Eventide™
Communications

NexLog
Express Recording Solutions

EXP SERIES

User Manual
Version 2025.4[7087]

P/N: #141354

P/N: #141354 Version 2025.4[7087]

Eventide Communications LLC
One Alsan Way
Little Ferry, NJ 07643
201-641-1200

www.eventidecommunications.com

Table Of Contents

1. Introduction

1.1. Welcome 13

1.1.1. Intended Use 13

1.2. Customer Support Information 13

1.2.1. Identifying NexLog Express Model and Version 14

2. General Specifications

2.1. NexLog Express Recorder 17

2.1.1. Front Panel 18

2.1.2. Rear Panel 18

2.1.3. Operating Limits 19

3. Recorder Setup

3.1. Unpacking the Recorder 21

3.2. Bench Test 21

3.3. Installation 23

- 3.3.1. Operating Limits 19
- 3.3.2. Location Considerations 24
- 3.3.3. Mounting Options 25
- 3.3.4. Connecting AC Power 25
- 3.3.5. Before Connecting Audio 27
- 3.3.6. Connecting Analog Audio 27
- 3.3.7. Connecting Digital Audio 30
- 3.3.8. Connecting to an Ethernet Network 31

4. Recorder Operation

4.1. Starting Up and Shutting Down 33

5. Client Software and Playback

6. The System Console User Interface

7. Configuration Manager

7.1. System 40

7.1.1. System Info 40

7.1.2. Date and Time 43

7.1.3. License Keys 47

7.1.4. Storage Devices 50

7.1.5. Translations 53

7.1.6. Configuration Files 59

7.1.7. System Diagnostics 61

7.1.8. Upgrade Recorder Software 62

7.1.9. Power Off 63

7.2. Networking 64

7.2.1. System Identification 64

7.2.2. Network Interfaces 65

7.2.3. VNC Settings 69

7.2.4. VPN Settings 70

7.2.5. SNMP Settings 71

7.3. Recording 74

7.3.1. Recording Interfaces 74

7.3.2. Replace Board 99

7.3.3. Retention Settings 99

7.3.4. Resource Groups 102

7.3.5. Call Suppression 108

7.3.6. Custom Fields 110

7.3.7. Alias Banks 114
7.3.8. Data Integrations 120
7.3.9. Geo-Location 133
7.3.10. Internal Vocoder 136
7.4. AI 139
7.4.1. Notifications 139
7.5. Archiving 146
7.5.1. Archives 146
7.5.2. Archive Configuration 149
7.5.3. Archive Media History 164
7.6. Users and Security 165
7.6.1. Users 166
7.6.2. System Security 180
7.6.3. Encryption and TLS 190
7.6.4. User Groups 198
7.6.5. Permissions 202
7.7. Alerts and Logs 205
7.7.1. Alert History 205
7.7.2. Active Alarms 206
7.7.3. Alert Codes 207
7.7.4. Logging 208
7.7.5. Email 211
7.7.6. Audit History 213
7.7.7. Client Activity 215
7.7.8. NexLog Monitoring 215

7.8. Utilities 217
7.8.1. Schedules 217
7.8.2. Upload Recorder Update 221
7.8.3. Re-Order Channels 221
7.8.4. Network Utilities 221
7.8.5. Packet Capture 222
7.8.6. Documents 223
7.9. Basic Reports 223
7.9.1. Recording Reports 223
7.10. Change Password 226

8. Software License

8.1. Product License and Usage Agreement 227

8.1.1. GNU GENERAL PUBLIC LICENSE 230

8.1.2. Preamble 230

8.1.3. TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION 231

8.1.4. END OF TERMS AND CONDITIONS 236

8.1.5. How to Apply These Terms to Your New Programs 236

A. Software Installation and Upgrade

A.1. Why Re-Installation May Be Necessary 239

A.2. Why Upgrades May Be Necessary or Desirable 239

A.3. The Software Upgrade/Installation Process 240

A.3.1. Booting DVD Installation Media 240

A.3.2. Upload Full Upgrade Image from your Desktop 243

A.3.3. Download Full Upgrade Image from Eventide VPN Server 244

A.3.4. Import Full Upgrade Image from an Archive Drive 244

A.4. Some Details, Especially About Installation 244

A.4.1. Restoring Archives When Installing New Software 245

A.4.2. Potential Issues 246

B. Installation from USB

B.1. Installation Prerequisites 247

B.2. Create Bootable USB 247

B.3. Booting from USB 249

C. Channel Wiring for Analog Input Boards

D. Alert Codes

E. Incident Evaluation Restore

F. RTP VOIP Templates

6.1. Avaya SBC 273

6.1.1. SBC Configuration 273

6.1.2. Recorder Configuration 288

6.2. Avtec Scout RTP Forwarding 289

6.2.1. AVTEC Scout™ Console Configuration 291

6.3. Carybyn Call Handling Solution 299

6.3.1. Carbyne Introduction 299

6.3.2. Logger Integration 300

6.3.3. Adding a Virtual Recording Interface 301

6.4. Cisco CallManager Skinny Protocol (SPAN) 304

6.4.1. Cisco CallManager Skinny Protocol (SPAN) Introduction 304

6.5. Cisco CallManager Built-in-Bridge 310

6.5.1. Built-in-Bridge Introduction 310

6.5.2. NexLog Express Configuration Overview 311

6.5.3. Cisco Unified Call Manager Built-in-Bridge Configuration Detail 312

6.6. Motorola Dimetra AIS Interface 318

6.6.1. Motorola Dimetra AIS Interface Introduction 319

6.6.2. Install and configure AIS and CRAM 319

6.7. EFJohnson Console Protocol 325

6.7.1. Configuring an Eventide Recorder to capture EFJohnson multicast P25 traffic 325

6.8. Harris P25 Recording 330

6.8.1. Harris P25 Recording Introduction 330

6.8.2. Adding a Virtual Recording Interface 301

6.9. Intrado SipRec Recording 335
6.9.1. Intrado SipRec Recording Introduction 336
6.9.2. Adding a Virtual Recording Interface 301
6.10. MCPTT 3GPP/LTE RADIO RECORDING 339
6.10.1. Recorder Configuration 288
6.11. Mitel Secure Recording Connector 340
6.11.1. Mitel Secure Recording Connector Introduction 341
6.12. MOTOTRBO Controller-less Recording Interface 346
6.12.1. MOTOTRBO Controller-less Recording Interface Introduction 346
6.12.2. Add Virtual Recording Interface 307
6.13. MOTOTRBO Capacity Max Recording Interface 353
6.13.1. MOTOTRBO Capacity Max Recording Interface Introduction 354
6.13.2. NexLog Capacity Max Configuration Detail 355
6.14. Omnitronics Recording 360
6.14.1. Omnitronics Recording Introduction 360
6.14.2. Recorder Configuration 288
6.14.3. Omnitronics Device Configuration 378
6.15. Tait Radio DMR/MPT Recording Interface 390
6.15.1. Tait Radio DMR/MPT Recording Interface Introduction 390
6.15.2. Add Virtual Recording Interface 307
6.16. Tait Radio Trunked P25 ISSI 399
6.16.1. Tait Radio Trunked P25 ISSI Introduction 399
6.16.2. RFSS Configuration Detail 399
6.16.3. NexLog Tait Radio P25 Configuration Detail 403
6.17. Zetron Logger 414

1. INTRODUCTION

1.1. Welcome

Thank You and congratulations on your purchase of an Eventide® NexLog Express Recorder.

Eventide invented the digital communications recorder in 1989. With thousands of communications recorders in service in such diverse applications as corporate call centers, NORAD, nuclear submarines, NASA, maximum security prisons, air traffic control, and 911 call centers throughout the world, Eventide continues its tradition of combining unmatched ease-of-use with mission-critical reliability.

This manual will help you maximize the use of your purchase. It includes:

- A quick-start bench test, for those who want to quickly familiarize themselves with some basic operations
- Guidance on installing your recorder
- Step-by-step instructions on how to set up and operate your recorder
- Descriptions of all of the controls and menu items on the System Console user interface

To help us reach you with information on updates and upcoming new features, please send us your warranty card. Eventide does not provide your information to marketers or any other outside organizations.

1.1.1. Intended Use

The NexLog EXP recorder is the ideal solution for capturing and storing telephone, radio, or intercom audio and available metadata for organizations that need 8 or fewer audio inputs recorded. The recorder is ideally suited for local Police, Fire, Education, Hospitals and Manufacturing facilities with critical recording requirements. Document is intended for trained Eventide Partners and their end users.

1.2. Customer Support Information

Eventide is committed to your satisfaction. If, after using this manual, you still have questions about the operation of your recorder, contact the Eventide Service department at service@eventidecommunications.com or call (201) 641-1200.

The Eventide website has additional information that may be helpful. Go to www.eventidecommunications.com.

1.2.1. Identifying NexLog Express Model and Version

You may need to identify the software version and serial number for the following products/components:

- Navigate to the recorder's address (example: http://192.168.2.100) with a web browser.

Fig. 1.1 MediaWorks EXP Login Screen (with arrow pointing to Setup Gear)

- Click the Configuration Manager gear icon in the bottom right corner.
- Log into the recorder here. Note that the default logon credentials for the recorder (before they are changed by the administrator) are User Name: *Eventide* Password: *<serial number>*. The Serial number of the recorder can be found on a sticker on the recorder.
- The system's Serial Number and current Firmware Version should be displayed.

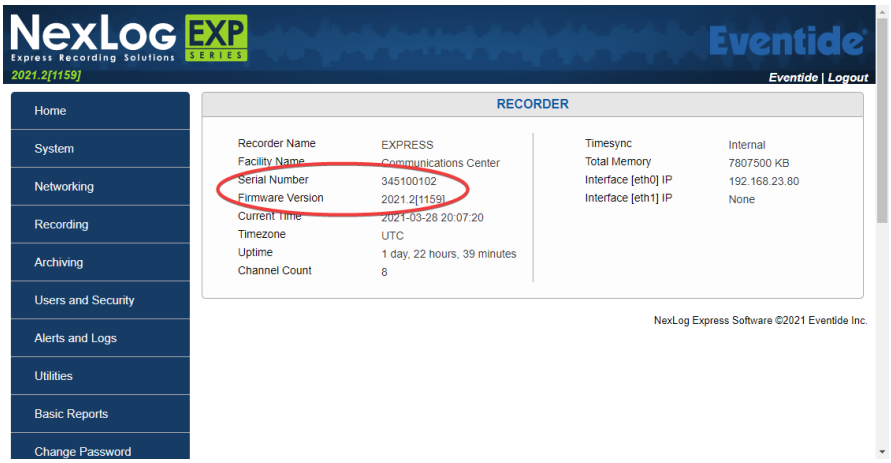


Fig. 1.2 Configuration Manager Home Screen (with Serial and Firmware circled)

- MediaWorks EXP: On the Help menu, select About to display the version information.

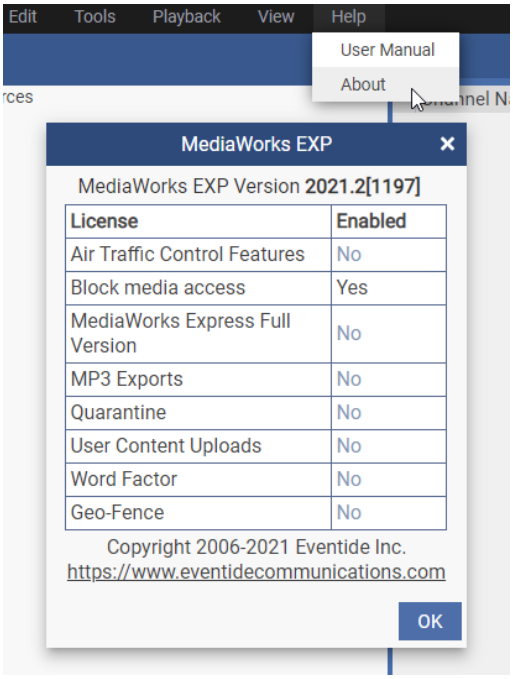


Fig. 1.3 MediaWorks EXP About Pop Up

This page was intentionally left 99.88% blank.

2. GENERAL SPECIFICATIONS

All Eventide NexLog Express Recorders are based on identical server (recorder) software and client (PC user) software. The primary differences among different units in the product line are physical, e.g., size, power, storage configuration, add-in board capacity etc. The following table highlights the differences among the products. This is a summary only and does not replace the individual unit specifications linked below.

2.1. NexLog Express Recorder

The NexLog Express Recorder is available with and without a touch screen control interface.

Table 2.1 Specification Summary

NexLog Express Recorder	
Product view	
Remote software	Web browser based NexLog Express Configuration Manager Web browser based MediaWorks EXP playback client
Operating System	Linux (embedded)
Call Record Database	Internal relational database with programmable retention
Channel Inputs	Compression Rates (Kbits/s): 13.3, 16, 32, 64 Mu-law Frequency Response: 200 to 3400 Hz Signal to Noise: -50dB Crosstalk: -60dB AGC: 24dB Boost Impedance: >10 K ohm
Network	Ethernet 1,000 Mbps (Qty. 2)
Height	1.75in (44.45mm) (1U)
Depth	14.5in (369mm)
Power Input	AC (100V ~ 240V) 260W

NexLog Express Recorder	
Weight	10.5 lbs (4.8kg)
Analog channels	0-8
Digital PBX channels	0-8
VoIP channels	0-8
Recording Capacity	80,000 hours
Standard Storage	Software RAID1
Optional storage	Removable USB media, NFS, SMB

2.1.1. Front Panel

Fig. 2.1 NexLog Express Recorder Front Panel

The NexLog Express Recorder requires that a monitor, keyboard, and mouse be plugged in for local configuration (setting of the IP address). Note that once basic networking setup is completed, it is possible to access all other configuration settings remotely via a web browser.

2.1.2. Rear Panel

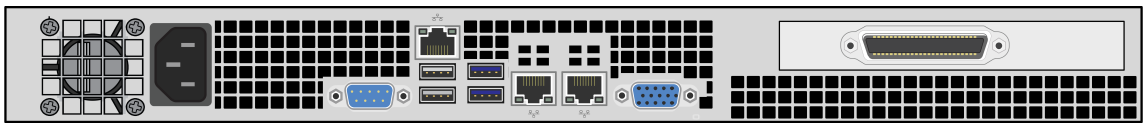


Fig. 2.2 Typical NexLog Express Recorder Rear Panel

The rear panel of this NexLog Express Recorder shows (from left to right): power supply, a RS-232 port for serial ANI/ALI and SMDR feeds or serial time sync, two USB 2.0 ports, two USB 3.0 ports, VGA and one slot for a telephony board.

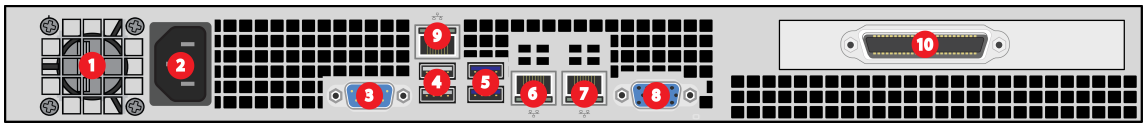


Fig. 2.3 Diagram of NexLog Express Recorder Rear Panel

1 - Power Module	6 - Ethernet Device 1 (Eth0)
2 - Power Plug (NEMA 5-15P)	7 - Ethernet Device 2 (Eth1)
3 - Serial Port 1 [1]	8 - VGA Output
4 - USB 2.0 Ports	9 - Dedicated IPMI Interface
5 - USB 3.0 Ports	10 - Add-on Telephony Board Slot (optional)

[1] The serial port is a standard RS232 DB 9 port.

2.1.3. Operating Limits

Table 2.2 Operating Limits

Parameter	Range or Limits
Voltage	100 - 240VAC
Frequency	50 - 60 Hz
Power (typical/ max)	200W - 260W
Temperature	Operating +5C (41F) to 40C (104F)
Humidity	10% - 80% relative, non-condensing

Parameter	Range or Limits
Altitude	Operating: 5,000ft Non-operating +22,000ft Note: If operated at high altitudes, take special care that airflow is unrestricted by dust or obstacles.
Vibration (Hard Disk Drives)	Operating: .2 G, 5-300 Hz Non-Operating: 1 G, 5-300 Hz Note: There is a variant of the NexLog Express available for high vibration environments, which adheres to MIL-STD-167-1A (25 Hz)
Shock (Hard Disk Drives)	Operating: 1 G, 11 ms half-sine Non-Operating: 40 G, 11 ms half-sine Note: There is a variant of the NexLog Express available, that has passed MIL-S-901D medium weight, Grade “B shock testing.
Orientation	The NexLog Express should always be mounted on a flat, non-sloping surface.

3. RECORDER SETUP

3.1. Unpacking the Recorder

Check the box for damage. A crushed box, holes, or water damage, for example, could indicate that the recorder has been damaged. Open the box and inspect the recorder and associated accessories. If the equipment appears damaged contact Eventide right away and save the damaged box and packaging!

Check that the unit is delivered with the expected configuration and accessories. The packing slip states the contents. In addition, the box will include:

- One power line cord per power supply module
- One server software DVD disk labeled “Eventide NexLog Express Software”
- A disk with this manual and other documents.

Other accessories may be included, depending on your order. For example, you may receive additional documentation, software, or cabling.

3.2. Bench Test

Before installing the unit, you may want to run a brief bench test, especially if you are unfamiliar with Eventide NexLog Express Recorders. The following steps are a suggested bench test procedure, which you may modify as you wish. If you change settings, note the defaults first and set them back to the defaults after you complete the test.

- Plug in the provided line cords to the appropriate line voltage.
- The boot process will start and diagnostic messages will scroll by on the display.
- After several minutes, the screen will show the INFO screen, one of three top-level screens. The others are SETUP and REPLAY, which are accessed by the magnifying glass button and the gears button respectively.

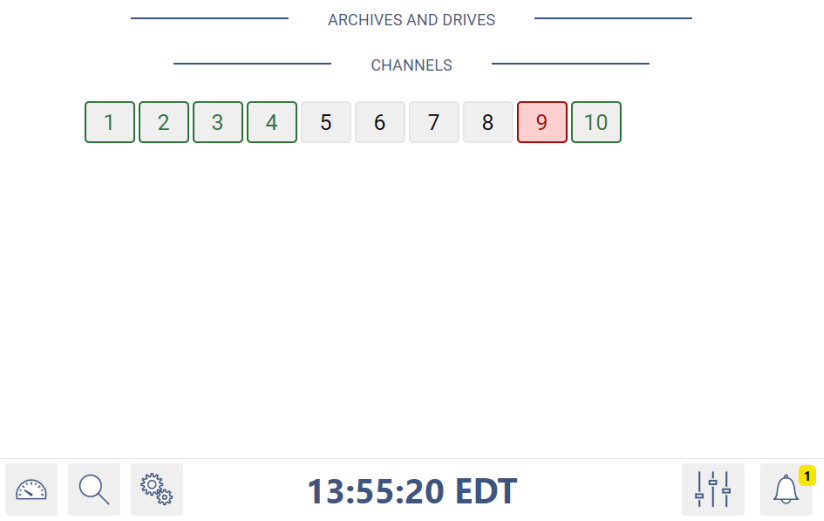


Fig. 3.1 System Console Info Screen

- The Channel Status section tells you which channels the recorder recognizes as ready for recording. For example, if you ordered analog-only you should see 8 green steady indicators. If you ordered 4 analog, plus 2 VoIP, you should see 4 green indicators, 4 gray, then 2 green. This is because an analog board has 8 physical channels, but only 4 would be enabled.
- Look at the menu buttons on the bottom left of the display to view the main screens for the System Console. The available screens are as follows:

Info Screen

- View channel status
- Listen to real time activity on channels (Live Monitor)
- View and manage archiving status

Replay Screen

- Research and play back recordings stored locally and on archives
- Export recordings to removable media.

Setup Screen

- Configure the recorder.

Alarms Screen

- Access active alarms on the recorder

Login Screen

This option is only visible and available under certain configurations. See Section 7.6.2.2 Front Panel for more details.

> **Warning**
>
> Do not force a shutdown by pulling the power plug or using the power switch. A forced shutdown can result in corrupted files and loss of data.

When you have finished viewing each screen, you can shut down the unit as follows:

1. Go to the SETUP screen.
2. Press the Gear a second time to open the configuration menu.
3. Select System.
4. Select Power Off.
5. Select the Shutdown button.
6. Enter a reason for the shutdown.
7. Answer *OK* to the prompt.

After the recorder completes its controlled shutdown procedures, the unit will automatically shut down.

3.3. Installation

NexLog Express Recorders are computer equipment. They have essentially the same requirements, both physical and electrical, as standard servers, and similar attention should be paid to their environment to assure long life and reliable operation. Site preparation, especially for larger installations, may include providing rack cabinets and concentrating communication wiring – phone lines, radio, etc. – nearby.

⚠ Caution

Loggers can be quite heavy, depending upon the model and options.

Do not attempt to lift or install these units without assistance.

Do not attempt to rack mount any model without either shelf or rack-slide support. Rack slides are available as an option from Eventide.

Do not support these units using only the mounting ears.

3.3.1. Operating Limits

The installation should allow the units to operate within their electrical and physical operational limits.

For model the operating limits, see the model's specification page in Section 2: General Specifications

3.3.2. Location Considerations

When choosing a location, consider the following:

- Operating Limits. The location must respect the unit's operating limits, as listed in the model's operating limits section of this manual.
- Convenience. If the unit will be operated from its System Console, then it should be comfortably accessible to the operator. Service personnel should have access to the unit. If the unit is to be installed in a rack, special rack units that provide a horizontal writing surface are commercially available.
- Security. If the unit must be physically secure, then it can be placed in a locked equipment room with limited access. This will also help ensure data security. Consider that a user with access to the unit can remove power, disconnect the input cables, play back recordings, monitor calls, remove archive media, and do other things to compromise your data. Logins are no protection against a determined attacker with physical access to a machine. In short, if you are concerned about malicious users making a purposeful effort to gain unauthorized access to your data, then the only real protection is to place the unit in a secure location.
- Cable lengths. For analog signals, such as POTS lines and radio receiver outputs, cable lengths are not likely to be an issue. An adequate level can be obtained hundreds of feet from the signal source.

The unit has programmable adjustments for low or high signal levels. That being said, shorter cable lengths will create less signal attenuation and pick-up less noise than longer cable lengths. For tapping digital PBX telephones and T1/E1 circuits, maximum cable lengths are extremely important, and can be different for different makes & models of telephone systems. Contact Eventide technical service for digital-tap cable length information for your particular digital phone system or T1/E1 circuits.

- Particulates. The fans and hard drives, can be damaged by smoke and dust. If you find dust build up on the surfaces or the fans being clogged, consider changing the location.
- Power dropouts or surges. The unit should be protected from power dropouts and surges. The chosen location should have line power available that is not on the same circuit as equipment that draws a large current on start-up, such as electric motors or compressors or banks of fluorescent lights. Line voltage fluctuations, brown-outs, and power outages can result in loss of data and damage to the unit. An Uninterruptible Power Supply is required to mitigate these problems. For a list of approved UPS units, see Section 3.3.4: Connecting AC Power.
- Spilled liquids. Liquids spilled on the unit can damage it. The location should not encourage people to place coffee cups on the unit, for instance.
- Vibration and Shock. Vibrating or physically shocking the unit while the hard drives are operating could damage the hard drives. The location should not be subject to vibration or jolting while the unit is operating.

3.3.3. Mounting Options

As normally provided, the unit can be mounted on any flat, non-sloping surface that can bear its weight. It can be rack mounted if the rack has a shelf to support it, and the supplied mounting ears can be attached to the rack with the rack screws provided, in order to prevent casual removal.

3.3.4. Connecting AC Power

The recorders use “universal” power supplies. All NexLog Express Recorder systems ship with US type power cords, end customer must provide a country appropriate power cord. This means you can plug the recorder into any line (mains) voltage from 100 volts to 240 volts nominal. However, to prevent unplanned shutdowns caused by power glitches or interruptions, Eventide strongly recommends the use of an Uninterruptible Power Supply (UPS) unit that meets certain minimum characteristics:

The UPS must provide power for a long enough period to allow orderly shutdown of the recorder in case of power failure.

If your facility has a backup generator, the UPS should provide power long enough to operate the recorder until the generator becomes operational following the start of a power failure (typically a minute or less) PLUS a period long enough to allow orderly shutdown of the recorder in case of generator failure.

The UPS should be an approved model, i.e., one that can communicate its status to the recorder. This isn't strictly necessary if your facility is manned and personnel are trained to shut down the recorder using the appropriate procedure in case of power failure before the UPS battery drains. However, an approved UPS will keep the recorder running and automatically signal to the recorder to perform a safe shutdown when its battery power gets low.

Eventide offers commercial-grade, heavy-duty rack-mount UPS units. Eventide has tested the following units and confirms they work with the recorders.

Table 3.1 Tested UPS Models

Manufacturer	Rating	Rack Height
APC / Tripp-Lite	1500VA, 940W, 120V	2U (3-1/2 inch)
APC / Tripp-Lite	1500VA, 940W, 240V	2U
APC / Tripp-Lite	750VA, 120V	2U
APC / Tripp-Lite	750VA, 240V	2U
APC / Tripp-Lite	3000VA, 2700W, 120V	2U
APC / Tripp-Lite	3000VA, 2700W, 240V	2U

In addition, consumer-grade UPS units may be available locally and are suitable for more casual installations and shorter run-times. Eventide has tested the following units and confirms that they work with the recorders.

Table 3.2 Tested UPS Models

Manufacturer	Model
APC	Back-UPS ES 500
APC	Back-UPS ES 725

To connect your recorder to a UPS, simply plug the UPS into an AC socket, and plug the recorder into the UPS using the power cords provided. If you use an approved UPS, also connect the UPS to one of the recorder's USB connectors on the rear panel using the cable provided with the UPS. This communication link will perform a safe shutdown when necessary, and also allow the recorder to notify you (by display and optionally by email) if there is a power problem.

> ⚠ Caution
>
> The power cords are used to disconnect NexLog Express Recorders from all main power. Remove all power cords before servicing the unit.

3.3.5. Before Connecting Audio

Before you connect the telephone lines, radio outputs, or other signals to be tapped and recorded, set the recorder's internal clock, date, time zone, and channel names. If you are installing new software on a currently operating recorder, disconnect the audio inputs until you have restored the configuration of the recorder, including channel selection and time zone. The reason for this is that the recorder will begin recording as soon as it detects an input signal. Calls with the wrong time, date, and time zone may get recorded and will likely remain on the recorder for a long time. This might be confusing later when you search, filter, and archive calls. Refer to Section 7.1.2 Date and Time of this document for configuration information including Date and Time settings.

3.3.6. Connecting Analog Audio

This section applies to units equipped with one or more Analog Input Boards. If you are not sure this board is installed, check the printed back-panel diagram that was packed with your recorder.

> ⚠ Warning
>
> To reduce the risk of fire, use only 26 AWG or larger telecommunication wire.

The Analog Input Board handles interfacing to analog audio signals. The number of channels per board will vary depending on which is ordered.

A mating connector is provided for each board unless a Quick Install Kit has been ordered (see The Optional Quick Install Kit). The connector has two rows of contacts. One row is numbered 1 through 25, and the other row is numbered 26 through 50. Numbering is such that pin 1 is opposite 26, and 25 is opposite 50. Each audio input requires two wires, in what is known as a “balanced” configuration. There is no “ground” connection. The channel and connector pin correspondence is detailed in Appendix C: Channel Wiring for Analog Input Boards.

To connect a telephone line to a given channel, simply connect the two wires to the two pins for that channel. It is not necessary to check or observe polarity.

To connect an audio source such as the line output or recording output of a radio, connect the “hot” lead to one pin and the ground or shield lead to the other. Again, there is no distinction between input pins. Either can be connected to the “hot” lead.

Any audio source may be connected, provided that the audio voltage is nominally in the .1 - 1 Volt range and remains fairly constant. Differing voltage levels are compensated for when setting up the board parameters from the recorder front panel. Not recommended are sources with greatly varying levels, such as “speaker” outputs. Also unusable are “microphone” signals, whose levels are too low by far to be usable without pre-amplification.

3.3.6.1. The Optional Quick Install Kit

For each telephone recording board in the recorder, you will have received either a mating blue-ribbon connector, or if ordered as an option, a Quick Install Kit. The connections for the mating blue-ribbon connector are detailed in Appendix C: Channel Wiring for Analog Input Boards. The pins are numbered on the connector itself for reference.

The Quick Install Kit, Eventide part #109033-003 (3-meter cable) and #109033-007 (7-meter cable), include the following components:

Table 3.3 Quick Install Kit Components

	Cable Connects the recorder telephony board to the punch block. The rear-entry connector (right in photo) goes to the recorder and is fastened to the telephony board rear panel with small wire bails on each side. The end-entry (left in photo)

RJ-21 male connector goes to the punch block and is held in place with a Velcro strip.

> Note: This cable may have special wiring! Before substituting a standard 50-pair extender cable for this cable, confirm that the telephony boards in you recorder do not have special connections. (Appendix C: Channel Wiring for Analog Input Boards). If you need a greater length, you may use an extender cable in series with the cable provided as part of the kit whether or not it is one with special wiring.

Punch Block

The punch block is a convenient, industry-standard appliance used to connect twisted pair telephone wiring to the recorder. It provides a central location to connect your physical wiring.

The 25-pair “Split 50” 66 Block has 50 rows and four columns. Each row contains four connectors (contacts). Each outside contact contains an electrical connection to the one next to it, creating a pair of contacts, but the left pair of contacts are electrically isolated from the right pair of contacts (thus, they are “split”).

Using a punch-down tool (not provided), the telephone wires are forced into a slit cut in the contacts in the block, which makes a firm electrical and physical connection. The blocks are usually mounted in the orientation shown.

The right side of the block has a female RJ-21 connector for the cable that goes to the recorder. The left side of the punch block (opposite the RJ-21 connector) is used to connect the telephone (or other audio) lines.

Bridging Clips

The right side (nearest the connector) has each column connected to an associated connector pin-pair so that the top row is connected to pin 1, the next row to pin 26, the third to pin 2, etc. Thus, adjacent vertical rows form one signal pair.

When you connect the first telephone line, you just start at the top and connect the wire pair to the first two rows on the left. The next wire pair would go to the next two rows down, on the left.

Finally, to connect the telephone line to its associated recorder input, slip two bridging clips over the two center contacts in each row.

The purpose of the punch block system is to centralize your connections, as well as to provide a clean way to isolate the telephone or radio system from the recorder, should it become necessary. The components can be isolated by removing clips, rather than removing wires.

3.3.7. Connecting Digital Audio

Note: For tapping digital PBX telephones and T1/E1 circuits, maximum cable lengths are extremely important, and can be different for different makes & models of telephone systems. Contact Eventide technical support for digital-tap cable length information for your particular digital phone system or T1/E1 circuits.

This section applies to units equipped with one or more Digital PBX Station tapping Boards. If you are not sure this board is installed, check the printed back-panel diagram that was packed with your recorder.

> **Warning**
>
> To reduce the risk of fire, use only 26 AWG or larger telecommunication wire.

The Digital PBX Station tapping Board handle interfacing to certain Digital PBX Station makes and models (check with Eventide for compatibility). The number of channels per board will vary depending on which is ordered. Eventide sells 8, 16, and 24 channels versions of the Digital PBX Station tapping Board.

A mating connector is provided for each board unless a Quick Install Kit has been ordered (see Section 3.3.6.1 The Optional Quick Install Kit). The connector has two rows of contacts. One row is numbered 1 through 25, and the other row is numbered 26 through 50. Numbering is such that pin 1 is opposite 26, and 25 is opposite 50. For most Digital PBX systems (except Mitel Supersets, Avaya Index phones, and ROLMphones), each Digital PBX Station requires two wires.

To connect a supported digital PBX telephone line to a given channel, connect the two wires to the two pins for that channel.

3.3.8. Connecting to an Ethernet Network

Connect to an Ethernet network by attaching a network cable between the RJ45 jack on the back of the recorder and your hub, switch or router. The cable should be CAT5 or equivalent with a male RJ45 plug for the recorder end and with the connector pin wiring going straight through from end to end. Alternatively, a crossover cable can be used to isolate the recorder from the network and connect directly to a PC's network connection without using a router or switch. NexLog Express systems have two RJ45 jacks and can be connected to multiple networks simultaneously.

See your model's Rear Panel section in Section 2: General Specifications for assistance identifying the ethernet port numbers.

This page was intentionally left 99.88% blank.

4. RECORDER OPERATION

4.1. Starting Up and Shutting Down

To start the recorder, use the front panel power switch.

NexLog Express Recorder: The power button is located on the front of the system.

> **Important**
>
> Do not hold the power button for more than one second.

To shut down the recorder, you can perform a controlled shutdown or a forced shutdown. In most circumstances, you should only perform a controlled shutdown. This allows the recorder to close all open files and complete current database operations before shutdown. A forced shutdown can result in corrupted files and loss of data. It can also damage any archive media in the process of being written, and possibly leave either gaps or duplications in your archives. (In addition, Eventide strongly recommends using the recorder with a UPS to allow a controlled shutdown in the event of a power failure.)

> **Warning**
>
> A forced shutdown can result in corrupted files and loss of data.

To perform a controlled shutdown of the recorder from the System Console:

- Press Setup (Gear icon)
- Press Setup again to open the side menu.
- Select System.
- Select Power Off.
- Select Shutdown, enter a reason and respond “OK” to the prompt.

If for some reason, it is not possible to use this standard method to perform a shutdown, a controlled shutdown can still be accomplished using the following, somewhat riskier, alternative.

Use the power switch to initiate a controlled shutdown by engaging the switch for up to one second.

Eventide does not recommend forcing a shutdown, but if it becomes necessary follow these steps.

> ⚠ Warning
>
> A forced shutdown can result in corrupted files and loss of data.

To perform a forced shutdown of the recorder:

- Engage the power switch for 10 seconds until it shuts down.
- An alternative way to perform a forced shutdown is to turn off the power supplies from the back panel, or unplug the power supplies.

5. CLIENT SOFTWARE AND PLAYBACK

NexLog Express Recorders are designed as standalone products, and it is not necessary to install the clients to use the product.

MediaWorks EXP does not require anything beyond a supported web browser and an appropriate internet connection to the recorder:

- Google Chrome
- Microsoft Edge (Chromium)
- Mozilla Firefox

For MediaWorks EXP to connect to the recorder with HTTP, port 80 must be open; for HTTPS, port 443 must be open.

A non-networked recorder controlled only through the recorder System Console may be adequate for some organizations. However, the advantages and extra functionality that are provided by the clients may be important to your needs.

This page was intentionally left 99.88% blank.

6. THE SYSTEM CONSOLE USER INTERFACE

The rear HDMI output provides direct System Console control over your NexLog Express digital logging recorder, enabling you to listen to recorded audio and manage recorded calls. To use it, simply connect a display, keyboard and mouse to the unit.

Upon connection to the System Console, you will be presented with options for Configuration Management and Recording Playback. See the related documentation for more information.

- Configuration Management: Section 7
- Recording Playabck: External MediaWorks Manual

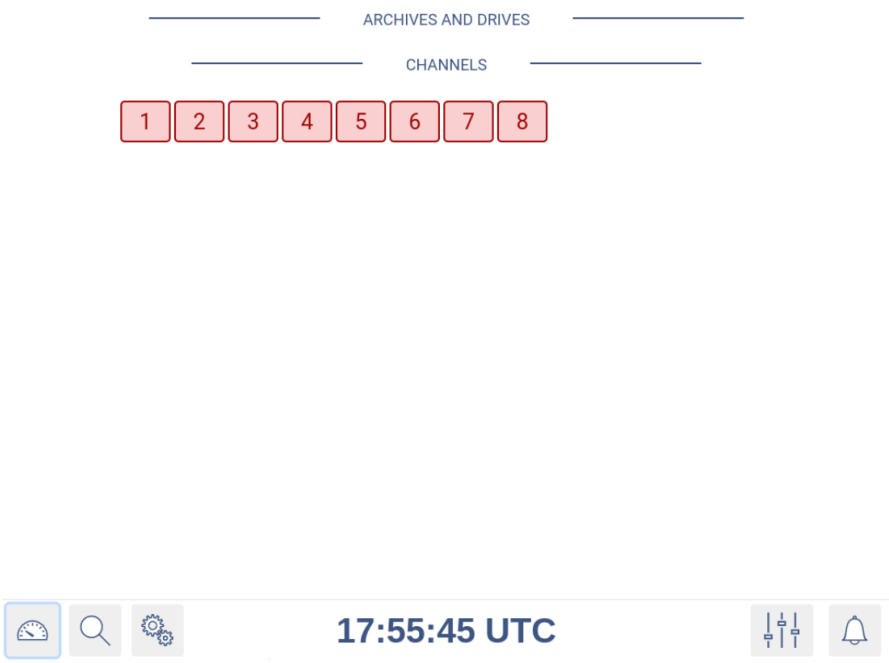


Fig. 6.1 System Console Info Screen

-  Info: Shows information about archives and channel activity at a glance.
-  Replay: Search, play and gather recordings into incidents.

-  Setup: This mode is used to configure the recorder.
-  Settings: Change settings for the System Console, such as disabling the on-screen keyboard.
-  Alerts: Display any active alerts for the system.

7. CONFIGURATION MANAGER

This section covers setup and administration of the system using the NexLog Express Configuration Manager tool.

Fig. 7.1 Configuration Manager Home Screen

> **Note**
>
> Eventide NexLog Configuration Manager has been tested with the following web browsers:
>
> - Google Chrome
> - Microsoft Edge (Chromium)
> - Mozilla Firefox
>
> Other web browsers will most likely be usable as well, but you may experience some visual glitches or missing functionality.

There's two ways to access Configuration Manager for remote management. One is to navigate to the IP address of the recorder and click the gear icon in the bottom right corner. The other is to add "/admin" after the base IP address or hostname in the address bar. For example: `http://192.168.2.1/admin`

Logging into the Web Configuration Manager always requires authentication. By default, the User Name: *Eventide* Password: *<serial number>* are installed at the factory. It's always recommended that these defaults are changed to something secure once the recorder is installed.

Navigation

Once authenticated through a web browser you will see the Eventide Configuration Manager. On the left side is a list of top level configuration categories. Clicking on a category will expand it, so you can see the configuration pages inside the category. Clicking on a link will take you to the corresponding Configuration Manager page. Each page is designed to allow the user to configure or view the status of an aspect of the recorder's configuration. The categories and their contents are listed below.

7.1. System

This section of Configuration Manager is used for configuring core system details such as licenses, storage devices, and time. Each sub-section is listed below.

7.1.1. System Info

This screen has 3 tabs labeled CONFIGURATION, IDENTIFICATION, and HISTORY. Clicking on a tab header will activate that tab.

7.1.1.1. Configuration

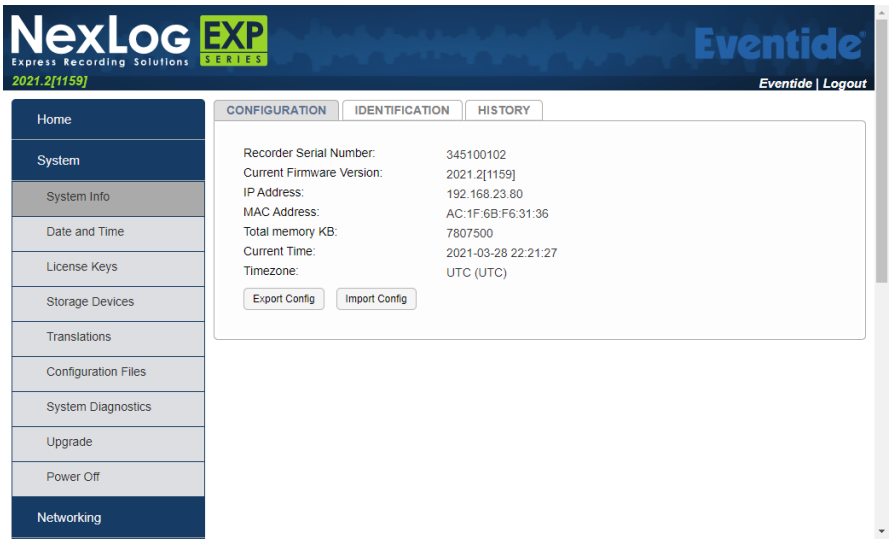


Fig. 7.2 System Configuration Screen

Recorder Serial Number: Assigned by the Eventide factory to identify a system.

Current Firmware Version: Software version and build number running on the recorder.

IP Address: Address of the first Ethernet port in the system.

MAC Address: Media Access Control (MAC) address of the first ethernet port in the system.

Total memory KB: Amount of usable RAM in the system.

Current Time: Current local date and time of the recorder.

Time zone: Time zone setting of the recorder.

In addition to all the information described above, this page contains two additional important buttons, 'Import Config' and 'Export Config'. Export Configuration allows you to export all of the recorder's configuration settings for back up and safe keeping. 'Import Config' allows these settings be re-loaded into the recorder. This is designed to allow you to back up and restore your settings, for example, if you want to reinstall your recorder's firmware. You can also use this option to import the configuration from a different recorder with identical hardware. It is not supported to import Configurations across different hardware (models, storage devices, telephony boards), or software versions. For example, if the configuration you want to import was exported under 2020.1[635], you should install 2020.1[635] on

the recorder, restore the configuration, and only then upgrade the recorder to the latest. After performing a configuration Import, it is required to immediately reboot your recorder for changes to take effect; this will happen automatically.

7.1.1.2. Identification

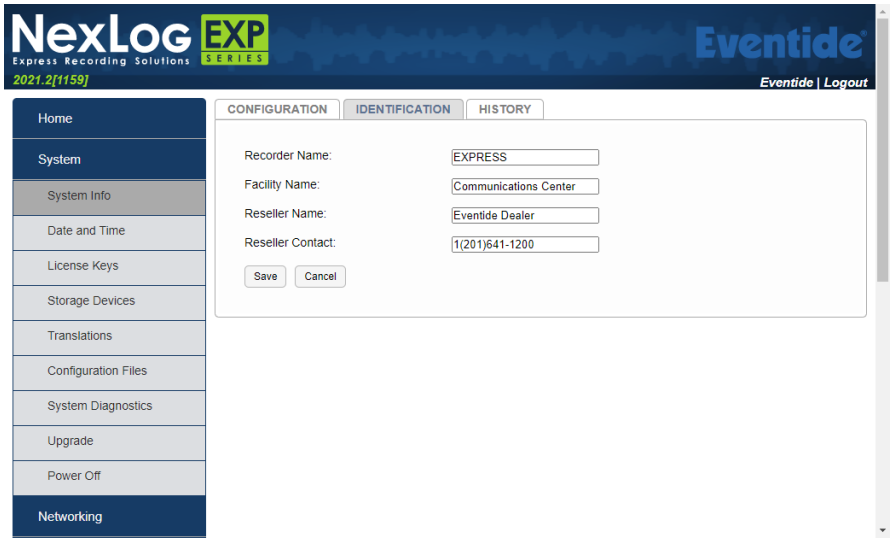


Fig. 7.3 System Identification Screen

Recorder Name: The logger name that will be displayed in remote clients.

Facility Name: The facility name (i.e.: location) that will be stored on archive media.

Reseller Name: The Eventide dealer providing maintenance and support.

Reseller Contact: The contact information for the Eventide dealer.

7.1.1.3. History

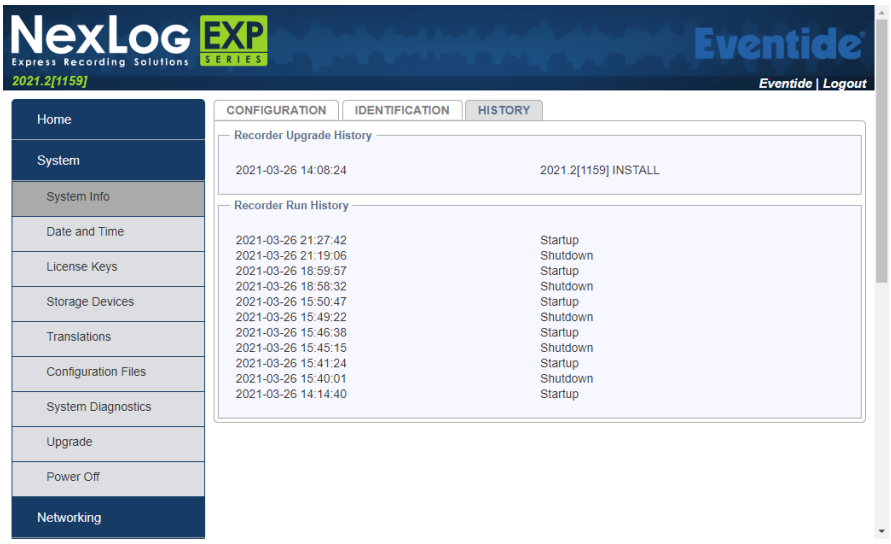


Fig. 7.4 System History Screen

Recorder Upgrade History: Displays a history of the first firmware install on the recorder and subsequent updates.

Recorder Run History: Displays a history of system startup and shutdown. Also note that unplanned shutdowns are noted in this list and usually indicate a power failure to the recorder. Unplanned Shutdowns can cause severe issues and should be avoided.

7.1.2. Date and Time

This page allows you to configure your date/time and time sync settings. The top two items are Time and Time zone. To modify these settings and have them take effect when you click 'Save', you must first click the 'Edit' checkboxes. This is to protect you from accidental changes.

Time and Time zone are very important settings on the system. It is recommended that the time is configured before any recordings begin. Recordings generated when time is incorrectly set will be recorded on the wrong dates/times and may be impossible to find or overlap with other properly recorded calls.

Regardless of the configured time zone, call records are actually stored in the recorder's database in UTC time zone and converted for display and querying. The time zone is also used for synchronizing with a time source that provides Local Time rather than UTC (see below.)

In addition to setting your time and time zone, this page allows you to set your Time Sync settings. Time sync settings allow you to adjust your system's internal clock to an external source to make sure the internal time and all recording timestamps remain accurate and synchronized across your organization. Eventide highly recommends the use of time sync. When you select a time source via the Time Sync dropdown, all configuration settings relevant to that time source will appear below.

The available time sources are:

- None: No Time sync, only the recorder's internal clock will keep time
- NTP: Network Time Protocol. You can configure the IPs of up to 4 NTP time servers. Only one will be used at a time, but others are backups in case the recorder cannot reach a primary time source. Normally, the recorder will slowly "slew" the current time to the time source's time if they do not match to prevent large time jumps. The Force Sync option will save the current settings and immediately set the recorder time. This is useful when first setting up a recorder.

New in version 2024.1.

In order to add an additional layer of security and prevent faulty time information, NTP authentication can be cryptographically-based by following the steps below:

- Click "Edit NTP Authentication Keys" under the NTP SETTINGS Section.
- Enter the Auth Key #, the hash function, and the authentication key, all of which should be provided by the NTP server admin (as seen below), then click "Save".

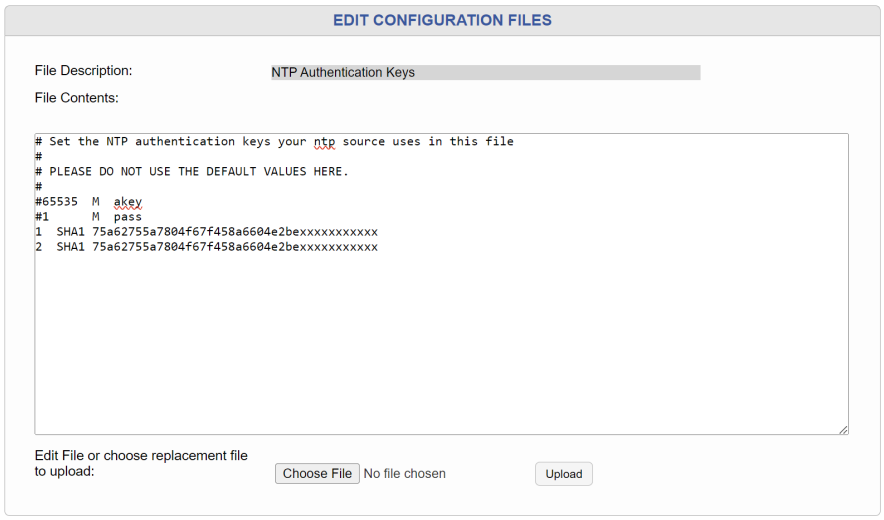


Fig. 7.5 Authentication Key

- Go back to System —> Date and Time —> NTP SETTINGS Section
- Enter the Server Address and the Auth Key # corresponding to what was provided in the NTP Authentication Keys configuration file
- Click “Save and Force Sync”

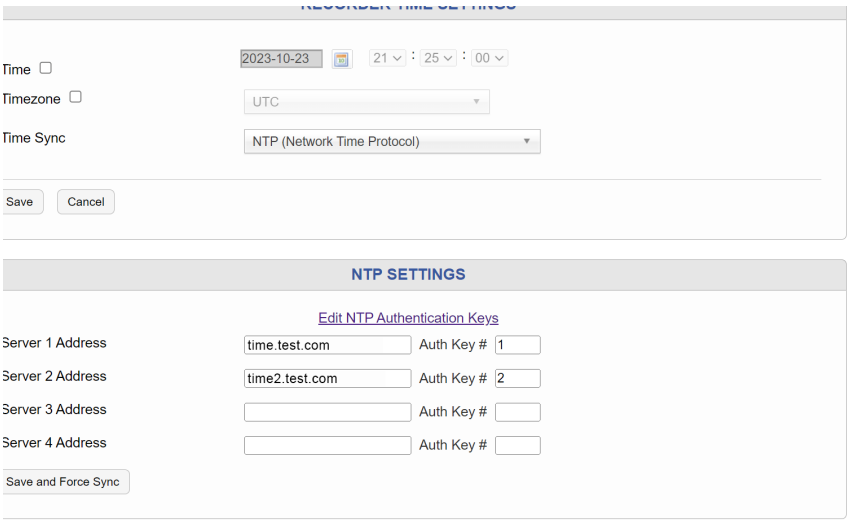


Fig. 7.6 NTP Server and Auth Key #

> **Note**
>
> Up to four NTP Authentication keys can be used.

- IRIG: Only relevant if you have purchased the optional IRIG-B time code reader for your recorder. IRIG-B is a time source protocol provided over a coaxial cable. You can select whether your IRIG-B time source is providing current time in the UTC Time zone, or in the Local Time zone you have configured under 'Time zone'
- RS-232: Some Time sources provide time over an RS232 (Serial) Cable plugged into the recorder. Here you can configure which serial port you have your time source plugged into and which of the supported formats the time source will be formatting the timestamps in. You also select serial settings to match your time source such as Baud Rate, Parity, Number of Data bits and Number of Stop Bits. Like IRIG-B you can configure whether your time source is sending time stamps in UTC or Recorder Local Time.
- NEMA: National Marine Electronics Association

  Select the serial port where your NEMA protocol GPS receiver is connected.
- Wharton: Wharton is a special case of RS232 time sync which does not have any options about baud rate or format, as this is hard coded as part of the protocol. In addition, only the first serial port can be used for Wharton.

Regardless of the time source you are attempting to sync to the recorder will only act on a timestamp received if it is within 5 minutes of the recorder's own clock as a precaution against the recorder receiving an invalid timestamp from the time source.

Therefore, when first syncing to a new time source it may be necessary to first manually set the recorder's time close to the time source's time. In addition, the recorder will not allow large jumps in time due to a time source input, but will instead slowly 'slew' the recorders time towards the time source time. The recorder attempts to avoid time ever moving backwards, as this could cause overlapping recordings.

At the bottom of this page is some diagnostic information about the configured time source, from which you can see information such as jitter and reach ability of your time source. This information is useful for troubleshooting problematic time sources. It includes information about which time sources are configured, which are reachable, and which, if any, the recorder is currently synchronized to. You must click the refresh button to see the most recent data. The formatting of this information is identical to the standard UNIX / Linux command 'ntpq –p'.

For more information on the data format used search online for ‘ntpq’.

7.1.2.1. NIST Time Servers for NTP

You can search the web for NIST Time Servers. Historically, a list of National Institute of Standards and Technology (NIST) internet time servers can be found on the web at:

NIST Internet Time Servers

This list provides each server’s name, IP address, and location. It is probably best to select one near to your location. If you have difficulty with using a server name, you can access the server using the IP address instead.

7.1.3. License Keys

License keys are purchased from Eventide to enable core and additional functionality. Your recorder will ship with one or more license keys installed, and you may also be sent additional license keys if you upgrade or add new options to your recorder. License keys are entered on this configuration page.

There are three kinds of license keys:

- Primary License Key
- EXP Software Update Subscription Key
- Hardware Warranty Key
- Add-On License Key

If the primary key and software subscription key are not entered, or does not match the hardware, the system will run normally for 7 days during a grace period, and then certain functions, such as archiving and call playback will become unavailable until a valid key is entered. You cannot delete a primary key or add more than one, only edit your primary key. Each license key is a string of number and letters provided by Eventide. When you add or edit a key, you will see it in the list along with either the text ‘Not a Valid License Key for this Recorder’ or a description of which features the license key enables. If the license key itself is valid for your recorder but does not provide adequate coverage for your installed configuration (for example if you add in an additional Analog Board beyond your licensed channel count), the particular field which is not adequate will be marked as “INVALID”. For the license to function on your recorder, it must be valid for the recorder itself, and cover the installed features. If your license key does

not cover your purchased features, such as if you purchase an additional Analog Board, you must get a new license key from Eventide.

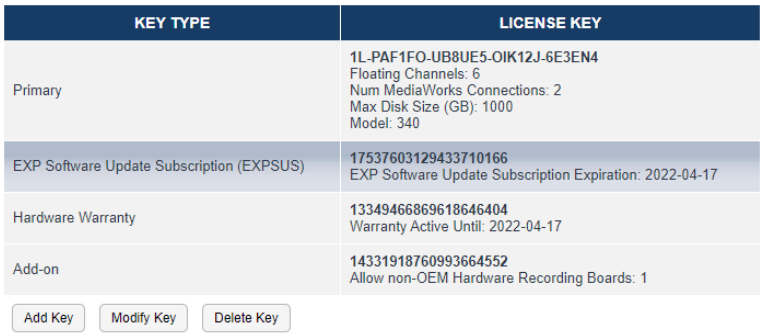


Fig. 7.7 Example License Page with a Primary key, Software Subscription, Hardware Warranty and two Add-on Licenses

7.1.3.1. Primary License

This license key controls your system's core functionality such as the system's model, the number of recording channels, and the maximum storage size.

7.1.3.1.1. Floating Channels

The maximum number or recording sources allowed on the system. This includes analog, digital, and IP (VoIP, RoIP) sources. Floating channels can be activated based on setup requirements. See Section 7.3.1: Recording Interfaces for more information on usage and configuration.

7.1.3.1.2. Num MediaWorks Connections

The maximum number of simultaneous MediaWorks EXP client playback connections allowed.

7.1.3.1.3. Max Disk Size (GB)

The maximum recording storage size allowed. When the used recording storage amount is exhausted. The system will purge the oldest unprotected records first.

7.1.3.1.4. Model

This value indicates the operating platform the license was issued for.

7.1.3.2. Software Update Subscription

NexLog Express Recorder Software is licensed on a subscription basis via the EXP Software Update Subscription (EXPSUS) license. See your recorder's System: License Keys page or System: Upgrade to check the date your subscription is valid through. Only software released prior to this date will be valid for this recorder. Please contact your reseller for more information on extending your software subscription.

> **Note**
>
> if your EXP Software Update Subscription is valid through May 1, 2022, and the version you want to upgrade to was released April 6th, 2022, you will be able to perform the upgrade on May 5th, 2022. It is the date that the full upgrade was released that is limited, not the date of applying the full upgrade.

License expiration warnings are automatically scheduled based on the following timelines:

- EXPSUS Alert comes up 37 days before license expiration
- EXPSUS Alert + Configuration Manager/MediaWorks DX red warning dialog comes up 30 days before license expiration
- EXPSUS Alert + Configuration Manager/MediaWorks DX red warning dialog comes up 7 days before license expiration
- EXPSUS Alert comes up when software license has expired

Expiration Warnings are listed under the NexLog Express logo, as seen below:

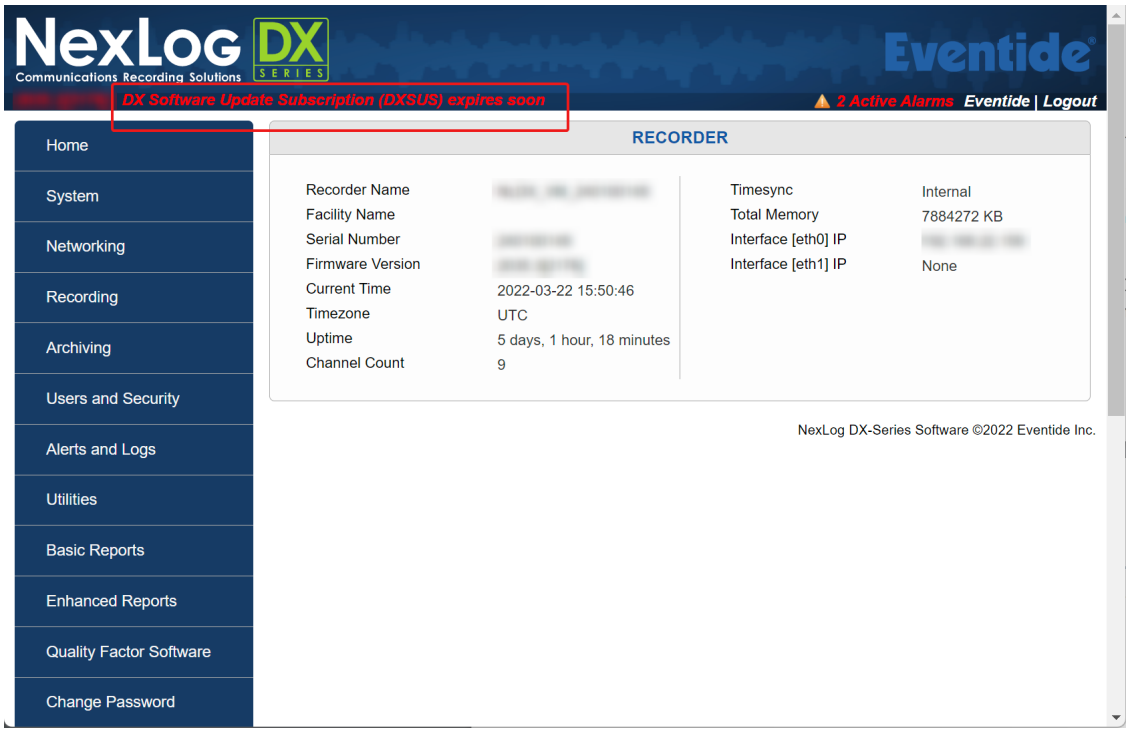


Fig. 7.8 EXP Software Update Subscription License Expiration Warning

7.1.3.3. Hardware Warranty License

The expiration date of your NexLog Express hardware's warranty will be listed in this license key. This is for the factory warranty only. Eventide Communications Dealers may offer an extended warranty for your hardware directly. Consult your Eventide Communications Dealer for more information.

7.1.3.4. Add-on License

Additional hardware and software features not covered by the Primary License will be listed as an Add-on License. This includes features such as playback client connections, archive destinations, VoIP recording channels, etc. Each add-on key can provide up to three features.

7.1.4. Storage Devices

This page presents information about hard drives and RAIDs connected to your recorder. You can visualize the amount of free and used space, the serial number of disk drives, and RAID Configuration and settings. The “Refresh” button is used to refresh the information provided on the page. After the page loads, you will see at the top of the page a Hard Drive Icon representing your RAID or SAN along with a description of what type of storage device your recorder has installed (Hardware RAID, Software RAID, or SAN). To the right of the icon will be a status indicator if the drive is degraded or rebuilding. The red text DEGRADED is displayed if the RAID is currently running in a degraded state. If the RAID is rebuilding, the yellow text ‘REBUILDING’ will be displayed as well as the current percentage of the rebuild that is complete. When a RAID is degraded, there is no data redundancy so it is important to replace the failed drive as soon as possible. Also displayed is an indicator of how full the storage device is. On a heavily loaded system or a system that has been running for some time, it is normal for a storage device to appear as full or almost full at all times. This is because the recorder is usually configured to remove older, unprotected media records as new media records begin.

Fig. 7.9 Storage Devices: Hardware RAID-1 Example

To the left of the icon is an icon that looks like a plus sign. Click this icon to expand the storage device to see details about the device.

The detail view will display information about the sizes of each partition on the drive, its size, and how much free space remains. Above this is a ‘history’ button. Pressing this button will display the device

history, which is a log of important events that have occurred on this drive, such as RAID Degrades. The 'Disks' heading which is only displayed for RAID Systems displays disk drives in the RAID. For each drive, the Device ID and Serial Number of the Hard Drive are displayed. In addition, the current status of the drive is displayed. The possible status values are as follows:

- ACTIVE: The drive is currently active and functioning in the RAID
- DEGRADED: The drive is in the RAID but not providing redundancy, either because it is failed or because it is still being rebuilt onto.
- REBUILDING: A new drive has been added to the RAID or an existing drive is being synced into the RAID. A completion percentage will be displayed; refresh the page to see this percentage update as the rebuild happens.

> **Note**
>
> The Verified Rebuilding Status on RAID 6 will now show the progress percentage when two drives are in the Rebuilding state. After the first drive completes its rebuilding process, the percentage will reset and start updating again with the progress of the second drive until it completes as well.

- REMOVED: There was a drive in this position (slot) in the RAID but it has been removed. RAIDs with REMOVED drives are by definition degraded. A new drive should be put in the REMOVED slot and added to the RAID as soon as possible.
- FAULTY: On software RAIDs this state indicates an otherwise well-functioning drive that has been forced into a failed state by a user. This state is the first step in removing an otherwise functioning drive.
- IDLE: The drive is not associated with the array in any way.

The 'Options' button next to the drive status will give you a menu of options for the selected drive:

- History: View a history of important events that have occurred to the drive.
- Remove: will remove the disk drive from the RAID if it's a hardware RAID or if the device is already FAULTY or DEGRADED
- Set Faulty: option to begin the removal process for a Software RAID system on a drive that is currently ACTIVE
- Add: A drive that is IDLE or REMOVED can be added into a RAID to be utilized by the RAID

The serial number displayed for each drive in the RAID can be helpful in the case of a failed drive, to verify which drive needs to be replaced.

Note

With some Hardware Raid controllers, it is normal to see storage device consistency check logs on first boot when viewing “History for All Devices” or for the History for the specific Raid device. This is the RAID controller reporting its actions as it initially makes the RAID consistent after installation.

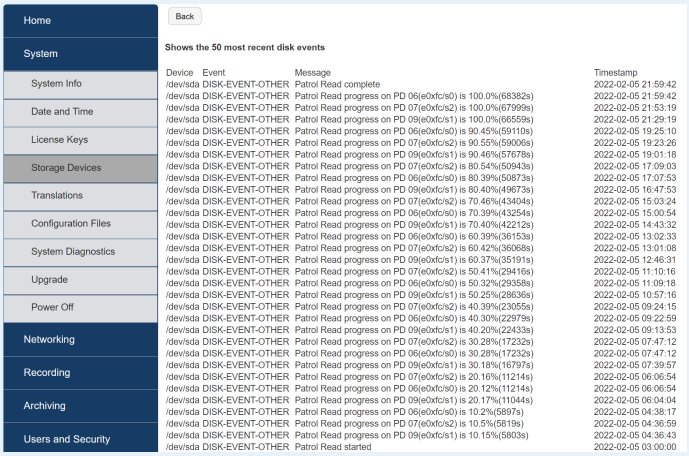


Fig. 7.10 RAID Consistency Check

7.1.5. Translations

NexLog Express supports using MediaWorks EXP in multiple languages via user-configurable translations. The translations are user-customizable and presented in a list of text “strings” that you can edit for clarity.

7.1.5.1. Translations Basics:

You can view, edit and upload Translation files stored on the recorder in Configuration Manager via the System: Translations page.

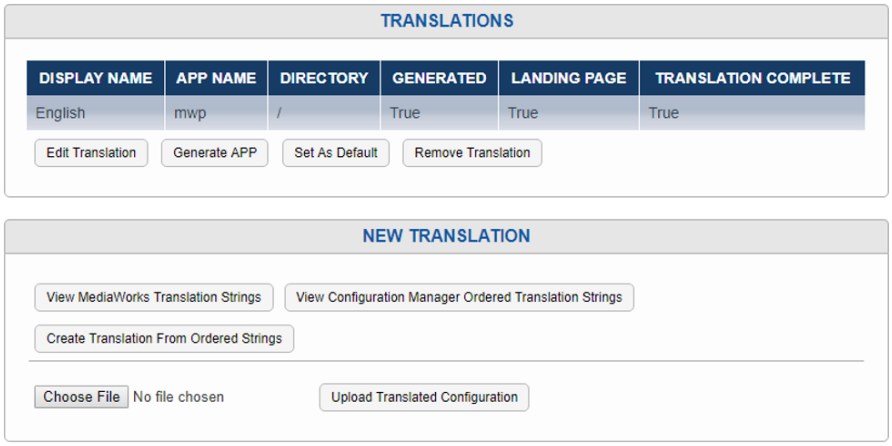


Fig. 7.11 Translations

At the top is a list of currently loaded Translation files, with important information displayed in a column view. Note that a full translation requires a pair of files, one for MediaWorks EXP and one for elements of MediaWorks EXP that draw on elements from Configuration Manager, such as Evaluations and Alerts. These are distinguished by App Name: mwp for MediaWorks EXP or webconfig for Configuration Manager.

The Display Name must be unique for each Translation, we recommend (Name of Language) (Name of APP) to keep things clear. For example, for French, we suggest having the display names be Française MWP and Française WC.

On the other hand, the Directory must be the same for each half of a translation. So, in this case, both Française MWP and Française WC should have a directory of “fr”.

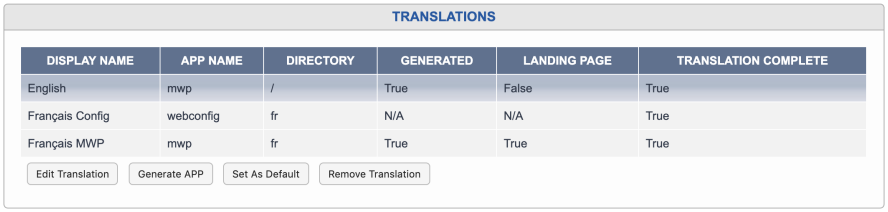


Fig. 7.12 Translations Configured

Set as Default changes which language the Welcome page will use as the main link to MediaWorks EXP. By default, this is English, and other language choices will appear below the MediaWorks EXP icon, listed by Display Name. On a system configured as above, however, the icon would link to the http://*your recorder-IP address here*/client/fr/mediaworks/ address, leading to the French translation.

Generate App will be covered in the next section, as it makes more sense in context.

7.1.5.2. Creating A Translation:

To create a new translation, start by clicking the View MediaWorks Translation Strings button. A string can be a word, a number, a sentence, and these strings make up all the text directly visible in the MediaWorks EXP client. Text that appears in alerts, quality factor and archiving is optional to translate and is covered in the Configuration Manager Translation Strings, which will be next.

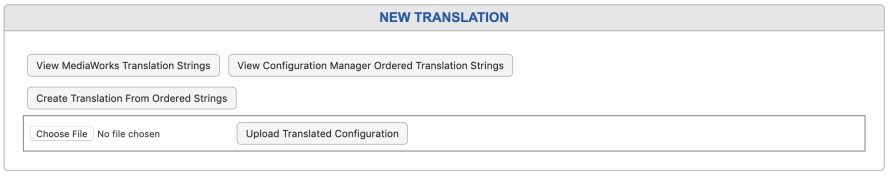


Fig. 7.13 New Translations

Once you've clicked View MediaWorks Translation Strings button, use the Select All button to select all the strings, then copy the selection and paste into a text file or word document. You can then translate each line manually, or, as we recommend, pass the lines through a machine translation service like Google Translate, to provide a first draft of a new translation and then refine the translation manually.

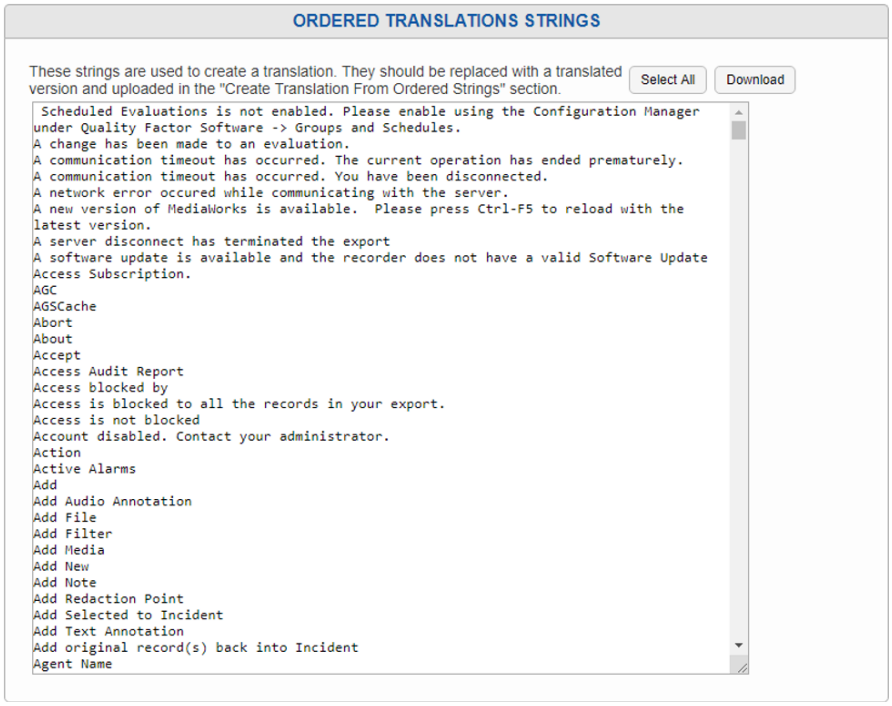


Fig. 7.14 Ordered Translations Strings Page

IMPORTANT NOTE: The translation created via Google will likely have amusing or embarrassing mistakes in it, for example, going from English to French it will change “Channel Name” into “Nom du canal” (“Name of Canal”), and from English to Russian it will want to “Rescue” your incidents rather than “Save” them. So, it is essential that a native speaker of the language-being-translated-to proofread the result to avoid obvious mistakes or confusing word choices made by the context-less machine translation.

ALSO IMPORTANT: The strings must be kept one to a line, in the exact order presented here, or the translation will not work correctly. Lines out of order will cause text to show up in the wrong places in the translation, or make the translation to not work at all.

Once you are ready to build a translation out of one set of strings, click the Create Translation From Ordered Strings button. This will bring up a page with a large text field pre-populated with this text:

```
[SETTINGS]
TRANSLATION\_DISPLAY\_NAME=<display name>
TRANSLATION\_OUTPUT\_DIRECTORY=<app path>
TRANSLATION\_APP=mwp
TRANSLATION\_DO\_DYNAMIC=1
```

```
TRANSLATION\_DISPLAY\_R\_TO\_L=0
[TRANSLATIONS]
```

Paste your translated lines beneath the [TRANSLATIONS] line, then scroll back up to the top of the field to fill in the settings:

```
[SETTINGS]
TRANSLATION_DISPLAY_NAME=Française MWP
TRANSLATION_OUTPUT_DIRECTORY=fr
TRANSLATION_APP=mwp
TRANSLATION_DO_DYNAMIC=1
TRANSLATION_DISPLAY_R_TO_L=0
```

Fig. 7.15 Translation Settings

The Display_Name must be unique for each Translation, we recommend (Name of Language) (Name of APP) to keep things clear. For example, for French, we suggest having the display names be Française MWP and Française WC. On the other hand, the Output_Directory must be the same for each half of a translation. So, in this case, both Française MWP and Française WC should have a directory of “fr”.

The Translation_APP is either MWP, for the MediaWorks EXP Strings or WebConfig, for the Configuration Manager Strings. Anything else will fail to load.

Translation_Do_Dynamic should be left as 1 if you want any custom field names to be translated; they will show up at the end of the app for editing once this is saved.

Translation_Display_R_To_L should be set to 1 if the target language reads right to left. Note this only changes the direction the text is written in; it does not flip the whole UI of MediaWorks EXP.

Once this is all configured, scroll down and click Save.

If successful, the Translations page will load again with a message saying: “Translation uploaded. Select “Generate APP” to enable the translation.” Click the Generate App button to create a custom version of MediaWorks EXP at the directory configured in the Translation settings.

The Generate App step is not required for Configuration Manager translations, but a MWP translation pointing to the same directory is required to make any use of it.

After making the MWP translation, one can translate Alerts, Quality Factor and Archiving windows shown in MediaWorks EXP by making a Configuration Manager Translation. Start by clicking the View Configuration Manager Ordered Translation Strings button and repeat the above steps, with one major difference: Alert strings contain variables such as <~1~> and <~112~>, which must remain whole during

this process. These variables substitute in text like the name of the recorder, the serial number of the recorder, error messages from the database, status messages passed along from third-party hardware installed in the system, etc.

Three things to note about the variables:

1. They must remain exactly as typed: <~1~> is good, but <~ 1 ~> is not. Translations by Google for some languages will modify the strings, and by using Find & Replace in Microsoft Word or other text editors, one can change all instances of <~ 1 ~> in the machine translation back to the required <~1~>. This must be repeated for <~110~>, <~111~>, etc, that you find throughout the list. Malformed variables will show up as plain text in the alerts.
2. The variables can be rearranged to better fit the grammar of the language. Missing variables are ignored. Extra variables are also ignored.
3. Because it is impossible to offer every possible string these variables can stand for, they are not translated and fall back to what they are by default in the English translation. In most cases, the variables will be easily understood numbers like software version or serial number; in other cases they will be highly specialized database strings that can will be useful when reported to dealers or Eventide Service when reporting a problem.

7.1.5.3. Editing an Existing Translation:

A translation may need a second draft; a word might feel awkward in context, or a phrase may be too long for the space available. Or perhaps an existing translation file is available, but your site wants to customize some of the terminology used. For these reasons and more we provide the option to edit existing translations.

To begin, select the file from the list and click the Edit Translation button. This will open the Edit Configuration File page for this language. You can edit the text here, or you can select all, copy, and paste into a separate text editor to make your changes, then copy and paste the entire list back into this page and save. If the file changed is a MediaWorks EXP translation, select the translation and click Generate APP to update it to the latest text.

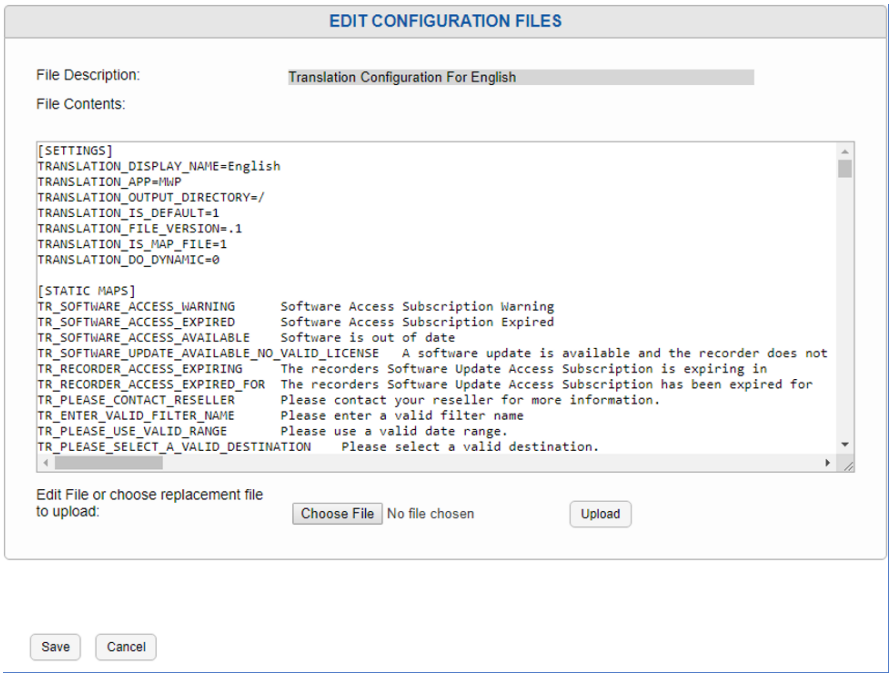


Fig. 7.16 Translations Edit Page

7.1.5.4. Upload Translated Configuration:

We recommend contacting Eventide Service to inquire about currently available translations, and then using the Upload Translated Configuration feature. To do so, choose the file with the Choose File button, then click Upload Translated Configuration. If the file chosen is a MediaWorks EXP translation, once it is loaded, select the translation and click Generate APP, to make it available on the welcome page.

7.1.6. Configuration Files

Here you can view and edit configuration files stored on the recorder. Most of the features that are configurable via files rarely need to be modified by end users. The contents for these files should be provided by Eventide or your Eventide Communications Dealer and simply pasted into the edit box. However, some of these are edited by end users, such as files for VoIP boards that need advanced configuration. Select your configuration file from the list and press the ‘View/Edit’ button.

Make any necessary changes here and press ‘Save’ to save your changes.

Briefly, here is a sample of the commonly edited files and their descriptions:

Advanced Network Configuration

Standard network configuration such as default gateways can be configured on the Network Page. This file is for adding additional networking routes to the recorder beyond default gateways. The format of the lines in this file is identical to the Linux route command. Use caution when editing this file, as mistakes may make the recorder unreachable. Note that changes made to this file will not take effect until the next reboot. Valid commands are “route”, “ifconfig”, and “iptables”.

Standard network configuration such as default gateways can be configured on the Network Page. This file is for adding additional networking routes to the recorder beyond default gateways. The format of the lines in this file is identical to the Linux route command. Use caution when editing this file, as mistakes may make the recorder unreachable. Note that changes made to this file will not take effect until the next reboot. Valid commands are “route”, “ifconfig”, “iptables”, and “ethtool”.

Terms of Service Display

A custom Terms of Service splash screen can be show at login time for all users if enabled in Users and Security: System Security. Edit this file to change the text shown at login.

Verbose Logging Filter Configuration

New in version 2023.1.

This file allows for targeted verbose logging that can be useful to Eventide technicians. Logging here can be configured for specific processes and channels so that the log files do not roll over as quickly. The specific processes can be configured in three different modes:

- NORMAL is the default logging level
- VERBOSE will provide additional log events
- MUTE will stop all logging from the process

Below is an example of how targeted logging can be configured:

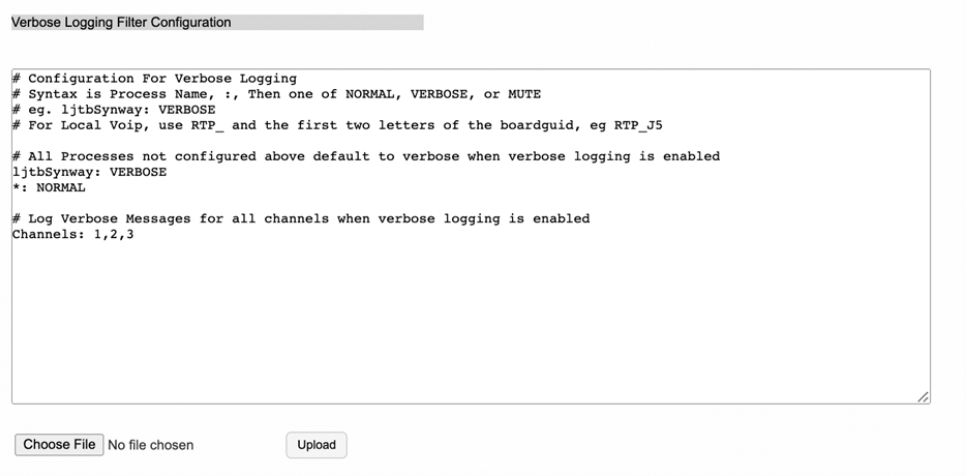


Fig. 7.17 Targeted Logging

In the example above the ljtbSynway process log messaging will be verbose, while all other processes will log in the default non-verbose mode. The verbose logging will only apply to channels 1,2 and 3.

> **Note**
>
> Ensure Enable Verbose Logging is selected for this feature (see Section 7.7.4 Logging)

7.1.7. System Diagnostics

Here you can view the current temperature of internal drives, processor cores and system, along with information about backup battery status, temperature, voltage, and write cache provided by the hardware RAID, if one is installed.

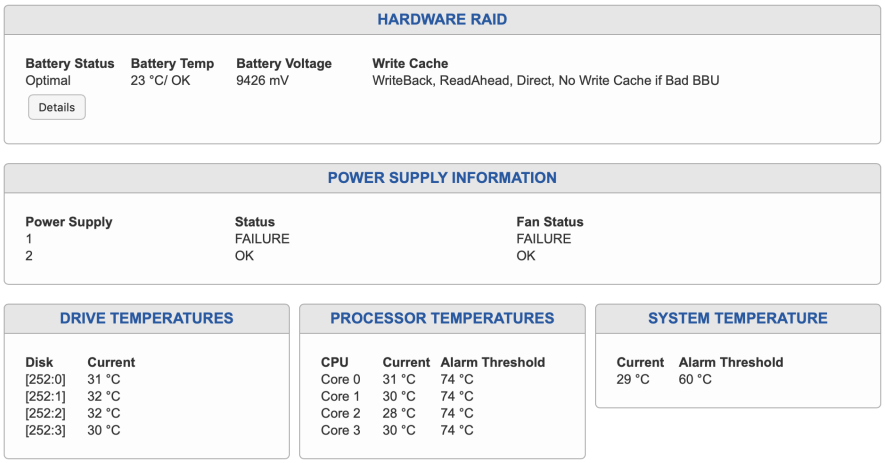


Fig. 7.18 System Diagnostics

In the example above, you can see that the Drive, Battery, Processor and System temperatures are all within specification, the Hardware RAID is fine, but the first Power Supply has failed.

7.1.8. Upgrade Recorder Software

Software Upgrades are made available for NexLog Express regularly. They include new features, system security updates, and refinements.

There are two kinds of Upgrades:

- Full Upgrade: This changes the version number of the software. A full upgrade will take you from 2020.1 to 2020.2, or 2020.X to 2021.1. This will include Debian security updates, new features and/or refinements recommended for all sites. Full Upgrades can only be applied if the recorder's Software Upgrade License expires after the date the Upgrade was released.
- Incremental Update: These are small incremental changes, often intended for a small number of specific sites in the interim between Full Upgrades. Applying an Incremental Update does not change the software version, but the Update will appear in the Upgrade History tab on the System Info page.

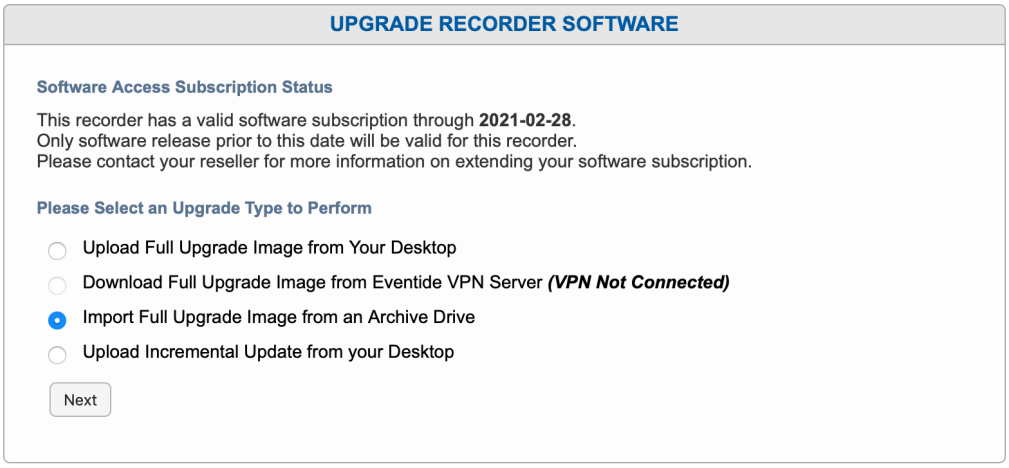


Fig. 7.19 Upgrade Recorder Software

Important

Before upgrading:

1. Archive all recordings!
2. Archive your recorder configuration!
3. Remove all archive media.

There are four options on this page:

- Download Full Upgrade Image from Eventide VPN Server: This will end with (VPN Not Connected) if VPN settings have not been configured and enabled.
- Import Full Upgrade Image from an Archive Drive: If you have a push upgrade zip image on archive media, you can insert it into the recorder and upgrade with this option.
- Upload Incremental Update from your Desktop: Use this to upload an incremental update provided by Eventide Service.

7.1.9. Power Off

This section allows a user to remotely power off or reboot a recorder. When rebooting a recorder, it's recommended that the recorder be physically available nearby in case any issues occur.

These actions are included in the audit history and choosing to reboot or shutdown the recorder will open a prompt to include a reason for the power off event.

7.2. Networking

This section of Configuration Manager is used for configuring the system network details, with the exception of Advanced Network Routes.

7.2.1. System Identification

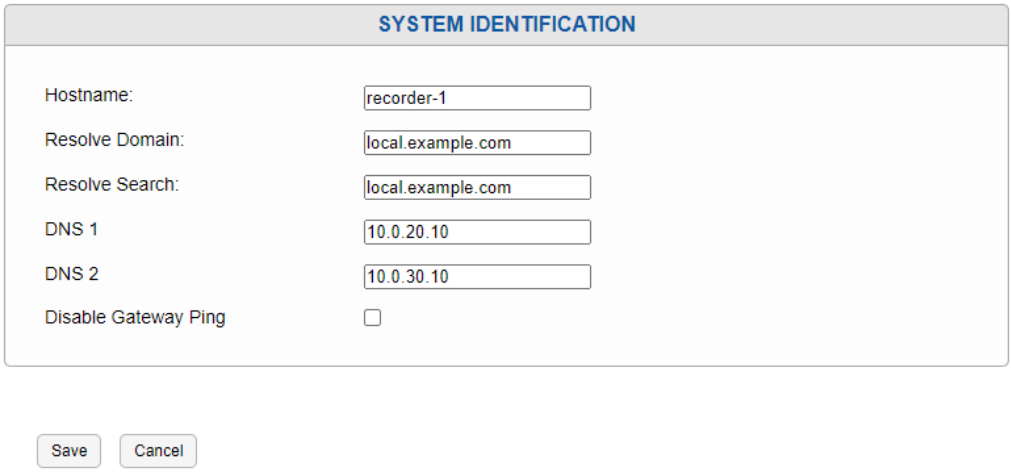


Fig. 7.20 System Identification

On this configuration page, information related to the identity of the recorder on the network can be modified or viewed. The network name of the recorder is configured using the hostname field. The hostname may require a naming scheme that is defined by your Network Administrator.

The domain name is configured under Resolve Domain, whereas Resolve Search is used to indicate what domain name should be searched in the event of machine name that is not provided with a complete fully qualified domain. For example, if the “Resolve Search” was set to “local.example.com” and you added an SMTP host (see Section 7.7.5 Email of “mail”, when the machine tries to resolve this name it will append “local.example.com” to “mail” making “mail.local.example.com” if it cannot initially find the machine under the simple name of “foo”. If you’re unsure, set “Resolve Search” to the same value in “Resolve Domain”.

This page also provides space to optionally configure to DNS (Domain Name Server) IP addresses, which the recorder will use to look up domain names. If no DNS Servers are configured then any external server configured for the recorder to access, such as an NTP Server or email server, must be provided as an IP Address and not a domain name.

7.2.2. Network Interfaces

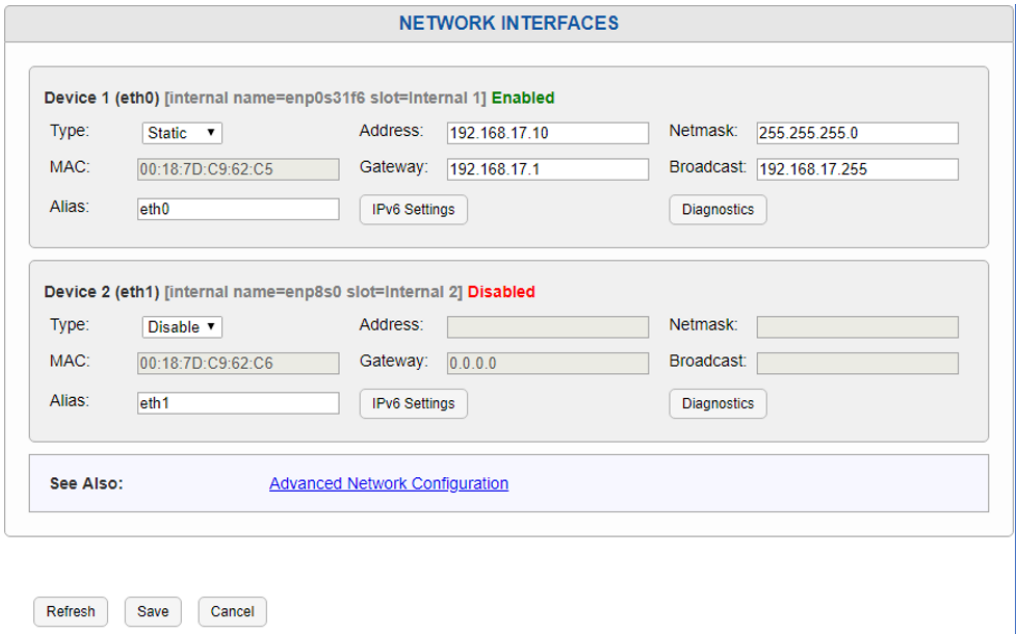


Fig. 7.21 Network Interfaces

This page allows for the configuration of each ethernet port or Network Interface Card (NIC) installed in the Recorder. You will see one entry on this page for each installed NIC. Depending on your NexLog Express Recorder and purchased options, you will have between two and ten NICs available for configuration. For each NIC, you have the following options to configure:

7.2.2.1. Type

Static, DHCP, SPAN, Bind, or Disable: This determines how the recorder will acquire its Network settings for the specified NIC such as IP address and Netmask.

- Static: If the type is set to Static, NexLog Express Configuration Manager will allow you to manually enter all the networking settings for this NIC. This information should be provided by your Network Administrator. The Address field is the IP Address being assigned to the recorder. Netmask, gateway, and broadcast should all be configured as well. The broadcast address is typically the last IP address available in the subnet.
- DHCP: If DHCP is selected, the data will be automatically received from a DHCP Server on the Network. If No valid DHCP server is configured on your network, this option will result in no IP address being assigned to the recorder and it will be inaccessible via the network. Note that since remote clients such as MediaWorks and MediaAgent, as well as Web Browsers need to know the IP address of the recorder in order to connect and interact with it, if DHCP is to be used, it is important to configure your DHCP server to be aware of the MAC Address of the recorder and to always assign the same known IP Address to that MAC. If DHCP causes a dynamic IP Address change, clients will no longer know what address to connect to in order to reach the recorder and other recorder functionality may not function as expected.
- SPAN: The third possible option is SPAN. A SPAN port is a port on a network switch or router that is “transmit only”. When a recorder’s NIC is connected to a SPAN port, it cannot send any traffic to that port, only receive any traffic that has been configured on the router to be forwarded to the SPAN port. SPAN ports are used for passive monitoring and recording of VoIP or RoIP traffic.
- Bind: If at least two NICs are present in your NexLog Express Recorder, you will also have a “BIND” option in Type. If BIND is selected on two Ethernet devices, they will be bound together into a single network link which is configured as a unit, rather than separately. This feature is sometimes known as “NIC Bonding” or “Link Aggregation” and is used to provide Network redundancy.
- Disable: Disables this NIC.

7.2.2.2. Alias

Alias is a field that maps a memorable name to the internal name of each NIC. It defaults to eth0, eth1… eth6 for each installed NIC. This is so you don’t have to remember the real internal name, like “enp7s0,” when configuring other parts of the Recorder, like RTP recording boards.

7.2.2.3. Gateway

It is recommended that gateway be set only on one NIC, and 0.0.0.0 entered in the rest. If you need a more complex configuration of gateway settings, use the Advanced Network Configuration option.

7.2.2.4. IPv6 Settings

NexLog Express can be connected to an IPv6 network for the purposes of using the recorder from IPv6 enabled clients. Administering the recorder through the configuration client and accessing recordings via MediaWorks EXP are supported over IPv4 and IPv6, however some functionality such as recording voip traffic and receiving IP Metadata feeds are currently only available via IPv4.

IPv4 uses 32-bit values made up of four 8-bit numbers, like 193.3.68.249; IPv6 uses 128-bit values made up of eight 16-bit numbers represented in hexidecimal, for example: 2001:0db8:85a3:0000:0000:8a2e:0370:7334

Note that IPv6 Netmask is just an integer (the number of bits in the netmask) as opposed to the IP-like format in IPv4. So the netmask in IPv4 will commonly be 255.255.255.254, in IPv6 this case would be 1.

Autoconfigure enables “IPv6 Stateless Autoconfiguration”. It is similar to DHCP in IPv4 in that the recorder will automatically get the IP, netmask, and gateway populated, but unlike DHCP, no DHCP server is required; IPv6 stack is capable of figuring out this information by looking at its network peers. DHCPv6 (DHCP for IPv6) is not supported by NexLog Express.

7.2.2.5. Diagnostics

This button opens a scrollable window showing the output of the command line tools *ifconfig*, *ethtool* and *lldp*. These are useful for troubleshooting network issues.

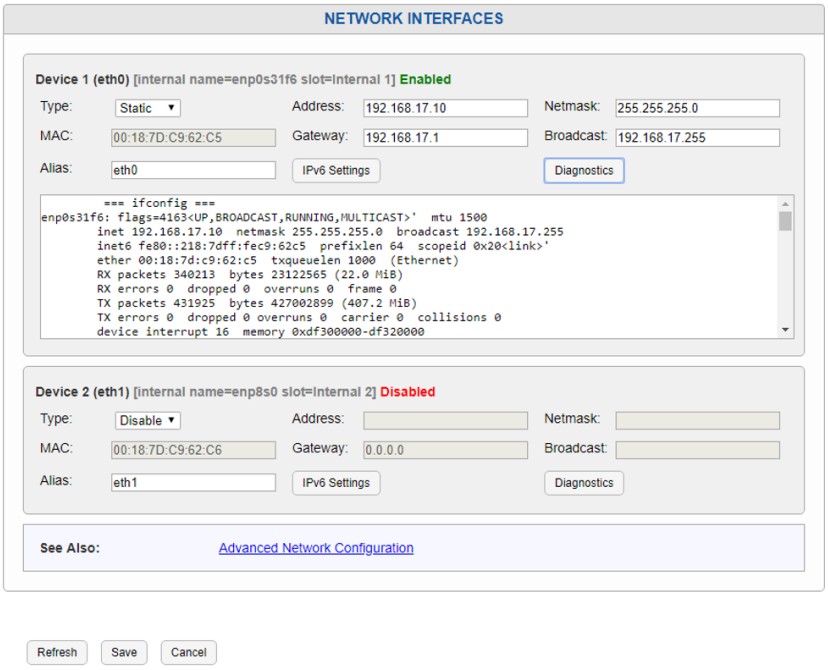


Fig. 7.22 Network Interface Expanded to show IPv6 Settings and Diagnostics

7.2.2.6. Advanced Networking Configuration

Standard network configuration such as default gateways can be configured on the Network Interfaces page. This file is for adding additional configuration not covered above. The format of the lines in this file is identical to Linux networking commands.

Note

The changes made to this file will not take effect until the next reboot.

Caution

Use caution when editing this file, as mistakes may make the recorder unreachable.

Valid commands are “route”, “ifconfig”, and “iptables”

Example:

```
route add -net 10.14.0.0 netmask 255.255.0.0 gw 10.14.47.254 eth1
```

7.2.2.7. Considerations When Using a Static IP Address

When using static IP addresses, the network parameters must be set manually from the front panel. There are some things you must consider when setting these parameters:

- The IP address must not be in use by another device. If it is, then the address may not be accepted, and even if it is accepted, operation will be unreliable.
- If you need the recorder to communicate with other devices on the network, such as an administration client, an NTP server, or the Internet, then the devices must either be on the same subnet, or on a different subnet that can be reached over a gateway. In the latter case, the address of the gateway must be added to the recorder.
- The subnet is determined by the Netmask setting. Your subnet is the result of an AND operation between the 4-octet net mask and the 4-octet IP address. See the Sample Net Mask and Subnet Settings table below for common examples of netmasks. Your facility's network administrator should be able to help you in assigning the proper IP address, netmask, broadcast address, and if necessary, gateway address for the recorder. If the recorder will be sending email, one or more DNS servers must be entered on the System Identification page.

Table: Sample Net Mask and Subnet Settings

Network/Subnet	IP Address	Netmask	Broadcast
192.168.0.0/16	192.168.1.3	255.255.0.0	192.168.255.255
192.168.1.0/24	192.168.1.1	255.255.255.0	192.168.1.255

7.2.3. VNC Settings

Virtual Network Computing (VNC) is a standard protocol widely used for

accessing PC Desktops remotely over the network. If enabled, you will be able

to connect to the recorder over VNC using any standard VNC Client such as RealVNC or TightVNC.

When you connect to the Recorder via VNC, you will be able to remotely view and interact with the Recorder's Front Panel. You will not be able to hear audio over this link as the VNC Protocol does not provide audio forwarding.

To use VNC, you must first enable the service by selecting the relevant check box on this page, and enter a password that VNC Clients will be expected to provide to gain access. The password must be entered twice to make sure it is entered correctly. Once enabled, NexLog Express VNC access is provided over port 5900.

7.2.4. VPN Settings

NexLog Express can join a Virtual Private Network (VPN) to make the recorder accessible to Eventide's Service technicians or certified dealers in the case assistance is required.

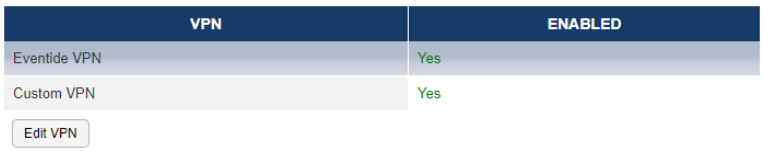


Fig. 7.23 VPN Connection List

Two VPN connections can be used simultaneously for instances where a certified Eventide dealer manages a secure remote management connection, as well a connection for Eventide's service technicians if the dealer must escalate a service ticket for Eventide's assistance.

Name: Name of the connection to easy identification

Host: Hostname and port of the VPN server

Example: `eventidedealer.com 1194` would connect to *eventidedealer.com* using port *1194*

Type: VPN server type. *OpenVPN* or *IPSec IKEv2*

7.2.4.1. Eventide VPN

This connection is configured when the NexLog Express system is manufactured. While it can be altered or overwritten, it is not recommended. Altering this connection would prevent Eventide's remote assistance if ever needed.

This connection should only be enabled if requested by an Eventide Service Technician, and it should be disabled when it is no longer needed.

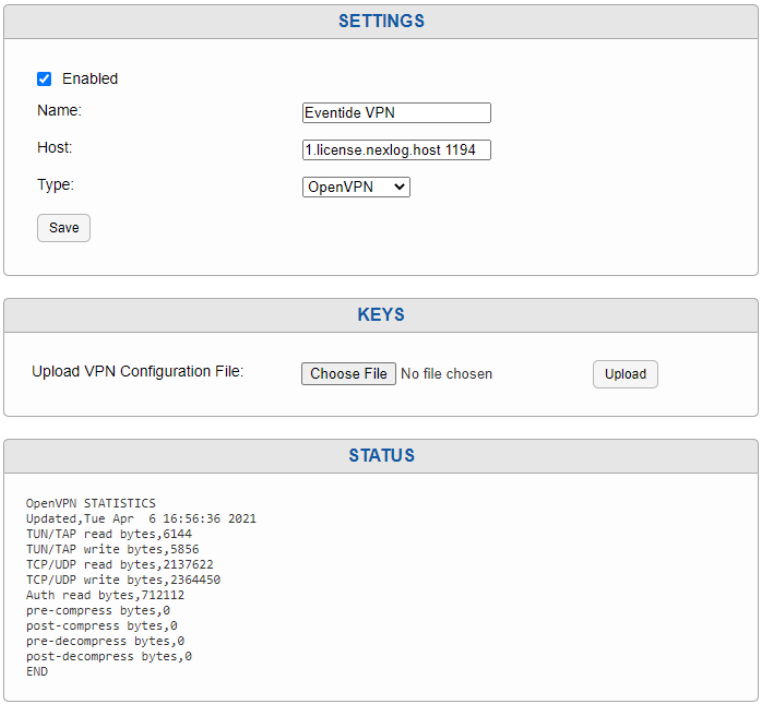


Fig. 7.24 Eventide VPN Connection

7.2.4.2. Custom VPN

This connection should be used by a certified Eventide dealer for connecting to their secured remote monitoring system.

7.2.5. SNMP Settings

“Simple Network Management Protocol”, or SNMP, provides a standard mechanism for System Administrators to manage devices over an IP Network. Many third party commercial and free utilities and consoles exist for monitoring systems using the SNMP Protocol. Eventide NexLog Express now supports SNMPv3 and provides a simple subset of SNMP Functionality (with Linux and SQL notifications) which can be configured here.

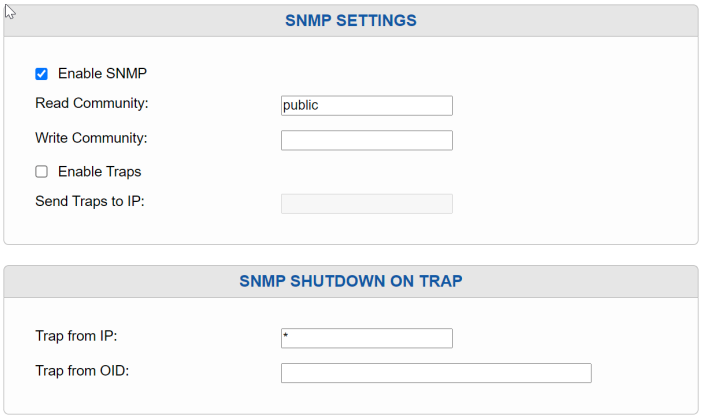


Fig. 7.25 SNMPv3 Setup

First, you must choose to enable SNMP on the recorder and provide a community to join. An SNMP community is similar to a Workgroup. Only SNMP Clients in the same community will be permitted to query the recorder via SNMP to retrieve information.

In addition to allowing third party utilities to monitor basic recorder status, you can configure an SNMP Trap, upon receiving which, the recorder will shut down. This can be used with a UPS which can be configured to generate a trap upon power failure (Though Eventide recommends using one of the UPS’s listed earlier in this manual which provides a USB connection to the recorder, since more information is available to the recorder in that case).

If this feature is used, the system generating the trap must be a member of the same community as the recorder. In addition, you can limit what IP address the recorder will allow the trap to be sent from by replacing the ‘*’ (meaning any) with the IP address in the “Trap from IP” field. Finally, you must provide the OID (Object Identifier) of the trap upon which you wish the recorder to shut down upon receiving, in the “Trap from OID” box.

Additional SNMP Configuration

To further edit SNMPv3 settings, refer to System

Configuration Files, and select SNMP Configuration (snmpd.conf)

Fig. 7.26 SNMP Configure View/Edit File

Here you'll find instructions and examples on how to edit, or upload pre-existing SNMP details for your system.

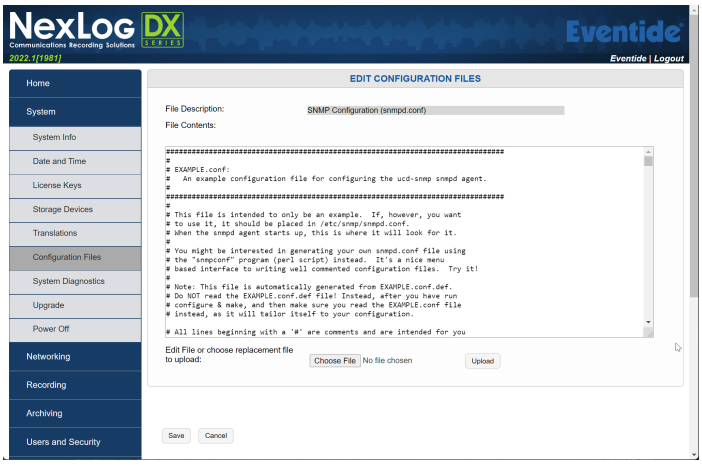


Fig. 7.27 SNMP Configure

7.3. Recording

7.3.1. Recording Interfaces

The Recording Interfaces page is where you configure the logger's primary recording functionality. Because of the real-time nature of recording, and the large number of editable parameters, special care has been taken to streamline the workflow of editing boards and channel configuration. Hence, this page does not follow the same convention that most of the other pages follow. The primary difference is that instead of editing settings and then having to click a 'Save' button to take effect, when you are on the main Recording Interfaces page, changes take effect immediately. Trying to adjust gain one decibel at a time while viewing the results on a level meter, for example, would not be possible without a live environment as it would take countless tweak, submit, check cycles. Note that even if your Web browser does not support the dynamic nature of editing directly on the live page, you will still be able to edit channels using the 'Edit Channel' page for making changes.

A board on a NexLog Express recorder is another name for "Recording Interface". The term comes because most recording interfaces are exactly that, PCIe Boards installed in the recorder, but there are also Virtual Boards, such as VoIP Boards, which are not physical boards in the system. Each board has its own configuration settings, and one or more channels that exist on that board.

For example, an Analog board with connections for 8 analog channels (2 wires per channel) would be considered an "8 Channel Analog Board".

Physical boards are constrained to a certain channel capacity via hardware. To change an 8 channel digital board to a 16 channel digital board requires physically removing the board then purchasing and installing a new one. Virtual Boards can often have their channel capacity expanded simply by purchasing a license and reconfiguring them, provided the recorder has enough capacity to handle the additional channel load.

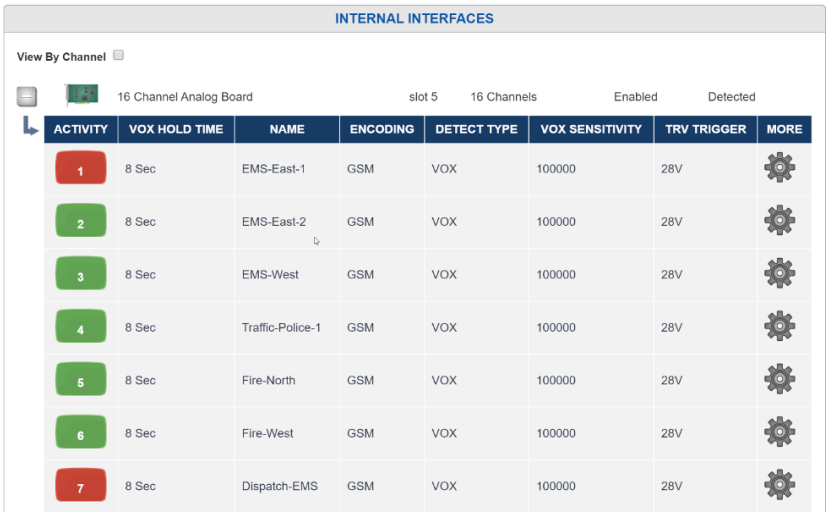


Fig. 7.28 Recording Interfaces

7.3.1.1. Navigation

With `View By Channel` disabled, the Recording Interfaces page will show one installed board per row. The left most icon `plus (+)` icon will expand the board so that all of its channels can be viewed below it. Upon expansion, the plus icon will turn to a `minus (-)` icon. Clicking that minus icon will "roll up" the channels into the board.

Clicking on the board's row will bring you to the Board Configuration "Edit Board" page where board settings can be modified. The next two columns display the board type (e.g., Analog, or Voice over IP), and the number of channels on the board. There will also be a column indicating if the board is enabled or disabled.

Boards that are disabled are not currently recording. For physical boards there is an additional field that tells if a board is "Missing" or "Present". A Missing board is one that was previously in the system, but has been removed. The board configuration and all configuration settings for it remain in the database. To remove the configuration settings and board entry for the missing board, you can delete the board from the 'Edit Board' page.

Expanding the board entry to display channels, or using the `View by Channel` option will display one row for each channel. Each channel row shows seven configuration settings for the channel along with a `More` button for displaying all options for the selected channel on one page.

To see and edit all settings in a non-live environment for a single channel, you can use the “more” button. It is often more convenient to modify channels settings directly on this page where they take effect immediately and you can see the values for multiple settings and channels at once. However, there is only space to display seven options on this page and there are many more than seven available options per channel. The seven fields default to the most commonly configured options, but you can click on the header above the table showing the channels to modify what field shows in that column to display a dropdown list of available column types to choose from.

7.3.1.2. Editing Values Inline

To edit a value, simply click the cell you want to edit, for example, Channel 4’s channel name. The cell will change to an edit control and when you click out of the cell or press `enter`, the value you changed will take effect immediately. Most options are either edit boxes where you can type your value, such as a channel name, or a dropdown list where you select an available value from the list, for example Detect Type. A few options are represented as checkboxes or sliders where appropriate.

The down arrow key will submit the changes for the current cell being edited and select the cell below for edit.

The `esc` key will cancel an edit and set the cell back to the original value

If you want to change a channel value for all channels in a board at once, a shortcut is provided. Click on the header of the column you wish to change, and scroll up to and select ‘Set All’. The column header itself will change to an edit control and changes made there will take effect for all channels in the board, for example to change the VOX Threshold of all channels on an analog board to the same value at once. In addition, you can select “Insert Column” to insert an additional column into the table.

Doing a “set all” on certain fields trigger special actions other than setting all of the channels to the value specified.

Name: Appends the channel ID relative to the board to the end of the specified name

RTP IP: increments the last Octet of the address unless the value is “127.0.0.1 or “dynamic”

RTP PORT: increments the port number starting at the specified port. In addition, two ports can be specified to be mixed together delimited by a “,”.

In addition to all the editable parameters for channels, there are a few special “read only” informational fields that are available for display including the Channel’s ID, Board, and BoardID, as well as an activity indicator. The activity indicator is a real time indicator of the channels status. Grey means disabled, Green is idle, Red is recording, Yellow means user disabled.

The meaning of the editable fields will be discussed in the “Edit Channel” page discussion below as the parameters there are the same.

Use the search bar to look up specific configurations to add to the column header. Start typing the name of a configuration option in the textbox to narrow down the list to ones that match the text entered.

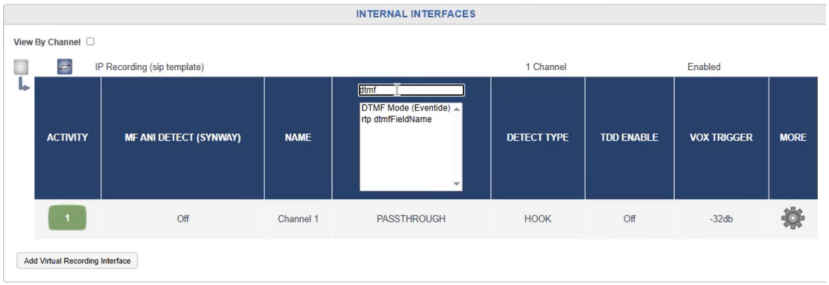


Fig. 7.29 Recording Interfaces Search Feature

7.3.1.3. Detail Level Graph

Clicking on channels “Input Level” parameter will expose a panel called the “Detail Level Graph”. The Detail Level Graph will give a histogram of channel levels. Note that this is only useful on certain recording interfaces.

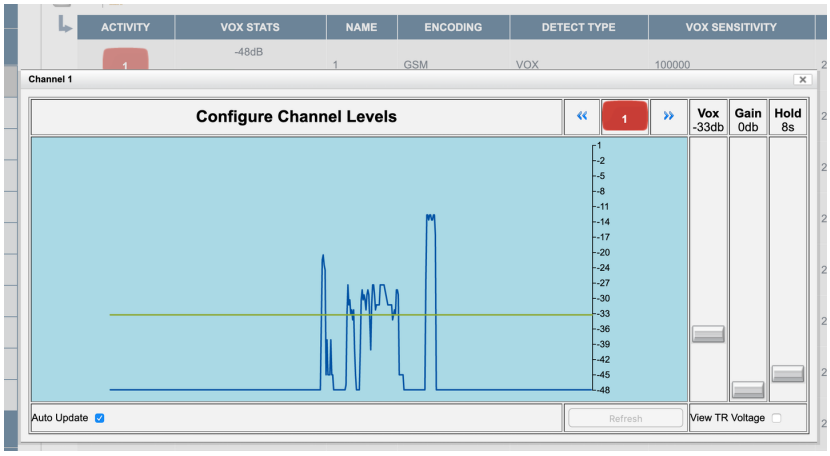


Fig. 7.30 Recording Interfaces Detail Level Graph

The Channel Level Details view provides a precise way to configure recording parameters. The yellow line indicates the current recording trigger point. The current channel being viewed can be seen in the channel status indicator. Note that changes to recording parameters take effect in real time, but do not effect historical information.

7.3.1.4. Edit Board

This Configuration Manager allows all of the settings and information about an individual board to be displayed and modified. To edit a board, click on the row describing the board from the main Recording Interfaces page.

No changes made to settings on the ‘Edit Board’ page will take effect until the ‘Save’ button is clicked.

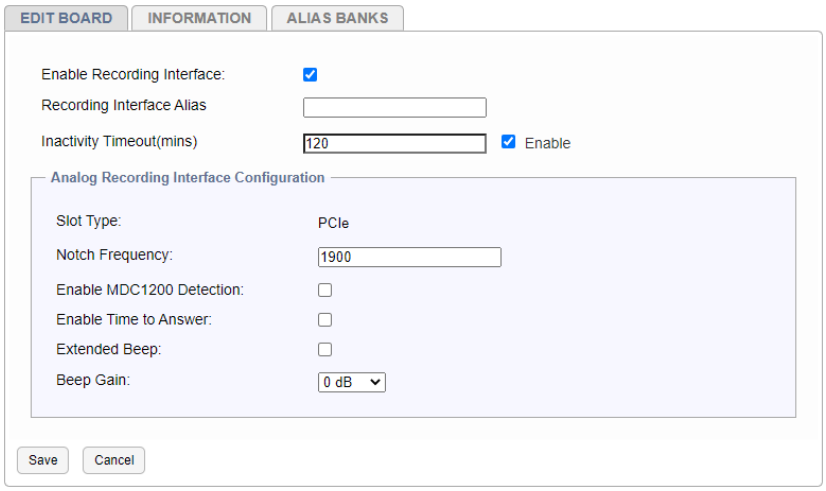


Fig. 7.31 Edit Analog Board

The first tab, “Edit Board”, contains the options available to be configured for this kind of board.

The “Information” tab contains information and status about the board.

The Board Name: e.g. “8 Channel Analog Board”

Serial: The board’s serial number. For a physical board the serial number is actually burnt into the boards ROM. For a virtual board, this is a GUID (Unique ID) created when the board was added to the system

Channels: The number of channels the board contains

Position: Boards added to the system are numbered starting at zero. This is the number of the board. This is not the physical position of the board

Address: The physical location of the board. For a physical board it’s the PCI Bus and Slot number, for a Virtual board it’s the IP address of the board resource

Detected: For a Physical board, zero if the board is missing, 1 if it’s detected. Undefined for a virtual board

Code: This is a status code for the board. The normal state should be “RI-FAIL-NONE”.

The “Alias Banks” tab shows a list of any Alias Banks configured for the channels of this board. You can jump directly to any Alias Bank by clicking the name of the Bank in this list. See Section 7.3.7 Alias Banks.

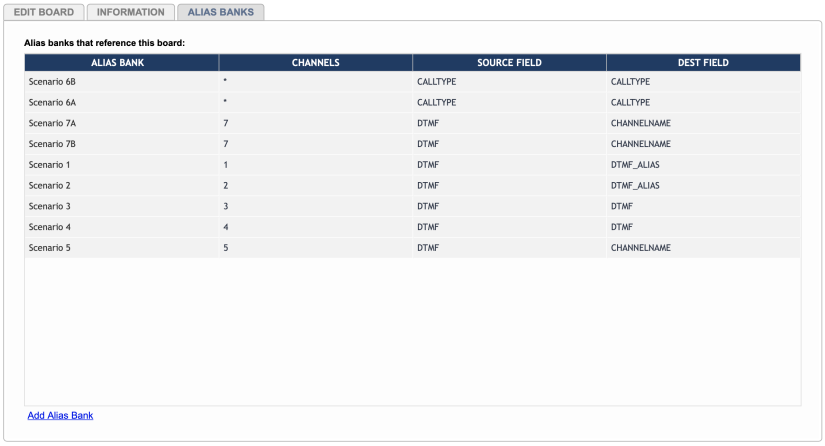


Fig. 7.32 Alias Banks tab of Board Edit

All boards also have an “Enable” checkbox to enable or disable a board. By default, when boards are added to the system they are enabled. Note that if you disable a board it will not record. It may be necessary to disable a board if you’re upgrading to a board with a higher channel capacity or if the board is malfunctioning and needs to be replaced. In some installations it’s a good idea to disable a board before making settings as to not make recordings before, for example, naming your channels.

The remainder of the informational and editable fields on the ‘Edit Boards” page are dependent on the board type:

7.3.1.5. Digital PBX Tapping Board

Synway PBX 8-channel, 16-channel, and 24 channel versions

Firmware Version: The version of the firmware loaded onto the PBX card, for diagnostic purposes only.

PBX Type: For a PBX Board to be able to record from a PBX, the PBX Type configured must be set to the model of the connected PBX. For PBX Model, version, and phone set compatibility, please contact Eventide.

Telco Encoding: This is the companding used on the digital voice sent between the PBX and the Phone. This is the format of the voice actually sent across the wire and is unrelated to any companding or compression codecs used to store the data on the recorder itself. If this is set incorrectly for your PBX, the recorded audio will sound scratchy and overdriven. MULAW is generally much more common than ALAW.

7.3.1.6. Analog Boards

8-channel, 16-channel, and 24 channel versions

Slot Type: This board is either PCI or PCIe

Notch Frequency: The Analog Board provides a Notch Filter to Notch out tones in the input signal. The frequency to notch must be configured on a board-wide basis. In addition, the Notch Filter needs to be enabled for each channel on the board, so you configure the frequency here, and then which channels on the board it should be applied to.

Enable MDC1200: If enabled, this board will process MDC1200 Radio tones which provide RadioID information (who is talking) on some Analog Radio systems. In addition, an add-on license key must be installed to allow the feature to be utilized and a User Defined Field (Recording: User Fields) must be added to the database to hold the RadioID. The field should be called `RADIO_ID`

Enable Time to Answer: When enabled, this will provide time in milliseconds between first ring and when the receiver goes off-hook. This only works with channels set to HOOK Detect type.

Extended Beep: If enabled, the beep for this board will be 1400 Hz and 424 ms, which is within the 1400 Hz ± 1.5% and 400ms ± 75ms specification for Australian requirements for beep on line recordings. (Beep is only available on PCIe analog boards)

Beep Gain: Allows you to adjust the volume of the beep from -21db to +18db, in 3db increments, relative to the default level.

7.3.1.7. Virtual Recording Interfaces

RTP and VoIP Virtual Boards can be added and configured using templates listed in the Appendix section. (See Section F RTP VOIP Templates)

IPv6 Support

IPv6 Recording is now available on the following VoIP templates:

- Generic Unicast UDP (Non-SPAN)
- All Non-SPAN SIP Trunk based integrations that use Eventide SIP Stack
- All SipRec based integrations (Including Cisco SBC/Cube)
- Cisco BIB

- ED137B
- ED137C
- Tait DMR

In order to use IPv6 with one of the above templates, select the IPv4 and/or IPv6 option that coincides with your template preferences.

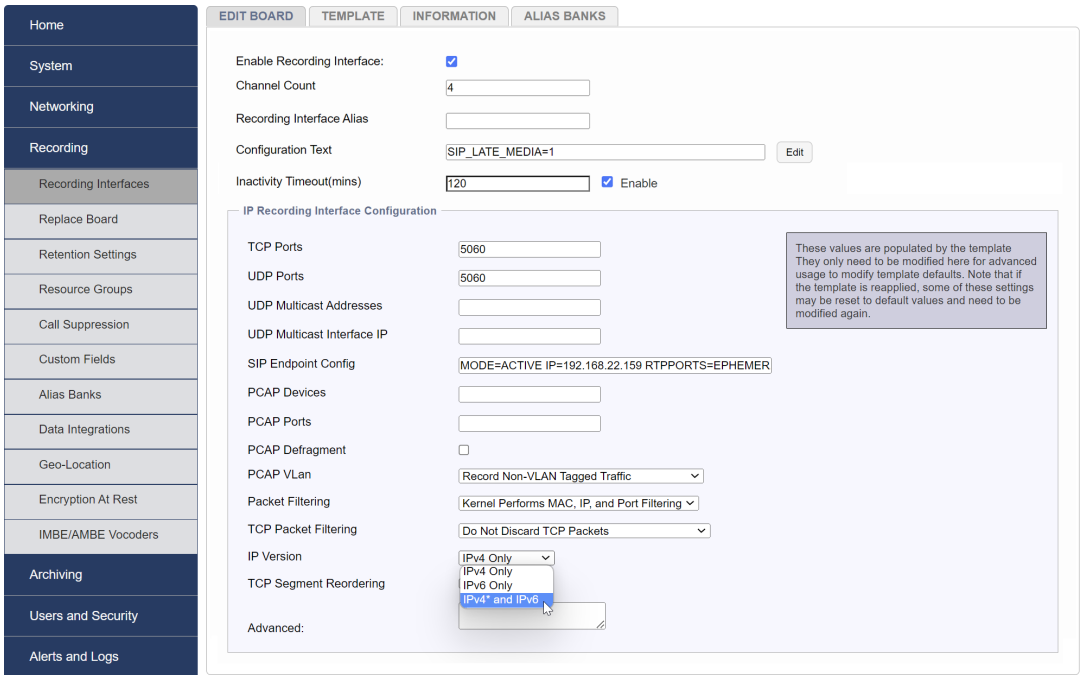


Fig. 7.33 Configuring Virtual Boards

> **Note**
>
> For more information on IPv6 Network setup, see Section 7.2.2.4 IPv6 Settings

7.3.1.8. VoIP template SRTP TLS Support and Configuration

Voice over IP (VoIP) traffic is increasingly encrypted to ensure secure communications. The NexLog Express system accommodates this need by supporting the Secure Real-Time Transport Protocol (SRTP) in conjunction with Transport Layer Security (TLS).

SRTP encrypts the actual media (audio and video) paths in a VoIP conversation, while TLS is used to encrypt the signaling traffic, including the negotiation of SRTP keys.

TLS Configuration

TLS is recommended for secure communication and is used alongside SRTP. However, it's important to note that TLS traffic cannot be recorded via SPAN (Switched Port Analyzer) as the recorder, in this scenario, cannot access the encryption keys negotiated between the two endpoints.

NexLog Express circumvents this limitation by functioning as an active participant in the TLS tunnel, thereby enabling the recording of TLS-encrypted traffic.

Supported Configurations: - NexLog Express supports TLS encryption on ED137 templates and various SIP-based templates where the recorder is not SPAN recording but configured as an endpoint.

Examples included but limited to:

- SIP Trunk
- SipRec Trunk
- Cisco Built-in-Bridge (BIB)
- Tait DMR

In addition to TLS-based encryption, NexLog Express supports non-TLS encryption methods used by various radio systems like EFJohnson, Motorola MotoTrbo, etc.

> **Note**
>
> To configure TLS for a template, the SSL/TLS License Addon Key is required.

By default, NexLog Express generates a self-signed certificate at installation for TLS connections. However, user-uploaded certificates (uploaded through standard procedures) are also supported and utilized for templates configured for TLS. See the Manage Certificates section for more details

- Current TLS versions supported are TLS 1.2 and 1.3, in line with the deprecation of older versions due to security concerns.

SRTP Configuration

SRTP enhances VoIP security by encrypting the media streams. NexLog Express supports a range of ciphers for SRTP, catering to diverse security requirements:

Supported SRTP Ciphers:

1. AES_256_CM_HMAC_SHA1_80
2. AES_256_CM_HMAC_SHA1_32
3. AES_CM_128_HMAC_SHA1_80
4. AES_CM_128_HMAC_SHA1_32
5. AEAD_AES_256_GCM
6. AEAD_AES_128_GCM

For detailed configuration instructions, refer to the RTP VOIP Templates section in the Appendix.

7.3.1.9. Configuration Text Editor

New in version 2024.1.

When editing boards or select channels, Configuration Text can now be added by selecting the edit button:

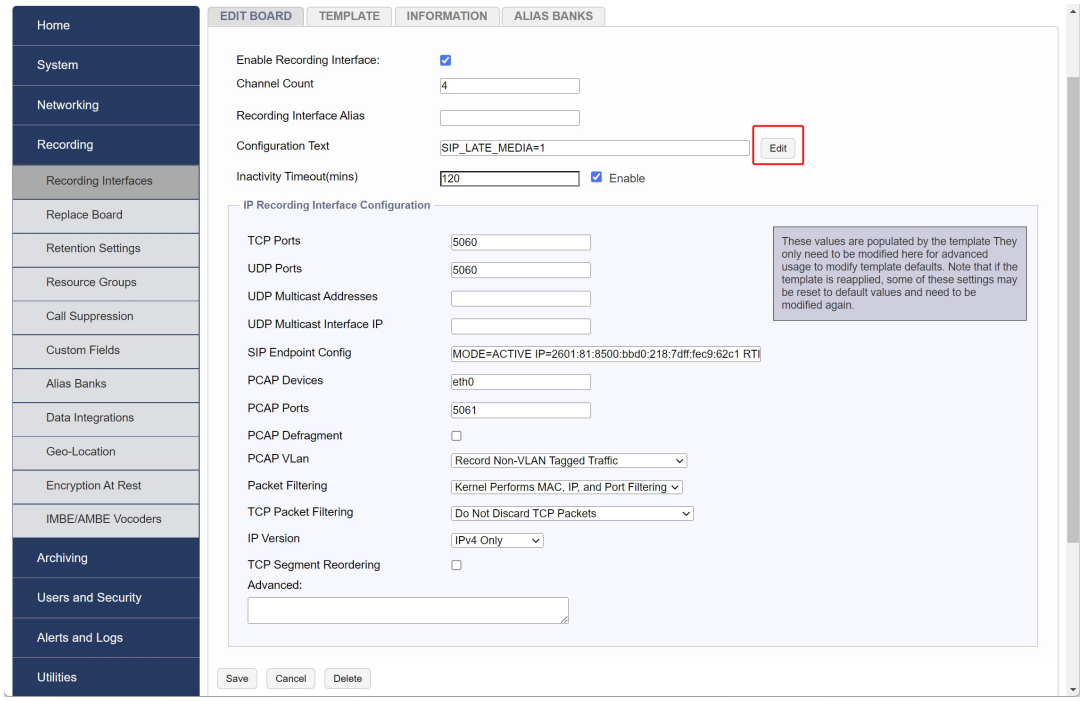


Fig. 7.34 Configuration Text

Here you'll be able to enter and add multiple Keys and Values using the Configuration Text Editor:

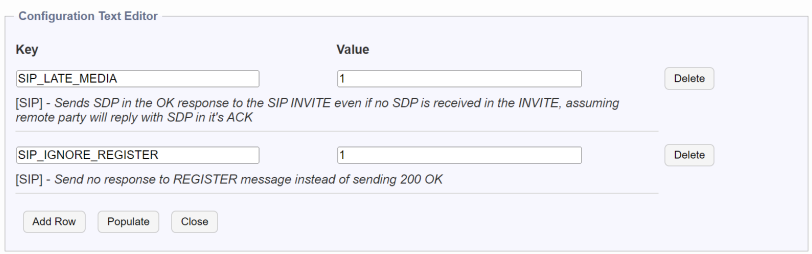


Fig. 7.35 Configuration Text Editor

Once added, select “Populate” to include in the board settings.

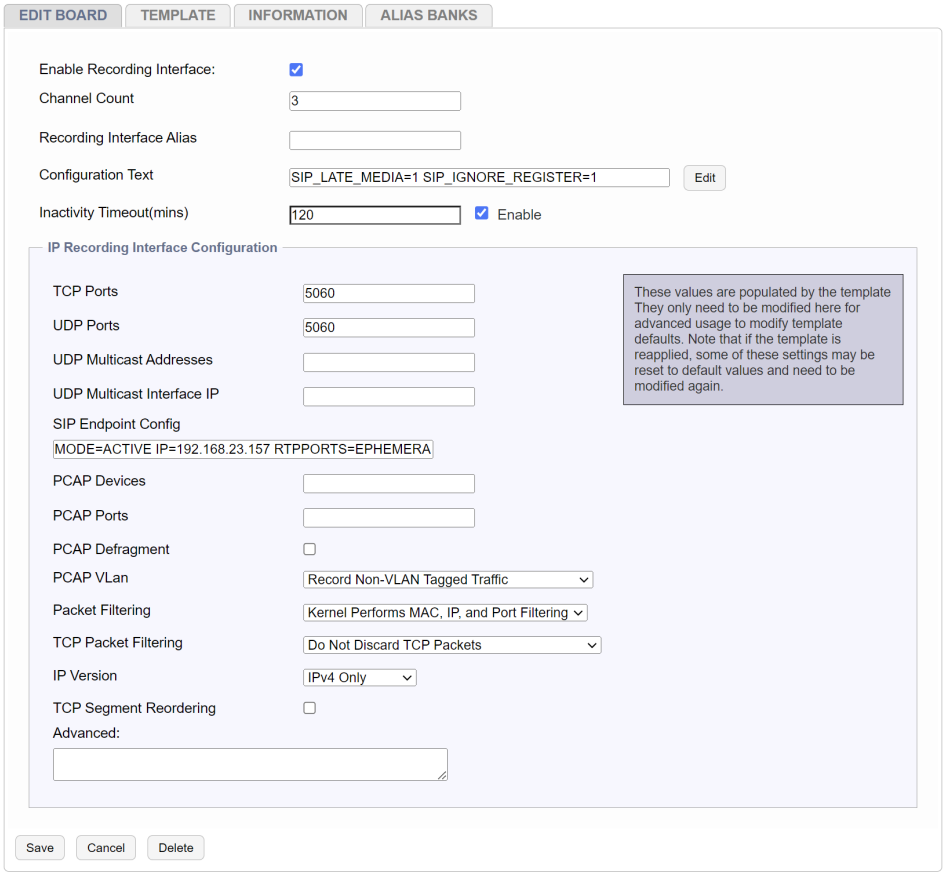


Fig. 7.36 Configuration Text Populated

> **Note**
>
> Channel Configuration Text can also be individually edited by navigating to the bottom of Edit Channel > Additional Settings.

7.3.1.10. Edit Channels

Clicking on the gear icon next to a channel allows you to set channel level parameters. Note that most of the common parameters for a channel can be configured in the main table channel table as well by clicking on a cell.

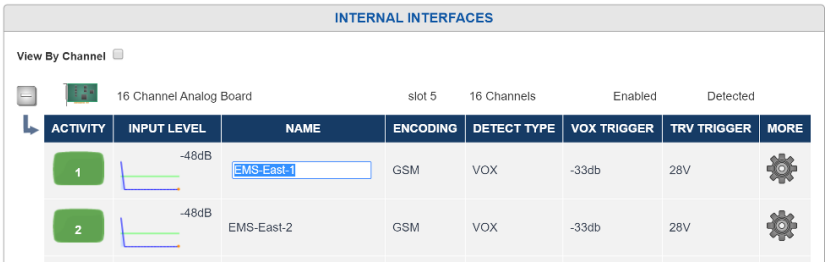


Fig. 7.37 Editing a Channel Name inline

In addition to editing channel information inline you can also edit it by clicking the gear icon.

> **Note**
>
> Some options described below are only available on some kinds of boards and not on others.

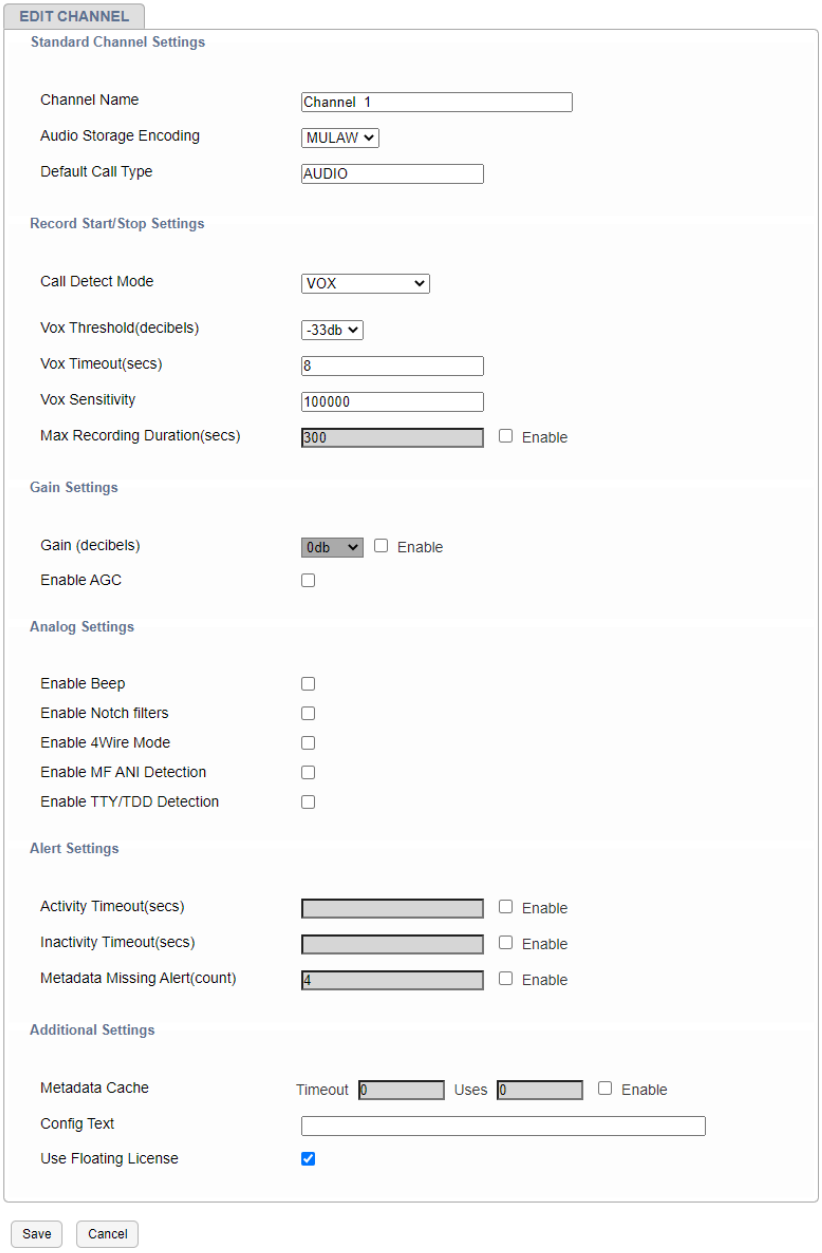


Fig. 7.38 Edit Analog Channel

7.3.1.10.1. Standard Channel Settings

Channel Name

Identifies the name of the specific recording resource signal.

The channel name can be up to 64 characters.Telephone number, radio station call letters, ATC frequency and function, or any other free-form data may be entered here. While up to 64 characters of data may be entered and saved, display constraints suggest that you choose the first few characters most carefully. There is no requirement to modify these identifiers. The factory default “Channel 01” … “Channel nn” may be serviceable.

Audio Storage Encoding

The field is editable and sets the encoding algorithm.

See Section 7.3.1.10.6.1 Choosing an Encoding Algorithm for more information.

Default Call Type

This is the value that will be entered into the `Calltype` field of all calls that come in on this channel, unless altered by a custom integration. See Section 7.3.6: Custom Fields

7.3.1.10.2. Record Start/Stop Settings

Call Detect Mode

This parameter determines when an input channel is active and should be recorded. It establishes the primary `recording control` for the channel.

- Analog Boards: Always, Disable, GPIO, Scheduled, Tip/Ring Voltage, Vox.
- Digital Boards: Script, Always, Disable, Vox. (Display-Only: Off Hook, Data Channel.)
- Local VoIP: Varies by RTP/VoIP template configured.
- Screen: Always, Script, Disable, Scheduled, User Activity.

The following are valid values for detect type:

VOX

(default) Starts recording if the voice (vox) or audio input signal is above the configured Vox threshold setting, and stops recording if the signal drops below that setting for the configured hold time.

TRUEVOX

[RTP only.] In regular VOX mode for RTP channels, the presence of data on the line will trigger recording, but some environments will transmit large durations of data that is actually silence, so this mode will analyze the contents of the packets and evaluate recording based on the volume of the contained audio.

TRVOLT

Starts recording if the DC input voltage is *lower* than the configured TRV (Tip-Ring Voltage) threshold, indicating an off-hook condition, and stops if the voltage rises above the configured setting for a period equal to or greater than the configured TRV Hold time. Note that TRV detect is only available for Analog boards and is only useful for audio sources that provide this DC voltage in addition to the analog signal (such as standard analog phone lines)

On

Records the channel continuously. For voice, audio, or call recording, it records regardless of input signal or voltage conditions. (This is useful if there are periods of silence that need to be recorded, such as dead air on a broadcast station or long periods of dead silence in a courtroom.) For screen recordings, the recording includes when the screen saver is on. This setting is not affected by the Activity Timeout or Inactivity Timeout parameters.

> **Note**
>
> If recording in `On` mode, it can be helpful to break the recording into smaller segments (such as 1-hour segments).

On Voxbreak

This is a detect type that is available specifically for Analog boards. It is a combination of On and Vox modes. Like 'On' mode above, it provides continuous channel recording, and like Vox mode it breaks calls into segments based on the VOX threshold. When the level of the audio input being provided is above the channel's configured VOX threshold, the recordings will be tagged with calltype Audio. Once the VOX Hold Time setting on the channel has elapsed, the channel will break the call and continue to record, tagging this new recording with calltype Inactivity until the VOX threshold is met again. This detect type is useful for sites that want to have 24/7 coverage while still being able to quickly find periods of activity or inactivity on the channel in MediaWorks EXP.

GPIO

Uses an input signal from an optional General Purpose Input/Output (GPIO) board to trigger recording start and stop. The pin pair that carries the input signal is specified in GPIO Pin column. Recording starts on a high signal and stops on a low signal. This allows a variety of external devices to trigger recording.

Scheduled

Uses Scheduled Recording to start and stop recording.

Script

Records based on start/stop requests from the NexLog Express Recorder itself. This is used in conjunction with custom scripts or other specialized programming created by Eventide Customer Engineering as a contracted professional service. This setting is not affected by the Activity Timeout or Inactivity Timeout parameters.

Disable

Disables recording for the channel.

Hook / Audio

These options are used for VoIP and Digital lines. They make start / stop decisions based on the available signaling from the data source connected to the channel. The exact behavior is dependent on the source. For example on an ISDN PRI Channel, this causes the recorder to take cue based on the ISDN Call Connection messages on the line. On Some PBXs this will use the actual hook state of the phone, while others (which do not provide accurate hook state), the recorder will use combinations of lights, button presses, etc.

VOX Threshold

This sets the trigger level for recording when Record Enable Mode is VOX. A value between -48dB and 0dB is typical. The factory default is -32dB. This setting is only used for Digital and Analog boards. For VoIP, VOX detect mode triggers off the presence or absence of RTP traffic, not the actual levels.

VOX Timeout

If Detect is set to VOX, this sets the number of seconds the channel will continue recording after the signal drops and remains below the threshold. The factory default is 8 seconds.

Setting this for too long a value will record long periods of silence at the end of transmissions or join two calls together; too short a value may break a single call into apparent multiple call records at pauses in the conversation.

TRV Threshold

This sets the DC voltage at which a phone line is assumed to be in the off-hook state and eligible for recording. On a normal, clean telephone line, this does not have to be set too finely. On-hook voltages are typically 40-55 volts, off-hook under 10 volts. The factory default of 28 volts will probably be suitable. Noisy telephone lines, lines at a great distance from the central office, and lines that are recorded at one location but answered at another can have unusual voltage profiles and may require adjustment. This setting is only available on Analog boards.

TRV Timeout

If Detect is set to TRV, this sets the number of seconds the call will continue to be recorded after the telephone goes on-hook. The factory default is 5 seconds. The on-hook state is then considered to define the end of the conversation.

With a line that has normal ringing voltage on it (+/-105V at 20-30 Hz), TRV will also respond to the ringing voltage. This means that, with a default of less than four seconds, each ring will appear to be a separate call. By setting TRV hold to five seconds or more, with a normal ringing cadence only one call will be logged from the beginning of the ring to completion of the conversation.

If you have set a channel to TRV, a special (non-programmable) feature will detect and flag a disconnected line if the tip/ring voltage stays below 3 volts for 1 minute. If this happens, it generates a severity 2 (warning) alert indicating `signal loss` (Alert #9016). When the voltage equals or exceeds 3 volts, it generates the corresponding "Resolved" alert for Alert #9016 to indicate the signal is restored. TRV Hold setting is only available on Analog boards.

Max Recording Duration

The maximum length of a recording in seconds. Recordings will be split into segments no larger than the specified size.

7.3.1.10.3. Gain Settings

Gain

Gain (or attenuation) in dB of the input channel - used to set recording level on analog boards. Valid settings are -18db, -12db, -9db, -6db, -4db, -2db, 0db, +3db, +6db, +9db, +12db, +15db, +18db.

Enable AGC

Activates or deactivates Automatic Gain Control for Analog channels. Automatic Gain Control assures that recordings take advantage of the full dynamic range of the recording process. If you record at too high a level, the signal will "clip" and sound very distorted. If you record at too low a level, the signal will sound very soft and have a poor signal-to-noise ratio. Enabling AGC gives extra margin when recording telephone calls where the local party may be much louder than the distant one-it will boost the gain by up to 24dB when the distant party is speaking. AGC should be enabled

in most cases. It can be disabled in installations where audio levels are well-controlled (e.g., broadcast radio stations).

7.3.1.10.4. Analog Settings

Enable Beep

Enables a “Beep tone” to signify to callers that the call is being recorded. Activating the beep places a short, distinctive tone on the respective channel of the input connector. This tone is approximately 65 milliseconds in duration at a frequency of 1455 Hz. It serves to indicate that the call is being recorded, and is required by some state laws. Of course, the beep will only be audible to the callers if the recorder is connected directly to the telephone line in question; if an amplifier or other device is interposed it will serve no purpose. Beep tones are only generated on analog input boards.

If extended beep is enabled (at the Board Edit page), the beep will be 1403.508772 Hz and 387.5 ms, which is within the 1400 Hz ± 1.5% and 400ms ± 75ms specification for Australian requirements for beep on line recordings.

Enable Notch Filters

Enables the Notch filter for this channel. The frequency for the notch is set at the board level.

Enable 4Wire Mode

Pairs this channel with one adjacent such that the audio received on this channel and its pair are mixed into a single call record. If enabled on an odd channel, it will pair with the next channel: Channel 1 will pair with Channel 2. If enabled on an even channel, it will pair with the previous channel: Channel 6 will pair with Channel 5.

The settings for each channel are independent so that you can configure them as needed, but you can live monitor and playback calls as one channel. Audio and metadata from both channels are recorded if the conditions to record are met on either channel.

Enable MF ANI Detection

Enables the channel to capture and decode MF ANI data transmitted on some analog CAMA trunks.

Enable TTY/TDD Detection

Calls coming in on this channel with TDD (Telecommunications Device for the Deaf) text data will be decoded and the TDD text stored in the RTTsummary custom field. The text feed can then be viewed in MediaWorks EXP when playing back the call. NexLog Express supports decoding of TDD data encoded using Baudot codes at 45.5 baud utilizing 1 start bit, 5 data bits, and 1.5 stop bits. This feature requires the TDD Add-on License and an `RTTsummary` custom field. Without this feature enabled and licensed, the audio feed of the TDD will be recorded, but the recorder will not decode the text for display and search purposes.

7.3.1.10.5. Alert Settings

Activity Timeout

Timeout value in seconds. When set, alert #3001 (“Channel was active for more than X seconds”) is issued if a channel is continuously active for longer than the timeout value. The factory default is to disable this function. This setting does not affect the actual recording of the call. It simply issues an alert.

Activity Timeout is useful for calling attention to open or defective telephone circuits. When a channel is set for TRV detection, a LOW voltage activates it. If the circuit is open due to a broken wire, the voltage will always be LOW, and the recorder will issue an alert if this condition persists. If you are going to use this feature, then you should set this value to one that is longer than any reasonably expected call or message to avoid nuisance alerts.

Inactivity Timeout

Timeout value in seconds. When enabled, an alert is issued if there is no activity on the channel for longer than the timeout value. It will be regularly updated so that the user has more accurate information for the period of inactivity. The alert triggered is #3002 (“Channel ‘123’ was inactive for more than ‘X’ days ‘Y’ hours ‘Z’ minutes.”)

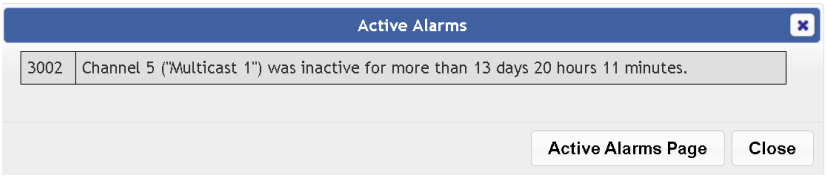


Fig. 7.39 Inactivity Timeout

This setting is disabled by default and does not affect the actual recording of the call. It simply issues an alert showing the amount of time the board was inactive after the Inactivity Timeout has been triggered.

Inactivity Timeout is useful for alerting you to circuits that should have signals but do not. If you are monitoring a radio channel and the radio is turned off, the inactivity timeout will eventually bring this to your attention. Likewise, an unused (but active and paid-for) telephone line can be identified with this feature. Of course, legitimate inactivity can span weekends and holiday periods. Setting periods too short can result in nuisance alerts.

Metadata Missing Alert

When metadata is being tagged to recordings, the system will raise an alert if the specified number of calls are recorded without additional metadata.

7.3.1.10.6. Additional Settings

Metadata Cache

When enabled, this option will reapply the received metadata to the number of recordings specified in the `Uses` field. The metadata can be held for the number of seconds specified in the `Timeout` field. The metadata will no longer be applied when the Uses or Timeout values are exceeded, whichever comes first.

Config Text

This is a special field that should only be used when asked to do so by an Eventide Service Agent.

Use Floating License

This option is only applicable when floating licenses are available on a system. Enabling this option will consume one of the available licenses. Disabling it will release the license. You can not consume more floating channels than are licensed.

These options are only visible when editing a channel inline:

Input Level

Real-time display of signal input level - useful for setting channel gain. This is not an editable item. This information is very useful for diagnosing recording problems, such as one call being broken up into multiple calls. Note that depending on the detect type this can either be TRVolt readings or VOX readings. Input level is available for Analog boards.

TRV Level

This non-editable item shows you the real-time minimum, maximum, and current value of the DC voltage at the channel input. The current value will indicate if the phone is on- or off-hook; the Min and Max will show the highest (on-hook) and lowest (off-hook) voltages seen by the channel input. If the current value fluctuates over a wide range when you are not using the telephone, it probably means that the line is very noisy. This information can help you set the TRV Thrsh value or diagnose problems such as spurious calls. This setting is only available for analog channels.

GPIO Pin

Specifies a value indicating the input pin on the GPIO board that is used for triggering recording to start or stop. The channel will record with the input pin is pulled high by connected to pin 49 and will stop recording with the pin is pulled low by connecting to ground with any even numbered pin. (This field is used with the detect GPIO setting.)

For the 24-channel GPIO board, values are as follows:

0: specifies pin 47 (PA0)	6: specifies pin 35 (PA6)
1: specifies pin 45 (PA1)	7: specifies pin 33 (PA7)

2: specifies pin 43 (PA2)	8: specifies pin 7 (PC4)
3: specifies pin 41 (PA3)	9: specifies pin 5 (PC5)
4: specifies pin 39 (PA4)	10: specifies pin 3 (PC6)
5: specifies pin 37 (PA5)	11: specifies pin 1 (PC7)

PBX Digital Sync Errors

This column is only important for Digital PBX tapping boards; it is used for installation and troubleshooting. The data will look like this: 1.1 / 0.66 [2,1,0]. The first two numbers are signal levels in volts. The first of the pair is the level of the signal coming from the PBX, and the second is the signal level coming from the phone set.

The three numbers inside the brackets are the total error counts for the channel since the last reconfiguration or restart:

- Sync errors are more general errors on the channel as a whole.
- PBX errors are errors in the signal from the PBX.
- Phone errors are in the signal from the phone.

These errors can signify problems and can affect recording: if the errors are increasing at a steady rate, it indicates that there is a problem with the telephone line connected to the recorder. However, if the error counts aren't all zero but do not increase, it might not be an indication of a serious issue: for example, someone may have unplugged and then plugged back in a phone.

Problems can be caused by:

- Line issues (bad taps, multiple taps, line lengths, tap lengths, marginal wiring between the phone and PBX).
- Unsupported phone set or line card.
- The wrong PBX is set in the board configuration.

7.3.1.10.6.1. Choosing an Encoding Algorithm

The following encoding algorithms are available:

- 13 kbit/s GSM (factory default)
- 16 kbit/s G726

- 32 kbit/s G726
- 64 kbit/s MuLaw

The data rate indicates the amount of storage used per second of recording. The default will give you the most channel-hours. Encoding algorithms always represent a compromise between storage space and perceived quality. All the algorithms listed are general-purpose, and are not restricted to voice. You might want to select either the 32 or 64 kbps algorithm if your recordings are going to be used by other decoding equipment, such as with fax recording. Fax in particular is very sensitive to the compromises made in reduced-bit-rate encoding. The human ear is much less so.

You can experiment with these algorithms to get the best balance between sound quality and storage space.

7.3.1.11. Steps for Setting Levels, Thresholds, and Hold Times

It is undesirable for single conversations to be broken up into multiple calls. There is a slight lag between each stop and start, so some of the conversation will be lost. Setting levels and thresholds properly will help you avoid this condition. This applies to channels set for VOX detect.

If you are seeing this condition, or if you simply want to check how well the default parameters match your facility, try this procedure:

- Disable AGC
- Set the Input Gain. It should be set with signals that best match what will be seen during normal operation. Watch the values and adjust the gain so that the current value ranges between -6dB and -1dB while a signal is present.
- Enable AGC (if desired). Not recommended for broadcast recording, recommended for communications or telephone channels.
- Using the Input level or the detail levels graph note the VOX Cur value with no signal present, but with the cabling still connected to account for line noise. Then note the VOX Cur value with the lowest-level input signal that you are likely to see during use.
- Set the VOX Threshold using the values from the previous step. The threshold should be higher than noise but lower than your lowest signal.

Another possible cause for conversations recorded on multiple separate calls is Hold time. This would apply to both VOX Detect and TRV Detect. Conversations with pauses longer than the Hold setting will generate a stop-recording signal. When the conversation resumes, a start-recording signal will create a second call. To determine if this is happening, listen to the last several seconds of a call. If you hear a pause in the conversation longer than the Hold time, followed by a second separate call of the same

conversation, then the length of the pause caused the stop-recording signal. If you wish, you can increase the Hold time. The downside is that longer periods of silence will be recorded at the end of EVERY call on that particular channel. For example, a 15-second Hold time on Channel 3 will cause a 15-second period of silence to be recorded on every call on Channel 3.

7.3.2. Replace Board

This section allows you to swap boards in your system for similar boards.

This is necessary in the unlikely event of hardware failure (due

to a power surge) or to expand channel count by replacing an 8 channel

analog board with a 24 channel board, for example.

When selecting the board to be replace it must be removed from the system.

The board that you are going to replace it with must be physically in the

system and disabled. Disable the board by going to the `Boards` setup page

and selecting the replacement boards configuration. When you have a possible

replacement candidate the Replace Board setup page will show a submit

button. If you do not a valid replacement configuration the button will

not be present and the text at the top of the page will explain why you

cannot do a replacement.

The act of replacing a board transfers all settings to the new board.

This includes channel ordering, channel names, and parameters specific

to the board type.

7.3.3. Retention Settings

Eventide NexLog Express Recorders store call data on their storage devices and provide a built in database for immediate retrieval and playback of recorded audio. Once the hard drives fill up with data, the oldest data will begin to be deleted from the system to make room for new data as new recordings are made. The Retention settings allow you to customize when this data is deleted.

Note: any Call Record which has been marked as “Protected” in the Front Panel or MediaWorks EXP will not be deleted to make room for new recordings regardless of retention settings. If both Limit retention time and Limit recording count fields are disabled, then call records will only be deleted if the hard drives are too full to store new recordings. Enabling and setting “Limit retention time (days)” will cause all call records older than the configured number of days to be deleted. For example, if set to 60 days, the recorder hard drives will contain a rolling history of the past 60 days of recordings, assuming adequate disk space to contain 60 days’ worth of calls.

In addition, Limit Recording Count allows a maximum number of Recordings to be specified. If this number is surpassed, the oldest recordings on the disk will be deleted to restore this constraint.

The Limit retention warning time (hours) setting will trigger an active alarm if the archive pointer for any archive drive is fewer than X hours ahead of the retention setting. For example:

On a system with 60 days of recordings, with the Warning Time set to 48 hours, and only uses a NAS to archive, and that archive is usually up-to-date, if someone stops the archive to browse and then forgets to start archiving again later, an alert will trigger in 58 days warning that the recordings are in danger of being deleted before they are archived. If someone starts the archive again at this point, the alarm will resolve after the archive pointer gets ahead of that 2 day window. If instead, no one reacts, recordings will start to be deleted before they have been archived and a second alarm will happen saying that the archive pointer is now behind the retention time.

We recommend setting the Warning Time to something high enough that your organization can respond to an issue that has arisen, such as 168 hours, which is one week.

Note that these settings have no effect on Archives. Eventide recommends Archive settings be properly configured and archive media to be properly maintained to put in effect a policy of making sure all recordings are archived to one or more archive media before being deleted due to retention policy.

By default, the option Delete record history with media is enabled. This option deletes the call record and associated metadata from the recorder database when deleting the record media (audio or screen.) For most users, this is the correct choice, but if you want to retain all information about call records that have come into your recorder even if they can no longer be played or exported, disable this option.

7.3.3.1. Reserves

Changed in version 2021.1: Reserve for attachments now includes User Content Uploads

There are three more fields to configure: Reserve for Attachments, Reserve for Reports, and Reserve for Cache, all in megabytes. These fields allow you to set a limit on disk space consumed by attachments (including User Content Uploads), reports and cache. The defaults are fine for most users. Unlike the limit fields, these fields do not cause deletion when exceeded; instead, no more attachments can be added to incidents, nor can more reports be generated. The recorder will have an active alarm if the reserve limit is met, allowing the system administrator to either increase the space available or contact users to have them delete unnecessary reports or attachments.

7.3.3.2. Retention Filters

The Retention Filters tab lists all Resource Groups with Retention Rules enabled. These groups are configured at the Resource Groups page, and the edit Retention Groups button will take you to the Resource Groups page, with the group filter set to show just Retention Groups.

7.3.3.3. Advanced Retention Settings

Clicking the Advanced tab will expose some advanced configuration settings. You generally would not need to change any of these settings unless recommended by Eventide or your Eventide Communications Dealer.

Delete Parent Media Record: Certain Custom Integrations purchased from Eventide are designed to break existing media records into multiple records. When this is done, this setting determines whether the original media record is also retained or deleted

Use Prefix on Ignore: Used with Some Custom Integrations for Motorola SmartZone recordings where the same recording will be recorded from two different towers. This setting will cause the secondary ‘backup’ recording to have its channel name prefixed with DUP_ for ‘Duplicate’

Use Unknown as Channel name: Normally the channel name of a call will be assigned with the configured name of the channel it is recorded on. This value can then be overridden by a Metadata Feed or Custom Integration. If no value comes in from these secondary sources, the name remains the name of the channel. If this option is checked, and no value comes in via a Metadata feed or custom integration, then

the channel name for the recording will be set to ‘Unknown’ instead of the name of the channel it was recorded on.

7.3.4. Resource Groups

This page allows you to view and manage Resource Groups. A Resource Group is a configured set of one or more resources available on the recorder, and the rules that apply to those resources. Resources are the call sources on a recorder, and they are identified by channel name, physical channel id, and talk groups. Leveraging these rules and groups allows you to gracefully administer your NexLog Express recorders in a powerful and flexible way.

Resource Groups allows you to manage all policy for a set of resources, instead of having a separate channel group for each rule. For example, if you have a group of channels recording Fire Department calls and another set for Police, you can now have a Resource Group named Fire that contains all channels with names that start with Fire, that grants permission to the correct users and follows the legal requirements for keeping Fire recordings, all in one place.

7.3.4.1. Resource Group Rules

The rules available are:

Permission

Grant access to these resources to a list of users.

The users can then use these resources when browsing, exporting, searching, live monitoring, etc., based on the other permissions they are assigned on the User: Permissions page or are currently granted by being a member of a User Group.

Archive

By default, an archive drive archives calls from all resources, but when included in an archive rule, only calls from the group’s resources will be archived on the drives configured. This way a recorder that is split between Fire and Police duties can archive its Fire calls to one drive and its Police calls to the other.

Note thatonly one archive group can control a specific archive drive at a time; when a new rule is configured using a drive in use by another rule, it supersedes the previous rule. If you are unsure of which rule is in effect, check the Archive Configuration Edit page for an archive to see which is assigned.

Playback

Groups calls at record time such that they get played back simultaneously in 'playback group mode'. If a resource in this group type is selected for *Evaluation*, the other resources will automatically be included in the evaluation form. This is useful for pairing or syncing an audio and screen channel together.

Record

Recording on all resources in the group will start if the configured "Master Channel" starts recording. The Master Channel must be specified by Resource Name.

Retention

Specify duration that the calls from the resources in this group will be retained before deletion. This number must be smaller than the global retention setting for it to take effect.

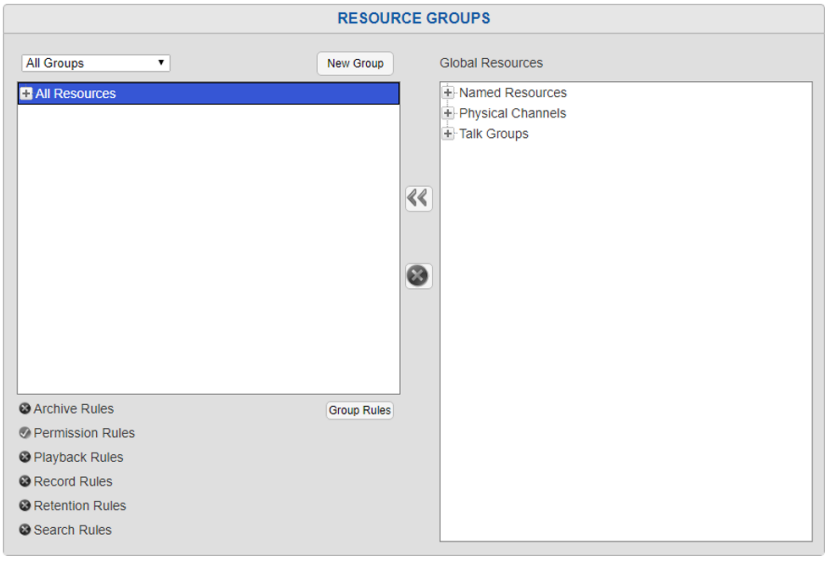


Fig. 7.40 Resource Groups

The main page is divided into two columns: the left displays all the configured groups, and the right shows all available resources, grouped in a tree by Named Resources, Physical Channels and Talk Groups. The groups can be individually filtered at the top, so that you can look only at groups that have Permission rules or Retention rules. The full list of filters is shown below.

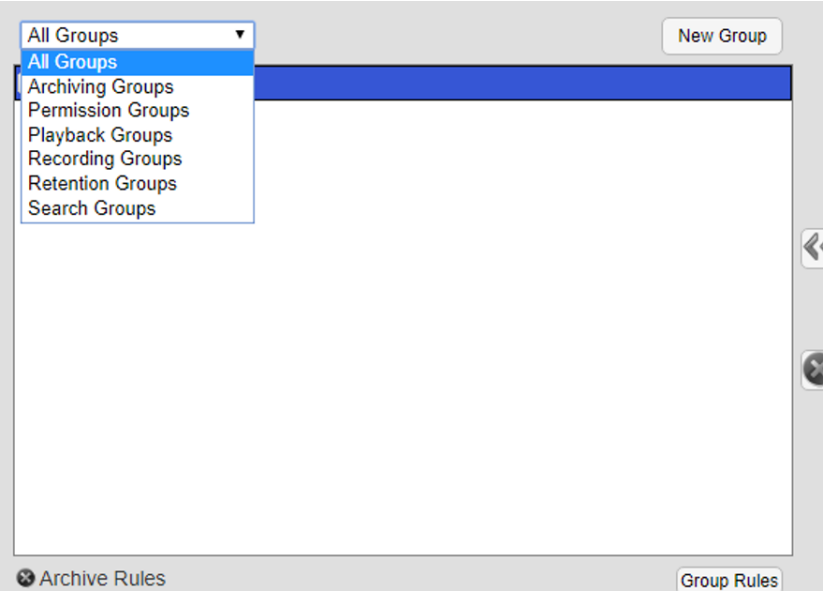


Fig. 7.41 Resource Group Rules Menu

At the bottom of the left column there is a summary of the currently selected group, showing which rules are currently configured and active for that group:

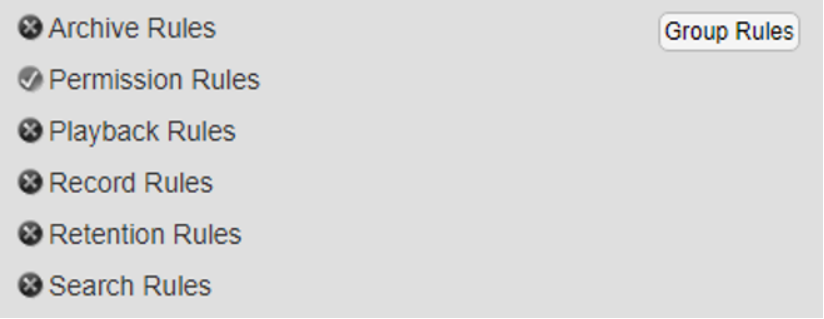


Fig. 7.42 Resource Group Rules Status

7.3.4.2. Creating Resource Groups

There are three ways to create a new Resource Group. The easiest way is to use the New Group button at the top of the left column on the Resource Groups page found in the Configuration Manager under Recording. There also two ways to create new groups in right-click menus that are detailed as we encounter them in the discussion below. The New Group button will create a new group and bring up the Group Edit window for that new group. Here you can name the group, select which rules apply, and configure each of those rules.

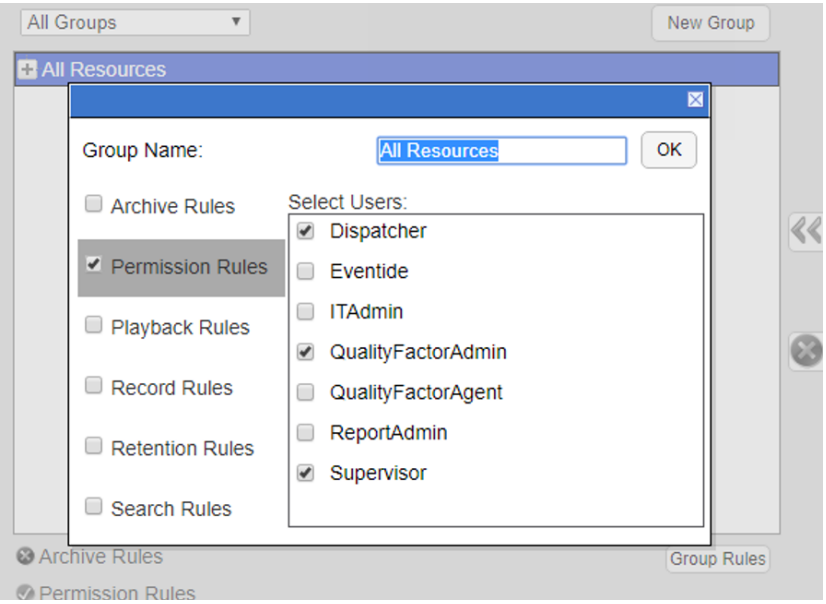


Fig. 7.43 Resource Group Edit: Permission Group View

Here we have a Resource Group named Front Hall, which has an active Permission Rule, granting users DJones, KPark, NLanders and WKing access to the channels in this group. A new group created with the New Group button will have no resources, which can be added in the two column view. Rules can be disabled by unchecking the checkbox; the rule's configuration will remain saved but not take effect while the checkbox is unchecked.

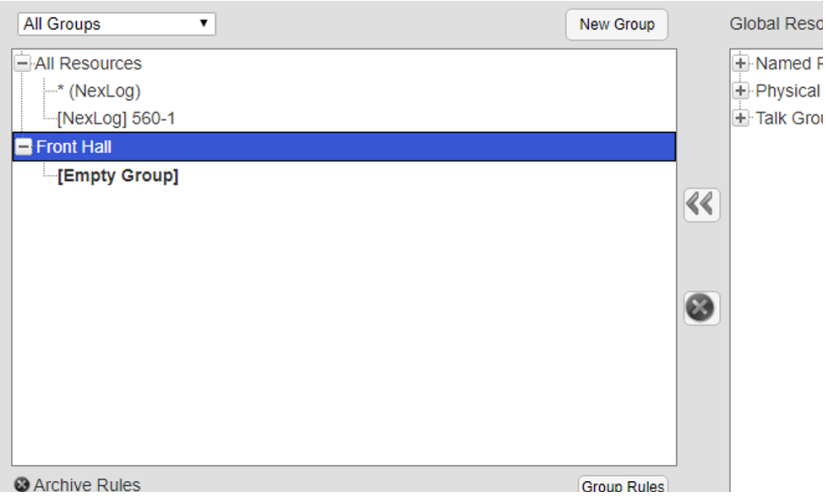


Fig. 7.44 Resource Group: Empty Group

7.3.4.3. Adding Resources to a Group

You can add resources to a group in a number of ways:

- The named resources and physical channel numbers in the right column can be clicked on to select them. Use Ctrl+Click or Shift+Click to select more than one at a time. Highlight a group in the right column by clicking on it. Then add the selected resources by clicking the leftward facing arrows between the columns.
- Select resources and a group in the right column as above, and then

  Right-Click them to reveal a pop up menu that allows you to Add to Selected Group.
- That pop-up menu also allows you to create a new group with these resources; it will open the group rules editor so that you can name and configure this new group.
- You can also select resources and click+drag them from the right column into the group you want them to be added to.
- You can right-click the name of the group and select from a menu, as seen in the figure below. From this menu, you can add a Name Filter, using * as a wild card to match multiple resources by name.
- This menu also allows you to add a Channel Filter, with which you can specify a range of resources by physical channel ID and their source, which defaults to Local. The source field is only relevant to configurations involving resources on the recorder originating from Centralized Archive sources; if

you want to group these, enter the serial number of the Centralized Archiving source into this field. Click the X to cancel and the Checkmark to save.

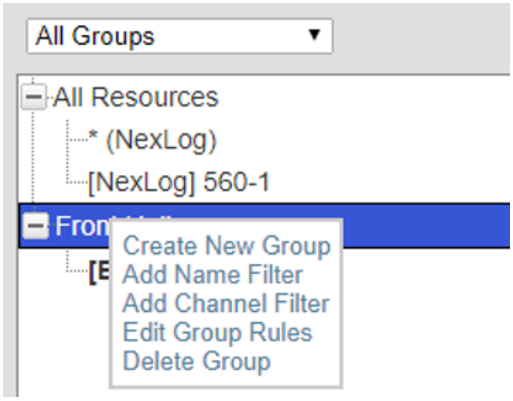


Fig. 7.45 Resource Groups: Right Mouse Button Menu

7.3.4.4. Deleting a Resource Group

You can delete a resource group in two ways:

- Select the Group in the left column, and click the X button between the columns.
- Right-Click on the group and select Delete Group from the pop up menu.

In both cases, you will be prompted to be sure that you really want to delete the group.

7.3.4.5. User Groups and Default Resource Groups

Resource Groups integrate with User Groups, in that a User Group can be configured to have User Permission Defaults. These defaults are a template rather than an active rule set. Defaults are granted to users when they are added to the group, but if the group's defaults are updated, the changes are not applied to the current members of the group.

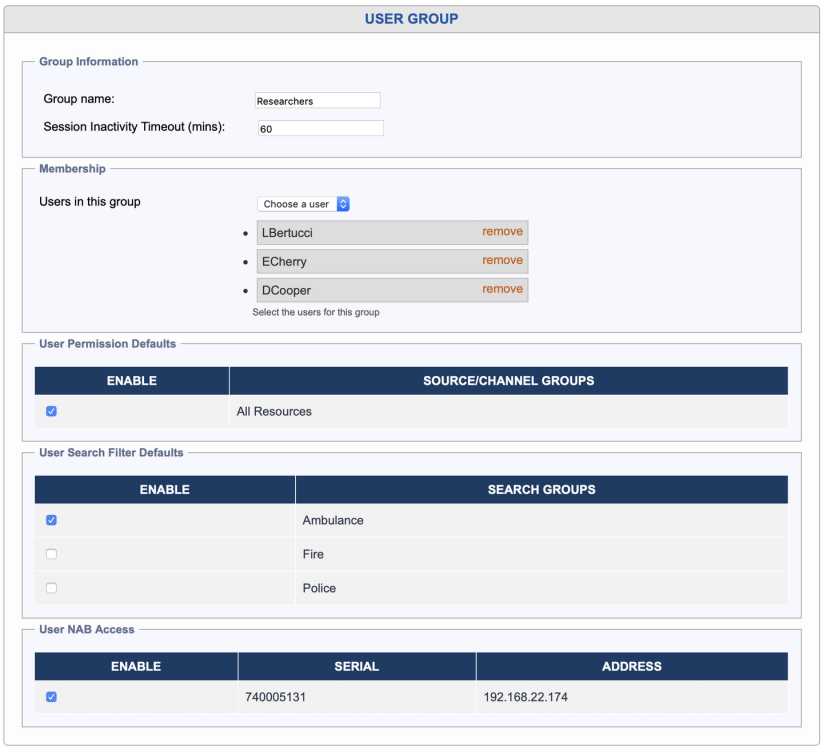


Fig. 7.46 User Group Edit

Following the behavior of previous NexLog Express versions the Browse, Exporter, Researcher and Monitor groups by default have All Resources as a Default Permission. Unless configured otherwise, all users in those groups will have access to all local resources on the recorder.

If there are configured Search Groups on the recorder, you can also assign a selection of these as defaults for the group. The default User Session Inactivity Timeout can also be set here.

7.3.4.6. User Specific Resource Permissions

In addition to permissions granted by a Resource Group with Permission Rules including them, a User can be configured to have specific resource permissions. A user may need to be given permissions to fewer resources than are granted by their membership in a user group, and by configuring it here you can narrow those permissions down to the desired set by deleting the set granted by default and recreating it with just the resources needed.

Conversely, a user may have a specific permission to access resources outside the normal scope of their user group, in which case these resources can be added individually.

7.3.5. Call Suppression

The Call Suppression form provides the means to suppress, or prevent, calls from recording (audio data will not be recorded, but the recorder retains non-audio data about the calls). This feature can be used for a variety of purposes, including implementing a legally mandated attorney-client privilege, or assuring privacy for undercover officers or high-ranking officials.

Two mutually-exclusive suppression methods are provided:

- Suppress on match (Blacklist): Suppresses recording for all calls that match a telephone number in the list. The recorder discontinues recording a call as soon as the telephone number is recognized.
- Record on match (Whitelist): Suppresses recording for all calls except for those that match a telephone number in the list.

The suppression method applies to the entire list of telephone numbers rather than to individual telephone number entries. To select a suppression method, click on the radio button next to it.

The Suppress DTMF feature applies to all call suppression. When recording is suppressed for a call and this feature is enabled, the recorder will not store a record of the telephone keypad dialing tones (Touch-Tones*) that occur during the call. This can be useful to prevent the storage of sensitive data transmitted by DTMF during a call, such as social security numbers, passwords, and personal identification numbers.

Click the *Suppress DTMF* checkbox to enable this feature.

To suppress recording, you must select a suppression method and create a list of telephone numbers. Then you must enable record suppression on a channel-by-channel basis via the boards setup page. The following instructions describe how to create and manage a list of telephone numbers.

To add a new entry to the list of numbers, click *Add Pattern* button. This allows you to enter in Suppression Digits, and a Description.

Enter a full or partial telephone number. A call containing this numeric sequence within its telephone number will cause a match. For example, if you enter 800-555-1234, any calls from this number will cause a match, but if you enter only 555, any calls with this sequence within the number will cause a match.

A partial number allows you to specify all calls from an area code or exchange. Whereas the Blacklist method is typically used for very specific telephone numbers, the Whitelist method is often used with a partial number sequence. For example, if you want to match on an area code and exchange, you can enter 800-555. (Note that a call from 900-*880-0555* will also match this number.)

Enter a description and click *Add*. The new pattern should appear in the suppression list.

When all patterns have been entered, click “Submit Global Settings” at the top of the page.

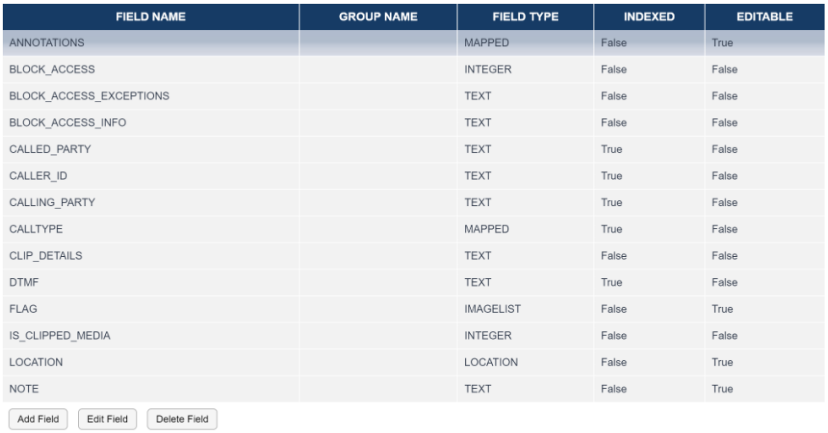
To enable suppression on a channel, add the “suppression” column on the Recording Interfaces page, then change Suppression from None to “Global List”

Note that Blacklist or Whitelists affect all channels where suppression is enabled. Suppression is not configurable per channel.

7.3.6. Custom Fields

By default, the NexLog Express database stores several pieces of information about each Record, such as the Channel Number and Name it was recorded on, the Date/Time it started, and its Duration. In addition to these standard fields, some optional features and custom integrations can fill in additional information. Since there is no preset field in the database to hold this information, you must configure a Custom Field to store the info. These fields are populated by various optional and standard subsystems, or by custom integrations. For example, upon a fresh installation, five custom fields are automatically added: `Annotations`, `Caller_Id`, `Calling_Party`, `Calltype` and `DTMF`. These fields are automatically filled in for calls which enter the system via certain board tasks. For example, a call received on an Analog card which contains DTMF Tones will have those tones automatically processed and the corresponding numbers entered into the database record for that recording as long as the DTMF custom field has not been deleted. If you are not using those fields they may be deleted for your convenience.

In addition to the five preset Custom Fields, certain optional features, both licensed and core, may utilize a preset custom field and for those features to operate, a custom field by the indicated name must be added. Examples of such custom fields are `MF_ANI` for storing the MFR2 ANI Number transmitted on some analog CAMA trunks, and `RadioID` for the ANI transmitted via MDC1200 on some analog Radio systems. Custom metadata integrations may require additional custom fields, for example, an ANI/ALI Spill for a 911 Call Center may contain information such as `Carrier` and `Street_Address`. These custom fields could be added to the system, and the metadata integration configured can populate them. Note that just adding a new custom field without an integration to populate it will not provide a useful function, just empty fields. Custom fields can be enabled as columns in the playback clients (MediaWorks EXP, etc.) to view the metadata associated with a call.



FIELD NAME	GROUP NAME	FIELD TYPE	INDEXED	EDITABLE
ANNOTATIONS		MAPPED	False	True
BLOCK_ACCESS		INTEGER	False	False
BLOCK_ACCESS_EXCEPTIONS		TEXT	False	False
BLOCK_ACCESS_INFO		TEXT	False	False
CALLED_PARTY		TEXT	True	False
CALLER_ID		TEXT	True	False
CALLING_PARTY		TEXT	True	False
CALLTYPE		MAPPED	True	False
CLIP_DETAILS		TEXT	False	False
DTMF		TEXT	True	False
FLAG		IMAGELIST	False	True
IS_CLIPPED_MEDIA		INTEGER	False	False
LOCATION		LOCATION	False	True
NOTE		TEXT	False	True

Add Field Edit Field Delete Field

Fig. 7.47 Custom Fields

The Main Setup page for Custom Fields shows a list of all fields currently configured, as well as a button to add a new custom field, and a button to Edit or Delete a selected custom field. Simply select the desired field, and then the desired action button. Each Custom Field has several options which can be configured and viewed. These are:

Field Name: This is what the field will is called in the MediaWorks EXP/Front Panel Column and also how it will by identified by the Server. Any field name can be used with a custom integration, but certain field names have specific uses on the server. For example, DTMF, CALLING_PARTY, CALLER_ID, MF_ANI, MDC_ANI, and USER_ID are special fields. If these fields exist on the recorder and the corresponding back end configuration options are enabled and configured, they will be populated by the systems. Other fieldnames will only ever be populated via Custom Integrations or manually by users using client software. Field names are limited to alphanumeric characters and must start with an alphabetical character. Underscores are also allowed and will be translated to spaces for display purposes.

FieldType

What type of data the field will be designed to hold in the database. This can be one of seven types: Integer, Text, Float, Location, List, Image List, Checkbox.

Group Name

Optional field used to group custom fields together in MediaWorks EXP search filters. For example, if you are using RSOS Location, you may want all RSOS fields to be in the RSOS group, so that they

show up grouped by RSOS rather than alphabetically in with all other configured fields. It has no effect on recording or the contents of the metadata.

Text

is generally always used unless efficient database searching based on “greater than” or “less than” will be utilized. Float is for numbers with a decimal place, whereas Integer fields contain only whole numbers. Location is used for Geolocation GPS data.

Image List

allows you to choose from a wide variety of images that can be assigned to a call record in MediaWorks EXP. By default, Image Lists that are editable will include an option to “unset” the value back to nothing. The “Color_Code” field created for the example below has 9 images selected and the unset option turned on:

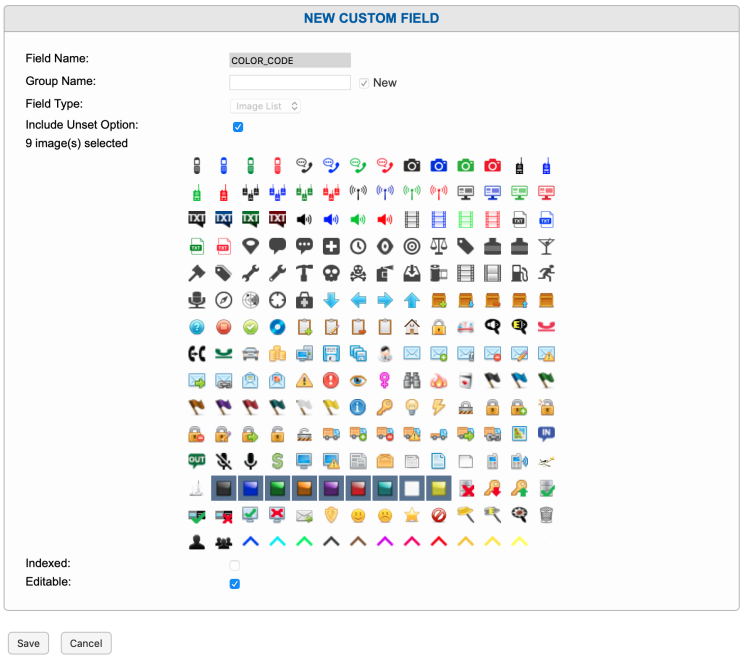


Fig. 7.48 Custom Image List Color_Code Example

These images can then be assigned to call records in MediaWorks EXP. The Color Code field of the selected call record in blue in this image has been double clicked, opening the menu to select the image from:

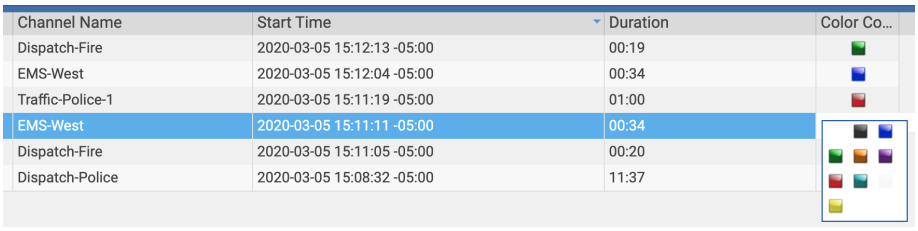


Fig. 7.49 Color_Code Example in MediaWorks EXP

List

is similar. It lets you create an arbitrary list of values that can be selected from a pull down menu. A Checkbox field will display a column of checkboxes in MediaWorks EXP. It is important to make List, Image List and Checkbox fields editable, if they are going to be set by end users in MediaWorks EXP.

Indexed

If this field is enabled, the recorder database will maintain an index on the metadata field. This index will make searching on the field in Front Panel and MediaWorks EXP more efficient and fast, at the expense of additional CPU load on the server to maintain the index. Fields that will commonly be searched on should be indexed.

Editable

If true, users will be able to edit the value of this field in MediaWorks EXP, otherwise only the Recorder itself will be able to control the value of the custom field for a call.

When adding new custom field, the above options can be configured. However, when editing an existing custom field, only the Verifier and Editable options can be changed. This is because the Field Name, Type, and Indexed Status end up in the database schema and cannot be efficiently changed. Changing these values would require deleting and re-adding the custom field, which would have the side effect of deleting any information stored in this field for any recording on the recorder.

Deleting a custom field using the ‘Delete’ Button will also delete any data stored in the custom field for any recording in the database.

7.3.6.1. Calltype

Calltype is a feature that automatically tags records with an image representing the kind of recording it is. By default, recordings made on Analog Recording cards will be tagged with Audio, T1/E1 with Phone, screen captures with Screen. These automatic mappings will only be set up when the system is installed or when a new board is added.

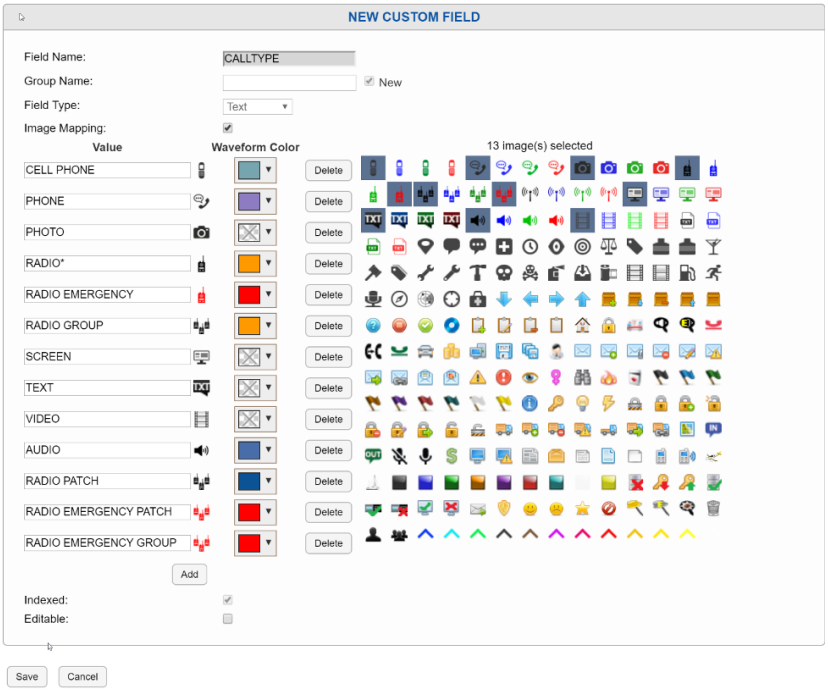


Fig. 7.50 Calltype Field Configuration

If you want to set up a new Calltype if the default mapping isn't appropriate for a channel, you can configure it by going to Recording: Boards, expanding a board and then clicking the Gear to edit the channel. Once on the Edit Channel page, change the Default Call Type field to match one of the entries in the Custom Field mapping. You can put any text here and it will be automatically tagged in this field for all calls that come in on this channel but if you want it to show an image in the timeline, you need to have this text match one of the entries in the map.

If you want to set the value for every channel of a board in one go, click a column header on the Recording Interfaces page and select Default Call Type and then click it again to select Set All Values → Default Call Type, enter the desired value and hit the enter key.

7.3.7. Alias Banks

Alias Banks is a feature that lets you to modify incoming metadata information to make it easier to understand, or to name channels on the fly as new calls come in, to move metadata from one field to another. It is useful for sites with complex needs, but also for simple tasks like taking calls that come in on one physical channel and assign them a resource name based on their talk group.

7.3.7.1. Add Alias Bank

Click this button to add a new Alias bank. Each field has a tool tip in a ? icon. Hover your mouse pointer over the icon to see an explanation of the field.

- Alias Bank Name

  The Name of the Alias Bank

- Output Formatter

  This field is used to format the output of the alias. By default it is {{ALIAS}}, which passes on the output as is.

- Enabled

  Checkbox to turn on or off this Alias Bank

- Alias From → Alias To

  This Alias Bank will take metadata from Field 1 and put it in Field 2. It can also be used to take metadata from Field 1, process it, and put the updated version back into the same

Field 1. These pull down menus have a search bar at the top to assist at sites with many custom fields configured.

- Only Apply Alias If

  This field lets the alias be predicated on a condition.

  - `=` exact match
  - `~=` contains this string
  - `!~=` does not contain this exact string
  - `!=` is not this exact string

- Applied Channels

  Which boards and physical channel numbers will this alias apply to. The field can contain * for all channels on this board, a comma delimited list of numbers, or ranges with a hyphen, or a mixture of these such as “1,4,7,9-12,15”

- Alias Rules

  These fields can accept Regex processing to take incoming metadata and format it into a new more readable format. See the examples below for details.

> **Note**
>
> If *CALLDIRECTION* is one of the fields involved in aliasing, please use ‘i’ instead of ‘Inbound’, ‘o’ instead of ‘Outbound’ and ‘u’ instead of ‘Unknown’.

When editing a board on the Recording Interfaces page, there is an Alias Banks tab that will show any Alias Banks relevant to the channels of the board being edited. You can jump directly to any Alias Bank in the list by clicking its name.

7.3.7.2. Alias Bank Examples

7.3.7.2.1. Scenario 1

A common use case for Alias Banks is for Radio Integrations where the Radio system sends a numeric RadioID showing which radio is talking, but does not provide Alias information. If the RadioID is put in a metadata field called RadioID, and we want to put a corresponding Alias in a field called RadioAlias. Lets say RadioID 100 should map to B.Smith, 101 to R.Jones, and 102 to J.Doe.

If you want to leave RadioAlias blank for RadioIDs with no match, here is how to configure it:

- Source: {{ALIAS}}
- Alias From: RadioID
- Alias To: RadioAlias
- Only Apply Alias If: n/a
- Applied Channels: (as needed)
- Alias Rules:
  - Source: 100 Alias: B.Smith
  - Source: 101 Alias: R.Jones
  - Source: 102 Alias: J.Doe

7.3.7.2.2. Scenario 2

If instead you want to put “Unknown” into RadioAlias for RadioIDs with no match, put a wild card match as the final rule, to catch all other options:

- Output Formatter: {{ALIAS}}
- Alias From: RadioID
- Alias To: RadioAlias
- Only Apply Alias If: n/a
- Applied Channels: (as needed)
- Alias Rules:
  - Source: 100 Alias: B.Smith
  - Source: 101 Alias: R.Jones

- Source: 102 Alias: J.Doe
- Source: * Alias: Unknown

7.3.7.2.3. Scenario 3

If instead of adding the Alias to RadioAlias, you want to change the RadioID to the Alias, do the same as scenario 2 and just change the Alias To to be RadioID as well:

- Output Formatter: {{ALIAS}}
- Alias From: RadioID
- Alias To: RadioID
- Only Apply Alias If: n/a
- Applied Channels: (as needed)
- Alias Rules:
  - Source: 100 Alias: B.Smith
  - Source: 101 Alias: R.Jones
  - Source: 102 Alias: J.Doe
  - Source: * Alias: Unknown

7.3.7.2.4. Scenario 4

If you wanted the RadioID field to contain “RadioAlias (RadioID)” eg. “BSmith (101)”, with “Unknown (135)” for unmapped values (such as 135) for a given Radio ID.

- Output Formatter: {{ALIAS}} ({{SOURCE}})
- Alias From: RadioID
- Alias To: RadioID
- Only Apply Alias If: n/a
- Applied Channels: (as needed)
- Alias Rules:
  - Source: 100 Alias: B.Smith
  - Source: 101 Alias: R.Jones
  - Source: 102 Alias: J.Doe
  - Source: * Alias: Unknown

7.3.7.2.5. Scenario 5

If a data integration provided a talk group name in a field called TalkGroup, and you wanted to set the ChannelName for each call to 'TG_{Talkgroup_Name}', eg "TG_FIRE1", here is how you would configure it:

- Output Formatter: TG_{{ALIAS}}
- Alias From: TalkGroup
- Alias To: ChannelName
- Only Apply Alias If: n/a
- Applied Channels: (as needed)
- Alias Rules:
  - Source: REGEX{{.*}} Alias: REGEX{{$0}}

7.3.7.2.6. Scenario 6

Suppose you wanted to set CALLTYPE to 'RADIO EMERGENCY' if the ChannelName for a call was 'EMERG1' or 'EMERG2', but otherwise wanted to not modify it. This would require two Alias Maps, one for each ChannelName:

EMERG1:

- Output Formatter: {{ALIAS}}
- Alias From: CallType
- Alias To: CallType
- Only Apply Alias If: ChannelName = EMERG1
- Applied Channels: (as needed)
- Alias Rules:
  - Source: * Alias: RADIO EMERGENCY

and EMERG2:

- Output Formatter: {{ALIAS}}
- Alias From: CallType
- Alias To: CallType
- Only Apply Alias If: ChannelName = EMERG2
- Applied Channels: (as needed)
- Alias Rules:
  - Source: * Alias: RADIO EMERGENCY

7.3.7.2.7. Scenario 7

If, for example, you had a T1 with DID (so every extension has its own phone number), every outgoing call will have CallerID identifying the outgoing line, and every inbound call will have DTMF indicating the same. If you wanted to set the ChannelName to an Alias based on the DTMF For Outbound Calls and CallerID on Inbound calls so that 555-1212 would get a channelname of “Main Office” and 555-1234 would get “Records Department”, here is how you would configure that:

Outbound Calls:

- Output Formatter: {{ALIAS}}
- Alias From: CallerID
- Alias To: ChannelName
- Only Apply Alias If: n/a
- Applied Channels: (as needed)
- Alias Rules:
  - Source: 555-1212 Alias: Main Office
  - Source: 555-1234 Alias: Records Department

and Inbound Calls:

- Output Formatter: {{ALIAS}}
- Alias From: DTMF
- Alias To: ChannelName
- Only Apply Alias If: n/a
- Applied Channels: (as needed)
- Alias Rules:
  - Source: 555-1212 Alias: Main Office
  - Source: 555-1234 Alias: Records Department

7.3.8. Data Integrations

Data Integrations page provides functionality that integrates with and accept data from third party systems and enable special handling of some data within the recorder. For example, a generic ANI/ALI integration could be configured to receive information over serial or IP, parse it based on user specified rules and apply it to ongoing calls.

This page shows a list of the available Data Integrations, with information on which are licensed and which are enabled. You can restrict the list to just the licensed integrations with the Hide unlicensed integrations checkbox.

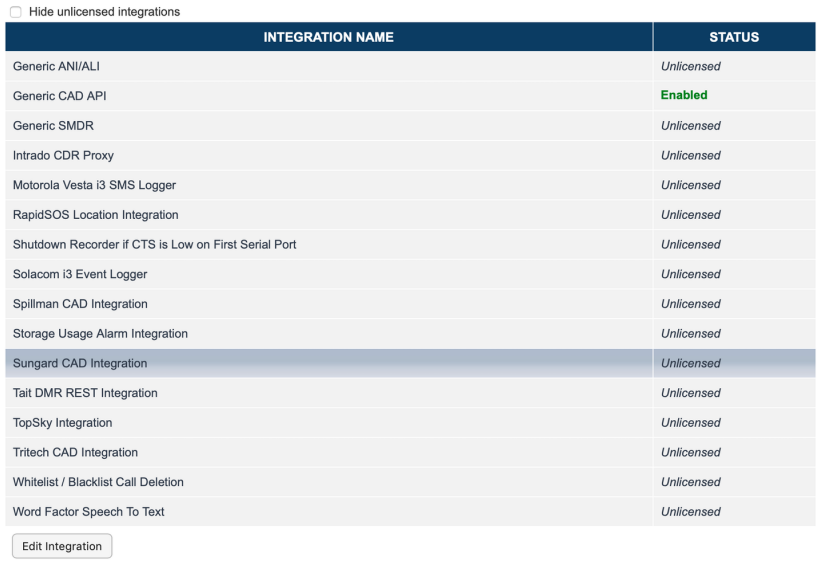


Fig. 7.51 Data Integrations Page

To configure or enable an Integration, select a licensed Data Integration from the list and click Edit Integration. This will open a page with:

- Script Version: This will show the System version and the Current version of the integration script. If an integration has been configured, it is not updated when an upgrade happens, to prevent it from breaking. To bring it up-to-date, copy the Configuration file to a text editor (for reference), disable the integration, save, edit again and reconfigure based on the new configuration file.
- Configuration File: This contains all variables that need to be set for the integration to work.
- Integration Enabled: This checkbox turns on or off this Integration.

Some integrations also offer these options:

- View Processing Logs: See how the Integration has processed the input.
- View Input Logs: See the input from the CAD system.
- Replay Timestamp: Copy the timestamp from the input log and enter it here to have it replay based on the current configuration setting. This allows for iterative development of the integration.

7.3.8.1. Broadcastify

Eventide Communications NexLog Express recording systems can support streaming one or more recorded streams to a feed on https://www.broadcastify.com/ Licensing is on a per-stream basis, and a stream can contain one or more recorded resources/talkgroups. Keep in mind that in this case they will be streamed together. Please contact Eventide Communications sales for the per stream pricing. Before attempting to stream from the NexLog Express to Broadcastify, a feed will need to be created on Broadcastify.com. Credentials and required details to stream to that feed will also need to be obtained. Instructions on how to establish a feed, and the terms and conditions related to streaming content to a feed are not part of this document. Please refer to the Broadcastify.com -> “Broadcast” section for further details. Administrative level knowledge of the NexLog Express configuration manager and tools is assumed when using this document. If you are not familiar with the NexLog Express Web Configuration Manager, please contact your local Eventide Communications dealer/reseller for assistance.

Software, Licensing and Configuration

Once the NexLog Express recorder is licensed for Broadcastify, the integration can be edited and enabled for streaming to the Broadcastify.com website.

Licensing

- Contact Eventide Communications Sales to purchase an add-on license key if your recorder is not already licensed for Broadcastify. You will need to know how many unique streams you plan to stream to Broadcastify. The license generated is on a per-stream-basis.
- Log in to the Configuration Manager
- Go to “System” -> “License Keys”
- Click “Add Key”
- In the “License Key” field, enter the add-on key provided by Eventide Communications

Configuration of the Broadcastify stream(s)

- Log in to the Configuration Manager

- Go to “Recording” -> “Data Integrations”
- Select “Broadcastify Integration” and click “Edit Integration”. Here you will need to configure a mount point for the Broadcastify stream. Details about the parameters to enter are shown in the screenshot below
- When complete check the “Integration Enabled” box (as seen in the screenshot below) and then click the “Save” button

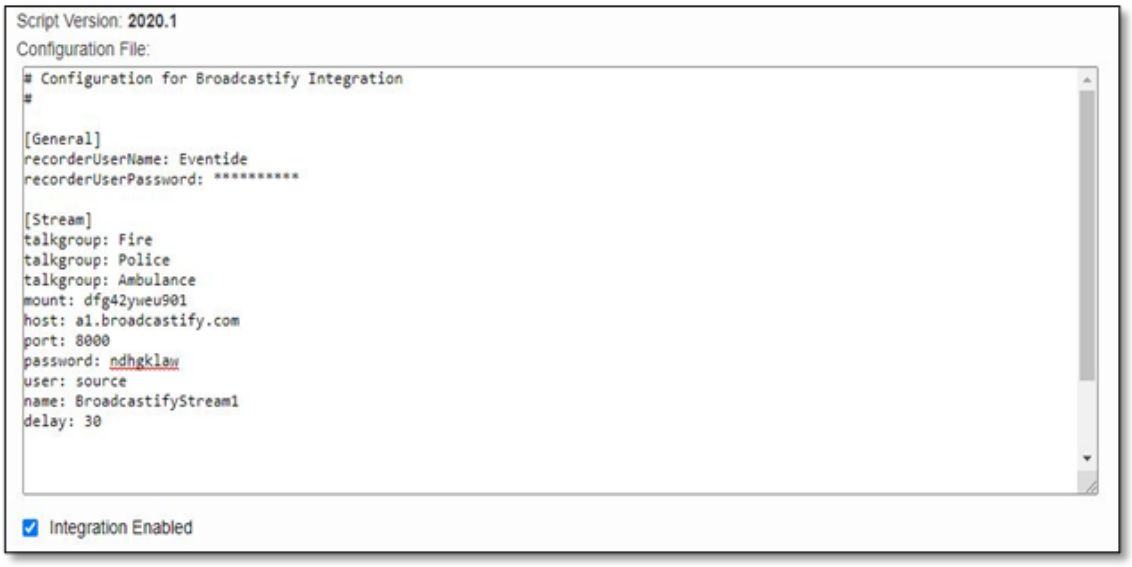


Fig. 7.52 Broadcastify Configuration

Below are descriptions of the configuration fields as seen in the above screenshot:

- recorderUserName: Recorder user that has access to playback of the resource/talkgroup being recorded
- recorderUserPassword: Password for the recorder user that has access to playback of the resource/talkgroup being recorded
- talkgroup (i.e. resource name): Name of the resource/talkgroup being recorded that will be associated with a Broadcastify playback stream. You can add multiple resources/talkgroups to one stream. Note, if multiple resources are configured for one stream, they may transmit audio over each other and may not be audible. Multiple separately streamed resources/talkgroups must be configured with their own unique [Stream] sections of the configuration.
- mount: Name of the mount where the Broadcastify playback stream can be accessed (acquired from Broadcastify)
- host: Server address of the Broadcastify playback stream (acquired from Broadcastify)
- port: Port to be used for the Broadcastify playback stream (acquired from Broadcastify)

- password: Source client password (acquired from Broadcastify)
- user: Source client username (acquired from Broadcastify)
- name: Name of the Broadcastify stream for identification on the NexLog Express DX server. If you configure multiple streams, then each stream should have a unique name. Refer below for details on how to configure multiple streams.
- delay: This is a configuration option that sets the delay between a recording and when it will playback on a Broadcastify stream. The default and minimum delay is 30 seconds, which means that the Broadcastify playback will occur 30 seconds after the recording. This can be reconfigured to suit local requirements, though must be less than the value used for retention time of the recording/resource itself.

Configuring Multiple Streams

You can configure a recorder to have multiple streams. Each stream requires the following:

- A separate “[Stream]” section as seen in the screenshot below. The first stream in the example below is dedicated to a “Fire” talkgroup, while the second stream is dedicated to a “Police” talkgroup
- Each stream should have its own unique mount as seen in the screenshot below
- Each stream should have its own unique name as seen in the screenshot below

Fig. 7.53 Broadcastify Configuration Multiple Streams

Configuring AGC and Gain

From software version 2020.4 onwards in the NexLog Express DX-Series, Broadcastify streams can be configured to enable AGC and gain settings.

AGC Configure

To configure AGC, follow the steps below:

- Log in to the Configuration Manager
- Go to “Recording” -> “Data Integrations”
- Select “Broadcastify Integration” and click “Edit Integration”.
- On a new line in this configuration file, add the following text: agc: 1
- Save the configuration file

To disable AGC, you can either change the configuration value from 1 to 0, or you can just remove the line of the text with the AGC configuration.

Gain Configure

- To configure gain, follow the steps below:
- Log in to the Configuration Manager
- Go to “Recording” -> “Data Integrations”
- Select “Broadcastify Integration” and click “Edit Integration”.
- On a new line in this configuration file, add the following text: gain: <value of gain>
- The supported gain values are: -4,-3,-2,-1,0,1,2,3,4,5 where -4 is the softest volume setting, and 5 is the highest.
- Save the configuration file

To disable a gain setting, you can either set the configuration value to 0, or you can just remove the line of text with the gain configuration.

Please also keep the following two points in mind when configuring AGC or gain:

- Both AGC and gain settings must be specified under a particular stream. They will apply to all talkgroups that are a part of that stream.
- If both AGC and gain are specified, only AGC will get applied.

Stream Address

Once the Broadcastify Integration Configuration File is saved, you will be able to access the Broadcastify stream by going to the address specified in the configuration file. The format of the address is:

<host>:<port>/<mount>

Based on the example in the screenshot above, the address of the mount would be:

a1.broadcastify.com:8000/dfg42yweu901

Connectivity and Access

The most common problem when setting up Broadcastify.com streaming is connectivity between the Eventide Communications NexLog Express system and the Broadcasity.com mount point. Configuring access between the NexLog Express system and Broadcastify is unique to each enterprise networking environment and outside the scope of this document.

7.3.8.2. ProPhoenix CAD Integration

New in version 2024.1.

This integration adds all the necessary custom fields to integrate ProPhoenix Computer Aided Dispatch (CAD) into the NexLog Express system.

License Required

This feature must be licensed to be used. Contact your Eventide Communications Dealer for assistance.

Once the Data Integration has been licensed and enabled, the following Fields are added to the Custom Fields menu:

FIELD NAME	GROUP NAME	FIELD TYPE	INDEXED	EDITABLE
CAD_ADDRESS	CAD	TEXT	False	False
CAD_AGENT	CAD	TEXT	False	False
CAD_ARRIVAL_TIME	CAD	TEXT	False	False
CAD_CALLNR	CAD	TEXT	False	False
CAD_CFS	CAD	TEXT	False	False
CAD_CFS_DESCRIPTION	CAD	TEXT	False	False
CAD_CSZ	CAD	TEXT	False	False
CAD_DISPATCH_TIME	CAD	TEXT	False	False
CAD_INCIDENT_ID	CAD	TEXT	False	False
CAD_LOCATION	CAD	TEXT	False	False
CAD_RPTDATE	CAD	TEXT	False	False

7.3.8.3. Tait DMR -SMS/SDS Integration

One of many benefits of DMR Digital two-way radios when compared to Analog radios is the ability to send text messages to just one individual or a group without switching channels.

This Data Integration allows supported systems to log SMS/SDS events.

License Required

This feature must be licensed to be used. Contact your Eventide Communications Dealer for assistance.

In the Recording -> Data Integrations Section, select the “Tait DMR REST Integration”, then click “Edit Integration”.

Changed in version 2024.1.

The following settings can be edited based on the user’s preferred DMR configurations:

- doSMS: 0 or 1 to enable tagging calls with text SMS as annotations.
- SMS_Pointer: a date in the format of “YYYYMMDD” to indicate how far back to start searching for SMS calls. If left empty, will start at the current time.

Fig. 7.54 Tait DMR Integration

Once settings have been configured, ensure Integration Enabled has been selected and click “Save”

DMR SMS and SDS events should now be recorded and visible via MediaWorks EXP.

7.3.8.4. NexLog Database Fusion

New in version 2024.1.

Eventide Communications NexLog Express has the ability to import data and tag recordings from any database system that has an accessible SQL database. For example, if your agency has a Computer Aided Dispatch(CAD) system with an accessible database, the NexLog Express Database Fusion can connect the data to easily associate incidents with recordings on your recorder.

This service is configured by an Eventide Communications technician and works by checking the database for new records or incidents and consuming them on a configurable interval. In most circumstances, 911 audio can be tagged with the associated CAD incident data within 15 seconds of being entered into the CAD system. As the CAD incident develops, other information is associated to the 911 recording such as units dispatched and unit arrival times. This integration often provides more detailed and flexible data than a customized CAD integration. For example, you can choose to import data like 'call disposition' or 'CAD notes'.

CAD records can be searched by agent or position to get a complete picture of all the data entered into the CAD system over a period. Researchers can easily locate the CAD record and then drill down with the new 'Show More' feature to locate the 911 Audio, radio, screen recordings, and other data associated with the Incident.

Additionally, the system can store CAD data unrelated to 911 calls, like automated security alarms and police-initiated events.

To use the "Eventide CAD Data Importer Service," the following conditions must be met:

- Provide a CAD replication database.
- The database should be an SQL database with ODBC or MSSQL connectors.
- The recorder must be able to network with the CAD replication database using the database connector port.
- The recorder requires credentials to authenticate with the replication database.
- The provided credentials must have access to the table or view from which the information will be retrieved.

Note

The SQL database requires a table view that matches the schema provided by Eventide Communications.

7.3.8.5. Prepared 911 Data Integration

New in version 2024.1.

License Required

This feature requires a Prepared911 Integration license to be used. Contact your Eventide Communications Dealer for assistance.

Prepared Live is a platform that facilitates communication and enables Public Safety Answering Points (PSAPs) to collect rich multimedia information directly from 911 callers before the arrival of any first responders. When integrated with Eventide Communications's |NL| recording solution, dispatchers and call-takers exchange messages with a caller and collect live video, photographs, videos, and GPS location.

7.3.8.5.1. NexLog Express Configuration

There are two parts to configuring the NexLog Express recorder:

- Get credentials from Prepared Live
- Add configuration to the NexLog Express software

To initiate the integration between Prepared Live and Eventide Communications NexLog Express, customers should follow these steps:

- Reach out to either their Prepared Live Customer Success Manager (CSM) or their Eventide Communications Dealer.
- Request their account to contact the NexLog Express dealer. It's important to note that the integration on Eventide Communications's end will not function unless a separate license from Eventide Communications is obtained.

- After completing the necessary steps with the dealer, and upon receiving approval from either the dealer or the customer, the Prepared Live Go-to-Market (GTM) representative will proceed.
- Once generated, Prepared Live will provide client_id and client_secret credentials to the CSM representative, who will then forward to the customer.

To configure the Prepared911 integration, log into NexLog Express Configuration Manager, then go to Recording > Data Integrations, select Prepared911 Integration and hit the Edit Integration button.

Here you'll select Enable Integration and add the Server, ClientId, and ClientSecret details that were provided by Prepared Live.

> **Note**
>
> For additional information, please contact your Eventide Communications Representative.

7.3.8.6. Motorola Premier One CAD Integration

New in version 2024.1.

This integration supports call tagging and data importing modes to connect your Motorola Premier One CAD system with your NexLog Express recorder.

> **License Required**
>
> PREMIERONE CAD INTEGRATION requires a license to be used. Contact your Eventide Communications Dealer for assistance.

Once this feature is Licensed and enabled, all data field variables are listed in order to properly configure this integration, including but not limited to:

- Server
- Port
- User
- Password

- Call Start Difference (the number of seconds to look ahead and behind of incident's created time for a recorded call to attach metadata to)

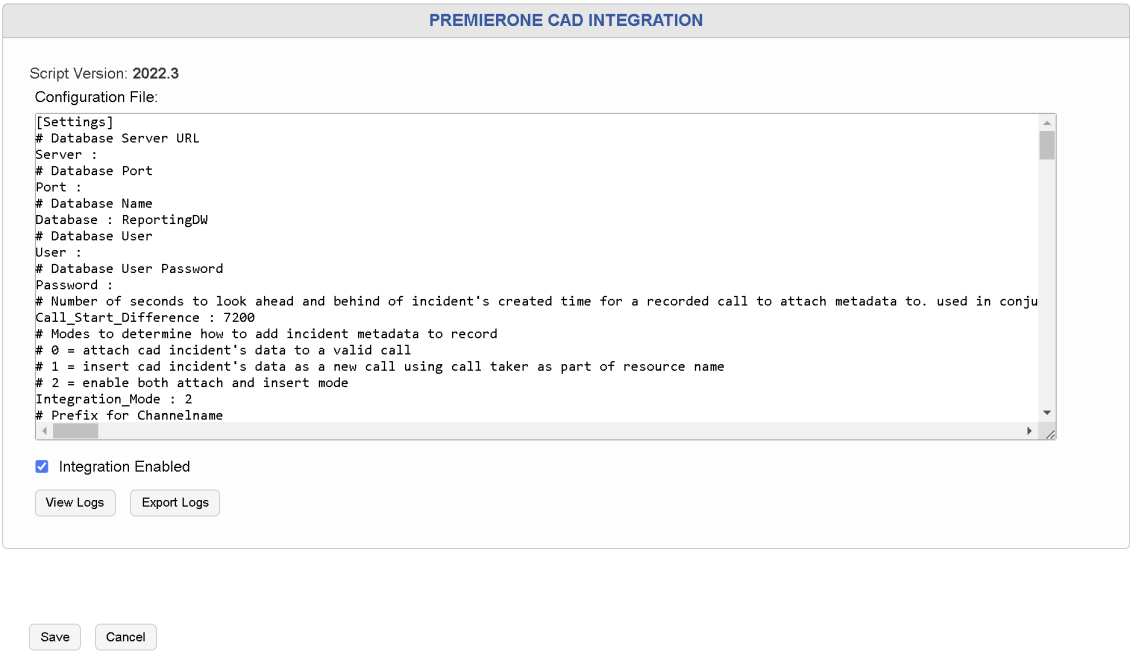


Fig. 7.55 PremierOne CAD Integration

For more details, please contact Eventide Communication's technical support.

7.3.8.7. Intelcan Skycom ATM Integration

New in version 2024.1.

The Intelcan Skycom ATM Integration establishes a connection between Eventide Communications's NexLog Express system and Intelcan's Skycom system. This connection aids in helping air traffic controllers effectively monitor, track, and control aircraft within their assigned airspace, utilizing information such as target data, flight plans, and other essential aeronautical data.

Additionally, the system is an important utility for supervisors, who use it to oversee operations, manage settings, and configure the system as needed.

License Required

Intelcan Skycom ATM Integration requires a license to be used. Contact your Eventide Communications Dealer for assistance.

Once this feature is Licensed and enabled, you have access to configuring the CommandPort.

Fig. 7.56 Intelcan Skycom ATM Integration

Note

The default port is 5000 but it can be configured when enabling the integration.

For more details, please contact Eventide Communication's technical support.

7.3.9. Geo-Location

License Required

This feature must be licensed to be used. Contact your Eventide Communications Dealer for assistance.

Call records can now be tagged with location metadata which can be used to visualize where calls are coming from. The location data can also be used as criteria for searches.

In order to set up Geo-Location, navigate to Recording > Geo-Location, choose “Enabled” and Save:

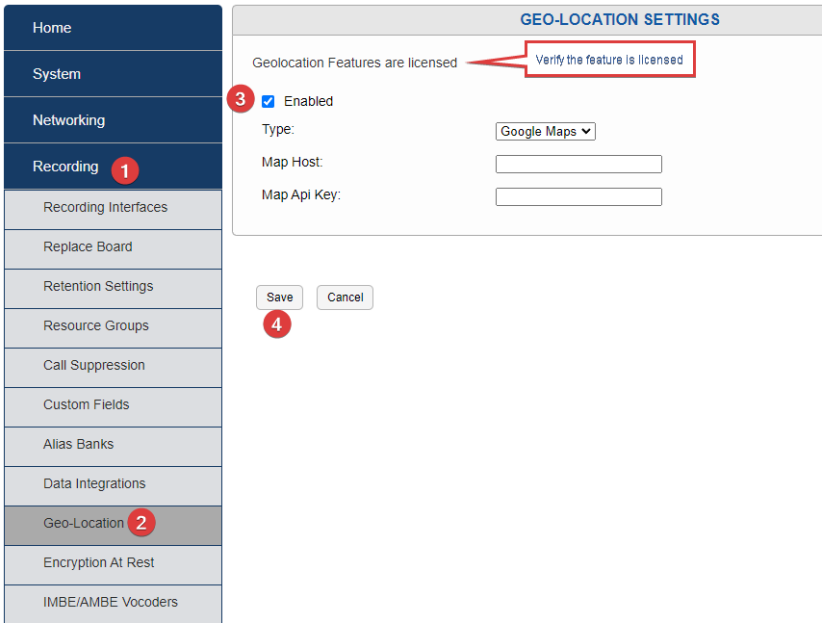


Fig. 7.57 Geo Location Configuration

Additionally, you’ll need to add a custom field to set up Location functionality by navigating to Recording > Custom Fields, and choose “Add Field”:

Fig. 7.58 Geo Location Custom Field

The Field Name should be set as “Location” and the Field Type should drop down to “Location”, then select “Add”:

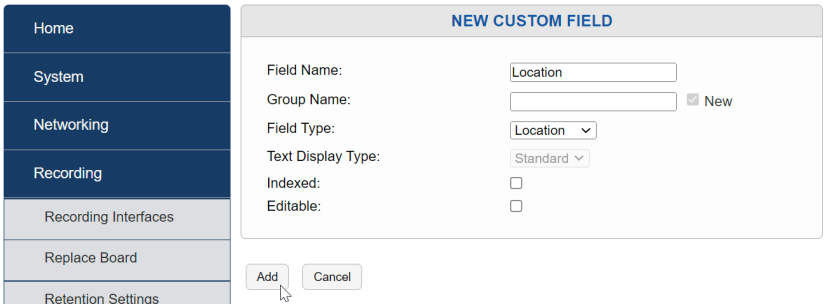


Fig. 7.59 Add Location Field

Note

Full Geo-Location details and functionality can be found in the MediaWorks EXP Manual.

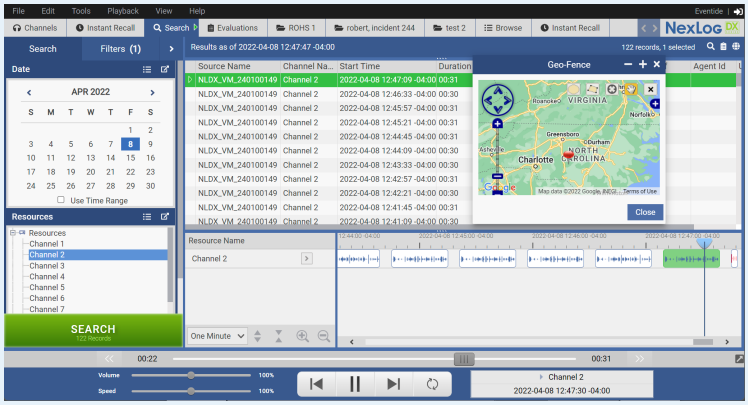


Fig. 7.60 MediaWorks EXP Geo-Location

7.3.10. Internal Vocoder

License Required

DVSI will require a “Num Internal Vocoder Resources” add-on license key. Contact your Eventide Communications Dealer for assistance.

In this section, you will see the number of internal IMBE/AMBE vocoders the recorder is licensed for, as well as the number of simultaneous users that can transcode calls via playback or export in MediaWorks DX.

The number of resources licensed corresponds to how many users can simultaneously transcode calls with a 1:2 relation.

Example:

- If you are licensed with 1 resource, then 2 users can simultaneously transcode calls.

This means that 2 users can simultaneously transcode calls via playback, or 1 user can transcode via playback and another user can transcode via export at the same time.

> **Note**
>
> If a 3rd user tries to transcode at that time, they'll receive a warning.

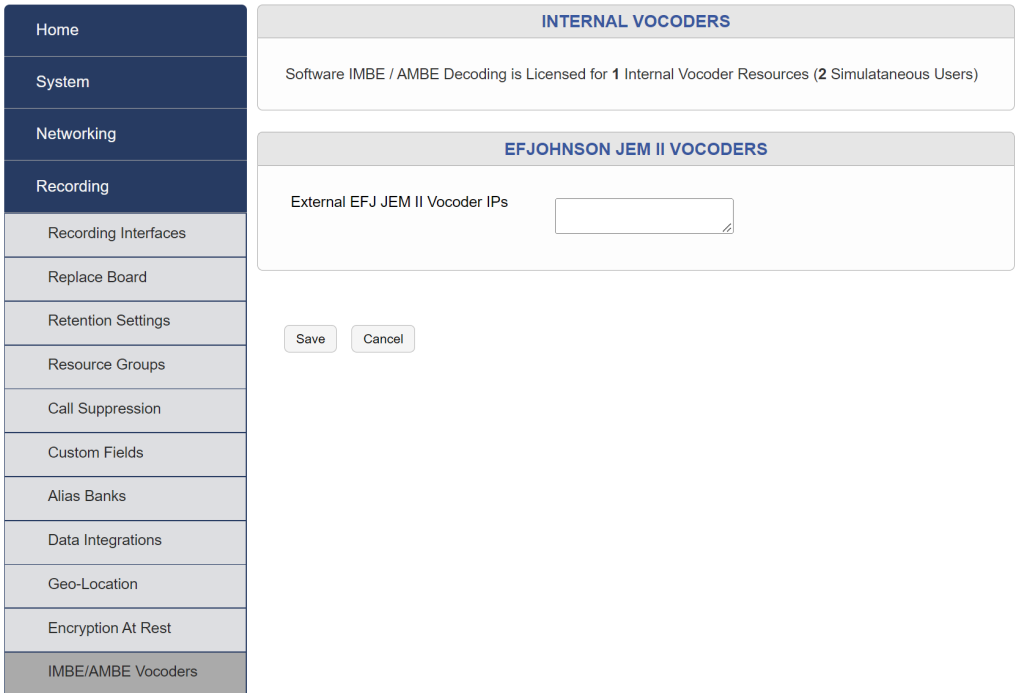


Fig. 7.61 Internal Vocoders

Once licensed, a user can transcode in MWP by playing back the calls

If you are using a JEM server vocoder for EFJohnson calls then you can configure as many as needed, one IP address per line.

> **Note**
>
> For customers using a pre-existing external DVSI Net-2000 Vocoder IP, configure as needed, one IP address per line.
>
> When internal hardware vocoders are present, it will show you how many are detected. To use this option, select the Enable box

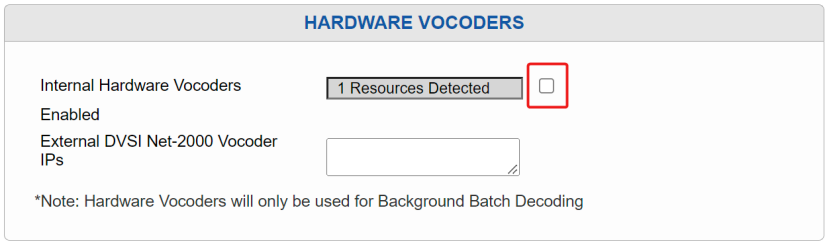


Fig. 7.62 Enable Internal Hardware

7.3.10.1. Background Batch Decocoding

> **Note**
>
> As of 2022.3, background vocoding is no longer necessary. Customers installed prior to 2022.3 can continue to use this function and will see an additional section in the UI indicating DVSI hardware vocoders.

As with previous releases, when recording P25 Audio from sources that provide audio in their native codec (IMBE or AMBE), the audio is stored on the recorder's hard drives in the same native format it was received in. When playback or export is selected from MediaWorks EXP or the front panel, the configured vocoding resources (External DVSI Net-2000 boxes, EFJohnson JEM II servers, or DVSI Vocoding hardware installed internally to the NexLog Express), are used to decode the audio on demand.

The advantage of this strategy is that AMBE and IMBE are very efficient at compressing audio, so much less disk space is needed to store the data. On the other hand, the disadvantage is that the amount of required vocoding hardware resources scales linearly with the number of users who are doing playback

or export at any one time. Exports of large numbers of files will be slow, generally no faster than 4x real time (e.g. an hour of calls will require at least 15 minutes to export.) And finally, during times when those resources are not being used, they are idle.

The Background Vocoding feature, if enabled, will use those idle resources to convert saved IMBE/AMBE calls on disk to a data format that can be played back without using the vocoding resources at playback time (G.726/16, G.726/32, and G.711 are supported). The advantage of having files pre-converted is that playback and export do not require the vocoder resources and will be just as fast as export/playback of other audio formats. The disadvantage of background vocoding, is that the data formats will require more space on disk than the native IMBE/AMBE data would have.

With the feature enabled, whenever a configured vocoding resource is idle, it will be put to work loading files from the disk, transcoding them, and then resaving them. When you go to playback/export a call, if it has already been vocoded, no vocoder resources will be required at playback and playback/export will be much faster.

The Channel Range to Decode option defaults to checking all calls on all channels, but you can configure this to only evaluate and vocode calls coming in on specific physical channel IDs. You can enter ranges with hyphens or delimit with commas; for example, if you want to decode channels `2,3,4,5,6,17,18,19`, you could enter `2-6,17-19`.

7.4. AI

7.4.1. Notifications

When a call is recorded on a given Resource Group, you can set up email or SMS notifications from the Notifications tab, to be sent to a specific group of users (e.g. Supervisors) based on conditional logic. For example, you can configure notifications to trigger based on either of the following options:

- Phrase Match
- Activity
- Metadata

These are explained in this section.

> **Note**
>
> To use transcriptions, the Notifications feature requires a Transcriptions addon license.

To set up notifications:

1. In the left navigation menu, select AI > Notifications. The Notifications configuration page opens.

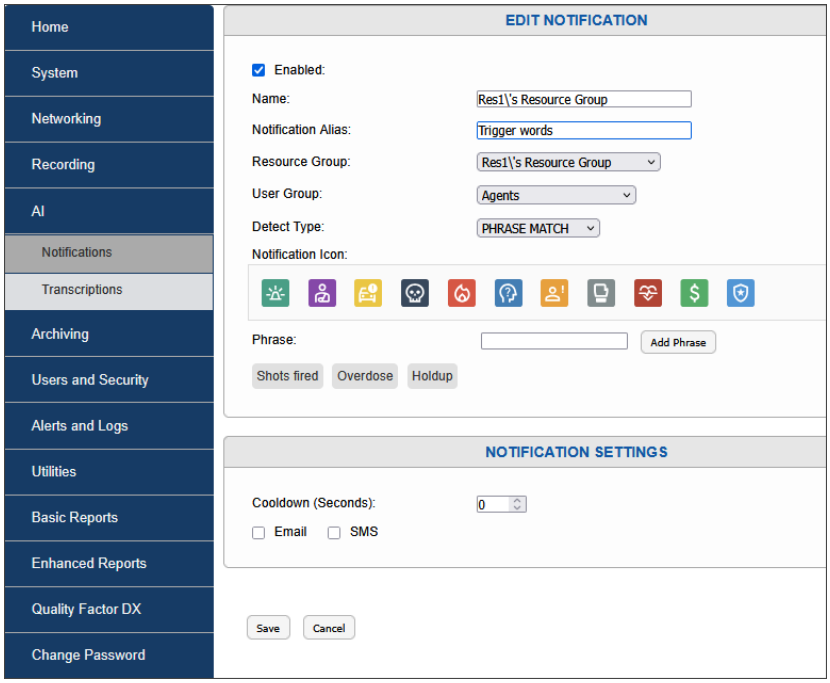


Fig. 7.63 Edit Notification Page

1. In the top Edit Notifications pane, In the Name field, enter a name for your notification.
2. Notification Alias: - not currently functional. This is intended to enable customization of notification names (future functionality).
3. Resource Group: Select the Resource Group to which the notification will be applied.
4. User Group: Select the User Group to which the notification will be sent.

5. Detect Type: In the Detect Type drop-down field, select the type of notification you want. The available notification criteria are as follows:

   - Phrase Match: – whether a pre-configured phrase is matched.
   - Activity: – refers to call activity triggered by a resource.
   - Metadata: – the type of metadata an active call contains matching a specific value.

   Phrase Match

6. In this example, select Phrase Match.

7. Select the Enabled checkbox.

8. Notification Icon: This feature is intended for future functionality and is not currently active.

9. In the Phrase Match field, type a word or short phrase, and then select the Add Phrase button. The word or phrase now displays beneath the Phrase Match field, bounded by a grey rectangle.

   For notifications to work, users must be added to a user group. All users included in that group must have an email address and cell phone number configured on the Users page.

> **Note**
>
> Email recipients will receive a notification email that contains a selectable hyperlink. However, to be able to open links in emails, users will first need to configure a Secure TLS connection. See Section 7.6.3 Encryption and TLS of this manual. In this context, users are required to specify a Fully-Qualified Domain Name (FQDN) from Networking → System Identification.

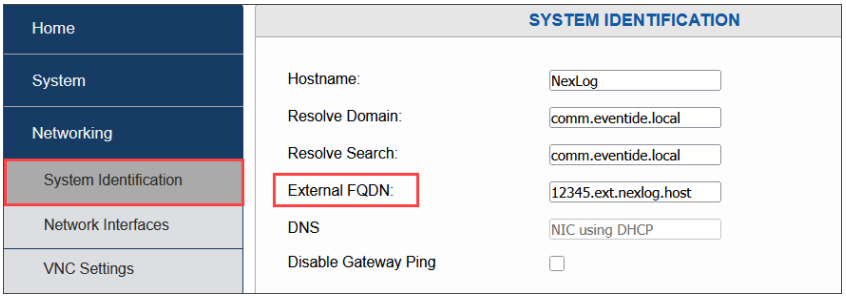


Fig. 7.64 External FQDN

10. Add additional words or phrases, as required. Beneath the Edit Notifications pane, in the Notification Settings pane, additional notification settings are available, depending on the notification type selected. If you selected Phrase Match from the Detect Type drop-down menu, the following configuration setting is displayed:

    - Cooldown (Seconds)

    Cooldown is a mechanism designed to limit the number of notifications sent to a user group. If a phrase match occurs and generates an alert from a call transcription, you can configure a time interval during which no additional notifications from additional calls that reference the same emergency incident will be sent until the cooldown period expires. This is intended to limit replication of notifications for the same incident, which would otherwise inundate notification recipients. Notifications that match a phrase are sent only once per call.

11. Select the checkbox(es) for the type of notification you want to receive, as appropriate:

    - Email
    - SMS

Fig. 7.65 Notification Settings: Cooldown

Activity

If you selected Activity in the Detect Type drop-down menu, the following additional configuration setting is displayed.

- Minimum Activity (Seconds): Refers to the minimum call duration in seconds required for a call to trigger an alert. If no minimum is specified, a single alert is triggered for each event. Use cases for this setting, for example, could be an unintentional 911 “pocket dial”, or if the caller dials and then hangs up.

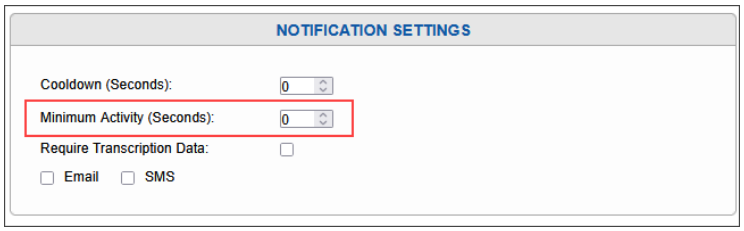


Fig. 7.66 Edit Notification: minimum activity

Metadata

The third notification type is Metadata. With this notification type, you can trigger notifications based on the type of metadata an active call contains by adding rules conditional rules. You can add as many rules as you like and group them according to the criteria you specify.

The following example illustrates how this works:

Example:

12. From the Type drop-down menu, select METADATA. The Metadata Rules field is now displayed.

Fig. 7.67 Metadata Notification Type

13. From the Select Metadata Field drop-down menu, select the metadata type you want from the list. In this example, AGENT_ID is selected.

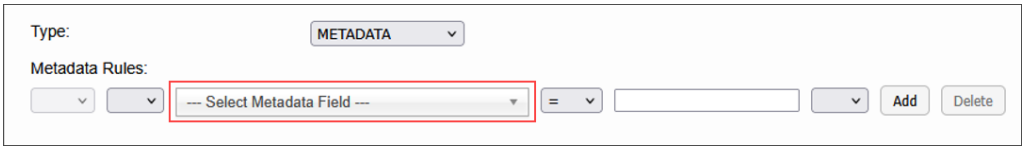


Fig. 7.68 Select Metadata Field

14. In the Comparison Operator drop-down menu to the right, select the operator you want, in this example, the “=” sign.

Fig. 7.69 Select Logical Operator

15. Enter a value for the AGENT_NAME, in this case, 'JDoe'.

Fig. 7.70 Notification Type Value

16. To add another condition, select the Add button. A new Metadata Rules field appears.

    In this use case, suppose we want to group two conditions together such that both conditions must be satisfied.

Fig. 7.71 Notification Type Value

17. From the Logical Operator drop-down menu on the left, select AND.

18. Select the metadata field you want, in this example, CALLTYPE.

Fig. 7.72 New Condition Added

19. Select the comparison operator you want, in this example, the "=" sign.

20. Enter a value of "Medical".

    For the purposes of metadata filtering, you can group together conditions that you have created by using AND/OR operations, for example, (a AND b), or (b OR c).

Now that a second condition has been added, you can now group them together, starting with the first condition.

To group conditional rules together:

1. Return to the first line, and in the drop-down menu to the immediate left of AGENT_ID select the single left parenthesis.

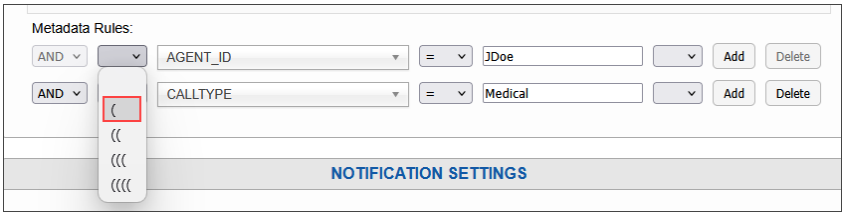


Fig. 7.73 Grouping Rules: Left Parenthesis

1. Finally, on the second line, from the right parenthesis drop-down menu to the right of the value “Medical”, select the single right parenthesis.

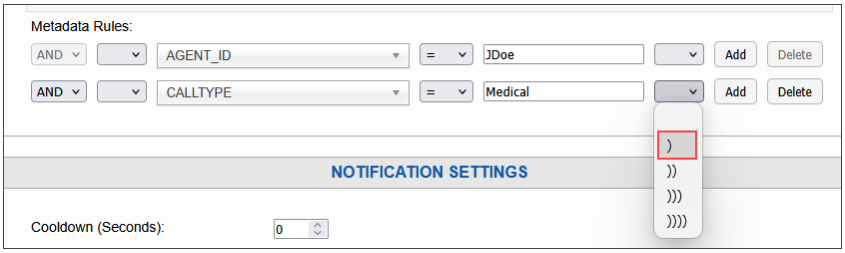


Fig. 7.74 Grouping Rules: Right Parenthesis

The two conditions are now grouped together. You can add or delete as many rules, as you like, based on the metadata in the call.

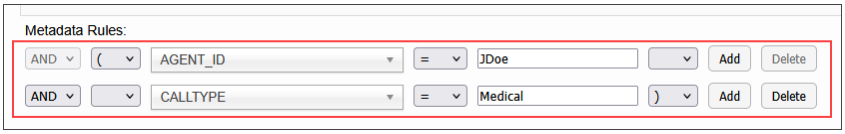


Fig. 7.75 Grouped Conditions

21. Select Save to save your changes. You will now receive notifications for any calls where these conditional rules are satisfied.

You can create nested rules of greater or varying complexity using up to four levels of parentheses. Creation of more complex examples is beyond the scope of this document.

> **Note**
>
> If you have created metadata rules but navigate away to select a different notification type before saving your metadata rules, your rules will not be saved.

7.5. Archiving

In addition to the online storage that NexLog Express provides for recordings on its hard drives (Storage Devices), the system can also archive recordings externally.

An archive is a portable USB drive, or network location onto which calls be archived for back up purposes.

7.5.1. Archives

Archives provide a way to store recordings long-term that will end up deleted from the system's internal storage due to retention settings and/or disk space availability. The NexLog Express archives page allows you to view the status of and perform actions on your archive drives.

NexLog Express supports two types of Archive Drives.

- Network
- Portable

Network

These archive types are not physically connected to the recorder, the recorder has no way to automatically detect these. They must be manually added to the recorder via the Archive

Configuration page. These archive drives include Network Attached Storage (NAS) Devices connected via SMB or NFS.

Portable

This archive type is physically connected and disconnected dynamically to the recorder, for example, external USB hard drives or USB flash drives. These archive drives will only show up on the setup page when they are physically connected to the recorder.

At the top of the Archives Page, is a list of all the current Archive Drives in the system. To the left is the archive drive name, consisting of the drive type and the number of the drive on the system. Next is a box showing the current status of the drive as well as a status bar giving a quick at-a-glance indication of how full the drive is.

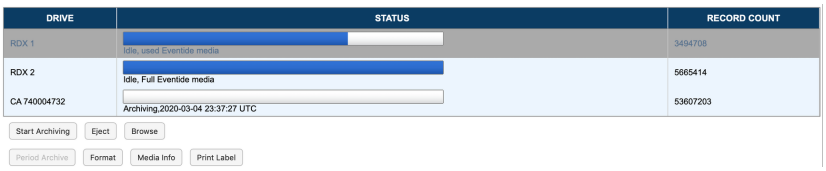


Fig. 7.76 Archive Display in Configuration Manager

Note that this display is redundant when using the Front Panel locally. The Info screen has a similar implementation with the same functionality.

To the right of the status indication is a count of how many calls are currently archived to the archive drive. If the drive is one that supports removable media, the number of calls on the currently inserted media is displayed. To perform an action on an archive drive, you must first click the drive to select the one you wish to take action on, and then click the action button below which corresponds to the action you wish to perform. Actions that are not applicable to the currently selected archive drive, due either to the drive type or to the status of the drive, will be grayed out.

The available actions are:

Start Archiving

Enable archiving to the selected drive. Call Records will begin transferring to the archive oldest-first beginning at the timestamp indicated by the current archive pointer for that drive (see Section 7.5.2 Archive Configuration). Call Records that meet the criteria for archiving to this drive will continue transferring one at a time until archiving is stopped (either manually or due to a condition set under 'Configure'), the drive fills up or another exception occurs (such as an error writing to the media). Once the archive pointer catches up to the current time, calls that meet the configured archive criteria will be transferred as they are recorded.

Stop Archiving

Stops archiving to the selected drive. Call Records will cease transferring until archiving is started again.

Eject

For a portable archive drive, such as a USB Drive, this action will render the drive safe to be unplugged without the risk of losing or corrupting data on the drive.

Browse

This loads the current archive for browsing and playback from both the Front Panel and MediaWorks EXP. When an archive drive is in browse mode, new calls cannot be archived to it until it is first taken out of browse mode.

Period Archive

Period archive allows you to manually archive a time range to an archive. It also allows you optionally select only protected media to be archived. Media must be formatted without any calls on it before period archiving can be used.

Format

For archive types that can be formatted by the recorder, this action will perform a format. Formatting the media will delete all existing data currently stored on the drive, whether it is an existing NexLog Express Archive, or data belonging to some other device or operation system. Always double-check the media before you format it.

Media Info

Displays additional information about the media currently inserted into the drive.

7.5.2. Archive Configuration

This section has the same basic display as “Archiving: Archives” but has different control buttons:

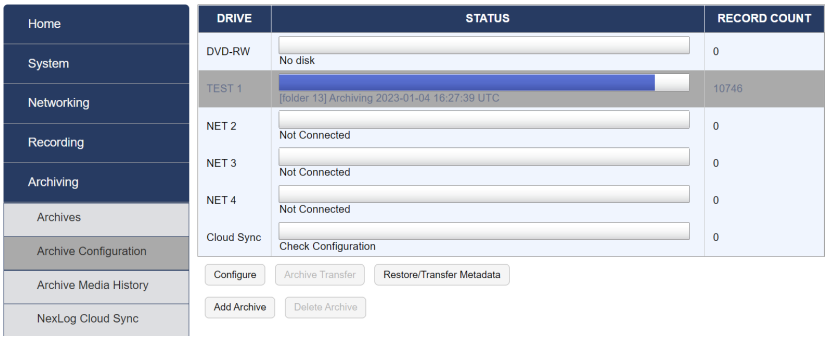


Fig. 7.77 Archive Configuration

Add Archive

Archive drives that connect to the recorder via networking must first be added to the recorder so that they show up as selectable drives on the Setup Archives page. Once added, they can then be configured using the ‘Configure’ button. As will all archive drives, the recorder must also have the correct license keys installed to be able to access the archive drives. After clicking this button, you must select which type of addable archive drive to add to the system. The options are NAS (Network Attached Storage, Windows SMB) or NFS (Network File System),which are also sometimes known as ‘Network Shares’. You will be able to configure archive parameters specific to

the archive here, these options are identical to the ones provided under ‘Configure Archive’ and are described below.

NexLog Express Recorders can be configured with one NAS or NFS archive, total, for free; configuring more than one requires an additional add-on license.

Delete Archive

Archive drives that have been previously added can be deleted via this button. Physical drives can not be deleted, only ejected.

Archive Transfer

If you insert previously-recorded archive media into a drive, this button can be used to perform a restore operation, i.e., copy the calls from that medium back to RAID. Several checks are performed before transferring the data:

- Does the serial number of the recorder that recorded the archive medium agree with that of the destination recorder?
- Are the channel names of the recorder the same as the destination?
- Does the format of the data on the archive conform to that of the destination?
- Is there any problem with or damage to the archive medium to be transferred?
- Are all (or some) of these calls duplicates of calls already on the recorder?

If none of these are appropriate for the medium, or if you indicated that you wish to proceed, the archive transfer will commence. All drives operate independently. You can restore archive media in all available drives, or you can even record archives on one medium while restoring from another.

Important

The restoration process cannot continue once the RAID is full, so unless you have a special reason for doing otherwise, always restore from the most recent archive backwards.

If you are restoring archives after a new installation, use the Set Archive Time facility to make sure that new archives are only recorded from the present forward. If you don't set this and begin new archiving after you have restored your archives from a previous installation, you might find yourself "re-archiving" the restored archives.

Restore/Transfer Metadata

Metadata archives contain just the metadata for calls on a system; this is a way to archive any notes, annotations, etc, that are applied after a recording is made. In the case of a system failure, restoring from an archive made at recording time will be missing any metadata added afterwards; restoring metadata will update the metadata on these calls to include what was present at the time metadata was archived. To create metadata archives, use the Backup User Edited Metadata feature of Schedules, discussed below under Utilities.

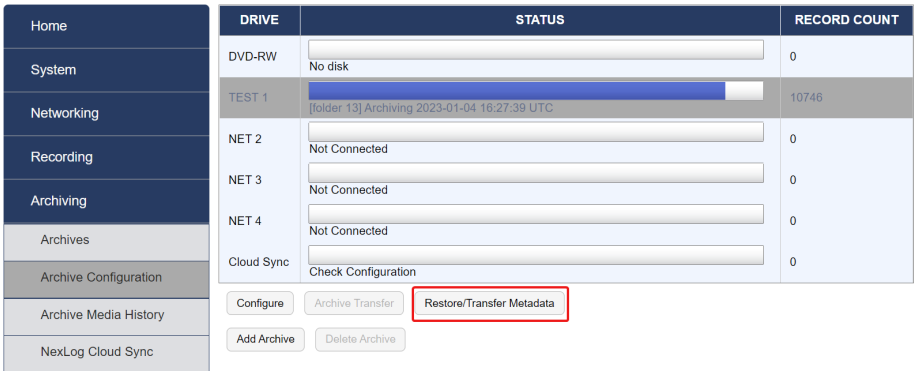


Fig. 7.78 Restore/Transfer Metadata

Configure

This screen allows you to configure your archiving drive. Once you've selected a specific archive on the Archive Configuration page, click "Configure" to access Settings, Time, Groups, Tracking, and NAS options.

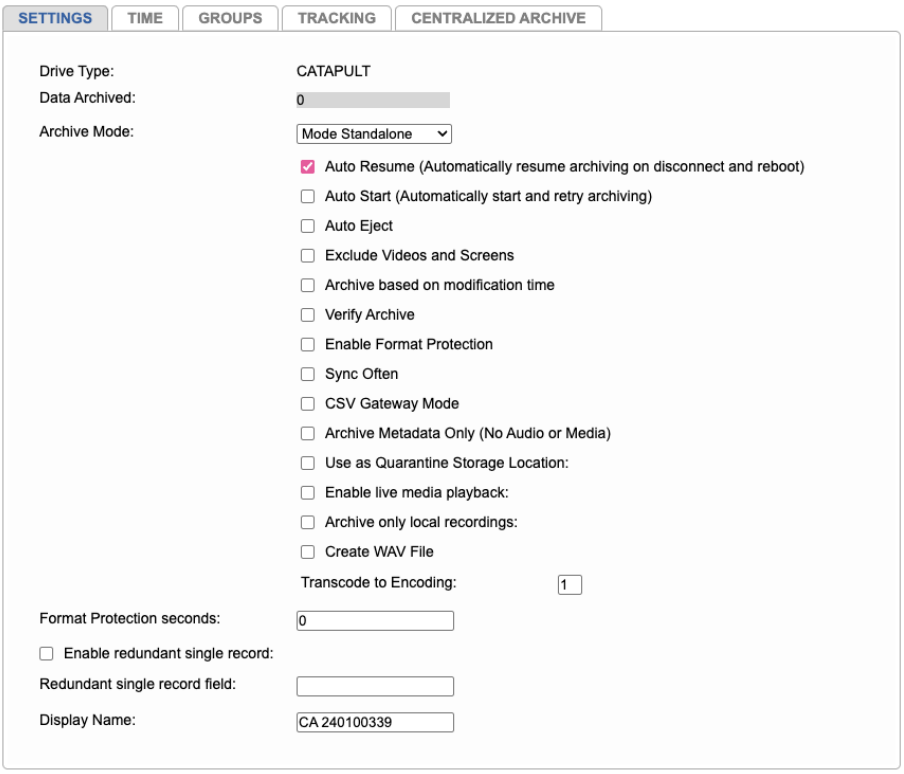


Fig. 7.79 Archive Display in Configuration Manager

7.5.2.1. Settings

Drive Type

The type of drive.

Data Archived

The amount of data archived since install. This number is in Bytes.

Archive Modes

Sequential

(Default) In this mode, archiving will automatically move on to the next available medium when current drive in use is full, continuing on to each available drive in order from top to bottom. This method also supports double sided disks and will continue in a similar manner once all drives have been used, returning back to the top to continue archiving on side B. (requires manually flipping the disk)

Parallel

In this mode, archiving will record to all available drives simultaneously capturing the same data, providing redundancy.

Standalone

Drive acts independently, writing on entire drive then stopping. This is the default setting for USB and network drives.

Period

When selected, blank drive will write specific time range to archive. This is triggered by selecting “Period Archiving” from Archive page.

Auto Resume

When enabled, a recorder that is turned off while archiving will resume archiving from the same spot once the recorder is restarted. This setting also applies to Network Archives after a network disconnect.

Auto Start

When enabled, archiving will begin automatically whenever the drive is in a state where archiving is available. Auto start will not archive when there is no media, media is full or damamged, a drive is in browse mode, or when another drive is currently archiving.

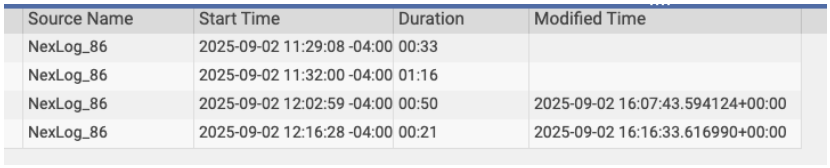
> **Note**
>
> It may be necessary to disable Auto Start option to eject or browse a drive while partially full.

Exclude Screens and Videos

This will exclude archiving of all screen and video recordings.

Archive Based on Modification Time

Use this setting to make sure that any metadata changes to archived calls will also get archived. When enabled, the field “Modified Time” is added to the recorder and appears in MediaWorks EXP. The “Modified Time” field is updated whenever a call’s metadata is altered, such as when a note is added to an already recorded call.



Source Name	Start Time	Duration	Modified Time
NexLog_86	2025-09-02 11:29:08 -04:00	00:33	
NexLog_86	2025-09-02 11:32:00 -04:00	01:16	
NexLog_86	2025-09-02 12:02:59 -04:00	00:50	2025-09-02 16:07:43.594124+00:00
NexLog_86	2025-09-02 12:16:28 -04:00	00:21	2025-09-02 16:16:33.616990+00:00

Fig. 7.80 Modified Time Field in MediaWorks DX

> **Note**
>
> This setting assigns modified time values only to calls that are recorded or modified after the setting is enabled in the Configuration Manager. Only these calls will be eligible for archiving.
>
> For example, if Call A was recorded before this setting was enabled and has not had any metadata changes, it would not be archived. However, if Call B was also recorded before this setting was enabled but had metadata changes after the setting was enabled, the call would be archived.

When using period archiving or the “Set Archive Time” configuration option, calls with a modified time within that period will get archived even if their start times fall outside the set time range. In other words, the modified time of a recording takes precedence over its start time when archiving based on modification time.

Verify Archive

When using optical media, filesystem check will run after finishing a write operation.

Enable Format Protection

Protects the media from being accidentally formatted until the time on the recorder is greater than the oldest call on the media plus the configured protection seconds. Note that this option only prevents you from formatting the media on the NexLog Express recorder, it does not protect against placing the media in a PC and formatting it there.

Sync Often

When enabled, writes out data regularly in order to reduce length of time needed to archive to prevent writing delays on shutdown.

CSV Gateway Mode

Saves data to PC which includes call info in a CSV file.

Archive Without Media (audio)

This option allows you to archive only the recording and metadata databases.

Archive only local recordings

When enabled, the recorder will only archive calls that were originally recorded on it.

Create WAV File

This option will include an 8-bit, 8.0khz WAV file of each call, playable directly from the disc in any computer able to read the archive media. This will of course reduce the number of calls that fit on a given disc as it consumes more space than just the native encoding.

Transcode to Encoding

When “Create WAV File” is enabled, The output format is determined by the encoding setting; 0 - raw pcm 1 - mu-law

Format Protection seconds

Works in conjunction with “Enable Format Protection” to add additional buffer time before formatting.

Display Name

Changes the Name of the Archive being configured.

7.5.2.2. Time

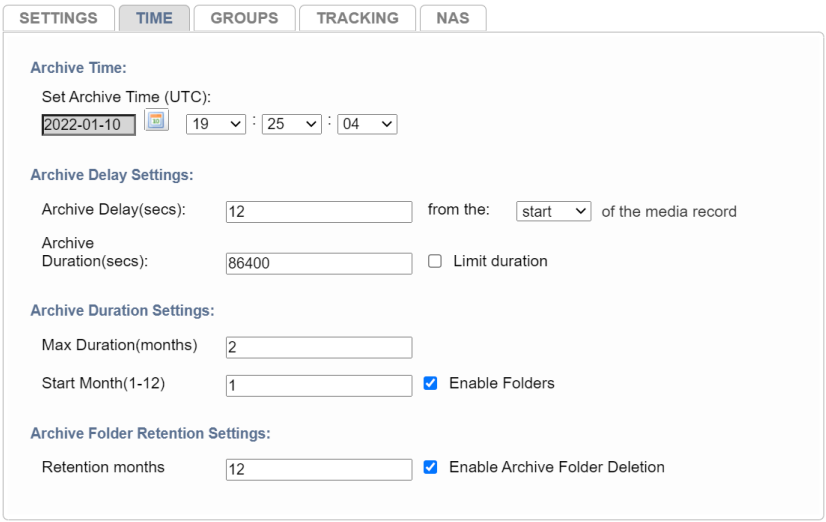


Fig. 7.81 Time Configuration

Set Archive Time

Allows you to set the current archive pointer.

When you start archiving, the first call to be archived is determined by an internal archive pointer. This pointer tracks where you left off archiving with the previous disk so that the next disk will begin where the previous one left off. Also, if you are in the middle of a disk and you stop archiving, for whatever reason, such as the need to browse calls on the disk, you can resume archiving at the point where you left off. The goal is to ensure that only consecutive calls are recorded on each disk, making labeling and searching easier. This pointer is maintained automatically.

However, there are times when you may want to manually set the current pointer location. For example, you may have misplaced an archive disk and you want to re-archive calls. Of course, to do so the calls must still be present on the RAID.

To manually set the current archive time, select a date and time using the calendar control and save the form. The next time you start archiving, the calls on your RAID closest to the new archive time setting will be archived first.

When you have completed recording a medium whose starting time you have selected with the Set Archive Time feature, the time pointer is set to the time of the end of the medium just recorded. It is NOT set to the end of other data that may have been archived. Sometimes this is desired behavior, such as when you want to record more data than what's able to fit on a single medium from the starting time you set. Sometimes it may not be, such as when you want to continue archiving from the end of the last medium you recorded in the normal sequence. If the second is your requirement, you can note the desired time and reset the archive pointer to this time. If you failed to make a note, you can take the most recent archive medium, read the "Media info" for that disk, and set the pointer to that time.

Important

As noted in the display, the Archive time is set in UTC time. If you are setting the archive time to start at the end of a previously recorded archive medium, you will probably use the “Media Info” feature to check on the end time of that medium. The recorder displays “Media Info” in UTC since the archives are portable and must be compatible over time zones and different playback hardware. To dovetail the recorded and new archive times, you must convert your local time to UTC for this setting.

Archive Delay

How long (in seconds) to archive behind the recorder’s current time.

Archive Duration

Max Duration (months)

When enabled, this setting dictates how many months will be saved to each folder.

Start Month (1-12)

Which month you choose to start archiving with (1=Jan, 2=Feb, etc)

- Example: If a user wants to set up a library of archives for each year, they would set the start month to 1 and the max duration to 12. In this manner, an archive started in March would run for the rest of the year and start a new archive folder in Jan.

Archive Folder Retention

When retention is enabled, NexLog Express will automatically archive and maintain the amount of months selected while overwriting the oldest information.

> **Note**
>
> The main purpose of this feature is to have an uninterrupted archiving process with a fixed timeline in order easily maintain the standards of your company's file retention policy and protocol.

7.5.2.3. Groups

Groups allow you to set up archiving for specific channels or a collection of channels called "Groups"

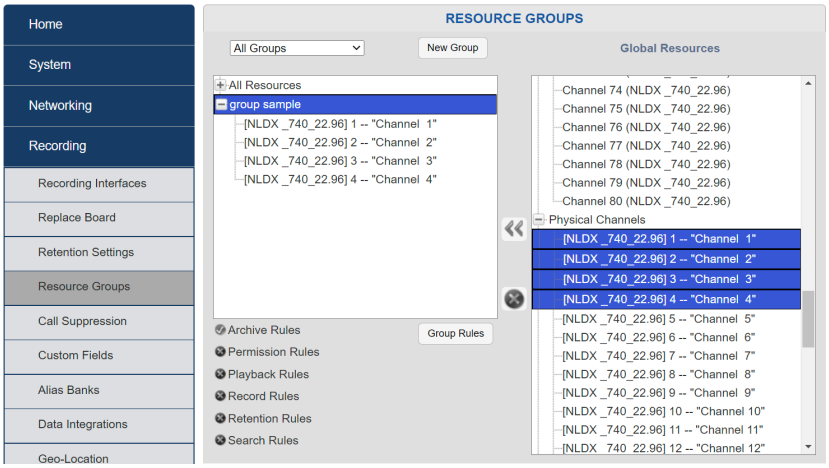


Fig. 7.82 New Channel Group

In order to create a Channel Group, you'll first need to make a new Group in the "Recording/Resource Groups" section. Start by creating a "New Group", then choose the channels from the Global resources on the right that you wish to archive, and drag/drop them into the new group.

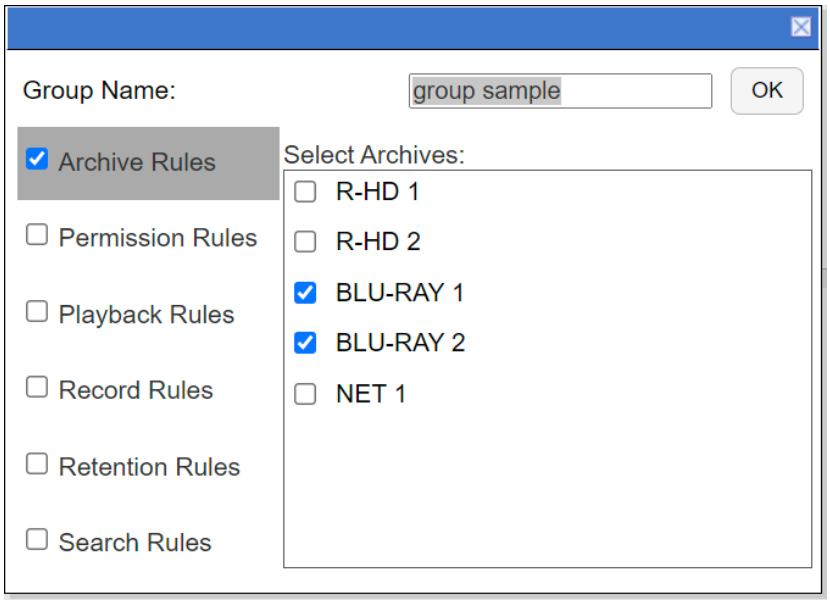


Fig. 7.83 New Group Rules

Once you have all selected channels in your group, you will select “Group Rules” to name your Channel Group, choose the drives you’d like to archive to, and enable “Archive Rules”.

Fig. 7.84 Use Channel Group

Next, simply navigate back to “Archive Configuration”, choose a drive to configure, and select the “Groups” tab to enable this feature and select the Channel Group that you’d like to archive.

7.5.2.4. Tracking

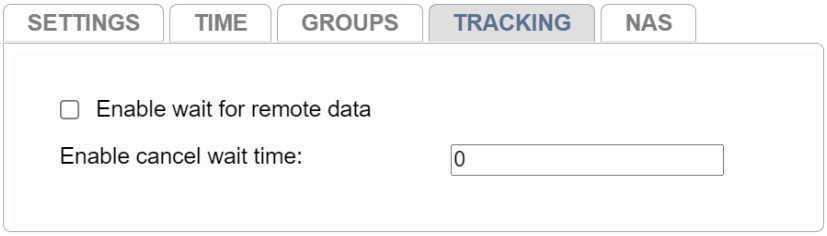


Fig. 7.85 Tracking Configuration

Tracking is an option that prevents calls from being left out of archives. Because of the inherent nature of the technology involved, recorders do not always receive calls from VoIP, Screen Capture and Centralized Archiving sources in real-time. They can, under certain conditions, end up receiving calls hours or even days after they were originally recorded. This can have a significant impact on archiving.

Take the following scenario for example:

- A busy NexLog Express Recorder with both local input board sources and screen channels.
- The archive pointer on a Blu-ray drive is set to current time.
- Calls are currently coming in on the local input channels.
- Due to temporary but severe network congestion, a screen capture client has buffered an hour's worth of calls, which is just now transferring to the NexLog Express Recorder.

In the above scenario, archiving calls to this Blu-ray drive would leave the hour of screen calls unarchived. To avoid this, use Enable wait for remote data function to prevent archive from writing until the screen system is fully synced and ready to archive in full.

Tracking is an option that prevents calls from being left out of archives. Because of the inherent nature of the technology involved, recorders do not always receive calls from VoIP sources in real-time. They can, under certain conditions, end up receiving calls hours or even days after they were originally recorded. This can have a significant impact on archiving.

Note

This feature is optional to accomodate continued archiving when a Call Source is temporarily offline. In this case, turn off option, create the archive you need, then enable and reset the archive time.

7.5.2.5. Network Archive Storage (NAS) Configuration

The recorder can not only archive its own internal drives and removable media, but it's also able to archive using a standard Microsoft Windows Network Attached Storage (NAS).

- Using more than one NAS on a recorder requires an Add-On License

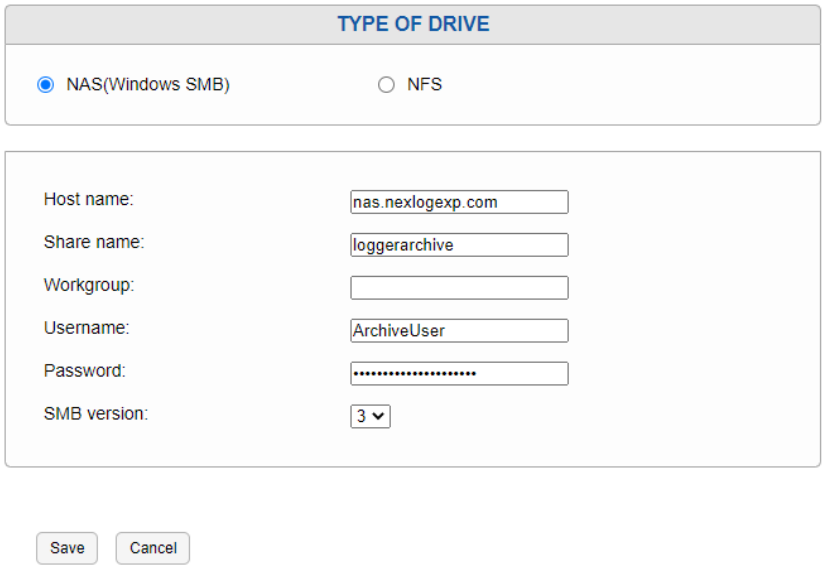


Fig. 7.86 Adding a NAS (Windows SMB) Network Archive

Hostname

The NETBIOS or DNS name of the server where the archives will be stored. This server must be a Microsoft Windows server or other system that emulates Microsoft Windows file sharing.

Share Name

The name of the share on the server where the archives will be stored. Microsoft Windows syntax for specifying a network location is:

```
\\Hostname\Sharename
```

For example, if your network administrator has specified that the recorder archives can be stored at

`\\BigServer\RecorderArchives`

The NAS Hostname should be configured as `BigServer` and the Share Name should be configured as `RecorderArchives`.

Workgroup

The Workgroup or Domain of the server where archives will be stored.

Username

A valid username that has been granted read/write access to the hostname and share name where the archives will be stored.

Password

The Password associated with the Username on the Microsoft Windows server.

SMB version

Option to set SMB based on your network settings.

> **Note**
>
> For more details on NAS storage and Incident Evaluation Sharing/Restoring, see Appendix E Incident Evaluation Restore

7.5.2.6. Centralized Archive Configuration

Centralized Archiving (CA) allows you to set up an archive drive that directs calls from one NexLog DX-Series recorder to another.

There are three main uses for Centralized Archiving:

- Central Pooling: Combine calls from multiple recorders into a single “central” recorder, allowing all recordings to be accessed in one place. Typically, these are then archived to a NAS drive, consolidating recordings from all site recorders.
- Redundancy: Ensure continuity by linking all site recorders to each other. If one recorder fails, others retain all calls up to that point. Each recorder can also archive to its own NAS, enhancing redundancy and access.
- Multi-Site Access: Enable users at different locations to access recordings from any recorder across distributed sites, provided network permissions allow connectivity between recorders.

By default, Centralized Archiving copies recordings as they occur from one recorder to another.

To prevent unintended loops where recordings continuously cycle between recorders, configure each drive to use the Archive only local recordings setting (See Section 7.5.2.1 Settings). This ensures only recordings originally recorded on the local system will get archived to the destination recorder.

For archiving to non-recorder destinations like NAS from ‘*Recorder A*’, leave the “Archive only local recordings” setting in the default off state on the NAS drive. This setup allows ‘*Recorder A*’ to send all recordings to the NAS independently, supporting multiple redundant archives.

Use Configuration Manager under Archiving –> Archive Configuration to adjust settings for each drive.

> **Note**
>
> Settings are configured individually for each drive, rather than applied globally across all drives.
>
> These settings are also applicable to the standard archive configurations, but are particularly beneficial when utilized with Centralized Archiving.

7.5.3. Archive Media History

The Archive Media History displays a history of all of the different archive media that have been inserted into the recorder. Archive Media will show up in this list regardless of whether or not they have actually been written to. Archives which are inserted into the recorder only for browsing and playback will also show up in this list.

If the list spans multiple pages of output, use the 'Next' and "'Prev' buttons on the bottom of the page to navigate through the list. Alternatively, you can alter the page number in the "page" box and press the "Go" button. Note that if an archive drive in the case of drives without removable media, or a media disk in the case of drives with removable media will gain a separate entry in this table for each time they were formatted and used.

Therefore, if you archive Jan-Mar on a Blu-Ray disc, then reformat it, and then archive Apr-Jun, you will have two entries for that disk in the archive media history, one for the first date range showing that the archive has been deleted, and one for the new date range.

The fields displayed for each archive media history entry are as follows:

- Recorder Serial: The serial number of the recorder on which the archive was written. This will be zero if created on the recorder you are logged into. It would only be nonzero in the case of an archive written on a different recorder and then inserted into this recorder for browsing and playback.
- Format Time: The Date and Time upon which the archive drive, or current archive media, was formatted.
- Start Time: The Date and time of the oldest call contained on the archive media.
- End Time: The Date and Time of the latest call contained on the archive media.
- Call Count: The number of calls archived to the archive media.
- Status: The current status of the archive media. The possibilities are:
  - DELETED: This media has since been reformatted on the recorder, and this archive is no longer available. Note that if an archive media is formatted on a different system or physically destroyed, the calls will also no longer be available, but this status will not be reflected in the recorder's archive media history
  - PARTIAL: Archive was started but not completed.
- Drive Type: The type of archive drive (e.g. BLU-RAY, USB Drive, NAS, etc.)
- Last Archive Time: The most recent time that archiving was started on this archive media.

7.6. Users and Security

All access to NexLog Express clients and features is predicated on having a user account with appropriate permissions to those clients and features. One must log in to play back recordings, archive, or configure channels, for example.

Admin accounts have access to all NexLog Express functionality and options. All other users will only be able to access aspects of the system as their permissions dictate. Permissions can be assigned directly to

user accounts, or permissions can be assigned to User Groups, which in turn will apply to all users in those user group. (See Section 7.6.4: User Groups and Section 7.6.1.4: Permissions).

7.6.1. Users

The Users page allows the creation and maintenance of user accounts on the recorder. It displays a table showing each user currently configured on the system.

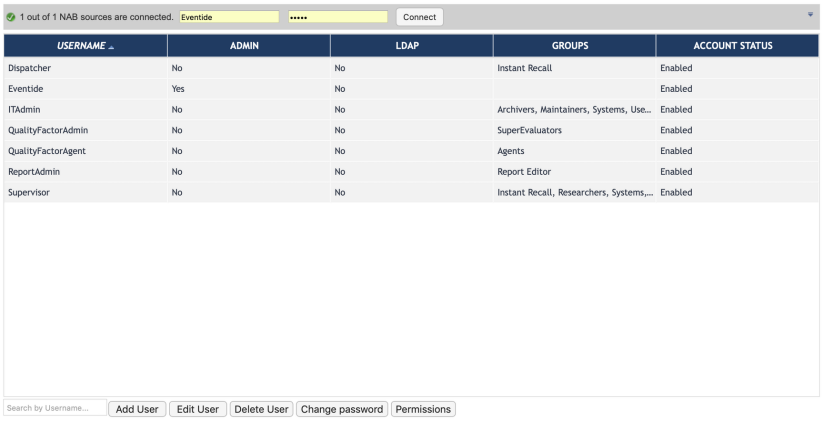


Fig. 7.87 User Configuration

This table can be sorted by clicking in the header on the column you want to sort by; the width of the columns is also adjustable. The columns shown are:

Username: The name the user will use to log into the system.

Admin: An indication of whether the user is an Administrator.

LDAP: An indication of whether the user is part of Active Directory LDAP server, or local to the recorder. If you have not configured Active Directory all users will display “No.”

Groups: A list of the user groups that this user is assigned to. If the user is a member of many groups only the first few will be displayed.

Below the main users table are several action buttons. All but the “Add User” button first require a user to be selected in the user table and they take effect on the selected User. The buttons are Add User, Edit User, Delete User, Change Password and Permissions. Delete User and Change Password can be applied to multiple users at once if you select more than one from the list with Shift+Click or Ctrl+Click.

The Search by Username… field is useful on systems with a lot of users; it will limit the displayed users to those containing the characters entered. For example, if you put “d” in the field in the figure above, it would show only DSigal and Eventide; if you put “b”, BBellerue & LBertucci.

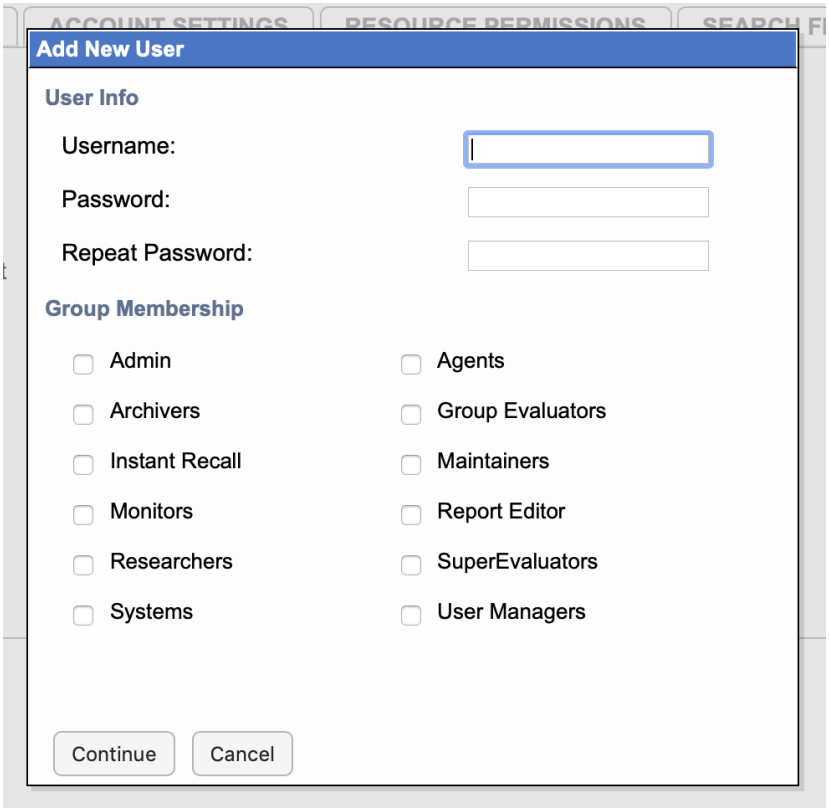


Fig. 7.88 Add New User Pop Up

7.6.1.1. Add User and Edit User

Add User will open a blank user to configure, starting with Add New User overlay that requires the entry of the most important information about a user account: Username, Password and Security Group.

Edit User brings up the same page, without the Add New User overlay, with the information and settings for the selected user. One difference between the ‘Add User’ page’ and ‘Edit User’ page, is that when adding a user, the ‘Username’ parameter is editable, whereas it cannot be changed when editing an existing user.

No options changed on any of these tabs will take effect until the ‘Save’ button at the bottom of the page is clicked, except for Resource Permissions and Search Filters which update in real time.

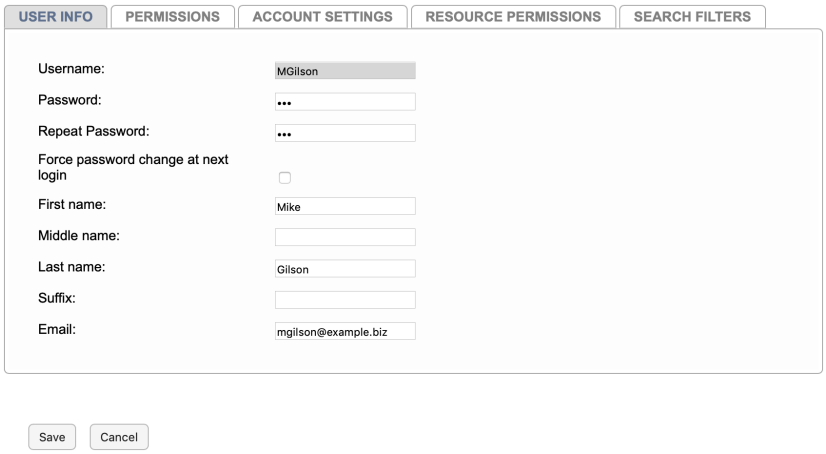


Fig. 7.89 Editing a User

The available parameters are described below:

7.6.1.1.1. User Info

Username: The name of the user being edited or added. The username of existing users cannot be changed. If you wish to change the name of a user, the user entry can be duplicated by right-clicking on the user and selecting Duplicate User, which will let you create a new user with the same settings.

Force password change at next login: If checked, the user will be forced to change their password the first time they log into the system. This can be used in conjunction with the Change Password option to allow someone to reset another user's password if they have forgotten what they set it to.

First Name: The user's first name

Middle Name: The user's middle name

Last Name: The user's last name

Suffix: The user's full name suffix (e.g., Jr.) if any

Email: The address associated with this user account. The primary purpose of the email parameter is that Users with Administrator access are emailed copies of any recorder alerts that are configured to send email. A valid email address also allows users to communicate on evaluations in Quality Factor.

7.6.1.1.2. User Permissions

Security

This control provides a check box for each user group configured for the system. By default, these groups are:

- Admin
- Agents
- Archivers
- Group Evaluators
- Instant Recall
- Maintainers
- Monitors
- Report Editor
- Researchers
- SuperEvaluators
- Systems

Checking the box makes the user a member of that group, and the user will inherit all permissions which that group provides. Except for 'Admin' (which is a hard-coded internal group name providing Administrator access) all the user groups on the system and what permissions they entail can be edited using the System: User Groups and System: Permissions NexLog Express Configuration Manager pages. Check a box to add the user to that group, or uncheck to remove the user from that group.

Table 7.1 Default Security Group Privileges at the System Console

Security Group	Privileges
Admin	All available privileges, including the ability to create new users, and receive emailed alerts.
Archiver	Ability to archive calls (INFO screen only).
Maintenance	Ability to change system settings (SETUP screen only).
Monitor	Ability to monitor live calls (INFO screen only).
Researcher	Browse and play back recorded calls (RECALL screen only).

Table 7.2 Default Security Group Privileges in NexLog Express Clients

Security Group	Privileges
Admin	All available privileges, including the ability to create new users, and receive emailed alerts.
Archiver	No access.
Evaluator	Evaluations Tab. Usually paired with Researcher group.
SuperEvaluator	Evaluations Tab. Usually paired with Researcher group.
Maintenance	No access.
Monitor	Ability to monitor live calls (Channels tab only).
Researcher	Browse, play and export recorded calls (Browse, Search, Incidents, Live Monitor).

More information about User Groups can be found below in the User Groups and Permissions sections.

Archive Drive Maintenance Access

This affects which drives a user can access at the front panel.

ROD Channels

This field uses the same formatting as the Channel IDs parameter above and determines what if any channels the user will be allowed to perform “Record On Demand” on. If the user has permission, they will be able to temporarily disable recording on the channels they have this permission on.

Instant Recall Replay Limit

On the System Console and the MediaWorks EXP and MediaAgent EXP clients, users have access to an Instant Recall functionality in which they can view the most recent calls on the recorder. Settings allow users can select which channels along with the amount of time they want to recall.

> **Note**
>
> Instant Recall user credentials can be used for Headless View in MediaWorks EXP

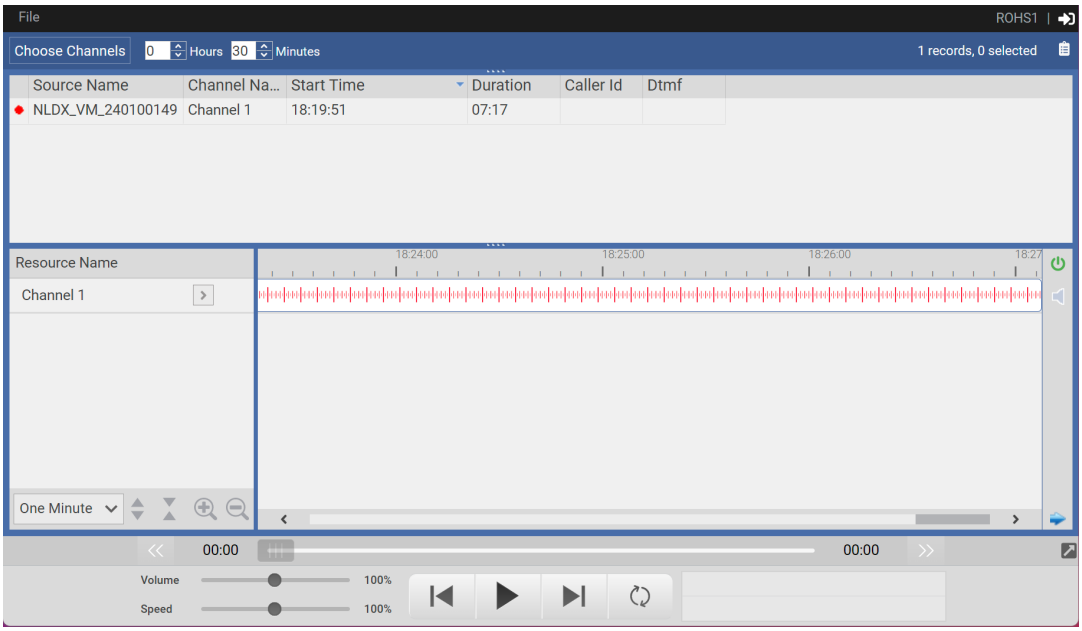


Fig. 7.90 Headless MediaWorks EXP Display

Restrict to user tagged recordings on Instant Recall tab

If this checkbox is selected, then when viewing the Instant Recall tab, users will only be able to view and play call records that have a metadata field called USER_ID which contains their username. For this setting to have any value, you must also create the USER_ID column in “Recording: Custom Fields” and provide USER_ID information to the field, either by manually placing User_IDs in individual calls using MediaWorks EXP, by configuring the “Quality Factor: Agent Mapping” section for Call Taker tracking, using “Windows User Tracker”, or by a custom integration. This does not apply to other tabs of MWP.

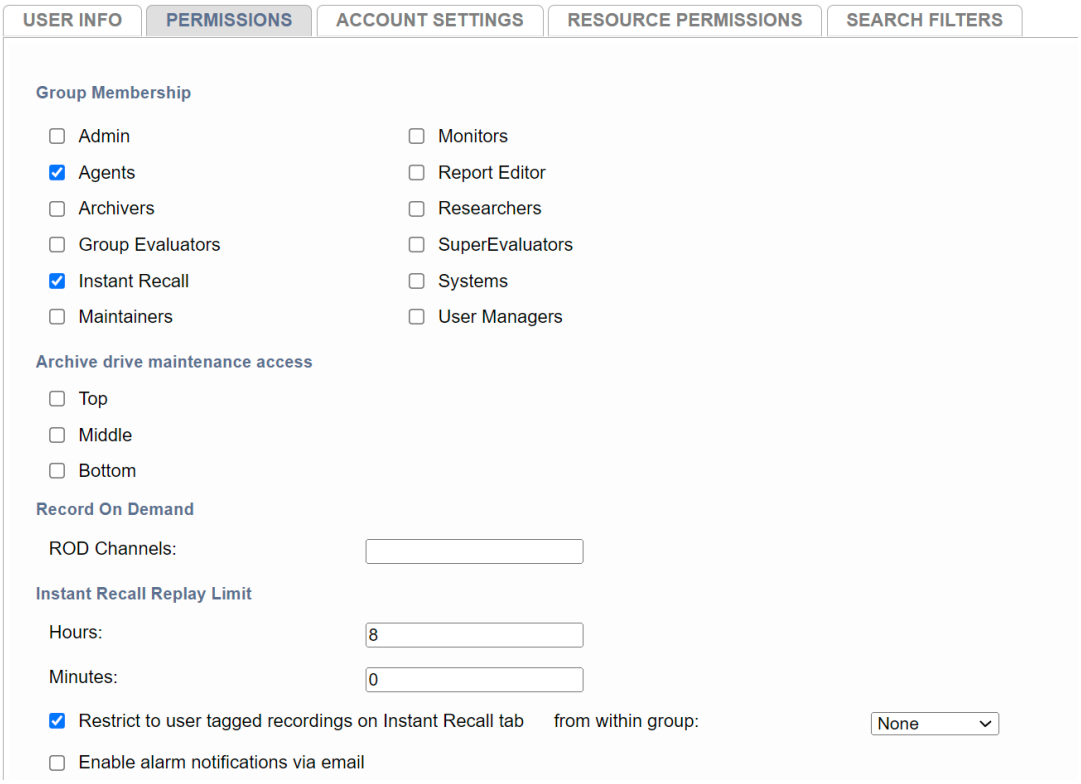


Fig. 7.91 Restrict to user tagged recordings

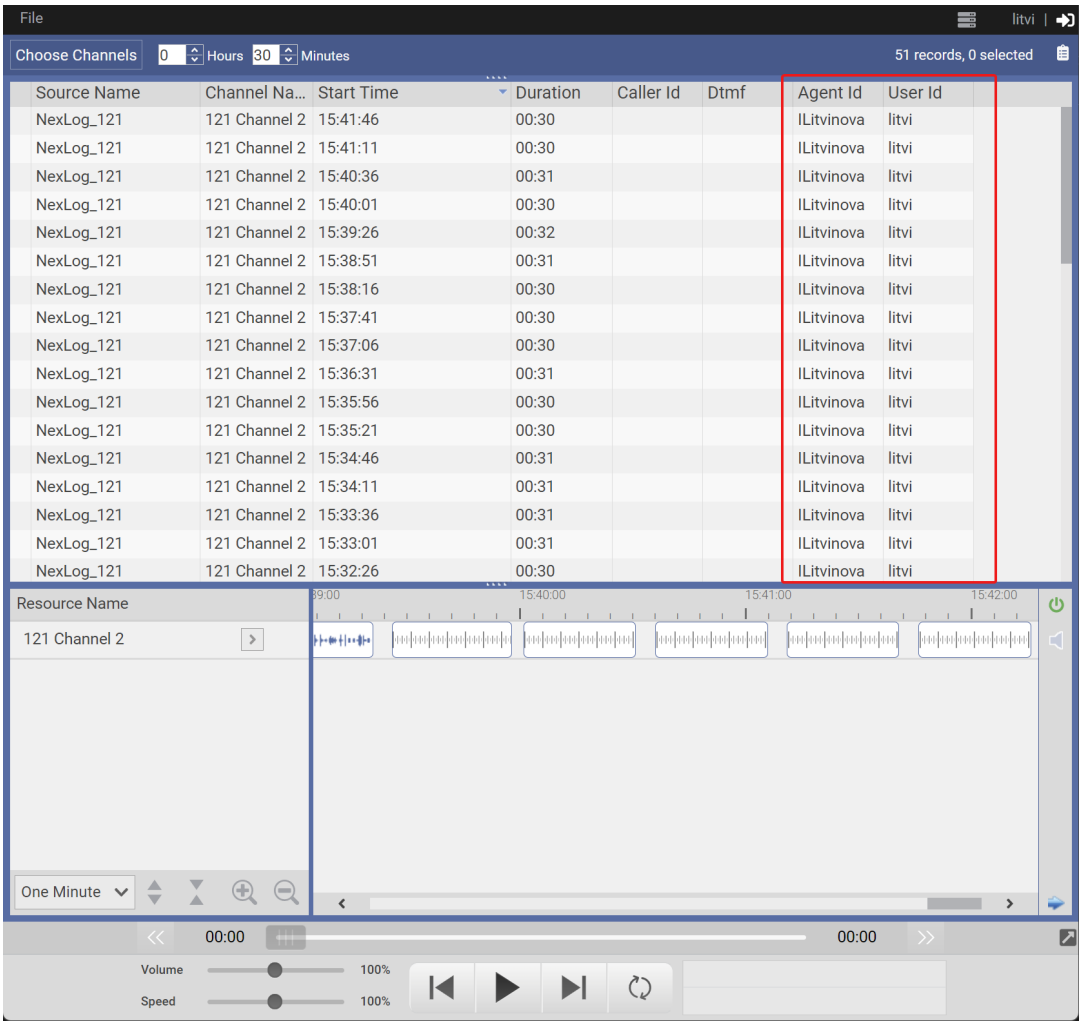


Fig. 7.92 MediaWorks Player Restrict to user tagged recordings

From within Group

When enabled, the “From within Group” function will filter which channels are available to a user based on the resource group permissions applied.

Under “Recording -> Resource Groups” create a “New Group”, and select the channels to include in your filter.

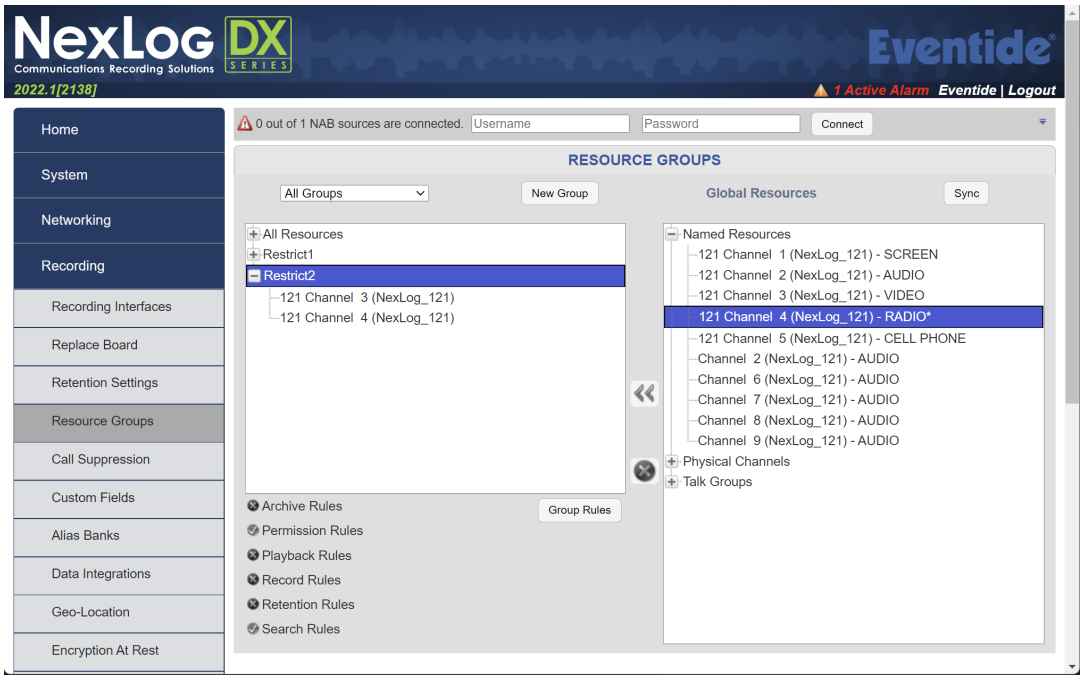


Fig. 7.93 Create Resource Group

Once created, edit “Group Rules” and ensure that “Permission Rules” and the specified user(s) are selected.

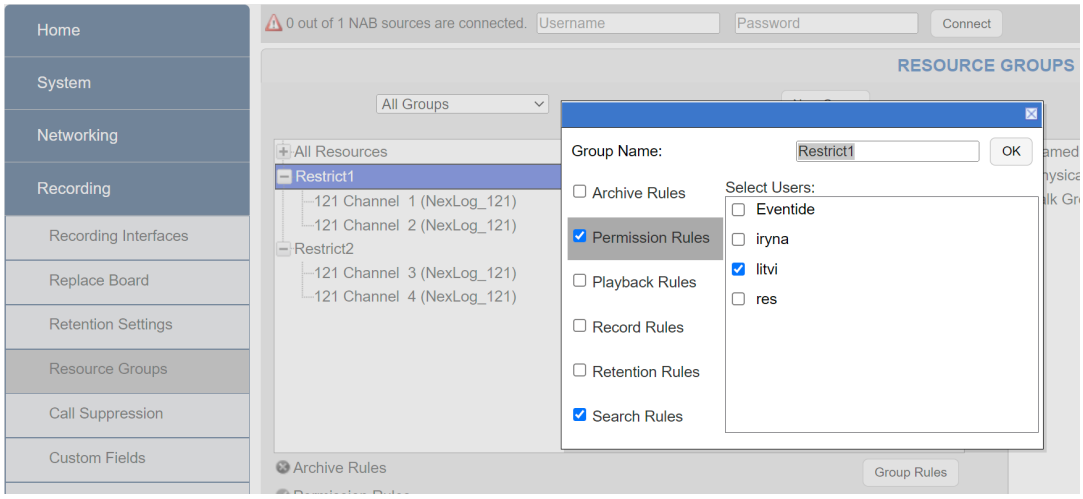


Fig. 7.94 Create Group Rules

Under the “Users” section, choose the intended user and select “Edit User”, then go to the “Permissions” Tab and select the appropriate resource group from the “From within Group” dropdown.

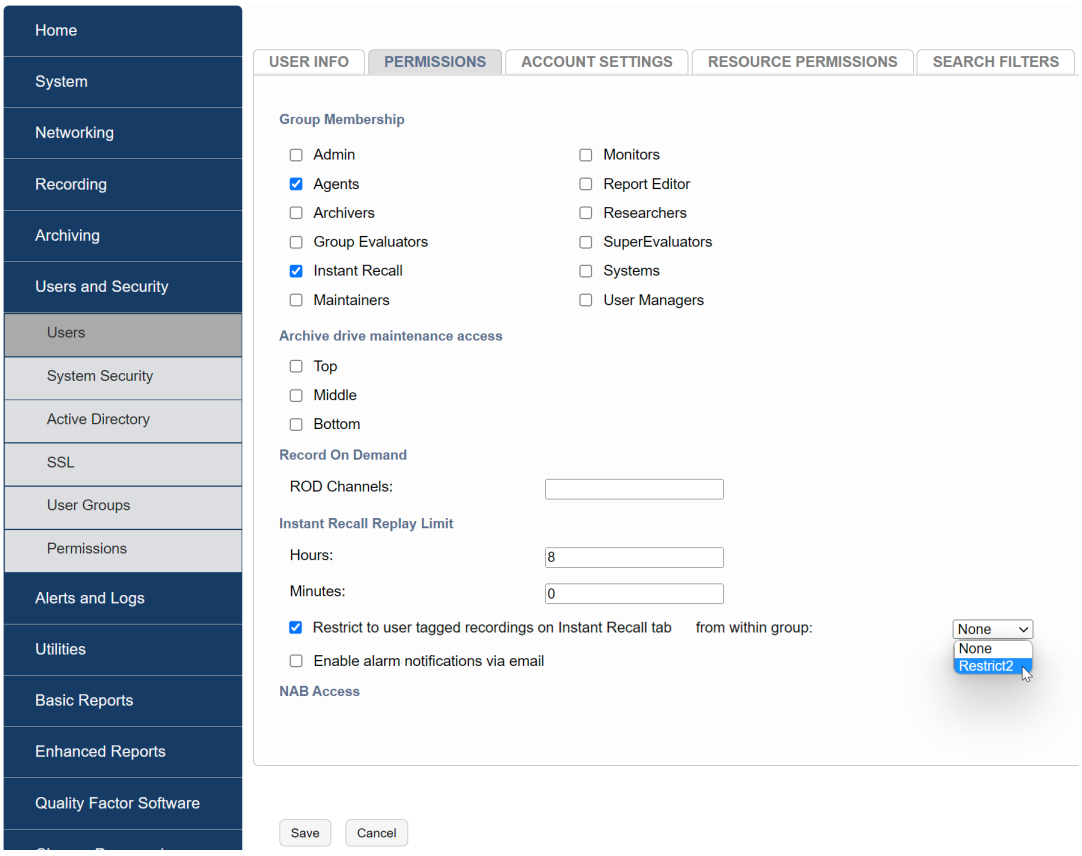


Fig. 7.95 From Within Group

When the user logs into MediaWorks EXP, they'll now have access to the specified Resource Group.

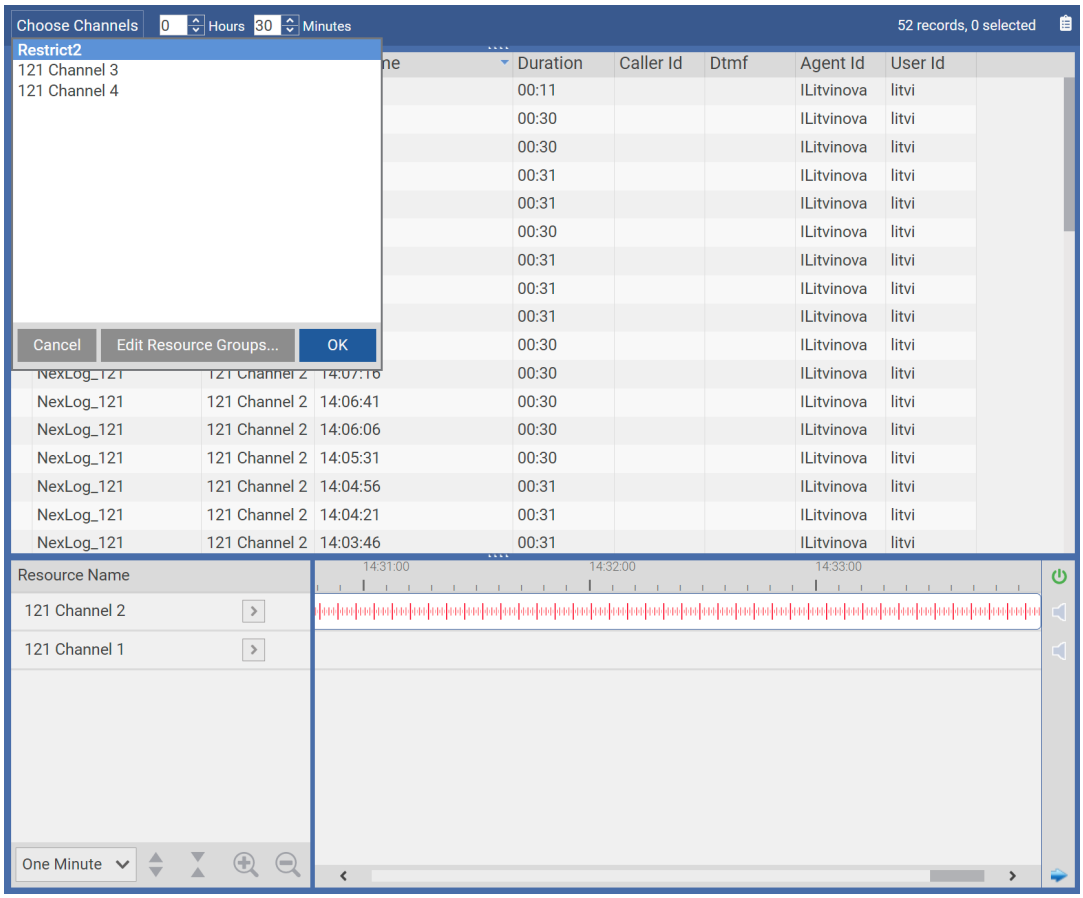


Fig. 7.96 From Within Group in MediaWorks EXP

Enable alarm notifications via email

If this checkbox is selected, the user will receive any email alerts or alarm notifications that are configured to do so in the “Alert Codes” section. This setting is enabled and cannot be disabled if the “Admin” permission is applied to the user. To receive the notifications via email, a valid email address must be configured in the “User Info” tab. The SMTP server settings must also be enabled and defined on the Alerts → Email page (Section 7.7.5 Email).

7.6.1.1.3. Account Settings

Can Change Password

If checked, the user can change their own password. If disabled, only Admins can change this user's password.

Require Two Factor Authentication

If checked, the account will be be enrolled in Two Factor Authentication on the next login. Disabling this option will remove the secret and unenroll the user. Re-enabling this option will generate a new secret for the user and start enrollment again.

Account Enabled

If checked, the account can be used. If unchecked, the account cannot be logged into.

Password Never Expires

If checked, the password expiry date has no effect.

Account Expiry Date

The account expiry date. After this date, user will not be able to log in. They will get an "Account expired" message instead.

Number of days after a password expires until the account is permanently disabled

If password complexity rules include expiring passwords, this is the number of days after a password is unchanged that the account will be permanently disabled. If configured, this will prevent long-dormant accounts from being logged into again.

Session Inactivity Timeout Enabled

By default, users will be logged out from Configuration Manager and MediaWorks EXP after an hour of inactivity. This toggles whether that is in effect.

Session Inactivity Timeout (mins)

Number of minutes of inactivity before the user is automatically logged out. If the Session Inactivity Timeout is not enabled, this value is ignored. The default is 60 minutes.

7.6.1.1.4. User Resource Permissions

These settings control what resources a user can search and playback in MediaWorks EXP and the System Console. This feature integrates with the Resource Groups feature detailed in Section 7.3.4 Resource Groups of this manual. You can add or delete individual resources or resource groups from the user's resource groups here.

7.6.1.1.5. User Search Filters

These settings control resource groups in MediaWorks EXP. This feature integrates with the Resource Groups feature detailed in Section 7.3.4 Resource Groups. You can add or delete individual resources or resource groups from the user's resource groups here.

7.6.1.2. Delete User

Delete User will delete the selected users from the system. Clicking this button will prompt for confirmation before deleting.

7.6.1.3. Change Password

Change Password will change the current password for the selected accounts.

7.6.1.4. Permissions

The Permissions button will load the Permissions page showing the selected user's permissions. See Section 7.6.1.4 Permissions for more details.

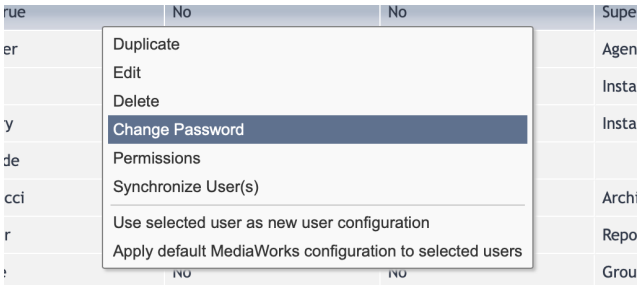


Fig. 7.97 User Table Right-Click Context Menu

7.6.1.5. User Table Right-Click Context Menu

There are additional features available on this page accessible by right-clicking on the user table: Duplicate, Synchronize User(s), Use Selected User as New User Configuration, and Apply Default MediaWorks Configuration to Selected Users.

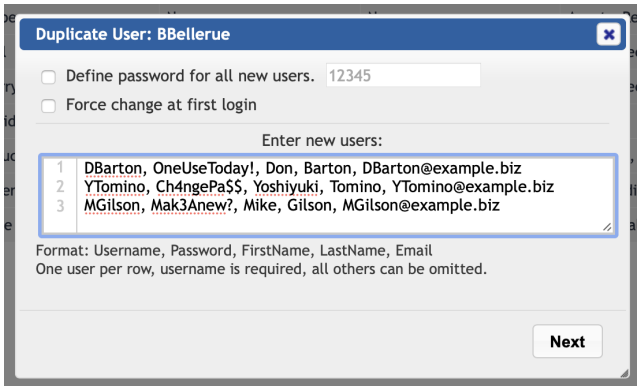


Fig. 7.98 Duplicate User

7.6.1.5.1. Duplicate

This option adds new users based on the selected user, with all the same options, user group memberships, permissions, resources and search filters. The users are added one per line with Username, Password, FirstName, LastName and Email as a comma delimited list. The only required entry is a Username.

The checkbox for “Define Password for all new users.” will let you assign a specific password to each user, who can then change it individually when they log in. If “Force change at first login” is selected, these users will be prompted to change password at first login.

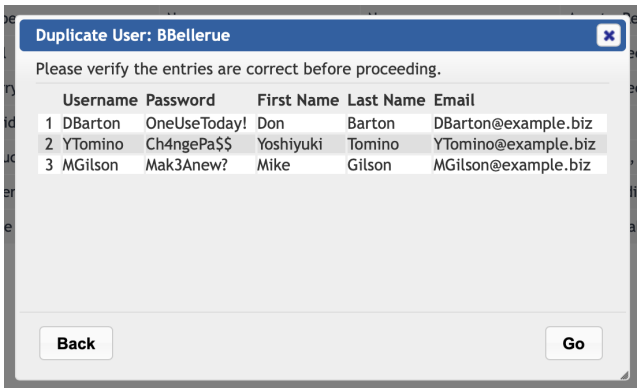


Fig. 7.99 Verify Duplicate User

After clicking Next, the user info will be presented for verification before being duplicated. Click “Back” to make corrections; click “Go” to create these users.

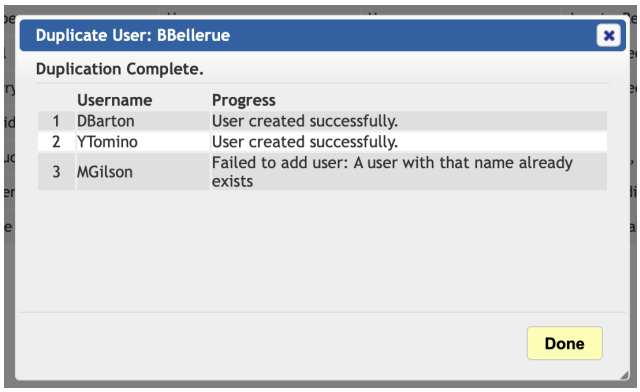


Fig. 7.100 Duplicate User Results, with Error for User That Already Exists

7.6.1.5.2. Use Selected User as New User Configuration

If you want to set up a custom MediaWorks EXP user configuration (tab layout and options), you can set up that configuration with any user and then use this option to make it the default for all new users.

7.6.1.5.3. Apply default MediaWorks Configuration

This will apply the current “New User Configuration” to the selected users.

7.6.2. System Security

NexLog Express Recorder provides options to allow recorder administrators to fine tune the recorder's security policies which are configured from the Security: System Security NexLog Express page.

7.6.2.1. General

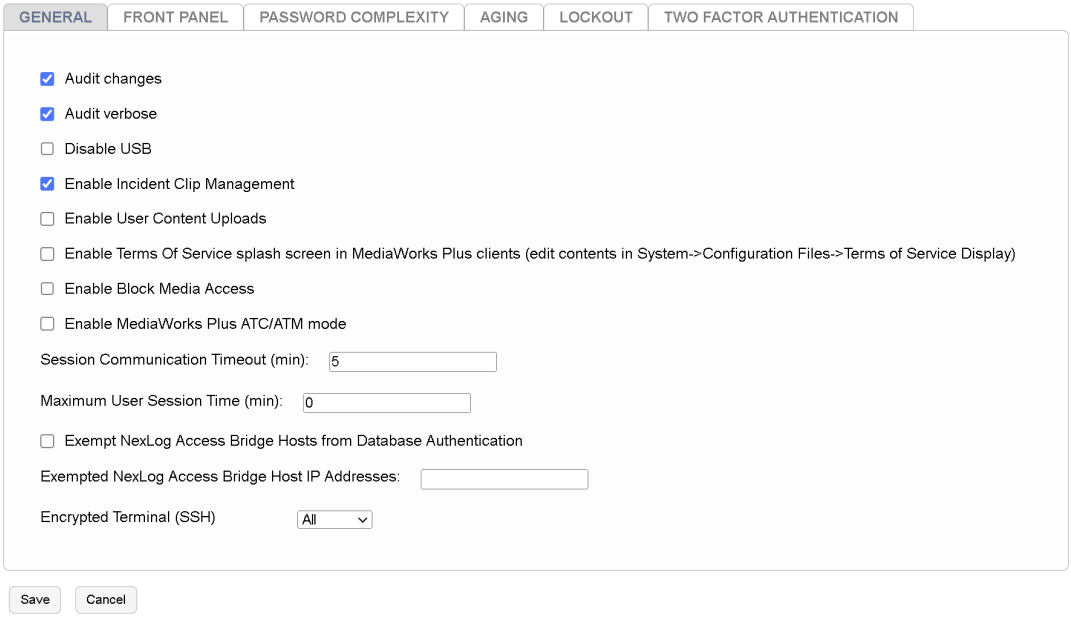


Fig. 7.101 General System Security Settings

Audit Changes

If this option is enabled, then any configuration changes made via NexLog Express Configuration Manager, Front Panel, or the SOAP Service will result in Audit event entries being placed in the audit history table. The audit history can be viewed by visiting the Alerts and Logs: Audit History Setup page.

Audit Verbose

To have an effect, this option requires "Audit Changes" to also be enabled. If enabled, then the difference between the previous state and the new state will be stored along with the audit entries

in the audit history table and visible for comparison. This information can be viewed by clicking on the audit event on the audit history page.

Enable Incident Clip Management

This enables the Incident Clip Management feature in MediaWorks EXP. This feature allows users to non-destructively splice or join analog calls that were inappropriately split or merged based on VOX hold settings. It is disabled by default so that administration can decide if this feature meets the needs of your site's policies. For more information on its use, see the MediaWorks EXP manual.

Enable User Content Uploads

If enabled, allows a user to upload media to a NexLog Express recorder channel, and use that media for incidents, evaluations, or general playback.

> **License Required**
>
> This feature must be licensed to be used. Contact your Eventide Communications Dealer for assistance.

Once enabled, create a new user group, and assign it the permission `Security Objects → Client Software → USER_CONTENT_UPLOADS`.

Enable Terms Of Service splash screen in MediaWorks EXP

A custom Terms of Service splash screen can be shown at login time for all users by enabling this. To configure the text for this, navigate to System Settings: Configuration Files and edit the file named Terms of Service.

Enable Block Media Access in MediaWorks

Allows an Admin or user with the appropriate permission the ability to prevent certain user groups from accessing a recording. Once enabled, the option can be found in the right-click context menu of MediaWorks EXP.

Enable MediaWorks EXP ATC/ATM mode

Makes changes to MediaWorks EXP to suit the needs of Air Traffic Control and Air Traffic Management sites. Enables the use of Impounds and Quarantines.

Session Communication Timeout (min)

If the recorder loses contact with a current client session, it will require a new log in at reconnection from that session after this many minutes.

New in version 2024.1.

Maximum User Session Time (min)

If this is enabled, it will automatically close any Configuration Manager or MediaWorks sessions based on the value that has been set. So for example, if it is set to 60 minutes, a user will be signed out after 60 minutes regardless of whether or not they were active in their session.

To disable it, you can set the value to 0.

Encrypted Terminal (SSH)

The SSH terminal is only used by Eventide Service personnel to assist with diagnostics. Off by default. Only change this setting if asked to by an Eventide Service engineer.

7.6.2.2. Front Panel

Desktop Mode

If enabled, the front panel interface can provide an experience similar to MediaWorks EXP.

Front Panel Login Required

If disabled, the Recorder's Front Panel will be usable without first logging in. If enabled, users will need to supply login credentials in order to view or use the Front Panel. Normally this would only be disabled if the recorder is physically secured, for example by being in a locked rack or in a locked room. The Front Panel auto-login user determines which user account is automatically logged in if "Front Panel login required" is disabled. When Front Panel Login requires is disabled, there is no way to log in to the front panel as any user other than the auto-login user other than first enabling Front Panel Login Required in setup.

Front Panel auto-login user

The user that will be automatically logged on. Many installations with high security requirements change the auto-login user to an unprivileged user that can just monitor channel activity.

Enable Screen Dim

If enabled, the front panel's LCD touchscreen will automatically adjust its brightness after the number of seconds specified in *Idle Seconds*. The screen will dim to the percentage specified in *Dim Level*. The default setting when enabled is to dim to 75% after 300 seconds. Setting *Dim Level* to *0* will turn the display off.

Front Panel Landing Page

This setting controls the default page displayed on the front panel after login, or activity timeout. The default setting is *Info*

7.6.2.3. Password Complexity

This section configures restrictions on NexLog Express passwords. If the "Enable Password complexity" option is disabled, then the only requirement on user passwords is that passwords contain at least one character so trivial passwords such as *1* are allowed. If this option is enabled, further restrictions can be applied. Note that password complexity constraints are enforced at password creation or modification time.

Newly configured password constraints will not have any effect on existing user passwords until the users attempt to change their password. When enabled, this option enforces basic “no dictionary words” password complexity constraints. In addition, additional configurable constraints can be enabled. Password complexity changes the configurable password restrictions are configured as follows:

Minimum Length

The minimum total number of characters a password must contain

Minimum Digits

The numerical characters 0-9 are considered digits. If this setting is greater than zero, then any password must contain at least that many digit characters to be allowed.

Minimum Lowercase Characters

Any password must contain at least this number of lowercase characters (a-z)

Minimum Uppercase Characters

Any password must contain at least this number of uppercase characters (A-Z)

Minimum Special Characters

Special Characters are the non-numeric, non-alphabetical characters that are available on the keyboard and result in a glyph being entered. For example, !@#$%^&*() are all Special Characters, but the CTRL key is not since it does not result in the insertion of a glyph when pressed. This setting indicates the minimum number of special characters that a password is required to contain.

New in version 2024.1.

Minimum Different Positions Of Characters From Old Password

If a password change attempt is made, then the new password will need to have characters changed in at least as many positions as the value that is set. This only applies to non-admin users.

7.6.2.4. Aging

The Password Aging sub header provides configuration options for the “Aging” or “Time Limiting” of passwords. If this option is enabled via the “Enable Password Aging” checkbox, users the system will require that users change their password on a certain configured schedule to continue to access the system. The configurable options are:

:Maximum password age:After this specified number of days have elapsed since the

user last changed their password, they will be required to change it again. For example, if this option were set to 7, users would be required to choose a different password each week. If a user’s password ‘expires’ and has not yet been changed, then if the user attempts to log in to NexLog Express via the web Configuration Manager or other clients, the only option they will have available to them is “Change Password”. They will not be able to utilize other client functionality until they successfully complete password modification.

Minimum password age

If this option is set to a value greater than zero, it configures a time period after which a user changes their password in which they are prevented from changing their password again.

Warn Before Password Expires

Will warn the user this many days before a password change is required.

Reject Previous Passwords Including Current

Remember historical passwords and don’t allow them to be re-used. If set to a value greater than zero, this option will prevent a user from reusing a recent password. For example, if set to three, a user required to change their password every three months could not simply rotate between ‘password1’ and ‘password2’. Normally this option would only be used in conjunction with the Minimum Number of Days feature described immediately above. Otherwise, users could simply

change their password several times quickly to clear out the configured “recent history” list to get around the security requirements.

7.6.2.5. Lockout

Clicking the “Lockout Settings” sub header provides configuration settings allowing user accounts to be temporarily “locked out” upon presentation of an invalid password. This can be used to prevent unauthorized personnel from gaining access to the recorder by using automatic scripts to attempt many passwords very quickly. To enable this option, check the “Enable Account Lockout” Checkbox and configure the two fields below:

Lock After Failed Attempts

The number of unsuccessful passwords that must be entered in order for a user’s account to enter the locked out state

Lock Duration

The number of seconds a user’s account remains in the lockout state once the threshold above is met.

None of the settings on this NexLog Express Configuration Manager page will take effect until the ‘Save’ button is pressed.

7.6.2.6. Two Factor Authentication

Two Factor Authentication (2FA), also known as Multi-Factor Authentication (MFA), enables a second piece of information that must be entered to log in to an account. This second factor is used in conjunction with your username and password.

2FA ensures that a user logging in is really who they say they are by requiring at least 2 of 3 common factors:

- Something you know (password)

- Something you have (smart card, token, PIV, CAC)
- Something you are (fingerprint, retina scanner)

NexLog Express natively uses *something you know* and *something you have*. *Something you are* and can be implemented externally by integrating with Active Directory.

In NexLog Express, the first factor is your username and password (something you know). The second factor (something you have), is a *Time-based*, *One-Time Password*, or *TOTP*.

7.6.2.6.1. TOTP

A Time-based, One-Time Password (TOTP) is a randomly generated token or code, that must be entered after logging in with your username and password.

As the name suggests, a TOTP token is only valid for a short period of time. The token is typically generated by a password manager or smartphone app. You may have used this second factor before without knowing it. Some online services (e.g., financial institutions) will send a random code to your mobile phone when logging in from an unknown location.

When this option is enabled for a user's account, a secure randomly generated *secret* will be provided to the user. The secret is then applied to their chosen authenticator for token generation. The time on the generation device should match that of the recording system.

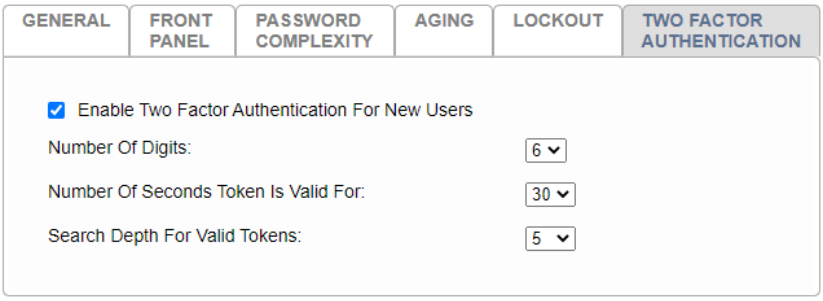


Fig. 7.102 TOTP Configuration

Enable Two Factor Authentication For New Users

Enable this option to enforce 2FA enrollment on every new user account created after enablement. Disabling this option will not unenroll accounts from 2FA, it will only allow new users to be created without it.

Number of Digits

This value controls the number of digits expected for user validation. The default setting (6), is the most commonly used in token generation applications. This value should only be changed if your token generation application supports it.

Number Of Seconds Token Is Valid For

This value controls how often a token is cycled, or its validity period. The default value (30), is the most commonly used in token generation applications. This value should only be changed if your token generation application supports it.

Search Depth For Valid Tokens

This value controls the allowed time drift for a token and is used along with the token validity period. The default setting is 5. If the depth and validity period are both set to their defaults, then a token generated within the previous or next 2 min 30 seconds would be valid.

(30 seconds) * (5 depth) = 150 seconds

7.6.2.6.2. TOTP Generators

This list of TOTP token generators is provided for your convenience. The products listed are neither supported nor affiliated with Eventide Communications LLC or NexLog Express.

7.6.2.6.2.1. Desktop TOTP

- Authy by Twilio
- LastPass
- SafeInCloud

7.6.2.6.2.2. Mobile TOTP

- Authy by Twilio
- Google Authenticator
- LastPass
- SafeInCloud

7.6.2.6.2.3. Hardware TOTP

Hardware tokens used for NexLog Express must support a programmable secret.

- Protectimus
- Token2

7.6.3. Encryption and TLS

When client software connects to the recorder and transfers data over the network, this data can be sent in plain text (unencrypted) over the network or can be encrypted using Transport Layer Security (TLS). TLS is the replacement of the now deprecated Secure Socket Layer (SSL). TLS is commonly referred to as SSL, and for the remainder of this guide, we will use the term SSL when referring to TLS.

While SSL is not required for client connections such as MediaWorks EXP, it is highly recommended to protect access to potentially sensitive information.

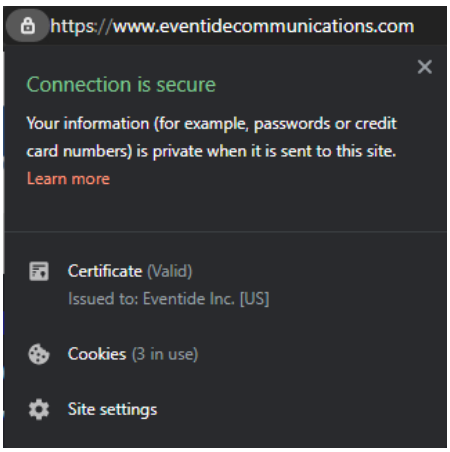


Fig. 7.103 TLS/SSL Connection Example

7.6.3.1. Issuing a Certificate

An SSL or TLS certificate must be issued or signed by a Certificate Authority (CA). A CA can be self-managed by a System Administrator or a trusted public third party. A common self-managed CA is Microsoft Certificate Services. Common public third-party CAs are Sectigo (formerly Comodo CA), DigiCert, GeoTrust, Thawte, or Verisign.

If you already have a TLS certificate that's ready to apply to the system, then you can upload a password protected PKCS #12 (PFX or P12) file directly. See Section 7.6.3.3.3 Upload PFX/P12 File. If you do not already have a certificate, you will first need to generate a PKCS #10 *Certificate Signing Request* (CSR), See Section 7.6.3.3.3 Upload PFX/P12 File.

After you have generated a CSR, you will need to submit the request to your CA.

Once your CA approves the request, they will issue your certificate and return either a PKCS #7 (P7B) file, or Base-64 PEM file with a *.crt* or *.cer* extension.

The P7B file is the easiest response to apply to the system. See Section 7.6.3.3.2 Upload P7B File.

Once a response has been applied, you can enable SSL for your system. See Section 7.6.3.5 Connection Settings.

If your system has a public DNS record pointing to it, you can use the *Let's Encrypt* option to obtain a publicly trusted certificate. See Section 7.6.3.3.5 Obtain Certificate from Let's Encrypt.

7.6.3.2. Generate CSR

To generate a CSR, you must enable the checkbox as shown in the example below

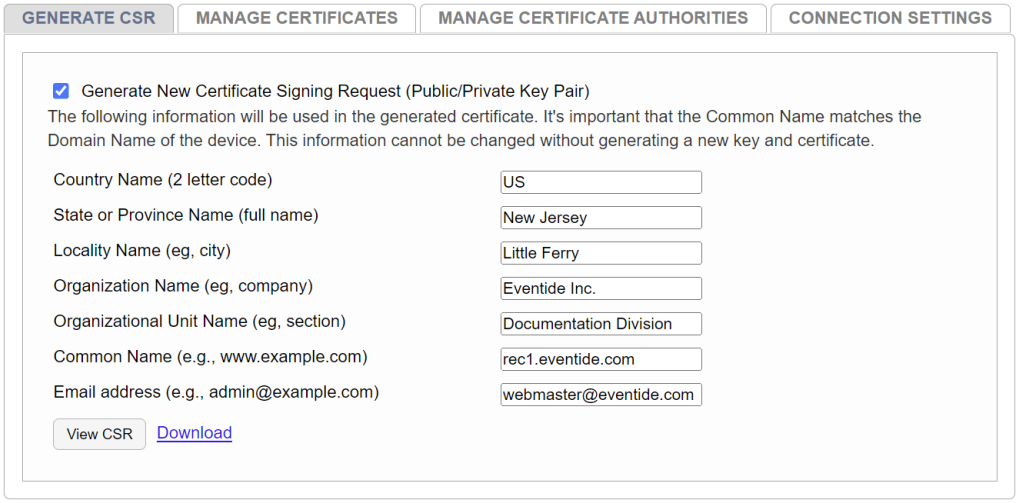


Fig. 7.104 Generate New CSR

Fill in all required details, with the critical information in this form being

Common Name. While all fields are mandatory, your CA may not use them.

The Common Name is the DNS name that you will be accessing the recorder from

- Example: *rec1.eventide.com*

After the CSR has been generated, you can view it for copy/pasting, or download it to send via email to your CA administrator.

Important

Do not reboot the system for 30 minutes after generating a new CSR request. The system will be building Diffie-Hellman parameters in the background.

7.6.3.3. Manage Certificates

This tab will allow you to manage existing certificates, apply the CA response from your CSR, or upload a new certificate directly.

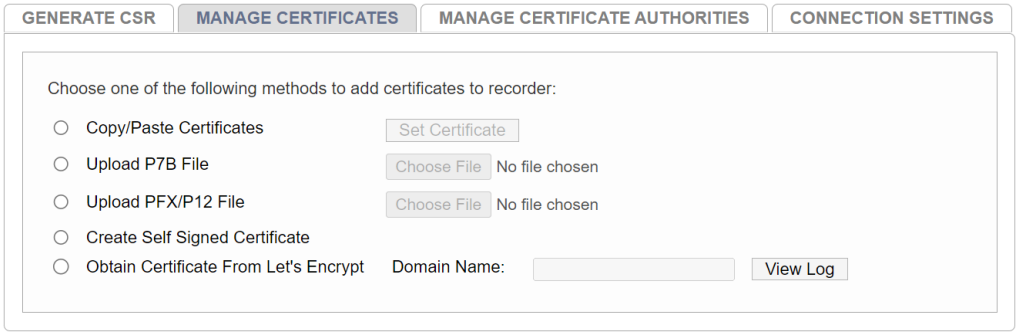


Fig. 7.105 Manage Certificates

7.6.3.3.1. Copy/Paste Certificates

If the response received from your CA is in PEM format, you can use this option to apply it.

> **Important**
>
> When copying a PEM certificate, be sure to include the header `-----BEGIN CERTIFICATE-----` and the footer `-----END CERTIFICATE-----`. Notice that there are 5 hyphens at the beginning and end of those strings.

Open the file in a text editor, copy the contents, and paste them into the field provided.

If a CA Bundle or PEM chain was provided, you can paste it separately by enabling the *Set Intermediate Certificates* checkbox. If there are multiple certificates in the bundle, be sure to include them all, excluding the Root Certificate.

7.6.3.3.2. Upload P7B File

A PKCS #7 file, typically a .p7b extension, contains a certificate and all of the intermediates in its signature chain.

After a CSR response has been received from your CA, you can upload a Base-64 P7B file directly to the system, if provided.

You would only upload a P7B, or copy and paste individual files (previous option), not both.

7.6.3.3.3. Upload PFX/P12 File

If you already have a certificate and private key to apply to the system, you can upload a PKCS #12 file, typically a .p12 or .pfx extension.

A common scenario where this would be the case is if you have a single wildcard certificate to apply on multiple systems. Example: **.recorders.example.com*

After choosing your file, you will be prompted for the password.

The PKCS #12 should have been created with the same password for the private key, and the container.

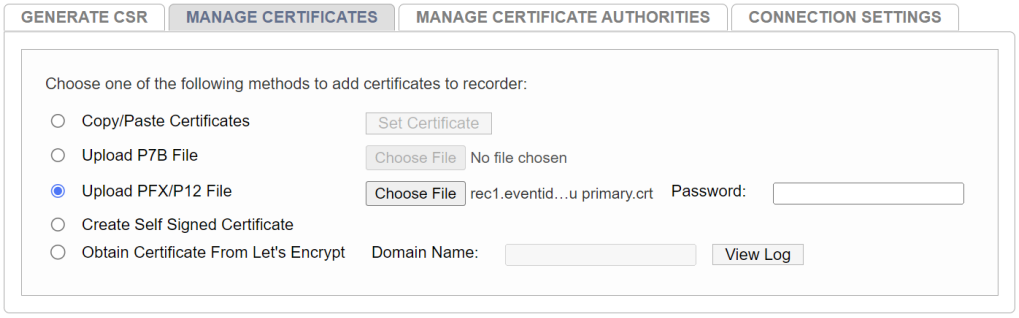


Fig. 7.106 PFX/P12 Password Prompt

7.6.3.3.4. Create Self Signed Certificate

Self Signed Certificates are usually used for testing purposes and are not recommended for production.

A self signed certificate can be created after generating a CSR.

The system will create a CA, and sign the certificate itself, so it will not be trusted by your client.

You must install the CA certificate into your client's trusted root certificate store in order for trust to be established.

Consult your operating systems documentation for how to install this certificate.

7.6.3.3.5. Obtain Certificate from Let's Encrypt

Let's Encrypt is a free, automated, and open certificate authority (CA), run for the public's benefit. It is a service provided by the Internet Security Research Group (ISRG).

If your system already has a public DNS name pointing to it, and it's accessible from the public internet, you can use this option.

Enter your full public DNS name in the Domain Name field.

Your full public DNS name would be the web address that is typed into the web browser to access your system. Example: `recorder.example.com`

Let's Encrypt certificates expire every 90 days, but the system will automatically renew it before then to insure that you always have an valid one.

> **Important**
>
> Your system must have a connection to the internet in order to renew this certificate type.

New in version 2023.1: New configuration options

When using Let's Encrypt CA, users now have access to adding and editing Let's Encrypt configurations

In more complex environments, it may be necessary to alter the default configuration used to create and renew Let's Encrypt certificates. This can be done by navigating to System → Configuration Files and editing Certbot cfg for Lets Encrypt.

Fig. 7.107 Let's Encrypt Configuration

Global Certbot configuration parameters can be modified in this file and will apply to the initial certificate. Renewals often have their own configuration based on the globals. If the configuration for an

exiting Let's Encrypt certificate needs to be altered, you will simply need to request a new one after editing the global configuration file.

7.6.3.4. Manage Certificate Authorities

New in version 2023.1: New Feature - Manage Certificate Authorities

When using an internal (not publicly trusted) certificate authority, the system will not typically trust it by default. This means that secure NAB and Centralized Archive connections may not work if the other end is using a certificate signed by the CA.

In order to trust the connections, the CA's root certificate must be uploaded.

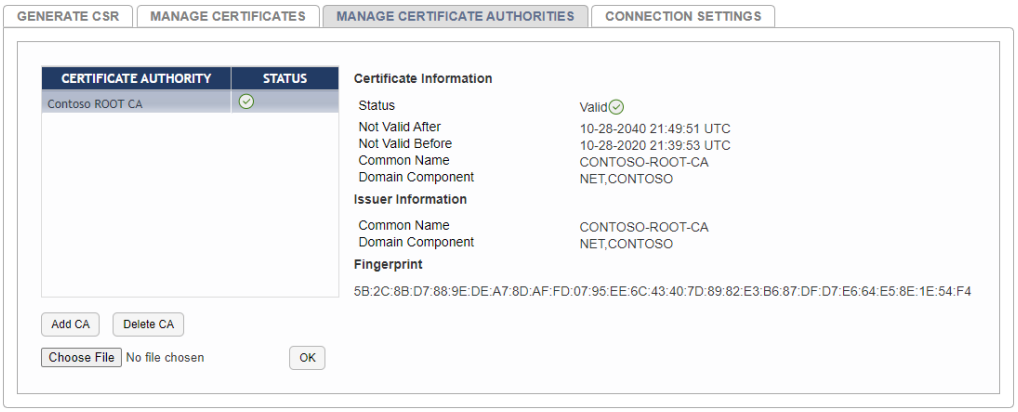


Fig. 7.108 Manage Certificate Authorities

To upload a new trusted CA certificate click Add CA and select your Base-64 PEM file. Click OK to complete the upload.

In very rare circumstances, a reboot may be required for some internal system components to trust the new root CA.

7.6.3.5. Connection Settings

This Setup page determines where encryption is used. For each entry, the recorder can be configured to accept Unencrypted Connections only, SSL Connections only or to accept both. When clients connect to the recorder they must use an enabled form of communication. Encryption provides for data security at

the expense of causing more CPU resources to be utilized on the recorder. The following connection types can each be configured:

Web Server Connections

Determines how web browsers are allowed to connect to the recorder.

New in version 2024.1.

By selecting “Limit config access to port 8443”, a user can separate the Configuration Manager from MediaWorks EXP when using encryption options (“SSL Only” or “Both”).

Examples:

- SSL Only (8443): Configuration Manager is only accessible over 8443. MediaWorks EXP is only on 443.
- Both (8443): Configuration Manager is accessible on both 80 and 8443. MediaWorks EXP is accessible on both 80 and 443.

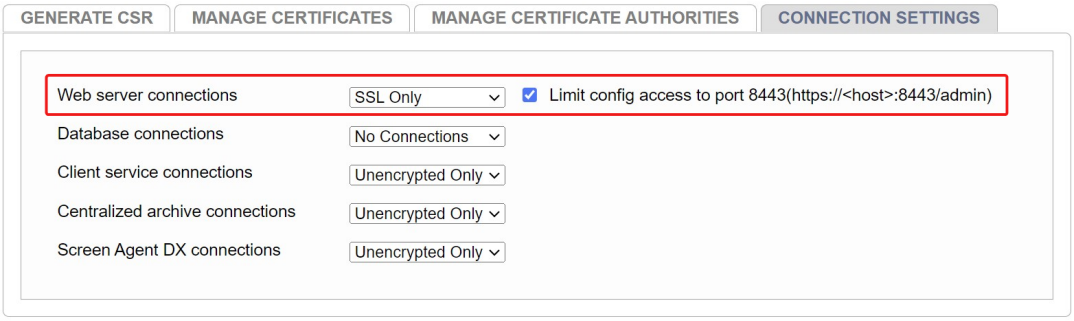


Fig. 7.109 Limit Config Access

Database Connections

This includes Eventide software such as MediaWorks EXP which communicates with the recorder’s onboard database as well as ODBC Connections to the recorder’s database made by third party applications such as Crystal Reports (TM).

Client Service Connections

Controls the live data sent between the Recorder and MediaWorks EXP/MediaAgent.

Centralized Archive Connections

Controls the connections made between two NexLog Express recorders when one acts as an archive destination for another.

Important

No changes made on this page will take effect until the recorder is rebooted.

7.6.4. User Groups

The User Groups Setup page allows User Groups to be managed and configured.

User Groups are a way to organize permissions and resources so that they can easily be granted to multiple users.

When a user is added to a group they receive the recorder permissions for the group. If they are removed from the group, they lose those permissions.

For example, you could create a Group called “Dispatchers” and give that group permission only to instant recall calls and view alerts, and then add the user accounts for all your dispatchers to that group.

The main User Groups page displays a table showing all the user groups configured on the system, one per row. Each group entry displays the Group Name and the Members of the group. If there are many members in the group, only the first few will be displayed here, and you must navigate to the ‘Edit Group’ page for the group to view the full set. Under the User Groups table is a set of action buttons. To perform any action, aside from using the ‘Add Group’ button, you must first select the desired group from the User Group table. Do this by clicking on the group within the table.

GROUPNAME	MEMBERS	RESTRICTED INCIDENT GROUP
Agents	DBylan, GHarrison	No
Archivers	CStevens	No
Central	JLennon, PMcCartney	Yes
East	CBerry, RStarr	Yes
Group Evaluators	CBerry	No
Instant Recall	JLennon, PMcCartney	No
Maintainers	CStevens	No
Monitors	DBylan	No
Report Editor	RStarr	No
Researchers	CStevens, PMcCartney, DBylan	No
SuperEvaluators	PMcCartney, RIsley	No
Systems	CStevens	No
User Managers	CStevens	No
West	CStevens, GHarrison	Yes

Add Group | Edit Group | Delete Group | Permissions

Fig. 7.110 User Groups

The default User Groups are:

Admin

Administrator group. Has all permissions by default. This group cannot be deleted.

Archivers

Group has permissions related to archiving, but not configuring archiving.

Group Evaluators

Can evaluate all users in an Agent Group, if the Group Evaluator is also configured as Group Leader

Instant Recall

Can log in and use the instant recall feature of MediaWorks EXP only.

Maintainers

Can configure the recorder and archive recordings but not use client software to search or playback recordings.

Monitors

Can use the channels tab of MediaWorks EXP and the Front Panel to live monitor incoming calls as they happen.

Researchers

Can use MediaWorks EXP to find, play, and export recordings and make incidents.

SuperEvaluators

Can evaluate any call. (See more info in the Quality Factor Manual)

'Add Group' and 'Edit Group' both navigate to the same page where group membership can be viewed and modified. 'Edit Group' provides access to the options for an existing group, while 'Add Group' creates a new group and provides access. In addition to a Group Name, this page allows you to modify which users are members of the group. To accomplish this task, choose a user from the drop down list of all users. Once chosen the user will appear below the dropdown list as being a member of this group. You can remove a user by simply clicking the 'remove' link next to the user name. You can also control a user's group memberships via the checkboxes on the Security: Users page. No changes will take effect on this page until the 'Save button' is clicked.

'Delete Group' will prompt for confirmation and then delete the currently selected user group from the system. Users that are members of that group will not be deleted, but they will no longer possess any permissions they were inheriting through their group membership.

The 'Permissions' button is a shortcut that navigates to the Security: Permissions: Edit Permissions page showing the permissions for the currently selected User Group. Members of a user group always have these permissions. The rest of the user group options are "defaults", which means that they are set when a user joins the group but can be overridden to customize a specific user's resources, search groups, or access.

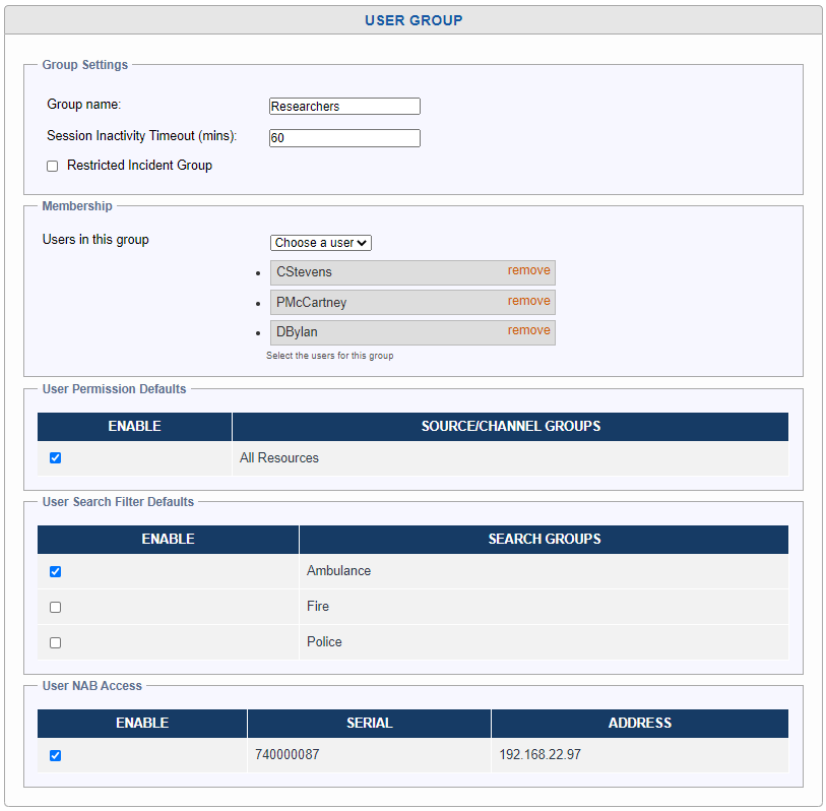


Fig. 7.111 User Group Edit

Defaults

User Session Inactivity Time Out, User Permission Groups, and Search Filter Groups can be set as a default here. Default in this context means that a new user made as a part of this group will get these settings by default, but they can be customized/overridden per user at any time without affecting their group membership. For example, you may want a user to be a researcher, but with fewer resource permissions; you can add them to this group and then customize that user's Resource Permissions on the User Edit page.

Restricted Incident Group

If multiple groups of users will be accessing a single system for playback, you can create an Incident Restricted Group by enabling this option. A user can only be a member of one restricted group. When a user is a member of an incident-restricted group, any incidents they create in MediaWorks DX will only be accessible to other members of the same group. This option will not affect an Admin user; they will be able to access all incidents on a system.

7.6.5. Permissions

The Permissions feature allows administrators to configure which actions users can take on the recorder. Without the appropriate permission, a user cannot playback recordings, export calls, or run reports. With the correct permissions, a user can evaluate their agent group, create incidents, or even create new users with permissions of their own. The actions permitted are further filtered by permissions granted to individual resources and channel names on the recorder, and to the individual pages of Configuration Manager.

At install time, your NexLog Express recorder is configured with a default set of User Groups and Permissions. Often, Recorder Administrators will simply assign users to the preexisting groups, and make minor modification to what permissions each group has.

The NexLog Express permissions system is flexible and allows for the creation of new user groups and the assignment of customized sets of permission to each group, so the entire security system behavior can be configured based on your site's needs. Permissions can be assigned directly to a user, or can be assigned to a user group; all users in a user group inherit the group's currently set permissions.

Each permission is assigned as a noun-verb pair of Security Object and Security Operation. For example, User Groups is a Security Object and Add, Delete, Read, and Update are Security Operations, so a user or user group can be assigned permission to Read User Groups, which would allow them access to see what User Groups exist, but not add, edit, or delete them.

Access to each page of Configuration Manager is also restricted by permissions. This is because some permissions apply to more than one page and it is easier to know what a user or group can do when access to entire pages is explicitly granted rather than implicity arrived at based on individual Read permissions.

Fig. 7.112 Permissions

The Users and Security: Permissions page shows a searchable and filterable list of users and user groups. Select any entry in this list and click Edit Permissions to see what Configuration Manager Pages and Security Operations are configured. The Permissions edit view can also be searched or filtered.

The filters available are:

- Show All: Shows all permission options.
- Show Permissions Granted: Shows only permissions selected for this user or group.
- Show Permissions Not Granted: Shows only permissions not selected for this user or group.
- Show Inherited: Shows only permissions this user has because of group membership. (Users Only)
- Show Permissions Granted And Inherited: Shows permissions this user been assigned directly and those they have because of group membership. (Users only)
- Show Changes Only: This last option only shows the changes being made to this user or user group during this editing session.

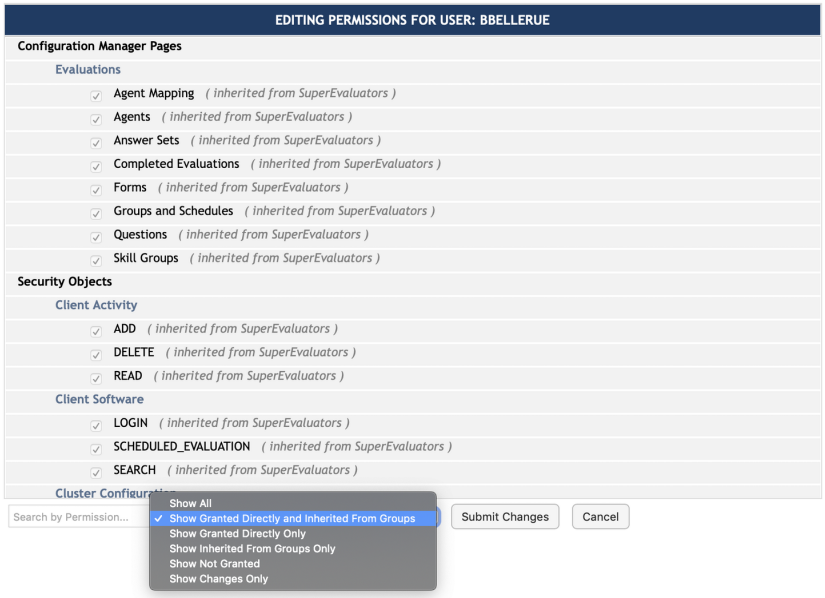


Fig. 7.113 Permissions with Filter Set to Show Granted Directly And Inherited From Groups

Right-click on any permission to set or unset permission to an entire section, or if you want to see which users and groups have a given permission, select “View All With This Permission”

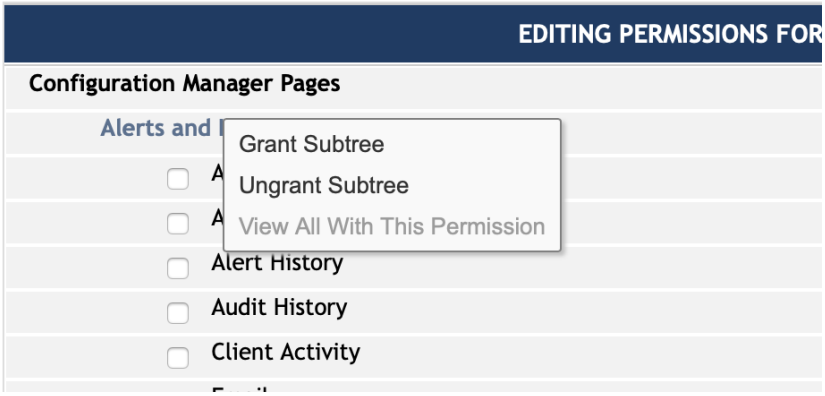


Fig. 7.114 Permissions Edit Page Context Menu

A fast way to assign the appropriate permissions for a group or user is to select the pages they should have access to and click save. This will bring up the Additional Recommended Permissions Pop Up, listing the permissions relevant for each page.

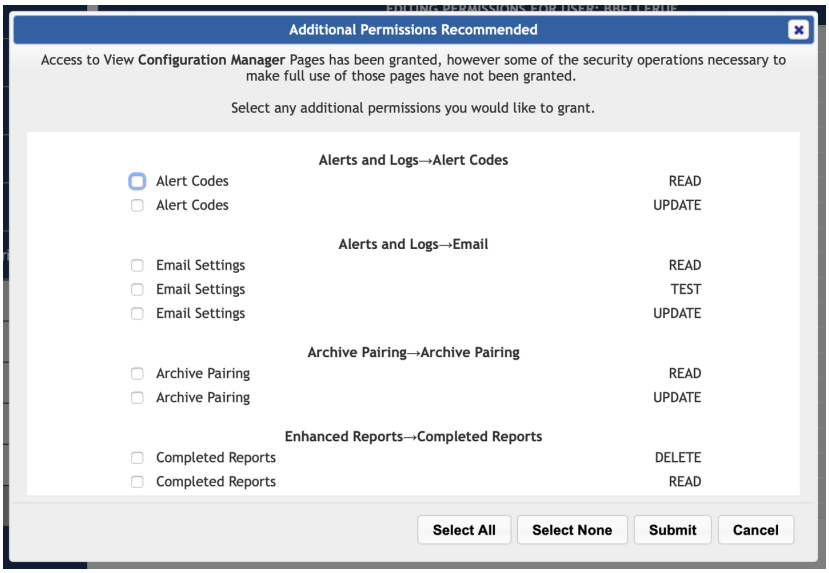


Fig. 7.115 Additional Permissions Recommended Pop Up Wizard

In the example above, the User was granted permission to load the Active Alerts, Archive Media History and Archives pages. The Additional Permissions Recommended wizard pop up appears to show the relevant Permissions relevant to actions performable on these pages. Without Update, the user cannot acknowledge an Active Alarm. Without Browse Archive, the user cannot put an archive into browse mode. The User already has Alert Read, so that permission is not suggested.

7.7. Alerts and Logs

7.7.1. Alert History

The alert history provides a detailed account of all alerts and alarms on the recorder. This screen is primarily used for diagnostic purposes. Alerts that are currently active alarm conditions will appear in bold on this page. For a detailed description of alerts see

Section 7.7.3 Alert Codes.

The fields displayed for each alert in the history are:

Time

The Date and Time the alert or alarm occurred. This information is displayed using your time zone information as configured currently.

Alert Code

Every alert occurrence has an alert code which can be cross-referenced with the information on the alert codes page

Alert Text

This is the corresponding text for the alert code with the specifics about the alert occurrence substituted in for the placeholders in the Alert Code's text.

Severity

The relative severity for this alert code as configured on the alert codes Page. Note that for alarms and other active alerts, you will see a separate entry in the alert history for when the alarm was resolved.

7.7.2. Active Alarms

An Alert on a NexLog system can either be an event or a state. Alerts that represent a state are also referred to as 'Active Alerts' or 'Alarms'. All alarms on a NexLog system are also alerts, but an alert is not necessarily an alert. For example, Alert Code #8 "Recorder Startup" is an informational alert informing of an event, but is not an Alarm. Alert Code #6001 "RAID is degraded" is an alarm, since when the event it is informing of will remain in effect until resolution (by replacing a drive). Some alerts which are not alarms will raise an alarm if the alert occurs more frequently than a preset threshold, or will show up as an Alarm for a few minutes after occurring, but then revert automatically to a non-alarm alert.

The Active Alarms page allows you to view the Alarms that have triggered on the system but have not yet been resolved. Therefore, these alarm states are actively in progress and awaiting resolution. Some alarm states will resolve on their own, for example, an alarm complaining that the networking cable has been disconnected, will be resolved automatically once the recorder detects that a network cable has

been reattached. Other alarms, such as the degraded RAID alarm, may require user intervention to resolve.

If there are any currently active alarms to show, you will see a table with one row per alarm. The columns are as follows:

Time: The date and time the alarm triggered and became active

AlertCode: The Alarm code for the alarm (See Alerts and Logs: Alert

Codes)

AlarmText: The user friendly description of what the alarm represents

Times: If the same alarm triggers multiple time, they can be 'compressed' down to a single alarm entry. In that case the "Times" field displays how many occurrences this single entry represents.

Acknowledge: The word 'Yes' if the Alarm has been acknowledged, otherwise a button containing the text 'Ack Now' which will acknowledge the alarm.

It is impossible to resolve an alarm from the Active Alarms Setup page. For an alarm to be resolved, the underlying cause must be fixed. Some alarms will automatically resolve, while others will require user intervention, such as replacing a disk drive. However, while an alarm cannot be resolved through Setup, it can be 'Acknowledged'. When an Alarm is acknowledged it remains active and in effect, but the recorder understands that the user is aware of the issue and makes less effort to draw the user's attention to the problem. Mainly, acknowledging an active alarm will prevent the alarm condition from causing the Front Panel's alarm indicator to blink red. It will also silence audio alarms associated with the alarm. In addition, the "Show Acknowledged Alarms' checkbox on this Configuration Tool page allows the user to determine whether or not acknowledged alarms should be displayed.

The final checkbox on this page is "Automatically Refresh Page" If checked, the alarms page will automatically refresh itself with the up to date status from the recorder approximately once per minute. This saves having to constantly refresh the page manually to see if any new alarms have arisen.

7.7.3. Alert Codes

Every unique alert and alarm the NexLog system can generate has an alert code. The Alert Codes Setup page allows the user to view all of the possible Alert Codes and set options for each one, such as whether or not the alert should generate an email when it occurs. The alert codes Setup page will display a table showing one available alert code on each row. At the bottom of the page are buttons for "Next Page"

“Previous Page” and “Edit Alert”. The Next and Previous buttons allow the user to navigate through all the available pages of alert codes as there are too many to fit on a single page. To edit the settings for an alert, first highlight the alert code by clicking on it and then click the ‘Edit Alert’ button.

Each alert code will display the code number for the alert, followed by its textual description. In the description you will see placeholders that look like <~1~>. These are filled in with the details of a specific alert occurrence when the alert triggers and gets inserted into the alert history table. Finally, the severity is an indication of how serious of an error the alert represents. These range from ‘INFO’ meaning it’s simply an informative alert, to ‘SEVERE’ meaning that the alert condition should be addressed immediately. Each alert code is preconfigured with a reasonable severity for each alert code, but you can use the ‘Edit Alert’ button to alter the severity of any given alert to better suit your recording application.

The ‘Edit Alert’ button will load the ‘Edit Alert Code’ Page. Here you can view and modify the settings for the selected alert code. First, the Alert Code and Display Text are read-only fields showing what alert you are currently editing. If the alert is an “Active Alert” or Alarm, there will also be a “Resolved Text” field which is a user visible description of what happens when the alarm is resolved. This is also read only.

After this is an Alert Severity Radio button set which allows for altering the severity of alert code. This determines the coloration of the alert in as displayed on the front panel as well as the behavior of certain features such as GPIO output on alerts which are configured elsewhere.

Repeat Warning Every X Seconds: If enabled, repeats the email notification every X seconds. (This is only in MediaWorks EXP where alerts pop up as a dialog box)

Alert Actions: These three checkboxes determine what action the recorder takes when an alert becomes active

Audio Alarm: Plays an audible alarm from the Front Panel speaker. Option is only available for alarms.

Send Email: If this box is checked, and email is configured as per Alerts and Logs: Email, an email will be sent out anytime an alert with this alert code triggers.

7.7.4. Logging

In addition to the alert history, the Eventide Communications NexLog Express recorder maintains some internal logs which are only useful to Eventide Communications Technicians. For service reasons, an Eventide Communications Technician may request the logs from your recorder. This page provides you a few options.

The first button ‘Enable/Disable Verbose Logging’ turns on and off verbose logging. When verbose logging is enabled, the size of the rolling log file is increased and certain log events that are not otherwise logged become logged. It is important to only run your recorder with Verbose Logging enabled at the request of Eventide Communications or your Eventide Communications Dealer’s Service personnel and to disable it when the recorder is in normal operation, as some of the verbose logging may interfere with normal behavior on busy systems.

The second button ‘Enable Analog/Digital Recording Board Driver Logging’ is a similar setting that is only requested when specifically requested by Eventide Communications Service personel.

The ‘Export logs’ button will zip up the log files on the recorder and allow you to download them to your computer to be sent to Eventide Communications or Dealer personnel. If running from the Front Panel rather than a web browser, then this option will give you the option of writing the logs to a plugged in USB Keychain drive or another archive medium rather than downloading.

7.7.4.1. Remote SysLog Settings

New in version 2024.1.

The NexLog Express recorder supports up to two Remote SysLog Logging Servers, which can also be encrypted for further security hardening when necessary.

Remote syslogging is enabled in the Configuration Manager under the Alerts and Logs → Logging page in the Advanced Settings section.

The recorder will use the existing webserver certificate for TLS negotiations.

The two remote syslog servers are supported and are configured independently. All fields are required to configure the remote syslog server. The Address can be an IP address or domain name. The standard syslog port is 514 and typically a TLS connection will be on a higher port such as 6514. TCP, UDP, and TLS (over TCP) protocols are supported and TLS is recommended. There are a variety of logging formats supported depending on deployment needs.

7.7.4.1.1. Trigger Log Exports On Alerts

Eventide Communications has implemented a feature to export recorder logs as soon as a specific alert code has been triggered, which may indicate an issue. Recorder logs can be exported to available archive drives, ensuring they are saved before getting overwritten.

In the “Alerts and Logs -> Logging” section, find “Automatic Log Export Trigger” in the Advanced Settings section.

- For ‘Trigger on Alert Codes’, enter the alert code that will prompt the recorder to export its logs
- For ‘Export to’, select the archive drive you would like the logs to be exported to

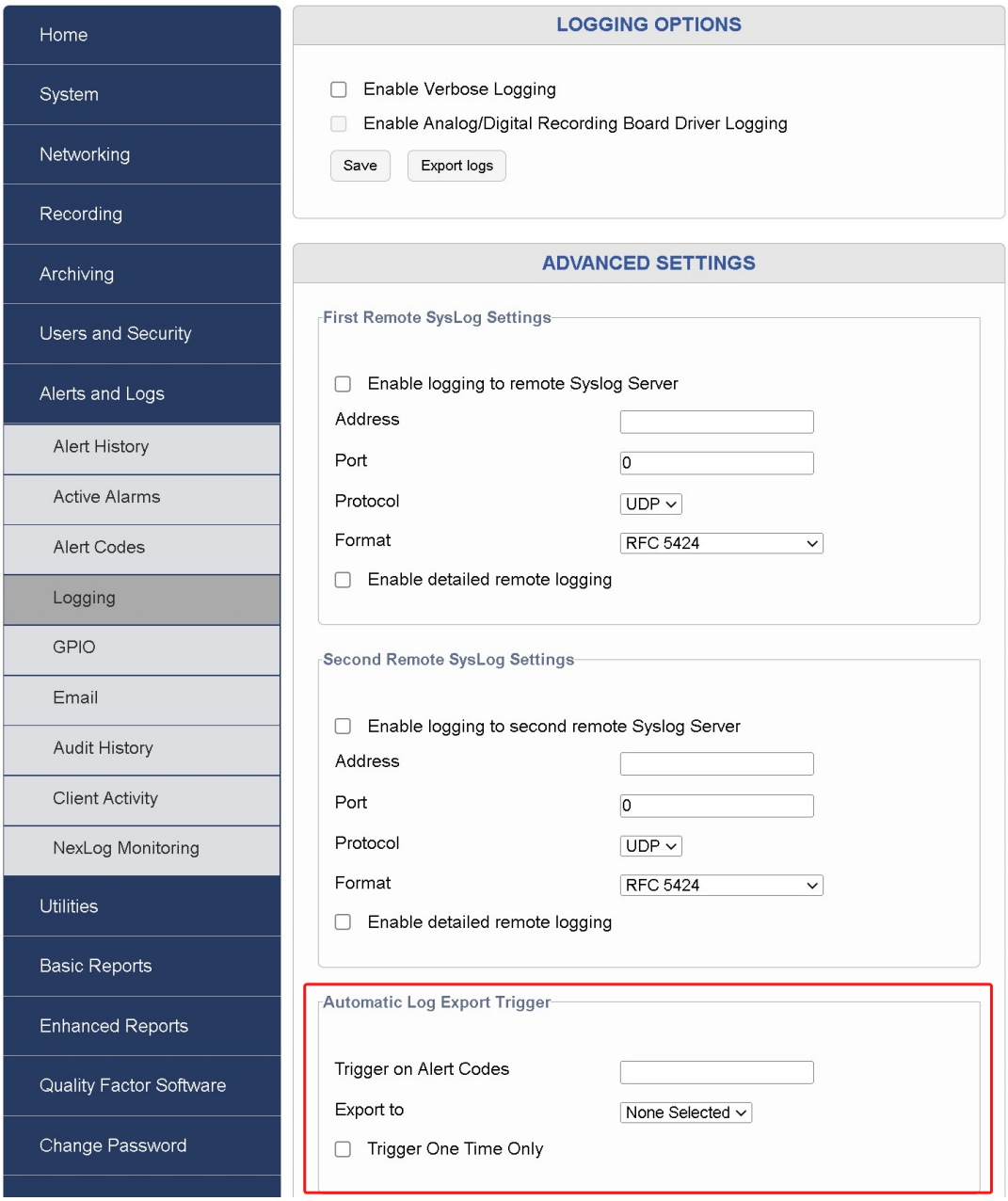


Fig. 7.116 Automatic Log Export Trigger

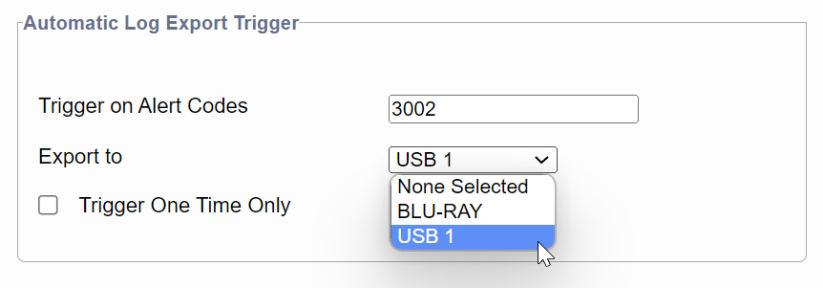


Fig. 7.117 Automatic Log Export Trigger

When “Trigger One Time Only” is selected, the recorder’s logs will only be archived once. If it is disabled, the recorder’s logs will be archived each time the alert is triggered.

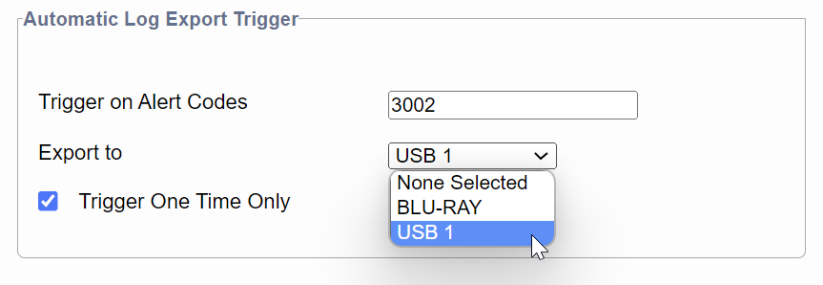


Fig. 7.118 Trigger One Time Only

> **Note**
>
> A list of all available Alert Codes can be found in the “Alert Codes” section of “Alerts and Logs”.

7.7.5. Email

The recorder can be configured to send email when specific alerts or warning conditions occur.

First click the ‘Enabled’ check box on this page. Then you must configure the parameters for the SMTP (Simple Mail Transfer Protocol)server you wish the recorder to use in order to send the emails.

Setting these parameters is very similar to the normal email setup procedure on a PC, e.g., the *Accounts* settings in Microsoft Outlook or Outlook Express. You will need the same information for these settings as you would for normal email, and can obtain them from your network administrator (or possibly by looking at your PC email settings).

All entries requiring IP addresses can either use fully qualified domain names (FQDN) or numerical addresses. Using a FQDN (e.g., <host.domain.com>) is recommended since IP addresses frequently change. The recorder does not have to be restarted for the email settings to take effect.

From Address: What the email alerts' 'From' field should read: e.g. recorder@yourdomain.com

ReplyTo address: Where the email alert should request replies be sent to e.g. support@yourdomain.com

Send Error To Address: Optional address to send email to if sending to user fails.

SMTP Host: The IP address of the SMTP server to send the email to

SMTP Login: The username the recorder should use to log in to the SMTP server

SMTP Password: The password the recorder should use to log in to the SMTP server

SMTP Localhost Name: Optional local network hostname of the SMTP server

SMTP Port: The port number the email should be sent to on the SMTP server's IP address. 25 is standard for SMTP traffic. SMTPS traffic over SSL uses a standard port of 465. SMTP over TLS uses a standard port of 587.

Finally, the "Force TLS" checkbox should be checked if your SMTP server is configured to only allow emails to be sent using TLS.

To define the email recipient for any alert or alarm, a valid email address must be configured in the user's profile. All users with the "Admin" permission will receive these email notifications. If a user does not have the "Admin" permission but should receive email notifications, the "Enable alarm notifications via email" setting should be enable from the permissions tab of the user's settings page.

A test email can be sent from the "Email Settings" page to verify that recipients have been properly configured. All recipients will be visible in the "To" line of the received email.

> **Note**
>
> SMTP fields are compliant with RFC 2821 standards.

7.7.6. Audit History

Your system stores an audit history of important events which have occurred on the system for security auditing. Auditing is on by default and the option to turn it off is under System Security in the Users and Security section.

The Audit history can be viewed from the 'Audit History' page. There are two views available: Tree (Sessions) and Table (Operations). The Tree view groups audited actions into sessions by user and the Table view is a list of all operations that have been audited. In either view, entries can be clicked to see more detail.

In Table view, each row in the table represents one auditable event, and auditable events are displayed in descending order by time, with most recent first. If more than one web page is required to display all the audit history events, you will find an "Older Entries' and "Newer Entries" buttons at the bottom of the page for navigation purposes.

Each audit history entry shows the following information:

Time: The Date and Time the audited event occurred are displayed using the currently configured time zone information for the recorder

User: The User Account which performed or attempted to perform the audited action

Success: If the action was successful, it is in black text. If it failed, it is in red.

Description: A human readable description of what happened.

Action: This describes the action that was performed. Valid action types include:

- USER-LOGIN: The user account logged into the system. The description will also specify what client software was used (e.g. MediaWorks EXP, Soap Client, etc.)
- USER-LOGOUT: The user account logged out of the system
- SHUTDOWN: A request was made to shut down the recorder
- REBOOT: A request was made to reboot the recorder
- MONITOR-ON: The user Live Monitored a channel and listened to the audio
- MONITOR-OFF: The user ceased live monitoring the channel
- FORCE-SUPPRESSION-ON: The user turned on call suppression for a channel
- FORCE-SUPPRESSION-OFF: The user turned off call suppression for a channel
- AUDIO-ACCESSED: The user played a media record

- ADD-ENTITY: A New entity (e.g. Custom Field, User Account, etc.) was added to the recorder. The description will tell which entity type was added.
- DELETE-ENTITY: An Entity (e.g., Custom Field, User Account, etc.) was deleted from the recorder. The description will tell which entity type and the primary key (name, number, etc.) of the entity.
- UPDATE-ENTITY: An Entity (e.g., Custom Field, DateTime, etc.) was modified. The description will tell the Entity Type and if applicable primary key of the entity.
- GET-ENTITY: An Entity (e.g., Custom Field, DateTime, etc.) was retrieved and viewed. The description will tell the Entity Type and if applicable the primary key of the entity
- GET-ALL-ENTITY: All Entities (e.g., Custom Field, DateTime, etc.) were retrieved and viewed. The description will tell the Entity Type
- SEARCH-ENTITY: An Entity was searched
- START-RECORDING: A user forced recording to start on a channel (this usually happens from a SOAP integration with the recorder)
- STOP-RECORDING: A user forced recording to stop on a channel (this usually happens from a SOAP integration with the recorder)
- ROD-DISABLE: A user forced a channel into a non-recording mode (this usually happens from a SOAP integration with the recorder)
- ROD-ENABLE: A user switched a channel back to its standard recording mode (this usually happens from a SOAP integration with the recorder)
- OPEN-TRAY: A user ejected an archive drive
- CLOSE-TRAY: A user injected an archive drive
- ACKNOWLEDGE-ALERT: A user acknowledged an alert
- SET-CHANNEL-METADATA: A user added metadata to be applied to each media record on a channel (this usually happens from a SOAP integration with the recorder)
- SET-CALL-METADATA: A user added metadata to a specific call (this usually happens from a SOAP integration with the recorder)
- SET-WORKSTATION-TAG: User set workstation tag for channel. (this usually happens from a SOAP integration with the recorder).
- UNSET-WORKSTATION-TAG: User unset workstation tag for channel. (this usually happens from a SOAP integration with the recorder).
- CHANGE-PASS: A user changed their pass (or someone else's if they are an admin)
- EXPORT-SYSTEM-INFO: A user took a backup of system information either to an archive drive or via download to a web browser.
- IMPORT-SYSTEM-INFO: A user uploaded or restored system information
- OFFLINE-DISK-FROM-RAID: A user marked a drive for removal
- ADD-DISK-TO-RAID: A user added a new drive to a RAID
- BOND-NICS: A user bonded 2 network interfaces together into 1 interface (this is advanced behavior for certain logger configurations and is not typical to see)

- START-ARCHIVING: A user started archiving on an archive device
- STOP-ARCHIVING: A user stopped archiving
- BROWSE-ARCHIVE: A user put an archive into Browse mode for viewing with the Front Panel or with client software
- UNBROWSE-ARCHIVE: A user took a browsed archive back offline
- PERIOD-ARCHIVE: A user initiated a period archive to an archive drive
- FORMAT-ARCHIVE: A user initiated a format of an archive drive
- SET-ARCHIVE-POINTER: A user moved the archive time pointer on an archive
- START-ARCHIVE-TRANSFER: A user started a transfer of archived data back to the recorder
- STOP-ARCHIVE-TRANSFER: A user stopped the transfer of archived data to the recorder.
- START-PCAP: A user started a network data capture
- STOP-PCAP: A user stopped a network data capture

The Audit History is designed to provide an audit trail of configuration changes as well as audio access to the recorder. There are options available under Security: System Security that allow for configuration of the level of detail in the audit history. If full details are enabled, then clicking on a configuration change audit event (e.g. UPDATE-ENTITY) will display the difference between the original and new configuration that was sent to the recorder to make the request. A Close button is provided to dismiss that window.

7.7.7. Client Activity

This information can sometimes be useful for troubleshooting client licensing issues as the client access is licensed on a per workstation basis. One client workstation is shown per row along with next/prev/go buttons for navigation as on other pages.

For each entry in the Client Activity table the following fields are shown:

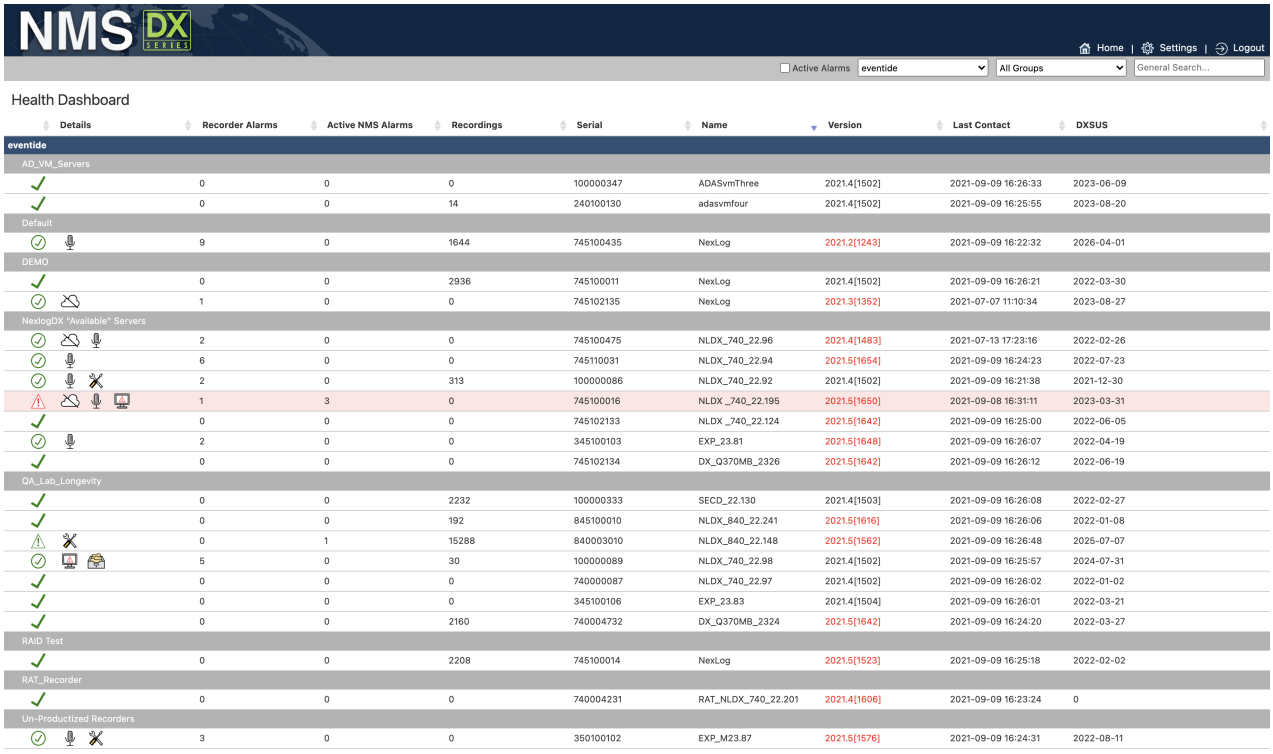
- Workstation: MAC address of the connecting client
- User: The Username with which the client was logged into the system
- Login Time: The date and time the login occurred
- Logout Time: the data and time the client logged out. Blank if still logged in
- License In use: Whether or not this client is currently holding a license.
- ClientType: Application used to connect to the recorder
- Client Address: The MAC address of the workstation from which the client logged in

7.7.8. NexLog Monitoring

New in version 2022.1.

The NexLog Monitoring Server (NMS) is a HTTPS based monitoring application for NexLog Express products. When licensed and configured, a NexLog Express will send a heartbeat to the NMS with alarms, call statistics, and database statistics. The NMS saves the alarm state and gives the user an organized dashboard to view all their NexLog DX-Series™ and their health 24x7. The NMS has the following features:

- Health Dashboard: A real time 24x7 dashboard to view all your NexLog Express and their health
- Alarm Filtering: Create custom reusable alarm filters for each recorder
- Contact Groups: Group Technicians together and assign them to specific recorders
- Recorder Groups: Group your NexLog Express together for easy access/organization



Details	Recorder Alarms	Active NMS Alarms	Recordings	Serial	Name	Version	Last Contact	DXSUS
eventide								
AD_VM_Servers								
	0	0	0	100000347	ADASvmThree	2021.4[1502]	2021-09-09 16:26:33	2023-06-09
	0	0	14	240100130	adasvmfour	2021.4[1502]	2021-09-09 16:25:55	2023-08-20
Default								
	9	0	1644	745100435	NexLog	2021.2[1243]	2021-09-09 16:22:32	2026-04-01
DEMO								
	0	0	2936	745100011	NexLog	2021.4[1502]	2021-09-09 16:26:21	2022-03-30
	1	0	0	745102135	NexLog	2021.3[1352]	2021-07-07 11:10:34	2023-08-27
NexlogDX *Available* Servers								
	2	0	0	745100475	NLDX_740_22.96	2021.4[1483]	2021-07-13 17:23:16	2022-02-26
	6	0	0	745110031	NLDX_740_22.94	2021.5[1654]	2021-09-09 16:24:23	2022-07-23
	2	0	313	100000086	NLDX_740_22.92	2021.4[1502]	2021-09-09 16:21:38	2021-12-30
	1	3	0	745100016	NLDX _740_22.195	2021.5[1650]	2021-09-08 16:31:11	2023-03-31
	0	0	0	745102133	NLDX _740_22.124	2021.5[1642]	2021-09-09 16:25:00	2022-06-05
	2	0	0	345100103	EXP_23.81	2021.5[1648]	2021-09-09 16:26:07	2022-04-19
	0	0	0	745102134	DX_Q370MB_2326	2021.5[1642]	2021-09-09 16:26:12	2022-06-19
QA_Lab_Longevity								
	0	0	2232	100000333	SECD_22.130	2021.4[1503]	2021-09-09 16:26:08	2022-02-27
	0	0	192	845100010	NLDX_840_22.241	2021.5[1616]	2021-09-09 16:26:06	2022-01-08
	0	1	15288	840003010	NLDX_840_22.148	2021.5[1562]	2021-09-09 16:26:48	2025-07-07
	5	0	30	100000089	NLDX_740_22.98	2021.4[1502]	2021-09-09 16:25:57	2024-07-31
	0	0	0	740000087	NLDX_740_22.97	2021.4[1502]	2021-09-09 16:26:02	2022-01-02
	0	0	0	345100106	EXP_23.83	2021.4[1504]	2021-09-09 16:26:01	2022-03-21
	0	0	2160	740004732	DX_Q370MB_2324	2021.5[1642]	2021-09-09 16:24:20	2022-03-27
RAID Test								
	0	0	2208	745100014	NexLog	2021.5[1523]	2021-09-09 16:25:18	2022-02-02
RAT_Recorder								
	0	0	0	740004231	RAT_NLDX_740_22.201	2021.4[1606]	2021-09-09 16:23:24	0
Un-Productized Recorders								
	3	0	0	350100102	EXP_M23.87	2021.5[1576]	2021-09-09 16:24:31	2022-08-11

Fig. 7.119 NMS Dashboard

License Required

This feature must be licensed to be used. Contact your Eventide Communications Dealer for assistance.

7.8. Utilities

7.8.1. Schedules

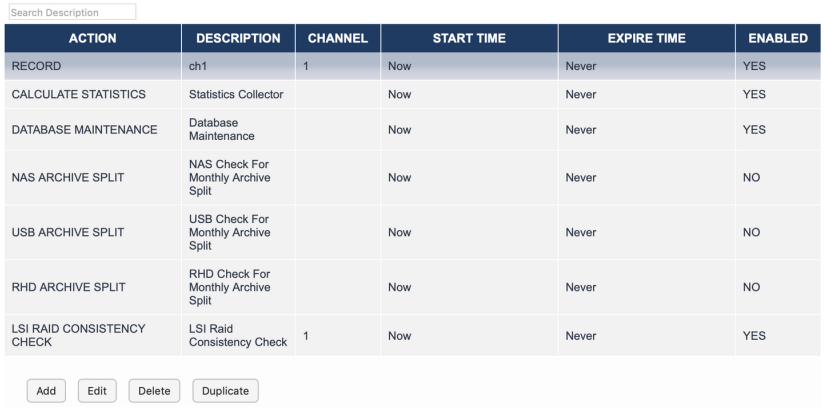


Fig. 7.120 Schedules

The Schedules Page allows the configuration and maintenance of Recording and other Schedules. A Schedule is an event that happens either once at a configured time, or repeatedly at a configured time, such as every Sunday at 2PM. The main Schedules Page shows a table with all configured scheduled events displayed one row per event. The fields displayed for each event are as follows:

Action: What action will occur when the schedule triggers:

- Record: Begin Recording on the configured channel and record for the configured duration of the scheduled event.
- Disable Channel: Disable a channel for the duration of the scheduled event
- Send Notification: Used for integrations and custom scripting. Has a Channel option.

- Calculate Statistics: Runs the Recorder's Daily Statistics Gathering Process which certain Reports depend on.
- Archive: Starts archiving on the drive specified for the duration configured. This is so that network based archiving such as NAS or Centralized Archiving can be scheduled for overnight shifts.
- Database Maintenance: Performs maintenance on the database. Performance will be slower than usual at this time, so it is recommended to schedule this at a time that is lower volume than usual.
- NAS Archive Splitter: Controls when and whether NAS drives will be split into month sized Archives for faster loading when browsing for playback.
- R-HD Archive Splitter: Controls when and whether R-HD drives will be split into month sized Archives for faster loading when browsing for playback.
- USB Archive Splitter: Controls when and whether the USB drives will be split into month sized Archives for faster loading when browsing for playback.
- Backup User Edited Metadata: Archives User Edited Metadata to the archive drive specified.
- Backup Incidents Evaluation Metadata: Archives all Incidents and Evaluations to the archive drive specified.
- Backup Database: Archives the database to the archive drive specified.
- Backup Configuration: Archive the current configuration.
- Status Email: Sends an email with a variety of logger status information, including any current alarms, the last 100 alerts, and call counts per channel for the last hour.
- LSI Consistency Check: For systems with LSI cards, this starts a Consistency Check on the hardware RAID.

Description: A user entered description of what this schedule represents, e.g. "Record 3PM Engineering Meeting"

Start Time: When the schedule will first become active

Expire Time: When the schedule will no longer be active and will no longer trigger

Enabled: If disabled, schedule events will not fire off when they otherwise should due to date/time.

Under the main table containing the list of configured scheduled events are buttons which allow actions to be taken. Except for the 'Add' button, all actions require a specific scheduled event to first be selected in the table below as they take effect on the scheduled event.

Delete: Deletes the selected scheduled event after prompting for confirmation

Add and Duplicate: Both of these allow you to create a new scheduled event and take you to an 'Edit' page for that new schedule. The difference between 'Add' and 'Duplicate' is that add displays the page with default values, and duplicate uses the currently selected scheduled event as a Template to set the

defaults, which you can then change. This is useful for creating several schedules that are all the same except for a couple of parameters, such as channel number.

Edit: The Add and Duplicate Page also take you to a page with the same parameters as 'Edit', though for a new schedule rather than an existing one, so the parameters described below are valid for those pages as well. The configurable parameters for a scheduled event are as follows:

7.8.1.1. Schedules Tab

Description: A User Friendly Description of what this scheduled event is

Enabled: IF not checked, this schedule is disabled and will not have any effect until enabled.

Channel: Used for scheduled events where the action is "Start Recording" or "Disable Recording". This determines the number of the channel upon which recording will be started or disabled

Scripting Tag: For use with custom scripting and Eventide integrations, it associates a static piece of data with the notification.

7.8.1.2. Activation / Expiration Heading

Activate Now: If checked the schedule becomes immediately active. If disabled, the Start Time becomes option below becomes available for editing. There you can use the calendar control and hour / minute / second boxes to set a start time. Note that all times are configured on this page should be in your currently configured local time zone (not UTC). The current time zone is listed in the heading above for convenience

Never expires: If checked, the schedule never expires, otherwise the Expire Time option below becomes available. It works identically to the Start Time parameter.

7.8.1.3. Action Heading

The radio buttons in this section allow you to specify the action that will take place when the schedule fires. The options are described below:

Start Recording: Recording will start on the channel specified above in the "Channel" parameter whenever the schedule fires and will continue recording for the duration configured below, at which time

it will stop recording. Note that in addition to configuring the schedule here, the channel must be configured for “Scheduled” in the Call Detect Type (configured under Recording: Boards).

Disable Recording: “Record On Demand” The channel will be disabled when the schedule fires and re-enabled after the duration. During this time the channel will not record, at all other times it will record based on its normal call detect types.

Send Notification: Triggers a notification event for use with custom scripting and Eventide integrations.

Run Statistics: Schedules the daily statistics to run. This should be run once daily, you should only ever change the time of day which it is run, to schedule it for the slowest volume period on your recorder.

7.8.1.4. Period Heading

These radio buttons determine how often the schedule repeats.

Hourly: Schedule triggers once per hour

Daily: Schedule triggers once per day

Weekly: Schedule triggers once per week Monthly

Monthly: Schedule triggers once per Month

One Time: Schedule triggers only once

Which of these options is selected will dictate what parameters are available under Period Options as well.

7.8.1.5. Period Options Heading:

Duration is always the same regardless of the Period set above and is the Minutes and Seconds time during which the schedule will be occurring (e.g., how long to record for if action is Start Recording). If action is Statistics, duration has no effect.

For Hourly: Start at X Minutes past the hour, the number of minutes past the hour the schedule will trigger

For Daily: Start at Hours: Minutes past midnight, the number of hours and minutes past midnight the schedule will trigger, so if set for 13:30, schedule will trigger at 1:30PM

For Weekly: Start at Hours: Minutes past Midnight, as above, but also checkboxes for which days of the week to trigger on are provided

For Monthly: Start at Hours, Minutes past midnight, and also what day of the month to schedule action for is supplied (e.g., 1 to trigger on 1st of the month), plus check boxes for which months to trigger on

One Time: Schedule only triggers once at activation time.

Repeat Every: If checked, the how many hours should pass between triggering. For example, for an hourly schedule if Start At is set for 30 and Repeat Every for 3 hours, and the schedule activation time is 1:45, then the schedule will trigger at 2:30, 5:30, 8:30, 11:30, etc. Repeat every is provided for Hourly and Weekly schedules

7.8.2. Upload Recorder Update

The Upload Recorder Update Utility page allows administrators to apply Incremental Updates provided by Eventide to update systems in the field. It is only for use when directed by Eventide Service and only works with Incremental Updates created by Eventide.

7.8.3. Re-Order Channels

This page allows you system administrators to arrange the channels as if it was installed with the current configuration. This is useful if the physical boards have been changed or moved or if virtual boards have been resized. The recorder will be automatically rebooted after performing this function.

7.8.4. Network Utilities

The Network Utilities page allows administrators to run Ping, Traceroute, Netcat, and Host Unix utilities from the recorder to identify network problems.

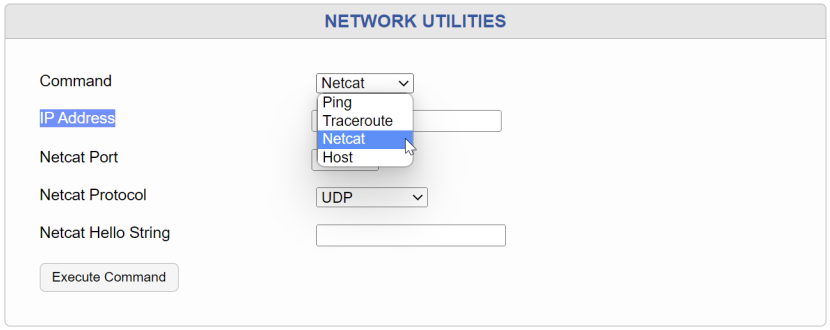


Fig. 7.121 Network Utilities

7.8.5. Packet Capture

Packet Capture is a diagnostic tool that allows you to easily capture a record of network traffic for analysis in a third party application such as Wireshark. You may be asked to use this feature in the course of a service call in order to allow Eventide to troubleshoot a networking or IP call situation.

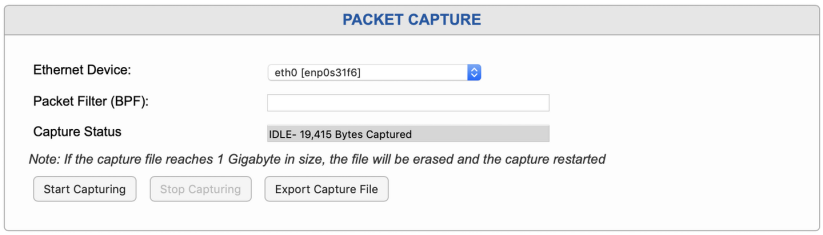


Fig. 7.122 Packet Capture

Ethernet Device: Allows you to choose the device you intend to capture the network traffic from.

Packet Filter (BPF): Allows you to apply additional rules to the captured network traffic. This field uses the standard Berkeley Packet Filter (BPF) syntax. For more details, perform a web search with using “bpf syntax”.

BPF example: To only capture the packets to or from a VoIP telephone with the IP address 192.168.1.16, you would enter “*host 192.168.1.16*”.

From the Configuration Manager, clicking Export Capture File will prompt you to save the capture as a file. When using packet capture from the front panel, Export Capture File will ask for an archive drive to write to.

Important

As noted in the display, the capture will automatically restart after 1 Gigabyte of data has been received.

7.8.6. Documents

This page include links to HTML and PDF versions of NexLog Express documentation.

DOCUMENT NAME	VERSION	ACTION
NexLog DX-Series Recorder	2021.1	View HTML Download PDF
NexLog API Manual	2021.1	View HTML Download PDF
MediaWorks DX	2021.1	View HTML Download PDF
Smart Edge Capture Device	2021.1	View HTML Download PDF
NexLog-AQUA Audio Plugin	2.2.0	View HTML Download PDF

Fig. 7.123 System Documentation

7.9. Basic Reports

7.9.1. Recording Reports

This section provides access to the Eventide NexLog Express Basic Reporting Package. Basic Reports provides a list of available report types which can be run.

After selecting one of the report types and clicking the “Run Report” button, you will be taken to a page where you can enter custom parameters for the report. Which parameters are available depend on which report type you are generating. Once you have selected all your parameters, click the ‘Run Report’ button to continue, or the ‘Cancel’ button to return to the previous screen without running the report.

Your report will be generated using the parameters you specified and will open in a new browser window. On the top of this window will be a 'Close' button to dismiss the report when you are finished looking at it. Note that reports may take up to several minutes to generate and display, especially if you are running a report over a large range of channels or dates, as the Reports engine must sift through a large amount of data in the database in order to generate the report. It is important to be patient and not click 'back' or 'refresh' in your browser while waiting for a report to be generated. Each report consists of a title followed by one or more charts or graphs. In your web browser, you can often 'mouse over' parts of the graphs to see additional information. If you wish to print your report, you can do so by using your Web Brower's build in 'Print' functionality, e.g. File → Print or File → Print Preview in Mozilla Firefox.

If the combination of parameters selected and data available in the recorder's database does not provide enough information for Reports to draw a specific graph or table, that graph will be replaced by a 'Not Enough Data' Message in your report. These messages will occur, for example, if you attempt to generate a Month-by-Month Report during your recorder's first month of usage, or attempt to generate a channel-by-channel report and give a channel range which does not have any recordings recorded on it.

Note that Dates and Times specified in Reports are generally in UTC and not your local time zone.

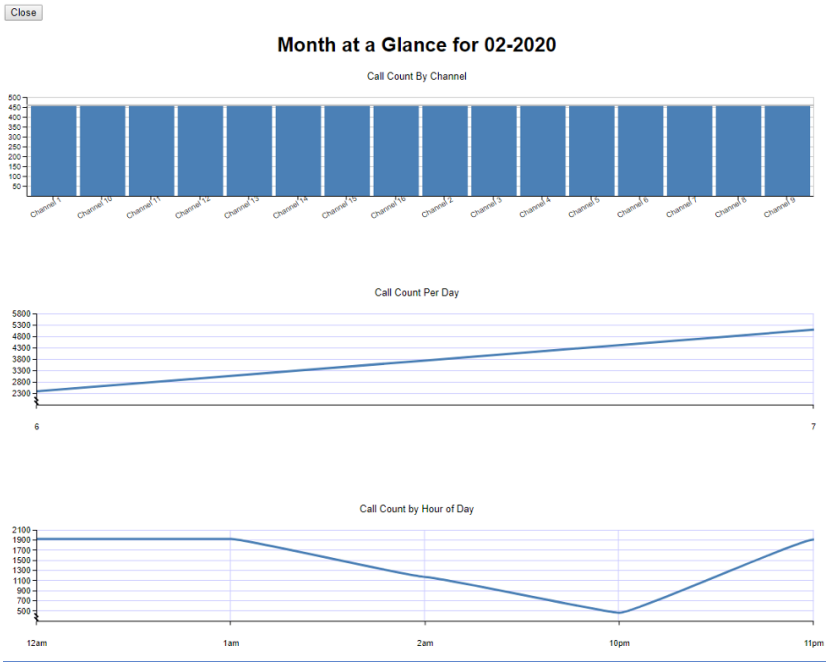


Fig. 7.124 Example Report for *Month at a Glance*

The remainder of this section will discuss some of the specific reports available:

Call Count by Metadata Field

The parameters are a month and year and a Metadata field (Metadata Fields are configured under Recording → Custom Fields). The report will contain a graph showing the call counts of the top 50 values in that metadata field. For example, if you select 'CallerID' as the Metadata field, and January 2020 as your month, you will see a graph of the call counts for each of the 50 most common numbers from which calls were recorded.

Month at a Glance

For this report, you will choose a specific month, such as 'January 2020', and a set of channels on the recorder via a Multiselect List Box. The Report will contain several graphs of call activity during the month on the selected channels broken down in various ways. For example, you will see a bar chart of call count per channel, and line graphs showing call volume by day and call volume by hour-of-day. In addition, you will see a bar chart of "total record time per day' showing how many channel/minutes of data were recorded during a specific day of the specified month on the channels selected.

Duration Outliers

A troubleshooting or abnormality report to show you how many very short or very long recordings were recorded. You select a Start Date and End Date for the report as well as a list of channels to be considered. In addition, you must choose a number of seconds for a recording to be considered 'Too short' or 'too' long for the purposes of the report. You will see per-channel bar charts showing how many calls on each channel were less than or greater than your thresholds in duration as well as the average recording duration for each channel.

Day at a Glance

For this report you select a single day as well as a set of channels you wish to run the report on. The report will contain data such as call count per channel, and call volume per hour of day for the day.

Total Call Records on Recorder per Day

This report shows information about how many total recordings existed on the recorder's hard drives at the end of each day. This takes into effect both new calls being recorded, and old calls being removed from the recorder due to your configured retention settings. Unlike the reports

above, this report's statistics include Recordings that are no longer present on the recorder. The only parameter is a date range of dates to be considered for the report. It shows the total number of recordings in the database each day as well as the total amount of disk space used by those calls each day. In addition, you can see a chart showing the date/time of the oldest recording in the database each day. This can show you where your recorder stands as far as deleting old call records due to your retention settings.

Unarchived Call Report

This shows the same data as the Total Call Records Per day, but only considers call records on the recorder that have not been archived to any Archive Media. It also shows how many hours back from real time your archive pointer is lagging, and how much data is being archived each day. This can help you visualize the progress and state of your Archiving.

7.10. Change Password

This page allows users with the proper permission (Users: CHANGEPASSWORD) to change their own login password. They must enter their new password twice, and press `Submit`.

If the new password does not meet the complexity requirements configured on the recorder, the password change will not be accepted.

8. SOFTWARE LICENSE

The Eventide® NexLog Express Recorder contains proprietary Eventide Firmware and Software. In addition, Eventide MediaWorks and Eventide MediaAgent are proprietary Eventide Software. The Software License for this software follows:

8.1. Product License and Usage Agreement

By installing, copying or otherwise using the Software, you agree to be bound by the terms of this License Agreement. If you do not agree to the terms of this License Agreement, do not use or install the Software.

1. License. YOU (either as an individual or an entity) MAY: (a) use this Software on a single computer; (b) physically transfer the Software from one computer to another provided that the Software is used on only one computer at a time and that you remove any copies of the Software from the computer from which the Software is being transferred; and (c) install a second copy of the Software in the event that the first Software installation is unusable. In addition, the Eventide NexLog Express firmware may only be installed on a purchased and licensed Eventide NexLog Express Recorder.

YOU MAY NOT: (a) distribute copies of the Software or the Documentation to others; (b) modify or grant sublicenses or other rights to the Software; and (c) use the Software in a computer service business, network, time-sharing, or multiple user arrangement without the prior written consent of Eventide.

The License is effective until terminated. You may terminate this License at any time by destroying the Software together with any copies in any form. This Agreement, including the license to use the Software, will terminate automatically if you fail to comply with any term of condition of this Agreement.

2. Ownership. This License is not a sale of the Software or any Firmware contained in the Product. Eventide and its licensors retain all rights, interest, title in and ownership of the Software, Firmware and Documentation, including all intellectual property rights. No title to the intellectual property in the Software and Firmware is transferred to you. You will not acquire rights to the Software and Firmware except as expressly set forth above.

3. No Reverse Engineering and Other Restrictions. You agree that you will not (and if you are a corporation, you will use your best efforts to prevent your employees and contractors from attempting to) reverse engineer, disassemble, compile, modify, translate, investigate or otherwise study the Product

(including, but not limited to any software, firmware, hardware components or circuits) in whole or in part.

4. Inclusion of free software. In addition to Eventide Proprietary Software, this distribution contains free software which is distributed in binary form as well as linked libraries which are licensed under GPL and LGPL licenses respectively. Usage of this software package binds you to the terms of the GPL and LGPL software licenses that can be found below this license agreement in your manual.

5. Compliance with Laws and Indemnification. You agree to use the Product in a manner that applies to all applicable laws in the jurisdiction in which you use the Product, including all intellectual property laws. You may not use the Software or Firmware in conjunction with any device or service designed to circumvent technological measures employed to control access to, or the rights in, a content file or other work protected by the copyright laws of any jurisdiction. You agree to indemnify, defend, and hold harmless Eventide from and against losses, damages, expenses, (including reasonable attorneys' fees), fines, or claims arising from or relating to any claim that the Product was used by you to violate, either directly or indirectly, another party's intellectual property rights.

6. Limited Warranty on Software. Eventide warrants that the media on which the Software is furnished will be free from defects in materials and workmanship under normal use for a period of ninety (90) days from the date of purchase. If a defect appears during the warranty period, return the diskette/compact disc to Eventide, and you will receive a free replacement, or at Eventide's option, a refund, so long as the Software, documentation, accompanying hardware, and diskettes are returned to Eventide with a copy of your receipts. This Limited Warranty is void if failure of the Software has resulted from accident, abuse, or misapplication. Any replacement Software will be warranted for the remainder of the original warranty period. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH VARY BY JURISDICITON.

7. No Other Warranties. Eventide AND ITS LICENSOR(s) (hereafter collectively 'Eventide') DO NOT WARRANT THAT THE Eventide SOFTWARE NOR ANY THIRD-PARTY SOFTWARE EMBEDDED ON THE DISK (collectively 'SOFTWARE') ARE ERROR FREE. YOU EXPRESSLY ACKNOWLEDGE THAT THE SOFTWARE AND DOCUMENTATION ARE PROVIDED AS IS. EVENTIDE DISCLAIMS ALL OTHER WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OF THIRD PARTY RIGHTS WITH RESPECT TO THE SOFTWARE, THE ACCOMPANYING DOCUMENTATION OR DISKETTES.

8. No Liability for Consequential Damages. IN NO EVENT SHALL EVENTIDE BE LIABLE TO YOU FOR ANY CONSEQUENTIAL, SPECIAL, INCIDENTAL OR INDIRECT DAMAGES OF ANY KIND ARISING OUT OF THE USE OF THE PRODUCT, EVEN IF Eventide HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. EVENTIDE'S LIABILITY FOR ANY CLAIM, LOSSES, DAMAGES OR INJURY,

WHETHER CAUSED BY BREACH OF CONTRACT, TORT OR ANY OTHER THEORY OF LIABILITY, SHALL NOT EXCEED THE FEE PAID BY YOU. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES OR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSIONS MAY NOT APPLY TO YOU.

9. Export. You acknowledge that the laws and regulations of the United States restrict the export and re-export of the Software and Documentation. You agree the Software will not be exported or re-exported without the appropriate U.S. or foreign government licenses. You also agree not to export the Software (including over the Internet) into any country subject to U.S. embargo.

10. Governing Law and Arbitration. This Agreement will be governed by the laws of the State of New Jersey and will be interpreted as if the agreement were made between New Jersey residents and performed entirely within New Jersey. All disputes under this Agreement or involving use of the Product shall be subject to binding arbitration in Little Ferry, NJ in accordance with the commercial arbitration laws of the American Arbitration Association. Notwithstanding anything contained in this Paragraph to the contrary, Eventide shall have the right to institute judicial proceedings against you or anyone acting by, through, or under you, in order to enforce Eventide's rights hereunder through reformation of contract, specific performance, injunction or similar equitable relief.

11. Entire Agreement. This is the entire agreement between you and Eventide AND supersedes any prior agreement, whether written or oral, relating to the subject matter of this Agreement. No amendment or modification of this agreement will be binding unless in writing and signed by a duly authorized representative of Eventide.

12. Government End Users. U.S. GOVERNMENT RESTRICTED RIGHTS. The Software and Documentation were developed at private expense, and are commercial computer software and commercial computer software documentation. If you are a U.S. Government agency or its contractor, pursuant to FAR 12.212(a) and/or DFARS -227.7202-1(a) and their successors, as applicable, use, duplication or disclosure by the Government of the Software and Documentation is subject to the restrictions set forth in this Agreement.

ALL FEATURES AND SPECIFICATIONS SUBJECT TO CHANGE WITHOUT NOTICE.

In addition to the proprietary Eventide software, some of the base underlying substructure of the firmware is provided by the Linux Kernel and the corresponding Open Source licensed Userspace. These components are not under the proprietary Eventide License, but under their own software licenses. Many of these packages are released under the GNU General Public License or the GNU Lesser General Public License. Note that none of the Eventide software that provides the recorder functionality is under this license nor is it linked into any software under this license. This license only protects the basic

underlying Operating System internally used by the NexLog Express recorder. Please see *IP address*/copyrights.txt file on any recorder for more information about the open source packages used and their respective licenses. The text of the GNU GPL v2 is provided here for convenience:

8.1.1. GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA

Everyone is permitted to copy and distribute verbatim copies

of this license document, but changing it is not allowed.

8.1.2. Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software–to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

8.1.3. TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and “any later version”, you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

8.1.4. END OF TERMS AND CONDITIONS

8.1.5. How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the “copyright” line and a pointer to where the full notice is found.

one line to give the program’s name and an idea of what it does.

Copyright (C) *yyyy name of author*

This program is free software; you can redistribute it and/or

modify it under the terms of the GNU General Public License

as published by the Free Software Foundation; either version 2

of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful,

but WITHOUT ANY WARRANTY; without even the implied warranty of

MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the

GNU General Public License for more details.

You should have received a copy of the GNU General Public License

along with this program; if not, write to the Free Software

Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) *year name of author*

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details

type `show w'. This is free software, and you are welcome

to redistribute it under certain conditions; type `show c'

for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and`show c'; they could even be mouse-clicks or menu items–whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright

interest in the program `Gnomovision'

(which makes passes at compilers) written

by James Hacker.

signature of Ty Coon, 1 April 1989

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License

By receiving a copy of these GPL components, this license grants you the legal right to gain access to the source code of said components. Source Codes can be downloaded at http://debian.org or directly from Eventide service@eventidecommunications.com

This page was intentionally left 99.88% blank.

A. SOFTWARE INSTALLATION AND UPGRADE

Software Upgrades are made available for NexLog Express regularly. They include new features, system security updates, and refinements.

Just as with any computer, Eventide NexLog Express Recorders require a software operating system and a number of application programs to be functional and to perform useful work. The operating system in this case is Linux, and the application programs are a combination of standard programs and programs written and maintained by Eventide to work with its custom hardware environment.

As part of the manufacturing process, Eventide installs the recorder software. Because the recorder software development is an on-going process, Eventide occasionally creates software upgrades to bring older recorders up to the current software version. It is sometimes desirable or even necessary to apply these upgrades to recorders at the customer site, and the purpose of this section is to explain the process so that customers can confidently perform upgrades (and even installations) without factory intervention.

A.1. Why Re-Installation May Be Necessary

The recorders use redundant disks, so a single drive failure should not cause loss of data or software. However, if multiple disks in an array fail due to a common cause (e.g., lightning or other power surge), you will have to re-install the software when they are replaced.

A.2. Why Upgrades May Be Necessary or Desirable

There are several reasons why you may need to do an upgrade:

- Hardware upgrades or changes require new software
- Valuable features are available in the new release
- Factory support requires a more recent software version
- Problems (bugs) are found in the version currently running

A.3. The Software Upgrade/Installation Process

The actual process of upgrading (or re-installing) your software is simple and much of it is automated. It goes like this:

First, prepare for upgrading by:

1. Archive your call data!
2. Archive your recorder configuration!
3. Remove all archive media.

Second, choose an upgrade method:

Using the Front Panel of the recorder:

- Boot to an Eventide Software Distribution DVD-ROM, at the front panel. This is the only way to do a fresh install that overwrites all data on the recorder, but it can also be used to upgrade the recorder.

Using Configuration Manager via a web browser:

- Upload Full Upgrade Image from your Desktop: Upload an upgrade.zip file and reboot the recorder to upgrade. The file name must fit the pattern “NexlogDX-20##.#[#]upgrade.zip” (for example “NexlogDX-2021.2[314]upgrade.zip”) and will be verified as a real upgrade file before a reboot takes place.

From the Front Panel or Configuration Manager:

- Download Full Upgrade Image from Eventide VPN Server: This will end with (VPN Not Connected) if VPN settings have not been configured and enabled.
- Import Full Upgrade Image from an Archive Drive: If you have an NexlogDX-202X.X[XXX]-upgrade.zip image on a USB drive or blu-ray, you can insert it into the recorder and upgrade with this option.

A.3.1. Booting DVD Installation Media

1. Insert the Eventide software distribution DVD-ROM in the top DVD drive.
2. Power down the recorder.
3. Restore power.
4. Wait until the software loads.

5. You should see a page that looks like this:

Fig. A.1 Installer/Upgrader

1. If installing, click Install, and see the Install specific instructions below. This will erase all data on the recorder.
2. If upgrading, it should correctly identify your software. Click upgrade to continue. A page like this one will appear:

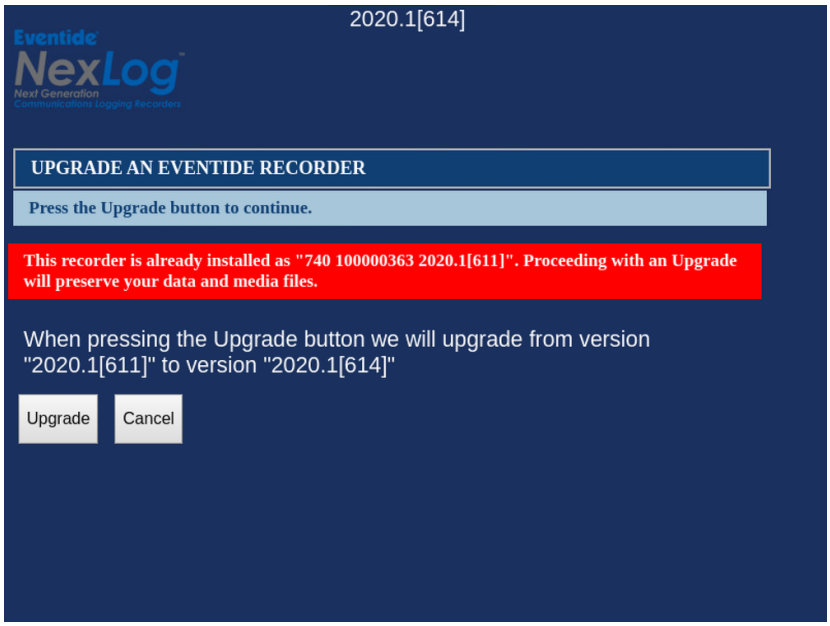


Fig. A.2 Upgrade

1. Click Upgrade and the upgrade will begin.
2. When finished, the DVD-ROM will eject automatically. Remove it from the tray.
3. Touch the touch screen or hit enter to reboot.
4. Wait until the new software completes its initialization.

Important

You may need to wait 20 minutes or more for an upgrade. Average wait time is under 10 minutes.

A.3.1.1. Install Specific Instructions

1. After clicking Install, you will see a page like this:

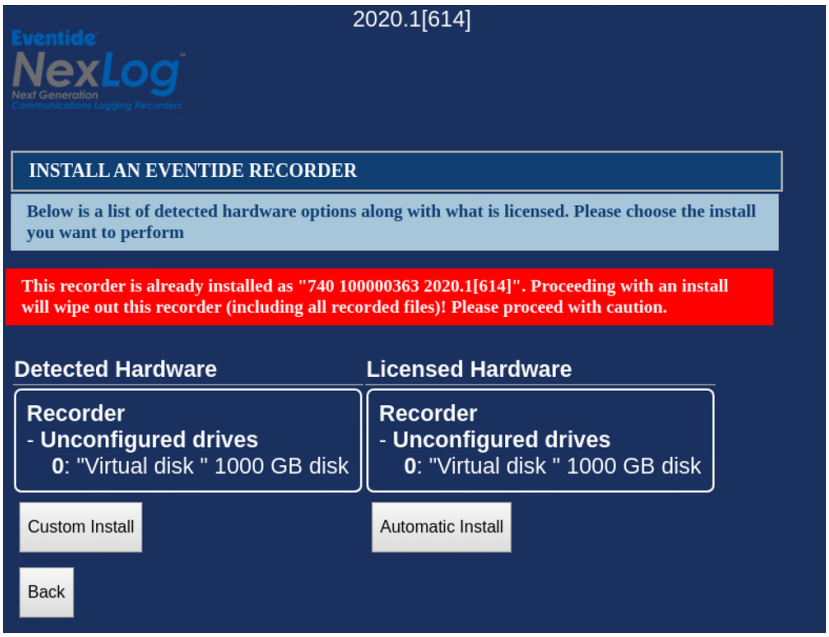


Fig. A.3 Install

1. Unless Eventide Service or your dealer tells you otherwise, click Automatic Install.
2. The Install will then begin.
3. When finished, the DVD-ROM will eject automatically. Remove it from the tray.
4. Touch the touch screen or hit enter to reboot.
5. Wait until the new software completes its initialization.
6. Restore your configuration.
7. Restore your archives, beginning with the most recent first.

This completes the procedure.

A.3.2. Upload Full Upgrade Image from your Desktop

Upload Full Upgrade Image from your Desktop: Upload an upgrade.zip file and reboot the recorder to upgrade. The file name must fit the pattern “NexlogDX-2020.1[601]-upgrade.zip” and will be verified as a real upgrade file before a reboot takes place.

You have the option to set this to automatically reboot and apply the upgrade once upload and verification of the image is completed. If you leave this unset, reboot manually from the System: Power Off page when ready to upgrade.

Important

You may need to wait 20 minutes or more for an upgrade. Average wait time is under 10 minutes.

A.3.3. Download Full Upgrade Image from Eventide VPN Server

If the recorder is configured to have VPN access to Eventide, you can kick off an upgrade from here. This option will show (VPN Not Connected) if VPN settings have not been configured and enabled.

A.3.4. Import Full Upgrade Image from an Archive Drive

Copy NexlogDX-202X.X[XXX]-upgrade.zip image on a USB drive or blu-ray, insert to the recorder and use the System: Upgrade Recorder Software page to apply this upgrade to the recorder by selecting this option. It will offer a list of all Eventide Upgrade Media present in the recorder. Select one of these and proceed to select which upgrade image on the drive to upgrade to.

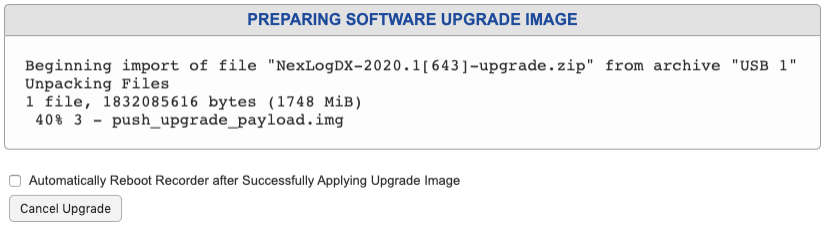


Fig. A.4 USB Upgrade In Progress, with Automatic Reboot Option

You have the option to set this to automatically reboot and apply the upgrade once upload and verification of the image is completed. If you leave this unset, reboot manually from the System: Power Off page when ready to upgrade.

A.4. Some Details, Especially About Installation

If you do an install on top of an existing system, all your calls will be erased. If you have archived your calls, you can restore them as described in the next section. An upgrade will leave your calls in the same state as they were earlier.

If you do a new installation, you will have to reconfigure the recorder in accordance with the setup instructions. This is greatly simplified by the “Read/Write Configuration to Archive” feature. Please read the information in SETUP carefully before you start the installation!

If you upgrade the recorder, be sure to read the release notes or other information to see if there are any new SETUP items that must be configured.

A.4.1. Restoring Archives When Installing New Software

In the Archiving section of the SETUP mode there is a menu item “Archive restore.” If you insert previously recorded archive media into one or more drives, it will allow you to select that drive with the knob and perform a restore operation; i.e., copy the calls from that medium back to RAID. Several checks are performed before the medium is transferred:

- Does the serial number of the recorder that recorded the archive medium agree with that of the destination recorder?
- Are the channel names of the recorder the same as the destination?
- Does the format of the data on the archive conform to that of the destination?
- Is there any problem with or damage to the archive medium data to be transferred?
- Are any of these calls duplicates of calls already on the recorder?
- User confirmation: Are you sure you want to go ahead with the transfer?

If none of these apply to the medium, or if you indicated that you wish to proceed anyway, the archive transfer will commence. All drives operate independently. You can restore archive media in all available drives, or you can even record archives on one medium while restoring from another.

Important

The restoration process will delete the oldest calls on the recorder to make room for the restored calls. In some cases, this will be the calls being restored. Always restore from the most recent archive backwards.

If you are restoring archives after a new installation, set the current archive time *to make sure that new archives are only recorded from the present forward*. If you don’t set this and begin new archiving after you have restored your archives from a previous installation, you might find yourself “re-archiving” the restored archives.

A.4.2. Potential Issues

For the most part, the process is automated. At least for an upgrade, beyond inserting/removing the disk, removing/applying power, and exhibiting patience, there is little for you to do.

One problem that can occur is failure to recognize the medium in the upgrade drive (the one in which you place the DVD). If this happens, the recorder just powers up normally and the DVD never ejects. In such a case, manually eject the DVD, and again shut down the unit. Next, visually inspect the medium, confirm it has no scratches, it's clean, it's right-side-up, and it's carefully centered in the drive tray. Then try again. If the drive persistently refuses to recognize the DVD, yet works correctly when archiving, you probably have a defective upgrade DVD, or one that differs enough from the drive's calibration to make reading the DVD problematic. You can try copying the DVD-ROM to another blank one, burning a new one, requesting a replacement, etc.

Much less common: The DVD can't be read completely, and the upgrade/install process hangs up and the DVD does not eject. In this case, try the procedure again from the beginning. For an installation, no damage will be done as long as the install eventually completes correctly. For an upgrade, there is a possibility that configuration information will have been lost, in which case it can be restored manually or from the configuration archive that you made before starting the upgrade. Do NOT, however, try to resume normal recorder operation until the upgrade has completed normally.

Note: Please read the release notes. Software upgrades will normally come with printed information, and possibly with a README file on the disk. If anything in the release notes contradicts something you read here, go with the release notes!

B. INSTALLATION FROM USB

NexLog Express software upgrades and clean installations can be completed via optical media, or USB. In instances where an optical drive or media is not available, a USB flash drive can be used.

B.1. Installation Prerequisites

These instructions assume that you are using a Microsoft Windows 1 computer. You may use another operating system, but the process may differ.

You must have the following to perform an installation via USB flash:

- 4GB or higher USB flash drive (USB 3.0 preferred)
- NexLog Express ISO installation file
  - Can be downloaded from the Eventide Communications Partner Resource Site https://www.eventidecommunications.com/downloads
- Rufus 2 v3.13 or newer https://rufus.ie/
- Keyboard, Mouse, Display

B.2. Create Bootable USB

After inserting the USB flash media into your PC, open the Rufus application.

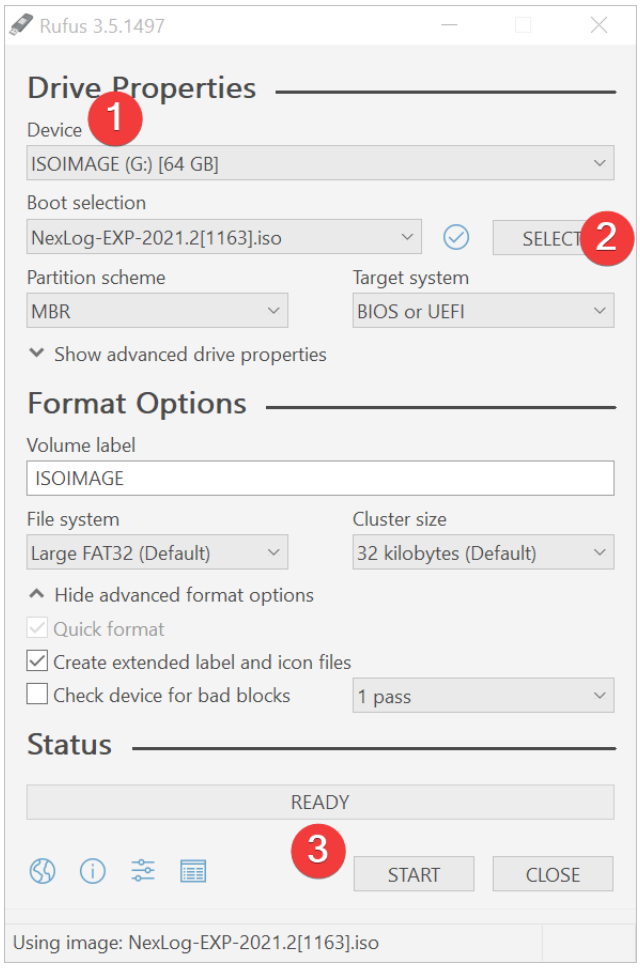


Fig. B.1 Rufus ISO writing utility

1. From the `Device` dropdown, select your USB flash media.
2. In the `Boot selection` section, press the `SELECT` button.
    1. In the file browser window, open the ISO installer file.
3. Ensure that the other options match Fig. B.1, then press the `START` button.

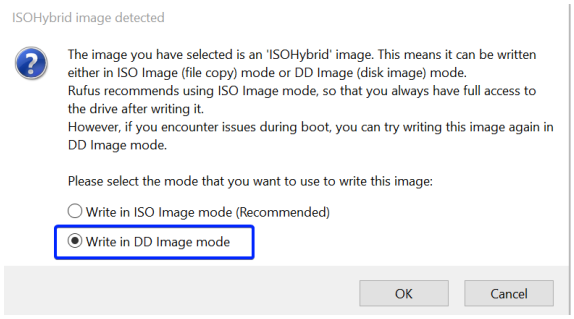


Fig. B.2 Rufus ISOHybrid mode selection

1. A prompt may appear to select the write mode, you should select `Write in DD Image mode` when this appears.

4. When the Rufus has finished, safely eject the USB flash media from the PC.

B.3. Booting from USB

When the NexLog Express is powered off, you can insert the bootable USB flash media into one of its available USB ports.

> **Tip**
>
> If you used USB 3.0 flash media, one of the blue colored USB ports will allow for a faster installation.

If a keyboard, mouse, and display are not already connected to the system, you will need to do so now.

1. Power on the system and repeatedly press `F11` on the keyboard to invoke the boot menu.

2. A menu should appear to *select a boot device*. Using the arrow keys on your keyboard (`↓` `↑`), select `USB DISK 3.0 PMAP`, then press `enter`.

Fig. B.3 Boot device selection menu

3. The system should boot to the NexLog Express installation wizard. The standard upgrade/ installation process can now be followed.

---

1 Microsoft® and Windows® are trademarks or registered trademarks of Microsoft Corporation.

2 Rufus is GNU GPL 3+ licensed and rufus.ie is copyrighted by Pete Batard

C. CHANNEL WIRING FOR ANALOG INPUT BOARDS

All Eventide NexLog Express recorders that are equipped to record analog telephone calls (POTS) are furnished with one or more analog input boards. Eventide provides 8-, 16-, and 24-channel analog input boards. Boards of any channel count will contain standard pin-outs on the Telco connector.

For standard pin-out assignments, see Table C.1: Analog Board Standard Pin-Outs (8-, 16-, and 24-Channel Boards) below.

The Eventide Quick Install Kits available for these boards come with cables that compensate (if necessary) for the pin ordering so that when wiring the punch down blocks, the lines are in order according to normal telephone company practice. Contact your Eventide representative to purchase your Quick Install Kit.

Table C.1 Analog Board Standard Pin-Outs (8-, 16-, and 24-Channel Boards)

Chan	Pins	Chan	Pins	Chan	Pins	Chan	Pins	Chan	Pins	Chan	Pins
1	1 + 26	5	5 + 30	9	9 + 34	13	13 + 38	17	17 + 42	21	21 + 46
2	2 + 27	6	6 + 31	10	10 + 35	14	14 + 39	18	18 + 43	22	22 + 47
3	3+ 28	7	7 + 32	11	11 + 36	15	15 + 40	19	19 + 44	23	23 + 48
4	4 + 29	8	8 + 33	12	12 + 37	16	16 + 41	20	20 + 45	24	24 + 49

This page was intentionally left 99.88% blank.

D. ALERT CODES

In the course of operation, the recorder may generate a variety of alerts, which are messages about aspects of the system operation. These messages have different severity levels that range from informational messages to severe errors. You can configure how alert notification is handled, as well as other alert features.

This section describes how to configure alert notification, including where to display and email the alerts. It also provides the following information about alert messages:

- Table D.1 — Alert Severity Levels: A list of alert severity levels and descriptions.
- Table D.2 — Alert Messages: A list of alert messages, including the alert code, severity level, & message text.

Resolved alerts are not new alerts (and are not Info alerts). MediaWorks receives only active alerts. Active alerts are resolved by a system process (e.g., when you replace a RAID), and are established by the RequireResolution flag (system centric name). Non-active alerts are one-time alerts that are not resolved by the system and may require user intervention. Most alerts are active alerts (~30 non-active).

Table D.1 Alert Severity Levels

Level	Name	Description
1	Info	An informational message or notice that does not require acknowledgement. Example: Alert #8, “Recorder Startup.”
2	Warning	Indicates trouble. Example: Alert #6004, “Primary RAID mount failed and the recorder recovered when secondary mount succeeded.”
3	Error	Indicates an error that could result in possible loss of data. Example: Alert #5010, “The UPS on recorder <name> was found but is not functioning properly.”
4	Severe Error	Indicates a serious problem. Example: Alert #9024, “Analog input Board <name> has malfunctioned and has been disabled.”

Table D.2 Alert Messages

CODE	ALERT TEXT	SEVERITY
0	blank	INFO
1	The system has received a test alert	INFO
2	The system has received a test alert(Auto Resolution)	INFO
3	The system has received a test alert(Manual Resolution)	INFO
5	The recorder <~1~>, has lost the network connection	WARNING
7	the <~110~> archive drive has been removed or is not functioning.	ERROR
8	Recorder Startup	INFO
9	The process <~110~> has malfunctioned on recorder <~1~>. No data loss or user intervention is expected.	INFO
10	The process <~110~> has malfunctioned on recorder <~1~>. Secondary systems may temporarily behave unexpectedly. No data loss or user intervention is expected	ERROR
11	The process <~110~> has malfunctioned on recorder <~1~>. The system is attempting to recover. Recent Data may have been lost	ERROR
14	The recorder was not properly shut down. This can cause serious loss of data. The shutdown time was approximately <~110~>.	WARNING
15	Recorder Shutdown	INFO
16	An error occurred while shutting down the system. Current archived data may be damaged.	WARNING
18	The system has detected a time change on the recorder. The time has changed from <~110~> to <~111~> in the elapsed time of <~112~> seconds. This may be normal.	INFO
21	Recorder time is not synchronized to any configured time source.	INFO
22	At least one configured time source is not currently reachable.	INFO
23	The process <~110~> has been manually terminated	INFO

CODE	ALERT TEXT	SEVERITY
24	<~110~><~111~><~112~><~113~>	INFO
25	This is a test email sent from recorder <~1~> at facility <~2~>	INFO
26	The system temperature of recorder <~1~> has exceeded the normal operating range. The system temperature is <~110~> C.	ERROR
27	Network cable unplugged	INFO
27	Network cable unplugged	INFO
28	Unable to contact ntpd.	INFO
50	Initial version <~110~> installed at <~111~>	INFO
51	Upgrade to version <~110~> from version <~111~> completed at <~112~>	INFO
52	The recorder does not have a valid license key. You are currently on day <~110~> of your 7 day grace period.	WARNING
53	The recorder does not have a valid license key. After a 7 day grace period, certain recorder functionality will be blocked until a valid license key is entered.	ERROR
54	The recorder has recorded calls that are later than the current recorder time. These calls will not get archived and may cause problems when you attempt to display them. Check the system clock and time zone. Contact Eventide for further info.	INFO
55	A valid license key has been entered.	INFO
56	An Integrated Metadata feed went <~110~> minutes without providing data.	WARNING
57	Configured Feature Add-on “<~110~>” exceeds the capabilities licensed	WARNING
58	Push upgrades to previous versions are not supported. Current version is “<~110~>” and an upgrade was attempted to version “<~111~>”	WARNING
59		ERROR

CODE	ALERT TEXT	SEVERITY
	The Metadata feed for channel <~110~> appears to be missing. <~111~> calls were recorded without providing metadata.	
60	Local RTP Engine Config Issue: <~110~>	ERROR
61	Recorder running inside VMWare, but no Keylok Dongle Found or No License key allowing Virtualization installed on Recorder.	SEVERE
62	The system hardware is not in the configuration database. The hardware has been identified as <~110~>	ERROR
63	Configured Feature Add-on "<~110~>" exceeds the capabilities licensed	WARNING
64	The operating system detected a fault and needed to be restarted.	ERROR
65	Remote vocoder is not responding: host <~110~>'	INFO
66	Remote vocoder encounterd an error: <~110~>'	INFO
67	The Recorder is contains an expired temporary addon license key	INFO
100	Kernel stopped process <~110~> : <~111~>	SEVERE
100	Kernel stopped process <~110~> : <~111~>	SEVERE
101	Initialization Error for Component: <~110~> : <~111~>	ERROR
102	The CPU temperature of recorder <~1~> has exceeded the normal operating range. The CPU temperature is <~110~> C.	ERROR
1002	A database record event failed. This is likely the result of a misconfigured integration. Please contact your dealer for assistance. Type: <~111~> ,Error: <~110~><~112~><~113~>	WARNING
1003	Calls are being removed from the hard disk without ever having being archived. The calls currently being deleted started on <~110~>	INFO
1004	Space used on hard disk has reached an upper limit. Normal operation continues, with new recordings now replacing the oldest recordings on disk, starting with <~110~>	INFO

CODE	ALERT TEXT	SEVERITY
1005	A small amount of data may have been lost from channel <~110~> on the call that started at <~111~>. This data loss may not be noticeable.	WARNING
1006	Calls are not being recorded due to a recording problem. Error:<~110~>	WARNING
1007	Failed to read configuration from the database. A possible corruption exists. Please contact Eventide. Error:<~110~>	SEVERE
1008	Data inconsistent on channel <~110~>. This may have occured because of process restart or delayed read of data. Last block read was <~111~> but found <~112~>.	ERROR
1009	Failed to upgrade the database. The system will continue to run with an older version of the database. Please contact Eventide to resolve this issue. Error:<~110~>	WARNING
1010	The system has pending database activity that has been queued for more than two minutes. Recordings may not appear in real time but are being recorded.	INFO
1011	The system has pending database activity that has been queued for more than two hours. Recordings may not appear in real time but are being recorded.	INFO
1012	A processing timeout has occured while recording data.	ERROR
1013	Recordings that are scheduled for preservation are close to being deleted.	WARNING
1014	The user storage partion for <~110~> is full. This must be resolved by either deleting stored items or increasing storage settings via the Configuration Manager → Recording → Retention Settings. You will not be able to <~111~> until this is resolved. This issue does not affect recording.	WARNING
2001	The media in the <~111~> archive drive is almost full	INFO
2002	The media with id <~110~> in the <~111~> archive drive of recorder <~1~> is full	INFO
2004	Warning: the operation of <~110~> was performed when the drive was in a bad state. Please retry the operation	INFO

CODE	ALERT TEXT	SEVERITY
2005	System configuration saved to the <~110~> archive drive	INFO
2006	System configuration was NOT saved to the <~110~> archive drive: <~111~>	WARNING
2006	System configuration was NOT saved to the <~110~> archive drive: <~111~>	WARNING
2007	System Logs have been successfully saved to the <~110~> archive drive	INFO
2008	System Logs were NOT saved to the <~110~> archive drive: <~111~>	WARNING
2009	System configuration was restored.	INFO
2010	System configuration was NOT loaded from the <~110~> archive drive because of the error: <~111~>	WARNING
2011	Metadata backup failed for backup type <~110~>. Error: <~111~><~112~>.	WARNING
2014	Writing archive to the <~110~> archive drive failed. Please dismiss this message by hitting the 'OK' soft key, insert new media into the <~110~> archive drive and then hit the 'resume' soft key to retry.	INFO
2016	The current archive time has been changed on the recorder from <~110~> to <~111~>.	INFO
2017	<~110~> archive drive action: <~111~>.	INFO
2019	Call Meta Information saved to the <~110~> archive drive	INFO
2020	Call Meta Information was NOT saved to the <~110~> archive drive: <~111~>	WARNING
2021	Call Meta Information was loaded from the <~110~> archive drive.	INFO
2022	Call Meta Information was NOT loaded from the <~110~> archive drive because of the error: <~111~>	WARNING
2024	The <~110~> archive drive medium was improperly removed and may be damaged. The recorder will attempt to recover but some data loss is	ERROR

CODE	ALERT TEXT	SEVERITY
	possible. In the future please use the Eject soft key and wait for the drive status to read “Safe To Remove Media”.	
2025	The recorder <~1~> is not archiving.	INFO
2026	The recorder <~1~> does not appear to be archiving properly. The recorder is recording calls, but they do not appear to be archived. This may be because of a time change on the system or other normal activity. If you believe this is a problem, please stop archiving and restart it.	WARNING
2027	All media on the recorder <~1~> is either full or in the wrong state to continue archiving	INFO
2030	The media loaded in the <~110~> archive drive is damaged. Error: <~111~>	INFO
2031	The media in the <~110~> archive drive with the start time of <~111~> and the end time of <~112~> has encountered a problem while saving data. The archive media may be faulty or damaged. Please insert new media and archive again. The system archive time has not been changed.	WARNING
2032	Archive media format failed on the <~110~> archive drive. Please check that the media is not write protected or damaged. Error: <~111~>	INFO
2033	A media error was encountered while loading the <~110~> archive drive to browse mode. The archive media may be damaged and have missing or incomplete calls. This error could be caused by defective media or an improper system shutdown. The archive has the start time <~111~> and end time <~112~>	INFO
2033	A media error was encountered while loading the <~110~> archive drive to browse mode. The archive media may be damaged and have missing or incomplete calls. This error could be caused by defective media or an improper system shutdown. The archive has the start time <~111~> and end time <~112~>	INFO
2200	Failsafe is not active for the recorder group <~110~>.	WARNING
2201	Archive Failsafe is armed for the recorder group <~110~>	INFO

CODE	ALERT TEXT	SEVERITY
2202	Archive Failsafe has been triggered on the recorder group <~110~> at archive position <~111~>. Error: <~112~>	WARNING
2203	The recorder <~1~> has been placed in standby mode for the group <~110~>.	INFO
2204	Archive Restore complete on the <~110~> drive of recorder <~1~>	INFO
2300	Network Archive connected to address <~110~>, share <~111~>	INFO
2301	Network Archive to address: <~110~>, share: <~111~> is NOT active. <~112~><~113~>	WARNING
2302	Network Archiving connection to address: <~110~>, share: <~111~> is not active. Error: <~112~><~113~>	WARNING
2400	Centralized Archiving is not connected to <~110~>. Error: <~111~>	ERROR
2401	The recorder at <~110~> is transferring duplicate calls. This may be because the archive pointer was reset.	ERROR
2402	The Centralized Archive source with serial number <~110~> is not connected	ERROR
3001	Channel <~110~> was active for more than <~111~> seconds.	INFO
3002	Channel <~110~> was inactive for more than <~11~> days <~12~> hours <~13~> minutes.	INFO
5000	Communications with the UPS backup power supply has been lost on the recorder <~1~> in facility <~2~>. Please ensure that the UPS is properly connected to the recorder	WARNING
5002	Power has been lost on the recorder <~1~> in the facility <~2~>. The UPS is currently providing power	WARNING
5005	Power has not been restored on the recorder <~1~> in the facility <~2~> and will be shut down shortly	WARNING

CODE	ALERT TEXT	SEVERITY
5008	The battery on UPS <~110~> has been exhausted. Recorder <~1~> is being shut down.	WARNING
5010	The UPS on recorder <~1~> was found but is not functioning properly	ERROR
5013	UPS is attached and functioning normally	INFO
5014	UPS is not attached to the recorder or not working properly	INFO
5014	UPS is not attached to the recorder or not working properly	INFO
5015	UPS battery is not functioning properly. Please test battery to ensure proper functionality.	INFO
6000	The hard disk <~110~> has failed on the recorder <~1~>. Please fix it	SEVERE
6001	RAID on recorder <~1~> is degraded. Replace the failed drive to correct the issue.	SEVERE
6002	The RAID has been changed: <~110~>	INFO
6003	The recorder <~1~> has a storage partition(<~110~>) that is dangerously close to being full(<~111~>). This is not a normal condition and should be resolved immediately to prevent possible data loss.	WARNING
6004	Primary RAID mount failed, and the recorder recovered when secondary mount succeeded.	WARNING
6005	The recorder <~1~> had a bad file system journal on volume group <~110~>. The problem was automatically fixed, but this condition is not normal and may have resulted in data loss.	WARNING
6006	The hard disk <~110~> is close to failure on <~1~>. Please replace it as soon as possible.	ERROR
6007	The hard disk <~110~> has timed out responding to the RAID controller on <~1~>. Please replace it as soon as possible.	ERROR
6008	The RAID Controller Write Cache is Disabled.	ERROR
6009		ERROR

CODE	ALERT TEXT	SEVERITY
	The RAID Controller Battery Backup for recorder <~1~> is reporting excessive heat.	
6010	The RAID Controller Battery Backup voltage is low.	ERROR
6011	The RAID Controller Battery Backup is offline and not providing backup to the RAID.	ERROR
6012	The RAID Controller Battery Backup is reporting a bad status.	ERROR
6016	RAID rebuild in progress.	INFO
6020	RAID on recorder <~1~> is degraded, there is a mismatch between drives defined and drives found.	SEVERE
7000	A problem occurred while sending email. Error <~110~>: <~111~>	INFO
7001	An unknown error code of <~110~> was received	INFO
7002	An email has been sent to <~110~><~111~> with the subject “<~112~>”	INFO
7003	The alert <~110~> has been acknowledged by user <~111~>	INFO
8001	The user <~110~> has requested a system shutdown	INFO
8002	The user <~110~> has been automatically logged out	INFO
8002	The user <~110~> has been automatically logged out	INFO
8003	Client login with username <~110~>, version <~111~>, client string <~112~>	INFO
8004	Client has logged out with username <~110~>	INFO
8005	Client login has failed with username <~110~>	INFO
8006	The system time has been changed on recorder <~1~> by user <~110~>. The old time was <~111~>. The new time is <~112~>	INFO
8007	Configuration change by user <~110~>: <~111~>	INFO
8008	Shutdown requested via key. Please wait.	INFO

CODE	ALERT TEXT	SEVERITY
8009	Archive Failsafe Mode Canceled by user <~110~>.	INFO
8010	One or more PC Workstations configured for monitoring are not responding to network requests. <~110~>	WARNING
8011	One or more PC Workstations has an outdated screen capture service. This may result in service instability and loss of data on <~110~>	WARNING
9000	The board of type <~110~> has failed on recorder <~1~>. The failed board is board number <~111~>. It has failed <~112~> times	SEVERE
9001	A recording board has been removed or is missing from the system	SEVERE
9002	Failed to open the board of type <~110~> in position <~111~>. Error: <~112~>	SEVERE
9003	Failed to configure the board of type <~110~> in position <~111~>. Error <~112~>	SEVERE
9004	DSP sync Error on the board of type <~110~> in position <~111~>. Sync error count is <~112~>. Over run count is <~113~>	WARNING
9005	Failed to configure port <~112~> on the board of type <~110~> in position <~111~>. Error <~113~>	SEVERE
9006	Signal lost on port <~112~> on the board of type <~110~> in position <~111~>	ERROR
9007	Frames lost on port <~112~> on the board of type <~110~> in position <~111~>	ERROR
9008	AIS alarm on port <~112~> on the board of type <~110~> in position <~111~>	WARNING
9009	Yellow alarm on port <~112~> on the board of type <~110~> in position <~111~>	WARNING
9010	LOSMF alarm on port <~112~> on the board of type <~110~> in position <~111~>	WARNING

CODE	ALERT TEXT	SEVERITY
9010	LOSMF alarm on port <~112~> on the board of type <~110~> in position <~111~>	WARNING
9011	LOCRC4MF alarm on port <~112~> on the board of type <~110~> in position <~111~>	WARNING
9012	TS16RAI alarm on port <~112~> on the board of type <~110~> in position <~111~>	WARNING
9013	Failed to open channel <~111~> on the board of type <~110~>. Error: <~112~>	WARNING
9014	Failed to configure channel <~111~> on the board of type <~110~>. Error: <~112~>	WARNING
9016	No signal present on channel <~111~> on the board of type <~110~>.	WARNING
9017	Recording could not be started on channel <~111~> on the board of type <~110~>.	WARNING
9018	Recording could not be stopped on channel <~111~> on the board of type <~110~>.	WARNING
9019	Read timeout on channel <~111~> on the board of type <~110~>.	ERROR
9020	Read fail on channel <~111~> on the board of type <~110~>.	ERROR
9021	Continuity check error on channel <~110~>.	ERROR
9022	The continuity number is not being updated on channel <~110~>.	SEVERE
9023	<~110~>(<~111~>) has not been heard from in <~112~> seconds. The recorder may not be recording.	SEVERE
9024	Analog Telephony Board <~110~> has malfunctioned and has been disabled	SEVERE
9025	Recording Interface is configured as disabled and not recording. Enable the device to begin recording	SEVERE
9026		WARNING

CODE	ALERT TEXT	SEVERITY
	One or More Digital PBX Channels are receiving a large number of line errors. Please check your wiring and phonesets	
9100	The recorder is experiencing a connection error with the remote gateway at address <~110~>. Error: <~111~>	ERROR
9101	The recorder lost the connection to the remote gateway at address <~110~>.	ERROR
9102	The Remote Gateway at address <~110~> contains a backlog of data that is <~111~> minutes old. The data is currently being uploaded	ERROR
9103	The time on the Remote Gateway at address <~110~> differs from the recorder time by <~111~> seconds. Please insure that NTP is running on the Remote Gateway and recorder	ERROR
9104	The screen channel with name “<~110~>”:<~111~> at address <~112~> is not connected. Error: <~113~>	ERROR
9104	The screen channel with name “<~110~>”:<~111~> at address <~112~> is not connected. Error: <~113~>	ERROR
9105	Screen Agent @<~110~>: <~111~>	WARNING
9110	The recorder is experiencing a connection error to the bridged recorder at address <~110~>. Error: <~111~>	ERROR
9150	Info from CT Gateway: <~110~>	INFO
9151	Error from CT Gateway: <~110~>	ERROR
9152	Fatal Error from CT Gateway: <~110~>	SEVERE
9160	Harris Connection Warning: <~110~>	INFO
9161	Harris Connection Error: <~110~>	ERROR
9170	MOTOTRBO Connection Warning: <~110~>	INFO
9171	MOTOTRBO Connection Error: <~110~>	ERROR

CODE	ALERT TEXT	SEVERITY
9172	RFSS has not acknowleged all ISSI Group Registration Requests	WARNING
9200	The local RTP Engine is receiving inconsistent data. <~110~> channels received inconsistent data. First channel is <~111~>, Error: <~112~>	INFO
9201	More simultaneous calls occurred than channels are configured. Excess calls are not being recorded.	ERROR
9202	More G.729 encoded calls in progress than recorder is licensed for. Excess calls are not being recorded.	ERROR
9203	Unable to Decrypt P25 Call with key <~110~>	ERROR
9204	OTAR Registration Unsuccessful: <~110~>	ERROR
9205	Recorder Received An Error Condition from KMF: <~110~>	WARNING
9206	OTAR Info: <~110~>	INFO
9207	TCP Connection to <~110~> failed to connect	ERROR
9208	Recorder has sent a certificate to the Mitel system at <~110~>. Recording can not begin until the administrator approves the certificate on the Mitel system.	ERROR
9209	Error: <~110~>	ERROR
9209	Error: <~110~>	ERROR
9300	AIS could not provide audio stream for transmissions. Reason is <~110~>	ERROR
9301	AIS Proxy has entered an error state: <~110~>	ERROR
9302	AIS Proxy received an error condition from AIS: <~110~>	WARNING
9303	AIS Proxy Info: <~110~>	INFO
9305	Recorder has not received Heartbeats from AIS Proxy for at least 30 seconds	ERROR
9306	AIS Proxy version is less than 2.7.0. Recommend upgrading.	ERROR

CODE	ALERT TEXT	SEVERITY
9307	AIS Proxy version does not match the authorized version - Contact your Eventide Reseller.	ERROR
10000	This Recorder, which is currently acting as the Cluster Master, is experiencing a failure to contact the Cluster Node at ip <~110~>. Error: <~111~>	ERROR
10001	This Recorder, which is currently acting as the Cluster Master, has lost its connection to the recorder at ip <~110~>.	INFO
10002	This Recorder is currently unable to synchronize to the cluster master at <~110~>.	INFO

This page was intentionally left 99.88% blank.

E. INCIDENT EVALUATION RESTORE

The NexLog Express supports restoring incidents across multiple recorders. Here we'll describe this process using a NAS Server as an example.

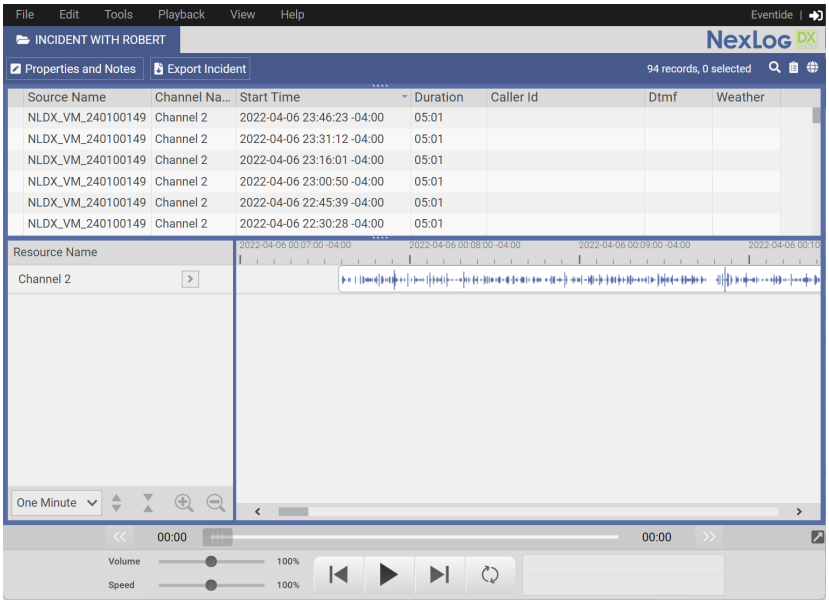


Fig. E.1 MediaWorks EXP Incident

Once you've ensured that your NAS drive is set up with two separate directories, one which will archive your recordings, and the other that will archive your incident, you can connect the MediaWorks EXP system to the NAS shared folders.

The recordings will be archived to NAS simply by selecting "Start Archive"

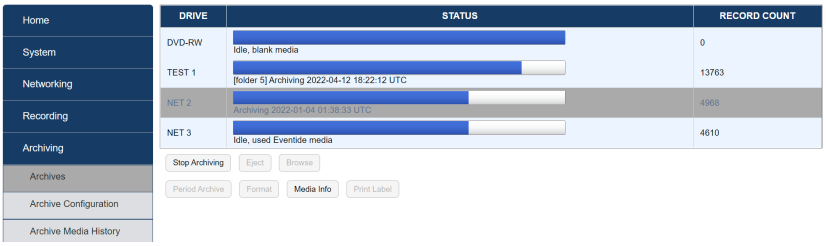


Fig. E.2 DX Archive Page

In order to Archive the incident, you must first schedule a “Backup Incidents Evaluation Metadata” in the “Utilities” section by selecting the correct archive drive to back it up to.

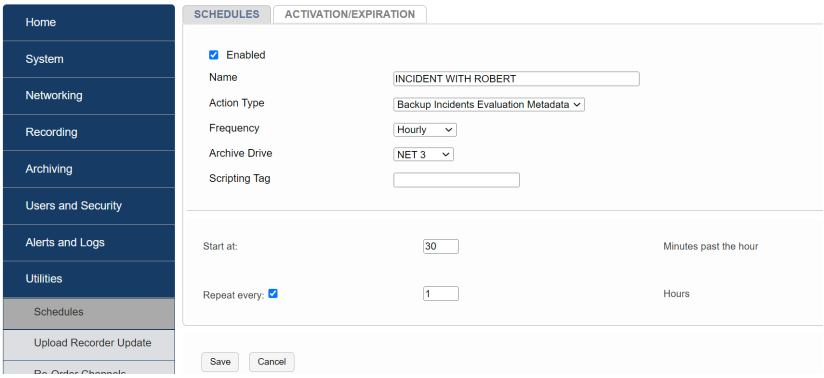


Fig. E.3 Schedule Metadata Backup

Now that the incident and recordings have been properly archived to the NAS drive, the files can be retrieved on the target NexLog Express system by connecting to the NAS drives mentioned above.

> **Note**
>
> In order for the target system to connect to the archived data ensure that “Enable Folders” is disabled.”

After connecting the NAS drives to the target DX-series system, first select “Archive Transfer” for the recordings NAS folder to transfer the recordings to the target system, then once that is done select “Restore Metadata” to transfer the incident to the target system. In MediaWorks DX, you can now see the shared archive incident along with its associated calls which can be played back.

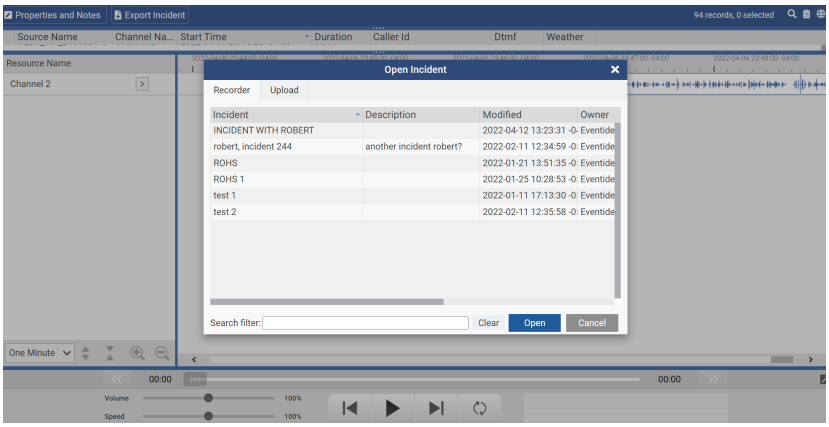


Fig. E.4 MediaWorks EXP Open Incident

This page was intentionally left 99.88% blank.

F. RTP VOIP TEMPLATES

This section contains RTP templates for VOIP recorder setup and configuration.

6.1. Avaya SBC

> **Important**
>
> Any changes to network interfaces needs to be followed by System Management → Restart Application.

6.1.1. SBC Configuration

Log into your Avaya SBC

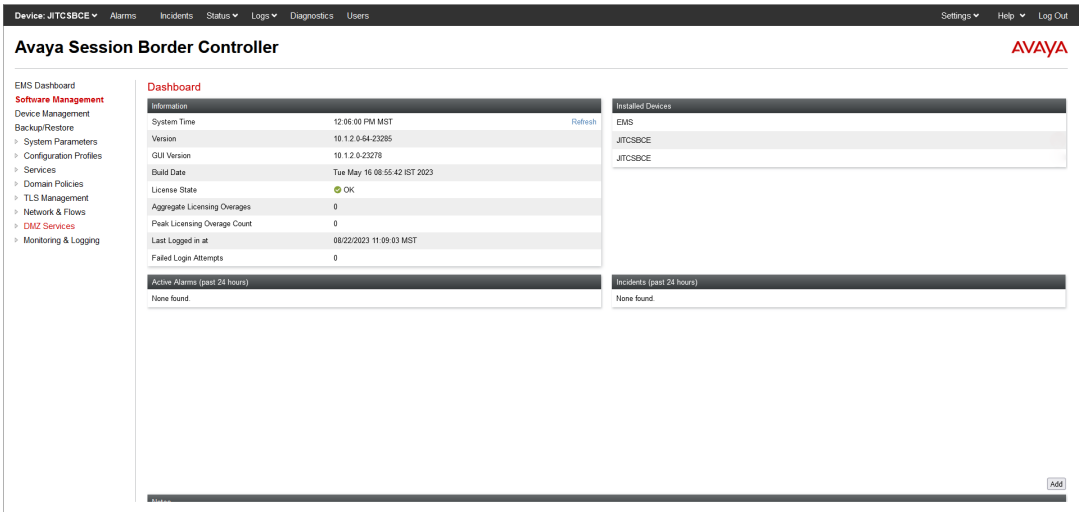


Fig. 6.2 Avaya SBC Login

6.1.1.1. Create a SIP Recording Server

Navigate to Services → SIP Servers → Add. Change the Server Type to Recording Server. For encryption, select your TLS Client Profile (Create the TLS profiles under TLS Management. Please see your IT administrator if you have questions). Add the NexLog Express IP address, RTP port, and transport type.

Add SIP OPTION heart beats to your SIP Recording Server.

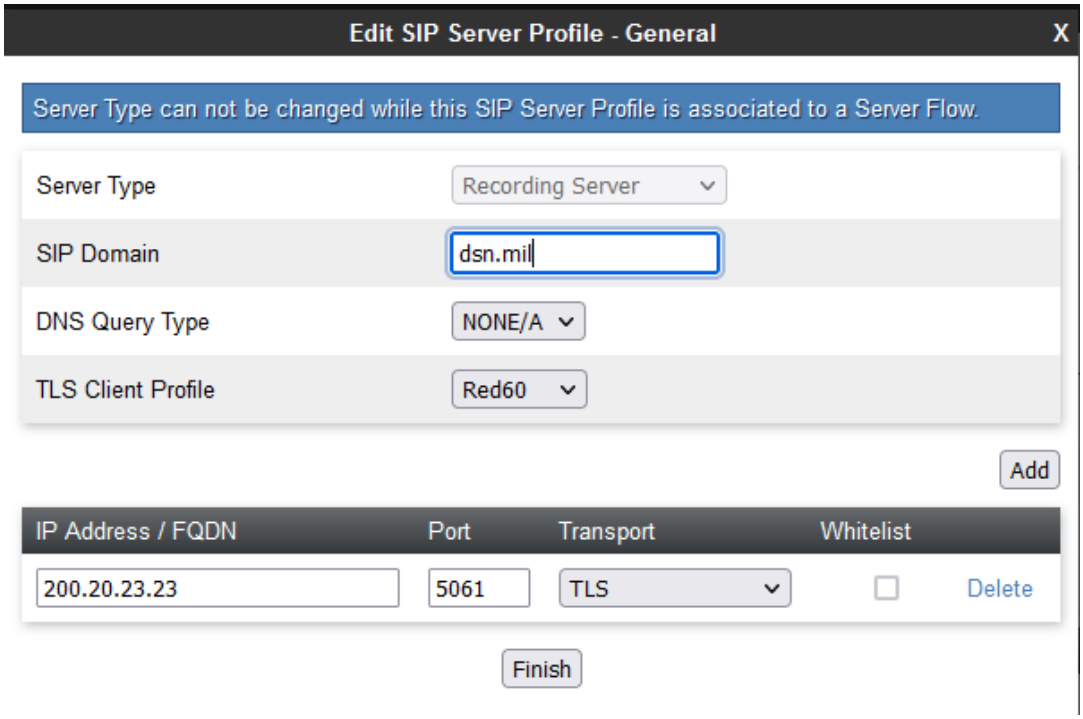


Fig. 6.3 Add SIP Server

Navigate to the Advanced Tab and Enable Grooming and Tolerant.

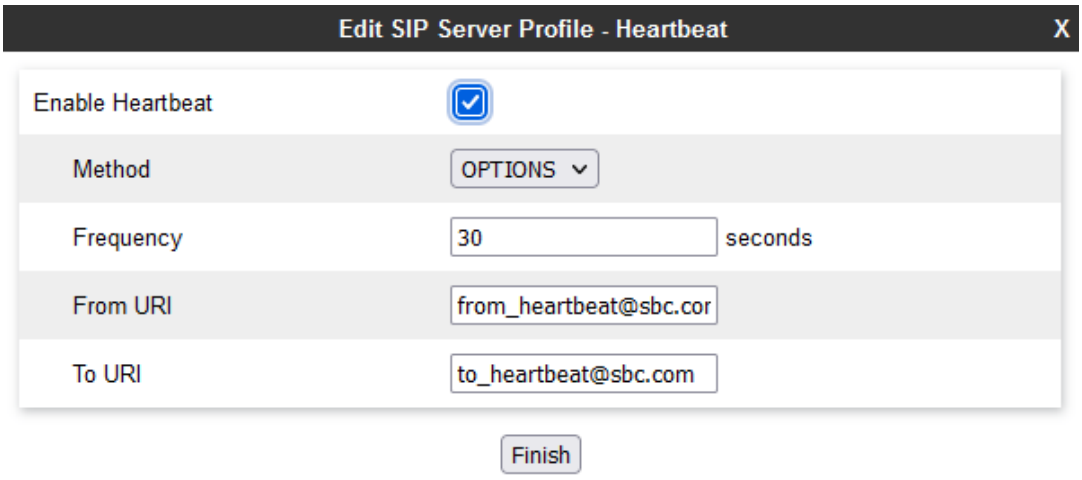


Fig. 6.4 Add SIP Option

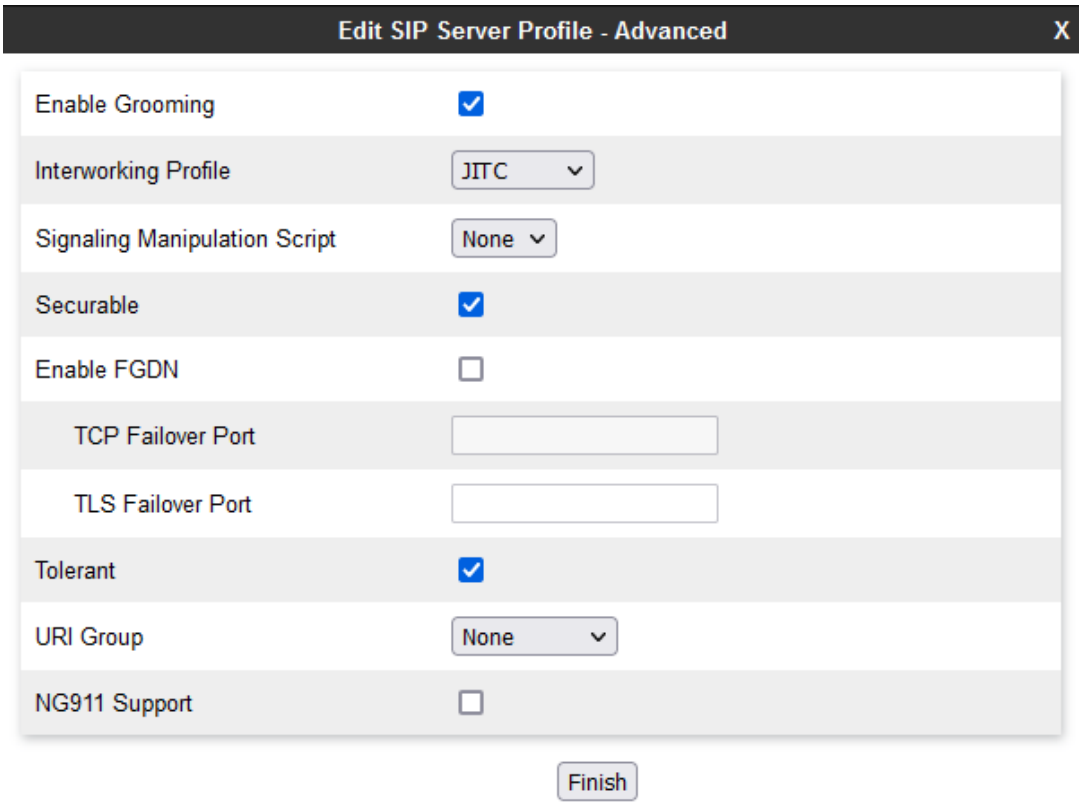


Fig. 6.5 Add SIP Server

6.1.1.2. Routing

Navigate to Configuration Profiles → Routing and create a route and select the SIP Recording Server from the last section.

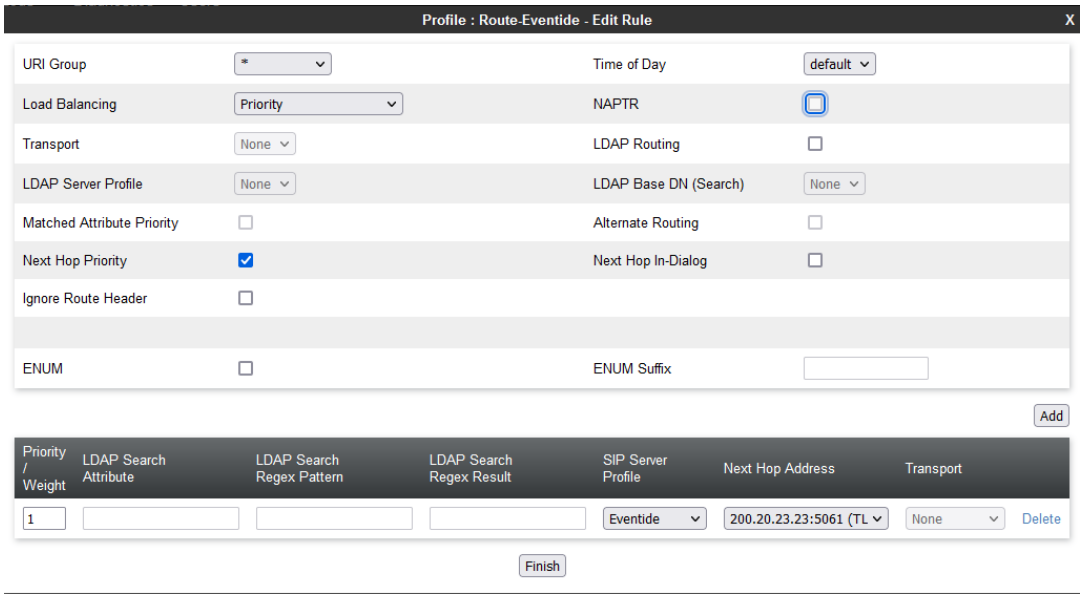


Fig. 6.6 Create Route

6.1.1.3. Recording Profile

Select the Routing Profile created in the last section and select the Recording Type as Full Time.

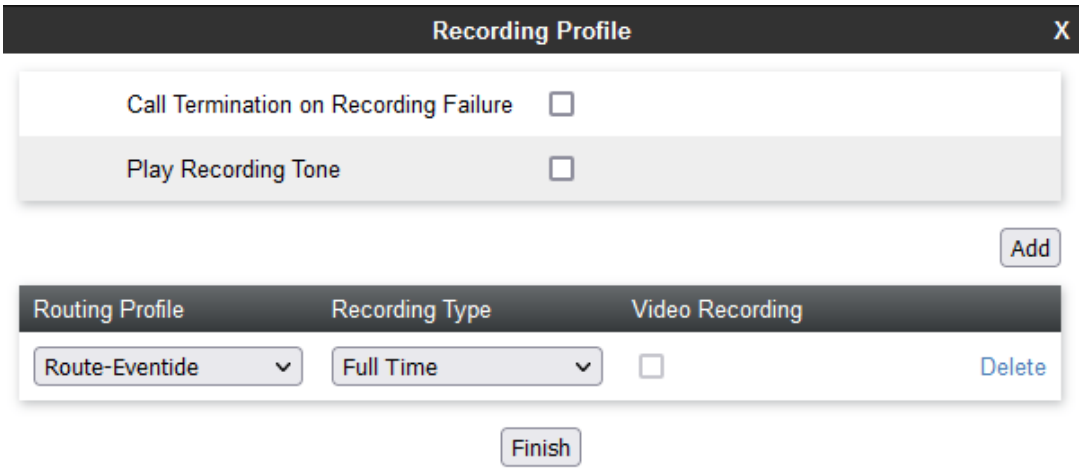


Fig. 6.7 Full Time

6.1.1.4. Server Interworking

Navigate to Configuration Profiles → Server Interworking and modify your profile to support DTMF RFC 2833 Relay & SIP Notify.

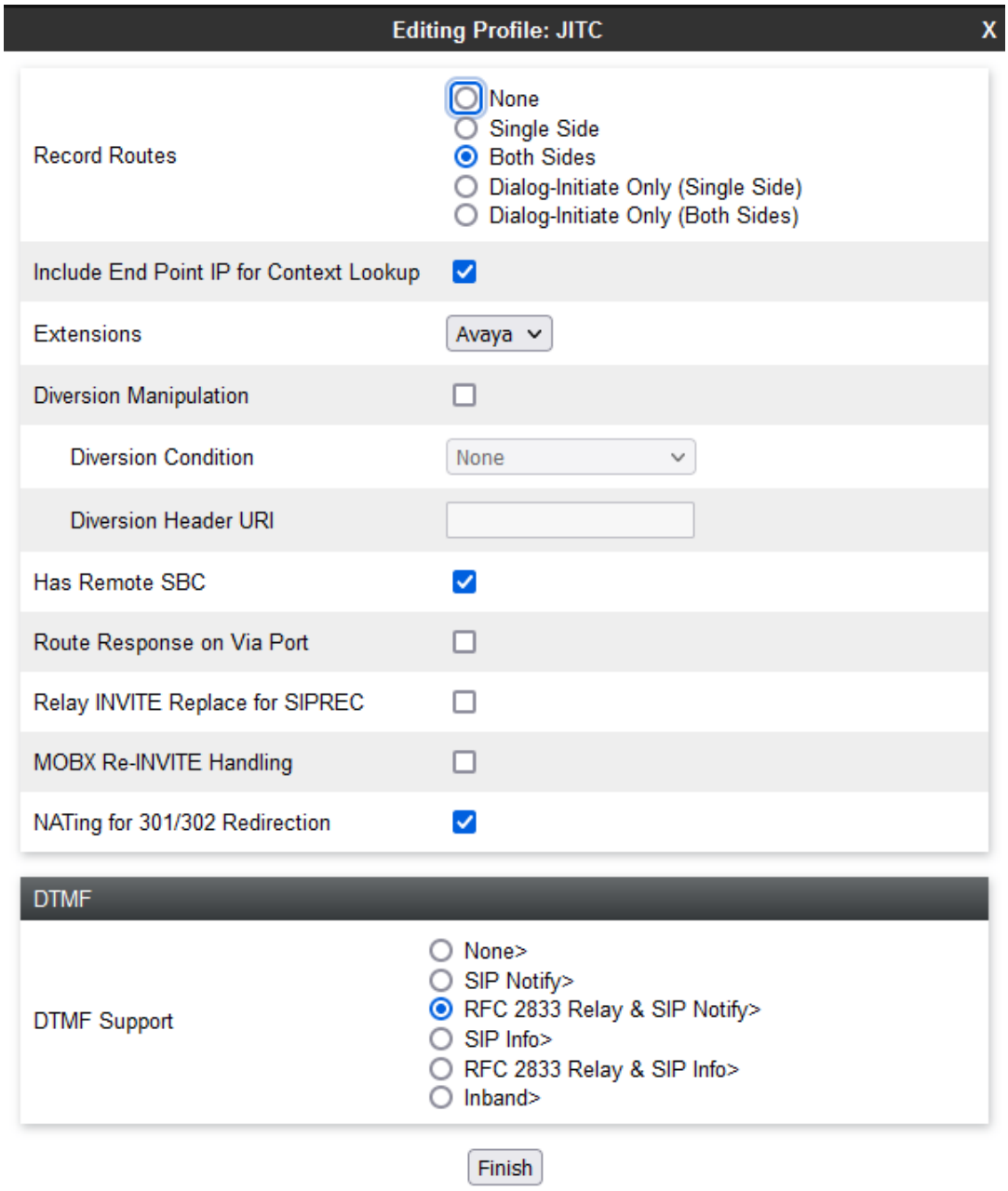


Fig. 6.8 Server Interworking

6.1.1.5. Application Rules

Navigate to Domain Policies → Application Rules and enable Audio in and out.

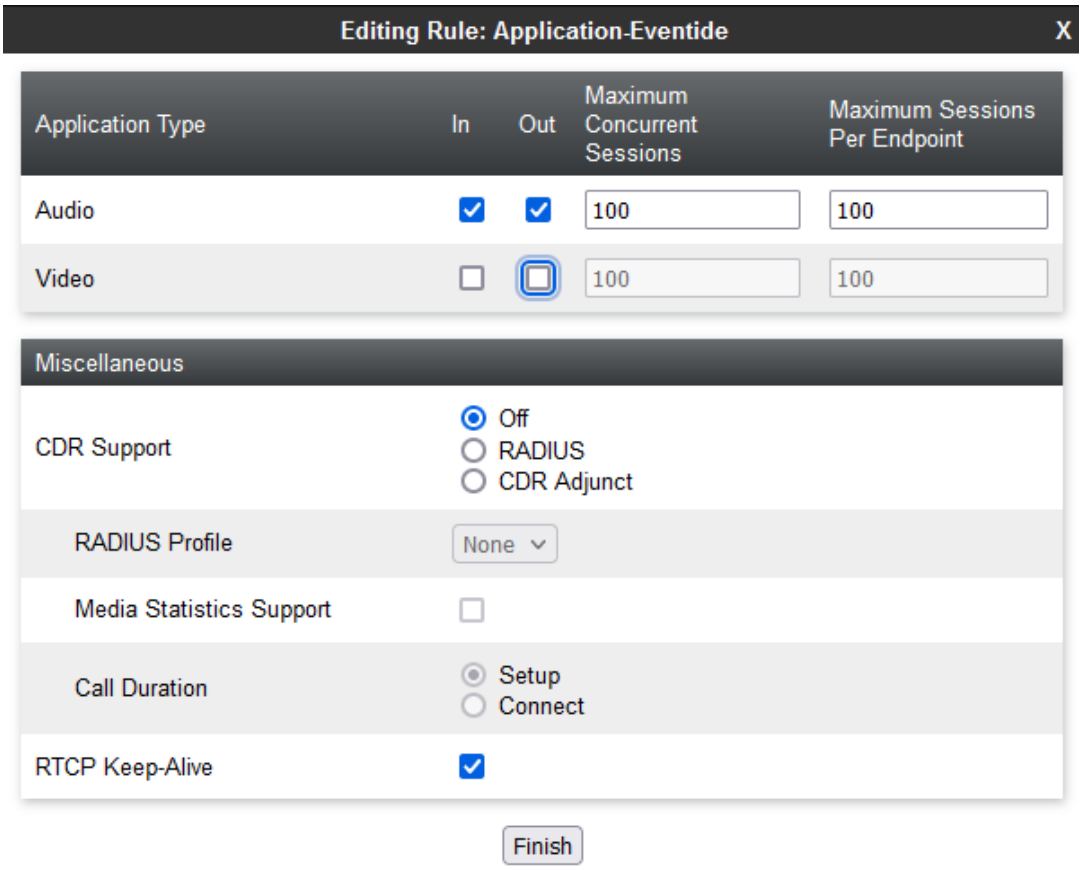


Fig. 6.9 Audio

6.1.1.6. Media Rules

Navigate to Domain Policies → Media Rules and set up your Audio Encryption preferred formats. Enable interworking.

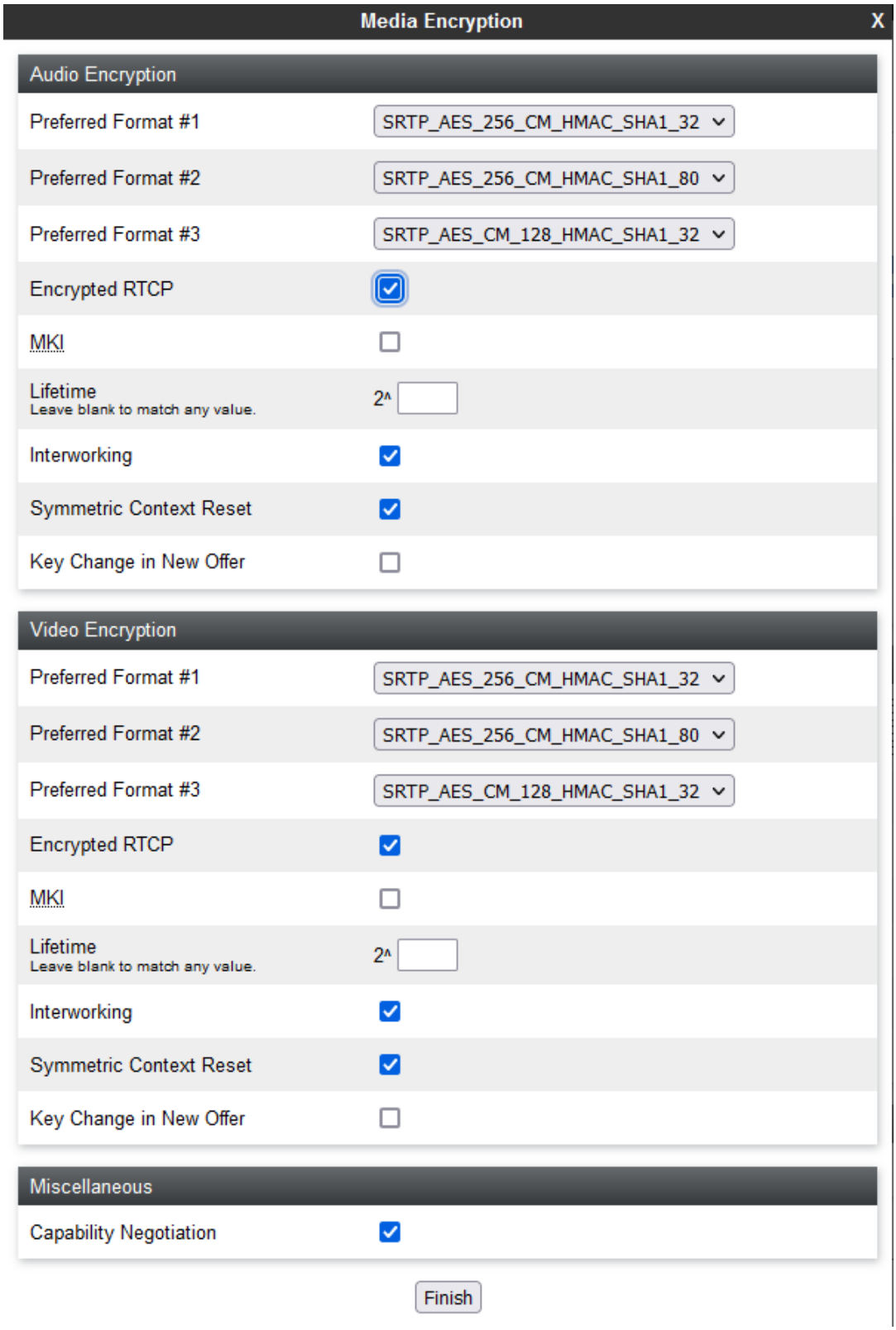


Fig. 6.10 Audio Encryption

6.1.1.7. Signaling Rules

Navigate to Domain Policies → Signaling Rules → Add. Set a unique UCID for the Session Manager and Signaling interface.

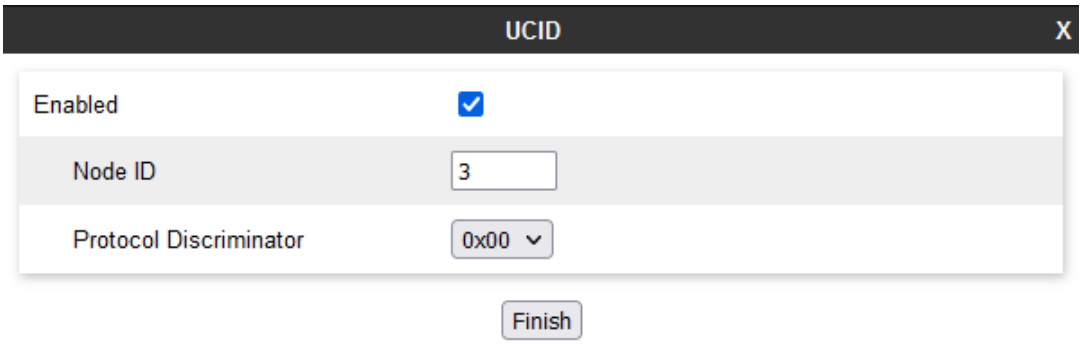


Fig. 6.11 Add Signaling Rules

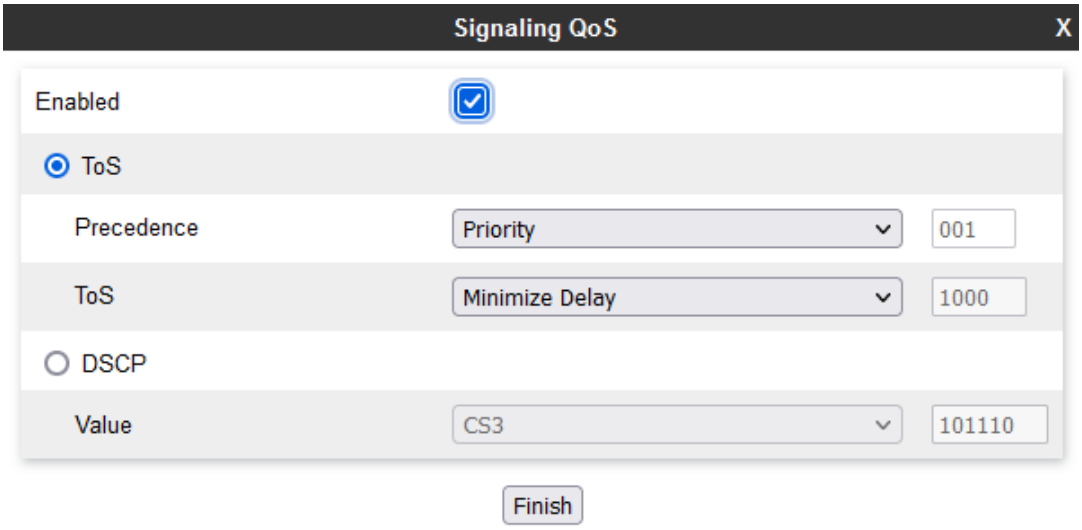


Fig. 6.12 Signaling Rules

6.1.1.8. End Point Policy Groups

Navigate to Domain Policies → End Point Policy Groups → Add. Set the Application Rule, Media Rule, and Signaling Rule created in the previous steps.

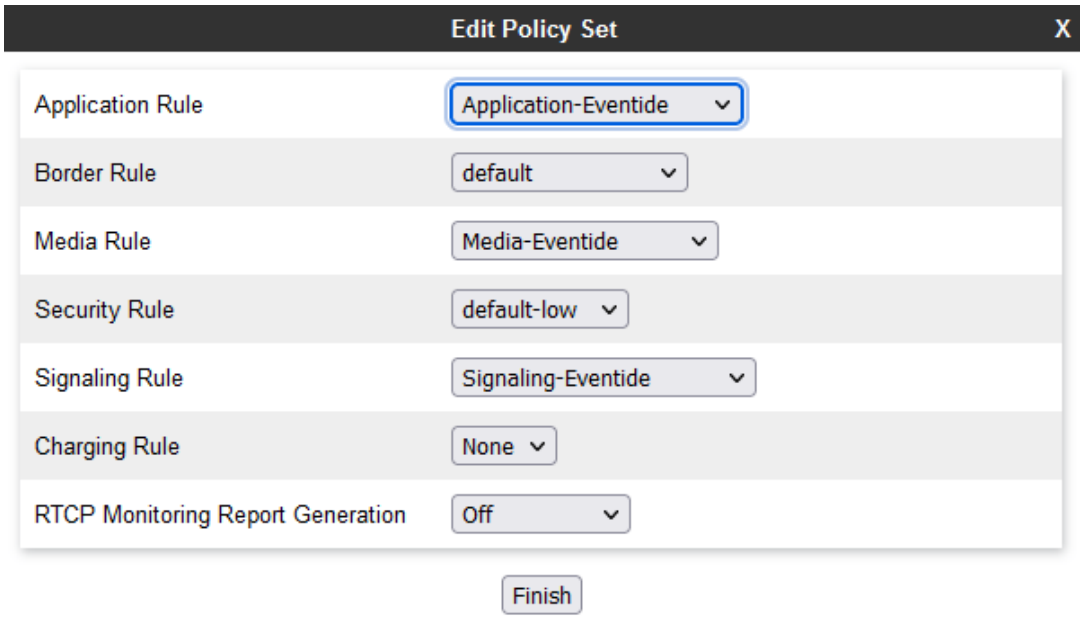


Fig. 6.13 End Point Policy Groups

6.1.1.9. End Point Flows

Navigate to Network & Flows → End Point Flows and Add. Create an internal and external end point depending on your infrastructure. SBC_RED_Eventide represents the internal (red side) Avaya Aura network and SBC_black_SIG represents the external (black side) network connected to the SIP Trunk. Configure the SIP Server Profile, Received Interface, Signaling Interface, Media Interface, End Point Policy Group, and Routing Profile created in the previous sections.

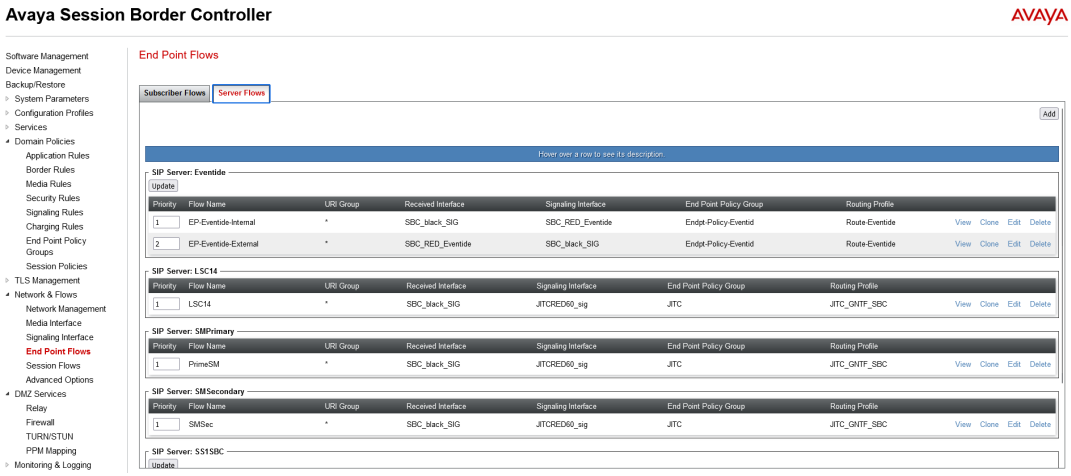


Fig. 6.14 End Point Policy Flows

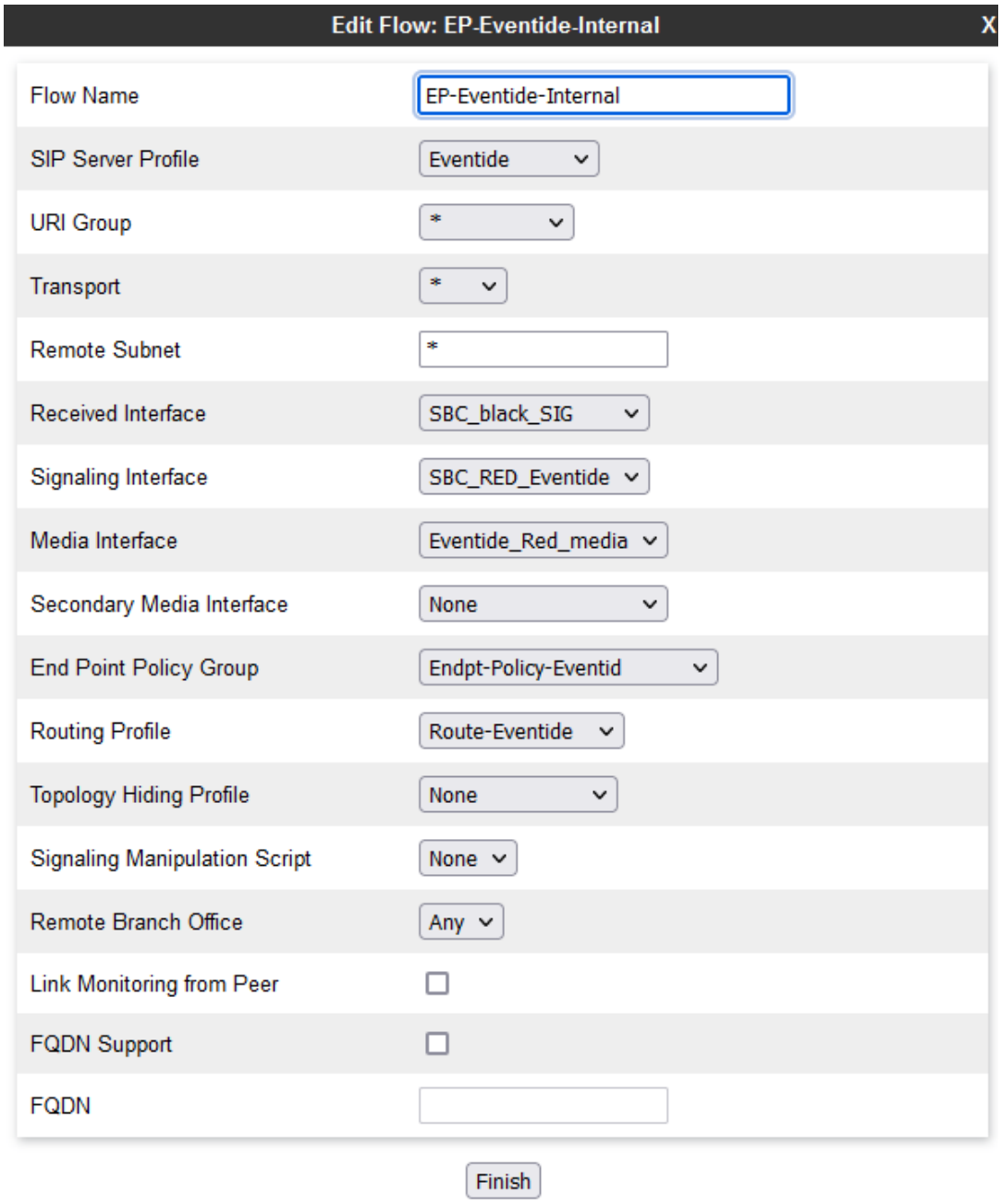


Fig. 6.15 End Point Policy Flows

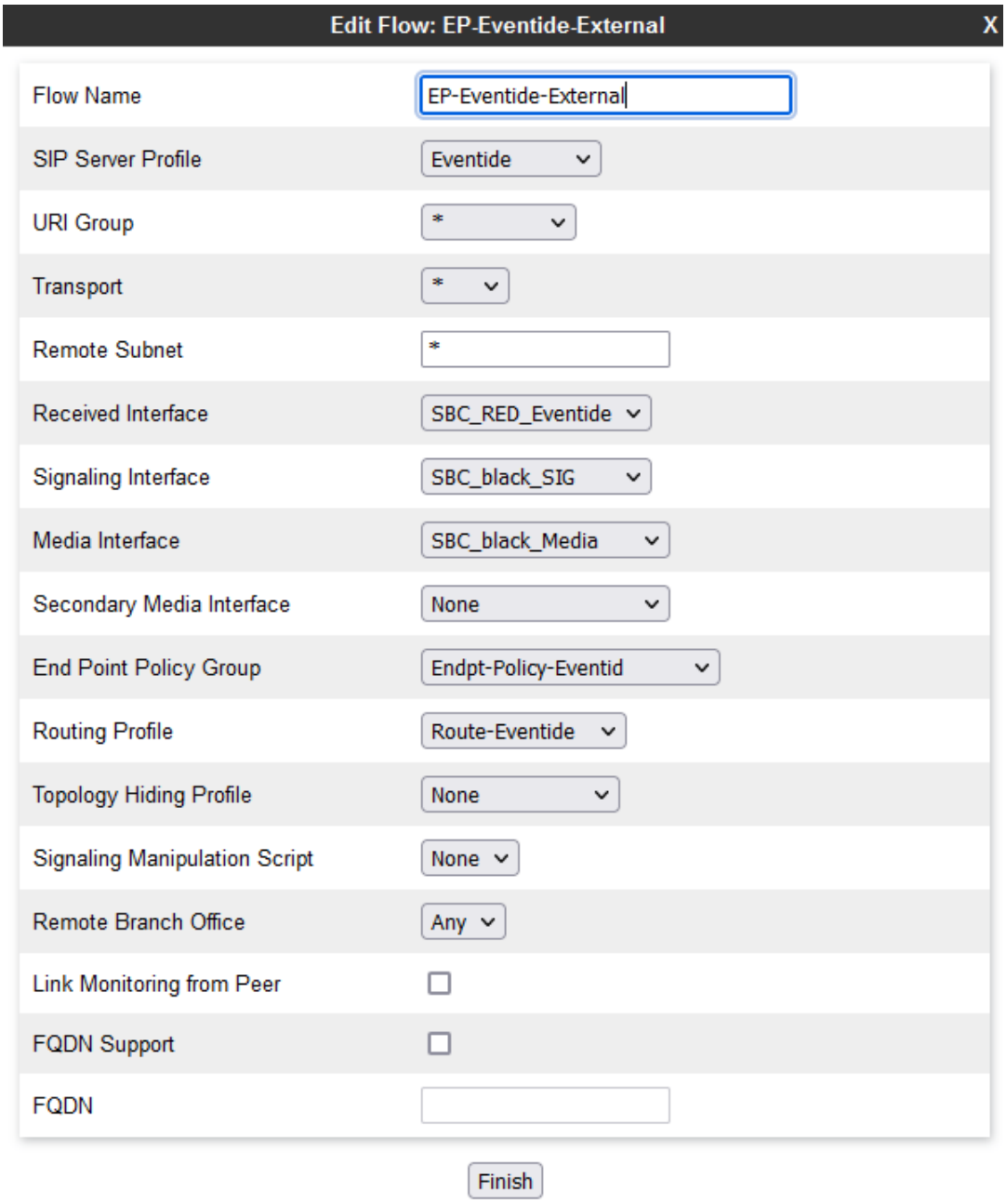


Fig. 6.16 End Point Policy Flows

6.1.1.10. Session Flow

Navigate to Network & Flows → Session Flows → Add. Create a Session Flow for the SBC to the NexLog Express.

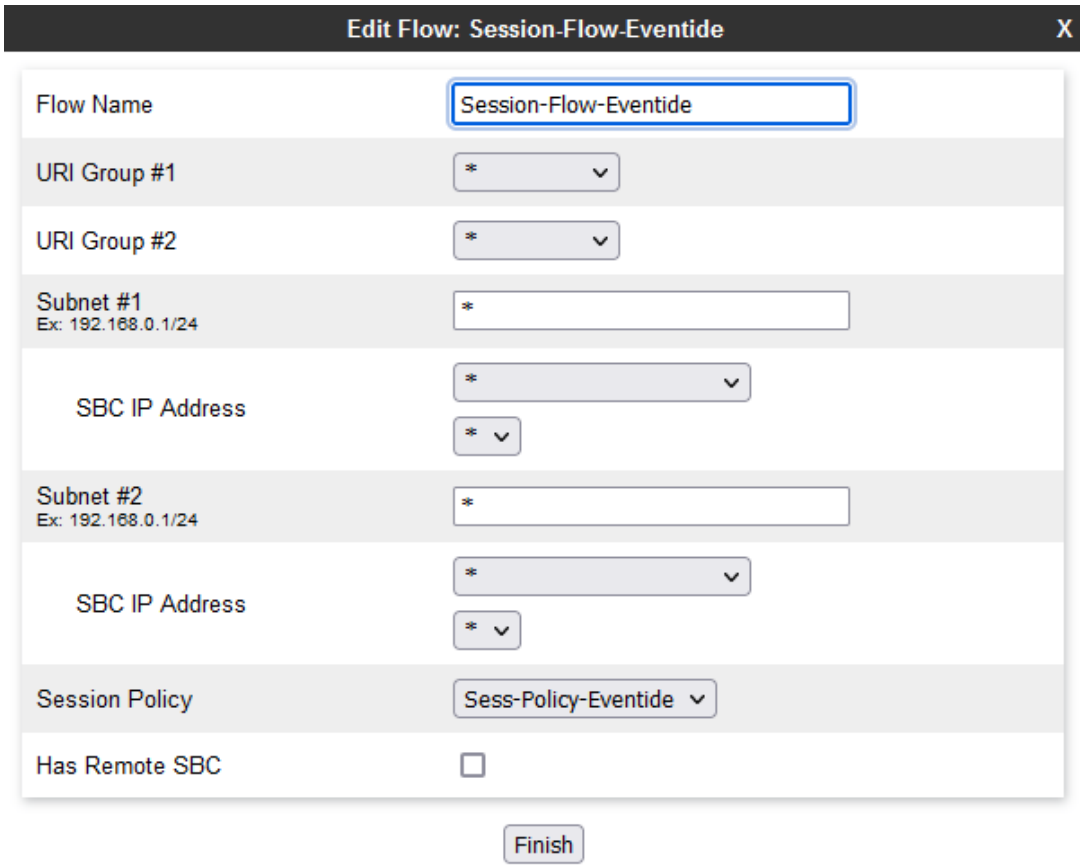


Fig. 6.17 Add Session Flows

6.1.1.11. Avaya SBC Troubleshooting

Log into the SBC and switch to the root user via `su root`.

Run the command `tracesbc` and start capturing.

Make a call and analyze the output.

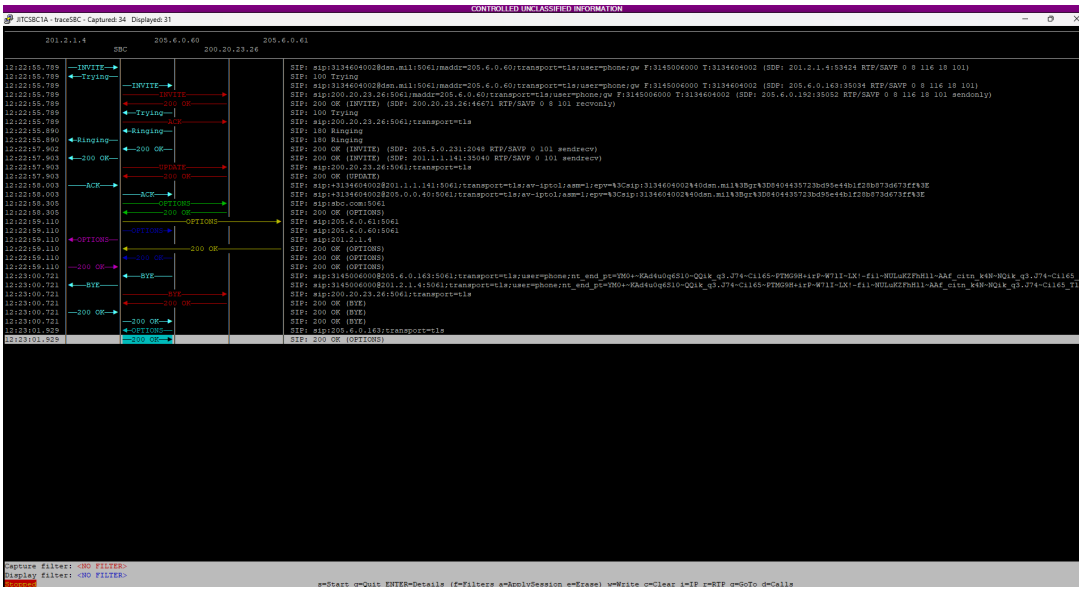


Fig. 6.18 Troubleshooting

In the figure above the `201.2.1.4` IP address represents the external (black side) network.

The SIP INVITE reaches the Avaya SBC and forwards the INVITE to the internal (red side) network `205.6.0.60`.

The SIP INVITE is then routed to the NexLog Express `200.20.23.26` on the red side.

`tracesbc` will automatically create a pcap to view on WireShark and a packet capture can be configured on the NexLog Express.

6.1.1.11.1. Possible Scenarios

6.1.1.11.1.1. Scenario One

SIP OPTION heart beats are not reaching the NexLog Express

If you do not see the SIP OPTIONS going from the external network, to the SBC, to the internal network, and the recorder, then you have a network issue. Please check your firewall rules.

6.1.1.11.1.2. Scenario Two

SIP OPTION heart beats are reaching the NexLog Express, but no SIP INVITES/RTP is reaching the NexLog Express.

The receiving, signaling, media interface, and/or the end point flow are most likely misconfigured or there is a firewall issue.

6.1.2. Recorder Configuration

Log in to the Configuration Manager and navigate to Recording → Recording Interfaces and select Add Virtual Recording Interface. Configure the Avaya SBC SipRec Recording template and select the proper Ethernet Device, SIPPort, Endpoint IP, and Recorder Sip Stack.

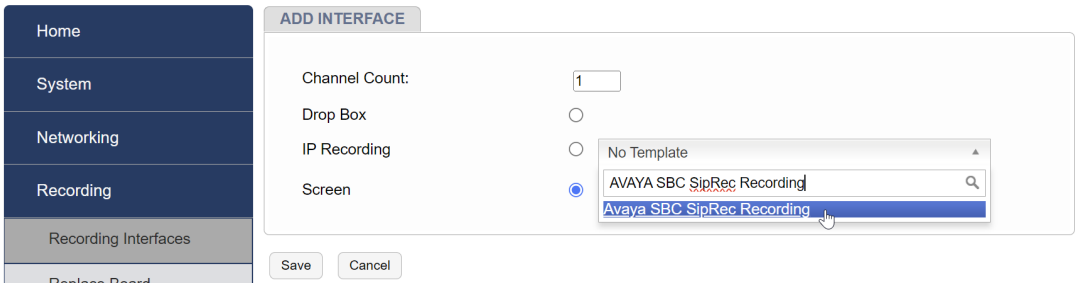


Fig. 6.19 Add Avaya SBC Interface

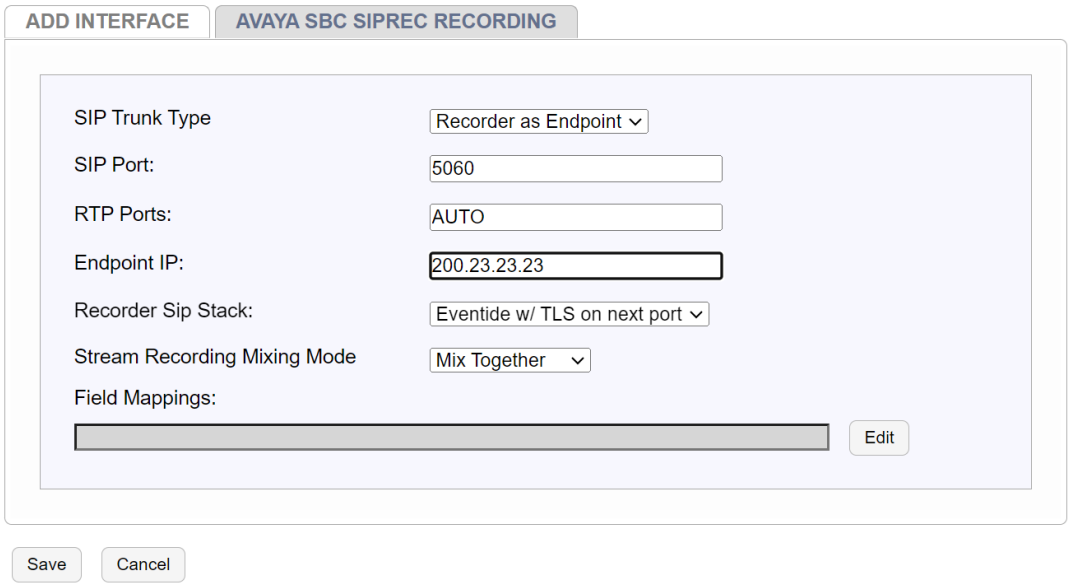


Fig. 6.20 Configure NexLog Express

6.1.2.1. Verifying Recording

You should now be able to make calls to confirm that recordings are taking place between the Avaya SBC and Eventide NexLog Express.

You can review actual recordings by logging into the MediaWorks EXP playback interface.

6.2. Avtec Scout RTP Forwarding

License Required

This feature must be licensed to be used. Contact your Eventide Communications Dealer for assistance.

The virtual AVTEC recording interface on the NexLog recorder utilizes one “Local VoIP/RTP channel” license for each channel allocated.

To check the number of licenses on the NexLog recorder, open the Configuration Manager and navigate to System -> License Keys on the left side. The licensed quantity will be listed on the right side under an “Addon” key. Look for the text “Num Local VOIP/RTP Channels = XX” where XX is the number of channels the NexLog is license for. License Allocation 1 Scout™ Console Select output = 1 license 1 Scout™ Console Unselect output = 1 license 1 VPGate™ radio output (Tx and Rx) = 1 license

Metadata Capture To capture the received metadata from the AVTEC sources, the Eventide NexLog will need to have an available metadata feed license.

One metadata feed license is required for each “Virtual Recording Interface”

The licensed quantity will be listed on the right side under an “Addon” key. Look for the text “Num Metadata Data Feeds = XX” where XX is the number of metadata feeds the NexLog is license for.

Licensing Example This example shows the licenses required to capture AVTEC audio on a single NexLog recorder with 1 IP address on a single Virtual Recording Interface.

Radio Recording Requirements:

- 5 - Scout Consoles, each one recording the “Select” audio feed, with metadata enabled
- 15 - VPGate Endpoints, each one recording transmit (Tx) and receive (Rx), with metadata enabled

Eventide NexLog Requirements:

- 20 - Local VOIP/RTP Channels
- 1 - Metadata Data feeds

6.2.1. AVTEC Scout™ Console Configuration

AVTEC Scout™ consoles may be configured to perform IP-based Audio Forwarding of Select and/or Unselect audio to the Eventide NexLog. Important! Any AVTEC system configuration instructions herein are provided for convenience. For definitive instructions on how to configure audio forwarding for Scout consoles, always refer to the latest AVTEC documentation.

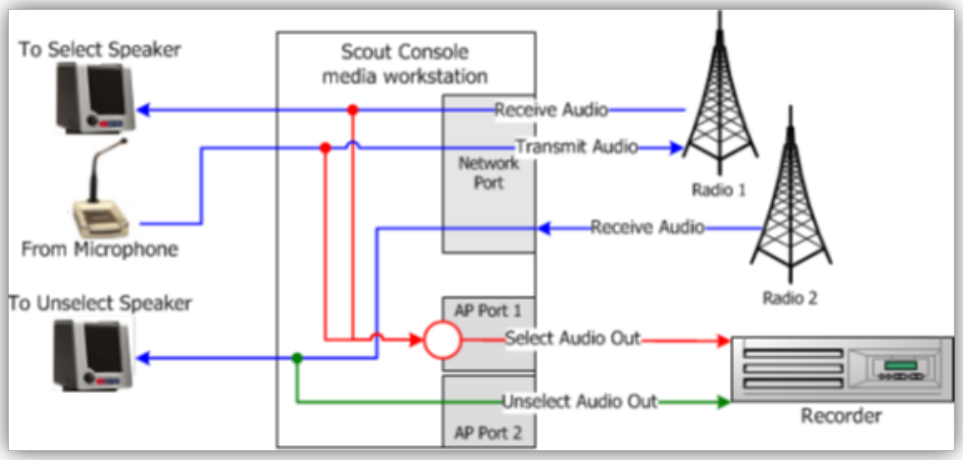


Fig. 6.21 Scout IP Audio Forwarding

The diagram in Figure 2 (from the AVTEC “Logging Recorder Compatibility Guide”) shows Scout™ Console IP audio and metadata being sent from the audio streams, through the ethernet port, over the network to the NexLog recorder. If E911 (NENA-compliant) audio is included in the Select audio, it is included in the recording.

6.2.1.1. Select Channel Audio Forwarding

The Scout™ Console Media Workstation (SCMW) may be configured to forward “Select Channel” audio packets to a single recorder’s IP address and UDP port. The SCMW can be configured to mix the Select receive audio and microphone audio into one stream before forwarding to the Eventide NexLog’s IP address. The following steps need to be performed for each Console where Select audio is to be recorded:

- Login to the SCMW configuration manager with an Administrative account
- Add a new Network Audio Device

- Enter a name for future identification
- Enter the IP address of the Eventide NexLog
- Enter the UDP Port number that will be assigned to record the particular Console's Select audio. Be sure to note this port number as it will be used for configuration on the NexLog recorder.
- Select G.711 for the VoIP Audio Codec
- Enable the microphone is you wish to capture the dispatcher's transmissions
- Enable Send Metadata if desired
- Select "Update" at the top of the page to enable to new device

Fig. 6.22 SCMW Select

6.2.1.2. Unselect Channel Audio Forwarding

The Scout™ Console Media Workstation (SCMW) may be configured to forward "Unselect Channel" audio packets to a single recorder's IP address and UDP port.

The SCMW mixes all Unselected audio the console received into one stream before forwarding to the Eventide NexLog's IP address. The following steps for each Console for which Select audio is to be recorded:

- Login to the SCMW configuration manager with an Administrative account
- Add a new Network Audio Device
- Enter a name for future identification
- Enter the IP address of the Eventide NexLog
- Enter the UDP Port number that will be assigned to record the particular Console's Unselect audio. Be sure to note this port number as it will be used for configuration on the NexLog recorder.
- Select G.711 for the VoIP Audio Codec
- Enable Send Metadata if desired
- Select "Update" at the top of the page to enable to new device

Fig. 6.23 SCMW Unselect

6.2.1.3. AVTEC VPGate™ Configuration

Audio to and from conventional radios or other Outpost™-connected circuits, P25 DFSI or CSSI endpoints, or non-Avtec endpoints (such as NXU2A network extension units) may be recorded via automatic audio forwarding from the AVTEC VPGate™ to the Eventide NexLog. Two UDP ports are used for audio forwarding (one UDP port for audio to the endpoint, and one UDP port for audio from the endpoint). The Eventide NexLog receives the forwarded IP-audio on the two UDP ports, mixes the two streams, and records the endpoint's audio on one voice logging channel.

In the case of IMBE/AMBE encoded audio, the VPGate™ transcodes to G.711 before forwarding to the Eventide voice logger.

Important

Any AVTEC system configuration instructions herein are provided for convenience. For definitive instructions on how to configure audio forwarding for Scout consoles, always refer to the latest AVTEC documentation.

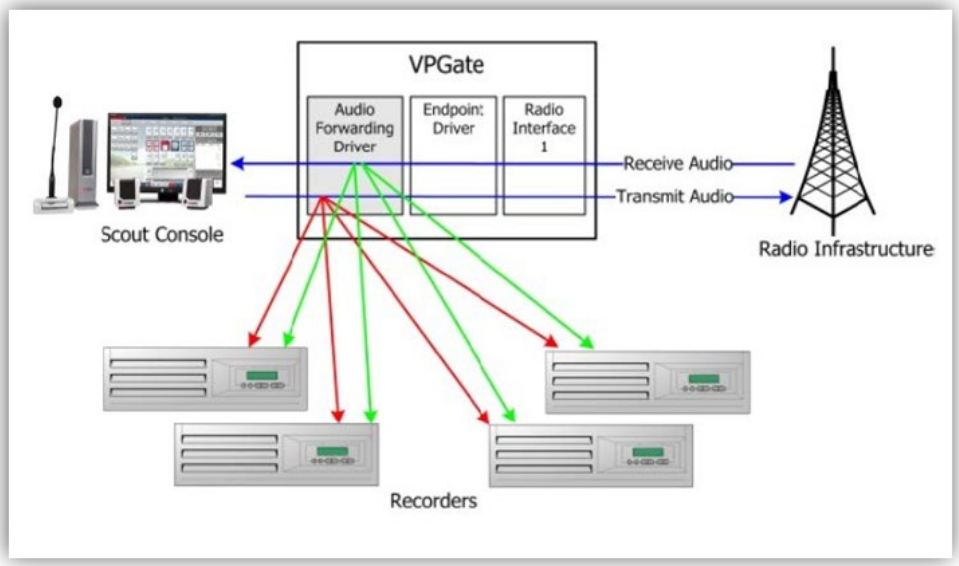


Fig. 6.24 VPGate IP Audio Forwarding

The diagram in Figure 5 (from the AVTEC “Logging Recorder Compatibility Guide”) shows VPGate™ Endpoint IP audio and metadata being sent from the audio streams, through the ethernet port, over the network to the NexLog recorder.

6.2.1.4. Endpoint Audio Forwarding

VPGate™ performs separate audio forwarding for audio that is transmitted toward the endpoint and for audio that is received from the endpoint. Thus, audio to/from a single endpoint will be forwarded to two UDP ports on the Eventide NexLog. The Eventide NexLog is normally configured to mix the audio streams from the two UDP ports of a VPGate™ Endpoint so that both are recorded to a single channel on the logger. AVTEC VPGate™ can be configured to perform IP-based Audio Forwarding of endpoint audio to up to 4 Eventide NexLogs simultaneously. To forward endpoint audio to the Eventide voice logger, an audio forwarding driver must be configured for the desired endpoint.

The following steps need to be performed for each endpoint where audio is to be recorded. This process describes enabling the capture of transmit and receive audio:

- Login to the Scout Project Manager with an Administrative account
- Select the Endpoint to be recorded
- In the “Drivers” section at the bottom of the page, select “Audio Forwarding” and Select “Add driver”
- Under Metadata Settings, enable Send Metadata if desired

Audio Transmitted Toward the Endpoint:

- Enter the IP address of the Eventide NexLog in the field labeled “IP Address #1”
- In the corresponding UDP port field, enter the UDP Port number that will be assigned to record the particular Endpoint’s transmit audio. Be sure to note this port number as it will be used for configuration on the NexLog recorder.

Audio Received From the Endpoint:

- Enter the IP address of the Eventide NexLog in the field labeled “IP Address #1”
- In the corresponding UDP port field, enter the UDP Port number that will be assigned to record the particular Endpoint’s receive audio. This port should not be the same as the transmit UDP port. Be sure to note this port number as it will be used for configuration on the NexLog recorder.
- Select “Update” at the top of the page to enable to new driver

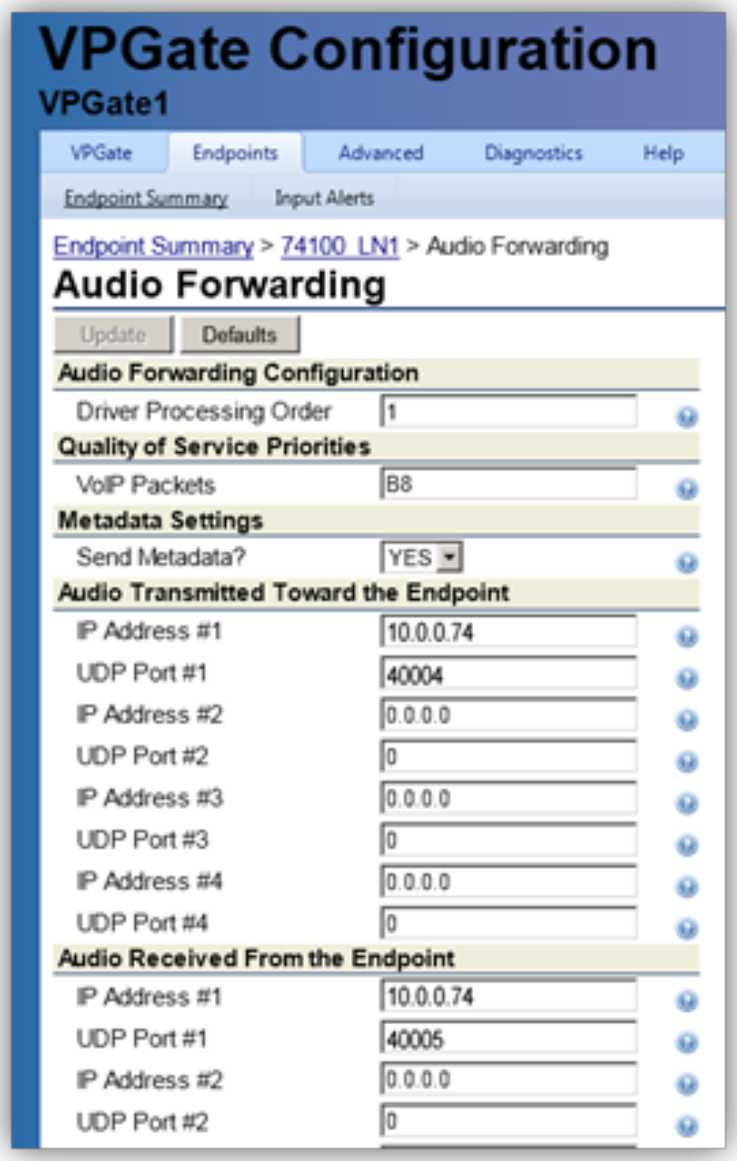


Fig. 6.25 Endpoint

6.2.1.5. Eventide NexLog™ Configuration

The Eventide NexLog receives the UDP audio packets from the VPGate™ and Scout™ Consoles and captures them on the assigned logging channels.

Before beginning the setup process, ensure that the AVTEC systems are able to pass traffic to the recorder's assigned IP address. This is particularly important when a firewall is configured between the NexLog and AVTEC network.

6.2.1.6. Virtual Recording Interface Setup

Once licensing is verified and the AVTEC components have been configured, you can begin the setup process to capture your AVTEC audio and metadata.

- Open the Eventide NexLog Configuration Manager's web page.
- Login with an Administrative account.
- Use the navigation on the left and go to Recording -> Boards.
- At the bottom of the page, select "Add Virtual Recording Interface".

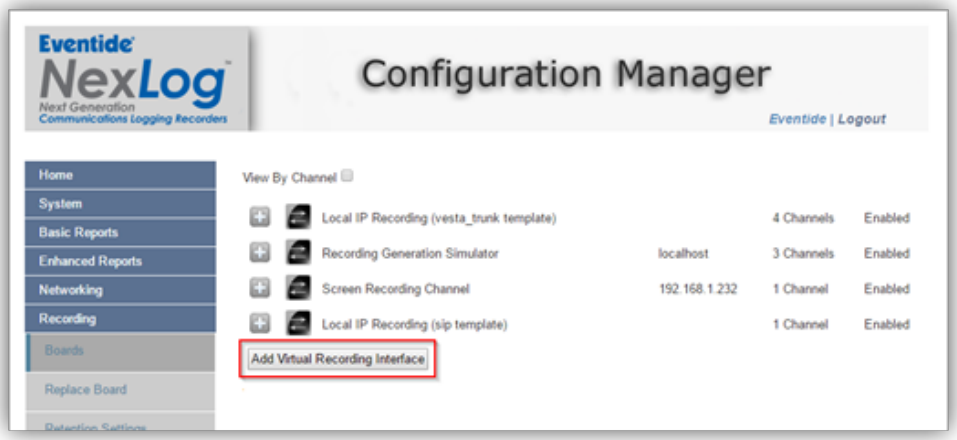


Fig. 6.26 Add Virtual Recording Interface

- Select the number of channels desired using the "Channel Count" field.
- In the "Local IP" field, select "Avtec Scout™ RTP Forwarding".

Fig. 6.27 Configure Virtual Interface

- In the “Base RTP Port” field, enter the starting range of your configured RTP ports. The default value is 40000.
- Update the Tx and Rx Ports to reflect the values configured in the SCMW and VPGate™. Scout™ Console Select and Unselect recording only requires the use of one UDP port. Enter that port number in the Tx field and leave the Rx field empty.
- Click the “Metadata” checkbox if metadata is expected to be received on the channel.
- Select “Save” when finished.

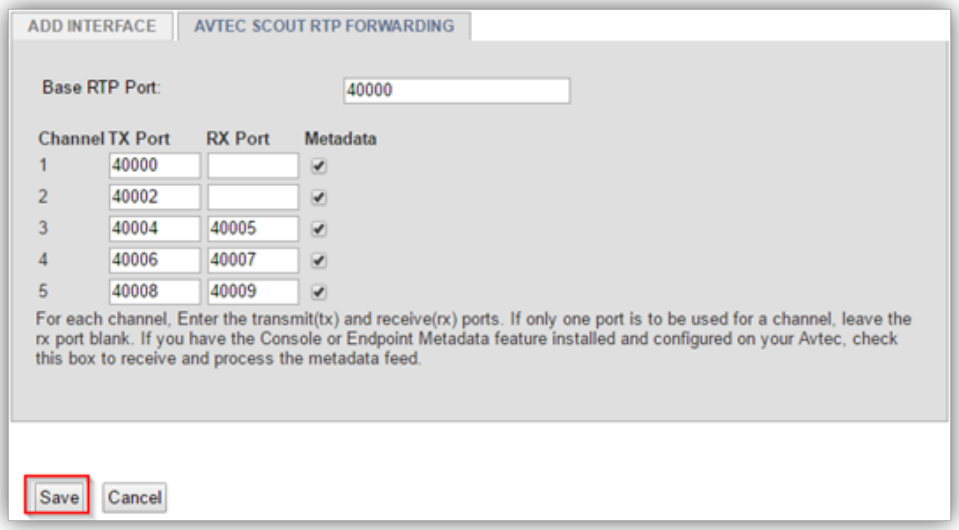


Fig. 6.28 Configure UDP Ports and Metadata

- Expand the new Virtual Recording Interface.

- Click on the new channel's name to update it. Select "Enter" to save it.

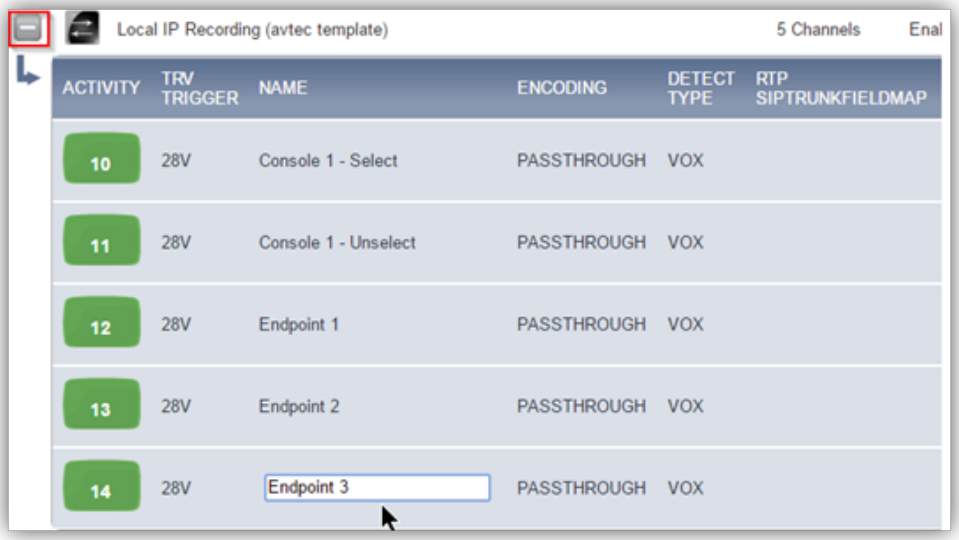


Fig. 6.29 Update Channel Names

6.3. Carybyn Call Handling Solution

6.3.1. Carbyne Introduction

The purpose of this document is to describe the steps to ensure successful integration between an Eventide NexLog Express and a Carbyne Recording System. The document assumes knowledge of the NexLog Express front panel interface and the browser-based configuration manager and does not discuss recording interfaces beyond the Carbyne integration. For more details on these interfaces, please refer to their respective manuals.

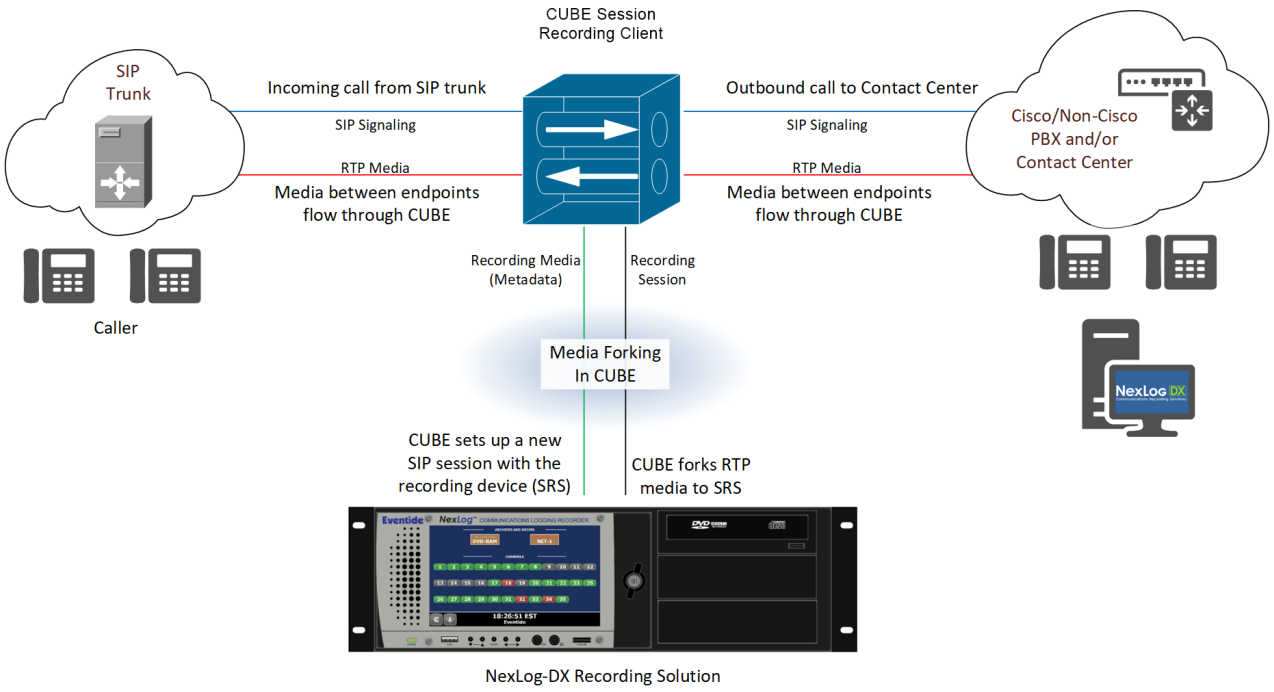


Fig. 6.30 Carbyne Diagram

License Required

This feature must be licensed to be used for the following:

- Local VoIP/RTP Channels
- Carbyne SIPREC Recording

Contact your Eventide Communications Dealer for assistance.

6.3.2. Logger Integration

Carbyne currently supports third party recorders via SIPREC plus a CAD spill to provide voice and data to the recorder while adhering to the RFC 7866 protocol.

Requirements:

- SIPREC support

- External static IP addresses
- Internal Static IP addresses
- Port forwarding on the firewall to send the signaling & media from our sources toward the Recording Server.
- Carbyne supports working on 5060 TCP (signaling) & 16384 - 32767 UDP (Media).

Note

Please make sure to open the ports listed above on the firewall to accept incoming traffic towards the Session Recording Server from our Session Recording Clients.

In the SIP Responses Requests that are sent from the Recording Server, please make sure that all Recording-Server's Private addresses are NATted from Private IP's to Public IP's (for all SIP Headers including SDP values).

For any other integration support, please contact your Carbyne Representative.

6.3.3. Adding a Virtual Recording Interface

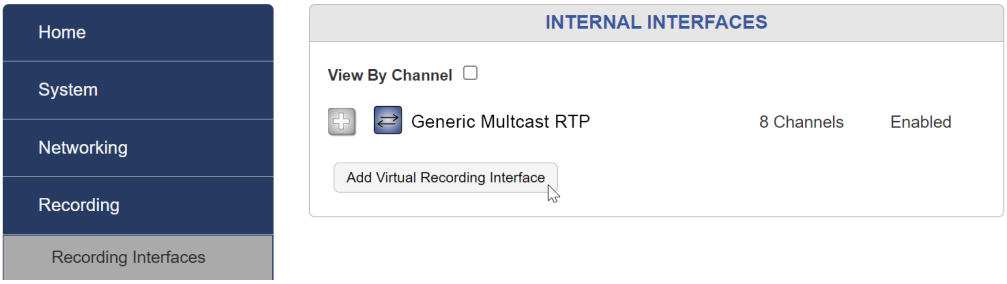


Fig. 6.31 Add Virtual Recording Interface

Select the number of IP channels/number of talk paths and "Carbyne Recording Interface" Template

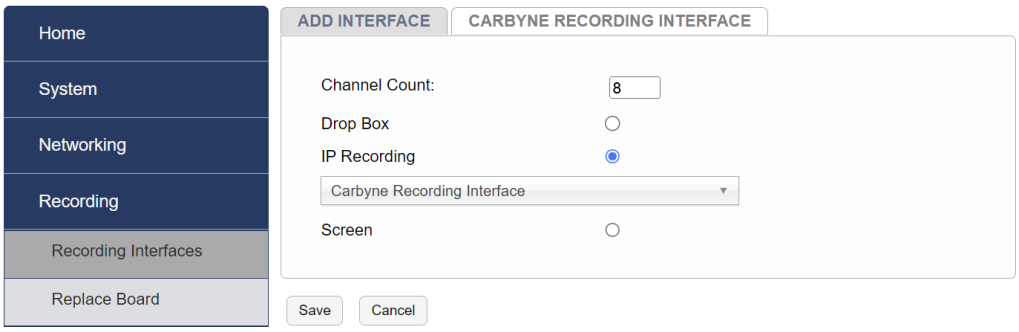


Fig. 6.32 Select Channels and Template

6.3.3.1. Template Field details

The following figure has the fields populated for illustrative purposes, however, the actual values in each installation will most likely be different. Verify each value with the Carbyne or the Customer Network Administrator.

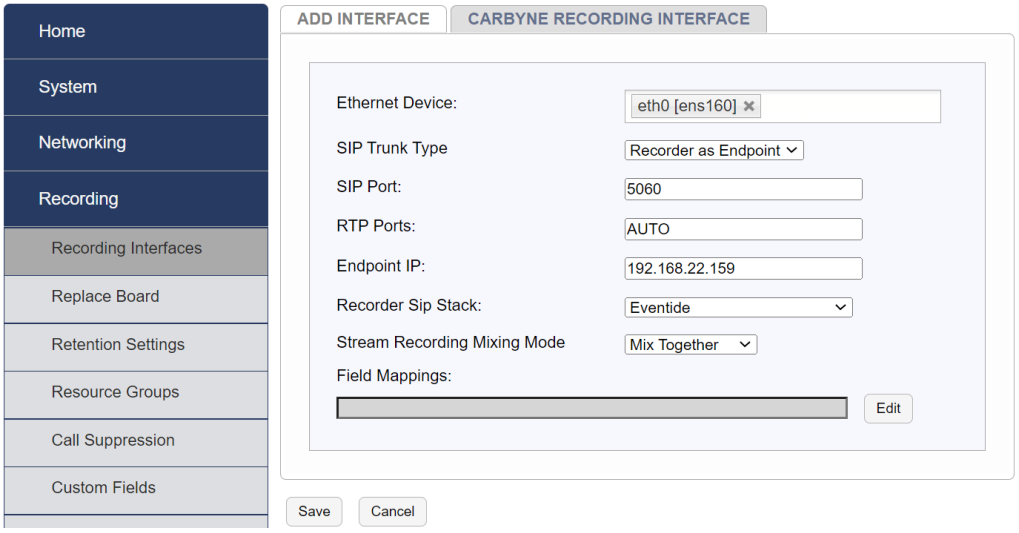


Fig. 6.33 Template Field Details

Ethernet Device: Select the physical Ethernet/NIC of the recorder which is connected to the network carrying the SIPREC call data

SIP Trunk Type: Recorder as Endpoint

SIP Port: 5060 (settings may differ)

RTP Ports: Auto

Endpoint IP: IP of the recorder's NIC which will receive the SIPREC/RTP data

Recorder Sip Stack: Can either be "Eventide" or "Eventide w/ TLS on next port"

Stream Recording Mixing Mode: Can be "Mix Together" or "Keep Separate"

6.3.3.2. Apply the template

After filling in all the fields, select "Save".

The following Custom Fields are automatically added to the recorder by the Carbyne template:

- PARTICIPANT1
- PARTICIPANT2
- PARTICIPANT3PLUS
- PARTICIPANTALL
- RECEIVER
- SENDER

Two alias banks are created to fill in the custom fields PARTICIPANT3PLUS and PARTICIPANTALL

- Carbyne - Participant3Plus - LOCALIP-<guid>
- Carbyne - ParticipantAll - LOCALIP-<guid>

Fig. 6.34 Alias Banks

6.3.3.3. Check for Alerts

Check the NexLog Express front panel and/or configuration manager for any system alerts or Carbyne-specific alerts.

6.3.3.4. Verify Recording

Place a series of test calls. Use MediaWorks EXP or the front panel display to verify the recording of all test calls.

6.4. Cisco CallManager Skinny Protocol (SPAN)

6.4.1. Cisco CallManager Skinny Protocol (SPAN) Introduction

The purpose of this document is to describe the steps to ensure a successful integration between an Eventide NexLog740 or NexLog840 Logging recorder and Cisco Call Manager using “SKINNY” Protocol via SPAN port.

This integration will be accomplished by utilizing the The Switch Port Analyzer (SPAN) feature of a managed IP switch, this is sometimes referred to as port mirroring. The NexLog will “sniff” the IP packets on the SPAN port, interpret the SKINNY protocol, and perform audio recording. The Switch Port Analyzer (SPAN) feature was introduced on IP switches initially for monitoring and debugging purposes. This same feature is used to aggregate VoIP call traffic from many VoIP calls/phones into one port. Once configured, the switch will forward IP packets from the mirrored ports to the designated “SPAN” port.

Configuring the Switch Port Analyzer (SPAN) feature on a Cisco switch (or other managed switch) is outside the scope of this document. However, a wealth of information can be found on a Cisco support page.

Once the switch is configured appropriately, there will be corresponding information to be entered into the “Cisco Call Manager “SKINNY” Protocol (SPAN)” template in the NexLog Web Configuration Manager.

6.4.1.1. Required Personnel

- Eventide dealer/reseller Technician
- LAN Administrator

6.4.1.1.1. Cisco Call Manager “SKINNY” Protocol (SPAN) configuration detail

6.4.1.2. NexLog firmware version and Licensing

Ensure that the NexLog is running Firmware Version 2.5.x (or greater). Ensure that the NexLog is licensed appropriately for VOIP/RTP VoIP Channels. VoIP recording is licensed in groups of 8 channels, this example system has 32 channels. If proper licenses are not present contact Eventide technical support before proceeding.

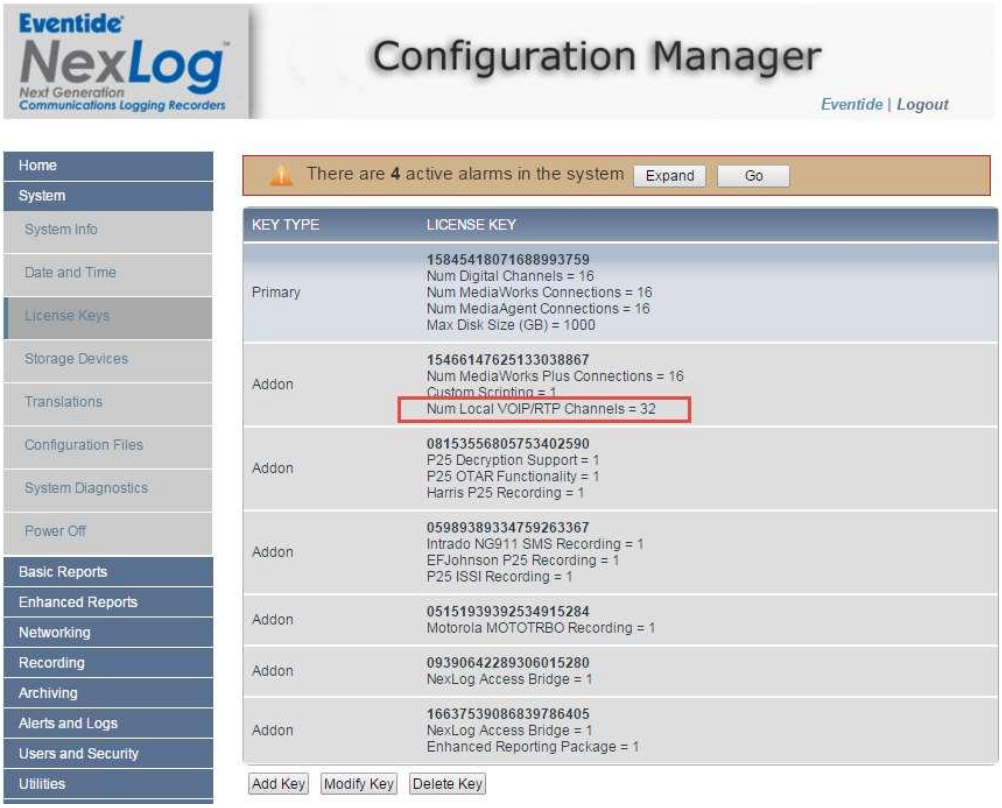


Fig. 6.35 Licenses in groups of 8

6.4.1.3. Configure physical Network Interface Card for SPAN

Connect a straight-through network cable from the Cisco Call Manager SPAN port to the corresponding physical network interface card that you are about to configure below.

On the network interfaces menu, select one of the currently unused Network Interface devices and Select “Type” SPAN. No other fields need to be entered.

Save the template.

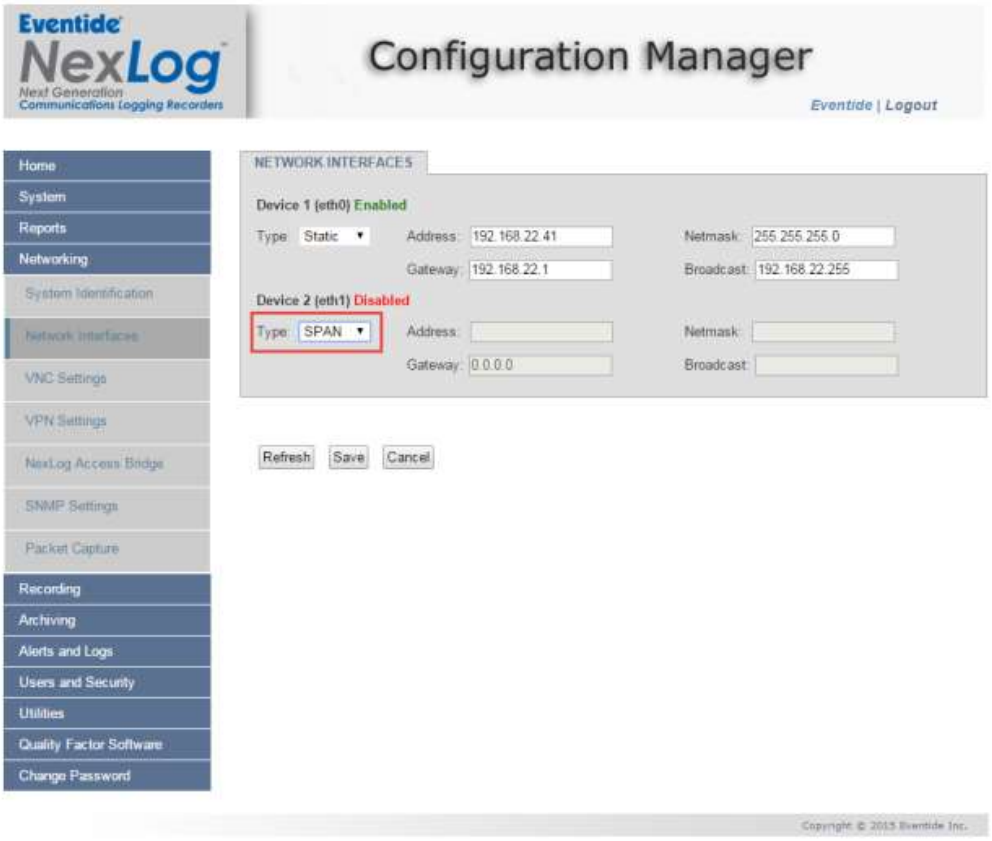


Fig. 6.36 Configure SPAN

6.4.1.4. Add Virtual Recording Interface

Fig. 6.37 Add Virtual Interface

6.4.1.5. Select the number of IP channels

Note, this is the maximum number of phones that can be recorded

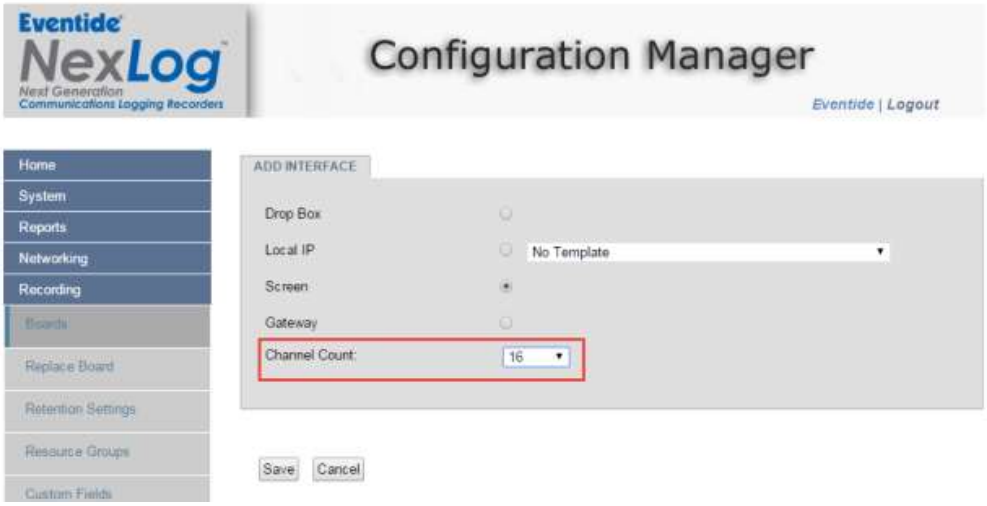


Fig. 6.38 Select IP Channels

6.4.1.6. Select “Cisco Call Manager “SKINNY” Protocol (SPAN)” Template

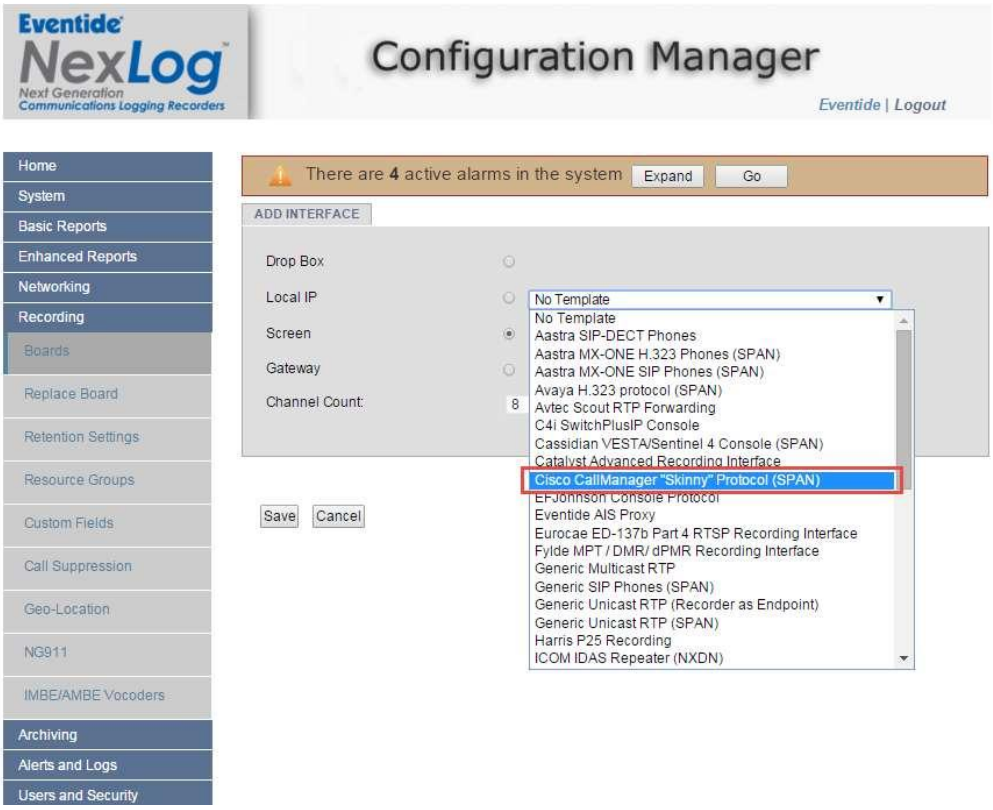


Fig. 6.39 Select Template

6.4.1.7. Fill in the Cisco Call Manager “SKINNY” Protocol (SPAN) Template Fields

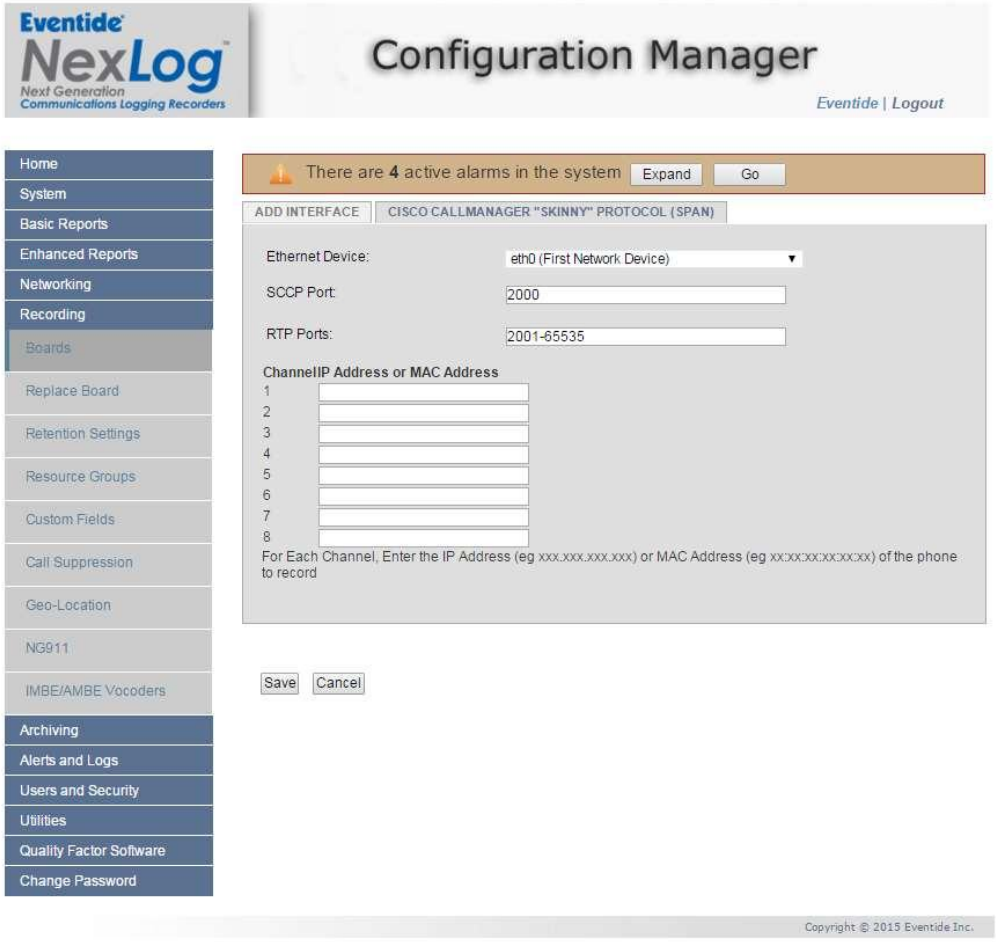


Fig. 6.40 Add Template Fields

Template Field Detail

Ethernet Device: Select the physical Ethernet/NIC of the NexLog recorder which is used to connect directly to the SPAN port, configured earlier in this section

- Typical Source: LAN Administrator

SCCP Port: Port used for SKINNY protocol, default is 2000 and typically this is used

- Typical Source: LAN Administrator

RTP Ports: RTP ports that the NexLog recorder will use to record audio, default is 2001-65535 and is typically not changed

- Typical Source: LAN Administrator

Channel IP or MAC Address: IP address or physical MAC addresses of phones connected to the ports to be recorded/mirrored to the SPAN port. If DHCP is used in the environment, it is recommended to use the physical MAC addresses

- Typical Source: LAN Administrator

6.4.1.8. Save the template

After filling in all the fields, select “Save”. The NexLog will configure itself to record from the configured SPAN port.

6.4.1.9. Verify Recording

Place a series of test calls between phones inside and outside calls. Use MediaWorks EXP or the front panel display to verify recording of all test calls.

6.5. Cisco CallManager Built-in-Bridge

6.5.1. Built-in-Bridge Introduction

The purpose of this document is to describe the steps to ensure a successful integration between an Eventide NexLog Express Logging recorder and Cisco Call Manager using Built in Bridge (BIB) for recording.

Built in Bridge, which Cisco defines as using the IP Phone’s internal DSP resources, not a SPAN of the Ethernet switch port, instead it uses a SIP trunk to record a duplicate stream of audio from the recorded phones via the phones own built in ‘bridge’. Following is a Cisco Diagram of the connectivity.

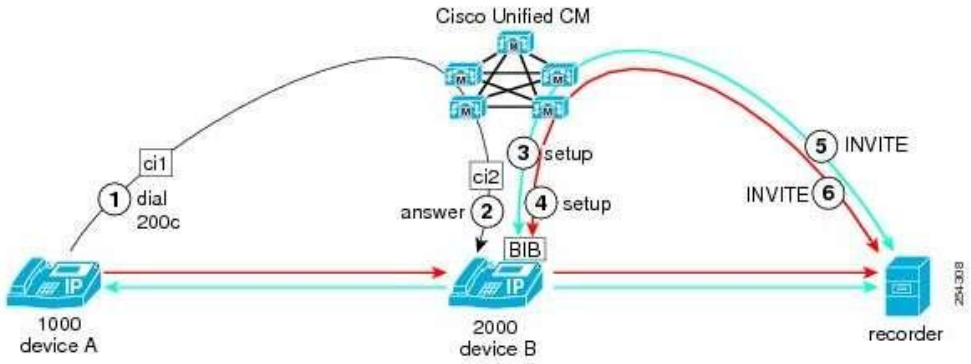


Fig. 6.41 Cisco Built-in-Bridge Diagram

Eventide supports Automatic Call Recording mode (without CTI), in this mode calls are delivered to the Eventide recorder of the previously mentioned SIP Trunk.

Configuring the Cisco Unified Call Manager for recording via the phones BIB is outside the scope of this document. However, the high level steps required are as follows:

- Ensure the Cisco Phones you want to record support the recording feature
- Create SIP profile for the Eventide recorder
- Create SIP trunk security profile
- Create SIP trunk that points to the Eventide recorder
- Create recording profile
- Create a route pattern for the Eventide recorder
- Enable Built-in-Bridge on all phones to be recorded
- Configure tones for recording
- Set the Codec configuration, Eventide supports G.711, G.722 by default and G.729a/b with optional licensing.

Once the Cisco Unified Call Manager is configured appropriately, there will be corresponding information that needs to be entered into the “SIP Trunk (SPAN, Endpoint, or Cisco BIB)” template in the NexLog Express Web Configuration Manager.

6.5.2. NexLog Express Configuration Overview

Each of the following steps will be explained or shown with screen shots:

- Confirm NexLog Express version and licensing
- Configure one of the NexLog Express physical Network Interface Cards to a free IP address

- Add a virtual recording interface board
- Select the number of VoIP channels and “Cisco CallManager Built-in-Bridge” Recording Template
- Fill in the required fields
- Save the template
- Verify recording

> **Note**
>
> Where data entry is required, the “Typical Source” to ascertain the data from is noted.

6.5.3. Cisco Unified Call Manager Built-in-Bridge Configuration Detail

6.5.3.1. NexLog Express firmware version and Licensing

Ensure that the NexLog Express is licensed appropriately for VOIP/RTP VoIP Channels. VoIP recording is licensed in groups of 8 channels, this example system has 32 channels. If proper licenses are not present contact Eventide technical support before proceeding.

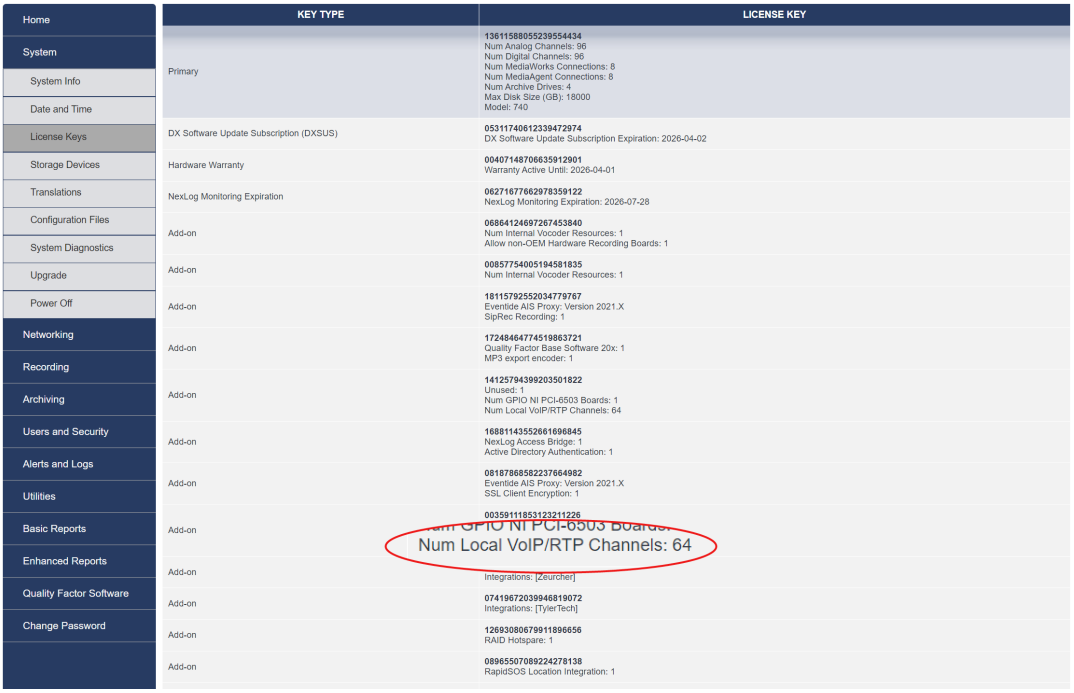


Fig. 6.42 VOIP License

6.5.3.2. Configure physical Network Interface Card

Connect a straight through network cable from the corresponding Network Interface Card on the Eventide recorder to a switch port that will have access to the network that the phones reside on.

On the network interfaces menu, select one of the currently unused Network Interface devices and Select “Type” Static. DHCP is supported, but not recommended because if the IP address changes, the new IP address will need to be entered into other configuration screens. Enter appropriate Netmask, Gateway and Broadcast addresses for the network.

Save the template.

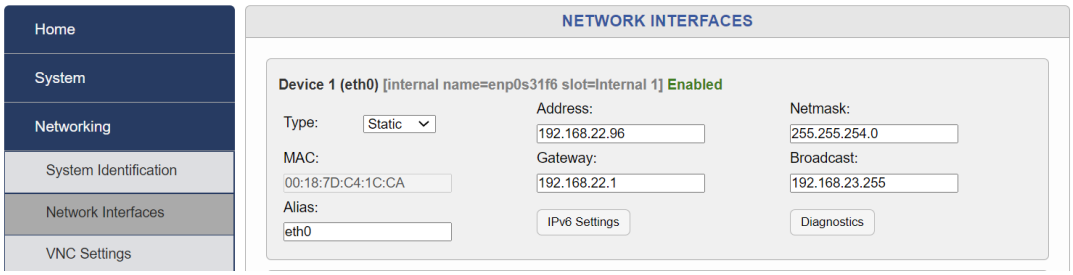


Fig. 6.43 Network Interface

6.5.3.3. Select “Cisco CallManager Built-in-Bridge” Template and Number of Channels

In order to add the Cisco CallManager Built-in-Bridge Template, Navigate to Recording > Recording Interfaces > Add Virtual Recording Interface

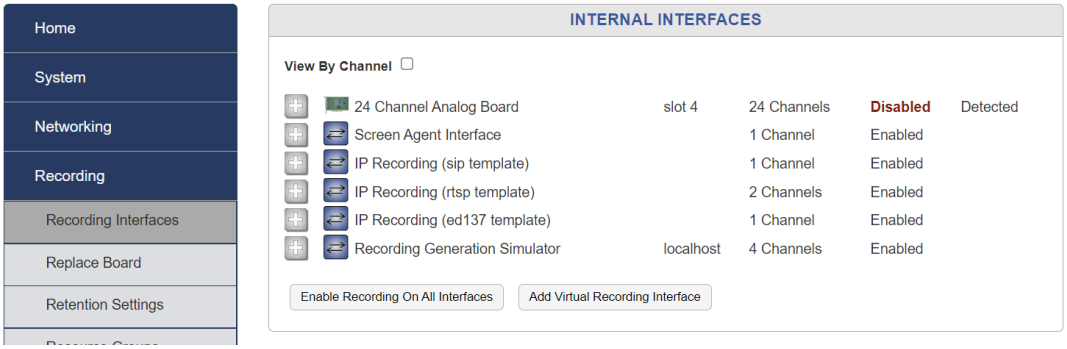


Fig. 6.44 Add Interface

Select Cisco CallManager Built-in-Bridge and note that the number of IP channels selected is the maximum number of simultaneous calls that can be recorded at one time. The NexLog Express must be licensed for at least this number of VoIP Channels.

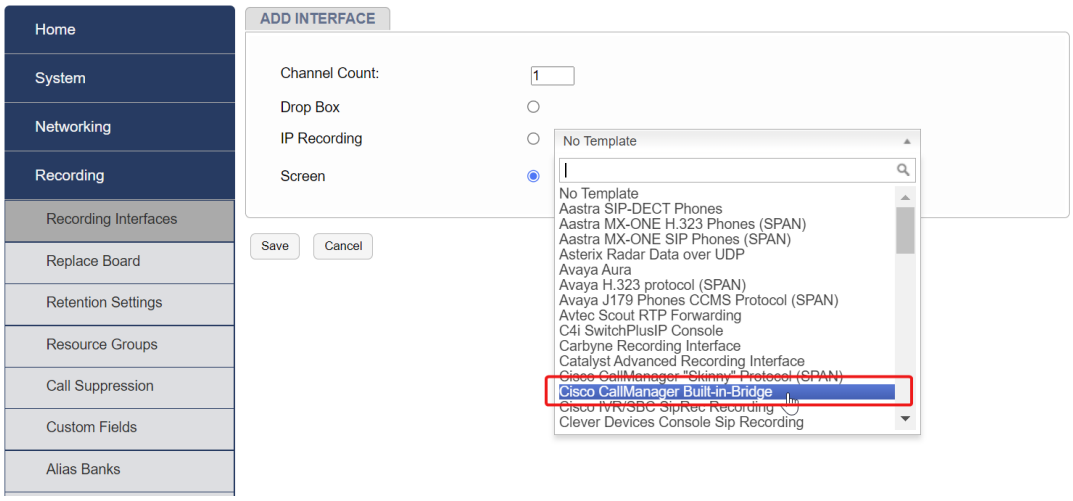


Fig. 6.45 Add BIB Interface

6.5.3.4. Fill in the “Cisco CallManager Built-in-Bridge” Template Fields

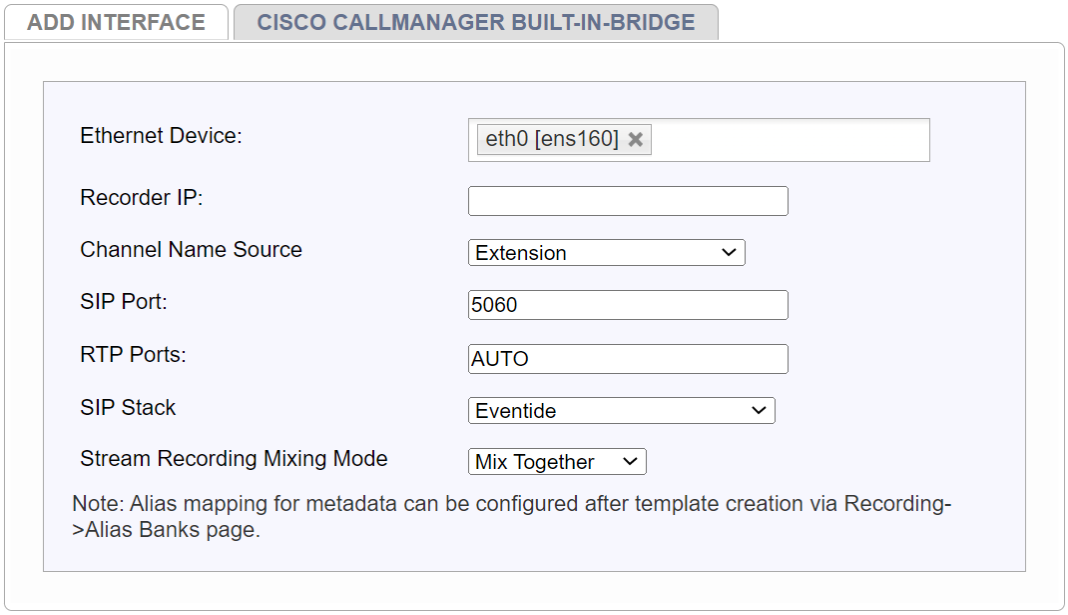


Fig. 6.46 Add BIB Interface Configurations

Template Field Detail

- Ethernet Device: Select the physical Ethernet/NIC of the NexLog Express recorder which is used to receive the SIP trunk carrying the BIB calls.

- Recorder IP: IP address of the Eventide recorders Network Interface Card
- Channel Name Source: Choose which piece of metadata will be used to name the channel when recordings are stored.
    - Extension: Use extension of the phone being recorded.
    - Near End Device Identifier: Use the device name identifier as defined in the Cisco Call Manager.
- SIP Port: Default is 5060 and should not be changed, unless otherwise instructed to do so.
- RTP Ports: Default is 6000-7000, do not change, unless otherwise instructed to do so.
- SIP Transport Protocol: Enter SIP over UDP or SIP over TCP as appropriate.

New in version 2024.1.

- Field Mappings: This optional section allows the ability to map and extract more complex metadata fields to channel name display, e.g. MAC Address.

To add specific Field Mapping data, select Edit and populate all requested Metadata Field Name and SIP Field Taxonomy data. Once entered, Select Populate then Save.

> **Note**
>
> Multiple entries can be added.

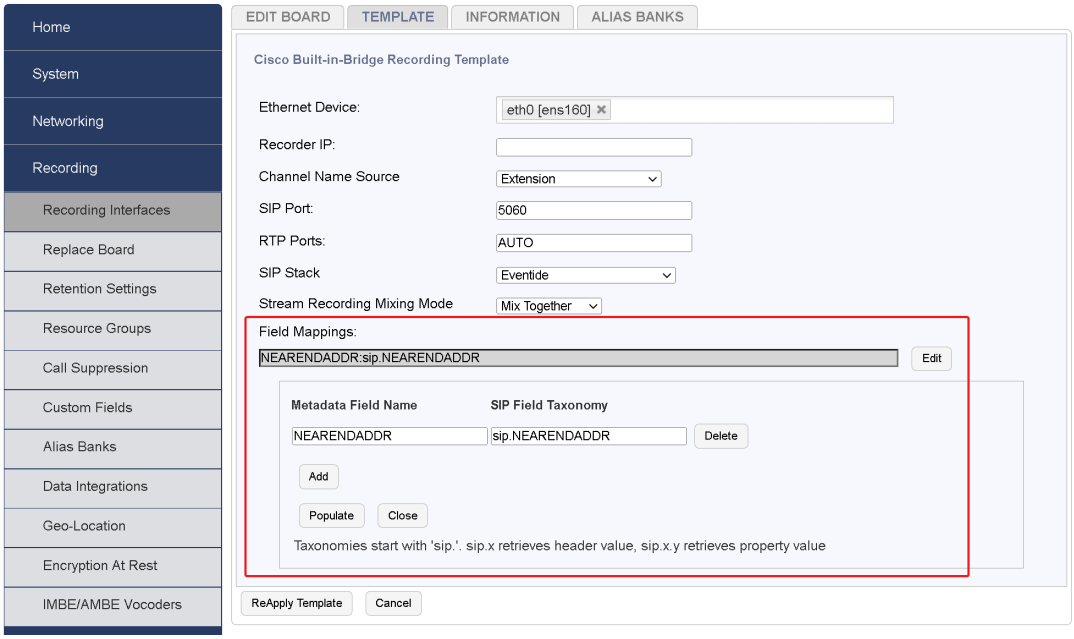


Fig. 6.47 Add BIB Field Mappings

These settings are also available by expanding the channel view and selecting the gear icon under the MORE tab.

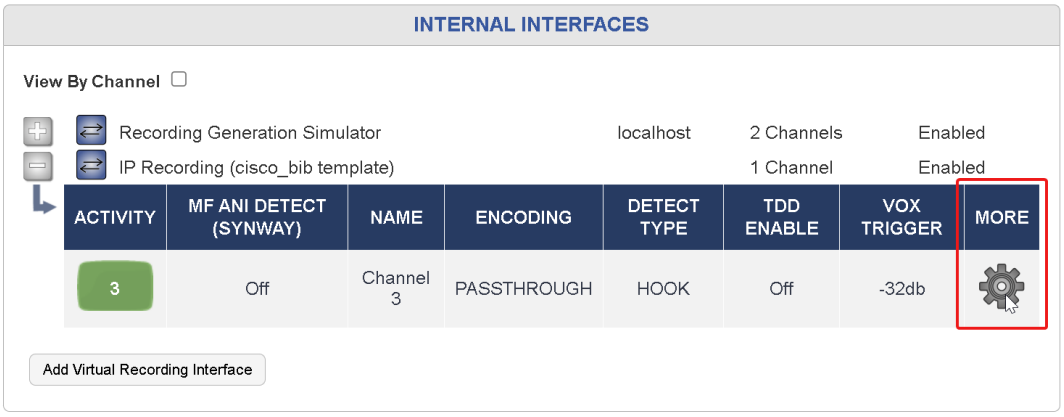


Fig. 6.48 Add BIB Field Mappings

The Field Mappings can be added under the RTP tab in the Metadata Settings.

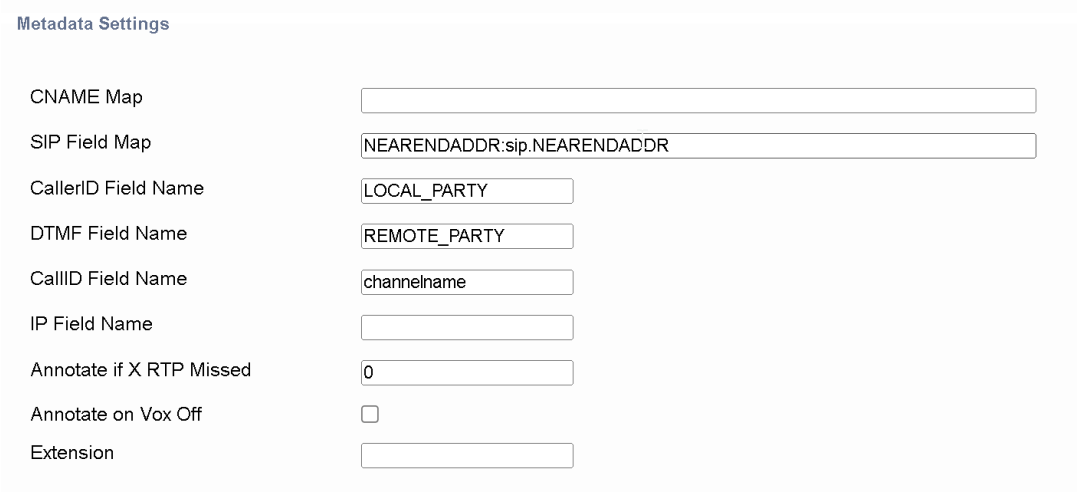


Fig. 6.49 Add BIB Field Mappings

6.5.3.5. Save The Template

After filling in all the fields, click Save. The NexLog Express is ready to record.

6.5.3.6. Verify Recording

Place a series of test calls between phones inside and outside calls. Use MediaWorks EXP or the front panel display to verify recording of all test calls.

6.5.3.7. Troubleshooting

SYMPTOM	Possible Causes/Solutions
NexLog Express Not Recording	Check IP connectivity between NexLog Express and Network port
MediaWorks EXP does not play back P25 calls	Check IP Connectivity between NexLog Express and local LAN

6.6. Motorola Dimetra AIS Interface

6.6.1. Motorola Dimetra AIS Interface Introduction

The purpose of this document is to describe the requirements for a successful integration between the Eventide NexLog Express 740/840 recorders and the Motorola DimetraIP, DimetraIP Compact or DimetraIP Micro via the Motorola MCC 7500 Archiving Interface Server (AIS), Voice Processing Module (VPM) and CRAM. The CRAM is a CORBA based software that provide an interface between the AIS and the NexLog Express recorder.

Required Personnel

- Eventide dealer/reseller Technician
- Motorola Field or Systems Engineer
- Customer Network Administrator
- Eventide support/deployment engineer

License Required

This feature must be licensed to be used. Contact your Eventide Communications Dealer for assistance.

6.6.2. Install and configure AIS and CRAM

The Archiving Interface Server (AIS) is Motorola provided software tool used to deliver audio and metadata to third party recording solutions, such as the Eventide NexLog Express products. In a Dimetra environment the AIS is effectively “wrapped” by the CRAM and the CRAM in turn presents an interface to the recording solution over the IP network. Detailed configuration details surrounding the AIS and CRAM are outside the scope of this document. However, the details of what is needed from the AIS/CRAM to properly configure the NexLog Express are outlined here.

- Install the AIS application and CRAM application on Motorola provided or specified workstation
- Configure the CRAM parameters via the “Remote API Configurator”, example screen shown below

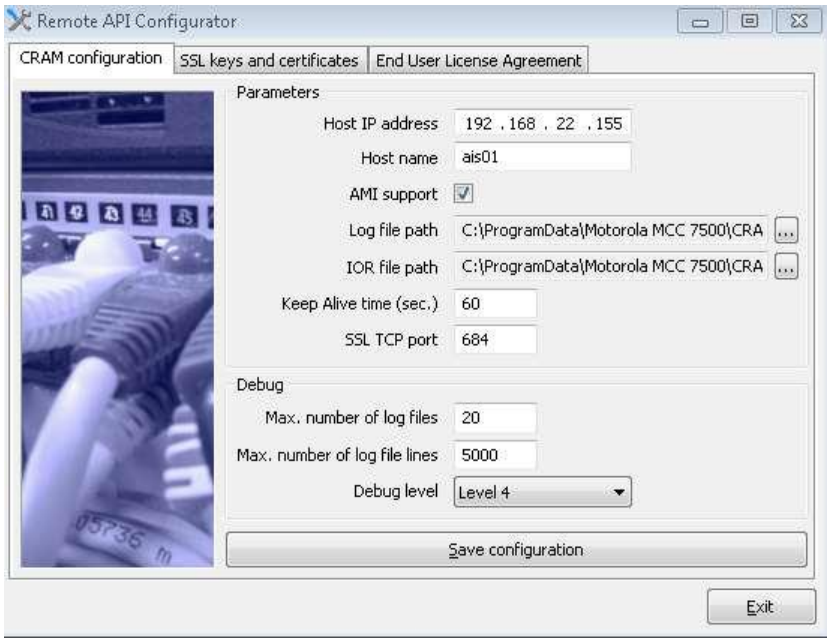


Fig. 6.50 CRAM Configuration

- Using the “SSL keys and certificates” tab in the “Remote API Configurator”, Generate the Common name (cert.), Common name (keys) and supply password.

> **Note**
>
> the files generated here will be used later to configure the NexLog Express Dimetra recording board.

6.6.2.1. Add Virtual Recording Interface

Select the number of IP channels/number of talk paths, then select the “Motorola Dimetra AIS Interface” Template

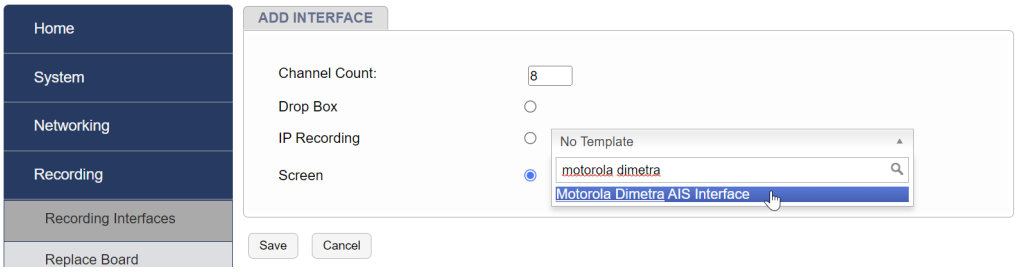


Fig. 6.51 Add Interface

> **Note**
>
> this is the maximum number of talk paths between the NexLog Express and the AIS that can be recorded. Not to be confused with “Talk Groups”, multiple Talk Groups can be on one “Talk Path”.

6.6.2.2. Motorola Dimetra AIS Interface Template Fields

The following figure has the fields populated for illustrative purposes, the actual values in each installation will most likely be different. Verify each value with the Motorola Field Engineer or the Customer Network Administrator.

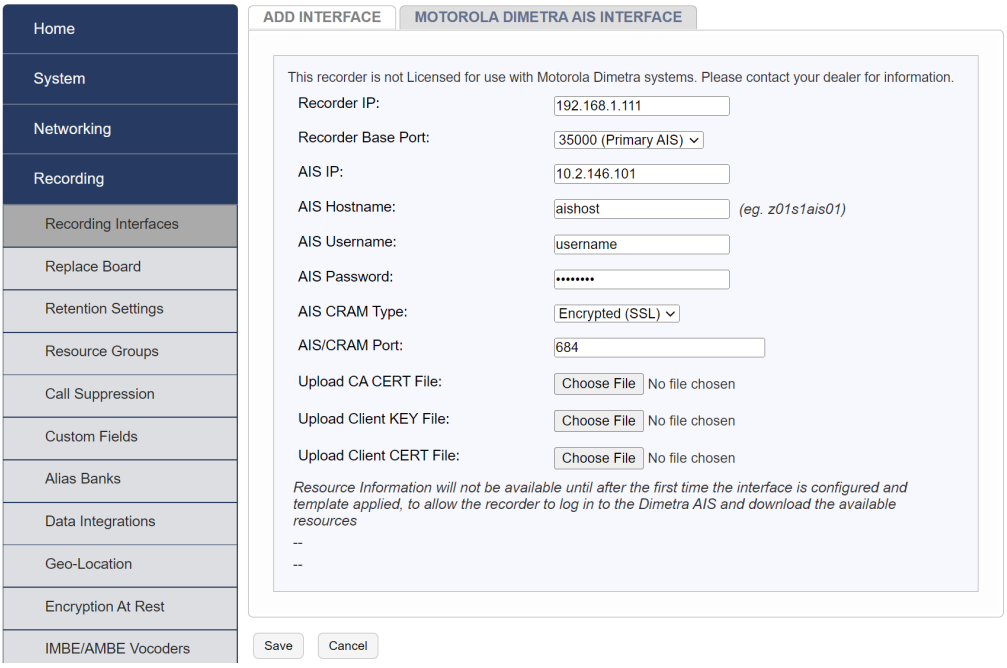


Fig. 6.52 Interface Configuration

Template Field Details

Recorder IP: IP address of the NIC device on the NexLog Express that has access to the AIS

- Typical Source: Customer Network Administrator

Recorder Base Port: 35000 when configuring primary AIS, 37000 when configuring secondary AIS

- Typical Source: Customer Network Administrator or Motorola Field Engineer

AIS IP: IP address of the AIS that will be serving the NexLog Express calls

- Typical Source: Customer Network Administrator or Motorola Field Engineer

AIS Hostname: Host name of the AIS on the network

- Typical Source: Customer Network Administrator

AIS Username and password: Credentials that can log into the AIS and access Dimetra resource information

- Typical Source: Customer Network Administrator or Motorola Field Engineer

AIS CRAM type: Select either SSL or non-SSL. As of the writing of this document, Eventide is of the understanding that Motorola does not support the non-SSL version

- Typical Source: Customer Network Administrator or Motorola Field Engineer

AIS CRAM Port: UDP port that will connect the NexLog Express Recorder and AIS/CRAM

- Typical Source:Customer Network Administrator or Eventide Communications Dealer/Reseller

Upload CA CERT File: This file will have been previously generated using the Motorola provided “Remote API Configurator”, see “Install and configure AIS and CRAM”

- Typical Source: Customer Network Administrator or Motorola Field Engineer

Upload Client KEY File: This file will have been previously generated using the Motorola provided “Remote API Configurator”, see “Install and configure AIS and CRAM”

- Typical Source: Customer Network Administrator or Motorola Field Engineer

Upload Client CERT File: This file will have been previously generated using the Motorola provided “Remote API Configurator”, see “Install and configure AIS and CRAM”

- Typical Source: Customer Network Administrator or Motorola Field Engineer

6.6.2.3. Apply the template

After filling in all the fields, select “Save”. The NexLog Express will now attempt to save the template data and initialize for recording.

Note

After selecting “Save”, it could take up to 30 seconds or more to complete the communication to the AIS/CRAM. When the process completes, you will be returned to the main recording boards page, example shown below

6.6.2.4. Select Talk Groups and Re-Apply the Template

Select the newly created “Local IP Recording (dimetra template), the template will now be populated with the same information initially entered, with the addition of lists of Group Calls and Private calls that could be setup to record. You can select the Group Call group name and Private call units to be recorded by selecting on the “record” checkbox. The priority of recording for that resource can also optionally be changed. Note, the lists can be large, so filters and select all options are provided as a convenience to the user. Once you have selected all the resources to be recorded, select the Re-apply Template button and Save the template.

After the system indicates successful saving of the template, the system should be ready to record.

6.6.2.5. Check for Alerts

Check the NexLog Express front panel and/or configuration manager (figure below) for any system alerts or Tait Radio specific alerts. There will be alerts specific to the Tait Radio integration if there are problems with downloading talk groups, managing crypto keys and OTAR.

6.6.2.6. Verify Recording

Place a series of test calls between radios on both encrypted and unencrypted talk groups. Use MediaWorks EXP or the front panel display to verify recording of all test calls. Following is an example of Diemtra test calls and some of the associated metadata available.

6.6.2.7. Verify Recording after Restart

Reboot the NexLog Express and verify that recording resumes automatically, this will verify that the system will continue to record after a power failure or shutdown.

6.6.2.8. Ensure the NexLog Express has a Time Synchronization source

It is important that the NexLog Express have a time synchronization source set to the same source as the AIS. It has been seen in the field that when the NexLog Express’s time drifts from the that of the AIS the

AIS can stop sending calls to the NexLog Express. The Time Sychronization settings on the NexLog Express can be found in the System>>Date Time section of Web Config.

6.7. EFJohnson Console Protocol

This document describes the steps necessary to configure an Eventide NexLog Express recorder to record and playback radio traffic from an EFJohnson radio system. These steps are in addition to any standard source independent steps to configure the NexLog Express recorder, such as adding license keys, etc.

6.7.1. Configuring an Eventide Recorder to capture EFJohnson multicast P25 traffic

License Required

This configuration requires the following licenses:

- Local RTP licenses to cover channel count being created on the template
- EFJohnson P25 Recording License
- Internal Vocoder Resources" license
- Num Internal Vocoder Resources

Contact your Eventide Communications Dealer for assistance.

Source audio from the EFJohnson radio system can arrive at the recorder in one of two formats depending on the radio system type and configuration. P25 Radio Channels will transmit the audio using the AMBE codec. AMBE is a popular codec used on P25 radio systems. Analog Radio channels may instead transmit the audio using the G.711 codec. Eventide NexLog Express recorder supports recording either codec, including hybrid systems providing some channels in analog and some in AMBE.

If AMBE channels are to be recorded, the NexLog Express will require a vocoder device to be configured. On playback, the NexLog Express will send the AMBE audio to the vocoder device to be decoded prior to sending the audio to the client. This is not necessary for G.711 audio, which can be fully decoded internally by the NexLog Express recorder.

6.7.1.1. Configuring the Eventide NexLog Express to capture multicast P25 traffic

Step 1: Determine the address of the Eventide NexLog Express recorder after connecting it to the network

- Select System
- Select System Info
- The IP address will be listed on the page
- Adjust the network settings

Step 2: Set a static IP on the Eventide NexLog Express recorder

- Use the Front Panel or a web browser pointed at the IP address discovered above
- Navigate to Networking->Network Interfaces
- Select Static from the Type drop-down box and change the IP address as needed

Step 3: Configuring EF Johnson RoIP capture

Either the Front Panel or a web browser can be used to configure the RoIP virtual board. The following instructions are for a desktop browser, which is the recommended method:

- Open your browser (Microsoft Edge, Firefox, Chrome) and go to the IP address of the recorder
- select the Configuration Manager icon
- When prompted, login with factory default credentials. Username: Eventide, password: *recorder's serial#*

> **Note**
>
> once installation/configuration is completed, Eventide recommends changing the default admin account to utilize a stronger password

- select the Recording menu item on the left
- Select Recording Interfaces
- select the Add Virtual Recording Interface button
- In the Channel Count drop-down select the number of channels you want to add. This number should be less than or equal to the number of Local VOIP/RTP Channel licenses

- Select the Local IP radio button
- Select EFJohnson Console Protocol in the template drop-down box
- Select the EFJOHNSON CONSOLE PROTOCOL tab
- Select the Ethernet device that is connected to the network with the RTP traffic
- Enter the IP address of the EFJohnson Atlas/JEM server in the AMBE Transcoder IP field.
- Select “Decrypt and Transcode at Playback” to leave the audio on the recorder’s RAID as encrypted (if incoming audio is encrypted). The recorder will use the JEM server to decrypt the radio traffic and also transcode it at playback time. Because the audio will be encrypted at all times and only decrypted when playback occurs, this setting is more cryptographically secure, however, the decryption keys must remain available in the JEM server for the life of the audio. If a key is removed or changed on the JEM server, the NexLog Express will no longer be able to playback audio encrypted with that key.
- Select “Decrypt at Record, Transcode at Playback” to use the JEM server to decrypt the incoming radio calls and store them unencrypted on the RAID. It will transcode calls on the recorder itself at Playback. If no encrypted audio will be used on the EFJohnson radio system, either option will work, but this one is recommended.
- It is likely the Default RTP Port field can remain 20000,30000, but it can be changed to match your configuration.
- Normally only a single transmission can be present on a given EFJohnson channel at a time. However, in the case of Console Preemption (Talkover) of an emergency radio call, the console performing the preemption may still be able to hear the radio audio being preempted, though other positions cannot. In this case, a single channel can be sending multiple audio feeds. To record both feeds, at least one channel should be dedicated to call preemption by entering TALKOVER in the IP address field. This channel will then be used as a destination channel for preemption audio. This will allow both the original call and the preempting call to be recorded at once. The number of TALKOVER channels configured determines the maximum simultaneous number of preemption call pairs that can be recorded.

> **Note**
>
> VLR Multicast Address, VLR Multicast Port, and Multicast Base Address are used for recording SuperGroups and can be left at their default values unless specific values are needed are required.

- Enter the multicast addresses for each channel. On some older EFJohnson systems a single channel may utilize multiple multicast addresses. If this is the case, enter the two IP addresses separated by a space. More recent EFJohnson radio systems utilize two ports (20000 and 30000) on a single multicast address to accomplish this instead, in which case this is not necessary. Note that only

audio transmitted over a configured multicast group will be recorded. Audio sent via Unicast or Supergroup will not be recorded.

- In the Codec drop-down for each channel select whether the channel will be recording P25 AMBE traffic or G.711 uLaw traffic
- select the Save button

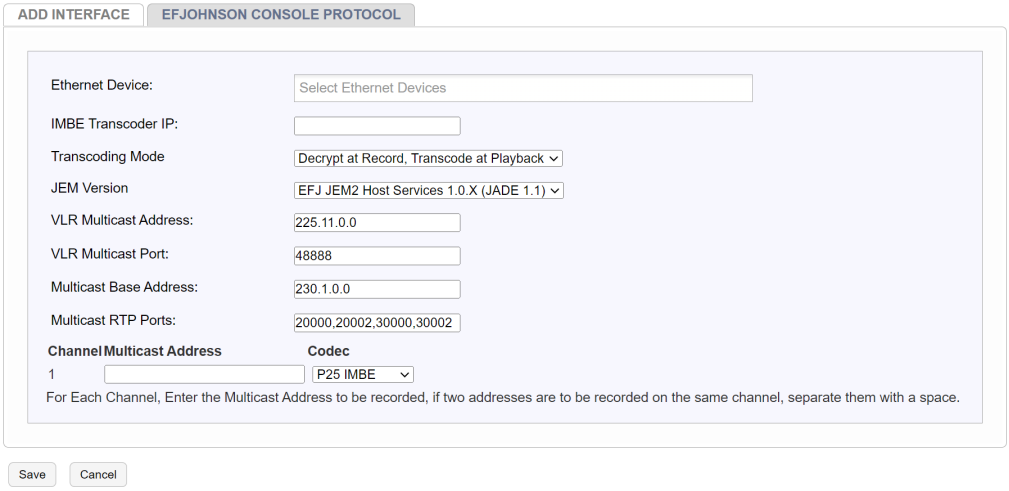


Fig. 6.53 EF Johnson Configuration

- select the plus sign (+) next to “Local Ip Recording (EFJohnson template)” to display the channels for the virtual board
- select the VOX HOLD TIME column header and select “Set All Values -> Timeout” from the drop-down menu
- Move the slider to the left until it displays “1 Sec.”
- select the VOX HOLD TIME column header again and select “Insert Col.”

Note

By default, the Talkgroup ID will be placed in the DTMF field. To change this field to a different name such as “TG_ID”, go to Recording->Custom Fields and then follow the following configurations:

- select on the UNSET column header and select “rtp dtmfFieldName” near the bottom of the list
- select on the RTP DTMFFIELDNAME column header and select “Set All Values -> rtp dtmfFieldName.”
- Type TG_ID into the entry field and press Enter

Important

Only one EFJohnson virtual board should be created per system.

Step 4: Modifying settings after initial configuration

- After configuring the recorder with the desired number of channels using a template, you can make future changes to the template by navigating to the Recording Interfaces page in the Configuration Manager, selecting the EFJohnson board, changing the template, and selecting the “ReApply Template” button. Note that if the template is reapplied any manual changes made to the board or board’s channels outside of the template prior to the reapply will be overwritten by the template application.

6.7.1.2. Playing back recorded AMBE calls

License Required

Playback requires a DVSI License for playback even though it uses the JEM server for conversion. Contact your Eventide Communications Dealer for assistance.

Recordings can be played back from either the Front Panel under Replay mode, via the MediaWorks EXP application, or via the MediaWorks EXP Express web application. Please consult the user’s manual for more information.

In MediaWorks EXP it is possible to determine how a call in the data grid is currently stored on the recorder by right selecting the data grid header and turning on the ‘compression’ setting. Calls recorded for JEM usage will initially always be EFJ_RAW (even if unencrypted). If configured to decrypt at record time they will be queued up for batch processing and changed to AMBE as the JEM server decrypts them. If configured to decrypt at playback, they will remain as EFJ-RAW.

6.7.1.3. Vocoder Related Recorder Alerts

There are two NexLog Express Recorder Alerts that can be raised by the NexLog Express relating to the vocoders. The JEM Server can result in a “Recorder Timeout” alert if the recorder sends audio to the JEM server for processing and gets no response within a few seconds. If the timeout was due to offline decryption, the recorder will automatically periodically retry the decryption. If the timeout was due to online decoding (playing a call in MediaWorks EXP) it will be necessary to restart the playback by double selecting the call in the data grid or pressing stop and then play in the transport, once the cause of the timeout is resolved. The most common causes of timeout alerts are lost packets on the network between the recorder and vocoder, or if the vocoder is unreachable on the network because it is powered down, configured for the wrong IP address, etc.

The second alert is raised in the following scenario. Each call received from the EFJohnson radio system will contain a header declaring whether the call is unencrypted, encrypted using the DES algorithm, or encrypted using the AES algorithm. If encrypted, it will also contain the KeyID of the key on the JEM server that should be used to decrypt the call. If the JEM server is not loaded with a key for that KeyID, the recorder will raise an alert about the invalid KeyID and will not be able to decrypt that call. Note that if a key of that ID is loaded on the JEM server but the key is incorrect, the recorder has no way to detect this and the JEM server will decrypt the audio incorrectly and it will not be intelligible on playback, but no alert will be raised.

6.8. Harris P25 Recording

6.8.1. Harris P25 Recording Introduction

The purpose of this document is to describe the steps to ensure successful integration between an Eventide NexLog Express and Harris’ VIDA System Release SR10A. The document assumes knowledge of the NexLog Express front panel interface and the browser-based configuration manager and does not discuss recording interfaces beyond the Harris integration. For more details on these interfaces, please refer to their respective manuals.

Required Personnel

- Eventide dealer/reseller Technician
- Harris Radio System Technologist (ST)
- Customer Network Administrator

- Eventide support/deployment engineer

License Required

This feature must be licensed to be used for the following:

- VOIP/RTP VoIP Channels
- P25 decryption (if Crypto is being used)
- OTAR functionality (if OTAR is being used)
- Harris P25 Integration

Contact your Eventide Communications Dealer for assistance.

6.8.2. Adding a Virtual Recording Interface

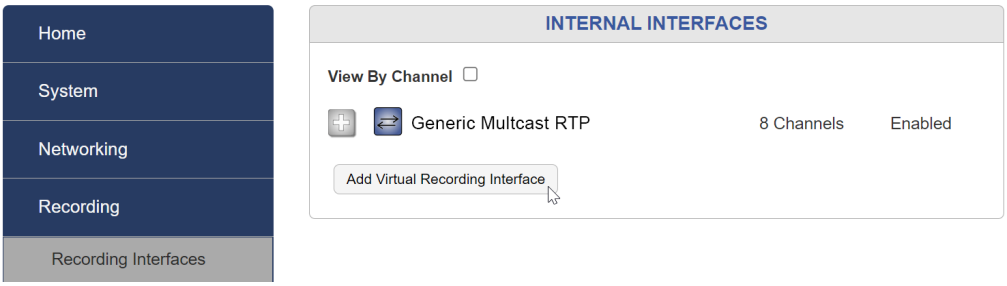


Fig. 6.54 Add Virtual Recording Interface

Select the number of IP channels/number of talk paths and “Harris P25 Recording” Template

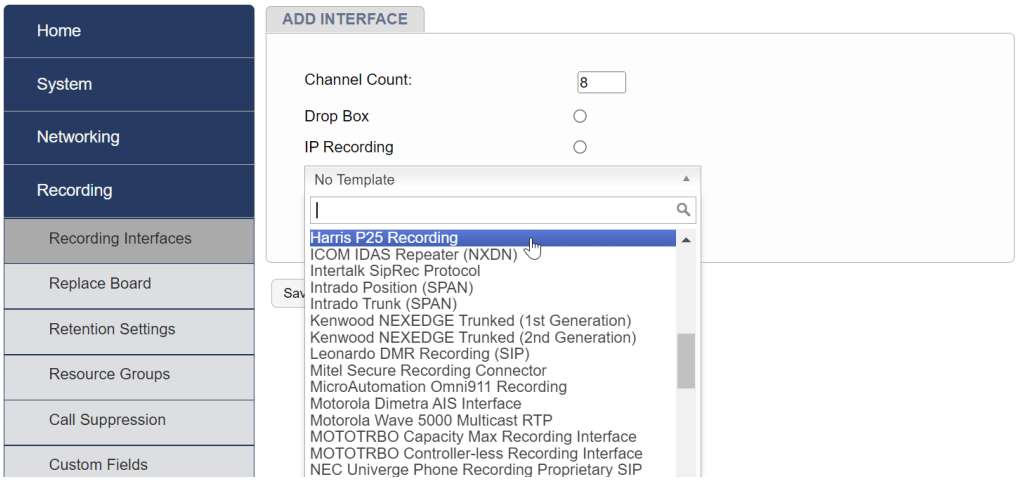


Fig. 6.55 Select Channels and Template

6.8.2.1. Template Field details

The following figure has the fields populated for illustrative purposes, however, the actual values in each installation will most likely be different. Verify each value with the Harris ST or the Customer Network Administrator.

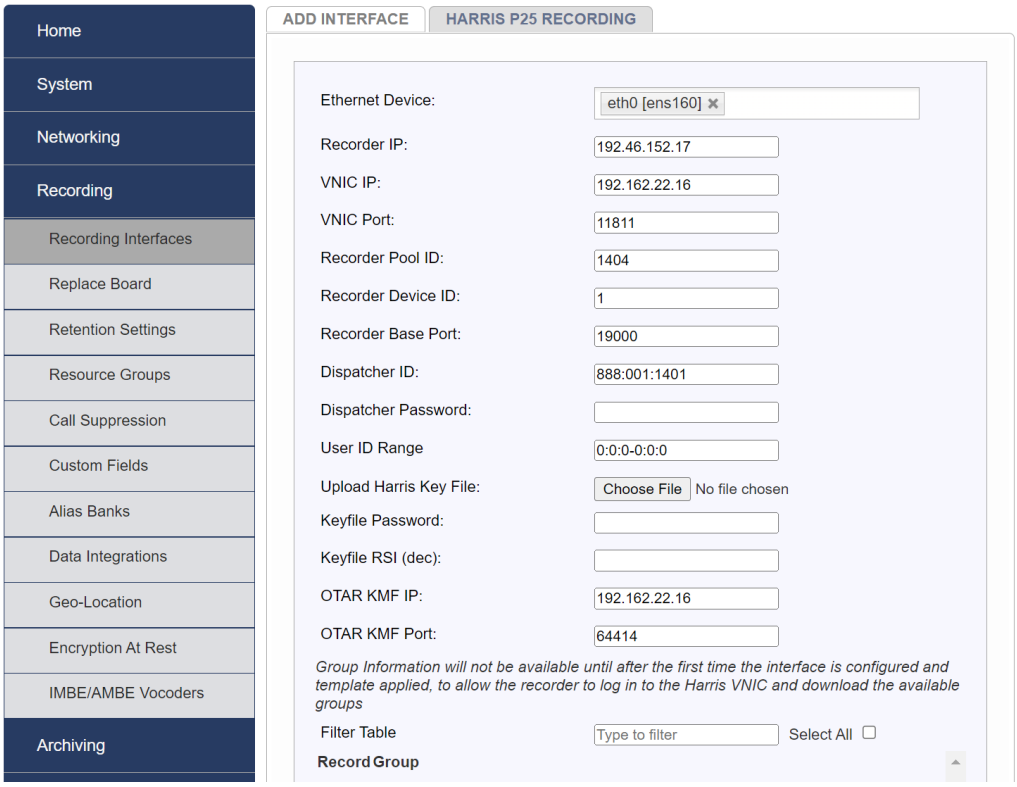


Fig. 6.56 Template Field Details

Ethernet Device: Select the physical Ethernet/NIC of the recorder which is connected the Harris VIDA LAN switch

- Typical Source: Customer Network Administrator

Recorder IP: IP address of the recorder

- Typical Source: Customer Network Administrator

VNIC IP: IP address of the VNIC on the VIDA Network which will be the interface to the recorder

- Typical Source: Harris ST

VNIC Port: UDP port on which the NexLog Express and VNIC will exchange control data during initial and subsequent configuration (Typically this is 11811)

- Typical Source: Harris ST

Recorder Pool ID: Unique recorder pool ID on the VNIC available for the recorder

- Typical Source: Harris ST

Recorder Device ID: Unique recorder device ID on the VNIC designated for the recorder (usually 1)

- Typical Source: Harris ST

Recorder Base Port: Base/Starting UDP port on which the NexLog Express will look for recording data (default 19000, unless otherwise advised, leave at 19000)

- Typical Source: Eventide support/deployment engineer

Dispatcher ID: Dispatcher ID within the VIDA environment that has access to all talk groups to be recorded

- Typical Source: Harris ST or Customer Network Administrator

Dispatcher Password: Password of the above ID

- Typical Source: Harris ST or Customer Network Administrator

User ID Range: Range of Radio User IDs that will be recorded during “I-calls” (defaults is “0:0:0-0:0:0”, meaning all, leave as the default unless otherwise informed)

- Typical Source: Harris ST

Upload Harris Key File: The crypto key file must be supplied by the Harris ST or Customer Network Administrator if any encrypted recording is required, regardless if OTAR will be used

- Typical Source: Harris ST or Customer Network Administrator

Key file Password: Password required to unlock the above Key File. If the key file is unencrypted, the password field is left blank

- Typical Source: Harris ST or Customer Network Administrator

OTAR KMF IP: IP address of the Key Manager Facility (KMF) which manages Over The Air Rekeying (OTAR), leave blank if OTAR will not be used

- Typical Source: Harris ST or Customer Network Administrator

OTAR KMF Port: UDP port over which the Key Manager Facility (KMF) will communicate to the recorder, leave blank if OTAR will not be used

- Typical Source: Harris ST or Customer Network Administrator

6.8.2.2. Apply the template

After filling in all the fields, select “Save”. The NexLog Express will now attempt to contact the VNIC and download the available talk groups to the recorder.

> **Note**
>
> Setup time can take anywhere from 3 seconds to more than a couple of minutes to return the available talk groups for recording, depending on the amount of data being returned. If the template does not return any talk groups, this must be resolved before proceeding further.

There are several reasons why the talk groups may not be returned:

- VNIC IP not visible to the NexLog Express, verify firewall settings with Harris ST
- UDP Ports between the recorder and VNIC are being blocked by the firewall
- Incorrect Dispatcher ID and/or password, verify with Harris ST

Select the desired talk groups and “Reapply Template”

6.8.2.3. Check for Alerts

Check the NexLog Express front panel and/or configuration manager (figure below) for any system alerts or Harris-specific alerts. There will be alerts specific to the Harris integration if there are problems with downloading talk groups, managing crypto keys, and OTAR.

6.8.2.4. Verify Recording

Place a series of test calls between radios on both encrypted and unencrypted talk groups. Use MediaWorks EXP or the front panel display to verify the recording of all test calls.

6.9. Intrado SipRec Recording

6.9.1. Intrado SipRec Recording Introduction

The purpose of this document is to describe the steps to ensure successful integration between an Eventide NexLog Express and Intrado's SipRec Recording system. The document assumes knowledge of the NexLog Express front panel interface and the browser-based configuration manager and does not discuss recording interfaces beyond the Intrado integration. For more details on these interfaces, please refer to their respective manuals.

Required Personnel

- Eventide dealer/reseller Technician
- Intrado Technologist (ST)
- Customer Network Administrator
- Eventide support/deployment engineer

License Required

This feature must be licensed to be used for the following:

- VOIP/RTP VoIP Channels
- P25 decryption (if Crypto is being used)
- OTAR functionality (if OTAR is being used)
- Intrado Integration

Contact your Eventide Communications Dealer for assistance.

6.9.2. Adding a Virtual Recording Interface

Start by adding a Virtual Recording Interface.

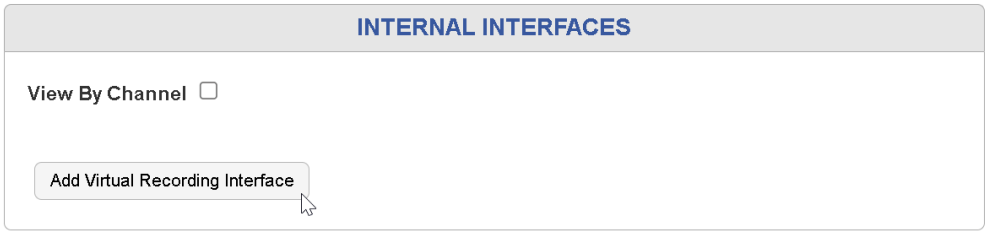


Fig. 6.57 Add Virtual Recording Interface

Select the number of IP channels/number of talk paths and “Intrado SipRec Recording” Template

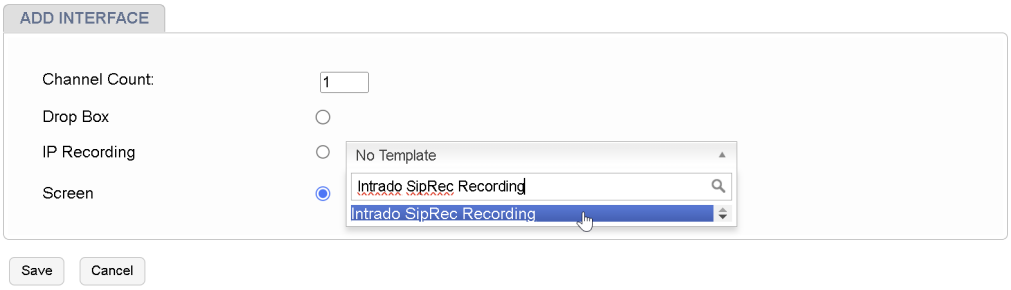


Fig. 6.58 Select Channels and Template

6.9.2.1. Template Field details

The following figure has the fields populated for illustrative purposes, however, the actual values in each installation will most likely be different. Verify each value with the Intrado ST or the Customer Network Administrator.

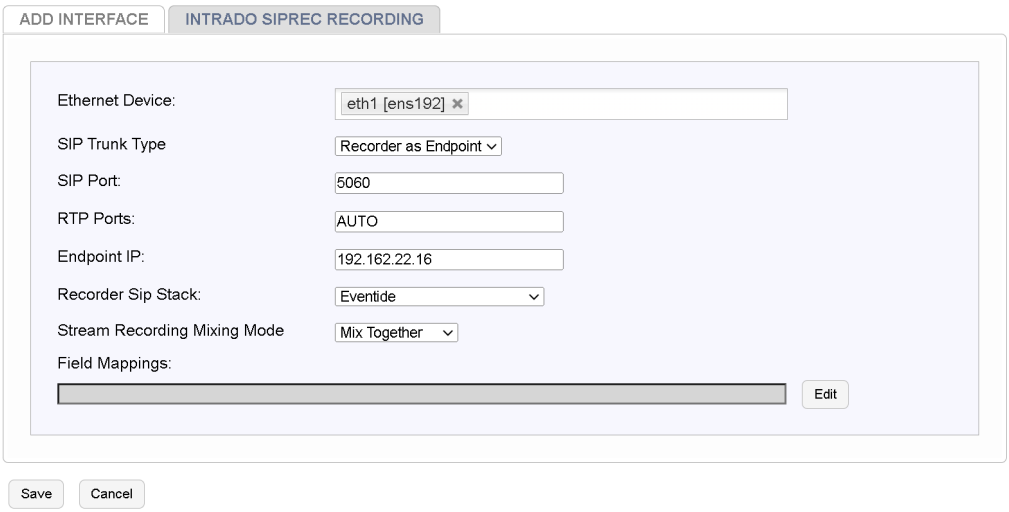


Fig. 6.59 Template Field Details

Ethernet Device: Select the physical Ethernet/NIC of the recorder which is connected to the network carrying the SIPREC call data

SIP Trunk Type: Recorder as Endpoint

SIP Port: 5060 (settings may differ)

RTP Ports: Auto

Endpoint IP: IP of the recorder's NIC which will receive the SIPREC/RTP data

Recorder Sip Stack: Can either be "Eventide" or "Eventide w/ TLS on next port"

Stream Recording Mixing Mode: Can be "Mix Together" or "Keep Separate"

6.9.2.2. Apply the template

After filling in all the fields, select "Save". The NexLog Express will now attempt to download the available talk groups to the recorder.

6.9.2.3. Check for Alerts

Check the NexLog Express front panel and/or configuration manager for any system alerts or Inrado-specific alerts. There will be alerts specific to the Inrado integration if there are problems with downloading talk groups, managing crypto keys, and OTAR.

6.9.2.4. Verify Recording

Place a series of test calls between radios on both encrypted and unencrypted talk groups. Use MediaWorks EXP or the front panel display to verify the recording of all test calls.

6.10. MCPTT 3GPP/LTE RADIO RECORDING

License Required

This feature must be licensed to be used. Contact your Eventide Communications Dealer for assistance.

The MCPTT 3GPP/LTE Radio Recording template is used to record a 3gpp standard compliant Mission Critical Push To Talk (MCPTT) radio system such as Ericson or Samsung's MCPTT solutions.

6.10.1. Recorder Configuration

In order to configure this template you must first enter the Softil configuration details under System -> Configuration Files -> Softil MCPTT Configuration before applying this template. These files should be configured to match the specific parameters of the MCPTT system you are attempting to connect with.

To select the template, go to Recording -> Recording Interfaces, click "Add Virtual Recording Interface", and select the "MCPTT 3GPP/LTE RADIO RECORDING" template from the drop down menu and add the number of channels equal to the max simultaneous calls you want to record.

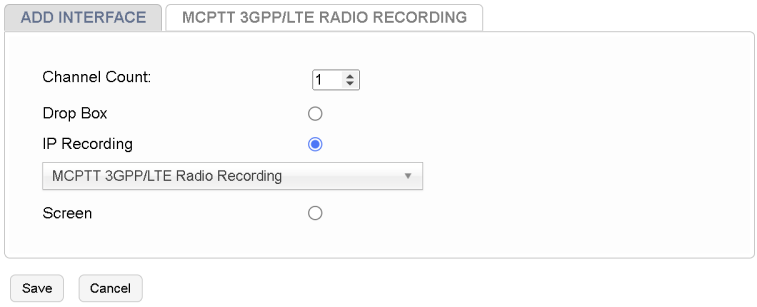


Fig. 6.60 MCPTT Template

On the following page, enter the supplied MCPTT password and Port information and select “Save”.

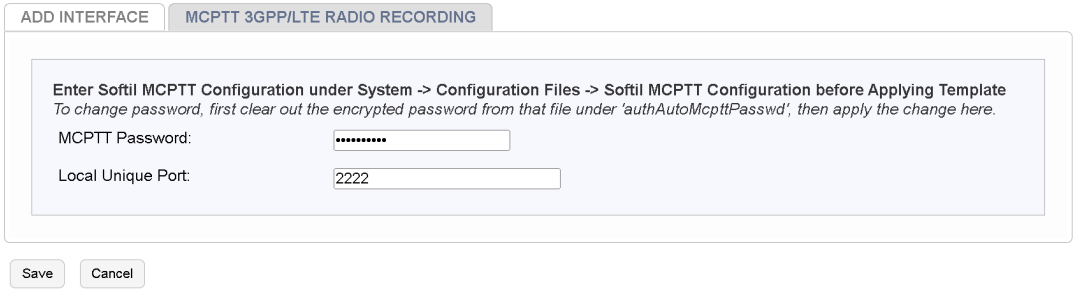


Fig. 6.61 MCPTT Template Details

6.10.1.1. Verifying Recording

You should now be able to make calls to confirm that recordings are taking place between your MCPTT radio solution and Eventide NexLog Express.

Recordings can be viewed by logging into the MediaWorks EXP playback interface.

6.11. Mitel Secure Recording Connector

6.11.1. Mitel Secure Recording Connector Introduction

The purpose of this document is to describe the steps to ensure successful integration between an Eventide NexLog Express system and Mitel 3300 IP PBX running MiVoice Business software, using Secure Recording Connector (SRC) for recording.

The SRC is a service of the Mitel Border Gateway, which facilitates the recording of Mitel Encrypted voice streams by third-party call recording equipment (CRE). The MBG server acts as a “broker” between the Mitel equipment and the CREs for adding and removing taps on the devices.

The Mitel 3300 and MBG must be appropriately licensed for the SRC service (this is done through Mitel). Configuring the Mitel 3300/MiVoice Business and MBG for recording via SRC is outside the scope of this document. More information can be found on their website:

https://www.mitel.com/support

Once the Mitel 3300 and MBG are configured appropriately, there will be corresponding information that needs to be entered into the “Mitel Secure Recording Connector” template in the NexLog Web Configuration Manager. Upon saving the correct data in the template a secure certificate will be issued to the MBG, which will then need to be accepted via the MBG menus.

6.11.1.1. Required Personnel

- Eventide dealer/reseller Technician
- LAN Administrator
- PBX Administrator

6.11.1.1.1. Mitel Secure Recording Connector(SRC) configuration detail

> **Note**
>
> Ensure that the NexLog is licensed appropriately for VOIP/RTP VoIP Channels. VoIP recording is licensed in groups of 8 channels, this example system has 16 channels. If proper licenses are not present contact Eventide technical support before proceeding.

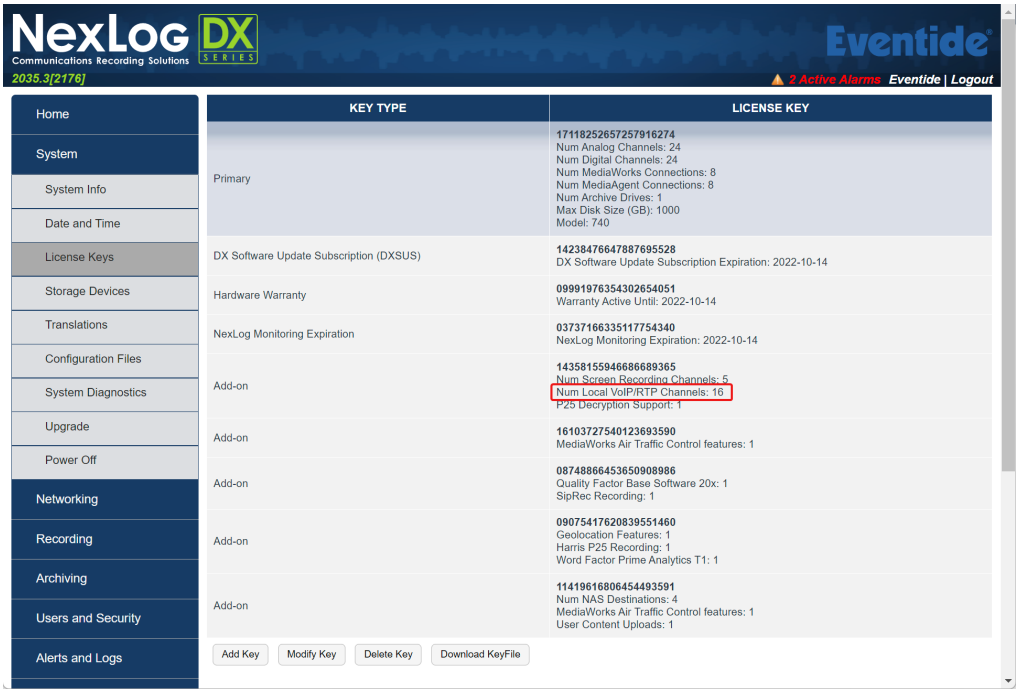


Fig. 6.62 Configuring VOIP Channels

6.11.1.2. Configure physical Network Interface Card

Connect a network cable from the corresponding Network Interface Card on the Eventide recorder to a switch port that will have access to the network that the MBG resides on.

In the Network Interfaces menu, select one of the currently unused Network Interface devices and Select “Type” Static. DHCP is supported, but not recommended because if the IP address changes, the new IP address will need to be entered into other configuration screens. Enter appropriate Netmask, Gateway, and Broadcast addresses for the network.

Save the template.

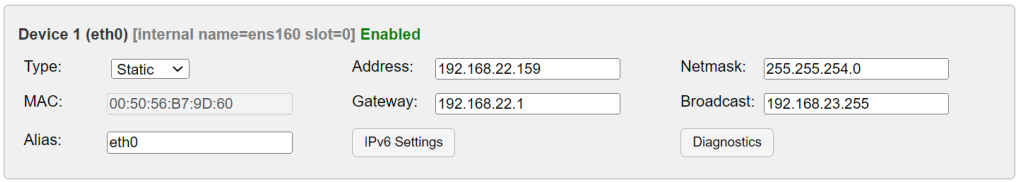


Fig. 6.63 Network Interface Configuration

6.11.1.3. Add Virtual Recording Interface

In the “Recording Interfaces” section, select “Add Virtual Recording Interface”, add Channel Count (the maximum number of simultaneous calls recorded, must be increments of eight), and select “Mitel Secure Recording Connector”

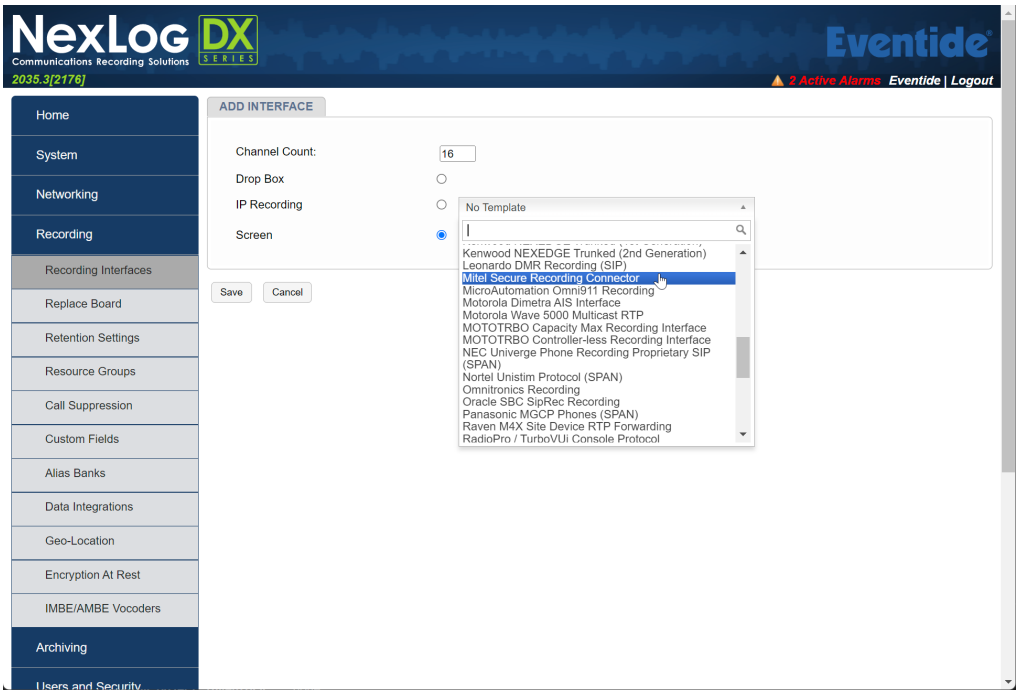


Fig. 6.64 VOIP Channel Configuration

6.11.1.4. Fill in the “Mitel Secure Recording Connector” Template Fields

Fill in the following information in the “Secure Recording Connector” section:

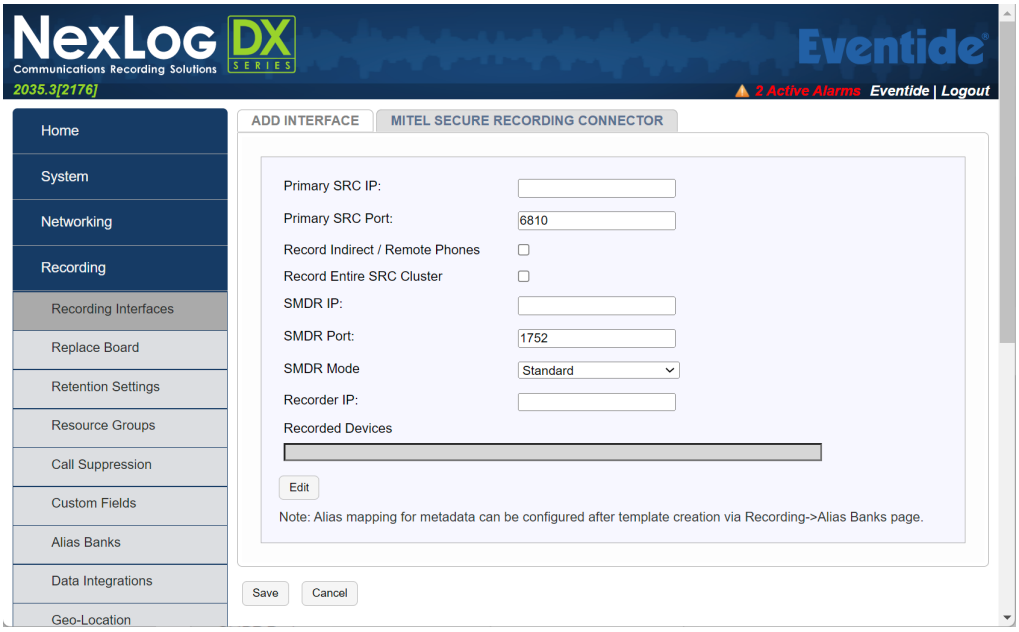


Fig. 6.65 Secure Recording Connector

Template Field Detail

Primary SRC IP: IP address of the primary Mitel Boarder Gateway (MBG) licensed for SRC. Note, there can be a master and slave MBG, this is the master.

- Typical Source: LAN or PBX Administrator

Primary SRC Port: Default is 6810 and should not be changed unless otherwise instructed to do so by the PBX administrator

- Typical Source: PBX Administrator

Record Remote Phones: When not selected only phones local to the SRC will be recorded, when selected remote phones will be recorded by sending audio directly to the recorder bypassing the SRC. Note, in the latter case some calls may not be recorded due to codec mismatches which the SRC would have resolved.

- Typical Source: LAN Administrator

Record Entire SRC Cluster: Multiple MBG nodes can be joined together and programmed to balance the connection load, and to provide redundancy and/or scalability, check if there are multiple MBG nodes with SRC. Recorder must have network access to all nodes in the cluster if this option is enabled

- Typical Source: PBX Administrator

SMDR IP: IP address of the Mitel 3300/MiVoice Business VM.

- Typical Source: PBX Administrator.

SMDR Port: Default is 1752 and should not be changed unless otherwise instructed to do so by the PBX administrator.

- Typical Source: PBX Administrator

SMDR Mode: Select the SMDR reporting mode being used on the Mitel 3300

- Typical Source: PBX Administrator

SMDR Action: SMDR can create standalone call event records, attach metadata to audio call records, or both. When attached, the SMDR doesn't always provide enough information on which call is active when multiple calls are in progress, so the recorder will note all possibilities in the metadata.

- Typical Source: PBX Administrator

Recorder IP: IP address of the physical network interface card on the recorder configured in section 4 b).

- Typical Source: LAN Administrator.

Recorded Devices: Enter the DN and descriptive name for each device to be recorded, then select "Add" to add additional DNs. Once complete, click "Populate" and information will be moved to the "Recorded Devices field, so it can be consumed by the recorder when the template is saved.

- Typical Source: PBX Administrator

6.11.1.5. Save the template

After filling in all the fields, click Save. The NexLog will configure itself to record and send an SRC certificate to the MBG. An alert will be raised in the recorder indicating that it is waiting for a certificate to be approved.

6.11.1.6. Accept the SRC Certificate on the MBG

On the MBG web interface, Browse to the Configuration tab, Click on ICPs, enable Indirect Call Recording for all ICPs On the MBG, navigate to the SRC Server webpage and accept the EVENTIDE Certificate The alert raised in the previous section should now be resolved on the recorder.

6.11.1.7. Verify Recording

Using MediaWorks EXP or the front panel display, place a series of test Calls to ensure your NexLog Express system is now properly recording.

6.12. MOTOTRBO Controller-less Recording Interface

6.12.1. MOTOTRBO Controller-less Recording Interface Introduction

The purpose of this document is to describe the steps to ensure successful integration between an Eventide NexLog740 or NexLog840 Logging recorder and MOTOTRBOTM Site Connect (IPSC), Capacity Plus (CPC) or Linked Capacity Plus (LCP) professional two-way radio system. The document assumes knowledge of the NexLog front panel interface and the browser-based configuration manager, it does not discuss recording interfaces beyond the MOTOTRBO integration. For more details on these interfaces, please refer to their respective manuals. This document also assumes knowledge of the Motorola Customer Programming Software (CPS) which is required to program the MOTOTRBO repeaters and site topology.

The NexLog will appear in the MOTOTRBO environment as a 3rd party application peer in any of the three radio system topologies. Therefore, the NexLog is required to have a unique Peer ID within the MOTOTRBO radio topology. The NexLog will also need to assume a set of appropriate parameters that are programmed into the MOTOTRBO Master Repeater. This is the overall purpose of the following Integration guide.

Required Personnel

- Eventide dealer/reseller Technician
- MOTOTRBO System Administrator/Technician

- Customer LAN Network Administrator

IP Network Connectivity The NexLog ideally will be assigned an IP address within the same LAN as the MOTOTRBO master repeater and peer repeaters. If the NexLog is separated from the LAN where the MOTOTRBO repeaters reside, it will most likely be separated by a firewall. If the latter is the case, consult the Customer LAN Network administrator to configure the firewall to allow all IP traffic to flow bi-directionally between the NexLog IP address and the MOTOTRBO repeater IP address.

License Required

This feature must be licensed to be used. Contact your Eventide Communications Dealer for assistance.

6.12.2. Add Virtual Recording Interface

Select the number of IP channels/number of talk paths

Select the “MOTOTRBO Recording Interface” Template

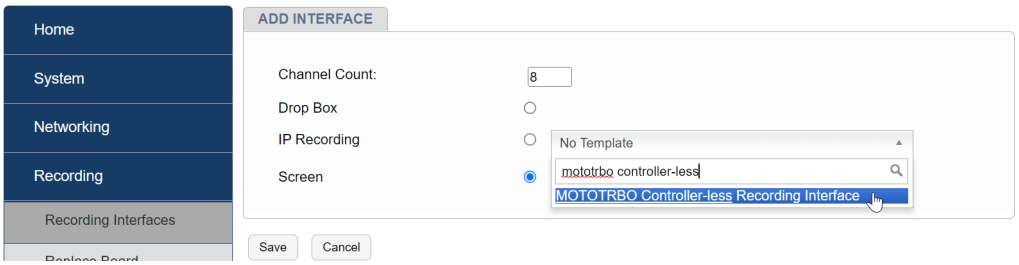


Fig. 6.66 Add Interface

Note

This is the maximum number of talk paths between the NexLog and the MOTOTRBO systems that can be recorded, and not to be confused with “Talk Groups”, multiple Talk Groups can be on one “Talk Path”.

6.12.2.1. Fill in MOTOTRBO Recording Interface Template Fields

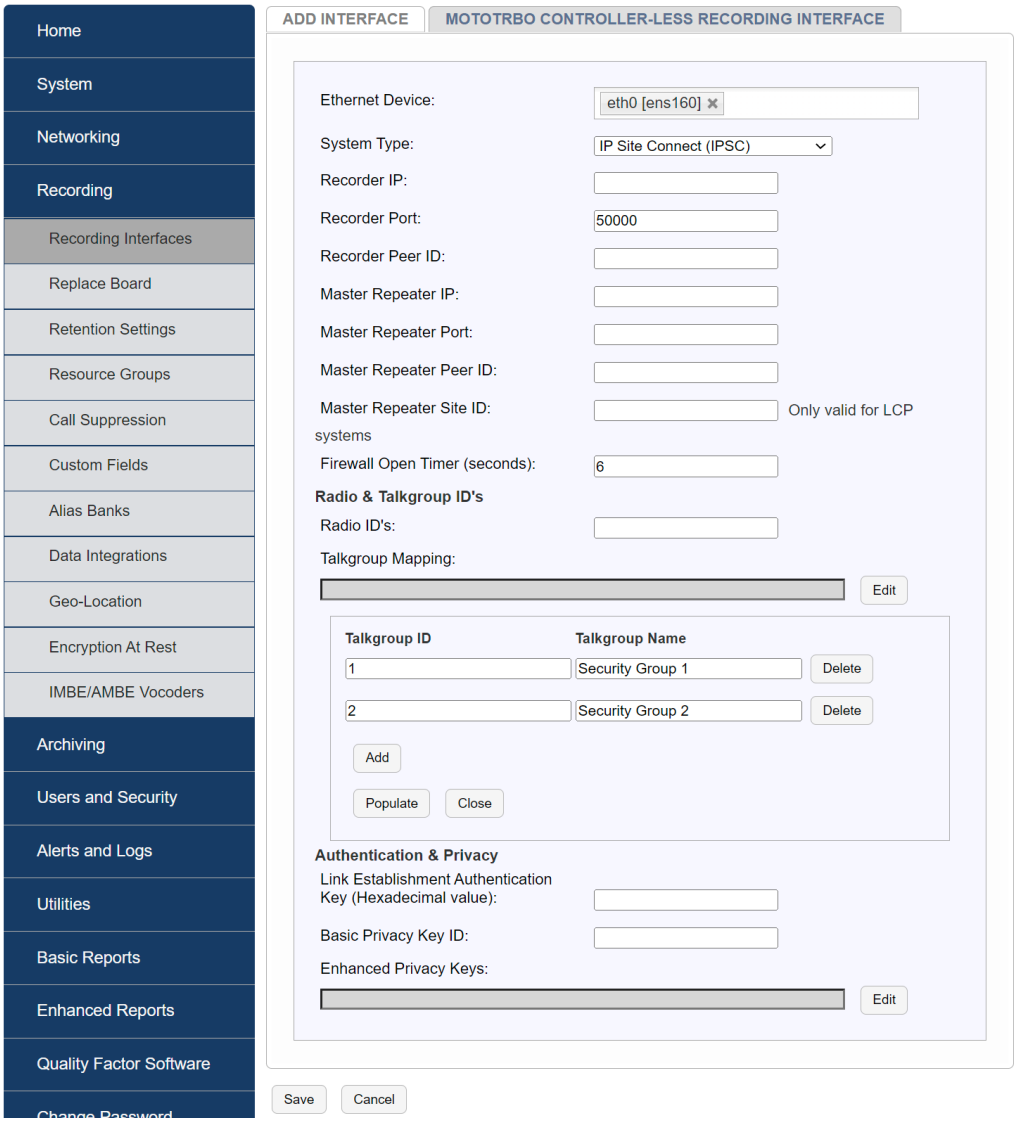


Fig. 6.67 Configure Interface

Select the MOTOTRBO “System Type”: There are three different types of MOTOTRBO systems supported by NexLog:

- Site Connect (IPSC)
- Capacity Plus (CPC)
- Linked Capacity Plus (LCP)

The data required for each system type is the same, except for Linked Capacity Plus (LCP), which requires one additional parameter, “Master Repeater Site ID”.

6.12.2.2. Network Administrator

Ethernet Device: Select the physical Ethernet/NIC of the NexLog recorder which is used to record MOTOTRBO radio transmissions and is physically connected to the same LAN as the MOTOTRBO Master Repeater

- Typical Source: Customer Network Administrator

Recorder IP: IP address of the NexLog Ethernet/NIC selected above

- Typical Source: Customer Network Administrator. Typical Source: Customer Network Administrator.

> **Note**
>
> The MOTOTRBO system employs a terminology where each repeater in the system is considered a “Peer” and each repeater has a unique Peer ID. The NexLog recorder appears to the MOTOTRBO system as 3rd party application peer

Select the MOTOTRBO “System Type”: There are three different types of MOTOTRBO systems supported by NexLog:

- Site Connect (IPSC)
- Capacity Plus (CPC)
- Linked Capacity Plus (LCP)

The data required for each system type is the same, except for Linked Capacity Plus (LCP), which requires one additional parameter, “Master Repeater Site ID”.

Recorder Port: UDP port that the NexLog recorder will use to record audio, default is 50000 and is typically not changed.

- Typical Source: Eventide dealer/reseller Technician.

Recorder Peer ID: Unique ID (Decimal Integer) designated for the NexLog recorder in the MOTOTRBO system. I.e. The NexLog is treated as 3rd party application peer.

- Typical Source: MOTOTRBO System Administrator/Technician.

Master Repeater IP: IP address of the MOTOTRBO Master Repeater.

- Typical Source: Customer Network Administrator.

Master Repeater Port: UDP port used by the MOTOTRBO Master Repeater.

- Typical Source: MOTOTRBO System Administrator/Technician.

vMaster Repeater Peer ID:** Unique ID (Decimal Integer) of the MOTOTRBO Master Repeater in the environment.

- Typical Source: MOTOTRBO System Administrator/Technician.

Master Repeater Site ID (applicable only to Linked Capacity Plus (LCP) environments): Unique ID (Decimal Integer) of the location/site where the MOTOTRBO Master Repeater is located.

- Typical Source: MOTOTRBO System Administrator/Technician.

Firewall Open Timer (seconds): Amount of seconds between 'keep alive' messages the recorder will send to retain membership in the MOTOTRBO peer group. Default is 6 seconds and not usually changed.

- Typical Source: MOTOTRBO System Administrator/Technician.

Radio IDs: Comma separated list of radio IDs that will be recorded when making Radio to Radio (private) calls. Enter a value of zero "0" for all radio IDs. Range of IDs can also be entered (e.g. 5-10,100-150)

- Typical Source: MOTOTRBO System Administrator/Technician.

Talk Group Mapping: Select "Edit" to create a relationship listed of mapping between the MOTOTRBO Talkgroup IDs and a more meaningful Talkgroup name that will be used by the NexLog for displaying the recorded channels. Multiple mappings can be created by clicking "Add". Click "Populate" to fill in and complete the Talkgroup Mapping.

- Typical Source: MOTOTRBO System Administrator/Technician.

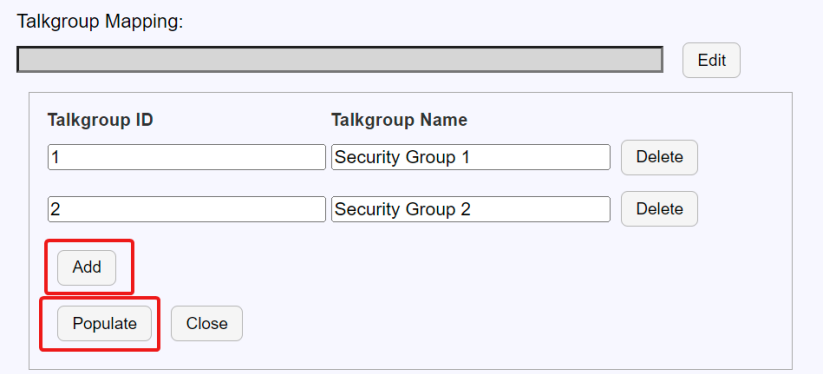


Fig. 6.68 Talk Group Mapping

Link Establishment Authentication Key: Hexadecimal value used to authorize link establishment, it is the same value on all repeaters and the NexLog. This is an optional security feature used in some MOTOTRBO environments. If this feature is not used, the field can be left blank.

- Typical Source: MOTOTRBO System Administrator/Technician.

Basic Privacy Key ID: Integer value 1-255, used to identify privacy key, it is the same value on all repeaters and the NexLog.

- Typical Source: MOTOTRBO System Administrator/Technician.

Enhanced Privacy Keys: Click “Edit” to create a relationship between Enhanced Privacy Key IDs and Key Values, multiple relationships can be added by clicking “Add”. Click “Populate” to fill in and complete the Key ID and Key-Value pairs.

- Typical Source: MOTOTRBO System Administrator/Technician.

Save the template

After filling in all the fields, click Save. The NexLog will now attempt to contact the Master Repeater and establish itself as a 3rd party application peer in the MOTOTRBO environment.

6.12.2.3. Configure internal or external DVSIs

License Required

DVSI will require a “Num Internal Vocoder Resources” add-on license key. Contact your Eventide Communications Dealer for assistance.

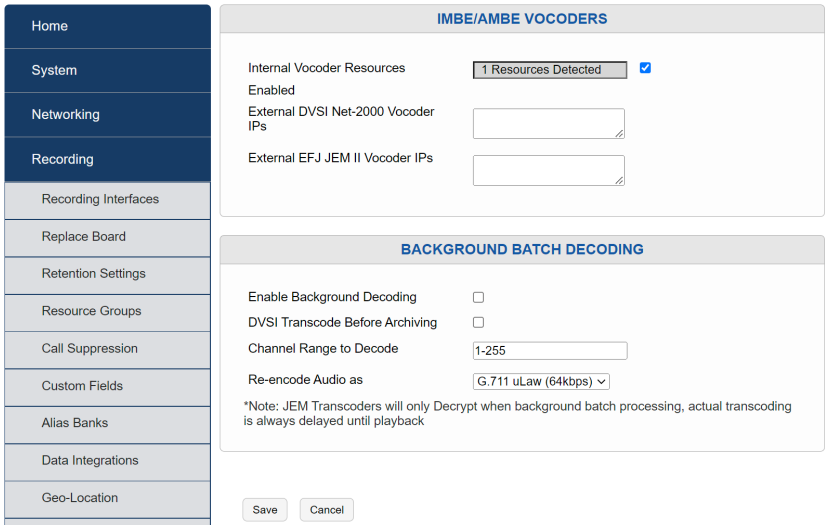


Fig. 6.69 IMBE/AMBE Vocoder Configuration

MBE Transcoder IP: This is the IP address of the DVSI brand decoder that is used to decode AMBE audio during playback.

Choose the appropriate next step based on the physical configuration of the DVSI vocoder. If the DVSI transcoder function is internal to the recorder, follow the “Configure Internal DVSI IMBE/AMBE Transcoder” step. If the DVSI is an external 2U device, follow the “Configure Multiple external IMBE/AMBE Transcoder IPs” step.

6.12.2.3.1. Configure Internal DVSI IMBE/AMBE Transcoder

If the DVSI IMBE/AMBE Transcoder is internal, the system will recognize the Vocoder. To use, select “Enable”

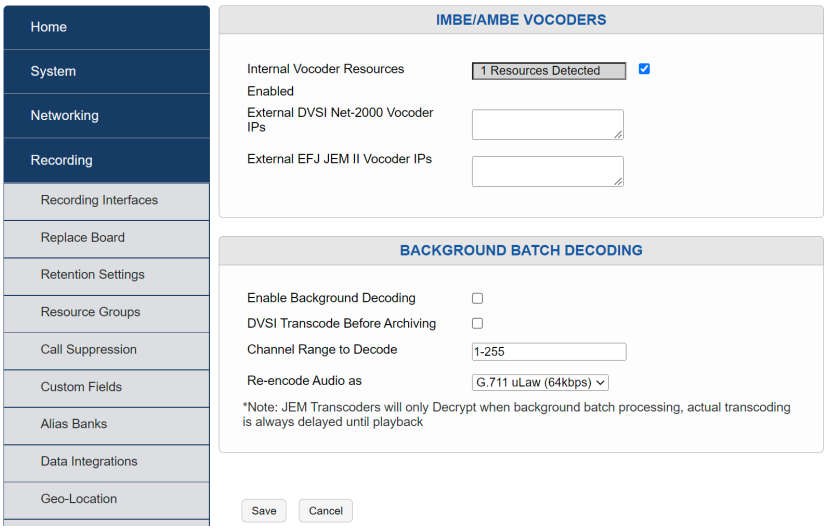


Fig. 6.70 IMBE/AMBE Vocoder Configuration

Note

There may be more than one in the environment to allow for higher amounts of simultaneous IMBE/AMBE transcoding for playback. If so, enter one of the IP addresses in this field, the remaining transcoders will be configured in the subsequent step.

6.12.2.4. Check for Alerts

Check the NexLog front panel and/or configuration manager for any system alerts or MOTOTRBO-specific alerts. There will be alerts specific to the MOTOTRBO integration if there are problems saving the template data.

6.12.2.5. Verify Recording

Place a series of test calls between radios on both encrypted and unencrypted talk groups. Use MediaWorks EXP or the front panel display to verify successful recording of all test calls.

6.13. MOTOTRBO Capacity Max Recording Interface

6.13.1. MOTOTRBO Capacity Max Recording Interface Introduction

The purpose of this document is to describe the steps to ensure a successful integration between an Eventide NexLog740 or NexLog840 Logging recorder and MOTOTRBO CAPACITY MAX DMR two-way radio system. The document assumes knowledge of the NexLog browser-based configuration manager, it does not discuss recording interfaces beyond the CAPACITY MAX integration. For more details on these interfaces, please refer to their respective manuals. This document also assumes knowledge of CAPACITY MAX configuration and setup.

The NexLog will interface to the CAPACITY MAX system through the Voice and Radio Command (VRC) Gateway, referred to in this document as the VRC Gateway. Each VRC gateway can support up to 100 active talkpaths. Each CAPACITY MAX system supports up to 5 pairs of primary and backup VRC Gateways. The NexLog can support multiple pairs of redundant VRC Gateways by creating a separate recording template for each pair of redundant VRC Gateways. Creating the recording templates is discussed further in this document.

The VRC Gateway audio recording interface supports the delivery of the following types of calls to the NexLog recorder

- Calls between Radios
- Calls between Radios and Dispatch
- Telephony Calls
- Broadcast, Site/Multisite All Call
- Emergency Voice Calls
- Individual / Group Calls
- Encrypted/ Clear Calls

Calls are recorded in AMBE+2 codec format, therefore, DVSI resources are required for playback. MediaWorks EXP is used to search and replay calls. It will also indicate the types of calls, as well as Privacy level which is indicated by “CLEAR” or “ENHANCED”

6.13.2. NexLog Capacity Max Configuration Detail

Add Virtual Recording Interface

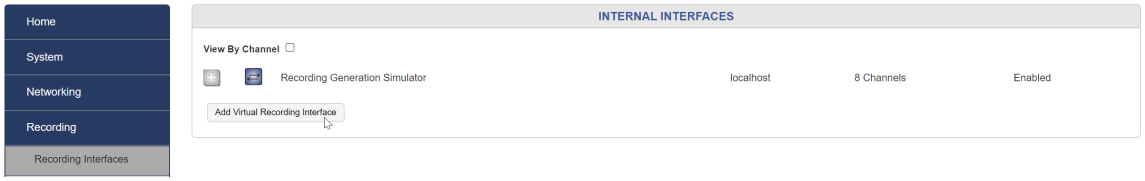


Fig. 6.71 Add Interface

Select the number of IP channels/number of talk paths and choose the “MOTOTRBO CAPACITY MAX Recording Interface” Template in the dropdown “Local IP” template section.

> **Note**
>
> This is the maximum number of talk paths between the NexLog and the CAPACITY MAX that can be recorded, and not to be confused with “Talk Groups”, multiple Talk Groups can be on one “Talk Path”.

6.13.2.1. Template Field Details

The following figure has the fields populated for illustrative purposes, the actual values in each installation will most likely be different. Verify each value with the CAPACITY MAX System Administrator/Technician or the Customer Network Administrator.

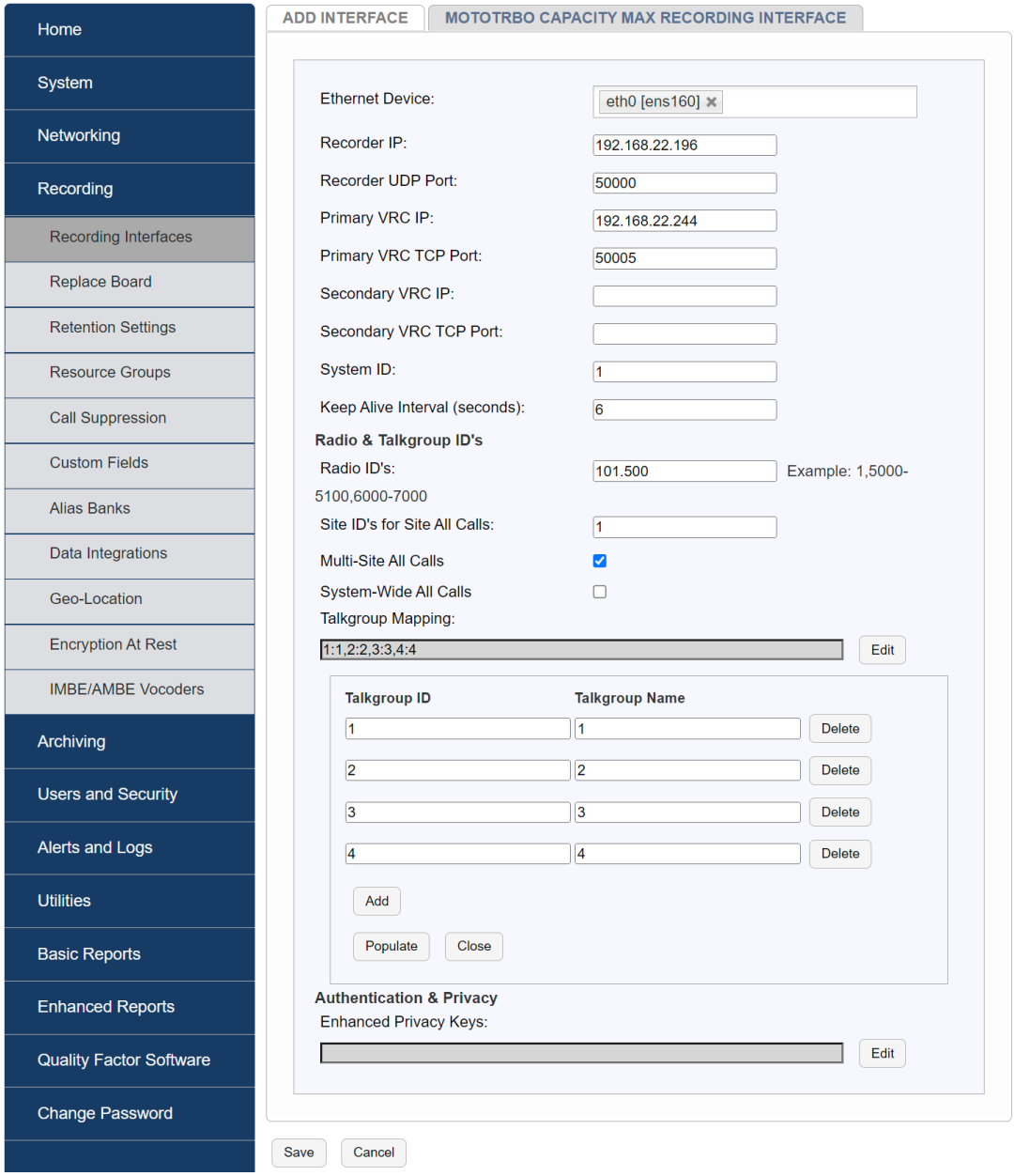


Fig. 6.72 Template Configuration

Ethernet Device: Select the physical Ethernet/NIC of the NexLog recorder which is used to record CAPACITY MAX radio transmissions and is physically connected to the same LAN as the CAPACITY MAX VRC Gateway

- Typical Source: Customer Network Administrator

Recorder IP: IP address of the NexLog Ethernet/NIC selected above.

- Typical Source: Customer Network Administrator

Recorder Port: UDP port that the NexLog recorder will use to record audio, default is 50000 and is typically not changed

- Typical Source: Eventide dealer/reseller Technician

Primary VRC IP: IP address of the CAPACITY MAX VRC Gateway

- Typical Source: CAPACITY MAX System Administrator/Technician

Primary VRC TCP Port: TCP port used by the VRC Gateway to send calls and data to the recorder

- Typical Source: CAPACITY MAX System Administrator/Technician

Secondary VRC IP: IP address of the CAPACITY MAX VRC Gateway. Can be left blank if there is not a redundant VRC Gateway

- Typical Source: CAPACITY MAX System Administrator/Technician

Secondary VRC TCP Port: TCP port used by the VRC Gateway to send calls and data to the recorder. Can be left blank if there is not a redundant VRC Gateway

- Typical Source: CAPACITY MAX System Administrator/Technician

System ID: Unique ID (Decimal Integer) of the CAPACITY MAX VRC Gateway

- Typical Source: CAPACITY MAX System Administrator/Technician

Keep Alive Interval (seconds): Amount of seconds between 'keep alive' messages the recorder will send to retain connection or determine failover to the Secondary VRC Gateway. Default is 6 seconds and not usually changed.

- Typical Source: CAPACITY MAX System Administrator/Technician

Radio IDs: Comma separated list of radio IDs that will be recorded when making Radio to Radio (private) calls. Enter a value of zero "0" for all radio IDs, or a range of IDs can also be entered (e.g. 5-10,100-150)

- Typical Source: CAPACITY MAX System Administrator/Technician

Talk Group Mapping: Click "Edit" to create a relationship listed of mapping between the CAPACITY MAX Talkgroup IDs and a more meaningful Talkgroup name that will be used by the NexLog for displaying the

recorded channels. Multiple mappings can be created by clicking “Add”. Click “Populate” to fill in and complete the Talkgroup Mapping

- Typical Source: CAPACITY MAX System Administrator/Technician

6.13.2.2. Authentication and Privacy

Enhanced Privacy Keys: Click “Edit” to create a relationship between Enhanced Privacy Key IDs and Key Values, multiple relationships can be added by clicking “Add”. Click “Populate” to fill in and complete the Key ID and Key-Value pairs.

- Typical Source: CAPACITY MAX System Administrator/Technician

After filling in all the fields, click Save. The NexLog will now be ready to receive calls and data from the CAPACITY MAX VRC Gateway.

6.13.2.3. Configure internal or external DVSIs

License Required

DVSI will require a “Num Internal Vocoder Resources” add-on license key. Contact your Eventide Communications Dealer for assistance.

CAPACITY MAX call recordings are saved to disk using a low bit rate codec, AMBE+2. To enable playback of these recordings there must be an AMBE/IMBE vocoder resources available to MediaWorks EXP. Completing this page will enable access to these resources.

Go to the IMBE/AMBE Vocoders page shown below and enter the fields according to the instructions below the diagram

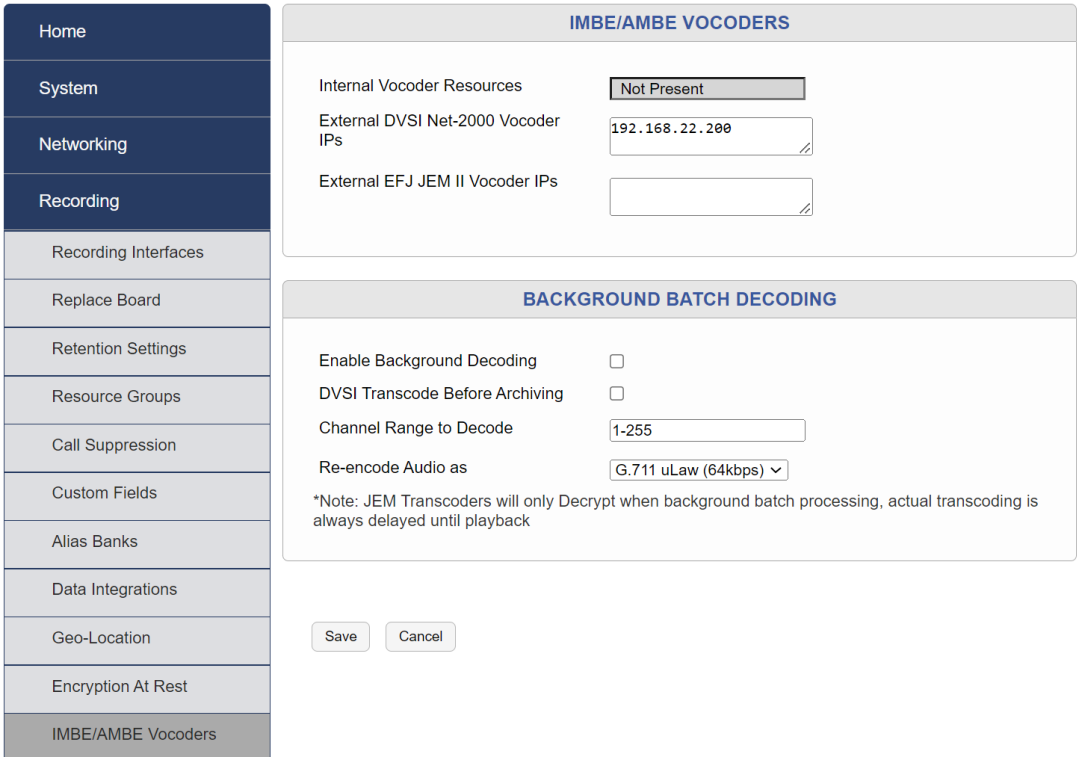


Fig. 6.73 IMBE/AMBE Vocoder Settings

Internal Vocoder Resources: If there are internal vocoders, they should be auto-detected. If not, there should be a check box available to detect them. Once completed skip to the “BACKGROUND BATCH DECODING” Section.

External EFJ JEM II Vocoder IPs: Not Applicable for Capacity Max recording (EF Johnson P25 Recoding only) Leave Blank.

6.13.2.4. Background Batch Decoding

Enable Backgroud Decoding: This is an optional setting that allows AMBE+2 encoded calls to be decoded while the DVSI vocoder resources are not being used. If this is unchecked, the vocoding will occur when a call is selected for replay from MediaWorks EXP.

Channel Range to Decode: Range of channels in the system to apply the background decoding.

Re-encode Audio as: Select the encoding algorithm that you would like the AMBE+2 recordings to be re-encoded as.

6.13.2.5. Check for Alerts

Check the NexLog front panel and/or configuration manager (figure below) for any system alerts or CAPACITY MAX-specific alerts. There will be alerts specific to the CAPACITY MAX integration if there are problems saving the template data.

6.13.2.6. Verify Recording

Place a series of test calls between radios on both encrypted and unencrypted talk groups. Use MediaWorks EXP or the front panel display to verify the recording of all test calls.

6.14. Omnitronics Recording

6.14.1. Omnitronics Recording Introduction

This application note discusses how to configure the NexLog Express to record VoIP audio from Omnitronics VoIP products. The NexLog Express is a VoIP recorder that is capable of recording and play-back of audio sent to/from Omnitronics VoIP products such as IPR100, IPR110+, IPR400, DRG100, DRG200i1, omnicore Console, RediTALK-Flex, altusomni IPE (REC mode), DX-Altus IPE (REC mode), and TetraGateway-DM.

> **Note**
>
> DRG200i is only available on special request; please contact your Omnitronics representative for information.

6.14.1.1. Methods of Recording Audio

There are a couple of ways in which audio from Omnitronics VoIP devices can be sent to the recorder as follows:

- Port mirroring - The local network duplicates network traffic going to/from one Ethernet port (Omnitronics device) to another port (Eventide Nexlog recorder). The advantage of this method is that no configuration changes are needed in the Omnitronics device(s), as audio is duplicated as-is to the recorder. However, since this method requires special configuration of the Ethernet switch, and since there are numerous Ethernet switch manufacturers and methods to achieve this with some requiring a high level of expertise, this application note will not cover port mirroring. You are welcome to configure your network and recorder this way when conferencing is not an option.
- VoIP conferencing/forwarding - The Omnitronics device is configured to conference/forward all audio to the Eventide Nexlog recorder IP address and port number. This is the method that is described in this application note.

6.14.2. Recorder Configuration

To configure the NexLog Express, you use its web-based configuration interface. You can access the interface by browsing the recorder's IP address using a web browser.

If you intend to configure an NexLog Express that is brand new from the factory, its typical default IP address is 192.168.1.101, however, it may be different from this—consult your Eventide documentation for further information if you are unsure. Usually, only one of the Ethernet ports is enabled (the others are usually disabled) by default, so you will need to connect at least one Ethernet cable to the first port to begin. Virtualized NexLog Express recorders have their IP address specified during installation.

6.14.2.1. Logging in to the Recorder

You must ensure that the computer is on the same network subnet as the NexLog DX Recorder otherwise, you cannot connect to the configuration manager.

To login to the NexLog DX Recorder configuration manager:

- Type the IP address of the Eventide NexLog DX Recorder into your web browser.
- Once you have connected to the recorder, you should see the NexLog DX Series opening page for MediaWorks.

Fig. 6.74 Template Field Details

Use MediaWorks to play back or export recorded audio—please refer to the NexLog Express for detailed configuration and playback instructions not covered by this application note.

- On the opening page, select the settings icon (in the lower right) to show the LOGIN page for the configuration interface.
- At the LOGIN page, type your username and password and then select Login

the default username is “Eventide” and the password is the serial number of your recorder

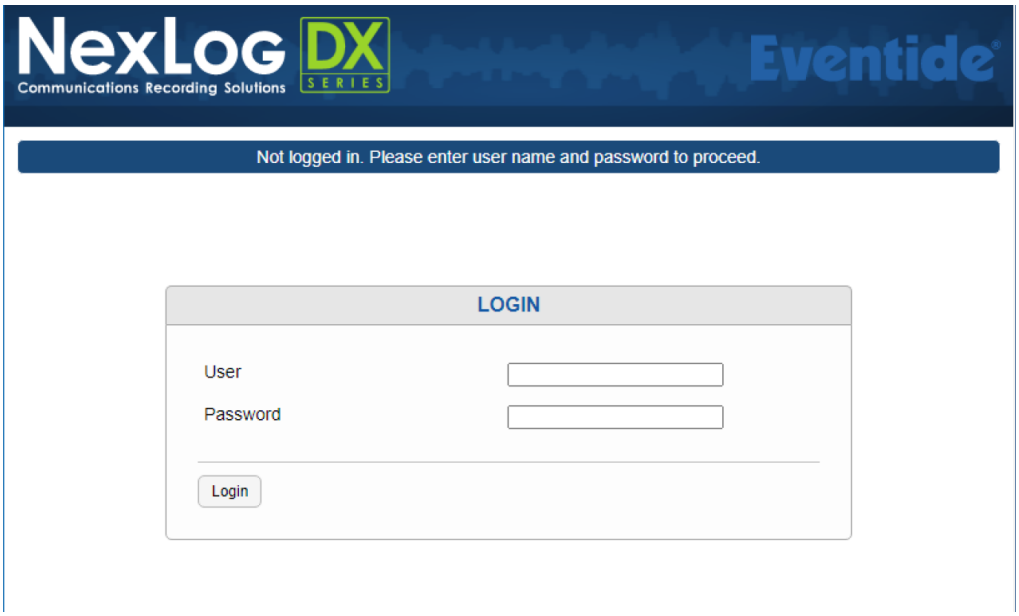


Fig. 6.75 Template Field Details

Once you have logged in, the Home page appears showing details about your recorder.

Fig. 6.76 Template Field Details

6.14.2.2. Recorder Configuration Methods

This section applies to setting up the NexLog Express Recorders to record audio to and from the following Omnitronics products: IPR100, IPR110+, IPR400, DRG100 (all variants), DRG200i (all variants), altusomni IPE (REC mode), DX-Altus IPE (REC mode), and TetraGateway-DM.

6.14.2.3. Configuring the NexLog DX Recorder

Use this method to configure the Eventide NexLog DX Recorder. Once you have enabled metadata recording in the DRG, you can commence configuration of the NexLog Express recorder using the procedure below

To configure the Eventide NexLog DX Recorder

- Login to the Configuration Manager
- On the menu, select Recording, and then select Recording Interfaces

This displays the analog recording interfaces installed (if any) as well as virtual recording interfaces, which must be created and configured to record audio from Omnitronics devices.

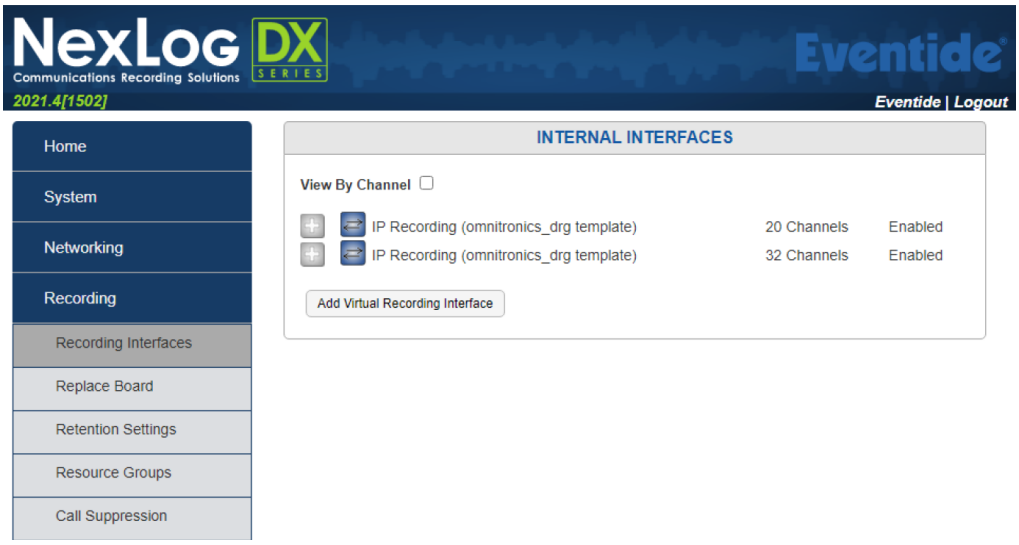


Fig. 6.77 Template Field Details

- Select Add Virtual Recording Interface to show the ADD INTERFACE page

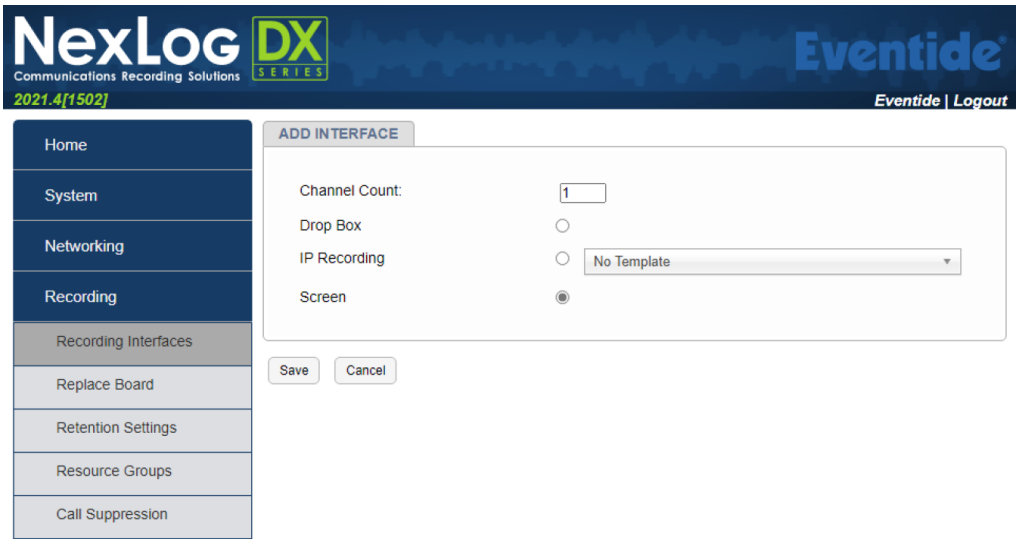


Fig. 6.78 Template Field Details

- On the ADD INTERFACE tab, configure the following settings:
- Set Channel Count to the total number of VoIP channels you want to record from Omnitronics devices.

For example, a system comprising 2 x IPR100 (2), 3 x IPR110+ (3), 2 x DRG100 (2), 2 x DRG200i (4), 2 x IPR400 (8), and 1 x IPE (8) (altusomni or DX-Altus), the total number of VoIP channels is 27 (2+3+2+4+8+8 = 27).

Omnitronics Device	Channel Count
IPR100, IPR110+, DRG100	1
DRG200i	2
IPR400	4
altusomni or DX-Altus IPE (in REC mode)	8
TetraGateway-DM	32

- Select IP Recording for the interface mode, and then select Omnitronics Recording from the dropdown list.

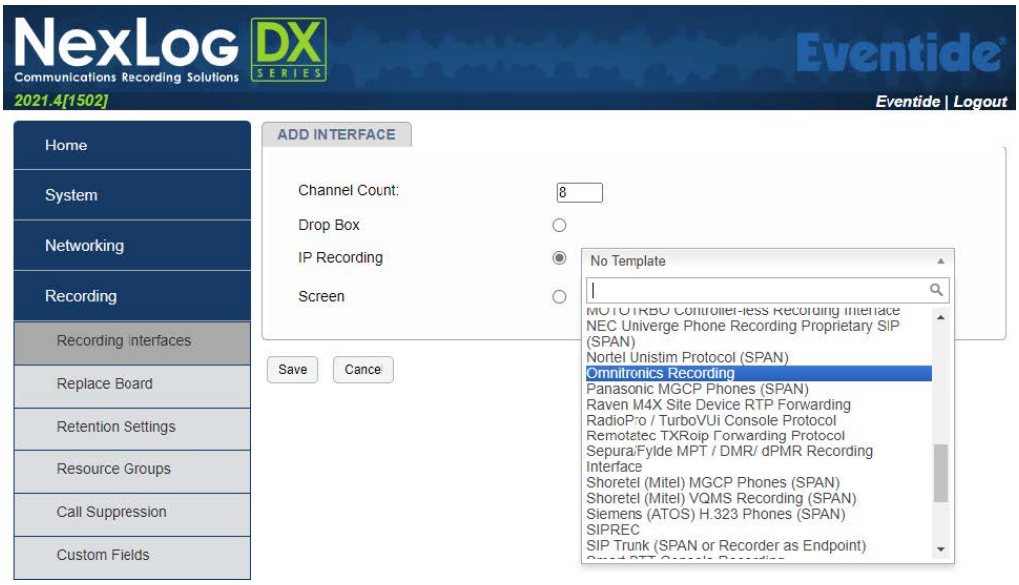


Fig. 6.79 Template Field Details

- On the OMNITRONICS RECORDING tab, for the Ethernet Device, select the Eventide Nexlog DX Recorder associated with the same network as the Omnitronics gateway device.

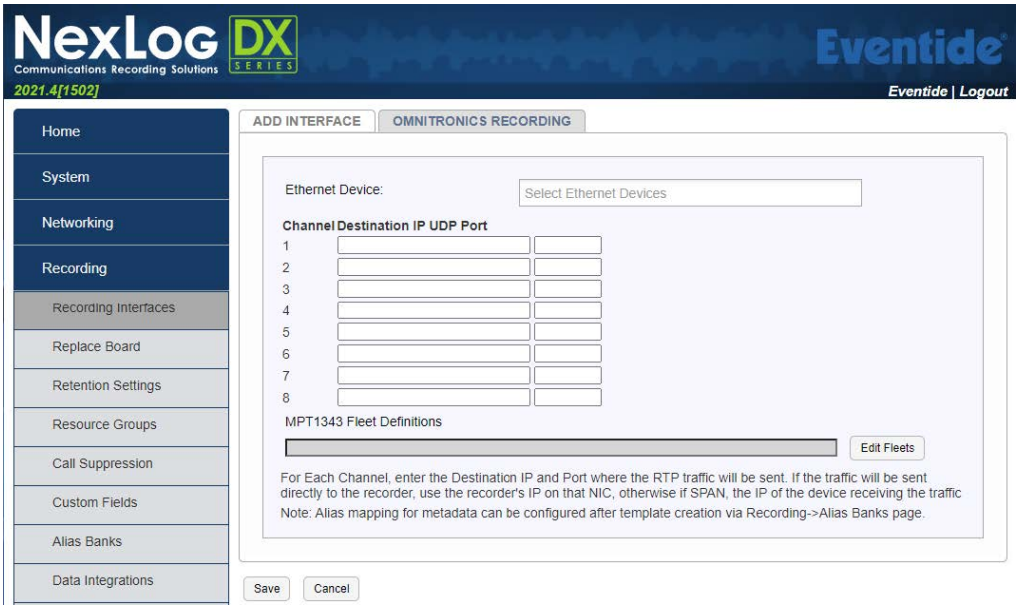


Fig. 6.80 Template Field Details

- Under Channel Destination IP UDP Port for each channel, type the IP address of the Eventide Nexlog DX Recorder in the first textbox, and then type the port number on which the recorder will

listen to the Omnitronics gateway device in the second textbox. If you are recording a device sending audio to a multicast IP address, enter the multicast IP address and port instead.

Note

Since the Omnitronics IPR/DRG gateway recording interface is tied to a network interface that has a particular IP address (e.g., eth0), the same IP address should be entered for all the channels here (except for multicast recording). If you need to record Omnitronics devices located across multiple ethernet interfaces/subnets of the Eventide system, you will need to create separate Omnitronics Recording interfaces that will be tied to those interfaces and IP addresses.

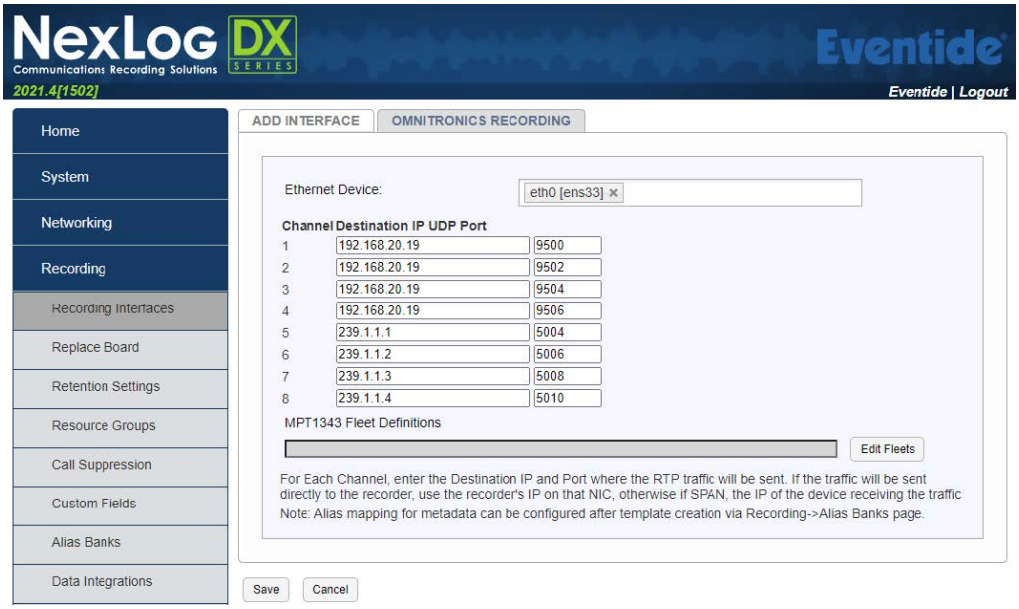


Fig. 6.81 Template Field Details

> **Note**
>
> You must specify the port on which the Omnitronics gateway device will send audio. The port number must satisfy the following: - Must not be a well-known port number (0 to 1024). - Must be an even number - Must be a unique port number for each device configuration and for the Eventide Nexlog recorder (do not use the same port number for recording different devices or ports and do not set it to the same port number used elsewhere in the VoIP/RTP or SIP or digital radio configuration for the device)

(Optional) If you need to record a Tait DMR-AIS system that uses MPT1343 Fleet definitions, select Edit Fleets to define fleet definitions for this recording interface, and configure your fleet definitions as follows:

- Enter the fleet prefix in the Prefix textbox, the Fleet Individual Number (FIN) in the FIN textbox, the Fleet Group Number (FGN) in the FGN textbox, the Number of Units in the Num Units textbox, the Number of Groups in the Num Groups text box, and the Digits in the Digits textbox (all fields are mandatory)
- If you have more than one fleet definition, select Add to add additional fleets to the list
- Select Populate to add your MPT1343 fleet(s) to the recording board interface (the fleets will be populated in the MPT1343 Fleet Definitions text box)
- If you need to remove any fleets from the populated list, select Delete next to the fleet definition, and then select Populate once more

Fig. 6.82 Template Field Details

> **Note**
>
> The fleet definition will apply to all recording IP addresses listed in the recording board. Ensure only DRGs interfaced to Tait DMR-AIS systems with MPT1343 fleets applied are included in the recording board.

- Select Save to add the virtual interface to the recorder

This will take you back to the Boards page and the new interface will be available in the list.

- Select the “+” next to the new interface to view the interface information.

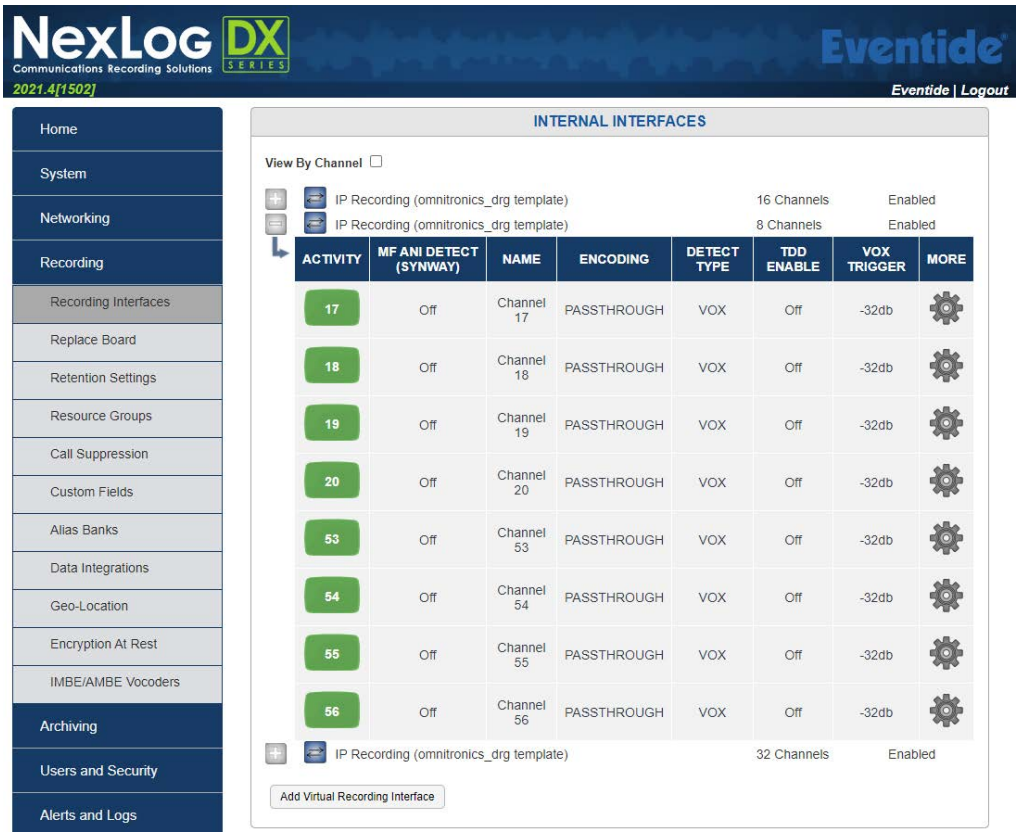


Fig. 6.83 Template Field Details

Optional: To change the name for a channel, select the current name of the channel, and then type a new name in the textbox (e.g., “Example Site”).

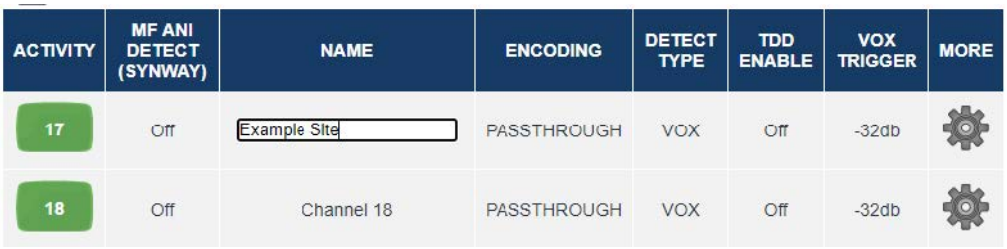


Fig. 6.84 Template Field Details

- Press Enter (or select on a blank space away from the name textbox) to save the configuration.

Configuration is now complete for the Eventide Nexlog recorder. The ACTIVITY column shows the recording status for a particular channel (green: idle; red: recording).

Optional: Configure Digital Radio Alias Banks

This optional step can only be performed on Nexlog DX-Series recorders. If you are recording digital radio metadata from a supported Omnitronics DRG, the Nexlog DX will record source and destination caller (radio) IDs as raw numbers, t]alk-group numbers as “GROUP_nnn” (e.g., GROUP_101), and all calls as “ALL_CALL”.

The following example screenshot from MediaWorks shows these default naming schemes for individual, group, and all calls. Note that the “Caller Id” column is the source radio ID, and the “Dtmf” column is the destination radio ID or group.

Source Name	Channel Name	Start Time	Duration	Caller Id	Connection ID	Dtmf	Calltype
OmniNexLog	DRG100 P25 122 7004	2021-12-15 13:52:20 +08:00	00:03	6	240100151	1000	
OmniNexLog	DRG100 P25 122 7004	2021-12-15 13:52:14 +08:00	00:05	1000	240100151	6	
OmniNexLog	GROUP_101	2021-12-15 13:51:53 +08:00	00:05	1000	240100151	GROUP_101	
OmniNexLog	GROUP_101	2021-12-15 13:51:30 +08:00	00:05	6	240100151	GROUP_101	
OmniNexLog	ALL_CALL	2021-12-15 13:51:08 +08:00	00:07	6	240100151	ALL_CALL	
OmniNexLog	ALL_CALL	2021-12-15 13:50:21 +08:00	00:04	1000	240100151	ALL_CALL	

Fig. 6.85 Template Field Details

If you wish to customize the default naming scheme so that the Nexlog recorder displays names instead of numbers, the Alias Banks feature may be used. Separate Alias Banks for Radio IDs and Talk Group/All Call numbers must be made.

6.14.2.3.1. Configure an Alias Bank for Radio IDs

To show names for your radio IDs instead of numbers, you can configure an alias bank for radio IDs. To configure an alias bank

- Login to the Configuration Manager (see “Log in to NexLog DX Recorder” on page 3)
- On the menu, select Recording, select Alias Banks, then Add Alias Bank

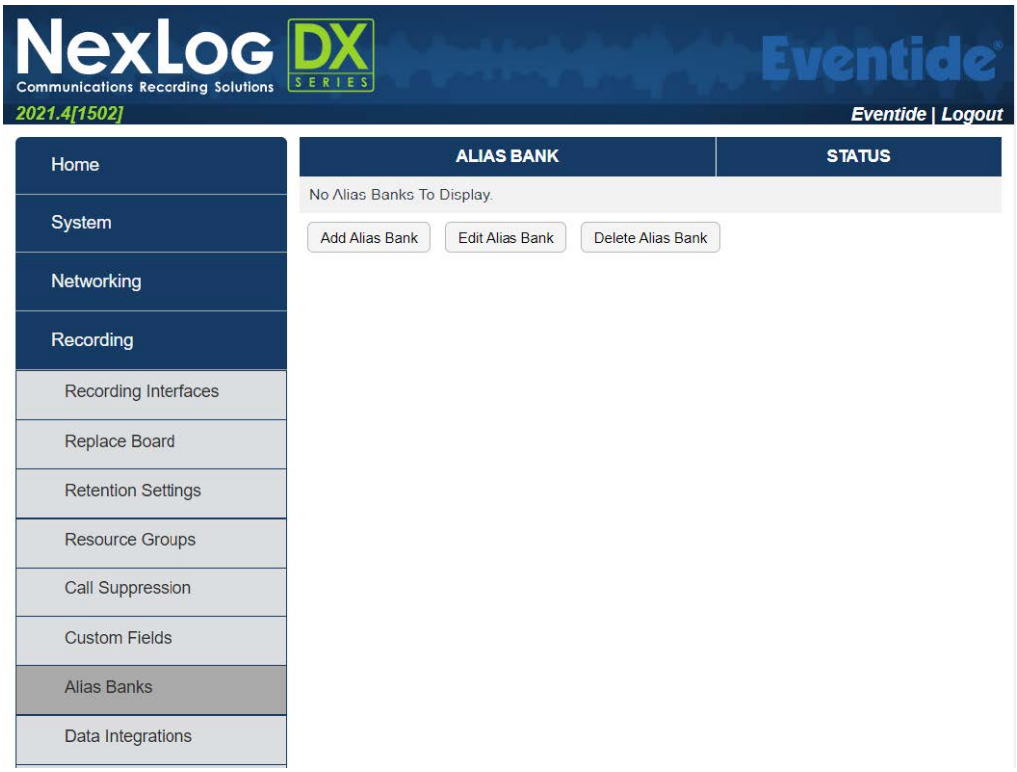
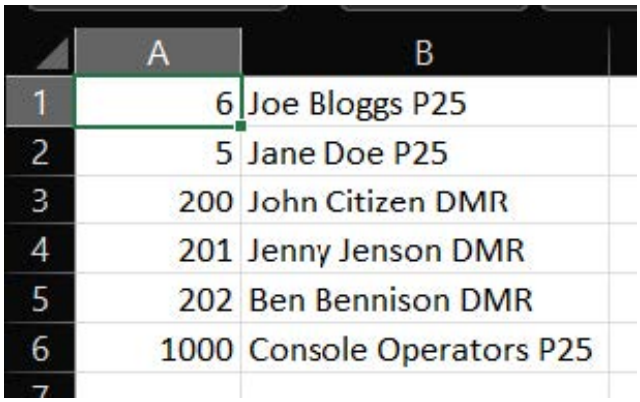


Fig. 6.86 Template Field Details

- On the Alias Bank screen: 3.1 Set the Alias Bank Name e.g., “Radio IDs to names”.
    - Leave the Output Formatter as {{ALIAS}}.
    - Set both Alias From and Alias To as “CALLER_ID”.
    - Leave Only Apply Aliases If unchecked.
    - In Applied Channels, check the box next to each IP Recording (Omnitronics template) board that is receiving the digital radio IDs. If you are unsure, select all of them.
    - In the Alias Rules section, set the raw radio ID numbers in the Source column, and their desired name in the Alias column.
    - Alternatively, you may import a .csv list of radio IDs and names using the Import Rules Button. Ensure the first column contains only radio IDs, and the second column contains only the names (do not include table headers). The following example is a .csv file edited with Microsoft Excel in this format: Graphical user interface, text, application, chat, or text message



	A	B
1	6	Joe Bloggs P25
2	5	Jane Doe P25
3	200	John Citizen DMR
4	201	Jenny Jenson DMR
5	202	Ben Bennison DMR
6	1000	Console Operators P25

Fig. 6.87 Template Field Details

Description automatically generated

- Once you have entered (or imported) all the IDs and their desired names, select Submit to save the changes.

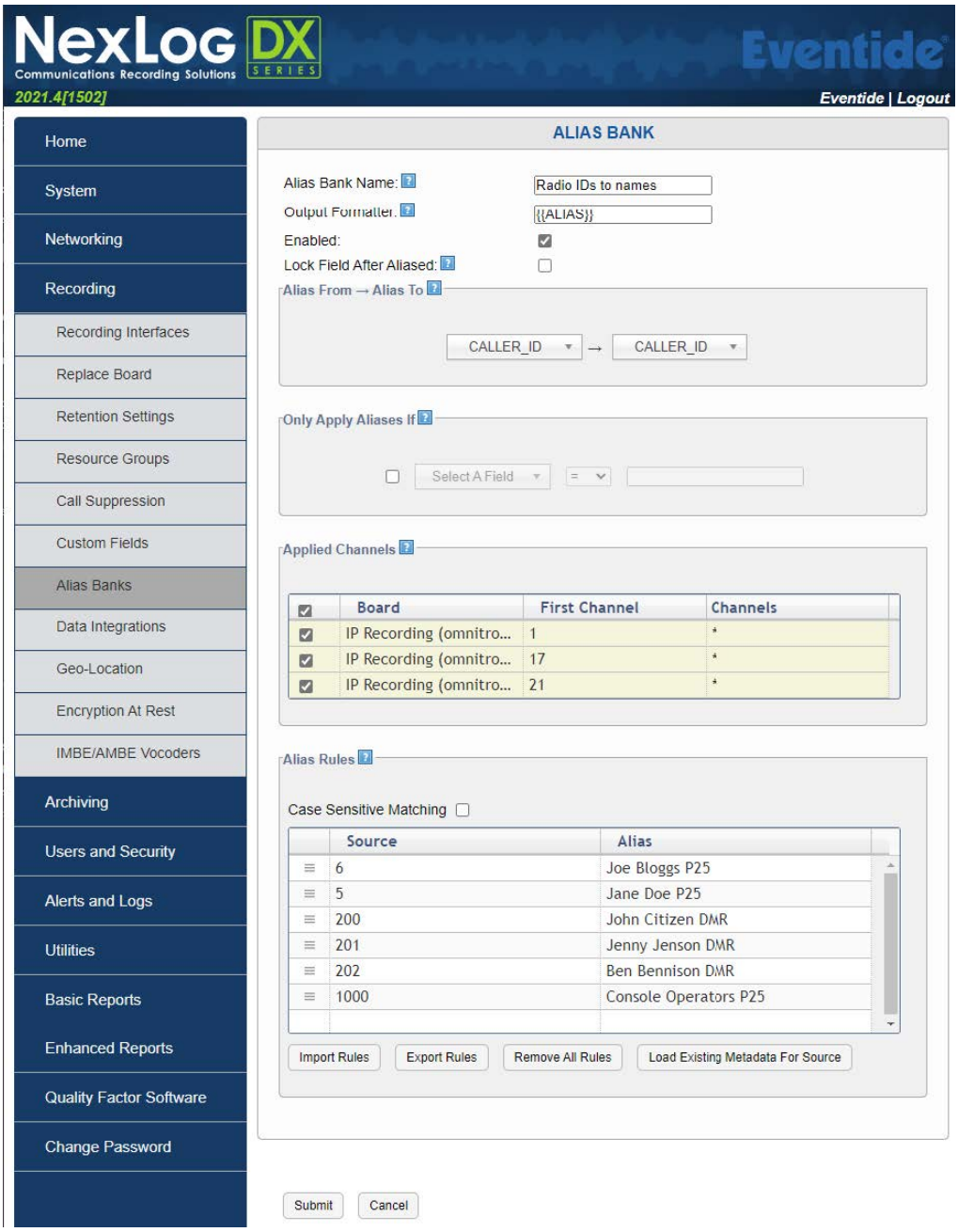


Fig. 6.88 Template Field Details

> **Note**
>
> Only new radio calls made after the configuration has been saved will have their IDs converted to the names defined in the Alias Bank.

6.14.2.3.2. Configure an Alias Bank for Talk Group/All Call IDs

To show names for your Talk Group/All Call IDs instead of numbers, you can configure an alias bank for Talk Group/All Call IDs. To configure alias bank for Talk Group/All Call IDs

- Login to the Configuration Manager (see “Log in to NexLog DX Recorder” on page 3)
- On the menu, select Recording, select Alias Banks, then Add Alias Bank

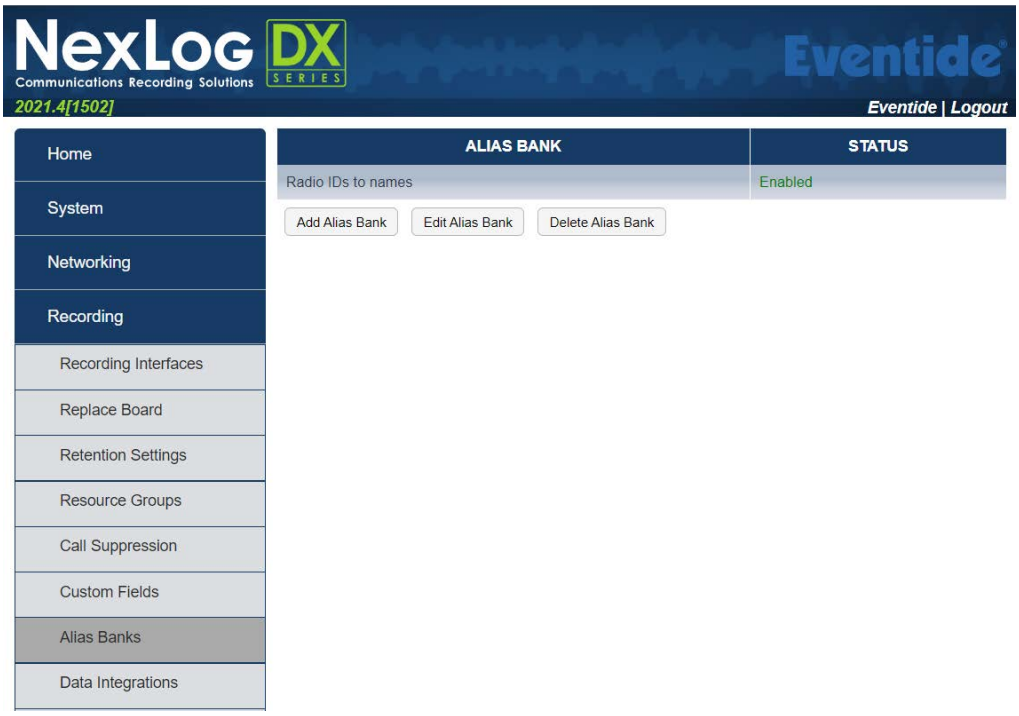
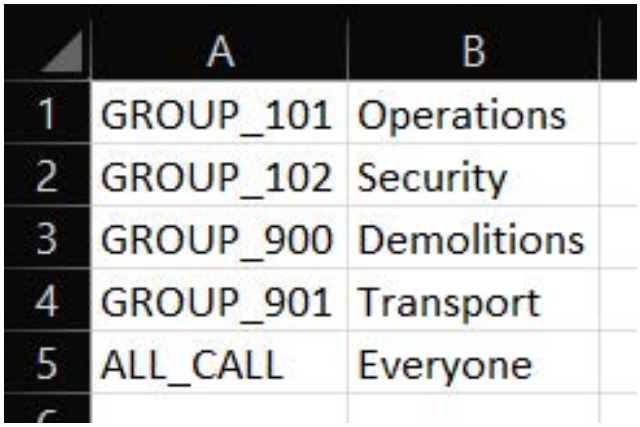


Fig. 6.89 Template Field Details

On the Alias Bank screen:

- Set the Alias Bank Name e.g. “Talkgroup IDs to names”
- Leave the Output Formatter as {{ALIAS}}

- Set both Alias From and Alias To as “DTMF”
- Leave Only Apply Aliases If unchecked
- In Applied Channels, check the box next to each IP Recording (Omnitronics template) board that is receiving the digital radio IDs. If you are unsure, select all of them.
- In the Alias Rules section, set the Source column to your group numbers in the format “GROUP_nnn” (e.g., GROUP_101) to match the raw talk group number. To change All Call naming, set this to “ALL_CALL”. Set the Alias column to the new desired group- or all-call name.
- Alternatively, you may import a .csv list of talk group IDs and names using the Import Rules Button. Ensure the first column contains the group numbers in the format “GROUP_nnn” (use “ALL_CALL” for All Call naming), and the second column contains only the desired names (do not include table headers). The following example is a .csv file edited with Microsoft Excel in this format: Graphical user interface, text, application, table, Excel



	A	B
1	GROUP_101	Operations
2	GROUP_102	Security
3	GROUP_900	Demolitions
4	GROUP_901	Transport
5	ALL_CALL	Everyone

Fig. 6.90 Template Field Details

- Once you have entered (or imported) all the groups and their desired names, select Submit to save the changes.

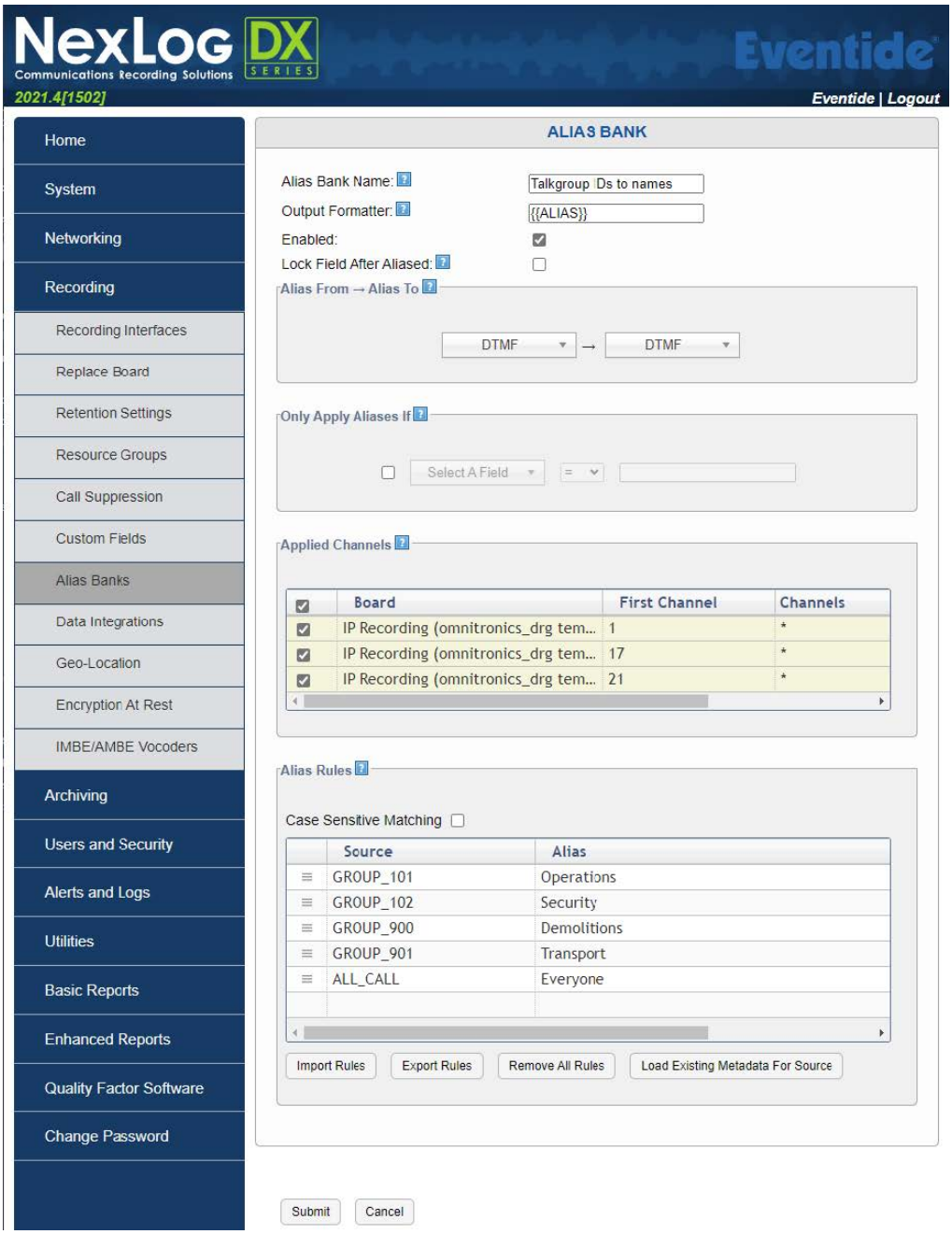


Fig. 6.91 Template Field Details

> **Note**
>
> Only new radio calls made after the configuration has been saved will have their IDs converted to the names defined in the Alias Bank.
>
> If your system is configured to make individual calls, Nexlog DX will place the individual call recipient in the “Dtmf” column, which will be a radio ID. Additional “DTMF” Alias Bank entries will need to be made should you wish to convert the individual call recipient to a name, where the Source is set to the raw radio ID, and Alias is set to the name of the radio.

6.14.2.3.3. Verify Alias Bank Names

Before verifying the applied alias bank rules, you must make at least one digital radio call on a configured ID/talk group before continuing.

Login to the MediaWorks DX web page for your recorder, then observe the “Caller Id” and “Dtmf” columns. Verify new radio calls made contain your configured names:

Source Name	Channel Name	Start Time	Duration	Caller Id	Connection ID	Dtmf	Calltype
OmniNexLog	ALL_CALL	2021-12-16 13:37:42 +08:00	00:05	Console Operators P25	240100151	Everyone	
OmniNexLog	GROUP_102	2021-12-16 13:26:45 +08:00	00:08	Console Operators P25	240100151	Security	
OmniNexLog	ALL_CALL	2021-12-16 13:26:24 +08:00	00:06	Console Operators P25	240100151	Everyone	
OmniNexLog	GROUP_101	2021-12-16 13:22:20 +08:00	00:10	Joe Bloggs P25	240100151	Operations	
OmniNexLog	GROUP_101	2021-12-16 12:08:46 +08:00	00:08	Console Operators P25	240100151	Operations	
OmniNexLog	GROUP_101	2021-12-16 12:08:39 +08:00	00:05	Jane Doe P25	240100151	Operations	

Fig. 6.92 Template Field Details

6.14.3. Omnitronics Device Configuration

This section deals with configuring Omnitronics devices to send audio to the Eventide Nexlog recorder.

6.14.3.1. IPR100, IPR110+, DRG100, DRG200i

Use the following procedure to configure IPR100, IPR110+, DRG100, and DRG200i devices.

To configure IPR100/IPR110+/DRG100/DRG200i devices

Using your web browser, log in to the Omnitronics IPR or DRG device you want to add to the recorder interface

Select Go to ADVANCED mode

On the menu, select VoIP/RTP to display the VoIP/RTP Configuration page

(DRG100 and DRG200i only) Select the option Enable digital radio RTP extension

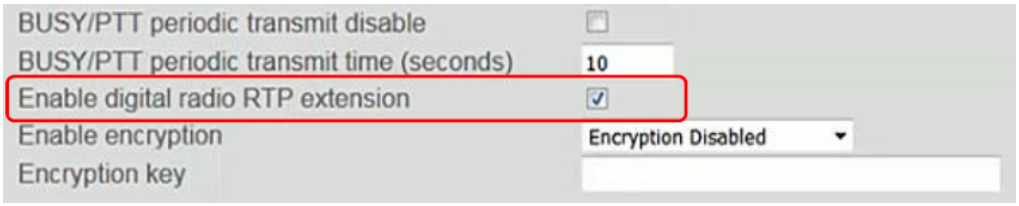


Fig. 6.93 Template Field Details

Note

Not all DRG100 and DRG200i firmware versions/variants support this option. Non-support for this option will not affect the operation of conference mode or audio forwarding to the recorder.

Under Conference Mode, do the following:

- Select the Enable conferencing option to enable Conference Mode
- For the Conference Mode, select Bridge server: audio linked
- For the next available IP address, select the Enable option
- In the IP Address text box, type the IP address of the Eventide Nexlog Recorder.
- In the Transmit Port text box, type the port on which the gateway will transmit (this is the port that was configured for this device in the recorder configuration)

In this example, the recorder's IP address is 192.168.20.18 and the port number for recorder is 7050.

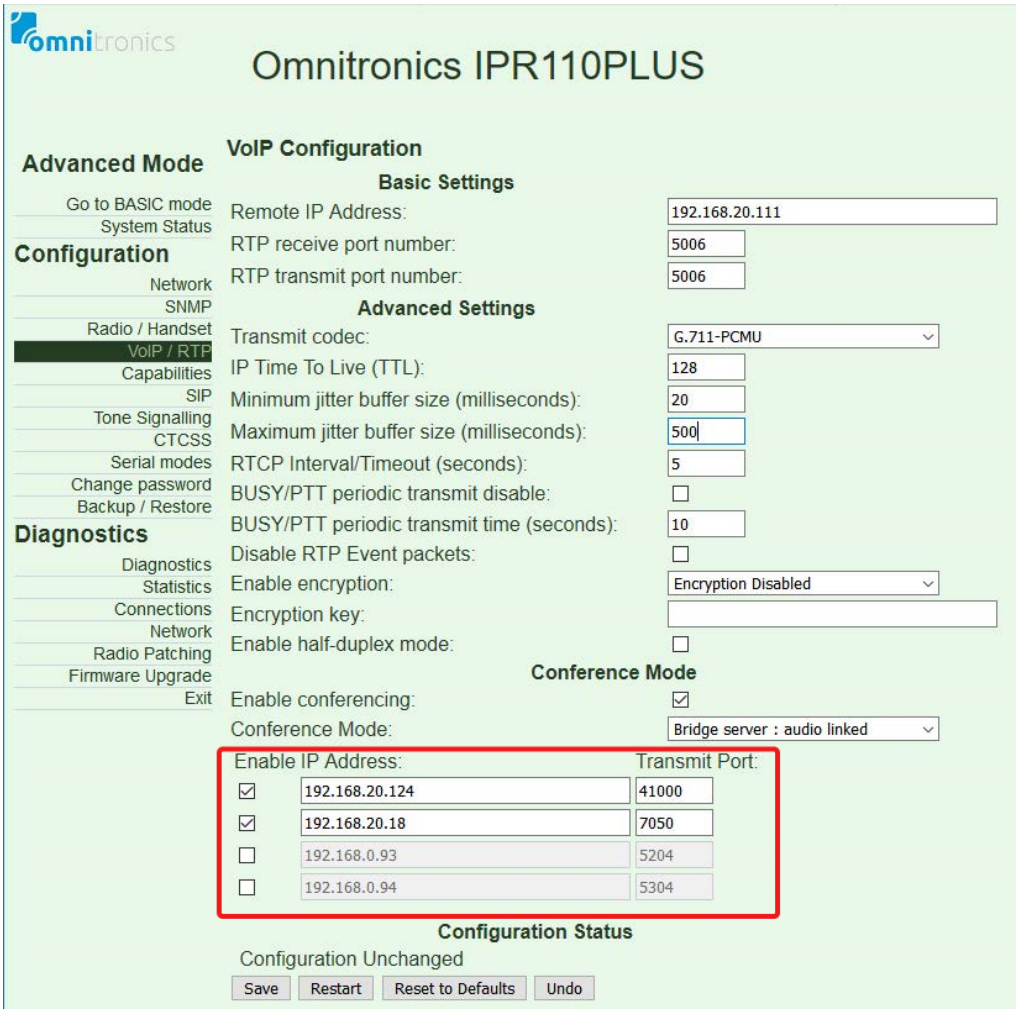


Fig. 6.94 Template Field Details

Select Save to save the configuration, and then select Restart for the changes to take effect.

Configuration of the IPR100/IPR110+/DRG100/DRG200i is now complete.

6.14.3.2. IPR400

Use the following procedure to configure IPR400/IPR400S2 device.

To configure IPR400 device

Using your web browser, log in to the Omnitronics IPR400 device you want to add to the recorder interface.

Under the Audio/Channel menu, select VoIP/RTP to display the VoIP/RTP Configuration for Channel 1.

Under Conference Mode, do the following:

- Select the Enable conferencing option to enable Conference Mode
- For the Conference Mode, select Bridge server: audio linked
- For the next available IP address, select the Enable option
- In the IP Address text box, type the IP address of the Eventide Nexlog Recorder
- In the Transmit Port text box, type port on which the IPR400 will transmit (this is the port that was configured for this device in the recorder configuration)

In this example, the recorder's IP address is 192.168.20.18 and the configured port number for recording is 7060:

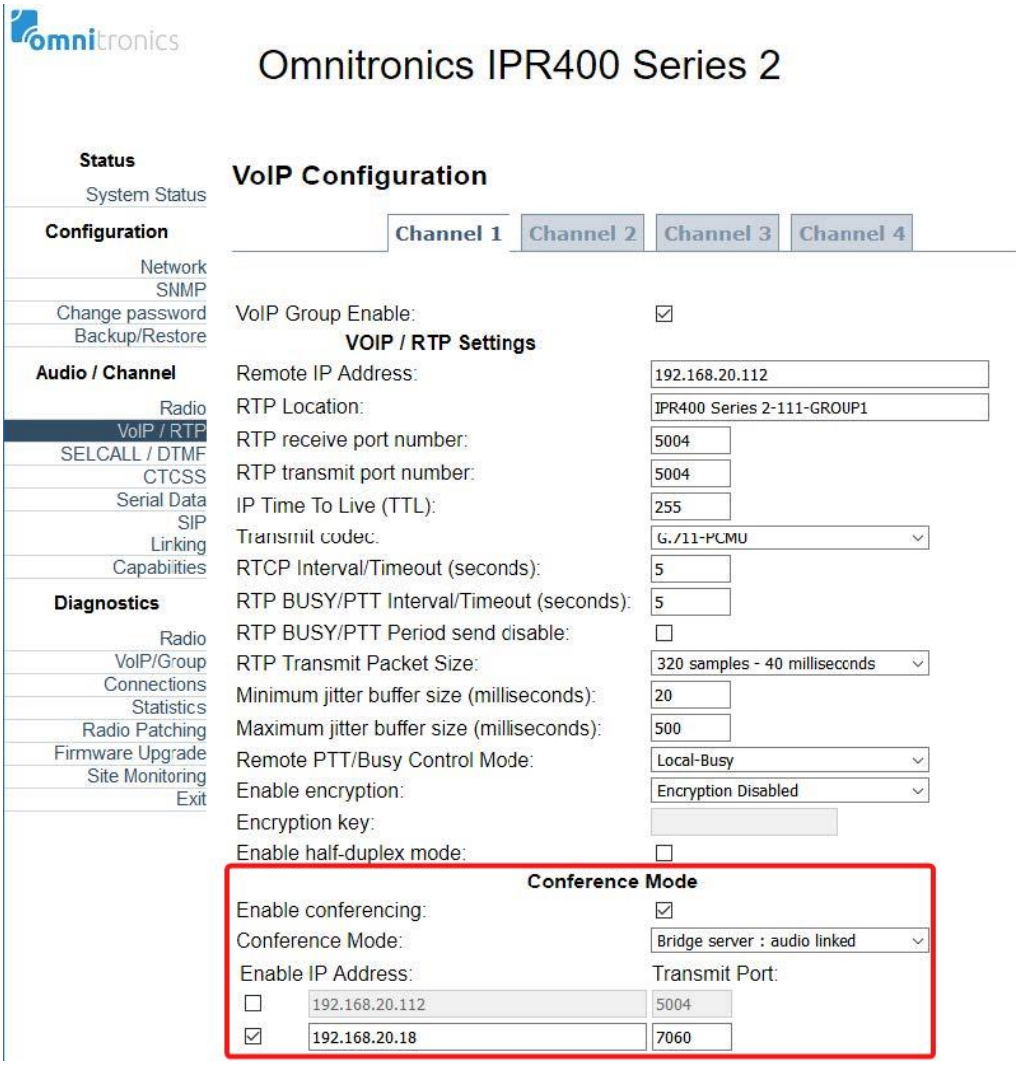


Fig. 6.95 Template Field Details

Select Save to save the configuration for this channel.

Select the tab for the next channel, and then repeat steps 3 and 4 to configure that channel.

> **Note**
>
> Ensure that the Transmit Port number is different from any other IPR400 channel, and the port numbers match those configured in the Eventide Nexlog configuration.

Select Restart for the changes to take effect.

Configuration of the IPR400 is now complete.

6.14.3.3. DX-Altus IPE

> **Note**
>
> The following procedure assumes that the DX-Altus system already has an IPE (in Recorder mode) installed and added to the Local Device configuration tab of the SCU. Refer to the *DX-Altus Installation Guide* for further configuration information.

To configure the DX-Altus IPE

Using a web browser, browse to the Main SCU IP address and log in.

Select Settings to expand the menu, and then select Devices to display the Devices page (the Local Devices page is selected by default).

On the Local Devices page, select the IPE in Recorder mode, and then select Edit.

Select the Recorder1 tab to display the page for Recorder1.

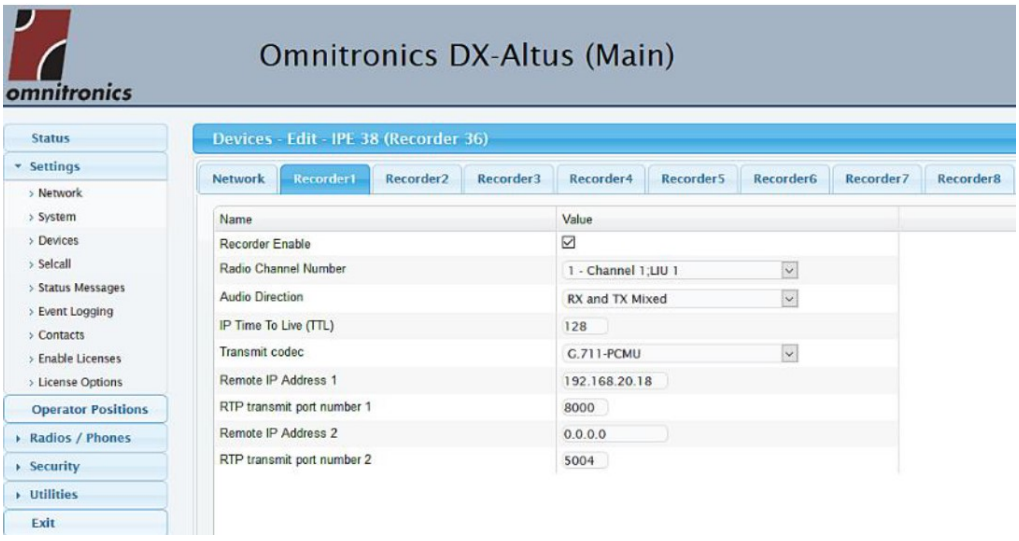


Fig. 6.96 Template Field Details

Configure the recorder settings as follows:

- Recorder Enable: Selected
- Radio Channel Number: The DX-Altus system channel you want to record
- Audio Direction: TX, or RX, or TX and RX mixed
- IP Time To Live and Transmit Codec: 128 (default)
- Remote IP Address 1: IP address of the Eventide NexLog recorder
- RTP transmit port number 1: TX port number configured in the Eventide NexLog recorder configuration
- Remote IP Address 2 and RTP transmit port number 2: *(Optional)* The IP address and port number of a secondary VoIP recorder

Repeat steps 4 and 5 to configure the other channels (up to the 8 channels) of the IPE recorder.

Select Save to save the configuration.

Under the Settings menu, select Devices to display the Devices page (the Local Devices page is selected by default).

On the Local Devices page, select the checkbox in the Restart column for the IPE in Recorder mode.

Select Save to complete configuration.

6.14.3.4. altusomni IPE

> **Note**
>
> The following procedure assumes that the altusomni system already has an IPE (in Recorder mode) installed and added to the Local Device configuration tab of the SCU. Refer to the altusomni Technical Manual for further configuration information.

To configure the altusomni IPE

Using a web browser, browse to the Main SCU IP address and log in.

Select Settings to expand the menu, and then select Devices to display the Devices page (the Local Devices page is selected by default).

On the Local Devices page, select the IPE in Recorder mode, and then select Edit.

Select the Recorder1 tab to display the page for Recorder1.

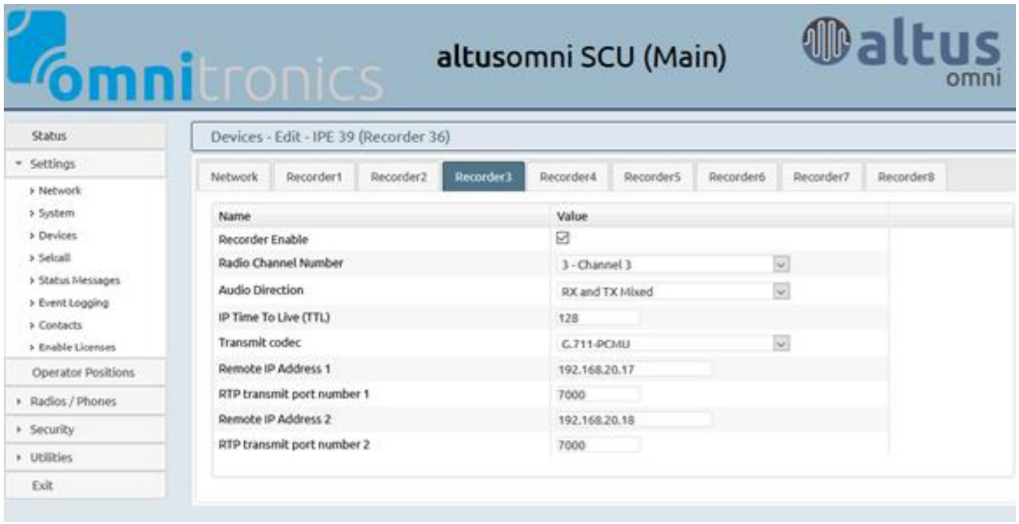


Fig. 6.97 Template Field Details

Configure the recorder settings as follows:

- Recorder Enable: Selected
- Radio Channel Number: The altusomni system channel you want to record
- Audio Direction: TX, or RX, or TX and RX mixed
- IP Time To Live and Transmit Codec: 128 (default)
- Remote IP Address 1: IP address of the Eventide NexLog recorder
- RTP transmit port number 1: TX port number configured in the Eventide NexLog recorder configuration
- Remote IP Address 2 and RTP transmit port number 2: *(Optional)* The IP address and port number of a secondary VoIP recorder

Repeat steps 4 and 5 to configure the other channels (up to the 8 channels) of the IPE recorder.

Select Save to save the configuration.

Under the Settings menu, select Devices to display the Devices page (the Local Devices page is selected by default).

On the Local Devices page, select the checkbox in the Restart column for the IPE in Recorder mode.

Select Save to complete configuration.

6.14.3.5. TetraGateway-DM

Use the following procedure to configure the TetraGateway-DM service.

> **Note**
>
> TetraGateway-DM does not support digital radio RTP extensions at the date of this publication.

To configure Tetra Gateway DM

Using your web browser, log in to the Omnitronics TetraGateway-DM web interface.

Select Settings, then select VoIP Connections.

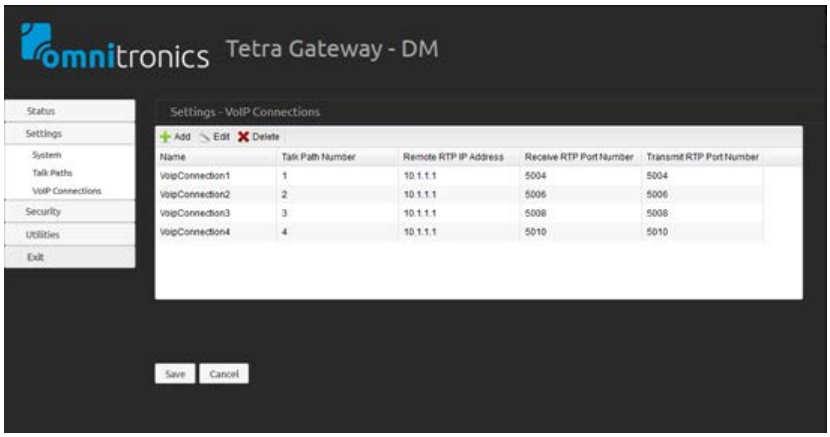


Fig. 6.98 Template Field Details

Select Add to add a new VoIP connection.

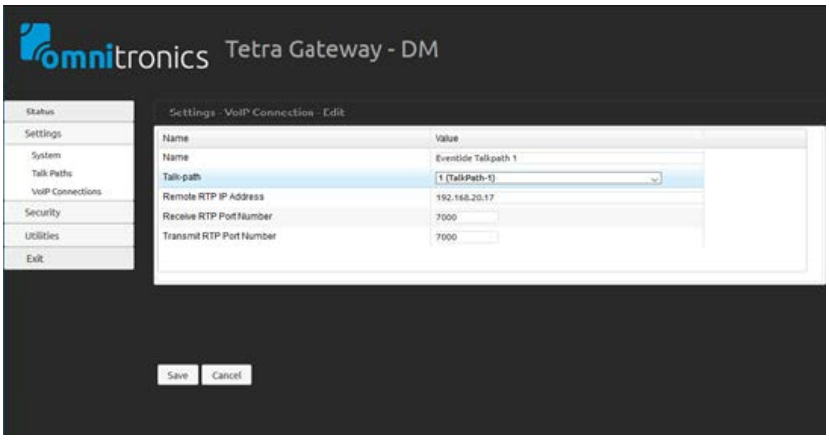


Fig. 6.99 Template Field Details

On the VoIP Connection Edit page, configure the following settings:

- Name: Type a name for the Eventide connection
- Talk-path: Select the desired TETRA talk-path that you want to record
- Remote RTP IP Address: Type the IPv4 address of your Eventide recorder
- Receive RTP Port Number and Transmit RTP Port Number: Set these ports to the same recording port number configured in Eventide for this talk-path

Select Save to save the settings.

Repeat steps 2 to 5 to add another TETRA talk-path that you wish to record, ensuring you assign a unique recording RTP port number to each talk-path.

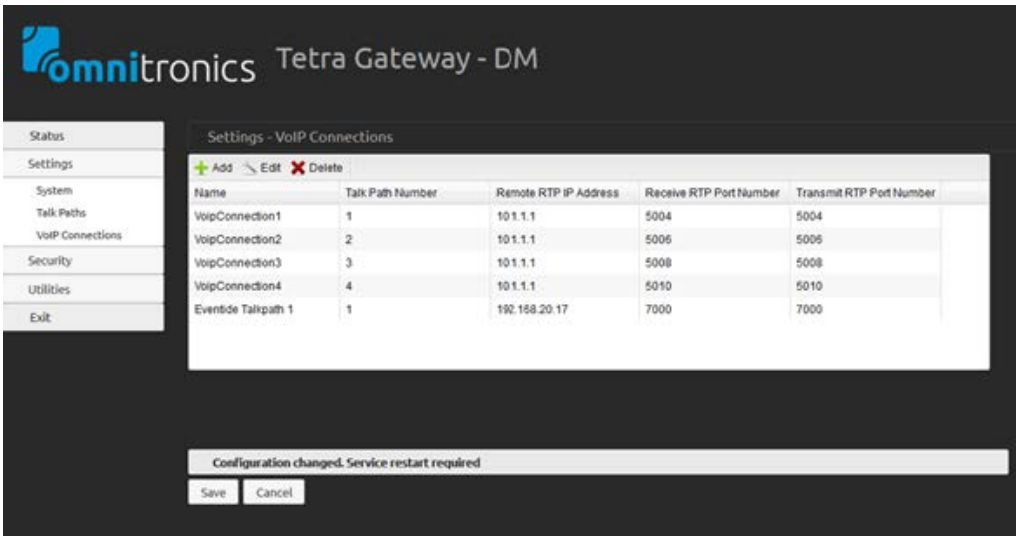


Fig. 6.100 Template Field Details

> **Note**
>
> After adding the Eventide talk-path(s) to the TetraGateway-DM, the service needs to be restarted for the changes to take effect (see procedure below).

To restart the TetraGateway-DM service

On computer running TetraGateway-DM, right-select the taskbar and select Task Manager

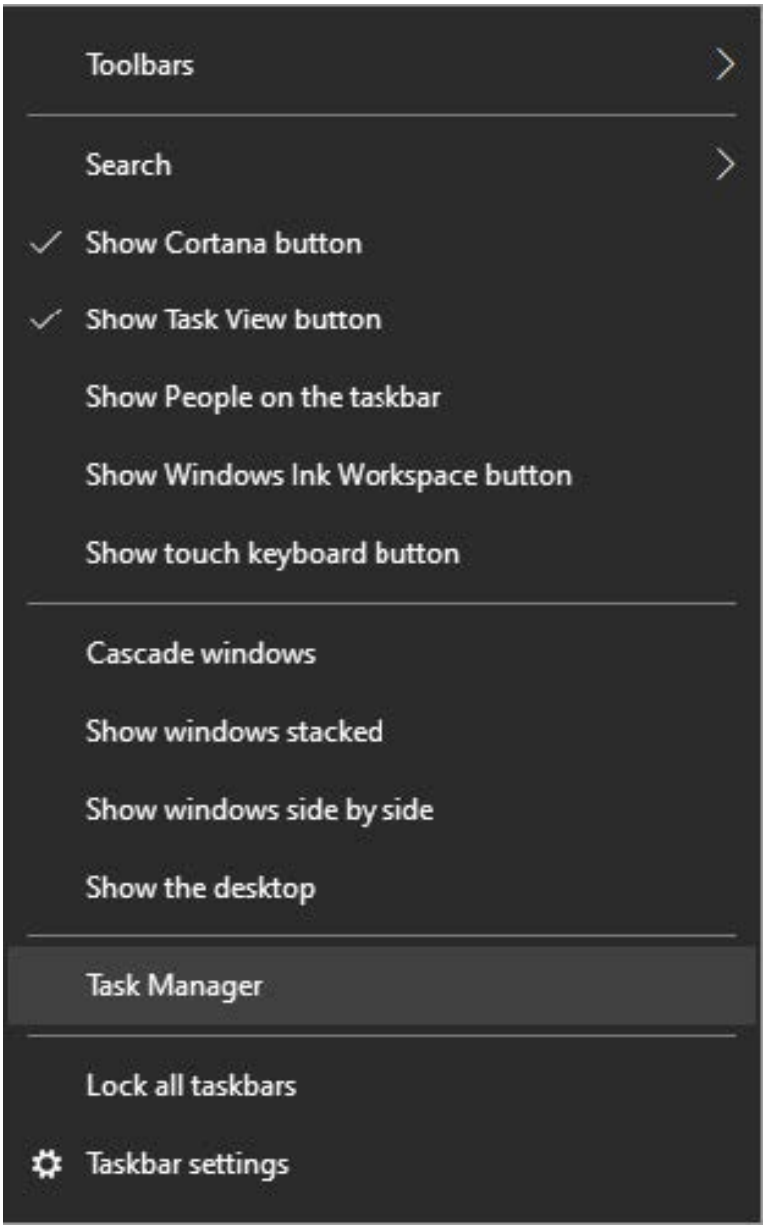


Fig. 6.101 Template Field Details

On the Task Manager window, select the Services tab.

In the list of services, right-click Omnitronics TetraGateway-DM and select Restart.

The service should restart after several seconds.

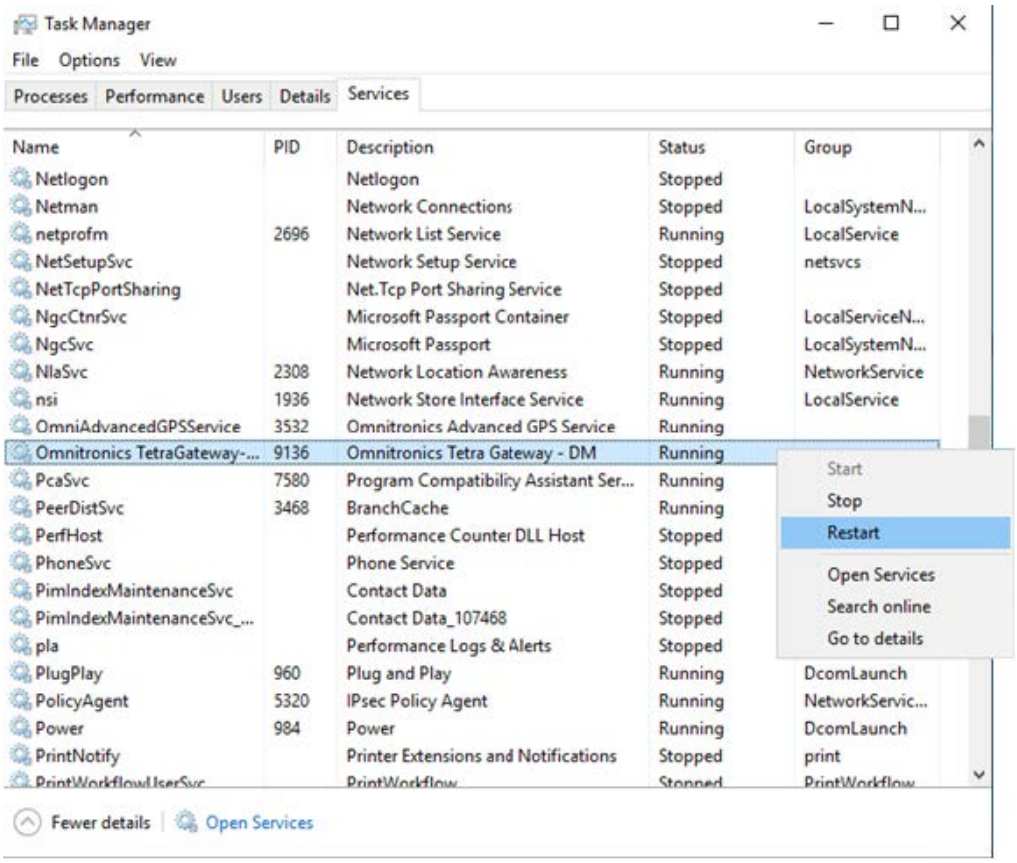


Fig. 6.102 Template Field Details

6.15. Tait Radio DMR/MPT Recording Interface

6.15.1. Tait Radio DMR/MPT Recording Interface Introduction

The purpose of this document is to describe the steps to ensure a successful integration between a NexLog Express and Tait DMR (Digital Mobile Radio) system.

The document assumes knowledge of the NexLog front panel interface and the browser based configuration manager and does not discuss recording interfaces beyond the Tait DMR integration. It also assumes familiarity with configuring the Tait system. For more details on these interfaces, please refer to their respective manuals.

6.15.2. Add Virtual Recording Interface

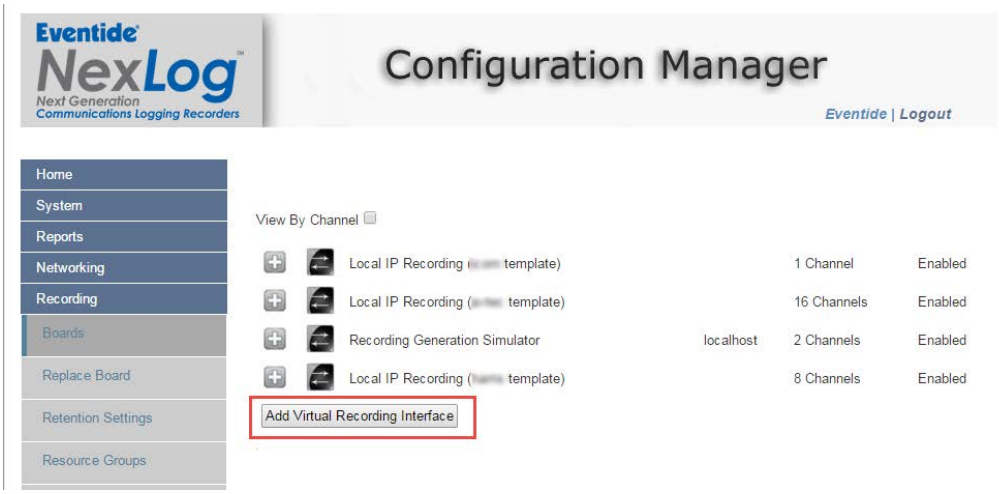


Fig. 6.103 Add Interface

Select the number of IP channels/number of talk paths

> **Note**
>
> This is the maximum number of talk paths between the NexLog and Tait Radio that can be recorded. Not to be confused with “Talk Groups”, multiple Talk Groups can be on one “Talk Path”.

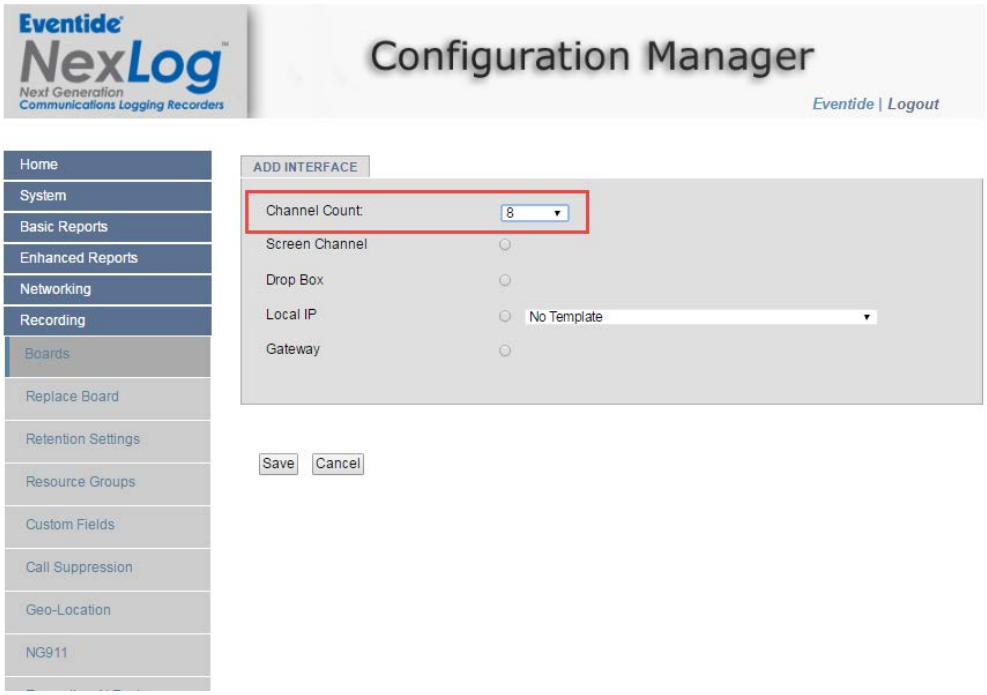


Fig. 6.104 Select IP Channel Count

Select the “Tait Radio DMR/MPT Recording Interface” Template

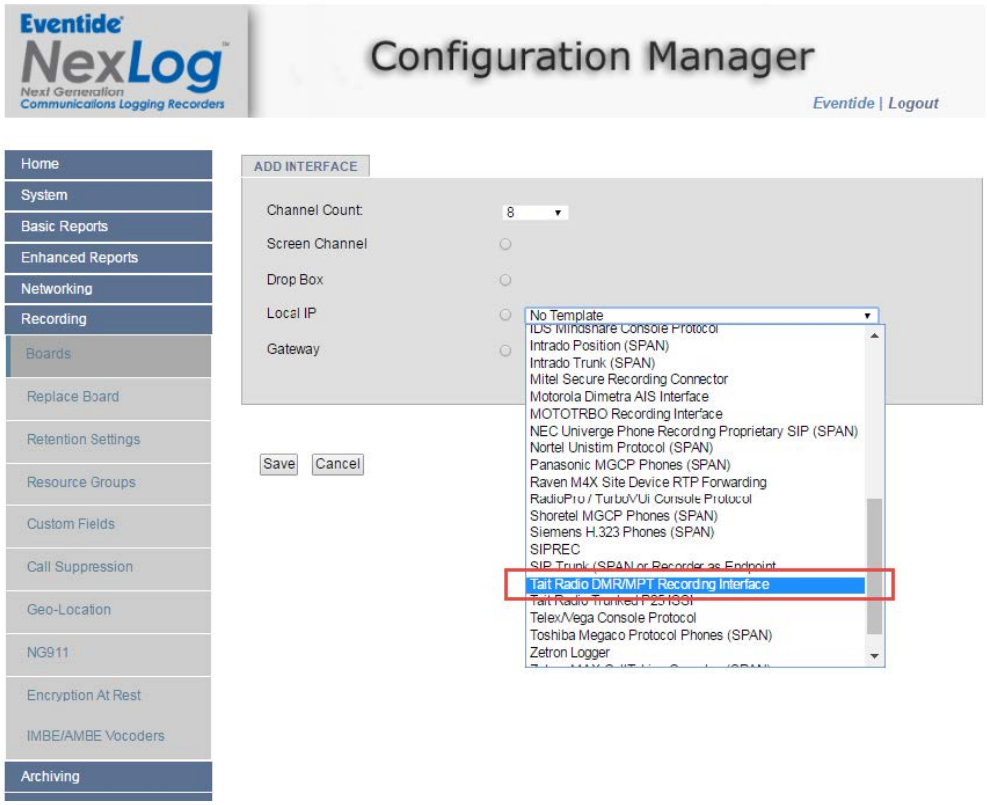


Fig. 6.105 Select Interface

Fill in the “Tait Radio DMR/MPT Recording Interface” template fields:

The following figure has the fields populated for illustrative purposes, the actual values in each installation will most likely be different. Verify each value with the Tait Radio ST or the Customer Network Administrator.

Template Field Detail

- Destination Port: Destination UDP port on the recorder where the Tait system is configured to send Voice Recorder Protocol traffic.

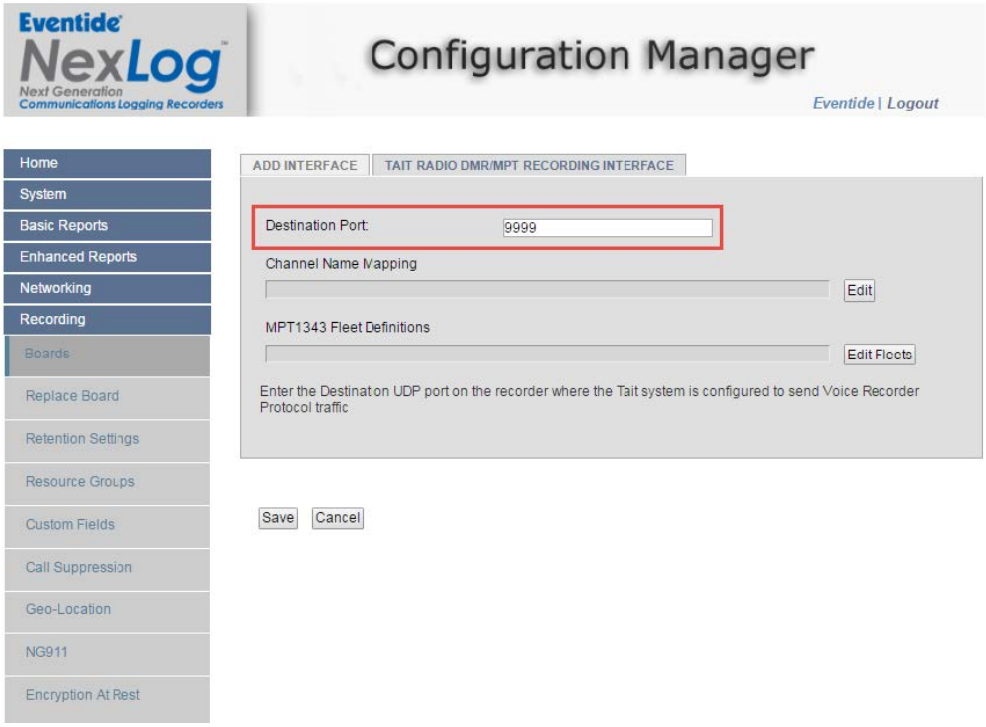


Fig. 6.106 Destination Port

- Create MPT1343 Fleet Definitions(optional): Here you can create a list of fleet definitions that can be used to map a fleet to a meaningful channel name under the Channel Name Mapping section. Note, Group and Radio IDs come over the wire in MPT1327 format, which may or may not match with a fleet definition that has been created. When fleet number in the MPT1327 address matches one of the definitions, it is converted into a MTP1343 address, then the MTP1343 address would be put into channel mapping section, to map the fleet to a meaningful channel name. For more information on MPT1337 and MPT1343 formatting, please see: https://en.wikipedia.org/wiki/MPT-1327

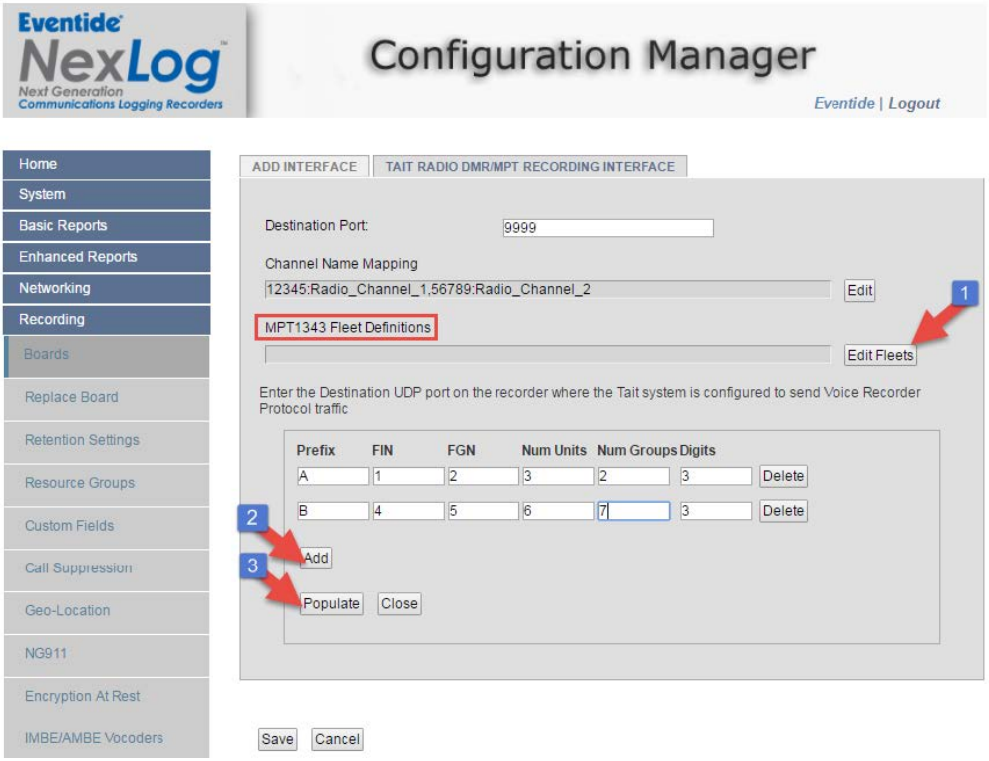


Fig. 6.107 MPT1343 Fleet Definitions

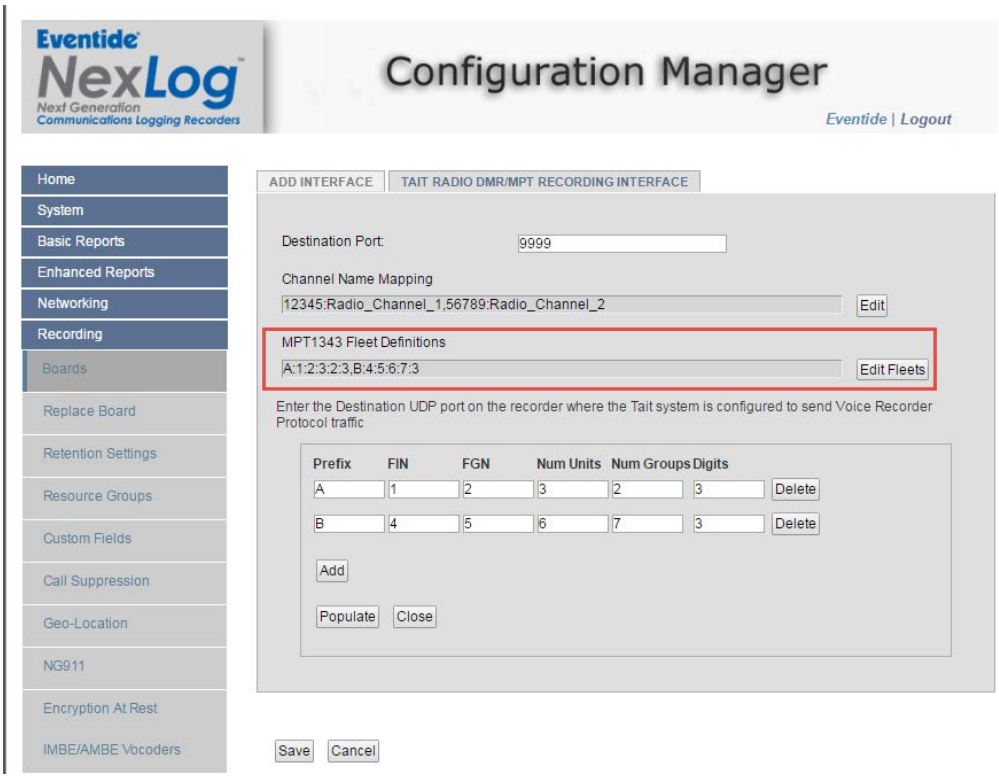


Fig. 6.108 MPT1343 Fleet Definitions

- Enter Channel Name Mapping(optional): Group IDs and Radio IDs delivered over the wire with MPT/DMR are in MPT1327 Format. You can map an MPT1327 raw input value to a more meaningful channel name. For more information on MPT1337 and MPT1343 formatting, please see: https://en.wikipedia.org/wiki/MPT-1327

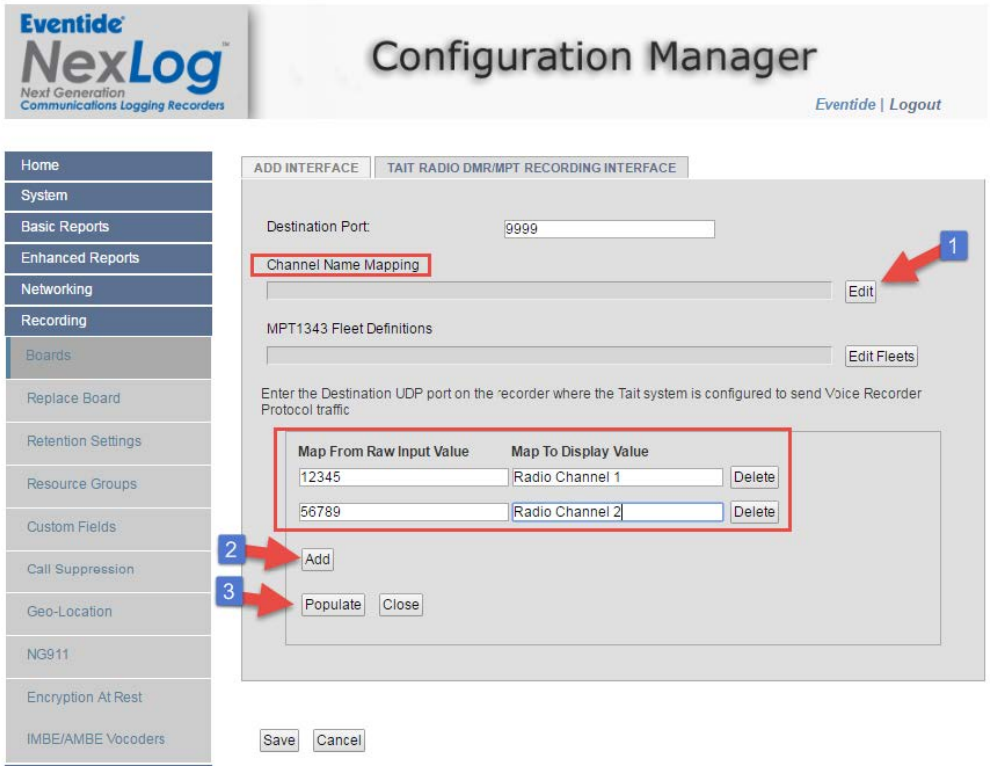


Fig. 6.109 Channel Name Mapping

After filling in all the fields, Select Save. The NexLog will now attempt to save the template data and initialize for recording.

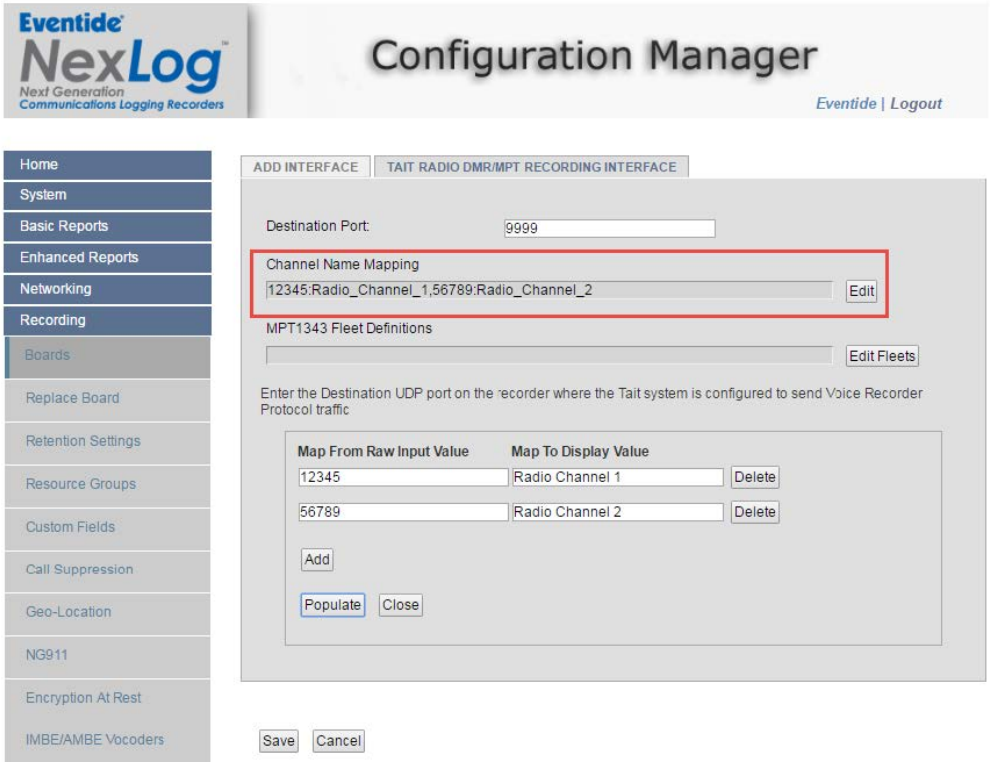


Fig. 6.110 Channel Name Mapping

6.15.2.1. Configure IMBE/AMBE Transcoder IP(s)

License Required

DVSI will require a “Num Internal Vocoder Resources” add-on license key. Contact your Eventide Communications Dealer for assistance.

P25 Systems and some DMR systems utilize IMBE/AMBE low bit rate encoding for recording. As a result, it is required to have at least one IMBE/AMBE vocoder (DVSI) resource available, which is used for playback of IMBE/AMBE encoded files.

There can be one or more IMBE/AMBE vocoders in the environment, each one’s unique IP address or internal status needs to be entered on the IMBE/AMBE configuration page. (Shown below).

6.15.2.2. Check for Alerts

Check the NexLog front panel and/or configuration manager (figure below) for any system alerts or Tait Radio specific alerts. There will be alerts specific to the Tait Radio integration if there are problems with downloading talk groups, managing crypto keys and OTAR.

6.15.2.3. Verify Recording

Place a series of test calls between radios on both encrypted and unencrypted talk groups. Use MediaWorks EXP or the front panel display to verify recording of all test calls.

6.16. Tait Radio Trunked P25 ISSI

6.16.1. Tait Radio Trunked P25 ISSI Introduction

The purpose of this document is to describe the steps to ensure a successful integration between an Eventide NexLog740 or NexLog840 and Tait Radio P25 Trunked system using ISSI (Inter RF Subsystem Interface). The document assumes knowledge of the NexLog front panel interface and the browser based configuration manager and does not discuss recording interfaces beyond the Tait Radio integration. It also assumes familiarity with configuring the Tait system. For more details on these interfaces, please refer to their respective manuals.

6.16.2. RFSS Configuration Detail

RFSS Voice Recorder Licensing

Using the TN9400 RFSS Manager (Configure->RFSS) ensure that both RFSS Controller A and B are licensed for voice recording, i.e. TNAS506 is non-zero, the number referring to the permitted number of voice recorder connections.

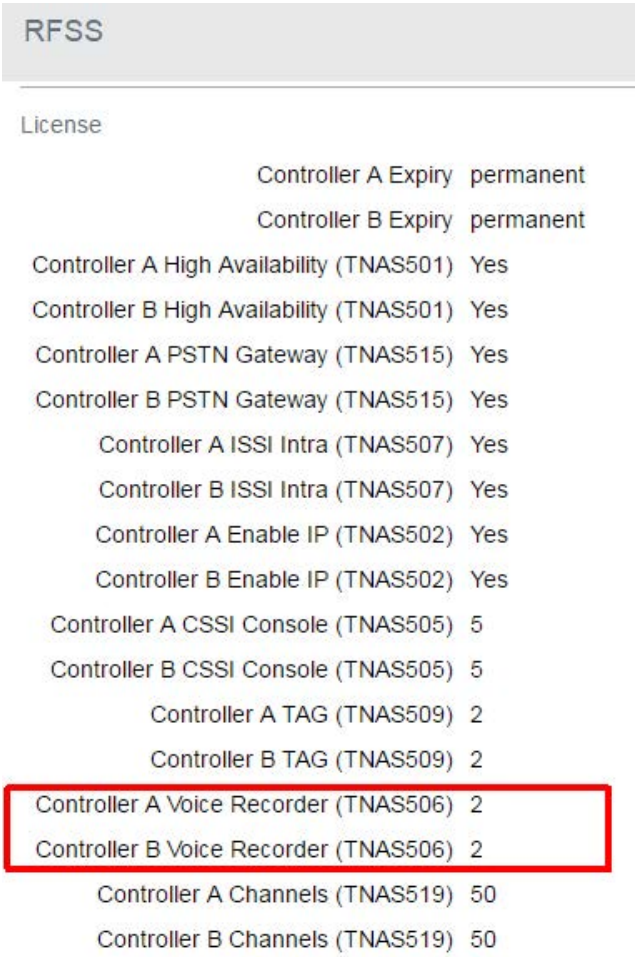


Fig. 6.111 Voice Recorder Licensing

Add the Nexlog as an external RFSS

Using the TN9400 RFSS Manager, accessed by selecting 'RFSS Manager' on the Tait Controller home page, add Nexlog as an External RFSS (Configure->External RFSSs).

The following figure has the fields populated for illustrative purposes; the actual values in each installation will most likely be different. Verify each value with the Tait Radio ST or the Customer Network Administrator.

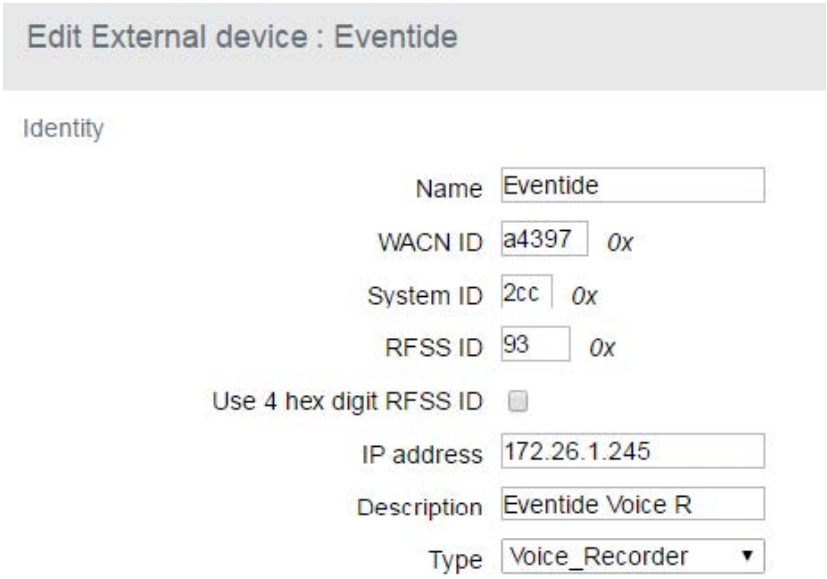


Fig. 6.112 Voice Recorder Licensing

Field Details

- Name: text string to identify the device
- WACN ID: WACN ID of the Nexlog, must match that of the RFSS
- System ID: System ID of the Nexlog, must match that of the RFSS
- RFSS ID: RFSS ID of the NexLog
- Use 4 hex digit RFSS ID: Leave unchecked as RFSS ID of Nexlog cannot be greater than 255
- IP Address: Enter the IP address of the Nexlog
- Description: User friendly description of the Nexlog
- Type: Set to Voice_Recorder

6.16.2.1. Push the configuration to both RFSS controllers

Log in to the RFSS command line using a secure shell tool such as putty. Execute the command RmCli send_all to push the new configuration to both controllers. Enter the Nexlog in the Locations table

Using the TN9400 Fleet Manager, accessed by selecting ‘Fleet Manager’ on the Tait Controller home page, enter Nexlog into the locations table. The following figure has the fields populated for illustrative purposes; the actual values in each installation will most likely be different. Verify each value with the Tait Radio ST or the Customer Network Administrator.

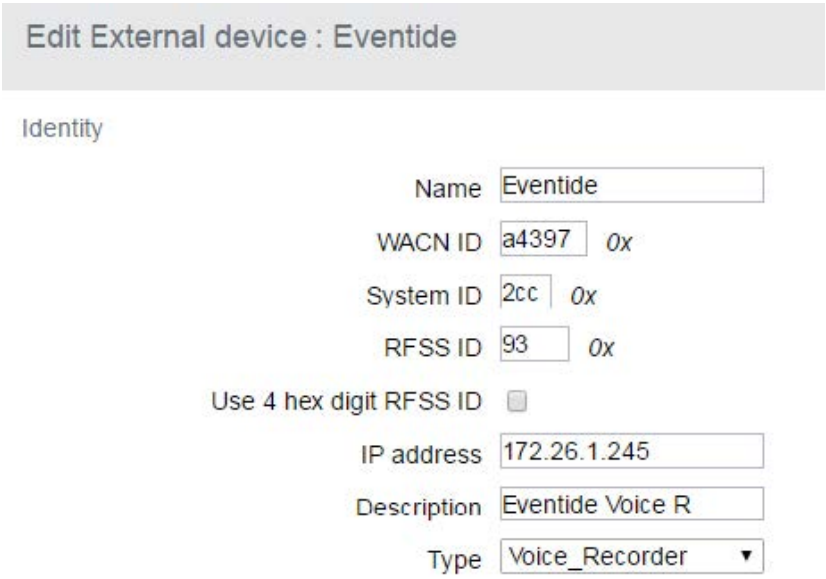


Fig. 6.113 Voice Recorder Licensing

Field Details

- Location ID: Hexadecimal quadruplet used to identify the NexLog Recorder (in the format rfss-id (of recorder).system-id.wacn-id.p25dr)
- Location Alias: text string to identify the device
- Location Type: 'Voice_Recorder'
- Vocoder Mode: Set to 'Full Rate/Half Rate' to record calls in both phase 1 and phase 2

6.16.2.2. NexLog Configuration Overview

Each of the follow steps will be explained or shown with screen shots: - Confirm NexLog version and licensing - Upload Tait P25 Talk Groups - Add a virtual recording interface board - Select the number of IP channels/number of talk paths - Select the Tait Radio Trunked P25 ISSI Recording Template - Fill in the required fields - Apply the template - Select the talk groups of interest (i.e. to be recorded) and Reapply the Template - Verify recording

> **Note**
>
> Where data entry is required, the "Typical Source" to ascertain the data from is noted.

6.16.3. NexLog Tait Radio P25 Configuration Detail

6.16.3.1. NexLog Licensing

Ensure that the NexLog is licensed appropriately for VOIP/RTP VoIP Channels, P25 decryption (if Crypto is being used), OTAR functionality (if OTAR being used) and Tait Radio P25 ISSI Integration. If proper licenses are not present contact Eventide technical support before proceeding.

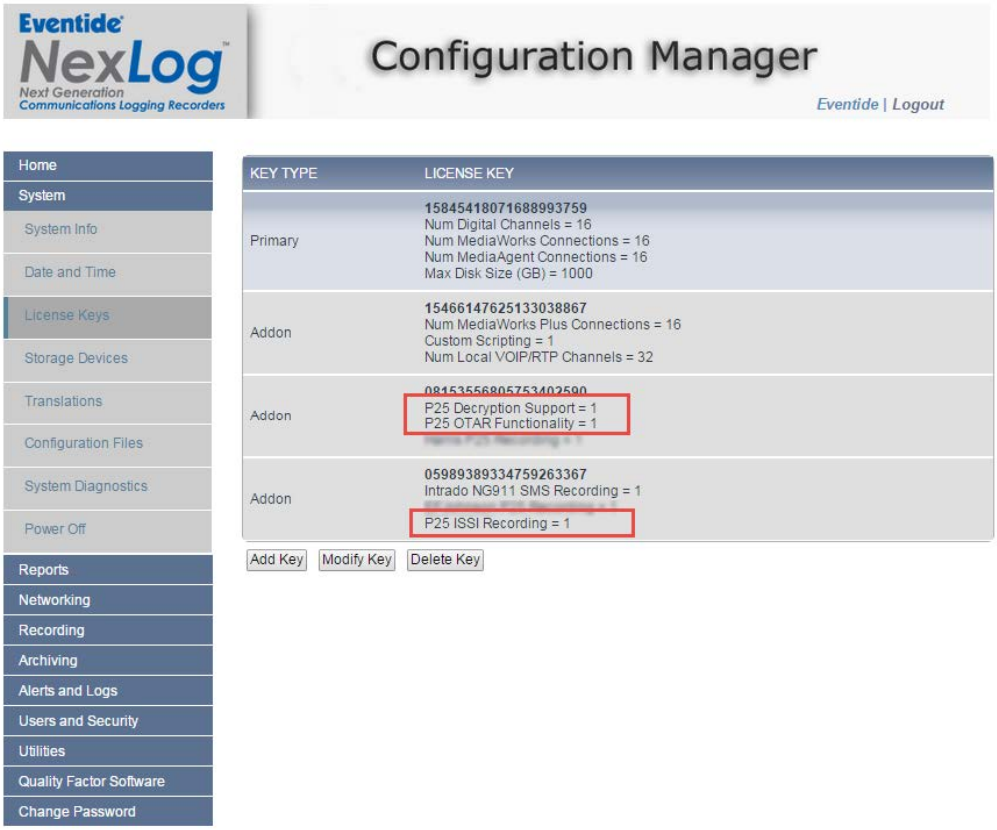


Fig. 6.114 Voice Recorder Licensing

Upload Tait P25 Talk Groups

The Tait P25 Talk Group configuration file is found on the 'System>>Configuration Files' Page (Shown below). Select "Tait P25 Groups List"

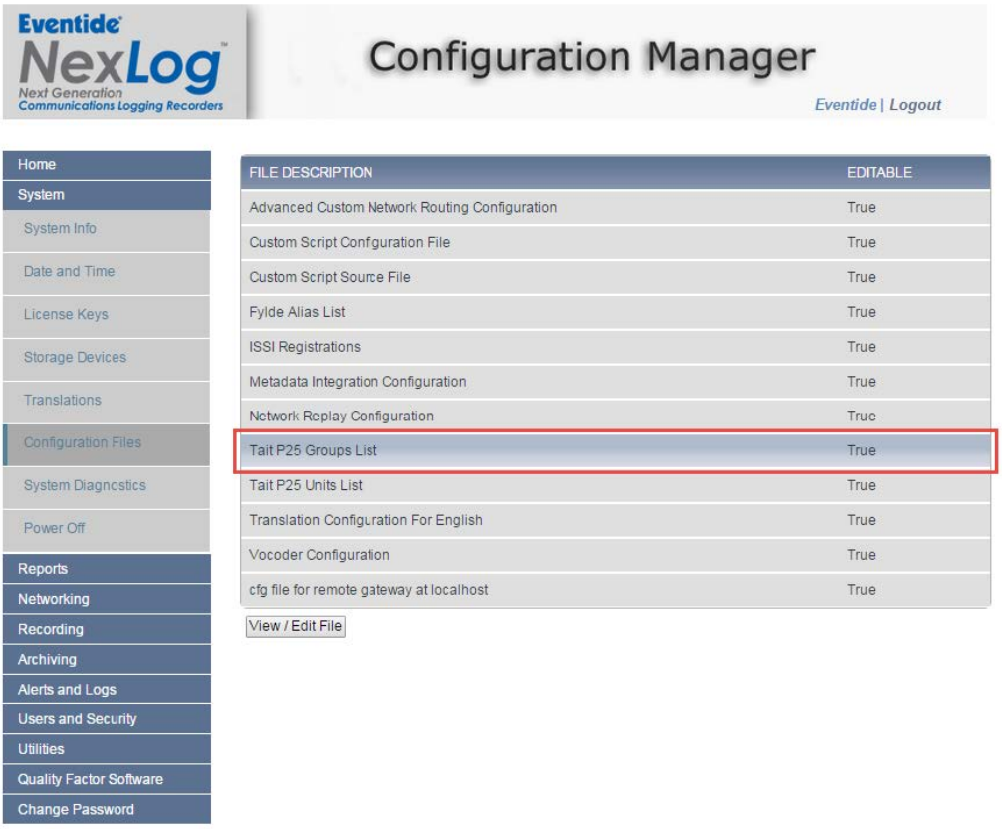


Fig. 6.115 Voice Recorder Licensing

It is recommended that the P25 Talk Groups be initially uploaded from a file provided by the Tait ST, using the menu shown below. The uploaded file contents will be shown on the page below. While it is not recommended, the contents can be updated directly on the web page.

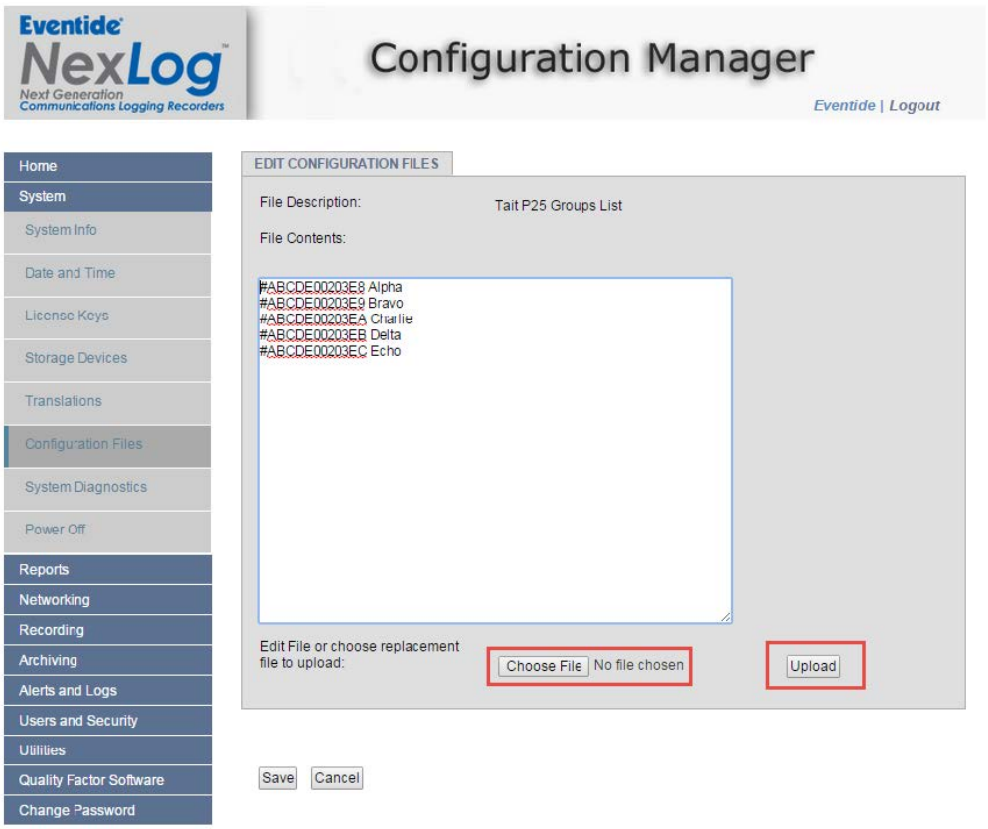


Fig. 6.116 Voice Recorder Licensing

Upload Tait P25 Units List (Optional)

The Tait P25 Units List file is found on the 'System>>Configuration Files' Page (Shown below).

Select "Tait P25 Units List". This is an optional step, however, uploading this file will enable useful name tagging of radio units that are being recorded.

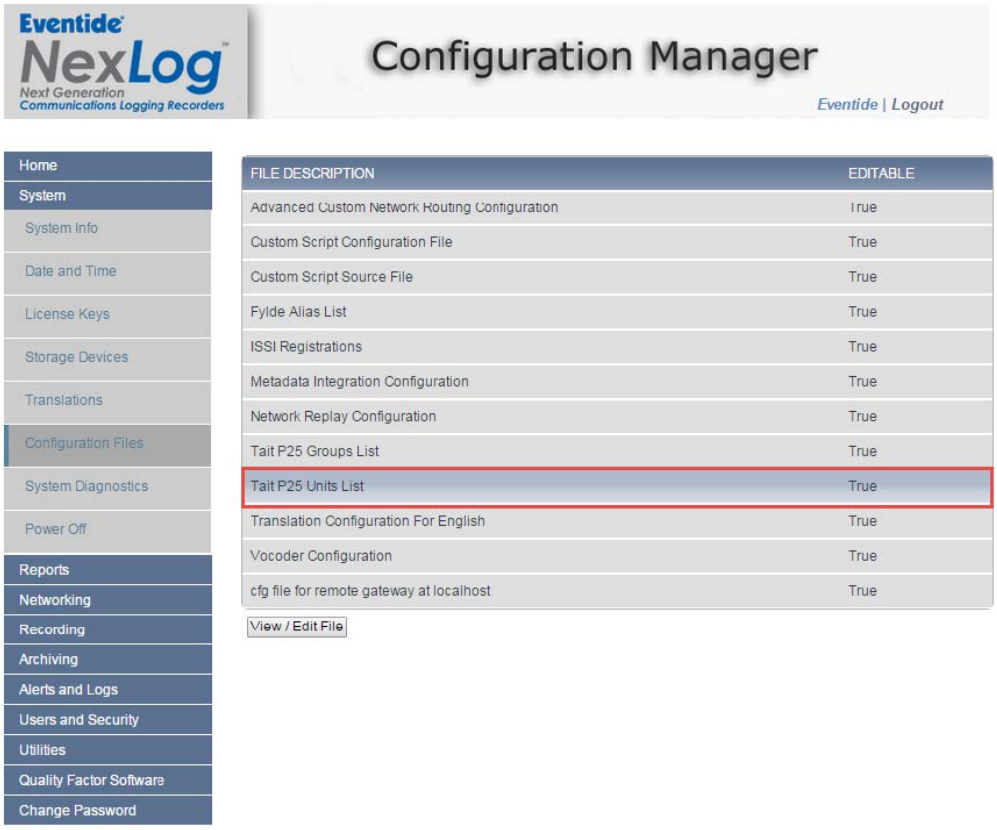


Fig. 6.117 Voice Recorder Licensing

It is recommended that the P25 Unit List be initially uploaded from a file provided by the Tait ST, using the menu shown below. The uploaded file contents will be shown on the page below. While it is not recommended, the contents can be updated directly on the web page.

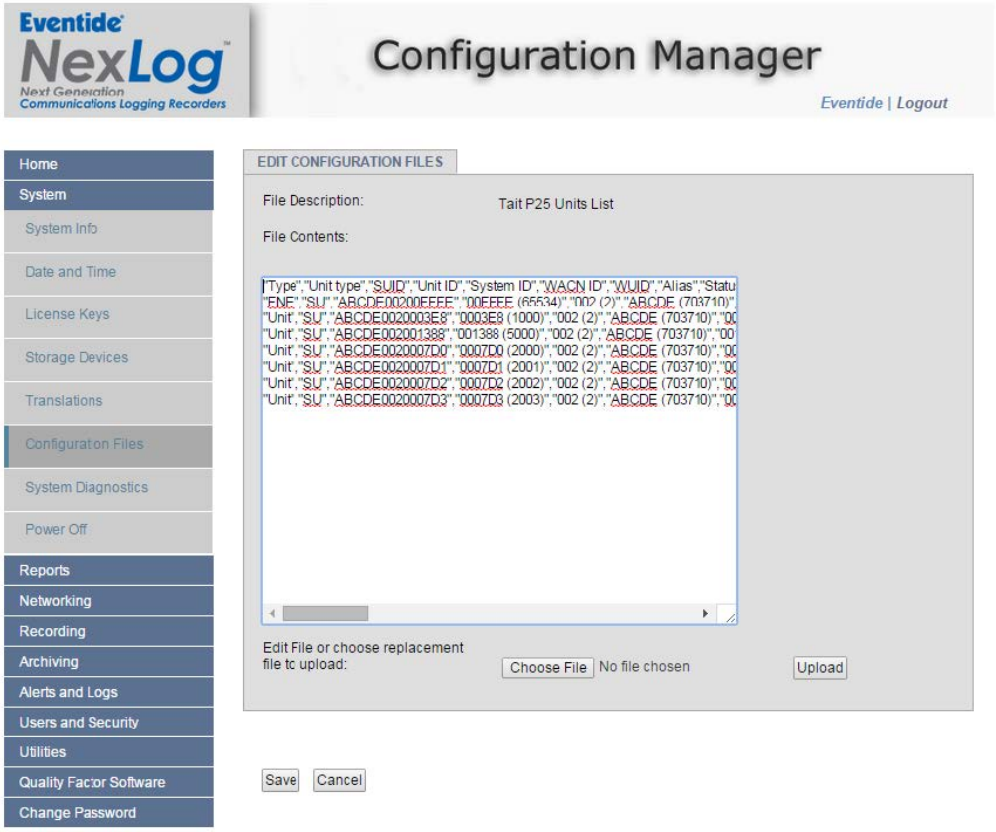


Fig. 6.118 Voice Recorder Licensing

Add Virtual Recording Interface

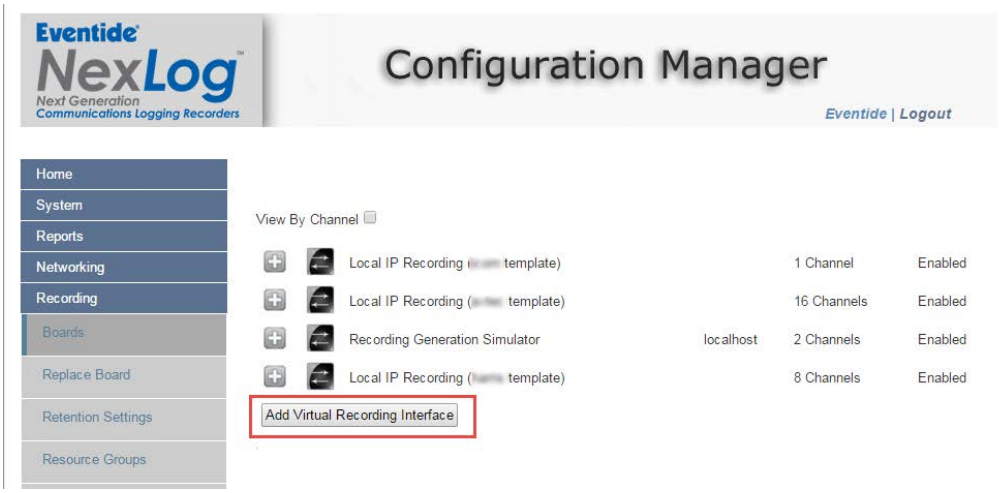


Fig. 6.119 Voice Recorder Licensing

Select the number of IP channels/number of talk paths

Note, this is the maximum number of talk paths between the NexLog and Tait Radio that can be recorded. Not to be confused with “Talk Groups”, multiple Talk Groups can be on one “Talk Path”.

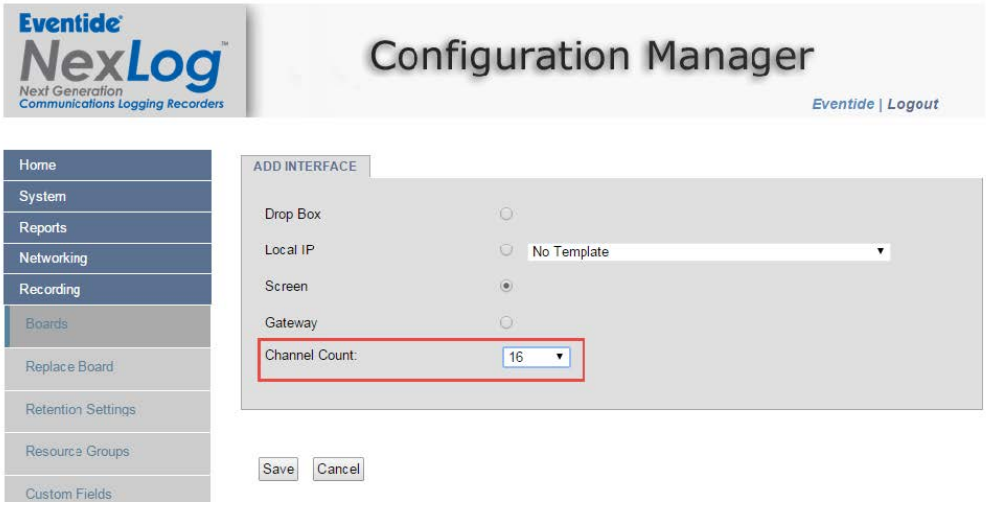


Fig. 6.120 Voice Recorder Licensing

Select the “Tait Radio Trunked P25 ISSI” Template

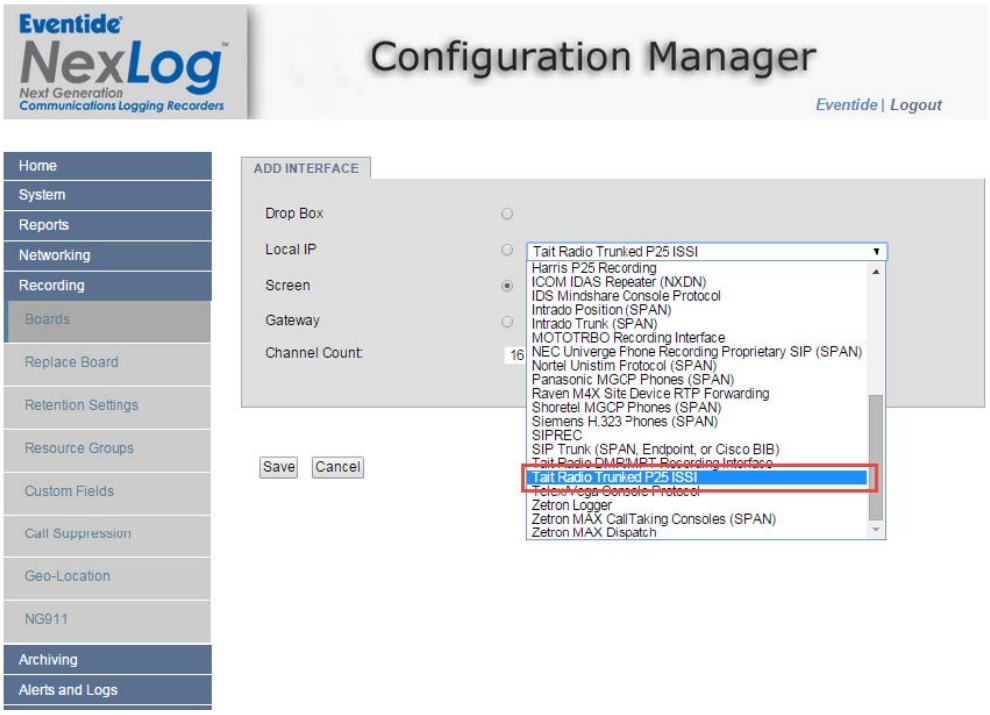


Fig. 6.121 Voice Recorder Licensing

Fill in the Tait Radio Trunked P25 ISSI Template Fields:

The following figure has the fields populated for illustrative purposes, the actual values in each installation will most likely be different. Verify each value with the Tait Radio ST or the Customer Network Administrator.

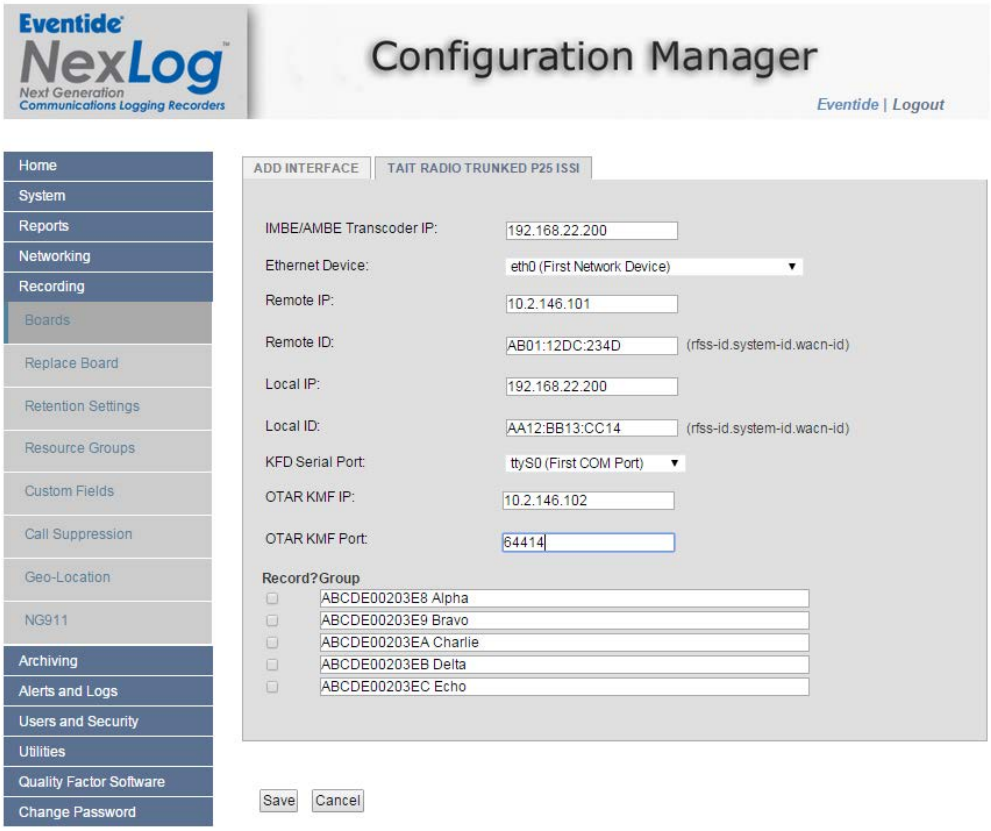


Fig. 6.122 Voice Recorder Licensing

Template Field Detail

- Ethernet Device: Select the physical Ethernet/NIC of the NexLog recorder which is connected the Tait Radio LAN switch
- Remote IP: Virtual IP address of the Tait Radio IP device that will send audio and metadata to the recorder (RFSS)
- Remote ID: Hexadecimal triplet used to identify the Tait Radio IP device that will send audio and metadata to the recorder (RFSS (in the format rfss-id.system-id.wacn-id))
- Local IP: IP address of the NexLog Recorder
- Local ID: Hexadecimal triplet used to identify the NexLog Recorder. (in the format rfss-id (of recorder).system-id.wacn-id)
- KFD Serial Port: Physical serial port on the back of the NexLog recorder that the Key Fill Device (KFD) will connect to (when applicable)
- OTAR KMF IP: IP address of the Key Manager Facility (KMF) which manages Over The Air Rekeying (OTAR), leave blank if OTAR will not be used

- OTAR KMF Port: UDP port over which the Key Manager Facility (KMF) will communicate to the recorder (Default port for Tait KMF is 64414), leave blank if OTAR will not be used
- Talk Groups to record: Select the talk groups to be recorded. These were uploaded to the recorder in a prior step

6.16.3.2. Apply the template

After filling in all the fields, select Save. The NexLog will now attempt to save the template data and initialize for recording.

6.16.3.3. Configure IMBE/AMBE Transcoder IP(s)

License Required

DVSI will require a “Num Internal Vocoder Resources” add-on license key. Contact your Eventide Communications Dealer for assistance.

P25 Systems utilize IMBE/AMBE low bit rate encoding for recording. As a result, it is required to have at least one IMBE/AMBE vocoder (DVSI) resource available, which is used for playback of IMBE/AMBE encoded files.

There can be one or more IMBE/AMBE vocoders in the environment, each one’s unique IP address or internal status needs to be entered on the IMBE/AMBE configuration page. (Shown below).

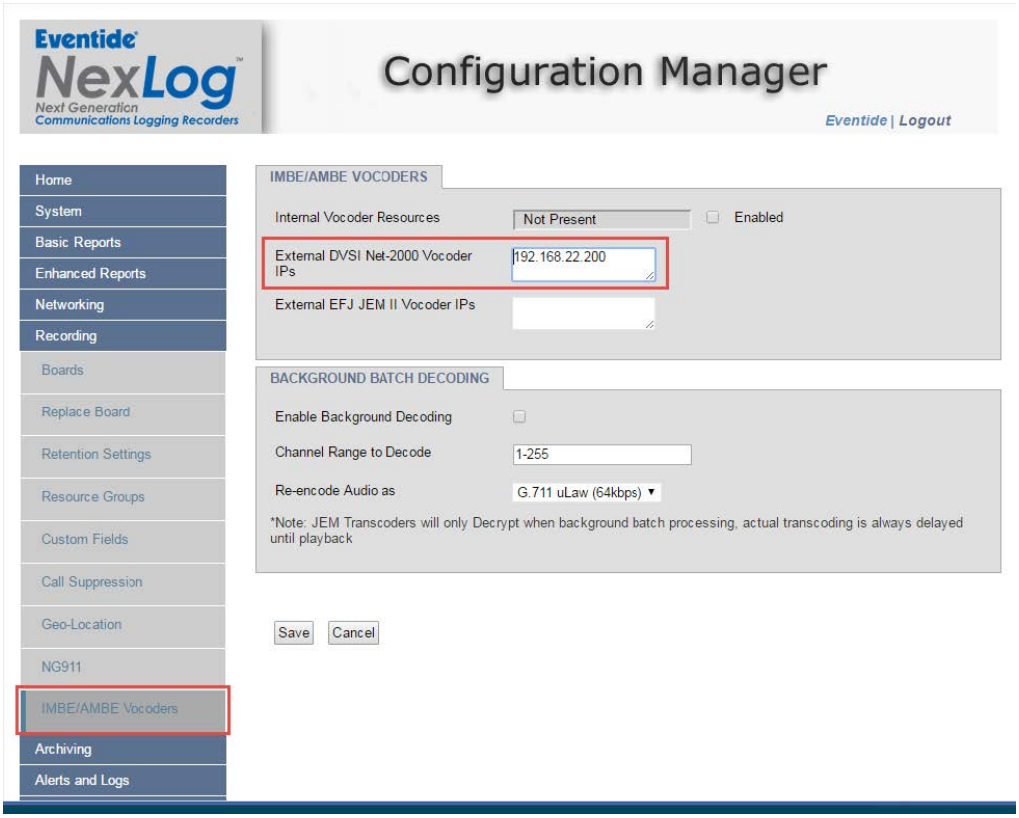


Fig. 6.123 Voice Recorder Licensing

> **Note**
>
> There is the possibility to have external or internal IMBE/AMBE vocoders. This example is using an external vocoder. Background batch decoding is not required and outside the scope of this document, please refer to the NexLog Recorder User Manual for further details.

6.16.3.4. Check for Alerts

Check the NexLog front panel and/or configuration manager (figure below) for any system alerts or Tait Radio specific alerts. There will be alerts specific to the Tait Radio integration if there are problems with downloading talk groups, managing crypto keys and OTAR.

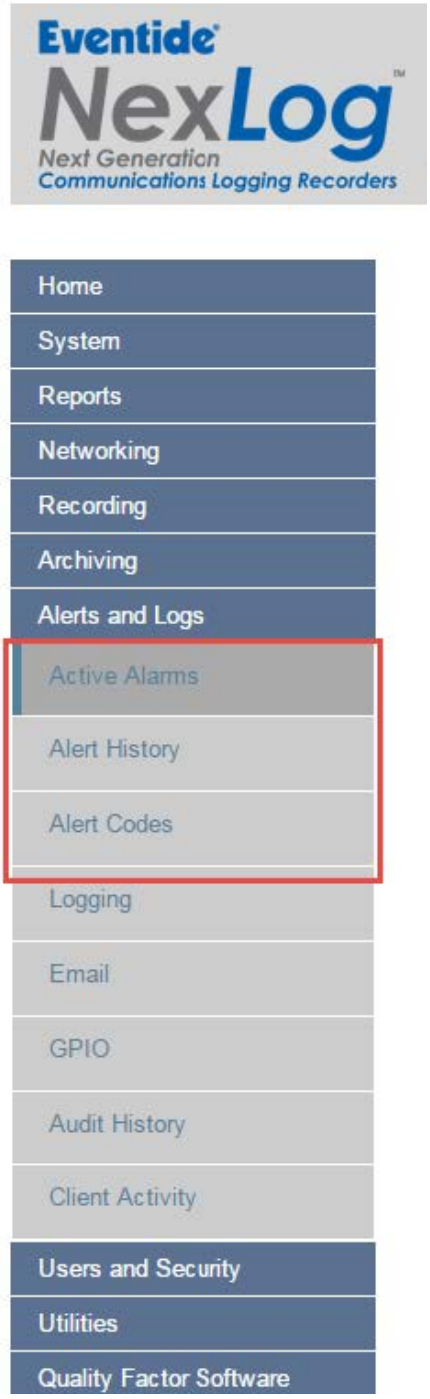


Fig. 6.124 Voice Recorder Licensing

6.16.3.5. Verify Recording

Place a series of test calls between radios on both encrypted and unencrypted talk groups. Use MediaWorks EXP or the front panel display to verify recording of all test calls.

6.17. Zetron Logger

Configuring Zetron interfaces on legacy NexLog vs. NexLogDX Setting up resource name mapping via Alias Bank in NexLog DX Series

The virtual board templates for Zetron interfaces are the same between legacy NexLog and NexLog DXSeries. The difference lies in the introduction of Alias Banks, which allows for mapping of raw metadata field values to more useful alias values. Following explains the use of Alias Banks.

Scope: Additional reference guide to assist with setting up resource name aliasing for a Zetron IP recording virtual board. Primary resource with additional examples available in the NexLog DX-Series Manual, section 6.3.7. Alias Banks

Step 1: Start by adding an Alias Bank from the Recording, Alias Banks section, using the Add Alias Bank button.

Step 2: Start with filling in the form by giving a name in the Alias Bank Name section

Step 3: Setup Alias From -> Alias To fields for the “CHANNELNAME” field in both options.

Step 4: Select the IP recording interface/s that will use this bank. In this case, it will be needed for all resources so the Channels will say as “*”. If you have multiple IP recording boards, they can all share the same bank.

Step 5: Setup the rules based on raw/source and what you want to use as an alias. You will have multiple lines here, so click enter to start a new line/entry.

Last step: Click Submit to save the alias bank.

Note: With firmware version 2020.3 and prior, there is a known issue where you will have to enable the “Case Sensitive Matching” option for the Alias Rules to function properly.

This page was intentionally left 99.88% blank.