Advanced Reporting Instructions - Scalar i40 and Scalar i80

Advanced Reporting Features

The Advanced Reporting license provides the following library features:

Control Path Failover (CPF) - Provides support for configuring the HP LTO-5 Fibre Channel (FC) drive for control path failover. When control path failover is used, one drive is assigned as the primary control path and another drive as the control path failover (secondary) drive. The control path failover drive is used whenever connectivity to the primary control path drive fails or the drive is inoperable.

Reports - Listed below are Advanced Reporting report names. You can view, configure, send via e-mail, and save and reuse report configurations as templates. In addition, you can automatically e-mail any of the reports to designated recipients at specified, scheduled times.

- **Drive Resource Utilization Report** - Provides tape drive usage information, showing you which tape drives are working at optimum capacity and which are under-utilized. This report can help you allocate your tape drive resources properly.

- **Media Integrity Analysis Report** - Provides TapeAlert count for various combinations of tape drives, tape cartridges, and TapeAlert flags. This report can help you determine if a problem is due to a specific tape drive or tape cartridge.

Logs - Listed below are available logs:

- **Media Security Log** - Lists media that has been removed from the library.

- **Media Usage Log** - Lists media usage information regarding capacity, and read and write errors for media ever mounted in a drive.

Required Firmware

To use all the features of Advanced Reporting, you should install the latest released version of library firmware on your library.

Installing Your Advanced Reporting License

Advanced Reporting is a licensable feature. You must have an Advanced Reporting license installed on your library in order to use the features described in this guide. To install or view your license, select **Setup > License** from the Web client, or **Setup > License Installation** from the operator panel.

The Advanced Reporting license applies to your entire library, regardless of library size. If you increase the number of slots in your library, your license applies to the new library configuration.

Working with Control Path Failover (CPF)

If an HP LTO-5 FC tape drive is the control path for a partition, you can select another HP LTO-5 FC tape drive in that partition for control path failover. This means that if the control path tape drive fails, the failover tape drive becomes the control path for the partition. The failed-over tape drive remains the control path for the partition unless it fails or the library is restarted. When either of these events occurs, the library starts over and attempts to use the original control path tape drive as the control path, and the original failover tape drive for failover.

The control path and failover tape drives are assigned by location in the library, so even if you replace a tape drive, the library will still fail over or revert to the specified location.

Prerequisites

To configure control path failover, you must have the following setup on your library:

- Advanced Reporting License.

- The control path and failover tape drives must both be HP LTO-5 FC tape drives, and you must have a minimum of two drives in a single partition.

- The control path and failover tape drives must have their topology configured as **Point to Point**.

When control path failover is configured for a partition, the partition uses a virtual port as the control path communication port. The World Wide Port Name (WWPN) for this virtual port is listed in the library's System Information Report in the Library Partitions section under Control Path.

Configuring CPF

You can configure control path failover from the Web client only.

1 Setup the drive topology.

Set the topology for the control path and control path failover tape drives to **Point to Point.**

a Select **Setup > Drive Settings**.

The **Setup - Drive Settings** screen displays.

Figure 1 Setup - Drive Settings Screen

b For the appropriate partition, select the Requested Topology of **Point to Point** from the drop down menu.

c Click **Apply**.

2 Select **Setup > Control Path**.

The **Control Path** screen displays for that partition.

Figure 2 Setup - Control Path
Screen
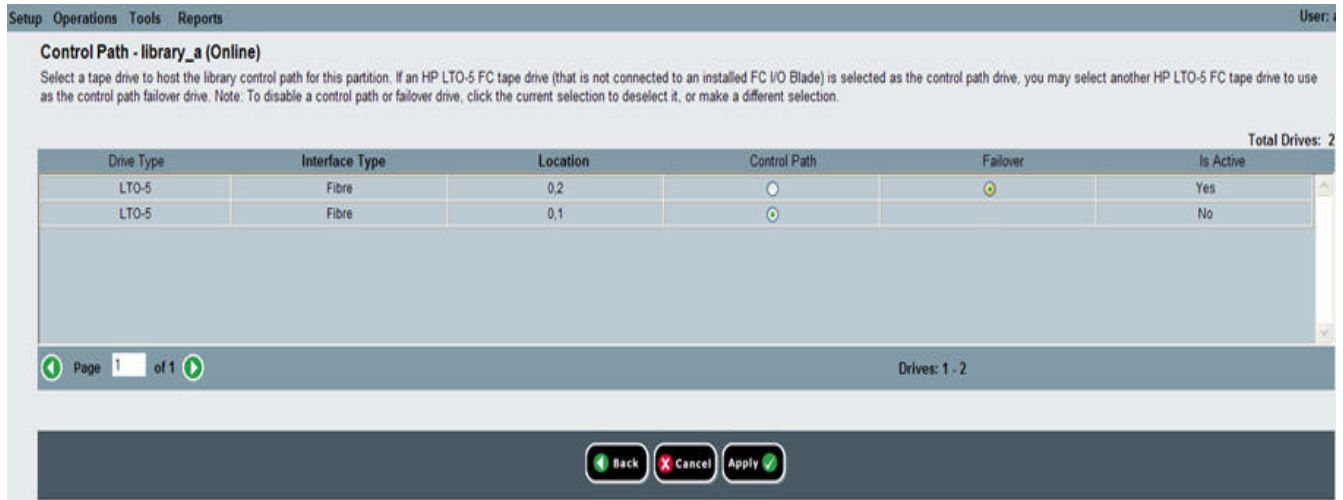
3 Select the Failover drive by clicking the **Failover** option.

4 Click **Apply**.

You can also manually force a failover (see Forcing CPF below).

Forcing CPF

You can manually force a control path failover. You might want to force a failover to check that the non-active tape drive still works, or to switch back to the original control path tape drive once the issue that originally caused the failover has been fixed.

1 Click **Tools > Drive Operations**.

The **Tools - Drive Operations** screen displays.

Figure 3 Tools - Drive
Operations Screen for CPF
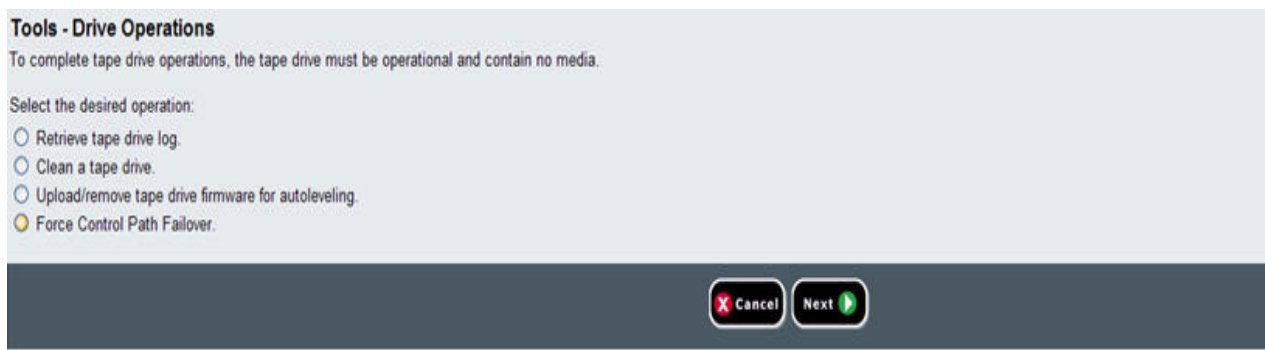
2 Select **Force Control Path Failover** and click **Next**.

The Force Control Path Failover screen displays (see Figure 4 below). All of the partitions that have control path failover enabled are listed. The location and status of the tape drive that is currently serving as the control path are listed in the Active columns. The location and status of the tape drive that is currently serving as the standby control path are listed in the Standby columns. For each partition, the following information is listed:

Column	Indicates
Active Drive	Location of the current control path tape drive.
Active Status	Ready status of the current control path tape drive.
Active Connected	Whether the current control path tape drive is connected and has a working link.
Standby Drive	Location of the standby tape drive.
Standby Status	Ready status of the standby tape drive.
Standby Connected	Whether the standby tape drive is connected and has a working link.

Figure 4 Force CPF Screen

Force Control Path Failover

Force a CPF enabled partition to fail over to the standby control path drive. This operation may cause a brief interruption of host connectivity.

Note: The standby drive must be ready and have a good FC link in order to force a failover.

Partition	Active Drive	Active Status	Active Connected	Standby Drive	Standby Status	Standby Connected
○ library_a	0.1	Ready	Connected	0.2	Ready	Connected

X Cancel   Apply ✓

3 Select the partition on which you want to force the failover, and click **Apply**.

> **Note:** The standby tape drive must be "ready" and "connected" in order to force a failover.

4 Click **Apply**.

The new active tape drive location displays in the **Active Drive** column. The new standby tape drive location displays in the **Standby Drive** column.

> **Note:** If the new tape drive locations do not display, refresh the browser.

Using Advanced Reporting Reports

The following notes will help you interpret the data listed on the reports.

- The data for these reports is collected in log files. When the log files reach their maximum size, the oldest information is deleted as new information is added. This may affect how much historical data you can access.

- The on-screen report contains a chart and a data table. When the log files are large, it would take an excessively long time to load all the historical data into the data table. For this reason, the table only contains a maximum of 1000 rows of data (beginning with the most recent) even if the log file contains more records. (The chart displays information for the entire range.) To view all of the data, you need to save or e-mail the data file. See Saving and E-mailing Advanced Reporting Data Files on page 13.

- The reports are built according to data in the log files, not your current library configuration. For this reason, your library may contain tape drives or cartridges that do not show up in the report. Similarly, the report may contain tape drives and cartridges that no longer reside in the library.

- Information about a tape drive, cartridge, or operation is not recorded in the Drive Resource Utilization log file until after a tape cartridge has been mounted (loaded) *and* unmounted (unloaded) from the tape drive.

- To see the exact values of each item in the displayed chart, move your mouse so that it "hovers" over the item you wish to see. An information bubble appears with the values listed in it. If you click on a bar, point, or slice, the information bubble locks in place and the hovering feature turns off until you reload the chart. The hovering feature does not work when the value equals zero.

- Values of zero do not appear in Pie charts.

Configuring the Drive Resource Utilization Report

This report identifies how tape drive resources are utilized in your library. You can use this report to help you determine the proper work load distribution between the tape drives in your library.

The following information is collected for each tape drive installed in the library:

- Drive location (module, row)
- Drive serial number
- Partition
- Megabytes read
- Megabytes written
- Time and date of mount (UTC)
- Time and date of dismount (UTC)
- Media motion time (in seconds)
- Tape cartridge barcode

You can only access this report from the Web client.

1 From the library menu bar, select **Reports > Advanced Reporting > Drive Resource Utilization**.

The Drive Resource Utilization Report configuration page opens. This may take several minutes.

2 Configure the report by specifying the following:

- Date Range — Specifies the range of time covered by the report. Choose Last 7 days; Last 4 weeks (default); Last 3 months; or All History (as far back as there is data in the log file).

- Attribute — Specifies which value is included in the report. Select one of the following:

  - Data Written/Read (default) — The amount of data written to and read from each tape drive, shown separately in the chart.

  - Total Read and Write — The combined total amount of data written to and read from each tape drive.

  - Media Mount Count — The number of tape cartridge mounts.

  - Media Mount Time — The total amount of time media spent in the selected drive(s).

  - Media Motion Time — The total amount of time media spent in motion while in the tape drive (writing, reading, rewinding, etc.).

- Chart — How the data is displayed in the chart. Choose Area, Bar (default), Line, or Pie.

- Type — The chart type. Select one of the following:

  - Rollup (default) — Displays the Grouping on the x-axis and the Attribute amount on the y-axis.

  - Trend — Shows how the Attribute amount changes over time for the selected Grouping.

- Grouping — Specifies which tape drive(s) or partition(s) to include in the report. Select one of the following:

  - All Drives by Coordinate (default) — Presents the sum total of the selected attribute for all tape drives according to their location in the library. If more than one tape drive resided in that location during the selected range, then the attribute values for all the tape drives that resided in that location are combined in the chart.

  - All Drives by Physical SN — Presents the sum total of the selected attribute for all drives according to the physical tape drive serial number.

  - All Partitions — Presents a comparison of all drives grouped by partition in the physical library.

  - Selected Drive by Coordinate — The report chart is based on an individual tape drive location in the library. If more than one tape drive resided in that location during the selected range, then the attribute values for all the tape drives that resided in that location are combined in the chart.

  - Selected Drive by Physical SN — The report chart is based on an individual tape drive identified by its physical drive serial number.

- Selected Partition — The report chart is based on an individual partition in the physical library.

> **Note:** Refer to the *Scalar i40 and Scalar i80 User's Guide* for an explanation of the location coordinates.

3 Click **Next**.

The report is generated and appears on the screen.

Configuring the Media Integrity Analysis Report

This report provides TapeAlert counts for various combinations of tape drives, tape cartridges, and TapeAlert flags. You can use this report to help determine if a problem is due to a specific tape drive or tape cartridge.

The Media Integrity Analysis report collects the following information for each TapeAlert:

- Date/Time
- Tape drive physical serial number
- Cartridge barcode
- TapeAlert value
- TapeAlert Description

You can only access this report from the Web client.

1 From the library menu bar, select **Reports > Advanced Reporting > Media Integrity Analysis**.

The Media Integrity Analysis Report configuration page opens. This may take several minutes.

2 Configure the report by specifying the following:

- Date Range — Specifies the range of time covered by the report. Choose Last 7 days; Last 4 weeks (default); Last 3 months; or All History (as far back as there is data in the log file).

- Attributes— Specifies which values are included in the report, and how they are combined. Select in any combination, including all (default) and none. If you select no attributes, the chart displays the TapeAlert count for the selected Grouping.

  - Cartridge Barcode — All relevant tape cartridges.

  - Drive Physical SN — All relevant tape drives.

  - TapeAlert — The TapeAlert flags that were issued. For a description of all TapeAlert flags, see the Web client online help or the *Scalar i40 and Scalar i80 User's Guide*.

- Chart — How the data is displayed in the chart. Choose Area, Bar (default), Line, or Pie.

- Type — The chart type. Select one of the following:

  - Rollup (default) — Displays the number of TapeAlerts for the combination of Grouping and Attributes you selected.

- Trend — Shows the occurrence of TapeAlerts over time.

- Grouping— Specifies which drive(s) or tape cartridge(s) on which to base the report. Choose one of the following:

  - All (default) — All tape drives and tape cartridges for which a TapeAlert was issued during the specified range.

  - Selected Drive by Physical SN — An individual tape drive. Only tape drives which issued a TapeAlert during the specified range appear in the report.

  - Selected Cartridge by Barcode — An individual tape cartridge. Only tape cartridges that were associated with a TapeAlert during the specified range appear in the report.

- Sorting — Specifies how the data will be sorted. Choose Alphabetical, Count (ascending), or Last Occurrence (default).

3 Click **Next**.

The report is generated and appears on the screen.

Using Advanced Reporting Templates

If you want to use the same configuration repeatedly, you can save it as a template. You can save up to 20 templates for each type of advanced report.

You can only work with templates from the Web client.

Creating or Accessing a Template

1 From the menu bar, select **Reports** > **Advanced Reporting**, and then select the desired report.

The configuration screen for that report appears.

2 For a new template, in the **Report Templates** box at the bottom of the screen, type a name for the template in the empty field next to the **Save** button. The name can have a maximum of 15 characters. You can use only lowercase letters, numbers, and the underscore character (_) in template names.

Figure 5 Template and Report Data Functions
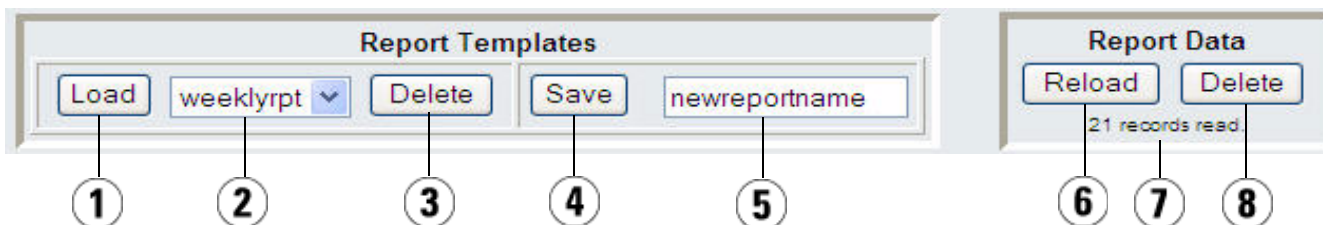
3 Click Save.

1	Loads the selected template.
2	Template drop-down list.
3	Deletes the selected template.
4	Saves a report configuration as a template.
5	Type name of new report here.
6	Reloads the data from the library log file to the Internet browser.
7	Lists the number of records currently loaded in the Internet browser for this report.
8	Deletes all the Advanced Reporting data.

The report appears in the drop-down menu next to the **Load** button.

Using a Saved Template

To use a saved template, select the template from the drop-down list and click **Load**.

Deleting a Template

To delete a template, select the template from the drop-down list and click **Delete**.

Loading and Reloading Advanced Reporting Data

When you first open an Advanced Report configuration screen, the system loads all the data from the library log file for that report to the Internet browser in preparation for creating your reports. If there is a lot of information in the log file, this may take several minutes.

The data that is loaded in the Internet browser remains unchanged until you log out of your library session or reload the data. If new data is added to the log file during your session (for example, a TapeAlert occurs), it will not appear in the on-screen report until you either log out of the library and log on again, or reload the data.

To reload the data without logging out, click the **Reload** button on the report configuration page (see). This action reloads all the data for that report, which may again take several minutes.

You can see how many records were loaded from the log file for this report by looking at the Report Data section of the report configuration page. A note says "XX records read," where XX is the number of records.

Deleting Advanced Reporting Data

In some circumstances, you may wish to delete the data contained in the library log files used to build the advanced reports. To do this, click the **Delete** button in the **Report Data** section of either report configuration page. This deletes the data for both the Drive Resource Utilization report and the Media Integrity Analysis report.

Caution: Once you delete the data in the log files, you cannot get it back. The **Reload** button does NOT retrieve deleted data! It is recommended that you save all the data for both the Drive Resource Utilization report and the Media Integrity Analysis report before deleting the data. See Saving and E-mailing Advanced Reporting Data Files on page 13.

Figure 6 Report Data Buttons

Saving and E-mailing Advanced Reporting Data Files

You cannot save the report as it appears on the screen, but you can save or e-mail the report data as a comma-separated values (.csv) file. You can then import the .csv data into a spreadsheet program and manipulate it to create your own reports for analysis. The .csv file contains all of the data in the log file that falls within the date range you specify.

You can only access this report from the Web client.

1 Generate a report.

2 Scroll down to the bottom of the report viewing screen to a box titled **Retrieve the Report Data File**. See Figure 7 below.

3 To save the report data as a.csv file, click **Save**.

4 To e-mail the report data as a .csv file, type the name of a recipient in the empty field next to the **E-mail** button, then click **E-mail**.

Figure 7 Saving and E-mailing the Report Data

Working with the Media Security Log

Media removal is detected by the library when it performs an inventory (at boot up, for example). The media security log lists media that have been removed from the library. You can configure the library to collect any or all of the following media removal events for the log.

- Unexpected Removal Detection After Power-up and Reboot Only
- Unexpected Removal Detection During Library Operation
- Expected Removal Detection From I/E Slots During Library Operation

Unexpected removal refers to tape cartridges that were removed from the library without being exported properly via the I/E station.
Expected removal refers to tape cartridges that were exported properly via the I/E station.

By default, all the options are disabled and the library collects nothing. You must enable at least one of the options for the library to begin collecting data. The log only lists media that is completely removed from the library. It does not list media that moves from one location to another within the library.

The log file contains the following information:

- Date and time of media removal
- Tape cartridge barcode
- Type of removal (expected or unexpected)
- Slot location coordinates (of the slot the cartridge is missing from)
- Slot type (I/E, storage, or cleaning)

When the log file reaches its maximum size, the oldest information is replaced as new information is added.

You can access and configure this log from only the Web client.

Configuring Media Security

You can choose to collect data in a log to list the following conditions that occur in your library:

- Unexpected removal of media after a power-up and reboot
- Unexpected removal of media during library operation
- Expected removal of media from I/E Slots during library operation

Once configured, the library issues diagnostic tickets for the selected conditions, and collects the media removal conditions in the logs. To configure the Media Security, do the following:

1   Select **Setup > Notifications > Advanced Reporting > Media Security**.

The Setup - Advanced Reporting Media Security screen displays.

2 Click to enable any or all of the options.

- Unexpected Removal Detection After Power-Up and Reboot Only

- Unexpected Removal Detection During Library Operation

- Expected Removal Detection From I/E Slots During Library Operation

---

Note: These options are disabled by default.

---

3 Click **Apply**.

The Progress Window displays. The Progress Window contains information on the action, elapsed time, and status of the requested operation.

- If **Success** appears in the Progress Window, the operation completed successfully. Click Close to close the Progress Window.

- If **Failure** appears in the Progress Window, the operation did not successfully complete. Follow the instructions listed in the Progress Window to resolve any issues that occurred during the operation.

4 To view the Media Security Log, select **Reports > Log Viewer** and then select **Media Security Log.**

Viewing, Saving, and E-mailing Media Security Log

Using the Web client, you can view, save, or e-mail the Media Security Log.

1 Select **Reports > Log Viewer**.

2 Select **Media Security Log** from the list of logs and click **Next**.

The report displays in a new window for viewing.

3 You can save or e-mail the report following the on-screen instructions.

Note: If you want to e-mail the log file to a recipient, type the recipient's name in the text box next to the **E-mail** button, and then click the **E-mail** button. You must have your e-mail notification configured in order to e-mail a log file.

Viewing the Media Usage Log

The Media Usage Log lists information regarding data written and read on the media and lists statistics pertaining to soft and hard read and write errors. The media usage log collects information on all media that have ever been mounted in the library, including media that are no longer in the library. Lifetime media usage metrics are associated with the cartridge and are kept on the embedded cartridge memory.

The log reflects what the drive reports from the embedded cartridge memory whenever the media is unloaded. If the tape cartridge was never mounted and unloaded, it will not appear in the log. When the log file reaches its maximum size, old information is deleted as new information is added. This may affect the amount of available historical data.

The log provides the following information:

- **Volser** — Media cartridge barcode label
- **SN** — Media cartridge serial number
- **Mfr** — Media cartridge manufacturer
- **Date** — Media cartridge manufacturing date (format: YYYYMMDD)
- **Type** — Media type
- **Mounts** — Cartridge mount count
- **RRE** — Recovered read errors
- **URE** — Unrecovered read errors
- **RWE** — Recovered write errors
- **UWE** — Unrecovered write errors
- **LW** — Cartridge lifetime MB written
- **LR** — Cartridge lifetime MB read
- **Enc** — Cartridge encryption status (U=Unknown, E=Encrypted, N=Not Encrypted)

You can access and configure this log from only the Web client.

1 To view, save, or e-mail the report, select **Reports > Log Viewer.**

2 Select **Media Usage Log** from the list of logs and click **Next**.

Automatically E-mailing Advanced Reporting Reports and Logs

You can configure the library to automatically e-mail Advanced Reporting logs and reports to specified recipients on a daily or weekly basis.

Note: Before the library can send e-mail notifications, you must configure the library e-mail account.

You can create up to 20 e-mail recipients. If you want to send the same recipient a different set of reports, you can enter the same e-mail address more than once, with different reports selected for each. Each entry counts as a unique recipient toward the 20 total.

Note: Duplicate entries are not allowed. A duplicate entry means the same recipient is set to receive the exact same reports in two different entries, regardless of the day or time. If you have duplicate recipients, make sure that the reports selected in each entry are not an exact match.

For example, if you have one entry in which Recipient A receives the Drive Utilization and Media Integrity reports on Monday, you cannot create another entry to send Recipient A the Drive Utilization and Media Integrity reports on Thursday. Instead, you can create one entry for Recipient A and send the reports every day (select **Daily** as the day to send the report), or you can change the reports you are sending so that they are not the same as the first entry. You could create three entries for Recipient A as follows: 1) send both reports out on Monday; 2) send Drive Utilization out on Thursday; and 3) send Media Integrity out on Thursday (in a different entry). The recipient is the same, but the reports sent in each entry are different.

Each e-mail notification includes an optional comment text box you can use to enter information about the library or the reports and logs that you want the recipient to know. This information appears in the body of the e-mail.

You can modify the settings of an existing e-mail notification at any time after it is created. If an e-mail notification is no longer needed, you can delete it.

Administrators can configure the library e-mail account and e-mail notifications. Users with user privileges can receive e-mail notifications, but they cannot configure the library e-mail account or e-mail notifications.

Creating a Recipient

1 Select **Setup > Notifications > Advanced Reporting > Receiver Addresses**.

The Setup - Advanced Reporting Receiver Addresses screen displays.

Figure 8 Setup - Advanced Reporting Receiver Addresses Screen
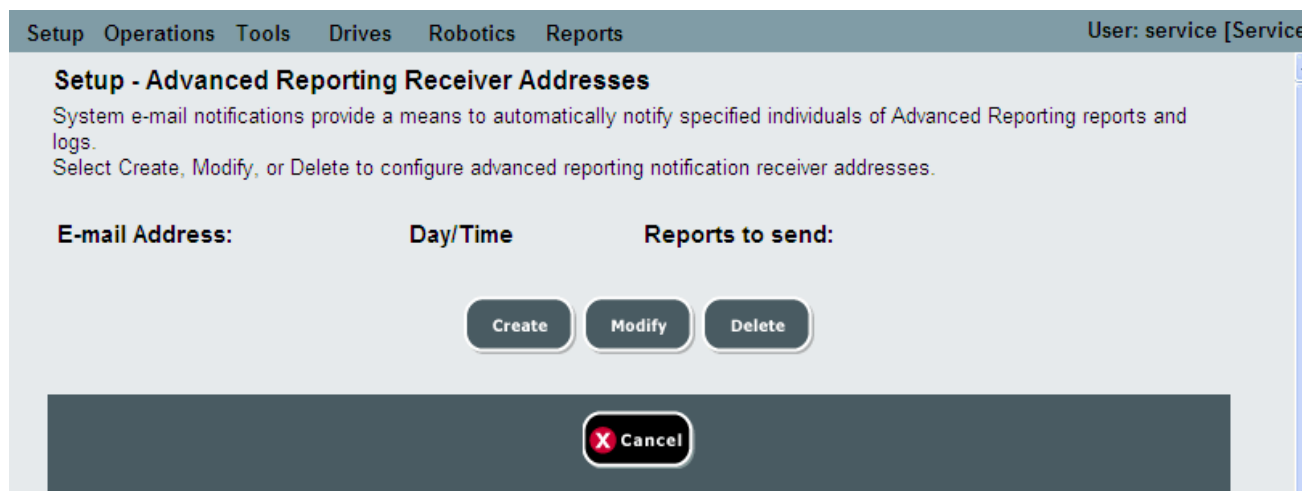
2 Click **Create**.

The Setup - Advanced Reporting Receiver Address Configuration screen displays. The screen lists all Advanced Reporting e-mail notifications that have been created, along with the day/time the e-mail is scheduled to be sent, and which reports and logs will be sent.

Figure 9 Setup - Advanced Reporting Receiver Addresses Configuration Screen
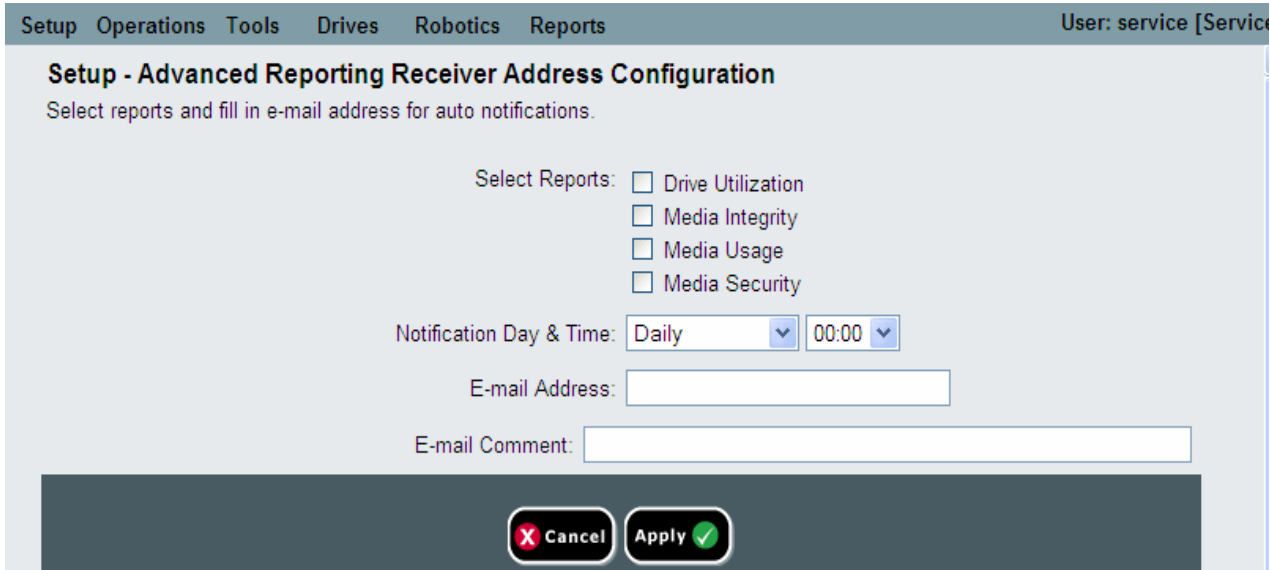
3 Under **Select Reports**, select the check box of the report(s) and log(s) you want to send.

4 Under **Notification Day & Time**, there are two drop-down lists. From the first drop-down list, select the day of the week you want to send the e-mail, or select Daily to send every day. From the second drop-down list, select the time of day to send the e-mail (hourly, using a 24-hour clock).

5 In the **E-mail Address** field, enter the recipient's e-mail address.

6 In the **E-mail Comment** field, enter a comment that will be sent in the body of the e-mail (optional).

7 Click **Apply.**

8 On the Success window, click **Close**.

9 Save the library configuration.

Modifying a Recipient

1 Select **Setup > Notifications > Advanced Reporting > Receiver Addresses**.

   The Setup - Advanced Reporting Receiver Addresses screen displays.

2 Click **Modify**.

3 Change any of the settings and click **Apply**.

4 On the Success window, click **Close**.

5 Save the library configuration.

Deleting a Recipient

1 Select **Setup > Notifications > Advanced Reporting > Receiver Addresses**.

   The Setup - Advanced Reporting Receiver Addresses screen displays.

2 Select a recipient and click **Delete**.

3 On the Confirmation window, click **OK**.

4 Save the library configuration.