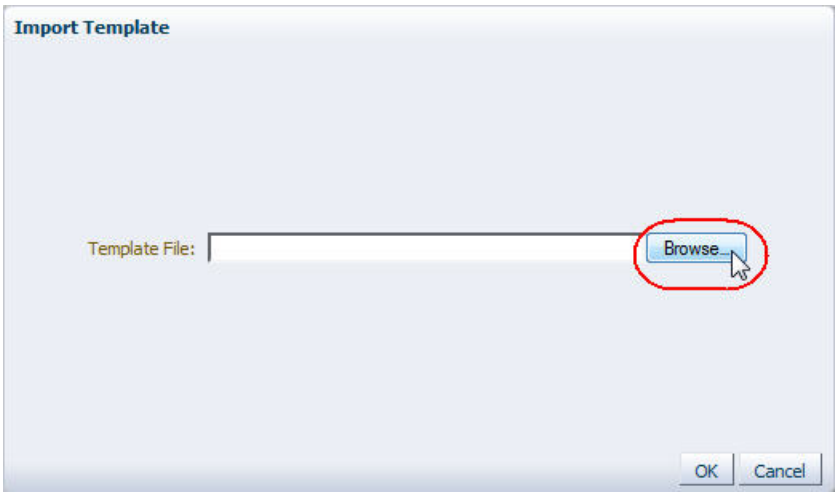
1. In the Navigation Bar, select **Setup & Administration**, then select **Templates Management**.
2. Click **Import Template** in the Templates Management Toolbar.



The Import Template dialog box appears.



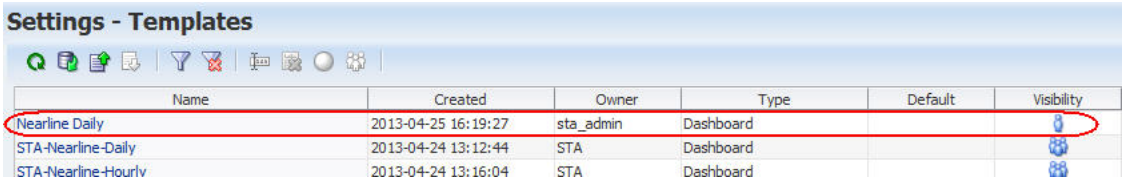
3. Click **Browse** and navigate to the location of the template file you want to import.



A navigation dialog box appears according to your browser settings. See your browser documentation for details.

4. Use the navigation dialog to locate the template file and upload it. The file must have a .xml extension.

5. The template is added to the list. The assigned Owner is your STA username, and the Visibility is set to Private.



Delete a Template

Use this procedure to delete a template from the STA application. The template is deleted for all STA usernames.

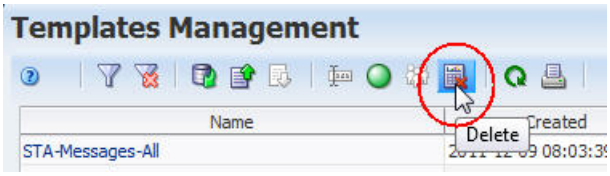
You can delete any custom template available to your STA username, even if you are not the owner. You can also delete STA predefined templates, except for the templates named "STA-Default."

Note: This procedure requires Operator or Administrator privileges.

Note: If you delete STA predefined templates, you can later restore them. See "Restore the STA Predefined Templates" on page 3-22 for details.

Note: If the deleted template was the screen default for any STA usernames, then the "STA-Default" template for that screen becomes their new default.

1. In the Navigation Bar, select **Setup & Administration**, then select **Templates Management**.
2. Select the template you want to delete.
3. Click **Delete** in the Templates Management toolbar.



The Delete Template confirmation dialog box appears.

Note: This dialog box does not appear if it has been turned off. See the *STA Screen Basics Guide* for details.

4. Click **Yes** to confirm the deletion.

The template is deleted and the Templates Management list is updated.

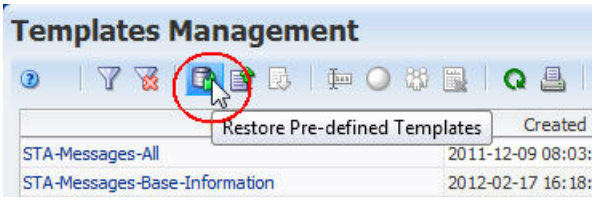
Restore the STA Predefined Templates

Use this procedure to restore the STA predefined templates after deleting them.

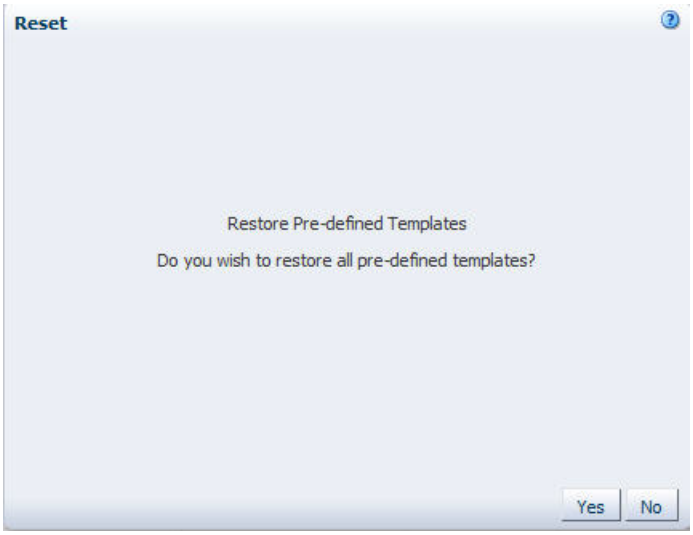
Note: This procedure requires Operator or Administrator privileges.

Note: This procedure does not affect custom templates you have created.

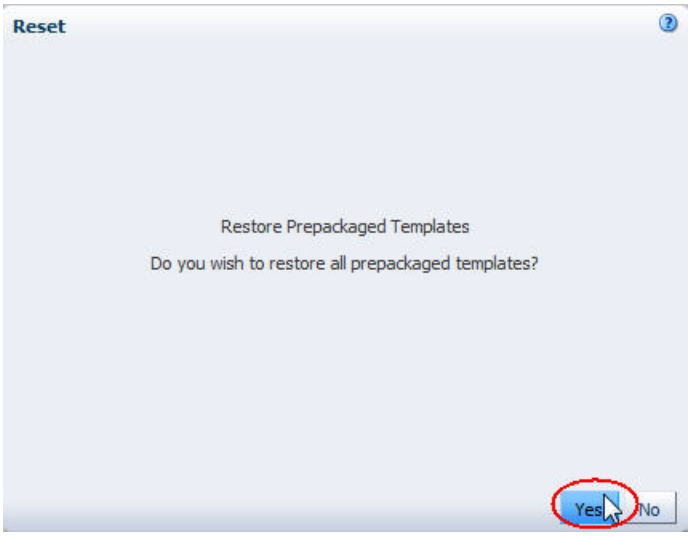
1. In the Navigation Bar, select **Setup & Administration**, then select **Templates Management**.
2. Select **Restore Predefined Templates** from the Templates Management toolbar.



The template Reset dialog box appears.



3. Click **Yes**.



The predefined templates are immediately restored to the STA application and available to all users. Any custom templates you have created are also still available. The Templates Management list is updated.

4

Filtering Data

STA enables you to filter the records displayed in pivot and list view tables. Filters allow you to focus on a subset of information by displaying just the records that meet specific criteria.

This chapter includes the following sections:

- About Filters
- Applying a Filter
- Filtering Tasks

About Filters

You can filter table data by any table attribute, whether or not that attribute is currently displayed on the table. You can specify filter criteria for any number of attributes, and you can choose whether any or all of the criteria must be met. See "Applying a Filter" on page 4-2 for complete details.

Once you apply a filter, the criteria are displayed in the Applied Filter area of the table. This allows you to verify which filter criteria have been applied to the current table view. If no criteria have been applied, this area is blank.

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

Filter Application

Some screens on the **Drives** and **Media** tabs are paired with one another. For these pairings, any filter applied on one screen is automatically applied to its partner. The screen pairings are as follows:

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

With the exception of these pairings, a filter applies only to the screen on which you apply it. Following are examples:

- If you apply a filter to the Drives – Overview screen, the same filter is automatically applied to the Drives – Analysis screen, but not to Drives – Cleaning Activities nor any other STA screen.

- If you apply a filter to the Libraries – Overview screen (a screen with no "partner"), the filter applies to that screen only.

Filter Duration

Once you have applied 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 to it later in the session, the filter will still be in effect. To change or remove a filter, you must take one of the following actions:

- Apply a new filter. See "Applying a Filter" on page 4-2 for details.
- Remove the filter. See "Clear the Current Filter" on page 4-12 for details.
- Apply a template; the filter criteria in a template overrides any existing criteria. See "Apply a Template" on page 3-8 for details.
- Log out of STA. See "Log Out of STA" on page 1-8 for details.

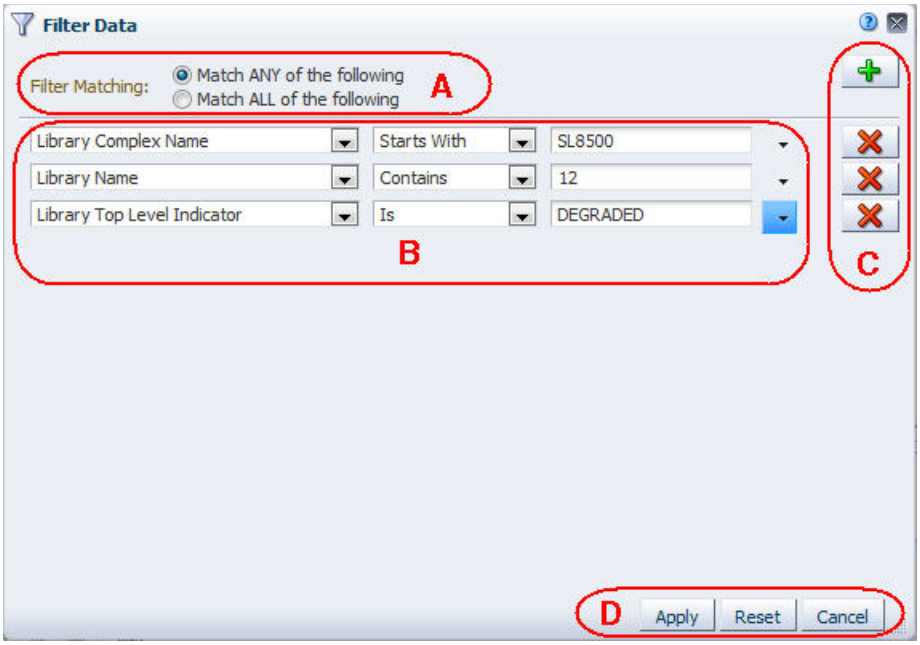
Applying a Filter

You can apply a filter in any of the following ways:

- By completing the Filter Data dialog box for a pivot or list view table. See "Filter Data Dialog Box" for details.
- By clicking an aggregate count link in a pivot table. See "Filtering Using Aggregate Count Links" on page 4-6 for details.
- By applying a template. See "Filtering by Applying a Template" on page 4-7 for details.
- By clicking a section of a bar chart or pie chart on the Dashboard. See "Filtering Using Dashboard Graphics" on page 4-8 for details.

Filter Data Dialog Box

The Filter Data dialog box appears when you click the **Filter Data** icon. A sample dialog box is shown below.



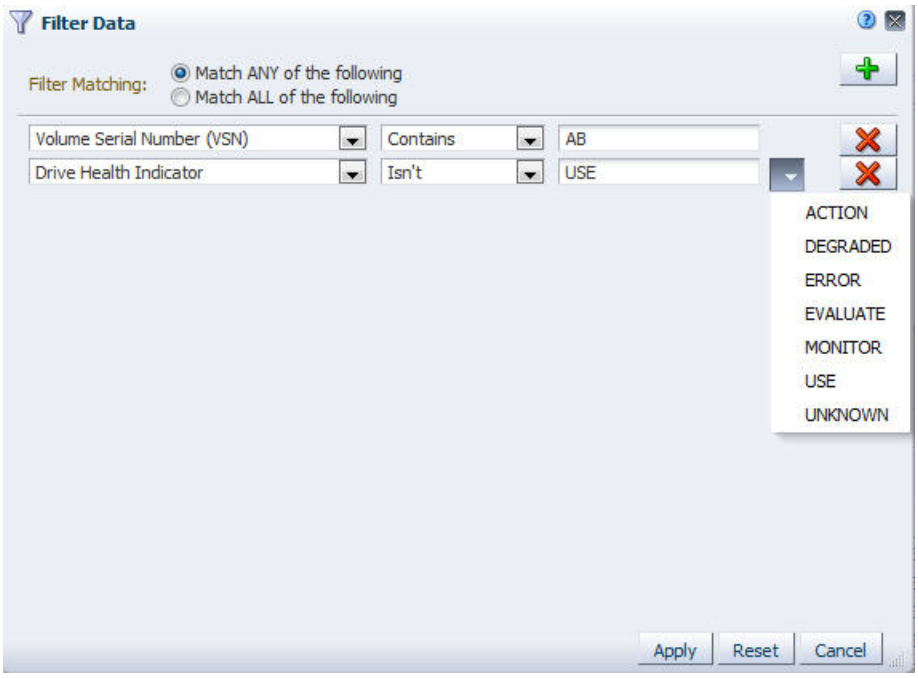
Item	Name	Description
A	Filter Matching field	Allows you to specify the type of match you want to perform. Select one of the following options: ■ **Match ANY of the following** – Selects table records that meet any of the criteria you specify. This is the default. ■ **Match ALL of the following** – Selects only records that meet all of the criteria you specify
B	Filter criteria rows	Each row specifies filter criteria to apply to the table. You can add as many rows as you want. On each row, you specify the criteria through the following menu selections: ■ Table attribute – All available attributes for the table are listed in the menu. **Note:** If you know the name of the attribute you want to select, you can type the first few letters to quickly move the cursor to that item in the menu. ■ Filter operators – Filter operators vary by attribute type. ■ Attribute value – Attribute values vary by attribute. See "Filter Operators by Attribute Type" on page 4-3 for descriptions of the filter operators and attribute values.
C	Filter criteria buttons	Buttons allow you to add new filter criteria rows or remove the associated row.
D	Buttons	Click one of the following buttons: ■ **Apply** – Applies the specified filter criteria to the table. See "Use the Filter Data Dialog Box to Change a Table Filter" on page 4-9 for details. ■ **Reset** – Removes all filter criteria so the table displays all records. See "Clear the Current Filter" on page 4-12 for details. ■ **Cancel** – Exits from the dialog box without applying any changes.

Filter Operators by Attribute Type

This section describes the operators used in creating selection criteria. 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.



- **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 an 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.

Text entries are not case-sensitive. For example, "ABC" matches "abc" or "Abc".

Some text attributes are free-form, in which case, you enter the string in the associated text entry field.

Other text attributes are predefined, in which case you select the value from a menu of possible values. The values listed do not necessarily reflect currently applied filters or the current removed drives and media display settings for your STA username. For example, the "Drive Health Indicator" drop-down menu may include health values that are not currently included in any monitored libraries

Logical group operators

When filtering by logical group, you can use the same operators as when filtering by other text attributes; however, because drives and media can be assigned to multiple logical groups, the "Is" and "Isn't" operators, which perform exclusive matches, may not produce expected results with logical groups. The "Contains" and "Doesn't Contain" operators are usually more appropriate when filtering by logical group.

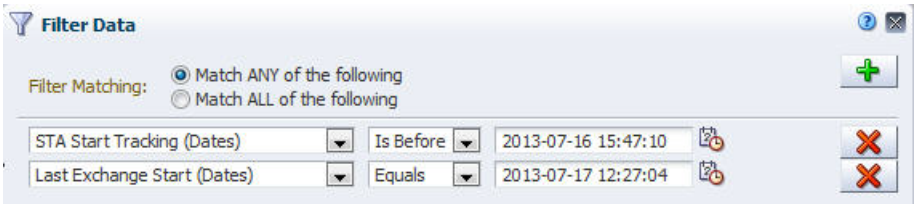
When used to filter by logical group, these operators produce the following results:

- **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 "Filtering by Logical Group" on page 7-4 for additional details.

Date and time stamp operators

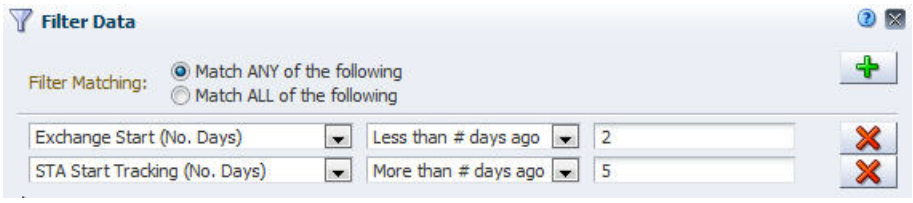
Examples of time stamp attributes include STA Start Tracking (Dates) and Last Exchange Start (Dates).



- **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

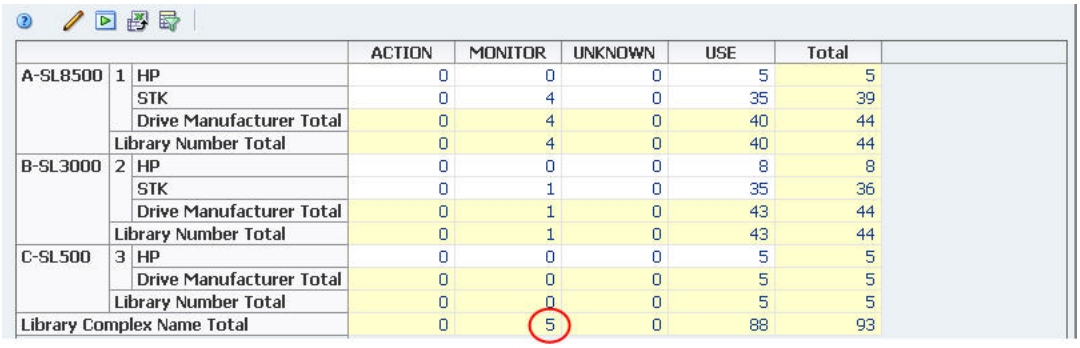
Examples of Boolean attributes include Cleaning Media and Exchange Write Inefficient

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

Filtering Using Aggregate Count Links

The cells within pivot tables contain aggregate counts of resources or events that meet specific criteria. A filter is therefore intrinsic to each aggregate count and is based on selection criteria represented by the pivot table edges. See the *STA Screen Basics Guide* for details on pivot table layers and filters.

For example, in the following Drives – Analysis pivot table, the "5" in the MONITOR column indicates that there are a total of five drives with a health status of "Monitor".

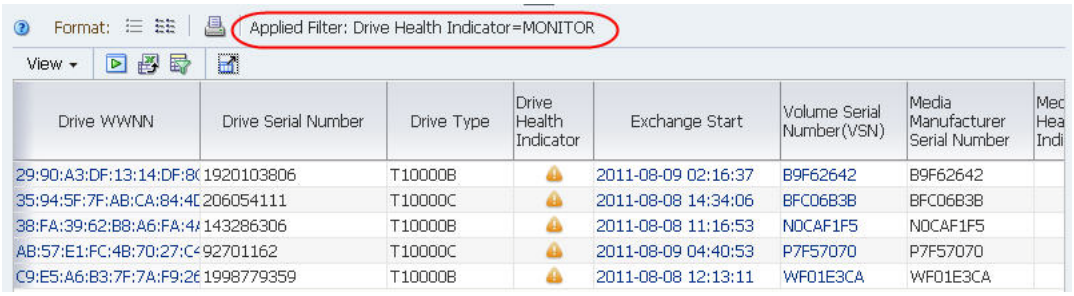


			ACTION	MONITOR	UNKNOWN	USE	Total
A-SL8500	1	HP	0	0	0	5	5
		STK	0	4	0	35	39
		Drive Manufacturer Total	0	4	0	40	44
		Library Number Total	0	4	0	40	44
B-SL3000	2	HP	0	0	0	8	8
		STK	0	1	0	35	36
		Drive Manufacturer Total	0	1	0	43	44
		Library Number Total	0	1	0	43	44
C-SL500	3	HP	0	0	0	5	5
		Drive Manufacturer Total	0	0	0	5	5
		Library Number Total	0	0	0	5	5
Library Complex Name Total			0	5	0	88	93

Clicking on this link takes you to the Drives – Overview screen and applies an appropriate filter based on the table edges The filter criteria are indicated in the Applied Filter area of the table.

Note: The filter based on the table edges overrides any filter already applied to the Analysis or Overview screens.

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



Drive WWNN	Drive Serial Number	Drive Type	Drive Health Indicator	Exchange Start	Volume Serial Number(VSN)	Media Manufacturer Serial Number	Mec Hea Indi
29:90:A3:DF:13:14:DF:8(	1920103806	T10000B	⚠	2011-08-09 02:16:37	B9F62642	B9F62642	
35:94:5F:7F:AB:CA:84:4(	206054111	T10000C	⚠	2011-08-08 14:34:06	BFC06B3B	BFC06B3B	
38:FA:39:62:B8:A6:FA:4/	143286306	T10000B	⚠	2011-08-08 11:16:53	N0CAF1F5	N0CAF1F5	
AB:57:E1:FC:4B:70:27:C4	92701162	T10000C	⚠	2011-08-09 04:40:53	P7F57070	P7F57070	
C9:E5:A6:B3:7F:7A:F9:2(	1998779359	T10000B	⚠	2011-08-08 12:13:11	WF01E3CA	WF01E3CA	

See "Use an Aggregate Count Link to Apply a Filter" on page 4-13 for detailed instructions.

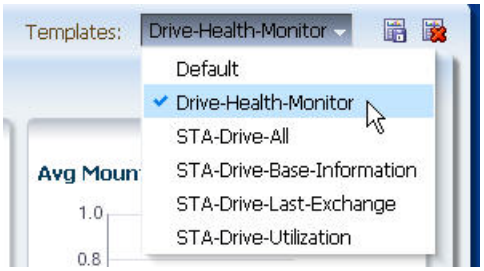
Filtering by Applying a Template

Applying a template automatically applies any filter criteria that are included in the template definition. These criteria override any filter that may already be in effect.

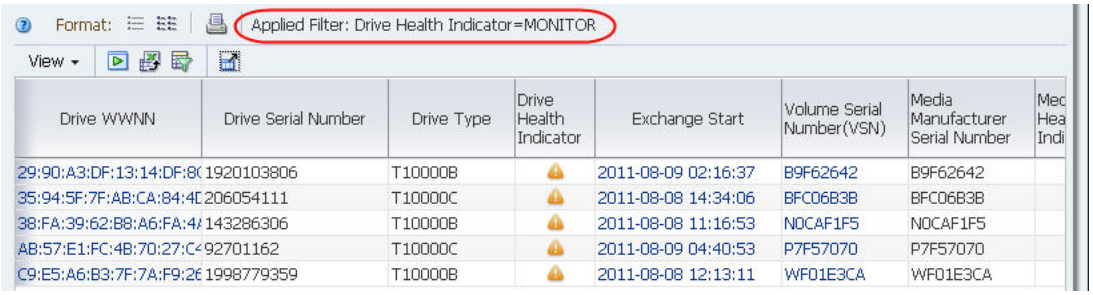
For example, the following Drives – Analysis pivot table has an applied filter, "Drive Health Indicator=USE".

Drive WWNN	Drive Serial Number	Drive Type	Drive Health Indicator	Exchange Start	Volume Serial Number(VSN)	Media Manufacturer Serial Number	M H I
0:9A:CD:F2:34:8E:61:B6	2118184903	T10000C	✓	2011-08-07 20:40:21	L47ED806	L47ED806	
12:F9:4A:4A:EA:FC:5:38	867332006	T10000B	✓	2011-08-09 03:43:19	F4956CA9	F4956CA9	
1F:23:4F:C5:FA:6F:A1:B2	1401403333	T10000B	✓	2011-08-08 17:07:11	P7F6D442	P7F6D442	
1F:FD:6C:2B:F3:98:7B:EC	1885765667	HP-LTO4	✓	2011-08-09 03:05:58	B6D032F3	B6D032F3	

Applying a template that includes a different filter, in this case "Drive Health Indicator=MONITOR", changes the table display and causes the original filter to be overridden.



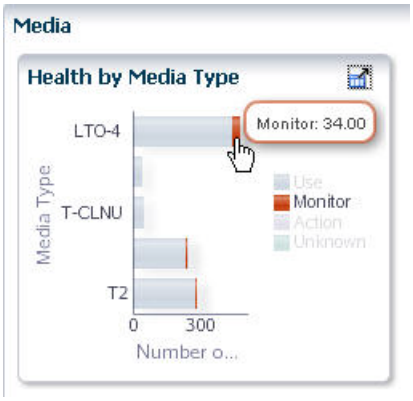
The new filter criteria are indicated in the Applied Filter area of the table.



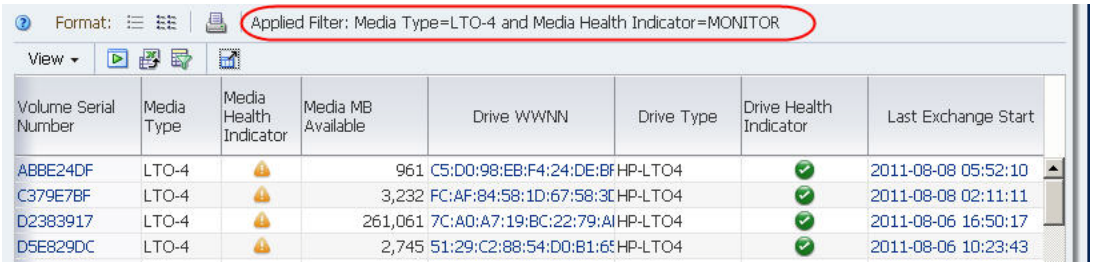
Filtering Using Dashboard Graphics

Bar, pie, and area charts on the Dashboard display aggregate data for resources or events that meet specific criteria. A filter is therefore intrinsic to each section of these Dashboard charts.

For example, in the following "Health by Media Type" graph, the selected section of the LTO-4 bar represents 34 drives with a health status of "Monitor".



Clicking this section of the bar takes you to the Media – Overview screen and applies the intrinsic filter. The filter criteria are indicated in the Applied Filter area of the table.



Filtering Tasks

- "Use the Filter Data Dialog Box to Change a Table Filter" on page 4-9
- "Clear the Current Filter" on page 4-12
- "Use an Aggregate Count Link to Apply a Filter" on page 4-13
- "Apply a Filter From the Dashboard" on page 4-16

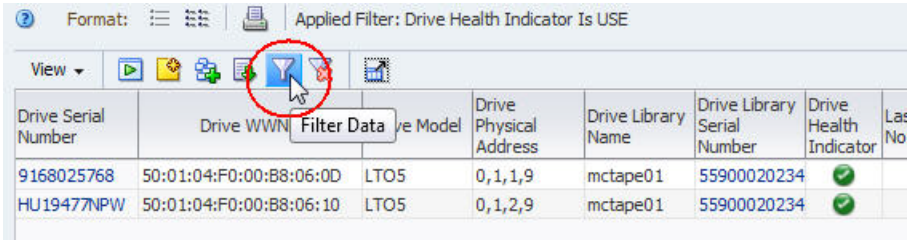
Use the Filter Data Dialog Box to Change a Table Filter

> **Note:** This procedure applies to both pivot and list view tables.

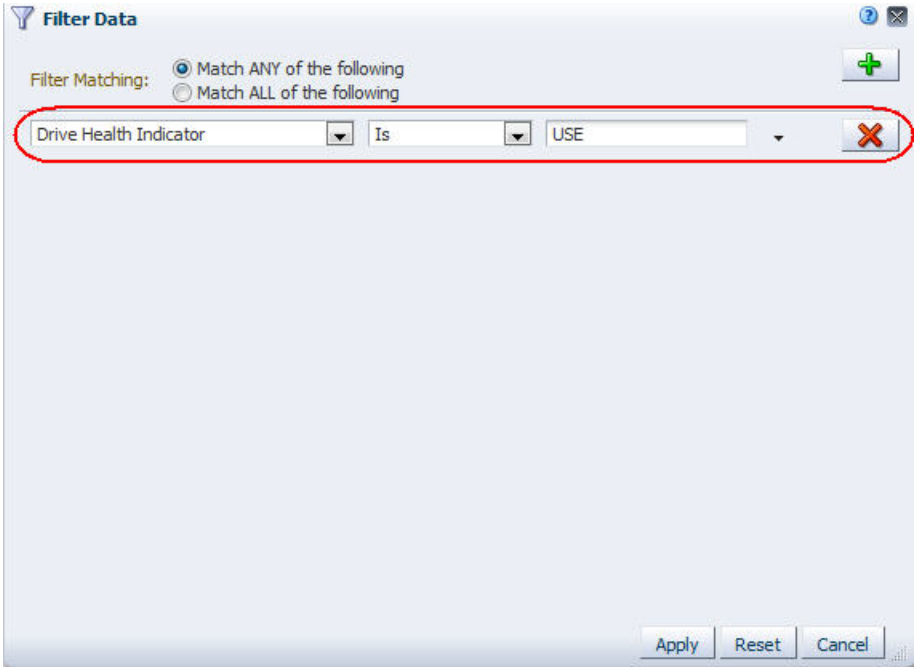
Use this procedure to apply new filter criteria to the current table. You can filter by one or more record attributes, and you can remove selected filter criteria.

For screens that are paired with a "partner", the filter applied to one screen is automatically applied to its partner. See "Filter Application" on page 4-1 for details.

1. Click **Filter Data** in the Table Toolbar.



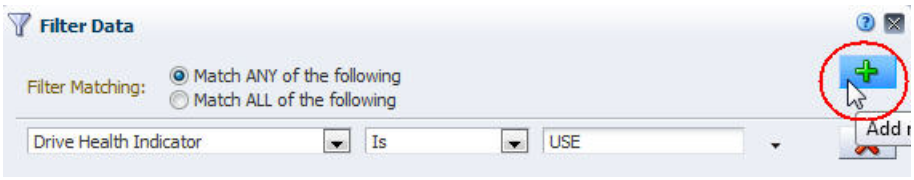
The Filter Data dialog box appears. If a filter has already been applied, the criteria are displayed in the dialog box, as in the example below.



2. Specify the filter criteria in the dialog box, as follows:

   a. In the **Filter Matching** field, select one of the options to indicate whether you want to match any or all of the criteria you specify. See "Filter Matching field" on page 4-3 for details.

   b. Click **Add New Filter Criteria** to add a new, blank filter criteria row to the dialog box.



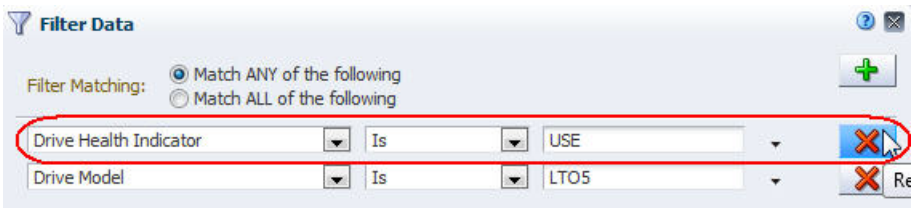
   c. Specify the filter criteria using the menus and text field on the row. See "Filter Operators by Attribute Type" on page 4-3 for details on filling out each row.

Note: When selecting an attribute for filtering, if you know the name of the attribute you want to select, you can type the first few letters to quickly move the cursor to that item in the menu.

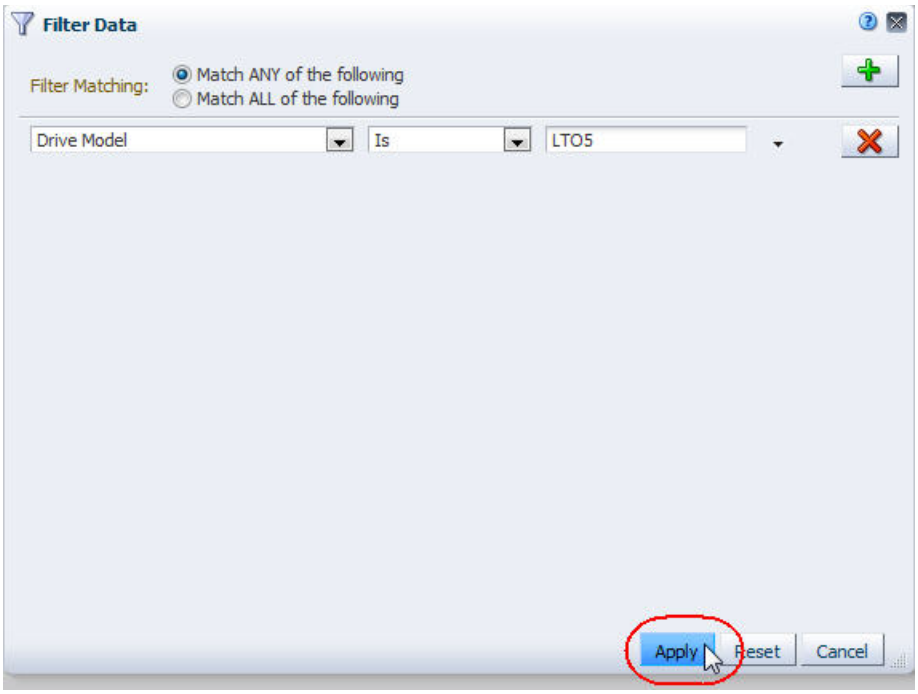
---

   d. You can add as many rows of filter criteria as you want.

   e. To remove filter criteria, click **Remove This Filter Criteria Row** for the associated row.

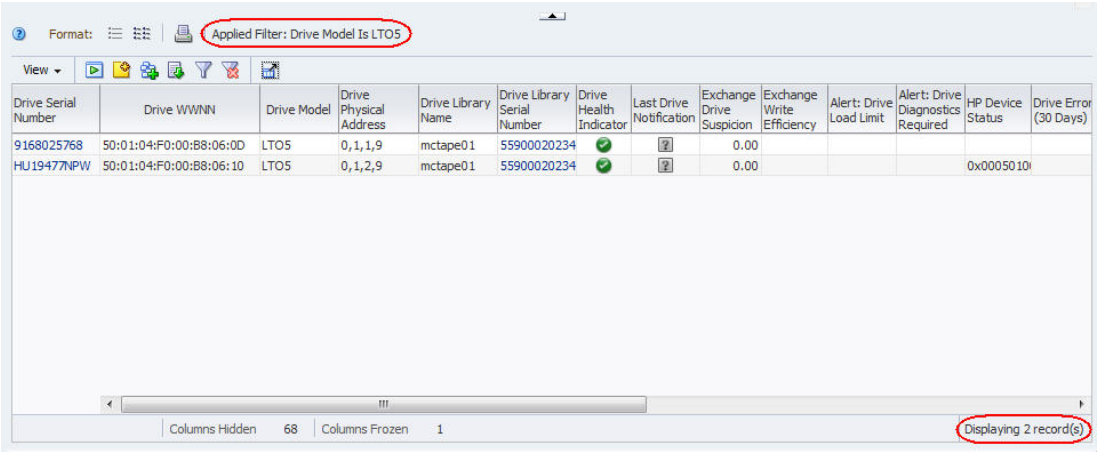


3. Verify that your specifications are correct, and then click **Apply**.

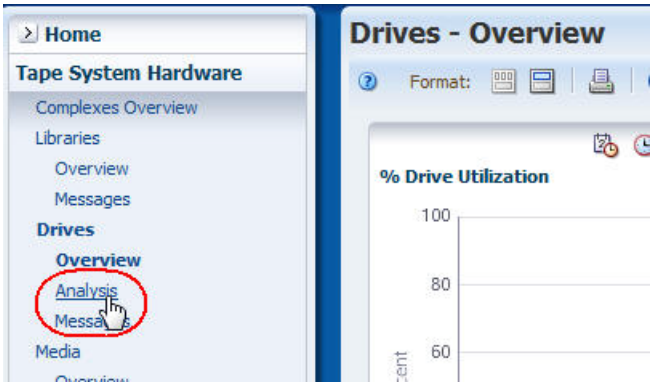


The following updates are made to the table:

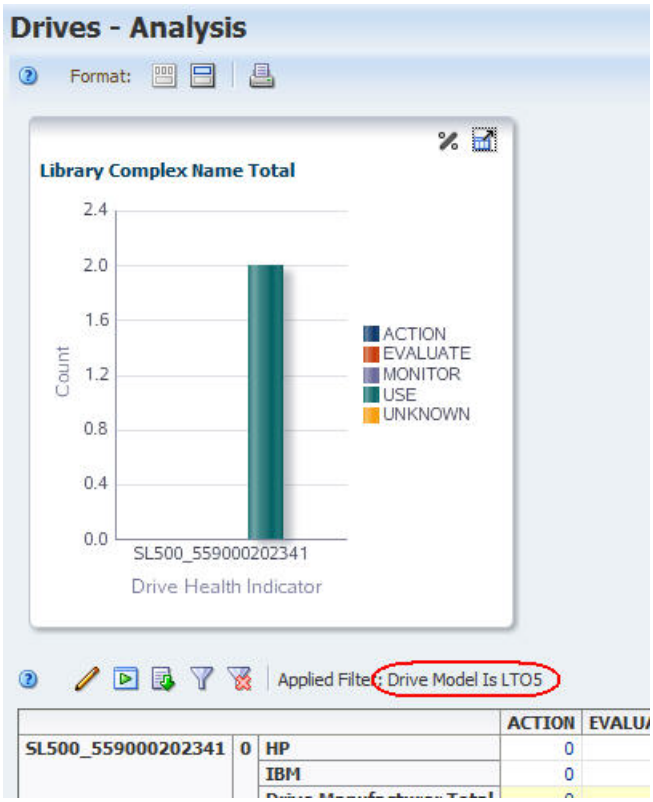
- The table displays only the records that match the criteria you have specified.
- The Applied Filter area indicates the specified criteria.
- For list view tables, the Table Status Line indicates the number of records.



4. If the screen is one of a Drives, Media, or All Messages screen pairing, the filter criteria are also applied to its partner. You can navigate to the partner screen to verify this.



The Applied Filter area of the tables on both screens indicate the same filter.



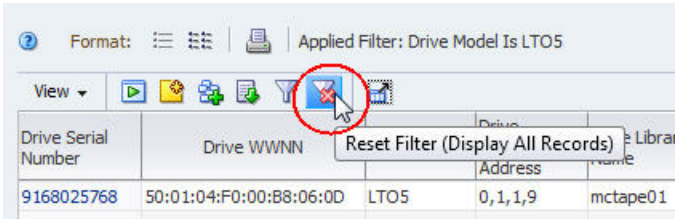
Clear the Current Filter

Note: This procedure applies to both pivot and list view tables.

Use this procedure to remove all filter criteria from a table.

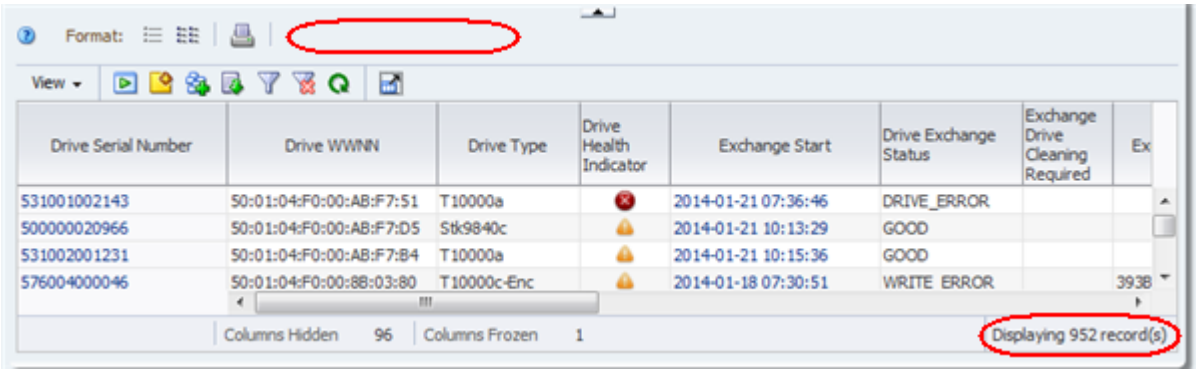
Note: To remove selected filter criteria from a table, see "Use the Filter Data Dialog Box to Change a Table Filter" on page 4-9.

1. Click **Reset Filter** in the Table Toolbar.



The following updates are made to the table:

- All filter criteria are removed from the table so it displays all available records.
- The Applied Filter area is blank, indicating no filter criteria are currently applied.
- For list view tables, the Table Status Line indicates the number of records displayed.



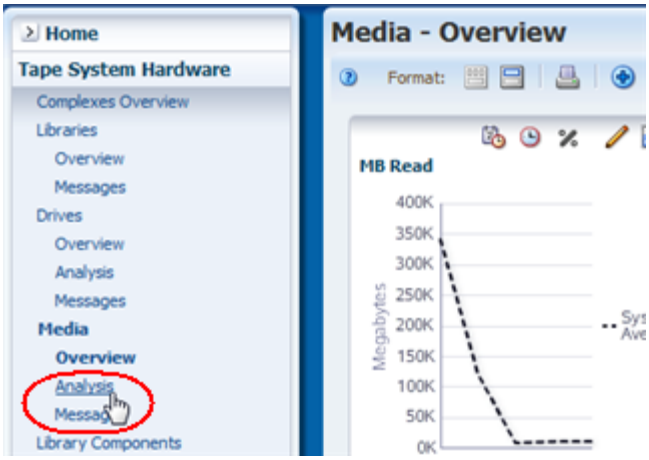
Use an Aggregate Count Link to Apply a Filter

Use this procedure to apply a filter to an Overview screen by clicking an aggregate count link in the "partner" Analysis screen pivot table. The resulting display shows detail for the aggregate count.

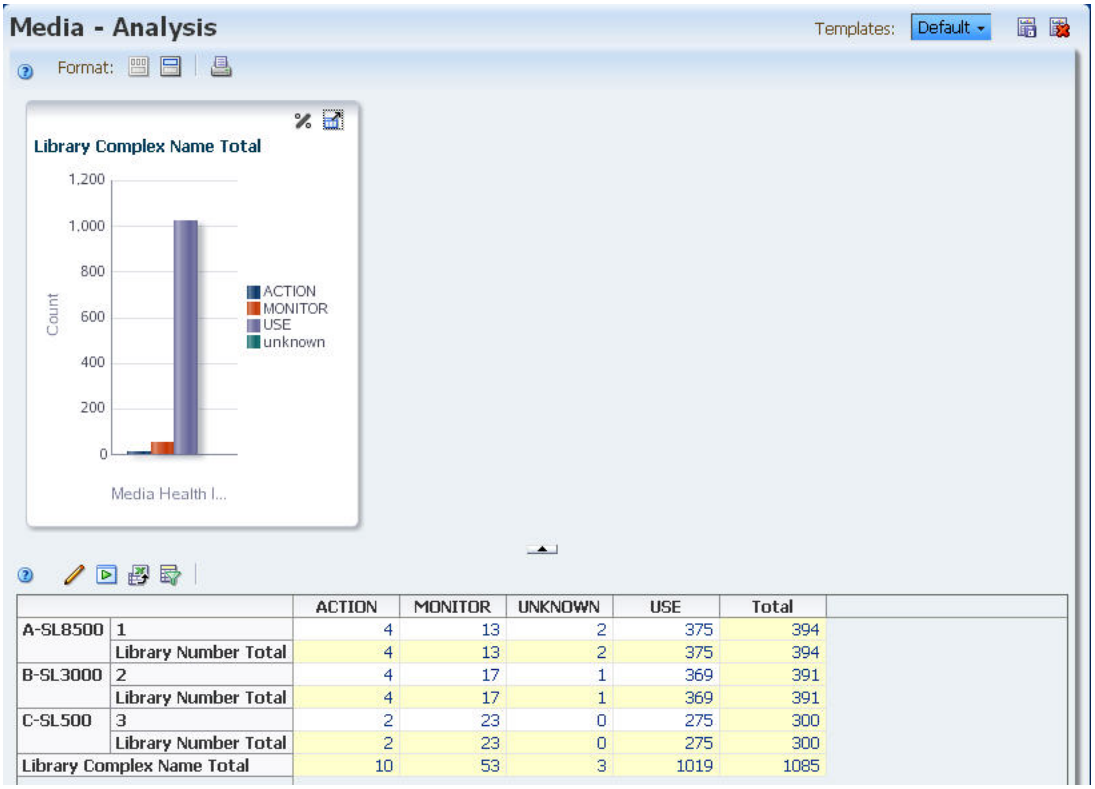
The aggregate counts in each table cell are the result of the filter criteria intrinsic to each table layer, joined by "AND" statements. Clicking an aggregate count link in a pivot table cell applies the associated filter criteria to the Overview screen.

Note: The filter applied with this method overrides any filter already applied to the Overview screen.

1. Use the Navigation Bar to bring up an Analysis screen.

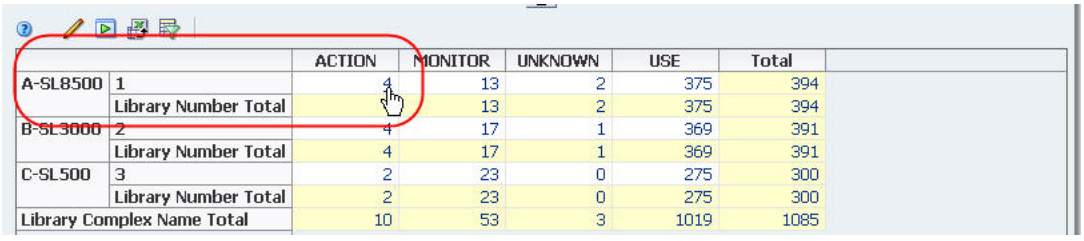


The Media – Analysis screen is used in this example.



		ACTION	MONITOR	UNKNOWN	USE	Total
A-SL8500	1	4	13	2	375	394
	Library Number Total	4	13	2	375	394
B-SL3000	2	4	17	1	369	391
	Library Number Total	4	17	1	369	391
C-SL500	3	2	23	0	275	300
	Library Number Total	2	23	0	275	300
Library Complex Name Total		10	53	3	1019	1085

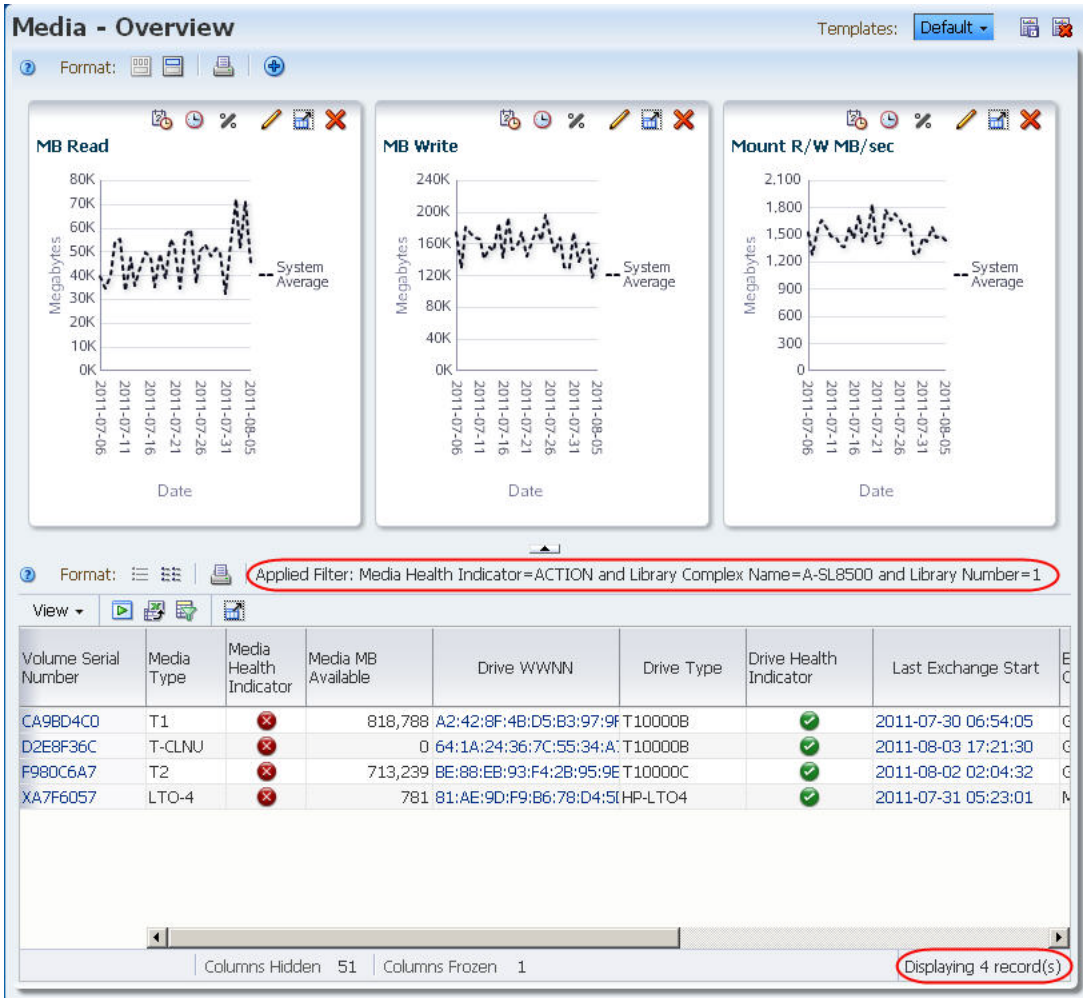
2. In the pivot table, click an aggregate count link.



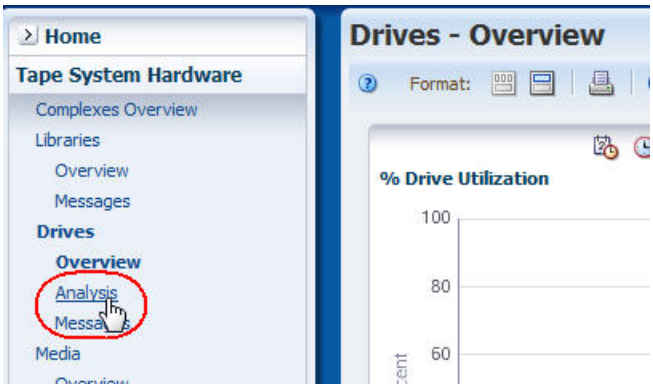
		ACTION	MONITOR	UNKNOWN	USE	Total
A-SL8500	1	4	13	2	375	394
	Library Number Total	4	13	2	375	394
B-SL3000	2	4	17	1	369	391
	Library Number Total	4	17	1	369	391
C-SL500	3	2	23	0	275	300
	Library Number Total	2	23	0	275	300
Library Complex Name Total		10	53	3	1019	1085

You are taken to the "partner" Overview screen (Media – Overview in this example), and the following updates are made to the list view table:

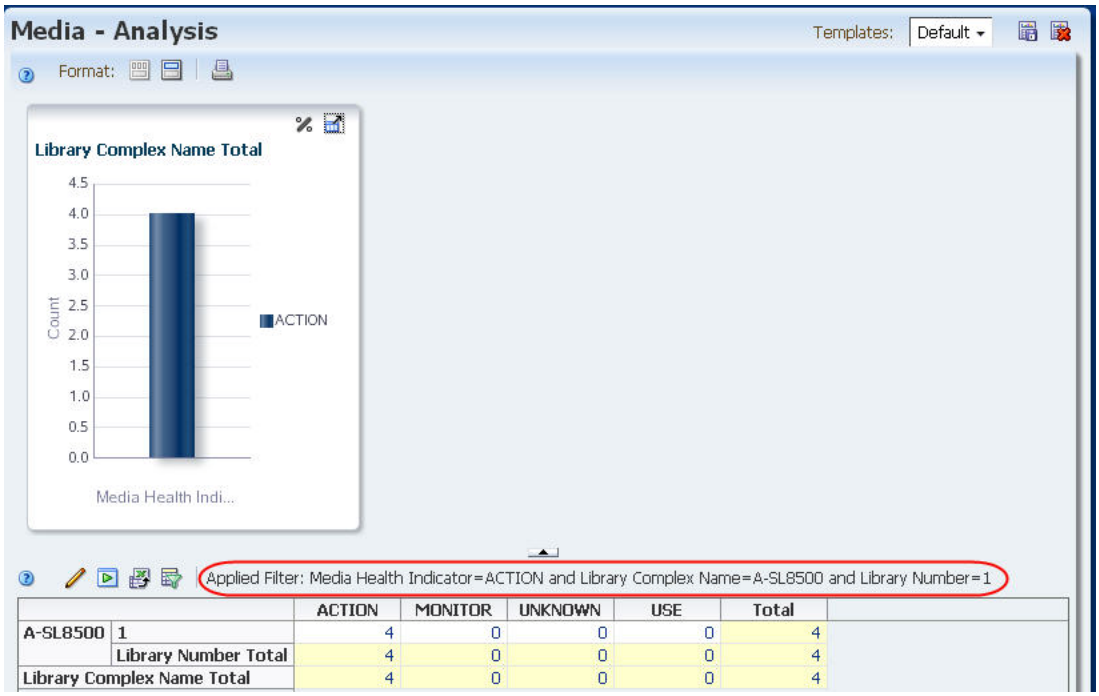
- The table displays only the records included in the pivot table aggregate count.
- The Applied Filter area indicates the filter criteria from the aggregate count.
- The Table status line indicates the number of records displayed; this number is the same as the aggregate count in the pivot table.



3. Use the Navigation Bar to return to the Analysis screen.



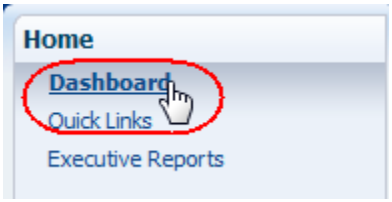
The filter remains active; therefore, the Analysis screen displays only the records that meet the selection criteria intrinsic to the original aggregate count link.



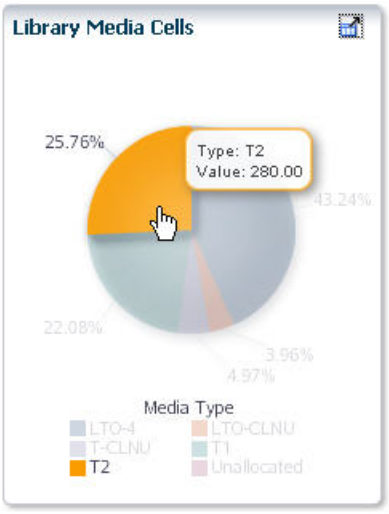
Apply a Filter From the Dashboard

Use this procedure to apply a filter by clicking a section of a bar or pie chart on the Dashboard. You are taken to the corresponding Overview screen, and the filter intrinsic to the bar or pie chart section is applied. This procedure allows you to display detail about data displayed on the Dashboard.

1. Use the Navigation Bar to go to the Dashboard.

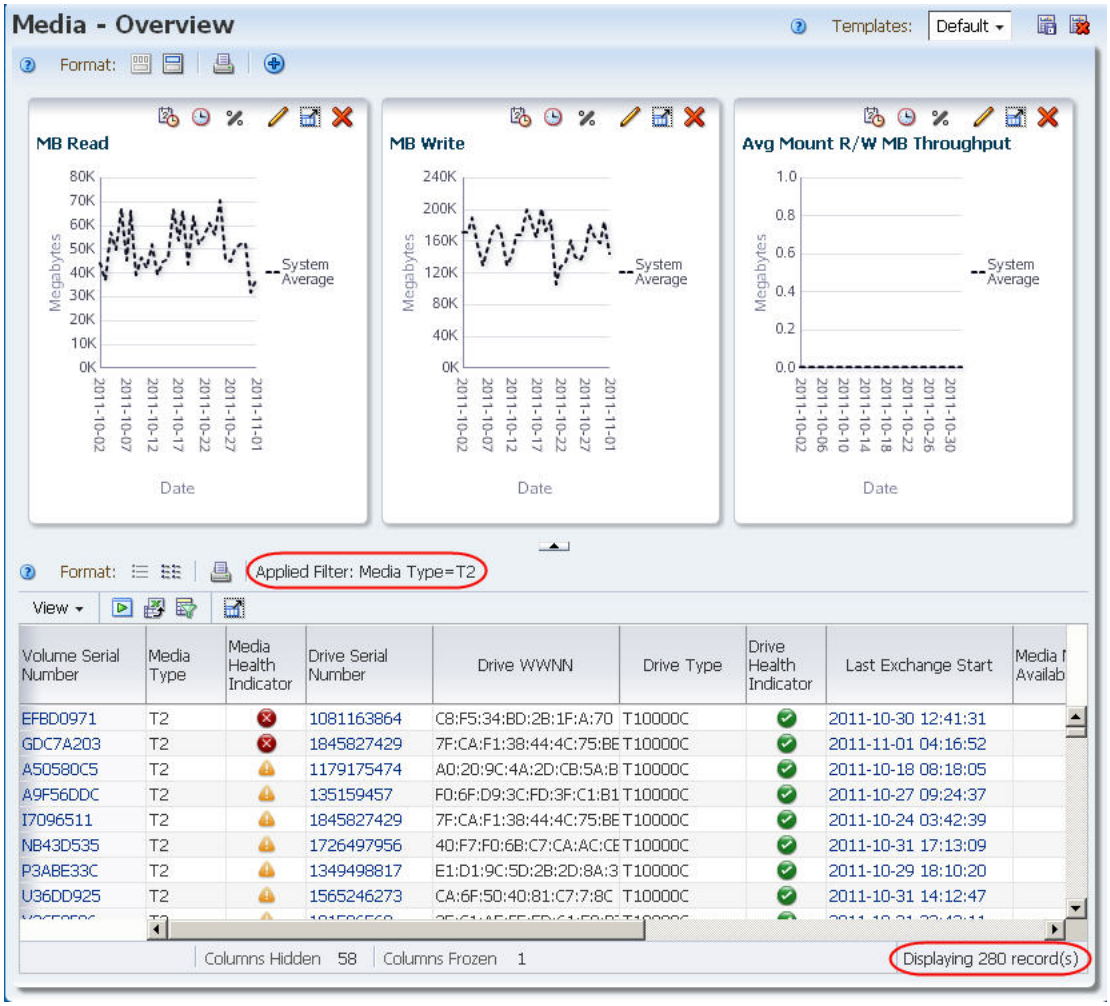


2. Click a section in a Dashboard bar or pie chart.



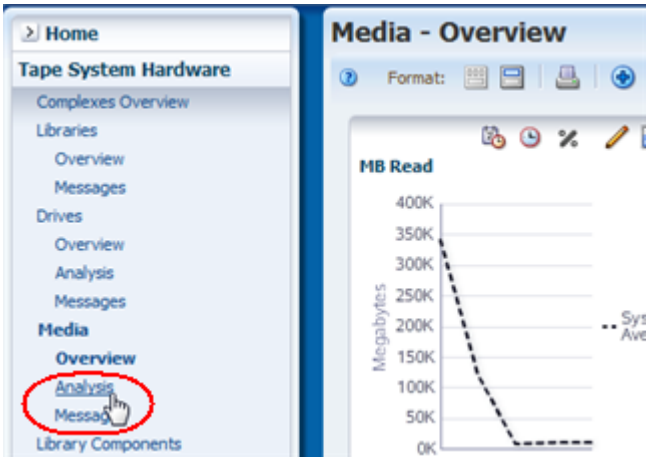
You are taken to the corresponding Overview screen (Media – Overview in this example), and the following updates are made to the list view table:

- The table displays only the records included in the selected Dashboard section.
- The Applied Filter area indicates the filter criteria from the selected section.
- The Table status line indicates the number of records displayed; this number is the same as the Value for the selected Dashboard section.

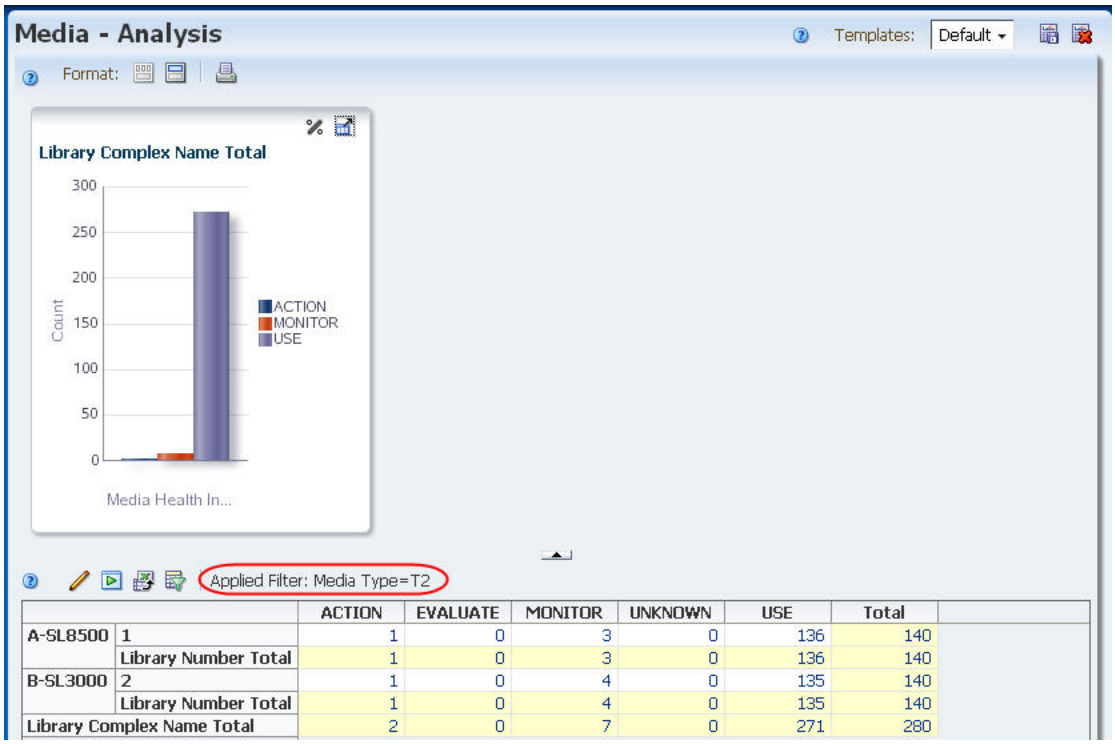


3. Use the Navigation Bar to select the "partner" Analysis screen, if applicable.

Note: This step applies to Drive, Media, and All Messages screens only.



The filter remains active; therefore, the Analysis screen displays only the records that meet the selection criteria intrinsic to the selected bar or pie chart section.



		ACTION	EVALUATE	MONITOR	UNKNOWN	USE	Total
A-SL8500	1	1	0	3	0	136	140
	Library Number Total	1	0	3	0	136	140
B-SL3000	2	1	0	4	0	135	140
	Library Number Total	1	0	4	0	135	140
Library Complex Name Total		2	0	7	0	271	280

5

STA Alerts

The STA alerts feature notifies you of events and conditions in your tape library system based on user-defined alert policies. You can create as many alert policies as you want. The alert policies identify the types of conditions and events to which you want to be alerted and the frequency at which alerts may be generated. Optionally, you can indicate that you want alerts sent to specified email addresses.

This chapter includes the following sections:

- How Alerts Work
- User Roles for Alerts Management
- Details on Defining Alert Policies
- Best Practices for Alert Policies
- Alert Emails
- Alerts Workflow
- Alert Management Tasks

How Alerts Work

The STA alerts process consists of the following parts:

- "Defining Alert Policies" on page 5-1
- "Alert Generation" on page 5-2
- "Monitoring Generated Alerts" on page 5-2

Defining Alert Policies

Users with Administrator privileges perform this part of the process from the Alerts Policies screen on the **Setup & Administration** tab.

When you create an alert policy, you can enable it immediately or leave it disabled for the time being. In addition, several sample alert policies are delivered with STA, and they are disabled by default (see "STA Sample Alert Policies" on page 5-8 for details). Only enabled alert policies are used to generate alerts.

To define an alert policy you specify the following information:

- Policy name – An alphanumeric identifier for the policy. Policy names must be unique.
- Policy description – Optional description of the policy.

- *Entity* type – Entities are tape library system resources or events. You must designate the types of entities to be evaluated by the alert policy. Options include libraries, drives, media, exchanges, and media validations. See "Alert Policy Entities" on page 5-3 for a complete list.
- Severity – Determines the frequency with which alerts may be generated whenever the criteria defined by this policy are met. See "Alert Policy Severities" on page 5-4 for details.
- Alert criteria – User-defined criteria by which the appropriate library system resources are evaluated. Alert criteria work in much same way as the STA filtering feature. See "Filter Data Dialog Box" on page 4-2 for details.
- Email recipients – Optional list of email addresses to receive emails whenever an alert is generated by the policy. See "Alert Emails" on page 5-10 for details.

Alert Generation

This part of the process is done automatically by STA.

STA continuously evaluates enabled alert policies in the background. Specifically, alert policies are evaluated whenever the following types of activities occur:

- An enabled alert policy is created or modified in any way.
- A drive/media exchange occurs.
- A media validation exchange occurs.
- An SNMP trap is received from a monitored library.
- A library data collection occurs.
- An STA application or server event occurs.

STA generates alerts based on the alert policy criteria and severity. If the policy criteria are matched and enough time has passed since the last alert for the same library resource and event, a new alert is generated. The time period is determined by the policy severity. See "Alert Policy Severities" on page 5-4 for details:

If the alert policy includes email addresses, an email containing details about the alert is sent to the designated addresses. See "Alert Emails" on page 5-10 for details.

For additional details about the alert policy evaluation process, see "Alert Policy Severity Examples" on page 5-4.

Monitoring Generated Alerts

Any STA user can perform this part of the process 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 "Alerts Workflow" on page 5-11 for details.

User Roles for Alerts Management

Table 5–1 summarizes the alert policy definition activities available to each STA user role.

Table 5–1 Alert Policy User Roles

User Role	Alert Policy Activity	Screen
Operator and above	Display, filter, and print a list of defined alert policies.	Select **Setup & Administration**, then select **Alerts Policies**.
Administrator only	Define an alert policy. Copy an alert policy. Rename a policy. Change the policy criteria. Change the list of email recipients. Enable or disable an alert policy. Delete an alert policy.	Select **Setup & Administration**, then select **Alerts Policies**.

Table 5–2 summarizes the alert monitoring activities available to each STA user role.

Table 5–2 Alert Monitoring User Roles

User Role	Alert Monitoring Activity	Screen
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.	Select **Tape System Activity**, then select **Alerts Overview**.
Operator and above	Annotate an alert.	Select **Tape System Activity**, then select **Alerts Overview**.

Details on Defining Alert Policies

This section provides additional detail to help you in creating alert policies. The following information is included:

- "Alert Policy Entities" on page 5-3
- "Alert Policy Severities" on page 5-4
- "Best Practices for Alert Policies" on page 5-9
- "STA Sample Alert Policies" on page 5-8

Alert Policy Entities

You can define alert policies for the following types of *entities*, or tape library system resources and events:

- Library complex
- Library
- Drive

- Media
- Robot
- CAP
- PTP – Relevant only to SL8500 libraries.
- Elevator – Relevant only to SL8500 libraries.
- Exchange – See "Alert Policy Severities" on page 5-4 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. See "STA Media Validation" on page 8-1 for details.
- STA application itself – To be notified whenever the STA application restarts.

Alert Policy Severities

The policy severity determines the frequency with which alerts may be generated from the policy. The severity levels are as follows:

- 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 Severity Examples" on page 5-4 for examples detailing the effects of the assigned severity levels.

Exchange and Media Validation Activities Alert Policies and Severities

Because exchanges and media validations are discrete events, not persistent resources, exchange and media validation alert policies 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 Example 5 and Example 6 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 "Avoiding too many alerts" on page 5-9 for details.

Alert Policy Severity Examples

The following examples illustrate how and when alerts are generated 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.

- Example 1, ""Warning" Policy for Drives"
- Example 2, ""Informative" Policy for Drives"
- Example 3, ""Severe" Policy for Media"
- Example 4, ""Severe" Policy for CAPs"
- Example 5, "Policy for Exchanges Using "Media Health Indicator""
- Example 6, ""Warning" Policy for Media Using "Media Health Indicator""

Example 1 "Warning" Policy for Drives

This 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.

Example 2 "Informative" Policy for Drives

This example presents the same policy criteria as Example 1 but with an "Informative" severity.

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

Policy entity: Drives

Policy severity: Informative – alerts are generated only once.

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.

Example 3 "Severe" Policy for Media

This 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.
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.

Example 4 "Severe" Policy for CAPs

This 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.
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.

Example 5 Policy for Exchanges Using "Media Health Indicator"

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. This example illustrates this point. See Example 6 for a similar example that results in fewer alerts.

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.

Time	Events	Evaluation	Result
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.

Example 6 "Warning" Policy for Media Using "Media Health Indicator"

This policy generates alerts for media with EVALUATE health. This example is similar to Example 5, 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 is 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.

Alert Policy Criteria

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.

STA Sample Alert Policies

Some sample alert policies are delivered with STA. These policies are meant to give you concrete examples for policy creation, and they are all disabled by default. You can enable as many of them as you want and use them as is, or you can use them as starting points for creating policies more specific to your needs.

Caution: 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 "Copy an Alert Policy" on page 5-18 for details.

It is also recommended that you print a record of the sample policies as delivered, so you can re-create them manually if necessary. See "Manage the List of Alert Policies" on page 5-12 for details.

All STA sample alert policies have names with an "STA" prefix. It is recommended that you preserve this naming convention for the sample policies and not use the "STA" prefix when naming your own alert policies. The Date Created/Updated for STA sample alert policies is the date when the STA application was last installed.

Best Practices for Alert Policies

This section includes tips for creating and managing alert policies.

Create custom alert policies

Create custom alert policies to address site-specific concerns. This is a parallel practice to creating custom templates.

See "Alert Management Tasks" on page 5-11.

Customizing the sample alert policies

When customizing the sample alert policies provided with STA, make copies rather than modifying the samples directly. Keep the sample policies even if you don't use them. Also, do not use the "STA" prefix when naming your customized versions.

See the following sections:

- "STA Sample Alert Policies" on page 5-8
- "Copy an Alert Policy" on page 5-18

Avoiding too many alerts

Oracle recommends defining alert policies using criteria specific to the policy entity type. And for exchange and media validation alert policies, Oracle recommends using 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

Alert policies and the "Contains" operator

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 "Filtering by Logical Group" on page 7-4.

Duplicate volser alerts

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

See "Duplicate Volume Serial Numbers" on page 12-10.

Alert Emails

Alerts can be sent to any number of email addresses. Through emailed alerts, users are notified of significant events in the tape library system without having to log in to the STA application. Alerts can even be sent to employees who do not have STA usernames.

The available email addresses must have been previously defined to STA on the Configuration – Email screen. See "Add an Available Email Recipient" on page 9-10 for instructions.

Example 5–1 and Example 5–2 are examples of the text of alert emails you might receive.

Example 5–1 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 5–2 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
```

Alerts Workflow

The alerts workflow is an optional manual process that is based on predefined states you can assign to selected alerts on the Alerts Overview screen. You can implement the alerts workflow in whatever manner best works for your site, but a suggested progression of alert states is as follows:

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" on page 5-28 for details.

See "Change the State of an Alert" on page 5-27 for details on using alert states to implement a manual workflow.

Alert Management Tasks

Alert Policy Definition Tasks

- "Manage the List of Alert Policies" on page 5-12
- "Create an Alert Policy" on page 5-12
- "Copy an Alert Policy" on page 5-18
- "Modify an Alert Policy" on page 5-19
- "Modify Email Recipients for an Alert Policy" on page 5-21
- "Enable or Disable an Alert Policy" on page 5-22
- "Delete an Alert Policy" on page 5-23

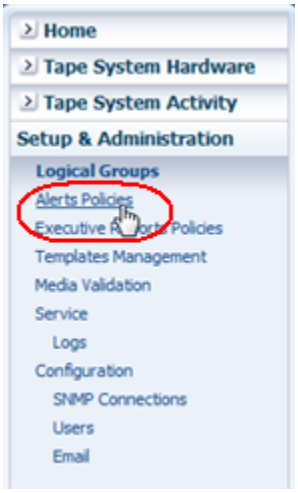
Alert Monitoring Tasks

- "Manage the List of Generated Alerts" on page 5-25
- "Display Detail For an Alert" on page 5-25
- "Show or Hide Dismissed Alerts" on page 5-28
- "Change the State of an Alert" on page 5-27

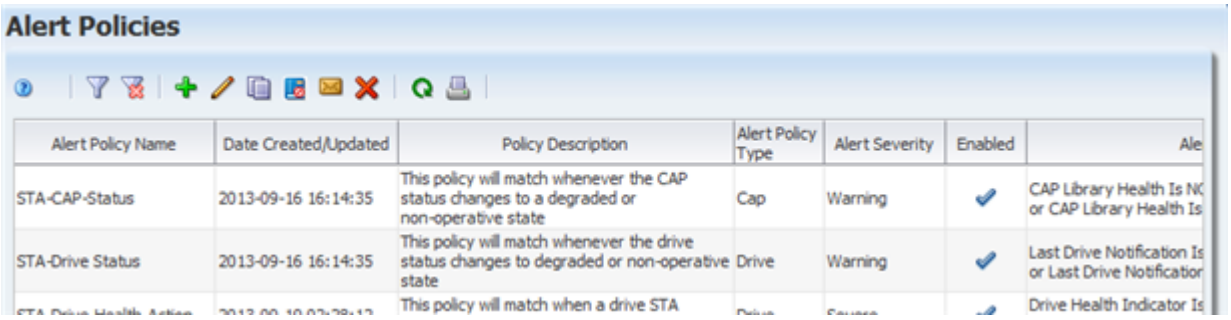
Manage the List of Alert Policies

Note: This procedure requires Operator or Administrator privileges.

1. In the Navigation Bar, select **Setup & Administration**, then select **Alerts Policies**.



The Alerts Policies screen appears, showing all sample and user-defined policies at your site.



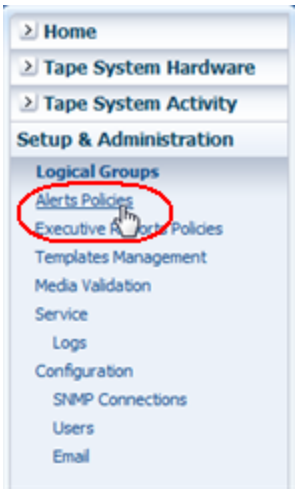
2. You can manage the list of alert policies by performing the following tasks:
   - Filter the table records; see "Use the Filter Data Dialog Box to Change a Table Filter" on page 4-9.
   - Reset a filter applied to the table; see "Clear the Current Filter" on page 4-12.
   - Refresh the table to display new policies; see the *STA Screen Basics Guide*.
   - Display a printable form of the table in a separate browser tab or window; see the *STA Screen Basics Guide*.

Create an Alert Policy

Use this procedure to create an alert policy. The Alert Policies wizard leads you through the steps to define all information for the policy.

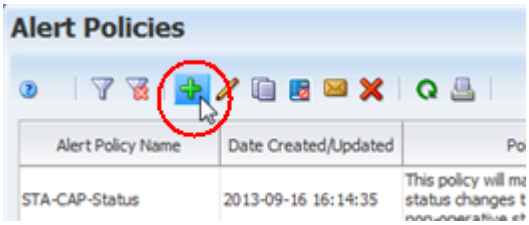
Note: This procedure requires Administrator privileges.

1. In the Navigation Bar, select **Setup & Administration**, then select **Alerts Policies**.



The Alerts Policies screen appears.

2. Click **New Alert Policy**.



The Alert Policies wizard appears.

3. Complete the first screen of the wizard as follows:

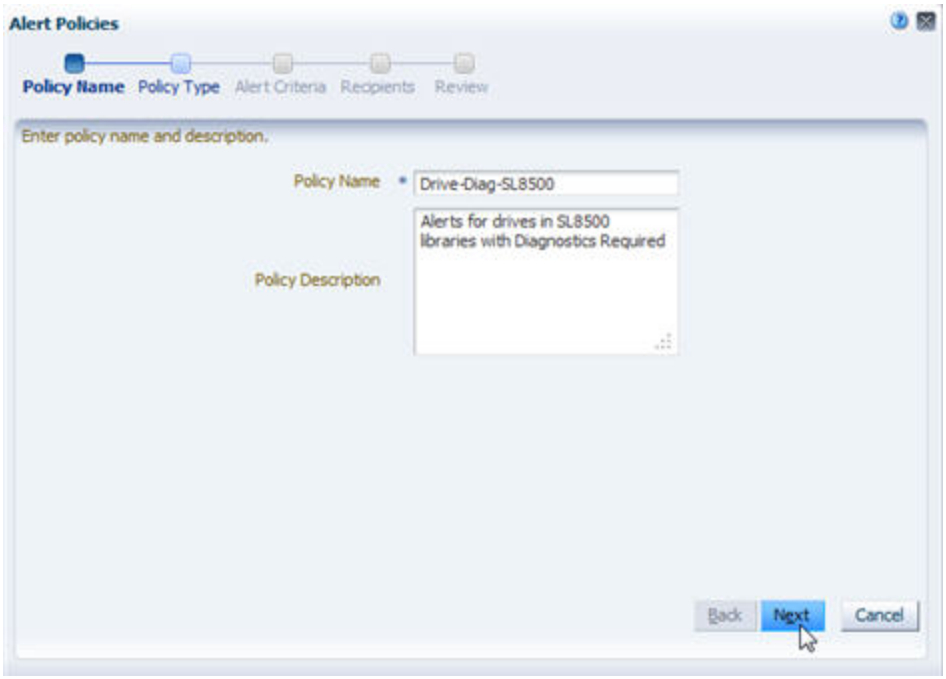
   a. In the **Policy Name** field, type a unique name.

      Your entry can include any alphanumeric characters up to 250 characters in length.

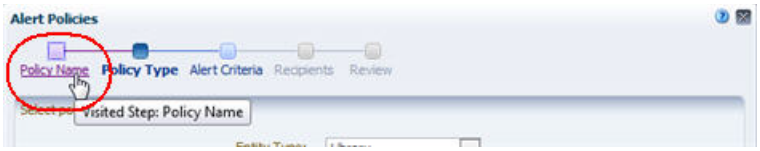
      Note: All sample alert policies delivered with STA have names beginning with "STA," so it is recommended that the names you assign to your alert policies not start with this prefix.

   b. In the **Policy Description** field, enter an optional description of the policy. 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.

   c. Click **Next**.



Note: On any screen of the wizard, you can select the breadcrumb links at the top of the dialog box to go directly to the next immediate screen or any screen you have already visited.

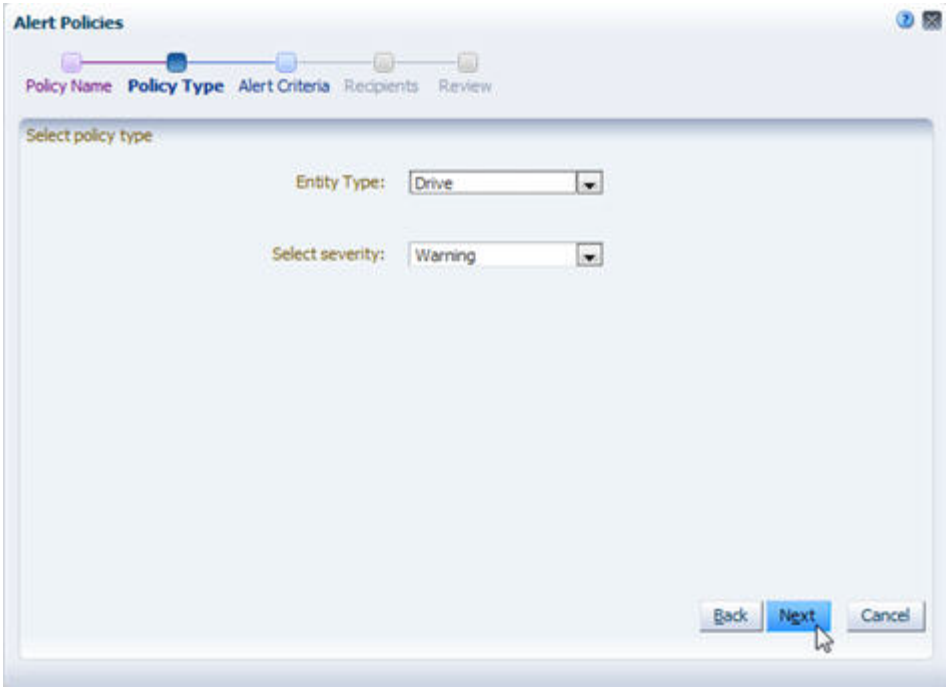


4. Complete the second screen of the wizard as follows:

   a. In the **Entity Type** menu, select the type of library system component for which this policy may generate alerts. See "Alert Policy Entities" on page 5-3 for information about the types.

   b. In the **Select Severity** field, select the severity level of the alert policy. See "Alert Policy Severities" on page 5-4 for information about severity levels.

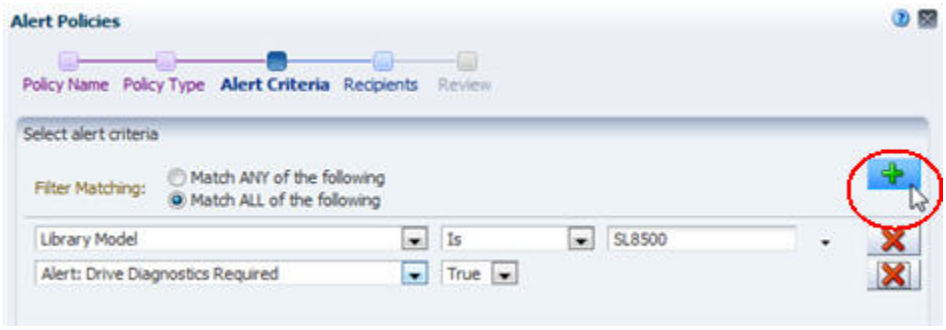
   c. Click **Next**.



5. On the third screen of the wizard, specify the alert policy criteria as follows:

   a. In the **Filter Matching** field, indicate whether you want to match any or all of the criteria you specify.

   b. Click the **Add New Filter Criteria Row** button to add a new, blank selection criteria row to the dialog box.



   c. Specify the selection criteria using the menus and text fields on the row. See "Filter Operators by Attribute Type" on page 4-3 for details on completing each row.

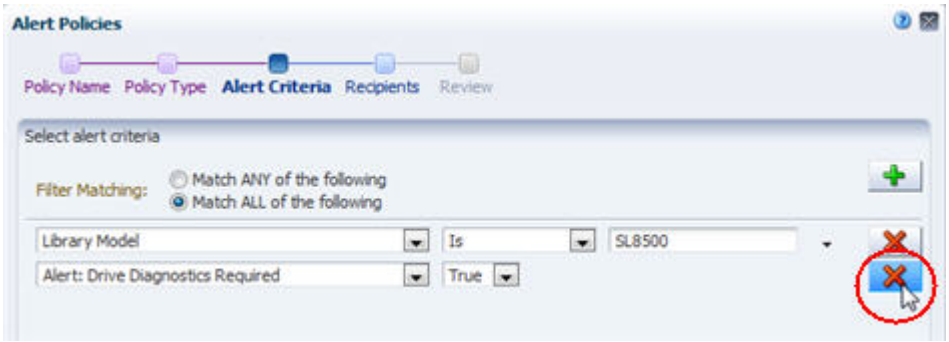
Note: When selecting an attribute for filtering, if you know the name of the attribute you want to select, you can type the first few letters to quickly move the cursor to that item in the menu.

---

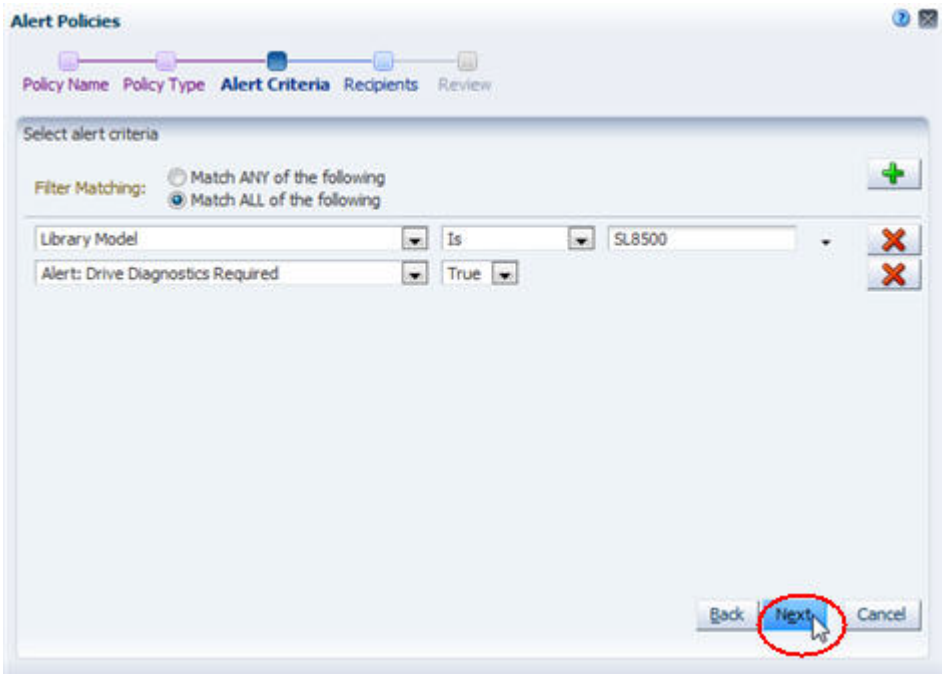
   d. You can add as many rows of selection criteria as you want.

Note: When basing selection criteria on logical groups, it is usually appropriate to use the "Contains" and "Doesn't Contain" operators, rather than the "Is" and "Isn't" operators. This is because drives and media can belong to more than one logical group at a time. See "Filtering by Logical Group" on page 7-4 for details.

e. To remove criteria, click the **Remove This Filter Criteria Row** button on the row you want to delete.



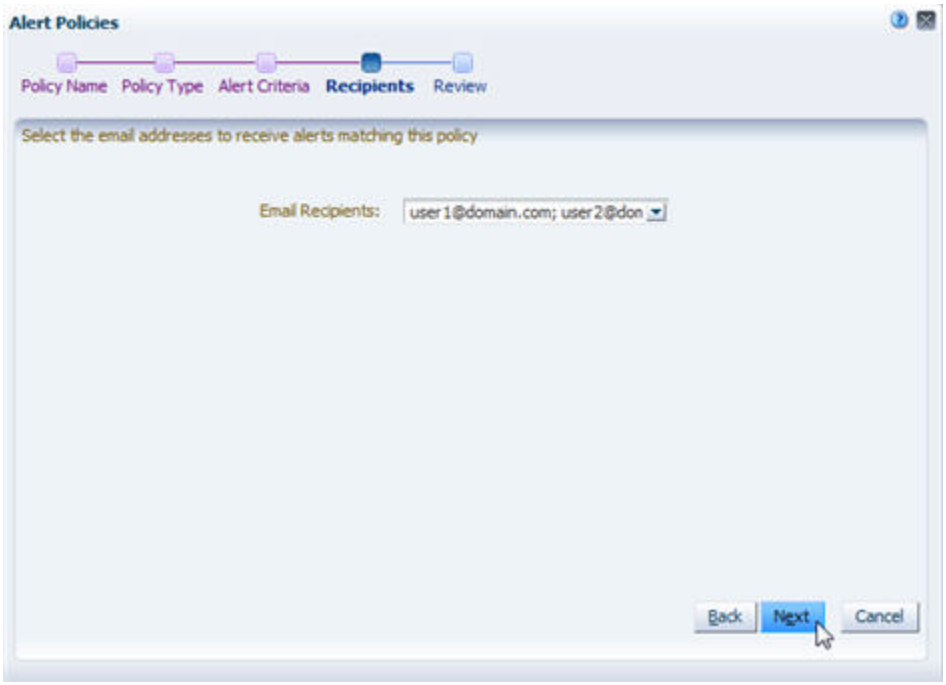
6. Verify that your criteria are correct and click **Next**.



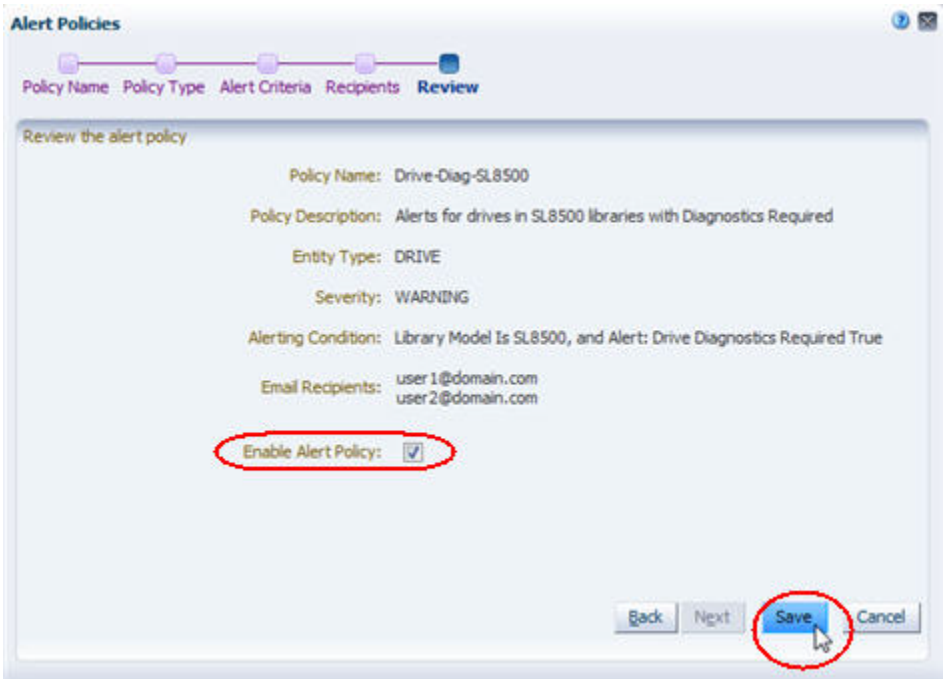
7. Complete the fourth screen of the wizard as follows:

   a. In the **Email Recipients** menu, select the email addresses to which you want emails to be sent whenever an alert is generated by this policy.

   b. Click **Next**.



8. Complete the last screen of the wizard as follows:
   a. Verify that all the policy information is correct.
   b. Use the **Enable Alert Policy** check box 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. You can enable it at a later time. See "Enable or Disable an Alert Policy" on page 5-22 for details.
   c. Click **Save**.



The policy is created. If the policy is enabled, then the appropriate library system resources are immediately evaluated against the policy and alerts are generated as appropriate. If the policy is disabled, then the policy is not evaluated for now.

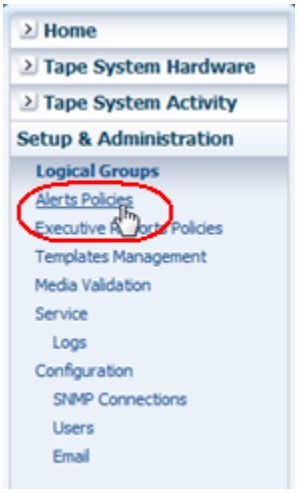
Copy an Alert Policy

Use this procedure to copy a selected alert policy. You can copy any user-defined policy or STA sample policy, depending on your needs. Following are some uses for this procedure.

- Use an existing policy as the basis for a new policy. Copy an existing policy that is similar to one you want to create, and then modify the copy. See "Modify an Alert Policy" on page 5-19 for details.
- Copy the STA sample policies to preserve the original versions. The STA sample policies are not write-protected and there is no way to restore the original versions if they are modified, so it is recommended that you keep copies of the original versions even if you do not use them.

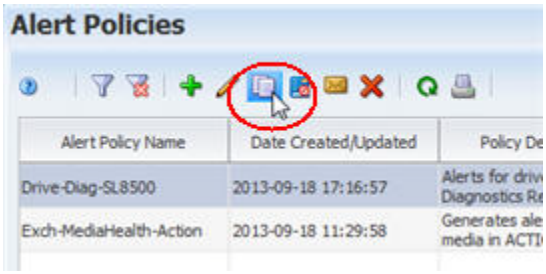
Note: This procedure requires Administrator privileges.

1. In the Navigation Bar, select **Setup & Administration**, then select **Alerts Policies**.



The Alerts Policies screen appears.

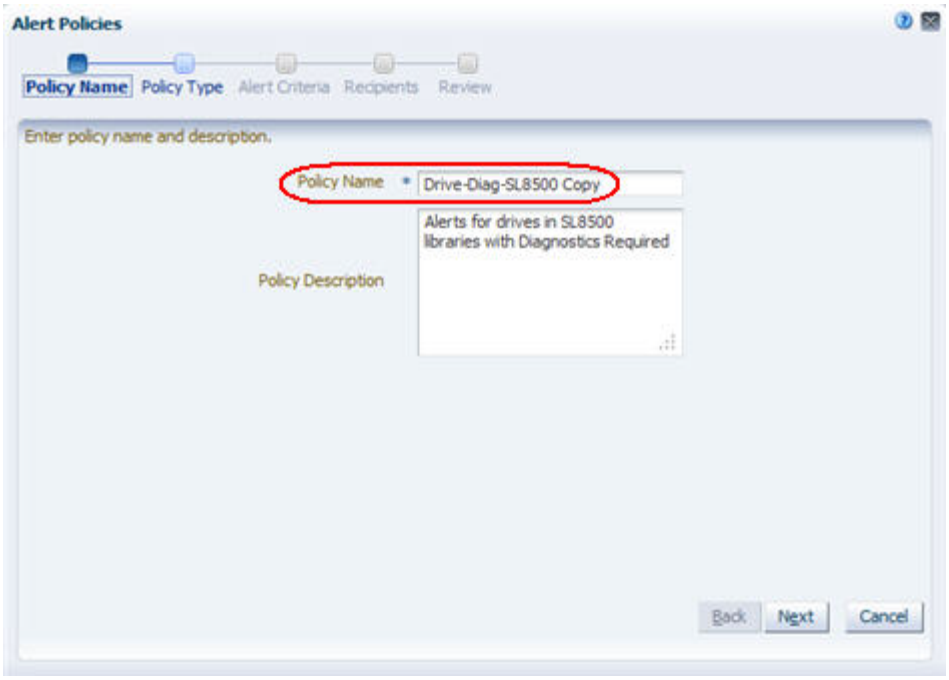
2. Select the alert policy you want to copy and click **Copy Alert Policy**.



The first screen of the Alert Policies wizard appears. The copy of the policy has all the same information as the original, except for the following:

- The word "Copy" is added to the end of the Policy Name.

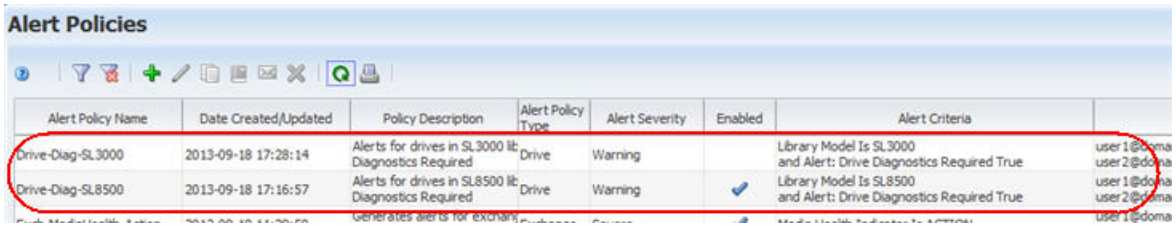
- No email recipients are defined.
- The policy is disabled (the **Enable Alert Policy** check box is deselected).



3. In the **Policy Name** field, type the name you want to assign.
4. Use the **Next** button or the wizard breadcrumbs at the top of the dialog box to navigate to the screens with the information you want to modify. See "Create an Alert Policy" on page 5-12 for details on completing these screens. You can also leave all information unchanged if you are simply copying the original policy to preserve it.
5. Click **Save** when done.

   The new policy is created, and the Alerts Policies screen is updated with the information.

   In the following example, the Drive-Diag-SL3000 policy was copied from the Drive-Diag-SL8500 policy, and the alert criteria were modified to evaluate drives in SL3000 libraries.



Modify an Alert Policy

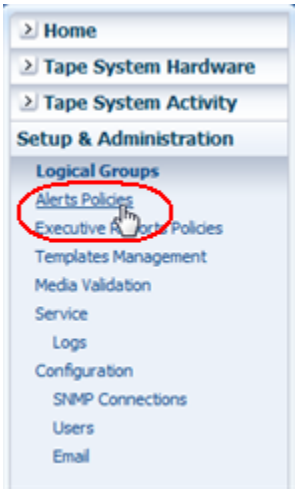
Use this procedure to make any of the following modifications to a selected alert policy.

- Change the policy name.
- Change the policy description.

- Change the tape library system resource or event to be evaluated by this policy.
- Change the policy severity.
- Add, delete, or modify the policy selection criteria.
- Add or delete email recipients; for a more direct method, see "Modify Email Recipients for an Alert Policy" on page 5-21.
- Enable or disable the policy; for a more direct method, see "Enable or Disable an Alert Policy" on page 5-22.

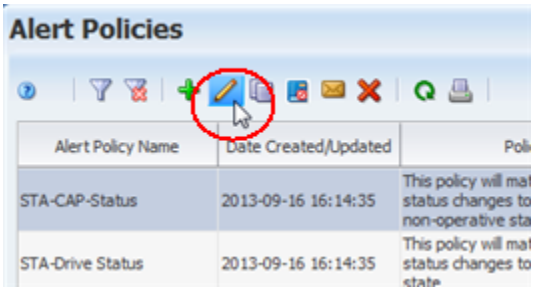
Note: This procedure requires Administrator privileges.

1. In the Navigation Bar, select **Setup & Administration**, then select **Alerts Policies**.

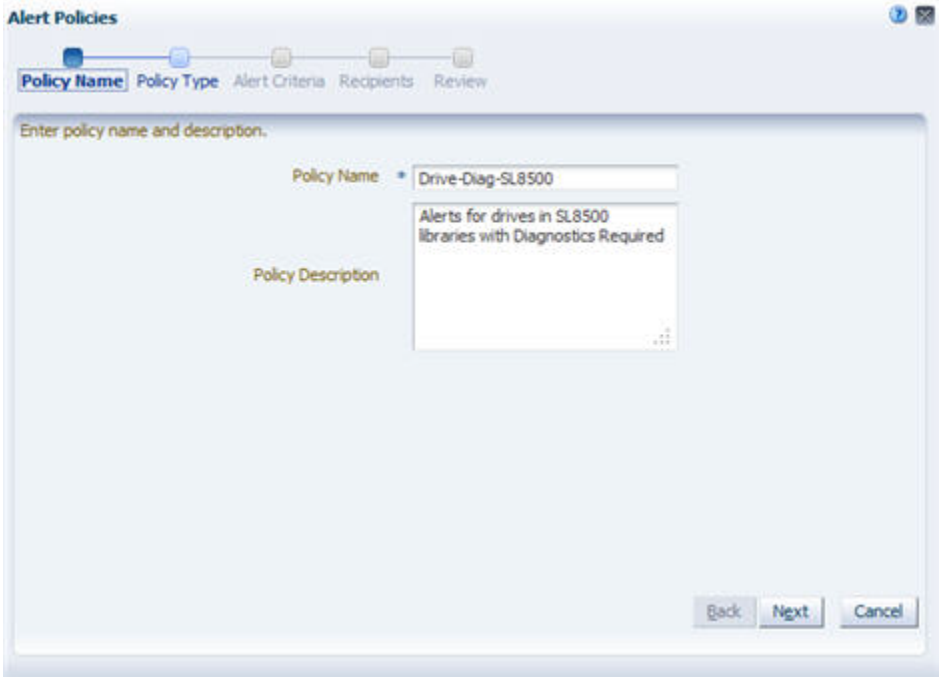


The Alerts Policies screen appears.

2. Select the alert policy you want to modify and click **Edit Alert Policy**.



The first screen of the Alerts Policy wizard appears, and the policy's current information is displayed.



3. Use the **Next** button or the wizard breadcrumbs at the top of the dialog box to navigate to the screens with the information you want to modify. See "Create an Alert Policy" on page 5-12 for details on completing these screens.
4. Click **Save** when done.

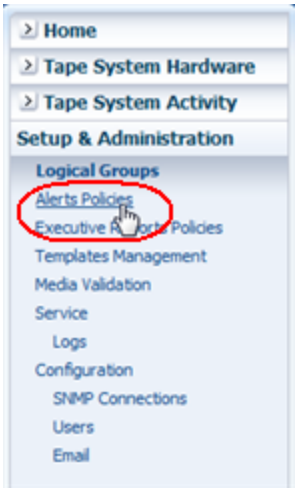
   The policy is updated, and the changes are displayed on the Alerts Policies screen.

Modify Email Recipients for an Alert Policy

Use this procedure to add or delete email recipients for a selected alert policy. The recipients are notified of all alerts generated by the policy. You can choose any number of addresses that have been predefined to STA in the Configuration – Email screen. See "Alert Emails" on page 5-10 for details.

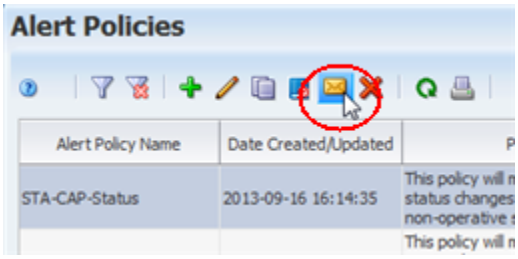
> **Note:** This procedure requires Administrator privileges.

1. In the Navigation Bar, select **Setup & Administration**, then select **Alerts Policies**.



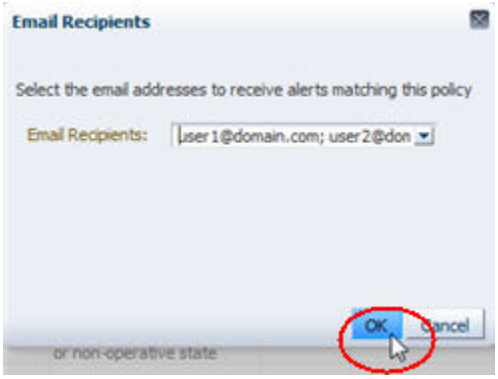
The Alerts Policies screen appears.

2. Select the policy you want to modify and click **Email Recipients**.



The Email Recipients dialog box appears.

3. In the **Email Recipients** menu, select the check boxes next to the addresses you want to receive alerts generated from this policy. Deselect the check boxes next to the addresses not to receive alerts.



4. Click **OK**.

The policy is updated according to your modifications.

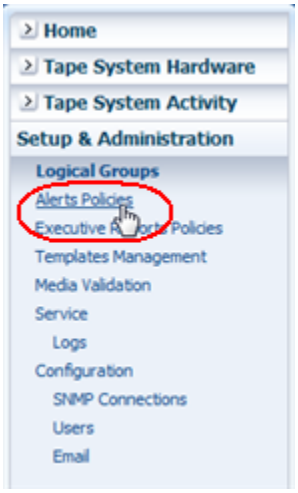
Enable or Disable an Alert Policy

Use this procedure to enable or disable a selected alert policy. Only enabled policies can generate alerts.

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" on page 5-21 for instructions.

Note: This procedure requires Administrator privileges.

1. In the Navigation Bar, select **Setup & Administration**, then select **Alerts Policies**.

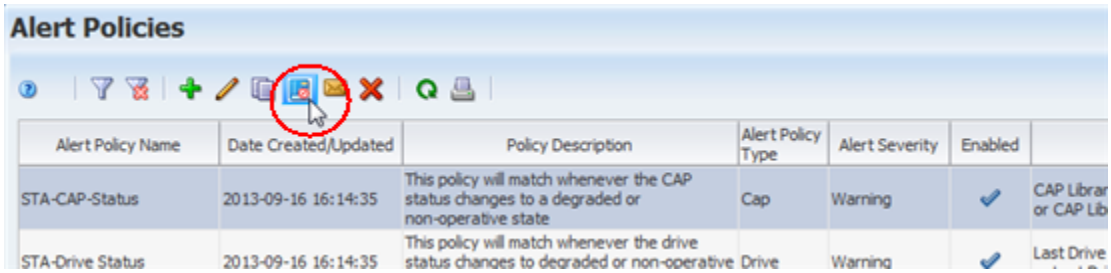


   The Alerts Policies screen appears.

2. Select the policy you want to modify.

   If the policy is currently enabled, the **Disable Alert Policy** icon in the Alerts Policies toolbar becomes active. If the policy is currently disabled, the **Enable Alert Policy** icon becomes active.

3. Click **Enable/Disable Alert Policy**.



   The policy is updated according to your selection.

   - If you have enabled the policy, the corresponding tape library resources or events are immediately evaluated against the policy criteria, and alerts are generated as appropriate.
   - If you have disabled the policy, alerts are no longer generated for the policy.

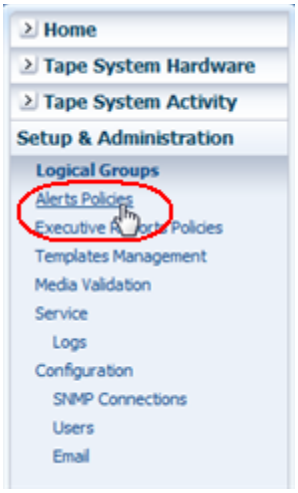
Delete an Alert Policy

Use this procedure to delete an alert policy. Deleting a policy does not delete alerts already generated from this policy; they are still available for viewing on the Alerts Overview screen. You do not have to disable an alert policy before deleting it.

Note: This procedure requires Administrator privileges.

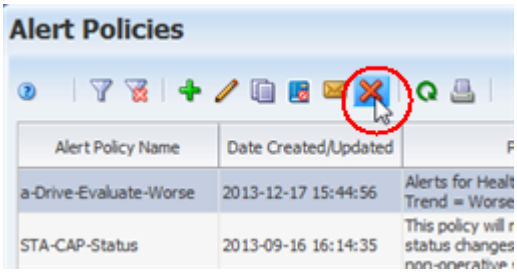
Caution: Be careful not to delete any of the STA sample alert policies because they cannot be restored except by manually re-creating them. All STA sample alert policies have names with an "STA" prefix.

1. In the Navigation Bar, select **Setup & Administration**, then select **Alerts Policies**.



The Alerts Policies screen appears.

2. Select the alert policy you want to delete and click **Delete Alert Policy**.



The Delete dialog box appears.

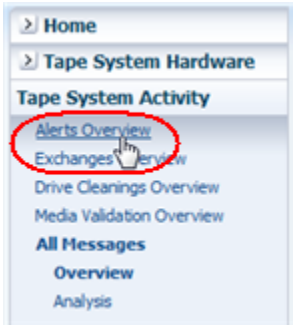
3. Verify your selection and Click **Yes** to confirm the deletion.

The policy is deleted and the list on the Alerts Policies screen is updated.

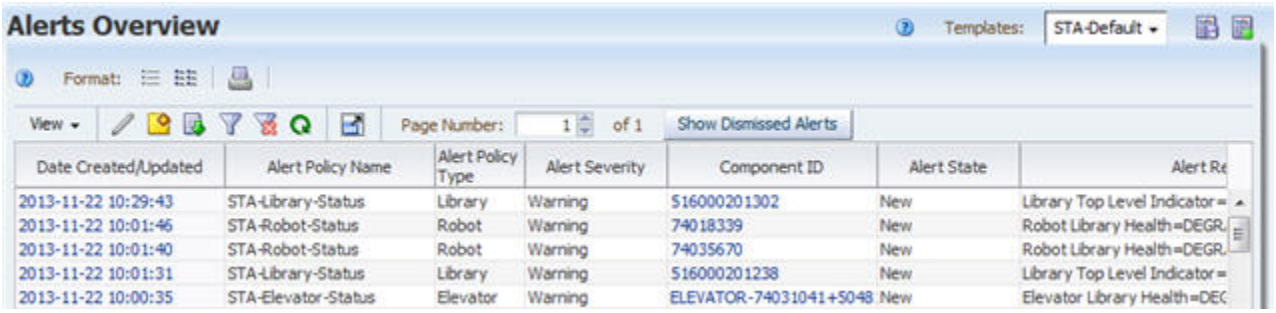
Manage the List of Generated Alerts

> **Note:** With the exception of annotating an alert, this procedure can be done by any STA user. Annotating requires Operator privileges.

1. In the Navigation Bar, select **Tape System Activity**, then select **Alerts Overview**.



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



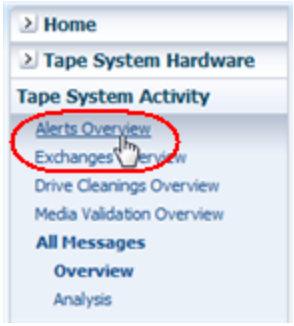
2. You can manage the list of alerts by performing the following procedures:
   - Display a printable form of the table in a separate browser tab or window; see the *STA Screen Basics Guide*.
   - Annotate an alert, see the *STA Screen Basics Guide*.
   - Export the list of alerts; see the *STA Screen Basics Guide*.
   - Filter the list of alerts; see "Use the Filter Data Dialog Box to Change a Table Filter" on page 4-9.
   - Reset a filter applied to the table; see "Clear the Current Filter" on page 4-12.
   - Refresh the table to display new alerts; see the *STA Screen Basics Guide*.
   - Detach the table from the screen and display it in a separate window in the browser foreground; see the *STA Screen Basics Guide*.
   - Go directly to a specific page on the screen; see the *STA Screen Basics Guide*

Display Detail For an Alert

Use this procedure to display an alert and trace it to the tape library system event or condition that triggered it.

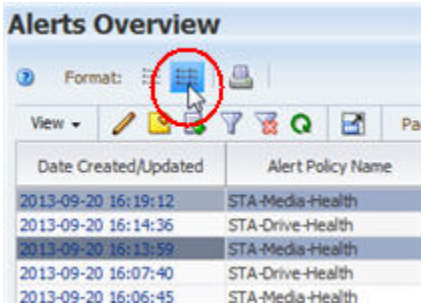
Note: This procedure can be performed by any STA user with Viewer privileges or above.

1. In the Navigation Bar, select **Tape System Activity**, then select **Alerts Overview**.



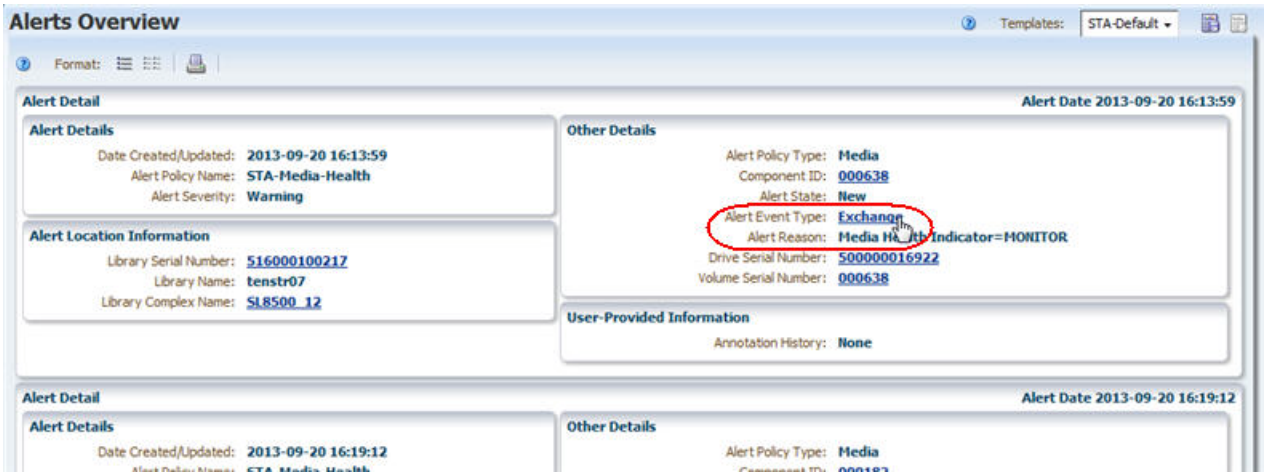
The Alerts Overview screen appears.

2. Select the alerts you want to view and click **Detail View**.

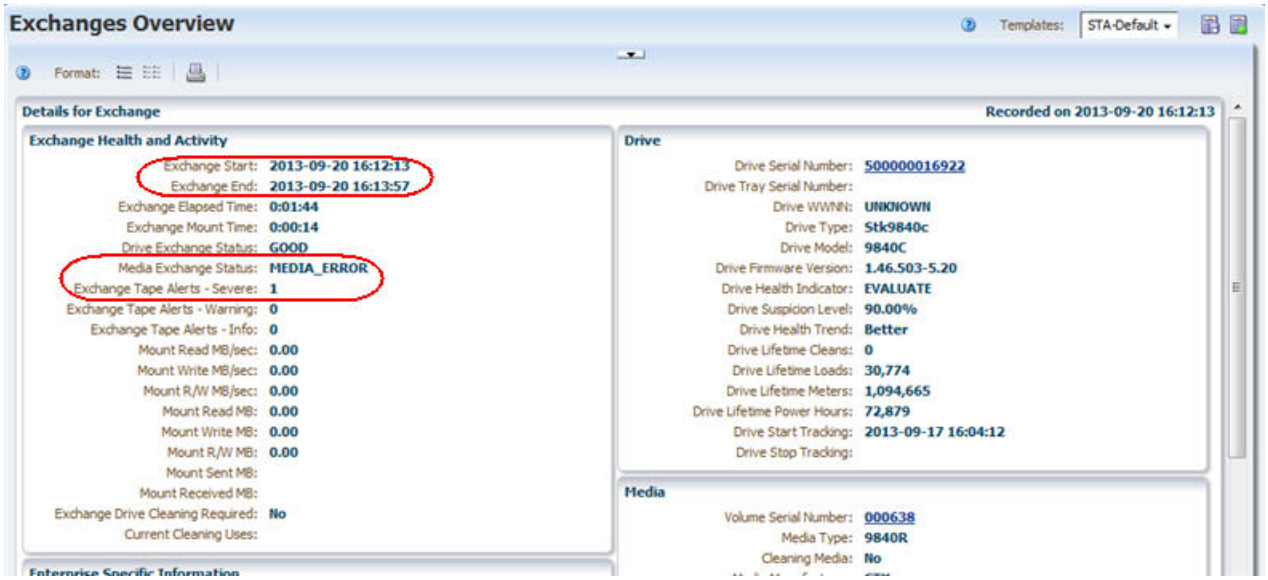


In the Detail View, each record you have selected includes several links to other screens containing related information.

3. Select the link in the Alert Event Type field (in this example, **Exchange**) to display detail for the event that triggered the alert.



You can use the information that is displayed to trace the cause of the alert and determine whether you need to take any action.

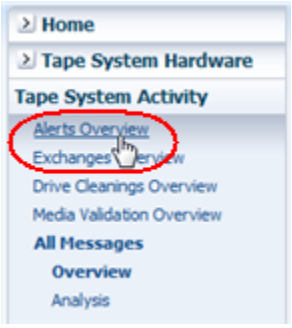


Change the State of an Alert

Use this procedure to change the state of selected alerts according to the alerts workflow process implemented at your site. See "Alerts Workflow" on page 5-11 for details on this process.

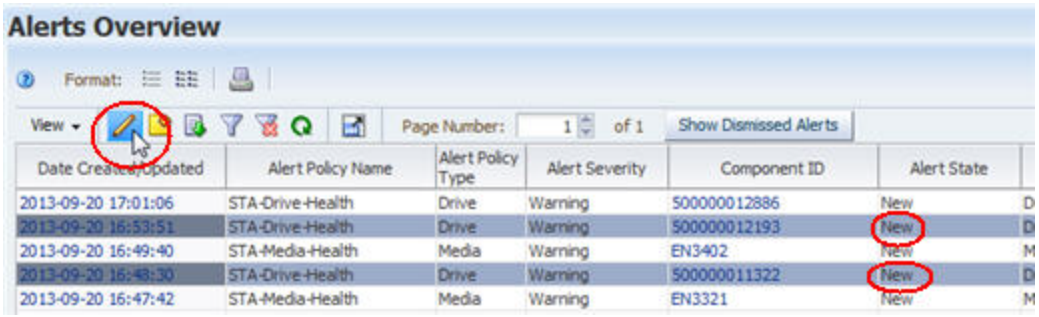
Note: This procedure can be performed by any STA user with Viewer privileges or above.

1. In the Navigation Bar, select **Tape System Activity**, then select **Alerts Overview**.



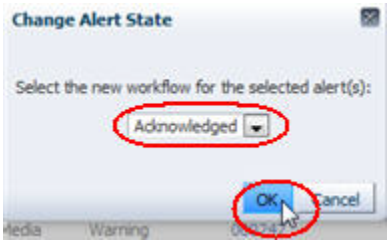
   The Alerts Overview screen appears.

2. Select the alerts you want to modify and click **Change Alert State**. You can select multiple alerts.



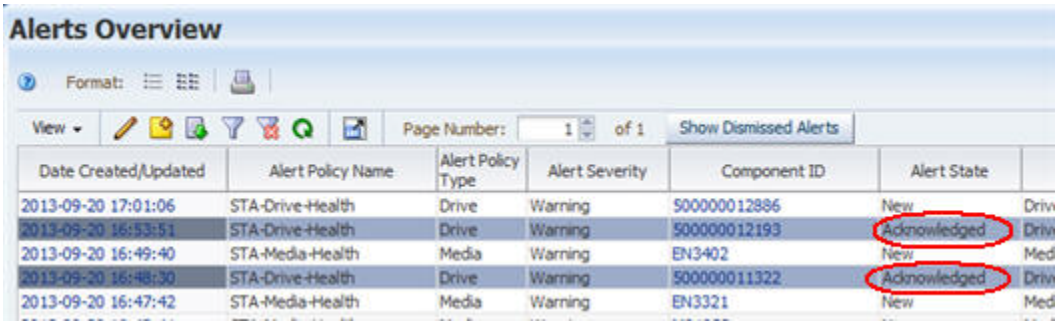
The Change Alert State dialog box appears.

3. In the menu, select the state you want to assign to the selected alerts. You can assign any available state, and then click **OK**.



The alerts are updated, and their new state is displayed in the Alerts Overview screen.

Note: 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" on page 5-28 for details on displaying dismissed alerts.



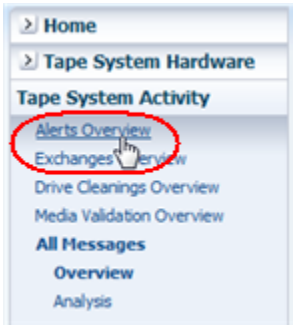
Show or Hide Dismissed Alerts

Use this procedure to toggle the display of dismissed alerts on the Alerts Overview screen. See "Change the State of an Alert" on page 5-27 for details on how alerts are dismissed.

Note: This procedure can be performed by any STA user with Viewer privileges or above.

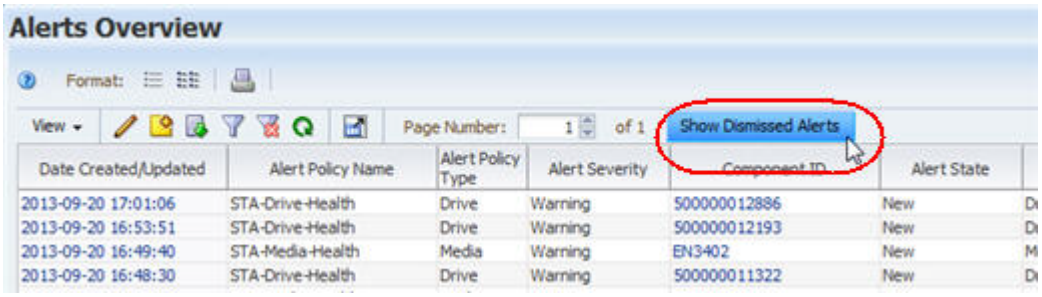
---

1. In the Navigation Bar, select **Tape System Activity**, then select **Alerts Overview**.

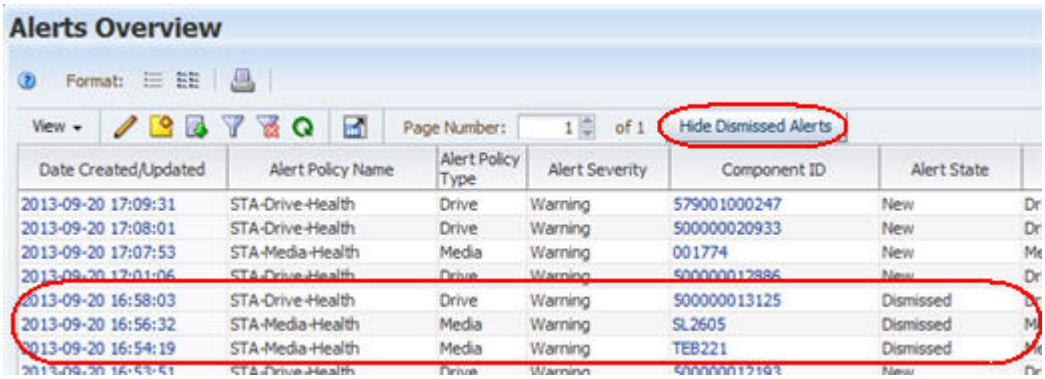


The Alerts Overview screen appears, and by default, all dismissed alerts are hidden from view.

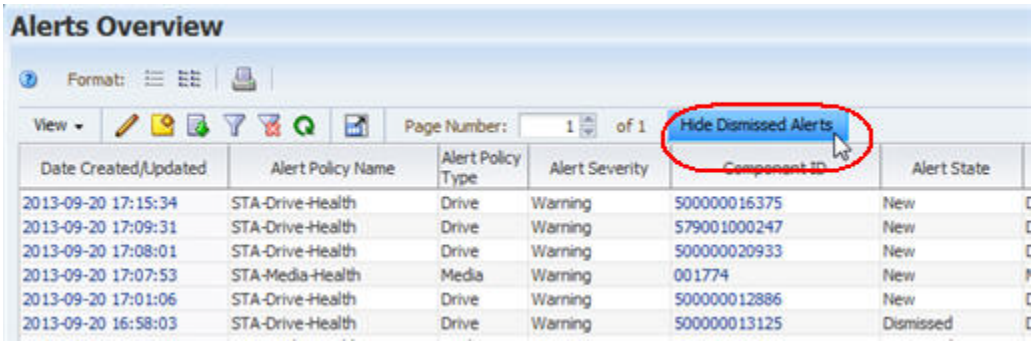
2. Click the **Show Dismissed Alerts** button in the table toolbar.



Dismissed alerts are now visible on the screen, and the button label has changed to **Hide Dismissed Alerts**.



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



6

Executive Reports

STA Executive Reports provide high-level views of your tape library system. Executive Reports are based on defined Dashboard templates, and all the information in the template is included in each report. Dashboard portlet annotations are also included in the reports if they have been added to individual Dashboard portlets and saved as part of the Dashboard templates.

All users have privileges to view Executive Reports, but defining report policies requires Administrator privileges, and running reports requires Operator privileges. See "User Roles for Executive Report Policies" on page 6-6 for more information.

This chapter includes the following sections:

- Executive Report Creation Process
- Using Executive Reports
- Executive Report Policies
- Best Practices for Executive Reports
- Executive Report File Tasks
- Executive Report Policy Tasks

Executive Report Creation Process

The process for running an Executive Report is as follows. Report files are not available until all of these steps have been completed.

1. An Operator or Administrator user defines and saves a custom Dashboard template. (This step is optional, as Executive Reports can also be based on the predefined templates delivered with STA.) See "Create a Template" on page 3-13 for details.
2. An Administrator user creates an Executive Report policy based on the Dashboard template. See "Create or Modify an Executive Report Policy" on page 6-11 for details.
3. An Operator or Administrator user runs the report on demand, or the report runs automatically according to the schedule defined in the policy. See "Run an Executive Report On Demand" on page 6-7 for details.
4. If the report policy includes a list of email recipients, the report file is sent to those users. See "Emailing Executive Reports" on page 6-6 for details.
5. Users view the report file. See "View an Executive Report" on page 6-8 for details.

Using Executive Reports

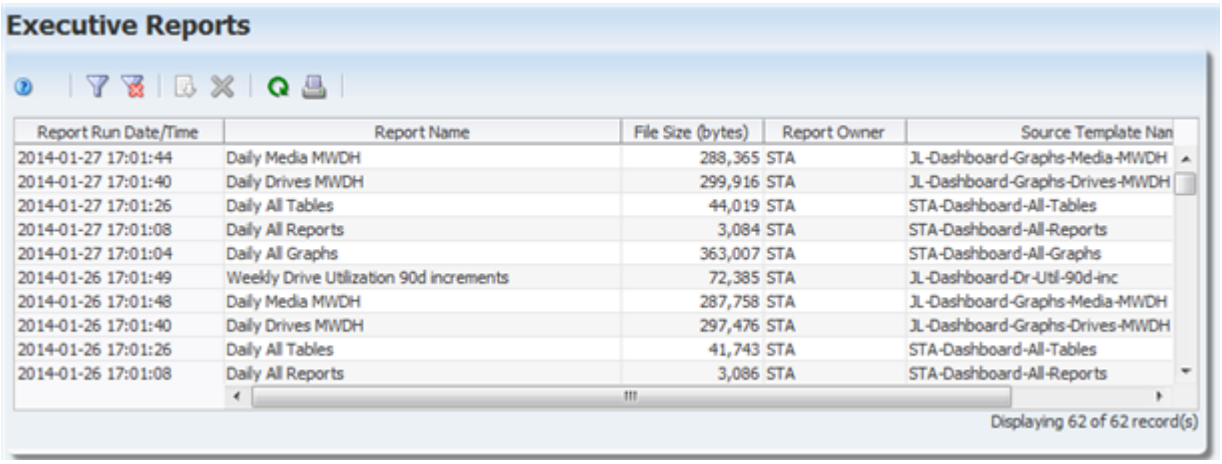
Executive Reports are produced in PDF format and saved to the STA database. Reports can also be sent automatically to designated email recipients.

Displaying Executive Reports

Once an Executive Report has been run, you can view it from the Executive Reports screen on the **Home** tab. Figure 6–1 is an example. The screen lists all report files available to your STA username. If the list is empty or does not include report files you should be able to view, see an STA Administrator user for assistance.

A report policy can be run multiple times, so you may see several instances of the same report, each with a different date and time stamp. Report files are saved in the STA database and are therefore backed up with the regular database backups. You may want to periodically remove old report files you no longer need. See "Delete an Executive Report File" on page 6-9 for details.

Figure 6–1 Sample Executive Reports Screen



Reports are created in PDF format, and you can either view them directly in your browser window or save them to your local computer for later viewing. See "View an Executive Report" on page 6-8 for instructions. Figure 6–2 is a sample page from an Executive Report.

You may also receive Executive Report output by email. This must be set up by a user with Administrator privileges. See "Emailing Executive Reports" on page 6-6 for details.

Figure 6–2 Sample Executive Report

Running Executive Reports

Executive Reports can be run on a regular schedule and on demand. Report schedules can be defined only by users with Administrator privileges. Reports can be run on demand by users with Operator privileges and above.

Report Schedule

Executive Reports can be run on a regular schedule at the following frequencies.

- Daily (every 24 hours)
- Weekly (every 7 days)
- Monthly (every 30 days)
- Quarterly (every 90 days)

- Yearly (every 365 days)

The user does not need to be logged in for a report to run. Reports always run automatically in the background shortly after 00:30 UTC time. The time displayed in the report header is in UTC time.

The report schedule is based on the Start Date of the report and is days-based, not calendar-based. Therefore, a monthly report runs on the specified Start Date and every 30 days thereafter, not necessarily on the same date every month. Following are some examples to clarify. The Start Date for all is 10/15/2013.

Frequency	Report Schedule
Daily	10/15/2013, 10/16/2013, 10/17/2013, and so on
Weekly	10/15/2013, 10/22/2013, 10/29/2013, and so on
Monthly	10/15/2013, 11/14/2013, 12/14/2013, 01/13/2014, and so on
Quarterly	10/15/2013, 01/13/2014, 04/13/2014, 07/12/2014, and so on
Yearly	10/15/2014, 10/15/2015, 10/15/2016, 10/14/2017, and so on

On-demand Reports

When run on demand, Executive Reports are run at the next available opportunity. Depending on system activity, there may be a delay of up to two minutes before the start of execution. On-demand report runs do not affect the regular report schedule—a report will run at its regularly scheduled times regardless of how many times it is run on demand.

User Roles for Executive Report Files

Some Executive Report file tasks can be performed by all user roles, whereas others are available only to Administrator or Operator roles.

Note: Regardless of user role, you can view reports run automatically or by any STA username.

Table 6–1 summarizes the Executive Report file activities available to each STA user role.

Table 6–1 Executive Report File User Roles

User Role	Report Activity	Screen
Operator and above	Run a public report on demand.	Select **Setup & Administration**, then select **Executive Reports Policies**.
Operator and above	Delete a public report file run automatically or on demand.	Select **Home**, then select **Executive Reports**.
Viewer and above	Display a list of public report files run automatically or on demand, as follows: ■ Export and view a report file. ■ Filter the report file list. ■ Print the report file list.	Select **Home**, then select **Executive Reports**.

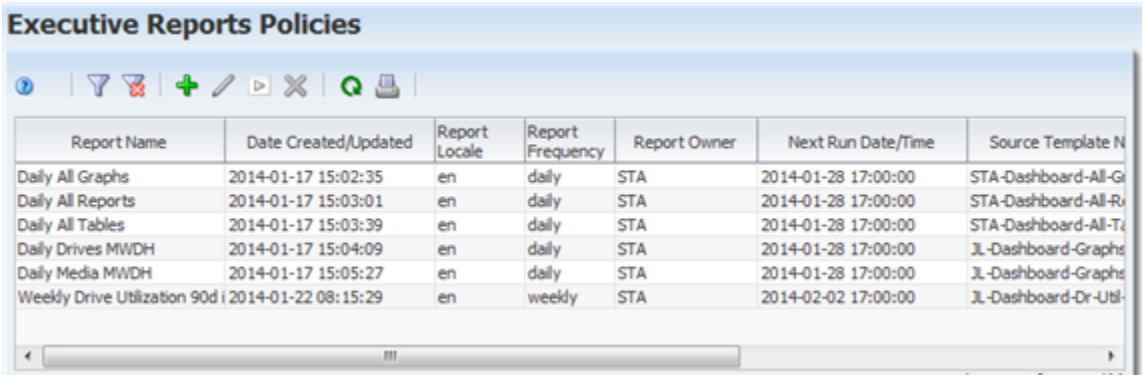
Executive Report Policies

This section provides information about Executive Report policies.

Defining Executive Report Policies

The Executive Reports Policies screen on the **Setup & Administration** tab displays all Executive Report policies. Figure 6–3 is an example.

Figure 6–3 Sample Executive Reports Policies Screen



Each Executive Report policy is based on a saved Dashboard template and includes the following elements:

- Report name – An alphanumeric identifier for the report. Report names are not required to be unique.
- Source Dashboard template – Reports can be based on any Dashboard template available to your STA username, except the one named "STA-Default." To create a report based on the template named "STA-Default," you must first save the template to a different name, and then base the report on the new name.
- Start Date – The first day that the report is scheduled to be run. See "Running Executive Reports" on page 6-3 for details. It will run automatically shortly after 00:30 UTC on this day.
- Frequency – The frequency at which the report is scheduled to be run. See "Running Executive Reports" on page 6-3 for details.
- Ownership – An Executive Report policy's ownership determines who can see and use the policy. Public policies are owned by the STA user. Private policies are owned by the STA Administrator username that created them. Private policies and the reports generated by them can be managed and viewed from the STA user interface only by the policy owner. Public policies and the reports generated by them can be viewed and managed by any user.

  Note: When an STA username is deleted, all private report policies owned by that username are automatically deleted or made public, according to the selection made by the Administrator user performing the deletion. See the "Delete an STA Username" on page 9-7 for details.

- Email recipients – Reports can be sent to any number of email addresses. Email addresses must be defined in the Configuration – Email screen. A PDF of the report is sent to the recipient after each report run has completed.

Emailing Executive Reports

Emailing reports is one way you can provide reports to people who are not regular users of STA and who do not have an STA username. Each Executive Report can be sent to any number of email addresses, which have been previously defined to STA through the Configuration – Email screen. See "Add an STA Username" on page 9-5 for instructions.

The email recipient list for each report can be defined only by a user with Administrator privileges. A PDF of the report is sent to each recipient as soon as it is run. See Figure 6–2 for a sample page from an Executive Report.

User Roles for Executive Report Policies

Table 6–2 summarizes the Executive Report policy activities available to the Operator and Administrator roles.

Table 6–2 Executive Report Policy 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. Modify a report policy, including public policies or private policies created by the current STA username, as follows: ▪ Define a regular schedule for the report. ▪ Assign public or private ownership to the policy. ▪ Designate email addresses to receive report files. ▪ Change the Dashboard template on which the report is based. ▪ Delete the policy.	Select **Setup & Administration**, then select **Executive Reports Policies**.
Operator and above	Display a list of public report policies only, as follows: ▪ Filter the report policy list. ▪ Print the report policy list.	Select **Setup & Administration**, then select **Executive Reports Policies**.

Best Practices for Executive Reports

This section includes tips for creating and using Executive Reports.

Get to know your site's operational profile

Use this process to discover the power of STA and get a solid overview of current operations and activity at your site.

1. Identify a set of existing templates—or create some new ones—that show the specific areas of interest at your site.

   See Appendix B, "STA Predefined Templates".

2. Use these templates to generate a set of Executive Reports for various periods: hourly, daily, weekly, and monthly.

   See "Create or Modify an Executive Report Policy" on page 6-11.

3. 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.

4. 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

Executive Report File Tasks

These tasks involve viewing and managing Executive Report output files, and they can be performed by all user roles. These tasks are performed from the Executive Reports screen on the **Home** tab.

> **Note:** You only have access to public reports and private ones owned by your STA username. You cannot perform these tasks on reports privately owned by another STA username. See "Defining Executive Report Policies" on page 6-5 for additional information.

- "View an Executive Report" on page 6-8
- "Delete an Executive Report File" on page 6-9
- "Manage the List of Executive Report Files" on page 6-10

Run an Executive Report On Demand

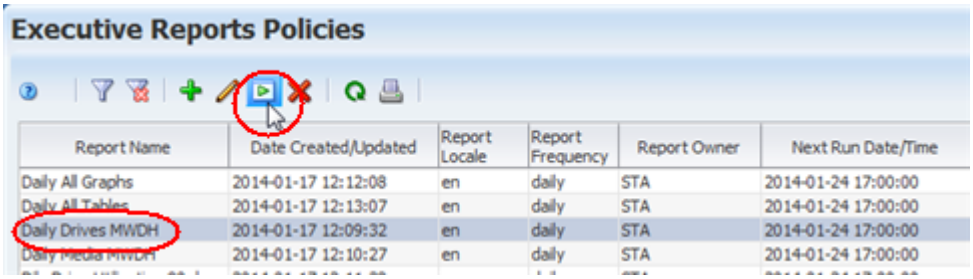
Use this procedure to run a selected Executive Report right away. The report is run at the first available opportunity, which could take up to two minutes. This does not affect the report's schedule—it will also be run at its regularly scheduled time.

> **Note:** This procedure requires Operator or Administrator privileges.

1. In the Navigation Bar, select **Setup & Administration**, then select **Executive Reports Policies**.

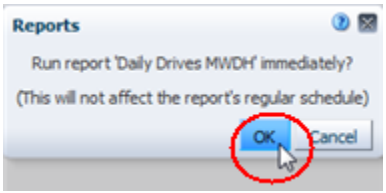
The Executive Reports Policies screen appears.

2. Select the report policy you want to run and click **Run**.



A confirmation dialog box appears.

3. Verify the information and click **OK** to run the report.

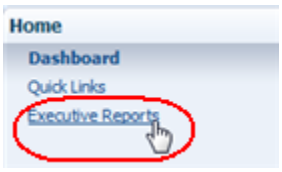


The report is run. See "View an Executive Report" on page 6-8 for instructions on displaying the output.

View an Executive Report

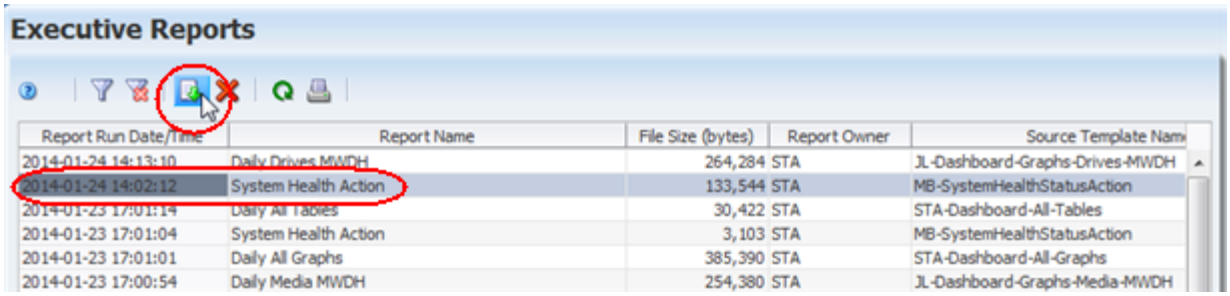
Use this procedure to view an Executive Report after it has been run. Reports are created in Adobe PDF format.

1. In the Navigation Bar, select **Home**, then select **Executive Reports**.

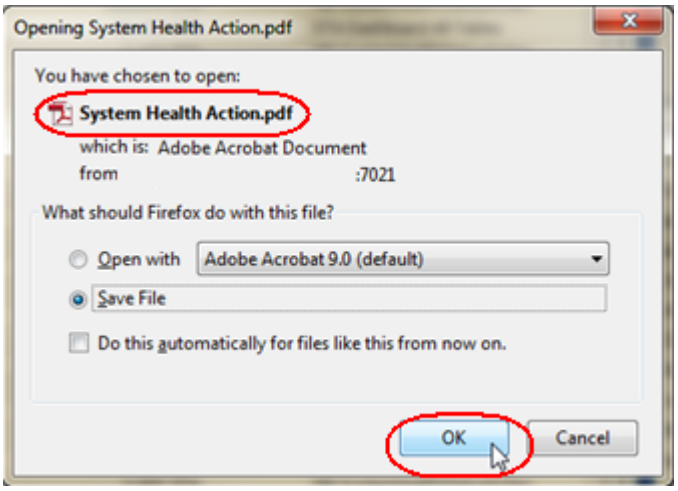


The Executive Reports screen appears, showing all report files available to your STA username.

2. Select the report file you want to view and click **Export**.



The file is downloaded to your computer according to your browser settings. See your browser documentation for details. Following is a sample dialog box you might see on a computer running Mozilla Firefox on Windows.



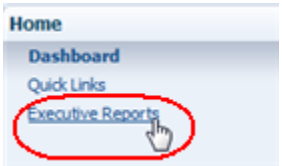
In this example, you would proceed as follows:

- Click **Save File** and **OK** to save the report to your local computer. The report is saved in PDF format and can be viewed with Adobe Reader at a later time.
- Click **Open with** and **OK** to view the report from your browser. This option requires the Adobe Acrobat add-on to be installed and enabled in your browser, and the exact functioning depends on your browser configuration. If you are not able to use this option, see your browser documentation for instructions.

Delete an Executive Report File

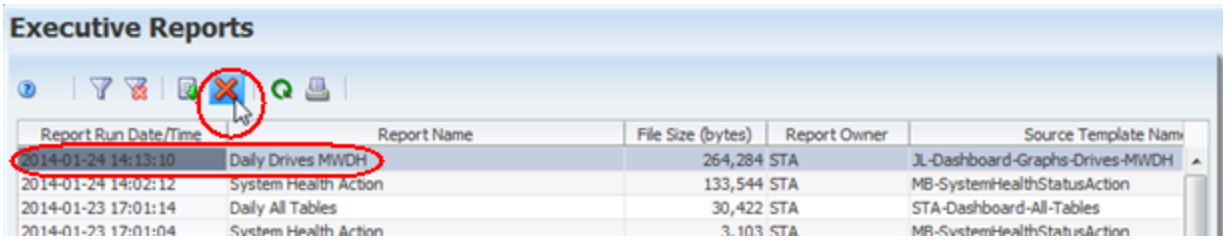
Use this procedure to delete a selected report file. This does not affect other report files, nor the report policy definition. You can select only one report file at a time to delete.

1. In the Navigation Bar, select **Home**, then select **Executive Reports**.



The Executive Reports screen appears, showing all report files available to your STA username.

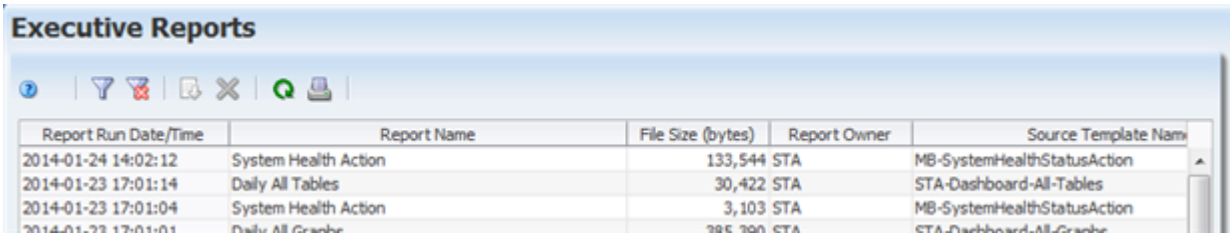
2. Select the report file you want to delete and click **Delete**.



A Delete confirmation dialog box appears.

3. Verify your selection and Click **Yes** to confirm the deletion.

The report file is deleted and is no longer available for viewing from the Executive Reports screen.



Manage the List of Executive Report Files

The list of Executive Report files is a List View table, similar to those found on Overview screens, and you can perform the same functions as for any List View table. See the following procedures for instructions:

- To filter the table records, see "Use the Filter Data Dialog Box to Change a Table Filter" on page 4-9.
- To reset a filter applied to the table, see "Clear the Current Filter" on page 4-12.
- To refresh the table to display any new report files, see the *STA Screen Basics Guide*.
- To display a printable form of the table in a separate browser tab or window, see the *STA Screen Basics Guide*.
- To detach the table from the screen and display it in a separate window in the browser foreground, see the *STA Screen Basics Guide*.

Executive Report Policy Tasks

These tasks involve creating and managing the Executive Report policies, and they require Operator or Administrator privileges. These tasks are performed from the Executive Reports Policies screen on the **Setup & Administration** tab.

> **Note:** You only have access to public reports and those owned by your STA username. You cannot perform these tasks on reports privately owned by another STA username. See "Defining Executive Report Policies" on page 6-5 for additional information.

- "Create or Modify an Executive Report Policy" on page 6-11.
- "Delete an Executive Report Policy" on page 6-14
- "Run an Executive Report On Demand" on page 6-7
- "Manage the List of Executive Report Policies" on page 6-15

Create or Modify an Executive Report Policy

Use this procedure to create an Executive Report policy or make any of the following modifications to an existing public policy or a private policy owned by your STA username.

- Change the name of the policy.
- Designate a different Dashboard template on which the policy is based.

> **Note:** You can make this modification only if the policy is based on a private template owned by your STA username or a public template.

- Change the regular schedule for when reports are generated from the policy.
- Change public or private ownership of the policy and the reports generated from it.
- Change the email recipients for reports generated by the policy.

Optionally, you can run the report on demand after making the changes.

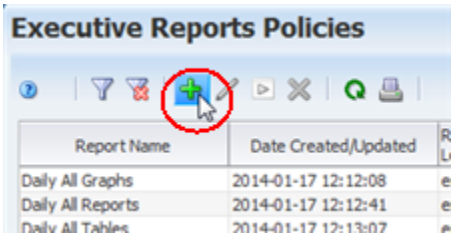
> **Note:** This procedure requires Administrator privileges.

1. In the Navigation Bar, select **Setup & Administration**, then select **Executive Reports Policies**.

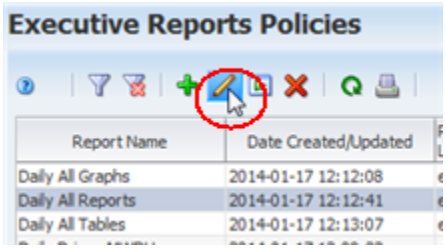
The Executive Reports Policies screen appears.

2. Proceed as follows:

   - To create a report, click **Add** in the Executive Reports Policies table toolbar.



   - To modify an existing report policy, select the policy in the table and click **Edit**. You cannot modify a private Executive Report policy owned by another STA username.



The Add/Edit Executive Reports Policy dialog box appears.

3. Complete the Add/Edit Executive Reports Policy dialog box as follows:

   a. In the **Report Name** field, type a unique name.

      Your entry can include any alphanumeric characters up to 250 characters in length.

   b. In the **Source Dashboard Template** menu, 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.

Note: This field is display-only if you are modifying a policy and the source template is owned privately by another STA username.

---

c. In the **Locale** menu, select English; this is the only option available at this time.

d. In the **Start Date** field, specify the date when you want scheduled runs of the report to begin. Reports are run shortly after 00:30 UTC, starting on this date.

e. In the **Run Frequency** menu, select the frequency at which you want the report to run.

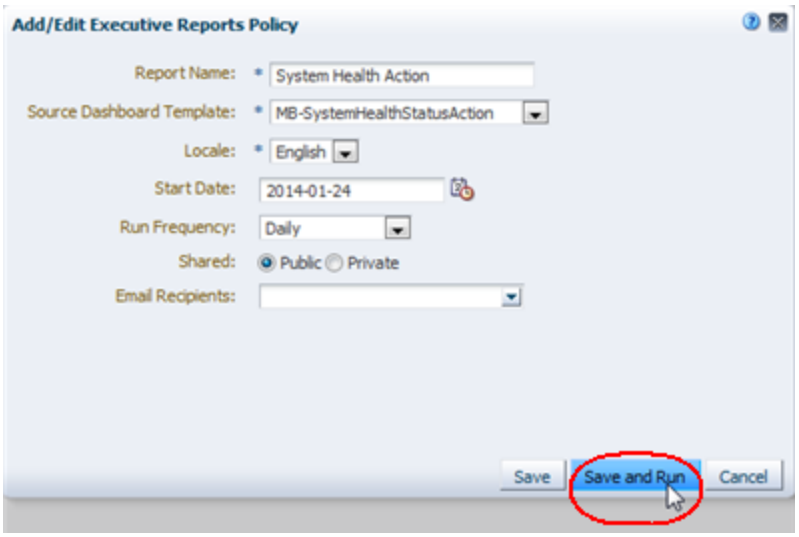
f. In the **Shared** field, select one of the following options:

- **Public** to make the report available to all users.
- **Private** to make the report available to the current STA username only. 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.

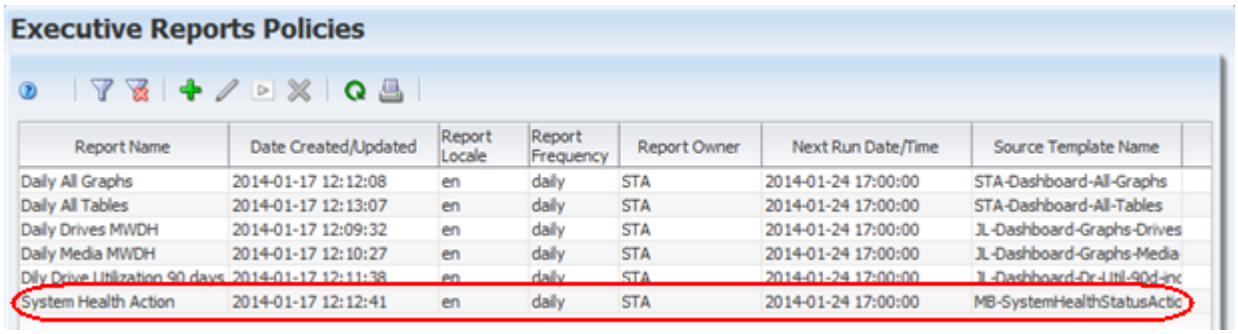
g. In the **Email Recipients** menu, select the email addresses to which you want copies of the report sent after each report run. The report is sent as a PDF attachment. The menu lists all email addresses that have been defined to STA.

4. Verify the information is correct, and then click one of the following buttons:

- **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 defined; it will also run at its regularly scheduled time, starting on the designated Start Date.



The Executive Reports Policies screen is updated with the new policy information.



If you selected **Save and Run**, the report is run in the background at the first available opportunity. It may take up to two minutes for the report to start running.

As soon as the report run finishes, the output is available from the Executive Reports screen on the **Home** tab. See "View an Executive Report" on page 6-8 for instructions on displaying the output.

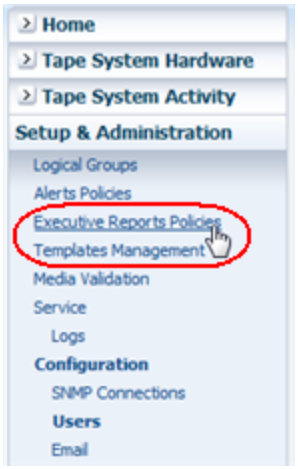
Delete an Executive Report Policy

Use this procedure to delete an Executive Report policy. You can only delete Public policies or Private policies that have been created by your STA username.

Deleting a report policy does not delete previously run report files; they are still available for viewing on the Executive Reports screen.

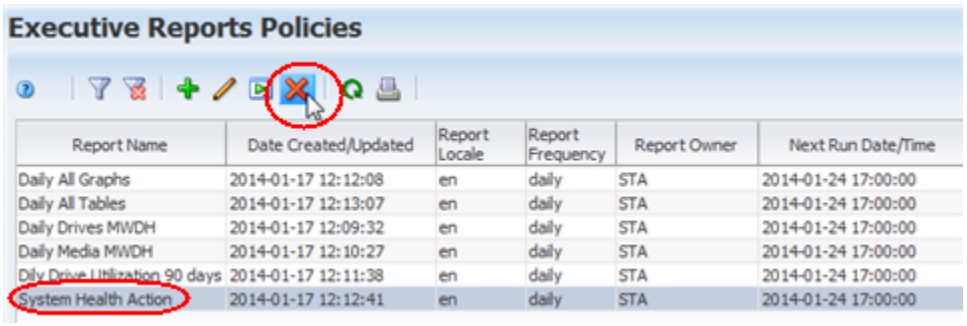
Note: This procedure requires Administrator privileges.

1. In the Navigation Bar, select **Setup & Administration**, then select **Executive Reports Policies**.



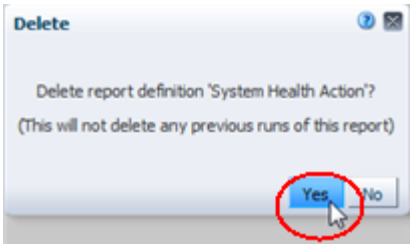
The Executive Reports Policies screen appears.

2. Select the report policy you want to delete and click **Delete**.



The Delete dialog box appears.

3. Verify your selection and Click **Yes** to confirm the deletion.



The report policy is deleted.

Manage the List of Executive Report Policies

The list of Executive Report policies is a List View table, similar to those found on Overview screens, and you can perform the same tasks as for any List View table. See the following procedures for instructions:

- To filter the table records, see "Use the Filter Data Dialog Box to Change a Table Filter" on page 4-9.
- To reset a filter applied to the table, see "Clear the Current Filter" on page 4-12.
- To refresh the table to display any new report policies, see the *STA Screen Basics Guide*.
- To display a printable form of the table in a separate browser tab or window, see the *STA Screen Basics Guide*.
- To detach the table from the screen and display it in a separate window in the browser foreground, see the *STA Screen Basics Guide*.

7

Logical Groups

STA's logical group feature allows you to create any number of user-defined groups of drives and media. Logical groups are useful for filtering and reporting STA data. If your site has enabled the optional STA media validation feature, you can use logical groups when defining automated media validation policies. See "Validating Media by Logical Group" on page 8-20 for details.

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.

Anyone with Operator or Administrator privileges can perform the activities described in this chapter.

This chapter includes the following topics:

- Using Logical Groups
- Logical Group Creation Process
- Types of Logical Groups
- Filtering by Logical Group
- Best Practices for Logical Groups
- Logical Group Creation and Management Tasks

Using Logical Groups

Following are some ways logical groups can help you to organize and report your STA data:

- Use logical groups to filter data on the following screens. See "Filtering by Logical Group" on page 7-4 for details.
  - Drives Overview and Drives Analysis
  - Media Overview and Media Analysis
  - Selected Dashboard portlets
- Save screen layouts that have been filtered by logical group as templates. The filters are saved as part of the templates. See "Screen Characteristics Included in the Template Definition" on page 3-3 for details.
- Create Executive Reports based on Dashboard templates that are filtered by logical group. See "Executive Reports" on page 6-1for details.

Logical Group Examples

Example 1 Logical Groups for 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.

Example 2 Logical Groups for 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.

Example 3 Logical Groups for 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.

Example 4 Logical Group for 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. See "Calibration Media Logical Group" on page 8-15 for details.

Logical Group Creation Process

The process for creating a logical group is as follows.

1. Create the logical group from the Logical Groups screen. You assign a name and designate whether it is a manual or dynamic group. See "Types of Logical Groups" on page 7-3 and for details.
2. Add drives and media to the group using either of the following methods:
   - If the group is manual, then you select individual drives and media to add to the group. This is done from the Drives Overview and Media Overview screens. See "Add Drives and Media to a Manual Logical Group" on page 7-13 for details.
   - If the group is dynamic, then you define the selection criteria by which drives and media are assigned to the group. This is also done from the Logical Groups screen. STA then automatically builds the group. See "Create and Define a Dynamic Logical Group" on page 7-17 for details.

Logical Group Ownership

A logical group is owned by the STA username that created it, and the ownership cannot be changed except when the owner is deleted. The logical group owner is displayed on the Logical Groups screen.

Note: When an STA username is deleted, all logical groups owned by that username are automatically deleted or made public, according to the selection made by the Administrator user performing the deletion. See "Delete an STA Username" on page 9-7 for details.

Types of Logical Groups

When you create a logical group, you designate whether it is manual or dynamic. Once you have created a group, you cannot change its type.

Manual Logical Groups

Manual logical groups are relatively static—membership does not change except through direct user intervention. You build manual logical groups by manually assigning selected drives and media to the group. You can add or delete drives and media from a group at any time. See "Create a Manual Logical Group" on page 7-11 for details.

Dynamic Logical Groups

Dynamic logical groups evolve over time as drive and media attributes change. Membership in a dynamic logical group is based on selection criteria that you define. Logical group selection criteria work in much same way as the STA filtering feature, and they can range from simple to very complex. See "Create and Define a Dynamic Logical Group" on page 7-17 for details.

Depending on the size of your tape library system, it may take some time to build a dynamic group for the first time. The group is built in the background, so you can proceed with other STA activities while the group is being built.

Updates to Dynamic Group Membership

Dynamic group membership is automatically updated as drives and media are added and removed from your library environment, and as the attributes of individual drives and media change. 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.

Group membership updates occur once per hour, but you can manually initiate a group update at any time. See "Force a Dynamic Logical Group Update" on page 7-22 for details.

You cannot manually add or delete individual drives and media from a dynamic group. To change the membership of a dynamic group, you can revise the selection criteria. See "Change the Selection Criteria for a Dynamic Logical Group" on page 7-21.

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. Following are some examples:

- Matching on Library Name selects both drives and media.
- Matching on Drive Type selects only drives.
- Matching on Cleaning Media selects only media.

Table 7–1 identifies the available criteria and whether they apply to drives only, media only, or both.

Table 7–1 Dynamic Logical Group Selection Criteria

Attribute	Drives Only	Media Only	Both
Cleaning Media		X	

Table 7–1 (Cont.) Dynamic Logical Group Selection Criteria

Attribute	Drives Only	Media Only	Both
Drive Firmware Version	X		
Drive Health Indicator	X		
Drive Serial Number	X		
Drive Type	X		
Drive Suspicion Level	X		
HLI Address			X
Library Complex Name			X
Library Model			X
Library Name			X
Library Number			X
Library Serial Number			X
Media Health Indicator		X	
Media Suspicion Level		X	
Media Type		X	
Partition Name			X
Partition Number			X
Partition Type			X
Physical Address			X
Rail Number			X
SCSI Element ID			X
STA Start Tracking (Number of Fays)			X
STA Start Tracking (Date)			X
Volume Serial Number		X	

Filtering by Logical Group

While only users with Operator or Administrator privileges can create and manage logical groups, all users, including those with Viewer privileges, can use existing logical groups to filter STA data. Filtering screens by logical group allows you to focus on just the drives and media in that group.

The data on the following screens can be filtered by logical group:

- Drives Overview and Drive Analysis
- Media Overview and Media Analysis
- Selected Dashboard portlets – See "Dashboard Portlets With Filtering by Logical Group" on page 7-10 for a list of the portlets.

In addition, you can use logical groups in the selection criteria for the following types of policies:

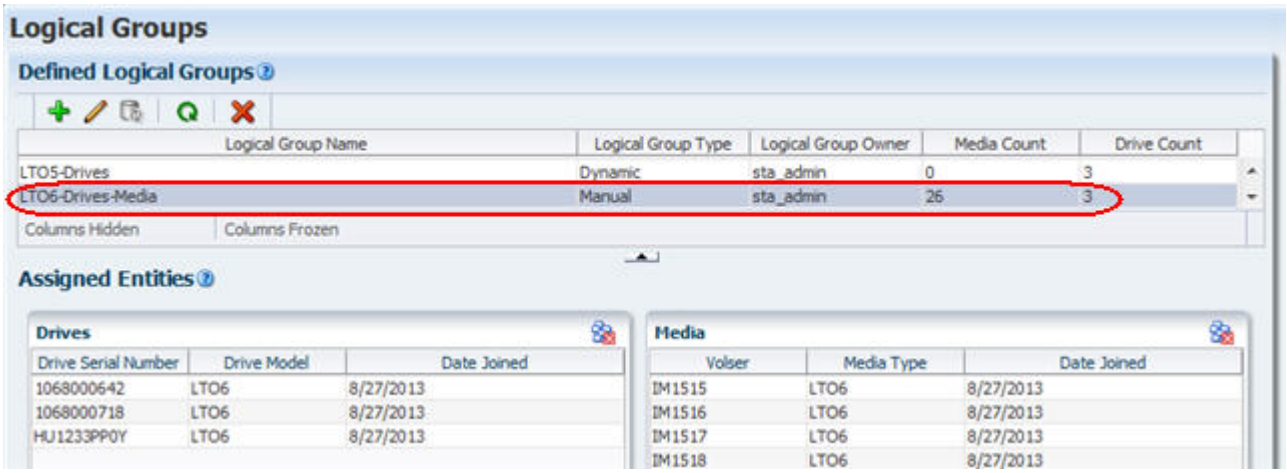
- Alert policies – See "Alert policies and the "Contains" operator" on page 5-10 for details.

- Media validation policies – See "Calibration Media Logical Group" on page 8-15 and "Validating Media by Logical Group" on page 8-20 for details.

Constructing Filters Using Logical Groups

Drives and media can belong to more than one logical group at a time. Therefore, when you construct selection criteria for filtering by logical group, it is usually appropriate to use the "Contains" and "Doesn't Contain" operators on the Filter Data dialog box, rather than the "Is" and "Isn't" operators. The "Is" and "Isn't" operators require an exclusive match and therefore may result in filters that select no records at all, or all records, rather than records belonging to the logical groups you specify.

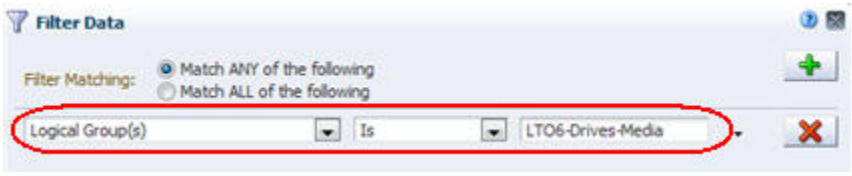
The examples below illustrate use of these operators. These examples use the "LTO6-Drives-Media" logical group, which includes three drives and 26 media.

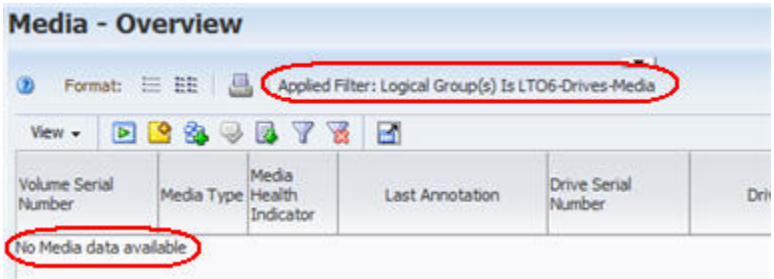


Example 1 Using the "Is" Operator

On the Media – Overview screen, using the "Is" operator to filter for the LTO6-Drives-Media logical group selects no records. This is because all media in the LTO6-Drives-Media group also belong to at least one other group.

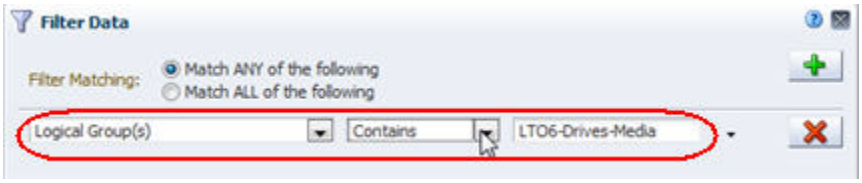
The "Is" operator selects only drives and media that belong exclusively to the specified logical groups. If the drives and media belong to any other groups as well, they are not selected by the filter.

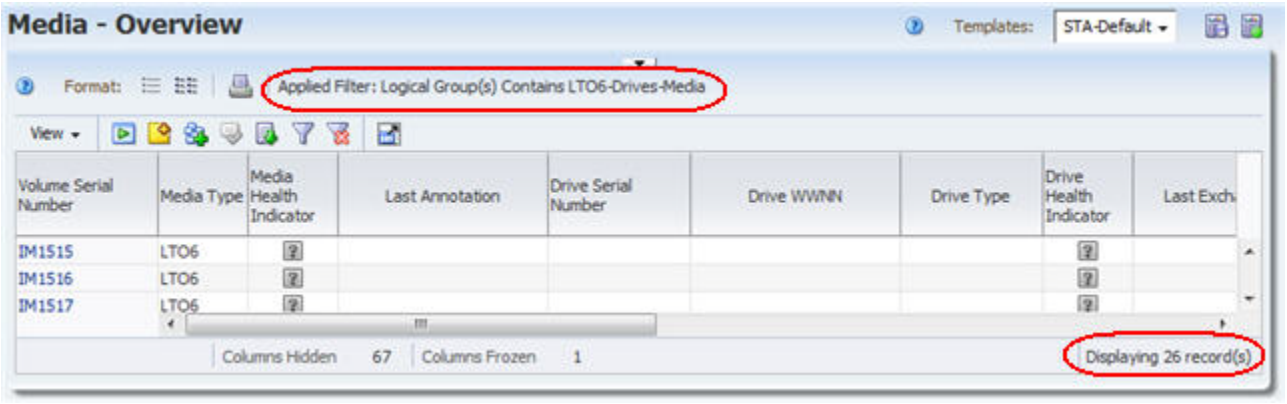




Example 2 Using the "Contains" Operator

Changing the filter operator to "Contains" selects all 26 media records in the logical group. The "Contains" operator selects drives and media that belong to the specified logical groups, as well as any number of other groups.



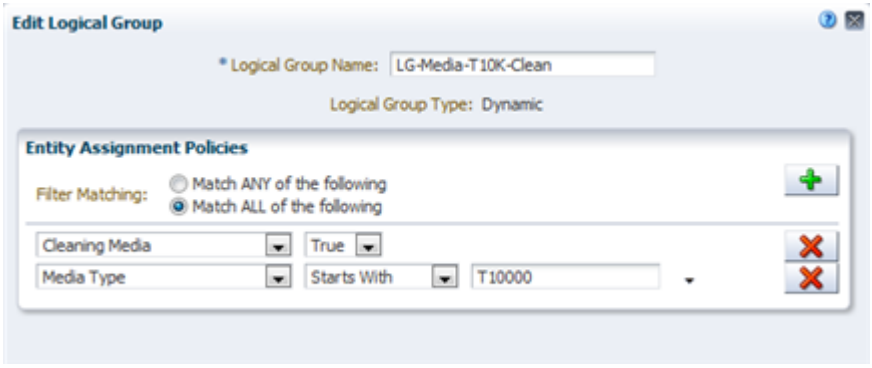


How Changes to Logical Group Definitions Can Affect Filters

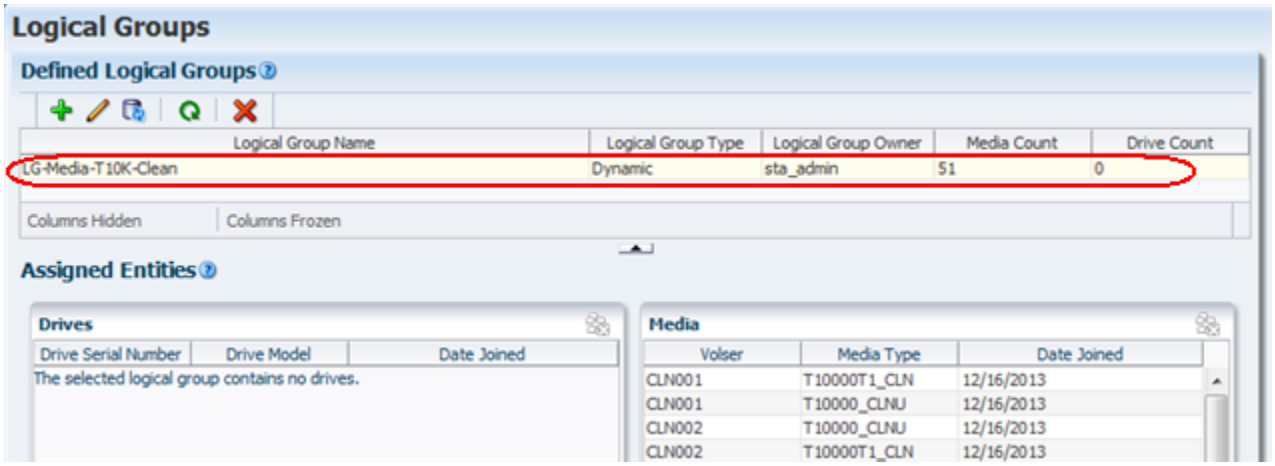
If a filter includes a logical group as part of its selection criteria, modifications to the definition of the logical group affect the behavior of the filter. The following example provides a step-by-step illustration of changes you might see.

Step 1 Define the Logical Group

On the Logical Groups screen, dynamic logical group "LG-Media-T10K-Clean," is created for all T10000 cleaning media. The group has the following definition.

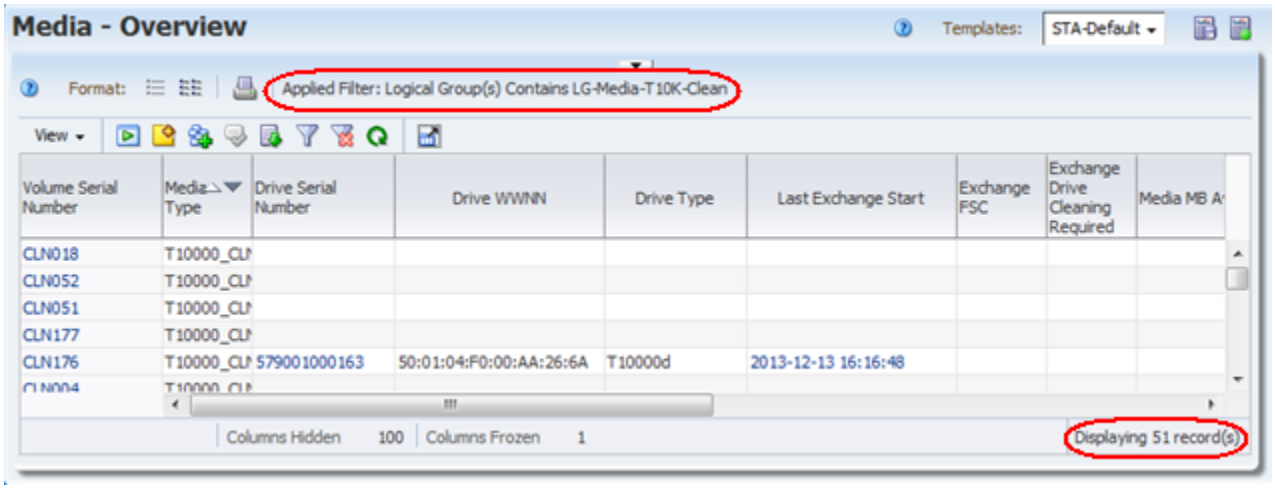


There are 51 media included in the logical group.



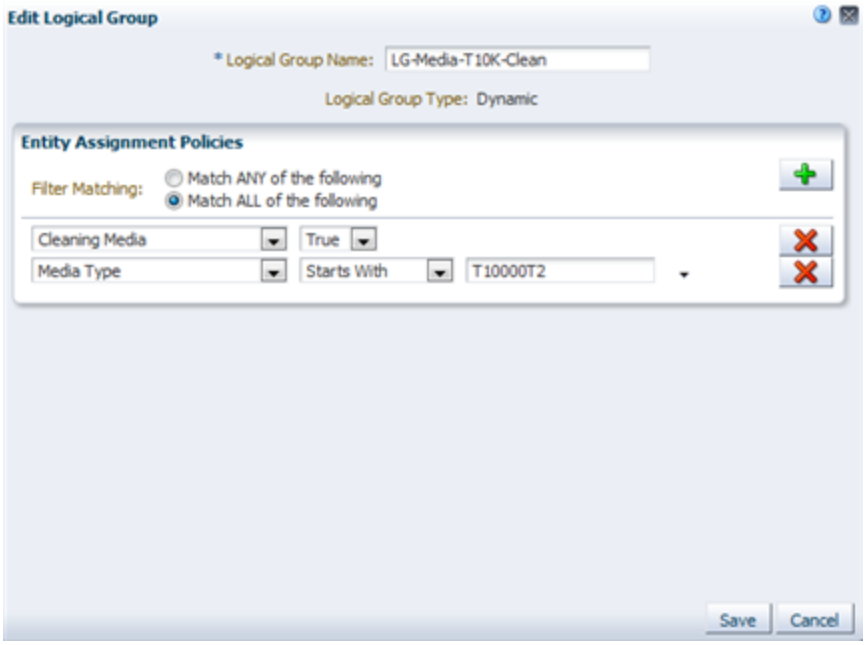
Step 2 Use the Logical Group in a Filter

The Media – Overview screen is filtered by this logical group. The 51 records included in the group are displayed.

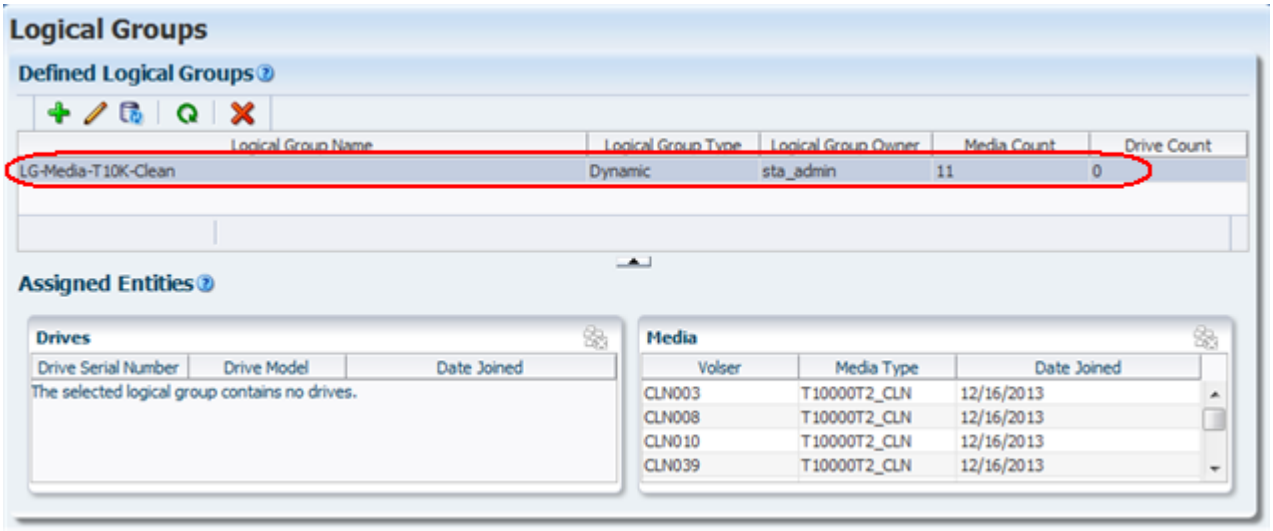


Step 3 Effects of Modifying the Logical Group Selection Criteria

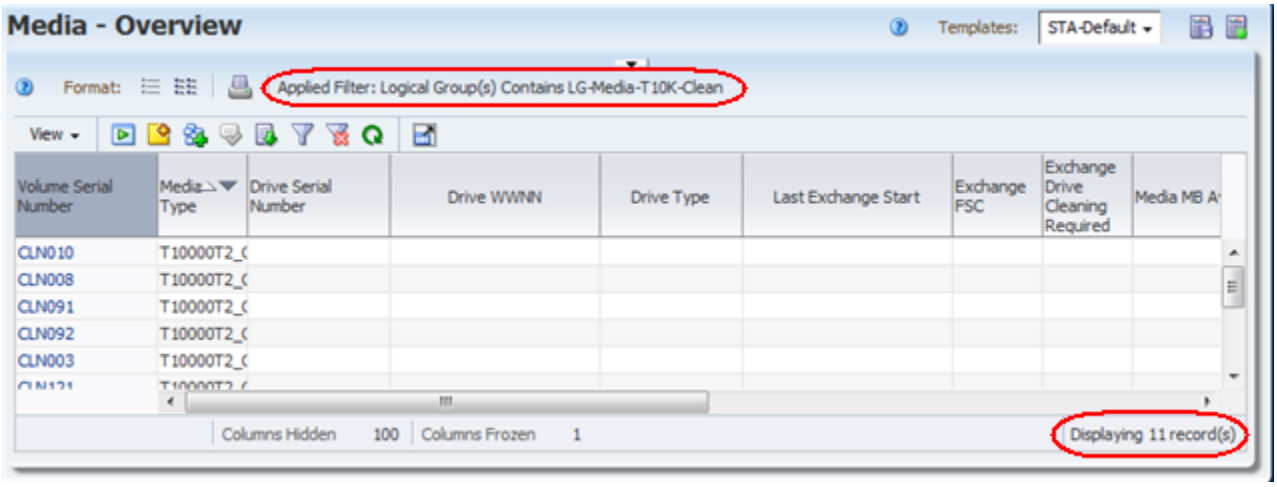
On the Logical Groups screen, the logical group definition is modified to include T10000T2 cleaning media only.



There are now just 11 media in the logical group.

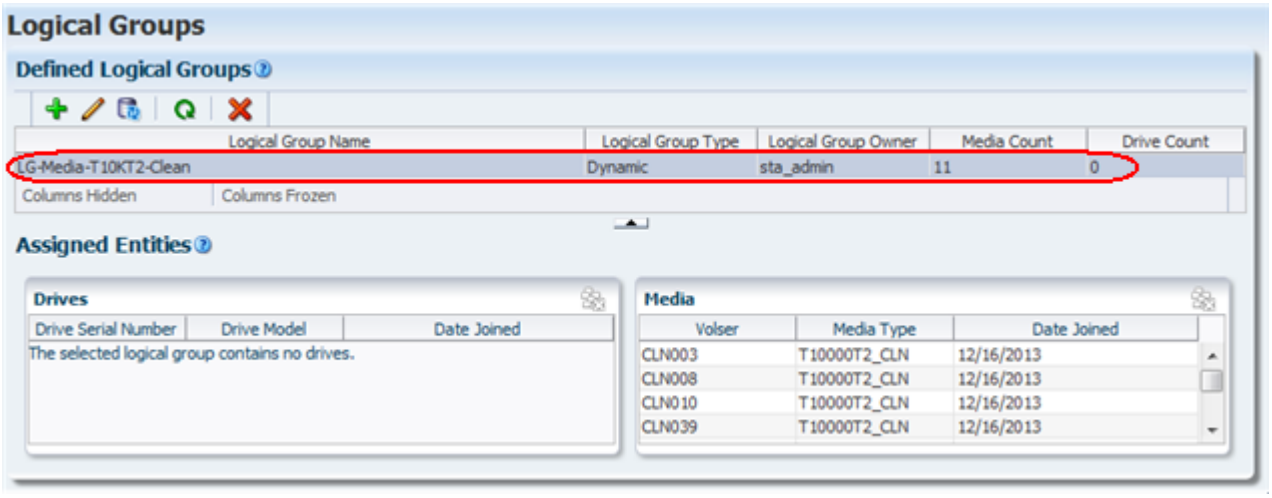


The Media – Overview screen is automatically updated to reflect the new logical group definition included in the applied filter.

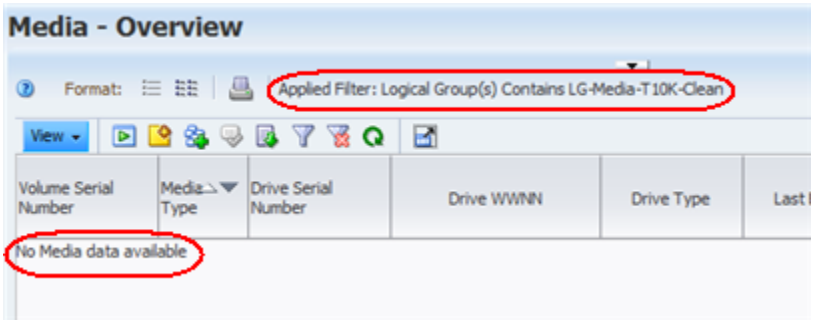


Step 4 Effects of Changing the Name of the Logical Group

On the Logical Groups screen, the name of the logical group is changed to "LG-Media-T10KT2-Clean." The logical group selection criteria remain the same, and the group still includes the same 11 media.



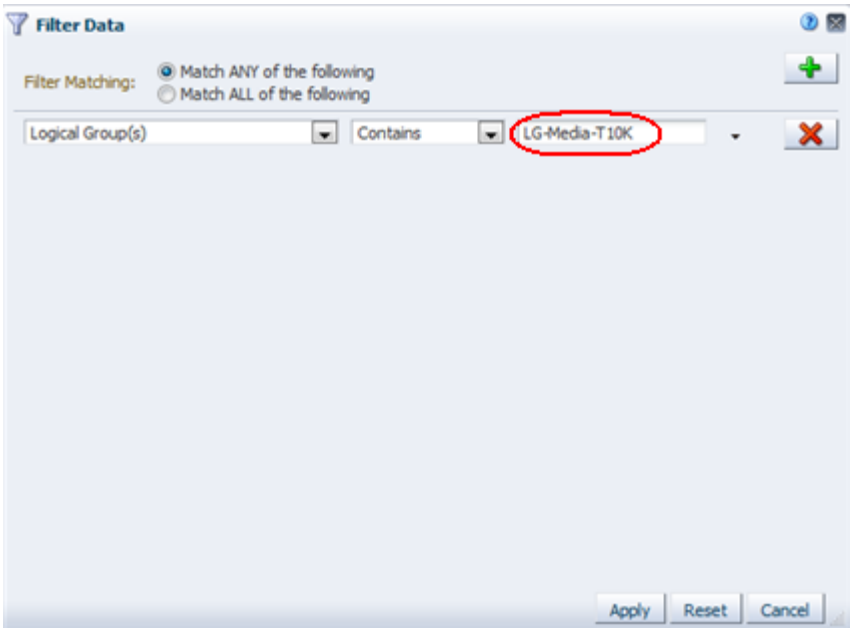
Because the old logical group name is still used in the filter applied to the Media – Overview screen, the screen now displays no records. The filter specifies a logical group name that no longer exists.



Step 5 Update the Filter

The filter must be updated, either to include the new logical group name in the selection criteria or to make the selection criteria more broad. In the example below,

the selection criteria are made more broad by specifying just a portion of the logical group name to match. If the filter were included in a template, the template would also need to be updated and re-saved.



Dashboard Portlets With Filtering by Logical Group

You can filter the following Dashboard portlets by logical group. See "Dashboard Portlets" on page A-1for descriptions.

Graph Portlets

- Drive Health
- Drive Utilization
- I/O Throughput
- Library Drive Bays
- Library Media Slots
- Maximum Mount Times
- Media Health
- Mounts

Table Portlets

- Drives Requiring the Most Cleanings Per Meter
- Drives Watch List
- Media Watch List
- Monitored Device Trends

Report Portlets

- Data Read Report
- Data Written Report
- Drives Health Report

- Media Health Report
- Monitored Device Counts

Best Practices for Logical Groups

This section provides tips for creating and managing logical groups.

Create an example
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.

Logical group names
Make logical group names meaningful and easy to distinguish so you can remember the purpose of the group.

Logical groups and the "Contains" operator
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 "Constructing Filters Using Logical Groups" on page 7-5.

Logical Group Creation and Management Tasks

All tasks in this section require Operator or Administrator privileges.

Manual Logical Groups Only

- "Create a Manual Logical Group" on page 7-11
- "Add Drives and Media to a Manual Logical Group" on page 7-13
- "Remove Drives and Media From a Manual Logical Group" on page 7-15

Dynamic Logical Groups Only

- "Create and Define a Dynamic Logical Group" on page 7-17
- "Change the Selection Criteria for a Dynamic Logical Group" on page 7-21
- "Force a Dynamic Logical Group Update" on page 7-22

All Logical Groups

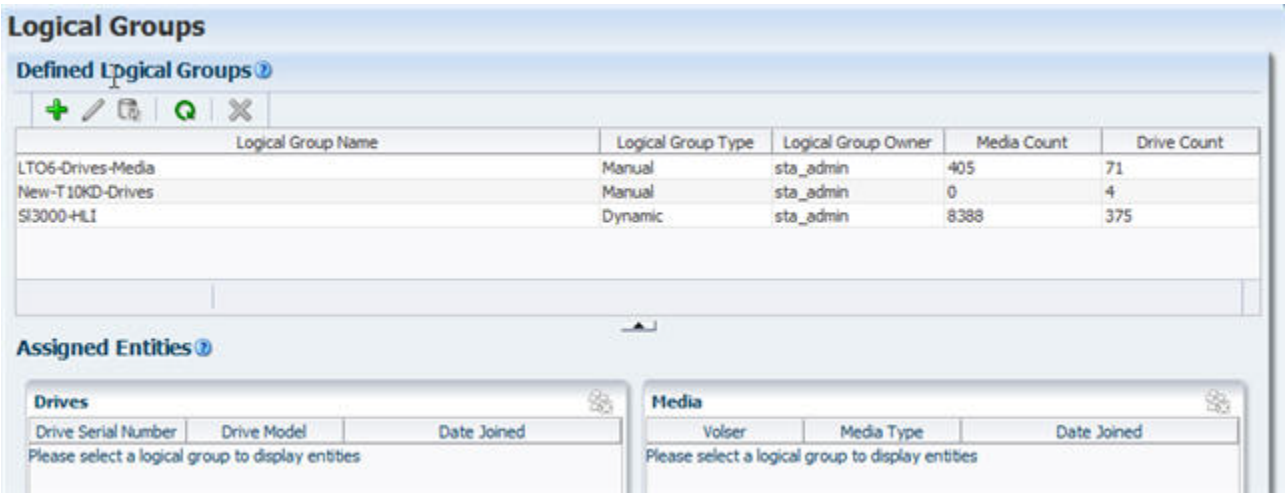
- "View Logical Group Assignments for Selected Drives or Media" on page 7-23
- "List All Drives and Media Assigned to a Logical Group" on page 7-24
- "Rename a Logical Group" on page 7-25
- "Delete a Logical Group" on page 7-27

Create a Manual Logical Group

Use this procedure to create a manual logical group.

1. In the Navigation Bar, select **Setup & Administration**, then select **Logical Groups**.

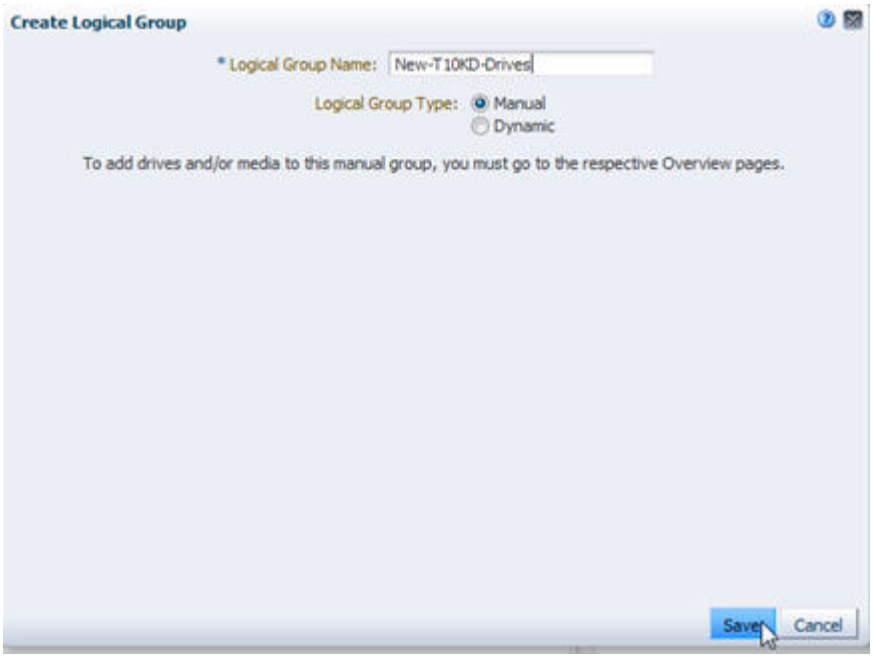
The Logical Groups screen appears.



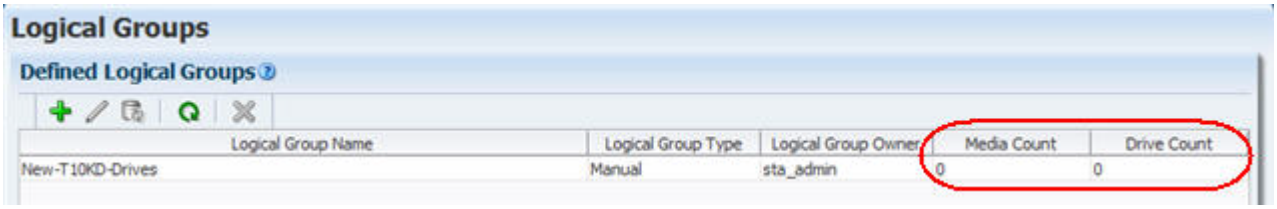
2. Click **Add Logical Group** in the Defined Logical Groups toolbar.

3. Complete the Create Logical Group screen as follows:
   a. In the **Logical Group Name** field, type a unique name.

      Your entry can include a maximum of 249 alphanumeric characters.
   b. In the **Logical Group Type** field, select **Manual**.
   c. Click **Save**.



The group is created and is added to the Defined Logical Groups table. For now the group is empty. See "Add Drives and Media to a Manual Logical Group" on page 7-13 for details on adding resources to the group.



Add Drives and Media to a Manual Logical Group

Use this procedure to add drives, media, or both to an existing manual logical group. You can add drives or media one at a time, or you can select multiple resources and add them all at once.

Note: The logical group must already exist. See "Create a Manual Logical Group" on page 7-11 for instructions.

Note: Removing drives and media from a logical group is done on the Logical Groups screen. See "Remove Drives and Media From a Manual Logical Group" on page 7-15 for instructions.

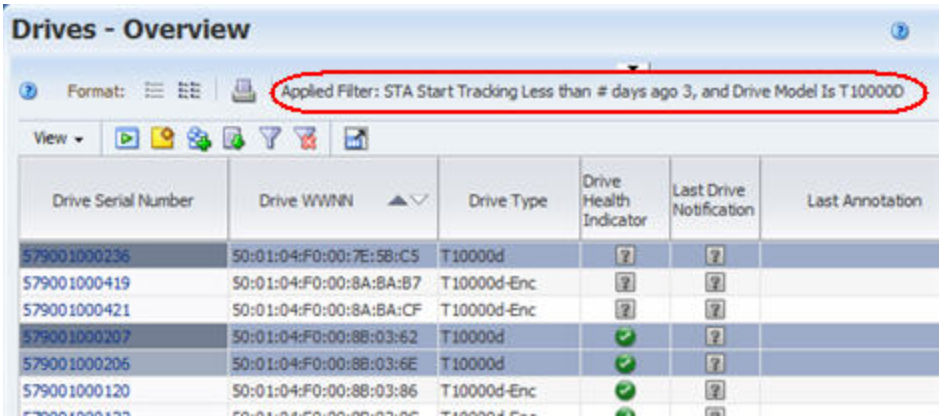
Note: You cannot add drives or media to a dynamic logical group. To change the membership of a dynamic group, see "Change the Selection Criteria for a Dynamic Logical Group" on page 7-21.

1. Go to the appropriate Overview screen, as follows:

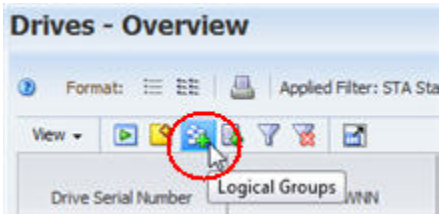
- To add drives to the logical group, select **Tape System Hardware**, then select **Drives – Overview** in the Navigation Bar.
- To add media to the logical group, select **Tape System Hardware**, then select **Media – Overview** in the Navigation Bar.

2. On the selected screen (Drives – Overview in this example), select the drives or media you want to add to the logical group.

   Optionally, you can apply a filter to the screen to narrow down the choices. The example below shows individual drives selected from a filtered list.



3. Click **Logical Groups** in the table toolbar.



   The Logical Groups dialog box appears.

4. In the menu, select the logical group to which you want to add the selected drives or media, and then click **OK**.

Note: The menu displays manual logical groups only.

The resources are added to the logical group. See "List All Drives and Media Assigned to a Logical Group" on page 7-24 to confirm the update.

5. Optionally, you can add additional resources to the group as follows:
   - To add additional resources of the same type (in this example, drives), stay on the current Overview screen and return to Step 2.
   - To add resources of the other type (in this example, media), return to Step 1 and select the corresponding Overview screen.

Remove Drives and Media From a Manual Logical Group

Use this procedure to remove selected drives, media, or both from a manual logical group.

Note: Adding drives and media to a logical group is done on the respective Overview screens. See "Add Drives and Media to a Manual Logical Group" on page 7-13 for instructions.

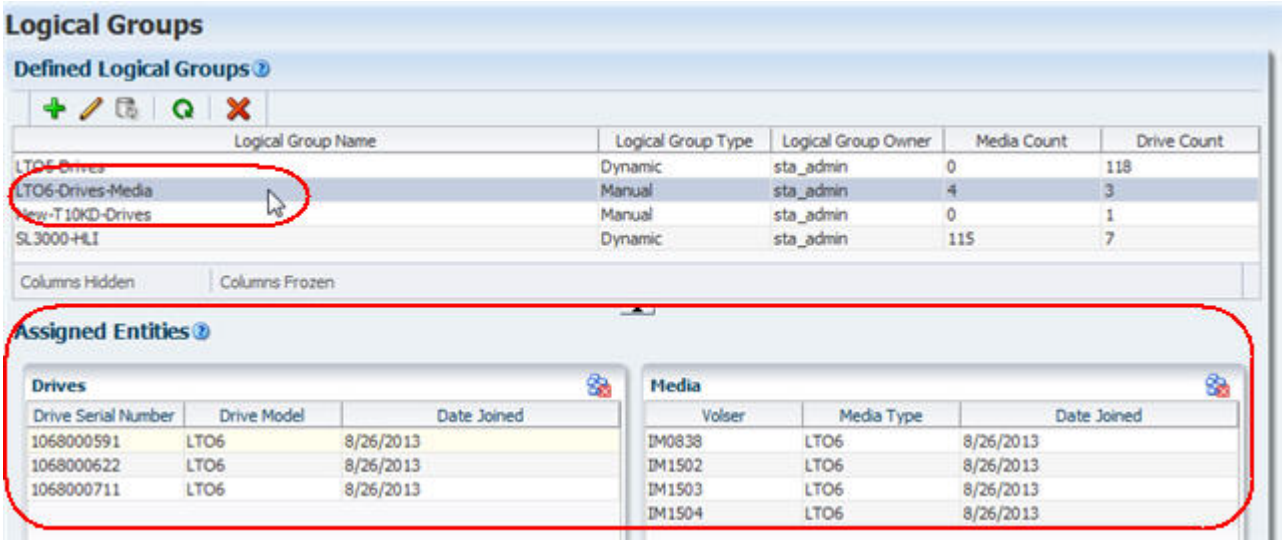
Note: You cannot delete drives or media from a dynamic logical group. To change the membership of a dynamic group, see "Change the Selection Criteria for a Dynamic Logical Group" on page 7-21.

1. In the Navigation Bar, select **Setup & Administration**, then select **Logical Groups**.

The Logical Groups screen appears.

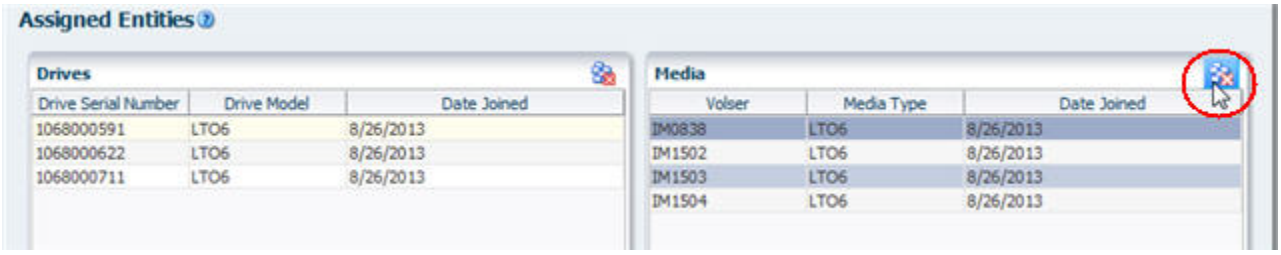
2. In the Defined Logical Groups table, select the manual logical group you want to modify.

   The drives and media assigned to the group are displayed in the Assigned Entities table.



3. In the Drives or Media table, select the resources 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.

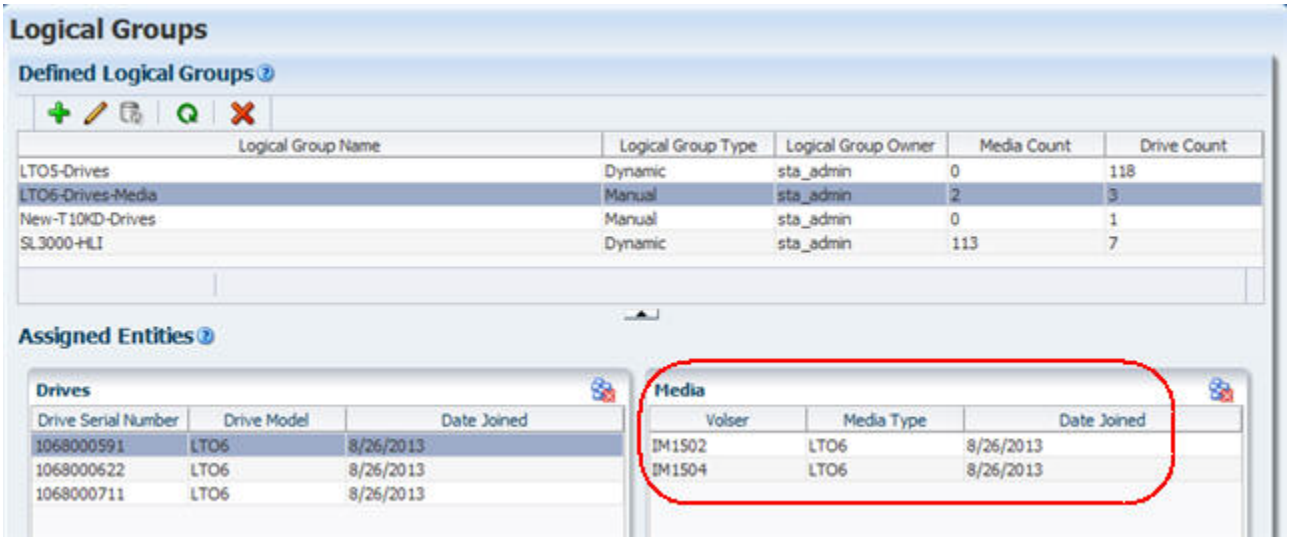
Note: The **Unassign Entities** button does not activate for dynamic logical groups. If the button is not activated, check to be sure you have selected a manual logical group.



The Unassign Entities dialog box appears.

4. Verify that you have specified the correct information and click **Yes**.

The selected resources are removed from the group, and the Assigned Entities table is updated.



5. To remove additional drives or media from the group, return to Step 3.

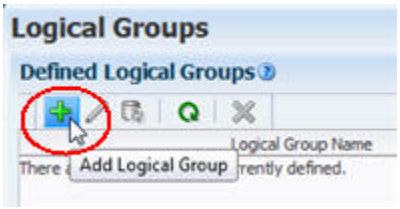
Create and Define a Dynamic Logical Group

Use this procedure to create a dynamic logical group and define the selection criteria that determine which drives and media are assigned to the group.

1. In the Navigation Bar, select **Setup & Administration**, then select **Logical Groups**.

The Logical Groups screen appears.

2. Click **Add Logical Group** in the Defined Logical Groups toolbar.



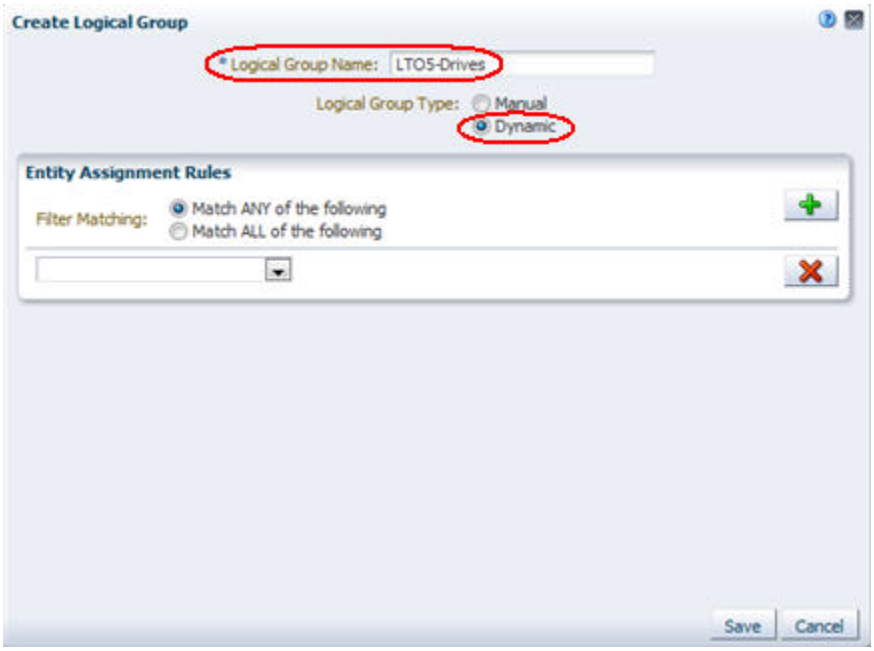
3. Complete the Create Logical Groups dialog box as follows:

   a. In the **Logical Group Name** field, type a unique name.

      Your entry can include any alphanumeric characters up to 250 characters in length.

   b. In the **Logical Group Type** field, select **Dynamic**.

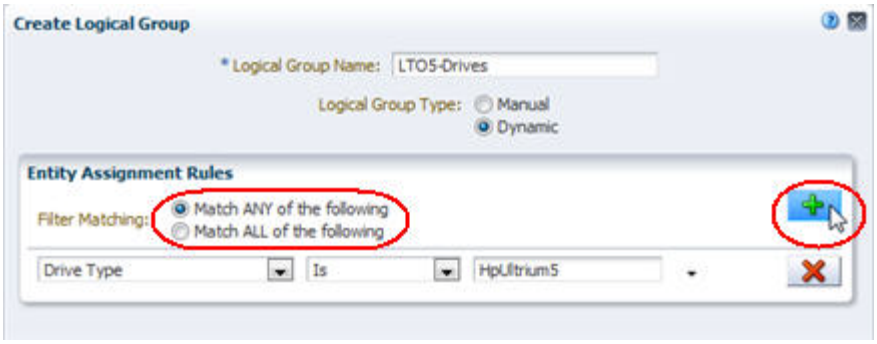
      The Entity Assignment Policies appear in the dialog box.



4. Specify the selection criteria as follows.

   a. In the **Filter Matching** field, indicate whether you want to match any or all of the criteria you specify.

   b. Click the **Add New Filter Criteria Row** button to add a new, blank selection criteria row to the dialog box.



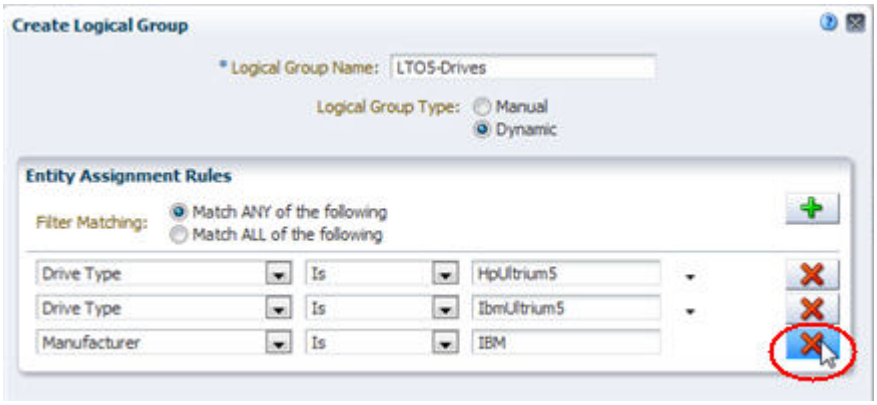
   c. Specify the selection criteria using the menus and text fields on the row. See "Filter Operators by Attribute Type" on page 4-3 for details on filling out each row.

Note: When selecting an attribute for filtering, if you know the name of the attribute you want to select, you can type the first few letters to quickly move the cursor to that item in the menu.

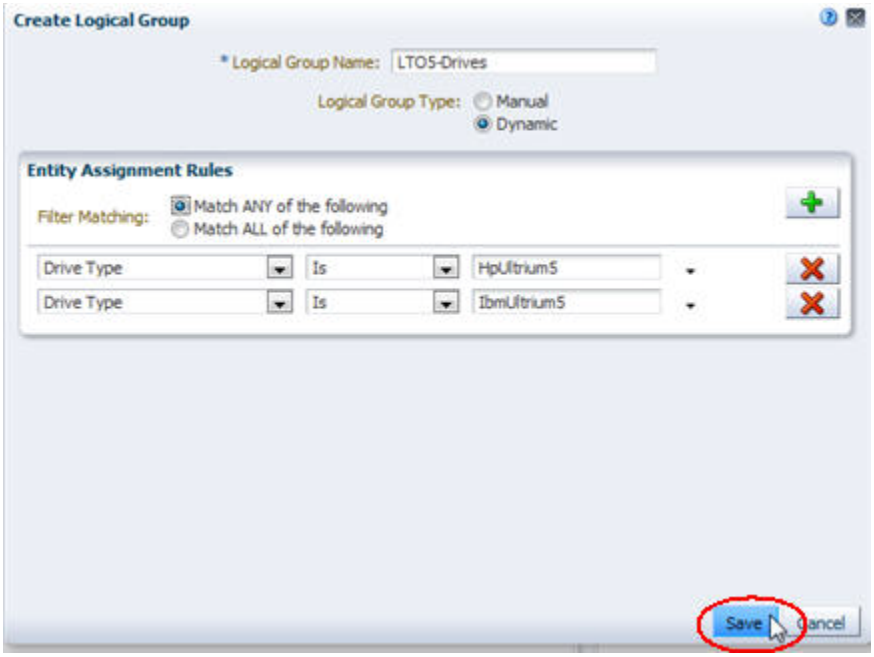
---

   d. You can add as many rows of selection criteria as you want.

   e. To remove criteria, click the **Remove This Filter Criteria Row** button on the row you want to delete.

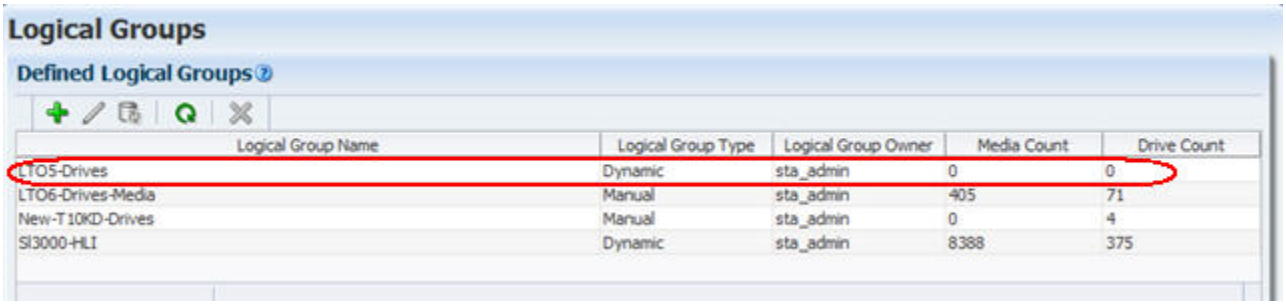


5. Verify that your criteria are correct and click **Save**.

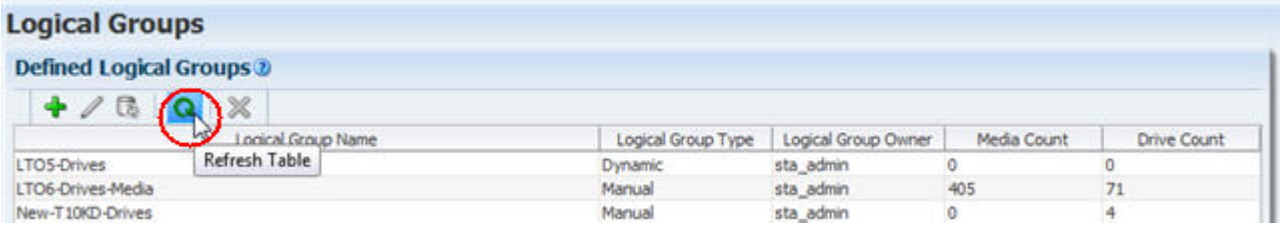


The group is created and added to the Defined Logical Groups table, and STA begins building the group in the background.

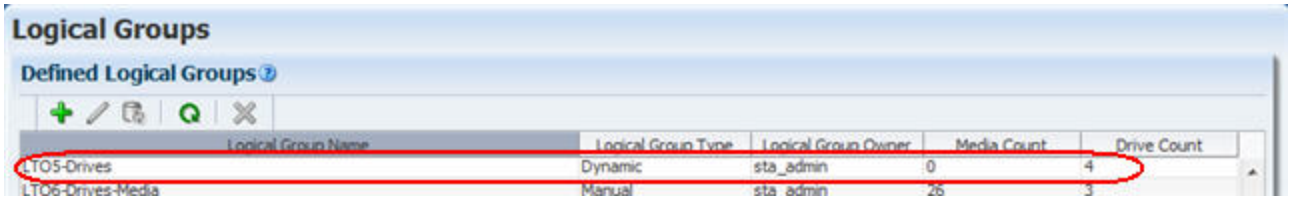
Initially, the media and drive counts for the group are displayed as zero. Depending on the size of your tape library system and the complexity of your selection criteria, it may take from a few seconds to many minutes for all qualifying drives and media to be added to the group. Leaving the Logical Groups screen does not interrupt this process.



6. As the logical group is built, you can click the **Refresh Table** icon to update the screen display with the in-progress drive and media counts.



The display is updated.



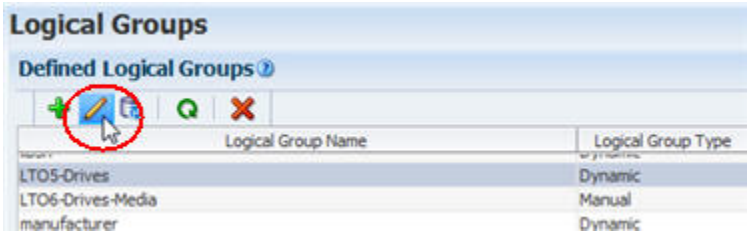
Change the Selection Criteria for a Dynamic Logical Group

Use this procedure to change the selection criteria for an existing dynamic logical group.

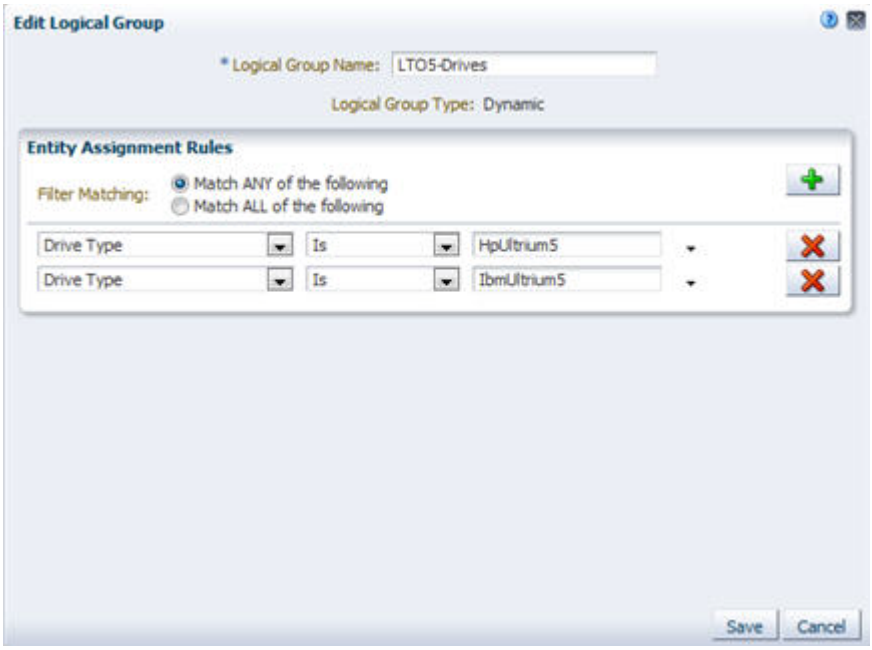
1. In the Navigation Bar, select **Setup & Administration**, then select **Logical Groups**.

   The Logical Groups screen appears.

2. In the Defined Logical Groups table, select the dynamic logical group you want to modify and click **Edit Logical Group**.



   The Edit Logical Group dialog box appears, and the group's selection criteria are displayed.



3. You can add, delete, and modify selection criteria as necessary. See "Create and Define a Dynamic Logical Group" on page 7-17 for instructions.

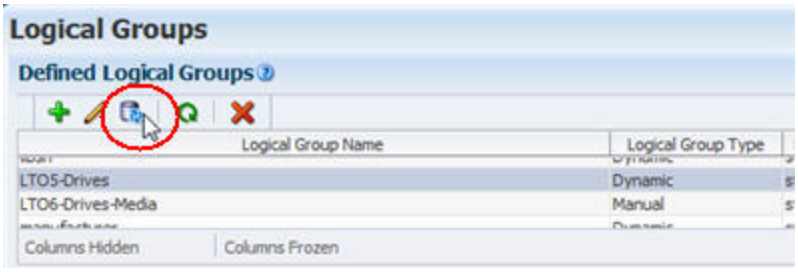
Force a Dynamic Logical Group Update

Use this procedure to initiate an immediate update of a dynamic logical group to reflect any changes in the qualifying drives or media. Dynamic groups are updated automatically every hour, but you can use this procedure to update groups between update cycles.

1. In the Navigation Bar, select **Setup & Administration**, then select **Logical Groups**.

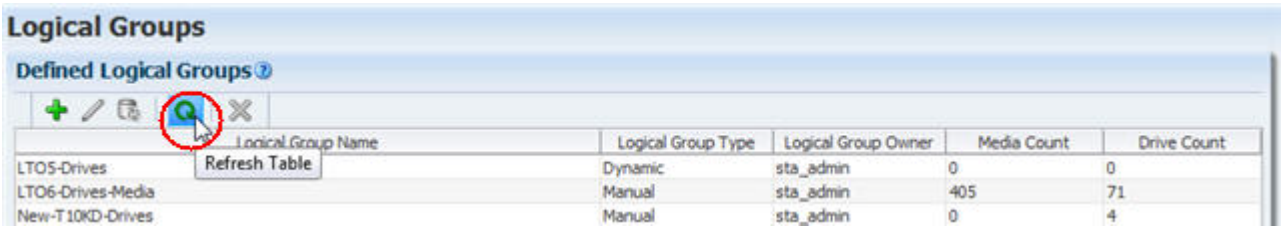
The Logical Groups screen appears.

2. In the Defined Logical Groups table, select the dynamic logical group you want to update and click **Refresh Dynamic Group**.



STA begins updating the group in the background. Depending on the size of your tape library system and the complexity of your selection criteria, it may take from a few seconds to many minutes for the update to complete. Leaving the Logical Groups screen does not interrupt this process.

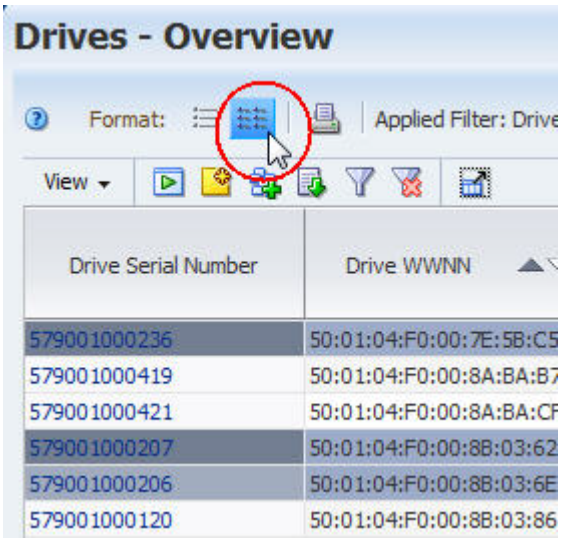
3. As the group is updated, you can click the **Refresh Table** button to update the screen display with the in-progress drive and media counts.



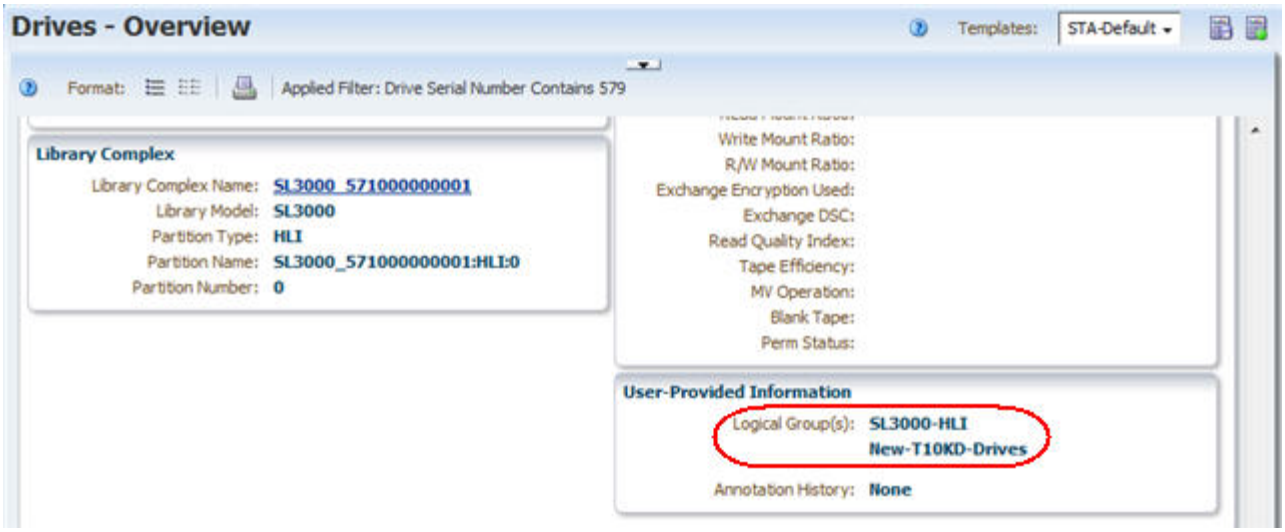
View Logical Group Assignments for Selected Drives or Media

Use this procedure to view the logical groups to which selected drives or media have been assigned.

1. From the Drives – Overview or Media – Overview screen, select the records you want to display, and click **Detail View**.



In the Detail View for each record you have selected, the logical group assignments are listed in the User-Provided Information section at the bottom of the display. All groups to which the resource is assigned are listed.



List All Drives and Media Assigned to a Logical Group

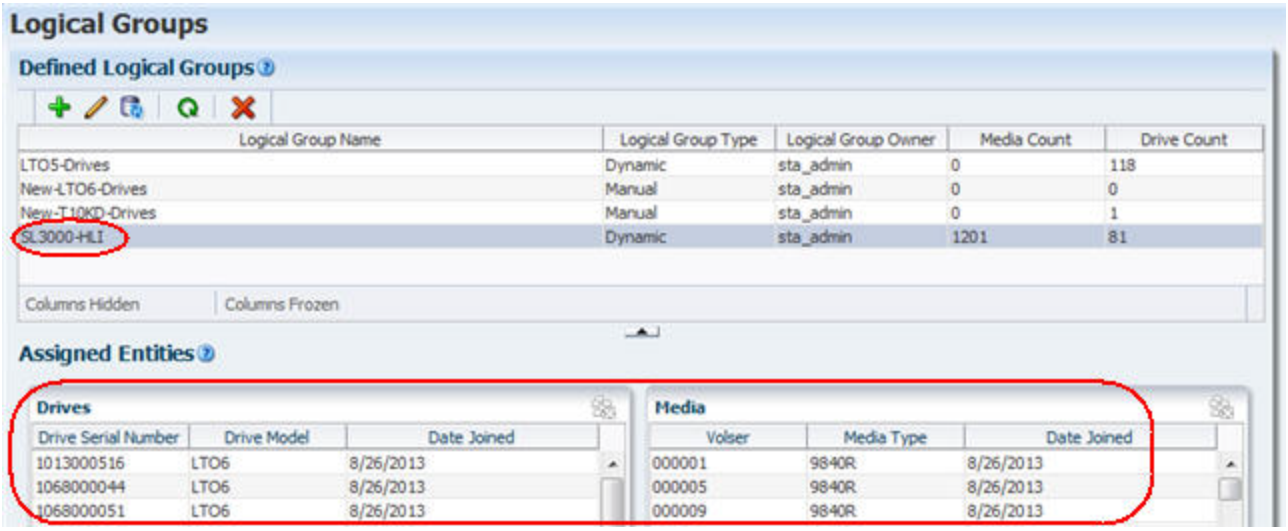
Use this procedure to display a list of all drives and media assigned to a selected logical group.

1. In the Navigation Bar, select **Setup & Administration**, then select **Logical Groups**.

   The Logical Groups screen appears.

2. In the Defined Logical Groups table, select the logical group you want to display.

   All assigned drives and media are displayed in the Assigned Entities table.



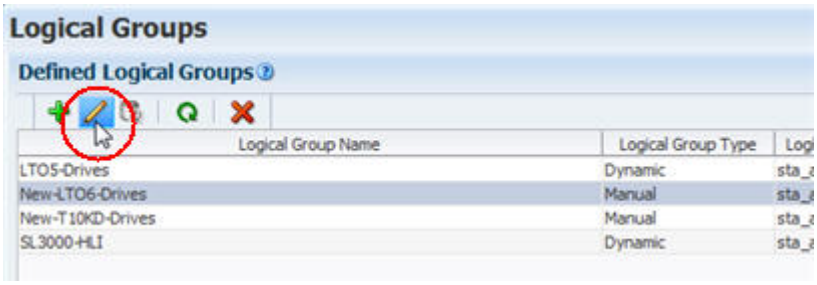
Rename a Logical Group

Use this procedure to change the name of an existing manual or dynamic logical group.

1. In the Navigation Bar, select **Setup & Administration**, then select **Logical Groups**.

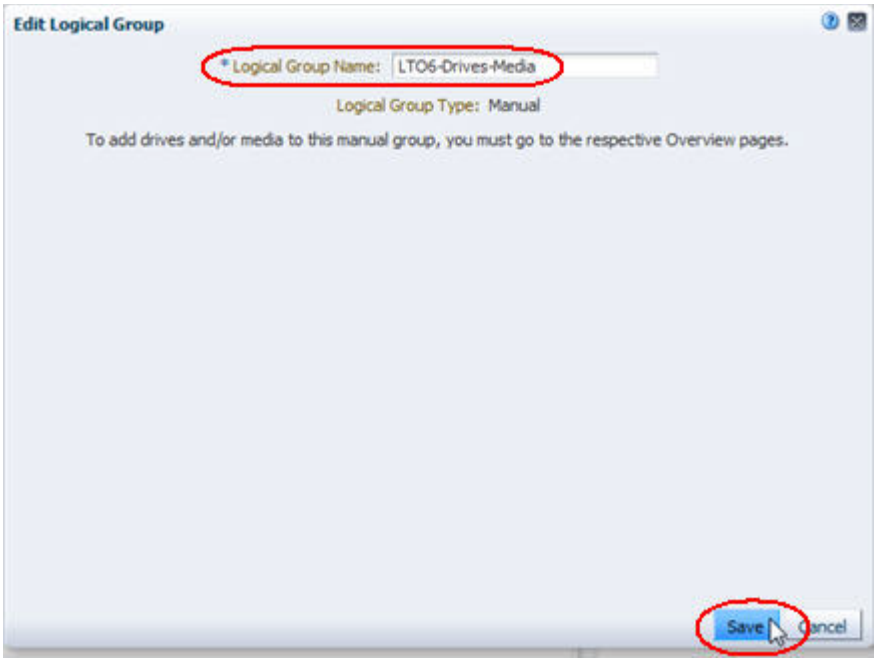
The Logical Groups screen appears.

2. In the Defined Logical Groups table, select the group you want to rename, and then click **Edit Logical Group**.



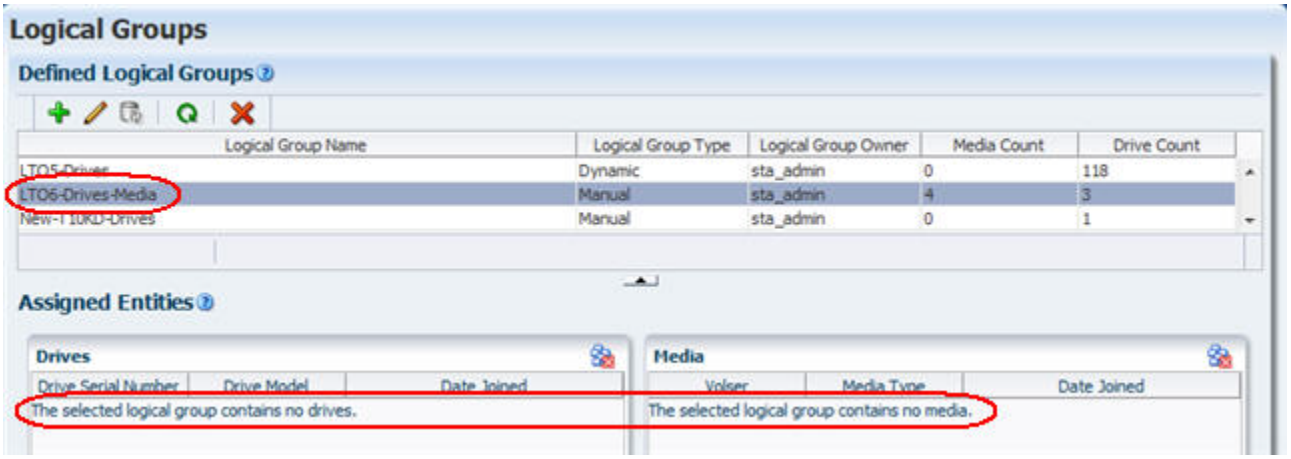
The Edit Logical Groups dialog box appears.

3. Type the new name in the Logical Group Name field, and then click **Save**. For dynamic logical groups, do not modify any other fields. For manual logical groups, this is the only field available.

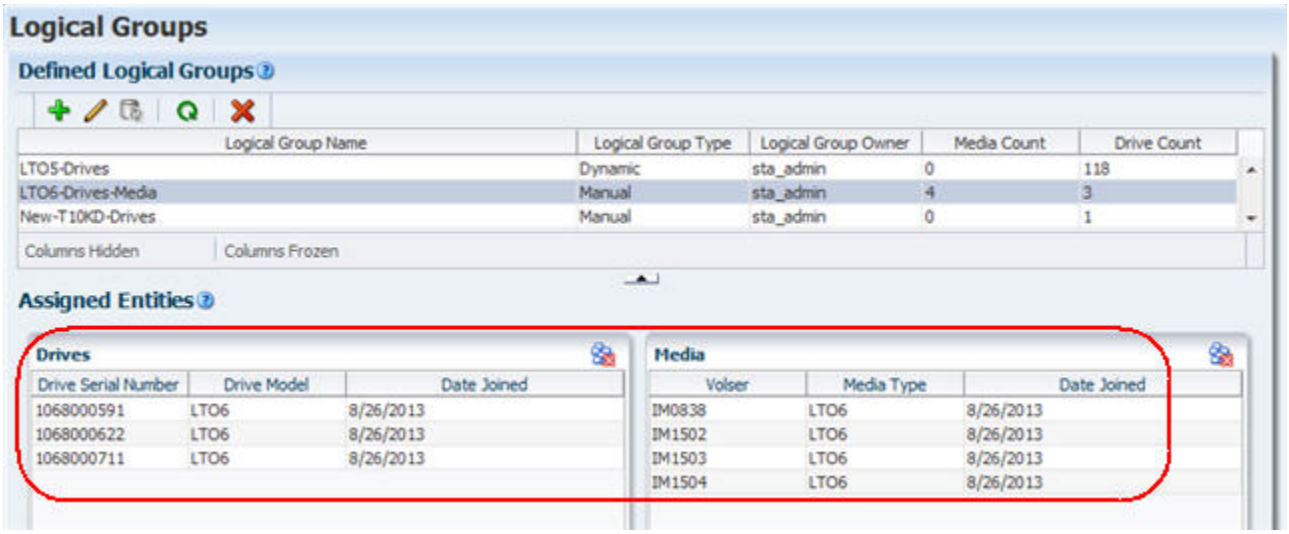


The Defined Logical Groups table is updated with the new name.

Note: The Assigned Entities table indicates the group contains no drives nor media. This is just lag in the table display.



4. To update the Assigned Entities table display, in the Defined Logical Groups table, deselect the logical group and then re-select it. The display is updated with the assigned drives and media.



Delete a Logical Group

Use this procedure to delete a selected manual or dynamic logical group. You can delete only one logical group at a time.

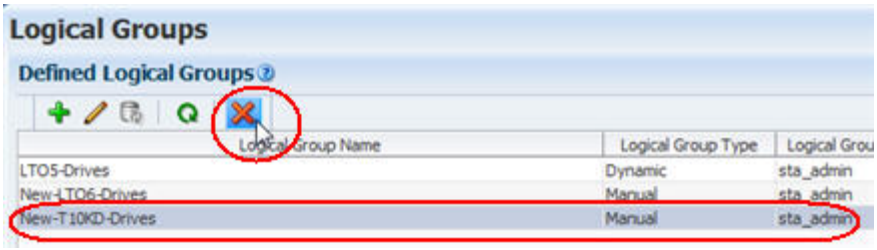
Note: This procedure deletes the entire logical group. To delete just selected drives or media from a manual group, see "Remove Drives and Media From a Manual Logical Group" on page 7-15.

---

1. In the Navigation Bar, select **Setup & Administration**, then select **Logical Groups**.

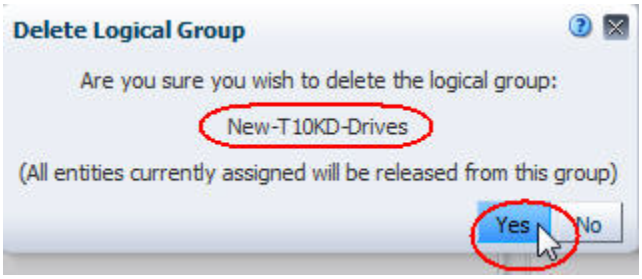
   The Logical Groups screen appears.

2. In the Defined Logical Groups table, select the group you want to delete, and then click **Delete Logical Group**.

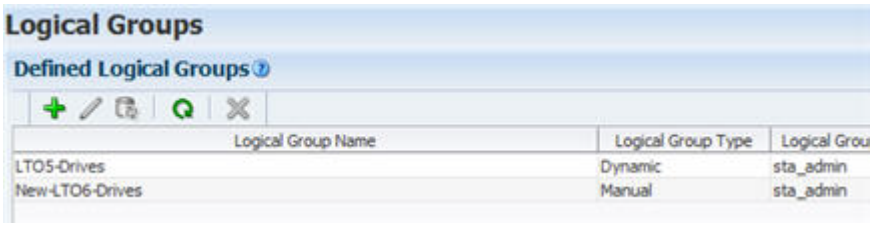


The Delete Logical Group dialog box appears.

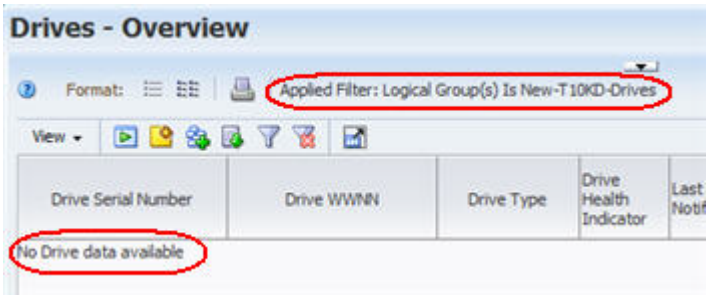
3. Verify that you have selected the correct logical group, and then click **Yes** to delete.



The group is deleted and removed from the Logical Groups screen.



Any screens, Dashboard portlets, or templates filtered by the group now show "No data to display" or "No data available."



8

STA Media Validation

STA media validation is an optional STA feature that helps to ensure long-term preservation of the data in your tape library system. It provides automated, policy-driven validation of production media in StorageTek SL300 and SL8500 libraries, using the data integrity checking capabilities of Oracle's StorageTek T10000C and T10000D drives. STA analyzes the validation results and makes recommendations for preserving your data.

> **Note:** STA media validation is supported only for tape library system configurations meeting the minimum requirements. See the *STA Requirements Guide* for a list of STA, library, drive, and media requirements.

This chapter includes the following topics:

- Overview of STA Media Validation
- Configuring STA Media Validation
- Drive Calibration and Qualification
- Submitting Manual Validation Requests
- Using Automated Media Validation
- Managing the STA Media Validation Request Queue
- User Roles for Media Validation
- Best Practices for Media Validation
- Media Validation Tasks

Overview of STA Media Validation

This section includes the following topics:

- "Features and Benefits of STA Media Validation" on page 8-2
- "Feature Comparison for STA and SL Console" on page 8-3
- "Types of Verification Tests" on page 8-3

Features and Benefits of STA Media Validation

With STA, you can use one user interface to automate and manage media validation activities across all SL3000 and SL8500 libraries in your tape library system. This section summarizes the advantages of STA media validation.

Increased Security With Reduced Cost and Complexity

STA media validation is done internally by the T10000C and T10000D 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. See "Drive Calibration and Qualification" on page 8-10 for details.

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 a compatible drive.

STA can initiate and process multiple validations simultaneously, depending on the number of drives you have set aside for validation activities. See "Using Automated Media Validation" on page 8-19 for details.

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. See "Managing the STA Media Validation Request Queue" on page 8-21 for details.

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 SL Console and Oracle's StorageTek Storage Archive Manager (SAM). STA analyzes validation results and makes recommendations for action you should take. See "Displaying the Status of Validation Requests" on page 8-21 for details.

Feature Comparison for STA and SL Console

Table 8–1 compares the media validation features available through STA and SL Console. An "X" in the column indicates the feature is supported by that product.

Table 8–1 Media Validation Feature Comparison for STA and SL Console

Feature	STA	SL Console
Configure the validation drive pool.		X
Support all T10000C and T10000D 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	
Display Dashboard summaries of validation activity on a PC or mobile device	X	
Receive emailed Executive Reports summaries of validation activity	X	

Types of Verification Tests

The T10000C and T10000D drives perform the following media validation tests, all of which are available through STA. When you define a media validation policy or initiate a manual media validation, you indicate which type of test to perform. See "Submit Manual Media Validation Requests" on page 8-39 and "Create a Media Validation Policy" on page 8-53 for instructions.

Basic Verify

Verifies that the media is mountable and the media information record (MIR) is valid. The drive simply mounts the media and validates the MIR. This validation detects whether the MIR is unreadable or out of sync and updates the following data attributes for the media:

- Exchange Recording Technique (recording format used by the drive to write to the media)
- Media Suspicion Level
- MB Written (total amount of data written to the media)

> **Note:** To be used by STA for policy-driven validation, media must have this information at a minimum. See "Media Eligible for Automated Validation" on page 8-20 for details.

This method takes approximately two minutes.

Standard Verify

Verifies that the highest-priority areas of the media are readable. The drive verifies records at 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 method typically takes a maximum of 30 minutes, regardless of the amount of data and the compression ratio used.

This test is not valid for blank tapes.

Complete Verify

Verifies that all data records on the media are readable. The drive does a record-by-record verification with no decompression nor decryption.

By default, the validation starting point is the beginning of tape (BOT). For T10000T2 media, you can optionally choose to resume validation from the last verified location, as indicated by the media RFID chip; validations of T10000T1 media must always start at the BOT.

The drive validates data at maximum tape velocity, regardless of the compression ratio used on the media. This method may take approximately five to nine hours, depending on the starting point, the amount of data on the media, and the drive type.

This test is not valid for blank tapes.

Complete Verify Plus

Verifies that all data records on the media are readable, including StorageTek Data Integrity Validation (DIV) checking. If the data records on the media include DIV cyclic redundancy check (CRC) codes added by the host, the data is decompressed and decrypted. Consequently, this test requires the validation drive to be encryption capable and connected to an Oracle Key Manager (OKM). This test is not valid for drives configured with a FICON interface.

By default, the validation starting point is the beginning of tape (BOT). For T10000T2 media, you can optionally choose to resume validation from the last verified location, as indicated by the media RFID chip; validations of T10000T1 media must always start at the BOT.

This method may take approximately five to nine hours, depending on the starting point, the amount of data on the media, the drive type, and the compression ratio.

This test is not valid for blank tapes.

Verify and Rebuild MIR
Verifies the MIR and rebuilds it if necessary. The drive first verifies the MIR. If there are errors, the drive finds the last known-good spot on the MIR, then does a high-speed locate to that point on the tape. The drive 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 gather the information necessary to rebuild the MIR, and then rebuilds it. Records are not decompressed nor decrypted.

You should use this method if there is a corrupt MIR on an exchange.

The drive reads the data at maximum tape velocity. This method may take approximately five to nine hours, depending on the starting point, the amount of data on the media, and the drive type. This is significantly faster than rebuilding the MIR with the drive Virtual Operator Panel (VOP).

Configuring STA Media Validation

This section includes the following topics:

- "Preparing for STA Media Validation" on page 8-5
- "Validation Drive Pools" on page 8-6
- "Enabling Media Validation" on page 8-8
- "Disabling Media Validation" on page 8-10

Preparing for STA Media Validation

Before enabling media validation on STA, you should perform the following preparation steps.

1. Determine the library complexes and standalone libraries in which you want to implement media validation.
2. On the STA Drives – Overview screen, review and choose drives in these libraries that you want to use for media validation. See "Validation Drive Pools" on page 8-6 for details.
3. Use SL Console to add the drives to the validation pools. You must log in to SL Console on the selected standalone library or a library that is part of the selected complex. See the library *User's Guide* for details.
4. Decide whether you want to use drive calibration and qualification, and if so, create the calibration media logical group. See "Drive Calibration and Qualification" on page 8-10 for details.

Note: Some of these steps may require Administrator privileges. See "User Roles for Media Validation" on page 8-25 for details.

Validation Drive Pools

> **Note:** The validation drive pools are maintained only through SL Console. See the library *User's Guide* for detailed instructions on maintaining the pools.

Validation drives are drives that have been set aside exclusively for the time-being for media validation. These drives are not accessible to host applications. They must be assigned to a media validation drive pool through the SL Console.

Each SL8500 library complex and standalone SL3000 or SL8500 library has its own validation drive pool, and up to ten drives can be assigned to each pool. You must assign at least one drive per library complex or standalone library in which you want to validate media. If you will be validating encrypted media, in each applicable library you must assign at least one drive that has been enabled for encryption and connected to an Oracle Key Manager (OKM).

> **Note:** You may have only one validation drive at your site, in which case any media to be validated must be moved to that library.

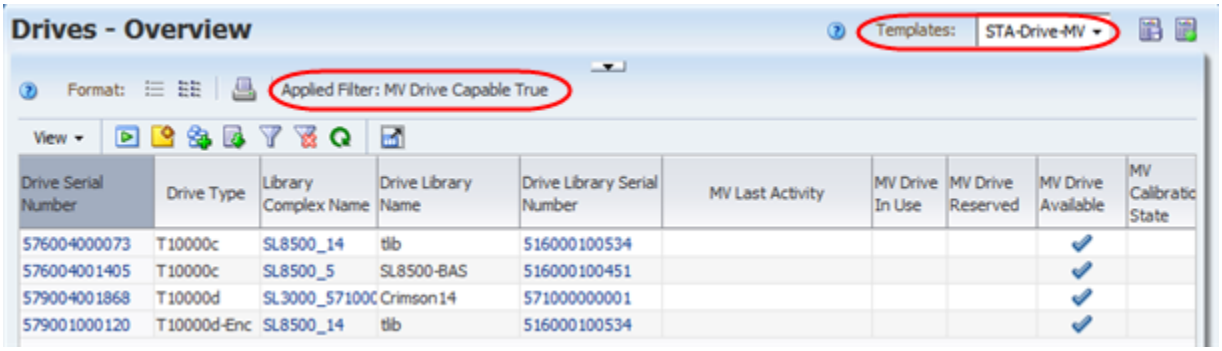
You can add and remove drives from the validation drive pools according to your needs. STA detects any changes and uses new drives as necessary.

Validation Drives That Can be Used by STA

SL Console does not check for STA minimum requirements when drives are added to the validation drive pools. As a result, drives in the pools may not necessarily be valid for use by STA. However, the STA Media Validation Configuration screen displays the total number of validation drives that do meet the minimum requirements for STA media validation. From there, you can link to the Drives – Overview screen, where you can see detail for these drives, such as drive type, Drive Health Indicator, and the drive location. See "Display Validation Drives for STA Media Validation" on page 8-27 for instructions.

You can also select the Drives – Overview screen directly from the Navigation Bar and apply the STA–Drive–MV template, which is an STA predefined template. Figure 8–1 is a sample display.

Figure 8–1 Validation Drives on the Drives – Overview Screen



Choosing Drives for the Validation Drive Pools

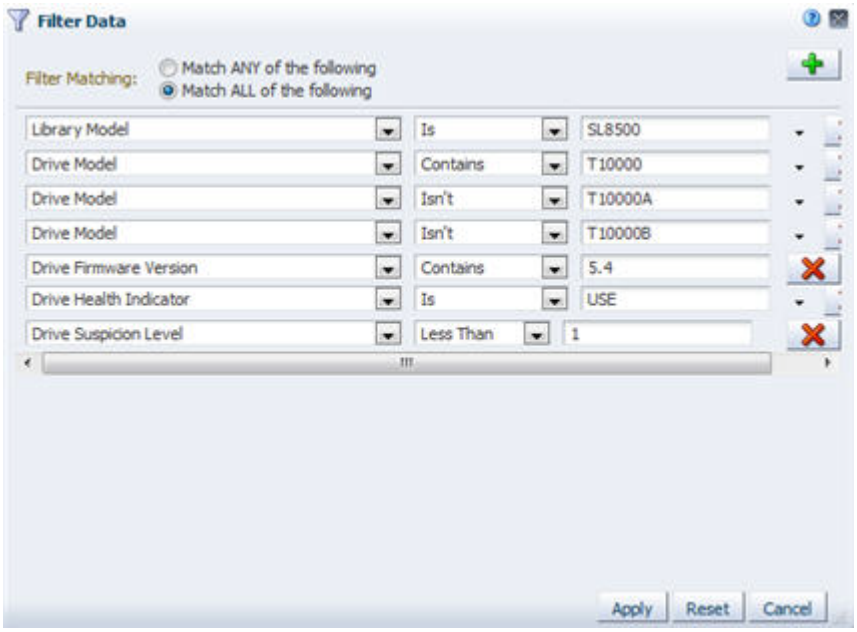
Although drives are assigned to the validation drive pools with the SL Console, you can use STA to review and select candidate drives.

You can assign any drives to the pools, but in order for STA to use them, they must meet the following minimum requirements:

- Drive Model is T10000C or T10000D.
- Drive Firmware Version ends in 5.40 or higher – This indicates the firmware supports TTI 5.4.
- Drive Health Indicator is Use.
- Drive Suspicion Level is 0.

Figure 8–7 is a sample filter you might use on the Drives – Overview screen.

Figure 8–2 Filter for Reviewing Validation Drive Candidates

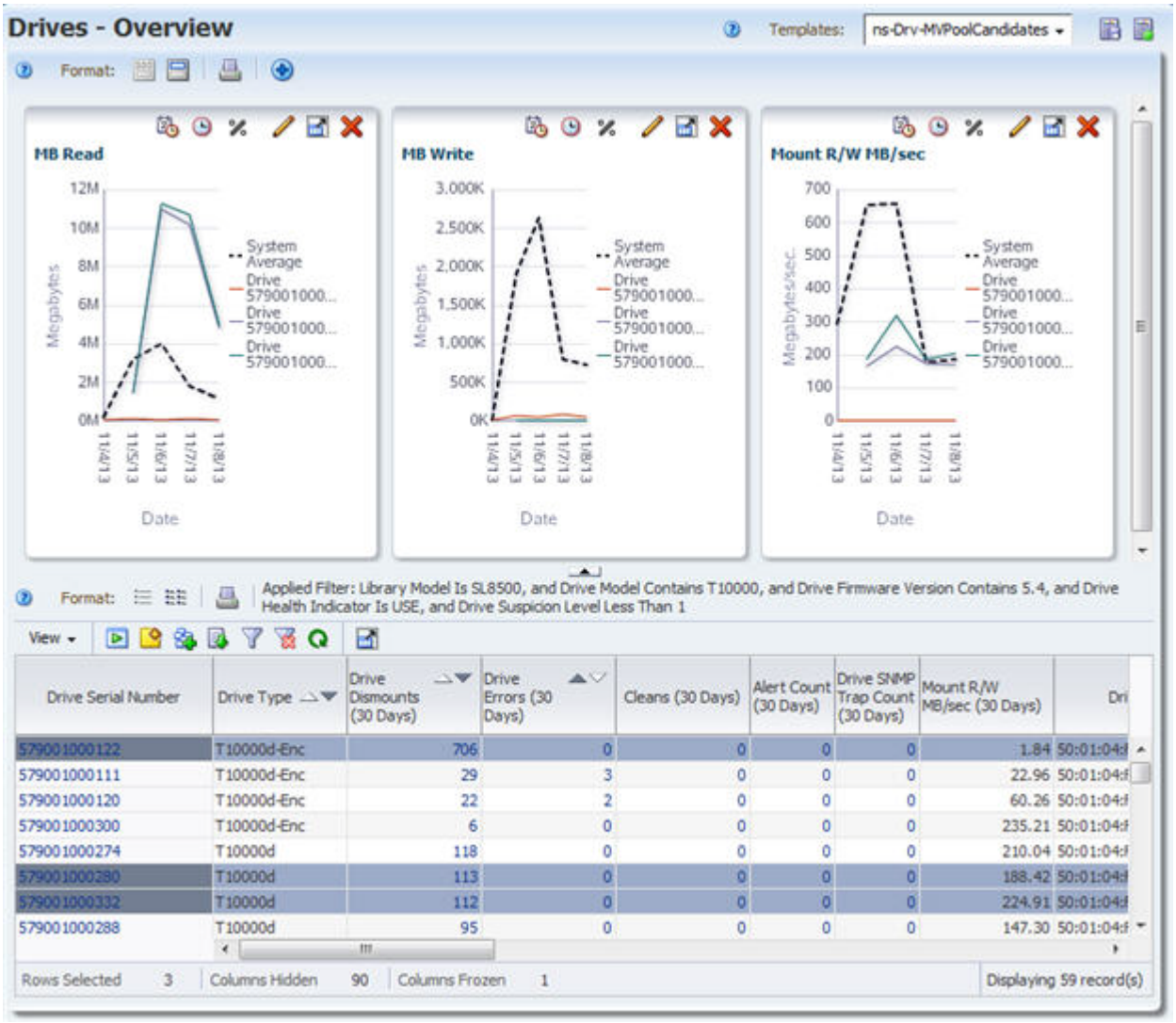


In addition to these minimum requirements, you should select drives that are of high quality, with some recent activity and few or no errors. Drives with the following characteristics may be good candidates for the validation pools:

- 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.

You may want to apply selected drives to the graphs to get a visual representation of the drive characteristics and confirm your selections. Figure 8–3 shows three candidate drives applied to the graphs on the Drives – Overview screen.

Figure 8–3 Drives – Overview Screen Showing Validation Drive Candidates



Enabling Media Validation

STA media validation is disabled by default, so you must explicitly enable it. This is a global setting, so once enabled, STA media validation is available for all SL3000 and SL8500 libraries in your tape library system. See "Enable or Disable Media Validation on STA" on page 8-30 for detailed instructions. Enabling and disabling media validation requires Administrator privileges.

Once media validation is enabled, you can begin using STA to perform the following activities:

- Create manual media validation requests. See "Submitting Manual Validation Requests" on page 8-17 for complete details.
- Display and manage the media validation request queue. See "Managing the STA Media Validation Request Queue" on page 8-21.
- Use media validation policies to perform automated validations. See "Using Automated Media Validation" on page 8-19 for complete details.

Note: You can create validation policies before enabling media validation on STA.

Media Validation Configuration Status Messages

The Media Validation Configuration screen displays the current configuration status of the STA media validation feature.

The following messages may appear while media validation is being configured without drive calibration and qualification. Figure 8–4 is an example.

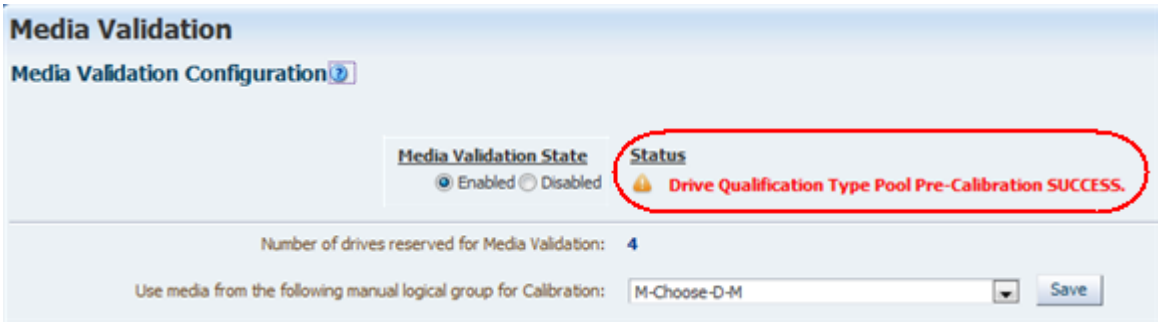
- Media Validation is DISABLED.
- Media Validation successfully enabled.
- Media Validation Enabled; Opted-out of Drive Calibration.

Figure 8–4 Media Validation Configuration Success Message

The drive calibration and qualification feature may take some time to enable and configure. You may see the following messages while this process is underway. Figure 8–5 is an example. See "Drive Calibration and Qualification" on page 8-10 for information about these features.

- 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.

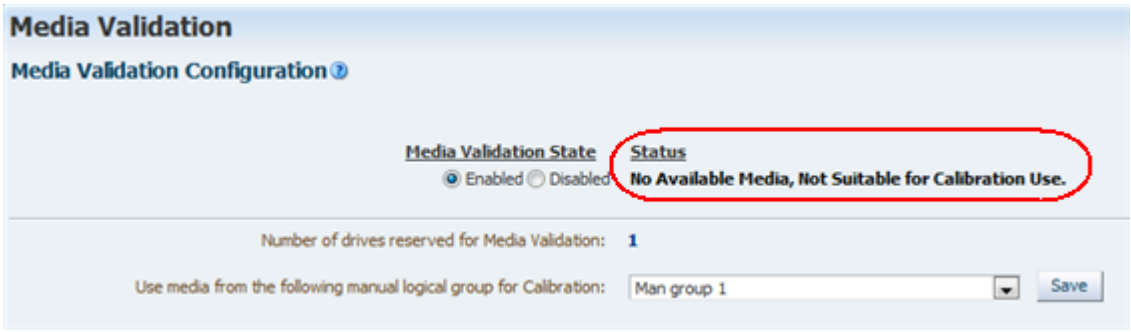
Figure 8–5 Drive Calibration Configuration Success Message



The following messages indicate a problem with media validation configuration. Figure 8–6 is an example.

- 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.

Figure 8–6 Drive Calibration Configuration Error Message



Disabling Media Validation

Once media validation has been enabled at your site, you may want to temporarily disable it on occasion for library maintenance. See "Enable or Disable Media Validation on STA" on page 8-30 for detailed instructions.

STA does not accept any new media validation requests while media validation is disabled. Any pending or in-progress requests are processed to completion unless you explicitly cancel them.

With media validation disabled, STA still displays requests initiated from other sources, such as SL Console and the library command-line interface (CLI).

Drive Calibration and Qualification

Drive calibration and qualification are optional STA features that confirm the validity of all media validation tests. When these features are enabled, STA uses only calibrated and qualified drives to perform media validation activities.

Calibration, which is a one-time, setup process, ensures that 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.

Together these features ensure that the results of each and every media validation reflect the true quality of the tested media and are not confounded by unknown issues with the validation drives.

This section includes the following topics:

- "Drive Calibration and Qualification Terms" on page 8-11
- "Benefits of Calibration and Qualification" on page 8-12
- "How Calibration and Qualification Work" on page 8-13
- "Preparing for Calibration and Qualification" on page 8-14

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.

Read Quality Index (RQI)
Measure of the amount of error correction left on the media. RQI 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.

RQI is reported as a percentage. A high value is desirable.

Data Quality Index (DQI)
Measure of the amount of error correction left on the media, similar to Read Quality Index (RQI), but targeted specifically to the media because it factors out the drive's contribution. During drive calibration and qualification, STA uses the DQI to determine whether the drive is qualified or disqualified.

DQI is reported as a percentage. A high value is desirable.

Benefits of Calibration and Qualification

Although drive calibration and qualification are optional features, it is highly recommended that you enable them on STA, as they provide the following significant advantages:

- Ensured Validity of Validation Results
- Ensured Health of Validation Drives
- Operational Efficiency

Ensured Validity of Validation Results

Because each exchange involves both a piece of media and a drive, when an exchange failure occurs, there is always uncertainty whether the problem is with the drive, the media, or both. For production media, STA uses sophisticated health and suspicion algorithms that reduce this uncertainty, in part by using available historical data for the media and the drive. The more data available, the more reliable the analysis.

Media validation failures carry the same inherent uncertainty. However, they are further complicated by the fact that validation exchanges tend to involve a higher-than-normal percentage of problem media and media that have little or no available history.

For example, an archive media that has not been used in over a year may have minimal STA data. If the media is validated on an uncalibrated drive and the validation fails, there is a possibility the failure is the result of problems with the validation drive, not the media being validated. With minimal historical data available for the media, there is increased uncertainty about the validation result. The STA drive calibration and qualification features directly address these uncertainties, providing you with assurance the failed validation has identified a problem with the media.

Ensured Health of Validation Drives

Another advantage of calibration and qualification concerns drive quality. 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. Drive problems are identified early so the verification drives can be serviced or replaced before they, in turn, begin to cause problems with production media.

Operational Efficiency

When a media validation fails, some action must be taken to verify the result and confirm there is a problem with the media. If drive calibration and qualification is disabled, you must do this verification manually. For example, you could perform a

Complete Verify on the media using a different drive, and if this validation also fails, then you could be reasonably certain the problem is with the media, not the drive. Depending on the amount of data on the media, this could take several hours.

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 and qualification are separate processes, but they are enabled and disabled together. Before using calibration and qualification, you must create a manual logical group for media that will be used for these activities. See "Preparing for Calibration and Qualification" on page 8-14 for details.

Drive Calibration Process

Drive calibration is a one-time setup process that begins as soon as drive calibration is enabled on the Media Validation screen. All drives in the validation pool are tested using a Standard Verify. This may take one to two hours per drive.

Once drive calibration is configured and enabled, it proceeds automatically with no need for manual intervention. If a new drive is added to the media validation pool, STA detects this and automatically begins calibrating the drive. STA also automatically recalibrates drives after a firmware update.

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 Data Quality Index (DQI) values from the validations. For a drive to be qualified, the following criteria must be met:
   - One media must have DQI >=75. This is assigned to the drive as the *primary* calibration media.
   - One media must have DQI >=50. This is assigned to the drive as the *secondary* calibration media.
3. Depending on the DQI 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 *disqualified*.

Results of Drive Calibration

If a drive passes calibration, two media are assigned to it as dedicated *primary* and *secondary calibration media*. During the calibration process, these media are confirmed to be of high quality. Each validation drive has its own primary and secondary calibration media, and these media are used for all drive qualification activities on the drive.

If a drive fails calibration, it is *disqualified*. Disqualified drives are assigned a Calibration State of "Not Suitable," and they are not used for any STA validation activities while drive calibration is enabled. They remain in the media validation drive pool until you explicitly remove them through the SL Console.

Note: 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.

Once all drives have been calibrated, 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. See "Display Validation Drives for STA Media Validation" on page 8-27 for instructions.

Validation Drive Qualification Process

Validation drives are qualified to assure the drives are still calibrated. Qualification is an ongoing process that runs automatically in the background and requires no user intervention. STA automatically initiates a qualification 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. Qualification follows a process similar to drive calibration.

Results of Drive Qualification

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.

Disqualified media are not used for drive calibration or qualification. They remain in the calibration media logical group until you explicitly remove them. See "Results of Drive Calibration" on page 8-13 for information about disqualified drives.

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.

Preparing for Calibration and Qualification

Before enabling calibration and qualification, you must perform the following preparation tasks.

1. On the Logical Groups screen, create a manual logical group for media that will be used for drive calibration. See "Calibration Media Logical Group" on page 8-15 for details. This task requires Operator or Administrator privileges.
2. On the Media – Overview screen, review and choose the media you want to use for drive calibration. See "Choosing Calibration Media" on page 8-15 for details.

3. Assign the media to the logical group. This task requires Operator or Administrator privileges.
4. Enable drive calibration and qualification. See "Enable Drive Calibration and Qualification" on page 8-34 for instructions. This task requires Administrator privileges.

Calibration Media Logical Group

The media used for drive calibration and qualification must be assigned to a manual logical group dedicated exclusively for this purpose. This is the *calibration media logical group*. Once a logical group has been designated as the calibration media logical group, the media in it cannot be used for host operations, and STA will not allow them to be used 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, and the media must reside in the same standalone libraries and library complexes as the validation drives. For example, if you have eight validation drives in complex SL8500 1 and one validation drive in standalone library SL8500-Seattle, the logical group must include at least 16 media from the libraries in complex SL8500 1 and two media from library SL8500-Seattle. There is no maximum number of media you can assign to the group.

Note: Since the purpose of this logical group is to identify media dedicated for calibration operations, Oracle recommends that you assign only media—no drives—to this group.

You can add and remove media from the logical group according to your needs. STA detects any changes and uses new media as necessary.

Choosing Calibration Media

It is highly recommended that you 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.

To be used for drive calibration and qualification, media must meet the following criteria:

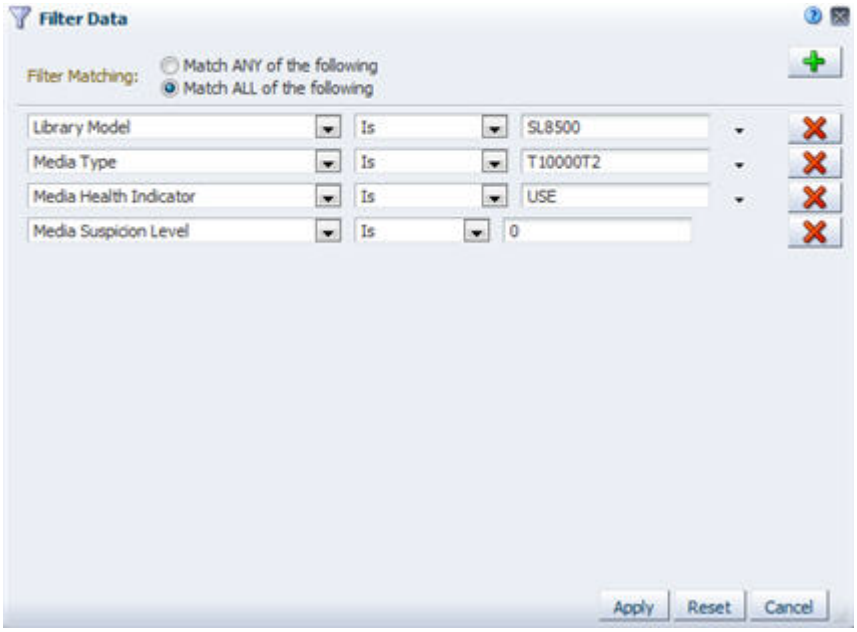
- Media Type is T10000T2 (indicating T100000T2 or T10000T2 Sport). Although T10000T1 media can be validated, they cannot be used for drive calibration and qualification.
- Media Health Indicator is Use.
- Media Suspicion Level is 0.
- At least two wraps of data have been written to the media.

Note: STA does not check for these criteria when you add media to the calibration logical group, so it is possible to assign media that cannot be used for calibration and qualification.

Note: If any media you assign to the calibration logical group do not have the minimum required STA history, STA automatically initiates a Basic Verify on them before attempting to use them for drive calibration. A Basic Verify provides the minimum required history. See "Types of Verification Tests" on page 8-3 for details.

To find media that meet these requirements, you can apply a filter to the Media – Overview screen. Figure 8–7 is a sample filter you might use on the Media – Overview screen.

Figure 8–7 Filter for Reviewing Calibration Media Candidates



You can sort the filtered results by the "Media MB Avail Post" attribute to find media with at least two wraps of data. This varies by recording format and media type. Table 8–2 provides a summary of required amounts.

Table 8–2 T10000T2 Media, MB Written (Compressed) for Two Wraps of Data

Media Type	MB Written
T10000D Standard	119,000 MB
T10000D Sport	23,800 MB
T10000TC Standard	97,000 MB
T10000TC Sport	19,400 MB

Submitting Manual Validation Requests

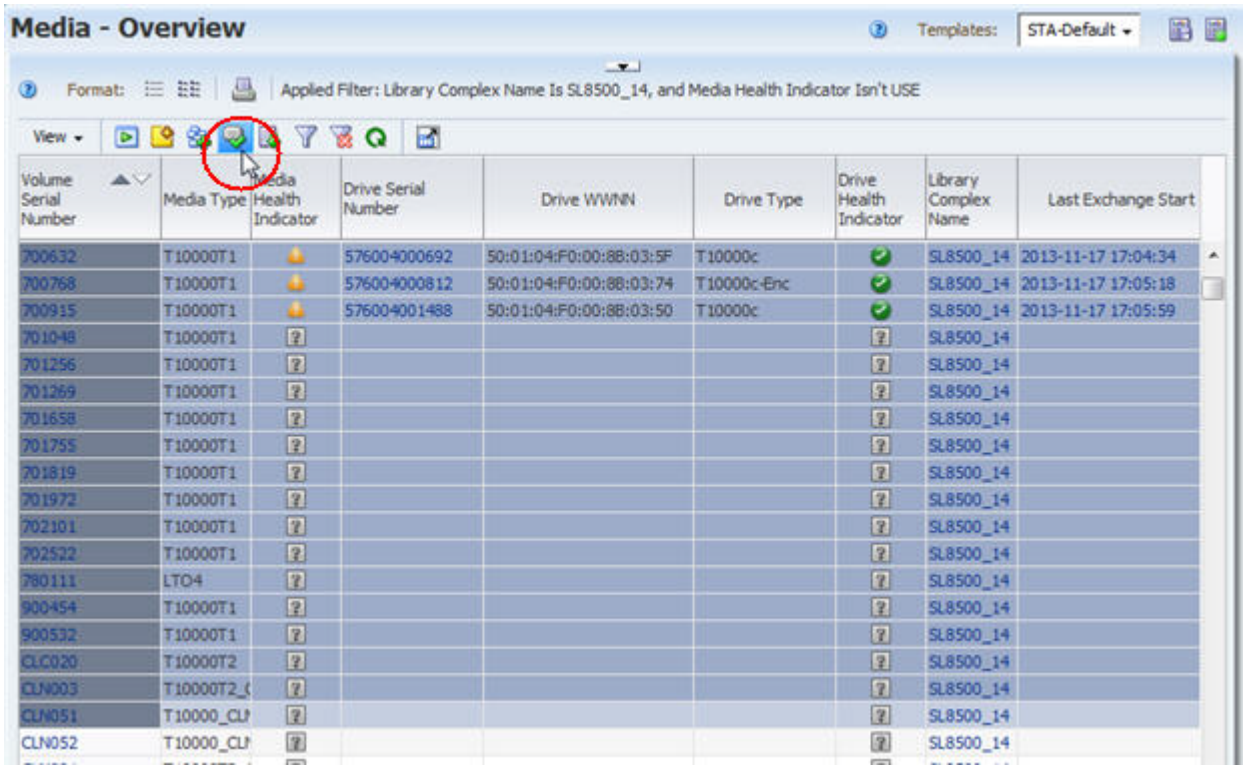
Once the validation drive pools have been created and media validation has been enabled on STA, you can use STA to submit manual validation requests and manage the validation request queue. See "Submit Manual Media Validation Requests" on page 8-39 for instructions.

> **Note:** If you have enabled drive calibration, the media included in the *calibration media logical group* cannot be included in manual or automated validation requests. STA will display an error message that the media are not eligible for media validation. See "Calibration Media Logical Group" on page 8-15 for details about these media.

You can submit manual validation requests from either of the following screens:

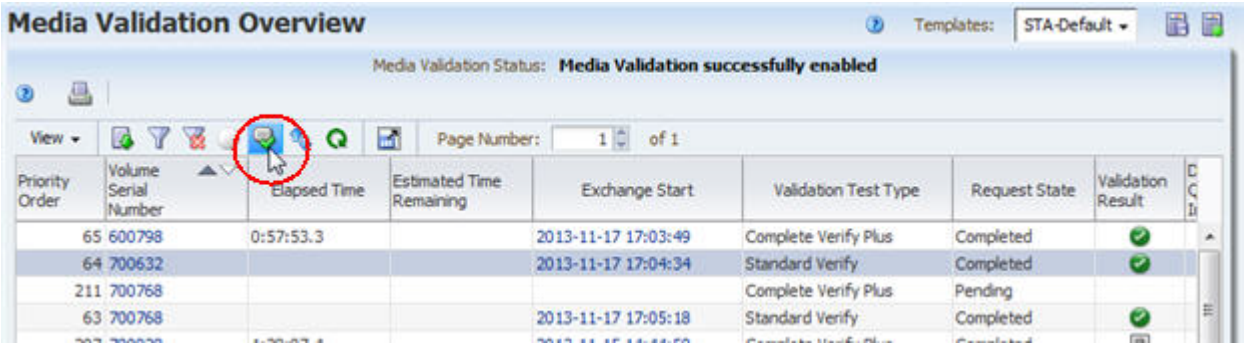
- Media Overview—You can select multiple media at once to be validated using the same verification test. Only the eligible media within the selection range are confirmed for validation. Figure 8–8 is an example. Note that the selection range includes a variety of media types, including some that are not eligible for media validation.

Figure 8–8 Initiating Media Validations From the Media – Overview Screen



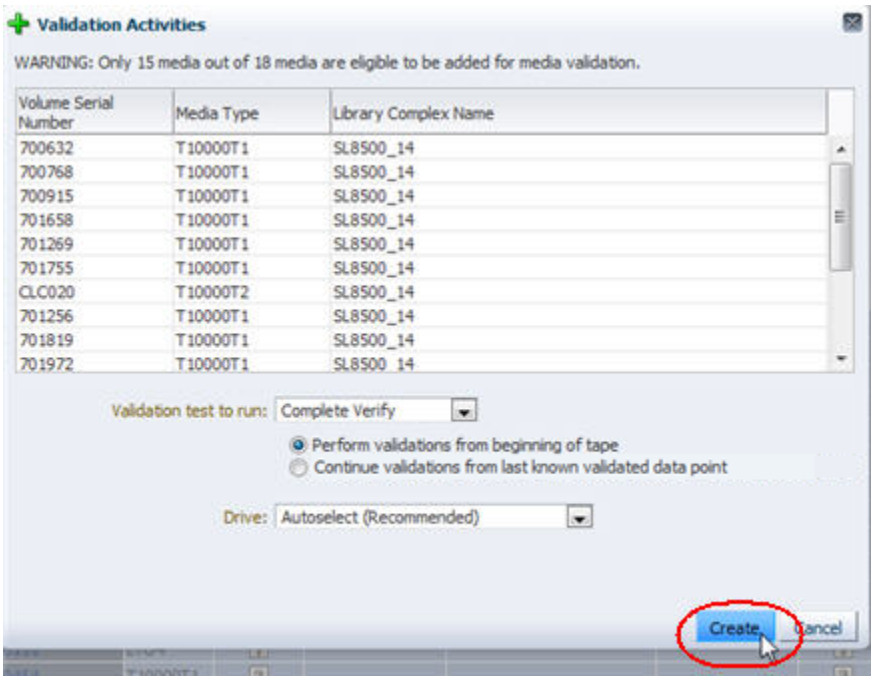
- Media Validation Overview—You can select only one media at a time for validation. Figure 8–9 is an example.

Figure 8–9 Initiating a Media Validation From the Media Validation Overview Screen



To generate a manual request, you specify the following information. Figure 8–10 is a sample manual validation request.

Figure 8–10 Sample Manual Validation Request for Multiple Media



- Media to be validated. STA allows you to generate requests for T10000 media only. If you select multiple media at once on the Media Overview screen and only some are T10000, then only the eligible media are confirmed for validation.
- Validation test type. This is the type of verification test to be performed on the media. See "Types of Verification Tests" on page 8-3 for detailed descriptions.
- Start from beginning of tape (BOT) or resume where the last interrupted validation left off. This option is available only if all of the following conditions are true. See "Resuming Interrupted "Complete Verify" Tests on T10000T2 Media" on page 8-24 for details.
  - You have selected T10000T2 media for validation. (T10000T1 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 validations for some or all of the selected media are not 100 percent complete. (Media for which the most recent validation was complete are always validated from the beginning of tape.)

- Validation drive – If your site has more than one validation drive, the recommended method of drive selection is to have STA select a compatible validation drive. However, if all selected media are in the same standalone library or library complex, you can manually specify the drive to use; STA provides a list of compatible drives from which to choose. If the media are distributed across multiple standalone libraries or complexes, then STA automatically selected the drives to use.

As soon as you submit the manual request, it is added to the STA media validation request queue. The validation is started when a compatible drive becomes available.

Manual Verify and Rebuild MIR Requests for Incompatible Media and Drives

Note: See the *STA Requirements Guide* for the minimum firmware levels discussed in this section.

If you submit a manual Verify and Rebuild MIR request for a media and drive that are incompatible (for example, you submit a request for a T10000C media to be validated by a T10000D drive), drives with minimum firmware levels for TTI 5.5.0 will correctly reject the request. Drives with firmware not meeting the minimum TTI 5.5.0 requirements may attempt to process the request, and if they are able to rebuild the MIR, may incorrectly report a success status for the request. This situation cannot arise for automatic requests, as STA only generates requests in which the media and drives are compatible.

The STA version of the Verify and Rebuild MIR request may be unable to rebuild a MIR if the last known good spot is at End of Data (EOD), in which case, you must use the drive Virtual Operator Panel (VOP) to rebuild the MIR.

Using Automated Media Validation

STA allows you to define any number of media validation policies, which automatically select media for validation based on a variety of user-defined criteria. For each selected media, STA generates a validation request, which is submitted to the STA validation queue. As soon as a compatible drive becomes available, the validation is started. This activity is all managed automatically by STA.

Depending on the number of media validation policies and how they are defined, a single piece of media could potentially be selected for validation several times a day. To prevent this from happening, STA limits automated validations to a maximum of 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.

Media Eligible for Automated Validation

> **Note:** If you have enabled drive calibration, the media included in the *calibration media logical group* cannot be included in manual or automated validation requests. STA will automatically exclude these media from any validation policies. See "Calibration Media Logical Group" on page 8-15 for details about these media.

To be used by STA for policy-driven validation, media must have a minimum history. Media must have values for the following attributes:

- Exchange Recording Technique (recording format used by the drive to write to the media)
- Media Suspicion Level
- MB Written (total amount of data written to the media)

If you want STA to validate media that does not have this history, you should manually initiate a Basic Verify to supply these attributes. See "Types of Verification Tests" on page 8-3 and "Submit Manual Media Validation Requests" on page 8-39 for details.

Defining Validation Policies

Users with Administrator privileges perform this part of the process from the Media Validation screen on the Setup & Administration tab. Media validation does not need to be enabled on STA for you to create validation policies, so you can do this ahead of time if you want.

When you create a validation policy, you can enable it immediately or leave it disabled for the time being. STA uses only enabled policies to generate validation requests.

To define a validation policy, you specify the following information:

- Policy name – Alphanumeric identifier for the policy. Policy names must be unique.
- Policy description – Optional description of the policy.
- Applicable media group – You can choose to apply the policy to media with specified recording formats in a specified library complex, or media in a specified logical group. See "Validating Media by Logical Group" on page 8-20 for details about logical groups.
- Selection criteria – Predefined criteria by which media in the applicable media group are selected for validation. See "Selection Criteria for Validation Policies" on page 8-21 for detailed descriptions.
- Validation test type – Type of verification test to be performed on the media. See "Types of Verification Tests" on page 8-3 for detailed descriptions.

See "Create a Media Validation Policy" on page 8-53 for detailed instructions.

Validating Media by Logical Group

You can apply a media validation policy to any existing logical group, one logical group per policy. The logical group identifies the media to be validated by the policy but not the drives to be used; drives are always selected from the validation drive pool defined through SL Console (see "Preparing for STA Media Validation" on page 8-5 for

details).

STA generates validation requests only for media in the group that meet both of the following criteria:

- T10000 media
- Media that reside in standalone SL3000 or SL8500 libraries or library complexes that have validation drive pools with drives meeting the STA minimum requirements

Selection Criteria for Validation Policies

STA can select media for validation based on any of the following predefined criteria:

- 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 – 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.

Managing the STA Media Validation Request Queue

The media validation request queue is displayed on the Media Validation Overview screen on the Tape System Activity tab. The queue lists all media validation activity that has occurred in your tape library system. This includes pending and completed validation requests initiated by STA or any other application. By default, requests are listed in reverse Priority Order, with the most recent requests at the top of the list.

From the Media Validation Overview screen, you can perform any of the following activities:

- "Displaying the Status of Validation Requests" on page 8-21
- "Canceling Pending or In-Progress Validation Requests" on page 8-24
- "Resuming Interrupted "Complete Verify" Tests on T10000T2 Media" on page 8-24

Displaying the Status of Validation Requests

The Media Validation Overview screen displays complete details about all validation requests. This section describes attributes of particular interest on this screen.

Note: If drives, media, or library connections are removed from your tape library system, any associated pending STA validation requests remain in the request queue until you explicitly cancel them. See "Cancel Pending Media Validation Requests" on page 8-49 for instructions.

Media Validation Request Priorities

The MV Priority Order attribute indicates the order of each validation request in the queue. When a new request is created, it is assigned the next available MV Priority Order value. STA processes requests in priority order, and you can reprioritize pending requests by moving them up or down in the queue. See "Reorder Pending Media Validation Requests" on page 8-46 for instructions.

Pending and in-process requests are listed in reverse Priority Order, so the most recently received requests are at the top of the list. Completed validations have a blank Priority Order value.

Media Validation Request States

The Request State indicates the progress of each validation request. Requests are typically processed through the following sequence:

1. 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.
2. Starting – The drive has been reserved for the validation operation.
3. 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.
4. Completed – The validation has completed. See "Media Validation Results" on page 8-23 for details about information STA may display.

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. See "Canceling Pending or In-Progress Validation Requests" on page 8-24 for details.

Media Validation Initiators

STA reports all media validation information it receives from your tape library system. Consequently, you may see media validations not initiated through STA. Media validations can be done from a variety of applications, and the Initiator attribute indicates the source. Options are as follows:

- Drive – Indicates the validation was initiated directly on the T10000C or T10000D drive.
- Host – Indicates an external host application, such as Oracle's StorageTek Storage Archive Manager (SAM). These applications do not use the internal media validation capabilities of the T10000C and T10000D drives.
- 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 library *User's Guide* for details.

- SLC – Indicates the 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 DQI

The data quality index (DQI) 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.
- 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 more than nine hours to complete. 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.

Canceling Pending or In-Progress Validation Requests

You may need to cancel validation requests, especially Complete Verify or Complete Verify Plus validations, which may take many hours to complete. From STA, you can cancel STA-initiated pending or in-progress validation requests only. You can cancel these requests at any time, and you can cancel multiple requests at once.

When a pending request is canceled, it is immediately removed from the validation request queue.

For in-progress validations, you can cancel Complete Verify or Complete Verify Plus tests only. When an in-progress request is canceled, the Request State changes to Stopped and STA sends a cancellation request to the drive. It 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 "Resuming Interrupted "Complete Verify" Tests on T10000T2 Media" on page 8-24 for details.

Resuming Interrupted "Complete Verify" Tests on T10000T2 Media

Note: This option is available for T10000T2 media only; validations of T10000T1 media must always start at the beginning of tape (BOT).

For T10000T2 media, Complete Verify and Complete Verify Plus validations that have been interrupted by host media requests or canceled manually can either be restarted from the beginning of tape (BOT) or resumed from the point where they left off. To resume a validation, the drive must be able to determine from the media RFID chip where the last validation left off.

This option is available both for manually submitted requests and for requests initiated by an STA media validation policy. See "Submit Manual Media Validation Requests" on page 8-39 and "Create a Media Validation Policy" on page 8-53 for instructions.

Note: 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 restart the operation from the beginning.

User Roles for Media Validation

Table 8–3 lists the user roles required for configuring STA media validation.

Table 8–3 Media Validation Configuration User Roles

User Role	Media Validation Configuration Activity	Screen
Viewer and above	Display drives in the media validation drive pools.	Select **Tape System Hardware**, then select **Drives Overview**.
Administrator only	Display drives in the media validation drive pools. Enable or disable media validation on STA. Enable or disable drive calibration by selecting the designated logical group of media.	Select **Setup & Administration**, then select **Media Validation**.

Table 8–4 lists the user roles required for managing the STA media validation request queue.

Table 8–4 Media Validation Request Queue User Roles

User Role	Media Validation Request Queue Activity	Screen
Viewer and above	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 pending media validation requests. Cancel selected pending or in-progress media validation requests. Resume an interrupted validation of a T10000T2 media.	Select **Tape System Activity**, then select **Media Validation Overview**.
Operator and above	Manually submit multiple media validation requests. Resume multiple interrupted validations of T10000T2 media.	Select **Tape System Hardware**, then select **Media Overview**.

Table 8–5 lists the user roles required for managing STA media validation policies.

Table 8–5 Media Validation Policy User Roles

User Role	Media Validation Policy Activity	Screen
Operator and above	Display and print the list of media validation policies.	Select **Setup & Administration**, then select **Media Validation**.
Administrator only	Display the list of media validation policies. Define a media validation policy. Enable or disable a media validation policy. Copy a media validation policy. Modify a media validation policy as follows: ▪ Rename a policy. ▪ Change the policy criteria. Delete a media validation policy.	Select **Setup & Administration**, then select **Media Validation**.

Best Practices for Media Validation

This section provides tips for using STA media validation.

SNMP v3 required
The STA media validation feature requires the use of SNMP v3 for communication between STA and the libraries.

See the *STA Requirements Guide*.

Calibration and qualification
If you are using media validation, it is highly recommended that you also enable the calibration and qualification features, as they help to ensure the validity of validation results, ensure the health of the validation drives, and provide operational efficiency for the media validation feature.

See "Benefits of Calibration and Qualification" on page 8-12.

Dedicated calibration media
The media used for drive calibration and qualification must be dedicated for this purpose; they cannot be used production data.

See "Calibration Media Logical Group" on page 8-15.

Media validation autoselect
When submitting manual media validation requests, let STA select the drives for validation operations (Autoselect) rather than selecting manually. This will ensure that the media is mounted on a compatible validation drive.

See "Submitting Manual Validation Requests" on page 8-17.

Media Validation Tasks

Media Validation Configuration Tasks

- "Display Validation Drives for STA Media Validation" on page 8-27
- "Enable or Disable Media Validation on STA" on page 8-30
- "Enable Drive Calibration and Qualification" on page 8-34
- "Disable Drive Calibration and Qualification" on page 8-36

Media Validation Request Management Tasks

- "Display the Media Validation Request Queue" on page 8-37
- "Submit Manual Media Validation Requests" on page 8-39
- "Reorder Pending Media Validation Requests" on page 8-46
- "Cancel Pending Media Validation Requests" on page 8-49
- "Cancel In-Progress "Complete Verify" Validations" on page 8-51

Media Validation Policy Tasks

- "Create a Media Validation Policy" on page 8-53
- "Display the List of Media Validation Policies" on page 8-58
- "Enable or Disable a Media Validation Policy" on page 8-59
- "Copy a Media Validation Policy" on page 8-61
- "Modify a Media Validation Policy" on page 8-62

- "Delete a Media Validation Policy" on page 8-64

Display Validation Drives for STA Media Validation

Use this procedure to display information about validation drives that meet minimum requirements for STA media validation. See "Validation Drives That Can be Used by STA" on page 8-6 for details.

Note: The validation drive pools are maintained only through SL Console. See the library *User's Guide* for detailed instructions on maintaining the pools.

Note: This procedure requires Administrator privileges.

You can perform this procedure using either of the following methods:

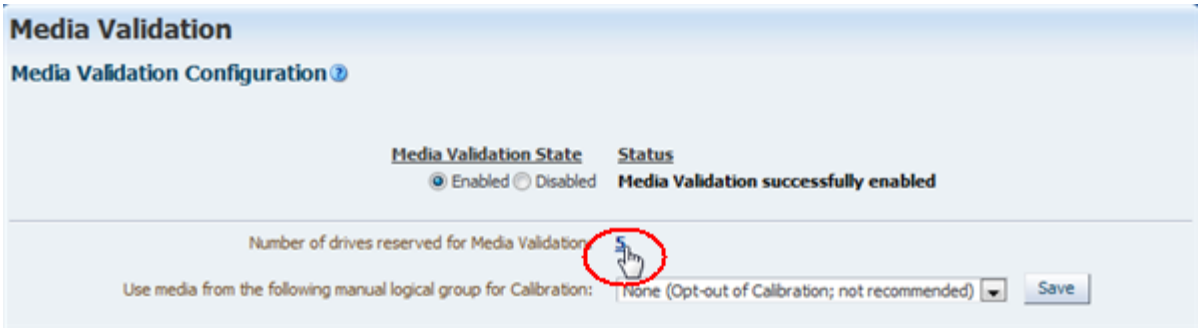
- "From the Media Validation Screen" on page 8-27
- "From the Drives – Overview Screen" on page 8-28

From the Media Validation Screen

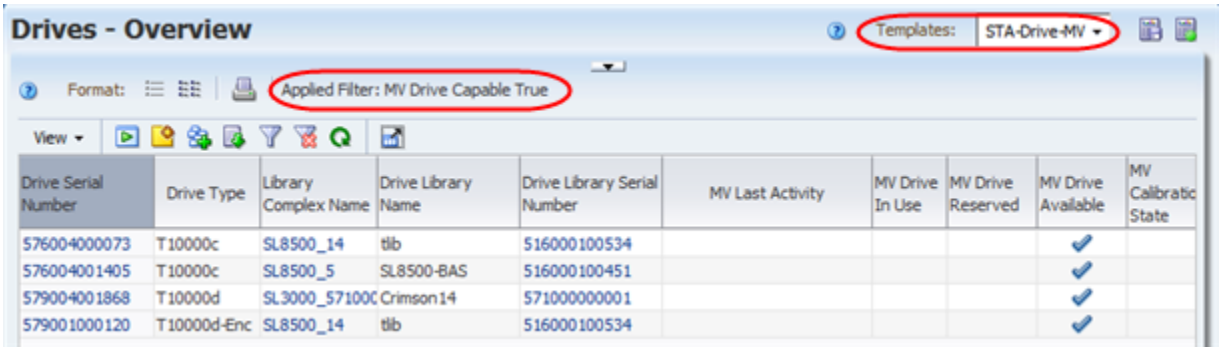
Note: This method requires Operator or Administrator privileges.

1. In the Navigation Bar, select **Setup & Administration**, then select **Media Validation**.

2. In the Media Validation Configuration section of the screen, the **Number of Drives Reserved for Media Validation** field displays the total number of drives assigned to the validation pools and that meet STA minimum requirements. Select the link.



You are taken to the Drives – Overview screen with a filter applied to show detail about these drives.



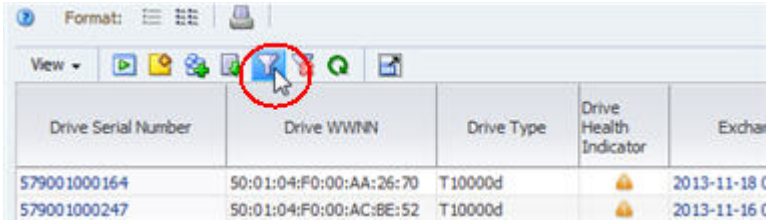
From the Drives – Overview Screen

Note: This method can be done by any user.

1. In the Navigation Bar, select **Tape System Hardware**, then select **Drives Overview**.

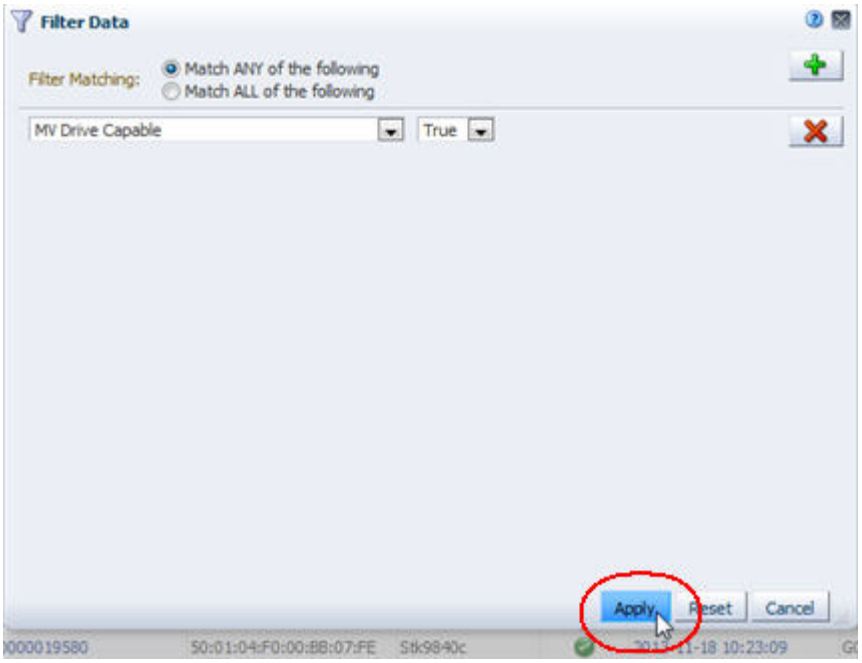
The Drives – Overview screen appears, displaying all drives in your tape library system.

2. In the Table Toolbar, click **Filter Data**.

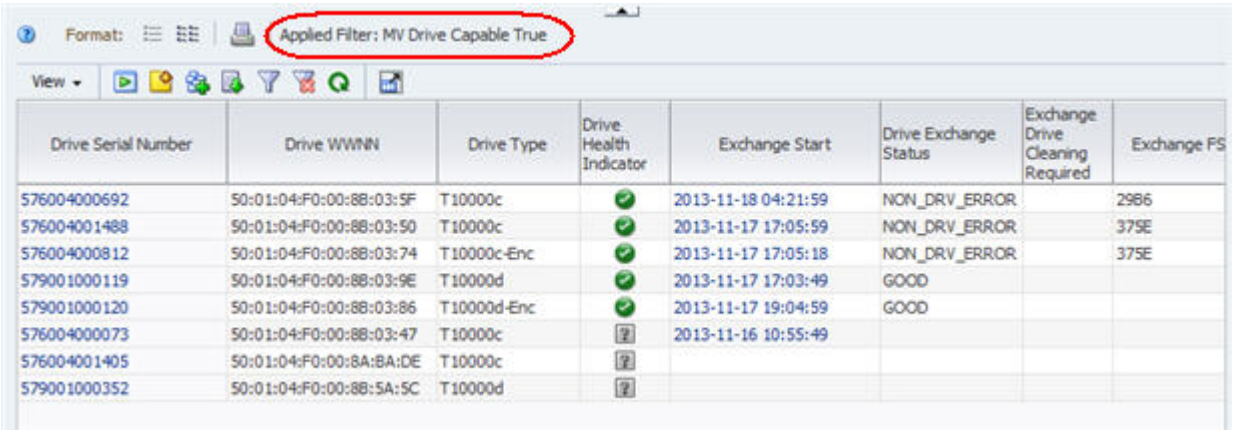


The Filter Data dialog box appears.

3. In the selection criteria menus, select **MV Drive Capable** and **True**. Then click **Apply**.



The table is updated to display only drives that have been assigned to the validation drive pools and that meet minimum requirements for STA media validation.



Enable or Disable Media Validation on STA

Use this procedure to review the current configuration of the media validation feature on STA and enable or disable it. By default, media validation is disabled when STA is installed. See "Enabling Media Validation" on page 8-8 and "Disabling Media Validation" on page 8-10 for details.

Note: 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, you can do so either before or after disabling media validation. See "Canceling Pending or In-Progress Validation Requests" on page 8-24 for details.

Note: This procedure requires Administrator privileges.

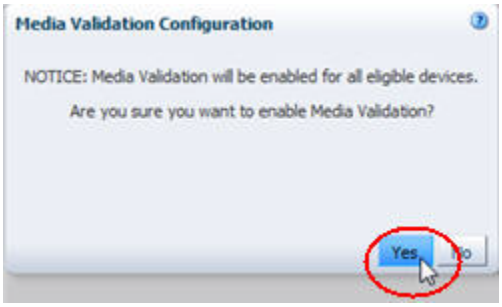
1. In the Navigation Bar, select **Setup & Administration**, then select **Media Validation**.

   The Media Validation screen appears.

2. In the Media Validation State field, select either **Enable** or **Disable**, as follows:
   - Enable – Enables STA media validation for all SL3000 and SL8500 libraries monitored by STA.
   - Disable – Disables STA media validation for all SL3000 and SL8500 libraries monitored by STA. You may want to temporarily disable media validation to perform library maintenance.

A confirmation dialog box appears.

3. Verify your selection, and click **Yes** to confirm.



The STA media validation state is updated according to your selection, and the new status is indicated on the screen. If media validation cannot be enabled at this time, the reason is indicated on the screen.

Create the Calibration Media Logical Group

Note: This is an optional procedure that you need to use only if you plan to enable drive calibration and qualification.

Use this procedure to create the logical group of media you want to use for drive calibration and qualification. The media in this group should be dedicated exclusively for these purposes. Oracle recommends that you assign only media—no drives—to this group. See "Calibration Media Logical Group" on page 8-15 for details.

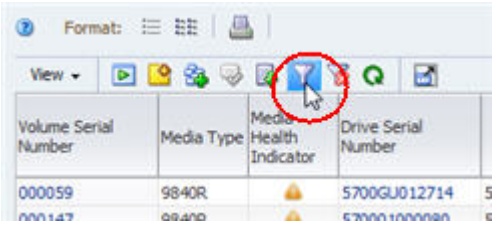
Note: Before using this procedure, you must create a manual logical group to be used exclusively for the calibration media. See "Choosing Calibration Media" on page 8-15 and "Create a Manual Logical Group" on page 7-11 for details.

Note: This procedure requires Operator or Administrator privileges.

1. In the Navigation Bar, select **Tape System Hardware**, then select **Media Overview**.

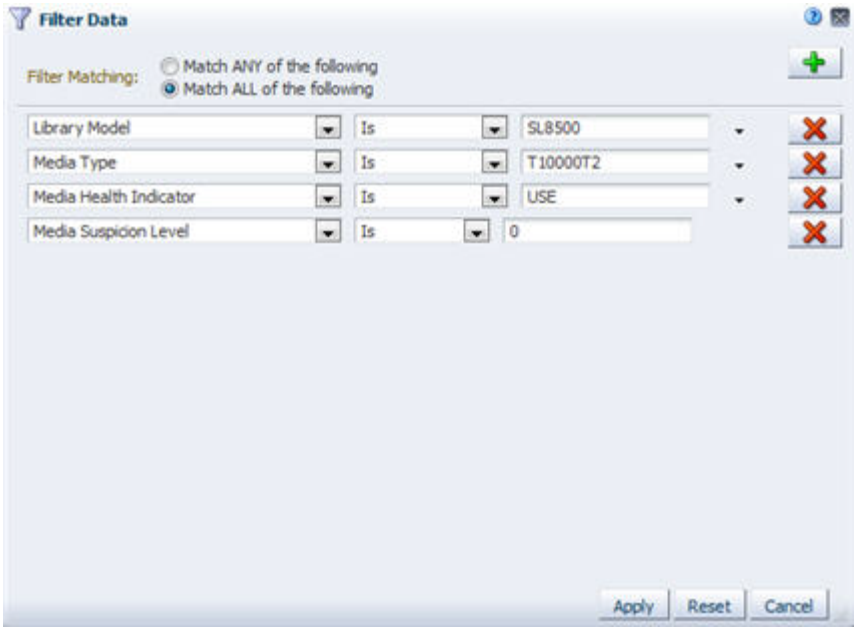
   The Media – Overview screen appears, displaying all media in your tape library system.

2. In the Table Toolbar, click **Filter Data**.



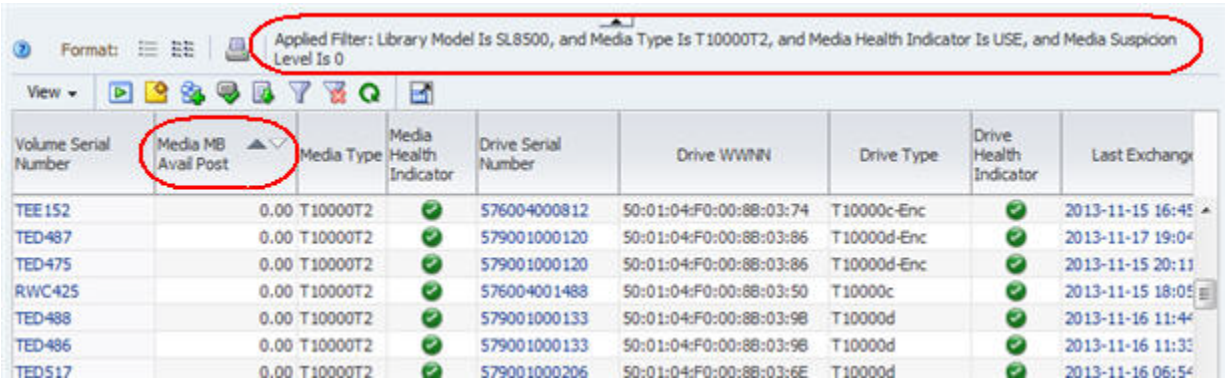
   The Filter Data dialog box appears.

3. In the selection criteria menus, enter the criteria specified in "Choosing Calibration Media" on page 8-15 Then click **Apply**.

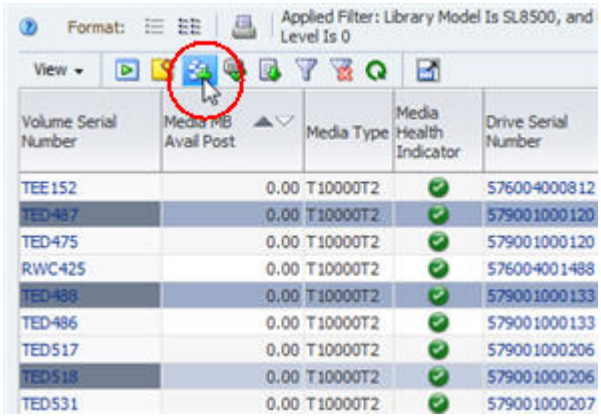


The table is updated to display only media that meet the criteria.

4. Sort the results by the Media MB Avail Post attribute to locate media with at least two wraps of written data.

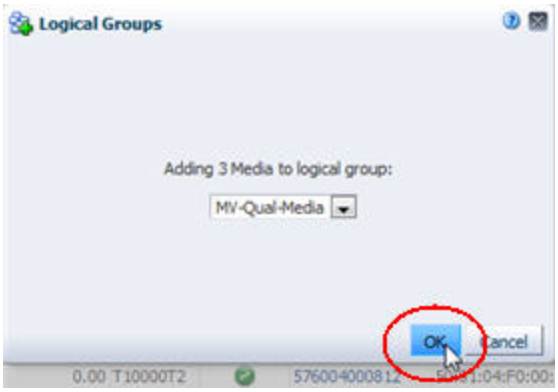


5. From the list, select the media you want to use for drive calibration and qualification. Then from the Table Toolbar, click **Logical Groups**.

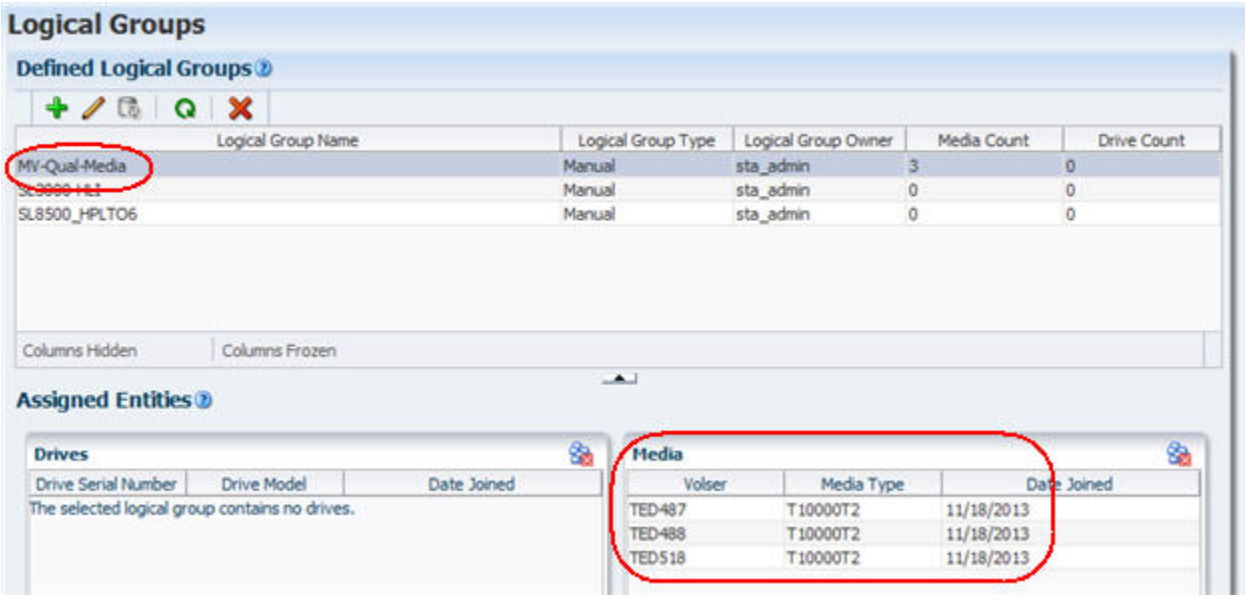


The Logical Groups dialog box appears.

6. In the menu, select the logical group you have created for the calibration media, and click **OK**.



The media are added to the logical group. You can display them on the Logical Groups screen. See "List All Drives and Media Assigned to a Logical Group" on page 7-24 for instructions.



Enable Drive Calibration and Qualification

Use this procedure to enable the optional drive calibration and qualification features on STA. These features are separate processes, but they are enabled and disabled together.

Note: It is highly recommended that you enable drive calibration and qualification if you are using STA media validation. See "Drive Calibration and Qualification" on page 8-10 for details on the benefits of these features.

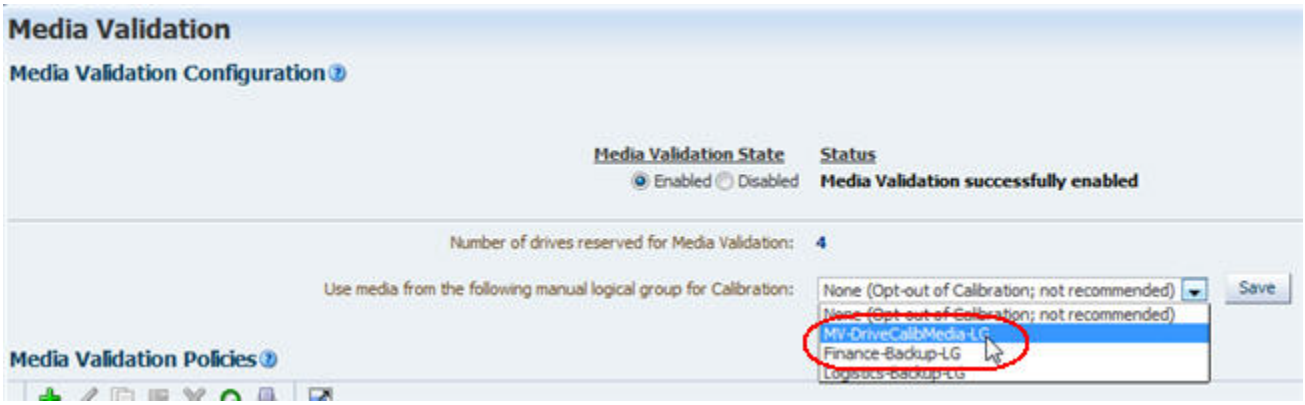
Note: Before using this procedure, you must create the calibration media logical group. See "Create the Calibration Media Logical Group" on page 8-31 for instructions.

Note: This procedure requires Administrator privileges.

1. In the Navigation Bar, select **Setup & Administration**, then select **Media Validation**.

The Media Validation screen appears.

2. In the **Use Media From the Following Manual Logical Group for Calibration** menu, select the logical group that includes the media you want to use for calibration and qualification. The menu lists manual logical groups only.



3. Verify your selection, and click **Save** to confirm.

Drive calibration and qualification are enabled, and STA begins calibrating drives in the media validation drive pool.

The new status is indicated on the screen. If calibration is successful, the screen displays the message, "Drive and Media Pool Setup Success--calibration has been successful." If there are any issues, they are also indicated.

Disable Drive Calibration and Qualification

Use this procedure to disable the optional drive calibration and qualification features on STA. These features are separate processes, but they are enabled and disabled together.

Note: It is highly recommended that you enable drive calibration and qualification if you are using STA media validation. See "Drive Calibration and Qualification" on page 8-10 for details on the benefits of these features.

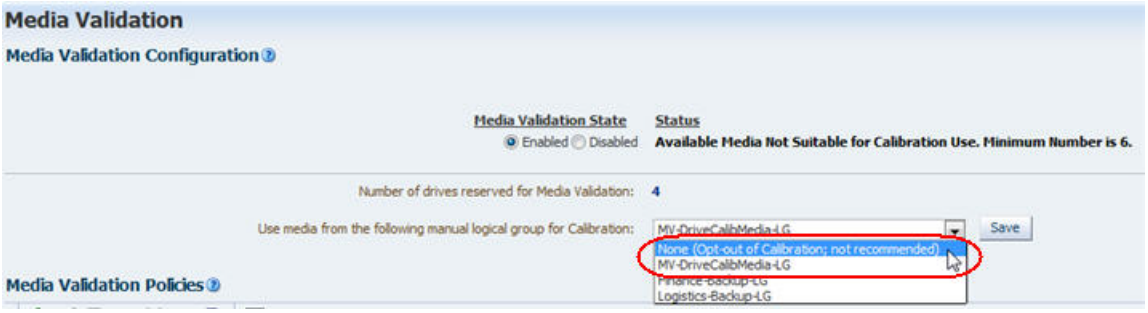
Note: This procedure requires Administrator privileges.

---

1. In the Navigation Bar, select **Setup & Administration**, then select **Media Validation**.

The Media Validation screen appears.

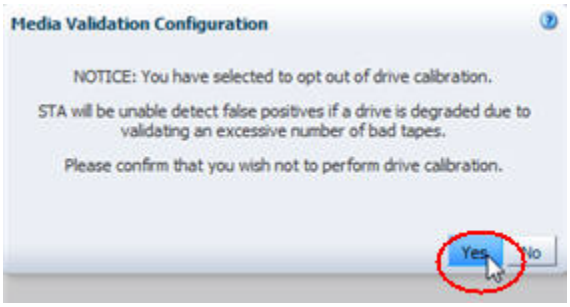
2. In the **Use Media From the Following Manual Logical Group for Calibration** menu, select None (Opt out of calibration; not recommended).



3. Verify your selection, and click **Save** to confirm.

The Media Validation Configuration dialog box appears.

4. Review the selection and click **Yes** to confirm that want to disable drive calibration and qualification.



Drive calibration is disabled, and STA does not begin any new calibration or qualification operations. Any in-progress calibration or qualification activities are processed to completion.

The new status is indicated on the screen. If there are any issues, they are also indicated.

Display the Media Validation Request Queue

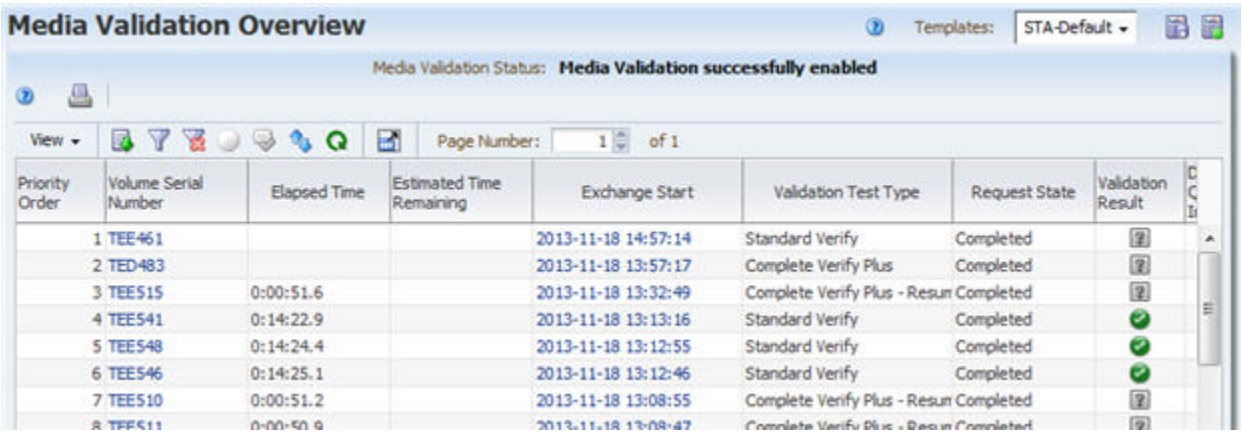
Use this procedure to display information about pending, in-progress, and completed media validation requests. See "Displaying the Status of Validation Requests" on page 8-21 for details.

Note: You can use this procedure even if media validation is disabled on STA.

Note: This procedure can be done by any user.

1. From the Navigation Bar, select **Tape System Activity**, then select **Media Validation Overview**.

The Media Validation Overview screen appears, displaying all validation requests for which STA has received information.



2. 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 more recent requests, you can either scroll to the bottom of the screen or select the **Descending Sort** arrow on the Priority Order column.
3. From this screen, you can manage the validation request queue by performing any of the following tasks:
   - "Submit Manual Media Validation Requests" on page 8-39
   - "Reorder Pending Media Validation Requests" on page 8-46
   - "Cancel Pending Media Validation Requests" on page 8-49
   - "Cancel In-Progress "Complete Verify" Validations" on page 8-51

   In addition, you can perform most of the same tasks as for any List View table. See the following procedures for instructions:
   - To display a printable form of the table in a separate browser tab or window, see the *STA Screen Basics Guide*. "
   - To export the list of media validation requests, see the *STA Screen Basics Guide*."
   - To filter the table records, see "Use the Filter Data Dialog Box to Change a Table Filter" on page 4-9.
   - To reset a filter applied to the table, see "Clear the Current Filter" on page 4-12.
   - To refresh the table to display any new requests, see the *STA Screen Basics Guide*"

- To detach the table from the screen and display it in a separate window in the browser foreground, see the *STA Screen Basics Guide*."

Submit Manual Media Validation Requests

Use this procedure to manually submit media validation requests to the validation request queue. You can use this procedure as soon as media validation is enabled on STA. See "Submitting Manual Validation Requests" on page 8-17 for details.

You can use this procedure to start new validations or to resume validations that were previously interrupted. The option to resume interrupted validations is available only if *all* of the following conditions are true:

- You have selected T10000T2 media for validation. (T10000T1 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 validations for some or all of the selected media are not 100 percent complete. (Media for which the most recent validation was complete are always validated from the beginning of tape.)

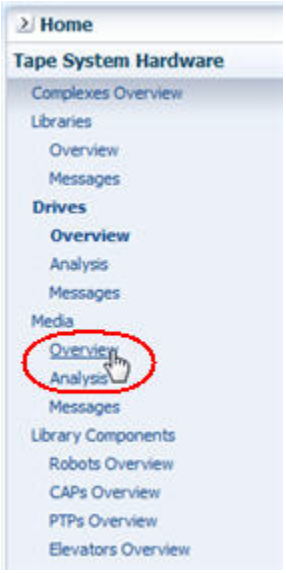
You can perform this procedure using either of the following methods:

- "From the Media – Overview Screen" on page 8-39. Using this method, you can submit multiple requests at once.
- "From the Media Validation Overview Screen" on page 8-43. Using this method, you can submit only one request at a time.

From the Media – Overview Screen

Note: This method can be done by any user.

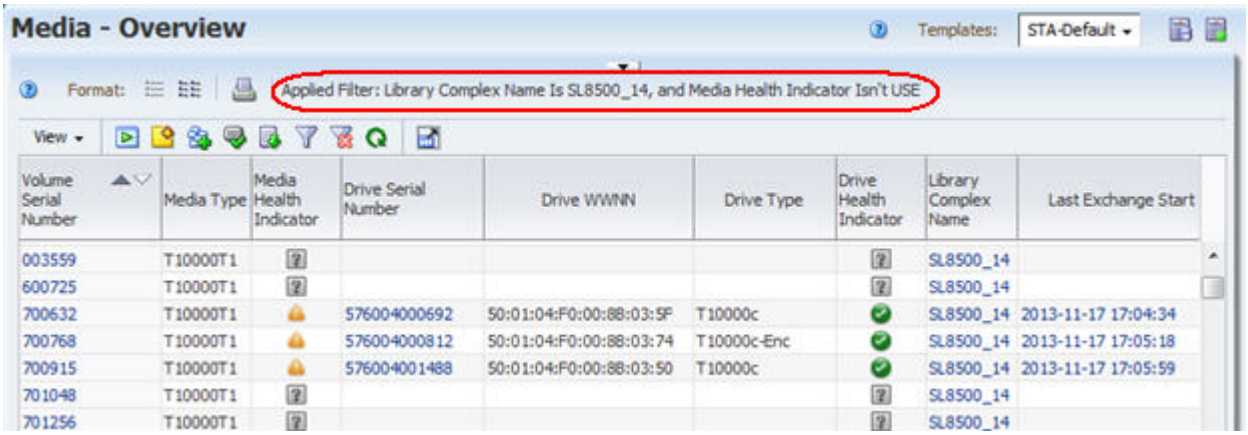
1. From the Navigation Bar, select **Tape System Hardware**, then select **Media Overview**.



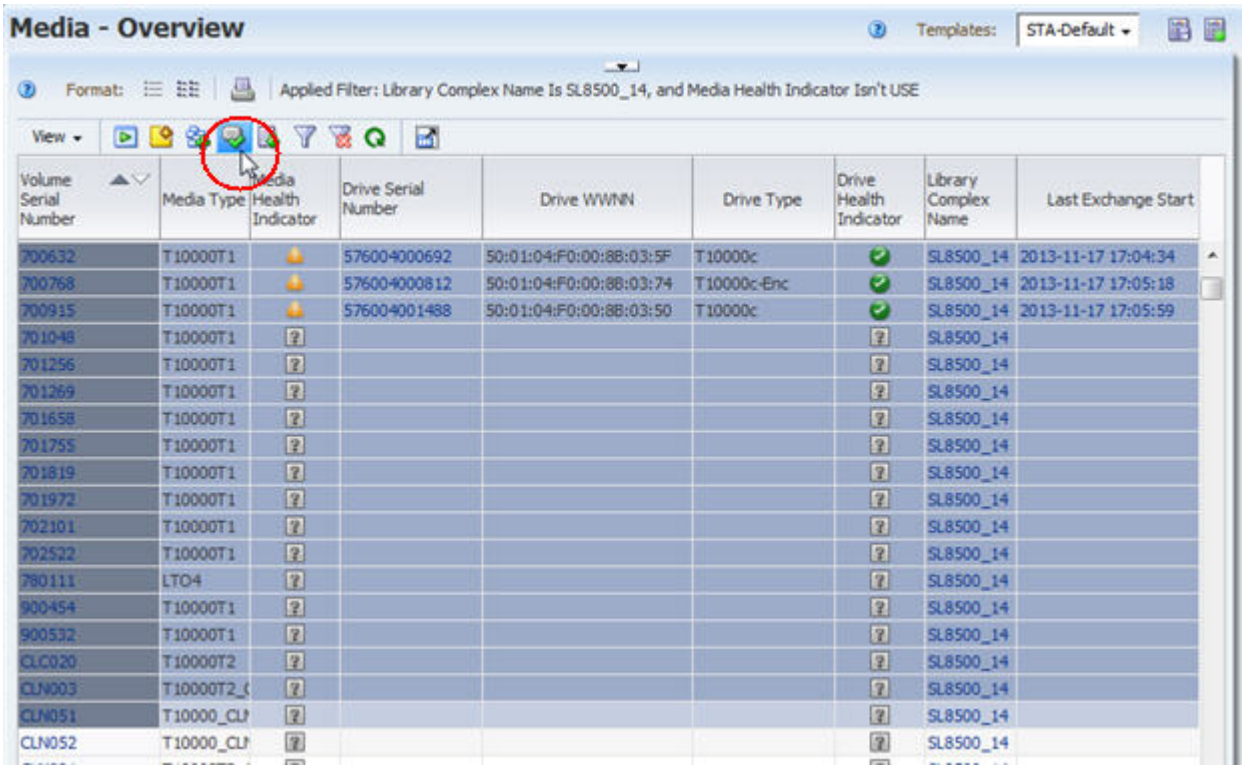
The Media – Overview screen appears, displaying all media in your tape library system.

2. Apply appropriate filter criteria to narrow down the list of media. In the following example, the screen is filtered to show media with "Library Complex Name Is SL8500_14, and Media Health Indicator Isn't USE."

Note: You may want to use the STA-Media-MV predefined template because it filters the screen to show only T10000-type media in SL3000 and SL8500 libraries.



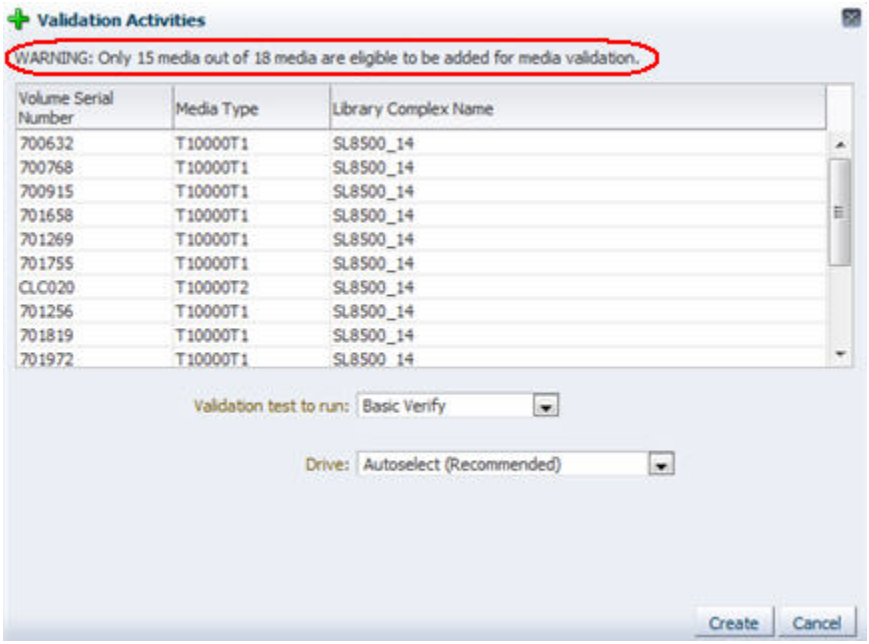
3. Select the media you want to validate. You can use multi-select to select as many media as you want. Then click **Media Validation** in the Table Toolbar.



The Validation Activities dialog box appears. A message indicates the total number of media eligible for validation, and the eligible media are listed. Media may be ineligible for any of the following reasons:

- The media are not T10000 type.
- The media are cleaning media.
- The media are not in an SL3000 or SL8500 standalone library or complex.
- Drives in the library or complex validation drive pool are not compatible with the media.
- Drives in the validation drive pool do not meet minimum requirements for STA media validation.

Note: If none of the selected media are eligible for validation, the message, "No valid media selected for validation" is displayed.



4. In the **Validation test to run** menu, select the type of verification test you want to perform. See "Types of Verification Tests" on page 8-3 for details about the options.

   If you select **Complete Verify** or **Complete Verify Plus**, you may also be required to select one of the following options. These options are available only if you are performing Complete Verify or Complete Verify Plus validations on T10000T2 media, and the most recent validations for these media were interrupted prior to completion.

   – **Perform validations from beginning of tape** – Indicates you want T10000T2 media to be validated from the beginning of tape (BOT).

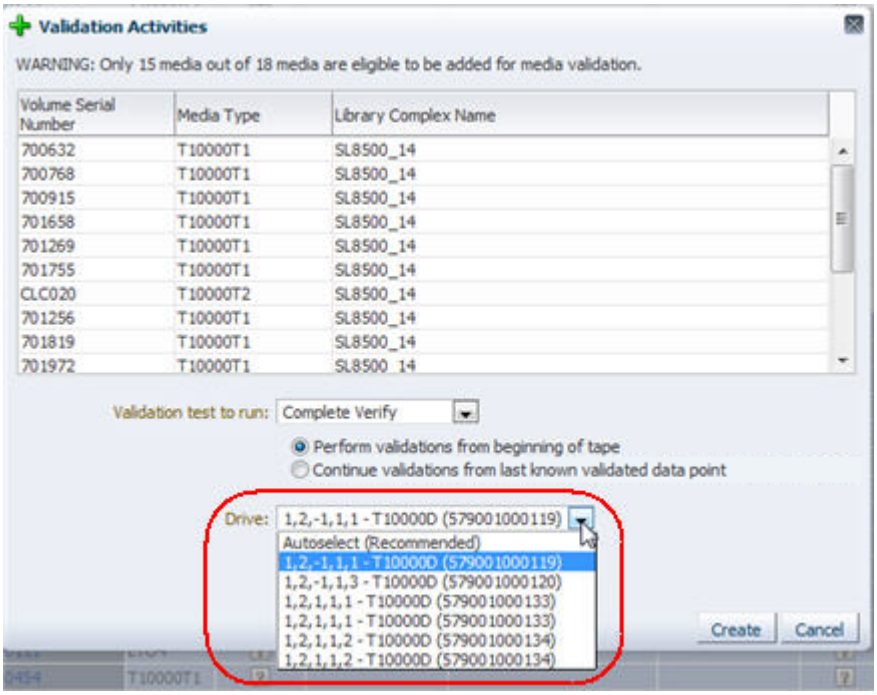
   – **Continue validations from last known validated data point** – Indicates you want testing of T10000T2 media that has been partially validated to resume where the previous validation left off, if the drive can determine this from the media RFID chip. If the drive cannot determine where the previous validation left off, it will start from the beginning of tape.

See "Resuming Interrupted "Complete Verify" Tests on T10000T2 Media" on page 8-24 for details on these options.

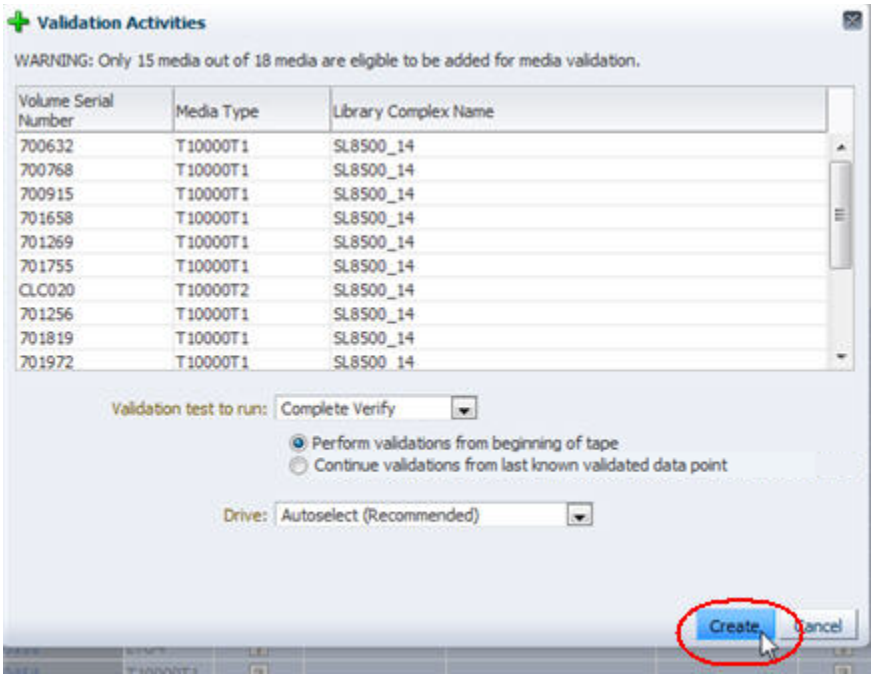
5. In the **Drive** menu, select the drive you want to use for the validations. This option is available only if the media you have selected all reside within the same library complex or standalone library. The menu lists the validation drives in the complex or standalone library.

Note: You select just one drive, which means all media will be validated by the same drive, if possible. If the drive is not compatible with some media—for example, you have selected to perform a Complete Verify Plus, and some of the media are 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.

Consequently, it is recommended that you choose Autoselect, which causes STA to automatically select a compatible validation drive for each media.



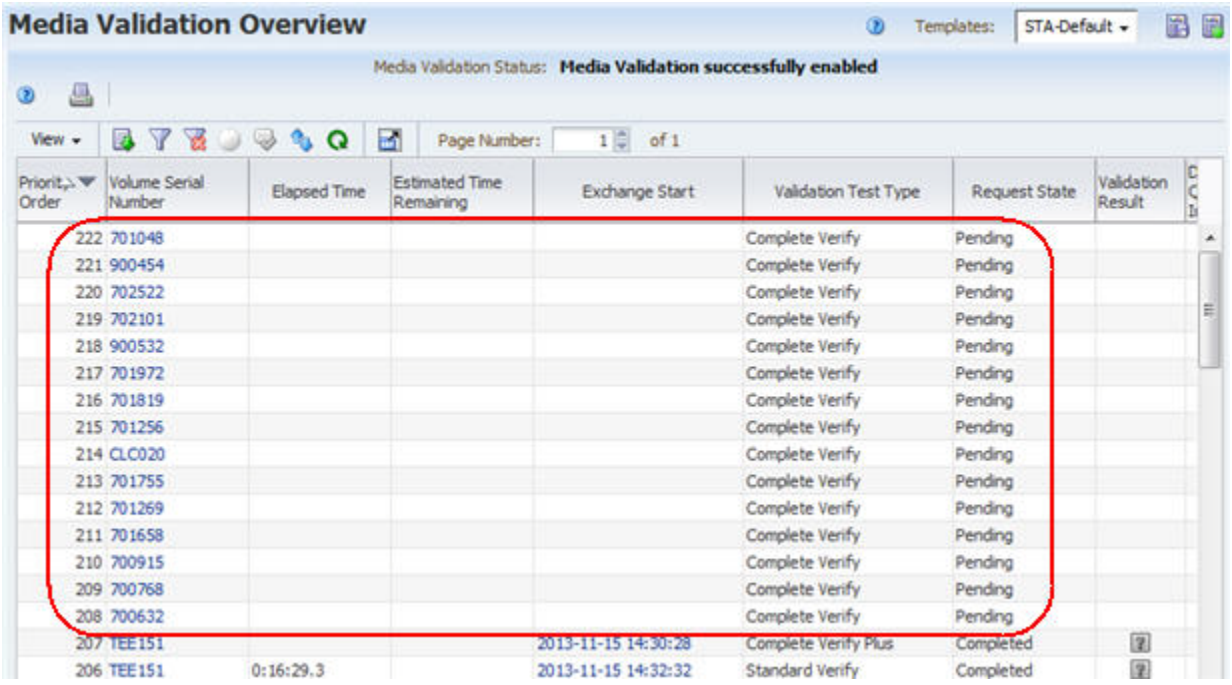
6. Click **Create**.



The validation requests are generated and added to the validation request queue.

7. You can view the requests on the Media Validation Overview screen. See "Display the Media Validation Request Queue" on page 8-37 for instructions.

   By default, each request is assigned the next available Priority Order as it is generated. See "Reorder Pending Media Validation Requests" on page 8-46 for instructions on reprioritizing them.



From the Media Validation Overview Screen

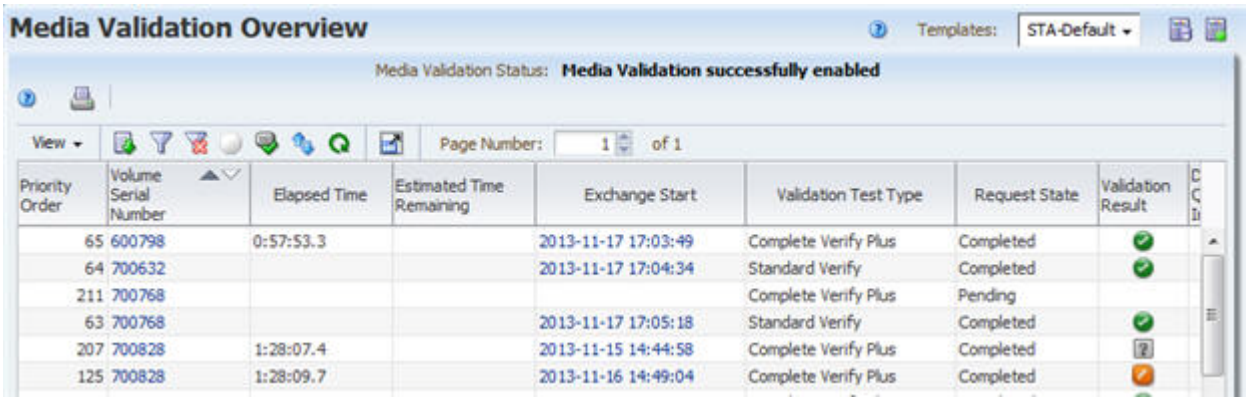
Using this method, you can submit only one request at a time. To submit multiple requests at once, see "From the Media – Overview Screen" on page 8-39.

Note: This method requires Operator or Administrator privileges.

1. From the Navigation Bar, select **Tape System Activity**, then select **Media Validation Overview**.

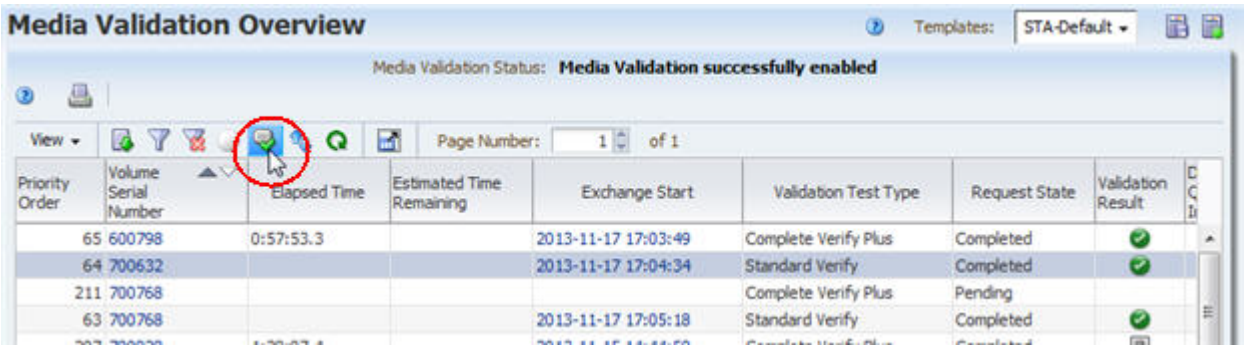
   The Media Validation Overview screen appears. By default, the screen is displayed in ascending Priority Order.

2. If you want to sort the screen by Volume Serial Number, select the **Ascending Sort** or **Descending Sort** arrow in that column.



3. Select the media you want to validate by selecting the request record. Then click **Media Validation** in the Table Toolbar.

Note: You can select only one record at a time, and you cannot select media with pending or in-progress validation requests.



The Resubmit Media dialog box appears.

4. In the **Validation test to run** menu, select the type of verification test you want to perform. By default, this field is set to Basic Verify, but you can choose any appropriate verification test for this media. See "Types of Verification Tests" on page 8-3 for details about the options.

   If you select **Complete Verify** or **Complete Verify Plus**, you may also be required to select one of the following options. These options are available only if you are performing a Complete Verify or Complete Verify Plus validation on a T10000T2 media, and the most recent validation for the media was interrupted prior to completion.

   – **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 "Resuming Interrupted "Complete Verify" Tests on T10000T2 Media" on page 8-24 for details on these options.

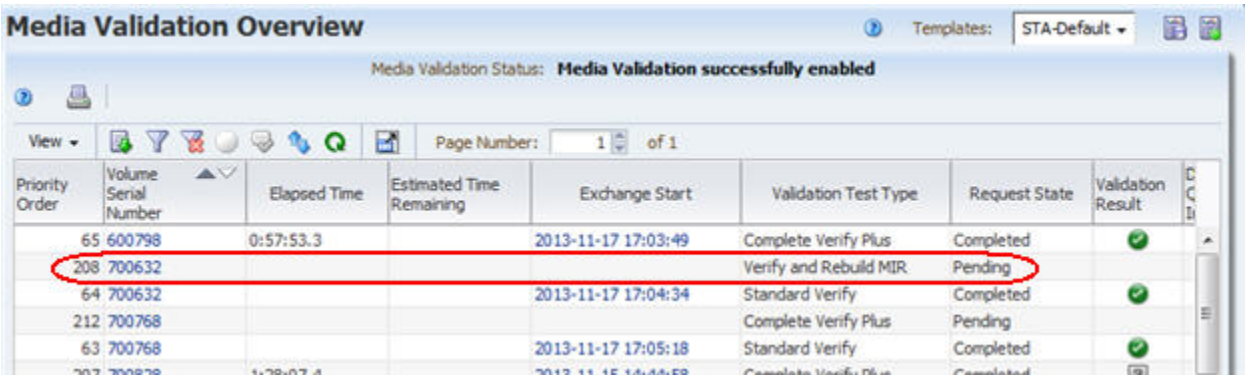
5. In the **Drive** menu, select the drive you want to use for the validation. The menu lists the validation drives in the complex or standalone library where the selected media currently resides.

   Note: If the drive you select is not compatible with the media—for example, you have selected to perform a Complete Verify Plus, and the media is encrypted but the drive is not encryption capable—the validation request will be added to the request queue, but it will remain in a pending state.

   Consequently, it is recommended that you choose Autoselect, which causes STA to automatically select a compatible validation drive for the media.

6. Click **OK**.

The request is generated and added to the validation request queue. By default, it is assigned the next available Priority Order. See "Reorder Pending Media Validation Requests" on page 8-46 for instructions on reprioritizing the request.



Reorder Pending Media Validation Requests

Use this procedure to reprioritize pending requests in the media validation request queue. See "Media Validation Request Priorities" on page 8-22 for details.

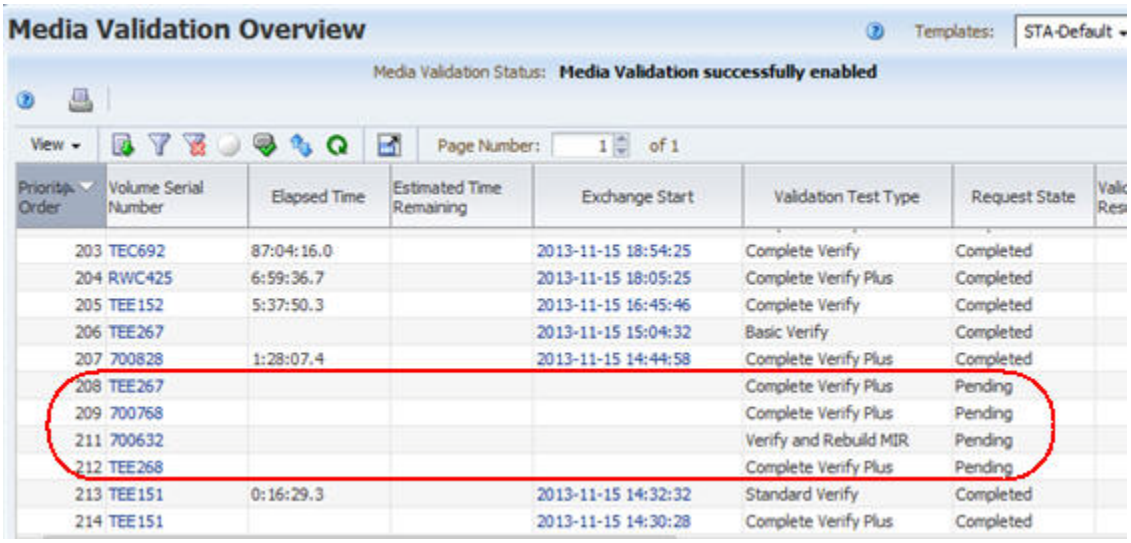
Note: You can use this procedure even if media validation is disabled on STA. For example, you may disable media validation for library maintenance and then reprioritize the pending requests left in the validation queue so they will be processed in a different order when media validation is reenabled.

Note: This procedure can be done by any user.

1. From the Navigation Bar, select **Tape System Activity**, then select **Media Validation Overview**.

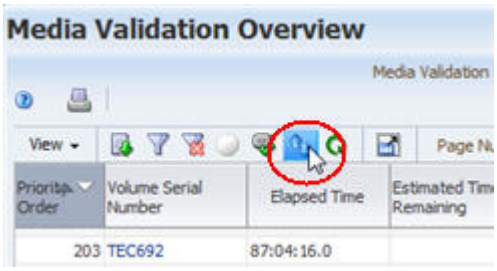
The Media Validation Overview screen appears.

2. By default, the requests are sorted in ascending Priority Order. To see more recent requests, scroll to the bottom of the screen. Note the pending requests.

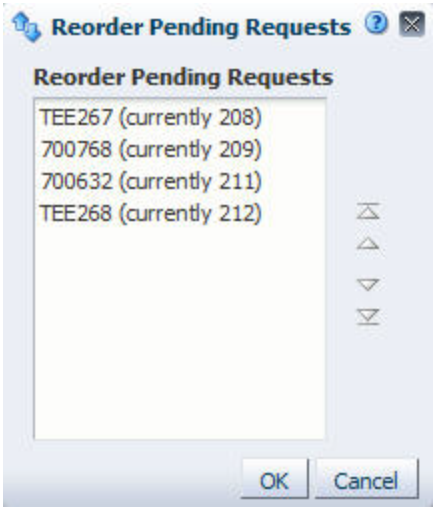


Priority Order	Volume Serial Number	Elapsed Time	Estimated Time Remaining	Exchange Start	Validation Test Type	Request State
203	TEC692	87:04:16.0		2013-11-15 18:54:25	Complete Verify	Completed
204	RWC425	6:59:36.7		2013-11-15 18:05:25	Complete Verify Plus	Completed
205	TEE152	5:37:50.3		2013-11-15 16:45:46	Complete Verify	Completed
206	TEE267			2013-11-15 15:04:32	Basic Verify	Completed
207	700828	1:28:07.4		2013-11-15 14:44:58	Complete Verify Plus	Completed
208	TEE267				Complete Verify Plus	Pending
209	700768				Complete Verify Plus	Pending
211	700632				Verify and Rebuild MIR	Pending
212	TEE268				Complete Verify Plus	Pending
213	TEE151	0:16:29.3		2013-11-15 14:32:32	Standard Verify	Completed
214	TEE151			2013-11-15 14:30:28	Complete Verify Plus	Completed

3. Click **Reorder Pending Requests** in the Table Toolbar.

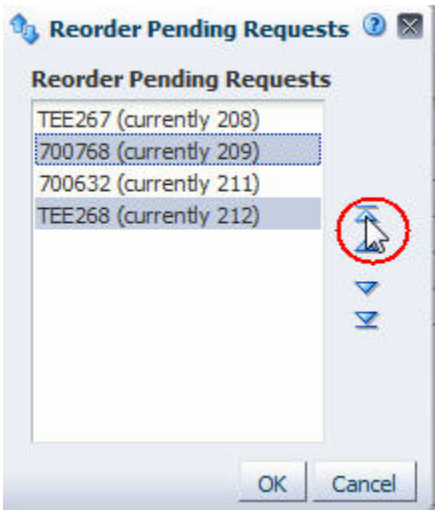


The Reorder Pending Requests dialog box appears, with all pending requests listed in their current priority order. The requests are identified by the media Volume Serial Number and the current Priority Order.

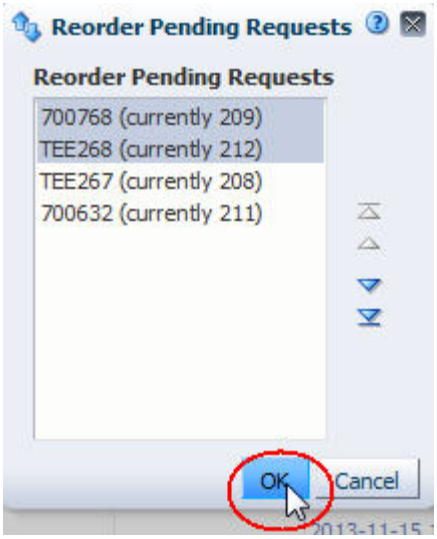


4. Select the requests you want to reprioritize, and click the appropriate arrows to move them in the list. This dialog box supports multi-select.

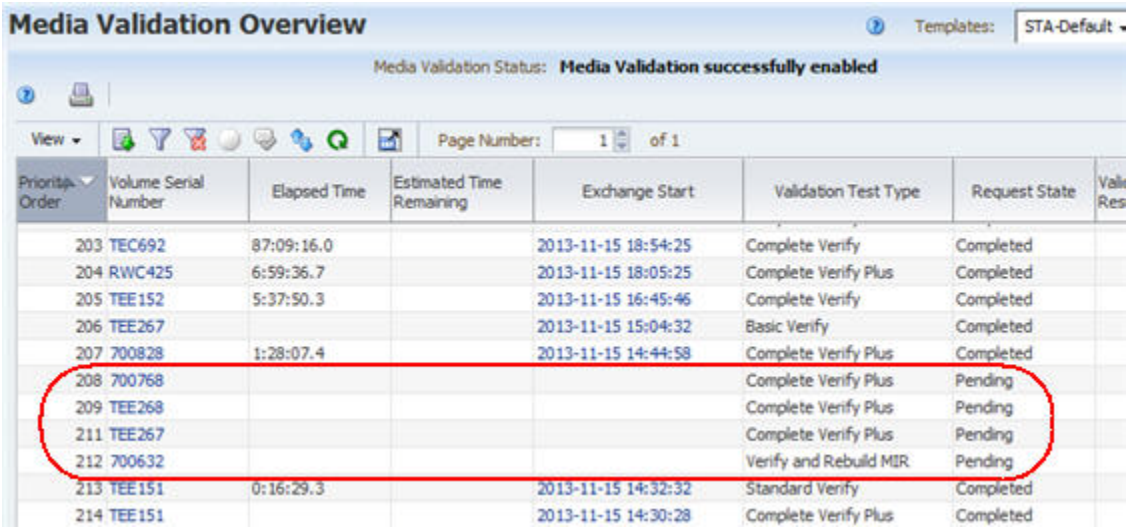
Arrows	Description
or	Move the selected item(s) up or down, one place at a time.
or	Move the selected item(s) to the top or bottom of the list.



5. When the requests are in the order you want, click **OK**.



The requests are reordered according to your selections, and the Priority Order values are updated on the Media Validation Overview screen to reflect the new order.



Cancel Pending Media Validation Requests

Use this procedure to cancel one or more pending media validation requests. Canceled pending requests are immediately removed from the validation request queue, and they cannot be resubmitted. See "Canceling Pending or In-Progress Validation Requests" on page 8-24 for details.

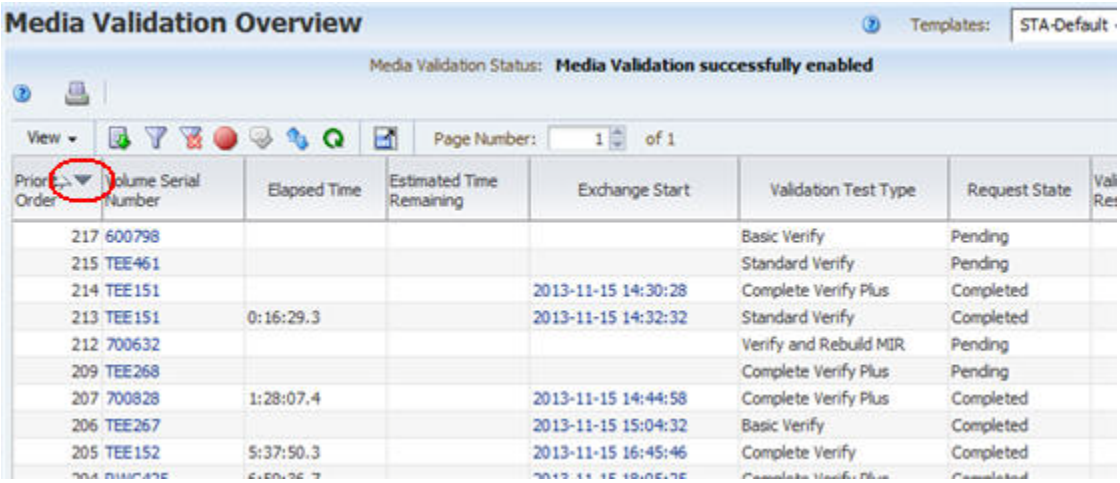
Note: You can use this procedure even if media validation is disabled on STA. For example, you may disable media validation for library maintenance and then cancel the pending requests left in the validation queue.

Note: This procedure can be done by any user.

1. From the Navigation Bar, select **Tape System Activity**, then select **Media Validation Overview**.

   The Media Validation Overview screen appears.

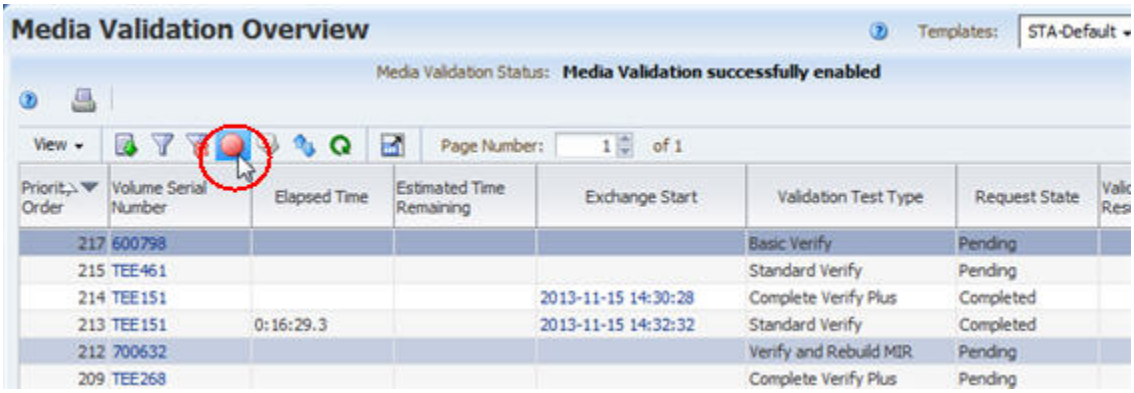
2. By default, the requests are sorted in ascending Priority Order. To see more recent requests, select the **Descending Sort** arrow on the Priority Order column. Note the pending requests.



Priority Order	Volume Serial Number	Elapsed Time	Estimated Time Remaining	Exchange Start	Validation Test Type	Request State
217	600798				Basic Verify	Pending
215	TEE461				Standard Verify	Pending
214	TEE151			2013-11-15 14:30:28	Complete Verify Plus	Completed
213	TEE151	0:16:29.3		2013-11-15 14:32:32	Standard Verify	Completed
212	700632				Verify and Rebuild MIR	Pending
209	TEE268				Complete Verify Plus	Pending
207	700828	1:28:07.4		2013-11-15 14:44:58	Complete Verify Plus	Completed
206	TEE267			2013-11-15 15:04:32	Basic Verify	Completed
205	TEE152	5:37:50.3		2013-11-15 16:45:46	Complete Verify	Completed

3. Select the requests you want to cancel, and click **Cancel** in the Table Toolbar. You can select any number of pending requests.

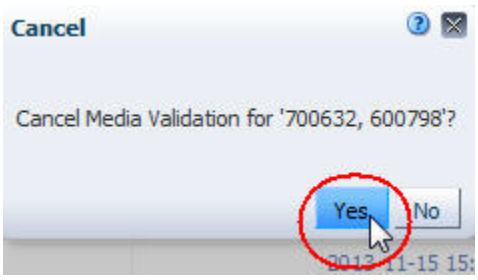
> **Note:** The **Cancel** button does not activate if you select any completed validations.



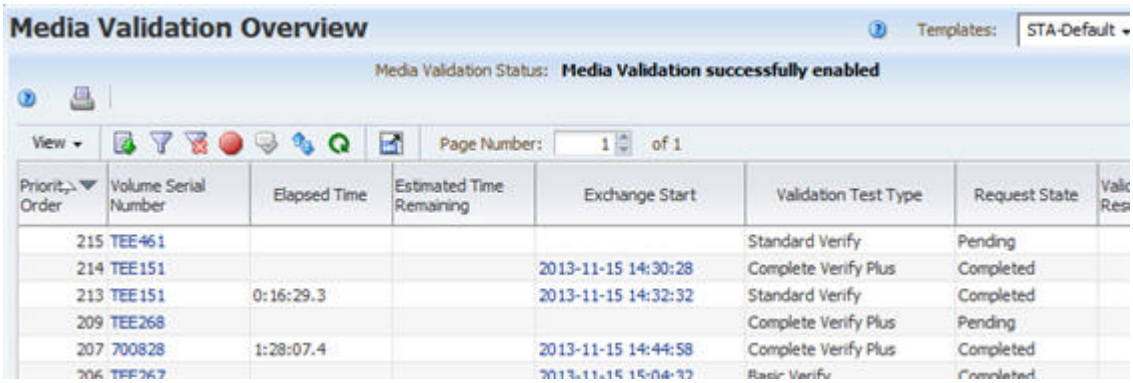
Priority Order	Volume Serial Number	Elapsed Time	Estimated Time Remaining	Exchange Start	Validation Test Type	Request State
217	600798				Basic Verify	Pending
215	TEE461				Standard Verify	Pending
214	TEE151			2013-11-15 14:30:28	Complete Verify Plus	Completed
213	TEE151	0:16:29.3		2013-11-15 14:32:32	Standard Verify	Completed
212	700632				Verify and Rebuild MIR	Pending
209	TEE268				Complete Verify Plus	Pending

The Cancel dialog box appears, listing the volume serial numbers of the requests you have selected.

4. Verify the list of volume serial numbers and click **Yes** to confirm the cancellations.



The requests are canceled and removed from the Media Validation Overview screen.



Cancel In-Progress "Complete Verify" Validations

Use this procedure to cancel one or more in-progress Complete Verify or Complete Verify Plus media validations. You cannot cancel other in-progress validation types. See "Canceling Pending or In-Progress Validation Requests" on page 8-24 for details.

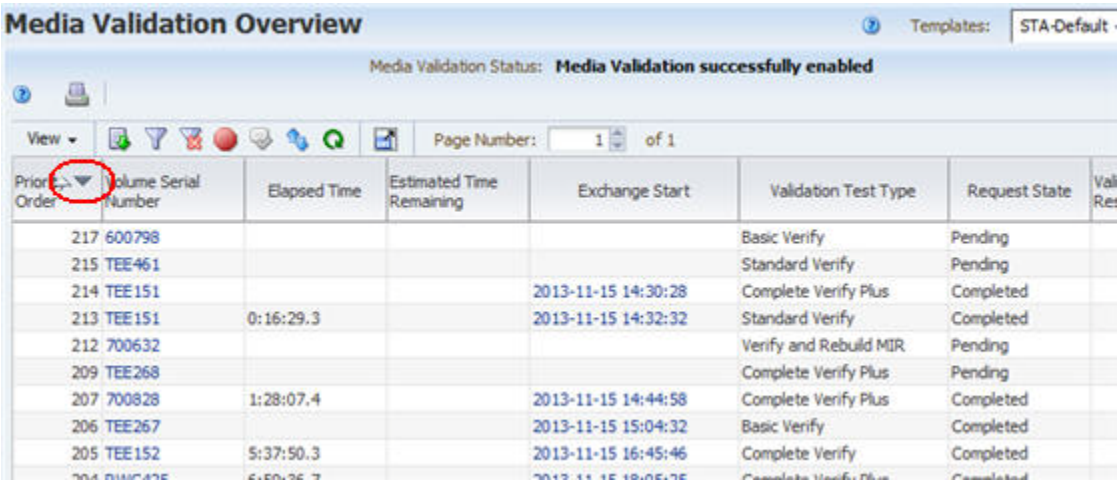
Note: You can use this procedure even if media validation is disabled on STA. For example, you may disable media validation for library maintenance and then cancel the in-progress Complete Verify requests left in the validation queue.

Note: This procedure can be done by any user.

1. From the Navigation Bar, select **Tape System Activity**, then select **Media Validation Overview**.

The Media Validation Overview screen appears.

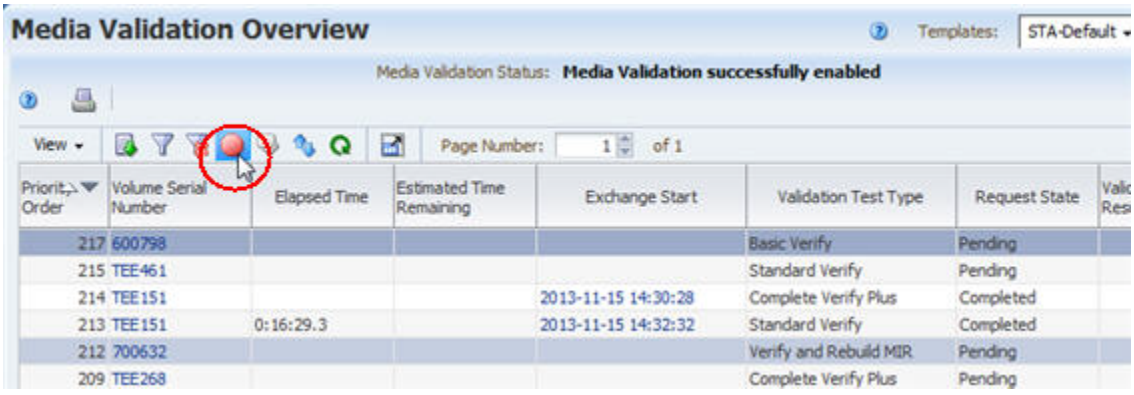
2. By default, the requests are sorted in ascending Priority Order. To see more recent requests, select the **Descending Sort** arrow on the Priority Order column. Note the in-progress validations.



Priority Order	Volume Serial Number	Elapsed Time	Estimated Time Remaining	Exchange Start	Validation Test Type	Request State
217	600798				Basic Verify	Pending
215	TEE461				Standard Verify	Pending
214	TEE151			2013-11-15 14:30:28	Complete Verify Plus	Completed
213	TEE151	0:16:29.3		2013-11-15 14:32:32	Standard Verify	Completed
212	700632				Verify and Rebuild MIR	Pending
209	TEE268				Complete Verify Plus	Pending
207	700828	1:28:07.4		2013-11-15 14:44:58	Complete Verify Plus	Completed
206	TEE267			2013-11-15 15:04:32	Basic Verify	Completed
205	TEE152	5:37:50.3		2013-11-15 16:45:46	Complete Verify	Completed

3. Select the validations you want to stop, and click **Cancel** in the Table Toolbar. You can select any number of in-progress Complete Verify or Complete Verify Plus validations.

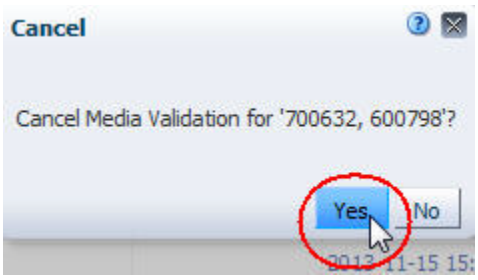
Note: The **Cancel** button does not activate if you select any completed validations.



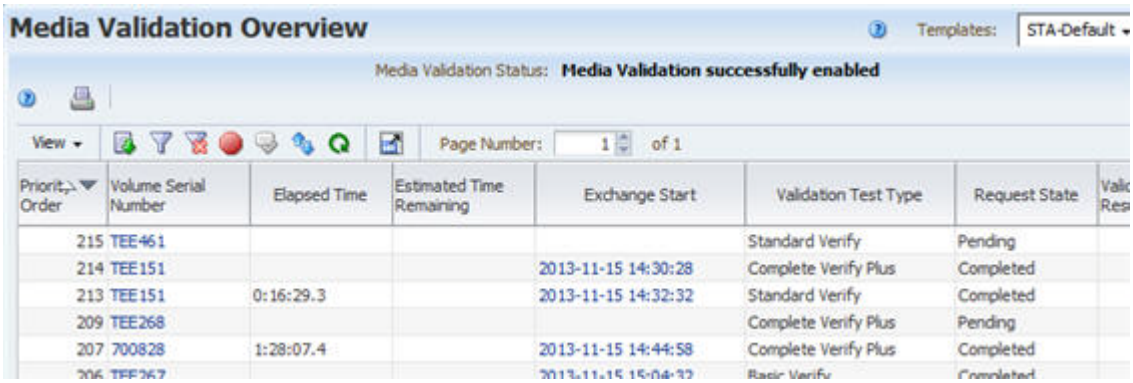
Priority Order	Volume Serial Number	Elapsed Time	Estimated Time Remaining	Exchange Start	Validation Test Type	Request State
217	600798				Basic Verify	Pending
215	TEE461				Standard Verify	Pending
214	TEE151			2013-11-15 14:30:28	Complete Verify Plus	Completed
213	TEE151	0:16:29.3		2013-11-15 14:32:32	Standard Verify	Completed
212	700632				Verify and Rebuild MIR	Pending
209	TEE268				Complete Verify Plus	Pending

The Cancel dialog box appears, listing the volume serial numbers of the validations you have selected.

4. Review the information displayed and click **Yes** to confirm the cancellation.



STA issues cancellation requests to the drives. This process may take several minutes to complete. Once each media has been dismounted from the drive and returned to a media slot, the associated validation request is removed from Media Validation Overview screen.



Create a Media Validation Policy

Use this procedure to create a media validation policy. Media validation policies allow you to automate media validation in your tape library system. See "Using Automated Media Validation" on page 8-19 for details.

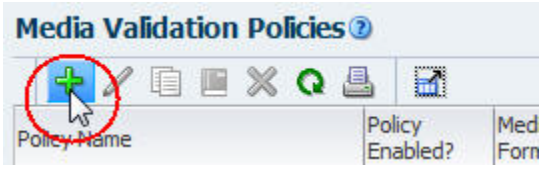
The Media Validation Policies wizard leads you through the steps to define all information for the policy.

Note: This procedure requires Administrator privileges.

1. In the Navigation Bar, select **Setup & Administration**, then select **Media Validation**.

The Media Validation Policies screen appears.

2. Click **New Media Validation Policy**.



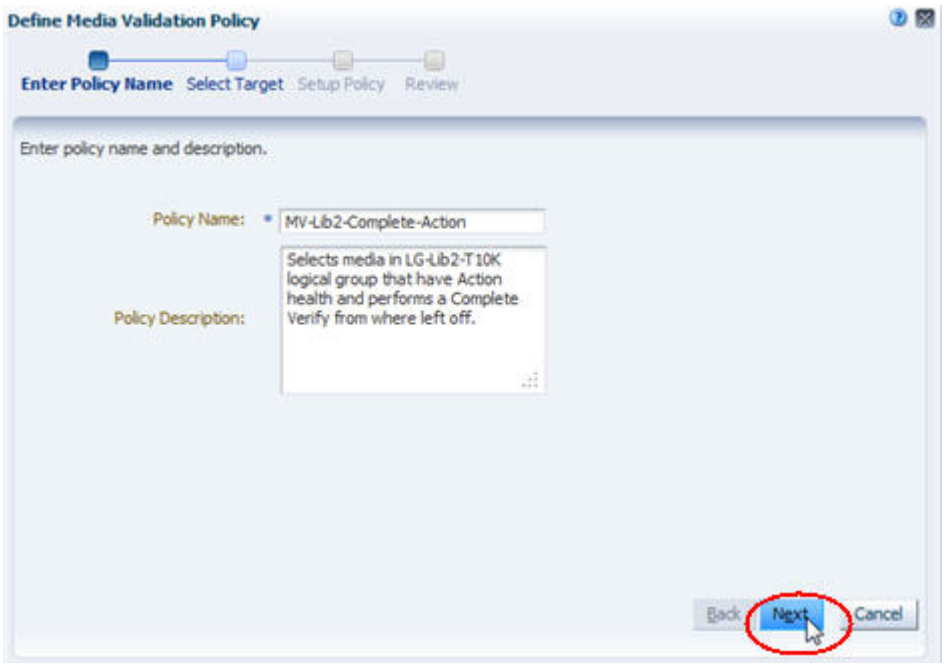
The Media Validation Policies wizard appears.

3. Complete the first screen of the wizard as follows:
   a. In the **Policy Name** field, type a unique name.

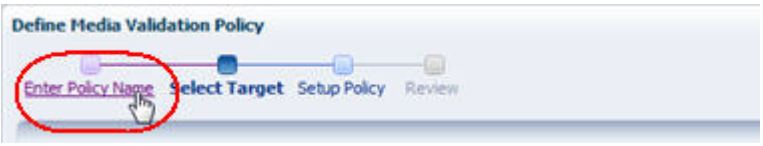
      Your entry can include any alphanumeric characters up to 250 characters in length.

   b. In the **Policy Description** field, enter an optional description of the policy.

   c. Click **Next**.



Note: On any screen of the wizard, you can select the breadcrumb links at the top of the screen to go directly to the immediate-next screen or any screen you have already visited.



4. On the second screen of the wizard, you indicate the group of media you want this policy to validate, as follows:

   - If you want this policy to validate media using a specific recording format, optionally within a specific library complex, select the **Select media format and optional library complex** option, and complete the associated fields as follows:

     – In the **Media Format** menu, select the media recording formats you want this policy to validate. You can select as many formats as you want. Options are: T10000A and T10000B, which are available for T10000T1 media; T10000C and T10000D, which are available for T10000T2 media.

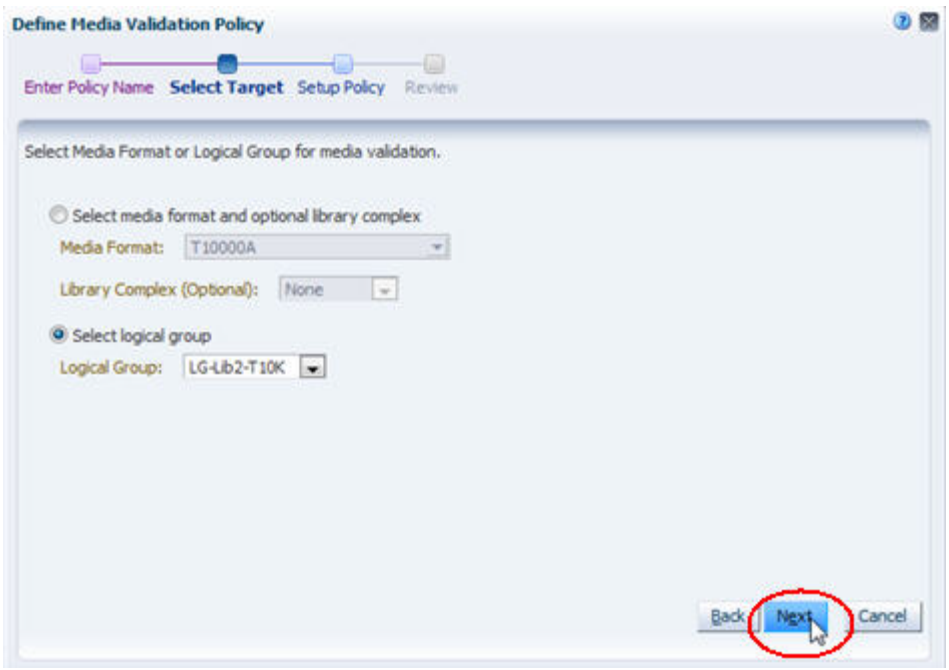
     – In the **Library Complex (Optional)** menu, select the library complex you want this policy to validate. If you select **None**, the policy will validate the specified media types across all complexes. If you select a library complex, the policy will validate media within that complex only.

   - If you want this policy to validate media in a specific predefined logical group, select the **Select logical group** option. In the **Logical Group** menu, select the logical group. The menu lists all logical groups that have been defined.

Note: Be sure to select a logical group that includes T10000 media in SL8500 complexes or standalone SL3000 or SL8500 libraries with validation drives, as 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 used; compatible drives are always selected from the validation drive pool defined through SL Console (see "Preparing for STA Media Validation" on page 8-5 for details).

5. Click **Next**.



6. Complete the third screen of the wizard as follows:

   a. In the **Policy Criteria** menu, select the criteria by which media will be selected for validation. See "Selection Criteria for Validation Policies" on page 8-21 for descriptions of the options.

      Depending on your selection, you may need to complete additional fields, as follows:

      – If you select Media Health = Action, Evaluate, or Monitor, you must also specify the successive **Number of exchanges** that must occur before a media is selected for validation. Options are 1–5. For example, if you specify "2", media are selected for validation as soon as two successive exchanges occur with the indicated media health.

      – If you select Extended period of non-use, you must also specify the **Number of days**. Options are 365–1095 (one to three years). For example, if you specify "730", media are selected for validation if 730 days or more have passed since their last exchange.

   b. In the **Validation Test Type** menu, select the type of verification test you want the drive to perform. See "Types of Verification Tests" on page 8-3 for descriptions of the options.

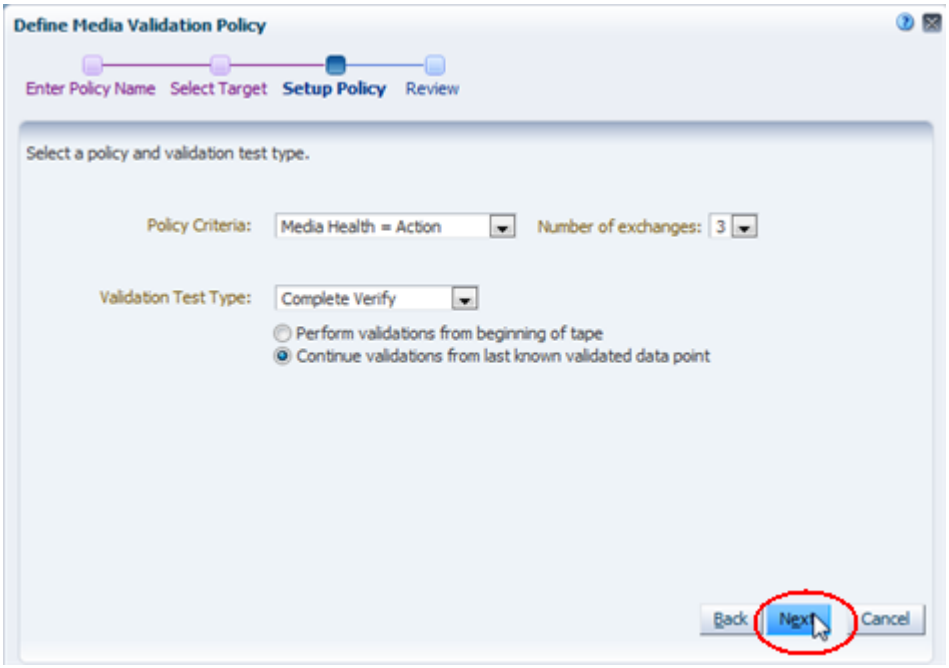
If you select **Complete Verify** or **Complete Verify Plus**, you must also select one of the following options.

Note: These options apply only to T10000T2 media; validations of T10000T1 media must always start at the beginning of tape (BOT).

- **Perform validations from beginning of tape** – Indicates you want testing of all T10000T2 media to start from the beginning of tape (BOT), even if the media has already been partially validated.
- 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 (BOT).

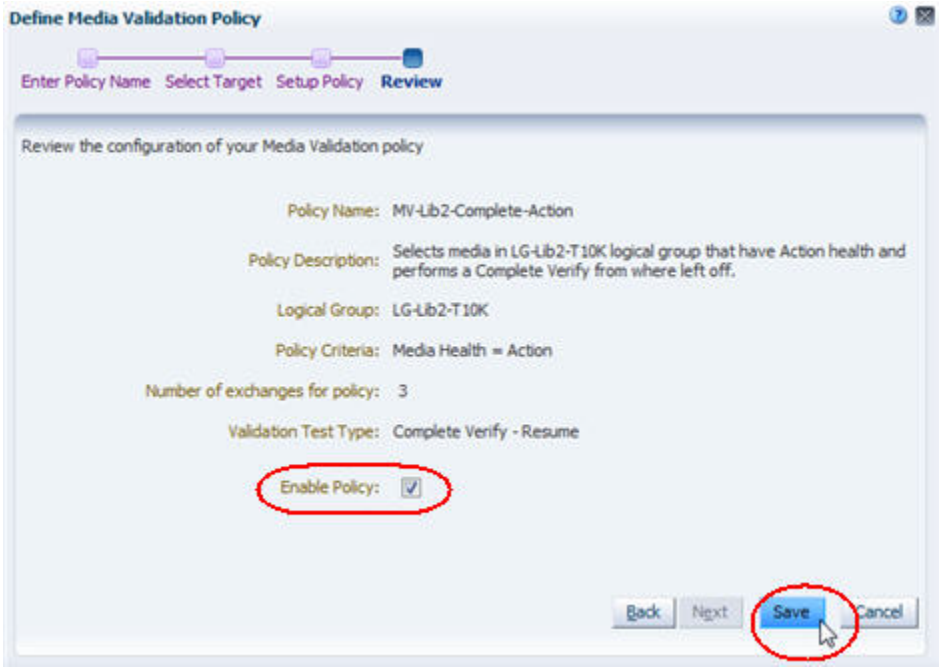
See "Resuming Interrupted "Complete Verify" Tests on T10000T2 Media" on page 8-24 for details on these options.

c. Click **Next**.



7. Complete the last screen of the wizard as follows:
   a. Verify that all the policy information is correct.
   b. Complete the **Enable Policy** check box 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. You can enable it at a later time. See "Enable or Disable a Media Validation Policy" on page 8-59 for instructions.

   c. Click **Save**.



The policy is created. If the policy is enabled, then STA immediately begins evaluating media against the policy and generating media validation requests as appropriate.

If the policy is disabled, then the policy is not evaluated for now.

Display the List of Media Validation Policies

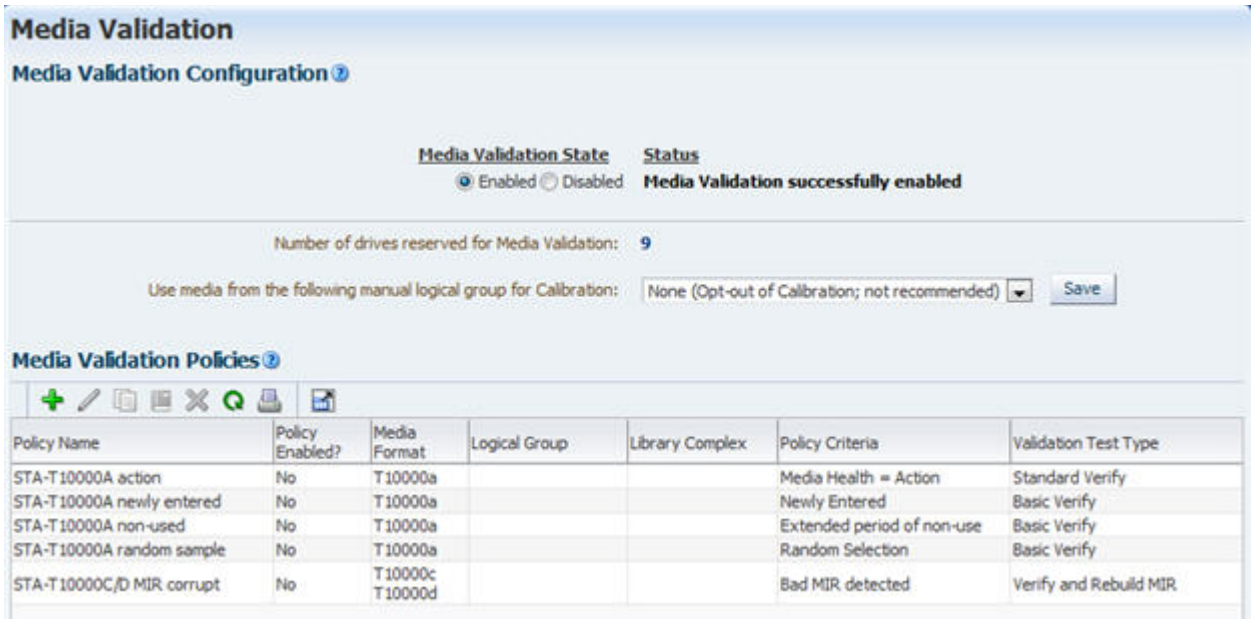
Use this procedure to display information about all STA media validation policies.

Note: These procedures require Operator or Administrator privileges.

---

1. In the Navigation Bar, select **Setup & Administration**, then select **Media Validation**.

The Media Validation Policies screen appears. The defined policies are listed in the Media Validation Policies section.



2. From this screen, you can manage validation policies by performing any of the following tasks:

   - "Enable or Disable a Media Validation Policy" on page 8-59
   - "Copy a Media Validation Policy" on page 8-61
   - "Modify a Media Validation Policy" on page 8-62
   - "Delete a Media Validation Policy" on page 8-64

   In addition, you can perform most of the same tasks as for any List View table. See the following procedures for instructions:

   - To display a printable form of the table in a separate browser tab or window, see the *STA Screen Basics Guide*. "
   - To export the list of media validation policies, see the *STA Screen Basics Guide*."
   - To filter the table records, see "Use the Filter Data Dialog Box to Change a Table Filter" on page 4-9.
   - To reset a filter applied to the table, see "Clear the Current Filter" on page 4-12.
   - To refresh the table to display any new policies, see the *STA Screen Basics Guide*"
   - To detach the table from the screen and display it in a separate window in the browser foreground, see the *STA Screen Basics Guide*."

Enable or Disable a Media Validation Policy

Use this procedure to enable or disable a selected media validation policy. STA uses only enabled policies to generate automated media validation requests. See "Using Automated Media Validation" on page 8-19 for details.

Disabling a policy does not affect any pending or in-progress media validation requests generated from the policy; they are processed to completion unless you cancel them.

Note: This procedure requires Administrator privileges.

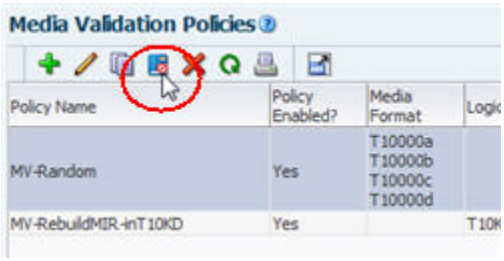
1. In the Navigation Bar, select **Setup & Administration**, then select **Media Validation**.

   The Media Validation Policies screen appears.

2. Select the policy you want to modify.

   If the policy is currently enabled, the **Disable Media Validation Policy** icon in the Media Validation Policies toolbar becomes active. If the policy is currently disabled, the **Enable Media Validation Policy** icon becomes active.

3. Click **Enable Media Validation Policy** or **Disable Media Validation Policy**, as applicable.



   The policy is updated to according to your selection.

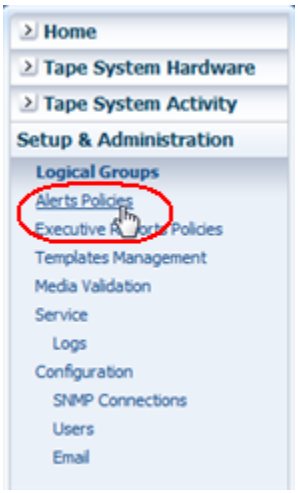
   - If you have enabled the policy, STA immediately begins evaluating media against the policy criteria and generating media validation requests, as appropriate.
   - If you have disabled the policy, STA no longer generates media validation requests for the policy. Any pending or in-progress media validation requests are processed to completion unless you cancel them. See "Canceling Pending or In-Progress Validation Requests" on page 8-24 for details.

Copy a Media Validation Policy

Use this procedure to copy a selected media validation policy. To use a policy as the basis for a new one, you can copy an existing policy that is similar to one you want to create, and then modify the copy. See "Modify a Media Validation Policy" on page 8-62 for instructions.

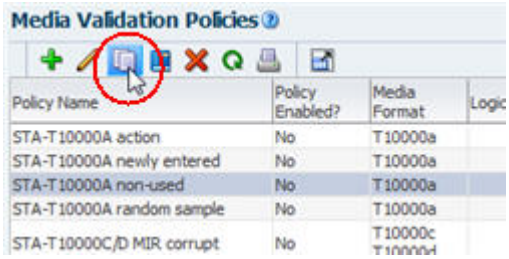
Note: This procedure requires Administrator privileges.

1. In the Navigation Bar, select **Setup & Administration**, then select **Media Validation**.



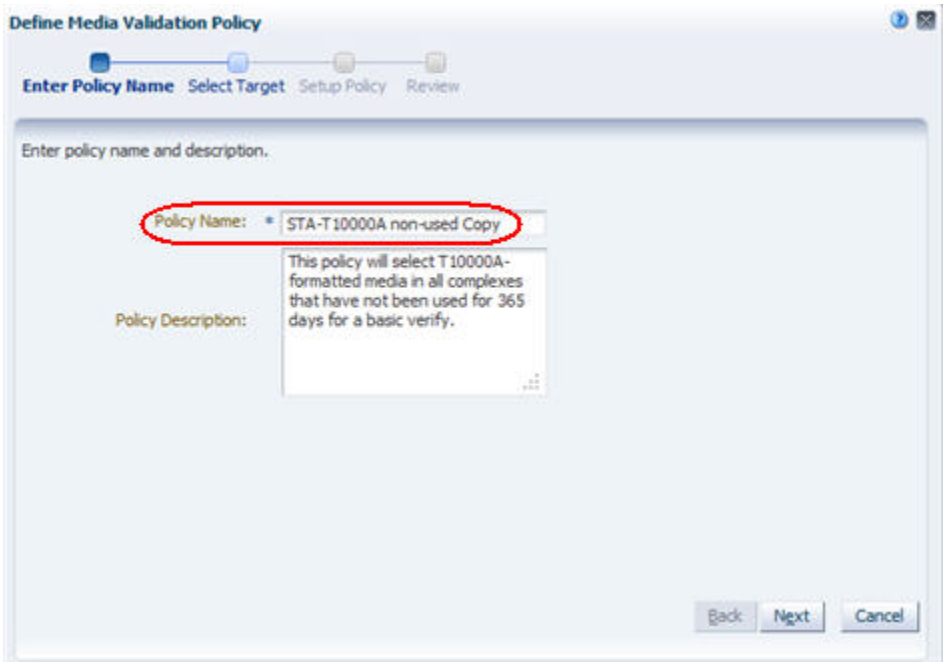
The Media Validation screen appears.

2. Select the media validation policy you want to copy and click **Copy Media Validation Policy**.



The first screen of the Media Validation Policies wizard appears. The copy of the policy has all the same information as the original, except for the following:

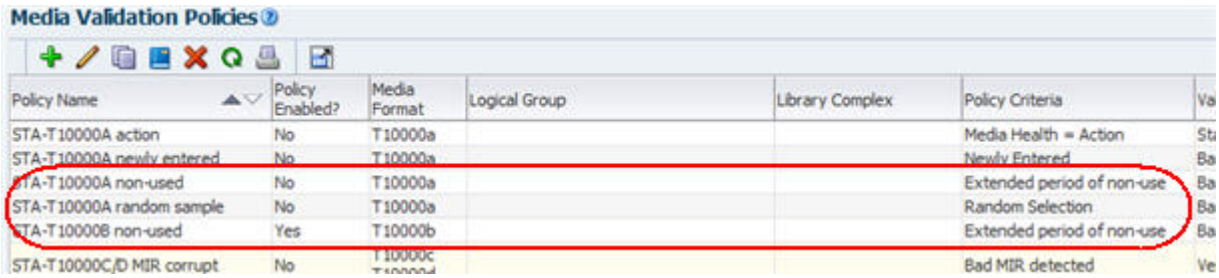
- The word "Copy" is added to the end of the Policy Name.
- The policy is enabled (the **Enable Validation Policy** check box is selected).



3. In the **Policy Name** field, type the name you want to assign, and modify the **Policy Description** as necessary.
4. Use the **Next** button or the wizard breadcrumbs at the top of the dialog box to navigate to the screens with the information you want to modify. See "Create a Media Validation Policy" on page 8-53 for instructions on completing these screens.
5. Click **Save** when you have finished.

   The new policy is created, and the Media Validation Policies screen is updated with the information.

   In the following example, the "STA-T10000B non-used" policy was copied from the "STA-T10000A non-used" policy, and the policy criteria were modified for T10000B media.



Modify a Media Validation Policy

Use this procedure to modify a selected media validation policy. You can change any attributes of a policy.

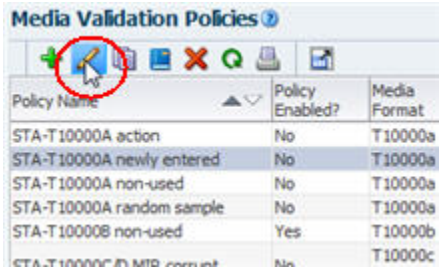
Note: For a more direct method of enabling or disabling a policy, see "Enable or Disable a Media Validation Policy" on page 8-59.

Note: This procedure requires Administrator privileges.

1. In the Navigation Bar, select **Setup & Administration**, then select **Media Validation**.

The Media Validation Overview screen appears.

2. Select the media validation policy you want to modify and click **Edit Media Validation Policy**.



The first screen of the Media Validation Policies wizard appears, and the policy's current information is displayed.

3. Use the **Next** button or the wizard breadcrumbs at the top of the dialog box to navigate to the screens with the information you want to modify. See "Create a Media Validation Policy" on page 8-53 for instructions on completing these screens.
4. Click **Save** when done.

   The policy is updated, and the changes are displayed on the Media Validation Policies screen.

Delete a Media Validation Policy

Use this procedure to delete a media validation policy. Deleting a policy does not delete media validation requests already generated from the policy; they are still available for viewing on the Media Validation Overview screen. Pending and in-progress requests generated from the policy are processed to completion.

You do not need to disable a media validation policy before deleting it.

> **Note:** This procedure requires Administrator privileges.

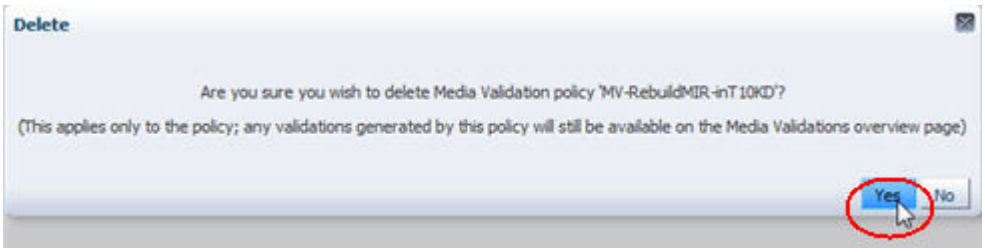
1. In the Navigation Bar, select **Setup & Administration**, then select **Media Validation**.

The Media Validation Policies screen appears.

2. Select the media validation policy you want to delete and click **Delete Media Validation Policy**.

The Delete dialog box appears.

3. Verify your selection and Click **Yes** to confirm the deletion.



The policy is deleted and the list on the Media Validation Policies screen is updated.

9

STA Usernames and Email

This chapter describes how to create and manage STA usernames and how to define available email recipients for STA alerts and Executive Reports.

This chapter includes the following sections:

- STA Usernames
- STA User Management Tasks
- Email Configuration Tasks

STA Usernames

The primary STA administrator username was created during STA installation. You can use the STA screens at any time to create and maintain any number of additional STA usernames. Each STA username must be unique and must have a password and an assigned user role.

Username and Password Requirements

Username requirements are as follows:

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

Password requirements are as follows:

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

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

Users can change their password at any time. See "Change Your Password" on page 1-9 for details.

STA User Roles

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

The user roles and privileges are summarized below; Table 9–1 provides complete detail.

Viewer

Viewers have display privileges to screens on the **Home**, **Tape System Hardware**, and **Tape System Activity** tabs in the Navigation Bar.

Viewers can modify the appearance of screens for the current login session only, filter screens, and apply templates created by users with higher privileges. They can also download Executive Reports created by users with higher privileges.

Viewers have no access to the **Setup & Administration** tab in the Navigation Bar.

Operator

In addition to all privileges available to Viewers, Operators can save and manage screen templates and run Executive Reports.

Operators have viewing access to all screens in the **Setup & Administration** tab in the Navigation Bar, allowing them to view STA policies and configuration settings defined by Administrator users; however, they cannot create policies or perform STA configuration tasks.

Administrator

Administrators have full access and privileges to all STA screens. In addition to all privileges available to Operators, Administrators can create STA policies, define configuration settings, and create STA usernames.

Table 9–1 User Role Privileges, Organized by Screen

Tab	Screen	Activity	Viewer	Oper	Admin
–	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 portlets.	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
Tape System Hardware	All	Modify the screen display for this session only by adding and changing graphs and table attributes.	X	X	X

Table 9–1 (Cont.) User Role Privileges, Organized by Screen

Tab	Screen	Activity	Viewer	Oper	Admin
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	All	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 – Overview	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
Setup & Administration	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 a logical group. Delete a logical group.		X	X
Setup & Administration	Alerts Policies	Display a list of defined alert policies.		X	X
Setup & Administration	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

Table 9–1 (Cont.) User Role Privileges, Organized by Screen

Tab	Screen	Activity	Viewer	Oper	Admin
Setup & Administration	Executive Reports Policies	Display a list of public Executive Report policies.		X	X
		Run a public report on demand.			
Setup & Administration	Executive Reports Policies	Create, modify, and delete a public report policy or a private policy created by your STA username.			X
		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.			
Setup & Administration	Templates Management	Display a list of all templates available to your STA username.		X	X
		Change the default screen template for your STA username.			
		Rename a custom template.			
		Change the public or private visibility settings of a template owned by your STA username.			
		Export a custom template.			
		Import a template.			
		Delete a template.			
		Restore the STA predefined templates.			
Setup & Administration	Media Validation	Display media validation configuration settings.		X	X
		Display drives in the media validation drive pools.			
		Display the list of media validation policies.			
Setup & Administration	Media Validation	Enable or disable media validation on STA.			X
		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.			
Setup & Administration	Service – Logs	Display a list of all available service log bundles.		X	X
		Create a log bundle.			
		Display run information for a log bundle.			
		Download a log bundle to your local computer.			
		Delete a log bundle.			
Setup & Administration	Configuration – SNMP Connections	Display SNMP client settings for STA.		X	X
		Display SNMP connection settings for all monitored libraries.			
		Export SNMP connection settings for all monitored libraries to a text file.			

Table 9–1 (Cont.) User Role Privileges, Organized by Screen

Tab	Screen	Activity	Viewer	Oper	Admin
Setup & Administration	Configuration – SNMP Connections	Configure SNMP client settings for STA.			X
		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.			
Setup & Administration	Configuration – Users	Display a list of all STA usernames and their roles.		X	X
Setup & Administration	Configuration – Users	Create and modify an STA username.			X
		Change the password for an STA username.			
		Delete an STA username.			
Setup & Administration	Configuration – Email	Display configuration settings for the STA SMTP server.		X	X
		Display a list of all available email recipients and their location information.			
Setup & Administration	Configuration – Email	Configure the STA SMTP server.			X
		Configure an available email recipient.			
		Send a test email to an available recipient.			
		Delete an available email recipient.			

STA User Management Tasks

These procedures allow you to manage STA usernames 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*.

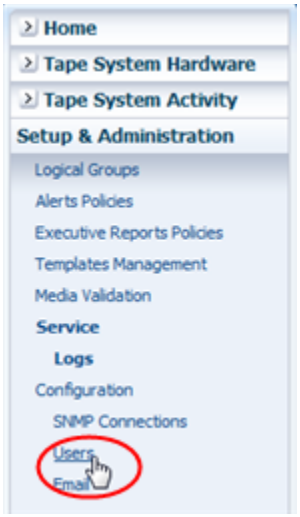
Note: All tasks in this section require Administrator privileges.

- "Add an STA Username" on page 9-5
- "Modify an STA Username" on page 9-6
- "Delete an STA Username" on page 9-7

Add an STA Username

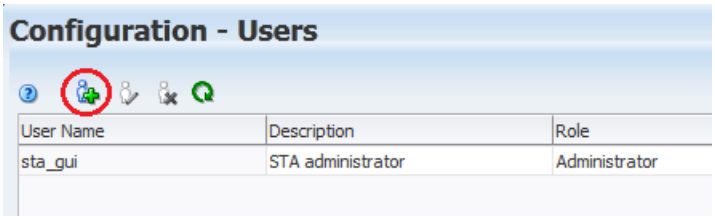
Use this procedure to add a new STA username.

1. In the Navigation Bar, select **Setup & Administration**, then select **Users**.



The Configuration – Users screen appears.

2. Click the **Create New User** icon.



The User Configuration dialog box appears.

3. Complete the dialog box as follows.
   - 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.
4. Click **Save**.

   The username is added, and the Configuration – Users table is updated.

Modify an STA Username

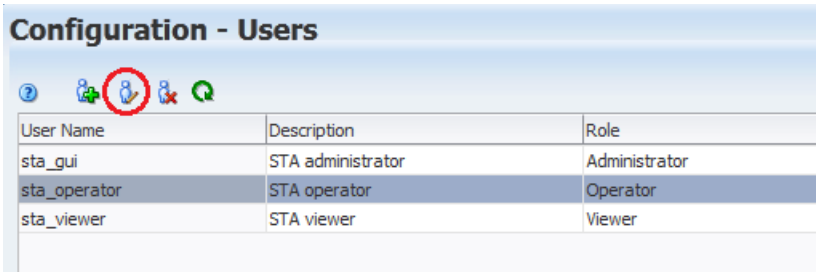
Use this procedure to modify properties of an existing STA username.

> **Note:** Any user can modify their own password by selecting **Preferences** and then **General** from the Main Toolbar. See "Change Your Password" on page 1-9 for instructions.

1. In the Navigation Bar, select **Setup & Administration**, then select **Users**.

   The Configuration – Users screen appears.

2. In the table, select the STA username you want to modify, then click the **Modify User** icon.



The User Configuration dialog box appears.

3. In the dialog box, modify the user Description, Role, or Password, and then click **Save**. See "Username and Password Requirements" on page 1-2 for detailed password requirements.

The username is updated according to your modifications.

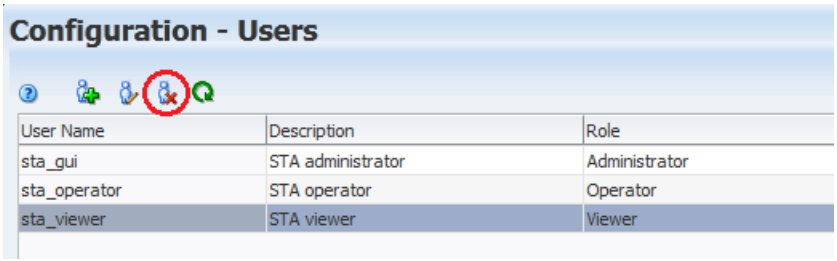
Delete an STA Username

Use this procedure to delete an STA username. You must designate whether logical groups and templates owned by the username should be deleted or retained and made public.

1. In the Navigation Bar, select **Setup & Administration**, then select **Users**.

The Configuration – Users screen appears.

2. In the table, select STA username you want to delete, then click the **Delete User** icon.



The Delete User dialog box appears.

3. In the dialog box, make one of the following selections, then click **Delete**.

- **Leave them in place, make them public**—Retain all templates and logical groups owned by this username. The items will be made public and available to all users.
- **Delete them**—Delete all templates and logical groups owned by this username.

Note: Deleting a logical group may invalidate any filters, templates, and Executive Reports using that logical group.

The STA username is deleted. Any templates and logical groups owned by the username are either updated or deleted, according to your selection.

Email Configuration Tasks

You can define STA alert and Executive Reports policies to automatically send emails to designated email addresses. Before doing this, you must use the following procedures to identify the STA email server and available recipient addresses. These procedures assume an email server has already been configured at your site.

See "Alert Emails" on page 5-10 and "Emailing Executive Reports" on page 6-6 for details about assigning available email recipients to the respective policies.

All tasks in this section require Operator or Administrator privileges.

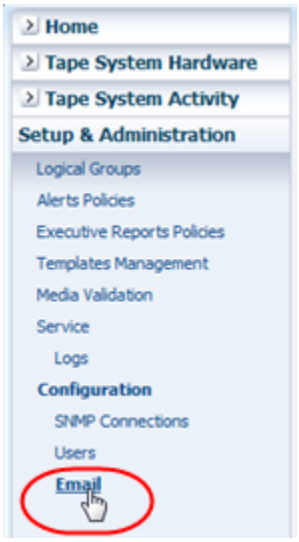
- "Define the STA SMTP Server" on page 9-8
- "Add an Available Email Recipient" on page 9-10
- "Display Email Configuration Information" on page 9-11
- "Test the Email Server and Recipient Definitions" on page 9-12
- "Modify an Available Email Recipient" on page 9-13
- "Delete an Available Email Recipient" on page 9-13

Define the STA SMTP Server

Use this procedure to define the STA email server. You can define only one email server.

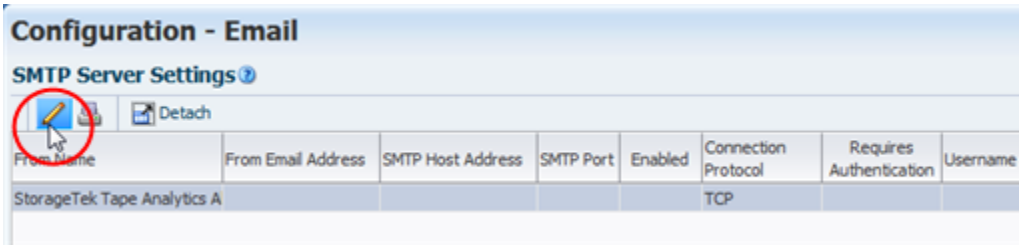
Note: This task requires Administrator privileges.

1. Contact your IT administrator to determine the host address and authentication requirements for the email server you want to use for sending STA emails.
2. In the Navigation Bar, select **Setup & Administration**, then select **Email**.



The Configuration – Email screen appears.

3. In the SMTP Server Settings table, select the StorageTek Tape Analytics Alerts record, then click the **Edit Selected SMTP Server** icon.



The Define SMTP Server Details dialog box appears.

4. 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.

     Note: 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.

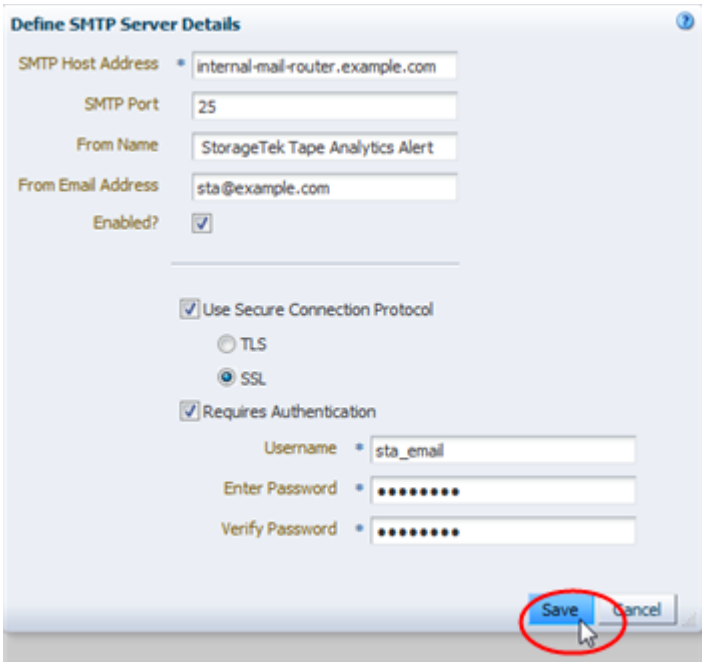
   - From Email Address—Enter the email address from which STA email is sent. This must be a valid address on the email server.

     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.

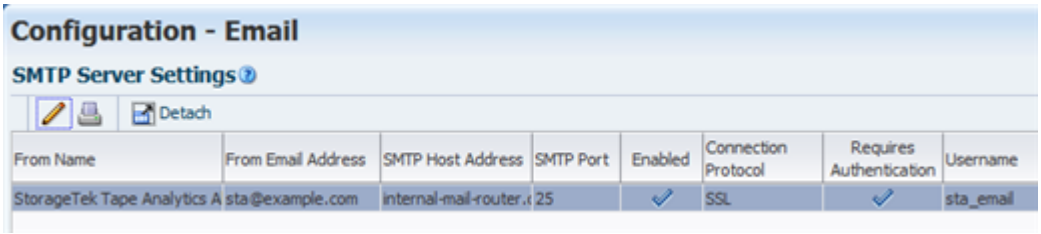
   - Use Secure Connection Protocol—To use a secure connection protocol, select the check box, and then select the protocol by clicking either TLS or SSL.

- 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.



5. Click **Save**.

   The SMTP Server Settings table is updated with the information you have entered.



Add an Available Email Recipient

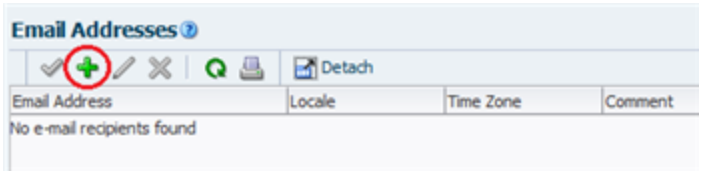
Use this procedure to add an email address to the list of recipients available to receive STA emails. A user does not need an STA username to receive STA emails.

> **Note:** This task requires Administrator privileges.

1. In the Navigation Bar, select **Setup & Administration**, then select **Email**.

   The Configuration – Email screen appears.

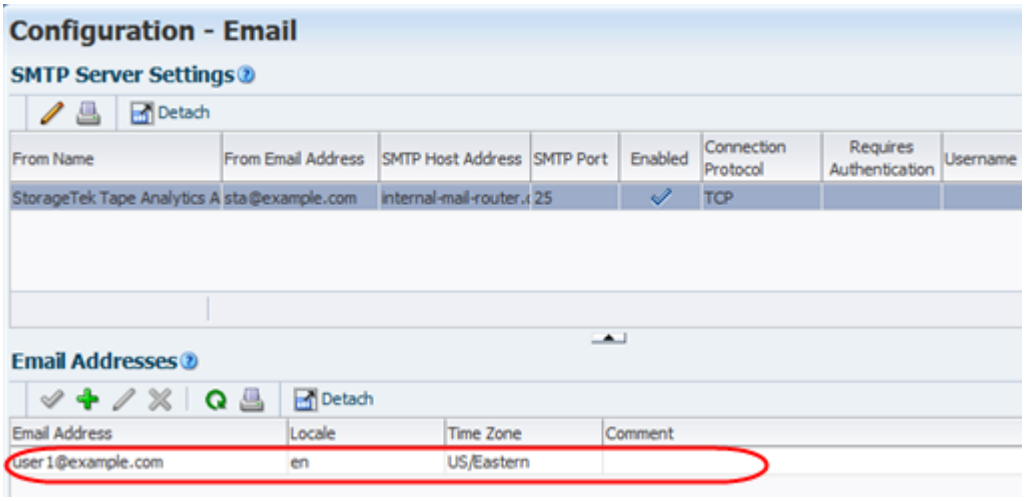
2. In the Email Addresses table, click the **Add Email** icon.



The Define Email Details dialog box appears.

3. Complete the dialog box as follows, 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.

The address is added to the Email Addresses table. The Comment field is left blank for now.



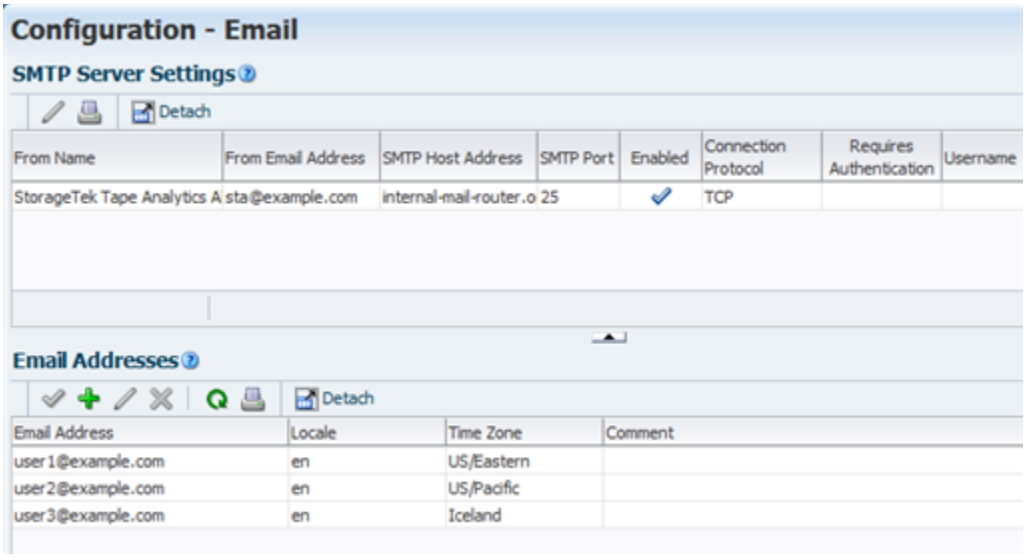
Display Email Configuration Information

Use this procedure to display details about the STA email server configuration and available email recipients.

Note: This task requires Operator or Administrator privileges.

1. In the Navigation Bar, select **Setup & Administration**, then select **Email**.

   The Configuration – Email screen appears.



   The SMTP Server Settings table shows all configuration information for the STA email server. The Email Addresses table shows all email addresses available to receive STA emails.

   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

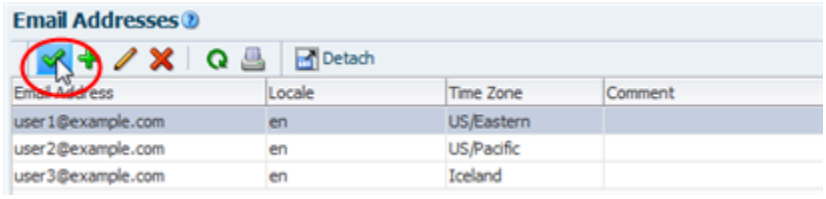
Use this procedure to verify the STA email server and recipient definitions by sending a test email to a selected recipient.You can test only one recipient at a time.

Note: This task requires Administrator privileges.

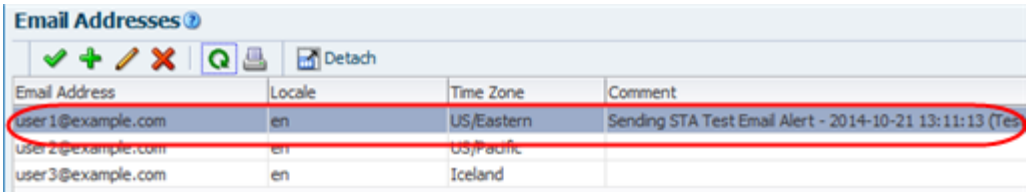
1. In the Navigation Bar, select **Setup & Administration**, then select **Email**.

   The Configuration – Email screen appears.

2. In the Email Addresses table, select the address you want to test, then click the **Test SMTP and Email Address Setup** icon.



   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.



3. Check the recipient's email to confirm receipt. Example 9–1 is a sample of the test email contents.

Example 9–1 Sample STA Test Email

```
From: stasmtp@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)
```

4. 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

Modify an Available Email Recipient

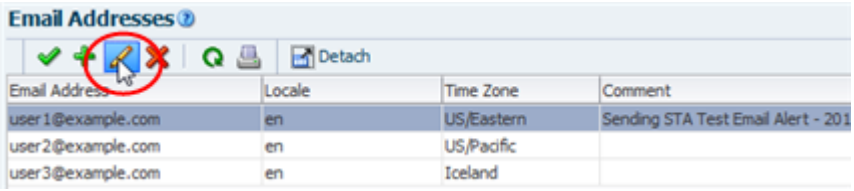
Use this procedure to modify an existing available email recipient. You can edit only one address at a time.

> **Note:** This task requires Administrator privileges.

1. In the Navigation Bar, select **Setup & Administration**, then select **Email**.

   The Configuration – Email screen appears.

2. In the Email Addresses table, select the address you want to change, then click the **Edit Selected Email** icon.



   The Define Email Details dialog box appears.

3. In the dialog box, make any necessary changes. Click **Save** when done.

   The email address is updated, and the changes are displayed in the Email Addresses table.

Delete an Available Email Recipient

Use this procedure to delete an email address from the list of available recipients. The address will no longer be able to receive emails from STA. 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.

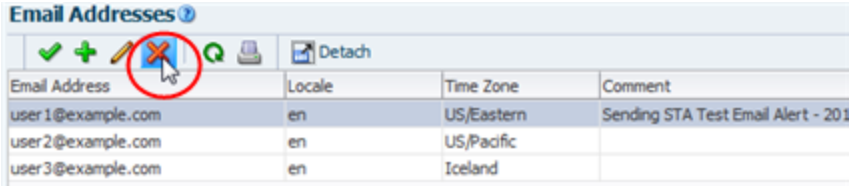
Caution: There is no confirmation dialog box for this operation. The email address is deleted as soon as you click the **Delete Selected Email(s)** button.

Note: This task requires Administrator privileges.

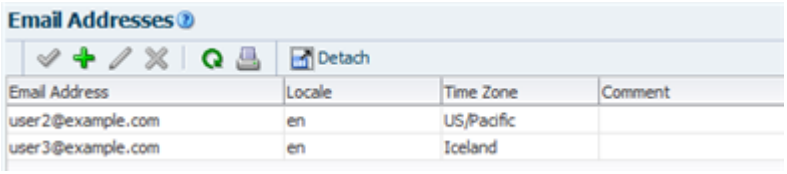
1. In the Navigation Bar, select **Setup & Administration**, then select **Email**.

   The Configuration – Email screen appears.

2. In the Email Addresses table, select the email address you want to delete, then click the **Delete Selected Email(s)** icon.



   The email address is deleted from the list of available recipients. It is also deleted from all alert and Executive Report policies in which was used.



10

STA Service Logs

Using Oracle's Remote Diagnostics Agent (RDA), STA collects information that your Oracle support representative can use to determine the source of a fault on the STA server.

This chapter includes the following sections:

- Service Log Overview
- Service Log Tasks

Service Log Overview

STA service logs are useful for resolving issues with the STA user interface and STA managed servers. Your Oracle support representative can use them for performance analysis, debugging, security analysis, usage analysis, and other related purposes.

> **Note:** The service logs are not used to resolve issues with the libraries and drives monitored by STA.

STA uses RDA to take a current snapshot of all logs related to the STA application and database, including operating system, installation, and configuration information. These logs are automatically grouped into a *log bundle* and assigned an associated date and timestamp.

Log bundles are retained indefinitely until you delete them and are only limited by the amount of disk space on the STA server. You can download a selected log bundle as a zip file and forward it to your Oracle support representative for analysis.

Reasons for Generating a Log Bundle

You may want to create a log bundle in the following situations. Oracle highly recommends you create the log bundle as soon as possible, as this will make it easier for Service or STA Development to find details leading up to the issue or event.

- An unexpected STA application event occurs and it appears to be a bug.
- Oracle Service requests that you take a snapshot.
- The STA user interface automatically displays a message indicating you should take a snapshot.

Taking a Log Snapshot

You can take a service log snapshot using either of the following methods. You can create and store multiple log bundles.

From the STA user interface

The easiest way to collect RDA service log information is with the STA user interface. Using this method, snapshots are stored in the following directory:

/*Oracle_storage_home*/Middleware/rda/snapshots

Where /*Oracle_storage_home* is the Oracle storage home location defined during STA installation. See the *STA Installation and Configuration Guide*for details.

From the system command line

If you are not able to access the STA user interface, you can use the rda.sh utility to create a log bundle manually from the system command line. Using this method, snapshots are stored in the following directory:

/*Oracle_storage_home*/Middleware/rda/output

Use any of the following commands to display additional 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.

Log Bundle Process

Following is an overview of the log bundle collection and submission process:

1. Take an STA log snapshot. See "Create a Service Log Bundle From the STA User Interface" on page 10-3 or "Create a Service Log Bundle From the System Command Line" on page 10-3.
2. Download the log bundle zip file to your computer. See "Download a Log Bundle" on page 10-6.
3. Forward the zip file to Oracle Support. See "Forward a Log Snapshot to Oracle Support" on page 10-7.

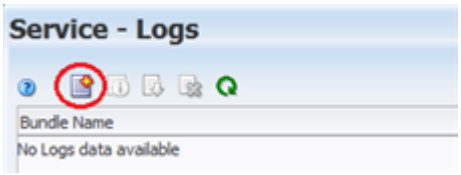
Service Log Tasks

- "Create a Service Log Bundle From the STA User Interface" on page 10-3
- "Create a Service Log Bundle From the System Command Line" on page 10-3
- "List Generated Log Bundles" on page 10-5
- "Display Log Run Information" on page 10-5
- "Download a Log Bundle" on page 10-6
- "Delete a Log Bundle" on page 10-7
- "Forward a Log Snapshot to Oracle Support" on page 10-7

Create a Service Log Bundle From the STA User Interface

Use this procedure to generate a log bundle containing a current snapshot of service information on the STA server.

1. In the Navigation Bar, select **Setup & Administration**, then select **Logs**.
2. Click the **Create New Log Bundle** icon.



3. In the Log Bundle Name field, enter a snapshot name meeting these requirements:
   - Maximum of 210 characters
   - Can only contain alphanumeric characters and underscores (but cannot contain four or more consecutive underscores)
   - If spaces are entered, they will be replaced with underscores
   - Cannot begin with the following uppercase characters: COM, LPT, PRN, CON, AUX, or NUL.
4. Click **Save**.

   A message appears indicating the job has been queued. It may take several minutes for the submitted job to appear in the table and for the process to complete. If you navigate away from the Service – Logs screen, the process will continue in the background.

Note: Click the **Refresh Table** icon to update the status of an in-process log run.

Create a Service Log Bundle From the System Command Line

Use this procedure to collect service information manually from the system command line.

1. Log on to the STA server as the system root user.
2. Change to the RDA directory. For example:

   # cd /Oracle/Middleware/rda
3. Verify that the RDA setup.cfg file is present.

   # ls -la setup.cfg

   ```
   -rw-r----- 1 root root 13467 Nov 13 11:25 setup.cfg
   ```
4. Enter the following command to generate the log bundle.

   # ./rda.sh –v –f

   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 name RDA.STA_*servername*.zip. This may take several minutes. Example 10–1 is an excerpt of the command output.

Example 10–1 Sample Service Log Creation Command Line Output

 # ./rda.sh –v –f

```
        Collecting diagnostic data ...
--------------------------------------------------------------------------------
RDA Data Collection Started 13-Nov-2014 10:46:33
--------------------------------------------------------------------------------
Processing Initialization module ...
Processing OCM module ...
Processing PERF module ...
Processing CFG module ...
Processing OS module ...
Processing PROF module ...
Processing NET module ...
Processing Oracle installation module ...
Processing WREQ module ...
Processing STA module ...
Hashing credential information......
Starting MySql STA database dump to /var/log/tbi/db/dump.......
MySql STA database dump complete
Processing RDSP module ...
Processing LOAD module ...
Processing End module ...
--------------------------------------------------------------------------------
RDA Data Collection Ended 13-Nov-2014 10:47:59
--------------------------------------------------------------------------------
        Generating the reports ...
                - STA_WREQ_d1_R00162_abbr.txt ...
                - STA_WREQ_d1_R00022_log_secureWebLogic_sh.txt ...
                - STA_WREQ_d1_R00114_log_nm_password_properties.txt ...
                - STA_WREQ_d1_R00107_log_readme_txt.txt ...
                - STA_WREQ_d1_R00171_log_dms_mbeans_xml.txt ...
                - STA_INST_R00009_oraInstall2014_10_30_03_53_34PM_out.dat ...
                - STA_INST_oracle_home.txt ...
                - STA_WREQ_o1_R00005_log_log_txt.txt ...

...

If this file was generated to assist in resolving a Service Request, please
 send /Oracle/Middleware/rda/output/RDA.STA_mystaserver.zip to Oracle Support by
 uploading the file via My Oracle Support. If ftp'ing the file, please be sure
 to ftp in BINARY format.

 Please note: Do not submit any health, payment card or other sensitive
 production data that requires protections greater than those specified in the
 Oracle GCS Security Practices

(http://www.oracle.com/us/support/library/customer-support-security-practices-0691
70.pdf).
 Information on how to remove data from your submission is available at
 https://support.oracle.com/rs?type=doc&id=1227943.1

        Updating the setup file ...
#
```

5. Rename the RDA zip file to a unique name. For example:

   # **mv RDA.STA**_servername_**.zip ./RDA.STA**_servername_xxxx_**.zip**

   Where *xxxx* is a unique extension of your choice.

6. Optionally, use one of the following methods to display the files just created.
   - Open a browser window on the STA server and navigate to the following URL:

     file:///*Oracle_storage_home*/Middleware/rda/output/STA_start.htm

   - Download the zip file to your local computer, unzip the bundle, and access the log files through the URL above.

List Generated Log Bundles

Use this procedure to display summary information about all log bundles on the STA server.

> **Note:** This procedure applies only to log bundles created from the STA user interface.

1. In the Navigation Bar, select **Setup & Administration**, then select **Logs**.

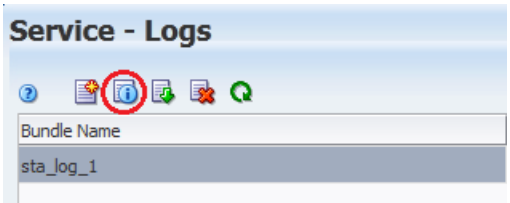
   The Service Logs screen displays the following information for each log bundle.
   - Bundle Name—User-defined name assigned to the log snapshot. See "Create a Service Log Bundle From the STA User Interface" on page 10-3.
   - State—The running state of the new log bundle (Running or Completed).
   - Date Created—The date and time you started the RDA run.
   - File Size (KB)—The size of the log file.

Display Log Run Information

Use this procedure to display detailed information about a selected log bundle. You can perform this procedure while the log run is in process or after it has completed.

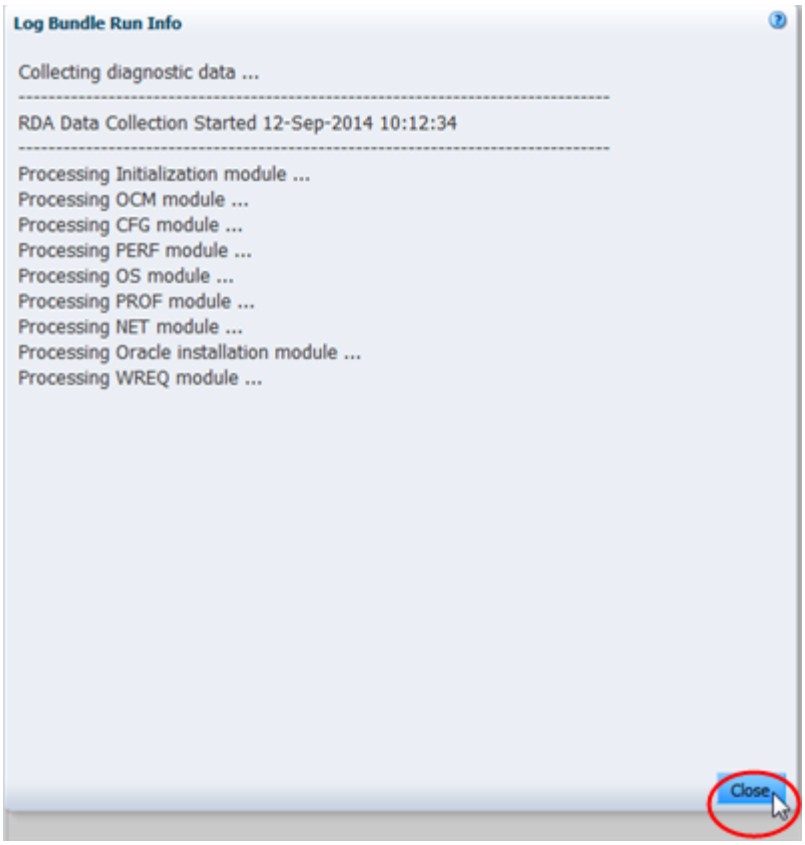
> **Note:** This procedure applies only to log bundles created from the STA user interface.

1. In the Navigation Bar, select **Setup & Administration**, then select **Logs**.
2. Select the log bundle you want to display.
3. Click the **Log Bundle Run Info** icon.



The Log Bundle Run Info dialog box is displayed, providing information about the log run.

4. Click **Close** to dismiss the dialog box.

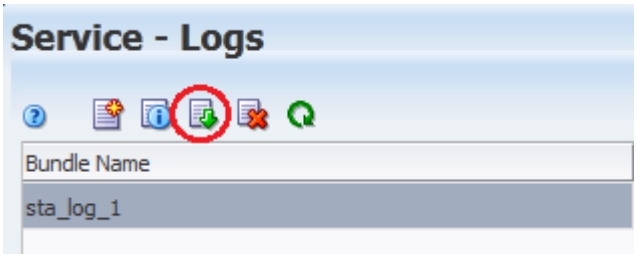


Download a Log Bundle

Use this procedure to download a completed log bundle to your local computer.

Note: This procedure applies only to log bundles created from the STA user interface.

1. In the Navigation Bar, select **Setup & Administration**, then select **Logs**.
2. Select the log bundle you want to download.
3. Click the **Download Selected Log Bundle** icon.



4. Save the file.

Note: If you see this error message in the log file, you may ignore it:

WARNING:

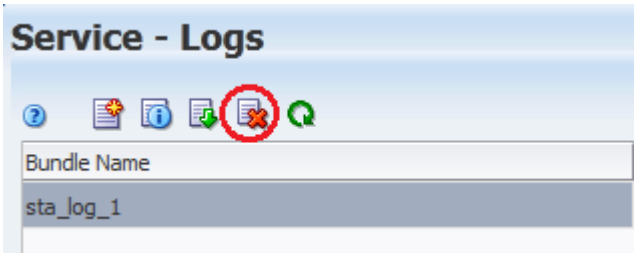
java.lang.ClassNotFoundException: oracle.tbi.view.faces.ExceptionHandler

Delete a Log Bundle

Use this procedure to delete a selected log bundle.

Note: This procedure applies only to log bundles created from the STA user interface.

1. In the Navigation Bar, select **Setup & Administration**, then select **Logs**.
2. Select the log bundle you want to delete.
3. Click the **Delete Selected Log Bundle** icon.



Forward a Log Snapshot to Oracle Support

Use this procedure to forward the log bundle to Oracle Support for evaluation. This procedure applies to log bundles created either from the STA user interface or from the system command line.

Note: This procedure applies to all log bundles.

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, and then select **Create SR**. Use the wizard tips to complete each required field.
4. Complete the **What is the Problem?** section with a summary and description of the issue.
5. Complete the **Where is the Problem?** section, and select the **Support** tab (software, hardware, cloud, etc.) for the issue type being reported.
6. Select a problem type from the list.
7. Select the applicable support identifier (SI), and click **Next**.
8. Review any preferred knowledge articles.
9. To continue with SR creation, upload files and provide additional information as needed.

10. Select severity, confirm contact information, and click **Submit**.

11

Managing SNMP Connections in STA

This chapter provides concepts and procedures for managing the SNMP connections between STA and the libraries it monitors. It assumes a basic understanding of the Simple Network Management Protocol (SNMP).

This chapter includes the following sections:

- SNMP Configuration for STA
- STA Data Store
- Maintaining SNMP Connections and the STA Data Store
- SNMP Maintenance Tasks Performed in STA
- Supporting SNMP Maintenance Tasks Performed on the Library
- Special SNMP Connection Update Tasks
- SNMP Connection Troubleshooting Tasks

SNMP Configuration for STA

Communication between STA and the libraries it monitors is through the SNMP interface. 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.

This chapter assumes you are using the recommended SNMP v3 protocol for SNMP communications between STA and the monitored libraries. For complete information about initial SNMP v3 configuration, including configuration tasks performed on the libraries, see the *STA Installation and Configuration Guide*.

STA Data Store

The STA data store is created and maintained through SNMP data received from the monitored libraries. It includes the following information types.

Library configuration model

This is a hierarchical view of the library and device configurations, properties, and statuses. To retrieve this information, STA initiates data collections through a series of SNMP requests sent to the library.

Exchange records

These records include detailed information about all drive and media exchanges, including drive clean activities. The library sends this data to STA through asynchronous SNMP traps.

Errors and events
These are records of significant library errors and events. The library sends this data to STA through asynchronous SNMP traps.

Maintaining SNMP Connections and the STA Data Store

Once the SNMP connection between STA and a library is established, 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 re-establish a connection.

This section includes the following topics, which provide background information for the tasks described later in this chapter.

- "Library Connection Status Information" on page 11-2
- "Understanding the Library Engine ID" on page 11-2
- "Testing Library SNMP Connections" on page 11-3
- "Collecting Library Configuration Data" on page 11-5

Library Connection Status Information

The connection status fields in the Monitored Libraries section of the Settings – SNMP Connections screen display the status of the most recent library connection test or data collection.

Table 11–1 describes these fields.

Table 11–1 Library Connection Status Fields in the Monitored Libraries Table

Field	Description
Last Successful Connection	Date and time of the most recent successful connection test or data collection.
Last Connection Attempt	Date and time when the most recent connection test or data collection was attempted. If the attempt failed, then this date and time are more recent than the "Last Successful Connection".
Last Connection Status	Status of the most recent connection test or data collection. In a data collection, the status is updated throughout the process according to the screen refresh rate defined for your STA username. Possible statuses are: ■ IN PROGRESS – A data collection is underway. ■ SUCCESS – The connection test or data collection completed successfully. ■ FAILED – The connection test or data collection failed. Possible reasons are listed in the Last Connection Failure Detail field. ■ REJECTED – The data collection request was rejected, possibly because the library is busy or unavailable. ■ DUPLICATE – The data collection request was rejected because another one is already is progress.
Last Connection Failure Detail	If the connection test or data collection failed or was rejected, possible causes are listed in this field.

Understanding the Library Engine ID

Every SNMP v3 agent has a globally unique hexadecimal engine ID to identify the device. This section describes how the Library Engine ID field is updated and displayed in the Monitored Libraries table on the Settings – SNMP Connections screen.

See "Configure the SNMP Connection to a Library" on page 11-11 for related information.

When you configure a new SNMP connection on STA, you 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. See "Test a Library SNMP Connection" on page 11-13 for details.

The Library Engine ID field may be blank in the following situations:

- This is a new library connection, and you have not yet performed a connection test.
- 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.

You should 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. See "Library Connection Status Information" on page 11-2 and "Troubleshoot a Failed Trap Channel Test" on page 11-25 for details.
- After a library firmware upgrade, you should clear the engine ID and perform a connection test. See "Update the SNMP Connection After a Library Firmware Upgrade" on page 11-21.

Testing Library SNMP Connections

A library connection test establishes, or re-establishes, the SNMP handshake between STA and a monitored library. It typically takes less than a second to test a library connection, but during this time no traps are received from any libraries. Therefore, although you can perform a connection test at any time, Oracle recommends you do so only when necessary. Only one library connection can be tested at a time. See "Test a Library SNMP Connection" on page 11-13 for instructions.

When to Perform a Connection Test

Certain activities performed in STA or on a monitored library may cause the SNMP connection with the affected library to be dropped, and STA will not be able to receive SNMP data from the library until after the next scheduled data collection is completed. Performing a connection test minimizes the time the library connection is dropped and prevents the loss of large amounts of SNMP data.

Oracle recommends you perform a connection test at the following times:

- After initial configuration of the SNMP connection between STA and a library. The initial connection test establishes the SNMP handshake between STA and the library.
- After modifying any settings for the STA SNMP client (see "Configure SNMP Client Settings for STA" on page 11-9 for details). These settings include the SNMP user name and the connection authorization and privacy passwords. If you modify any of these settings, you need to test the connections of all monitored libraries.
- After modifying any SNMP settings for a monitored library (see "Configure the SNMP Connection to a Library" on page 11-11 for details). Whenever you modify these settings, the Library Engine ID field is cleared to indicate that the SNMP

connection with the library has been dropped. To restore the proper connections, you only need to test the connection of the affected library.

- After a monitored library has been rebooted. You should wait until the library is fully operational before initiating the connection test (see "Verify the Library is Operational" on page 11-18 for details). If more than one library is rebooted, you only need to test the connection for one of them, but you should wait for all libraries to be fully operational before doing so.
- After a Redundant Electronics switch has taken place on a monitored library (SL3000 and SL8500 libraries only). You should wait until the switch has completed and the library is fully operational before initiating the connection test. See "Update the SNMP Connection After a Library Redundant Electronics Switch" on page 11-21 for details.
- Anytime you suspect loss of SNMP data from one or more libraries.

Connection Test Status Messages

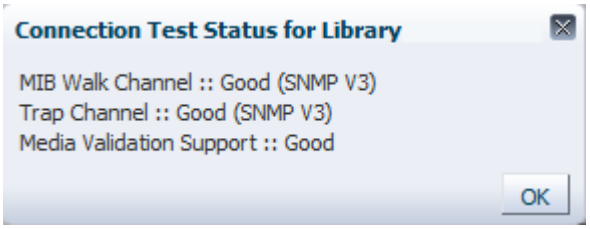
The SNMP connection test includes the following parts:

- 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.

When the connection test completes, the Connection Test Status message box displays results for each of these tests. Example 11–1 through Example 11–4 are examples of possible connection test results.

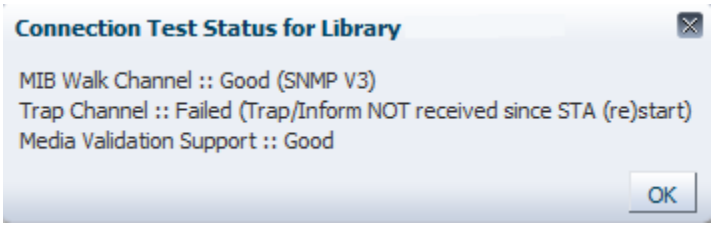
If a connection test fails, see "SNMP Connection Troubleshooting Tasks" on page 11-23 for suggested troubleshooting procedures.

Example 11–1 Successful Connection Test

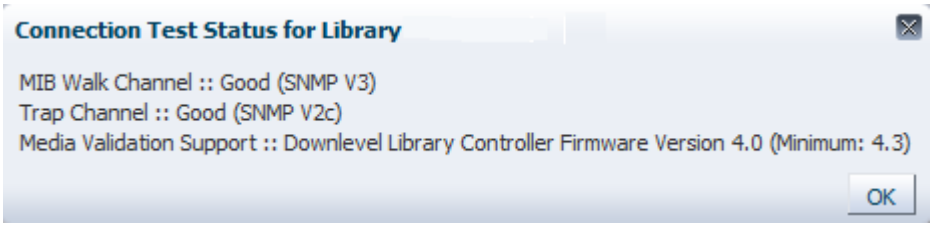


Example 11–2 Failed MIB Walk Channel Test

Example 11–3 Failed Trap Channel Test



Example 11–4 Failed Media Validation Support Test



Collecting Library Configuration Data

Once an SNMP connection has been established with a library, STA begins receiving SNMP traps and stores this data in the STA data store. This data is not displayed in the user interface, however, until the STA library configuration model has been built.

Building the STA Library Configuration Model

For STA to build the initial configuration model for a library, you should initiate a manual data collection as soon as the library connection has been established. See "Perform a Manual Data Collection" on page 11-15 for instructions.

During the initial data collection, STA retrieves all library configuration information, including:

- 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, and during this time you may see fluctuations in various analytic and summary data; this is normal.

Keeping the Configuration Model Up-to-date

After the initial data collection, the STA library configuration model is updated through regular data collections. Only one data collection can be performed on a particular library at a time, and only five data collections can be running simultaneously.

How Data Collections Are Initiated

Data collections can be initiated in any of the following ways:

- Scheduled—Scheduled data collections occur automatically every 24 hours at a user-defined time. This is a full collection of all library configuration data and should be scheduled during low levels of library activity. See "Configure the SNMP Connection to a Library" on page 11-11 for instructions.
- Triggered—STA automatically initiates triggered 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, for a data collection triggered by the addition of a new media, only the media configuration information is updated. 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 "Perform a Manual Data Collection" on page 11-15 for instructions.

Data Collections and Library Performance

The libraries process SNMP activity, and therefore 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 scheduled and manual data collections be performed during periods of lower library activity.

Required Data Collection Times

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

- When a new library connection is configured. This builds the initial STA library configuration model.
- After modifying SNMP settings in STA and on the library. See "Configure the SNMP Connection to a Library" on page 11-11 for details.
- When a Redundant Electronics switch has occurred. See "Update the SNMP Connection After a Library Redundant Electronics Switch" on page 11-21.

Recommended Data Collection Times

For STA to be notified as soon as possible of changes in the library environment, Oracle recommends you perform a manual data collection at the following times:

- When a large number of media are entered or ejected from a library, such as through an SL3000 access expansion module (AEM). STA initiates a triggered data collection as soon as the library notifies it of any enters and ejects, but notifications of large-scale changes may take some time to complete.
- When a drive is added, removed, or swapped. This is especially important for drive swaps, where a drive is installed in a slot that previously had a different drive. There may be a lag between the time when the old drive is removed, the new drive is installed, and the library notifies STA of the changes. During this time, any exchanges that use the new drive could result in co-mingling of data between the new and old drives. Initiate the data collection according to the following guidelines:
  - 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.
- When a robot is added, removed, or swapped.
- When a Redundant Electronics switch occurs, or the library active storage regions or partitions are modified. Although STA initiates a triggered data collection as soon as the library notifies it of these types of changes, it is recommended that you initiate a manual data collection because these modifications can have a significant impact on the STA library configuration model. Initiate the data collection according to the following guidelines:
  - For changes to the library active storage regions or partitions, wait 15 minutes after the library controller database has been updated.
  - For a Redundant Electronics switch, wait 15 minutes after the newly active controller card has fully initialized. See "Update the SNMP Connection After a Library Redundant Electronics Switch" on page 11-21 for instructions.
- Anytime you suspect library configuration data is out of sync on STA. See ""Missing" Media" on page 12-10 and "Duplicate Volume Serial Numbers" on page 12-10 for additional information.
- Anytime you suspect a data collection failed because of a reason external to STA.

SNMP Maintenance Tasks Performed in STA

The following tasks maintain the SNMP connections between STA and the libraries it monitors. You should perform these procedures as necessary.

Unless indicated otherwise, these procedures are performed from the STA user interface by a username with STA administrator privileges.

- "Verify SNMP Communication With a Library" on page 11-7
- "Configure SNMP Client Settings for STA" on page 11-9
- "Configure the SNMP Connection to a Library" on page 11-11
- "Test a Library SNMP Connection" on page 11-13
- "Perform a Manual Data Collection" on page 11-15
- "Export SNMP Connection Settings to a Text File" on page 11-16
- "Remove a Library Connection From STA" on page 11-17

Note: The procedures in this section assume you are using the recommended SNMP v3 protocol for STA communications.

Verify SNMP Communication With a Library

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

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

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

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

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

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

   Where:

   - v3 indicates SNMP v3
   - *SNMP_user* is the SNMP v3 user name.
   - SHA indicates the authentication protocol.
   - *auth_pwd* is the authorization password.
   - DES indicates the privacy protocol.
   - *priv_pwd* is the privacy password.
   - authPriv indicates that privacy is performed on the command.
   - *library_IP_addr* is the IP address of the public port on the library.
     - For SL150 libraries, this is Network Port 1.
     - For SL500 libraries, this is port 1B.
     - For SL3000 and SL8500 libraries, there may be multiple ports to test, depending on whether Dual TCP/IP or Redundant Electronics are activated on the library. If there are multiple ports, run this command for each IP address.
   - 1.3.6.1.4.1.1211.1.15.3.1.0 is the SNMP object identifier (OID) for the library, which is the same for all library models.

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

Example 11–5 Successful snmpget Command

 # snmpget –v3 –u STAsnmp –a SHA –A authpwd1 –x DES –X privpwd1 –l authPriv 192.0.2.20 1.3.6.1.4.1.1211.1.15.3.1.0

SNMPv2–SMI::enterprises.1211.1.15.3.1.0 =STRING: "SL8500"

Example 11–6 Failed snmpget Command—Network Timeout

 # snmpget –v3 –u STAsnmp –a SHA –A authpwd1 –x DES –X privpwd1 –l authPriv 192.0.2.20 1.3.6.1.4.1.1211.1.15.3.1.0

Timeout: No Response from 192.0.2.20.

Example 11–7 Failed snmpget Command —Invalid Password

 # snmpget –v3 –u WrongUsr –a SHA –A authpwd1 –x DES -X WrongPwd -l authPriv 192.0.2.20 1.3.6.1.4.1.1211.1.15.3.1.0

snmpget: Authentication failure (incorrect password, community or key)

3. Test the SNMP v2c connection.

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

   Where:

   - -v2c indicates SNMP v2c
   - -c stasnmp indicates the SNMP v2c community string.
   - -l authPriv indicates that privacy is performed on the command.
   - *library_IP_addr* is the IP address of the public port on the library.

4. If both SNMP connection tests are successful, you can quit this procedure. If either test fails, proceed to the next step to troubleshoot suspected network issues, as necessary.

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

   # **traceroute –I** *library_IP_addr*

   Where:

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

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

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

   # **tcpdump –v host** *library_IP_addr* **> /var/tmp/***file_name* **&**

   Where:

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

Configure SNMP Client Settings for STA

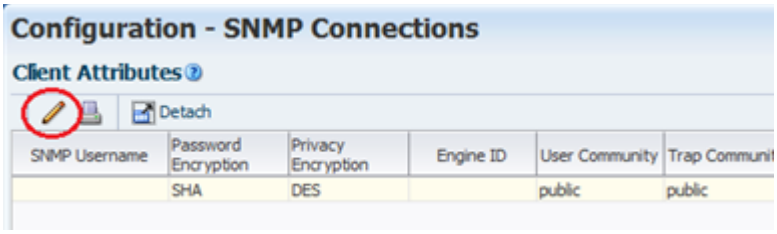
Use this procedure to add or modify SNMP client settings for STA. These settings configure STA to receive SNMP data from one or more libraries.

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

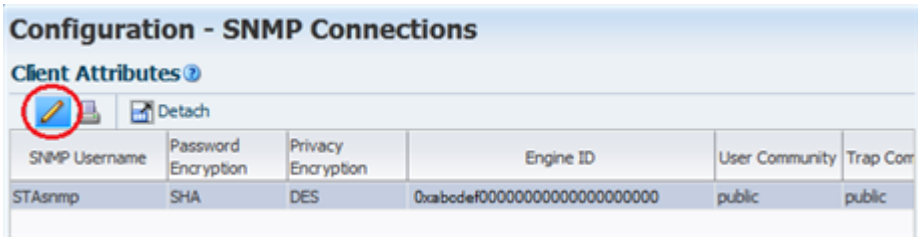
1. In the Navigation Bar, select **Setup & Administration**, then select **SNMP Connections**.

2. Proceed as follows:

   - To configure the client settings for the first time, select the empty table row in the Client Attributes table, then click **Edit**.



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



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

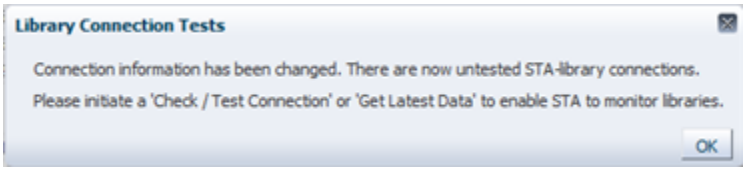
3. Complete the dialog box as follows. The values you specify must match the corresponding ones on the libraries.

Note: Even if STA will only be monitoring libraries configured for SNMP v2c communication, you must complete all fields, including those applicable to SNMP v3. You cannot leave any fields blank.

- STA SNMP Connection Username (Auth)—Type the SNMP v3 user name.
- Enter STA SNMP Connection Password (Auth)—Type the connection authorization password.
- Enter Privacy Encryption Password (Privacy)—Type the privacy encryption password.
- User Community—Type the SNMP v2c community string specified on the library. This field is required for the SNMP handshake with the library.
- Trap Community —Type the SNMP v2c community string specified on the library. This field is used only if SNMP v2c is used for communication with the library.

4. Click **Save**.

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



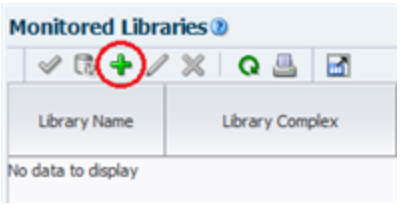
5. Click **OK** to dismiss the message.

Configure the SNMP Connection to a Library

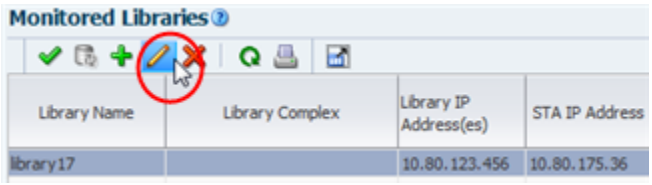
Use this procedure to configure an SNMP connection to each library you want STA to monitor, or to modify an existing connection. For existing connections, you *must* perform this procedure if there are changes to any of the SNMP configuration settings on a monitored library, such as a change to the library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

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

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



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



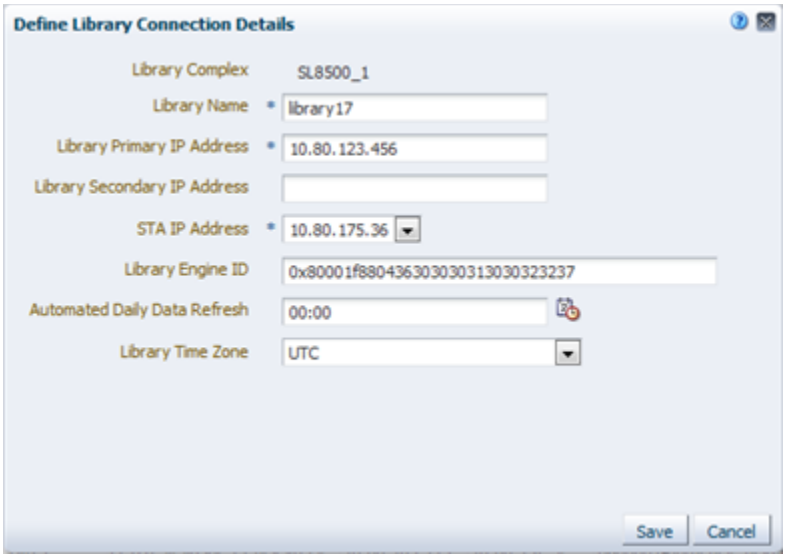
The Define Library Connection Details dialog box appears. If this is a new library connection, the fields are blank.

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

   - Library Name—Type a name to identify the library throughout the STA user interface screens (for example, the library host name).
   - Library Primary IP Address—Type the IP address of the primary public port on the library. You cannot specify the IP address of another monitored library.
   - Library Secondary IP Address—Applies only to SL3000 and SL8500 libraries using Dual TCP/IP or Redundant Electronics. Specify the IP address of the secondary public port on the library. You cannot specify the IP address of another monitored library. Leave the field blank for all other libraries, including all SL500 and SL150 libraries.
   - STA IP Address—Select the IP address of the STA server.
   - Library Engine ID—Do not modify this value. 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. See "Understanding the Library Engine ID" on page 11-2 for additional details.
   - Automated Daily Data Refresh—Specify the time of day you want STA to collect the latest configuration data from the library. The data is collected automatically every 24 hours at this time. You should choose a time when there is typically lighter library usage. The default is 00:00 (12:00 am). Use 24-hour time format.

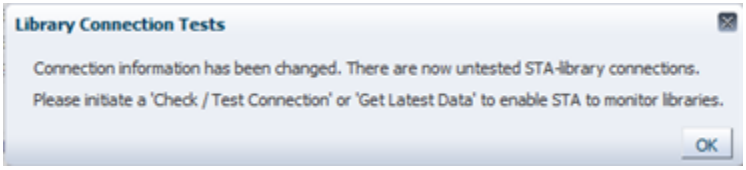
     Caution: If you leave this field blank, scheduled automatic library data collections are disabled. This will cause your STA library configuration data to become out of sync with the library.

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



4. Click **Save**.

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



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

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

Test a Library SNMP Connection

Use this procedure to test the SNMP connection between STA and a library and establish or re-establish the communication handshake. See "When to Perform a Connection Test" on page 11-3 for required and recommended times to perform this procedure.

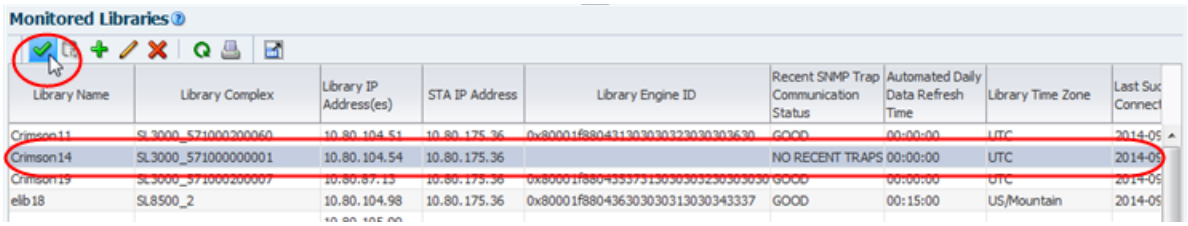
You can test only one library connection at a time.

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

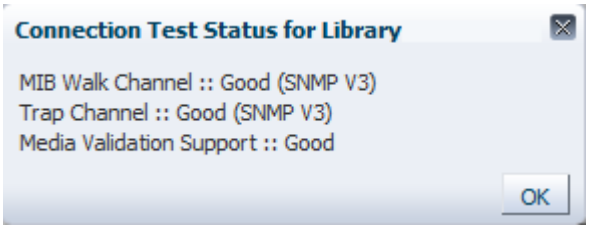
Note: Before performing this procedure, you may want to verify that the library is operational.

1. In the Navigation Bar, select **Setup & Administration**, then select **SNMP Connections**.

2. In the Monitored Libraries table, select a library, and then click **Check / Test Connection**.

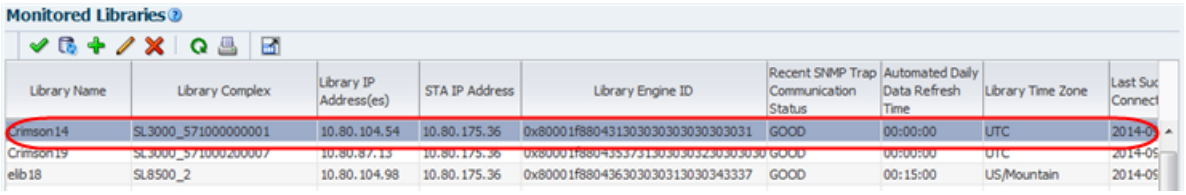


The Connection Test Status message box appears, displaying results for the MIB Walk Channel, Trap Channel, and Media Validation Support tests.



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

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



- If the Library Complex field is blank, it will be supplied after you perform a manual data collection.
- Library Engine ID indicates the unique SNMP engine ID for the library. See "Understanding the Library Engine ID" on page 11-2 for details.
- Last Connection Attempt indicates the date and time when the connection test was initiated.
- Last Successful Connection indicates the date and time when the test was completed, if successful.
- Last Connection Status indicates the results of the test. If the test fails, STA provides information in the Last Connection Failure Detail field. (You may need to extend the column width to see the entire value.)

4. If the test fails, repeat this procedure as follows:
   - If the test fails because of a timeout, repeat this procedure during a period of lower library activity. Once the test completes, you can compare the timestamps to verify that the library is providing current information
   - If the test fails for any other reason, edit the connection details for the library and clear the Library Engine ID field before repeating this procedure. See "Configure the SNMP Connection to a Library" on page 11-11 for instructions.

Perform a Manual Data Collection

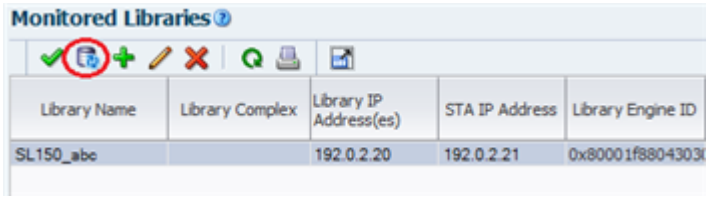
Use this procedure to initiate a manual data collection for a library and get the latest library configuration data. If this procedure is completed successfully, STA begins monitoring the library and performing analytics on the data.

Although STA performs a data collection automatically every 24 hours at the scheduled time, you must perform a manual data collection for each monitored library whenever you add or change SNMP configuration settings for the library or the STA client. See "Required Data Collection Times" on page 11-6 and "Recommended Data Collection Times" on page 11-6 for additional details about when to perform this procedure.

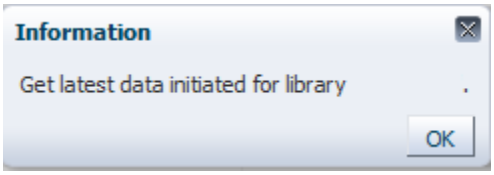
Data collections may take several minutes to an hour, depending on library size.

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

1. In the Navigation Bar, select **Setup & Administration**, then select **SNMP Connections**.
2. Select a library in the Monitored Libraries table, and then click **Get latest data**. You can select only one library at a time.



A confirmation message box appears.



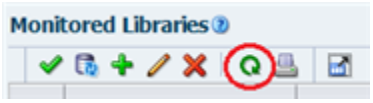
3. Click **OK** to dismiss the message box.

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

   - Library Complex indicates the library complex ID.
   - Library Engine ID indicates the unique SNMP engine ID for the library. See "Understanding the Library Engine ID" on page 11-2 for details.
   - Last Connection Attempt indicates the date and time when the data collection was initiated.
   - Last Successful Connection indicates the date and time when the data collection was completed, if successful.
   - Last Connection Status is updated as follows:
     - IN PROGRESS: The data collection process is underway.

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

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



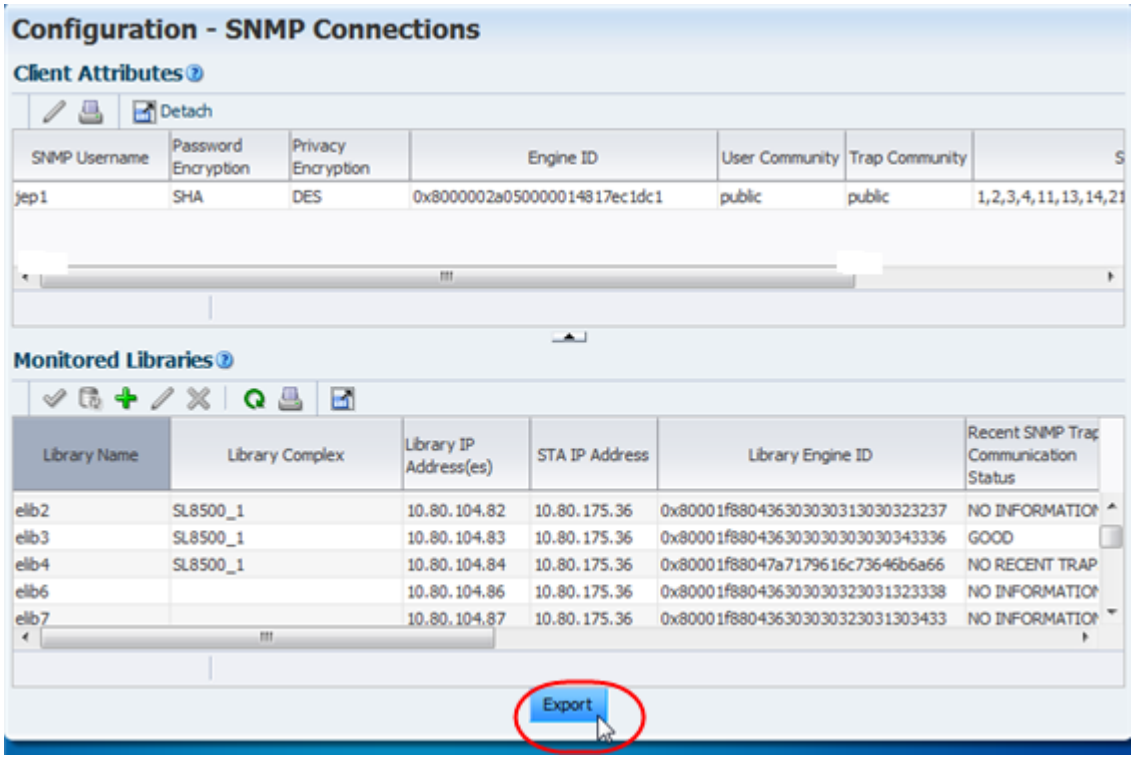
- Recent SNMP Trap Communication Status may intermittently indicate MISSED HEARTBEAT. This is normal.

Export SNMP Connection Settings to a Text File

Use this procedure to export all SNMP connection information to a text file. Passwords are not included in the file.

This file is useful for troubleshooting connection issues or re-entering connection information. Example 11–8 is a sample file.

1. In the Navigation Bar, select **Setup & Administration**, then select **SNMP Connections**.



2. At the bottom of the screen, click **Export**.

   The file is saved with the name SnmpConfiguration.txt.

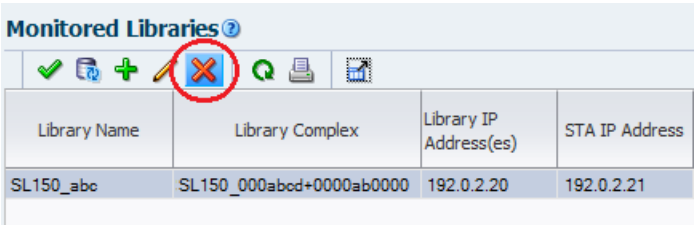
Example 11–8 Sample SNMP Configuration File

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

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

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

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

STA IP Address = 10.80.145.78
Library Name = SL3000A
Library Complex = SL3000_5720123200089
Library Primary IP Address = 10.80.104.51
Library Secondary IP Address = Not Specified
Library Engine ID = 0x80001f8804313030301231233030000
Requested MIB Walk Time = 00:00:00
Library Serial Number = 5720123200089
Library Time Zone = UTC
Recent SNMP Trap Communication Status = GOOD
Last Connection Status = SUCCESS
Last Connection Failure Detail = Not Specified
```

Remove a Library Connection From STA

Use this procedure to remove a library SNMP connection from STA. All existing data for the library will be removed from the STA screens but will be retained in the STA data store. See "Removed Libraries" on page 12-8 for details about the impact of this procedure.

1. In the Navigation Bar, select **Setup & Administration**, then select **SNMP Connections**.
2. In the Monitored Libraries table, select the library to remove, and then click **Delete**.



3. Delete the STA SNMP trap recipient from the library.

   snmp deleteTrapRecipient id *index*

   Where:

- *index* is the index number of the trap recipient to be deleted.

For example:

```
ADMIN> snmp deleteTrapRecipient id 1
requestId 1
requestId 2
Device 1,0,0,0
Success true
Done
Failure Count 0
Success Count 1
COMPLETED
```

Supporting SNMP Maintenance Tasks Performed on the Library

Use these procedures as necessary to display or modify SNMP connection information on the library.

- "Verify the Library is Operational" on page 11-18
- "Display All SNMP Trap Recipients" on page 11-19
- "Delete or Modify the STA Trap Recipient" on page 11-20

Verify the Library is Operational

Use this procedure to verify that the library is fully initialized and operational. You may want to perform this procedure before doing an SNMP 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 time, to minimize library disruption, complete this procedure for all libraries before testing the SNMP connections.

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

SL500 Libraries

1. Log in to the library with the SL Console.
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 Libraries

1. Log in to the library with the SL Console.
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.

SL150 Libraries

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

Display All SNMP Trap Recipients

Use this procedure to display all trap recipients defined on the library and verify the settings.

All libraries except SL150

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

   snmp listTrapRecipients

   For example:

   ```
   ADMIN> snmp listTrapRecipients
   requestId
   requestId 1
   Attributes Auth SHA
    AuthPass *****
   Engine Id 0x80001f88807ad87e39453f
   Host 192.0.2.20
   Index 1
   Name STAuser
   Port 162
   Priv DES
   Priv Pass *****
   Trap Level 1,2,3,4,11,13,14,21,25,27,41,45,61,63,65,81,85,100
   Version v3
   Object Snmp snmp
   Done
   Failure Count 0
   Success Count 1
   COMPLETED
   ```

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

SL150 libraries

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.

Delete or Modify the STA Trap Recipient

Use this procedure to 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.

All libraries except SL150

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

   requestId 1

   requestId 2

   Device 1,0,0,0

   Success true

   Done

   Failure Count 0

   Success Count 1

   COMPLETED
3. Re-add the trap recipient, as necessary. See the *STA Installation and Configuration Guide* for instructions.

SL150 libraries

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**.

Special SNMP Connection Update Tasks

The following tasks are required only in special situations. See

- "Update the SNMP Connection After a Library Redundant Electronics Switch" on page 11-21
- "Update the SNMP Connection After a Library Firmware Upgrade" on page 11-21
- "Update the SNMP Connection After a Change to the STA Server IP Address" on page 11-22

Update the SNMP Connection After a Library Redundant Electronics Switch

Note: This procedure applies to SL3000 and SL8500 libraries only.

If STA is configured to support Redundant Electronics 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 the following manual procedure after the switch completes.

This procedure is performed from the STA user interface.

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 a Library SNMP Connection" on page 11-13 for instructions.
3. Perform a data collection to retrieve the current library configuration data. See "Perform a Manual Data Collection" on page 11-15 for instructions.
4. If a controller card is replaced after the Redundant Electronics switch, the IP address for the library changes, so you must re-enter the SNMP connection information in STA. See "Configure the SNMP Connection to a Library" on page 11-11 for instructions.

See the *STA Installation and Configuration Guide* for full details on configuring STA to support Redundant Electronics.

Update the SNMP Connection After a Library Firmware Upgrade

Note: This procedure does not apply to SL150 libraries.

Use this procedure to update the library and STA SNMP configurations after upgrading to one of the following library firmware versions or higher:

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

Starting with these firmware versions, the library engine ID is generated with a new 32-bit value. You must perform the following tasks so that STA can receive SNMP traps from the library.

- "Update SNMP Settings in STA" on page 11-21
- "Verify SNMP Settings on the Library" on page 11-22

Update 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" on page 11-11.

   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 a Library SNMP Connection" on page 11-13 for instructions.
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. See "Display All SNMP Trap Recipients" on page 11-19 for instructions.
3. Verify the SNMP Version level displayed 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" on page 11-20 for instructions.
7. Re-add the STA SNMP v3 trap recipient using the new library engine ID. See the procedure for creating an SNMP v3 trap recipient in the *STA Installation and Configuration Guide* for instructions.

Update the SNMP Connection After a Change to 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.

The procedure is divided into the following parts:

- "Confirm Network and SNMP Connectivity" on page 11-22
- "Update SNMP Settings on the Library" on page 11-22
- "Update SNMP Settings in STA" on page 11-23

Confirm Network and SNMP Connectivity

1. Confirm good communication between STA and the library. See "Verify SNMP Communication With a Library" on page 11-7 for instructions.

Update SNMP Settings on the Library

1. Retrieve the index number of the STA trap recipient. See "Display All SNMP Trap Recipients" on page 11-19 for instructions.
2. Delete the STA trap recipient with the old IP address. See "Delete or Modify the STA Trap Recipient" on page 11-20 for instructions.
3. Add the STA trap recipient with the new IP address. See the *STA Installation and Configuration Guide* for instructions.

Update SNMP Settings in STA

1. Update the STA IP address in the SNMP connection settings. See "Configure the SNMP Connection to a Library" on page 11-11 for instructions.
2. Re-establish the SNMP connection with the library. See "Test a Library SNMP Connection" on page 11-13 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 "Perform a Manual Data Collection" on page 11-15 for instructions.

SNMP Connection Troubleshooting Tasks

The following tasks help to diagnose and resolve issues with the SNMP connection between STA and a monitored library. Use the procedures that apply to the problem you are experiencing.

- "Troubleshoot a Failed MIB Walk Channel Test" on page 11-23
- "Troubleshoot a Failed Trap Channel Test" on page 11-25
- "Troubleshoot a Failed Media Validation Support Test" on page 11-26
- "Troubleshoot Unsuccessful Trap Processing" on page 11-26

See "Connection Test Status Messages" on page 11-4 for examples of the messages displayed with failed connection tests.

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.

Use this procedure to diagnose and resolve the issues. See the *STA Installation and Configuration Guide* for detailed instructions for steps performed on the library.

Steps to Perform on the Library

1. Log in to the library CLI.
2. Verify that the library is fully initialized. See "Verify the Library is Operational" on page 11-18 for instructions.
3. Check communication from the library to the STA server. This command is not available on the SL150.
   - SL8500 and SL3000:

     traceRoute *sta_server_IP_addr*

   - SL500:

traceroute *sta_server_IP_addr*

Where:

– *sta_server_IP_addr* is the IP address of the public port on the STA server.

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 the procedure for enabling SNMP on the library in the *STA Installation and Configuration Guide* for instructions.
5. Verify that there is one and only one SNMP v2c user. See the procedure for ensuring there is an SNMP v2c user in the *STA Installation and Configuration Guide* for instructions.
6. 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 the procedure for creating an SNMP v3 user in the *STA Installation and Configuration Guide*.
7. Verify that a static IP address has been assigned to the library. See the procedure for retrieving the library IP address in the *STA Installation and Configuration Guide* for instructions.
8. 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** *library_IP_addr*

   Where:

   – -I (upper-case "I") indicates to use Internet Control Message Protocol (ICMP) echo request packets instead of User Datagram Protocol (UDP) datagrams.

   – *library_IP_addr* is the IP address of the public port on the library.

   The output shows the number of hops and the round-trip time to reach each one. The round-trip time (the last line in the command output) should be less than one second. If it is not, confirm the network's performance with your network administrator.
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" on page 11-7 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 Settings for STA" on page 11-9 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" on page 11-11 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, 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. See the *STA Installation and Configuration Guide* for detailed instructions for steps performed on the library.

1. Verify that the library is running the recommended or higher firmware. See the *STA Requirements Guide* for detail. Lower firmware versions may not support the test trap (13).
2. After upgrading to STA 2.0.x, 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" on page 11-11 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" on page 11-19 for instructions.
   - Engine Id: Must match the library engine ID displayed in Step 3. 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 from Step 3 matches the value in the STA Monitored Libraries screen. See "Configure the SNMP Connection to a Library" on page 11-11 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 a Library SNMP Connection" on page 11-13 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 this procedure to diagnose and resolve the issues. See the *STA Installation and Configuration Guide* for detailed instructions for steps performed on the library.

1. Verify that the library and drives meet the minimum firmware levels required for media validation. See the *STA Requirements Guide* for details.
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 *STA Installation and Configuration Guide*.

See the *STA User's Guide* for details about configuring media validation.

Troubleshoot Unsuccessful Trap Processing

Use this procedure 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** *library_IP_addr* **> /var/tmp/***file_name* **&**

   Where:

   - -v indicates verbose output.
   - host indicates to collect packets to or from the indicated host only (in this case, the library).
   - *library_IP_addr* is the IP address of the public port on the library.
   - *file_name* is the name of the file to which to save the output.
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" on page 11-25.
5. Verify that SNMP port 162 is available for STA. The STA trap listener processes traps through this port.

   If necessary, perform the following steps to 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 –l snmp**

   # **netstat –anp |grep ":162"**

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

   # **chkconfig —list**

6. If the snmpd or snmtrapd services are running, perform the following steps to ensure they are turned off permanently.

   a. Deconfigure SNMP services.

      # **chkconfig snmpd off**

      # **chkconfig snmptrapd off**

   b. Stop SNMP services.

      # **service snmptrapd stop**

      # **service snmpd stop**

   c. Stop and restart STA services.

      # **STA stop 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 *STA Installation and Configuration Guide* 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. See the procedures for setting the volume label format in the *STA Installation and Configuration Guide* for details.

12

Understanding STA Analytics

This section provides concepts and tasks to help you interpret and use the data provided by STA. It assumes a basic understanding of STA features and functions.

This chapter includes the following sections:

- Data Retention
- Incomplete Exchanges
- Dimmed Values on STA Screens
- Removed Drives and Media
- Removed Libraries
- What Happens to Data When an SL8500 Library is Moved to a New Complex
- "Missing" Media
- Duplicate Volume Serial Numbers
- Mapping Host and STA Drive Identifiers

Data Retention

Data in the STA data store is retained indefinitely as a historical record and never deleted. However, data for removed resources—libraries, drives, and media—may be hidden from the STA data screens depending on the Data Handling settings for your username. See "Removed Drives and Media" on page 12-2 and "Removed Libraries" on page 12-8 for details.

When STA first begins tracking a library, drive, or media, that resource is assigned an STA Start Tracking timestamp. If the resource is later removed from the library environment, an STA Stop Tracking timestamp is assigned. And then if the resource is later re-added, the STA Start Tracking attribute reflects the original timestamp assigned when STA first began tracking the resource.

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

Incomplete Exchanges

A media exchange may take from seconds to hours to process and complete depending on the nature of the initiating host request. To perform full analytics on an exchange and update drive and media health, STA must receive information from both the media mount and dismount events. If a library connection is dropped while

exchanges are in process, you may notice incomplete exchanges on the Exchanges Overview screen.

Following are some reasons why library connections may be dropped:

- 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.

When the library connection is restored, STA processes and reports all new exchanges normally. While the connection is down, however, STA receives no exchange information, which has the following effects:

- STA receives no record of exchanges that start and finish completely during the connection down time. These exchanges do not appear on the STA screens and are not used in calculating drive or media health.
- STA receives only partial information for exchanges that either start or finish while the connection is down. For example, for exchanges that start while the connection is down and finish after it has been restored, STA receives only the dismount information. Conversely, STA receives only the mount information for exchanges that start while the connection is up but finish while it is down. For these partial exchanges, STA does not have enough information to perform full analytics, and attributes such as Drive and Media Health, Exchange Elapsed Time, Exchange Mount Time, and Media and Drive Exchange Status on the Exchanges Overview screen are set to null or "Unknown". Additionally, these exchanges are not used in calculating drive or media health.

Dimmed Values on STA Screens

At times you may see data elements or resource identifiers that are *dimmed*—or grayed out—on the screen. While these data elements are usually active links leading to additional detail, the dimmed values are not links. Following are elements that may be dimmed:

- Removed drives; see "Removed Drives and Media" on page 12-2 for details.
- Removed media; see "Removed Drives and Media" on page 12-2 for details.
- Exchanges not yet complete; once the exchange completes, the identifier is no longer dimmed, and the link is active.
- Alert Event types for which a corresponding element does not exist

Dimmed data elements may also be the result of an upgrade in progress. They gradually become active links as they are processed.

Removed Drives and Media

By default, drives and media that have been removed from your tape library environment do not appear on the STA screens. The Data Handling preferences for your STA username allow you to turn on the display of removed drives, removed media, or both. Your selections take effect immediately, so depending on your needs, you can selectively show or hide removed drives and media throughout your login session. See the following sections for additional detail:

- The *STA Screen Basics Guide* for instructions on changing these display settings.
- "Identifying Removed Drives and Media" on page 12-3 for how removed drives and media are displayed on Overview screens.

- "Impact of Removed Drives and Media on Calculated Totals" on page 12-3 for how calculated values are affected by these display settings.

> **Note:** Data for removed drives and media is never removed from the STA data store. See "Data Retention" on page 12-1 for details.

Identifying Removed Drives and Media

If you choose to display removed drives or media, they are identified by the following attribute values on the Drives – Overview and Media – Overview screens:

- 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. Because there may be a lag between the time when a drive or media is removed and when the library notifies STA of the change, this value may differ slightly from the time when the item was physically removed.
- The following attributes are set to "REMOVED":
  - Library Complex Name
  - Drive Library Name or Media Library Name
  - Library Model
  - Partition Type
  - Partition Name
  - Physical Address

  On activity screens, such as Exchanges – Overview and Media Validation Overview, the identifiers for removed drives and media are dimmed. See "Dimmed Values on STA Screens" on page 12-2 for details.

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. As drives and media are added and removed from your system, the total number of drives and media used for STA calculations also varies. These variations can result in differences between a historical summary value, such as a 30-day rolling average, and a corresponding value calculated using only currently displayed records.

- 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; therefore, they are not affected by the removed drives and media settings for your STA username. For example, a drive removed on day 10 of a 30-day period will be included in calculating summaries and averages for the first 10 days of the period, but not for the remaining 20 days. See "How Removed Drives and Media Affect Calculated Summaries" on page 12-4 for examples.
- Currently Displayed Values—Totals and aggregations displayed on Overview and Analysis screens are calculated based on the number of records currently displayed; therefore, they are affected by the removed drives and media settings for your STA username. For example, if your removed drives display setting is turned off, removed drives will not be listed on the Drives – Overview screen, nor will they be included in the total record count on that screen, nor in the aggregations on the Drives – Analysis screen. See "How Removed Drives and Media Affect Overview and Analysis Screens" on page 12-4 for examples.

How Removed Drives and Media Affect Calculated Summaries

STA calculates a wide variety of daily and 30-day summary attributes, such as megabytes read, written, sent, and received; number of drive errors and cleans; and percent drive utilization. Drives and media are included in calculating these values up until the time they are removed from the tape library system.

For example, removing a drive from a monitored library at 17:00 on April 15 has the following impacts to these summary values:

- Daily summaries — The drive's activity for April 15 before 17:00 is included in the day's daily summaries. Because the drive has been removed, it will not have any activity to include in daily summaries for April 16 and beyond.
- 30-day summaries — The drive's activity is included in all 30-day summaries for April 15 and the next 30 days, although the number of days' activity included will be reduced with each succeeding day, as the 30-day window moves forward. The 30-day summary on May 15 will be the first one that does not include any activity for the drive.

How Removed Drives and Media Affect Overview and Analysis Screens

This section provides examples illustrating the effects of your removed drives and media display settings on the following screens.

- "Drives – Overview Screen" on page 12-4
- "Drives – Analysis Screen" on page 12-6
- "Exchanges and Cleaning Activities Screens" on page 12-7
- "Alerts Overview Screen" on page 12-8
- "Media Validation Overview Screen" on page 12-8

Note: While these examples focus on removed drives, the same principles and screen display characteristics apply to removed media and the "Show Removed Media" settings.

Drives – Overview Screen

Figure 12–1 shows the Drives – Overview screen after the "Show Removed Drives" setting has been selected. Removed drives are listed on the Drives – Overview screen, and the total number of records includes the removed drives. In this example, there are a total of 1,024 drives, and drive HU180214PT is highlighted to show that the Library Complex Name and Drive Library Name both indicate "REMOVED," and the date the drive was removed is displayed in the STA Stop Tracking column.

Figure 12–1 Drives – Overview Screen, Show Removed Drives Setting "On"

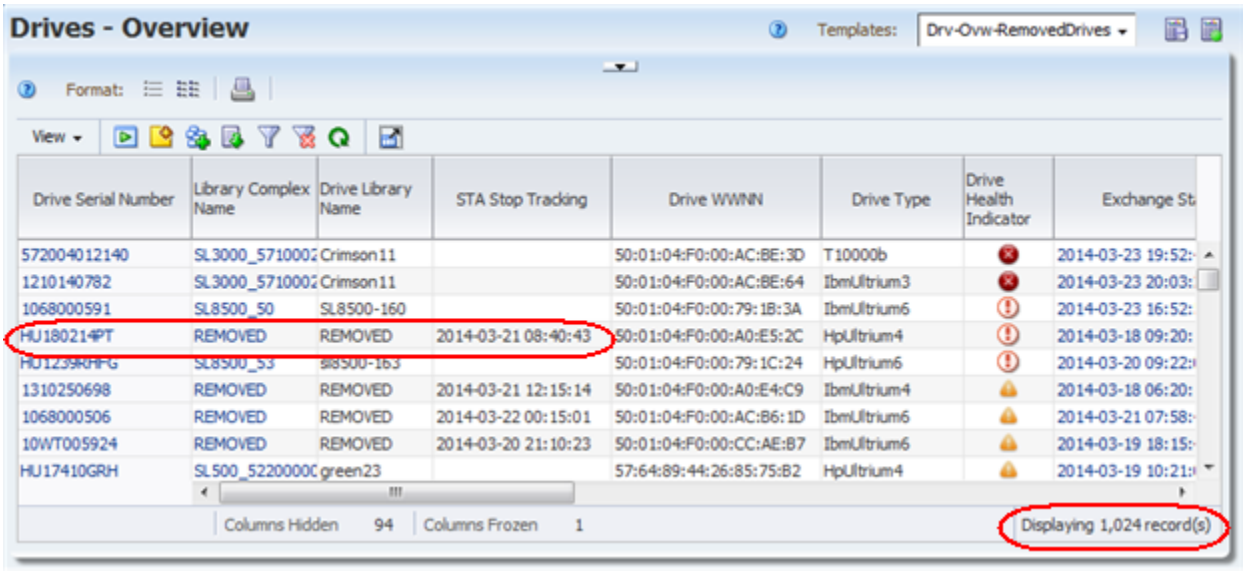
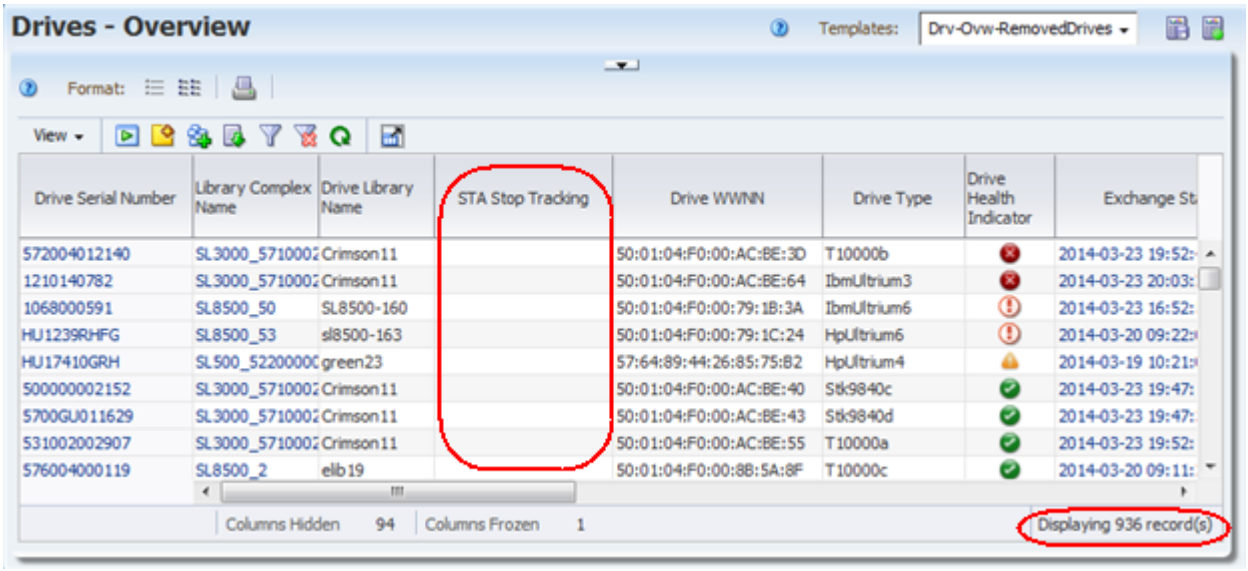


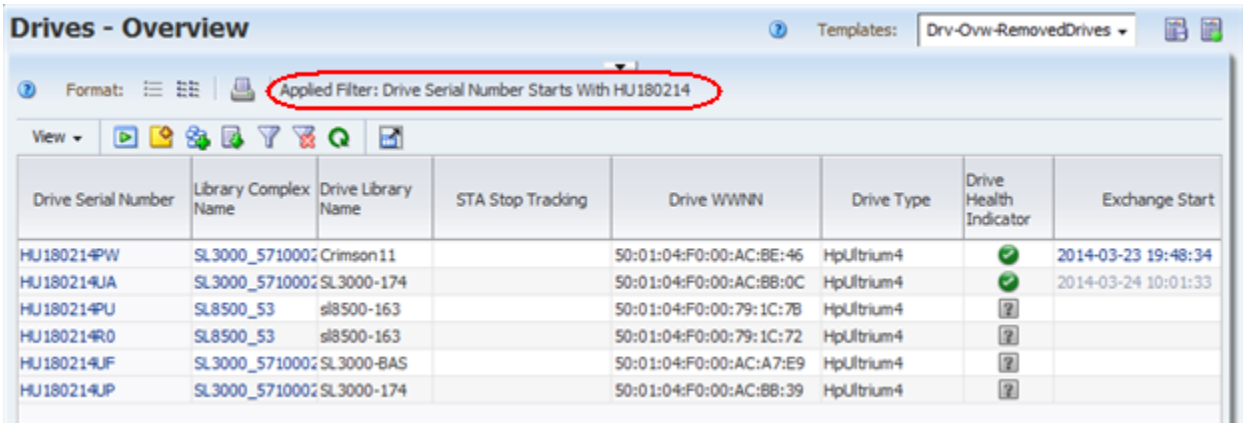
Figure 12–2 and Figure 12–3 show the Drives – Overview screen after the "Show Removed Drives" setting has been deselected. Removed drives are not listed on the Drives – Overview screen, and the total number of records does not include removed drives. In Figure 12–2, there are a total of 936 drives, and the STA Stop Tracking date is blank for all drives displayed.

Figure 12–2 Drives – Overview Screen, Show Removed Drives Setting "Off"



In Figure 12–3, the Drives – Overview screen has been filtered to show all drives with serial numbers starting with "HU180214." The removed drive HU180214PT does not appear in the list.

Figure 12–3 Drives – Overview Screen, Show Removed Drives Setting "Off" and Filtered for a Known Removed Drive



Drives – Analysis Screen

Figure 12–4 shows the Drives – Analysis screen after the "Show Removed Drives" setting has been selected. Aggregated data for removed drives are included under the headings Library Complex Name "REMOVED" and Drive Library Number "-1". The total number of drives is 1024, and the total removed drives is 88.

Figure 12–4 Drives – Analysis Screen, Show Removed Drives Setting "On"

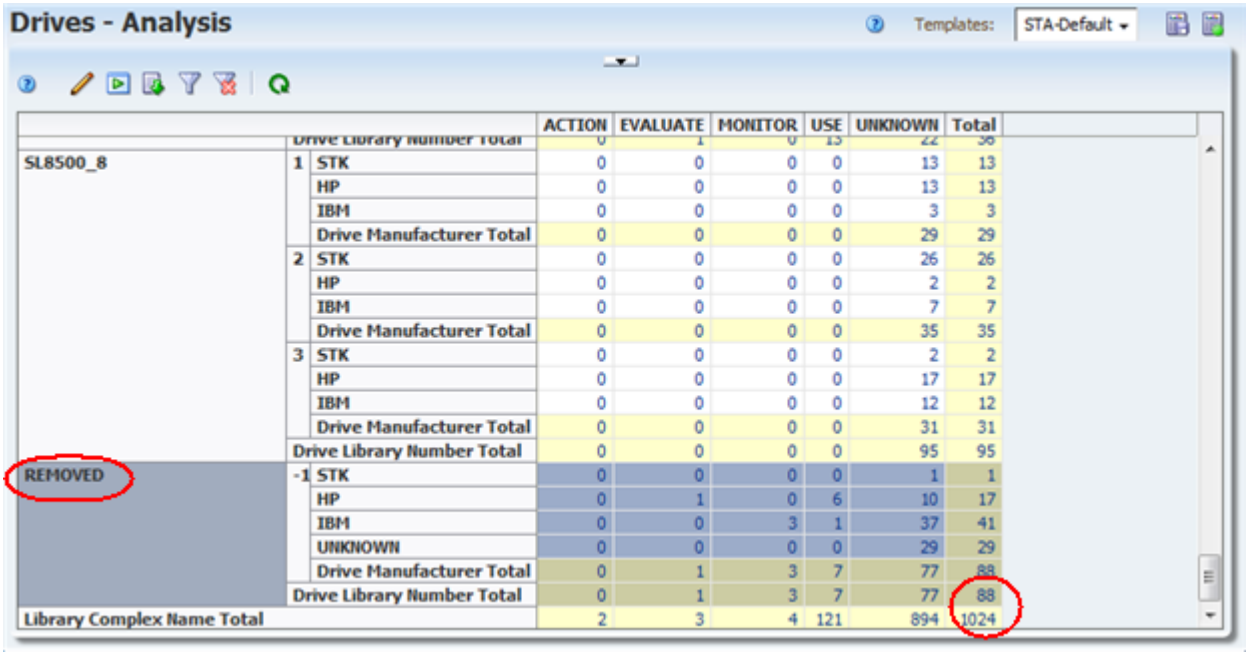
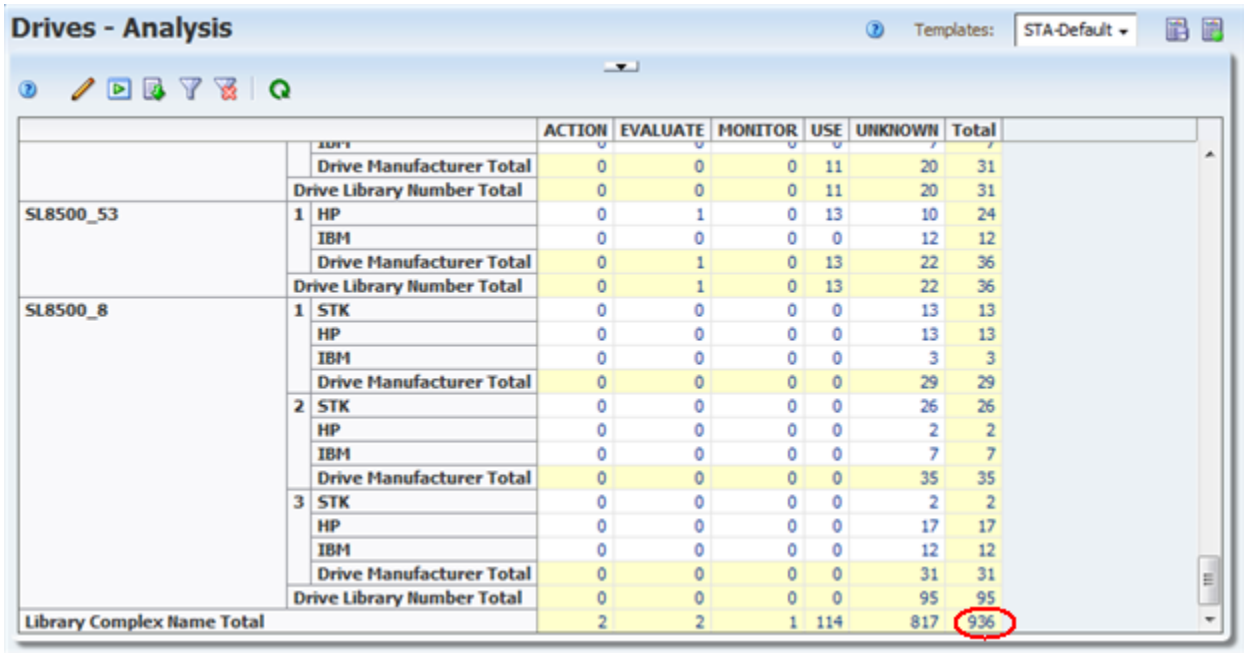


Figure 12–4, shows the Drives – Analysis screen after the "Show Removed Drives" setting has been deselected. Aggregated data for removed drives are not included in the table. There are no headings for Library Complex Name "REMOVED" and Drive Library Name "-1". The total number of drives is 936.

Figure 12–5 Drives – Analysis Screen, Show Removed Drives Setting "Off"



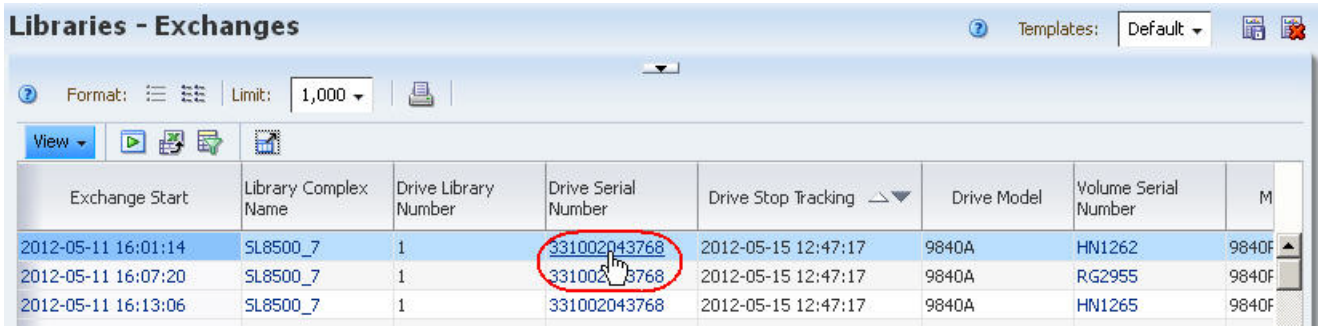
			ACTION	EVALUATE	MONITOR	USE	UNKNOWN	Total
		Drive Manufacturer Total	0	0	0	11	20	31
	Drive Library Number Total		0	0	0	11	20	31
SL8500_53	1	HP	0	1	0	13	10	24
		IBM	0	0	0	0	12	12
		Drive Manufacturer Total	0	1	0	13	22	36
	Drive Library Number Total		0	1	0	13	22	36
SL8500_8	1	STK	0	0	0	0	13	13
		HP	0	0	0	0	13	13
		IBM	0	0	0	0	3	3
		Drive Manufacturer Total	0	0	0	0	29	29
	2	STK	0	0	0	0	26	26
		HP	0	0	0	0	2	2
		IBM	0	0	0	0	7	7
		Drive Manufacturer Total	0	0	0	0	35	35
	3	STK	0	0	0	0	2	2
		HP	0	0	0	0	17	17
		IBM	0	0	0	0	12	12
		Drive Manufacturer Total	0	0	0	0	31	31
	Drive Library Number Total		0	0	0	0	95	95
Library Complex Name Total			2	2	1	114	817	936

Exchanges and Cleaning Activities Screens

The Exchanges Overview and Drive Cleanings Overview screens always show exchanges involving removed drives and media, regardless of your display settings. All screen attributes indicate the values at the time of the exchange.

In Figure 12–6, the "Show Removed Drives" setting is selected. The "Drive Serial Number" entries for removed drives are active links to the Drives – Overview, Detail View screen.

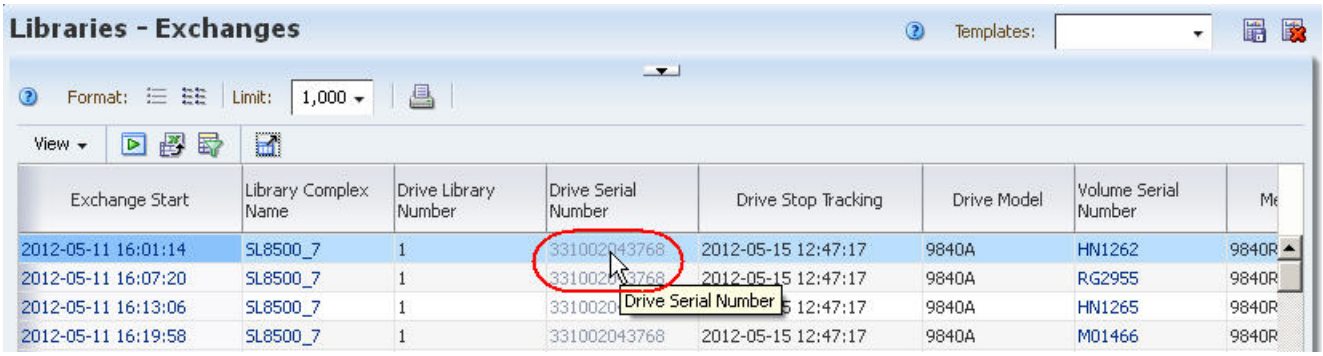
Figure 12–6 Exchanges Overview Screen, Show Removed Drives Setting "On"



Exchange Start	Library Complex Name	Drive Library Number	Drive Serial Number	Drive Stop Tracking	Drive Model	Volume Serial Number	M
2012-05-11 16:01:14	SL8500_7	1	331002043768	2012-05-15 12:47:17	9840A	HN1262	9840F
2012-05-11 16:07:20	SL8500_7	1	331002[illegible]3768	2012-05-15 12:47:17	9840A	RG2955	9840F
2012-05-11 16:13:06	SL8500_7	1	331002043768	2012-05-15 12:47:17	9840A	HN1265	9840F

In Figure 12–7, the "Show Removed Drives" setting is deselected. The "Drive Serial Number" entries for removed drives are dimmed and are not active links.

Figure 12–7 Exchanges Overview Screen, Removed Drives Setting "Off"



Alerts Overview Screen

The Alerts Overview screen always shows alerts involving removed drives and media, regardless of your display settings. Alerts are always retained, even after the associated drive or media has been removed.

In the following example, your "Show Removed Drives" setting has been deselected. STA is monitoring LibraryABC, which has 60 drives, and two drives are responsible for all 27 drive alerts seen in the last 30-day period. The two drives are subsequently removed from the library.

On the Drives – Overview screen, the value of the Drive Alerts (30 Days) attribute is "0" for all drives in LibraryABC. This is because the drives responsible for all 27 alerts have been removed from the library.

On the Alerts Overview screen filtered by "Alert Type Is Drive", 27 alerts are shown.

Media Validation Overview Screen

Pending STA media validation requests for removed drives and media remain in the validation request queue until you explicitly cancel them. See "Cancel Pending Media Validation Requests" on page 8-49 for details

Removed Libraries

If you remove a library from the tape library environment, the following updates are made immediately to the STA screens:

- STA no longer collects data from the library, and you can delete the STA server trap recipient from the library SNMP configuration.
- The library is removed from the Libraries Overview and Complexes Overview screens.
- The drives and media included in the library are removed from the Drives and Media screens.
- All exchanges and cleaning activities that have occurred in the library are removed from Exchanges Overview and Drive Cleanings Overview screens.
- All messages for the library and its drives and media are removed from the Drives Messages, Media Messages, and All Messages Overview screens.
- Pending STA media validation requests remain in the validation request queue until you explicitly cancel them. See "Cancel Pending Media Validation Requests" on page 8-49 for details

See "Remove a Library Connection From STA" on page 11-17 for instructions.

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. See "Data Retention" on page 12-1,.

What Happens to Data When an SL8500 Library is Moved to a New Complex

Note: This information applies to SL8500 libraries only; other library models cannot be moved between complexes.

Because STA rolls up all data to the applicable library complex, moving an SL8500 library from one complex to another affects the way data is displayed, sorted, and filtered on all STA screens.

In STA, each library complex is identified by a unique Library Complex Name. For SL8500 complexes, the value for this attribute is a concatenation of the library model and the complex ID—for example, SL8500_1 or SL8500_53. Oracle Service manually assigns the SL8500 complex ID to the library when it is installed and ensures that each complex at your site has a unique ID. See the *STA Installation and Configuration Guide* for additional details about complex IDs.

All SL8500 libraries in a multi-library complex share the same Library Complex Name, and if a library is moved from one complex to another, its Library Complex Name changes to reflect the new complex ID. This affects how data for the library is rolled up and displayed, as described in the following scenario.

1. An SL8500 library, "BigLibrary1", 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 BigLibrary1. The Library Complex Name for BigLibrary1 is SL8500_1.
3. STA monitors BigLibrary1, and all data for the library is rolled up to Library Complex Name SL8500_1.
4. After three months, you decide to move BigLibrary1 to a new complex. You remove the STA connection to BigLibrary1, and all data for the library is retired, as described in "Removed Libraries" on page 12-8.
5. Oracle Service moves BigLibrary1 to the new complex, which has complex ID 2.
6. You reestablish the STA connection to BigLibrary1. This has the following effects on new and historical data for the library:
   - Because BigLibrary1 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 BigLibrary1 is associated to two different complexes, depending on the time period.

"Missing" Media

Media must be in a library storage cell or drive at the time of a data collection in order for it to be detected (see "Maintaining SNMP Connections and the STA Data Store" on page 11-2 for details about the data collection process). Media in a "transient" location is not detected by a data collection. Transient locations are defined as any of the following:

- Robot hand
- Elevator — SL8500 libraries only
- Pass-thru port (PTP) — SL8500 complexes only
- Drive, at the time of library initialization; that is, the library was re-initialized while the media was left in the drive.

The STA application includes logic to handle these transient movements — media that has unexpectedly "disappeared" is kept on the STA screens in anticipation of detecting it again within a specific short period of time. STA removes the media from the screens only if it still does not detect the media within that time period. Although this is a rare occurrence, you are most likely to observe it in an SL8500 complex, where media cartridges are frequently transferred from one library to another through pass-thru ports (PTPs).

If you cannot find a volume serial number (VSN or volser) that you expect to see on the Media – Overview screen, it is recommended that you do the following:

1. Verify that you have the correct volser.
2. Filter the Media – Overview screen for that volser, to be sure it is really missing from the list.
3. If the volser appears on the Media – Overview screen, check the Start Tracking, End Tracking, and Ejected Date attributes. The Ejected Date indicates the media was ejected through a cartridge access port (CAP) or access expansion module (AEM) (SL3000 libraries), or mailslot (SL150 libraries).
4. If the media has an End Tracking date but no Ejected Date, the media may have been removed from the library environment by an unsupported method, such as through an open library door. On the Dashboard, check the Media Exception Report portlet. 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 "Perform a Manual Data Collection" on page 11-15 for instructions.

Duplicate Volume Serial Numbers

In the STA data store, media history is retained by volume serial number (VSN or volser). That is, all history for a particular piece of media is tied to its volser. For this reason, it is recommended that you avoid duplicate volume serial numbers (VSNs or volsers) in the tape environment monitored by STA. 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 to be duplicates only if the media with the same volser also have the same domain and 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.

- T10000T1 – "T10000" is the domain and "T1" is the type.

The same volser used on two different LTO4 cartridges would be considered duplicate, while the same volser on an LTO4 cartridge and an LTO5 or T10000T1 cartridge would not.

True duplicate volsers may occur for a variety of reasons, such as:

- In the case of cleaning media, there are only 999 globally available volsers. Large tape environments with 1,000 or more cleaning media will of necessity have duplicate volsers.
- Various tape management applications may allow duplicate volsers. This is the case only for libraries with SCSI host connections —SL150, SL500, and some SL3000 libraries. Libraries with Host Library Interface (HLI) host connections — SL8500 and some SL3000 libraries — use Oracle's StorageTek Enterprise Library Software (ELS) or Oracle's StorageTek Automated Cartridge System Library Software (ACSLS), which do not allow duplicates.

Following are situations in which there may appear to be duplicate volsers, but in fact there is just one media and the volser is unique:

- A media is moved from one library to another.
- A media is ejected from a library, taken off site for some time, and then re-entered into a library.

"Duplicate Detected" Flag on Exchanges

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 volser to one of the media, as the data for the two will be co-mingled. See the *STA Data Reference Guide* for additional information.

> **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.

Mapping Host and STA Drive Identifiers

In STA, tape drives can be identified by drive serial number, World Wide Name (WWN), or physical location within the library. However STA does not know, and cannot display, the logical device ID that a host uses to identify a drive. If you want to map the host drive identifiers to the STA identifiers, you must do this manually.

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 DRives 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.

Example 12–1 Sample ELS Display DRives 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.

Example 12–2 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
#
```

13

Using STA to Answer Tape Environment Questions

This chapter combines elements and procedures described in the previous chapters to address common questions about tape storage operations and health. The methods described are not exhaustive, but are meant as examples of some ways you can use STA to answer these and similar questions, and in the process build your expertise in using the STA product.

Each procedure includes a "Referenced Tasks" section, which refers to the elements and procedures from previous chapters.

This chapter includes the following topics:

- Drive and Media Health Questions
- Capacity and Resource Management Questions
- Best Practices for Investigating Tape Environment Issues

Drive and Media Health Questions

Question	Task
Which drives and media have had the most errors in the last 30 days? Are there any correlations between the two?	"Report the Media and Drive With the Most Errors" on page 13-1
Which drives have had the most errors this week? Have their error rates gone up?	"Report Trends in Drive Error Rates" on page 13-8
Which drives have had significantly declining efficiency over time?	"Report Drive Efficiency Trends" on page 13-14
Is the drive that failed twice today the same one that caused problems two months ago?	"Report Trends in Drive Failures" on page 13-17
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?	"Report Information to Help Troubleshoot Tape Job Errors" on page 13-19
What critical errors were reported to STA last month? Is the total number trending up, down, or staying stable?	"Report Trends in Critical Errors" on page 13-23

Report the Media and Drive With the Most Errors

These procedures address the questions, "Which drives and media have had the most errors in the last 30 days? Are there any correlations between the two?"

The following methods are described:

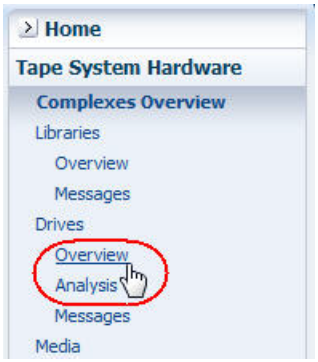
- "Report Drives With the Most Errors", below
- "Report Media With the Most Errors" on page 13-4
- "Display Correlations Between the Two" on page 13-6

Referenced Tasks

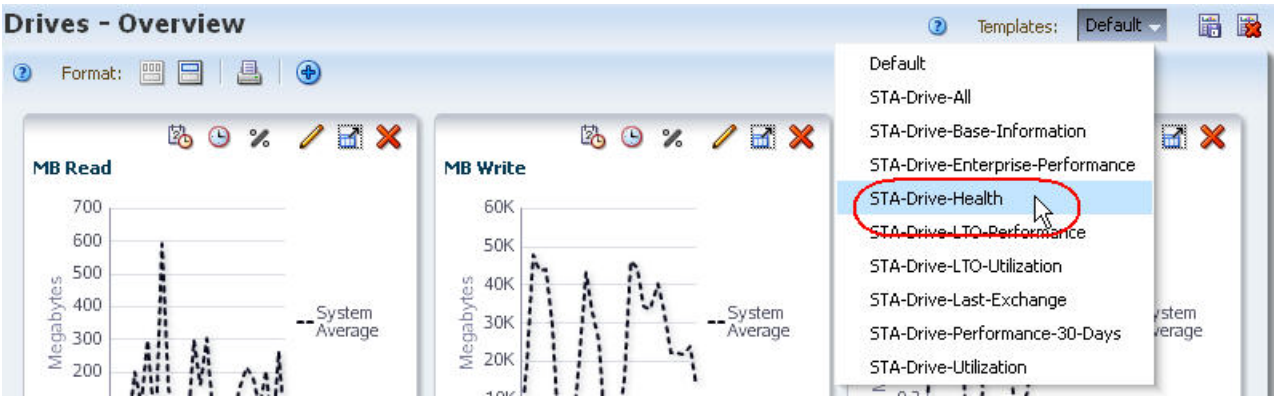
- "Apply a Template" on page 3-8
- *STA Screen Basics Guide*, to sort by a column
- *STA Screen Basics Guide*, to apply library resources to graphs
- "Use the Filter Data Dialog Box to Change a Table Filter" on page 4-9

Report Drives With the Most Errors

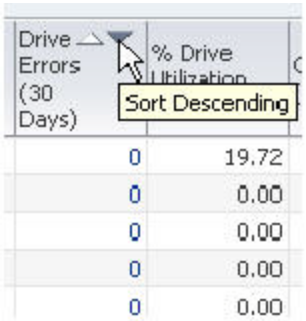
1. In the Navigation Bar, select **Tape System Hardware**, then select **Drives Overview**.



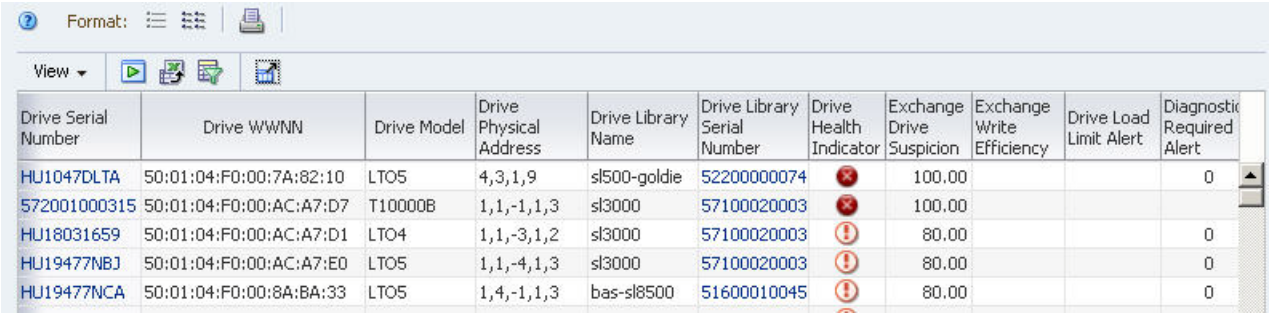
2. In the **Templates** menu, apply the "STA-Drive-Health" template.



3. In the Drive Errors (30 Days) column, click the **Sort Descending** arrow.



The drives with the most errors are brought to the top of the list.

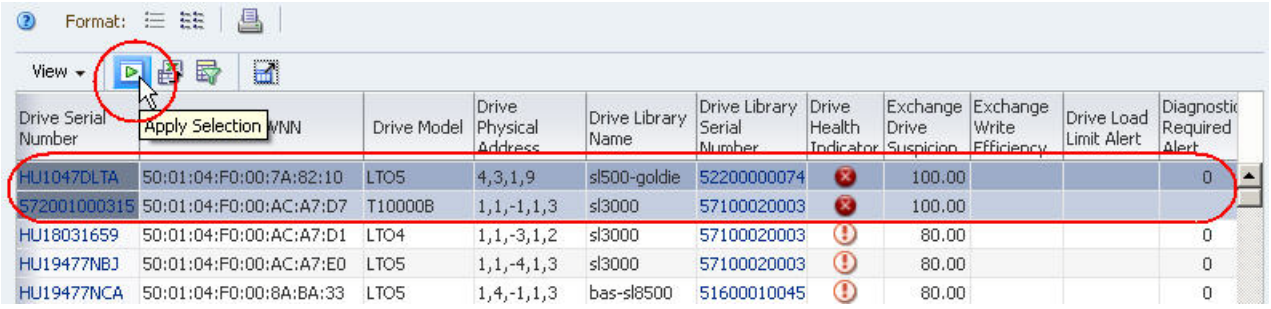


4. Use the following steps to add selected drives to the graphs.

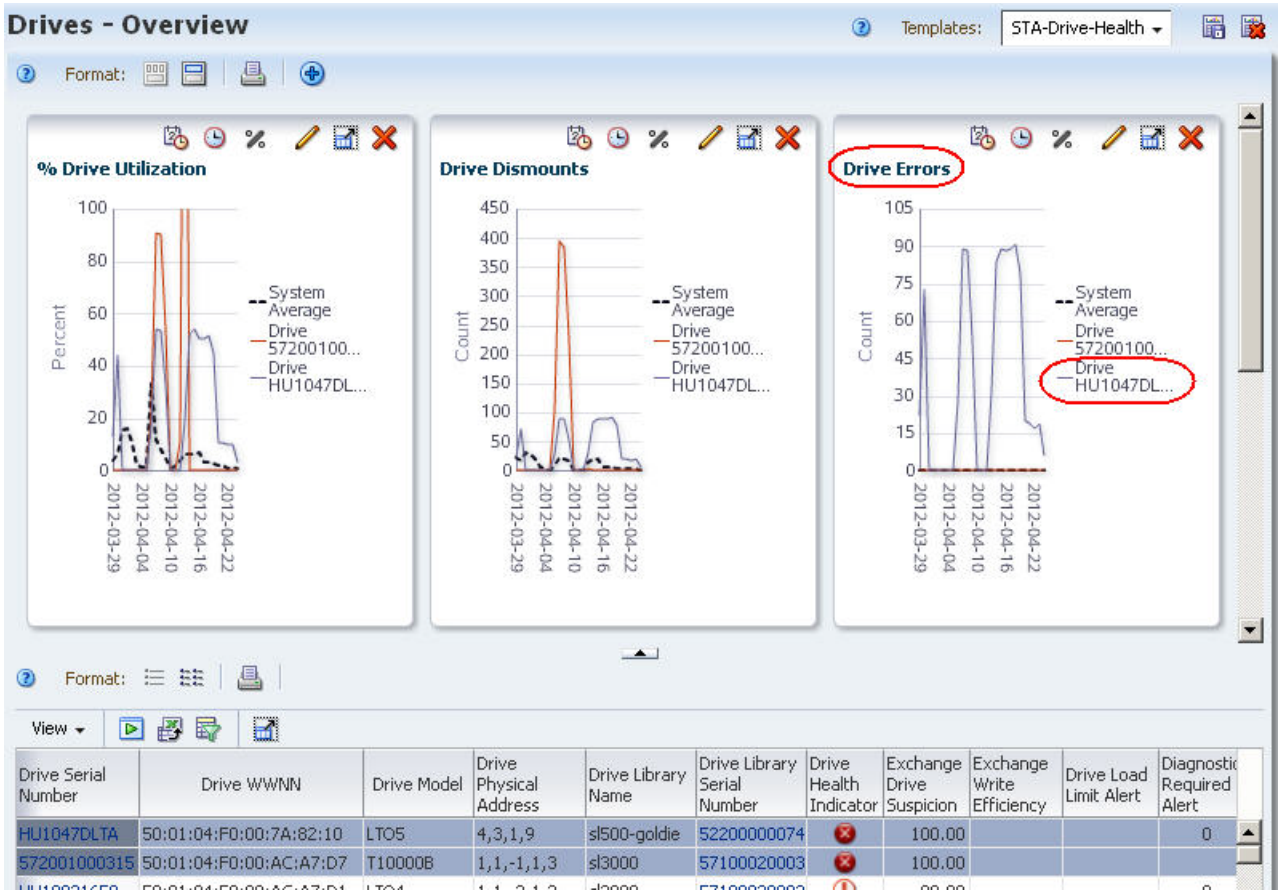
   Adding the drives to the graphs allows you to compare their attribute values against the system average. By default, graphs always include the system average.

   a. In the List View table, select the drives you want to add to the graphs.

   b. Click **Apply Selection** on the Table Toolbar.



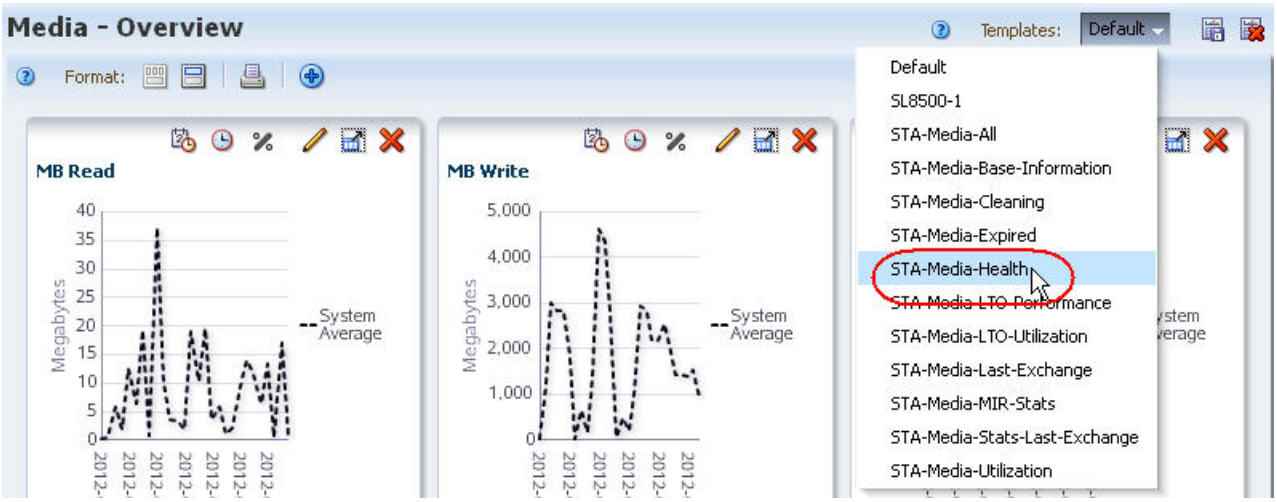
The graphs are updated with the drive data. In the example below, one of the drives shows a high level of errors when compared with the system average.



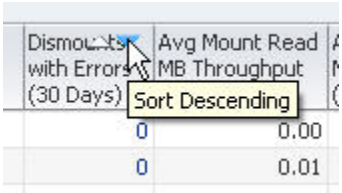
Report Media With the Most Errors

1. In the Navigation Bar, select **Tape System Hardware**, then select **Media Overview**.

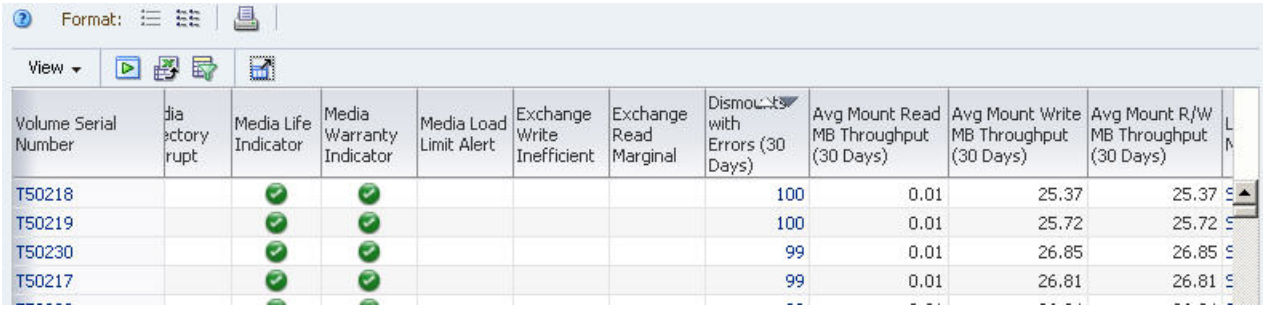
2. In the **Templates** menu, apply the "STA-Media-Health" template.



3. In the Dismounts With Errors (30 Days) column, click the **Sort Descending** arrow.



The media with the most errors are brought to the top of the list.

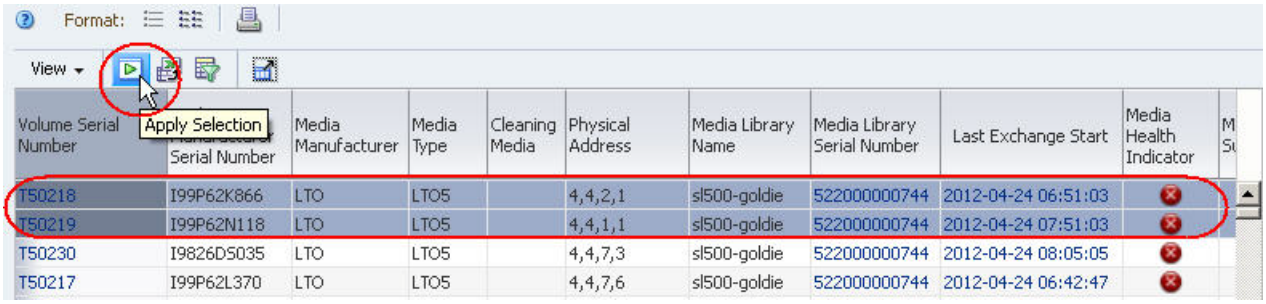


4. Use the following steps to add selected media to the graphs.

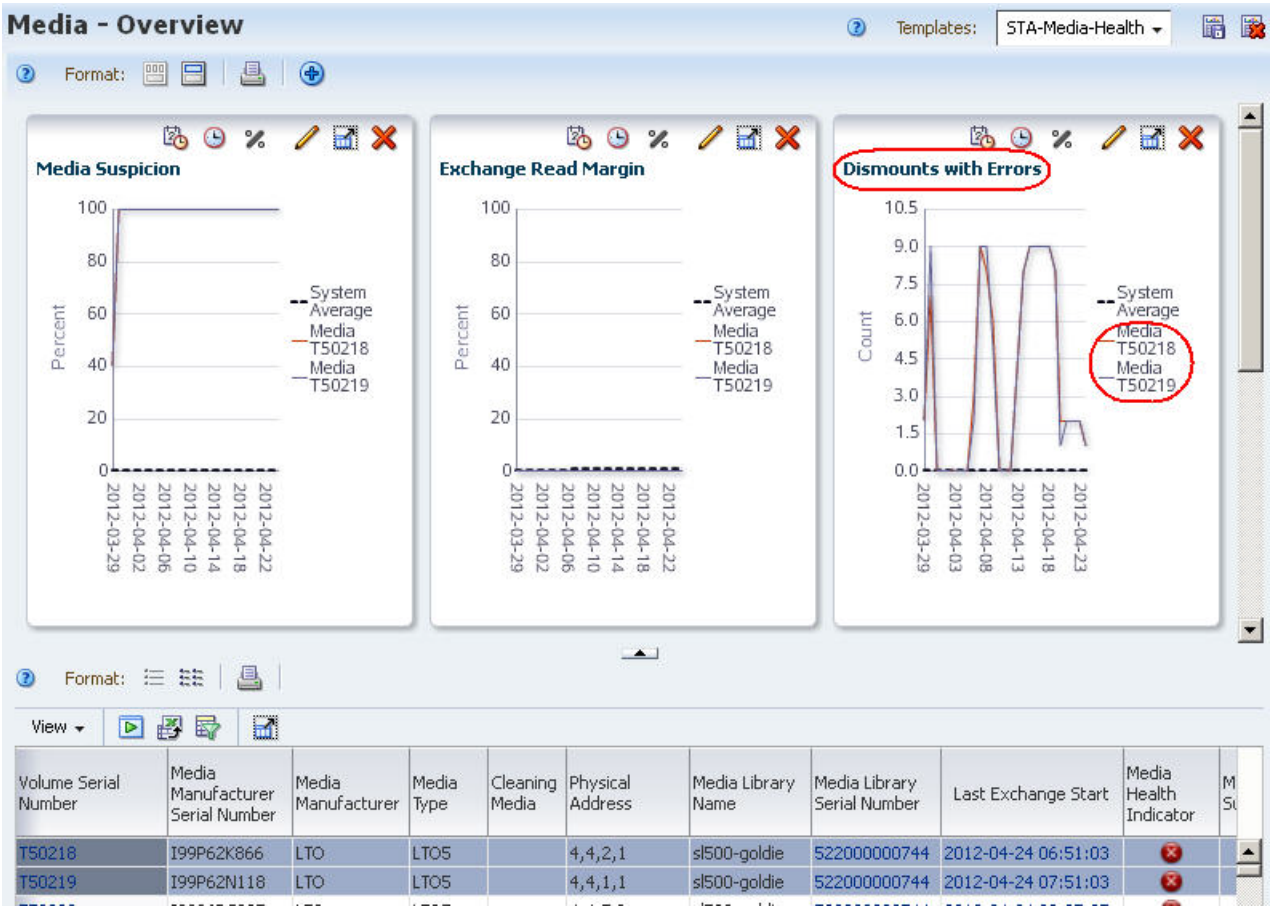
   Adding the media to the graphs allows you to easily compare their attribute values against the system average. By default, graphs always include the system average.

   a. In the List View table, select the media you want to add to the graphs.

   b. Click **Apply Selection** on the Table Toolbar.



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.



Display Correlations Between the Two

This procedure helps you to determine whether there are correlations between the drives and media with most errors. The Exchanges Overview screen is the most useful for this activity because each exchange involves exactly one drive and one piece of media.

1. In the Navigation Bar, select **Tape System Activity**, then select **Exchanges Overview**.

2. Use the following steps to display only those exchanges that took place within the last 30 days and that involve the drive with the most errors.

The drive with the most errors was identified in "Report Drives With the Most Errors" on page 13-2.

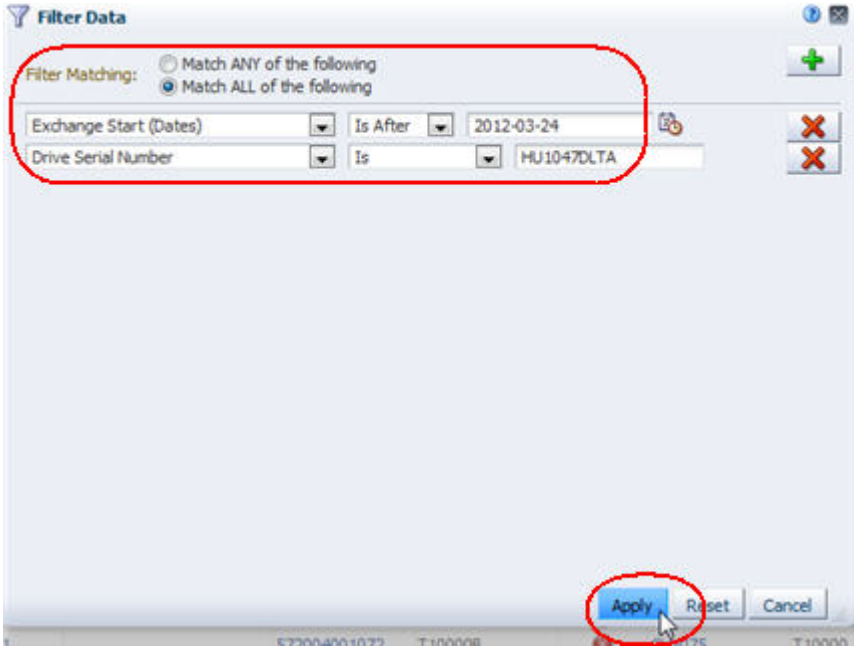
a. Click **Filter Data**.

b. In the **Filter Matching** field, select **Match ALL entered criteria**.

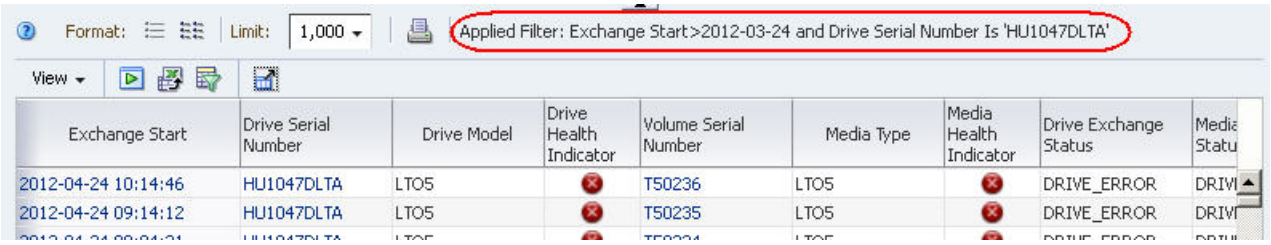
c. Add the following filter criteria:

* **Exchange Start (Dates)** is after a date 30 days ago
* **Drive Serial Number** is the serial number of the drive with the most errors

d. Click **Apply**.

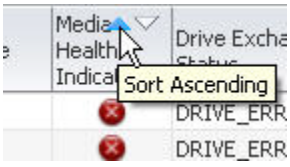


The table is updated according to your selection criteria.



3. To focus on the media involved in the errors, sort the table by a related column.

Suggested columns are Media Exchange Status, Exchange FSC, or Media Health Indicator.



4. Visually scan the Volume Serial Number field to see if there are any correlations between drive errors and specific media.

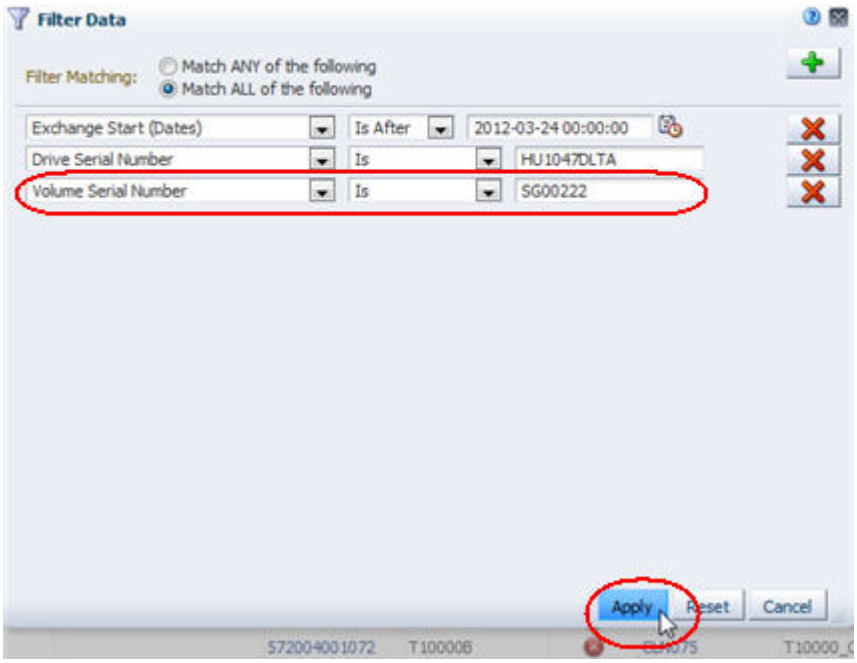
5. If you do find a potential correlation, use the following steps to filter the data further to display just the exchanges that involve both the faulty drive and the suspect media.

   a. Click **Filter Data**.

      The selection criteria already in effect are displayed in the Filter Data dialog box.

   b. Leave the current criteria rows as is, and add the following row:

      * **Volume Serial Number** is the volser of the suspect media identified in Step 4.



   c. Click **Apply**.

      The table is updated according to your selection criteria.

Report Trends in Drive Error Rates

This procedure addresses the questions, "Which drives have had the most errors this week? Have their error rates gone up?"

Although STA screens show 30 days worth of data by default, you can use filter and selection criteria to narrow down to just the current week. The following methods are described:

- "Using the Drives – Overview Screen", below
- "Using the Exchanges Overview Screen" on page 13-11
- "Using the Drives – Messages Screen" on page 13-13

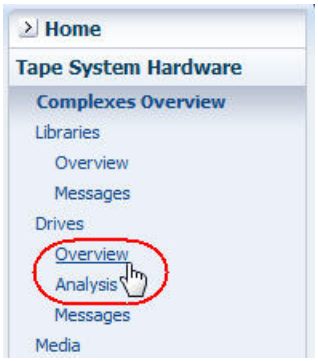
Referenced Tasks

- "Apply a Template" on page 3-8
- *STA Screen Basics Guide*, to sort by a column
- *STA Screen Basics Guide*, to apply library resources to graphs

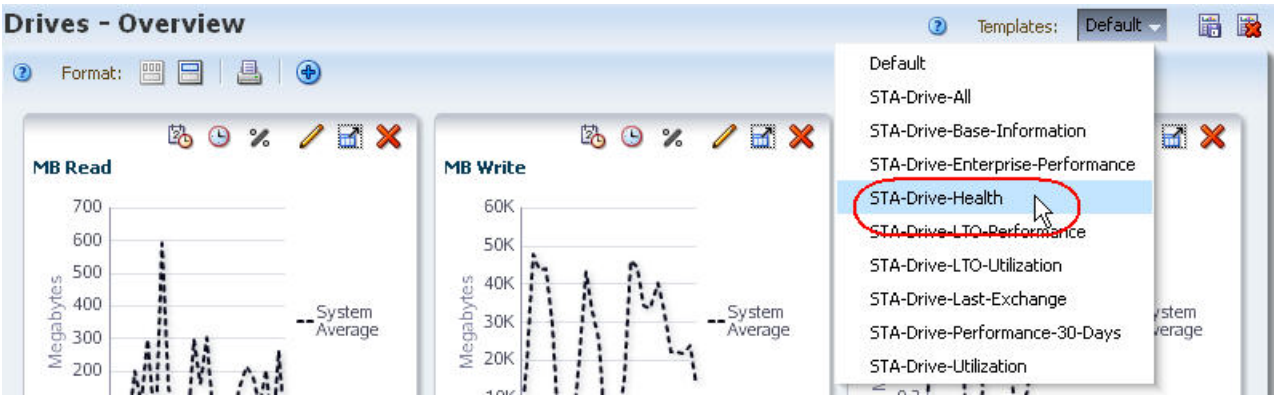
- *STA Screen Basics Guide*, to change a date range
- *STA Screen Basics Guide*, to move a column
- *STA Screen Basics Guide*, to hide and reveal columns
- "Use the Filter Data Dialog Box to Change a Table Filter" on page 4-9

Using the Drives – Overview Screen

1. In the Navigation Bar, select **Tape System Hardware**, then select **Drives Overview**.

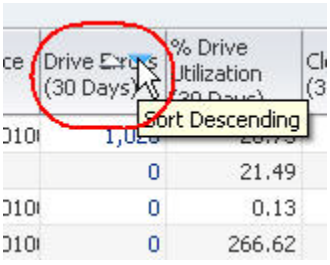


2. In the **Templates** menu, apply the "STA-Drive-Health" template.



running 30-day sum of drive errors is shown in the table and one of the graph panes.

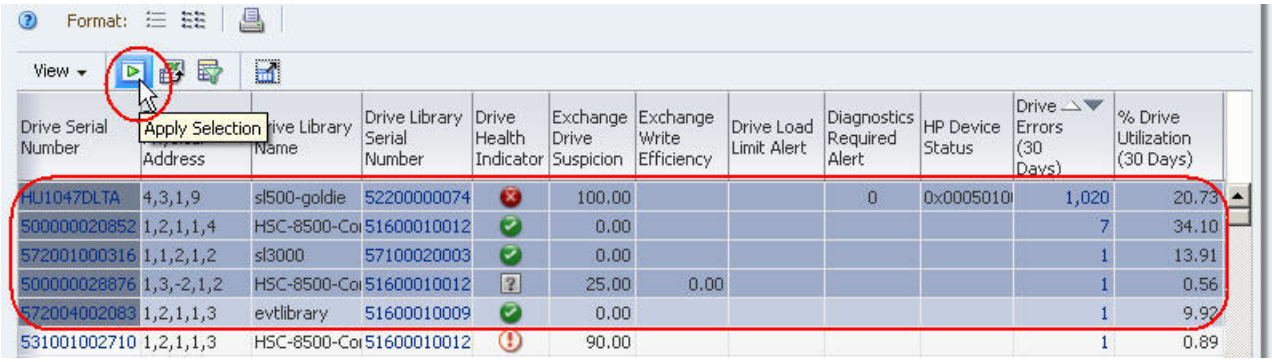
3. In the Drive Errors (30 Days) column, click the **Sort Descending** arrow.



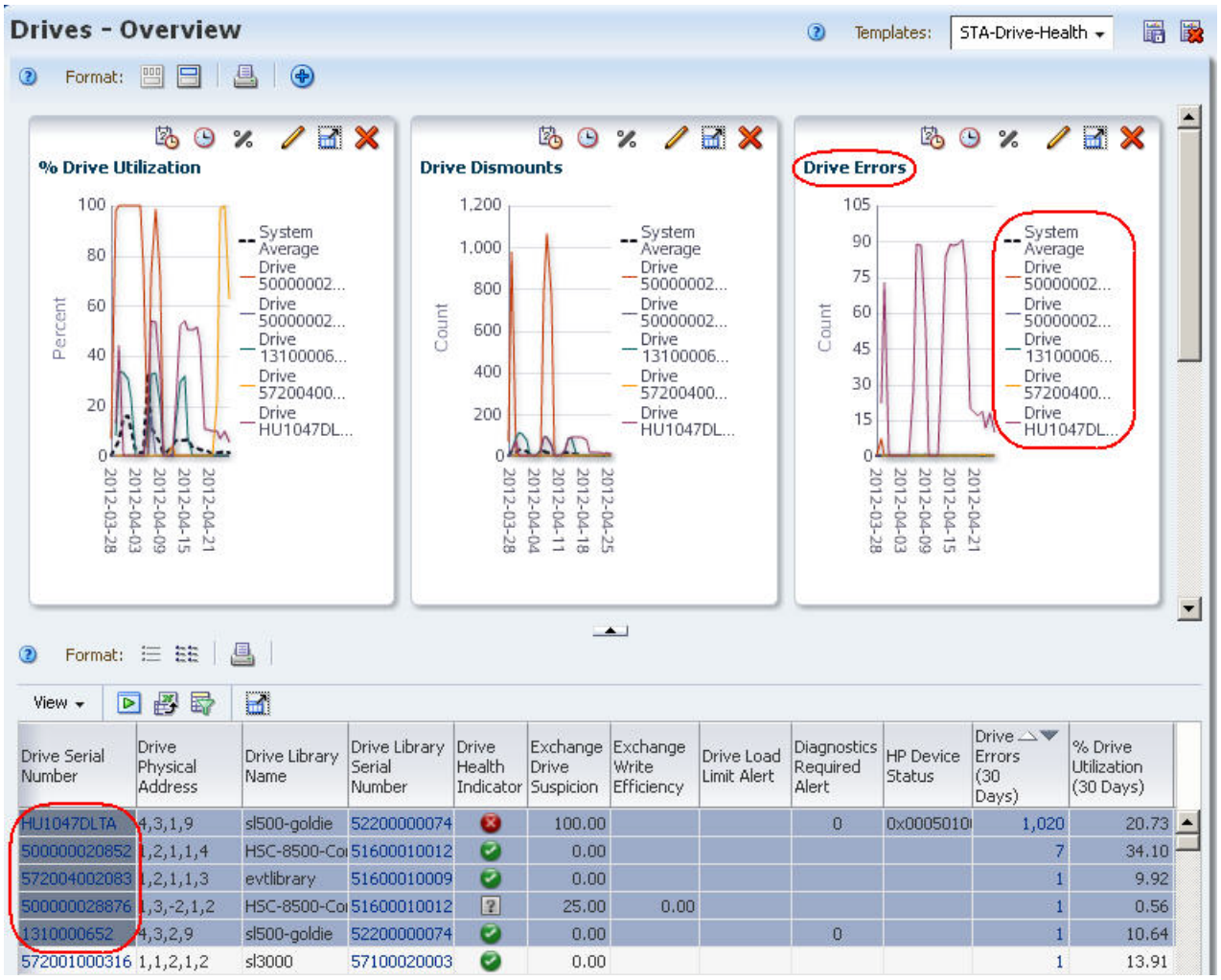
The drives with the most errors are brought to the top of the list.

4. Use the following steps to add the top five drives to the screen graphs.
   a. In the List View table, select the top five drives.

b. Click **Apply Selection** on the List View Toolbar.

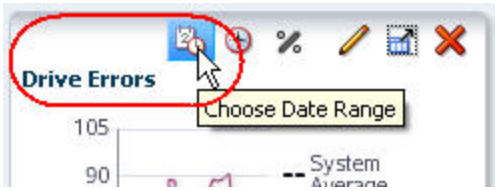


All graphs, including Drive Errors, are updated to show these drives over a 30-day period.



5. Use the following steps to narrow down the date range on the Drive Errors graph pane.

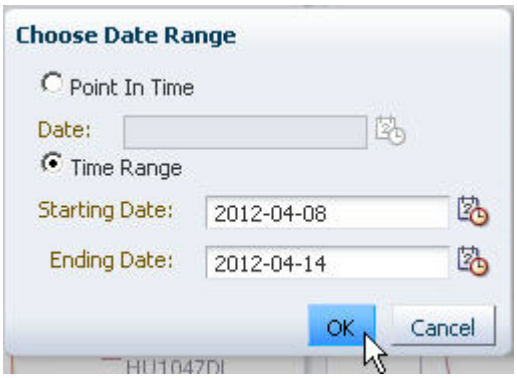
a. Click **Choose Date Range** on the Drive Errors Graph Pane Toolbar.



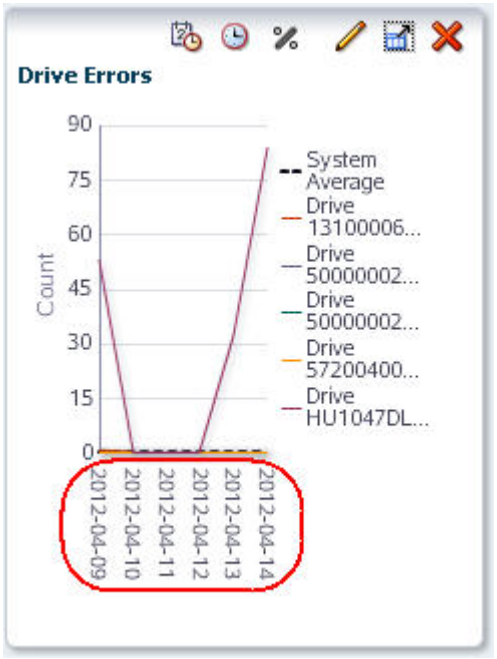
b. Complete the Choose Date Range dialog box as follows:

* 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 is updated according to your selection criteria. The variations in the graph lines show increases and decreases in error rates during the week.

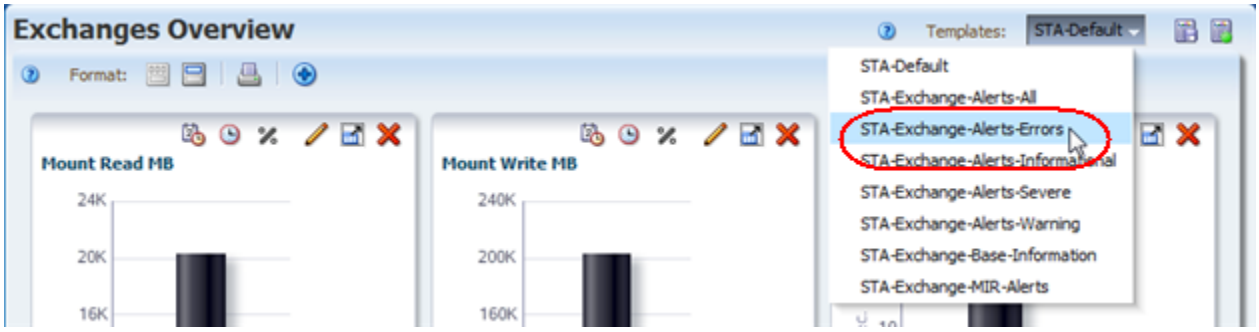


Using the Exchanges Overview Screen

1. In the Navigation Bar, select **Tape System Activity**, then select **Exchanges Overview**.

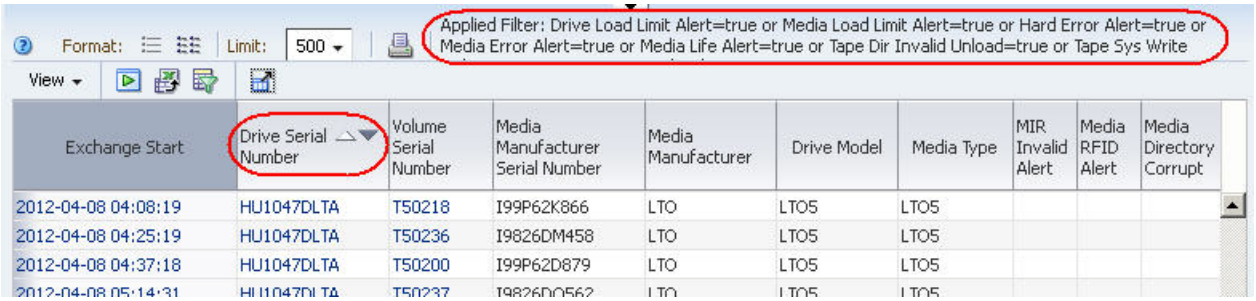
2. In the **Templates** menu, apply the "STA-Exchange-Alerts-Errors" template.

   This template applies a filter to show only exchanges with errors.

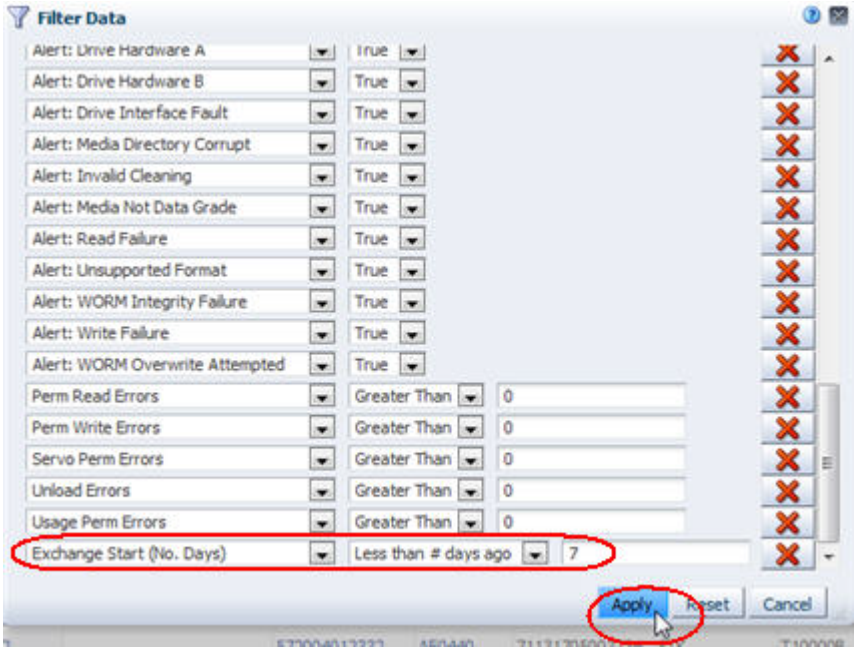


3. In the Drive Serial Number column, click the **Sort Ascending** or **Sort Descending** arrow.

   Errors are grouped by drive, allowing you to bring focus to faulty drives.



4. To focus on specific errors, use the following tasks to move columns around and remove empty columns, as applicable.
   - *STA Screen Basics Guide*, to move a column
   - *STA Screen Basics Guide*, to hide and reveal columns
5. Use the following steps 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 following selection criteria:
      * **Exchange Start (No. Days)** is less than 7 days ago
   d. Click **Apply**.



The table is updated according to your selection criteria.

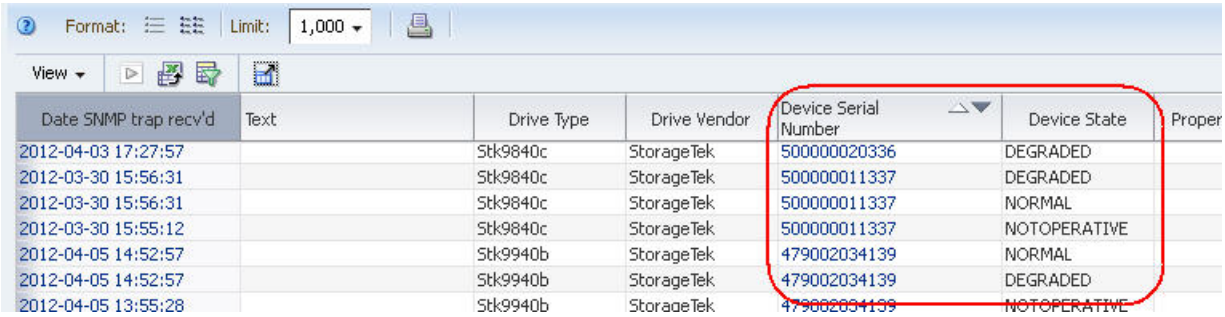
Using the Drives – Messages Screen

Since most messages do not contain a specific drive reference, the information from this method is not as comprehensive as from the others. However, this method does provide a quick snapshot of drives whose health state has changed.

1. In the Navigation Bar, select **Tape System Hardware**, then 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.



3. Visually scan the list for changes in the device state of individual drives.

Report Drive Efficiency Trends

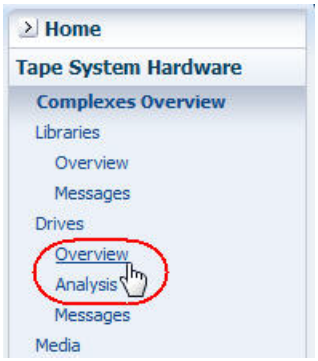
This procedure addresses the question, "Which drives have had significantly declining efficiency over time?"

STA records and displays many measures of data transfer rate efficiency, including read, write, and read/write combined rates. STA collects the rates per exchange and then summarizes them into daily and 30-day time periods. In addition, some drive types also provide their own efficiency calculations. Following are some efficiency attributes reported by STA.

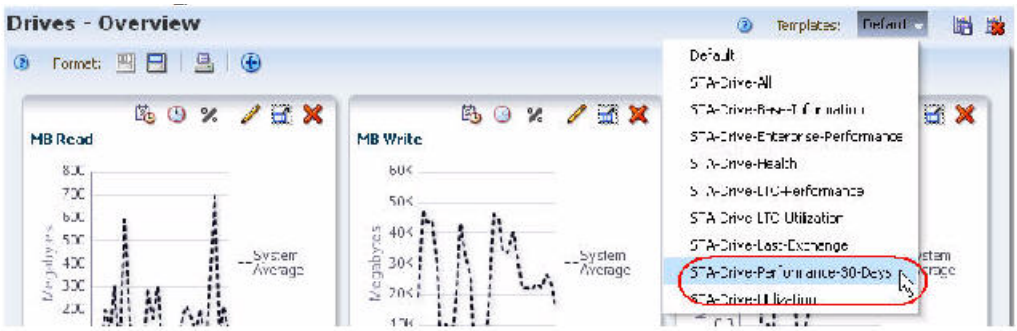
Referenced Tasks

- "Apply a Template" on page 3-8
- *STA Screen Basics Guide*, to add a graph pane
- *STA Screen Basics Guide*, to change the graphed attribute
- *STA Screen Basics Guide*, to apply library resources to graphs

1. In the Navigation Bar, select **Tape System Hardware**, then select **Drives Overview**.

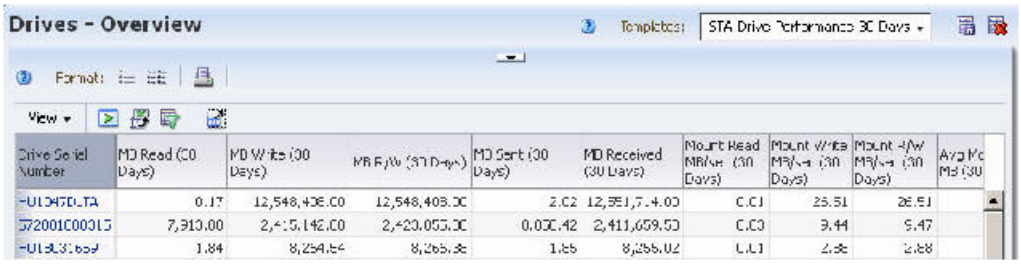


2. In the **Templates** menu, apply the "STA-Drive-Performance-30-Days" template.



This template includes attributes related to drive performance. It does not include any graph panes.

Note: Some measures are null or zero if STA has not been monitoring a drive long enough to gather data and calculate accurate numeric values.



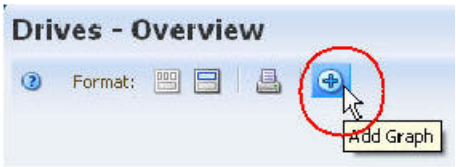
3. Use the following steps to add graphs of interest to the Graph Area.

   By graphing selected attributes, you can see increases or decreases in efficiency over time, and compare individual drive efficiency numbers to the system average.

   a. Click **Restore Pane** at the top of the screen to display the Graphics Area.

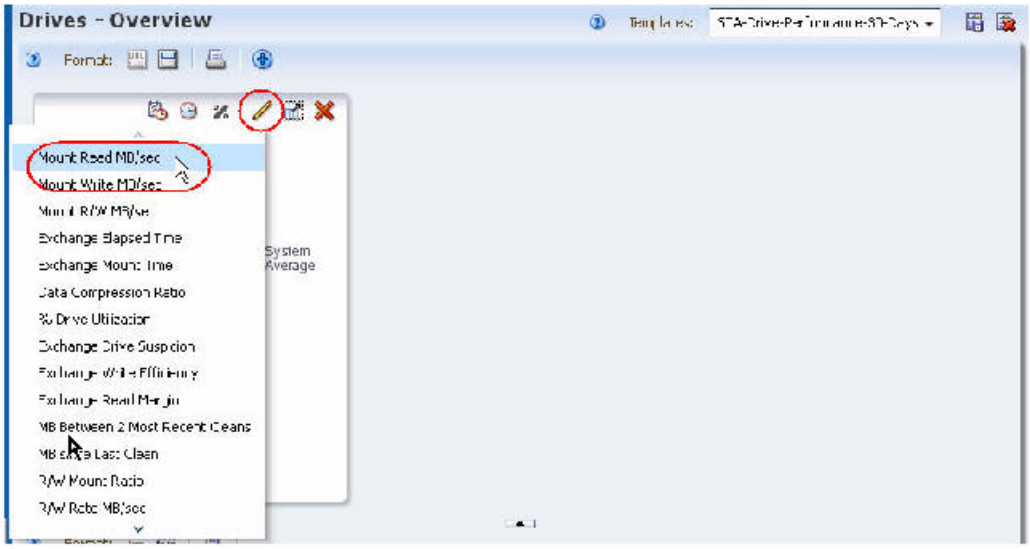
      The Graphics Area is blank.

   b. Click **Add Graph** in the Graphics Area Toolbar.



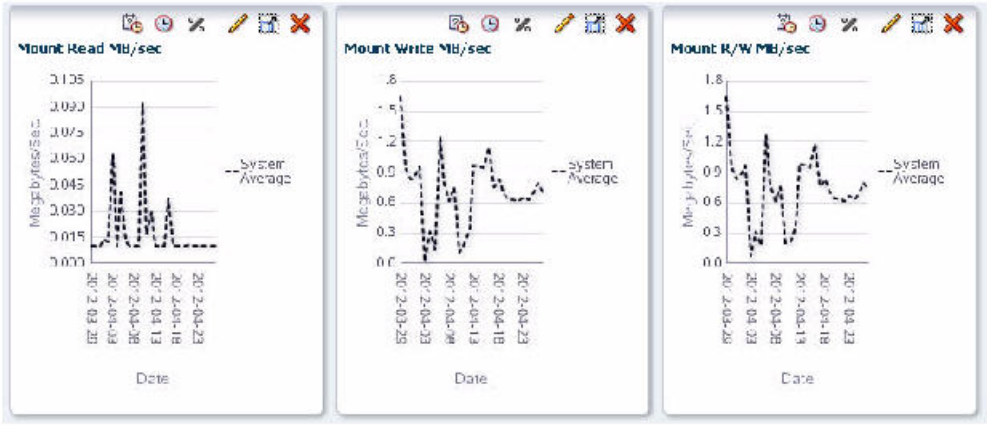
      A new graph pane, with the attribute MB Read, is added to the Graphics Area display.

   c. Click **Change Graphed Attribute** in the Graph Pane Toolbar, and select an attribute of interest.



d. Repeat the previous two steps for any additional attributes you want to graph.

The graphs are updated to display the system average for the attributes you have selected. The examples below show Mount Read MB/sec, Mount Write MB/sec, and Mount R/W MB/sec.

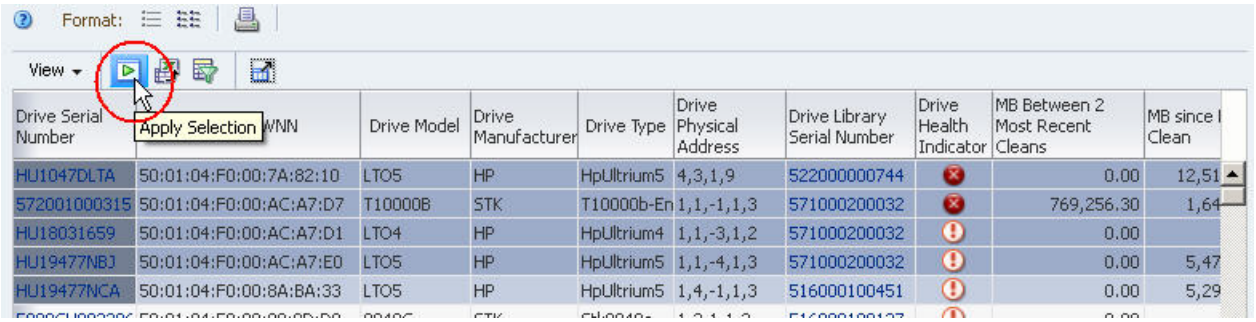


4. Use the following steps to add the top five drives to the graphs.

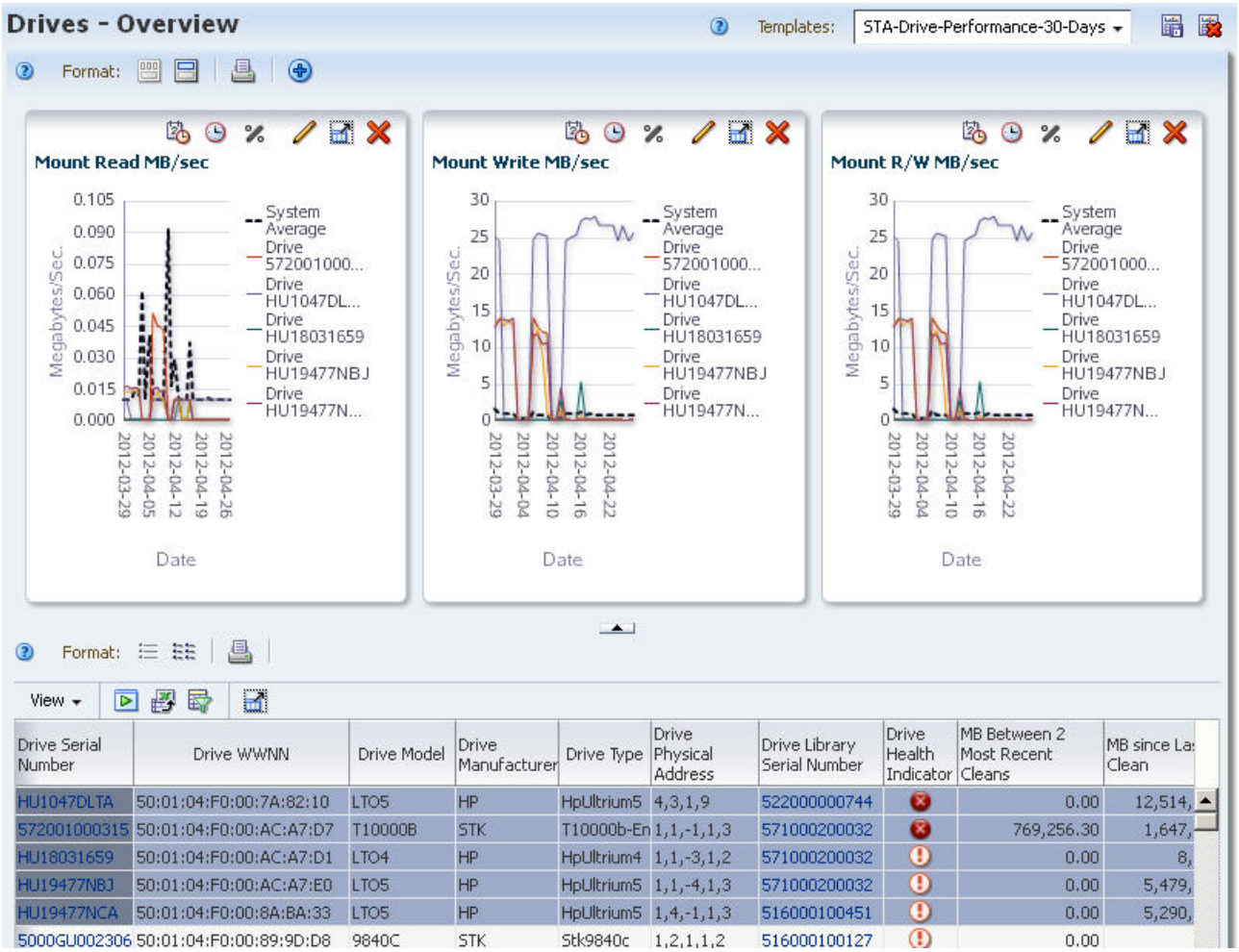
Adding the drives to the graphs allows you to compare their attribute values against the system average. By default, graphs always include the system average.

a. In the List View table, select the top five drives.

b. Click **Apply Selection** on the Table Toolbar.



The drives are added to all the screen graphs.



Report Trends in Drive Failures

This procedure addresses the question, "Is the drive that failed twice today the same one that caused problems two months ago?"

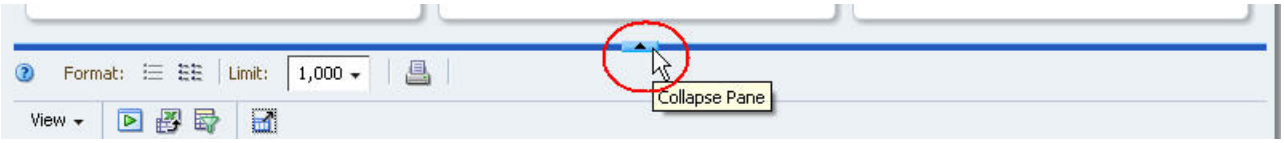
If the drive errors appear in the Messages or Exchanges tables, you can filter the tables by drive ID and then look at current and historical data. The Exchanges table, in particular, allows you to select data for a specific time period.

Referenced Tasks

- *STA Screen Basics Guide*, to collapse and restore the Graphics Area
- "Use the Filter Data Dialog Box to Change a Table Filter" on page 4-9

1. In the Navigation Bar, select **Tape System Activity**, then select **Exchanges Overview**.

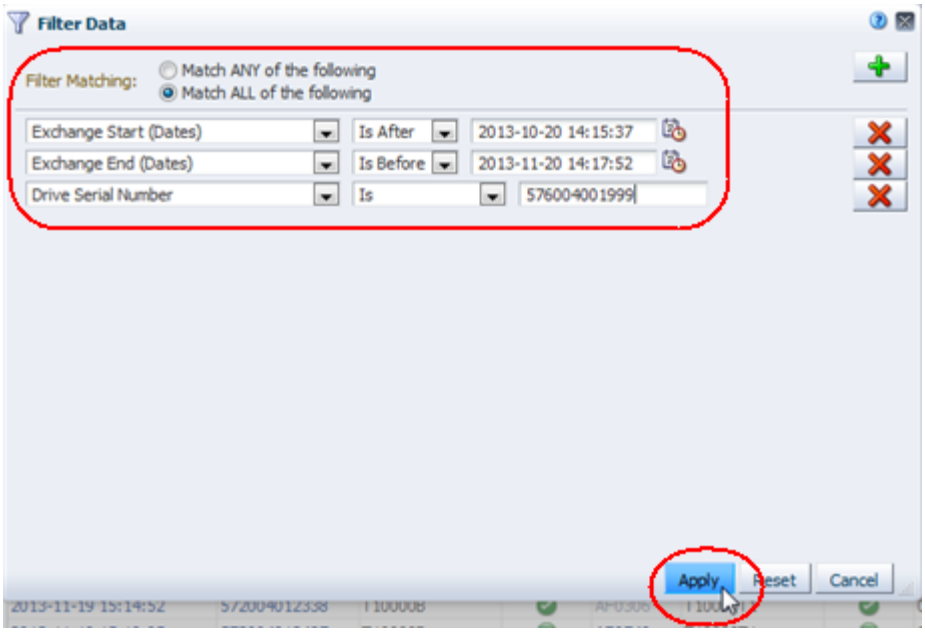
2. To view more of the table data at once, click the **Collapse Pane** icon in the middle of the screen to expand the table vertically.



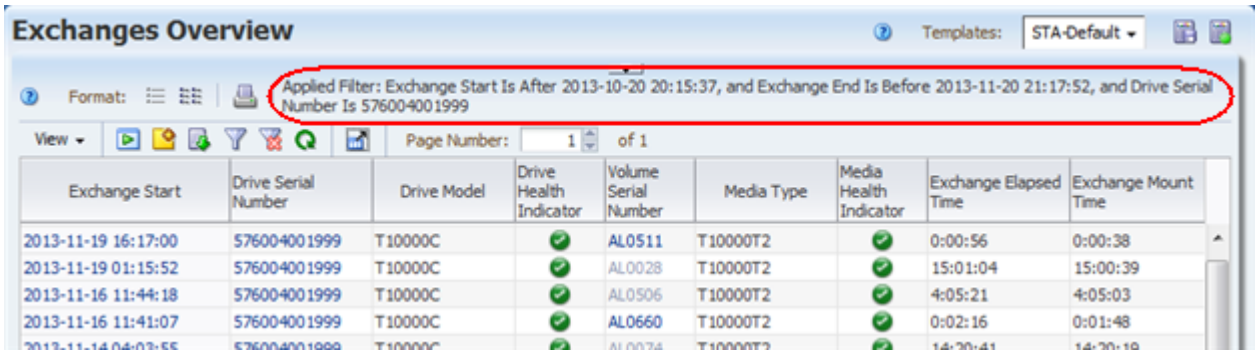
3. Use the following steps to narrow down the data to exchanges that occurred between four and five months ago involving the suspect drive.
   a. Click **Filter Data**.
   b. In the Filter Matching field, select **Match ALL entered criteria**.
   c. Add the following selection criteria:
      * **Exchange 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

      Note: 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**.



The table is updated according to your selection criteria.



4. Visually scan the data to determine whether the drive experienced exchanges with errors during this period.

Report Information to Help Troubleshoot Tape Job Errors

This procedure addresses the questions, "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?"

The following methods are described:

- "Using the Exchanges Overview Screen"
- "Using the All Messages – Overview Screen"

Referenced Tasks

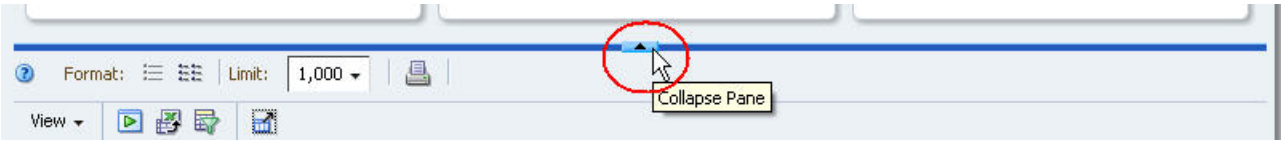
- *STA Screen Basics Guide*, to collapse and restore the Graphics Area
- "Use the Filter Data Dialog Box to Change a Table Filter" on page 4-9
- *STA Screen Basics Guide*, to navigate using links

Using the Exchanges Overview Screen

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 Navigation Bar, select **Tape System Activity**, then select **Exchanges Overview**.

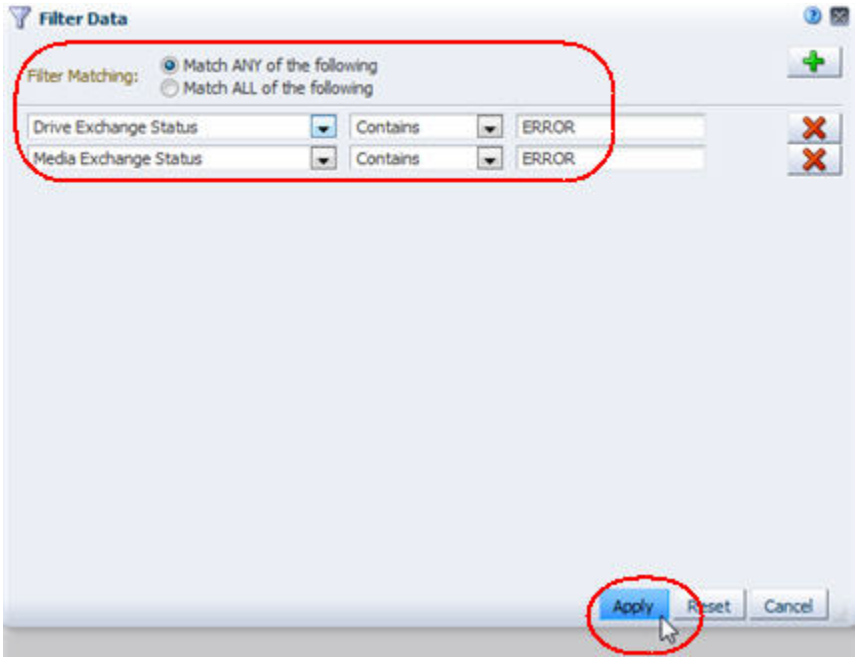
2. So you can view more of the table data at once, click the **Collapse Pane** icon in the middle of the screen to expand the table vertically.



3. Use the following steps 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 the following selection criteria:
      * **Drive Exchange Status** contains "ERROR"
      * **Media Exchange Status** contains "ERROR"

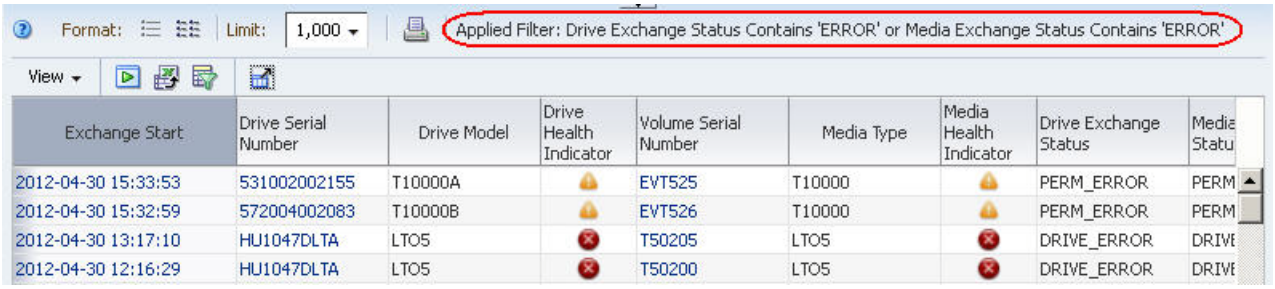
      Note: Entries are not case-sensitive, so "ERROR" will match "error" or "Error".

   d. Click **Apply**.



The table is updated according to your selection criteria.

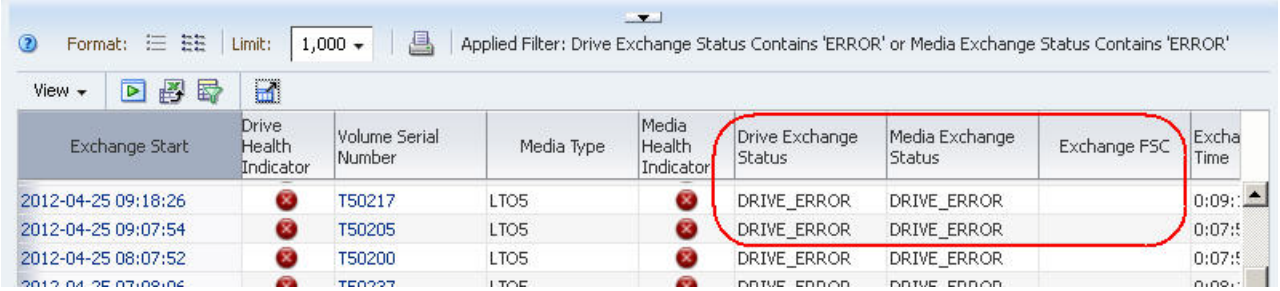
Note: The Drive Health Indicator and Media Health Indicator columns may indicate Use even after an error. This is because the values of these attributes are aggregated over time. The specific values depend on the frequency and severity of errors, and whether there have been subsequent exchanges with no problems. Recent exchanges with no problems move the aggregated value toward a "Use" status.



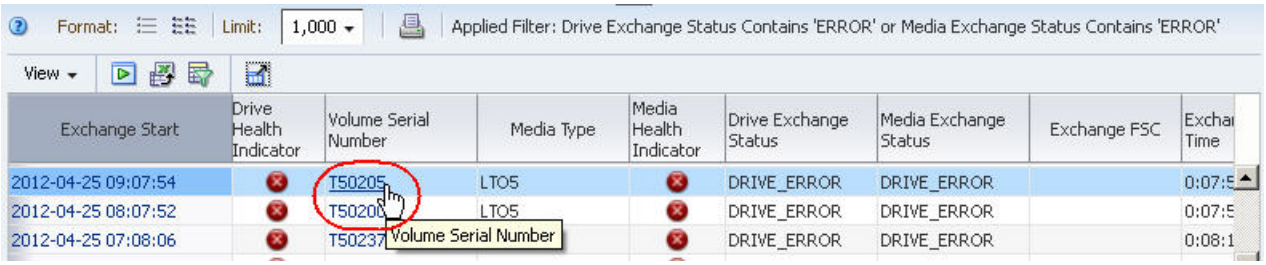
Exchange Start	Drive Serial Number	Drive Model	Drive Health Indicator	Volume Serial Number	Media Type	Media Health Indicator	Drive Exchange Status	Media Statu
2012-04-30 15:33:53	531002002155	T10000A		EVT525	T10000		PERM_ERROR	PERM
2012-04-30 15:32:59	572004002083	T10000B		EVT526	T10000		PERM_ERROR	PERM
2012-04-30 13:17:10	HU1047DLTA	LTO5		T50205	LTO5		DRIVE_ERROR	DRIVE
2012-04-30 12:16:29	HU1047DLTA	LTO5		T50200	LTO5		DRIVE_ERROR	DRIVE

4. Scroll to exchanges that occurred around 9:00 am today, and review the information in the Drive Exchange Status, Media Exchange Status, and Exchange FSC columns for details about the errors.

   By default, the rows of the table are sorted by Exchange Start time.



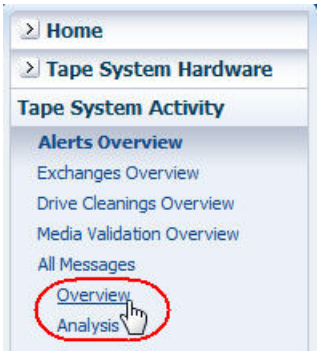
5. Optionally, to display detail about a drive or media involved in an error, select the text link in either the Drive Serial Number or Volume Serial Number column.



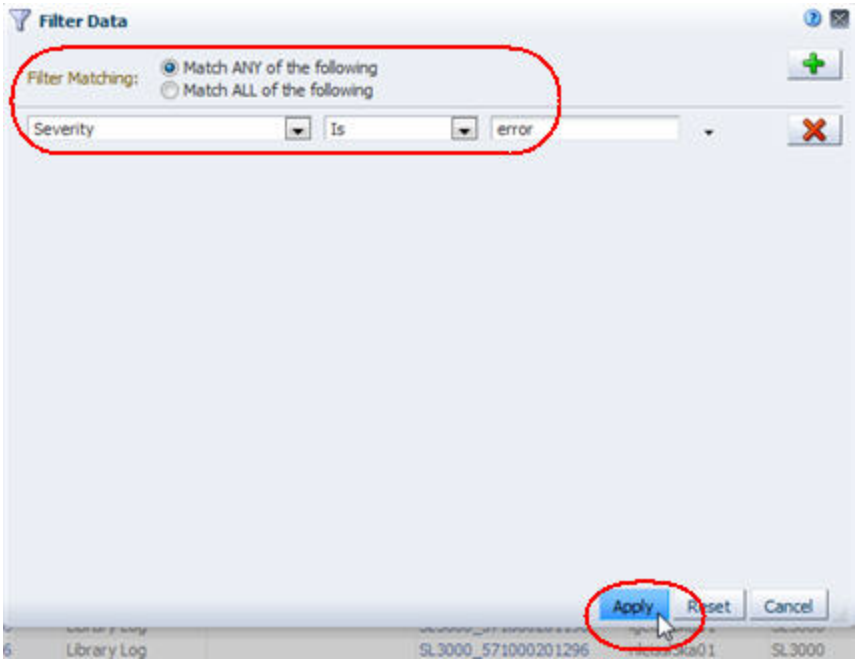
Using the All Messages – Overview Screen

In cases where you know the time of a job failure, you can use this method to check for related STA error messages.

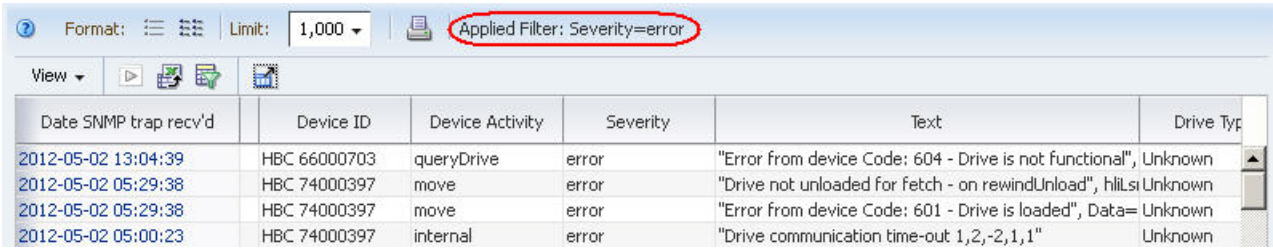
1. In the Navigation Bar, select **Tape System Activity**, then select **All Messages Overview**.



2. Use the following steps to narrow down the data to just traps that involved errors.
   a. Click **Filter Data**.
      * **Severity** is **error**
   b. Click **Apply**.



The table is updated according to your selection criteria.



3. Scroll to traps that were received around 9:00 am today, and review the entries.

   By default, the rows of the table are sorted by Date SNMP trap recv'd time.

Report Trends in Critical Errors

This procedure addresses the questions, "What critical errors were reported to STA last month? Is the total number trending up, down, or staying stable?"

STA reports instances of a wide variety of error types. This procedure provides instructions for exporting the error data to a spreadsheet application, which can then be used to summarize error trends over time.

The following methods are described:

- "Using the All Messages – Overview Screen"
- "Using the Exchanges Overview Screen" on page 13-25

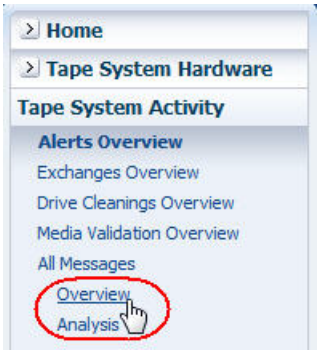
Referenced Tasks

- "Use the Filter Data Dialog Box to Change a Table Filter" on page 4-9
- *STA Screen Basics Guide*, to move a column
- *STA Screen Basics Guide*, for information on tooltips
- *STA Screen Basics Guide*, to change the width of a column

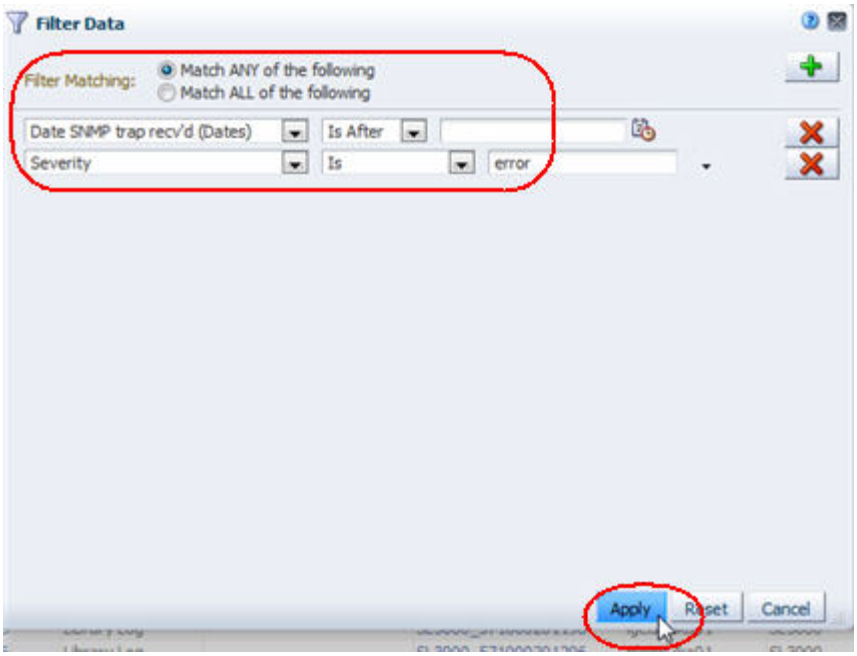
- *STA Screen Basics Guide*, to export table data
- "Apply a Template" on page 3-8
- *STA Screen Basics Guide*, to collapse and restore the Graphics Area
- *STA Screen Basics Guide*, to add a graph pane
- *STA Screen Basics Guide*, to change the graphed attribute

Using the All Messages – Overview Screen

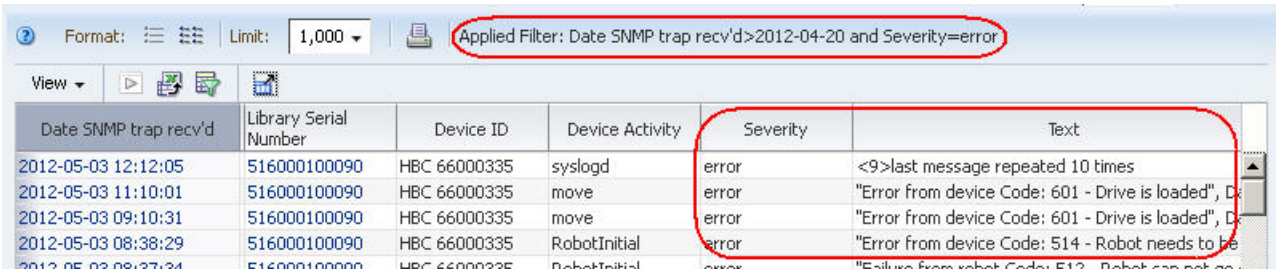
1. In the Navigation Bar, select **Tape System Activity**, then select **All Messages Overview**.



2. Use the following steps to narrow down the data to traps sent within the last month.
   a. Click **Filter Data**.
   b. In the Filter Matching field, select **Match ALL entered criteria**.
   c. Add the following selection criteria:
      * **Date SNMP trap recv'd (Dates)** is after a date one month ago
      * **Severity** is **error**
   d. Click **Apply**.

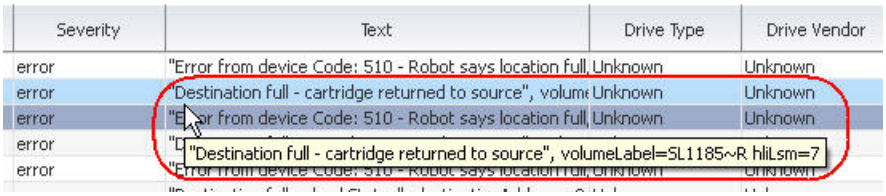


The table is updated according to your selection criteria. The Severity and Text columns are adjacent, allowing you to review them together. You may need to scroll to the right to see the columns.



3. You can use any of the following methods to see the full error message text.

   – Move the mouse over the bottom border of the cell; the full text is displayed in a tooltip.



   – Widen the Text column.

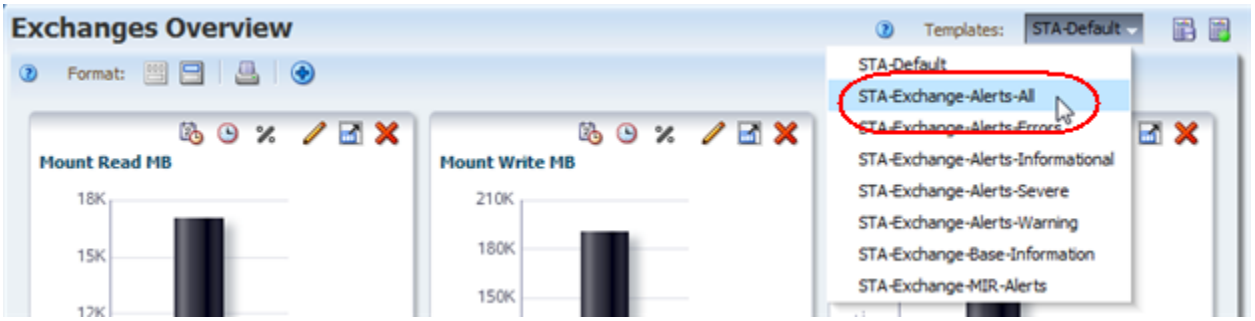
   – Export the table to a file. Then use a compatible spreadsheet application to open the file and format the error message text so it wraps within the table column.

Using the Exchanges Overview Screen

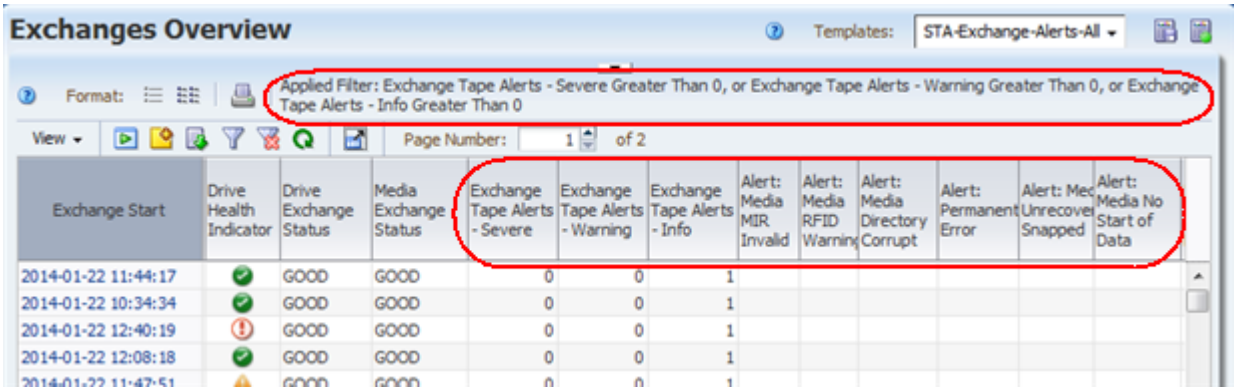
Drive and media errors are reported as a result of exchanges. Therefore, it is more efficient to look for errors on the Exchanges Overview screen, where drive and media data is consolidated, rather than on the Drives or Media screens.

1. In the Navigation Bar, select **Tape System Activity**, then select **Exchanges Overview**.

2. In the **Templates** menu, apply the "STA-Exchanges-Alerts-All" template (alternatively, apply the "STA-Exchanges-Alerts-Errors" template for a smaller subset).



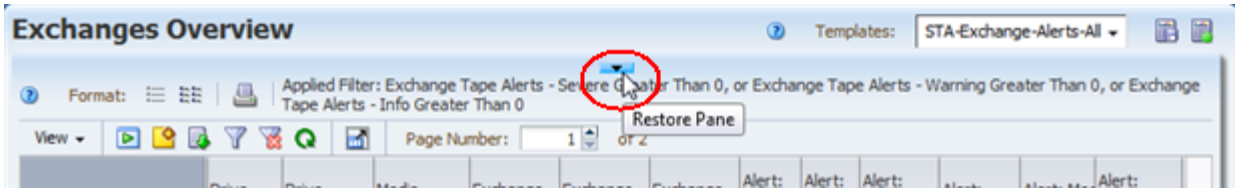
This template includes several columns that indicate different types of errors. The exchanges are sorted in reverse chronological order, — most recent exchanges first — allowing you to see at a glance which error types have predominated at your site over the last month.



3. If there are enough errors to indicate possible trends, use the following steps to add graphs of interest to the Graph Area.

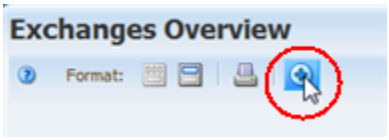
   Attributes that may correlate to errors include Write Efficiency, Read Margin, and R/W Rate MB/sec.

   a. Click the **Restore Pane** icon at the top of the screen to display the Graphics Area.



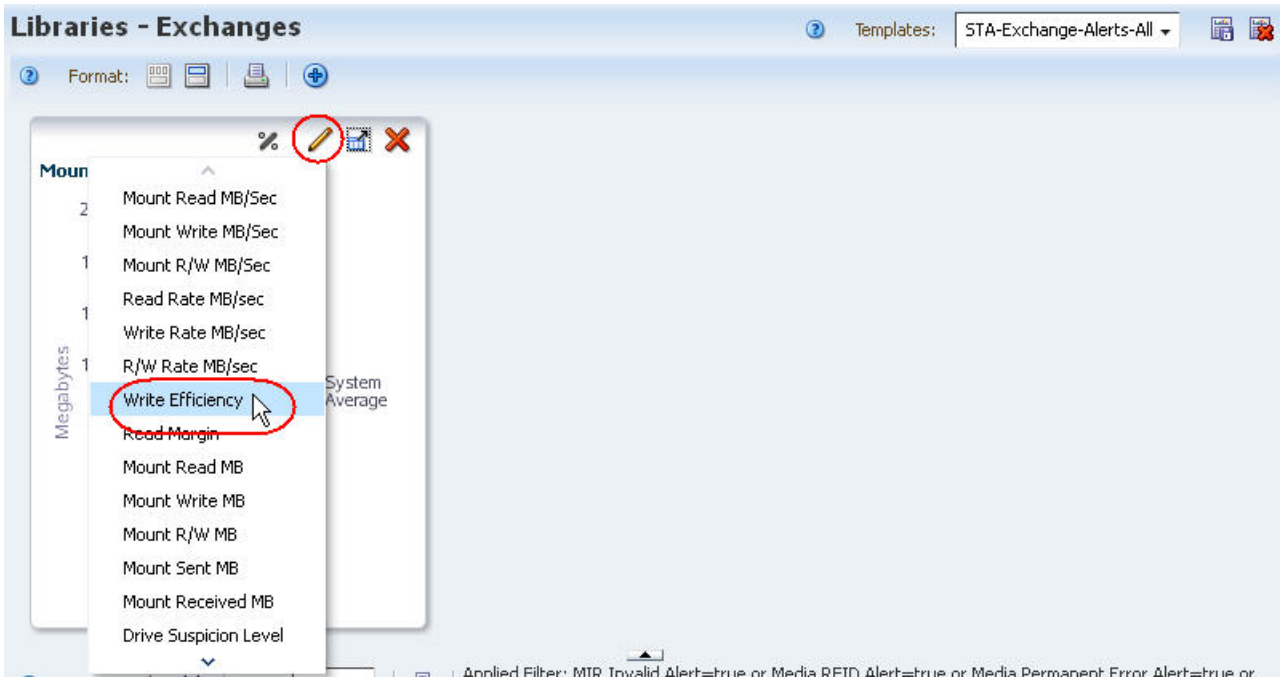
The Graphics Area is blank.

b. Click the **Add Graph** icon in the Graphics Area Toolbar.



A new graph pane, with the attribute Mount Read MB, is added to the Graphics Area display.

c. Click the **Change Graphed Attribute** icon in the Graph Pane Toolbar, and select an attribute you want to graph.

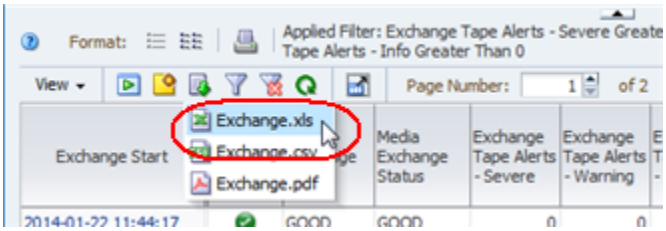


d. Repeat the previous two steps for any additional attributes you want to graph.

The graphs are updated to display the system average for the attributes you have selected. The samples below show Write Efficiency, Read Margin, and R/W Rate MB/sec.

4. To calculate total errors by error type, you must use an external spreadsheet application. Use the following steps to export the data displayed in the table to an HTML-based Excel-compatible file.

   a. Click the **Export** icon in the Table Toolbar and select **Exchange.xls**.



   b. Save the file to a location on your local computer.

   c. Use a compatible spreadsheet application to open the file and summarize the data.

Capacity and Resource Management Questions

Question	Task
How many libraries, drives, or media are in my tape system environment?	"Report Total Libraries, Drives, or Media" on page 13-29
How many drives or media of a particular type are in my tape system environment?	"Report Drive and Media Types" on page 13-31
Which are the top three drives in terms of utilization?	"Report Drives With the Highest Utilization" on page 13-33
Which types of media are in short supply? Do I have an oversupply of any type?	"Report Shortages or Surpluses of Media" on page 13-36
Am I likely to need more media, drives, or storage cells next year? If so, how many?	"Project Future Media, Drive, or Storage Cell Requirements" on page 13-40
Which types of drives or media are used the most in my tape system?	"Report Resources With the Highest Utilization" on page 13-46
Which library in my tape environment is the busiest? Which is the least busy?	"Report Library Relative Activity Levels" on page 13-51

Question	Task
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?	"Report Media Approaching Capacity" on page 13-54
Have all my drives been upgraded to the latest firmware?	"Report Drive Firmware Levels" on page 13-56

Report Total Libraries, Drives, or Media

These procedures address the question, "How many libraries, drives, or media are in my tape system environment?"

The following methods are described:

- "Using the Dashboard"
- "Using Overview Screens" on page 13-30
- "Using Analysis Screens" on page 13-30

Related Topics

- *STA Screen Basics Guide*, for information on tooltips
- "Clear the Current Filter" on page 4-12

Using the Dashboard

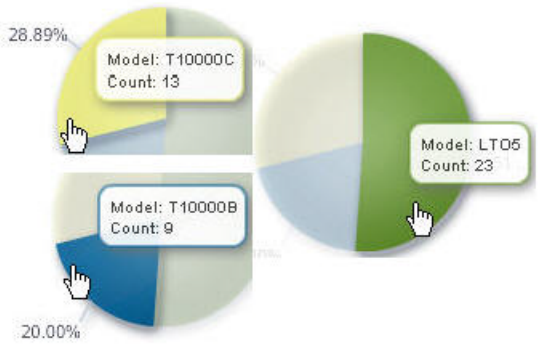
1. In the Navigation Bar, select **Home**, then select **Dashboard**.

2. If the number of resources (libraries, drives, or media) is small, you can do a quick visual count just by reading the graph.

   In the sample below, you can estimate from the graph that there are ten libraries total: (8 +2).

3. If the number of resources is high, you can move the mouse over each slice in the pie chart to display tooltips of descriptive information, including totals.

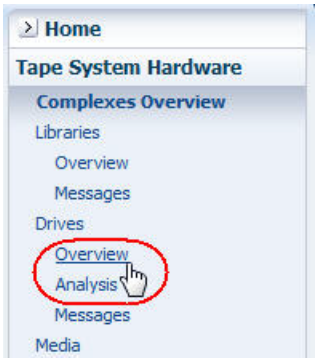
   In the sample below, the pie chart tooltips yield the count: 13 + 9 +23 =45 total.



Using Overview Screens

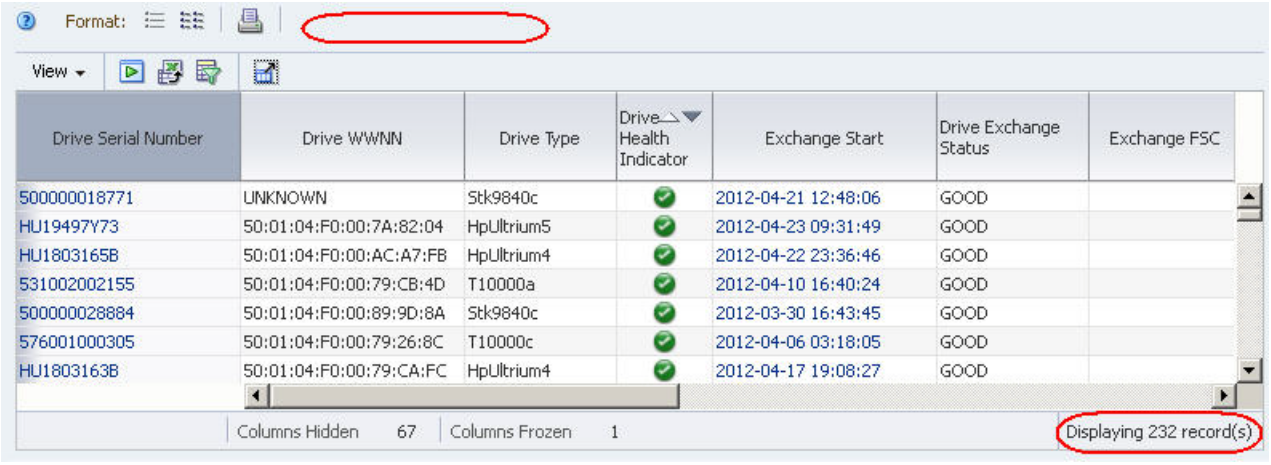
In Overview screens, the total number of records displayed is listed at the lower-right corner of the List View table. As long as there are no filters applied, this number is the total of that type of resource (libraries, drives, or media) monitored by STA.

1. In the Navigation Bar, select an Overview screen.



2. Check the Applied Filter area of the table, and verify that there is no filter in effect. If one has been applied, see "Clear the Current Filter" on page 4-12 for instructions on clearing it.

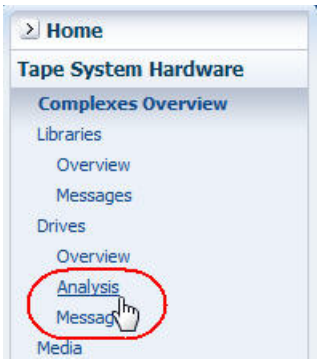
   In the sample below, no filter has been applied, and the Drives – Overview screen indicates there are 232 total drives monitored by STA.



Using Analysis Screens

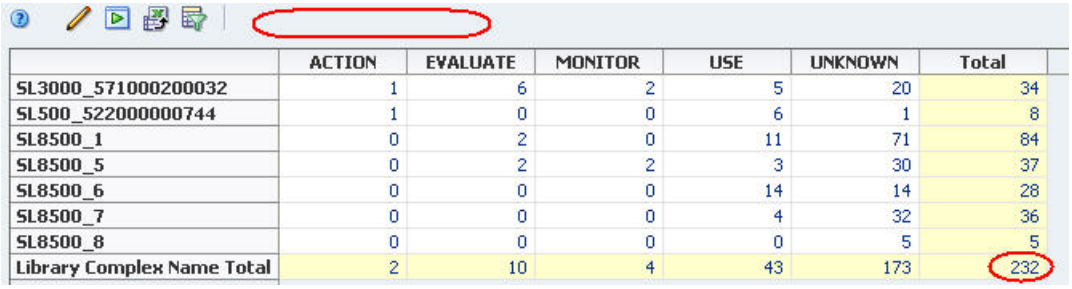
Analysis screens aggregate data according to a variety of criteria.

1. In the Navigation Bar, select an Analysis screen.



2. Check the Applied Filter area of the table, and verify that there is no filter in effect. If one has been applied, see "Clear the Current Filter" on page 4-12 for instructions on clearing it.

   In the sample Drives – Analysis screen below, no filter has been applied, and the pivot table breaks down the 232 total drives by library complex and state.



	ACTION	EVALUATE	MONITOR	USE	UNKNOWN	Total
SL3000_571000200032	1	6	2	5	20	34
SL500_522000000744	1	0	0	6	1	8
SL8500_1	0	2	0	11	71	84
SL8500_5	0	2	2	3	30	37
SL8500_6	0	0	0	14	14	28
SL8500_7	0	0	0	4	32	36
SL8500_8	0	0	0	0	5	5
Library Complex Name Total	2	10	4	43	173	232

Report Drive and Media Types

These procedures address the question, "How many drives or media of a particular type are in my tape system environment?"

The following methods are described:

- "Using the Dashboard"
- "Using Analysis Screens" on page 13-32

Referenced Tasks

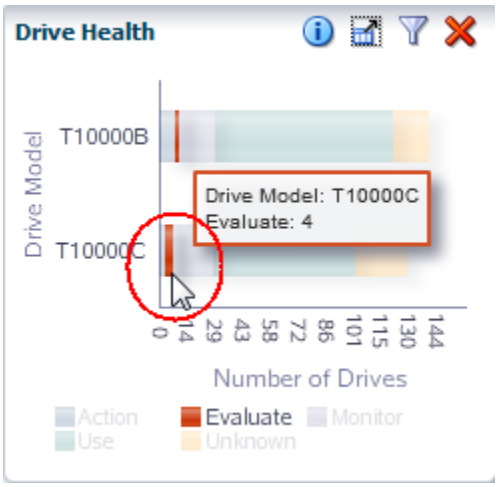
- *STA Screen Basics Guide*, for information on tooltips
- *STA Screen Basics Guide*, to navigate using links

Using the Dashboard

1. In the Navigation Bar, select **Dashboard**.

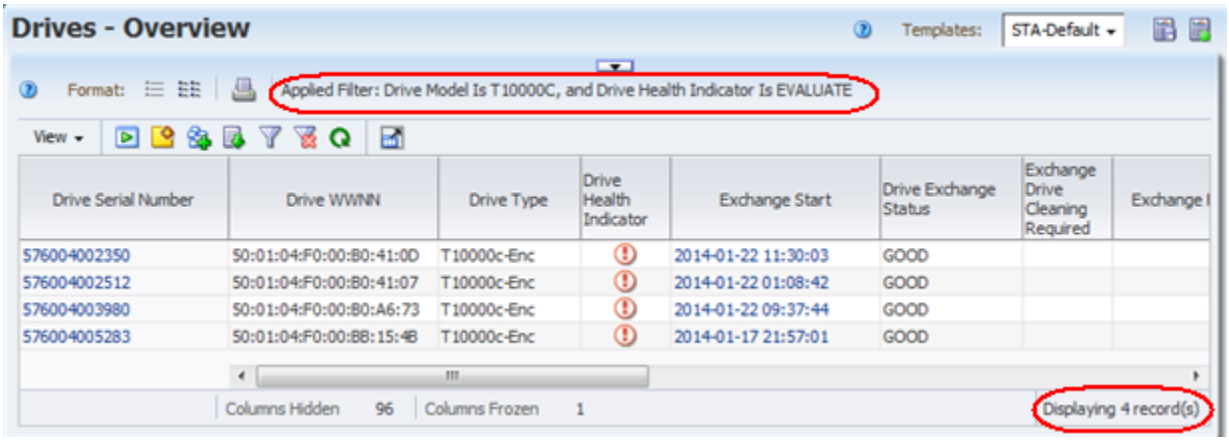
2. Move the mouse over the relevant section of a pie or bar chart to display a tooltip with descriptive information and totals.

   In the following sample, moving the mouse over the T10000C bar reveals there are four T10000C drives with an "Evaluate" health.



3. If you select a section of a bar or pie chart, you are taken to the associated Overview screen, filtered for that type of drive or media.

   In the sample below, the Drives – Overview screen is displayed, filtered to display only T10000C drives with an "Evaluate" health.



Using Analysis Screens

This method is especially useful if you want data aggregated by a series of criteria, such as by library and media state. The pivot table on Analysis screens presents this information in a concise format.

1. In the Navigation Bar, select an Analysis screen (Drives – Analysis or Media – Analysis).

In the sample Media – Analysis screen below, subtotals and totals are provided at the bottom of each column and to the right of each row.

		ACTION	EVALUATE	MONITOR	USE	UNKNOWN	Total
SL3000_571000200032	1	7	0	0	125	459	591
	Library Number Total	7	0	0	125	459	591
SL500_522000000744	1	0	0	0	16	5	21
	2	0	0	0	8	3	11
	3	0	0	0	6	12	18
	4	10	0	0	8	1	19
	Library Number Total	10	0	0	38	21	69
SL8500_1	1	0	0	1	6	941	948
	2	0	0	0	19	534	553
	Library Number Total	0	0	1	25	1475	1501
SL8500_5	1	1	0	0	44	413	458
	Library Number Total	1	0	0	44	413	458
SL8500_6	1	0	0	0	86	204	290
	Library Number Total	0	0	0	86	204	290
SL8500_7	1	0	0	1	5	314	320
	Library Number Total	0	0	1	5	314	320
SL8500_8	1	0	0	0	0	434	434
	Library Number Total	0	0	0	0	434	434
Library Complex Name Total		18	0	2	323	3320	3663

Report Drives With the Highest Utilization

These procedures address the question, "Which are the top three drives in terms of utilization?"

Utilization can be defined in several ways, including lifetime hours in use, amount of data passed, and total number of mounts. The following methods are described:

- "Using Total Time in Motion"
- "Using Time in Use Over the Last 30 Days" on page 13-35

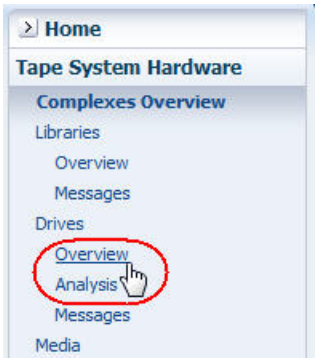
Referenced Tasks

- "Apply a Template" on page 3-8
- *STA Screen Basics Guide*, to sort by a column

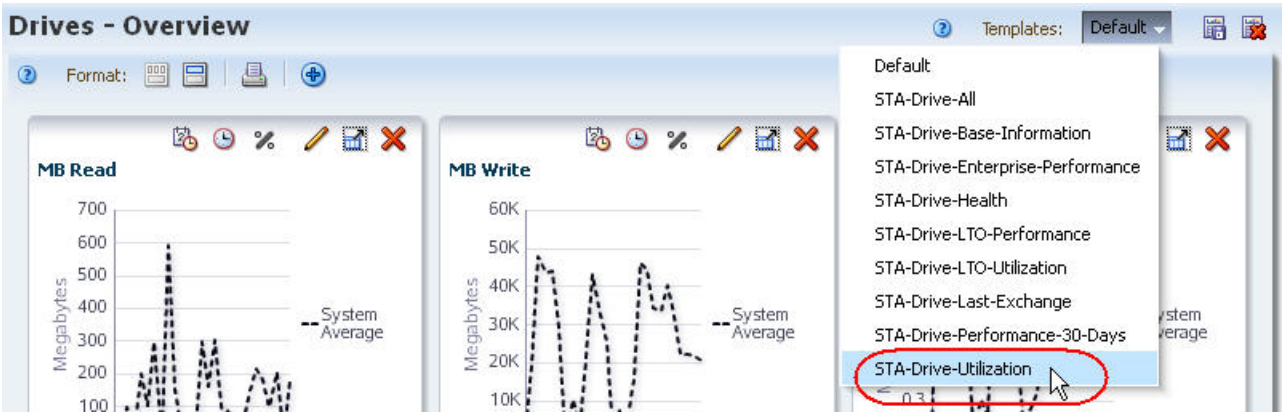
Using Total Time in Motion

Note: This information is provided only by StorageTek enterprise drives.

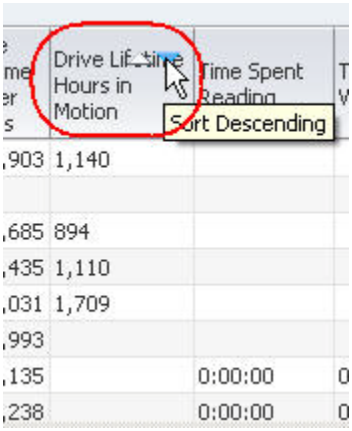
1. In the Navigation Bar, select **Tape System Hardware**, then select **Drives Overview**.



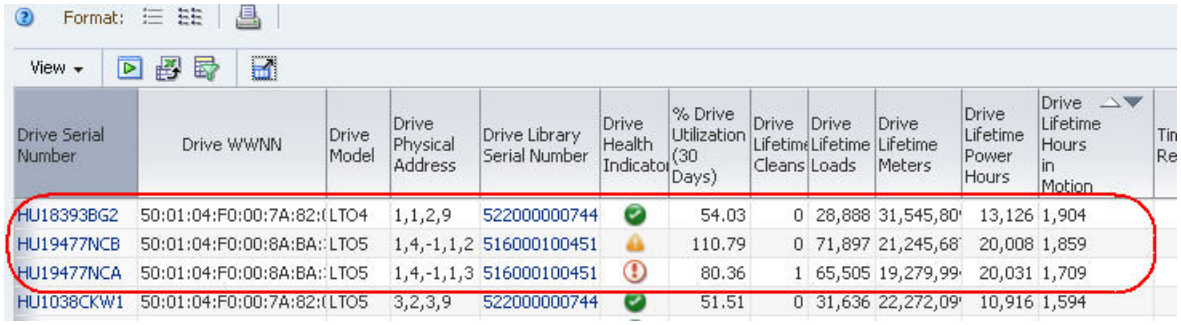
2. In the **Templates** menu, apply the "STA-Drive-Utilization" template.



3. In the Drive Lifetime Hours in Motion column, click the **Sort Descending** arrow.

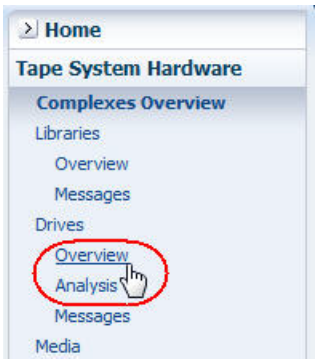


The top three drives in terms of time in motion are displayed at the top of the list.

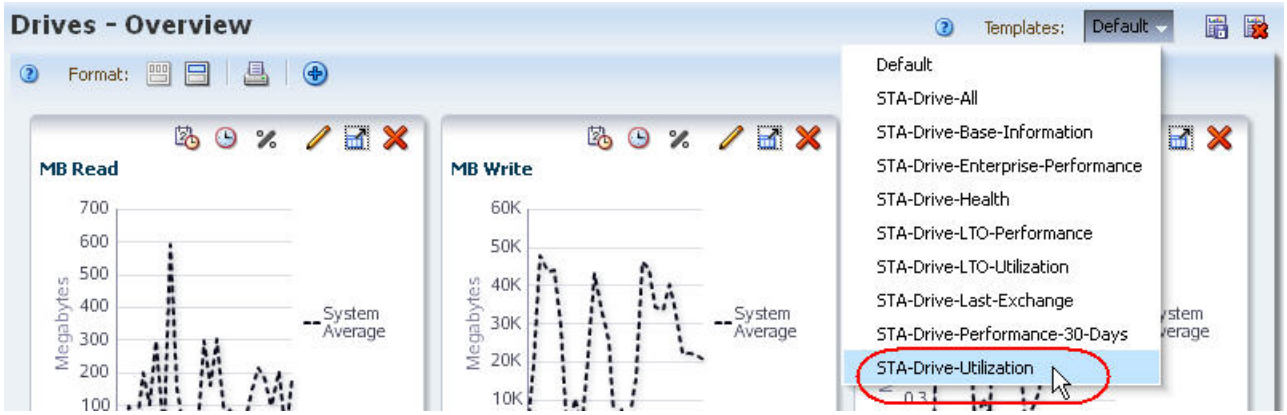


Using Time in Use Over the Last 30 Days

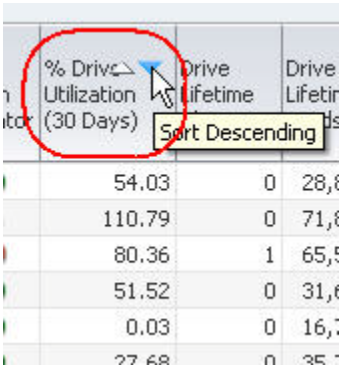
1. In the Navigation Bar, select **Tape System Hardware**, then select **Drives Overview**.



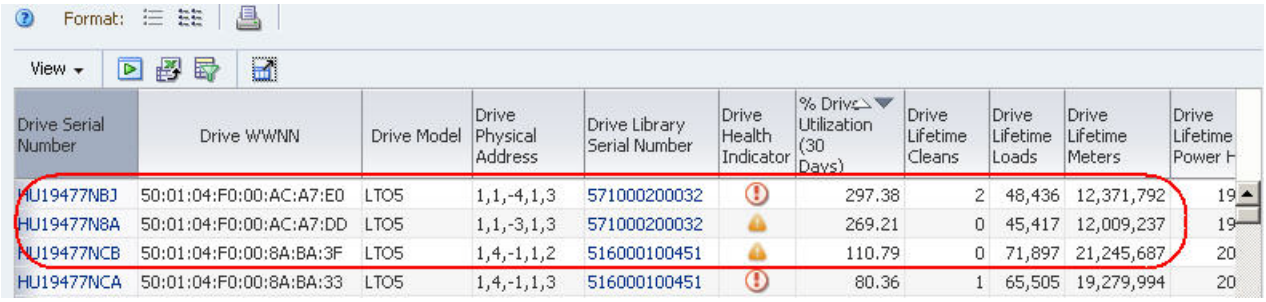
2. In the **Templates** menu, apply the "STA-Drive-Utilization" template.



3. In the % Drive Utilization (30 Days) column, click the **Sort Descending** arrow.



The top three drives in terms of percentage time in use are displayed at the top of the list.



Report Shortages or Surpluses of Media

This procedure addresses 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.

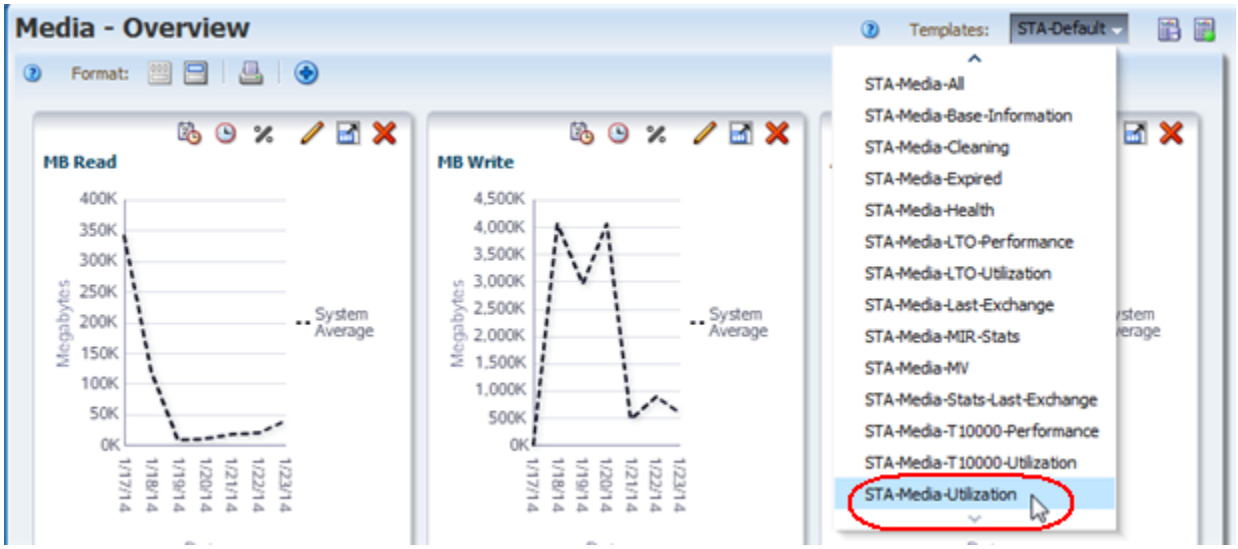
Referenced Tasks

- "Apply a Template" on page 3-8
- "Use the Filter Data Dialog Box to Change a Table Filter" on page 4-9
- *STA Screen Basics Guide*, to sort by multiple columns
- *STA Screen Basics Guide*, to move a column
- *STA Screen Basics Guide*, to export table data

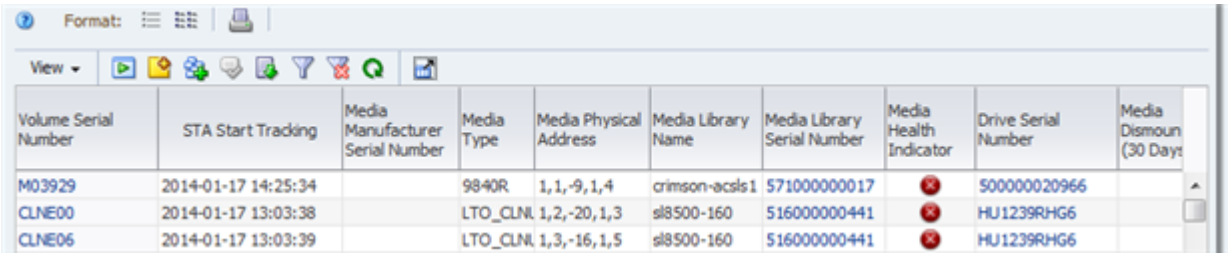
1. In the Navigation Bar, select **Tape System Hardware**, then select **Media Overview**.

2. In the **Templates** menu, select the "STA-Media-Utilization" template.

> **Note:** Depending on the number of templates available to your STA username, you may need to scroll down in the menu to see the selection.



This template includes all the attributes related to utilization, such as Media Dismounts (30 Days), MB Read (30 Days), and Media Life Indicator.



3. Use the following steps to eliminate any media for which capacity or availability information is not available.

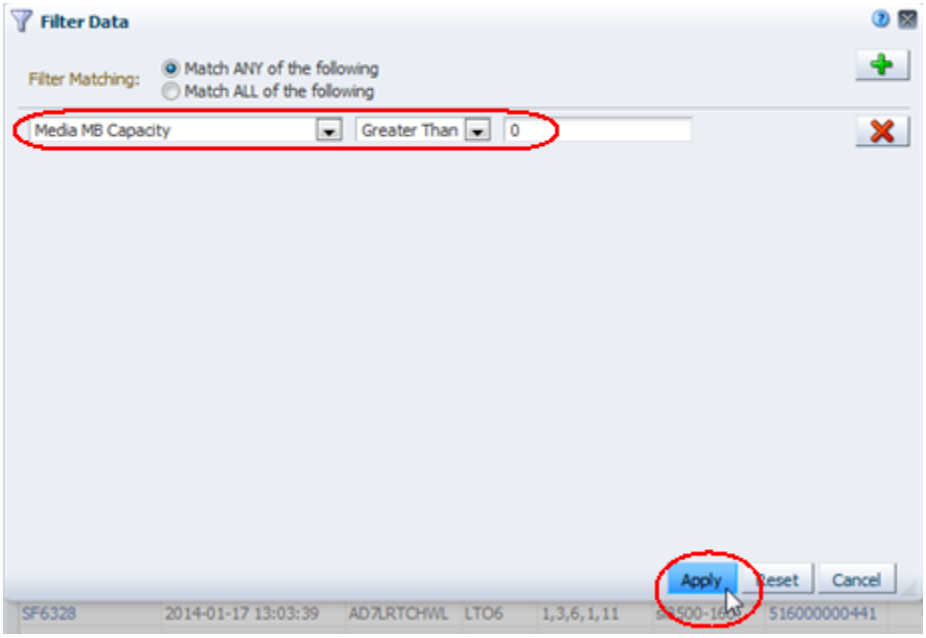
The longer STA monitors the libraries, the more exchange data it receives, and the lower the overall uncertainty level.

a. Click **Filter Data**.

b. Add the following selection criteria:

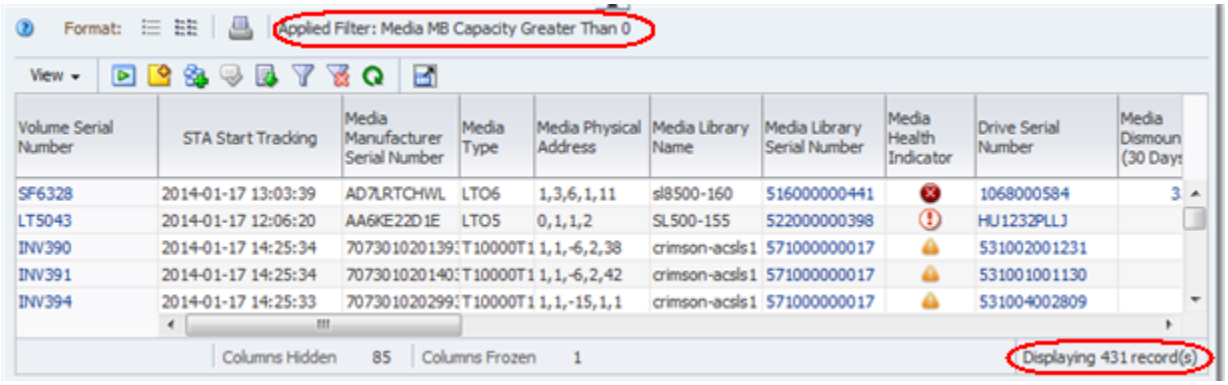
* **Media MB Capacity** is greater than 0

c. Click **Apply**.



4. Note the number of records eliminated, since it reflects the level of uncertainty.

   In the sample below, the number of records goes from 647 to 431, indicating a high uncertainty level. This library has been monitored for only a few days.



5. For the media in the resulting list, use the following steps to display the capacity and space available for each piece of media displayed.

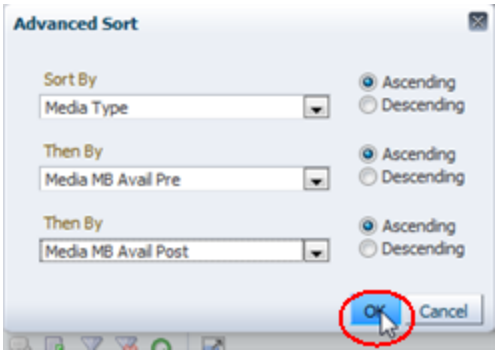
a. In the Table Toolbar, select **View**, then select **Sort**, then select **Advanced**.

b. Complete the Advanced Sort dialog box as follows:

* In the Sort By menu, select **Media Type**.
* In the first Then By menu, select **Media MB Avail Pre**.
* In the next Then By menu, select **Media MB Avail Post**.

Note: 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.

c. Click **OK**.



The table is sorted according to your criteria.

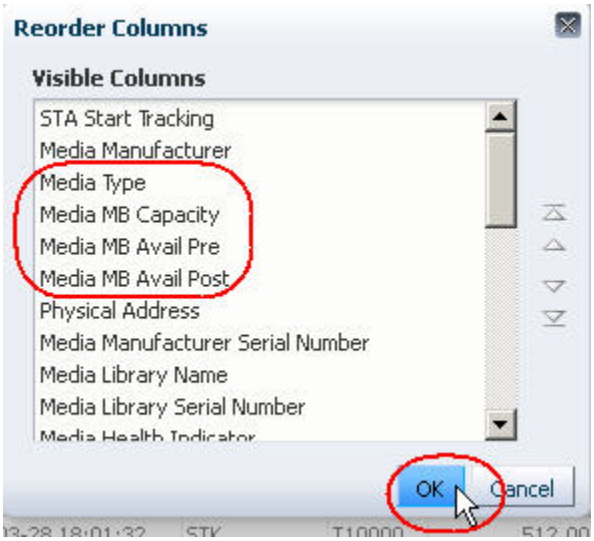
6. To better view the capacity data together on the screen, use the following steps to reorder the table columns.

   a. In the Table Toolbar, select **View**, then select **Reorder Columns**.

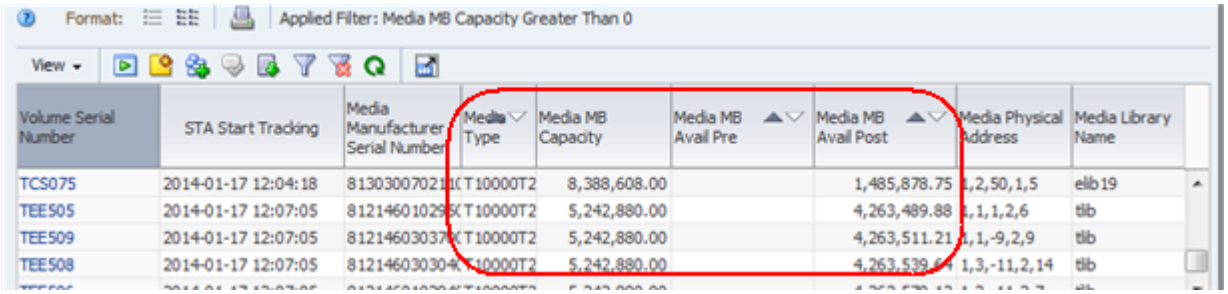
   b. In the Reorder Columns dialog box, arrange the following attributes so they are listed together.

      * Media Type
      * Media MB Capacity
      * Media MB Avail Pre
      * Media MB Avail Post

   c. Click **OK**.

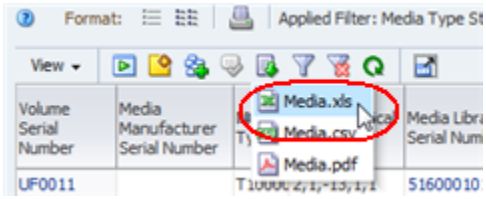


The table columns are reordered according to your criteria.



7. To calculate the total capacity and space available for each media type, you must use an external spreadsheet application. Use the following steps to export the data displayed in the table to an HTML-based Excel-compatible file.

   a. Click the **Export** icon in the Table Toolbar and select the **Media.xls** option.



   b. Save the file to a location on your local computer.

8. Use a compatible spreadsheet application to open the file and summarize the data. For example, you may want to calculate totals, percentages used, or averages by media type.

Project Future Media, Drive, or Storage Cell Requirements

These procedures address the questions, "Am I likely to need more media, drives, or storage cells next year? If so, how many?"

The criteria for determining whether drives or media need replacement varies by site.

For drives, STA tracks many applicable criteria — in particular, several *drive lifetime* measures, such as Drive Lifetime Loads, Drive Lifetime Meters, and Drive Lifetime Power Hours. See "Report Percent Drive Utilization", below, for one example.

For media, STA provides data that is useful in a variety of scenarios, including the following:

- Your site is migrating off one type of media and you need to replace it with another; see "Report Data Related to Media Migration" on page 13-43 for details.
- Existing media are ageing or showing errors beyond your site-defined reasonable threshold; see "Report Data Related to Media Ageing" on page 13-45 for details.
- Existing media are filling up; see "Report Shortages or Surpluses of Media" on page 13-36 for details.

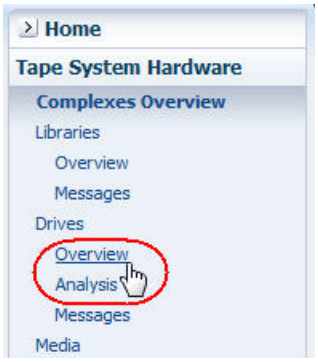
Referenced Tasks

- "Apply a Template" on page 3-8
- *STA Screen Basics Guide*, to sort by a column
- "Use the Filter Data Dialog Box to Change a Table Filter" on page 4-9
- *STA Screen Basics Guide* for information on tooltips

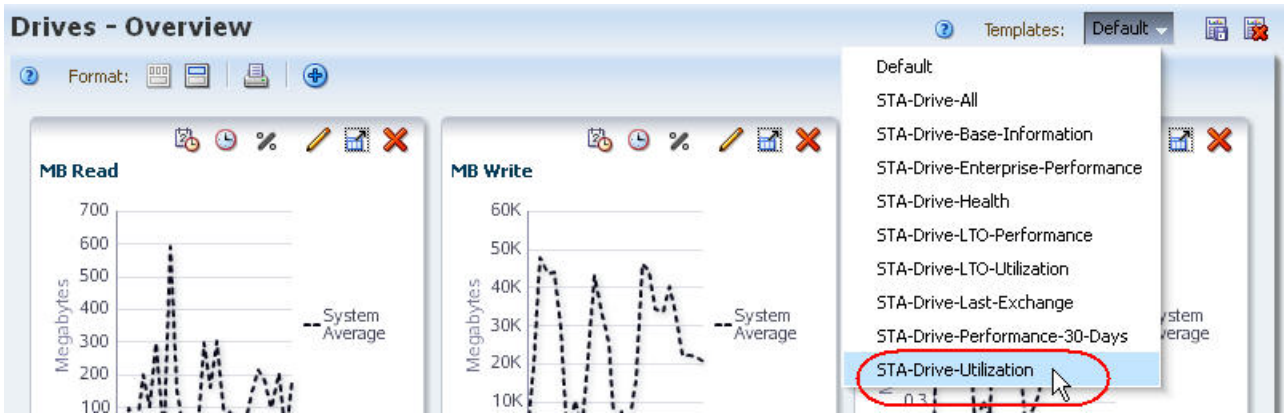
- "Create a Template" on page 3-13

Report Percent Drive Utilization

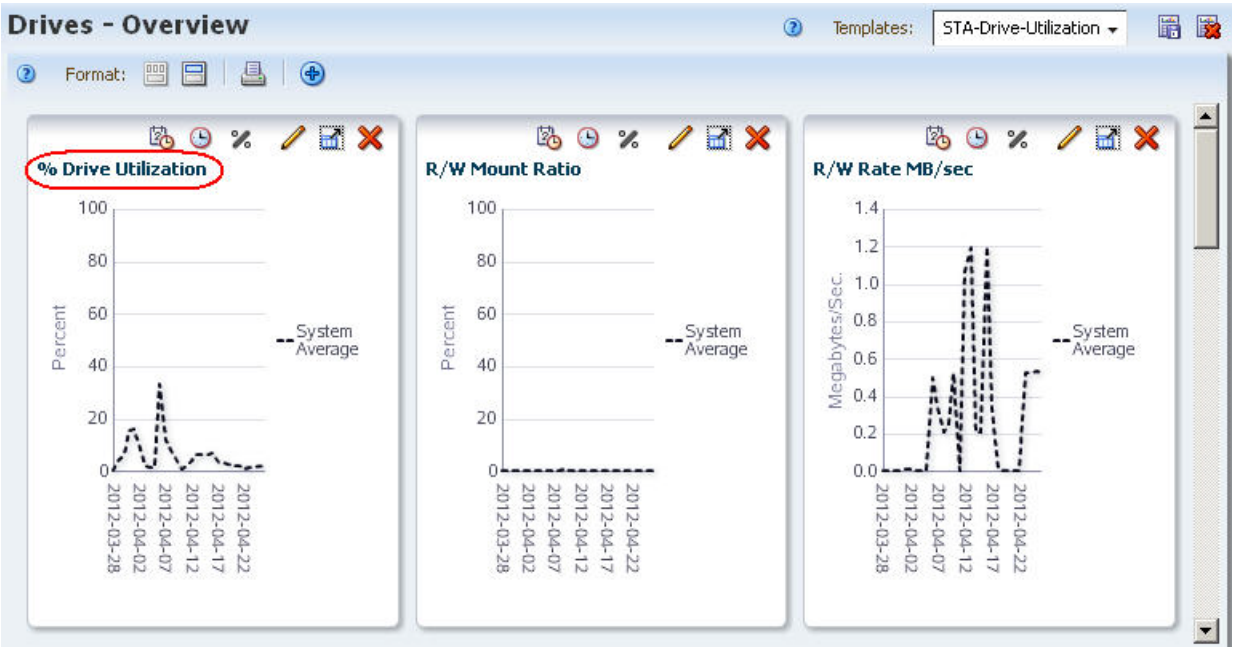
1. In the Navigation Bar, select **Tape System Hardware**, then select **Drives Overview**.



2. In the **Templates** menu, select the "STA-Drive-Utilization" template.

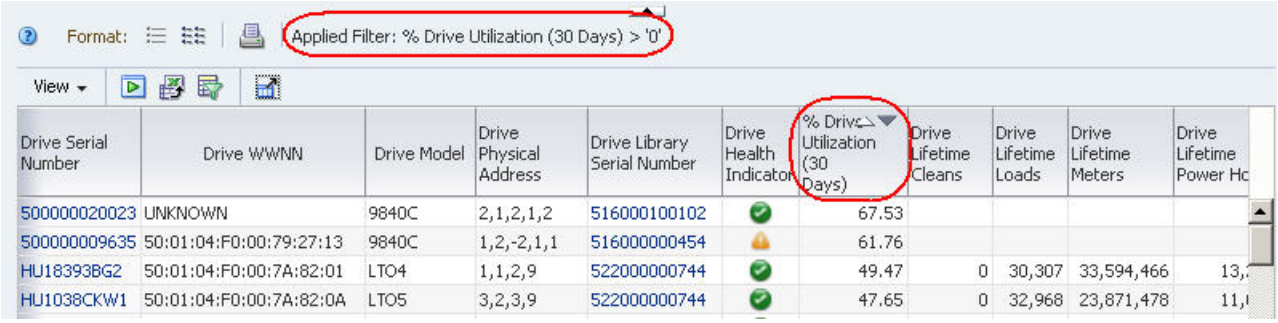


The first graph on the screen is % Drive Utilization, which displays the system average of percent drive utilization over time. This provides a high-level measure of activity for all drives in your environment.



3. To differentiate and compare the activity levels of individual drives, and to identify potential *hot spots*, you can sort or filter the drives in the table by various criteria, such as drive type or library.

   In the sample below, the table is sorted in descending order of % Drive Utilization (30 Days) — highest percentage utilization first.



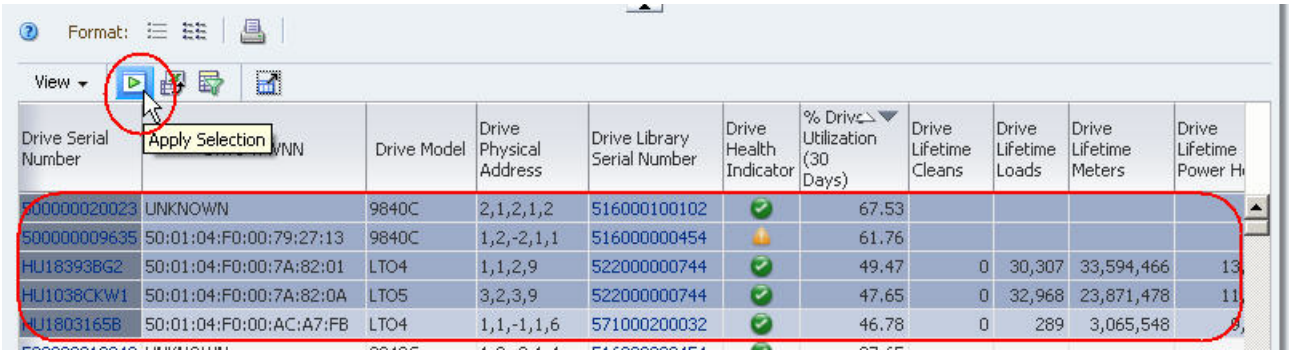
Drive Serial Number	Drive WWNN	Drive Model	Drive Physical Address	Drive Library Serial Number	Drive Health Indicator	% Drive Utilization (30 Days)	Drive Lifetime Cleans	Drive Lifetime Loads	Drive Lifetime Meters	Drive Lifetime Power Hc
500000020023	UNKNOWN	9840C	2,1,2,1,2	516000100102		67.53				
500000009635	50:01:04:F0:00:79:27:13	9840C	1,2,-2,1,1	516000000454		61.76				
HU18393BG2	50:01:04:F0:00:7A:82:01	LTO4	1,1,2,9	522000000744		49.47	0	30,307	33,594,466	13,
HU1038CKW1	50:01:04:F0:00:7A:82:0A	LTO5	3,2,3,9	522000000744		47.65	0	32,968	23,871,478	11,

4. Use the following steps to add the top five drives to the screen graphs.

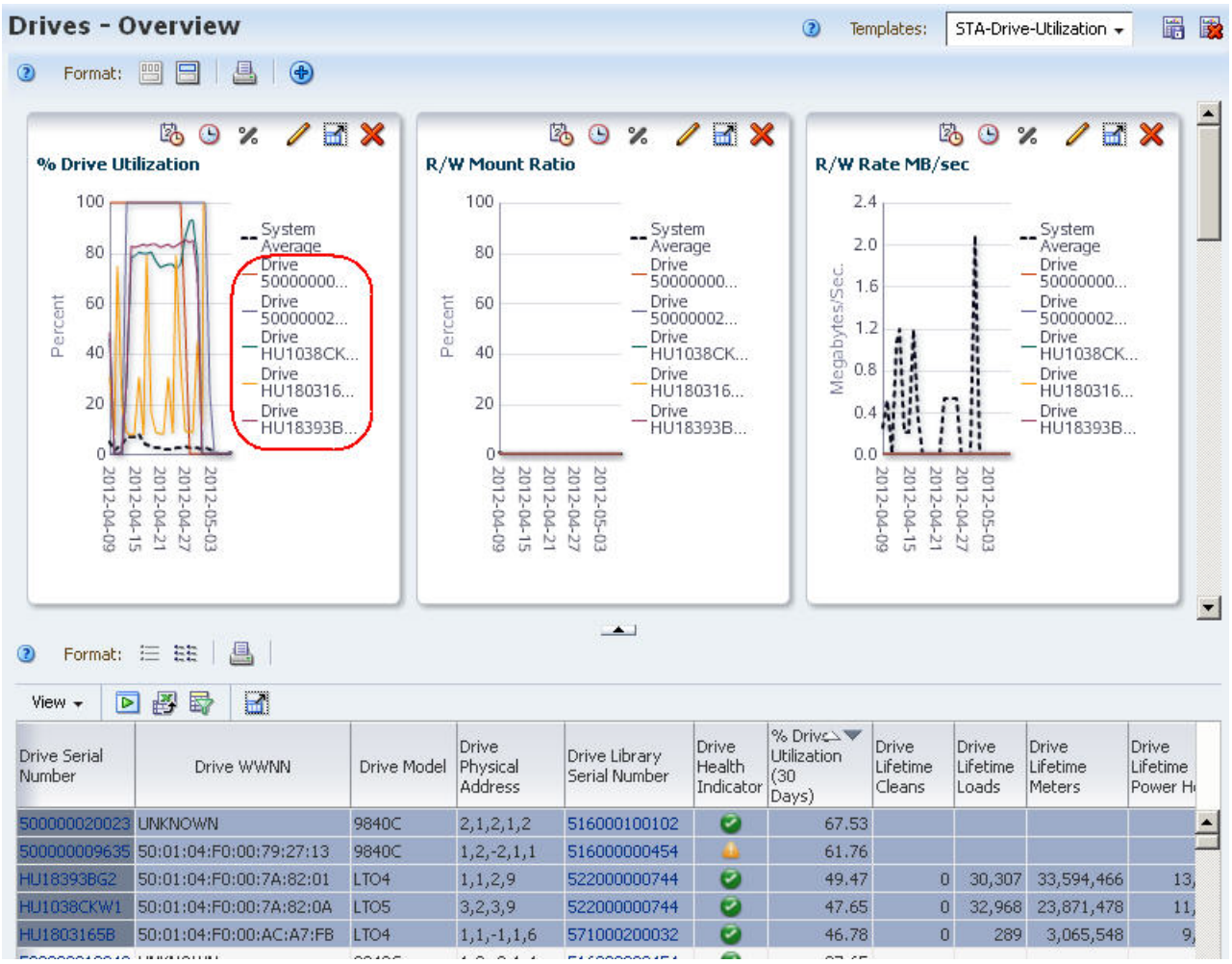
   Adding the drives to the graphs allows you to compare their attribute values against the system average.

   a. In the List View table, select the top five drives.

   b. Click the **Apply Selection** icon on the List View Toolbar.



The drives are added to the graphs.



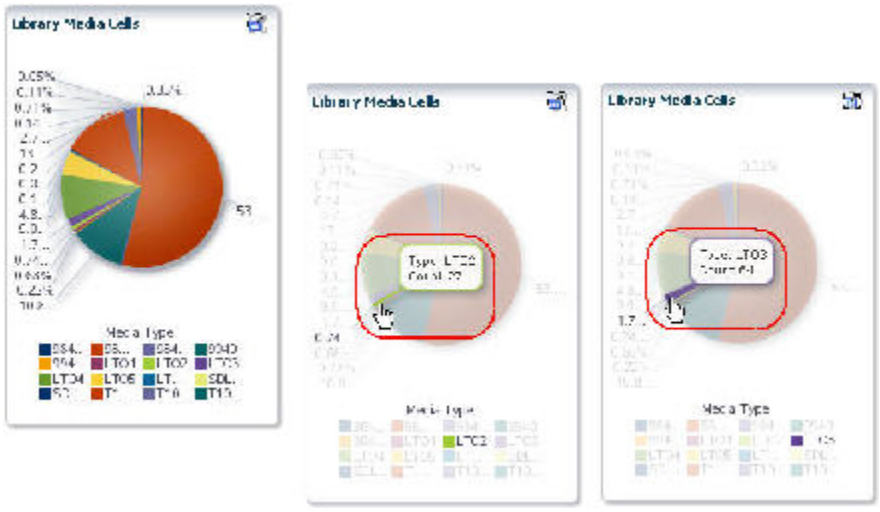
Report Data Related to Media Migration

1. In the Navigation Bar, select **Home**, then select **Dashboard**.

The screen provides a high-level view of the number of media, aggregated by type.

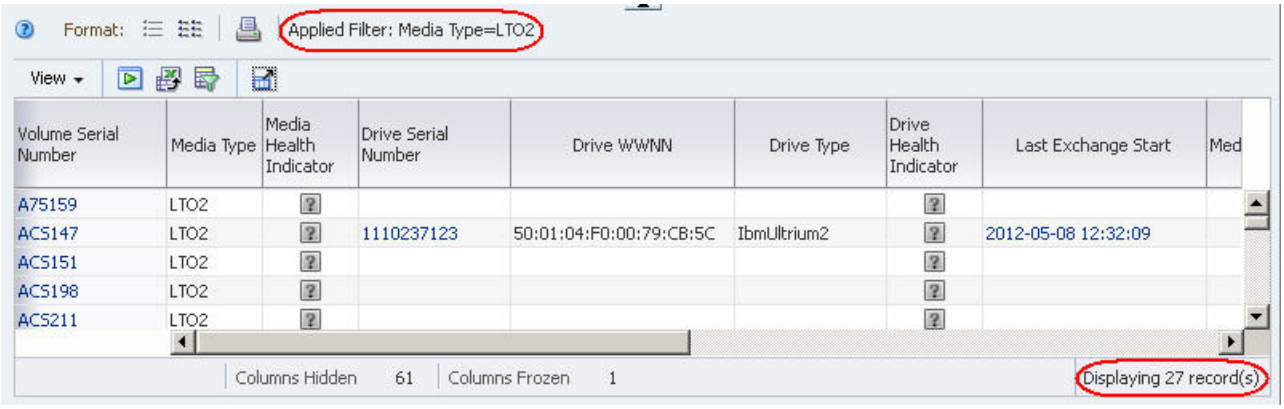
2. Move the mouse over the Library Media Cells graph to display detail for each type of media stored in the library system.

   The sample below illustrates a site planning to migrate off older generation LTO2 and LTO3 tapes. Moving the mouse over these two sections of the pie chart reveals there are a total of 27 LTO2 and 64 LTO3 media that must be replaced.



3. Select a section of the pie chart to go to the Media – Overview screen filtered for that type of media.

   The sample below shows the screen filtered for LTO2 media. On this screen, you can organize the media records by remaining capacity, physical location, or other attributes pertinent to the migration process.



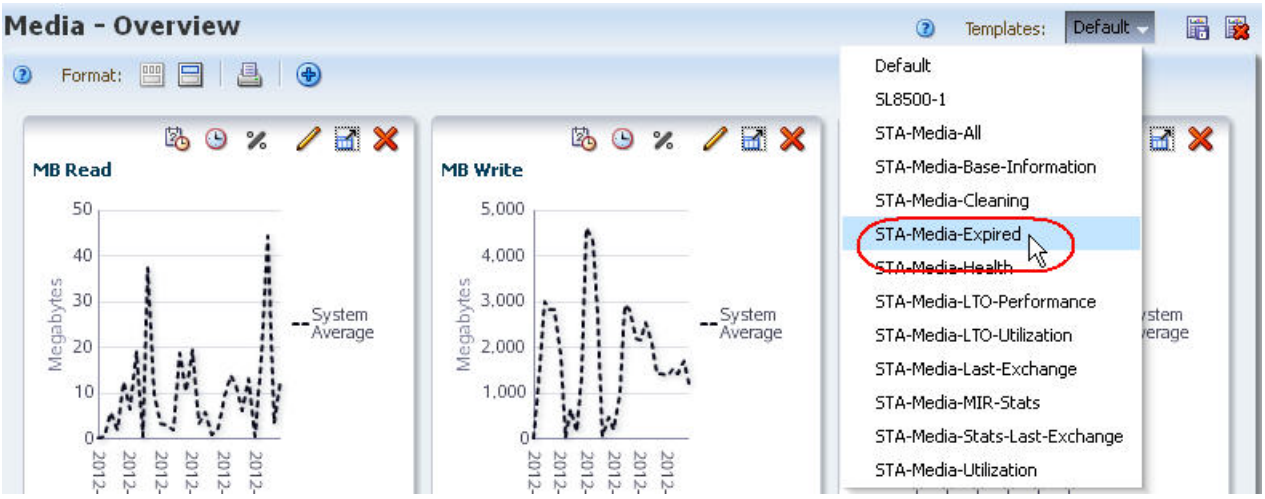
4. Alternative approaches for gathering this information are to use either of the following screens, which can summarize, filter, or aggregate media totals by type.

- Media – Overview
- Media – Analysis

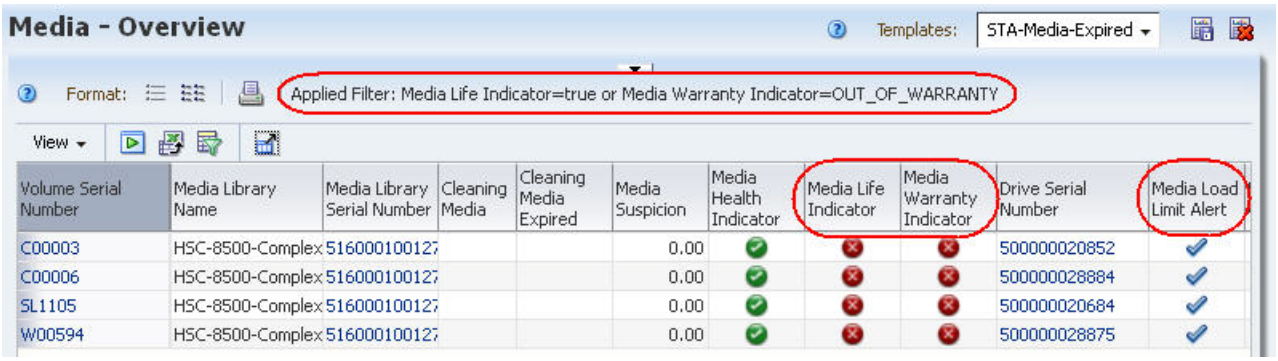
Report Data Related to Media Ageing

1. In the Navigation Bar, select **Tape System Hardware**, then select **Media Overview**.

2. In the **Templates** menu, select "STA-Media-Expired".



This template includes a filter and attributes related to media that have expired and should be retired from service.



Report Resources With the Highest Utilization

This procedure 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*.

The following methods are described:

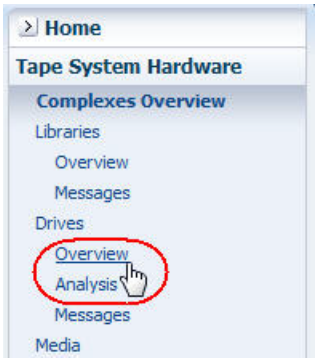
- "Report Drive Utilization"
- "Report Media Utilization" on page 13-48

Referenced Tasks

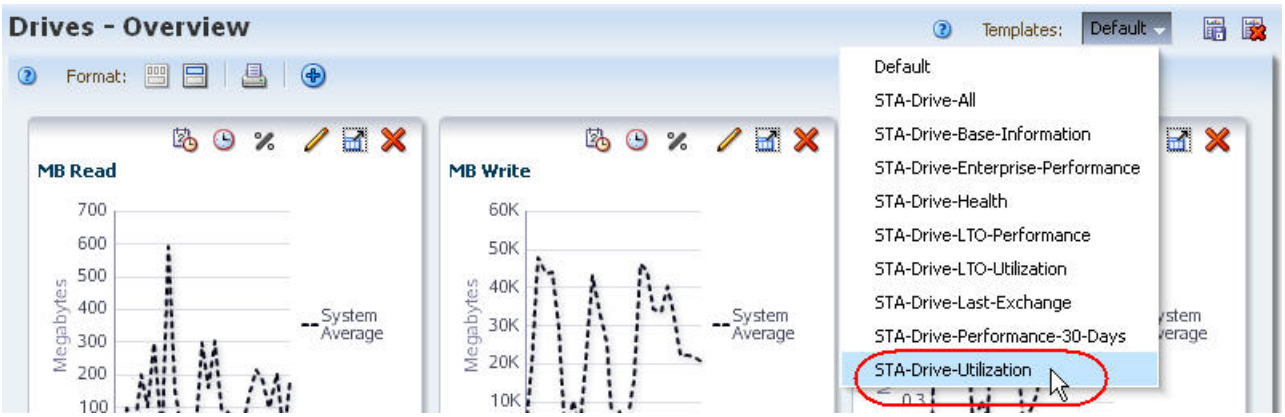
- "Apply a Template" on page 3-8
- "Use the Filter Data Dialog Box to Change a Table Filter" on page 4-9
- *STA Screen Basics Guide*, to sort by multiple columns
- *STA Screen Basics Guide*, to export table data

Report Drive Utilization

1. In the Navigation Bar, select **Tape System Hardware**, then select **Drives Overview**.



2. In the **Templates** menu, apply the "STA-Drive-Utilization" template.



This template displays utilization statistics for all drive types.

3. Use the following steps to remove drives for which STA has no utilization data.

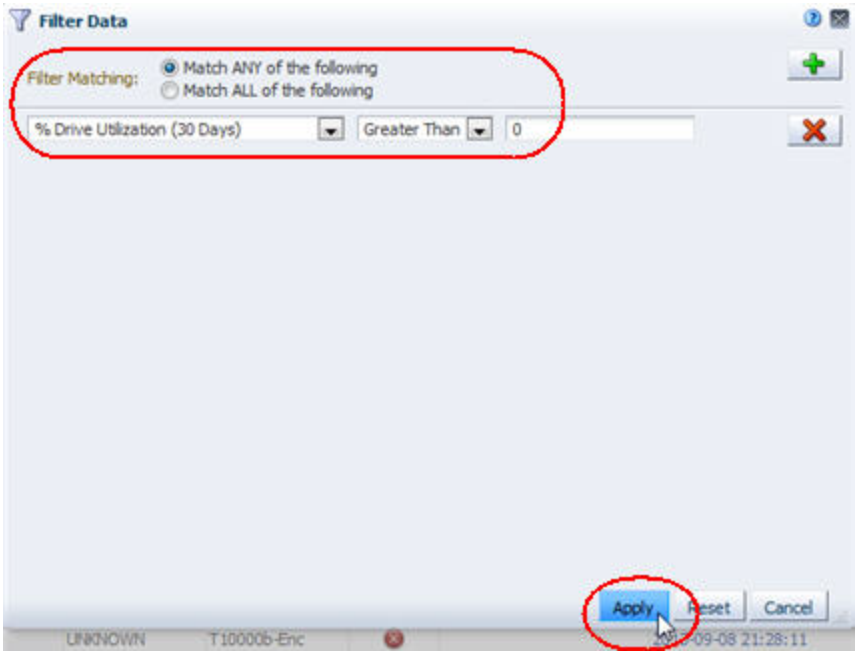
a. Click **Filter Data**.

b. In the selection criteria, select the attribute that represents the utilization measure of interest to you. Select **Greater than** and enter 0.

   Following are some suggested attributes for measuring drive utilization.

   * To identify drives with the highest utilization rates, use % Utilization (30 Days).
   * To identify drives that have recorded the most new data, use MB Write (30 Days), or MB Received (30 Days).
   * To identify drives that have passed the most data at the drive head, use MB R/W (30 Days).
   * For drives that have been in the library for their entire periods of use, the drive *lifetime* attributes are also useful measures of activity — for example, Drive Lifetime Loads or Drive Lifetime Hours in Motion.

c. Click **Apply**.



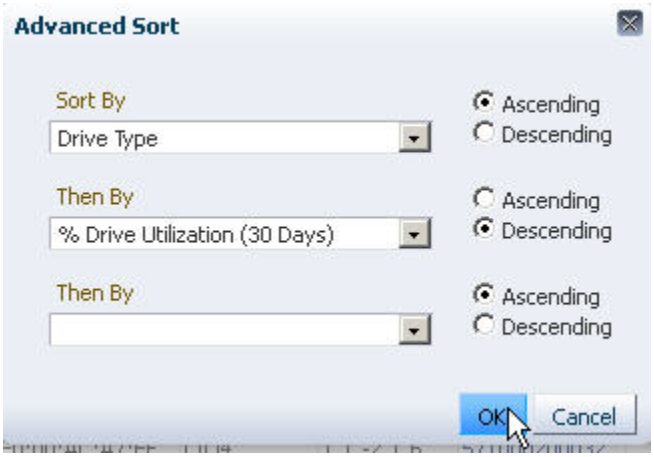
4. Perform a multiple-column sort to group the records by drive type and then utilization.

   a. In the Table Toolbar, select **View**, then select **Sort**, then select **Advanced**.

   b. Complete the Advanced Sort dialog box as follows:

      * In the Sort By field, select **Drive Type**.
      * In the Then By field, select the attribute that you used in Step b above, and **Descending**.

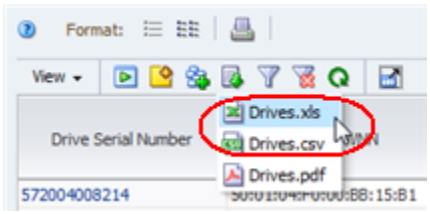
   c. Click **OK**.



The table is sorted according to your criteria.

5. To summarize the data by drive type, you must use an external spreadsheet application. Use the following steps to export the data displayed in the table to an HTML-based Excel-compatible file.

   a. Click the **Export** icon in the Table Toolbar, and select **Drives.xls**.



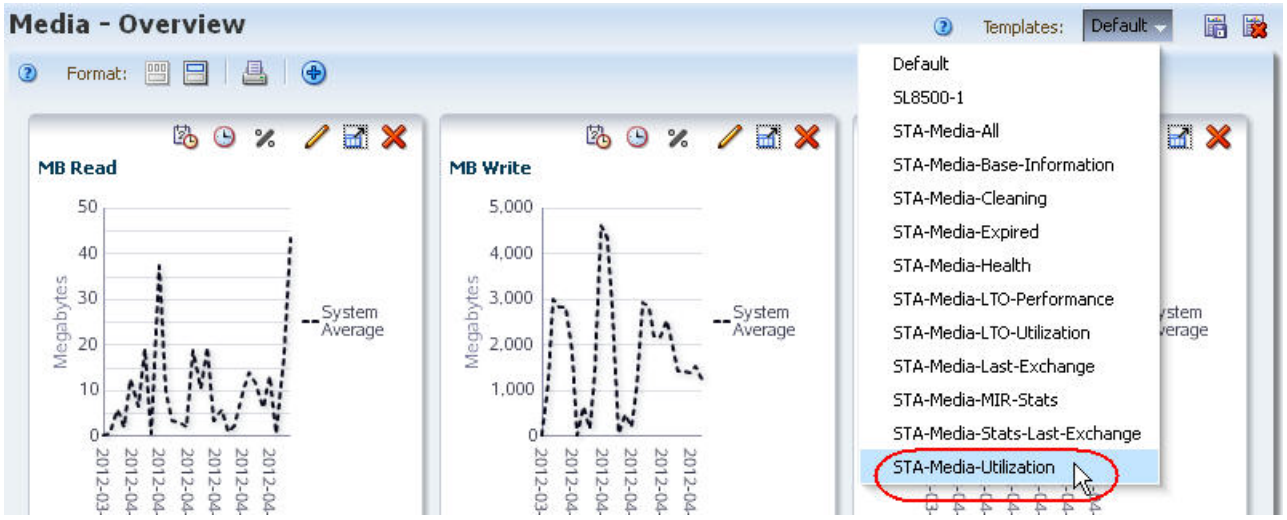
   b. Save the file to a location on your local computer.

6. Use a compatible spreadsheet application to open the file and summarize the data.

Report Media Utilization

1. In the Navigation Bar, select **Tape System Hardware**, then select **Media Overview**.

2. In the **Templates** menu, apply the "STA-Media-Utilization" template.



This template displays utilization statistics for all media types.

3. Use the following steps to remove media for which STA has no utilization data.

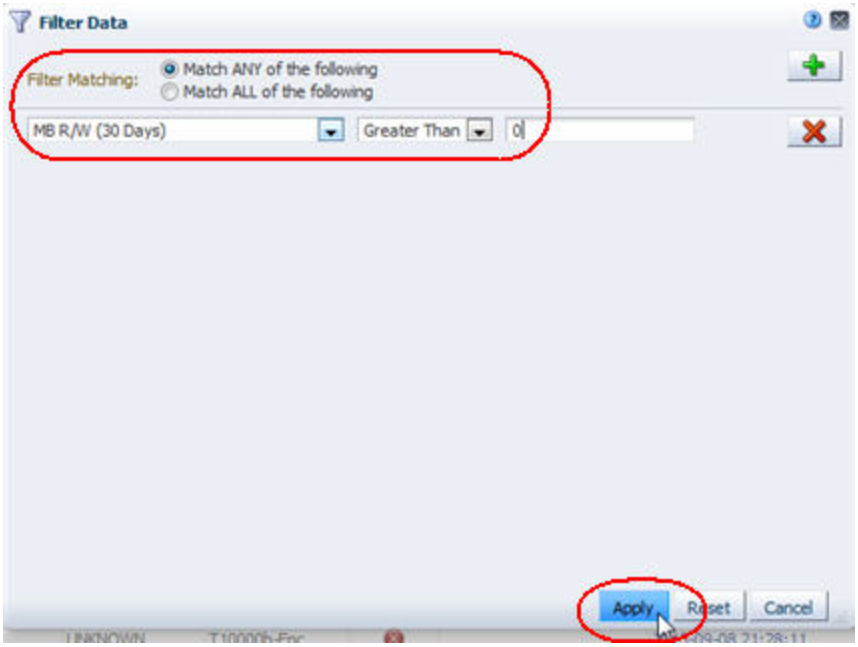
   a. Click **Filter Data.**

   b. In the selection criteria, select the attribute that represents the utilization measure of interest to you. Select **Greater than** and enter 0.

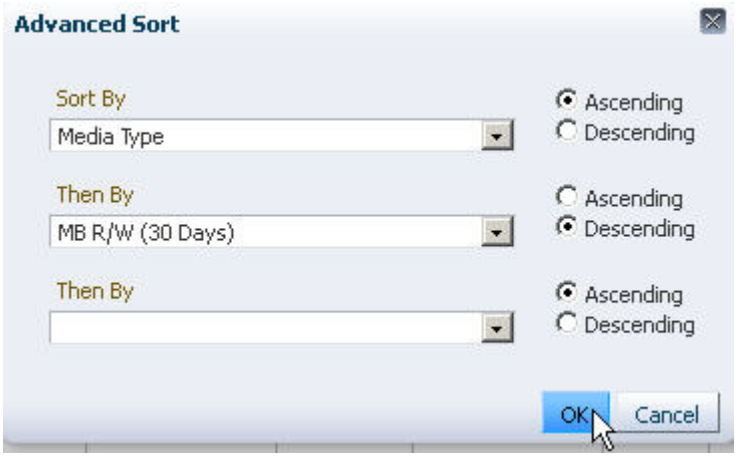
      Following are some suggested attributes for measuring media utilization:

      * To identify media with the greatest amount of movement, use Time spent reading or writing.
      * To identify media below a specific threshold of available space, use Media MB Avail Pre/Post
      * To identify media with the greatest number of mounts and dismounts, use Media Dismounts (30 days).
      * To identify media with the greatest amount of data read or written, use MB R/W (30 days).

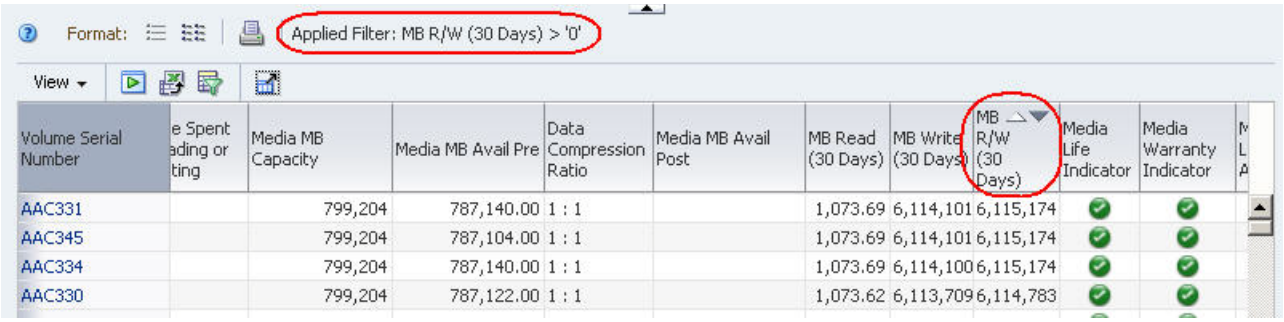
   c. Click **Apply**.



4. Perform a multiple-column sort to group the records by media type and then utilization.
   a. In the Table Toolbar, select **View**, then select **Sort**, then select **Advanced**.
   b. Complete the Advanced Sort dialog box as follows:
      * In the Sort By field, select **Media Type**.
      * In the Then By field, select the attribute that you used in Step b above, and **Descending**.
   c. Click **OK**.

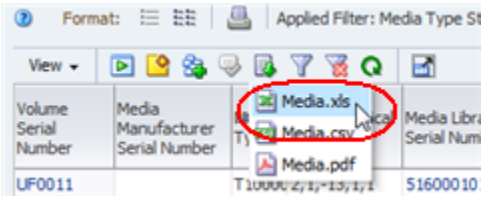


The table is sorted according to your criteria.



5. To summarize the data by media type, you must use an external spreadsheet application. Use the following steps to export the data displayed in the table to an HTML-based Excel-compatible file.

   a. Click the **Export** icon in the Table Toolbar, and select **Media.xls**.



   b. Save the file to a location on your local computer.

6. Use a compatible spreadsheet application to open the file and summarize the data.

Report Library Relative Activity Levels

This procedure addresses the questions, "Which library in my tape environment is the busiest? Which is the least busy?"

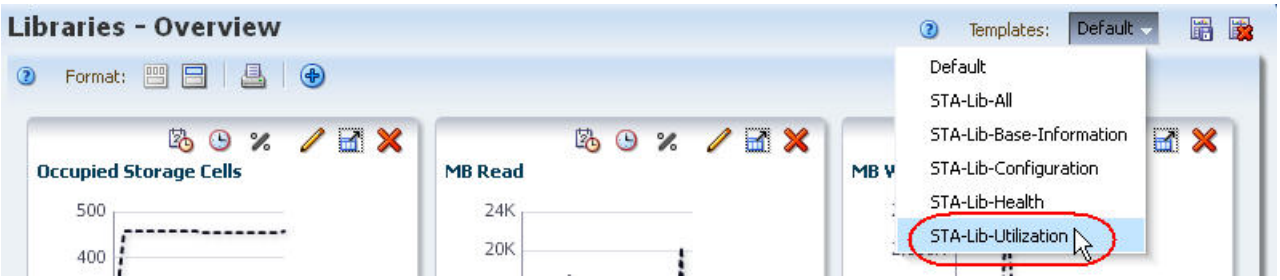
The definition of *busy* varies by site; common definitions include the number of exchanges, mounts, or dismounts. This procedure uses the number of mounts. In addition, it provides instructions for graphing the data so you can compare the libraries to one another and to the system average.

Referenced Tasks

- "Apply a Template" on page 3-8
- *STA Screen Basics Guide*, to sort by a column
- *STA Screen Basics Guide*, to add a graph pane
- *STA Screen Basics Guide*, to change the graphed attribute
- *STA Screen Basics Guide*, to apply library resources to graphs
- *STA Screen Basics Guide*, to detach a graph pane

1. In the Navigation Bar, select **Tape System Hardware**, then select **Libraries Overview**.

2. In the **Templates** menu, apply the "STA-Lib-Utilization" template.



3. In the Mounts (30 Days) column, click the **Sort Ascending** or **Sort Descending** arrow.

Note: Other columns you might want to sort by are Enters (30 Days), Ejects (30 Days), Occupied Storage Cells, or MB R/W (30 Days).

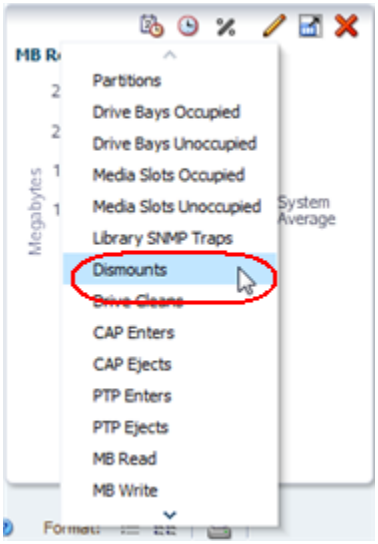
Library Serial Number	upied rage s	Empty Storage Cells	Occupied Drive Bays	Empty Drive Bays	Enters (30 Days)	Ejects (30 Days)	Mounts (30 Days)	% Drive Utilization (30 Days)	MB R/W (30 Days)	MB Read (30 Days)	MB Write (30 Days)
516000100127	948	9,140	50	14	0	0	27,296	3.01	0	0	0
522000000744	69	311	8	0	4	5	16,599	28.46	132,599,968	29,949	132,570,016
571000200032	591	1,214	34	14	0	0	13,696	20.29	38,170,824	29,116	38,141,708
516000100451	458	2,718	37	27	0	0	10,696	7.14	16,037,375	17,363	16,020,013
516000100102	553	895	34	30	0	1	7,057	0.97	210,250	69,862	140,388
516000000454	290	1,158	28	36	0	0	5,367	4.15	3,607,462	577,915	3,029,547
516000100090	320	1,128	36	28	18	19	54	0.29	812,857	360,703	452,154
516000100561	434	9,654	5	59	0	0	0	0.00	0	0	0

4. Use the following steps to add a graph pane showing dismounts.

   a. Click the **Add Graph** icon in the Graphics Area Toolbar.

A new graph pane, with the attribute MB Read, is added to the end of the Graphics Area display. You may need to scroll down to see the graph.

b. Click the **Change Graphed Attribute** icon in the Graph Pane Toolbar, and select the **Dismounts** attribute from the menu.



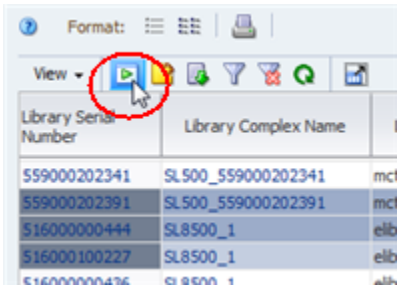
The graph is updated to display the system average for dismount data.

5. Use the following steps to add selected libraries to the screen graphs.

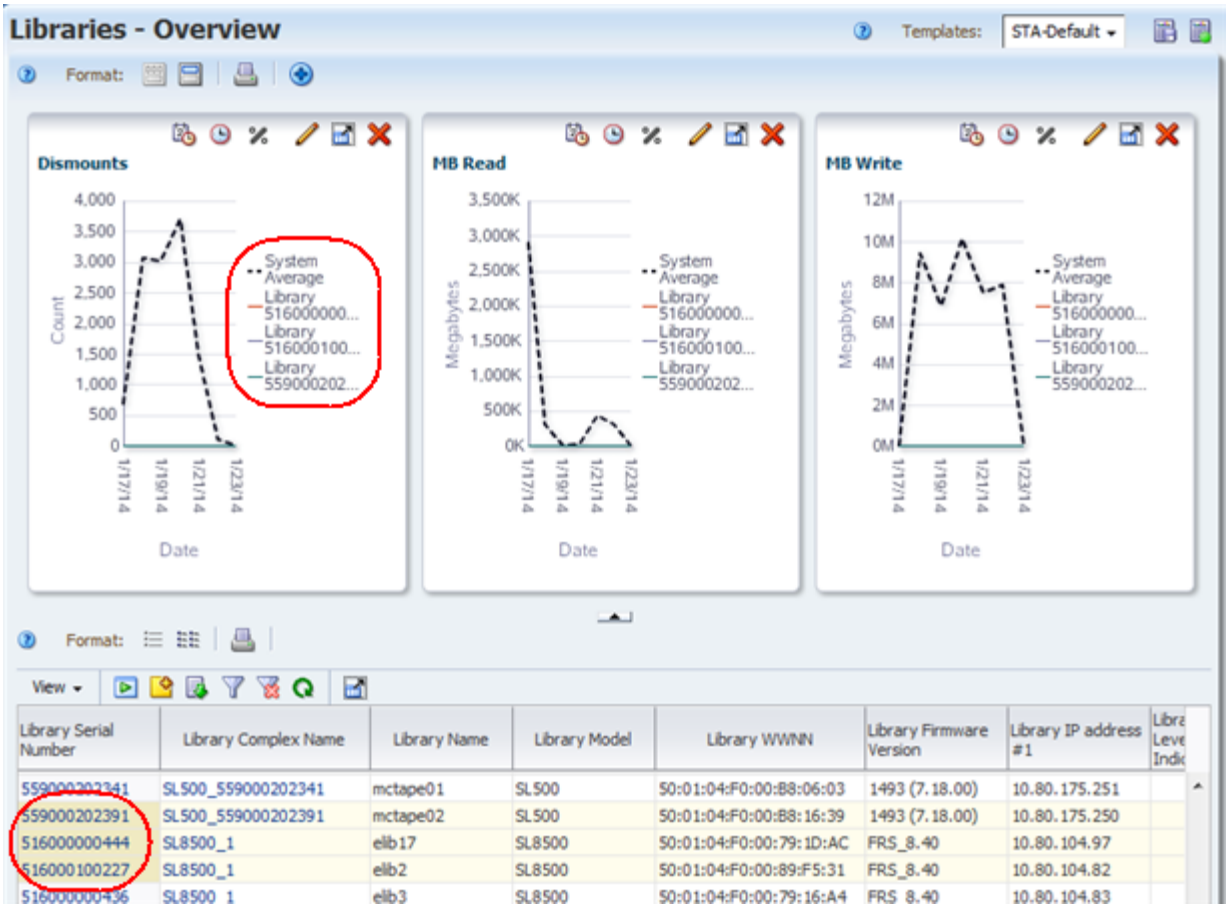
Adding the libraries to the graphs allows you to compare their attribute values against the system average.

a. In the List View table, select the libraries you want to add to the graphs.

b. Click the **Apply Selection** icon on the List View Toolbar.



In the sample below, the three libraries with most mounts are added to all the graphs.



6. In the Dismounts graph pane, click the **Detach Pane** icon to detach the graph to enlarge it and display more detail.

Report Media Approaching Capacity

This procedure addresses the questions, "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?"

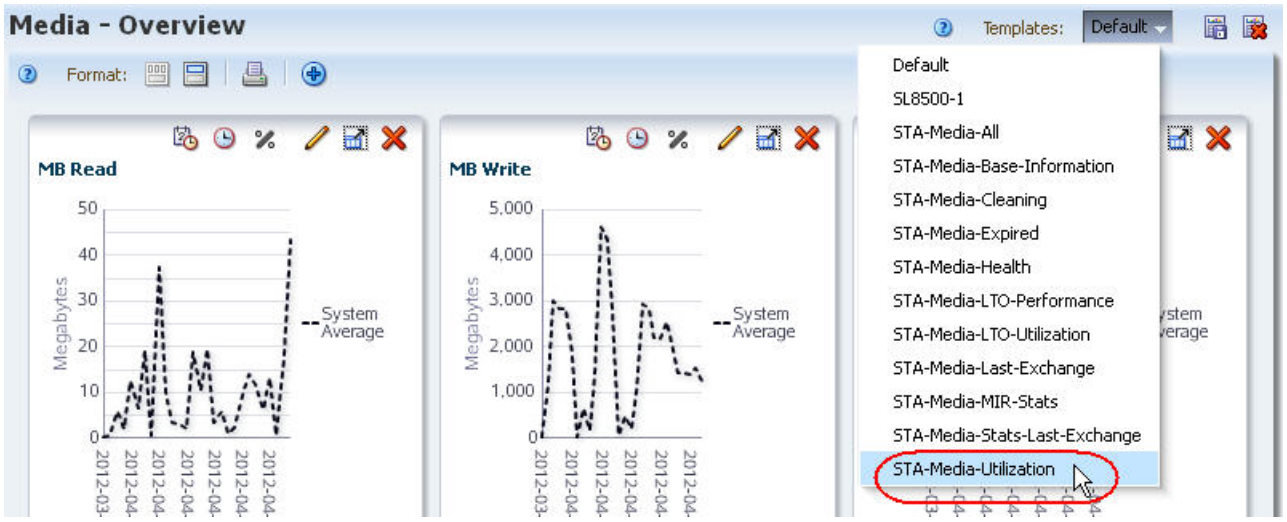
STA reports media capacity and available space as numeric values only, not as percentages. This procedure provides instructions for exporting the numeric values to a spreadsheet application, which can then be used to calculate percentages. The resulting list can be used by a media eject script.

Referenced Tasks

- "Apply a Template" on page 3-8
- *STA Screen Basics Guide*, to sort by a column
- *STA Screen Basics Guide*, to export table data

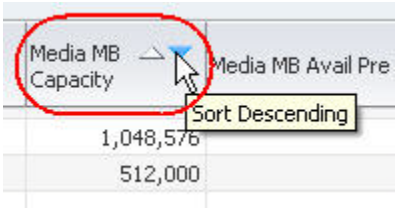
1. In the Navigation Bar, select **Tape System Hardware**, then select **Media Overview**.

2. In the **Templates** menu, apply the "STA-Media-Utilization" template.



This template includes the Media MB Available and Media MB Capacity attributes.

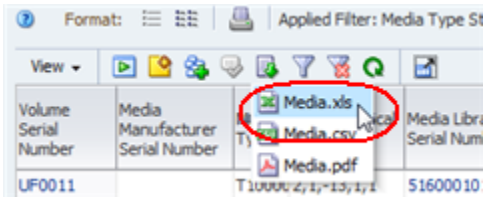
3. In the Media MB Capacity column, click the **Sort Descending** arrow.



The media with the highest capacity are brought to the top of the list. This sort also has the advantage of grouping media by type, since capacity tends to vary by media type.

4. To create a list that can be used by a media eject script, you must use an external spreadsheet application. Use the following steps to export the data displayed in the table to an HTML-based Excel-compatible file.

   a. Click the **Export** icon in the Table Toolbar and selected the **Media.xls** option.



   b. Save the file to a location on your local computer.

5. Using a compatible spreadsheet program, add a Percentage Full column, containing calculated values derived from the attributes in the exported table. Sort the table by the column values and identify a list of media over 90 percent full.

Report Drive Firmware Levels

This procedure addresses the question, "Have all my drives been upgraded to the latest firmware?" Firmware levels are usually evaluated by drive type or model.

The following methods are described:

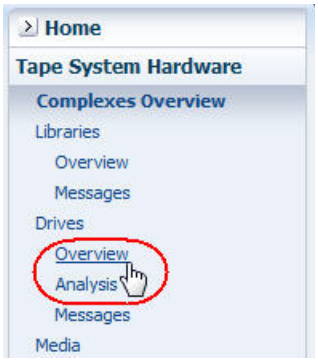
- "Using the Drives – Overview Screen"
- "Using the Drives – Analysis Screen" on page 13-60

Referenced Tasks

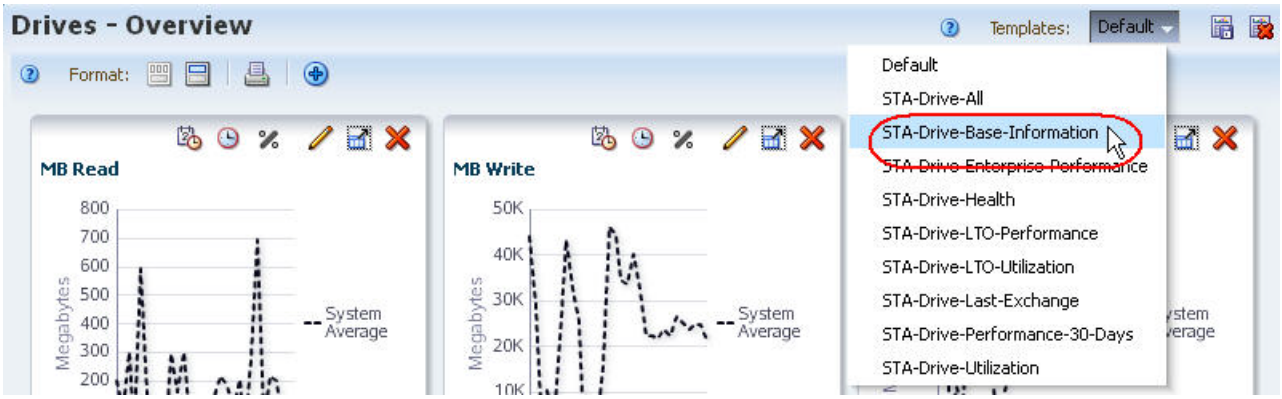
- "Apply a Template" on page 3-8
- *STA Screen Basics Guide*, to move a column
- *STA Screen Basics Guide*, to sort by multiple columns
- "Use the Filter Data Dialog Box to Change a Table Filter" on page 4-9
- *STA Screen Basics Guide*, to change the height of a row
- *STA Screen Basics Guide*, to navigate using aggregate count links

Using the Drives – Overview Screen

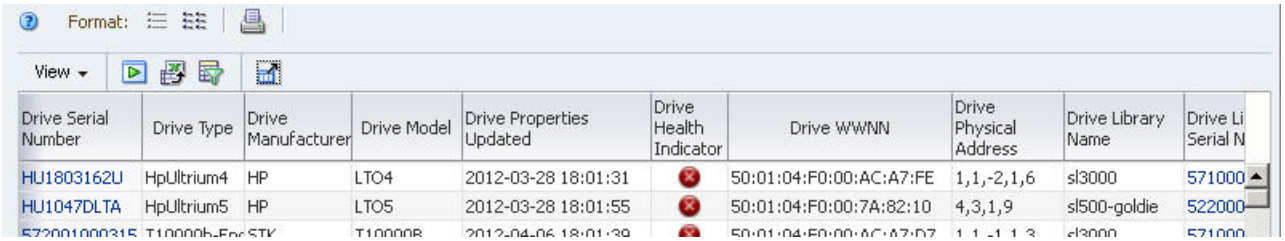
1. In the Navigation Bar, select **Tape System Hardware**, then select **Drives Overview**.



2. In the **Templates** menu, apply the "STA-Drives-Base-Information" template.

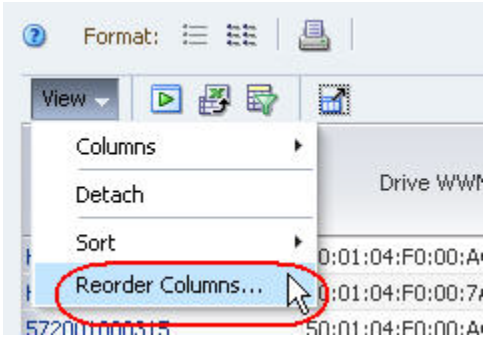


This template includes the drive firmware version and other related attributes.



3. Use the following steps to reorder the table columns so the drive firmware level is displayed next to the drive model.

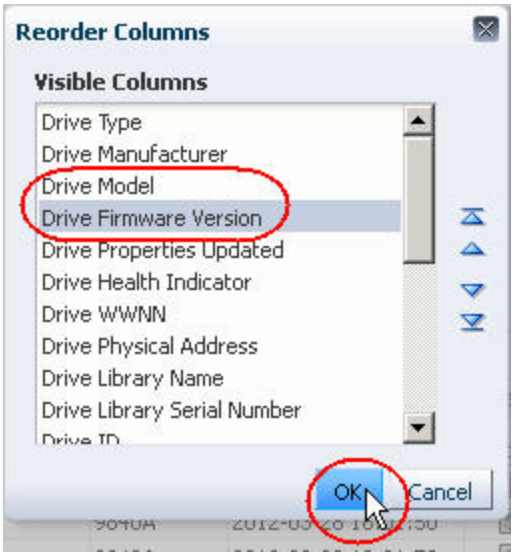
   a. In the Table Toolbar, select **View**, then select **Reorder Columns**.



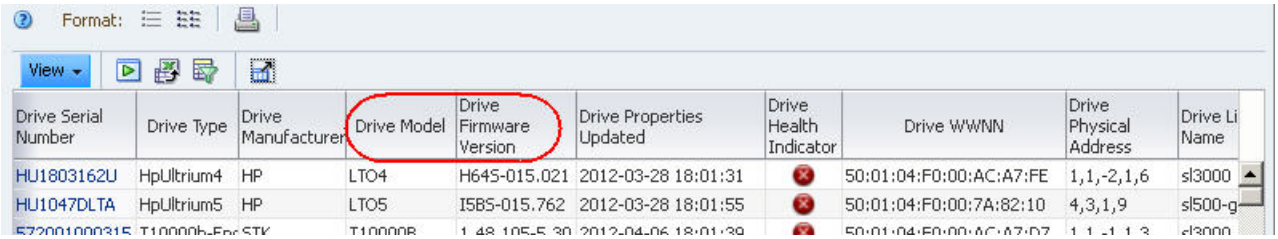
   b. In the Reorder Columns dialog box, arrange the following attributes so they are listed together.

* Drive Model
* Drive Firmware Version

c. Click **OK**.



The table columns are reordered according to your criteria.



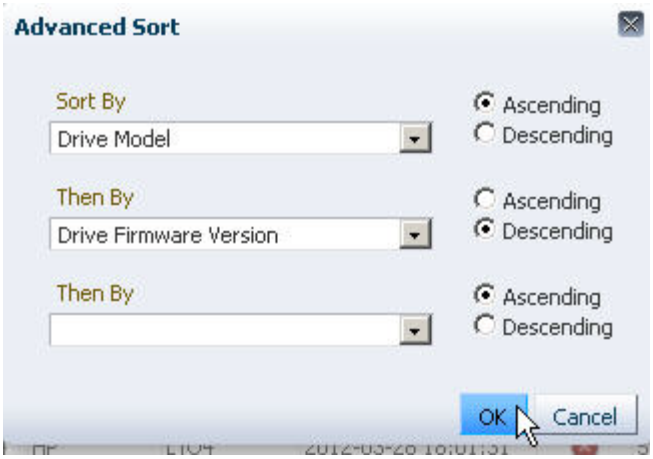
4. To display firmware levels by drive type, use the following steps to set up a multiple-column sort.

   a. In the Table Toolbar, select **View**, then select **Sort**, then select **Advanced**.

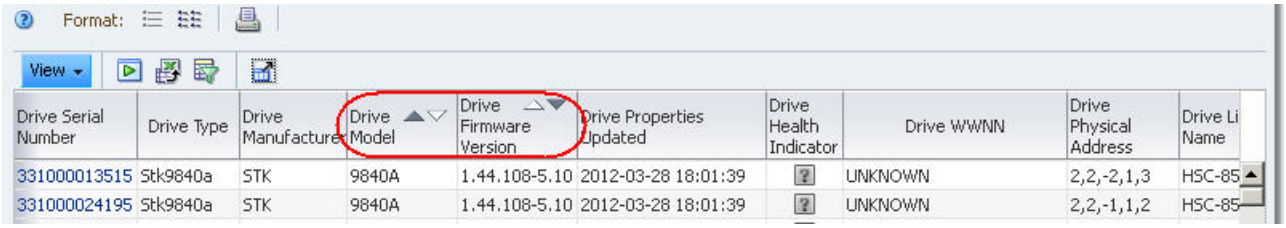
   b. complete the Advanced Sort dialog box as follows:

      * In the Sort By field, select **Drive Model**.
      * In the Then By field, select **Drive Firmware Version** and select **Descending**.

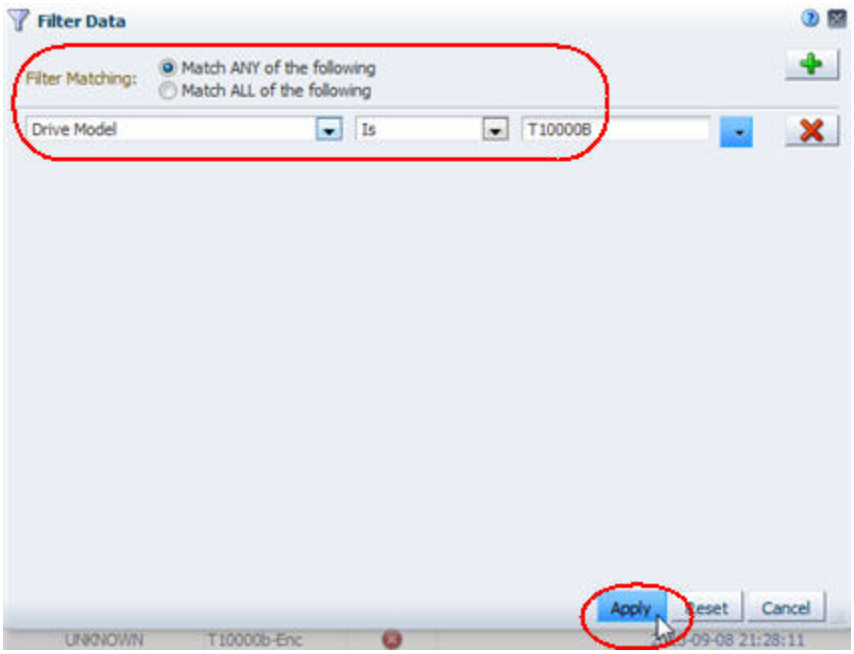
   c. Click **OK**.



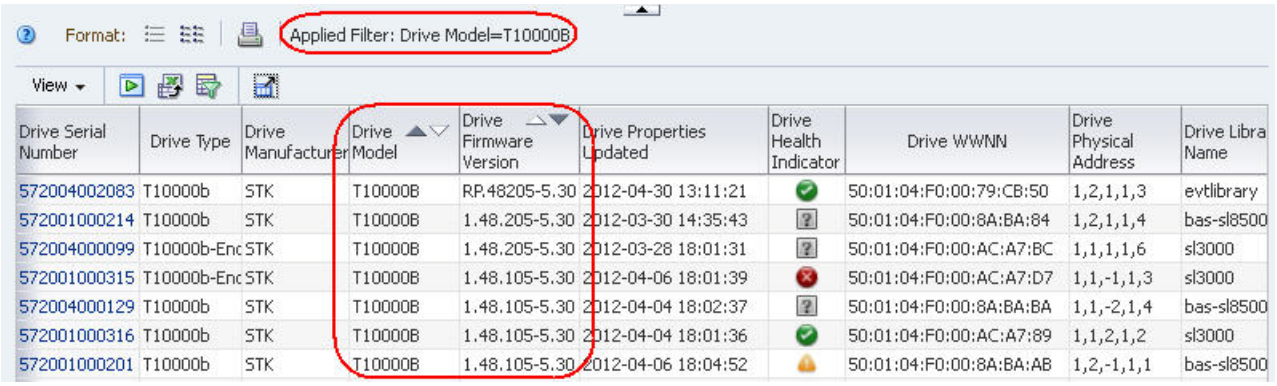
The table is sorted according to your criteria.



5. Use the following steps to display firmware levels for a specific drive model.
   a. Click **Filter Data**.
   b. Specify the following selection criteria:
      * **Drive Model** is the drive model of interest.
   c. Click **Apply**.



The table is updated according to your selection criteria.

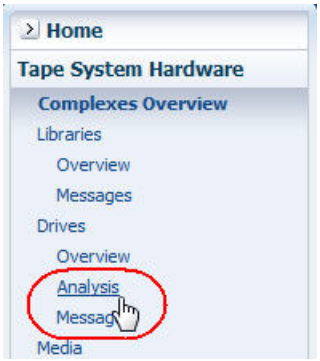


Drive Serial Number	Drive Type	Drive Manufacturer	Drive Model	Drive Firmware Version	Drive Properties Updated	Drive Health Indicator	Drive WWNN	Drive Physical Address	Drive Libra Name
572004002083	T10000b	STK	T10000B	RP.48205-5.30	2012-04-30 13:11:21		50:01:04:F0:00:79:CB:50	1,2,1,1,3	evtlibrary
572001000214	T10000b	STK	T10000B	1.48.205-5.30	2012-03-30 14:35:43		50:01:04:F0:00:8A:BA:84	1,2,1,1,4	bas-sl8500
572004000099	T10000b-Enc	STK	T10000B	1.48.205-5.30	2012-03-28 18:01:31		50:01:04:F0:00:AC:A7:BC	1,1,1,1,6	sl3000
572001000315	T10000b-Enc	STK	T10000B	1.48.105-5.30	2012-04-06 18:01:39		50:01:04:F0:00:AC:A7:D7	1,1,-1,1,3	sl3000
572004000129	T10000b	STK	T10000B	1.48.105-5.30	2012-04-04 18:02:37		50:01:04:F0:00:8A:BA:BA	1,1,-2,1,4	bas-sl8500
572001000316	T10000b	STK	T10000B	1.48.105-5.30	2012-04-04 18:01:36		50:01:04:F0:00:AC:A7:89	1,1,2,1,2	sl3000
572001000201	T10000b	STK	T10000B	1.48.105-5.30	2012-04-06 18:04:52		50:01:04:F0:00:8A:BA:AB	1,2,-1,1,1	bas-sl8500

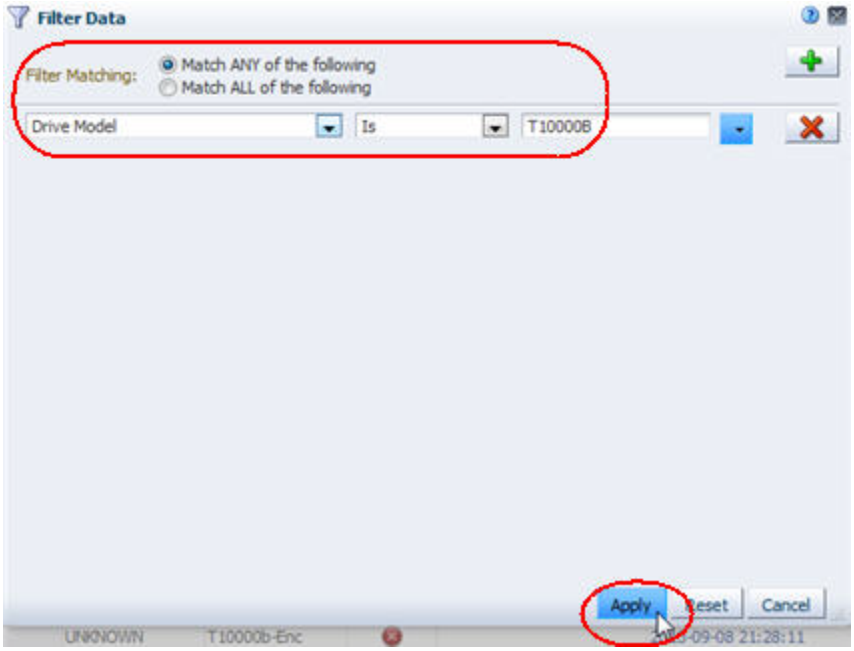
Using the Drives – Analysis Screen

This method provides totals by drive and firmware level, and aggregates the totals by library complex.

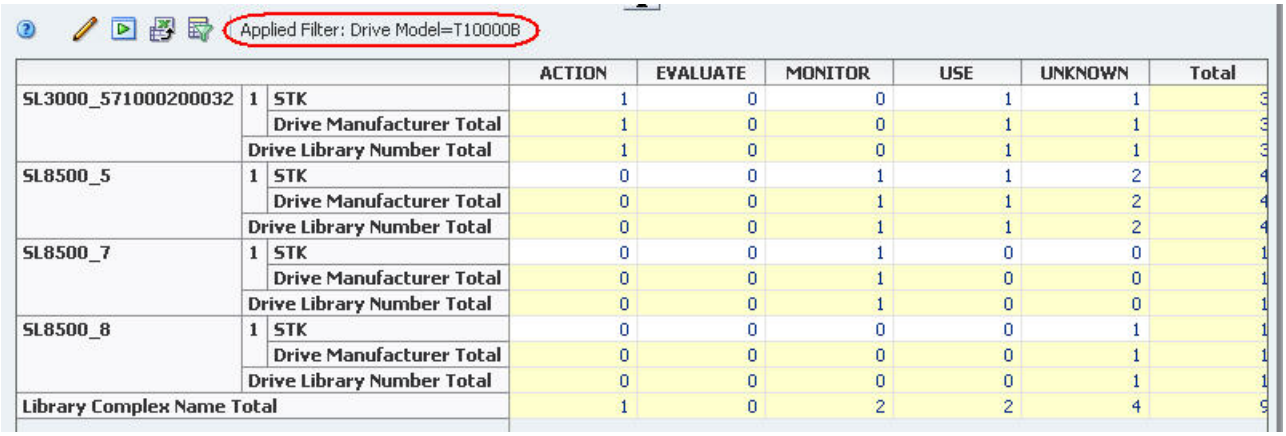
1. In the Navigation Bar, select **Tape System Hardware**, then select **Drives Analysis**.



2. Use the following steps to display firmware levels for a specific drive model.
   a. Click **Filter Data**.
   b. Specify the following selection criteria:
      * **Drive Model** is the drive model of interest.
   c. Click **Apply**.



The table is updated according to your selection criteria.



			ACTION	EVALUATE	MONITOR	USE	UNKNOWN	Total
SL3000_571000200032	1	STK	1	0	0	1	1	3
		Drive Manufacturer Total	1	0	0	1	1	3
		Drive Library Number Total	1	0	0	1	1	3
SL8500_5	1	STK	0	0	1	1	2	4
		Drive Manufacturer Total	0	0	1	1	2	4
		Drive Library Number Total	0	0	1	1	2	4
SL8500_7	1	STK	0	0	1	0	0	1
		Drive Manufacturer Total	0	0	1	0	0	1
		Drive Library Number Total	0	0	1	0	0	1
SL8500_8	1	STK	0	0	0	0	1	1
		Drive Manufacturer Total	0	0	0	0	1	1
		Drive Library Number Total	0	0	0	0	1	1
Library Complex Name Total			1	0	2	2	4	9

3. Use the following steps to reorganize the pivot table to aggregate firmware levels by drive model.

   a. Click the **Change Attribute** icon on the Pivot Table Toolbar.

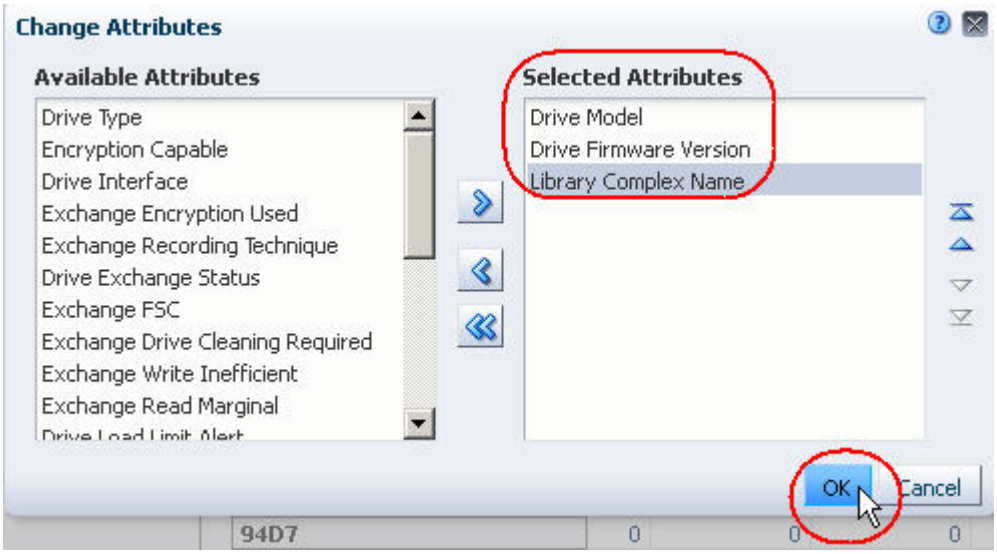
   b. In the Change Attributes dialog box, rearrange the attributes so the Selected Attributes list is as follows:

      * Drive Model
      * Drive Firmware Version
      * Library Complex Name

Note: The last attribute in the list — in this case, Library Complex Name — always designates the column headers. The remaining attributes designate the row layers, nested in the order listed — in this case, Drive Firmware Version within Drive Model.

---

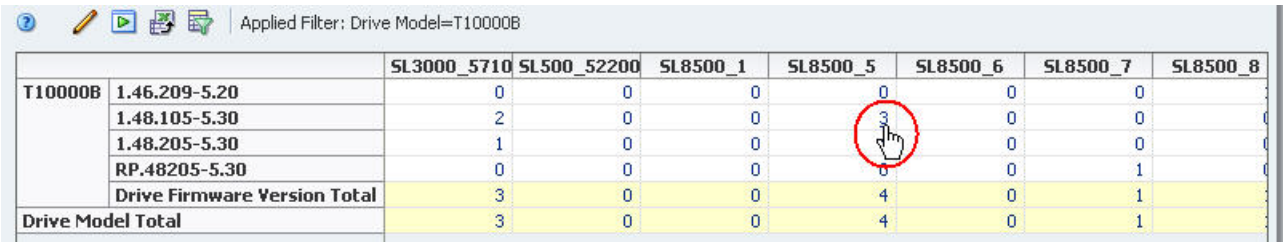
c. Click **OK**.



The pivot table is updated according to your criteria.

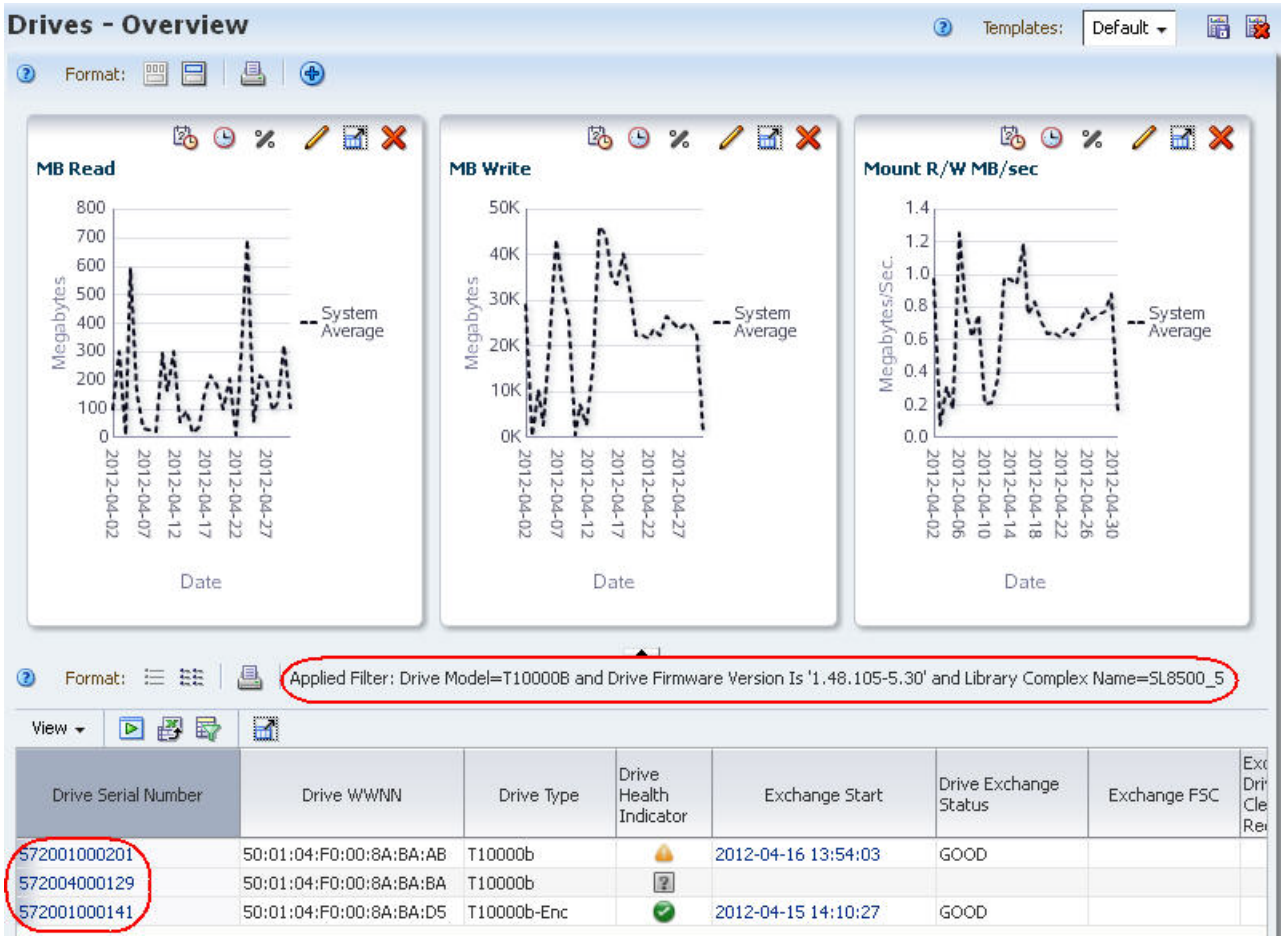
		SL3000_5710	SL500_52200	SL8500_1	SL8500_5	SL8500_6	SL8500_7	SL8500_8
T10000B	1.46.209-5.20	0	0	0	0	0	0	
	1.48.105-5.30	2	0	0	3	0	0	
	1.48.205-5.30	1	0	0	1	0	0	
	RP.48205-5.30	0	0	0	0	0	1	
	Drive Firmware Version Total	3	0	0	4	0	1	
Drive Model Total		3	0	0	4	0	1	

4. To display a detailed listing of any of the subtotals, click the text link in a cell.



		SL3000_5710	SL500_52200	SL8500_1	SL8500_5	SL8500_6	SL8500_7	SL8500_8
T10000B	1.46.209-5.20	0	0	0	0	0	0	
	1.48.105-5.30	2	0	0	3	0	0	
	1.48.205-5.30	1	0	0	1	0	0	
	RP.48205-5.30	0	0	0	0	0	1	
	Drive Firmware Version Total	3	0	0	4	0	1	
Drive Model Total		3	0	0	4	0	1	

You are taken to the Drives – Overview screen, which displays additional detail for the drives included in the selected subtotal.



Best Practices for Investigating Tape Environment Issues

This section provides tips for 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

See the *STA Data Reference Guide* for detailed tape alert descriptions.

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 ""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.

A

Dashboard Portlets

This section includes descriptions of the available Dashboard portlets.

- Graph Portlets
- Table Portlets
- Report Portlets

> **Note:** All data on Dashboard portlets is reported in UTC time. See "Times Displayed on the Dashboard" on page 2-3 for details.

Graph Portlets

Graph portlets include several formats. Bar and pie charts are point-in-time reports of related data. Line graphs and area charts show values over a selected date range. See the *STA Screen Basics Guide* for additional information about these graph formats.

Depending on when you display the Dashboard, the last time period on each graph may show a drop-off in data because it is just a partial period.

Alerts

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

> **Note:** 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.

> **Note:** 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.

Cum 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 portlet 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.

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

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.

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

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 portlet 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 portlet 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 portlet 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 portlet 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."

> **Note:** 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 Portlets

Some table portlets are point-in-time reports of related data. Others are trend reports, showing start and end, and high and low values over a selected date range. You can hover the cursor over a table cell to display a tooltip containing detailed values and dates.

Trend reports include embedded *spark charts*, which are small line graphs that plot up to four key values—Start, End, High, and Low—for a selected date range. See the *STA Screen Basics Guide* for details about 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 portlet displays values for dates within the last six months (180 days) only. If you filter for a date range extending past the previous six months, the portlet 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), SL3000 access expansion module (AEM), SL150 mailslot. This is as of the current point in time.

Media Validation

Summarizes media validation results by verification test type. By default, this portlet 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:

- Use – MV Result is Use
- 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. See "Media Validation Initiators" on page 8-22 for details.

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 Portlets

Report portlets 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 True. 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 Requirements 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. However, when filtered by STA Start Tracking Date (Days) or STA Start Tracking Date (No. Days), the report counts include the number of devices with STA Start Tracking dates that fall in the specified range of dates or number of days. For example, if you use the filter "STA Start Tracking Date Less Than 7 Days Ago," the report only counts devices that were added to the tape library environment during the last seven days; devices monitored for longer are not included.

B

STA Predefined Templates

This section includes short descriptions of the predefined templates for each Overview, Analysis, and Messages screen. STA predefined templates are always prefixed "STA–".

Home Tab

- "Dashboard Templates" on page B-2

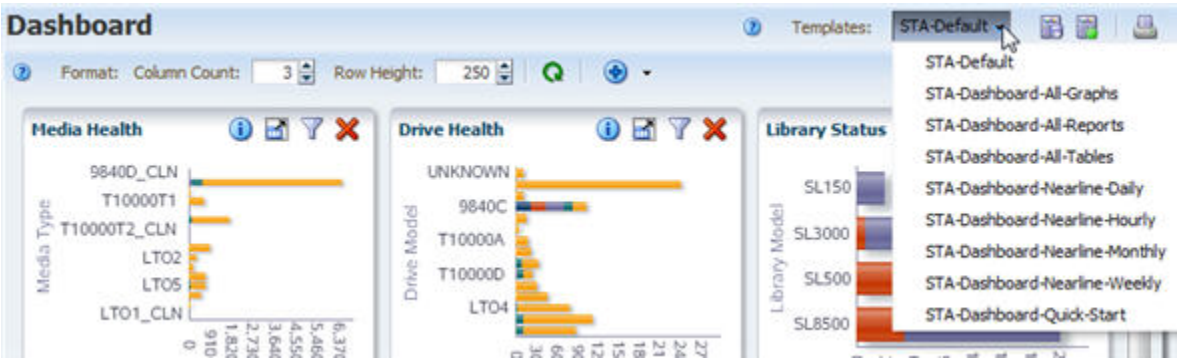
Tape System Hardware Tab

- "Complexes Overview Templates" on page B-3
- "Libraries – Overview Templates" on page B-4
- "Libraries – Messages Templates" on page B-4
- "Drives – Overview Templates" on page B-5
- "Drives – Analysis Templates" on page B-6
- "Drives – Messages Templates" on page B-6
- "Media – Overview Templates" on page B-6
- "Media – Analysis Templates" on page B-8
- "Media – Messages Templates" on page B-8
- "Robots Overview Templates" on page B-8
- "CAPs Overview Templates" on page B-8
- "PTPs Overview Templates" on page B-9
- "Elevators Overview Templates" on page B-9

Tape System Activity Tab

- "Alerts Overview Templates" on page B-9
- "Exchanges Overview Templates" on page B-10
- "Drive Cleanings Overview Templates" on page B-11
- "Media Validation Overview Templates" on page B-11
- "All Messages – Overview Templates" on page B-11
- "All Messages – Analysis Templates" on page B-12

Dashboard Templates



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 portlets in alphabetical order. This template is useful for selecting portlets to include in Dashboard templates and Executive Reports.

STA-Dashboard-All-Reports
Displays all available report portlets in alphabetical order. This template is useful for selecting portlets to include in Dashboard templates and Executive Reports.

STA-Dashboard-All-Tables
Displays all available table portlets in alphabetical order. This template is useful for selecting portlets 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 portlets summarize mount activity, I/O throughput, drive and media utilization, and drive and media slot availability.

Note: 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 portlets summarize mount activity, I/O throughput, drive and media utilization, and drive and media slot availability.

Note: 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 portlets summarize mount activity, I/O throughput, drive and media utilization, and drive and media slot availability.

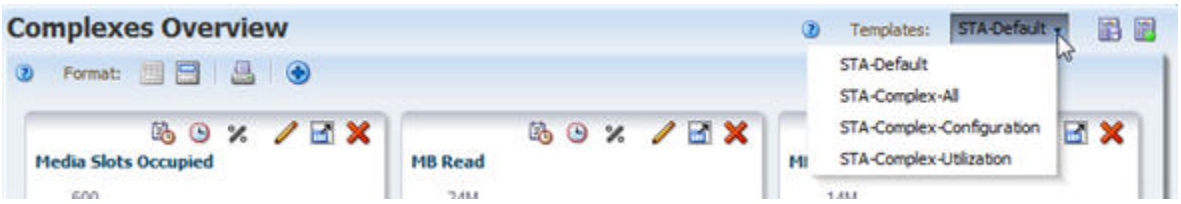
> **Note:** Data displayed in this template is updated at the end of each month. For bar charts, at least one full month's worth of data must have been collected by STA in order for data to be displayed. For line graphs, at least two data points are required, so at least two months' worth of data are 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 portlets summarize mount activity, I/O throughput, drive and media utilization, and drive and media slot availability.

> **Note:** 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 *STA Quick Start Guide*.

Complexes Overview Templates



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 Templates

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.

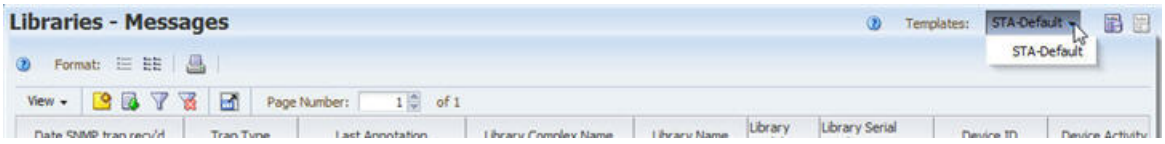
STA-Lib-Configuration
Displays information about the library physical and partition configuration. Also includes connection information useful for troubleshooting connection issues.

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 Templates



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 Templates

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-Enterprise-Performance
Displays summary performance data for enterprise drives only.

STA-Drive-Health
Displays current and summary health and activity information for all drives.

STA-Drive-Last-Exchange
Displays information for the last exchange that occurred on each drive.

STA-Drive-LTO-Performance
Displays performance data for LTO drives only.

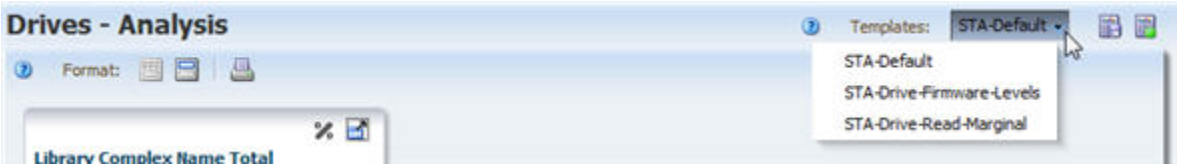
STA-Drive-LTO-Utilization
Displays utilization statistics for LTO drives only.

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-Utilization
Displays utilization statistics for all drives.

Drives – Analysis Templates

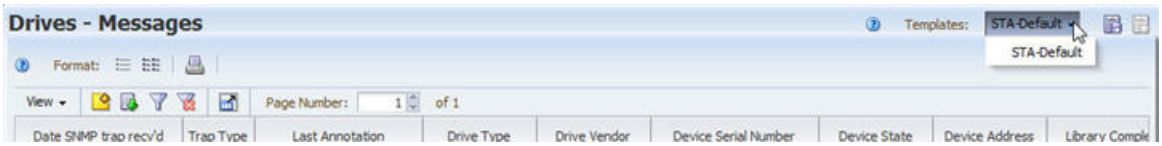


STA-Default
Summarizes current drive health by library complex.

STA-Drive-Firmware-Levels
Summarizes current drive firmware levels by drive type.

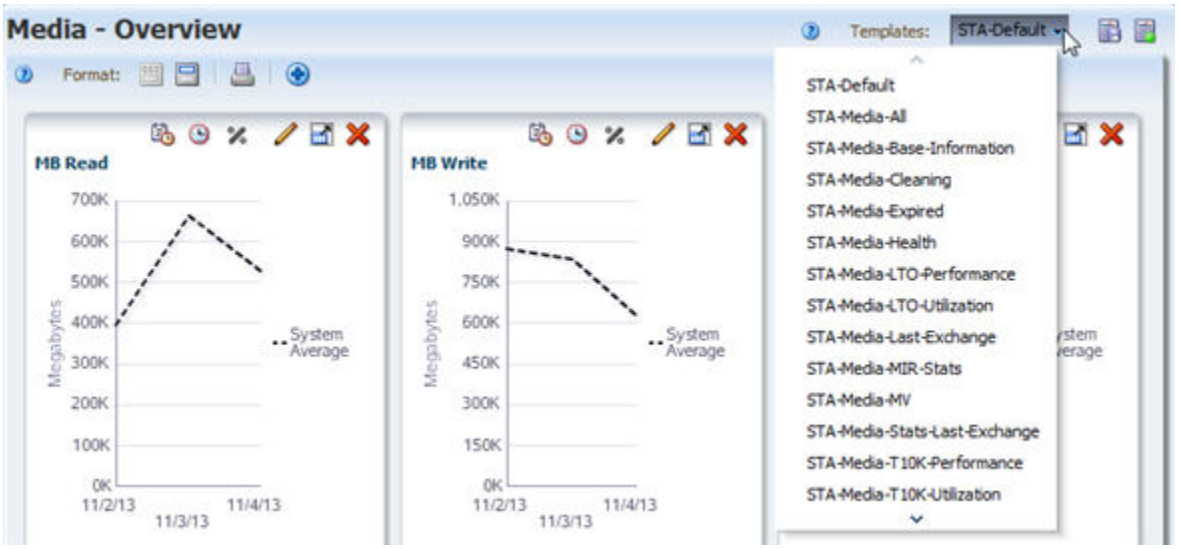
STA-Drive-Read-Marginal
Summarizes the "Exchange Read Marginal" status for applicable drives, by library complex name. Applicable to StorageTek T10000 drives only.

Drives – Messages Templates



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 Templates



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-Last-Exchange
Displays information about the last exchange for each piece of 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-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-T10K-Performance
Displays summary performance information for T10000 media only.

STA-Media-T10K-Utilization
Displays summary utilization information for T10000 media only.

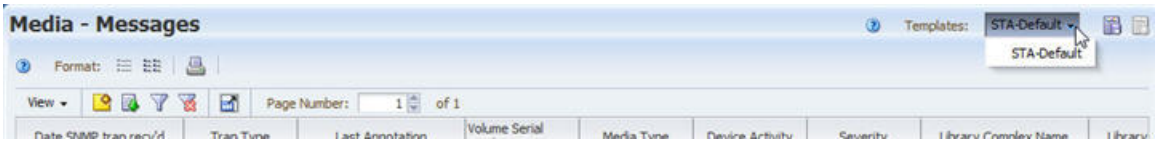
STA-Media-Utilization
Displays summary utilization information for all media.

Media – Analysis Templates

STA-Default
Summarizes current media health by library complex.

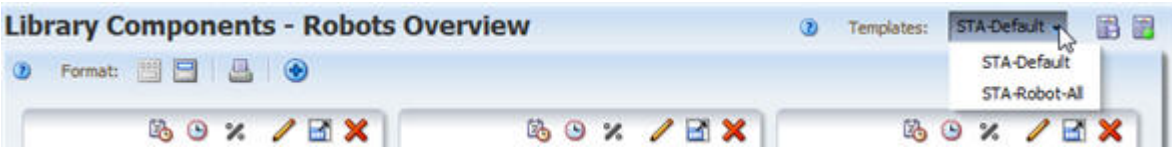
STA-Media-HealthByMediaType
Summarizes current media health by media type.

Media – Messages Templates



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.

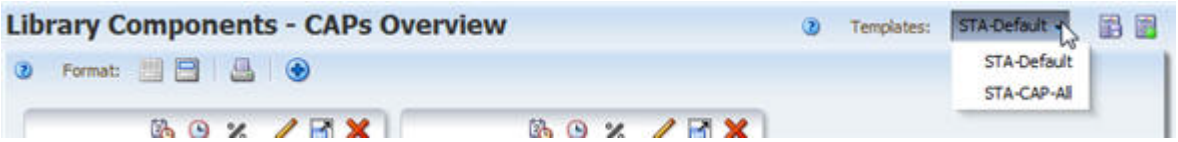
Robots Overview Templates



STA-Default
Displays properties and activities for all library robots.

STA-Robot-All
Displays all available data attributes for all library robots.

CAPs Overview Templates



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

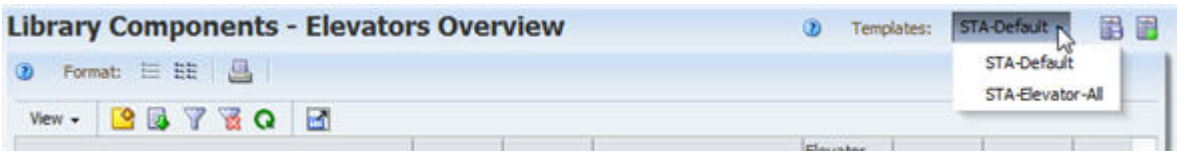
STA-CAP-All
Displays all available data attributes for all library CAPs, SL3000 AEMs, and SL150 mailslots.

PTPs Overview Templates

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.

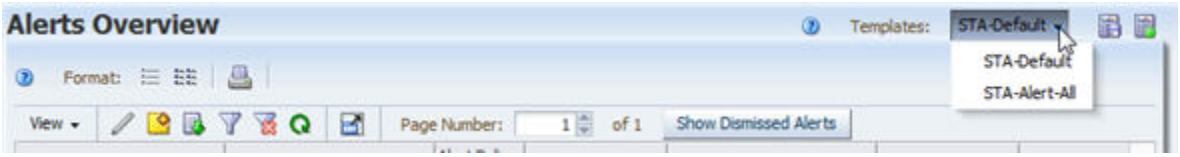
Elevators Overview Templates



STA-Default
Displays properties and activities for all SL8500 library elevators.

STA-Elevator-All
Displays all available data attributes for all SL8500 library elevators.

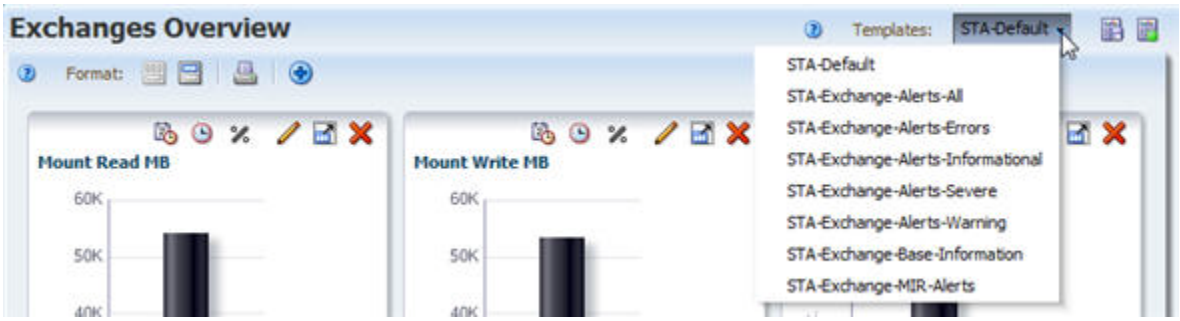
Alerts Overview Templates



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 Templates



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.

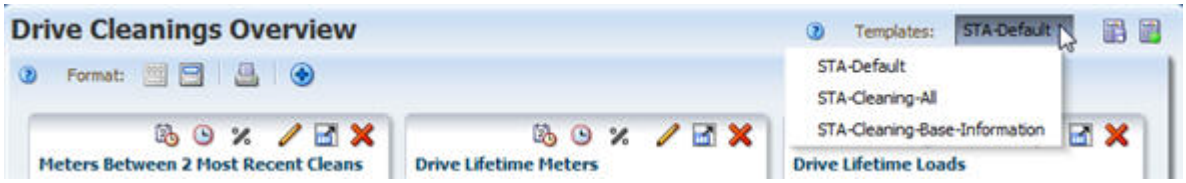
STA-Exchange-Alerts-Severe
Displays all exchanges that resulted in at least one severe tape alert. The displayed attributes provide detail about the types of errors that occurred. Severe tape alerts indicate an error on the exchange that may put your data at risk.

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 Templates

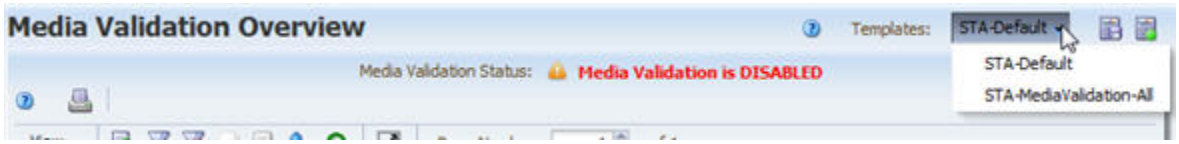


STA-Default
Displays identification and status information for the drive, media, and library involved in each cleaning exchange.

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.

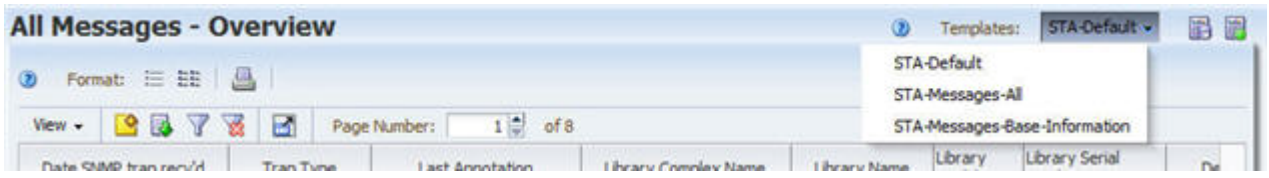
Media Validation Overview Templates



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 Templates



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 Templates

STA-Default
Summarizes STA message severity levels by library complex.

C

STA Dialog Box Reference

This section contains reference information for the following types of STA data entry dialog boxes.

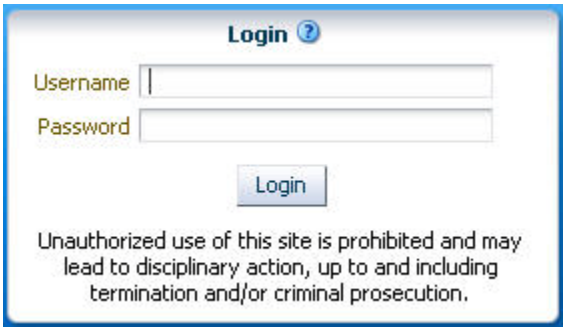
- Login Dialog Box
- Dashboard Dialog Box
- Filter Dialog Box
- Media Validation Overview Dialog Boxes
- Logical Groups Dialog Boxes
- Alerts Policies Dialog Boxes
- Executive Reports Policies Dialog Boxes
- Templates Management Dialog Boxes
- Media Validation Policy Wizard and Dialog Boxes
- Service Log Dialog Boxes
- SNMP Connections Dialog Boxes
- User Management Dialog Boxes
- Email Configuration Dialog Boxes

For descriptions of dialog boxes relating to user preferences and tables, see the *STA Screen Basics Guide*.

Login Dialog Box

- "Login" on page C-1

Login



Description

This dialog box appears when you enter the URL of the STA server in your browser. Your STA administrator will provide you with an STA username and password for logging in.

> **Note:** You have up to five chances to log in successfully. 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, so you must wait the full 30-minutes before attempting to log in again.

Screen Fields

Username

Required.

Enter the STA username you want to log in with.

Password

Required.

Enter the password assigned to the STA username.

Buttons

Login

Click to log in. Once your username and password are authenticated, you are taken to the Dashboard.

> **Note:** The Accessibility Settings dialog box may appear before the Dashboard.

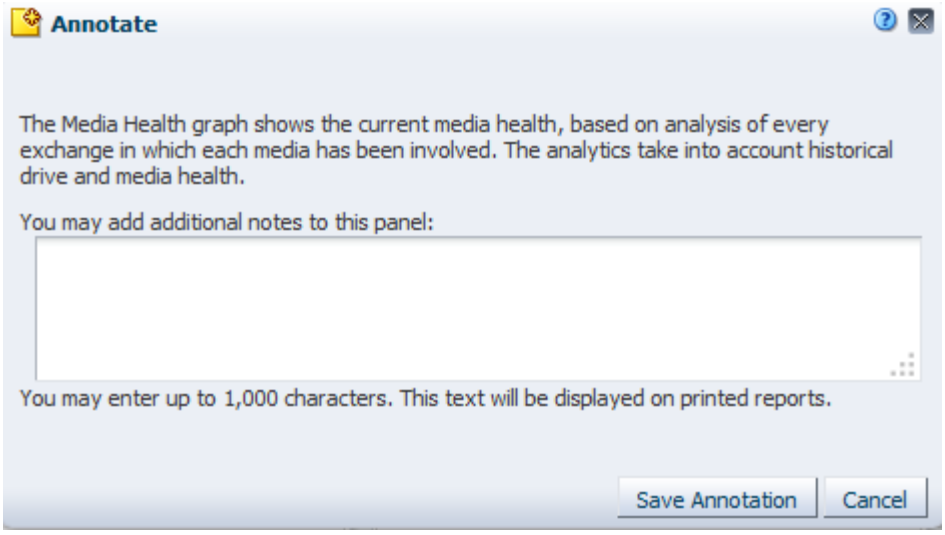
See Also

- "Log In to STA" on page 1-4

Dashboard Dialog Box

- "Annotate" on page C-3

Annotate



Description

This dialog box allows you to add or modify a Dashboard portlet annotation. It appears when you click **Portlet Information** on a Dashboard portlet.

Note: The text you enter is specific to the current Dashboard template. For example, if the Drive Health portlet appears in several Dashboard templates, each instance of the Drive Health portlet can have a different annotation associated with it.

Note: Annotation text is specific to your STA username. For example, annotations entered by one user on the Drive Health portlet do not appear to a user logged in with a different STA username.

Screen Fields

You may add additional notes to this panel:

Type the text you want to appear on Executive Reports.

Annotations can be up to 1,000 ASCII characters in length. There are no formatting options, such as boldface or color. Also, spacing options, such as forced line feeds, are not preserved on the Executive Reports.

Buttons

Save Annotation

Click to apply the annotation to the Dashboard portlet.

Cancel

Click to dismiss this dialog box without applying the annotation.

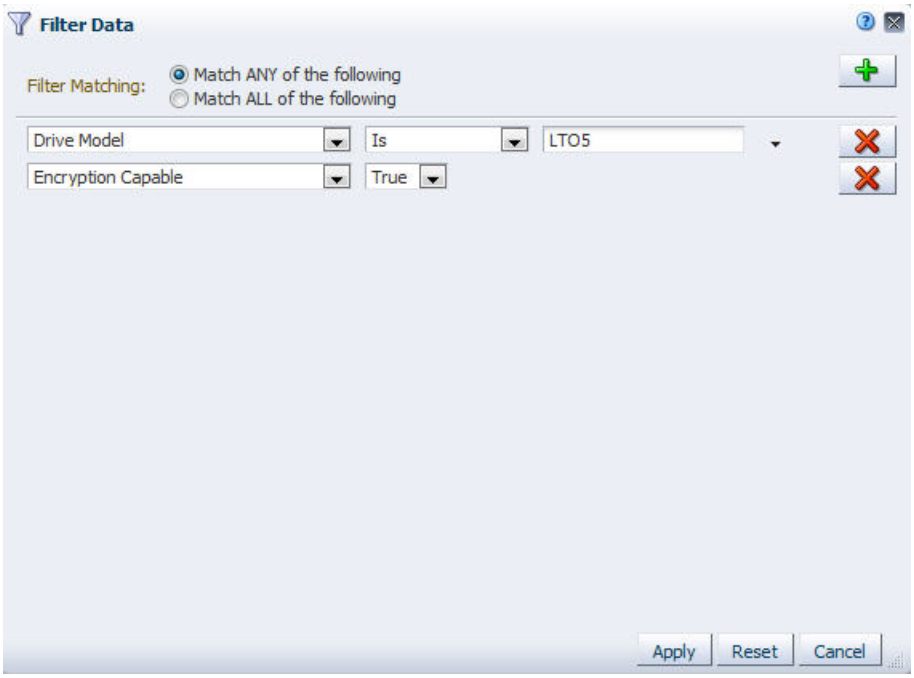
See Also

- "Add or Change a Dashboard Portlet Annotation" on page 2-17

Filter Dialog Box

- "Filter Data" on page C-4

Filter Data



Description

This dialog box allows you to specify the criteria you want to use to filter data in a List View or Pivot table. You can specify any number of criteria.

This dialog box appears when you click **Filter Data** on a table toolbar.

Screen Fields

Filter Matching

Indicate the type of matching you want to use for the filter. Options are:

- Match ANY of the following – Selects table 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.

Filter criteria list

Enter the filter criteria you want to apply to the table. You can add as many rows as you want. On each row, you specify the criteria through the following menu selections:

- Table attribute – All available attributes for the table are listed in the menu.

> **Note:** If you know the name of the attribute you want to select, you can type the first few letters to quickly move the cursor to that item in the menu.

- Filter operators – Filter operators vary by attribute type.
- Attribute value – Attribute values vary by attribute.

See "Filter Operators by Attribute Type" on page 4-3 for details about the menu selections.

Buttons

Add new filter criteria row
Click to add a new row to the list of filter criteria.

Remove this filter criteria row
Click to delete the current row of filter criteria.

Apply
Click to apply your entries. The table is updated to display only those records that meet the selection criteria you have specified.

Reset
Click to reset the dialog box to the default settings.

Cancel
Click to dismiss this dialog box without applying your entries.

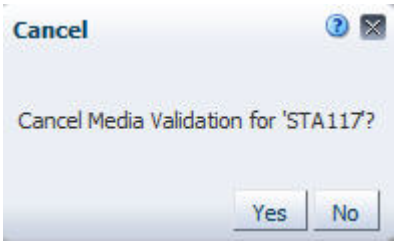
See Also

- "Use the Filter Data Dialog Box to Change a Table Filter" on page 4-9

Media Validation Overview Dialog Boxes

- "Cancel Requests" on page C-5
- "Resubmit Media" on page C-6
- "Reorder Pending Requests" on page C-7

Cancel Requests



Description

This dialog box allows you to cancel a selected media validation request. It appears when you select an in-progress or pending media validation request on the Media Validation Overview screen and then click **Cancel**.

Buttons

Yes
Click to cancel the selected media validation request.

No
Click to dismiss the dialog box without canceling the media validation request.

See Also
- "Cancel Pending Media Validation Requests" on page 8-49
- "Cancel In-Progress "Complete Verify" Validations" on page 8-51

Resubmit Media

Description
This dialog box allows you to resubmit a selected media validation request. It appears when you select a completed media validation request on the Media Validation Overview screen and then click **Resubmit Media**.

Screen Fields

Validation test to run
Select the media validation test you want to run. The menu lists all verification tests available on T10000C and T10000D drives.

Perform validations from beginning of tape
Appears only if you have selected Complete Verify or Complete Verify Plus. Select this option if you want all selected media to be validated from the beginning of tape (BOT).

Resume interrupted validations when possible, otherwise start at beginning
Appears only if you have selected Complete Verify or Complete Verify Plus. Select this option if you want the selected media to be validated from wherever the previous validations left off, if this can be determined from the media information record (MIR).

Drive
Select the validation drive you want to use. The menu displays all validation drives in the standalone library or library complex.

This option is available only if all media you have selected for validation are in the same standalone library or library complex. If this option is not available, STA automatically selects compatible drives to perform the validations.

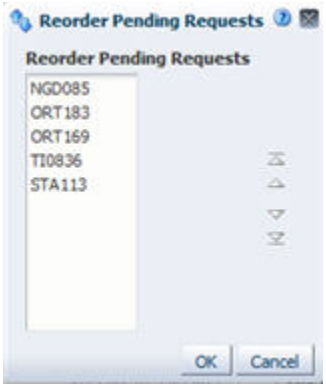
Buttons

OK
Click to submit the request.

Cancel
Click to dismiss the dialog box without submitting the request.

See Also
- "Submit Manual Media Validation Requests" on page 8-39

Reorder Pending Requests



Description
This dialog box allows you to reorder pending media validation requests. It appears when you click **Reorder Pending Requests** on the Media Validation Overview screen.

Screen Fields

Reorder Pending Requests
List of all pending media validation requests, in the order they are to be run. Select one or more requests you want to re-order. This field supports multi-select.

Buttons

Ordering arrows
These buttons are active only if you have selected one or more items in the Reorder Pending Requests list.

Arrows	Description
or	Move the selected item(s) up or down, one place at a time.
or	Move the selected item(s) to the top or bottom of the list.

OK
Click to apply your updates.

Cancel
Click to dismiss the dialog box without applying your updates.

See Also

- "Reorder Pending Media Validation Requests" on page 8-46

Logical Groups Dialog Boxes

- "Logical Groups" on page C-8
- "Create or Edit Logical Group" on page C-9
- "Delete Logical Group" on page C-11
- "Unassign Entities" on page C-11

Logical Groups

Description

This dialog box allows you to add drives or media to a manual logical group. It appears when you select one or more drives or media on the Drives – Overview or Media – Overview screen and then click **Logical Groups**.

Screen Fields

Adding to Logical Group menu

Select the logical group to which you want to add the selected drives or media.

Buttons

OK

Click to apply your entries.

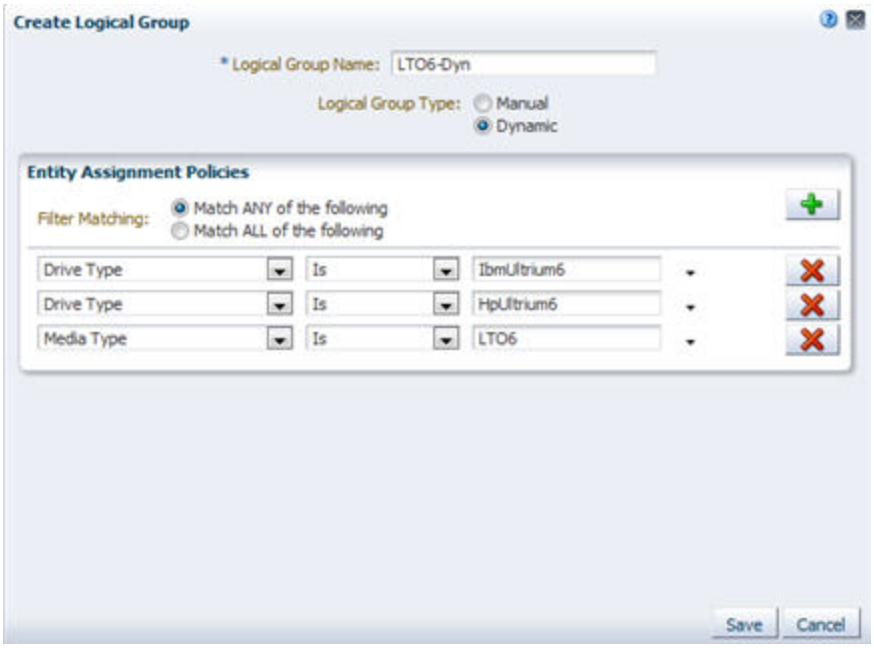
Cancel

Click to dismiss this dialog box without applying your entries.

See Also

- "Add Drives and Media to a Manual Logical Group" on page 7-13

Create or Edit Logical Group



Description

This dialog box allows you to create manual and dynamic logical groups. For dynamic groups, you use this dialog box to define the matching policy criteria for selecting drives and media for the group.

This dialog box appears when you click **Add Logical Group** or **Edit Logical Group** on the Logical Groups screen.

Screen Fields

Logical Group Name

User-assigned name for the logical group. Your entry can be up to 249 alphanumeric characters, and it must be unique.

Logical Group Type

Required field for the Create Logical Group dialog box. Display-only field for the Edit Logical Group dialog box.

Indicate the type of logical group. Options are:

- Dynamic – Drives and media are automatically selected for this group based on the selection criteria you define.
- Manual – Drives and media are selected for this group manually.

Filter Matching

> **Note:** This field appears only for dynamic logical groups.

Indicate the type of matching you want to use for the selection criteria. Options are:

- Match ANY of the following – Selects drives and media that meet any of the criteria you specify. This is the default.

- Match ALL of the following – Selects only drives and media that meet *all* the criteria you specify.

Selection criteria rows

> **Note:** These fields appear only for dynamic logical groups.

Enter the selection criteria you want to use for this group. You can add as many rows as you want. On each row, you specify the criteria through the following menu selections:

- Drive and media attributes – Selected drive and media attributes are listed in the menu. See "Dynamic Group Selection Criteria" on page 7-3 for the complete list.

> **Note:** If you know the name of the attribute you want to select, you can type the first few letters to quickly move the cursor to that item in the menu.

- Selection operators – Selection operators vary by attribute type. These are similar to the operators in the Filter Data dialog box. See "Filter Operators by Attribute Type" on page 4-3 for details.
- Attribute value – Attribute values vary by attribute.

Buttons

Add new filter criteria row

> **Note:** This button appears only for dynamic logical groups.

Click to add a new row to the list of selection criteria.

Remove this filter criteria row

> **Note:** This button appears only for dynamic logical groups.

Click to delete the associated selection criteria row.

Save

Click to save the logical group. If it is a dynamic group, STA begins building the group according to the specified selection criteria.

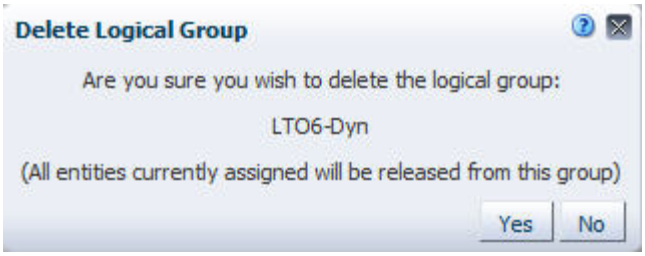
Cancel

Click to dismiss this dialog box without applying your entries.

See Also

- "Create a Manual Logical Group" on page 7-11
- "Create and Define a Dynamic Logical Group" on page 7-17

Delete Logical Group



Description

This dialog box allows you to confirm whether you want to delete the selected logical group. It appears when you when you select a logical group on the Logical Groups screen and then click **Delete**.

Buttons

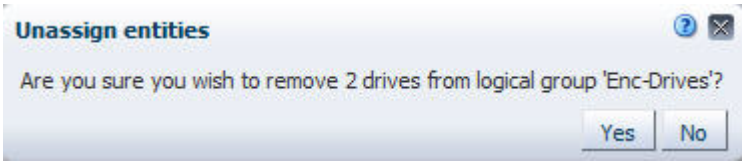
Yes
Click to delete the selected logical group.

No
Click to cancel the deletion and keep the selected logical group.

See Also

- "Delete a Logical Group" on page 7-27

Unassign Entities



Description

This dialog box allows you to confirm whether you want to remove the selected drives or media from the manual logical group. It appears when you select one or more records in the Drives or Media table on the Logical Groups screen and then click **Unassign Entities**.

Buttons

Yes
Click to remove the selected drives or media from the group.

No
Click to cancel the removal and keep the keep the selected drives or media in the group.

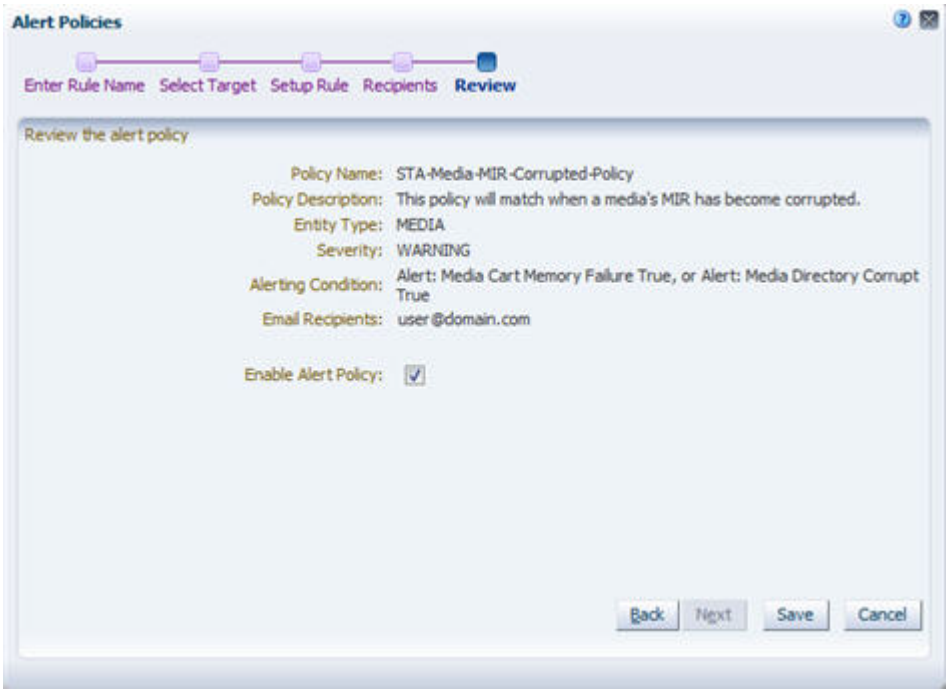
See Also

- "Remove Drives and Media From a Manual Logical Group" on page 7-15

Alerts Policies Dialog Boxes

- "Alert Policy Wizard" on page C-12

Alert Policy Wizard



Description

This wizard allows you to define and enable new alert policies. It also allows you to modify information for existing policies.

This wizard appears when you select **New Alert Policy** or **Edit Alert Policy** on the Alerts Policies screen.

Screen Fields

Policy Name

Policy Name

User-assigned name for the alert policy. Your entry can be up to 250 alphanumeric characters, and it must be unique.

Policy Description

Optional field. User-assigned description of the alert policy.

Policy Type

Entity Type

Select the type of library system component or event for which this policy may generate alerts.

Select Severity

Select the severity level of the alert policy. Options are:

- Severe – May generate alerts every hour
- Warning – May generate alerts every 24 hours
- Informative – May generate just one alert

Alert Criteria

Filter Matching

Indicate the type of matching you want to use for the alert policy criteria. Options are:

- Match ANY of the following – Triggers an alert when any of the criteria you specify are met. This is the default.
- Match ALL of the following – Triggers an alert only when *all* the criteria you specify are met.

Alert criteria rows

Enter the criteria you want to use for this alert policy. You can add as many rows as you want. On each row, you specify the criteria through the following menu selections:

- Attributes – The attributes vary according to the selected Entity Type.

> **Note:** If you know the name of the attribute you want to select, you can type the first few letters to quickly move the cursor to that item in the menu.

- Selection operators – Selection operators vary by attribute type. These are similar to the operators in the Filter Data dialog box. See "Filter Operators by Attribute Type" on page 4-3 for details.
- Attribute value – Attribute values vary by attribute.

Recipients

Email Recipients

Select the check box of each email address to receive emails whenever alerts are generated from this policy.

Review

Enable Alert Policy

Select the check box to create the policy and enable it immediately. De-select the check box to create the policy but leave it disabled for now; you can enable it at a later time.

Buttons

Breadcrumbs

Breadcrumbs are activated for wizard screens you have already visited and for the next immediate screen. Click a link to go directly to the selected screen.

Back

Click to go back to the previous screen in the wizard.

Next

Click to go to the next screen in the wizard.

Cancel
Click to exit the wizard without applying your entries.

Save

> **Note:** This button appears only on the last screen of the wizard.

Click to apply your entries and create or update the alert policy.

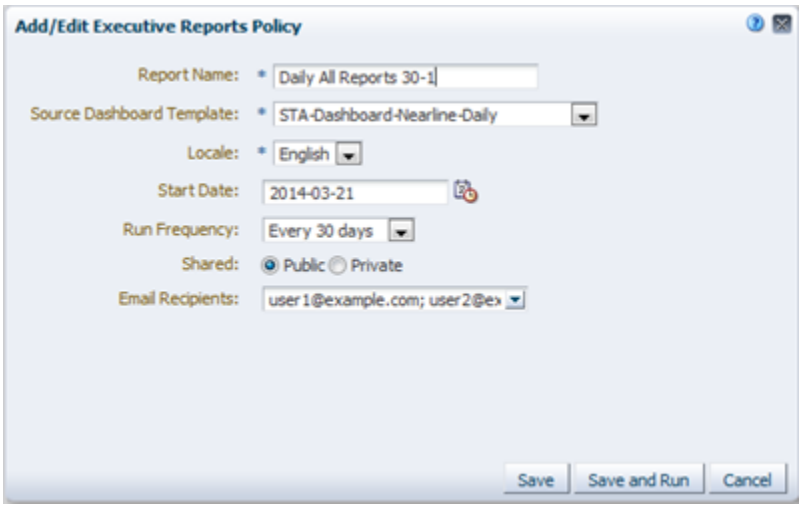
See Also

- "Create an Alert Policy" on page 5-12
- "Modify an Alert Policy" on page 5-19

Executive Reports Policies Dialog Boxes

- "Add/Edit Executive Reports Policy" on page C-14
- "Reports" on page C-16
- "Delete" on page C-16

Add/Edit Executive Reports Policy



Description

This dialog box allows you to define or modify an Executive Report definition, including name, source Dashboard template, run frequency, shared status, and email recipients.

This dialog box appears when you click **Add** or **Edit** on the Executive Reports Policies screen.

Screen Fields

Report Name
Type the name you want to assign to the report. Your entry can be up to 255 alphanumeric characters.

Source Dashboard Template
The menu lists all Dashboard templates that are available to the current STA username. Select the template you want to use as the basis of the Executive Report. The report will include all information in this template.

Locale
The menu lists all languages in which Executive Reports can be produced. Select English.

Start Date
Specify the date when you want scheduled runs of this report to begin. Reports are run shortly after 00:30 UTC, starting on this date. The default is tomorrow, in which case the report runs for the first time shortly after 00:30 UTC the day after it is defined.

Run Frequency
In the menu, select the frequency at which you want the report to run. Options are:

- Daily
- Every 7 days
- Every 30 days
- Every 90 days
- Every 365 days

Shared
This field allows you to specify whether this report can be shared with all STA users in the STA user interface. You must select one of the following options:

- Public – Report is available to all users.
- Private– Report is available to the current STA username only. This does not affect the email recipients list—copies of the report can be emailed to any addresses that have been defined to STA, as described below.

Email Recipients
Specify the email addresses to which you want copies of this report emailed after each report run. An email is sent to each address with a PDF attachment of the report.

The menu lists all email addresses that have been defined to STA. In the menu, select the check box next to each email address you want to receive this report. You can select as many addresses as you want. Select the "All" check box to select all check boxes in the list.

Buttons

Save
Click to apply your entries. The report will be run automatically at the first scheduled date. You can also run the report manually by selecting **Setup & Administration**, then **Executive Reports Policies**.

Save and Run
Click to apply your entries and run this report now. This does not affect the report's regular schedule.

Cancel
Click to dismiss this dialog box without applying your entries.

See Also

- "Create or Modify an Executive Report Policy" on page 6-11

Reports

Description

This dialog box allows you to confirm whether you want to run the selected Executive Report. The report is run at the first available opportunity, which could take up to two minutes.

This dialog box appears when you click **Run** on the Executive Reports Policies screen.

Buttons

OK

Click to run the report.

Cancel

Click to dismiss the dialog box without running the report.

See Also

- "Run an Executive Report On Demand" on page 6-7

Delete

Description

This dialog box allows you to confirm whether you want to delete the selected Executive Report definition.

This dialog box appears when you click **Delete** on the Executive Reports Policies screen.

Buttons

Yes
Click to delete the selected Executive Report definition. This does not affect copies of this report that have already been run; they can still be viewed by selecting **Home**, then **Executive Reports**.

No
Click to cancel the deletion and keep the selected Executive Report definition.

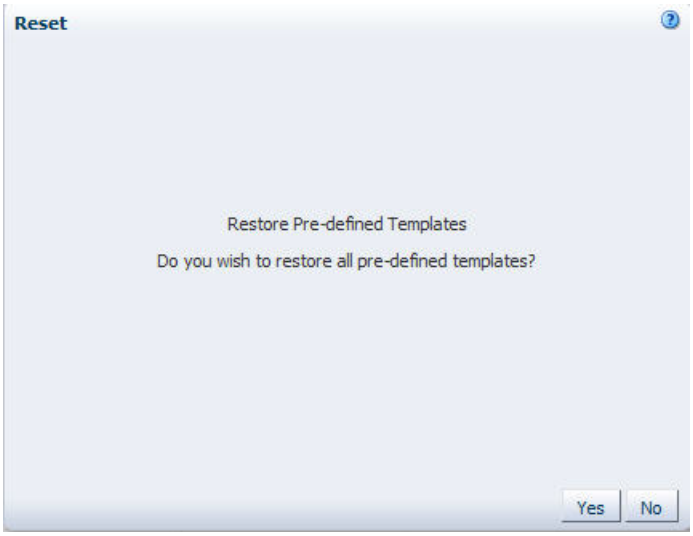
See Also

- "Delete an Executive Report Policy" on page 6-14

Templates Management Dialog Boxes

- "Reset (Templates)" on page C-17
- "Import Template" on page C-18
- "Rename Template" on page C-19
- "Delete Template" on page C-20
- "Save Template" on page C-21
- "Save Template (Overwrite)" on page C-22
- "Default Template" on page C-22

Reset (Templates)



Description

This dialog box allows you to restore all STA predefined templates that have been deleted. The templates will be restored and made available to all users.

This dialog box appears when you click **Restore Predefined Templates** on the Templates Management screen.

Screen Fields

None

Buttons

Yes

Click to restore all STA predefined templates.

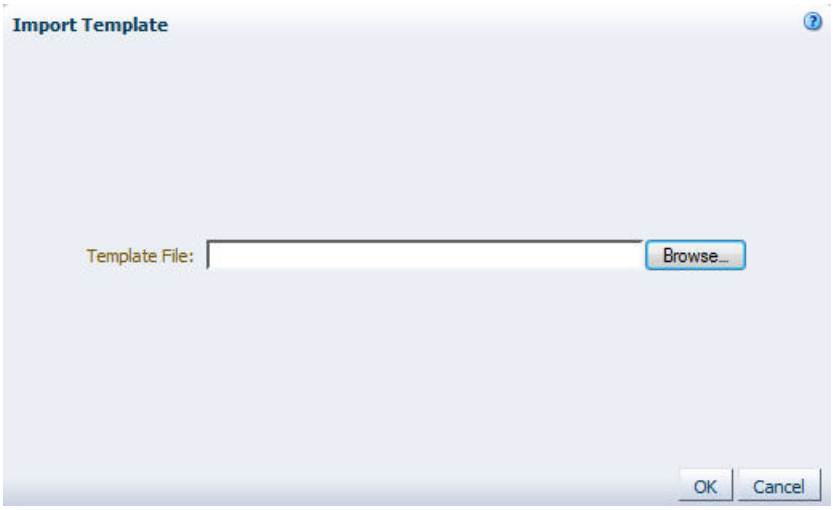
No

Click to dismiss this dialog box without restoring the templates.

See Also

- "Restore the STA Predefined Templates" on page 3-22

Import Template



Description

This dialog box allows you to import a template from your local computer so it is available to your STA username.

Screen Fields

Template File

Click **Browse** and navigate to the location of the template file you want to import. The file must have a .xml extension.

Buttons

OK

Click to import the specified template.

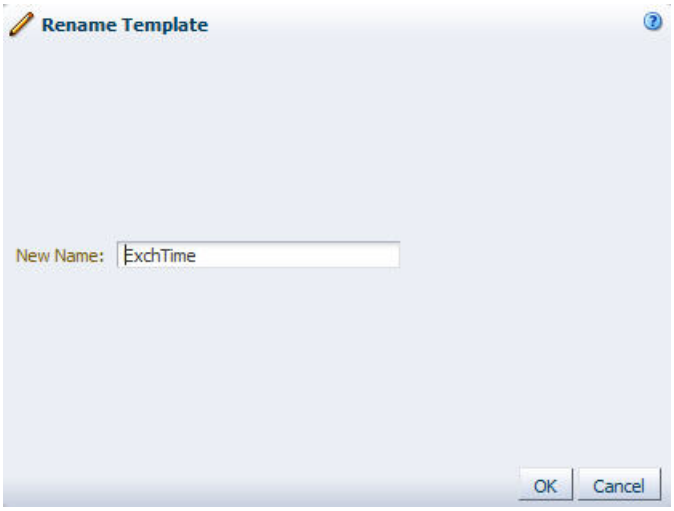
Cancel

Click to dismiss the dialog box without importing the template.

See Also

- "Import a Template" on page 3-19

Rename Template



Description

This dialog box allows you to rename a custom template.

Screen Fields

New Name

Type the name you want to assign. Your entry can be up to 255 alphanumeric characters, and it must be unique.

Buttons

OK

Click to apply your changes.

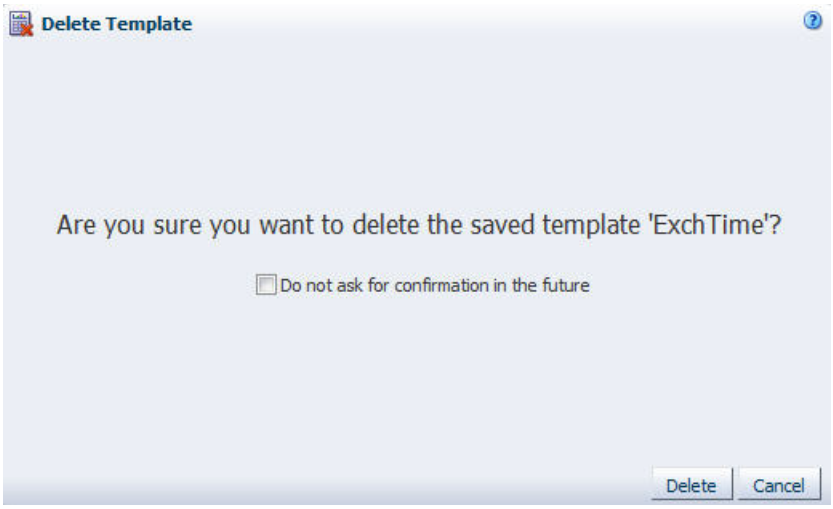
Cancel

Click to dismiss the dialog box without applying your changes.

See Also

- "Rename a Template" on page 3-18

Delete Template



Description

This dialog box allows you to confirm the deletion of a template. It appears when you click **Delete** on the Templates Management screen and your Confirmation preferences indicate you want to be prompted before deleting a template.

Screen Fields

Do not ask for confirmation in the future

Select this check box to suppress this dialog box for future template deletions.

You can restore the dialog box at any time; see the *STA Screen Basics Guide* for instructions.

Buttons

Delete

Click to delete the template.

Cancel

Click to dismiss the dialog box without deleting the template.

See Also

- "Delete a Template" on page 3-21

Save Template

Description

This dialog box allows you to save the current screen settings as a template. It appears when you click **Save Template** on the Templates Toolbar.

Screen Fields

Template Name

User-defined name for this template. Your entry can be up to 255 alphanumeric characters in length.

If you type a new name, a new template is created. If you type a name that already exists, the specified template is overwritten with any changes you have made to the screen. Depending on your Confirmation preferences, you may be prompted for a confirmation before overwriting an existing template.

Shared

Indicate whether you want the template to be visible to other STAusernames. Options are:

- Private – The template is available to the current STAusername only.
- Public – The template is available to all STAusernames.

Buttons

Yes

Click to save the template.

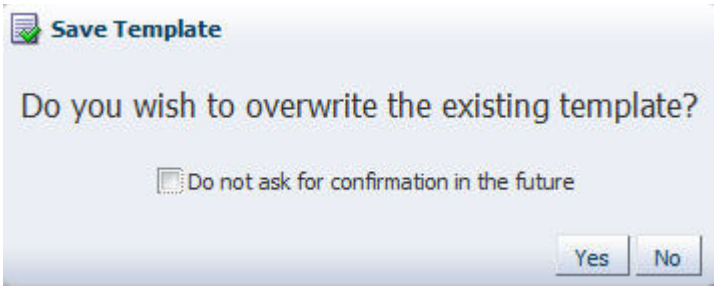
No

Click to dismiss the dialog box without saving the template.

See Also

- "Create a Template" on page 3-13

Save Template (Overwrite)



Description

This dialog box allows you to confirm modifications to an existing template. It appears when you are about to overwrite an existing template and your Confirmation preferences indicate you want to be prompted before doing so.

Screen Fields

Do not ask for confirmation in the future

Select this check box to suppress this dialog box for future template modifications.

You can restore the dialog box at any time; see the *STA Screen Basics Guide* for instructions.

Buttons

Yes

Click to overwrite the template to match the current layout.

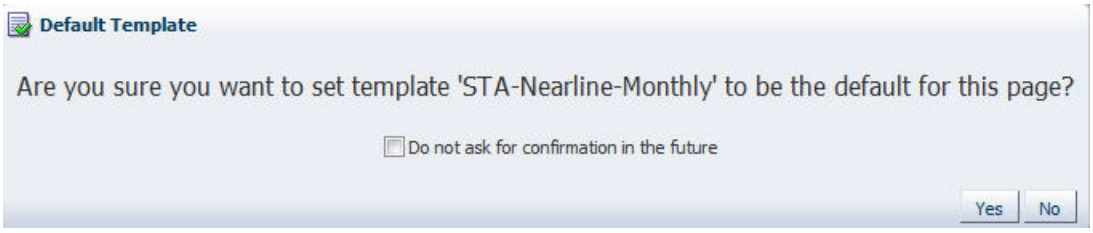
No

Click to dismiss the dialog box without overwriting the template.

See Also

- "Modify a Template" on page 3-15

Default Template



Description

This dialog box allows you to confirm the currently applied template as the default for this screen. It appears when you click **Default Template** in the Templates toolbar on any screen and your Confirmation preferences indicate you want to be prompted before setting a new default.

Screen Fields

Do not ask for confirmation in the future
Select this check box to suppress this dialog box when you set a default template in the future.

You can restore the dialog box at any time; see the *STA Screen Basics Guide* for instructions.

Buttons

Yes
Click to set this template as the default.

No
Click to dismiss the dialog box without setting the default template.

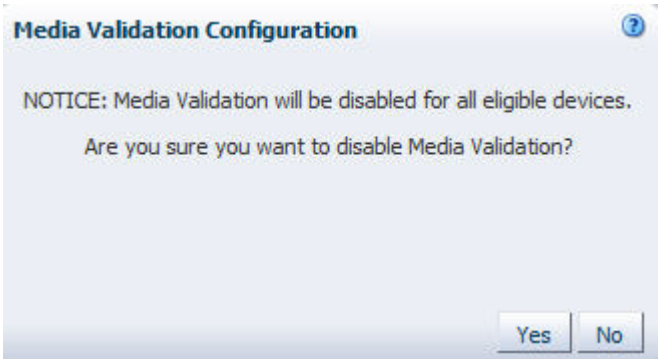
See Also

- "Set the Default Template for a Screen" on page 3-11

Media Validation Policy Wizard and Dialog Boxes

- "Media Validation Configuration Confirmation" on page C-23
- "Media Validation Policy Wizard" on page C-24

Media Validation Configuration Confirmation



Description

This dialog box allows you to confirm whether you want to enable or disable the media validation feature on STA. This is a global setting and affects media validation operations for your entire tape library system.

This dialog box appears when you select the **Enabled** or **Disabled** radio buttons in the Media Validation State field on the Media Validation Configuration screen.

Buttons

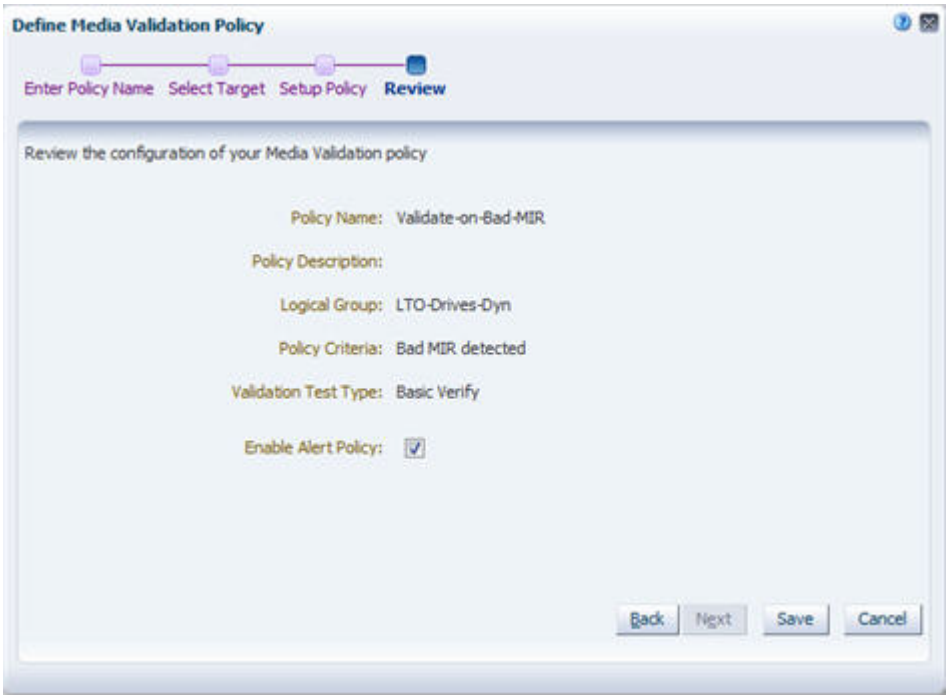
Yes
Click to confirm you r selection.

Cancel
Click to dismiss this dialog box without applying your selection.

See Also

- "Enable or Disable Media Validation on STA" on page 8-30

Media Validation Policy Wizard



Description

This wizard allows you to define and enable new media validation policies. It also allows you to modify information for existing policies.

This wizard appears when you click **New Media Validation Policy**, **Edit Media Validation Policy**, or **Copy Media Validation Policy** on the Media Validation Policies toolbar.

Screen Fields

Enter Policy Name

Policy Name

User-assigned name for the media validation policy. Your entry can be up to 250 alphanumeric characters, and it must be unique.

Policy Description

Optional field. User-assigned description of the media validation policy.

Select Target

Select media type and optional library complex

Click this button to indicate you want to have media selected for validation based on media type and optional library complex.

Media Type

Select the type of media.

Library Complex (Optional)
Select the library complex.

Select logical group
Click this button to indicate you want to have media selected for validation based on a defined logical group.

Logical Group
Select the logical group.

Set Up Policy

Policy Criteria
Select the criteria for selecting media within the group you have specified on the previous screen. Options are:

- Random selection – This is the default.
- Media Health = Action
- Media Health = Evaluate
- Media Health = Monitor
- Extended period of non-use
- Newly entered
- Bad MIR detected

Validation Test Type
Select the type of validation to be performed by this policy. Options are:

- Basic Verify
- Standard Verify
- Complete Verify
- Complete Verify Plus
- Verify Rebuild MIR

Review

Enable Policy
Select the check box to create the policy and enable it immediately. De-select the check box to create the policy but leave it disabled for now; you can enable it at a later time.

Buttons

Breadcrumbs
Breadcrumbs are activated for wizard screens you have already visited and for the next immediate screen. Click a link to go directly to the selected screen.

Back
Click to go back to the previous screen in the wizard.

Next
Click to go to the next screen in the wizard.

Cancel
Click to exit the wizard without applying your entries.

Save

Note: This button appears only on the last screen of the wizard.

Click to apply your entries and create or update the alert policy.

See Also
- "Create a Media Validation Policy" on page 8-53
- "Modify a Media Validation Policy" on page 8-62

Service Log Dialog Boxes

- Section , "Create New Log Bundle"
- Section , "Log Bundle Run Info"
- Section , "Delete Selected Log Bundle"

Create New Log Bundle

Description
This dialog box allows you to assign a name to a new RDA (Remote Diagnostic Agent) log bundle.

This dialog box appears when you click **Create New Log Bundle** on the Logs Toolbar.

Screen Fields

Log Bundle Name
Enter a name. Log name requirements are:

- Maximum of 210 characters
- Can only contain alphanumeric characters and underscores, but cannot contain four or more consecutive underscores.
- Spaces are replaced with underscores.

- Cannot begin with the following uppercase characters:

  COM
  LPT
  PRN
  CON
  AUX
  NUL

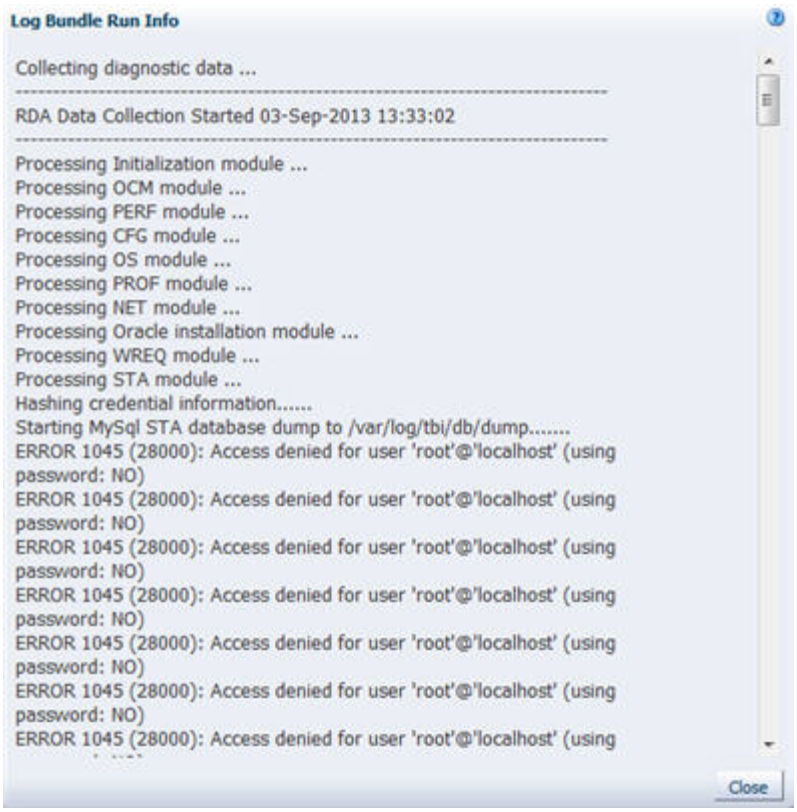
Buttons

Save
Click to apply your entries.

Cancel
Click to dismiss this dialog box without applying your entries.

See Also
- "Create a Service Log Bundle From the STA User Interface" on page 10-3

Log Bundle Run Info



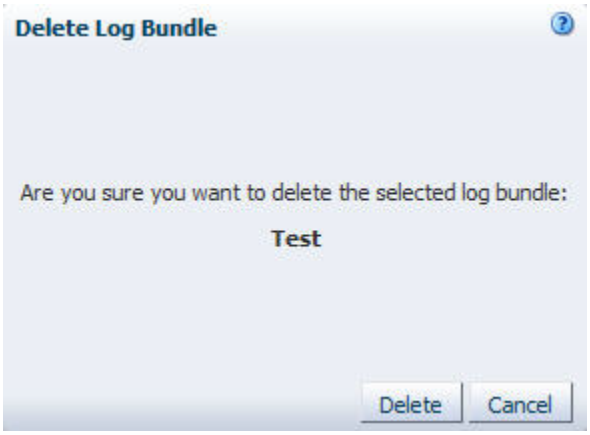
Description
This dialog box displays detailed information from the latest log bundle creation run. It appears when you select a log bundle on the Service – Logs screen and click **Log Bundle Run Info**. This is a display-only dialog box.

Buttons

Close
Click to dismiss the dialog box.

See Also
- "Display Log Run Information" on page 10-5

Delete Selected Log Bundle



Description
This dialog box allows you to confirm whether you want to delete the selected log bundle. It appears when you when you select a bundle on the Service – Logs screen and then click **Delete**. The name of the selected bundle is displayed in the dialog box.

Buttons

Delete
Click to delete the log bundle.

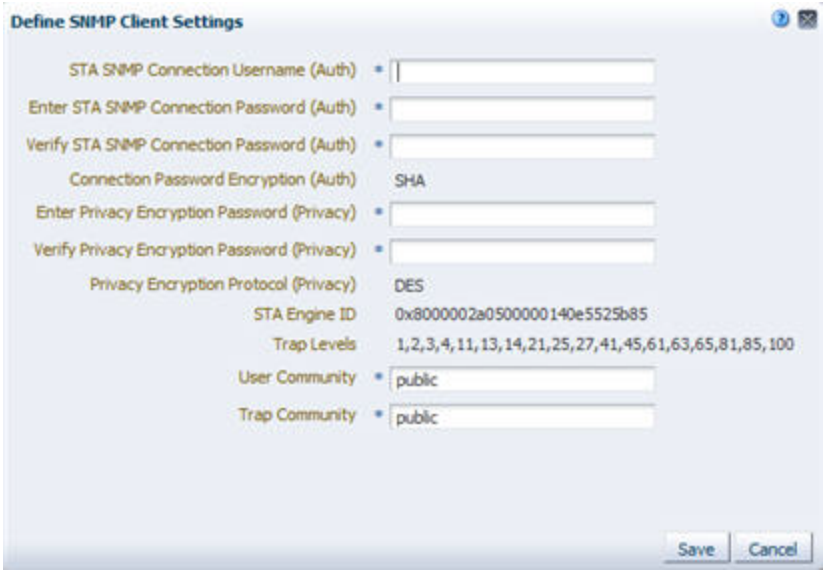
Cancel
Click to dismiss the dialog box without deleting the log bundle.

See Also
- "Delete a Log Bundle" on page 10-7

SNMP Connections Dialog Boxes

- "Define SNMP Client Settings" on page C-29
- "Define Library Connection Details" on page C-31
- "Confirmation (Delete Library Connection)" on page C-33

Define SNMP Client Settings



Description

This dialog box allows you to define SNMP connection settings for STA so it can receive SNMP data from one or more libraries. You must define settings for both the SNMP v3 and SNMP v2c protocols. The appropriate settings (SNMP v3 or SNMP v2c) will be used with each monitored library, depending on library firmware level and which SNMP protocol the library is configured to use.

You must define all of the following settings:

- For SNMP v3 connections:
  - User name
  - Connection authorization password
  - Privacy password
- For SNMP v2c connections:
  - User community name
  - Trap recipient name

This dialog box appears when you click **Edit** on the SNMP Client Attributes Toolbar.

Screen Fields

> **Note:** The following fields define the SNMP v3 connection settings for STA, and all are required. If all monitored libraries use SNMP v2c for STA communications, these entries will be ignored and you can enter any values.

STA SNMP Connection Username (Auth)
Required.

Enter the name of the STA SNMP v3 user. This user must also be defined on all monitored libraries that use the SNMP v3 protocol for STA communications.

Enter STA SNMP Connection Password (Auth)
Required.

Enter the connection authorization password for the SNMP v3 user. This password must also be defined on all monitored libraries that use the SNMP v3 protocol for STA communications.

Verify STA SNMP Connection Password (Auth)
Required.

Re-type the connection password to ensure that you have entered it correctly. An error message will be displayed if the two passwords do not match.

Connection Password Encryption (Auth)
Display only.

Encryption technique for storing the connection password. This is always SHA (Secure Hash Algorithm).

Enter Privacy Encryption Password (Privacy)
Required.

Enter the privacy encryption password for the SNMP v3 user. This password must also be defined on all monitored libraries that use the SNMP v3 protocol for STA communications.

Verify Privacy Encryption Password (Privacy)
Required.

Re-type the privacy password to ensure that you have entered it correctly. An error message will be displayed if the two passwords do not match.

Privacy Encryption Protocol (Privacy)
Display only.

Encryption technique for the SNMP privacy mechanism. This is always DES (Data Encryption Standard).

STA Engine ID
Display only.

Globally unique SNMP engine ID for the STA server. This is assigned by STA and is distinct from the library engine ID provided by each library. Both are required to ensure secure communication.

Trap Levels
Display only.

List of all the SNMP traps that STA can process. This does not necessarily mean that these traps have been configured on the monitored libraries; you must verify this on each library.

Note: The following fields define the SNMP v2c connection settings for STA, and both are required.

User Community
Required.

Enter the name of the STA SNMP v2c user. This user must also be defined on all monitored libraries that use the SNMP v2 protocol for STA communications. The default is public.

> **Note:** If all monitored libraries use SNMP v3 for STA communications, this entry will be ignored and you should leave the value set to public.

Trap Community

Required.

Enter the name of the STA SNMP v2c trap recipient. This trap recipient must also be defined on all monitored libraries that use the SNMP v2 protocol for sending traps to STA. The default is public.

> **Note:** If all monitored libraries use SNMP v3 for sending STA traps, this entry will be ignored and you should leave the value set to public.

Buttons

Save

Click to apply your entries.

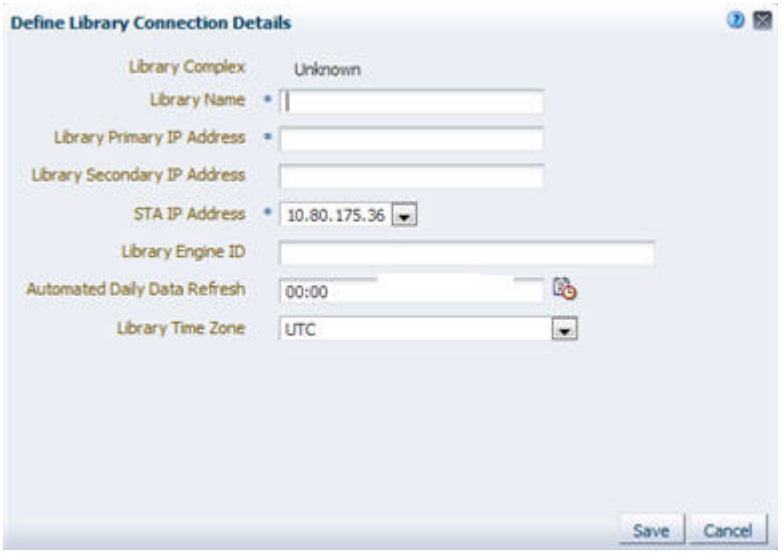
Cancel

Click to dismiss this dialog box without applying your entries.

See Also

- "Configure SNMP Client Settings for STA" on page 11-9

Define Library Connection Details



Description

This dialog box allows you to define connection details for a library that you want to connect to STA.

This dialog box appears when you click **Add** or **Edit** on the SNMP Monitored Libraries Toolbar.

Screen Fields

Library Complex
Display only.

Library complex ID. This ID is automatically generated by STA when you successfully retrieve the latest library configuration data.

Library Name
Required.

Enter the name you want to assign to the library. This name will be used to identify the library throughout the STA screens. You may want to use the library host name.

Library Primary IP Address
Required.

Enter the IP address of the public port on the library. For SL150 libraries, this is the Network Port 1 port; for SL500 libraries, it is the 1B port; for SL3000 and SL8500 libraries, it is the 2B port.

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

Library Secondary IP Address
This field does not apply to SL150 and SL500 libraries and should be left blank.

For SL3000 and SL8500 libraries, your entry in this field depends on the specific configuration of the library. 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.

- For libraries with the Redundant Electronics feature, enter the IP address of the 2B port on the alternate (standby) controller card
- For libraries with the Dual TCP/IP feature, enter the IP address of the 2A port on the active controller card.
- For libraries with both features, you can choose which IP address to enter, depending on which feature you want STA to support without interruption.
- For libraries with neither of these features, leave this field blank.

STA IP Address
Required.

The menu lists all available IP addresses for the STA server. Select the IPv4 address the library should use to send SNMP data to the server. If there is more than one listed and you are not sure which one to use, see your STA administrator for assistance.

Library Engine ID
Unique SNMP engine ID of the library automatically provided by the library whenever a library data collection is performed.

Under normal circumstances, you should not modify this field. However, if you have reason to believe the library engine ID has changed (due to a firmware upgrade, for

example), you should blank out this field and STA will detect the new engine ID during the next **Check/Test Connection** or **Get Latest Data** operation. This is the only time you should modify this field.

Automated Daily Data Refresh

Enter the time of day when you want STA to collect the latest configuration data from the library. The data will be collected automatically every 24 hours at this time, local to the time zone you specify in the Time Zone field.

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

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

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

Library Time Zone

In the menu, select the library's local time zone.

Buttons

Save

Click to apply your entries.

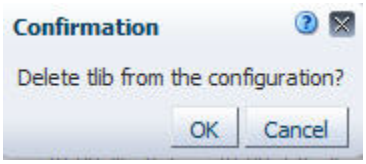
Cancel

Click to dismiss this dialog box without applying your entries.

See Also

- "Configure the SNMP Connection to a Library" on page 11-11

Confirmation (Delete Library Connection)



Description

This dialog box allows you to confirm whether you want to delete the selected library connection. It appears when you when you select a monitored library on the Configuration – SNMP Connections screen and then click **Delete**.

Buttons

OK

Click to delete the selected library connection.

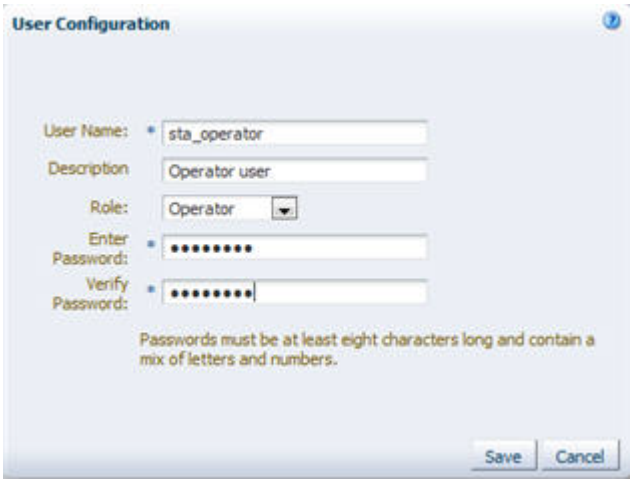
Cancel
Click to cancel the deletion and keep the library connection.

See Also
- "Remove a Library Connection From STA" on page 11-17

User Management Dialog Boxes

- "User Configuration" on page C-34
- "Delete User" on page C-35

User Configuration



Description
This dialog box allows you to create or modify an STA username.It appears when you click **Create New User** or **Modify User** on the Configuration – Users screen.

Screen Fields

User Name

> **Note:** This field is active only for **Create New User**.

Type the name you want to assign to this STA user.

STA username requirements are as follows:

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

Description
Type a brief description of the STA username.

Role
Select the role you want to assign to this STA username. Options are:

- **Viewer** – Can access all Home, Tape System Hardware, and Tape System Activity screens.
- **Operator** – Has all privileges of the Viewer role. Also has editing privileges for some Setup & Administration screens and view-only privileges on Configuration screens.
- **Administrator** – Has all privileges of the Operator role, plus has full editing privileges for all Setup & Administration screens.

Enter Password
Type the password to want to assign to the user. The entry is masked as you type. See "Username and Password Requirements" on page 1-2 for detailed requirements.

Verify Password
Type the password again to verify that you have entered it correctly.

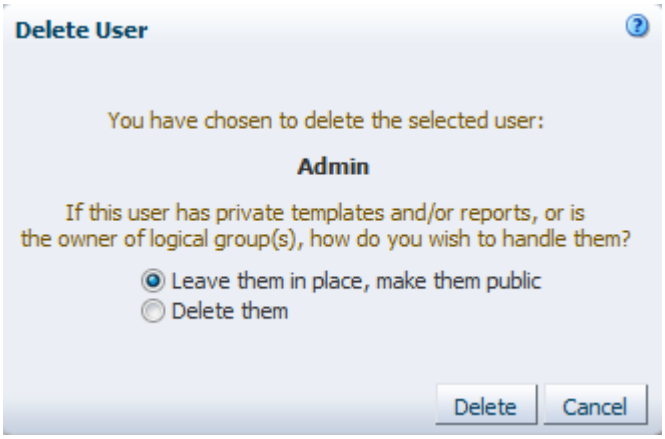
Buttons

Save
Click to apply your entries.

Cancel
Click to dismiss this dialog box without applying your entries.

See Also
- "Add an STA Username" on page 9-5

Delete User



Description
This dialog box allows you to confirm whether you want to delete the selected user. It appears when you select an STA username on the Configuration – Users screen and then click **Delete**.

Screen Fields

If this user has private templates or groups, how do you wish to handle them?
Indicate what you want to do with any logical groups or private templates owned by this STA username. Options are:

- Make them public – Keep the templates, Executive Report policies, and logical groups, but make them public and available to all STA usernames. This is the default.
- Delete them – Delete all private templates, Executive Report policies, and logical groups owned by this STA username.

Buttons

Delete
Click to delete the STA username.

Cancel
Click to dismiss the dialog box without deleting the STA username.

See Also

- "Delete an STA Username" on page 9-7

Email Configuration Dialog Boxes

- "Define SMTP Server Details" on page C-36
- "Define Email Details" on page C-38

Define SMTP Server Details

Description

This dialog box allows you to define the email settings for the SMTP server used to send emails from the STA application.

This dialog box appears when you click **Edit Selected SMTP Server** on the Configuration – Email screen.

Screen Fields

SMTP Host Address
Enter the IP address or fully qualified DNS alias of your SMTP email server.

SMTP Port
Enter the SMTP port number for outgoing mail transport. Typically, this is port 25, but check with your IT system administrator to verify that this is the port used at your site.

From Name
Enter the name you want displayed in the "From" line in email from the server.

From Email Address
Enter the email address from which the email is being sent. If you do not want users to reply to this email, you may want to enter an address in the format:

DoNotReply@Your_Company.com

Enabled?
Select this check box to enable the SMTP email server. De-select this check box to disable the email server.

Use Secure Connection Protocol
Select this check box to select the appropriate secure connection protocol. See your IT system administrator to determine which connection is right for you. You must select one of the following options:

- TLS – Click to select Transport Layer Security.
- SSL– Click to select Secure Sockets Layer.

Requires Authentication
Select this check box to indicate that the SMTP server requires authentication.

Username
Enter a username supported by the SMTP server. Required only if you have selected the **Requires Authentication** check box.

Enter Password
Enter the password assigned to the user. Required only if you have selected the **Requires Authentication** check box.

Verify Password
Enter the password again to verify that you have entered it correctly. Required only if you have selected the **Requires Authentication** check box.

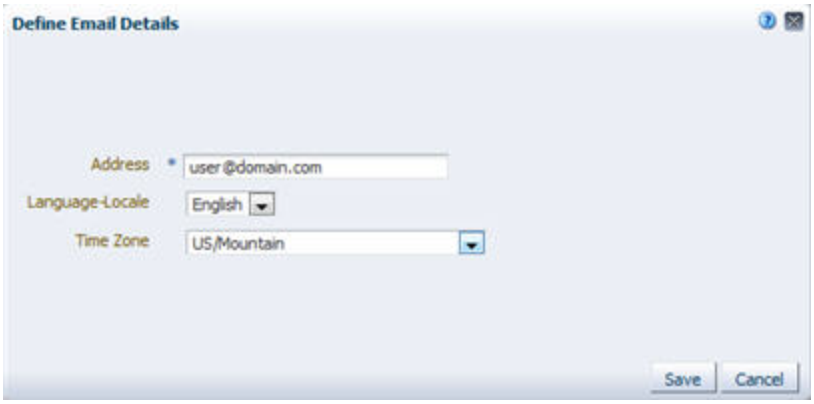
Buttons

Save
Click to apply your entries.

Cancel
Click to dismiss this dialog box without applying your entries.

See Also
- "Define the STA SMTP Server" on page 9-8

Define Email Details



Description

This dialog box allows you to add an email address eligible to receive emails from STA.

This dialog box appears when you click **Add Email** or **Edit Selected Email** on the Email Addresses Toolbar on the Configuration – Email screen.

Screen Fields

Address

Enter a destination to send email to in the form:

your_name@your.company.com

Language-Locale

In the menu, select English if it is not already displayed.

Time Zone

In the menu, select the recipient's local time zone.

Buttons

Save

Click to apply your entries.

Cancel

Click to dismiss this dialog box without applying your entries.

See Also

- "Add an Available Email Recipient" on page 9-10

Index

Symbols

'About' link, 1-9
"missing" media, 12-10

A

Accessibility Settings dialog, 1-5
alert emails
  eligible addresses, C-38
alert policies, 5-1
  avoiding too many alerts, 5-9
  copying, 5-18
  defining, 5-1, 5-3, 5-4, 5-11, 5-12
  defining email recipients, 5-10, 5-16, 5-21
  deleting, 5-23
  disabling, 5-17, 5-22
  enabling, 5-1, 5-17, 5-22
  entities, 5-3, 5-14
  managing the list of, 5-12
  modifying, 5-19
  severities, 5-4, 5-14
    best practices, 5-9
    examples, 5-4
    for exchanges, 5-4
    for media validation activities, 5-4
  STA sample, 5-8
    deleting, 5-9, 5-24
    modifying, 5-9
    naming convention, 5-9, 5-24
  user roles for, 5-3
  using logical groups to define, 5-10
Alert Policies wizard, 5-13, 5-18
alerts
  changing the state of, 5-27
  described, 5-1
  dismissed
    displaying, 5-28
    hiding, 5-28
  dismissing, 5-11, 5-27
  displaying detail, 5-25
  emails, 5-10, 5-21
  generating, 5-1, 5-2
  managing the list of, 5-25
  manual workflow (optional), 5-11, 5-27
  monitoring, 5-2, 5-11
    user roles for, 5-3
alerts process, 5-1

C

changing SNMP client attributes, 11-9
client attributes, 11-9
configuration data
  building, 11-5
  collecting, 11-5
  keeping up to date, 11-5
connection status, 11-2
connection test
  described, 11-3
  library reboot and, 11-4
  modifying library SNMP settings and, 11-3
  Redundant Electronics switch and, 11-4
Create New Log Bundle dialog, C-26

D

Dashboard, 2-1
  changing the column and row layout, 2-6, 2-14
  complex arrangements and loading time, 2-3
  custom templates, 2-3
  customizing, 2-3, 2-6, 2-14
  Executive Reports and, 2-17, 6-1, 6-5
  filtering, 2-3, 2-20
  linking to detail screens, 2-4
  mobile display, 2-11
    accessing, 2-13, 2-22
    requirements, 2-12
  STA default, 2-1, 2-3
  UTC time and, 2-3
Dashboard Portlet Toolbar, 2-8
Dashboard portlets
  adding, 2-15
  annotations
    and Executive Reports, 2-17
    changing, 2-17
  described, A-1
  filtered by logical group, 7-10
  filtering, 2-18
  graphs, 2-9, A-1
  layout, 2-6
  maximum displayed, 2-3, 2-15

number of, 2-3
reports, 2-11, A-6
spark charts, 2-10
tables, 2-10, A-4
Dashboard Toolbar, 2-7
data quality index
media validation and, 8-23
data store
data retention, 12-1
types of data, 11-1
drive efficiency
trends, 13-14
drive errors
associated with a media, 13-6
drives with the most, 13-2
rates, 13-2, 13-8
trends, 13-8, 13-23
drive failures
trends, 13-17
drive firmware levels, 13-56
drive identifiers
mainframe, 12-11
mapping host and STA, 12-11
open systems, 12-12
drive types, 13-31
drive utilization, 13-33
drives
calibration for media validation, 8-10
logical groups and, 7-1, 7-13, 7-15
qualification for media validation, 8-10
viewing logical group membership, 7-23
duplicate volume serial numbers
'duplicate detected' flag, 12-11
avoiding, 12-10
defined, 12-10
reasons for, 12-11
dynamic logical groups, 7-3

E

email
adding addresses, 9-10, 9-11
define server details, 9-8
deleting addresses, 9-13
editing addresses, 9-13
testing setup, 9-12
Email Details dialog, C-38
emails from STA
add eligible addresses, C-38
define SMTP Server, C-36
Executive Report emails
eligible addresses, C-38
Executive Report files
backups, 6-2
creation process, 6-1
date and time stamp, 6-2
deleting, 6-2, 6-9
managing, 6-2, 6-10
PDF format, 6-2, 6-9
private
email recipients and, 6-13
viewing, 6-7
public, 6-7
receiving in emails, 6-2, 6-6
running on demand, 6-1, 6-4, 6-7
effect on schedule, 6-4, 6-7
user roles for, 6-4
viewing, 6-1, 6-2, 6-7, 6-8
Executive Report policies
creating, 6-1, 6-5, 6-11
Dashboard templates and, 6-1, 6-5, 6-12
defining a schedule
frequency, 6-5
on-demand reports and, 6-4, 6-7
Start Date, 6-3, 6-5
defining email recipients, 6-1, 6-5, 6-6
defining ownership, 6-5, 6-13
deleting, 6-14
effect on report files, 6-14
managing the list of, 6-15
modifying, 6-11
private, 6-5
deleting an STA username and, 6-5
user roles for, 6-6
export connection settings, 11-16

F

Filter Data dialog box, 4-2, C-4
filtering
by applying a template, 4-7
by logical group, 7-4, 7-6
from the Dashboard, 4-16
using aggregate count links, 4-6, 4-13
using Dashboard graphics, 4-8
using the Filter Data dialog box, 4-9
filters
and screen pairings, 4-1
clearing, 4-12
clearing on Dashboard portlets, 2-20
clearing selected criteria, 2-21, 4-12
described, 4-1
duration of, 4-2
on Dashboard portlets, 2-18, 2-20
tasks, 4-9
ways of applying, 4-2
firmware upgrades, tasks after, 11-21

H

Help buttons, 1-11

L

libraries
comparing activity levels, 13-51
library configuration
troubleshooting, 11-23
library configuration model
defined, 11-1
library connections, removing, 11-17

library resources
projecting requirements, 13-40
reporting numbers, 13-29, 13-36
utilization, 13-46
List View tables
clearing a filter, 4-12
filtering
using aggregate count links, 4-13
using the Filter Data dialog box, 4-9
log out of STA, 1-8
session memory and, 1-8
log snapshot
access to logs screen, 10-5
deleting, 10-7
displaying run information, 10-5
downloading, 10-6
how to take, 10-3
process, 10-2
reasons for taking, 10-1
logging, 10-1
collecting RDA information
with CLI, 10-3
with user interface, 10-2
forwarding log snapshot to Oracle Support, 10-7
overview, 10-1
logical groups
creation process, 7-2
Dashboard portlets filtered by logical group, 7-10
defined, 7-1
deleting, 7-27
dynamic, 7-3
creating and defining, 7-17
forcing an update, 7-22
selection criteria, 7-3, 7-21
updates to membership, 7-3
examples, 7-2
filtering by, 7-1, 7-4
constructing filters, 7-5
effects of updates to membership, 7-6
listing assigned drives and media, 7-24
manual, 7-3
adding drives and media, 7-13
creating, 7-11
removing drives and media, 7-15
media validation and, 7-1, 8-55
ownership, 7-2
renaming, 7-25
templates and, 7-1
uses, 7-1
Login dialog, C-1
logs
create new bundle, C-26

M

manual data collection
adding drives to a library and, 11-6
entering cartridges into a library and, 11-6
library active storage region changes and, 11-7
library partition changes and, 11-7
when to perform, 11-6
manual logical groups, 7-3
media
logical groups and, 7-1, 7-13, 7-15
viewing logical group membership, 7-23
media approaching capacity, 13-54
media errors
associated with a drive, 13-6
rates, 13-4
trends, 13-23
media shortages and surpluses, 13-36
media types, 13-31
media validation
benefits, 8-2
canceling in-progress validations, 8-51
configuring, 8-5, 8-26
user roles for, 8-25
described, 8-1
disabling, 8-10, 8-30
drive calibration and qualification, 8-10
benefits, 8-12
calibration media criteria, 8-15
calibration media logical group, 8-15, 8-31
choosing calibration media, 8-15
described, 8-13
disabling, 8-36
enabling, 8-34
preparing for, 8-14
process, 8-13, 8-14
results, 8-13, 8-14
terms, 8-11
eligible media, 8-20
enabling, 8-8, 8-30
features, 8-2, 8-3
library complexes and, 8-6, 8-55
logical groups and, 7-1, 8-55
operational efficiency, 8-12
preparing for, 8-5
resuming interrupted validations, 8-57
SL Console and, 8-3, 8-6
user roles for, 8-25
using policies to automate, 8-19
validation drives, 8-6
assigning to pools, 8-6
choosing, 8-7
displaying, 8-27
ensuring health of, 8-12
library complexes and, 8-6
STA minimum requirements, 8-6
verification test types, 8-3, 8-56
Basic Verify, 8-4
Complete Verify, 8-4
Complete Verify Plus, 8-4
Standard Verify, 8-4
Verify and Rebuild MIR, 8-5
media validation policies, 8-19
copying, 8-61
creating, 8-20, 8-53
deleting, 8-64
disabling, 8-57, 8-59

enabling, 8-57, 8-59
library complex, 8-55
listing, 8-58
logical groups and, 8-20
managing, 8-26
media format, 8-55
modifying, 8-62
policy criteria, 8-56
resuming interrupted validations, 8-57
selection criteria, 8-21
user roles for, 8-25
validation test type, 8-56
Media Validation Policies wizard, 8-54, 8-61, 8-63
media validation requests
canceling in-progress, 8-24
canceling pending, 8-24, 8-49
displaying the queue of, 8-37
initiators, 8-22
managing, 8-21, 8-26
manual, 8-17, 8-39
pending, 8-22, 8-46, 8-49
priorities, 8-22, 8-46
reordering pending, 8-46
resuming interrupted validations, 8-24
states, 8-21, 8-22, 8-24
user roles for, 8-25
media validation results, 8-23
DQI, 8-23
ensuring validity of, 8-12
recommendations, 8-23
mobile Dashboard, 2-11
accessing, 2-13, 2-22
requirements, 2-12

P

password requirements, 1-2, 9-1
pivot tables
clearing a filter, 4-12
filtering
using aggregate count links, 4-13
using the Filter Data dialog box, 4-9

Q

Quick Links screen, 3-5
predefined templates and, 3-7
using to apply templates, 3-10

R

redundant electronics, tasks after a switch, 11-21
removed drives and media
displaying, 12-2
examples, 12-4
identifying, 12-3
impact on summaries, 12-3, 12-4
STA Stop Tracking timestamp, 12-1, 12-3
removed libraries, 12-8
removed library resources
impact to data screens, 12-4
re-adding later, 12-1
removing library connections, 11-17
Reset Templates dialog, C-17

S

screen pairings, 4-1
SMTP Server dialog, C-36
SNMP
configuration data, 11-5
confirm connectivity, 11-7
connection test, 11-3
management
add trap recipient, 11-20
change client attributes, 11-9
delete or modify trap recipient, 11-20
display trap recipients, 11-19
export connection settings, 11-16
library, 11-18
remove library connection, 11-17
with user interface, 11-7
managing, 11-1
testing connections, 11-3
SNMP Client Settings dialog, C-29
SNMP connection
define client settings, C-29
define library connection, C-31
library reboot and, 11-4
SNMP Library Connection dialog, C-31
software version information
displaying, 1-9
spark charts in Dashboard portlets, 2-10
STA configuration
email, 9-1, 9-8
troubleshooting, 11-23
users, 9-1, 9-5
status, connection, 11-2

T

tables
filter data, C-4
tape job errors
troubleshooting, 13-19
templates
applying, 3-8
from the Quick Links screen, 3-5, 3-10
with the Templates Toolbar, 3-9
Confirmations preferences and, 3-15
creating, 3-3, 3-13
custom, 3-2
deleting, 3-21
description, 3-1
exporting, 3-4, 3-19
importing, 3-4, 3-19
logical groups and, 7-1
managing, 3-3, 3-4, 3-13
modifying, 3-15
ownership, 3-3
predefined, 3-2, 3-3, 3-22

Alerts Overview, B-9
All Messages - Analysis, B-12
All Messages - Overview, B-11
CAPs Overview, B-8
Complexes Overview, B-3
Dashboard, B-2
described, B-1
Drive Cleanings Overview, B-11
Drives - Analysis, B-6
Drives - Messages, B-6
Drives - Overview, B-5
Elevators Overview, B-9
Exchanges Overview, B-10
Libraries - Messages, B-4
Libraries - Overview, B-4
Media - Analysis, B-8
Media - Messages, B-8
Media - Overview, B-6
Media Validation Overview, B-11
PTPs Overview, B-9
Quick Links screen and, 3-7
recovering, 3-22
Robots Overview, B-8
renaming, 3-18
saving, 3-13
screen characteristics
included, 3-3
not included, 3-3
screen default, 3-1, 3-3
clearing, 3-12
setting, 3-11
sharing, 3-4
sticky behavior, 3-3
usage tasks, 3-8
user roles
for managing, 3-4
for using, 3-2
visibility, 3-4
changing, 3-18
private, 3-4
public, 3-4
Templates Management screen, 3-7
Templates Toolbar, 3-5
testing connections, 11-3
testing connections, when to perform, 11-3
transient library locations, 12-10
trap recipients
adding, 11-20
deleting, 11-20
displaying, 11-19
modifying, 11-20
troubleshooting, 11-23
failed connection test, 11-23
failed data collection, 11-23
unsuccessful trap processing, 11-26

U

upgrading firmware, tasks after, 11-21
user roles
template management, 3-4
template usage, 3-2
usernames, 1-2, C-2
users, STA
adding, 9-5
deleting, 9-7
modifying, 9-6
roles, 9-1
UTC time on the Dashboard, 2-3