Eventide®

Communications Division

NexLog Best Practices

Monitoring Solutions

Part Number: 141280-01
Published: August 2, 2016

| *This page is intentionally blank* |

Overview

Reliable Information Technology equipment is vital to the successful operation of any mission critical contact center. NexLog Communication Recorders strive to be as reliable as possible and are built to run for over 10 years without maintenance. However, like all IT equipment external factors exist that are outside of the control of NexLog Communication Recorders. It is therefore recommended that users observe these best practices for monitoring a NexLog.

The NexLog Communication Recorder is considered an appliance server, due to its embedded operating system and all-in-one package. It primarily contains common components found in any rack mounted server. One benefit of using an appliance like sever is that it is calibrated for it's known hardware and software tolerances. This allows a properly configured server to notify personnel to take action when the unexpected happens. This makes monitoring a NexLog Communication Recorder easier then a standard server.

There are countless benefits gained from call recording in a mission critical environment; from training personnel to legal defense and life saving instant replay. This is all the more reason to ensure that recordings are there when you need them. The NexLog administrator should take these simple steps to insure that their NexLog is as reliable as possible.

While monitoring a server may sound like a daunting task, Eventide NexLog Communication Recorders make it easy by providing several 'out of the box' monitoring methods. This document will cover the best practices for setting up the following monitoring solutions:

- Simple Email Alerts
- Status Emails
- NexLog Monitoring Appliance
- Simple Network Management Protocol (SNMP)

Simple Email Alerts

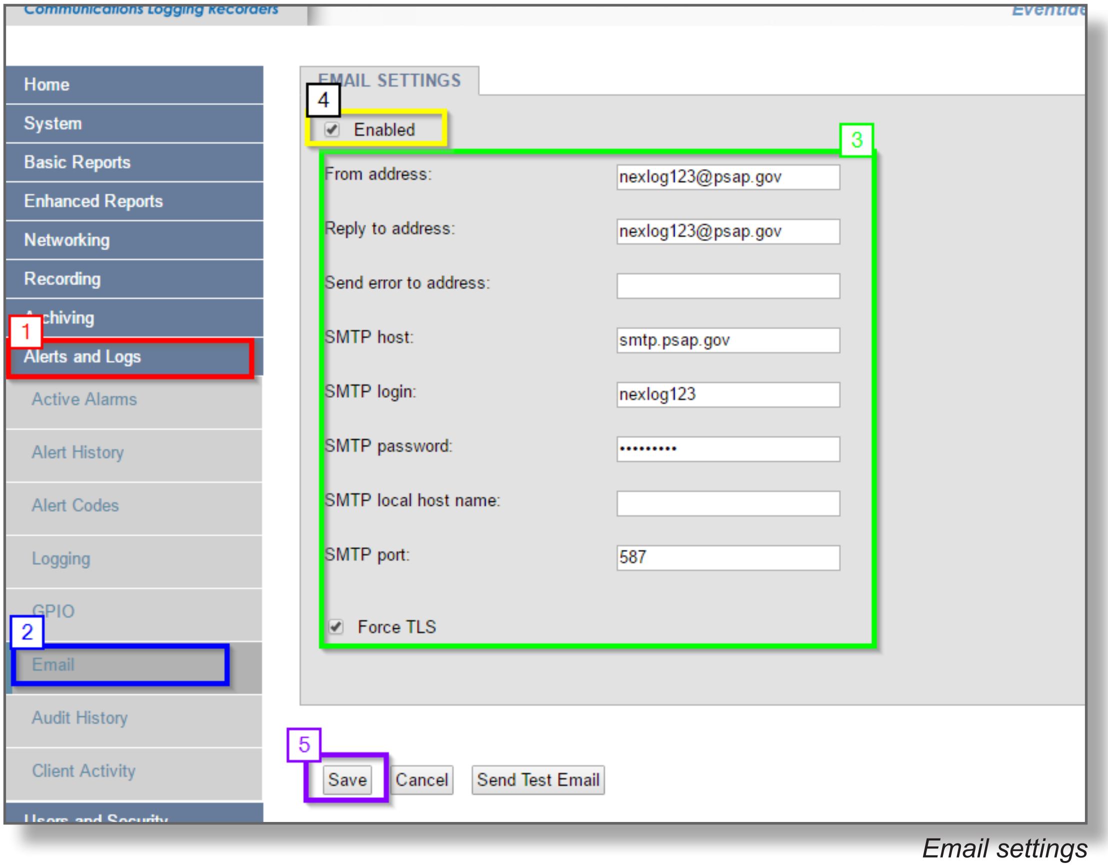
The easiest way to monitor a recorder's activity is via email alert notification. However, this method is only as reliable as the person receiving them. When an alert arrives in the destination's inbox, the recipient must decide the action that should be taken against it. This method is only practical for receiving a notification after an event has already occurred.

To set up email alerts, you will first need to set up the recorders SMTP email account.

Setting up the email account will require you to obtain the following information from your email provider:

From Address
SMTP Host
SMTP Login
SMTP Password
SMTP Port
TLS/SSL Required

Then navigate to the Configuration Manager and select (1) Alerts and Logs, then (2) Email. (3) Enter the details collected above into the fields provided. (4) Click Enable. (5) Press Save at the bottom of the page.



☑ Enabled

From address: nexlog123@psap.gov

Reply to address: nexlog123@psap.gov

Send error to address:

SMTP host: smtp.psap.gov

SMTP login: nexlog123

SMTP password: •••••••••

SMTP local host name:

SMTP port: 587

☑ Force TLS

Email settings

Once the SMTP account has been set up, you will need to enter an email address for the alert recipient. To do this, Navigate to Users and Security, then Users. Select the username that you would like to add an email address to. Then click Edit User at the bottom of the page.

On the User Info tab, you will see a field for Email at the end of the list. Enter the recipient's email address and click Save.

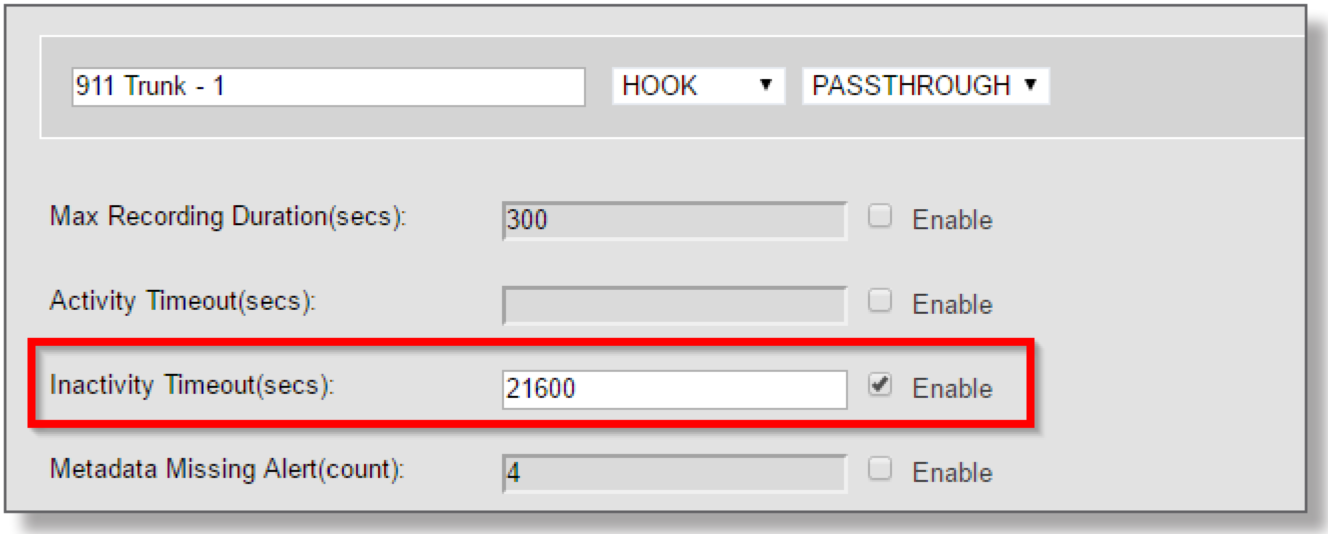
Once the recipient has been added, navigate to the Email Settings and press Send Test Email at the bottom of the page. If the test email was received (Code 25) then your emails have been configured successfully.

At this stage, you have successfully set up hardware monitoring to send email alert notifications to your defined recipient. This will alert you of hardware conditions after they occur. **Keep in mind that these alerts can not be sent during a loss of power or network communication.**

Monitoring Recording Activity

Any mission critical channels should be monitored for inactivity timeouts. Before setting this up, you should have a clear idea of which recorded channels are most important, and how often a recording should occur on them.

In the Configuration Manager, navigate to Recording, then Boards. Click on the ⚙ for the channel you would like to set an inactivity alert for. Enable the field and enter the timeout in seconds. In the example below; "911 Trunk - 1" will alarm if it does not record for 6 hours.



911 Trunk - 1 | HOOK ▾ | PASSTHROUGH ▾

Max Recording Duration(secs): 300 ☐ Enable

Activity Timeout(secs): ☐ Enable

Inactivity Timeout(secs): 21600 ☑ Enable

Metadata Missing Alert(count): 4 ☐ Enable

Channel settings

The following alert types are configurable on a per channel basis from the channel settings page.

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. It 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 billed) 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 set, alert #59 (“The Metadata feed for <channel> appears to be missing. X calls were recorded without providing metadata.”) is issued if the consecutive count of calls have been recorded and metadata was not tagged to them. The factory default is to disable this function.

This setting does not affect the actual recording of the call. It simply issues an alert. Metadata Missing Alert is useful for alerting you to a disconnected CDR or ANI/ALI feed. If you are going enable this alert, then you should set this count to one that is longer than reasonably expected to avoid nuisance alerts. For example, if recording in a 911 call center, administrative calls may not receive CDR or ANI/ALI. The value should be higher than the number of consecutive administrative calls the call-taker would answer.

Status Emails

Simple Email Alerts are one of the most basic monitoring options provided. They alert you of a problem or system concern after it has already occurred. This is because every environment is unique and we can't predict exactly when YOU should act. The standard hardware and software alerts are set based on the feedback end-users have provided us with.

When your environment does not fit the default settings, it's time for you to move your proactive monitoring to the next level. With Status Emails, you can receive an email at your specified interval informing you of the NexLog's system statistics.

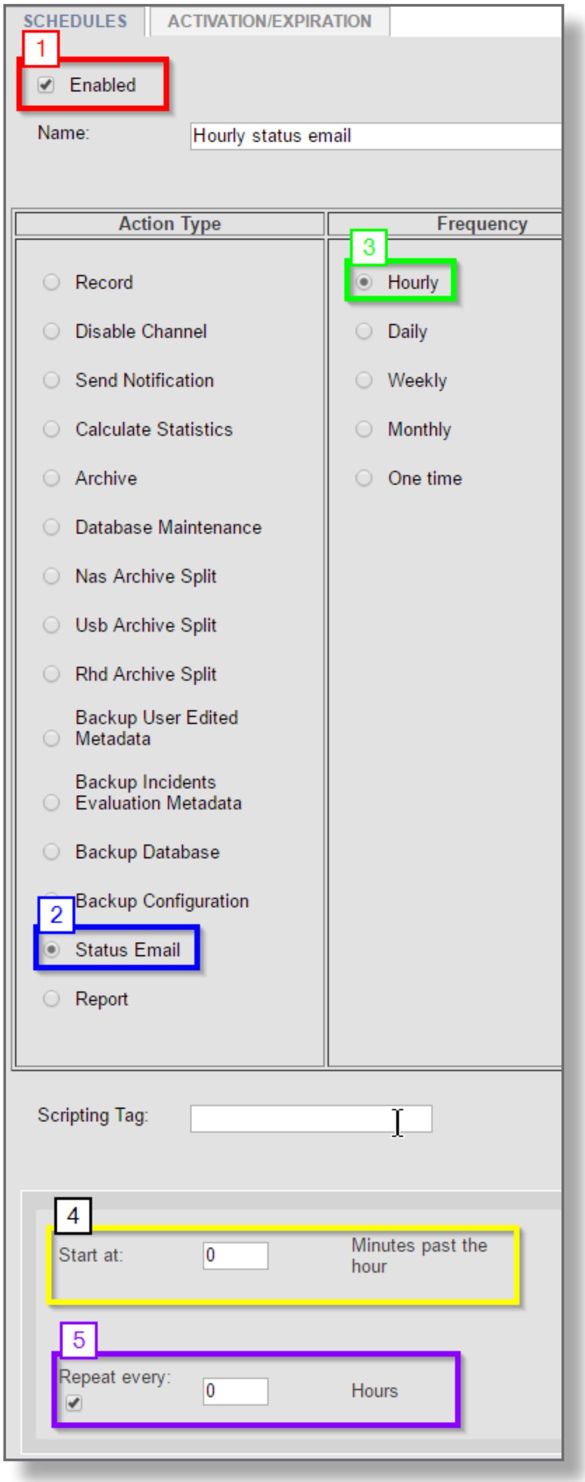
To set up the Status Emails:
Log in to the Configuration Manager and navigate to Utilities, then Schedules. Click Add at the bottom of the screen.

(1) Click the Enable check box at the top, (2) then select "Status Email" in the list on the left. (3) Set your desired interval from the right side list. If choosing Hourly, (4) set the minutes past the hour to whatever is desired. (5) To repeat every hour; check the "Repeat every" options and enter 0 for Hours. Enter a 1 in the hours field if you only want the Status Email every other hour.

To set the Status Email recipient, navigate to Email Settings and enter the recipient's email address in the "Send error to address" field.

The Status Email will provide you with

- IP Address Details
- Current UTC Timestamp
- Last 100 Alerts
- Call Count by Channel Number for the Last Hour
- Call Count by Resource Name for the Last Hour
- Last Recording Archived
- Load Statistics
- HDD utilization
- Running Processes



SCHEDULES | ACTIVATION/EXPIRATION

1 ☑ Enabled

Name: Hourly status email

Action Type:

- ○ Record
- ○ Disable Channel
- ○ Send Notification
- ○ Calculate Statistics
- ○ Archive
- ○ Database Maintenance
- ○ Nas Archive Split
- ○ Usb Archive Split
- ○ Rhd Archive Split
- ○ Backup User Edited Metadata
- ○ Backup Incidents Evaluation Metadata
- ○ Backup Database
- ○ Backup Configuration
- 2 ● Status Email
- ○ Report

Frequency:

- 3 ● Hourly
- ○ Daily
- ○ Weekly
- ○ Monthly
- ○ One time

Scripting Tag:

4 Start at: 0 Minutes past the hour

5 Repeat every: ☑ 0 Hours

Schedules configuration

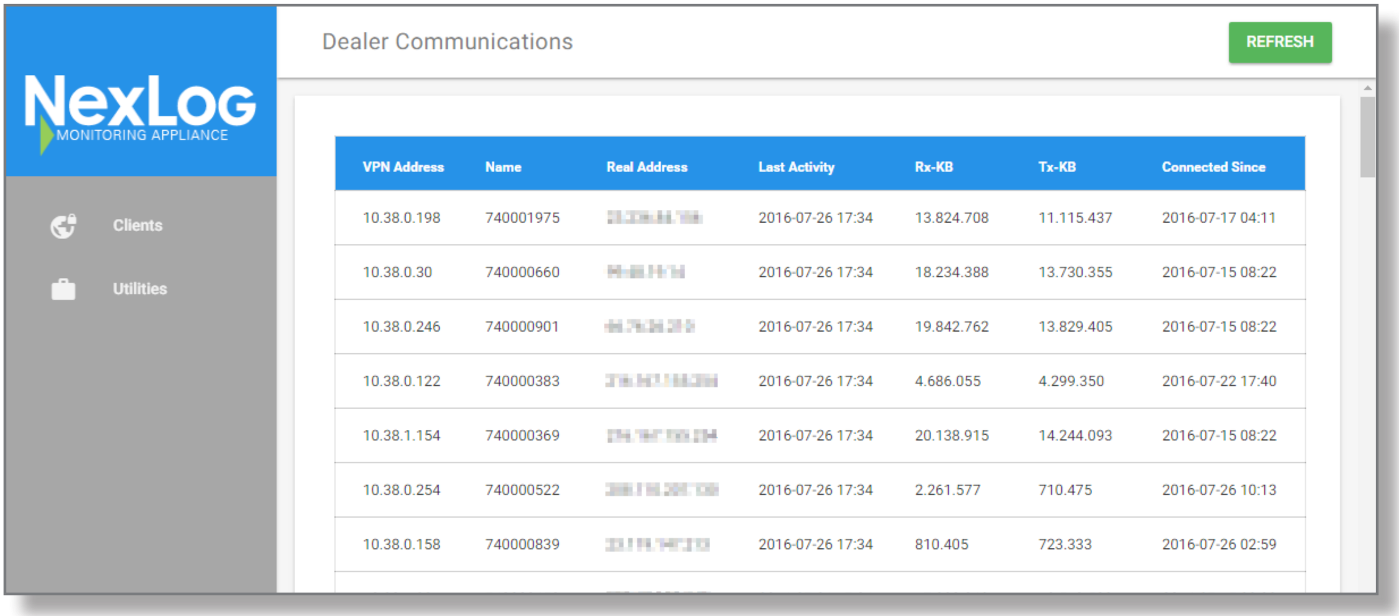
NexLog Monitoring Appliance (NMA)

When remote monitoring and administration of multiple NexLog recorders is required, the NexLog Monitoring Appliance (NMA) should be deployed.

The NexLog Monitoring Appliance (NMA) is a virtual machine designed to be run on a virtual machine platform such as VMWare, Citrix XenServer, or Microsoft Hyper-V. The NMA can also be deployed in a cloud environment using Amazon AWS, or Microsoft Azure.

The NMA is used for monitoring Eventide NexLog recorders over the Internet via a Virtual Private Network. NexLog recorders connected to the NMA can only be accessed via the NMA itself or another system designated as the control system. A control system can be a dealer technician or a third party monitoring appliance. NexLog recorders connected to the NMA are not accessible via other recorders also attached to the NMA.

Once a NexLog recorder is connected, a connected control system can monitor the it via SNMP, connect to the Configuration Manager to make configuration changes or connect to MediaWorks Plus to play back calls.



VPN Address	Name	Real Address	Last Activity	Rx-KB	Tx-KB	Connected Since
10.38.0.198	740001975	[redacted]	2016-07-26 17:34	13.824.708	11.115.437	2016-07-17 04:11
10.38.0.30	740000660	[redacted]	2016-07-26 17:34	18.234.388	13.730.355	2016-07-15 08:22
10.38.0.246	740000901	[redacted]	2016-07-26 17:34	19.842.762	13.829.405	2016-07-15 08:22
10.38.0.122	740000383	[redacted]	2016-07-26 17:34	4.686.055	4.299.350	2016-07-22 17:40
10.38.1.154	740000369	[redacted]	2016-07-26 17:34	20.138.915	14.244.093	2016-07-15 08:22
10.38.0.254	740000522	[redacted]	2016-07-26 17:34	2.261.577	710.475	2016-07-26 10:13
10.38.0.158	740000839	[redacted]	2016-07-26 17:34	810.405	723.333	2016-07-26 02:59

NMA landing portal

To obtain the NexLog Monitoring Appliance virtual image, contact Eventide Dealer Support.

For operation instructions, see the NexLog Monitoring Appliance Manual (P/N:142379-01)

Simple Network Management Protocol (SNMP)

Advanced monitoring is available on-site or via the NexLog Monitoring Appliance using Simple Network Management Protocol (SNMP).

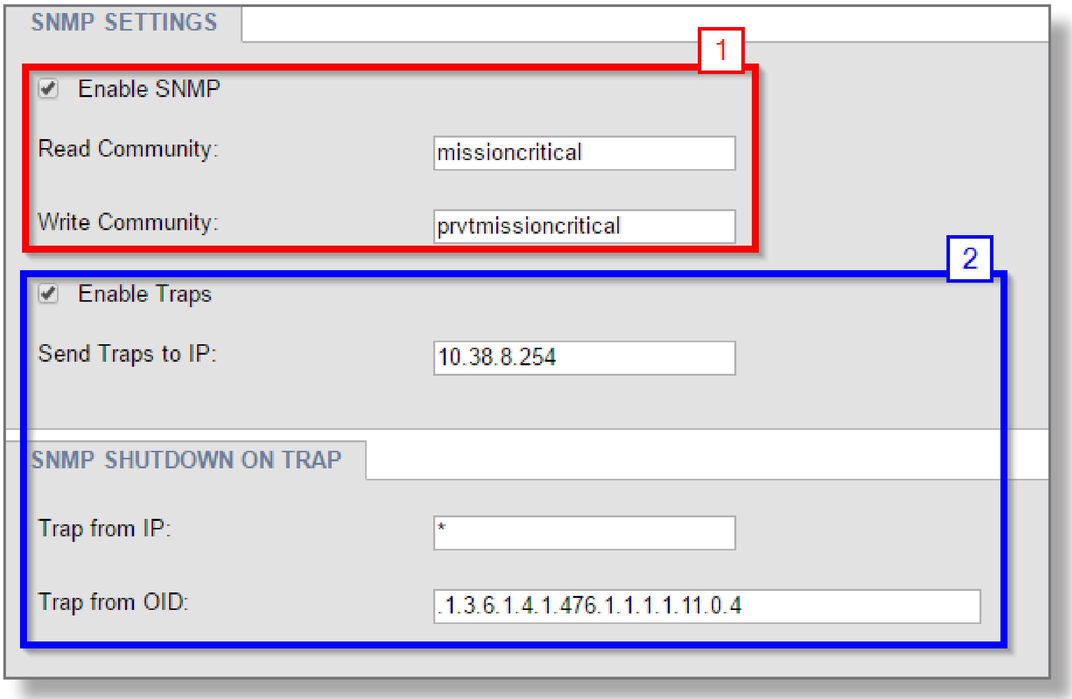
SNMP provides a standard mechanism for System Administrators to manage devices over an IP Network. Many third party commercial and free utilities and consoles exist for monitoring systems using the SNMP Protocol.

NexLog recorders provide a simple subset of SNMP functionality using basic Linux and PostgreSQL profiles.

A custom Eventide NexLog Management Information Base (MIB) file is available for integrations to your SNMP system. To obtain a copy, contact Eventide Dealer Support.

To set up SNMP on a NexLog recorder, log in to the Configuration Manager and navigate to Networking, then SNMP Settings. Check the option to enable SNMP and enter your desired read and write community names. 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 the user manual which provides a USB connection to the recorder. More power 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 when received, in the "Trap from OID" box.



SNMP SETTINGS

☑ Enable SNMP

Read Community: missioncritical

Write Community: prvtmissioncritical

☑ Enable Traps

Send Traps to IP: 10.38.8.254

SNMP SHUTDOWN ON TRAP

Trap from IP: *

Trap from OID: .1.3.6.1.4.1.476.1.1.1.1.11.0.4

SNMP settings

General Purpose Input/Output (GPIO)

Some environments may require a hardware notification for NexLog recorder conditions. This may be a warning light in an Air Traffic Control tower, or a buzzer in a busy call center. For these situations, a GPIO trigger may be the perfect companion to a proactive monitoring solution. A GPIO trigger is a relay that closes a circuit based on defined alerting conditions.

Eventide NexLog Communication Recorders use the National Instruments PCI-6503 Board (24-Channel) for all GPIO functions. The board has uses TTL signaling and has a maximum I/O rating for each line of −0.5 V to 5.5 V/2.4mA with respect to GND. Eventide nor National Instruments are liable for any damages resulting from signal connections that exceed these maximum ratings.

For detailed specifications, refer to PCI-6503 on the National Instruments web site (www.ni.com). For NexLog configurations, consult the latest NexLog manual available with your software version or contact Eventide Dealer Support.

GPIO licenses are available for the NexLog in *12 Input/12 Output* and *24 Input*. For monitoring purposes, you would need the *12 Input/12 Output* license. This means that you can configure up to 12 hardware alert conditions. By default, alerts of severity 3 or 4 (Error or Severe) will trigger a signal on the first output pair of the board.

The static port assignments on the PCI-6503 are as follows.

Input pins 0–7: Port A (PA0–PA7); odd numbered pins 47 to 33
Input pins 8–11: Port C upper nibble (PC4–PC7); odd numbered pins 7 to 1

Output pins 0–7: Port B (PB0–PB7); odd numbered pins 31 to 17
Output pins 8–11: Port C lower nibble (PC0–PC3); odd numbered pins 15 to 9

PC7	1	2	GND
PC6	3	4	GND
PC5	5	6	GND
PC4	7	8	GND
PC3	9	10	GND
PC2	11	12	GND
PC1	13	14	GND
PC0	15	16	GND
PB7	17	18	GND
PB6	19	20	GND
PB5	21	22	GND
PB4	23	24	GND
PB3	25	26	GND
PB2	27	28	GND
PB1	29	30	GND
PB0	31	32	GND
PA7	33	34	GND
PA6	35	36	GND
PA5	37	38	GND
PA4	39	40	GND
PA3	41	42	GND
PA2	43	44	GND
PA1	45	46	GND
PA0	47	48	GND
+5V	49	50	GND

PCI-6503 pinout mapping

Analog Channel Card Relay

All analog channel cards have an output relay on pair 25. This relay is non-configurable and can be used to determine if the NexLog is powered on, or if the channel card has failed.

8CH and 16CH cards include a configurable relay on pair 24.

Conclusion

This document has covered all of the monitoring solutions, but which one should you choose?

On-Site NexLog Administrator

If you are managing NexLog recorders on a single network, our best practice monitoring recommendation for you is SNMP. There are a countless number of free (open-source) and commercial SNMP solutions that will allow you to monitor your NexLog recorders as well as the other devices on your network.

Eventide is not affiliated with nor do we offer any warranties or guarantees, expressed or implied for any third party SNMP server. As of this document's publication, *Nagios* remains the number one solution in the open-source category. Other options for open-source are *Zenoss*, *OpenNMS*, *Splunk*, and *PandoraFMS*. For a commercially supported free solution, *SpiceWorks* is available. SpiceWorks is able to monitor most devices on your network with little configuration. WhatsUp, SolarWinds, and HP OpenView are a few options for contracted commercial solutions. We encourage you to do your own research to find a product that fits your environment.

Eventide NexLog Dealer

A dealer managing multiple NexLog recorders spread across a large geographic area on their own independent networks, should use a combination of a NexLog Monitoring Appliance with SNMP, and Status Emails.

All deployed NexLogs should connect via VPN to the NMA for monitoring (where allowed). An SNMP monitoring server should be set up and connected to the NMA to monitor each connected recorder. See the section above for a list of potential SNMP servers. This would alert the dealer of any current or potential system issues. Status Emails should also be sent hourly to a monitored email account. Your monitoring system should be configured to alert you if a Status Email was not received.

Most management system also allow ping monitoring. Enabling this would allow alert you as soon as a NexLog recorder goes offline.

If you have any questions regarding the configuration of the NexLog's monitoring components, please contact Eventide Dealer Support.

| *This page is intentionally blank* |

~ End of Document~