Tektronix®

Sentry Series
Video Quality Monitors

User Manual

077-3202-01

Sentry Series Video Quality Monitor

User Manual

Tektronix®

SENTRY SERIES VIDEO QUALITY MONITOR

User Manual: Cable Operations

© 2004-2016 Tektronix, Inc.
All rights reserved.
Printed in U.S.A.

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

Federal copyright law protects this publication. No part of this publication may be copied or distributed, transmitted, transcribed, stored in a retrieval system, or translated into any human or computer language in any form or by any means (electronic, mechanical, magnetic, manual, or otherwise); or disclosed to third parties without the express written permission of Tektronix, Inc.

Tektronix makes no representation or warranties with respect to the contents hereof and specifically disclaims any warranties, merchantability, or fitness for any particular purpose. Furthermore, Tektronix reserves the right to revise this publication and to make changes from time to time in the contents hereof without obligation of Tektronix to notify any person of such revisions or changes.

Trademarks

Tektronix, the Tektronix logo, and Sentry 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 Sentry, Sentry Verify, Sentry Assure or Sentry ABR 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 Sentry Series User Manual* introduces you to the Sentry, Sentry Verify, Sentry Assure and Sentry ABR Video Quality Monitors, and describes in detail Sentry's features.

This user manual shows you how to configure, control and use Sentry, Sentry Verify, Sentry Assure and Sentry ABR. Please note that some of the features and applications described in this manual may not apply to all products. Refer to the Sentry Family Product Matrix for more information.

Screen Shot Note

While all screen shots 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 **11**

Preface **13**

Who Should Use This Manual *13*

How to Get Help *13*

Introduction **15**

What is Tektronix Sentry? *15*
The Engine 15
Internal database 15

What does Tektronix Sentry do? *17*
Monitoring 17
Reporting 17
Alerting 18

Getting Started **19**

Front Panel Functions (2009 to present models only) *19*
IP address on the front panel 19
Manual power down from front panel 19
LED Brightness 20

Interface Components *21*
Main Page Menu 21
Login Info 21
Page Title Bar 22
Thumbnails 22
Group Tabs and Input Ports 22
Change a Port Assignment 24
ASI Port tab 24

Basic Operations *25*

Bitrate Violation *26*

Reports **27**

Programs *28*
Current Status 28
To Filter the Ports on the Report 30
Filter Sentrys licensed with VLAN support 31
Program Status 32
ASI Models 35
Program Search and display 36
Column Sort By arrows 37
Bell Icon for Alert creation 37
Configure Report History 38
Configure Provider Name 40
Other Configurable Items 41

Program Bandwidth Graph *42*
Program Details Screen 42
Access Program Details 42
Color Key 43
Error Seconds 44
PID Type descriptor 44
Refresh Thumbnail 45
Capture button 45
Stream button 45
Detailed Graph View 48
Other Program information 49
Quality of Experience Details 50
Access the QoE Details 50
Average Video QoE from the Program Status Page 51
Scoring QoE 52
Reason Codes Definitions 54
Perceptual Video Quality (eMOS) 55
Over-compression Artifacts 56
Group of Pictures (GOP) Length Reporting (Group of Pictures) 57
Audio Volume Level Details 58
Functionality 58
Access Audio Level Details 58
Graphing 59
Thumbnail Timeline 60
Discontinuity Details 61
Alert Details 62
PCR Details 63

Data Detect *65*
Report Types 65
Copy Generation Management System (CGMS) 65
Closed Caption Data 66
Other Data 67
Generate a Report 68

Ad Cue Info (Digital Ad Insertion) *70*
Access Ad Cue Info 70
Reading the Ad Cue Info report 72
Ad Splice Command Types 75
Drill down/Zoom In 76
Blackout Detection 76
Repeated commands 77
Audio Level Graph 77

Program Statistics (Report and Export) *78*
Access Program Statistics: 78
Tab View 78
Create a Program Statistics Report 79
History tab 82

Port Statistics *83*
Summary tab 83
Create a Port Statistics Report 84

Program Groups *86*

Using Program Groups ... 86
Program Groups Bandwidth ... 88
Access Program Groups Bandwidth ... 89
Dynamic Program Groups ... 91

Thumbnail Wall View ... *95*

Transport ... *96*
Transport Status ... 96
Transport Bitrate History ... 98
PSIP ... 100
TR101/290 Status ... 103
Access TR101/290 Status ... 103
Show TR101/290 Priorities ... 105
IP Stats ... 106
Functionality ... 106
The Leaky Bucket Buffer Analogy ... 106
Access IP Stats ... 108
IP Stats Welcome Page ... 109
Graphing Ports ... 110
Zoom in on a Graph ... 111
Create IP Stats Alerts for Arrival Interval ... 111
Create Alerts for Delay Factor ... 114
IP Stats Monitoring Notes ... 114

Carousel Status ... *115*
OCAP Carousel ... 115
Access OCAP Carousel ... 116
OCAP Summary tab ... 117
OCAP Files tab ... 118
Files tab ... 120
Applications tab ... 123
Events tab ... 124
Set Alerts in OCAP Status ... 126
Review OCAP Alerts in Alert History ... 128
BFS Status ... 130
Monitoring the S-A Broadcast File System (BFS) ... 130
BFS Overview ... 130
BFS Mapping ... 130
Access BFS Status ... 132
Summary tab ... 133
Detail tab ... 134
Drill Down to BFS Detail View ... 136
EBIF Status ... 138
Access EBIF Status ... 138
Summary tab ... 138
Detail tab ... 139
Viewing Program Detail from EBIF Status ... 140
Applications tab ... 142
Events tab ... 144

Alerts ... *145*
Alert History ... 145
Report Export ... 147
Alert Analysis ... 150

Access Alerts Analysis 150
Alert Analysis Summary Screen 151
Report Navigation tabs and New Report icons 152
Counts tab 152
Trends tab 156
Trend Details tab 157
Distributions tab 159
History tab 160
Program Alert Definitions Report 161
Create/Edit tab 162
History tab 165

Configure 167

Configure Alerts 168
How Sentry Handles Alerts 168
Create an Alert 169
Create Alerts Step by Step 172
View Created Alerts 176
Delete Alert 176
Modify an Alert 176
Access Alerts Summary 177
Scrambled Alerts 179
Transport tab 181
Types of Transport Alerts 182
PID Alerts 184
Any PID on a Port 184
Table on a Port 185
Table on a PID 185
PMT 185
DSM-CC on a Port 185
DSM-CC 187
Port Alerts 187
Sample Transport Alerts 188
Create Audio Level Alerts 188
Create a Transport NULL PID Bitrate Alert 192
Create Mean Audio Level Alerts 193
Create Audio Dialnorm Alert 194
Buffer overrun/underrun detection 195
Configure Buffer overrun/underrun detection 196
BFS tab 198
Types of BFS Alerts 199
BFS Source 199
BFS Carousel 199
BFS File 199
Types of OCAP Alerts 200
File Alerts 200
Folder Alerts 200
Extension Alerts 200
Configure Program Availability Definitions 201
Create Program Template Alerts 204
Template Alerts 204
Create an alert from a Template using a Program Alert 209

Create an alert template without a Program Group 212

Program Groups *214*
Create Program Groups 214
Access Program Groups 214
Groups Summary tab 215
Add unlisted programs 218

Configure Program Mappings *220*
Add a New Mapping 220
Delete a Mapping 223
Modify a Mapping 223

Configure Port Names *224*

Configure BFS Settings *225*

Configure Triggered Stream Captures *226*
Access Alert Stream Captures 226
Create Alert Stream Captures (When none currently exist) 227
Deactivate or Delete a Stream Capture (when one previously exists) 234
Retrieve Captured Files 235
Delete Captured Files 235
Defaults tab 236

Configure Triggered Stream Captures(via Nexidia Comply™) *237*
Configure the Nexidia Server 237
Create a Nexidia Comply Profile 238
Create Caption Profile 239
Choose a Program to Verify 239
Review Job History 241
Review Closed Caption Verification Results 243

Configure Schedules *246*
Create a Daily schedule 246
Create a Weekly Schedule 249

Dashboard Graphs *251*
Create a Dashboard Graph 252

Configure MPEG Input Settings *253*
IGMP v3 SSM Support 253
Access MPEG Input System Settings 253
Set SSM 255
Multicast Stream Collision Errors (Multiple Sources Detected on Input Ports) 256
Sentry with 2nd MPEG Input Option Installed 257
Sentry with VLAN Support Enabled 258
Configure VLAN monitoring option 258
Assign/Configure Ports on a VLAN 260
Move a Port between VLANs 260
Reviewing Port/VLAN Assignments and VLAN Status 261

Configure System Preferences *262*

Configure TR101/290 Settings *264*

Configure System Settings *265*
Network settings 266

Set the Time 267
Set the Locale 268
Maintenance Mode 269

System Diagnostics *270*
Email Diagnostics 270
Network connectivity 270
System Communication 271
SNMP Trap 271

Configure Import/Export Settings *272*
Export tab options 274
Import tab options 276

Configure Users *277*
API Access 277
Add a User 277
Delete a User 279
Modify a User 280

Configure System Upgrades *281*
Upgrade Procedure 281
Upgrade Errors 284
Recoverable error 284
Error Requiring a Patch 284
Uploading the Error Patch File 285
Upgrade History 285

Configure Power Off and Restart Capability *286*
Accessing Remote Restart and Power Off 286
Power Off a unit: 286
Restart a unit 287

Status 289

ASI Status page 290
System Status for Sentry with Second MPEG Input Option Installed 290

About 291

Appendix A: Sentry ABR 293

Configure: Alerts Summary *293*
Manifest Alerts 293
Create a Manifest Alert 294

Representation Alerts *296*
Representation Alerts Definitions 296
Create Representation Alerts 297

Dynamic Program Groups *299*

Configure MPEG Input Settings *301*
Administrator Set up Notes 301

Reports *303*
Program Statistics: ABR Stats 303
Create/Edit tab 303

History tab 305

Port Statistics *306*
Summary tab 306
Create a Port Statistics Report 307

Media Set Status Report *310*
Media Set Details 312
HTTP Status Codes 312
Representations Statistics 312
Fragment Load Headroom 313
Fragment Load Time 314
Fragment Load Latency 314
Fragment Load Bitrate 315
Fragment Size 315

System Status *316*

Appendix B: Sentry Edge, Edge II, Edge III-S, and Edge III-T 318

Preface *318*

Getting started *319*
Product description 319
Sentry Edge RF Monitoring Products 321
Sentry Edge Family Features and benefits 321
Sentry Applications 321
Sentry Edge I Features and benefits 321
Sentry Edge II Features and benefits 322
Sentry Edge III-S Features and Benefits 322
Sentry Edge III-T Features and Benefits 322
Standard and optional accessories 323
Power cord options 323
Configuration 324
Recommended steps 324
Configure the RF Stats Alerts 325
Configure the MPEG settings 326
Activate an RF input connection 327
To define/edit import settings for an RF configuration. 327
Filter options 329
Update the schedule/import schedule information 330
Import a configuration from a CSV file 331
To schedule an import 332
View/edit RF configuration details 333
Change the schedule 333
Configure port names for a channel 334
Configure schedule summary 335
Create a new schedule 336

Operating basics *338*
Reports 338
Current Status report 338
Port / channel numbers 338
Program Detail report : Tuning information 339
Program graph options 340
RF Stats 341

Constellation Diagram 342
Frequency Domain Graphs 344
Status 347
Park a tuner for a set amount of time 348
To park a tuner (alternate method) 350
To park a tuner for a set amount of time: 351

Appendix C: Acronyms 352

Appendix D: Examples 354

Notices 358

Trademarks 358

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 this 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 Sentry family of video quality monitors and the web browser-based interface. This manual introduces the components and features, so you can begin using the device.

Who Should Use This Manual

This manual is intended for service providers who use Tektronix Sentry products 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 Sentry?

Tektronix Sentry is an MPEG transport stream monitoring device that supports next generation digital services and traditional program monitoring. Sentry supports MPEG-2, H.264 AVC, MPEG-4 part 10, and VC-1 video compression standards. The components of Sentry are:

The Engine

Internal database

Sentry supports real-time monitoring through single- and 4-port ASI and Gigabit Ethernet (GigE) input of all MPEG source streams within the headend or hubs.

Sentry digs deep into the complex and private data residing within the stream, allowing video service providers to gain insight and solve problems in their digital networks. Sentry's extensive feature list includes:

- Audio and Video Quality of Experience Scoring System
- Audio Silence and Audio-level Issue Detection
- Detect Black Video, Frozen Video, Tiling/Macroblocking
- Perceptual Video Quality (eMOS)
- Live Thumbnails
- User Triggered and Alert Triggered Stream Captures
- Stream to View
- Historical Reporting and Graphing
- Transport Stream Bandwidth Graphing
- Program Group Bandwidth Graphing
- Carousel Monitoring (SA-BFS, DSM-CC, tru2way™)
- Digital Program Insertion
- 24/7 Real-time QoE Monitoring of Entire Channel Lineup
- Detect Intermittent Problems
- Alert Notification and Historical Reporting
- Error Second and Program Availability Reporting

Sentry's video quality monitoring solutions provide unique flexibility to enable you to implement any combination of monitoring components for any digital application, using the same Sentry hardware.

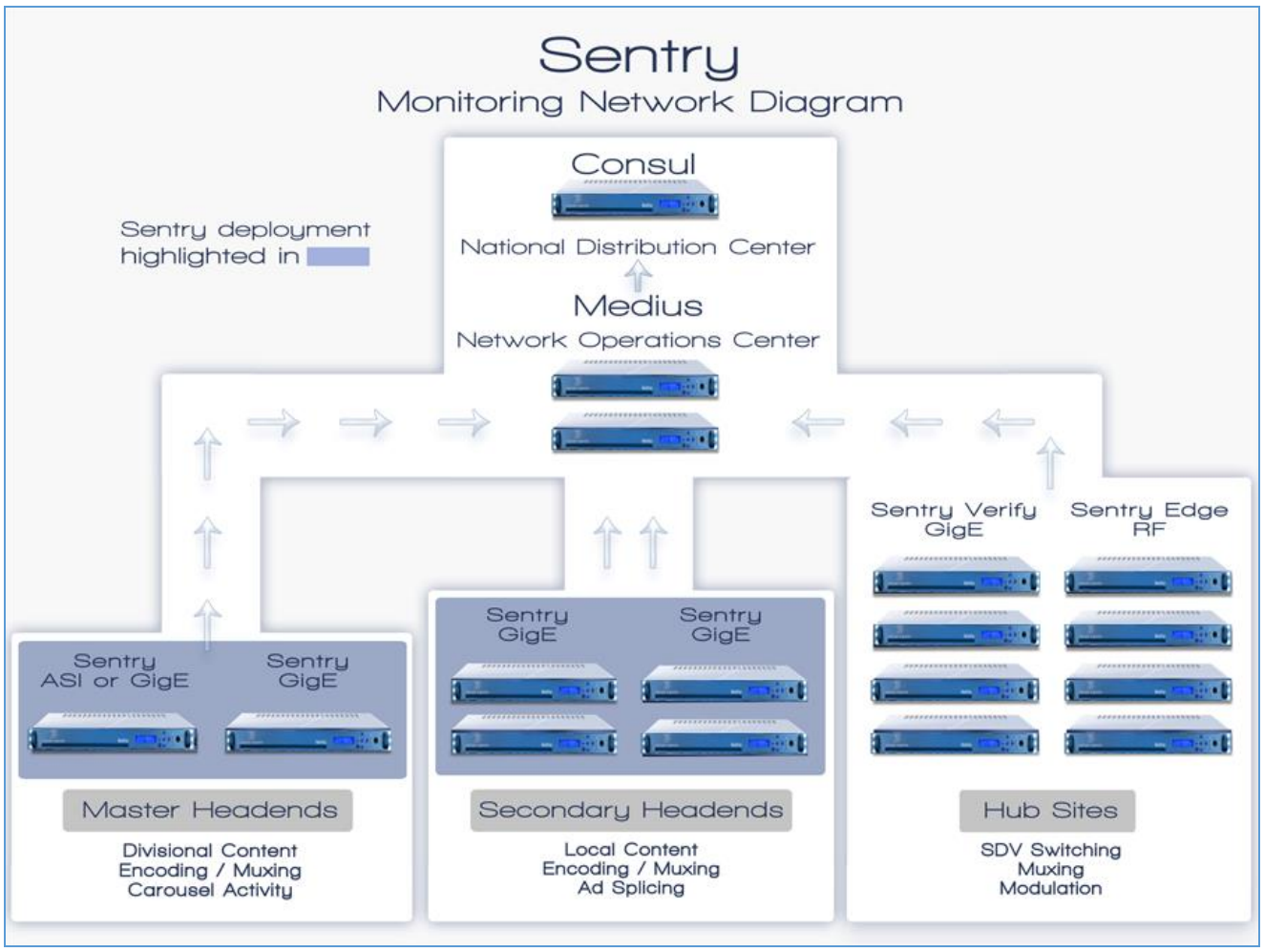


Figure 1: Sentry Network Diagram

What does Tektronix Sentry do?

Functioning completely within the digital domain, Sentry receives MPEG transport streams and monitors them for normal and unusual activity.

The primary features of Sentry are:

- **Monitoring**
- **Reporting**
- **Alerting**

Monitoring

Sentry tracks, and fully dissects the content of the digital media stream as it leaves the headend, including:

- Application data decode and verification
- Closed captioning compliance
- Bandwidth utilization
- Broadcast data decode and verification
- Carousel monitoring
- BFS monitoring
- OCAP monitoring
- Ad insertion auditing
- Tagged verification
- PSI/SI/PSIP/PMT decode
- Bitrate monitoring

Reporting

The Sentry web interface allows you to configure parameters and view the output of the Sentry engine historically and in real-time. In addition to standard reports accessible from the menus on the displays, detail views (e.g., program detail, BFS detail, ad cue detail) are available by clicking on various elements in the displays.

Standard Sentry reports include:

- **Current Status**
  An overview of the current state of the programs
- **Program Status**
  Provides a configurable history of all MPEG programs and their PID contents
- **Data Detect Report**
  Identifies specific program content
- **Ad Cue Info**
  Displays composite and component ad cues inserted into the stream.
- **Transport Status**
  Dissects the transport packets

- **TR101/290 Status**
  TR101/290 is a DVB standard for measurement and analysis of MPEG transport streams. Refer to the section on TR101/290 for a more in-depth discussion of this report and its features.
- **IP Stats**
  Displays information relating to IP packet arrival interval and delay factor.
- **OCAP Status**
  Displays the status of OCAP streams.
- **EBIF Status**
  Displays monitoring information EBIF Status
- **BFS Status**
  Displays the status of the Broadcast File System. Refer to Scientific-Atlanta Broadcast File System for a more in-depth discussion of this report and its features
- **Alert History**
  Lists alerts detected by the system. Refer to the section on Reports for a more in-depth discussion of this report and the section on Configure: Alerts for a discussion of creating alerts.
- **Alert Analysis**
  Provides an easy to use graphic analysis to visually represent alerts

Alerting

Sentry enables real-time alerts to indicate if content within a stream is invalid, a stream goes down, or user thresholds are exceeded. Alerts are visible within the web user interface (**Alert History**) and can be sent via email and SNMP trap. There are three major alert types:

- **Thresholds**
  Alert when a given bandwidth level or cycle time has exceeded or falls below on a PID, program, table, DSM-CC, or BFS. Alert when a program's PCR arrival interval or PCR jitter has exceeded or falls below a given level.
- **Thresholds with Frequency**
  Alert when a given threshold condition is met and it has occurred twice or more in a given time period.
- **Content**
  Alert when a selective piece of content has been received or transmitted correctly or incorrectly. Alert when a given PID or program is active or not-active. Alert if a PID, program, table, DSM-CC, or BFS drops. Alert if audio silences or video freezes.

Refer to the **Configuring Alerts** section for more information.

Getting Started

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

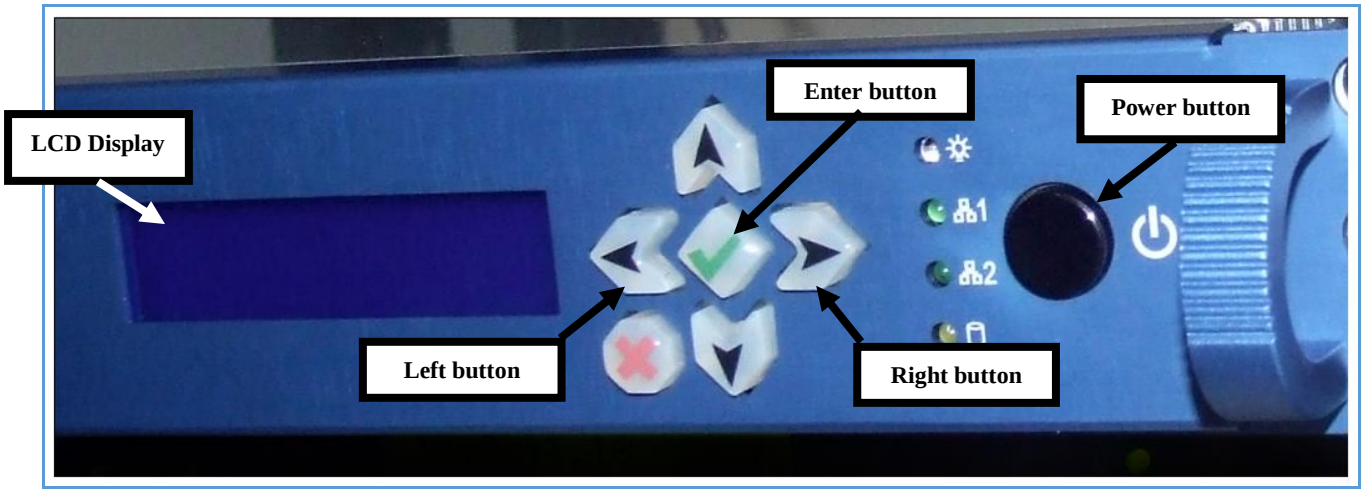


Figure 2: Sentry front panel

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 of the display corresponds to the **Management interface** and the lower line corresponds to the **MPEG/IP input**.

Manual power down from front panel

NOTE: ***The preferred method for rebooting or powering off a Sentry is through the web interface. Please see the Remote Power Off and Restart Capability section of this manual for more detail.***

WARNING*: When moving a Sentry, it is very important to properly power off the Sentry via the web interface.*

Never unplug a Sentry without performing the Power Off procedure. Improper shutdown may cause file corruption and failure of the Sentry.

In addition to powering down through the Sentry 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.

Interface Components

The Sentry interface consists of the following areas:

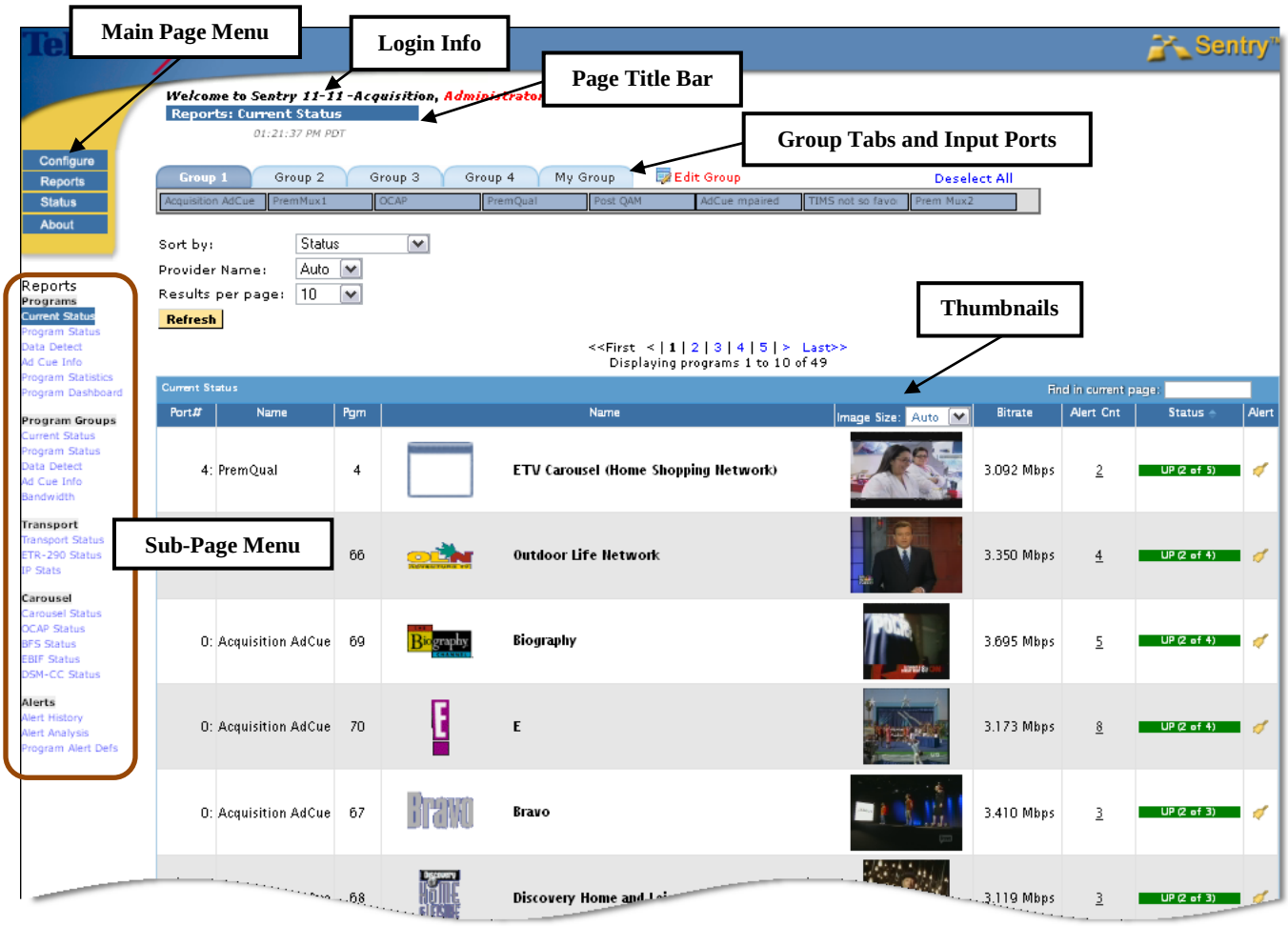


Figure 3: Sentry Interface Components

Main Page Menu

The buttons in this area (**Configure, Reports, Status**, and **About**) are the main categories of pages available for collecting information, reporting, and configuring the system. **Configure** and **Reports** contain sub-pages, accessible through drop-down menus.

Login Info

This area displays the username of the logged on user and provides a link to log out of Sentry.
Click **Logout** to log out of the system. The date and time of the most recent refresh of the screen is also shown.

Click **Refresh** to refresh the screen; otherwise the screen will refresh automatically at a periodic rate (~ every 300 sec.).

Page Title Bar

The title bar identifies the name of the page currently in view.

Thumbnails

Current Status also features **thumbnail visual confirmation** of the content of each program or service. You can control the size of the **thumbnail** at the top of the column. You can also refresh the thumbnail manually or it will refresh automatically every 5 minutes. Settings for thumbnails can be found in **System Preferences**.

Group Tabs and Input Ports

Input ports indicate the sources of transport stream input, which can be either ASI (one or four ports) or GigE (MPEG over IP unicast IP port or up to 30 multicast groups, each consisting of a Group ID and an IP Port). Sentry allows you to organize input ports into system and user groups. You must have Administrator privilege to create and modify system groups.

If the number of input ports is greater than one, then default system groups will be automatically created (two groups for a four port Sentry and four groups for Sentrys with more than four ports). Settings that the user has specifically saved are retained as they navigate from page to page.

For example, the figure below shows the groups and ports of a GigE Sentry. The Group 3 tab is selected showing that Ports 16 through 23 are in Group 3. Selecting a group will report only on the data from the ports in that group. Ports can also be renamed.

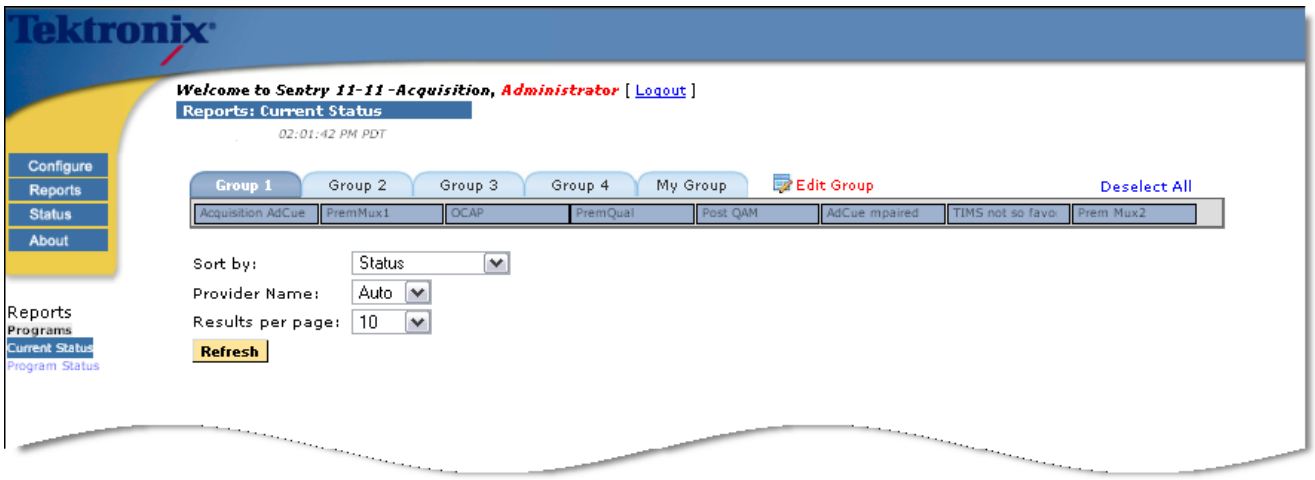


Figure 4: Groups and Ports of a GigE Sentry

Below are groups and ports of a four port ASI Sentry.

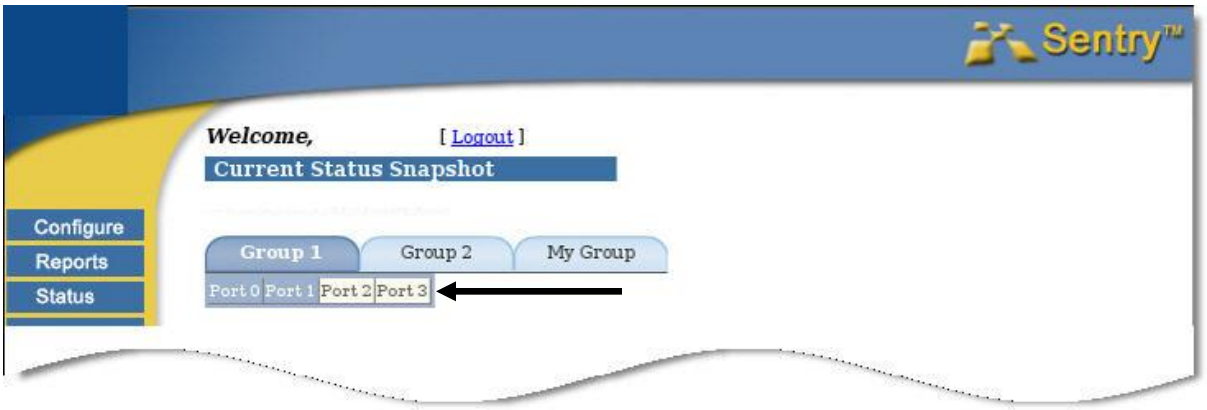


Figure 5: Groups and Ports of a 4 Port ASI Sentry (0, 1, 2, 3)

In the case of ASI models, the port is known from the hardware. For MPEG over IP models, the port is known from the configuration (refer to Configuring MPEG Input Settings.

Mouse over an input port to see a popup showing the input source.

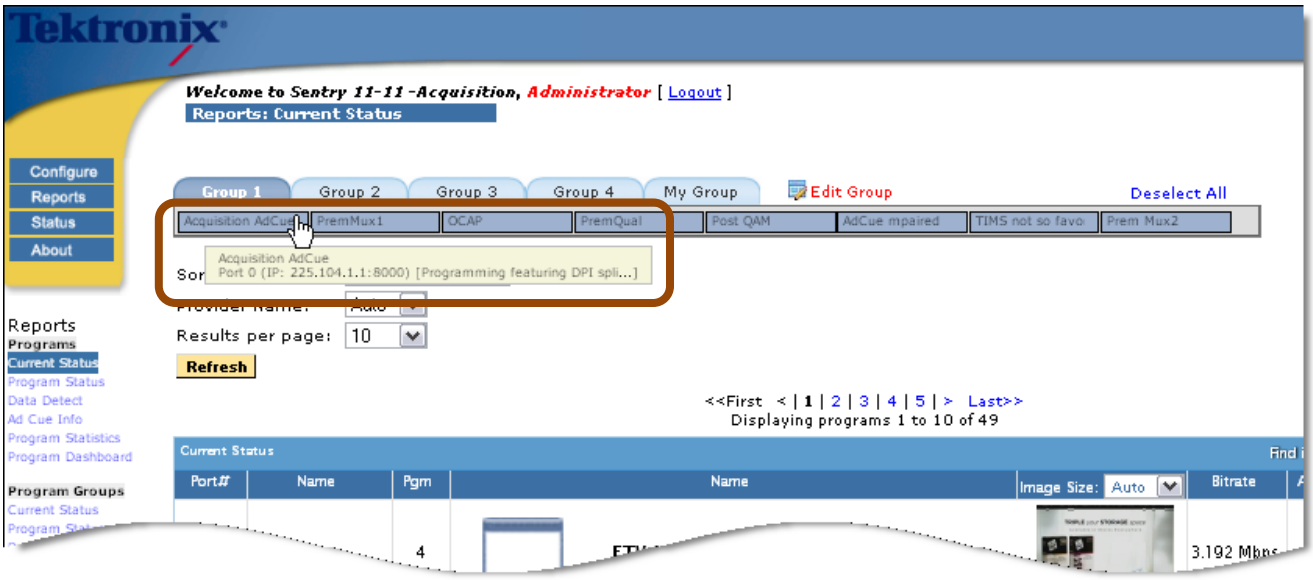


Figure 6: Group 1 Acquisition AdCue port popup message showing the input source

- Ports that are not configured are displayed as a light gray.
- Ports that are configured and assigned to a group are shown as dark gray.
- Ports that are configured but not assigned to a group are shown as white.
- The user can change the group assignments by clicking on ports, which toggle as assigned (dark gray) and unassigned (white).

Change a Port Assignment

1. Click on the port you wish to change.
2. Click **Save** to save the assignments. Click on the **Reset** button to reset the assignments.

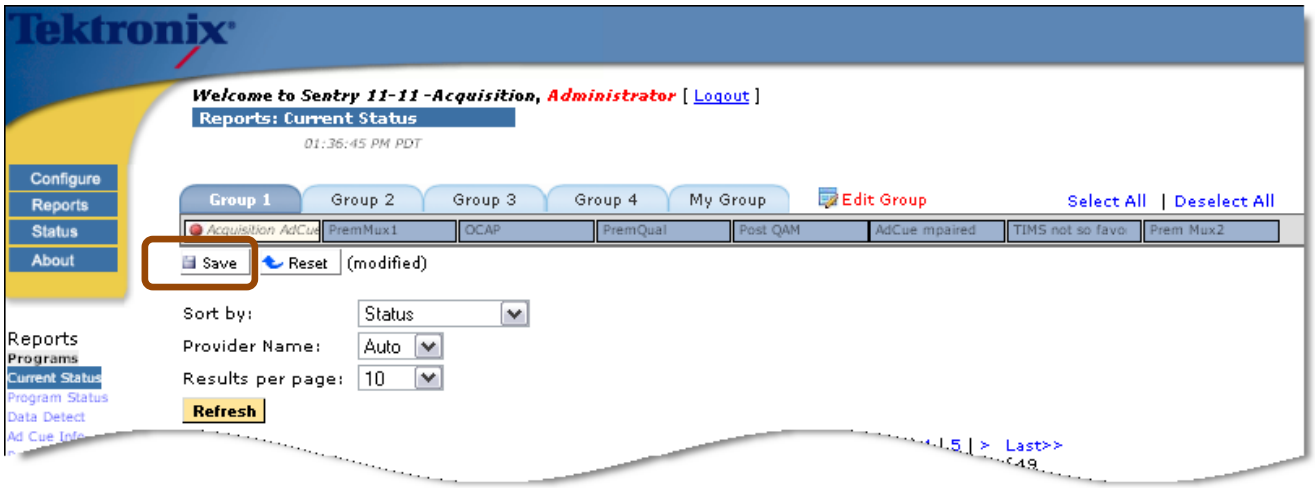


Figure 7: Save Button indicating Changed Port to Group Assignments

3. Selecting the **Refresh** button on the page before the assignments are saved will result in a note that assignments have been modified. A **Reset** button to reinstate the original settings will also be displayed.

ASI Port tab

A single port ASI Sentry has only one port tab and therefore has no need for a group tab.

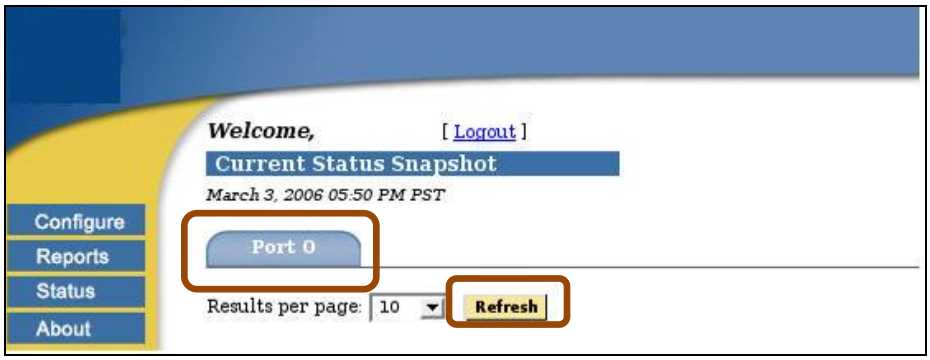


Figure 8: Port 0 of a Single Port ASI Sentry

Basic Operations

The web-based interface allows the user to administer Sentry in the following manner:
Select from a series of pages and sub-pages, and modify fields to create the desired configuration.
Submit the changes on any given page using the appropriate update or refresh buttons. If the user selects a new page or end the session without submitting the information, the changes are lost.

NOTE 1: ***To access the full functionality of the web interface, you must log in as a user with Administrator privileges.***

NOTE 2: ***If multiple Sentry administrators apply changes to the same set of parameters concurrently, the latest applied changes take precedence. Up to ten simultaneous browser connections are allowed.***

Bitrate Violation

If Sentry exceeds the combined bitrate for which it was licensed, a bitrate violation occurs. A violation warning is displayed on the opened page. Clicking on the **More info…** link in the violation warning provides more detail about the licensed bitrate and the violation.

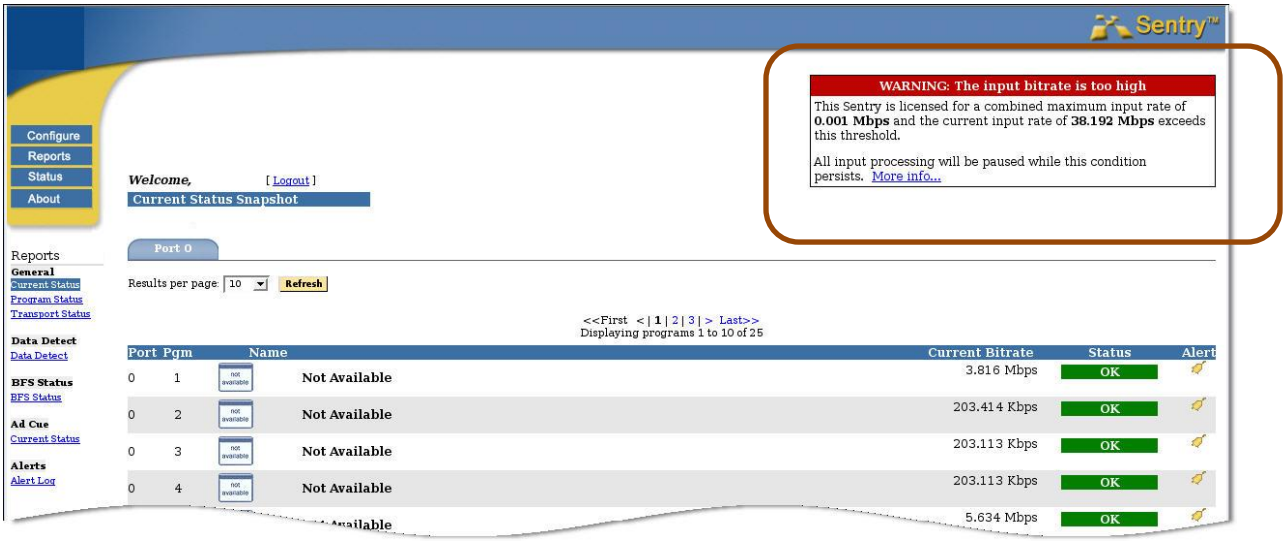


Figure 9: Bitrate Violation Notice

Processing will pause while the condition persists and the last known state is displayed.

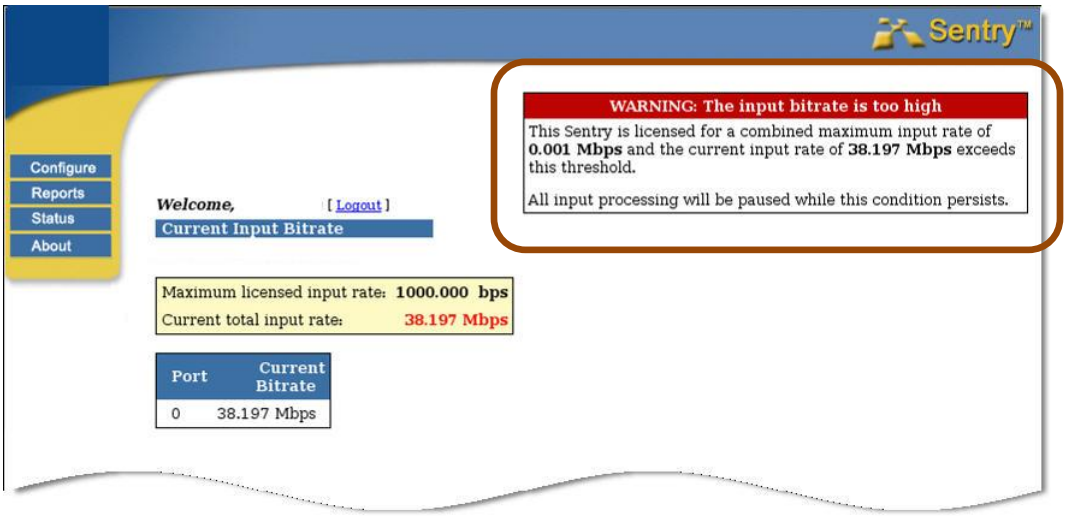


Figure 10: Bitrate Violation additional information

Reports

Reports are configurable to give you a real-time or historical view of transport activity. There are five main categories of reports, and all reports offer the capability to drill down to view additional detail:

- **Programs**
  - **Current Status**
  - **Program Status**
  - **Data Detect**
  - **Ad Cue Info**
  - **Program Statistics**
  - **Program Dashboard**

- **Program Groups**
  - **Current Status**
  - **Program Status**
  - **Data Detect**
  - **Ad Cue Info**
  - **Bandwidth**

- **Transport**
  - **Transport Status**
  - **TR101/290 Status**
  - **IP Stats**

- **Carousel**
  - **Carousel Status**
  - **OCAP Status**
  - **BFS Status**
  - **EBIF Status**
  - **DSM-CC Status**

- **Alerts**
  - **Alert History**
  - **Alert Analysis**
  - **Program Alert Defs**

Programs

Programs provide 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.

Current Status

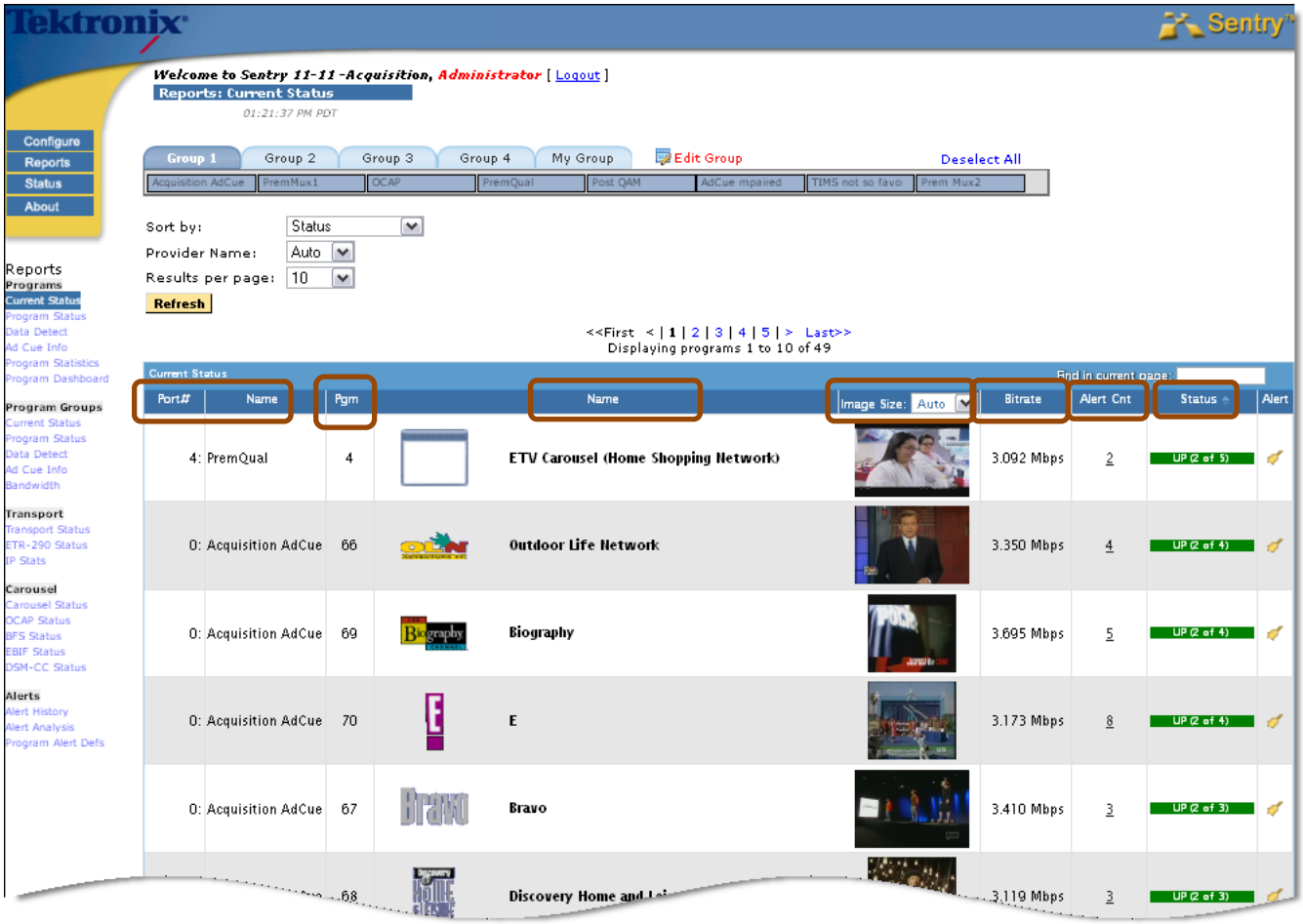


Figure 11: Current Status Snapshot Report

The main 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**
  Refers to the program provider icon and name, derived according to the **Provider Name** selection (refer to **Configuring the Provider Name**). 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 Sentry's **Configuring Mappings**. XDS data consisting of the show name and rating is also displayed if it exists.

- **Thumbnails**
  Provides a current image of the selected program. Thumbnail size may be adjusted using the settings located directly in the column header.

- **Current Bitrate**
  The current (last minute) bitrate of the program.

- **Alert Count**
  Shows the number of active alerts for each program.

- **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, e.g., 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.***

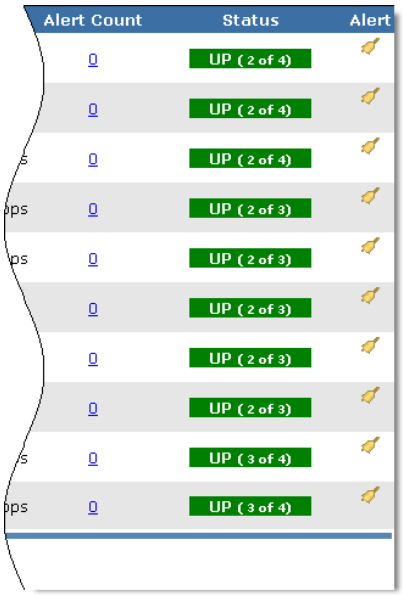


Figure 12: Status Column in Current Status

- **Alert Icon**
  When selected will automatically display and configure the **Creating Program Alerts** page for the selected program (See: **Alerts**).

To Filter the Ports on the Report

To narrow down the group of ports returned in the non-program group report, click **Edit Group**. The **Edit Group** display provides the following options:

- **Show All Ports**
  Show all port available to system
- **Show Active Port Only**
  Show only the ports that are actively monitoring input.
- **Filter on Selected VLANs**
  For Ethernet boxes licensed for VLAN support, filter on ports configured on a specific VLAN.
- **Select All**
  Select all only configured ports on this page only.
- **Remove All**
  Remove all selected ports
- **Cancel**
  Cancel action and go back to last page
- **Apply and Exit**
  Apply changes and go back to last page
- **Save**
  Save changes and stay on this page

1. Select **Edit Group**.

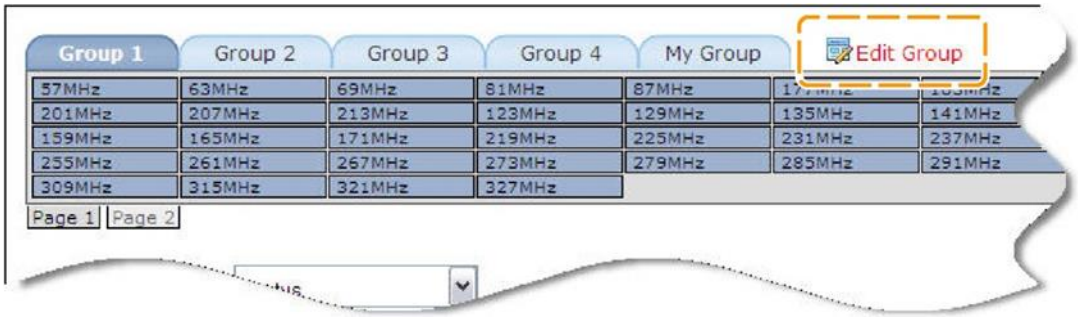


Figure 13: Editing a group

2. Select **Ports** as needed.

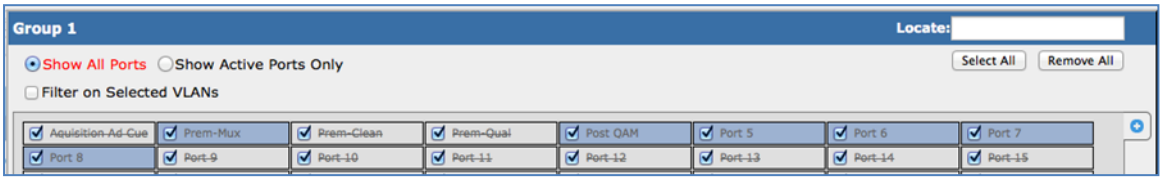


Figure 14: Editing a group (ports selected)

3. Select **Apply** and **Exit** when done.

Filter Sentrys licensed with VLAN support

To filter on specific VLANs, select **Filter on Selected VLANs** and check the desired VLANs.

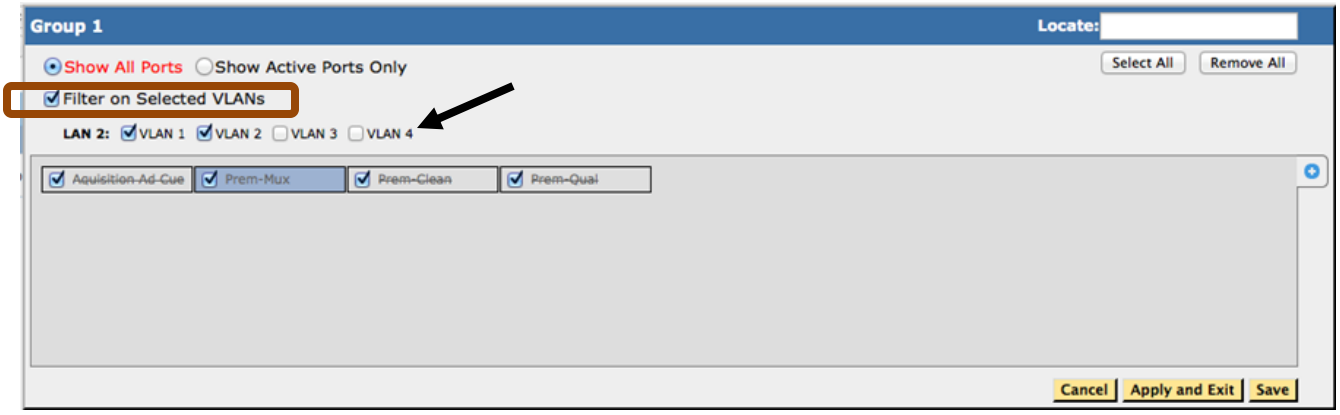


Figure 15: Editing a group

Program Status

The **Program Status** report gives a configurable history of all MPEG programs and their PID contents.

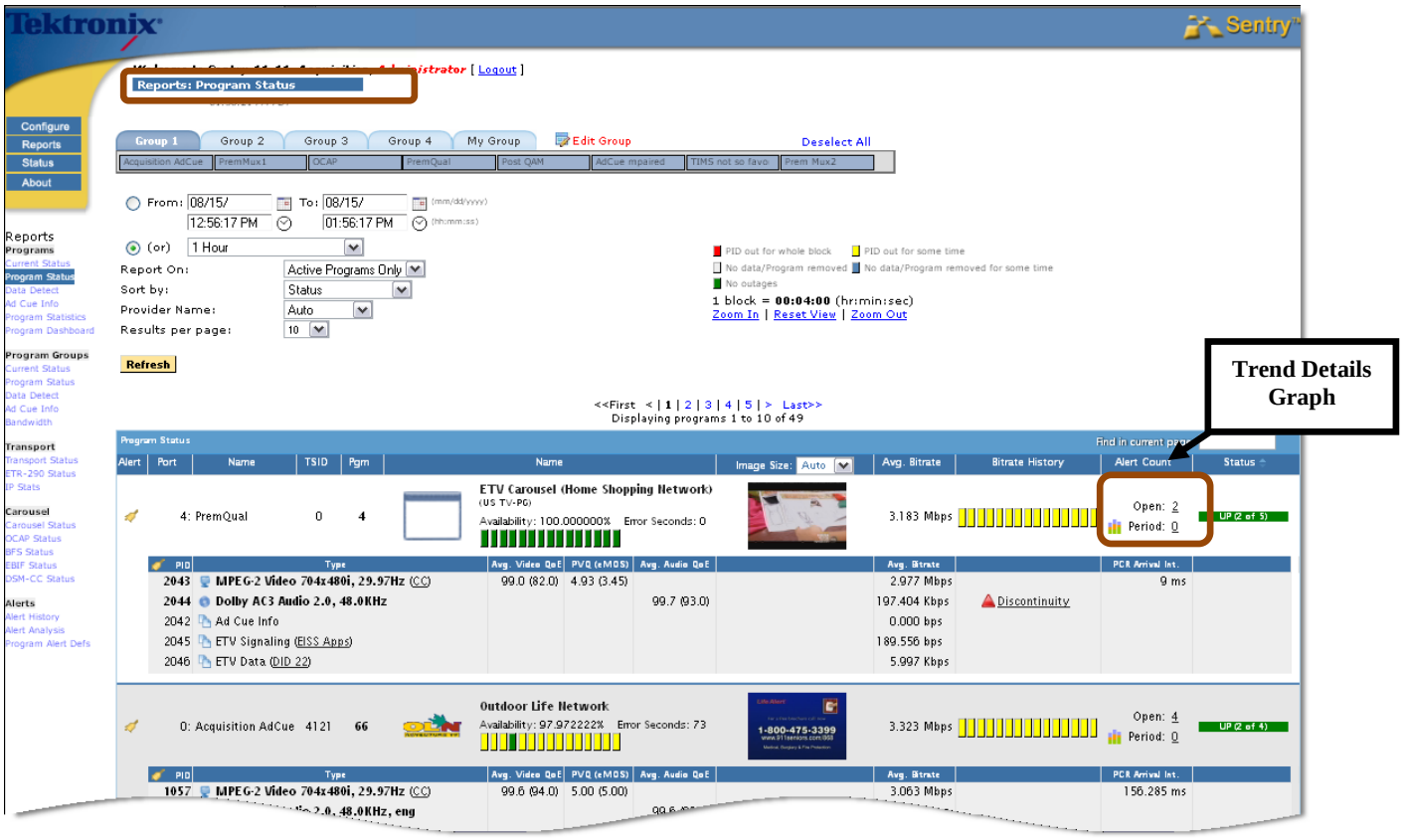


Figure 16: Program Status Report Overview

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:**
  The **Transport Stream ID** derived from monitoring the stream.
- **Name:**
  Program Availability and Error Seconds for the selected time range is added to the Name field in Program Status. **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. **Error Seconds** is the number of seconds a program was unavailable as defined by the program availability definitions.
  - **Green** indicates no errors
  - **Yellow** indicates there was an error for some time
  - **Red** indicates there was an error for the whole block
- **Avg. Bitrate**
  The program bitrate averaged over the time range shown in the **Current View**.

- **Bitrate History**
  The PID data in the stream over the selected time range, shown as color-coded discrete blocks.
  - **Gray** indicates no data
  - **Yellow** indicates PID out for some time
  - **Red** indicates PID out for whole block
  - **Green** indicates 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.
- **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 scores for the specified time period.
- **PVQ (eMOS)**
  Shows the average and minimum scores for the specified time period.
- **PCR PID Arrival Interval**
  Tells 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.
- **Discontinuity**

  The presence of discontinuities; the absence of any indication means no discontinuities.
  - Three types of PID indicators will be drawn for **Video**, **Audio** and **Data PIDs**. An indication of **Copy Generation Management System** (**CGMS**), **Closed Caption** (**CC**), or scrambled (**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 type.

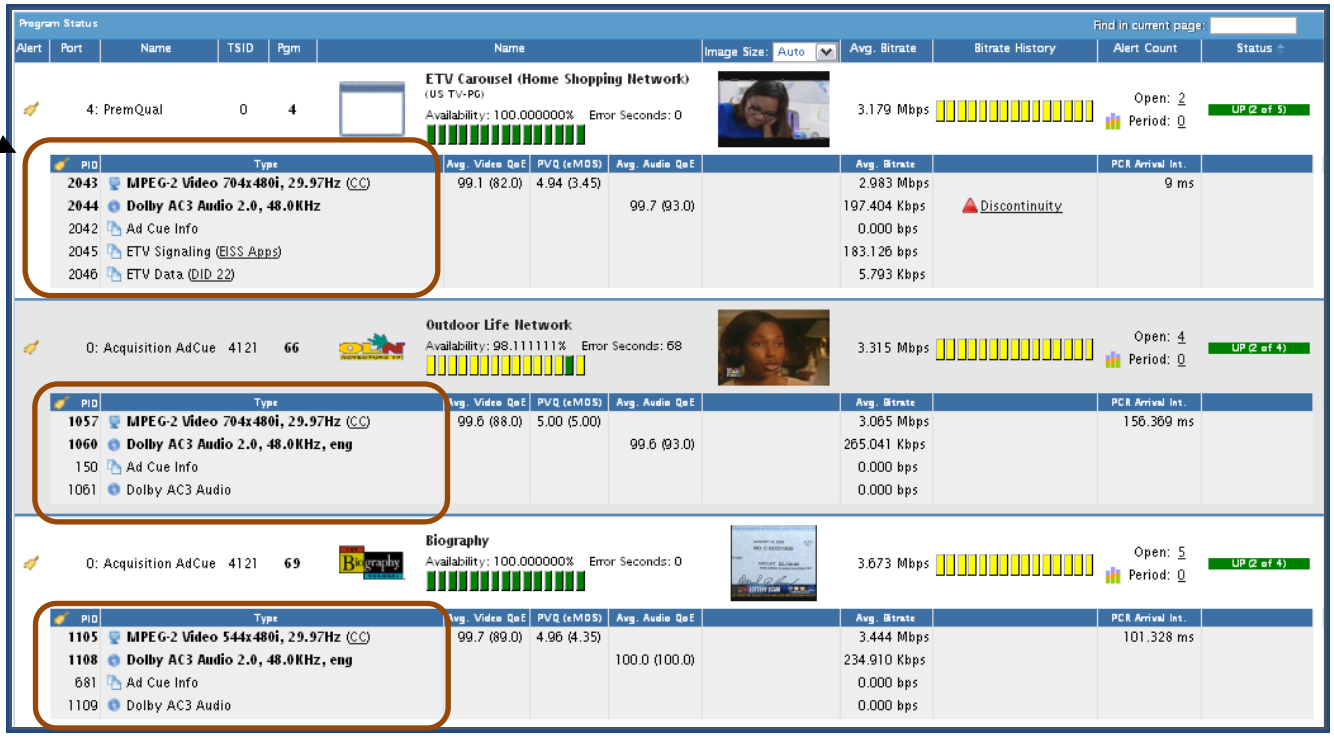


Figure 17: PID Types with details in bold

The **PID Type** descriptor displays the following:

- **Video**
- **Video resolution**
- **Refresh rate**
- **Audio**
- **Audio Mode (2.0 = stereo . 1.0= mono, 5.1 = surround sound)**
- **Sample rate**
- **Language version**

ASI Models

The ASI model Sentrys will display PCR arrival interval and minimum, average, and maximum jitter over the time range.

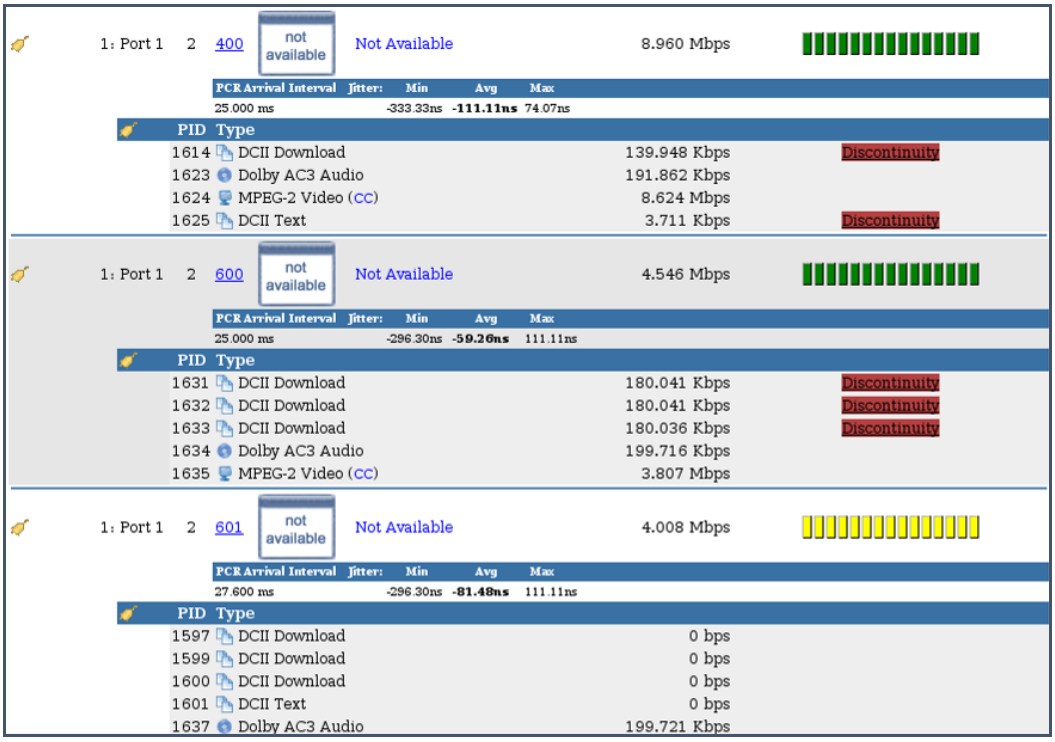


Figure 18: Program Status on an ASI Sentry

Program Search and display

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

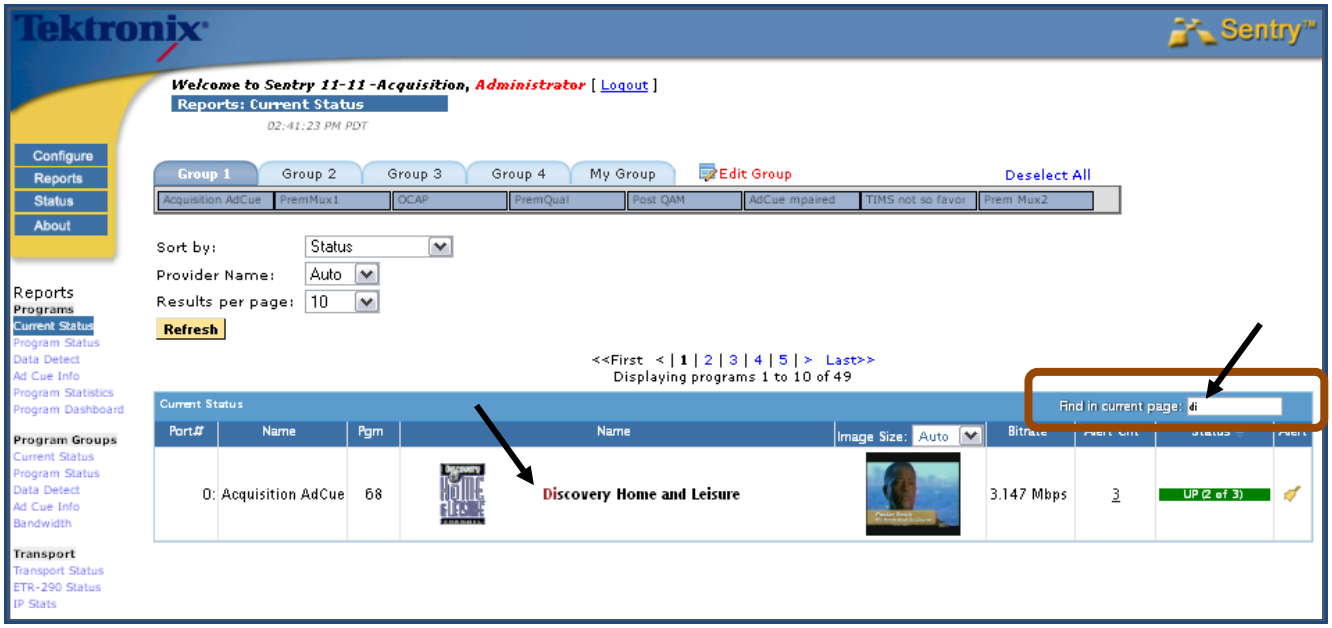


Figure 19: Program Search field. A search with "di" yields Discovery Home

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:

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.

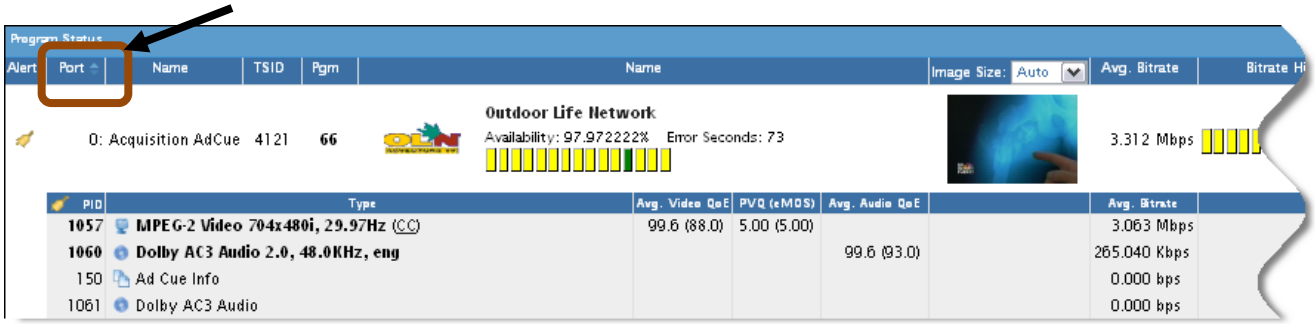


Figure 20: Column header Sort By arrows

Bell Icon for Alert creation

When selected, the **Bell Icon** provides a drop-down menu of types of alerts that may be created for this program.

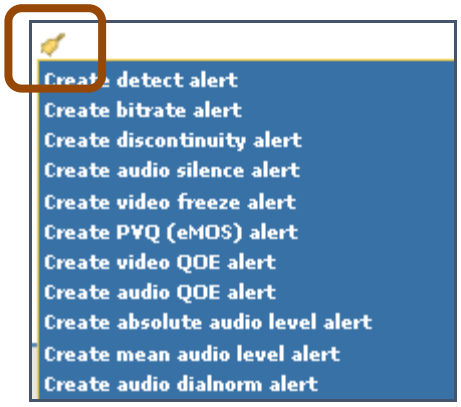


Figure 21: Alert Types drop-down menu

Configure Report History

For historical reporting, the user is able to configure the time range of the report, either by choosing a **Current View** as in the **Program Status** report or by specifying a range of time as in **Program Detail**.

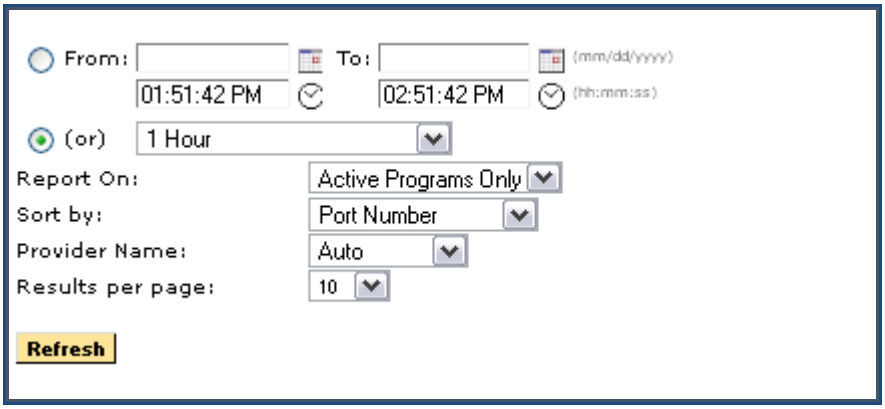


Figure 22: Selecting a Current View

To specify the exact date and time you want the report to start and exactly when you want it to stop:

1. Select **From:/To:**
2. To display the calendar, click on the calendar icon adjacent to the **From and To** boxes.
3. Select the date that you wish to start or stop on and type it in the appropriate field.
4. Illegal dates such as **From > To** or future dates are prohibited and will be automatically reset to a legal state.
5. The exception to this rule is the **Ad Cue** Info report where dates up to two weeks in the future are allowed.

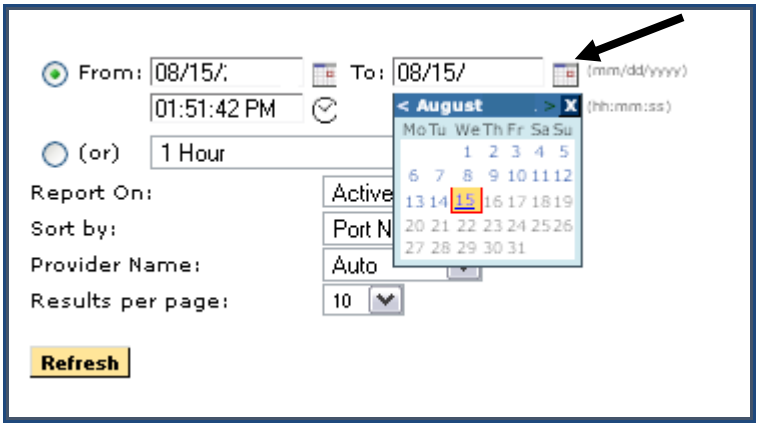


Figure 23: Report Calendar Option

To pick a specific time, either type in the time or click on the clock icon to bring up a clock entry dialog.

The minimum **From/To** interval is one minute. Entering an end time such that the time interval is less than one minute will reset the begin time to one minute before the end time.

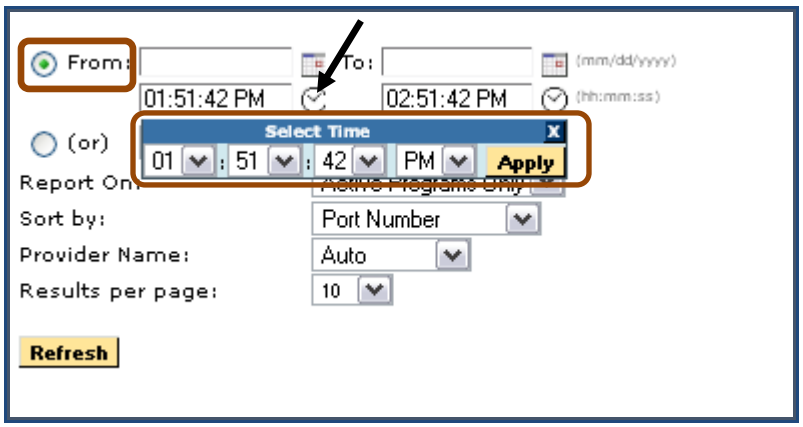


Figure 24: Report Clock Option

The pages that offer the **From:/To:** option also offer a drop-down option consisting of **Most Recent** and **Standard** selections.

1. Select the (or) radio button and click on the desired setting.

   For example, if you would like to see all activity for the last hour, you would select this menu item to display **1 Hour**. The default time period is 1 hour.

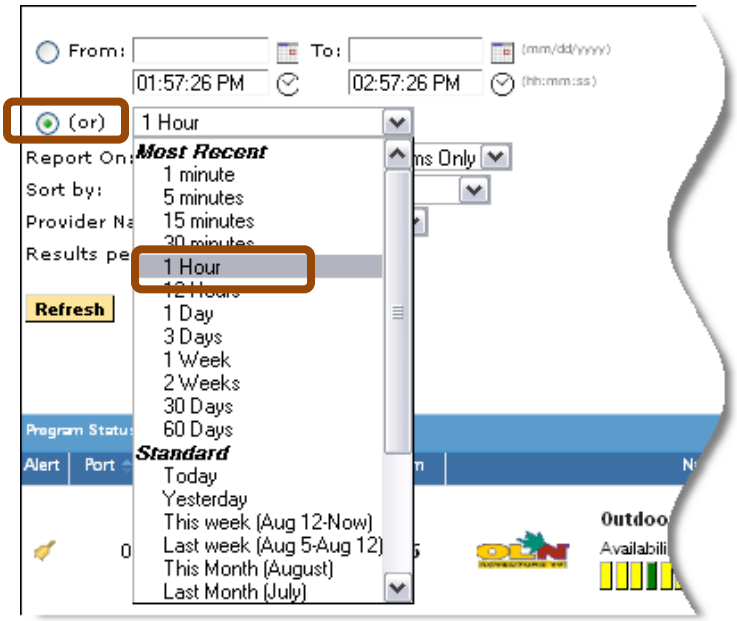


Figure 25: Report Option to Select Most Recent Time Range

2. Click the **Refresh** button to generate the report with the new configuration. You may see the message: **Generating Report**.
3. For reports based on a most recent time period, real-time activity is included in the time period and will continually update as time passes.
4. A time range set for a page will be preserved when the same page is selected again.

Configure Provider Name

The **Current Status** and **Program Status** reports allow you to select the source of the program provider, using the **Provider Name** drop-down list. The list contains: **Auto, XDS**, **SDT** (if the data exists) and **Mapping**.

If **Auto** is selected (the default), then the provider name and icon are determined by the following logic:

- If a **Program-Provider** mapping exists, display the mapping. (see **Configure Mappings**).
- If any PID on the program has a BFS source, display the BFS name and icon.
- If the program has XDS data, use the XDS provider name (or show name if there is no provider name) to compare with mappings defined in the system.
- If there is an exact match, display the XDS provider name and icon.
- If there is a partial match, display the XDS provider icon only.
- If there is no XDS data and SDT data exists, then use the SDT service name to determine the provider name according to the above logic for XDS data.
- If XDS or SDT is selected from the drop-down Provider Name list, then only the XDS or SDT, data is used to determine the provider. SDT will appear in the list only if there is SDT data.

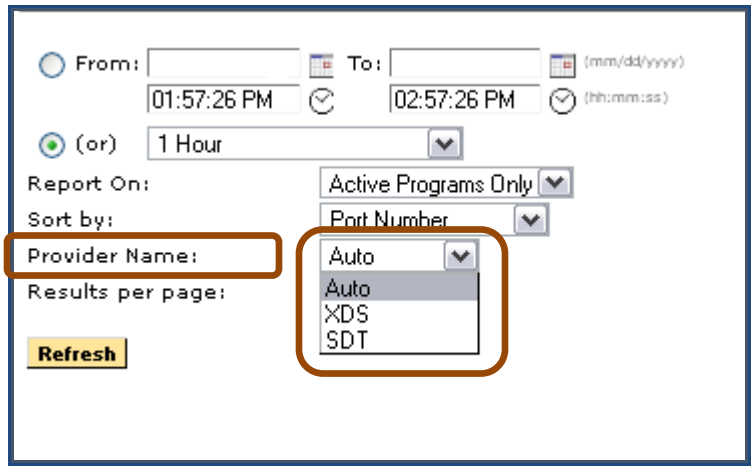


Figure 26: Auto Provider Name Selected (Default)

The **Mapping** method will ignore XDS and SDT data and just show any name mapped on the Program Mappings page.

Other Configurable Items

Other configurable items include the ability to sort and to select the number of results displayed per page.

1. Select the sorting options from the **Sort by** drop-down menu. There are a number of different items to sort from including **Video** and **Audio QoE, PVQ, Bitrate, Availability** or **Error Seconds**.

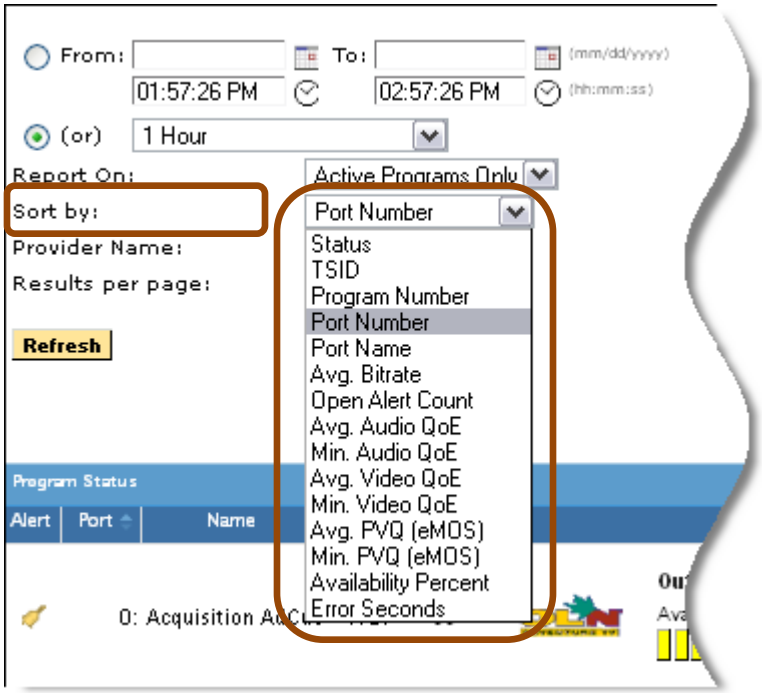


Figure 27: Options for Sorting

2. Select the results displayed per page from the **Results** per page drop-down menu.
3. Click **Refresh** to activate the selection.

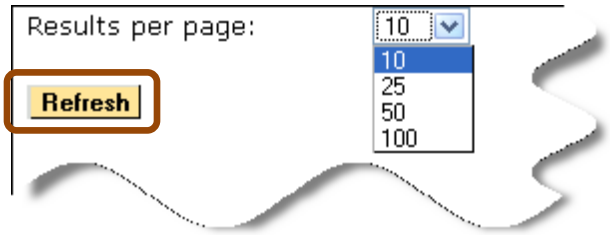


Figure 28: Selecting Results per Page

A report can also be sorted by clicking on a column header. A report that has a **Sort by** drop-down menu will sort ascending only.

A page that supports sorting by clicking on a column header only will toggle between ascending and descending.

Program Bandwidth Graph

The **Program Bandwidth Graph** is a function of Sentry available through the **Program Details** screen. Within this window, users may monitor specific details for a selected program and may 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

From the Sentry welcome screen, choose the program you wish to view **Program Details** for by selecting its logo or program name from the **Displaying Programs** list. For this example, we selected the logo for **Outdoor Life Network.**

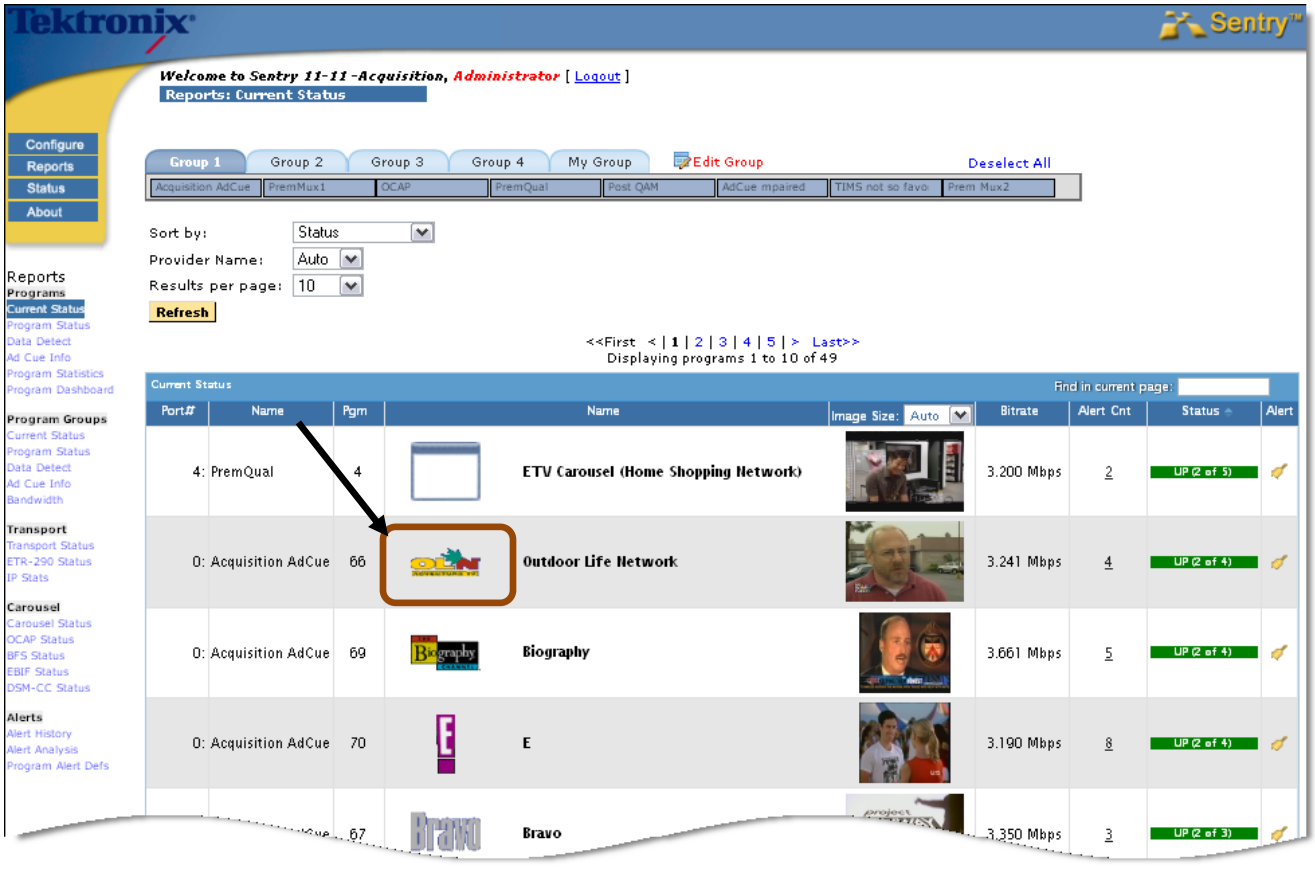


Figure 29: Selecting a program

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

a. Assist in assessing the health of the selected program

b. 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 **Bitrate**, **Quality of Experience, Audio Volume Level, 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.

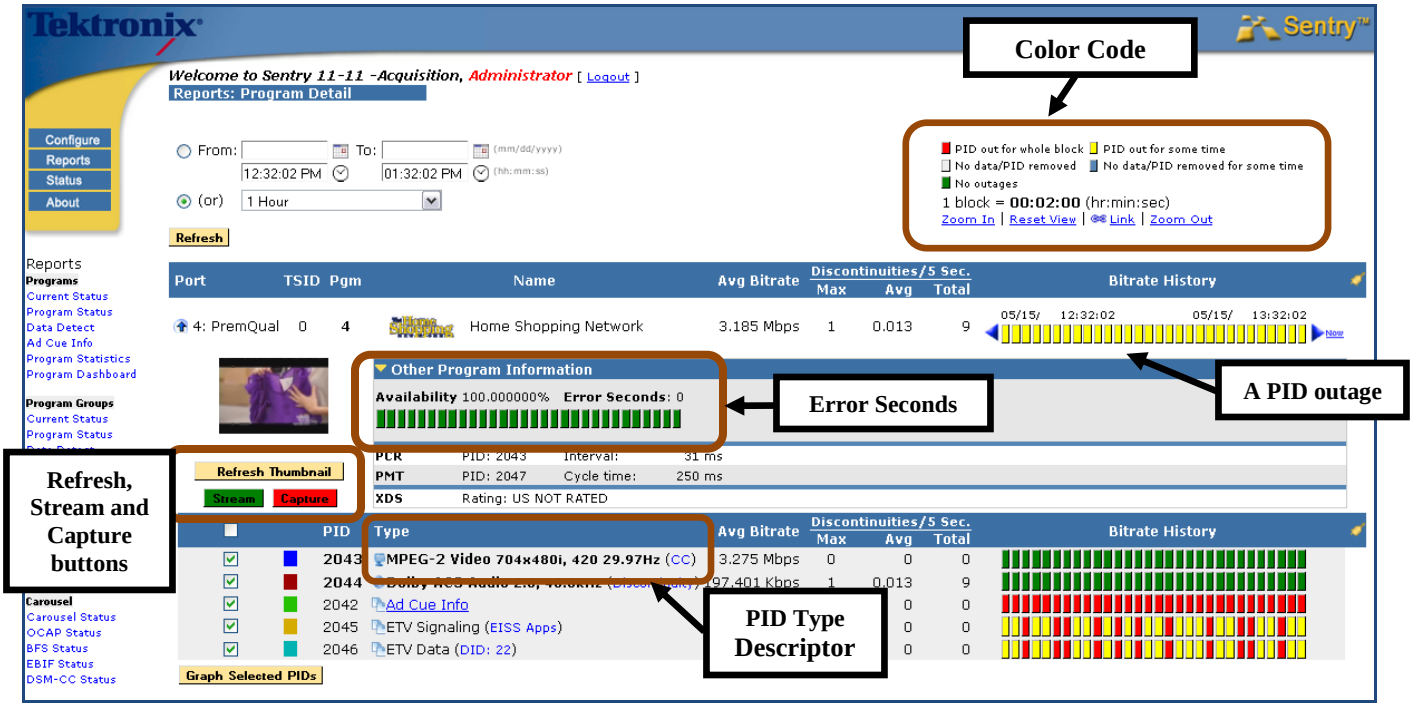


Figure 30: Program Details screen

Color Key

Shows the color legend for screen

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.

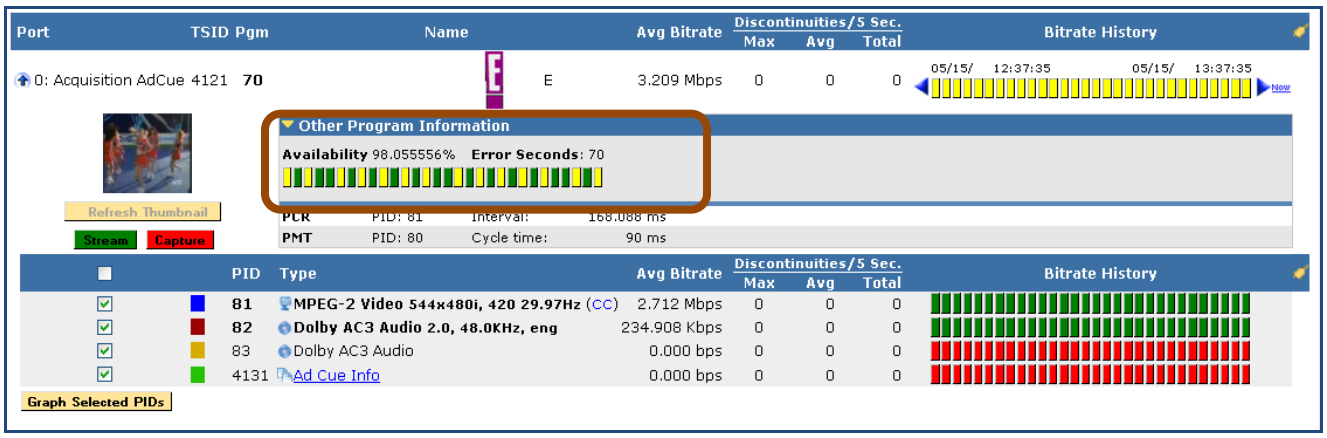


Figure 31: Error Seconds from the Program Detail screen

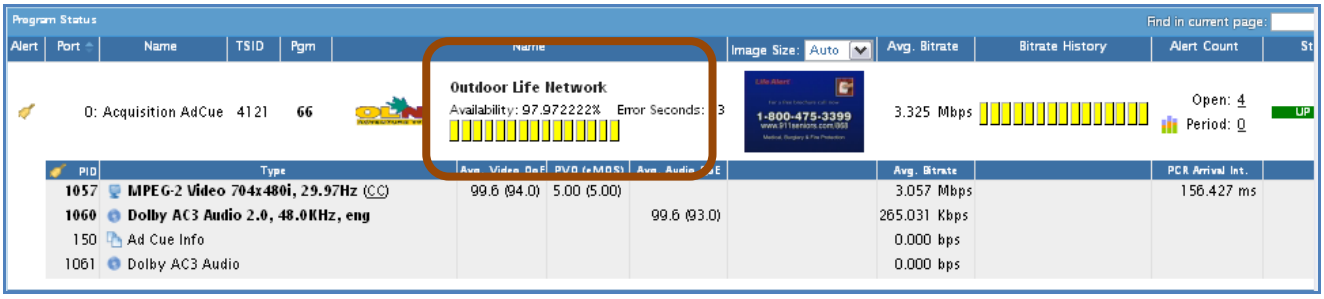


Figure 32: Error Seconds in all other locations

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 port. In the example, the MPEG 2 video and one channel of the Dolby AC3 audio were in good shape (**Green**) while the **Ad Cue** info and second Dolby channel where out for the whole block (**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 **Port** and **PID** information.

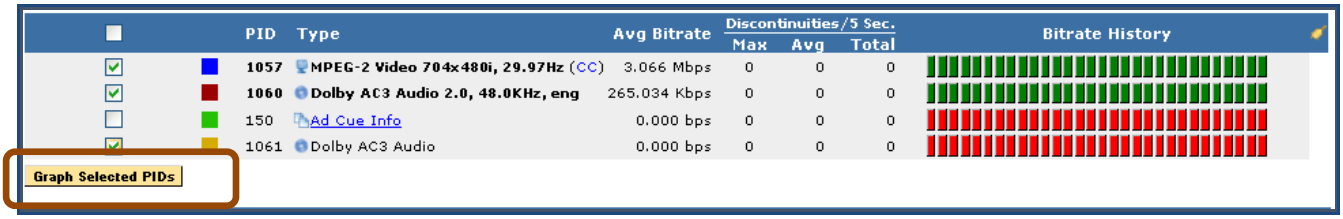


Figure 33: Graph Selected PIDs

The resulting graph will look similar to the one below.

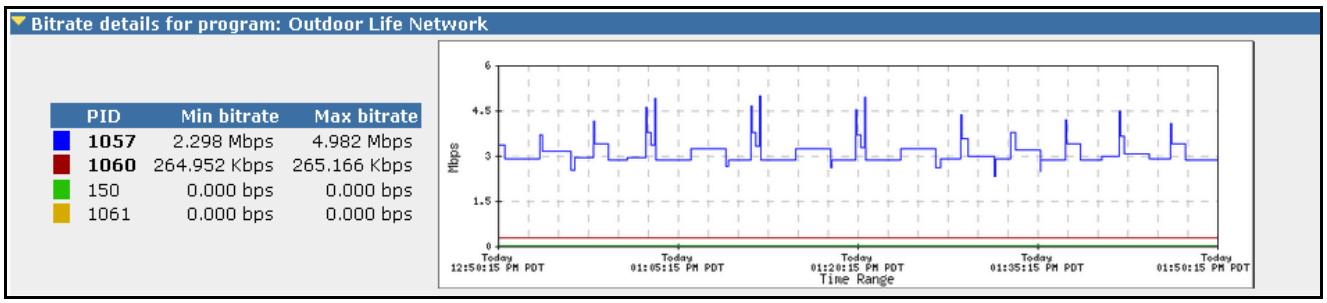


Figure 34: Bitrate Graph

Refresh Thumbnail

Manually refreshes current thumbnail.

Capture button

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

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.

Configure VLC to receive stream to view content

For an additional viewing option Video LAN Client (VLC) is a free player for files and streaming protocols. Installing VLC on a computer allows you to receive the **Stream to View**. This is an optional viewing utility.

1. Download and install **VLC.**
2. Open **VLC.**
3. Browse to **Media**> **Open Network Stream.**
4. Enter the following into the address box for the network URL:

   Udp://@:<port to stream to> where <port to stream to is a number between 1024 and 65535>.

   In the example below, 8000 is used

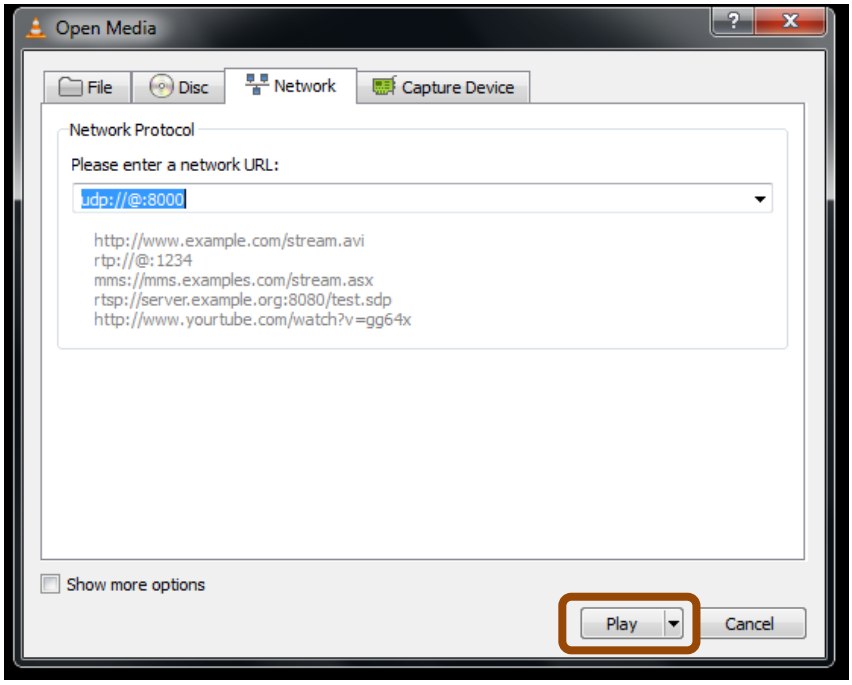


Figure 35: VLC Install

5. Click **Play.**
6. From the **Program Detail Report**, click on the **Stream button.**
7. Enter in your computer's IP address and desired UDP port (such as 8000) in the IP address field.
8. Choose the duration of stream.

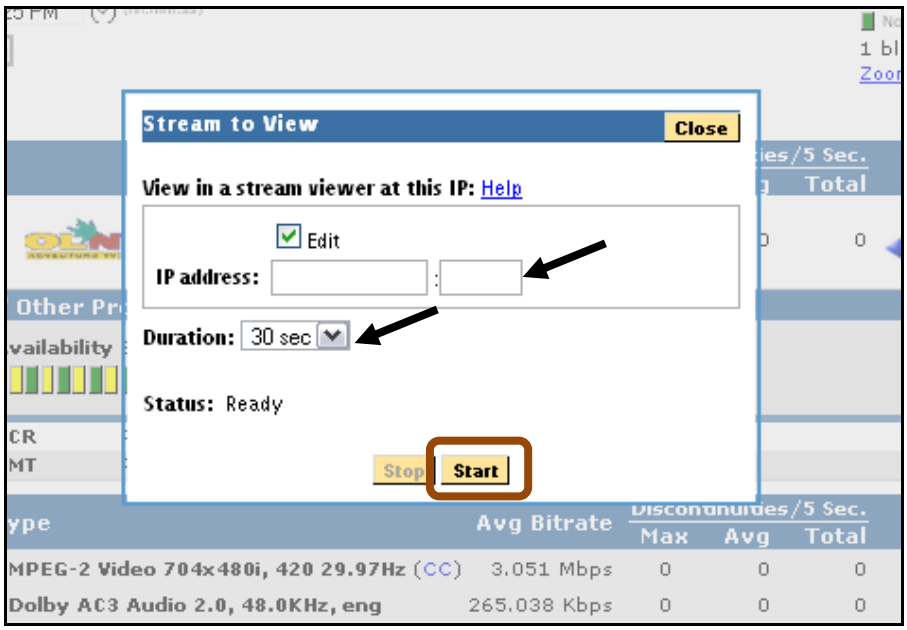


Figure 36: Stream to View parameters

9. Click **Start**
10. You should now see the stream appear in VLC.

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 then reload and display a more detailed view of selected time frame. In the example below, we selected a **Time Range** between 10:07 AM and 10:17 AM and the resulting graph went from a span of activity covering a 15 minute span to a graph showing activity for every 10 seconds.

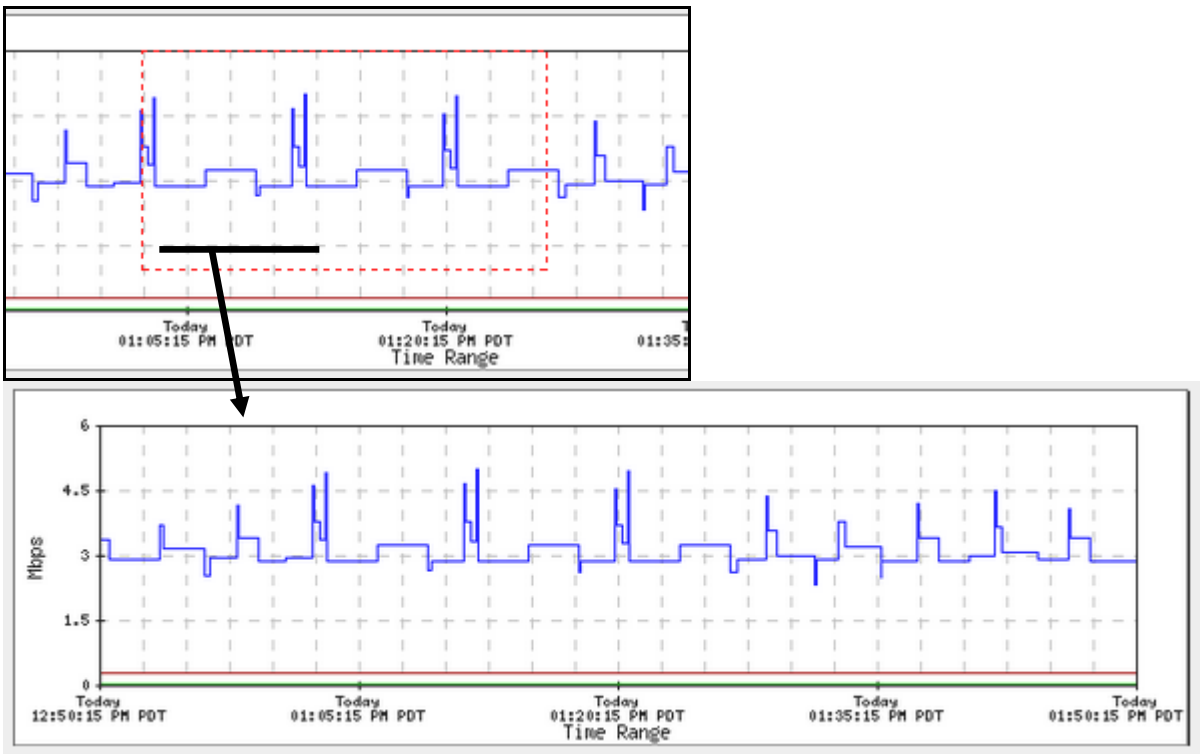


Figure 37: Selecting a section for a detailed view

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

Figure 38: 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.

Other Program Information

- PCR Program Clock Reference,
- PMT programs Map Table
- IDR Instantaneous Decoder Refresh
- EBP Encoder Boundary Point
- SDT Service Description Table
- XDS Extended Data Services

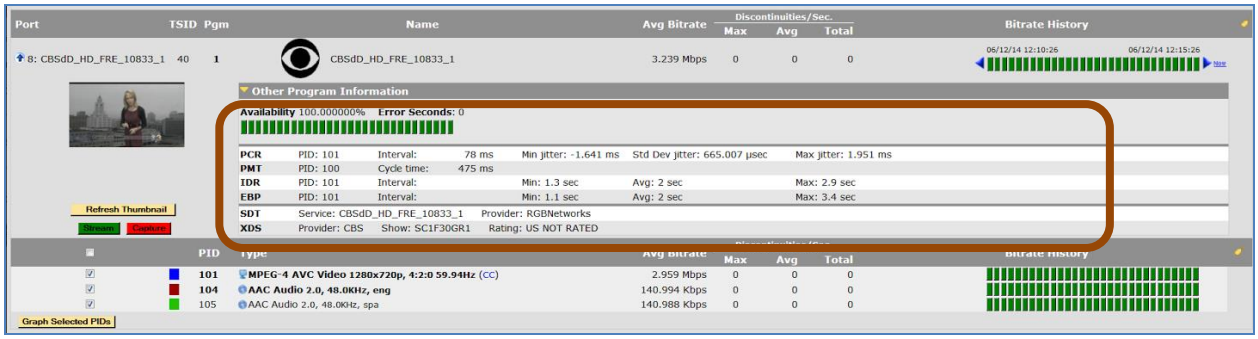


Figure 39: Program Availability and Other Program Information

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

Quality of Experience Details

The **Quality of Experience (QoE)** details allow 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 he 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, he will leave the dial alone at the 100 setting.

However, should an event such as tiling, freezing, macro-blocking, etc, affect the quality of his viewing experience, he will turn down the dial. The fictional viewer will keep the dial turned down for a short time past when the picture recovers until his confidence starts to recover. As his confidence returns, he 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
- How frequently it occurs

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

Figure 40: 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 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.

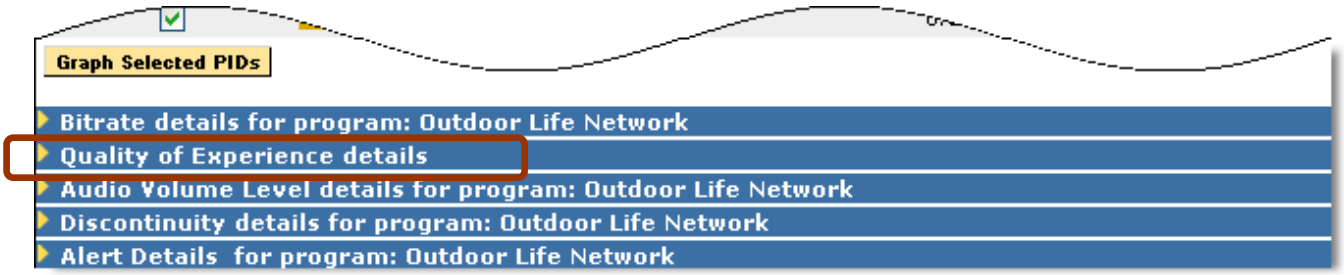


Figure 41: Expanding the QoE region

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.

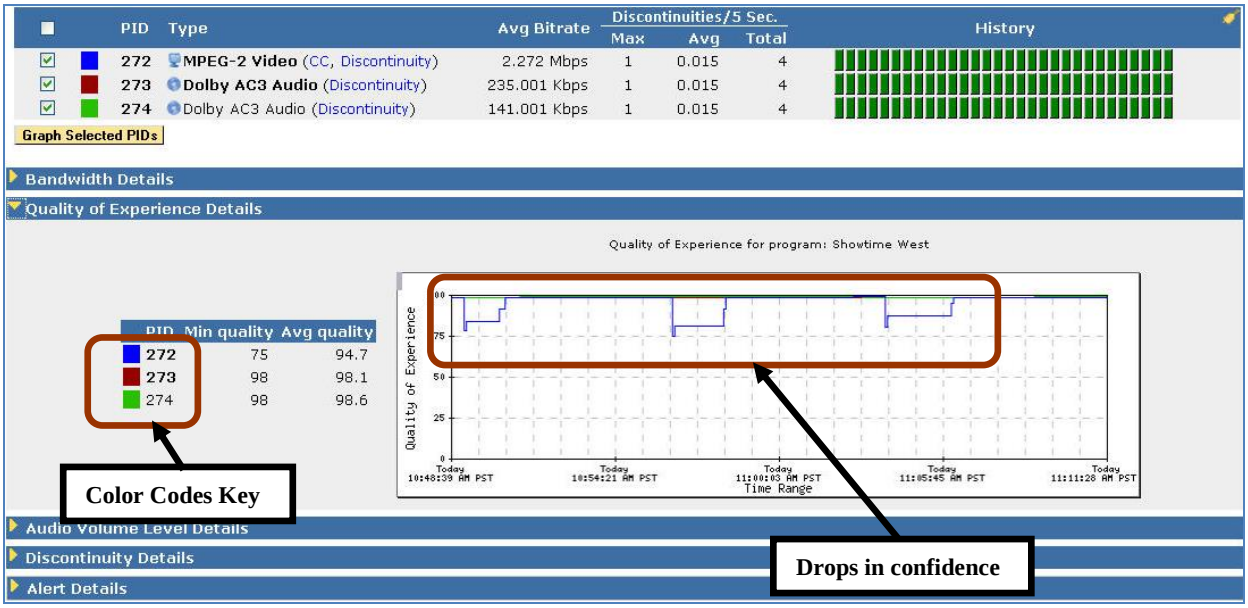


Figure 42: Expanded Quality of Details Region Graphing a blue coded 272 PID

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 at the top of the report.

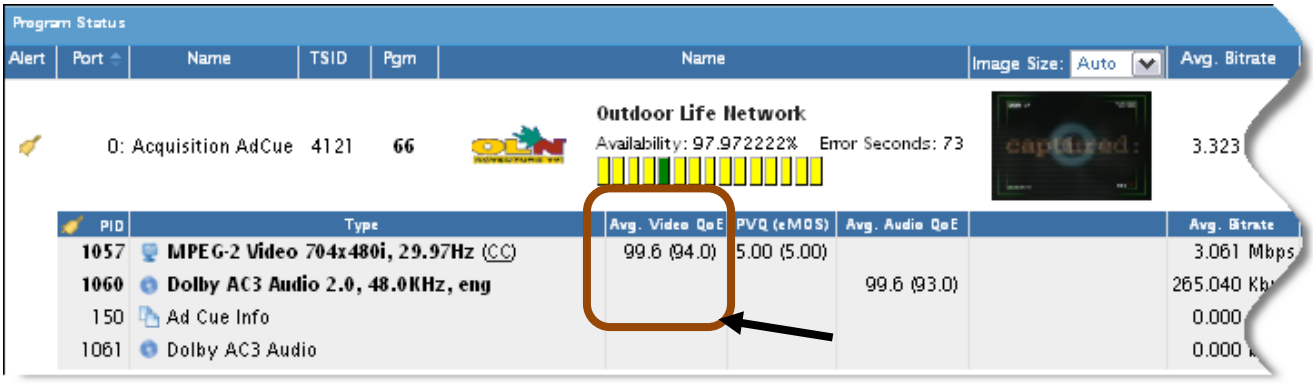


Figure 43: Average Video QoE column

Scoring QoE

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

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.

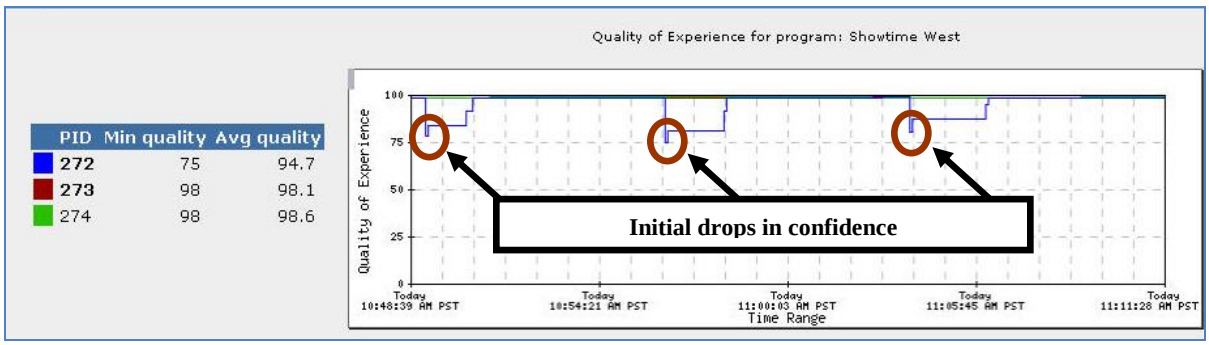


Figure 44: Quality of Experience Graph showing the initial drops in confidence

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.

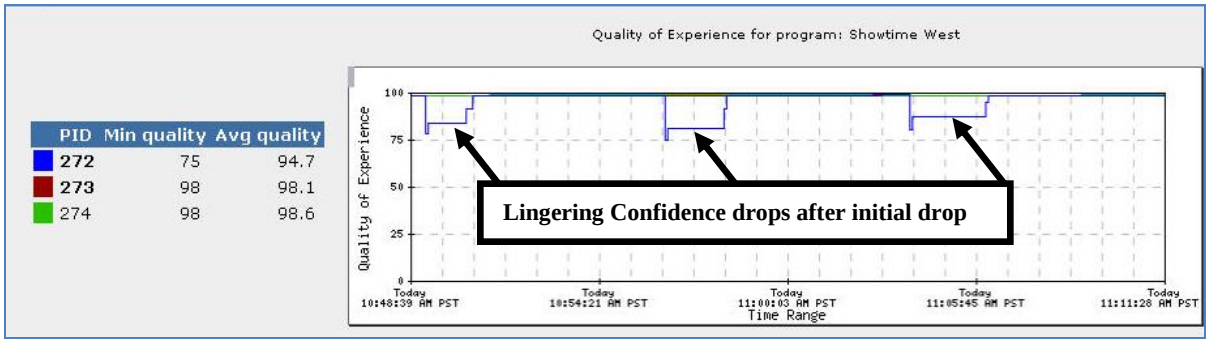


Figure 45: Lingering confidence drops, not necessarily a continuing issue

In addition to displaying the QOE scores, Sentry 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.

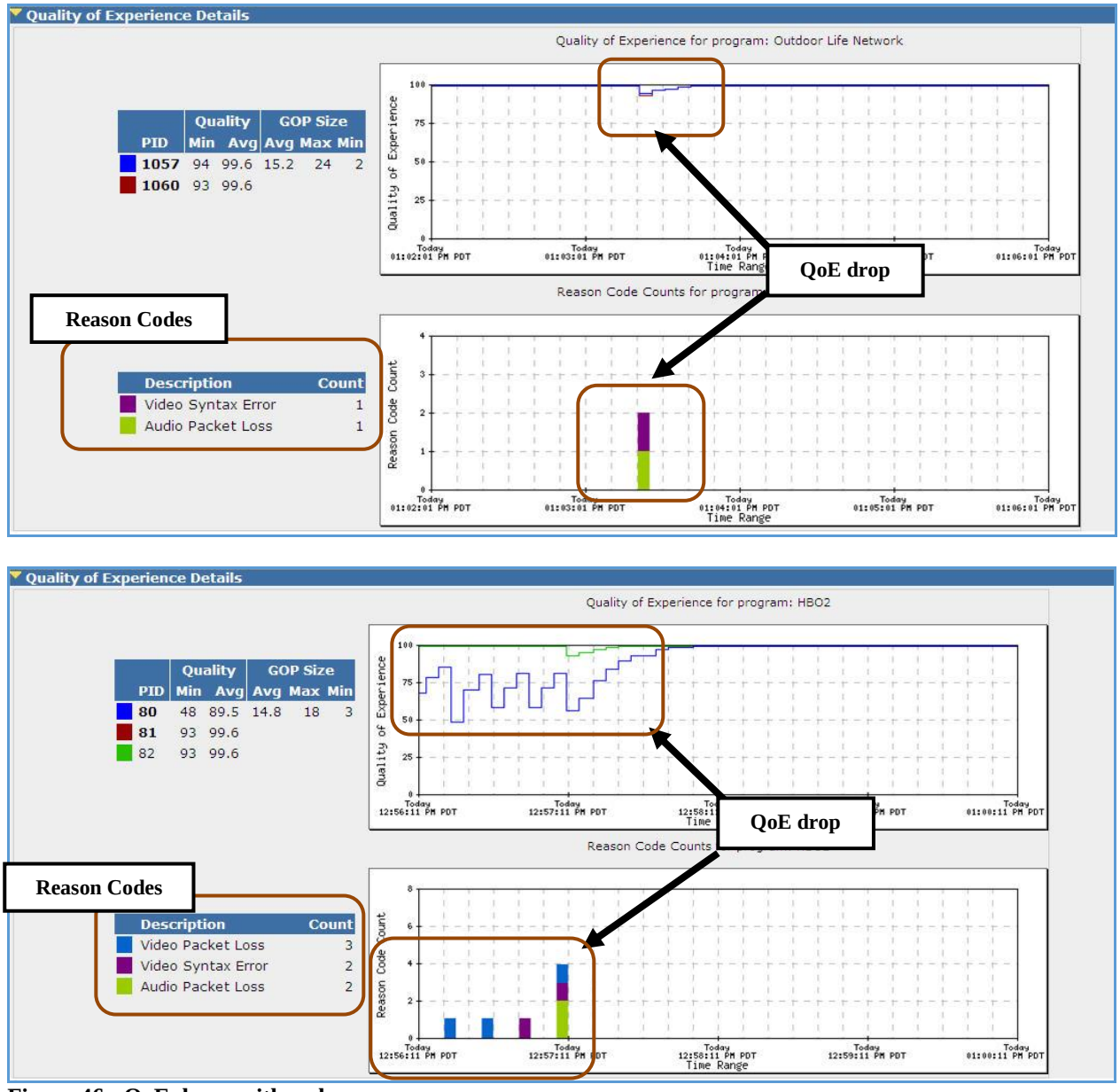


Figure 46: QoE drops with codes

Reason codes are also added to the **SNMP QOE** alert notifications.

Reason Codes Definitions

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 drop more than 20% in 5 seconds. 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 Buffer Overrun	A video frame's DTS value was > 3 seconds for MPEG-2 or > 5 seconds for H.264 behind the current PCR resulting in a decode buffer overrun.
Video Buffer Underrun	A video frame's DTS value was >= the current PCR resulting in a (decode) buffer underrun.
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. 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.
Video Syntax Error	An unexpected state occurred while decoding video slice data.

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.*

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.

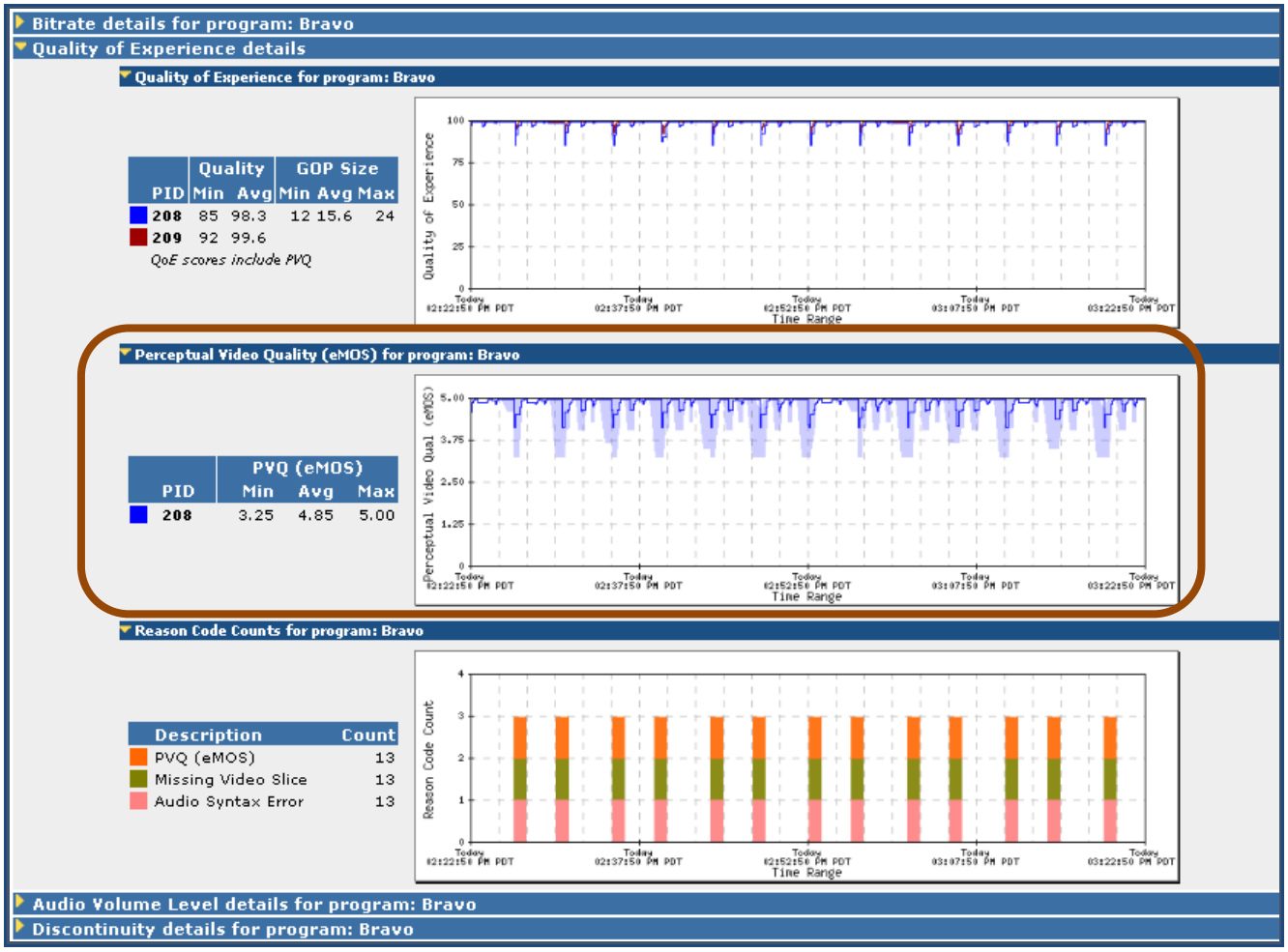


Figure 47: Perceptual Value Quality(eMOS) drops

There are two primary uses for video quality monitoring:

- **Real time alerting:**
  Use 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 (e.g., 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**
  Use Sentry Program Statistics (non-alert based) report for quantitative analysis. Use Sentry 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.

Sentry can accurately detect these non-error-related video artifacts 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.

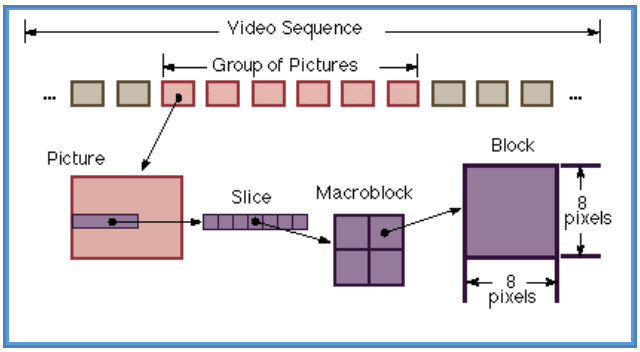


Figure 48: GOP, Picture, Slice, and Macroblock

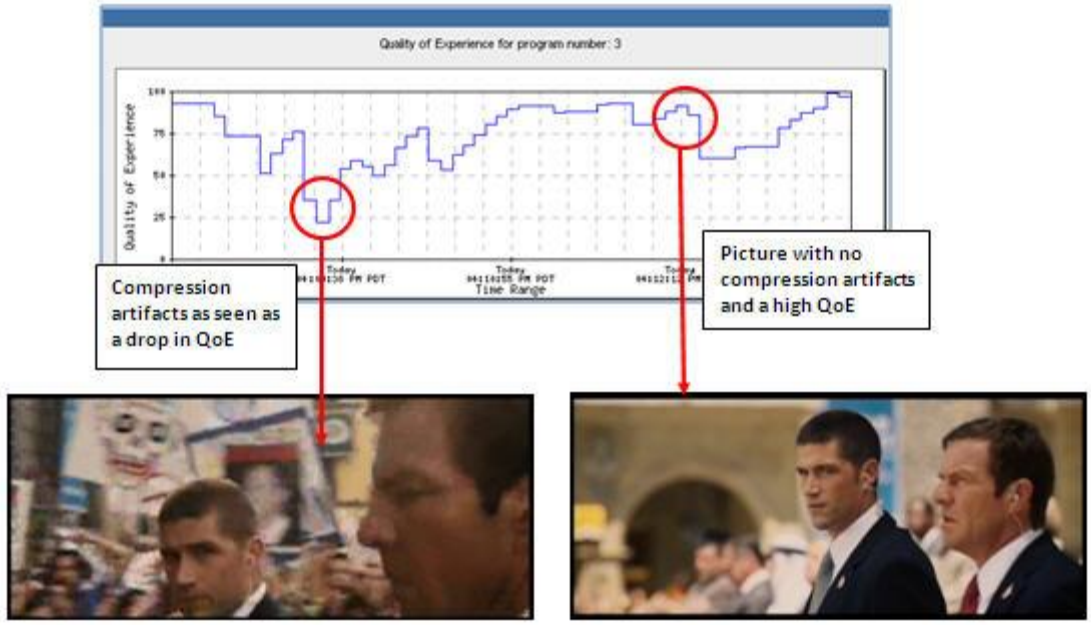


Figure 49: Picture on the left shows compression artifacts in the background and the picture on the right shows clear of compression artifacts.

Group of Pictures (GOP) Length Reporting (Group of Pictures)

The **GOP (Group of Pictures) Size** table displays the **Average**, **Maximum**, and **Minimum GOP** size for the specified time period.

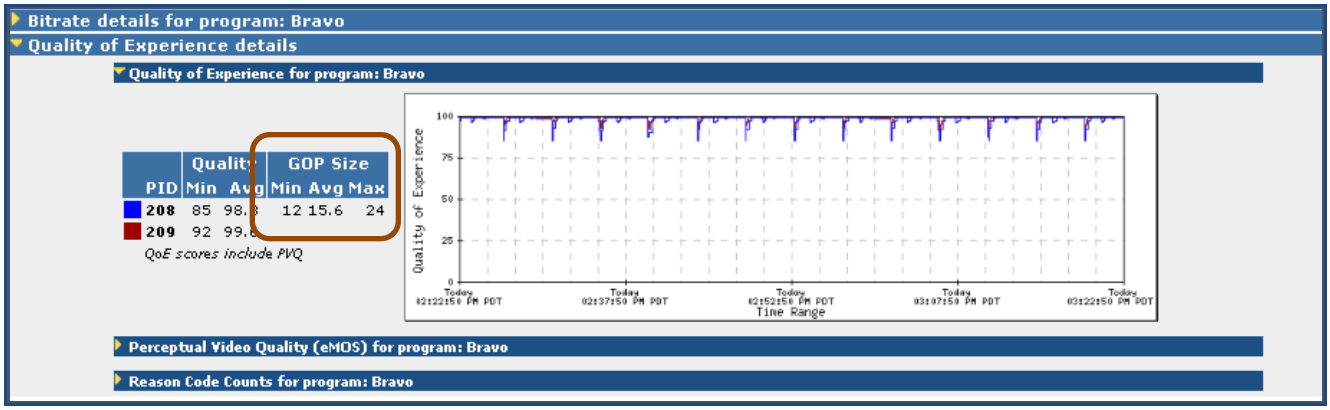


Figure 50: GOP display

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. Sentry will monitor and report this problem so it can be adjusted by the operator.

This function differs from 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.***

Audio loudness measurement is supported on the following audio codecs:

- AC3
- E-AC3 (Dolby Digital Plus)
- AAC
- HE-AAC v1 and v2
- MPEG-2

Access Audio Level Details

1. Select the logo/name of the desired program from any 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.

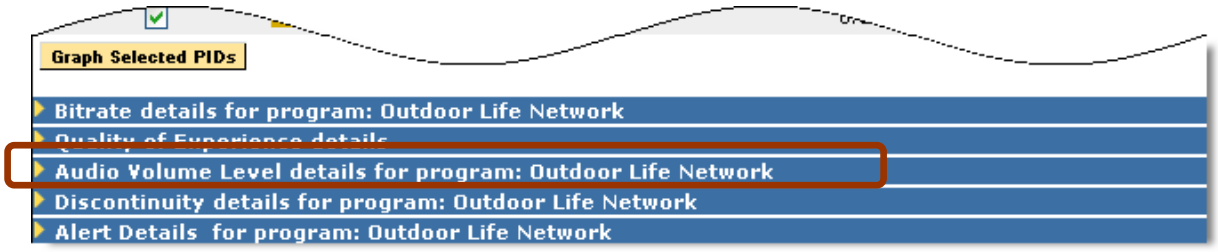


Figure 51: Expanding the Audio Volume Level Details region

Graphing

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

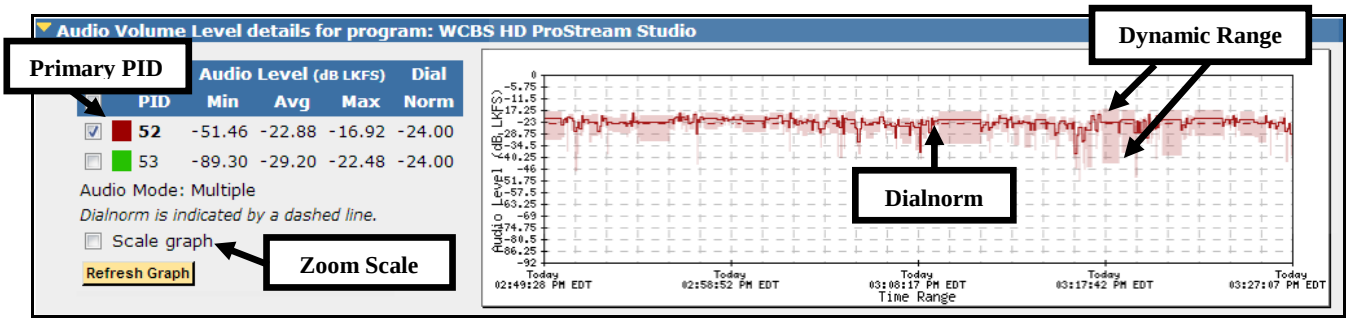


Figure 52: Audio Levels

- **Dashed line**
  Represents the **Dialnorm** level that is specified in this audio stream.
- **Solid line**
  Represents the weighted average audio level.
- **Shaded area**
  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 shaded areas are not markers of time, but rather markers of the minimum and maximum audio levels.

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.

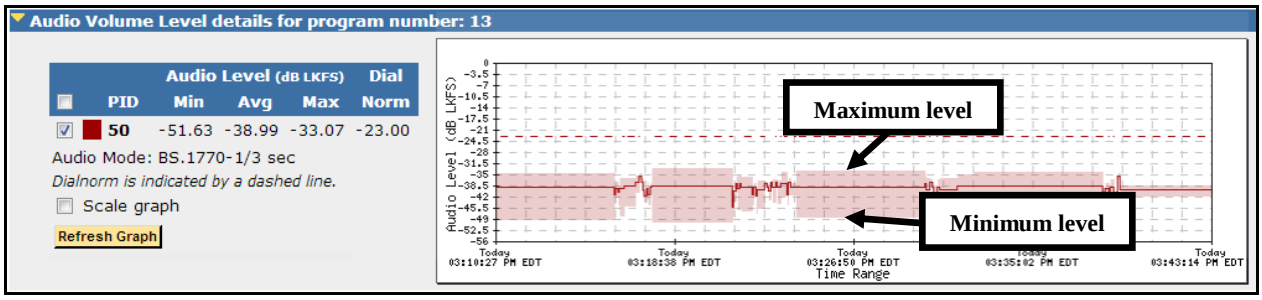


Figure 53: Audio Levels with poor volume

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.

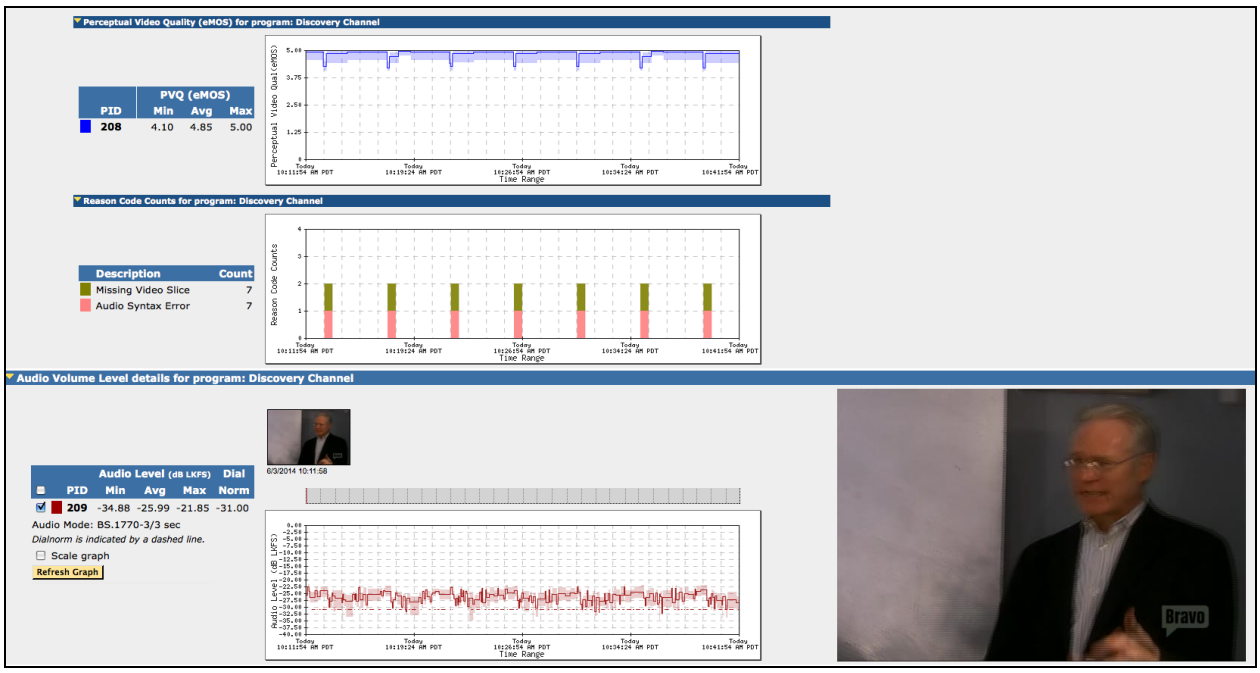
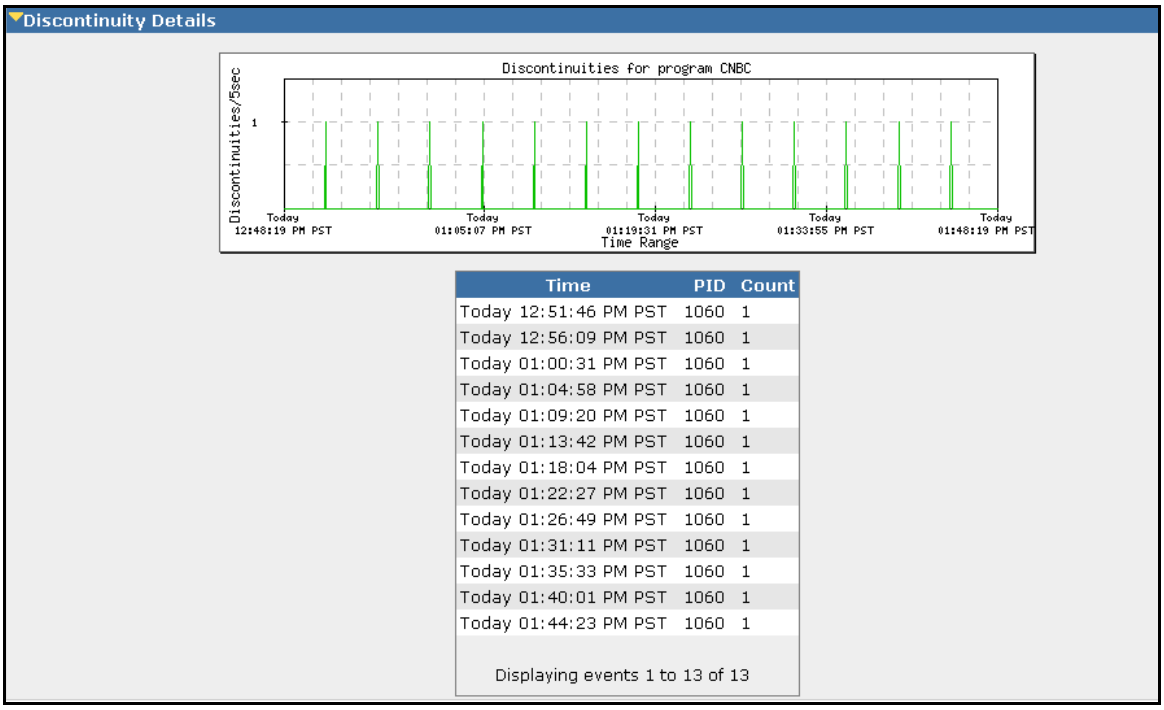


Figure 554: Thumbnail Timeline

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.



Time	PID	Count
Today 12:51:46 PM PST	1060	1
Today 12:56:09 PM PST	1060	1
Today 01:00:31 PM PST	1060	1
Today 01:04:58 PM PST	1060	1
Today 01:09:20 PM PST	1060	1
Today 01:13:42 PM PST	1060	1
Today 01:18:04 PM PST	1060	1
Today 01:22:27 PM PST	1060	1
Today 01:26:49 PM PST	1060	1
Today 01:31:11 PM PST	1060	1
Today 01:35:33 PM PST	1060	1
Today 01:40:01 PM PST	1060	1
Today 01:44:23 PM PST	1060	1

Displaying events 1 to 13 of 13

Figure 55: 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.

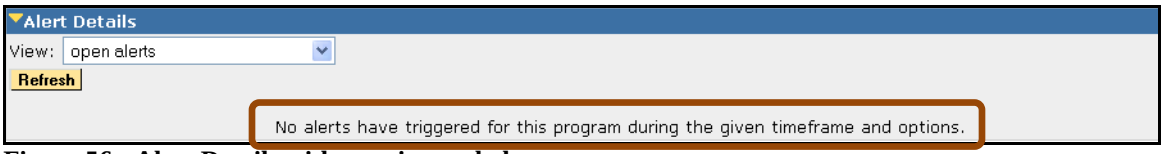


Figure 56: Alert Details with no triggered alerts

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 57: 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.

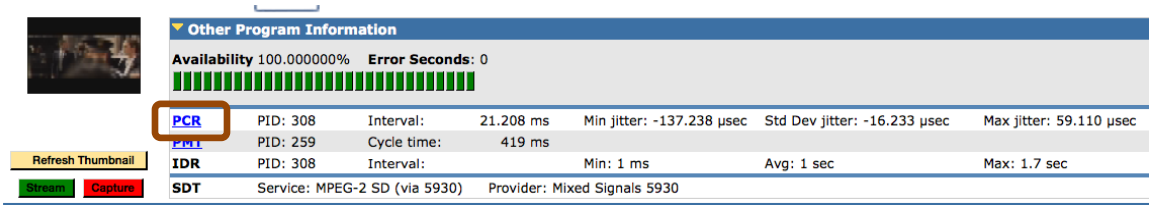


Figure 58: Program Detail report

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 59: PCR 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.

Data Detect

The **Data Detect** report is a detailed report on specific content within the MPEG transport stream.

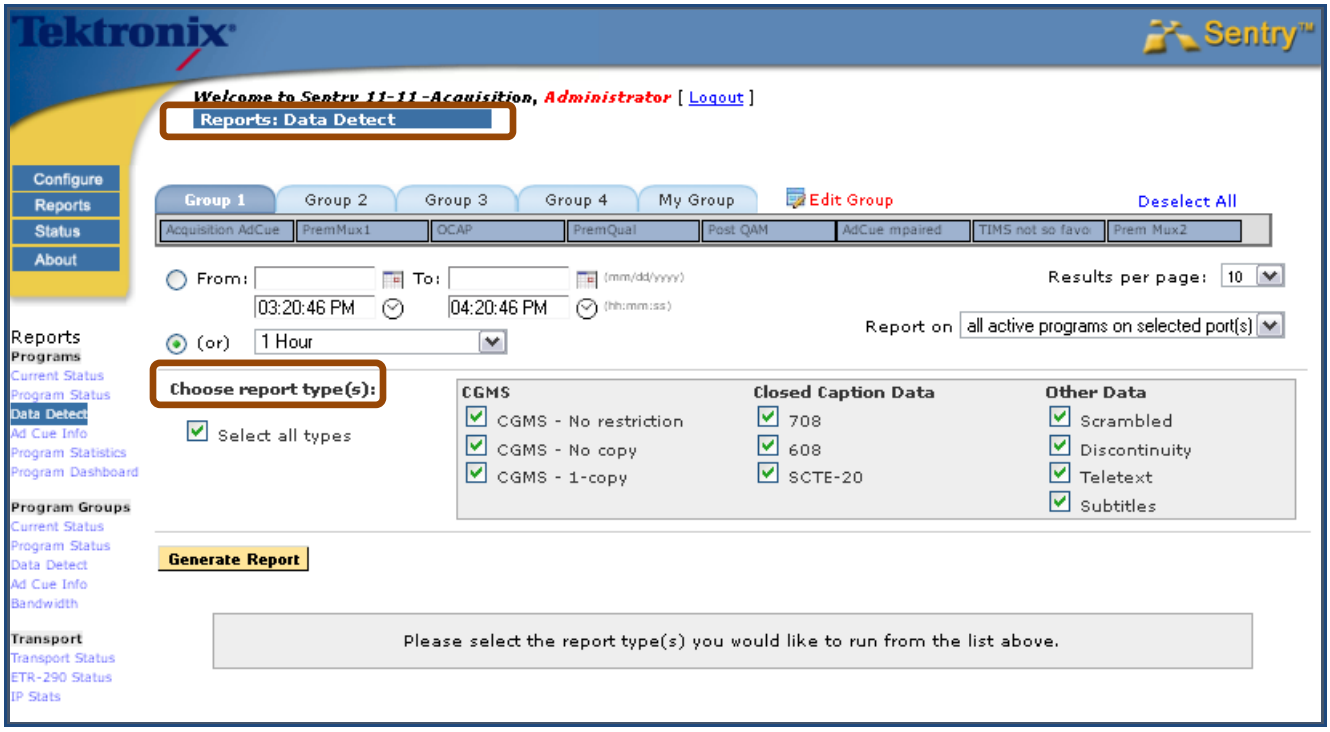


Figure 60: Data Detect Report Types

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 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

From this report, you can select **CEA-608**, **CEA-708**, and **SCTE-20 Closed Captioning** reporting, in addition to the existing **Closed Captioning** options. You can also configure new **Program Alerts** to monitor and report occupancy and error rates for these standards.

- **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 bitstreams. This method is favored by North American cable operators to encode traditional VBI line-21 (EIA-608) closed captioning into digital cable MPEG bitstreams.

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

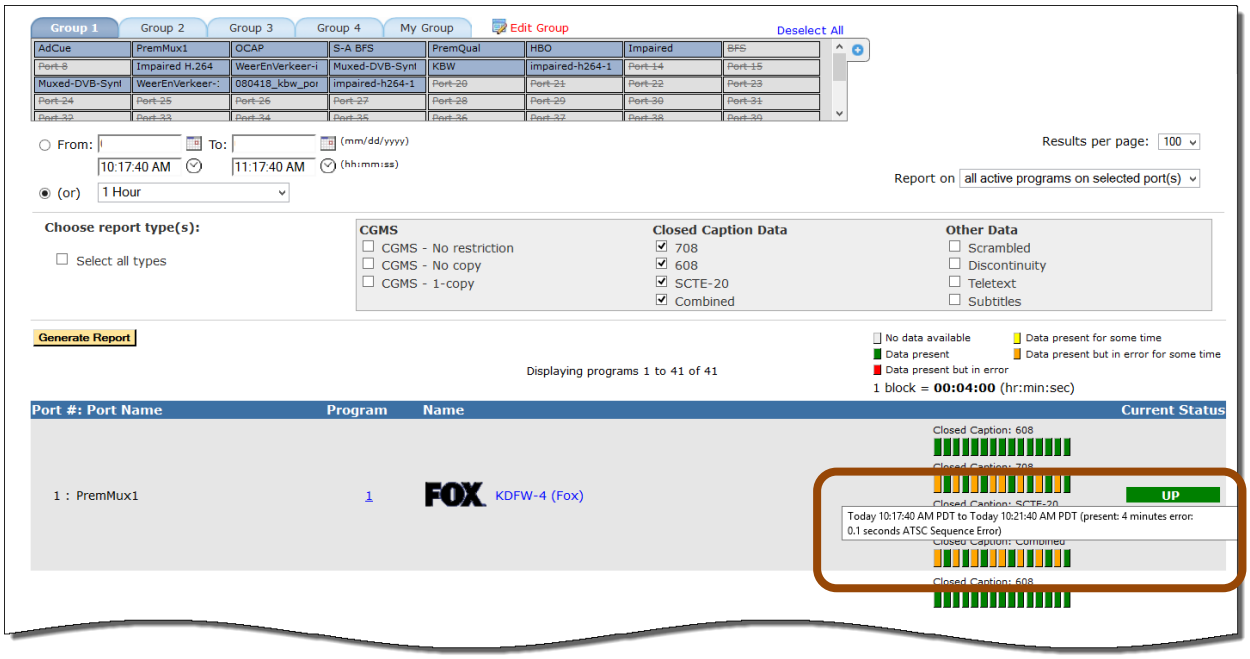


Figure 61: Hover your pointer over any orange or red block to see the closed caption errors

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.

Generate a Report

The **Data Detect** report displays a status key to display the detection of **Closed Captioning** errors, in addition to the current tiles indicating the detection of **Closed Caption** data. It also supports reporting the percentage of invalid and partially invalid **Closed Captioning** data.

1. After choosing the report type, select **Generate Report** to view the report based on the criteria you have selected.

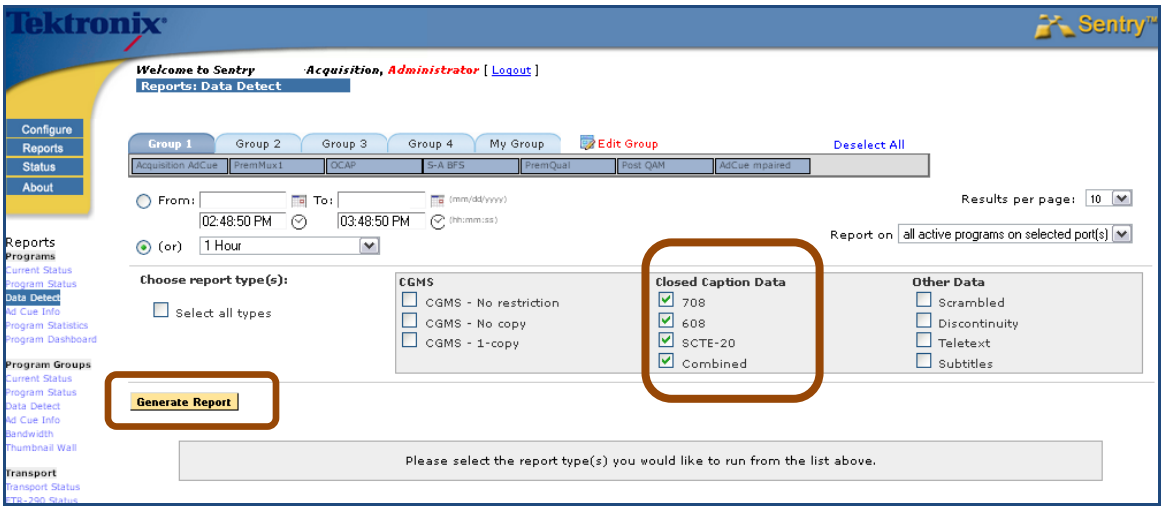


Figure 62: Data Detect Report

2. From screen you can see the status key and the closed captioning status.

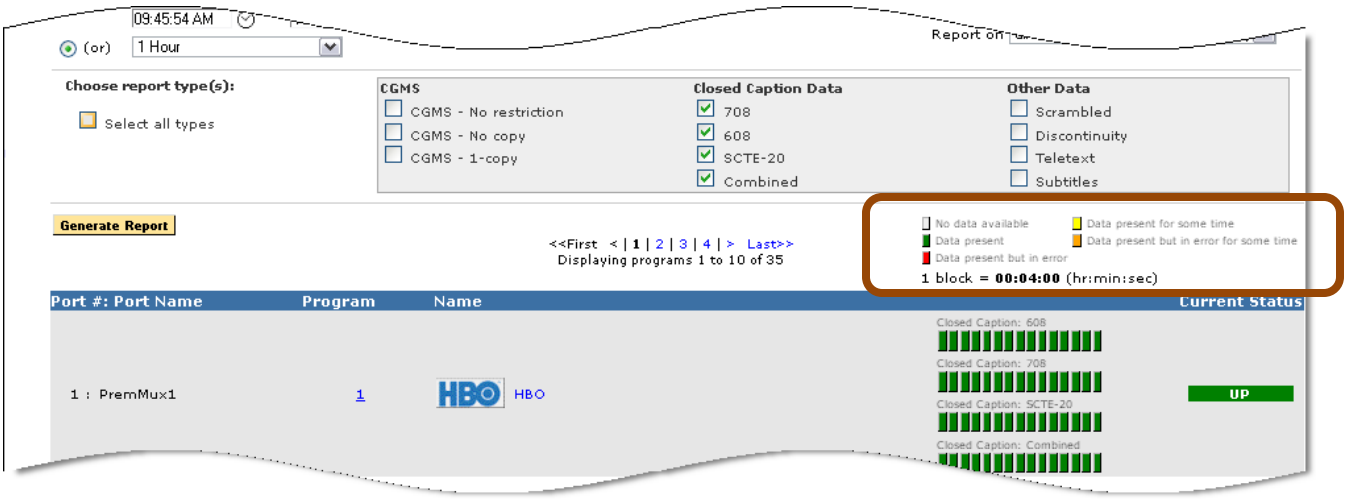


Figure 63: Data Detect Report

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

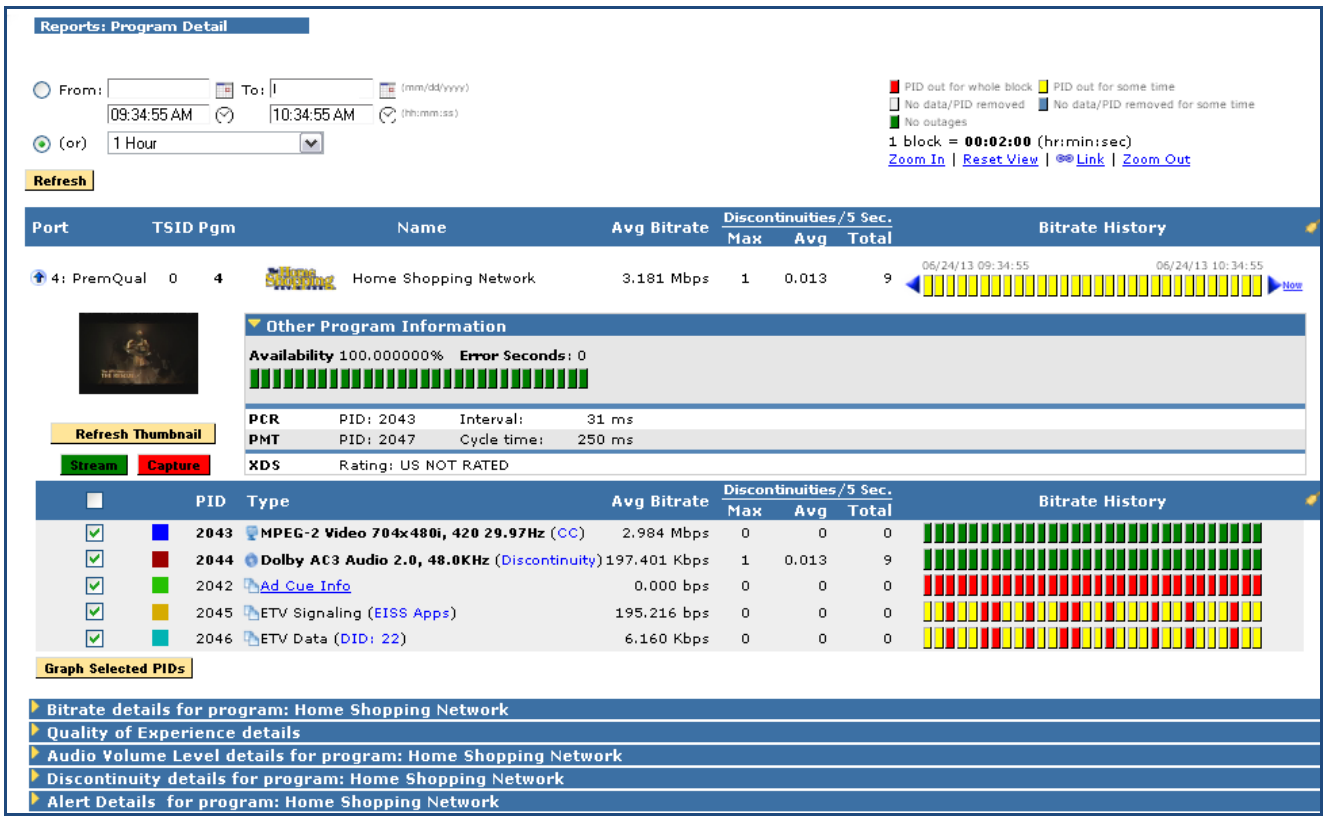


Figure 64: Program Detail from the Data Detect Report

4. 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, i.e., **CC**, **CGMS**, and **Discontinuity**.

5. 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, Sentry 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. To view the commands that Sentry monitors, select **Reports** and then **Programs: Ad Cue Info** from the main page menu.

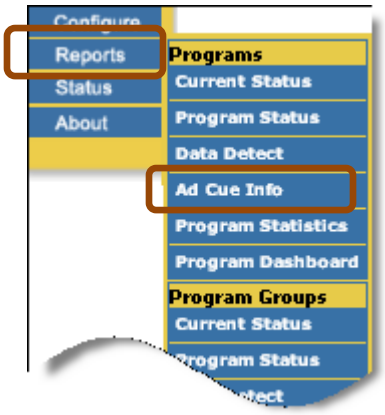


Figure 65: Ad cue Info menu

2. Next, select the time range of interest.

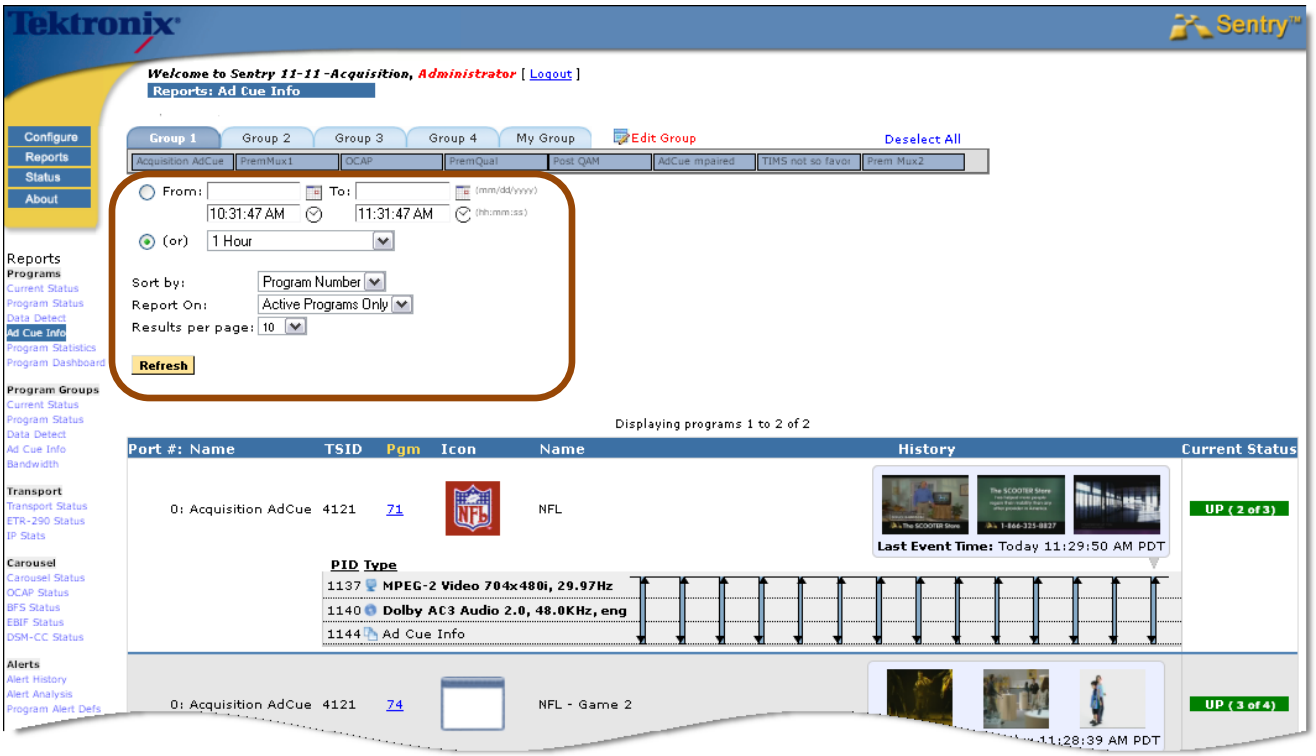


Figure 66: Ad Cue Info Welcome

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

4. 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!

Reading the Ad Cue Info report

Sentry 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 Sentry 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 displays 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.

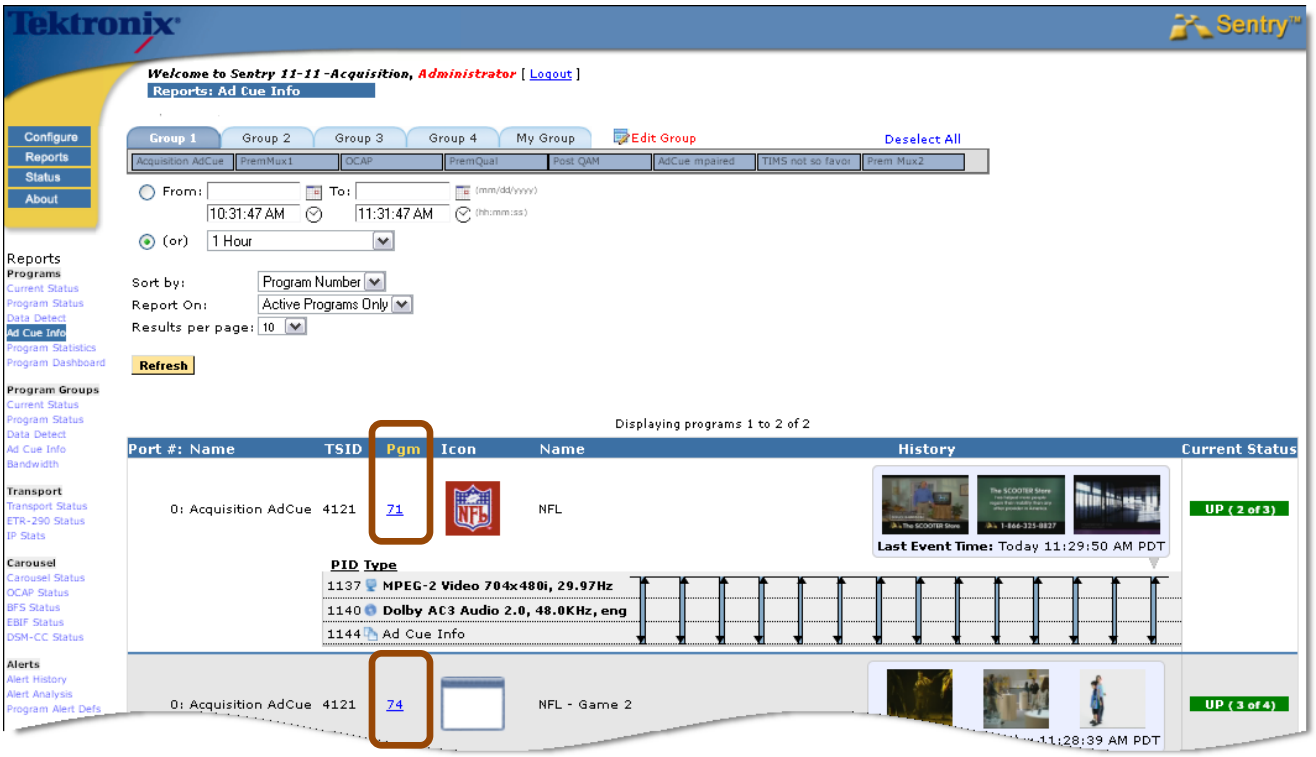


Figure 67: Ad Cue Info Report

Click on a program link in the **Pgm** column to view the details for the ads of the selected programs.

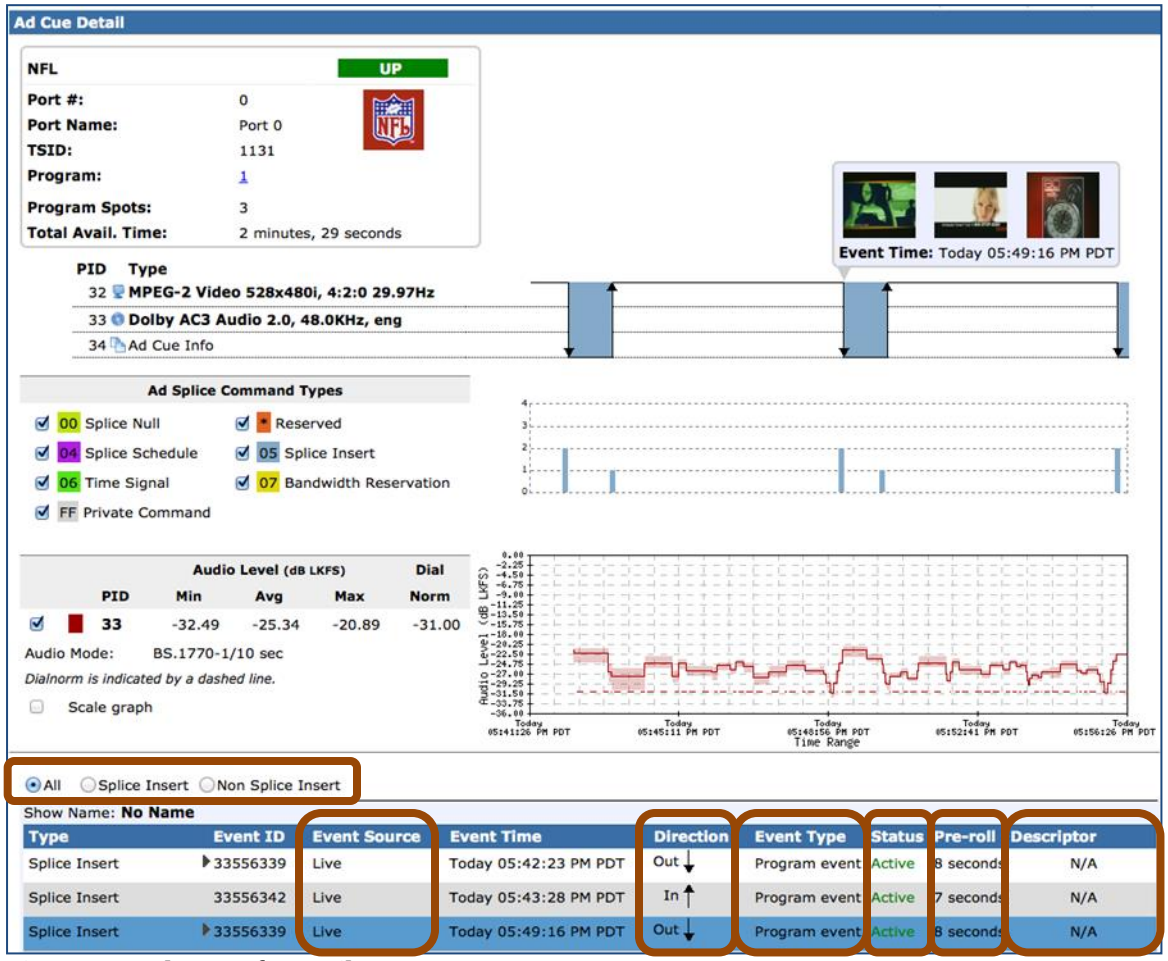


Figure 68: Ad Cue Info Detail Report

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.

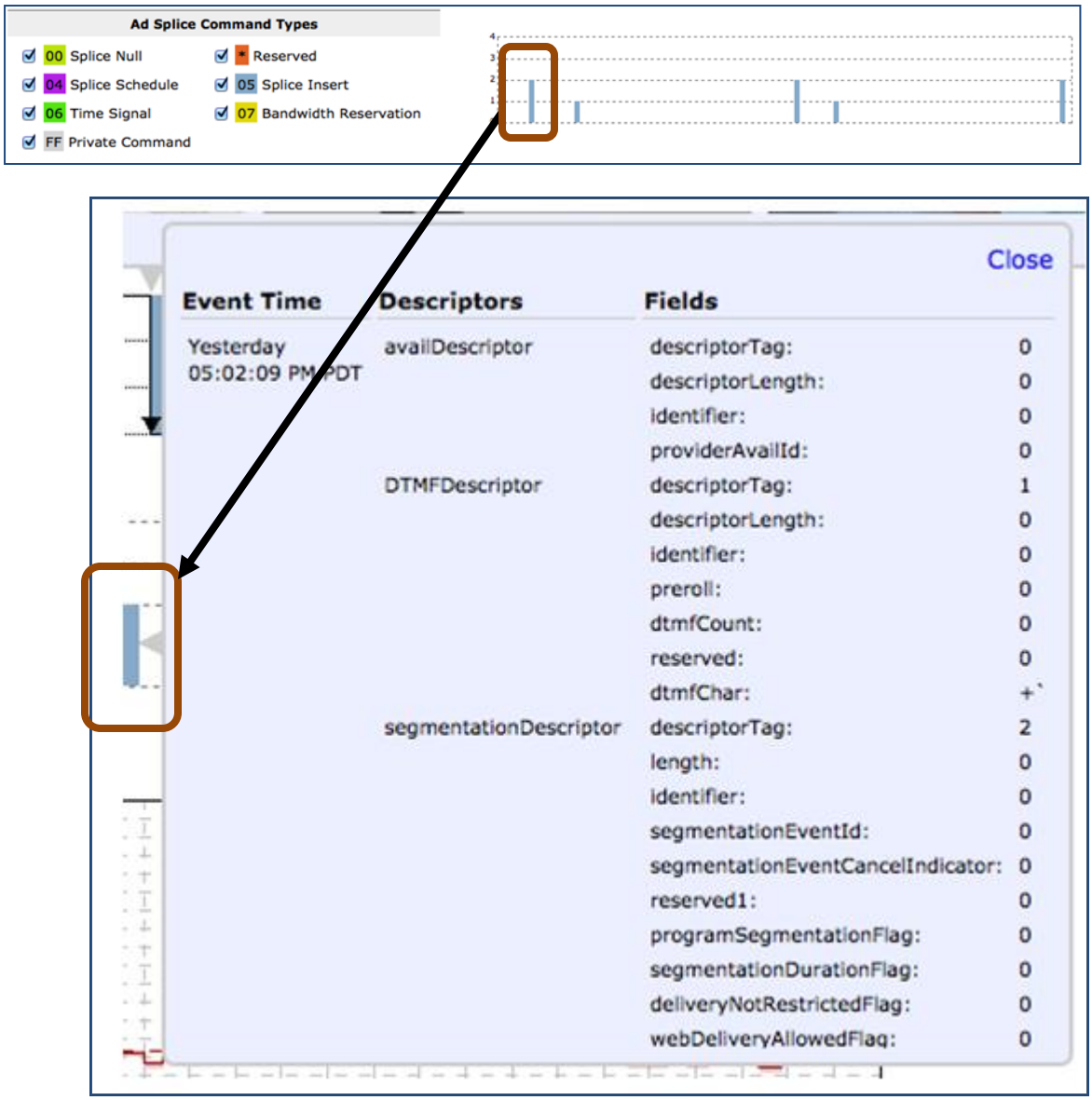


Figure 69: Hover over bar graph for Descriptor Information

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.

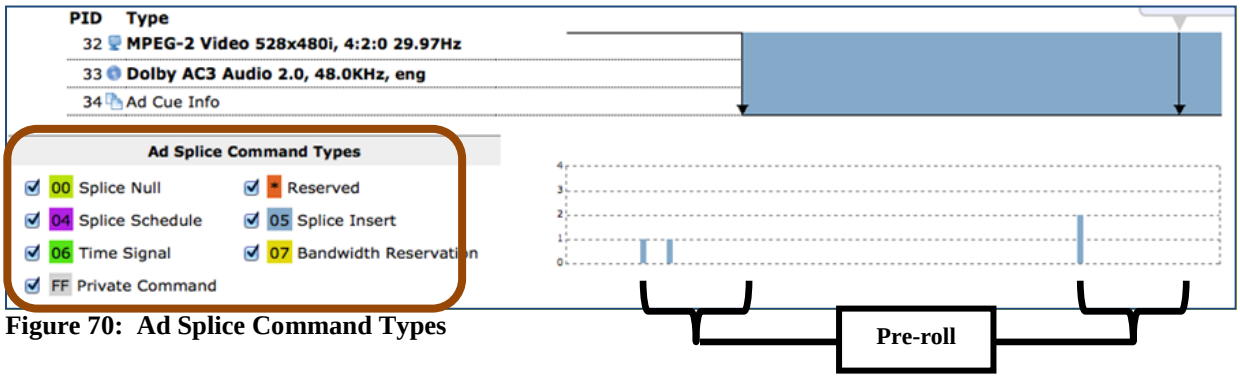


Figure 70: Ad Splice Command Types

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 71: 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.

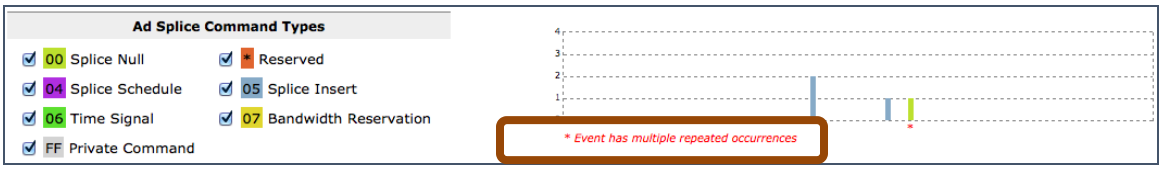


Figure 72: Asterisk showing there are multiple occurrences of the same command

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.

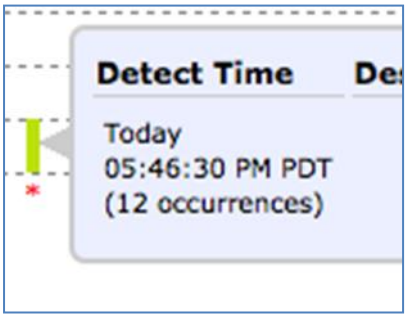


Figure 73: Descriptor information showing 12 occurrences of a command.

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

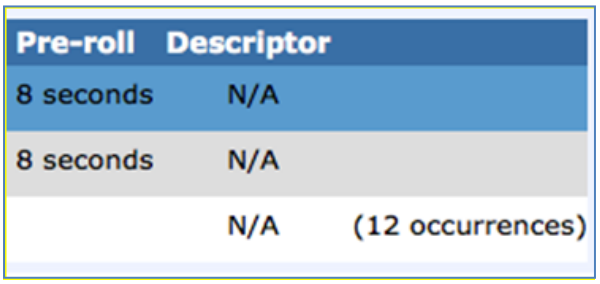


Figure 74: Multiple commands as shown in the report

Audio Level Graph

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

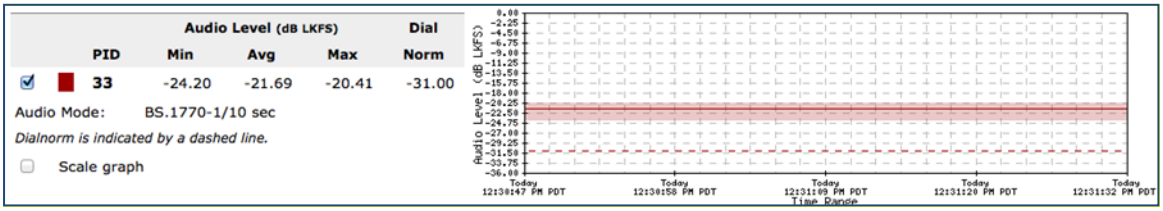


Figure 75: Audio Level Graph

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:

Select **Reports** and then **Program Statistics**.

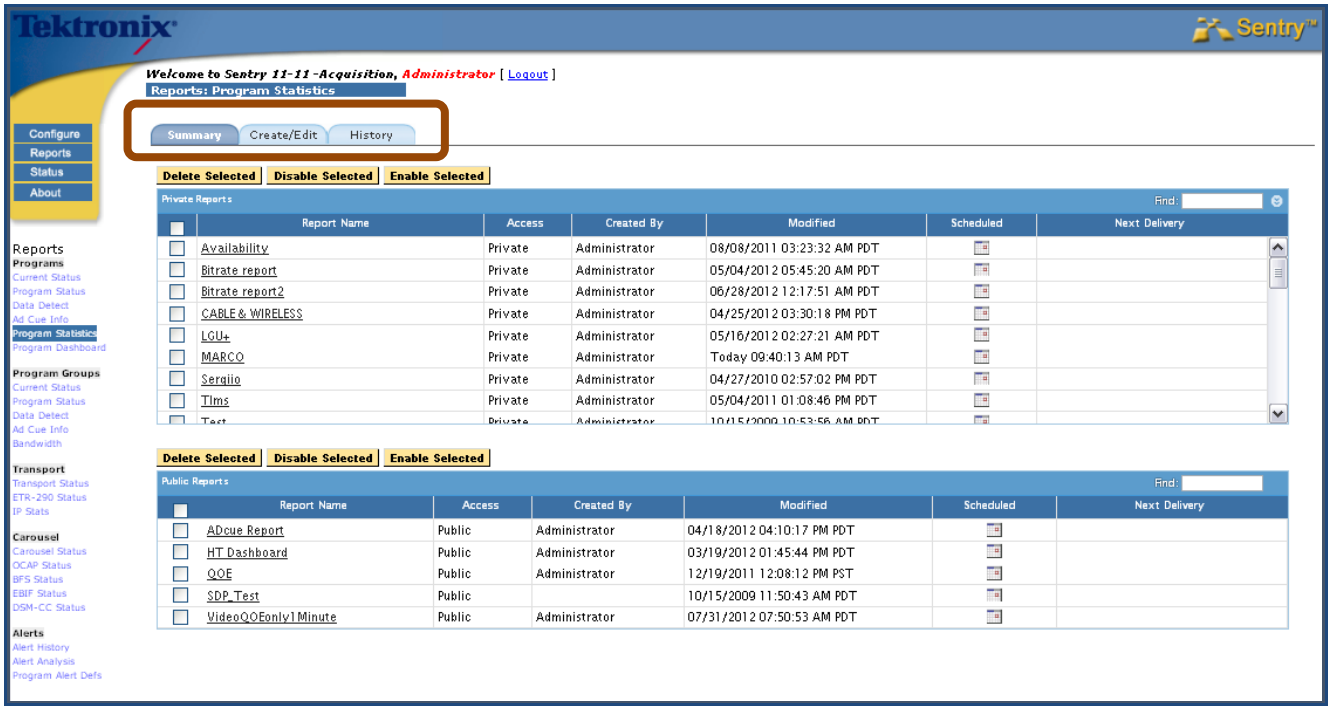


Figure 76: Summary, Create/Edit and History tabs

Tab View

Summary tab
Displays which reports have been created and saved.

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

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 and volume levels
- Totals for bitrate and discontinuities
- Maximum and minimum and averages of GOP length
- Maximum and minimum and averages of PVQ

Create a Program Statistics Report

1. Select the **Create/Edit** tab.

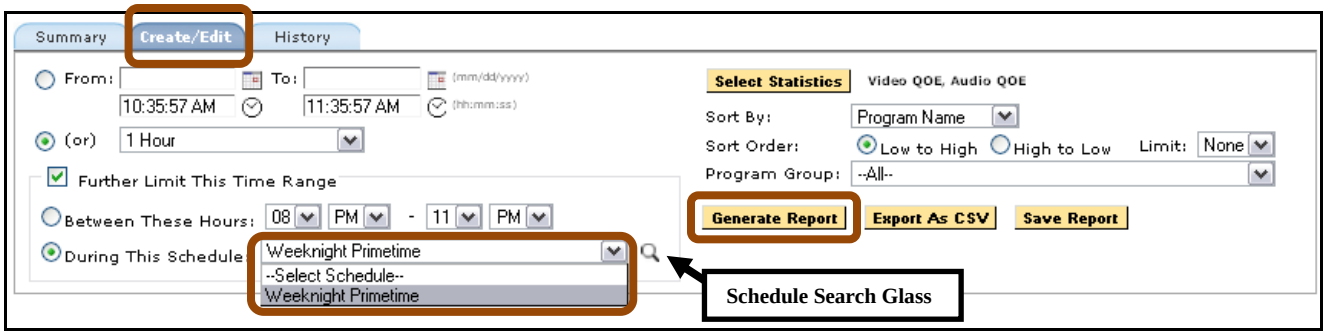


Figure 77: Generating a Statistics Report set up

2. Select your time frame.
   a. You can further restrict the time range by selecting **Further Limit This Time Range.**
   b. Select your desired schedule from the drop down menu. In this example we selected **Weeknight Primetime.**
   c. Select the **Search Glass** to see the selected schedule**. See Configure Schedules** for information on how to create schedules**.**

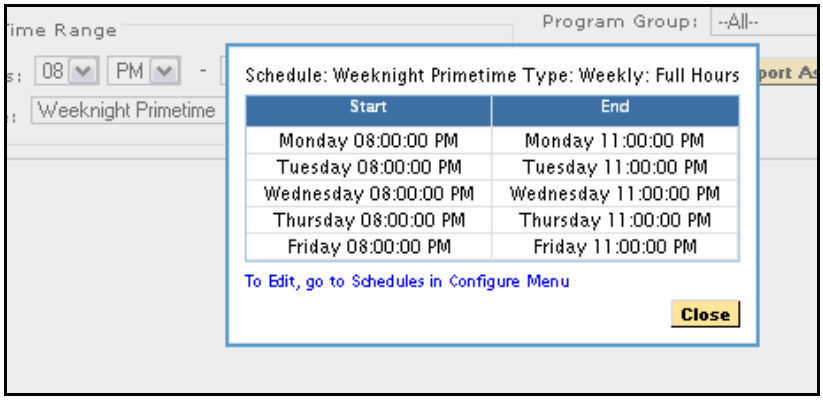


Figure 78: Weeknight Primetime schedule

3. Select the **Statistics** you want to view.
4. Sort and limit as desired.

5. Select **Generate Report**.
6. The **Displaying Program** box appears.
7. Review all data.
   a. Select column header to sort data.

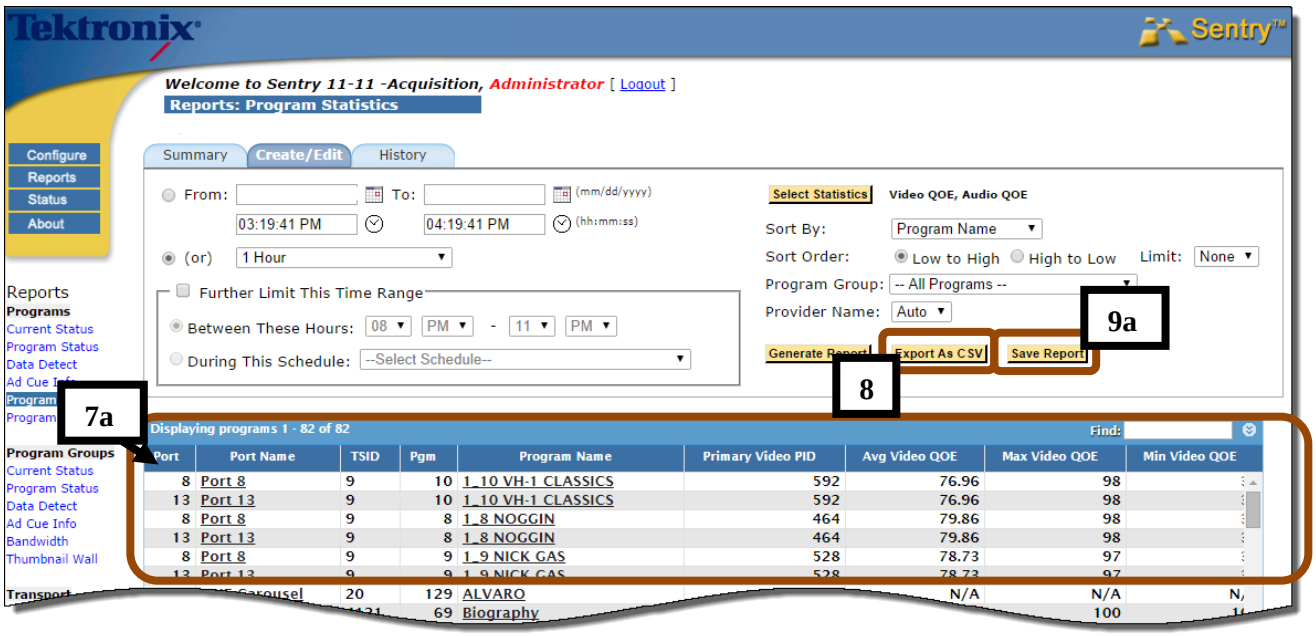


Figure 79: Exporting as CSV

8. 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.
9. When you are satisfied with the report output:
   a. Select **Save Report.** The screen will reload to show the save options.
   b. Name your **Report**.

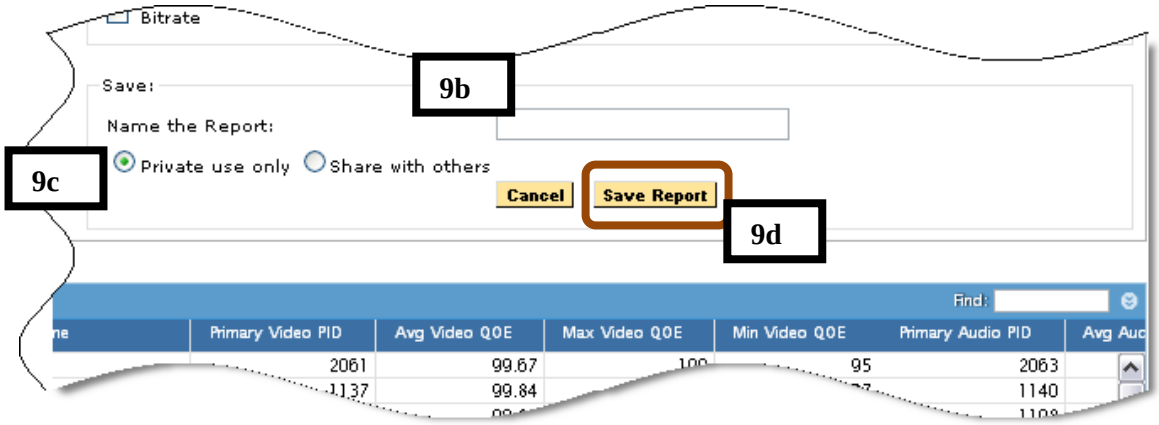


Figure 80: Saving the Report

c. Choose **Private use only** or **Share with others**.

d. Select **Save**.

10. 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.

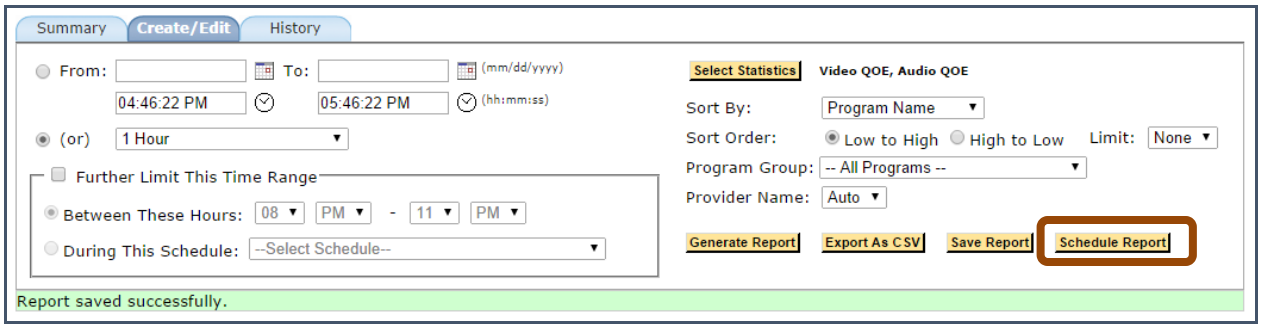


Figure 81: Scheduling the report

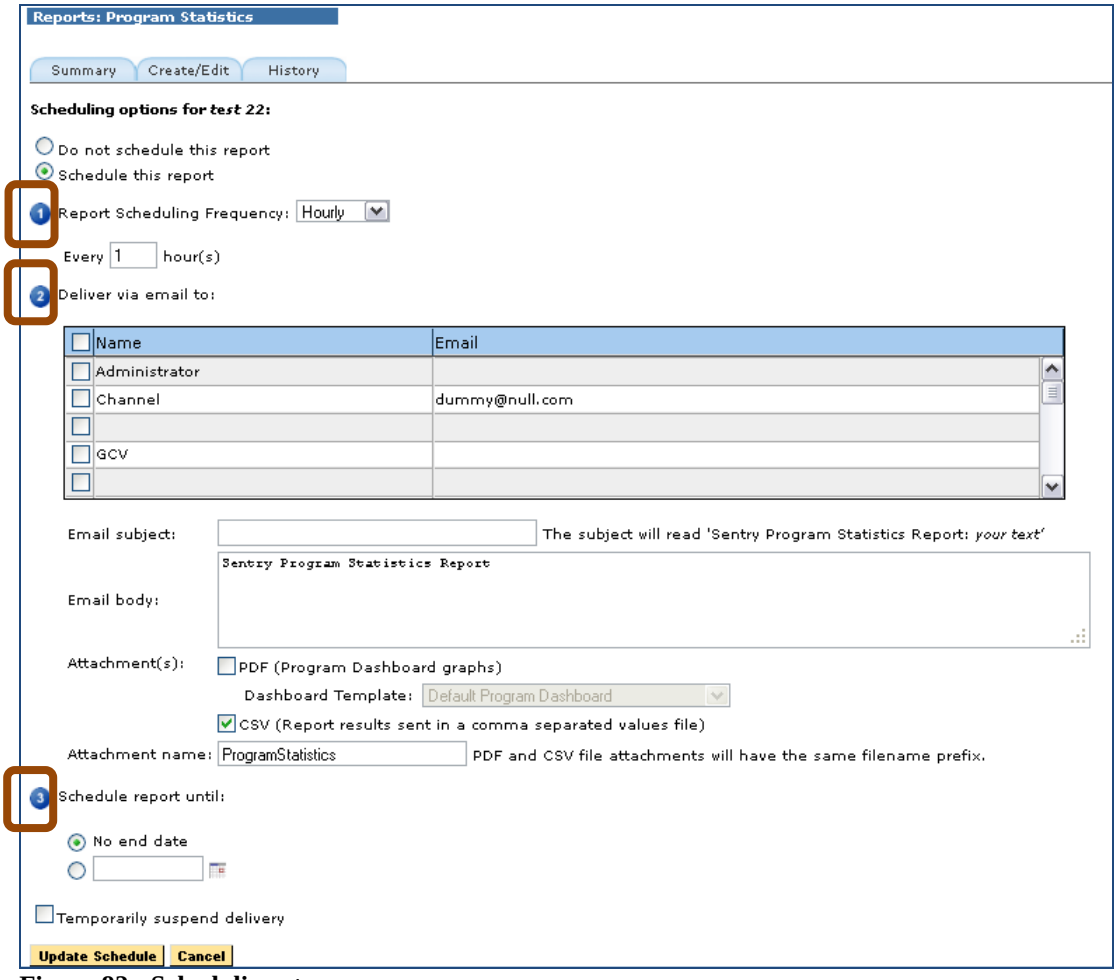


Figure 82: Scheduling steps

11. For **Step 3**, select who you want to email
12. Schedule how long you want the report to run.
13. Select **Update Schedule** when complete.

History tab

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

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

Port Statistics

Port Statisitics provides non-alert data on a port level that allows you to see information on the transport bitrate and other releveant statistics.

Summary tab

The **Summary tab** shows the list of **Public** and **Private** saved reports.

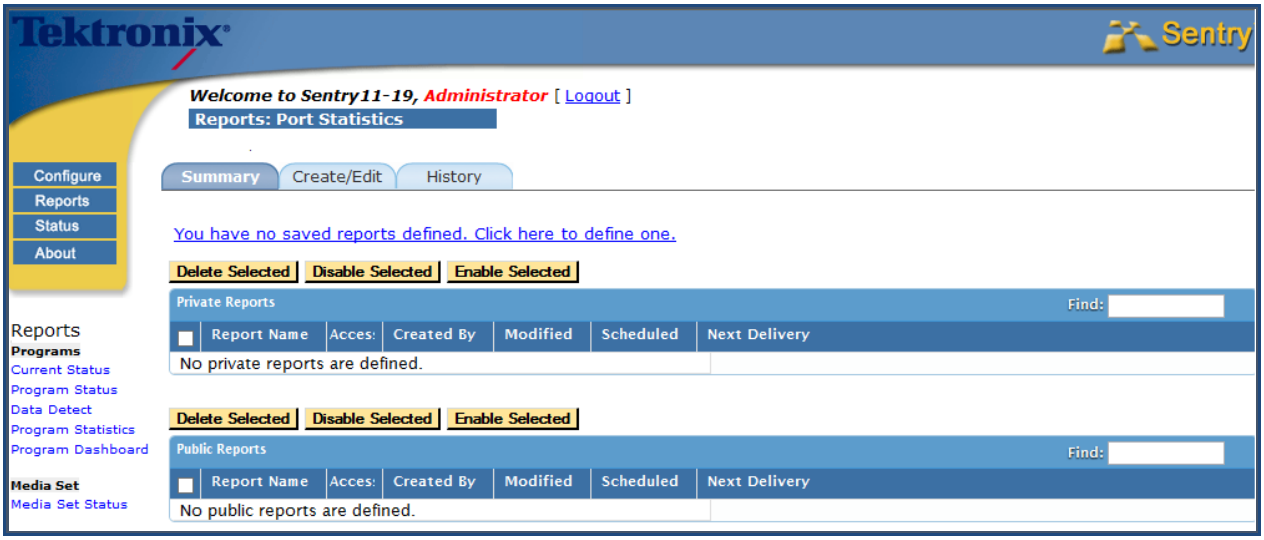


Figure 83: Port Statisitics

Create a Port Statistics Report

1. Select the **Create/Edit tab.**
2. Choose date/time frame for your report.
3. Select **Statistics.**

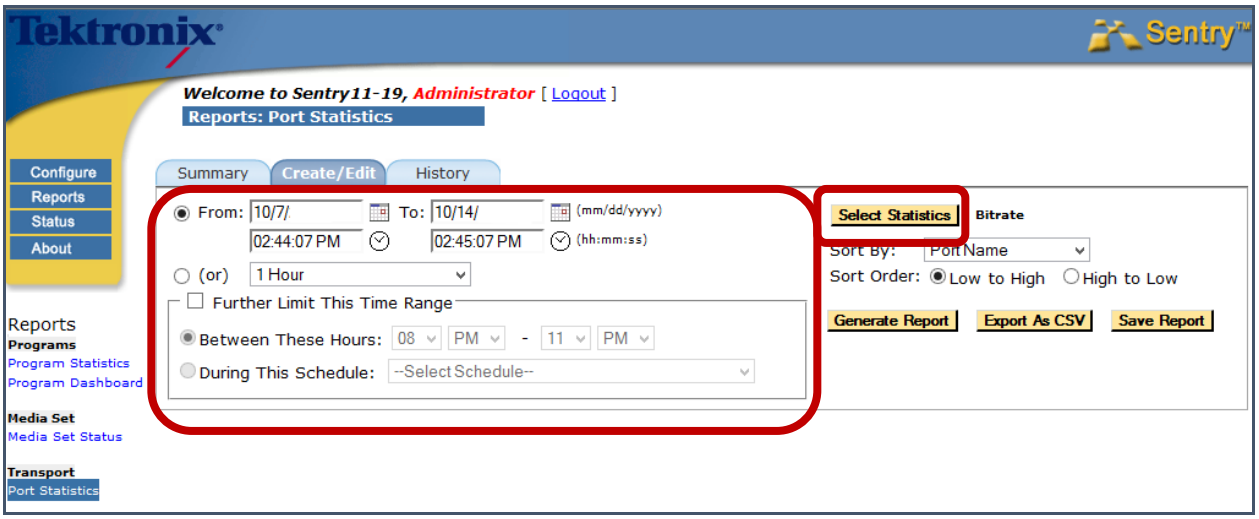


Figure 84: Setting the date or time range

4. Choose any **Statisitics** you to include.
5. Select **Accept.**

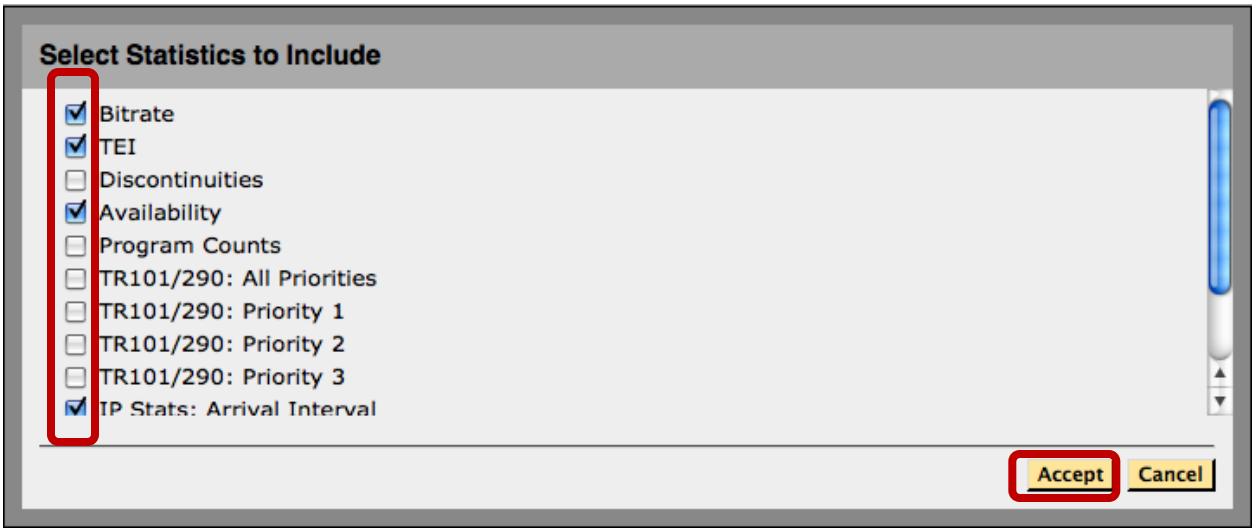


Figure 85: Secting the statistics to include

6. Select any other filter filters you wish to apply.

7. Select **Generate Report**.

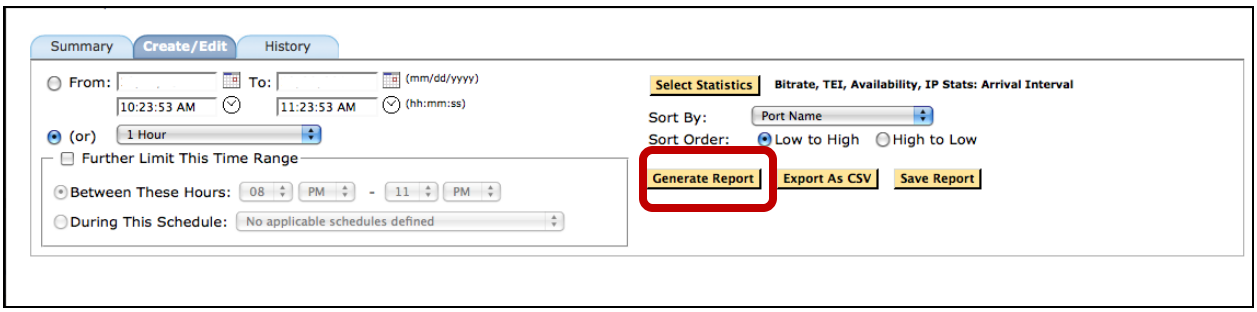


Figure 86: Generate the report

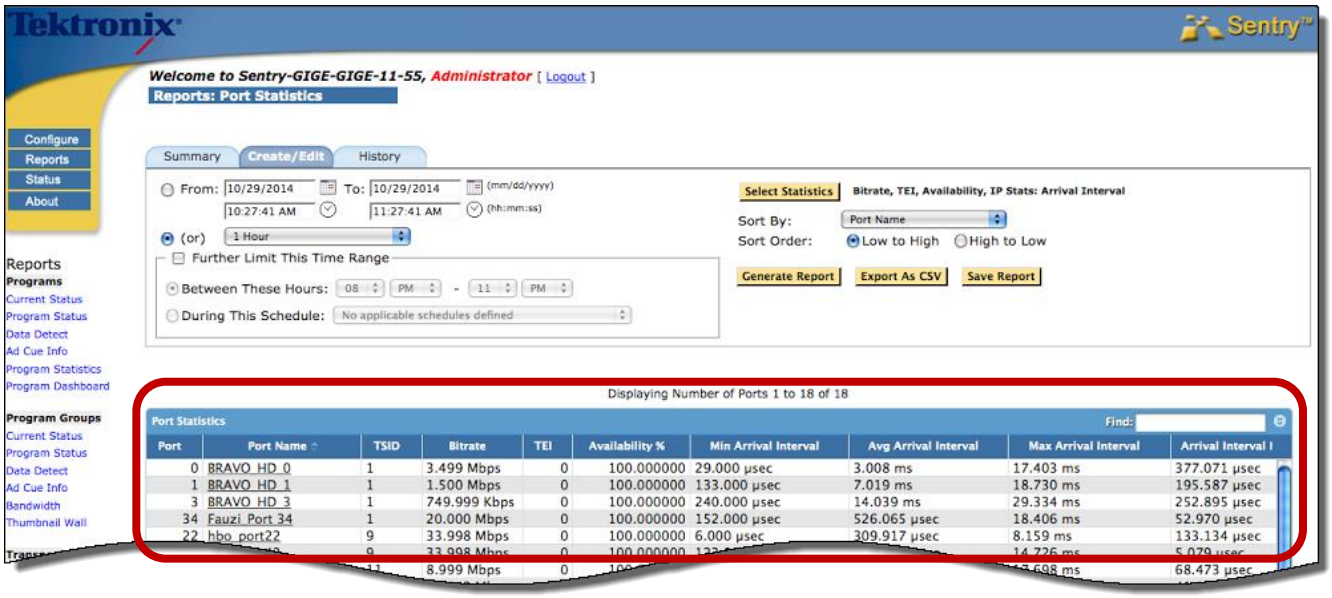


Figure 87: Port Statisitics displayed

Program Groups

Program Groups allows you to customize any programs on Sentry as a group for convenient alert template application and for problem isolation. For example you can create **Program Groups** by their content type (music program group, HD program group) for applying the most appropriate type of alert. If Sentry is set up to monitor the same programs at different locations (e.g., acquisition vs. post multiplexing), you can create two program group respectively by different location for comparison and for problem isolation.

For more info on the **Program Status**, **Data Detect** and **Ad Cue Info** reports, see the respective sections in **Programs**.

Using Program Groups

Program Groups have several additional functions once they have been created. Our example below, **Current Status**, is just one of the many reports that can be used.

1. From the **Reports** toolbar, select **Current Status** under the **Program Groups** header.

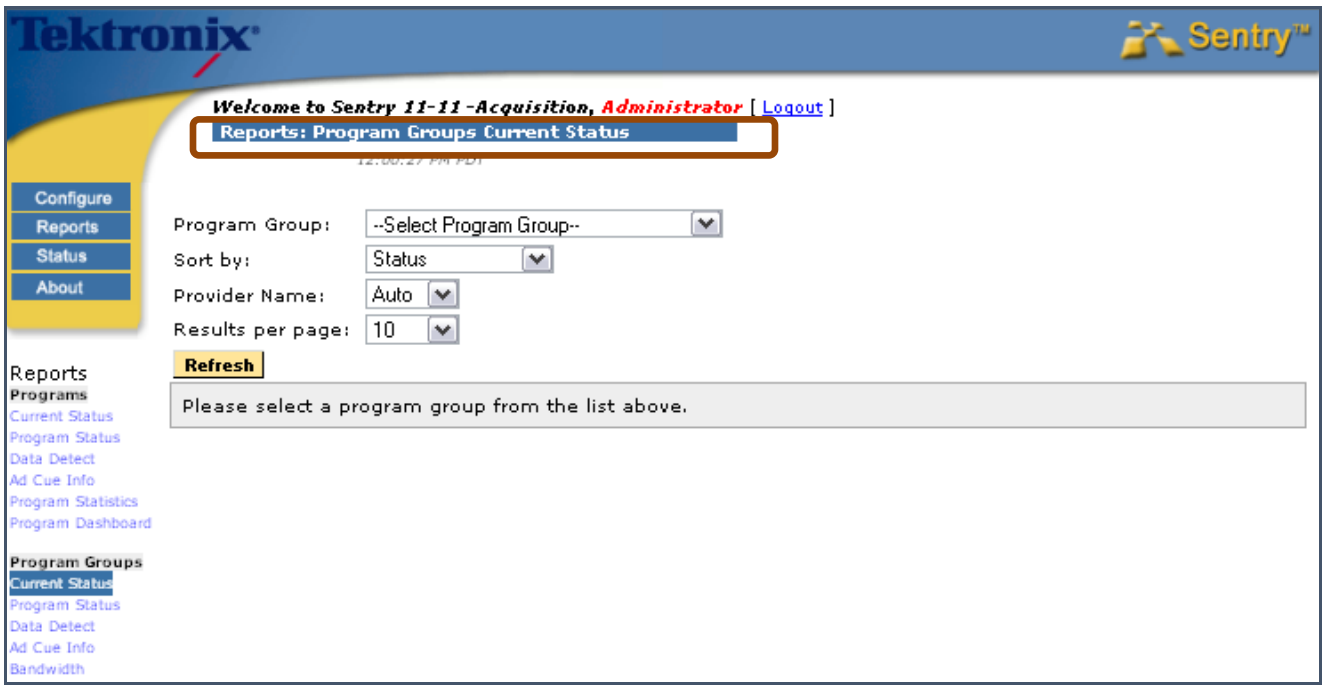


Figure 88: The Current Status Welcome page

2. Select a **Program Group** and then click the **Refresh** button.

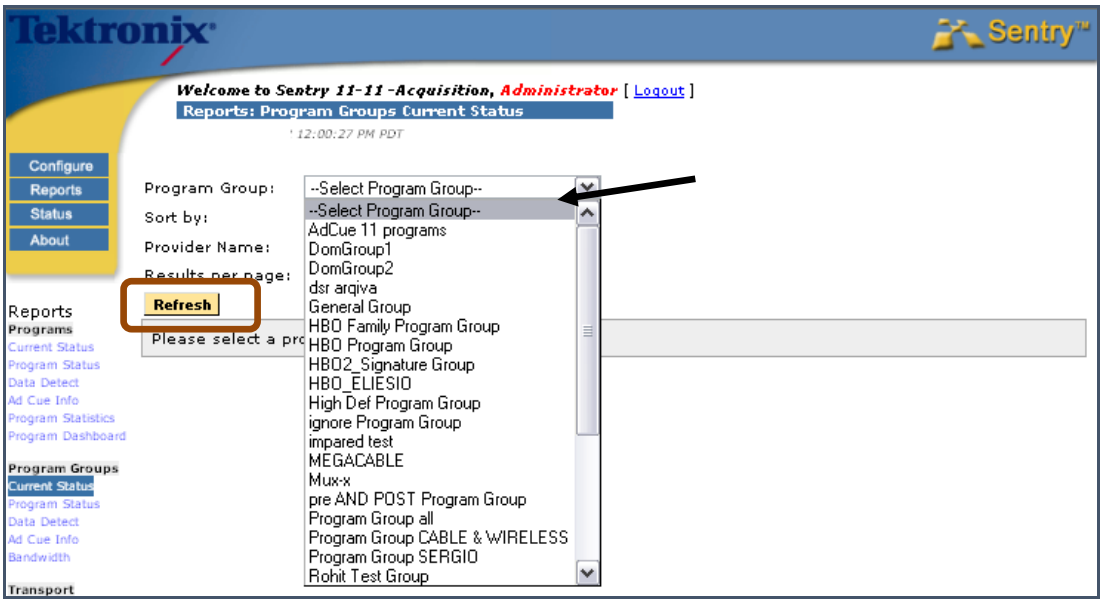


Figure 89: Selecting a Program Group

3. The programs that were in the selected group and its current status will populate in the bottom display.

NOTE: ***You are not choosing a PORT at this point, you are choosing a PROGRAM.***

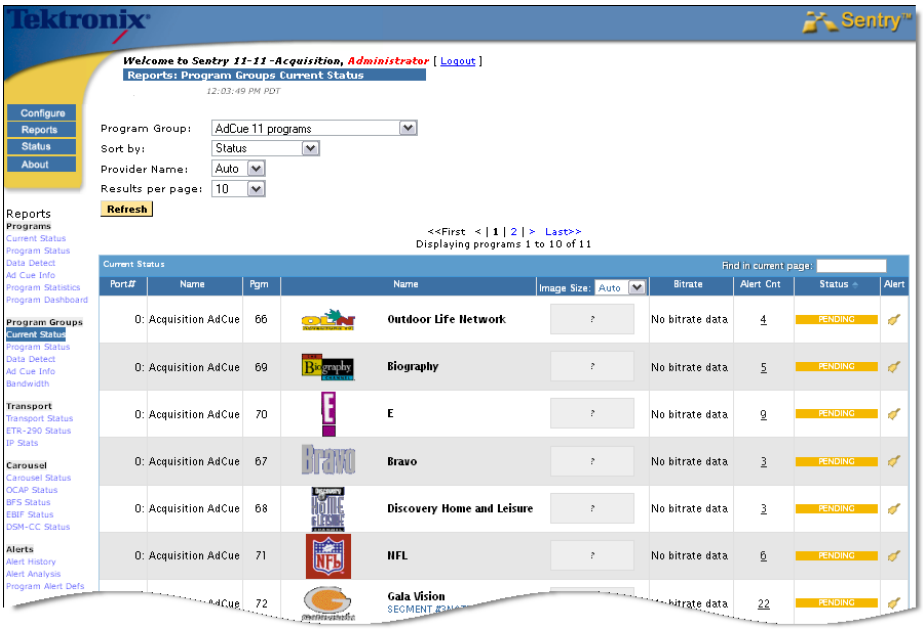


Figure 90: Displaying the Program group

4. Repeat the steps as needed to use **Program Status**, **Data Detect** or **Ad Cue Info**.

Program Groups Bandwidth

Program Groups Bandwidth provides a per program stacked bandwidth graph for a defined program group.

This report provides a visual understanding of overall transport bandwidth as well each individual program's bandwidth.

Examples for use would include:

- Planning for transports
- Examining existing transports

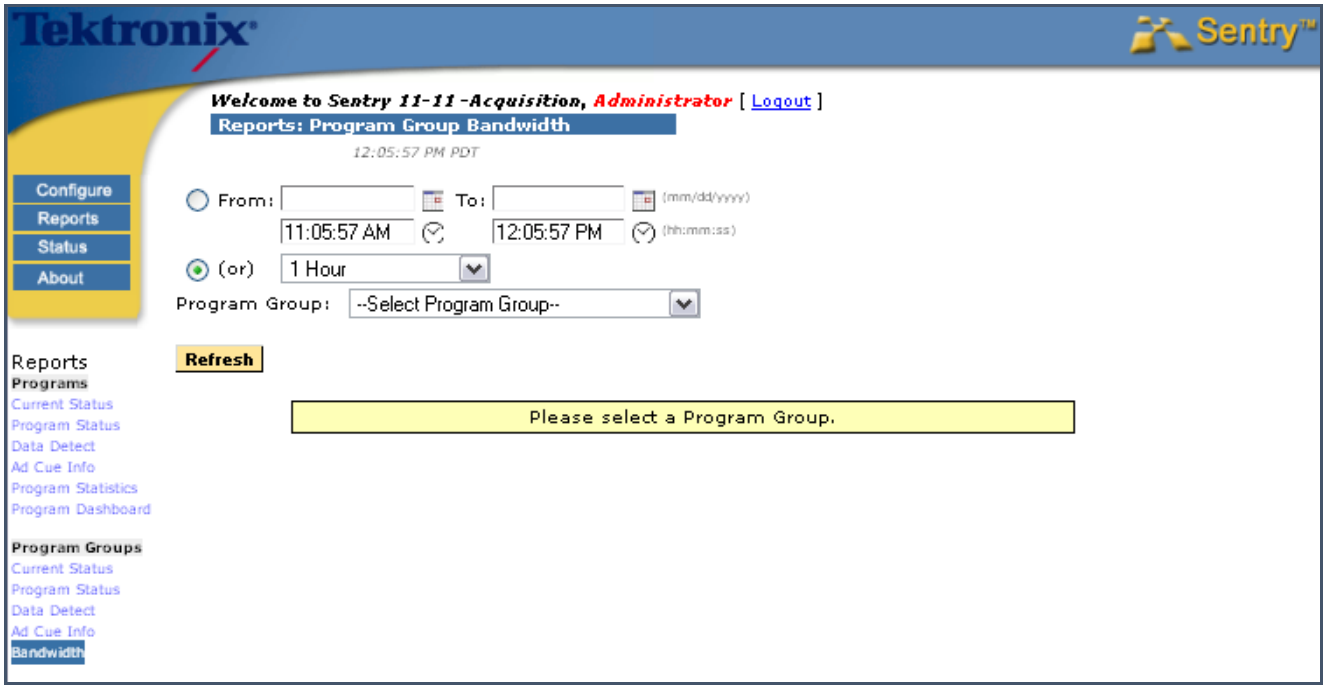


Figure 91: Program Group Bandwidth

Access Program Groups Bandwidth

1. Select **Bandwidth** from the **Reports** menu.

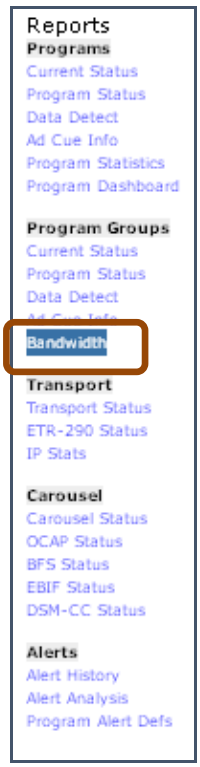


Figure 92: Accessing Program Group Bandwidth

2. Choose your time frame
3. Choose program group
4. Select **Refresh**.

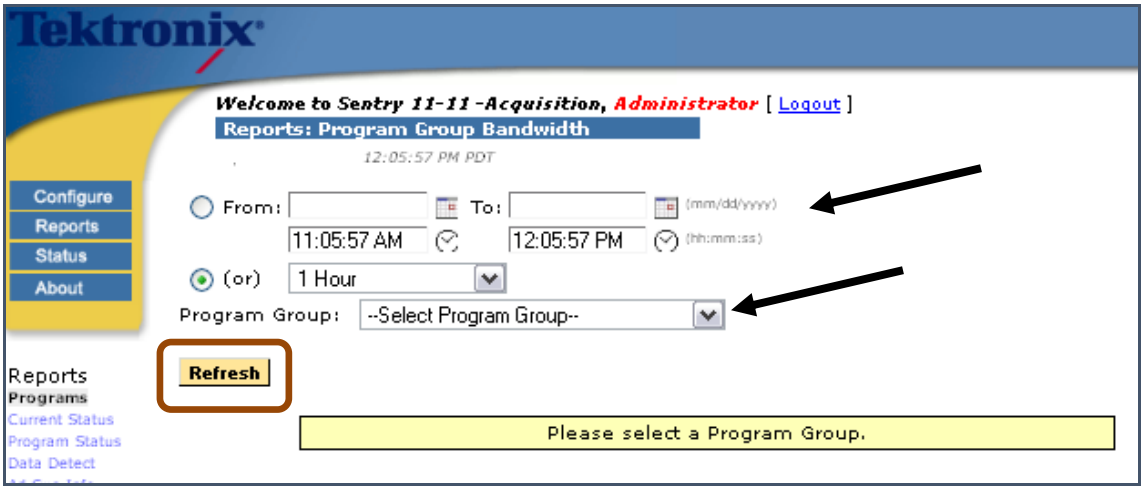


Figure 93: Selecting time frame and Program Group

In this example the transport streams bandwidth was graphed for one hour. You can see that some programs take more bandwidth than others.

The pink line (Program 75) is using more bandwidth than the olive green line (program 73).

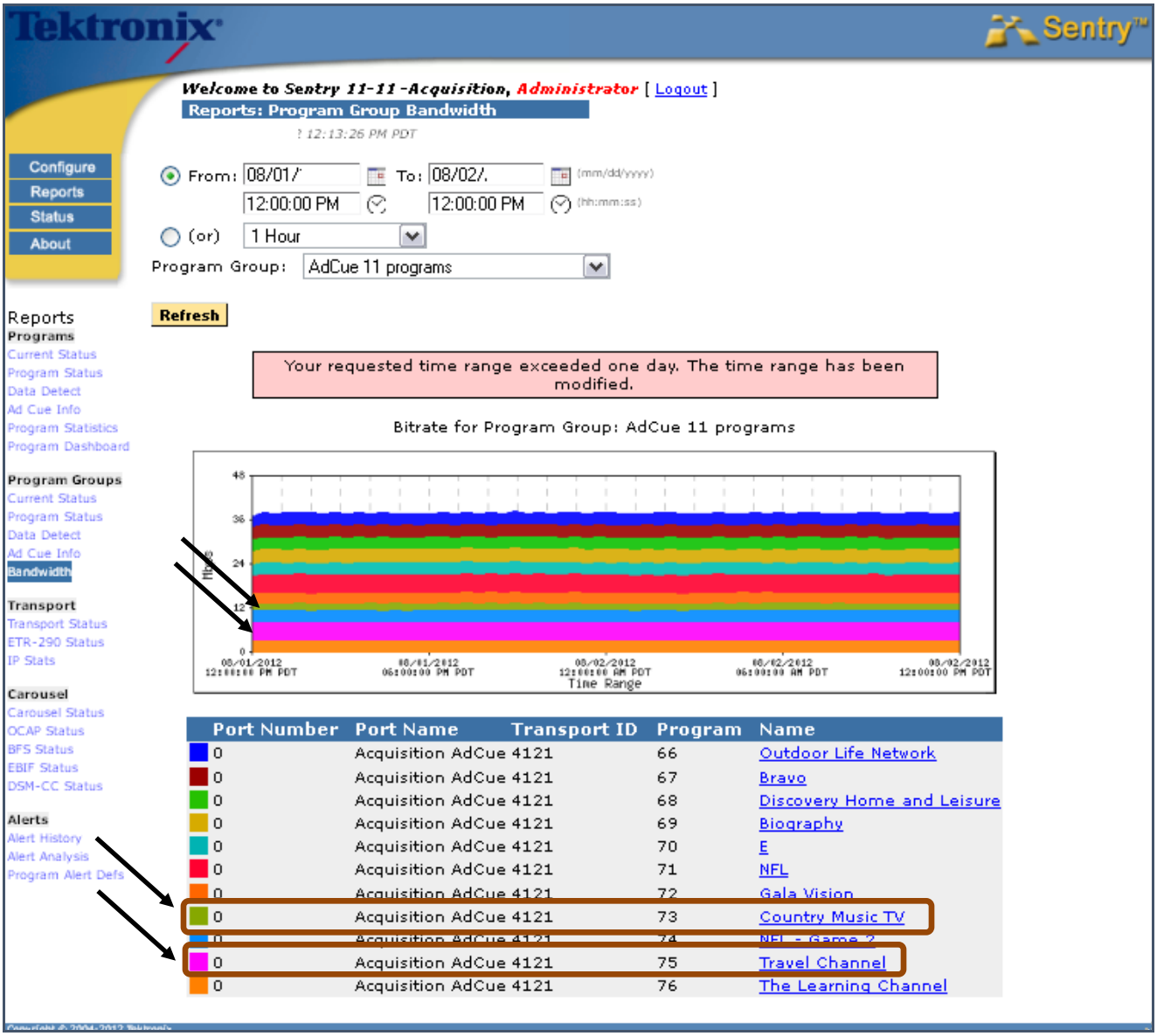


Figure 94: Program Group Bandwidth result

Dynamic Program Groups

Dynamic Program Groups allow you to define a program group based on dynamic program attributes instead of just listing the program numbers.

Select **Configure** and **Dynamic Program Groups from** the main menu.

The resulting page will be a list of all of the existing **Dynamic Program Groups**.

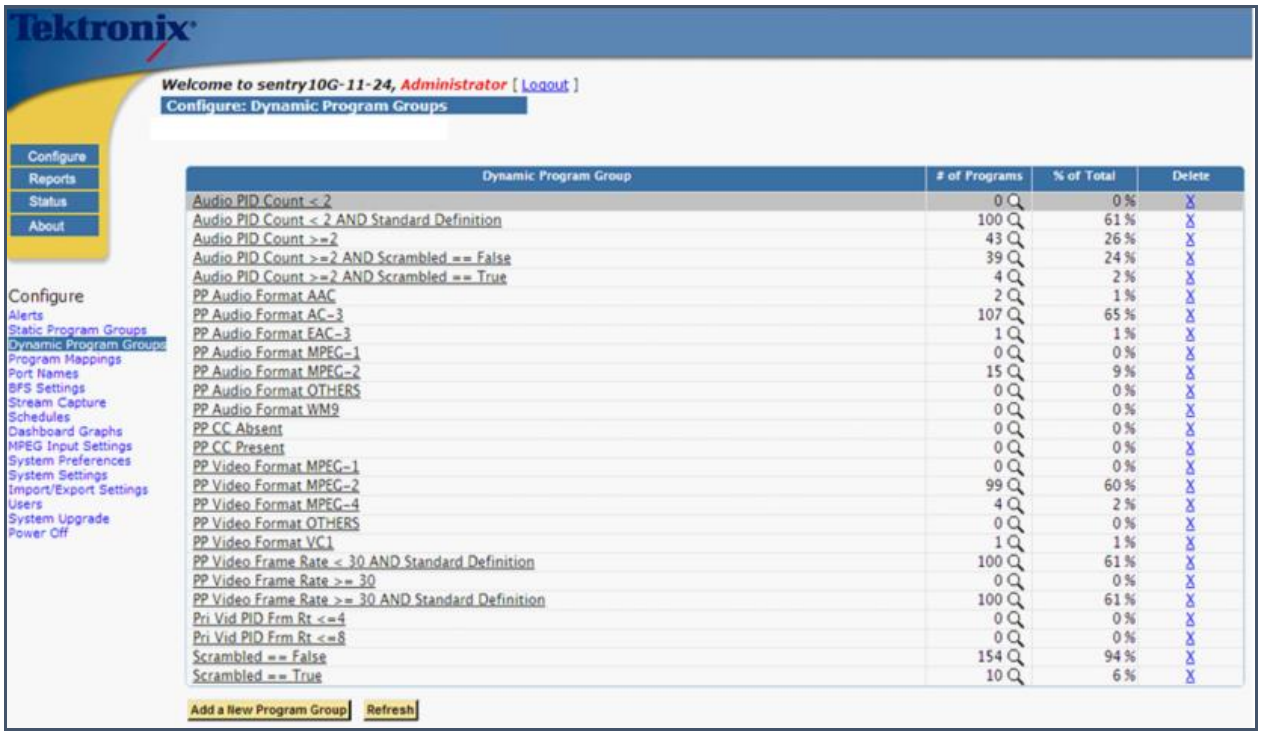


Figure 95: Dynamic Program Groups

Create a New Program Group

Scroll down to **Program Group Configuration** and either select a current filter (or filters) or create a new one.

Example 1: Create a new Dynamic Program Group that uses new Program Group Configuration criteria

1. Select **Show more filters types…**

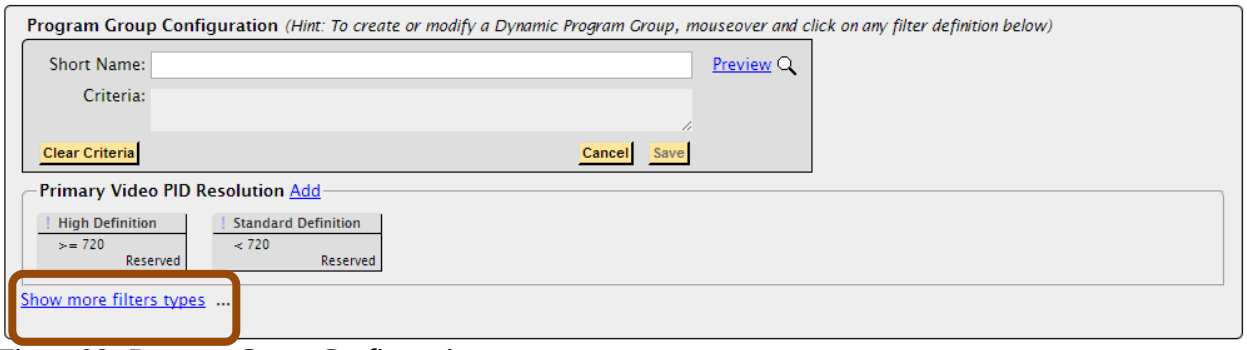


Figure 96: Program Group Configuration

2. Choose the criteria section and click **Add** next to the name**.**

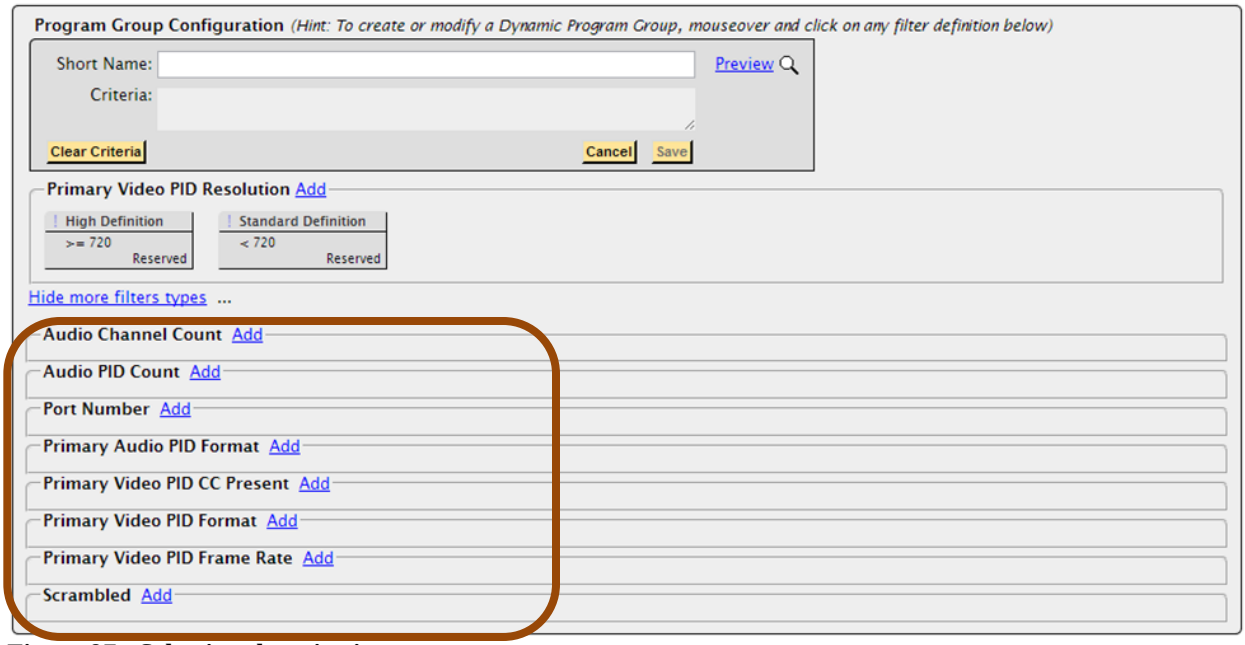


Figure 97: Selecting the criteria

3. In this example, we want to create an **Audio Channel Count** filter that only shows services that contain 2 audio channels.

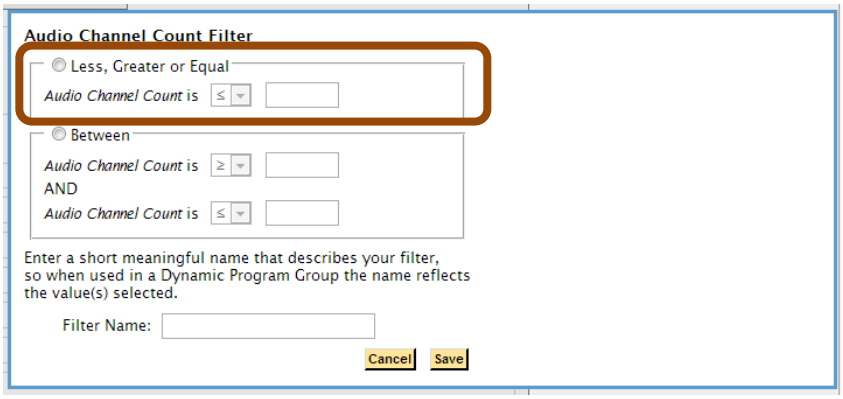


Figure 98: Setting the Audio Channel Count part 1

4. Enter in the filter criteria and a name for the filter. Click **Save**.

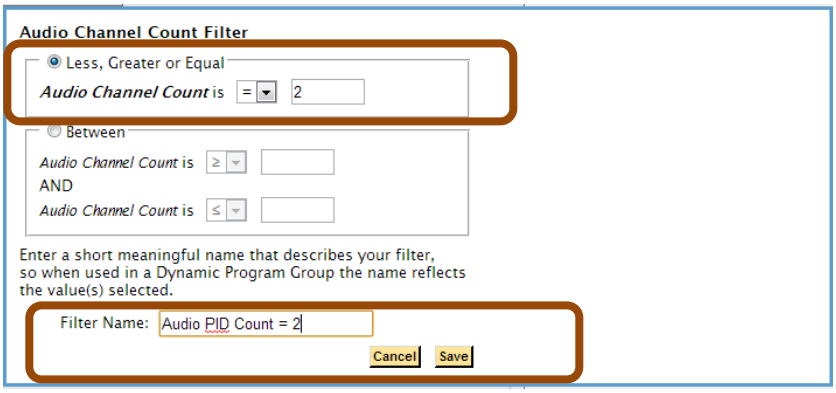


Figure 99: Setting the Audio Channel Count part 2

5. You will now see the filter that we just created.

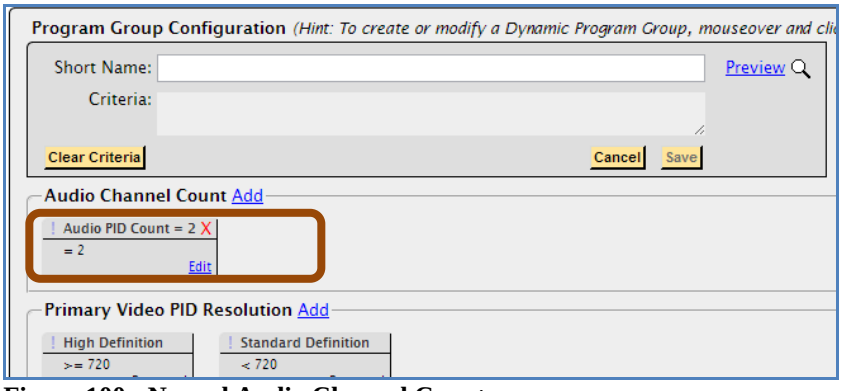


Figure 100: Named Audio Channel Count

6. Now that you have created the filter criteria the next step is to create the **Dynamic Program Group**.
7. Enter a name for the **Dynamic Program Group** in the **Short Name** dialog box.
    a. Continuing our previous example, call it **Audio PID Count = 2**.
    b. Next click on the filter criteria that was just created. It will turn green and the **Criteria** dialog box will list the criteria.

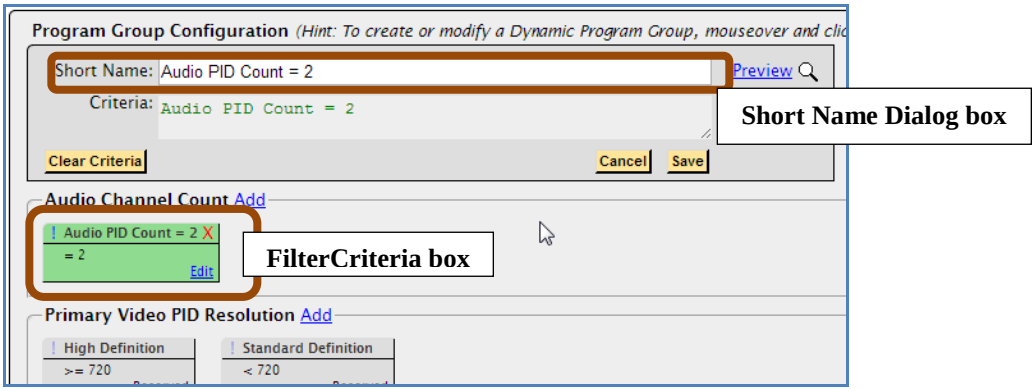


Figure 101 Entering the Short Name and selecting the Filer Critera box

8. Click **Save**. Now we can use this **Dynamic Program Group** anywhere that **Program Groups** are used.

Example 2. Create a new Dynamic Program Group that has more than one filter criteria

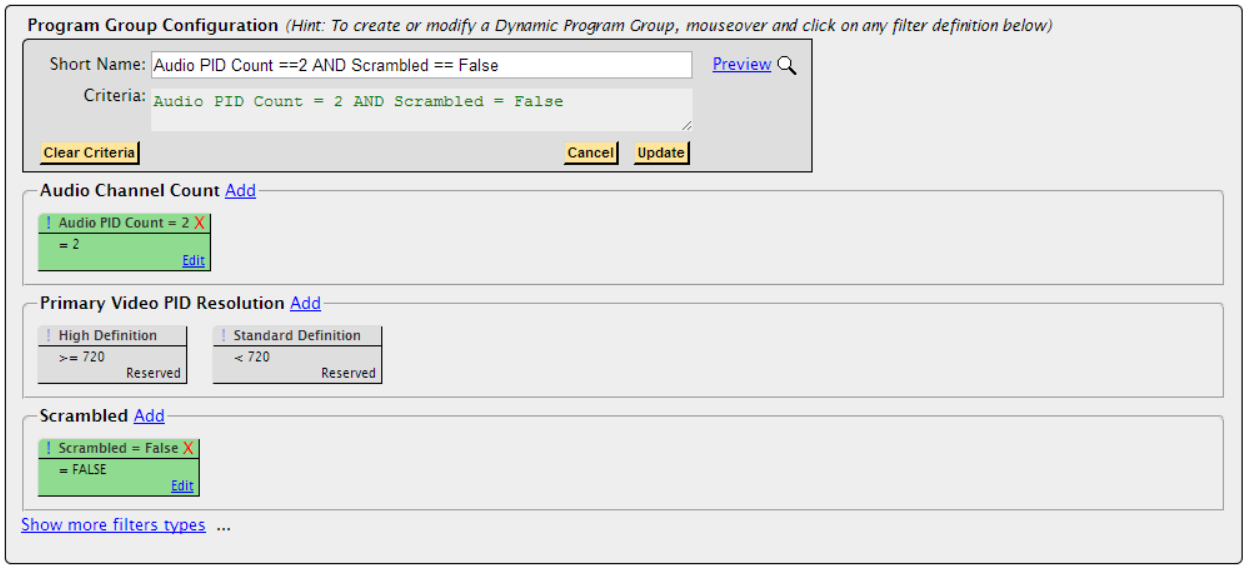


Figure 102: Multiple filter critera

Thumbnail Wall View

You can view thumbnails of active programs on a single screen, using the **Program Group** of your choice.

Each thumbnail includes an alert status indicator, similar to what you see on the Medius **Program Alert Dashboard.**

- Green indicates no triggered alerts
- Yellow indicates triggered alerts,
- Red indicates open alerts

You can sort the thumbnails by **Program Number**, **Program Name** (default), **Port Number**, and **Port Name**.

The **Thumbnail Wall** view refreshes every 60 seconds and individual thumbnails can be manually refreshed.

To access, click on **Reports**, then on **Thumbnail Wall** under the **Program Groups Menu.**

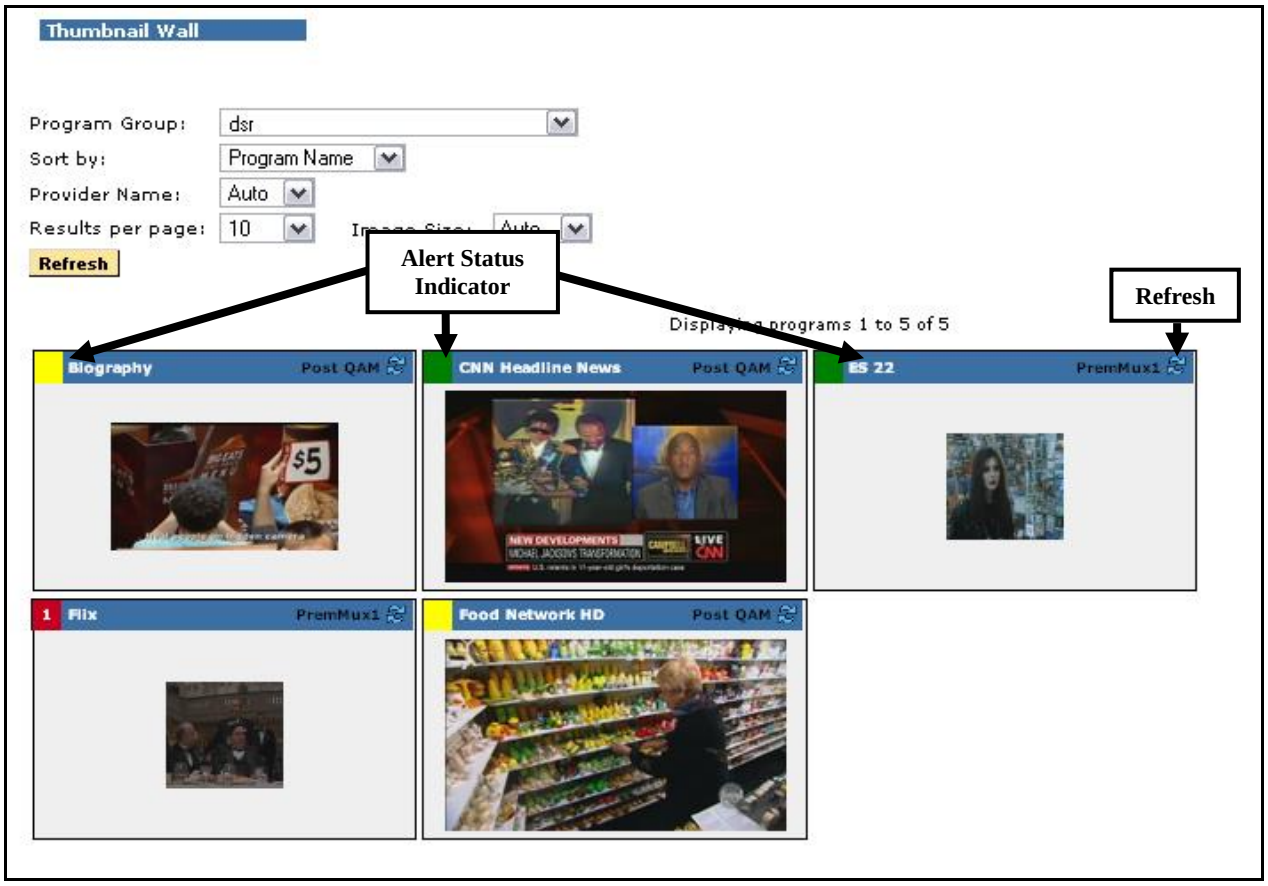


Figure 103: Thumbnail Wall View

Thumbnail size directly corresponds to resolution of video: the bigger the thumbnail, the higher the resolution.

Transport

Transport Status

The **Transport Status** report gives both a summary and a breakdown of statistics on all the MPEG tables within the transport stream, including:

- **System Info Tables** (PAT and PMTs)
- **DSM-CC Tables**
- **PSIP Tables**
- **Other Tables** (if they exist)
- **Ghost PIDs** (defined to be PIDs containing no tables and not part of any program)
- Referenced PIDs: PIDs mentioned in the tables, mainly the **Program Map Table** or **PMT**
- Reserved PIDs: example: **Program Association Table**, PID 0

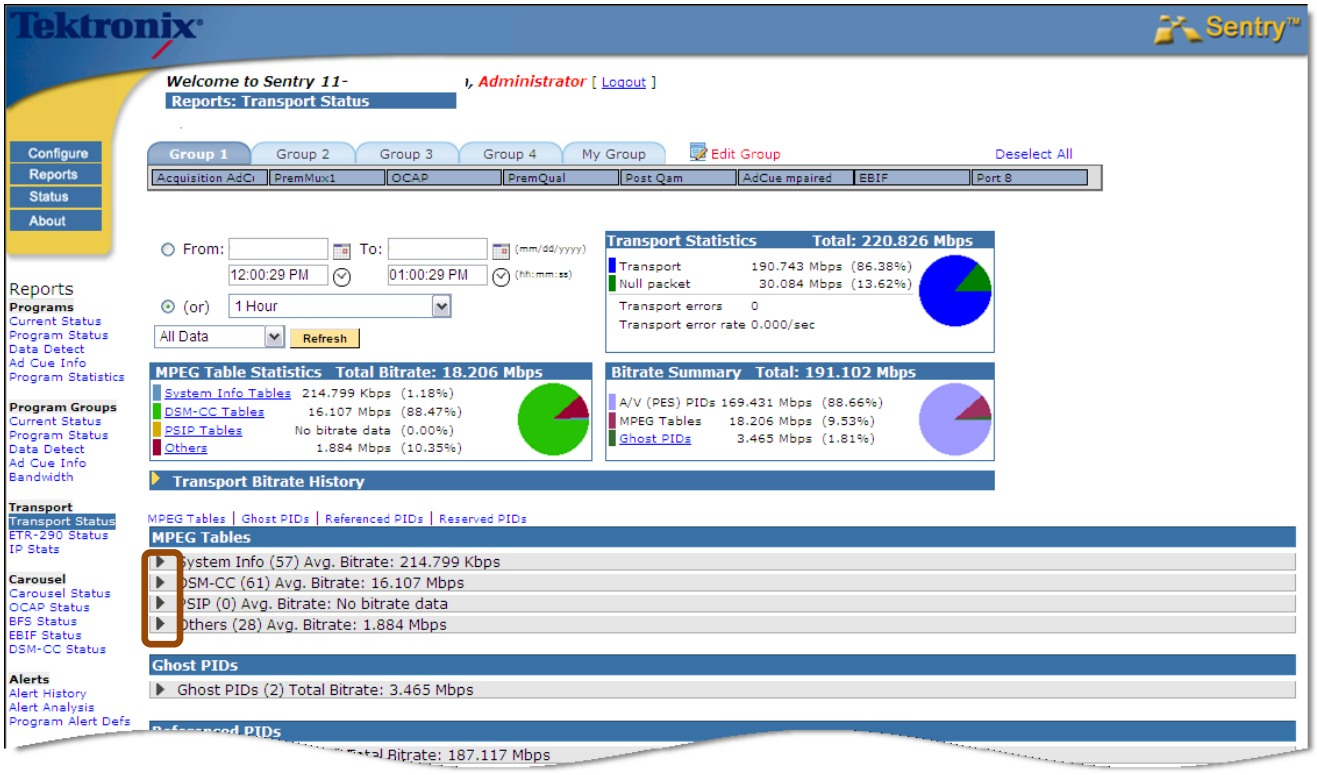


Figure 104: Transport Status Report: All Tables Collapsed

The **Transport Status** report includes both graphical and tabular representation of statistics for the time range displayed as the **Current View**. The default time range is the most recent hour.

You have the choice to specify your time frame to view the **Status Report**.

You also can **View All Data** or only **Active Data.** If you choose **View All Data**, you will see active and removed PIDs/Tables.

Transport Statistics

Show the overall transport packet bitrate, the null packet bitrate, the total bitrate, and the average number of transport errors per sec. The transport bitrate is derived from the Sentry engine's report of the total bitrate and the null packet bitrate. It is the transport packets that the Sentry engine decodes as part of its monitoring.
It is important to note that the **Transport Statistics** include both active and inactive statistics in the time range.

For example, if a multicast group changes via **Configure: MPEG Input Settings**, the programs that are announced are active and the programs that are destroyed are inactive but both remain in the statistics.

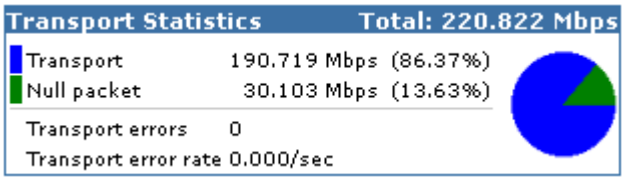


Figure 105: Transport Statistics

MPEG Table Statistics

Show only what is currently active in the transport. These include the total table bitrate and the bitrates of the S**ystem Info**, **DSM-CC**, and **PSIP** tables. Others, which is not a defined category, will be included only if other tables exist in the transport.

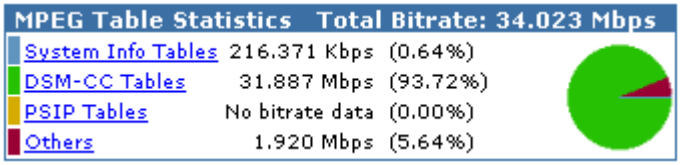


Figure 106: Active MPEG Table Statistics

Active Bitrate Summary

Shows only what is currently active in the transport, broken down into **Audio/Video (A/V) Packetized Elementary Stream (PES) PIDs** (i.e., PIDs that do not have tables on them), **MPEG** tables, and **Ghost PIDs**.

Overhead is not included in the table bitrate resulting in a discrepancy between the total displayed in the Transport Statistics and the **Active Bitrate Summary** total, even if the Transport Statistics include only what is active in the transport.

The actual amount of overhead is given by the ratio of **Avg. Bitrate** to **PID Avg. Bitrate** where **Avg. Bitrate** is the average table bitrate (see **Ratio** column in the expanded table reports).

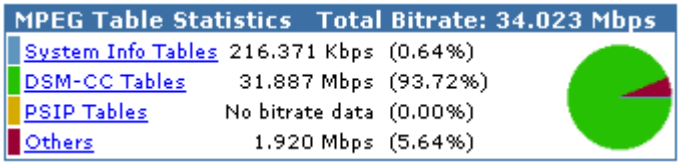


Figure 107: Active Bitrate Summary

Transport Bitrate History

The **Transport Bitrate History** graph shows the null PID bitrate for the transport. This report is one useful tool to track potential available bandwidth on a transport stream.

Access Transport Bitrate History

1. Expand the **Transport Bitrate History** section by clicking the arrow.

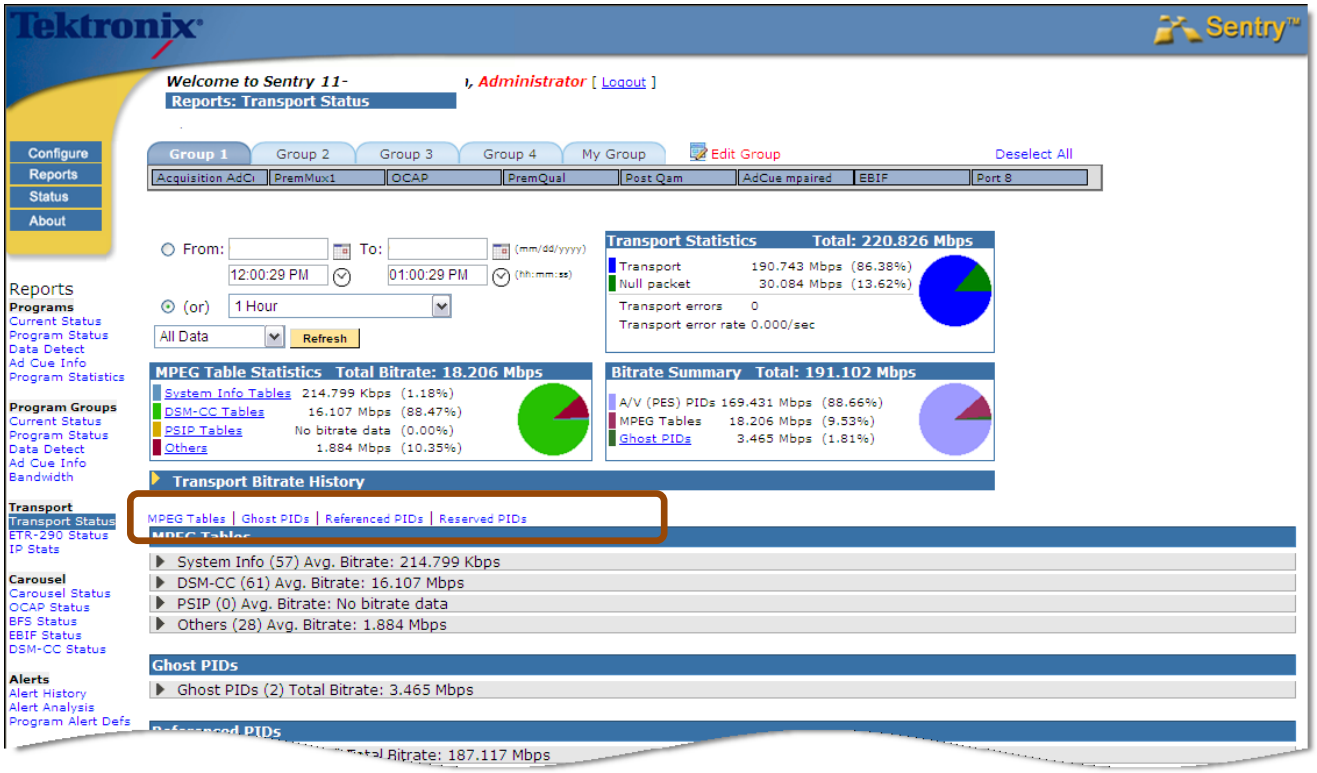


Figure 108: Transport Bitrate History

2. This sample shows a bitrate stream that is well optimized.

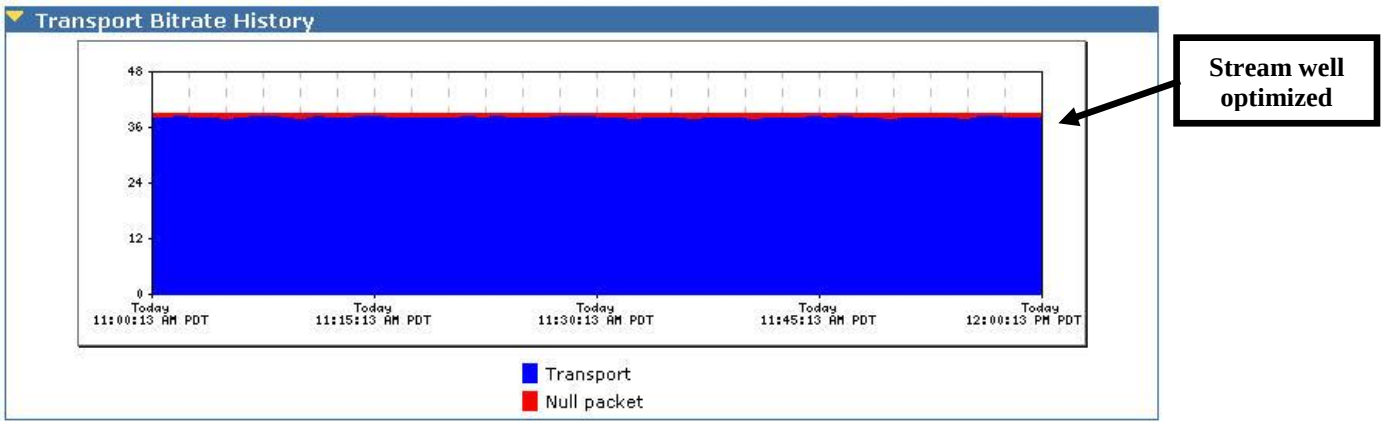


Figure 109: Transport Bitrate History (stream is well maximized)

3. This sample shows a bitrate stream that could possibly be a source for more bandwidth.

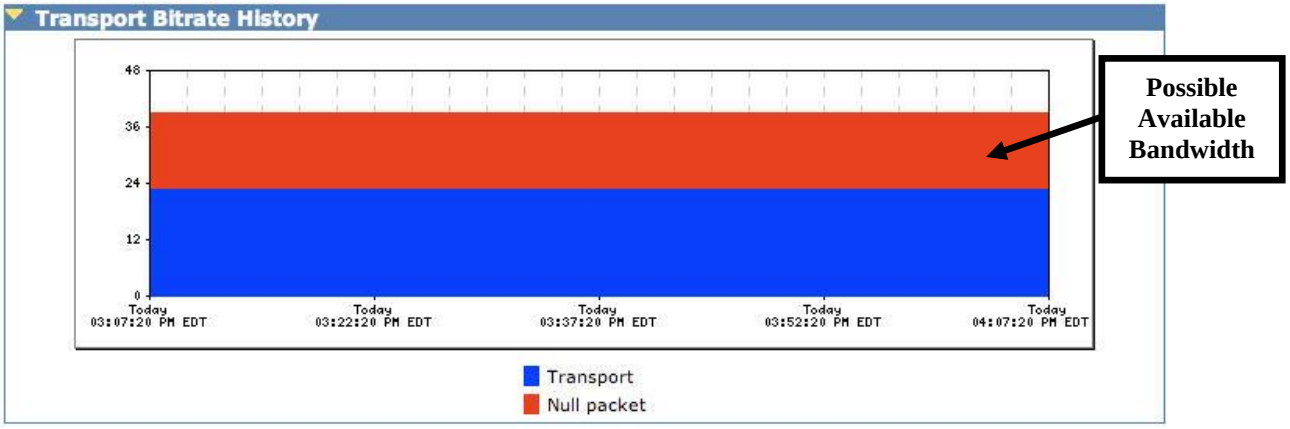


Figure 110: Transport Bitrate History (possible available room)

PSIP

PSIP stands for **Program and System Information Protocol**.

PSIP is the protocol used in the ATSC digital television standard for carrying metadata about each channel in the broadcast transport stream of a TV station. **PSIP** also used for publishing information used in electronic viewer guides.

PSIP defines virtual channels and content ratings, as well as electronic program guides with titles and (optionally) descriptions to be decoded and displayed by the ATSC tuner. For more information on how these tables are used, go to http://www.PSIP.org

Access PSIP

To monitor **PSIP** tables select **Transport Status** from the **Reports** menu.

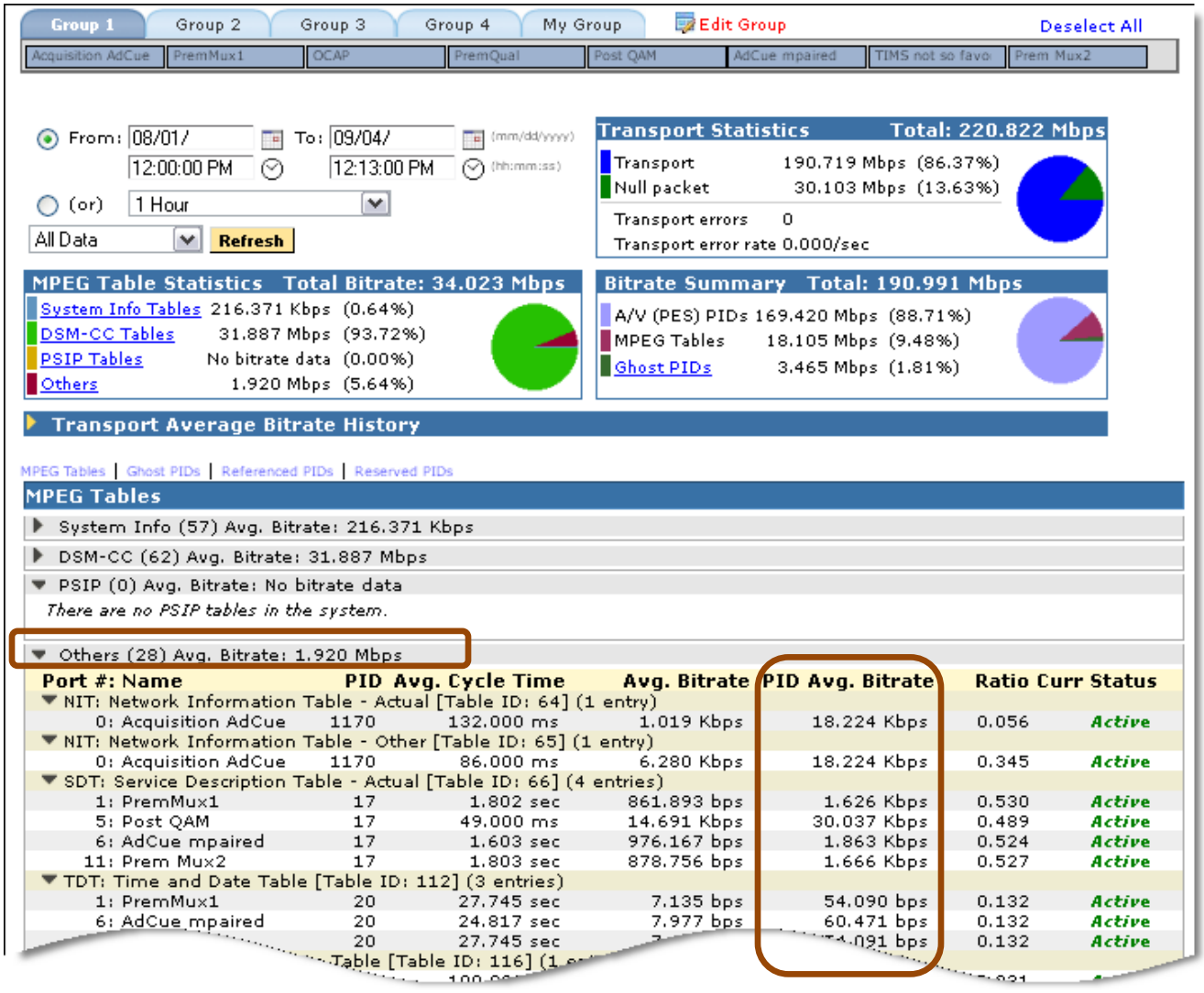


Figure 111: Transport Status with PSIP expanded

Creating an Alert for PSIP tables

You may create an alert to notify you if the **PSIP** tables are no longer present.

1. To set an alert, select **Configure** from the main menu
2. Next select **Alerts** from the drop-down menu.
3. From **PID Alerts**, select **Create**.

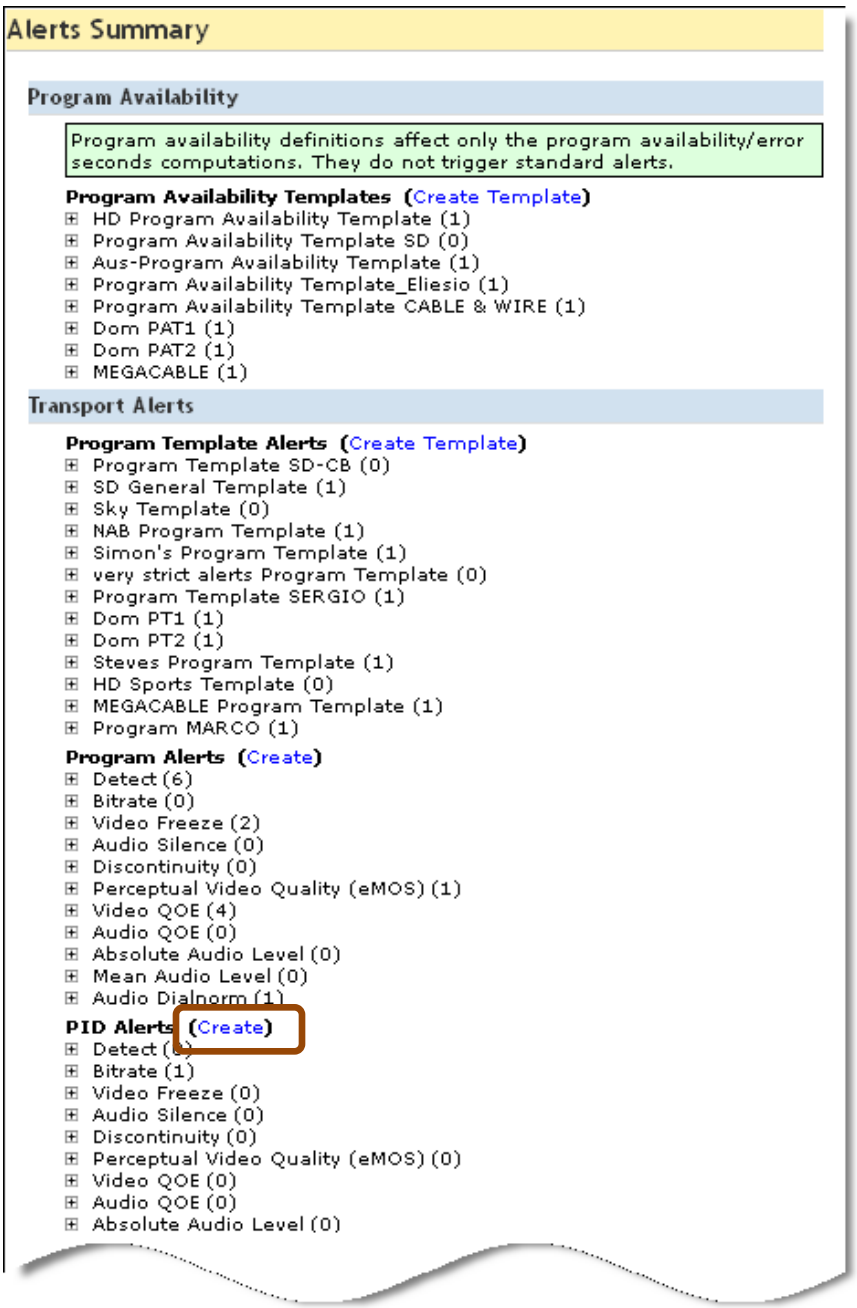


Figure 112: Create a PID Alert

4. Walk through the sections on the **Creating PID Alerts** page:

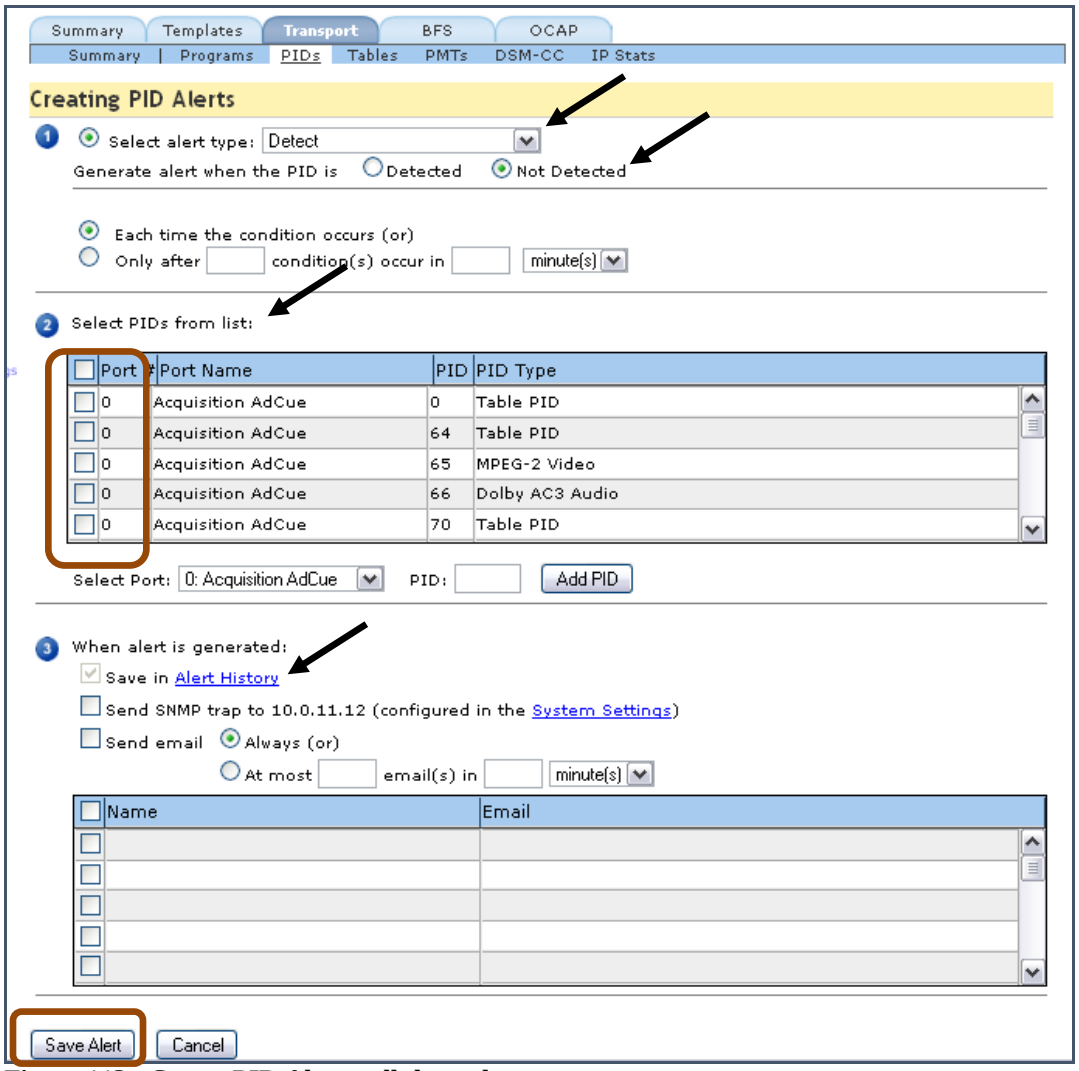


Figure 113: Create PID Alert walkthrough page

5. **Section** 1**:**

   Set the **Select Alert Type to Detect.**

6. Next, set **Generate alert when the PID is to Not Detected.**

7. **Section** 2**:**

   Select the required PIDs from the list

8. **Section** 3**:**

   Select the persons you wish to be notified.

9. Select **Save Alert**.

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 **Reports** from the main navigation bar. Next, select **TR101/290 Status** from the drop-down menu.

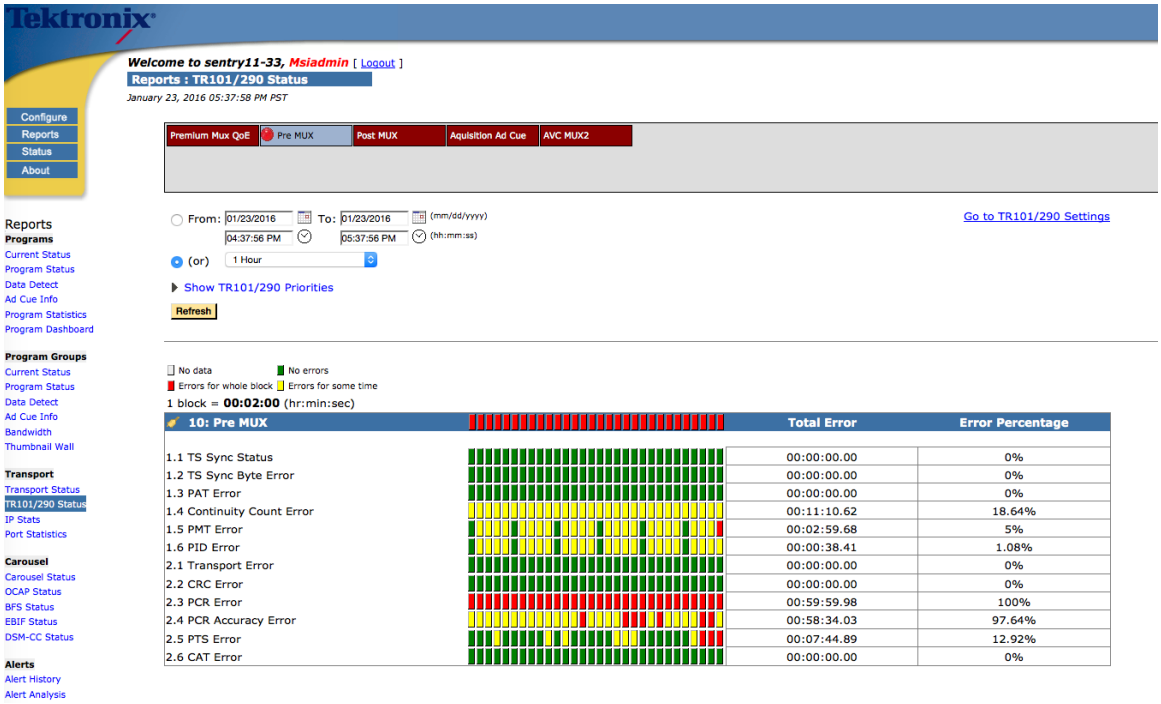


Figure 114: TR101/290 Status report

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:

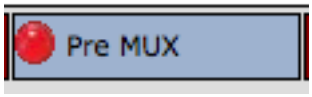


Figure 115: TR101/290 selected port indicator

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 midlevel 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

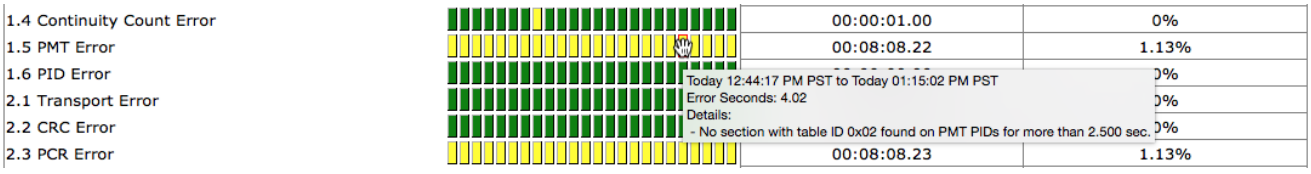


Figure 116: TR101/290 status block hover readout

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 117: 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.

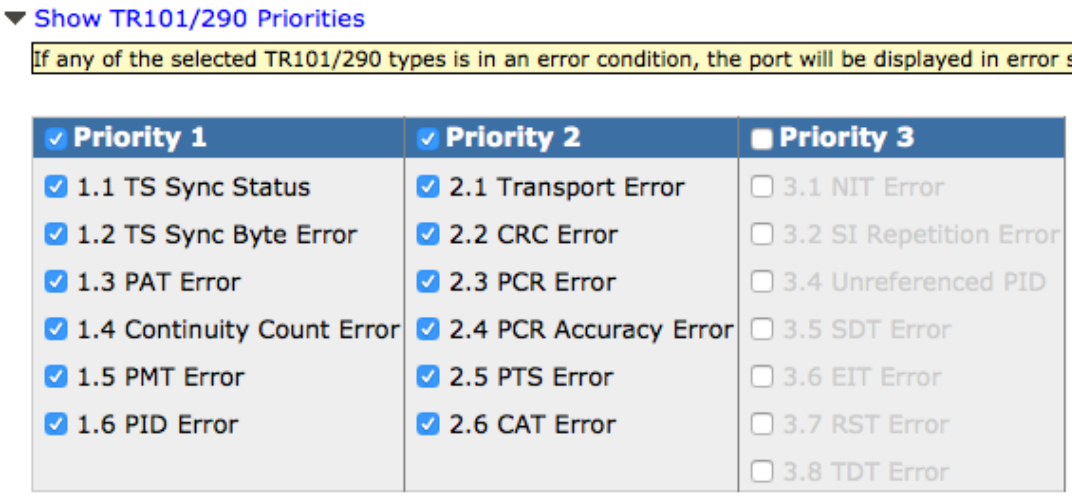


Figure 118: TR101/290 Priorities list

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

IP Stats

IP Stats is a part of Sentry's transport monitoring solution. It has three primary uses:

- **To monitor the health of the UDP/IP transport network over time**
  Sentry can be configured to send out an email and SNMP trap alerts when there is packet delay and network jitter (usually caused by traffic congestion) which could potentially impact audio and video quality.
- **IP Network Analysis**
  To perform root cause analysis on the IP network by using built-in analytical tools and historical reporting to correlate IP anomalies (packet delay and network jitter) with occurrences of other problems as discontinues, audio silence, video freeze alerts, etc.
- **Historical Reports**
  IP Stats can provide a historical graphical report on the entire IP network health with the exact time and respective severity level on any IP network anomalies.

Functionality

IP Stats primarily monitors IP packet **Arrival Interval** , **Delay Factor**, **Partial datagrams** and **Invalid Packets**.

The Leaky Bucket Buffer Analogy

When dealing with video over IP, the device buffer is critical in the reassembly of the MPEG packets. The buffer can be compared to an intentionally leaky bucket.

The data (the IP Packet) is represented in the example below by the water entering and exiting the bucket. The bucket itself, and the water it can hold, is the buffer for a particular device.

The optimal way for this bucket to work is for the same amount of water to drip in to the bucket as drips out of it. For our example, the same amount water (data) that flows in, flows out of the bucket (the buffer), thus keeping a constant level in the bucket.

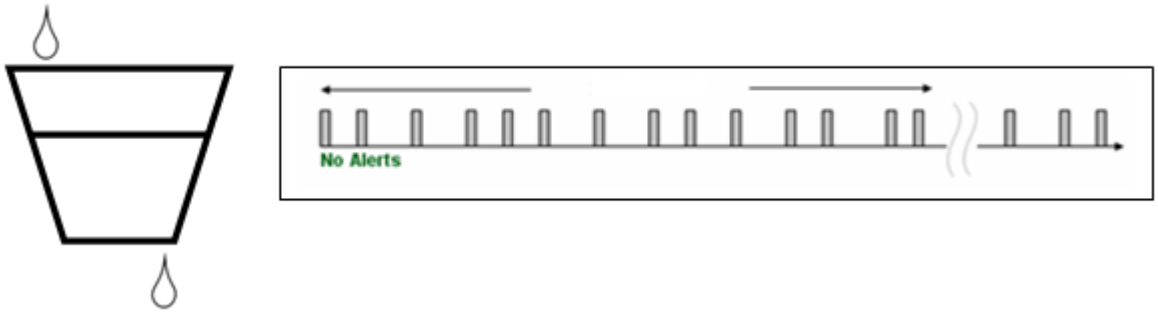


Figure 119: Evenly consistent flow

If the top flow (data) stops or slows down, the buffer will run out. This will cause a sharp increase in your **Arrival Interval** and **Delay Factor** averages.

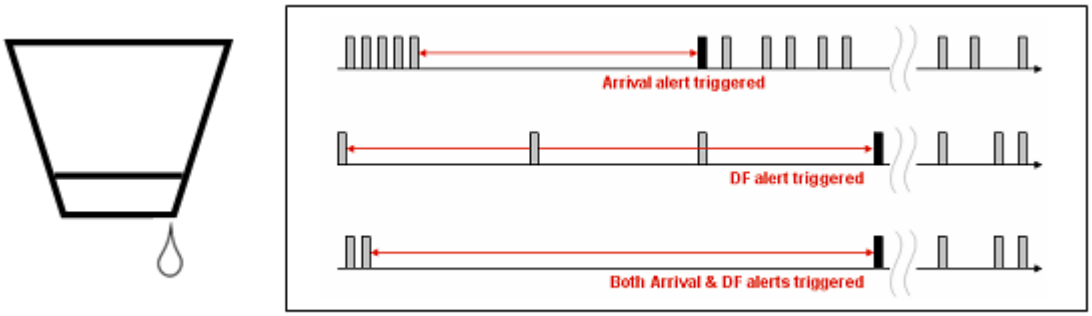


Figure 120: Not enough flow

If the top flow goes too fast, the bucket fills up and spills over. If the buffer becomes full, packet loss will occur. Here, your **Arrival Interval** average will decrease and the **Delay Factor** will remain constant until the buffer is full. At that point, the **Delay Factor** will increase.

Figure 121: Buffer too full

If the data becomes "bursty" (starts and stops in uneven bursts), packet loss can occur. If this occurs; you may see a change either way in your **Arrival Interval** average. Your **Delay Factor** would likely show an increase.

Access IP Stats

From the home page, select **Reports** and then **IP Stats** from the drop-down menu.

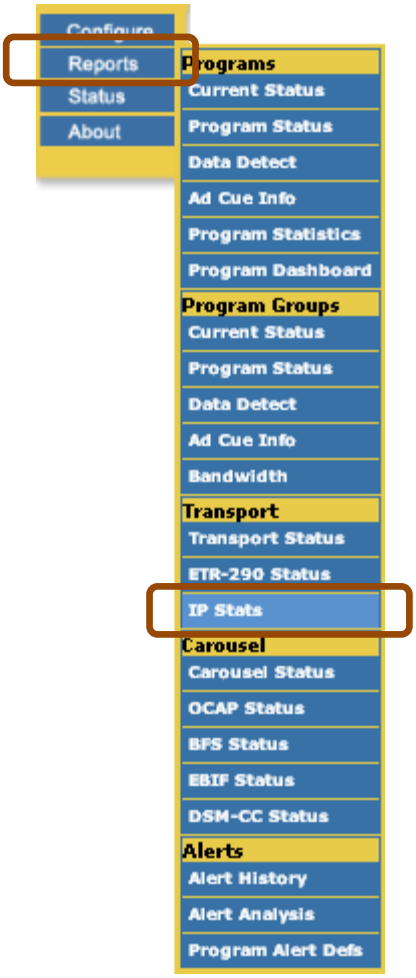


Figure 122: Selecting IP Stats

IP Stats Welcome Page

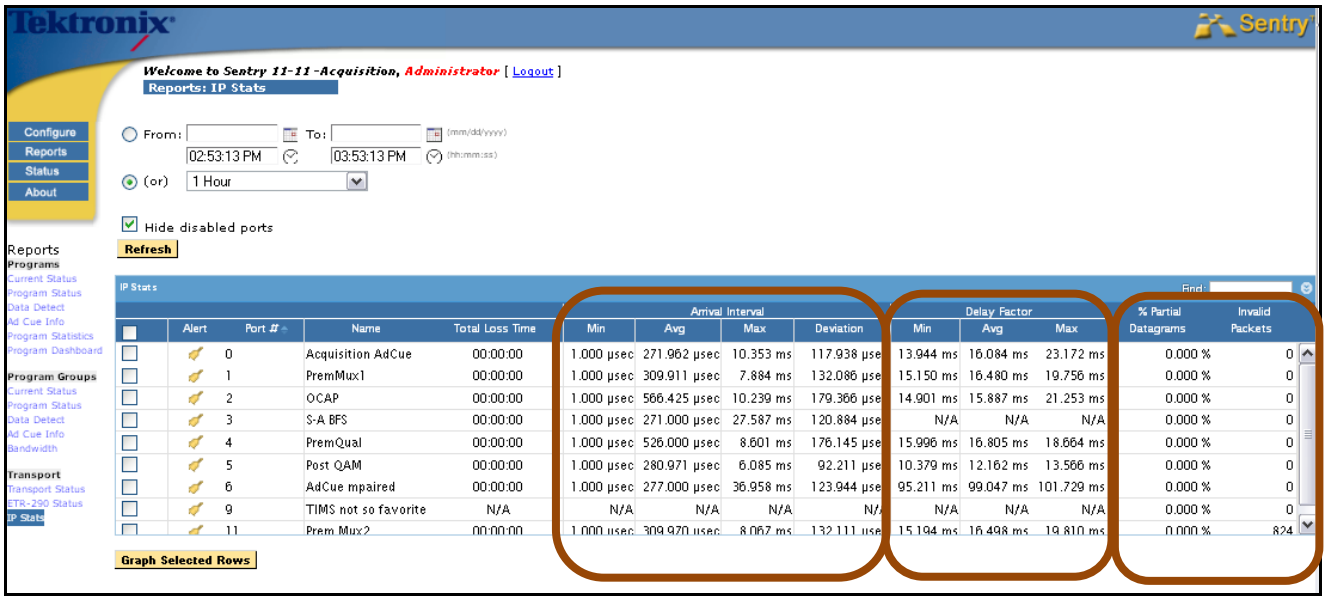


Figure 123: IP Stats Welcome Page

- **Date/Time selection or interval selection**
- **Sort by port number**
- **Arrival interval**
  Indicates the time between the arrival of UDP packets
- **Delay factor**
  Indicates how long a data stream must be buffered (i.e., delayed) at its nominal bit rate to prevent packet loss.
- **Partial Datagram**
  The percentage of UDP packets with a partial payload.
- **Invalid Packets**
  The number of IP packets that are discarded because they are corrupted.

Graphing Ports

To see a port or group of ports in a graph, select the desired ports by clicking the check box next to each port. You may only graph up to six ports at a time.

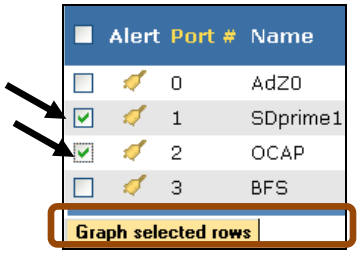


Figure 124: Selecting ports to graph

Next, select **Graph** selected rows.

By default, the graph shows the **Delay Factor**, **Arrival Interval**, **Partial Datagrams** and **Invalid Packets**, but you may also select or unselect any of the data sets as needed. The pages are also color coded.

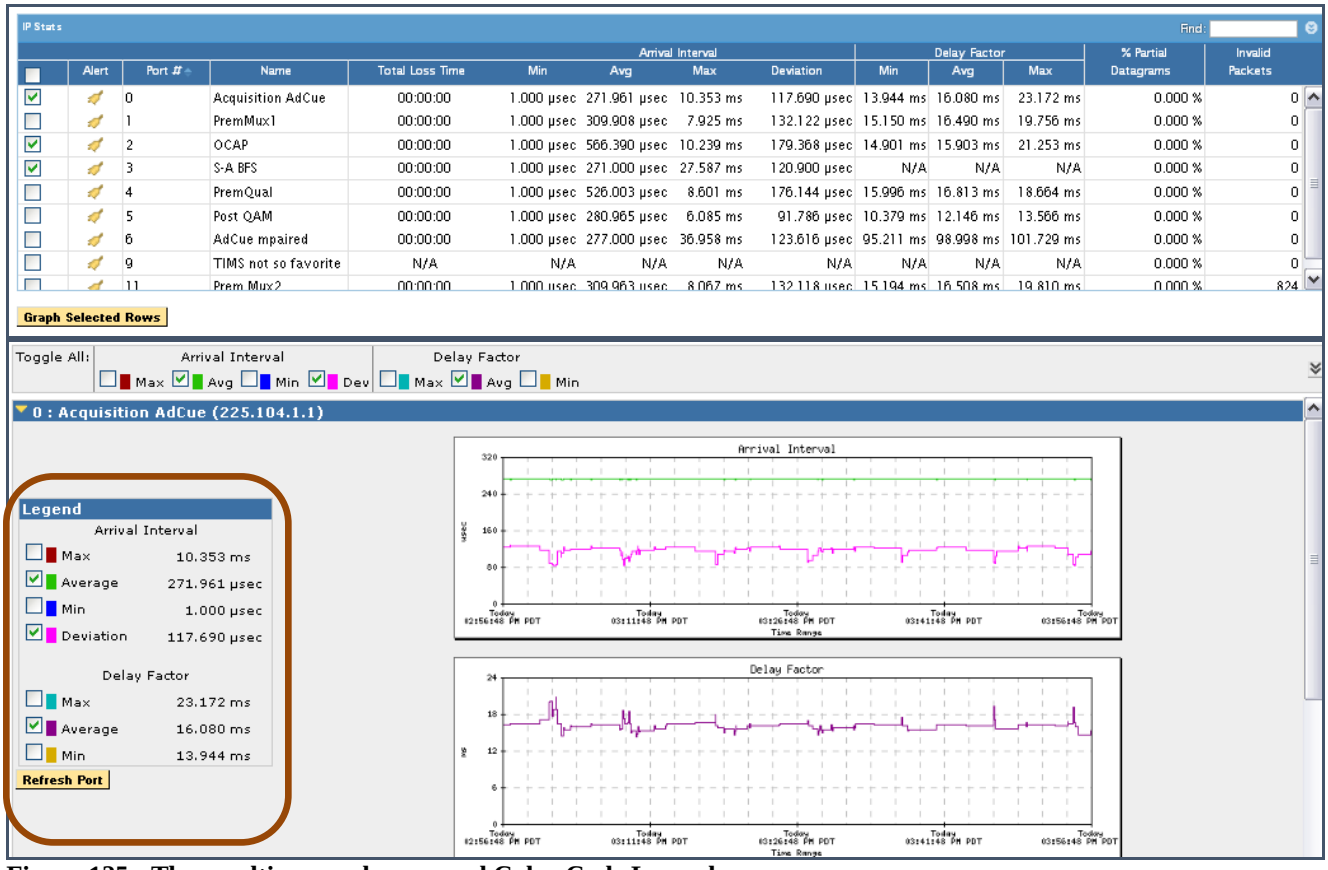


Figure 125: The resulting graph page and Color Code Legend

Zoom in on a Graph

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

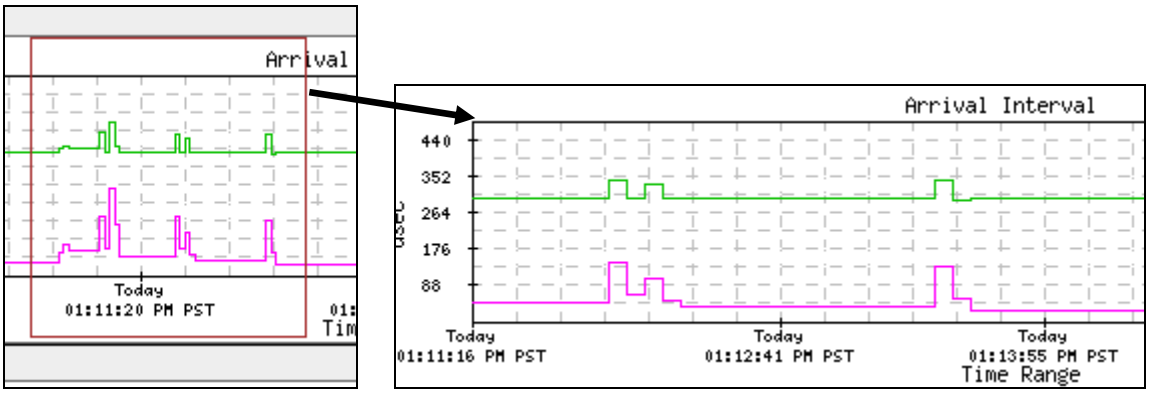


Figure 126: Drawing the box and the resulting page

The graph will then reload and display the selected time period in detail.

Create IP Stats Alerts for Arrival Interval

Alerts for **IP Stats** do not come pre-set. You will need to set the alerts to your specific needs.

1. Allow Sentry to collect data on your network for 15 minutes. This will allow you to find the average for **Arrival Interval** and **Delay Factor**. You will need these averages to set your alerts.

2. Next, click on the **bell icon** on the **Alert** bar for the port you wish to set an alert for. You will be automatically directed to the **Creating IP Stats Alerts** window for that port.

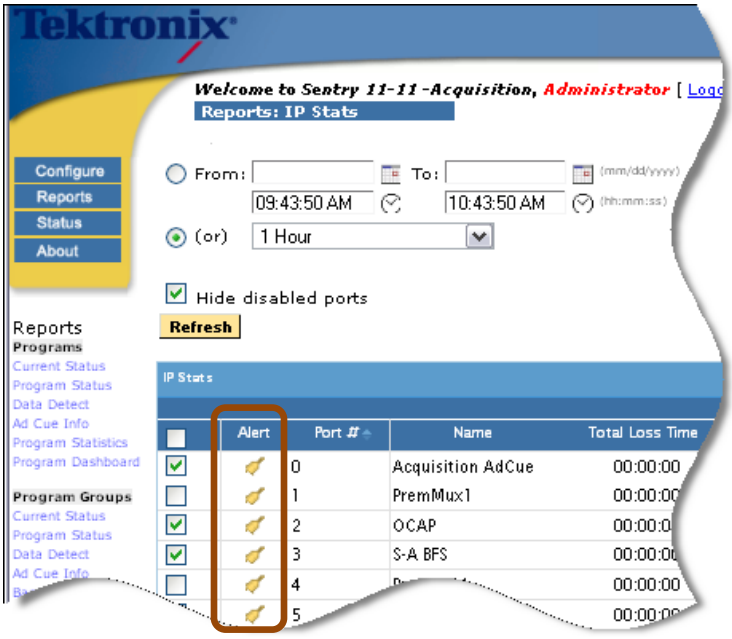


Figure 127: Bell Icons for Setting Alerts

3. The **Creating IP Stats Alerts** window is laid out to walk the user through the three step creation process.

4. Starting at **Section** 1, the **Arrival Interval** option should be already set. If not, you may select it from the drop-down menu.

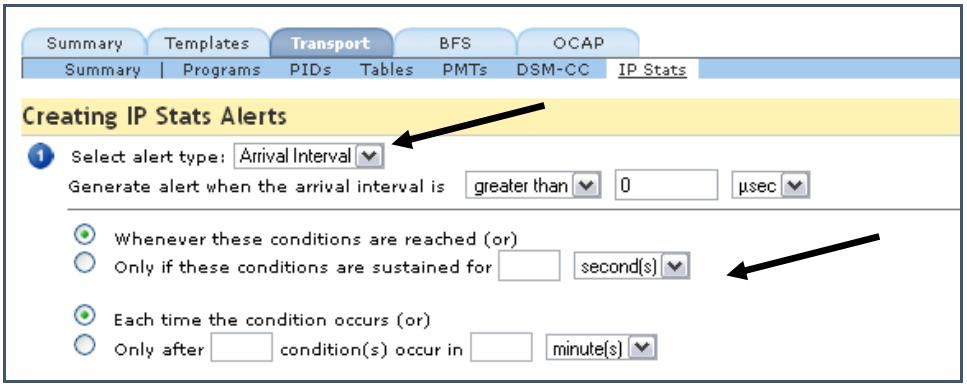


Figure 128: Step 1 Selecting Alert Type

5. Set the **Generate alert when the arrival interval is** section to **greater than 2000 µsec**.

6. This section is very subjective and depends entirely on the average speed of your network. This area can always be adjusted later if the interval seems to fast or slow for your actual network.

7. For **Section** 2, the default port will be set to 0. You can select or de-select any of the ports at this time. To save time, if all the ports have approximately the same **Arrival Interval** averages, you may select them, all.

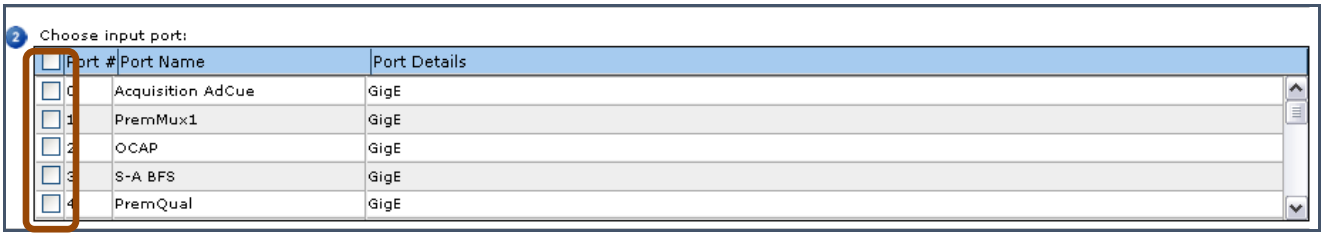


Figure 129: Step 2 Selecting the ports

8. For **Section** 3, choose what you want to happen when the alert is generated.

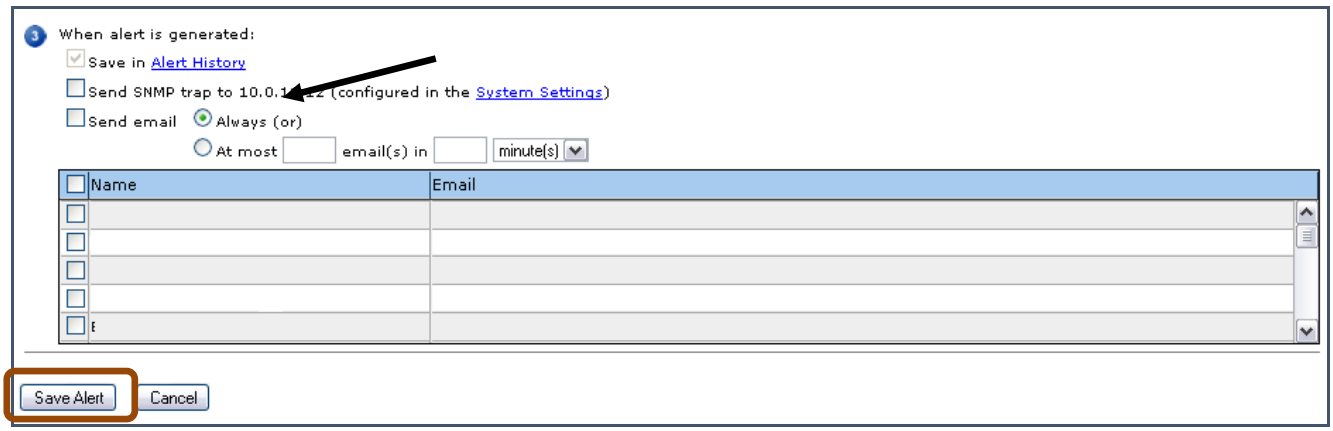


Figure 130: Selecting notifications and Save Alert

9. At this point, you may enter any email addresses you wish the alerts to be delivered to. The default setting will always save the alert in **Alert History**.
10. After you have finished **Section** 3, review the previous steps to make sure they are accurate and complete.
11. When you are finished, select **Save Alert.**
12. A **Save Alert** confirmation box will appear. Select **OK** to continue.

Figure 131: Save Alert Confirmation

13. After the alert has been set, you will be returned to the **IP Stats** alert page. From this page, you should be able to view the alert you just created.

Create Alerts for Delay Factor

NOTE: ***Suggested baseline starting point*- When you are working with Delay Factor, instead of 2000 µ, use 50000 ms as your Delay Factor average.**

1. To create alerts for **Delay Factor**, go back to **Alerts IP Stats** welcome page as seen in the **Arrival Interval** section of this manual.
2. Select the **bell icon** for the correct port**.**
3. When you are redirected to the **Creating IP Stats Alerts** page, choose **Delay Factor** alerts from the drop-down menu.

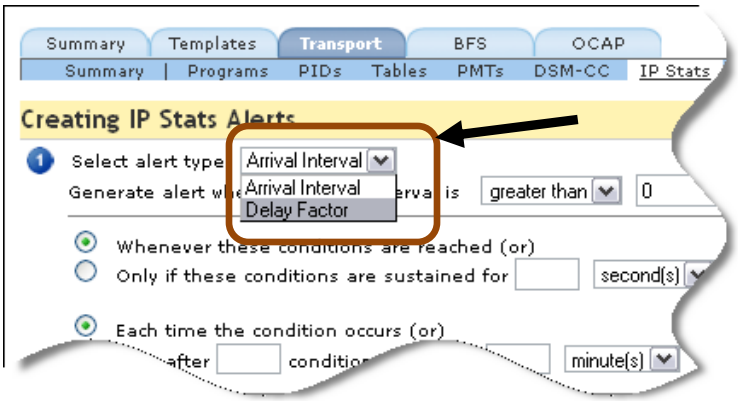


Figure 132: Setting alert for Delay Factor from right click menu

4. Follow steps in **Sections 1-3** as seen in the **Arrival Interval** section, keeping in mind that the following suggested settings are only a baseline starting point. Your actual value will depend on the bitrate of the stream and the equipment used in the network.

IP Stats Monitoring Notes

The graphs in IP Stats can be useful for basic trouble shooting. When packets are lost on your network, Sentry displays complete data loss as a large red block. The red block indicates that there was no data for that time period.

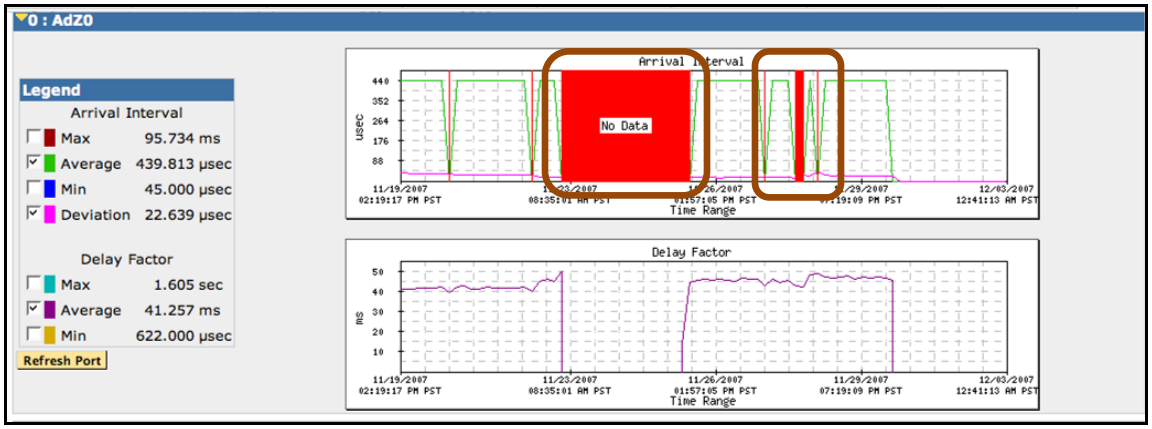


Figure 133: Two sets of lost packets

Carousel Status

Carousel Status shows all the available data carousels on Sentry.

These are:

- **OCAP**
- **BFS**
- **EBIF**

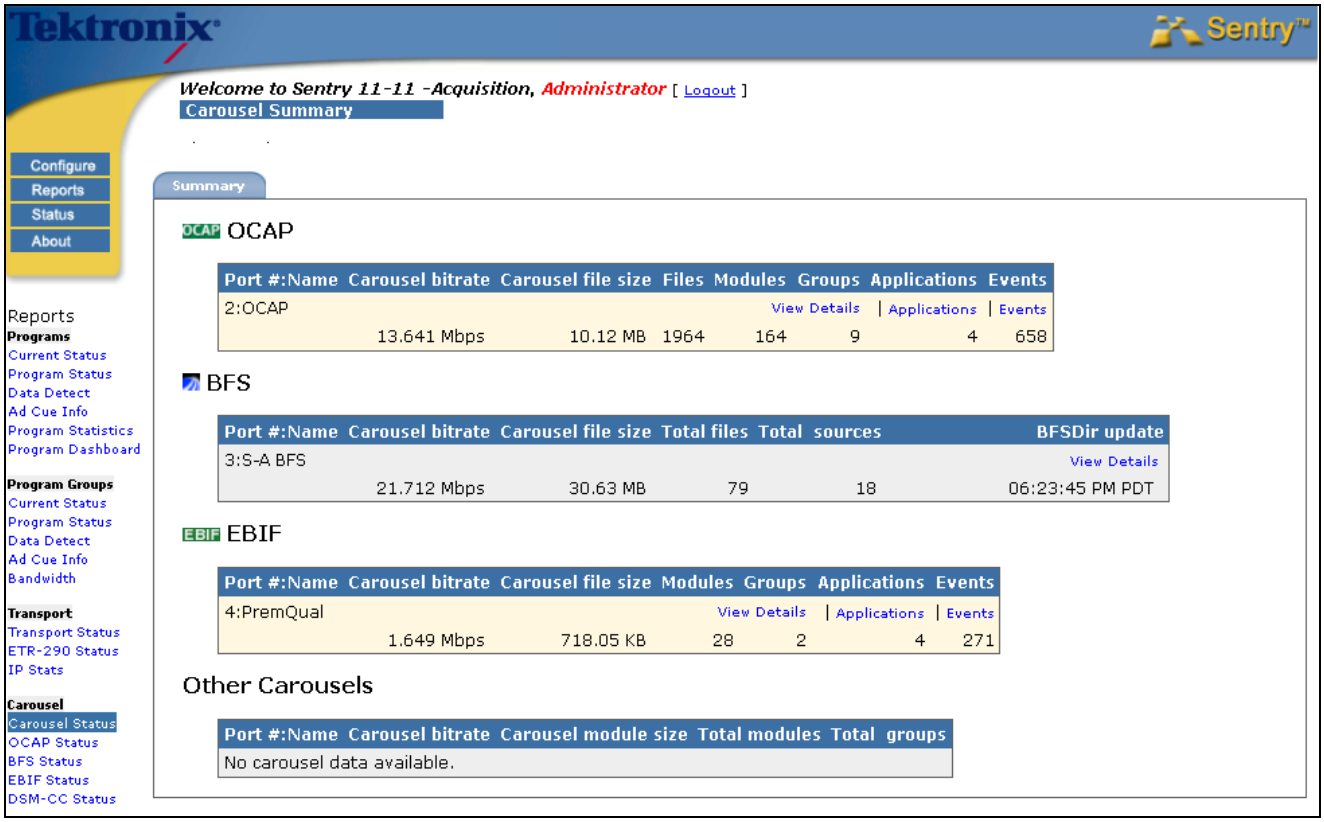


Figure 134: Carousel Status page

OCAP Carousel

Open Cable Application Platform (OCAP) provides a set of specifications to assist the cable industry with deploying interactive services.

More specifically to Sentry, OCAP is an add-on module that is available for purchase that is used for the monitoring of OCAP streams and systems.

NOTE: ***Recently, the OCAP standard has been renamed tru2way ™.***

However, it is still referred to as OCAP in this manual and on Sentry.

Access OCAP Carousel

From the home page, select **Reports** and then **OCAP** Status from the drop-down menu.

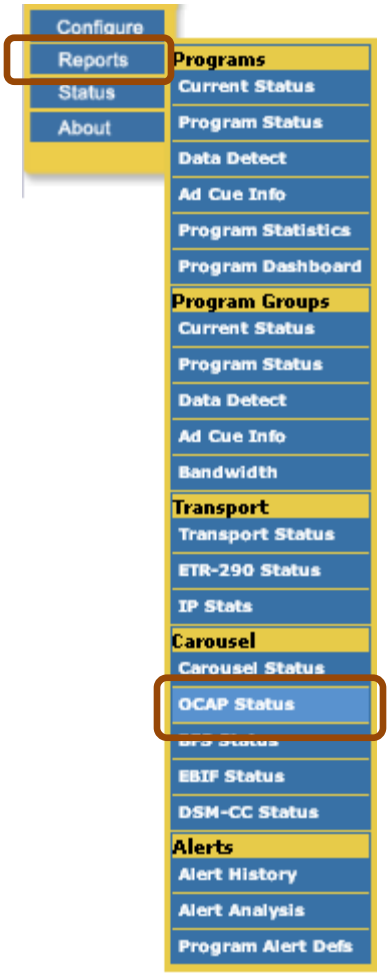


Figure 135: OCAP Status menu

OCAP Summary tab

The opening page for OCAP Status is the OCAP Summary. The user may navigate to any of the four tabs for more information on the selected OCAP stream.

- **Summary**
  A snap shot view of all the OCAP streams currently being monitored
- **Files**
  Opens a file browser window showing files for a selected OCAP stream
- **Applications**
  Shows available applications in the OCAP stream
- **Events**
  Show detailed view of events added, removed or changed

You may also navigate to the other tabs by selecting from the mini-menu within each OCAP row.

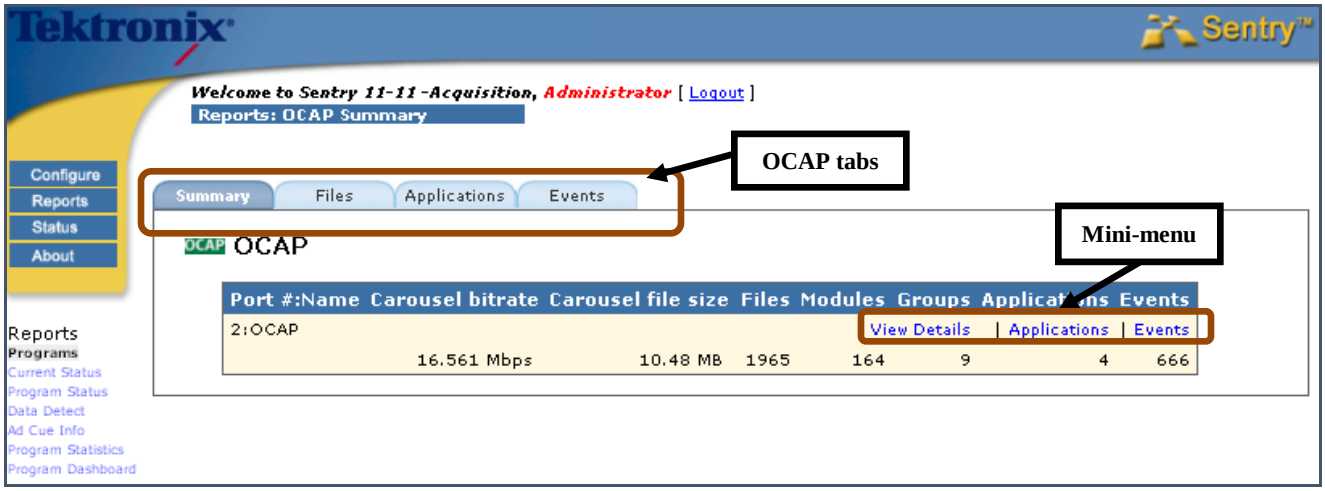


Figure 136: OCAP Summary page

NOTE: ***View Details on the Mini-menu will take you to the same screen as the Files tab.***

OCAP Files tab

The **OCAP Files** tab will allow you to view the details for the selected OCAP stream. In the figure below the port was named **OCAP**.

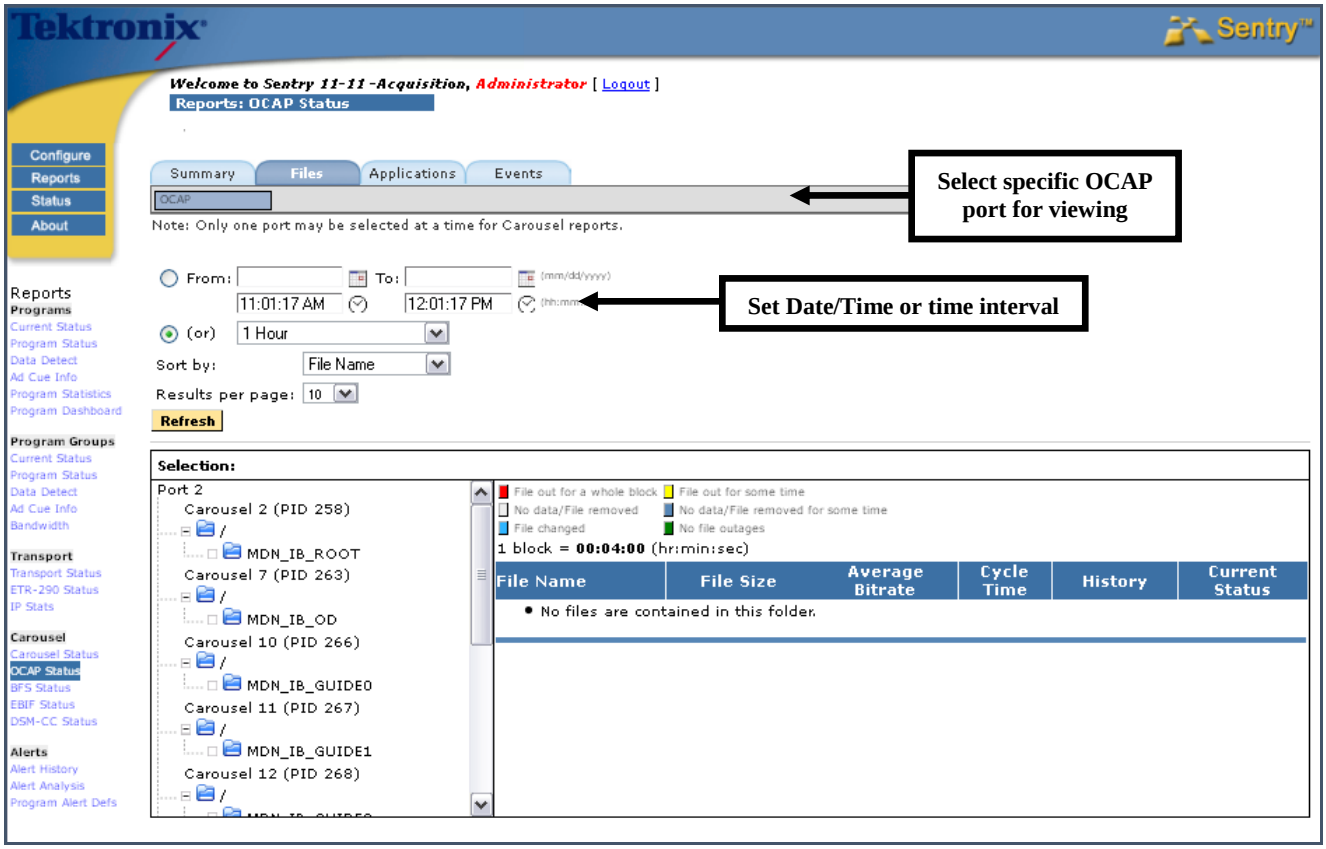


Figure 137: Files tab

Select the Viewing Time Frame

You may narrow the time frame that you wish to monitor by setting the date and time section. The radio button will auto select as soon as you click in the **Date/Time** selection fields.

If you just need to view a recent event, you may select the required time interval from the drop-down box located under the **Date/Time** select. The radio button will auto select as soon as you click on the time frame button.

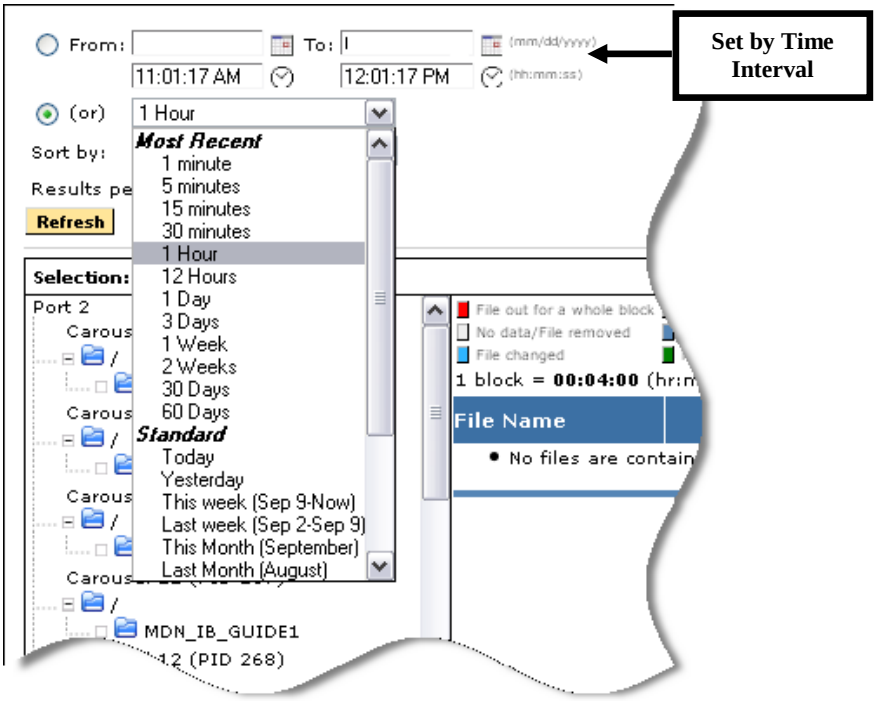


Figure 138: Setting the Time Interval

Files tab

The left pane shows all the available directories and the right pane shows the details for the carousels selected on the left. From the left pane, you may also expand directories to view the sub-directories.

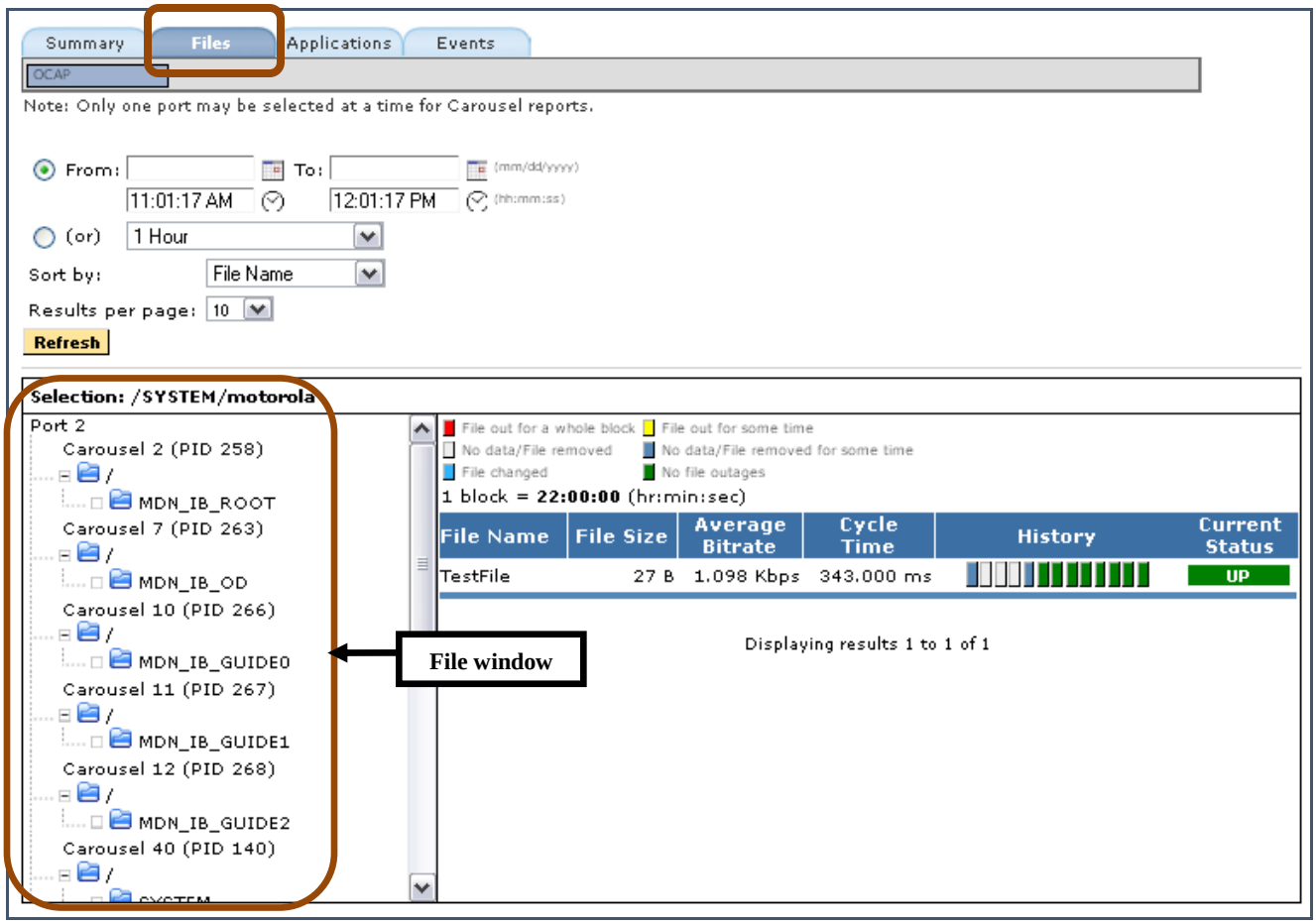


Figure 139: File window

Selecting and expanding a Directory

1. Select a directory to see more details. The details may take a moment to load.

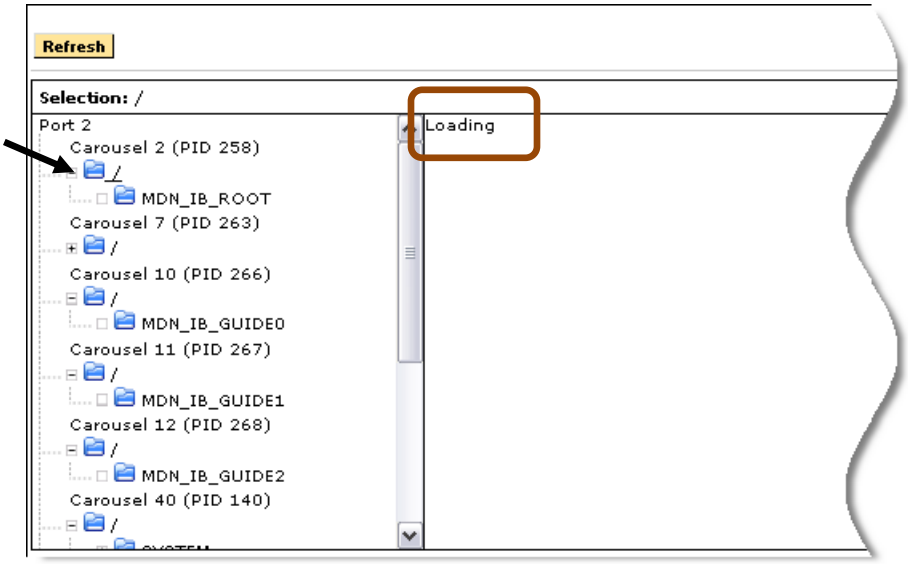


Figure 140: Selecting a directory and loading details

2. The resulting information will show the details for that carousel for the given time period.

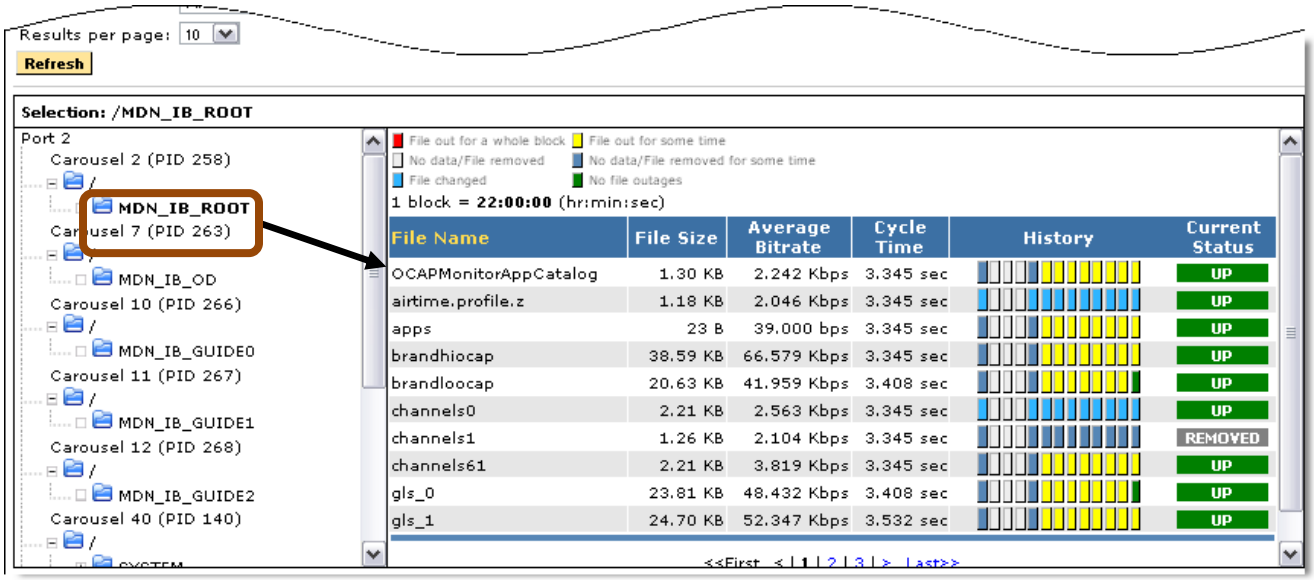


Figure 141: The details for MDN_IB_Root

3. To see subdirectories, click the plus sign next to the directory to open it and then select the sub directory you wish to see.

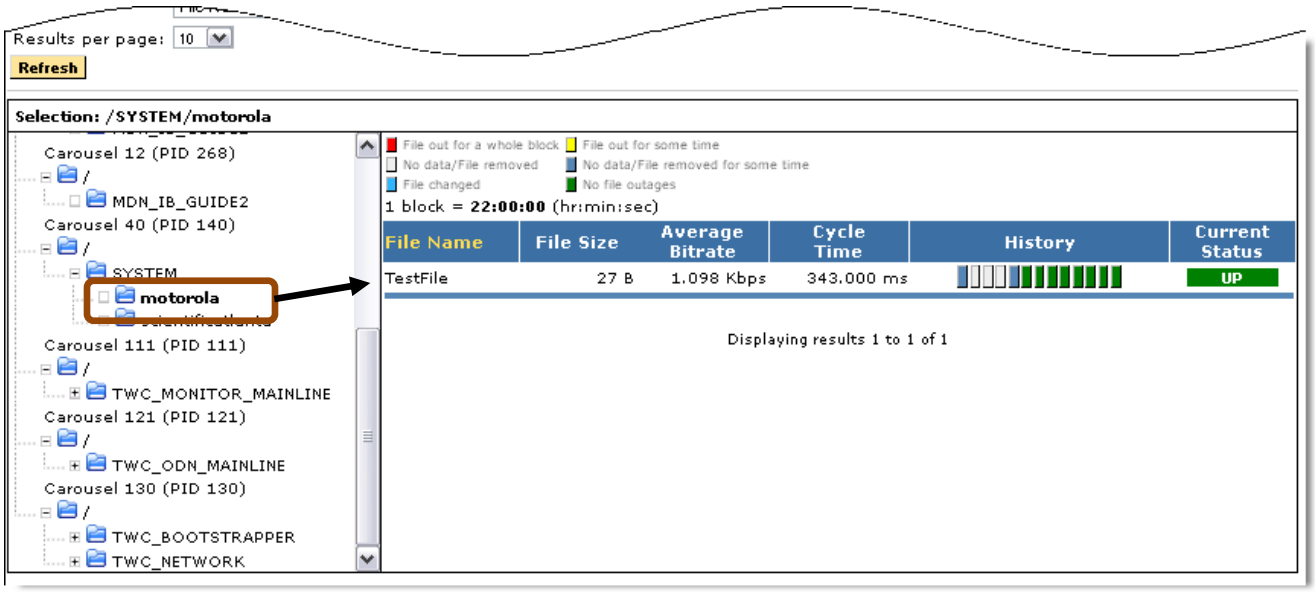


Figure 142: The Motorola sub-directory with details

Color Code Key

The following color coding applies throughout the **OCAP Status** pages.

Grey	No Data	No file referenced at this time (not a concern as no file was supposed to be referenced)
Green	No file outages	The file was present for that time period
Yellow	File out for some time	A file was present for part of the specified period
Red	File out for a whole block	File was missing for entire specified period but was supposed to be there. This may be a cause for concern
Blue	File Changed	File is present but has changed contents

Applications tab

The **OCAP Applications** tab shows what applications are referenced in the **XAIT** and **AIT**. This is where the set top box can look for particular applications to use.

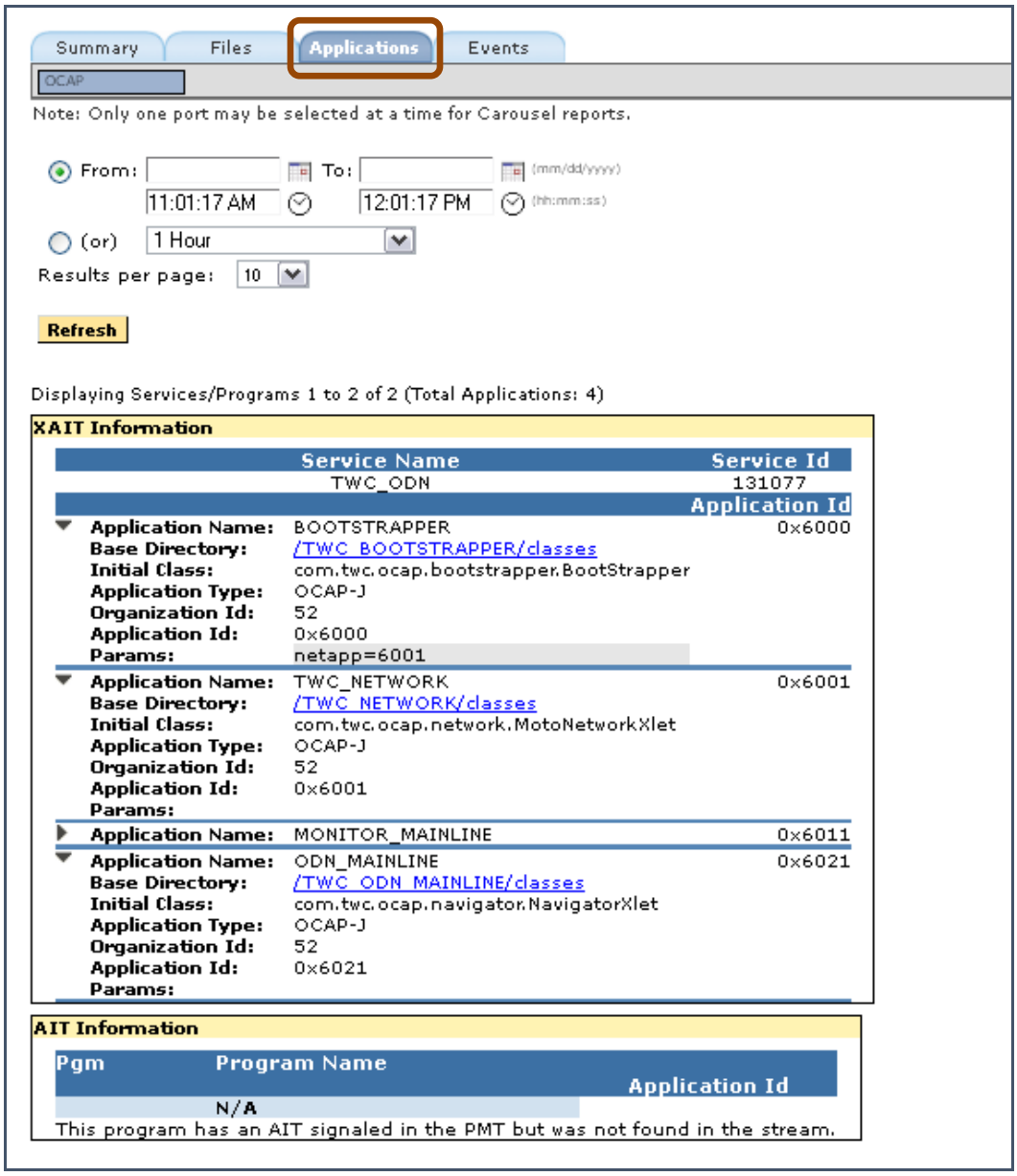


Figure 143: Applications tab

Events tab

The **Events** tab provides an **Events History** and a **File History**.

The **Events History** provides a tabular view of files and directories that have been added, removed or changed for a specified time period.

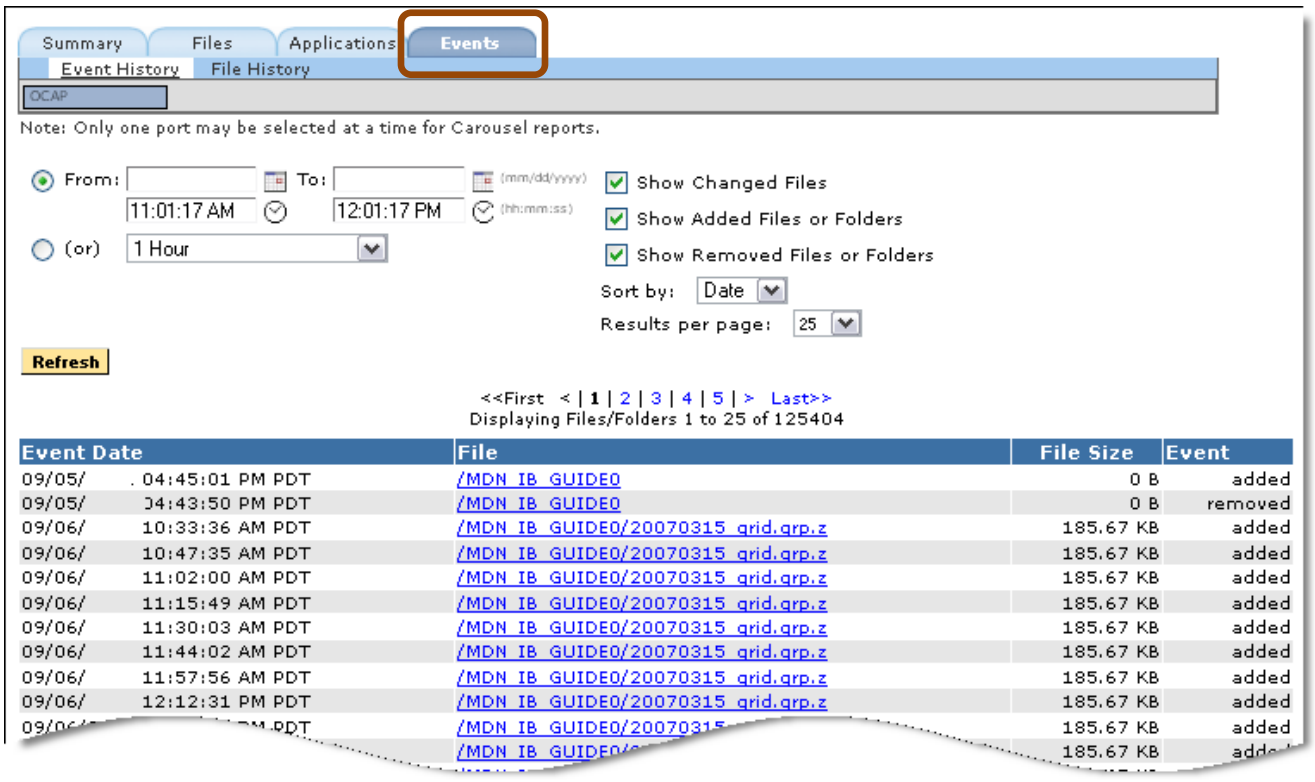


Figure 144: Event History

File History allows the user see files status for a particular time frame.

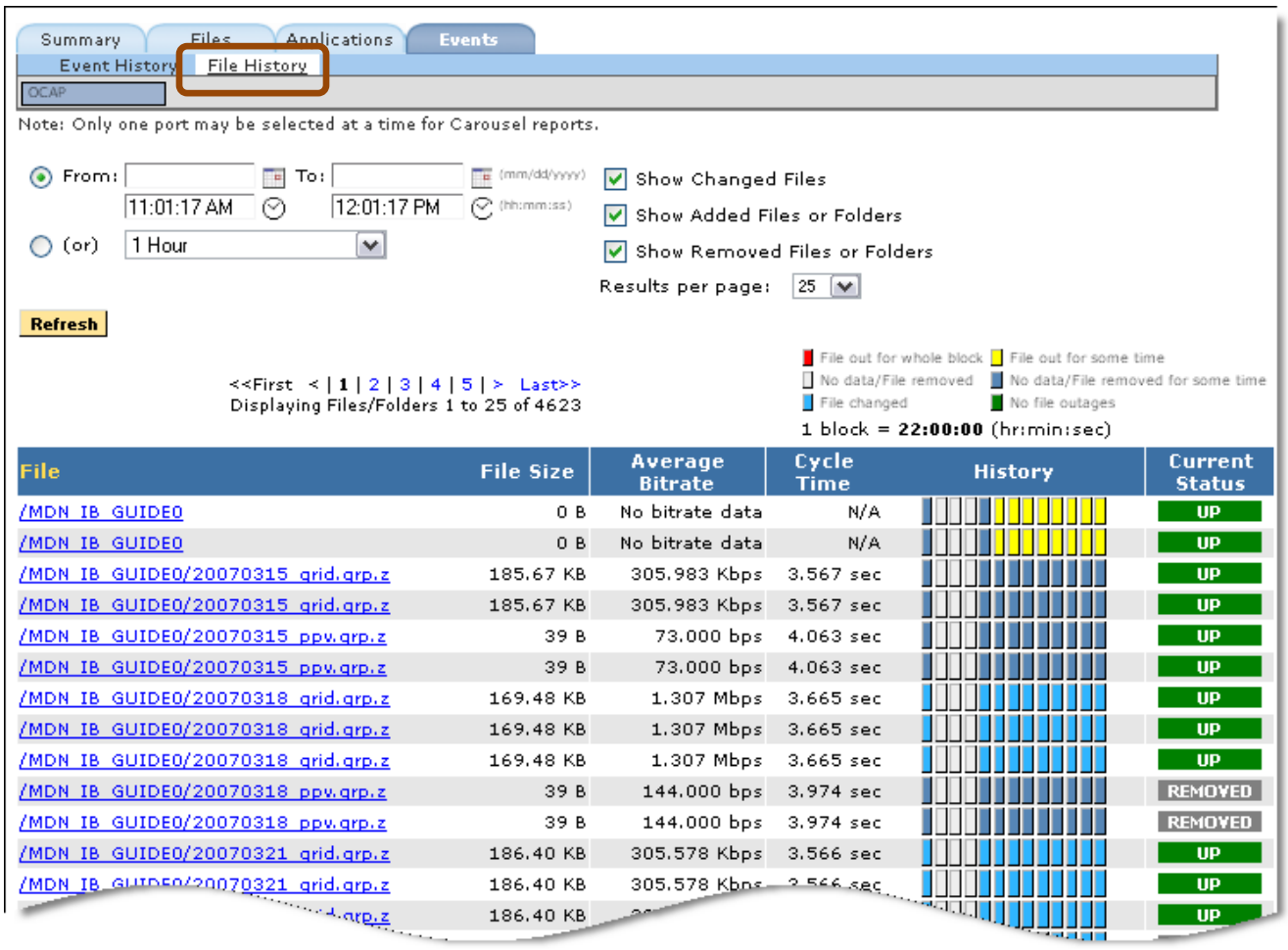


Figure 145: File History

Set Alerts in OCAP Status

1. Select **Configure** and **Alerts** from the main menu**.**
2. Next, select the **OCAP** tab.
3. From the resulting **OCAP Alerts Summary** page, you can create alerts for your particular OCAP carousel.

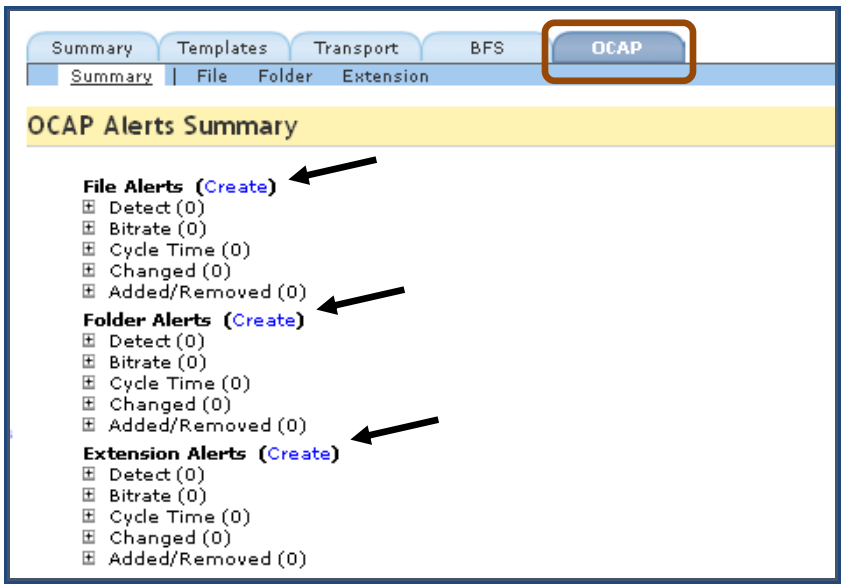


Figure 146: OCAP Alerts Summary page

4. **File Alerts** allows you to set alerts to watch a particular file or series of files.
5. **Folder Alerts** allows you to set alerts based on a series of folders and/or directories.
6. **Extension Alerts** allows you to set alerts based on a file's extension. (Ex. You can set an alert for all ".zip" files)
7. Select **Create** next to the type of alert you wish to set. In this example, we are creating a **File Alert**.
8. In **Section** 1, specify the parameters for the alert.

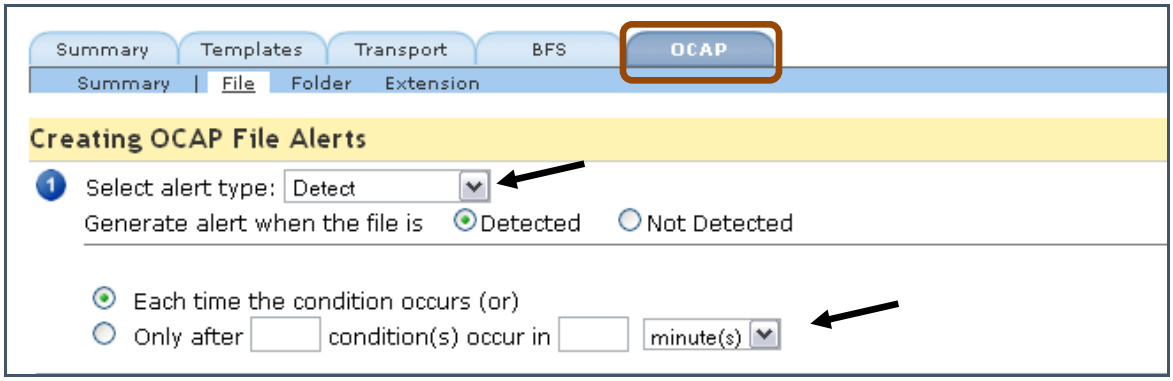


Figure 147: Step 1 Type of Alert and Time Conditions

9. In **Section** 2, for this example, locate the directory you wish to monitor by looking through the file browser.
10. Select any sub folders you wish to monitor by selecting **[add]** next to their name. They will appear in the box below the main table.

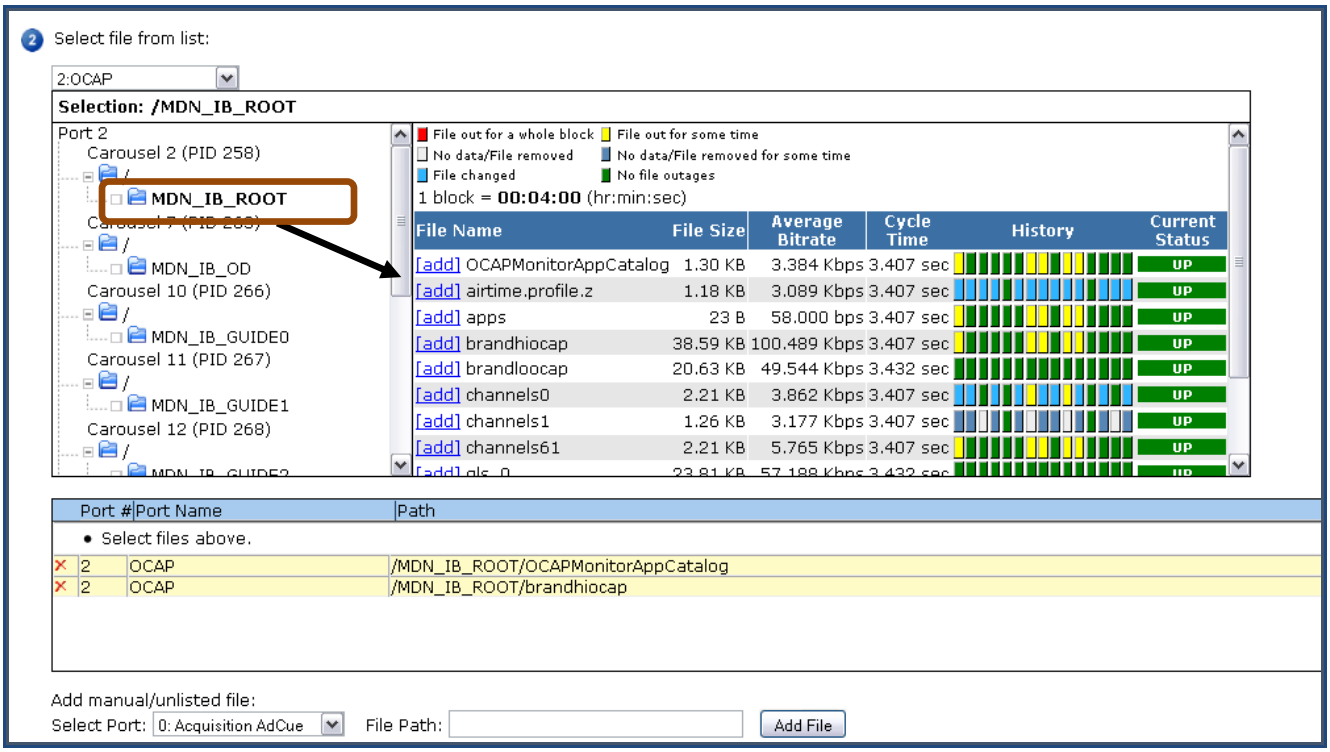


Figure 148: Step 2 Selecting directories to monitor

11. In **Section** 3, choose what you wish to happen when the alert triggers.

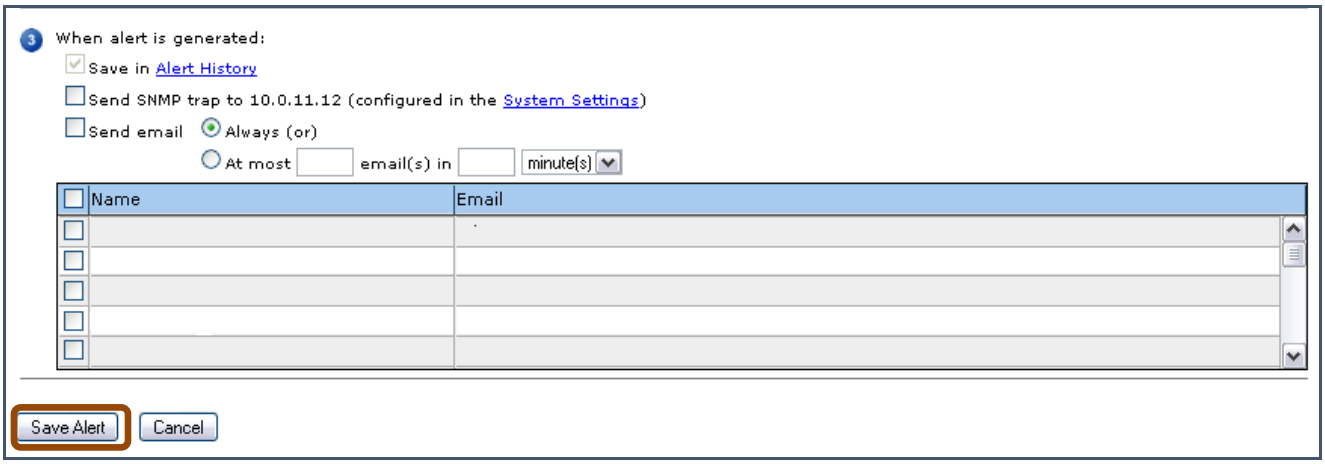


Figure 149: Step 3 Notifications

12. When you are finished, review the page, and select **Save Alert**.

Review OCAP Alerts in Alert History

1. To view any of the **OCAP Alert History**, select **Reports**: **Alert History**.
2. Next, locate **Alert Type** and click on **Select**.

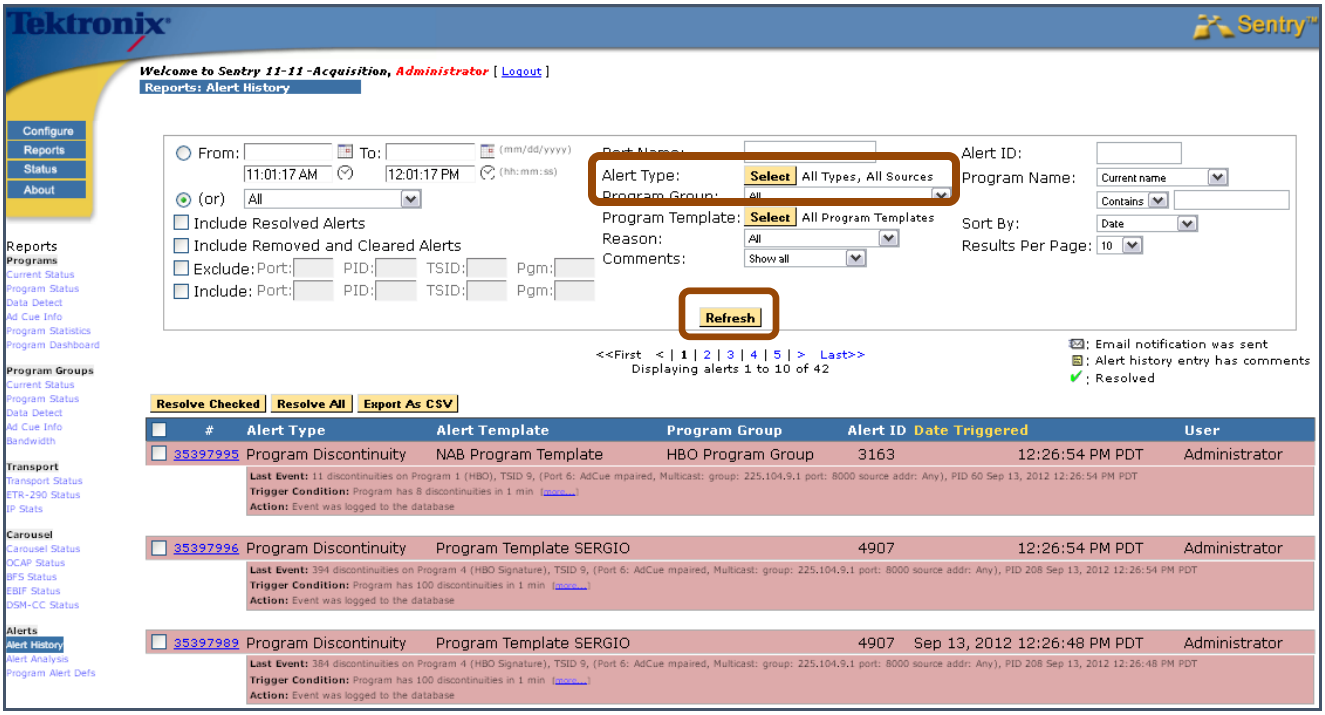


Figure 150: Alert History and Alert Source selections

3. Unselect the **All Types** option.
4. To get the options for OCAP alerts, select the following alert types (one or any combonation):
   - **Detect**
   - **Bitrate**
   - **File added or removed**
   - **Change**
   - **Cycle time**

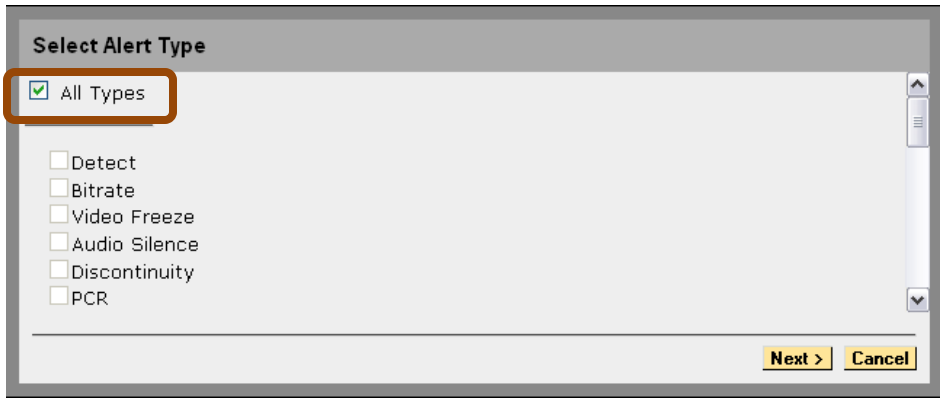


Figure 151: Unselect All Types

5. Then select **Next**.
6. Unselect **All Sources**.

Figure 152: Unselect All Sources

7. Select the OCAP alert you wish to sort by (**OCAP File, OCAP Folder** and/or **OCAP File Extension**).

Figure 153: Select the OCAP alert

8. Select **Accept.**
9. When you are returned to the **Alert History** screen, specify the the time frame you wish to view.
10. Select **Refresh**.
11. For more information see the **Alert History** section of this manual.

BFS Status

Monitoring the S-A Broadcast File System (BFS)

Sentry is designed to identify and work with data carousels within the transport. This feature is available with all versions of Sentry.

BFS Overview

The BFS provides a network file system for delivering broadcast data from server to client. Data placed in the BFS is repeatedly transmitted over the network, providing virtual storage for the DHCT. This allows an application client to quickly access the data at any time without having to request the data from the server. This mechanism is useful when all DHCTs running the application use the same data.

An example is a stock quote and statistics application that makes the same stock information available to any DHCT that has access to the application. Rather than sending the information to each DHCT or having each DHCT request the information, the application server updates the data once in the BFS and it is then broadcast over the network to the DHCTs. BFS files can be transmitted in-band over QAM or out-of-band over QPSK. Application clients access files over the BFS using the PowerTV Stream Manager interface.

BFS Mapping

There is a direct mapping from the S-A BFS to Sentry. All S-A BFS servers map to programs within Sentry (see figure below). All PIDs carrying these programs are associated with these servers.

The following **S-A BFS** information is available within Sentry (including reports and alerts on **S-A BFS** activity):

- **Server available or not available**
- **Sessions active or not active**
- **Server datarate**
- **Frequency and duration of events**
- **Datarate verification**
- **Server source type**
- **Server aggregate**

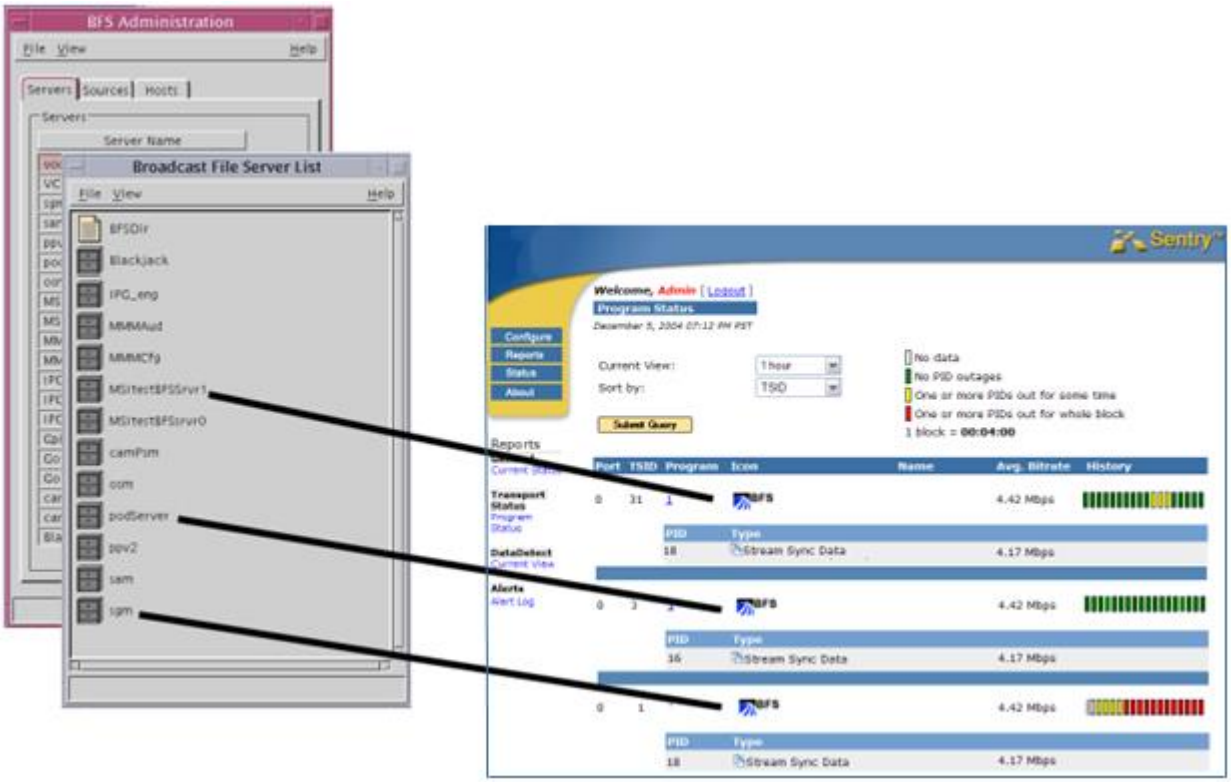


Figure 154: Mapping between Scientific-Atlanta's DNCS BFS Servers and Sentry Programs

Access BFS Status

Select **Reports** and then **BFS Status.**

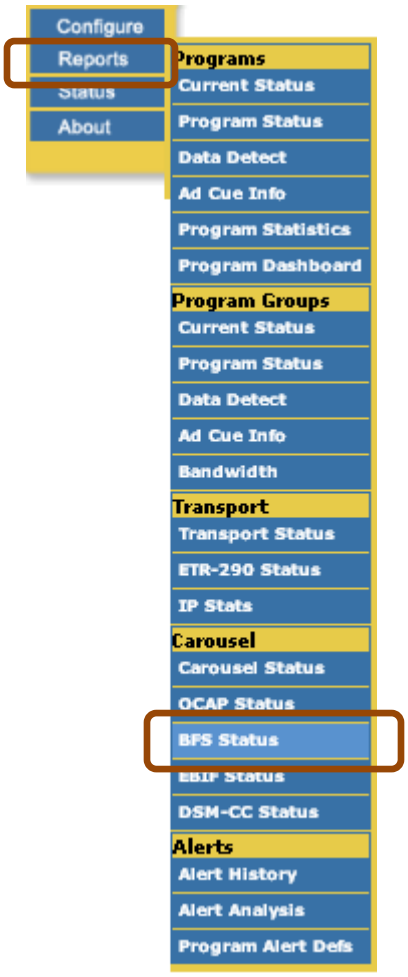


Figure 155: Accessing BFS Status

Summary tab

Click on the **Summary** tab for a summary view of the BFS status on ports that have carousel data.

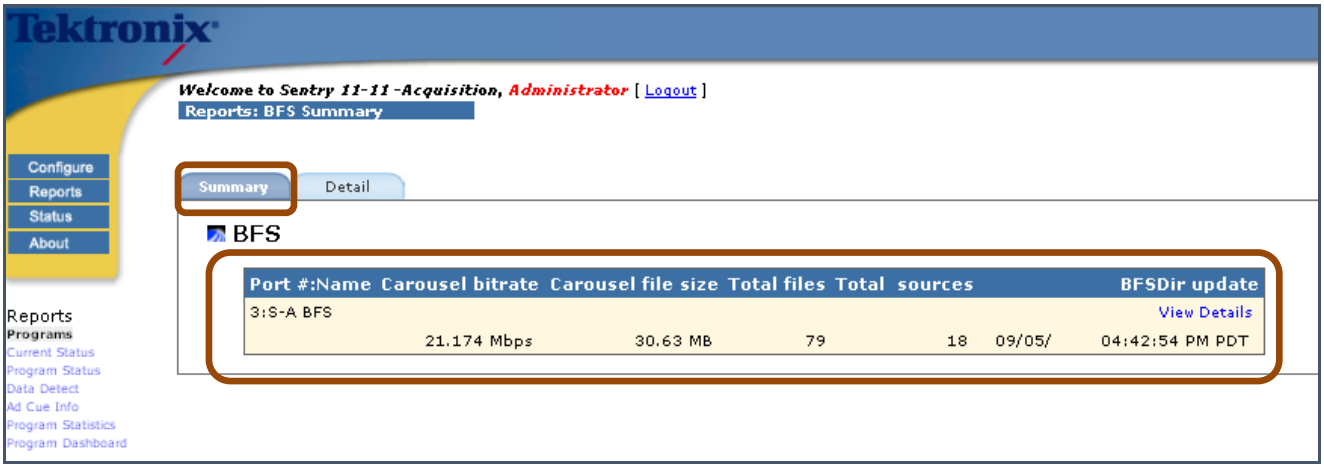


Figure 156: BFS Status Summary

- **Carousel bitrate**
  The total bitrate for the entire **BFS.**
- **Carousel file size**
  The total size of all the files on the **BFS.**
- **Total files**
  The number of files being carouseled on the **BFS.**
- **Total Sources**
  The total number of sources being pulled from.
- **BFSDir update**
  The last time the **BFSDir** file was updated. The **BFSDir** file is a special file in the source that contains the file names that are shown when the source is expanded. It is designated as such in **Configure: BFS Settings**.

Detail tab

For a detailed view of **BFS** data on one port, select the **Detail** tab

To view the details for a specific port, click on the desired port from the table.

Only one input port may be selected at a time for BFS reports.

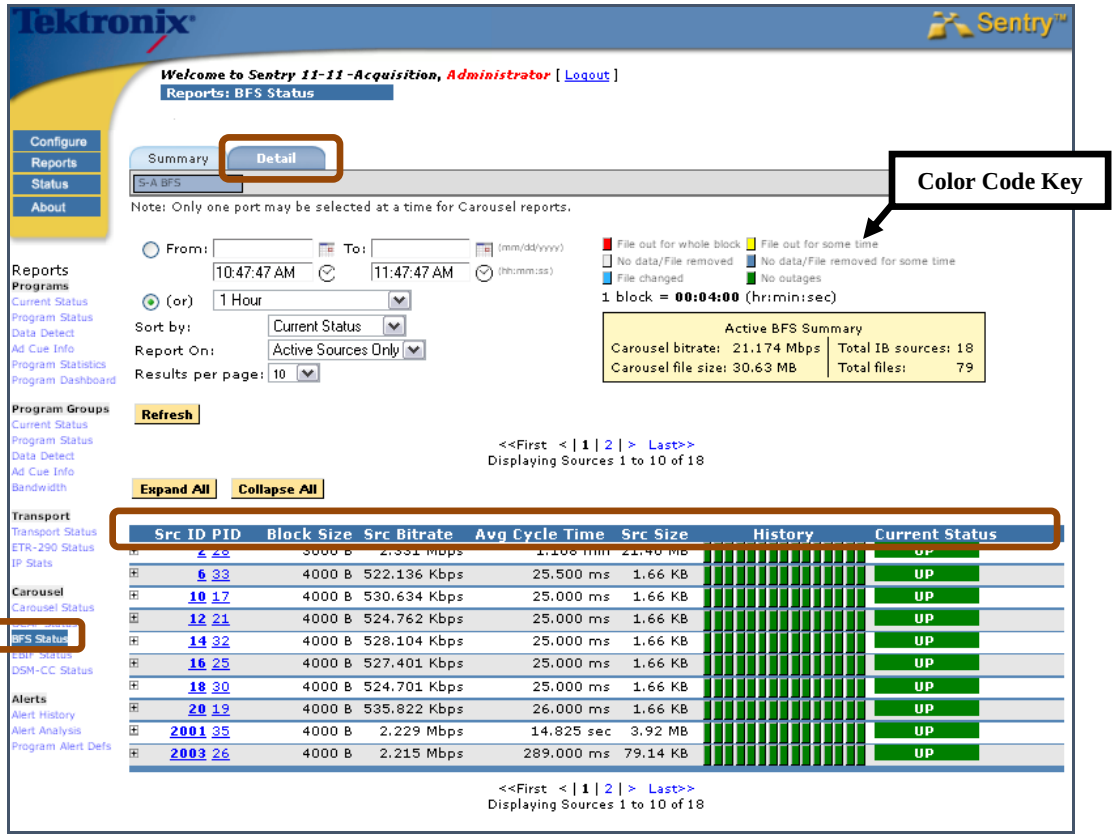


Figure 157: BFS Status Detail tab (expanded)

- **Source ID**
  The source ID assigned to this source on the BFS
- **PID**
  The PID that is assigned to the source
- **Block Size**
- **Src Bitrate**
- **Average cycle time**
  The average time that the source takes to complete one cycle
- **Source size**
  The sum of all file sizes in the source
- **History**
  A color-coded graphical view of the status of the source over a selectable period of time

- **Current Status**
  Indicates UP (green) if all files in the BFS Source are getting data. If some but not all files are getting data, the Status indicates UP annotated with the number of up files out of all files, e.g., 7 of 8. The Status indicates DOWN (red) if the bitrate for all files is zero.

File cycle times are measured from block 0 (zero) of the file until the next time it sees block 0 again. Using this method you can see how long it takes for a given file to be delivered, which is very helpful when trying to tune your BFS to lower load times on the set top box.

BFS Status may also be expanded to see all data in detail via the **Expand All** button or may be expanded one section at a time with the plus/minus buttons.

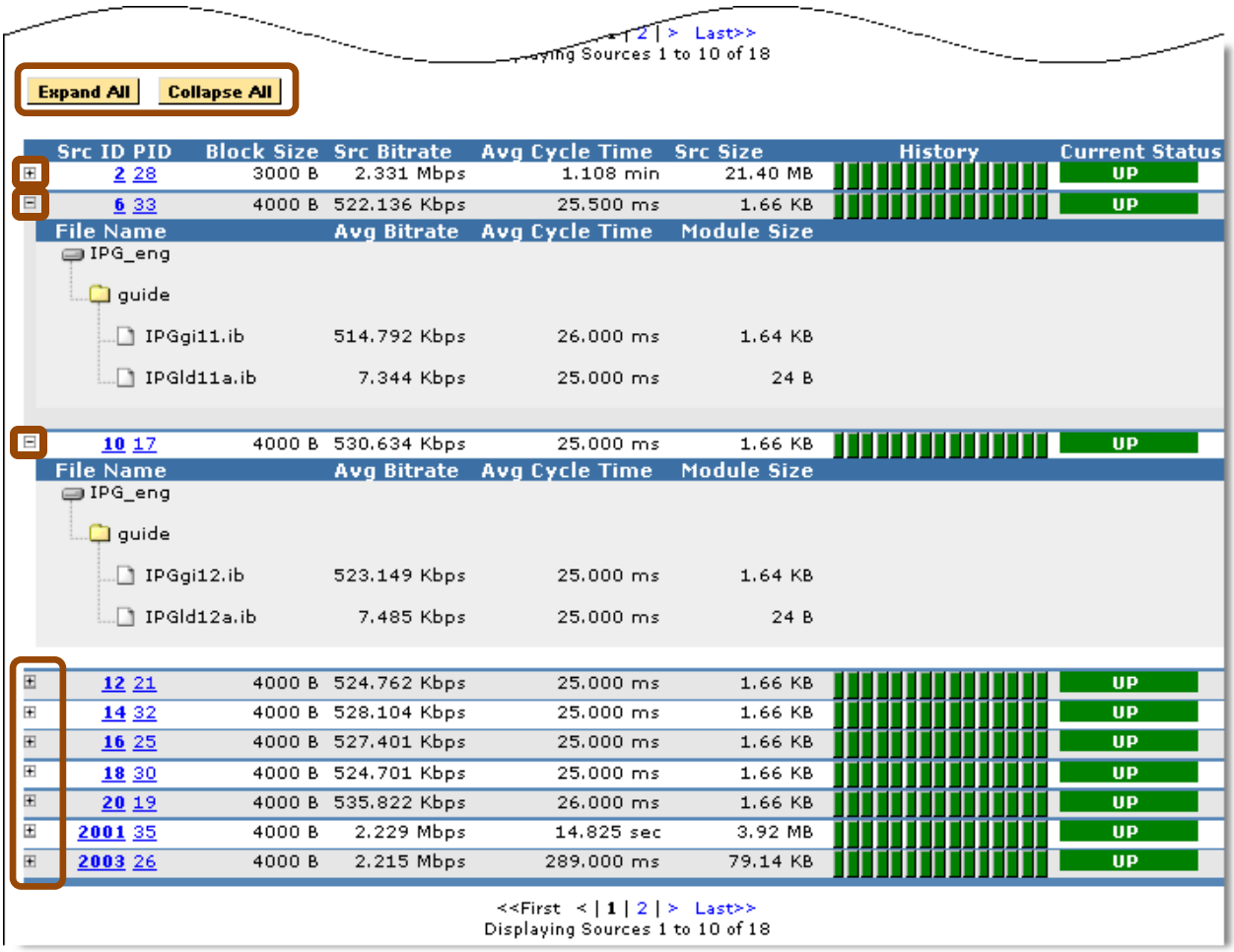


Figure 158: BFS Status Report with the top Three Sources Expanded

Drill Down to BFS Detail View

To go to the **BFS Detail View**, select the **BFS Source ID**

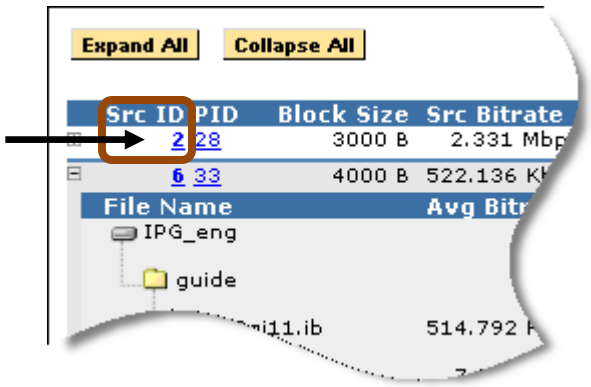


Figure 159: Select Src ID number

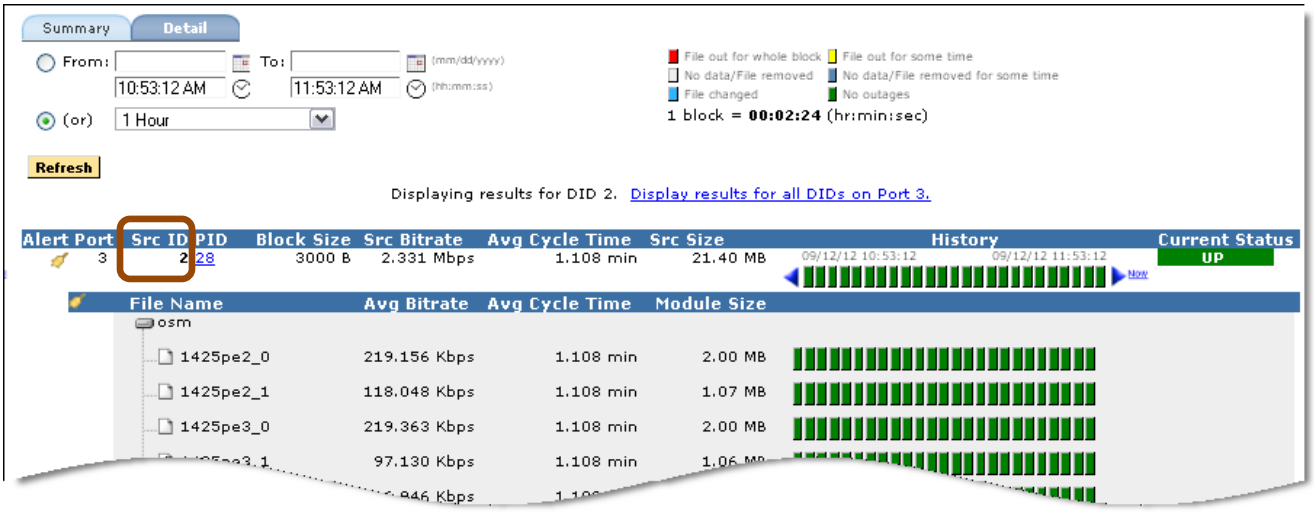


Figure 160: BFS Detail View for Source ID 2

To navigate to the **Program Detail** page for a particular PID, select the PID assigned to the **Source ID**.

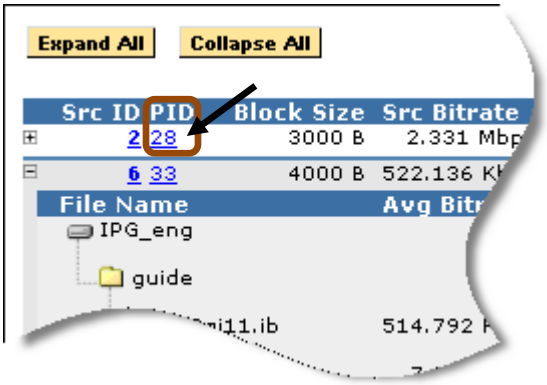


Figure 161: Selecting the PID

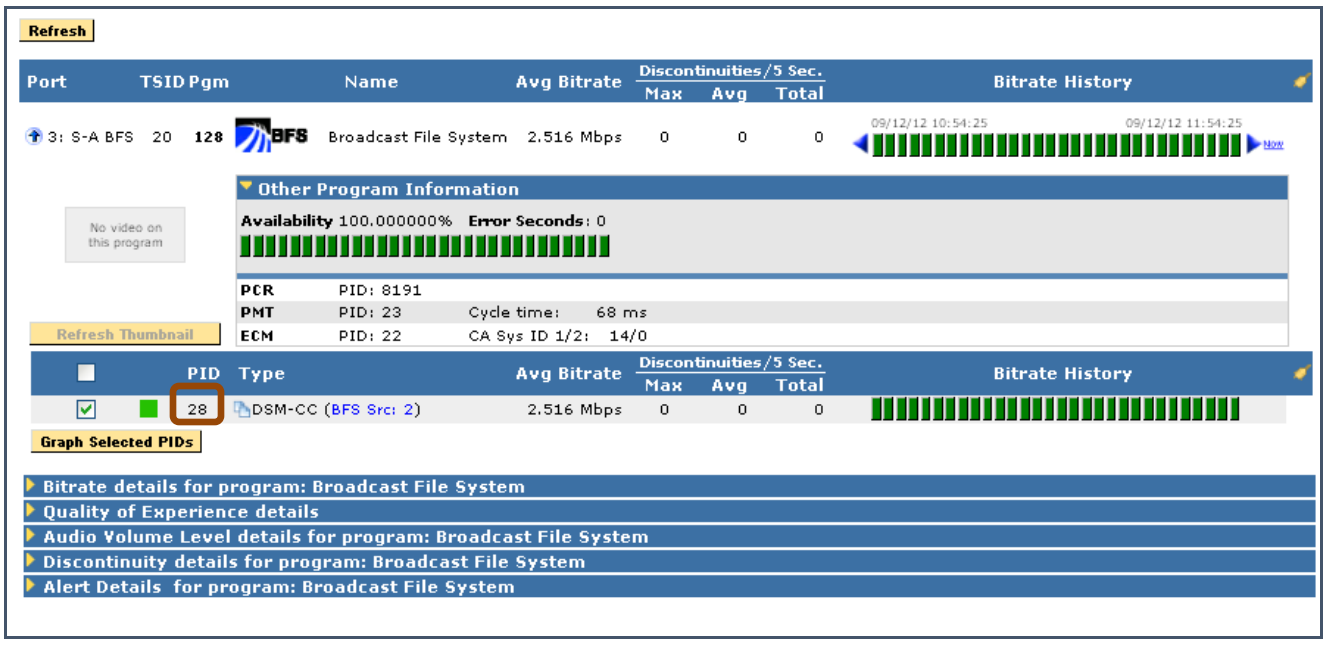


Figure 162: Source Program Detail from selecting PID 113

EBIF Status

EBIF (Enhanced TV Binary Interchange Format) is an industry standard for an optimized collection of code specifications that control interactive widgets that define one or more multi-media pages used specifically for enhanced television or for an interactive television system.

EBIF can also be defined as a standardized data carousel that is used in enhanced television systems.

An **EBIF** file is a sequence of bytes that conforms to the **EBIF** content format, and forms the primary information contained in an **ETV** application. An **ETV User Agent** then acquires, decodes, presents (by way of widgets), and executes (by way of actions) data contained in an EBIF resource in order to present a multimedia page to an end-user.

EBIF is an optional module on a Sentry line of products. If you have an **EBIF** module installed, the Sentry will perform a full decode of the **EBIF** carousel and log relevant data concerning structure and attributes.

All tabs and column headers link to the same pages. For instance, the **Applications** tab links to the same page as the **Applications** column header.

Access EBIF Status

1. Select **Reports** and then **Carousel**.
2. Next, select **EBIF Status**.

Summary tab

The **Summary** tab displays an overview of all ports and their relevant information.

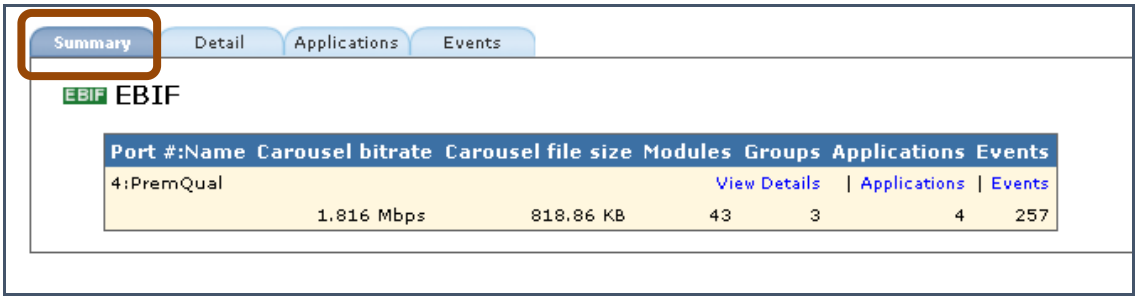


Figure 163: Summary tab

Detail tab

The **Detail** tab shows detailed reports on any selected **Port**. Only one **Port** may be viewed at a time.

View a report:

1. From the **Detail** tab, choose the port for the multicast. (In this example, Port 0.)
2. Select the desired time frame and select Refresh.

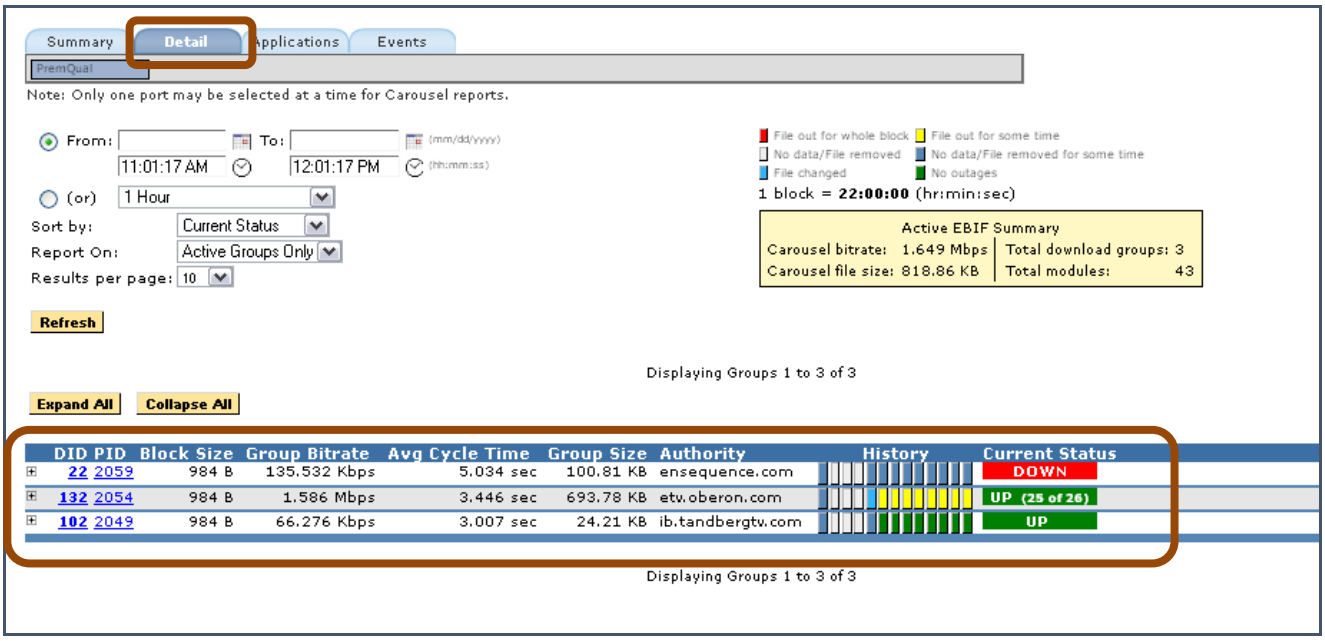


Figure 164: Detail tab

- **DID (Download ID)**
  Select to get a report of the history of each individual module.
- **PID (Packet ID)**
  Select to go back to the associated program that the EBIF carousel is bound to.
- **Block Size**
  The size of the DDB component that makes up the smallest "packet" (or block) of data for the files / modules listed on the BFS, OCAP and DSM-CC reports
- **Group Bitrate**
  The sum of all the bitrates of all the modules in the bitrate ID
- **Avg Cycle time**
  The average of the cycle times for all the modules
- **Group Size**
  The size of the current group

- **Authority**
  The server name
- **History**
  The block view following the main legend
- **Current Status**
  Up: The number of modules currently present.
  Down: The number currently down.
- **Pending**
  Data coming in but is still processing.

Viewing Program Detail from EBIF Status

To view the **EBIF Report** for a particular PID, select the desired PID in the first column of the table on the **Details** tab.

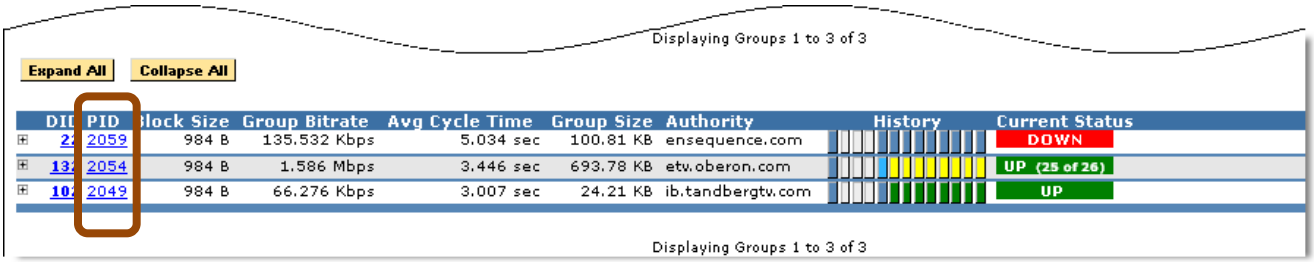


Figure 165: Selecting PIDs for EBIF Details

The resulting screen will take you to the **Program Detail** page. All blue underlined sections are clickable links.

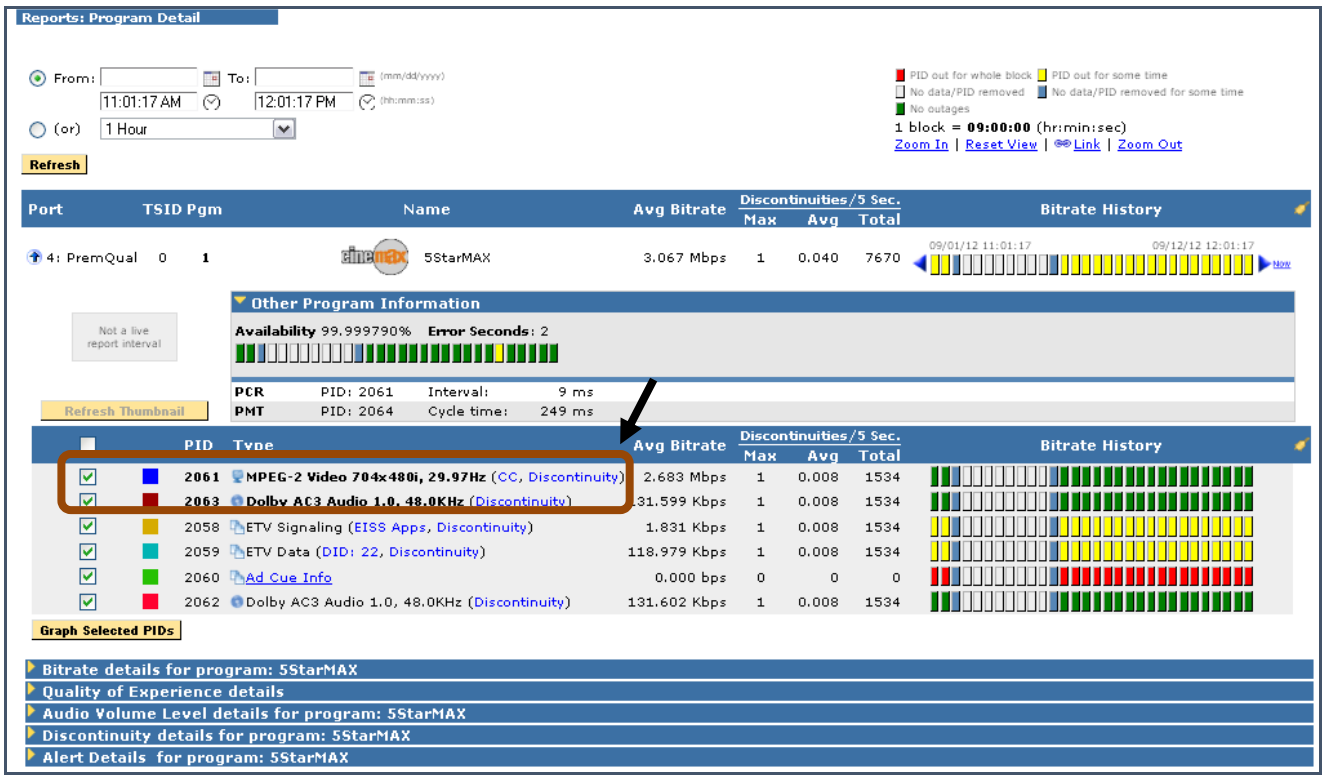


Figure 166: EBIF Program Details screen

- **EISS Apps (EISS-ETV Integrated Signaling Stream)**
  - Carries Media Time Line Messages, Stream Events, EISS Tables for an ETV application.
  - Tells the user application when to function and when data is present
  - Clicking this link will take you to the Application tab for the port that contains this program.

- **ETV Data**
  - Some services have constant EBIF data, while others are intermittent.
  - Other providers may only have them together during selected commercial breaks.
  - Clicking on the DID will take you to the EBIF Detail report for that particular DID.

Applications tab

The **Applications** tab shows you the application EISS history for a specified time frame for that particular port.

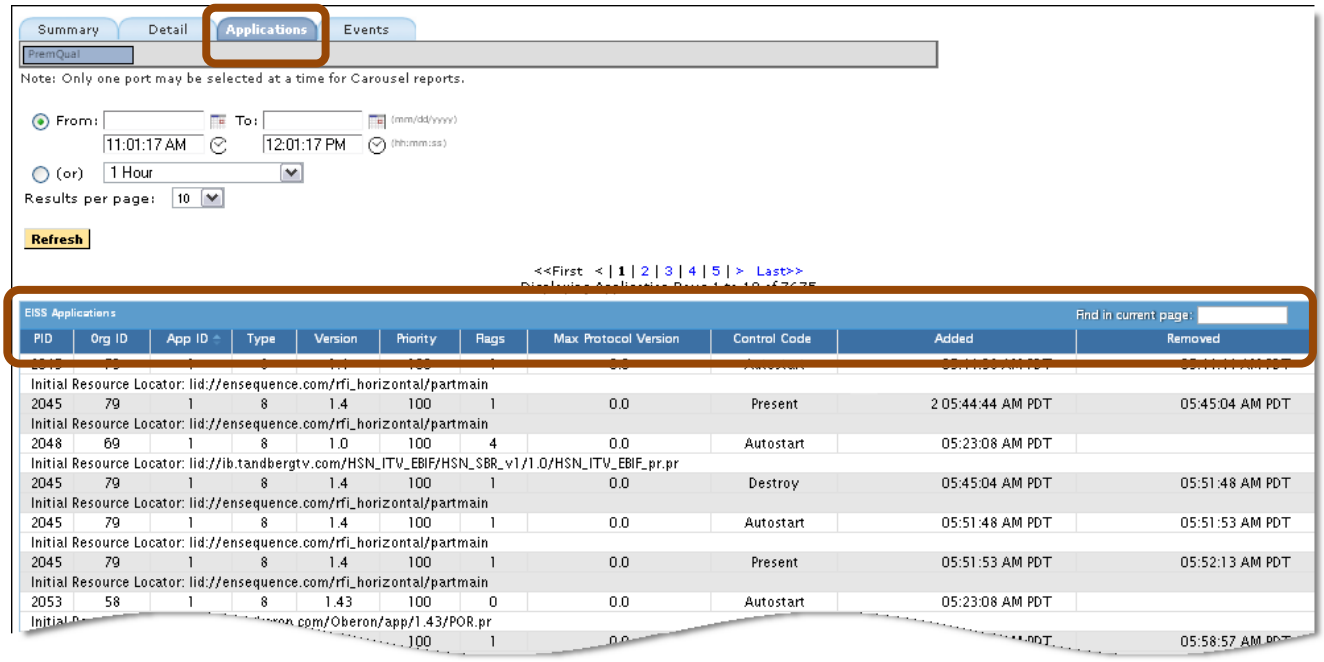


Figure 167: Applications tab

- **Organization ID (Org ID)**
  - This 32 bit field is a globally unique value identifying the organization that is responsible for the application.
  - These values are registered in ETSI TR 101 162 [10].
  - Values of zero will not be encoded.
- **Application ID (App ID):**
  - This 16 bit field uniquely identifies the application function.
  - This is allocated by the organization registered with the Organization ID who decides the policy for allocation within the organization.
  - Values of zero will not be encoded.
- **Type**
  - This 16-bit integer identifies the type of application being signaled.
  - At the time of this writing, type 8 corresponds to "ETV-Binary Interchange Format (ETV-BIF) application."
- **Version**
  Application version number.
- **Priority**
  This field identifies a relative priority between the applications signaled in this service. The greater the numerical value, the higher the application priority.

- **Flags**
  Each application has a set of flags. This field represents the test flag.

- **Max protocol version**
  This field, if non-zero, specifies the maximum major (EISS) protocol version supported by user agents that should decode this application.

- **Control Code**
  This field controls the state of the application. As of this writing, currently defined values for Control Code are:
  - **Autostart -** The primary application resource is loaded and the application is started, subject to the usual restrictions, etc.
  - **Present -** The primary application resource is loaded, but is not started, pending the receipt of another trigger, or Application Information descriptor.
  - **Destroy -** The application is signaled to quit by generating a DESTROY event to the application.

- **Added / Removed**
  Date time stamps when this application was added / removed from the stream.

Events tab

The **Events** tab shows a history view of when modules were changed, added or removed.

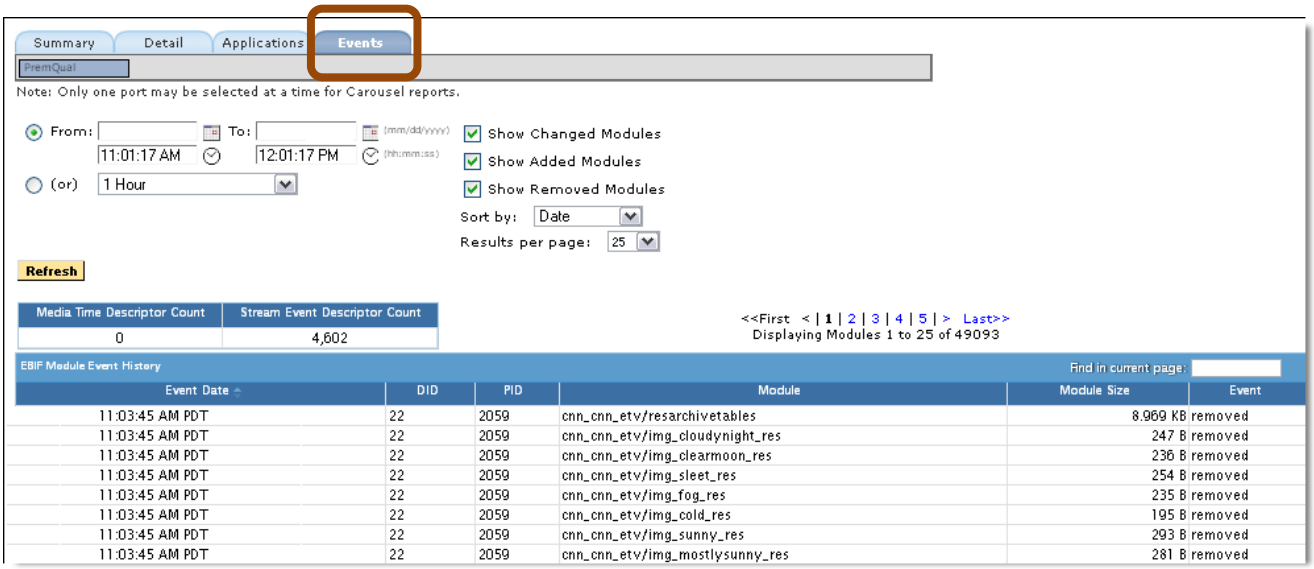


Figure 168: Events tab

Alerts

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 **#** in the first column of the log is unique for each alert detected while the **Alert ID** column is unique for each alert configured. Refer to **Configure Alerts** for types of alerts and how to create/modify/delete them.

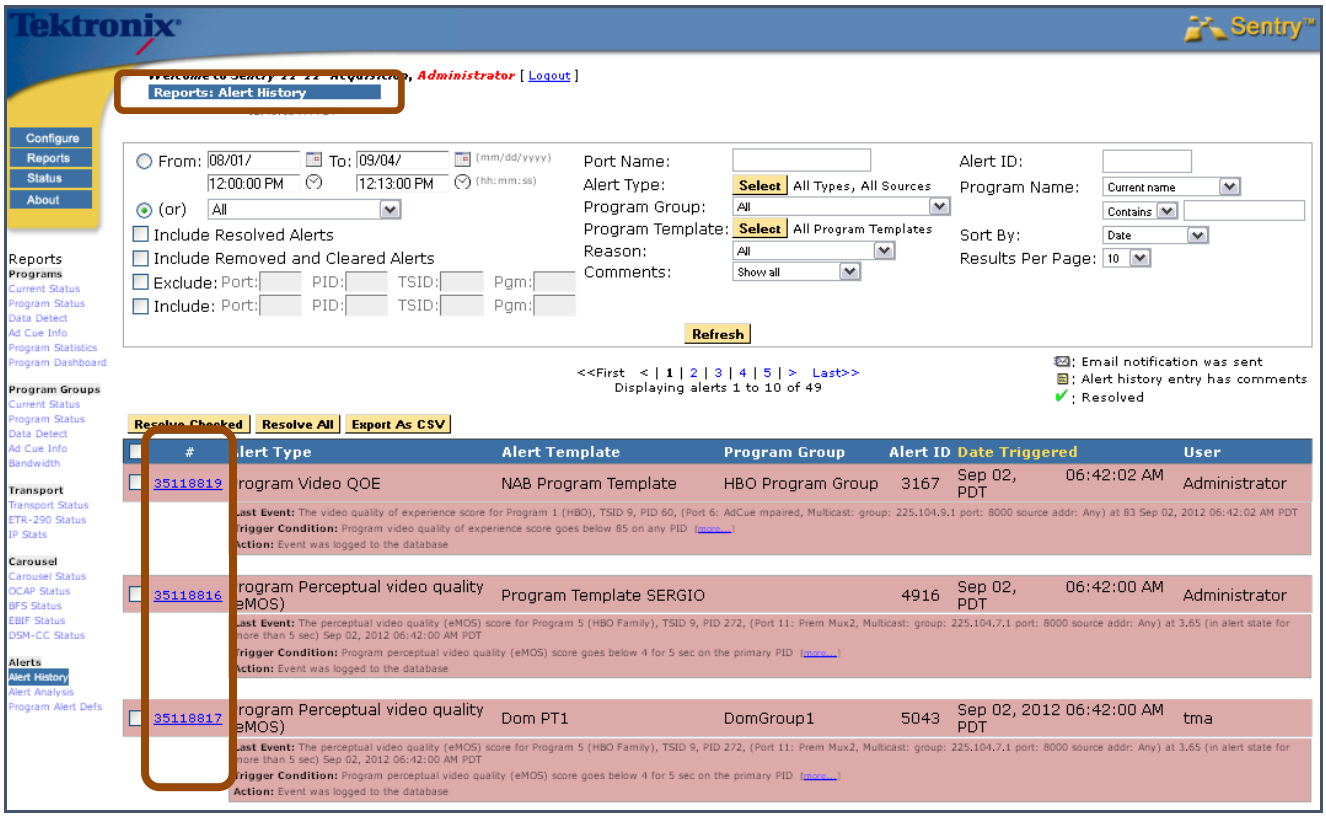


Figure 169: Alert Log

For any program alert, you may click on the program name in the **Alert History** and it will take you to the half hour on either side of where the error occurred. Click on the program name in the **Event Log** to take you to the **Program Detail Report** for specified alert.

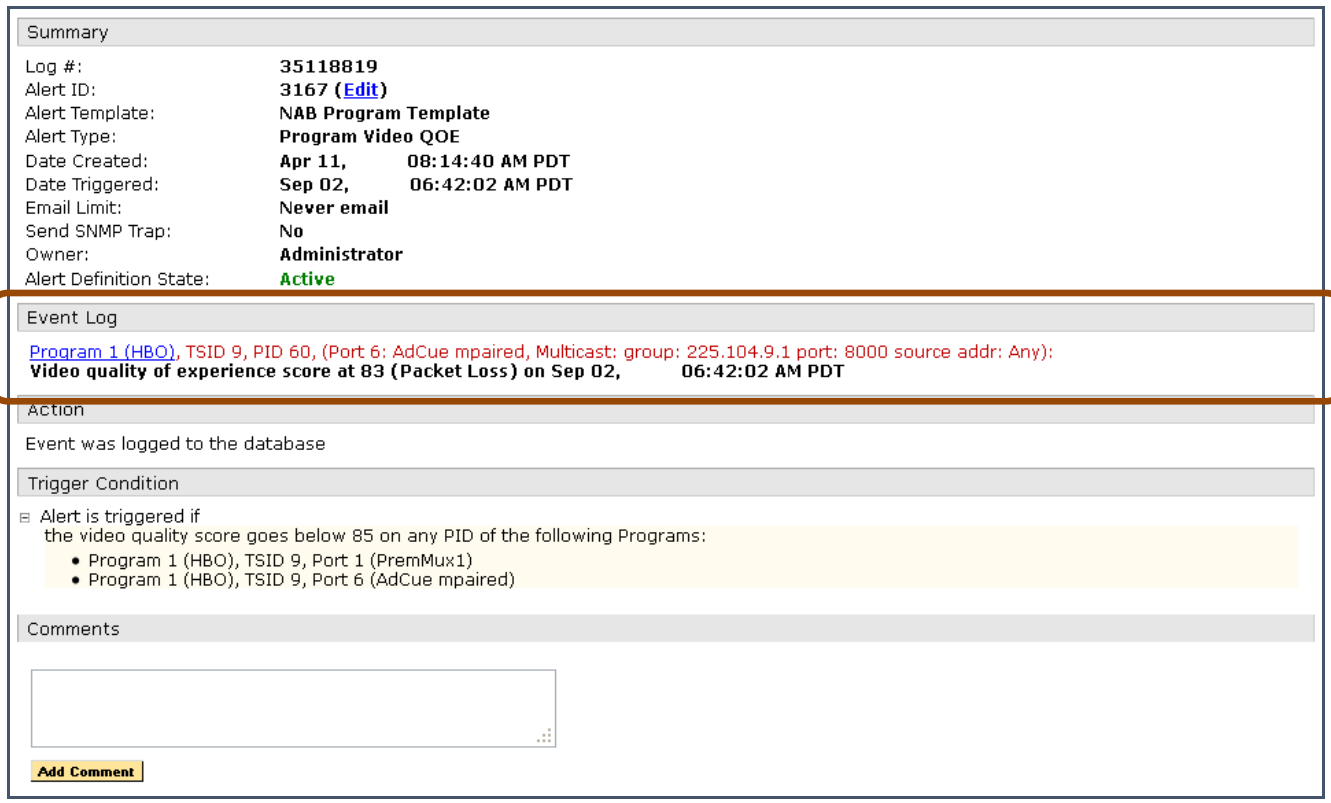


Figure 170: Event Log detail

An alert that has been deleted from the configuration is shown as **Deleted** in the **Status** column. An alert that is still active in the system is shown as **Active** in the **Status** column.

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 Log**), 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 **Delete Checked** or **Delete All**. The contents of the list can be filtered using the many filter options at the top of the **Alert Log**, and only the filtered items will appear in the log.

For any **PID Alert**, the program associated with the PID is reported in the **Alert History**, emails and SNMP traps.

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.

Accessing Report Export

Select **Alert History** from the **Reports Toolbar**.

Figure 171: Accessing Alert History

Exporting a file as a CSV

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

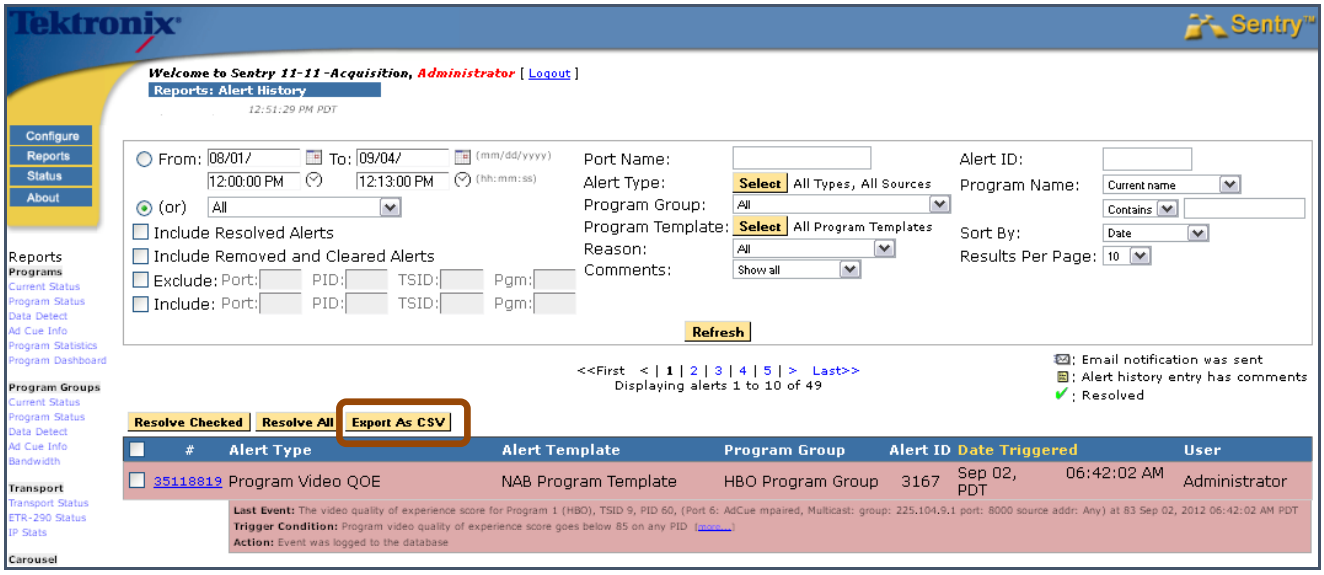


Figure 172: Selecting a Report from the Alert History Page

NOTE: ***The Export to CSV function will export ONLY what is currently displayed on the alert history. If your report spans multiple pages, you will need to run an export per page.***

---

2. 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**.

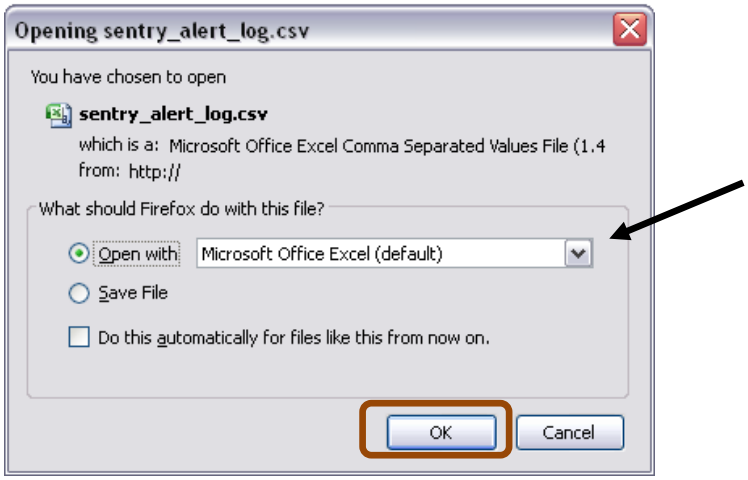


Figure 173: The Export To dialog box

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

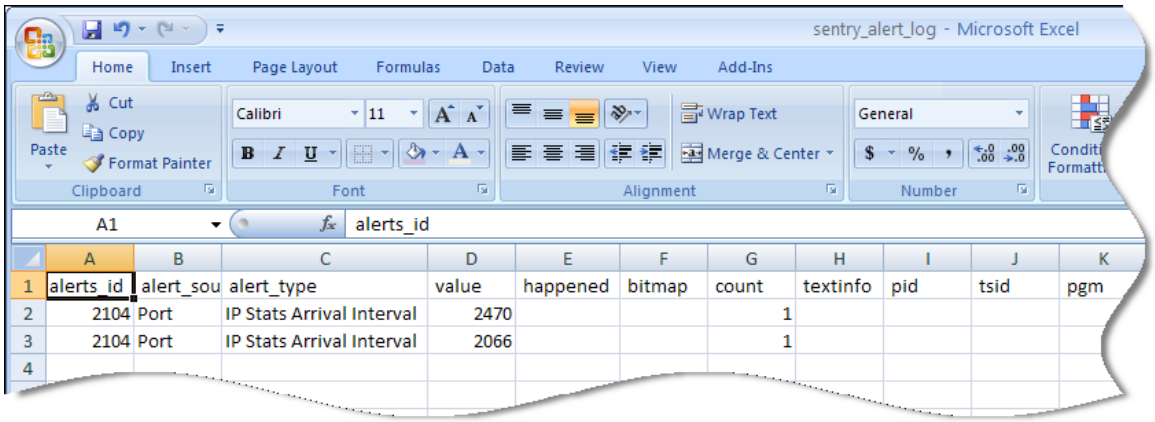


Figure 174: A report exported to MS Excel

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.

Results are shown in groups of 30 for easy navigation.

Access Alerts Analysis

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

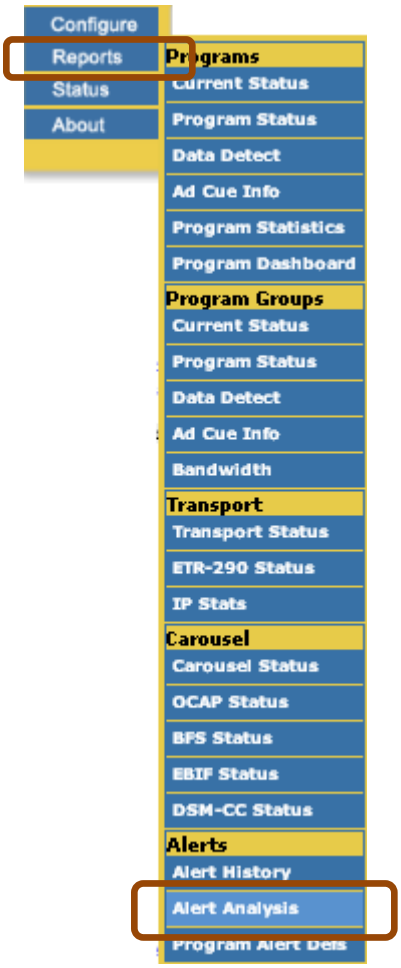


Figure 175: Accessing Alert Analysis

Alert Analysis Summary Screen

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

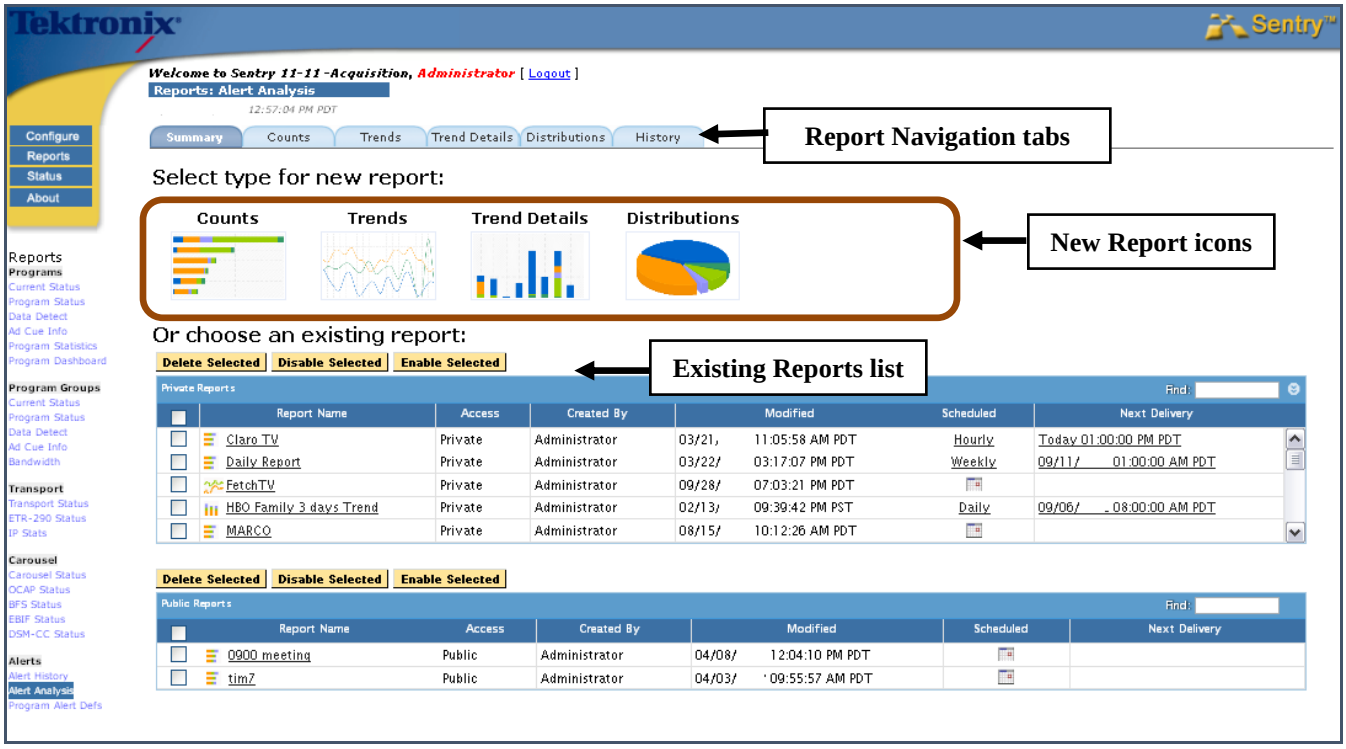


Figure 176: Alert Analysis Screen

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 and/or modify saved reports.
- **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) Takes user to a history of when and what alerts were emailed.

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.

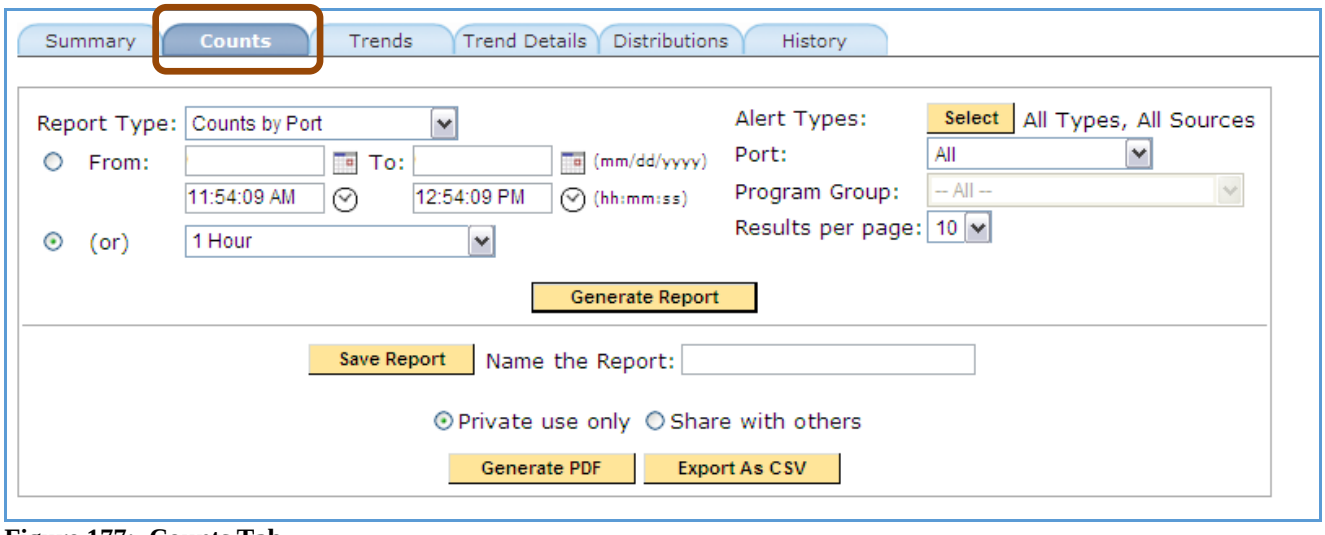


Figure 177: Counts Tab

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** at **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**.

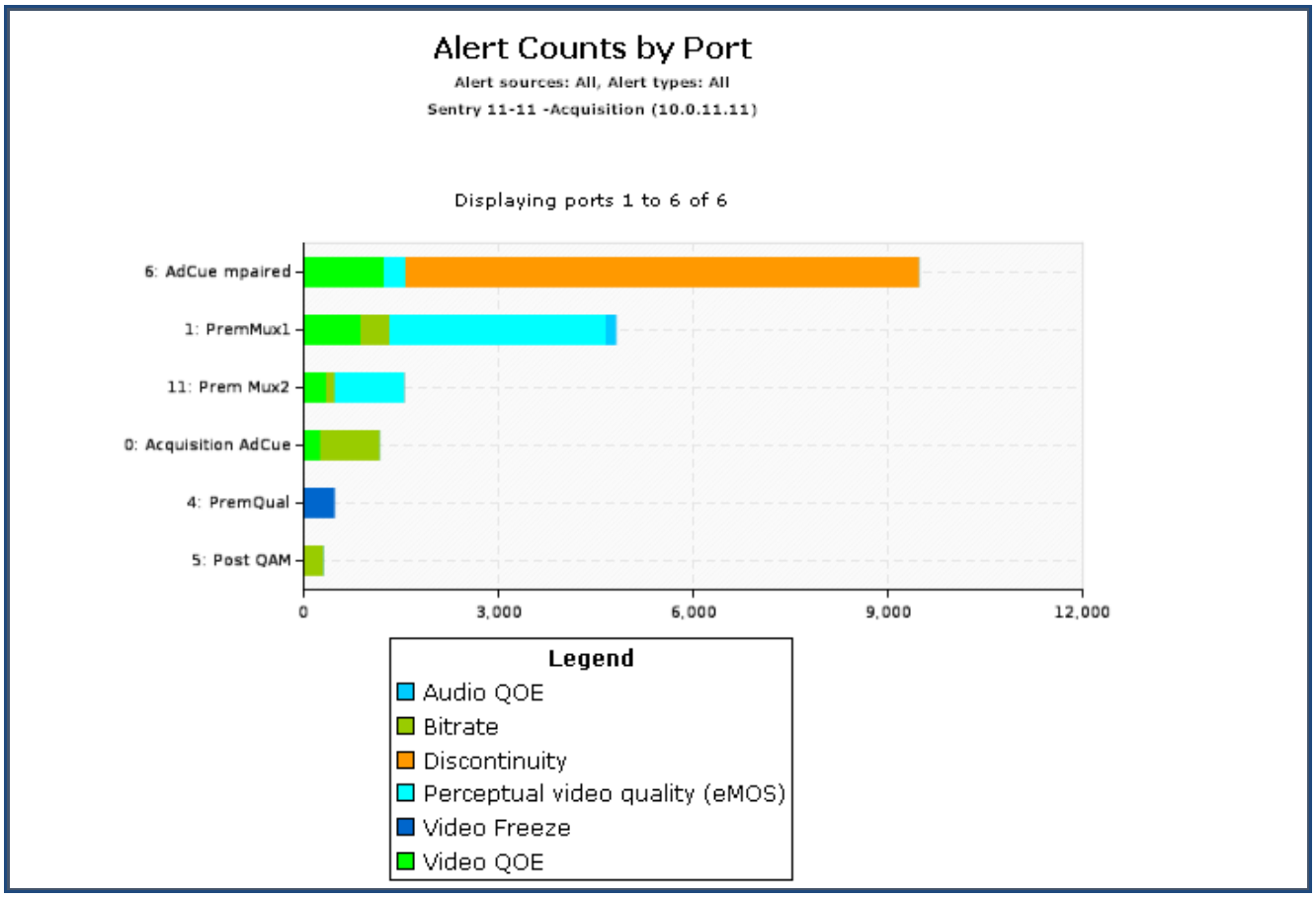


Figure 178: Alert Counts by Port

NOTE*: If you create a Counts By Program report, the program links within the table will link back to the Program Detail report for the time period specified.*

Saving a configured 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. Give the report a name and select **Save Report**. You cannot schedule a report that hasn't been saved.
2. .Select the **Schedule** button that appears after the report has been saved.

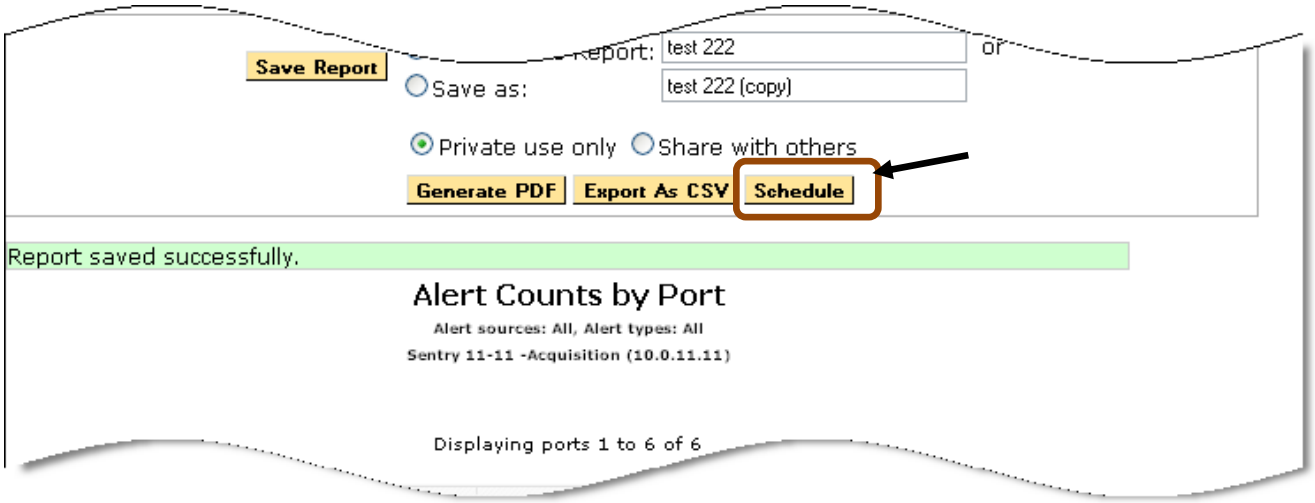


Figure 179: Selecting Schedule

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

4. **Section 2: Select recipients**
   a. Format the email

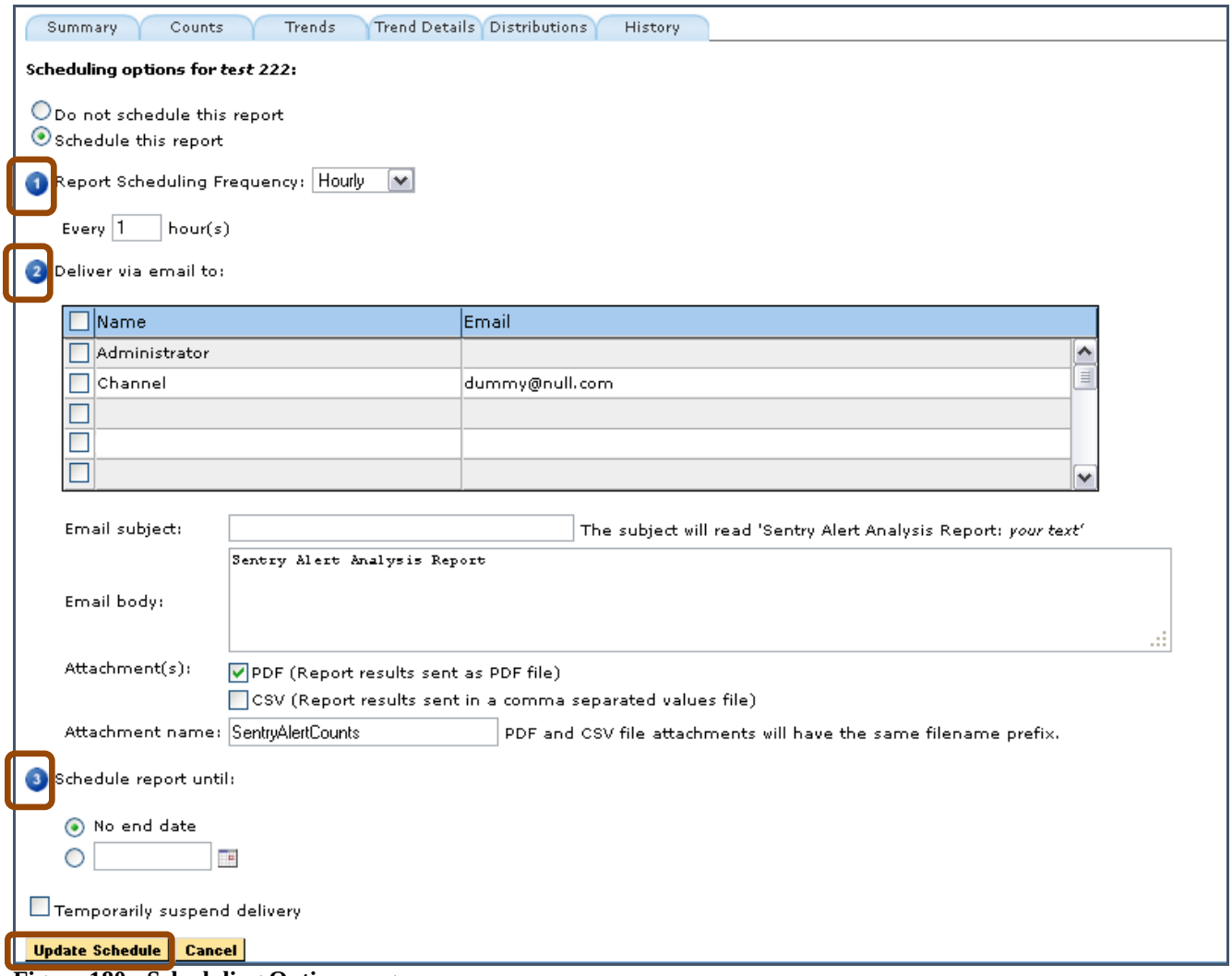


Figure 180: Scheduling Options page

5. **Section 3**: Schedule the delivery end times.
   You may set it to only email you one time, every time or to end on a particular date.

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

6. 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.

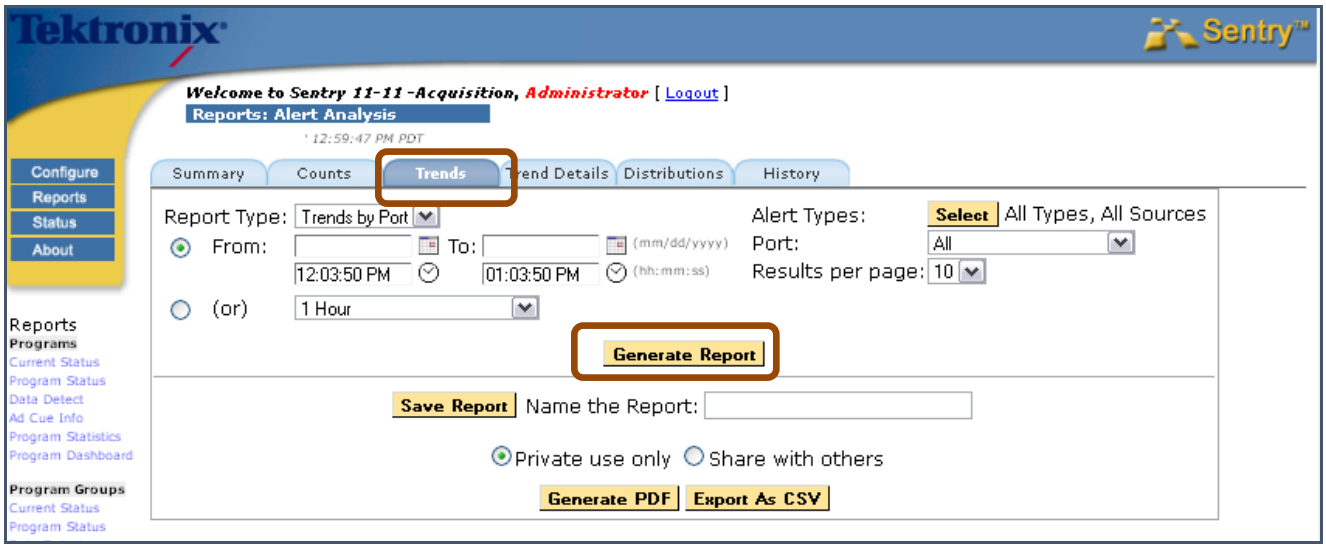


Figure 181: Trends tab options

Set a Trends report

1. Choose time frame for the report.
2. Select alert types you wish to view.
3. Select which port you will be watching.
4. Select your limit (top 10, 20 or 30).
5. 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**

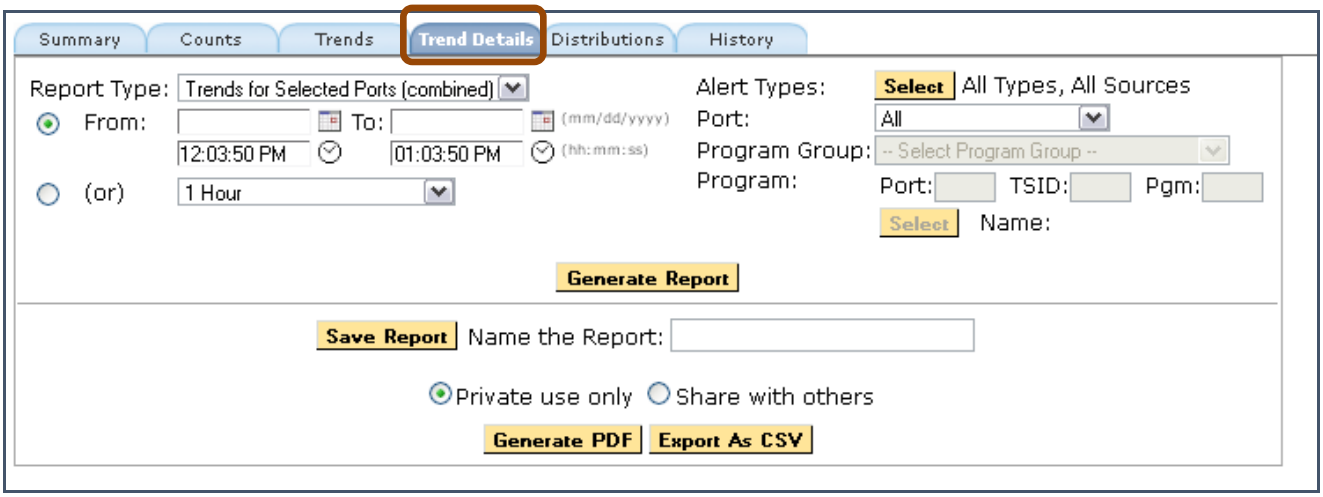


Figure 182: Trend Details options

2. Select **Trends for Selected Ports** (combined) from the drop-down menu.
3. Set the time period.
4. Select the **Alert Type.**
5. Select an individual port or **All.**
6. Select **Generate Report.**

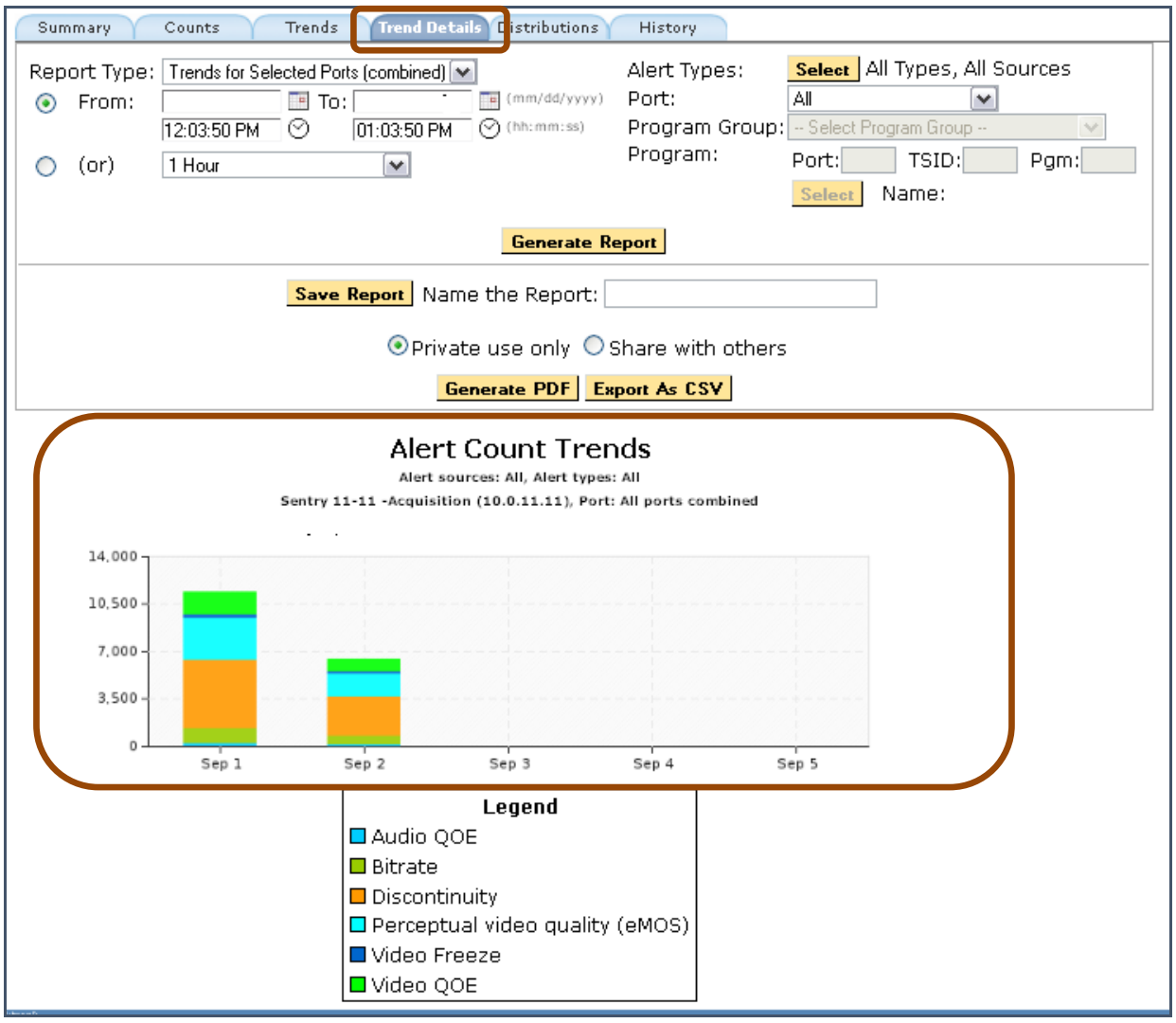


Figure 183: The resulting Trend Details graph

Distributions tab

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

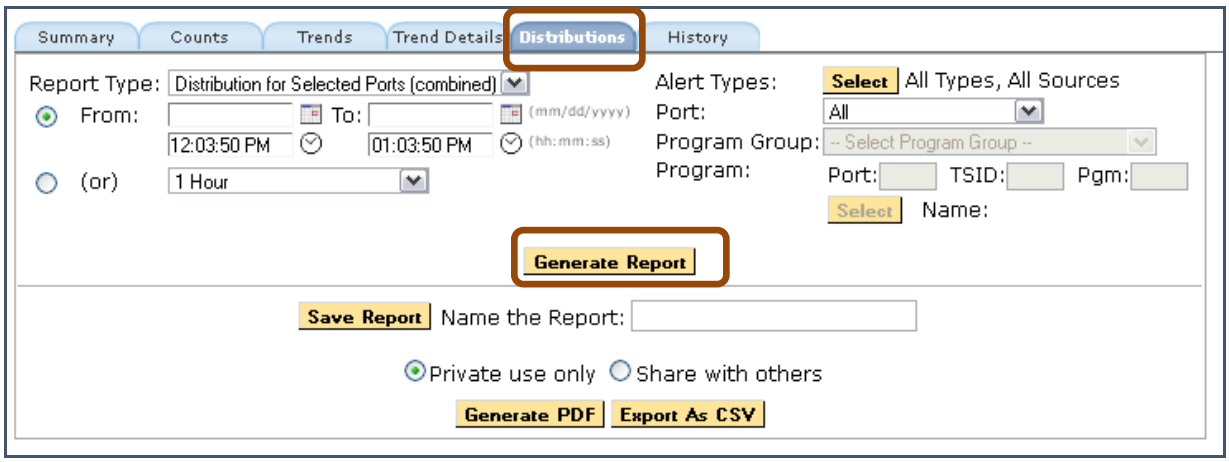


Figure 184: The Distributions tab

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. Select program **Group/Program.**
5. Select **Generate Report.**

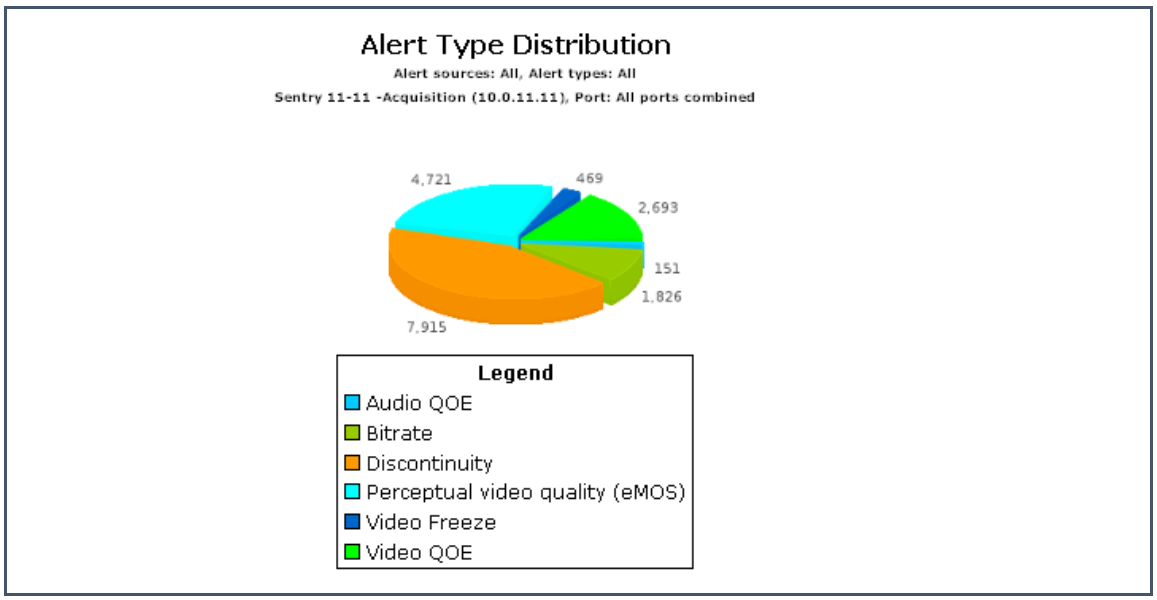


Figure 185: The resulting Distributions pie chart

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 what alerts and when they are receiving them.

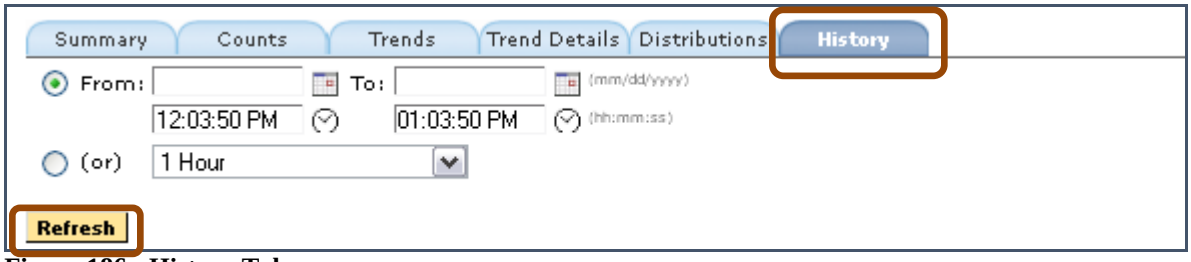


Figure 186: History Tab

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

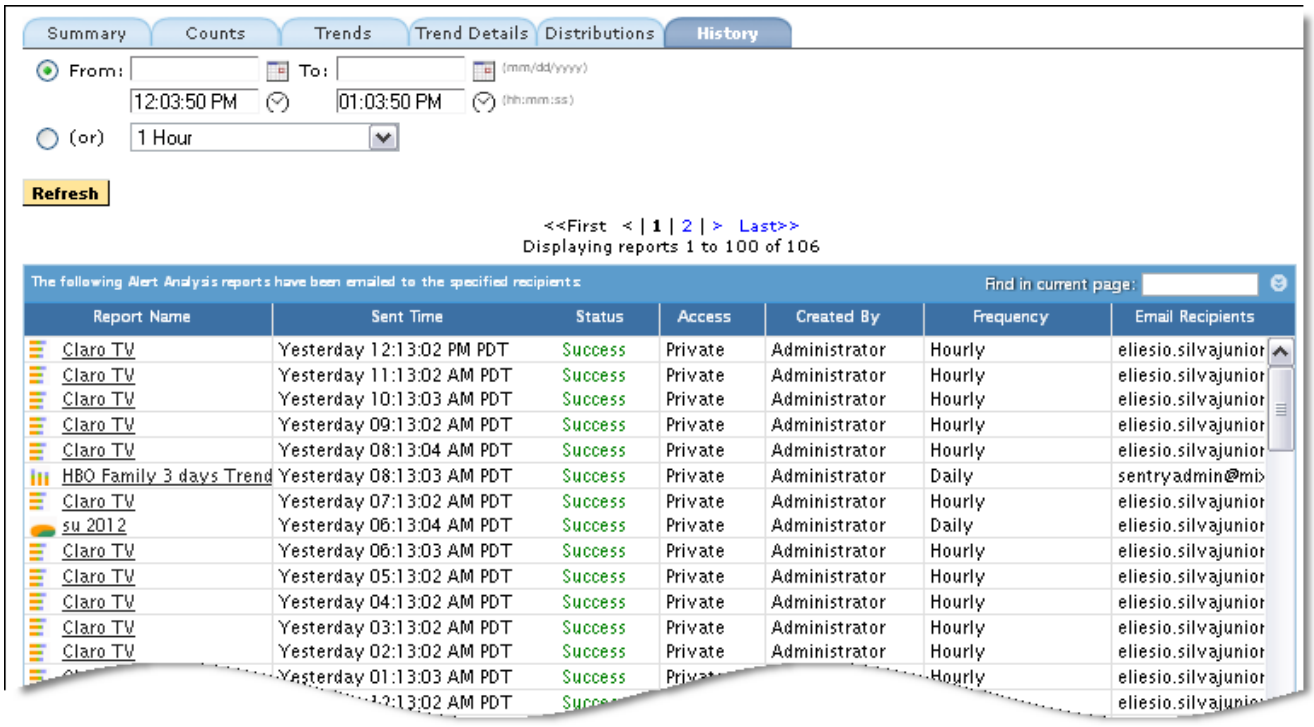


Figure 187: Alert Analysis reports results

Program Alert Definitions Report

The **Program Alert Definitions** (**Program Alert Defs**) report allows you to view alerts defined to every program and to quickly find programs with no alerts set.

Filters can be set by counts. For example, you could select to show all programs without any set alerts.

These reports can be scheduled for CSV delivery via email.

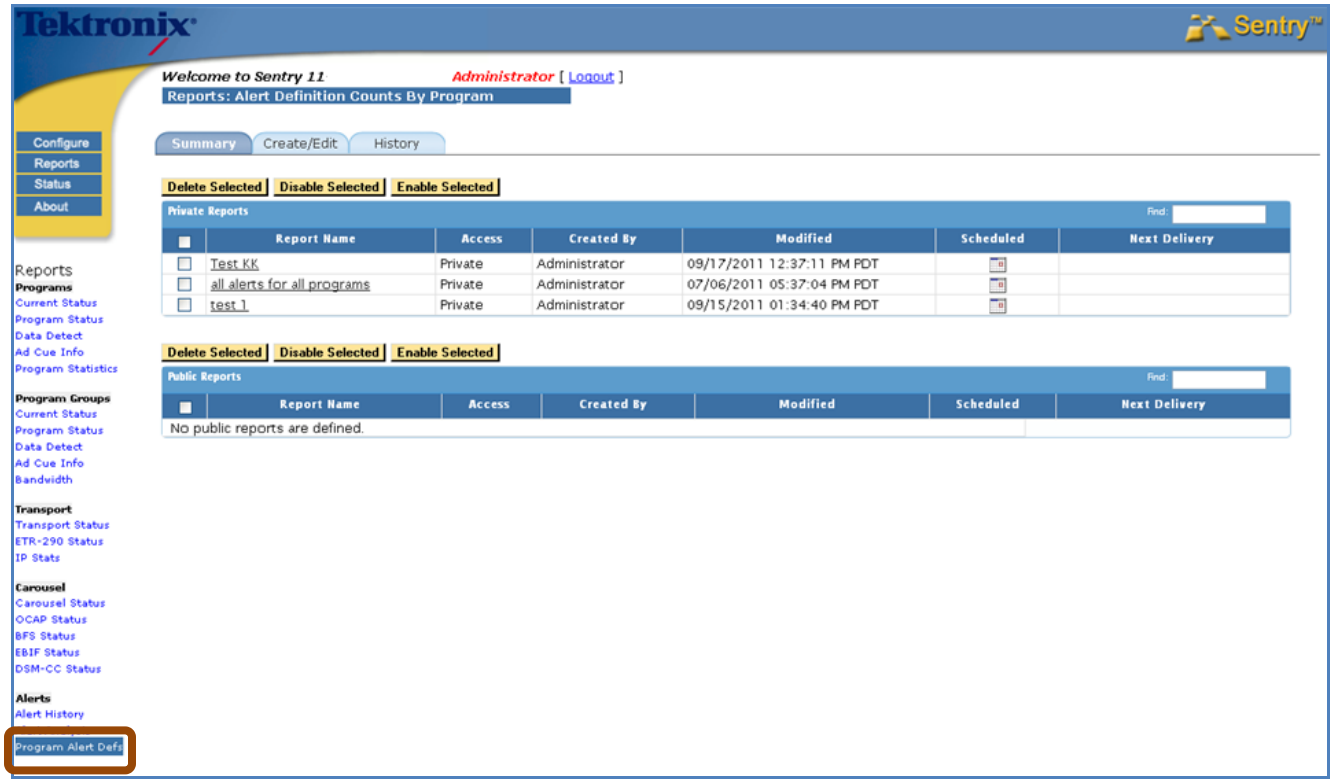


Figure 188: Alert Definition Count by Program Summary screen.

Create/Edit tab

How to Set Program Alert Definition Counts

1. Select **Program Alert Defs** from main menu
2. Select the **Create/Edit** tab

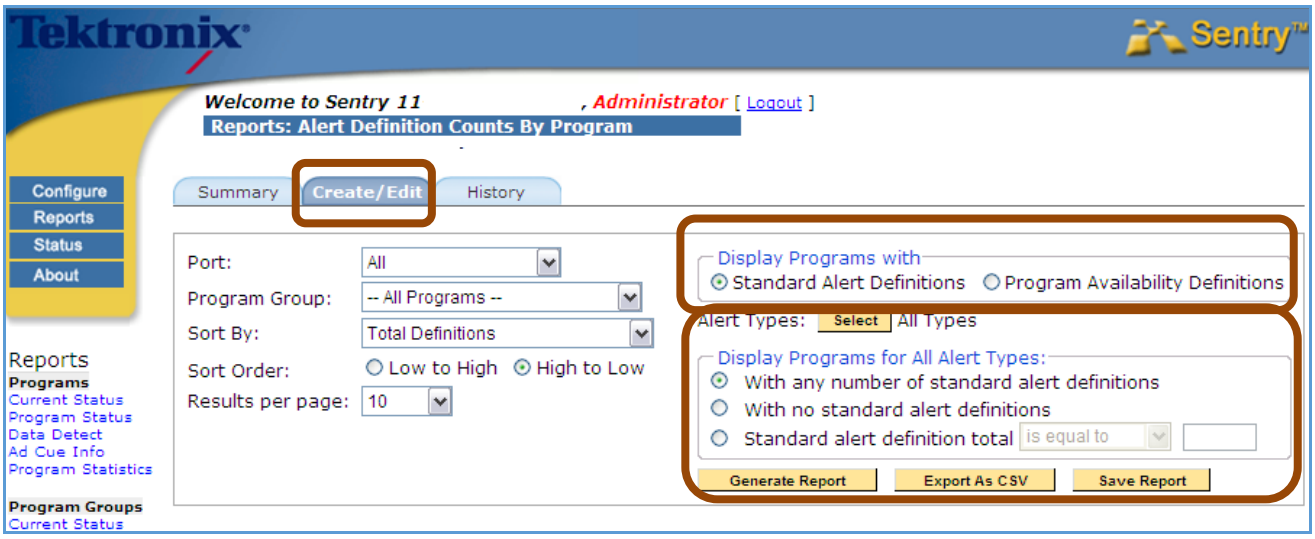


Figure 189: Create/Edit tab

3. **Example 1: To find programs with no set alerts**
   a. Accept the defaults in the **Display Programs with** box.
   b. In **Display Programs for All Alert Types**, change the default to **With no standard alert definitions**.
   c. Select **Generate Report.**

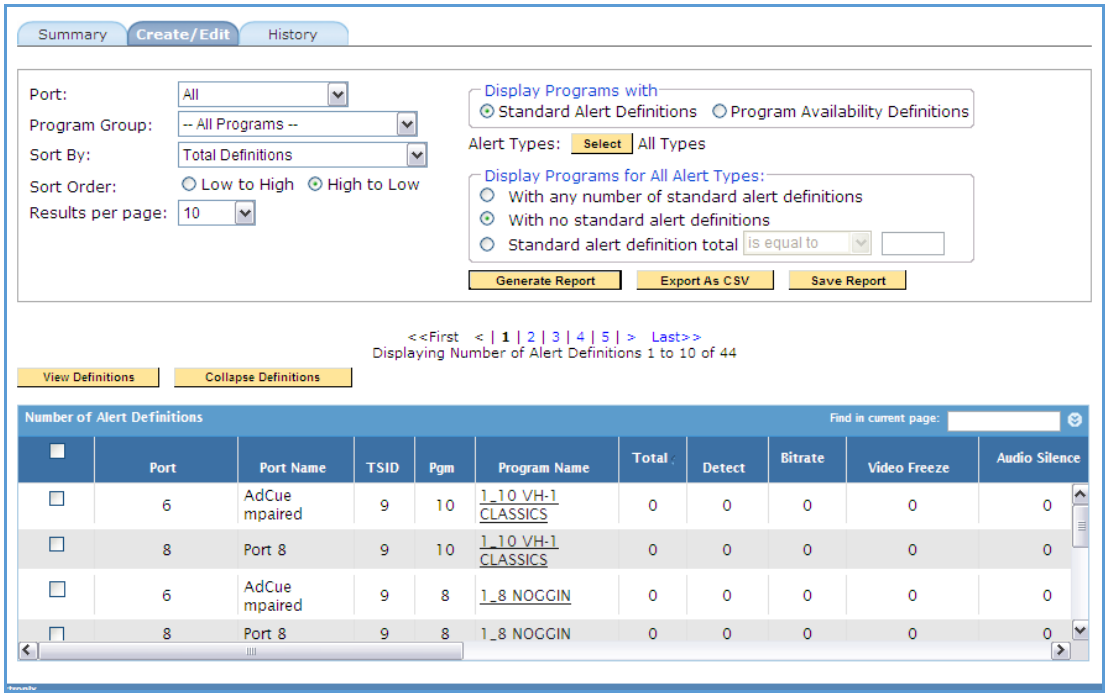


Figure 190: Finding programs with no set alerts

4. **Example 2:** Track program with duplicate alerts. Used to monitor if there are more alerts set than you thought.
   a. Accept all defaults.
   b. Select **Generate Report**.

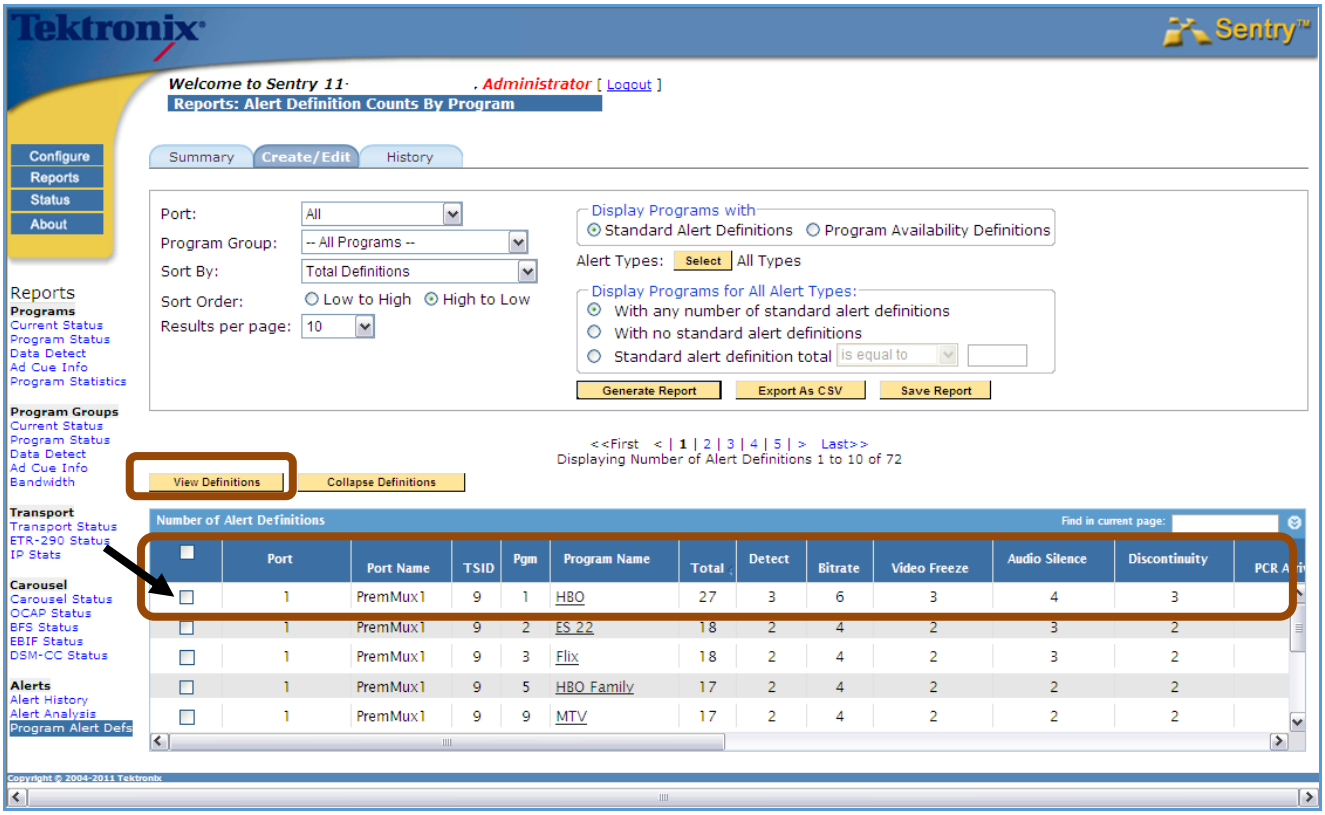


Figure 191: Tracking programs with multiple alerts

In this example, HBO has 27 total **Alert Definitions**.

   c. Check left box.
   d. Check **View Definitions**. This generates a detailed list of all the alerts, including where they are coming from.

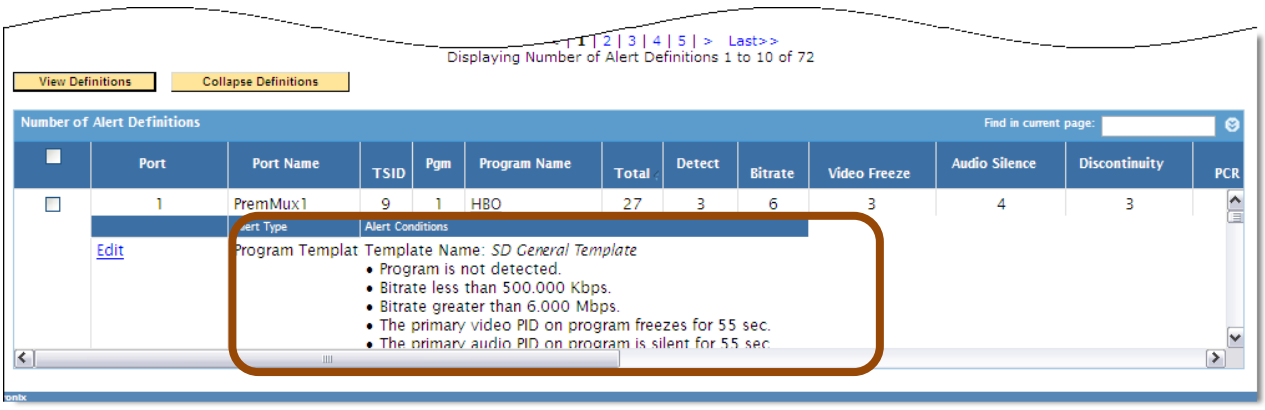


Figure 192: View Definitions

5. Select **Save Report** button and give the report a name**.**

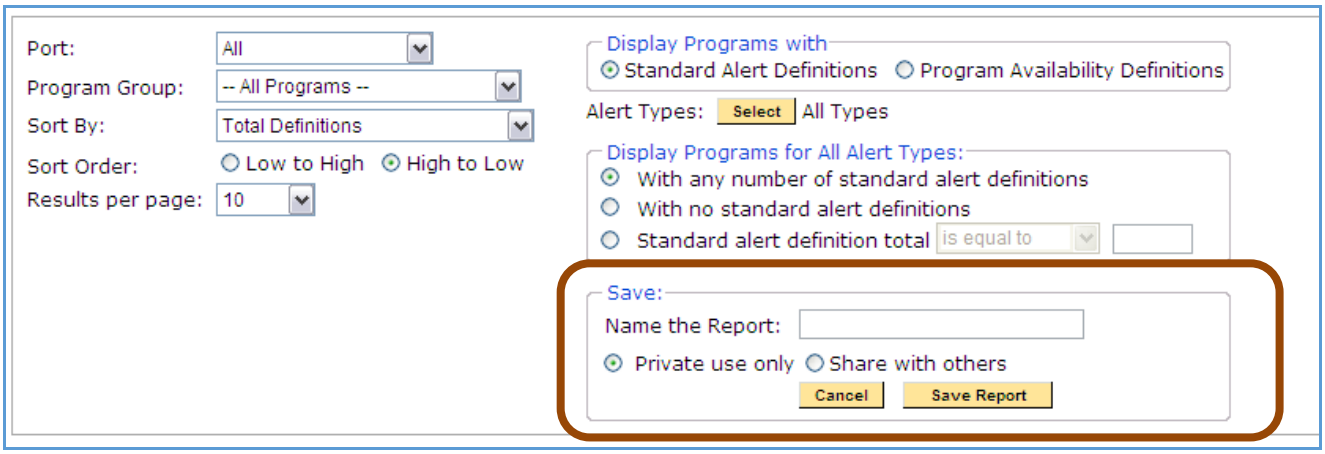


Figure 193: Saving the report

6. Select **Yes** on the confirmation pop up box.
7. Select **Schedule Report.**

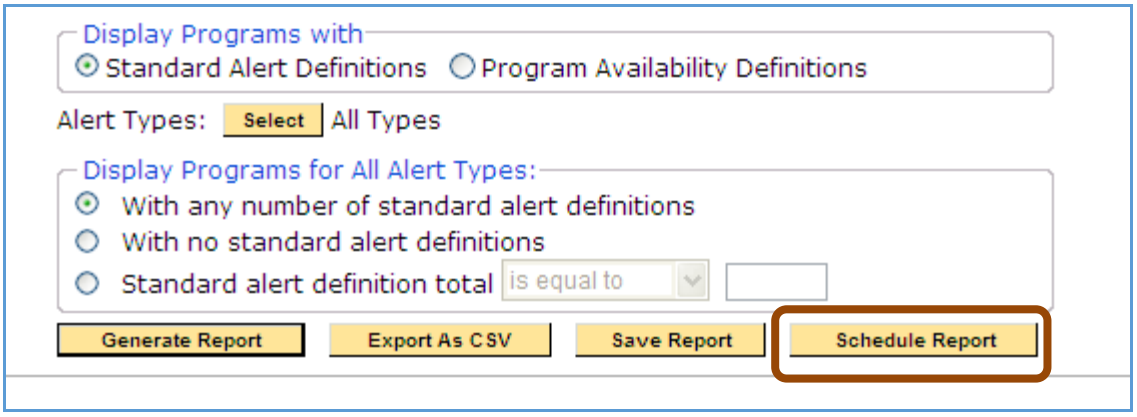


Figure 194: Schedule the Report

8. Complete scheduling steps as shown in **Scheduling Alerts**.

History tab

The **History** tab shows if any **Alert Definition Counts by Program** reports have been emailed to specified recipients.

Configure

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

NOTE: ***To configure and set parameters, you must log in with Administrator privileges***.

The following are configurable items:

- **Alerts**
  Create and delete PID, program, table, PMT, DSM-CC, IP Stats, BFS and OCAP alerts.
- **Program groups**
  Customize programs as a group
- **Program Mappings**
  Add, modify and delete program mappings.
- **Port Names**
  Provide names for individual ports
- **BFS Settings**
  Enter the source ID for the BFSdir file.
- **Stream Capture**
  Select program for stream captures
- **Dashboard Graphs**
  Configure public or private program dashboard graphs
- **MPEG Input Settings**
  Select Unicast or Multicast for MPEG over IP and configure settings.
- **System Preferences**
  Select whether or not to include ad cue PIDs in the Program Status

  Select whether or not to include the PVQ score in the Video QoE results
- **System Settings**
  Configure Sentry hardware: Ethernet address, NTP servers, email gateway and DNC.
- **Import/Export Settings**
  Allows you to backup the configuration of the unit for safe keeping or mirror a configuration to another unit
- **Users**
  Add, modify and delete users in the system
- **System Upgrade**
  Remotely upgrade Sentry to the latest software version
- **Power Off**
  Power down Sentry

Configure Alerts

Alerts are a key component of Sentry and are used to identify particular transport stream conditions. All 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 Log** 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** (refer to Configure System Settings) when the alert is generated.

How Sentry Handles Alerts

Alerts that you define in the system are triggered (i.e., Sentry generates an alert) and then reset when the condition for the alert no longer exists.

For example, a PID bitrate greater than a set limit will trigger when the limit is exceeded and then will only trigger again when the bitrate falls below the limit (reset) and at a later time exceeds the limit again. Some types of alerts need clarification.

- **Detect/Present**
  When the alert is first set, Sentry alerts if the data source exists. Subsequently Sentry alerts if the data source is added.
- **Detect/Not Present**
  When the alert is first set, Sentry alerts if the data source does not exist. Subsequently Sentry alerts if the data source did exist and gets removed.
- **Bitrate**
  Note that low bandwidth can result in no data during a 5-sec. interval, causing the bitrate to be set to zero. Therefore an alert trigger condition of bitrate greater than zero will be reset and will generate the alert once the bitrate is again greater than zero. This can result in multiple alerts for bitrate greater than zero due solely to low bandwidth conditions.
- **Cycle Time/Greater Than**
  Sentry alerts when the maximum cycle time in the last 5 sec. exceeds the set limit. The alert is reset when the maximum cycle time falls below the set limit.
- **Cycle Time/Equal To**
  Sentry alerts when the average cycle time equals the set limit.
- **Cycle Time/Less Than**
  Sentry alerts when the minimum cycle time in the last 5 sec. falls below the set limit. The alert is reset when the minimum cycle time exceeds the set limit.
- **The Cycle Time Greater Than/ Equal To/ Less Than**
  Tests are independent so it is possible, for example, to have multiple **Greater Than** alerts without a corresponding number of **Less Than** alerts.
- **File/Added**
  Sentry alerts if the file did not exist and is added.
- **File/Removed**
  Sentry alerts if the file did exist and gets removed.

Create an Alert

Alerts can be created one of two ways:

- By selecting **Configure** and then Alerts from the main menu
- Or by clicking on the alert icon to the right or left of the stream you wish to create an alert for

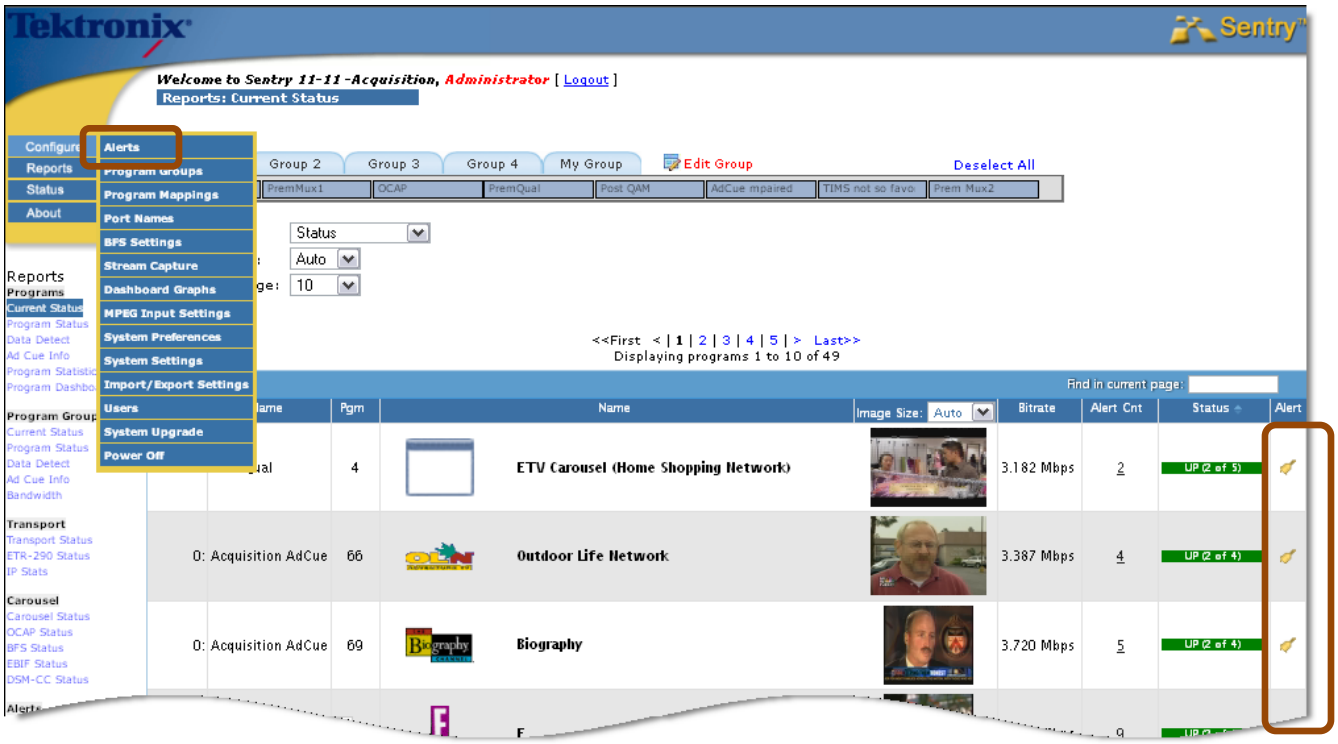


Figure 195: Create Alerts via the main menu or by selecting the Alert Bell icon on the correct stream

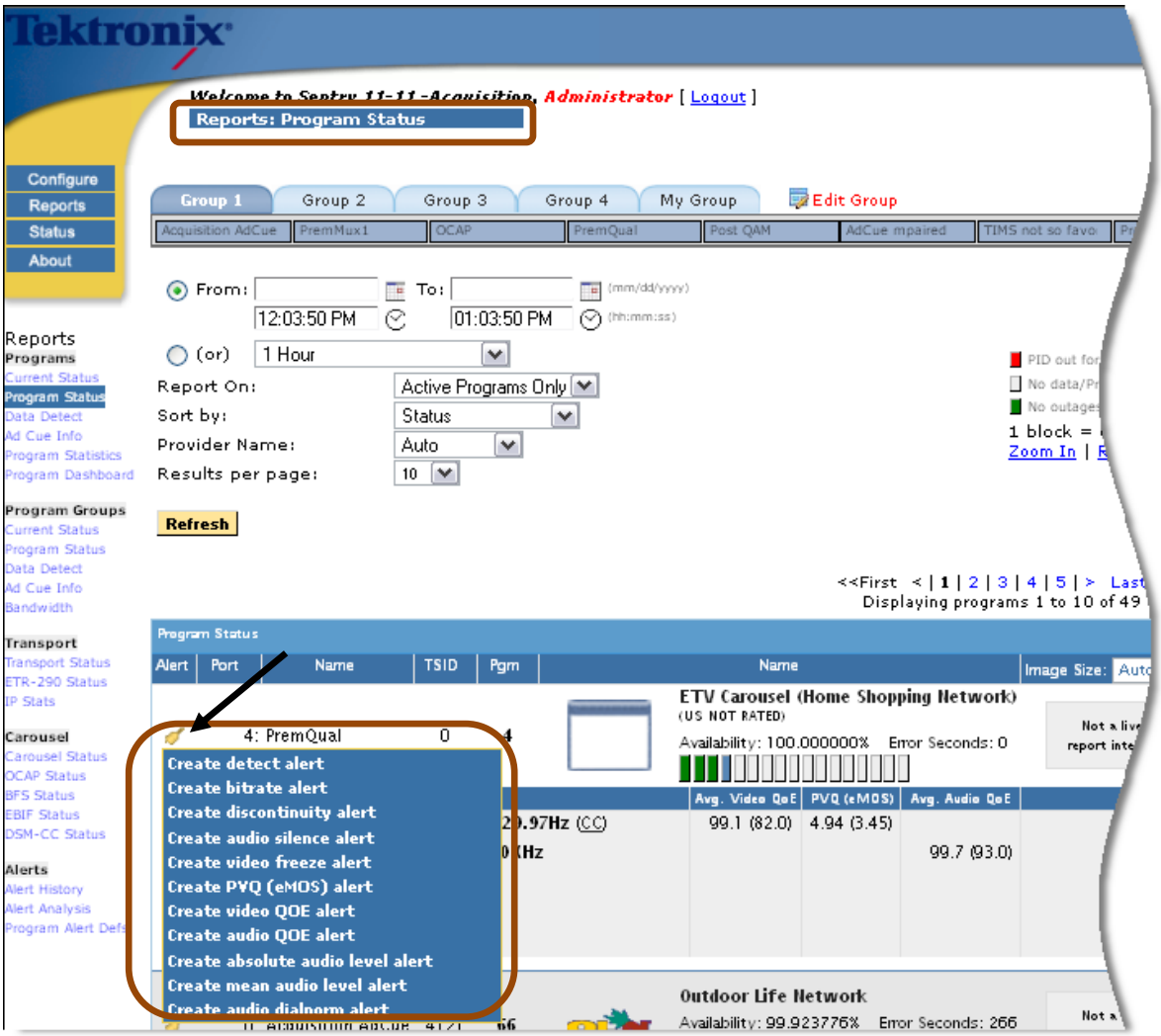


Figure 196: Creating Program Alerts via the Program Status Report

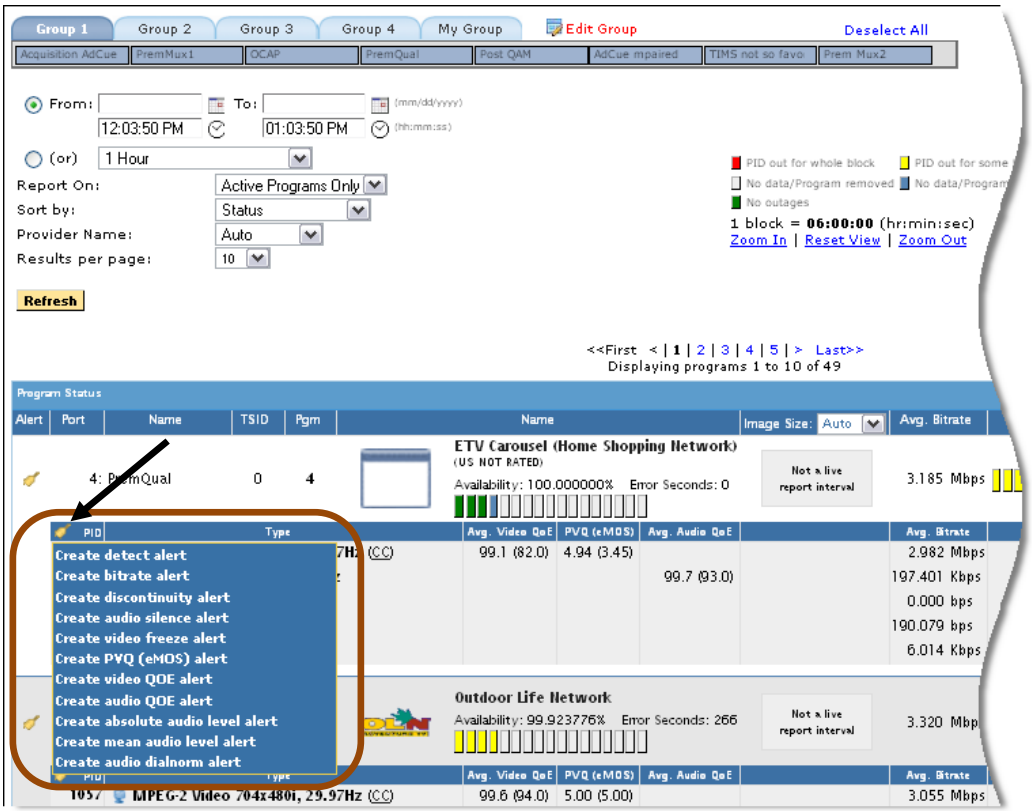


Figure 197: Creating PID Alerts via the Program Status Report

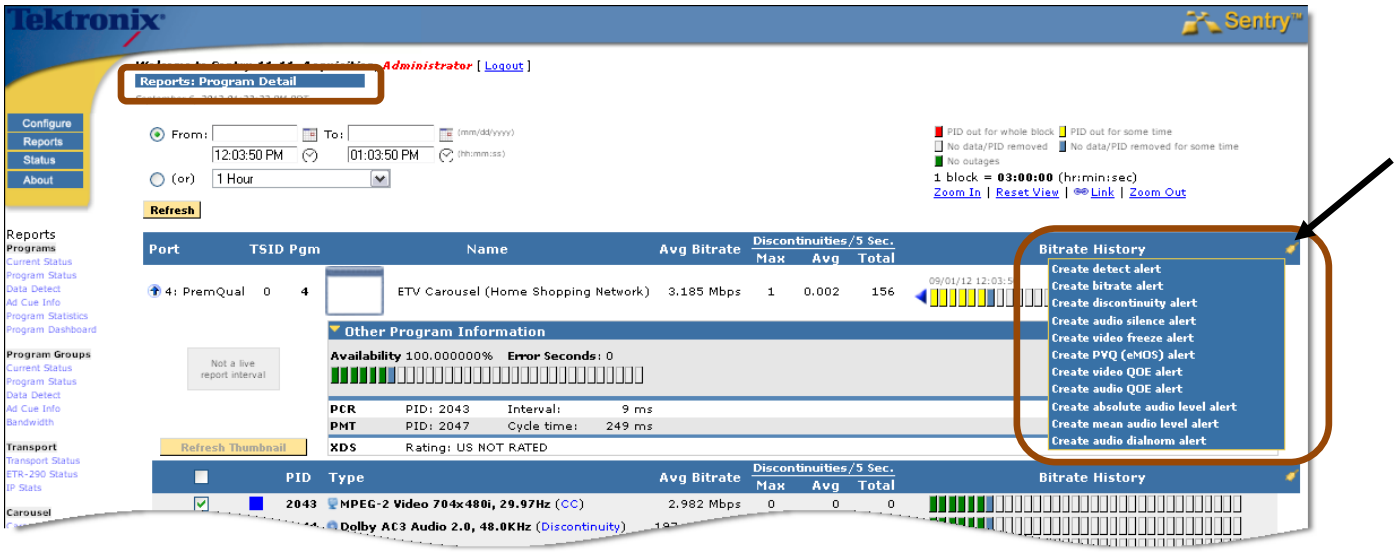


Figure 198: Creating Program Alerts via the Program Detail Report

NOTE: ***PCR Interval and PCR Jitter alerts only appear in the Program alerts menu if the Sentry is an ASI model.***

Create Alerts Step by Step

Access the alert you want from the Alerts summary page.

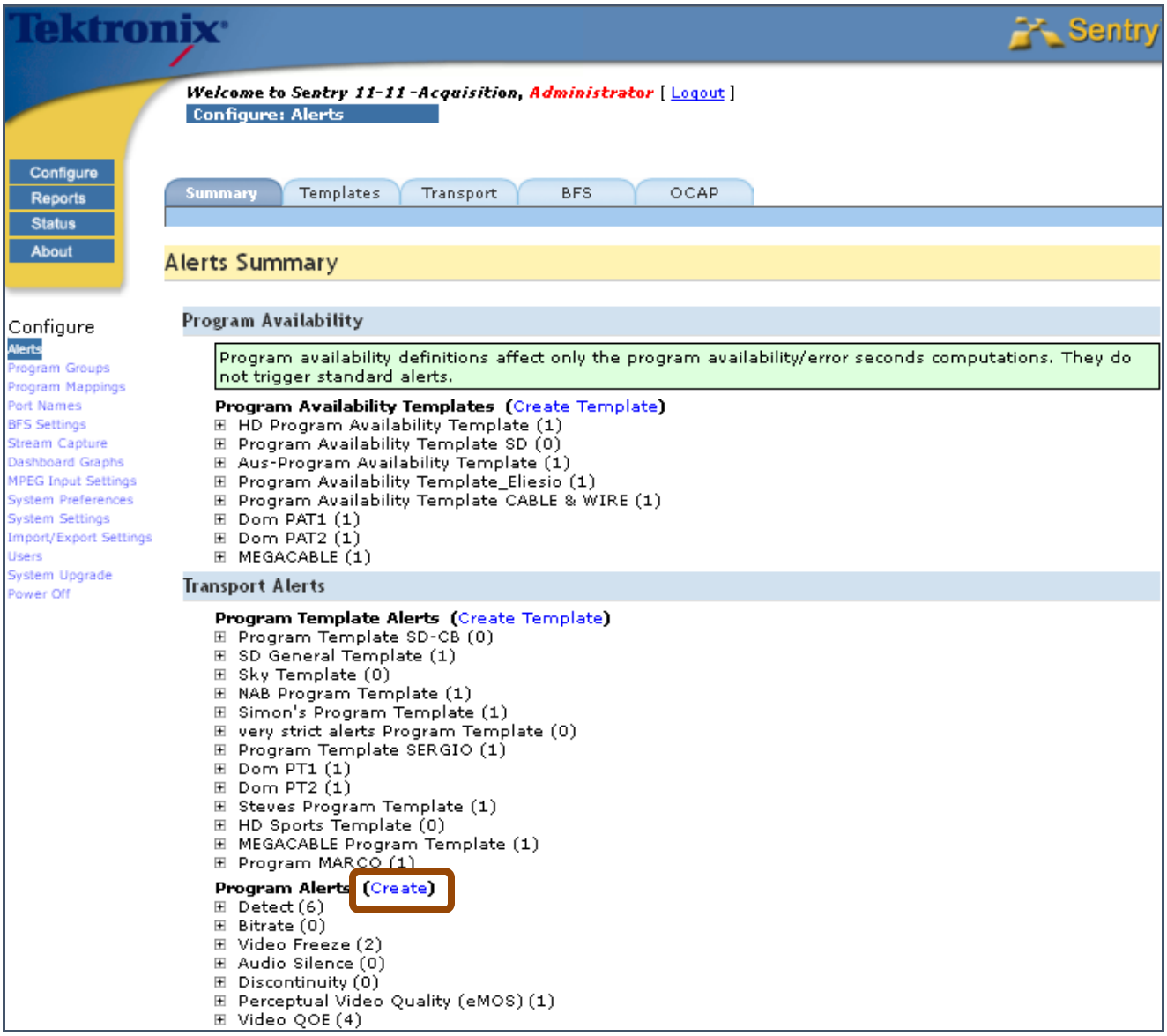


Figure 199: Select Create

Once **Create** or a link is selected, the corresponding **Creating Alerts** page opens. Each **Creating Alerts** page is divided into three main sections, identified by 1, 2, and 3

NOTE: ***Sections ❶ and ❷ differ with the type of alert. Section ❸ is the same for all types of alerts.***

Section ❶ allows you to select the type of alert and set the condition for its generation.

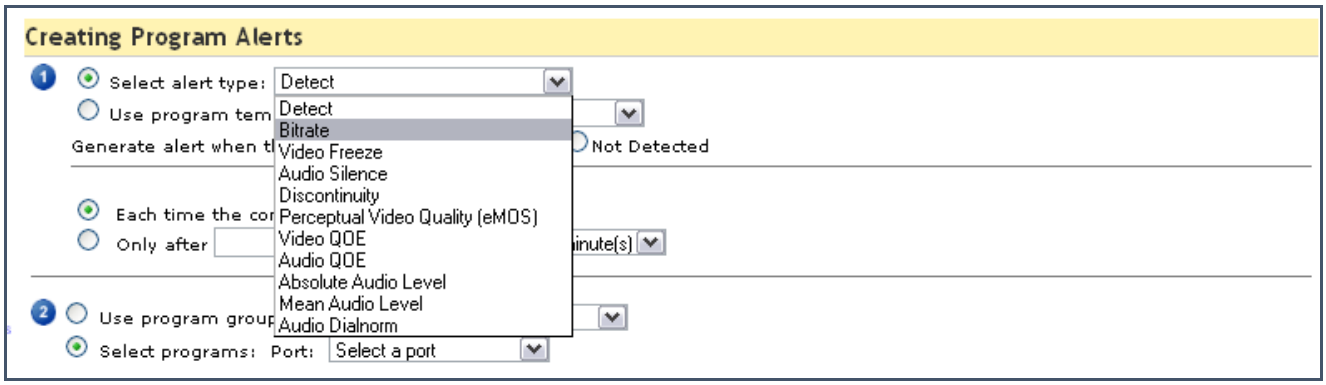


Figure 200: Selecting the Alert Type

Section ❷ allows you to identify what you want to alert on. **Ports**, programs, **PIDs**, etc. can be added and removed by checking and un-checking the boxes to the left of the list. Ports and PIDs can also be sorted by clicking on the column headers.

1. Select a port from the drop down menu to populate the port box below.

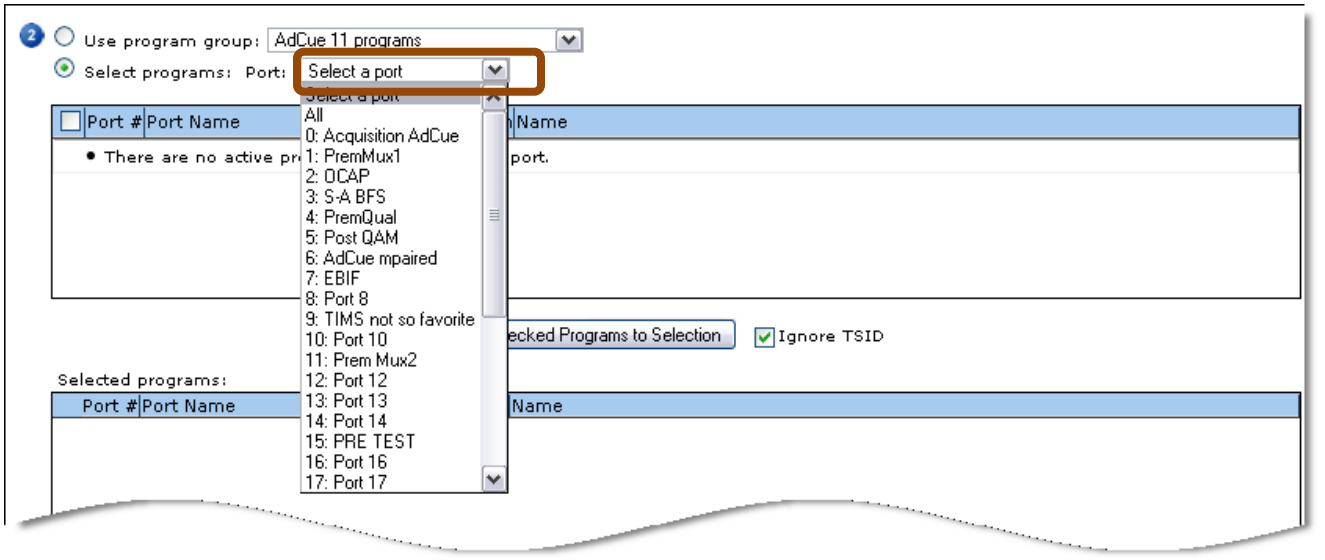


Figure 201: Selecting the port

2. Select the desired **Port** names from the list and select **Add Checked Boxes to Selection** button. The selections will appear in the window below.

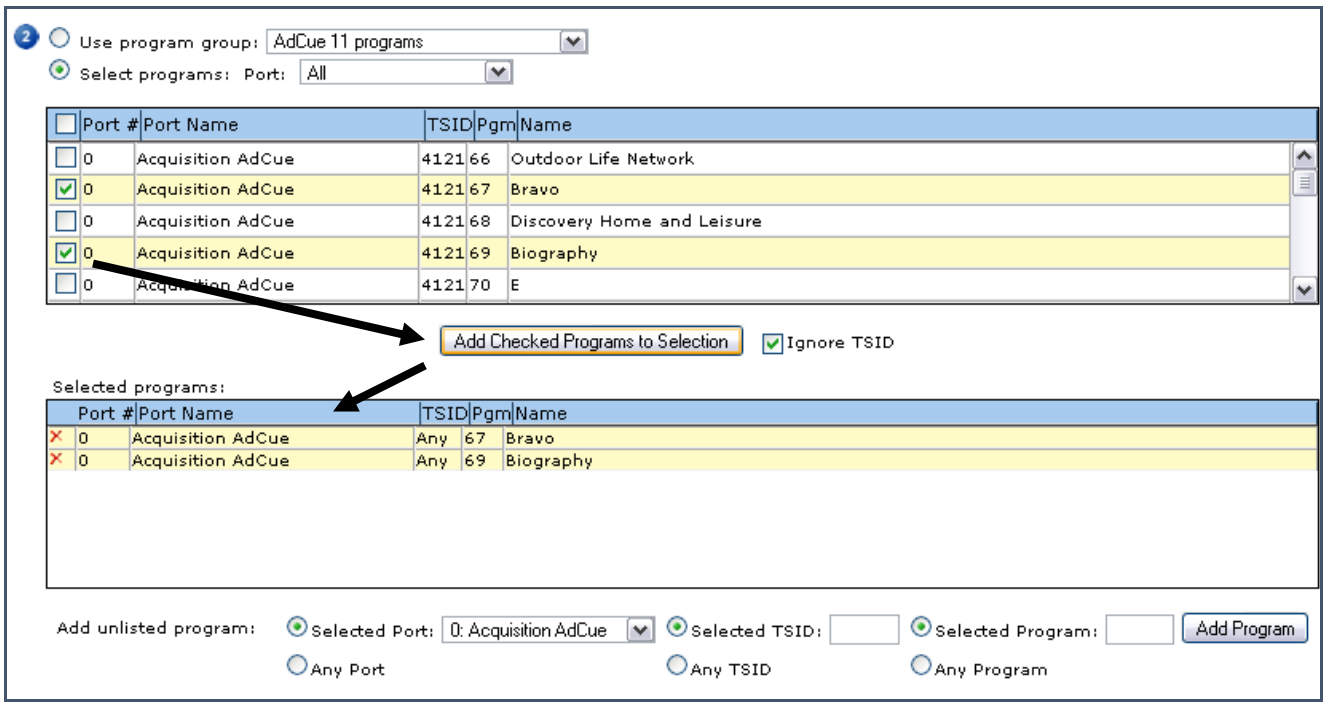


Figure 202: Selecting PIDs to Alert On

Section 3 allows you to specify who will be notified of the alert. The alert will be logged to the database automatically. Select if you want to be notified via email or SNMP trap.

You can also select how many emails are sent in a given time frame and whom they are sent to.

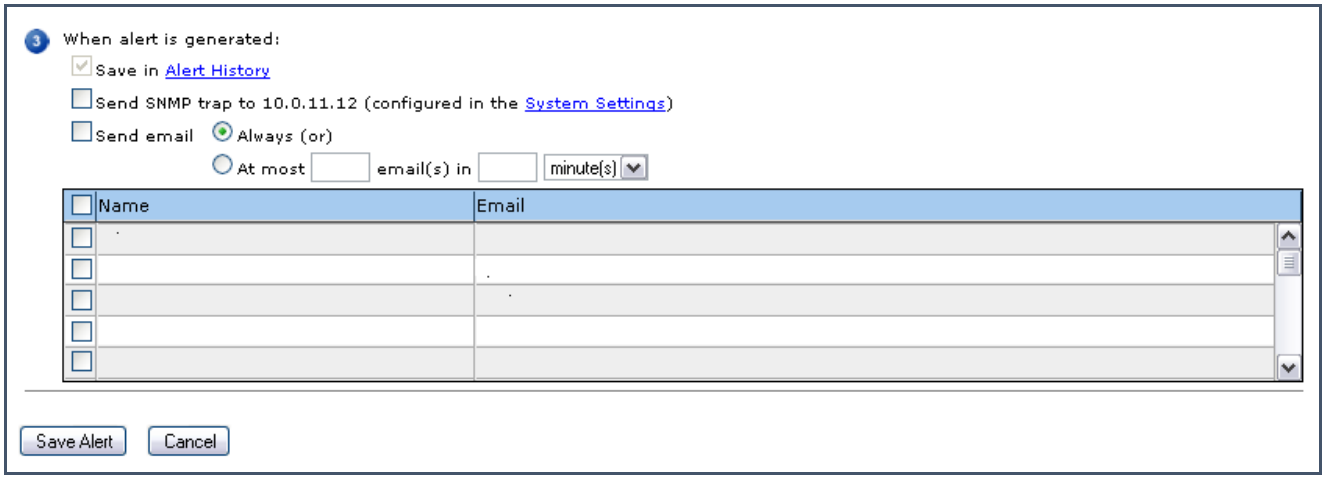


Figure 203: The Alert Notification section

Select **Save Alert** to save and activate your new alert. The system will respond with an **Alert Saved** message whose content is specific to the alert.

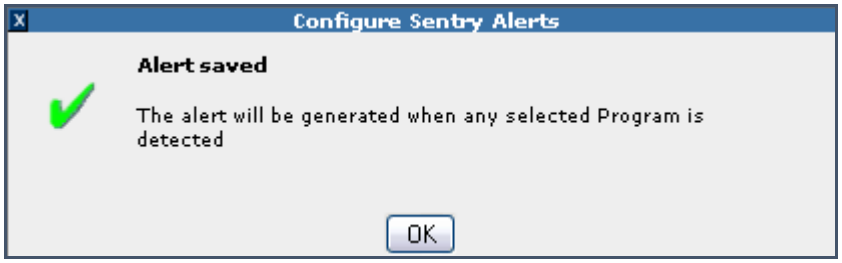


Figure 204: PID Alert Saved Message

The alert will now show up on the **Alert Summary** page

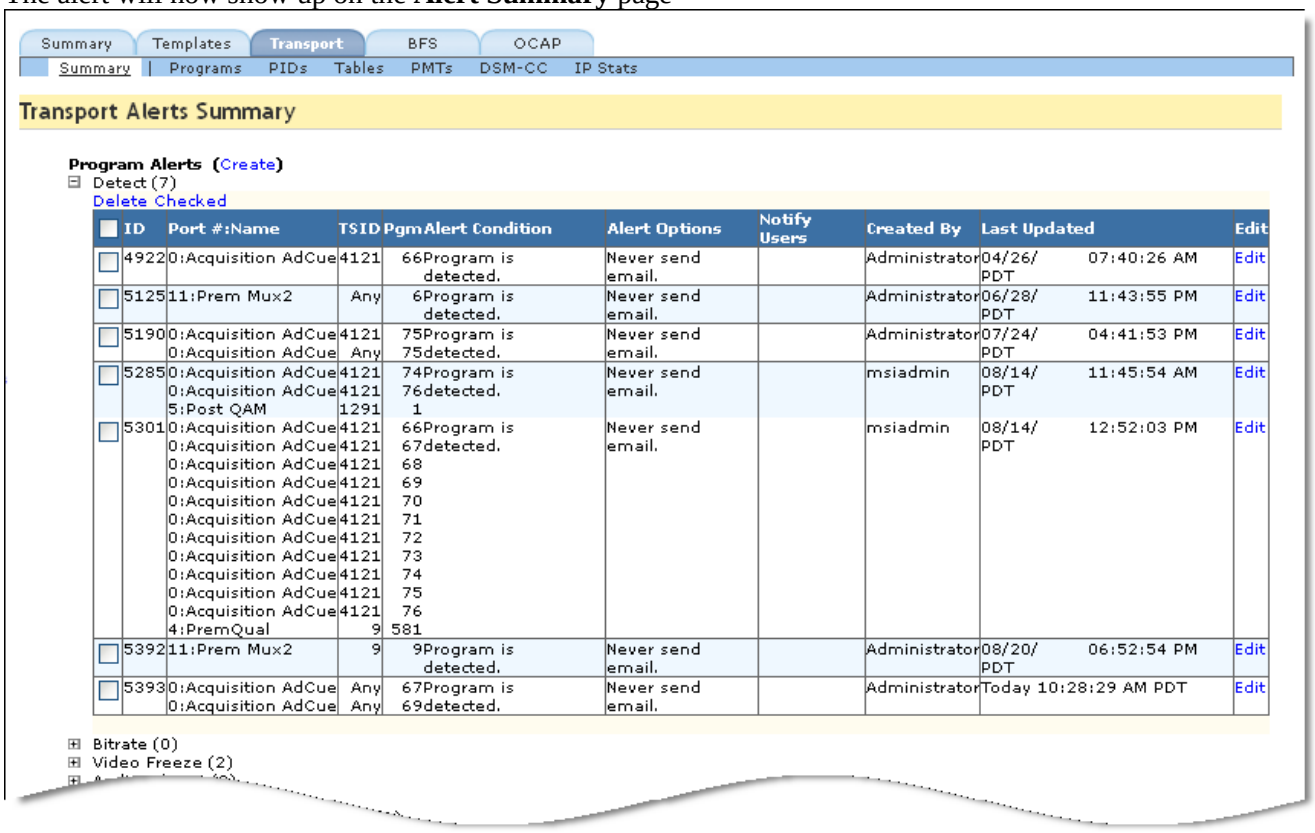


Figure 205: Alert Summary page showing created Alert

View Created Alerts

The alerts that have been created can be viewed from the **Alerts Summary** page by expanding alert types that have a number greater than zero in parentheses.

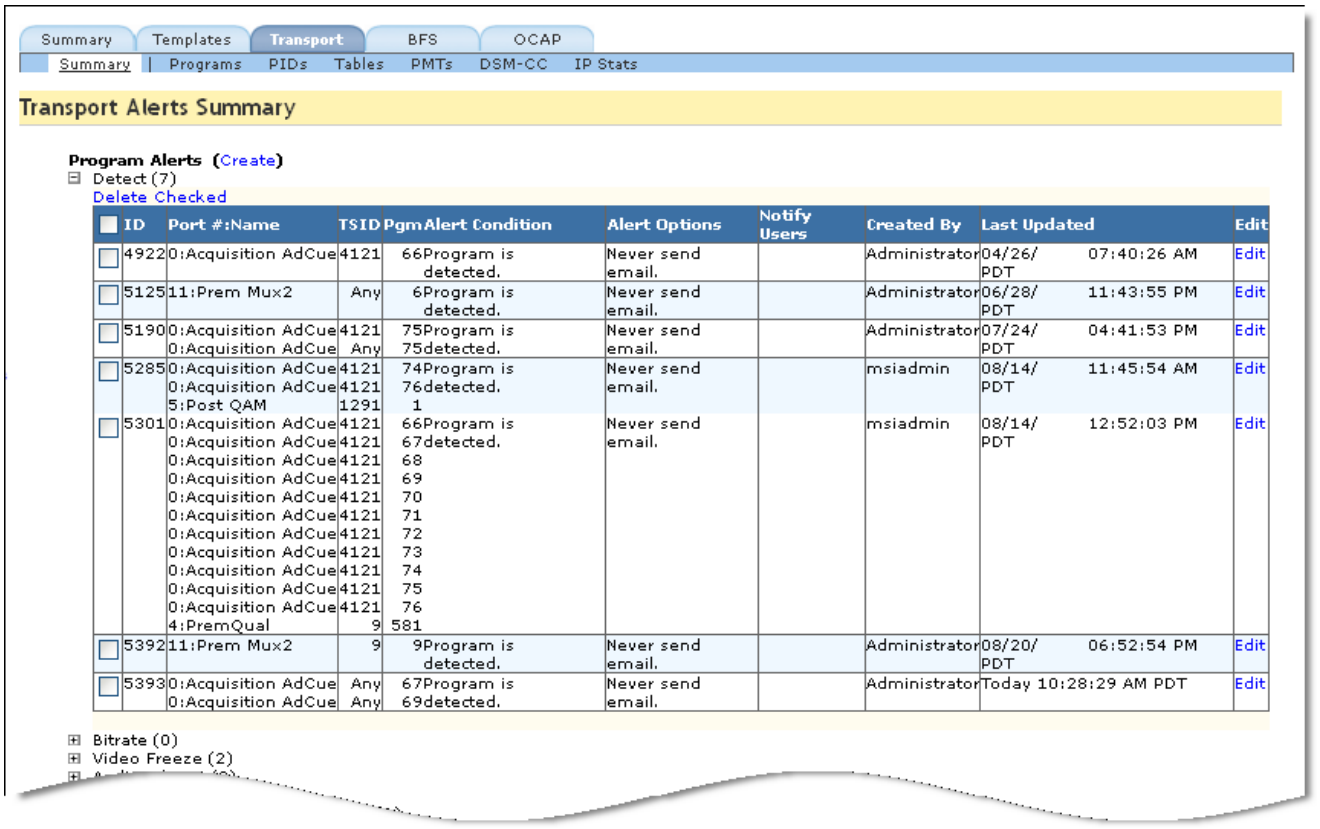


Figure 206: Alerts Summary Page showing Created Alerts

Delete Alert

1. To delete an alert, expand the group of alerts you wish to delete.
2. Check the box located to the left of the alert you wish to delete or check the box in the upper left to delete all alerts in the group.
3. Click **Delete Checked** above the alerts listed.

Modify an Alert

1. To modify an alert, click **Edit** adjacent to the alert you wish to edit.
2. The corresponding **Creating Alerts** page will be displayed populated with the current alert criteria, which can then be edited and saved.

Access Alerts Summary

To open up a list of all available alerts, select **Configure** and **Alerts** from the main menu.

This will open the **Alerts Summary** page.

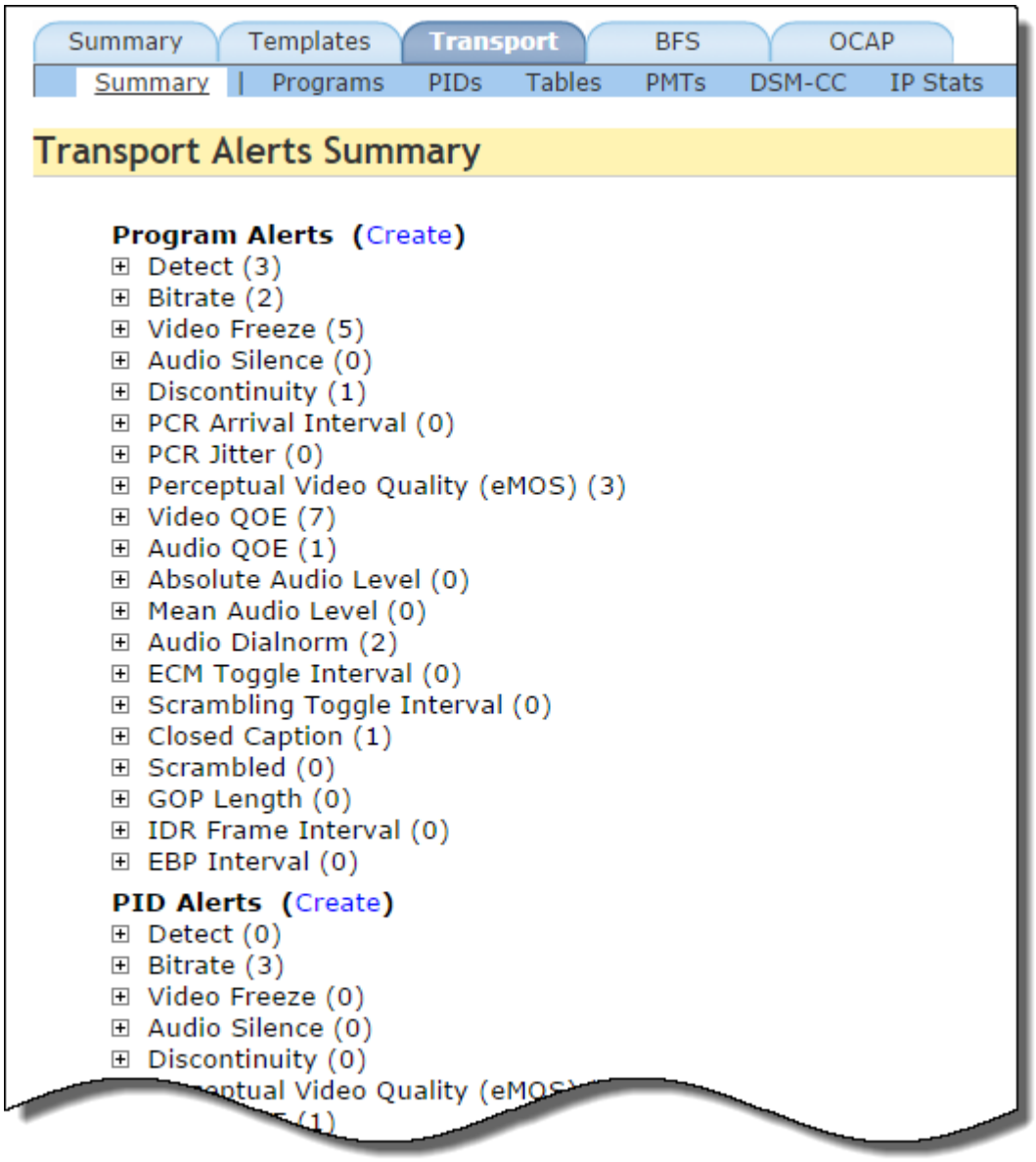


Figure 207: Alerts Summary page

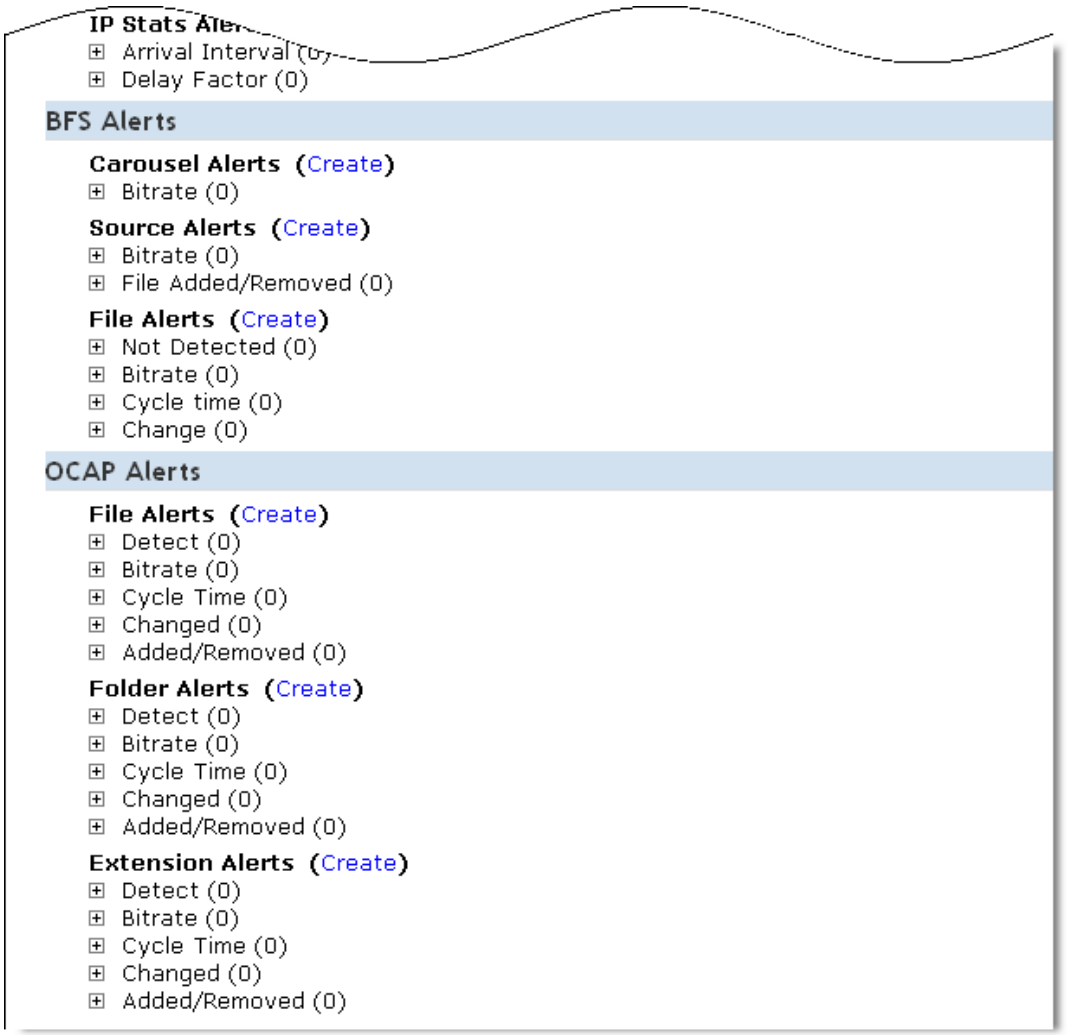


Figure 208: Alerts Summary page bottom

Scrambled Alerts

You can set **Program**-based and **PID**-based **Scrambled Alerts** from a **Program Availability Template** or the **Program Template Alert**. The alert can be set to trigger upon the detection of scrambled or unscrambled content, or when the CA descriptor value conflicts with actual stream content.

To access, select **Create Template**.

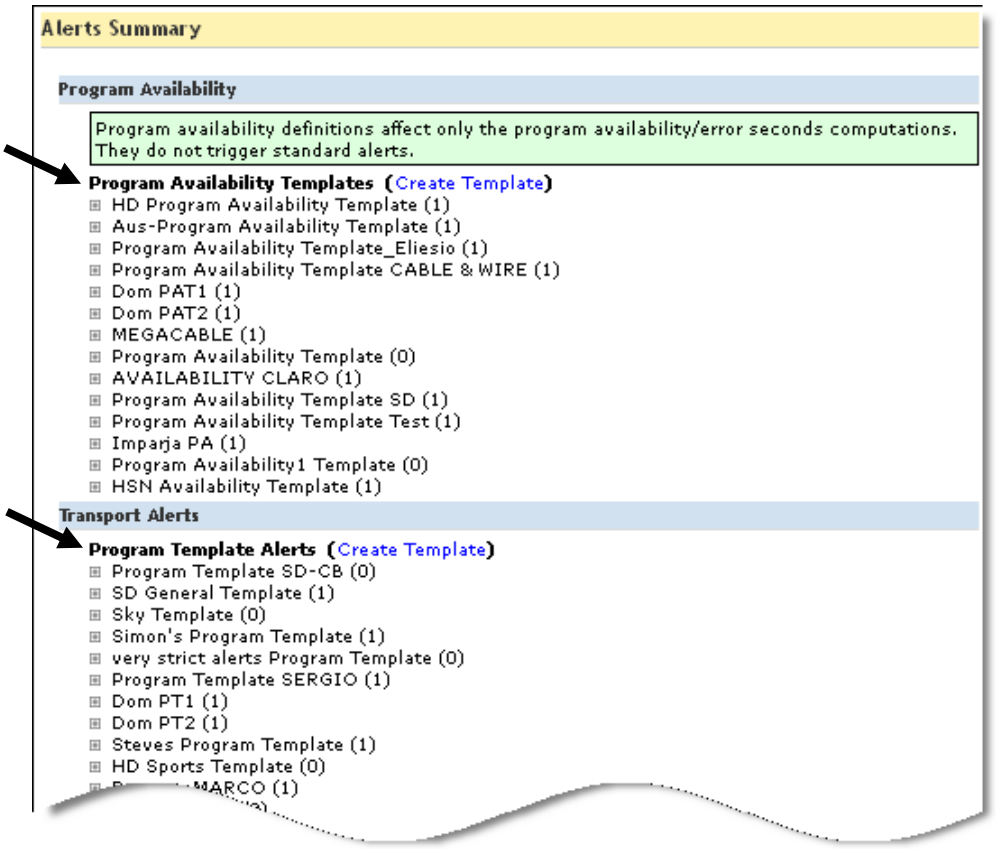


Figure 209: Select the Program Availability Template

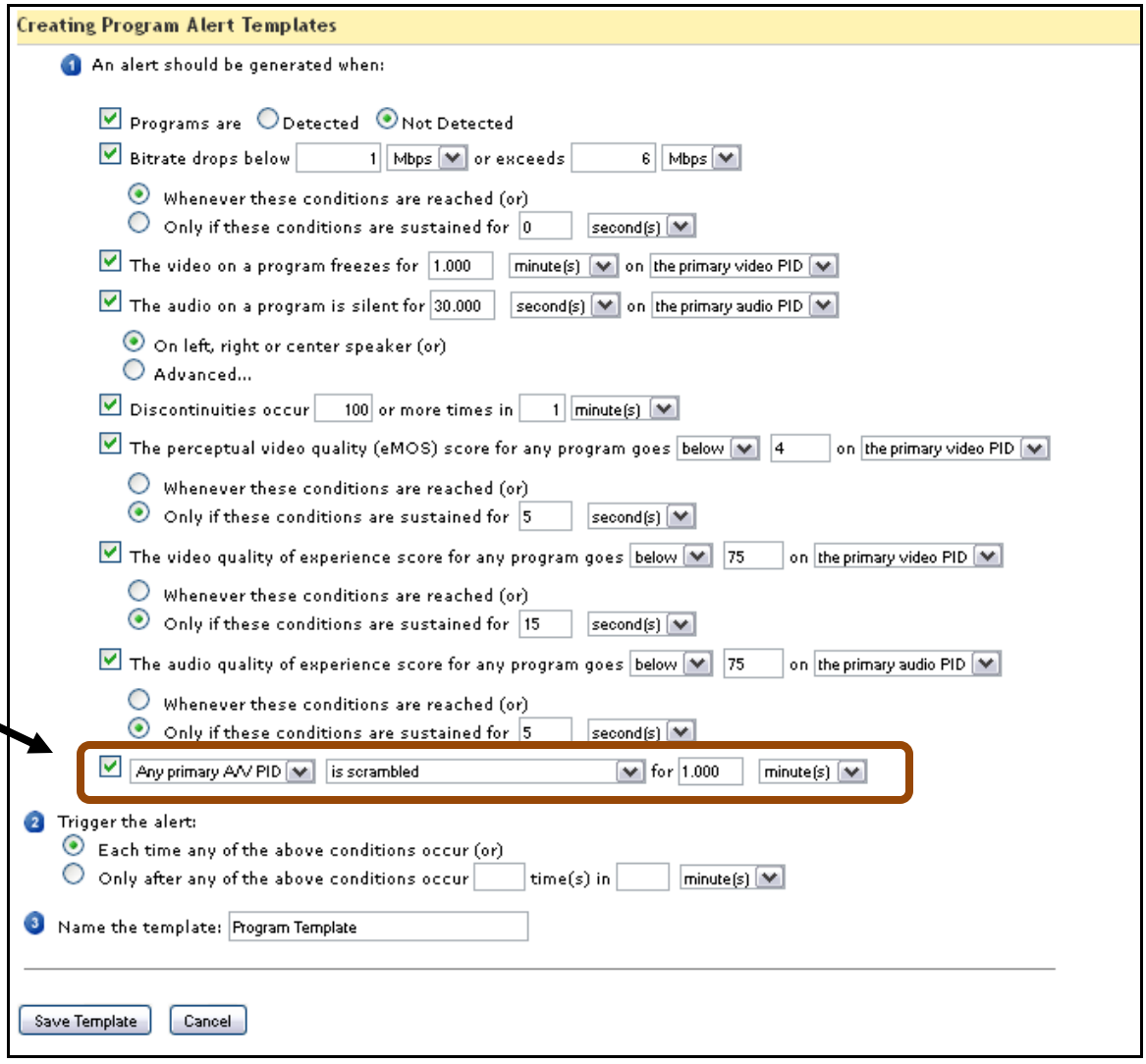


Figure 210: Selecting Scrambled Alerts

Transport tab

Selecting the **Transport** tab opens the **Transport Alerts Summary**.

Figure 211: Transport Alerts 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.

- **PCR Arrival Interval**
  Generates the alert when the arrival interval between PCRs is greater than, equal to, or less than a specified number of milliseconds for any of the selected programs. The number of milliseconds can be negative to represent "early" arrivals.

- **PCR Jitter**
  Generates the alert when the PCR jitter is greater than, equal to, or less than a specified number of nanoseconds (converted by Sentry to 27Mhz units) for any 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.

- **ECM Toggle Interval**
  Generates the alert when the ECM toggle interval is greater than or less than *x* number of seconds.

- **Scrambling Toggle Interval**
  Generates the alert when the scrambling toggle interval is greater than or less than *x* number of seconds.

- **GOP length**
  Generate an alert when the GOP length for any program is greater or less than X on the primary video or any video PID

- **IDR Frame Interval**
  Generates an alert when the IDR frame interval is either greater than or less than x number of seconds on either the primary video PID or any video PID.

- **EBP Interval**
  Generate an alert when the EBP interval for any program is greater or less than X seconds on the primary video PID or any video PID.

- **PTS Alignment of IDR/EBP Frames**
  The Presentation Timestamp (PTS) alignment of IDR/EBP frames varies by more than X milliseconds. This alert can only be defined against static program groups that are used to define the MBR (Multiple Bitrate) streamset for the alert.

- **PID Added/Removed from PMT**
  Generates an alert when a PID of a selected type (any PID, any A/V PID, any primary A/V PID, or any data/splice PID) is added or removed from the program's PMT.

- **PMT PID Type Change**
  Generates an alert when any selected **PID Type Change** (**PID Type**, **PID Type Family** or Primary PID designation) for a selected PID type (any PID, any A/V PID, any primary A/V PID, or any data/splice PID) occurs in the program's PMT. A **PID Type Family** is defined as either **Video**, **Audio**, **DSM-CC**, **Text**, **Splice**, **Scrambled or Other**.

- **PMT Contents**
  Generates an alert when the program's PMT does not meet the specified number of video PIDs, audio PIDs, DSM-CC PIDs, text PIDs, splice PIDs, scrambled PIDs, and/or other PIDs.

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**
  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.

Sample Transport Alerts

Create Audio Level Alerts

1. From the main menu, select **Configure** and then **Alerts**.

2. You will be redirected to the **Alerts Summary** page. Under **Transport Alerts**, scroll down to **Program Alerts** and select **Create**.

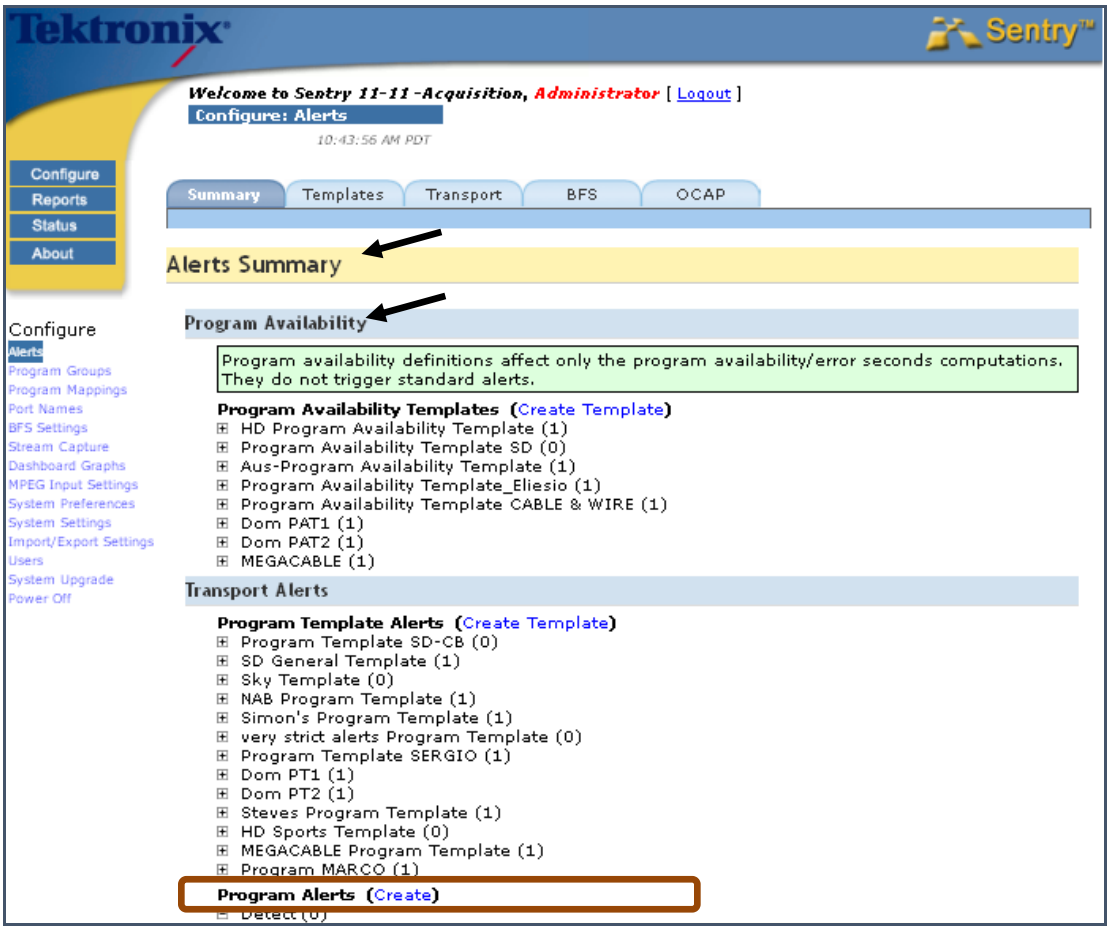


Figure 212: Alerts Summary page

3. You will be redirected to the **Creating Program Alerts** page.

4. In **Section** (1), select **Absolute Audio Levels** from the drop-down menu.

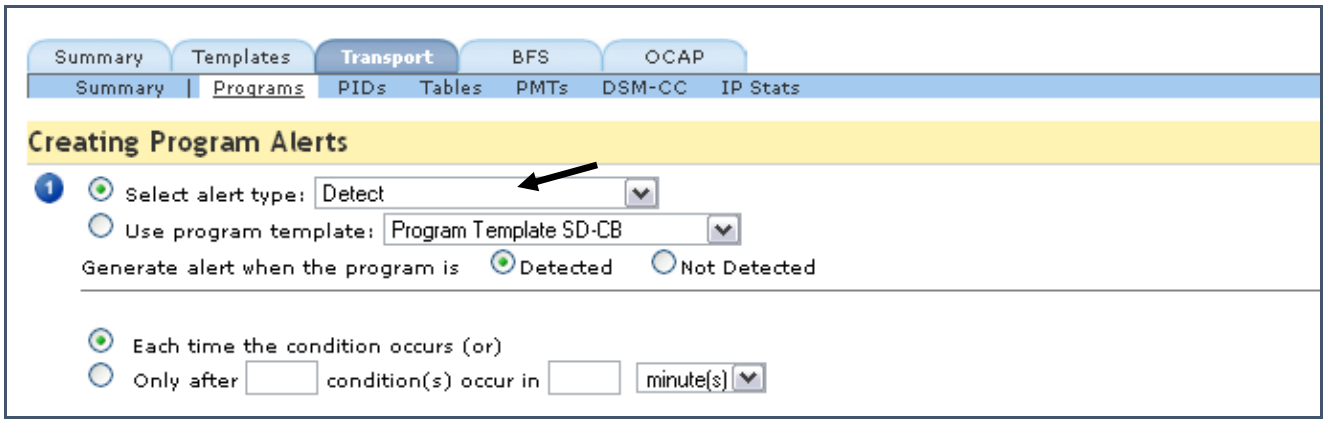


Figure 213: The drop-down menu in Step 1

NOTE: ***Absolute Audio Levels will determine if levels go above or below a certain db rating.***

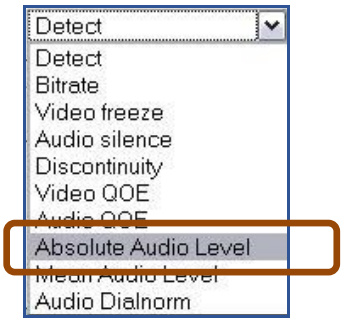


Figure 214: Selecting Absolute Audio Level

5. Section 1 will automatically expand to include the following:

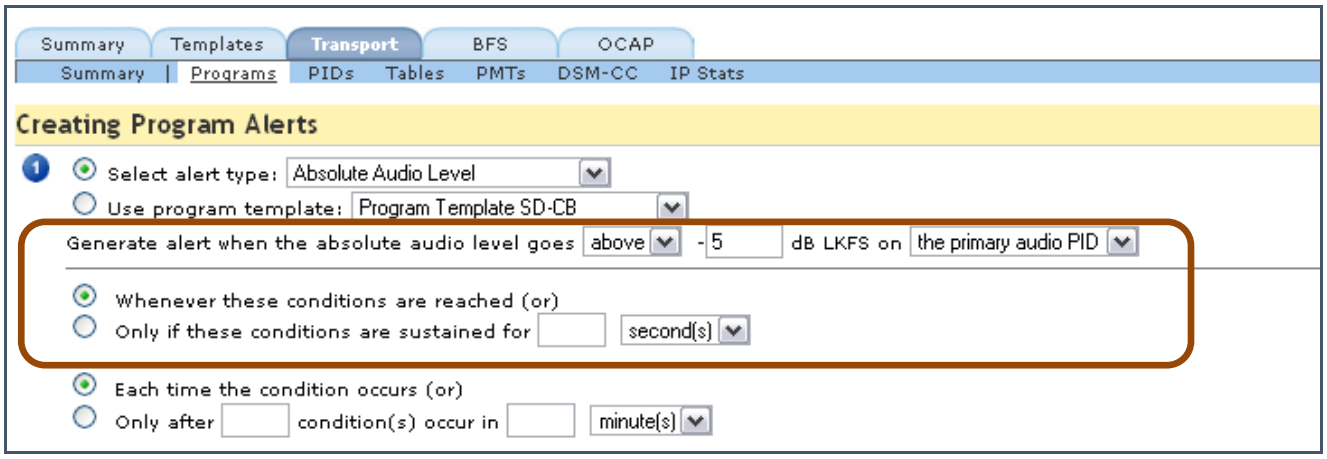


Figure 215: Expanded information area including the fields for "Generate alert when"

6. Set **Generate alert when the absolute audio level goes above/below the dB** for the desired audio program.
7. Set the dB to the desired measurement.
8. Next, select **Only if these conditions are sustained and select the time** requirements.
9. **Section** 2
   Select the **Program Groups** to be monitored from the drop-down menu.

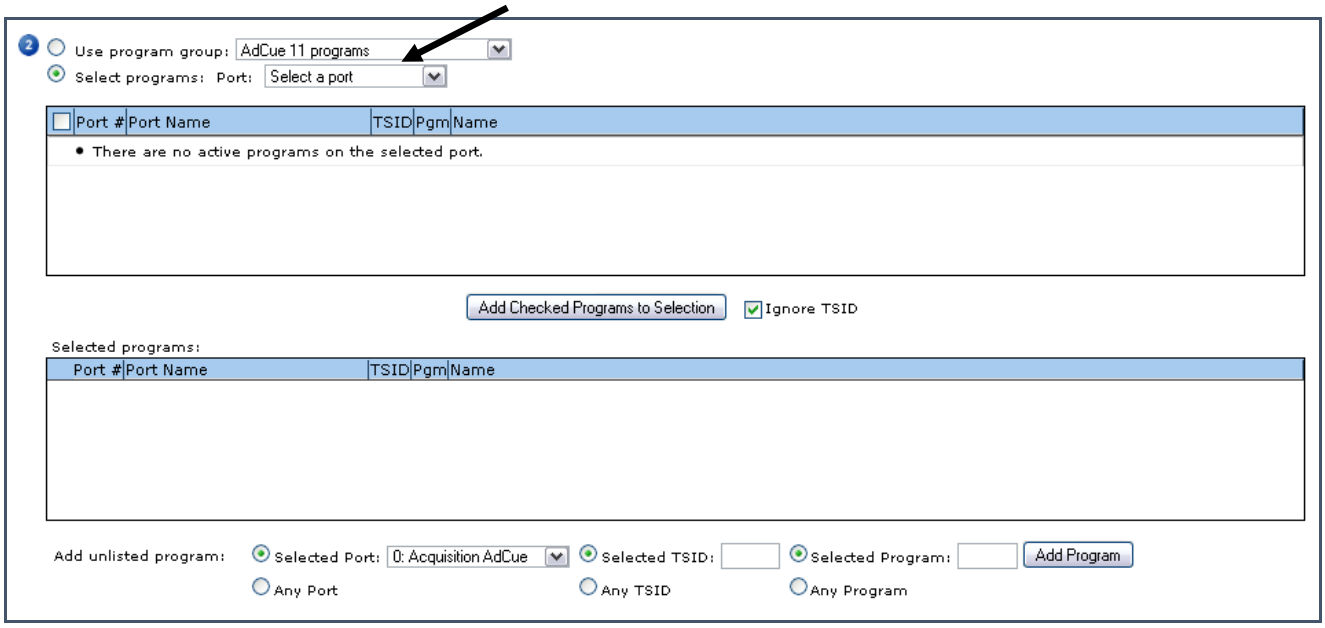


Figure 216: Section 2

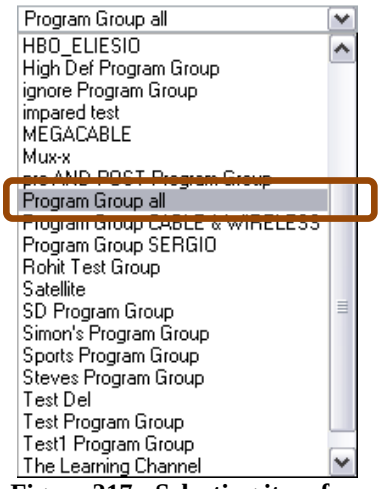


Figure 217: Selecting item from the drop-down menu

10. The table for **Section** 2 will automatically fill with the program information.

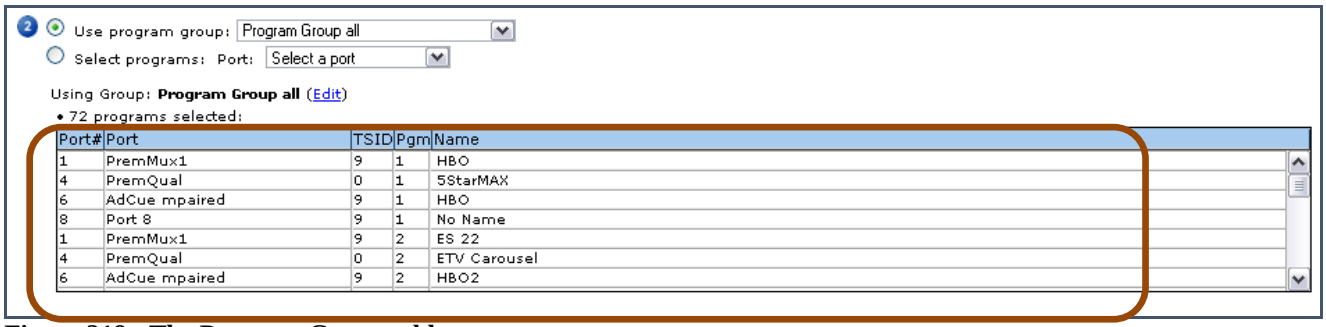


Figure 218: The Program Group table

11. Section 3

Select the email settings for desired notifications.

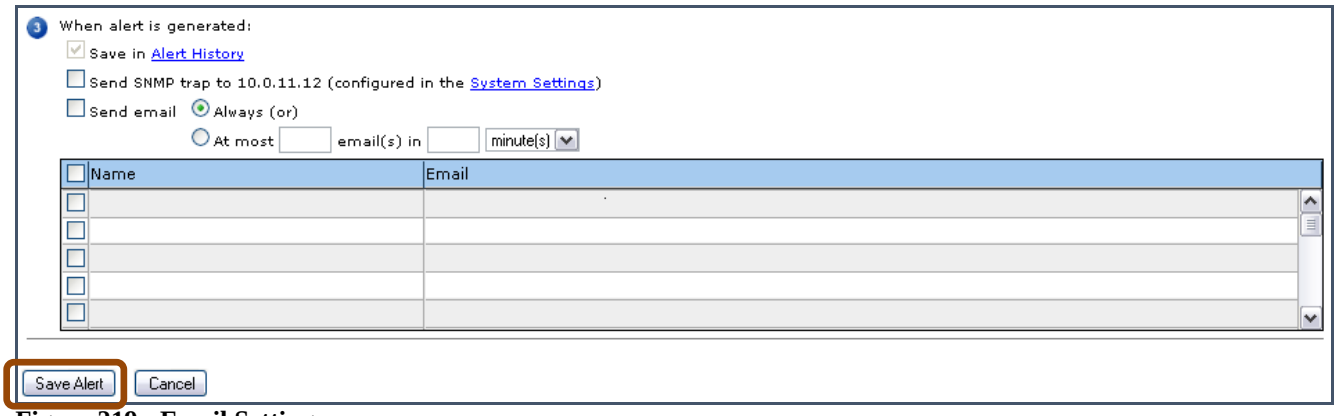


Figure 219: Email Settings

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

Create a Transport NULL PID Bitrate Alert

1. From the main menu, select **Configure** and then **Alerts**.
2. From the **Transport Alerts** column, scroll down to **PID Alerts** and select **Create**.
3. Finally, from the **Creating PID Alerts** page, work your way through **Sections 1-3**.
4. **Section** 1
   Select **Bitrate** from the drop-down menu.

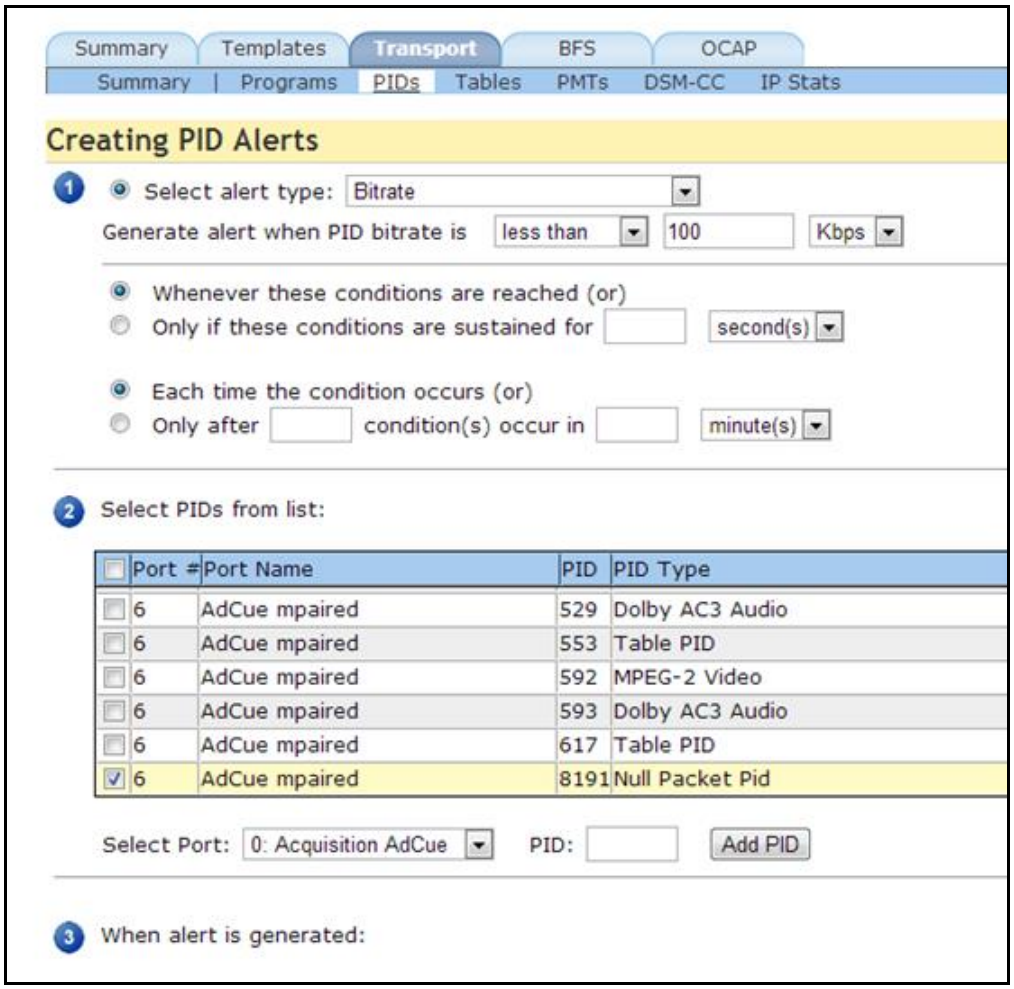


Figure 220: PID alerts template (Transport tab)

5. Set **Generate alert** when the PID bitrate is **less than**.
6. Next select the desired bitrate.
7. Choose any further required limitations.
8. Select PIDs from list.
9. Review **Sections 1-3** and select **Save Alert** when finished.

Create Mean Audio Level Alerts

Mean Audio Level alerts looks to see if the audio level changes by specified amount of dB from the ongoing average over a specified time period. It does NOT measure the average change for that time period. For example, if you specify a 30 dB increase over 10 seconds, Sentry will alert you if the volume increases by 30 db at any point in the last 10 seconds.

1. From the main menu, select **Configure** and then **Alerts**.
2. From the **Transport Alerts** column, scroll down to **Program Alerts** and select **Create**.
3. Finally, from the **Creating Program Alerts** page, work your way through **Sections 1-3**.
4. **Section** 1
   Select **Mean Audio Level** from the drop-down menu

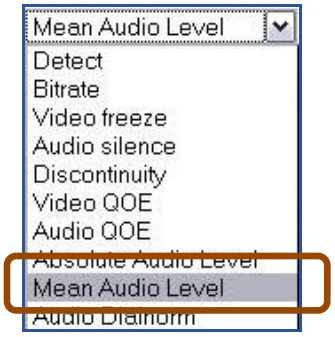


Figure 221: Selecting Mean Audio Level

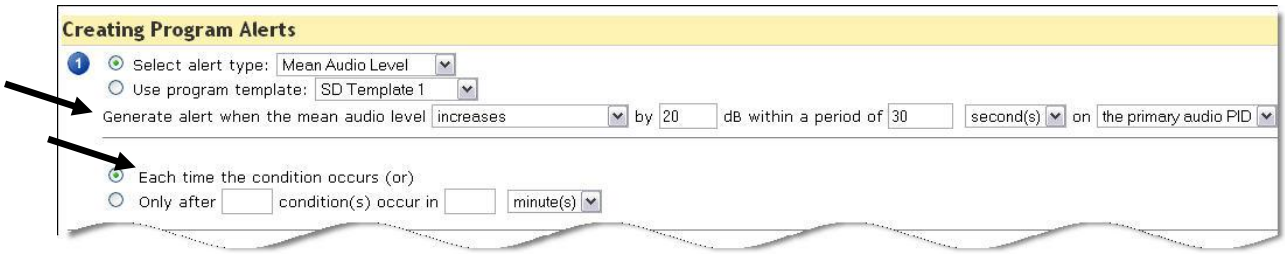


Figure 222: Creating Program Alerts page/ Step 1

5. Set **Generate alert** when the mean audio level to **Increases/Decreases/Either**.
6. Next select the desired dB level and the period of time you wish it to be monitored.
7. Next, select one of the following buttons:
   a. **Each time the condition occurs (or)**

   or

   b. **Only after ___ condition(s) occur in___.**
8. Review **Sections 1-3** and select **Save Alert** when finished.

Create Audio Dialnorm Alert

1. From the main menu, select **Configure** and then **Alerts**.
2. From the **Transport Alerts** column, scroll down to **Program Alerts** and select **Create**.
3. Finally, from the **Creating Program Alerts** page, work your way through **Sections 1-3**.
4. **Section** 1
   Select **Audio Dialnorm** from the drop-down menu

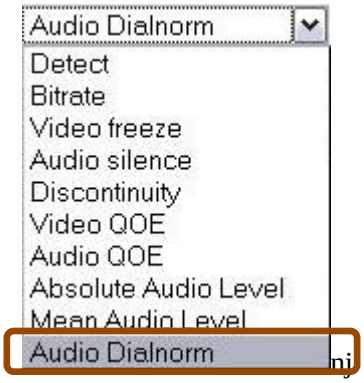


Figure 223: Selecting Audio Dialnorm

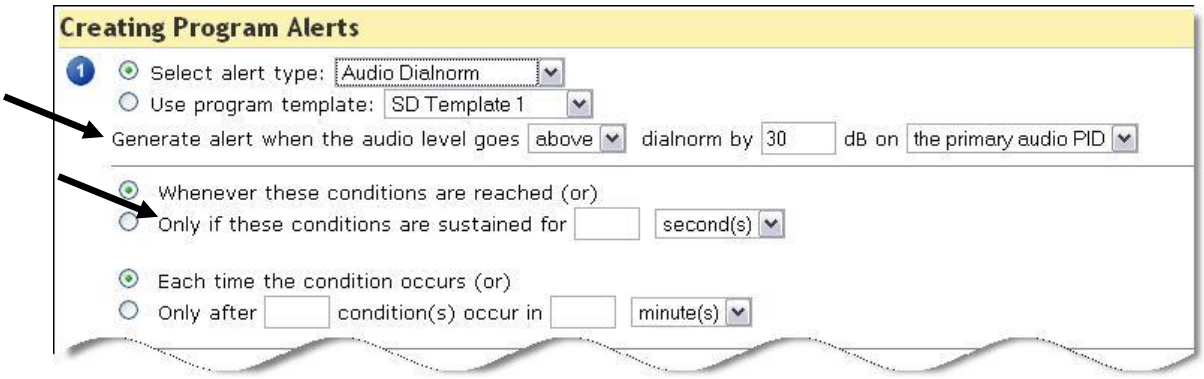


Figure 224: Creating Program Alerts page/ Step 1

5. Set the **Generate alert when the audio level goes** to **above/below.**
6. Next select the desired dB level.
7. Next, select the **Only if these conditions are sustained** button and set the period of time you wish it to be monitored.
8. 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; greater than or equal to 100ms.
- **Audio Buffer Underrun**
  Buffer timing violation causing buffer underrun; equal to0 seconds, meaning that the buffer is empty.
- **Video Buffer Overrun**
  Buffer timing violation causing buffer overrun; greater than or equal to 1 sec.
- **Video Buffer Underrun**
  Buffer timing violation causing buffer underrun; equal to 0 seconds, meaning that the buffer is empty.

Configure Buffer overrun/underrun detection

NOTE*: The Audio Silence Alerts template is the only place to set the Audio 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 looking for specific buffer issues.*

1. From the main menu, select **Configure** and then **Alerts**.
2. Next to the **Program Alerts** heading, select **Create**.

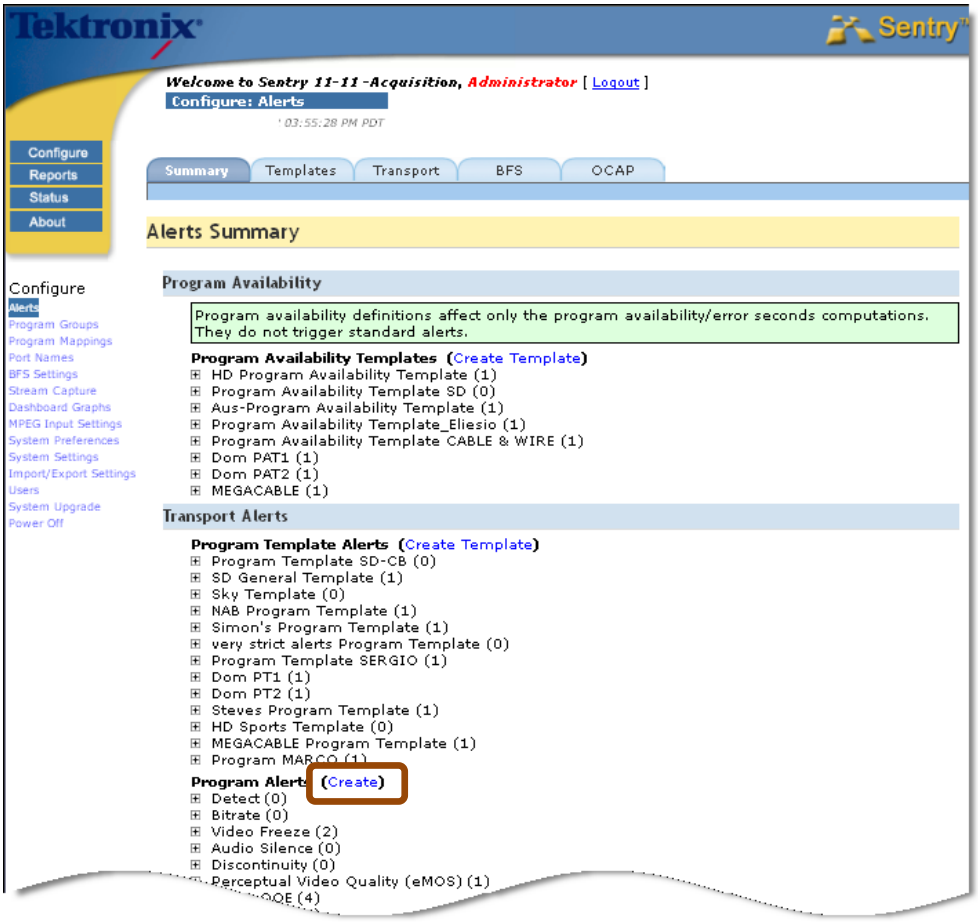


Figure 225: Creating a template for Buffer Overrun/ Buffer Underrun alerts

3. On **Section** 1, select alert type, select **Audio Silence.**

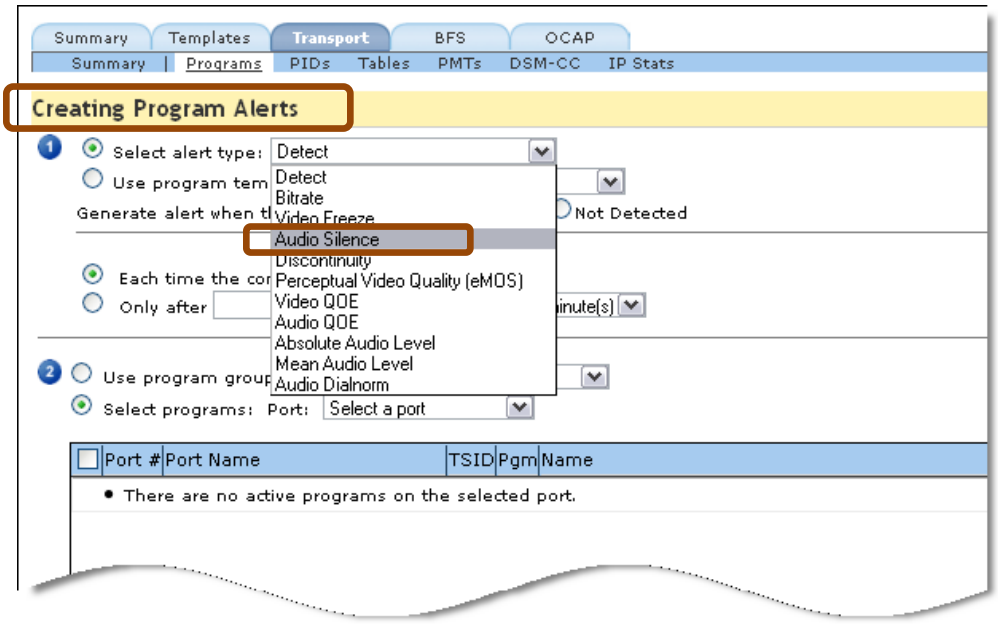


Figure 226: Selecting alert type

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

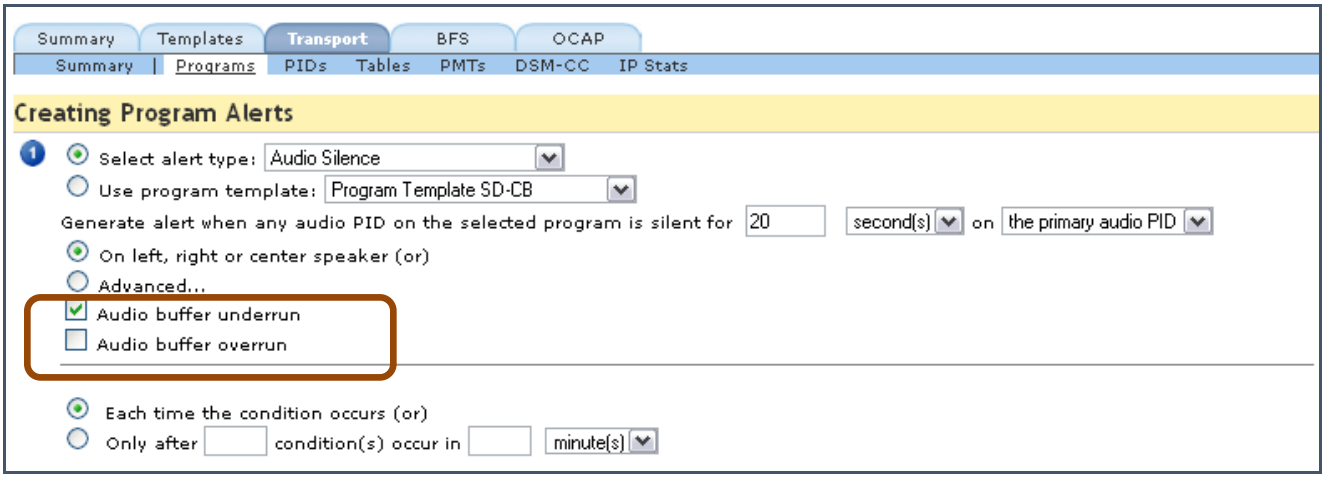


Figure 227: Selecting underrun and/or overrun

5. Please refer to **Chapter 4: Configuring Alerts** for the steps to complete this process.

BFS tab

The **BFS** tab opens the **BFS Alerts Summary** page.

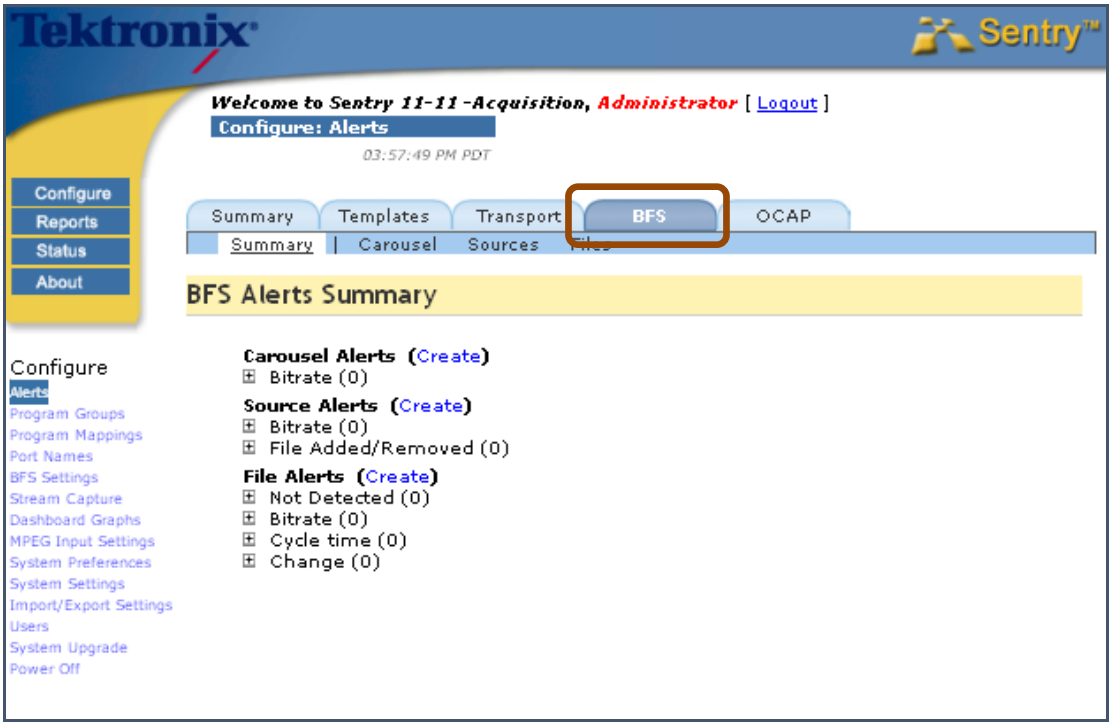


Figure 228: BFS Alerts Summary Page

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.

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.

Configure Program Availability Definitions

1. From the main toolbar, select **Configure** and then **Alerts**.

2. From the resulting page, under **Templates**, select **Create Template** next to the **Program Availability Templates** header.

NOTE: ***Program availability definitions affect only the program availability/error seconds computations. They do not trigger standard alerts.***

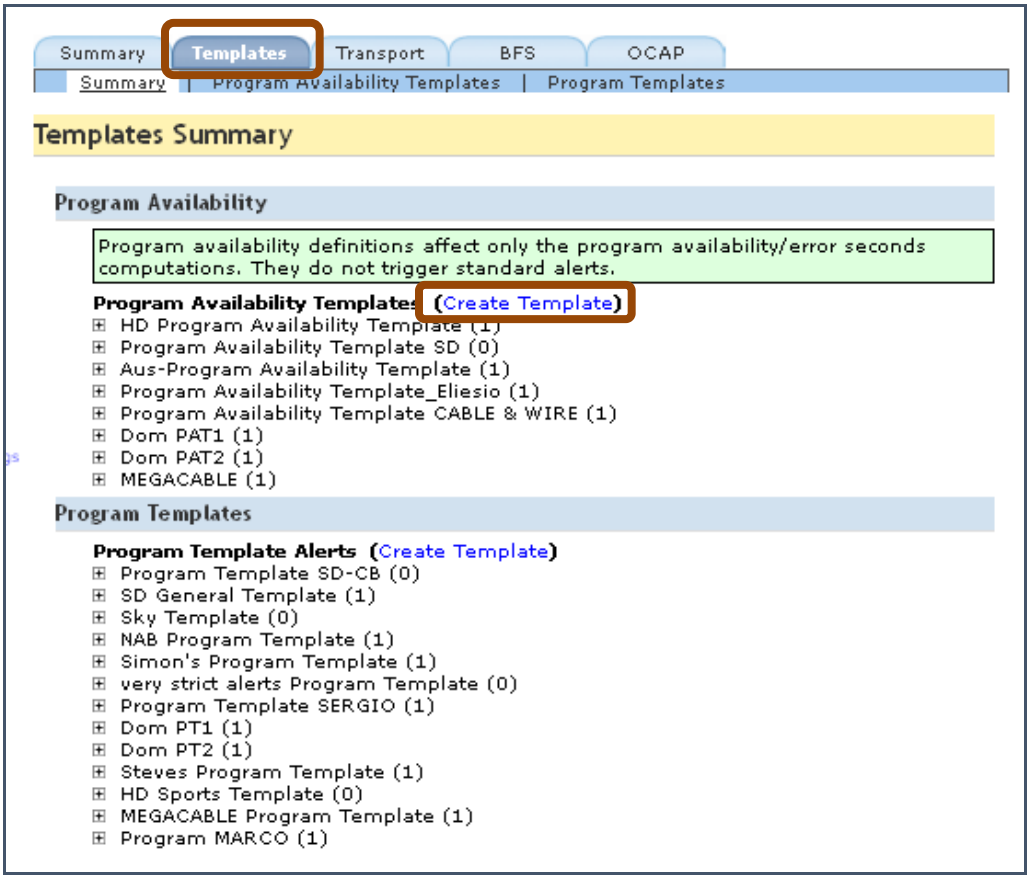


Figure 229: Create a Program Availability Template

3. 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.

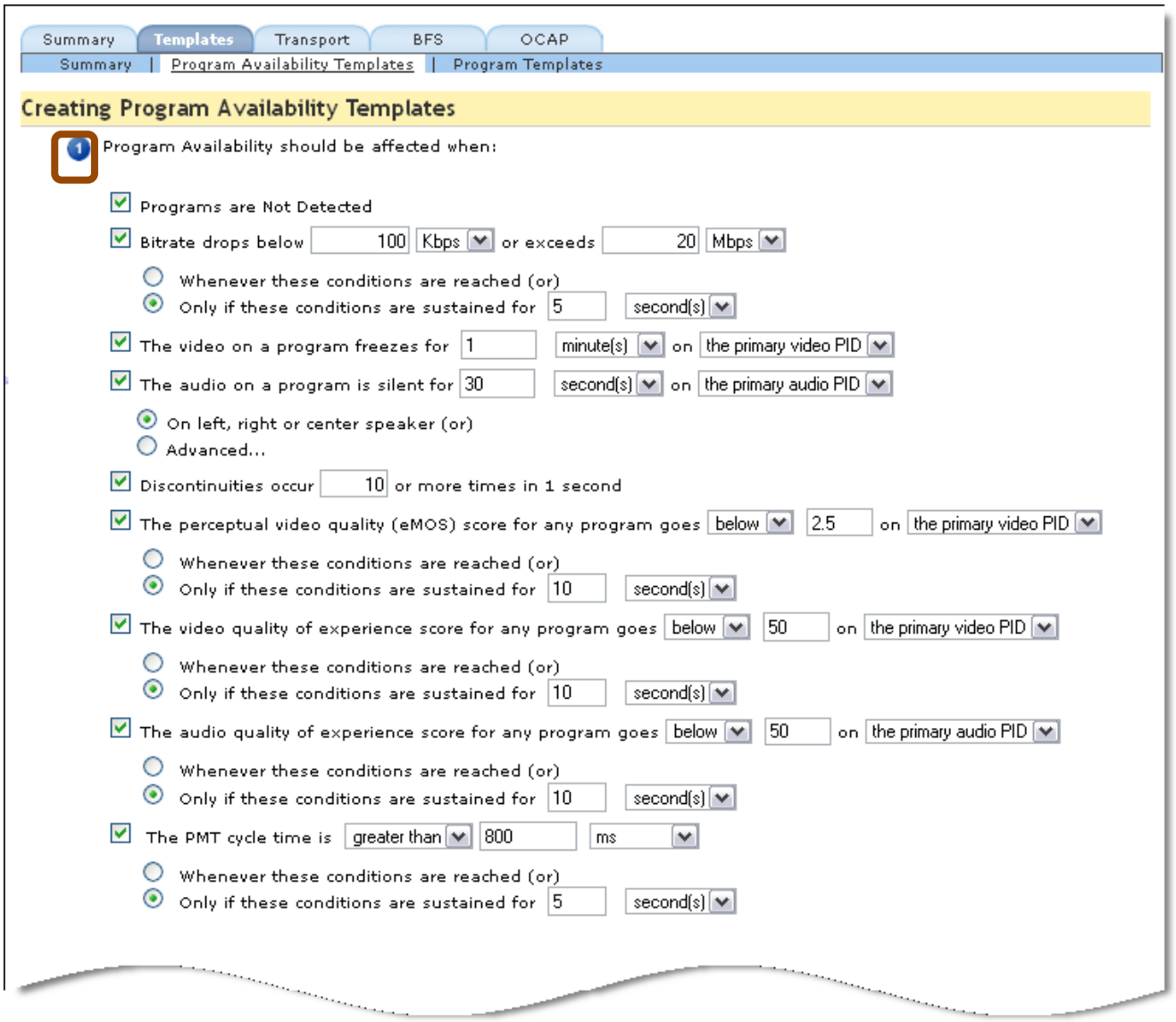


Figure 230: Step 1 for Creating Program Availability Templates

4. In **Section** , 2 name the template and select **Save Template**.

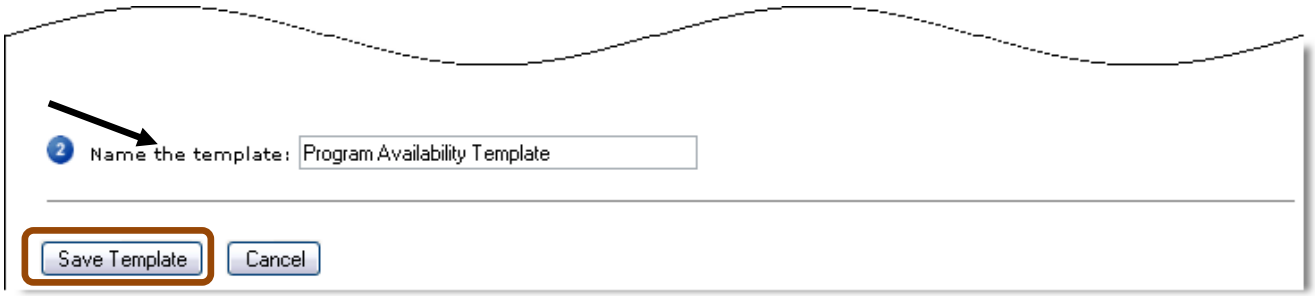


Figure 231: Step 2 Naming and Saving the template

Figure 232: Template Saved dialogue box

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

Create Program Template Alerts

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

Template Alerts

1. From the main toolbar, select **Configure** and then **Alerts**.

Figure 233: Selecting Alerts

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

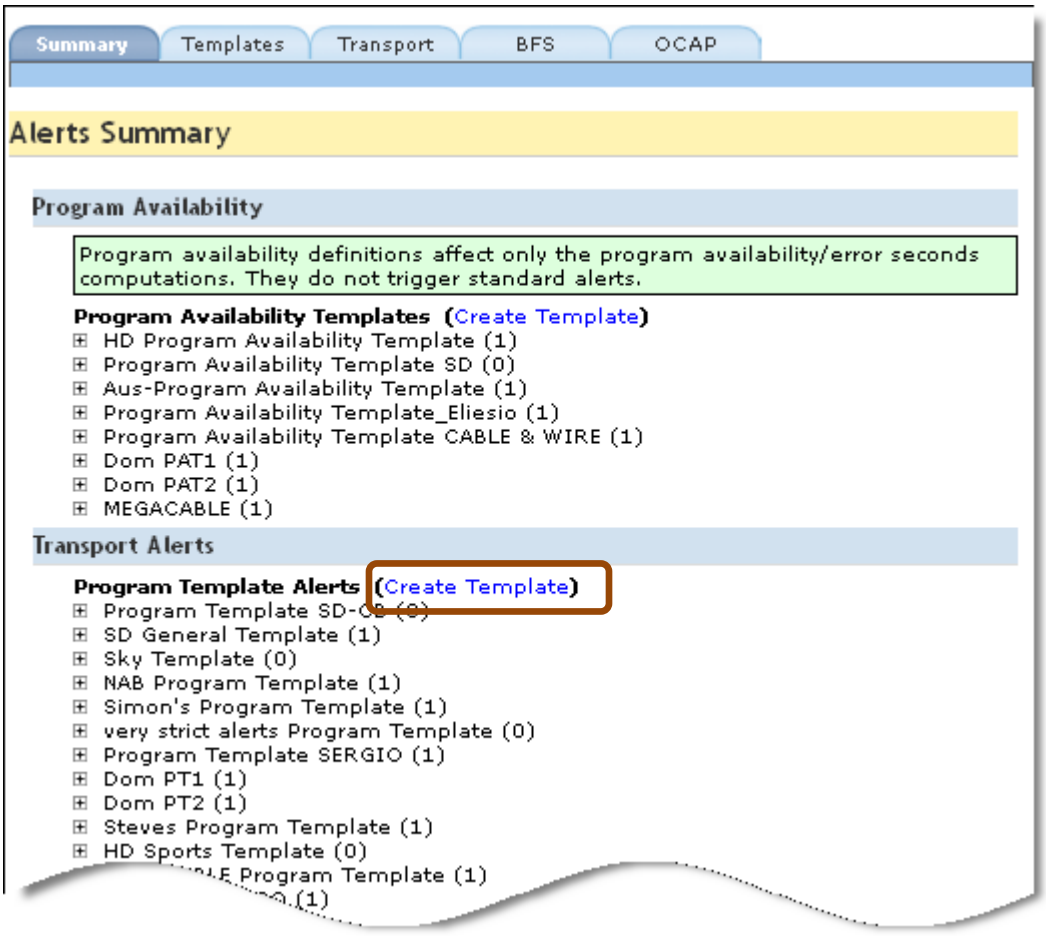


Figure 234: Create a Template

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

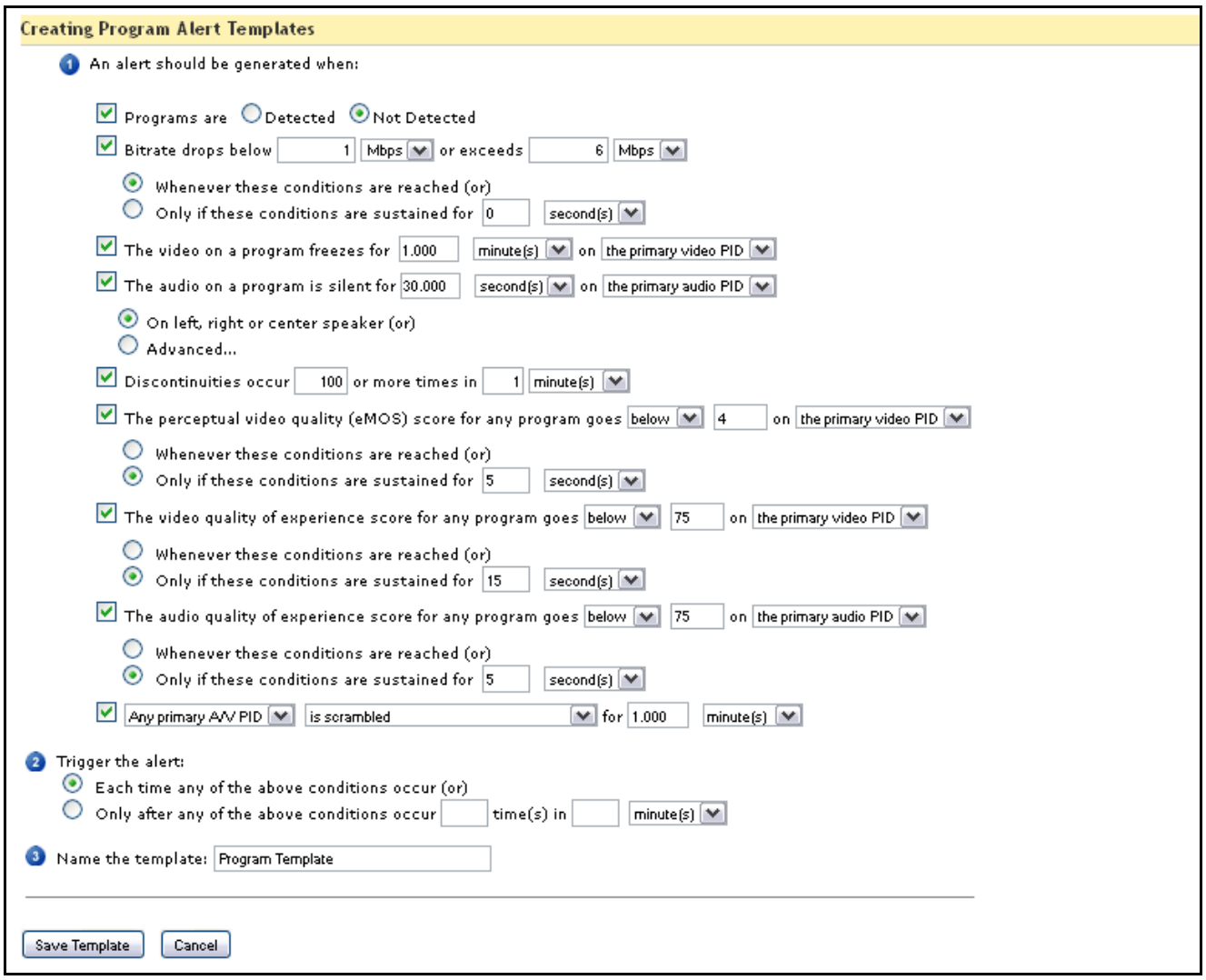


Figure 235: Three steps to Creating Program Alert Templates

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.

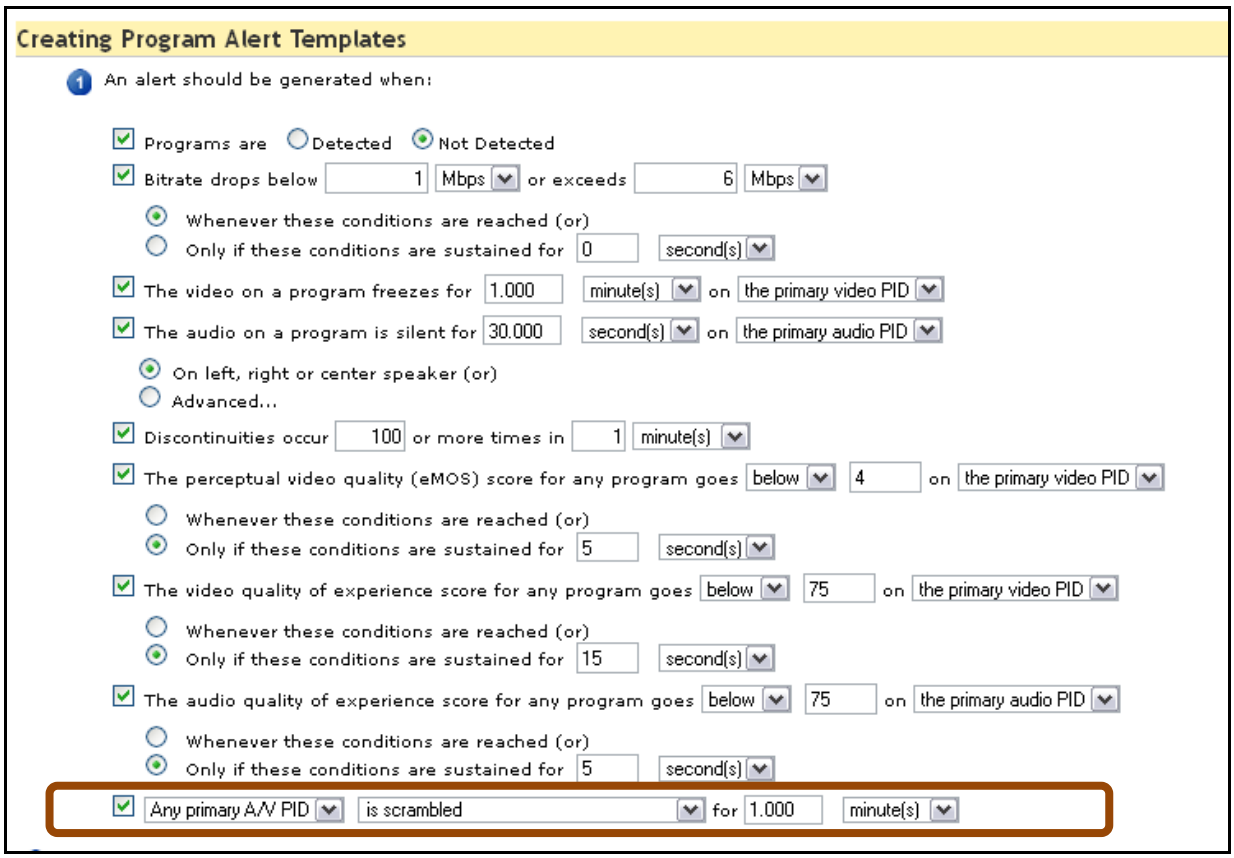


Figure 236: Step 1 Selecting when the alert should be generated

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.

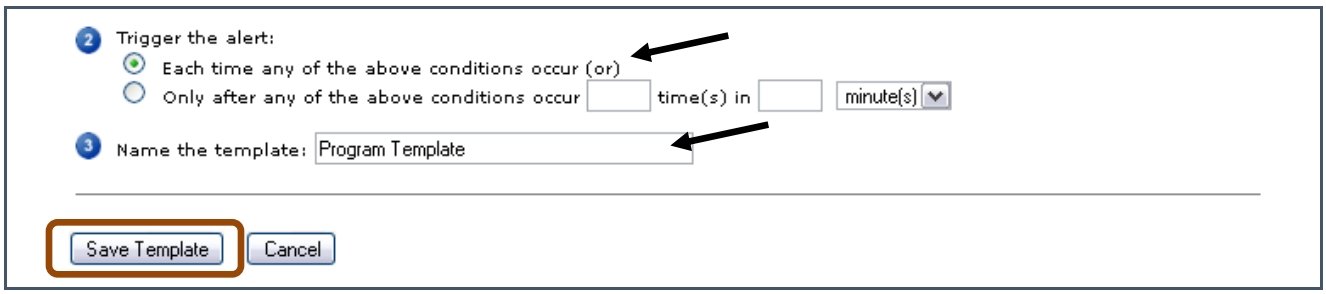


Figure 237: Step 2 Triggering the alert , Naming the Alert and Saving the template

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

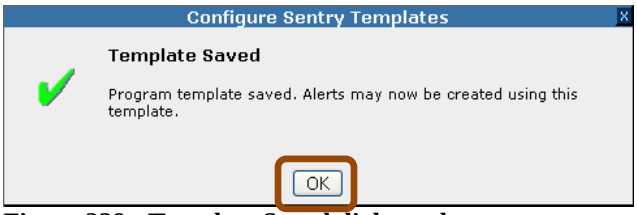


Figure 238: Template Saved dialogue box

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 Sentry 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.

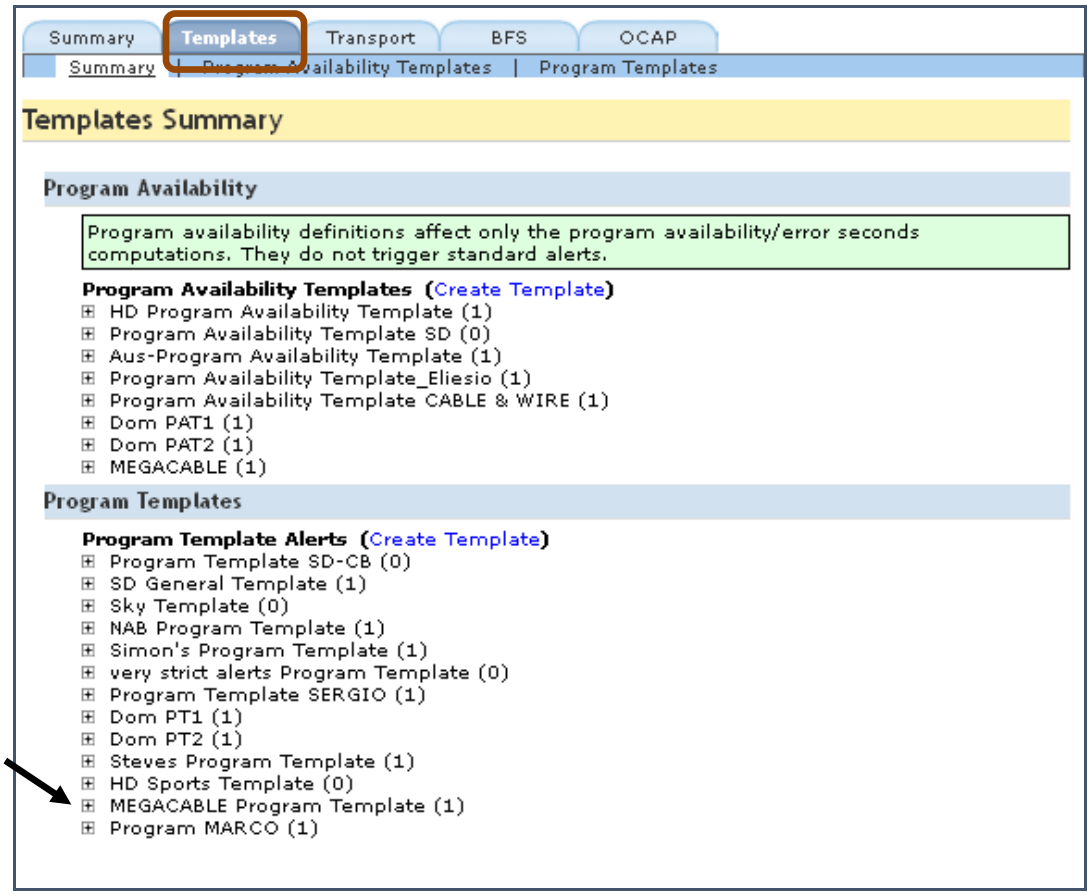


Figure 239: Expanding Program Template Alpha

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

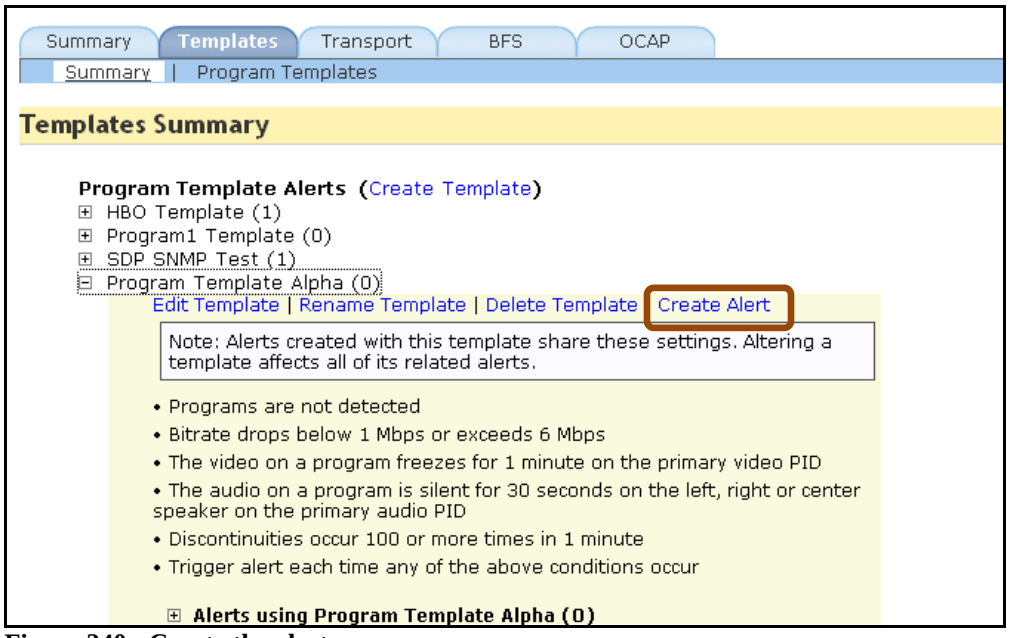


Figure 240: Create the alert

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.

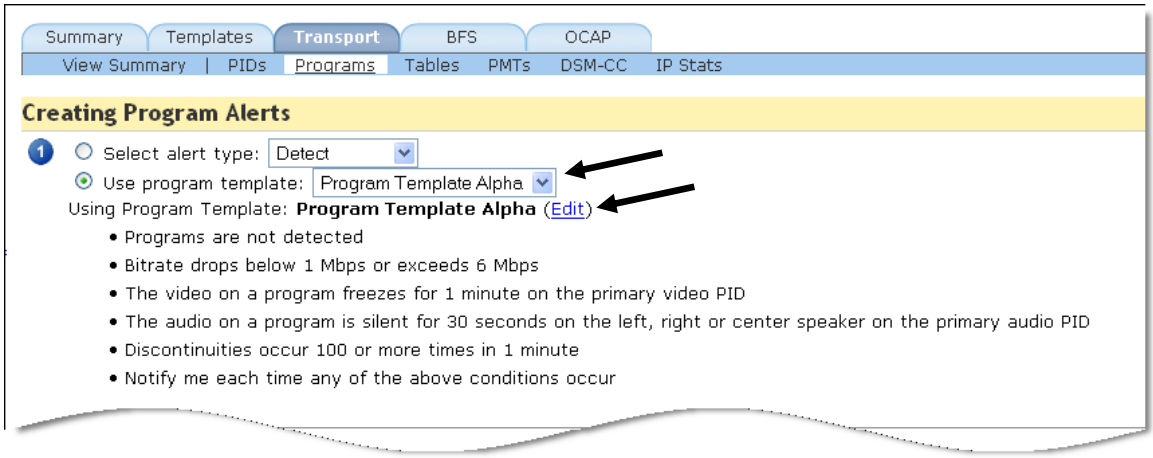


Figure 241: Step 1 Checking for correct Program Template

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.

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

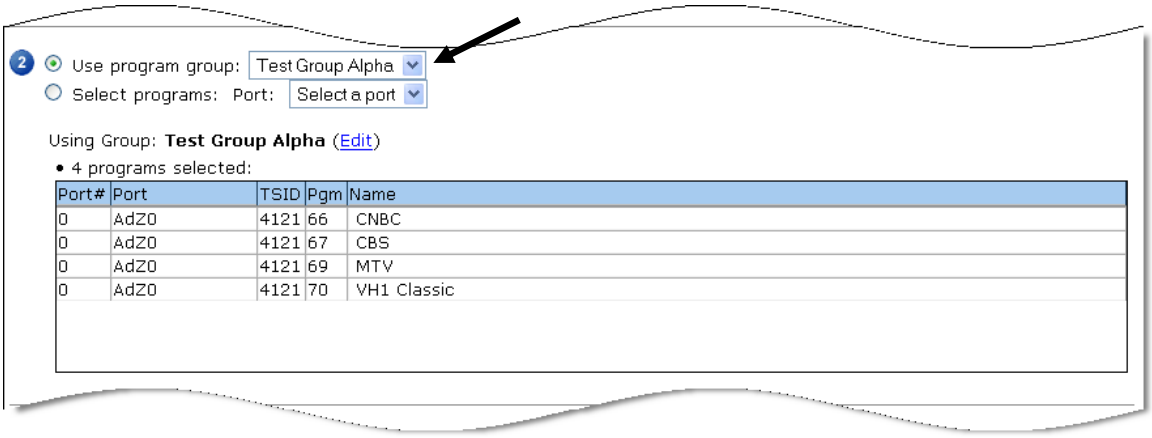


Figure 242: Selecting the Program Group

6. Section 3, set the notifications for the alert.

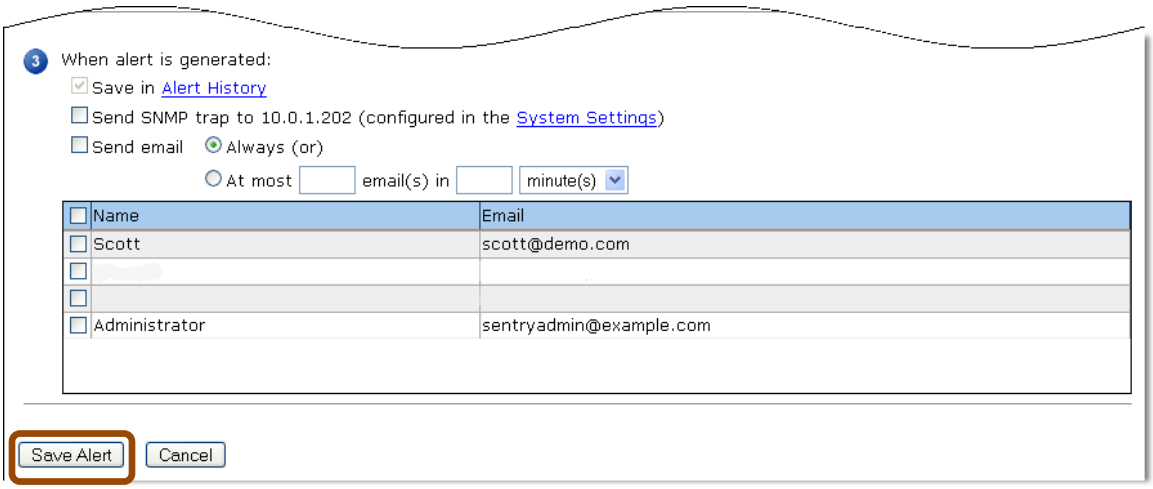


Figure 243: Set Notifications and Save

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

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

Create an alert template without a Program Group

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

2. In **Section** 2 select the radio button for **Select Programs** and click on the drop-down menu for the desired transport stream.

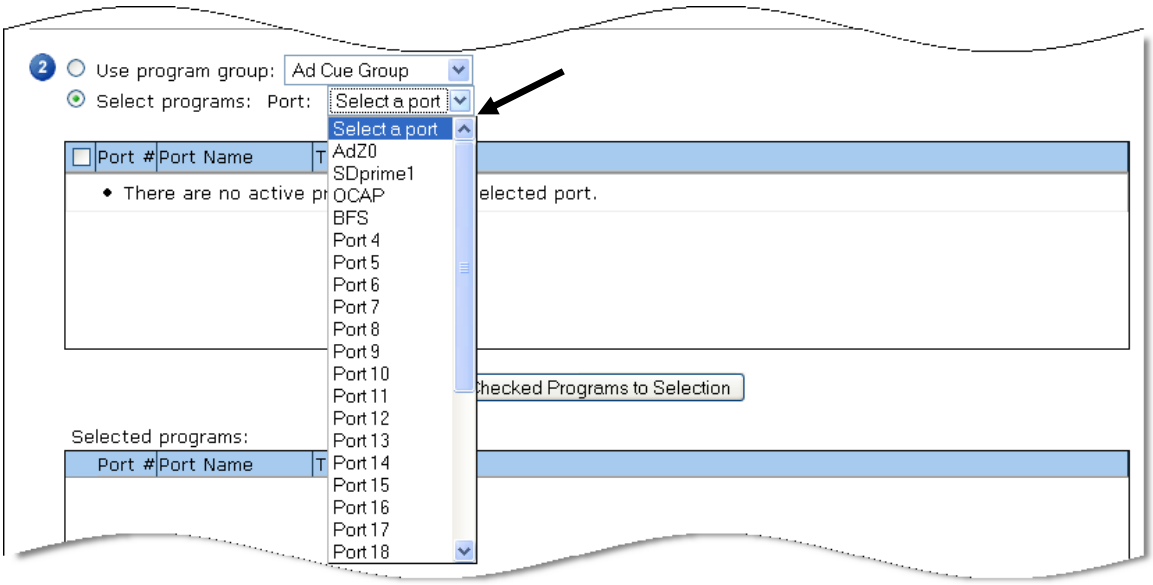


Figure 244: Selecting the Port

3. Select the desired programs by checking their corresponding boxes. 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.

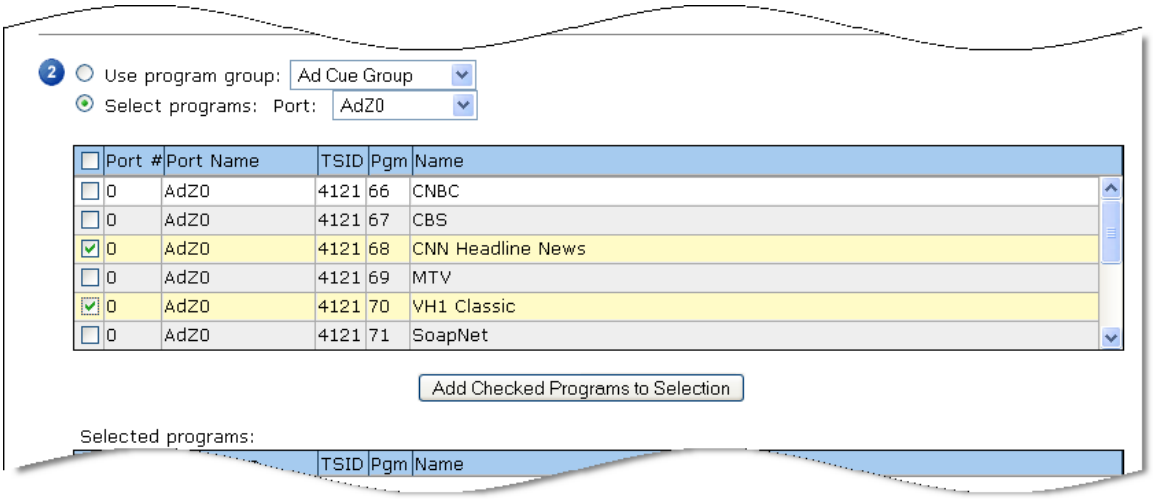


Figure 245: Selecting programs

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

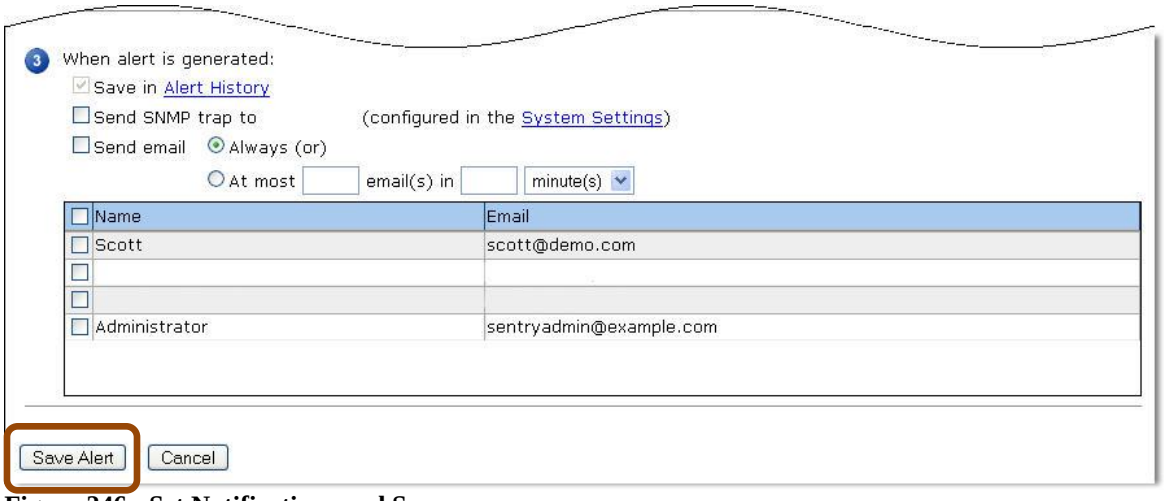


Figure 246: Set Notifications and Save

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

Program Groups

Program Groups allows you to customize any programs on Sentry as a group for convenient alert template application and for problem isolation. For example you can create **Program Groups** by their content type (music program group, HD program group) for applying the most appropriate type of alert. If Sentry is set up to monitor the same programs at different locations (e.g., acquisition vs. post multiplexing), you can create two program group respectively by different location for comparison and for problem isolation.

Create Program Groups

Access Program Groups

1. Select **Configure** and then **Program Groups.**

Figure 247: Selecting Program Groups from the main menu

Groups Summary tab

The **Groups Summary** tab has two primary sections to lead you through the creation process.

1. Start by selecting **Create Group**.

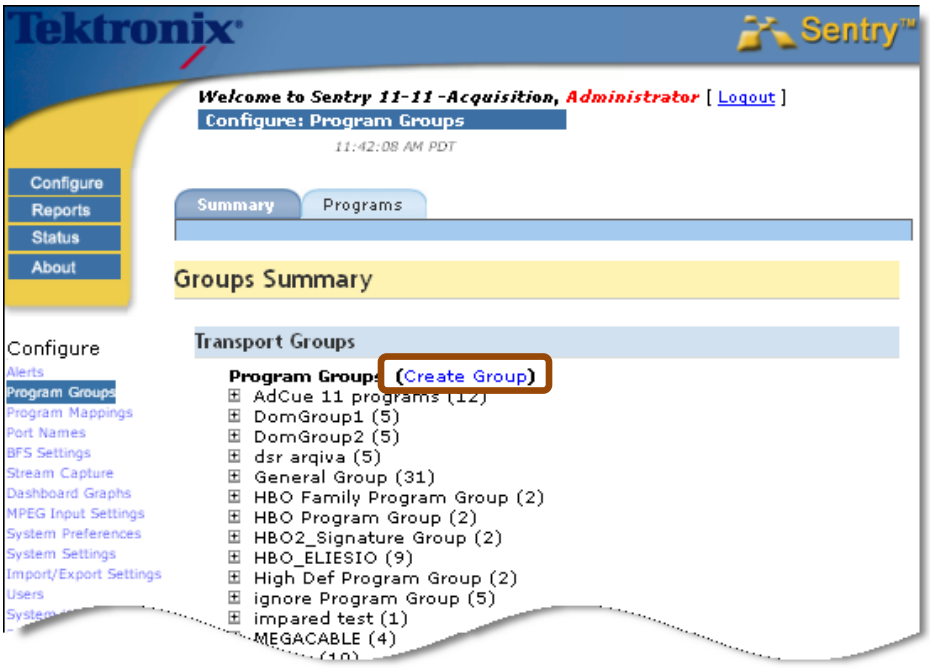


Figure 248: Create a Group

2. **In Section** 1**,** select a port from the drop-down menu**.**

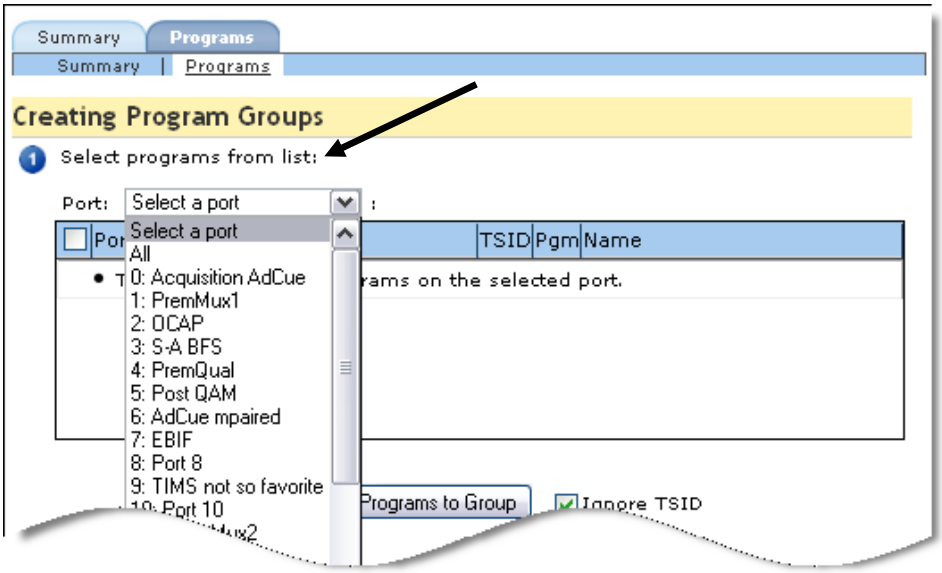


Figure 249: Selecting a Port

3. The result should look similar to this:

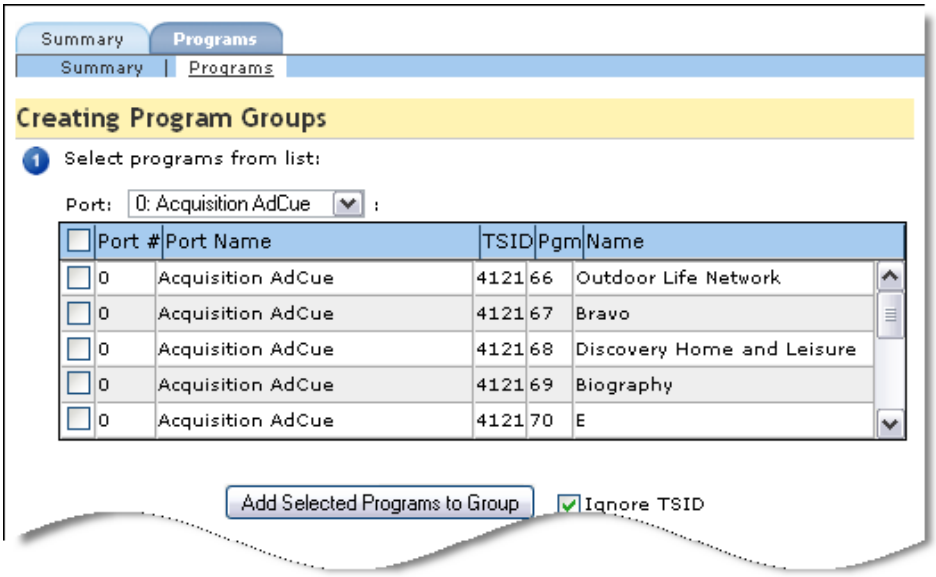


Figure 250: Backfilled Port information

4. Next select the programs you wish to add to the group by checking the appropriate box. When you have finished selecting programs, and click **Add Selected Programs** to **Group**.

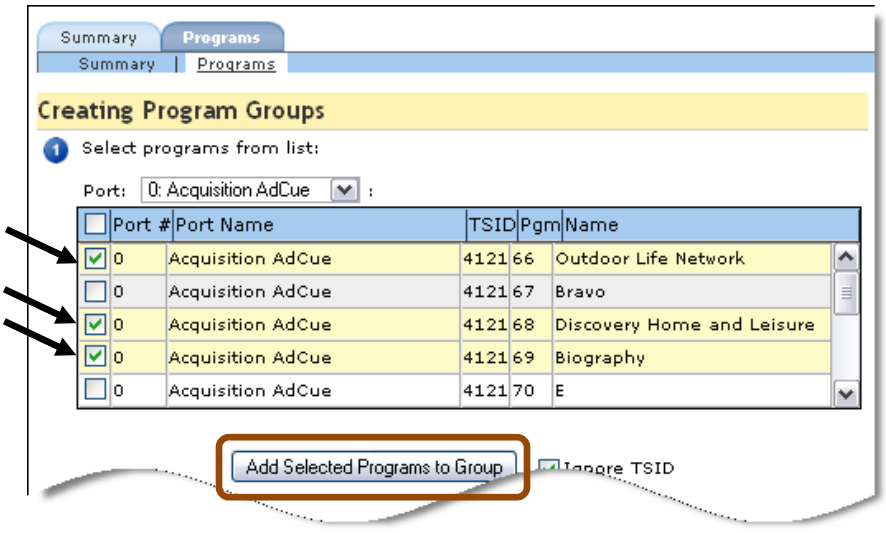


Figure 251: Selecting Programs for a Group

5. The selected programs will now move to **Programs** in group at the bottom of this step. You may continue this process until all desired programs are showing in the **Programs** in group window.

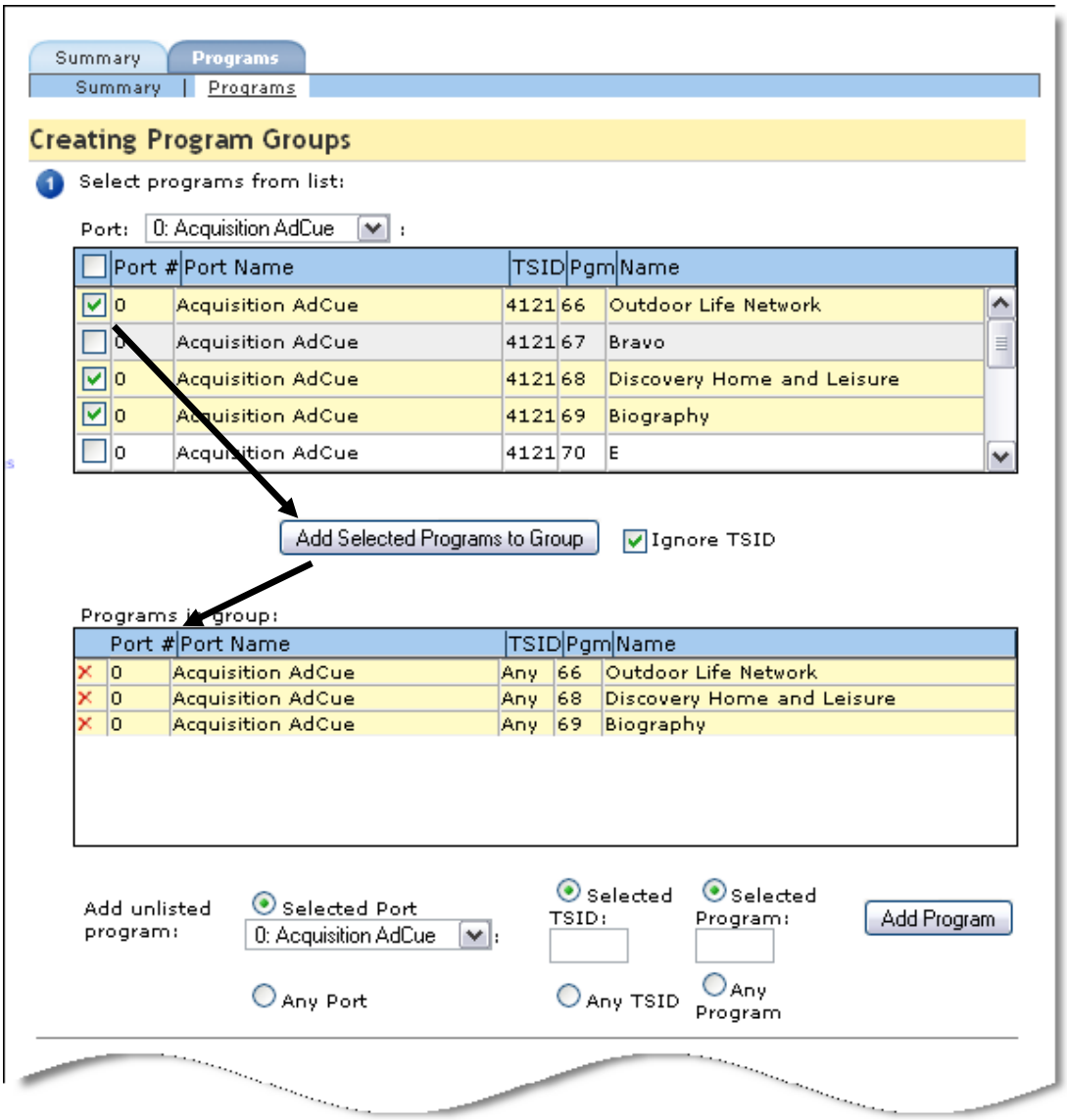


Figure 252: Select the program and add it to the group

6. See the next section, **Adding Unlisted Programs** for the rest of this process.

Add unlisted programs

At this time, you may also add programs to the group that are not on the list by using the section at the bottom of **Section** 1. This is a handy feature for upcoming programs.

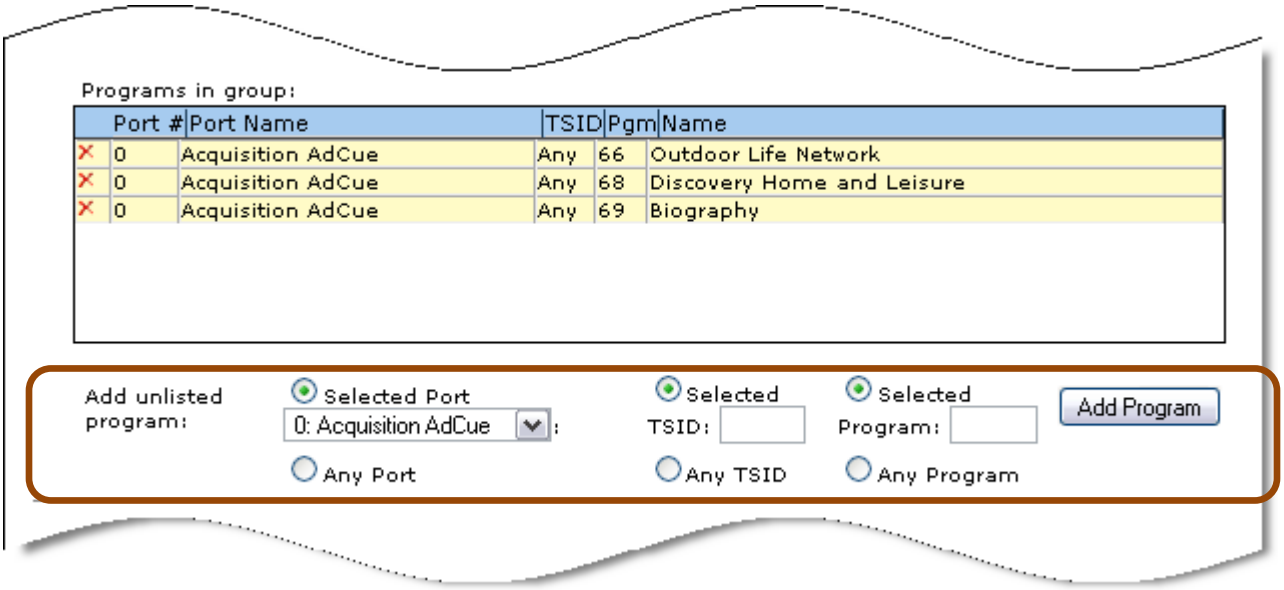


Figure 253: Add unlisted programs

1. Select the **Port**, **TSID** and **Program**.
2. Select the **Add Program** button to add it to the **Programs** in group list. To delete it from the list, select the **X** button on the left.
3. In **Section** 2, type in the name of the group and select **Save**. The name may be anything you think would make a good reference name.

Figure 254: Save the Group

4. To finish the creation process, review **Sections** 1 and 2 and then select **Save Group**.

5. You will receive the following notification box. Select **OK** to continue.

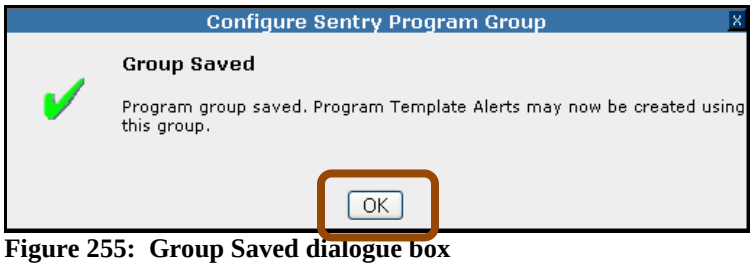


Figure 255: Group Saved dialogue box

6. You will be sent to the **Program Groups** Summary page where the new group name will appear.

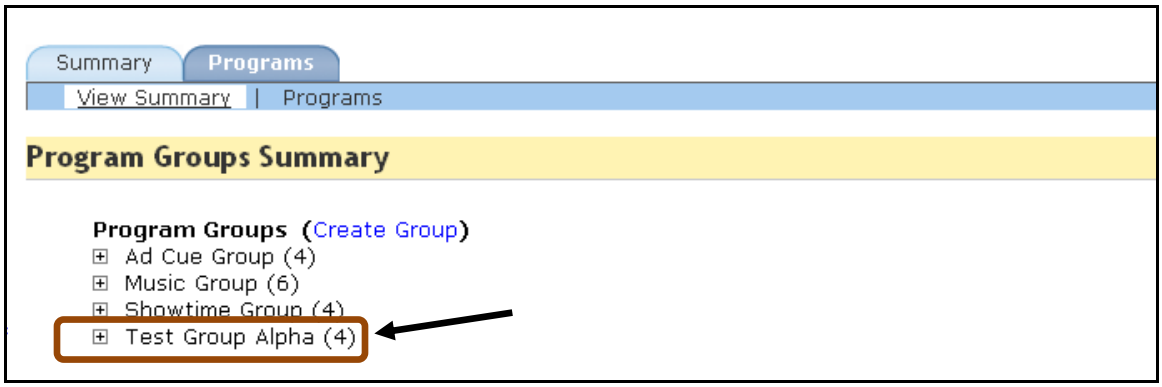


Figure 256: The new program group

7. You are now done creating a **Program Group**.

Configure Program Mappings

Sentry automatically detects program names and associated icons within the transport stream; however, in some cases this data is not available. **Configure: Mappings** 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 **Configure: Mappings** from the main page menu or sub-page menu.

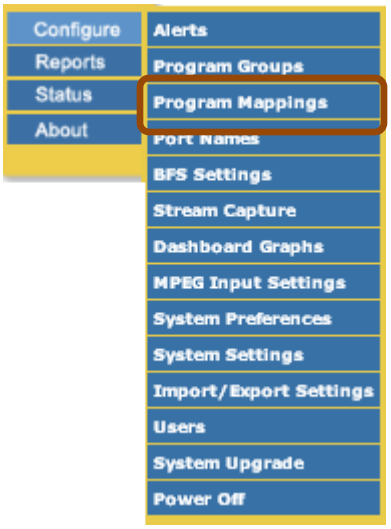


Figure 257: Selecting Program Mapping

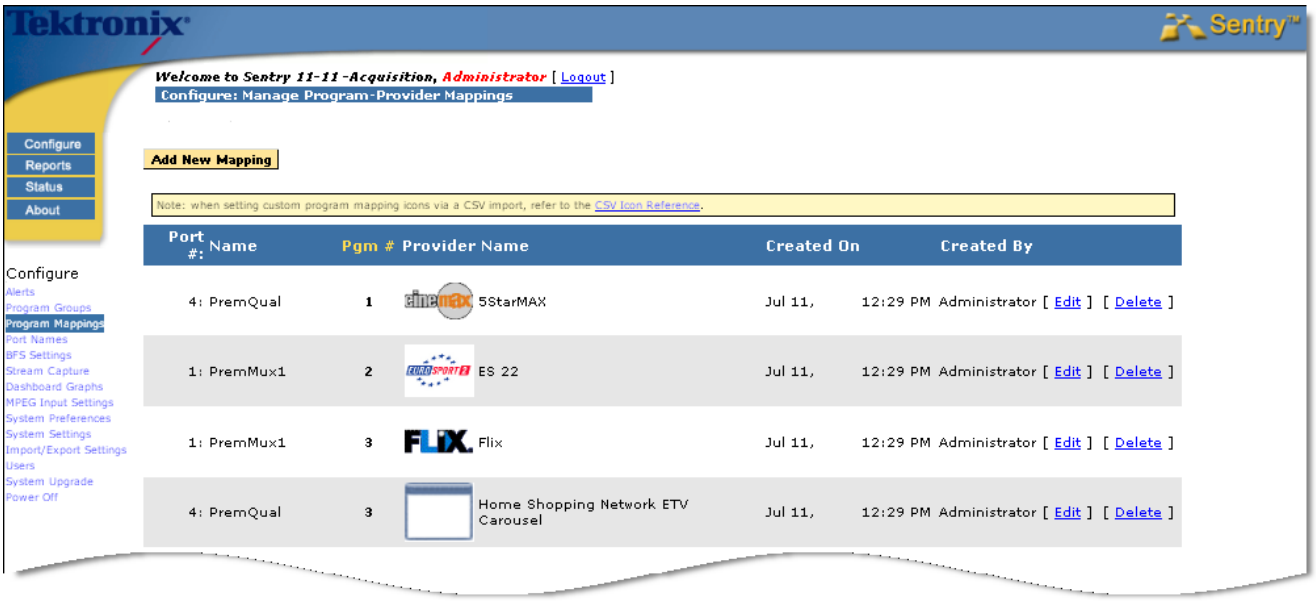


Figure 258: Program Mapping welcome screen

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

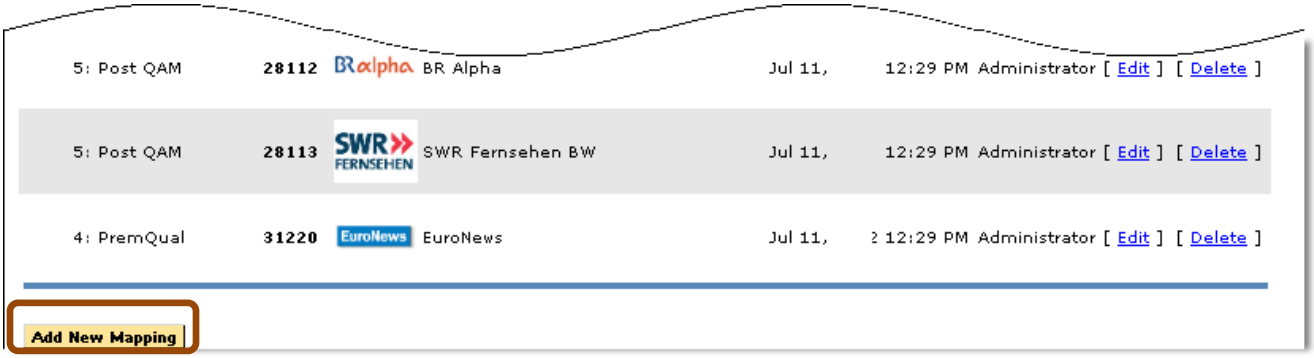


Figure 259: Add New Mapping button

3. Next, select the port and program number for which you want to create the mapping.

4. 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 entered manually.

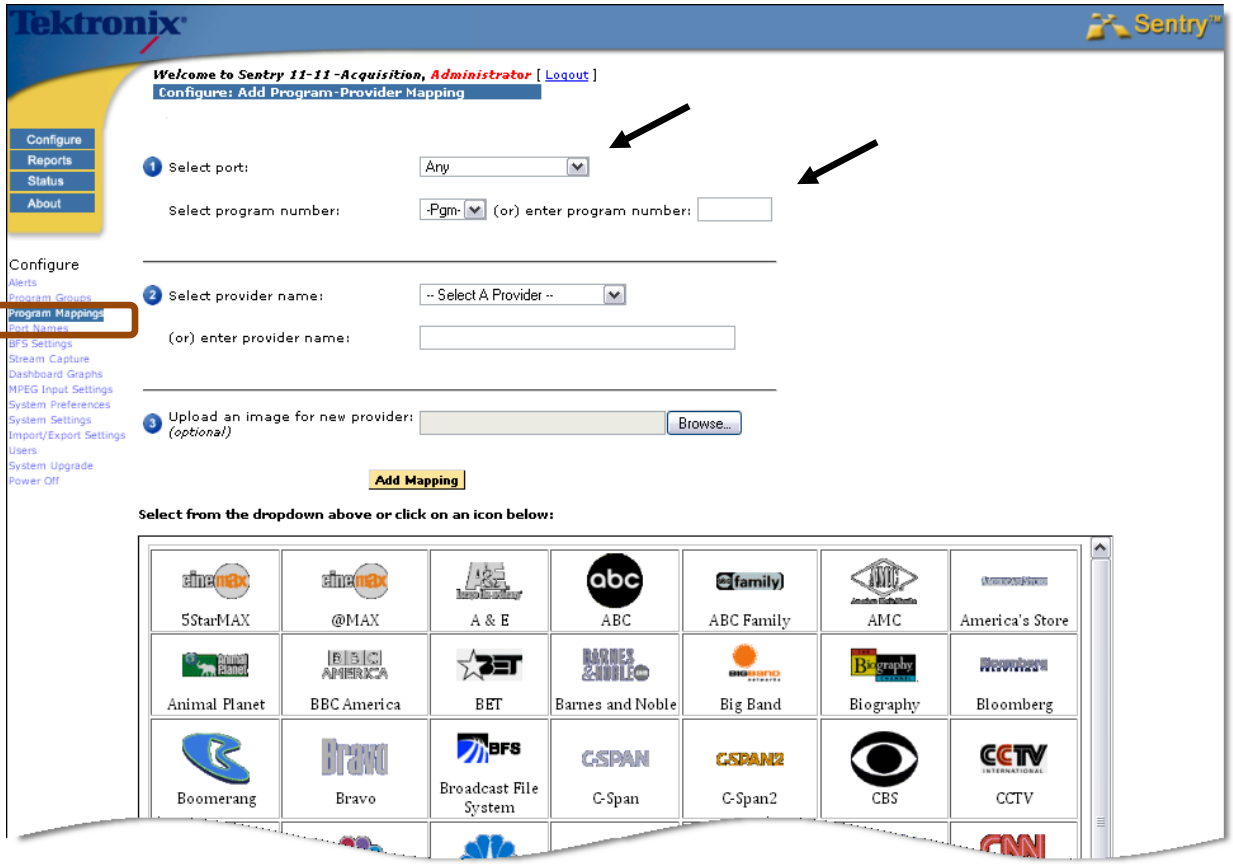


Figure 260: Select a Port and Program

5. Select the provider either from the drop-down list or by clicking on one of the available icons. There is a one-to-one correspondence between the provider name and the icon.
6. Click **Add Mapping**.

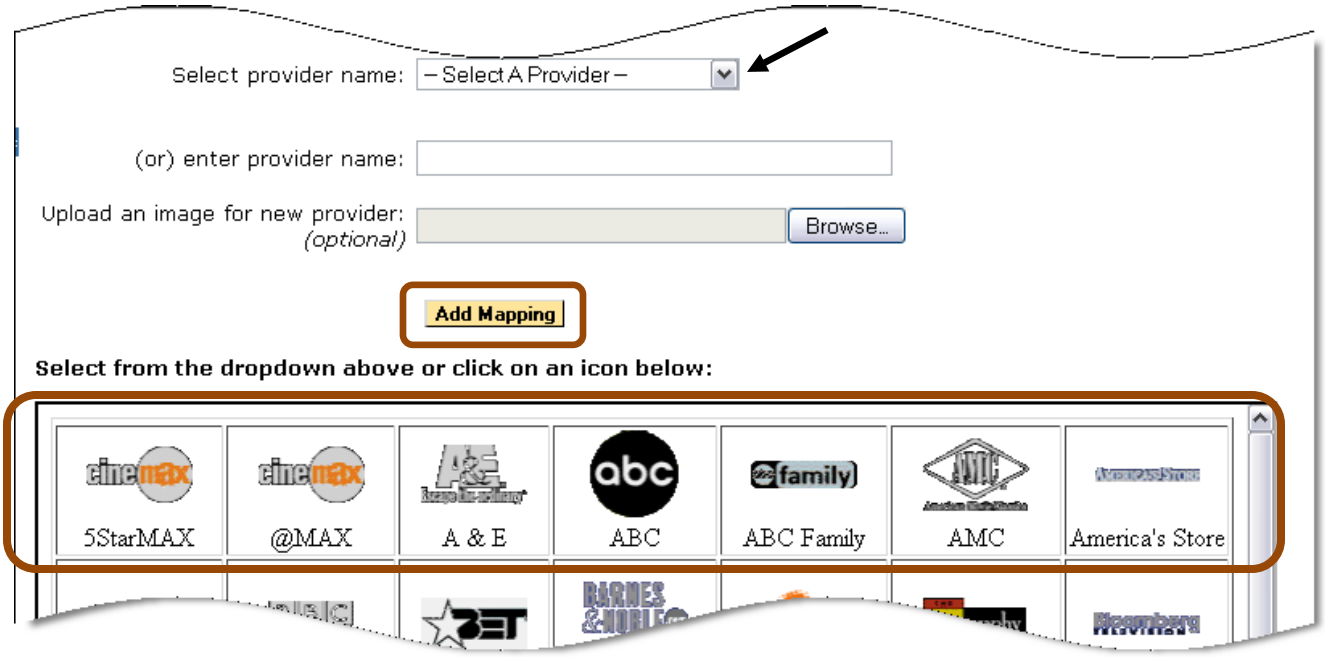


Figure 261: Select Provider and Icon

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

NOTE 1: Existing **Mappings** will be 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.

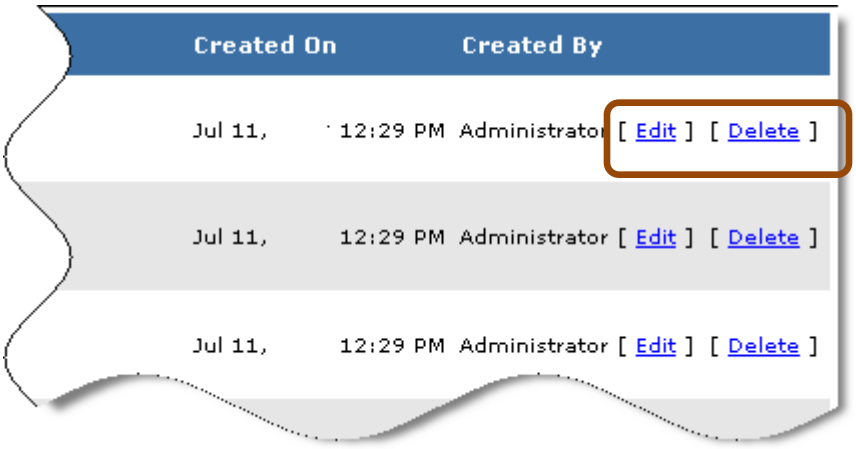


Figure 262: Delete a Mapping link

Modify a Mapping

To modify a mapping select the **Edit** link.

The **Configure: Add Program-Provider Mapping** page opens configured with the selected program's mapping, which may then be modified.

Configure Port Names

1. Sentry offers the capability to name an individual port.
2. Start by locating the unnamed port and clicking **Edit**.

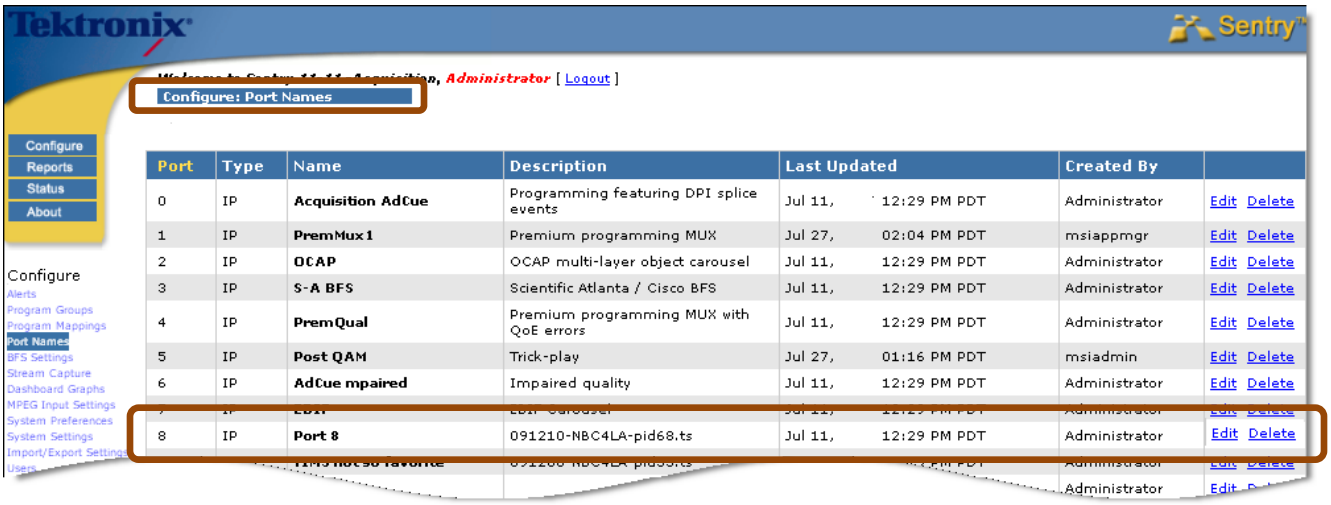


Figure 263: Configure Port Names

3. Next, add the new port name in the appropriate field.
4. The port names appear on each report, including on the **Current Status** page.

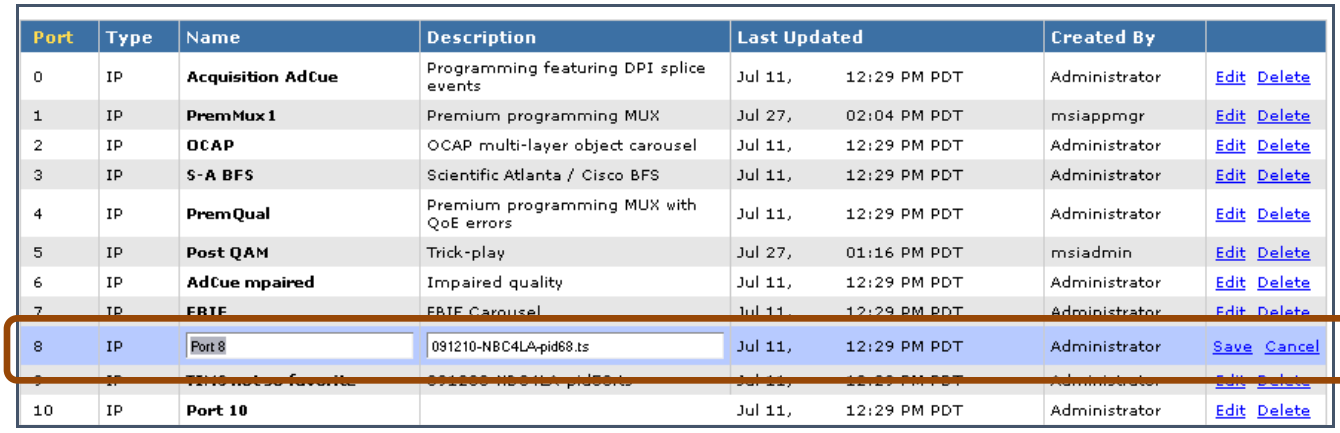


Figure 264: Port Names

Configure 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**.

1. To configure, enter the source ID for the **BFSdir file** in the corresponding field.

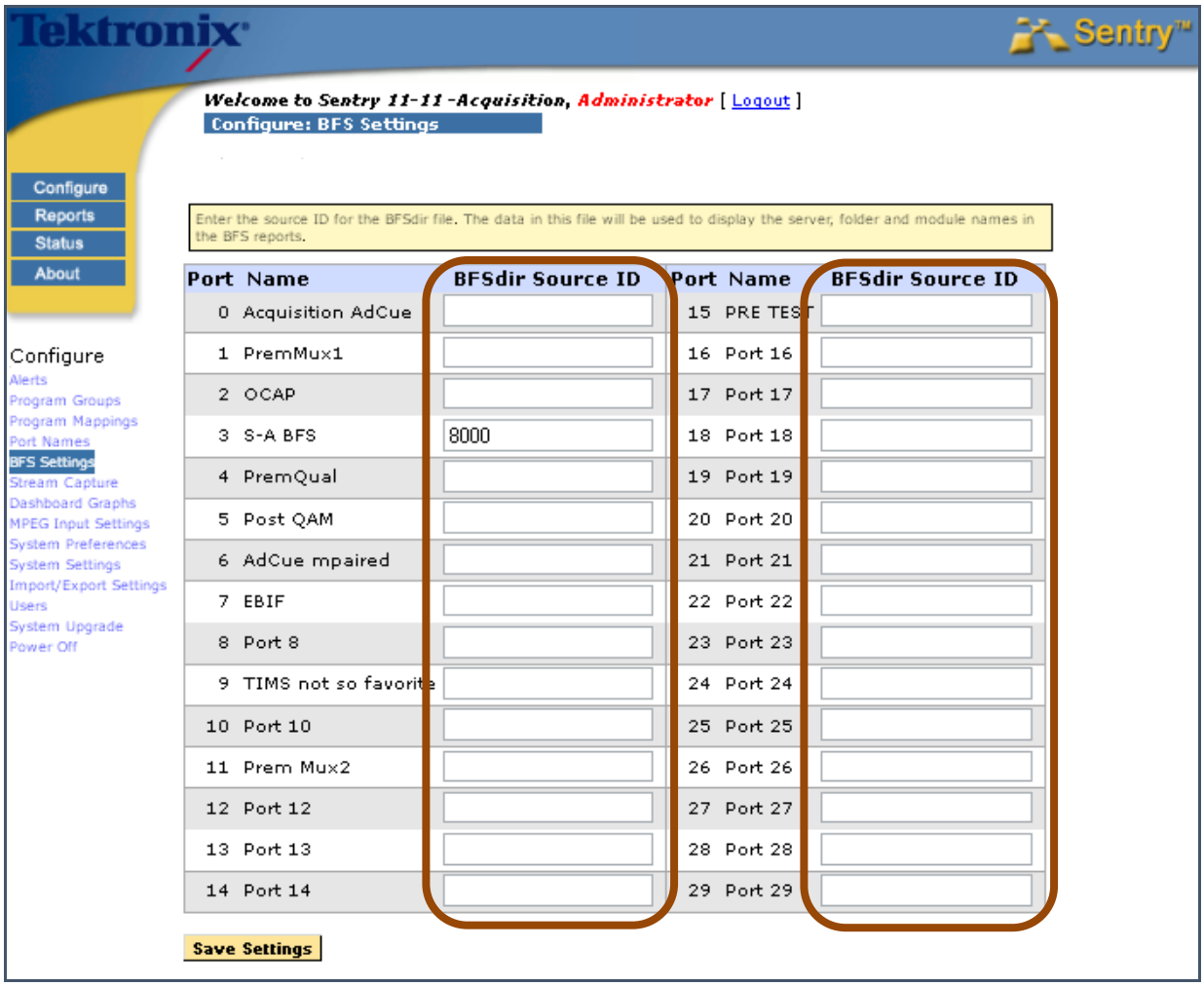


Figure 265: BFS Settings

2. Select **Save Settings** when complete.

Configure Triggered Stream Captures

Alert Triggered Stream capture allows you to save a program to a file when specified conditions occur.

You can get a stream capture one of two ways:

- **Triggered by Alert**
  Captures automatically through an alert you set up to fire under certain conditions. This captures the same data as the **Capture Now** button on the Program Details screen.
- **Triggered by User**
  Captures manually through the **Capture Now** button.

See the **About** section on your Sentry for license specifications on your particular unit. (See your Tektronix Account Manager for more information.)

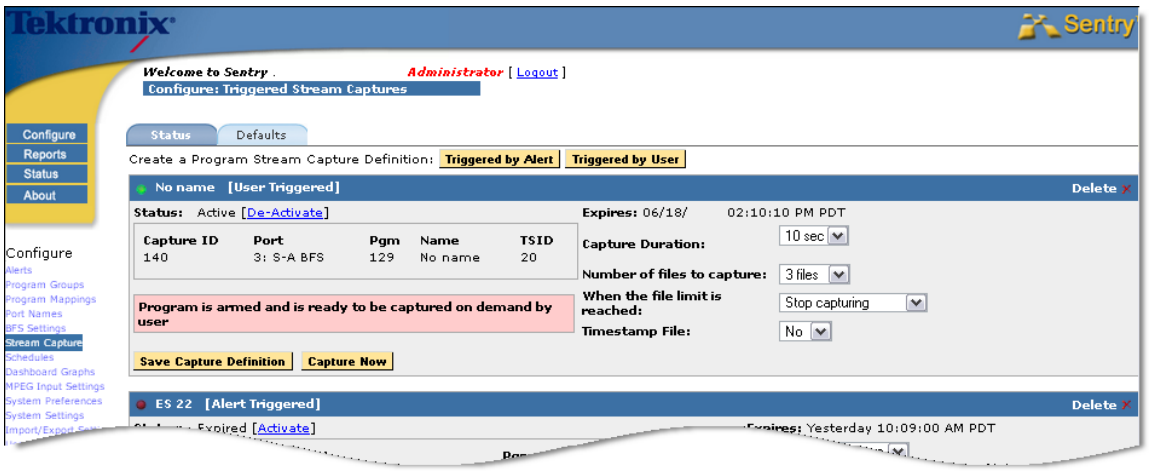


Figure 266: Alert Triggered Stream Captures overview

Access Alert Stream Captures

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

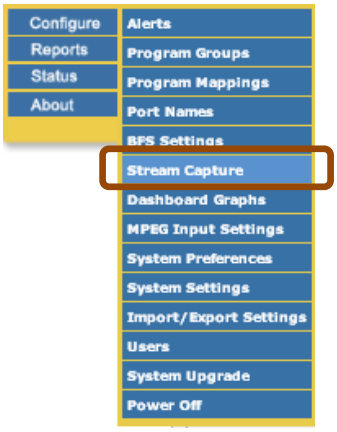


Figure 267: Accessing Stream Captures

Create Alert Stream Captures (When none currently exist)

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

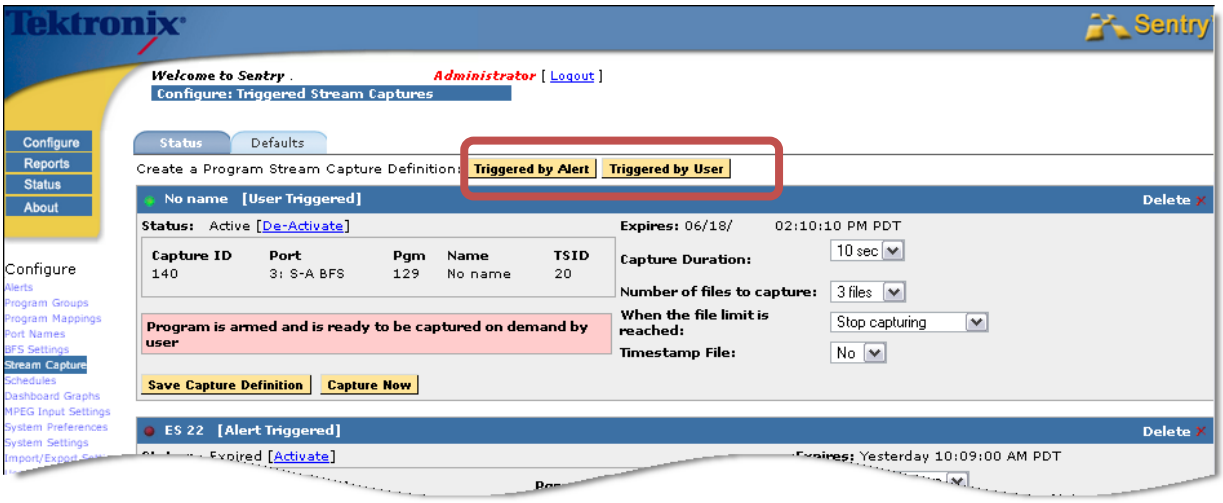


Figure 268: Stream Capture trigger buttons

1) Next, select either **Triggered by Alert** or **Triggered by User**

Triggered by Alert

1) Select a port and a program

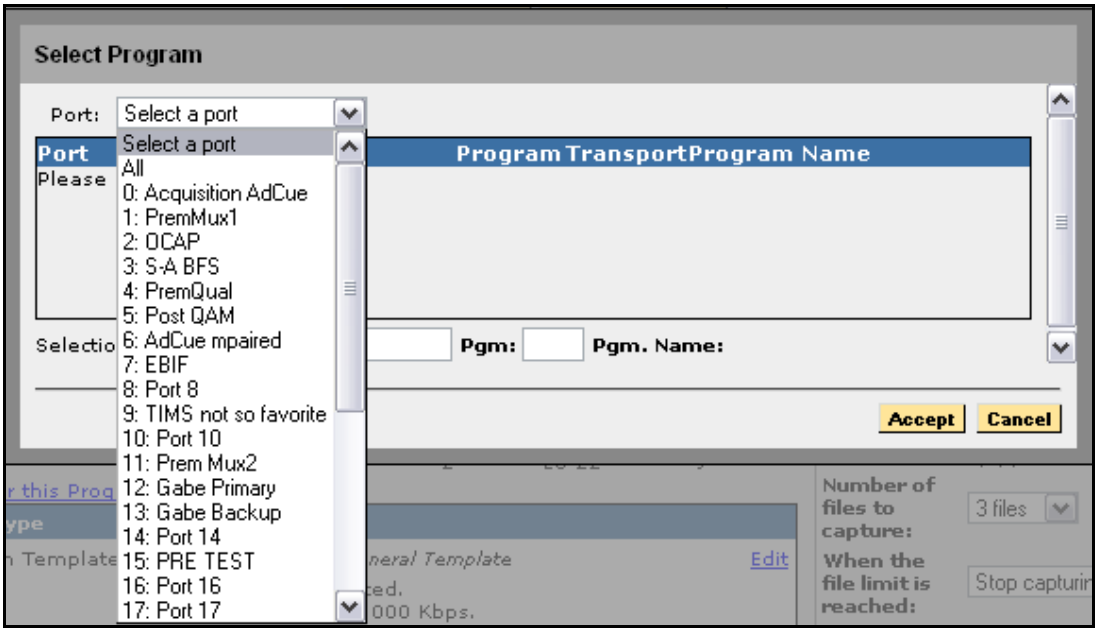


Figure 269: Select a Port

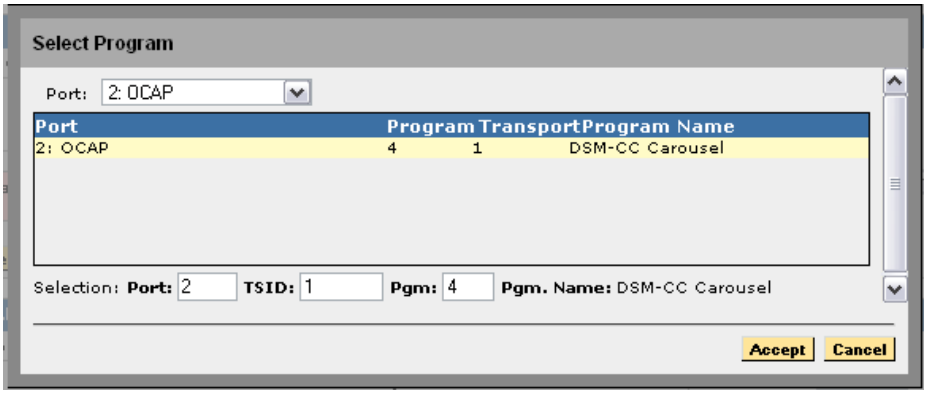


Figure 270: Select a Program

2) Select **Accept**.

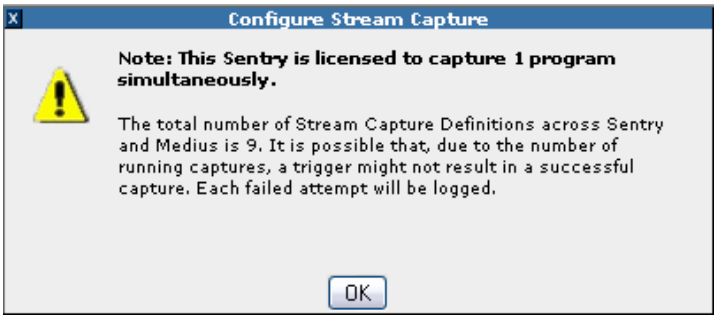


Figure 271: License Notice

3) 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.

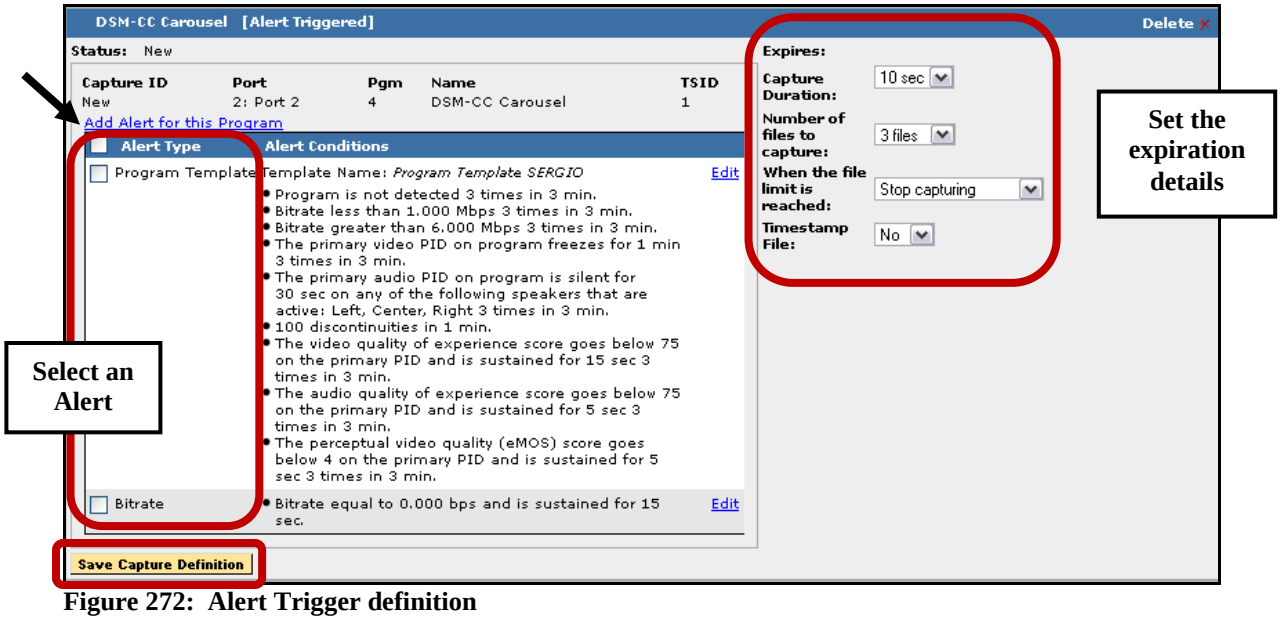


Figure 272: Alert Trigger definition

4) 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

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

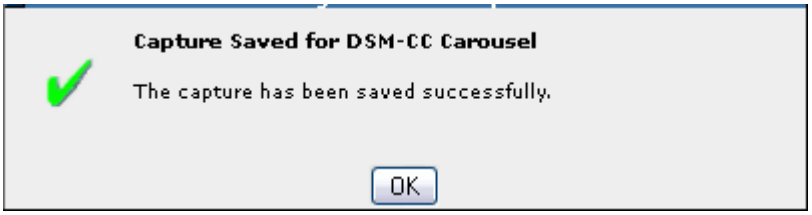


Figure 273: Success dialog box

6) Wait for alerts to trigger.

7) Once the alerts have triggered, return to the bottom of the screen capture page to see the screen captured files

8) Scroll down the page to the bottom and find **Captured Files**.

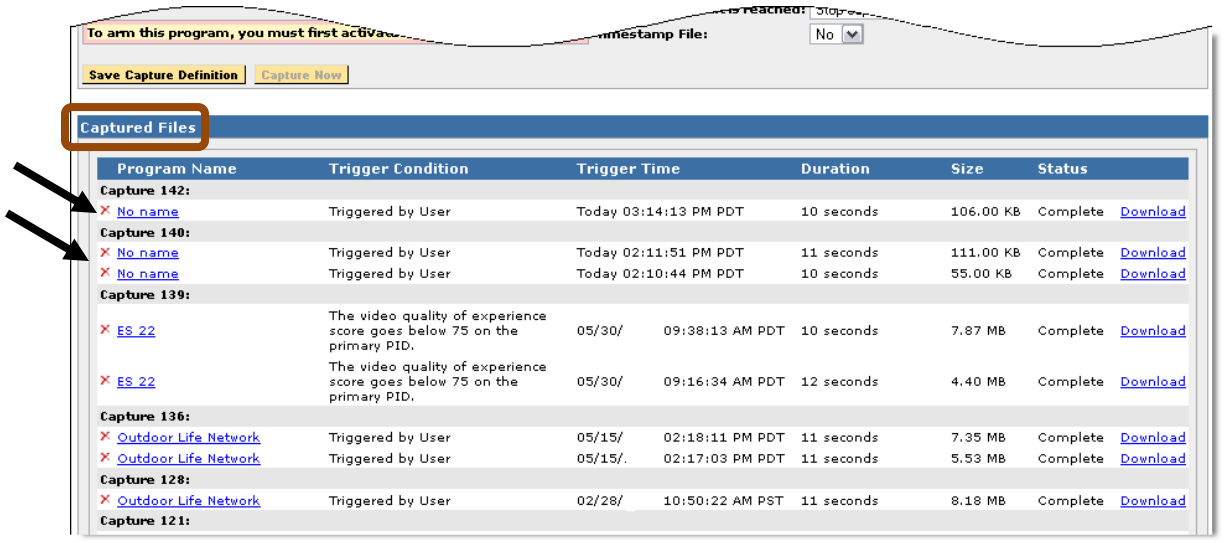


Figure 274: Captured Files

9) Locate the capture that you want to download.

10) Right click on **Download** to save ts file.

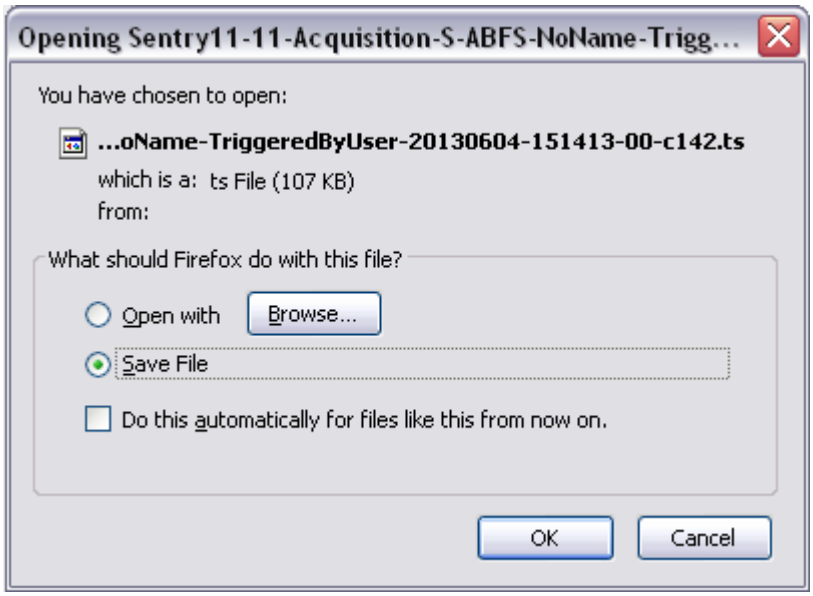


Figure 275: Save File dialog box

Triggered by User

1) Select a port and a program.

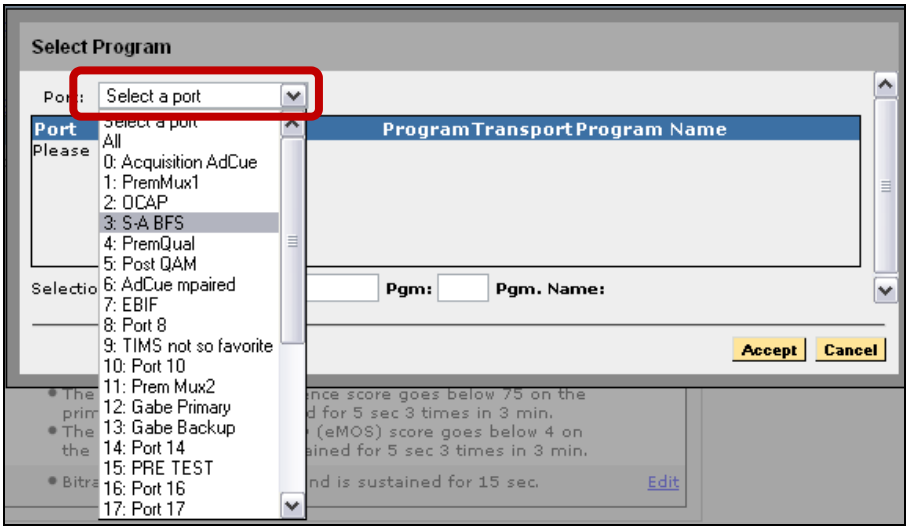


Figure 276: Select a Port

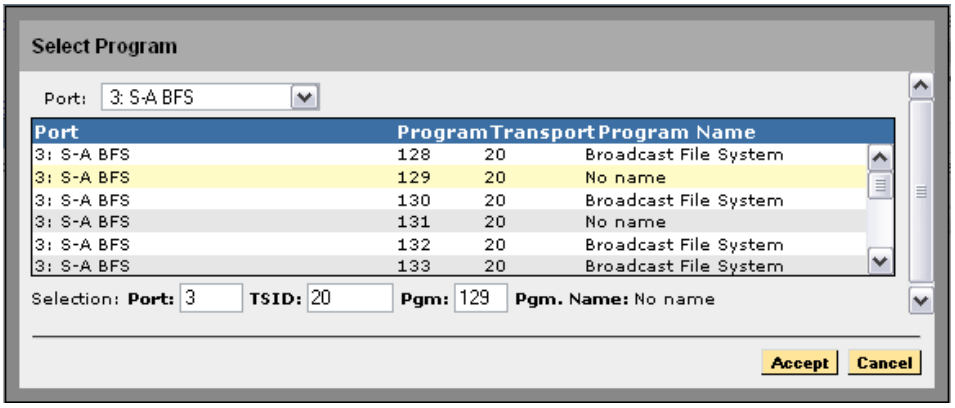


Figure 277: Select a Program

2) Select **Accept**.

3) 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

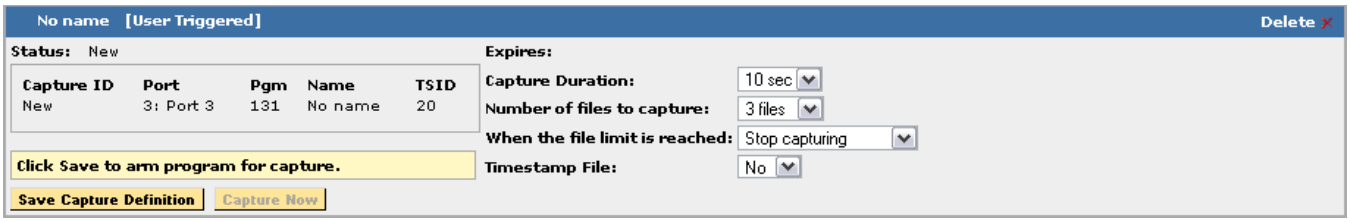


Figure 278: Capture definition

4) Review information and click **Save Capture Definition** when finished.

5) Select **OK** in Confirmation box.

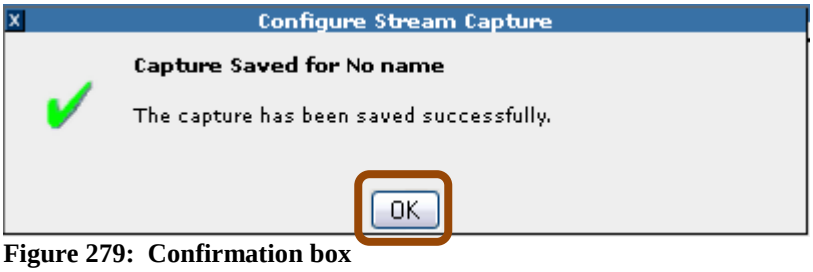


Figure 279: Confirmation box

6) Find the **User Triggered** definition that you just created, and select **Capture Now**.

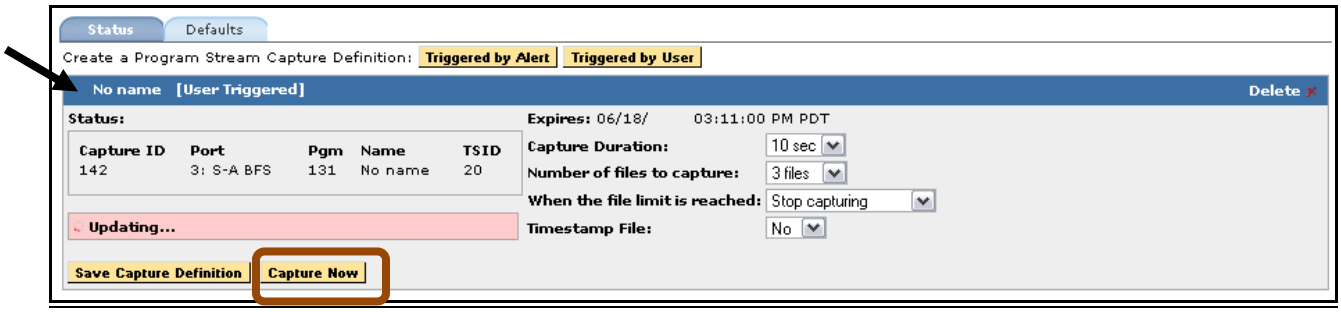


Figure 280: Find the new definition and select Capture Now

7) Scroll down the page to the bottom and find **Captured Files**.

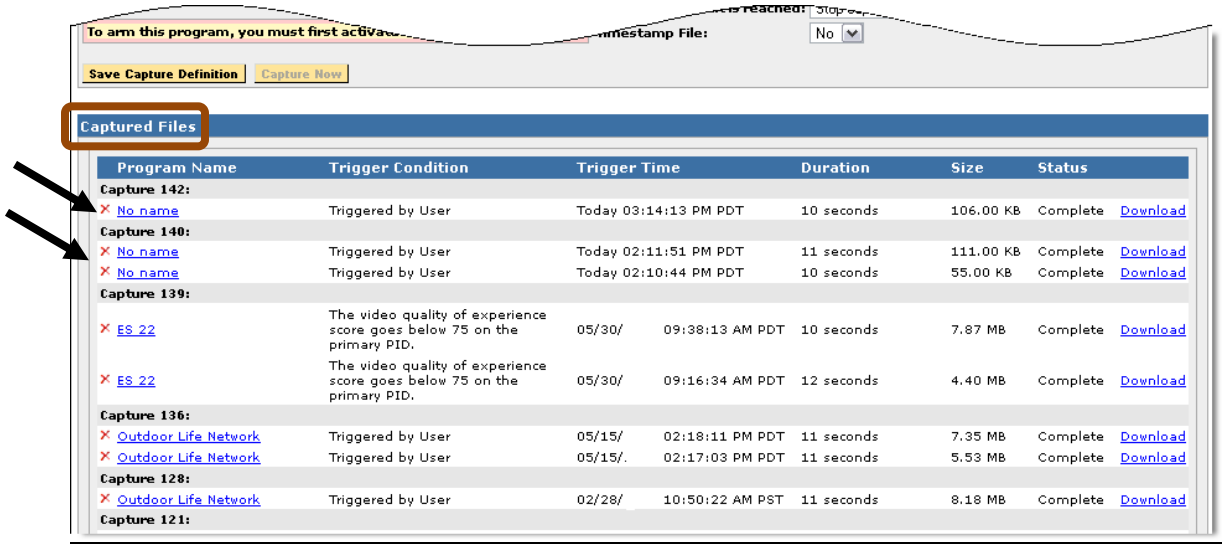


Figure 281: Captured Files

8) Locate the capture that you want to download.

9) Right click on **Download** to save ts file.

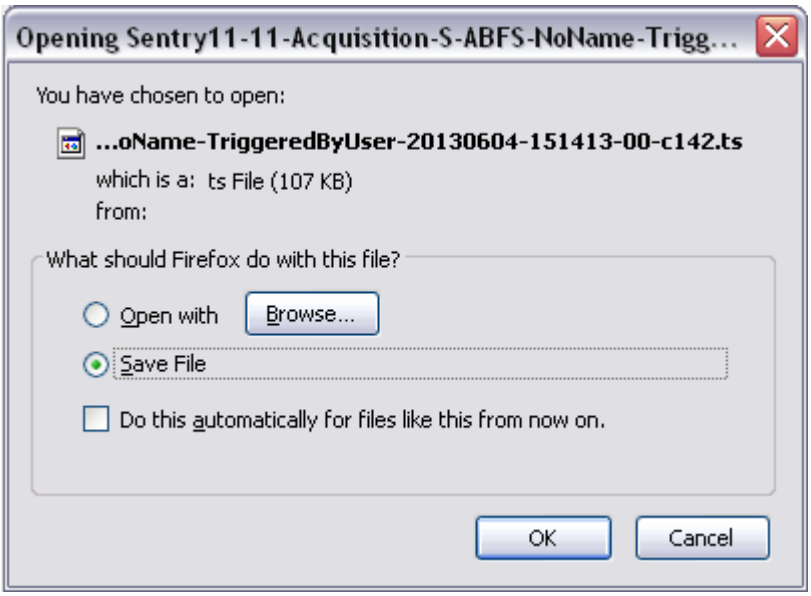


Figure 282: Save File dialog box

Deactivate or Delete 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**.

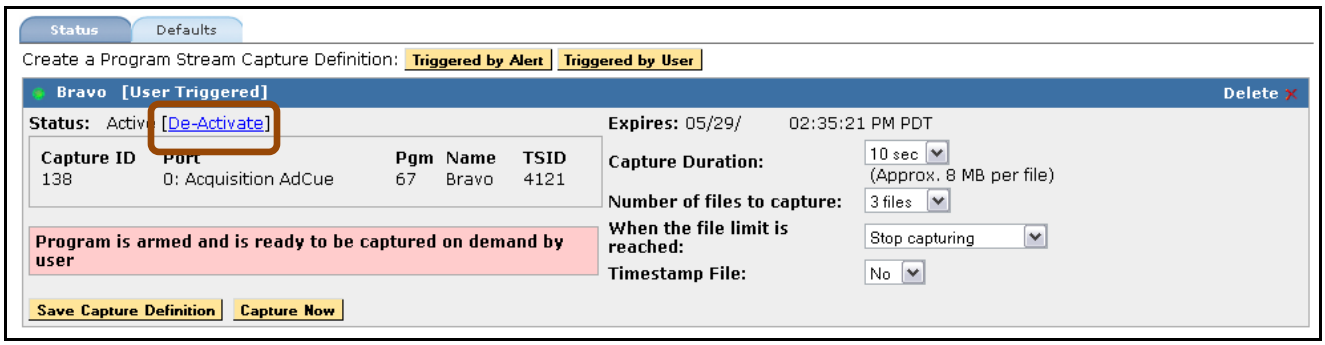


Figure 283: Deactivating a Stream Capture

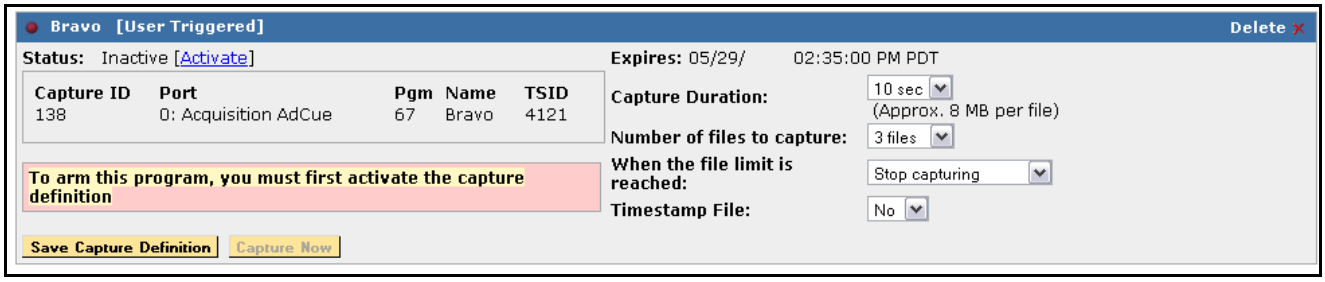


Figure 284: Stream Capture Deactivated

2. 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.

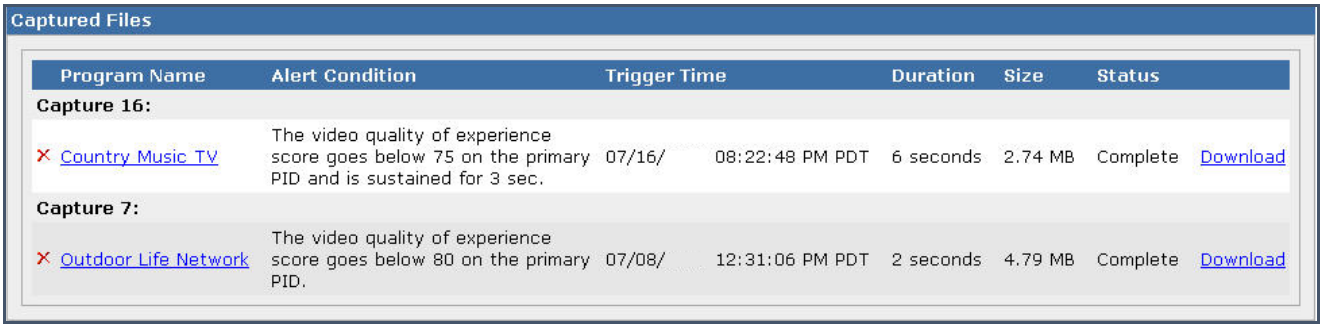


Figure 285: Captured Files

- **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
- **Download link**
  Provides a link to a download of the capture. All captures are saved as transport stream files.

Delete Captured Files

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

Defaults tab

The **Defaults** tab shows all default settings for a new stream capture.

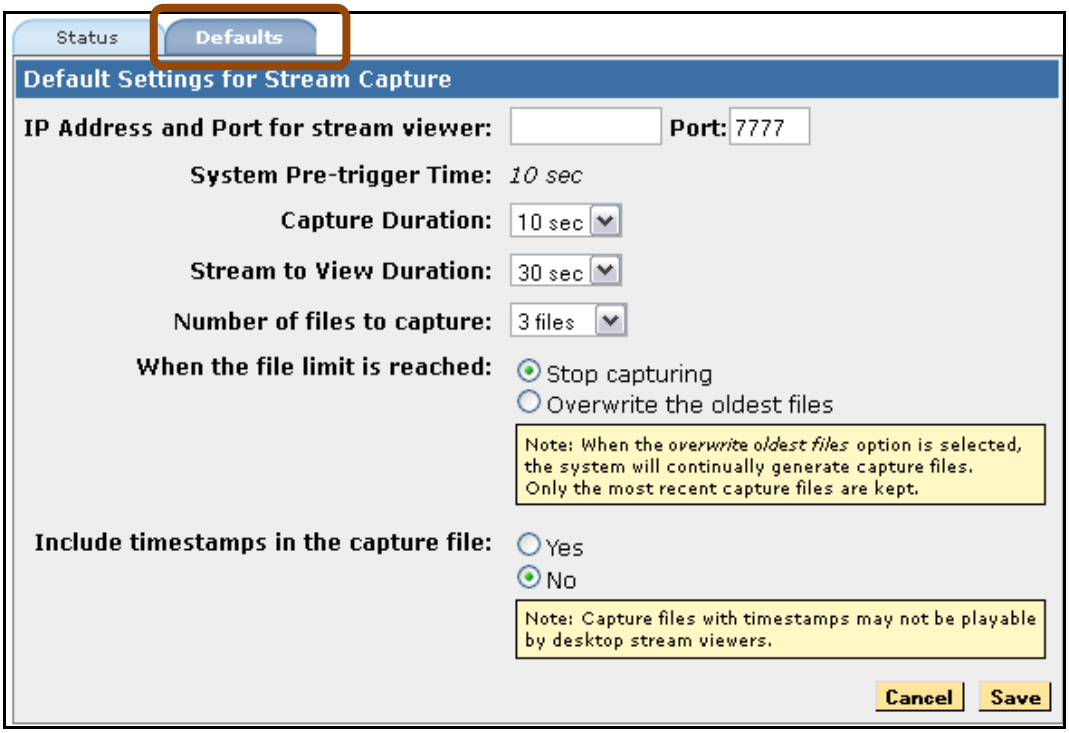


Figure 286: Defaults tab and settings

Configure Triggered Stream Captures(via Nexidia Comply™)

Closed Caption Verification performs an 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 of the verification will then be displayed in the **Data Detect** and **Program Group Data Detect** reports.

Configure 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.

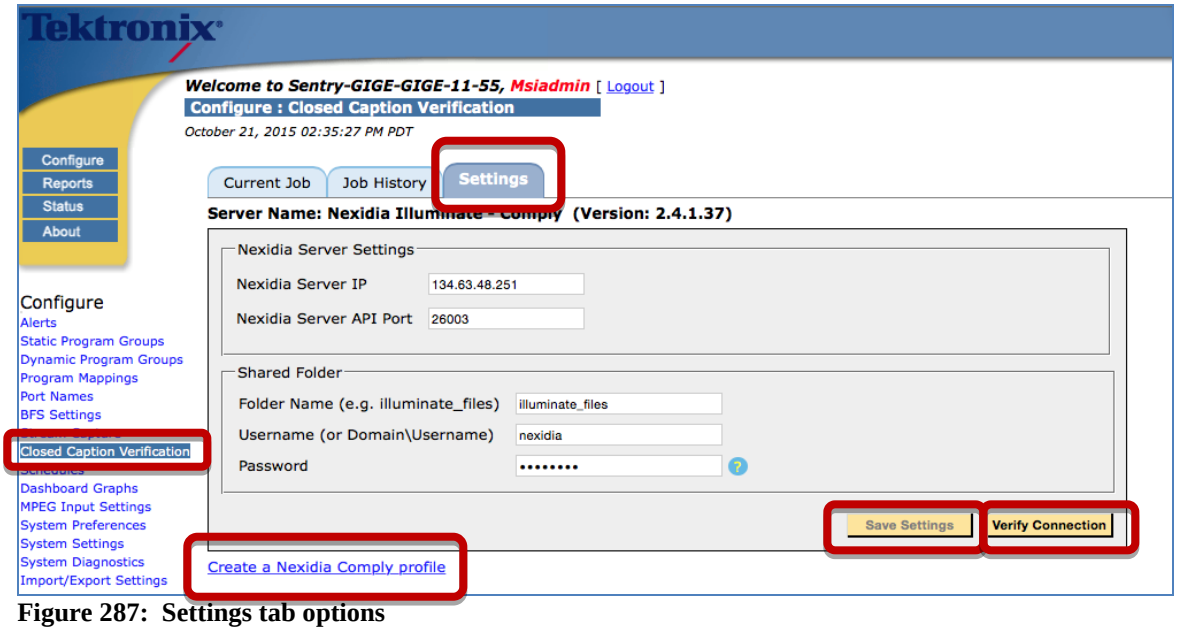


Figure 287: Settings tab options

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 you can perform for the Closed Caption verification.

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

To create a Nexidia profile on the Nexidia server, select **Create a Nexidia Comply Profile** from the **Settings** tab (see above figure).

The resulting page will look similar to the following.

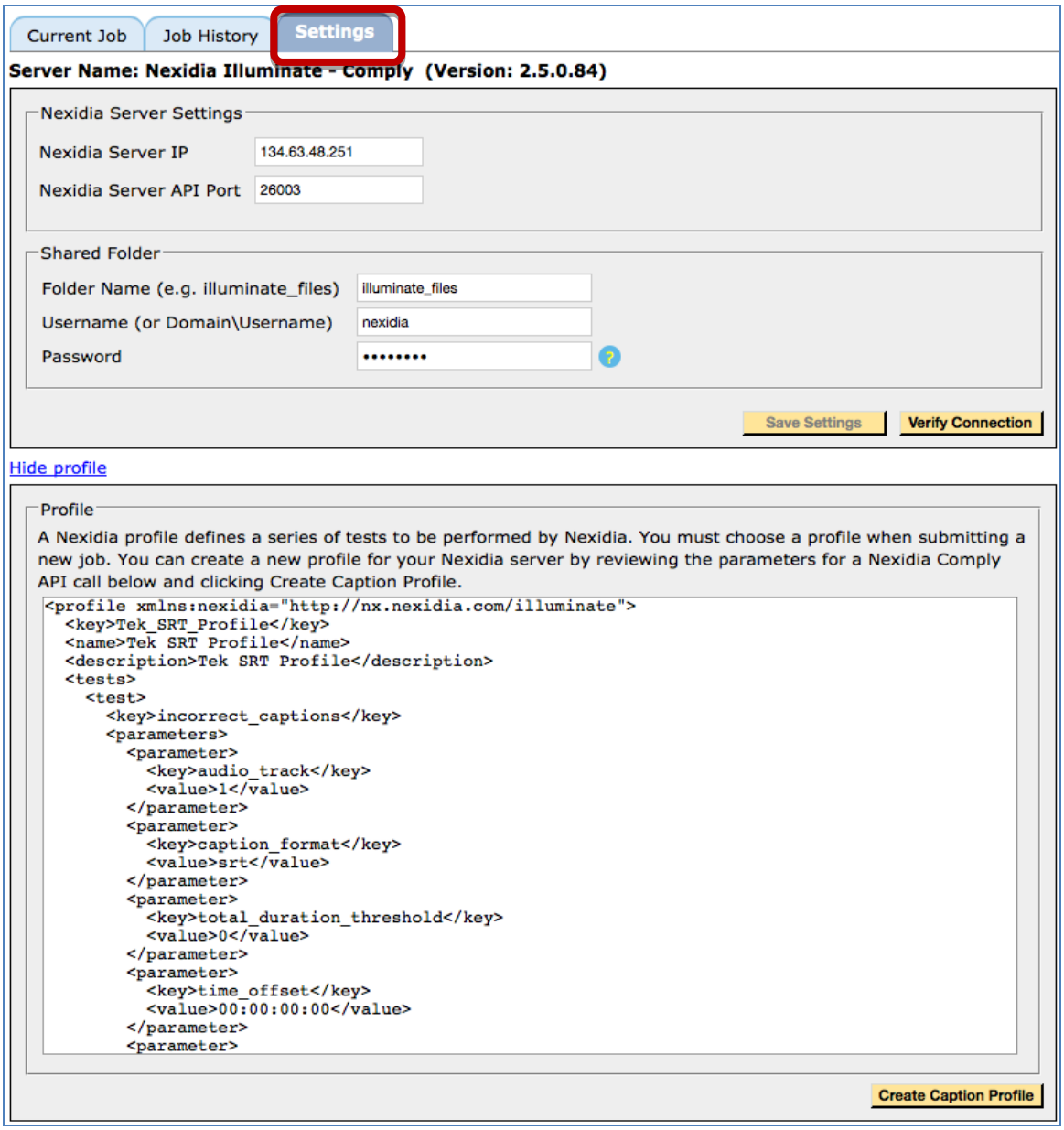


Figure 288: Resulting page after selecting Creating a Nexidia Comply Profile

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, select the **Create Caption Profile** button.

Choose 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.

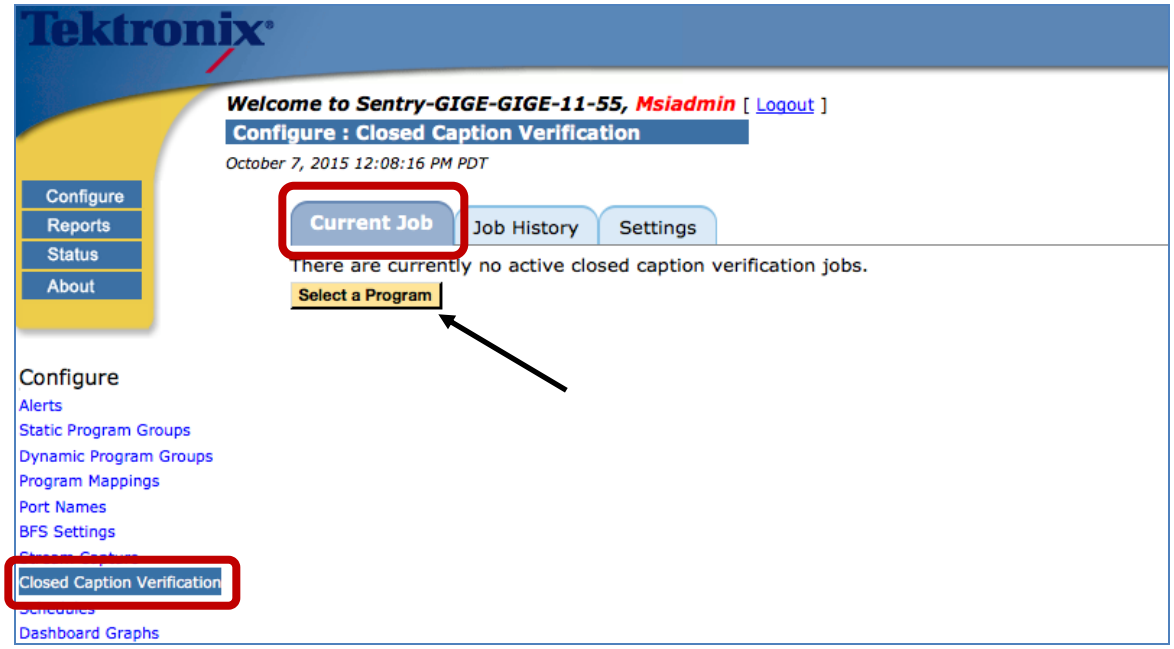


Figure 289: Current Job tab

3. You can configure one program 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**.

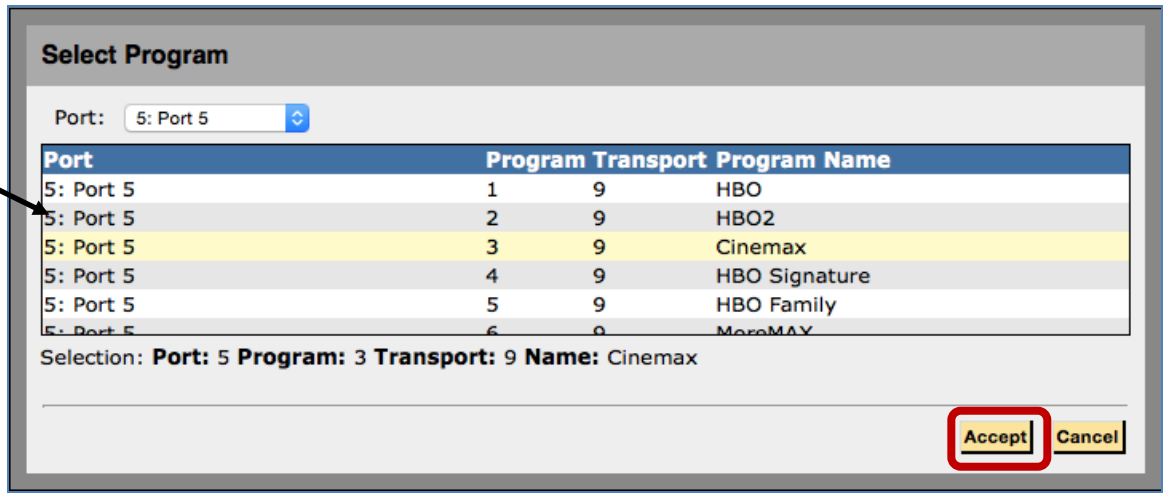


Figure 290: Select Program window

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.

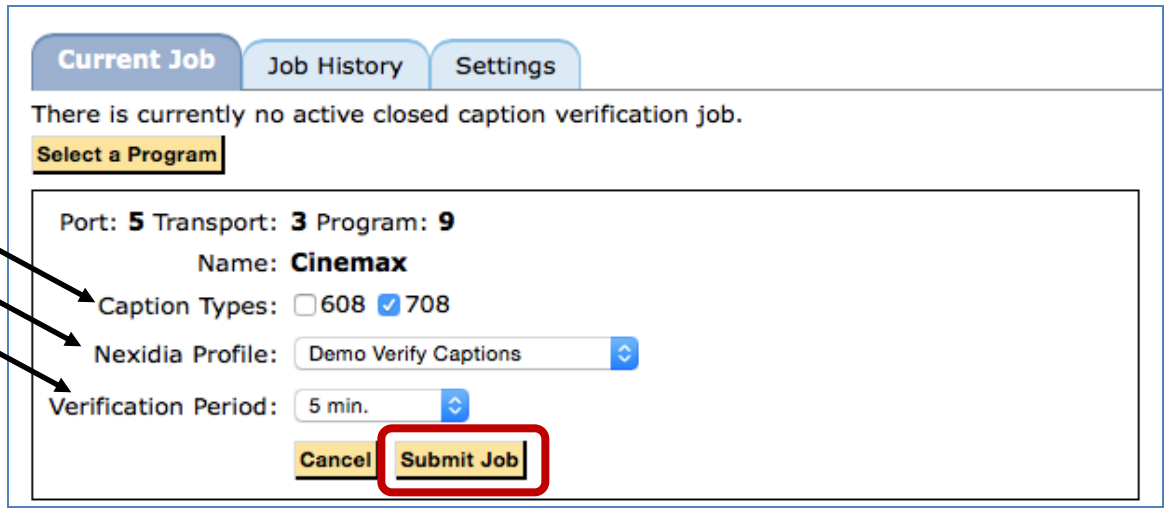


Figure 291: Current Job verification

6. Click **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.

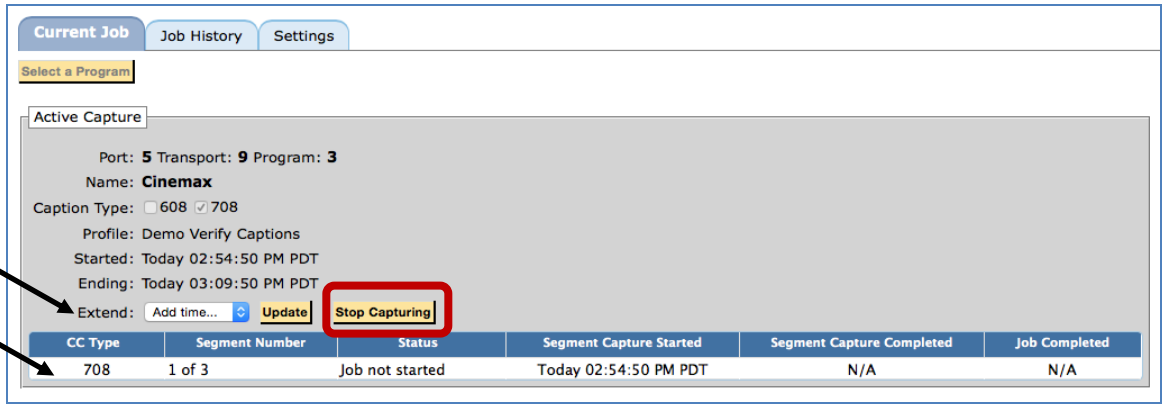


Figure 292: Verification table

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**.

Review Job History

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

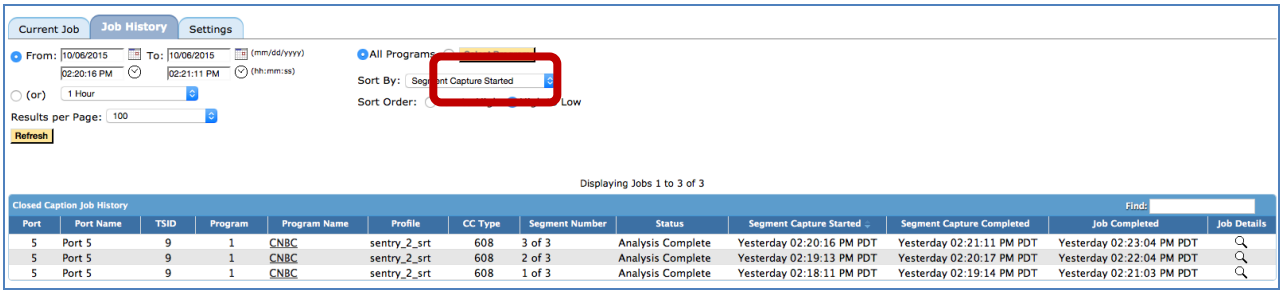


Figure 293: Select Program buttons and capture flows

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.

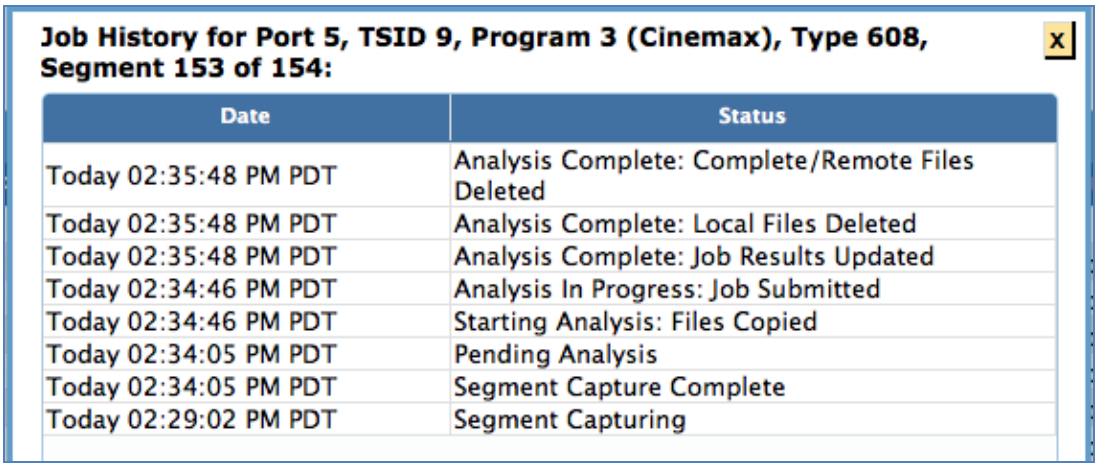


Figure 294: Job Details

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.

Review 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.

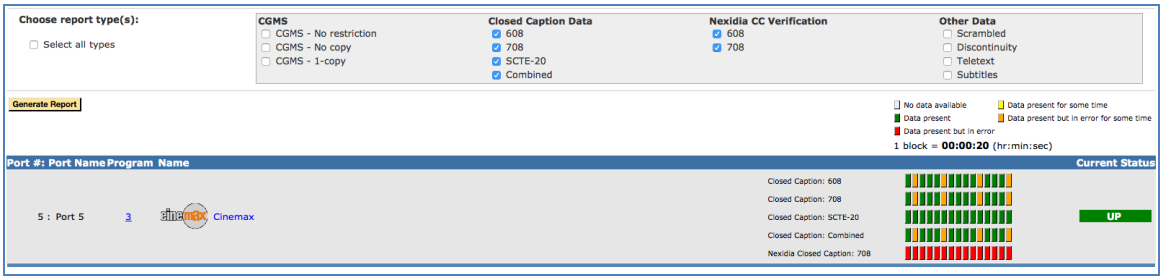


Figure 295: Verification Results

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.

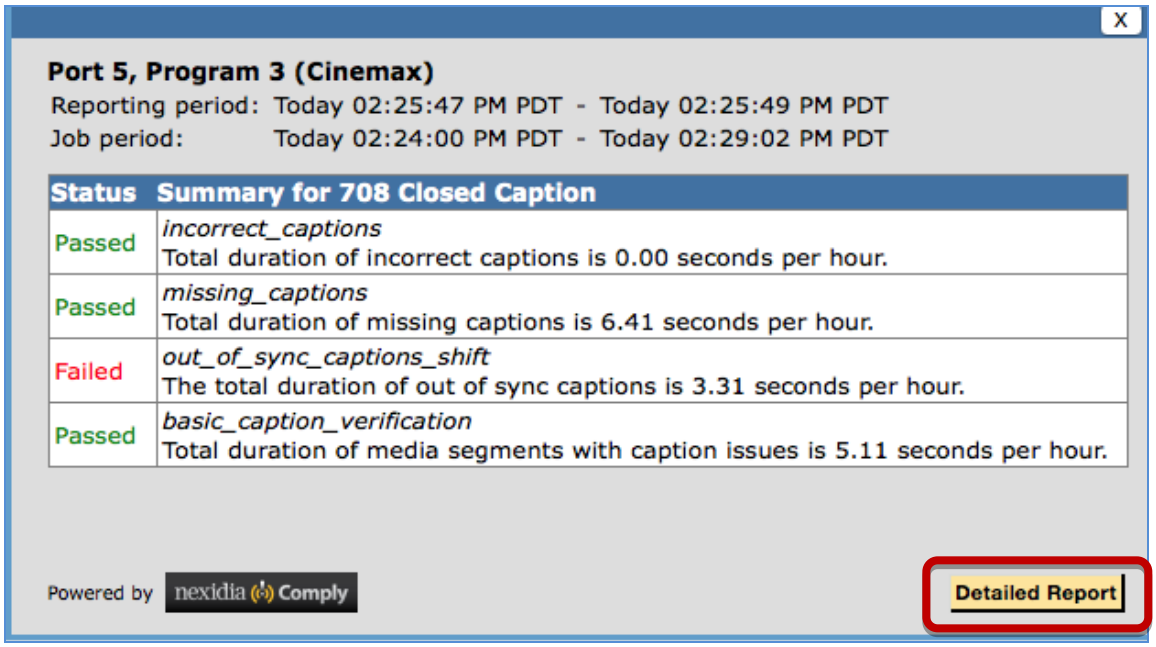


Figure 296: Status Summary

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

Figure 297: Detailed Report

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

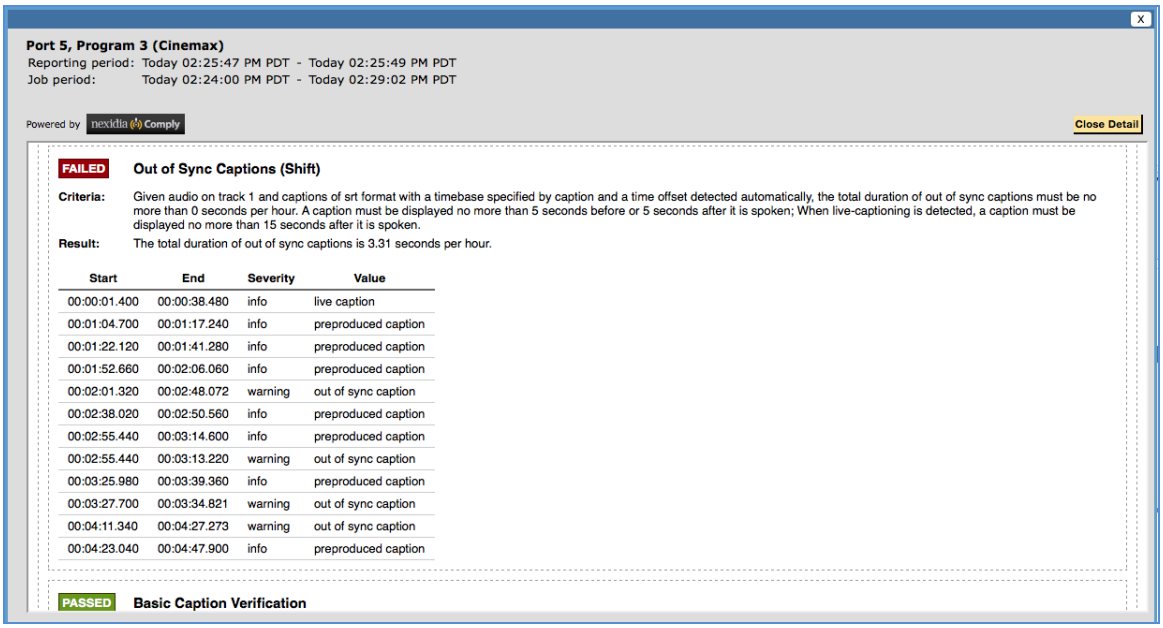


Figure 298: Additional Details

Click **Close Detail** to exit.

Configure Schedules

Configure Schedules allows the user to make schedules to use in the **Program Statistics** report to further limit the time range. You may choose to limit by either **Daily** or **Weekly** schedules.

- **Daily** allows you to choose a time range to run every day.
- **Weekly** allows you to choose the days and the times for the reports.

To access, select **Configure** from the main menu and then choose **Schedules**.

Create a Daily schedule

1. Select **Create**.

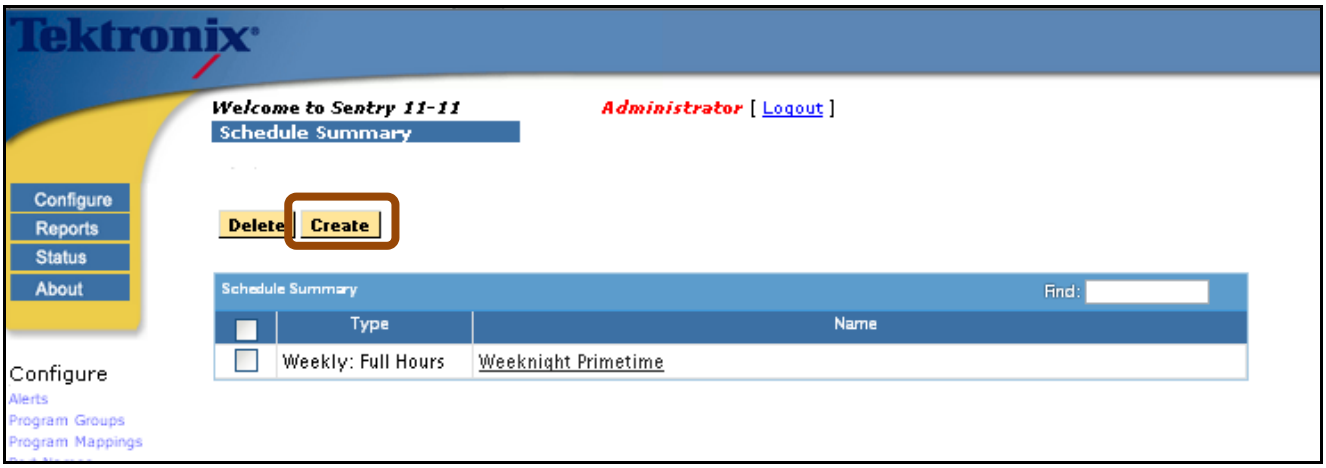


Figure 299: Schedule Summary Create button

2. Select **Daily: Full Hours** from the **Schedule Type** drop down menu.

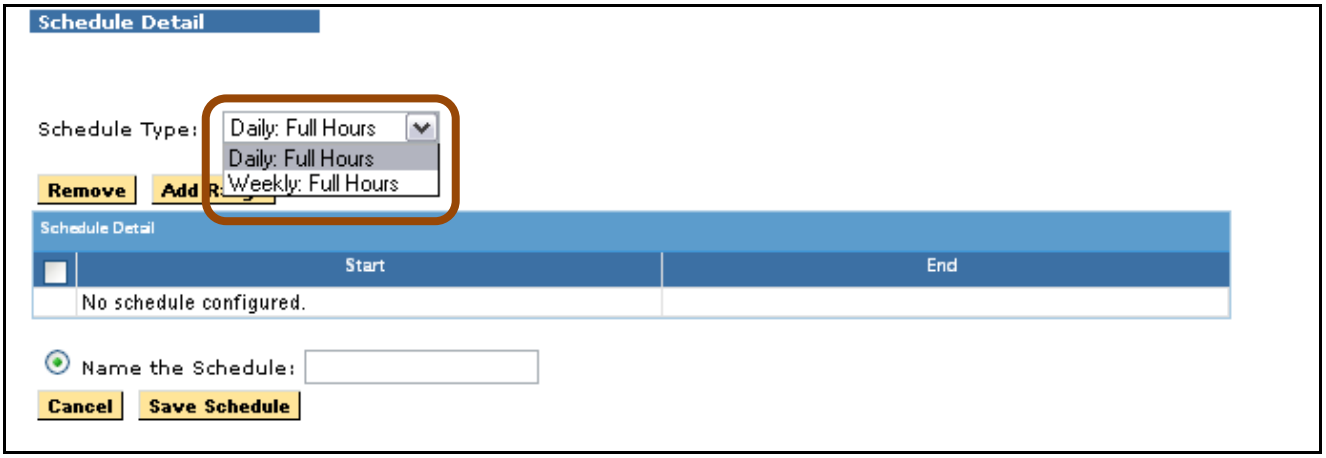


Figure 300: Select Daily: Full Hours

3. Select **Add Range**.

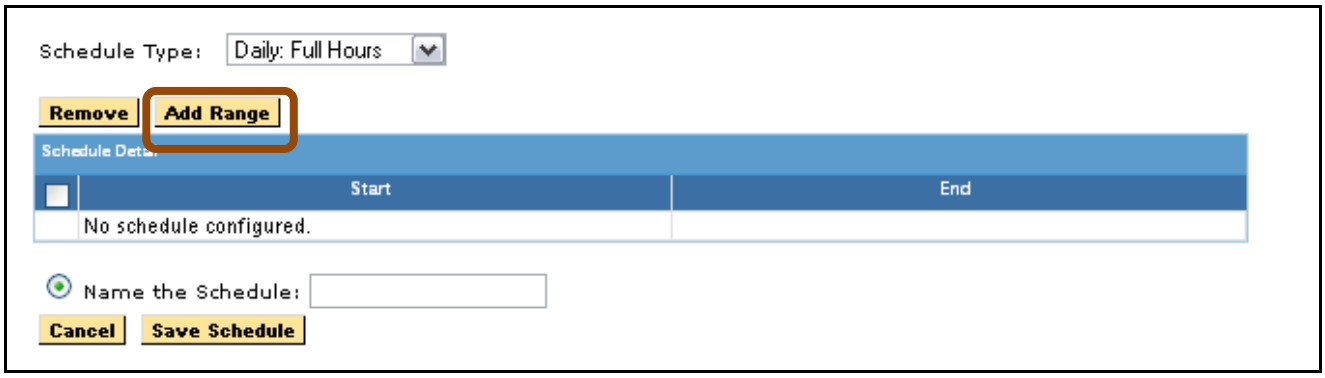


Figure 301: Add Range

4. Select your start and end time and select **Apply**. Then select **Add.**

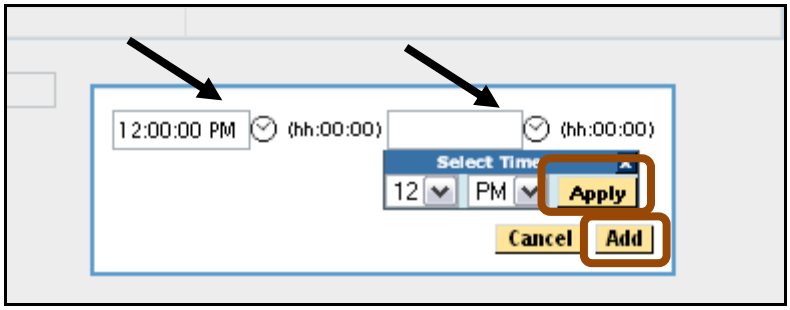


Figure 302: Start and end times

5. Repeat steps 3 and 4 as needed.
6. Select the box under **Schedule Detail**.
7. Name the schedule and select **Save Schedule**.

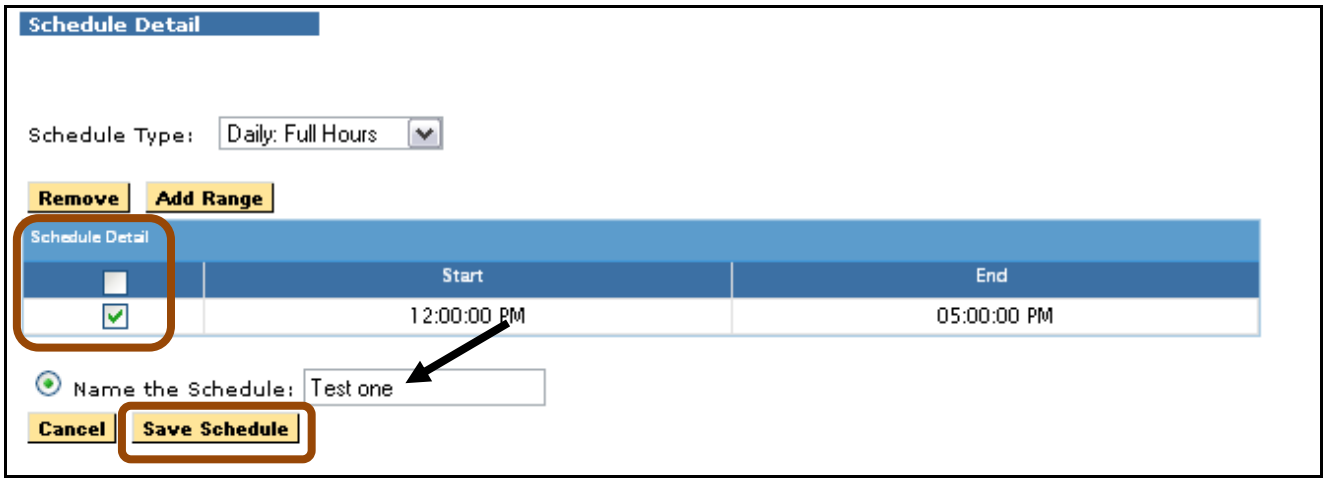


Figure 303: Schedule Detail, Name and Save Schedule

8. The new schedule will now show on the **Schedule Summary page** and on the menu for **Program Statistics** reports.

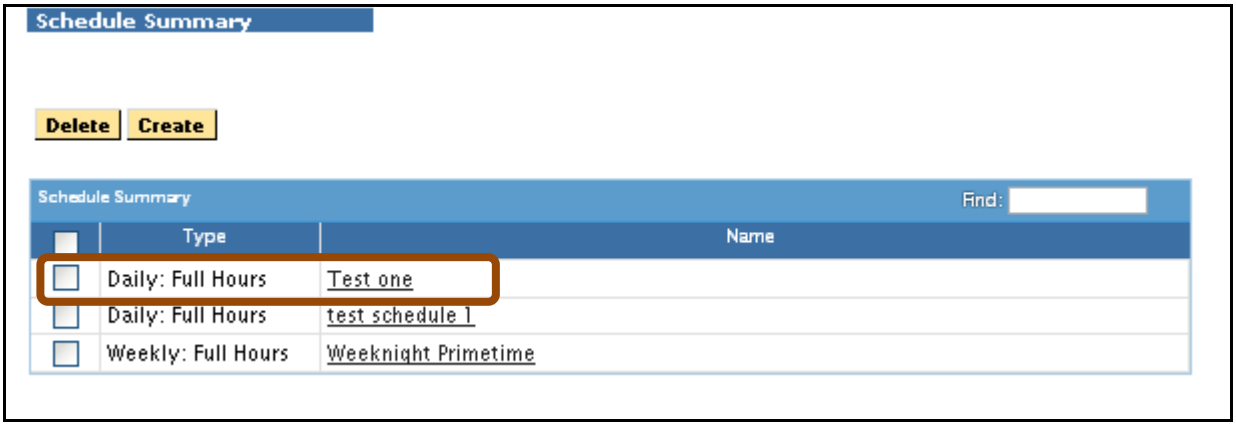


Figure 304: The new schedule

9. Repeat as needed.

Create a Weekly Schedule

1. Select **Create**.

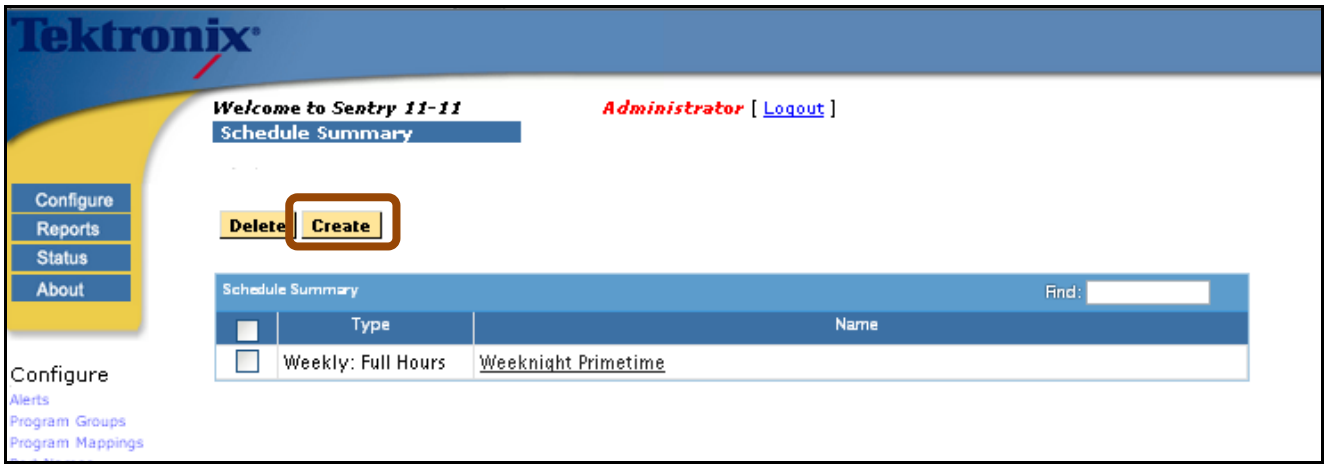


Figure 305: Create

2. Select **Weekly: Full Hours** from the **Schedule Type** drop down.

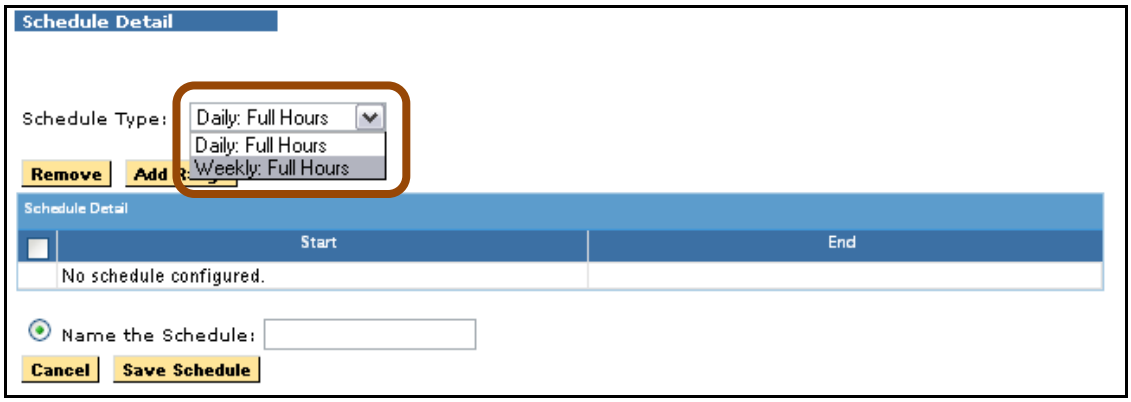


Figure 306: Drop down menu for Weekly: Full Hours

3. Select **Add Range**

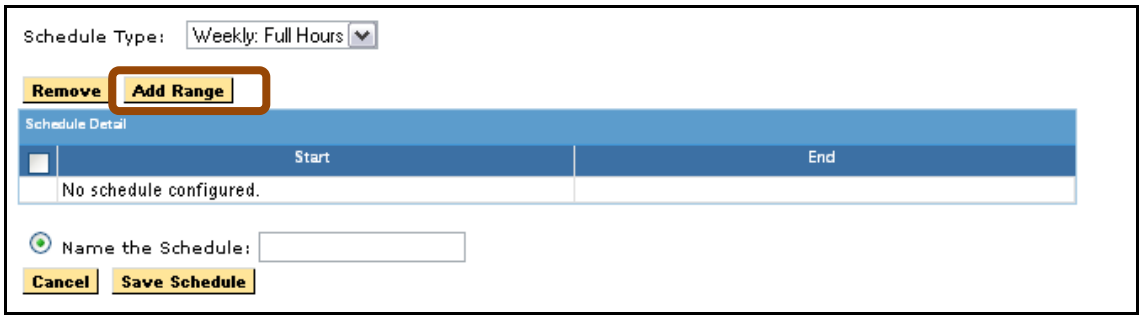


Figure 307: Add Range

4. Select the days of the week for your range.

5. Select the time period for each day and select **Apply** to each time period

6. Select **Add** when done.

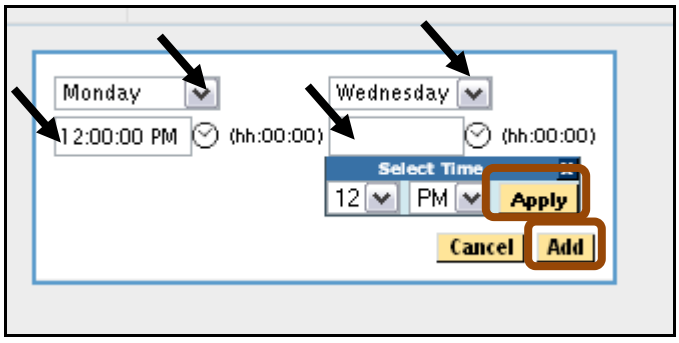


Figure 308: Days and Times

7. Repeat steps 3-6 as needed.
8. Select the box under **Schedule Detail**.
9. Name the schedule and select **Save Schedule**.
10. The new schedule will now show on the **Schedule Summary page** and on the menu for **Program Statistics** report.

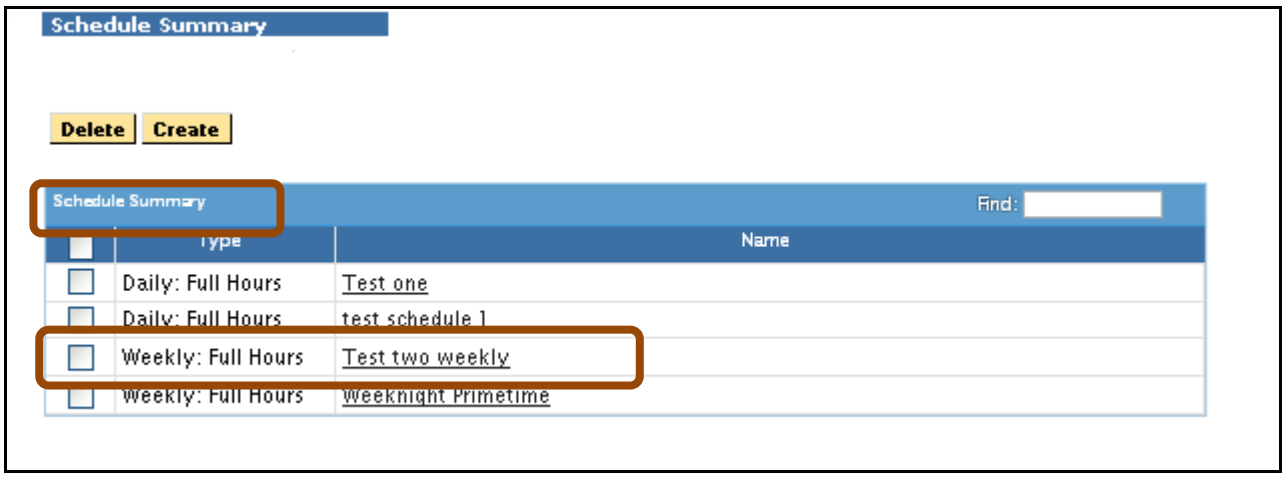


Figure 309: Newly Created Schedule

11. Repeat as needed.

Dashboard Graphs

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

You have two options for creating a Dashboard display:

- **Private Program Dashboard Graphs** are only visible to you
- **Public Program Dashboard Graphs** are available for use by other users

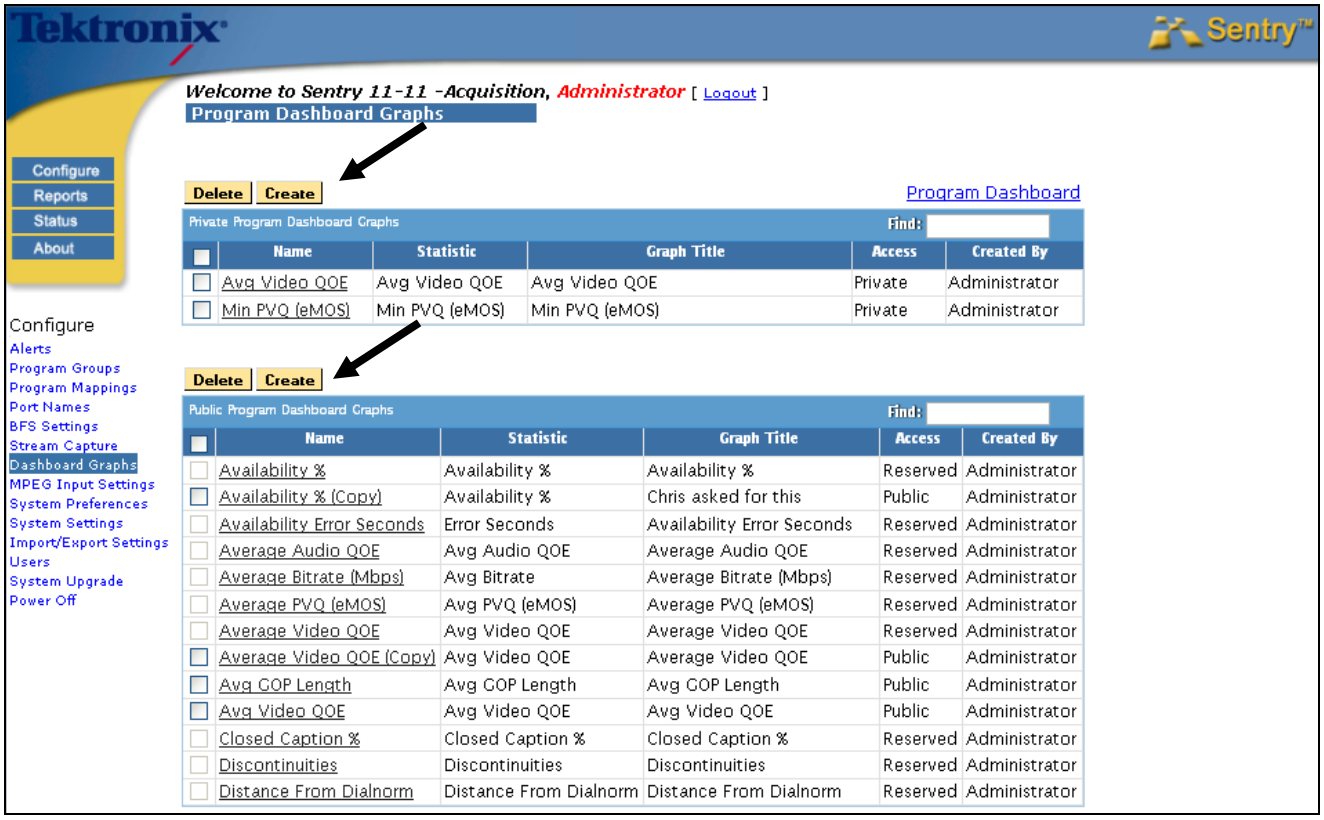


Figure 310: Program Dashboard Graphs

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**.

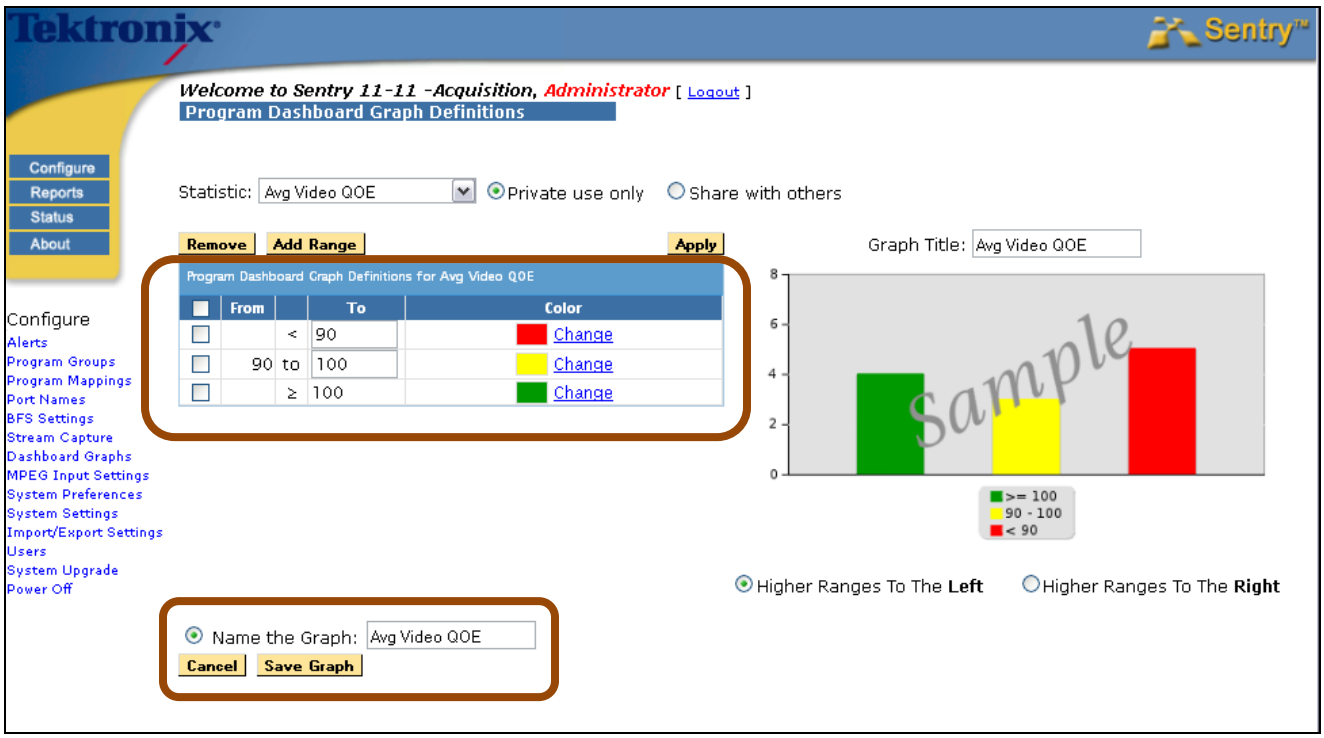


Figure 311: Creating Dashboard Graphs

Configure 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.

IGMP v3 SSM Support

The **Internet Group Management Protocol (IGMP)** is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships.

Source Specific Multicast (SSM) was designed specifically to support IGMP v3 and is fully backward compatible with earlier versions.

Access MPEG Input System Settings

1. Select **MPEG Input System Settings** from the main menu

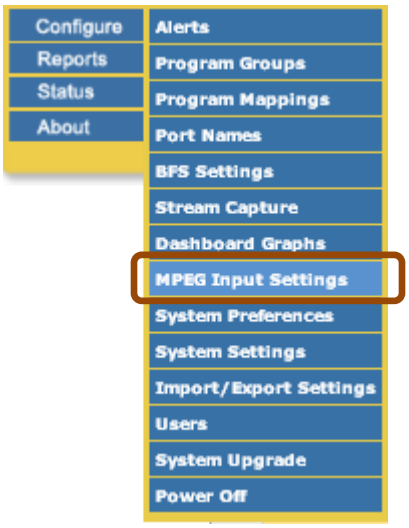


Figure 312: Selecting MPEG Input

2. Adjust settings as needed.
3. Select **Save Settings**.

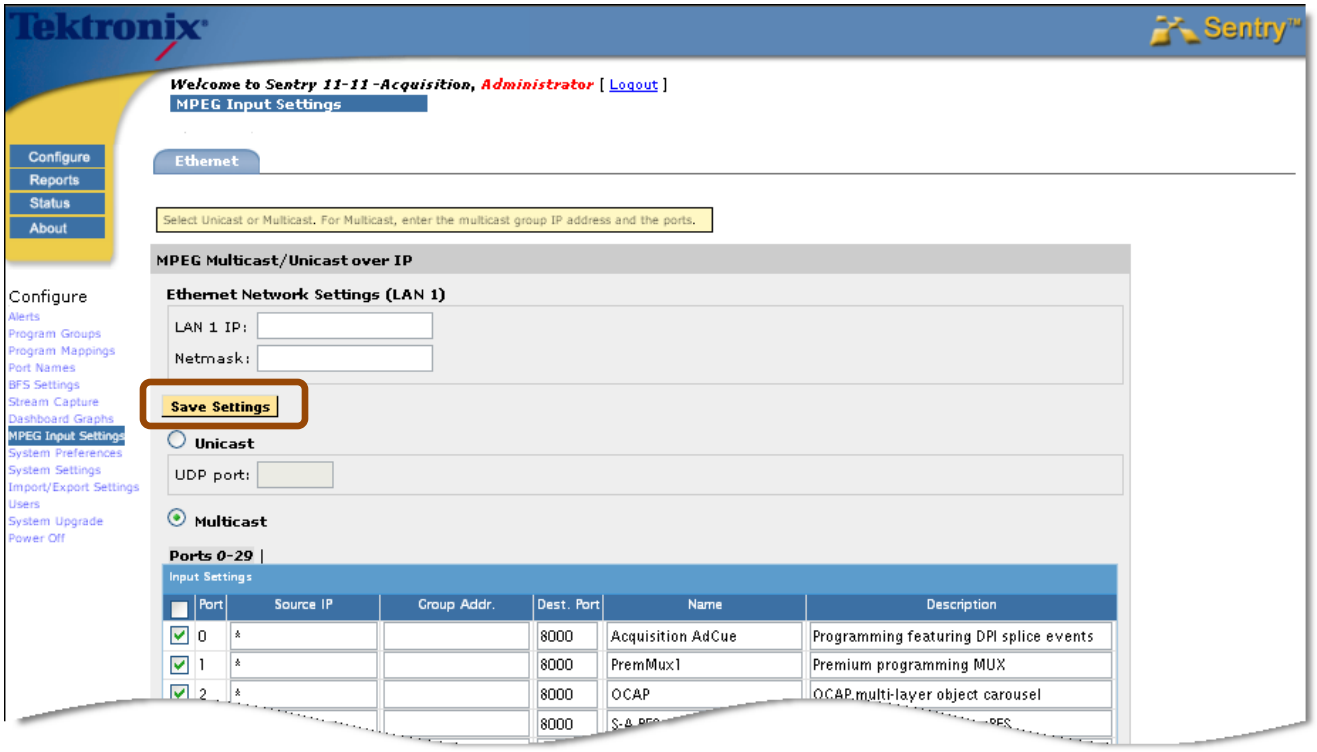


Figure 313: MPEG over IP with Multicast

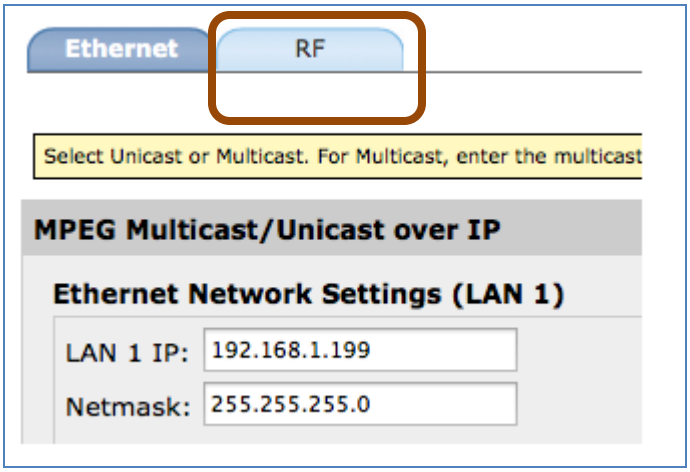


Figure 314: tabs with RF settings option

Set SSM

SSM is set to default with a *****. If you are using SSM, enter your source IP address for the **Multicast** in the **source IP** field. If you do not wish to use this feature, enter a ***** or leave it at the default setting.

NOTE*: SSM applies only to Multicast.*

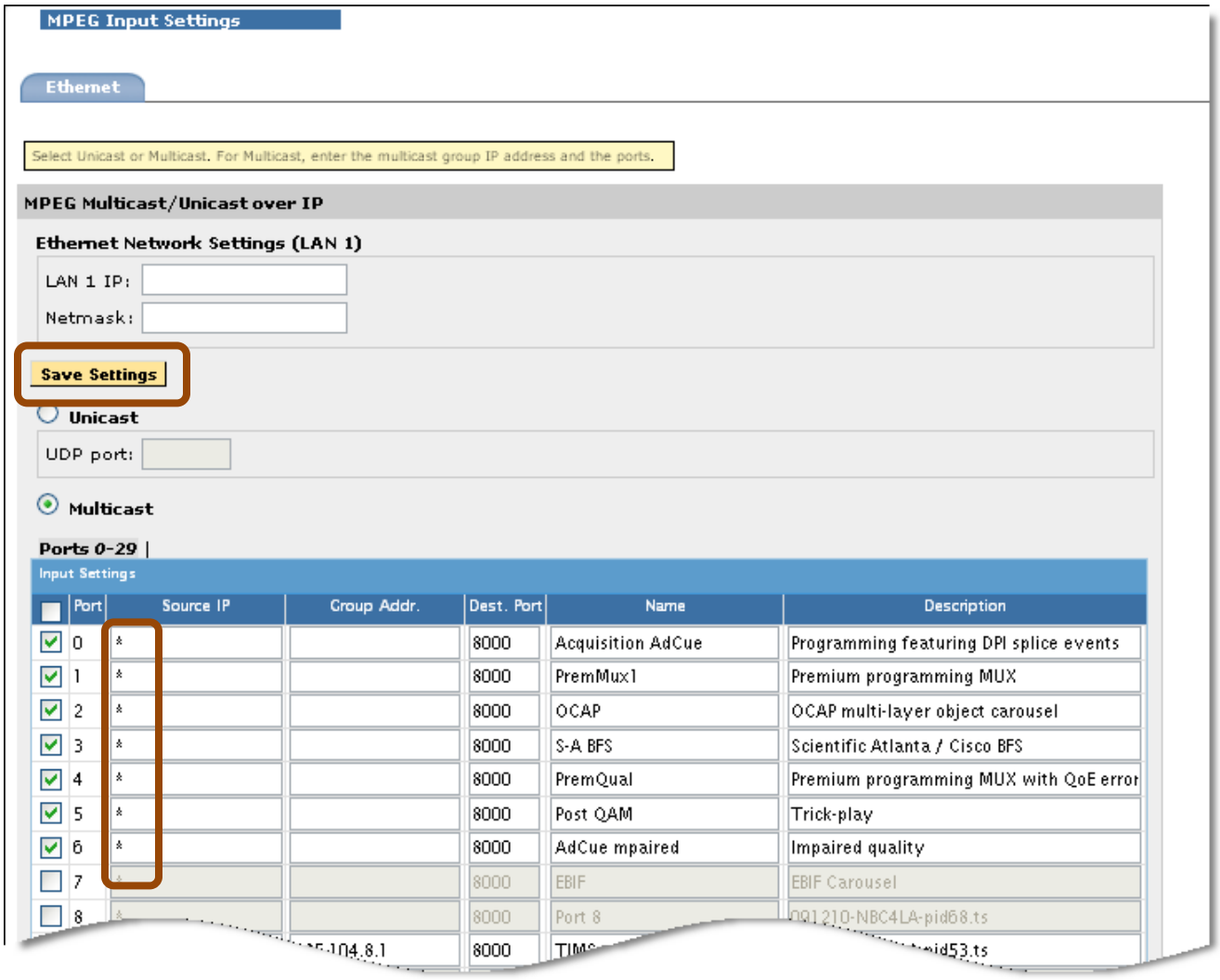


Figure 315: MPEG Input

After making the required changes, select **Save Settings**.

Multicast Stream Collision Errors (Multiple Sources Detected on Input Ports)

In the event that multiple sources are sending data using the same multicast address and port, the Sentry will display a banner telling the user that there are multicast collisions on the specified port(s).

If this occurs, disable the specified port, or edit the configuration to specify a specific port.

Figure 316: Multicast stream collision error type 1

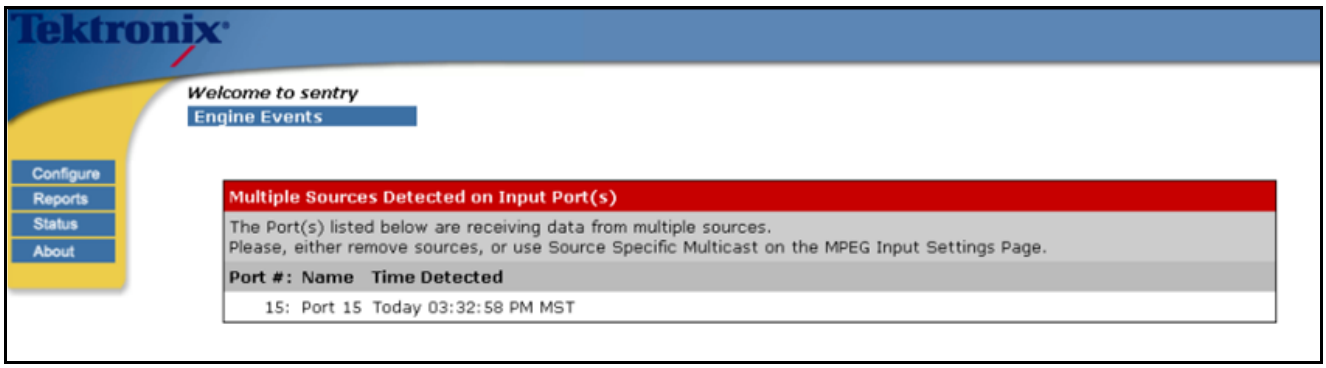


Figure 317: Multicast stream collision error type 2

Sentry with 2nd MPEG Input Option Installed

Configuring the **MPEG Input Settings** is slightly different if the Sentry unit has two network interfaces for MPEG monitoring. This difference allows for monitoring two networks, increased overall throughput and/or monitoring both primary and redundant transport streams.

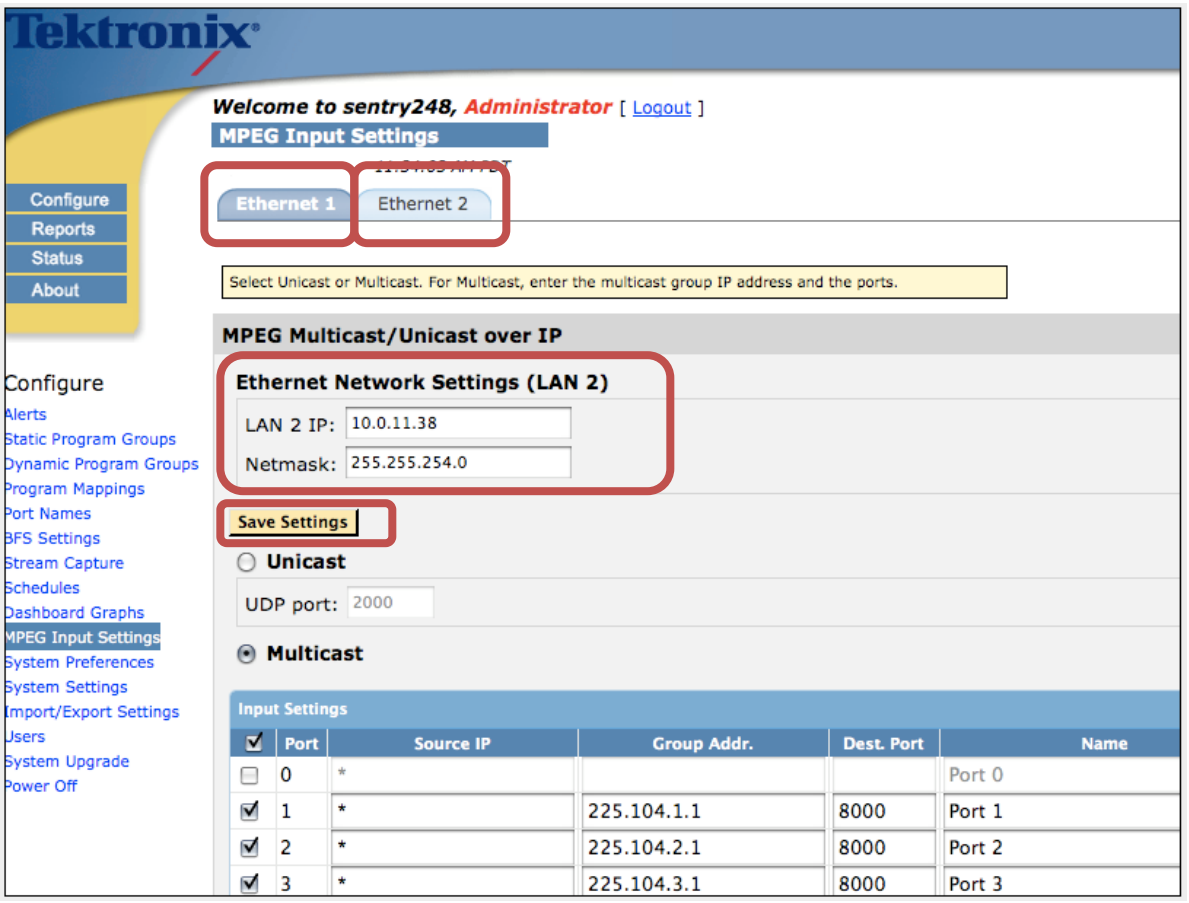


Figure 318: MPEG Input Settings

If the Sentry has the second MPEG input option installed, there will be two copper network interfaces directly on the box for MPEG monitoring. Therefore, configuration of MPEG inputs has some additional options.

In the **Configure MPEG Settings** there are two tabs, one for each network interface.

1. Select the interface you want to work with by clicking on the tab.
2. Next, change the **IP address**, **Netmask** and **Unicast** settings if needed.
3. Select **Save Settings** when done.

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.

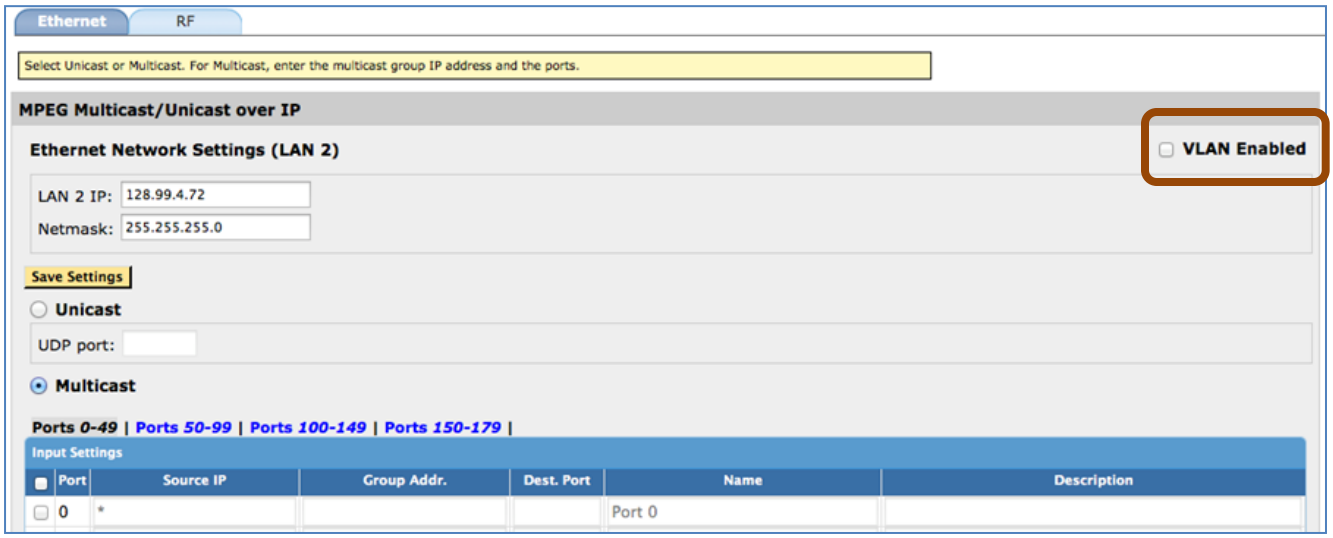


Figure 319: Sentry with VLAN Enabled support

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:

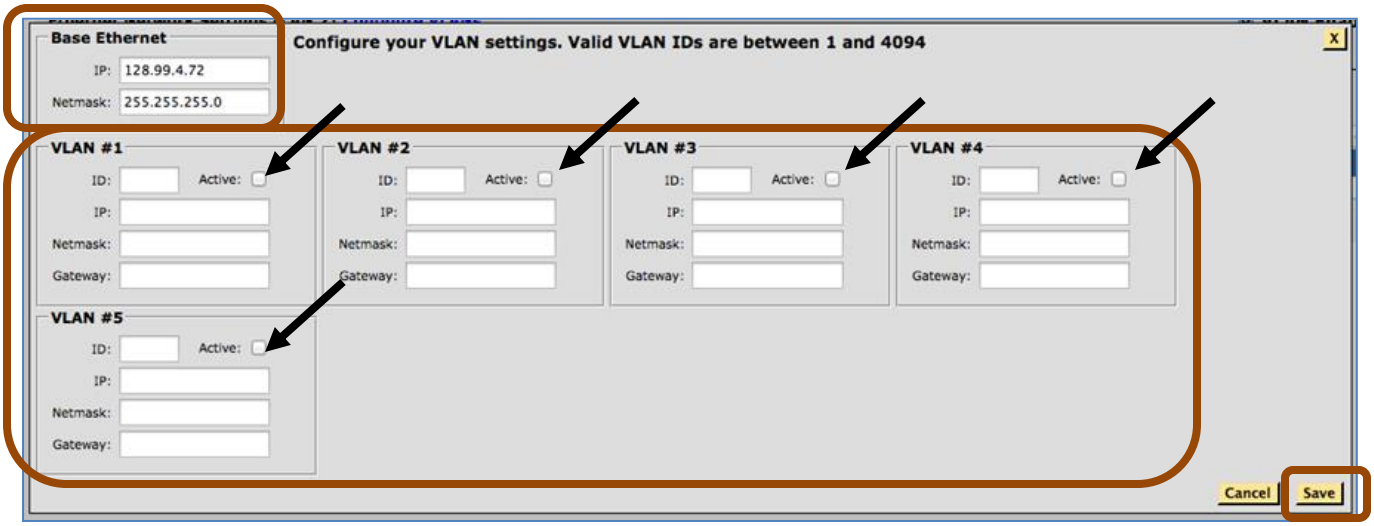


Figure 320: Configure VLAN settings

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 deactivate 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.

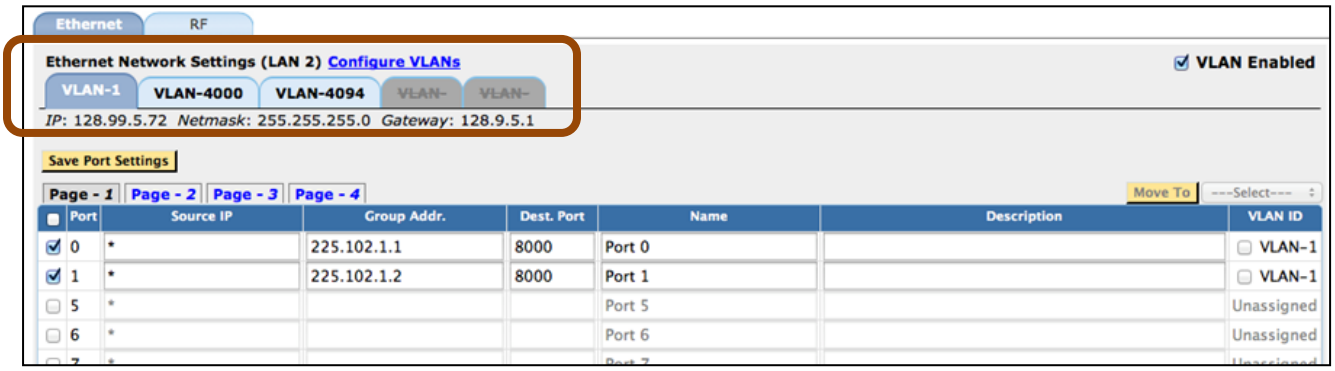


Figure 321: Newly created VLAN tabs

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:

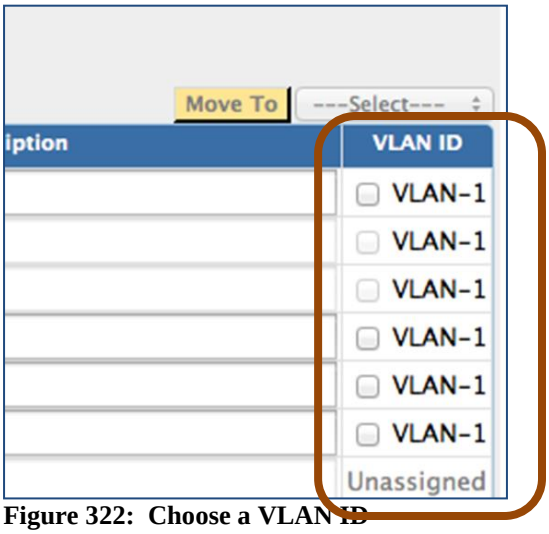


Figure 322: Choose a VLAN ID

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

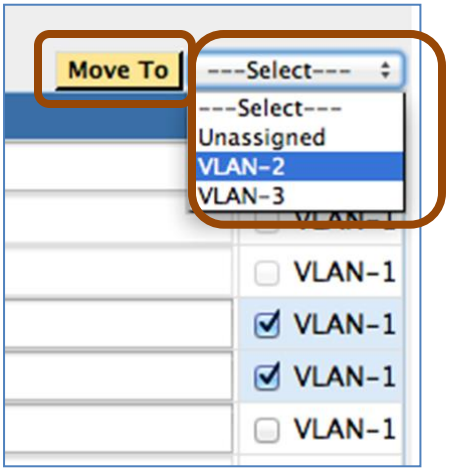


Figure 323: Select a VLAN to move selected items to

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.

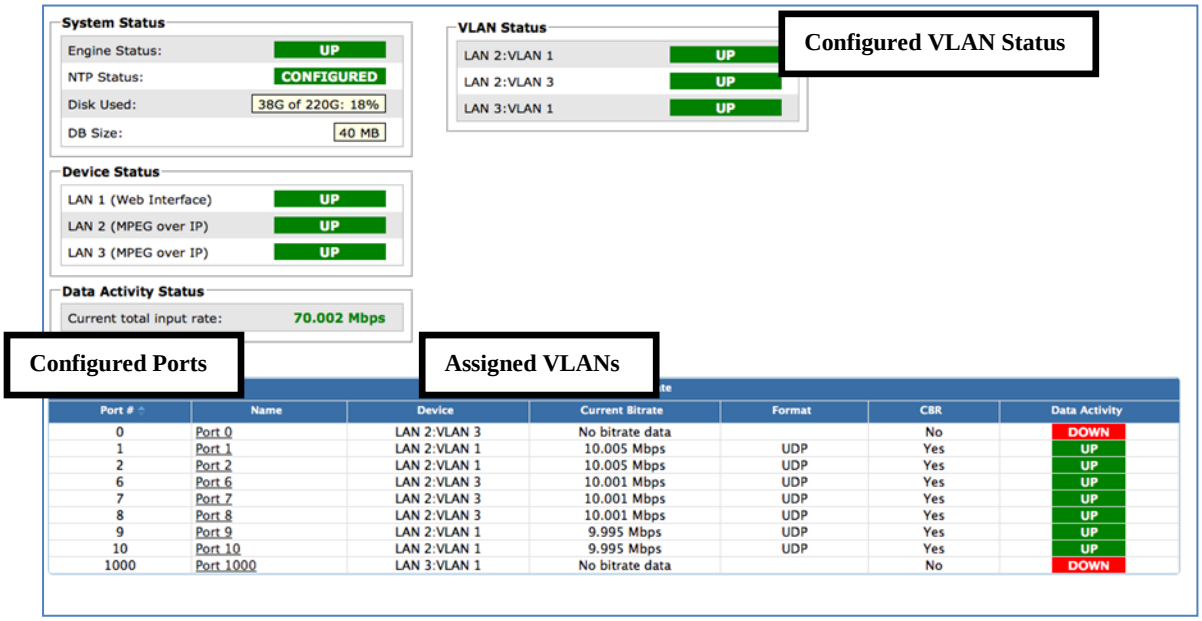


Figure 324: Reviewing Port/VLAN status

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.*

Configure System Preferences

The **System Preferences** page offers options for:

- **Ad Cue PIDs**
- **Perceptual Video Quality (eMOS) Settings**
- **Default Provider Name Settings**
- **Provider Name Parsing**
- **Audio Measurement Mode**
- **Thumbnail Settings**

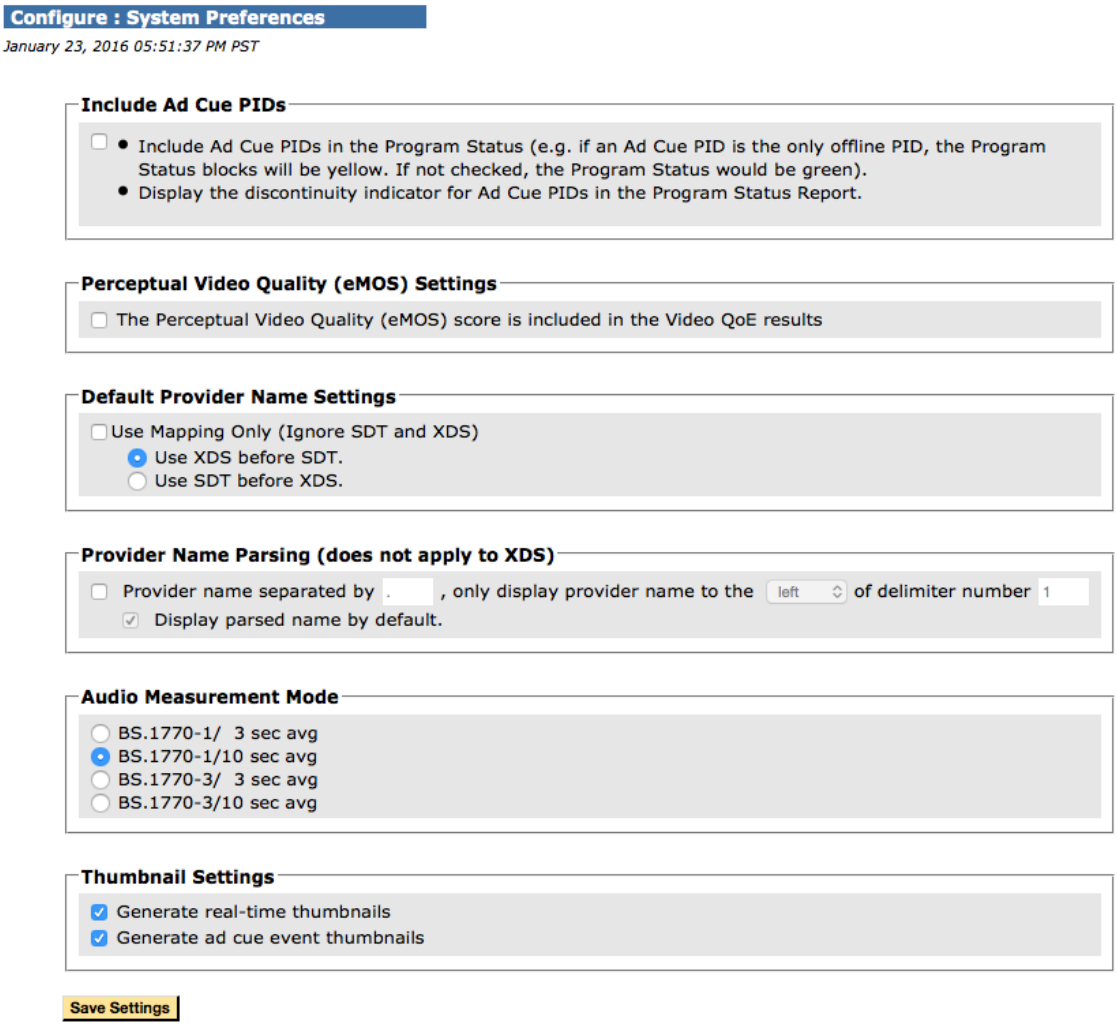


Figure 325: System Preferences options

In support of CALM Act compliance, you can select the audio measurement mode from the **Configure**: **System Preferences** section. You can also set the sliding window average to either three or ten seconds.

Additionally, the **Program Statistics Report** now contains a column to indicate the **Audio (Measurement) Mode**. The **Audio (Volume) Level** graphs include the method of measurement in the legend.

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

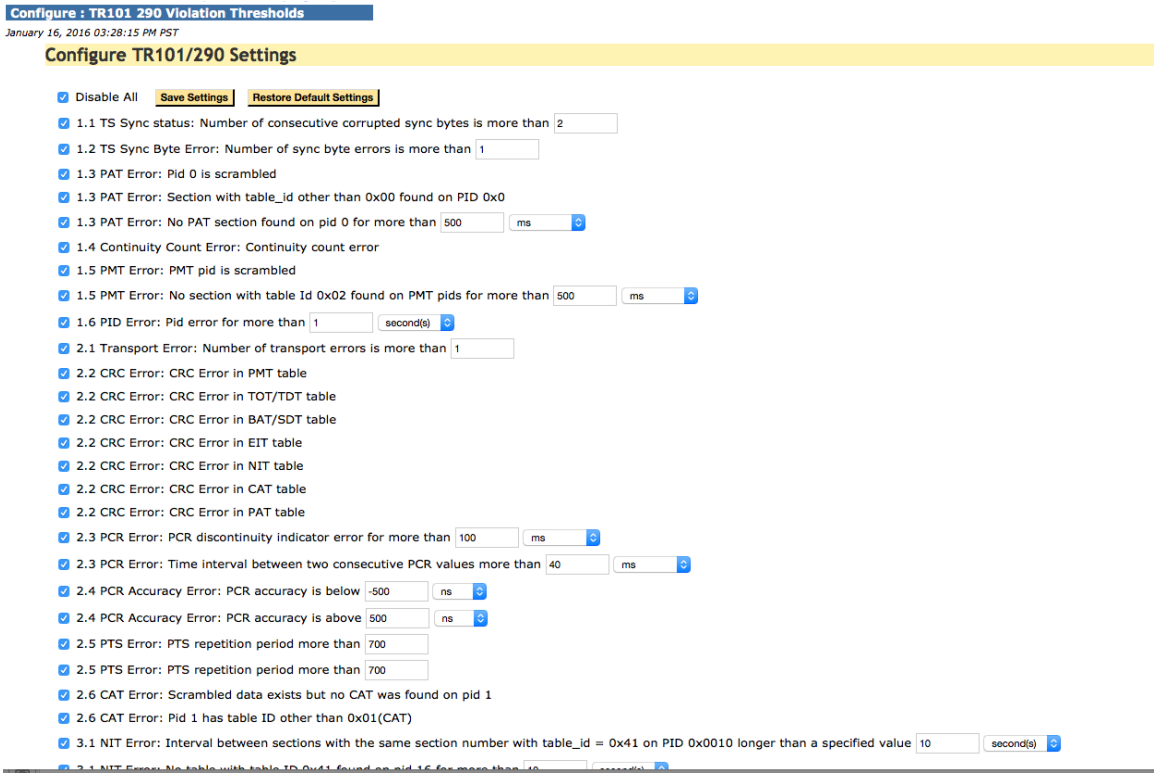
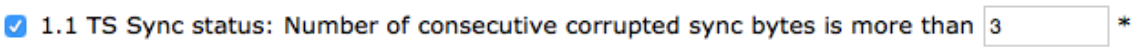


Figure 326: TR101/290 Settings page

To update any of the settings, make the changes on the page and click **Save Settings**.

Click **Restore Default Settings** to refresh the screen with all of the factory default settings. You'll then need to click **Save Settings** 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.

Configure System Settings

There are four categories of system settings: **Network**, **Time, Locale and Maintenance Mode**.

1. Select **System Settings** from the **Configure** main-menu.
2. Click on the **Network** tab to view the network system settings.

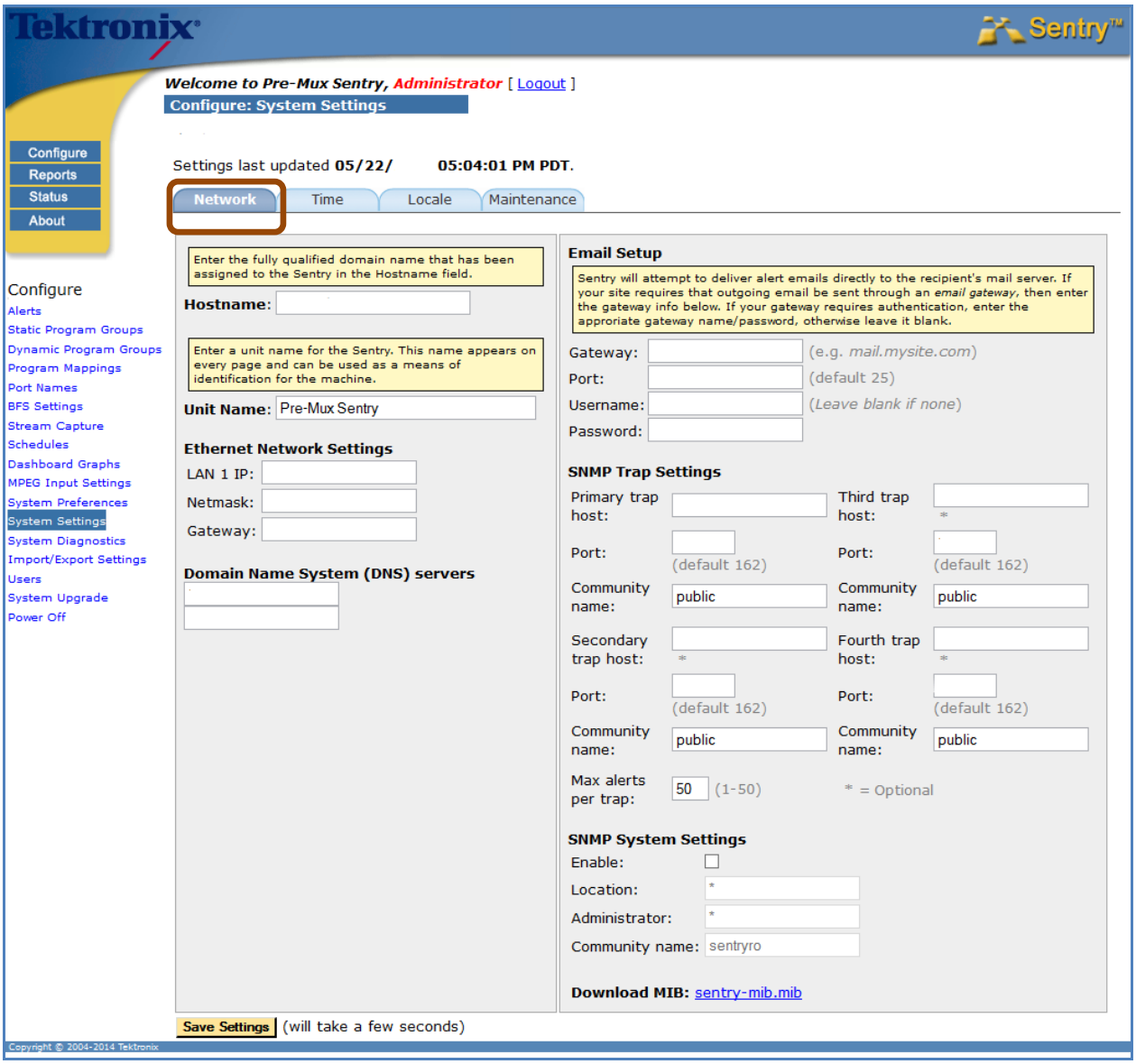


Figure 327: Configure System Settings: Network tab

Network settings

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.

Changing this information may affect your ability to access Sentry or receive alerts.

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

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

- **Ethernet Network Settings**
  1. 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.
  2. 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.
  1. Enter the port number that the email server is listening on in the Port field.
  2. 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. Sentry supports up to four destinations for SNMP traps.

  To set the SNMP Trap
  In the Primary trap host IP 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.

Set the Time

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

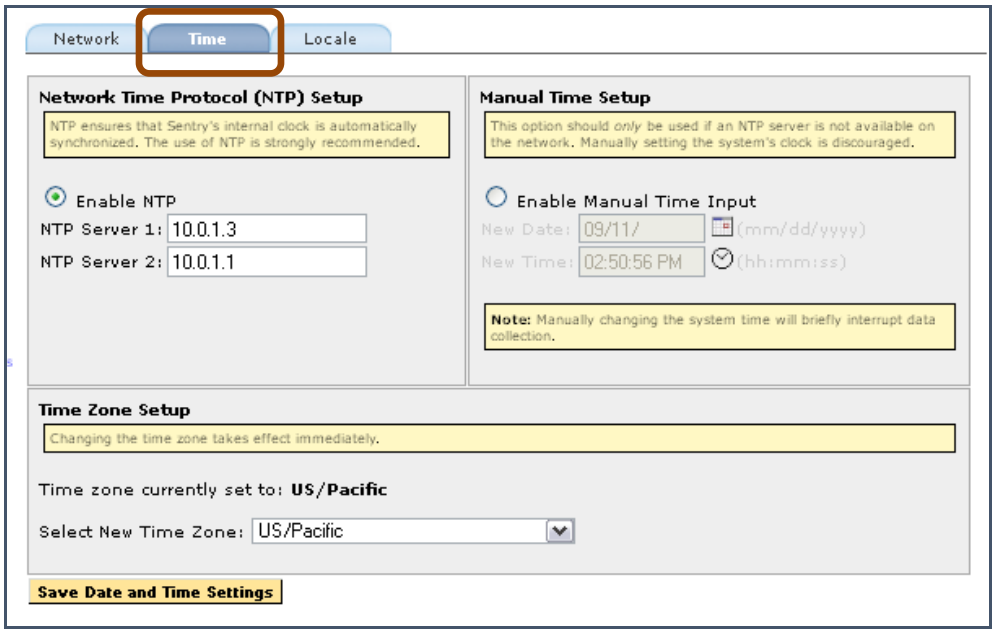


Figure 328: Time tab

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.

Set the Locale

The **Locale** determines what character set will be used in the text of Sentry. For example: **Western** or **Chinese Traditional.**

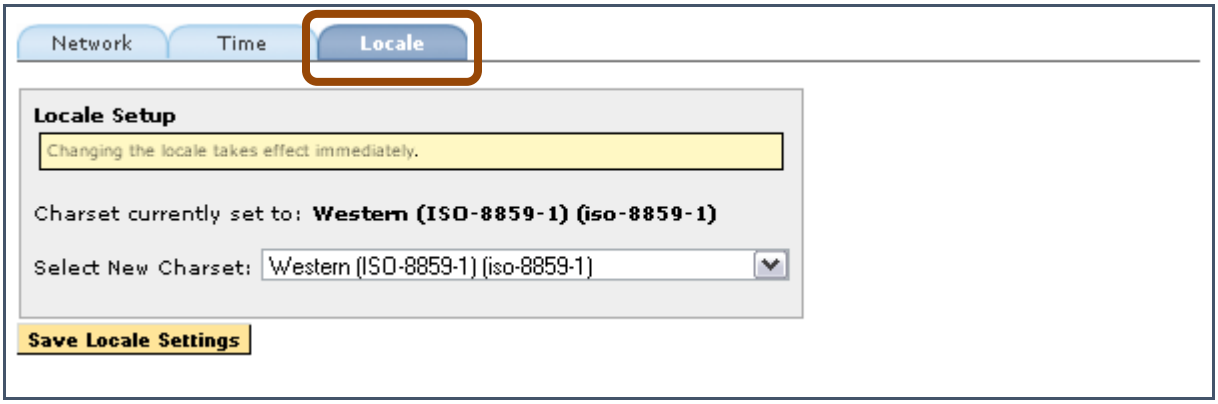


Figure 329: Locale tab

Maintenance Mode

The **Maintenance** tab allows you to schedule times where the Sentry will not send any email or SNMP notifications. Storage of alerts for **Alert History** and **Alert Analysis** reporting will be retained during these periods, but no notifications will be sent.

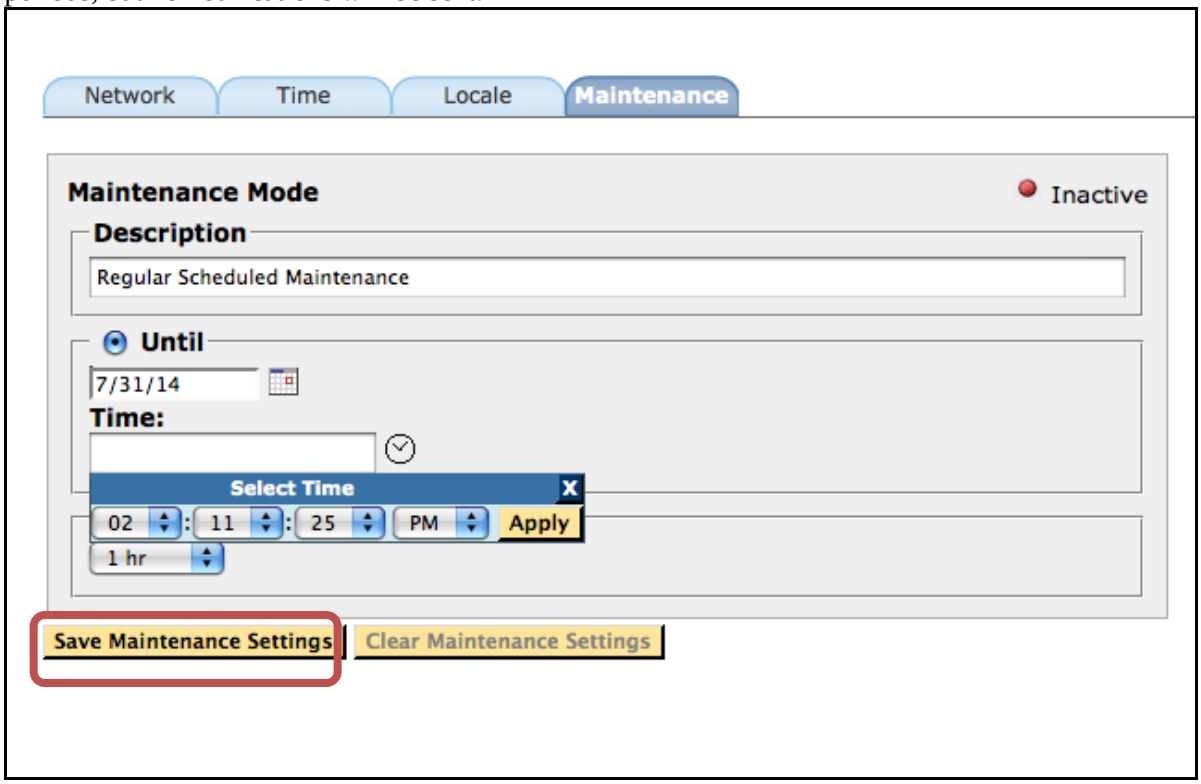


Figure 330: Setting Maintenance Mode options

1. 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 pages when the Sentry is in **Maintenance Mode**.

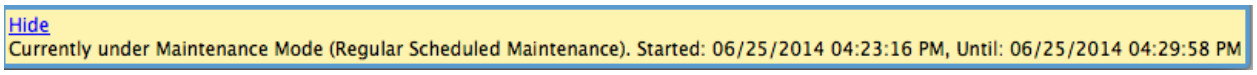


Figure 331: Maintenance Mode banner

2. 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 Diagnostics

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

Email Diagnostics

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

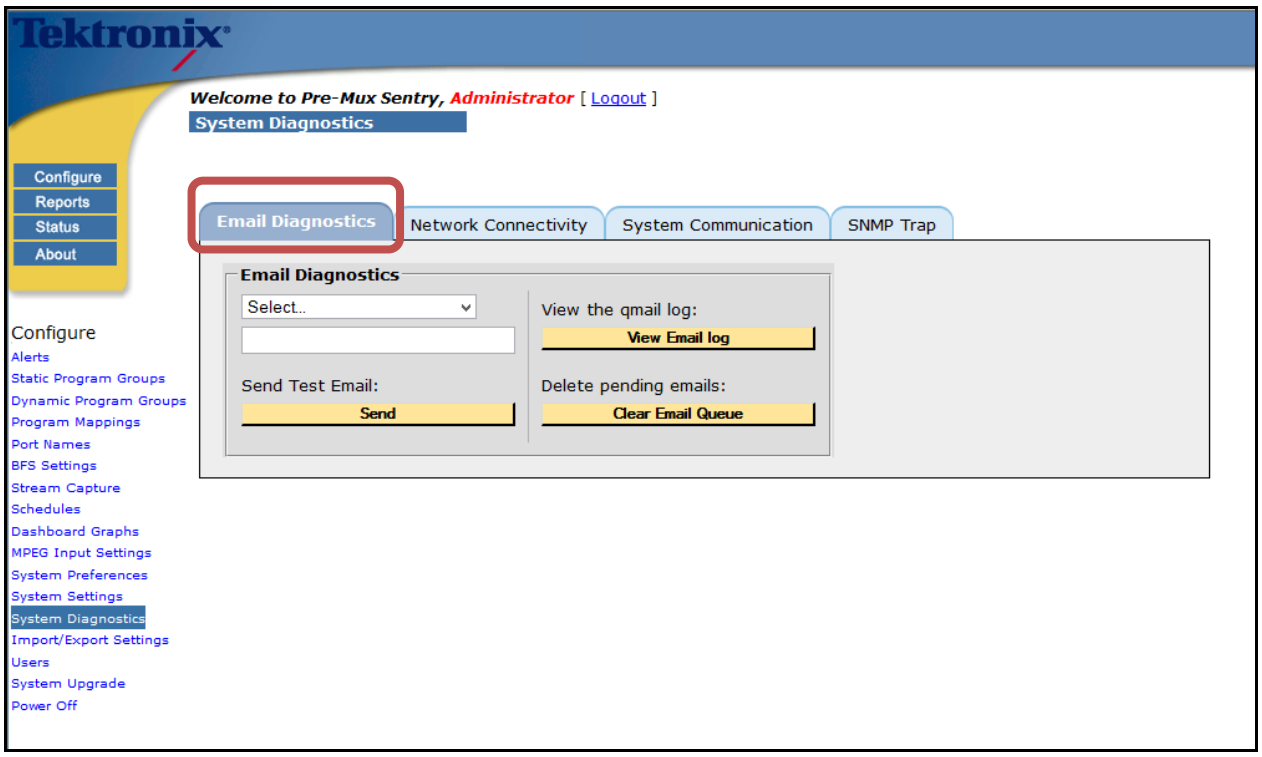


Figure 332: Email Diagnostics tab

Network connectivity

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

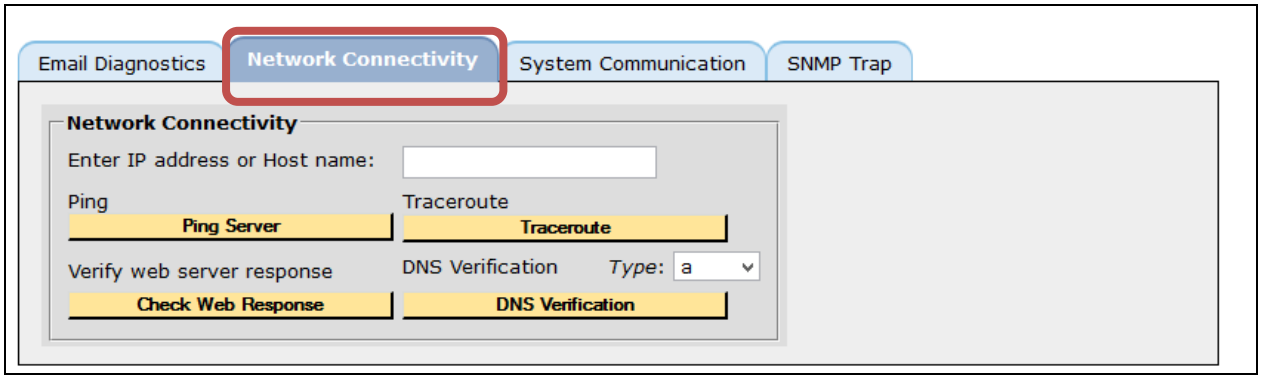


Figure 333: Network Connectivity tab

System Communication

Validates that the communication between Sentry and Medius is working.

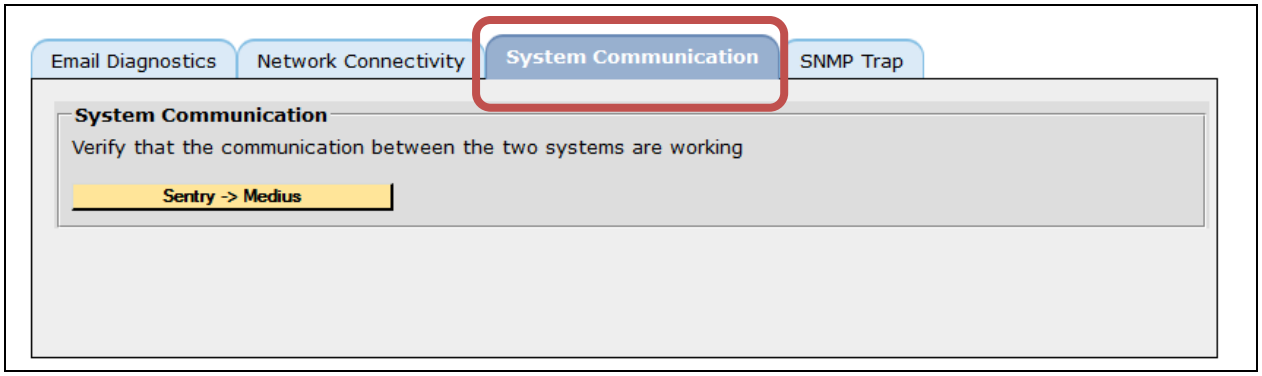


Figure 334: System Communications tab

SNMP Trap

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

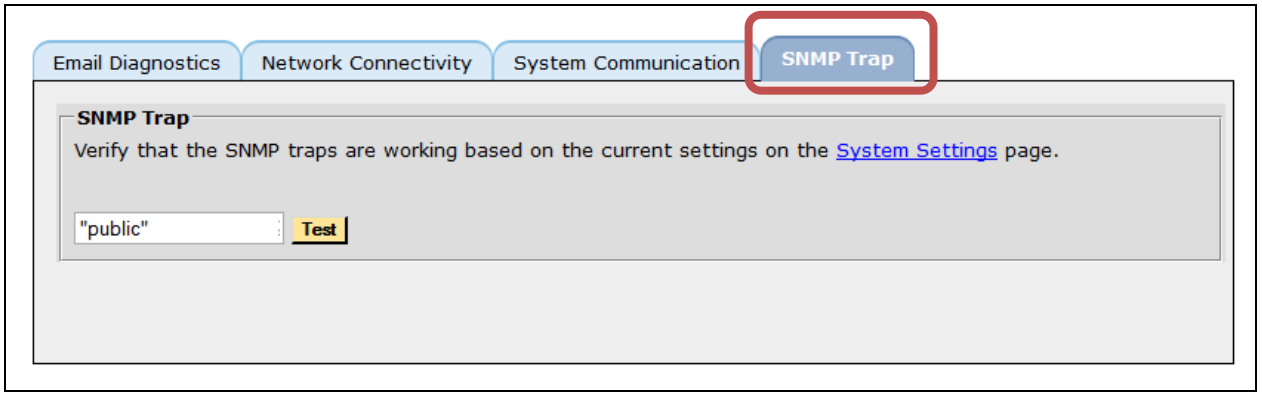


Figure 335: SNMP Trap tab

Configure Import/Export Settings

The **Import/Export Settings** function allows you to backup the configuration of the unit for safe keeping or to mirror a configuration to another unit. This allows you to set up multiple units with the same configuration without having to repeat the set up steps over and over again.

The **Export** and **Import** tabs allow you select whether you are importing your settings from one Sentry to another, or exporting the settings from one unit to another Sentry.

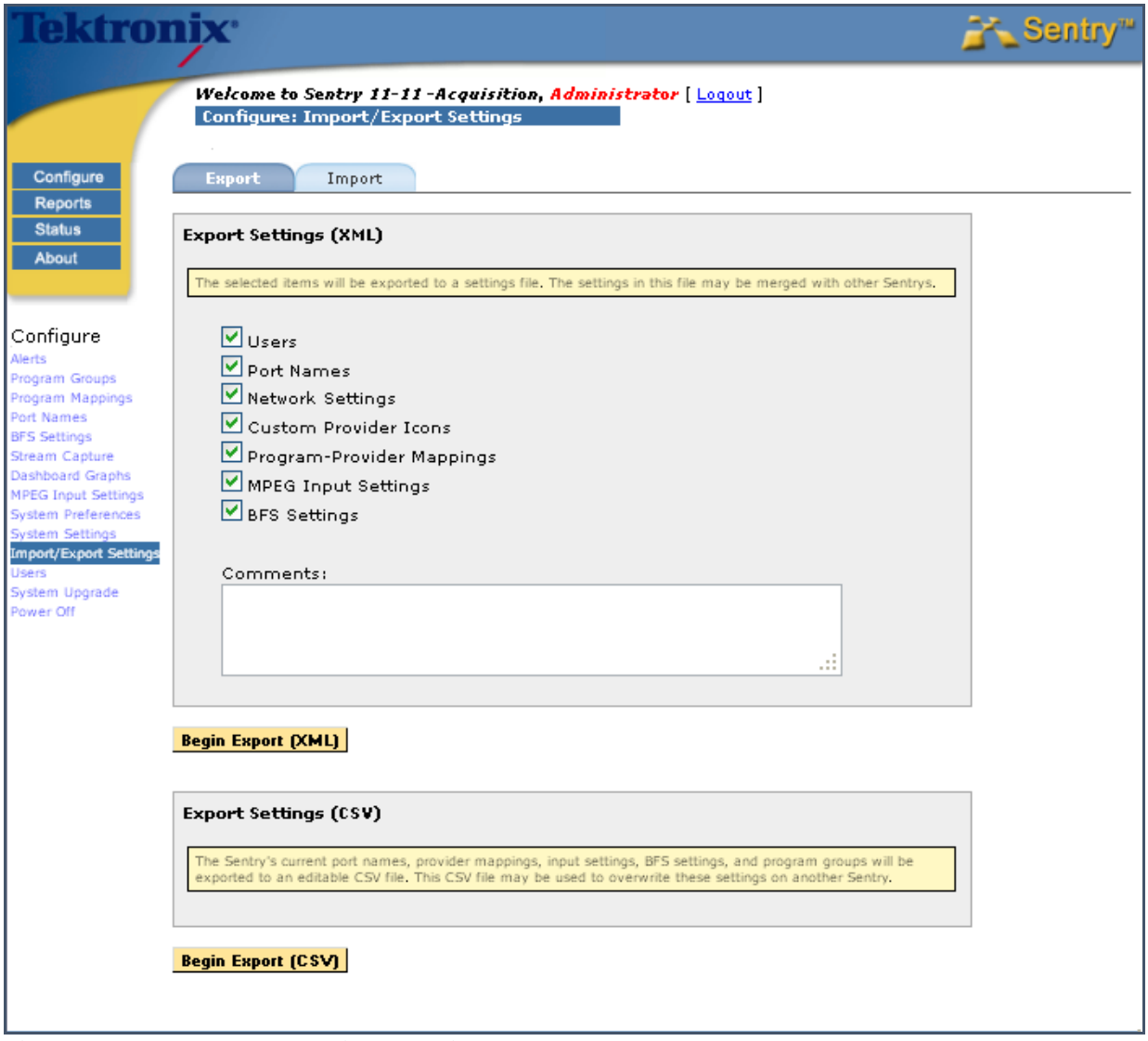


Figure 336: Import/Export Settings overview

- **Export Tab**
  You may choose to export in one of two ways: in XML or CSV. There are various reasons to choose each.

- **XML pros**
  - Allows for more control in set up by users.
  - Allows for the use of custom made provider icons.

- **XML cons**
  - Very hard for user to edit the settings within the file.
  - XML is recommended for backup and restore only. Not recommended for changing settings and re-importing.

- **CSV pros**
  - Very easy to edit using a spread sheet application such as Excel
  - Allows you to easily push your configuration on to a new device. You can edit the file as needed and then import it to another device.
  - Allows for quick set up of multiple units.

- **CSV cons**
  - Cannot add users
  - Cannot add custom provider icons

Export tab options

1. From the main menu, select **Configure** and then **Import/Export Settings**.
2. Select either the CVS or XML format
3. Select the desired fields for the export.
4. Add comments to the **Comment** field if desired.

NOTE*: You cannot select fields when choosing CSV export.*

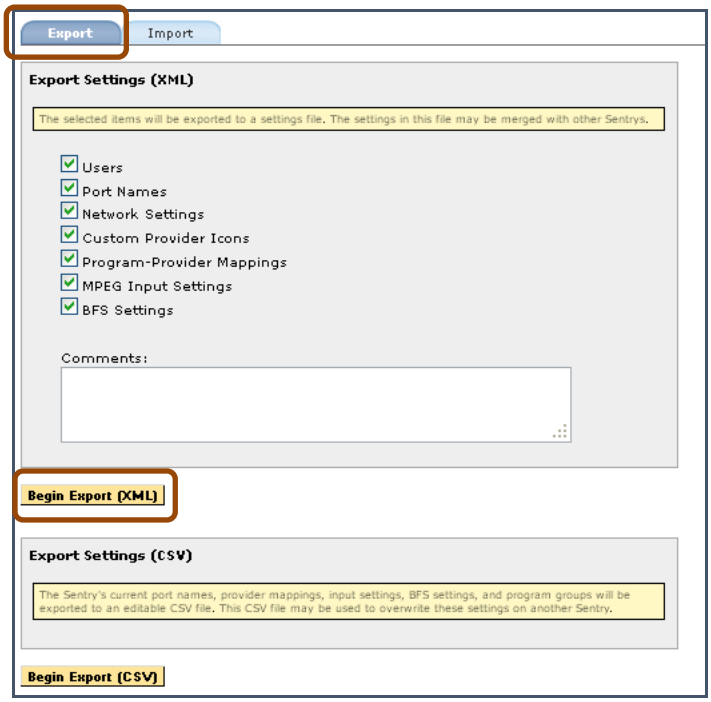


Figure 337: Export/ Import tabs

5. Select the **Begin Export** button.
6. The **Export** will begin automatically.

Figure 338: Export in progress

7. You will then receive the **Export Complete** notice. You will automatically be prompted by your system to download the configuration file.

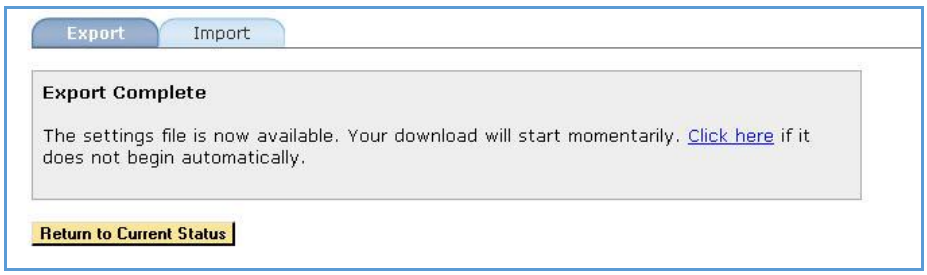


Figure 339: Export Complete

8. Select **Save File** and note the location for later retrieval.

Figure 340: Saving the Export settings

9. When complete, select the **Return to Current Status** button from the **Export Complete** page.

Import tab options

1. Select the **Import** tab.

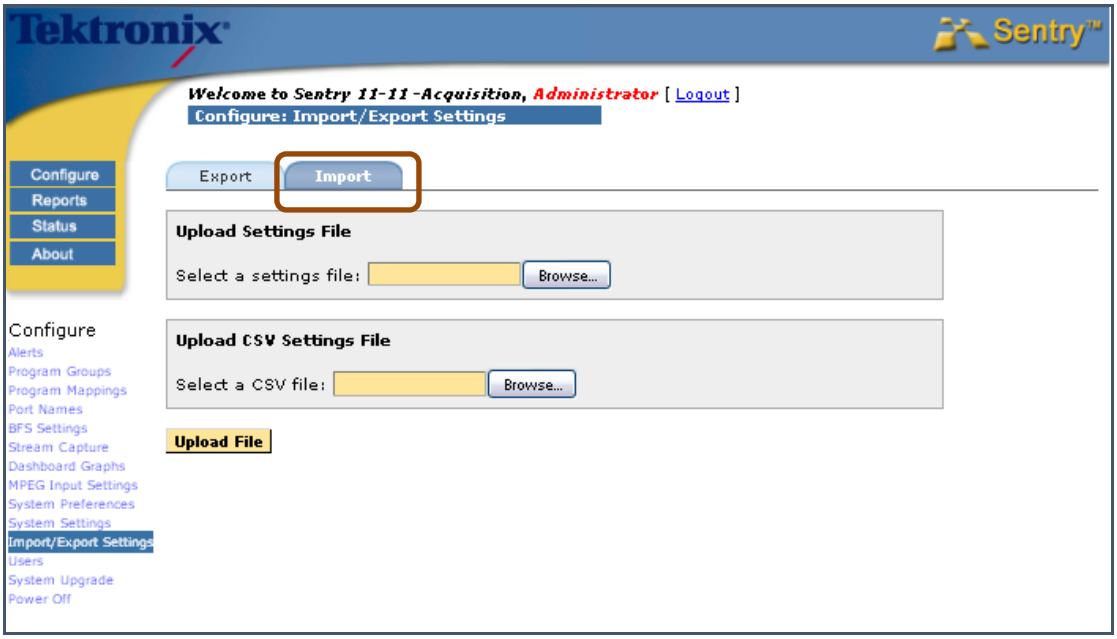


Figure 341: Import options

2. Upload the imported settings
3. Browse for file location for either the XML settings (top) or the CSV file (bottom).
4. Complete the validation check on file
5. You will either receive an **Error** report or get confirmation that the file transferred correctly.
6. If the upload was correct, select **OK** to run it.

NOTE: If you are importing new MPEG input settings: after completing the import, you will need to go to **Config MPEG Input** for the unit and click **Save** for your Multicast settings to take effect.

Configure 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.

API Access

Sentry supports a non-interactive automation interface for determining device status, downloading measurement data and upgrading various system settings.

NOTE: ***If you have API access, current API documentation can be obtained by selecting Help next to the API Access header. (See figure below.)***

This requires a different username/password than the Sentry/Medius login information and must be entered when enabling API access for a user.

Add a User

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

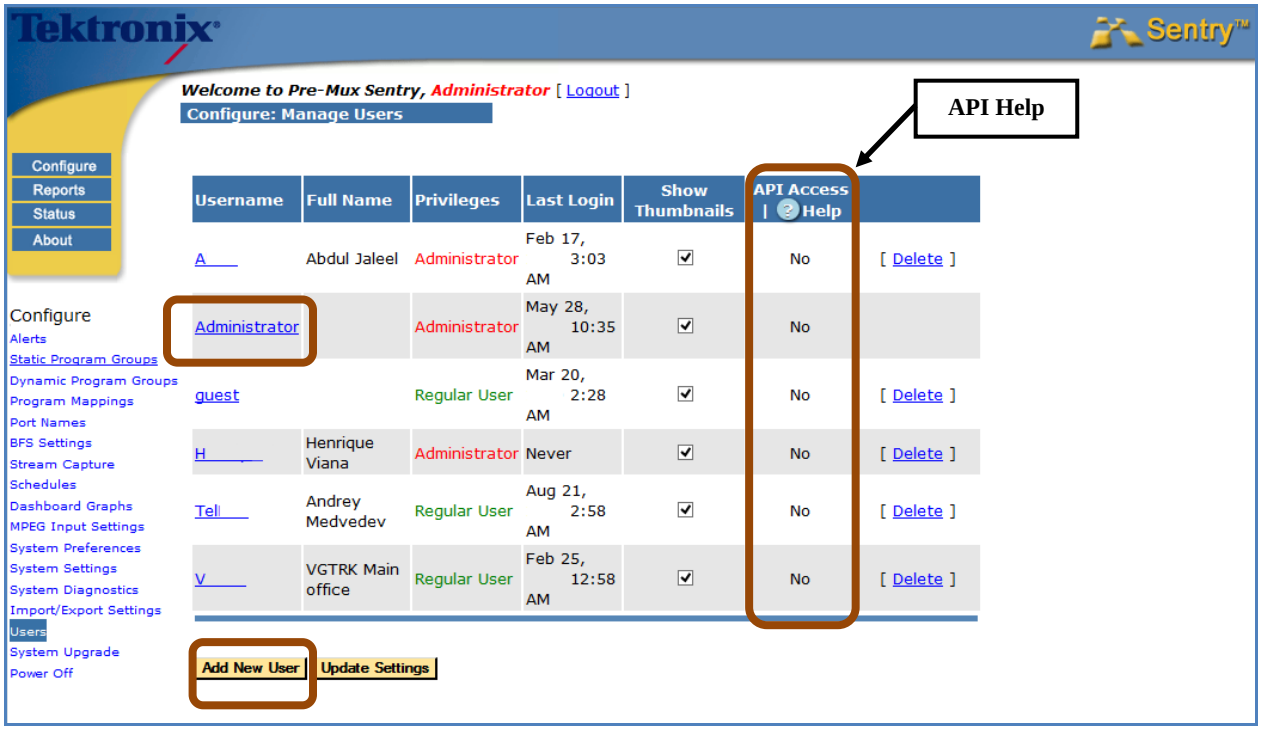


Figure 342: Manage Users Page

2. Enter the new user's information.
3. Any information that is highlighted in red is required.

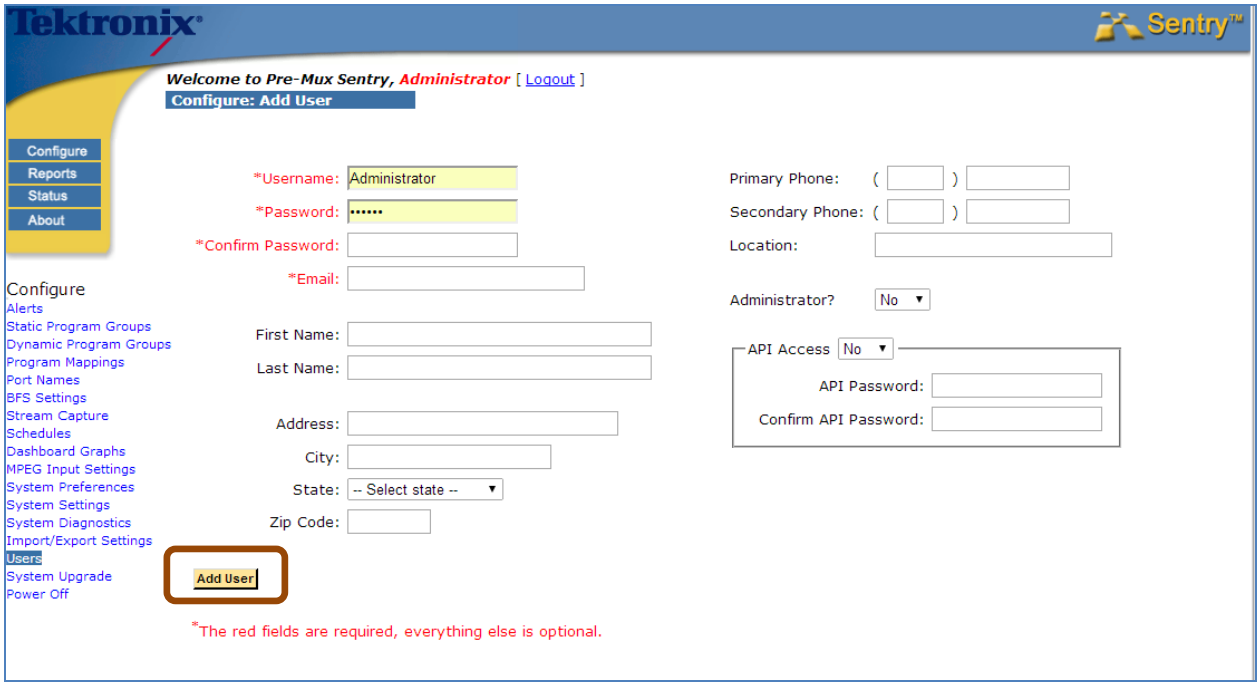


Figure 343: Add User Page

CAUTION: ***All Administrator passwords must be kept in a secure location.***

If you forget your Administrator password, contact Tektronix Customer Support.

Delete a User

To delete a user select **Delete** located to the right of a user. You will be presented with a confirmation dialog and, if confirmed, Sentry will remove the user from the system. Once users are deleted, there is no recovery. The only "recovery" is to re-create the user.

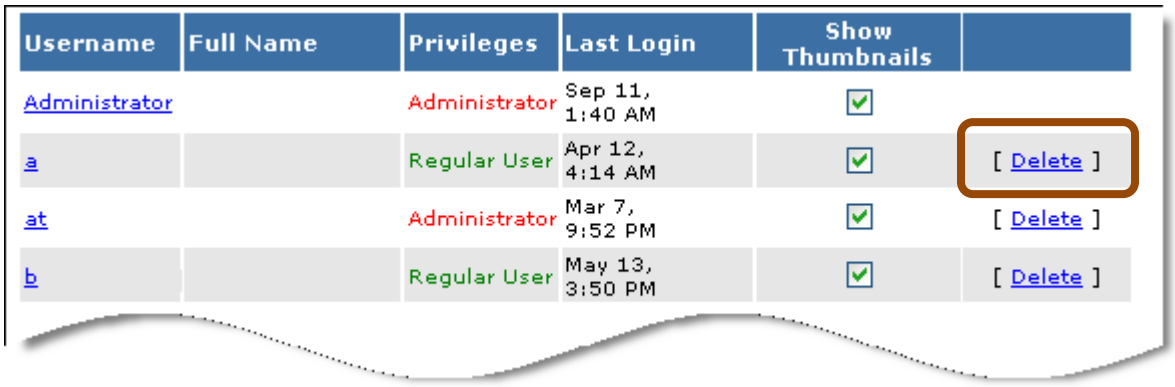


Figure 344: Delete a User

Figure 345: Delete User Confirmation Page

Modify a User

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

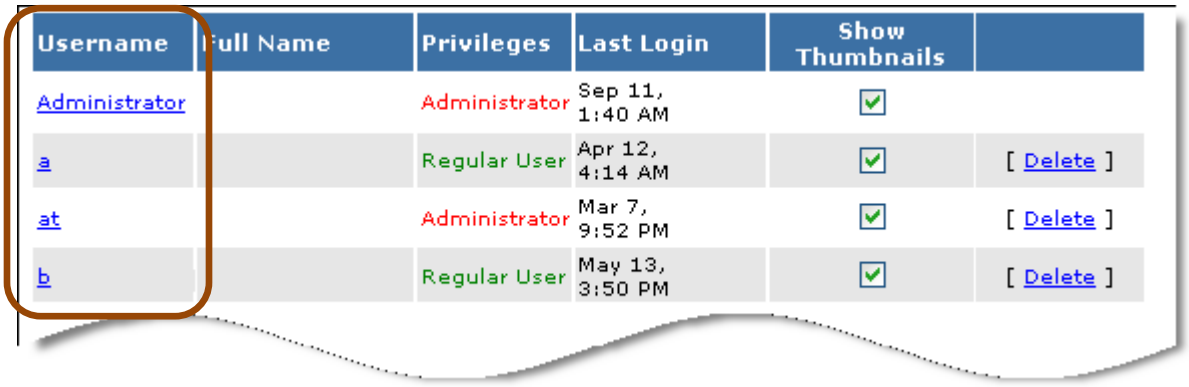


Figure 346: Select a Username

This action displays the **Update User** page to allow you to change the user information.

Once you make changes, click **Update User** to save the changes.

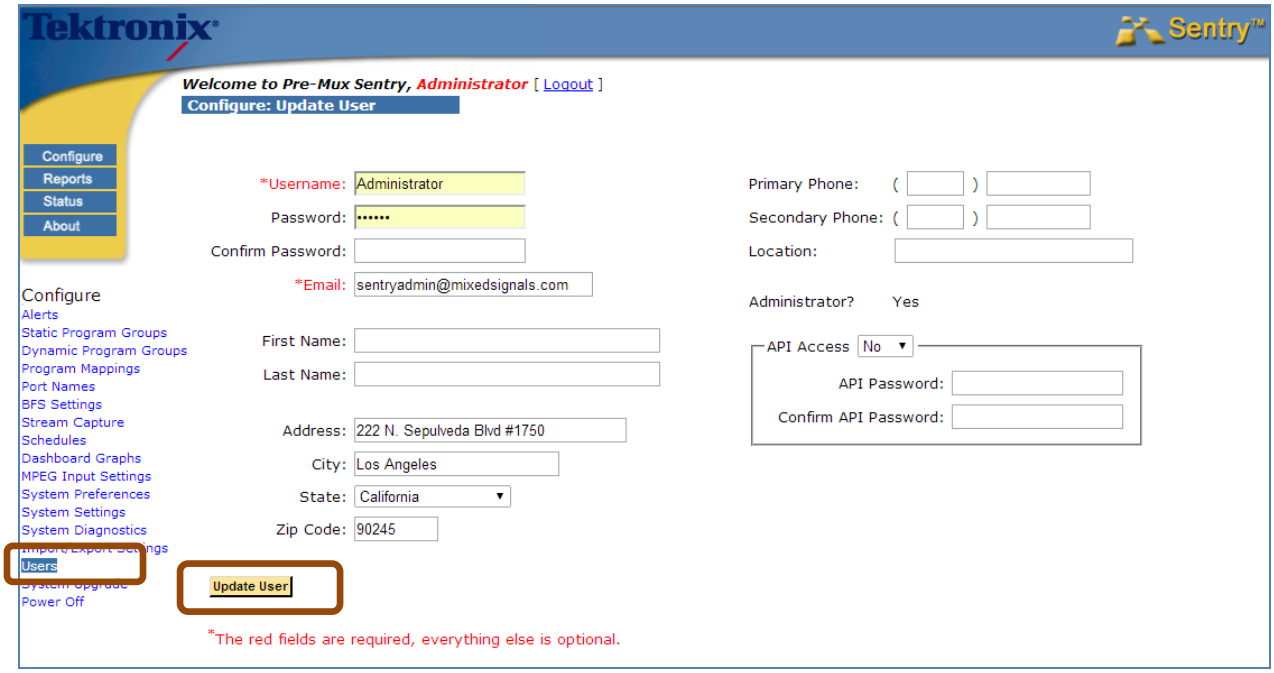


Figure 347: Update User

Configure System Upgrades

Remote Upgrade allows supported users to remotely upgrade their Sentry's to the latest software releases. The upgrade can be performed by anyone with administrator access.

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

If your Sentry unit is registered to a Medius:
You will need to upgrade your Sentry, and all other Sentrys registered to that Medius through the Medius System Upgrade pages. (See the *Medius User Manual* for more information).

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

Upgrade Procedure

1. For stand-alone Sentrys, you can begin your upgrade by choosing the **Configure**- and then **System Upgrade** from the menu option.

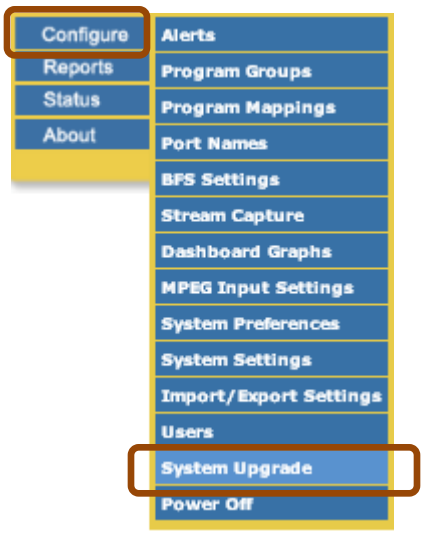


Figure 348: System Upgrade

2. The resulting page allows the user to either **Upgrade** or see a **History** of past upgrades.
3. Upgrading the Sentry is a two step process.

Figure 349: System Upgrade welcome screen

4. **Section** 1 : If 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 350: Upgrade Sentry button

7. **Section** 2 : Upon returning to the **System Upgrade** screen, you should see another ✔ next to **Section** 1 .

8. **Section** 2 will show the upgrade information and an arrow leading from the old version to the new version. Select **Upgrade Sentry** to continue.

9. 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**.

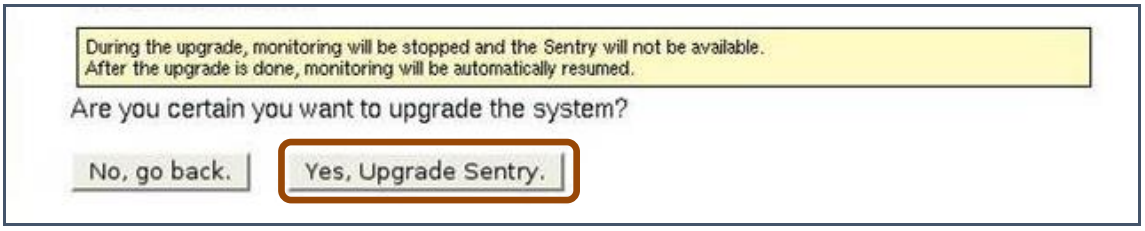


Figure 351: Upgrade confirmation

10. 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.

Figure 352: Successful Upgrade

11. 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 Sentry pages.
12. Click **Return to Sentry** to return to the main Sentry pages.

Upgrade Errors

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

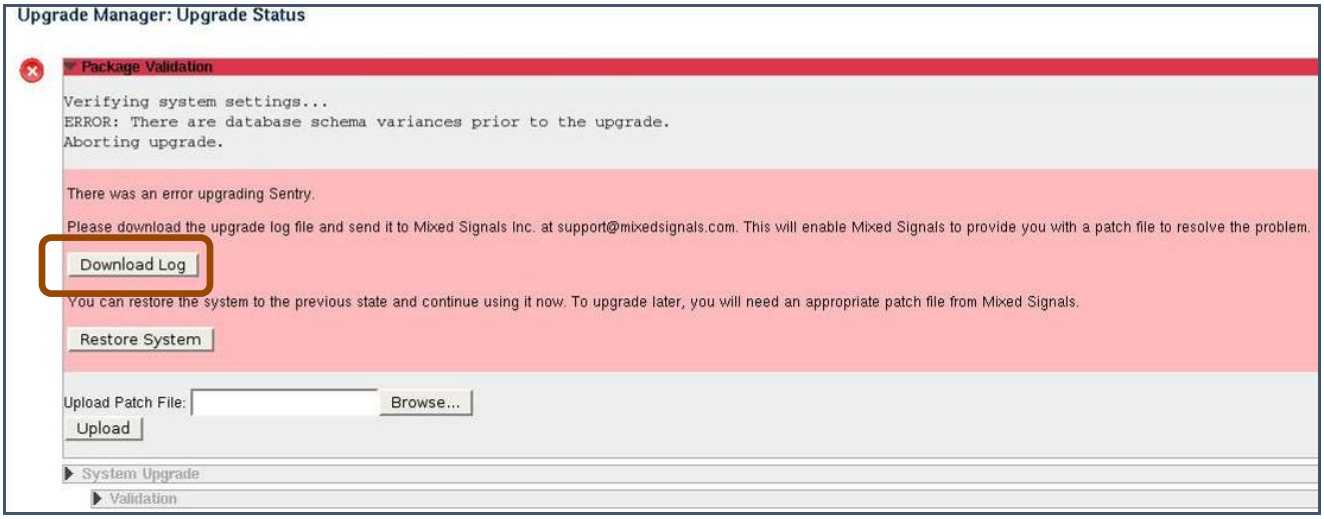


Figure 353: Upgrade Errors

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

In order to help your support representative to 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.

Uploading the Error Patch File

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

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

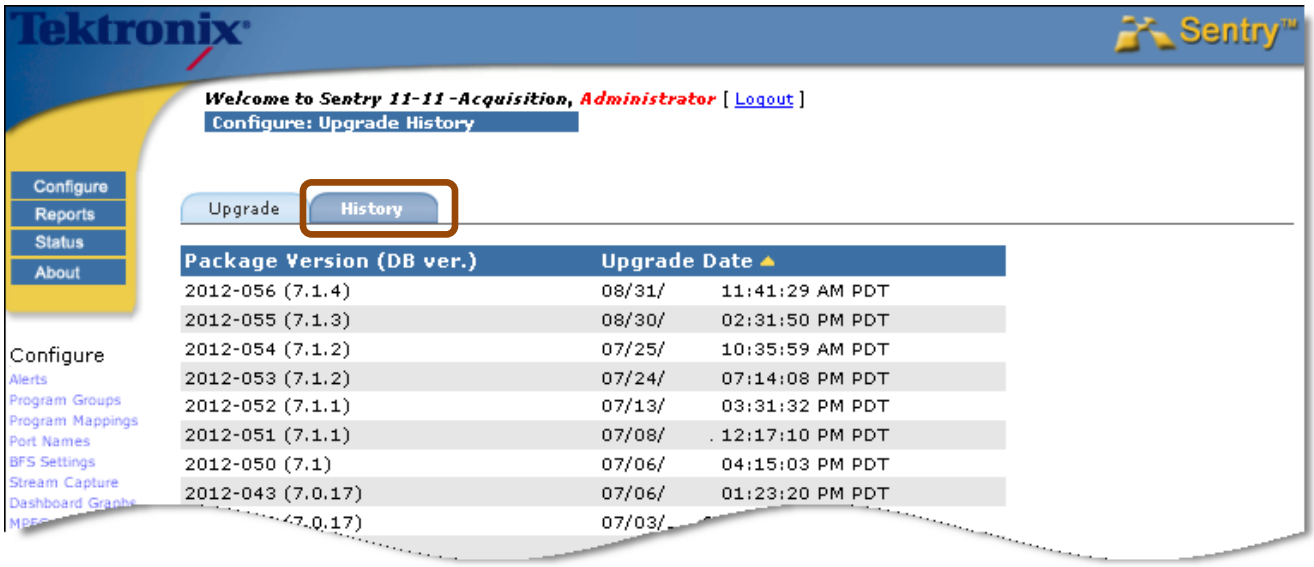


Figure 354: Upgrade History tab

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

Configure Power Off and Restart Capability

Sentry allows users to do a remote **Reset** or **Power Off** of any unit.

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

WARNING: ***When moving a Sentry, it is very important to properly power off the Sentry via the web interface.***

Never unplug a Sentry without performing the Power Off procedure. Improper shutdown may cause file corruption and failure of the Sentry.

Accessing Remote Restart and Power Off

Start at the main menu and select **Configure** and then **Power Off**.

Power Off a unit:

1. Select **Power Off**.
2. Select **Submit**. The next screen will show a conformation.

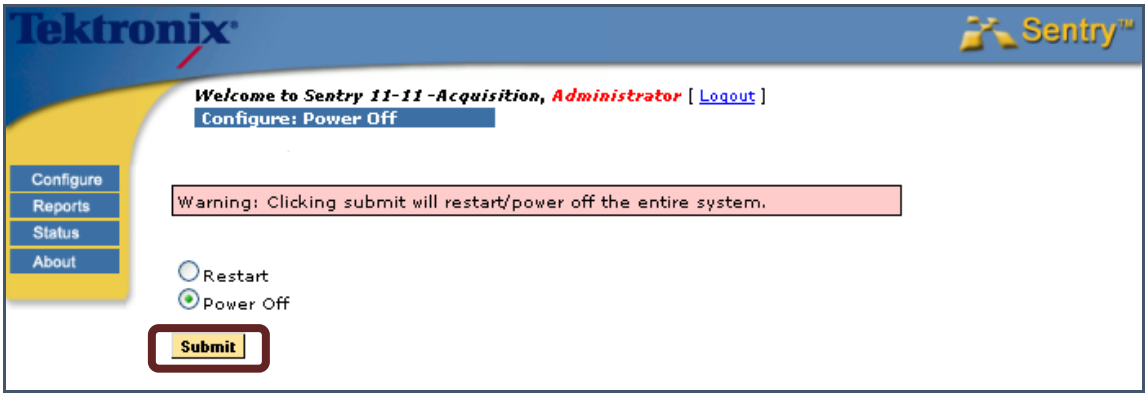


Figure 355: Powering off a unit remotely

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

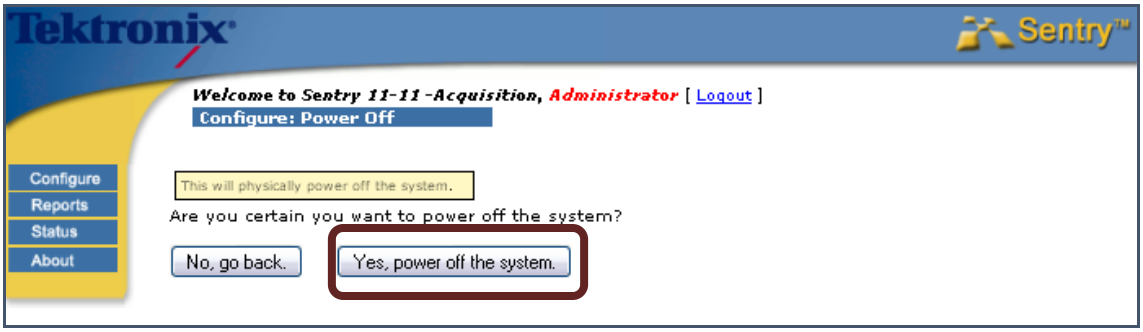


Figure 356: Powering off confirmation

Restart a unit

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

1. Select **Restart**.
2. Select **Submit**. The next screen will show a conformation.

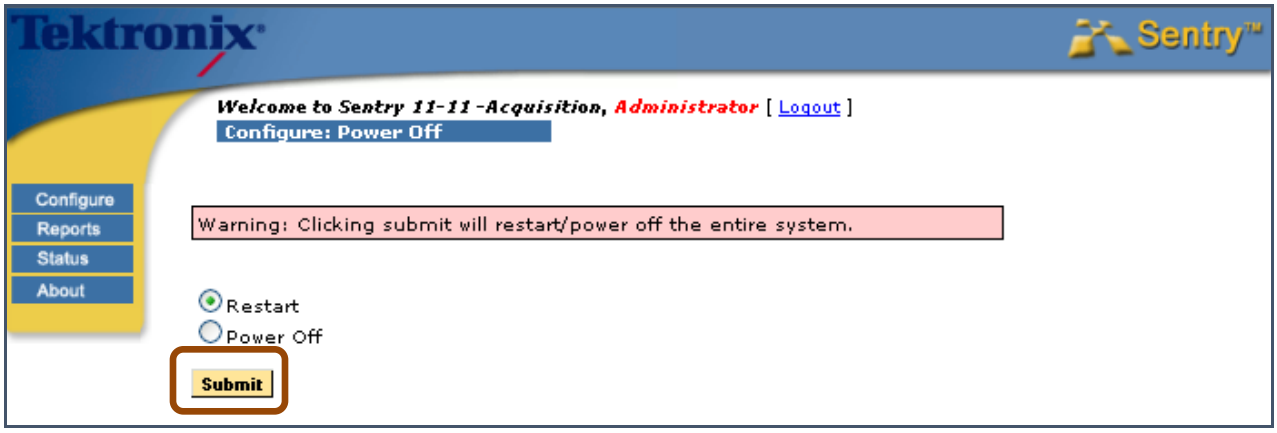


Figure 357: Restarting a unit remotely

3. Select **No** if you wish to cancel the action or **Yes** if you wish to continue with the restart.

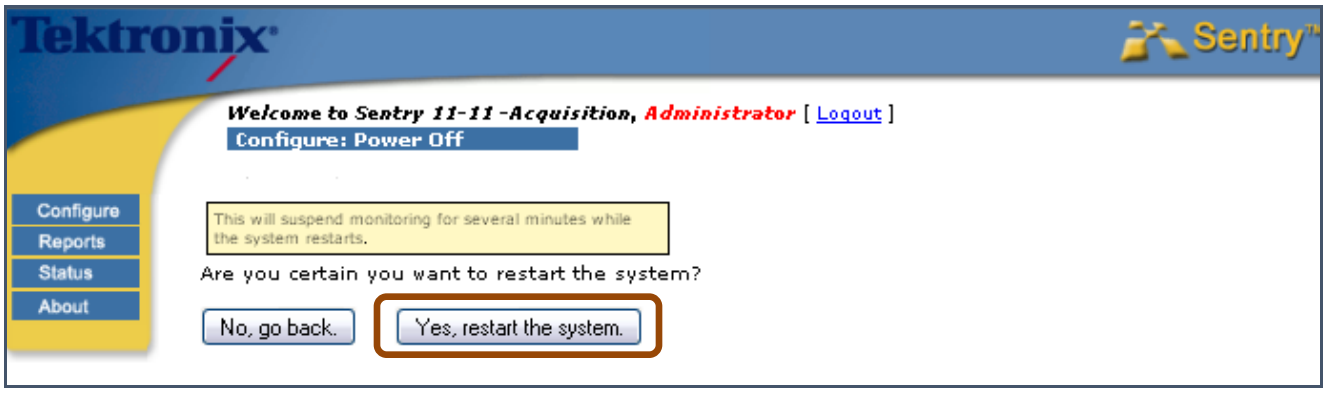


Figure 358: Confirmation of Restart

Status

The **Status** page shows the overall status of Sentry and consist of the following:

- **System Status**
  Shows general information on the **System** such as **Engine**, **NTP** and **Database** percentage 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.
- **Data Activity Status**
  Displays the current total input rate.
- **Current Input Bitrate**
  Displays the **Port Number** and **Name, Device**, **Current Bitrate**, **Report Format (UDP or RTP), CBR,** and the **Data Activity** (as **UP/DOWN** based on the bitrate).
  - When the **CBR** indicator is true, it shows that the **PCR** statistics and alerts will be analyzed assuming a highly stable delivery source (the transport has Constand Bitrate encoding) rather than the normal "bursty" characteristics of network traffic.

NOTE: ***The Format column will either read UDP or RTP.***

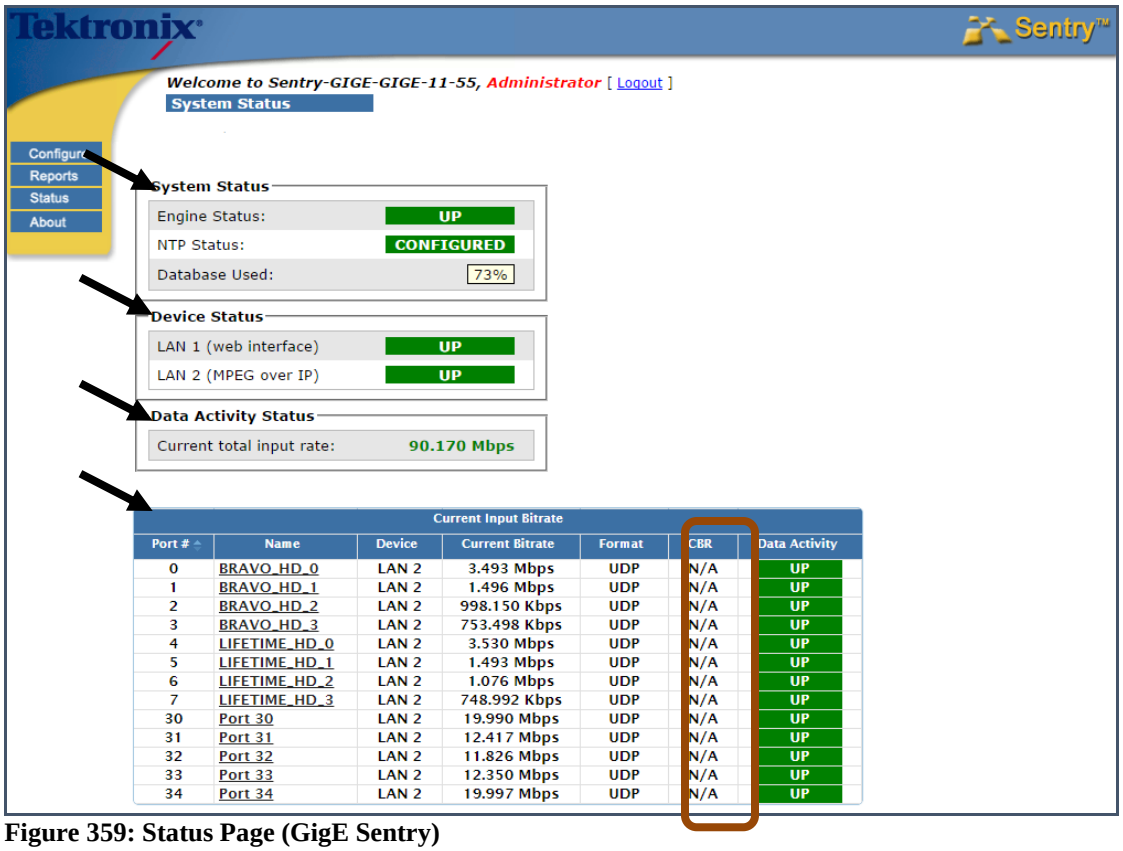


Figure 359: Status Page (GigE Sentry)

ASI Status page

The ASI **Status** page displays the **Port Number**, **Name, Device**, **Current Bitrate**, and the **Data Activity** as **UP/DOWN** based on the bitrate.

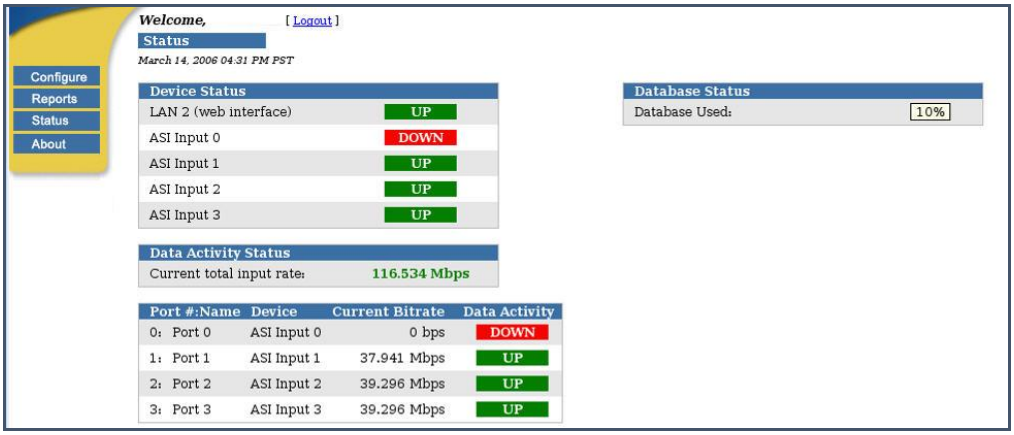


Figure 360: Status Page (Four-port ASI Sentry)

System Status for Sentry with Second MPEG Input Option Installed

If the Sentry has two network interfaces for MPEG monitoring, the **System Status** page will show an additional line referring to it in the **Device Status** section.

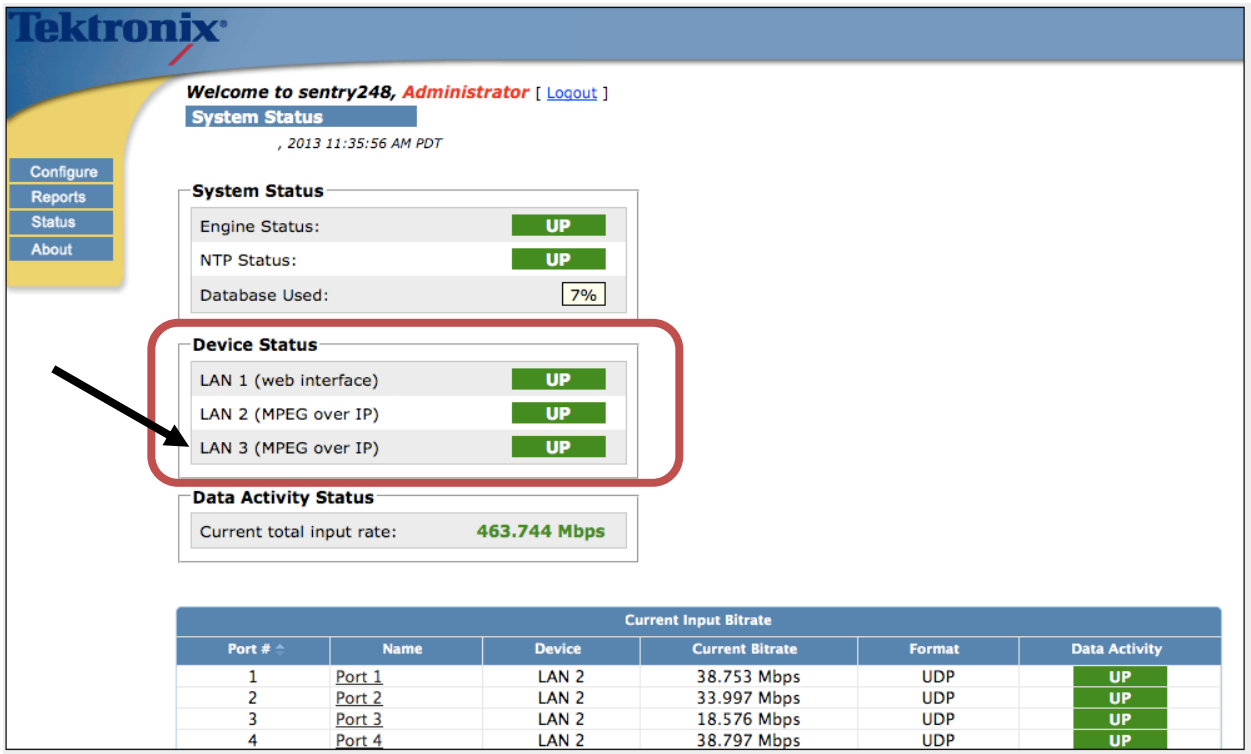


Figure 361: The extra line in Device Status box

About

The **About** page shows the Sentry engine and database version numbers of the current release, and directs you to technical assistance if needed.

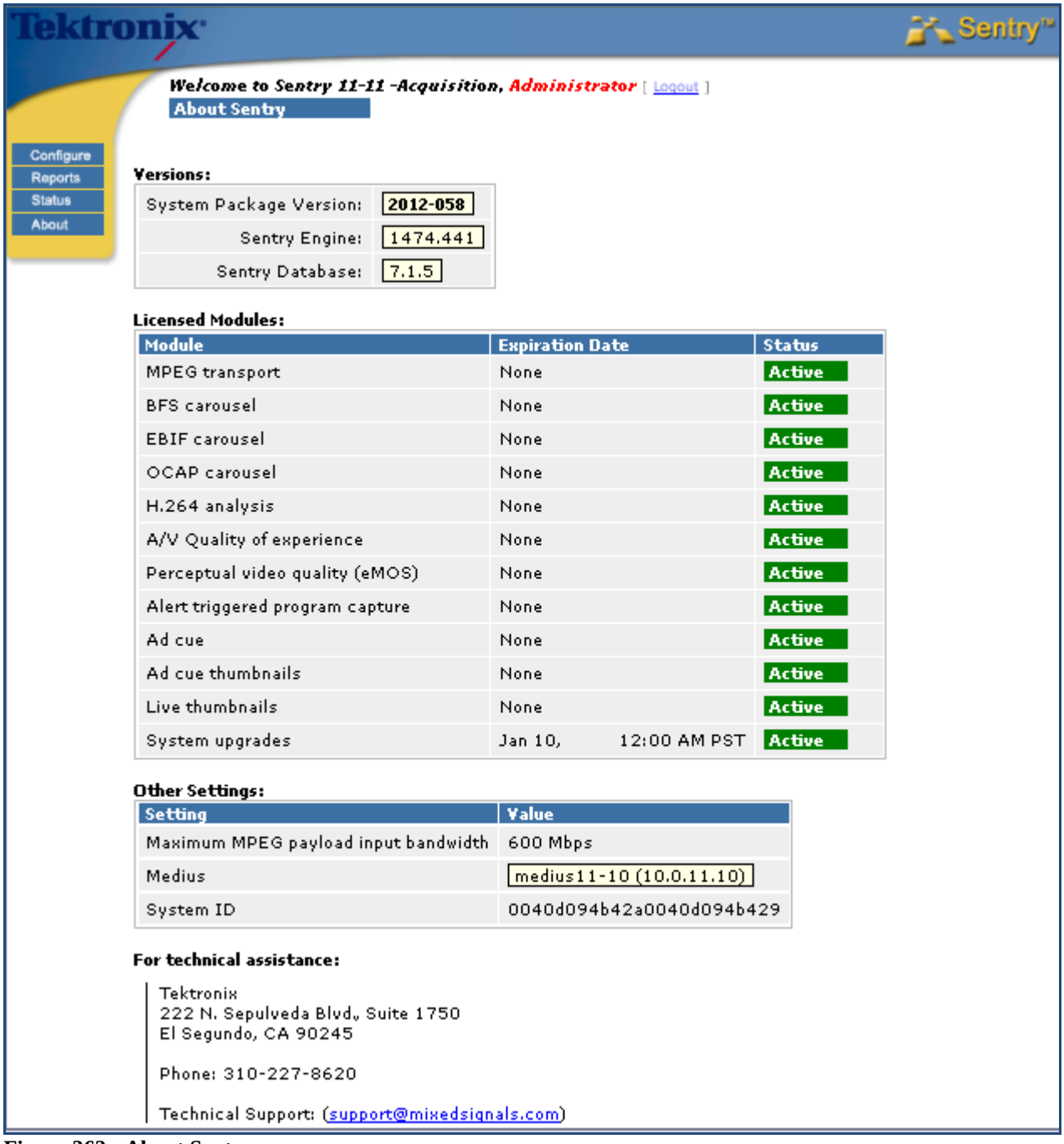


Figure 362: About Sentry

Appendix A: Sentry ABR

Sentry ABR is an active adaptive bitrate monitoring solution that proactively monitors ABR content on origin servers or CDN caching servers. It does this by actively requesting and validating program playlists / manifests that it has been configured to monitor.

Sentry ABR then requests from the server, in turn, all of the fragments of each profile/representation for each program. It then calculates availability and performance metrics and generates alerts in real time.

Sentry ABR can operate as a stand-alone monitor, or as an extension to an existing Sentry/Medius deployment that offers a unified platform for both linear broadcast and ABR video service monitoring.

Sentry ABR has a licensable option to decode the HTTP content. If Sentry ABR has this license, all of the MPEG related reports will be available (like program status, program detail, etc..). Otherwise, those pages will not be accessible.

Configure: Alerts Summary

Manifest Alerts

Sentry ABR contains a number of specific alerts. The first set are alerts on the metadata that surrounds the ABR streams. They are based on errors that could occur when examining the manifest file. The alerts are:

- **Parsing Error**
  Error encountered while parsing the manifest file
- **HTTP Error**
  HTTP error code received when attempting to receive the manifest file
- **URL Error**
  An illegal URL.
  Illegal syntax for the **Origin Server/Hostname** in a URL.
- **Unsupported ABR Standard**
  The manifest file cannot be parsed because it conforms to a currently unsupported ABR standard.

Create a Manifest Alert

1. Select **Configure** and then **Alerts** from the main menu.
2. Select the **ABR** tab.
3. From the **Manifest Alerts** list, select **Create**.

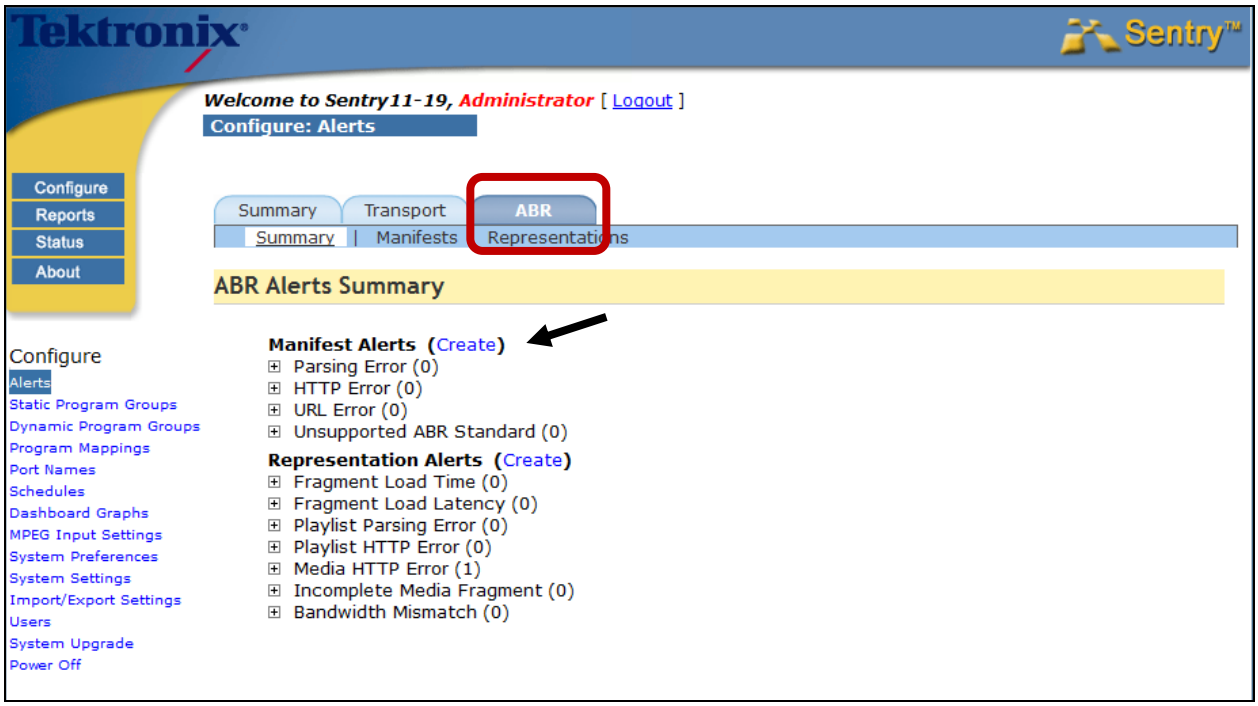


Figure 363: Alerts Summary

4. Step 1 : Select the **Alert Type.**
5. Step 2 : Choose the input manifest.
6. Step 3 : Select the desired notification settings.

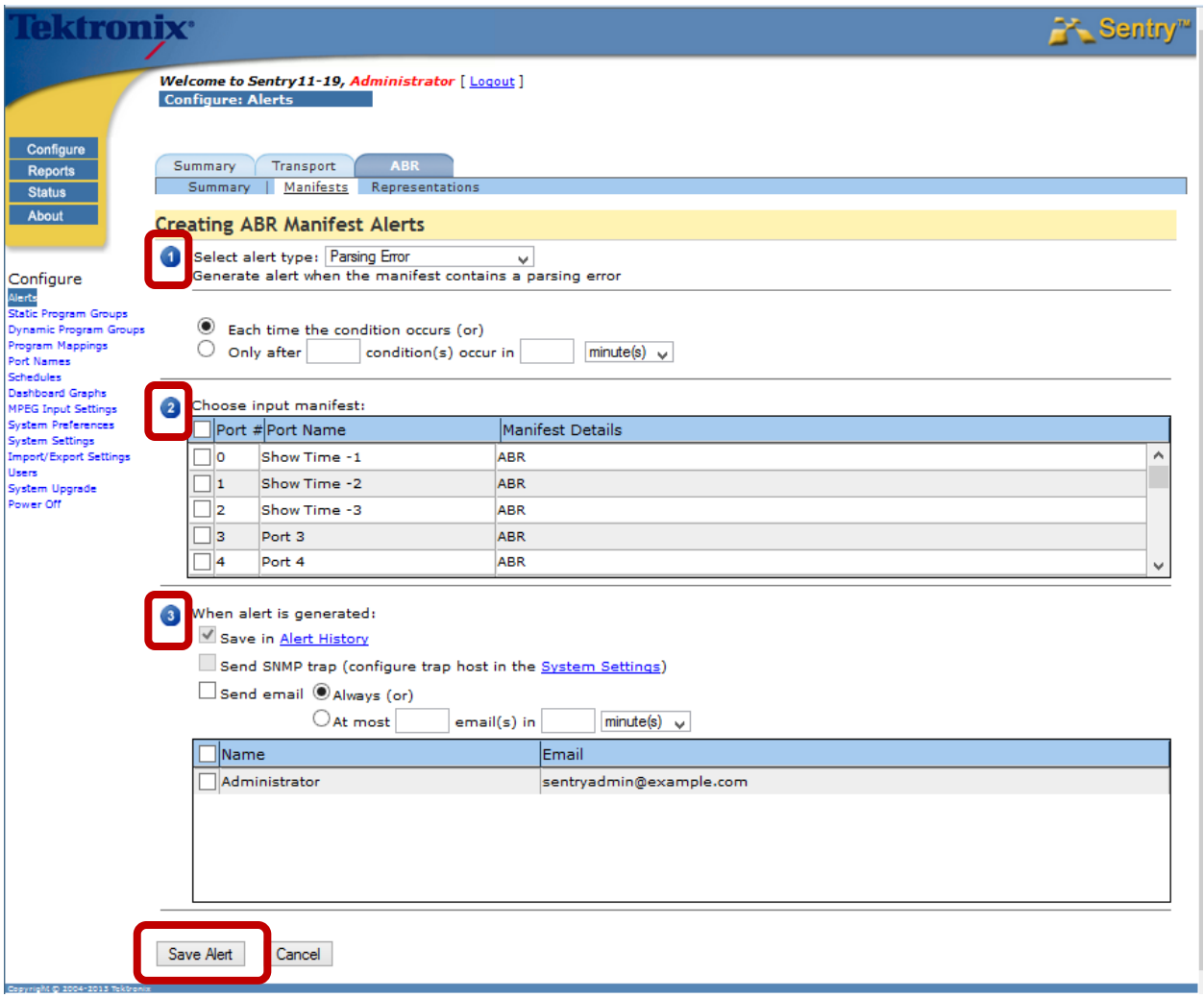


Figure 364: ABR Manifest Alerts template

7. Select **Save Alert** when complete.

Representation Alerts

Representation Alerts Definitions

- **Fragment load time**
  The time it took to load a media fragment
- **Fragment load latency**
  The time between when an HTTP request was made and when we first started to receive the fragment
- **Playlist Parsing Error**
  Error because of a corrupted playlist file or because of unrecognized syntax (HLS only)
- **Playlist HTTP Error**
  If an HTTP error returned when attempting to request a playlist file (HLS only)
- **Media HTTP Error**
  If an HTTP error is returned when attempting to request a media fragment
- **Incomplete Media Fragment**
  If another HTTP header is detected before completely receiving the previous fragment
- **Bandwidth Mismatch**
  The manifest file(s) contain a max bandwidth for each representation (profile / quality level). The user can define an alert which will trigger if the bandwidth falls below (or goes above) a specified percentage.

Create Representation Alerts

1. Select **Configure** and then **Alerts** from the main menu.
2. Select the **ABR** tab.
3. From the **Representation Alerts** list, select **Create**.

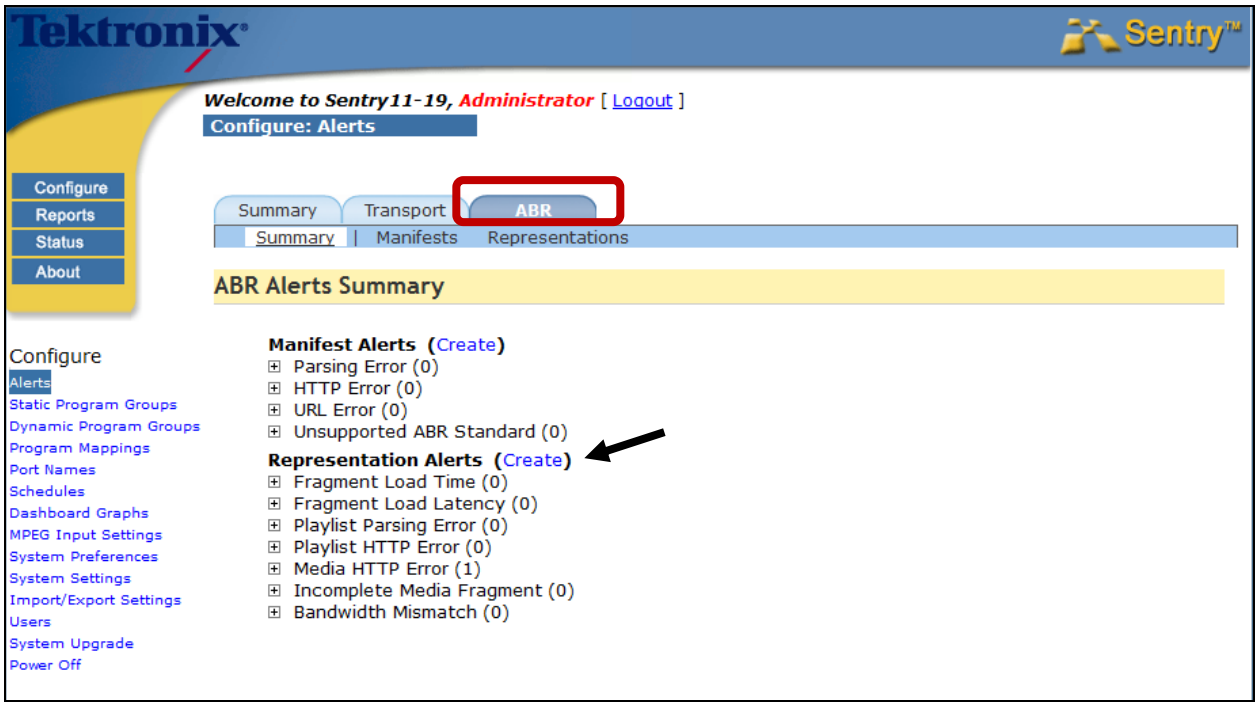


Figure 365: ABR Representation Alerts template

4. **Step** 1 : Select the **Alert Type**
5. **Step** 2 : Choose either the **Program(s)** or **Program Groups**.
6. **Step** 3 : Select the desired notification settings.

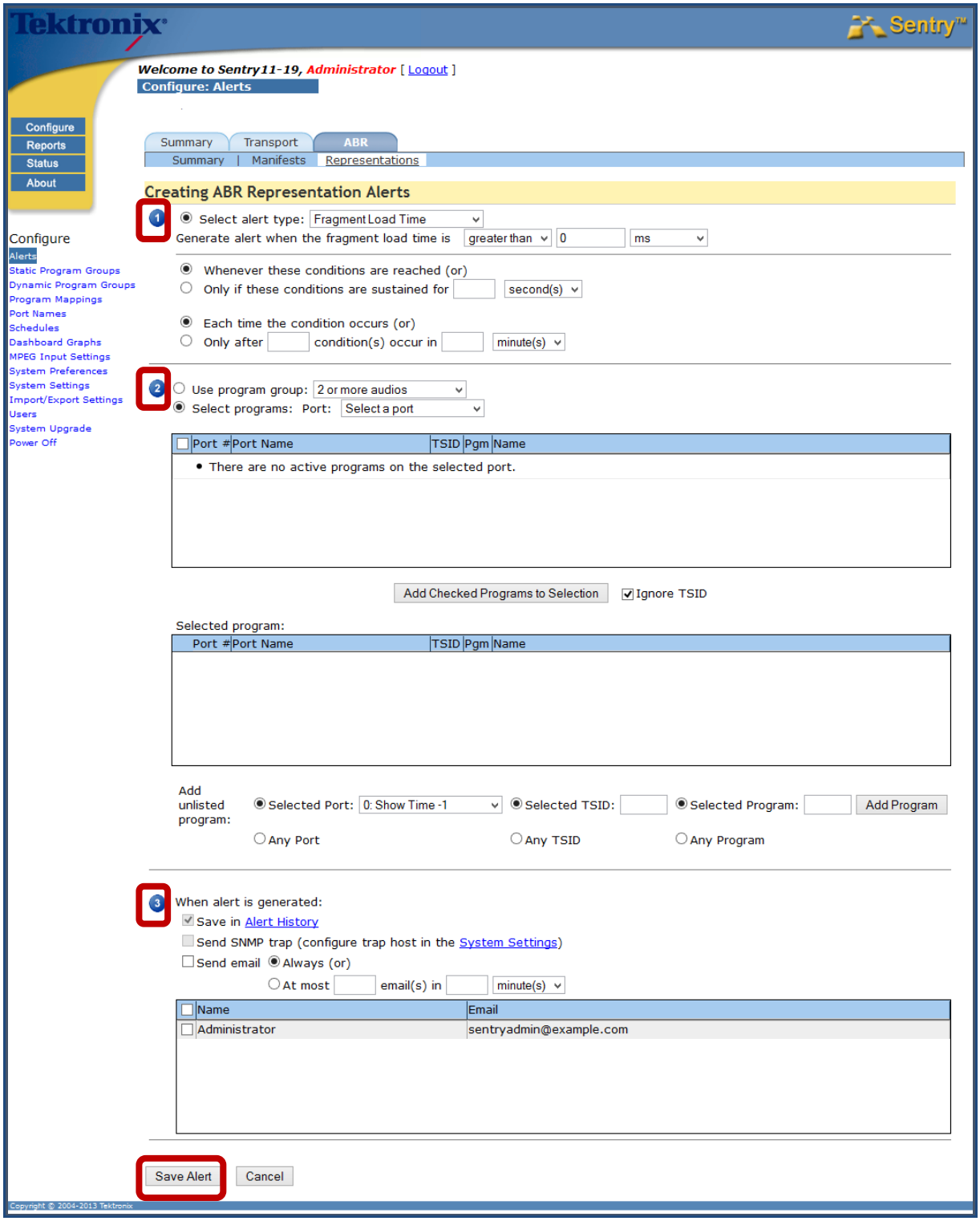


Figure 366: ABR Representation Alerts template

7. Select **Save Alert** when complete.

Dynamic Program Groups

Dynamic Program Groups allow you to define a program group based on dynamic program attributes, instead of just listing the program numbers.

Example
You can define a **Dynamic Program Group** for each program where the **Manifest Profile Index = 1.** Such a program group can be used for alerting and/or reporting.

When configuring the **MPEG Inputs**, you will not need to go back to your program group/alert definitions because, any time a new **Media Set** (ABR URL) is monitored, the **Dynamic Program Group** will always pick up the highest quality representation from that **Media Set**.

For ABR, you have the ability to define a program group based on certain criteria These criteria are

- **Port number**
- **Manifest bit rate**
- **Manifest Representation**

Select **Configure** and **Dynamic Program Groups from the main menu.**

The resulting page will be a list of all of the existing **Dynamic Program Groups**.

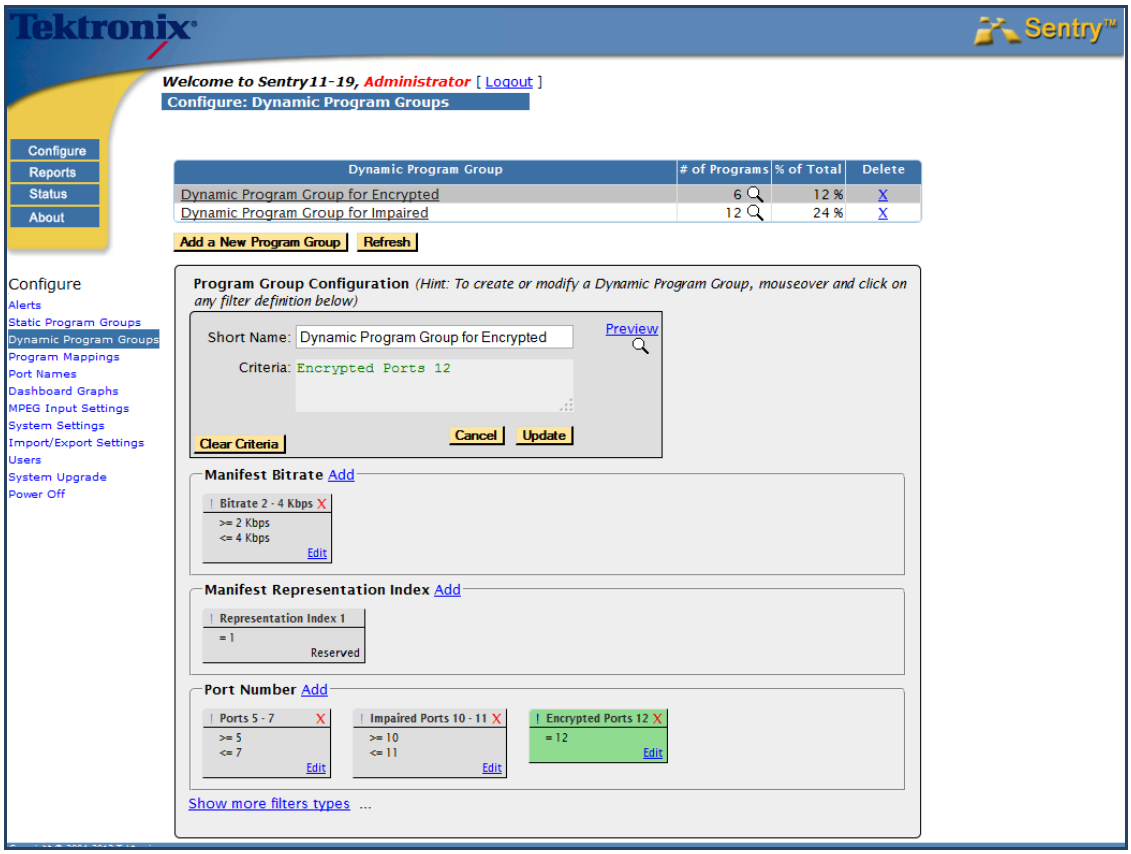


Figure 367: Dynamic Program Groups

Filters are used to define the **Dynamic Program Group**.

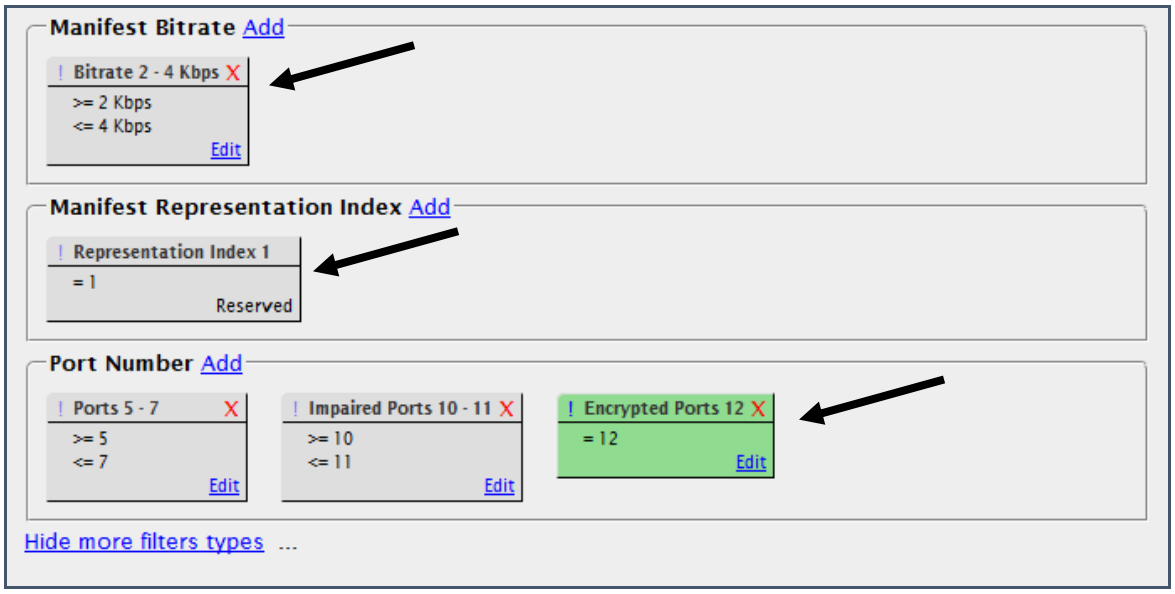


Figure 368: Filters for Dynamic Program Groups

Configure MPEG Input Settings

Administrator Set up Notes

The URLs for the manifest files have to be explicitly defined.

1. Select **Configure** and then **MPEG Input Settings** from the main menu.
2. Enter the **IP address**, **Netmask**, and **Gateway** of the MPEG monitoring port that will receive the ABR traffic. The administrator will also need to specify the maximum bandwidth (Mbps) that Sentry ABR may simultaneously request.
3. Next, enter the URLs for the manifests that they are monitoring, as well as a **Name** (required) for the manifest and a **Description** (optional).
4. Click Auto Icon for the ports for which you'd like the system to automatically derive a provider icon based on the input name.
5. Choose the Decrypt/Decode Mode as follows:
   - Http QoS: Does not decode the content. Only performs analysis of the http traffic.
   - In the Clear: A licensable option to decode the mpeg content, but not decrypt.
   - Additional licensable decryption methods
     - Depending on the decryption method selected there will be an icon to click to update the varied decryption key settings.
6. Select **Save Settings** when complete.

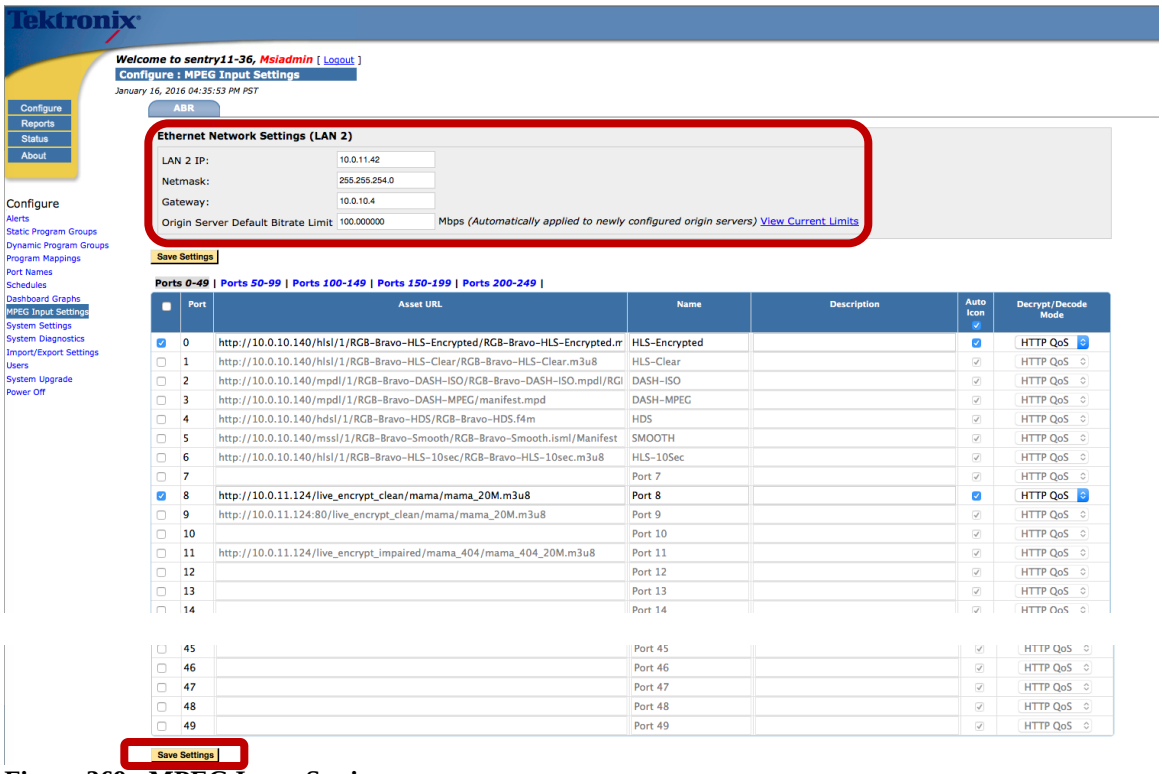


Figure 369: MPEG Input Settings page

Reports

Program Statistics: ABR Stats

For more information on **Program Statistics**, please refer to that section of this manual.

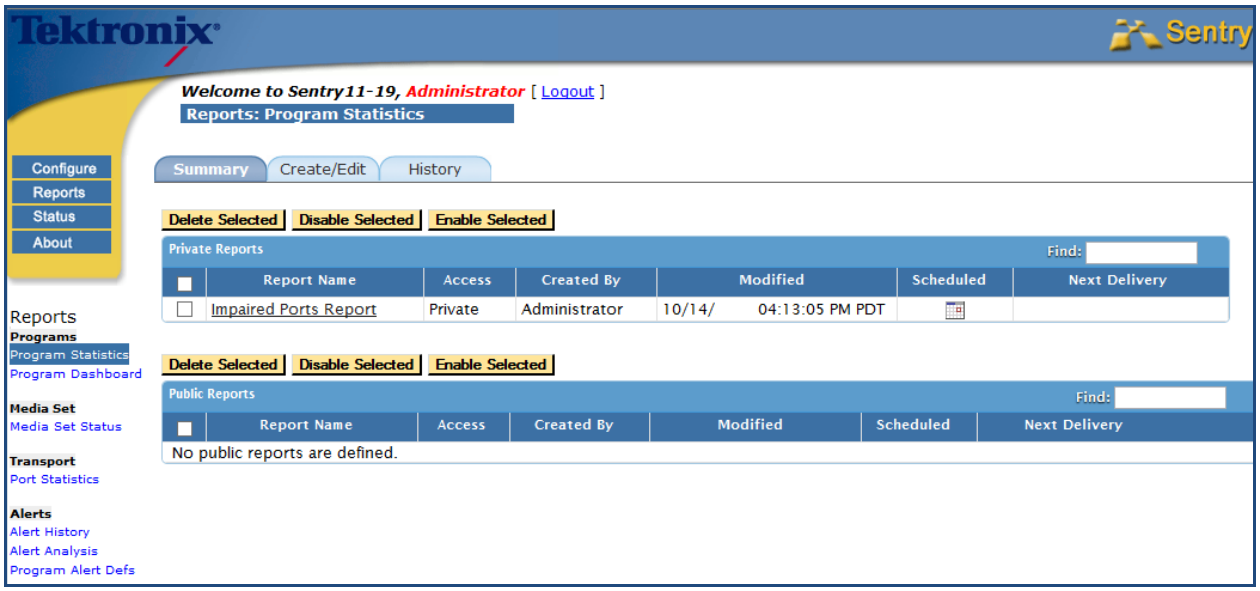


Figure 370: Program Statistics Summary ta

Create/Edit tab

Click the **Create/Edit tab** to create a **Program Statistics** report using ABR information.

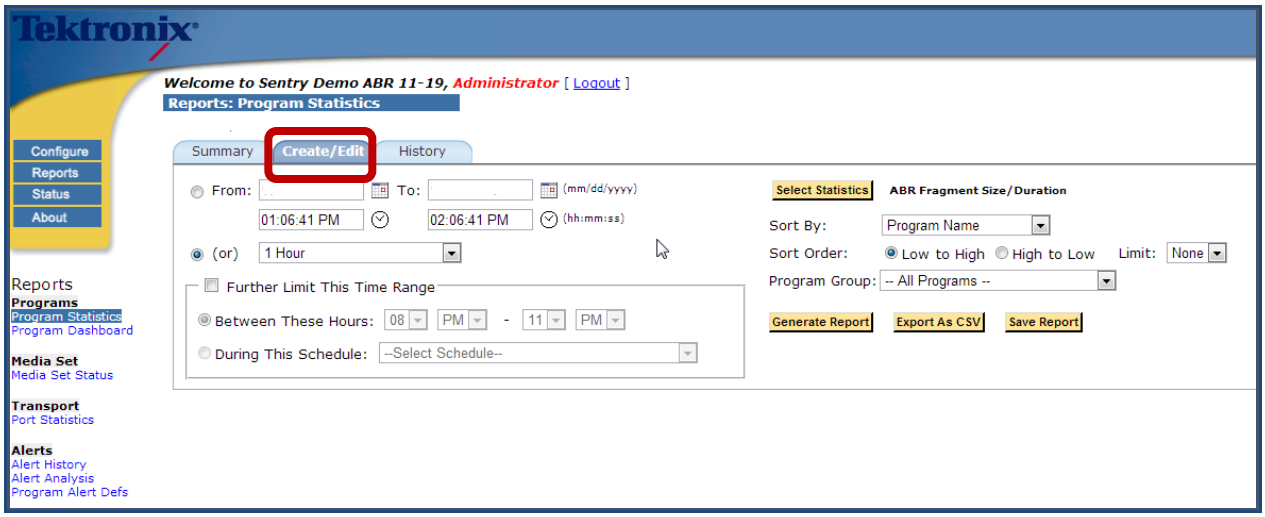


Figure 371: Create/Edit tab

Sentry ABR will return the following data:

- **Port Number**
  The port is the same one as defined **MPEG Input Settings** page
- **Port Name**
  The **Media Set** name as defined in the **MPEG Input Configuration** page
- **TSID**
  Transfer Stream ID (always zero)
- **Program Number**
  Virtual program number
- **Program Name**
  User defined that can be configured by the **Program Mapping Setting**
- **Representation Index**
  The order the **Representation** is listed in the **Manifest file**
- **Manifest Bitrate**
  The bitrate that is listed in the **Manifest file** for the **Representation**
- **Fragment Size/Duration**
  Average Fragment Duration in seconds and **Min/Avg/Max Fragment Size** in Kilobytes/Megabytes
- **Fragment Load Time**
  Min/Avg/Max Fragment Load Time in milliseconds/seconds
- **Fragment Load Bitrate**
  Min/Avg/Max Fragment Load Bitrate in bps
- **Fragment Load Latency**
  Min/Avg/Max Fragment Load Latency in milliseconds/seconds
- **HTTP Status**
  Percentages of HTTP response codes
  - 100s Informational
  - 200s Success
  - 300s Redirection
  - 400s Client Error
  - 500s Server Error
  - Other Non-Http Errors (This percentage will be of total Http Requests)

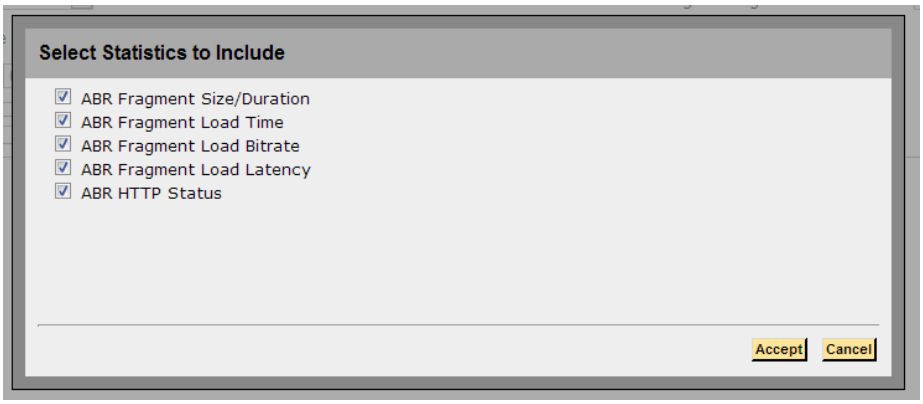


Figure 372: Options for Select Statistics to Include

History tab

View the report history for a selected time period or range.

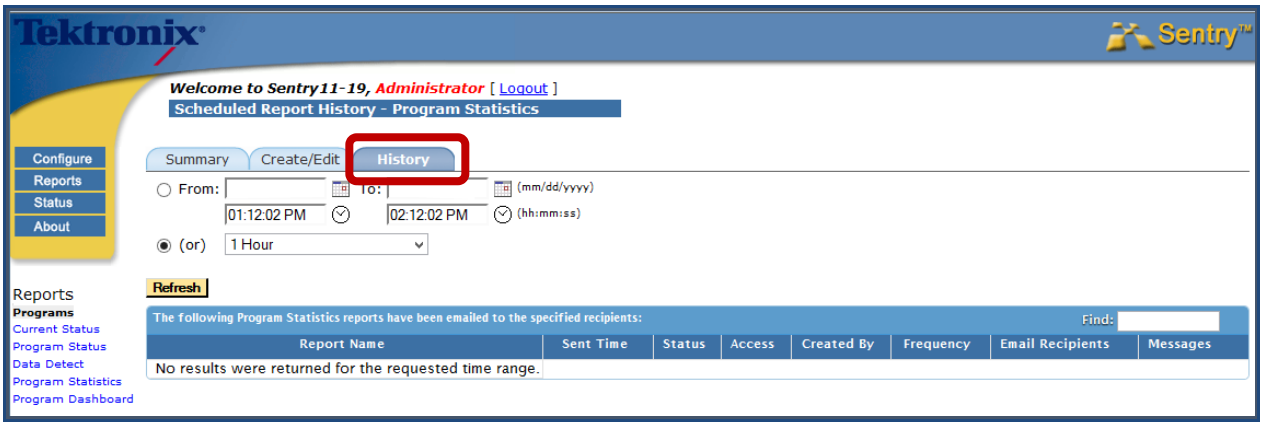


Figure 373: History tab

Port Statistics

Port Statisitics provides non-alert data on a port level that allows you to see ABR information on the transport bitrate and other releveant ABR statistics.

Summary tab

The **Summary tab** shows the list of **Public** and **Private** saved reports.

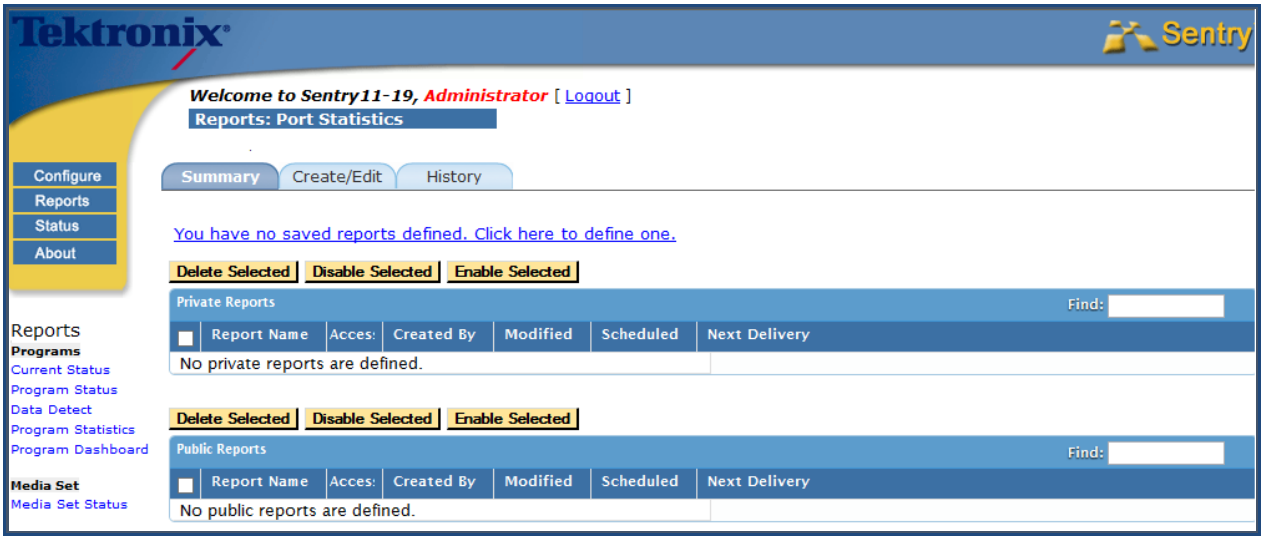


Figure 374: Port Statisitics

Create a Port Statistics Report

8. Select the **Create/Edit tab.**
9. Choose date/time frame for your report.
10. Select **Statistics.**

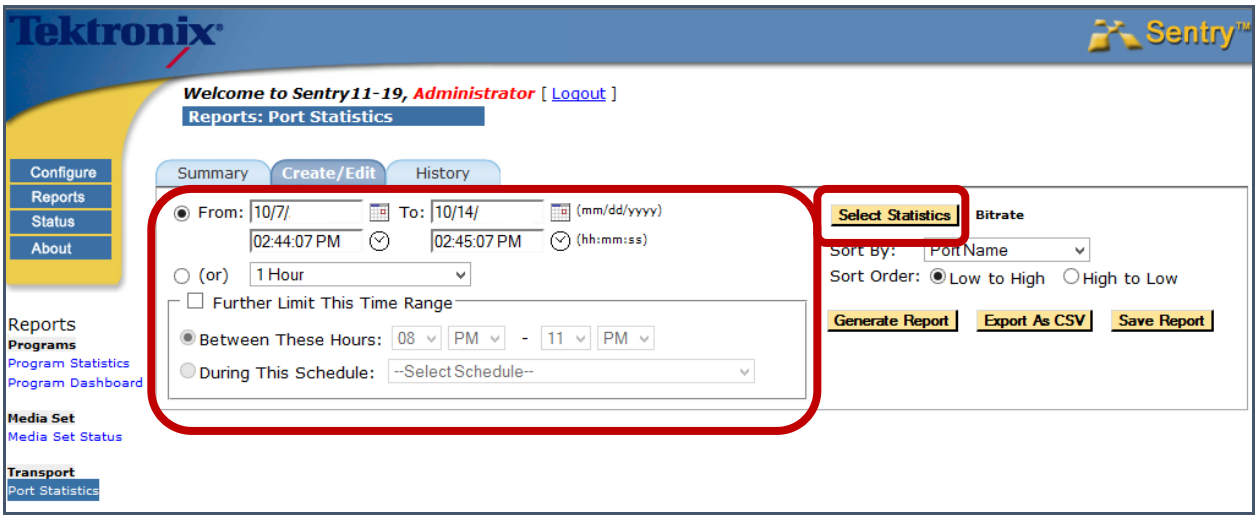


Figure 375: Setting the date or time range

11. Choose any **Statisitics** you to include.
12. Select **Accept.**

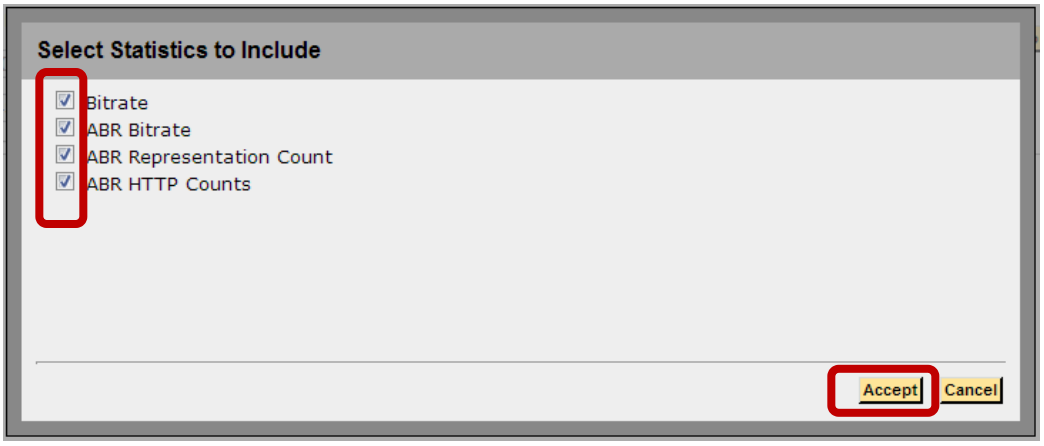


Figure 376: Secting the statistics to include

13. Select any other filter filters you wish to apply.

14. Select **Generate Report.**

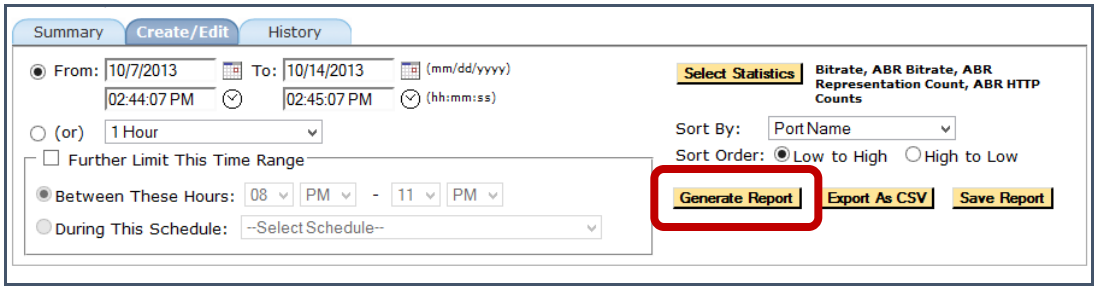


Figure 377: Generate the report

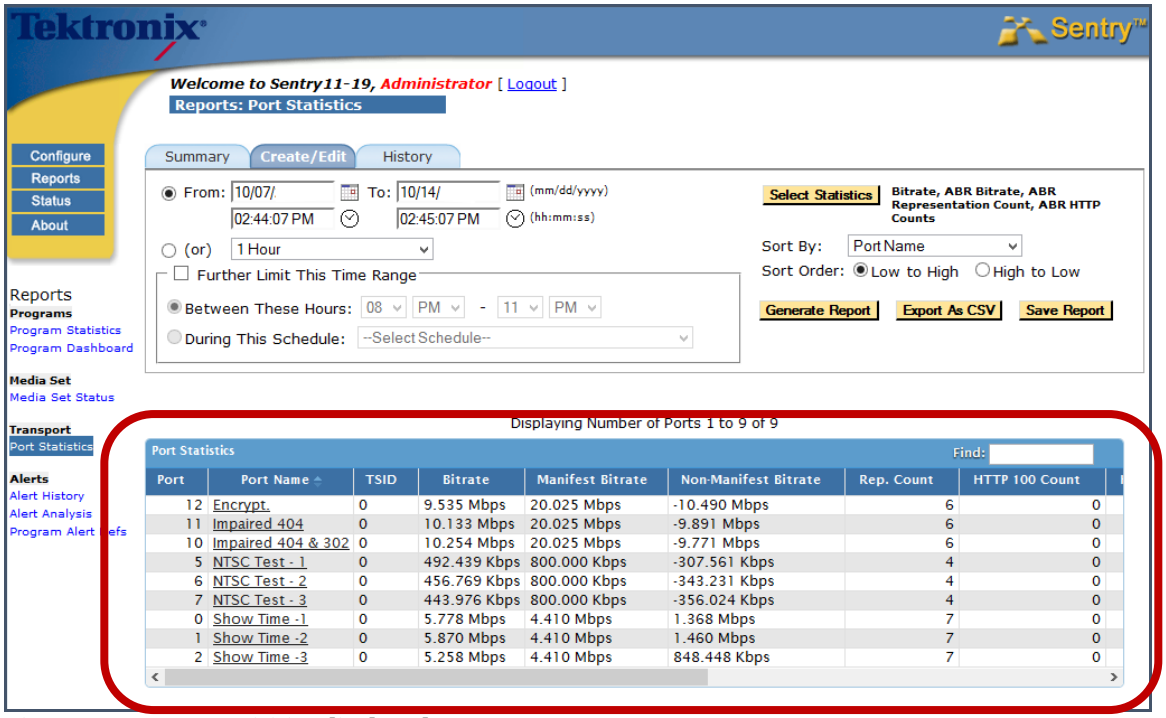


Figure 378: Port Statisitics displayed

- **Port Number**
  The port is the same one as defined MPEG Input Settings page
- **Port Name**
  This is the same as the **Media Set** name name as defined in the **MPEG Input Configuration** page
- **TSID**
- **Bitrate**
  Total Port Bitrate in Mbps
- **Non-Manifest Bitrate**
  Manifest Bitrate and Non-Manifest Bitrate in Kbps/Mbps
- **Rep Count (Representation Count)**
  A count of the number of **Representations** on the **Port**

- **HTTP Counts**
  Counts of the number of HTTP return codes. Columns exist for 100, 200, 300, 400, 500 and Other counts.

Media Set Status Report

The **Media Set Status** report shows the overall health of the monitored content. The **Media Set** shows you the number of **Representations** that are present for each **Manifest File**.

- **Representation**
  A version of the same content at a different resolution or bit rate
- **Media Set**
  A group of **Representations** as defined in the **Manifest File**
- **Manifest file**
  The file that lists all of the **Representations** that are available for the requested service

1. Select **Reports** and **Media Set Status** from the main menu.

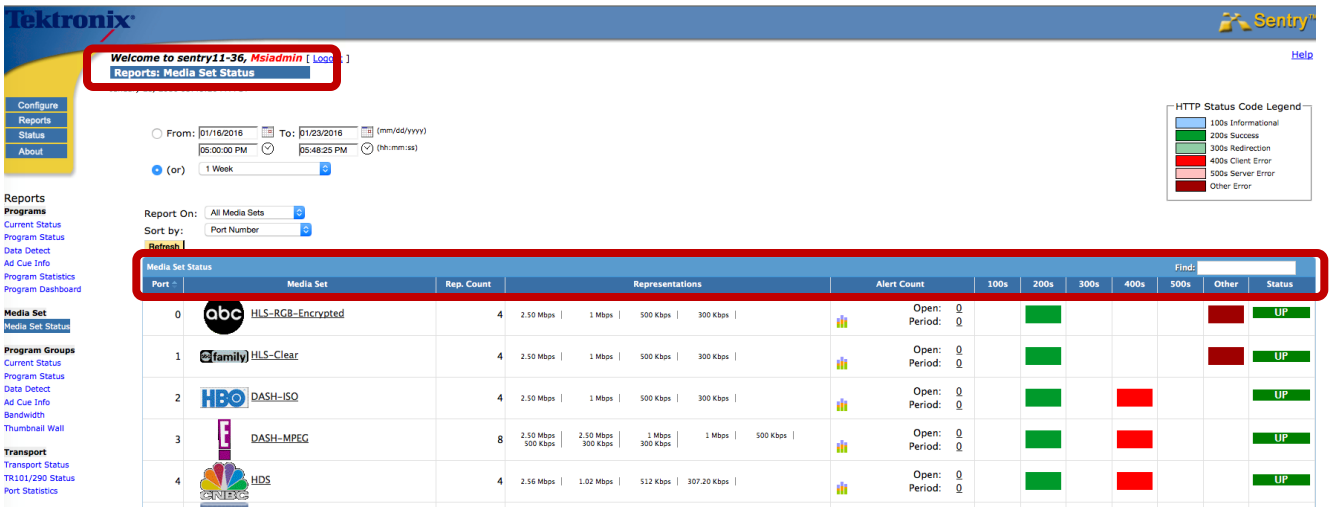


Figure 379: Media Set Status overview

When the report first loads, you will see the following set of information:

- **Port Number**
  The port is the same one as defined **MPEG Input Settings** page
- **Media Set name**
  The name is set in the MPEG Input page.
  A user can click on the **Media Set** name to open the **Media Set Detail Report.**
- **Rep Count (Representation Count)**
  The number of representations listed in the **Manifest** file.
- **Representations**
  A list of all of the bitrates of the **Representations** as listed in the **Manifest** file.
- **Alert Count**
  A count of the **Open and Date/Time Period Alerts**
- **100s, 200s, 300s, 400s, 500s, Other**
  Colored blocks in the columns mean that there are corresponding HTTP return codes for the selected time period.
- **Status**
  Displays the current state of the **Media Sets** as **UP** or **DOWN**

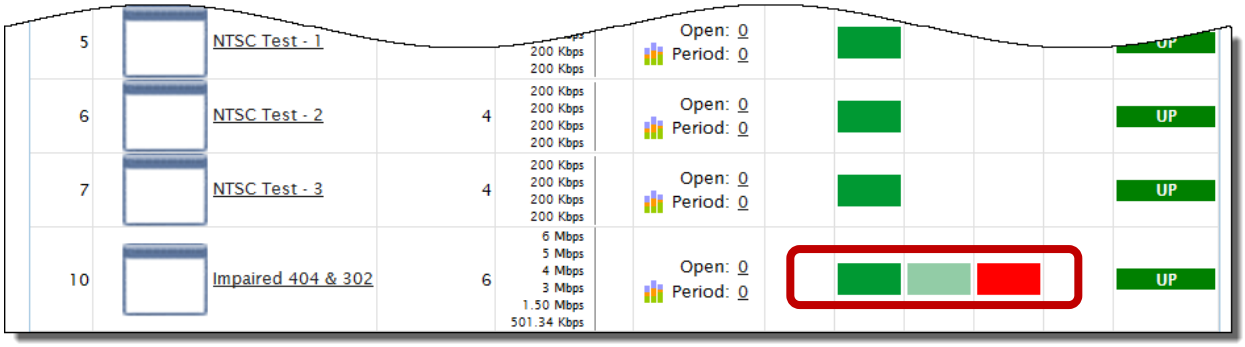


Figure 380: Media Set Status color warnings showing Success, Redirection and Warning

2. Select any program icon from the **Media Set column** to see the **Media Set Details** for that content.

Media Set Details

This report contains several graphs and charts that can be drilled for more detailed information and include:

- **HTTP Status Codes**
- **Representations Statistics**
- **Fragment Load Headroom**
- **Fragment Load Time**
- **Fragment Load Latency**
- **Fragment Load Bitrate**
- **Fragment Size**

HTTP Status Codes

HTTP Status Code shows you a count of all the HTTP return codes by **Representation** for the specified time period. It also allows you to drill down to specific **HTTP Status Code** errors and can show any combination of your specific representations

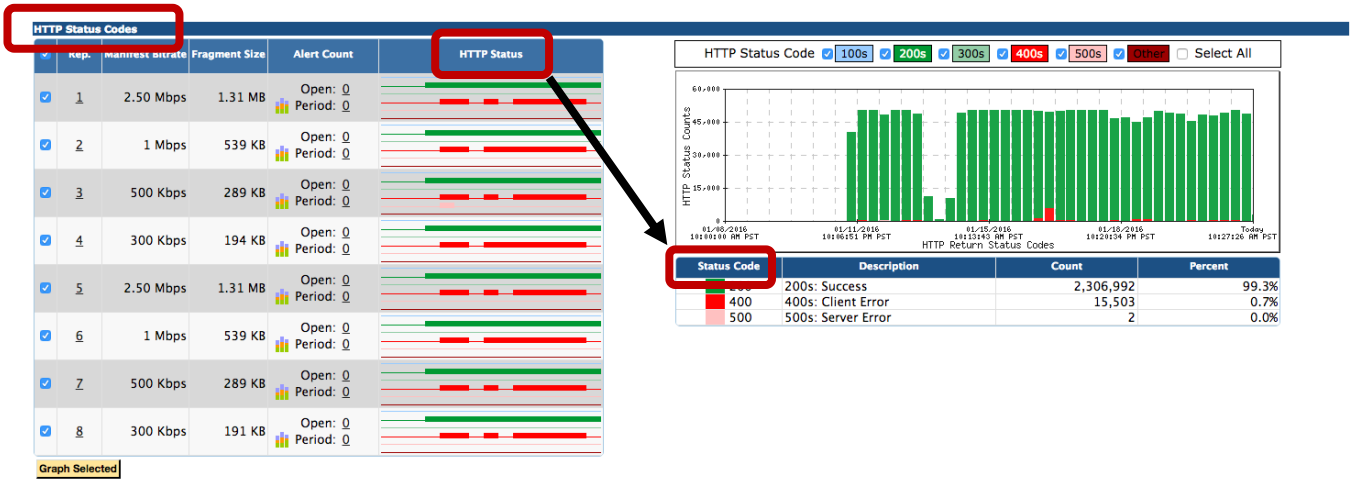


Figure 381: HTTP Status Codes

HTTP Status column allows you to mouse over the **Status Code** bar to get the quantity of status codes over a particular reporting interval.

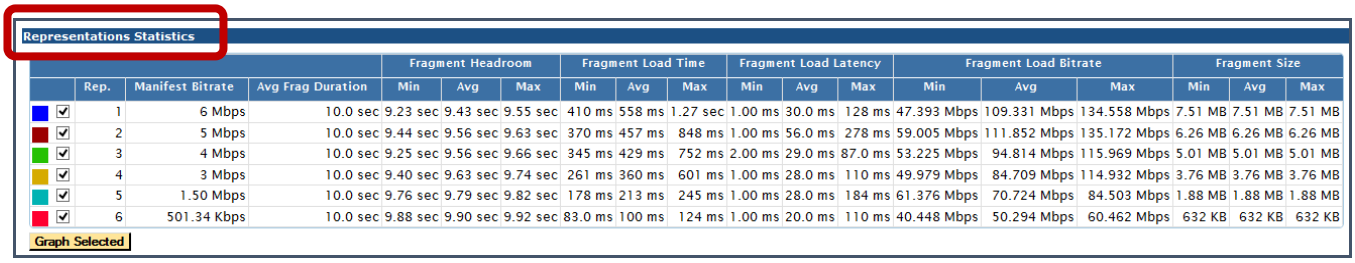
Select the bar to update the **HTTP Status** code graph which will indicate the specific status code error.

Representations Statistics

Representation Statistics provides numeric account of all the statistics Sentry ABR is tracking for all of the representations in the media set. It then charts the following set of information in tabular form and allows you to graph the following statistics:

- **Representation number** as defined in the **Manifest file**
- **Representation bitrate** as defined in the **Manifest file**
- **Average Fragment Duration**

- **Fragment Headroom**
- **Fragment load time**
- **Fragment Load Latency**
- **Report Load Bitrate**
- **Fragment Size**



Representations Statistics

	Rep.	Manifest Bitrate	Avg Frag Duration	Fragment Headroom			Fragment Load Time			Fragment Load Latency			Fragment Load Bitrate			Fragment Size		
				Min	Avg	Max	Min	Avg	Max	Min	Avg	Max	Min	Avg	Max	Min	Avg	Max
☑	1	6 Mbps	10.0 sec	9.23 sec	9.43 sec	9.55 sec	410 ms	558 ms	1.27 sec	1.00 ms	30.0 ms	128 ms	47.393 Mbps	109.331 Mbps	134.558 Mbps	7.51 MB	7.51 MB	7.51 MB
☑	2	5 Mbps	10.0 sec	9.44 sec	9.56 sec	9.63 sec	370 ms	457 ms	848 ms	1.00 ms	56.0 ms	278 ms	59.005 Mbps	111.852 Mbps	135.172 Mbps	6.26 MB	6.26 MB	6.26 MB
☑	3	4 Mbps	10.0 sec	9.25 sec	9.56 sec	9.66 sec	345 ms	429 ms	752 ms	2.00 ms	29.0 ms	87.0 ms	53.225 Mbps	94.814 Mbps	115.969 Mbps	5.01 MB	5.01 MB	5.01 MB
☑	4	3 Mbps	10.0 sec	9.40 sec	9.63 sec	9.74 sec	261 ms	360 ms	601 ms	1.00 ms	28.0 ms	110 ms	49.979 Mbps	84.709 Mbps	114.932 Mbps	3.76 MB	3.76 MB	3.76 MB
☑	5	1.50 Mbps	10.0 sec	9.76 sec	9.79 sec	9.82 sec	178 ms	213 ms	245 ms	1.00 ms	28.0 ms	184 ms	61.376 Mbps	70.724 Mbps	84.503 Mbps	1.88 MB	1.88 MB	1.88 MB
☑	6	501.34 Kbps	10.0 sec	9.88 sec	9.90 sec	9.92 sec	83.0 ms	100 ms	124 ms	1.00 ms	20.0 ms	110 ms	40.448 Mbps	50.294 Mbps	60.462 Mbps	632 KB	632 KB	632 KB

Graph Selected

Figure 382: Representations Statistics

Fragment Load Headroom

Fragment Load Headroom allows for a safety margin in the fragment request timeline. It is the fragment duration minus the fragment load time and shows the **Min/Avg/Max** headroom in seconds.

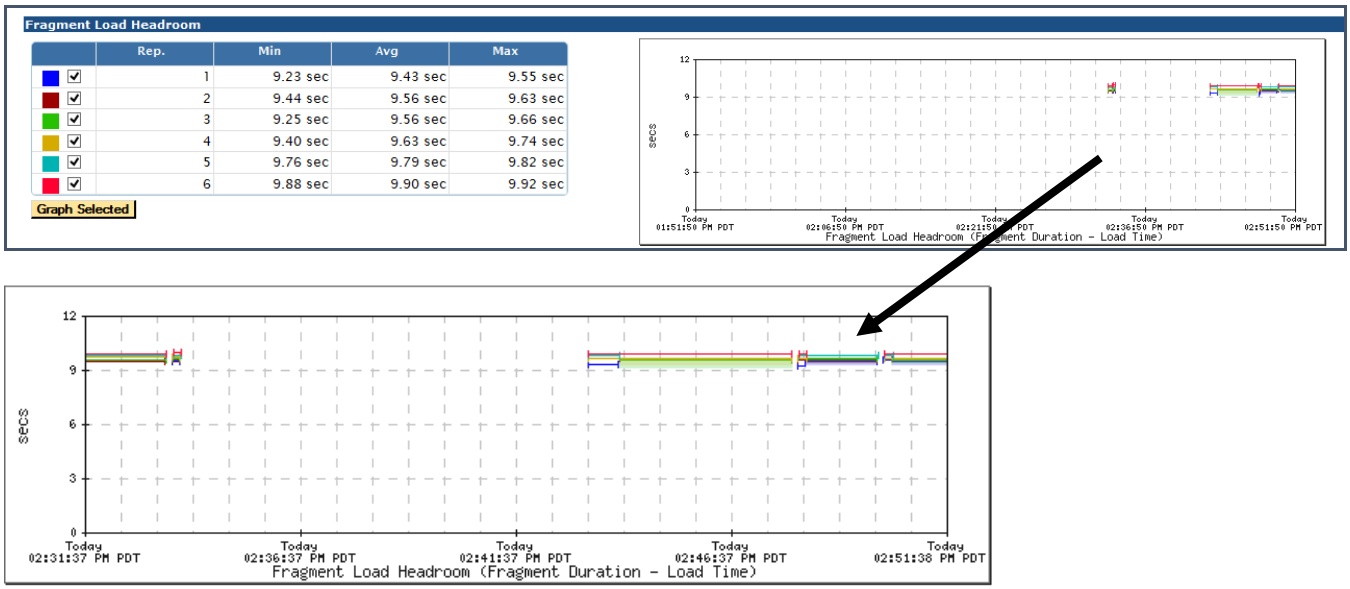


Figure 383: Fragmemt Load Head and graph drill down

Fragment Load Time

Fragment Load Time is the time measured between when the HTTP header for a fragment is detected and when enough bytes have been received to equal the fragment size**.** It shows the **Min/Avg/Max** of the loadtime in milliseconds.

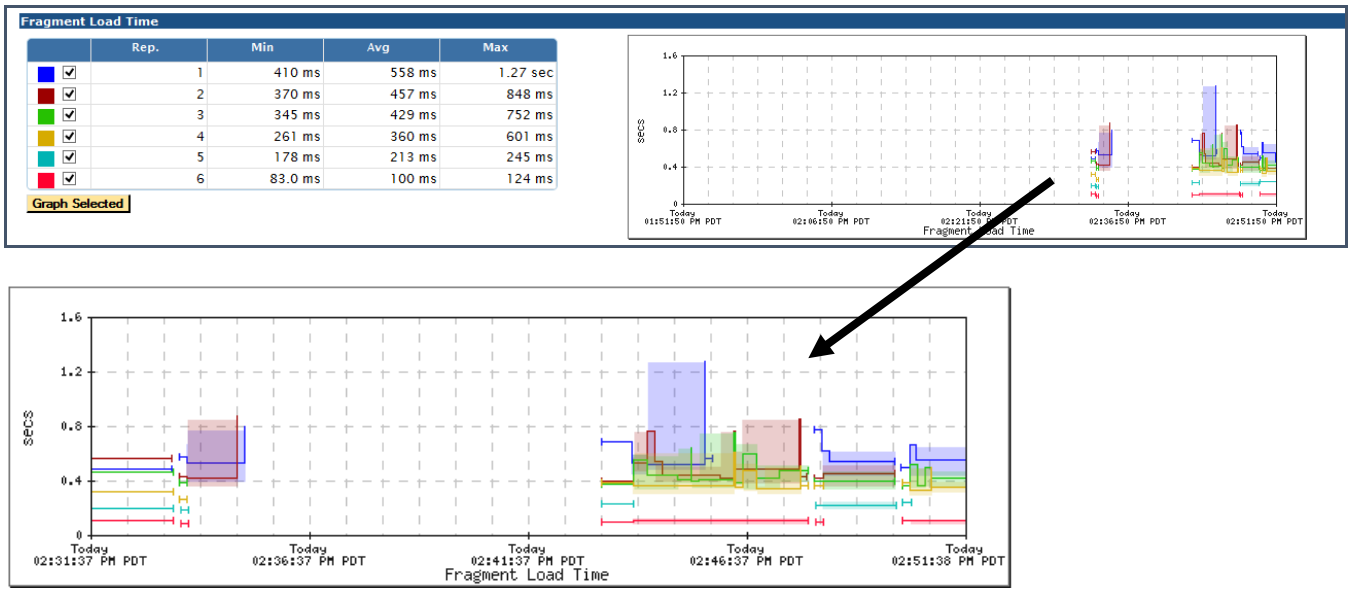


Figure 384: Fragmemt Load Time and graph drill down

Fragment Load Latency

Fragment Load Latency is the time between when a request is made for a fragment (at the socket level) and when the HTTP header for the fragment is detected. It shows the **Min/Avg/Max** latency in milliseconds.

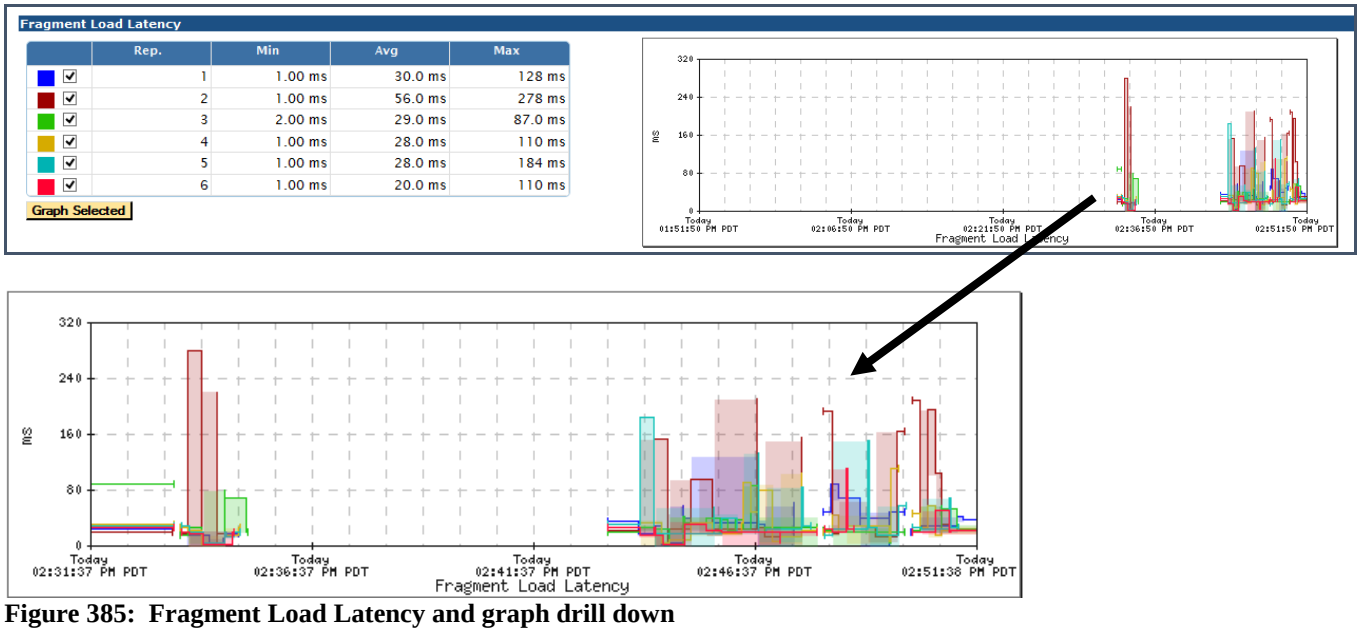


Figure 385: Fragment Load Latency and graph drill down

Fragment Load Bitrate

Fragment Load Bitrate is the fragment size / fragment load time shows the **Min/Avg/Max** bitrate in Kbps or Mbps.

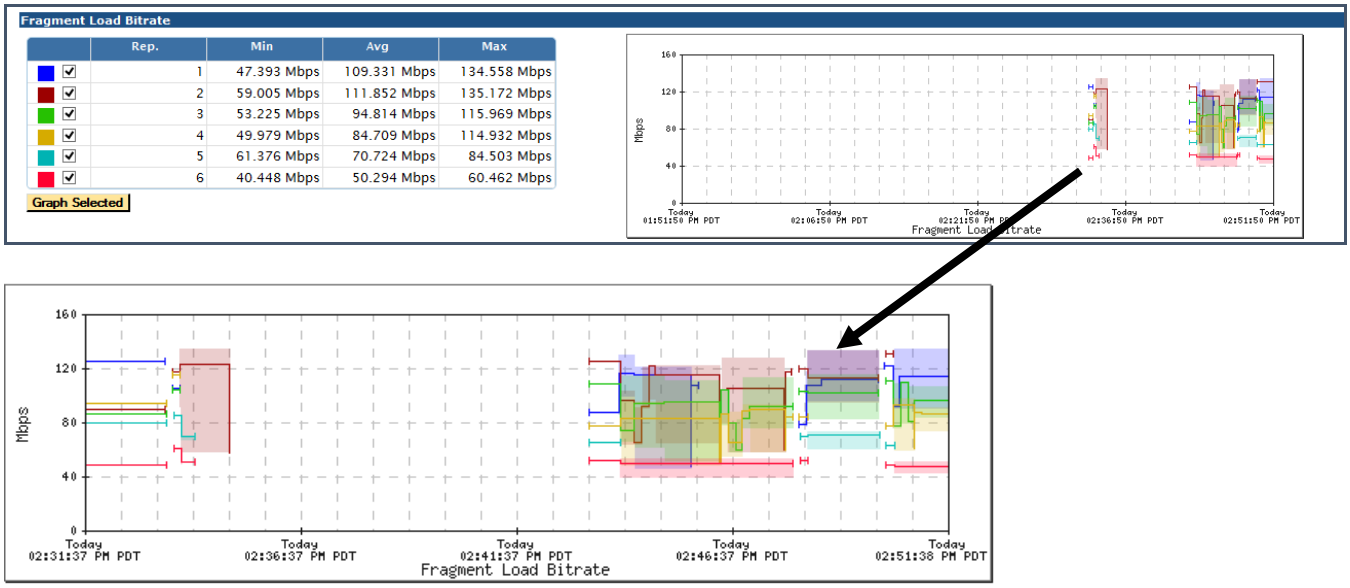


Figure 386: Fragment Load Bitrate and graph drill down

Fragment Size

Fragment Size shows the **Min/Avg/Max** size in Kilobytes or Megabytes.

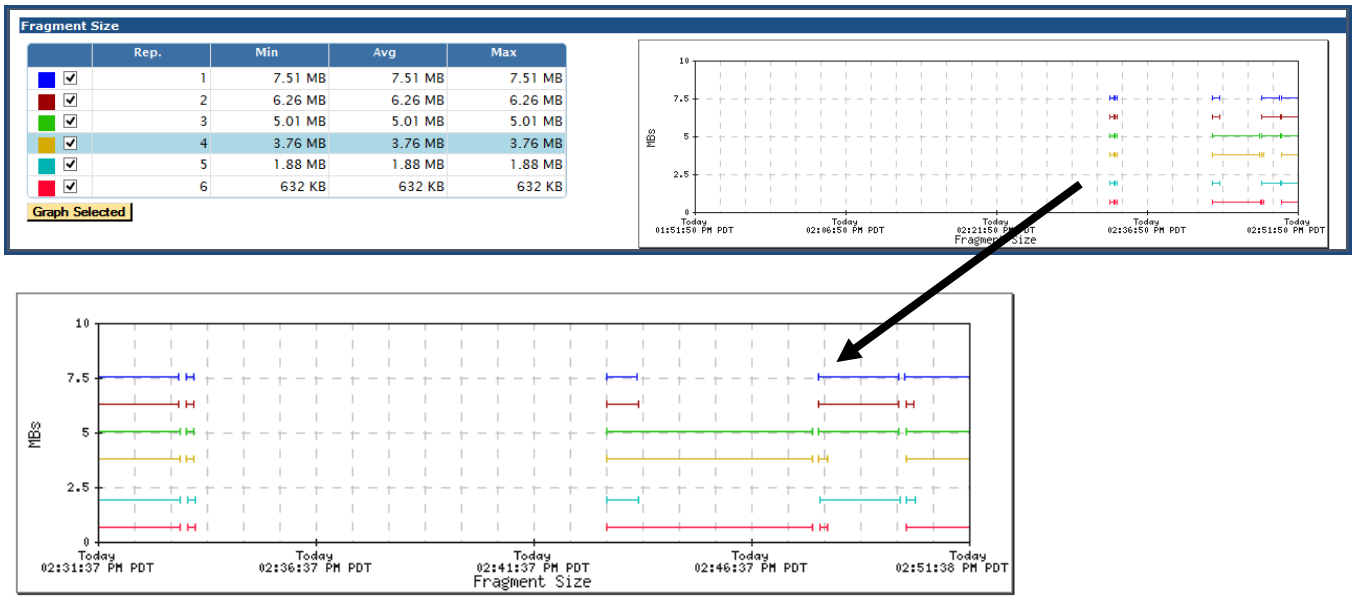


Figure 387: Fragment Size and graph drill down

System Status

The **System Status** report gives you an overview of each inbound rate port overall information.

Select **Status** from the main menu.

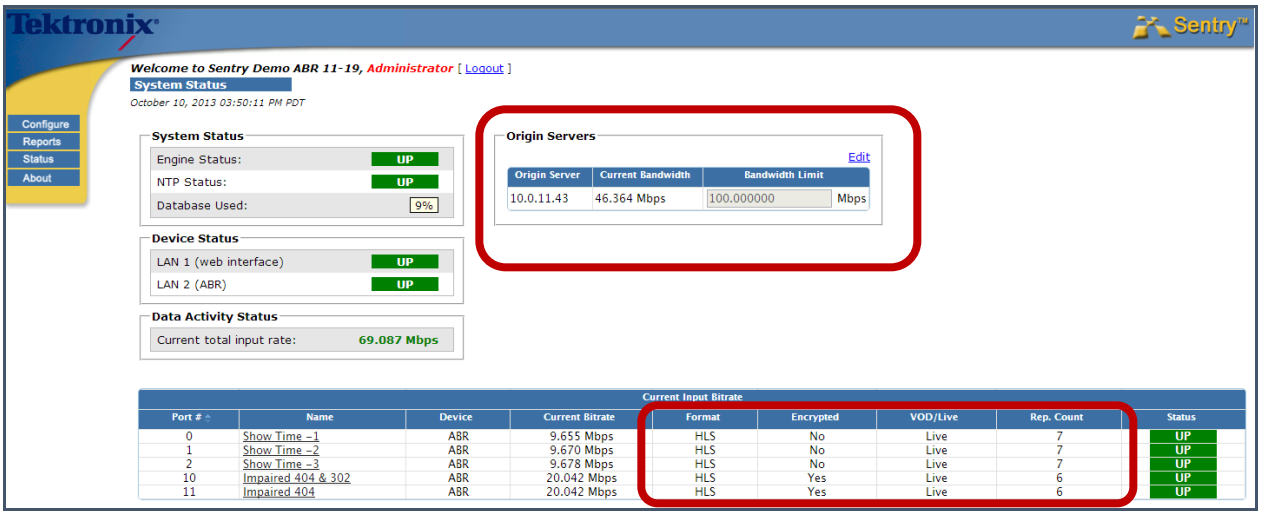


Figure 388: System Status screen

- **Origin Servers**
  Provides a list of the servers being monitored,the Current Bitrate (the sume of the Current Bitrate for all the Media Sets on that server) and the Bandwitdth Limit. The Bandwith Limit column shows the defined limits for each server and is editiable from this location.
- **Current Intput Bitrate**
  - **Port #**
    The port is the same one as defined MPEG Input Settings page
  - **Name**
  - The **Media Set** name as defined in the **MPEG Input Configuration** page
  - **Device**
    Type of traffic
  - **Current Bitrate**
    Total bitrate of all the **Representations** on that port
  - **Format**
    The type of ABR traffic being monitored. (HLS, DASH,) etc.)
  - **Encrypted**
    Shows if the stream is encrypted or not.
  - **VOD/Live**
    Shows if content is LIVE or On Demand (VOD)
  - **Rep. Count**
    A count of the reprisentations avialiable in the stream
  - **Status**
    Shows **UP** or **DOWN**

Appendix B: Sentry Edge, Edge II, Edge III-S, and Edge III-T

Preface

This user manual for the Tektronix Sentry Edge™, Sentry Edge II™, Sentry Edge III-S™ and Sentry Edge III-T™ Video Quality Monitor describes how to configure, control, and use the product.

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

NOTE: *See the Sentry Series Installation and Safety Instructions manual that was supplied with the product for instructions on how to install the instrument.*

Getting started

Product description

Sentry Edge, Sentry Edge II, Sentry Edge III-S and Sentry Edge III-T are the high-performance, high-density RF monitoring solutions from Tektronix. The product detects transport stream and RF modulation errors generated by equipment errors or failures, and provides reporting and alerting capabilities for services in the RF and TS domains. All Sentry Edge products deliver high quality RF measurements at scale for 24/7 video monitoring environments economically.

Sentry Edge II takes RF monitoring to the next level with monitoring density of 4 or 8 tuners per unit. More tuners per unit reduce the time to round robin, so RF issues can be identified sooner. Customers can round robin or park on any of the tuners, or chose any combination of these options. Sentry Edge III-S provides 2 tuners.

Sentry Edge II and Edge III provide excellent MER performance across the entire frequency range to let service providers detect a drop in signal quality before there is impact to subscribers.

Figure 389: Sentry Edge Video Quality Monitor

Sentry Edge is designed to deliver precision measurements at scale in fast-paced video network environments. The product provides comprehensive, highly accurate RF measurements to speed problem isolation.

The Sentry family of video quality monitoring products comprise a S2E (Source-to-Edge) monitoring solution. This solution is a comprehensive 24/7 real-time monitoring system with a 60-day historical database, executive reports, and trending analysis. Multiple Sentry Edge units can be managed using the Medius Application Manager.

As shown below, all Sentry Edge products monitor the edge of the video network just before content is sent to subscriber homes. It can also be used at headends for QAM HFC distribution monitoring.

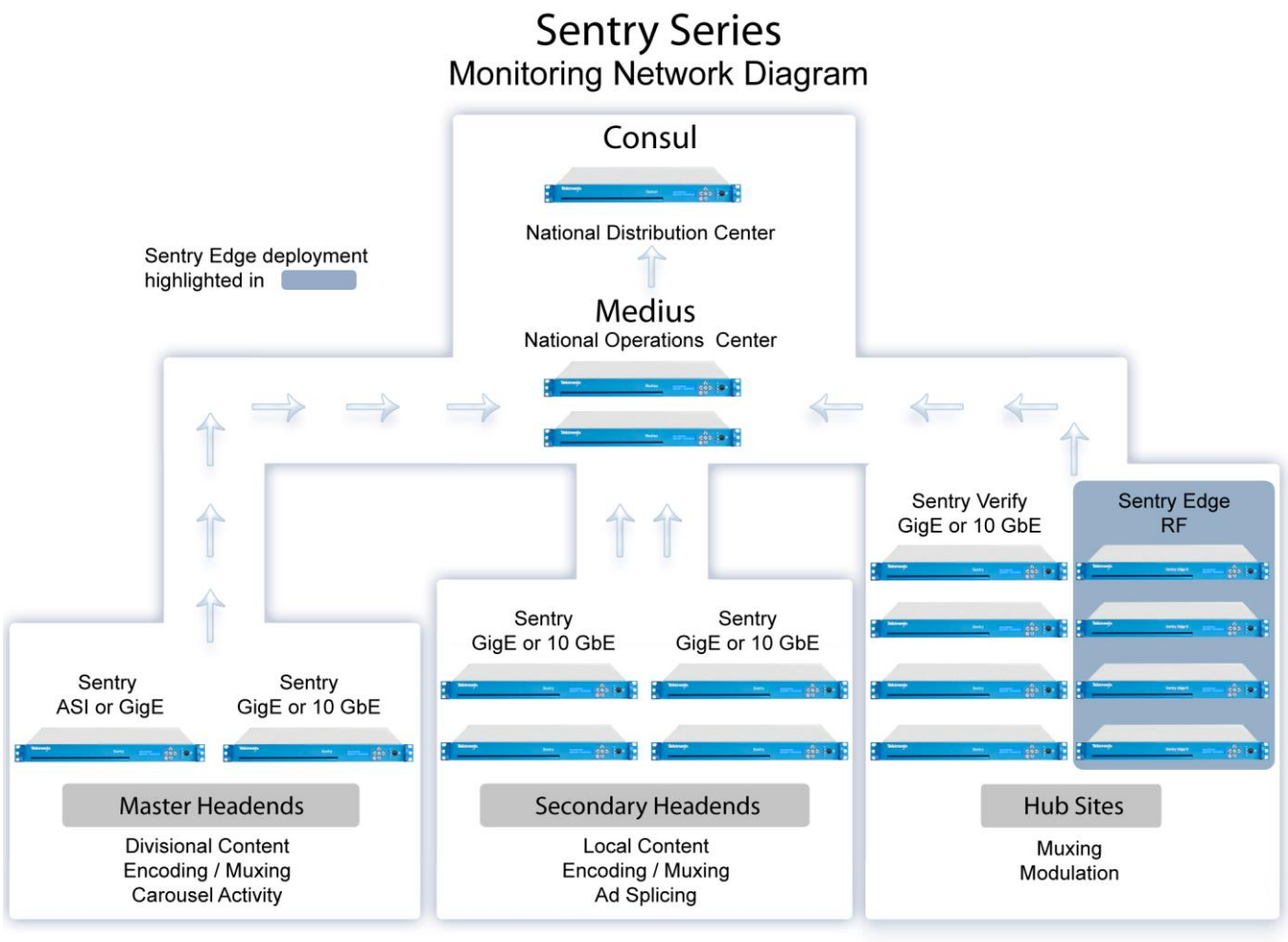


Figure 390: Sentry monitoring network diagram

Sentry Edge RF Monitoring Products

- Edge I: Dual Tuner 8VSB and/or QAM B
- Edge II: Single Input 4 Tuner or Dual Input 8 Tuner QAM A/B/C
- Edge III-S: Dual Satellite DVB-S/S2
- Edge III-T: Single Input Dual Tuner DVB-T/T2

Sentry Edge Family Features and benefits

- Remote management of RF measurement collection
- Proactively detect RF issues before they impact subscribers
- Full range of Transport Stream monitoring capabilities
- 1RU footprint minimizes rack space and power costs
- Highly scalable solution where multiple units can be managed by the Medius Application Manager
- Additional service monitoring capabilities available for QAM channels in the clear: audio/video QoE, perceptual video quality (PVQ), Ad Verification, EBIF, tru2way™, MHP, and DSM-CC carousel analysis

Sentry Applications

- RF measurements post-QAM at the hub and at headends where QAM is used
- Multiple RF inputs to simultaneously monitor from different sources
- Graphing for one or both RF inputs at the same time
- MER measurements for quick detection of demodulation issues
- Comprehensive RF reporting for targeted, rapid problem isolation
- Cost-effective solution enables more effective monitoring of the network edge
- Remote management of RF measurement collection saves time and money for providers now collecting data in the field

Sentry Edge I Features and benefits

- Dual Tuner
- 8VSB for reception of ATSC-1 signals.
- QAMB 64/256 for North American Cable
- QAM RF Measurements include:
  - RF Lock Indication
  - Input Signal Strength
  - MER
  - CNR
  - Pre-RS BER
  - Post-FEC Uncorrectable TS Packet Count
  - Carrier Offset
- Monitors RF signals up to 850 MHz

Sentry Edge II Features and benefits

- High-density solution: 2 RF inputs with 8 parallel QAM tuners or 1 RF input with 4 tuners
- Analyzer-quality QAM RF Measuring Capability. RF Measurements include:
  - RF Lock Indication (including LED on rear panel)
  - Input Signal Strength (Channel Power) EVM
  - MER
  - CNR
  - Pre-RS BER
  - Post-FEC Uncorrectable TS Packet Count
  - Carrier Offset
- Constellation diagram provided for diagnostics
- Monitors RF signals up to 1 GHz
- QAM A/B/C support

Sentry Edge III-S Features and Benefits

- Analyzer-quality QPSK/APSK RF Measuring Capability. RF Measurements include:
  - RF Lock Indication (including LED on rear panel)
  - MER
  - CNR
  - Pre-RS BER
  - Post-FEC Uncorrectable TS Packet Count
- Constellation diagram provided for diagnostics
- Supports two channels in QPSK / 8-PSK mode

Sentry Edge III-T Features and Benefits

- Monitor DVB-T and DVB-T2 Terrestrial Broadcasts.
- Analyzer-quality RF Measuring Capability. Measurements include:
  - RF Lock Indication (including LED on rear panel)
  - MER
  - CNR
  - Pre-RS BER
  - Post-FEC Uncorrectable TS Packet Count

Standard and optional accessories

You should receive the following accessories with your instrument:

Item	Tektronix part	Description
Sentry Series Installation and Safety Instructions	071-3007-xx	Describes how to install the product and provides important safety precautions to avoid injury and prevent damage to this product or any products connected to it
Sentry Series User Manual (This Manual)	077-3202-xx	Describes how to configure, control, and operate the product
Power cord	NA	The power cord option you ordered

Power cord options

Option	Description
A0	North America power
A1	Universal EURO power
A2	United Kingdom power
A3	Australia power
A4	240 V, North America power
A5	Switzerland power
A6	Japan power
A10	China power
A11	India power
A12	Brazil power
A99	No power cord or AC adapter

Configuration

NOTE: ***See the Sentry Series Installation and Safety Instructions manual that was supplied with the product for instructions on how to install the instrument.***

Recommended steps

Listed below are the recommended steps for configuring the Sentry Edge instrument. The tasks are shown in their most beneficial order.

1. Configure the management port. Instructions are located in the **Configure System Settings** section of the ***Sentry Series Video Quality Monitor User Manual***.
2. On the back of the instrument, connect the RF cable to the rightmost F-connector on the RF card.
3. Next, set the RF Connection level to 0 dbmv from the output of the RF patch.
4. Define or import your desired channel plan.
   To define/edit import settings for an RF configuration see **To define/edit import settings for an RF configuration** below.
   To update the schedule/import schedule information see **Update the schedule/import schedule information** below.
5. From **RF Input Connection**, select the desired **Active RF Input Configuration** and select **Save RF Settings**.
6. From **Input Settings**, select any ports which need to be disabled.
7. Configure the **Program Mappings**. Instructions are located in **Configure Program Mappings** of the ***Sentry Series Video Quality Monitor User Manual*** or ***the Medius Application Manager User Manual***.
8. Add the Sentry Edge, Edge II or Edge III instrument to Medius, if one is available. Instructions are located in **Configure: Add Sentrys** of the ***Medius Application Manager User Manual***.
9. Build the desired **Medius Program Group**, if one is available. Instructions are located in **Reports: Program Group Bandwidth** of the ***Medius Application Manager User Manual***.
10. Build the desired **RF Stats alerts**. Instructions are located in **Alerts** of the ***Sentry Series Video Quality Monitor User Manual*** or the ***Medius Application Manager User Manual***.

NOTE***: RF Stats alerts cannot be defined in a template. You need to define them individually.***

11. Create the desired alerts. Instructions are located in the **Creating a Program.**
12. Alert section of the ***Medius Application Manager User Manual***.

Configure the RF Stats Alerts

Configuring alerts in Sentry Edge works much like the process in Sentry. Additionally, you may configure RF Stats Alerts to alert you when the selected RF statistic (for example, CNR, MER, or EVM) goes above or below a certain value.

1. Select **Configure** and then **Alerts**.
2. Under **Transport Alerts**, find **RF Stats Alerts** and then select **Create**.

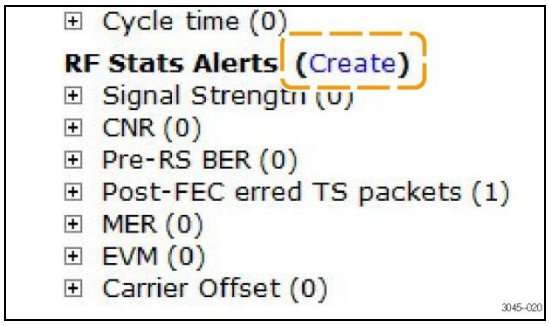


Figure 391: Creating an RF Stats Alert

3. Proceed through Sections 1-3 as described in the *Configure Alerts* section of the ***Sentry Series Video Quality Monitor User Manual.***

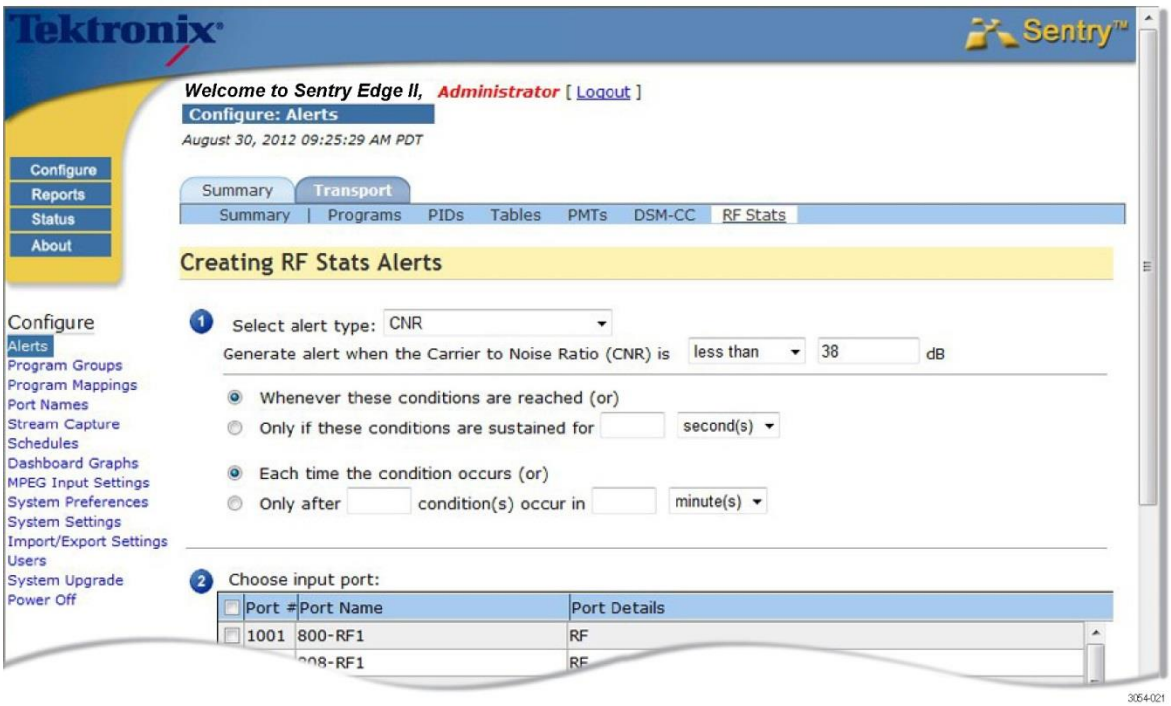


Figure 392: Creating a CNR alert

Configure the MPEG settings

Sentry Edge and Edge II offer 2 RF inputs with 8 parallel QAM tuners or 1 RF input with 4 tuners. Sentry Edge III-S has two inputs and two tuners, whereas Sentry EdgeIII-T has a single input with a tuner. The tuners incorporate a round-robin approach to monitor all of the frequencies in the active configuration.

The tuners each tune every few seconds, perform an analysis and then tune to the next frequency

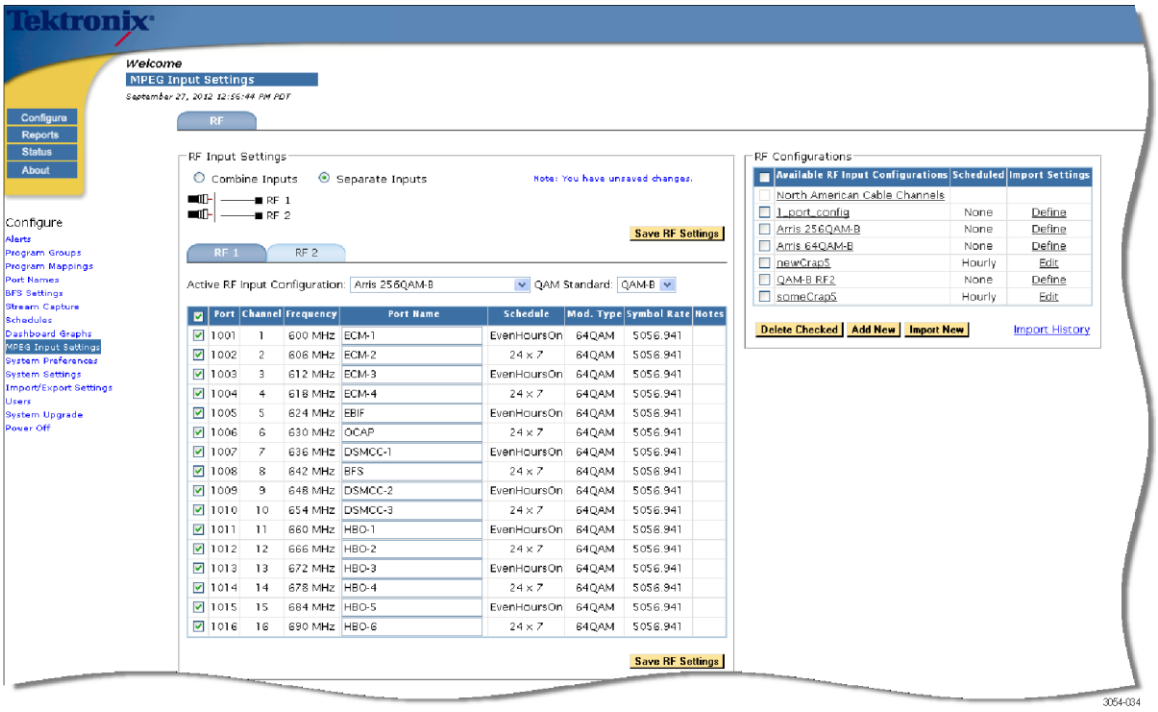


Figure 393: RF Input Settings overview (8 tuner model)

- **RF Input Settings**

  Lists the frequency and **Port Name** information about the channels in the active configuration and lets you customize a port name for each of the channels. You can also enable and disable (stops polling for that channel) the channels by selecting the check boxes as needed. Disabling stops the polling for that channel.

  On the 8-tuner configuration, you are given the option of combining the inputs. This gives you one "tuner pool" or one virtual RF input with 8 tuners. You can also select to have separate inputs. This gives you two separate RF inputs with 4 tuners each.

- **RF Configurations**

  Lists all of the currently defined configurations and allows you to edit them using the underlined name. You may also define/edit import settings.

  - **Delete Checked** deletes all checked items
  - **Import New** allows you to import a configuration from a CSV file
  - **Import History** displays the import history of all scheduled RF imports

Activate an RF input connection

1. Select an input connection from the drop down menu.

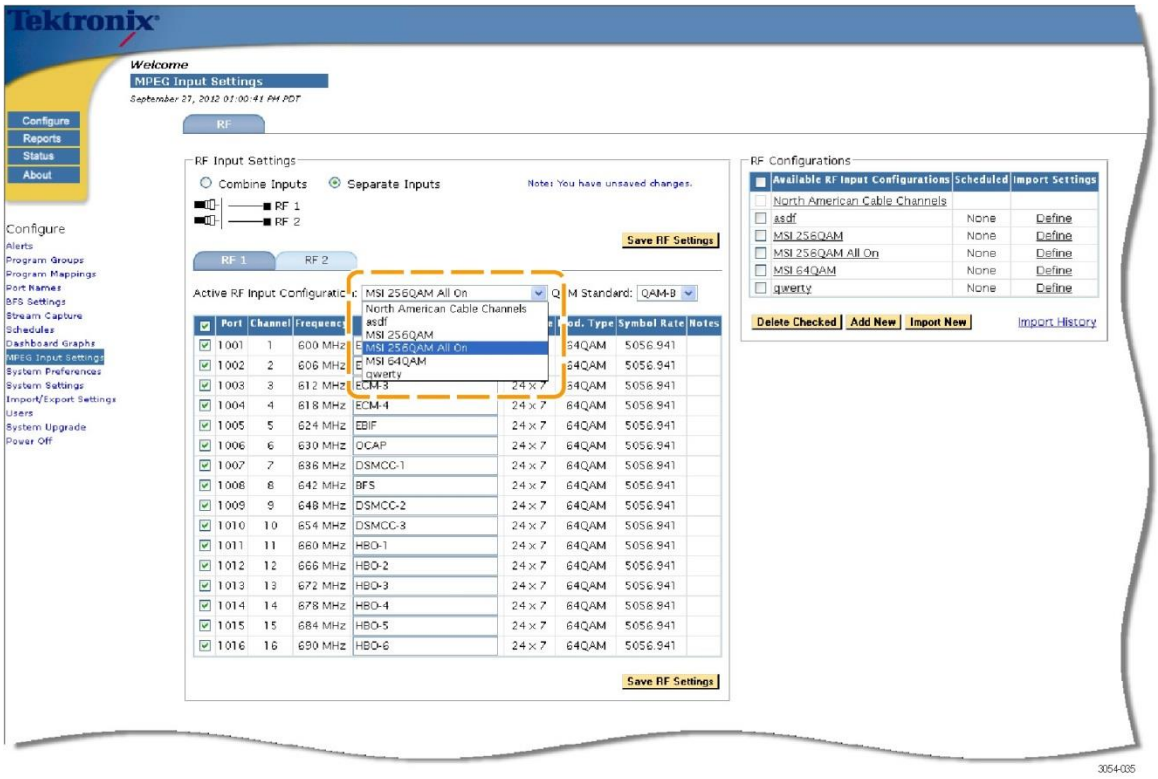


Figure 394: RF Input Connection drop-down menu

2. Click **Save RF Settings** when finished.

To define/edit import settings for an RF configuration.

Note: Not available on Sentry Edge III-S and Sentry Edge III-T.

The following steps are for working with an already existing RF configuration where you are changing the settings for the selected configuration.

1. Select **Define** in the far right hand column.

Figure 395: Defining RF configurations

2. On the resulting page, complete fields as necessary in the **Import Settings** section.

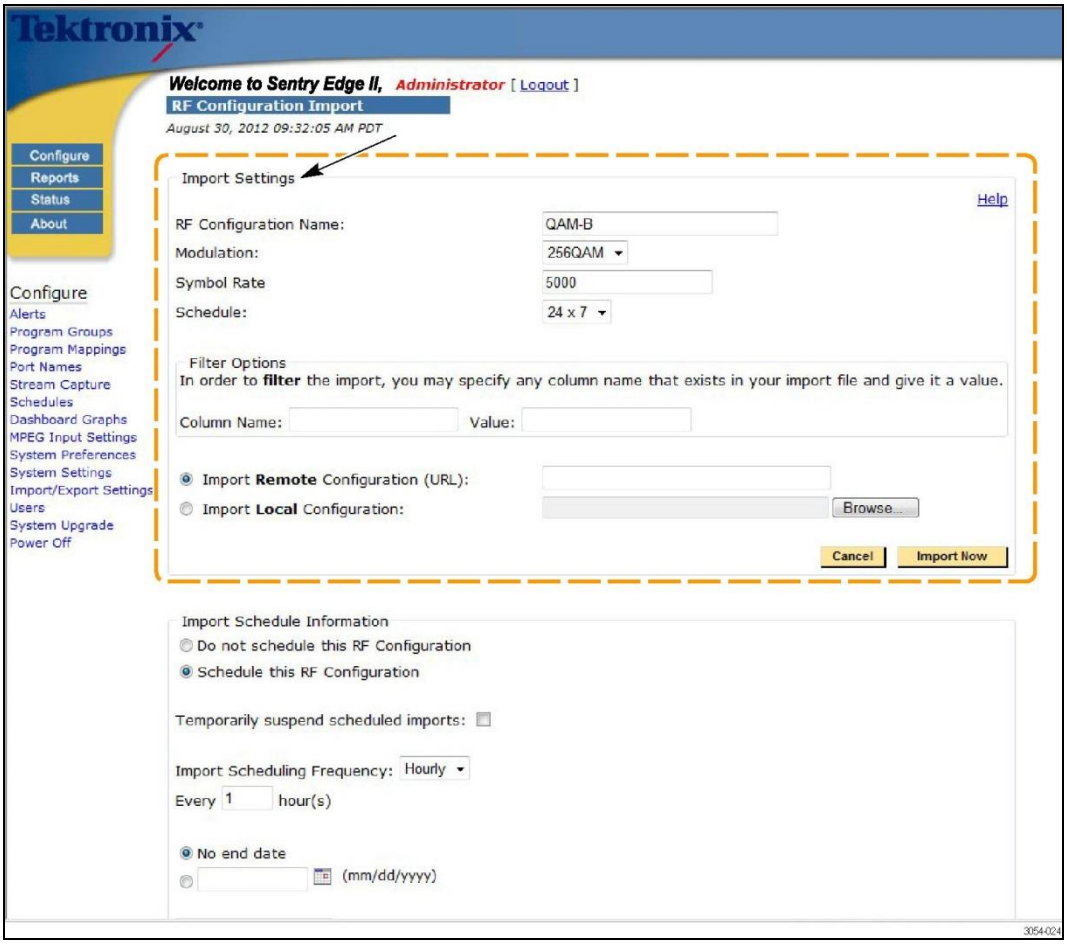


Figure 396: RF Configuration Input screen

- **RF Configuration Name**
  The unique name of the configuration being used.
- **Modulation**
  The desired modulation type (64 QAM, 256 QAM, etc.).
- **Symbol Rate**
  A parameter of the receiving demodulator that needs to be set accurately in order to properly demodulate the signal. These demodulation parameters should be provided by the manufacturer of your modulation equipment.
- **Schedule**
  Specifies the monitoring schedule for this RF configuration; normally this will be 7x24 but it can be customized.

Filter options

- **Column Name**

  The name of the column in your existing spreadsheet which needs to be renamed to match one of our supported column names (Tuned Channel, Frequency, MPEG Source # or Source Name) for the import to work correctly.

- **Value**

  The value you want the column to be re-named to (Tuned Channel, Frequency, MPEG Source # or Source Name).

- **Import configuration (URL)**

  The URL where the configuration is located. For use with a shared file server where there exists a preconfigured CSV file formatted with columns for input into the Sentry (Tuned Channel, Frequency, MPEG Source # or Source Name). Sentry Edge supports HTTP or FTP.

- **Import Local Configuration**

  Allows you to browse your local hard drive for the configured CSV file to be imported.

NOTE: *Select the Help button to view options for column names as shown below.*

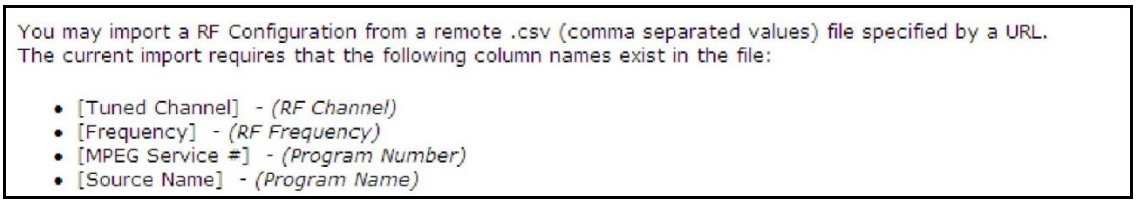


Figure 397: Online help column names

3. When finished, select **Import Now**.
4. If you wish to schedule this configuration, proceed to the *To update the schedule/import schedule information* section in this manual.
5. If you do not want to schedule the configuration, select **Do not schedule this RF Configuration** and then **Update Schedule**.

Update the schedule/import schedule information

1. After you complete the **Import Settings** configuration, if you wish to schedule the import, select the checkbox for **Schedule this RF Configuration**.

2. Select the frequency to update the configuration from the **Import Scheduling.**
   a. **Frequency** drop-down menu (**Hourly**, **Daily**, etc.).

3. Enter the desired frequency time frame (1 hour, 2 hour, 1 day, 2 days, etc).

4. If applicable, set the **Import Schedule** end date. This is used when an import location is temporary or if you do not wish to continue automatic updates after a certain period.

5. Select **Update Schedule**.

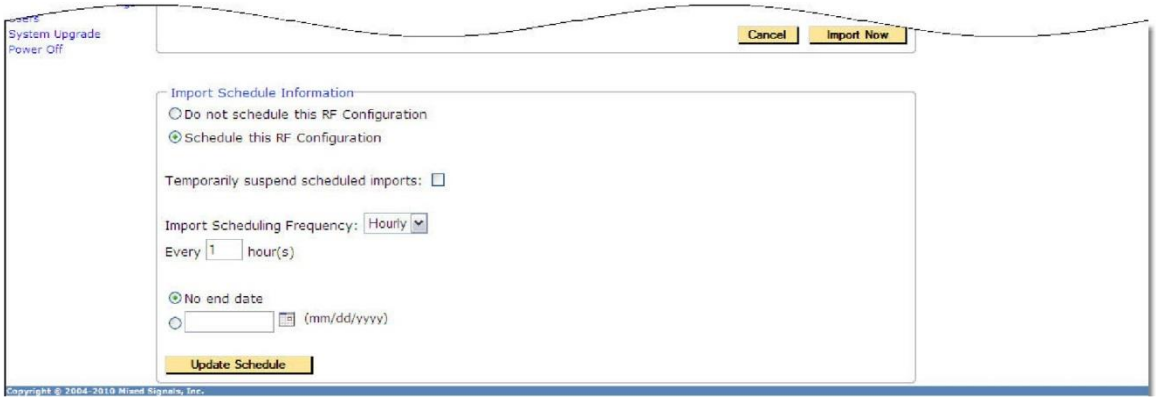


Figure 398: Import schedule information

Import a configuration from a CSV file

1. Select **Import Remote Configuration** or select **Import Local Configuration** and fill in their respective fields.

2. Select the **Import Now** button from the **RF Configuration Details** page.

3. Select **Help** to view the guidelines for the file format.

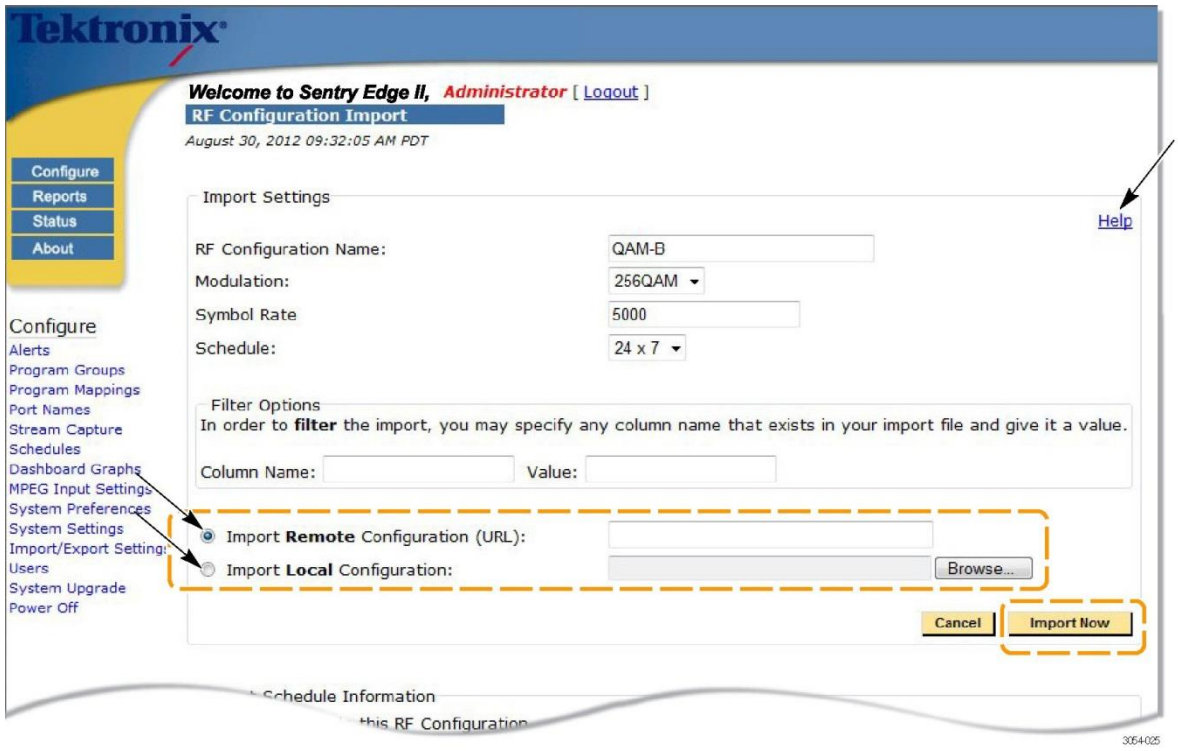


Figure 399: Importing configuration

To schedule an import

Scheduling an import will cause the import to look for the file and then change the configuration based on that systems failure.

1. Complete the field for **Import Remote Configuration (URL)**.

2. Complete the **Import Schedule Information** section.

3. Select **Update Schedule**.

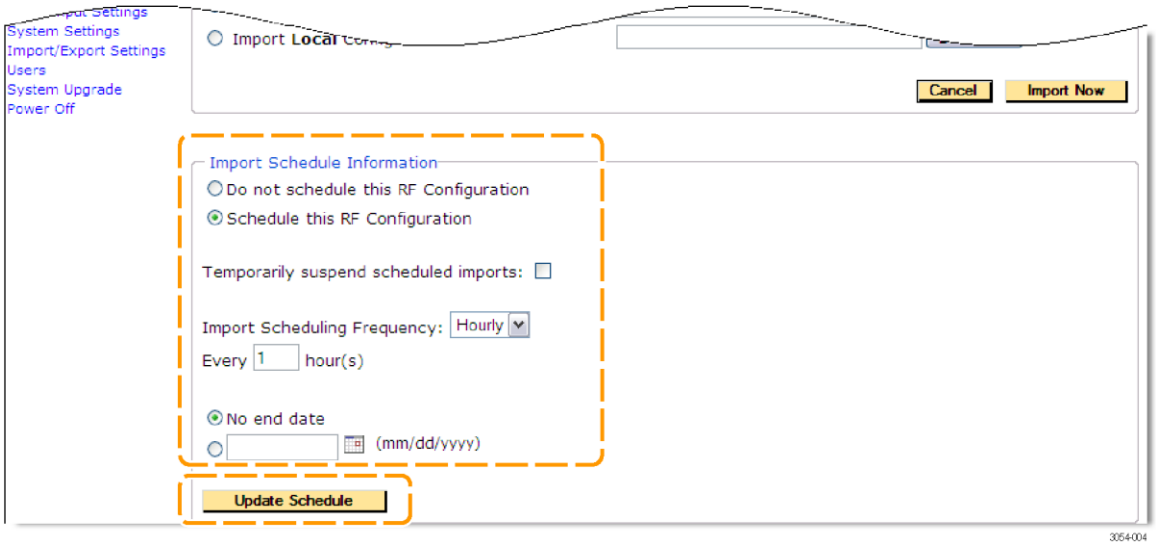


Figure 400: Completing the schedule information

View/edit RF configuration details

1. Click on any of the names in the **RF Configuration** list.

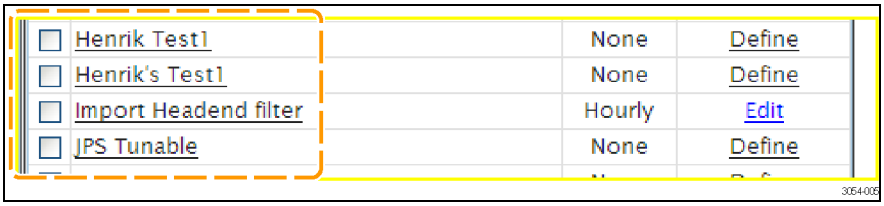


Figure 401: RF input connection

2. From the resulting page, you can change the **Channel** number, **Frequency**, **Channel Name**, **Modulation**, and **Schedule** for each individual RF frequency that you wish to monitor.

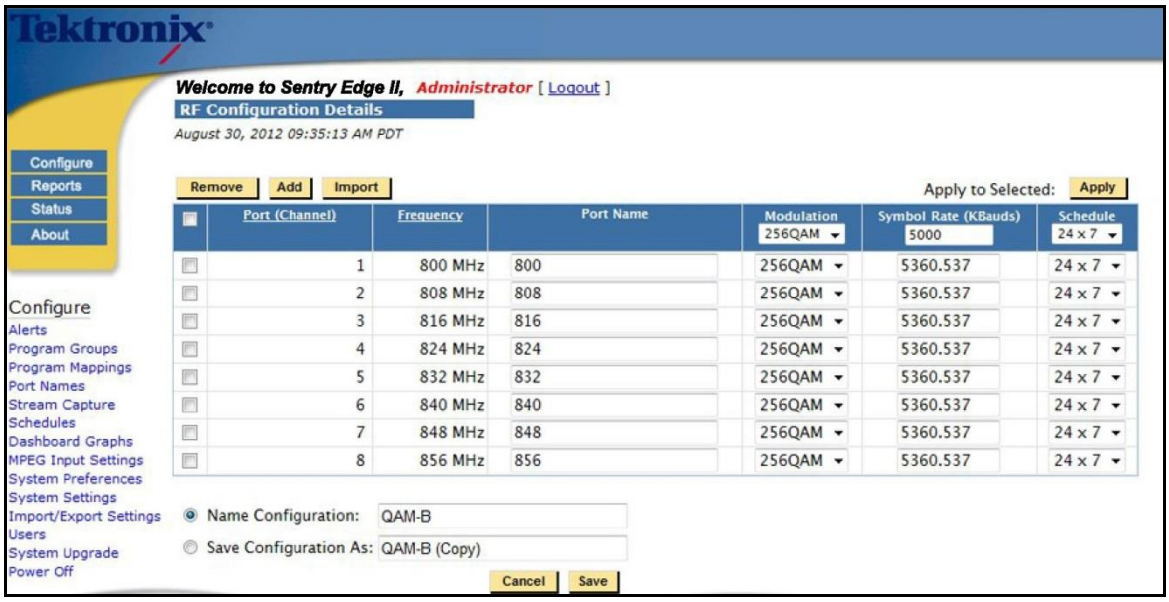


Figure 402: RF configuration details

3. Check the boxes to add or remove services. The **Import** box will take you to a different page for bulk import.

4. Select **Cancel** or **Save** when finished.

Change the schedule

Select the predetermined monitoring schedules from the drop down menu. The default is 24x7 but you may customize this to fit your needs.

Configure port names for a channel

1. You may change the port name from the **MPEG Input Settings** page at any time by clicking in the **Port Name** field and entering the desired name.
2. Select **Save RF Settings** when finished.

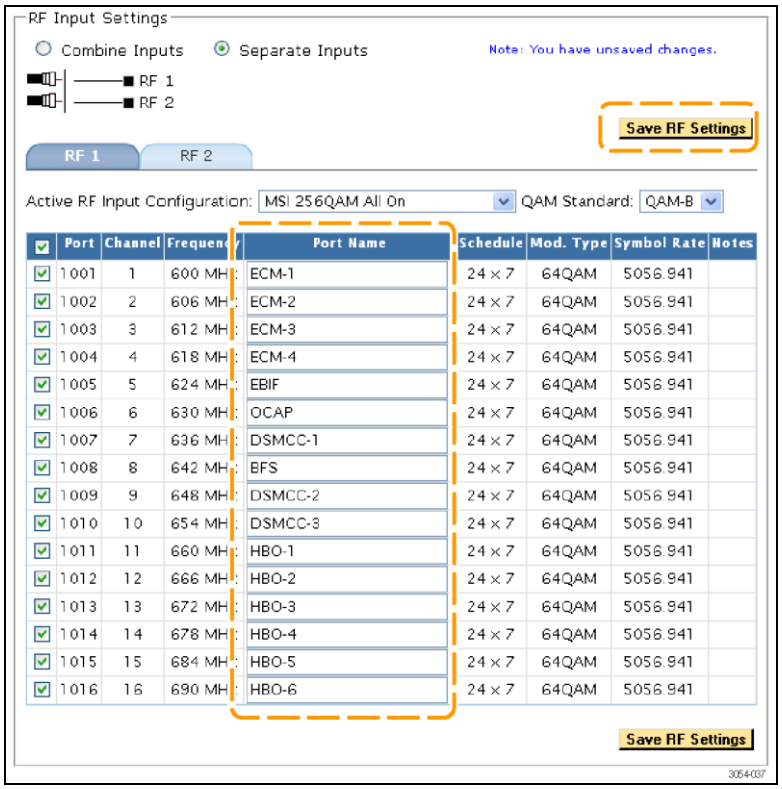


Figure 403: Configuring port names

Configure schedule summary

The **Schedule Summary** page shows the schedule **Type** (**Absolute/one-time, Daily, Weekly**) and the **Delete**, **Create** schedule buttons.

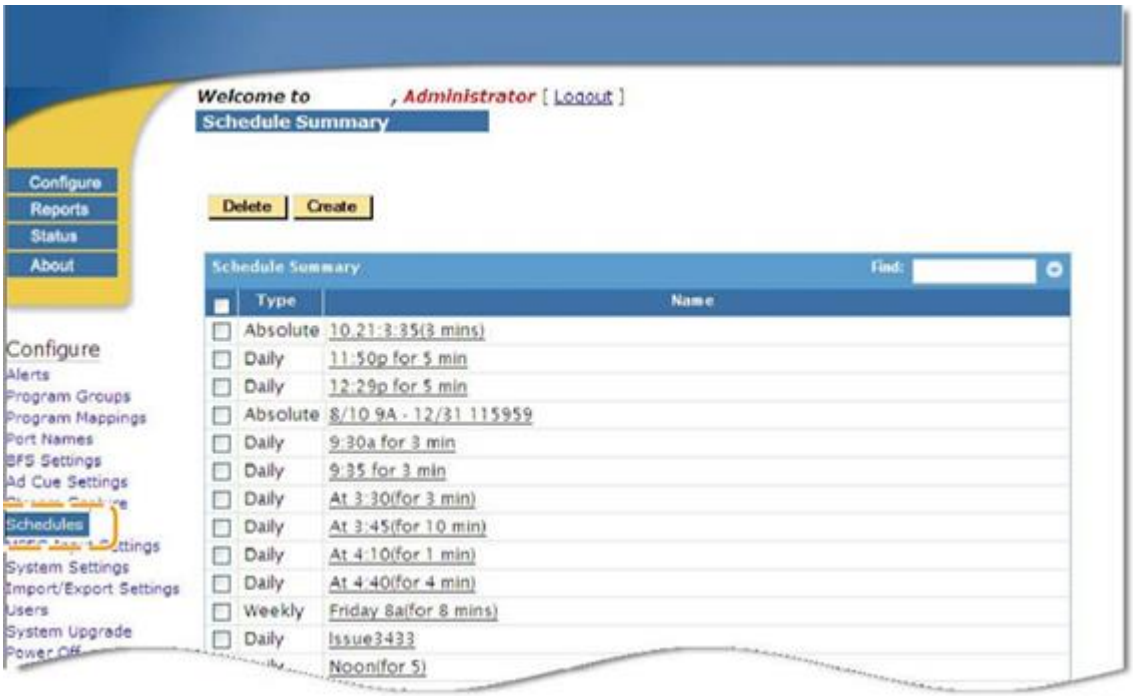


Figure 404: Schedule summary

Create a new schedule.

You can use the schedule you just defined with the **MPEG Input Settings** to set the RF monitoring schedules.

1. Select **Create**.

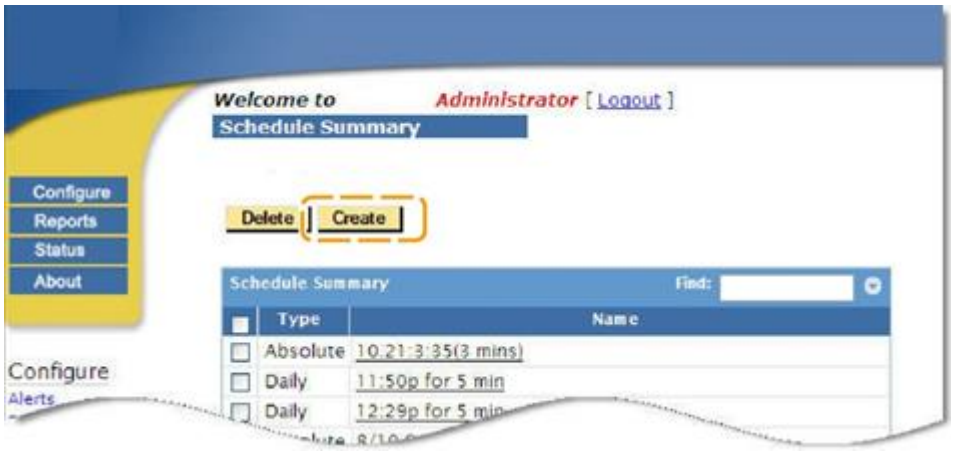


Figure 405: Creating a new schedule

2. Select the **Schedule Type** (**Daily, Weekly or Absolute/one time**) from the drop-down menu.

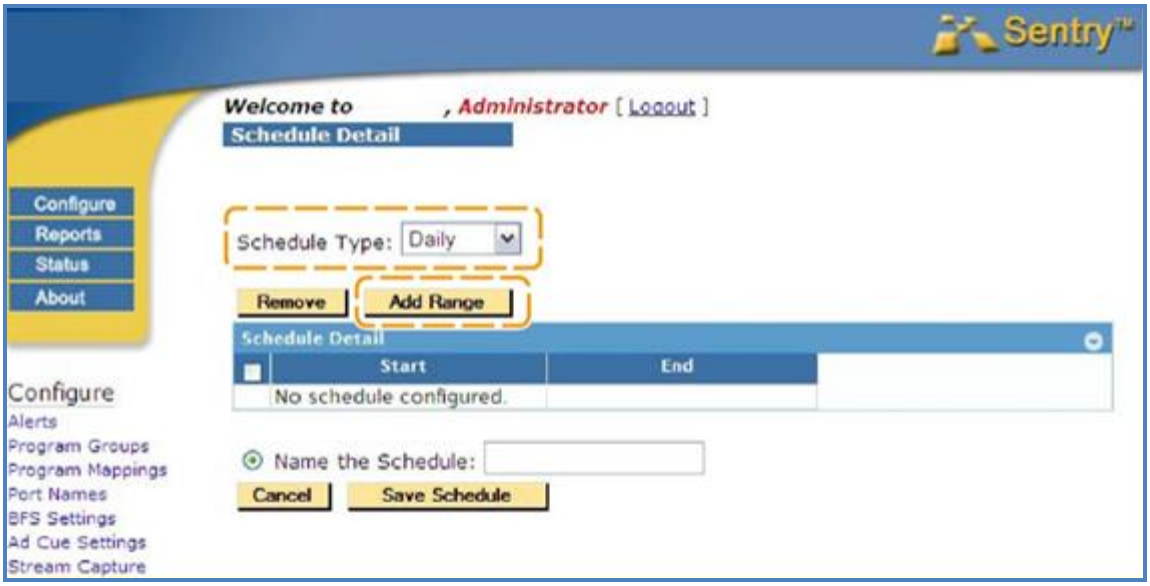


Figure 406: Schedule detail

3. Select **Add Range**.

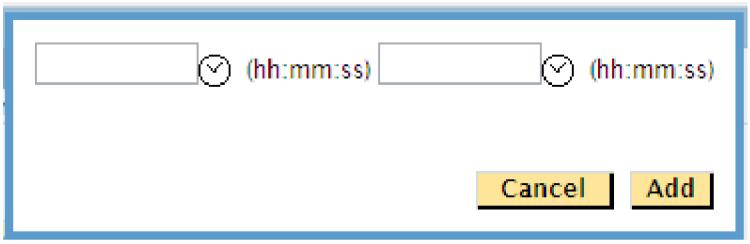


Figure 407: Daily time range

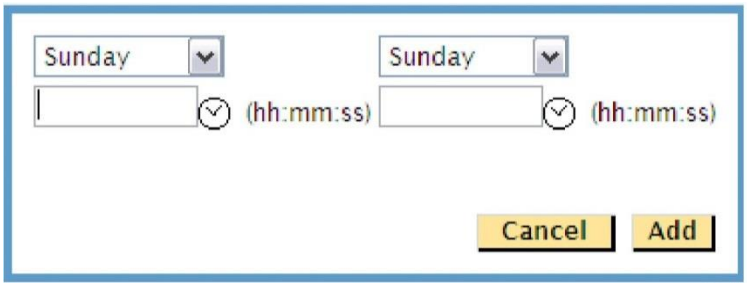


Figure 408: Weekly time range

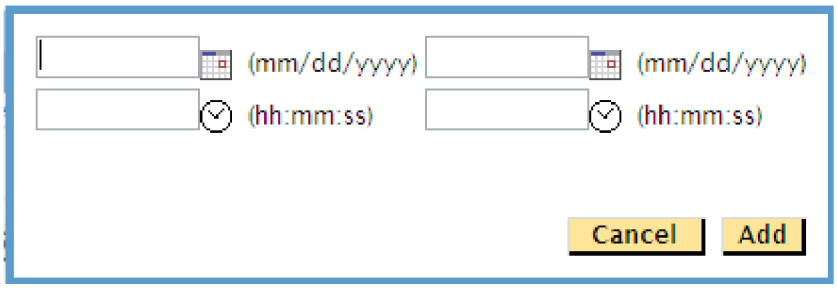


Figure 409 Absolute time range

4. Fill in the required fields and select **Add**.

5. Add as many ranges as needed by repeating until done.

6. Select **Name the Schedule** and enter a name in the entry box.

7. Click **Save Schedule**.

Operating basics

Reports

All reports can be supported in Sentry Edge/EdgeII/EdgeIII, including **QoE** and **Audio Loudness.** See the *Sentry Series Video Quality Monitor User Manual* for further details.

Current Status report

The **Current Status** report for all Sentry Series instruments allows you to customize and view a grouping of ports/channels. For **Sentry Edge**, the terms **Channel** (**Ch#)** and **Port** are interchangeable.

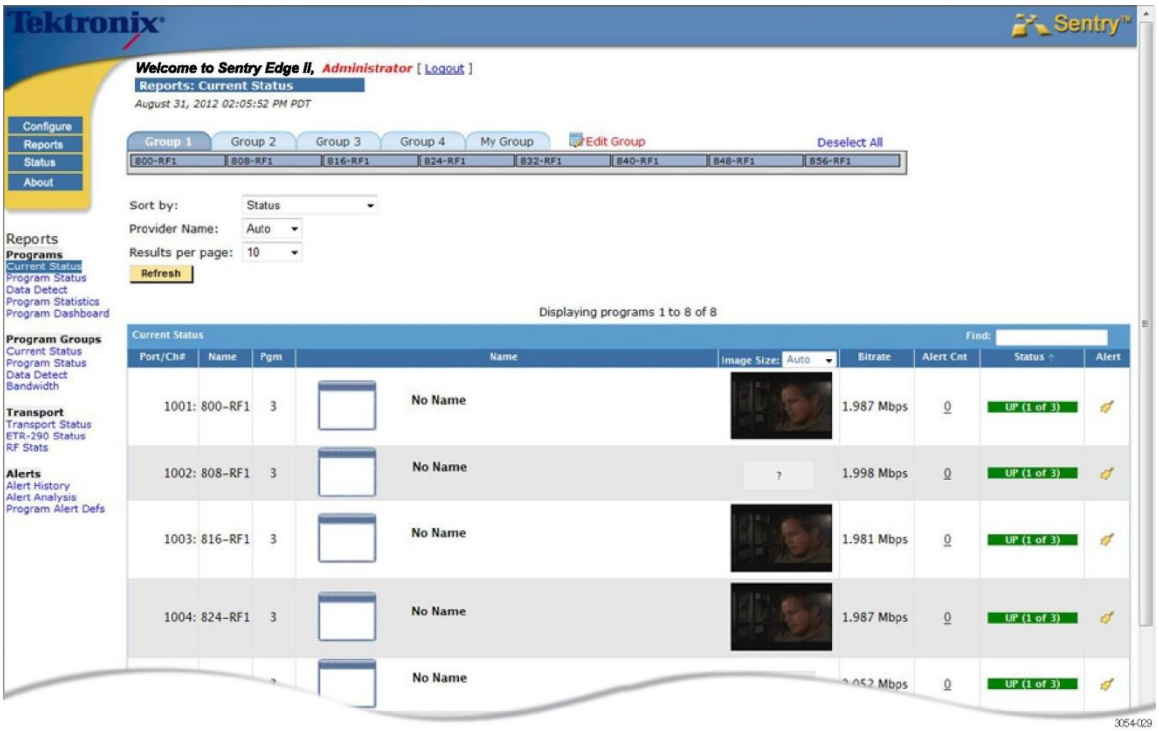


Figure 410: Current Status overview

Port / channel numbers

The Port / channel numbers are named depending on which RF connector is carrying the signal. The ports on the RF1 connector are numbered 1000 + the channel number (i.e. 1001, 1002, 1003, etc.). The ports on the RF2 connector are numbered 2001, 2002, 2003, etc.

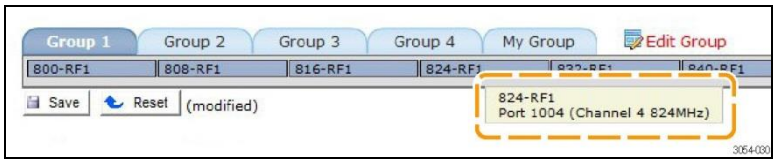


Figure 411: Port / channel cut away

Program Detail report : Tuning information

- **Avg Length**
  Average tuning length.
- **Avg Time Between**
  The average time between tuning.
- **Last Tuned in Period**
  The last time the channel was monitored

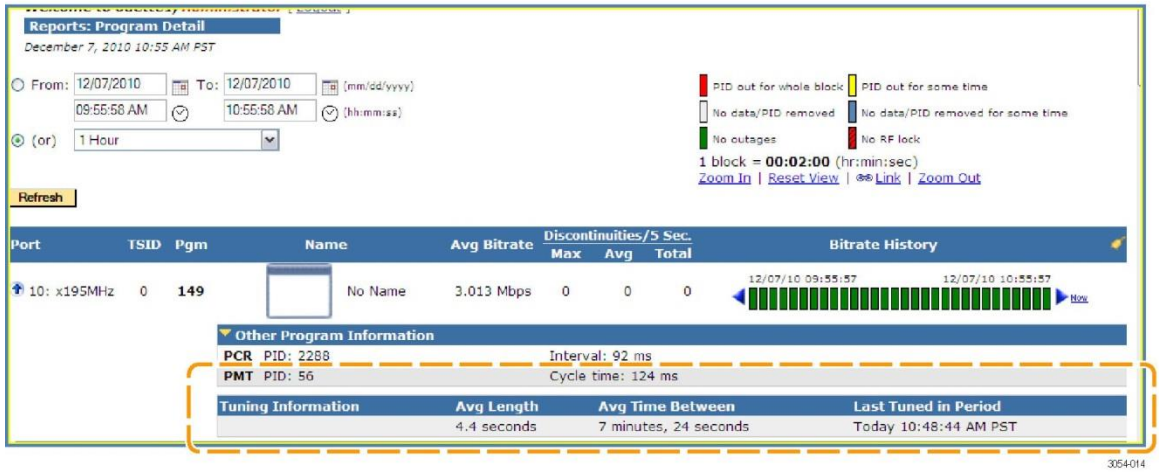


Figure 412: Tuning information

Program graph options

Bitrate graphs will always be present. Other graphs may not be available depending on chosen module license and data availability. Green areas on the graph indicate where Sentry Edge was tuned and monitoring.

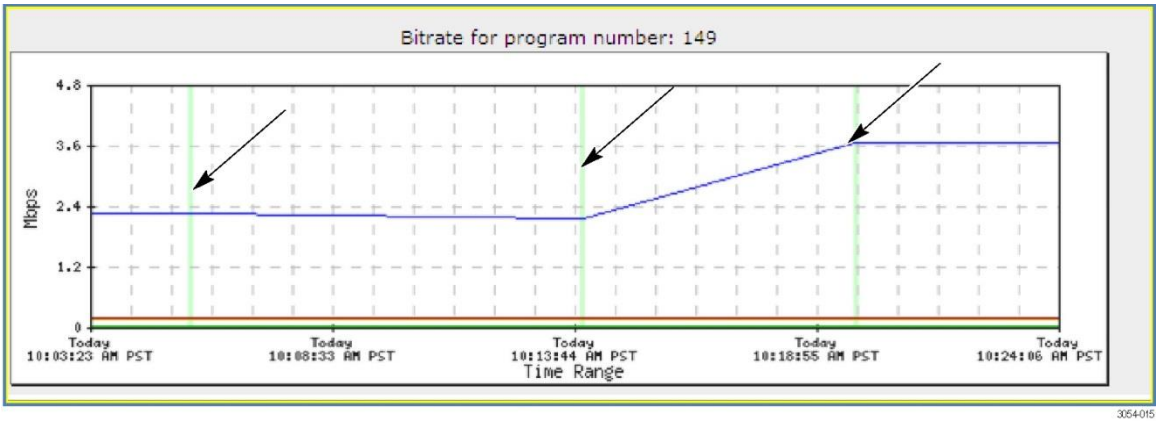


Figure 413: Bitrate graphs with green lines

- Audio Volume levels will only be present if the program is unencrypted.
- QOE graphs will only be present if the program is unencrypted and the optional QOE license has been purchased.

RF Stats

RF Stats allows you to create a summary report of each of the monitored RF statistics for each monitored RF Channel/Frequency. From this report, you may then generate graphs on each of these statistics for visual trend analysis.

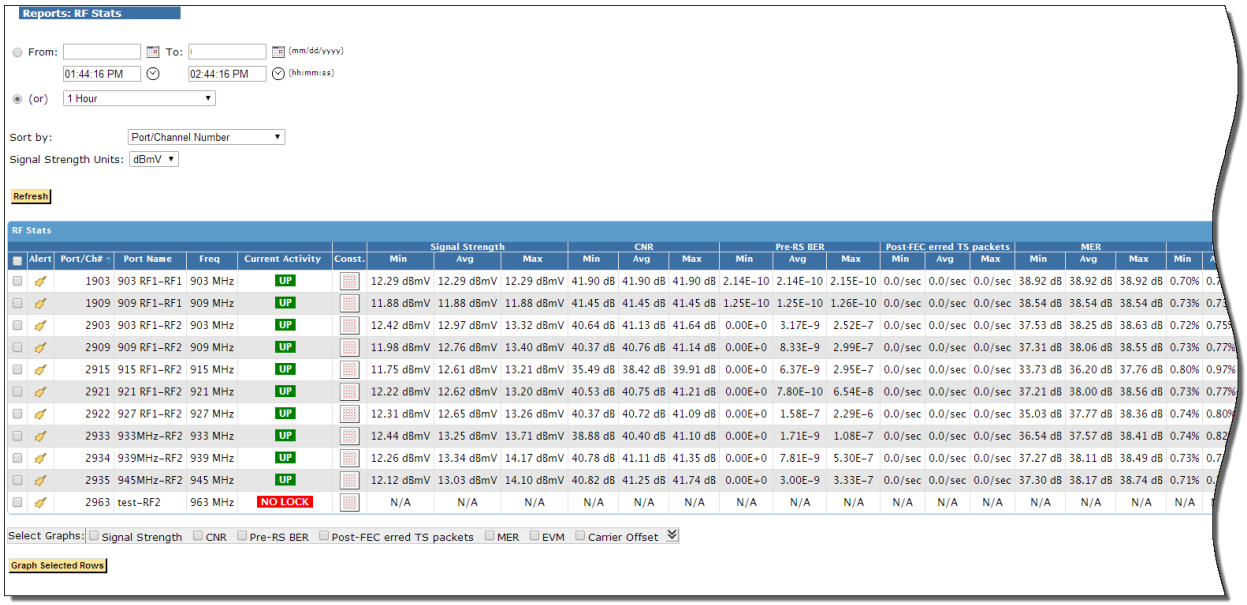


Figure 414: RF Stats overview page

Constellation Diagram

Note: Not available for Sentry Edge and Sentry Edge III-T.

A **Constellation Diagram** is a representation of a signal modulated by quadrature amplitude modulation (QAM).

This diagram displays the signal as a two-dimensional scatter diagram and can be used to recognize the type of interference and distortion in a signal.

From the **RF Stats** page, select the **Constellation** box for the RF channel you wish to diagram.

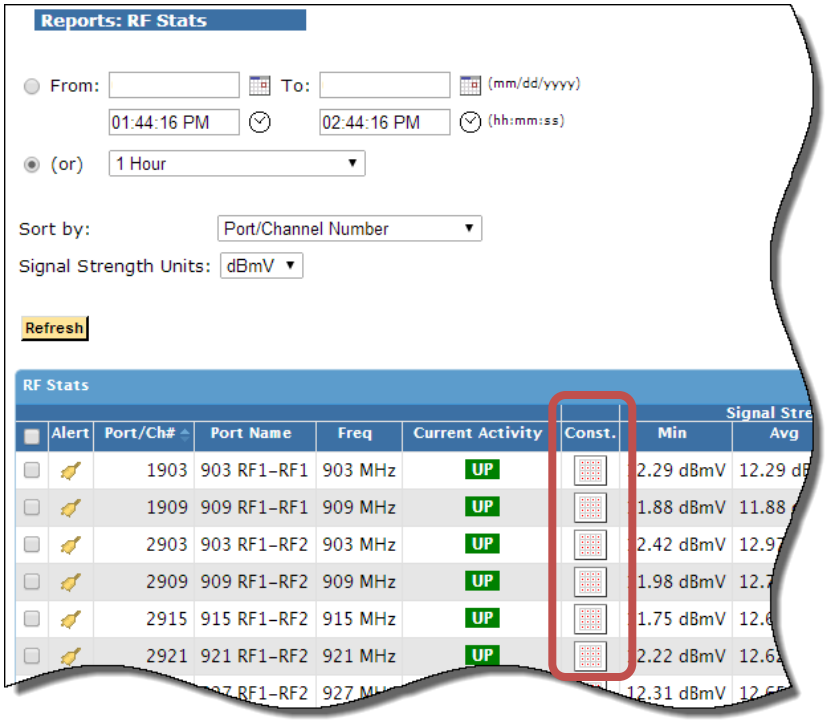


Figure 415: The Constellation boxes

The resulting box will appear.

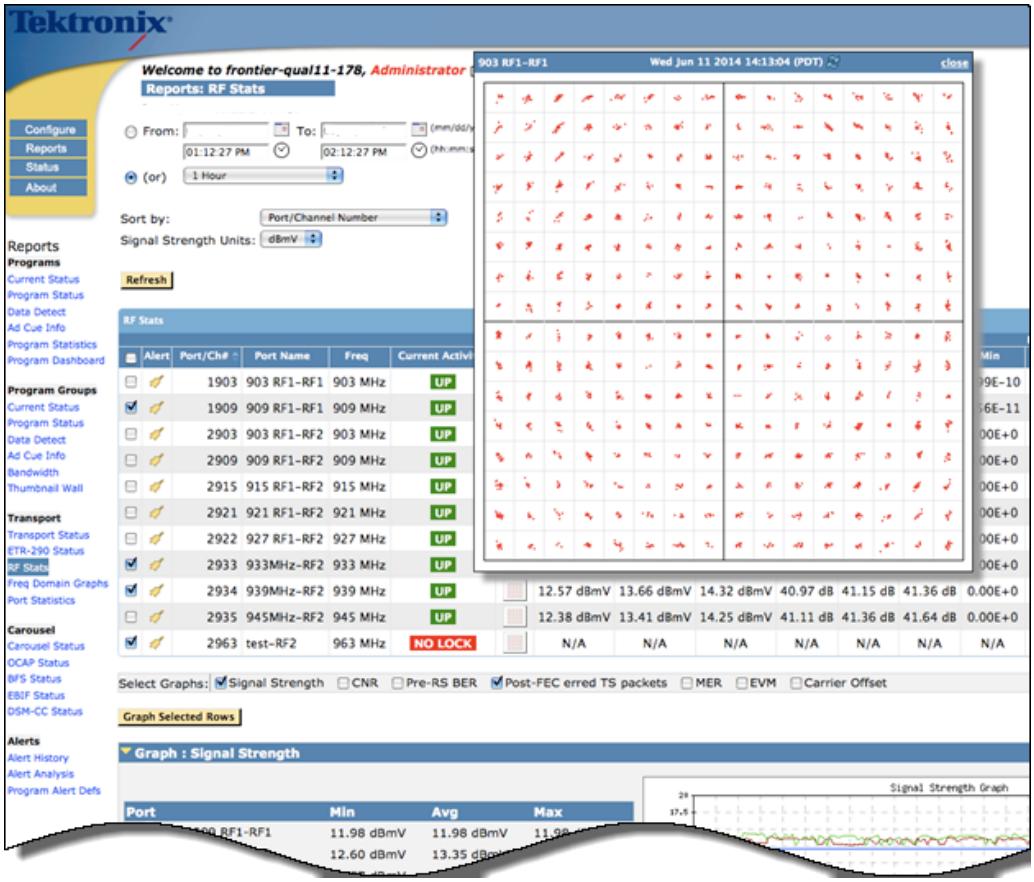


Figure 416: The resulting constellation diagram

Frequency Domain Graphs

Frequency Domain Graphs allows you to graph the ranges of each of the statistics for all of the frequencies at once.

Select **Frequency Domain Graphs** from the **Reports** menu.

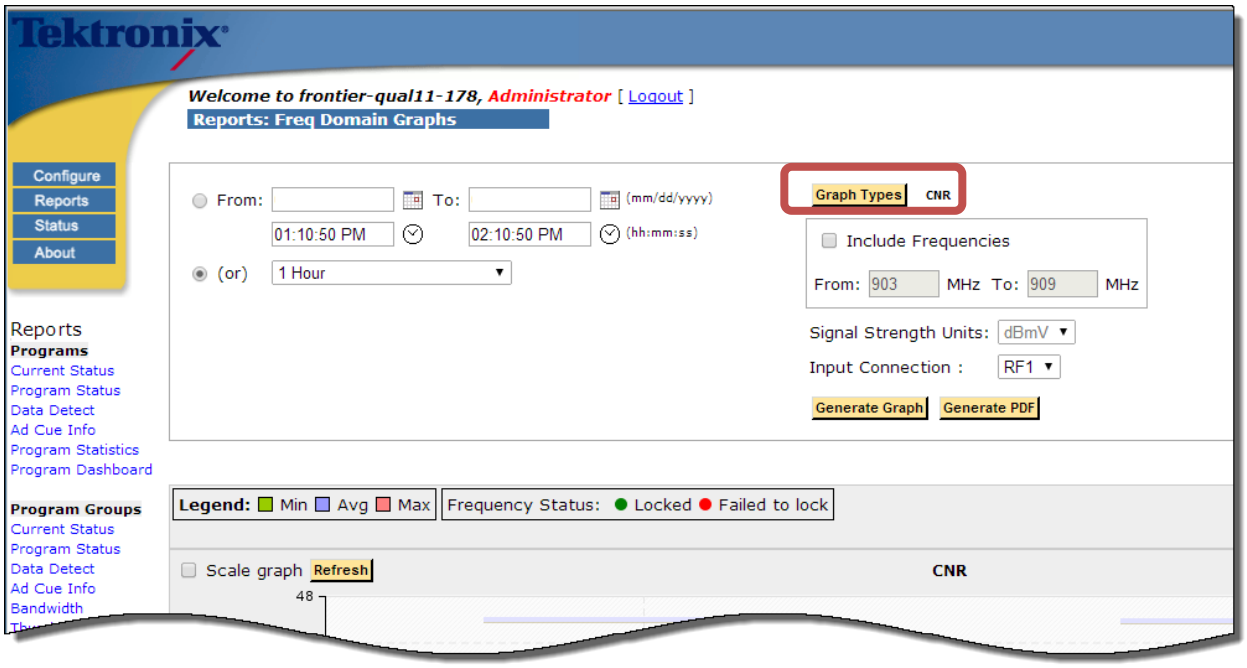


Figure 417: Frequency Domain page

1. Select the desired time range.
2. Select **Graph Types**.

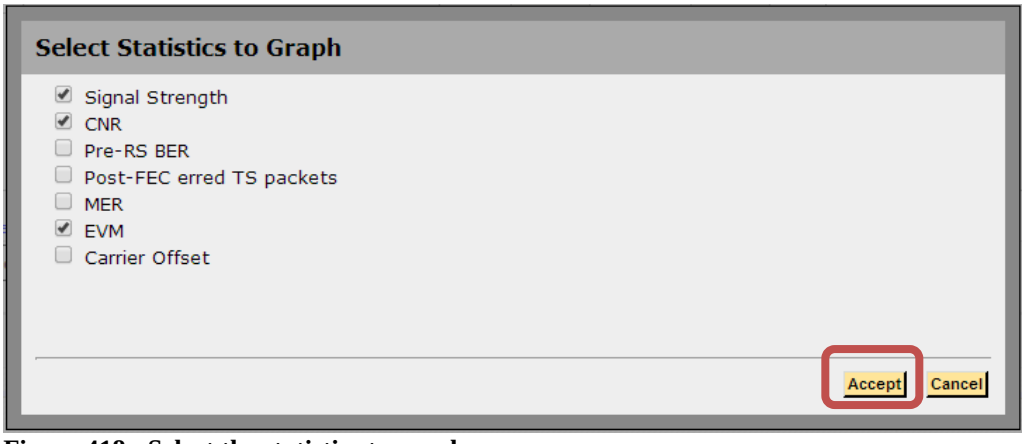


Figure 418: Select the statistics to graph

3. Select the RF statistics you want to graph. In this case, **CNR** was already selected and **Signal Strength** and **EVM** were added.

NOTE: ***If you select to graph Signal Strength, select dBmV, dBm, or dBuV.***

4. Select **Accept**.

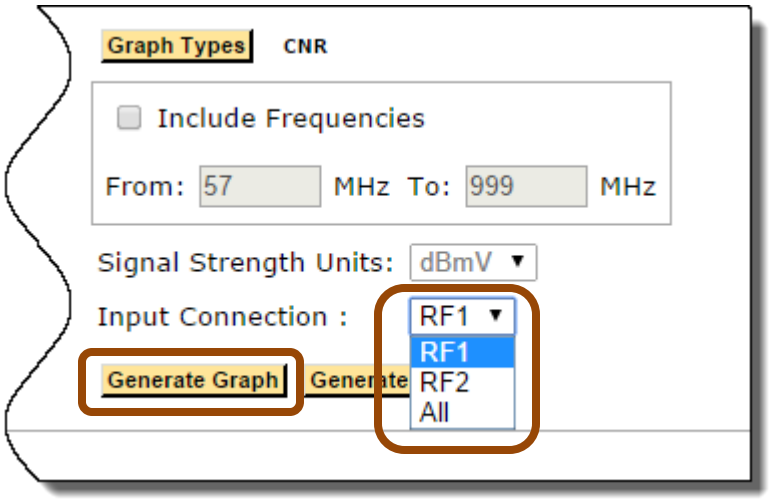


Figure 419: Select the Input Connection and Generate Graph

5. If there are multiple input connections, select the connection you want from the **Input Connection** drop down menu.

6. Select **Generate Graph** to refresh the graphs on the screen or Generate PDF to generate a PDF file with the graphs.

7. **Generate Graph** will produce the following:

Figure 420: Frequency Domain graphs

NOTE: ***The Scale Graph option allows you to zoom in for a higher resolution view on the vertical scale of the graph.***

Status

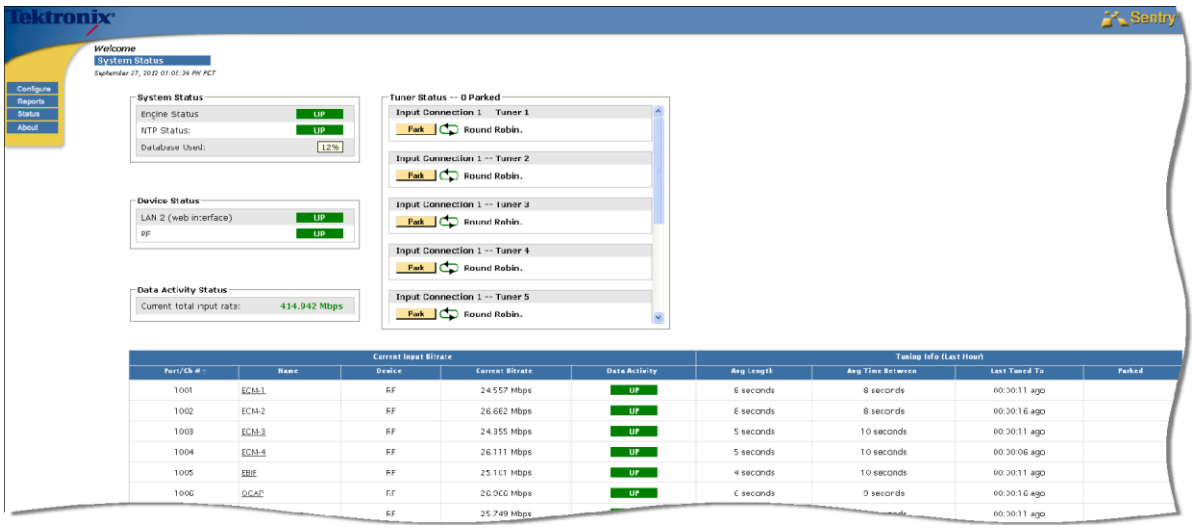


Figure 421: System Status overview

- **Tuner status**
  Tuner Status is specific to the **RF Tuning**. It displays the current state of each tuner and allows you to park one of the tuners on a specific frequency. You also have the option to park both of the tuners on a specific frequency, as long as they are not both on the same frequency. **Tuner Status** also shows if the unit is contained within the round robin.
- **System status**
  System Status shows if the **Engine** and the **NTP Status** are **UP** or **DOWN** and what percentage of the database is in use.
- **Device status**
  Device Status shows if LAN 2 (the web interface) and the RF are **UP** or **DOWN**.
- **Data activity status**
  The **Data Activity** column shows status types specific to RF tuning:
- **Up**
  A tuner has successfully tuned to the frequency and is receiving an input bitrate
- **Down**
  A tuner has successfully tuned to the frequency, but is receiving no input bitrate
- **Paused**
  A particular frequency is not in the round robin queue.
  This status is the result of one of two scenarios.
  1. Either all of the tuners in that tuning pool are parked on other channels or;
  2. The channel/port is not scheduled.
- **No lock**
  A tuner is attempting to tune the specified frequency but is unable to obtain a lock on that frequency. Check to make sure the frequency is a tunable one.
- **Pending**
  A tuner has begun to tune the channel/port but has not yet collected enough data to display.

Park a tuner for a set amount of time

1. Select **Park** for the tuner you wish to park.

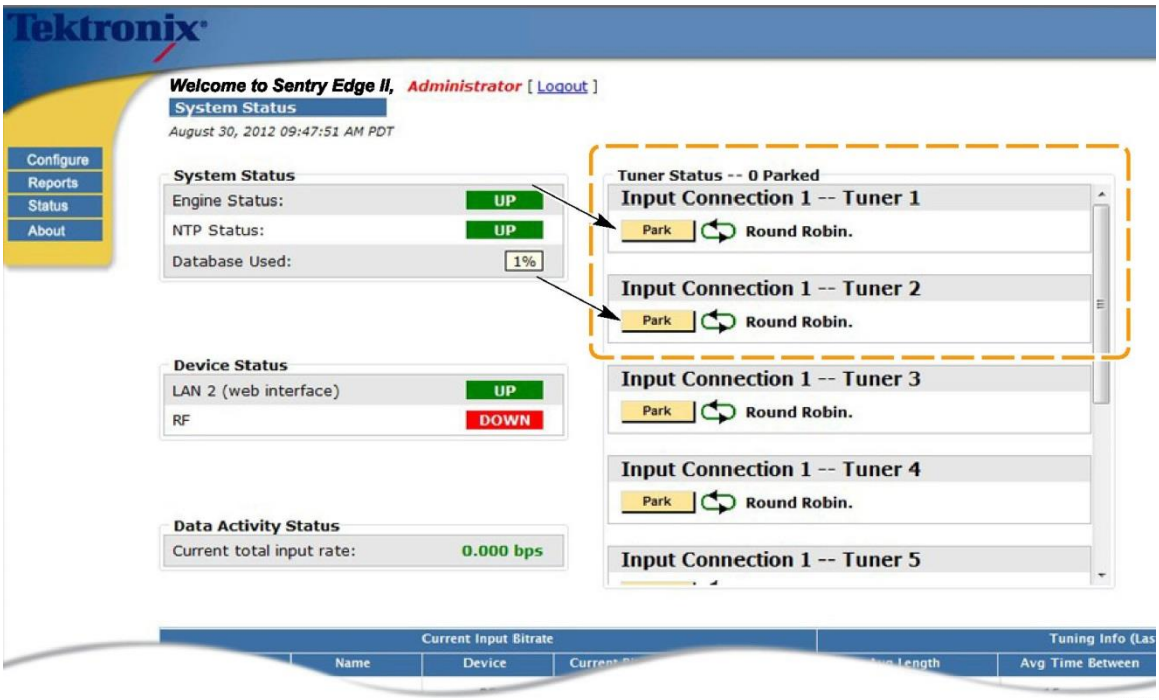


Figure 422: Selecting a tuner to park

2. You will see the following confirmation message:

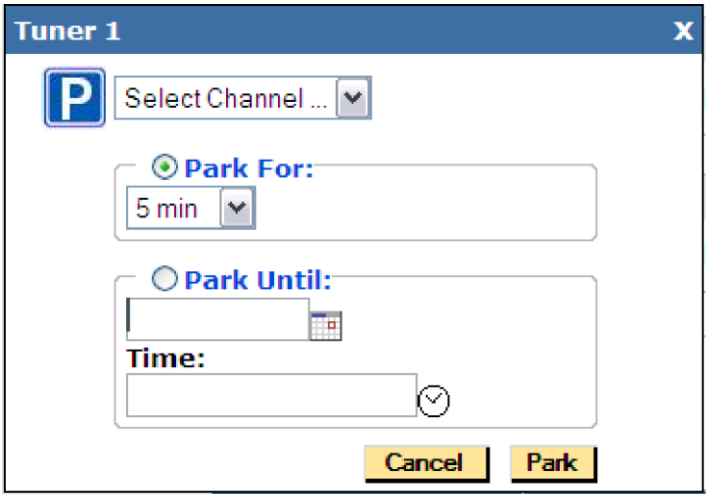


Figure 423: Selecting the Park For option

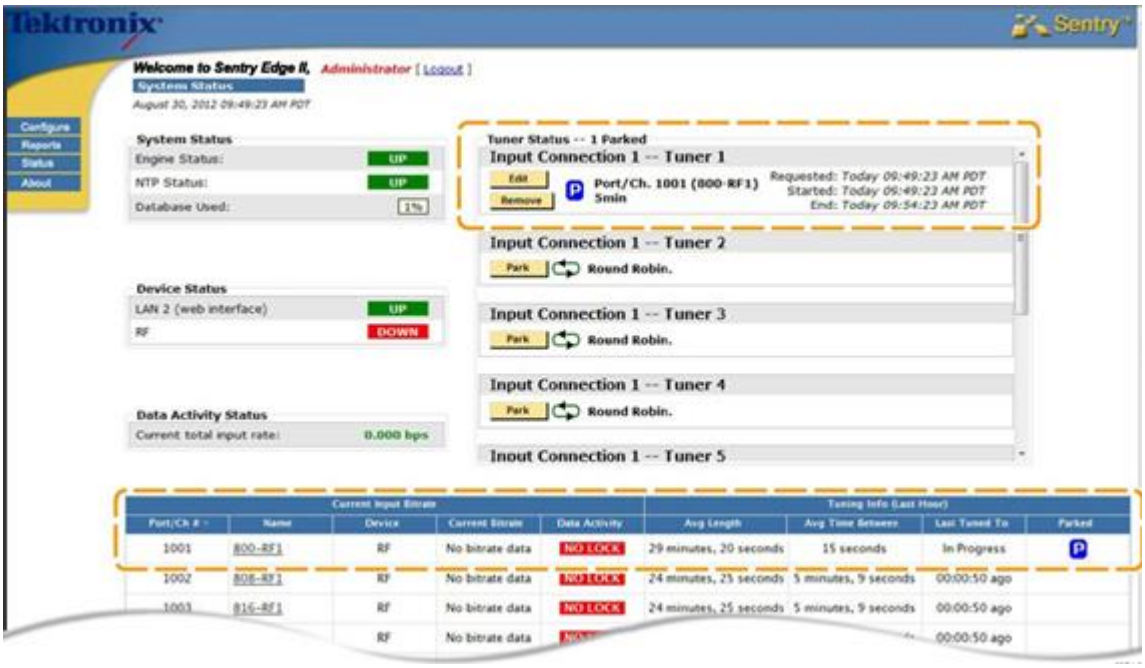


Figure 424: The parked tuner

3. Select the **Channel** you wish to park.

4. Select the amount of time you wish to park the tuner for or select the date and time you wish to park the tuner until.

5. Select **Park**.

6. Once it is parked, the tuner will show the following:

   - That it is parked
   - What channel is parked
   - For how long
   - When the park was requested and when it will start and end

7. The unit will also show as parked in the **Tuning Info Table** below the **Status** information. All columns are sortable.

To park a tuner (alternate method)

There are several ways to access the System Status page to park a tuner. Here is another option:

1. From the **Program Detail** screen, click **Additional reports focusing on this port** to access the drop-down menu.

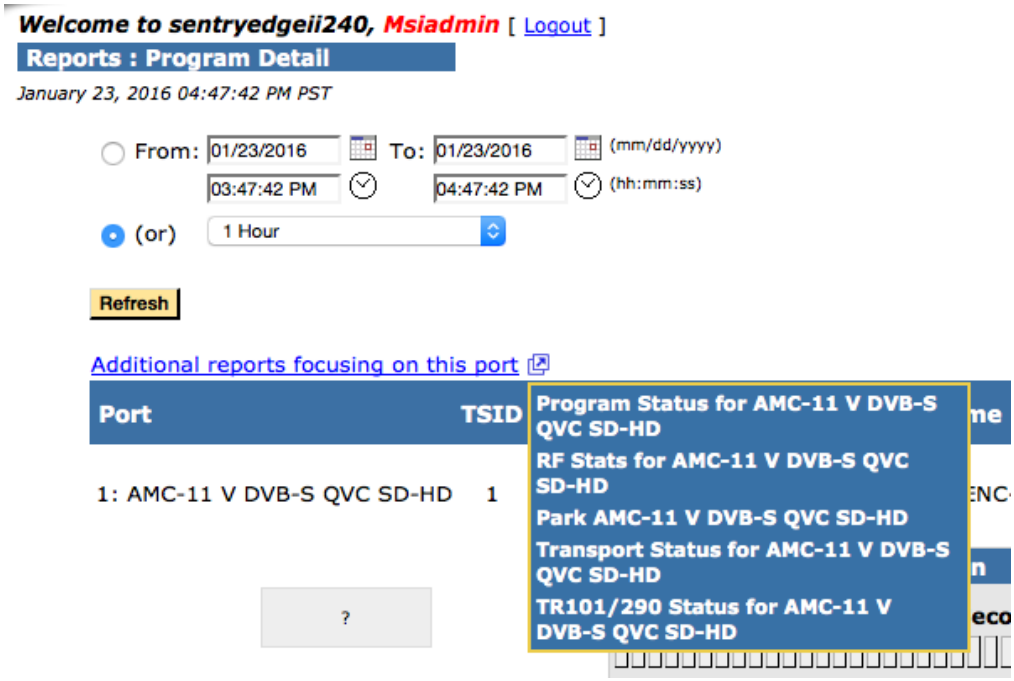


Figure 425: Program Detail drop-down menu

2. Select the tuner you wish to park.

3. You will then be taken to the System Status page to complete the process as described in the previous *To park a tuner for a set amount of time* procedure.

To park a tuner for a set amount of time:

1. Select **Park Until**.
2. Select the date you wish the park to end.
3. From the **Program Detail** screen, select the up arrow button to access the drop-down menu.

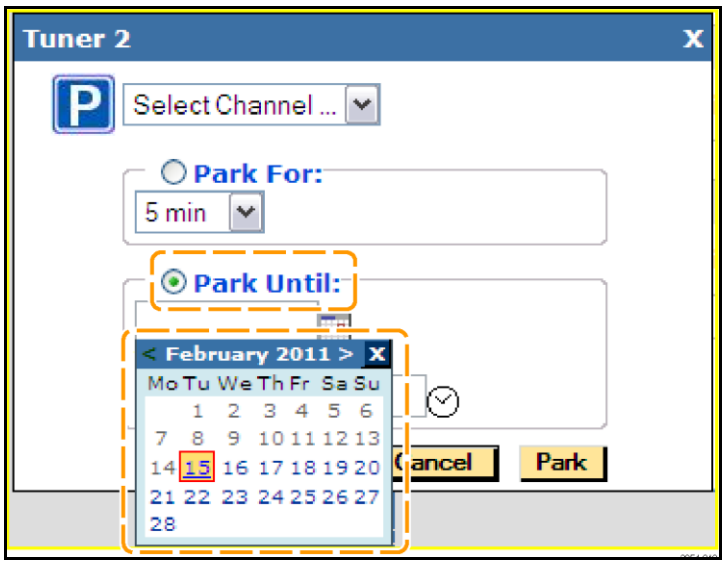


Figure 426: Selecting a date

4. Select the time you wish the park to end.

Figure 427: Selecting the time

5. Select **Apply**.

Appendix C: Acronyms

The following table contains an overview of acronyms that relate to cable network operations. Items in this list are referenced in this document.

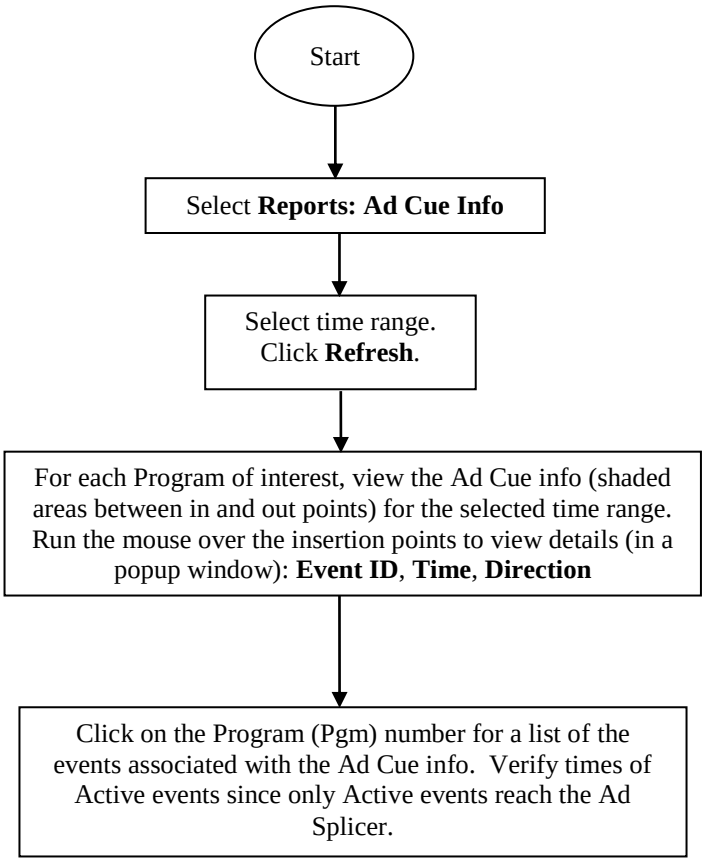
ANSI	American National Standards Institute
ANSI/SCTE 20	Method for Carriage of Closed Captions and Non-Real Time Sampled Video
ASI	Asynchronous Serial Interface
ATSC	Advanced Television Systems Committee
A/V	Audio/Video
AVC	Advanced Video Coding
B	Byte
BFS	Broadcast File System
CEA	Consumer Electronics Association
CEA-708-B	Digital Television (DTV) Closed Captioning specification
CGMS	Copy Generation Management System
DBDS	Digital Broadband Delivery System
DC	Download Cancel
DHCT	Digital Home Communications Terminal
DII	Download Info Indication
DNCS	Digital Network Control System
DNS	Domain Name Server
DSM-CC	Digital Storage Media Command and Control
DTV	Digital Television
EIA	Electronic Industries Alliance
EIA/CEA-608-B	Line 21 Data Services, a technical standard and guide for using or providing Closed Captioning services or other data services embedded in Line 21 of the vertical blanking interval of the NTSC video signal
EPG	Electronic Program Guide
FQDN	Fully Qualified Domain Name
GigE	Gigabit Ethernet
GUI	Graphical User Interface
HDTV	High Definition Television
IP	Internet Protocol
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
IT	Information Technology
iTV	Interactive Television
Kbps	Kilobits per second
LAN	Local Area Network
LED	Light Emitting Diode
MB	Megabyte
Mbps	Megabits per second
MIB	Management Information Base
MPEG	Moving Picture Experts Group
ns	Nanosecond (one billionth of a second)

NTSC	National Television Systems Committee
NTP	Network Time Protocol
PAT	Program Association Table
PCR	Program Clock Reference
PES	Packetized Elementary Stream
PID	Packet Identifier
PMT	Program Map Table
PSI	Program Specific Information
PSIP	Program and System Information Protocol
PVR	Personal Video Recorder
QAM	Quadrature Amplitude Modulation
QPSK	Quadrature Phase-Shift Keyed
SCTE	Society of Cable Telecommunications Engineers
SCTE 35	Digital Program Insertion Cueing Message for Cable
SDT	Service Description Table
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TSID	Transport Stream Identifier
URL	Uniform Resource Locator
VBI	Vertical Blanking Interval
VOD	Video on Demand
XDS	Extended Data Services

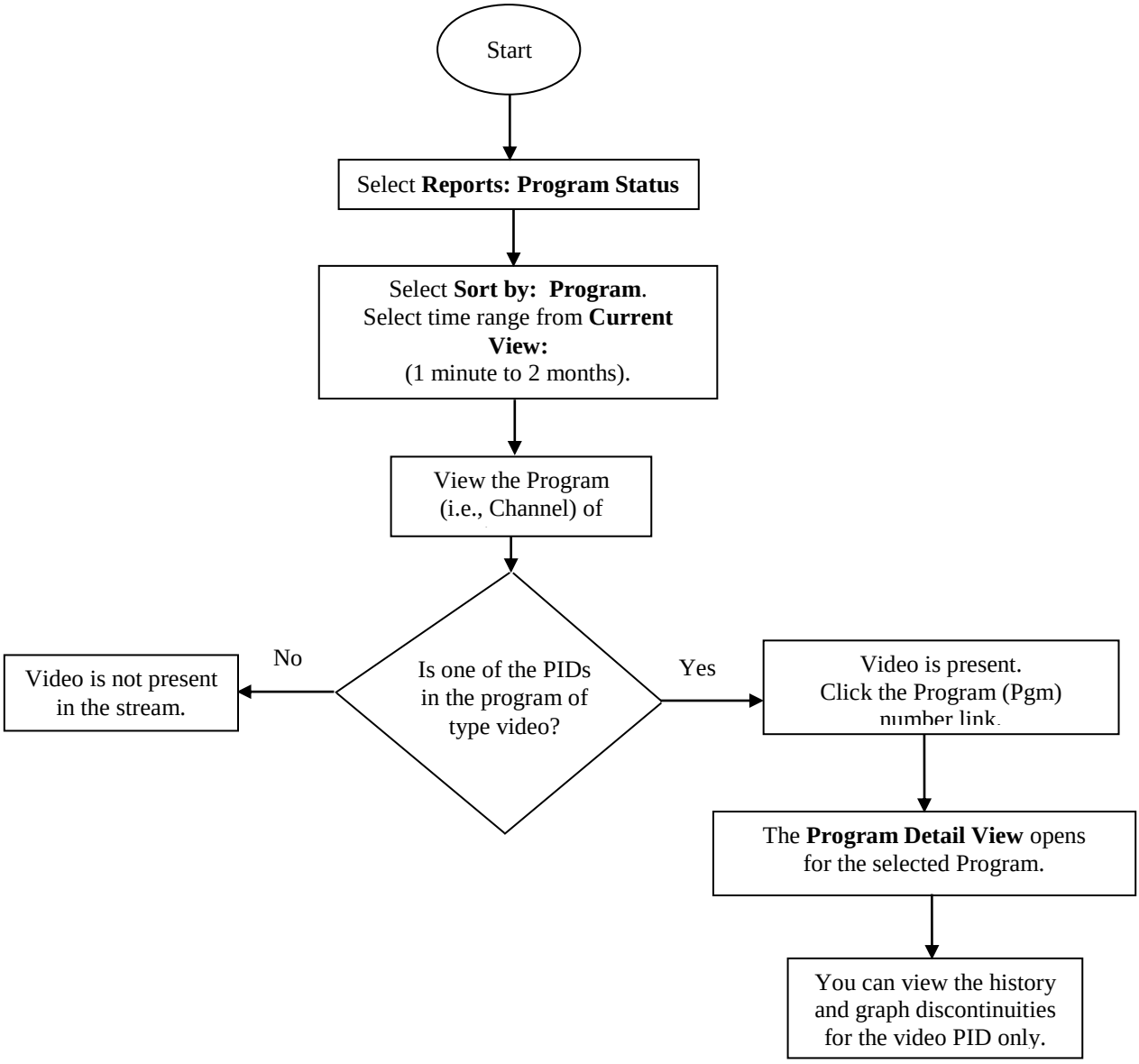
Appendix D: Examples

Sentry allows you to address the following types of problems:

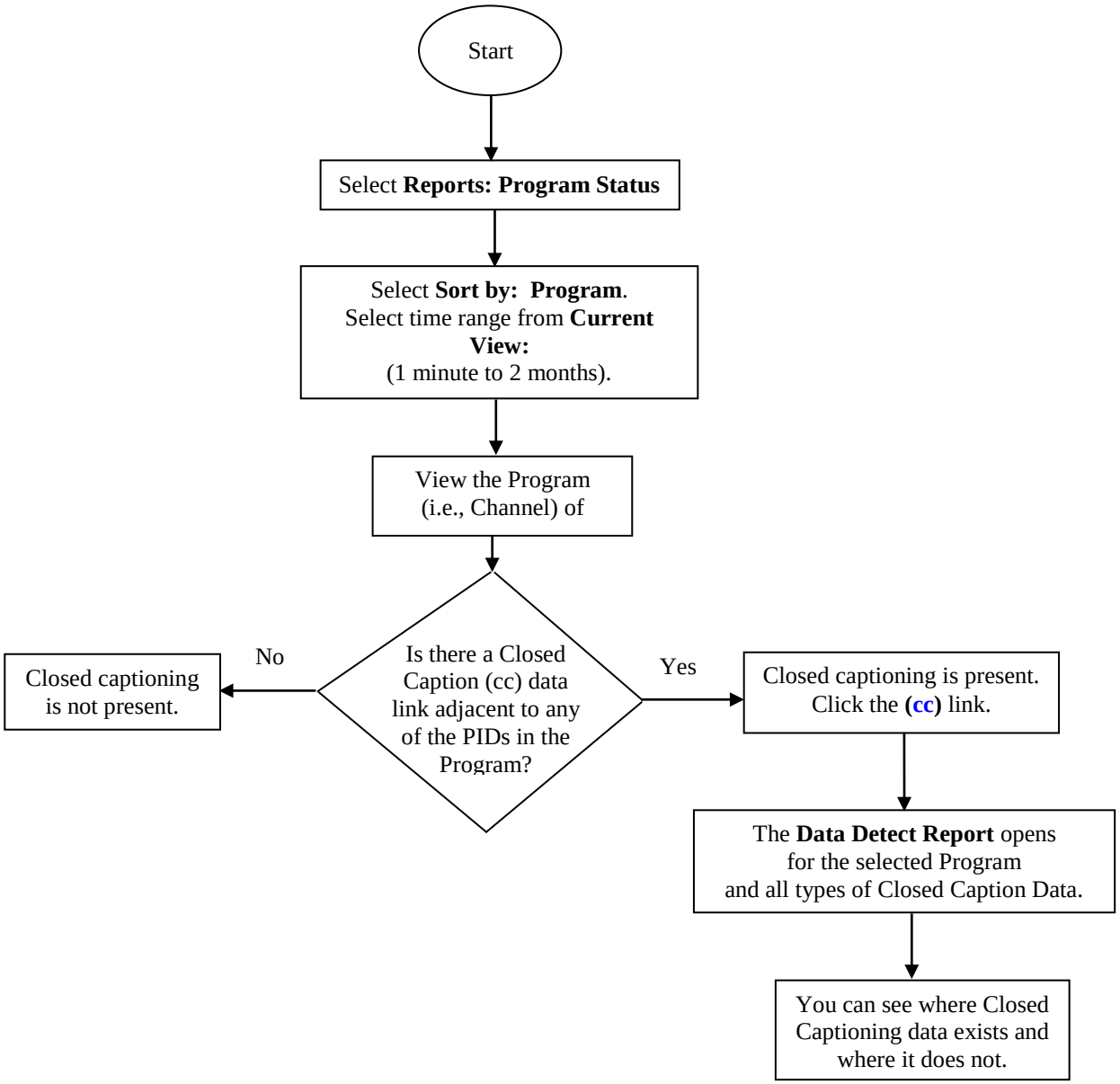
You want to find out if ad cue messages are reaching the ad splicer and if they have the correct times in them.



There is a new channel being launched and no video is being displayed. You need to find out if it is a table problem or an encoding or provider problem.



Closed captioning is not working on a certain channel. You need to find out if it is or is not present.



Notices

Trademarks

Scientific-Atlanta, Scientific-Atlanta ARCS logo, and EXPLORER are registered trademarks of Scientific-Atlanta, Inc. PowerKEY, DNCS, BFS, VCR Commander, and Tape ‘N View are trademarks of Scientific-Atlanta, Inc.

All other trademarks listed herein are the property of their respective owners.