Eventide®

NexLog DX
SERIES

Communications Recording Solutions

User Manual

Version 2021.3[1336]

P/N: #141338

Table Of Contents

7. Configuration Manager

1. Introduction

1.1. Welcome

Thank You and congratulations on your purchase of an Eventide® NexLog DX-Series™ 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 Front Panel 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.

1.2. 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 DX-Series™ 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.

- 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.

- **MediaWorks DX™:** On the **Help** menu, select **About** to display the version information.

2. General Specifications

All Eventide NexLog DX-Series™ 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 740 DX-Series™ Recorder

The NexLog 740 DX-Series™ Recorder is available with and without a touch screen control interface.

Table 2.1 **Specification Summary**

	NexLog 740 DX-Series™ Recorder	NexLog 740 DX-Series™ Recorder (Blank Panel)
Product view		
Front Panel Access	1024 x 600 touch screen display (and/or use an external display via HDMI, DVI, VGA)	None (use external display attached via HDMI, DVI, VGA)
Front Panel I/O	USB 2.0 (type A), 1/8-inch line level output, 1/8-inch headphone output	
Remote software	Web browser based NexLog DX-Series™ Configuration Manager Web browser based MediaWorks DX™ playback client (Optional) Windows-based remote playback clients (Optional)	
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	5 1/2 inches (3 rack units)
Depth	24 inches
Power	350 watts
Power supplies	Dual hot-swap
Weight	50-80 pounds
Analog channels	8-120
Digital PBX channels	8-120
T1/E1/ISDN PRI channels	24-240
ISDN BRI channels	4-60
VoIP channels	8-560
Maximum hard disk capacity	2 or 4 drives, RAID1, RAID5, RAID10
Standard archive drive	1 X Multi-Drive for Blu-ray Archiving (for Blu-ray media, 25GB)
Standard hard disk storage	2 X 1 TB fixed-mount, software RAID1
Optional storage	Removable hard drives, RDX archive drives

2.1.1. Front Panel
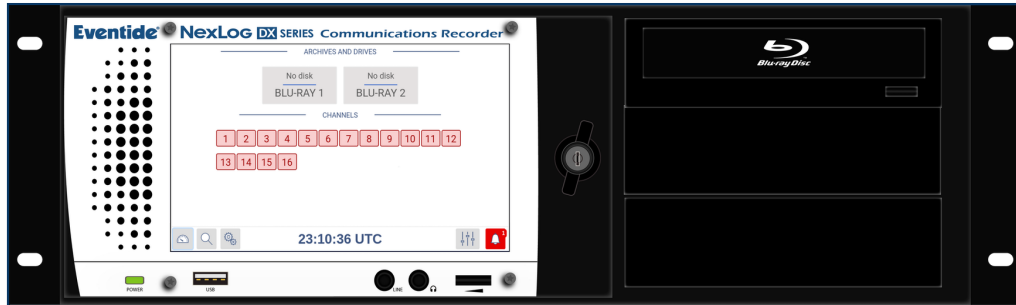
Fig. 2.1 **NexLog 740 DX-Series™ Recorder with Touch Screen (Door Closed)**

The touch screen display is on a locking door that protects the power switch and optional hot-swap RAID array.
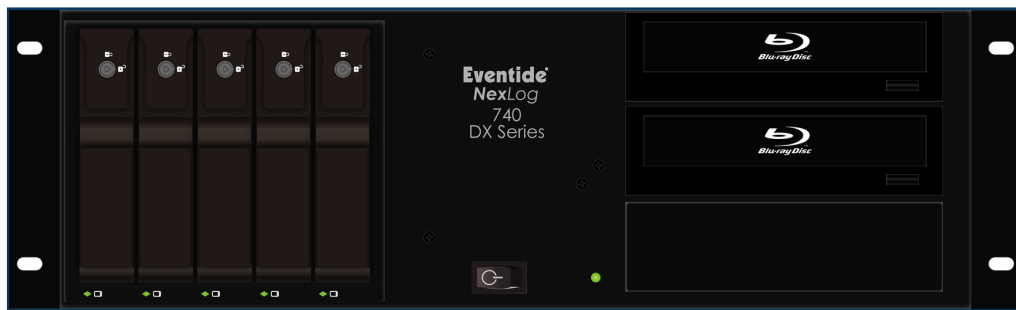
Fig. 2.2 **NexLog 740 DX-Series™ Recorder with Touch Screen (Door Open)**

The NexLog 740 DX-Series™ Recorder with the touch screen door open, showing the optional hot-swap RAID hard drives.

The standard NexLog 740 DX-Series™ Recorder configuration use a touch screen display for control and doesn't require a mouse or keyboard. All functions can be accessed from this interface. When necessary, an alphanumeric keyboard appears on the screen so that data such as channel names can be entered.

Systems without a touch screen display require 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.

The RAID disk array (up to 16 TB of storage) can be accessed and disks can be replaced while the recorder is operating by opening the monitor door (hot-swap hard drive option required). One Blu-Ray multi-drive is standard for archiving on the NexLog 740 DX-Series™ Recorder.

Audio monitoring/playback is accomplished with an integral amplifier/speaker unit (left) with headphone jack, line-level output, and volume control below the LCD screen.

Fig. 2.3 **Touch Screen (Close-Up)**

The door lock can be opened to access the recorder power switch (NexLog 740 DX-Series™ Recorder) and the hot-swap RAID disk array. Two keys are supplied.
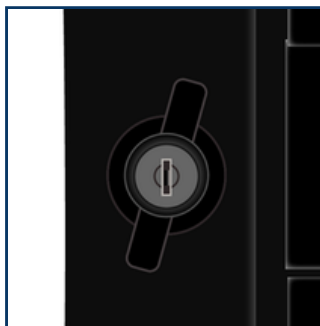
Fig. 2.4 **Front Panel Door Lock (Close-Up)**

Copyright © 2021, Eventide Inc.
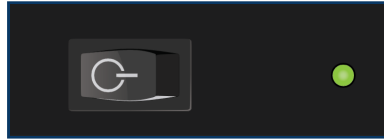
Fig. 2.5 **Power Switch (Close-Up)**

The NexLog 740 DX-Series™ Recorder power switch is behind the locked door. Note: Avoid using the switch to power down the unit. Use it to power up only.

Fig. 2.6 **Front Panel Audio Ports and Volume (Close-Up)**

The audio section provides a 1/8-inch headphone jack and a 1/8-inch constant level Line Out jack for convenient re-recording. The volume control adjusts speaker and headphone volume.

2.1.2. Rear Panel

Fig. 2.7 **Typical NexLog 740 DX-Series™ Recorder Rear Panel**

The rear panel of this NexLog 740 DX-Series™ Recorder shows (from left to right): Dual Hot-Swap power supplies, two RS-232 ports for serial ANI/ALI and SMDR feeds or serial time sync, connector panel for PS/2 mouse and keyboard, two USB 2.0 ports, HDMI, VGA, DVI, two Ethernet ports, four USB 3.0 ports, and audio in/out (unused- use the front audio connectors instead). On the right side of the

unit are spaces for five telephony boards, 2 (second from far left) through 6. Slot one is reserved for the optional hardware RAID controller. The sixth and seventh slots are reserved for PCI(e) add-on boards, one of which can be used for recording. You can see these clearly labeled below in a numbered illustration. Each board slot is labeled with its number , which is left to right when looking at them from behind the NexLog 740 DX-Series™ Recorder.

The redundant power supplies have an alarm that will sound when power is disconnected from either supply, whether from being unplugged or from a hardware failure. To acknowledge this alarm and silence it, press the small red button at the left-most edge of the back panel. It is labeled 7 in the diagram below.

The larger red switch, labeled 8, is the breaker reset. If someone plugs in an incompatible power supply, the breaker will trip, cutting all power to prevent electrical damage. After the power supply is replaced, press this switch to reset the breaker and restore power to the system.

Fig. 2.8 **Diagram of NexLog 740 DX-Series™ Recorder Rear Panel**

1 - Power Plug 1 (NEMA 5-15P)	14 - VGA Output
2 - Power Module 1	15 - DVI Output (hot-swappable)
3 - Power Plug 2 (NEMA 5-15P)	16 - Ethernet Device 1 (Eth0)
4 - Power Module 2	17 - USB 3.0 Ports
5 - Serial Port 1 1	18 - Ethernet Device 2 (Eth1)
6 - Serial Port 2 1	19 - USB 3.0 Ports
7 - Power Supply Alarm Reset	20 - Line In Jack (Unused)
8 - Breaker Reset	21 - Line Out Jack 2
9 - Fan Module 1	22 - Microphone Line In Jack (Unused)

10 - Fan Module 2	23 - RAID Controller (optional)
11 - Keyboard/Mouse Port	24 - Add-on Network Card (optional)
12 - USB 2.0 Ports	25 - Digital Recording Card (optional)
13 - HDMI Output (hot-swappable)	26 - Analog Recording Card (optional)

1 (1,2)

The serial ports are standard RS232 DB 9 ports.

2

Line Out Jack will provide alarm audio on left channel and playback on right channel.

2.1.3. Operating Limits

Table 2.3 **Operating Limits**

Parameter	Range or Limits
Voltage	100 - 240VAC
Frequency	50 - 60 Hz
Power (typical/ max)	NexLog 740 DX-Series™ Recorder 200W/350W, NexLog 840 DX-Series™ Recorder 200W/400W
Temperature	Operating +5C (41F) to 40C (104F)
Humidity	10% - 80% relative, non-condensing
Altitude	-2,000 to +2,000 feet operating (to 22,000 feet non-operating). If operated at high altitudes, take special care that airflow is unrestricted by dust or obstacles.

Parameter	Range or Limits
Vibration (Hard Disk Drives)	These units contain hard disk drive storage units and mechanical components that are sensitive to mechanical vibration. They are intended for operation in fixed locations. Typical vibration limits for the hard disk drives are as follows: Operating: .2 G, 5-300 Hz Non-Operating: 1 G, 5-300 Hz Note: There is a variant of the NexLog DX-Series™ available for high vibration environments, which adheres to MIL-STD-167-1A (25 Hz)
Shock (Hard Disk Drives)	Typical shock limits for the hard disk drives are as follows: Operating: 1 G, 11 ms half-sine Non-Operating: 40 G, 11 ms half-sine Note: There is a variant of the NexLog DX-Series™ available, that has passed MIL-S-901D medium weight, Grade "B shock testing.
Orientation	The archive drives are very sensitive to orientation. The recorder should always be mounted on a flat, non-sloping surface.

2.2. NexLog 840 DX-Series™ Recorder

The NexLog 840 DX-Series™ Recorder is available with and without a touch screen control interface.

Table 2.4 **Specification Summary**

	NexLog 840 DX-Series™ Recorder	NexLog 840 DX-Series™ Recorder (Blank Panel)
Product view		

Front Panel Access	1024 x 600 touch screen display (and/or use an external display via HDMI)	None (use external display attached via HDMI)
Front Panel I/O	USB 2.0 (type A), 1/8-inch line level output, 1/8-inch headphone output	
Remote software	Web browser based NexLog DX-Series™ Configuration Manager Web browser based MediaWorks DX™ playback client (Optional) Windows-based remote playback clients (Optional)	
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	5 1/2 inches (3 rack units)	
Depth	24 inches	
Power	350 watts	
Power supplies	Dual hot-swap	
Weight	50-80 pounds	
Analog channels	8-120	
Digital PBX channels	8-120	
T1/E1/ISDN PRI channels	24-240	
ISDN BRI channels	4-60	
VoIP channels	8-560	

Maximum hard disk capacity	2 or 4 drives, RAID1, RAID5, RAID10
Standard archive drive	1 X Multi-Drive for Blu-ray Archiving (for Blu-ray media, 25GB)
Standard hard disk storage	2 X 1 TB fixed-mount, software RAID1
Optional storage	Removable hard drives, RDX archive drives

2.2.1. Front Panel
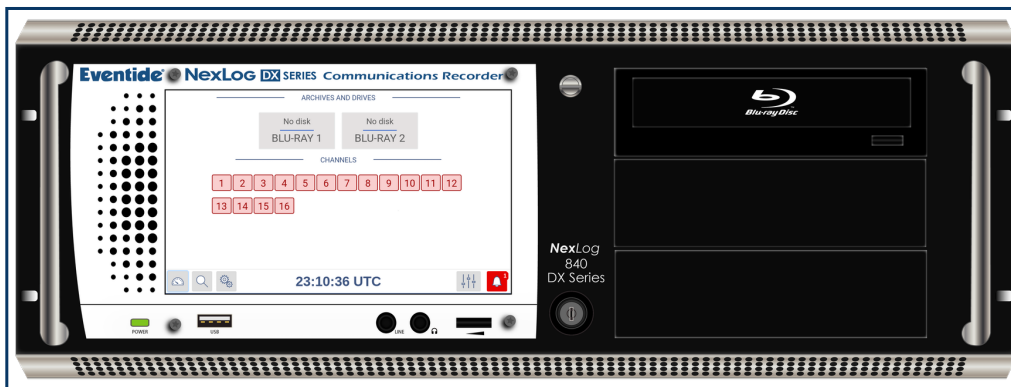
Fig. 2.9 **NexLog 840 DX-Series™ Recorder with Touch Screen**

The NexLog 840 DX-Series™ Recorder uses a horizontal hinge at the bottom of the unit. Loosening the thumb screw on the front will allow then entire front face to fold down for hard drive access.

The standard NexLog 840 DX-Series™ Recorder configuration use a touch screen display for control and doesn't require a mouse or keyboard. All functions can be accessed from this interface. When necessary, an alphanumeric keyboard appears on the screen so that data such as channel names can be entered.

Systems without a touch screen display require 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.

The RAID disk array (up to 16 TB of storage) can be accessed and disks can be replaced while the recorder is operating by opening the monitor door (hot-swap hard drive option required). One Blu-Ray multi-drive is standard for archiving on the NexLog 840 DX-Series™ Recorder.

Audio monitoring/playback is accomplished with an integral amplifier/speaker unit (left) with headphone jack, line-level output, and volume control below the LCD screen.

Fig. 2.10 **Touch Screen (Close-Up)**

The NexLog 840 DX-Series™ Recorder uses a keyed power switch on the front of the unit. Turn the key counter-clockwise to engage it. Holding the key in this position for more than 8 seconds, will forcefully power off the unit. Note: Avoid using the switch to power down the unit. Use it to power up only.

Fig. 2.11 **Front Panel Audio Ports and Volume (Close-Up)**

The audio section provides a 1/8-inch headphone jack and a 1/8-inch constant level Line Out jack for convenient re-recording. The volume control adjusts speaker and headphone volume.

2.2.2. Rear Panel
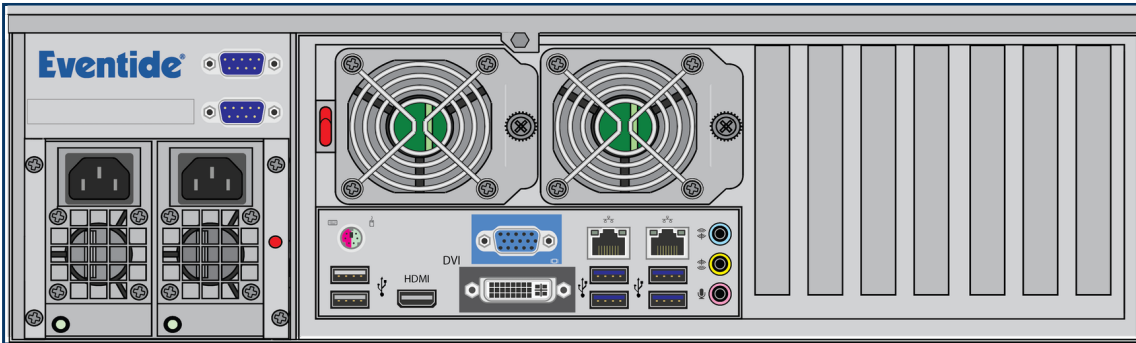
Fig. 2.12 **Typical NexLog 740 DX-Series™ Recorder Rear Panel**

The rear panel of this NexLog 740 DX-Series™ Recorder shows (from left to right): Dual Hot-Swap power supplies, two RS-232 ports for serial ANI/ALI and SMDR feeds or serial time sync, connector panel for PS/2 mouse and keyboard, two USB 2.0 ports, HDMI, VGA, DVI, two Ethernet ports, four USB 3.0 ports, and audio in/out (unused- use the front audio connectors instead). On the right side of the unit are spaces for five telephony boards, 2 (second from far left) through 6. Slot one is reserved for the optional hardware RAID controller. The sixth and seventh slots are reserved for PCI(e) add-on boards, one of which can be used for recording. You can see these clearly labeled below in a numbered illustration. Each board slot is labeled with its number , which is left to right when looking at them from behind the NexLog 740 DX-Series™ Recorder.

The redundant power supplies have an alarm that will sound when power is disconnected from either supply, whether from being unplugged or from a hardware failure. To acknowledge this alarm and silence it, press the small red button at the left-most edge of the back panel. It is labeled 7 in the diagram below.

The larger red switch, labeled 8, is the breaker reset. If someone plugs in an incompatible power supply, the breaker will trip, cutting all power to prevent electrical damage. After the power supply is replaced, press this switch to reset the breaker and restore power to the system.

1 - Power Module 1	14 - Serial Port 2 [1]
2 - Power Module 2	15 - RAID Controller (optional)
3 - Power Plug 1 (NEMA 5-15P)	16 - Microphone In Jack (unused)
4 - Power Plug 2 (NEMA 5-15P)	17 - Line In Jack (unused)
5 - Power Switch 1	18 - Line Audio Out [2]
6 - Power Status Light 1	19 - Audio Out To Front Panel [2]
7 - Power Switch 2	20 - Sub Audio Output (unused)
8 - Power Status Light 2	21 - Audio Pass Through To Front Panel
9 - Power Alarm Reset Button	22 - USB 3.1 Ports
10 - Add-On Network Card (optional)	23 - Ethernet Port 0
11 - Digital Recording Card (optional)	24 - Ethernet Port 1
12 - Analog Recording Card (optional)	25 - HDMI Output
13 - Serial Port 1 [1]	

1 (1,2)

   The serial ports are standard RS232 DB 9 ports.

2 (1,2)

   Line Out Jack will provide alarm audio on left channel and playback on right channel.

2.2.3. Operating Limits

Table 2.6 **Operating Limits**

Parameter	Range or Limits
Voltage	100 - 240VAC
Frequency	50 - 60 Hz
Power (typical/max)	NexLog 740 DX-Series™ Recorder 200W/350W, NexLog 840 DX-Series™ Recorder 200W/400W
Temperature	Operating +5C (41F) to 40C (104F)
Humidity	10% - 80% relative, non-condensing
Altitude	-2,000 to +2,000 feet operating (to 22,000 feet non-operating). If operated at high altitudes, take special care that airflow is unrestricted by dust or obstacles.
Vibration (Hard Disk Drives)	These units contain hard disk drive storage units and mechanical components that are sensitive to mechanical vibration. They are intended for operation in fixed locations. Typical vibration limits for the hard disk drives are as follows: Operating: .2 G, 5-300 Hz Non-Operating: 1 G, 5-300 Hz Note: There is a variant of the NexLog DX-Series™ available for high vibration environments, which adheres to MIL-STD-167-1A (25 Hz)
Shock (Hard Disk Drives)	Typical shock limits for the hard disk drives are as follows: Operating: 1 G, 11 ms half-sine Non-Operating: 40 G, 11 ms half-sine Note: There is a variant of the NexLog DX-Series™ available, that has passed MIL-S-901D medium weight, Grade "B shock testing.
Orientation	The archive drives are very sensitive to orientation. The recorder 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 DX-Series™ 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 DX-Series™ 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.

- Look at the menu buttons on the bottom left of the display to view the main screens for the Front Panel. The available screens are as follows:

3.2.1. Info Screen

- View channel status

- Listen to real time activity on channels (Live Monitor)

- View and manage archiving status

3.2.2. Replay Screen

- Research and play back recordings stored locally and on archives

- Export recordings to removable media.

3.2.3. Setup Screen

- Configure the recorder.

3.2.4. Alarms Screen

- Access active alarms on the recorder

3.2.5. Login Screen

- This option is only visible and available under certain configurations. This will be explained later during System Security Settings.

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

Important! 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.

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 DX-Series™ 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 Front Panel, 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 3.3.5: 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. Other Considerations

NexLog 740 DX-Series™ Recorder: The recorder is shipped with two keys for locking and unlocking the front door of the recorder. One key should be kept in a safe place as a backup spare. You should consider preventing casual access to the other key as well. The switch behind the front panel should be used to power up the recorder only and not be used to power down the recorder unless absolutely necessary. The logger should be shut off using the SETUP/Power Off option. Otherwise, data corruption could occur. If it is necessary to use the switch to shut down the recorder, hold it for one second and release. **Do *not* continue holding it until the recorder shuts down**.

NexLog 840 DX-Series™ Recorder: The recorder is shipped with two keys for the power key-switch on the front panel of the recorder. One key should be kept in a safe place as a backup spare. You should consider preventing casual access to the other key as well. The power key-switch should be used to power up the recorder only and not be used to power down the recorder unless absolutely necessary. The logger should be shut off using the SETUP/Power Off option. Otherwise, data corruption could occur. If it is necessary to use the key-switch to shut down the recorder, insert the key, turn it for one second, and release. **Do *not* keep the key turned until the recorder shuts down**.

3.3.5. Connecting AC Power

The recorders use "universal" power supplies. All NexLog DX-Series™ 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 DX-Series™ Recorders from all main power. Remove all power cords before servicing the unit.

3.3.6. 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 of this document for configuration information including Date and Time settings.

3.3.7. 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 B: 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.

3.3.7.1. 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 B: 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 B: 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.

3.3.8. 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 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.

3.3.9. 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 DX-Series™ 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.

3.3.10. Connecting a Keyboard

A keyboard can be connected to a recorder to allow easier and faster data entry and interaction than is permitted by the recorder's optional front panel interface. This can be useful for performing system administration tasks from the front panel and for diagnostic work.

> **ⓘ Note**
>
> The same configuration capabilities that are available on the Front Panel can be accessed via a web browser from a PC, using the browser-based NexLog DX-Series™ Configuration Manager. Under most circumstances this will allow for a quicker setup procedure.

The following methods are available for connecting a keyboard to the recorder:

- Connect a USB keyboard to any USB connector on the recorder. This may be done while the recorder is running and does not require a shutdown and restart of the recorder.

- Connect a PS/2 keyboard to the PS/2 connector on the recorder back panel (purple on the NexLog 740 DX-Series™ Recorder only). This should be done while the recorder is off, so if the recorder is running, it requires a shutdown of the recorder before it is installed.

3.3.11. Connecting Headphones

Optionally, connect headphones to the 1/8-inch jack labeled "Headphone" on the front panel. Suitable headphones are available from Eventide (part# 324200). Most headphones with an appropriate plug can be used and adjusted to a comfortable level with the front panel volume control.

3.3.12. Connecting Line-Level Equipment

A line-level audio output is available at the 1/8-inch jack labeled "Line Out" on the front panel, if you wish to connect an external recorder such as a Philips Cassette recorder to the recorder for excerpting calls to cassette. Most standard cassette units with record capability can derive an appropriate signal level from this jack.

4. Recorder Operation

4.1. Starting Up and Shutting Down

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

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 Front Panel:

- 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 DX-Series™ Recorders are designed as standalone products, and it is not necessary to install the clients to use the product.

MediaWorks DX™ 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 DX™ 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 Front Panel 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 99.75% blank.

6. The Front Panel User Interface

This page was intentionally left 99.75% blank.

7. Configuration Manager

> **ⓘ 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

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

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

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.

- **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

- DX 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.

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 Analog Channels

The maximum number of physical analog recording sources allowed.

7.1.3.1.3. Num Digital Channels

The maximum number of physical analog recording sources allowed.

7.1.3.1.4. Num MediaWorks Connections

The maximum number of simultaneous MediaWorks DX™ client playback connections allowed.

7.1.3.1.5. Num MediaAgent Connections

The maximum number of simultaneous MediaAgent DX™ client playback connections allowed.

7.1.3.1.6. Num Archive Drives

The maximum number of archive destinations allowed. This includes optical, portable, and network destinations.

7.1.3.1.7. 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.

7.1.3.1.8. Model

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

7.1.3.2. Software Update Subscription

NexLog DX-Series™ Recorder Software is licensed on a subscription basis via the DX Software Update Subscription (DXSUS) 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.

To be clear: if your DX 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.

7.1.3.3. Hardware Warranty License

The expiration date of your NexLog DX-Series™ hardware's warranty will be listed in this license key. This is for the factory warranty only. Eventide Dealers may offer an extended warranty for your hardware directly. Consult your Eventide 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. 7.4 **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.

· 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.

Copyright © 2021, Eventide Inc.

- **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.

7.1.5. Translations

NexLog DX-Series™ supports using MediaWorks DX™ 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.
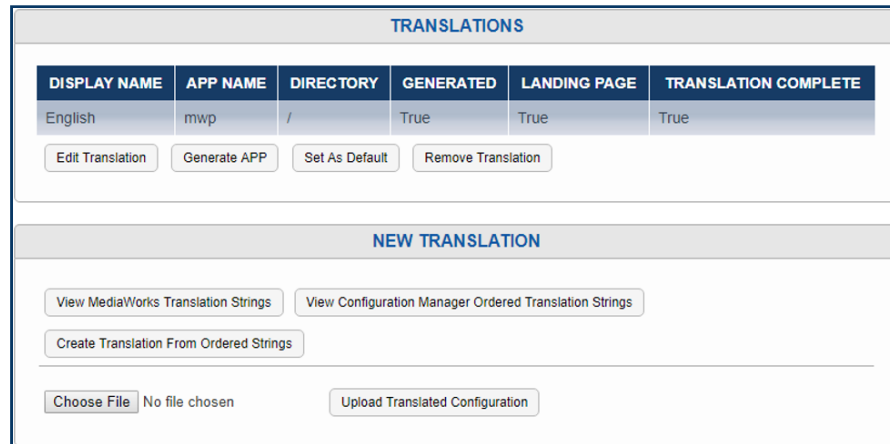
Fig. 7.5 **Translations**

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 DX™ and one for elements of MediaWorks DX™ that draw on elements from Configuration Manager, such as Evaluations and Alerts. These are distinguished by App Name: mwp for MediaWorks DX™ 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".
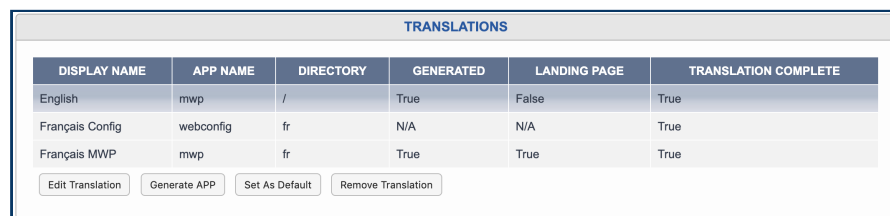
Fig. 7.6 **Translations Configured**

Set as Default changes which language the Welcome page will use as the main link to MediaWorks DX™. By default, this is English, and other language choices will appear below the MediaWorks DX™ icon, listed by Display Name. On a system configured as above, however, the icon would link to the *http://recorder-IP/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 DX™ 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.
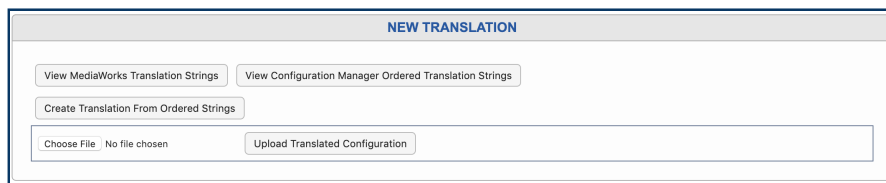
Fig. 7.7 **New Translations**

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.
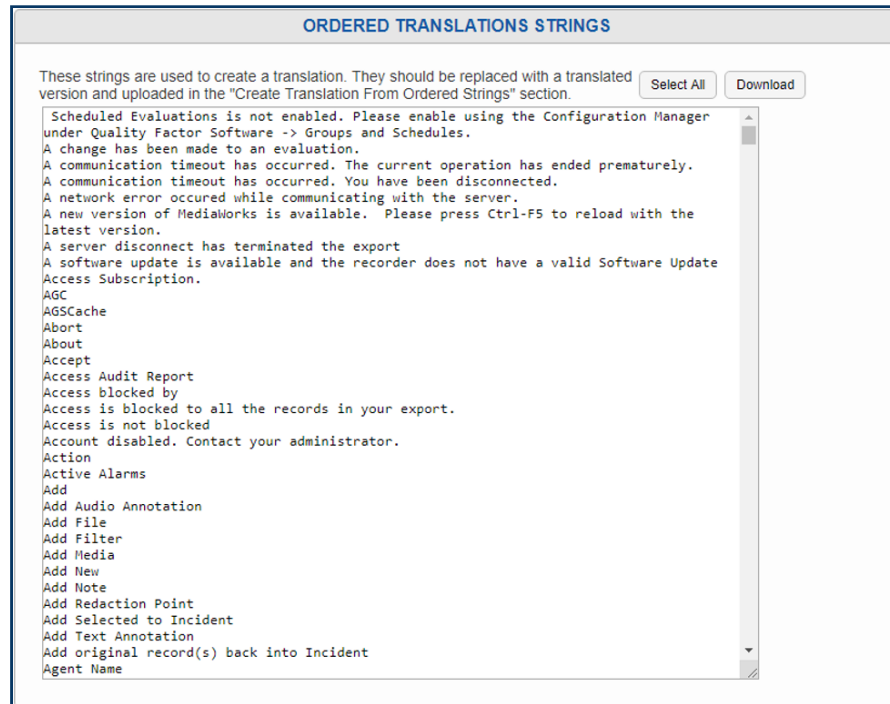
Fig. 7.8 **Ordered Translations Strings Page**

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:

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 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 DX™.

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 DX™ at the directory configured in the Translation settings.

The **Generate App** step is not required for WebConfig 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 DX™ 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 DX™ translation, select the translation and
click Generate APP to update it to the latest text.
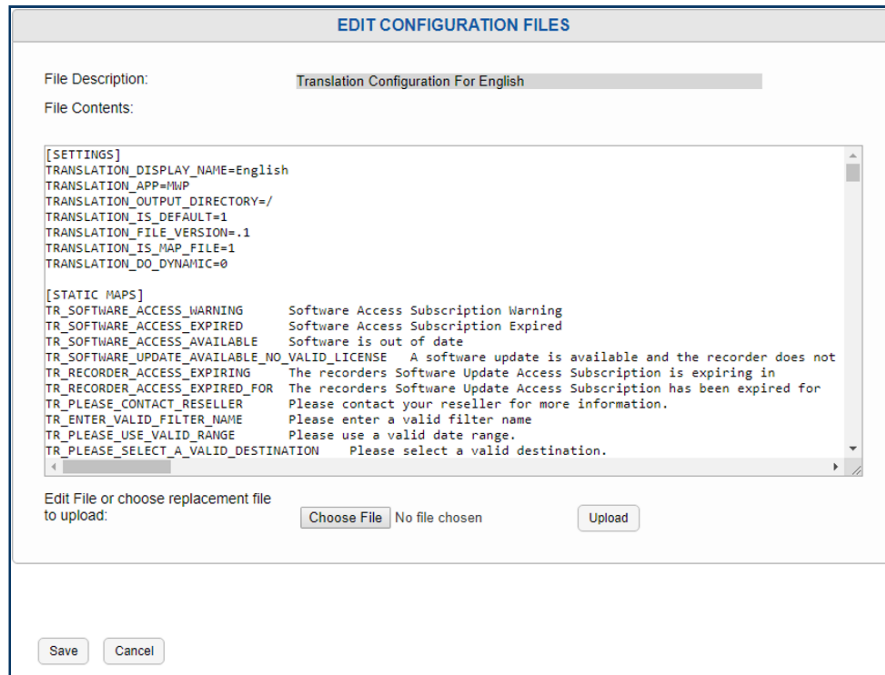
Fig. 7.9 **Translations Edit Page**

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 DX™ 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 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".

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.

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. 7.10 **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 DX-Series™ 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. 7.11 **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
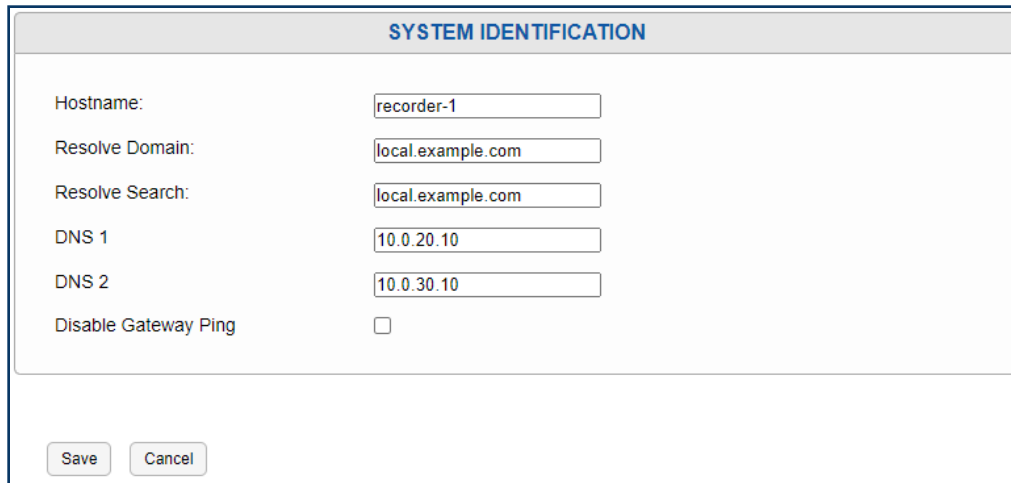
This section allows a user to remotely power off or reboot a recorder. When rebooting a recorder, it's recommended that the recorder be physically available nearby in case any issues occur.

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. Each sub-section is listed below.

7.2.1. System Identification

Fig. 7.12 **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 Alerts and Logs: 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. 7.13 **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 DX-Series™ 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 DX-Series™ 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 DX-Series™ 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 DX-Series™ 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 DX™ 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 DX-Series™.

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. 7.14 **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.

> **ℹ️ 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

7.2.2.8. Dual NICs with Bonding Operation

When configured with NIC bonding, the dual network interface devices provide failover operation. Because they share the same IP address, if one of the devices or its connection should fail, the other device will maintain the network connection. Each bonded pair can only be made from two physical NICs, but there can be two separate bonded NIC pairs per system.

To configure two network devices with NIC bonding, change the Type to Bind on each device, then save. The Bind setting is only available on devices already configured for DHCP or Static.

Once you have bound two devices together, they will be presented as a single device, set to DHCP (and can be configured for Static or SPAN), with an additional menu for Bond Type. This will let you configure the kind of device bonding used.

Note: After you have configured the network interface devices for NIC bonding operation, if you change them back to separate operation, you will then have to reboot the recorder for the changes to take effect.

There are three types of NIC Binding available. Be sure to select the type that matches the requirements of your network's configuration.

- **0 (balance-rr):** Round-robin policy: Transmit packets in sequential order from the first available slave through the last. This mode provides load balancing and fault tolerance.

- **1 (active-backup):** Active-backup policy: Only one slave in the bond is active. A different slave becomes active if, and only if, the active slave fails. The bond's MAC address is externally visible on only one port (network adapter) to avoid confusing the switch. This mode provides fault tolerance.

- **2 (balance-xor):** Transmit based on (source MAC address XOR'ed with destination MAC address) (modulo slave count). This selects the same slave for each destination MAC address. This mode provides load balancing and fault tolerance.

🔥 *New in version 2021.1.*

- **4 (802.3ad):** IEEE 802.3ad Dynamic link aggregation. Creates an aggregation group that shares the same speed and duplex settings. Utilizes all adapters in the active aggregator according to the 802.3ad specification. This option requires that the attached peer also has 802.3ad configured.

7.2.3. VNC Settings
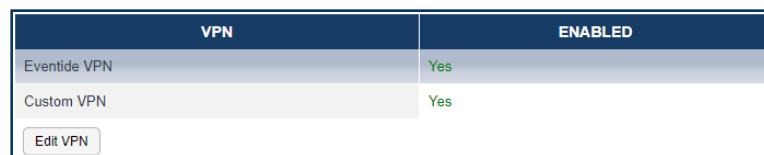
Virtual Network Computing (VNC) is a standard protocol widely used for accessing PC Desktops remotely over the network. If enabled, you will be able to connect to the recorder over VNC using any standard VNC Client such as RealVNC or TightVNC. When you connect to the Recorder via VNC, you will

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 DX-Series™ VNC access is provided over port **5900**.

7.2.4. VPN Settings

NexLog DX-Series™ 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.

VPN	ENABLED
Eventide VPN	Yes
Custom VPN	Yes
Edit VPN	

Fig. 7.15 **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 DX-Series™ 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. 7.16 **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

SNMP stands for "Simple Network Management Protocol" and 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 DX-Series™ provides a simple subset of SNMP Functionality (with Linux and SQL notifications) which can be configured here. 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.

7.2.6. NexLog Access Bridge

NexLog DX-Series™ Recorders can be bridged together to integrate multiple recorders for unified user administration and client access. NexLog Access Bridge (NAB) allows for sync of users (including user groups and permissions), and access to call records across multiple recorders from one MediaWorks Plus session.

For example, a site may have two NexLog DX-Series™ Recorders, one a dedicated screen recorder, and the other recording related phone calls, and both sets of recordings can be browsed and played back at the same time, from the same MediaWorks Plus window. The user accounts for both systems can be administered on the first system and synchronized in real time to the other. This section covers the basics about NAB but for comprehensive information about NexLog Access Bridge and how it works with MediaWorks Plus and User Configuration Sync, please consult the **Eventide NexLog Access Bridge Manual** (part number 141307-01.)

NexLog Access Bridge is configured here:

Fig. 7.17 **NexLog Access Bridge**

Click Add Bridge to configure a new Access Bridge. Enter the serial number and address of the source NexLog DX-Series™ Recorder you want to access from the recorder you are currently configuring (the primary). Then save the configuration. You can modify and delete configured Access Bridges here as well.

Fig. 7.18 **New NexLog Access Bridge**

For NexLog Access Bridge to work, the systems configured must be able to reach each other over the network. The required open ports are 2022, and 5432. Additionally, it is recommended that Session Timeouts and Users be configured to be the same across all Access Bridge systems, whereas Channel names and Recorder Names should ideally be unique across all systems.

There are four options for each NAB:

7.2.6.1. Com Link

The Com Link option allows Resource Groups for Recording to work across NAB. The primary use for this is when there is a NexLog DX-Series™ dedicated to screen recording, which records only when phone calls come in, which are recorded on another NexLog DX-Series™. With this option enabled, a resource group on this recorder can be configured to link the two channels across systems.

7.2.6.2. Enable Redundant NAB Base

By default, NAB User Management Sync only propagates configuration information relevant to each Source recorder; information about a Resource Group that only involves Recorder A and B will not be synced to Recorder C. Enabling this option will instead sync all information to this base. This includes:

   · All Users, their settings, user group memberships and resource permissions.

   · All User Groups

   · All Resource Permission and Search Groups

   · And finally, all NAB sources

This last step means if the Primary system in a current NAB set up has a hardware failure, one can switch over to the Redundant NAB Base, enable Primary status and then deal with addressing the problem with the now- previous Primary system without interruption to client access nor configuration. NexLog Access Bridge requires a NAB License on the primary recorder and to use it with MediaWorks Plus, a MediaWorks Plus license must be available for each concurrent source recorder user.

7.2.6.3. Enable SSL

With this enabled, NAB will work over HTTPS/TLS connections.

7.2.6.4. Enable Host Authentication

Host Authentication allows for better performance with more concurrent MediaWorks Plus users. This setting should be considered when the system has more than 32 simultaneously connected users. In order to enable the feature you must enable "Exempt NexLog Access Bridge Hosts from Database Authentication" on the source recorders System Security page and enable "Enable Host Authentication" on the base recorder for the source recorder on the NAB configuration page. The feature works by enabling a large connection pool of anonymous database users. Database access permissions will be controlled on the base recorder instead of by the individual source recorder.

NexLog Access Bridge requires a NAB License on the primary recorder and to use it with MediaWorks Plus, a MediaWorks Plus license must be available for each concurrent source recorder user.

For more information on how to use NexLog Access Bridge in MediaWorks Plus, please consult the MediaWorks Plus manual for more information.

For more information about how to use NexLog Access Bridge to sync Users and Permissions, see the Users and Security chapter below.

7.2.6.5. NAB Connection Toolbar in Configuration Manager

There is a NAB Connection Manager at the top of pages with NAB sync features (Resource Groups, Users, User Groups). This tool allows you see how many NAB sources you are logged into at any given time, and if expanded will show the status of each connection.

When expanded, the X beside each connected NAB source can be clicked to disconnect that source. If an error occurred while trying to connect, that error will be shown here.

Fig. 7.19 **NexLog Access Bridge Connection Manager**

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 DX-Series™ 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. 7.20 **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.

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.
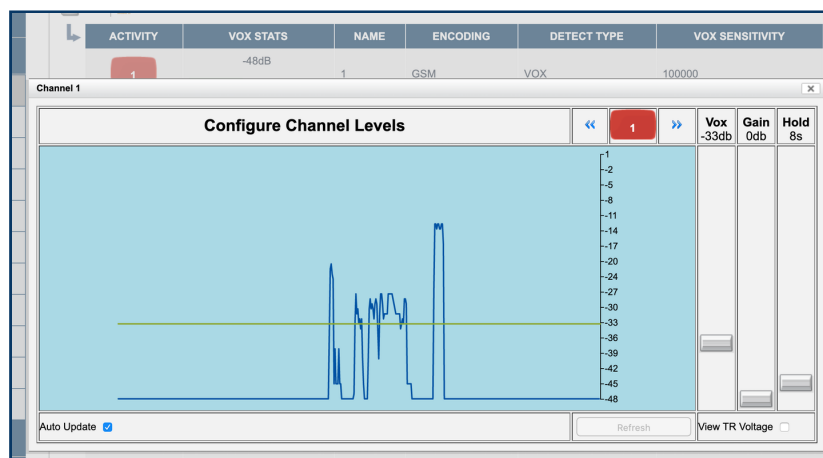
Fig. 7.21 **Recording Interfaces Detail Level Graph**

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. 7.22 **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 Alias Banks.

ALIAS BANK	CHANNELS	SOURCE FIELD	DEST FIELD
Scenario 6B	*	CALLTYPE	CALLTYPE
Scenario 6A	*	CALLTYPE	CALLTYPE
Scenario 7A	7	DTMF	CHANNELNAME
Scenario 7B	7	DTMF	CHANNELNAME
Scenario 1	1	DTMF	DTMF_ALIAS
Scenario 2	2	DTMF	DTMF_ALIAS
Scenario 3	3	DTMF	DTMF
Scenario 4	4	DTMF	DTMF
Scenario 5	5	DTMF	CHANNELNAME

Fig. 7.23 **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. T1/E1 Board Active and Passive Boards

These boards come in Single Port and Dual Port versions for recording one or two T1 or E1 Trunks. The Dual Port versions simply provide the same configuration options separately for each Port. For each port the options are as follows:

Port Type: Whether the Trunk is a T1 or E1 (must be the same on both ports on a dual port board)

Protocol: The Protocol used on the T1/E1. Options are None (Recording is VOX Only), ISDN, or CAS/RBS

Protocol Variants:

- **Line Coding**: Whether the Line coding on the T1/E1 is AMI, B8Zs or HDB3

- **Framing Format**: Whether the Framing format is SF, ESF, G704, or CRC4

  - **Interface Side**: TE or NT. For an active board, this needs to be set to the opposite of the setting on the equipment terminating the other end of the T1/E1. For passive boards this can normally be left at the default setting, which is TE.

Passive T1/E1 Boards are used for tapping between two T1/E1 endpoints, both of which terminate their end of the T1/E1 circuit, with the recorder passively listening in between by use of a 'T-adaptor' wiring tap. These are typically used for tapping and recording a T1/E1 circuit, for example, between a PBX and the telephone company, where the recorder is not involved in the communications and just listening in the middle.

With an active T1/E1 the board will terminate one end of the T1/E1 connection. If the board is configured for ISDN call control, the recorder will also answer calls placed over the T1/E1 link and record all the audio sent to it during the call. The recorder will never place a call to the remote end over the T1/E1.

7.3.1.8. Eventide RTP / VoIP Virtual Boards

See Recording VoIP or RoIP Calls.

7.3.1.9. 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.

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. 7.24 **Edit Analog Channel**

7.3.1.9.1. 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 7.3.1.9.6.1 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

7.3.1.9.2. 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 DX™.

- 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 DX-Series™ 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.

  VOX Threshold

- **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. 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.

7.3.1.9.3. 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).

7.3.1.9.4. 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 DX™ when playing back the call. NexLog DX-Series™ 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.

7.3.1.9.5. 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 set, alert #3002 ("Channel was inactive for more than X seconds") is issued if there is no activity on the channel 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.

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 call 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.

7.3.1.9.6. 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.

7.3.1.9.6.1. 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.

7.3.1.10. 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 DX-Series™ 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 DX™ 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 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'

User 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 DX-Series™ 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 that only 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.
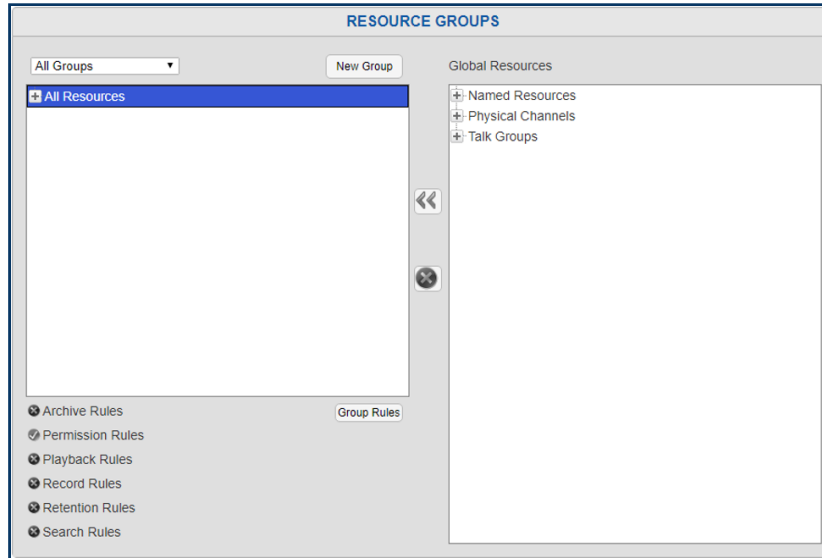
Fig. 7.25 **Resource Groups**

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.
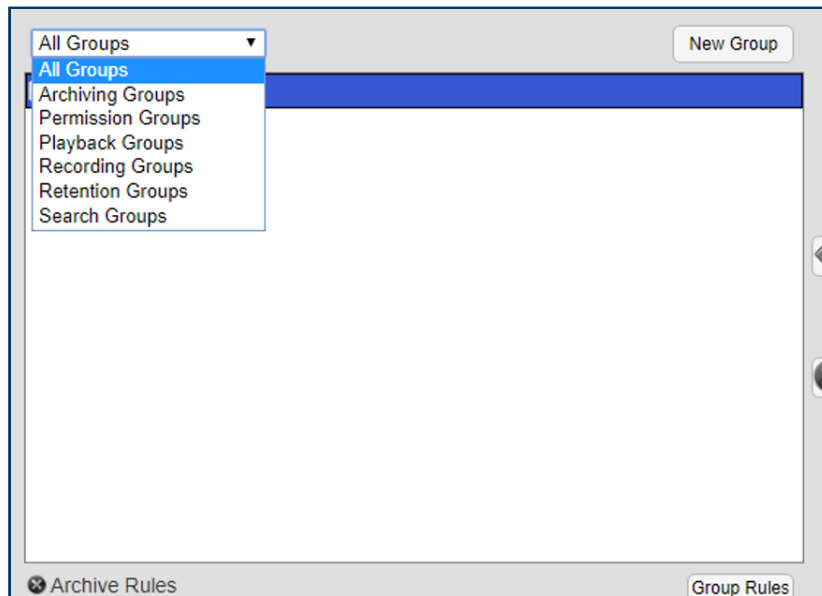
Fig. 7.26 **Resource Group Rules Menu**

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:
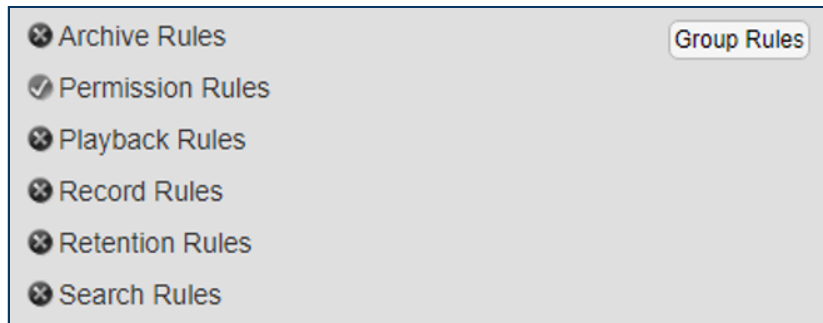
Fig. 7.27 **Resource Group Rules Status**

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.
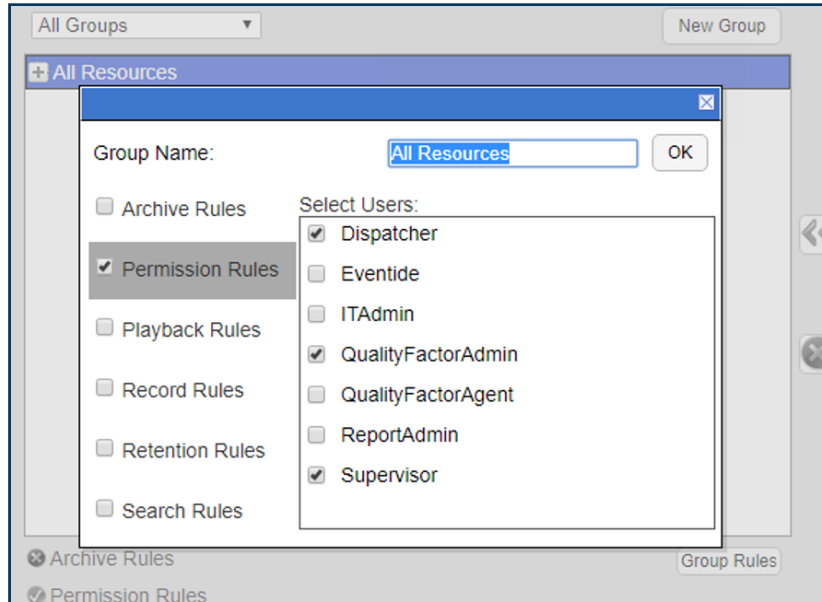
Fig. 7.28 **Resource Group Edit: Permission Group View**

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.
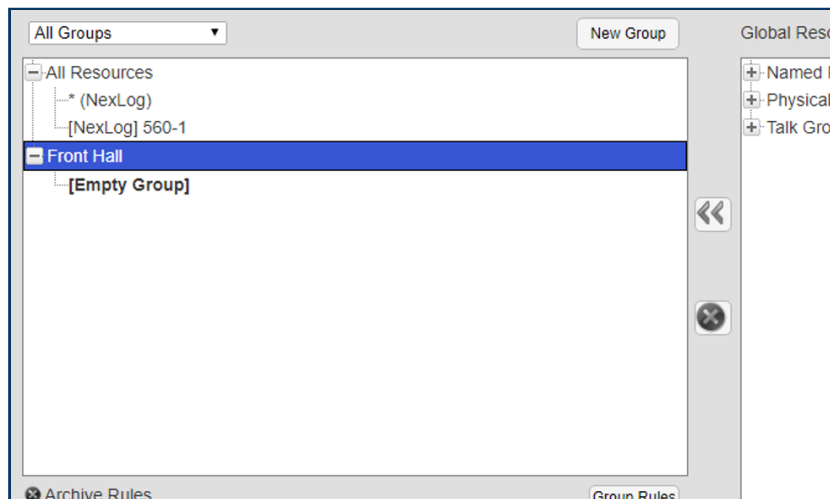
Fig. 7.29 **Resource Group: Empty Group**

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.
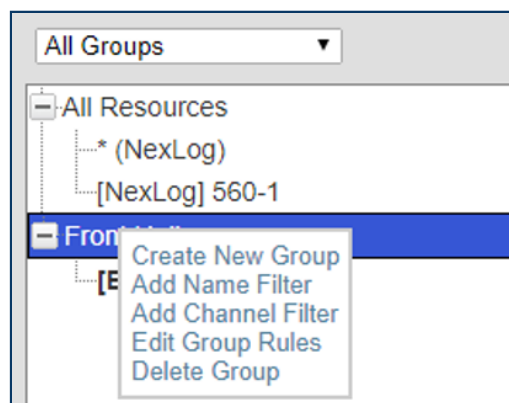
Fig. 7.30 **Resource Groups: Right Mouse Button Menu**

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 integrates 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. 7.31 **User Group Edit**

Following the behavior of previous NexLog DX-Series™ 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.

7.3.4.7. Resource Groups and NexLog Access Bridge

When NexLog Access Bridge is configured, Search Filter Groups can include resources and name filters that bridge across multiple recorders. When you load the Resource Groups page, at the top there will be a NAB Connection row that allows you to enter a username and password to login to each NAB source with. This will prompt to reload the page after it succeeds, to update the list of available resources.
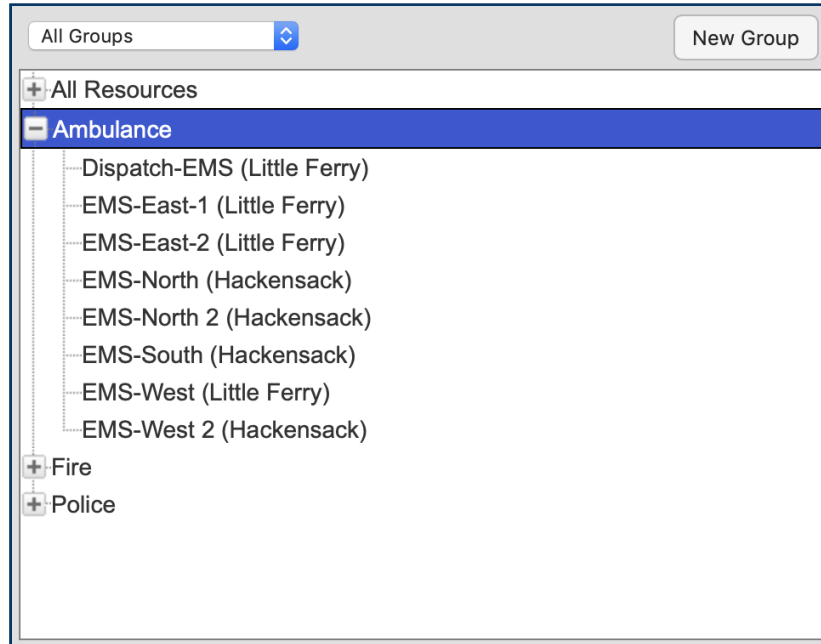
Fig. 7.32 **Resource Group Including Resources from Multiple Recorders**

Once logged in, the resources list in the right column will include all available resource names and physical channel ids from these sources. With named resources, if multiple recorders have resources with the same name, you can add all of them at once, or expand the entry to select a specific resource by NexLog DX-Series™ system name.

For example, in the figure above there is one NAB source configured for this recorder: the host system is named NexLog DX-Series™ 44 and the NAB is NexLog DX-Series™ 101. The resource names listed inside the Radio and Screen group tell you which recorder they point to by including the name in parenthesis at the end. In the Global Resource list, you can see that resource names that are present on both are displayed with a tree to expand and when expanded you can select a single entry or both and add them to the selected Resource Group.

NexLog Access Bridge also allows for syncing permission groups. While logged in, any permission group involving channels from remote recorders will be synced to those recorders. For efficiency, groups are only synced to systems that have relevant channels; if group X gives permissions to channels on the host and one source, but not a second source, it is synced from the host to the first source and not the second. If you have made changes while disconnected and want to sync those changes, log in with the NAB Connection tool bar and click the Sync button, which will sync all Permission Groups to all connected NAB sources.

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 900-8*80-0555* 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 DX-Series™ 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 DX™, 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. 7.33 **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 DX™/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 DX™ 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 DX™. 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:
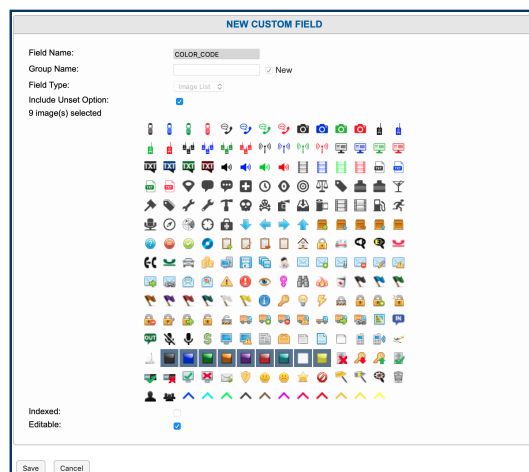
Fig. 7.34 **Custom Image List Color_Code Example**

These images can then be assigned to call records in MediaWorks DX™. 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:

List

Fig. 7.35 **Color_Code Example in MediaWorks DX™**

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 DX™. It is important to make

List, Image List and Checkbox fields editable, if they are going to be
set by end users in MediaWorks DX™.

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 DX™ 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 DX™, 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.
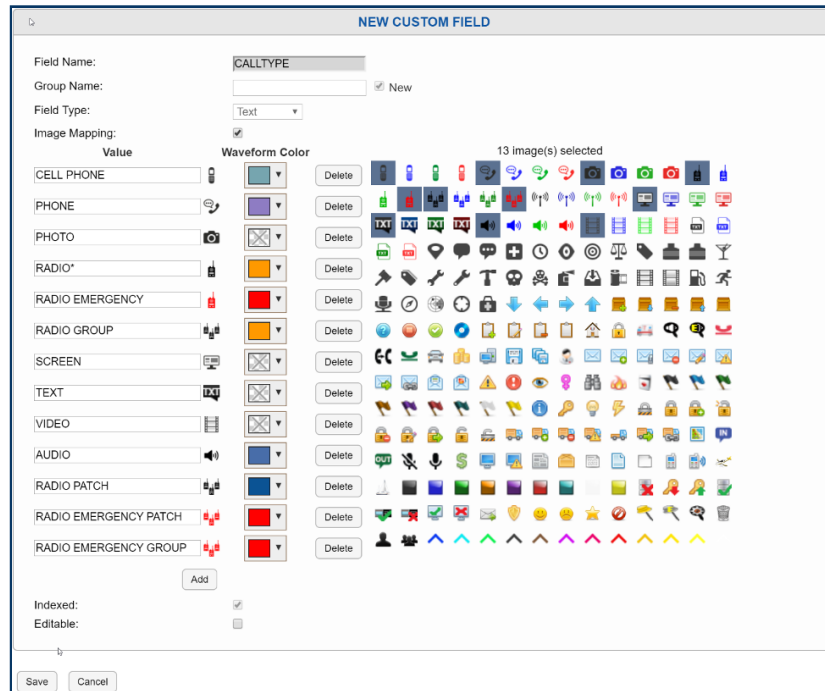
Fig. 7.36 **Calltype Field Configuration**

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.

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.

INTEGRATION NAME	STATUS
Generic ANI/ALI	Unlicensed
Generic CAD API	Enabled
Generic SMDR	Unlicensed
Intrado CDR Proxy	Unlicensed
Motorola Vesta i3 SMS Logger	Unlicensed
RapidSOS Location Integration	Unlicensed
Shutdown Recorder if CTS is Low on First Serial Port	Unlicensed
Solacom i3 Event Logger	Unlicensed
Spillman CAD Integration	Unlicensed
Storage Usage Alarm Integration	Unlicensed
Sungard CAD Integration	Unlicensed
Tait DMR REST Integration	Unlicensed
TopSky Integration	Unlicensed
Tritech CAD Integration	Unlicensed
Whitelist / Blacklist Call Deletion	Unlicensed
Word Factor Speech To Text	Unlicensed

Fig. 7.37 **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.

7.3.9. Encryption At Rest

This page allows you to configure your recorder to encrypt the recordings stored on its internal RAID hard disk drives for increased security. By default, Encryption at Rest is disabled. Enabling this feature requires a license key activation by Eventide (Eventide P/N: 271148).

If Encryption at Rest is not configured, disabled, or unlicensed, all call audio will be recorded on the NexLog DX-Series™'s internal RAID in a proprietary, but unencrypted, format. The proprietary nature of the audio format makes the data difficult, but not impossible, to play back with off the shelf utilities.

If Encryption at Rest is enabled, all call audio will be recorded and encrypted using a 256-bit AES key. This enhances security by making it impossible to play back audio without the original key. The AES keys are stored in the recorder on internal NAND flash memory, using a Key Encrypting Key (KEK). This allows the NexLog DX-Series™ to decrypt the calls for playback. Since the keys are stored on separate media, they remain safe in the event that someone gains physical access to your RAID hard disk

drives. Physical access can typically be gained when a failed hard drive is replaced and disposed of. When this occurs, Encryption at Rest will securely protect your recordings even if they are able to be recovered from the failed drive.

Encryption at rest can be enabled for any audio channels on a licensed NexLog DX-Series™ recorder. When encryption is enabled on a channel, the unencrypted audio is stored in memory where your active AES key is used to encrypt the audio file before it ever touches the internal RAID.

> **ⓘ Note**
>
> Screen Recording calls will not be encrypted, even if the channel has been configured for encryption.

> **ⓘ Note**
>
> Virtual Machines do not have internal NAND flash memory and will save the AES key to the main storage.

AES KEY	ACTIVE FOR ENCRYPTING
AB005DF053D552E301B5BE09059A407FA0F3E2CA8450B2D2A661BD673B8D70D2	True
E99900FFCAA026DAAC3088A5D7FA288337FE92A81F1459A9544BE46613B1D165	False
32E7A266E4701E6DC72B89B5A2E7B3F3DA4F82834BBBC36CF88DBE8F7E3F0A83	False
ADCF2411735F16D09D9A5134884D90D0A8C43EBF6FE89FB09B22A1FDED1D3220	False

Add Key   Activate Key   Delete Key

Fig. 7.38 **Encryption At Rest Configuration**

7.3.9.1. Active vs Inactive AES Keys

In the figure above, you can see an example of four AES Keys. The top key is in an Active state (True). This means that it is the AES key that is currently encrypting the configured channels. For better security, keys should be changed or rotated regularly. Changing the active key ensures encryption integrity by reducing the likelihood that someone with malicious intent can gain access to all of your recordings. If only one key were to become compromised, only the recordings captured while that key was in effect can be decrypted.

When you change or rotate keys, you will simply need to select the key from the list and click *Activate Key*. In doing so, the previously used key will become Inactive (False). Inactive keys are only used for decrypting recordings for playback or export (see Encrypted Playback and Exporting Encrypted Recordings). This means that if you intend to access recordings that were encrypted using a key that isn't the currently Active key, it will need to remain on the system in an Inactive state.

> **ⓘ Important**
>
> Deleting a key is irreversible and only advised if no recordings were encrypted using the key you intend to delete. If a key is mistakenly deleted and you have it stored in an alternate location, adding the key back into the system, as Inactive, will allow you to resume playback. Caution should be taken in verifying that the key was not used on recordings currently on the NexLog DX-Series™ recorder, or recordings stored in an Archive backup (see Archiving Encrypted Recordings).

> **ⓘ Note**
>
> Eventide is not able to recover recordings encrypted with a missing or deleted AES key.

7.3.9.2. Adding an AES Key

The NexLog DX-Series™ Administrator should generate a secure encryption key using a high quality source of entropy. For enhanced security the NexLog DX-Series™ recorder does not generate or provide you with original AES keys. If you do not have your own key generation utility, you can perform a websearch for "Random Byte Generator". The website www.random.org/bytes provides a generator that uses atmospheric noise for its source of entropy.

> **ⓘ Note**
>
> Eventide is not affiliated with Random.org and cannot warrant use of, or the availability and reliability of their operations.

> **❗ Important**
>
> Once you have generated a secure 32 byte AES key, it is recommended that you store it in a safe or another secure location. You should also maintain your own external record of key changes, rotations, and deletions with dates and timestamps. Configuration Backups will contain the KEK version of your encryption keys, but this should not be your only method of key backup. Eventide is not able to recover encrypted recordings if the AES key is not available.

AES Key: (32 Hex Bytes) [   ]
Make this Key Active ☐

[Add]   [Cancel]

Fig. 7.39 **Adding an Encryption Key**

1. click *Add Key* at the bottom of the Encryption at Rest page.

2. Then paste your AES encryption key. Your encryption key should be a 256-bit AES key represented using 32 Hex Bytes, or 64 hexadecimal characters (A-F,0-9). It should not contain spaces or symbols. Keys are not case-sensitive.

3. If this will be the key used to actively encrypt recordings, click the active checkbox. Otherwise, the key will be added in an Inactive state.

4. Click *Add* at the bottom of the page.

Once you add an AES key, the recorder will encrypt your AES key using a Key Encryption Key and store then it on internal NAND flash memory. This will protect your keys in the event of a total hard drive failure. A backup copy should still be maintained.

7.3.9.3. Enabling Encryption at Rest

Once your AES key has been added to the recorder, click the **Enable** checkbox and enter the channels you would like to be encrypted. The channel field supports multiple channels using comma separation and ranges. The example in **Figure 67** shows that channels 5,6,7,9, and 23 through 48 will be encrypted before written to the hard drive. After your channels have been entered, press *Submit Global Settings.*

Future recordings will now be stored on the internal RAID and archived in an encrypted format. Encryption at Rest will not encrypt recordings that have already been created and stored on the RAID or on pre-existing archives.

7.3.9.4. Encrypted Playback

Once your recordings are encrypted, there will be no noticeable changes in the way you playback recordings. The recorder will automatically decrypt them before streaming them to MediaWorks DX™.

In order for the recorder to decrypt the recordings, the encryption key must remain on the system. Deleting a key that was previously used will render any recordings that were encrypted with it unplayable. As shown in the figure below, if the AES key used to encrypt a played recording is not available, the system will display a "!" indicating that the recording is inaccessible. Hover the mouse over the exclamation point to confirm the reason.

	Source Name	Channel Name	Start Time	▲ Duration	Encrypted On Disk
!	NexLog DX-Series	Back Hallway	2020-03-18 07:25:59 -04:00	00:09	Yes
!	NexLog DX-Series	Back Hallway	2020-03-18 07:26:17 -04:00	00:07	Yes

Fig. 7.40 **Encrypted Recording Unavailable**

	Source Name	Channel Name	Start Time	▲ Duration	Encrypted On Disk
!	NexLog DX-Series	Back Hallway	2020-03-18 07:25:59 -04:00	00:09	Yes
Failed to decrypt media		Back Hallway	2020-03-18 07:26:17 -04:00	00:07	Yes

Fig. 7.41 **Encrypted Recording Mouse Over Explanation**

Adding the original key back into the NexLog DX-Series™ will allow playback to resume. (see Adding an AES Key)

Fig. 7.42 **Encrypted Call Playback in MediaWorks DX™**

Once Encryption at Rest is enabled, a new metadata column will be created in MediaWorks DX™. To view it, right click the column header in the callgrid and enable *Encryption on Disk*.

A value of *Yes* means that the recording is encrypted.

A value of *Partial* means that only a portion of the recording was encrypted. This can occur if a recording was in progress when Encryption at Rest was enabled/disabled, or while the active key was being changed.

A blank value means that the recording is not encrypted. The channel in question may not have been included in the Encryption at Rest channel field.

7.3.9.5. Encryption with NexLog DX-Series™ Access Bridge

If NexLog DX-Series™ Access Bridge is being used for playback, the AES key will only need to reside on the source recorder that originally captured and encrypted the recording. It is unnecessary to load the AES key on other recorders.

7.3.9.6. Archiving Encrypted Recordings

Once Encryption at Rest is enabled, any encrypted recordings set to archive will remain in their encrypted state. If the need arises to playback or restore archived encrypted recordings, the original AES key will need to be added to the playback recorder. If encrypted recordings are being Central Archived, the receiving recorder will need the AES keys originally used to encrypt them.

> **ⓘ Note**
>
> Encrypted local archives cannot be played in MediaWorks DX™ Desktop since the archives do not contain any AES keys. The archive must be mounted to a NexLog DX-Series™ as a remote archive, and the NexLog DX-Series™ must original AES key loaded.

7.3.9.7. Exporting Encrypted Recordings

When exporting an encrypted recording, the NexLog DX-Series™ will automatically decrypt the file before downloading it to your computer. If you wish to maintain recording encryption, you will need to export the files as a password protected local incident. For enhanced security, this method will not use your original AES key, instead it will encrypt the recordings using the password entered on export.

7.3.9.8. Background Vocoding Encrypted Recordings

The IMBE/AMBE Vocoder section below discusses the use of background vocoding for IMBE and AMBE recordings. If encryption is enabled on channels recording P25 radio traffic, the recordings will be encrypted before writing them to the internal RAID. If background vocoding is enabled, the recording will be decrypted before being vocoded. Once the recording is vocoded, it will be encrypted again using the currently active AES key. If the original key is not available for the initial decryption, alert code 66 will be triggered to alert you that a key is missing.

7.3.10. IMBE/AMBE Vocoder

This page allows you to configure your recorder to use internal or external IMBE/AMBE Vocoders to decode IMBE/AMBE encoded audio, such as P25 or DMR, etc. If your NexLog DX-Series™ recorder is fitted with an internal DVSI Vocoder or two, the Internal Vocoder Resources field will show the number available. Check the box to enable these.

If you are using an external DVSI Net-2000 Vocoder IPs or external EFJohnson JEM II Vocoder IPs, you can configure as many as needed, one IP address per line.

7.3.10.1. Background Vocoding

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 DX™ 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 DX-Series™), 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.

Fig. 7.43 **IMBE/AMBE Vocoders Configuration**

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. Archiving

In addition to the online storage that NexLog DX-Series™ provides for recordings on its hard drives (System: Storage Devices), the system can also archive recordings externally.

7.4.1. 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 (Recording: Retention) and/or disk space availability. The NexLog DX-Series™ archives page allows you to view the status of and perform actions on your archive drives.

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.

DRIVE	STATUS	RECORD COUNT
RDX 1	Idle, used Eventide media	3494708
RDX 2	Idle, Full Eventide media	5665414
CA 740004732	Archiving,2020-03-04 23:37:27 UTC	53607203

Start Archiving   Eject   Browse

Period Archive   Format   Media Info   Print Label

Fig. 7.44 **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 Archive Configuration below). 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.

Copyright © 2021, Eventide Inc.

| Browse | This loads the current archive for browsing and playback from both the Front Panel and MediaWorks DX™. 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 DX-Series™ 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.

7.4.2. Archive Configuration

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

Fig. 7.45 **Archive Configuration**

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 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.

Configure

This screen allows you to configure your archiving drive. Select the Archive on the Archive Configuration page and then click Configure and you will be greeted by this tabbed page that lets you configure settings, time, groups and tracking.
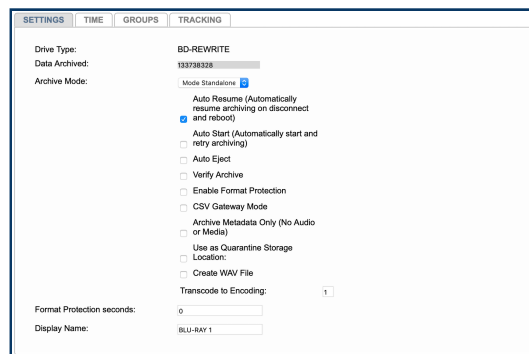
Fig. 7.46 **Archive Display in Configuration Manager**

7.4.2.1. Settings

Drive Type

The type of drive.

Data Archived

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

Archive Mode

Archive drives mounted inside the NexLog DX-Series™ recorder are set to sequential by default. Sequential means that after the current drive finishes archiving it will start archiving on the next drive in the chain, assuming the media is inserted and formatted without any data on it. Parallel mode allows systems with two drives to be used simultaneous for two different archiving tasks.

Auto Resume

A recorder that is turned off while an archive medium is being recorded will automatically continue recording that archive from where it left off when the recorder is restarted. If it isn't enabled, then any archive media in the recorder when power is applied will appear as they would if they were simply inserted in the drive. This setting also controls auto resuming on Network Archives after a network disconnect.

Auto Start

An archive drive set to Auto Start will automatically start archiving anytime the drive is in a state where archiving is available. The only times it will not start archiving are when there is no media, full (or damaged) media, the drive is in browse mode, or when the other drive in a sequential pair is already archiving. You may need to turn this off temporarily to be able to eject or browse a drive if you want to do so while it is only partially full.

Format Protection

Protects the media from being accidently 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 DX-Series™ recorder, it does not protect against placing the media in a PC and formatting it there.

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.

7.4.2.2. Time

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 will 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

only want one day's worth of recordings on a media, for example.

7.4.2.3. Groups

Use Channel Group

Set an archive drive to use one of the configured archive groups.

7.4.2.4. Tracking

This feature is optional only because a Call Source may be temporarily offline and one needs to archive calls anyway. In that case, turn off CST, create the archive you need, then turn CST back on and reset the archive time.

7.4.2.5. Media Selection

This section assumes you are using Blu-ray disks for archiving. Eventide recommends any of the following configurations of media for Blu-ray archiving:

- For NexLog DX-Series™ recorders equipped with the Blu-Ray drives, use the following media:

  ◦ Optical Quantum 25 GB BD-RE, single-sided media, (non-cartridge)

> **ⓘ Note**
>
> **Regarding Data Protection**: Although the recorder incorporates an archive protection mechanism, this is only effective when playing the archive in the recorder itself. When playing the archive in an ordinary PC, it is not protected from being overwritten.

CD-R Media: CD-R and DVD-R/RW/RW+, etc. media are **not supported** for archiving. They are supported for exporting media via the Front Panel. If you try to archive onto a CD-R, it won't work, and

it may not be immediately clear why, so be sure to confirm that you are using the proper (Blu-ray or DVD-RAM) archive medium.

7.4.2.6. Sequential and Parallel Modes

These modes apply only to recorders with more than one archive drive. Otherwise, the setting has no effect.

Sequential mode

means that archiving will continue automatically to the next available medium. In the following figure, the top disk is writing calls. When the disk fills up, archiving will continue on the middle drive, and then on the bottom drive. The middle and bottom drives must contain formatted, blank media. After the disks are full, they can be flipped if they are double-sided, and the process will continue. For example, when the top disk Side A fills up, the middle disk Side A will begin recording. When that is full, the bottom disk Side A will begin recording. After Side A is full on any of the disks, you can flip the disk to Side B. After the bottom disk, Side A, is full, the recording will continue on the top drive Side B, and so on.

Parallel mode

means that archiving will *not* continue automatically on the next available drive. Instead, you can begin recording on the top drive and on the middle drive simultaneously (and the bottom drive if you wish) and all drives will record the same data. This mode uses more disks but provides redundancy.

7.4.2.7. Network Archive Storage (NAS) Configuration

The recorder can archive not only to its own internal drives and removable media, it can also use network attached storage (NAS) on a typical Microsoft Windows network for archiving. Using more than one NAS on a recorder requires an Add-On License.

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

Tthe 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.

7.4.2.8. Archive Splitter

Archiving media that has the potential to contain a very large amount of call data, such as R-HD, NAS and USB drives, can be configured to be split into month sized folders, for faster loading times and search results when put into browse mode. The splitter is configured with the Schedules page found under Utilities.

7.4.3. 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.
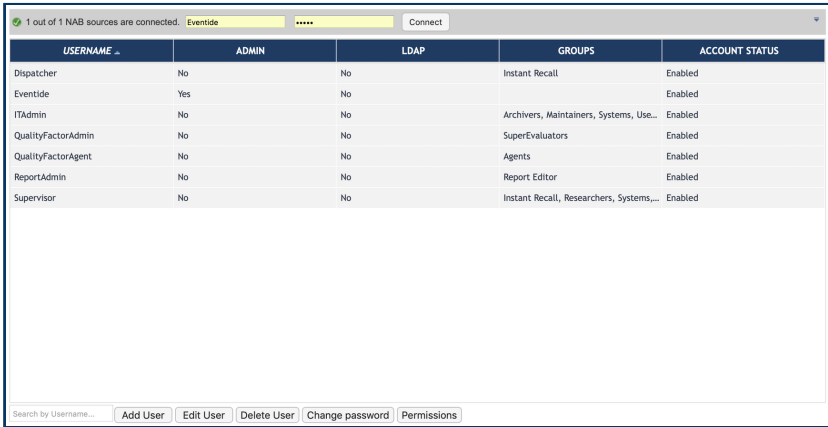
7.5. Users and Security

All access to NexLog DX-Series™ 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 DX-Series™ 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 7.5.5: User Groups and Section 7.5.1.4: Permissions).

7.5.1. Users

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

USERNAME ▲	ADMIN	LDAP	GROUPS	ACCOUNT STATUS
Dispatcher	No	No	Instant Recall	Enabled
Eventide	Yes	No		Enabled
ITAdmin	No	No	Archivers, Maintainers, Systems, Use...	Enabled
QualityFactorAdmin	No	No	SuperEvaluators	Enabled
QualityFactorAgent	No	No	Agents	Enabled
ReportAdmin	No	No	Report Editor	Enabled
Supervisor	No	No	Instant Recall, Researchers, Systems,...	Enabled

Fig. 7.48 **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. 7.49 **Add New User Pop Up**

7.5.1.1. 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. 7.50 **Editing a User**

The available parameters are described below:

7.5.1.1.1. 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.

7.5.1.1.2. 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 and User Managers. 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 DX-Series™ 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 Front Panel**

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 DX-Series™ Clients**

Security Group	Privileges
Admin	All available privileges, including the ability to create new users, and receive emailed alerts.
Archiver	No access.

Security Group	Privileges
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).

Archive Drive Maintenance Access

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

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 Front Panel and the MediaWorks DX™ and MediaAgent DX™ clients, users may have access to an `Instant Recall` functionality in which they can view the most recent calls on the recorder. Users can select how far in back they wish their view to contain calls from. The Limit configured here places an upper bound on how far back the user can set this limit when performing instant recall.

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 which 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 DX™, 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.

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 7.6.5).

7.5.1.1.3. Account Settings

Can Change Password

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

🔥 *New in version 2021.1.*

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 DX™ 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.

7.5.1.1.4. User Resource Permissions

These settings control what resources a user can search and playback in MediaWorks DX™ and the Front Panel. This feature integrates with the Resource Groups feature detailed in Section 7.3.4 of this

manual. You can add or delete individual resources or resource groups from the user's resource groups here.

7.5.1.1.5. User Search Filters

7.5.1.2. Delete User

7.5.1.3. Change Password

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

7.5.1.4. Permissions

The Permissions button will load the Permissions page showing the selected user's permissions. See Section 7.5.1.4 Permissions for more details.
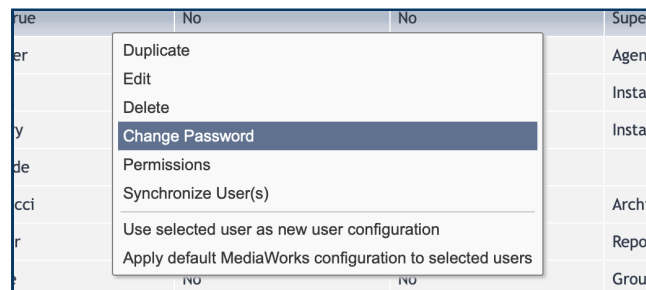
Fig. 7.52 **User Table Right-Click Context Menu**

7.5.1.5. 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.
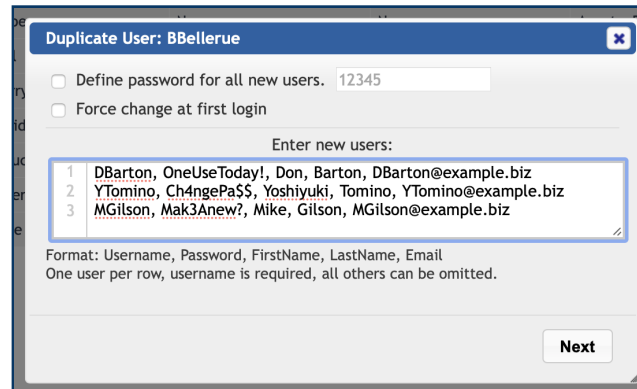
Fig. 7.53 **Duplicate User**

7.5.1.5.1. 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.
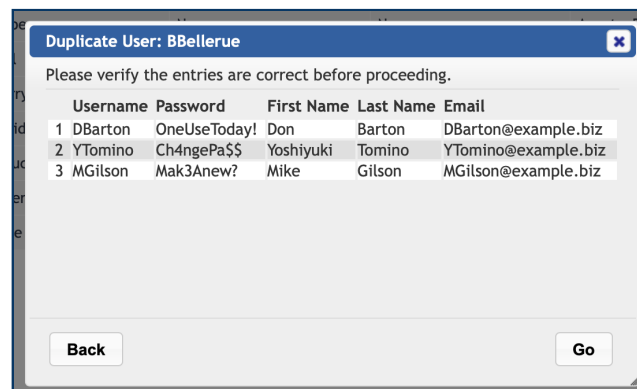
Fig. 7.54 **Verify Duplicate User**

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.
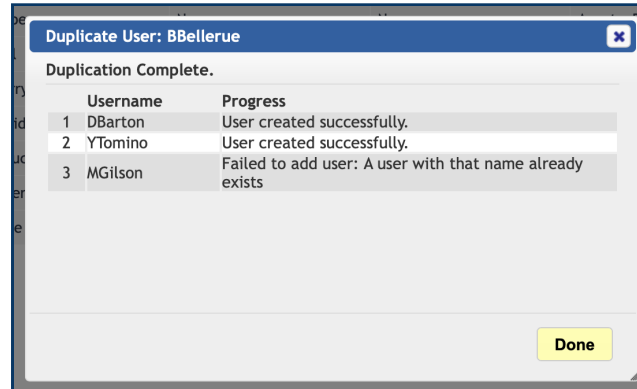
Fig. 7.55 **Duplicate User Results, with Error for User That Already Exists**

7.5.1.5.2. Synchronize User(s)

Synchronize User(s) will sync the selected user to all NAB sources currently connected. (This option is only present for systems with NexLog Access Bridge.)

7.5.1.5.3. Use Selected User as New User Configuration

If you want to set up a custom MediaWorks DX™ 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.

7.5.1.5.4. Apply default MediaWorks Configuration

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

7.5.1.6. NexLog Access Bridge Sync

If the recorder is licensed and configured as a NexLog Access Bridge host, the NAB Connection Manager tool will appear at the top of the user page. Enter an admin username and password here to connect to all configured NAB sources.

While connected via NAB, all users created, edited and deleted will be created, edited and deleted across all sources as well as the host.

7.5.2. System Security

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

7.5.2.1. General

🔥 *Changed in version 2021.1.*

Audit Changes

If this option is enabled, then any configuration changes made via NexLog DX-Series™ 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 DX™. 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 DX™ manual.

🔥 *New in version 2021.1.*

Enable User Content Uploads | If enabled, allows a user to upload media to a NexLog DX-Series™ 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 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 DX™ | A custom Terms of Service splash screen can be show 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 DX™.

Enable MediaWorks DX™ ATC/ ATM mode | Makes changes to MediaWorks DX™ 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.

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.

7.5.2.2. Front Panel

🔥 *Changed in version 2021.1.*

Desktop Mode   If enabled, the front panel interface can provide a an experience
                                      similar to MediaWorks DX™.

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*

7.5.2.3. Password Complexity

This section configures restrictions on NexLog DX-Series™ 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.

7.5.2.4. 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	Once this many days have passed since the user has last changed the password before they are 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 DX-Series™ 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 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.

7.5.2.5. 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 DX-Series™ Configuration Manager page will take effect until the 'Save' button is pressed.

7.5.2.6. Two Factor Authentication

🔥 *New in version 2021.1.*

Two Factor Authentication (2FA), also known 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 DX-Series™ natively uses *something you know* and *something you have*. *Something you are* and can be implemented externally by integrating with Active Directory.

In NexLog DX-Series™, 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*.

7.5.2.6.1. TOTP

🔥 *New in version 2021.1.*

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 an 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. 7.56 **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.

$$(30 \text{ seconds}) * (5 \text{ depth}) = 150 \text{ seconds}$$

7.5.2.6.2. TOTP Generators

This list of TOTP token generators is provided for your convenience. The products listed are neither supported nor affiliated with Eventide Inc or NexLog DX-Series™.

7.5.2.6.2.1. Desktop TOTP

- Authy by Twilio

- LastPass

· SafeInCloud

7.5.2.6.2.2. Mobile TOTP

· Authy by Twilio

· Google Authenticator

· LastPass

· SafeInCloud

7.5.2.6.2.3. Hardware TOTP

Hardware tokens used for NexLog DX-Series™ must support a programmable secret.

· Protectimus

· Token2

7.5.3. Active Directory

🔥 *Changed in version 2020.1.*

The Eventide Active Directory software add-on, its configuration and use are detailed in the Eventide Active Directory Configuration Manual, (Eventide P/N: 141267).

This page is for configuring the Active Directory feature and provides four options for Authentication:

· **Local Recorder Only:** No Active Directory features in use. The default. All Authentication done using local User configuration.

· **Network File Share (SMB):** Configure the recorder to test user authentication against an SMB share. If the user's credentials allow access to the folder, they are authenticated to the recorder. Allows for the use of Domain credentials but no other AD user management features.

· **LDAP:** Use LDAP to assign user groups to recorder users. Add-on License required. Covered in detail in the Active Directory manual.

- **Active Directory Domain:** Join the recorder to an Active Directory Domain to authenticate with domain credentials and enable single sign on. Add-on License required. Covered in detail in the Active Directory manual.

7.5.3.1. Local Recorder Only

This option is the default and allows you to user authentication directly from NexLog DX-Series™.

7.5.3.2. Network File Share (SMB)

This option allows for basic Active Directory Authentication to a Windows file share. The NexLog DX-Series™ server does not have to join the domain in order to use this credentialing method however users and permissions must be managed on the recorder. All users must be created via the NexLog DX-Series™ User configuration interface before logging in.

7.5.3.3. LDAP

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

Lightweight Directory Access Protocol (LDAP) is a vendor-neutral application protocol used to maintain distributed directory info in an organized, easy to query manner.

This credentialing method does not require the recorder to be joined to the domain, but does require a domain user for querying.

7.5.3.4. Active Directory Domain

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

Active Directory Domain allows users to log in to their NexLog DX-Series™ user accounts with their Windows credentials (username and password,) via LDAP user management. It allows the system administrators to manage group level user permissions from one place. With the Single Sign-On option, logging into MWP can be as simple as clicking a link.

This is much more comprehensive than the Network File Share setting: for example, with enhanced Active Directory, users that exist on the domain but have not been previously created on the NexLog DX-Series™ can be automatically created on the recorder at first login, including inheriting their proper group memberships and resource permissions, if configured correctly on the domain.

Active Directory requires a NexLog DX-Series™ Add-on License Key. The Eventide Active Directory software add-on and its configuration and use are detailed in the Eventide Active Directory Configuration Manual, (Eventide P/N: 141267).

7.5.4. SSL

🔥 *Changed in version 2021.1.*

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 SSL for client connections such as MediaWorks DX™, it is highly recommended to protect access to potentially sensitive information.
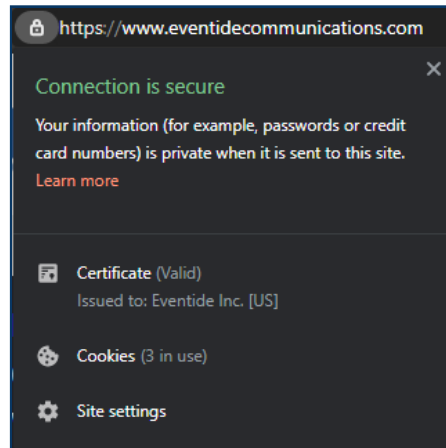
Fig. 7.57 **TLS/SSL Connection Example**

7.5.4.1. 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 7.5.4.3.3 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 7.5.4.3.3 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 7.5.4.3.2 Upload P7B File.

Once a response has been applied, you can enable SSL for your system. See Section 7.5.4.4 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 7.5.4.3.5 Obtain Certificate from Let's Encrypt.

7.5.4.2. Generate CSR

🔥 **Changed in version 2021.1:** The CSR can be downloaded to a file.
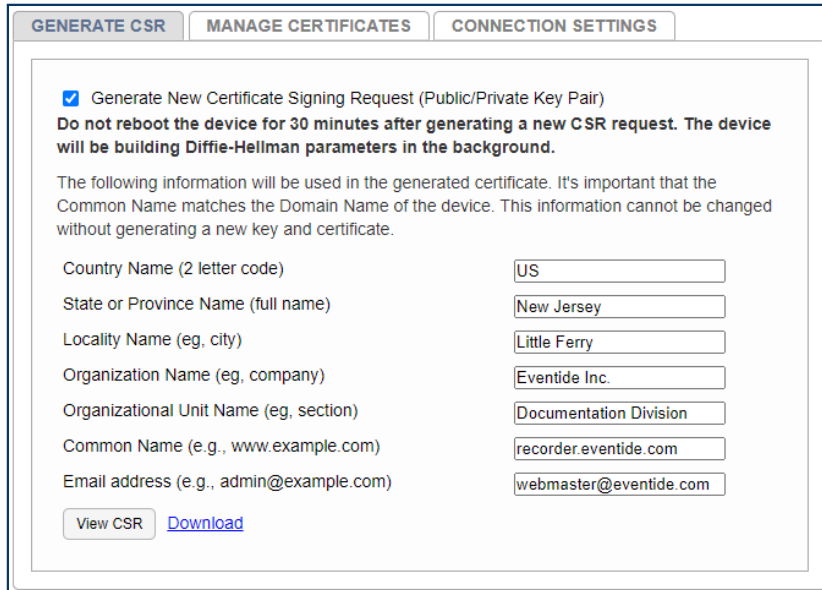
Fig. 7.58 **Generate New CSR**

To generate a CSR, you must enable the checkbox as show in Fig. 7.58. Fill in form details, the critical information in this form is the **Common Name**. You must fill in all other fields, but your CA may not use them.

The Common Name is the DNS name that you will be accessing the recorder from. Example: *https:// recorder.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.

7.5.4.3. Manage Certificates

🔥 ***Changed in version 2021.1:*** New certificate options

This tab will allow you to manage existing certificates, apply the CA response from your CSR, or upload a new certificate directly.

Fig. 7.59 **Manage Certificates**

7.5.4.3.1. Copy/Paste Certificates

🔥 ***Changed in version 2021.1:*** Updated interface

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 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.

7.5.4.3.2. Upload P7B File

🔥 *New in version 2021.1.*

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.

7.5.4.3.3. Upload PFX/P12 File
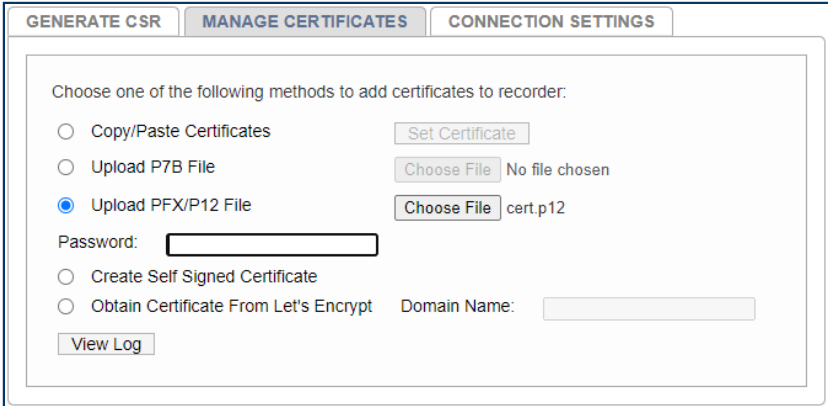
🔥 *New in version 2021.1.*

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. 7.60 **PFX/P12 Password Prompt**

7.5.4.3.4. 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.

7.5.4.3.5. Obtain Certificate from Let's Encrypt

🔥 *New in version 2021.1.*

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.

7.5.4.4. 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. Plaintext is used for *http:// and Encrypted for `https://*

Database Connections

This includes Eventide software such as MediaWorks DX™ which communicate 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 DX™/MediaAgent.

Centralized Archive Connections

Controls the connections made between two NexLog DX-Series™ 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.

7.5.5. 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 are a set of action buttons. Except for the 'Add Group' button, all actions require you to first select the group you wish to perform the action on from the User Group table by clicking on it in 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. 7.61 **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 a Agent Group, if the Group Evaluator is also configured as Group Leader

- Instant Recall

  Can login and use instant recall feature of MediaWorks DX™ 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 DX™ and the Front Panel to live monitor incoming calls as they happen.

- Researchers

  Can use MediaWorks DX™ 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 provided access. In addition to a Group Name, this page allows you to modify which users are a member 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 check boxes on the Security: Users page. No changes will take effect on this page until the 'Save button' is clicked.

'Delete Group' will prompt for conformation 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 which 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. 7.62 **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.

🔥 *New in version 2021.1.*

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 a **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 by other members of the same group. This option **will not** have an affect on an Admin user; they will be able to access all incidents on a system.

7.5.6. 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 DX-Series™ 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 DX-Series™ 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.

USER OR GROUP NAME ▲	TYPE
Agents	Group
Archivers	Group
ASaunders	User
BBellerue	User
DBarton	User
DCooper	User
DSigal	User
ECherry	User
Eventide	Admin User
Group Evaluators	Group
Instant Recall	Group
LBertucci	User
Maintainers	Group
MGilson	User
Monitors	Group
Report Editor	Group

Search by User or Group...   Show All ▼   Edit Permissions

Fig. 7.63 **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.
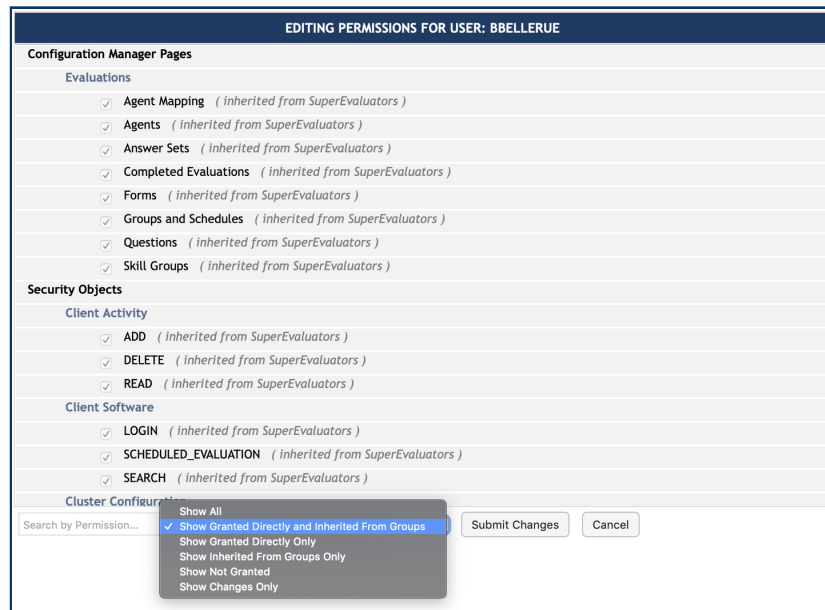
Fig. 7.64 **Permissions with Filter Set to Show Granted Directly And Inherited From Groups**

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"
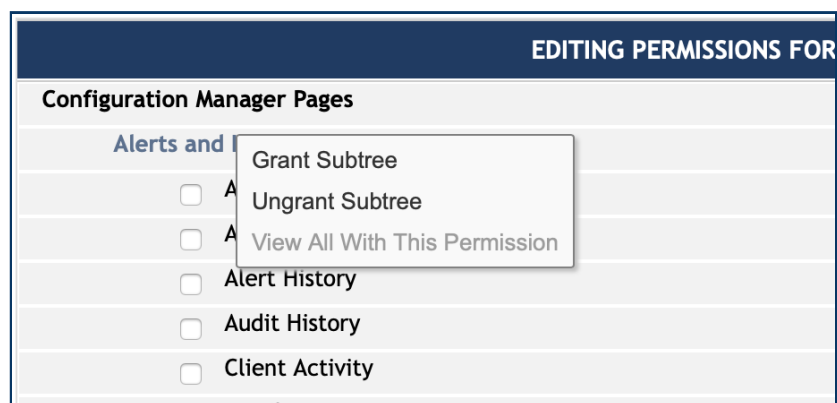
Fig. 7.65 **Permissions Edit Page Context Menu**

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.
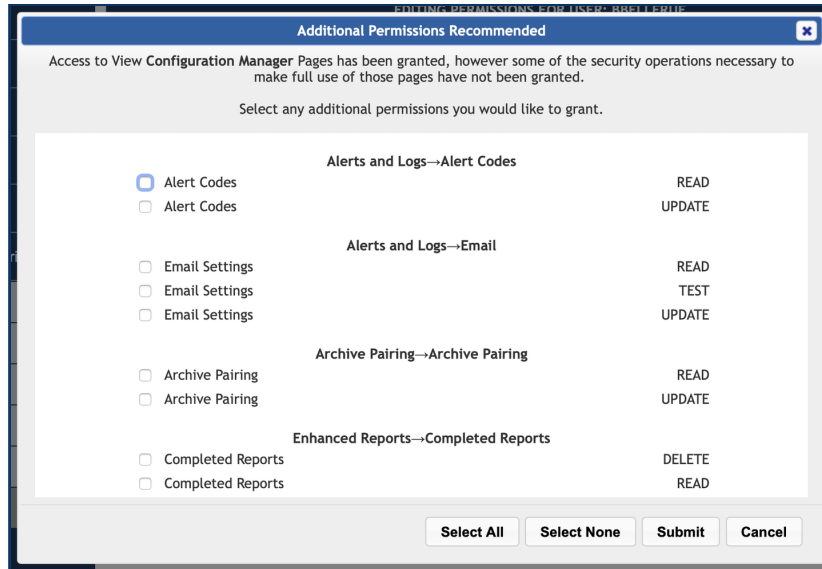
Fig. 7.66 **Additional Permissions Recommended Pop Up Wizard**

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.

7.6. Alerts and Logs

7.6.1. 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 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 place holders 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.

7.6.2. 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.

7.6.3. 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 DX™ 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.

7.6.4. Logging

In addition to the alert history, the Eventide NexLog recorder maintains some internal logs which are only useful to Eventide Technicians. For Service reasons, an Eventide Technician may request the logs from your recorder. This page provides two buttons.

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 or your Eventide 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 '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 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 other archive medium rather than downloading.

7.6.5. Email

First click the 'Enabled' check box on this page. Then you must configure the parameters for the SMTP 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.

7.6.6. GPIO

The following uses can be made of a GPIO board:

- The start and stop of recording on a channel can be triggered by a GPIO board input signal. (For more information, see Recording Interfaces.) The logic of GPIO-triggered recording can be customized using the custom script feature.

- A recorder alert can trigger a GPIO output signal. Alerts of severity 3 or 4 (Error or Severe) will by default trigger a signal on the first output pair of the board. Further customization is possible via a custom integration script available from Eventide.

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

To configure an alarm output, go to the NexLog Configuration Manager: Alerts and Logs menu, and select GPIO. For each GPIO board in the system there will be an entry on the page with a description of the board, like "Contec PCI-E (DIO-48D-PE)," the number of the physical slot the board in installed in, and the pin count for each board.

Click on the Edit Board button for the board you want to configure. For each Pin Block (1-A Port [1-8], 1-B [9-15], 1-C Port (Low)[16-19], etc) you can select the I/O mode to either be Input or Output.

For each input pins, you can configure channels that should record when the pin is active. This can be a single channel, or a comma-delimited list of channels. One limitation: channels can only be controlled by one pin, so you cannot set pin 1 to control 1,2,3 and pin 2 to control 2, because 2 is already configured for pin 1. When configuring a pin for input, the channels configured's GPIO pin field on the Recording Interfaces page is set, but the detect type still needs to be manually changed to GPIO.

You can configure pins to trigger an output when an alert of a certain severity or above is triggered. The alert severities in escalating order are Info, Warning, Error, and Severe. If configured to alert on Warning or above, the pin will be off if an info alert happens but on for any other kind of alert. You can also configure a relay closure only for unacknowledged alarms of those types.

The relay can also be activated by the recorder just being powered on, it will remain active while the recorder is on and turn off when shutdown. If you want a specific alert code to trigger the output go to the Alert Codes page and find the code you want. For example, alert code 6001 is for a degraded RAID. Enter 6001 in the Alarm Code entry field and click Add.

Multiple rules can be configured for each output, and using boolean logic, these rules are OR'ed together. For example, you may configure Minimum Alert Severity to be SEVERE, and Minimum Unacknoledged Alert Severity to WARNING. In this case, an alert of type ERROR will trigger the pin, but acknowledging it will turn off the pin, but an alert of SEVERITY will cause the pin to trigger until the alert is resolved. The only rule that cannot be combined with other rules is **Always On**. The pin is always active while the recorder is on if Always On is set, so it does not make sense to use with other rules, as it will never turn off.

7.6.7. 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 DX™, 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.

7.6.8. 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

7.6.9. NexLog Monitoring

🔥 *New in version 2021.1.*

🔑 **License Required**

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

NexLog Monitoring provides Eventide and/or your Eventide Dealer with system health information for priority support and service.

Contact your Eventide Dealer for more information.

7.7. Utilities

7.7.1. Schedules

ACTION	DESCRIPTION	CHANNEL	START TIME	EXPIRE TIME	ENABLED
RECORD	ch1	1	Now	Never	YES
CALCULATE STATISTICS	Statistics Collector		Now	Never	YES
DATABASE MAINTENANCE	Database Maintenance		Now	Never	YES
NAS ARCHIVE SPLIT	NAS Check For Monthly Archive Split		Now	Never	NO
USB ARCHIVE SPLIT	USB Check For Monthly Archive Split		Now	Never	NO
RHD ARCHIVE SPLIT	RHD Check For Monthly Archive Split		Now	Never	NO
LSI RAID CONSISTENCY CHECK	LSI Raid Consistency Check	1	Now	Never	YES

Fig. 7.67 **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:

7.7.1.1. 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.

7.7.1.2. 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.

7.7.1.3. 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.

7.7.1.4. 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.

7.7.1.5. 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

7.7.2. 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.

7.7.3. 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.

7.7.4. Network Utilities

The Network Utilities page allows administrators to run Ping, Traceroute and Netcat Unix utilities from the recorder to identify network problems.

Figure — Network Utilities

Fig. 7.68 **Network Utilities**

7.7.5. 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. 7.69 **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.

7.7.6. Documents

This page include links to HTML and PDF versions of NexLog DX-Series™ 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. 7.70 **System Documentation**

7.7.7. Downloads

Fig. 7.71 **System Downloads**

This page includes links to NexLog DX-Series™ clients, software, and plugins, including:

- **MediaWorks DX Desktop Client**: Desktop client for playback and offline incident review.

- **MediaAgent DX Client**: Desktop client for Instant Recall.

- **Screen Capture Agent**: Installation utility for screen capture.

- **AutoUnpacker**: This Windows software will automatically unpack any media exported from MediaWorks to your defined default location by using Eventide AutoUnpacker, if installed and configured.

🔥 *New in version 2021.1.*

- **AIS Proxy**: Installation utility for Motorola Astro® AIS servers

🔥 *New in version 2021.1.*

- **AQUA Plugin**: Installation utility for Priority Dispatch AQUA Evolution® and AQUA Ascent®

7.8. Basic Reports

7.8.1. Recording Reports

This section provides access to the Eventide NexLog DX-Series™ 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.
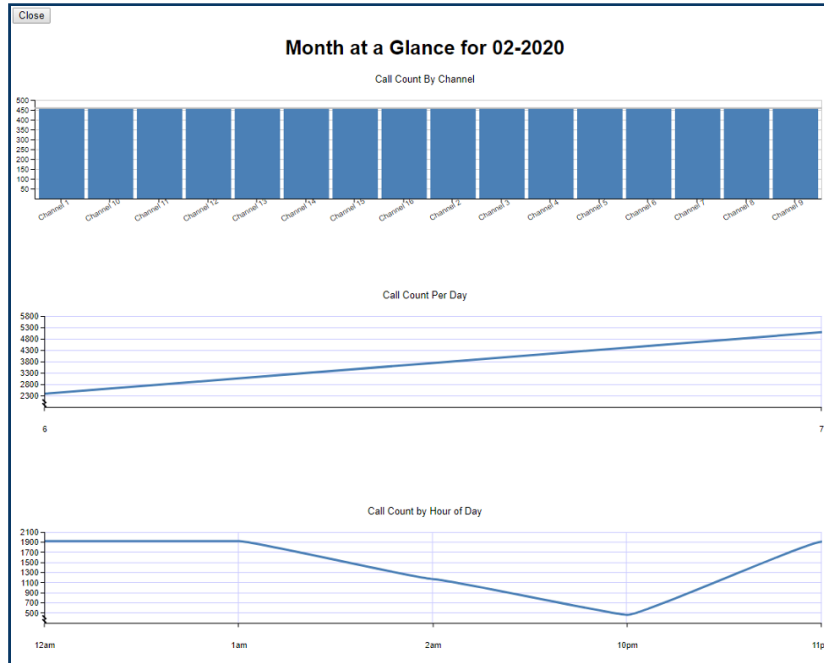
Fig. 7.72 **Example Report for** *Month at a Glance*

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.

7.8.2. Quality Factor Reports

This tab is part of the Eventide Quality Factor software add-on, and its use is detailed in the Eventide Quality Factor Software Manual (part number 141216.)

7.9. Enhanced Reports

Eventide NexLog DX-Series™ has two reporting mechanisms. The Basic Reporting feature is available on all NexLog DX-Series™ recorders and provides a mechanism to run simple pre-defined reports inside of a web browser.

🔑 License Required

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

Unlike Basic Reporting, Enhanced Reporting allows complex custom reports to be designed by the end user. This is done by choosing and configuring Report Templates from provided report components called Report Blocks. Some of these correspond to the reports available in the Basic Reporting feature, while many others are only available in the Enhanced Reporting Package. In addition, even when the same building block is available in both, the Enhanced Reporting version will often have additional parameters and configuration options, providing more flexibility and power.

The Enhanced Reporting Package provides many other features not available with Basic Reports. For example, it allows reports to be designed once and then run later, even to be run automatically on a schedule such as nightly or weekly. It also allows reports to be automatically emailed out when they are run. Enhanced Reports can be available not only in HTML format to be viewed in a web browser, but also as PDFs. It is also possible to export the raw data from the reports in Excel format for further customization. Enhanced Reports also provides permissions on a per-report basis, so a user can be given permission to run and/or view specific reports, without being able to see others.

The Eventide Enhanced Reporting Package software add-on and its use are detailed in the Eventide Enhanced Reporting Package Manual (Eventide P/N: 141268).

7.10. Quality Factor Software

This page is for configuring the Eventide Quality Factor call evaluation add-on software. For information on this see the Eventide Quality Factor Manual (Eventide P/N: 141216).

🔑 License Required

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

7.10.1. Agent Mapping

The Agent Mapping screen is used to assign specific channels to a workstation location and an agent (user), so that calls can be tagged with that information. When a user is logged in at a designated workstation, calls received at that location will have the user name and location saved in the call metadata.

Agent Mapping allows you to tag incoming and outgoing calls on a channel number or channel name with information about the Agent or User handling the call.

With Static Mapping, all calls on a specific channel name or channel number are tagged with an Agent_ID. This is ideal for situations where an Agent has his or her own telephone that is not shared by other agents.

To use Static Agent Mapping, you must first go to Recording → Custom Fields and add a Custom Field for Agent_ID, of type Text.

With Dynamic Mapping, calls are tagged with a User_ID based on active logins from Workstations identified via MAC address. If the User also has an associated Agent account, the call is also tagged with the Agent_ID. This is ideal for situations where a call taker desk is used by multiple people over the course the day and each call taker has their own user account to log into the Workstation with.

For Dynamic Agent Mapping, you must first go to Recording → Custom Fields and add Custom Fields for User_ID and Agent_ID, both of type Text.

If an Agent is associated with a User account, and calls are tagged with either method, the other field will be automatically filled out as well. The User ID field must match the User account name exactly; if you are using Windows User Tracker to tag calls, the recorder user account and the Windows user account must be named identically for the Agent field to also be populated.

For more information about this feature, see the Eventide Quality Factor Manual (Eventide P/N: 141216.)

7.11. 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.

This page was intentionally left 99.75% blank.

8. Software License

The Eventide® NexLog DX-Series™ 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 DX-Series™ firmware may only be installed on a purchased and licensed Eventide NexLog DX-Series™ 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.

Copyright 2007-2013, Eventide Inc. and its licensors. All rights reserved.

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 DX-Series™ recorder. 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 licensed components; this license grants you a legal right to gain access to the source code to these components. The Easiest way to get access to the source for the components utilized is to go to http://debian.org, and download the source code you want. Alternatively, you may request a copy of these components be sent to you directly from Eventide. To do so, send a written letter to Eventide at:

Eventide Inc.

ATTN: NexLog Engineering – GPL Software Request

1 Alsan Way

Little Ferry, NJ 08731

USA

Included with your letter, please provide:

- **The GPL/LGPL licensed packages you are requesting source to. Please**

    use the Debian Apt package naming standards to request packages.

- Enough blank CD-R Media Disks to fit the packages you are requesting.

- **A Self Addressed Padded Return Envelope with sufficient space and**

    postage for your media to be returned to you with the requested data.

- **A US Postal Money Order or Check drawn on a US Bank made out to**

    Eventide Inc. for $10.00 per Media to cover duplication costs.

A. Recorder Software Installation and Upgrade

Software Upgrades are made available for NexLog DX-Series™ regularly. They include new features, system security updates, and refinements.

Just as with any computer, Eventide NexLog DX-Series™ 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. Boot to an Eventide Software Distribution DVD-ROM

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:
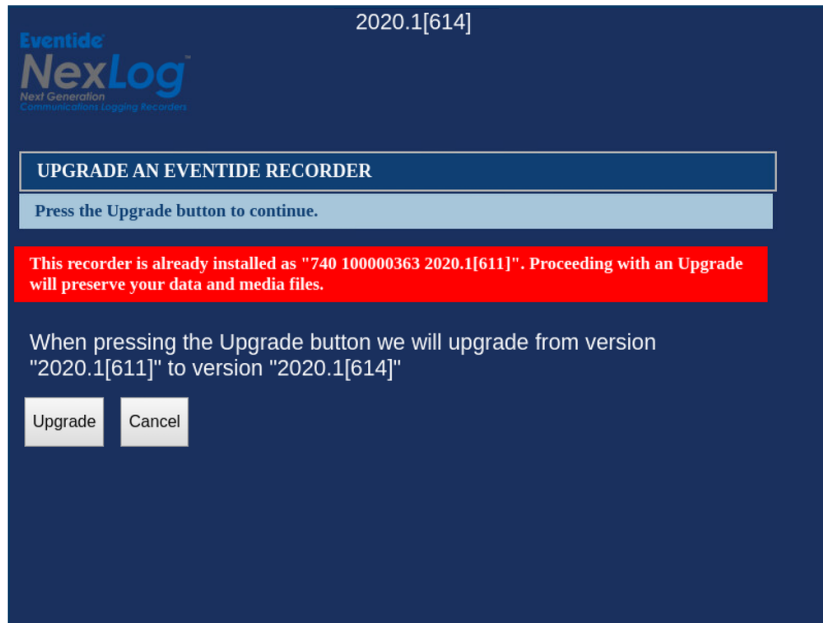
Fig. A.2 **Upgrade**

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:
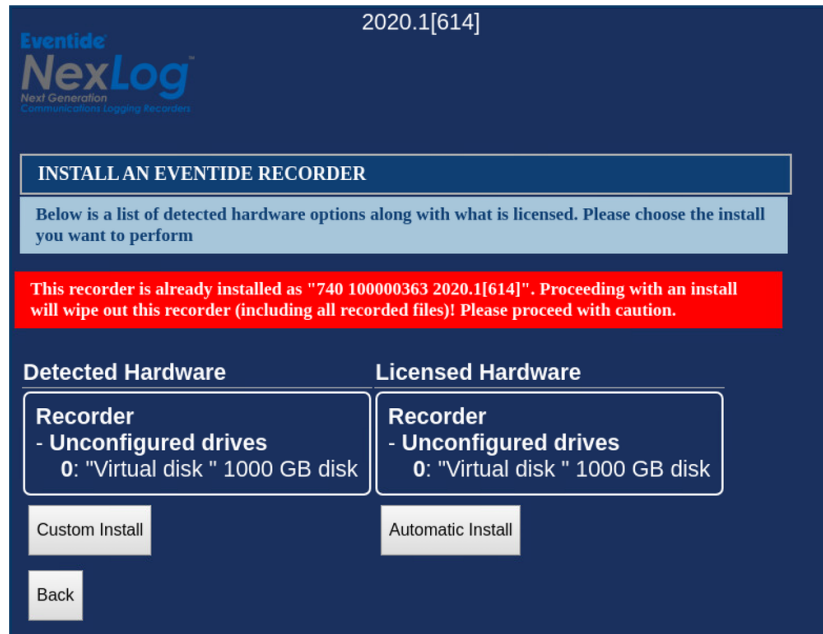
Fig. A.3 **Install**

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.
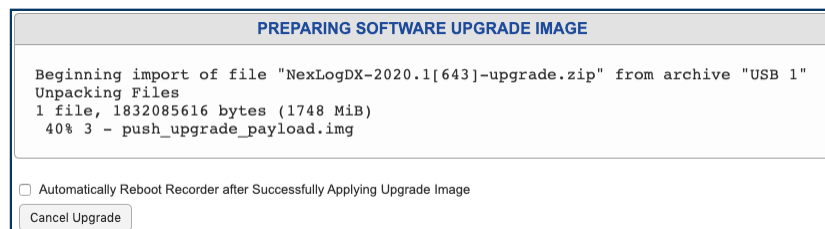
Fig. A.4 **USB Upgrade In Progress, with Automatic Reboot Option**

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: Restoring Archives When Installing New Software. An upgrade will theoretically leave your calls in the same state as they were earlier, and, in fact, it almost always does. But why take chances? You should be archiving anyway, so can it hurt to be up to date?

If you do a new installation, you will have to reconfigure the recorderx in accordance with the Setup instructions. This is greatly simplified by the Read/Write Configuration to Archive featxure. 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. A*lways 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!

This page was intentionally left 99.75% blank.

B. Channel Wiring for Analog Input Boards

All Eventide NexLog DX-Series™ 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 B.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 B.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 99.75% blank.

C. 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 C.1 — Alert Severity Levels: A list of alert severity levels and descriptions.

- Table C.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 C.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 C.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
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

CODE	ALERT TEXT	SEVERITY
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	The Metadata feed for channel <~110~> appears to be missing. <~111~> calls were recorded without providing metadata.	ERROR
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

CODE	ALERT TEXT	SEVERITY
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
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

CODE	ALERT TEXT	SEVERITY
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
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

CODE	ALERT TEXT	SEVERITY
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 possible. In the future please use the Eject soft key and wait for the drive status to read "Safe To Remove Media".	ERROR
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 <~111~> seconds.	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
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

CODE	ALERT TEXT	SEVERITY
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	The RAID Controller Battery Backup for recorder <~1~> is reporting excessive heat.	ERROR
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
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

CODE	ALERT TEXT	SEVERITY
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
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

CODE	ALERT TEXT	SEVERITY
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
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	One or More Digital PBX Channels are receiving a large number of line errors. Please check your wiring and phonesets	WARNING

CODE	ALERT TEXT	SEVERITY
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
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

CODE	ALERT TEXT	SEVERITY
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
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

D. Recording VoIP or RoIP Calls

D.1. Introduction to Recording VoIP or RoIP Calls

This topic describes information related to recording Real-time Transport Protocol (RTP) data.

- Voice Over Internet Protocol (VoIP) calls

- Radio Over Internet Protocol (RoIP) calls

Eventide NexLog DX-Series™ recorders support both VoIP and RoIP, but this topic mainly describes VoIP. However, because RoIP is similar to VoIP, much of the information applies equally to both.

- Cisco 7 through 10.5 are supported under the Local VoIP/RTP recording.

- SIP Endpoints are also supported by Local VoIP/RTP Recording.

- NG9-1-1 "SIP Invite" recording uses the Local VoIP/RTP feature on Eventide NexLog DX-Series™ recorders.

- RoIP recording and IP Dispatch Console recording uses the Local VoIP/RTP feature on Eventide NexLog DX-Series™ recorders.

D.1.1. What is VoIP?

VoIP (Voice over Internet Protocol) is a technology that allows telephone calls to be made over local area networks (LAN) or the Internet. VoIP systems convert analog voice signals into digital data

packets and supports real-time, two-way transmission of conversations using the Internet Protocol (IP).

1. VoIP calls can be made on the Internet using a VoIP service provider and standard computer audio systems. Alternatively, some service providers support VoIP through ordinary telephones that use special adapters to connect to a home computer network.

2. VoIP services convert voice or audio data into a digital signal that travels over a computer network such as a company intranet or the Internet. If you are calling a regular phone number, the signal is converted to a regular telephone signal before it reaches the destination. VoIP can allow you to make a call directly from a computer, a special VoIP phone, or a traditional phone connected to a special adapter.

D.1.2. The Advantages VoIP Provides

With traditional telephone service, also known as Plain Old Telephone Service (POTS), a telephone call is made on an analog telephone line through a pair of copper wires connected between the caller and the called party. This creates a physical connection dedicated for a single call, so the conversation is transmitted using a single, static pathway over the telephone network. It uses the Public Switched Telephone Network (PSTN), which is a circuit-switched network, meaning the connection between the endpoints (telephones) is made through switches that connect the lines together.

On the other hand, VoIP transmits the call using a packet-switched network. With VoIP, the audio signal of the telephone call is digitized and encapsulated into data packets that are sent over the network to the other party. The packets may take one or more paths over the network to reach the called party. At the other end of the line, the packets are reassembled and converted back into analog voice signals. This network can be used at the same time by other communications, which may include other VoIP telephone calls as well as a variety of packetized information such as data and video.

Because the VoIP network can carry many conversations at the same time and because it can also transmit other types of information, VoIP is a more efficient and flexible method for transporting voice. It can also produce a richer experience for the user if it is combined with other features, such as video. In addition, it can be cost-effective to implement because you may be able to add VoIP telephony services to an existing network infrastructure.

VoIP systems can interconnect and co-exist with existing PBX systems as well the traditional circuit-switched network. Of course, power sources are a consideration when implementing any VoIP system,

because VoIP phones do not derive power from a PBX or from the telephone company Central Office. So, to protect against loss of telephone service due to power outages, it is necessary to install uninterruptible or back-up power supplies for both the LAN equipment and VoIP telephones.

D.1.3. Technical Considerations

The handling of audio data in VoIP differs significantly from how it is done on a conventional, circuit-switched network. On the latter, once a connection is established, it is defined between two fixed points, and both the upstream and downstream data are handled by the same pair of wires. The digital architecture of VoIP separates upstream and downstream data, and the transmission path across the network can vary. Audio is carried through RTP (Real Time Protocol) packets, which can be routed along different paths. As a result, data packets of audio data can become unsynchronized and be delivered out of their original sequence.

To address this, VoIP uses a buffering system that synchronizes delayed packets. The inherent delay caused by packet buffering should never exceed 500 ms.

Networks are by no means limited to carrying only voice data. As such, a packet filtering mechanism is used to detect and isolate RTP audio data packets from other data types carried across the network.

D.2. Network Requirements

The following requirements apply to recording VoIP calls:

- Unlike a PBX phone system, which has a centralized switch from which to tap the telephone calls, a VoIP system transmits the calls over a distributed intranet, which also carries other data traffic. To capture and record VoIP calls from the intranet, you must configure your intranet topology to mirror or send a copy of the VoIP packets to a single Ethernet port, which is connected either to the Eventide NexLog Recorder (for Local VoIP) or, in now rare cases, to an Eventide VoIP Gateway. For example, this can be accomplished using a Cisco Systems Ethernet switch that supports Switched Port Analyzer (SPAN) technology or Remote Switched Port Analyzer (RSPAN) technology. These components create copies of the audio packets being sent across the network and send them to another designated port for network analysis. In the case of RSPAN, it places audio traffic on a SPAN port from different network switches.

For detailed information on SPAN and RSPAN, consult with your network switch manufacturer's documentation.

In addition to SPAN or RSPAN, some systems use direct unicast or multicast connections to the recorder.

When using the **Local VoIP** feature on an Eventide NexLog DX-Series™ recorder, the recorder must be equipped with two network interface cards (NICs) if you are using SPAN/RSPAN. (One port is used for the unidirectional VoIP traffic sent to the recorder, and one port for bidirectional traffic with clients.)

· Both the gateway and recorder need a second NIC card to be able to capture from a SPAN port. Since the SPAN port is unidirectional and in the case of the gateway it needs to be able to have bidirectional access to the recorder. Or in the case of the recorder it needs to have bidirectional access to the client applications.

· Eventide suggests implementing VoIP on a virtual local area network (VLAN). A VLAN is a logical group on the network that effectively prioritizes network traffic to ensure enough bandwidth. VLANs also greatly ease the configuration issues surrounding SPAN and RSPAN ports.

· **The MAC or IP addresses of all active phone sets must be designated.** This information is entered in Configuration Files area of the NexLog Recorder Configuration program. Additionally, **port ranges** for both the signaling ports (the call's attributes) and audio ports (the actual audio data packets) must be designated. Only calls that occur on ports in these designated ranges are recorded; all others are ignored.

D.3. Local VoIP and RoIP

Local VoIP and RoIP refer to the feature of Eventide NexLog DX-Series™ recorders that provides the capability to record VoIP and RoIP without using an Eventide . This local IP recording capability is also used for recording IP-based P25 radio systems (by EF Johnson and others).

The Eventide NexLog DX-Series™ recorders support capturing and recording voice or radio traffic appearing in RTP packets on an Ethernet network. The recorder is able to monitor and record Ethernet Voice over Internet Protocol (VoIP) or Radio over Internet Protocol (RoIP) traffic directly.

To configure the recorder for VoIP (or RoIP) traffic, you must first add a virtual board of type Local IP and the required number of virtual channels to the system.

The text input field at the top of the menu allows you to filter the list on characters or a word.

If your system is not in the list of templates, select No Template and see the Advanced Local VoIP Recorder configuration section below.
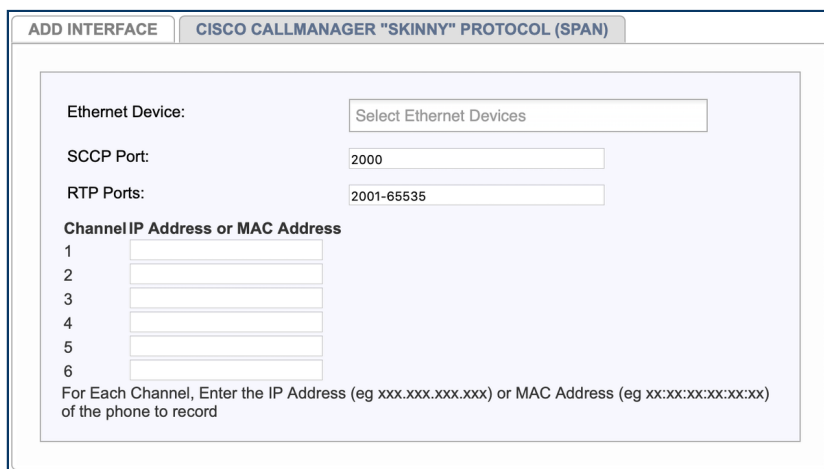
D.4. Local VoIP and RTP Templates

Local IP boards can be set up using a template that will automatically create a configuration based on the settings required for the type of board selected.

Any IP board configured with a template can be re-configured using the same template; this will effectively recreate the board from scratch, so if you have made per-channel changes, those will be reset to defaults. As such, you may want to make any necessary edits manually instead.

The templates included with NexLog DX-Series™ are:
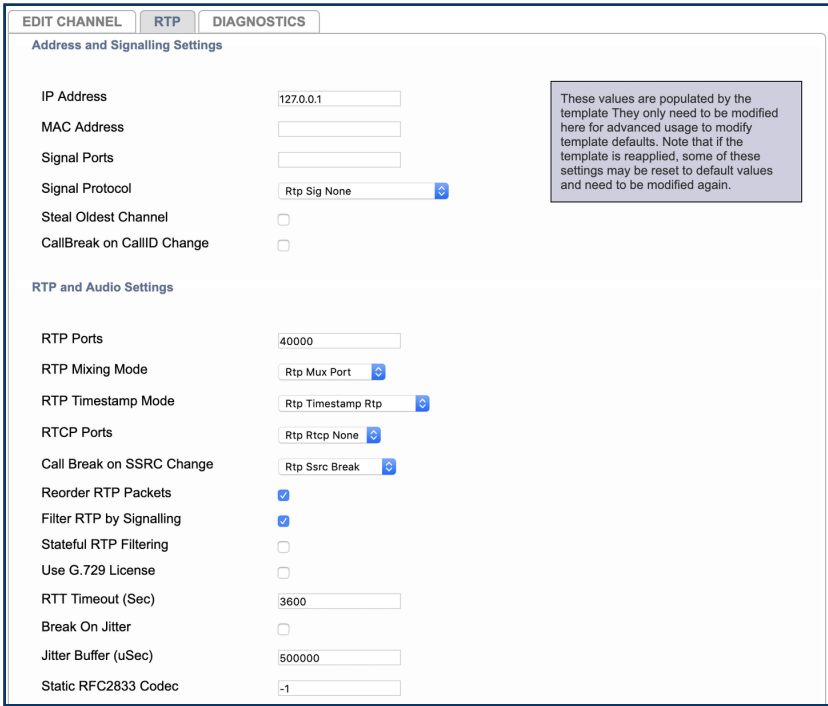
D.5. Cisco VoIP Template

Fig. D.4 **Cisco Callmanager "Skinny" Protocol (SPAN) Template**

To configure Cisco Callmanager with Local VoIP recording, use the Cisco Callmanager "Skinny" Protocol (SPAN) template. Enter the SCCP and RTP ports in use, and then enter an IP address (xxx.xxx.xxx.xxx) or MAC address (xx:xx:xx:xx:xx:xx) for each phone line in the system.

D.6. Local VoIP and RTP Channel configuration

Like other board types, configuration of channels on local IP boards is done on the Recording → Boards page by opening the board and then clicking the gear on the channel you wish to edit. The channel edit page has three tabs. The first is the standard Edit Channel tab. The second and third are RTP and Diagnostics.

D.6.1. RTP

Fig. D.5 **Top Half of Local IP Channel RTP Tab**

This tab allows you to configure all the RTP specific options detailed below in the Channel Parameters subsection of the Advanced Local VoIP Recorder configuration section of this chapter.

Fig. D.6 **Bottom Half of Local IP Channel RTP Tab**

D.6.2. Diagnostics

The third tab is Diagnostics. It displays diagnostic information showing what data is arriving for the channel and can be used to help troubleshoot whether the channel is configured properly.

Fig. D.7 **IP Channel Diagnostics Example**

Each channel has up to 4 RTP queues for incoming RTP queues and signaling queue. These queues show the number of packets that have arrived and been Enqueued, and the number that have been

Dequeued and handled. The remaining columns (Source, Dest, Elapsed, Codec, SSRC, Seq) display data about the most recent packet to arrive for that queue.

- Source: The ip address and port of the source of the packet.

- Dest: The IP address and port of the destination of the packet.

- Elapsed: How much time since the packet came in.

- Codec: How the audio was encoded. (RTP only)

- SSRC: Source Identifier. (RTP only)

- Seq: Sequence number of the packet. (RTP only)

When MUX is NONE, there will only be one RTP queue all packets to go. If MUX is DIR (one RTP queue will be for incoming packets and one for outgoing packets (relative to the IP address configured for the channel). If MUX is Port or IP_Port, queue assignments are made per port.

The Refresh button, as expected, refreshes the data displayed to be current.

D.7. Advanced Local VoIP Recorder configuration

The following information describes low level configuration of the built-in recorder based VoIP/RTP configuration, which is used for recording RoIP, NG9-1-1 "SIP Invite", and IP Dispatch Consoles.

D.7.1. VoIP: Edit Board

The board level parameters are accessible by clicking on the board name in the Recording Interfaces NexLog Configuration Manager page. The board is named "Local IP Recording." On that page the board can be configured to capture RTP traffic in different ways.

The UDP section is for configuring the virtual board to capture UDP packets addressed directly to the NexLog recorder's IP address.

The PCAP section is for configuring Promiscuous Mode Packet Capture. This capture method allows the recorder to capture traffic not addressed to its IP address.

D.7.2. Board Level Configuration Parameters

The following information lists the parameters and valid values that can be specified in board level configuration. (**Boldface** indicates a default value.) They are described in the sections that follow.

D.7.2.1. List of Board Level Parameters

- UDP Ports: port-list

- UDP Multicast Addresses: IP-address-list

- UDP Multicast Interface IP: IP-address

- SIP Endpoint Config: contact Eventide for usage

- PCAP Devices: eth0, eth1, eth2, etc.

- PCAP Ports: port-list

- PCAP Vlan: **unchecked (off)**, checked (on)

- PCAP Defragment: unchecked (off), **checked (on)**

- Packet Filtering: Bpf None, Bpf Port, **Bpf Full**

- Channel Count: number-of-channels-on-virtual-board

D.8. Device Information

PCAP Ports and UDP Ports: Specifies a port list (port numbers and/or port ranges) for ports to record. All ports that are used by all channels must appear in the list. The ports should also be specified in the channels specific pages. Valid Range: 1-65535. Format: To specify multiple port numbers, separate them with commas; for example: 1,2,3,5,9. To specify a port range, separate it with a hyphen or dash; for example: 1-3. To specify multiple port ranges, separate the ranges with a comma; for example:

1-3,7-12. To specify multiple port numbers and port ranges, separate each type with a comma; for example: 1,2,5,9,12-15,19,22-25,29,30. For readability and maintenance (and to avoid duplications), it is recommended that you specify port numbers in numerical order.

> **ⓘ Note**
>
> For **PCAP Ports**, the smaller the range, the better the performance, so it is a good practice to identify only those ports that will be used. The ports belong to VoIP devices such as IP phones, IP softphones, IP PBX ports, or other VoIP endpoints on the network that you wish to record. Any packet received by the recorder that uses ports in this list as either destination or source will make it past the filter and be processed by the recorder.

> **❗ Important**
>
> For UDP Ports**, it is very important to specify only the ports that will be used, because opening these ports will consume resources on the recorder. For example, specify 3,5 rather than 3-5 if port 4 will not be used.

UDP Multicast Addresses: Specifies one or more IP multicast group addresses from which to record. [Join or subscribe to.] Format: to specify multiple IP multicast group addresses, separate them with a comma; for example: 239.1.1.1,239.1.1.9.

UDP Multicast Interface IP: Specifies the IP address of the NexLog Recorder's network interface device which will be used to capture the multicast traffic.

SIP Endpoint Config: Specifies a special parameter to configure the NexLog Recorder as a SIP Trunk endpoint instead of its usual configuration as a "listen only" device. Contact Eventide Service for assistance in configuring this parameter.

PCAP Devices: Ethernet Device name. Specifies the NexLog Recorder's network interface device (NIC) containing the Ethernet port that will be used to record RTP data. Valid Values: eth0, eth1, etc. Typically, one Ethernet port on the recorder is used to record the VoIP traffic sent to the recorder and one port is used for bidirectional traffic with recorder clients, such as a PC with Eventide MediaWorks that is used for playback or live monitoring.

PCAP Vlan: Virtual Local Area Network. Enables the Packet Pre-Filtering (BPF) for use on a VLAN, which is often used with SPAN and RSPAN setups. This setting is used because the port/IP address information appears in a different location in packets depending upon whether the traffic is from a VLAN or LAN. Valid values:

· **unchecked**: Disabled (default), for use on a LAN.

· **checked**: Enabled, for use on a VLAN.

PCAP Defragment: Enables IP defragmentation. When disabled, only the first fragment is processed and subsequent fragments are ignored. It is usually unnecessary to enable IP defragmentation, because voice packets are typically small enough to avoid fragmentation, or if they are sent in multiple fragments, the necessary data is usually in the first fragment, and the rest can be ignored. (Fragmentation occurs when the payload results in a data packet size that is greater than the maximum transmission unit of the sending switch.) Valid values:

· **unchecked**: Disabled (default). No IP defragmentation is performed.

· **checked**: Enabled. IP defragmentation is performed.

D.8.1. Packet Filtering and Handling

Because networks carry many types of data packets that are bound for different destinations, the recorder uses a /*packet filtering*/ mechanism to detect and isolate the desired RTP audio data packets from other data types forwarded by the network to the recorder's Ethernet port.

Packet Filtering: Berkeley Packet Filtering. Specifies a source port pre-filtering method for capturing RTP packets. Packets are pre-filtered at the NexLog Recorder network interface. This can reduce the load on the recorder, which is especially important in saturated high-throughput networks. BPF is a method used to capture and filter packets from a network interface that is used in promiscuous mode. When the NexLog Recorder network interface is in promiscuous mode, it receives a copy of each RTP packet appearing on the port, which is then run through a filter, so that only packets of interest are passed to the recording application layer. This pre-filtering can reduce the traffic load on the recorder CPU (except when no filtering is used).

The following settings can be used:

· **Full**: (default) Accepts traffic from all source ports identified in the configuration by IP or MAC address or port number.

- **Port**: Accepts traffic from all source ports identified in the configuration independent of IP or MAC address. This setting is used when the IP addresses may change.

- **None**: No pre-filtering is performed. Accepts traffic from all source ports.

Typically, it is either set to FULL or to a list of ports, except when using dynamic channel mapping, in which case, it should be set to NONE or a list of ports.

D.8.2. Channel Parameters

The channel level configuration is accomplished the same way as other boards. Click on the plus sign (+) next to the board name to open the list of channels for a board. From there clicking on the gear icon will show the channel specific configuration. On the channel page there is an RTP tab where VoIP specific parameters can be changed. The settings include channel mapping parameters, which direct RTP packets from a specific IP address, MAC address, or port number to record on the specified channel (or which specifies dynamic channel mapping).

When a virtual board is added the virtual channels are added to the recorder and are assigned recorder channel numbers based on the channel numbering sequence. The channel numbering sequence starts with hardware based channels, beginning with installed telephony boards, followed by the channels on virtual boards in the order they were added via NexLog Configuration Manager. For example, if the recorder has 8 hardware-based channels, then the first virtual channel (Channel 1 of the virtual board) will be assigned to recorder channel 9.

D.8.3. Channel Configuration Parameters

The following information lists the channel configuration parameters and valid values that can be specified.

D.8.4. List of Channel Parameters

- IP Address: <IP-address>

- MAC Address: <MAC-address>

- RTP Ports: <port-list>

Signal Ports: <port-list>
·

· RTP Mixing Mode: **Rtp Mux None**, Rtp Mux Dir, Rtp Mux Port, Rtp Mux Ip Port, Rtp Mux Ssrc

· Signal Protocol: **Rtp Sig None**, Rtp Sig Sip Trunk, Rtp Sig Zetron Rds, Rtp Sig Cisco Forked, Rtp Sig Telex Ip223, Rtp Sig Telex Ip223 Trunked, Rtp Sig Efjohnson

· RTCP Ports: **Rtp Rtcp None**, Rtp Rtcp Odd, Rtp Rtcp Even

· Break on SSRC: Rtp Ssrc Nobreak, Rtp Ssrc Break, Rtp Ssrc Fuzzy

· Jitter Buffer (uSec): <millionths-of-second>

· CallID Field Name: <SIP-field>

· IP Field Name: <optional name of metadata field>

· Steal Oldest Channel: *unchecked (off)*, checked (on)

· Break On Jitter: *unchecked (off)*, checked (on)

· Custom Protocol Handling: *unchecked (off)*, checked (on)

· RFC2833 Codec: -1, <codec-number>

D.8.5. Channel Mapping

VoIP calls can be mapped to NexLog Recorder channels using the following options:

IP Address: Map the IP address of a VoIP device to a recorder channel using static channel mapping. Mutually exclusive with MAC address. A specific IP address can be used or Dynamic which can map VoIP calls to a bank of channels using a dynamic assignment that is controlled by other means, such as call control or custom programming. Used when the port range or IP address is variable or floats, such as with VoIP trunking (e.g., SIP trunking, where negotiation of the SIP phone call includes ports to use), or when using custom scripts or programming from Eventide. When used with SIP trunking, set channel 1 to the IP address of the SIP source (for example, the SIP PBX or the local SIP trunk endpoint), and set the other channels to Dynamic.

MAC Address: Map the MAC address of a VoIP device to a recorder channel using static channel mapping. Mutually exclusive with IP address.

RTP Ports: Map a set of ports on a device to a recorder channel using static channel mapping.

Signal Ports: Specifies the signaling ports when signaling is used (when Signal Protocol is set to a value other than Rtp Sig None). Like traditional telephone calls, VoIP calls offer **full-duplex communication**, which allows the connected parties or devices to communicate with each other in both directions at the same time. However, with VoIP, the full-duplex call is composed of two halves: a stream of audio packets that are transported from party A to party B and a stream of audio packets that are transported from party B to party A.

It is typical to record the combined conversation rather than each side separately. Mixing options allow you to merge both halves of the conversation into one channel, or to record each party on separate channels.

Each channel is associated with a MAC or IP address (or is dynamically assigned). Traffic to this address is considered inbound and traffic from it is considered outbound.

RTP Mixing Mode: Specifies the type of audio stream mixing for the recording. Valid values include:

- **Rtp Mux None**: (default) No mixing is performed. The channel must be set up to receive only a single RTP stream at any given time.

- **Rtp Mux Dir**: Mix inbound and outbound audio streams belonging to a VoIP device (that is, mix traffic going in both *directions*). Direction mixing is typically used with the PCAP method, because the audio streams could be coming in from any port in the range.

- **Rtp Mux Port**: Mix audio streams from multiple ports, where each port carries a separate audio stream. Port mixing is typically used with the UDP method.

- **Rtp Mux Ip Port**: Mix audio streams from a destination IP address and port. IP Port mixing is used with the UDP method or SIP Trunk signaling.

- **Rtp Mux Ip Ssrc**: Mix audio streams by detecting which stream a packet belongs to using the RTP packet's SSRC field. Only recommended in case where IP_PORT cannot be used due to multiple streams received on the same port

Signal Protocol: Specifies the type of signaling used. We recommend leaving it as set by the template used.

RTP packets contain information in their headers identifying the sources of the RTP data stream. This includes the following identifiers:

- **Synchronization Source (SSRC)**: A unique numeric ID for a unidirectional stream of RTP packets. The synchronization source within the same RTP session is unique.

- **Contributing Source (CSRC)**: A unique numeric ID identifying a contributing source for a mixed stream of RTP packets (a stream that has been generated from multiple sources). In some situations, it is used to identify a previous origin of a stream of RTP packets (that is, a previous SSRC).

These data are used to identify audio streams, and hence, the audio that belongs to a VoIP call.

In addition, the SSRC is also used to aid in identifying call termination. When the SSRC changes, it is an indicator that the audio stream from one party has ended. However, there may be cases where the SSRC changes briefly but does not indicate a separate call. This can result in a call being broken inappropriately into two parts or in a spurious call with a very short call length (e.g., 0 seconds). The following parameter is used to control call breaks for these different situations.

Break on SSRC: Controls how to handle SSRC changes in determining call termination. Valid values are as follows:

Rtp Ssrc Nobreak: When the SSRC changes, do not "break" the call.

Rtp Ssrc Break: (default) When the SSRC changes, "break" the call (that is, treat it as a new call).

Rtp Ssrc Fuzzy: When the SSRC changes, "break" the call. However, if the new SSRC is numerically close to the current SSRC, do not break the call. This setting is used with some VoIP implementations that have atypical SSRC changes, such as with certain configurations of Cisco Call Manager.

Jitter Buffer: Jitter Buffer Size in microseconds. Default: 2000000 (2 seconds). Range: 0 to 5000000 (5 seconds). The recorder uses a jitter buffer to enable proper synchronization and a smoother flow of data. The larger the jitter buffer, the higher the recorder memory usage, as well as the higher the load on the recorder CPU when jitter is encountered.

CallID Field Name: If this value is set to the name of a text metadata field that has been added to the recorder's database, and the signaling protocol from the PBX includes CallID information (a unique identifier assigned to the call by the PBX), then the CallID for the call will be attached to each call record by placing the CallID in this field.

RFC2833 Codec: Enables out-of-band digits when signaling is used.

-1: Disabled (default), no out-of-band digits.

<codec-number>: Enabled to receive out-of-band digits using the specified codec number used by the particular IP phone system (PBX and phones). Example: 128. The codec number is application-specific and can be obtained by checking with the manufacturer of the system or by analyzing the signaling data.

E. Archive Pairing

Archive Pairing is an archiving scheme created to put a focus on constant archiving to DVD-RAM. It takes advantage of two recorders to ensure all recorded data is archived. This appendix explains the requirements for Archive Pairing, how to set it up, and how it works.

E.1. Requirements

Archive Pairing requires two recorders. These recorders should have identical hardware profiles and software configurations, and must receive the same call input. Each recorder should have two DVD-RAM drives. The recorders should also be synced to the same time source, for example NTP, and be in the same network with the ability to communicate with each other. Additionally, an appropriate license is required for this functionality but this license is only needed on the "primary" recorder.

1. VoIP calls can be made on the Internet using a VoIP service provider and standard computer audio systems. Alternatively, some service providers support VoIP through ordinary telephones that use special adapters to connect to a home computer network.

2. VoIP services convert voice or audio data into a digital signal that travels over a computer network such as a company intranet or the Internet. If you are calling a regular phone number, the signal is converted to a regular telephone signal before it reaches the destination. VoIP can allow you to make a call directly from a computer, a special VoIP phone, or a traditional phone connected to a special adapter.

E.2. Operation

Archive Pairing enables the end-user to archive their data in a more streamlined way than traditional archiving with the benefits of system redundancy. With this feature enabled, recorded information will continue to archive on the next available DVD-RAM drive when a disc fills, the user manually stops archiving on a particular DVD-RAM drive, or if some external factor disrupts normal operation

of one of the loggers (such as a power failure). Flow between drives is automatic. The end-user simply has to flip or change out the media as the drives fill for constant coverage.

The functionality works by creating a global archive pointer that both recorders will use to determine what recorded data they should be archiving. The two recorders are referred to as the "primary" recorder and the "secondary" recorder. The distinguishing feature between them is that the primary recorder is where the Archive Pairing license must be entered.

With Archive Pairing enabled, DVD-RAM drives with formatted media will enter a state called "Standby". This means the drive is ready to archive as part of the Archive Pairing scheme. The first drive of the primary logger will automatically begin archiving at the point that is set to start at for that drive. This will establish the starting point for all archiving. The initial archive pointer should be set before any calls have occurred on the recorder but should also be no earlier than January 1st, 1989. There is no need to set the archive pointer for each drive, just the first one.

When a DVD-RAM media fills, it will automatically begin archiving where it left off on the next drive that is in Standby. Typically, the flow is first drive on the primary recorder, then the second drive on the primary, followed by the first drive secondary, and finally the second drive secondary. If an archive is manually stopped, archiving will automatically resume on the next available Standby archive. In the event that all drives are full, Archive Pairing will wait until new media is inserted, formatted, and enters Standby.

In the event that maintenance is to be performed on one or both of the recorders, a recorder can be shut down and worked on while the other recorder continues archiving from the point that the first recorder is shutdown, and then once the first recorder is back up and running, the same procedure can be performed on the other recorder. This method should be employed when upgrading to future software releases or for any required hardware maintenance.

1. VoIP calls can be made on the Internet using a VoIP service provider and standard computer audio systems. Alternatively, some service providers support VoIP through ordinary telephones that use special adapters to connect to a home computer network.

2. VoIP services convert voice or audio data into a digital signal that travels over a computer network such as a company intranet or the Internet. If you are calling a regular phone number, the signal is converted to a regular telephone signal before it reaches the destination. VoIP can allow you to make a call directly from a computer, a special VoIP phone, or a traditional phone connected to a special adapter.

E.2.1. Pairing Setup

Prior to setting up the software, the following items are assumed:

- Recorders are racked or placed with accordance to site specifications

- The software on the recorders is the same version on both.

- A valid license has been entered into the recorder

- The recorders are networked in the same IP network

- The recorders have the same call sources attached to both

- Eventide approved Blu-ray or DVD-RAM media is available

After the above is satisfied, the recorder should be configured to have the dates and time synced to the same external clock. The channels for both recorders should be configured the same and be properly recording. After that has been setup, insert blank Blu-Ray or DVD-RAM discs into the drives. Format them if required.

Before enabling Archive Pairing, the archive pointer of the first drive should be checked to make sure it will catch all calls. To view and set the archive pointer, in Configuration Manager expand the menu item Archiving and click Archive Configuration. Select the DVD-RAM 1 device and select the Configure button. On the resulting screen, select the TIME tab and observe the Archive Time. Make sure the date is before any calls have occurred but after 1/1/89. After you have a date/time you are satisfied with, select Save.

After the archive time has been set, add a license for Archive Pairing. A new menu option will become available via Configuration Manager as seen in the following image. The options are also available via the Front Panel Setup menu.

After the archive time has been set, add a license for Archive Pairing. A new menu option will become available via Configuration Manager as can be seen in the following image. The options are also available via the Front Panel Setup menu.

The Host field should contain the IP address of the secondary recorder. The User and Pwd fields should contain information for a valid administrator on the secondary logger. Once that information has been entered, check the Enabled box and click the Save button. The primary recorder will communicate with the secondary recorder to make sure the system is in sync. Drives that are in the

state "Idle, blank media" should become "Standby" on both recorders automatically. Archiving should also automatically begin on the first drive of the primary recorder.

Connect to Configuration Manager on the secondary recorder to set the remaining settings. Under Archiving and Archive Configuration, select the first DVD-RAM drive and click Configure. In the resulting window, check the Auto Start box then Save. Do the same for the second DVD-RAM drive.

After Auto Start has been enabled for both DVD-RAM drives, Archive Pairing configuration should be complete. The only thing that should require attention at this point is making sure media is flipped or replaced as needed to keep archived records up to date.