Tektronix®

# Medius
# Application Manager

## User Manual

077-3009-01

# Medius Application Manager


# User Manual

Tektronix®

MEDIUS APPLICATION MANAGER

# User Manual



Tektronix, Inc.
14150 SW Karl Braun Drive
P.O. Box 500
Beaverton, OR 97077
USA

## Trademarks

Tektronix, the Tektronix logo, and Medius are trademarks of Tektronix, Inc.

## Contacting Tektronix

Tektronix, Inc.
14150 SW Karl Braun Drive
P.O. Box 500
Beaverton, OR 97077
USA

**For technical support:**
Sentry Technical support is available on Business Days from 6:00 AM to 5:00 PM Pacific Time and 9:00 AM to 5:00 PM Indian Standard Time on the following numbers:

| | |
|---|---|
| US/Canada toll-free | 1-844-219-5329 |
| India toll-free | 1800-3000 4835 |
| Russia toll-free | 810800-22554411 |
| United Kingdom | 44 1344 39 2541 |
| Europe* toll-free | 00800-22554411 |

*Austria, Belgium, France, Germany, Ireland, Italy, Netherlands, Spain, Sweden, Switzerland, UK

Worldwide, please email videosupport@tektronix.com

## About This Document

**Audience**
This user manual is intended for service providers who use Tektronix Medius for monitoring, historical reporting, and alerting from MPEG-2, H.264 AVC, MPEG-4 part 10, and VC-1 transport streams. We assume that you understand the concepts and tools used in a head-end environment. We assume that you are familiar with basic computer operations such as click, drag and drop, and that you are also familiar with the operation of an internet browser.

**Purpose**
The Tektronix Medius User Manual introduces you to the Medius Digital Content Monitor, and describes in detail Medius' features.

This user manual shows you how to configure, control, and use Tektronix Medius. This user manual also describes the Medius hardware installation.

**Screen Shot Note**
While all screen shot s in this document are accurate and truthful representations of the product, some may have been edited to remove information that could pose a security risk.

# Table of Contents

# Sentry Family Product Matrix

This Sentry product manual contains technical information on the Sentry family of video quality monitors. Information for the Sentry Edge products can be found in Appendix B of the *Sentry Series User Manual*.

Some of the features and purchasable options described in this manual are not supported on all of the products. For a breakdown of features and options by product, please refer to the table below.

| Service | Sentry (ASI, GigE, 10G) | Sentry Verify, Verify 10G | Sentry Assure | Sentry ABR | Sentry Edge (I - III) |
|---|---|---|---|---|---|
| ***Comprehensive MPEG Quality of Experience (QoE) Monitoring*** | | | | | |
| Video QoE real time monitoring | ✔ | | | **Optional** | **Optional** |
| Video eMOS/PVQ real time monitoring | **Optional** | | | **Optional** | **Optional** |
| Audio QoE real-time monitoring | ✔ | | | **Optional** | **Optional** |
| Audio loudness & AC-3 Dialnorm (ITU-R BS.1770) monitoring | ✔ | | ✔ | **Optional** | **Optional** |
| Video freeze detection | ✔ | | | **Optional** | **Optional** |
| Audio Silence detection | ✔ | | | **Optional** | **Optional** |
| ***Comprehensive MPEG Quality of Service (QoS) Monitoring*** | | | | | |
| Transport Stream QoS Monitoring | ✔ | ✔ | ✔ | **Optional** | ✔ |
| IP (UDP) statistics | ✔ | ✔ | ✔ | | |
| HTTP Statistics | | | | ✔ | |
| Closed captioning (708, 608, SCTE-20), DVB Subtitle, Teletext reporting | ✔ | ✔ | ✔ | **Optional** | ✔ |
| Error Seconds and Program Availability Reporting | ✔ | ✔ | ✔ | **Optional** | ✔ |
| GOP length reporting | ✔ | ✔ | ✔ | **Optional** | ✔ |
| Video and Audio PID metadata | ✔ | ✔ | ✔ | **Optional** | ✔ |
| Program/PID discontinuity | ✔ | ✔ | ✔ | **Optional** | ✔ |
| Program/PID/Transport Stream/Program Group bandwidth graphing | ✔ | ✔ | ✔ | **Optional** | |
| PCR interval & jitter | ✔ **ASI Only** | | | **Optional** | ✔ |
| MPEG-PSI, DVB-SI, ATSC-PSIP table detect, bit rate, cycle time | ✔ | ✔ | ✔ | **Optional** | ✔ |
| TR101/290 (priority 1, 2, 3) reporting | ✔ | ✔ | ✔ | | ✔ |
| Scalable RF Monitoring (16/64/256 QAM A, B, or C) | | | | | ✔ |

| *Service* | *Sentry (ASI, GigE, 10G)* | *Sentry Verify, Verify 10G* | *Sentry Assure* | *Sentry ABR* | *Sentry Edge (I - III)* |
|---|---|---|---|---|---|
| ***Purchasable Software Options*** | | | | | |
| QoE Monitoring | ✔ | | | **Optional** | **Optional** |
| Carousel monitoring (tru2way / OCAP / MHP / DSM-CC) | **Optional** | **Optional** | **Optional** | **Optional** | **Optional** |
| Ad Insertion/Digital Program Insertion | **Optional** | **Optional** | ✔ | **Optional** | **Optional** |
| EBIF Monitoring | **Optional** | **Optional** | **Optional** | **Optional** | **Optional** |
| SA-BFS Monitoring | **Optional** | **Optional** | **Optional** | **Optional** | **Optional** |
| Perceptual Video Quality (eMOS) on MPEG-2 & H.264 | **Optional** | | | **Optional** | **Optional** |
| Audio Loudness Monitoring (includes CALM Compliance) | ✔ | | ✔ | **Optional** | **Optional** |
| ***Video & Audio*** | | | | | |
| Video: HD, SD, MPEG-2, MPEG-4 AVC (H.264), VC1 | ✔ | ✔ | ✔ | **Optional** | ✔ |
| Audio: Dolby AC-3, MPEG-1 Layer II, AAC, HE-AAC, and HE-AAC v2 | ✔ | ✔ | ✔ | **Optional** | ✔ |
| ***Interfaces*** | | | | | |
| ASI | ✔ **ASI Only** | | | | |
| GigE | ✔ **GigE Only** | ✔ | ✔ | ✔ | |
| Dual GigE | ✔ | | | | |
| Single-Mode or Multi-Mode LC SFP+ | ✔ **10G Only** | ✔ **10G Only** | | ✔ **10G Only** | |
| 8VSB & QAM-B | | | | | ✔ **Edge Only** |
| QAM A, B, or C | | | | | ✔ **Edge II Only** |
| DVB-S2 receiver supports two channels in QPSK / 8-PSK mode | | | | | ✔ **Edge III-S Only** |
| Single-channel DVB-T2 receiver for VHF/UHF | | | | | ✔ **Edge III-T Only** |
| RF Measurements: Level, MER, CNR, Pre-RS BER, Post-FEC Erred Packets | | | | | ✔ **Edge II and Edge III Only** |
| RF Measurements: EVM, Carrier Offset | | | | | ✔ **Edge II Only** |

# Preface

This user manual describes the Medius Application Manager and its web browser-based interface. This manual introduces the components and features of Medius, so you can begin using the device.

## Who Should Use This Manual

This manual is intended for service providers who use Tektronix Medius for monitoring, reporting and alerting from MPEG transport streams. You should understand the concepts and tools used in a headend environment. You should also be familiar with basic computer operations such as click, drag and drop, as well as the operation of a web browser.

## How to Get Help

If you purchased a service contract for your Tektronix Sentry products from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.
If you purchased a Tektronix service program, contact Tektronix technical support:

**For technical support:**
Sentry Technical support is available on Business Days from 6:00 AM to 5:00 PM Pacific Time and 9:00 AM to 5:00 PM Indian Standard Time on the following numbers:

| | |
|---|---|
| US/Canada toll-free | 1-844-219-5329 |
| India toll-free | 1800-3000 4835 |
| Russia toll-free | 810800-22554411 |
| United Kingdom | 44 1344 39 2541 |
| Europe* toll-free | 00800-22554411 |

*Austria, Belgium, France, Germany, Ireland, Italy, Netherlands, Spain, Sweden, Switzerland, UK

Worldwide, please email videosupport@tektronix.com

Additional information about the Tektronix Sentry family of video quality monitors is available at the following URL: http://www.tek.com/video_quality_monitors/

# Introduction

## What is Tektronix Medius?

The Medius is an aggregation device that provides a central location to view manage and configure your Sentrys.

The Medius allows you to compare like programs across multiple Sentrys, to correlate reports for anomalies and view trending data for all of your services.

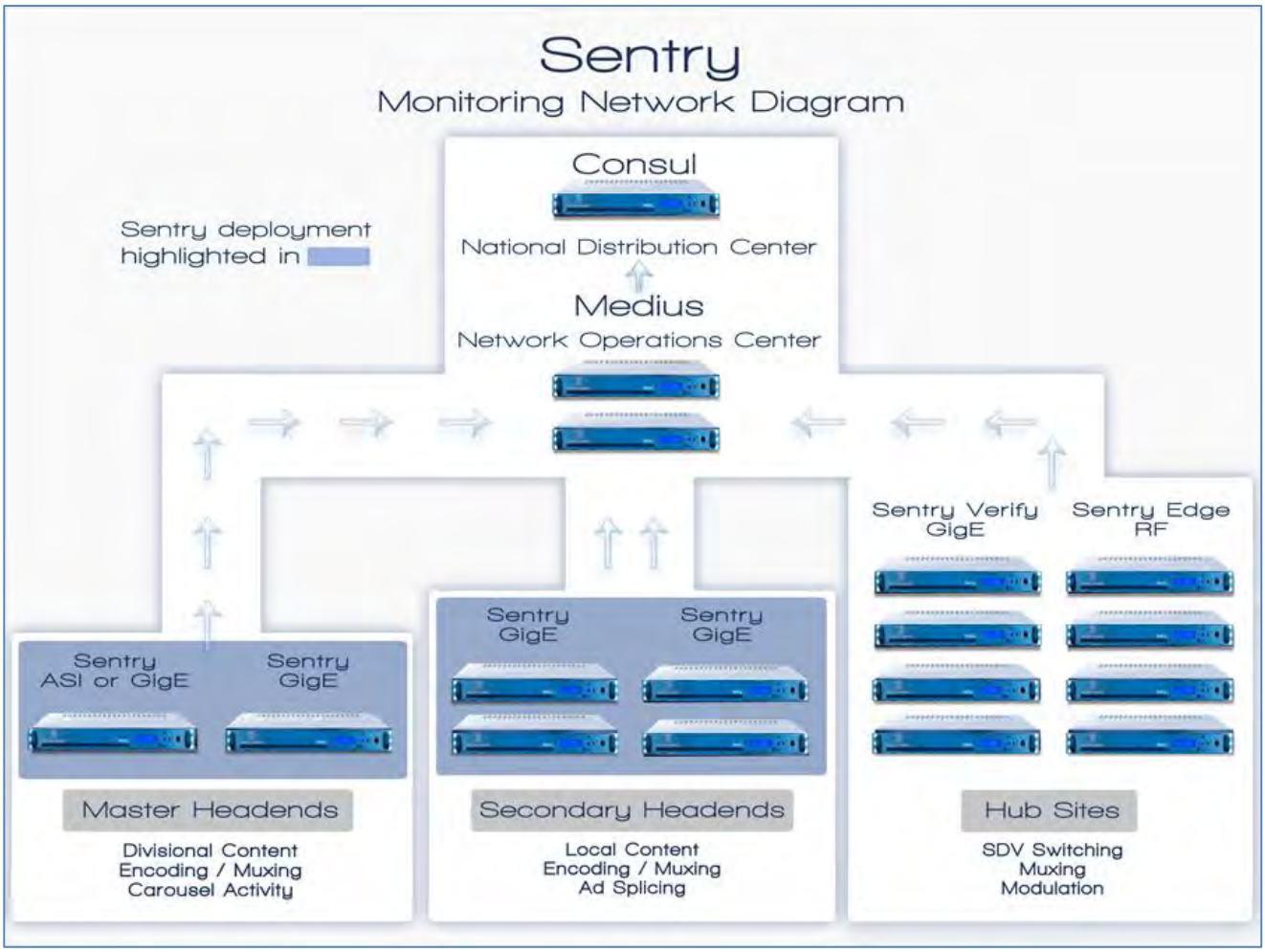



**Figure 1: Sentry Network Diagram**

# Getting Started

## Requirements

You will need a web connection accessible via any modern web browser. We recommend Mozilla Firefox as the browser.

---

**NOTE**: Before installing the system in an equipment rack, make sure that:

- The operating temperature is between 0 °C (32 °F) and 35 °C (95 °F).
- The operating relative humidity is between 0% and 80%.
- There is sufficient airflow around the unit.
- The electrical circuits are not overloaded.
- The equipment is properly grounded.
- No objects are placed on top of the unit.

---

## Setting up the System

To set up Medius you need:

- A 10Base-T network connection
- Network parameters including address of DNS and NTP servers on your network. (Refer to the section **Configure: System Settings**.)

### Making the Connection

1. On the management port, connect one end of a Cat5 Ethernet cable to the LAN2 connector on the Medius unit and the other end to the network socket that connects to the LAN network.
2. Connect the power cord to the system and plug it in to an electrical outlet.
3. Turn on the main power switch on the front of the system.

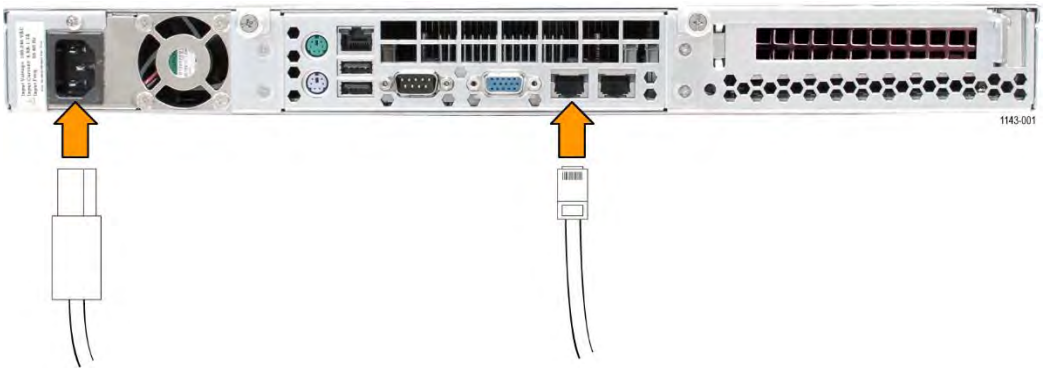



**Figure 2: Making final connections**

# Front Panel Functions (2009 to present models only)

The following applies only to units made in 2009 to present and that have a blue LED backlit display.

These models are able to provide the following functions:

- IP address display on LED
- Manual Reboot option from front panel
- LED Brightness control

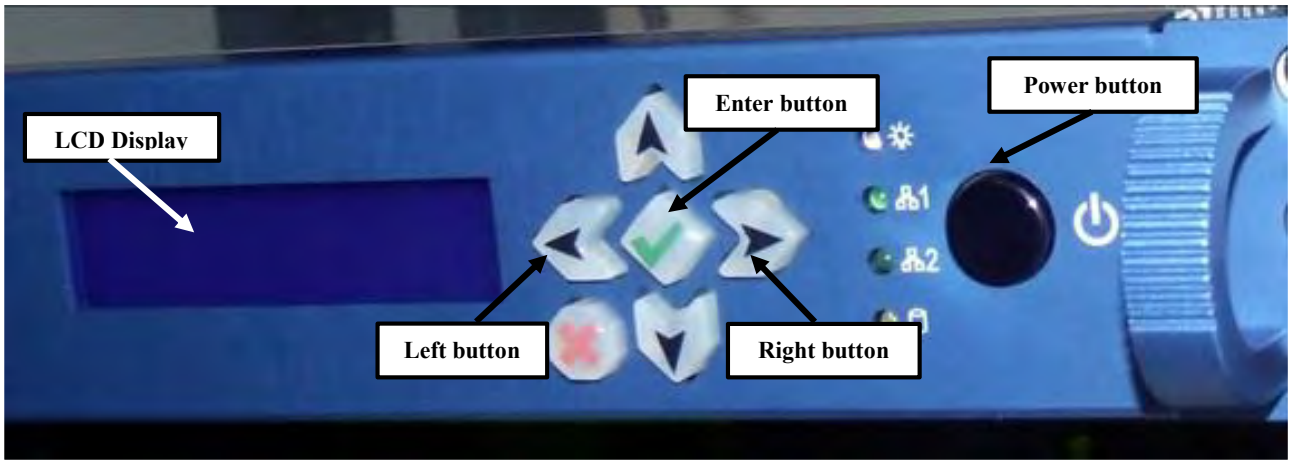



**Figure 3: Sentry front panel**

## IP address on the front panel

To see a display of the IP addresses of both of the system network interfaces on the front panel LCD display:

1. Press and hold **Enter** (green check mark) on the front panel.
2. The address displayed on the top line corresponds to the **Management** interface and the lower line corresponds to the **MPEG/IP input**.

## Manual power down from front panel

In addition to powering down through the Medius interface, you may also use the front panel button.

1. Start the power down of the unit by pressing the front panel power button two times quickly within 2 seconds.
2. Within moments, the LCD display will indicate that the unit has begun the **Safe Power Off** process, and several seconds following, the unit will power down completely.

## LED Brightness

1. The brightness of the LCD display backlight can be changed by selecting either the left arrow or right arrow buttons on the front panel. The left button will dim the display while the right will brighten it.
2. Changes to the brightness level persist until the unit is rebooted or powered down.

## Starting the Web-Browser Interface

1. Start your web browser.
2. Enter the IP address assigned to Medius in the web browser's URL field.

   For example, if the Medius IP address is 192.168.1.1, you would enter the following:


**Figure 4: IP Address Entry**

**NOTE:** ***Medius is fully functional if JavaScript is disabled in your browser, however the look and feel of the UI may differ in some areas from that presented in this User Manual.***

3. Log in with the user name and password for the account.


**Figure 5: Medius Log In Screen**

4. The Medius opens to the **Program Alert Dashboard** view.

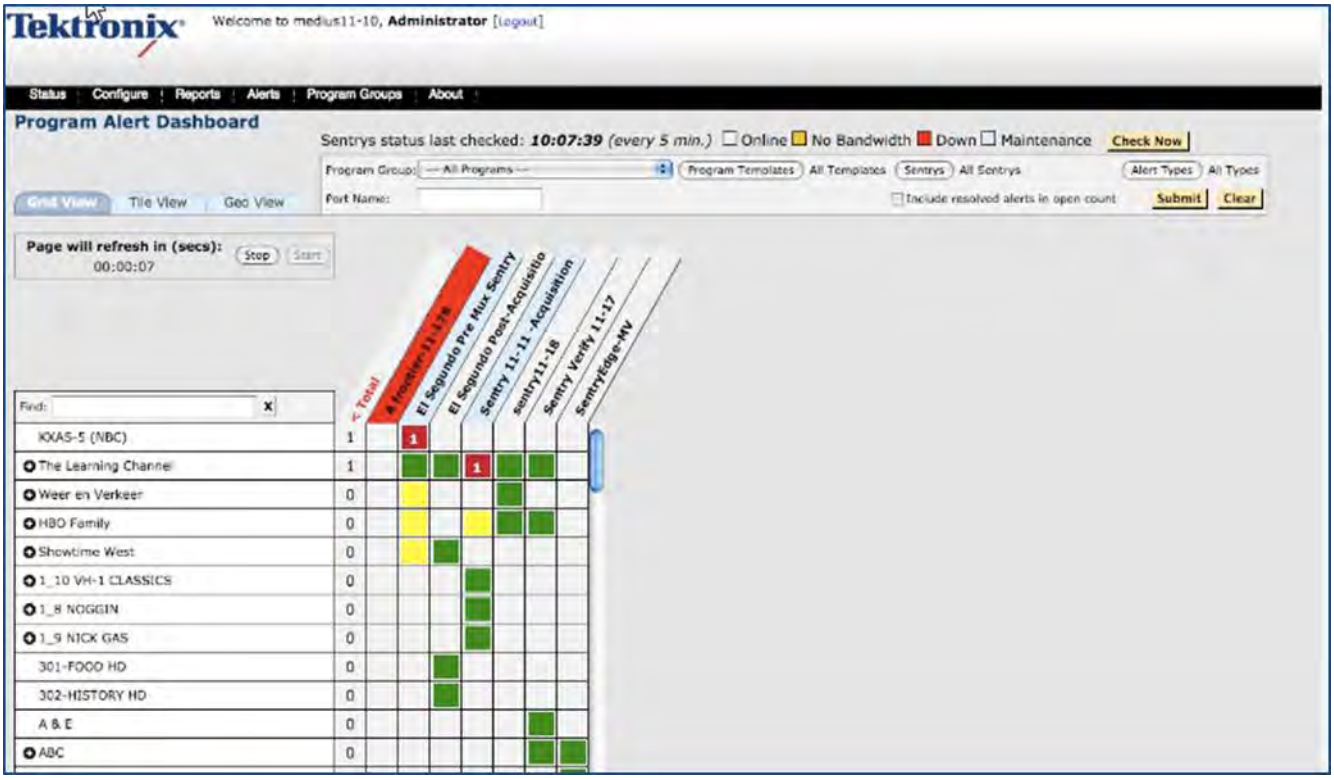



**Figure 6: The Dashboard**

**NOTE**: ***There may be a few seconds delay while the Dashboard screen collects data. Do not stop the browser while loading is in progress***

# Status

From the **Main Menu**, select **Status** then select the particular status view you want to see. All pages are set to automatically refresh themselves making monitoring almost real time.

## Program Alert Dashboard

**Program Alert Dashboard** gives you a quick overview of all set and recorded alerts.

### Access Program Alert Dashboard

Select **Status** from the main menu and then select **Program Alert Dashboard**.

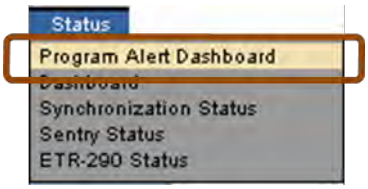



**Figure 7: Program Alert Dashboard**

### Interface Components

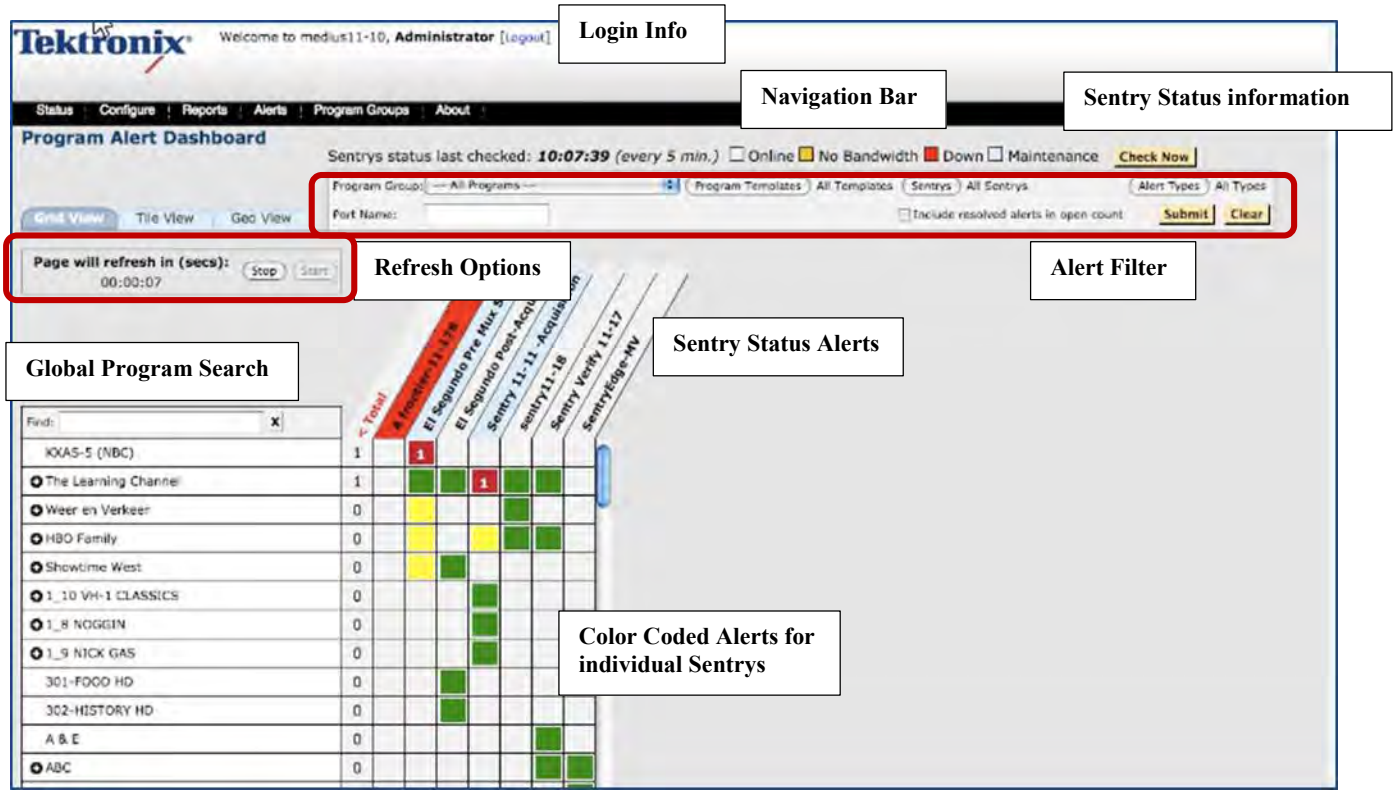


**Figure 8: Program Alert Dashboard overview**

### Login Information

The **Login Information** area displays the username of the logged on user and provides a link to log out of Medius.

Click **Logout** to log out of the system. The username and date and time of the most recent refresh of the screen are also shown.

### Navigation bar

The **Navigation** bar provides the main navigation for the Medius. It includes drop-down menu items for **Status**, **Configure**, **Reports**, **Alerts**, **Program Groups** and **About**.

### Sentry Status Information

Provides the currentoverall status of monitored Sentrys and a color code for the **Status** area. This will show if they are **Online**, **No Bandwidth**, **Down** or undergoing **Maintenance**.

### Alert filter

The Alert Filter allows you to set requirements for alerts, including a checkbox option **Include resolved alerts in open count**.

### View Tabs

The **View** tabs allow you to view the current status by selecting **Region Location View** or **Program Groups View**.

### Refresh options

All views in **Program Alerts Dashboard** will refresh every 15 seconds without moving the page or scroll position.

### Global Program Search

From the **Find** box, you may search and sort all programs across all devices. Example: A search for Discovery Channel will bring up all instances of Discovery Channel on all connected Sentrys.

### Color Coded Alerts for Individual Sentrys

This section shows the current alert status of individual Sentrys (per program)

- **Red**: Open alert
- **Red** cell with number: Number of alerts in the last hour
- **Green**: No alerts
- **Grey**: Not being monitored by the given Sentry
- **Yellow**: Alerts resolved in the last hour

# Grid View

The **Grid View** tab displays a table of programs, the Sentrys monitoring those programs and a color coded alert guide. This makes for a quick and easy reference for troubleshooting problem areas.

In this example**, H.264** is being monitored by two Sentrys and is showing five alerts in one of them. This gives it an overall total of score of 5.

**ETV Carousel**, however, is being monitored by four Sentrys and is showing one error each in two of them, giving it an overall score of two.

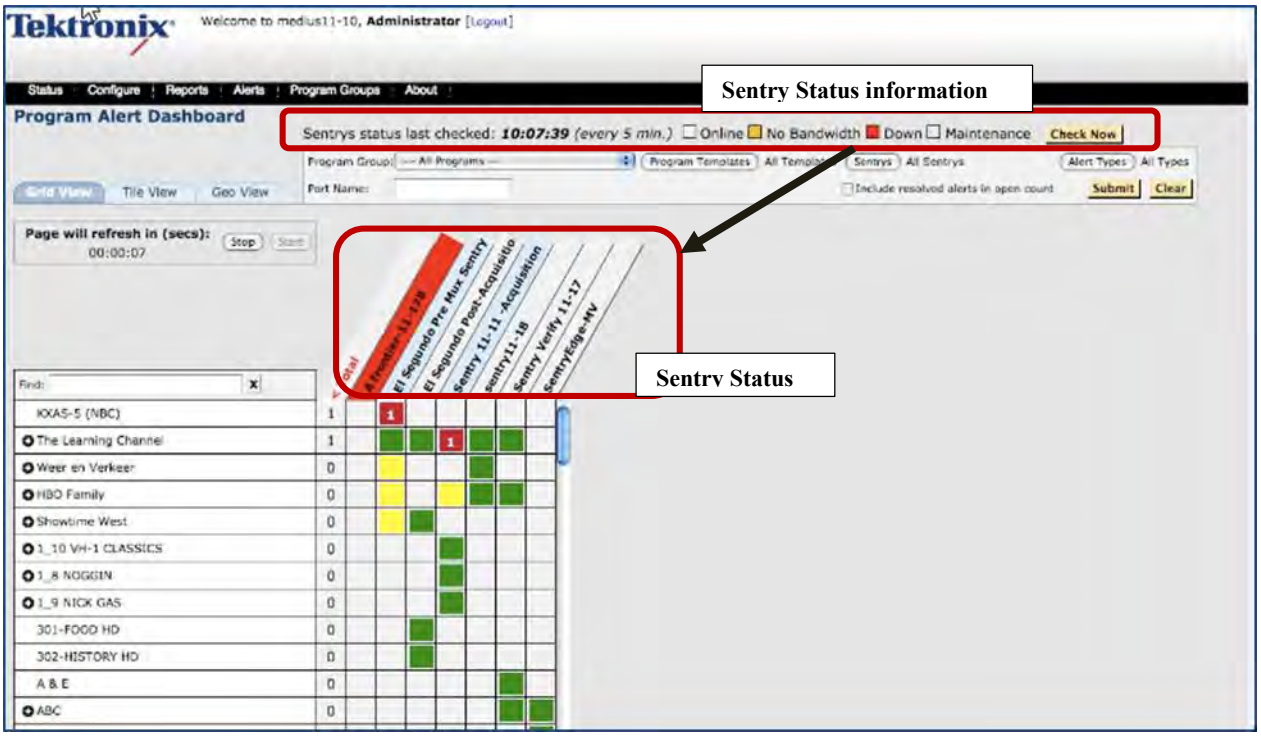



**Figure 9: Grid View tab**

Selecting a red cell will show the **Alert History** report for that program on Sentry. Selecting yellow will show the alerts triggered for that program in the last hour.

This page may also be filtered by program name, **Program Alert** template, **Program Group**, Sentry region/location, alert type or port name.

Plus signs in front of each program name will take you to a detailed view showing the port number, port name, TSID, and program number.

**NOTE:** ***To make full use of the Grid view, adopt identical program names across all Sentrys***

## Tile View

The **Tile View** tab shows a color coded view of the alert status of all programs or services. The programs with the greatest number of alerts are located at the top of the columns. The program name appears in each cell along with the alert totals for the last hour.

This page may also be filtered by program name**, Program Alert** template, **Program Group**, Sentry region/location, alert type or port name.

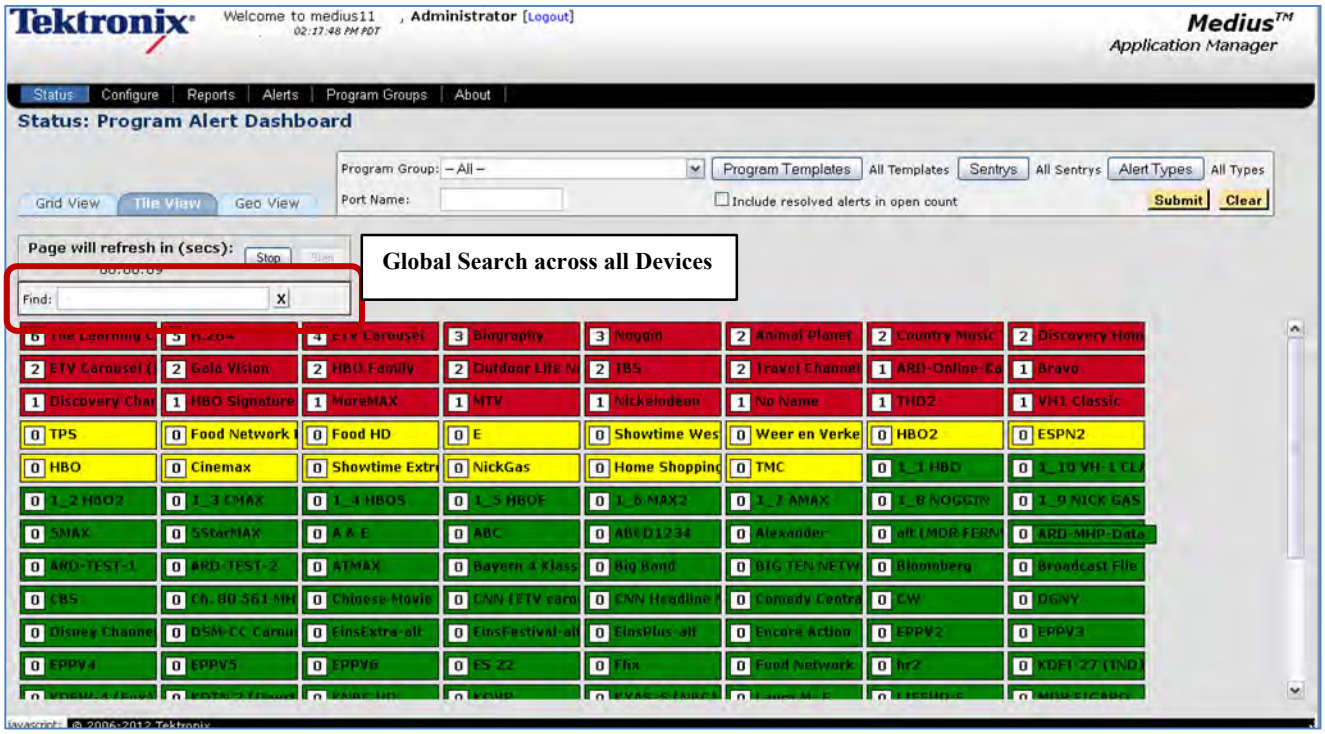



**Figure 10: Tile View tab**

## Geo View

The **Geo View** shows all selected Sentrys and their alerts on a color coded map. This allows for monitoring by region.

Mouse over any Sentry to see the open alerts for that unit.

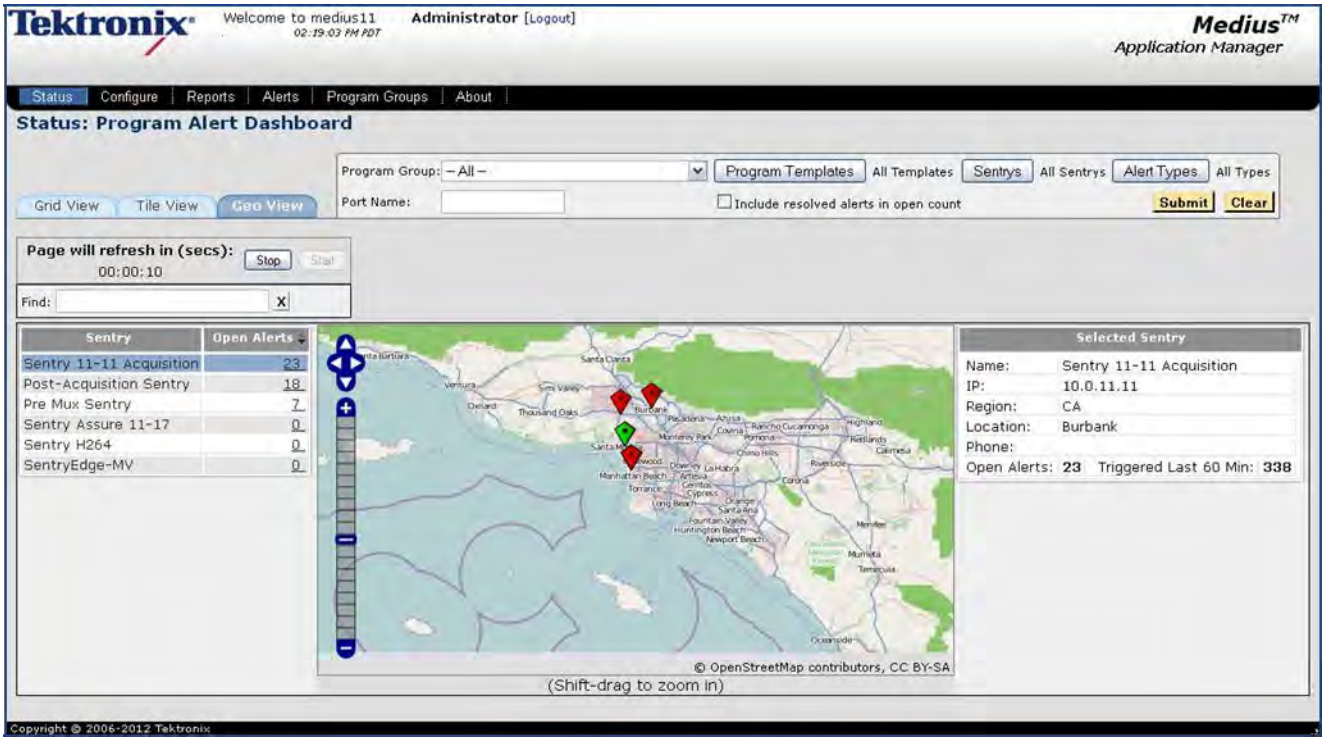



**Figure 11: Geo View tab**

For the **Geo View** function to work properly, you will need to enter the longitude and latitude for each device. To set the longitude and latitude for a device, see the section: ***Configure: Register Sentrys***.

# Program Alert Dashboard

The **Program Alert Dashboard** can be used to quickly see exactly what alerts are occurring for a particular program on a given Sentry.

The alerts shown in the Grid View directly correspond with the alerts on the **Program Detail** page.

The following example shows how to quickly drill down to the **Program Detail** page to get more information about that specific alert.

1. Here, **The Learning Channel** has one error on the **11-11 Sentry** (as shown in the red numbered square) and the **Frontier** Sentry is down completely.

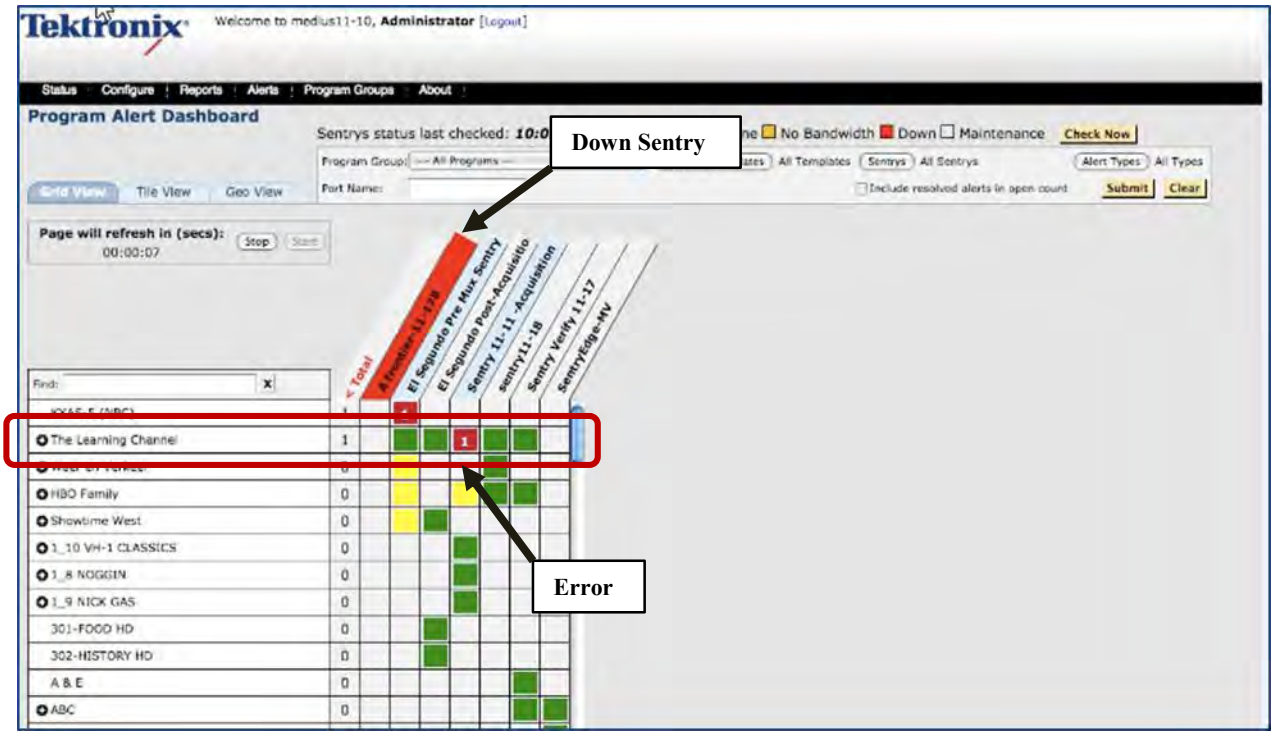



**Figure 12: Select the program name (The Learning Channel) to see details on the alerts (shown in red)**

2. Select a program name to view.

3. The resulting screen will show you every single instance of **The Learning Channel** program across all Sentrys.
4. We want to see instance of **The Learning Channel** on port 0 (**Acquisition AdCue**) on Sentry 11-11, so we select to see that particular instance from the list. It is showing two errors.

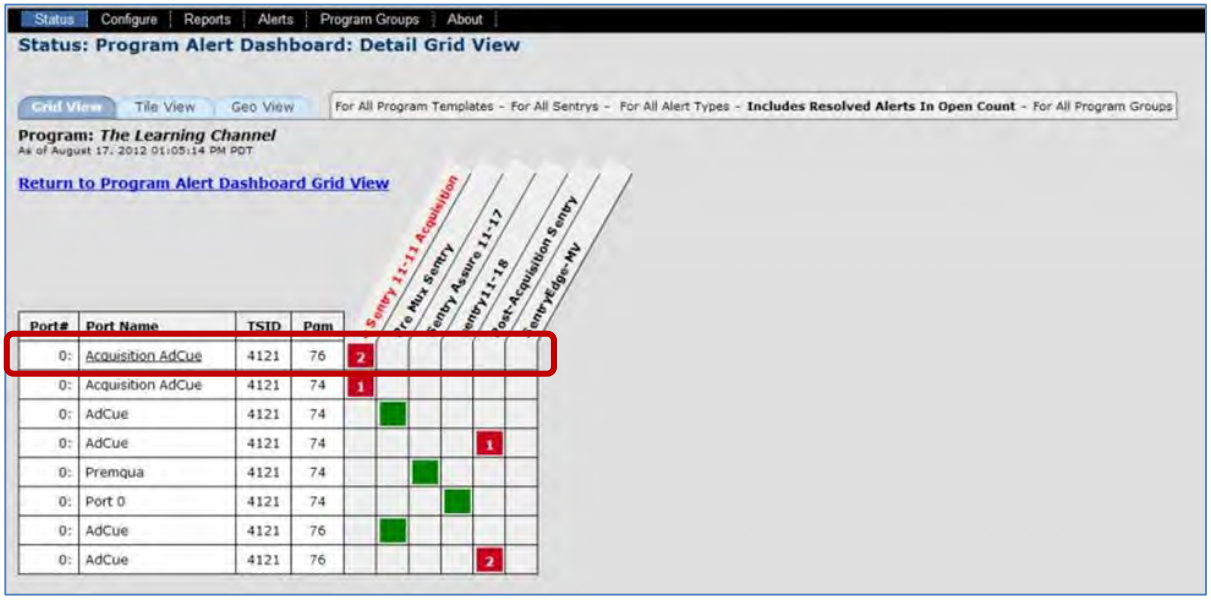



**Figure 13: Drilling down to the individual errors**

5. This takes you to **Program Detail Report** for that instance of **The Learning Channel**. In the **Alert Details** section, at the bottom of the report, you will see all active alerts. The two alerts shown above in red are the exact two alerts shown in the previous **Program Alert Dashboard Detail** report.


**Figure 14: Alert Details from the Program Alerts screen. These are the same two errors from the screen above**

# Dashboard

The **Dashboard** view shows the Sentrys by **Region, Location** and **Program Group**.

## Access Dashboard

Select **Dashboard** from the **Status** main menu.

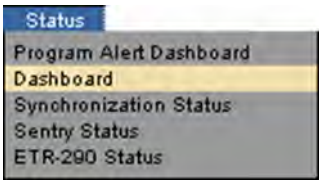



**Figure 15: Dashboard**

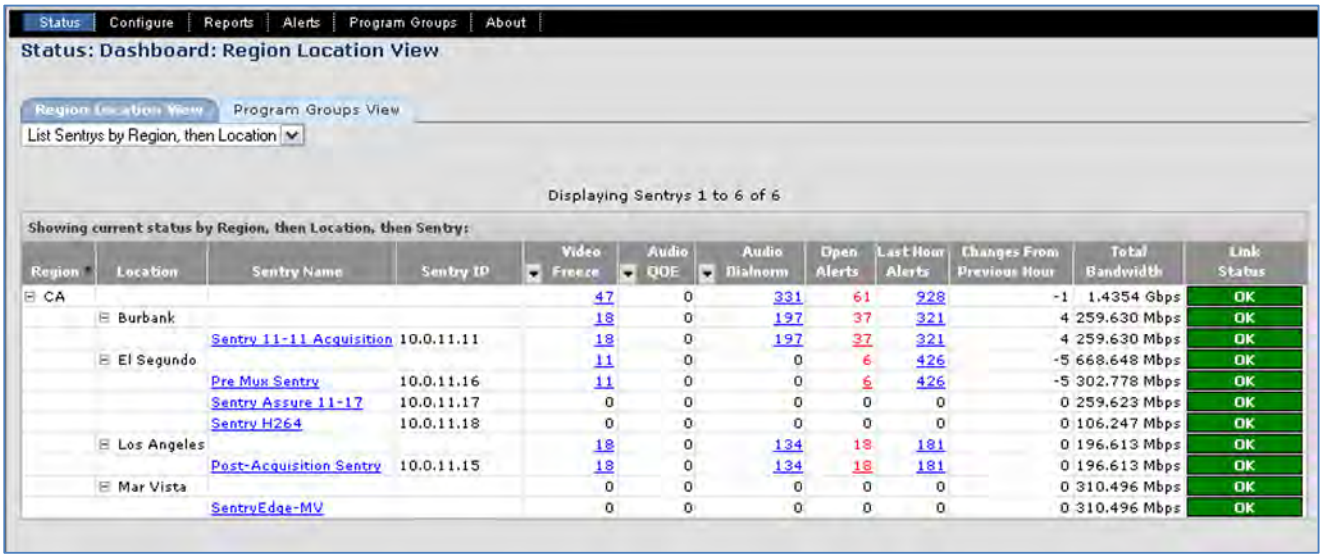



**Figure 16: Dashboard Region Location view**

# Synchronization Status

To get the most accurate readings and reports from your Medius and Sentry units, it is vital that they are in sync. This simply means that they are in communicating and are working together.

## Access Synchronization Status

Select **Synchronization Status** from the **Status** drop-down menu.

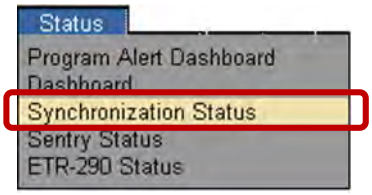



**Figure 17: Synchronization Status**

A green dot in the Sy**nchronization Status** column indicates that all Sentrys in this group are in sync. A red dot indicates they are out of sync.

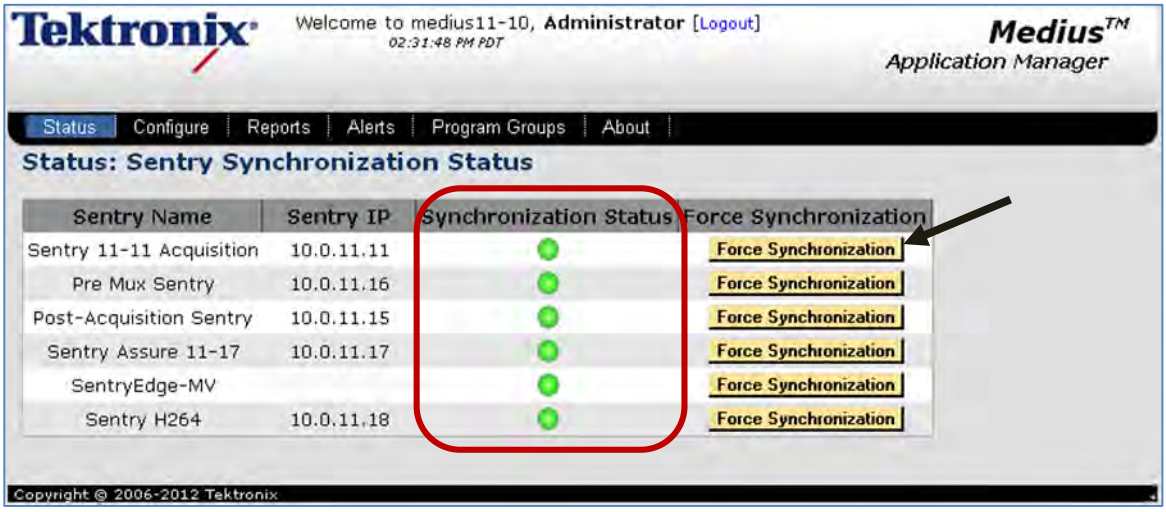



**Figure 18: Synchronization Status in sync**

### *Re-syncing units*

1. To attempt a re-sync of the units, select the **Force Synchronization** button.
2. If the sync is successful, the button will turn **green**.
3. If it is not successful, it will stay **red**. Contact Customer Support for additional assistance.

## Sentry Status

The **Sentry Status** page shows the overall status of any chosen Sentry.

### *Access Sentry Status*

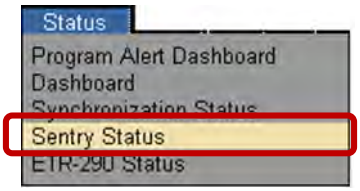



**Figure 19: Sentry Status**

Locate the Sentry you need to work with and select **View** from that row.

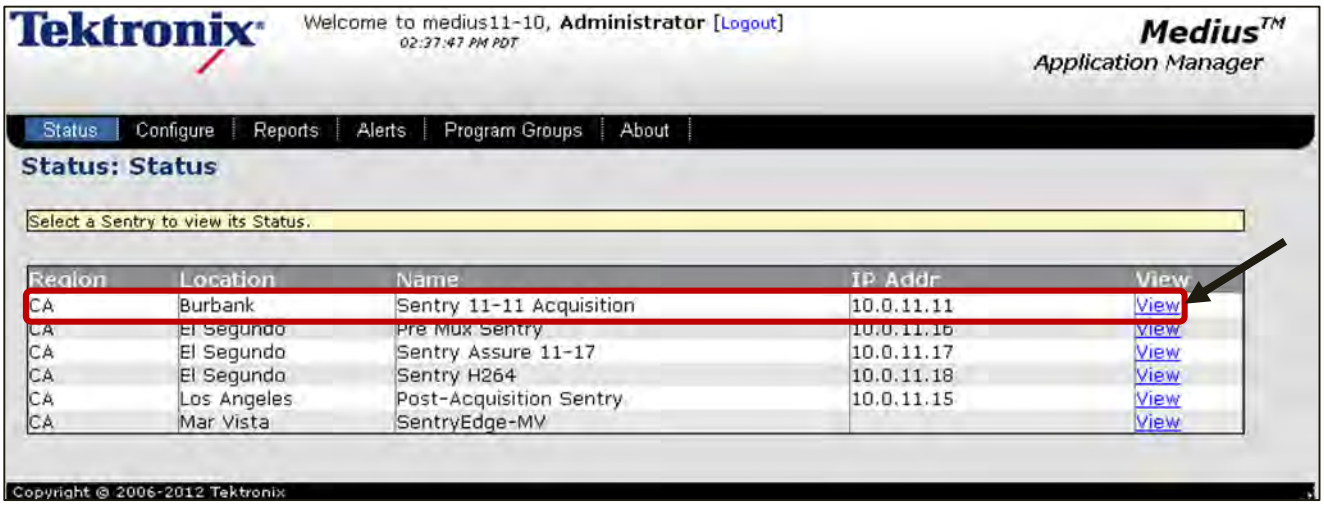



**Figure 20: Select a Sentry to view**

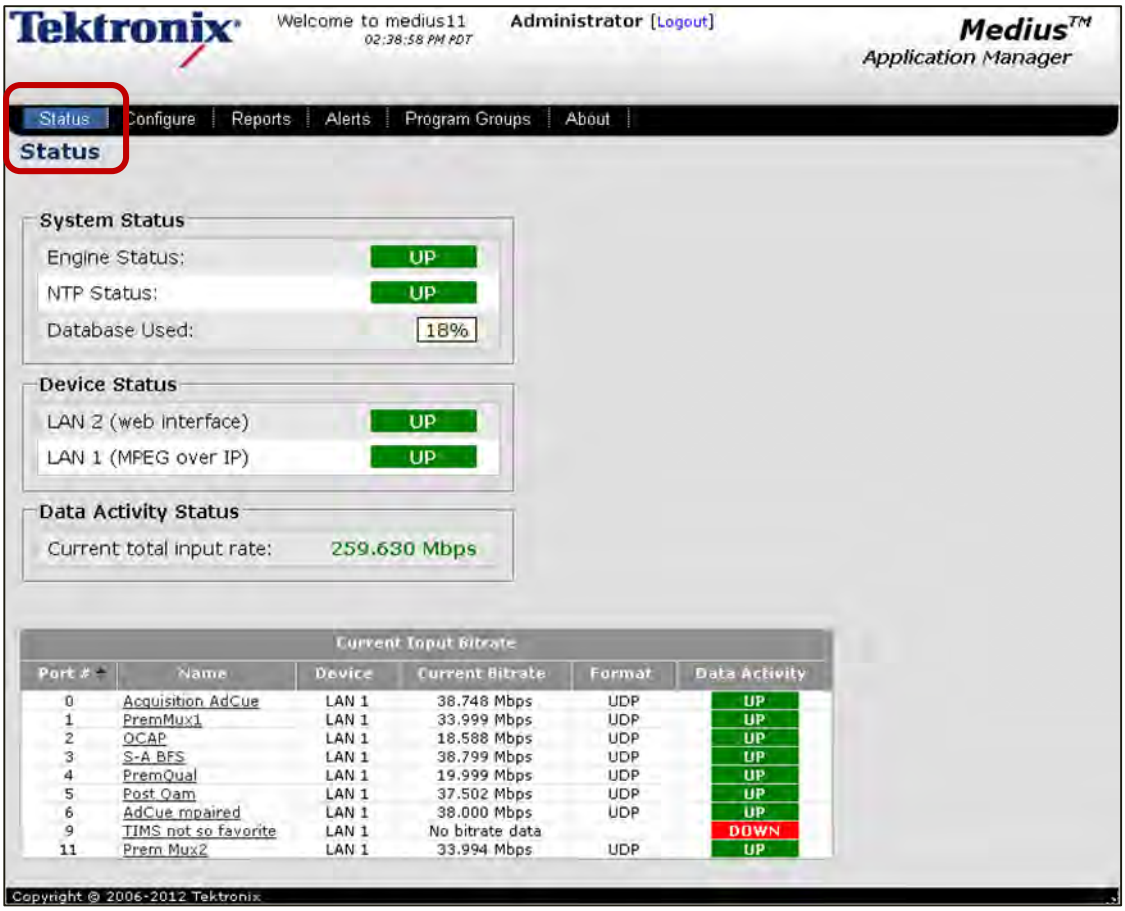



**Figure 21: Sentry Status screen**

The **Sentry Status** page consists of the following:

- **System Status**
  - **Engine Status**
    Displays if engine is UP or DOWN
- **Data Activity status**
  - **Current aggregate input rate**
- **Database Status**
  Displays the percentage of the total database that has been used. Sentry will delete from the database any information older than 60 days.
- **Device Status**
  Displays all the active devices (LAN1, LAN2, ASI ports) and their UP/DOWN state.
- **Current Bitrate**
  Displays the current total input rate and format (UDP or RTP).

# TR101/290 Status

The **TR101/290 Status** report is used to monitor the basic health of the MPEG transport stream. From the **TR101/290 Status** page, you can look at each individual transport stream and see its stats in real time.

## Access TR101/290 Status

To access **TR101/290 Status**, select **Status** from the main navigation bar. Next, select **TR101/290 Status** from the drop-down menu. Then select the desired Sentry and click **View**.

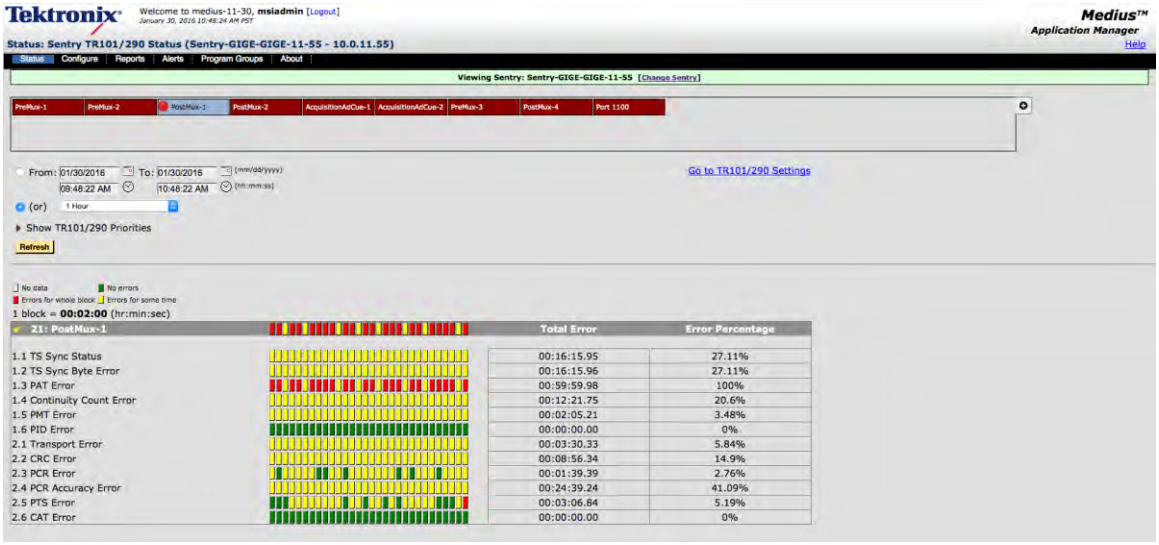



**Figure 22: TR101/290 Status report**

The top section of the TR101/290 Status report shows a single status for each active port. The color of the block depicts the overall status of that port as follows:

- Green: No violations of any type on that port over the selected reporting interval
- Yellow: No current violations on that port, but there were violations over the selected reporting interval that have gone away.
- Red: There are current violations on that port.

Click on the desired port, to view TR101/290 details for that port. Your selected port will be displayed with a colored dot as follows:


**Figure 23: TR101/290 selected port indicator**

The section at the bottom shows the detailed status of each specific TR101/290 priority. There is significance to each priority level.

- **Priority 1** represents the most basic and most critical of all the functions.
  - If you are experiencing errors on Priority 1 this will affect all programs on the transport streams.
- **Priority 2** represents mid level tests for transport stream health.
  - If you are experiencing errors on Priority 2 it MAY affect programs on the transport stream.
- **Priority 3** (Tests that are hidden by default).
  - If these tests are needed, they can be viewed by clicking the **Show TR101/290 Priorities** link.

Each priority is represented as a row in the table. For each row there is a series of colored blocks representing the status through time. The colored blocks have a slightly different meaning than the colors at the port level:

- Green: No violations for that priority during that block of time.
- Yellow: That priority was in violation for part of that block of time, but not for the entire time.
- Red: That priority was in violation for the entire block of time.
- Grey: There was no data being monitored during that block of time on the selected port.

Hovering over a block will show you the specific time range represented by that block. If you hover over a red or yellow block, it will also show:

- The specific test(s) that failed. Note: many of the TR101/290 priorities have several checks being performed.
- The number of seconds that priority was in error during that block of time

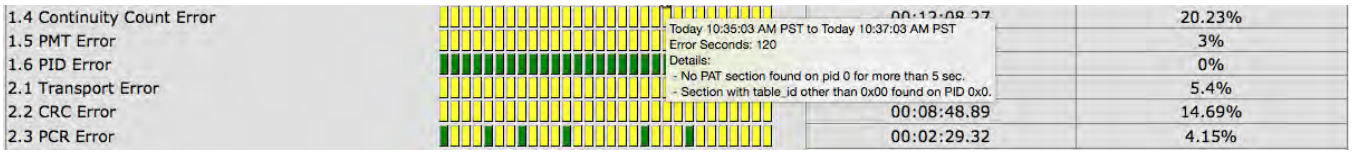



**Figure 24: TR101/290 status block hover readout**

Each priority row also shows the following:

- **Total Error**: The amount of time in which that priority was in error.
- **Error Percentage**: The percent of time that priority was in error. This is a percentage of the time that port was being monitored.

The summary blocks at the top simply show the worst state of any of the underlying priorities during that time range. In other words, if an underlying priority was red during the timeframe, the summary block will be red. Otherwise, if there was a yellow block, the summary will be yellow.


**Figure 25: TR101/290 summary block indicators**

Click the alarm icon next to the port name to quickly create a TR101/290 alert for that port.

## Show TR101/290 Priorities

Clicking the Show TR101/290 Priorities link will display a list of each priority. All unchecked priorities will not be displayed on your report. If a priority is checked, as long as those tests are enabled in the **Configure->TR101/290 Settings** page, that priority will be displayed as a row in the table.

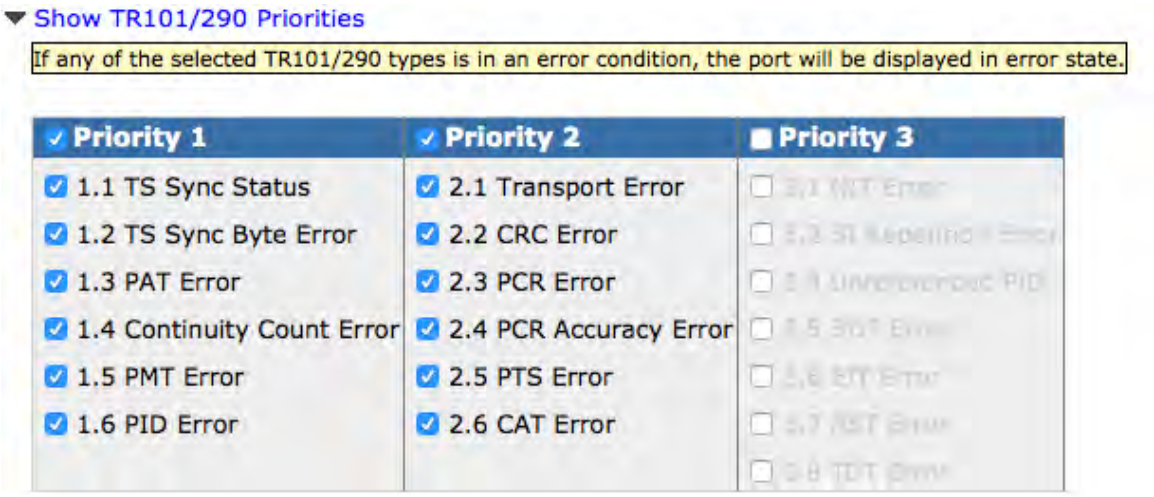



**Figure 26: TR101/290 Priorities list**

Click the **Go to TR101/290 Settings** link to configure any threshold or to disable/enable any TR101/290 test.

# Configure

The **Configure** menu section is used to configure and set parameters that stay constant throughout Medius and/or Sentry reports and forms.

There are two configurable sections: one for Medius and one for each Sentry.

1. For Medius, you can:
   **Registered Sentrys**
   Edit Sentrys registered to this Medius

   **Dashboard Graphs**
   Create custom graphs for all **Dashboard** views

   **Medius Users**
   Edit users with access to this Medius

   **Medius System Settings**
   Edit settings for this Medius

   **System Upgrade**
   Perform upgrade functions

   **Power Off**
   Turn off power for this Medius

2. For Sentry, you can:
   **Program Mappings**
   Modify **Program Mappings** for a selected Sentry

   **Port names**
   Modify **Port Names** for a selected Sentry

   **BFS Settings**
   Modify the **BFS Settings** for a selected Sentry

   **Stream Capture**
   Control a stream capture from a selected Sentry

   **Schedules**
   Create and modify schedules for a selected Sentry

   **MPEG Input Settings**
   Modify the **MPEG Input** settings for a selected Sentry

   **Sentry Users**
   Allows **Administrators** to **Add**, **Edit** and **Delete** users

   **System Preferences**
   Set up options such as **Ad Cue**, **Perceptual Video Quality, Provider Name** and **Thumbnails** for a selected Sentry

   **Sentry System Settings**
   Modify **System Settings** on a selected Sentry

## Access Configure menu items

1. Select **Configure** from the **Navigation** bar and then **Registered Sentrys**.


**Figure 27 Configure menu**

# Registered Sentrys

Select **Registered Sentrys** from the **Configure drop-down menu**.

From the main screen, the user may:

- **Register New Sentry**
- **Add New Location**
- **Add New Region**
- **Help Changing IPs and Help with Replacement Unit**

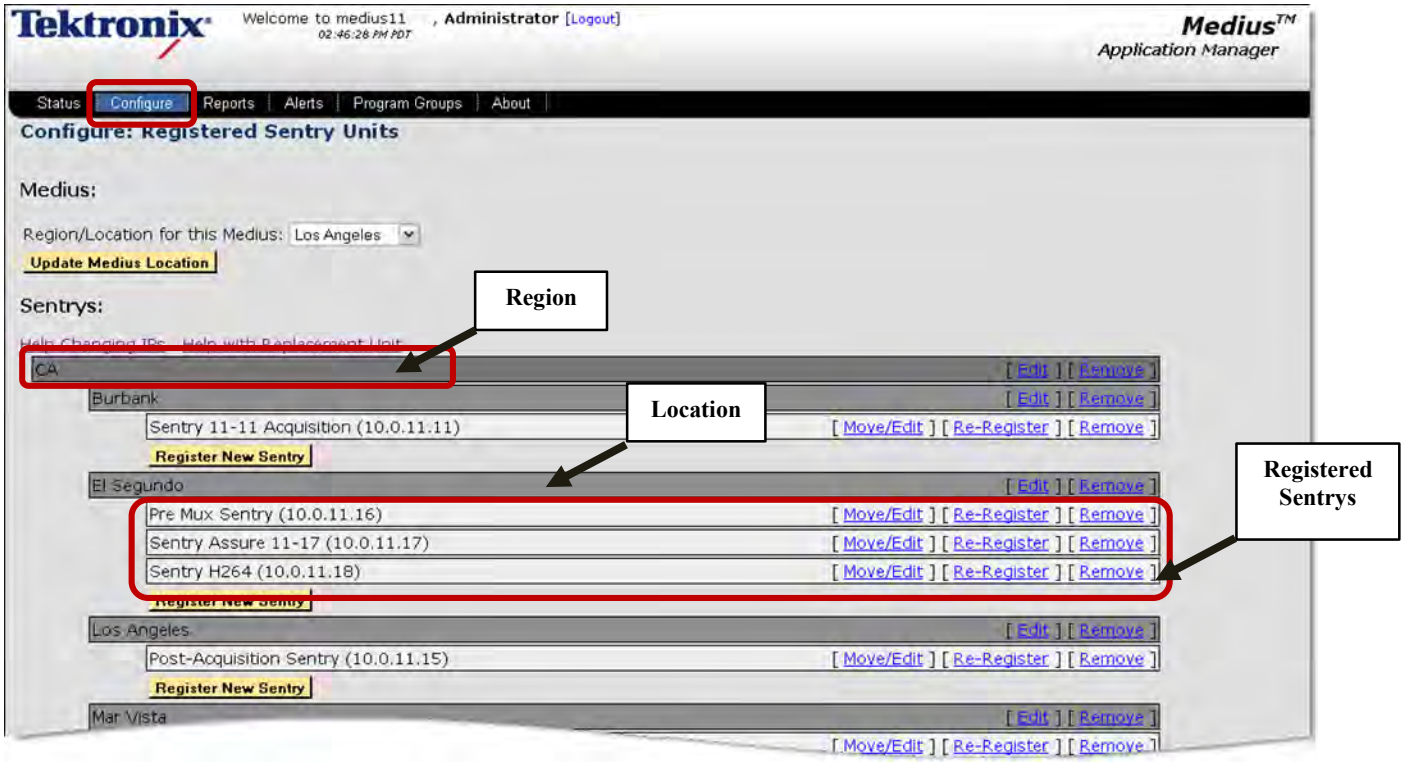



**Figure 28: Configuring Sentry**

## Add Sentrys

To add a new Sentry from the **Registered Sentrys** page:

1. Select the **Register New Sentry** button.

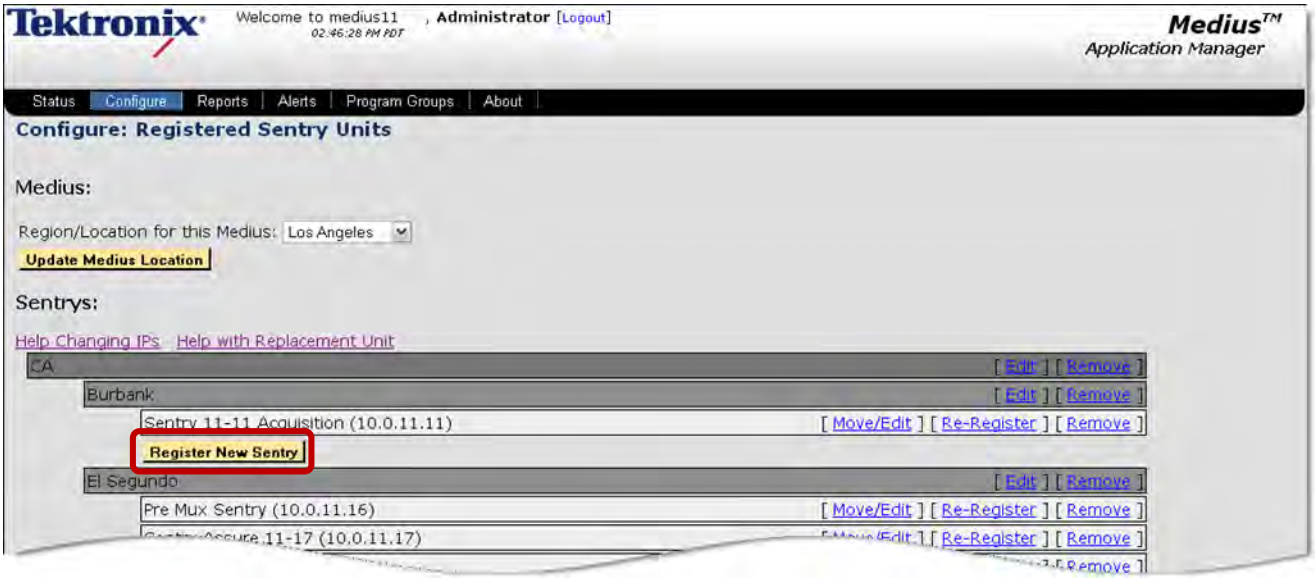



**Figure 29: Register a new Sentry**

2. Enter the IP address for the desired Sentry then select the **Get Sentry Info** button.


**Figure 30: Entering the IP address**

3. Medius will the retrieve the information for that Sentry.

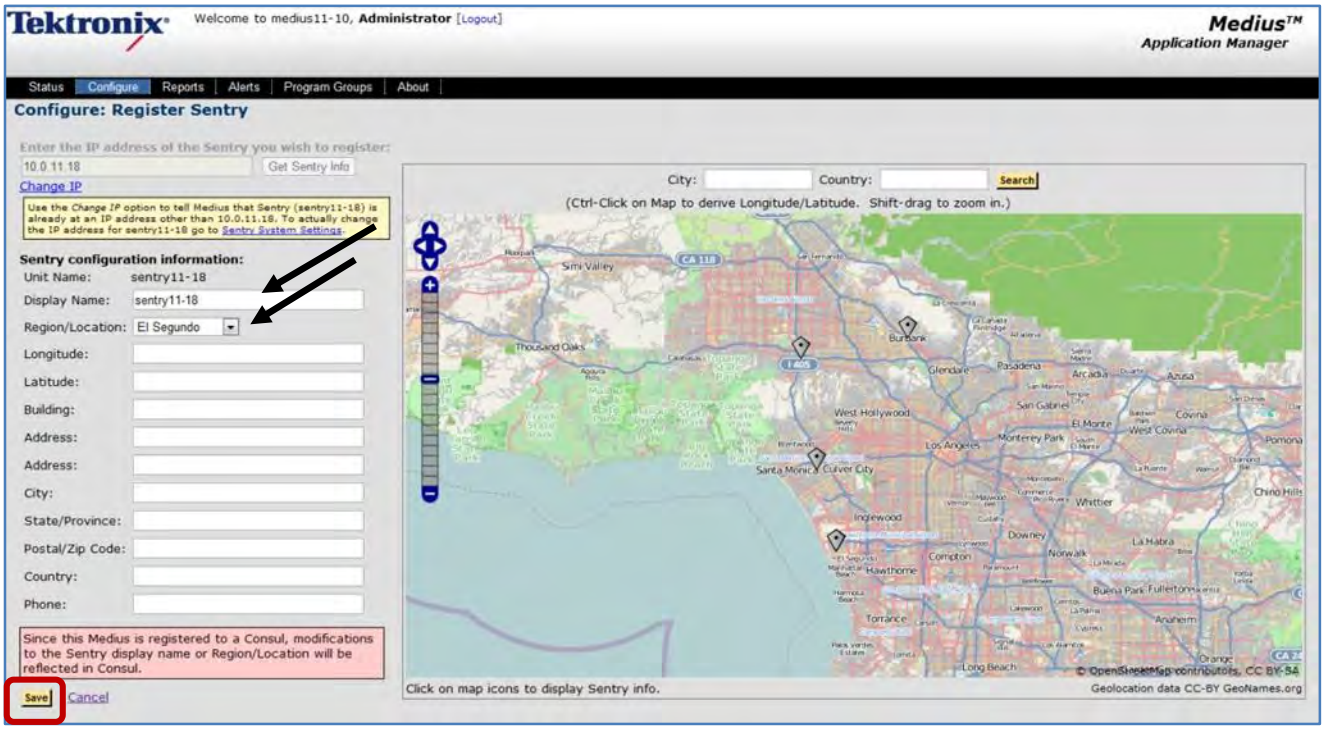



**Figure 31: Sentry Configuration Information**

4. Enter the **Display Name** for Sentry

5. Enter the **Region/Location**.

6. Enter the **Longitude/Latitude** or the physical address of the Sentry. The physical address will not automatically fill in the **Longitude/Latitude** information.

7. To have **Longitude/Latitude** auto-fill, locate the location of the unit on the map. Next, select that area with a **Control-Click** on the map.

8. If this Sentry is in the same location as previously entered Sentry, give the unit a unique name and click on existing unit from the map. The location information will automatically back fill.

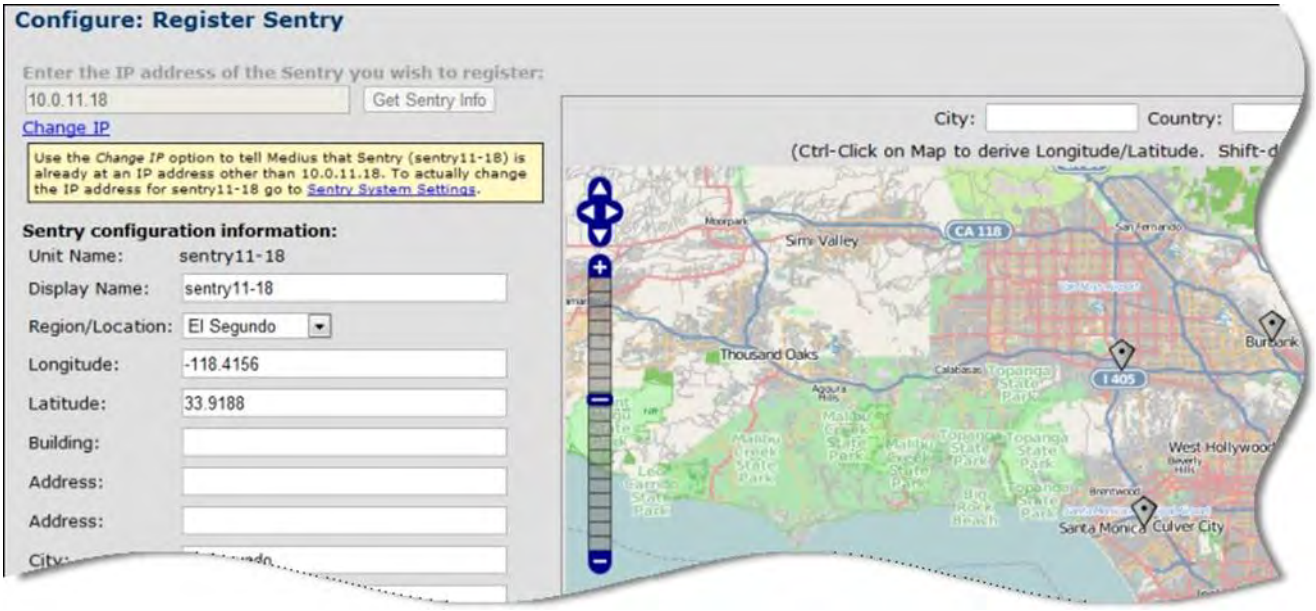



**Figure 32: Click an existing unit to back fill the configuration information**

9. Select **Save.**

## Remove Sentrys

1. Select **Remove** from the **Registered Sentrys** page.

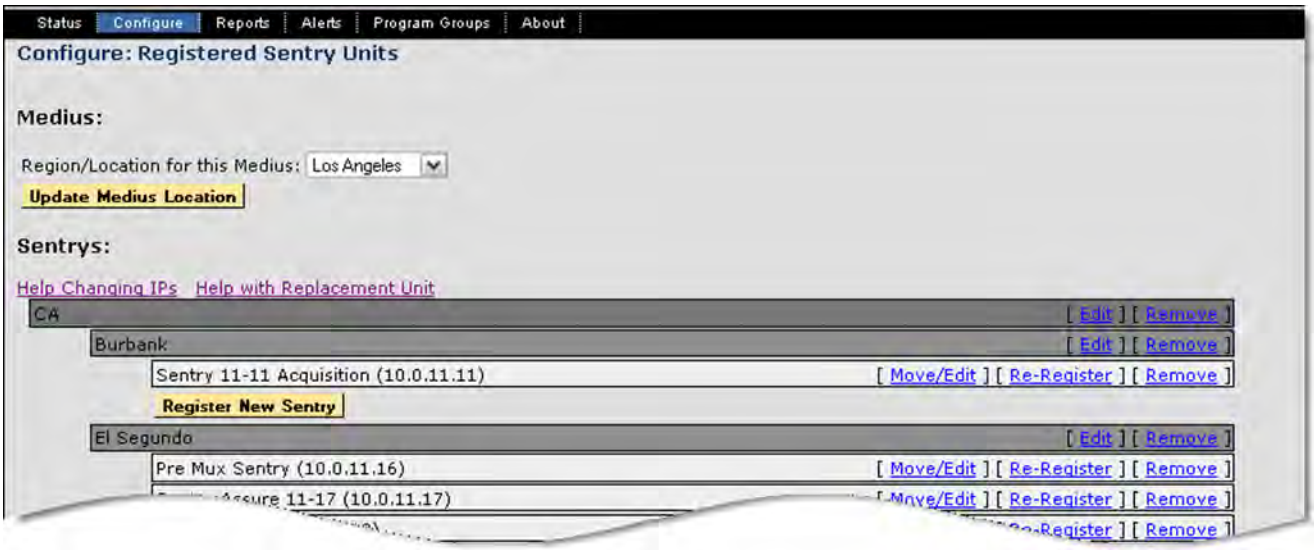



**Figure 33: Removing a Sentry**

2. The Sentry will return a **Warning** message stating that you are about to remove a Sentry unit.

3. To proceed, select **Yes, remove the Sentry**.

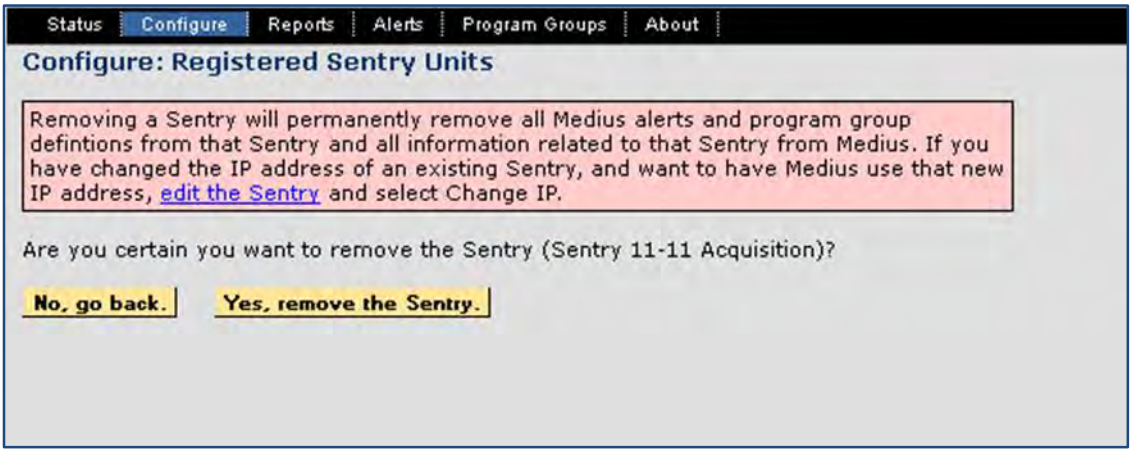



**Figure 34: Removal Confirmation screen**

4. The **Registered Sentrys** list will return showing that the selected Sentry has been successfully removed.

## Move/Edit Sentry

**NOTE:** ***After completing an edit to a Sentry, you will be prompted to re-register the unit. Re-registering initially clears all alerts and program definitions for that Sentry and then automatically reinstalls them after the re-registration.***

1. Select the **Move/Edit** button from the **Registered Sentrys** page.

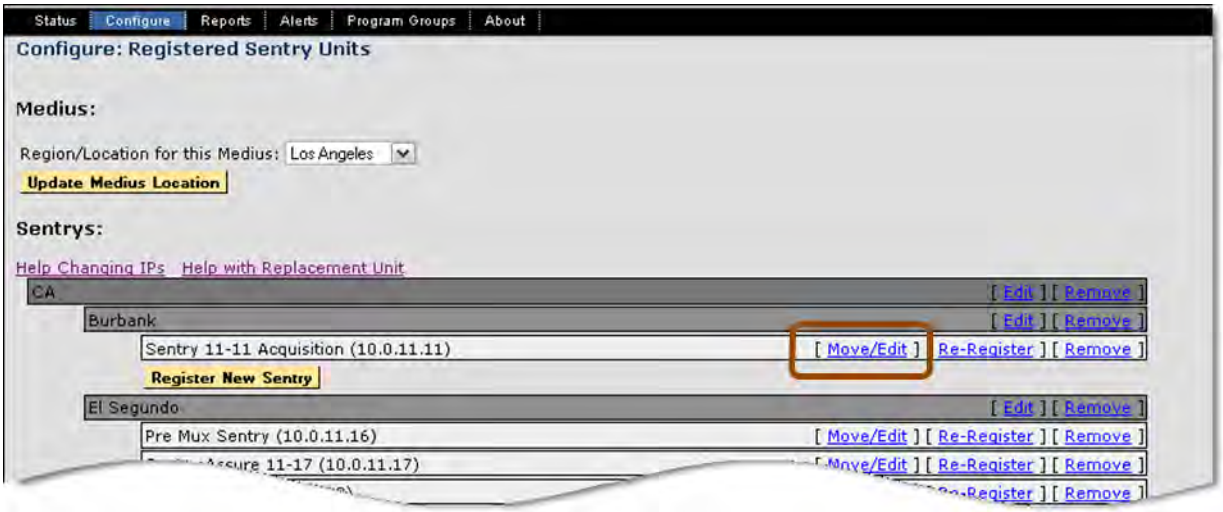



**Figure 35: Move or Edit a Sentry**

2. From the **Edit Sentry** page, select the fields you wish to edit and make your desired changes. You may change the **IP address**, the **Display** name and the **Region/Location**.

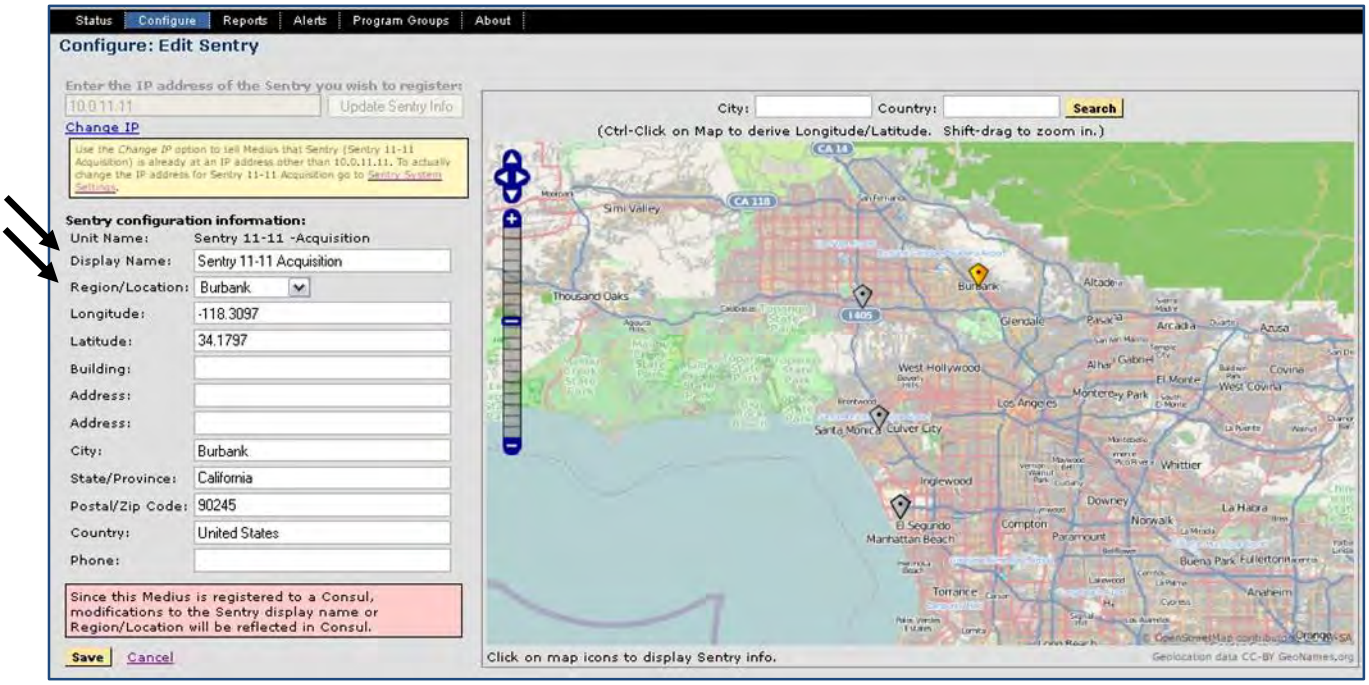



**Figure 36: Editing Sentry Information**

1. Select **Save**.

2. You will next be prompted to re-register the Sentry. To continue, select **Yes, re-register the Sentry.**

## *Set Longitude/Latitude for a Sentry*

1. Select the **Move/Edit** from the **Registered Sentrys** page.

2. If you know the exact longitude and latitude, you may enter them manually.

3. If you do not know the longitude and latitude, enter the city and country that they are located in to the search field.
    a. A street view map will appear. Place the Sentry on this map and the longitude and latitude will automatically backfill.

## Register New Sentry

1. Select **Register New Sentry** from the **Registered Sentry Units** main page.

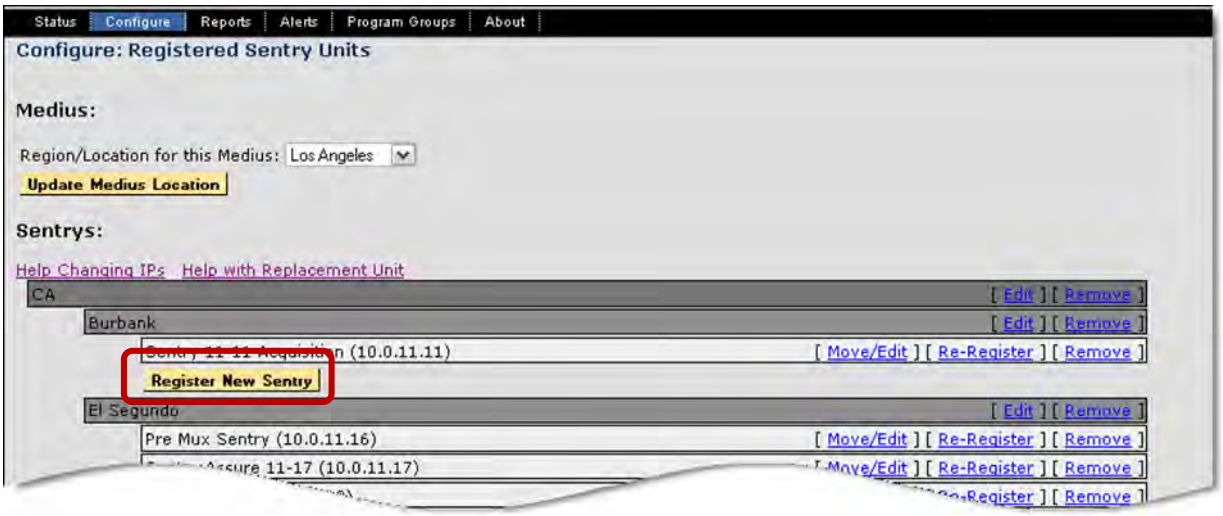



**Figure 37: Register a New Sentry**

2. Fill in the IP address to start the registration process.

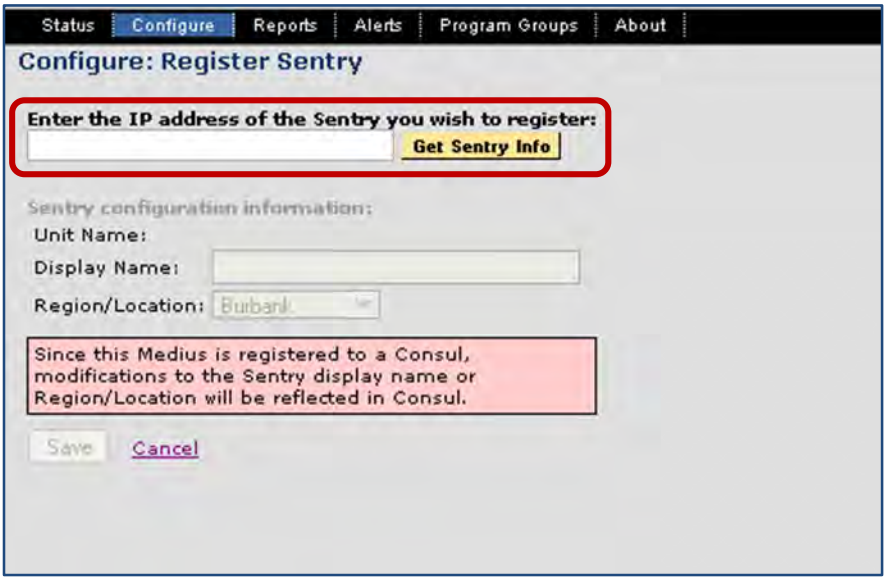



**Figure 38: Enter the IP information**

## Change IP Address

1. Select **Medius: Registered Sentrys** on the **Configure** drop-down menu.
2. Select **Move/Edit.**

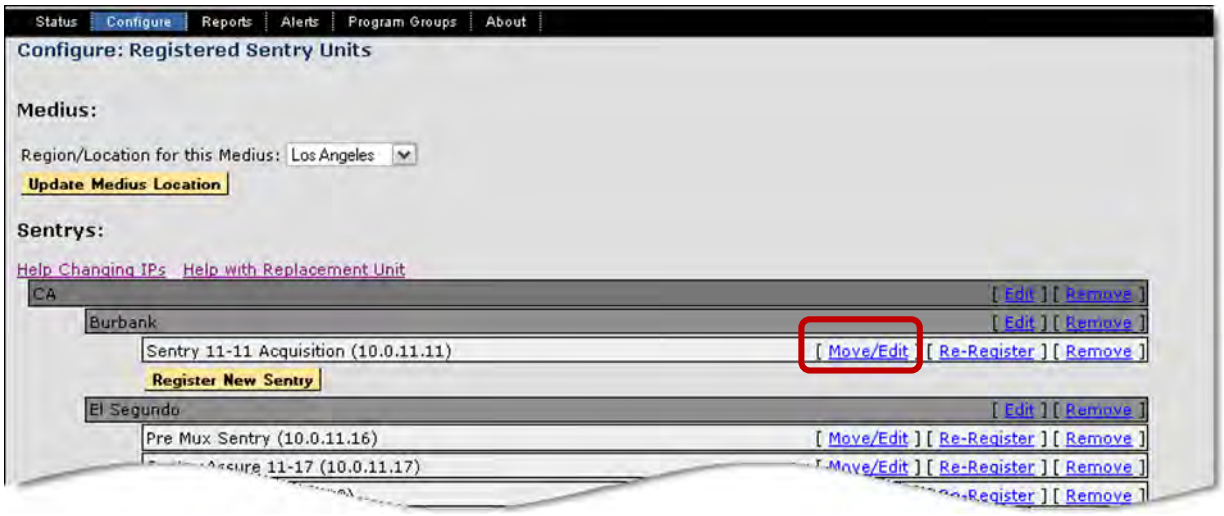



**Figure 39: Selecting Move/Edit to change an IP address**

3. Select **Change IP**. The current IP address in the yellow box will change from gray to black font.

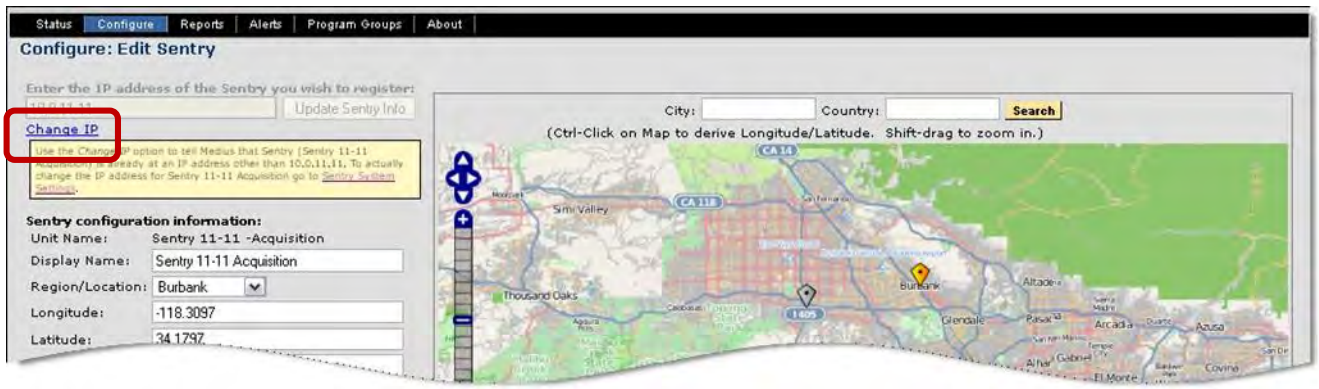



**Figure 40: Selecting Change IP**

4. Enter the new IP address.

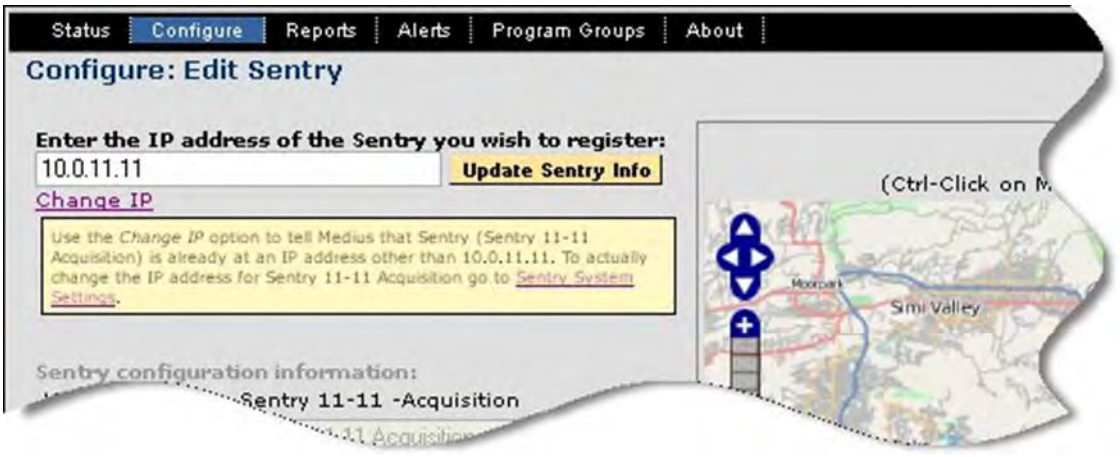



**Figure 41: Entering the IP address**

5. Select **Update Sentry Info**.

6. Select Save to finish updating this Sentry.

7. Repeat steps for each Sentry you wish to update.

## Add New Location

The user may categorize the Sentrys by Geographical location or by another logical category (i.e. **Ad Insertion** and **MUX groups**) for ease of use.

1. From the **Registered Sentrys** page, select **Add New Location**.
2. Enter the name of the **New Location**.
3. Select **Add**.

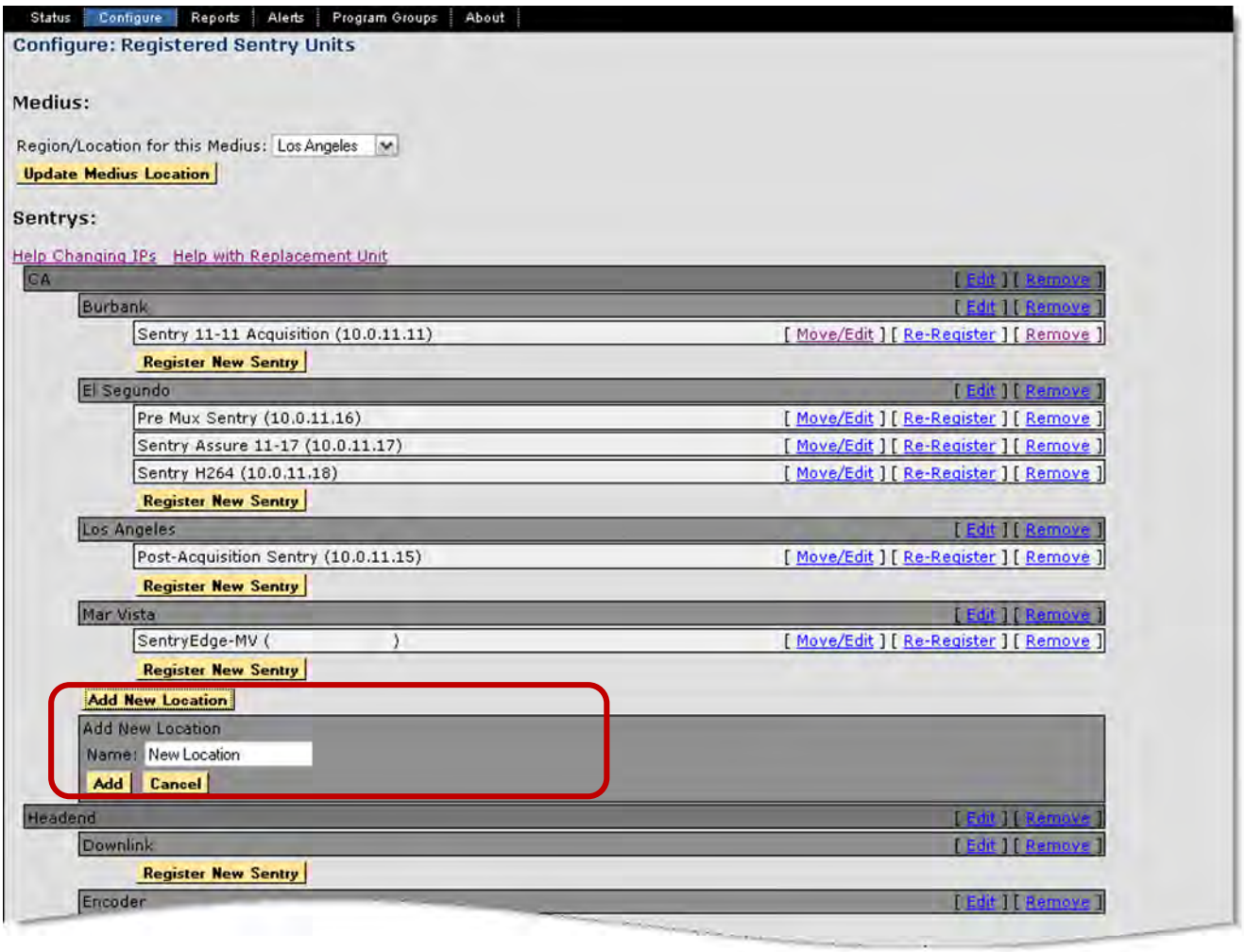



**Figure 42: Add a New Location**

4. Complete fields as needed and select **Save**.

### Add New Region

The user may further categorize the Sentrys by region for ease of use.

1. From the Registered Sentrys page, **Select Add New Region**.
2. Enter the name of the **New Region**.
3. Select **Add**.

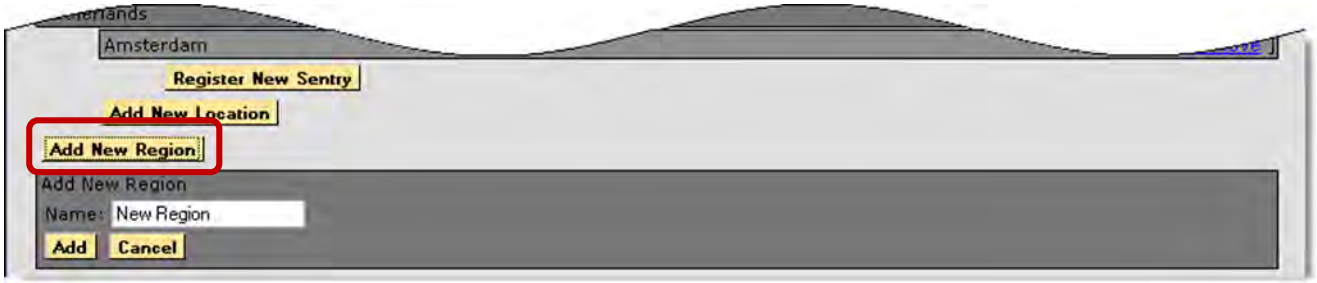



**Figure 43: Add a New Region**

4. Complete fields as needed and select **Save**.

# Dashboard Graphs

**Dashboard Graphs** allow you to create or delete graphs you see on the **Program Dashboard** screens.

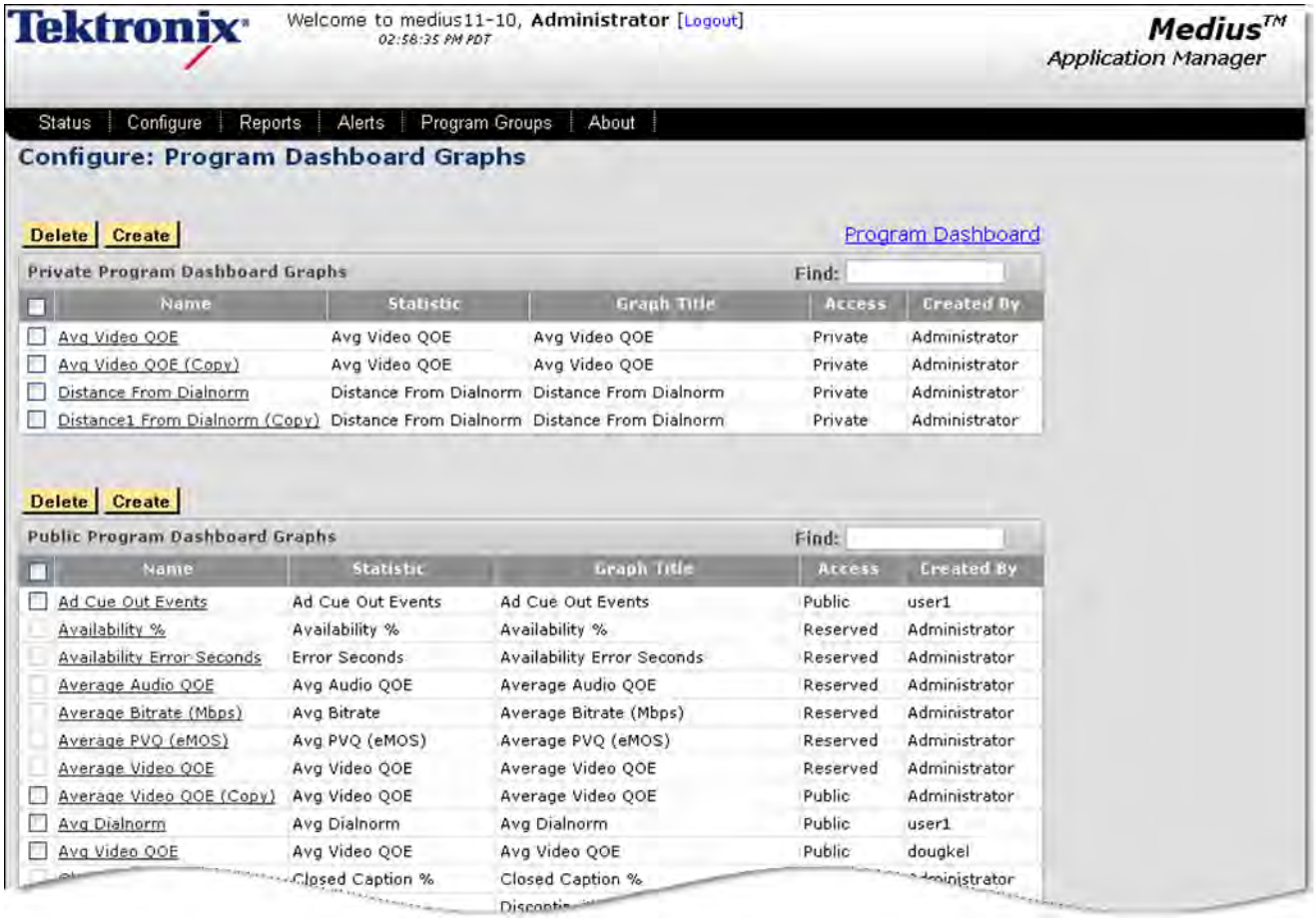



**Figure 44: Program Dashboard Graphs**

## Create a Dashboard Graph

1. Select **Create** from the **Dashboard Graphs** page.
2. Set the **Statistics**, **Ranges** (shown as bars on the graph) and **Color** as needed.
3. Enter the name of the new graph.
4. Select Save **Graph**.

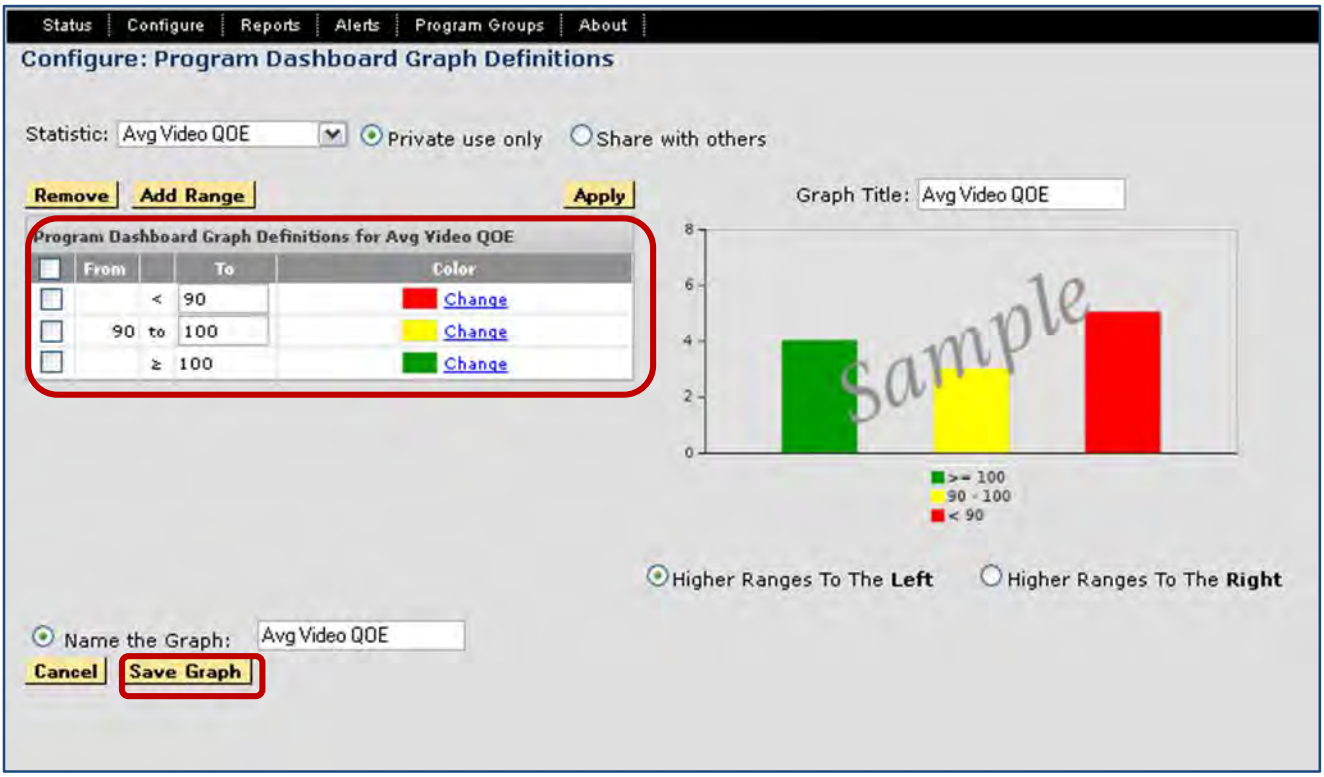



**Figure 45: Creating Dashboard Graphs**

# Medius Users

Medius supports any number of users. Users are defined by two categories of privileges: **Administrator** and **Regular User**.

An **Administrator** can make system wide configuration changes and is the only one who can create user accounts.

A **Regular User** cannot add users, set alerts or make any changes to the system wide settings.

Medius also supports a non-interactive automation interface for determining device status, downloading measurement data and upgrading various system settings. You may select which users have access to these features through the **Configure: Medius Users** screen.

## Access Medius Users

1. Select **Medius Users** from the Configure drop-down menu.

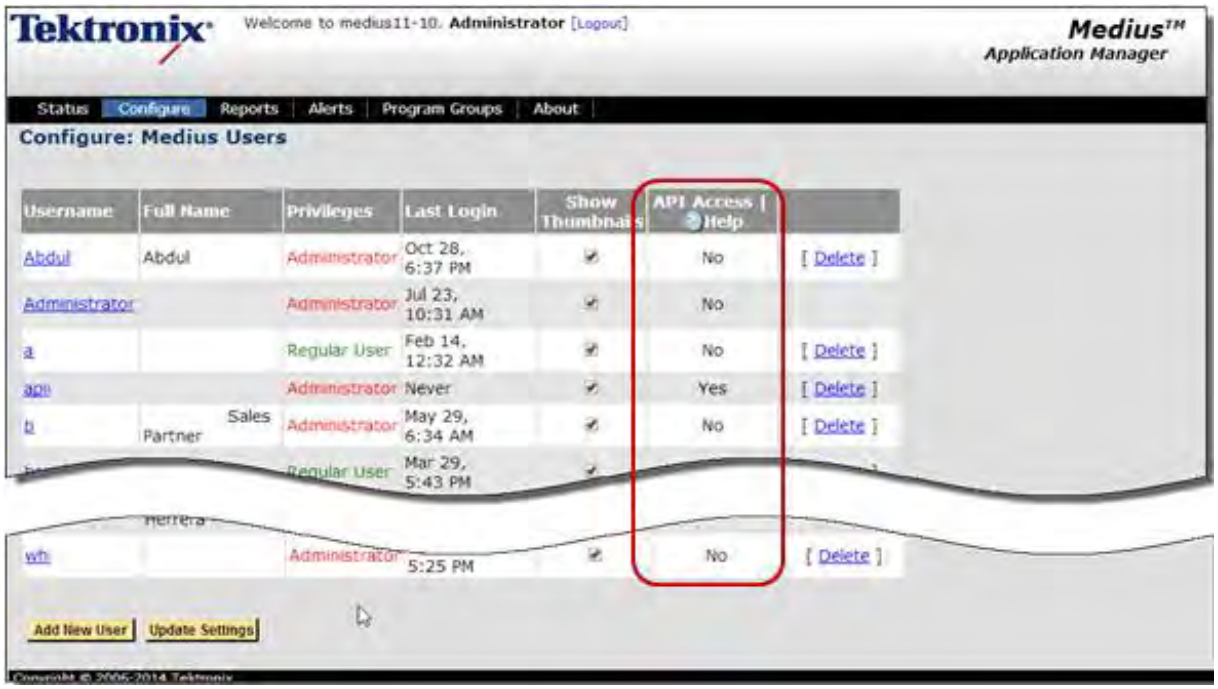



**Figure 46: Manage Users Page**

2. Select **Add New User**.

3. Enter the new user's information.

4. Any information that is highlighted in red is required.

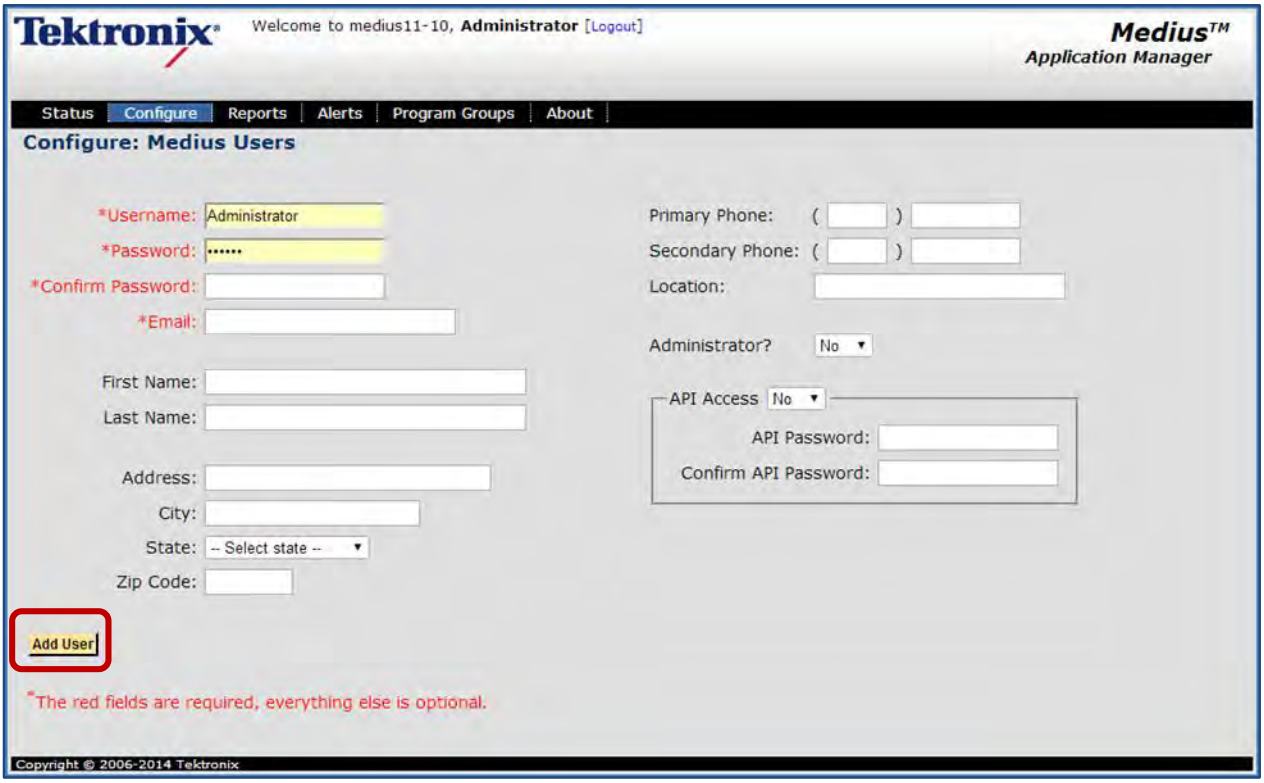



**Figure 47: Configure User options including API Access**

5. Select **Add User** when finished.

***CAUTION: All Administrator passwords must be kept in a secure location. If you forget your Administrator password, contact Tektronix Customer Support***

## Delete a User

**CAUTION***: Once users are deleted, there is no recovery.*
***To reinstate a user, you must manually add them back to the system.***

1. To delete a user select **Delete** located to the right of a user name.

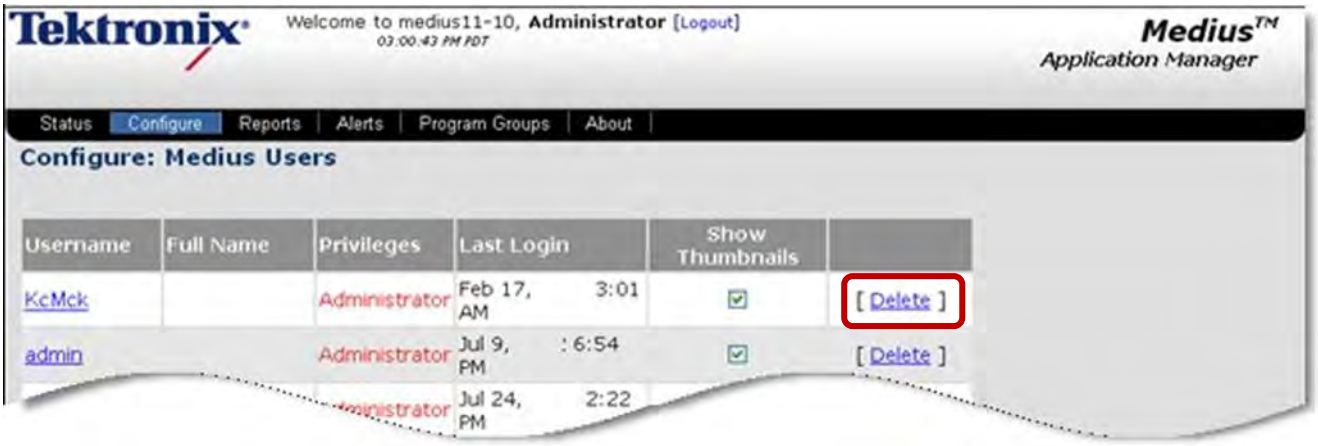



**Figure 48: Deleting a User (at your own risk!)**

2. You will be presented with a confirmation dialog. Select **Yes**, **delete this user** to completely remove the user from the system.


**Figure 49: Delete User Confirmation**

## Modify a User

1. To modify a user, select a name from the **Username** column.

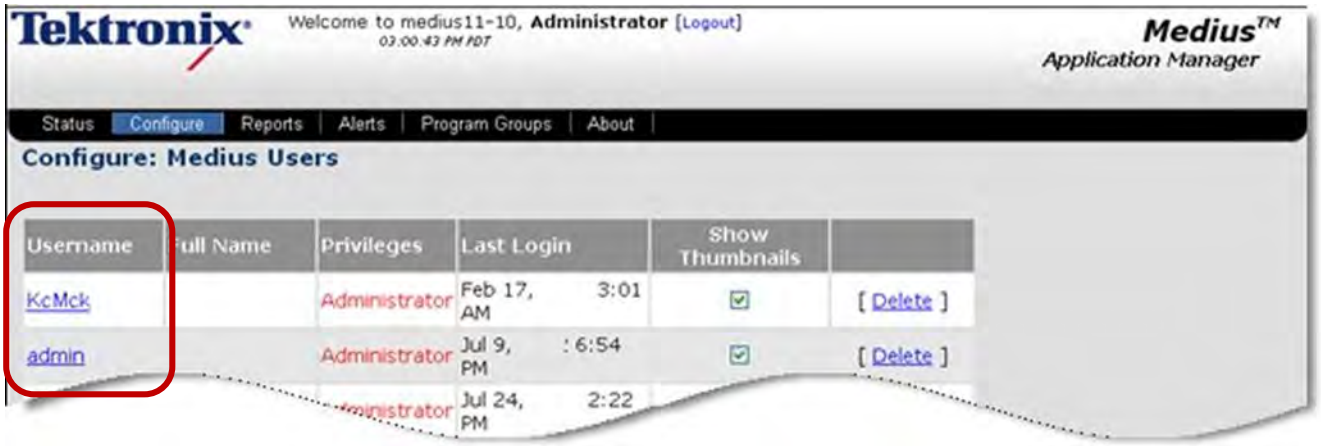



**Figure 50: Select a Username**

2. From the updates page, change the user information as needed.

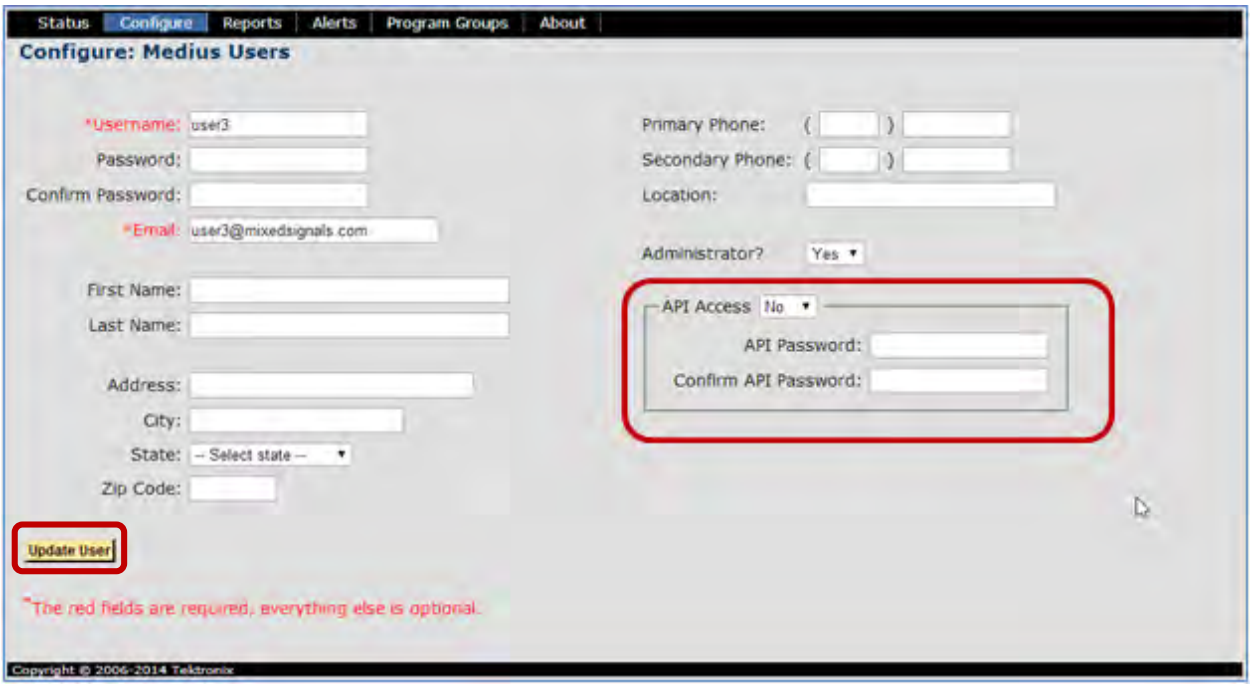



**Figure 51: Updating User options, including API Access**

3. When finished, click **Update User** to save the changes.

# Medius System Settings

**Users may change a host of basic settings on Medius such as Network, Time, Locale, Location, Consul and Maintenance.**

## Access System Settings

1. **Select Medius System Settings from the Configure drop-down menu.**

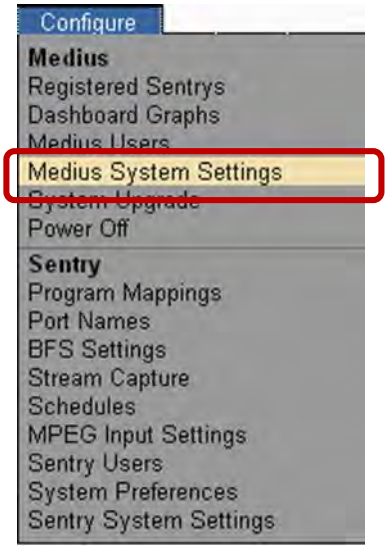



**Figure 52: Medius System Settings**

2. Select the tab of the function you wish to review or change.

# Network settings tab

## SNMP Settings

**SNMP (Simple Network Management Protocol)** provides the ability to send traps, or notifications when one or more conditions have been met. Sentry supports up to four destinations for SNMP traps.

---

**NOTE***: If changing the IP address on a registered Sentry, please refer to the Changing the IP Address section of this manual.*

---

## To set the SNMP Trap

In the **Primary trap host** field, enter the IP address of the SNMP manager that will receive the trap. There is a limit of between 1 and 50 alerts per trap.

1. From the **Network** tab, review or change the information as needed.

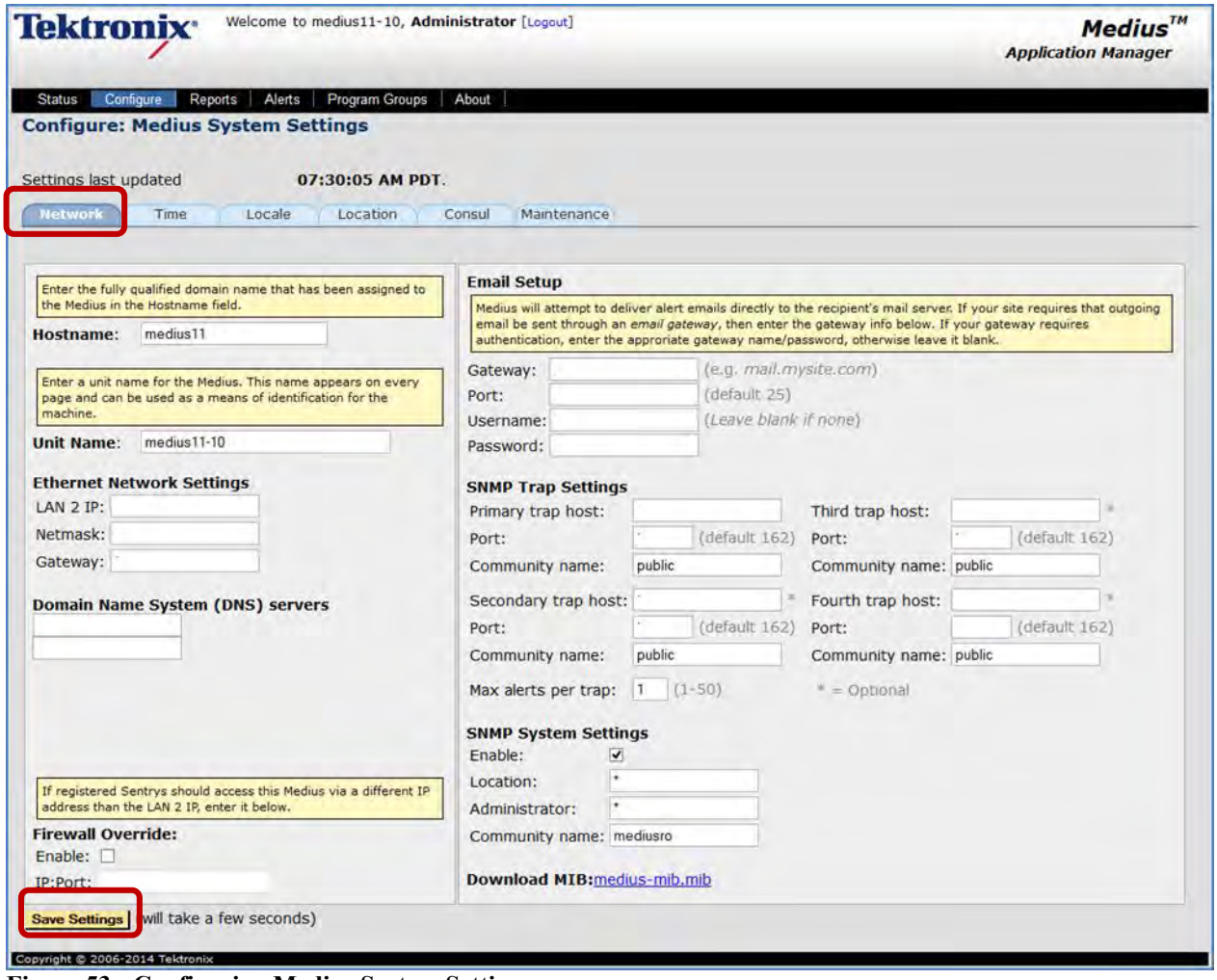



**Figure 53: Configuring Medius System Settings**

2. Select **Save Settings** when finished.

## Time tab

1. From the **Time** tab, enter or review the information as needed.

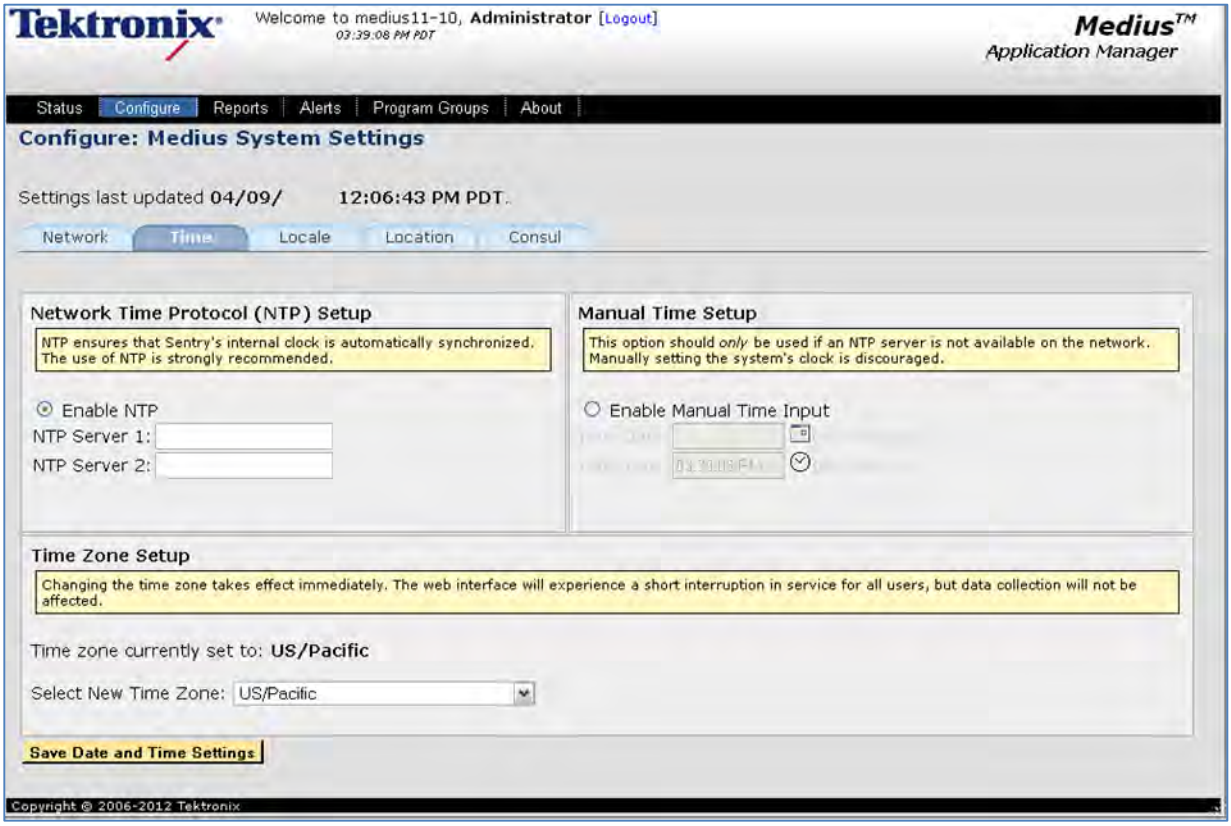



**Figure 54: Configuring Medius Time Settings**

2. Select **Save Date and Time Settings** when finished.

## Configure Locale tab

**Locale** is used for STD auto-naming function as well as XDS display. This allows you to choose what character set to use in the interface. Example:. Western alphabet or Chinese Kanji.

1. From the **Locale** tab, complete or review the information as needed.


**Figure 55: Configuring Locale Settings**

2. Select **Save Locale Settings** when finished.

## Location tab

The **Location** tab allows you to set and record the exact location of a Medius.

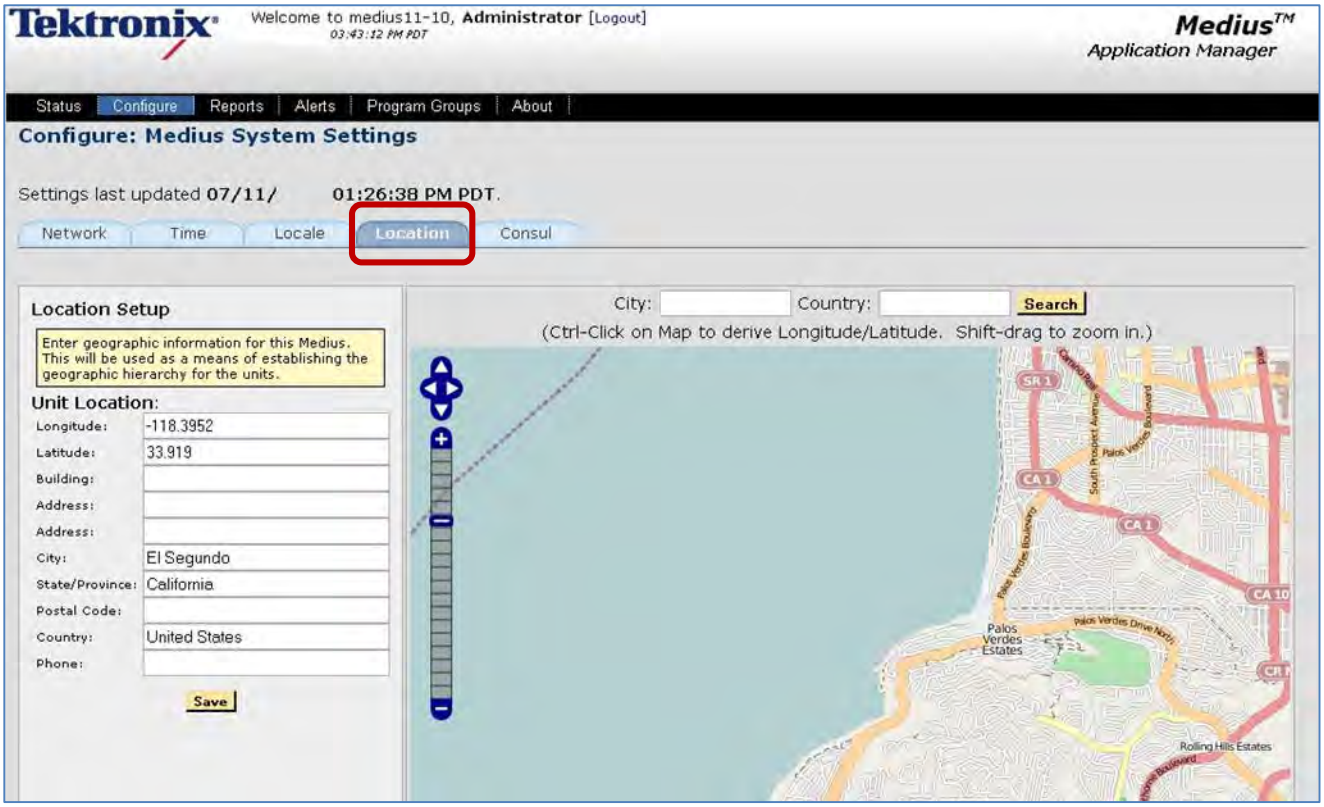



**Figure 56: Location tab**

## Consul tab

The **Consul** tab allows you to view the **Consul** registration information for a Medius.

You may register or unregister **Consuls** here as well.


**Figure 57: Consul tab**

## Maintenance tab

The **Maintenance** tab allows you to set a time range to stop alert notifications from being generated when you are doing maintenance in the system. This stops unnecessary emails from going out to your designated mailing lists. These settings can also stop SNMP traps from going out and thus may prevent false alarms in any systems monitoring Sentry alerts.

Storage of alerts for **Alert History** and **Alert Analysis** reporting will be retained during these periods, but no notifications will be sent.

1. Select **Configure: Medius System Settings** from the main menu.
2. Select the **Maintenance** tab.

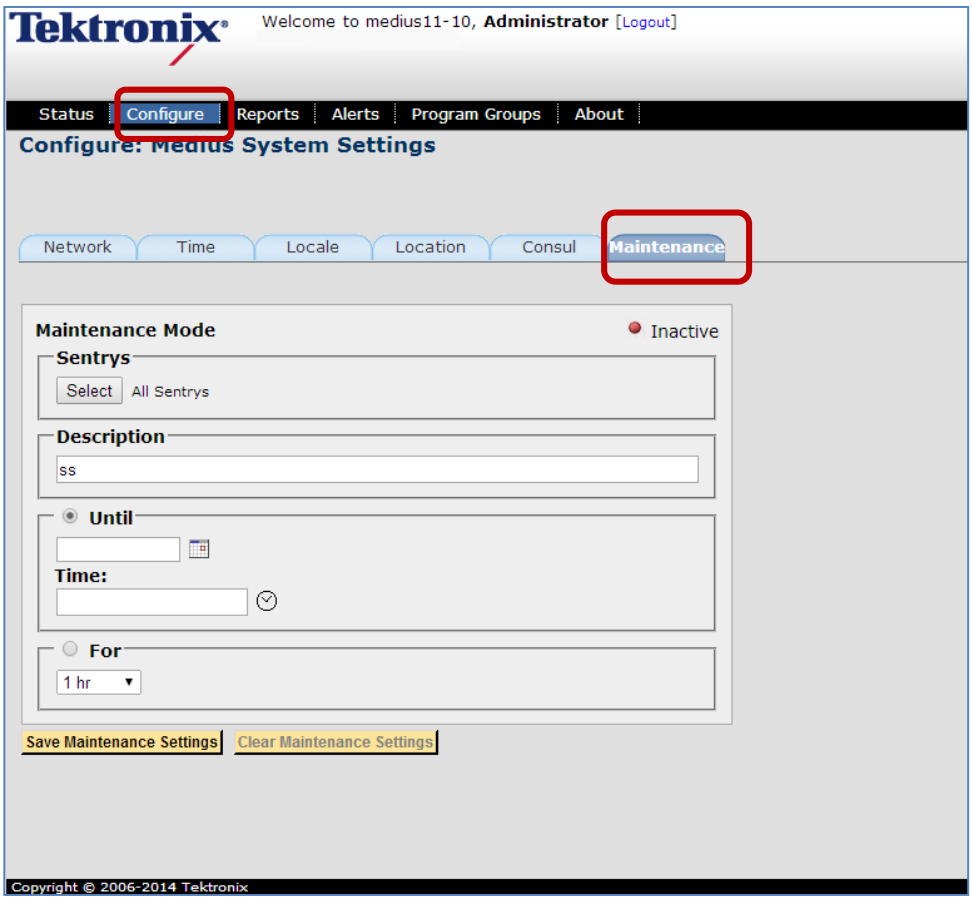



**Figure 58: Maintenance Mode settings**

3. Select the needed Sentrys.

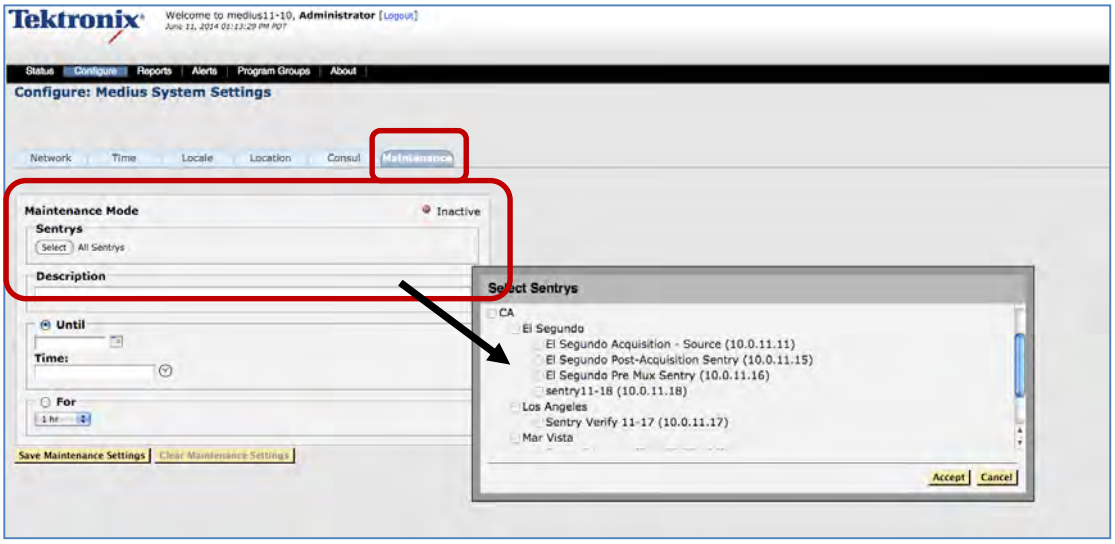



**Figure 59: Select the Sentrys**

4. Enter a **Description** of the mode you are setting. This is an optional step and will show up in the banner on the bottom right section of all **Maintenance Mode** pages.

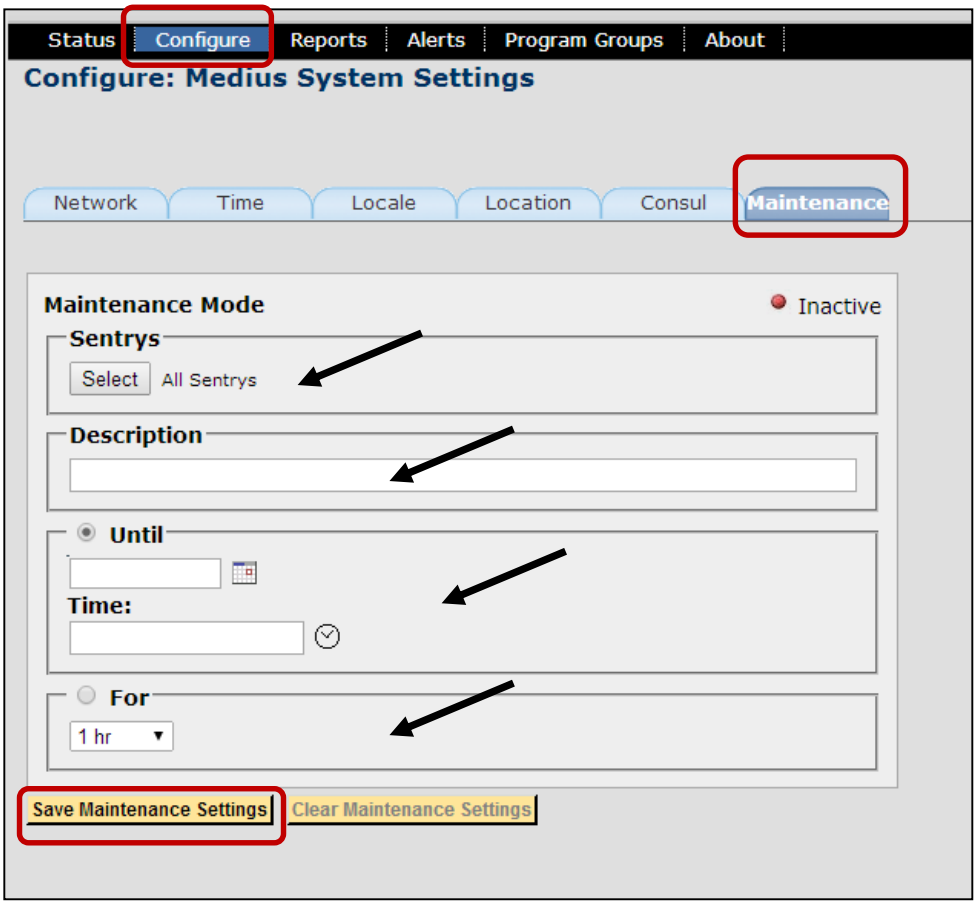



**Figure 60: Save the Maintenance settings**

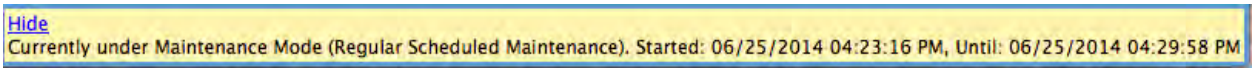



**Figure 61: Maintenance Mode banner**

5. Either choose a maintenance mode stop date and time length **–or–** select a time length for the maintenance period (from 5 minutes up to 7 days).

# System Upgrades

**System Upgrade** allows system **Administrators** to remotely upgrade their Medius and Sentrys to the latest software releases. The upgrade can be performed by anyone with administrator access.

**System Upgrade** will also allow you to view a log of past updates, including their name and date applied via the History tab.

If your support contract is current, you can perform a Medius and Sentry system upgrade. To get started, you must first obtain an upgrade package from Tektronix. Please call your Tektronix Service Representative for more details.

---

**NOTE***: If your Sentry unit is registered to a Medius:*

---

1. You will need to upgrade your Sentry, and all other Sentrys registered to that Medius through the **Medius System Upgrade**.

2. You may upgrade all your Sentrys at one time, via the Medius.

---

**WARNING***: During a Medius or Sentry system upgrade, all monitoring will be suspended and users will not be able to access the Sentry pages. Choose your upgrade time accordingly.*

---

## Medius Upgrading Procedure

1. Select **System Upgrade** from the Configure drop-down menu.

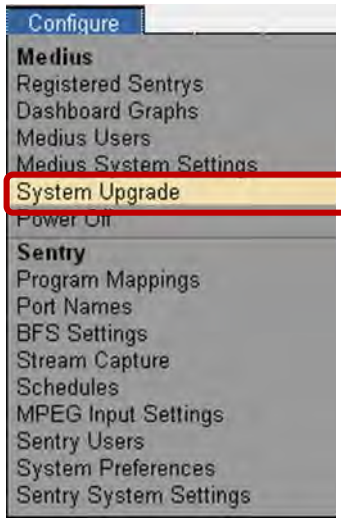



**Figure 62: System Upgrade**

2. The resulting page allows the user to either **Upgrade** or see a **History** of past upgrades for both the Medius unit and all Sentrys assigned to it. Stay on the Upgrade tab for this procedure.

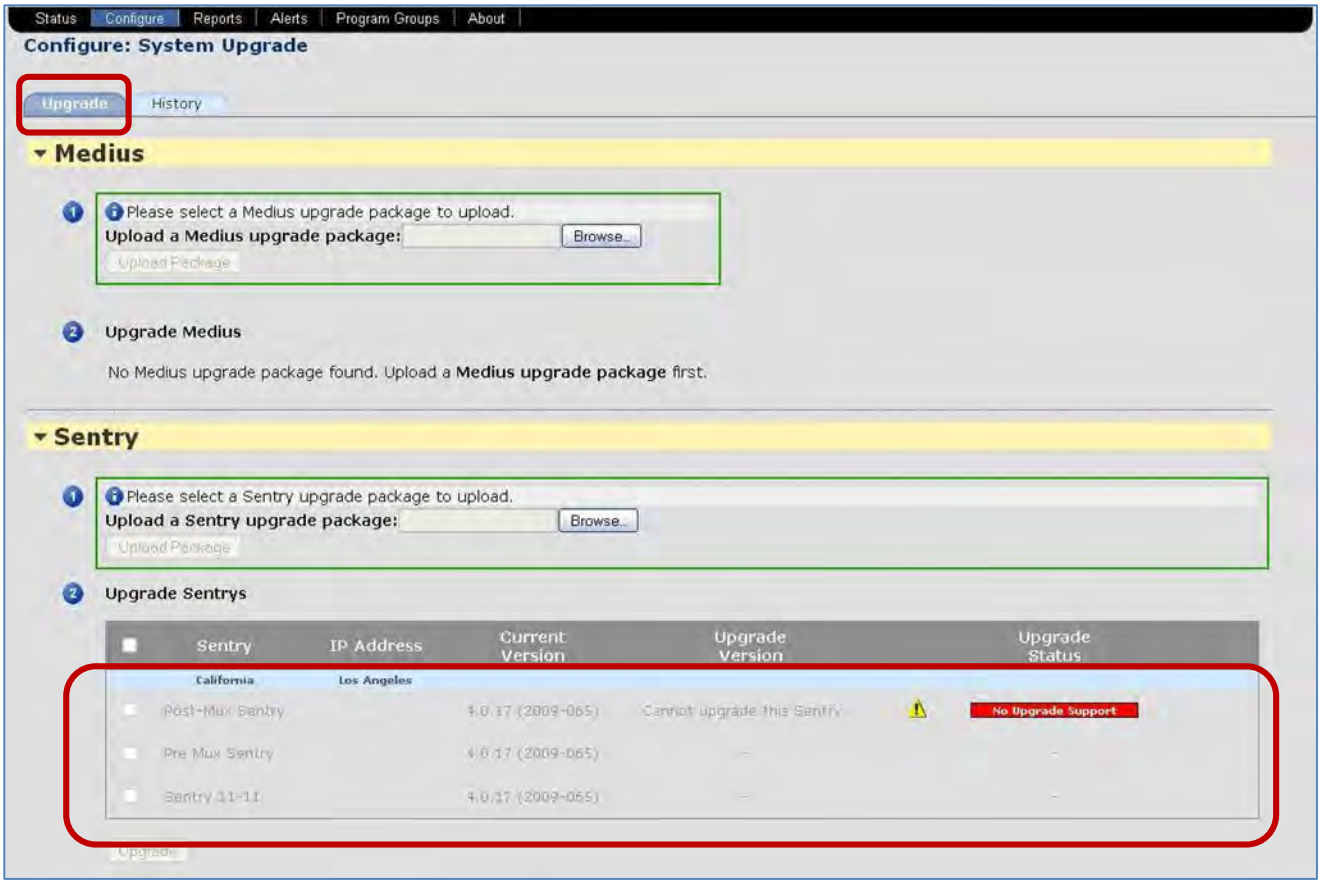



**Figure 63: Configuring a System Upgrade (No Upgrade Support screen) - Contact Customer Support**

**Section** 1

3. Once you have received a valid Medius upgrade package from Tektronix, navigate to this file by clicking the **Browse** button and selecting your upgrade package file from its current location.

4. Next, click **Upload Package** to upload the upgrade package file to Medius.

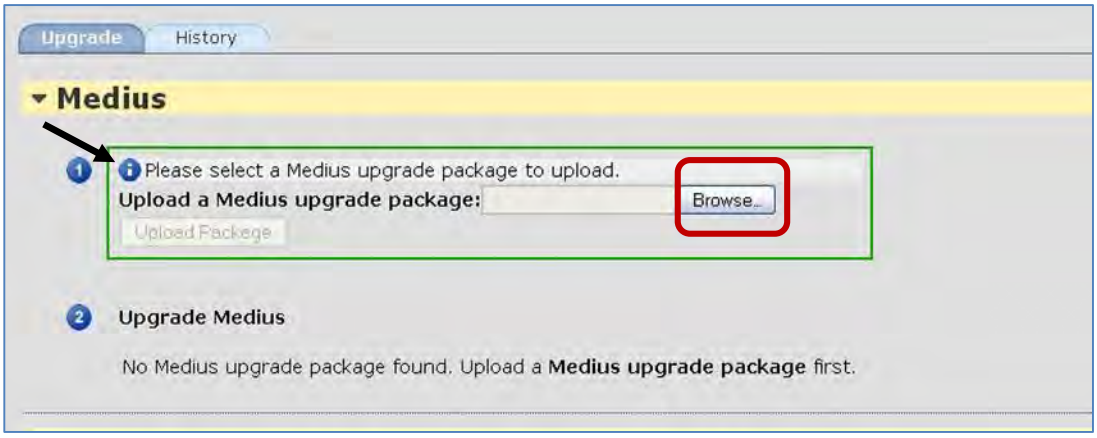



**Figure 64: System Upgrade welcome screen**

5. Medius will perform an automatic check to make sure this is a valid upgrade for the system. Once it has been validated, the following screen will appear:


**Figure 65: Upgrade package confirmation and Upgrade Medius button**

**Section** 2

6. Upon returning to the **System Upgrade** screen, you should see another ✔ next to **Section** 1.
7. **Section** 2 will show the upgrade information and an arrow leading from the old version to the new version. Select **Upgrade Medius** to continue.
8. The next screen will warn you that during a Medius system upgrade, all monitoring will be suspended and users will not be able to access the Sentry pages. If you wish to continue with the upgrade, click **Yes, Upgrade Medius.**

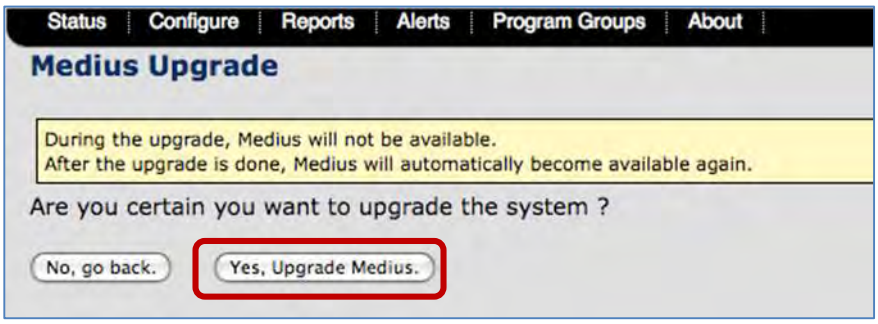



**Figure 66: Upgrade confirmation**

9. You will then be routed to the **Upgrade Status** page. From here, you will be able to monitor the progress of the **Upgrade**. A ✔ will appear next to each completed **Section**. The number of steps varies from upgrade to upgrade.

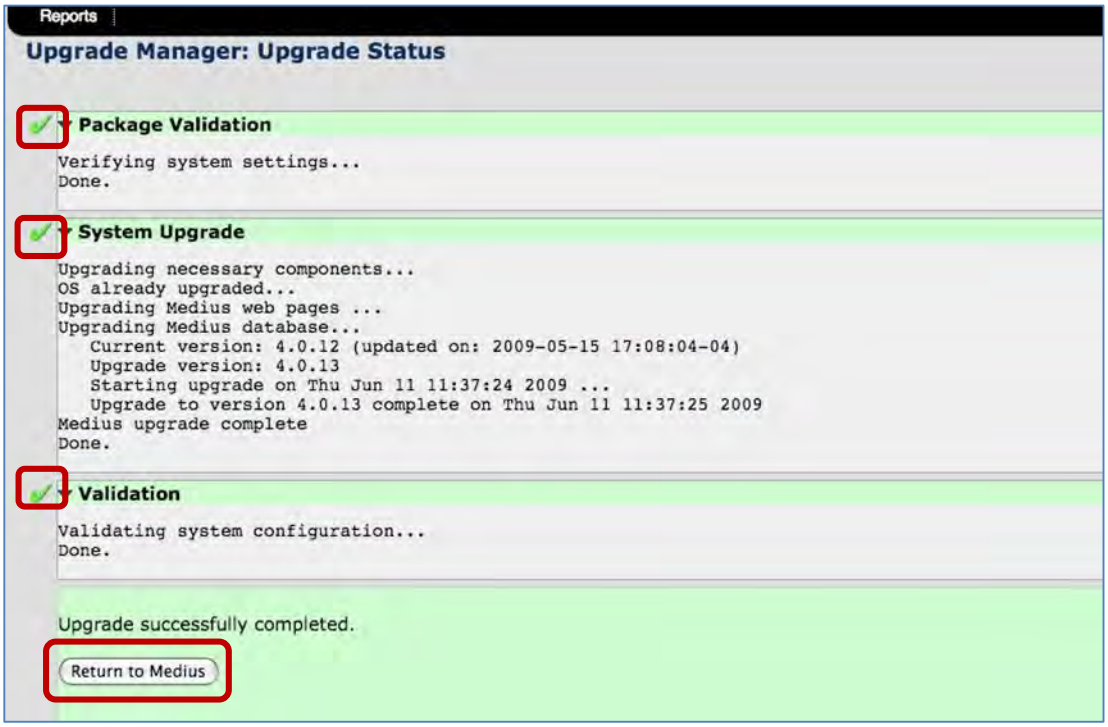



**Figure 67: Successful Upgrade**

10. The system will begin upgrading and will display the status. If the system upgrades successfully, all system monitoring will resume automatically and users will be able to access the Medius pages.

11. Click **Return to Medius** to return to the main Medius pages.

## Upgrade Sentrys through the Medius

You may apply one upgrade to multiple Sentry units via the Medius.

To upgrade standalone Sentrys, please see the Sentry Manual.

1. Begin by choosing **Medius: System Upgrade** from the **Configure** drop-down menu.

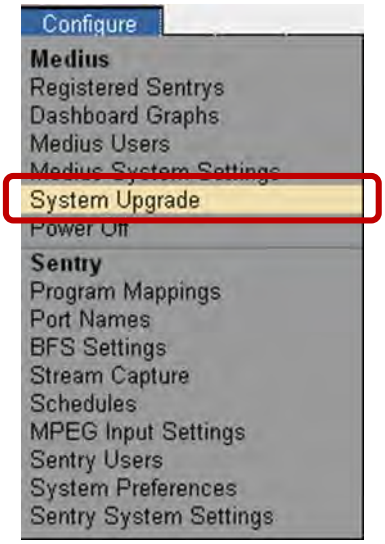



**Figure 68: System Upgrade**

2. The resulting page allows the user to either **Upgrade** or see a **History** of past upgrades for both the Medius unit and all Sentrys assigned to it. Stay on the **Upgrade** tab for this procedure.
3. Scroll down to the Sentry section of the page.


**Figure 69: System Upgrade welcome screen for Sentry**

**Section** 1

4. Once you have received a valid Sentry upgrade package from Tektronix, navigate to this file by clicking the **Browse** button and selecting your upgrade package file from its current location.

5. **Next, click Upload Package to upload the upgrade package file to Sentry.**

6. Sentry will perform an automatic check to make sure this is a valid upgrade for the system. Once it has been validated, the following screen will appear:

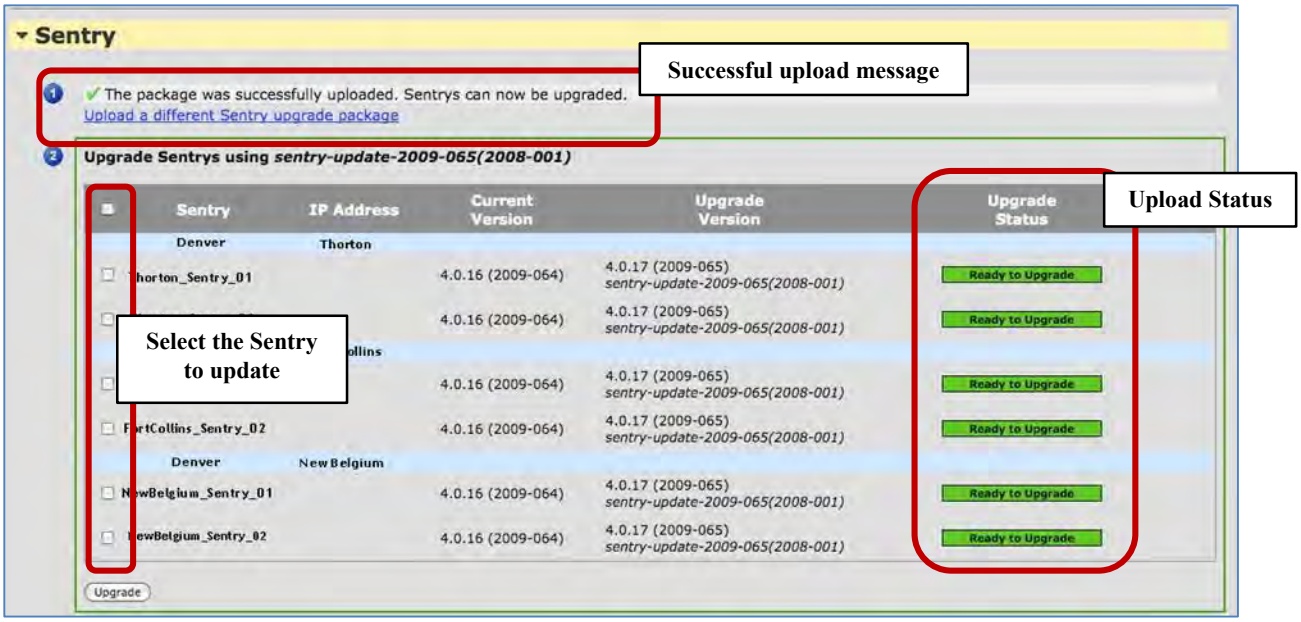



**Figure 70: Upgrade Sentry button**

**Section** 2

7. Next, select the Sentrys you wish to update from the list.

---

**NOTE***: Sentrys with a red upgrade status are not eligible for upgrade packages. Talk to your Tektronix representative for more details.*

---

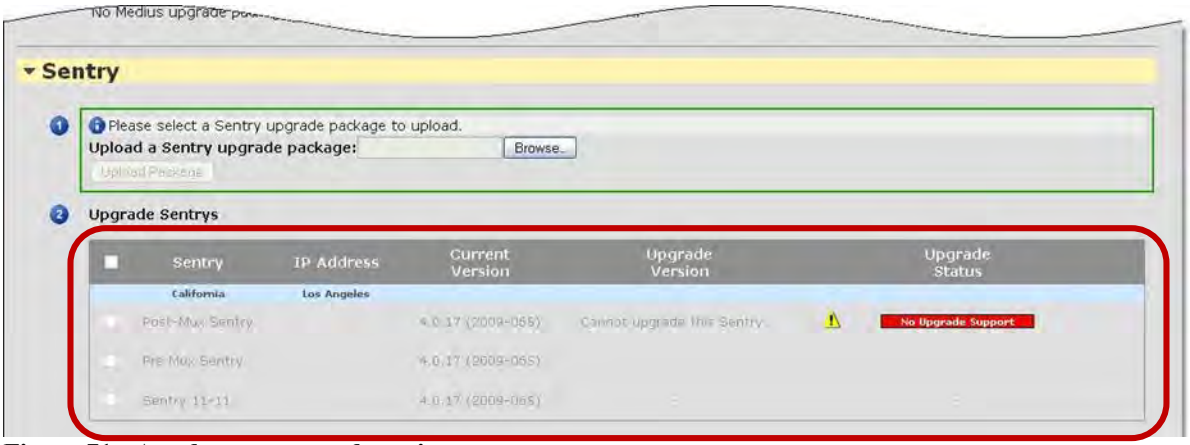



**Figure 71: A red status upgrade notice**

8. Upon returning to the **System Upgrade** screen, you should see another ✔ next to **Section** 1.
   a. **Section** 2 will show the upgrade information and an arrow leading from the old version to the new version.

9. Select **Upgrade Sentry** to continue.

10. The next screen will warn you that during a Sentry system upgrade, all monitoring will be suspended and users will not be able to access the Sentry pages. If you wish to continue with the upgrade, click **Yes, Upgrade Sentry.**

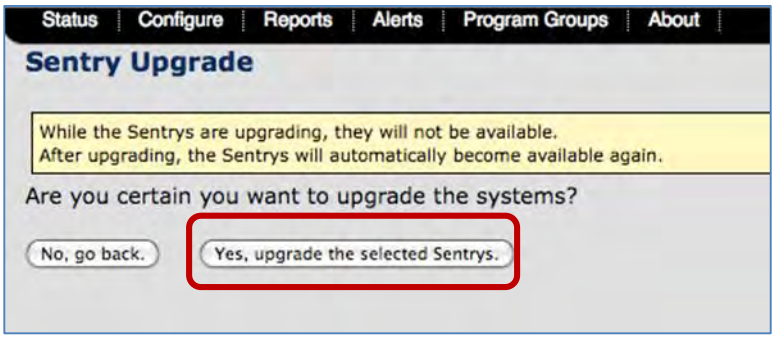



**Figure 72: Upgrade confirmation**

11. You will then be routed to the **Upgrade Status** page. From here, you will be able to monitor the progress of the **Upgrade**. A ✔ will appear next to each completed step. The number of steps varies from upgrade to upgrade.

12. You will also see a "**1 of 3, 2 of 3**" type message as the upgrades are applied to each selected Sentry.

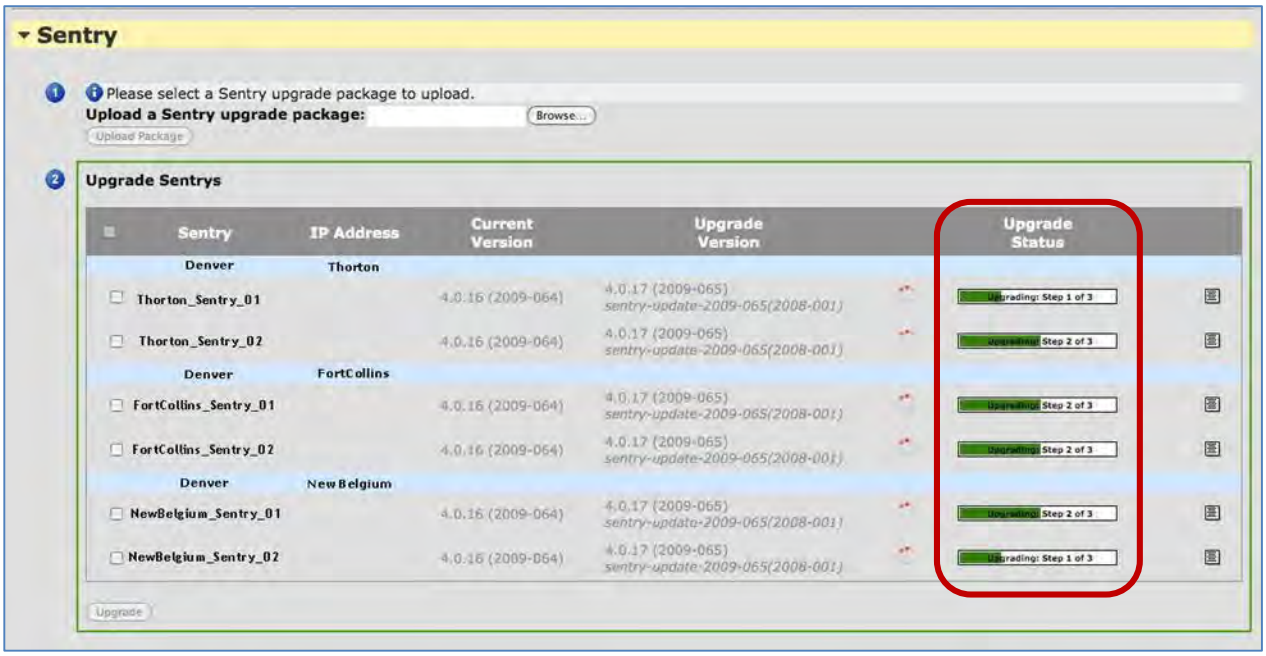



**Figure 73: Upgrade in progress**

13. If the system upgrades successfully, all system monitoring will resume automatically and users will be able to access the Sentry pages.
14. Click **Return to Sentry** to return to the main Sentry pages.

## Upgrade Errors for Medius

If any type of error occurs during the upgrade or the pre-verification steps of the upgrade, you will see the following:

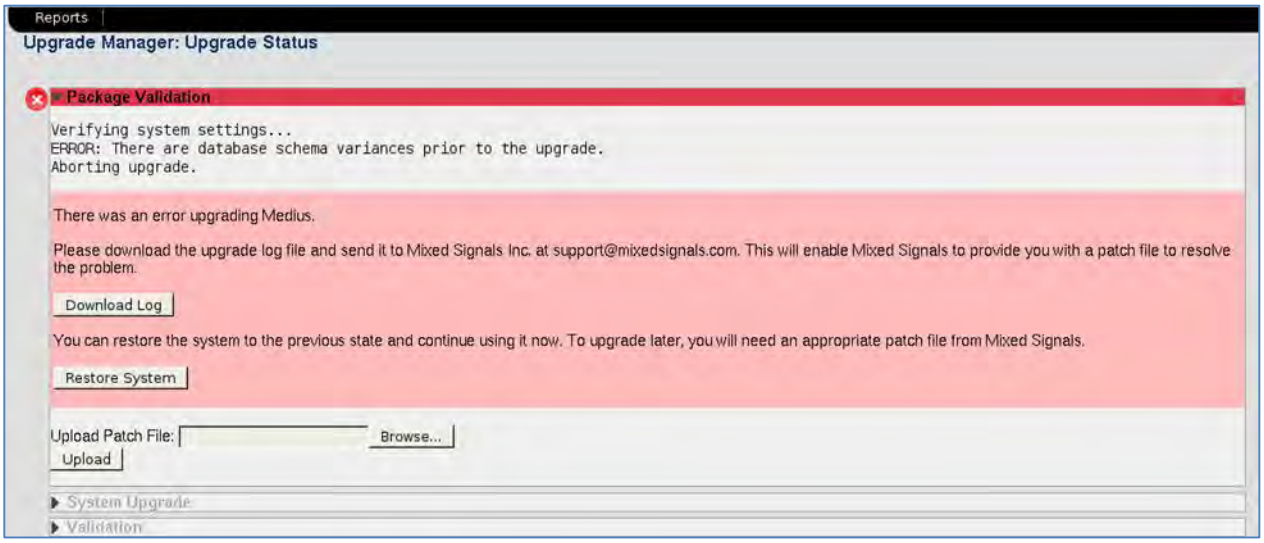



**Figure 74: Upgrade Error**

You will need to contact a Tektronix Support representative to troubleshoot and resolve the issue.

In order to help your support representative resolve the problem, you will need to download the upgrade log and provide it to Tektronix. This log file is an encrypted file with detailed information that is critical to Tektronix to being able to diagnose your problem.

1. Click **Download Log** to save the upgrade log file.

There are two types of errors you might encounter:

### *Recoverable error*

This is generally an error that happens in the pre-verification step. Such errors are recoverable, in that you can roll back the upgrade and return to the pre-upgrade state. If the error is Recoverable, you can click the Restore System button.

For such an error, providing the upgrade log to your Tektronix representative is still crucial, because Tektronix will still need to provide you with a patch in order for you to complete your upgrade.

### *Error Requiring a Patch*

If the error is not a recoverable error, it will require a patch from Tektronix to resolve. At this point, you must provide your Tektronix support representative with the upgrade log file. After diagnosing the problem, Tektronix will provide you with an upgrade patch file.

## Upload Error Patch File

1. To upload the patch file click **Browse** and select the file.

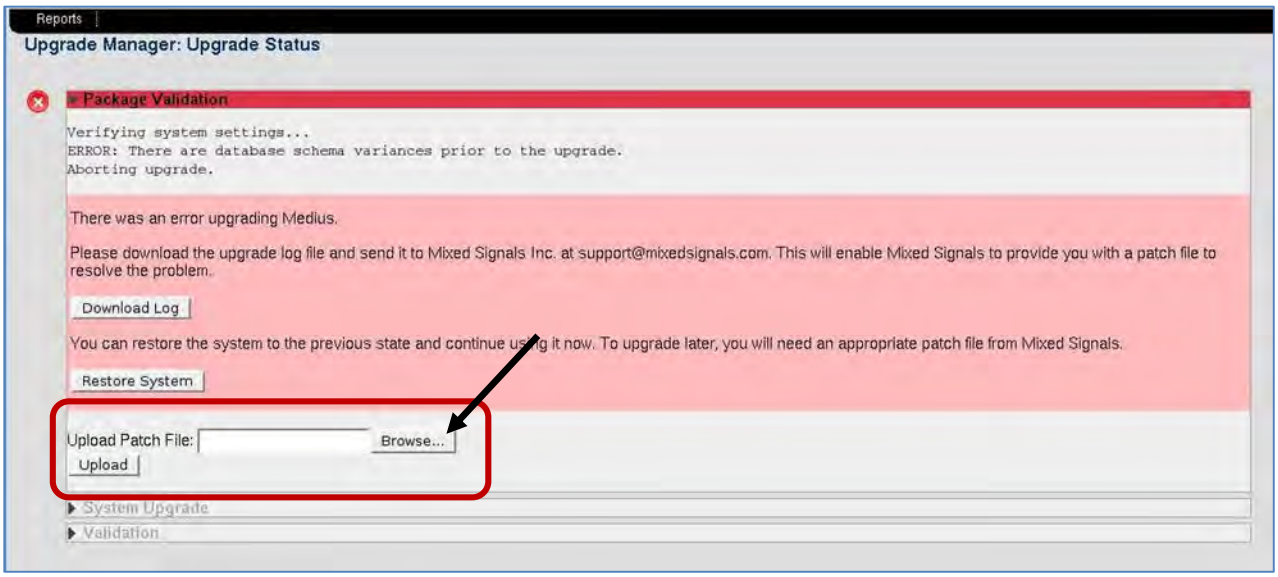



**Figure 75: Uploading the patch**

2. Next, click **Upload**.

3. If this is a valid patch for this Sentry at this time, you can click **Apply Patch** to apply the patch and resume the upgrade.

---

**NOTE**: ***If you didn't download the upgrade log from this page, you can do so later by clicking the History tab on the System Upgrade page.***

---

## Upgrade errors for Sentry via Medius

1. If any type of error occurs during the upgrade or the pre-verification steps of the upgrade, you will see the following:

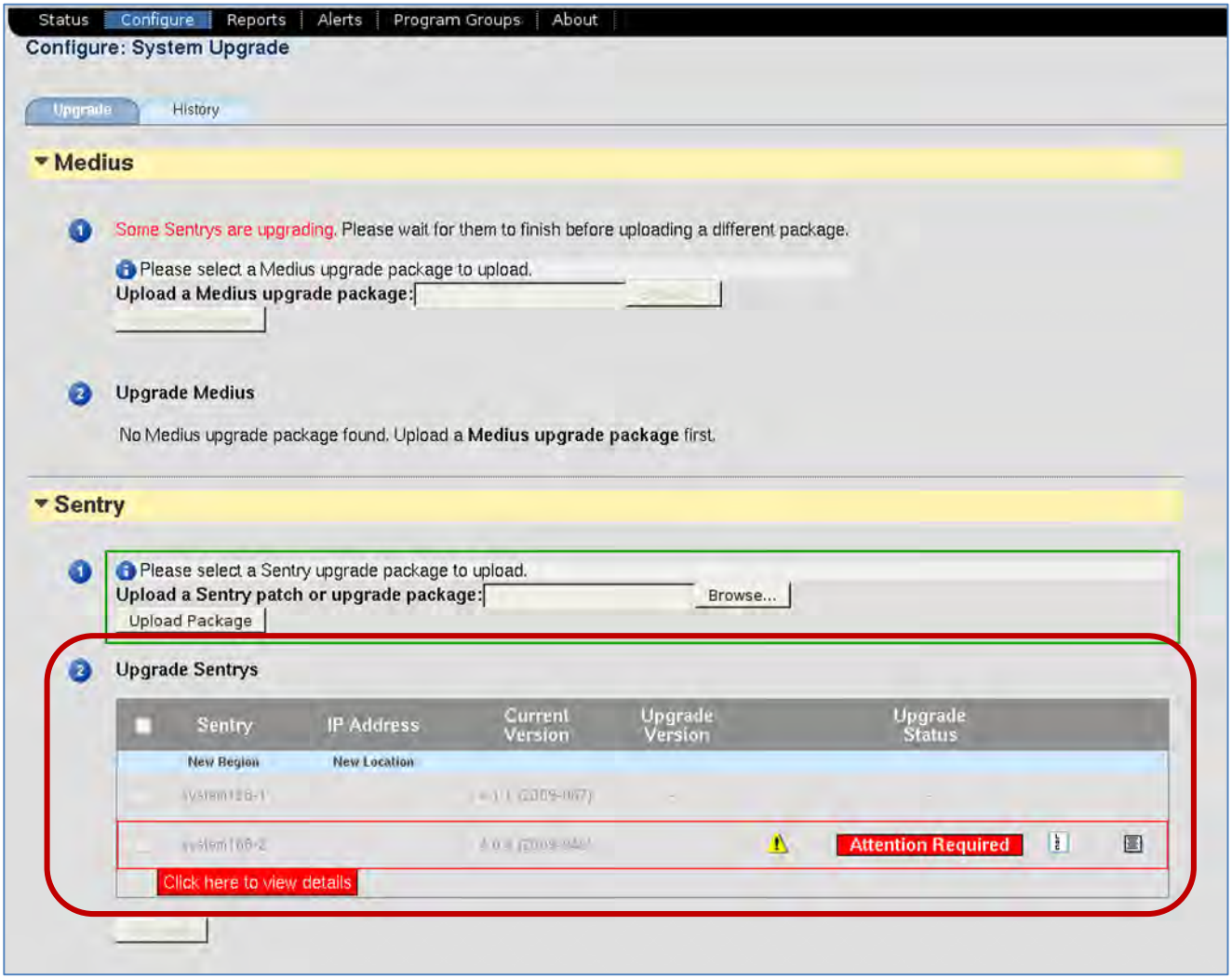



**Figure 76: Sentry Upgrade Errors**

2. Select the **Click here to view details** button to see a more detailed report of the failure.

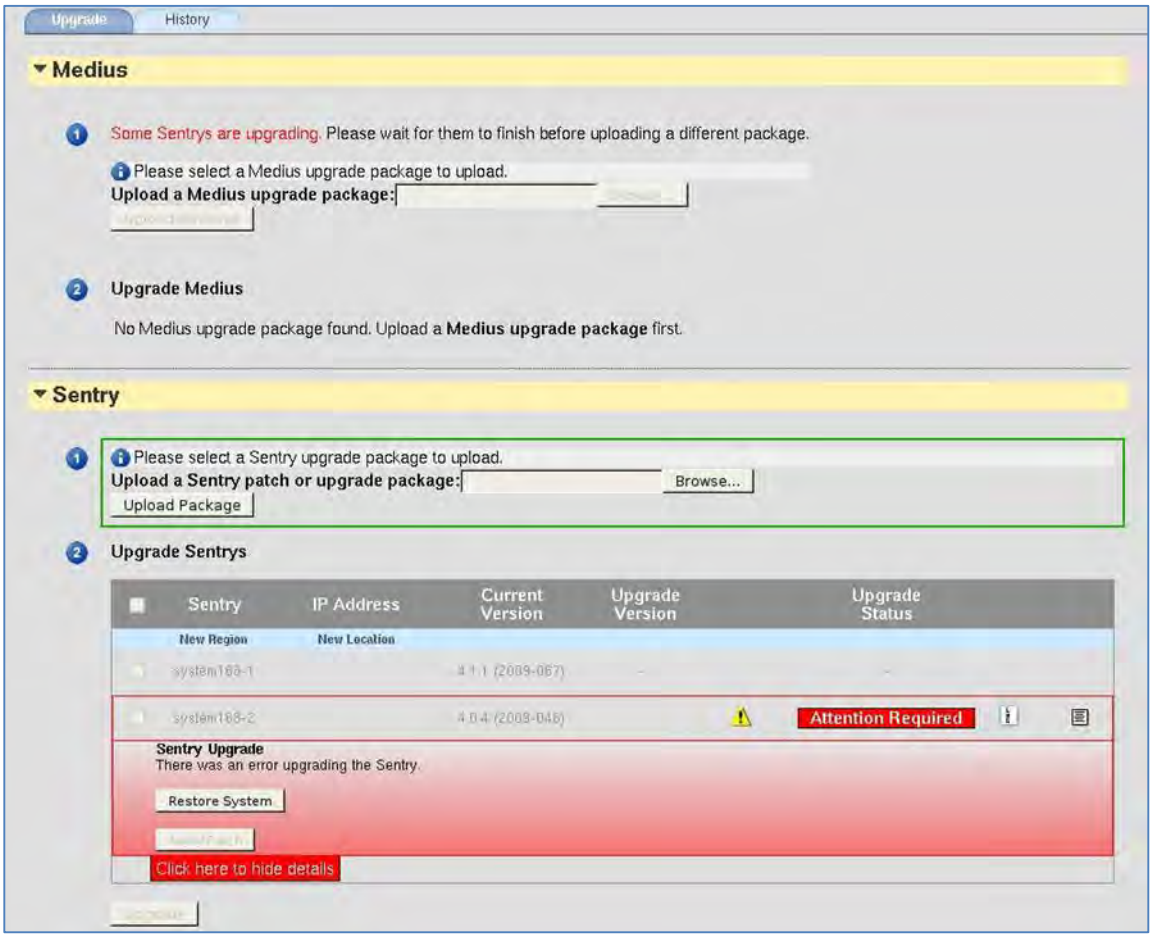



**Figure 77: Upgrade error details**

## Upgrade History

The **History** tab on the **System Upgrade** page will display a history of all system upgrades performed.

To access, select **System Upgrade** from the **Configure** drop down menu and then select the history tab.

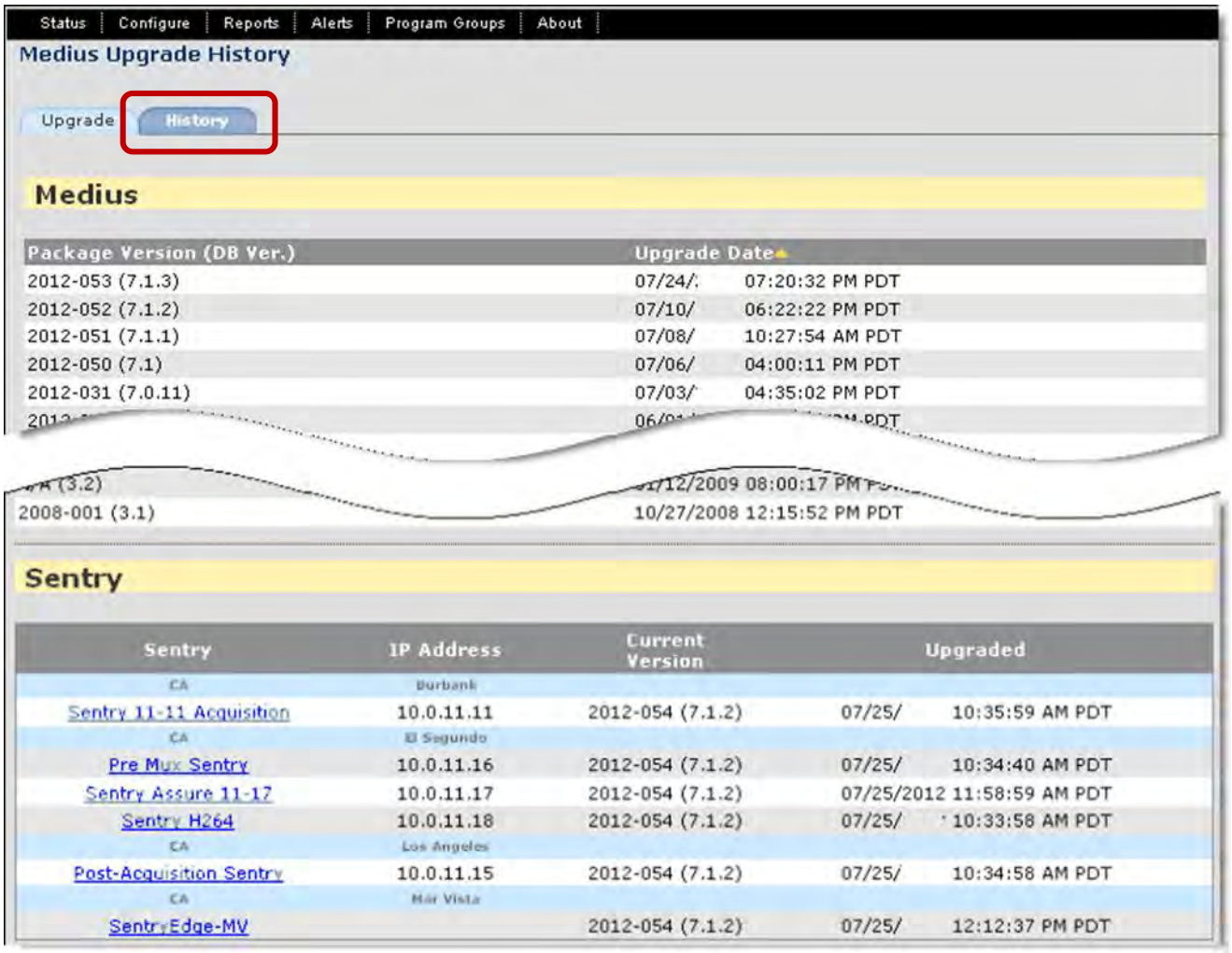



**Figure 78: Upgrade History tab**

If there are any errors with the current upgrade, you can access the upgrade log from this page.

# System Diagnostics

**System Diagnostics** allows you to perform basic tests for connectivity and communications between Medius and other devices.

## Email Diagnostics

- **Send:** Send a test email
- **View Email Log:** View the email servers log file
- **Clear Email Queue:** Delete unsent emails on the email queue

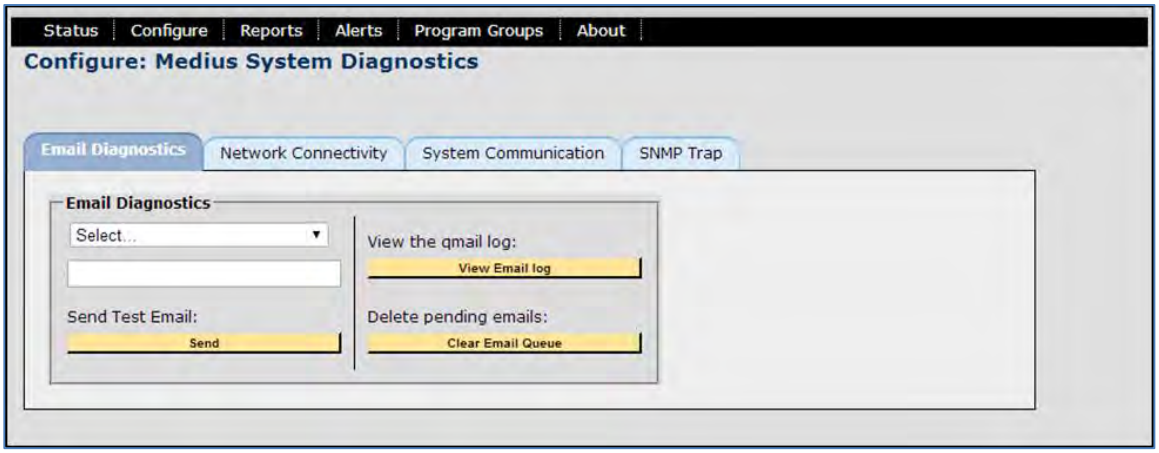



**Figure 79: Email Diagnostics tab**

## Network connectivity

- **Ping Server**: ICMP ping to validate connectivity
- **Traceroute:** Preform a path trace to host
- **Check Web Response: P**erforms WGET to the host specified on TCP port 80
- **DNS Verification: C**hecks to see if DNS servers are reachable and working

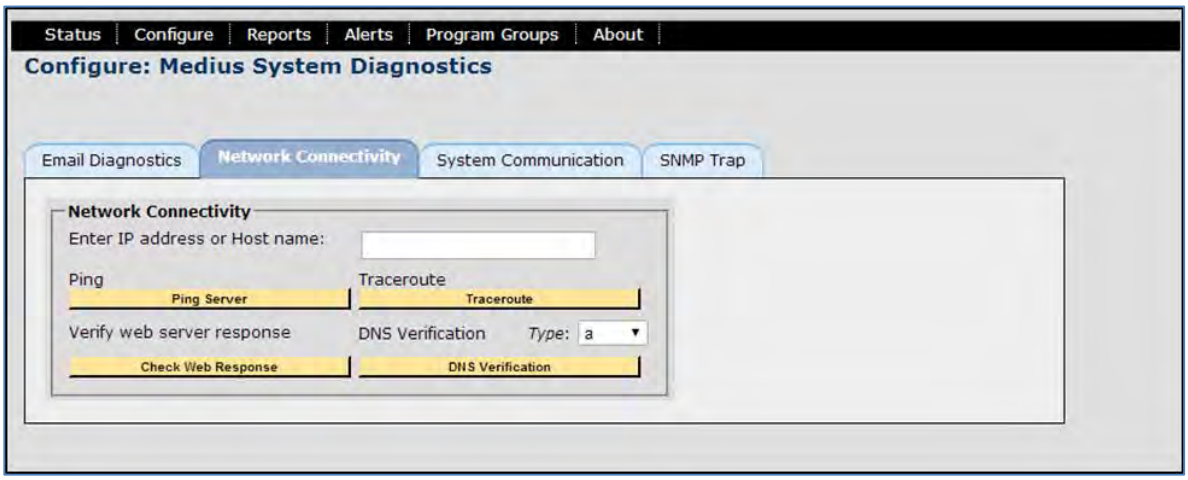


**Figure 80: Network Connectivity tab**

## System communications

Validates communication between Sentry and Medius is working.

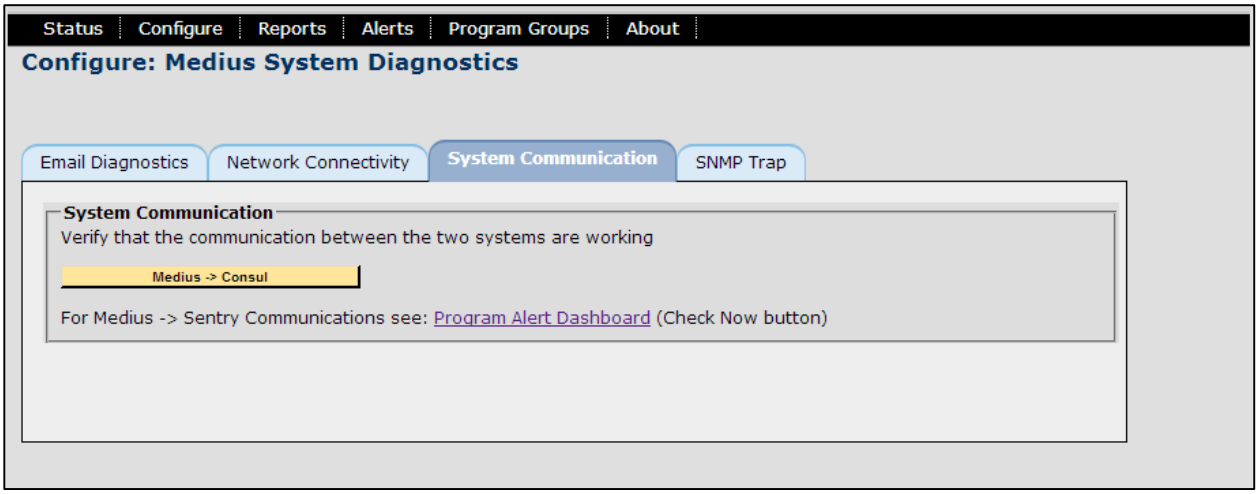



**Figure 81: System Communications tab**

## SNMP trap

Sends a test SNMP trap to verify the SNMP host on the **System Settings** page.

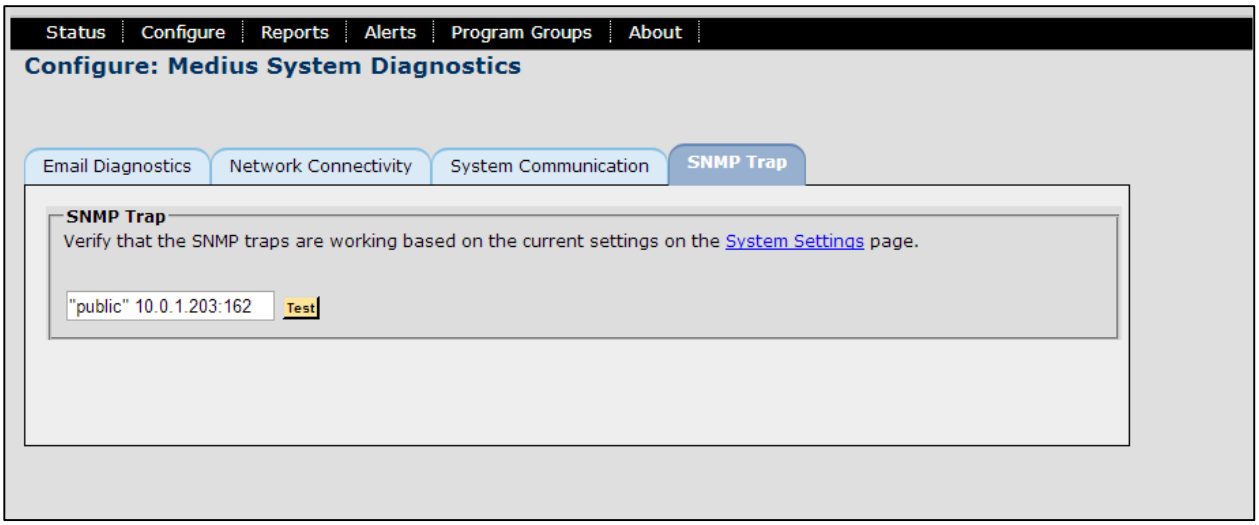



**Figure 82: SNMP Trap tab**

# Power Off and Remote Restart

Medius allows users to do a remote **Restart** or **Power Off** of any Medius unit.

You cannot **Power Off** or **Restart** a Sentry unit from a Medius. That action must be done from the Sentry itself.

**WARNING**: ***When moving a Medius, it is very important to properly power off the Medius. Never unplug a Medius without performing the Power Off procedure. Improper shutdown may cause file corruption and failure of the Medius.***

**NOTE**: ***A Restart or Power Off may make it difficult to troubleshoot the cause of the problem later on as log information has the potential to be permanently lost.***

To navigate to the **Remote Restart** and **Power Off** page, go to the main menu and select **Configure** and then **Power Off**.

## To Power Off a unit:

1. Select **Power Off.**

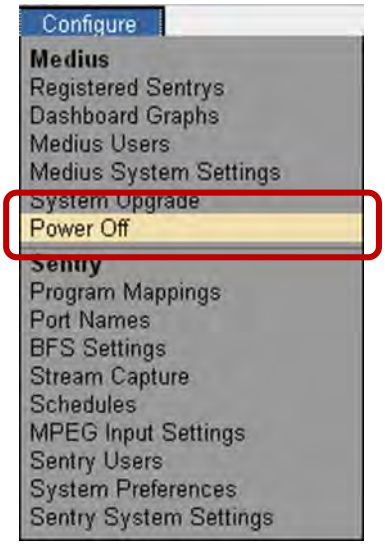



**Figure 83: Power Off**

2. Select **Submit.**

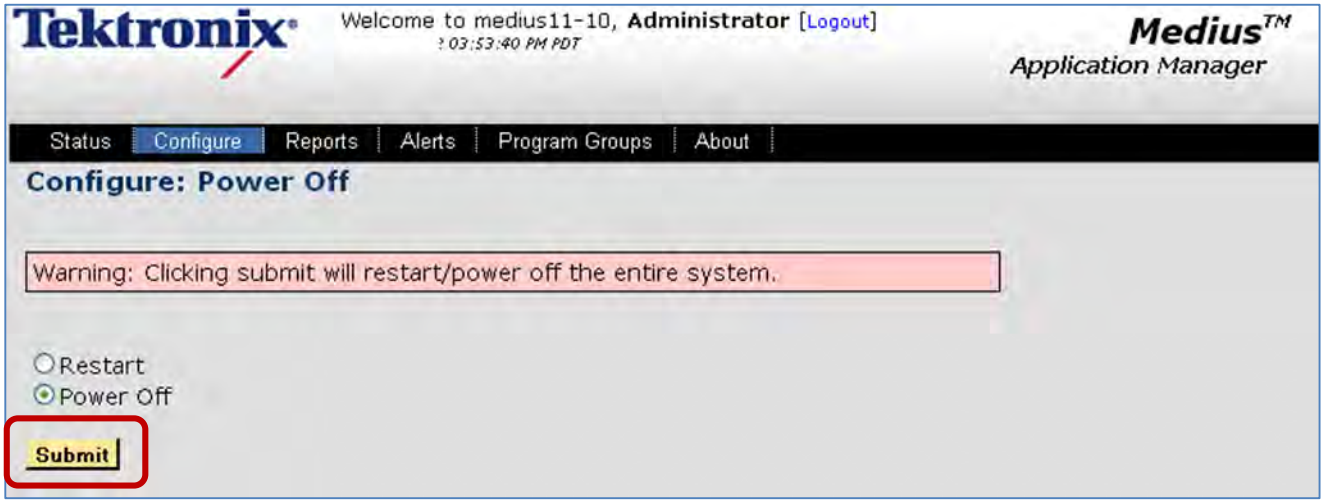



**Figure 84: Selecting Power Off**

3. The next screen will show a conformation.

4. Select **No** if you wish to cancel the action or **Yes** if you wish to continue with the power off.

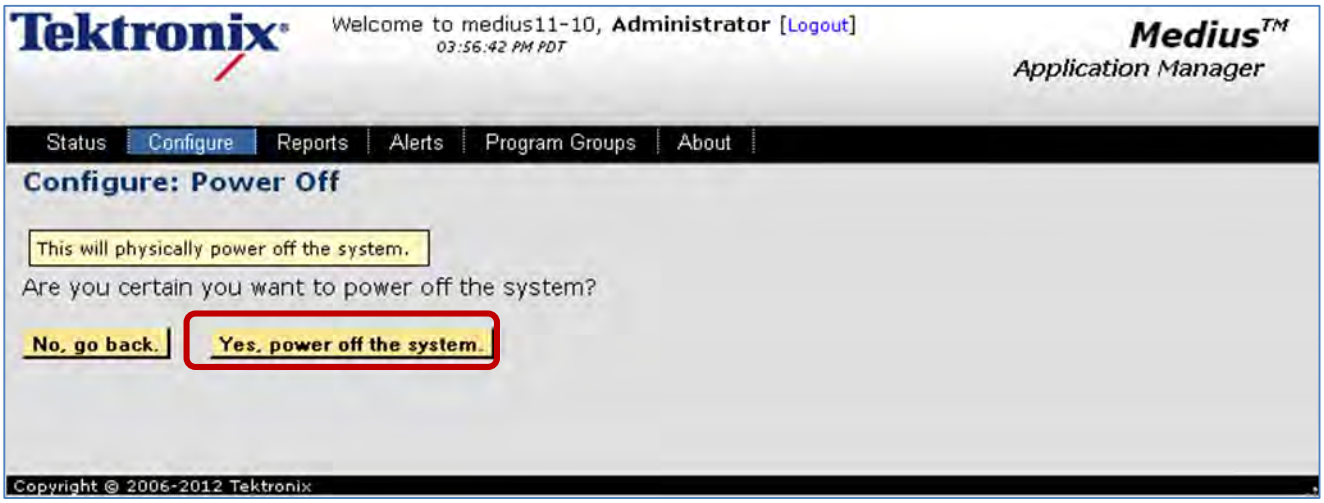



**Figure 85: Power Off confirmation**

## Restart a unit

In the unlikely event that the Medius is not behaving as expected, as last resort, you may attempt a **Restart**.

1. Select **Restart.**
2. Select **Submit.**

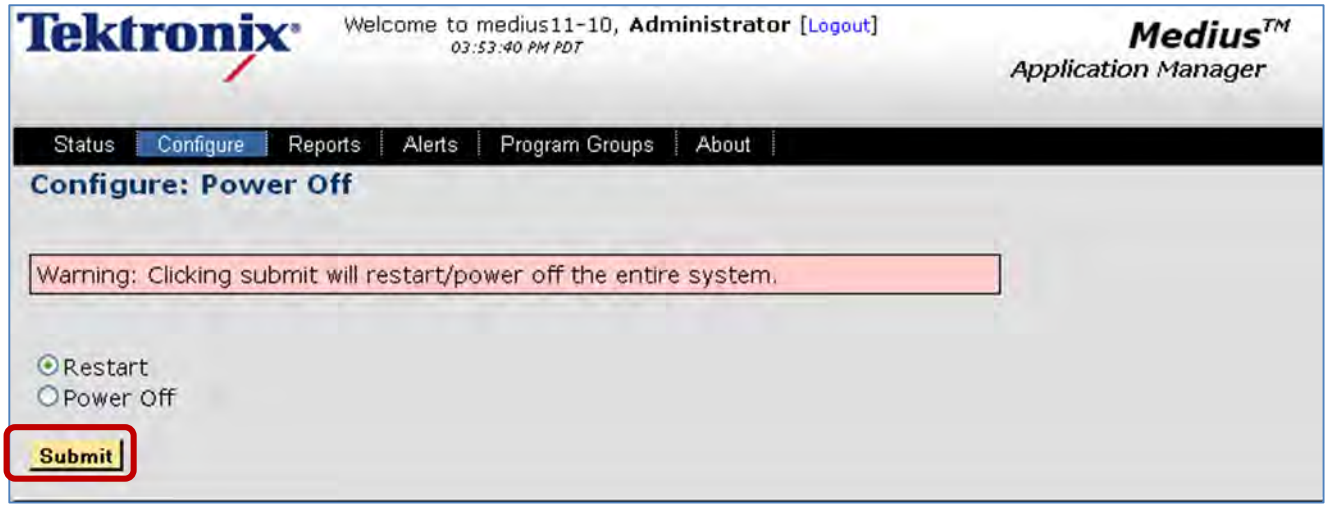



**Figure 86: Selecting Restart**

3. The next screen will show a conformation.
4. Select **No** if you wish to cancel the action or **Yes** if you wish to continue with the restart.

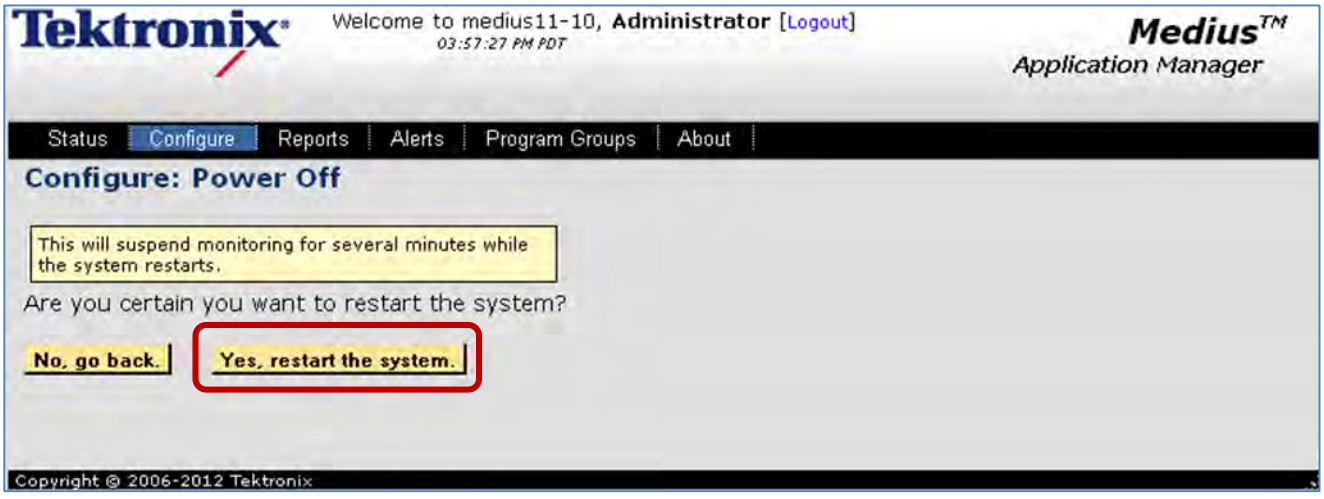



**Figure 87: Restart Confirmation**

# Configure Sentry Program Mappings

Sentry automatically detects program names and associated icons within the transport stream; however, in some cases this data is not available. The **Configure: Sentry Program Mappings** page enables you to associate a particular icon and network name with a port and program number. This association is saved in the internal relational database. Mappings can be created, modified, and deleted at any time.

## Add a New Mapping

1. Select **Program Mappings** from **Configure** drop-down menu.

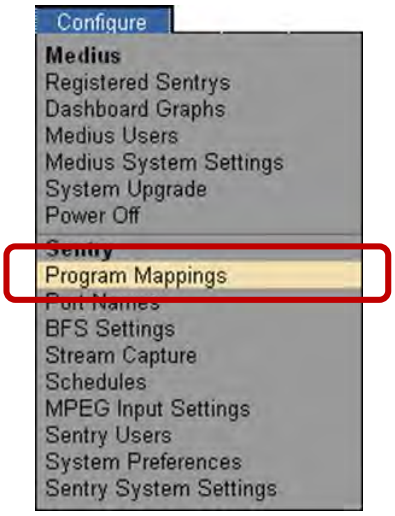



**Figure 88: Selecting Program Mapping**

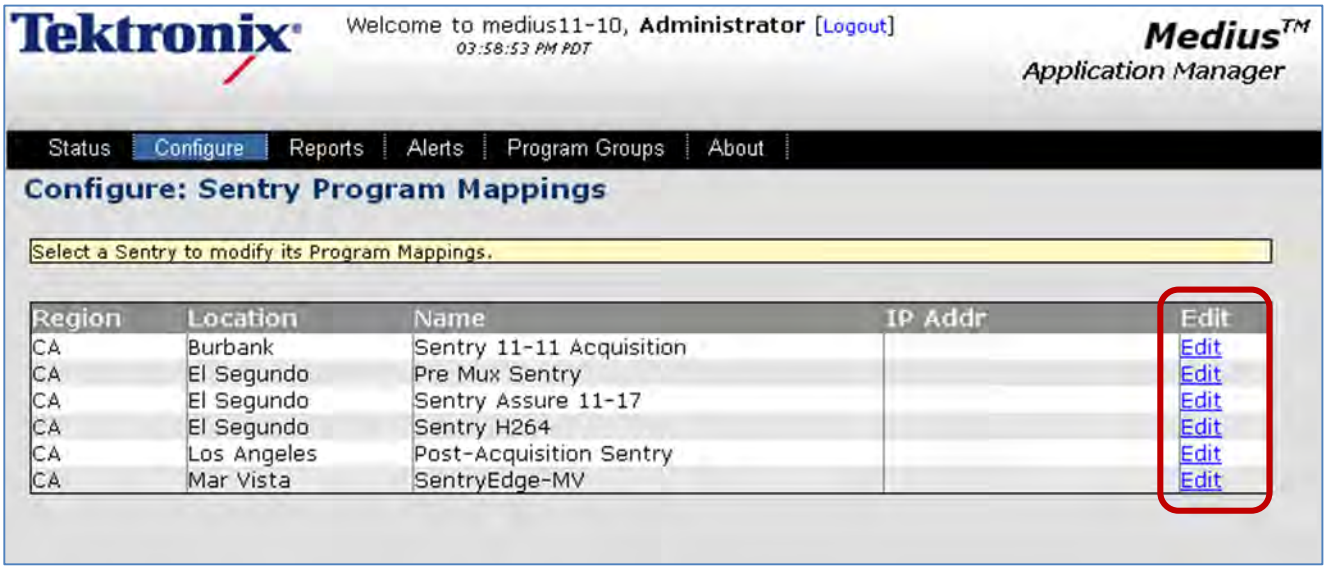



**Figure 89: Program Mapping overview screen**

2. Select **Edit** on the Sentry you wish to work with.

3. To add a new mapping, click **Add New Mapping** button located at the bottom of the page.

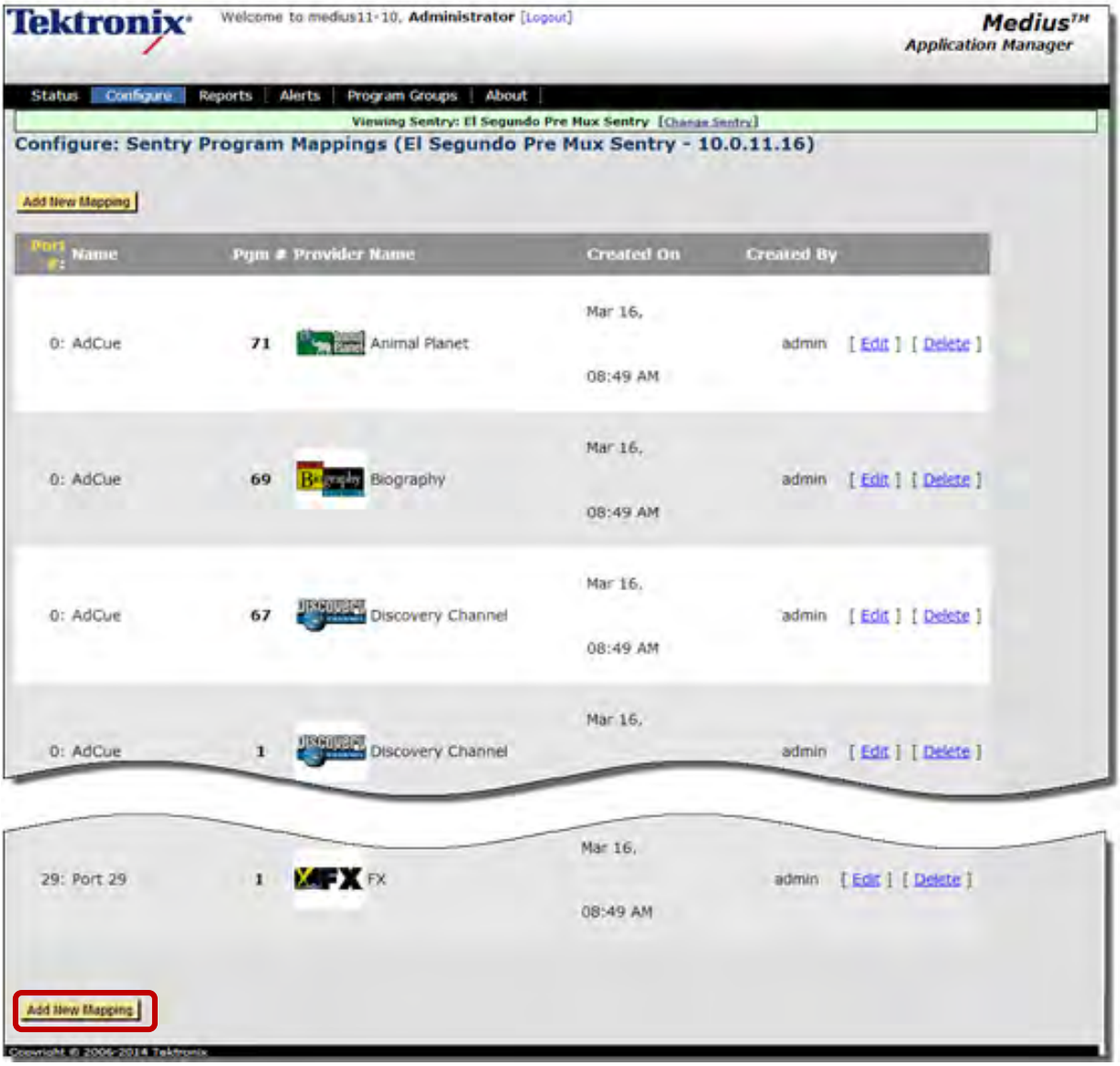



**Figure 90: Add New Mapping**

4. Next, select the port and program number you want to map.

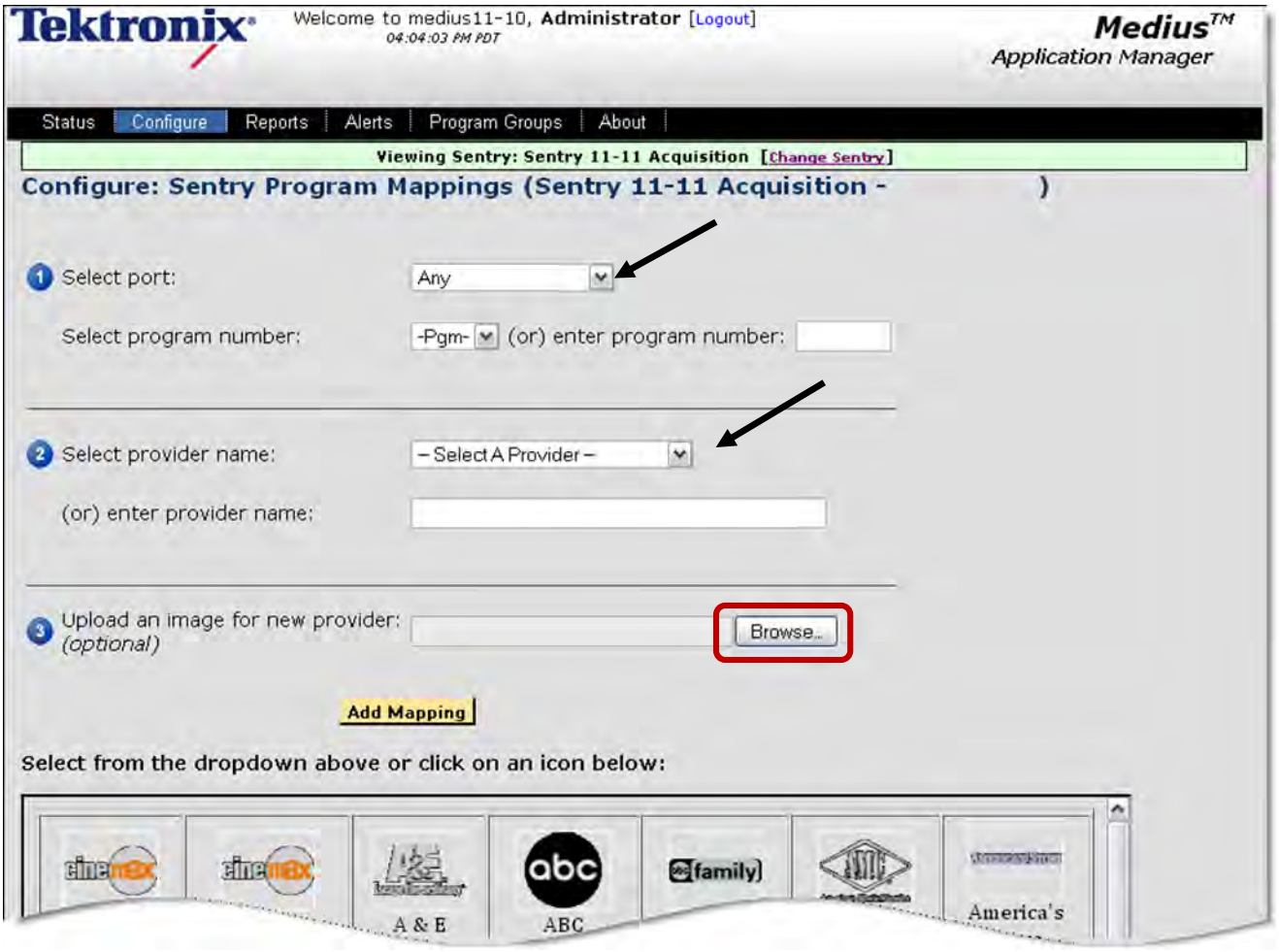



**Figure 91: Select a Port and Program**

5. All program numbers contained in the transport streams on all ports will be included in the drop-down list. A program number can also be manually entered.

6. **Select A Provider** either from the drop down list or by clicking on one of the available icons.
   a. Selecting the provider name is the exact same as selecting the icon.

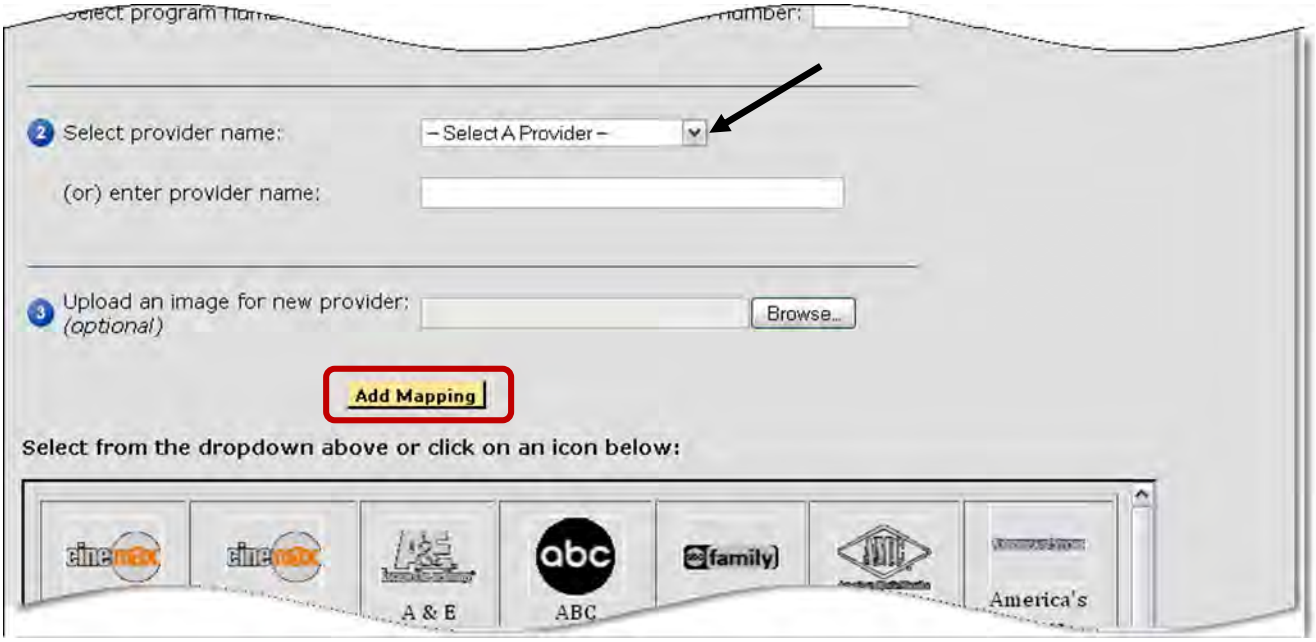



**Figure 92: Select Provider and Icon**

7. Click **Add Mapping**.
8. The new mapping will appear in the mappings list.
9. You can also manually add a provider name in the text field and upload an associated icon.

---

**NOTE 1:** ***Existing Mappings will not be overridden if Sentry automatically detects the correct program name and symbol.***

**NOTE 2:** ***If you switch to a different transport stream, you will need to remap your program numbers if they are not exactly the same as the ones in the previous transport stream.***

---

## Delete a Mapping

To delete a mapping select the **Delete** link. This will remove the mapping. Once mappings are deleted, the user will have to re-create them if they are needed again.


**Figure 93: Delete a Mapping link**

## Modify a Mapping

1. To modify a mapping select the **Edit** link.
2. The **Configure: Sentry Program Mappings** page opens configured with the selected program's mapping, which may then be modified.
3. Make your required changes.

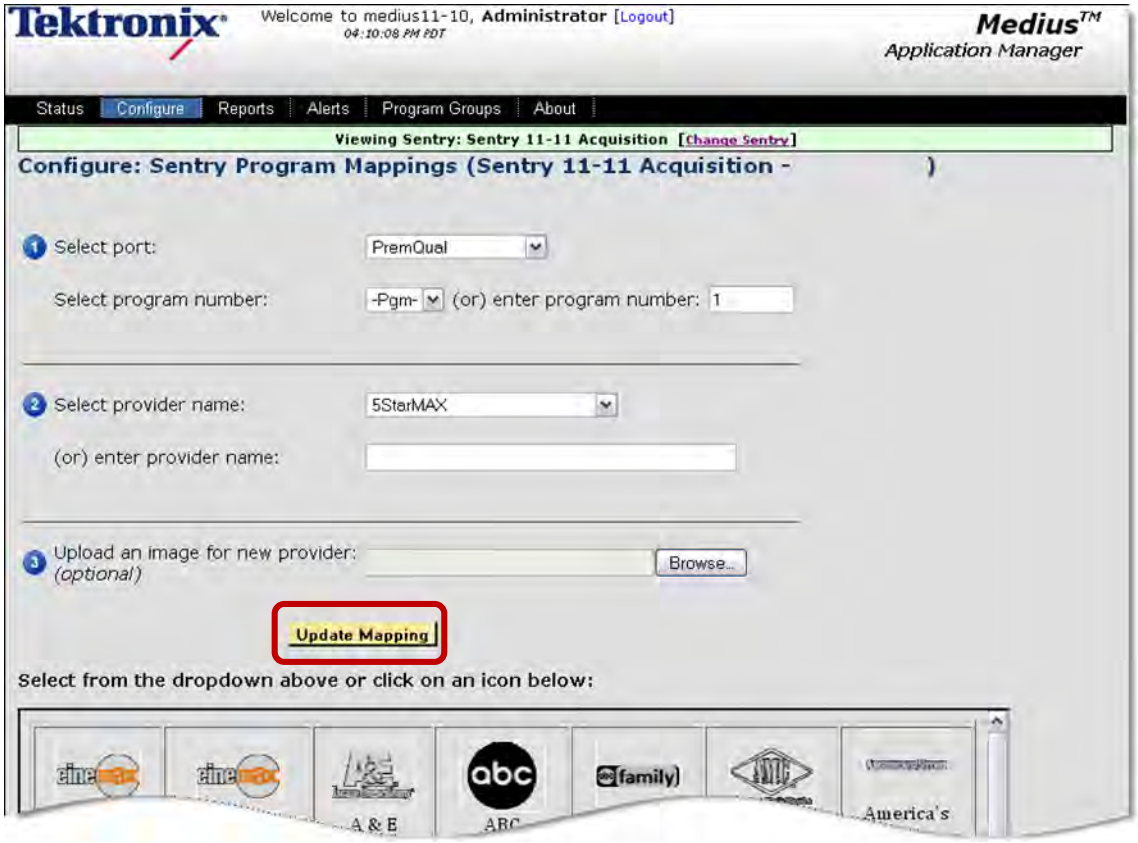



**Figure 94: Add Mapping button**

4. Select **Add Mapping** when finished.

# Configure Port Names

Sentry offers the capability to name an individual port.

1. Select **Port Names** from the **Configure** drop-down menu.
2. Select a Sentry from the list by clicking on **Edit**.

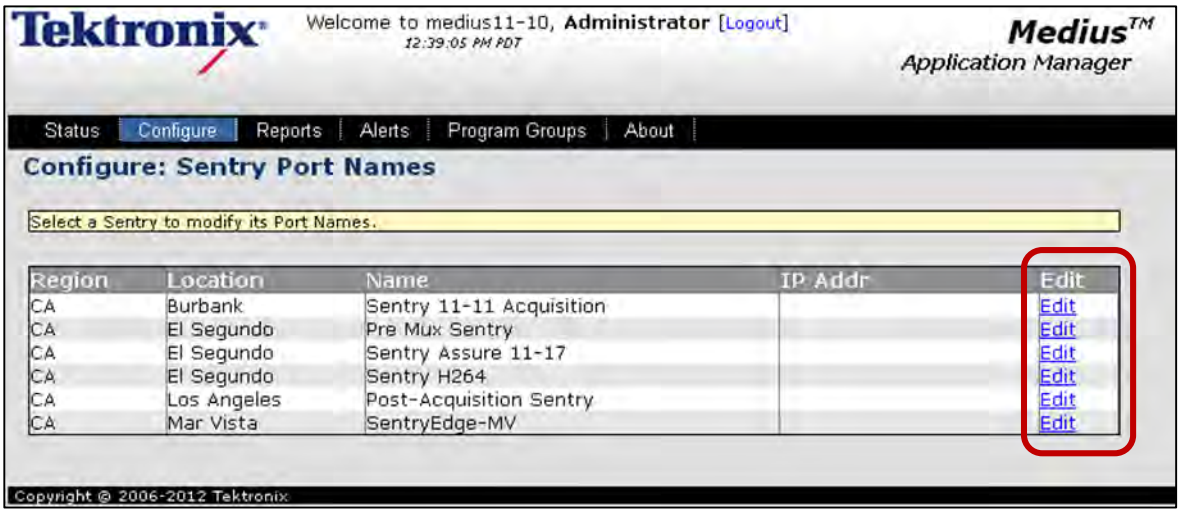



**Figure 95: Configure Sentry Port Names**

3. Select an unnamed port and type the new name and description in the given field.

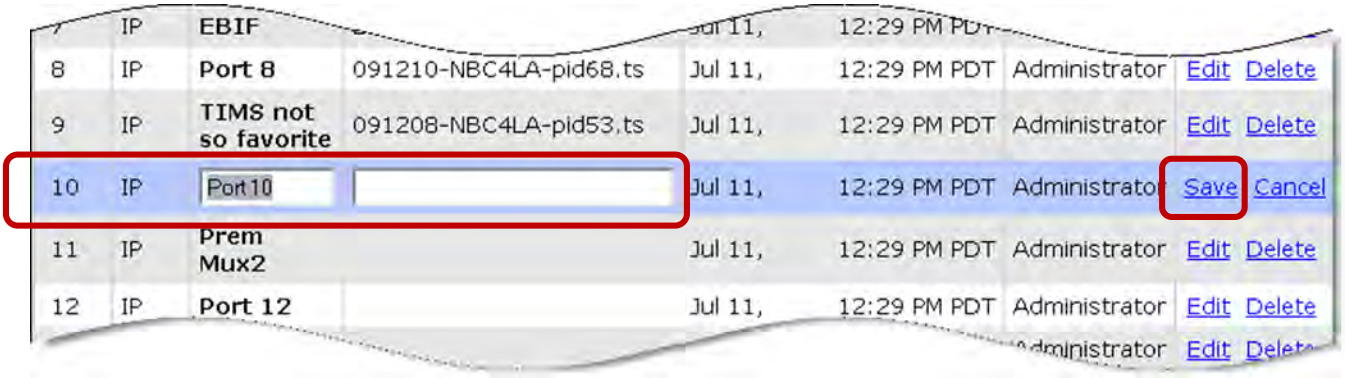



**Figure 96: Adding a Port Name**

4. Select **Save** when complete.
5. The port names appear on each report, including on the **Current Status** page.

## Edit Port Screen Names

1. You may **Edit** and **Delete** the port names from this page by selecting **Edit** from next to the Sentry name you wish to work on.
2. Next, type in the **Name** and **Description** in the given fields.
3. Select **Save** when complete or b to return to the previous page.


**Figure 97: Editing Port Name and Description**

## Delete a Port

1. Select **Delete** to remove a port name from the list.

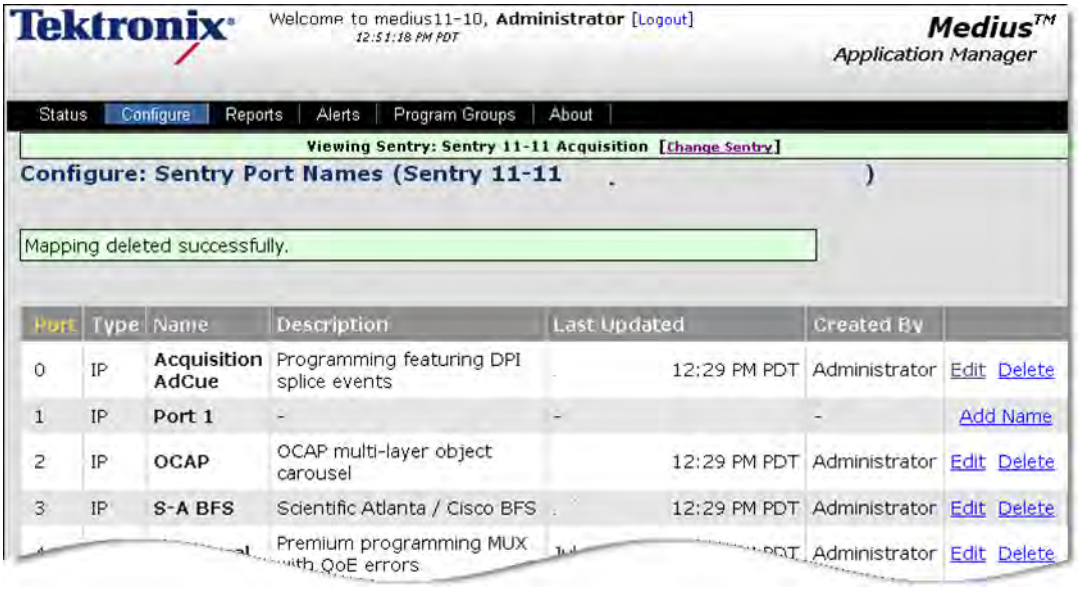



**Figure 98: Deleting a port name**

# BFS Settings

The **BFSdir** file contains data used to display the server, folder, and file names corresponding to the **BFS Source** in the **BFS Reports**. Enter the source ID for the **BFSdir** file.

## Access BFS Settings

1. Select **BFS Settings** from the **Configure** drop-down menu.

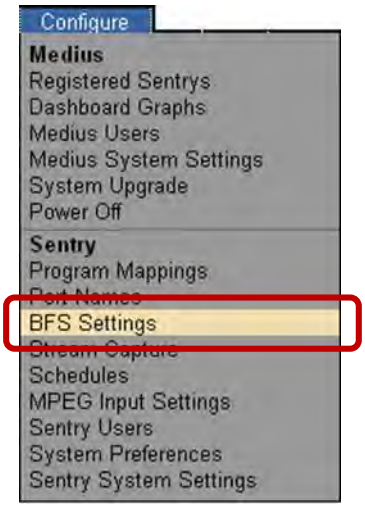



**Figure 99: BFS Settings**

2. Next, select **Edit** next to the Sentry you wish to configure.

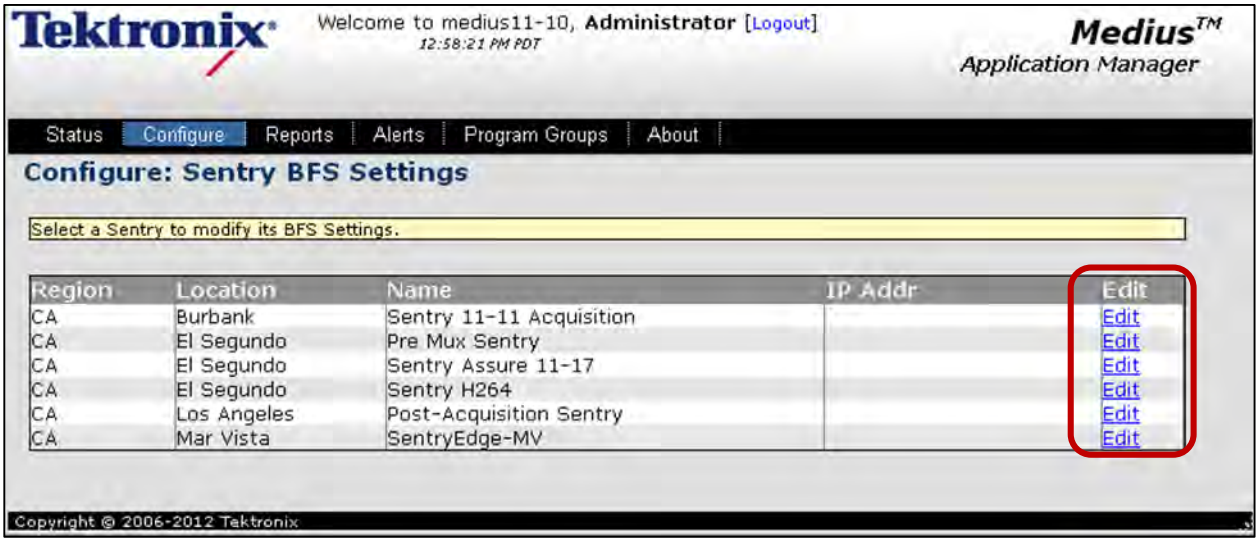



**Figure 100: Selecting a Sentry to Edit**

3. Add the requested information.

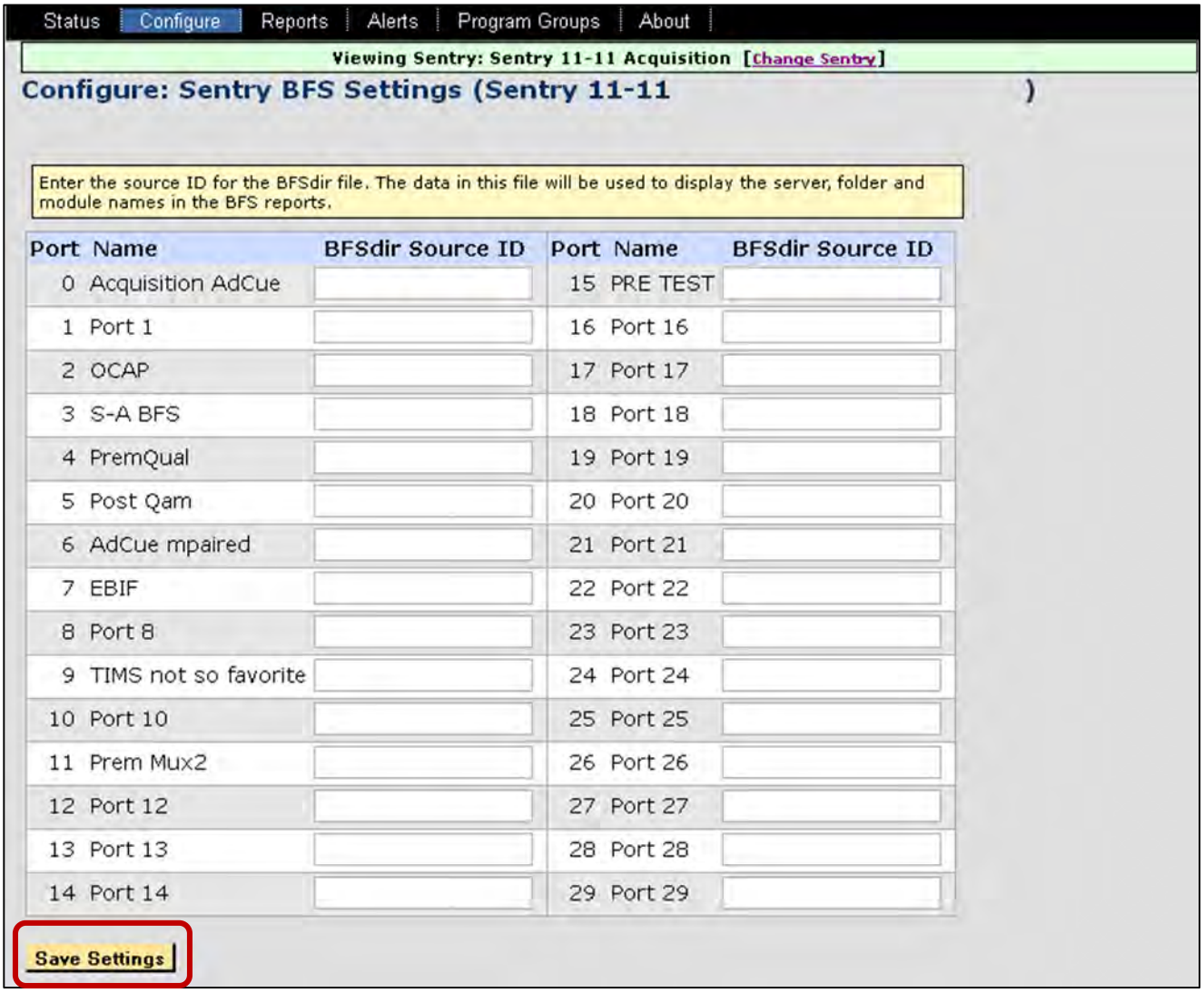



**Figure 101: BFS Settings**

4. Select **Save Settings** when finished.

# Stream Captures

**Alert Triggered Stream Capture** allows you to save a program to a file when specified alert conditions occur. You can use existing alerts or define new alerts for the **Alert Triggered Stream Capture**.

Some examples for this option would include:

- Setting an alert for a low QoE score for later viewing for analysis
- Playback of what a low QoE score event for analysis

The **Alerts** can be triggered off any alert type or types.

You may only create one **Alert Triggered Stream Capture** at a time.

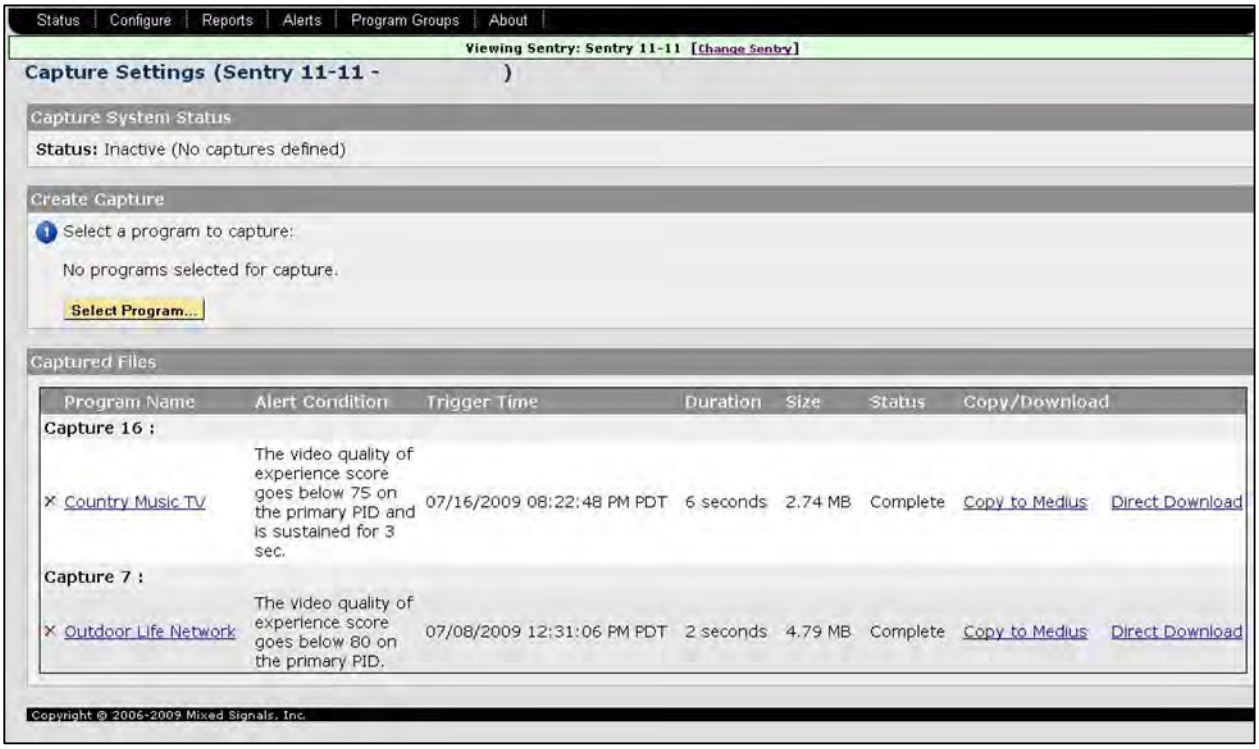



**Figure 102: Alert Triggered Stream Captures overview**

## Access Alert Stream Captures

1. Select **Configure** and then **Stream Capture**

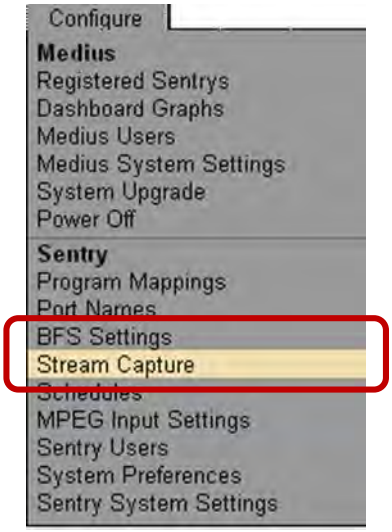



**Figure 103: Accessing Stream Captures**

2. Select the desired Sentry from the list by clicking **View**.

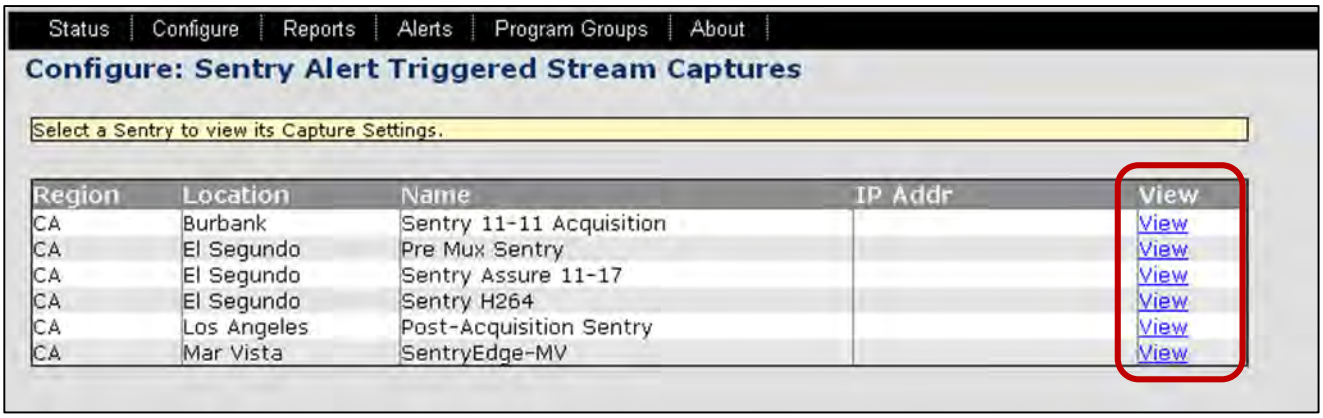



**Figure 104: Selecting a Sentry**

---

**NOTE:** ***You will receive a warning message if you try to create the capture from the Medius if there is already a capture defined directly on the Sentry. You can still create the capture but it will override the capture that is on the Sentry.***

---

## Create Alert Stream Captures (When none currently exist)

There are two ways to setup a capture from your selected Sentry: **Triggered by Alert** and **Triggered by User**.

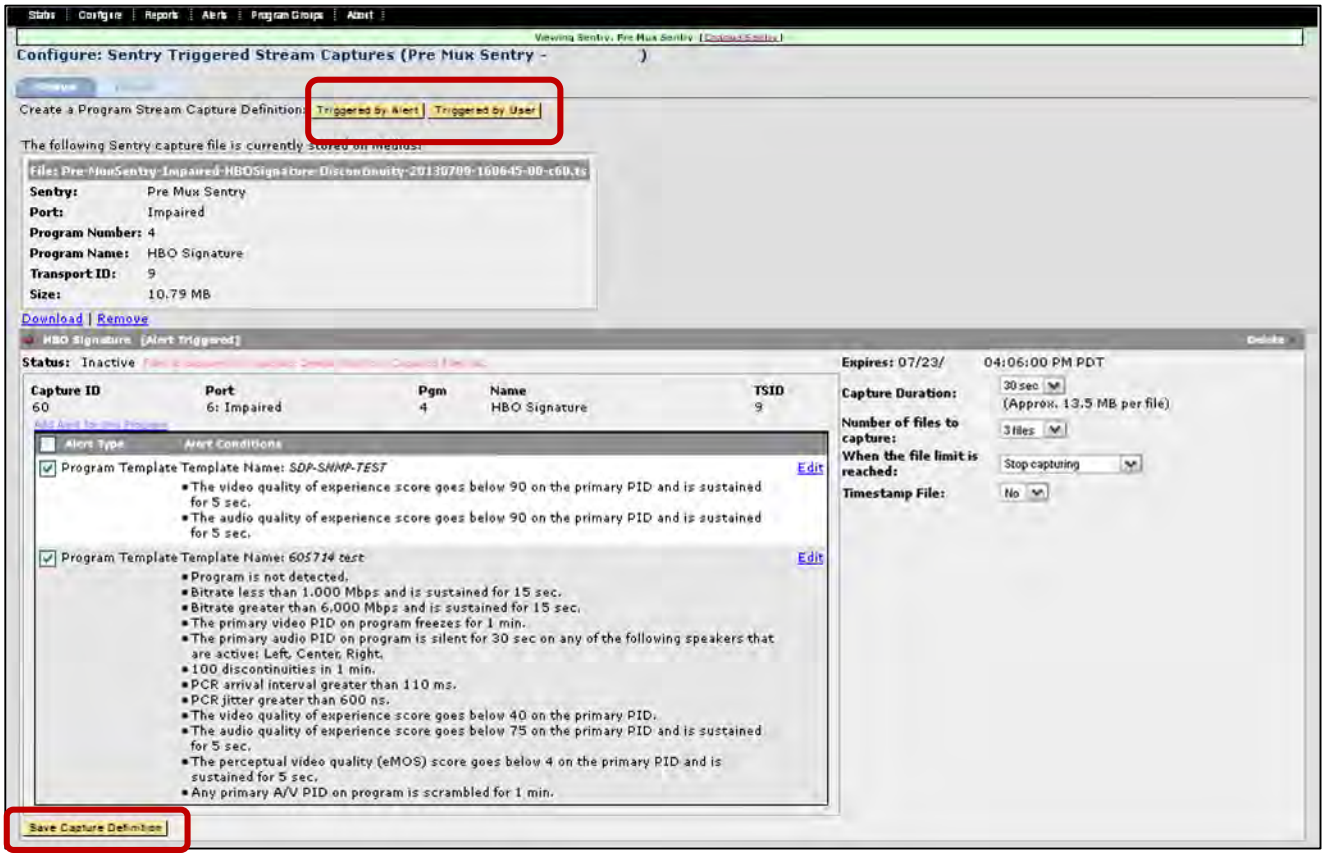



**Figure 105: Stream Capture trigger buttons**

1. To begin the set up for either capture, start by selecting either **Triggered by Alert** or **Triggered by User.**

### *Triggered by Alert*

2. Select a port and a program.

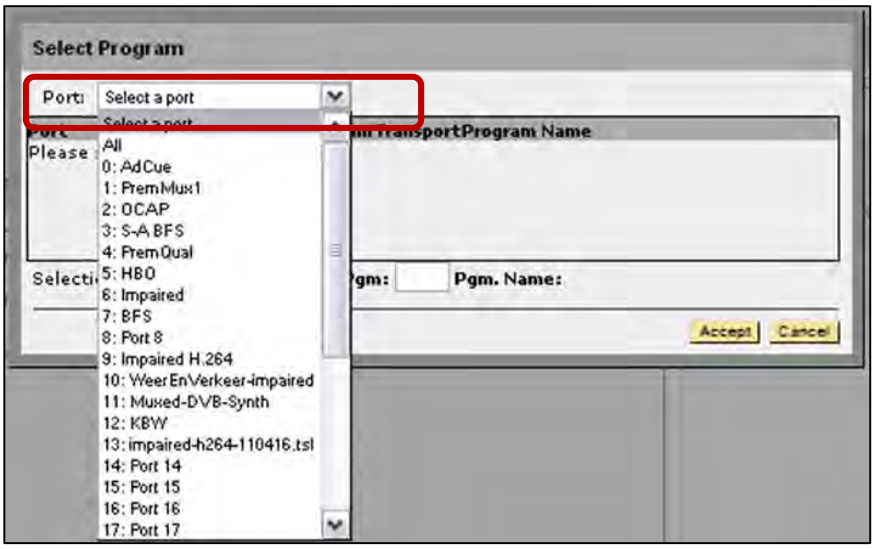



**Figure 106: Selecting the Port**

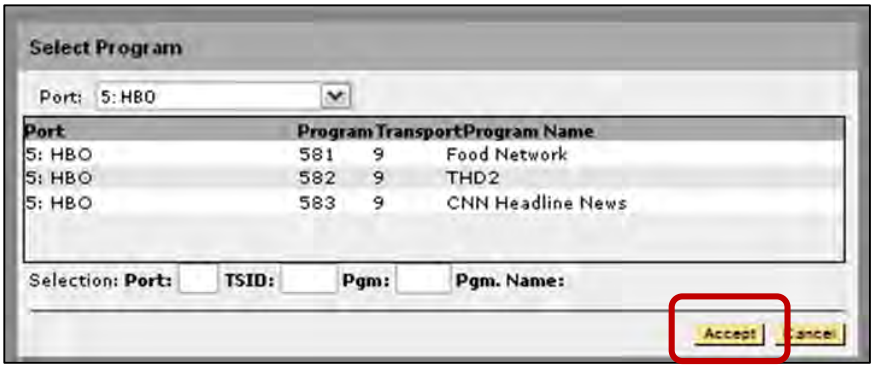



**Figure 107: Selecting the Program**

3. Select **Accept.**

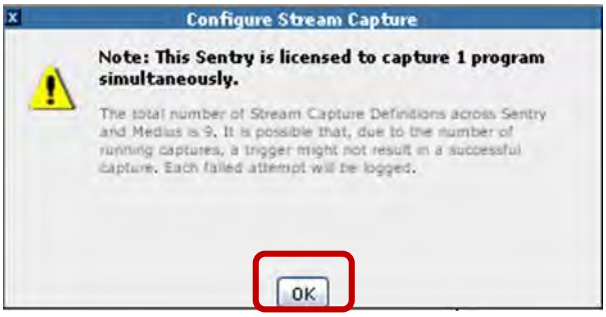



**Figure 108: License Notice**

4. Select **OK**.

5. **Section 2:** Select one or more of the alert types you wish set the trigger for.

6. Select an **Alert Type**
   a. To use **Add Alert for this Program**, select and then go through the step by step process and return to step 1.

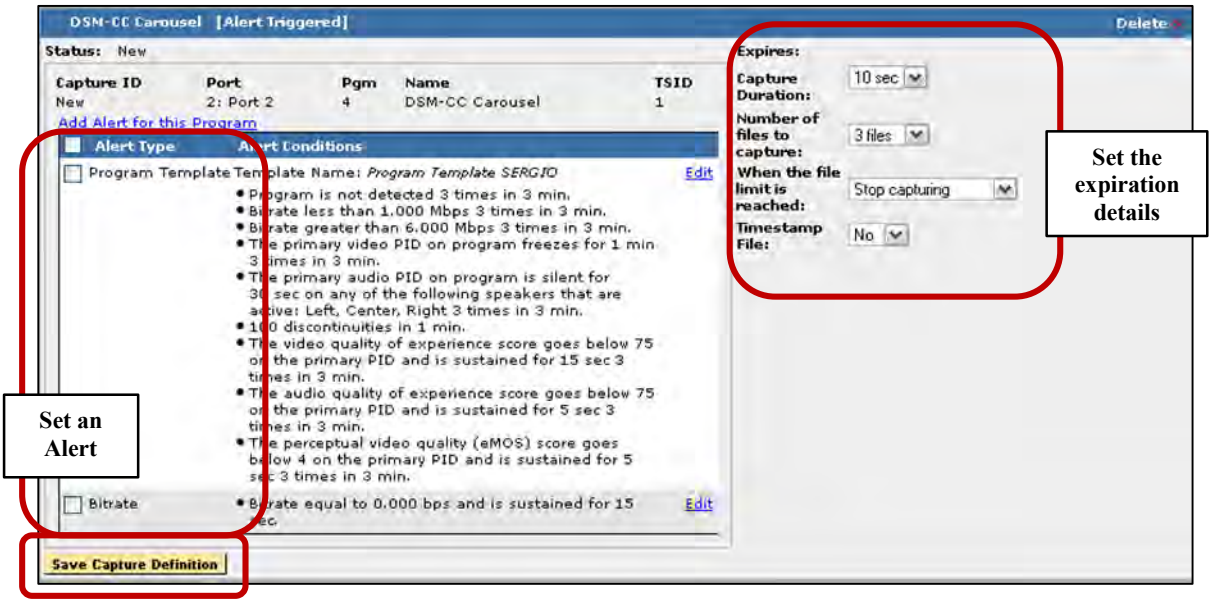



**Figure 109: Alert Trigger definition**

---

**NOTE**: ***In this example the program that was selected has alerts defined for it already. If you choose a program with no alerts defined, you will need to create alerts for the program before you can create a capture.***

***For more details, see the Creating Alerts section.***

---

7. Next, select the expiration details, including:
   - **Capture Duration**
     How long the capture should last
   - **Number of files to capture**
     How many files you need for the capture
   - **When the file limit is reached**
     What to do when the capture limit is reached
   - **Timestamp File**
     If you want the files time stamped or not

8. Click **Save Capture Definition**.
   a. a. If capture definition is successful, the following dialog box will appear.

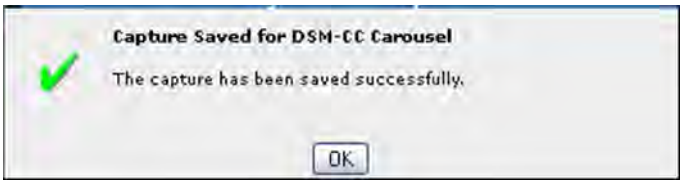



**Figure 110: Success dialog box**

**NOTE**: ***It is recommended that you do not select "Include Timestamps in the Capture File." This option adds extra information that is only useful for certain third party analyzers.***

9. Select **Save Capture**.
10. Select **OK** when complete.
11. Wait for alerts to trigger.
12. Once the alerts have triggered, return to the bottom of the screen capture page to see the screen captured files
13. Scroll down the page to the bottom and find **Captured Files**.


**Figure 111: Captured Files**

14. Locate the capture that you want to download.
15. Right click on **Direct Download** to save ts file.

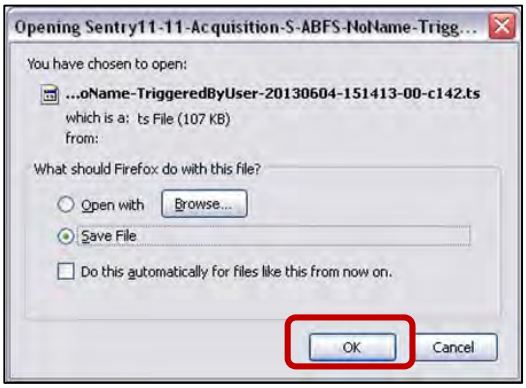



**Figure 112: Save capture to file**

## Deactivate a Capture/Creating a Stream Capture when one previously exists

To create a **Stream Capture** when one currently exists, you will first need to deactivate the existing capture. This will allow you to create a new **Stream Capture.**

1. Select **Deactivate** on the existing **Capture.**

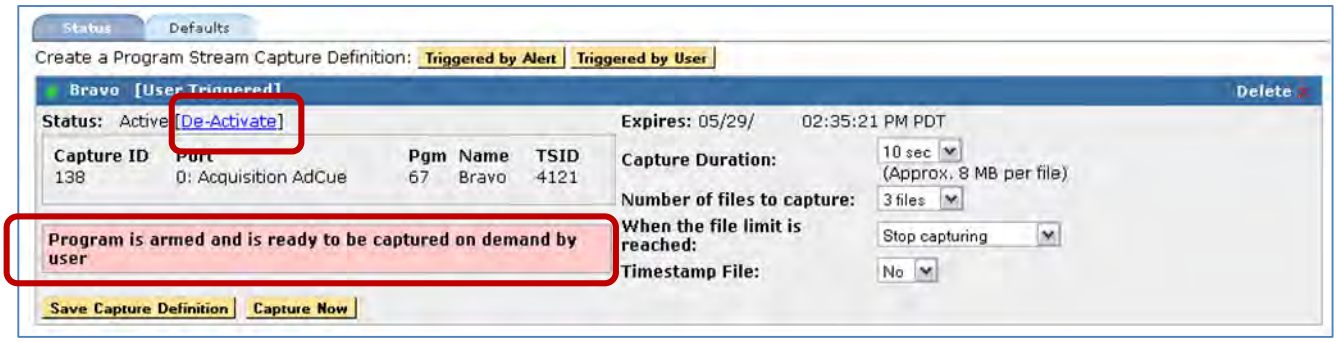



**Figure 113: Deactivating a Stream Capture.**

2. The following message will appear:

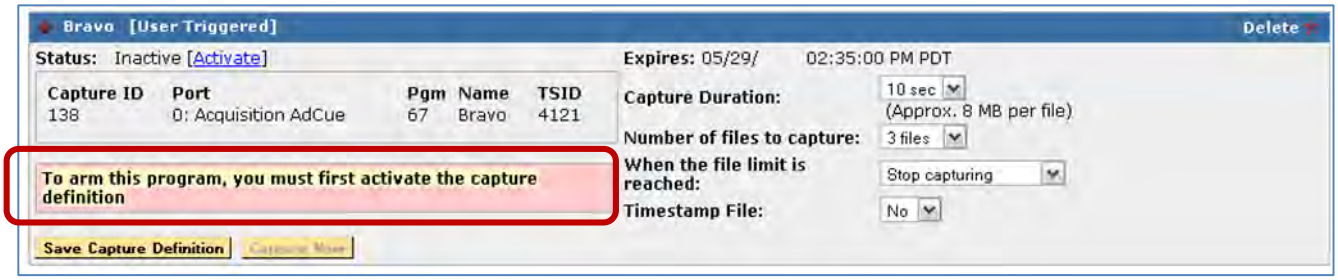



**Figure 114: Stream Capture Deactivated**

3. Continue with steps for **Creating a Stream Capture Where One Currently Does Not Exist**.

## Retrieve Captured Files

The **Captured Files** section lists all of the saved captured files along with its reference information.


**Figure 115: Captured Files**

- **Program Name**
  The name of program
- **Alert Condition**
  The condition that triggered the capture
- **Trigger Time**
  Date and time the alert was triggered
- **Duration**
  How long the capture lasted
- **Size**
  The size of the captured file
- **Status**
  Either **Complete** or **Active**
- **Copy/Download**
  Provides a link to a download of the capture. All captures are saved as transport stream files.
  - Click **Copy to Medius** to download the file from the Sentry to Medius. This is handy when the Sentry is not reachable (ex. Medius is ***outside*** of a firewall and Sentry is ***inside*** a firewall.).
  - Click **Direct Download** to download the file directly from the Sentry to the location of your choosing.

### *Delete Captured Files*

To delete any captured file, select the **X** next to the file's name.

# Closed Caption Verification (via Nexidia Comply™)

The **Closed Caption Verification** performs in-depth closed caption analysis by integrating with Nexidia Comply™.

With a license for this feature, you can perform an in-depth closed caption verification on the program of your choice. You can perform any analysis for up to three days at a time. The results will then be displayed in the **Data Detect** and **Program Group Data Detect** reports.

## Configuring the Nexidia Server

Only a user with system administrator permissions may make these changes.

1. Select **Configure** and then **Closed Caption Verification** menu.
2. Next, select the **Settings** tab.

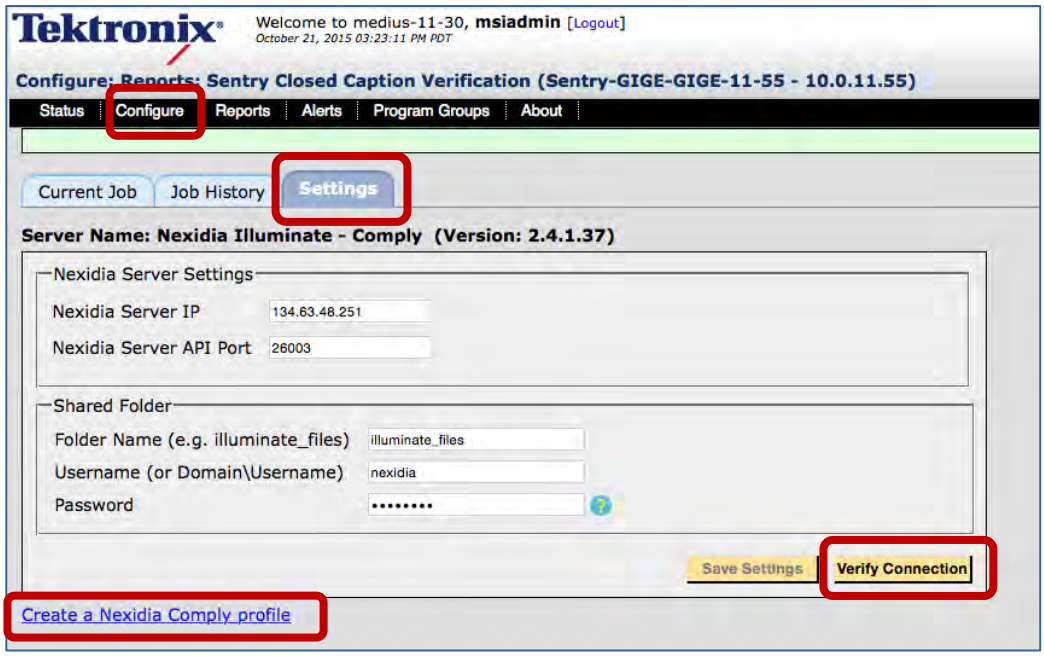



**Figure 116: Settings tab options**

3. Enter the following:
   - **Nexidia Server IP**
   - **Nexidia Server API Port**
   - **Folder Name**
     Sentry must be able to copy files to this shared folder on the Nexidia server with the specified username/password. Your system administrator is responsible for creating this shared folder.
   - **Username**
   - **Password**

4. Select **Save Settings**. You may also select **Verify Connection** to validate the connections.

### Create a Nexidia Comply Profile

A Nexidia profile is a group of tests to perform for the Closed Caption verification.

You must have a Nexidia profile defined in order to schedule verification jobs.

1. To create a Nexidia profile on the Nexidia server, select **Create a Nexidia Comply Profile** from the Settings tab (see above figure).
2. The resulting page will look similar to the following.

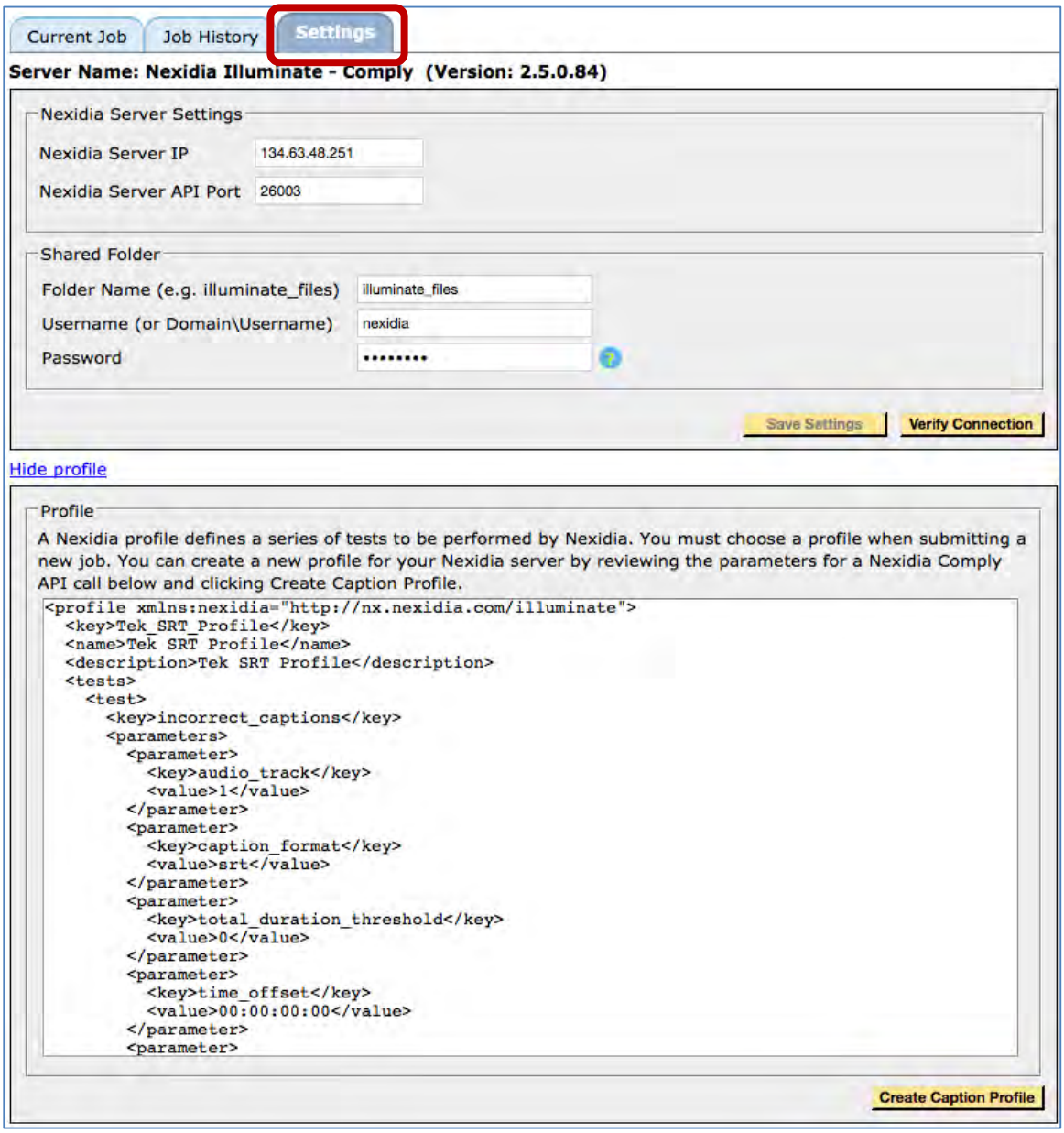



**Figure 117: Resulting page after selecting Creating a Nexidia Comply Profile**

## Create Caption Profile

The user may submit an API request to the Nexidia server to create a profile. The request will be seeded with default parameters. Sentry only supports type srt profiles.

To create the profile, click the **Create Caption Profile** button.

## Choosing a Program to Verify

Only a user with system administrator permissions may make these changes.

1. To verify and review the results of the verification jobs a program, select **Configure** and then **Closed Caption Verification.**

2. Next, select the **Current Job** tab.


**Figure 118: Current Job tab**

3. You can configure one program on each Sentry to be verified at any one time. If no program is currently being verified, you can choose a program by clicking **Select a Program**.

4. Select the desired program and then select **Accept**.

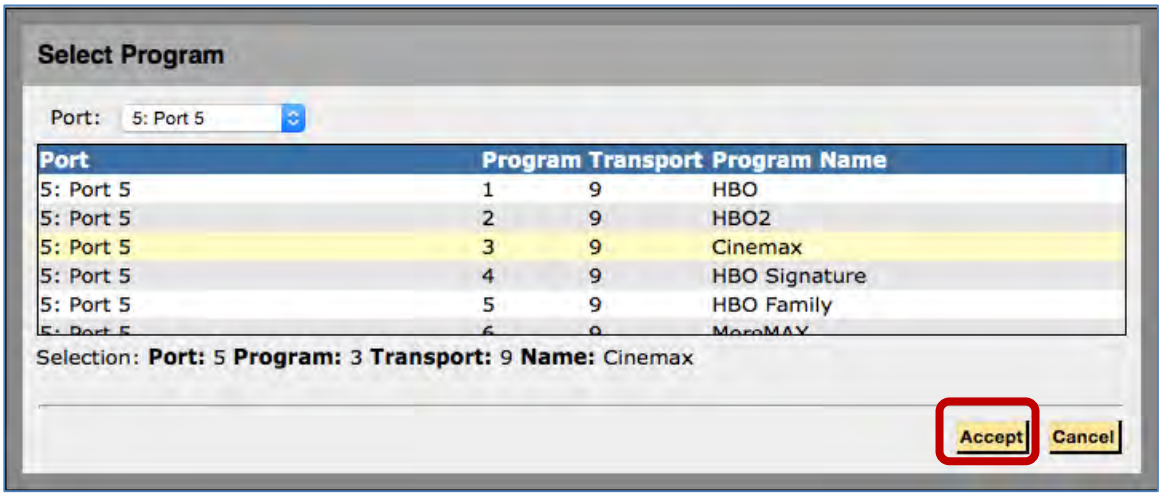



**Figure 119: Select Program window**

5. Select and make changes to the following as needed:
   - **Caption Types**
     The type(s) of captions you'd like to verify (608 and/or 708)
   - **Nexidia Profile**
     This is a list of the profiles (which tell Nexidia what types of verification checks to perform) that have been configured on the Nexidia server.

     Sentry only supports type srt profiles. If you have configured Nexidia profiles for non-Sentry purposes with other formats, choosing a non-srt profile from this list will result in job errors.
   - **Verification Period**
     Up to 3 days.

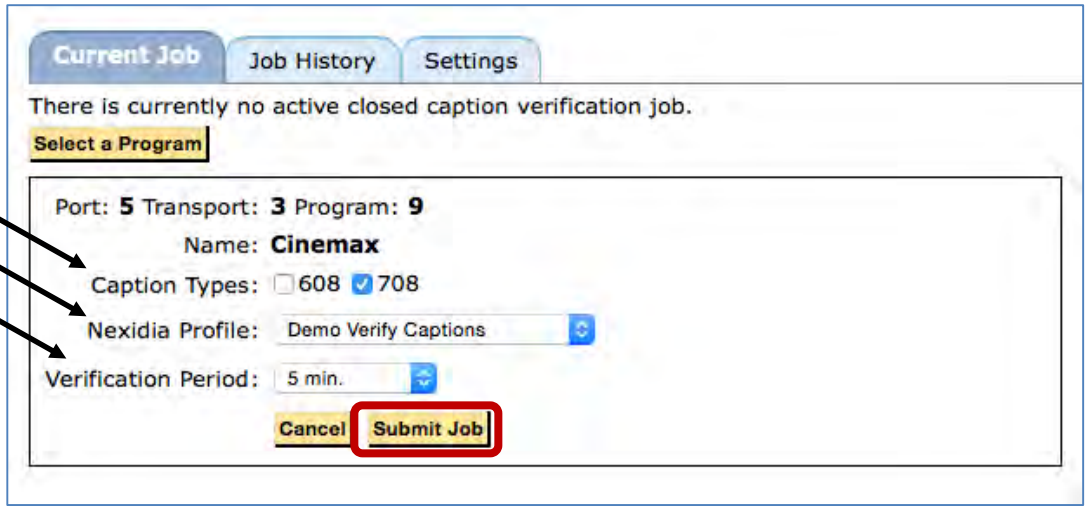



**Figure 120: Current Job verification**

6. Select **Submit Job** to begin the verification.

When the verification job is submitted, you will see the status of the current job in a table. The process works as follows:

**a.** Sentry will begin capturing audio files (segments), and will do so in five-minute segments.
**b.** When each segment is captured it will then be submitted to Nexidia Comply for closed caption verification.
**c.** When Nexidia Comply is done verifying each job segment, the results will be returned to Sentry and available in the **Data Detect** report.

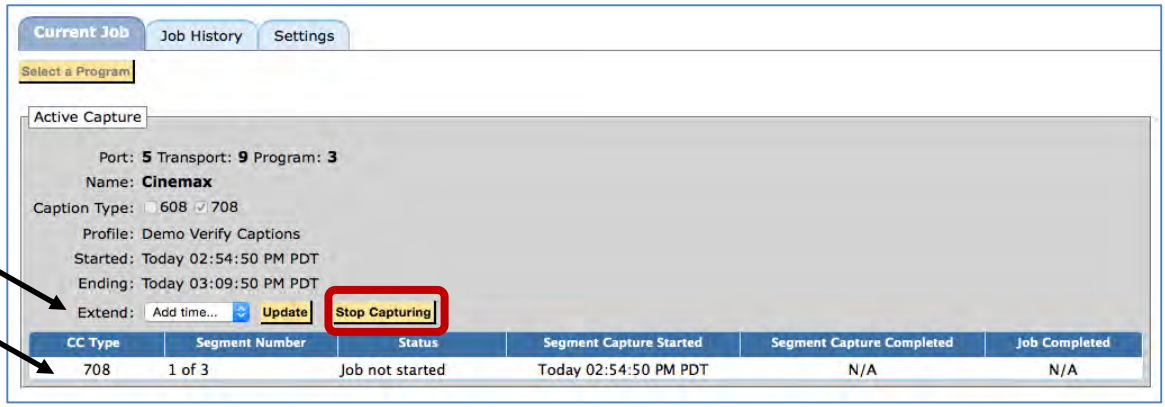



**Figure 121: Verification table**

**7.** When a verification job is in process, you can update it as follows:

- **Extend**
  Extend the time by up to three more days by choosing the length of time you'd like to extend and selecting **Update**.
- **Stop Capturing**
  Cancel the job by selecting **Stop Capturing**.

## Reviewing Job History

An administrator can click on the **Job History** tab to review the status of all jobs both current and completed.

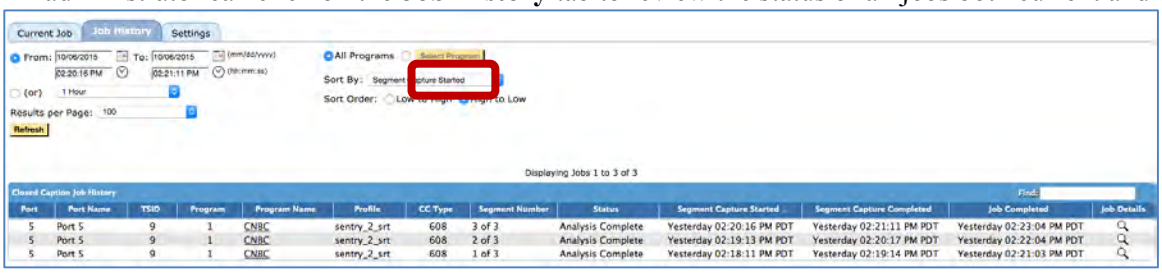



**Figure 122: Select Program buttons and capture flows**

Choose a time range to narrow down the results.

To further filter the results by a specific program, clicking the radio button next to **Select Program** and then select the **Select Program** button.

You can sort results by any of the columns by clicking on the column header or selecting that column from the **Sort By** drop-down menu.

- **Profile**
  The Nexidia profile that you chose for the verification job. This profile tells Nexidia what types of verification checks to perform.
- **CC Type**
  608 or 708
- **Segment Number**
  The verification period for each job is broken into a number of five-minute segments.
- **Status**
  Mouse over the status to get more detailed status information.
- **Segment Capture Started**
  The start time of the audio capture segment.
- **Segment Capture Completed**
  The end time of the audio capture segment.
- **Job Completed**
  The time when the verification results were completed and ready for viewing in the **Data Detect** report.
- **Job Details**
  Select the magnifying glass to see a log of when the job hit each of the various statuses.

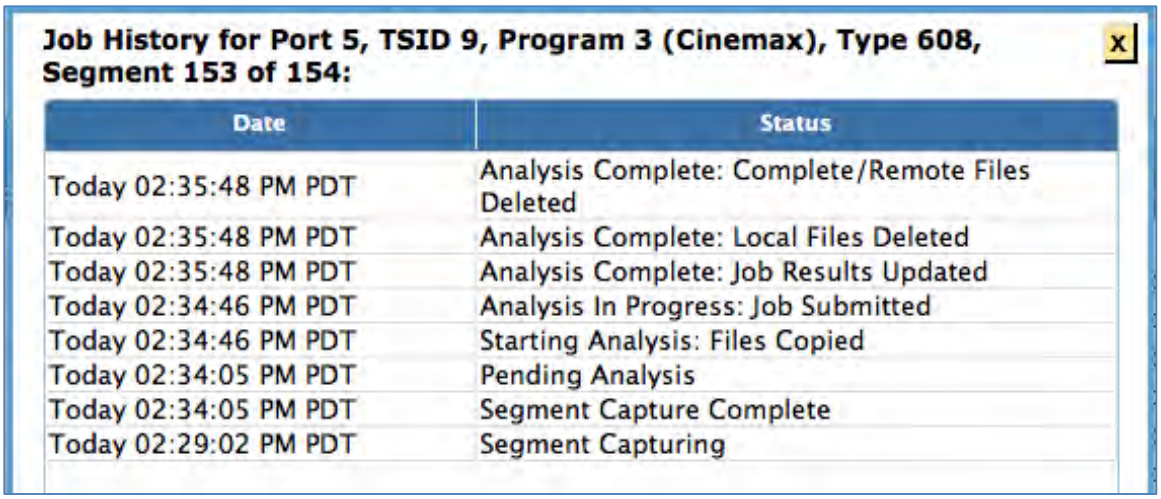



**Figure 123: Job Details**

To review the **Closed Caption Verification Results** for a given program segment, click on the program name. This will take you to the **Data Detect** report for that program and time period.

## Reviewing Closed Caption Verification Results

If your Sentry has a **Closed Caption Verification** license, a new column of types (Nexidia CC Verification) will show up on the **Data Detect** and **Program Group Data Detect** reports.

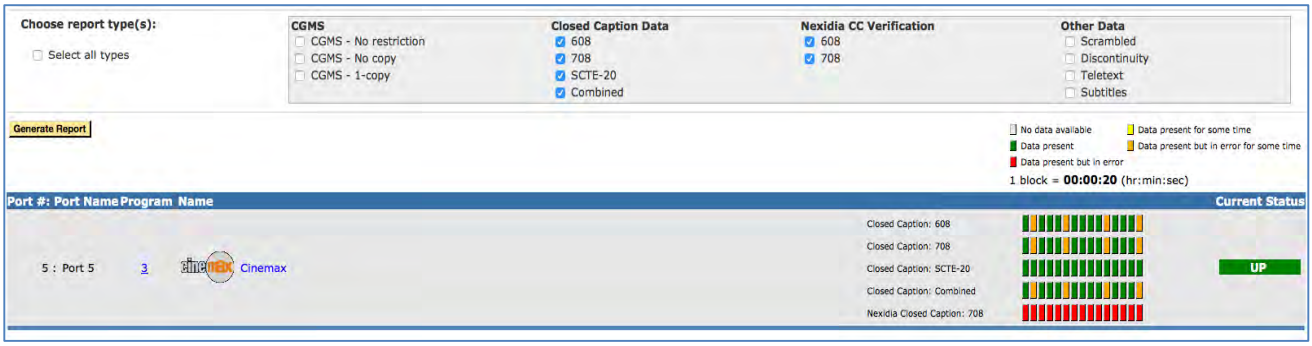



**Figure 124: Verification Results**

To see all programs that had **Closed Caption Verification** performed against them during the report timeframe, select the appropriate Nexidia CC Verification options.

- **Grey** means there was no **Closed Caption Verification** performed at that time.
- **Green** means **Closed Caption Verification** was performed at that time, but there were no error conditions detected.
- **Orange** means **Closed Caption Verification** was performed at that time and the time period in the block contains both segments with error conditions and segments without error conditions.
  In this case, zoom in by clicking the orange block, to see exactly when the error conditions occurred.
- **Red** means there was **Closed Caption Verification** performed at that time, and there were error conditions detected.

At any time you can zoom in on a report by clicking on the colored blocks.

To view the details of the **Closed Caption Verification** for any block, hover over that block.

This will summarize the checks that were performed during that segment, as outlined by your Nexidia profile and the results of each check.

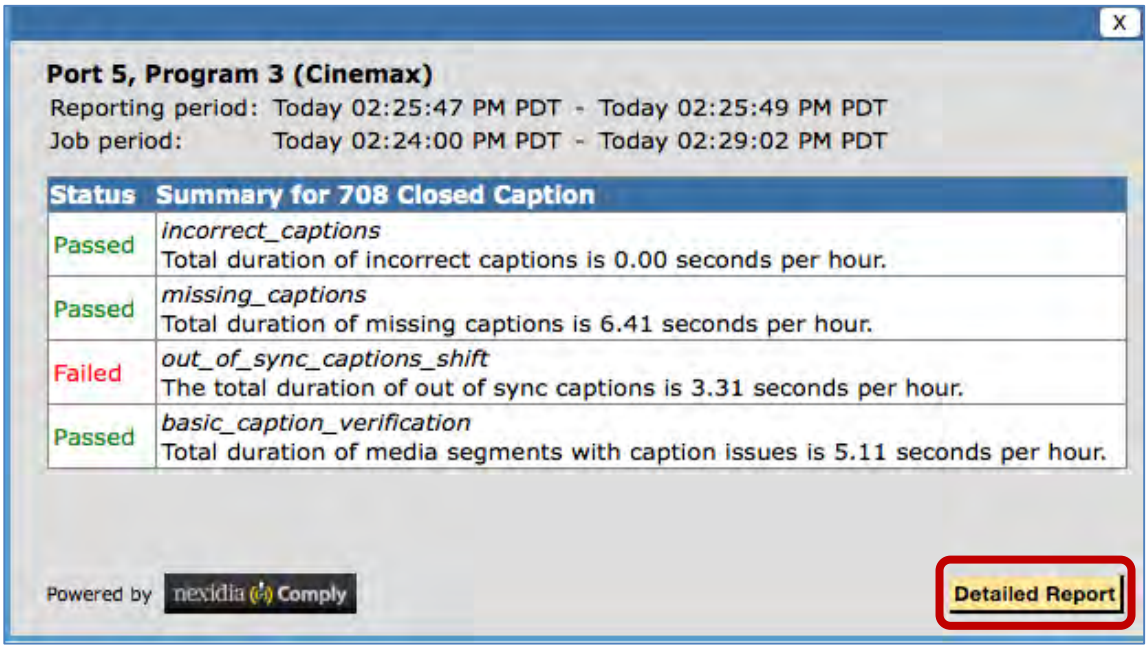



**Figure 125: Status Summary**

To see more detailed information about each check, click **Detailed Report**.

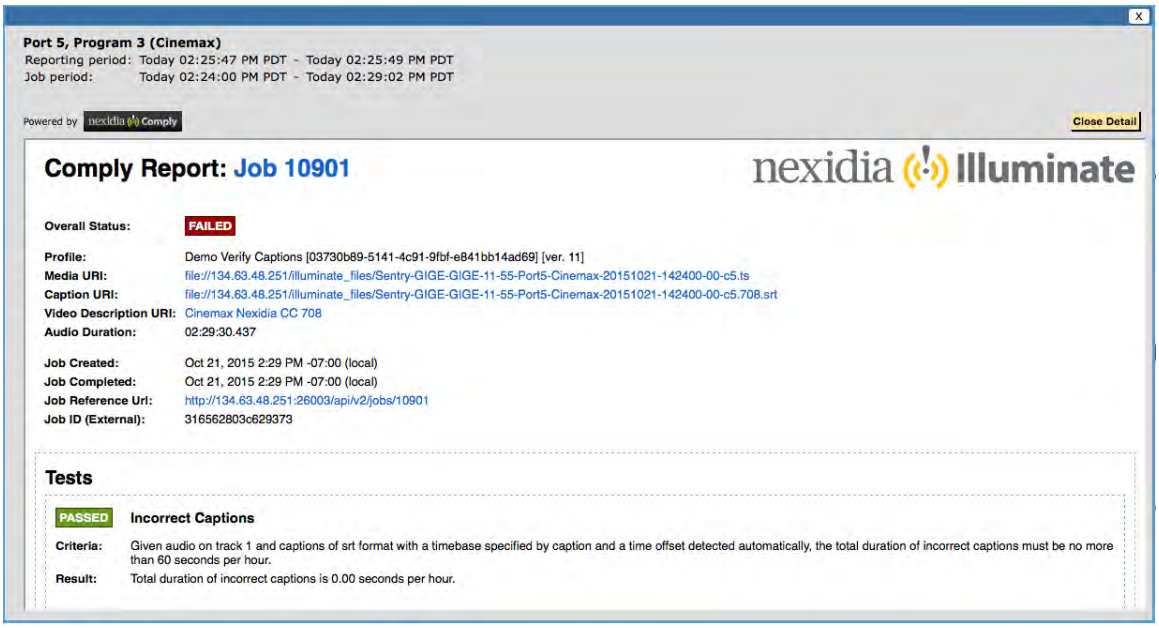



**Figure 126: Detailed Report**

Scroll down in the detailed window to see all of the details provided by the Nexidia tests.

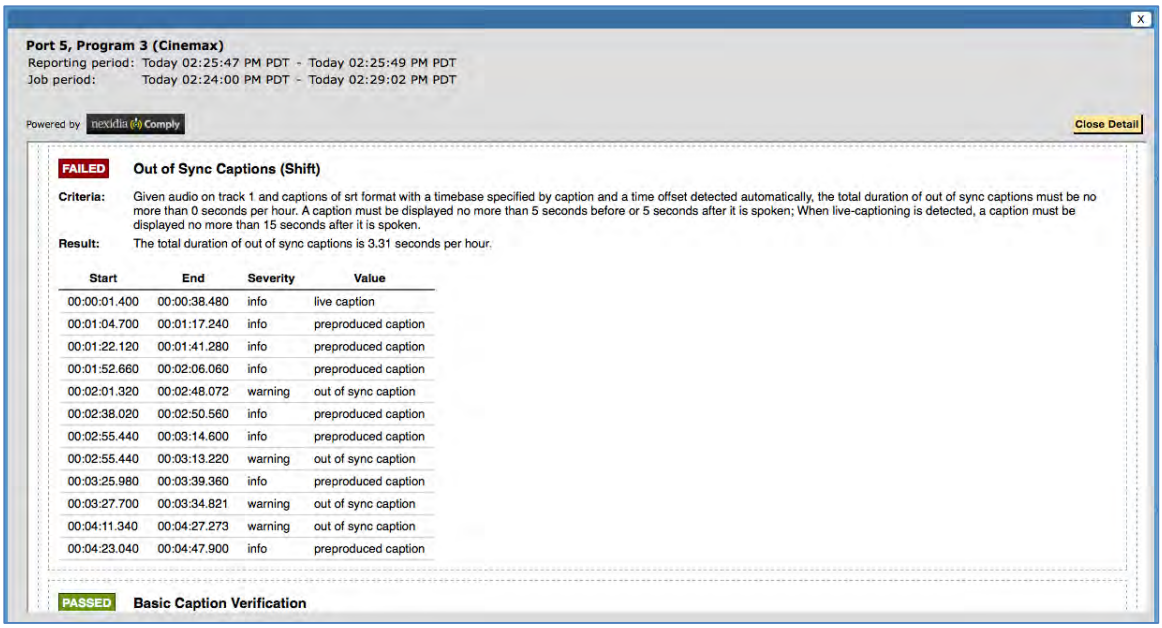



**Figure 127: Additional Details**

Click **Close Detail** to exit.

# MPEG Input Settings

Sentry models are either ASI or MPEG over IP (GigE). Sentry is aware of its connections so the web page to **Configure MPEG Input Settings** exists only in MPEG over IP models of Sentry.

Use **Configure: MPEG Input Settings** to configure the LAN1 Ethernet connection. Sentry will not receive the transport stream input over the Ethernet unless the settings are correctly configured.

Use MPEG Input Settings to specify **Unicast** or **Multicast** transport stream input. If using **Unicast**, only one input port is required. If using **Multicast**, up to 30 input ports and corresponding **Group IP** numbers can be specified. There are validity checks on the values entered but input ports from 1 to 65535 are valid.

### Access MPEG Input System Settings

1. Select **MPEG Input System Settings** from the **Configure** drop-down menu.

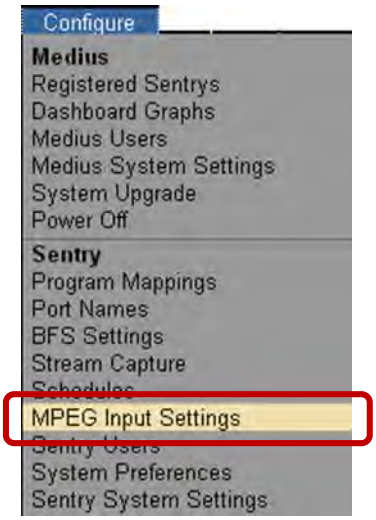



**Figure 128: Selecting MPEG Input**

2. Select **Edit** for the Sentry you wish to change.

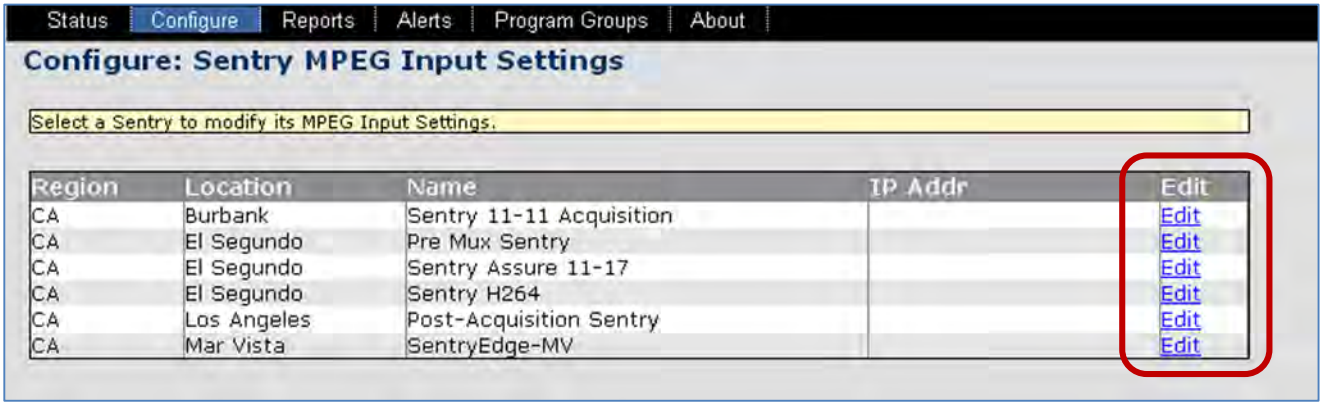



**Figure 129: Selecting a Sentry to Edit**

3. Adjust settings as needed.

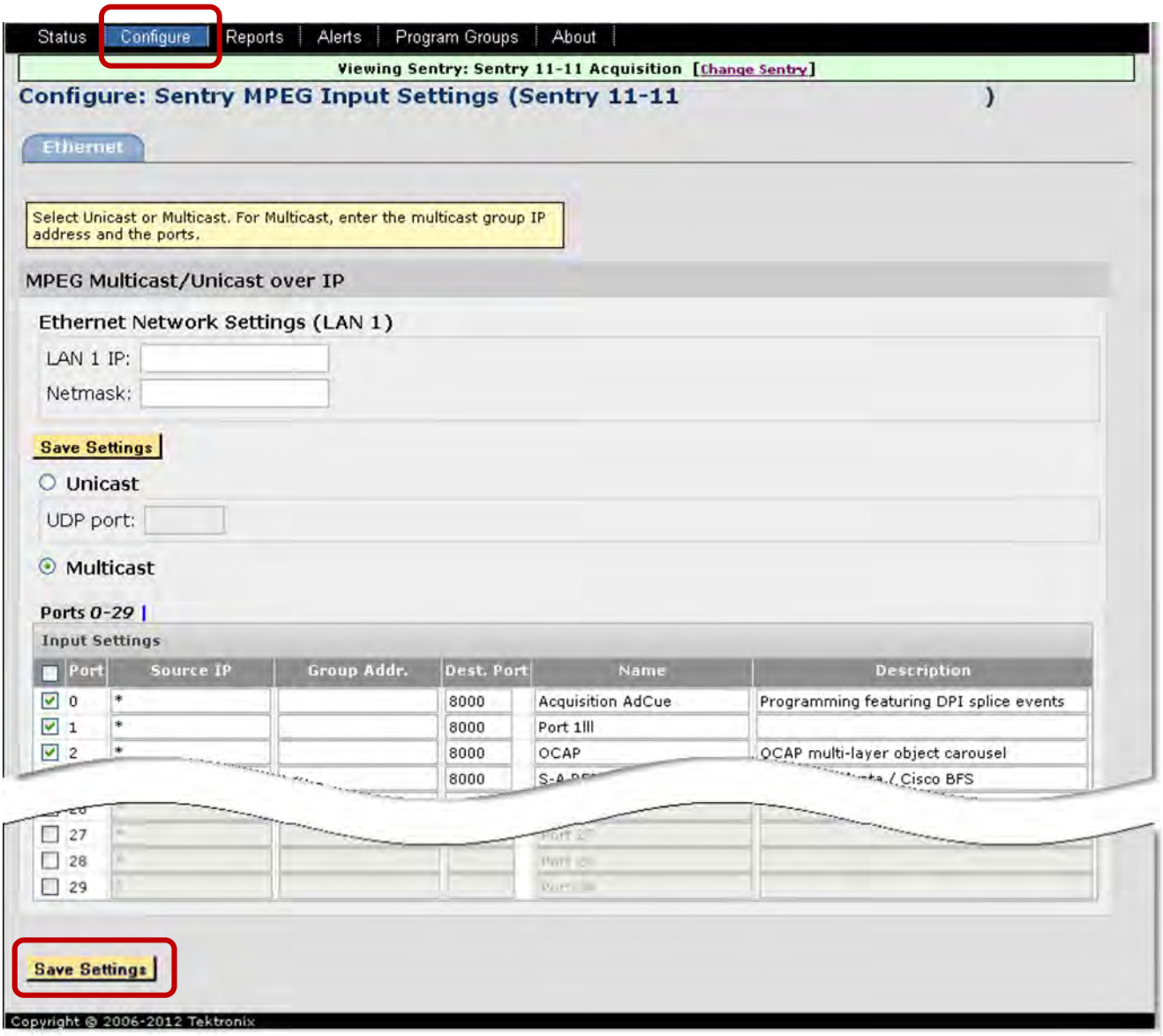



**Figure 130: MPEG over IP with Multicast**

4. Select **Save Settings** when finished.

## Sentry with VLAN Support Enabled

Any Sentry may be licensed to monitor MPEG content on VLANs (Virtual Local Area Networks). (Contact Customer Service for more information on enabling this feature.)

A system that is licensed for **VLAN Monitoring** will have a **VLAN Enabled** checkbox in the upper right section of the **Ethernet MPEG Input Configuration** page.

### *Configure VLAN monitoring option*

1. Select the **VLAN Enabled** checkbox to allow configuration of the VLANs that you will be monitoring.

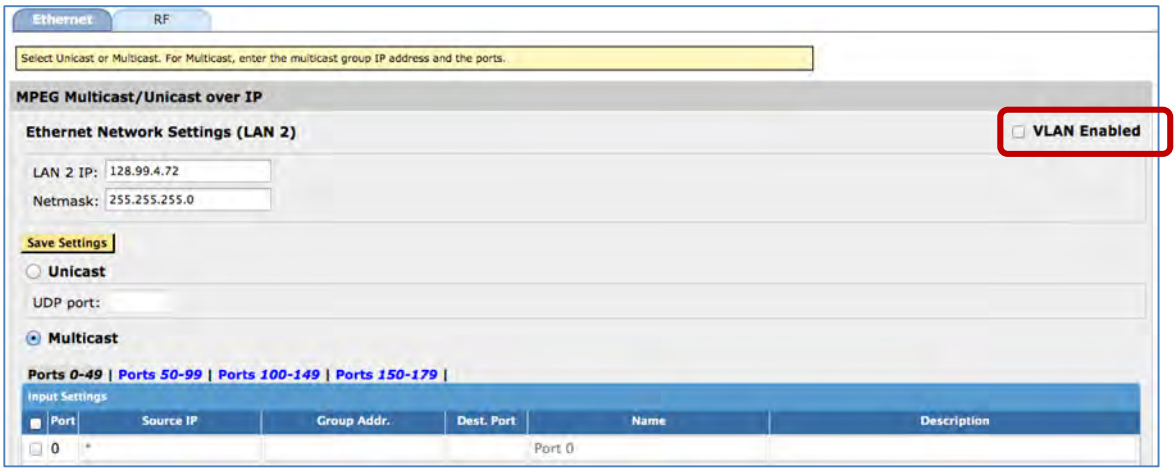



**Figure 131: Sentry with VLAN Enabled support**

---

**NOTE**: *You may elect to not enable VLAN on any Ethernet input, and continue to monitor inputs from a physical LAN.*

*Before you attempt to use VLAN Monitoring, please familiarize yourself with the specifics of your network. Each VLAN requires a network address, gateway and subnet mask to associate with the VLAN.*

*In effect, each VLAN is a treated as an independent network interface by the Sentry.*

---

2. The first time you configure your VLANs, you will see the following:

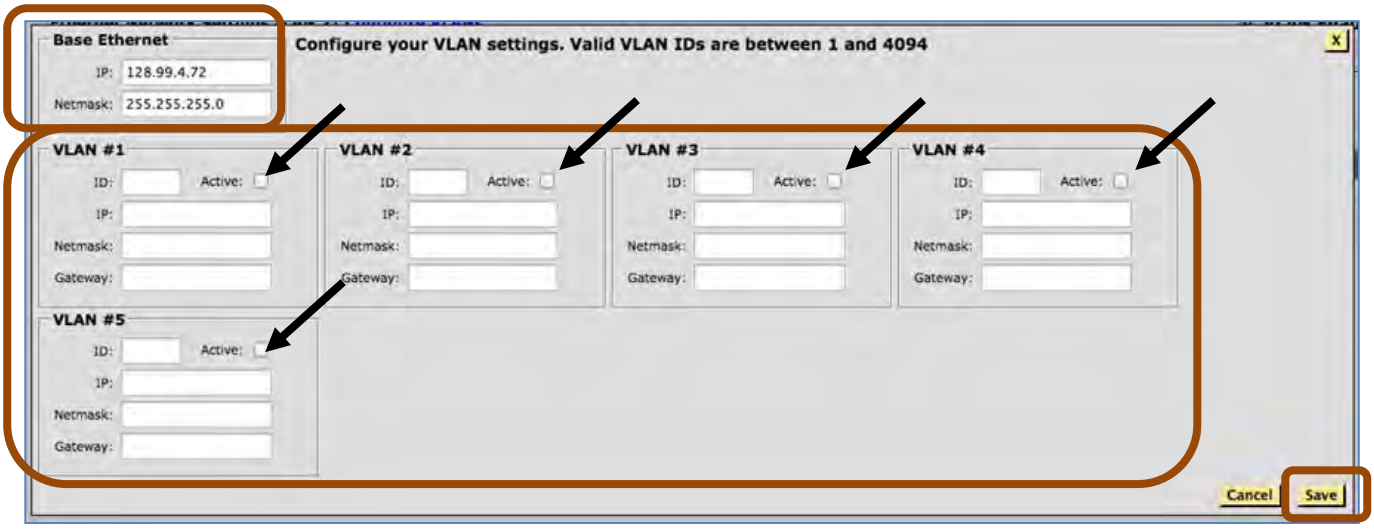



**Figure 132: Configure VLAN settings**

3. Enter the Base Ethernet settings. These are the standard IP and Netmask for the physical Ethernet input.

4. You will see VLANs on each Ethernet input, up to your licensed maximum. Define the following for each available VLAN:
   - **ID (**Valid values are 1-4094. These must be unique within a given Ethernet input)
   - **IP Address**
   - **Netmask**
   - **Gateway**

5. Select Active for each VLAN you'd like to monitor. Using this checkbox, you may also de-activate a VLAN for system maintenance as needed.

6. Select Save when you have completed your VLAN configuration.

7. You will now see tabs for each of the VLANs on that input.

8. Inactive VLANs will show up as gray tabs.

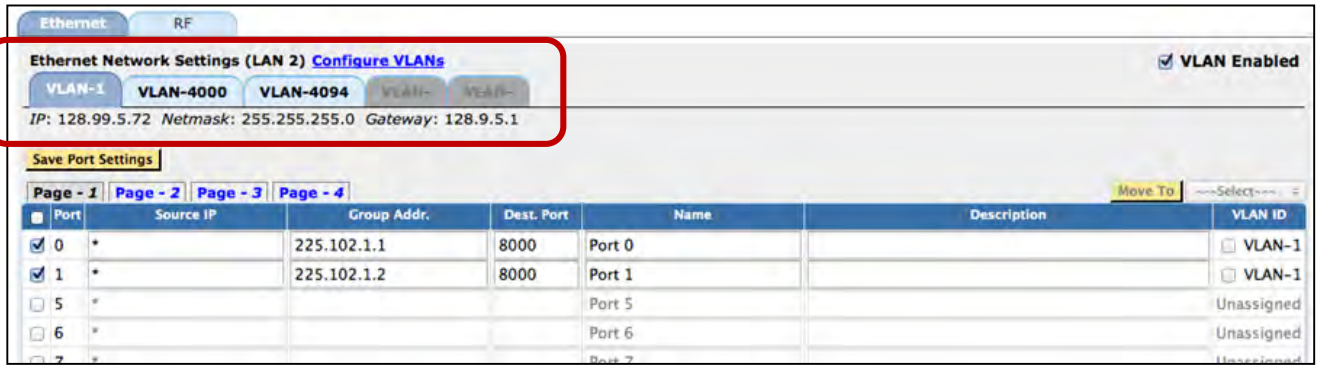



**Figure 133: Newly created VLAN tabs**

### Assign/Configure Ports on a VLAN

1. Select the tab for your desired VLAN. This VLAN tab will first list the ports that are already configured on that VLAN, and then all of the unassigned ports (those that are not configured and assigned to a given VLAN).

2. Select the check box to the left of any unassigned port and enter the **Source IP**, **Group Address**, **Destination** and **Port Name** (and **Description** if desired).

---

**NOTE**: *Each multicast **Source IP**, **Group Address** and **Destination Port** combination must be unique within a given VLAN.*

*If the **Source IP** uses the * wildcard, then the **Group Address / Destination Port** combinations must be unique.*

*Each VLAN, however, can monitor the same multicast **Source IP**, **Group Address** and **Destination Port** if desired.*

---

3. Select **Save Port Settings**, to assign those newly configured ports to the VLAN.

### Move a Port between VLANs

1. Select the checkbox in the **VLAN ID** column of the ports that you would like to move:

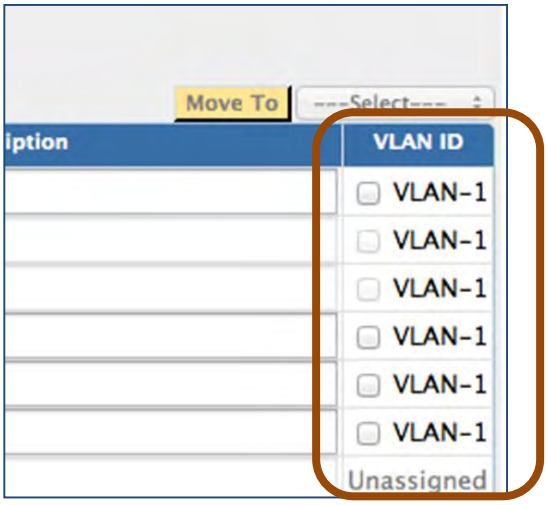



**Figure 134: Choose a VLAN ID**

2. Select the VLAN you are moving the ports to via the drop down menu.

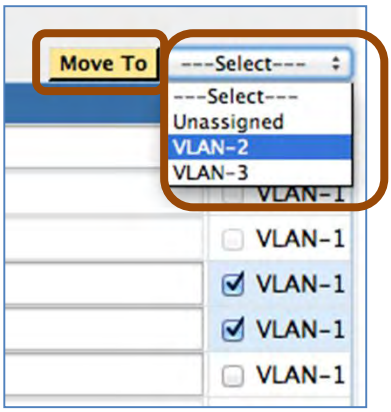



**Figure 135: Select a VLAN to move selected items to**

3. After choosing the destination, select **Move To** and the ports will be reassigned**.**

## *Reviewing Port/VLAN Assignments and VLAN Status*

Select **Reports-**and then **Status** to view all of the configured ports, the VLANs to which they are assigned and the status of each configured VLAN.

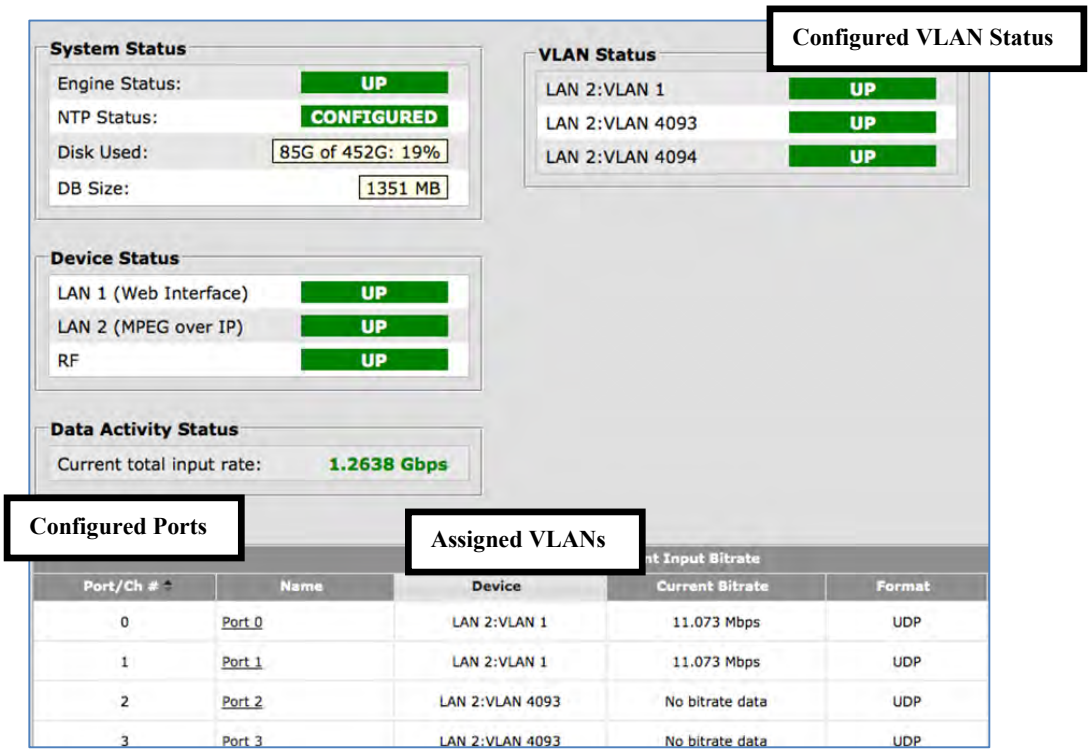



**Figure 136: Reviewing Port/VLAN status**

---

**NOTE***: **VLAN Configurations** and **Port/VLAN** assignments are supported in the **CSV Import/Export files**.*

***Port/VLAN** assignments are supported via the Sentry API methods.*

---

# Sentry Users

Sentry supports any number of users. Users are defined by two categories of privileges: **Administrator** and Regular **User**. An **Administrator** can make configuration changes while a **Regular User** cannot. An **Administrator** must therefore create all user accounts. **Sentry Users** are also independent of **Medius Users**.

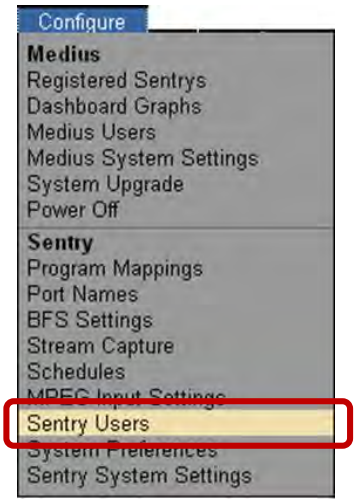



**Figure 137: Sentry Users**

## Add a User

**CAUTION**: ***All Administrator passwords must be kept in a secure location. If you forget your Administrator password, contact Tektronix Customer Support.***

1. Select **Edit** for the Sentry you wish to configure.

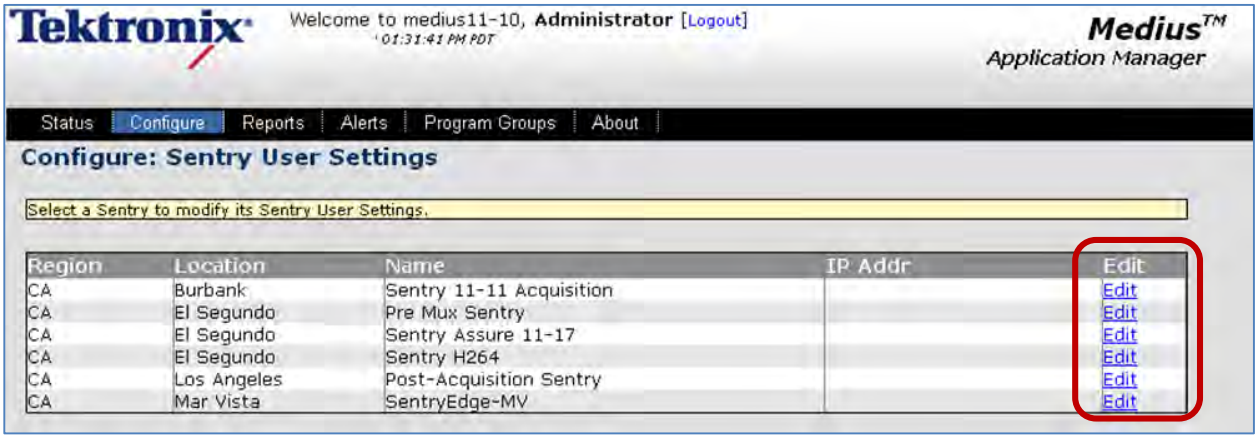



**Figure 138: Selecting a Sentry to Edit**

2. To add a new Sentry user, click **Add New User**.

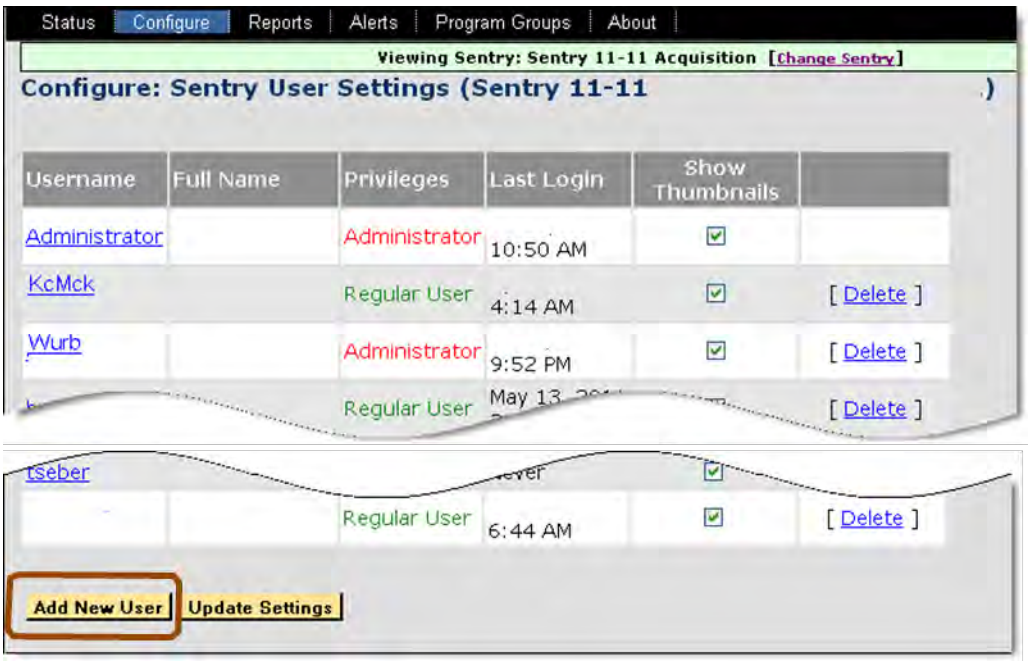



**Figure 139: Manage Users page**

3. Enter the new user's information

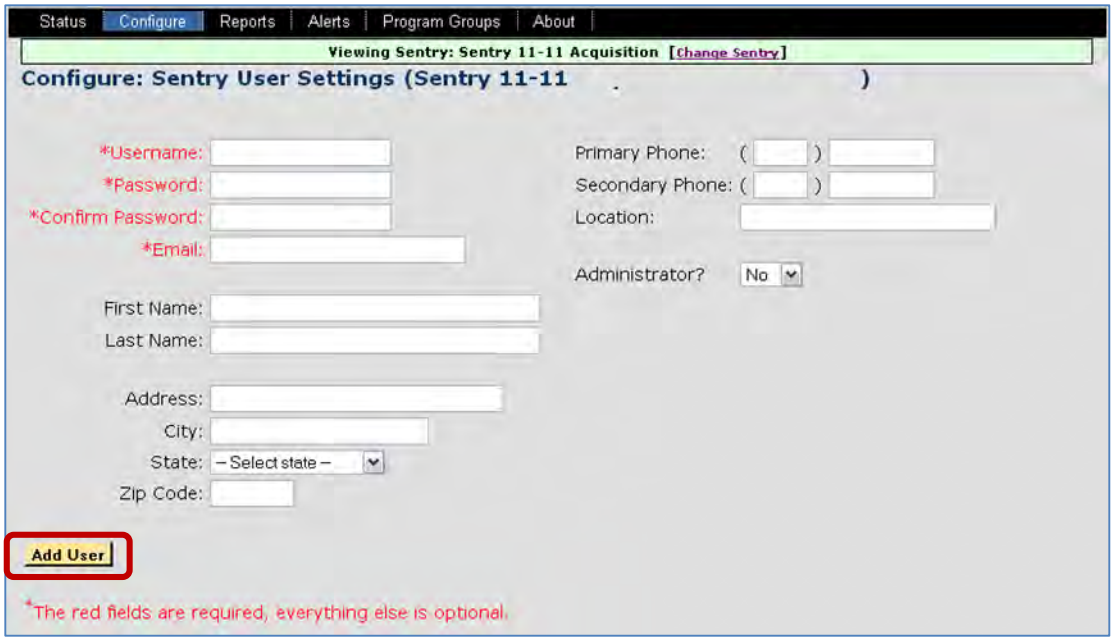



**Figure 140: Add User page**

4. Any information that is highlighted in red is required. Select **Add User** when complete.

## Delete a User

**CAUTION***: Once users are deleted, there is no recovery. You will have to re-create the user if needed.*

1. To delete a Sentry user select **Delete** located to the right of a user.
2. You will be presented with a confirmation dialog and, if confirmed, Sentry will remove the user from the system.
3. Select **Delete** from the **User Setting** screen.

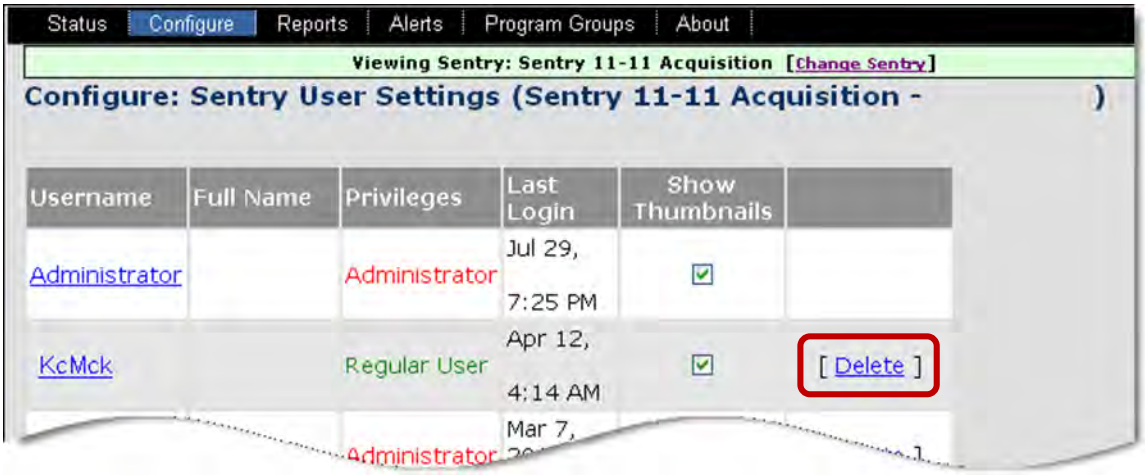



**Figure 141: Deleting a User**

4. Select the **Yes, delete this user** button.

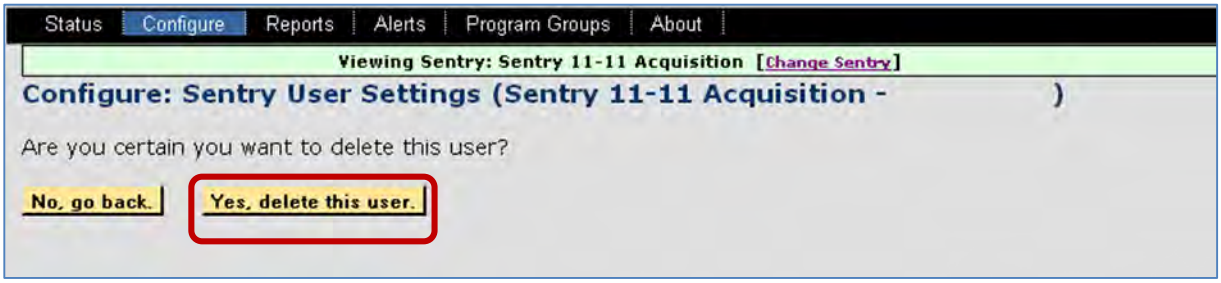



**Figure 142: Delete User Confirmation Page**

## Modify a User

1. To modify a Sentry user, select the **Username** link.


**Figure 143: Select a Username**

2. Enter the new information in the appropriate fields.

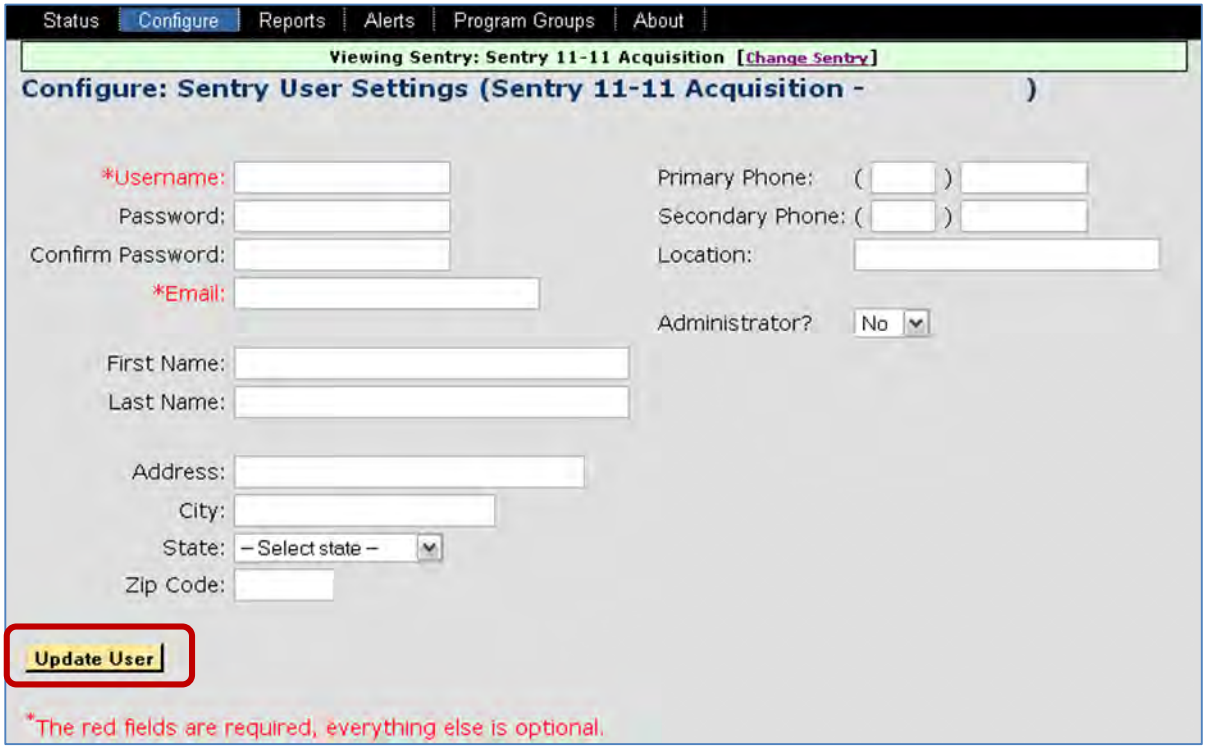



**Figure 144: Update User**

3. Click **Update User** to save the changes.

# Configure TR101/290 Settings

The Configure TR101/290 Settings page allows you to:

- Modify the thresholds for TR101/290 tests
- Disable any desired TR101/290 test

Choose **TR101/290 Settings** from the Configure menu, and then choose your desired Sentry and click **view**.

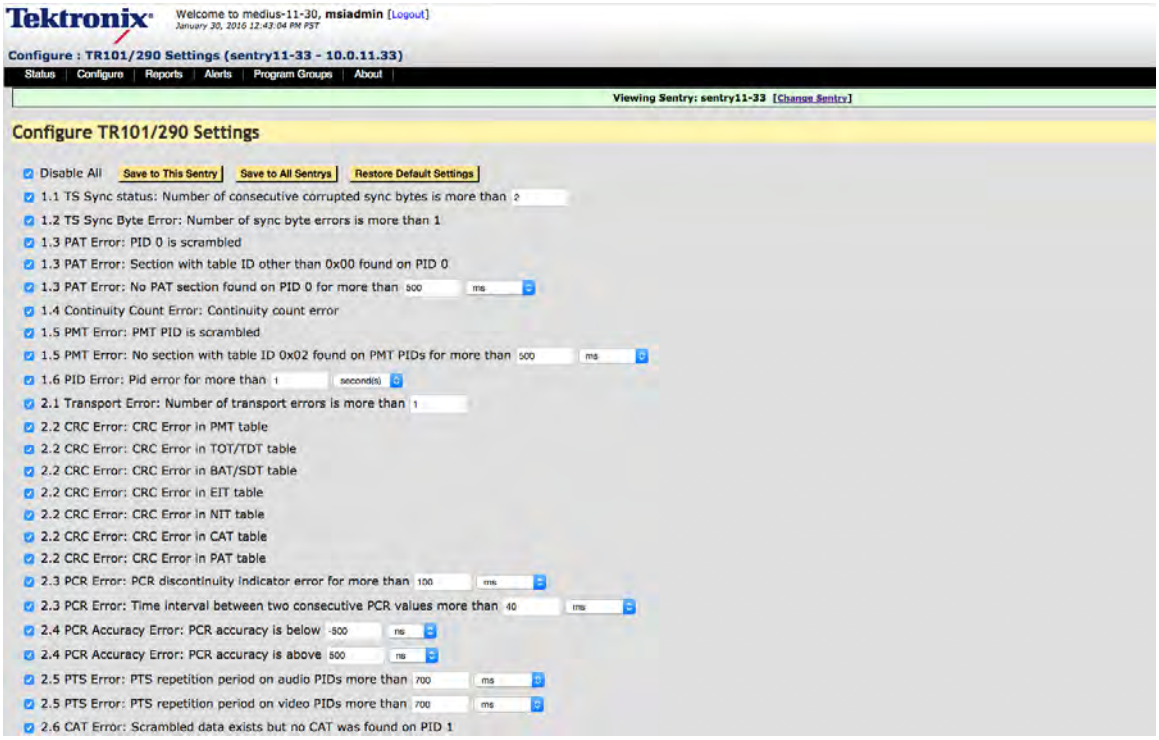
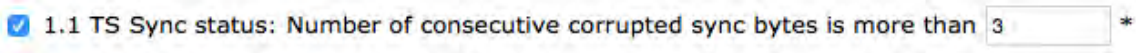



**Figure 145: TR101/290 Settings page**

To update any of the settings, make the changes on the page and click **Save to This Sentry**.
If you'd like the settings from the Sentry you are working on to be applied to all Sentrys, click **Save to All Sentrys**.

Click **Restore Default Settings** to refresh the screen with all of the factory default settings. You will then need to click **Save to This Sentry** or **Save to All Sentrys** to save the default settings.

All settings that are not using the default value will be denoted by an *.




Hover over the * to see the factory default setting.

Sentry will stop performing any of the disabled tests. Additionally, if all of the tests for a given priority are disabled, that priority will no longer appear on the TR101/290 Status report.

Note: Sentry is not designed for frequent disabling and re-enabling of a given priority. It is designed to permanently turn off tests that are of no value to you. Consequently, if a priority is disabled and then re-enabled, the TR101/290 Status report will show green blocks for the disabled period.

### *Ensuring Consistent Settings Across all Sentrys*

If you would like all TR101/290 settings to be the same across all Sentrys, make sure to click **Save to All Sentrys** whenever making changes.

If there are any differences between the Sentry you are working on and all other registered Sentrys a warning will appear:

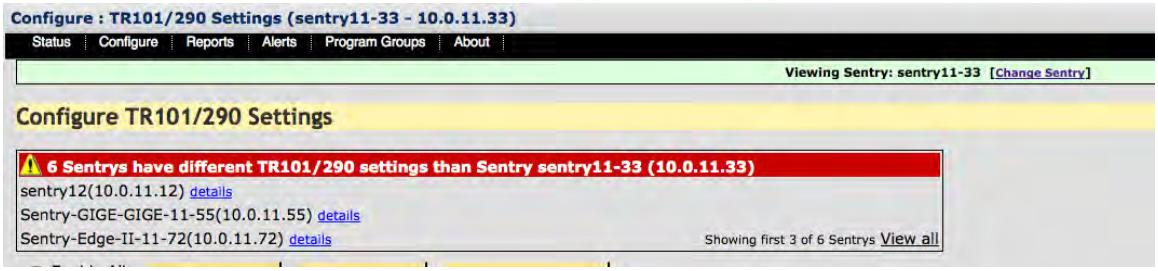



**Figure 146: TR101/290 warning message**

To review the differences with the listed Sentrys click **details**.

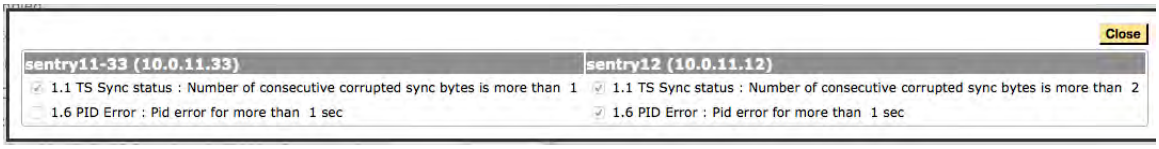



**Figure 147: TR101/290 warning message details**

Click **View All** to see the complete list of Sentrys with differences.

# System Preferences

The **System Preferences** page offers options for **Ad Cue PIDs, Perceptual Video Quality (eMOS) Settings, Default Provider Name Settings and Thumbnail settings.**

1. Choose **System Preferences** from the **Configure** menu
2. Select the desired settings and then select **Save Settings** when complete.

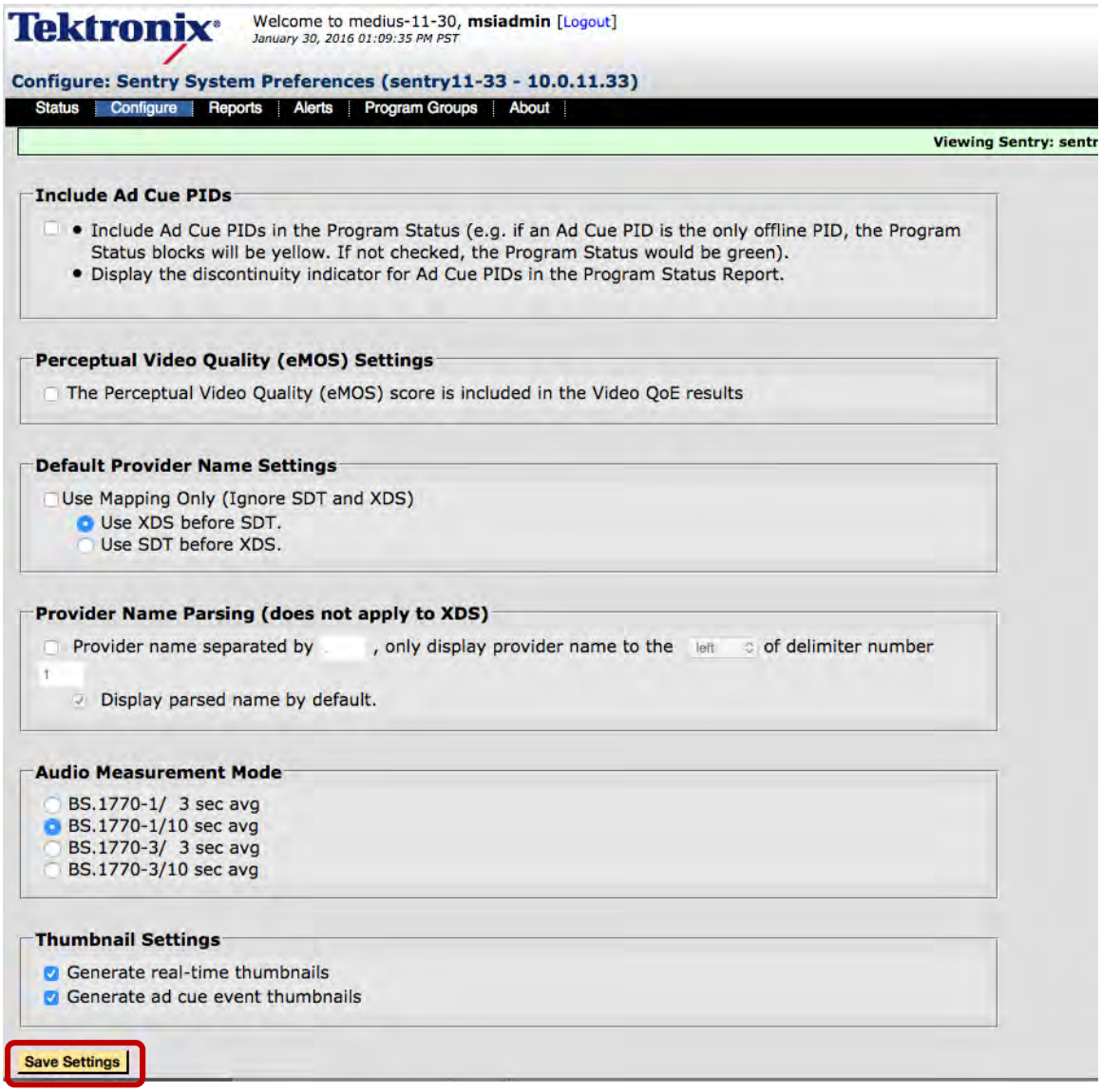



**Figure 148: Selecting a Sentry to Edit**

# Sentry System Settings

There are three categories of **Sentry System Settings: Network**, **Time** and **Locale**.

## Access Sentry System Settings tabs

1. Select **Sentry System Settings** from the **Configure** drop-down menu.

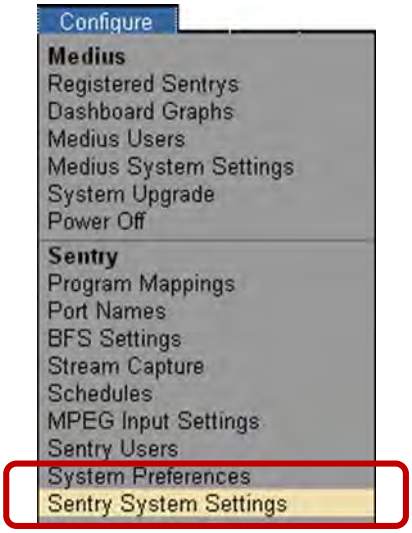



**Figure 149: System Settings menu**

2. Select **Edit** for the Sentry you wish to configure.

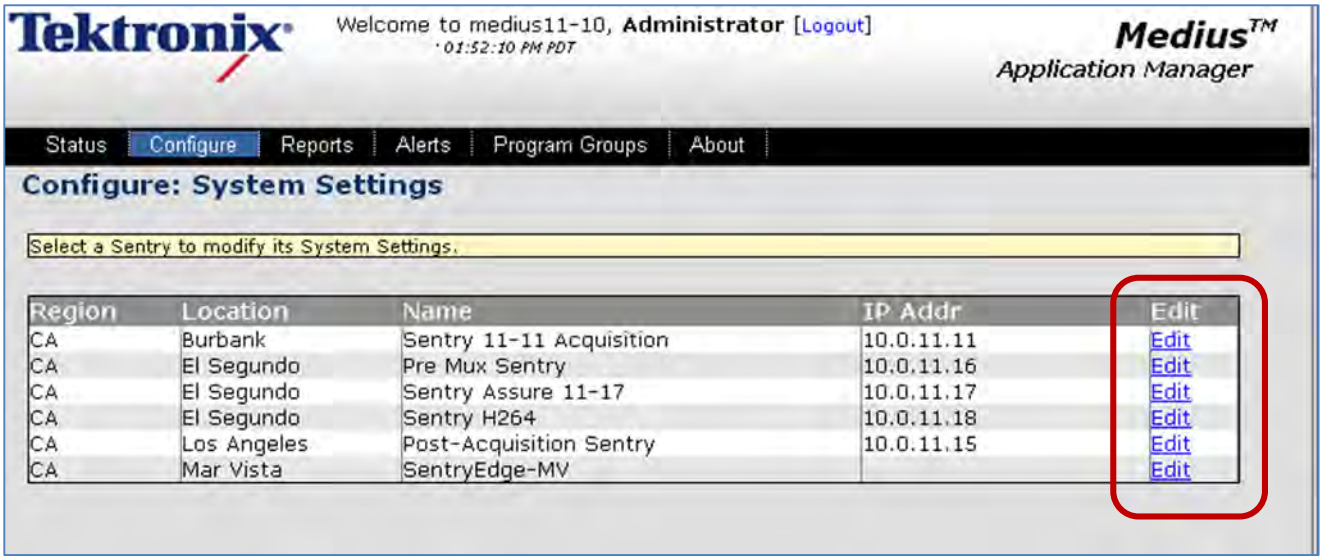



**Figure 150: Selecting a Sentry to Edit**

# Sentry Network Settings

**NOTE 1**: ***Changing this information may affect your ability to access Sentry or receive alerts.***

**NOTE 2**: ***Click on the Network or Time tab to refresh the page.***

1. Click on the **Network** tab to view the network system settings.

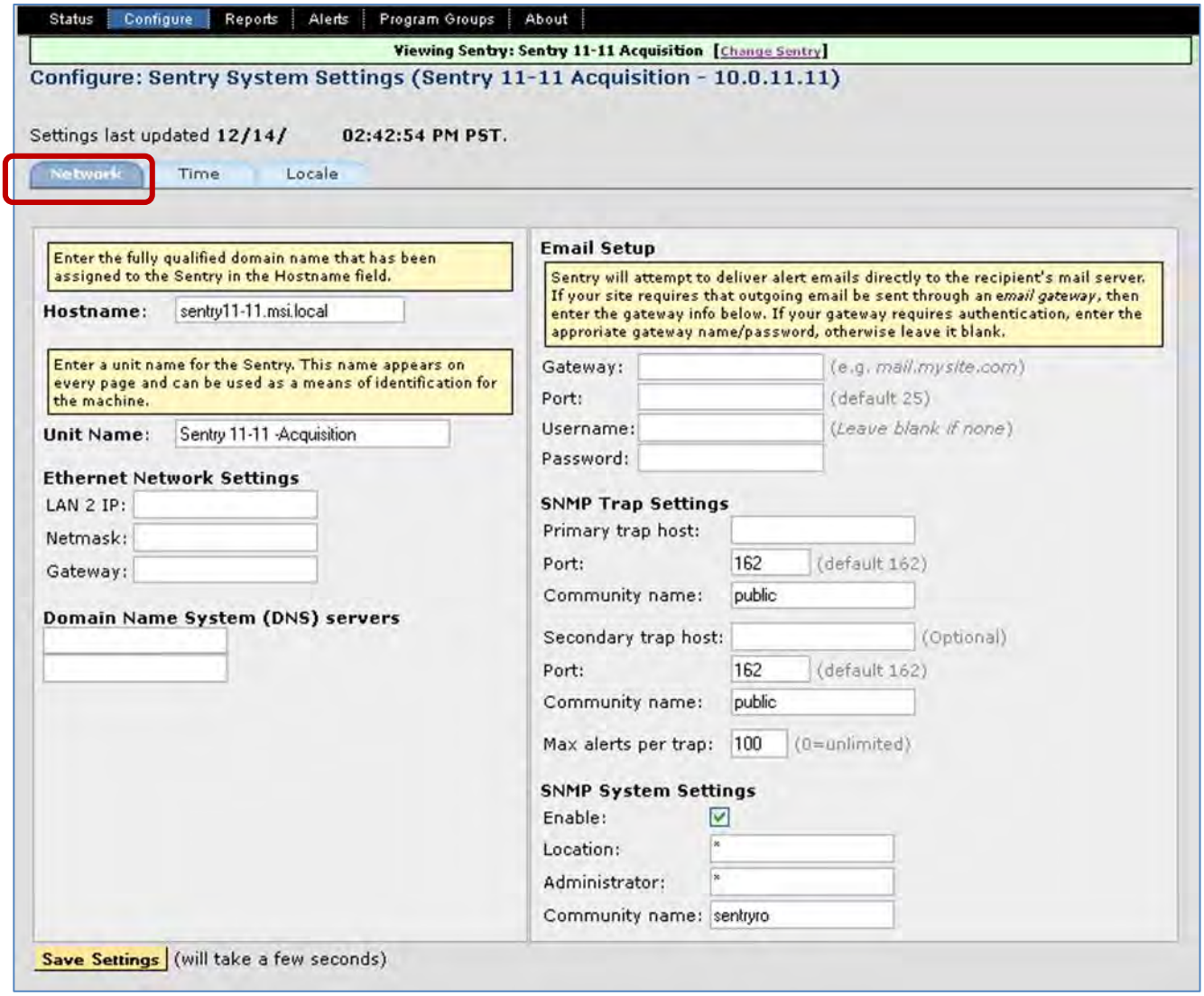



**Figure 151: Configure System Settings: Network tab**

**2.** The **Network** page allows you to specify Sentry's full name and configure the LAN2 Ethernet connection, the management connection that enables Sentry's web interface. TCP/IP and the internet require that every host, i.e., computer, be uniquely identified by both name and address.

- **Hostname**
  This is Sentry's full name, specifically its fully qualified domain name (FQDN).

- **Ethernet Network Settings**
  Enter the IP address that has been assigned by the network administrator to Sentry's LAN2 network interface, and enter the Netmask and Gateway IP addresses that apply to your network. Your network administrator should be able to advise you on the values that are correct for your network.

- **Email Setup**
  Sentry will attempt to deliver alert notification emails directly to the recipient's mail server. If your site requires that all outgoing email be sent through an email gateway, then enter the fully qualified domain name (or IP address) of the gateway in the Gateway field. Enter the port number that the email server is listening on in the Port field. If your gateway requires authentication, enter the appropriate name/password; otherwise leave it blank.

- **Domain Name System (DNS) Servers**
  Sentry uses DNS to translate domain names into IP addresses (and vice versa) while sending alert emails, among other things. Specify the fully qualified domain name or IP address of at least one DNS server.

- **SNMP Settings**
  SNMP (Simple Network Management Protocol) provides the ability to send traps, or notifications, when one or more conditions have been met. Enter the IP address of the SNMP manager, which will receive the trap, in the Trap host IP field. Enter the port number that the SNMP manager is listening on in the Port field. Enter the Community name of the SNMP agent, or client, in the Community name field. Click on the Download MIB link to download the MIB (Management Information Base) file used by the SNMP manager.

## Set the Time on Sentry

1. Select the **Time** tab to view the time system settings.

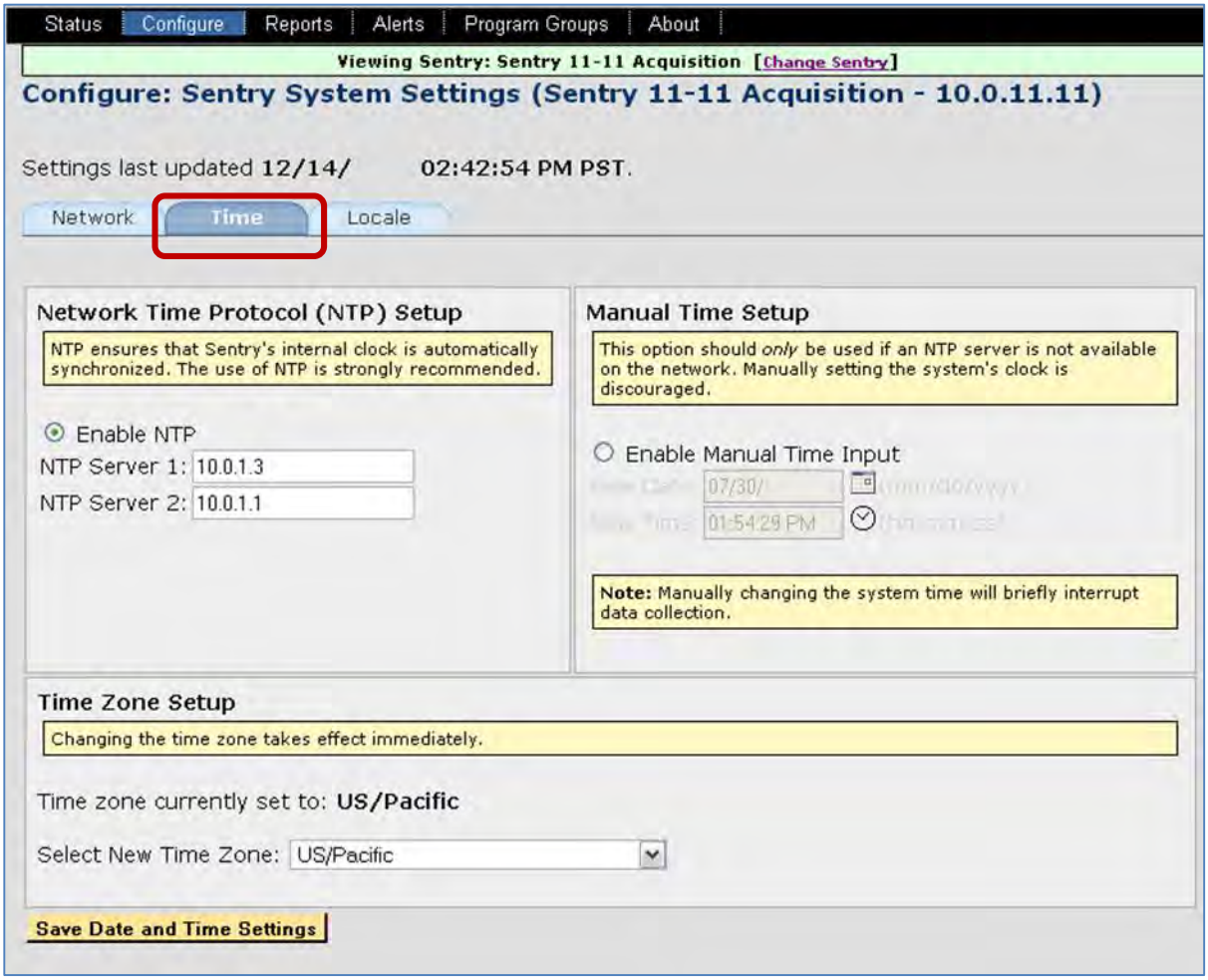



**Figure 152: Time tab**

The time page allows you to enter the IP addresses for the NTP server(s) and to manually set the **Time** and **Time Zone** if an installation does not have NTP servers.

- **Network Time Protocol (NTP) Setup**
  Sentry synchronizes its internal clock with external time servers to insure a high degree of accuracy. Specify the fully qualified domain name or IP address of at least one NTP server.

- **Manual Time Setup**
  For installations that do not have NTP servers, the time page provides the capability to set the **Time** and **Time Zone**. Entering a manual time sets the system clock to that time.

## Modify the Locale

1. To change the **Locale** of the Sentry, select the **Locale** tab.

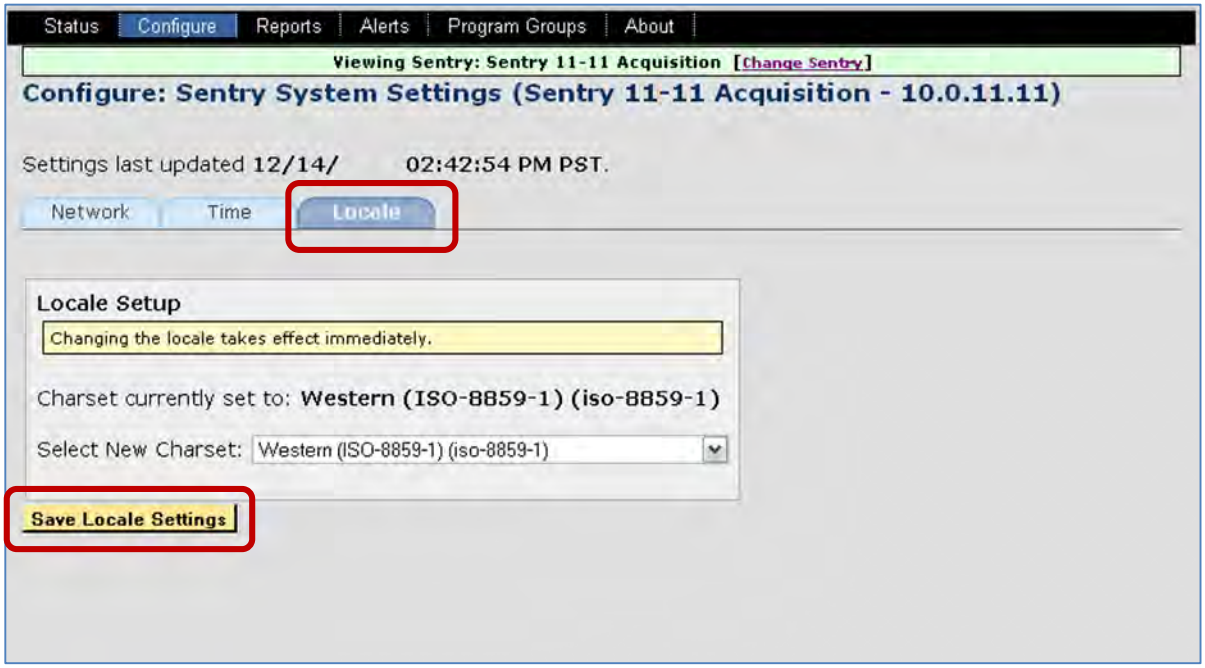



**Figure 153: Modifying a Locale**

2. Select **Save Local Settings** when finished.

# Reports

Medius **Program Groups Reports** provides an overview of the contents of the MPEG transport stream, and consist of four types: **Current Status**, **Program Status**, **Data Detect** and **Ad Cue Info**. **Current Status** and **Program Status** reports are MPEG program centric in the sense that all data and PIDs are grouped according to the programs with which they are associated. All **Reports** within Medius are based upon **Program Groups**.

## Why run a Medius report vs. a Sentry report?

1. Medius can generate reports with data aggregated from multiple Sentrys, while Sentry reports are based on data from a single Sentry.

2. Medius allows you to generate reports only on services you want to see. These program groups could consist of all services in a particular MUX group, all premium services, different ad zones, etc. You can use **Program Groups** to compare like services from different parts of the network.

# Current Status

**Current Status** allows the user a quick view of the program groups available on any given Sentry assigned to the Medius.

**Current Status** also features **thumbnail visual confirmation** of the content of each program or service. You may control the size of the **thumbnail** at the top of the column. You may refresh the thumbnail manually or it will refresh automatically every 5 minutes.

## Access Current Status

1. Select **Current Status** (under **Medius Program Groups**) from the **Reports** drop-down menu.

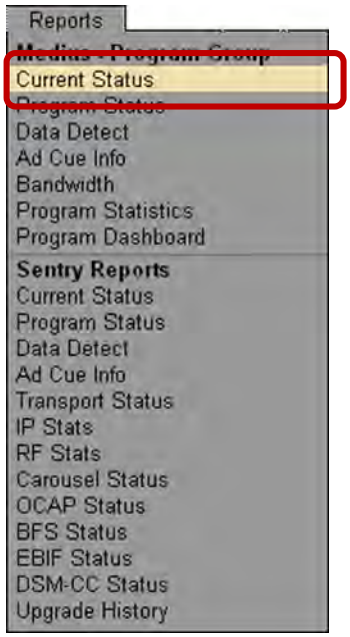



**Figure 154: Accessing Current Status**

2. Next, choose a **Program Group** from the drop-down menu.


**Figure 155: Selecting Program Group**

3. For most functions, leave **Provider Name** on **Auto**.
4. Auto will automatically choose a service name depending on data that is available
5. Choose **Results** per page.
6. Select **Refresh**.

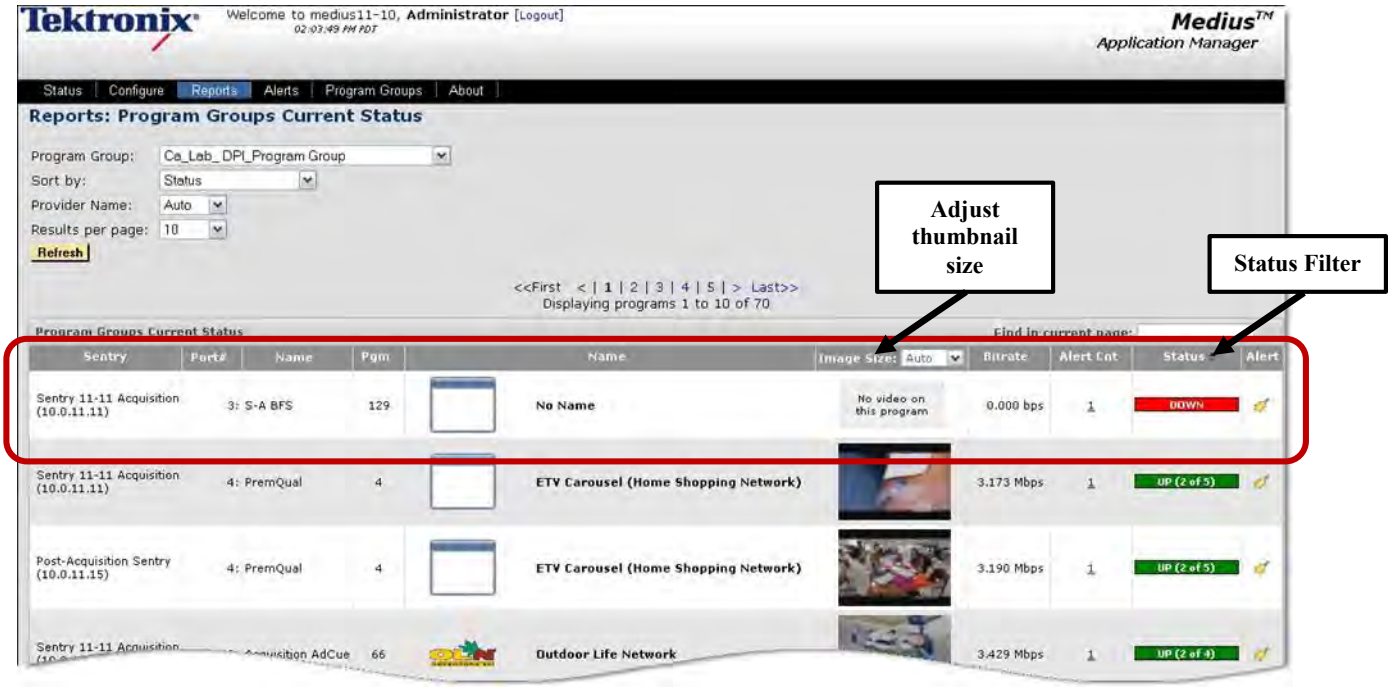



**Figure 156: Current Status component columns**

Components of the **Current Status** report are:

- **Port #** and **Name**
  The number and name of the input port receiving the data
- **Pgm (Program Number)**
  The program number that was derived from monitoring the transport stream.
- **Name**
  - The program provider icon and name, derived according to the **Provider Name** selection.
  - If Sentry cannot determine the provider, a placeholder will be inserted, e.g., **Not Available**.
  - The user can also manually associate a network name and icon with a program using **Configuring Mappings** for each Sentry. XDS data consisting of the show name and rating is also displayed if it exists.
- **Bitrate**
  The current bitrate of the program. It refreshes about every 60 seconds.
- **Alert Count**
  The number of active alerts for each program.

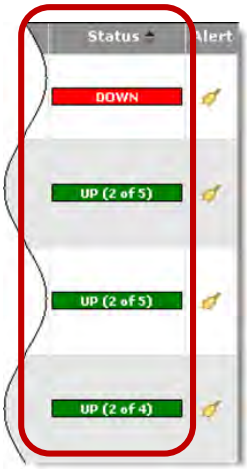



**Figure 157: Status column and Alert column in Current Status**

- **Status**
  - Shows **UP** (green) if all **PIDs** in the program are getting data. If some but not all PIDs are getting data, the **Status** displays **UP** along with the number of up **PIDs** out of all **PIDs**, (example., **UP(2 of 4**.)
  - The **Status** will display **DOWN** (red) if the bitrate for all **PIDs** is zero. If there is no bandwidth information, Current **Bitrate** shows "**No bitrate data**" and the **Status** is **DOWN**.

---

**NOTE**: ***The only time that Sentry will not receive bandwidth data is when there is a Bandwidth Violation.***

---

- **Alert Icon**

  When selected, will automatically display and configure the **Creating Program Alerts** page for the chosen program.

# Program Status

The **Program Status** report (located under Medius **Program Group**) gives a configurable history of all MPEG programs and their PID contents.

## Access Program Status

1. Select **Program Status** from the **Reports** drop-down menu.

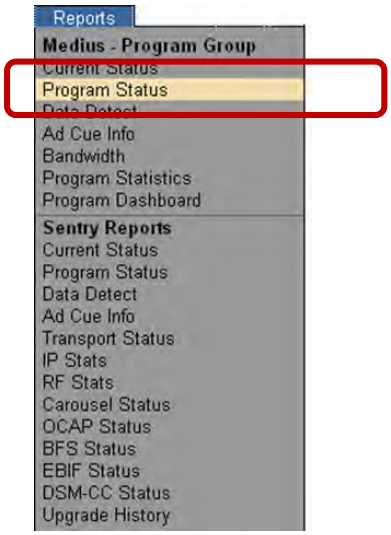



**Figure 158: Accessing Program Status**

2. Next select the **Program Group** you wish to view and then select **Refresh**.

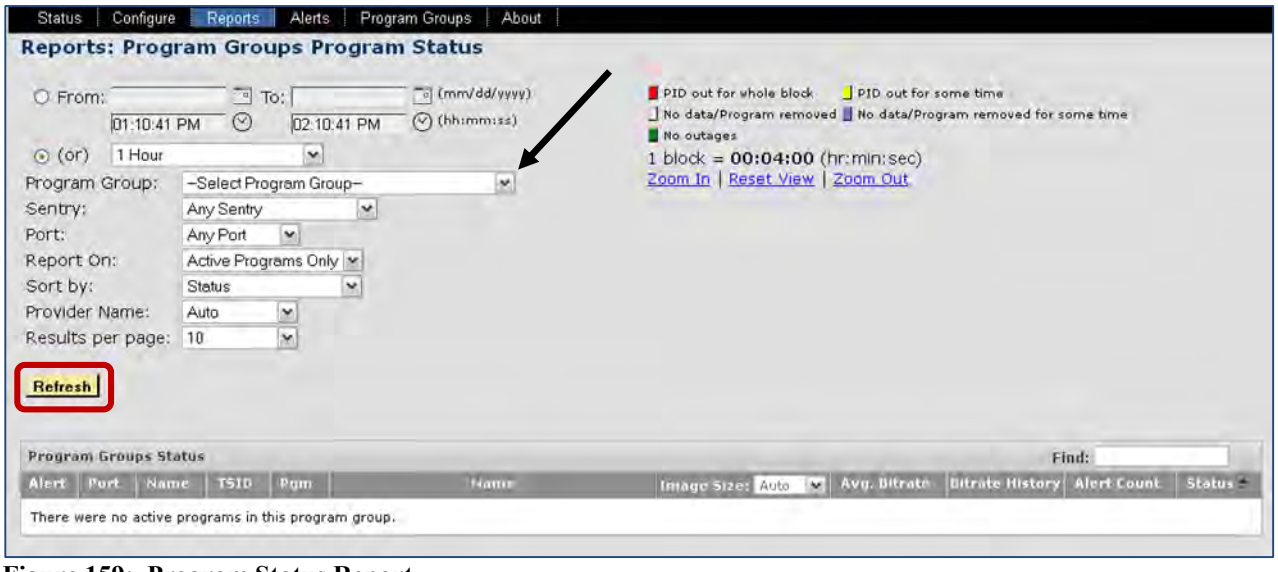



**Figure 159: Program Status Report**

3. The page will expand to include the selected **Program Groups**.

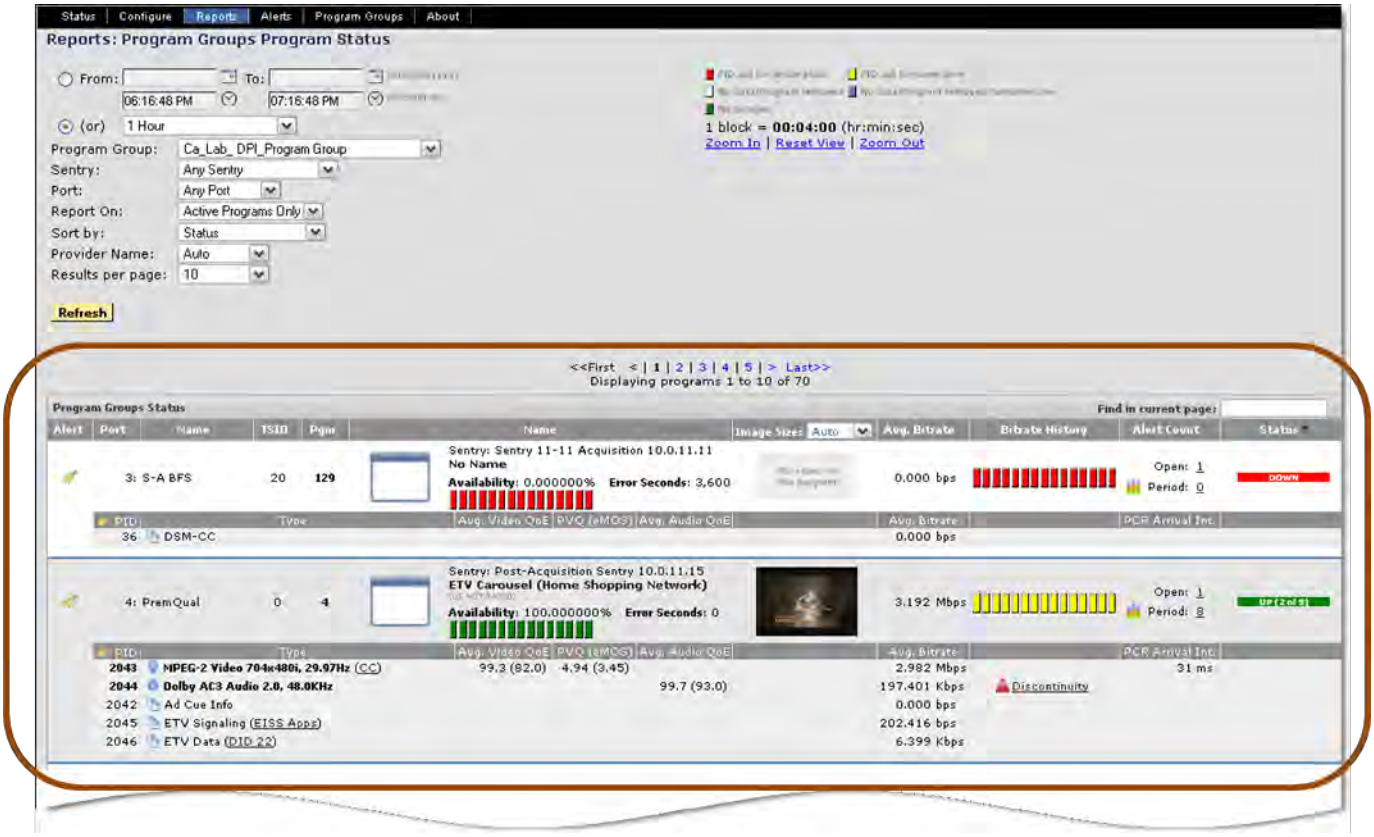



**Figure 160: Expanded view of Program Groups**

4. In addition to the same components seen in the **Current Status Snapshot** report (i.e., **Alert, Port#: Name**, **Pgm**, **Name**, **XDS data**), the **Program Status** report has the following additional components:

- **TSID** is the **Transport Stream ID** derived from monitoring the stream.
- **Avg. Bitrate** is the program bitrate averaged over the time range.
- **History of PID** data in the stream over the selected time range, shown as color-coded discrete blocks.
  - **Gray** indicates no data
  - **Yellow** shows there was a PID out for some time
  - **Red** means there was a PID out for the whole block
  - **Green** shows no outages
- **Alert Count** shows the amount of alerts that are open over a given period. Selecting the Trend Detail **Graph** will take you to **Alert Trends** if there are alerts for this program.

- **Current Status** shows you if the program is up or down and if it is missing any PIDs.
- **Video and Audio QoE** shows the average and minimum **QoE** scores for the specified time period.
- **PCR PID Arrival Interval** tells you which **PID** is carrying **PCR** as well as the average arrival interval for a given time period.
- **Program PID Detail** shows each **PID** associated with the program: the **PID** number, type, data content, PID average bitrate and an indication whether and discontinuities, i.e., breaks in the sequence of MPEG transport packets detected by Sentry's continuity counter, have occurred.
- The presence of discontinuities is indicated by a **Discontinuity** notification. The absence of any notification means there have been no discontinuities.
    - Three types of PID indicators will be drawn for **Video**, **Audio** and **Data PIDs**. An indication of **CGMS**, **CC** (Closed Caption), or **Scrambled** data follows the PID type if applicable and you can click on a data type to display the **Data Detect Report** for the program and the data.

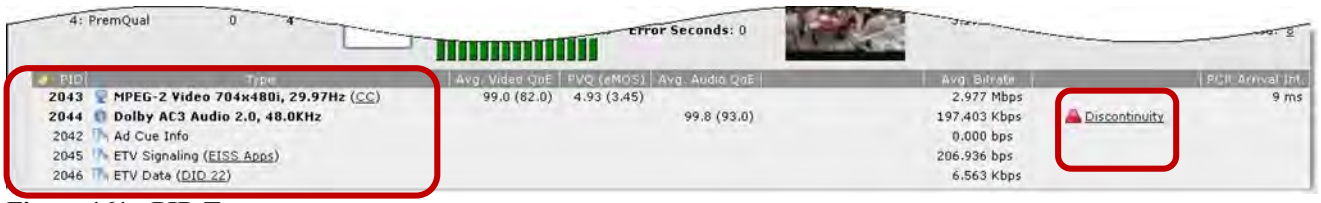



**Figure 161: PID Types**

## Other features

### *Sort by Video/Audio QoE*

To view the **Average** and **Minimum QoE** scores, you may sort by them in the top section of any **Program Status** page.

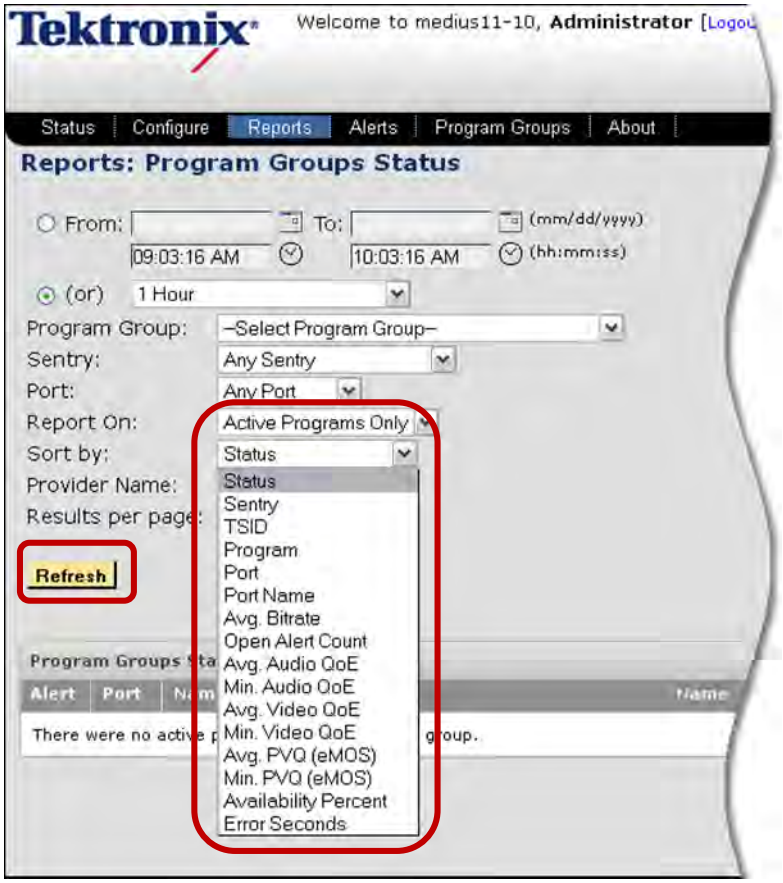



**Figure 162: Sort By drop down menu Figure 163: Sort By drop down menu**

## Program search and display

You may search any **Current Status** page for any Sentry under Medius using the search box located in the upper right corner of the table.

This function is available both on the **Group Current Status** page and the individual **Status** page.


**Figure 164: Search and Display for the search on "di"**

The program search will search the current page based on what you enter into the field. You may enter either the program name, or the service name.

The program search will only search for what is currently displayed. For example, if you have 100 programs on the screen, but there are 137 programs overall, it will only search on the displayed 100 programs.

To conduct a search, simply enter the search term into the field. **Program search** is a live search entry field meaning you only have to type your request, and the search will begin immediately. There is no need to hit return

### Column Sort By arrows

All primary column headers in the **Program Status Report** data include a **Sort by** arrow that allows for easy sorting.

To activate, click on the desired column header once and the resulting screen will return the same page with the available arrows in the column header.

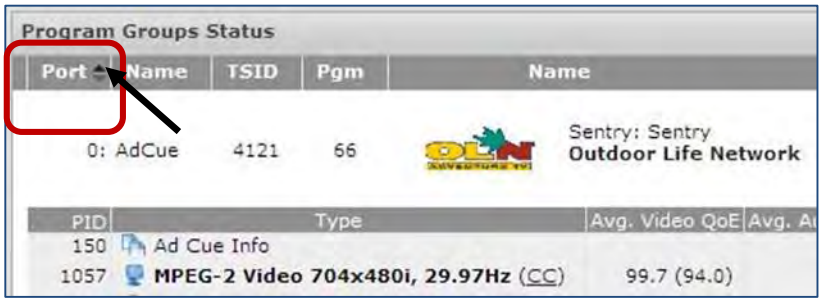



**Figure 165: Column header Sort By arrows**

# Data Detect

The **Data Detect** report (located under the **Medius Program Group** heading) is a detailed report on specific content within the MPEG transport stream.

## Access Data Detect

1. Select **Data Detect** from the **Reports** drop-down menu.

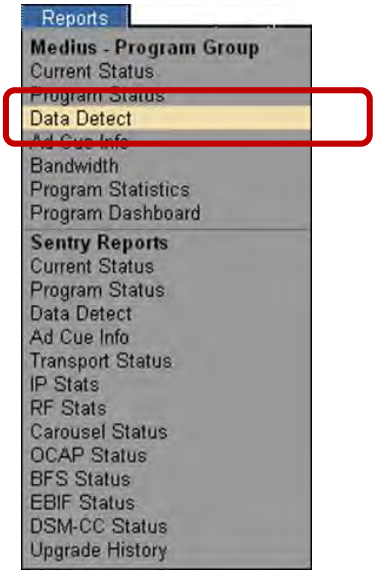



**Figure 166: Data Detect**

2. Next, select a **Program Group** from the drop-down menu.

3. Select the **Report Types** and then select **Generate Report.**

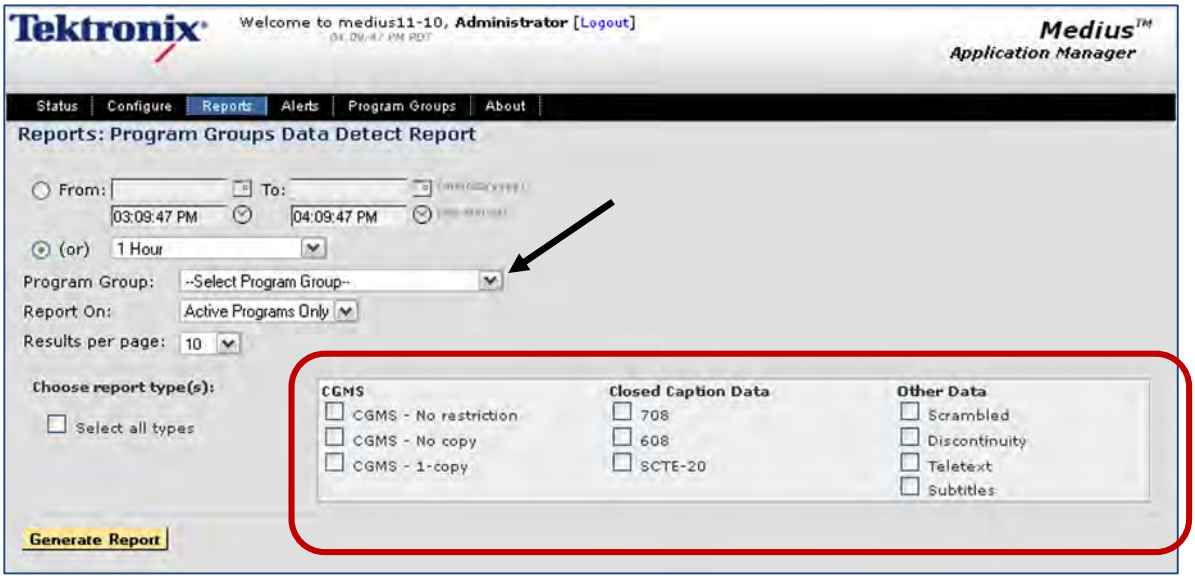



**Figure 167: Data Detect Report Types**

4. From **the Data Detect** report you can click on a **Program** number to view the **Program Detail View**.

   To view the **Closed Captioning** errors, hover pointer over any orange or red block for more information.

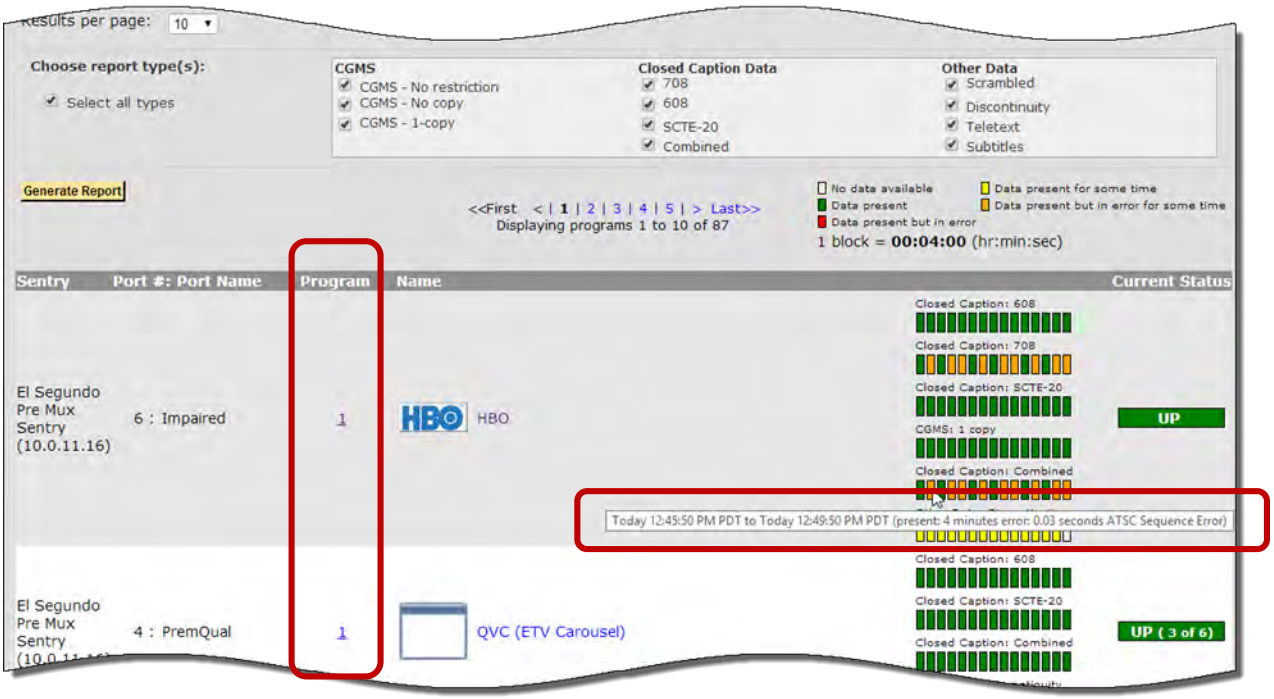



**Figure 168: Program Numbers in Data Detect overview page and error information**

A **Data Detect Report** can also be generated for one program only from the **Program Status** page or the **Program Detail** page by clicking on a link that represents one of the **Data Detect** report types (such as **CC**, **CGMS**, and **Discontinuity**).

The **Data Detect** report is automatically generated for the selected program and the selected report type. Other report types can be generated for the selected program by choosing the report type and clicking **Generate Report.**

# Ad Cue Info (Digital Ad Insertion)

With the advent of digital ad insertion, it has become difficult for both cable operators and the vendors of digital ad insertion equipment to verify that specific ads have actually run as contracted.

**Ad Insertion** systems separate splicing commands from the input transport stream, switch between the network feed and the local ad server, and provide signaling and coordination. Using the SCTE 35 splice format identifier values, Medius is able to monitor the commands that are being sent to the ad insertion device.

These values include:

- **Splice insert**
- **Splice null**
- **Splice schedule**
- **Time signal**
- **Bandwidth reservation**
- **Reserved**
- **Private commands**

## Access Ad Cue Info

1. From under the **Medius Program Group** header, select **Ad Cue Info** from the **Reports** drop-down menu.

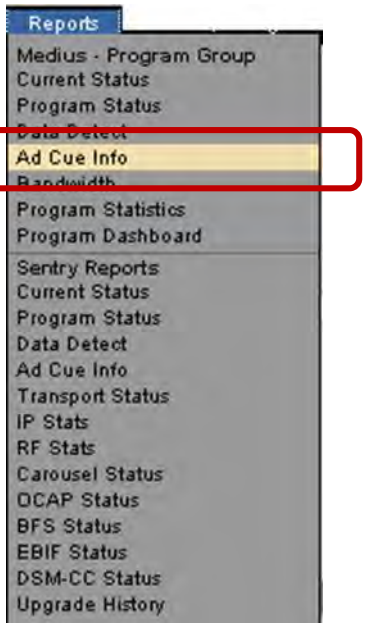



**Figure 169: Accessing Ad cue Info**

2. Select the **Program Group** you wish to view.

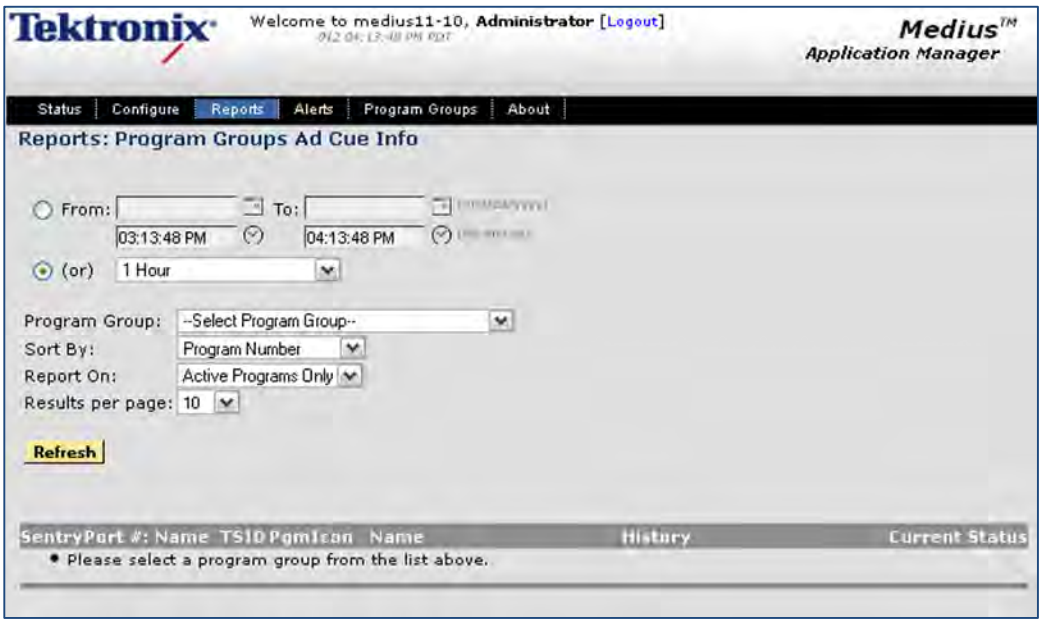



**Figure 170: Selecting a Program Group**

3. Select the time range of interest.

4. Select the **Program Group** and **Sort By** options as needed

5. Select **Refresh** to see the **Ad Cue Info** results.

---

**NOTE**: ***The Ad Cue Info report allows a time range up to two weeks in the future. This is the only report that allows future times!***

---

The **Ad Cue Info** report allows a time range up to two weeks in the future. This is the only report that allows future times!

## Reading the Ad Cue Info report

Medius monitors the **Event IDs** for the ads that are sent to the ad insertion device. Matching the **Event IDs** with the ad log of the ad insertion device will verify that the ad was received but there is no guarantee that the ad actually ran.

If Medius' reporting shows that the video and audio in the transport had no problems at the time of the ad, then it is likely that the ad ran.

The **Ad Cue Info** reports display the in points and the out points of the ad cue message that are used to signal the start and end of an insert and the **Event IDs** of the insert messages.

To drill down on the graph, select a portion with your mouse. Select **Reset View** to go back to the original graph.

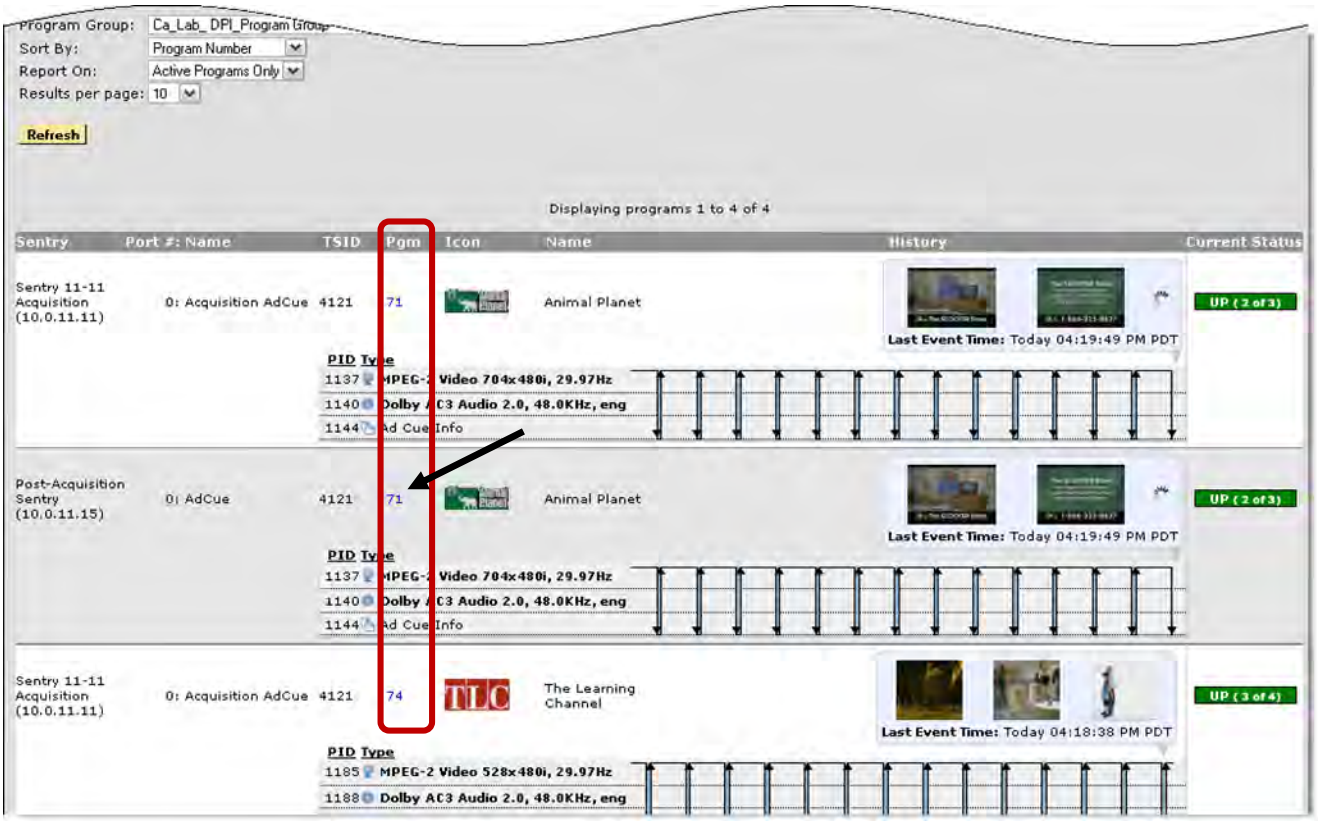



**Figure 171: Ad Cue Info report**

Click on a program link in the **Pgm** column of the **Ad Cue** Info display to view the details of the selected program's ad cues.

The **Ad Cue Info** reports display the in points and the out points of the ad cue message that are used to signal the start and end of an insert and the **Event IDs** of the insert messages.

Click on any program Icon to get a detailed report.

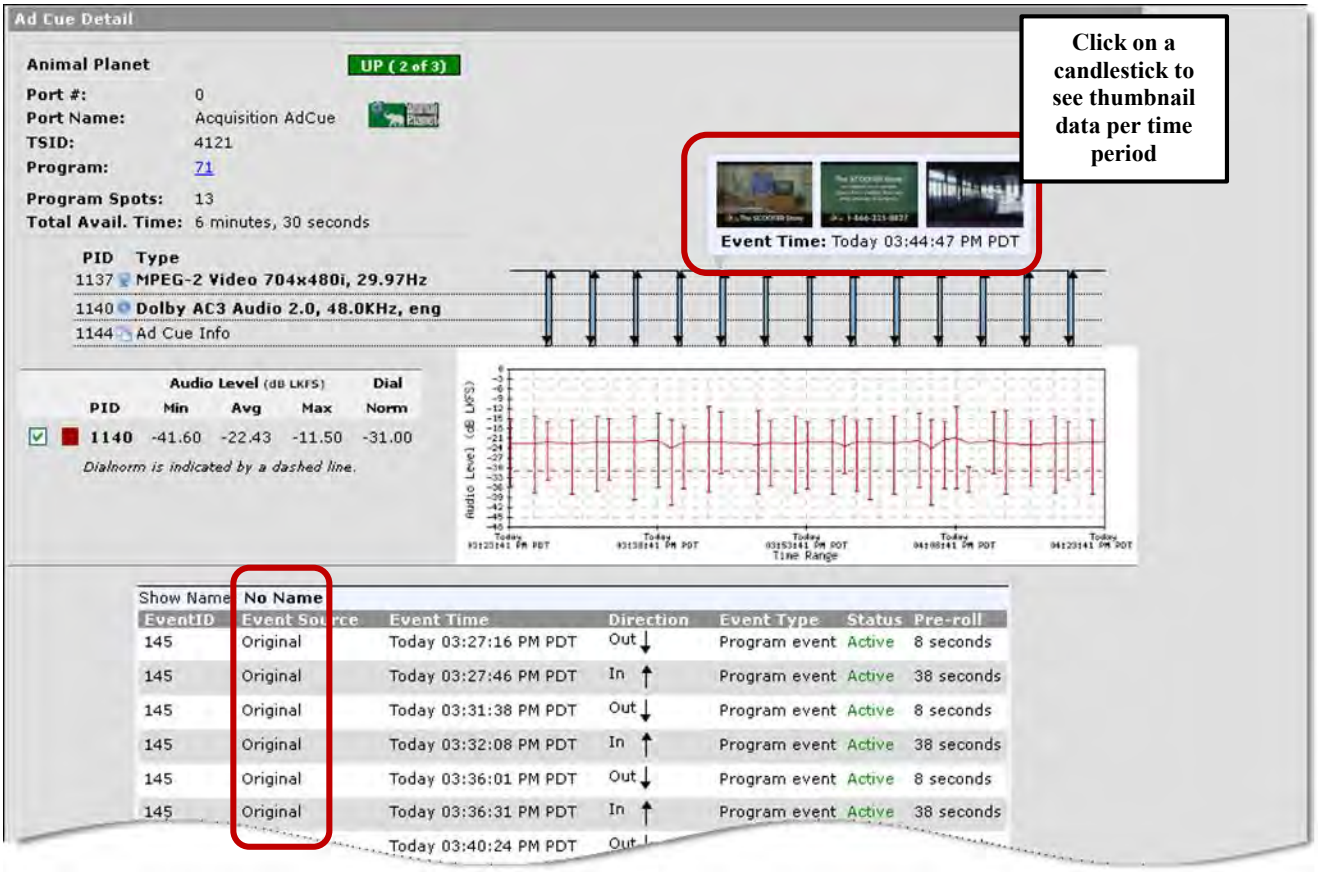



**Figure 172: Ad Cue Info Detail report**

### Type

The radio buttons directly above **Type** allow you to choose whether you want to see all command types, **Splice Insert Only,** or **Non-Splice Insert Only.**

### Event ID

Hover your mouse over the graphical display of an ad insertion point and a popup window will show up with the **Event ID**, the direction of the splice message, and the time that it occurred.

### Event Source

The **Event Source** indicates how the ad cue was inserted into the stream. It is only relevant for **Splice Insert Event**. Such events will be one of the following:

- **Original:** Cue embedded in original source material
- **Automation:** Cue created by automation system switching
- **Live:** Cue created by live event trigger system
- **Local:** Cue created by local content replacement system

### Direction

Indicates if the splice message is running **In** or **Out**.

**Event Type**
Ads are either component (**PID Event**) or composite (**Program Event**).

- A composite ad interrupts the program's audio and video (**Event Type = Program Event**).
- A component ad interrupts one or more but not all of the PIDs in a program (**Event Type = PID Event**).

**Status**
The **Status** of an ad cue splice insert is either **Active**, indicating that it was valid when it ran, or **Obsolete**, indicating that it was replaced by another event before it ran.

**Pre-roll**
For splice insert events, the amount of time between the sending of the event and the actual running of the ad.

**Descriptor**
Each ad splice command might contain additional descriptor information that carries additional data about the specific command. When descriptor information is present for a command, the **Descriptor** column will have a **View** link. Hover over that link to see the descriptor for that command.

## Ad Splice Command Types

The **Ad Splice Command Types** graph displays all of the command types that were sent. Each command may also contain descriptor information.

To view the descriptor information for a command type, hover over the appropriate bar on the graph.

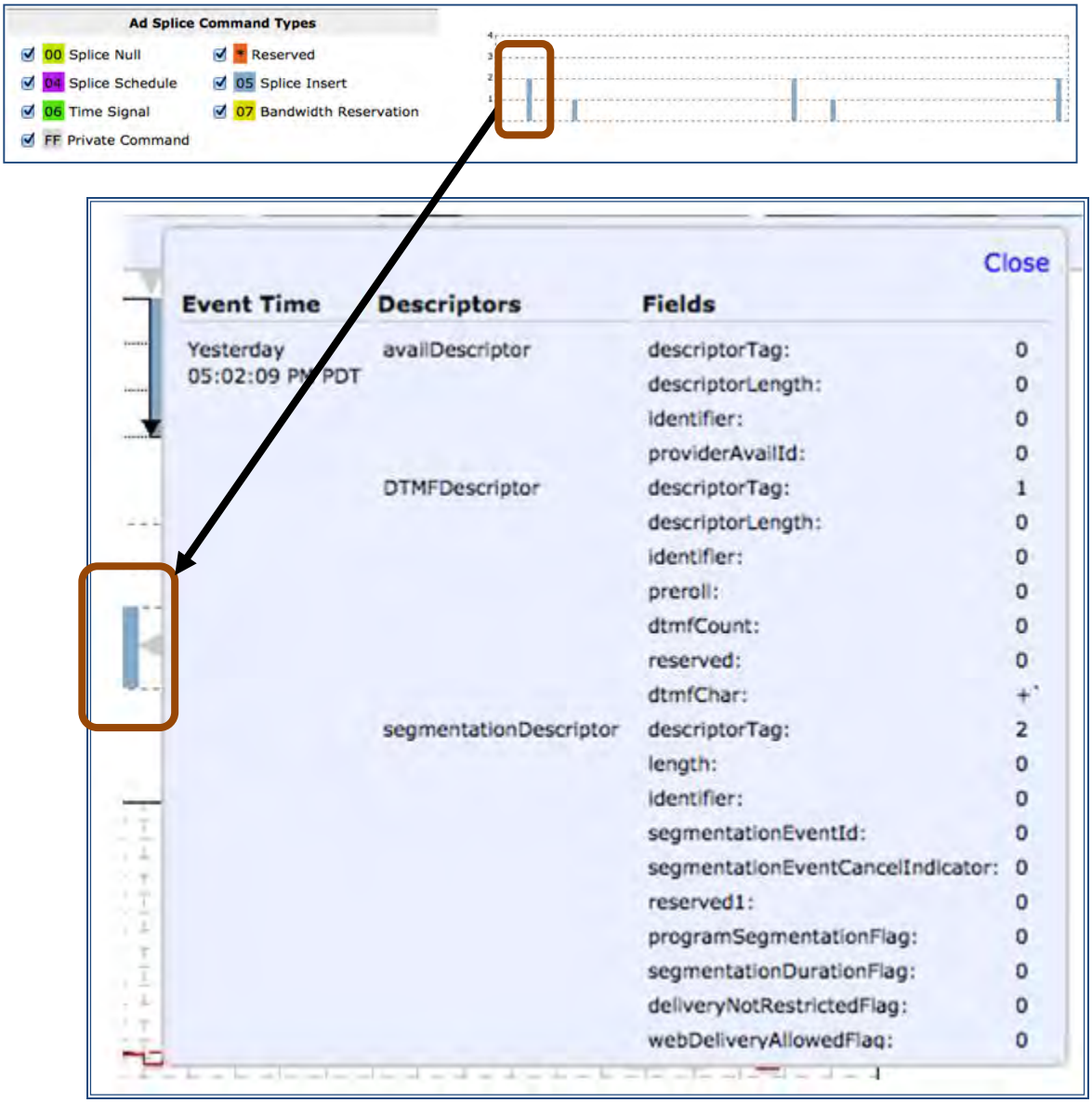



**Figure 173: Hover over bar on graph for Descriptor Information**

The resulting pop up is the **Descriptor** information for that command.

If there is more than one command of a given type shown by the bar, the descriptors for the first two commands will be displayed.

## Drill down/Zoom In

To drill down on the graph, select the desired portion of the graph with your mouse by right clicking and dragging left to right. This will enable you to see the **Descriptor** information for any command.

You can also select which command types you would like to show on the graph by clicking the checkboxes on the legend.

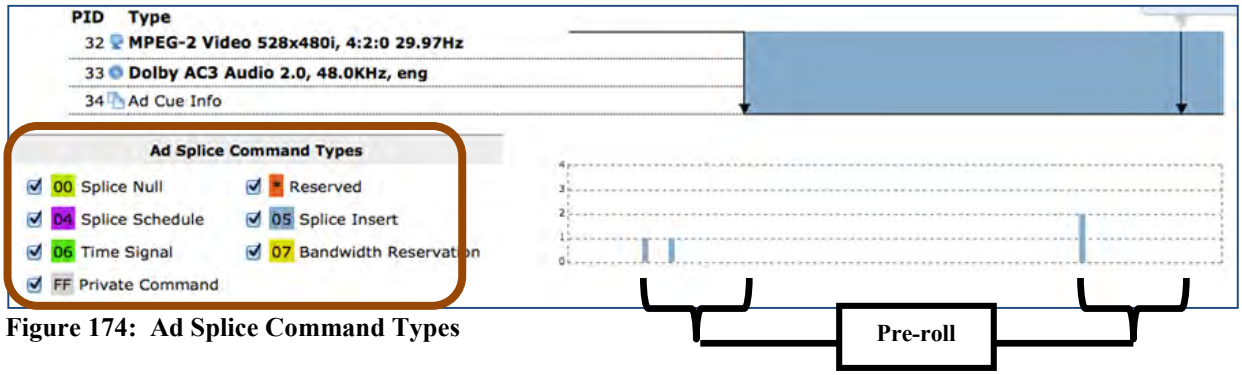



**Figure 174: Ad Splice Command Types**

The number of commands by type runs up and down on the graph and the number of days scrolls left to right.

If the blue bar represents more than two commands, the **Descriptor** for ONLY the first 2 commands will be shown.

To see the **Descriptors** for the rest of the commands, you will need to zoom in on the graph.

The **Ad Splice Command Types** graph shows all commands as they were detected. For splice insert commands, this will generally be before the associated splice insert event (as indicated by the pre-roll time).

Viewing the two graphs together allows a visual display of the pre-roll time, in addition to commands that were subsequently overwritten by other commands.

## Blackout Detection

If an **Ad Splice** command contains one or more blackout periods, a horizontal black bar will be displayed at the bottom of the graph for each blackout period.

You can see details of the command containing the blackout information by reviewing the command descriptors for the command at the start of the blackout period.

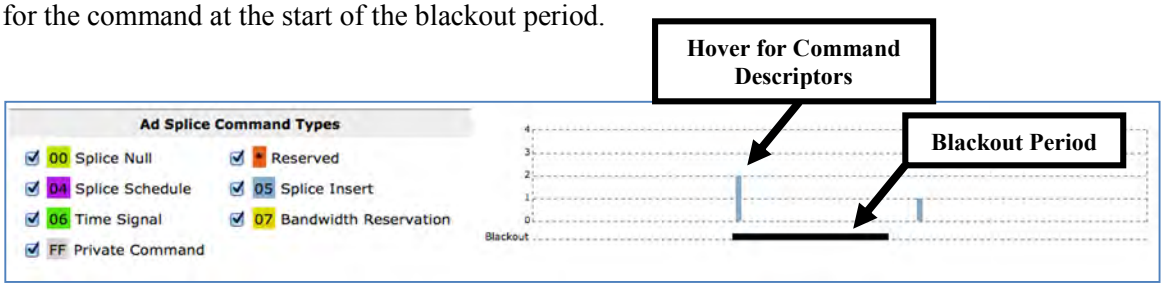



**Figure 175: Blackout period and Command Descriptors**

## Repeated commands

There are times during normal operation when the same **Ad splice** command is repeated over and over (as frequently as every second). Rather than cluttering the graph and overloading the system with each such occurrence, you will see a red * (asterisk) underneath a bar on the **Ad Splice Command Types** graph.

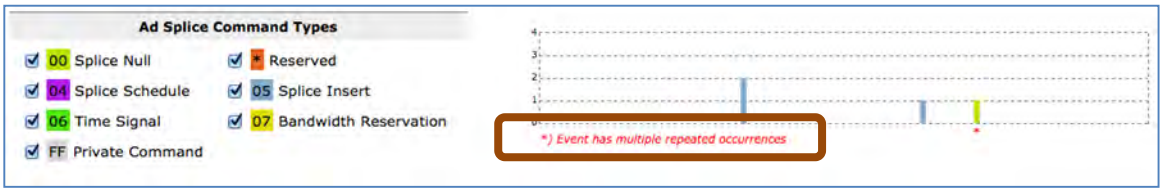



**Figure 176: Asterisk showing there are multiple occurrences of the same command**

Hover over the vertical bar to review the descriptor information for that command. You will see the count of commands that Sentry is grouping into that single bar.

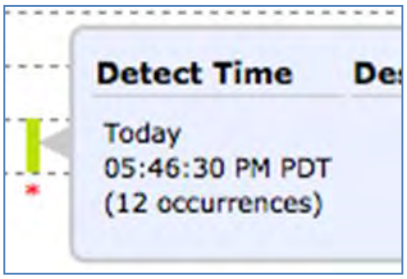



**Figure 177: Descriptor information showing 12 occurrences of a command.**

For repeated commands, the event count will also be displayed on the detailed table at the bottom of the report.


**Figure 178: Multiple commands as shown in the report**

## Audio Level Graph

The **Audio Level** graph can be used to see how the audio level changed during ad cue insertion.

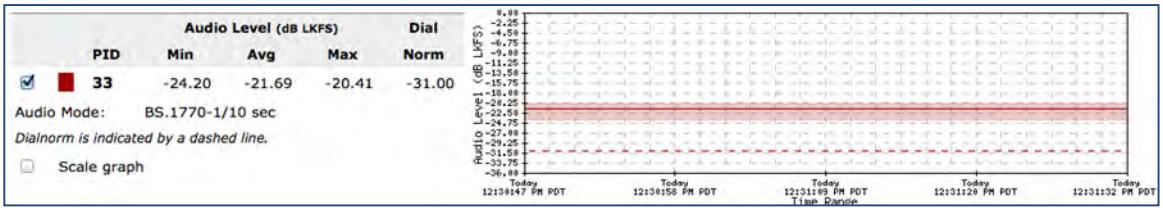



**Figure 179: Audio Level Graph**

# Bandwidth

**Bandwidth** is available through both the **Reports** drop-down menu and the **Program Details** screen. On this page, users may monitor specific details for a selected program and can create a detailed graph in order to view the following areas:

- **Bandwidth Details**
  Shows the bitrates over a period of time for the selected service
- **Discontinuity Details**
  Shows the discontinuities for the selected service as well as PID counts
- **Alert Details**
  Shows the results of any previously set alerts

## Program Details screen

### *Access Program Details*

There are many ways to access **Program Details**. The easiest method is to choose a program icon/program name from virtually any report.

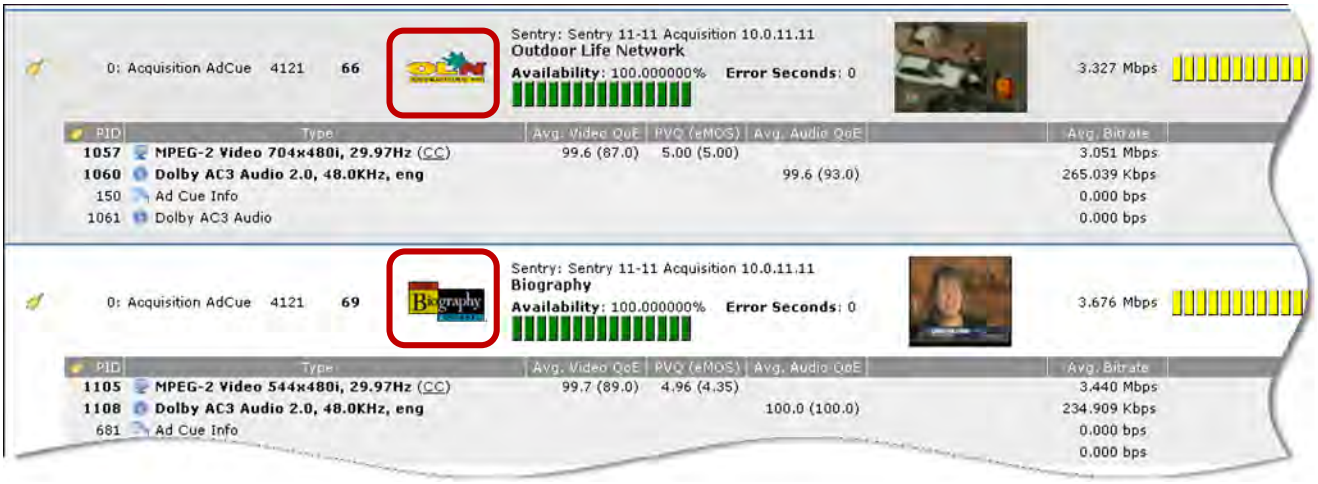



**Figure 180: Accessing Program Details**

From the **Program Details** screen, the user may view many of the details that:

- Assist in assessing the health of the selected program
- Assist in basic troubleshooting.

The **Program Details** screen starts with information about the **Port** and **PID** at the top and allows for viewing details for **Bandwidth**, **Discontinuity** and **Alerts** at the bottom of the page.

Starting at the **Date/Time** selection field, select the time frame you wish to view.

From this point, the user may view the information regarding discontinuities on the port.

**NOTE***: The History graph is color coded using the Color Code Key in the upper right hand section of the screen.*

In the example below, the yellow graph indicates that the PID has been out for some time.

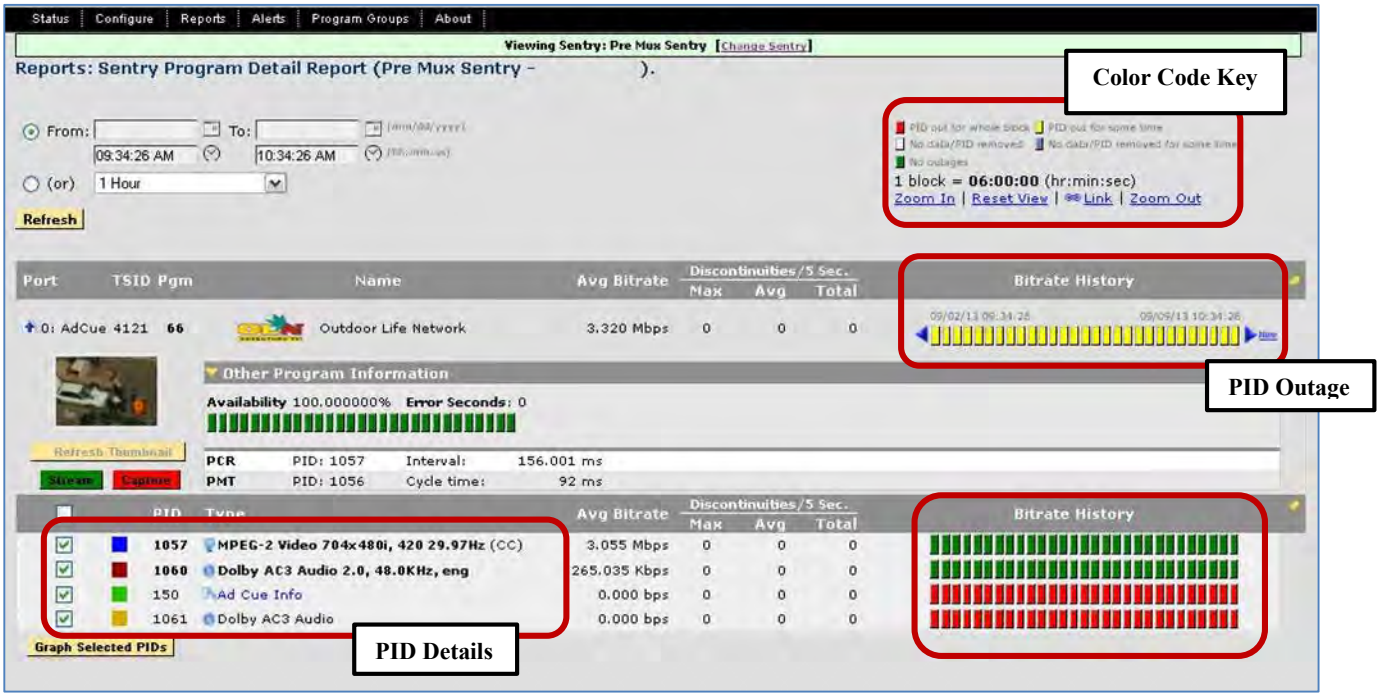



**Figure 181: Program Details screen**

### Refresh Thumbnail

Manually refreshes current thumbnail.

### Capture button

Captures stream. Collects same information as **Triggered By User** button. (See **Configure Stream Captures** in the Sentry manual).

### Stream button

The **Stream** button opens a separate dialog box that allows you to configure where to send the UDP unicast. The network path has to allow UDP unicasts from the Sentry and the receiving computer/device. You may also have to open the specified port in your computer's firewall.

***Please see the Sentry Manual for more information on Stream to View.***

### PID Types

The **PID Type** descriptor displays the following (if available):

- **Video:**
  - Video resolution
  - Refresh rate
- **Audio**
  - Audio Mode (1.0 = mono . 2.0= stereo,, 5.1 = surround sound)
  - Sample rate
  - Language descriptor
    - The Sentry will display the language descriptor exactly as described in the stream.

In the next table, the user can see the specifics of each PID on the given program. In the example, the MPEG 2 video and one channel of the Dolby AC3 audio were in present (**Green**) while the **Ad Cue** info and second Dolby channel where out for the whole time period specified (**Red**).

To view a graph for the bitrate over a given amount of time for the **PID**, select the **Graph Selected** PIDs button located below the PID information.

**NOTE***: Any PID that is in bold is the primary PID.*

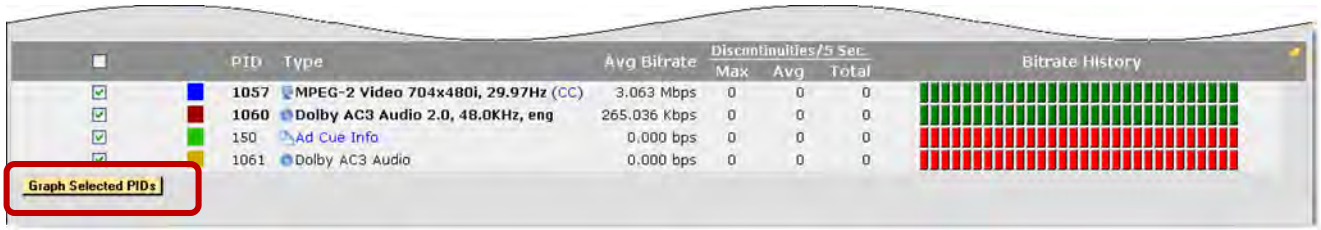



**Figure 182: Graph Selected PIDs**

The resulting graphs will look similar to the ones below.

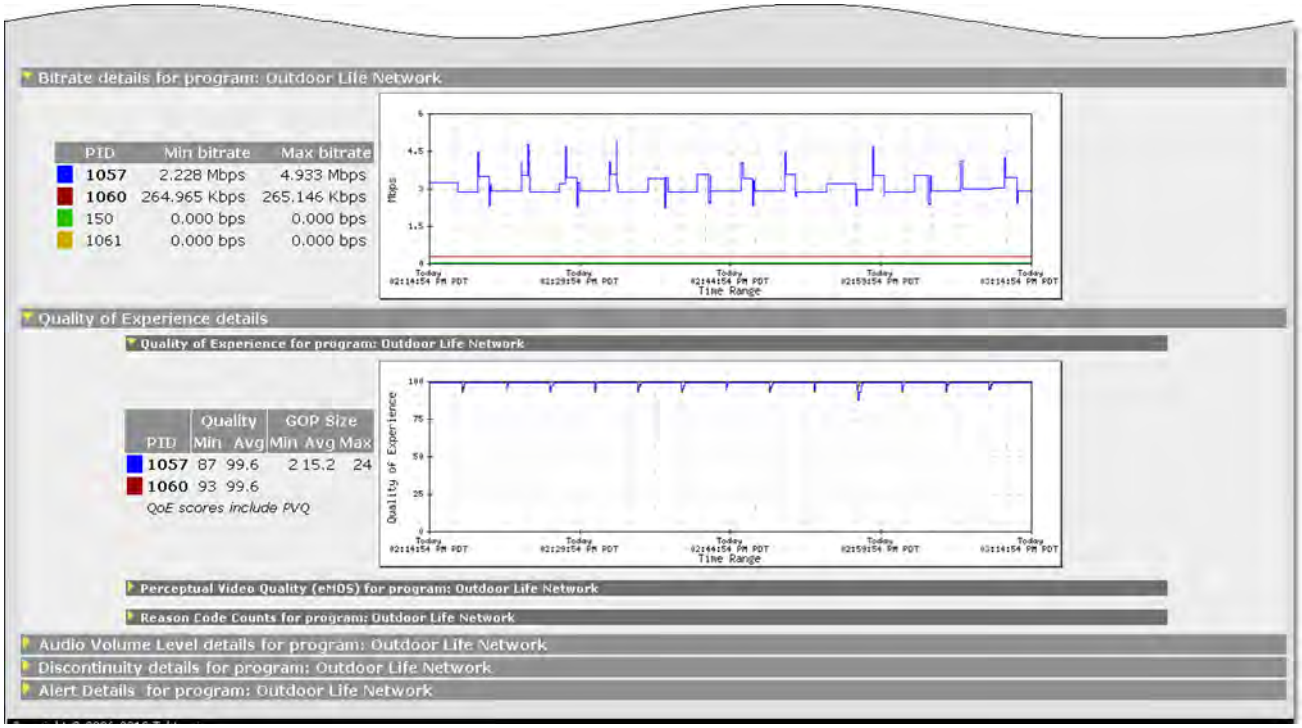



**Figure 183: Bitrate Graph**

## Detailed Graph View

To see more detail on the graph, click on the graph itself and draw a box around the area you wish to view.

The graph will reload and display a more detailed view of selected time frame. In the example below, a **Time Range** between 8:58 AM and 8:59 AM was selected and the resulting graph went from a span of activity covering a 15 minute span to a graph showing activity for every 10 seconds.

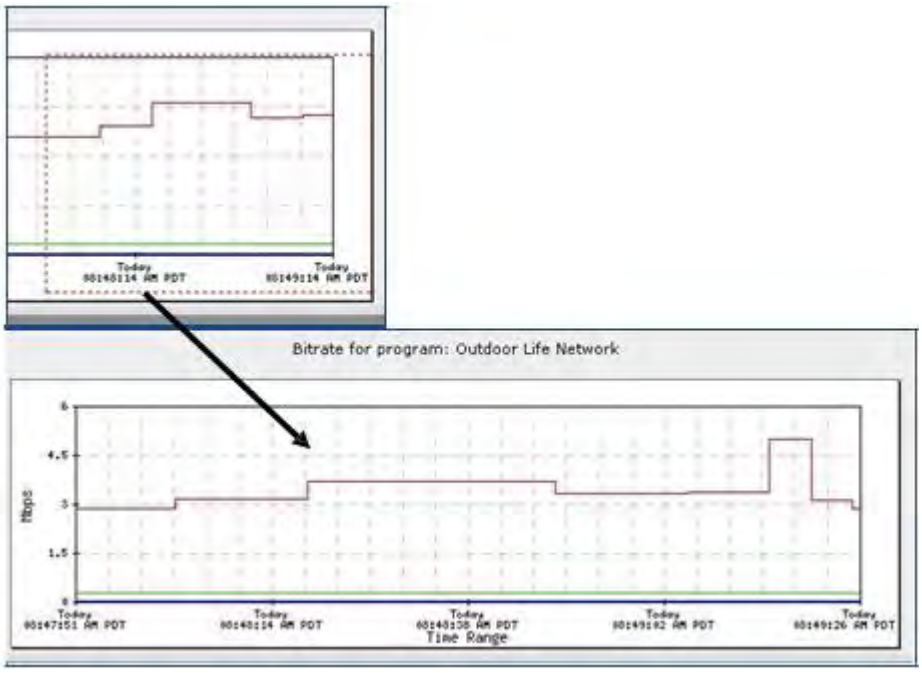



**Figure 184: Selecting a section for a detailed view**

To return to the original graph, select **Reset View** from the top right of the screen.

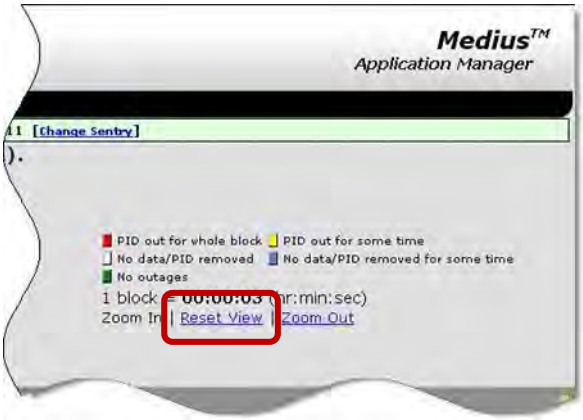



**Figure 185: Reset the graph to its original view**

# Other Program information

## *Program Availability*

**Program Availability** is the number of non-error seconds over total number of seconds for a specified time period. It is expressed as a percentage.

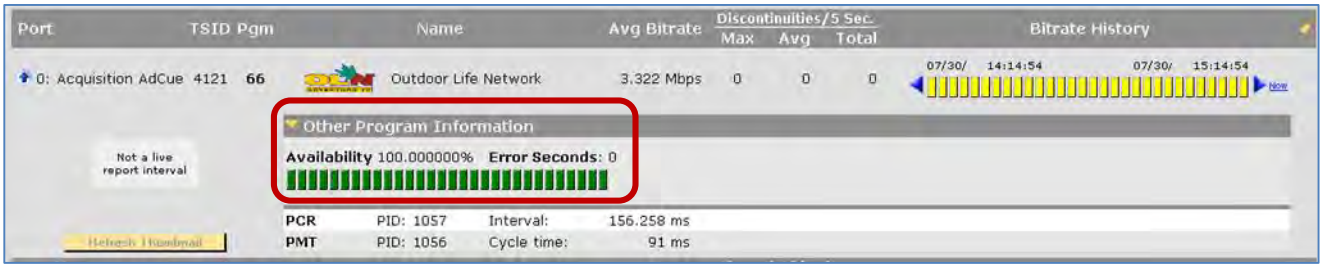



**Figure 186: Program Availability**

To configure **Program Availability** definitions, please see the **Configuring Program Availability Definitions** section of this manual.

## Error Seconds

**Error Seconds** is a user customizable set of parameters used to define when a given program is available or not.

Once set, whenever these parameters are exceeded a clock is started for that program and that amount of time is represented as **Error Seconds**. It is calculated and displayed as an **Availability** percentage.

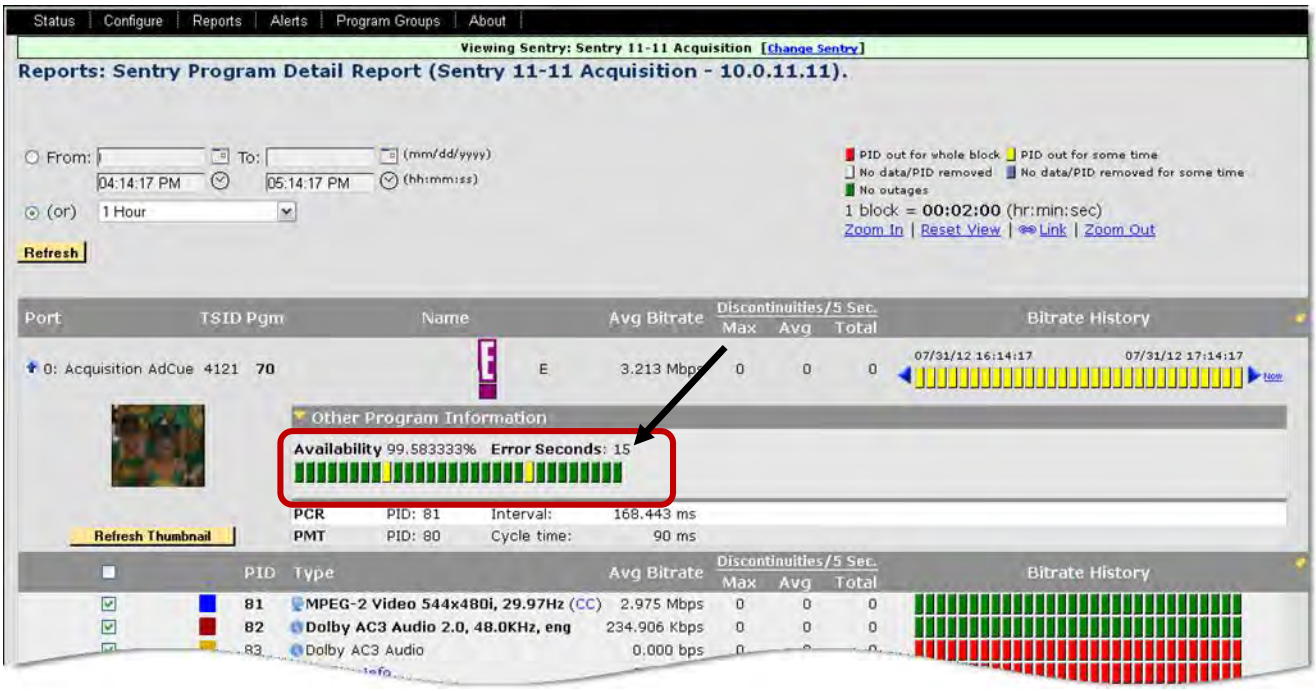



**Figure 187: Error Seconds from the Program Detail screen**

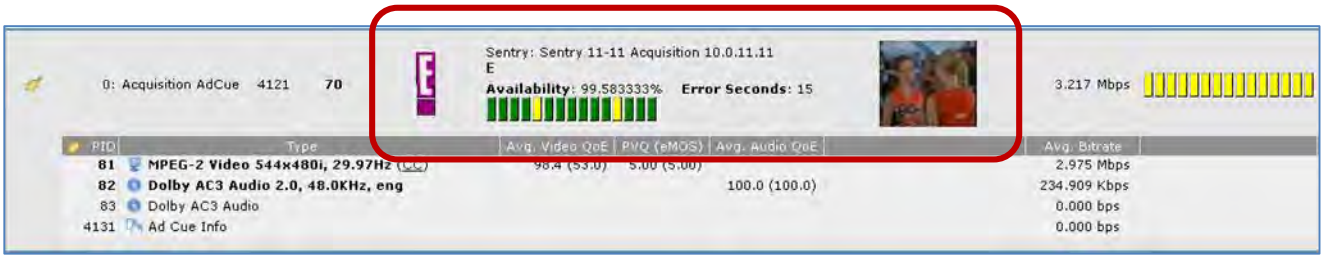



**Figure 188: Error Seconds in all other locations**

To configure **Program Availability** definitions, please see section the **Configuring Program Availability Definitions** of this manual.

## Quality of Experience Details

The **Quality of Experience (QoE)** details allows the user the unique option to assess a smart approximation of the frustration level of an average viewer. This approximation pretends that an average viewer is watching a certain channel while holding a dial that indicates how much she likes or dislikes the quality of the picture he is watching (with 100 being the best score and 0 being the worst). When the quality of the picture is good, she will leave the dial alone at the 100 setting.

However, should an event such as tiling, freezing, macro-blocking, etc, affect the quality of her viewing experience, she will turn down the dial. The fictional viewer will keep the dial turned down for a short time past when the picture recovers until her confidence starts to recover. As her confidence returns, she will slowly return the dial to the top setting.

The **QoE** score is decided by:

- Analyzing where on the screen the picture degraded
- How large of a problem it is for the picture
- How frequently problem occurs

The event is noted, analyzed and reported on the **Quality of Experience Details** screen.

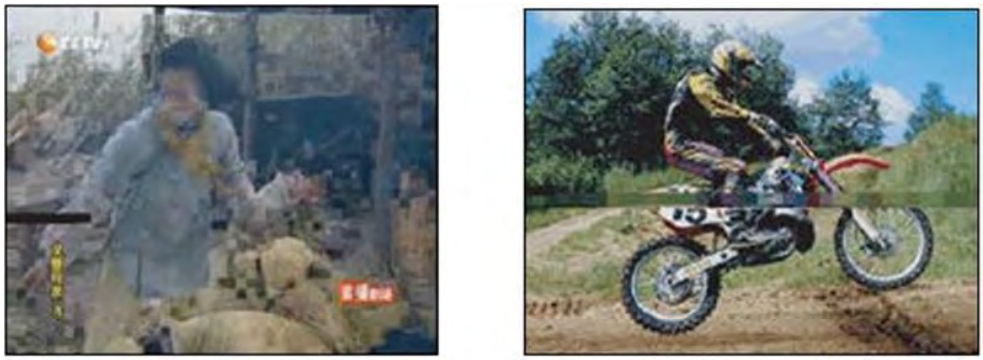


**Figure 189: Examples of Major tiling/long duration . . . and Minor Tiling/short duration**

### Access the QoE Details

1. Select the logo/name of the desired program from any Medius or Sentry page.
2. This will take you directly to the **Program Details** screen.
3. Expand the **Quality of Experience Details** region by clicking on the appropriate arrow.

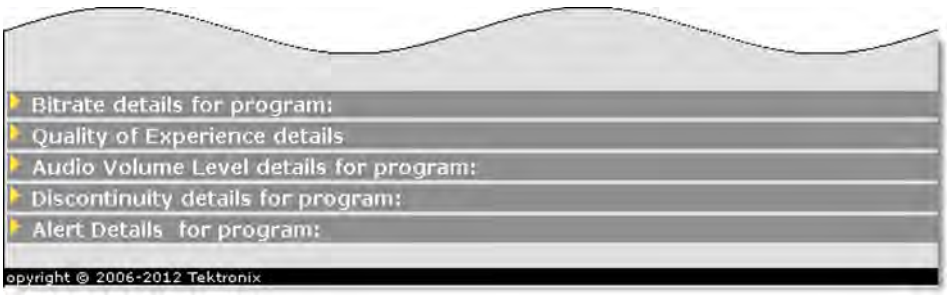



**Figure 190: Expanding the QoE region**

The graph is shown in real-time, though it does not represent regular intervals.

**NOTE***: Colors that appear at the beginning of a graph will remain that particular color throughout. For example a video PID that has a blue label on detail section will also appear as blue in the subsequent detailed graphs. A red labeled PID would stay red.*


**Figure 191: Expanded Quality of Details Region Graphing a blue coded 272 PID**

### *Average Video QoE from the Program Status Page*

The **Average QoE** score may also viewed from the **Program Status** page. The score in the parenthesis is the minimum for the time frame specified.

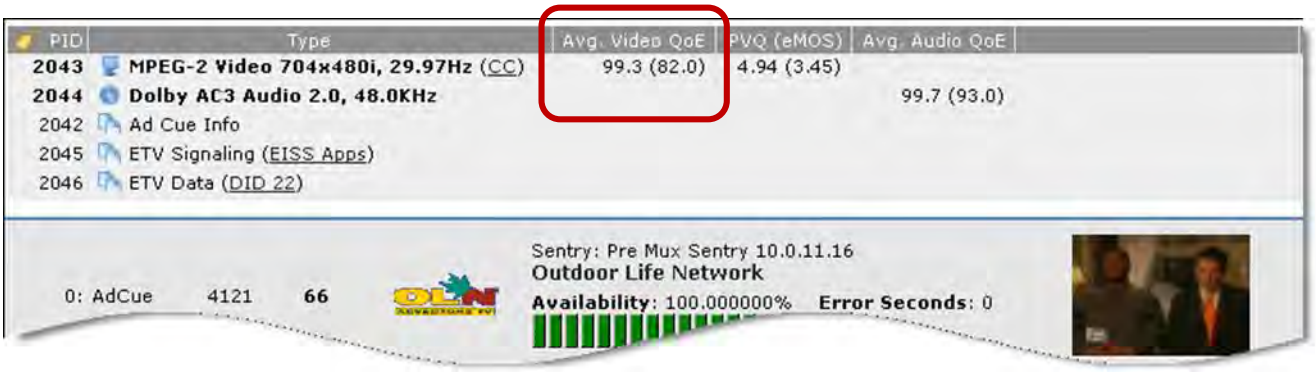



**Figure 192: Average Video QoE column**

## Scoring QoE

The **Minimum** and **Average Quality Numbers** indicate a particular time frame the user is observing.

The **Average Video** and **Audio QoE** scores can also be found on the **Program Status** report.

In this example, the graph shows three incidences of a **Quality of Experience** drop.

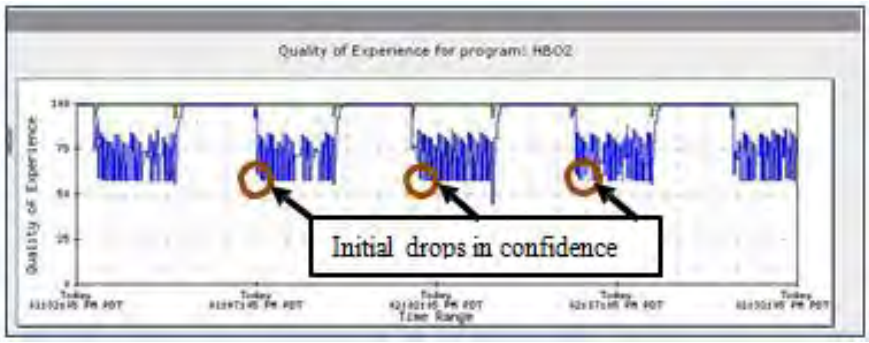



**Figure 193: Quality of Experience Graph showing the initial drops in confidence**

In this example, you can see the initial drop in the video QoE score followed by a flat spot. The flat spot represents the lowered confidence that the customer is experiencing due to the initial drop. These flat sections are not necessarily a continuing issue but rather represent a confidence drop for the average viewer.

Once the initial impacting event has cleared and the customer's confidence is restored, the QoE score will slowly increase.

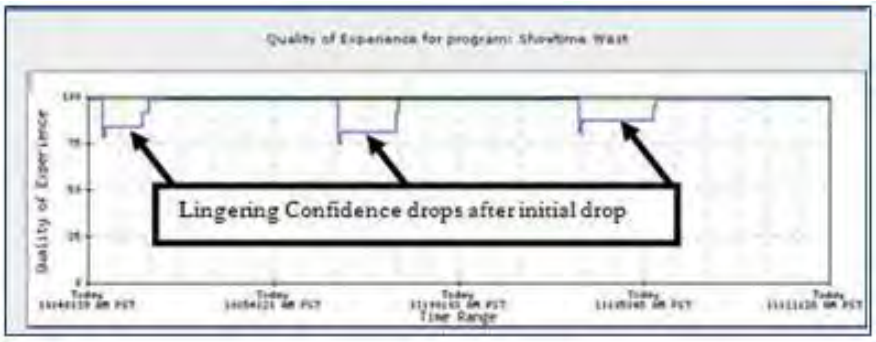



**Figure 194: Lingering confidence drops, not necessarily a continuing issue**

In addition to displaying the QOE scores, Medius also reports the reason(s) why the QOE scores went down. The QoE reason codes are shown directly below the QoE graph and correspond to the beginning of the QoE drop.

For example, if the QoE score is 0 for a period of 1 minute and the reason code is **Video Syntax Error,** the reason code is shown as a bar at the beginning of the 1 minute period.


**Figure 195: Examples of QoE drops and their corresponding Reason Codes**

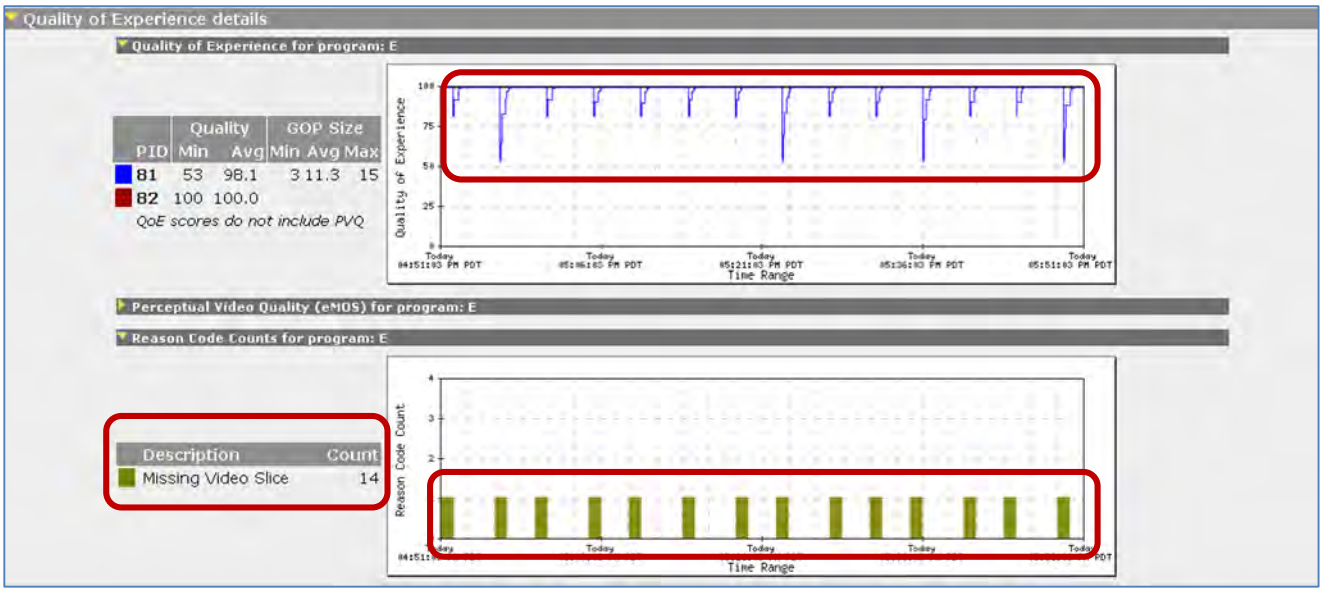



**Figure 196: Reason Codes and QoE drops**

## Perceptual Video Quality (eMOS)

Sentry offers PVQ (or effective eMOS) and Video QoE as two separate alerting and reporting systems. This gives you the ability to evaluate compression artifacts separately from video errors. In this case, independent to the configuration to include or to exclude eMOS contribution in video QoE, the user can always evaluate eMOS as a distinct metric and as one of the key performance and quality indicators.


**Figure 197: Reason Codes and PVQ drops**

The shaded area of the PVQ graph indicates the minimum and maximum score over time. The solid line indicates the average over time.

There are two primary uses for video quality monitoring:

- **Real time alerting:**
  Combined video QoE + eMOS to generate real time alerts when the score drops to a certain level for a period of time (e.g., below 75 for more than 10 seconds) or for a certain number of times in a duration (Example.: below 75 for 5 times in one minute), so operators can fix the problem before a large number of viewers are impacted.

- **Generate comprehensive KPI reports for uptime and quality levels over time**
  - **Program Statistics** (non-alert based) report for quantitative analysis.
  - **Alert Analysis** (user sets alerts) for qualitative analysis.

## Over-compression Artifacts

Unlike macro-blocking, which is caused by errors, over-compression artifacts can take place when the video has no errors in the payload and the picture can be structured correctly for the screen. However, the picture quality seems degraded to the viewers.

This often takes place in clips involving high motion and complex scenes when there are not enough bits available in the compressed video to clearly present necessary details needed to deliver a high quality picture.

Medius can accurately report on these non-error-related video artifacts detected by Sentry and score them as PVQ (or eMOS), which ranks video quality in a similar way as a Mean Opinion Score (MOS). eMOS can be used (in the case when there are no technical errors in the transport stream) to measure perceptual video quality in the compressed stream.

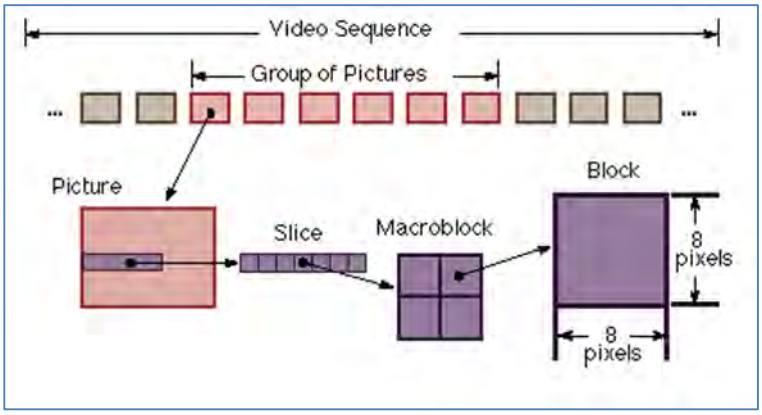



**Figure 198: GOP, Picture, Slice, and Macroblock**


**Figure 199: The picture on the left shows compression artifacts in the background (general fuzziness) and the picture on the right shows one clear of compression artifacts.**

## Reason Codes List

| Reason Code | Definition |
|---|---|
| **Audio Buffer Overrun** | Buffer timing violation causing buffer overrun and is greater than or equal to 100ms. |
| **Audio Buffer Underrun** | Buffer timing violation causing buffer underrun is equal to 0 seconds, meaning that the buffer is empty. |
| **Audio Packet Loss** | When there are CC errors or incomplete audio frames are received, but the dropout is small (less than 200 msec) |
| **Audio PID Dropout** | When there is a dropout (may or may not be accompanied by a CC error) and dropout duration greater than 200 msec. |
| **Audio Syntax Error** | When there are no CC errors but there is an error in audio frame decode. |
| **eMOS(PVQ)** | Generates an alert when the PVQ goes above or below a user set threshold. This is not coupled with any particular QOE event or alert. |
| **Missing Video Slice** | Slice start code missing. |
| **Port dropout** | When there is a transport dropout of at least 5 seconds. |
| **Unexpected Video Header** | The video header was an unexpected value. |
| **Video Packet Loss** | There are CC errors but the dropout is small (i.e., duration of dropout is less than 200 msec.) |
| **Video PID Dropout** | When there is a dropout (may or may not be accompanied by a CC error) and the dropout duration is longer than greater than 200 msec.<br>A CC error is not the only indication of a dropout. There can also be start code errors in video or incomplete audio frames due to dropout. If the duration of dropout is long, it qualifies for the PID dropout reason code. |

**NOTE***: A CC error will never generate a reason code of Syntax Error because cc errors clearly indicate data loss. It will generate either Packet Loss or PID dropout reason codes.*

## VQoE H.264 support

H.264 is a standard for video compression and a version of MPEG 4. H.264 is used in such applications as direct-broadcast satellite television services, cable television services, and real-time videoconferencing.

## GOP Length Reporting (Group of Pictures)

The **GOP Size** table displays the **Average**, **Maximum**, and **Minimum** GOP size for the specified time period.

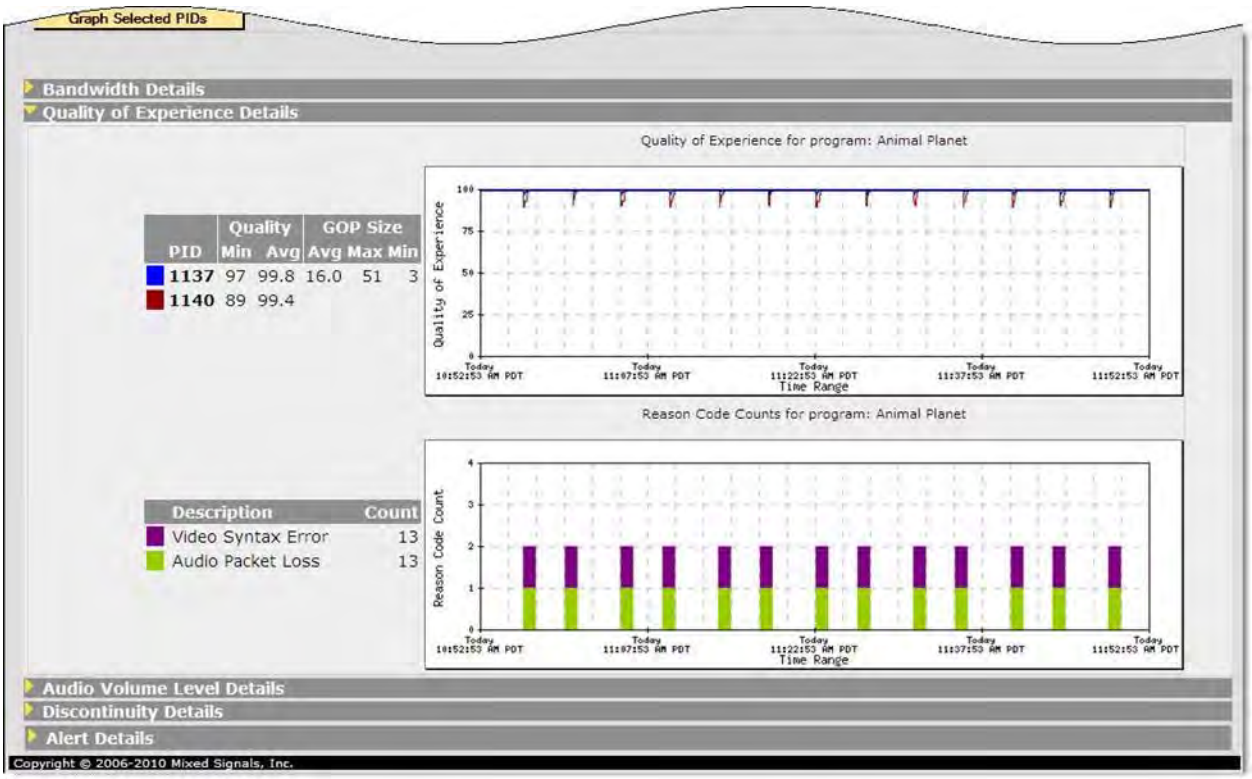



**Figure 200: GOP Length Reporting**

## Audio Volume Level Details

**Audio Volume Level Details** allows you to track problems within the actual audio stream, or audio PID. This monitoring and report feature allows the user to address the common problem that exists with varying volume levels on different channels (evident when the viewer changes channels) or during commercial inserts. Medius and Sentry will monitor and report this problem so it can be adjusted by the operator.

This function differs from Medius/Sentry's **Audio Quality of Experience** in that each one measures different qualities.

### *Functionality*

Sentry decodes and analyzes the audio stream in order to determine the true energy level so it can detect issues such as low perceived level. Sentry also reads the **Dialnorm** that has been encoded in the metadata. The resulting graph is a good representation of how the human ear will perceive the audio with respect to where the **Dialnorm** is set to.

**NOTE:** ***The value of the Dialnorm in a bit stream should indicate the level of the average spoken conversation within the encoded audio program.***

### *Access Audio Level Details*

1. Select the logo/name of the desired program from any Medius /Sentry page.
2. This will take you directly to the **Program Details** screen.
3. Expand the **Audio Volume Level Details** region by clicking on the appropriate arrow.

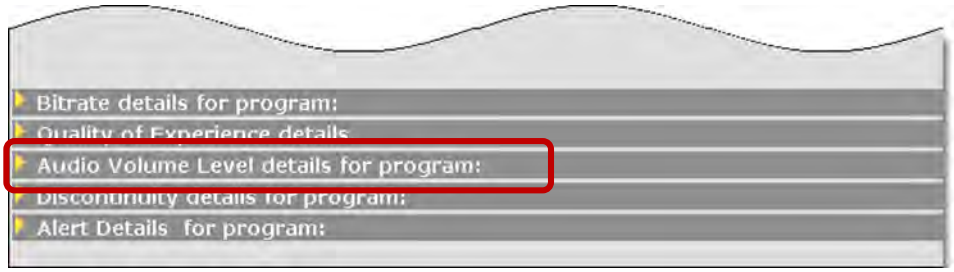



**Figure 201: Expanding the Audio Volume Level Details region**

## Graphing

A graph of the primary PID will be generated by default, although either PID can be selected for graphing.

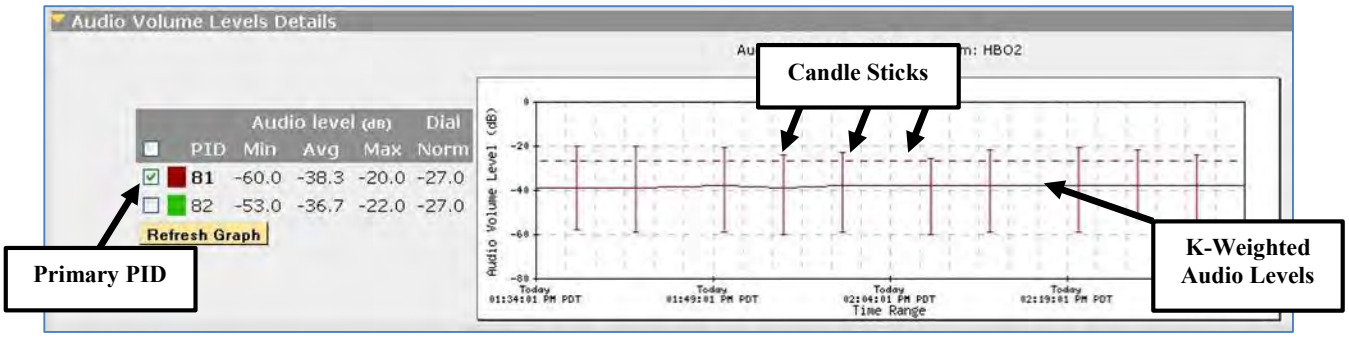



**Figure 202: Audio Levels**

- **Dashed line**
  Represents the **Dialnorm** level that is specified in this audio stream.
- **Solid line**
  Represents the K-weighted audio level.
- **Candlesticks**
  While the audio is measured on a continuous basis, the minimum and maximum points are not continuously displayed. This makes the graph clearer and easier to read. The candlesticks are not markers of time, but rather markers of the minimum and maximum audio levels for a particular section.

In the example below, the average audio level is much lower than the specified **Dialnorm** for this stream. To the audience, the audio would be perceived to be quieter than it should be.

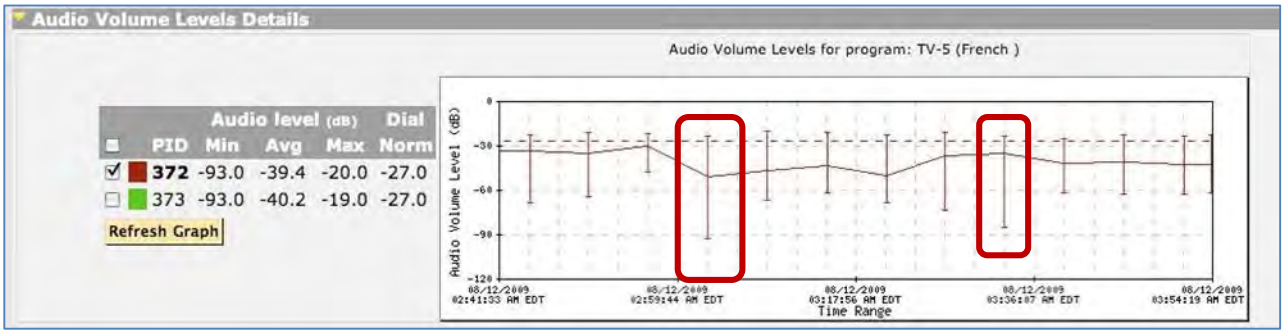



**Figure 203: Audio Levels with poor volume**

## Thumbnail Timeline

**Thumbnail Timeline** captures thumbnail images to help visually confirm the relative location of audio issues (i.e., during programming or commercials). This function supports both MPEG-2 and H.264 thumbnails.

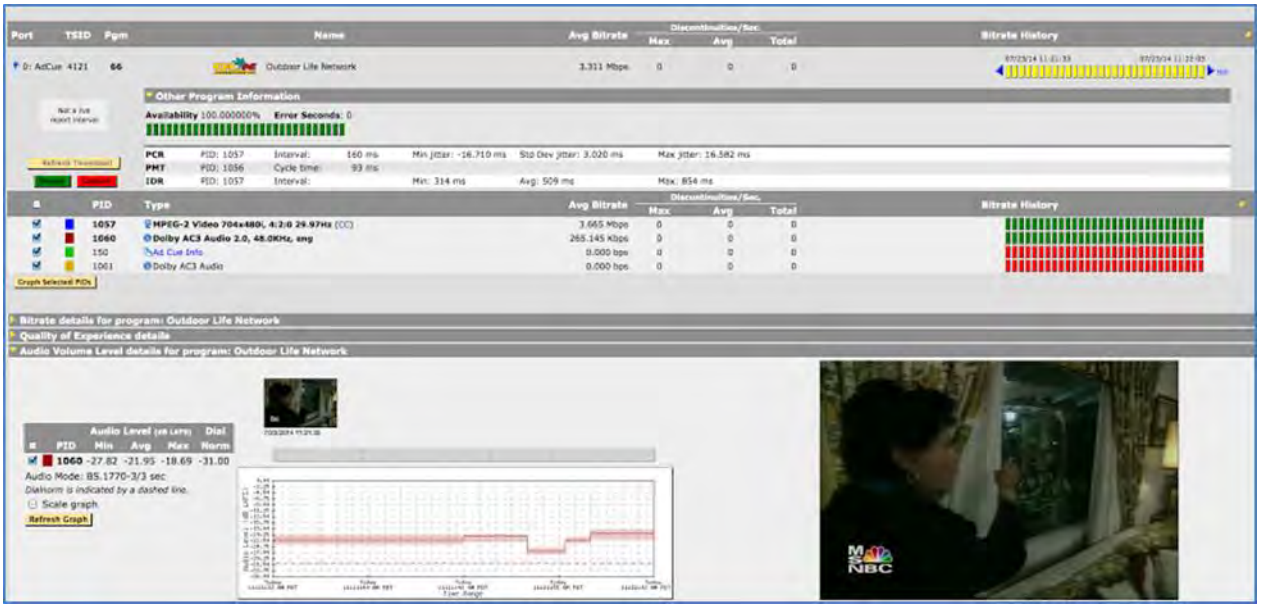



**Figure 204: Thumbnail Timeline**

## Discontinuity Details

**Discontinuity** is defined by a missing or out of sequence MPEG packet. Discontinuities can result in various levels of audio and video problems depending on the number and frequency of occurrence.

The **Discontinuity Detail** graph allows you to view the number of discontinuities over time. You can use this information to troubleshoot or look for large patterns or spikes of discontinuities.

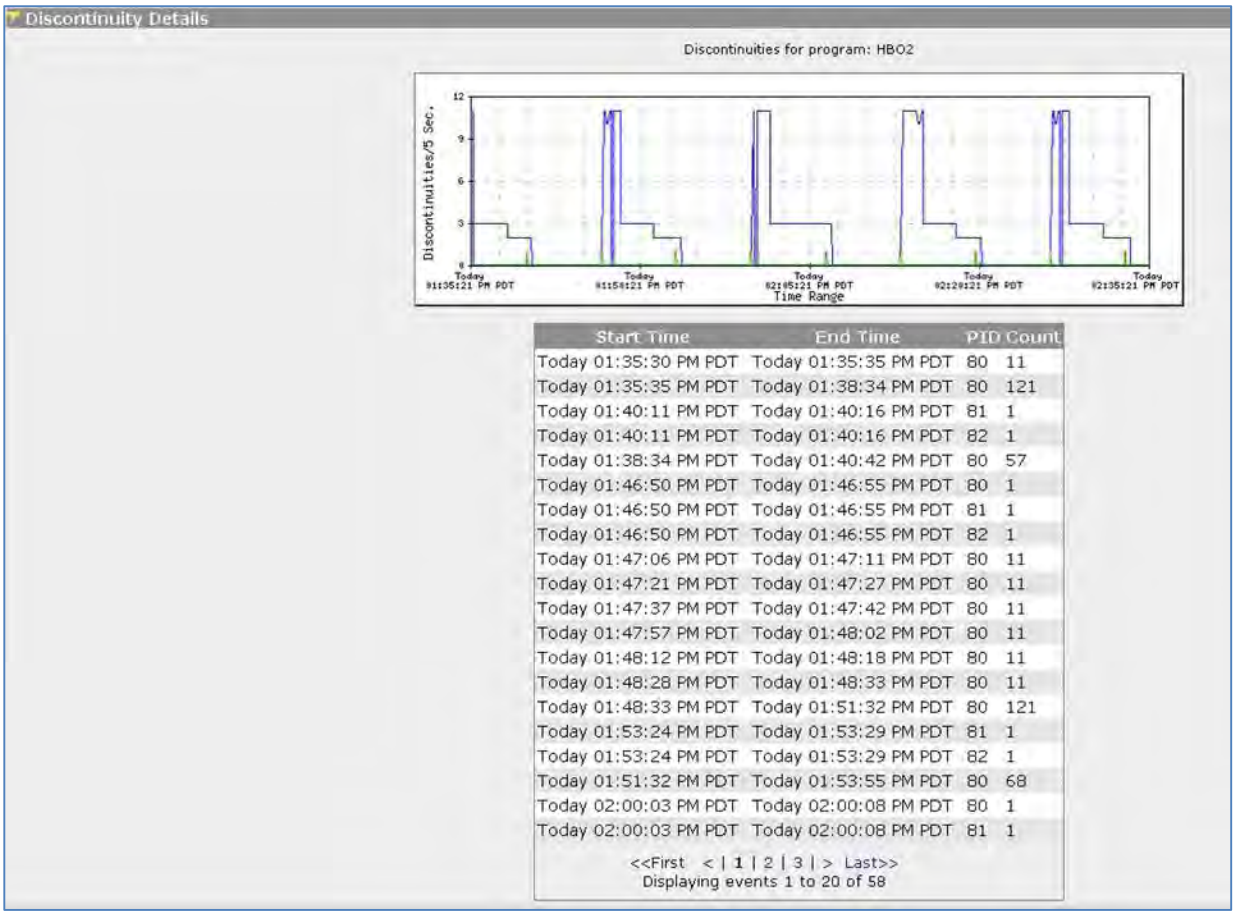



**Figure 205: Discontinuity Graph and table**

## Alert Details

**Alert Details** has two different views that the user may select from the drop-down menu: open alerts and all alerts triggered in a time frame.

**Open alerts** shows the user the current active alerts for this program.

In this example, a "**No alerts have been triggered**" message is returned.

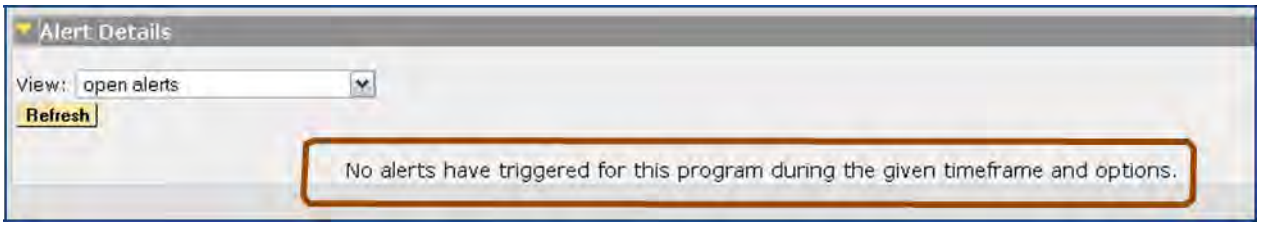



**Figure 206: Alert Details with no triggered alerts**

To see all alerts instead of just the open alerts, select all alerts triggered in time frame from the drop-down menu. This view shows you all of the alerts, either active or cleared, in the time frame specified at the top of the page.

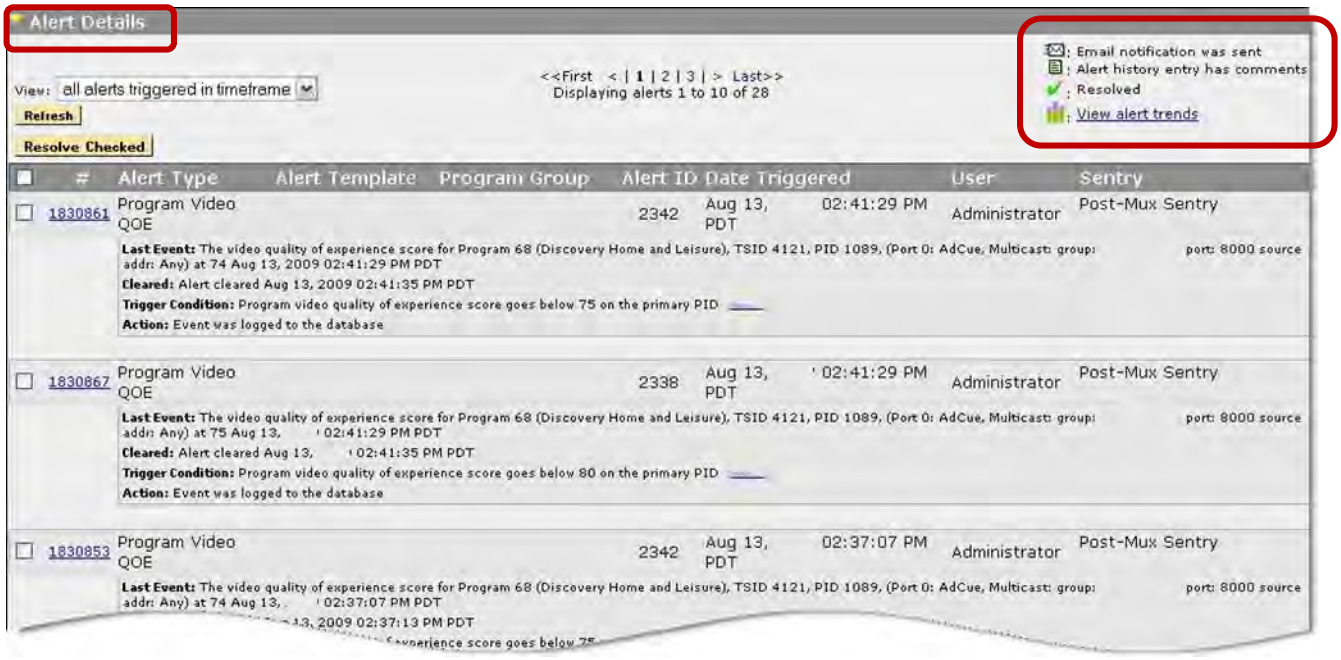



**Figure 207: Alert Details expanded**

## PCR Details

To access detailed information about a program's PCR PID, click on the **PCR** link on the program detail report.

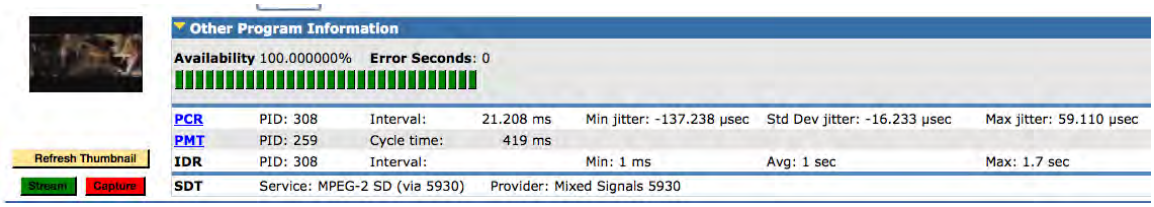



**Figure 208: Program Detail report**

The PCR Details page will show summary values and detailed graph for the following PCR statistics:

- PCR Drift
- PCR Frequency Offset
- PCR Jitter
- PCR Cycletime


**Figure 209: Program Details page**

As with all graphs, you can zoom in on any graph to narrow your time range. Just click on the graph where you want to start, hold the mouse down, drag to where you want to end and release the mouse.

Other helpful operations:

- Click the **Zoom In** link to look at a shorter time window.
- Click the **Reset View** link to return to the report's original timeframe.
- Click the **Link** link to modify the report URL to show the current timeframe that you are viewing. When zooming in on the graph the report URL does not change, so this option is helpful if you want to copy and paste the URL into a message or an email.
- Click the **Zoom Out** link to look at a longer time window.

# Report Types

## Copy Generation Management System (CGMS)

Check one or more of the boxes to see if **CGMS** embedded data is or is not present in the video PID. As defined in **EIA/CEA-608-B, CGMS** provides a mechanism for content creators to inform a consumer electronic device, such as a personal video recorder (**PVR**), advanced set top receiver, etc., as to whether the content may be stored or copied. There are three different modes for this data type.

- **No Restriction**
  Any video stream can be copied to any device. In the case of a VCR connected to the output of a PVR or TiVo device, any stored video files can be copied to a VCR tape.
- **No Copy**
  No video stream can be copied to any device. In the case of a VCR connected to the output of a PVR or TiVo device, no stored video files can be copied to a VCR tape.
- **1 Copy**
  A video stream can be copied to any device only once. In the case of a VCR connected to the output of a PVR or TiVo device, any stored video files can be copied only once to a VCR tape.

## Closed Caption Data

- **608**
  Refers to the specification EIA/CEA-608-B for encoding data into NTSC video on video line 21. This is the traditional location for closed captioning, XDS (e.g., program names, v-chip), and analog interactive television triggers.
- **708**
  Refers to the specification CEA-708 "Digital Television DTV Closed Captioning", also known as ATSC/53 captioning. Most DTV/ (including HDTV) programming that includes closed captioning uses this standard. Many programs that are converted from NTSC to HDTV have both 608 and 708 data embedded simultaneously.
- **SCTE-20**
  Refers to the specification ANSI/SCTE-20 for carriage or embedding of Vertical Blanking Interval (VBI) services into MPEG compliant bit-streams. This method is favored by North American cable operators to encode traditional VBI line-21 (EIA-608) closed captioning into digital cable MPEG bit- streams.

## Other Data

- **Scrambled**
  Indicates the presence of scrambled (i.e., encrypted) MPEG transport packets as described in ISO/IEC 13818-1. There are multiple indicators within a transport stream that instruct down-stream equipment to scramble the stream; however, this indicator reflects whether the transport packets actually are scrambled or not.
- **Discontinuity**
  Indicates a break in the sequence of MPEG transport packets for a particular PID. Dropped packets or a hard splice will generally result in discontinuities being indicated. Dropped packets can sometimes result in poor video or audio quality.

**Teletext**
Refers to a television information retrieval service developed in the United Kingdom. It offers a range of text-based information, typically including national, international and sporting news, weather and TV schedules.

- **Subtitles**
  Refers to closed-captioning data that is transmitted in the teletext signal.

## Program Statistics (Report and Export)

The **Program Statistics** report gives you non-alert based statistical data from your programs. You can use this information to observe trends over time for such items as audio volume levels, bit-rates, QoE scores, etc.

The **Program Statistics** page simplifies access to summary program data by providing a set of navigational tabs:

- **Summary**
  Summary of saved reports.
- **Create/Edit**
  Create and/or edit a report.
- **History**
  Provides a history of the emails for scheduled reports.

## Access Program Statistics

1. Select **Reports** and then **Medius: Program Statistics**.
2. Click on Select Statistics.

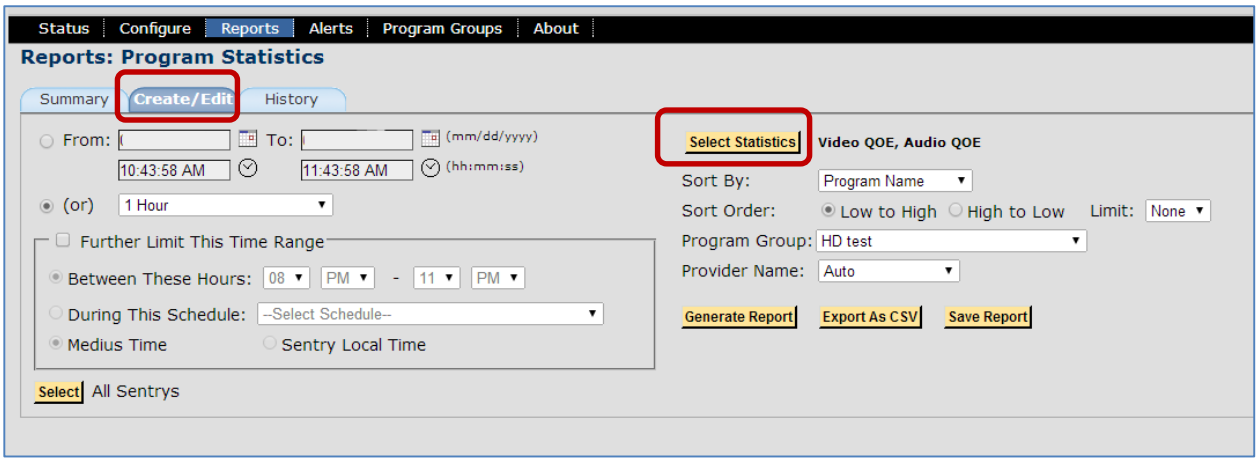



**Figure 210: Select Statistics**

A scrolling window with the following options will appear.

- **Video QOE**
- **Audio QOE**
- **Audio QOE (2nd)**
- **Audio Loudness Level**
- **Audio Loudness (2nd)**
- **Bitrate**
- **Discontinuities**
- **GOP Length**
- **Perceptual Video Quality (eMOS)**
- **Availability**
- **Ad Cue Events**
- **Closed Caption**
- **608 Closed Caption**
- **708 Closed Caption**
- **SCTE Closed Caption**
- **ABR Fragment Size/Duration**
- **ABR Fragment Load Time**
- **ABR Fragment Load Bitrate**
- **ABR Fragment Load Latency**
- **ABR HTTP Status**
- **IDR Frame Interval**
- **EBP Interval**

3. Select the statistics you want included in your report and click on **Accept**.

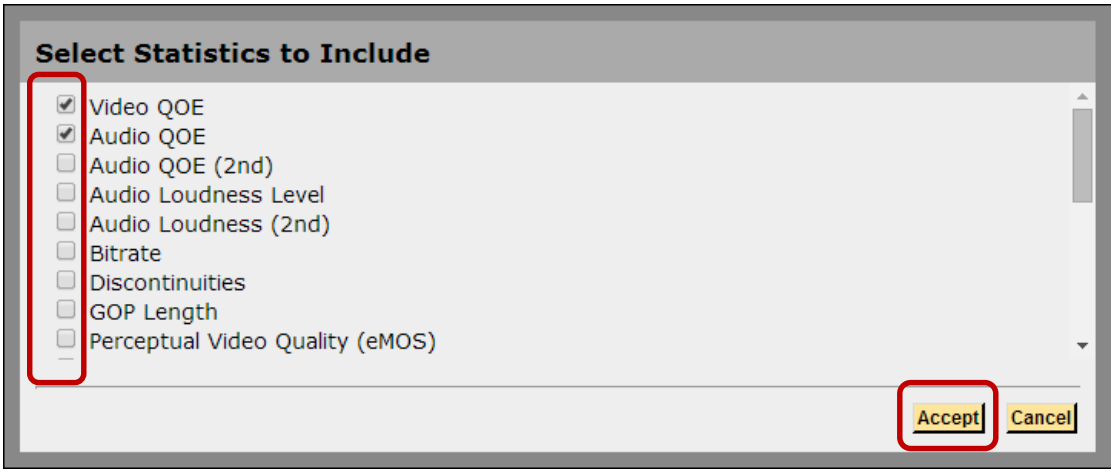



**Figure 211: Statistic options window**

4. The selected options will now appear next to the **Select Statistics** button.

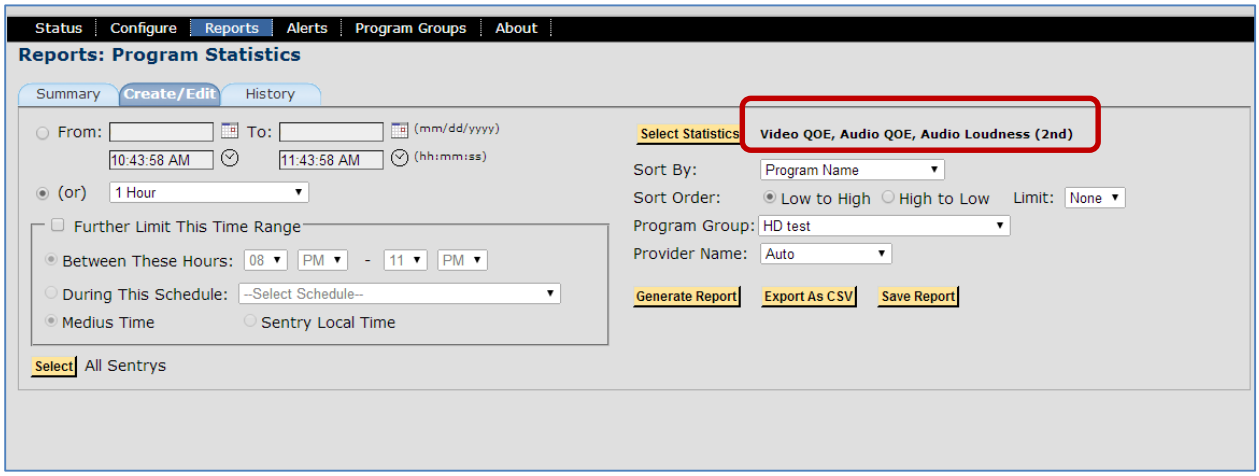



**Figure 212: Selected statistics**

## Summary tab

The **Summary** tab displays which reports you have been created and saved.

- **Private reports** are only viewable from your login.
- **Public reports** are viewable to anyone who can log in.

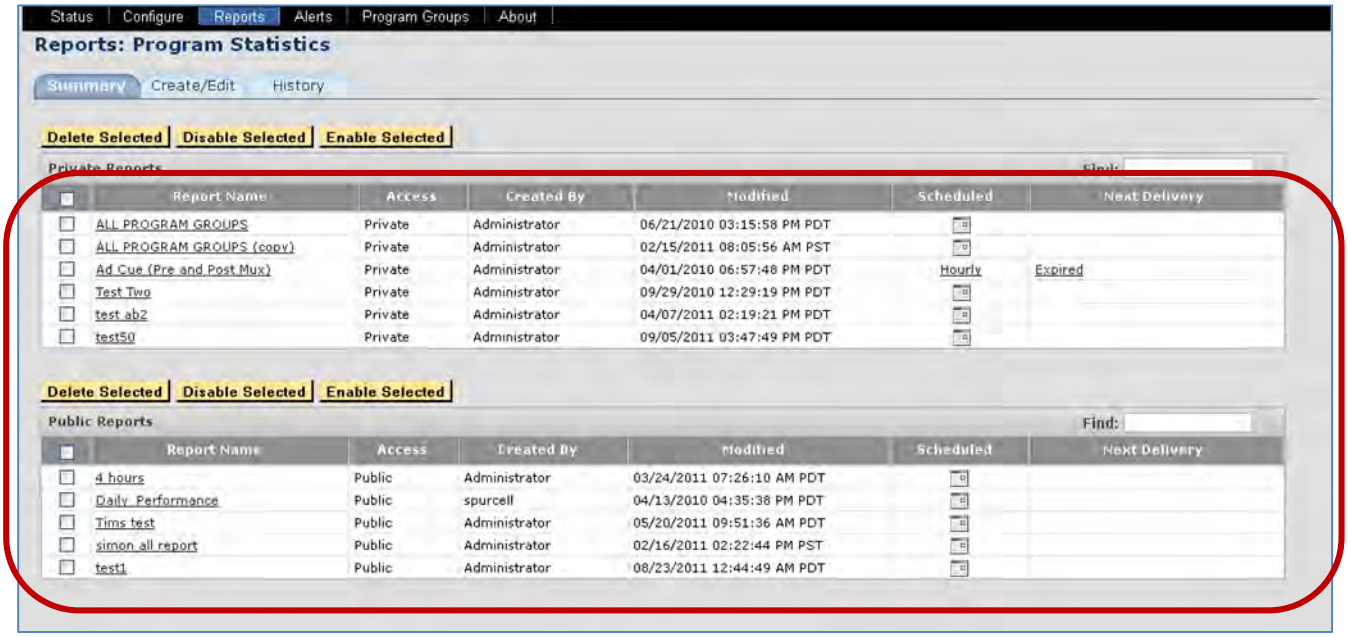



**Figure 213: Program Statistics report**

## Create/Edit tab

The **Create/Edit** tab allows you to generate the following data when creating or editing a report:

- Maximum and minimum and averages of video QOE, audio QOE audio loudness levels, GOP Lengths
- Average for Bitrate program **Availability** percentage and percentage of CC.
- Totals for Ad Cue events and discontinuities
- Maximum and minimum and averages of GOP length
- Maximum and minimum and averages of PVQ

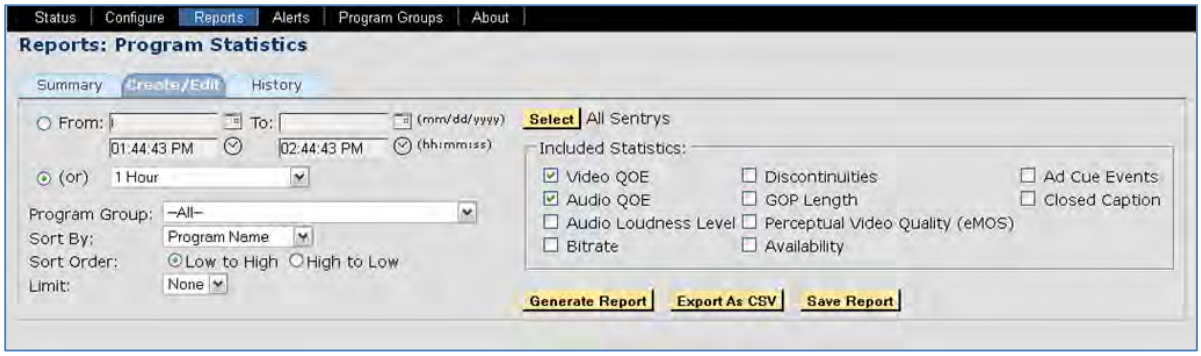



**Figure 214: Program Statistics**

### *Create a Program Statistics Report*

1. Go to **Reports** and then under **Medius Program Group**, select **Program Statistics**.
2. Select the **Create/Edit** tab.
3. Select your time frame.
4. Select the Stats you want to view.
5. Select **Program Group**(s) (optional)
6. Sort and limit as desired.
7. Select Sentrys (optional)
8. Select **Generate Report**.

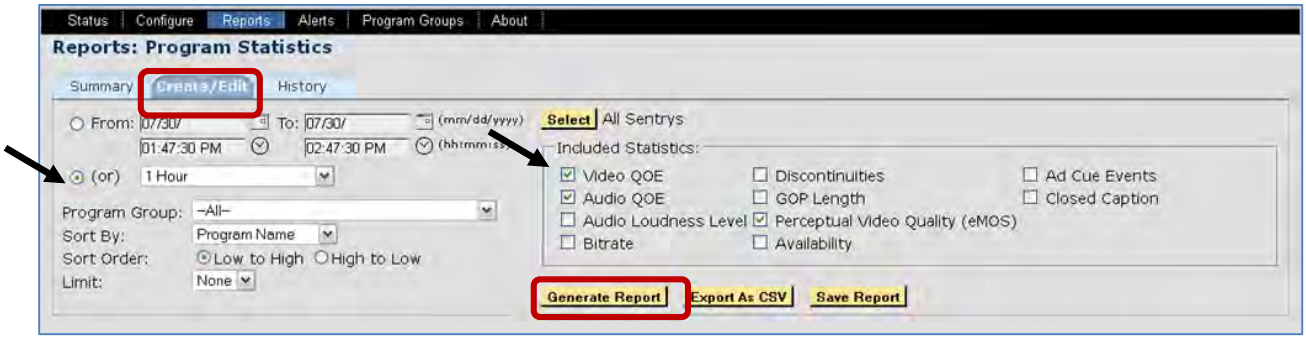



**Figure 215: Creating a Program Statistics Report**

9. The displaying program box appears.

10. Review all data.
    a. Select column header to sort data.

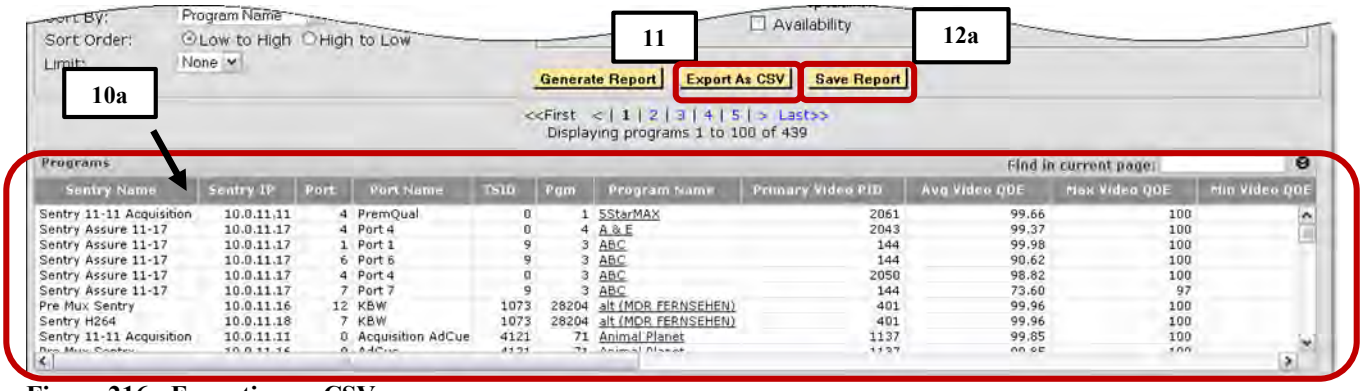



**Figure 216: Exporting as CSV**

11. Selecting the **Export as CSV** button allows user to export visible data as a CSV (Comma Separated Value) file that you can put into a spreadsheet application for further analysis.

12. When you are satisfied with the report output and wish to save it:
    a. Select **Save Report**. The screen will reload to show the save options.
    b. Name your **Report**.

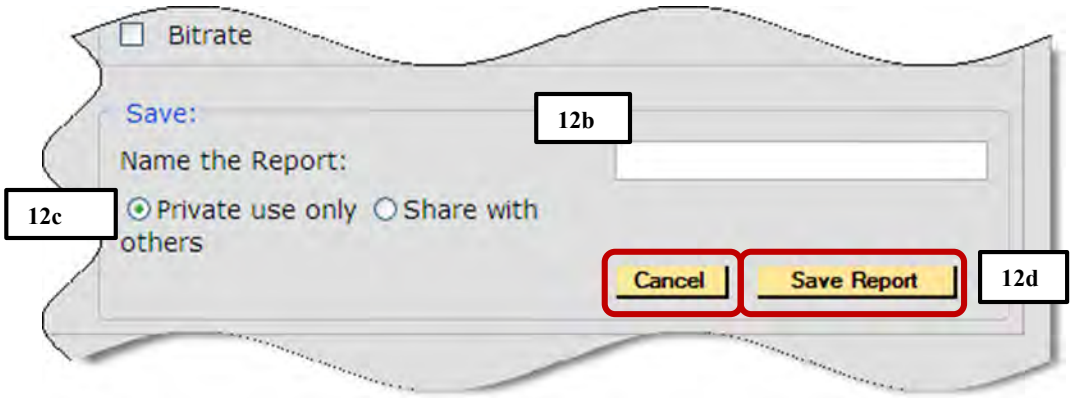



**Figure 217: Scheduling**

    c. Choose **Private** use only or **Share with others**.
    d. Select **Save**

13. Once you have saved the report, you can schedule it to run and automatically email you the results.
    a. Select **Schedule Report** and follow steps as per **Scheduling Email** portions of this manual.

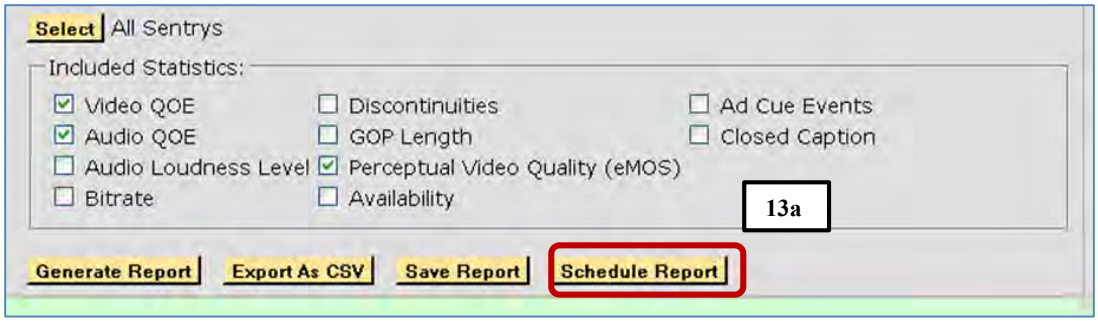



**Figure 218: Schedule a report**

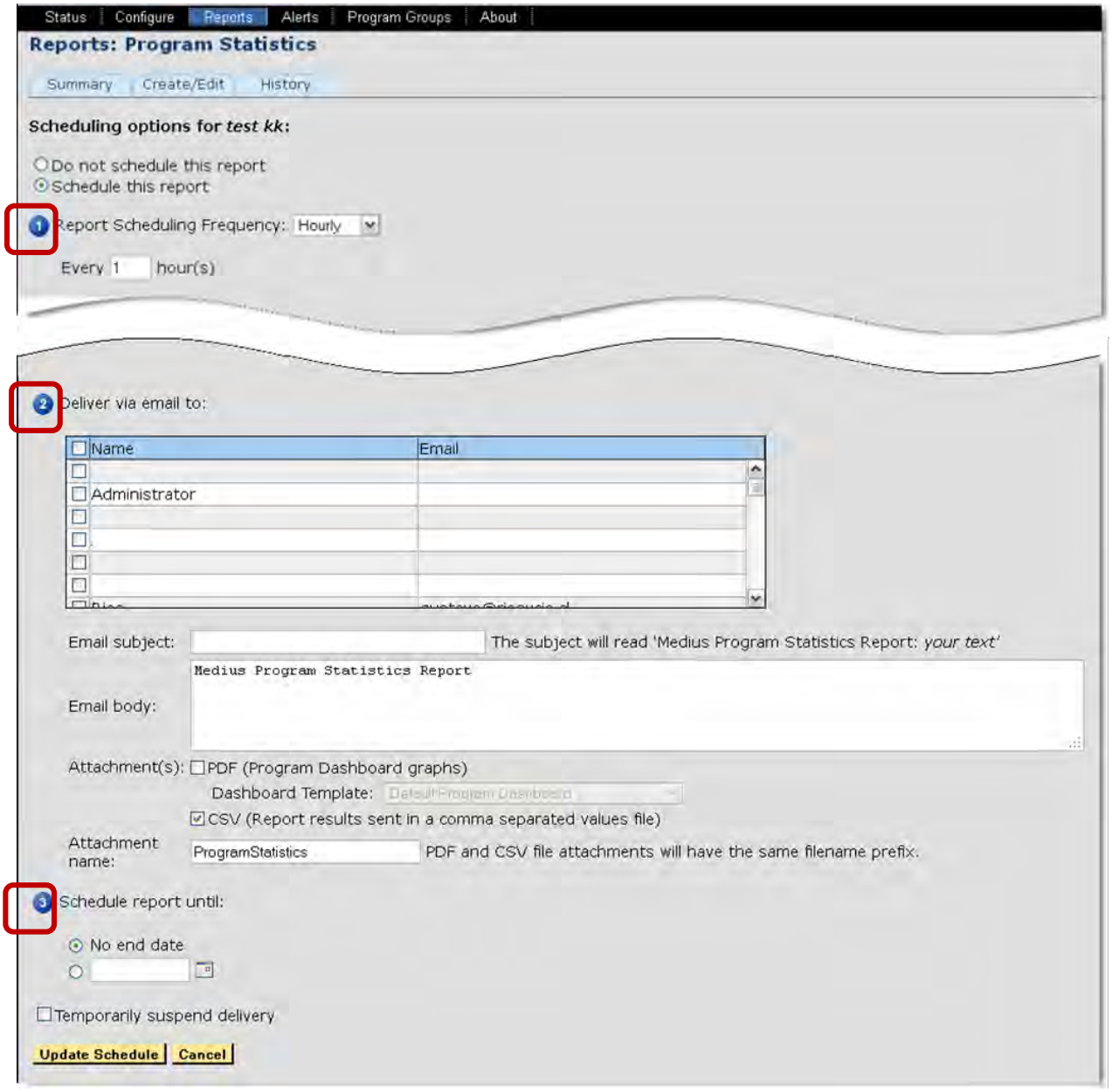



**Figure 219: Scheduling Options**

14. Pick the frequency you wish the report to run.

15. Select who you want to email

16. Schedule how long you want the report to run.

## History tab

The **History** tab shows you the history of the email for scheduled program stat reports.


**Figure 220: History tab**

***NOTE: The program stats CSV export includes the selected stop and start times (for the time period the user selected).***

# Program Dashboard

**Program Dashboard** allows you to see graphs of all running reports. You may also **Configure Graphs** from this page.

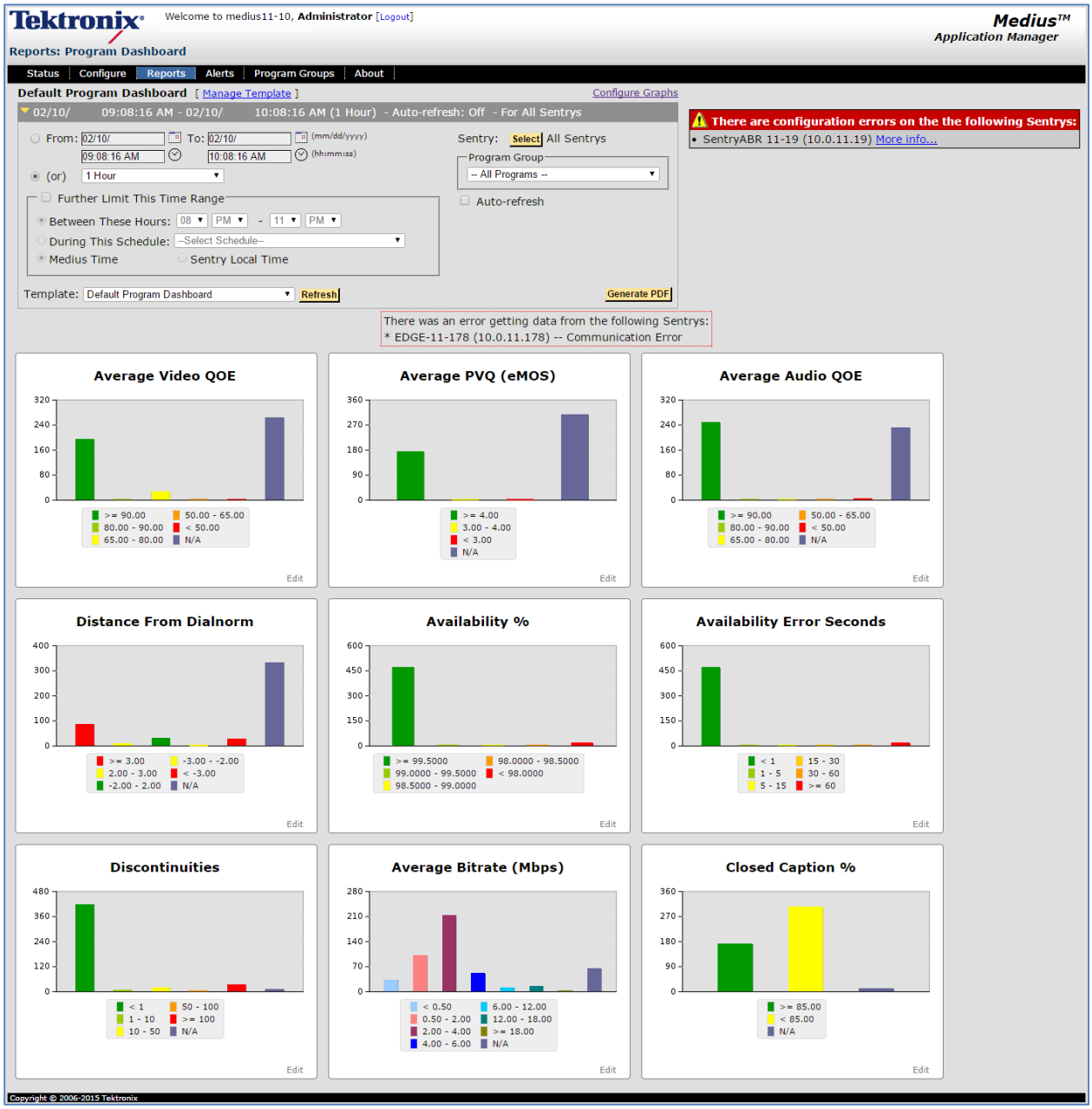



**Figure 221: Program Dashboard**

# Sentry Reports

Medius contains access to all the reports that can be run on Sentry. After accessing the **Report** from the Medius, please see the Sentry Manual for complete step by step details.

## Access Sentry Reports

1. From the **Reports** drop-down menu and under the **Sentry Reports** header, select the report of your choice.

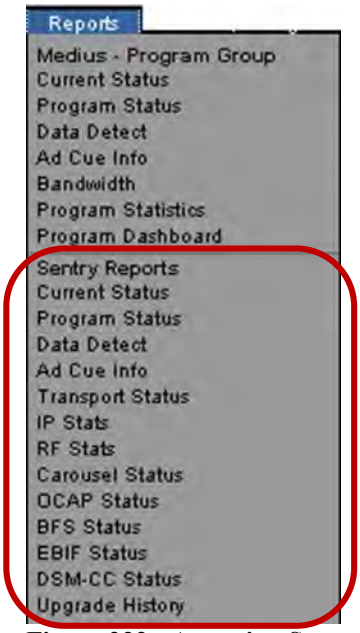



**Figure 222: Accessing Sentry Reports**

2. Next, select the Sentry you wish to view.

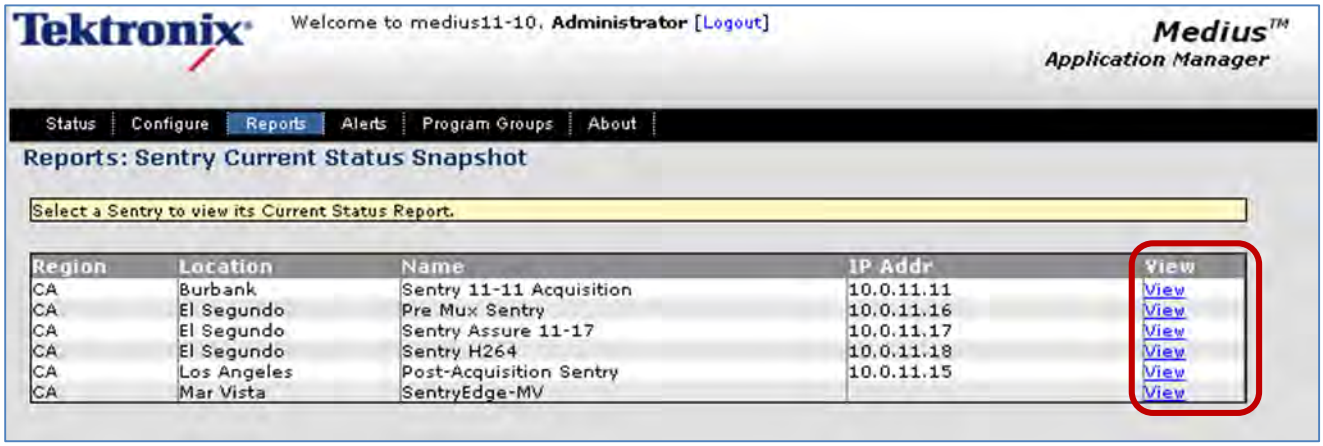



**Figure 223: Selecting a Sentry to view**

3. Please see the ***Sentry Manual*** for further details and step by step instructions.

# Alerts

Alerts are a key component of Medius and are used to identify particular transport stream conditions. They are also completely independent from the **Sentry Alert** systems. All Medius alerts are fully-configurable and real- time, and are active globally within the system. If an alert condition is met, the alert will be generated and the **Alert History** will display the alert.

If the alert is configured to send an email, it will be sent to the designated user(s) when the alert is generated. If the alert is configured to send an SNMP trap, it will be sent to the **Trap host IP** configured in the **System Settings** when the alert is generated.

The last field in the SNMP trap contains a URL that links to the most relevant page concerning the alert type.

## Access Alerts Summary

1. Select **Summary** from the **Alerts** drop-down menu.

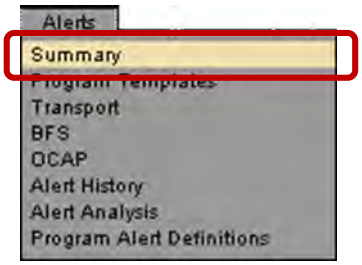



**Figure 224: Accessing Summary**

# Transport Alert Summary

## Access Transport Summary

1. Select **Transport** from the **Alerts** drop-down menu.


**Figure 225: Accessing Transport alerts**

2. From the Tr**ansport Alerts Summary** page, you may view existing alerts or create new alert by selecting **Create Template**.

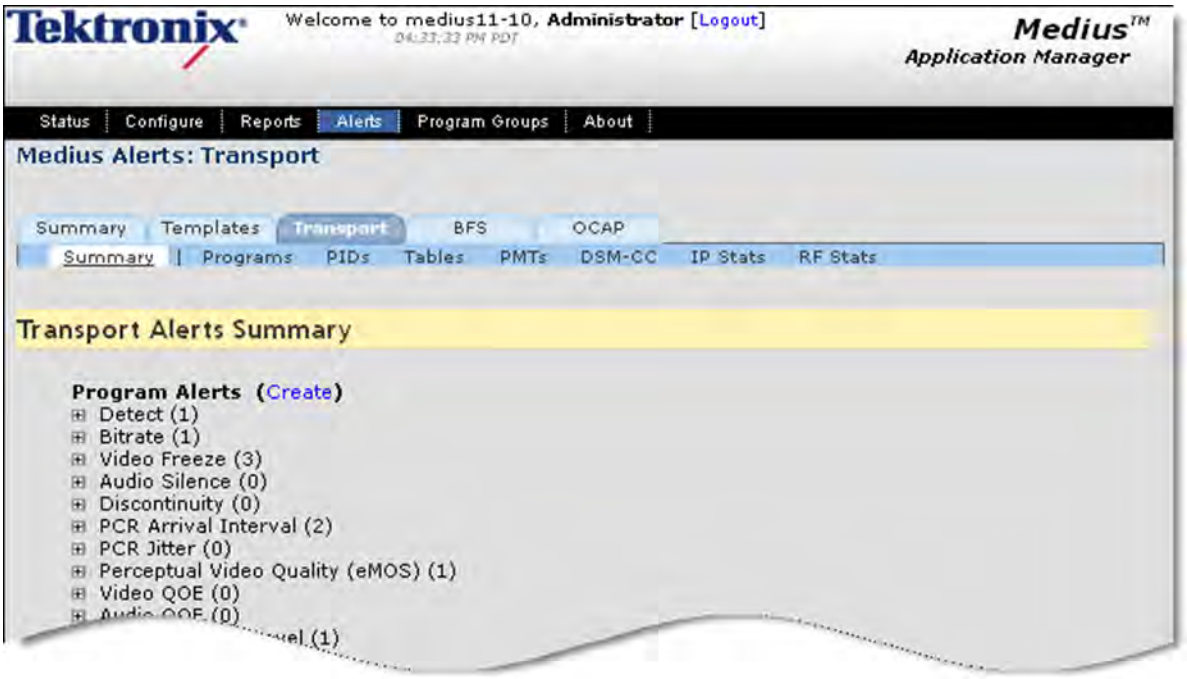



**Figure 226: Transport Alerts Summary**

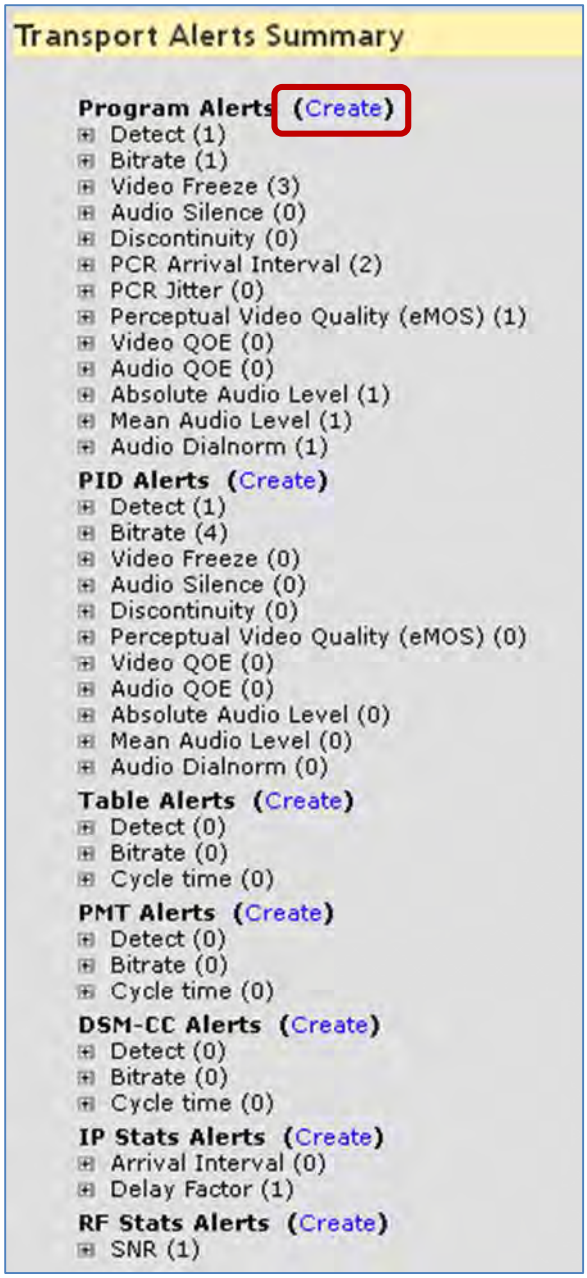



**Figure 227: Transport Alert Summary page**

## Types of Transport Alerts

### *Program Alerts*

- **Detect**
  Generates the alert when any of the selected programs is present or absent in the database. When the alert is first created the condition (present or absent) is checked, and thereafter is only checked when the program is created or destroyed.

- **Bitrate:**
  Generates the alert when the total bitrate of any of the selected programs is greater than, equal to, or less than a specified bitrate.

- **Video Freeze**
  Generates the alert when the video remains unchanged (i.e., frozen) for a specified length of time on any PID on any of the selected programs.

- **Audio Silence**
  Generates the alert when the audio is silent for a specified length of time on any PID on any of the selected programs on a group of channels.

- **Discontinuity**
  Generates the alert after a specified number of discontinuities is counted on all the PIDs on any one of the selected programs.

- **Perceptual Video QOE(eMOS)**
  Generates an alert when the PVQ goes above or below a user set threshold. This is not coupled with any particular QOE event or alert.

- **Video QoE**
  Generates the alert when the video QoE score for any program goes above or below a specified value on either the primary video PID or any video PID (Out of a possible score of 100).

- **Audio QoE**
  Generates the alert when the audio QoE score for any program goes above or below a specified value on either the primary audio PID or any audio PID (Out of a possible score of 100).

- **Absolute Audio Level**
  Generates the alert when the absolute audio level goes above or below a specified dB value on either the primary audio PID or any audio PID.

- **Mean Audio Level**
  Generates the alert when the mean audio level either increases, decreases, or both by a specified dB value within a given time frame on either the primary audio PID or any audio PID.

- **Audio Dialnorm**
  Generates the alert when the audio level goes above or below dialnorm by a specified dB value on either the primary audio PID or any audio PID.

### PID Alerts

- **Detect**
  Generates the alert when any of the selected PIDs is present or absent in the system. When the alert is first created the condition (present or absent) is checked, and thereafter is only checked when the PID is created or destroyed.
- **Bitrate**
  Generates the alert when the bitrate of any of the selected PIDs is greater than, equal to, or less than a specified bitrate.
- **Video Freeze**
  Generates the alert when the video remains unchanged (i.e., frozen) for a specified length of time on any of the selected PIDs.
- **Audio Silence**
  Generates the alert when the audio is silent for a specified length of time on any of the selected PIDs on a group of channels.
- **Discontinuity**
  Generates the alert after a specified number of discontinuities is counted on any one of the selected PIDs.
- **Perceptual Video QOE(eMOS)**
  Generates an alert when the PVQ goes above or below a user set threshold. This is not coupled with any particular QOE event or alert.
- **Video QoE Video QoE**
  Generates the alert when the video QoE score for any PID goes above or below a specified value (Out of a possible score of 100).
- **Audio QoE**
  Generates the alert when the audio QoE score for any PID goes above or below a specified value (Out of a possible score of 100).
- **Absolute Audio Level**
  Generates the alert when the absolute audio level goes above or below a specified dB value.
- **Mean Audio Level**
  Generates the alert when the mean audio level either increases, decreases, or both by a specified dB value within a given time frame.
- **Audio Dialnorm**
  Generates the alert when the audio level goes above or below dialnorm by a specified dB value.

### Any PID on a Port

- **Audio Silence**
  Generates the alert when the audio is silent for a specified length of time on any PID on any of the selected ports on a group of channels.
- **Video Freeze**
  Generates the alert when the video remains unchanged (i.e., frozen) for a specified length of time on any PID on any of the selected ports.

### Table on a Port

- **Detect**
  Generates the alert when the selected Table ID is present or not present on any selected port. When the alert is first set the condition (present or not present) is checked, and thereafter is only checked when the table is created or destroyed.

- **Bitrate**
  Generates the alert when the total bitrate for all tables of the selected ID on any selected port is greater than, equal to, or less than a specified value.

- **Cycle Time**
  Generates the alert when any table of the selected ID on any selected port has a cycle time greater than, equal to, or less than a specified value.

### Table on a PID

- **Detect**
  Generates the alert when the selected table is present or not present. When the alert is first set the condition (present or not present) is checked, and thereafter is only checked when the table is created or destroyed.

- **Bitrate**
  Generates the alert when the total bitrate for all the selected tables is greater than, equal to, or less than a specified value.

- **Cycle Time**
  Generates the alert when any of the selected tables has a cycle time greater than, equal to, or less than a specified value.

### PMT

- **Detect**
  Generates the alert when the selected PMT is present or not present. When the alert is first created the condition (present or not present) is checked, and thereafter is only checked when the PMT is created or destroyed.

- **Bitrate**
  Generates the alert when the total bitrate for all the selected PMTs is greater than, equal to, or less than a specified value.

- **Cycle Time**
  Generates the alert when any of the selected PMTs has a cycle time greater than, equal to, or less than a specified value.

### DSM-CC on a Port

- **DC Detect**
  Generates the alert when the selected DC is present or not present on any selected port. When the alert is first created the condition (present or not present) is checked, and thereafter is only checked when the DC is created or destroyed.
- **DC Bitrate**
  Generates the alert when the total bitrate for all DCs on any selected port is greater than, equal to, or less than a specified value.
- **DC Cycle Time**
  Generates the alert when any of the selected DCs on any selected Port has a cycle time greater than, equal to, or less than a specified value.
- **DII Detect**
  Generates the alert when the selected DII is present or not present on any selected port. When the alert is first created the condition (present or not present) is checked, and thereafter is only checked when the DII is created or destroyed.
- **DII Bitrate**
  Generates the alert when the total bitrate for all DIIs on any selected port is greater than, equal to, or less than a specified value.
- **DII Cycle Time**
  Generates the alert when any of the DIIs on any selected port has a cycle time greater than, equal to, or less than a specified value.

### DSM-CC

- **DC Detect**
  Generates the alert when the selected DC is present or not present. When the alert is first set the condition (present or not present) is checked, and thereafter is only checked when the DC is created or destroyed.
- **DC Bitrate**
  Generates the alert when the total bitrate for all the selected DCs is greater than, equal to, or less than a specified value.
- **DC Cycle Time**
  Generates the alert when any of the selected DCs has a cycle time greater than, equal to, or less than a specified value.
- **DII Detect**
  Generates the alert when the selected DII is present or not present. When the alert is first created the condition (present or not present) is checked, and thereafter is only checked when the DII is created or destroyed.
- **DII Bitrate**
  Generates the alert when the total bitrate for all the selected DIIs is greater than, equal to, or less than a specified value.
- **DII Cycle Time**
  Generates the alert when any of the selected DIIs has a cycle time greater than, equal to, or less than a specified value.

### Port Alerts

- **Arrival Interval**
  Generates the alert when the arrival interval is greater than, equal to, or less than a specified value.
- **Delay Factor**
  Generates the alert when the delay factor is greater than, equal to, or less than a specified value.
- **TR101/290**
  Generates the alert when any of the selected TR101/290 priorities is in error a specified amount of time.

## Create a Program Alert

1. Select **Transport** from the **Alerts** drop-down menu.


**Figure 228: Selecting Transport alerts**

2. Select **Create** from the **Program Alerts** section.

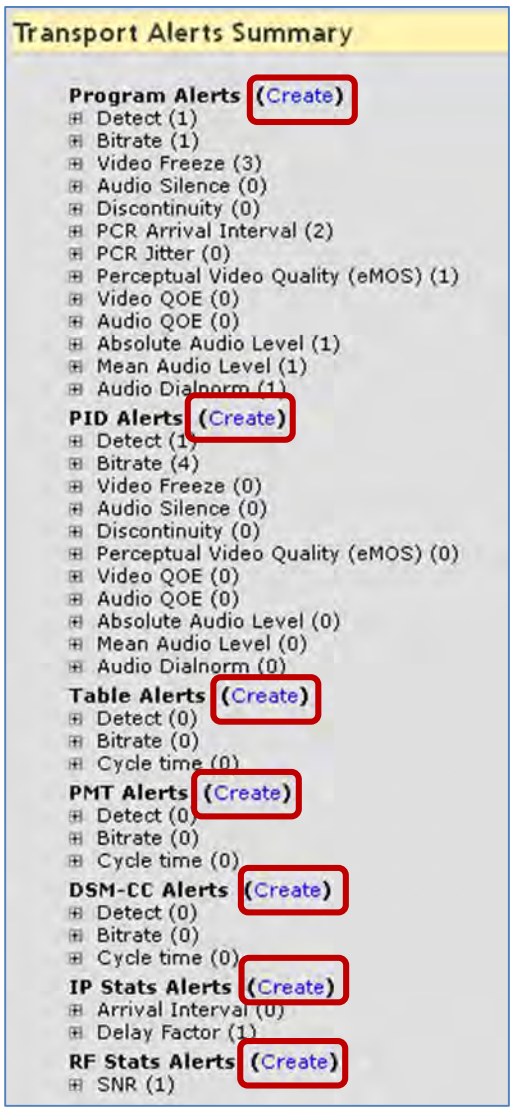



**Figure 229: Transports Alert Summary page**

3. Choose the type of alert you wish to create and then the information for **Section 1** will automatically populate.

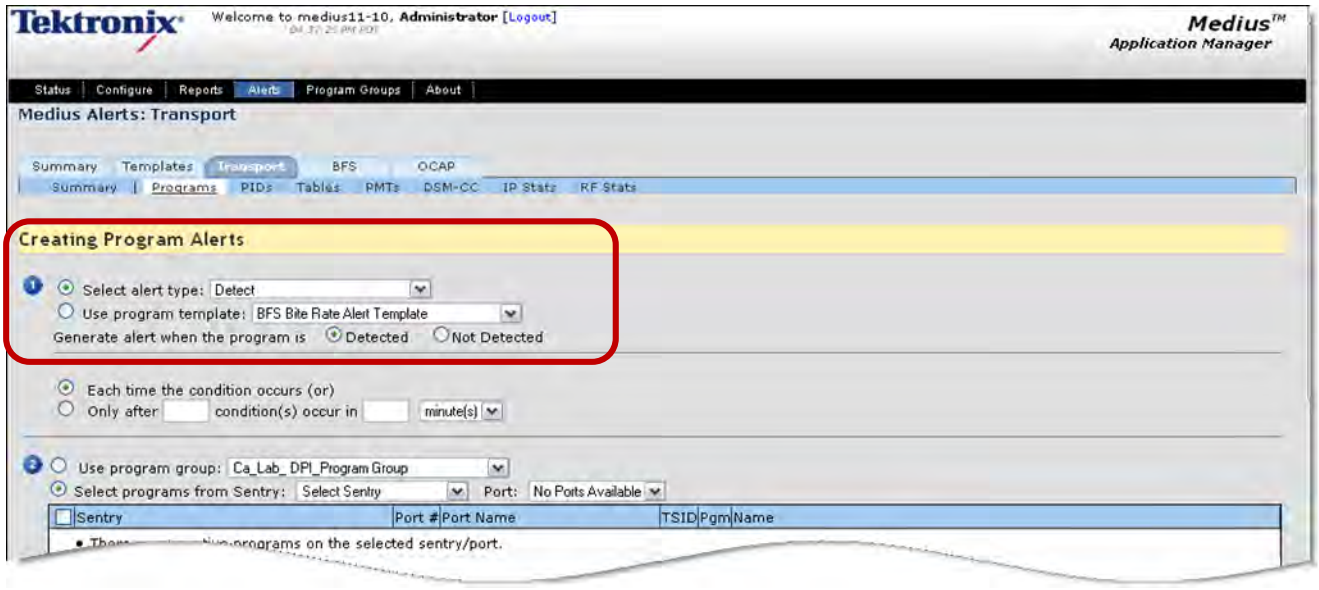



**Figure 230: Creating Program Alerts**

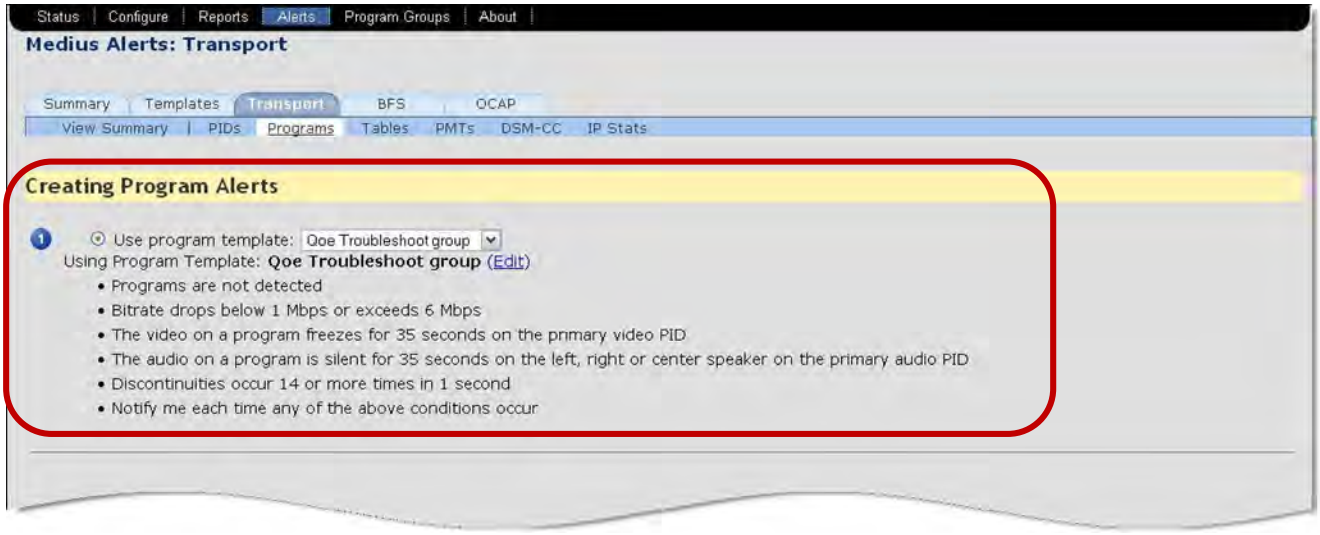



**Figure 231: Creating Program Alerts Step 1**

4. In **Section 2,** select the **Program Group** and individual Sentry.

5. The **Program** section will automatically populate.

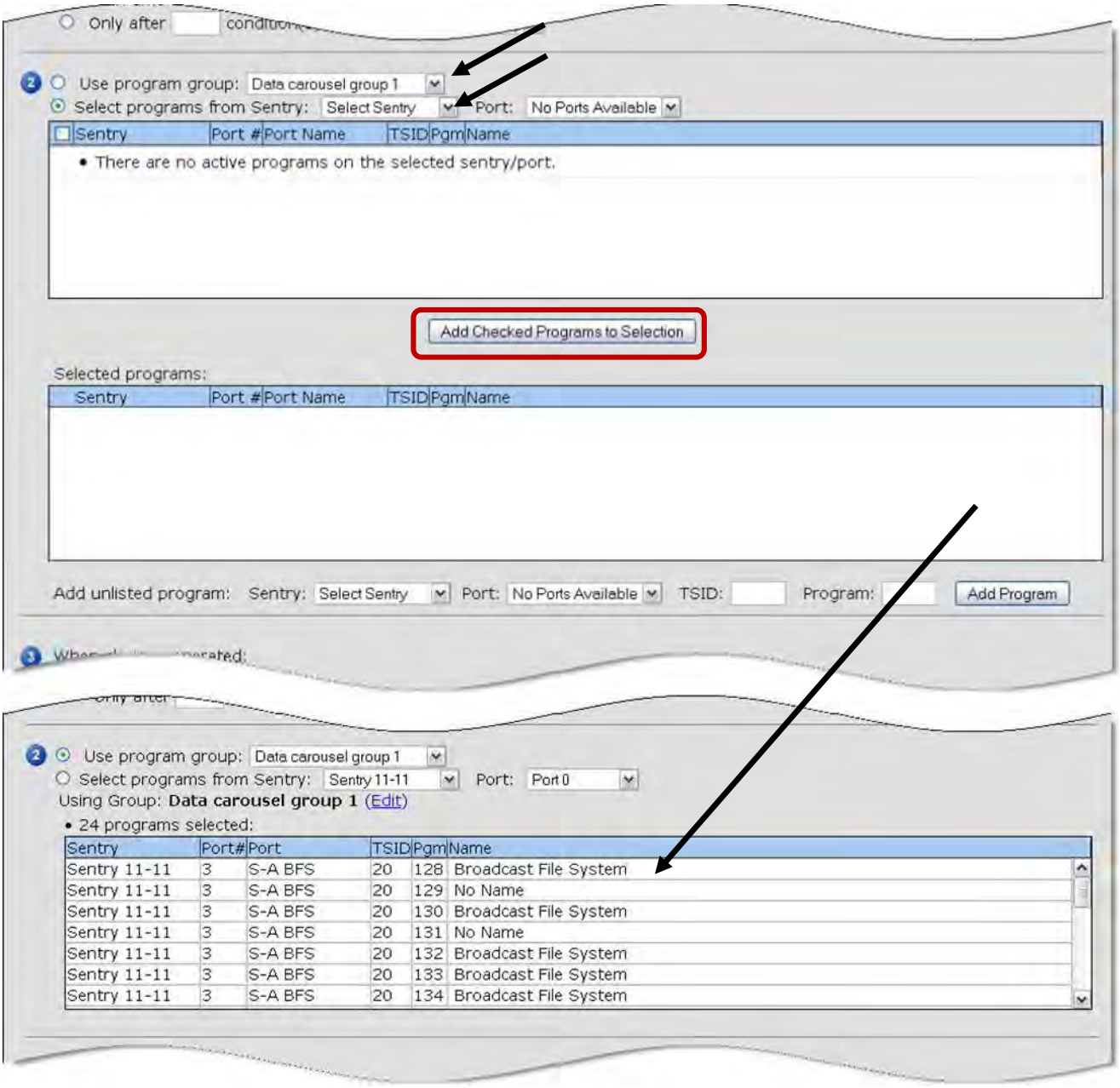



**Figure 232: Creating Program Alerts Section 2 (adding the selected programs)**

6. For **Section 3,** select the notification email information for when the alert is generated.

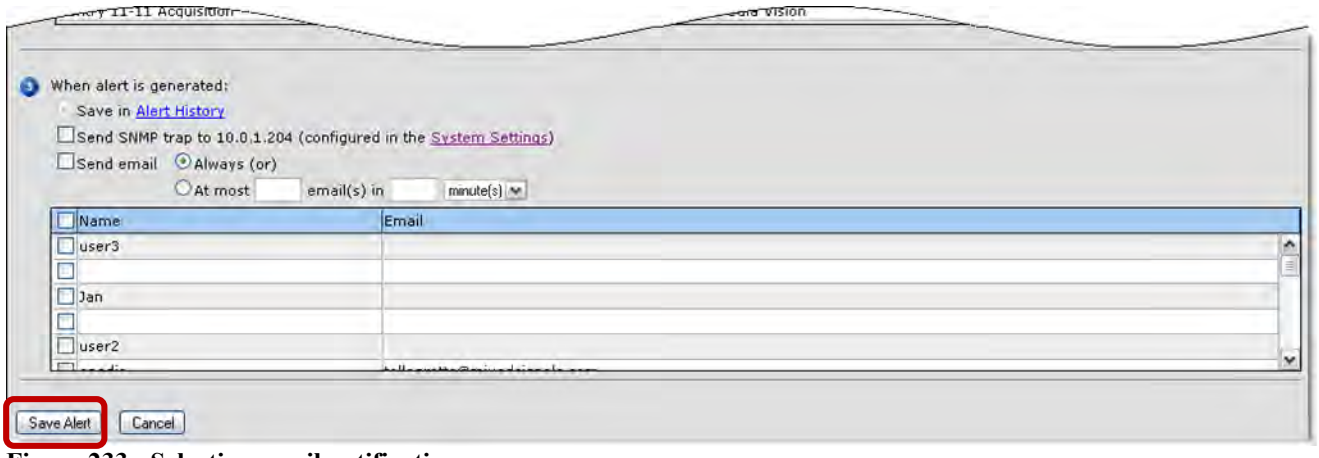



**Figure 233: Selecting email notifications**

7. Select **Save Alert** when finished.

## Create a Transport NULL PID Bitrate Alert

1. From the main menu, select **Alerts** and then **Transport**.
2. From the **Transport Alerts Summary** column, scroll down to **PID Alerts** and select **Create**.

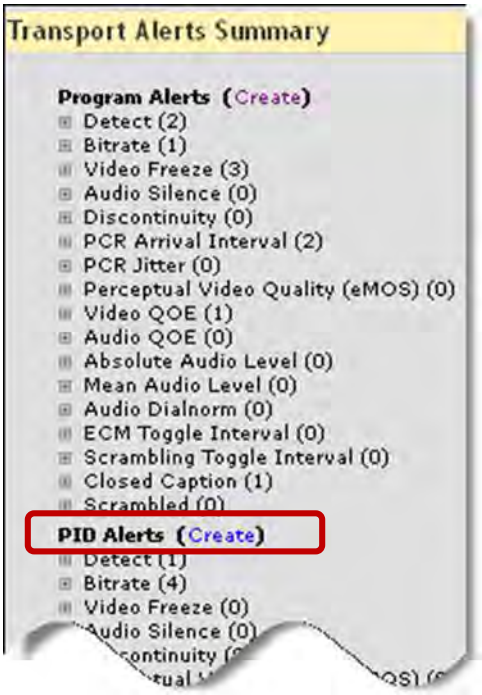



**Figure 234: Selecting Create for PID Alerts**

3. From the **Creating PID Alerts** page, work your way through **Sections 1-3.**

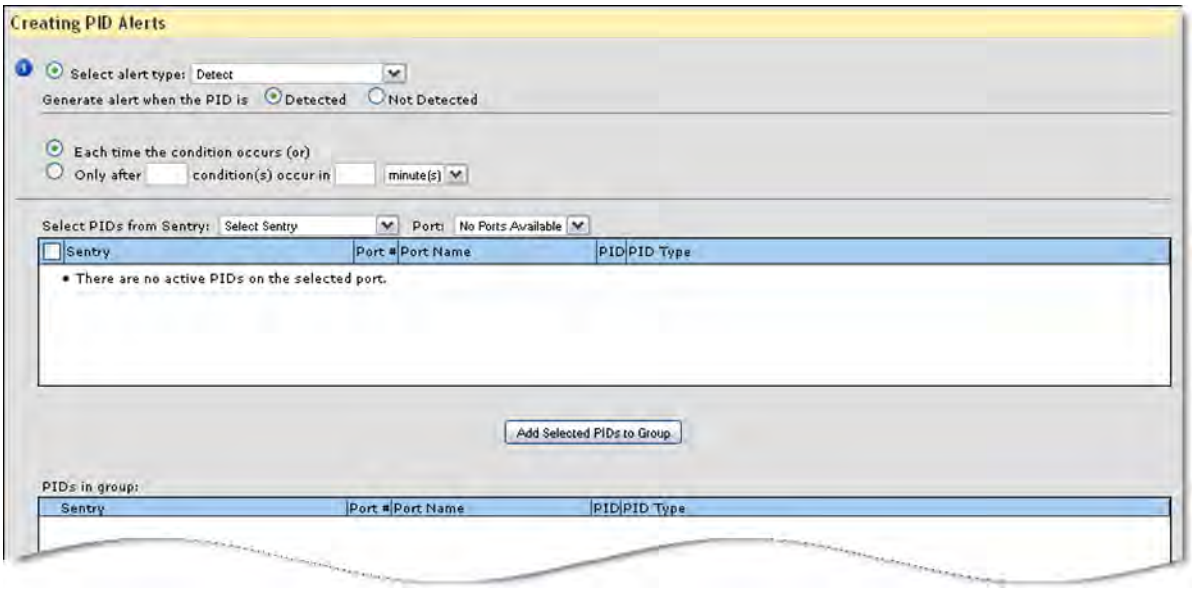



**Figure 235: PID alerts Overview**

4. **Section** 1
   Select **Bitrate** from the drop-down menu.

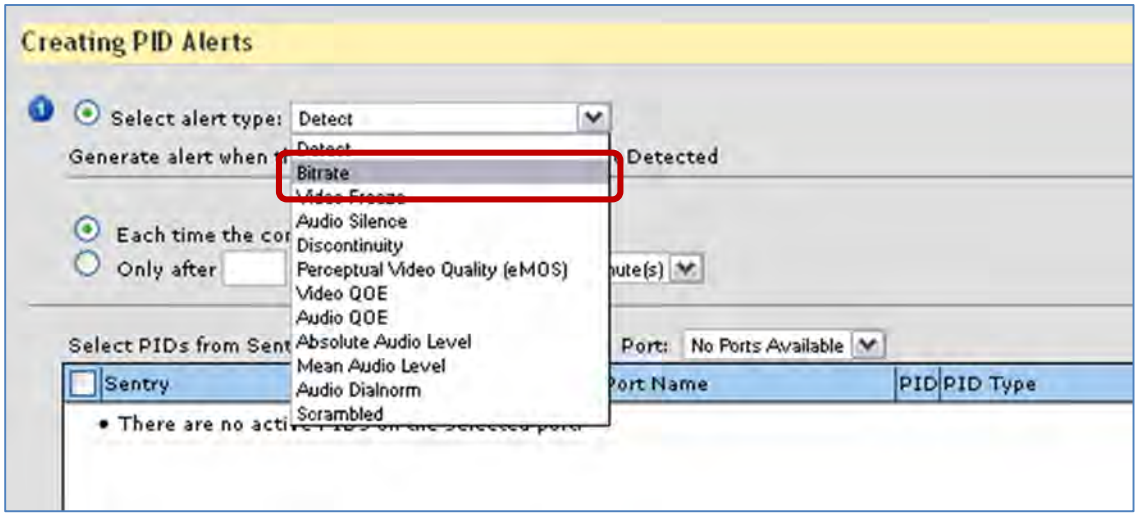



**Figure 236: Selecting the Alert Type**

5. Section 2 Select the Sentry you are setting the alert for.

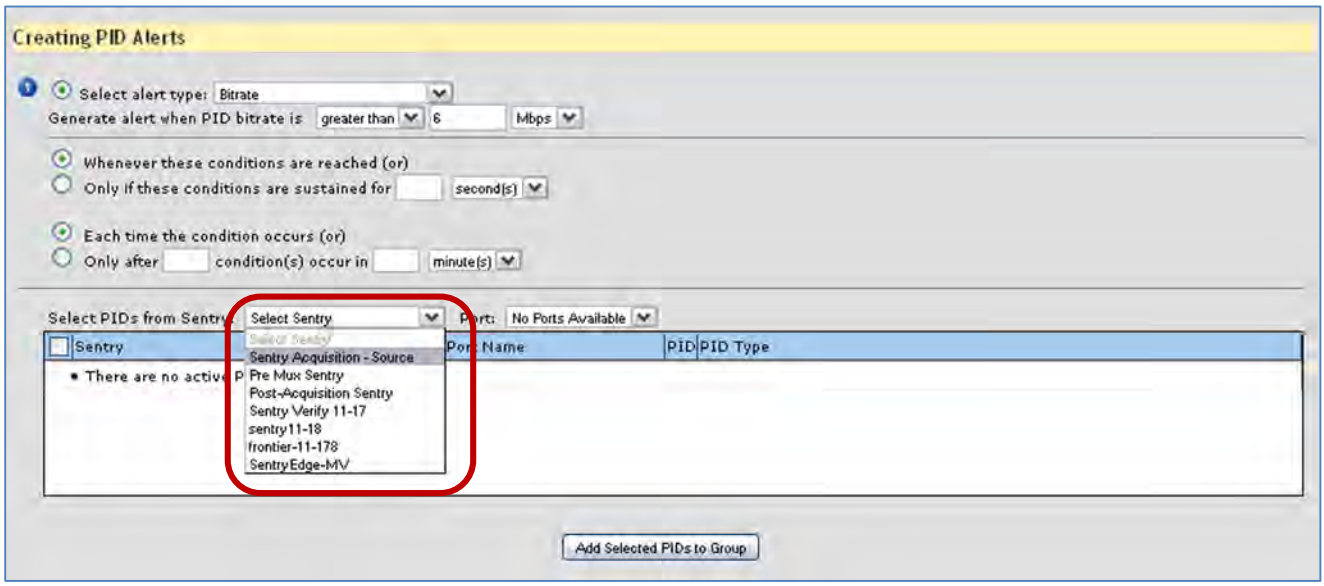



**Figure 237: Selecting Sentrys**

6. Set **Generate alert when the PID bitrate is less than.**
7. Next select the desired bitrate.
8. Choose any further required limitations.
9. Select PIDs from list.

**10.** Scroll down the list and select the **Null Packet PIDs.**

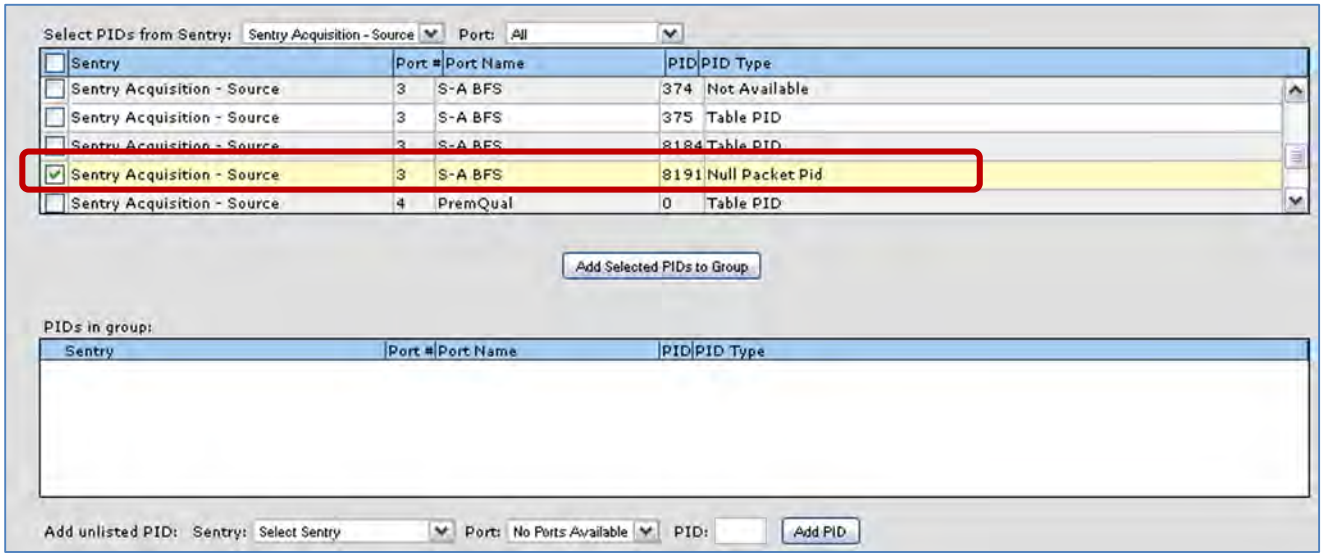



**Figure 238: Selecting PIDs**

**11.** Then select **Add Selected PIDs to Group.**

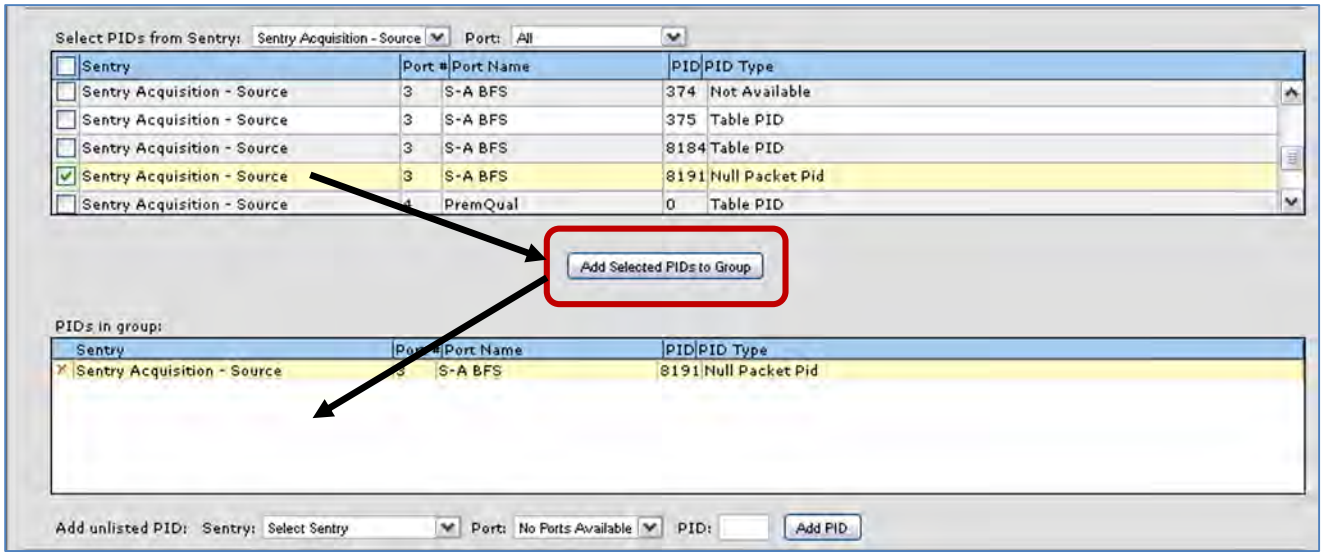



**Figure 239: Adding selected PIDs to Group**

**12.** Review **Sections 1-3** and select **Save Alert** when finished.

## Buffer overrun/underrun detection

Buffer overrun and underrun can occur for a variety of reasons, such as network jitter, improper MUXing, improper encoding, etc. Buffer overruns/underruns can cause the picture or sound to drop out completely or freeze for a short time, then resume. Some set top boxes, mainly older units, are more sensitive to buffer overruns than other models.

Buffer overruns and underruns occur under the following conditions:

- **Audio Buffer Overrun**
  Buffer timing violation causing buffer overrun. >= 100ms
- **Audio Buffer Underrun**
  Buffer timing violation causing buffer underrun. = 0 seconds, meaning that the buffer is empty
- **Video Buffer Overrun**
  Buffer timing violation causing buffer overrun. >= 1 sec
- **Video Buffer Underrun**
  Buffer timing violation causing buffer underrun. = 0 seconds, meaning that the buffer is empty

## Configure the Buffer overrun/underrun detection

**NOTE**: ***The Audio Silence Alerts template is the only place to set the Audio/Video Buffer overrun/underrun detection. You cannot do this from the Program template. As the QoE score looks at buffer issues, these alerts should only be set if you are looking for specific buffer issues.***

1. From the menu bar, select **Alerts** and then **Program Templates**
2. Select the **Transport** tab.
3. Next to the **Program Alerts** heading, select **Create.**


**Figure 240: Creating a Program Alert**

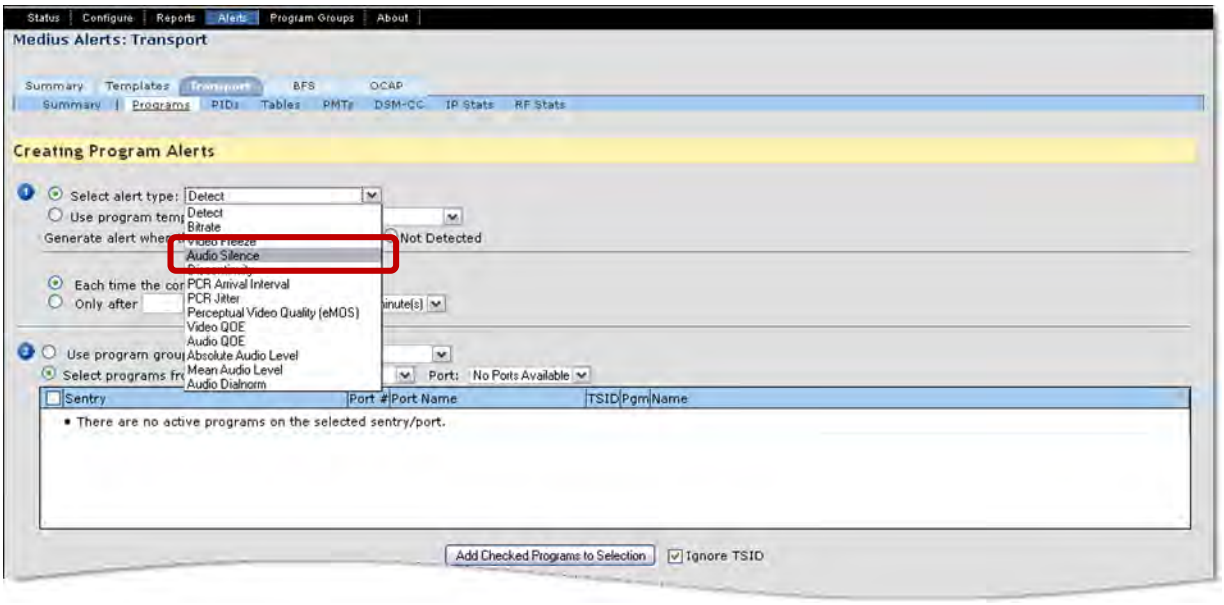



**Figure 241: Selecting Audio Silence**

4. Next, select either the **Audio buffer underrun** or **Audio buffer overrun** box or both, as needed.

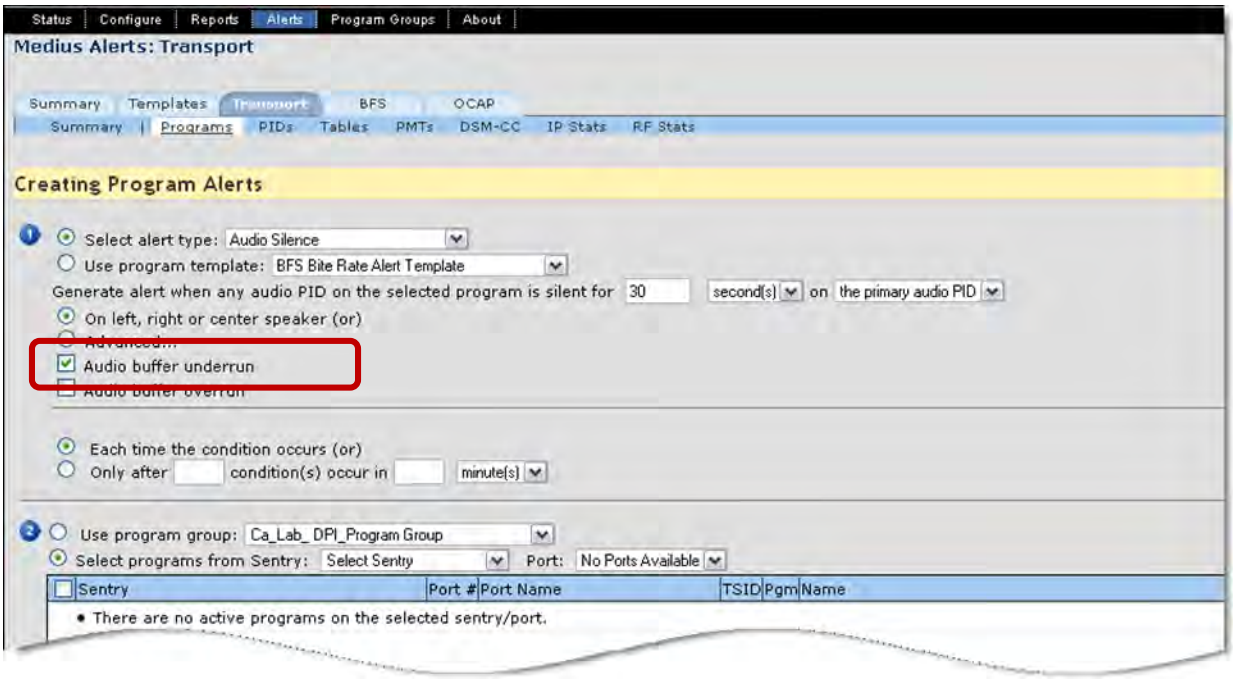



**Figure 242: Selecting Audio buffer underrun/overrun**

5. Refer to **Sentry Chapter 4: Configuring Alerts** for the steps to complete this process.

# Create Program Template Alerts

One of the primary functions of the Medius unit is to allow the user to monitor their programs through a series of **Alerts** that they can configure for optimal use.

The best way to set up different types of alerts and be able to apply them to multiple programs is to create an Alert **Template**. This allows the user to apply a set of alerts with pre-configured parameters to speed the alert creation and application process.

---

**NOTE**: ***This process only creates the Alert Template.***

***Once the Alert Template is complete, you must also create an alert!***

***Until you apply the template to the programs, no alerts will be generated.***

---

## Access Program Templates

1. Select **Program Templates** from the **Alerts** drop-down menu.

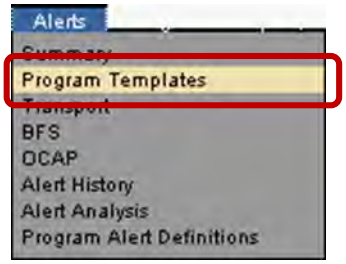



**Figure 243: Accessing Program Templates**

2. From the resulting page, select **Create Template** from next to the **Program Template Alerts** header.

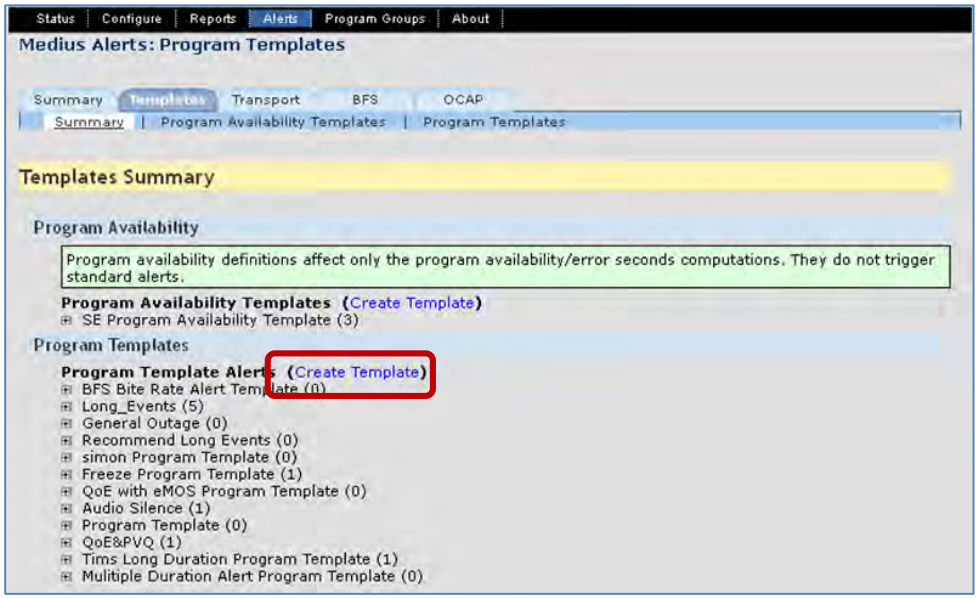



**Figure 244: Create a Template**

3. From the **Creating Program Alert Templates page**, you may create a template that can be used almost anywhere in the alert creation process. For example, you may create an alert template to fit your particular programs, such as **HD**, **SD,** or **Music** only.

4. **For Section** 1 , defaults are provided but any setting can be customized for your needs. You can also disable parameters that you do not wish to use by un-checking the appropriate box.

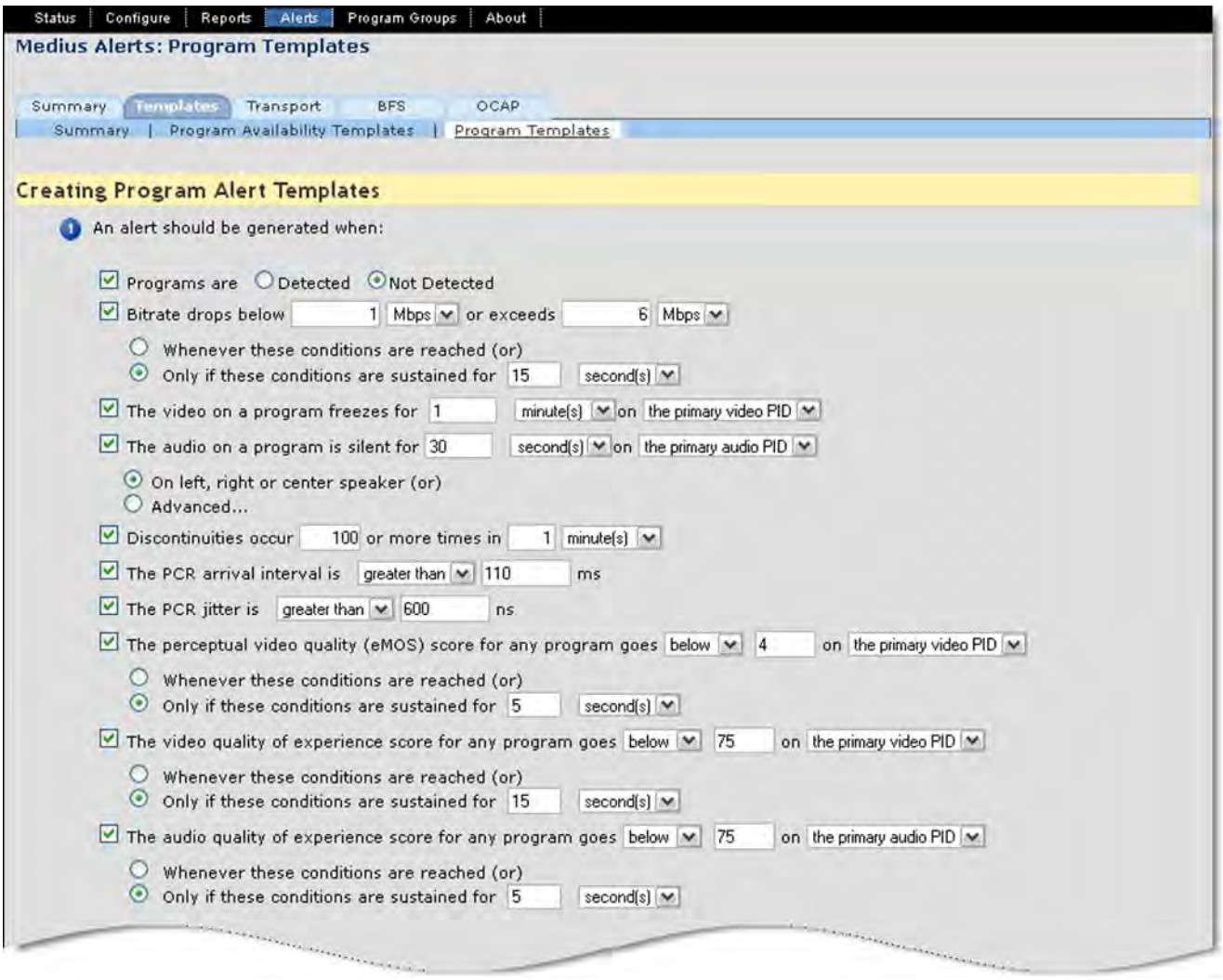



**Figure 245: Section 1 Selecting when the alert should be generated**

5. For Section 2 , select when you want to trigger an alert either each time the condition occurs or only after any of the above conditions occur in a specified amount of time.

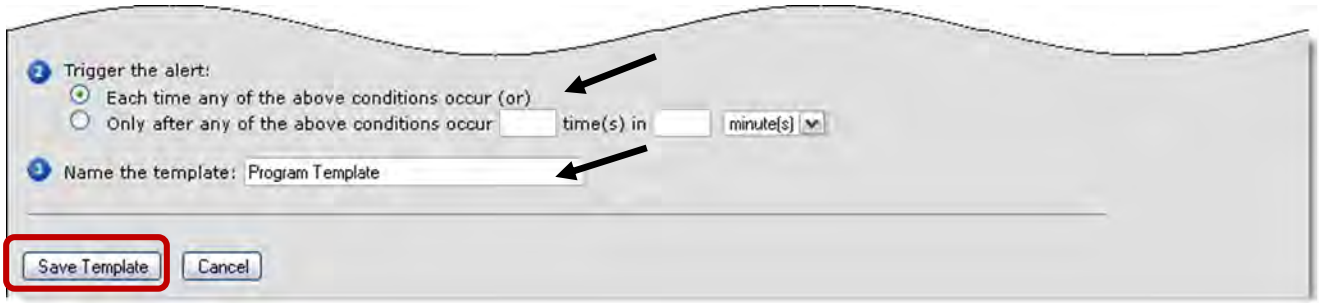



**Figure 246: Step 2 Triggering the alert, Naming the Alert and Saving the template**

6. In **Section** 3, name the template and select **Save Template**.

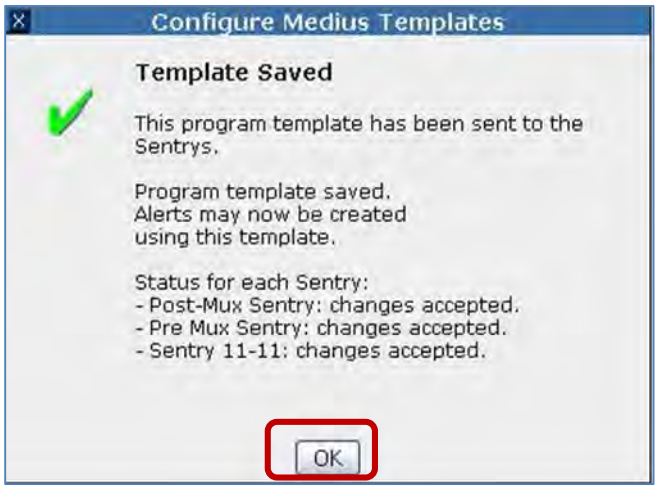



**Figure 247: Template Saved dialogue box**

7. Select **OK** on the **Template Saved** confirmation.

---

**NOTE**: ***Now that you have created the Alert Template, the next step is to actually create the alert!***

***You have just created a list of parameters that Medius can use to apply to specific programs. Until you apply the template to the programs, no alerts will be generated.***

---

## Create an alert from a Template using a Program Alert

1. Select the desired **Program Template Alert** from the list and click the expand button.


**Figure 248: Expanding Program Template Alpha**

2. Next, select **Create Alert**.

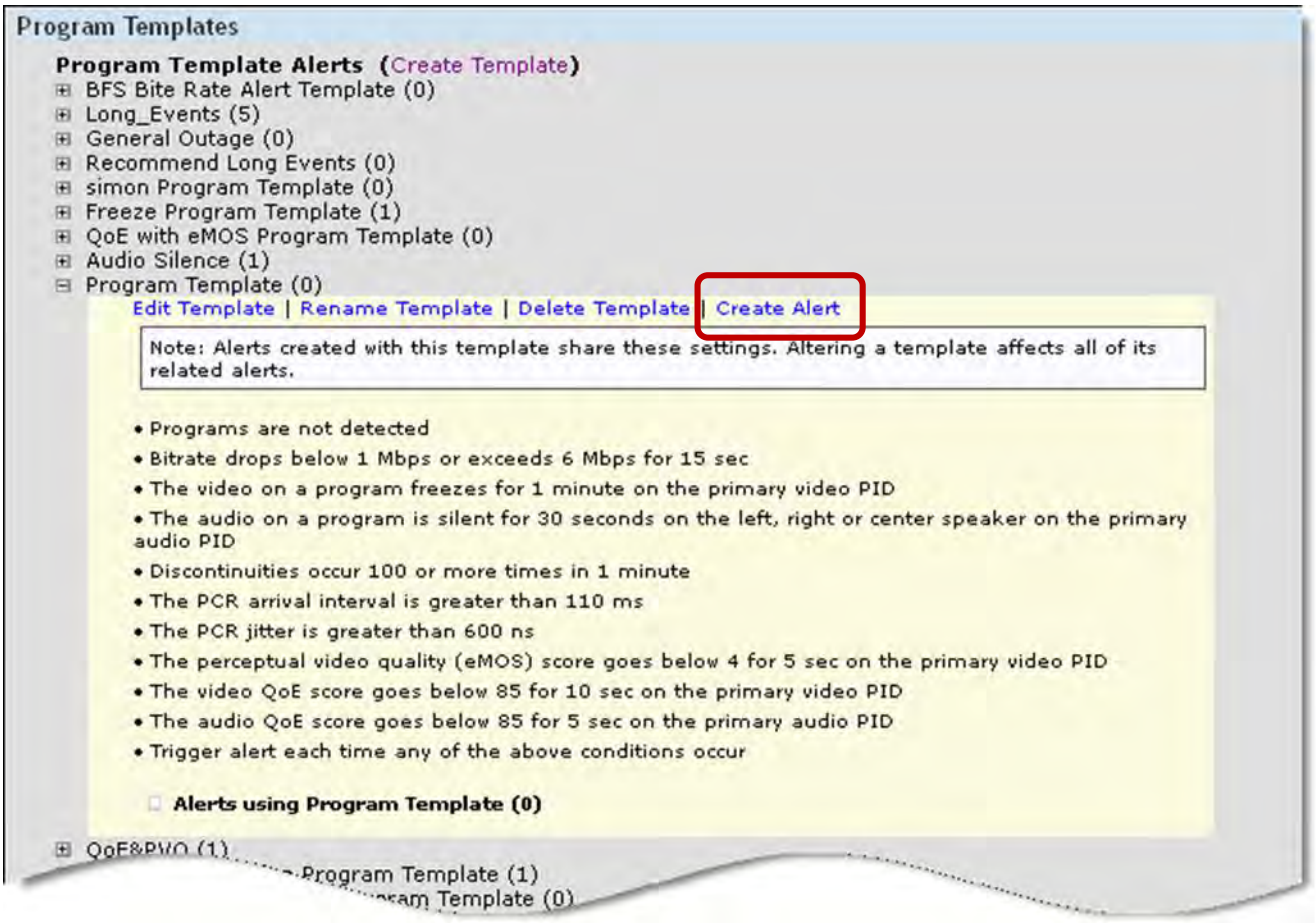



**Figure 249: Create the alert**

3. From the **Creating Program Alerts** page, start at **Section** 1 and verify that the previously selected **Program Template** is showing in the drop-down menu.

4. Review the parameters for the template. If you wish to change any of the parameters, select the **Edit** button. This will take you to the **Editing Program Alerts Template** page where you may make the desired changes.

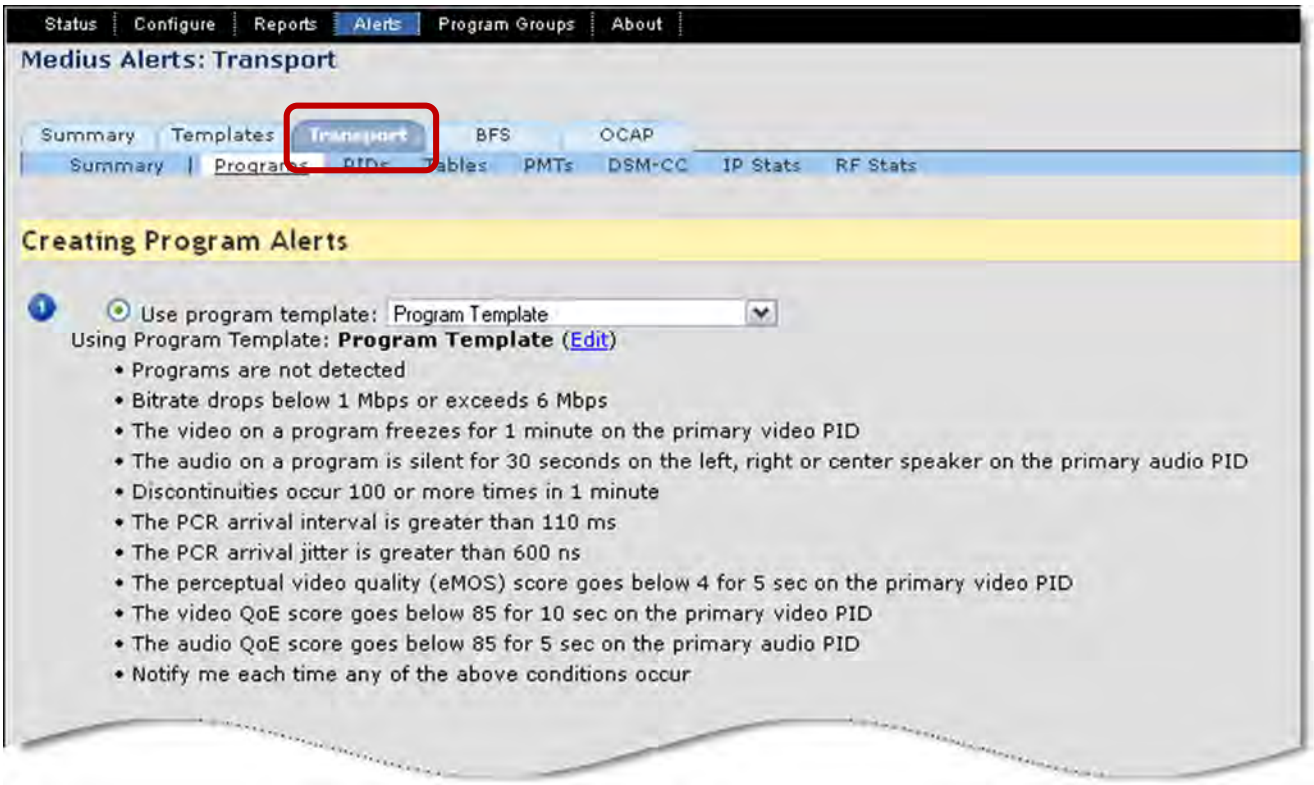



**Figure 250: Section 1 Checking for correct Program Template**

5. In Section 2, select the program group you wish to use from the drop-down menu.

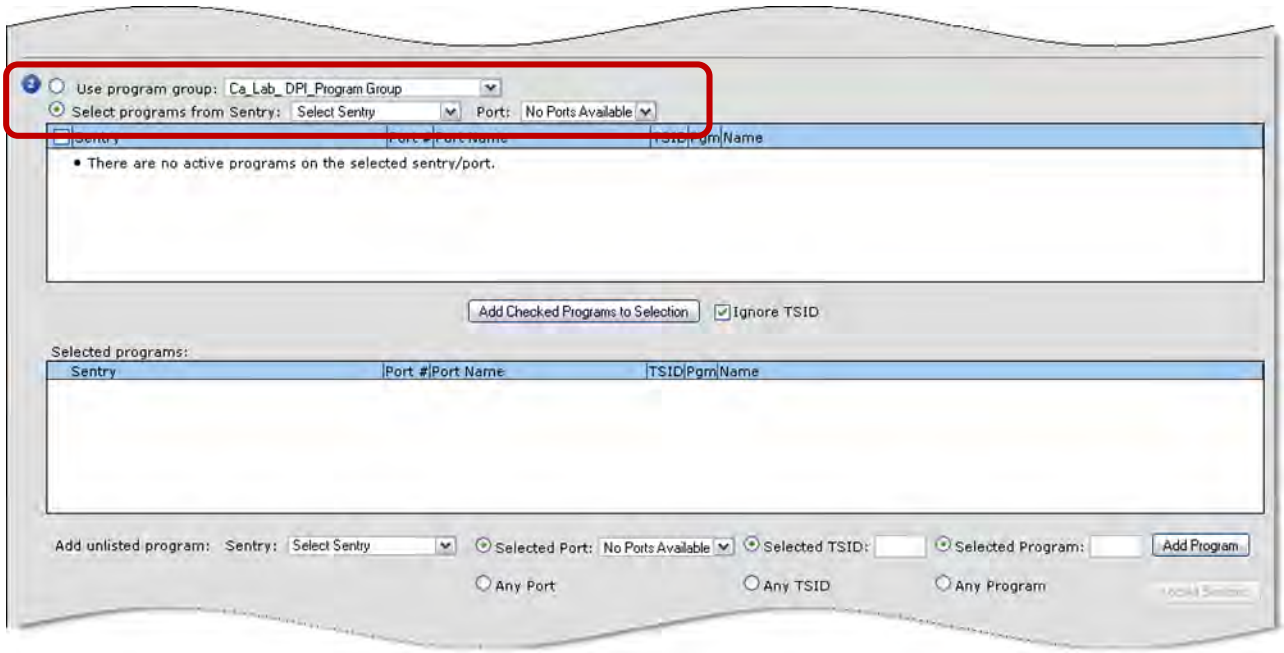



**Figure 251: Selecting the Program Group, Sentry and Port**

6. Select the Sentry and Port you are creating the alert for.

7. Finally, in Section 3, set the notifications for the alert.

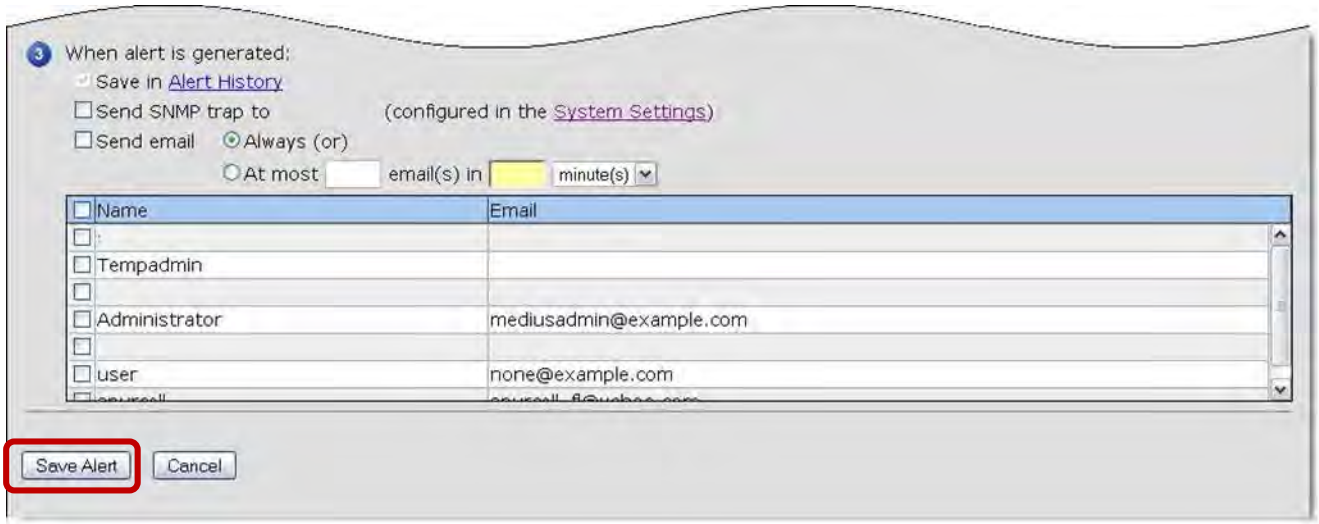



**Figure 252: Set Notifications and Save**

8. Review the page and select Save Alert when you are finished.

9. Now the Sentry will start to monitor those programs with the parameters you selected.

## Create an alert template without a Program Group

Follow the entire process up until **Section** 2 of the **Creating Program Alerts** page.

1. In **Section** 2, select the radio button for **Select Programs** and click on the drop-down menus to select the desired **Sentry** unit and **Port**.

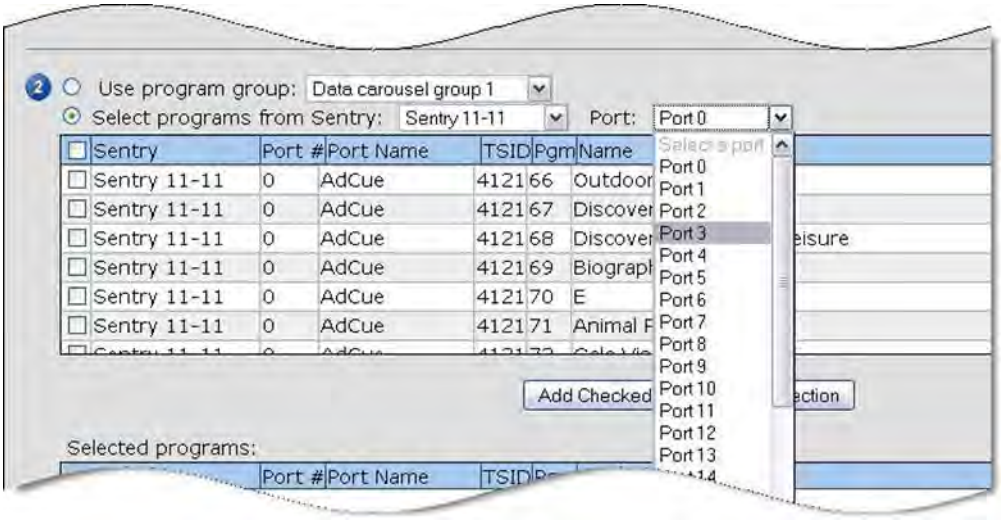



**Figure 253: Selecting the Port**

2. Select programs by checking their corresponding boxes.
3. When finished, select **Add Checked Programs to Selection**. If you need programs on other ports, select a new port from the drop-down menu and repeat the process.

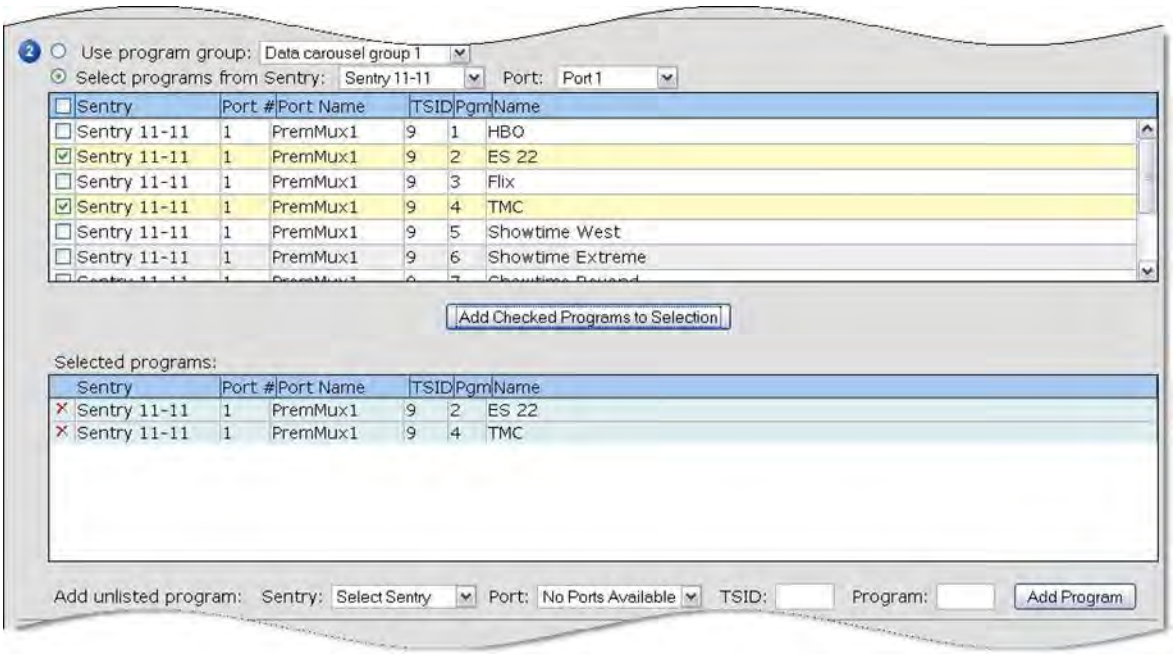



**Figure 254: Selecting programs**

4. Finally, in **Section** 3, set the notifications for the alert.

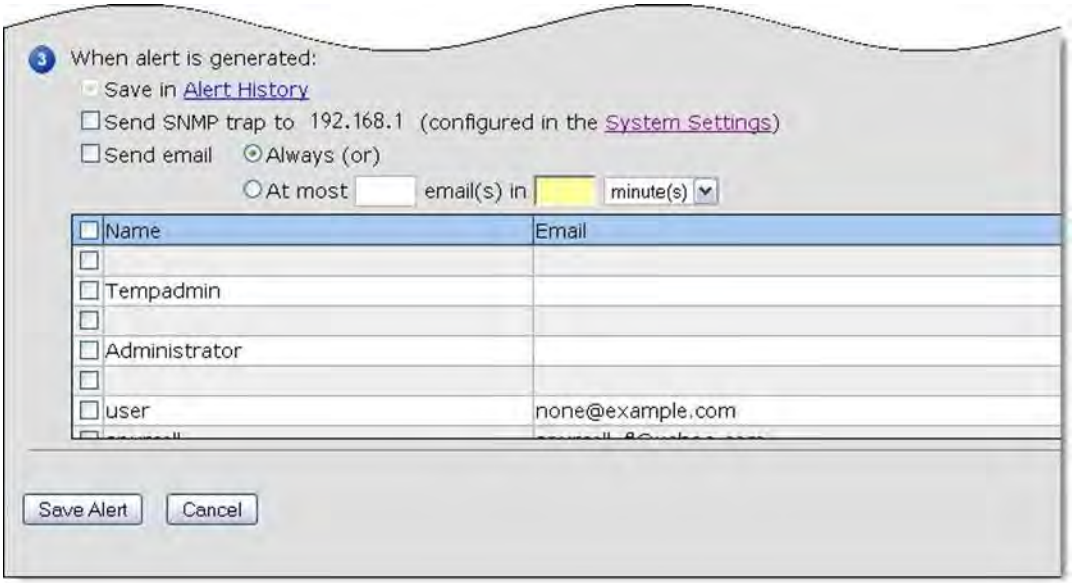



**Figure 255: Set Notifications and Save**

5. Review the page and select **Save Alert** when you are finished.

# BFS Alert Summary

## Access BFS

1. Select **OCAP** from the **Alerts** drop-down menu.

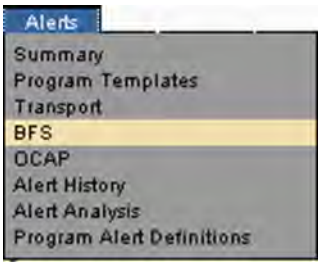



**Figure 256: Selecting BFS**

2. From the **BFS Alerts Summary** page, you may view existing alerts or create new alert by selecting **Create**.

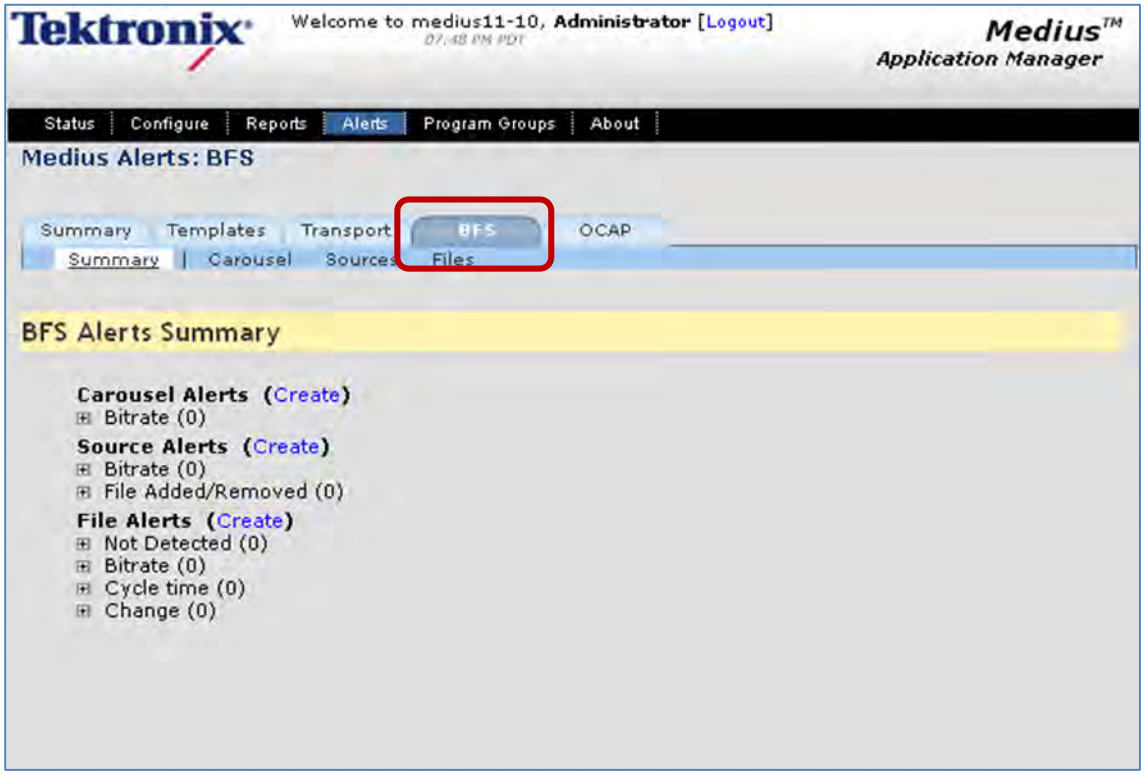



**Figure 257: BFS Alerts Summary**

# Types of BFS Alerts

## *BFS Source*

- **Bitrate**
  Generates the alert when the total bitrate of any of the selected sources is greater than, equal to, or less than a specified bitrate.

- **File Added/Removed**
  Generates the alert when any file is either added to or removed from any of the selected sources. The condition (added or removed) is not checked when the alert is created, the alert is only generated when the file is added or removed.

## *BFS Carousel*

- **Bitrate**
  Generates the alert when the total bitrate of any of the selected carousels is greater than, equal to, or less than a specified bitrate.

## *BFS File*

- **Not Present**
  Generates the alert when any of the selected files is absent in the database. When the alert is first set the condition (absent) is checked, and thereafter is only checked when the file is destroyed.

- **Bitrate**
  Generates the alert when the bitrate of any of the selected files is greater than, equal to, or less than a specified bitrate.

- **Cycle Time**
  Generates the alert when the cycle time of any of the selected files is greater than, equal to, or less than a specified cycle time.

- **File Change**
  Generates the alert when any of the selected files changes or when any of the selected files has not changed for a specified amount of time.

# OCAP Alert Summary

## Access OCAP

1. Select **OCAP** from the **Alerts** drop-down menu.

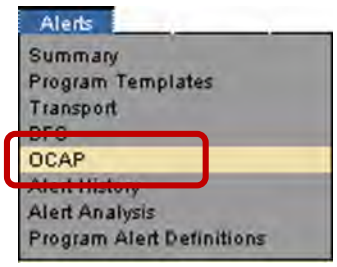



**Figure 258: Selecting OCAP alerts**

2. From the **OCAP Alerts Summary** page, you may view existing alerts or create new alert by selecting **Create**.


**Figure 259: OCAP Alerts Summary page**

# Types of OCAP Alerts

## File Alerts

- **Detect**
  Generates the alert when the selected file is present or is not present.
- **Bitrate**
  Generates the alert when the file bitrate is greater than, equal to, or less than a specified value.
- **Cycle Time**
  Generates the alert when the file cycle time is greater than, equal to, or less than a specified value.
- **Changed**
  Generates the alert when the file changes or has not changed for a specified time period.
- **Added/Removed**
  Generates the alert when the file is added or removed.

## Folder Alerts

- **Detect**
  Generates the alert when the selected folder or any files contained within it are present or are not present.
- **Bitrate**
  Generates the alert when the entire folder's contents bitrate or any file within the folder is greater than, equal to, or less than a specified value.
- **Cycle Time**
  Generates the alert when the file cycle time is greater than, equal to, or less than a specified value.
- **Changed**
  Generates the alert when files within the folder change or have not changed for a specified time period.
- **Added/Removed**
  Generates the alert when the folder or any files contained within it are added or removed.

## Extension Alerts

- **Detect**
  Generates the alert when the files with a specific extension are present or are not present.
- **Bitrate**
  Generates the alert when the entire folder's contents bitrate or any file within the folder with a specific extension is greater than, equal to, or less than a specified value.
- **Cycle Time**
  Generates the alert when the file cycle time (for files having a specific extension) is greater than, equal to, or less than a specified value.
- **Changed**
  Generates the alert when files within the folder (having a specific extension) change or have not changed for a specified time period
- **Added/Removed**
  Generates the alert when files with the given extension are added or removed.

# Alert History

The **Alert History** shows a detailed list of alerts that have been detected by the system based on alerts that been configured within the system. The **# (pound sign)** in the **Alert History** column is unique for each alert detected while the **Alert ID** column is unique for each alert configured. Refer to **Configuring Alerts** for types of alerts and how to create/modify/delete them.

## Access Alert History

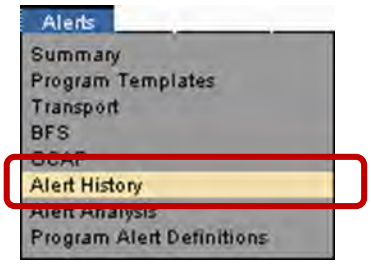



**Figure 260: Accessing Alert History**

For any program alert, you may click on any red area in the lower section. You will then be redirected to the **Detail** page for that specific alert.

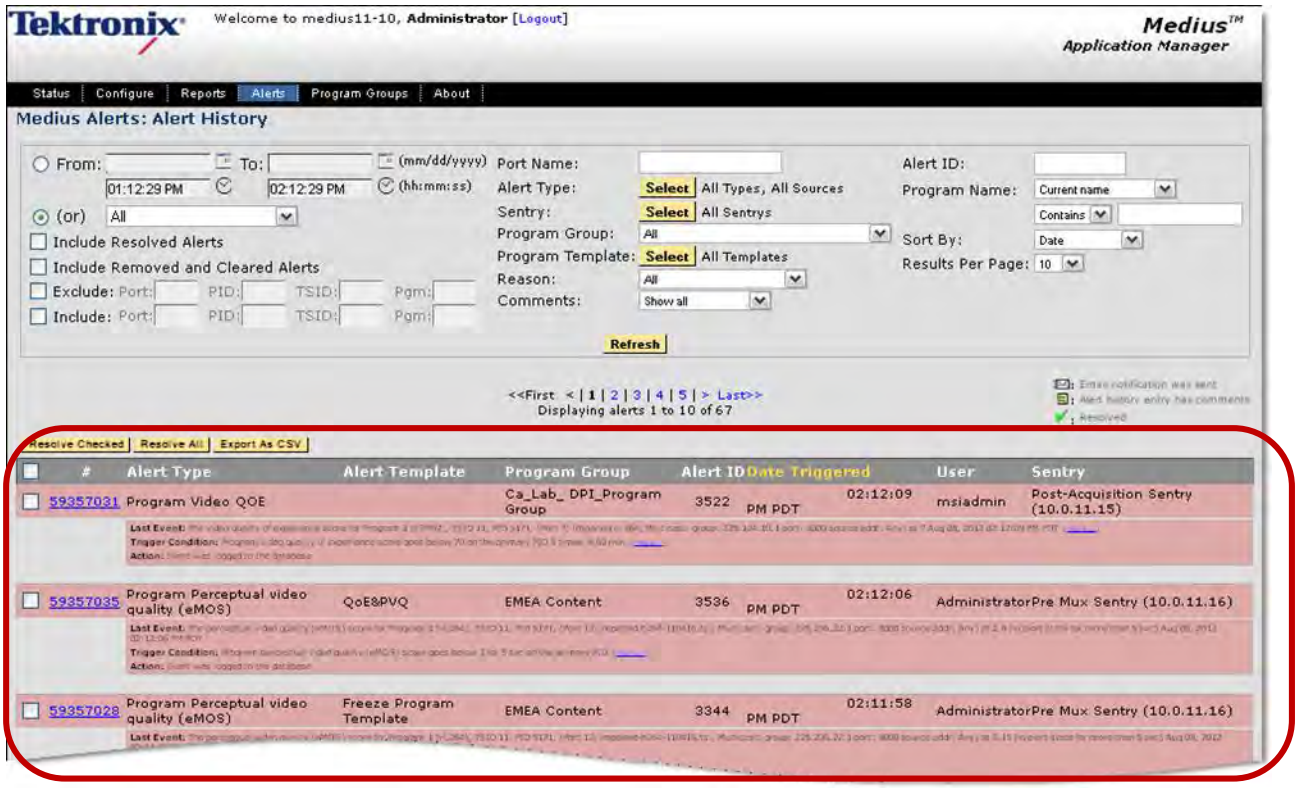



**Figure 261: Alert History**

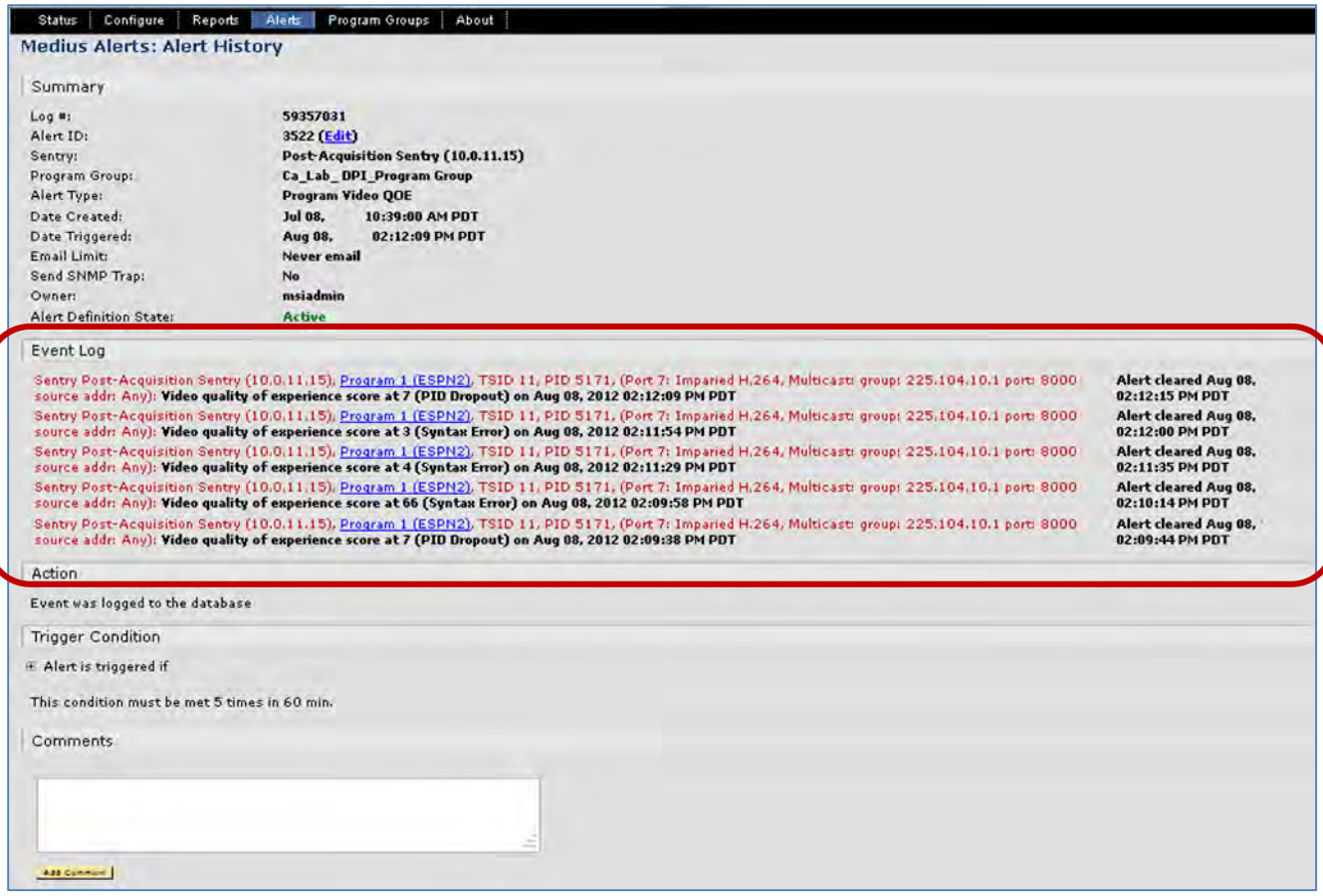



**Figure 262: Event History Log detail**

Deleted alerts will no longer be triggered while active alerts will continue to be triggered when their trigger conditions are met. If email notification was sent or the alert generated has comments attached to it (via the **Detailed Alert History**), then the log entry is tagged with the respective icon.

The entire list of alerts or individual items can be permanently deleted from the internal database by clicking **Resolve Checked** or **Resolve All**. The contents of the list can be filtered using the many filter options at the top of the **Alert History**, and only the filtered items will appear in the log.

# Report Export

**Report Export** allows you to export any report you have created to a comma separated value file which can be imported into a program such as MS Excel.

## Access Report Export

1. Select **Alert History** from the **Alerts** drop-down menu.

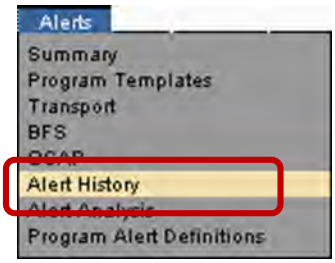



**Figure 263: Accessing Alert History**

## Export a file as a CSV

1. From the **Alert History** page, configure the report as needed. **Next**, select **Export As CSV.**

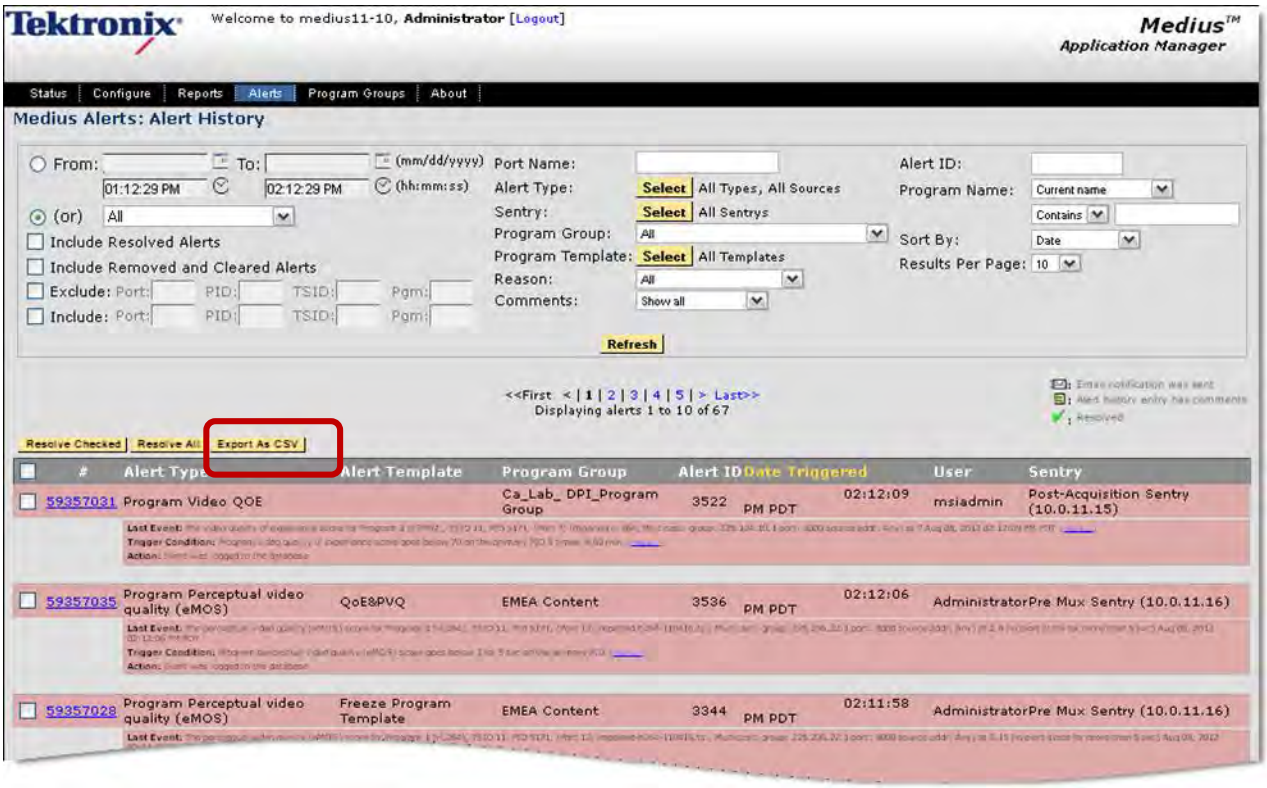



**Figure 264: Selecting a Report from the Alert History Page**

**NOTE*: Export to CSV function will export ONLY what is currently displayed on the alert history.***

2. If your report spans multiple pages, you will need to run an export per page.

3. You will then be prompted to select the program you wish to export to. Select the program (it will usually default to MS Excel) and select **OK**.

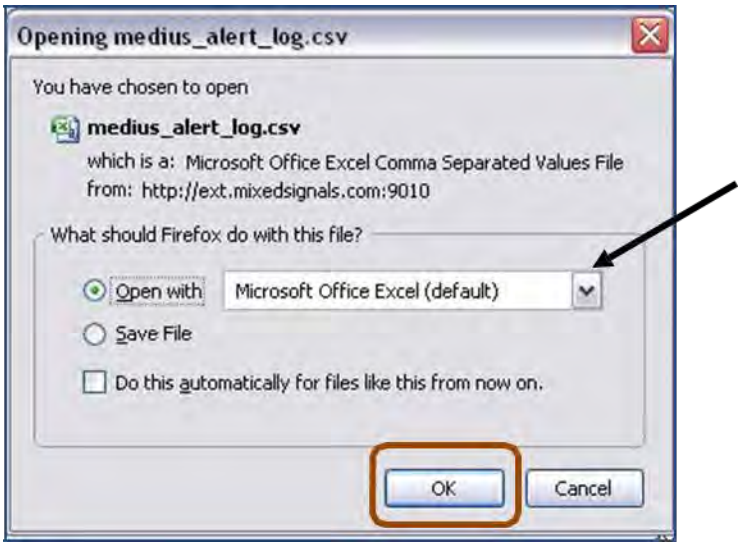



**Figure 265: The Export To dialog box**

4. The result of an export to MS Excel would look similar to the following:

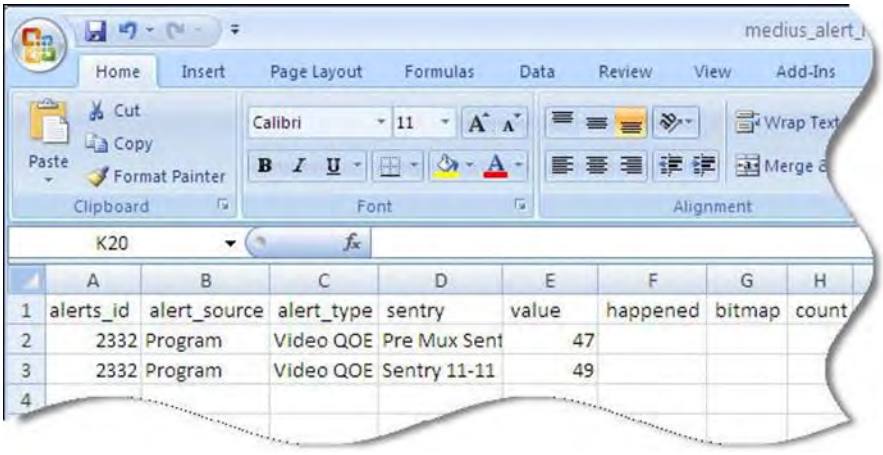



**Figure 266: A report exported to MS Excel**

# Alert Analysis

**Alert Analysis** provides an easy to use graphic analysis to visually represent alerts. These representations can be useful to track trends and to display a variety of information for any viewer, regardless of their technical experience.

## Access Alerts Analysis

Select **Alert Analysis** from the **Reports** drop-down menu.

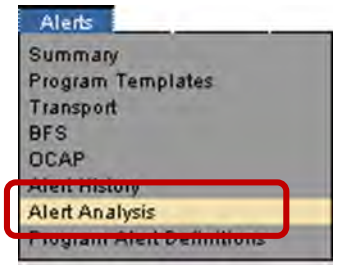



**Figure 267: Accessing Alert Analysis**

The summary screen consists of the following areas:

- **Report Navigation tabs** takes user to new reports.
- **New Report icons** allows user to select type for new report.
- **Existing Reports list** allows user to choose existing public and private reports.

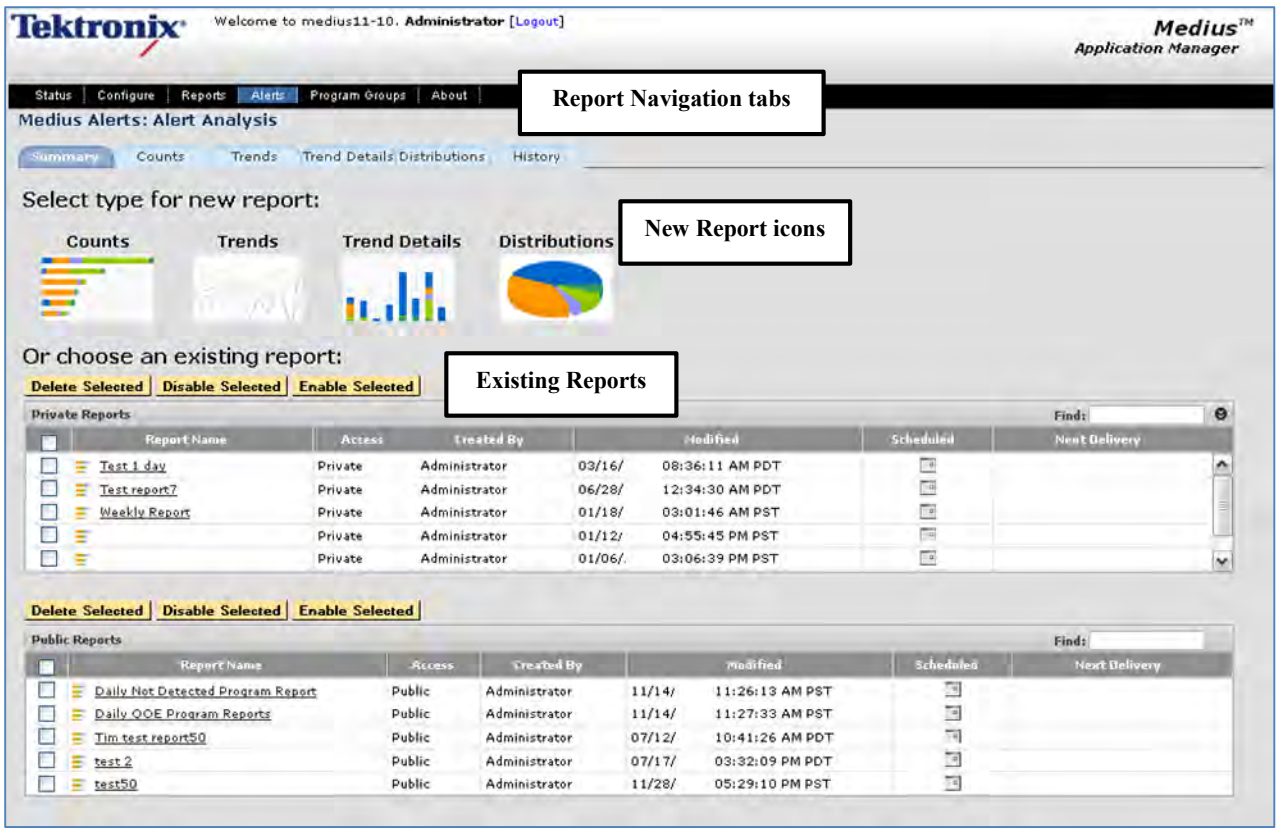



**Figure 268: Alert Analysis Screen**

### *Report Navigation tabs and New Report icons*

The **Report Navigation** tabs contain most of the same areas that the **New Report** icons do. Either may be used according to your preference.

- **Summary**
  Create a new report or view or modify an existing report
- **Counts**
  Shows the user a top 10 (20 or 30) count by port/program/program group for a given time period.
- **Trends**
  Totals the alert count over time for all or selected ports.
- **Trend Details**
  Allows user to create a more detailed **Trend** report.
- **Distribution**
  Creates a pie chart showing total alerts by type for a given time period
- **History**
  (Not included on the **New Report** icons) Selecting the **History** tab above the **New Report** icons will take the user to a history of what alerts were emailed and when.

## Counts tab

The **Counts** tab shows the user a top 10 (20 or 30) count by port/program/program group for a given time period.

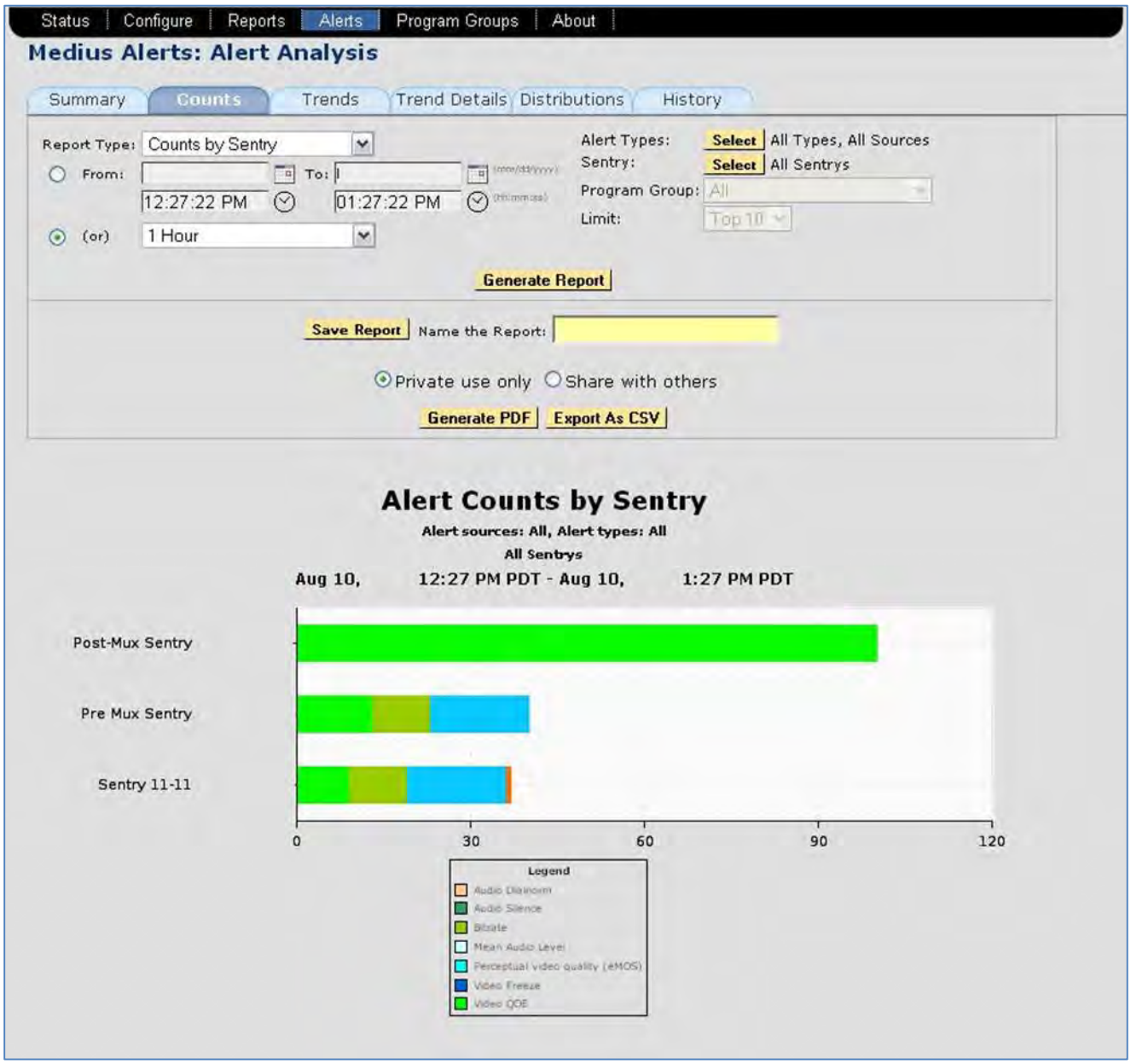



**Figure 269: Counts Tab**

### How to create a sample Counts report

This function allows you to set your counts to count by program for specified time frame. Selecting **Top 10** will generate the top 10 alert counts by program.

This is used to see what your problem channels are.

1. Set **Report Type** to **Count's by Program**.
2. Set the dates for a one week period.
3. Set **Alert Type** to one of the following: all alerts port/all program group/all limit top 10.
4. Select **Generate Report**.

---

**NOTE***: The bottom of the report is a tabular view of the programs in chart form. Click on the link to go to the specified time period for that particular Program Detail Report.*

---

### Saving a report

Once you have a report the way you like it, save it so that you can run it again without having to reconfigure it. If you make it public, others users will be able to use it as well. Selecting **Private** will make it only viewable for your specific login.

You can also set it to email you automatically.

1. Name the **Report**.
2. Select either **Private/Share** with others.
3. Select **Save** report.
4. Select **OK**.

## Schedule a Report

You can schedule a report to run automatically and email a PDF of the results.

1. Select the **Schedule** button that appears after the report has been saved.

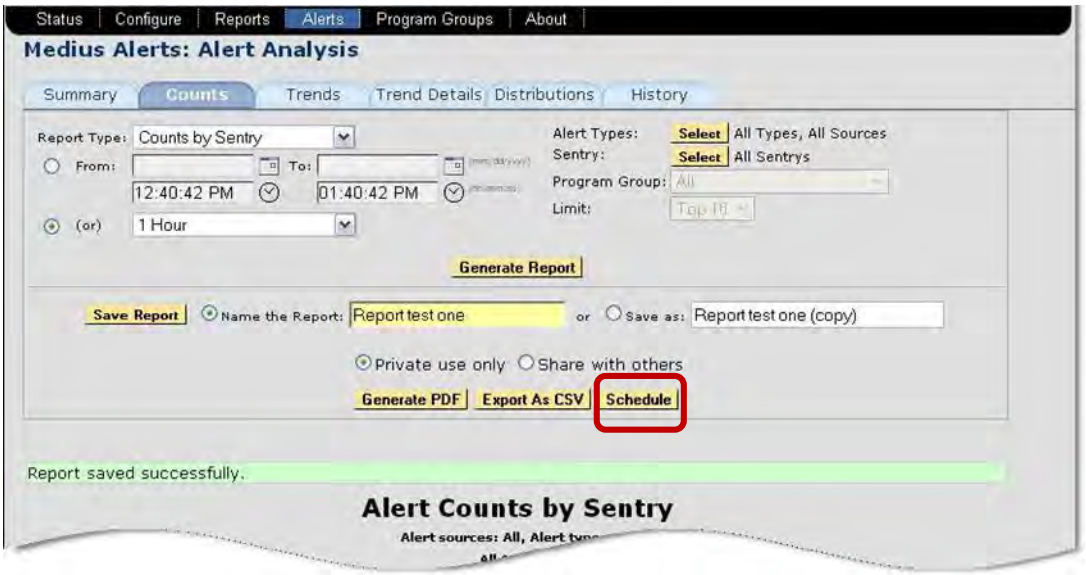



**Figure 270: Selecting Schedule**

2. The **Scheduling** options page will automatically load.

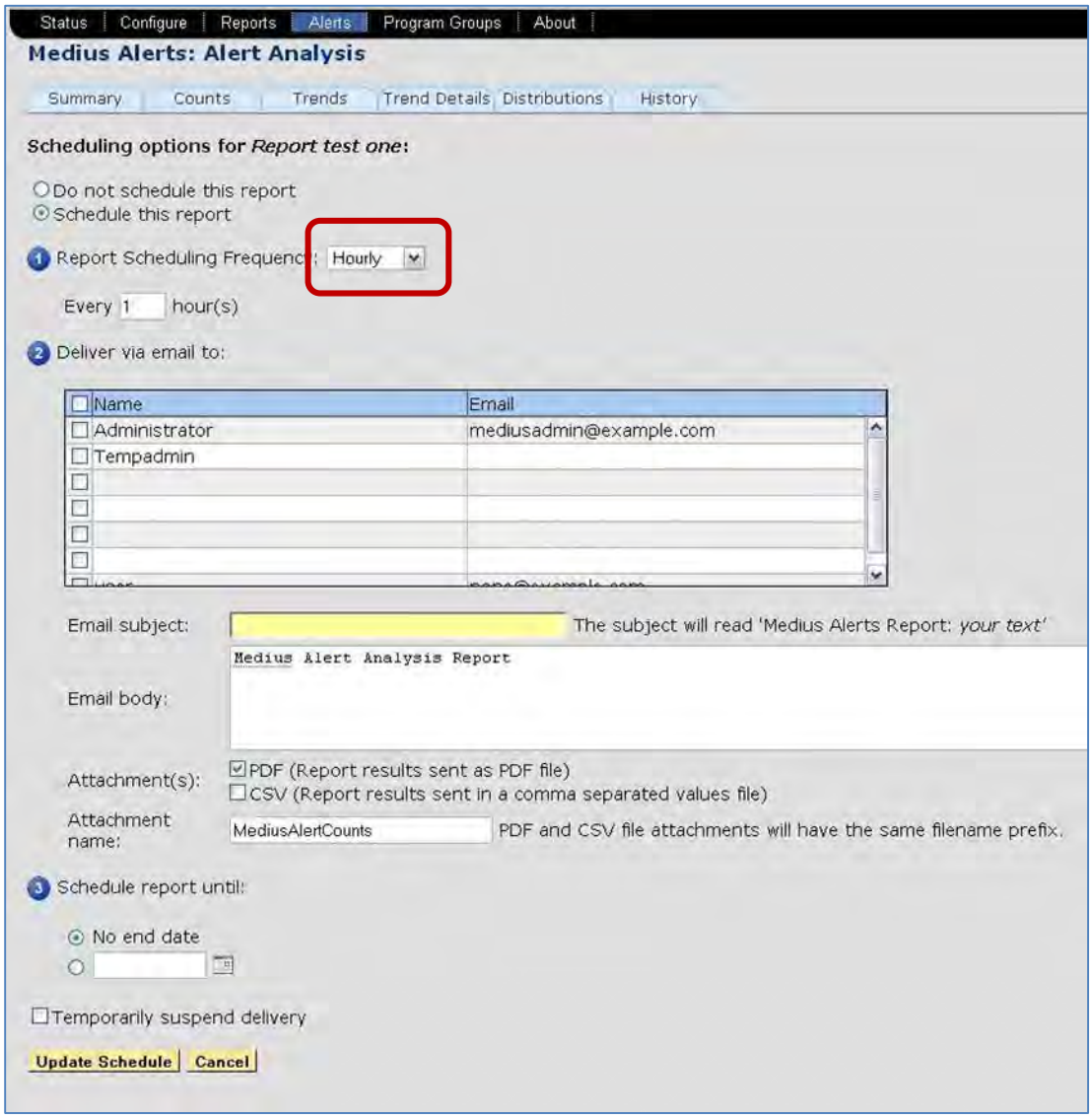



**Figure 271: Scheduling Options page**

3. **Section** 1: Select the **Frequency**.

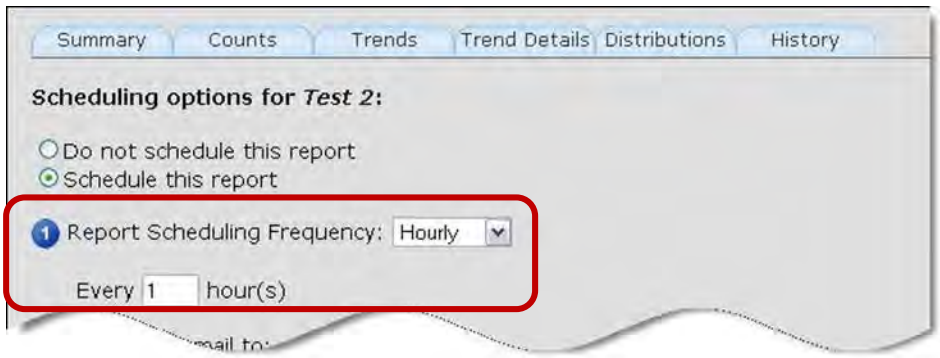



**Figure 272: Select the Frequency**

4. Section 2: Select recipients and format the email (Subject, Email body, etc.)

5. Select whether you want Medius to attach the report as a **PDF** or **CSV** file.

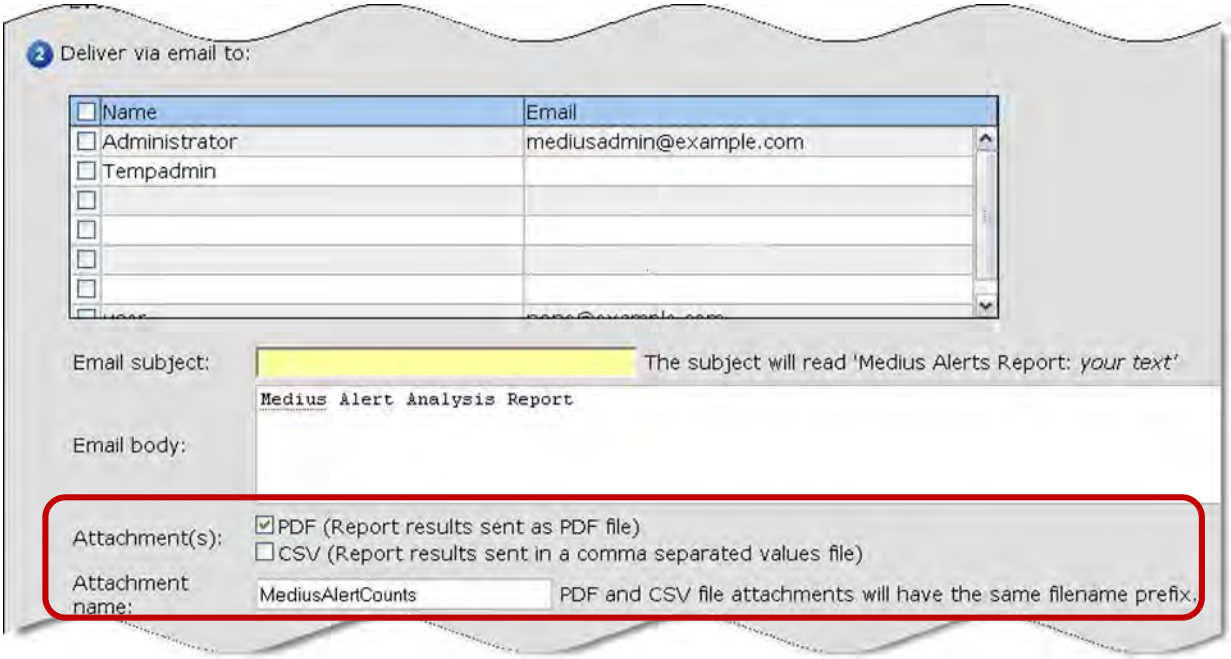



**Figure 273: Section 2-Email Settings**

6. Section 3 Schedule the delivery termination

7. You may set it to only email you one time, every time or to end on a particular date.

8. You may also temporarily suspend delivery (for vacations, etc)


**Figure 274: Update Schedule**

9. Select **Update Schedule.**

## Trends tab

The **Trends** tab totals the alert count over time for all or selected ports. This report will generate a line graph of the number alerts for a time period per port.

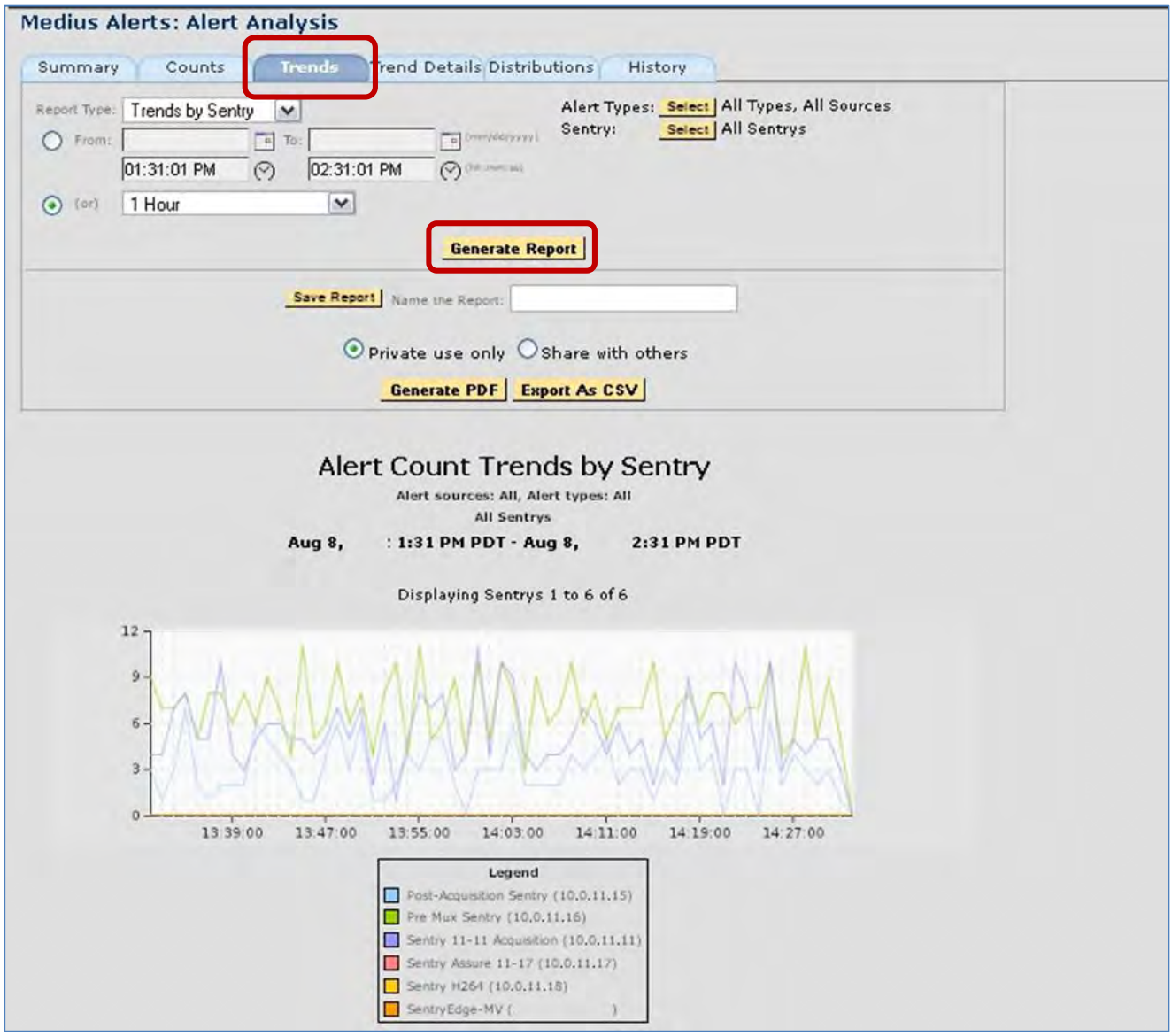



**Figure 275: Trends tab options**

### *Set a Trends report*

1. Choose time frame for the report.
2. Select alert types you wish to view.
3. Select which Sentry/Sentrys you wish to view.
4. Select **Generate Report**.

## Trend Details tab

**Trend Details** allows you to create an expanded **Trend** report. This is a handy report to run if you want to further investigate something from the **Trend** report.

1. Select **Trend Details**.

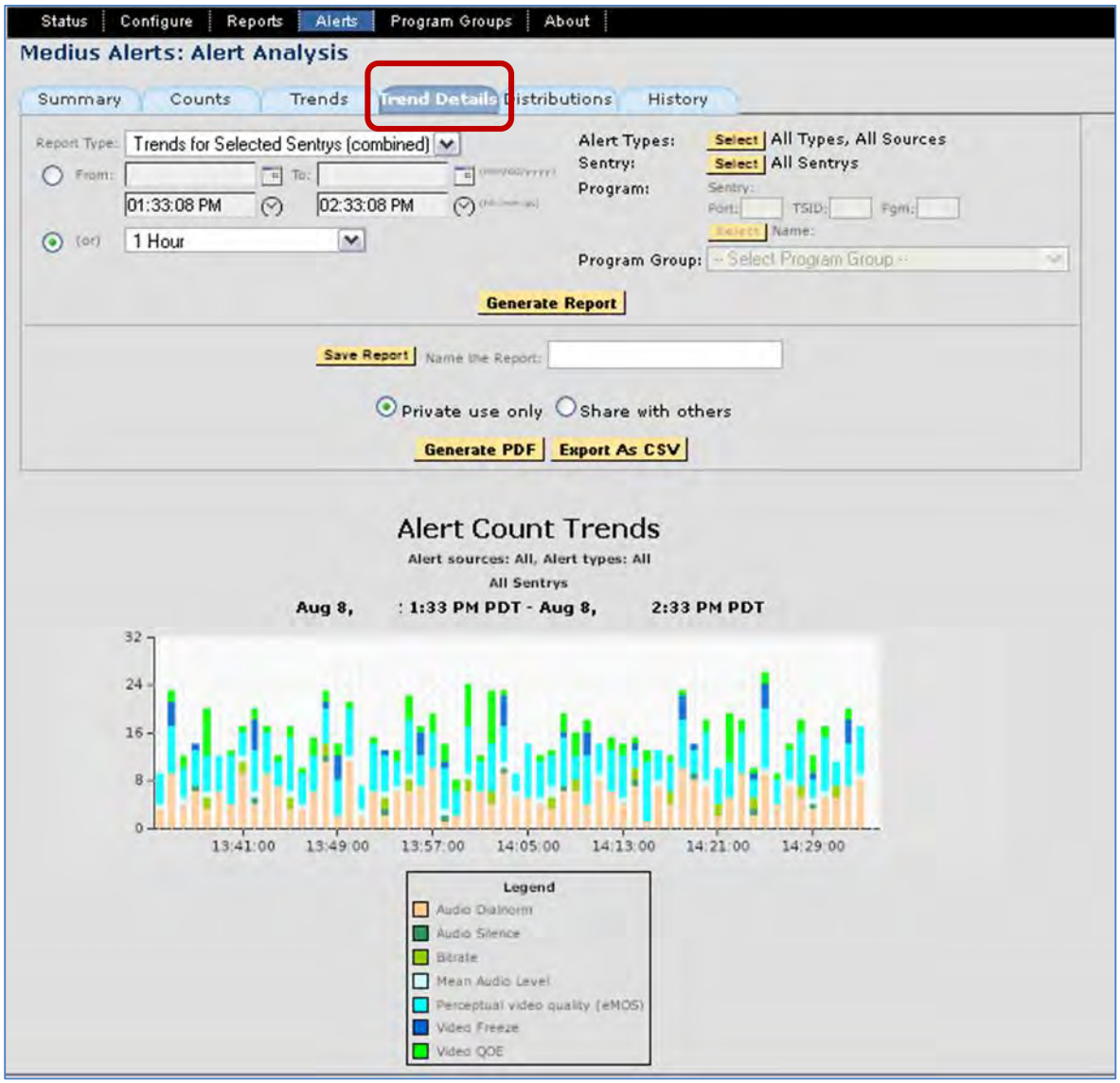



**Figure 276: Trend Details options**

2. Select the **Report** type (ex. **Trends for Selected Sentrys**(combined)) from the drop-down menu.
3. Set the time period.
4. Select the **Alert Type**.
5. Depending on the report type you need, select which Sentry/Sentrys program you wish to view.
6. Select **Generate Report**.

## Distributions tab

**Distributions** will give you a pie chart graphic that shows the break out of all the different types of alerts.

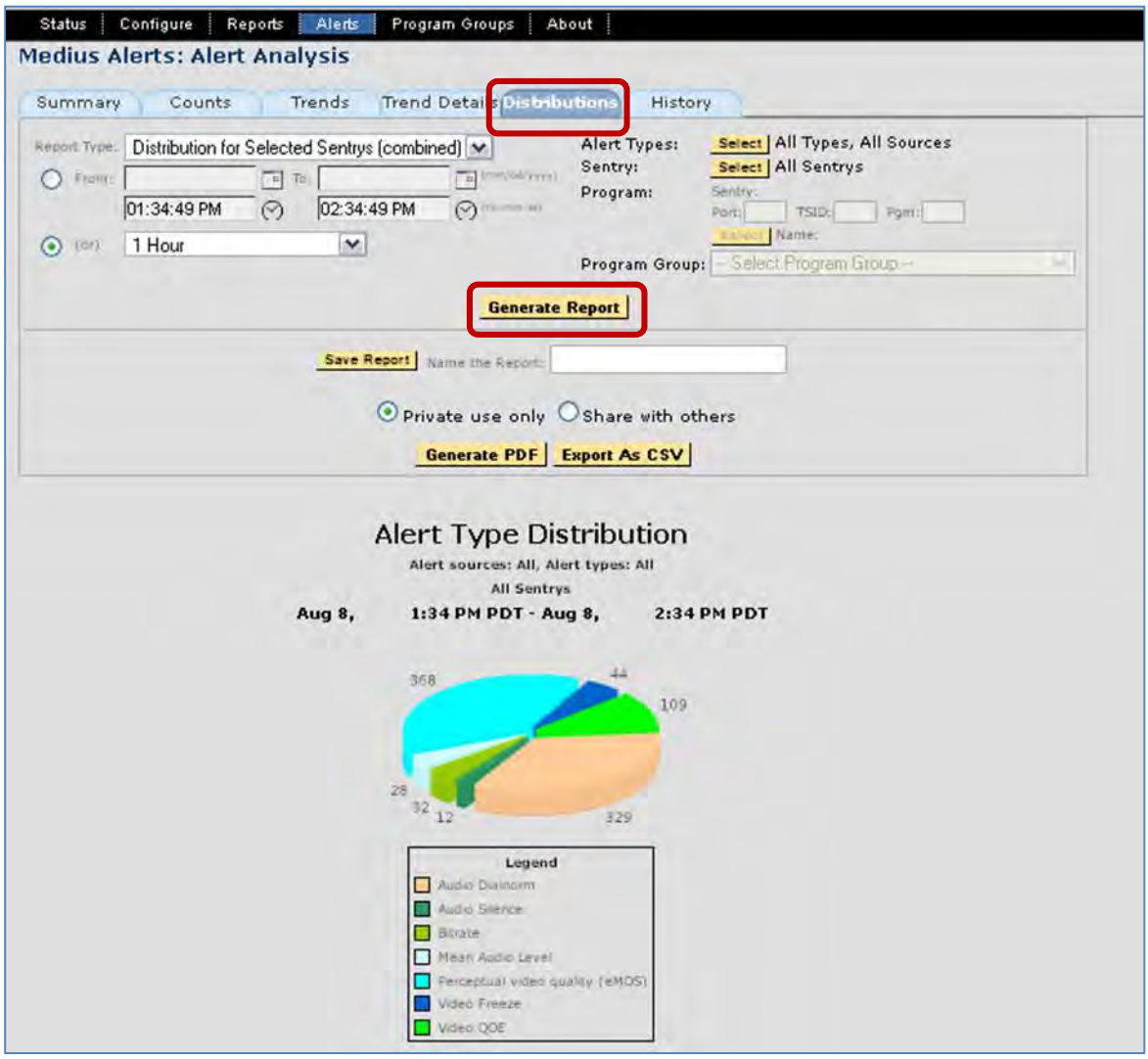



**Figure 277: The Distributions tab**

Use this to see a distribution summary of all of your alerts for a given time period. This could be handy to know what percentage of all your alerts are of a certain type.

1. Select the **Report Type**.
2. Select the required time period.
3. Select **Alert Type**.
4. Depending on the report type you need, select which Sentry/Sentrys program you wish to view.
5. Select **Generate Report**.

## History tab

The **History** tab allows the user to see a schedule of reports that have been mailed. It is primarily used to see who is receiving which reports and when they are receiving them.

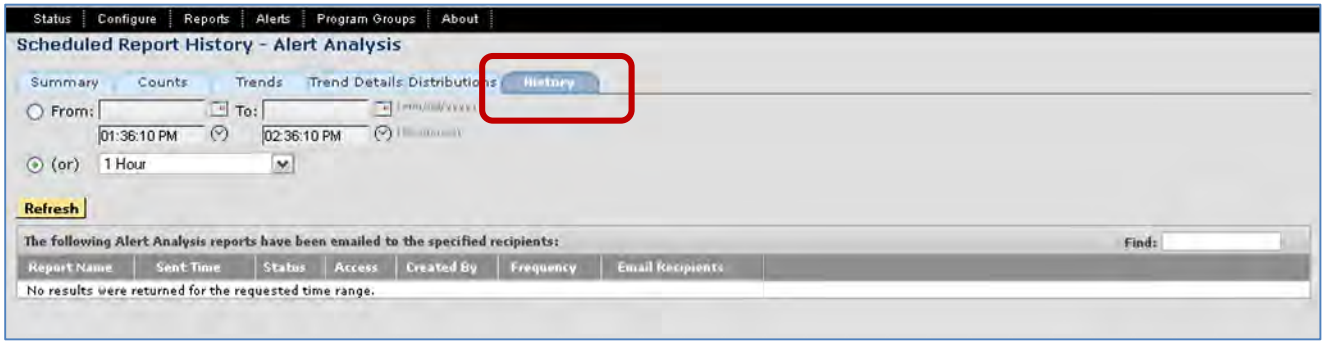



**Figure 232: History tab**

1. Select the time range of the reports you wish to see.
2. Select **Refresh**.

# Program Alert Definitions Report

The **Program Alert Definitions Report** helps you monitor which alerts are set for each individual program. This report is useful in finding programs that have no alerts. Reports can be configured and saved based on various parameters and these reports can be scheduled for email delivers as CVS files.

## Access Program Alert Definitions Reports

From the main menu, select **Alerts** and then **Program Alert Definitions Report.**

Any saved reports will be visible.

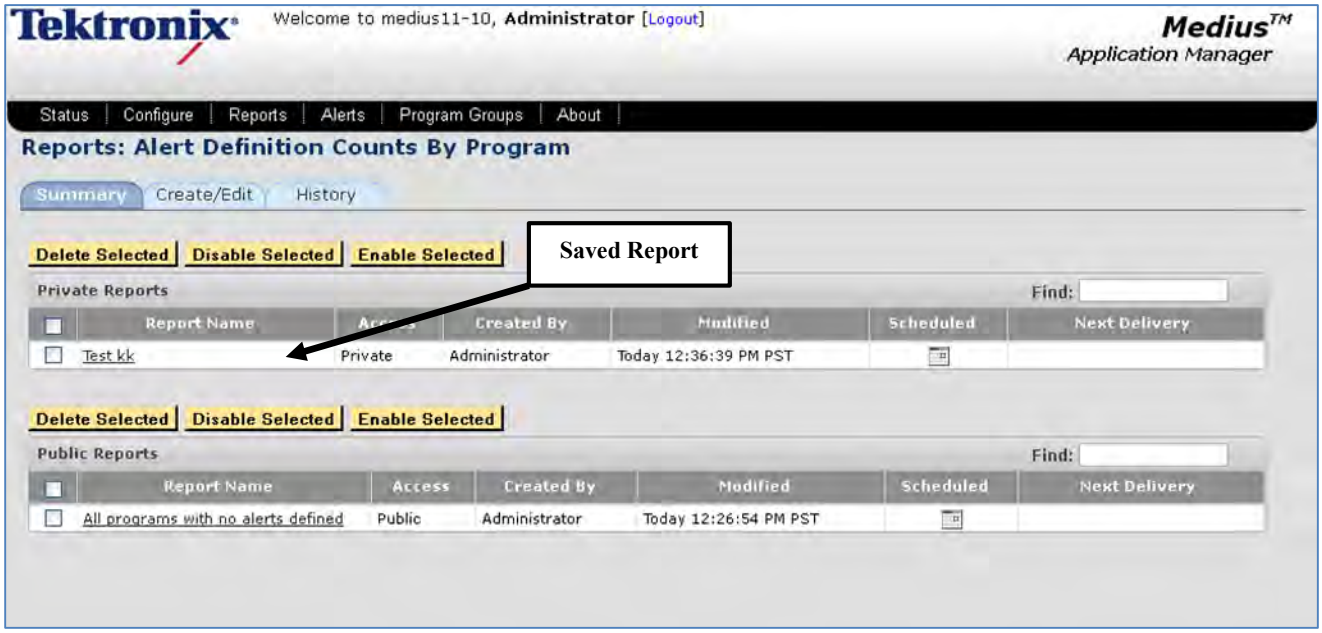



**Figure 278: Summary tab**

## Create an Alert Definition Counts By Program report

1. Select the **Create/Edit** tab.

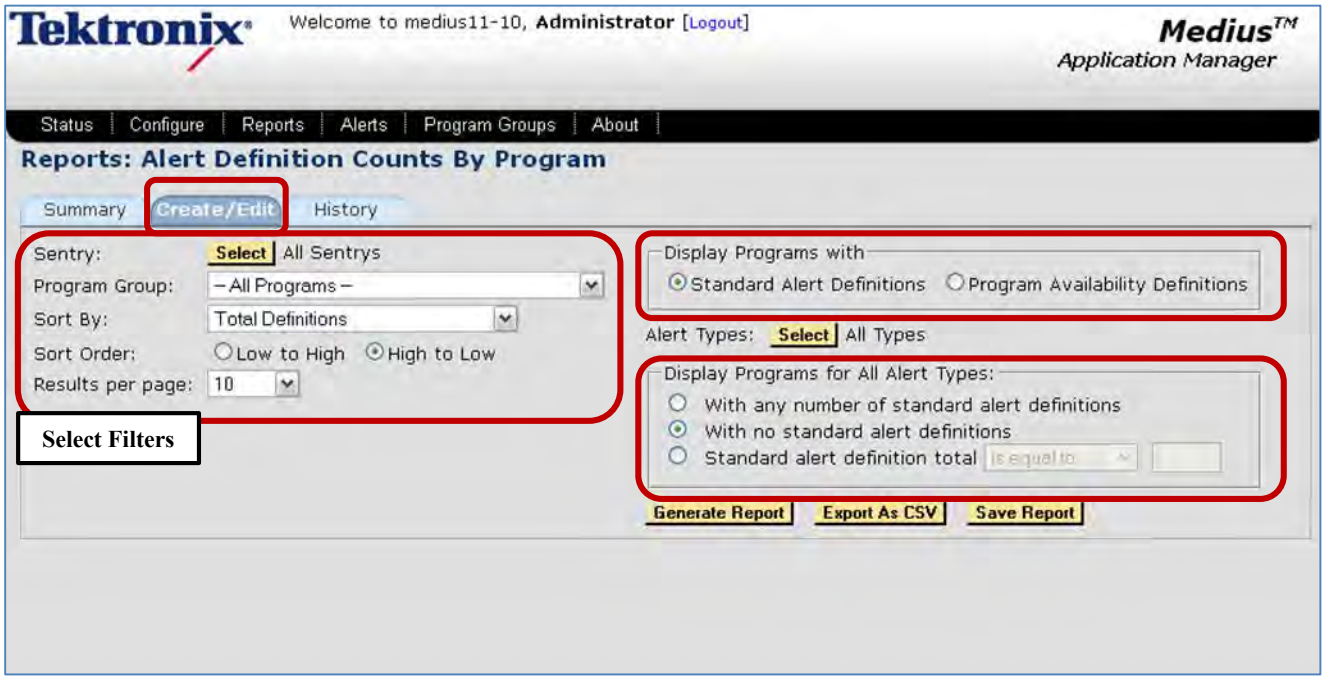



**Figure 279: Create/Edit tab**

2. Select filters as needed

3. Select what kind of programs you want to be displayed.
   - Select **Standard Alert Definitions** if you are looking for programs that do or do not have standard definitions. A standard alert definition is an alert that would notify you if there was an issue with the service.
   - Select **Program Availability Definitions** to determine the uptime of a program.

4. Next, set the **Display Programs for All Alert Types.** In this example, select **With No standard alert definitions**.

5. Select **Generate Report.**

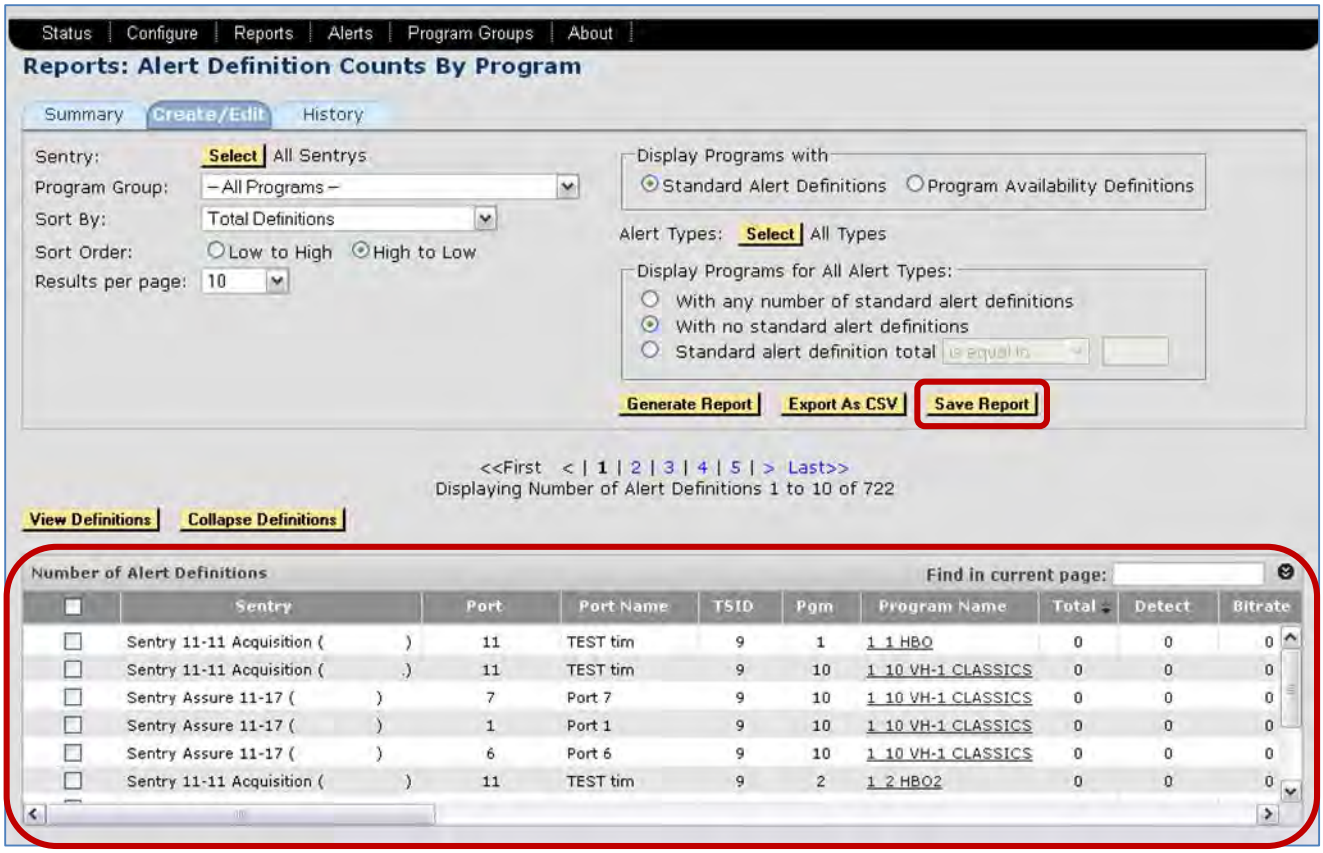



**Figure 280: The final report**

6. Select **Save Report** if you want to use it again.

# Program Groups

**Program Groups** allows you to work within existing groups and create new groups. You may:

- **Edit Group**
  Change or remove programs from the group
- **Rename Group**
  Renames the program group name
- **Delete Group**
  Deletes the **Program** group
- **Create alert**
  Creates an alert for the **Program** group.

---

**NOTE***: Medius Program Groups are completely independent from the Program Groups in Sentry.*

---

## Access Program Groups

1. Select **Manage Program Groups** from the **Program Groups** drop-down menu.


**Figure 281: Accessing Manage Program Groups**

2. From the **Program Groups Summary** page, expand the program group you wish to work with.


**Figure 282: Manage Program Groups Summary page**

3. Next, select the function you wish to perform. You may **Create**, **Edit**, **Rename** or **Delete** a group, as well as **Create an Alert** for a group.

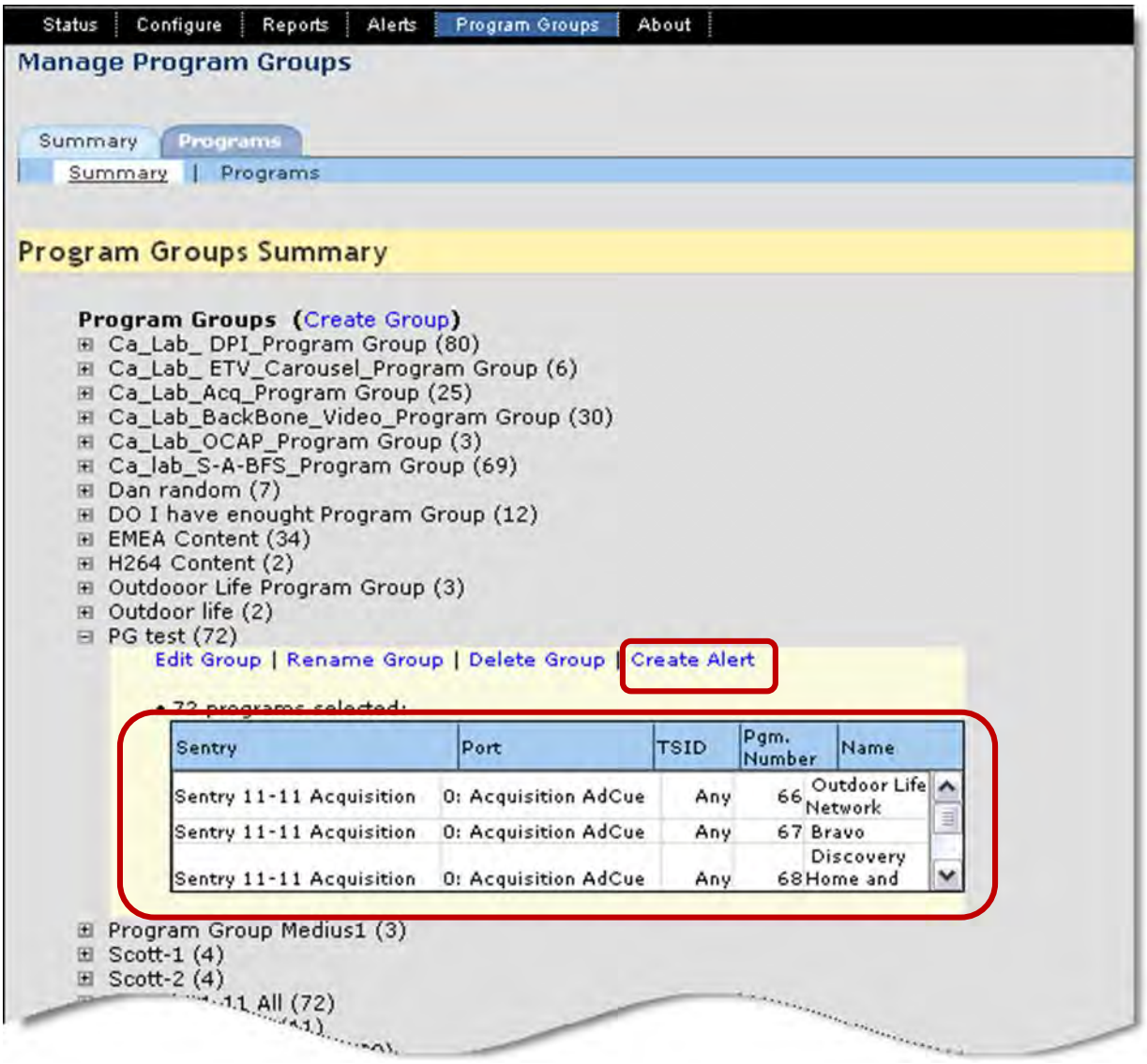



**Figure 283: Manage Program Groups Summary page (expanded view with editing options)**

## Create a program group

1. Select **Create Group** from the **Program Group** sub-menu.

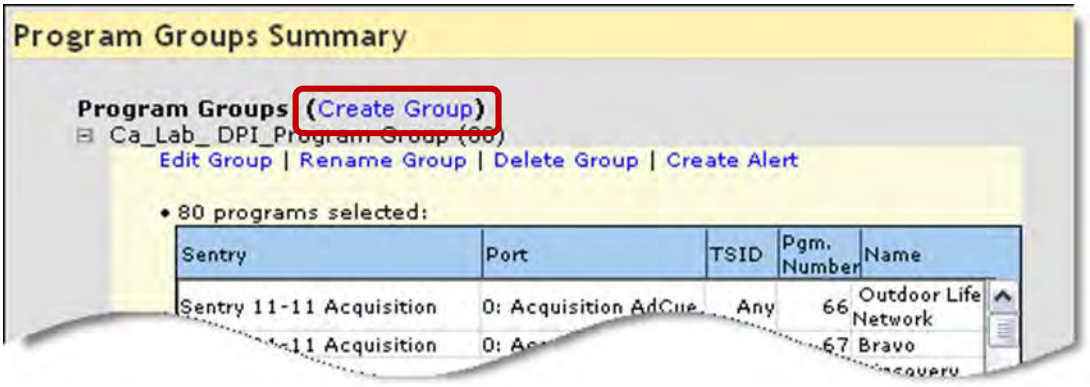



**Figure 284: Create a group**

2. From **Section 1**, select your Sentry and/or **Port** from the drop-down menu.

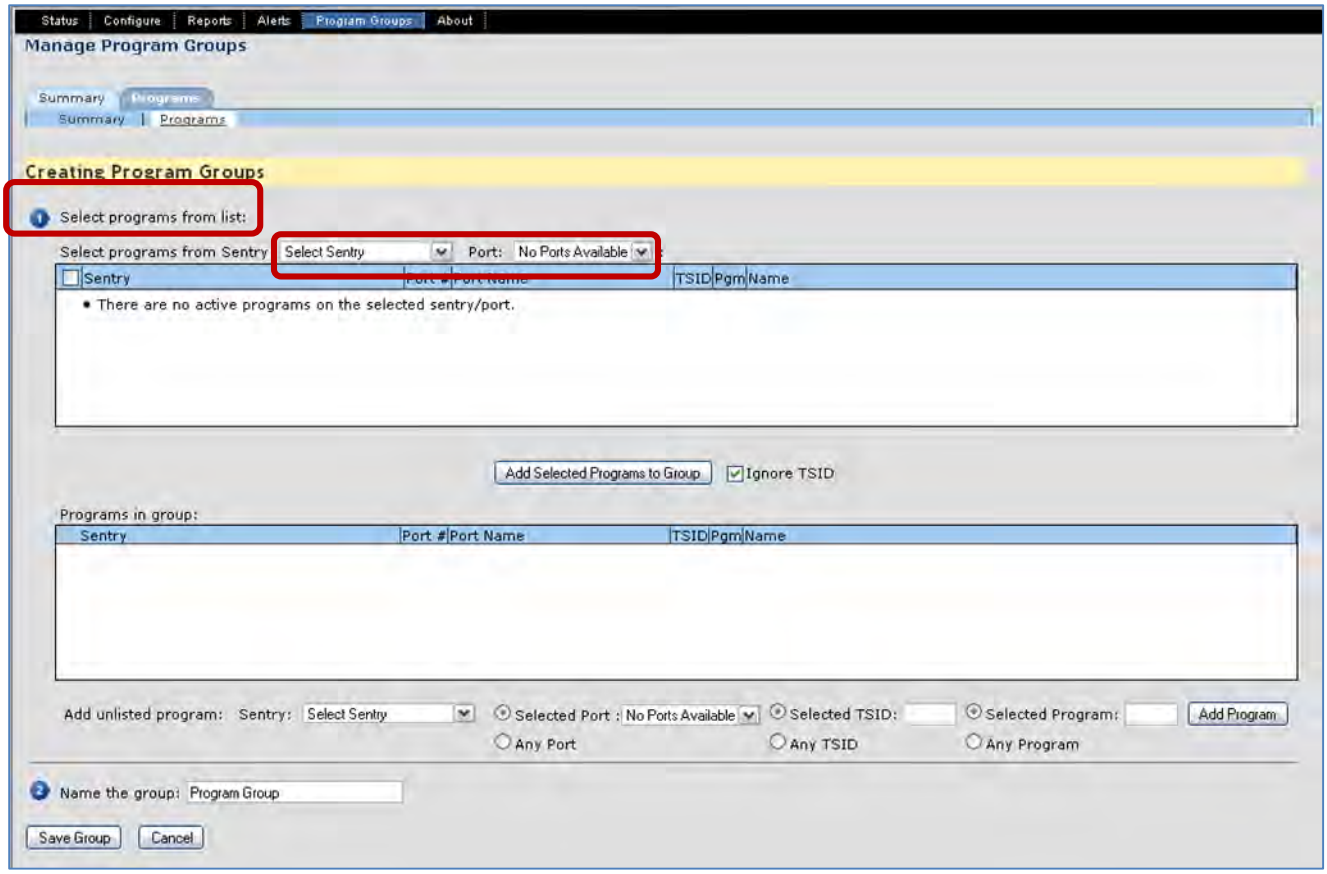



**Figure 285: Create a Program Group Step 1 (selecting Sentry and Ports)**

3. The **Programs** will automatically load.

4. Select the **Programs** you wish to add to the group by checking the appropriate box.

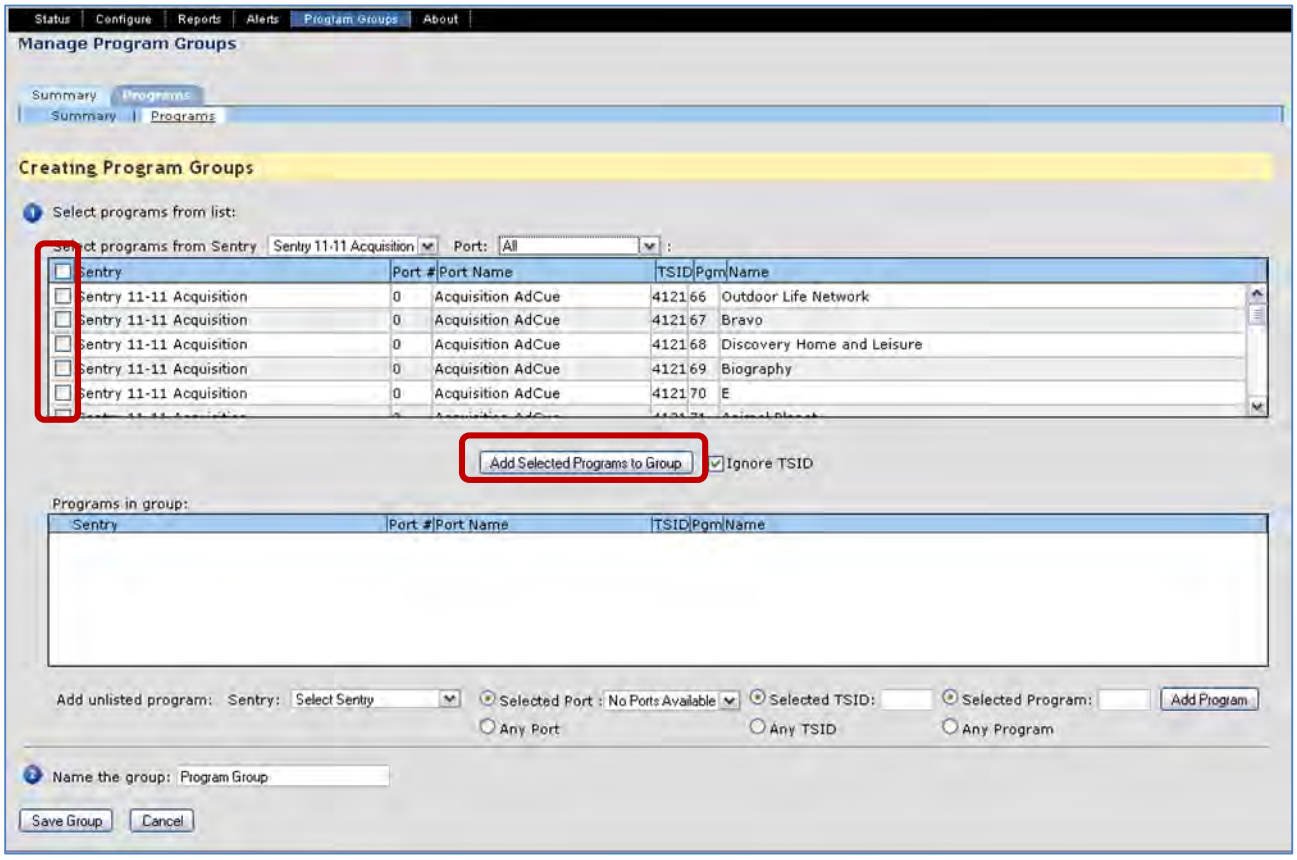



**Figure 286: Create a Program Group Step 1 (selecting programs)**

5. When you have finished selecting programs, and click **Add Selected Programs to Group**.

6. The **Programs** you select will then be added to the **Programs** in group box.

7. Repeat steps 2 through 5 if you want to add programs from other Sentrys to the program group.

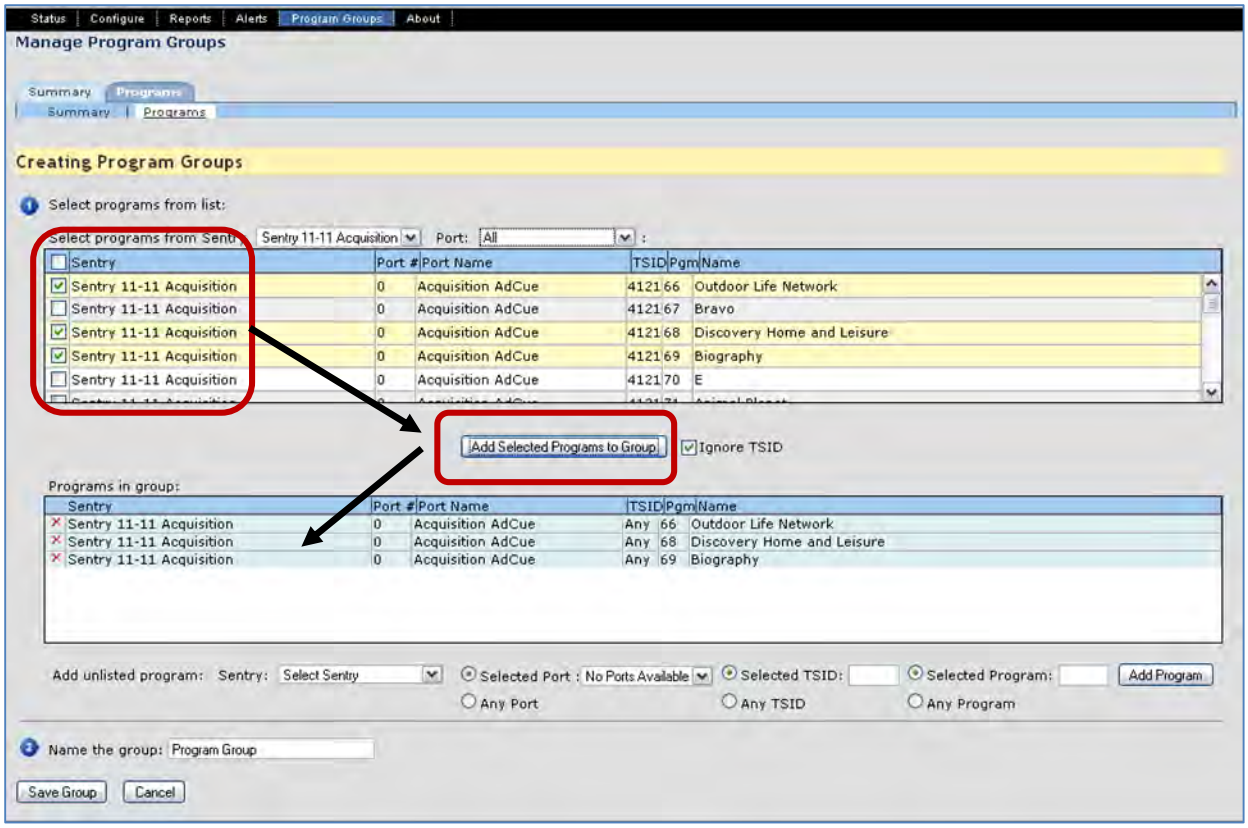



**Figure 287: Create a Program Group Step 1 (adding selected programs to groups)**

8. In **Section 2**, add the group name to the **Name** the group field and then select **Save Group**.

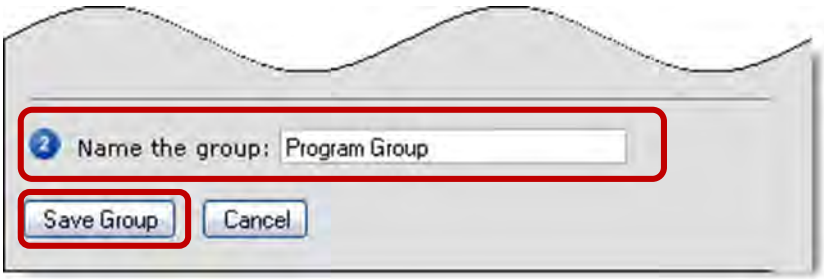



**Figure 288: Name new group**

9. Select **Ok** on the confirmation box to return to the **Program Groups** screen.


**Figure 289: Group Saved notification**

10. Your new group will now appear on the summary list.


**Figure 290: New group as it appears on Program Groups Summary page**

## Edit Program Groups

1. From **Program Groups** menu, select **Edit** for the group you wish to modify.

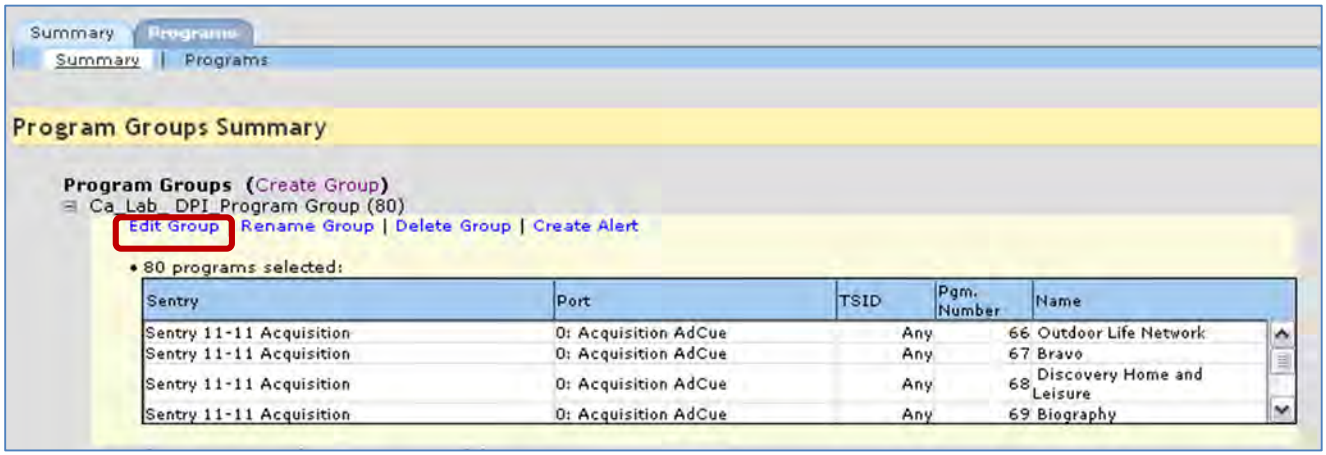



**Figure 291: Edit Group**

2. In **Section 1** select the Sentry you wish to edit.

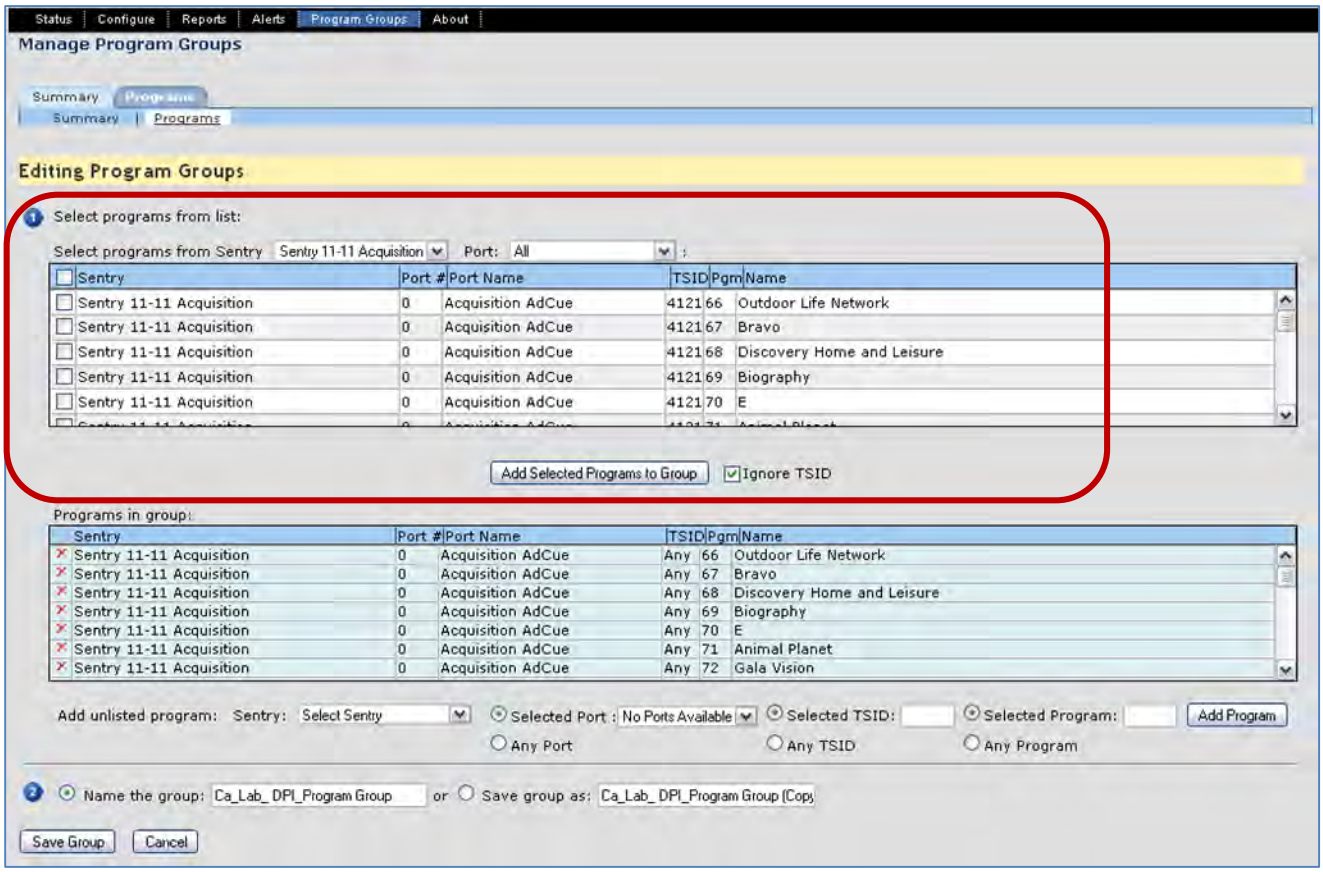



**Figure 292: Edit Program Groups Step 1 (select programs)**

3. Select the programs you wish to add and then select **Add Selected Programs to Group**. The selected groups will be added to the **Programs** in group box.

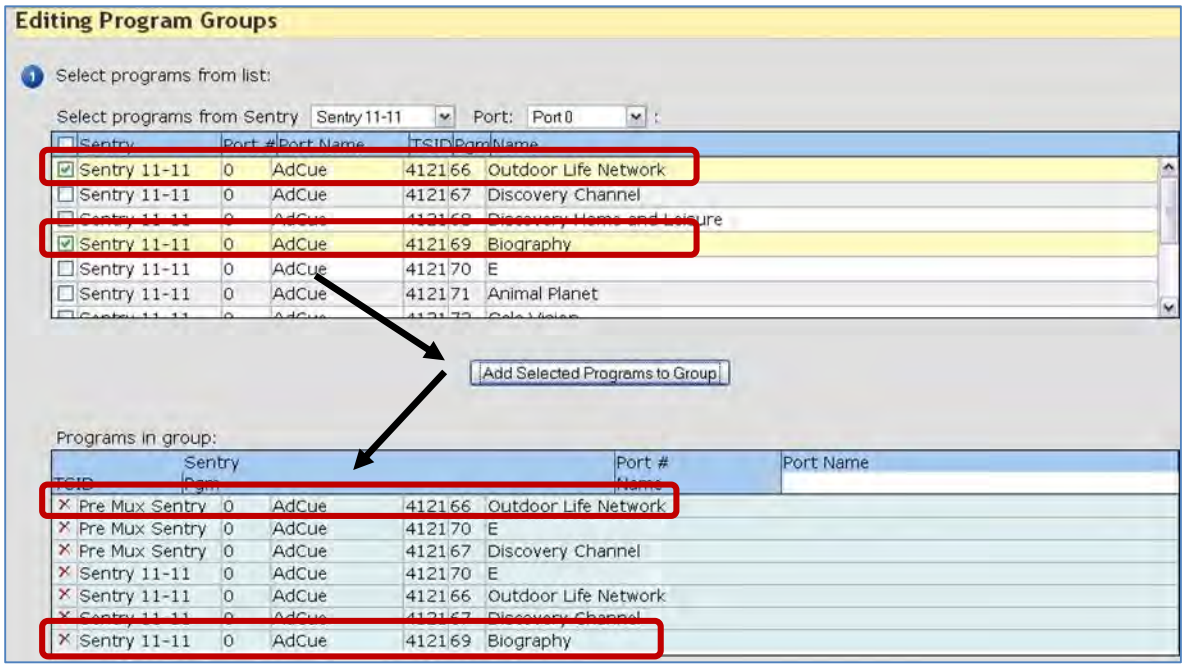



**Figure 293: Edit Program Groups Step 1 (add programs to a group)**

4. To remove any programs from the group, click on the red X next to the program in the **Programs** in group box.

5. You may save the group under a new name (**Name the Group**) or save the group under the existing name (**Save Group as**).


**Figure 294: Name the Program Group or save to an existing name**

6. Select **Save Group** to finish.

## Delete a Group

1. Select **Delete Group** from the sub menu of the group you wish to remove.

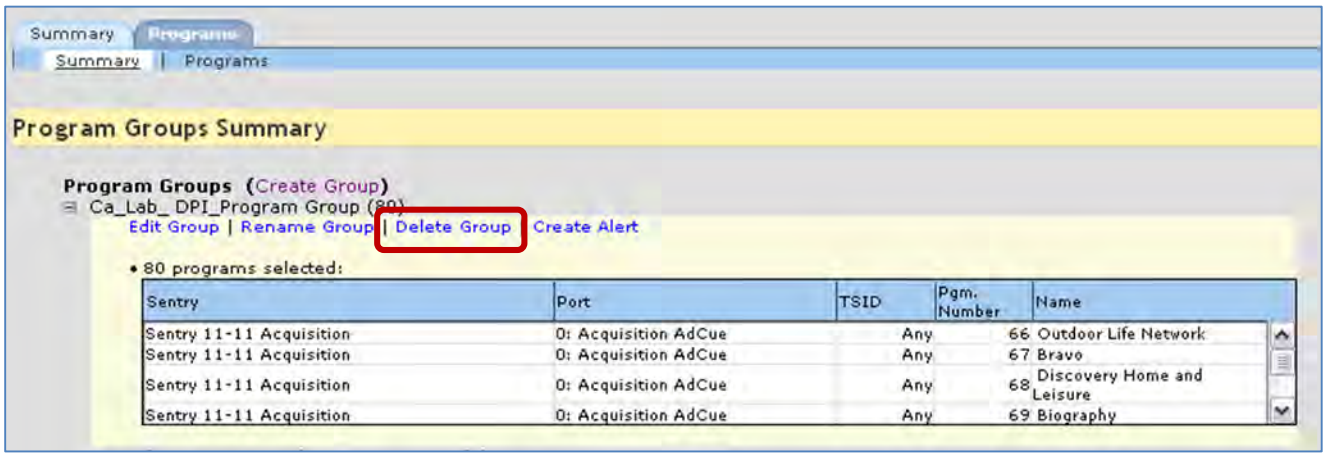



**Figure 295: Delete a group**

2. The resulting warning indicates that all alerts and alert analysis reports for that group will also be deleted.


**Figure 296: Delete Program Group warning**

3. Select **Delete** to continue or **Cancel** to abort.

## Create an Alert

This is the same information as found in the **Creating Alerts** section.

1. Select **Create** from the **Program Alerts** section.

2. After selecting the **Program Type**, the information for **Section 1** will automatically populate.

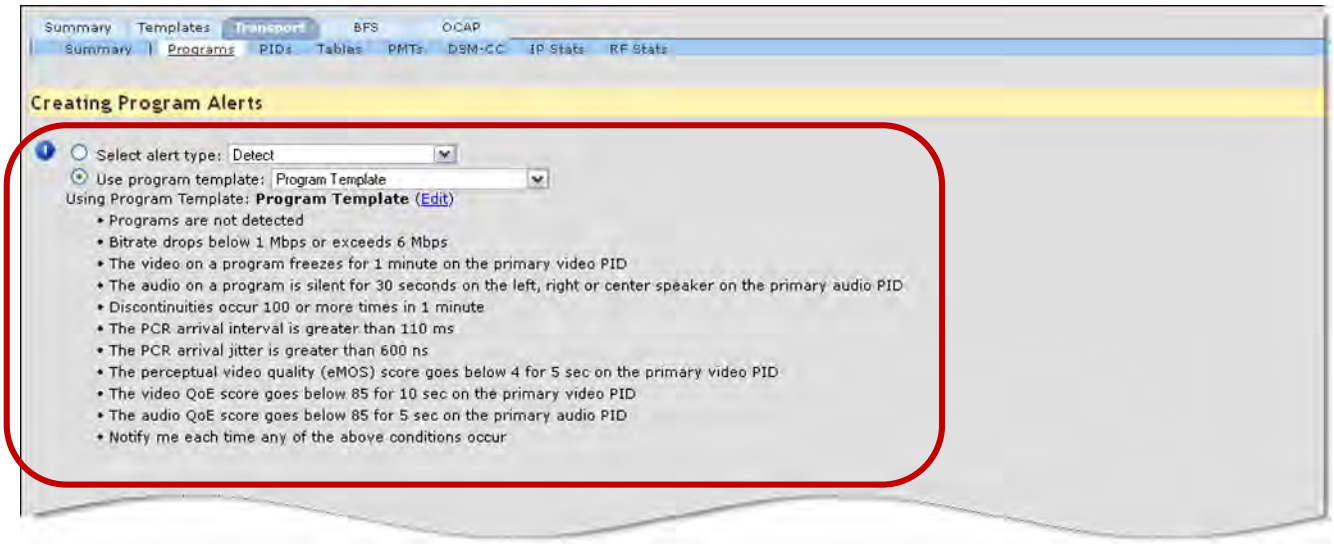



**Figure 297: Create an alert (Section 1)**

3. In **Section 2** select the Program Group and individual Sentry.

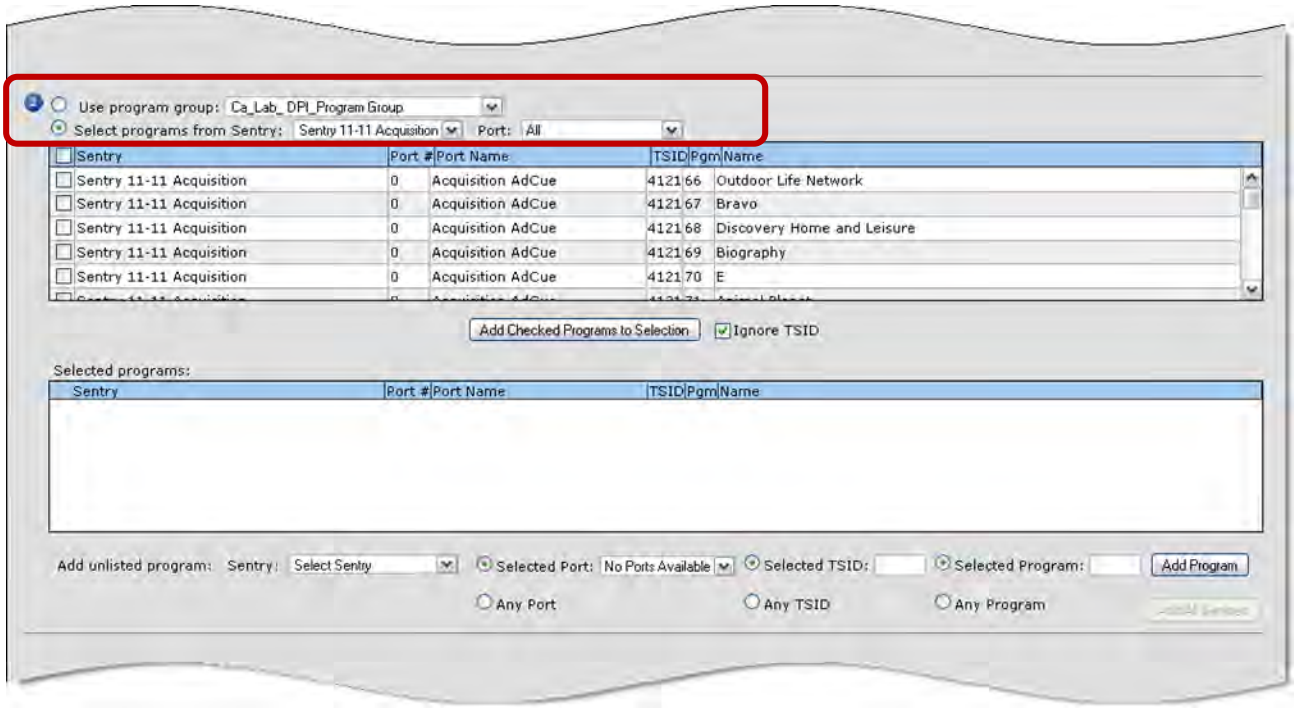



**Figure 298: Selecting a program group (Section 2)**

4. The **Program** section will automatically populate.

5. For **Section 3**, select the notification email information for when the alert is generated.

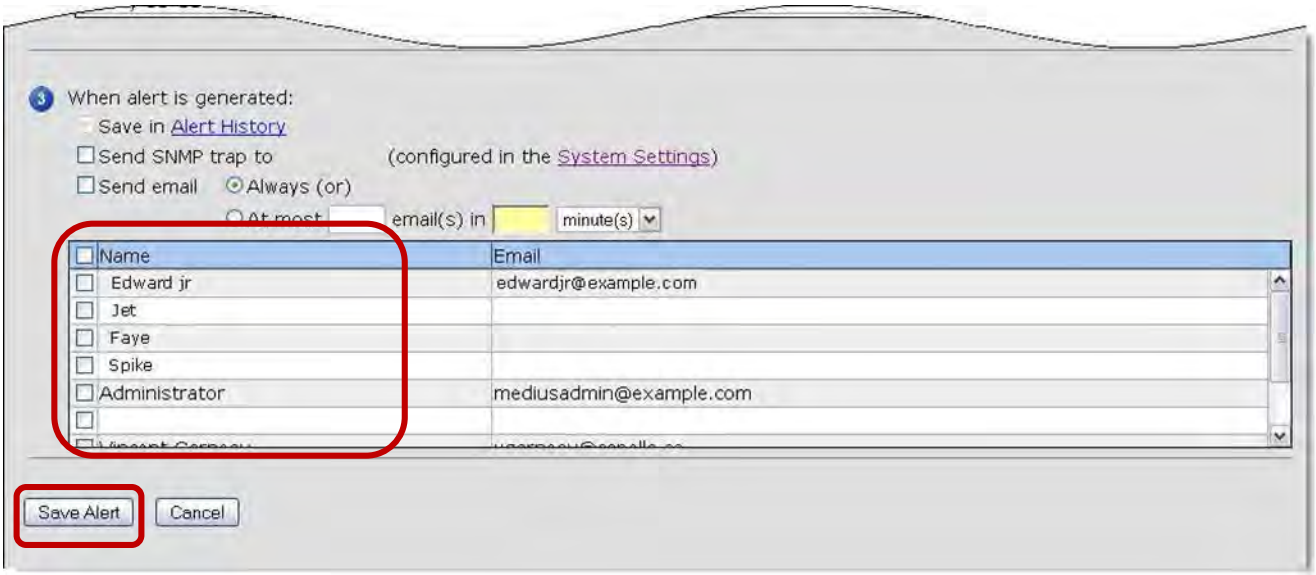



**Figure 299: Selecting notification emails and Saving Alert (Section 3)**

6. Select **Save Alert** when finished.

# About

## For Medius

The **About** menu gives you the option to view information about the identity of the Medius and the Sentrys assigned to it.


**Figure 300: About Medius**

## For Sentry

The **About Sentry** page shows you more information, including **Version**, and **Licensed Modules**. This is helpful for determining when your system upgrade license expires.

1. Select **View** next to the Sentry you wish to look at.

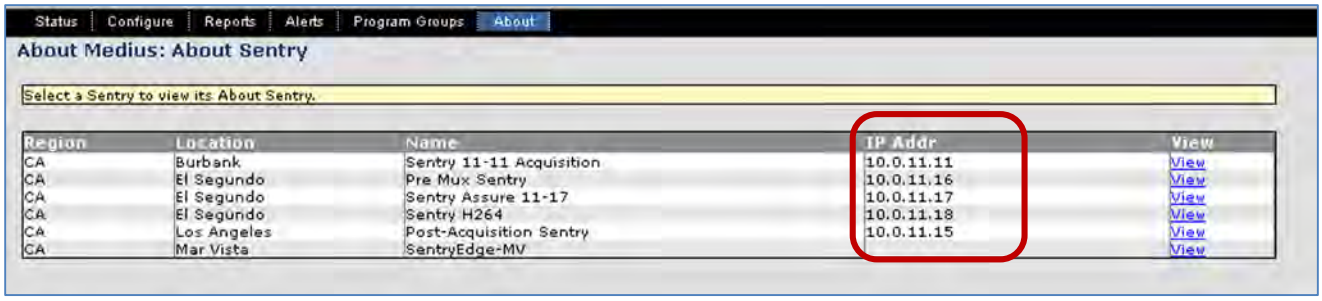



**Figure 301: About Sentry**

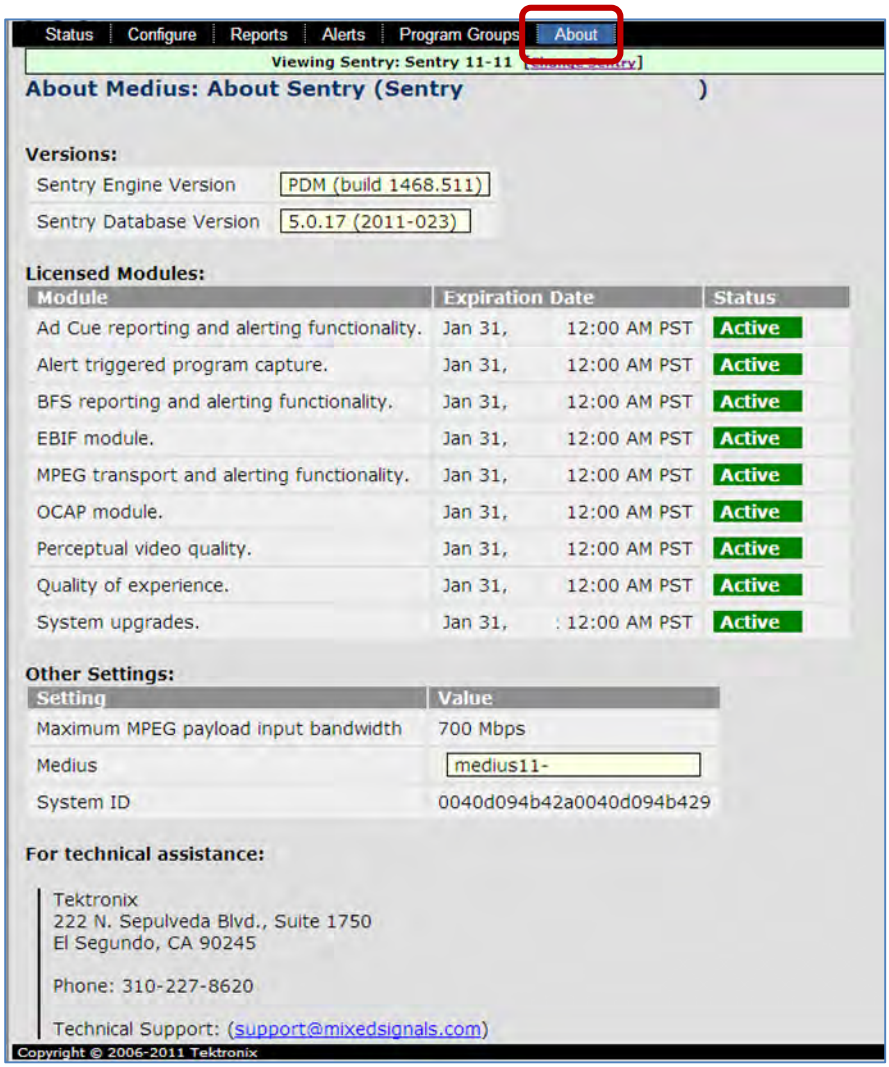



**Figure 302: About information for an Individual Sentry Unit**

# Medius and Sentry Specifications

**Supporting protocol:**

1. Video—MPEG-2, H.264 and VC-1
2. Audio—Dolby AC-3 (5.1 surround), MPEG-1 layer II (mono, stereo), H.264 AAC
3. Carousel—OCAP, BFS, MHP/DSM-CC
4. Program insertion (local ads)—SCTE-35
5. HD/SD programs, SPTS or MPTS, multicast (IGMP V3) & unicast
6. MPEG-PSI, DVB-SI, ATSC-PSIP table support
7. SCTE-35 DPI detection/decode
8. SNMP trap and MIB support

**Browser support**

1. Firefox, IE and Safari

**Management port:**

1. 1000-base T Ethernet Interface (Back)

**Physical characteristics:**

1. 1 RU x 19”
2. Weight: 9.2 kg
3. 100-240V, 50-60 Hz power supply
4. 3-prong standard plug with AC ground

**Environmental conditions:**

1. Max storage temperature: 70c
2. Max operating temperature: 35c
3. Max humidity: 85%