Eventide™ Communications

Critical Insights AI

Implementation Guide

Version 2025.2[6460]

P/N: #142447

P/N: #142447 Version 2025.2[6460]

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

www.eventidecommunications.com

Table Of Contents

1. About This Document

2. Audience

3. Assumptions

4. Terminology

5. Related Documentation

6. Critical Insights AI Overview

6.1. CIAI Feature Overview 18

7. CIAI Licensing

8. CIAI Deployment Requirements Overeiew

8.1. Eventide Communications Deployment Tasks 23

8.1.1. CIAI Hosting and Setup 23

8.1.2. Licenses Included in CIAI Service Purchase 23

8.2. CIAI Service Provider Deployment Task Summary 24

9. Deploying Critical Insights AI

9.1. Completing the Pre-Sales Checklist Form 27

9.2. Placing the Purchase Order 27

9.3. Completing the CIAI SaaS Deployment Form 28

9.4. Receiving the CIAI SaaS Deployment Card 29

9.5. Configuring the Source Recorder 31

- 9.5.1. Verifying Source Recorder Firmware 32
- 9.5.2. Adding the CloudSync License 32
- 9.5.3. Configuring Networking for the On-Premises Recorder 33
- 9.5.4. Configuring Recording 35
- 9.5.5. Verifying Recording 35
- 9.5.6. Configuring the CloudSync Connection 36

10. Configuring the CIAI User Interface

10.1. Changing the CIAI Service Provider Administrator Account Password 41

10.2. Verifying Transferred Recordings 41

10.3. Creating User Accounts 42

10.3.1. Configuring User Permissions 44

10.3.2. Configuring Account Settings 46

10.3.3. Configuring Resource Permissions 47

10.3.4. Configuring Search Filters 48

10.3.5. Verifying Access to User Accounts 49

10.3.6. Verifying User Permissions 50

10.4. Creating Resource Groups 50

10.5. Configuring Transcriptions 56

10.5.1. CIAI Background Transcriptions 56

10.5.2. Manual Transcriptions 58

10.5.3. Configuring Boost 59

10.6. Configuring Retention Settings 63

10.7. Configuring Custom Fields 65

10.8. Configuring NexLog Reports 69

10.9. Configuring CIAI User Interface Default Settings 70

10.9.1. Adding Default Header Columns 70

10.9.2. Displaying and Docking the Call Properties Pane 71

10.9.3. Displaying Default Tabs 72

10.9.4. Displaying the Transcriptions Tab 72

10.9.5. Displaying Transcriptions in the Timeline 76

10.9.6. Saving the Current Header Columns Layout as Default 77
10.9.7. Running Queries with AI Research Assistant 78
10.9.8. Verifying Resource Groups 80
10.9.9. Adding Call Type Icons 80
10.9.10. Applying the Default Configuration to New Users 84
10.9.11. Applying the Default Configuration to Selected Users 84
10.10. Monitoring and Alerts 85
10.10.1. Configuring Email Alerts 85
10.10.2. Exporting and Importing Alerts 90
10.10.3. Exporting Logs 90
10.10.4. Monitoring with NMS 92
10.10.5. Setting Up NMS Monitoring 94

11. Onboarding Customers and End Users

12. Troubleshooting

13. Contact Information

1. ABOUT THIS DOCUMENT

This configuration, support, and maintenance guide is intended for Eventide Communications™ reseller (a.k.a. CIAI Service Provider) technicians and provides step-by-step instructions to configure, deploy and support Critical Insights AI (a.k.a. CIAI) and its applications and services from Eventide Communications for NexLog™ DX-Series recorders.

For this deployment, Eventide Communications and the reseller each have differentiated sets of configuration tasks to perform. Eventide Communications (EC) is responsible for the initial set of pre-deployment tasks, comprising hosting and account services. These tasks will be completed before the reseller technician begins deployment tasks.

Where appropriate, this document will reference related supporting documentation, including the NexLog DX-Series DX User Manual.

This page was intentionally left 99.88% blank.

2. AUDIENCE

This document is intended for Eventide Communications reseller technicians who will use it as a guide to configuring, deploying, and supporting Critical Insights AI (CIAI) for NexLog DX-Series recorders.

This page was intentionally left 99.88% blank.

3. ASSUMPTIONS

CIAI Service Provider responsibilities include high and low-level configuration of the on-premises NexLog DX-Series recorder and the CIAI portal, which is based on MediaWorks DX. Administrator-level knowledge of the Web Configuration Manager and the MediaWorks DX playback UI is assumed.

The CIAI Service Provider technician will be in possession of all required connectivity and licensing information, including any optional addon licenses, additional documentation, and other required information items for the deployment, such as custom configuration requests from the customer.

This page was intentionally left 99.88% blank.

4. TERMINOLOGY

This section explains how specific terms are used in this document, including any variations, interchangeable terms, or custom definitions applied in the context of the CIAI product. Critical Insights AI: The Eventide Communications platform for storage, research, AI analysis of data, reporting, Quality Assurance, and more. Critical Insights AI is not a recorder but ingests data from a source recorder.

CIAI: Abbreviation for Critical Insights AI. Refers to both the CIAI product as a suite of functional components, including AI tools, and to the web service or web-based user interface that a user signs into for searching, playback and research.

CIAI User Interface: Refers specifically to the web-based user interface used to access recordings, Reports, QA, and administrative configuration settings. This user interface is based on the NexLog MediaWorks DX user interface and is commonly just referred to as CIAI.

CIAI SaaS Deployment Form: A form jointly completed by a CIAI Service Provider and the customer with respect to a specific CIAI customer deployment.

CIAI SaaS Deployment Card: Information returned to a reseller that contains credentials and access information for a specific CIAI customer deployment.

CIAI Service Provider: The trusted reseller who provides support and services to the end user. Providers are typically a combination of Tier 1 and Tier 2 type support roles. EC provides CIAI in collaboration with its trusted resellers. A trusted reseller may also be referred to as the 'Service Provider'.

CloudSync: The CaaS capability to securely transfer information to an EC SaaS device. See 'CaaS'.

CaaS: Refers to the technology that EC uses to transfer recordings and metadata from one device to another. This is CloudSync or the Centralized Archive transfer technology used in NexLog recorders.

EC: Informal abbreviation for the organization Eventide Communications LLC.

PO: Purchase Order. The PO commits the customer to the CIAI service.

Recorder: The device or 'source' from which the information was captured. This is usually a NexLog DX-Series device. The web-based CIAI device is not a recorder. Rather, it ingests recordings from the recorder.

Resource Groups: A group of resources or channels either on CIAI or NexLog recorder. Used interchangeably in this document with the term ‘Channel Groups’.

5. RELATED DOCUMENTATION

Related customer-facing documentation for the Critical Insights AI suite of applications includes:AI Research Assistant Quickstart User Guide

- QA Assistant Quickstart User Guide
- Supervisor Assistant Quickstart User Guide
- Enhanced Reports Manual
- NexLog documentation
- MediaWorks documentation

In addition, the NexLog DX-Series User Manual is available and will be referred to as a foundational reference document. It is located in the Web Configuration Manager under Utilities → Documents.

This page was intentionally left 99.88% blank.

6. CRITICAL INSIGHTS AI OVERVIEW

Critical Insights AI from Eventide Communications™ is a SaaS Service that comprises a suite of AI-based software productivity tools used to help PSAPs increase their productivity and achieve regulatory compliance goals. These tools are made available from Critical Insights AI, the new web-based CIAI user interface (hereinafter referred to as CIAI), which is based on MediaWorks DX.

The CIAI UI is virtually identical in appearance to the standard familiar MediaWorks DX UI and retains most of its standard features. However, CIAI has been modified and features some important differences, taking advantage of AI and other enhanced features of NexLog DX-Series recorders.

> **Note**
>
> A principal difference between the CIAI Service and MediaWorks DX is that the CIAI Service running on the cloud-hosted machine does not have recording capabilities, i.e., it is not a recorder. Rather, it ingests recordings from either a NexLog DX-Series recorder, an Eventide Communications Secure Edge Capture Device, or other third-party recording solution, such as Webex API.

CIAI is currently deployed as a SaaS offering in Amazon Web Services (AWS), hosted by Eventide Communications, and employs a single deployment model dedicated to each agency (rather than being a multi-tenant environment). This means customers' data is partitioned off from that of other customers, security-wise.

Future deployments that support appliance-based NexLog™ DX-Series recorders (i.e. on-premises) and virtual appliances (VMs) are anticipated, and will be made available in due course, coinciding with the evolving Eventide Communications product road map.

For more information about on-premises deployments, Contact Eventide Communications Sales.

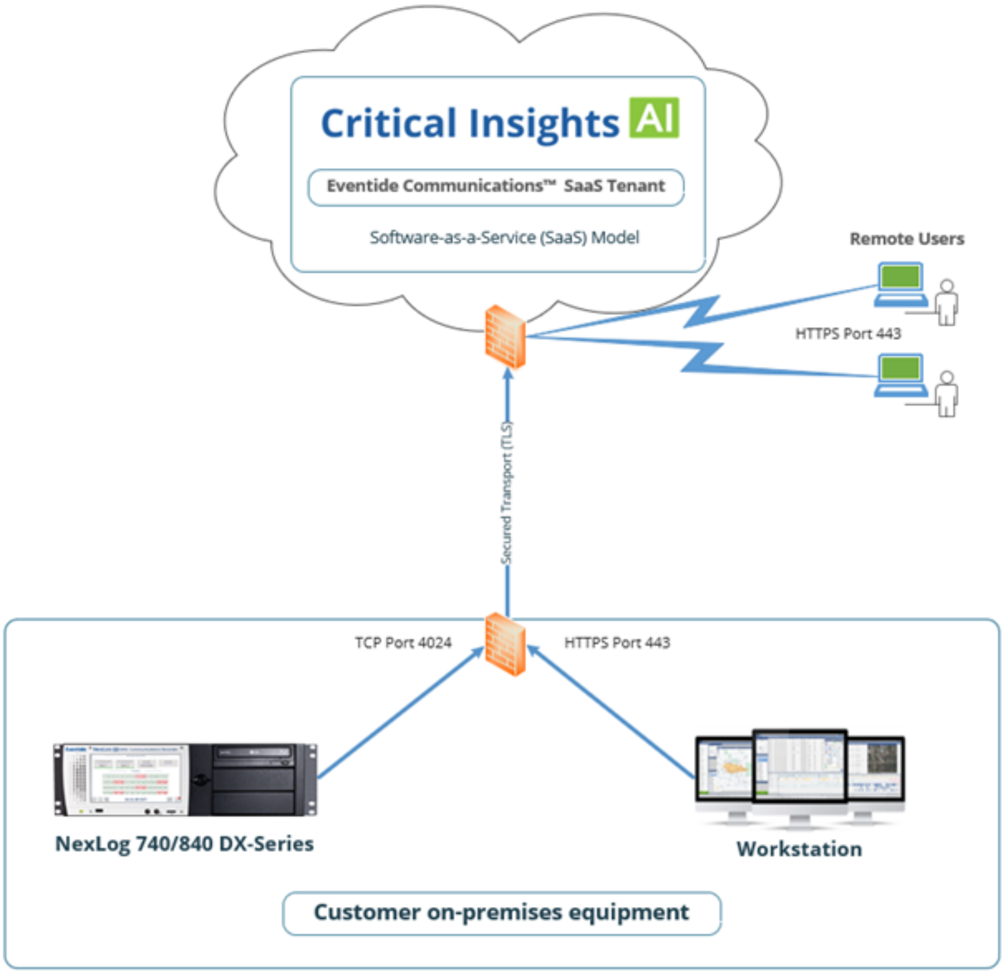


Fig. 6.1 **Critical Insights AI**

6.1. CIAI Feature Overview

Feature-wise, CIAI functionality and capabilities include:

- Centralized access for the transfer and replication of call recordings and metadata to the CIAI SaaS user interface from one or more NexLog DX-Series recorders.
- End user access to recordings and media from geographically-dispersed source recorders and ability to replicate recordings to CIAI, a single centralized location.
- Metadata tagged to calls based on insights derived from NexLog recordings.
- AI-based agents called "Assistants" that help users with various tasks.

There are four types of assistants:

AI Research Assistant:

- Locate specific recordings or search for calls by using keyword search analysis.
- Build incidents, analyze call transcripts, or conduct research for police or legal investigations and Freedom of Information Act (FOIA) requests.

QA Assistant:

- Facilitate 911 agent call-handling QA evaluations for compliance with state and local regulatory reporting and auditing requirements, e.g., 911 telecommunicator training mandates. Runs in the background.
- Increase situational awareness during 911 calls.

Supervisor Assistant: Used for the following PSAP agency objectives:

- Assist agencies with reporting and auditing requirements to maintain agency operational standards
- Assist with staffing management decisions.
- Report on agent health and well-being through voice sentiment analysis.

Library Assistant:

- Enable assignment of tasks to the Library Assistant when evaluating a transcript.
- Run tasks automatically: directs the AI Assistant to automatically evaluate transcripts.
- Enable users to assign tasks to AI when performing Agent QA evaluations.

Note

The Library Assistant is internally configured and runs in the background. It does not have a customer-facing user interface.

This page was intentionally left 99.88% blank.

7. CIAI LICENSING

Required and optional licenses for the CIAI SaaS user interface are installed by Eventide Communications Service technicians during the pre-deployment phase. Licensing is based on the quoted call capacity and is evaluated yearly.

If capacity is exceeded, EC will contact the Service Provider. EC will install yearly licenses after receiving payment. The CIAI purchase includes the client-side CloudSync license. The CIAI Service Provider will be responsible for installing the following client-side CloudSync license on the source NexLog DX-Series recorder.

- DX936-NexLog CloudSync (Client-Side).

To add this license, see Section 9.5.2 - Adding the CloudSync License.

The next chapter details deployment requirements.

This page was intentionally left 99.88% blank.

8. CIAI DEPLOYMENT REQUIREMENTS OVERIEW

This section provides an overview of the CIAI deployment requirements. For this deployment, Eventide Communications and CIAI Service Provider have differentiated sets of responsibilities and tasks. Eventide Communications is responsible for initial CIAI setup and pre-deployment tasks, including AWS hosting and allocation of Microsoft Azure resources. CIAI Service Providers are responsible for configuring CIAI.

8.1. Eventide Communications Deployment Tasks

Eventide Communications service technicians are responsible for completing the following required tasks:

8.1.1. CIAI Hosting and Setup

- Configuration of TLS (HTTPS) access Configuration of the cloud-hosted CIAI Service with unique credentials for the CIAI Service Provider Administrator
- Configuration of TLS (HTTPS) access
- Configuration of NTP
- Configuration of AI Technologies (e.g., AI Assistants)
- Enabling Transcription (SFAI)

8.1.2. Licenses Included in CIAI Service Purchase

EC is responsible for installing the following product licenses for the CIAI Service.

- CIAI - Critical Insights AI
- VM740DX-TB - NexLog Cloud Sync Subscription
- DX929 - Speech Factor AI Transcribe
- 271077/271082 Quality Factor Base Software 20x
- 271111-MP3 Audio Creation
- 271167 Packaged Player Incident Export (on/off)

- DX949- 911 Call Handling Report
- 271098-Geolocation Features
- DX985/115021-NexLogDX Advanced Analytics Reporting/Enhanced Reports
- 271098-GeoLocation Features

EC also allocates appropriate customer storage space (as per the CIAI Pre-sales Checklist).

8.2. CIAI Service Provider Deployment Task Summary

For CIAI Service Providers, deploying CIAI consists of both administrative and technical tasks. The following items in this Section represent a checklist of the technician's tasks, which are thoroughly detailed in the relevant listed document sections:

Step 1: Pre-Sales

Complete the CIAI Pre-sales Checklist Form and email it to: broberts@eventidecommunications.com. See Section 9.1 - Completing the Pre-Sales Checklist Form

Step 2: Ordering Process

Place a Purchase Order (PO) by contacting: loggers@eventidecommunications.com. See Section 9.2 - Placing the Purchase Order

Step 3: Gathering Site Information

Upon processing the PO, EC will email the CIAI SaaS Deployment Form. Complete the form in conjunction with the customer's requirements. The reseller will return the form to EC via email. See Section 9.3 - Completing the CIAI SaaS Deployment Form

Step 4: Receiving the CIAI SaaS Deployment Card

This document contains essential CIAI sign-in credentials and licensing and configuration information for connecting to the CIAI user interface. See Section 9.4 - Receiving the CIAI SaaS Deployment Card

Step 5: Transferring Recordings

Configure the source on-premises NexLog DX-Series recorder for the CIAI deployment. The CIAI instance will be available when you receive the CIAI SaaS Deployment Card. This is usually sent within 1-2 business days of receiving the CIAI SaaS Deployment Form.

To configure CIAI on the NexLog recorder and transfer recordings

1. Verify the source recorder firmware. See Section 9.5.1 - Verifying Source Recorder Firmware.
2. Add the CloudSync license. See Section 9.5.2 - Adding the CloudSync License.
3. Configure networking for the on-premises recorder. See Section 9.5.3 - Configuring Networking for the On-Premises Recorder.
4. Verify connectivity. See Section 9.5.3.1 - Verifying Connectivity.
5. Configure Recording. See Section 9.5.4 - Configuring Recording.
6. Verify Recording. See Section 9.5.5 - Verifying Recording.
7. Configure the CloudSync connection on the on-premises recorder to connect to CIAI. See Section 9.5.6 - Configuring the CloudSync Connection

Step 6: Configuring CIAI

Configure the CIAI user interface. The CIAI Service Provider performs the following tasks to set up and configure CIAI features for the customer, including UI default settings for the CIAI instance:

1. Verify transferred recordings. See Section 10.2 - Verifying Transferred Recordings.
2. Create end user accounts. See Section 10.3 - Creating User Accounts.
3. Configuring user permissions. See Section 10.3.1 - Configuring User Permissions.
4. Configuring account settings. See Section 10.3.2 - Configuring Account Settings.
5. Configuring resource permissions. See Section 10.3.3 - Configuring Resource Permissions.
6. Configuring search filters. See Section 10.3.4 - Configuring Search Filters.
7. Verifying access to user accounts. See Section 10.3.5 - Verifying Access to User Accounts.
8. Verifying user permissions. See Section 10.3.6 - Verifying User Permissions.
9. Creating Resource Groups. See Section 10.4 - Creating Resource Groups.
10. Configuring CIAI Transcriptions. See Section 10.5 - Configuring Transcriptions.
    - Background Transcriptions: See Section 10.5.1 - CIAI Background Transcriptions.
    - Manual Transcriptions: See Section 10.5.2 - Manual Transcriptions.
    - Boost Feature: configure boost words/phrases for customer: See Section 10.5.3 - Configuring Boost.

1. Configuring Retention Settings. See Section 10.6 - Configuring Retention Settings.
2. Configuring Custom Fields. See Section 10.7 - Configuring Custom Fields.
3. Configuring NexLog Reports. See Section 10.8 - Configuring NexLog Reports.
4. Configuring CIAI User Interface Default Settings. See Section 10.9 - Configuring CIAI User Interface Default Settings.
5. Adding Default Header Columns. See Section 10.9.1 - Adding Default Header Columns.
6. Displaying and Docking the Call Properties Pane. See Section 10.9.2 - Displaying and Docking the Call Properties Pane.

7. Display Default Tabs. See Section 10.9.3 - Displaying Default Tabs.
8. Displaying the Transcriptions tab. See Section 10.9.4 - Displaying the Transcriptions Tab.
9. Display Transcriptions in the Timeline. See Section 10.9.5 - Displaying Transcriptions in the Timeline.
10. Saving the Current Header Columns Layout as Default. See Section 10.9.6 - Saving the Current Header Columns Layout as Default.
11. Running queries with AI Research Assistant. See Section 10.9.7 - Running Queries with AI Research Assistant.
12. Verifying Resource Groups. See Section 10.9.8 - Verifying Resource Groups.
13. Adding Call Type Icons. See Section 10.9.9 - Adding Call Type Icons.
14. Applying the default configuration to new users. See Section 10.9.10 - Applying the Default Configuration to New Users.
15. Applying the default configuration to Selected Users. See Section 10.9.11 - Applying the Default Configuration to Selected Users.
16. Monitoring and Alerts. See Section 10.10 - Monitoring and Alerts.
17. Configuring Email Alerts. See Section 10.10.1 - Configuring Email Alerts.
18. Exporting and Importing Alerts. See Section 10.10.2 - Exporting and Importing Alerts.
19. Exporting Logs. See Section 10.10.3 - Exporting Logs.
20. Monitoring with NMS. See Section 10.10.4 - Monitoring with NMS.

Step 7: Customer Onboarding and Training

- Onboarding the customer and end user. See Section 11 - Onboarding Customers and End Users.

9. DEPLOYING CRITICAL INSIGHTS AI

This chapter covers required CIAI Service Provider tasks to deploy the customer instance of Critical Insights AI. Once Eventide Communications technicians have completed their hosting and setup tasks, the CIAI Service Provider technician will carry out various administrative and setup tasks for the on-premises NexLog recorder and the CIAI user interface.

In addition to this deployment guide, the CIAI Service Provider technician should retain the following information/items on-hand:

- Required connectivity information obtained from the CIAI SaaS Deployment Form that the customer will have completed and returned to the CIAI Service Provider. The form should contain all the information required to connect the NexLog DX-Series recorder to the CIAI Service host machine. Technicians should have this form plus the CIAI SaaS Deployment Card email on hand.
- CloudSync License key required to be added to the NexLog DX-Series recorder.
- All supplemental information concerning the type of calls that end users want to transfer to CIAI (for example, 911 calls, radio, admin, etc.). This also includes information concerning any custom configurations the customer may have requested.

9.1. Completing the Pre-Sales Checklist Form

- The CIAI Service Provider fills out the Pre-sales Checklist. The information in this form advises EC on sizing and
- which features will be used in CIAI. The CIAI Service Provider should contact EC for assistance in filling out this form if needed.
- Email the form to broberts@eventidecommunications.com.

9.2. Placing the Purchase Order

- The CIAI Service Provider places a Purchase Order (PO) by contacting loggers@eventidecommunications.com.

The PO must contain a reference to the customer who will use the CIAI service. CIAI is priced according to the volume of recordings to be analyzed with AI. So EC must be able to associate the Purchase Order (PO) with the Pre-sales Checklist Form. Once the PO is placed and processed, EC returns a confirmation email to the Service Provider that validates the PO against the associated Pre-sales Checklist Form. Attached to this email is the CIAI SaaS Deployment Registration Form for the next step. The PO confirmation email contains the CIAI SaaS Deployment form specific to this PO.

9.3. Completing the CIAI SaaS Deployment Form

After the PO for CIAI is processed, Eventide Communications emails a CIAI SaaS Deployment Form to the CIAI Service Provider, which the Provider jointly fills out with the customer. The CIAI SaaS Deployment form provides the technical details for the deployment of the CIAI instance.

The customer returns the completed form to EC at: loggers@eventidecommunications.com. This deployment form is associated with both the Pre-sales Checklist and the PO and is specific to each customer. It contains the NexLog serial number(s) for the associated recorder(s). For this form, the Service Provider will:

1. add email contacts and also contacts for automated alerts to the relevant form question fields, partially completing the form.
2. email the CIAI SaaS Deployment Form to the customer to supply their information, required to launch the CIAI instance. The customer then returns the fully completed form to EC.

The following table details the CIAI SaaS Deployment Form required information:

Table 9.1 **CIAI SaaS Deployment Form**

CIAI SaaS Deployment Form	
Requested Information	**Explanation**
Desired external address/URL	External address/URL used to access Critical Insights AI Service, i.e. <*domainName.ciai.cloud*>. This could either be the agency name or alternatively, a short abbreviation.
Geographic location (U.S. State) of the source recorder(s)	The geographic location of the source recorder(s) that will be sending recordings to CIAI. EC will use this location to determine the hosting zones to which to deploy the instance.
Source recorder(s) public IP address(es):	Providing this IP address is recommended to prevent access from unauthorized IP addresses to

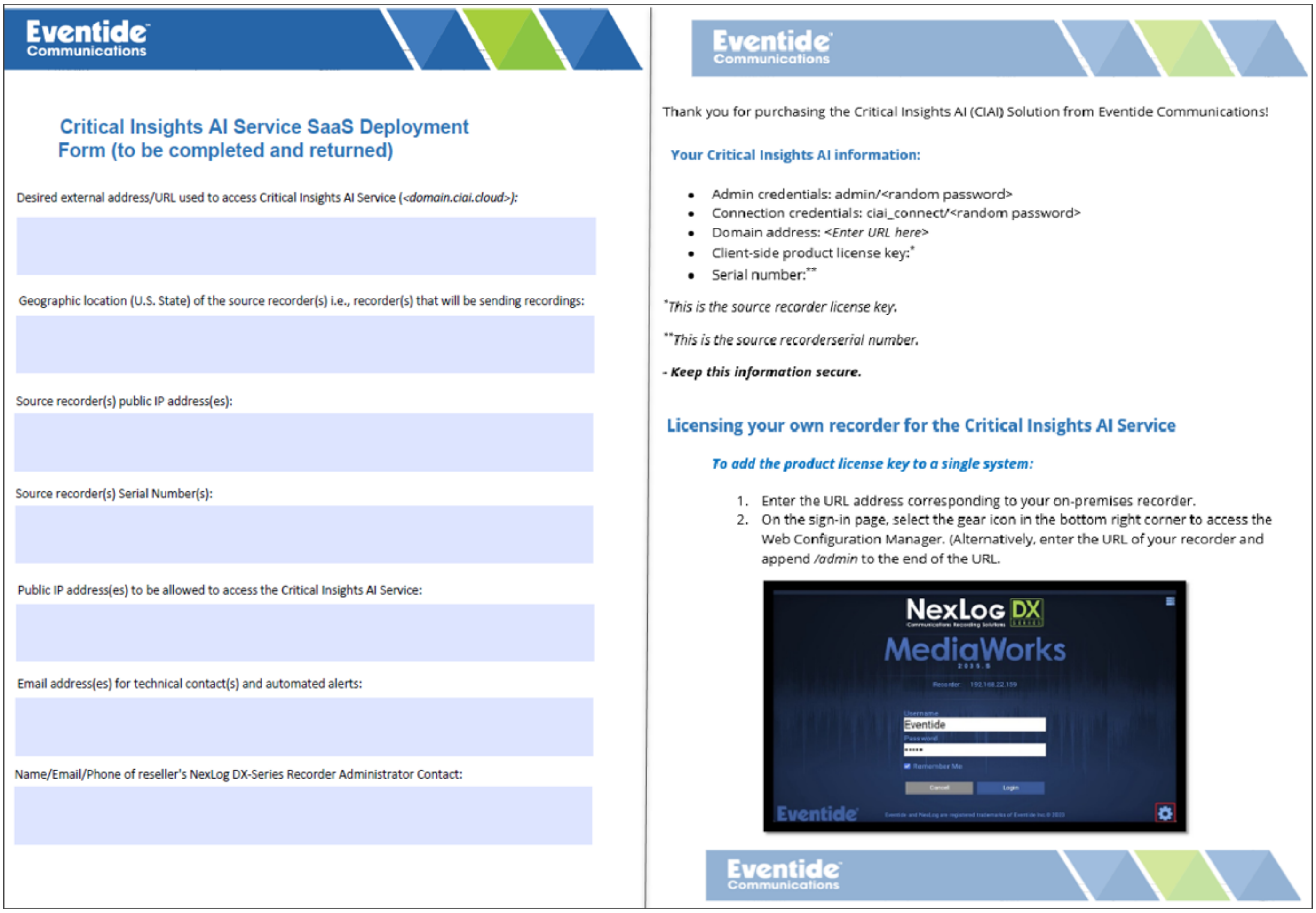
CIAI SaaS Deployment Form	
	the customer's CIAI instance. EC will create a firewall rule in the Cloud Infrastructure to restrict access. The source recorder's public IP address can be determined and tested from the recorder's Network Utility page.
Source recorder(s) Serial Number(s):	The Serial Number(s) of the source recorder, the origin of recordings. This will be used to generate the license required to upload recordings.
Public IP address(es) to be allowed to access the Critical Insights AI Service:	Public IP address(es) to be allowed to access the Critical Insights AI Service in case different from Source recorder public IP address(es). This could be a home address or geographic region. If not specified, EC will limit connections to those originating from inside the U.S.
Email address(es) for technical contact(s) and automated alerts:	Names of people to contact in the event of technical issues and automated alerts with respect to the AWS infrastructure. EC provides automated monitoring of CIAI and its connectivity status and will notify the provided addresses by email.
Name/Email/Phone of reseller's CIAI Administrator contact:	Name/Email/Phone of the CIAI Service Provider's NexLog DX-Series Recorder Administrator Contact. This is where the response to this form will be sent with initial one-time credentials.

9.4. Receiving the CIAI SaaS Deployment Card

After receiving the completed CIAI SaaS Deployment Form from the customer, EC issues a CIAI SaaS Deployment Card, which typically takes from 1-5 business days. This card contains the connectivity information and credentials required for the CIAI Service Provider to sign in to the CIAI SaaS instance and begin configuration, as illustrated in Table 9-2:

Table 9.2 **CIAI SaaS Deployment Card**

CIAI SaaS Deployment Card	
Requested Information	**Explanation**
Admin credentials:	User Admin credentials to access CIAI
Connection credentials:	Credentials to be used for the CloudSync (CaaS) connection
Domain address:	This is the address through which to access the CIAI instance.
Client-side product license key:	The CloudSync/Centralized Archive (CaaS) transfer license key(s) to be added to the source recorder(s).
Serial number:	This is the serial number of the source recorder.



Eventide Communications

Critical Insights AI Service SaaS Deployment Form (to be completed and returned)

Desired external address/URL used to access Critical Insights AI Service (*<domain.ciai.cloud>):*

Geographic location (U.S. State) of the source recorder(s) i.e., recorder(s) that will be sending recordings:

Source recorder(s) public IP address(es):

Source recorder(s) Serial Number(s):

Public IP address(es) to be allowed to access the Critical Insights AI Service:

Email address(es) for technical contact(s) and automated alerts:

Name/Email/Phone of reseller's NexLog DX-Series Recorder Administrator Contact:

Eventide Communications

Thank you for purchasing the Critical Insights AI (CIAI) Solution from Eventide Communications!

Your Critical Insights AI information:

- Admin credentials: admin/<random password>
- Connection credentials: ciai_connect/<random password>
- Domain address: *<Enter URL here>*
- Client-side product license key:*
- Serial number:**

**This is the source recorder license key.*

***This is the source recorderserial number.*

*- **Keep this information secure.***

Licensing your own recorder for the Critical Insights AI Service

To add the product license key to a single system:

1. Enter the URL address corresponding to your on-premises recorder.
2. On the sign-in page, select the gear icon in the bottom right corner to access the Web Configuration Manager. (Alternatively, enter the URL of your recorder and append */admin* to the end of the URL.

Eventide Communications

Fig. 9.1 **CIAI SaaS Deployment Form and CIAI SaaS Deployment Card**

At this point, the CIAI Service Provider technician can begin configuration of the customer's source recorder to connect to the CIAI Service.

9.5. Configuring the Source Recorder

To configure the on-premises NexLog DX-Series source recorder that will be capturing recordings, the CIAI Service Provider technician must complete the following series of setup and configuration tasks:

9.5.1. Verifying Source Recorder Firmware

- Verify the source recorder firmware version, which should be 2025.1. For more information, see *Section 7.1.1."System Info" of the NexLog DX User Manual.*

9.5.2. Adding the CloudSync License

The next step is to add the CloudSync/Centralized Archive license key (client-side) to the source NexLog recorder to enable transfer of recordings.

- DX936-NexLog CloudSync (Client-Side)

To add the CloudSync license to the recorder:

1. Sign in to the source NexLog DX-Series recorder's Configuration Manager with your credentials.
2. Have the 20-digit CloudSync license key ready, as provided in the CIAI SaaS Deployment Card.
3. In the left navigation menu, select System → License Keys.
4. In the right pane, select the Add Key button.

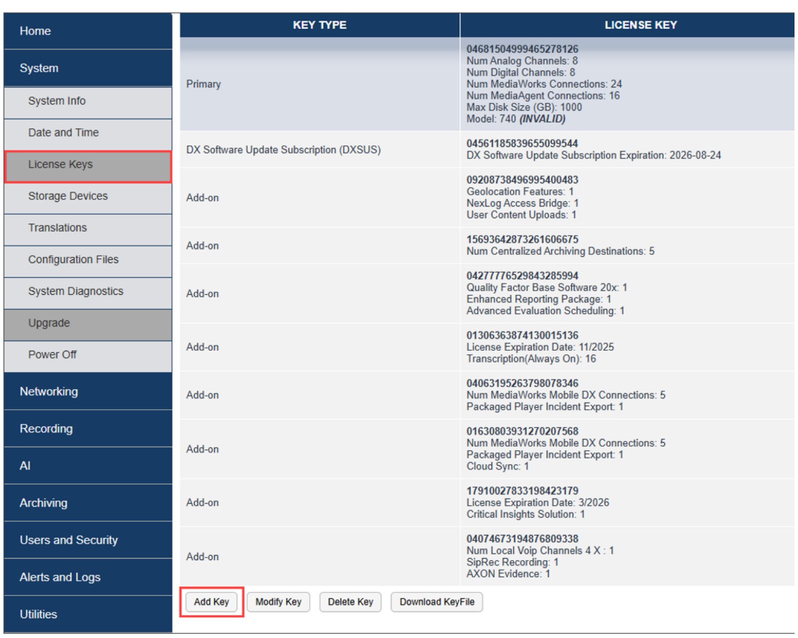


Fig. 9.2 **Adding the CloudSync License to the NexLog DX-Series Recorder**

5. In the License Key field, enter the 20-digit license key for the Critical Insights AI Service and select Add.

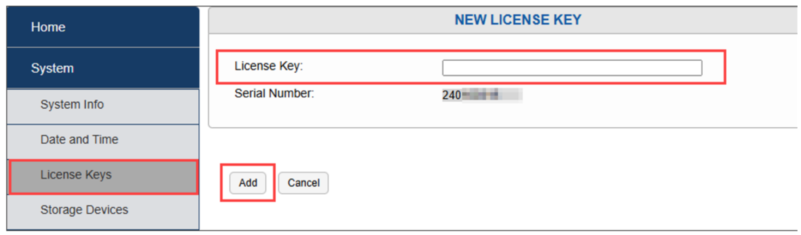


Fig. 9.3 **Entering the License Key**

6. Repeat steps 3 and 4 to add any other required addon licenses as required.
7. On the License Keys page, in the License Key column, confirm that the product license(s) was successfully added. A separate license must be added for each recorder.

9.5.3. Configuring Networking for the On-Premises Recorder

Configuring networking for the on-premises NexLog recorder is a customer/end user task. However, the CIAI Service Provider should verify networking requirements with the customer and ensure that the on-premises source recorder can reach the CIAI Service over port 4024.

The CIAI Service Provider should communicate to the customer that they should open outbound access from the on-premises recorder to the CIAI Service on the following firewall ports:

- TCP/4024 Secure transfer of recordings using the Central Archiving/CloudSync protocol
- TCP/443 (HTTPS) for CIAI User Interface access

Note

HTTP is blocked by default. You can only access the recorder using HTTPS. All public IP addresses from which your organization's users will access CIAI must first be whitelisted by Eventide Communications. This includes any IP addresses from which calls will be transferred and the IP addresses of Service Providers and technicians.

Eventide Communications will provide the destination CIAI service's domain name in the CIAI SaaS deployment card.

9.5.3.1. Verifying Connectivity

To verify recording:

- Confirm connectivity and that recordings are transferring to CIAI in real time, as per the Transfer Rate as shown in the following diagram.

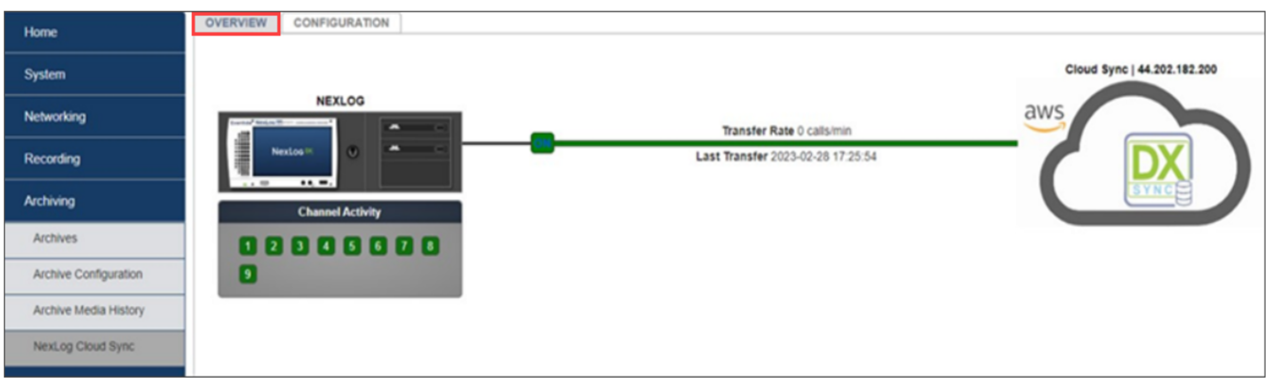


Fig. 9.4 **Verifying Connectivity**

If there is no connectivity, or there is connectivity, but recordings are not being transferred, at this stage, refer to Section 12 - Troubleshooting.

9.5.4. Configuring Recording

The Service Provider technician should verify that recording is correctly configured for accurate recording. To this end, Stream Recording Mixing Mode should be configured (where supported) if not already configured. This ensures that call audio from caller and call-taker is separated. This feature is configured from Web Configuration Manager within the customer's existing data integration template.

To configure stream recording mixing mode:

1. In the left navigation menu, under Recording Interfaces, select the Template tab.

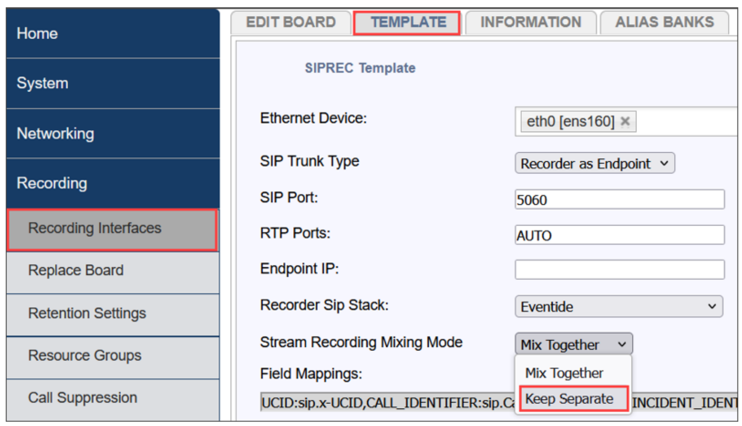


Fig. 9.5 **Configuring Stream Recording Mixing Mode**

2. In the Field Mappings section, select Keep Separate, if not already selected.

3. Select Save to re-save the template.

9.5.5. Verifying Recording

To verify recording:

1. Verify that recording is occurring correctly on the source. Some configuration changes may be necessary to remove 'echo' or call breaks from recordings.
2. Correct any echo issues on call installation equipment. Echo in calls negatively affects the quality of transcription and the quality of the AI analytics that can be performed.

9.5.6. Configuring the CloudSync Connection

CIAI Service Provider technicians will configure the connection from the agency's on-premises NexLog DX-Series recorder to CIAI. This connection is established from the CIAI Service Provider's local administrator account within Web Configuration Manager on the customer's on-premises recorder. When activated, this connection enables the transfer or replication of call recordings and metadata from the on-premises NexLog DX-Series recorder to the cloud-hosted CIAI Service machine.

This is made possible through a function called Centralized Archive, which is enabled after the required CloudSync license is added to the recorder. Once this connection is established after the prior recorder tasks have been carried out, subsequent recorder configuration is performed from Web Configuration Manager from the CIAI user interface.

The following procedure provides the steps to configure a NexLog DX-Series recorder to connect to the cloud-hosted CIAI Service, which sets up and initiates the transfer of recordings.

To connect to the CIAI Service:

1. In the left navigation menu, select Archiving –> NexLog Cloud Sync.
2. Select the Add Cloud Sync button.

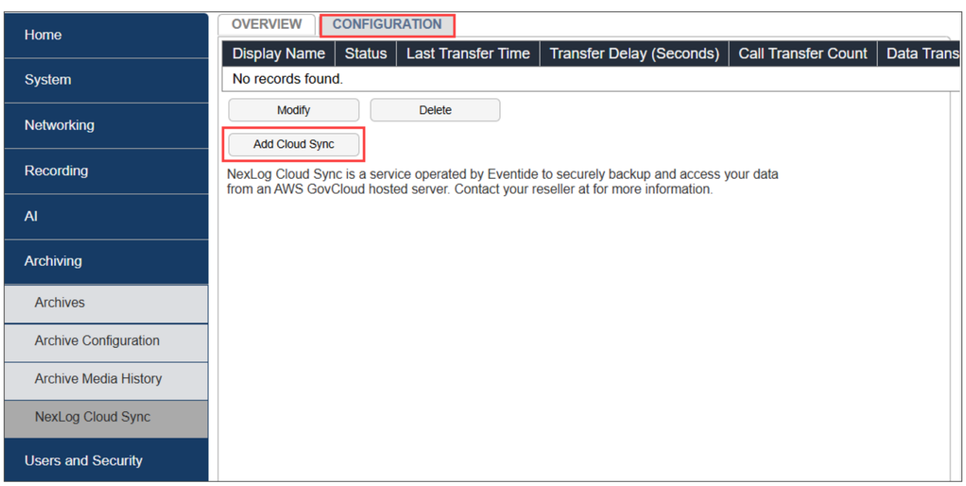


Fig. 9.6 **Adding NexLog Cloud Sync**

In the fields provided, fill in the appropriate connection information as provided in the CIAI SaaS Deployment Card, namely:

1. In the NexLog Cloud Sync Display Name field, enter *CIAI Connect* or name of your preference.
2. In the NexLog Cloud Sync Address field, type the domain name of the (cloud-based) CIAI Service, i.e. *<domainName.ciai.cloud>*
3. In the Username field, type *ciai_connect* (username is case-sensitive).
4. In the Password field, type the password for the 'ciai_connect' account.
5. TLS: This checkbox will be selected by default. Leave as-is.

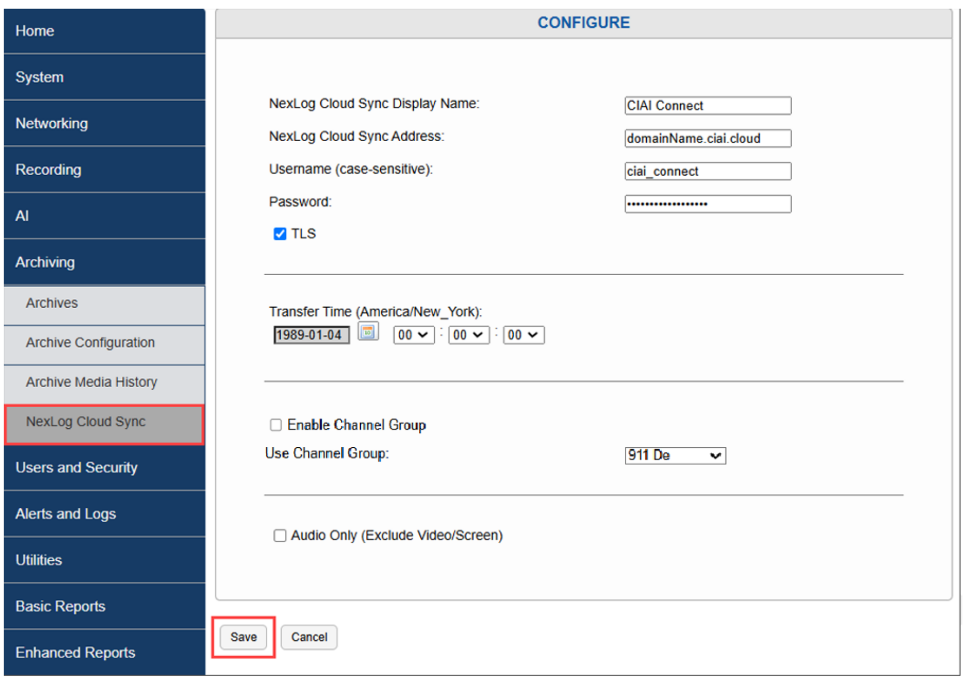


Fig. 9.7 **Configuring the NexLog Cloud Sync Connection**

6. Select the calendar icon for the Transfer Time setting (<*Time Zone*>) and select the *Year, Month, and *Day* for the time period the CIAI Service machine. Set this to the current time (presumably).
7. Select the time of day in hours, seconds, and minutes (*hh:mm:sec)* from each of the three drop-down fields to the right.

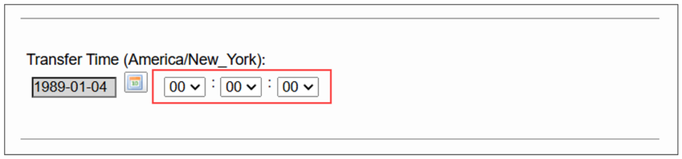


Fig. 9.8 **Configuring the NexLog Cloud Sync Transfer**

One of two recording transfer scenarios will be the case: the customer will be either transferring *all* call recordings or a *sub-set* of recordings on a specific channel.

8. If transferring *all* recordings:

    - leave the Enable Channel Group checkbox un-selected. This means *all* call recordings on *all* channels will be replicated to CIAI.

    If just transferring a sub-set of call recordings:

    - select the Enable Channel Group checkbox.

    This latter action will enable the Use Channel Group setting, which will activate the channel selected for the calls in the drop-down menu to the right. This means that all calls on that selected channel will be transferred.

9. Audio Only (Exclude Video/Screen): Select this checkbox (video/screen should be excluded).

10. Select the Save button.

As soon as these settings are saved, recordings automatically start to transfer and replicate to the CIAI Service host machine, based on the configured Transfer Time and Time of Day settings.

1. Verify that the destination CIAI instance is successfully deployed by signing in into the cloud-based CIAI user interface. Note that firewall restrictions can limit connectivity.
2. Confirm connectivity to the CIAI SaaS user interface. This includes verifying that the customer's CIAI Service is accessible from approved locations, as may be specified in the CIAI SaaS Deployment Form.

Note

Note that incidents, QA Evaluations, and annotations are not automatically transferred across to CIAI along with recordings during deployment. If you need to transfer any of these items to CIAI, contact Eventide Communications to schedule a request to synchronize this data/metadata over CaaS (referring to the CloudSync or the Centralized Archive transfer technology that EC uses to transfer recordings and metadata from one NexLog recorder to another).

This page was intentionally left 99.88% blank.

10. CONFIGURING THE CIAI USER INTERFACE

The next task is to configure the CIAI user interface to default settings for a positive customer experience.

10.1. Changing the CIAI Service Provider Administrator Account Password

To change the CIAI Service Provider administrator account password:

1. Sign in with your credentials to your CIAI Service Provider administrator account.
2. When prompted, change the CIAI Service Provider Administrator “Admin” password to a strong, private password.

> **Note**
>
> CIAI Service Providers and Eventide Communications maintain separate administrative accounts.
>
> Do *not* change the existing Eventide Communications Administrator account password, since Eventide Communications technicians will still require administrative access to that account for all required configuration, post-deployment.

10.2. Verifying Transferred Recordings

- Search for recorded calls replicated earlier to CIAI and verify recordings are working correctly and being properly replicated. Recorded calls should show up on the same recorder channels.

10.3. Creating User Accounts

CIAI Service Provider technicians should create and configure the accounts of all customer end users who will be signing into CIAI, as required.

To add a user for CIAI:

1. In the left navigation menu, go to Users and Security –> Users.

2. Select the Add User button.

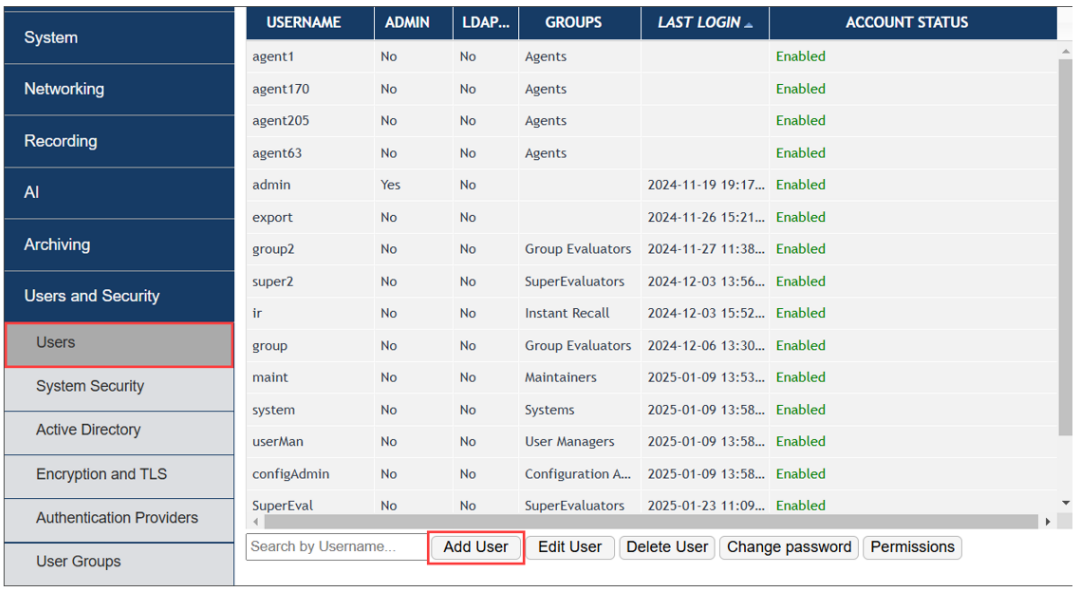


Fig. 10.1 **Adding a CIAI User Account**

The Add New User dialog opens.

3. In the Username field, enter the username (note: the username *cannot* contain punctuation marks or spaces).

4. In the Password field, enter the password.

5. In the Repeat Password field, re-enter the password to confirm it.

6. In the Group Membership section, select the specific checkbox(es) for the group role(s) or permissions you want the user to have, in this instance, “Agents”.

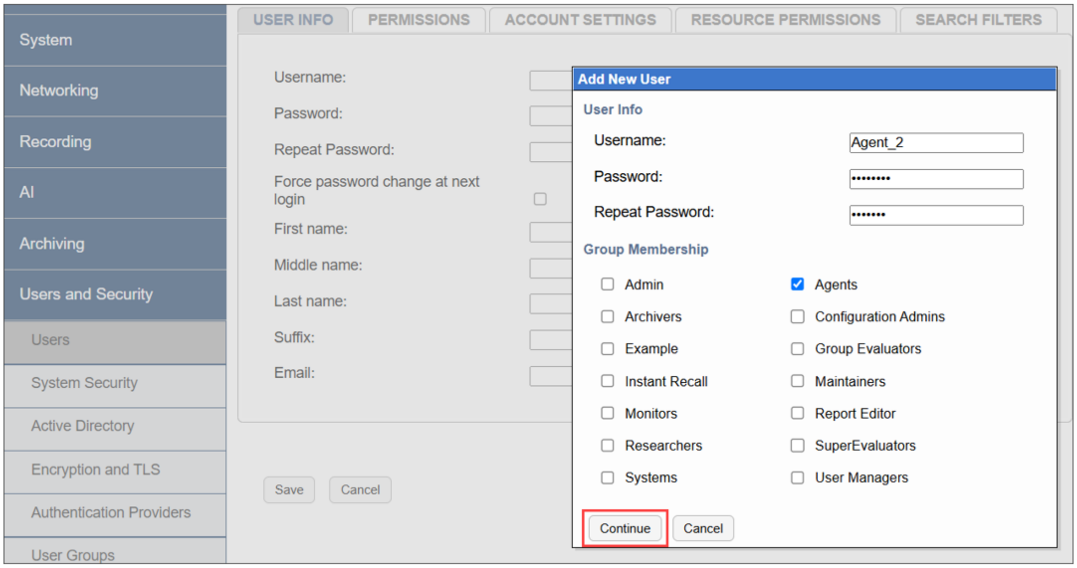


Fig. 10.2 **Configuring Group Membership of a CIAI User Account**

7. Select the Continue button. The User Info tab opens.

8. In the corresponding fields, enter the user's First, Middle, and Last names, Suffix, and email address.

9. Select the Force password change at next login checkbox.

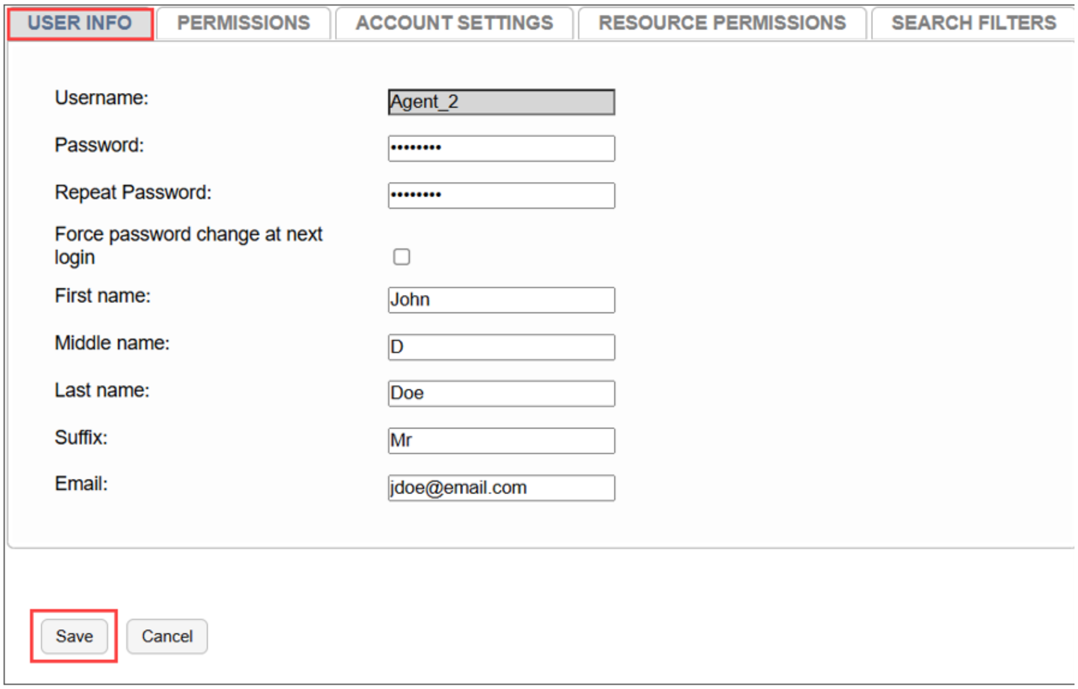


Fig. 10.3 **Saving the CIAI User Account Information**

10. Optionally, select the Save button now (present and global across all tabs, meaning you only need to select Save once). You can continue configuring your selections and just select Save at the end. The new user is now listed with account status 'Enabled'.

USERNAME	ADMIN	LDAP	GROUPS	LAST LOGIN	ACCOUNT STA...
Agent_2	No	No	Agents		Enabled
Eventide	Yes	No		2025-02-01 22:17:...	Enabled
Super	No	No	SuperEvaluators	2025-01-29 12:19:...	Enabled
SuperEval	No	No	SuperEvaluators	2025-01-23 11:09:...	Enabled
admin	Yes	No		2024-11-19 19:17:...	Enabled

Fig. 10.4 **CIAI User Account 'Enabled' Status**

10.3.1. Configuring User Permissions

You can configure or re-configure permissions for users you create and assign or re-assign them as members of specific groups.

To configure user permissions:

1. Go to Users and Security → Users and select the Permissions tab.

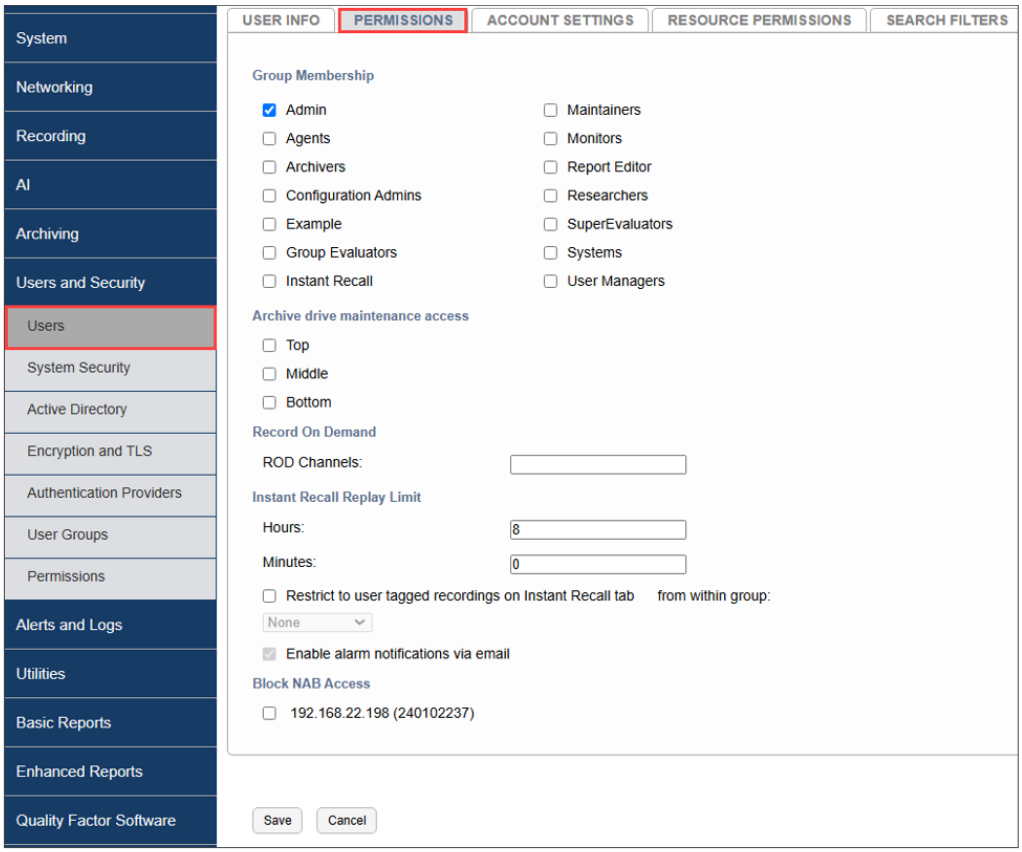


Fig. 10.5 **Configuring User Permissions**

2. Under Group Membership, select the checkboxes for group(s) you want the user to be a member of, for example, 'Admin'. It is also possible to select multiple categories if required. For example, you might also want a Manager to be also a Group Evaluator, as per customer requirements.

   - **Archive Drive Maintenance Access:** This checkbox is un-selected by default.
   - **Record on Demand, ROD Channels:** This checkbox is un-selected by default.
   - **Instant Recall Replay Limit:** This checkbox is un-selected by default.
   - **Restrict to user tagged recordings on Instant Recall tab:**

     If this checkbox is selected, when viewing the Instant Recall tab, users will only be able to view and play call records that have a metadata field called USER_ID that contains their username.

For additional information on configuration settings, refer to the NexLog DX-Series manual.

3. **From Within Group:** Select the appropriate resource/channel group. When enabled, this group function filters the channels that are available to the user, based on the resource group permissions applied.

4. Select the checkbox Enable alarm notifications via email. This checkbox enables users to receive alarm notifications. Members of the Admin group automatically receive alarm notifications by default. All other user groups can receive email notifications by selecting the checkbox.

5. **Block NAB Access**: Leave at configured defaults.

10.3.2. Configuring Account Settings

To configure account settings:

1. Select the Account Settings tab. Default settings are shown in the following screenshot. The account should be enabled.

2. Leave settings at configured defaults unless the customer has expressed a preference.

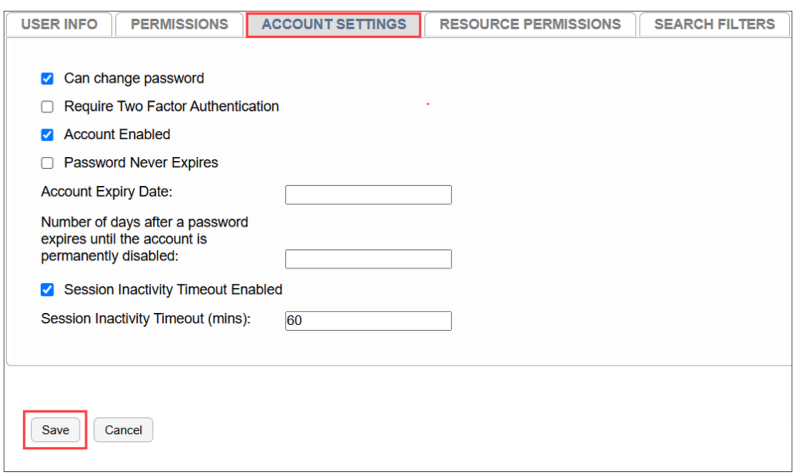


Fig. 10.6 **Configuring Account Settings**

10.3.3. Configuring Resource Permissions

On the Resource Permissions tab, you can add the customer's preferred channels to the Channel Permissions pane.

To add preferred channels to the channel permissions pane:

1. Select the Resource Permissions tab.

2. If the selected user belongs to the 'Admin' group:

   - No action required. The left pane is the Channel Permissions pane. For the Admin group, this pane will *not* be populated because Admins have permissions to *all* channels by default, so it is unnecessary to add channels here.

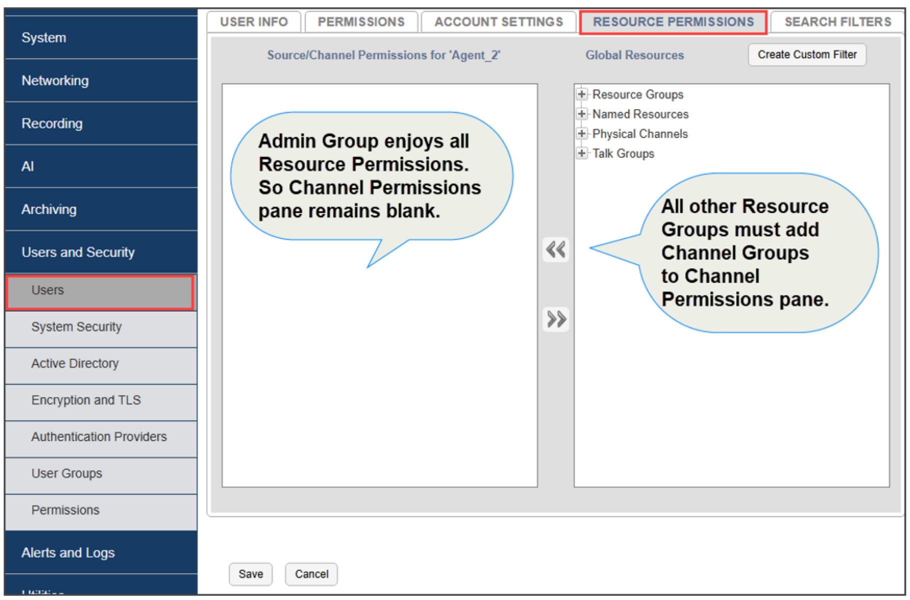


Fig. 10.7 **Adding Preferred Channels to the Channel Permissions Pane**

3. For non-admin group roles (for example, the *Researchers* group) under Resource Groups, select your source or preferred channels to add them to the Source/Channel Permissions pane on the left.

4. Select the left-pointing chevron to add the channel to the source or channel permissions for previously-created Agent_2.

The selected channel is now added to the Source/Channel Permissions pane. The current (non-admin) user now has access permissions to view recorded calls recorded on the '911 Positions' channel.

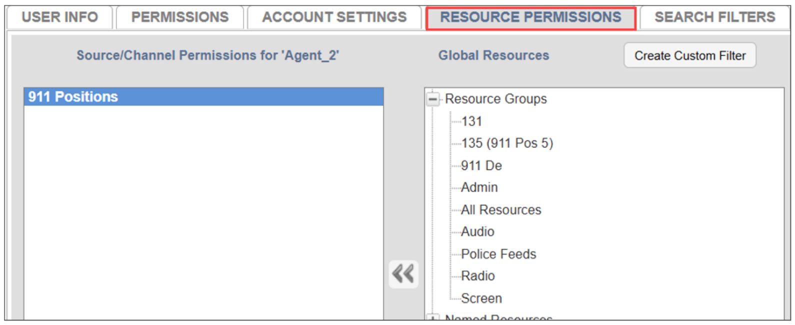


Fig. 10.8 **Channels Successfully Added to the Source/Channel Permissions Pane**

5. Add further channels to the Source/Channel Permissions pane as required as per customer request.

10.3.4. Configuring Search Filters

On the Search Filters tab, you will add channels to the search filters pane to allow users to filter on the selected channels.

To configure search filters:

1. Select the Search Filters tab.

2. Select a channel for which you want to allow search filter permissions for Agent_2.

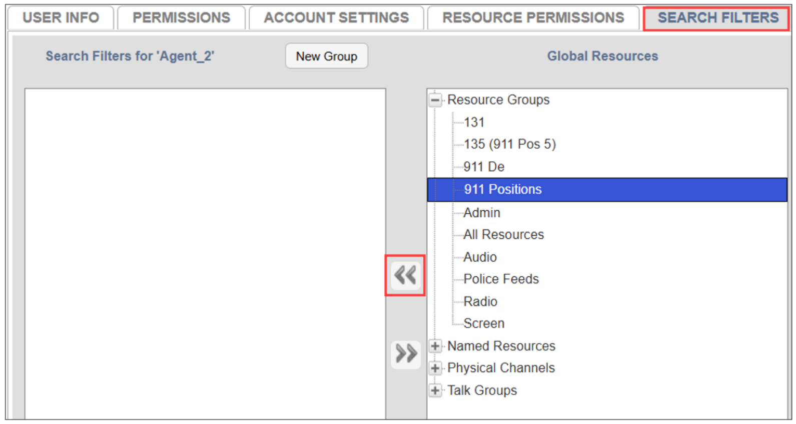


Fig. 10.9 **Adding a Channel to Allow Search Filter Permissions**

3. Select the left-pointing chevron to add the channel to the source or channel permissions for Agent_2.

4. Select the Save button.

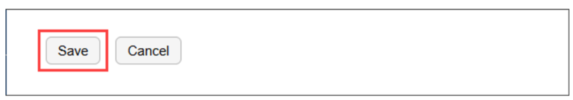


Fig. 10.10 **Saving the CIAI User Account Configuration Settings**

5. To re-configure or edit user account configuration options, at the bottom of the page, select the Edit User button.

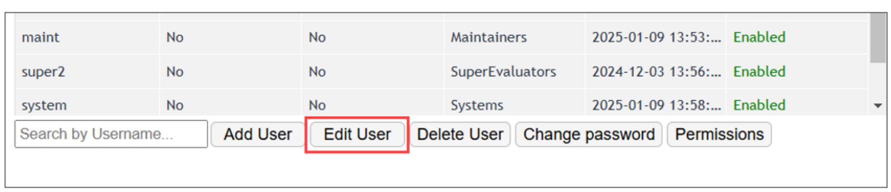


Fig. 10.11 **Additional User Account Configuration Options**

10.3.5. Verifying Access to User Accounts

- Verify that you can successfully sign in and access each new end user's account with the corresponding credentials.

10.3.6. Verifying User Permissions

- Verify that a user from the “Agent” group, for example (who should only have access to QA evaluations) cannot perform other tasks, such as conduct searches or view or do anything else. Attempting a search with this user should generate a permissions error.

  For additional user account information, refer to *Section 7.5.1. “Users”* of the NexLog DX-Series User Manual.

10.4. Creating Resource Groups

This section covers how to create Resource Groups, *a.k.a*. Channel Groups. In this document, the terms ‘Resource Group’ and ‘Channel Group’ will be used interchangeably. A Resource Group is a set of configured resources available on the recorder and their applicable rules.

Resources represent the call sources of a NexLog DX-Series recorder, identified by Channel Name, Physical Channel ID, and Talk Group. Resource Groups allow Administrators to manage all policy for a set of resources, instead of having a separate Channel Group for each rule.

For example, if one group of channels records fire department calls and another set records police calls, you might create a Resource Group called ‘Fire’ that contains all channels with names starting with ‘Fire’ exclusively for that group, and grant permissions to the correct users all in one place. For CIAI, Eventide Communications recommends using the default Resource Group names. If customers wish to customize these names, they should contact Eventide communications.

CIAI Service Provider technicians should create and configure the following default Resource (or Channel) Groups:

- 911 Positions
- Admin
- Audio
- Radio
- CAD Positions

The following procedure covers the steps to create a new Channel Group. As an example, we will use the Channel Group ‘911 Positions’.

> **Note**
>
> When creating Resource (or Channel) Groups, *exclude* screen and video calls.

To create a new resource group:

1. Navigate to Recording → Resource Groups to display the Resource Groups page. The left pane contains Resource Groups; the right pane represents Global Resources, which includes Named Resources, Physical Channels, and Talk Groups.

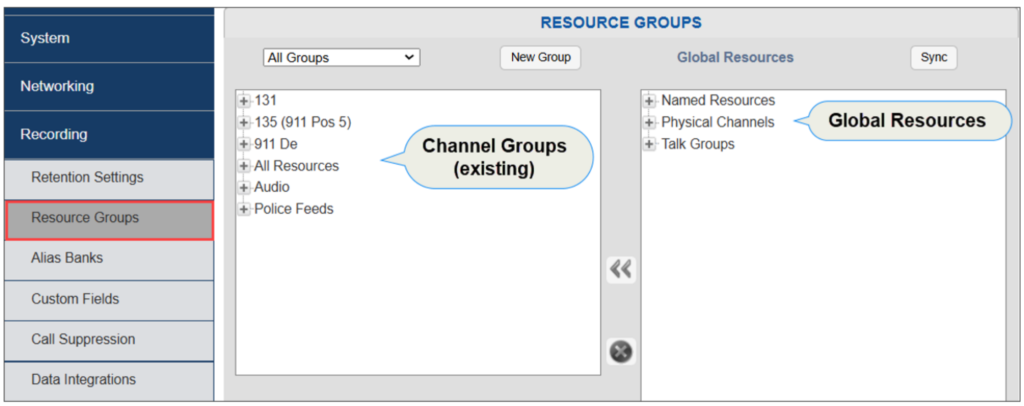


Fig. 10.12 **Global Resources and Channel Groups**

2. At the top of the page, select New Group (i.e. a Resource Group).

Fig. 10.13 **Creating a New Channel Group**

3. In the Group Name dialog that opens, type its name, '911 Positions'.

4. Select the checkboxes for the type of rules you want to enable.

5. Here select Permissions Rules and Search Rules as the default rules.

6. Under Select Users, select the user(s) or user groups you want to enable to access to use the '911 Positions' Channel Group. In this case, the "admin" group role is selected.

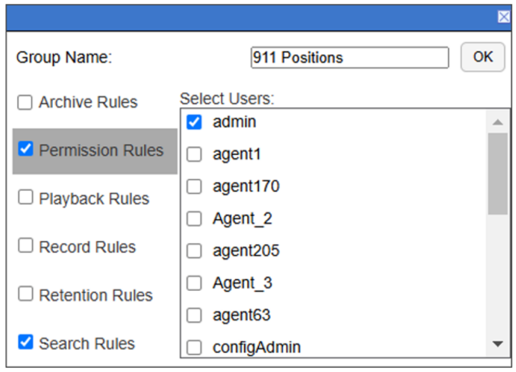


Fig. 10.14 **Selecting Permissions Membership Groups and Rules**

7. Select OK. The '911 Positions' Channel Group is now created. It is currently empty and requires one channel to be added to it at minimum.

   Next, we will add select channels to the new '911 Positions' Channel Group from the Global Resources pane on the right, under the Named Resources category. The All Resources Channel Group must exist.

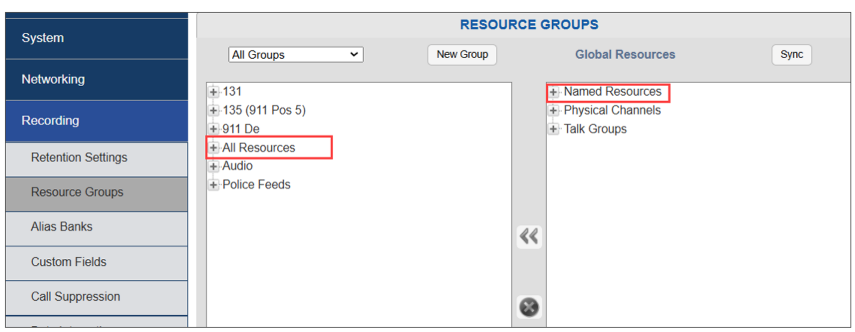


Fig. 10.15 **Adding Channels to a New Channel Group**

To add a channel to the '911 Positions' channel group

1. First select the new '911 Positions' Channel Group in the left pane to expand it. It will be currently empty.

2. In the Global Resources pane, select the plus (+) sign beside Named Resources to expand it and view its channels.

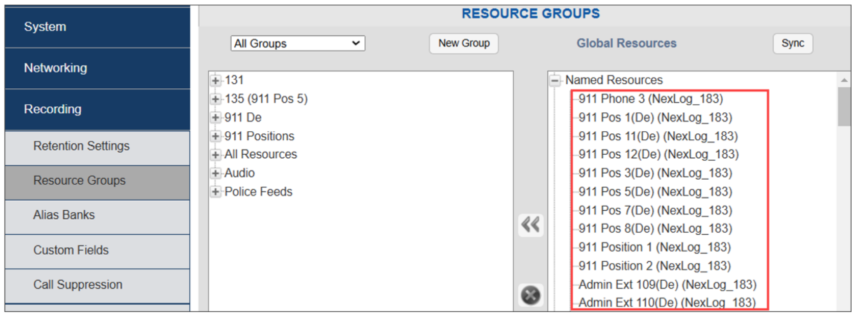


Fig. 10.16 **Viewing Available Channels**

3. In the right pane, select a channel from the expanded Named Resources category.

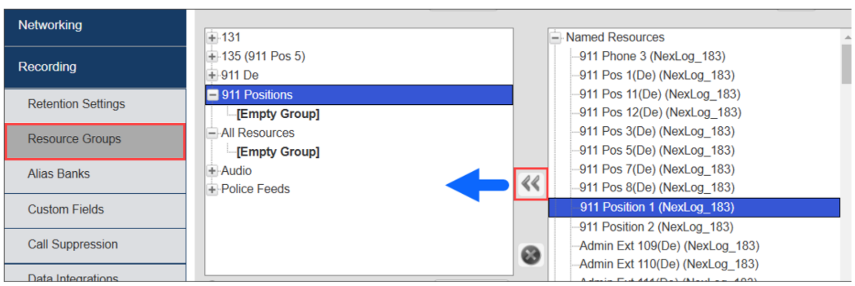


Fig. 10.17 **Selecting Channels to Add to a New Channel Group**

4. Select the left-pointing chevron in the pane divider to add the channel to the '911 Positions' Channel Group in the left pane.

Fig. 10.18 **Channels Added to the New Channel Group**

5. Similarly select additional channels as required.

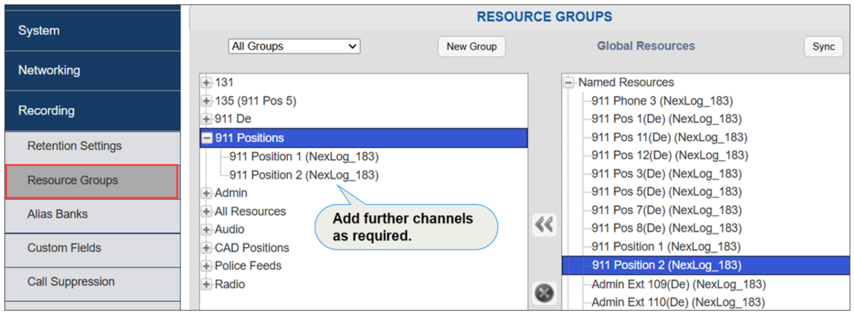


Fig. 10.19 **Adding Further Channels**

6. Repeat steps 3 through 9 to create additional Channel Groups, as required, namely, Admin, Audio, Radio, and CAD positions as shown in the next screenshot.

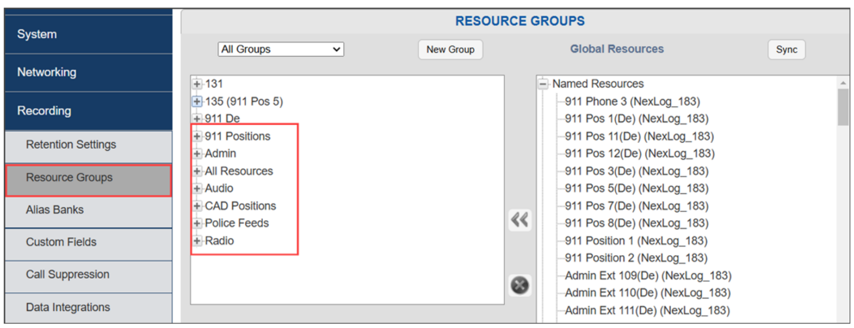


Fig. 10.20 **Creating Additional Channel Groups**

7. (Optional) To remove or delete a channel from the Channel Group, select the channel and select the circular 'X' icon in the pane divider.

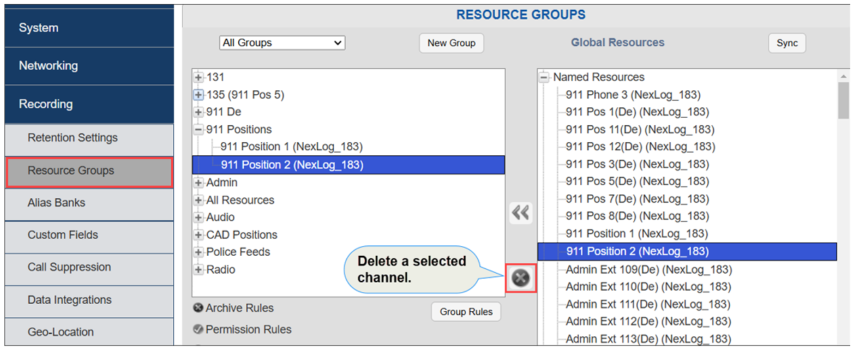


Fig. 10.21 **Deleting a Channel from the Channel Group**

8. Optionally, for additional Channel Group filtering and editing options, or to even delete the Channel Group, right-select it and then choose the appropriate menu option.

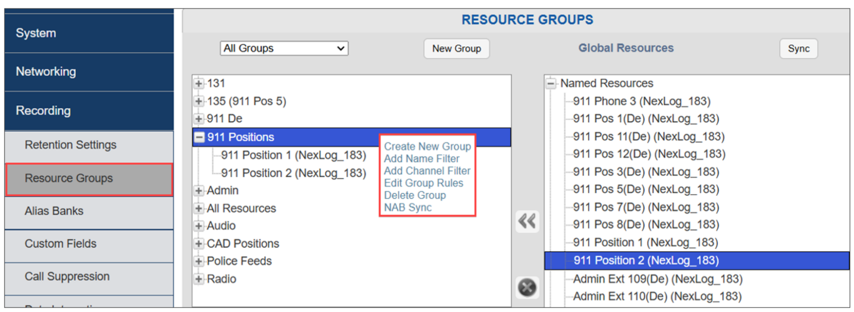


Fig. 10.22 **Additional Channel Group Filtering and Editing Options**

9. Similarly, optionally right-select a channel from the Channel Group to view filtering and editing options for each channel.

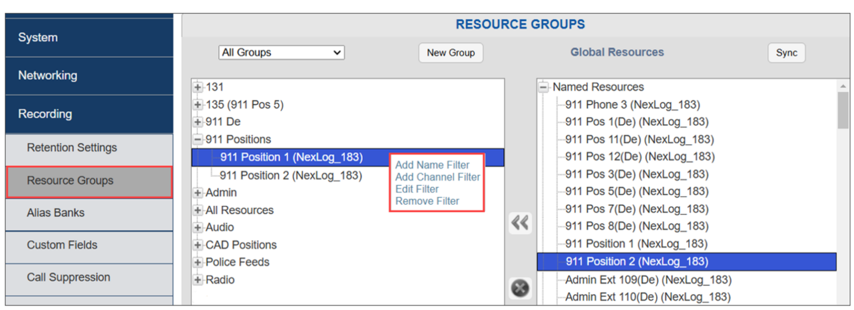


Fig. 10.23 **Viewing Channel Filtering and Editing Options**

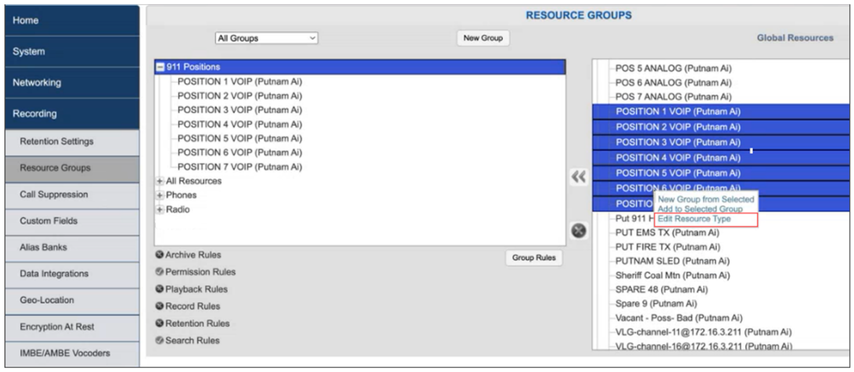


Fig. 10.24 **Viewing Channel Filtering and Editing Options (2)**

After completing these steps, the Channel Groups and their corresponding channels will now display in the CIAI user interface.

10.5. Configuring Transcriptions

With Critical Insights AI, you can configure a NexLog DX-Series recorder for AI transcriptions. Transcription functionality includes the following features:

- Background Transcriptions
- Manual Transcriptions
- 'Boost' Transcriptions

10.5.1. CIAI Background Transcriptions

Background transcriptions refers to the CIAI transcription feature that can be enabled to automatically transcribe calls as they record. Note that if the customer wants to use Scheduled (automatic) Evaluations, background transcriptions *must* be enabled for that feature to work.

To enable background transcriptions:

1. In the left navigation menu, select AI → Transcriptions. The Transcription page opens.

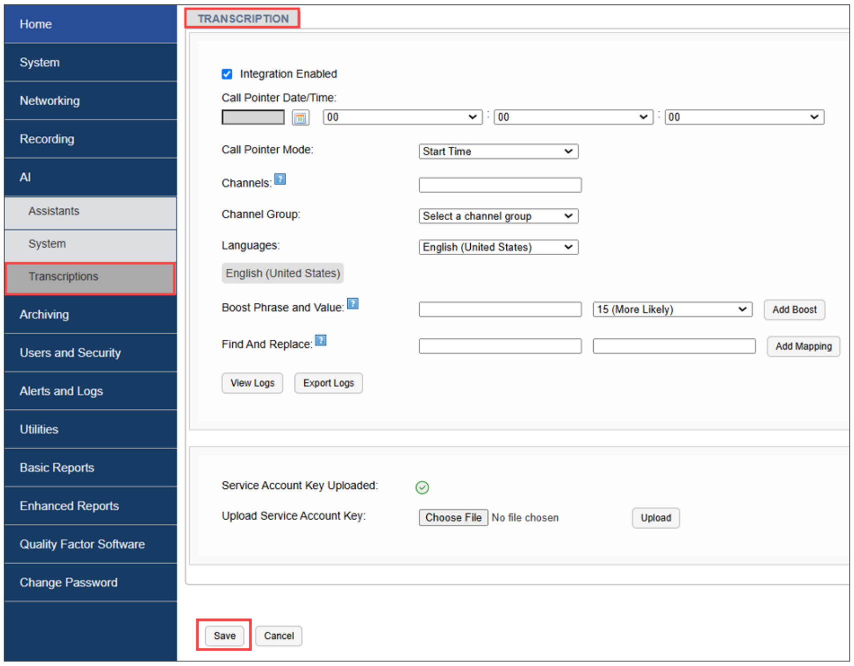


Fig. 10.25 **Enabling Background Transcriptions**

2. Make sure that the Integration Enabled checkbox is selected.

3. Under Call Pointer Date/Time, select the calendar icon and then select a date to populate the field.

4. To the right of Call Pointer Date/Time, select the time in hh:mm:sec for each of the three drop-down menu fields to specify when transcriptions will start.

Fig. 10.26 **Selecting the Date and Time**

5. From Channel Group, select a Channel Group to use to automatically transcribe calls.

6. In the Languages drop-down menu, you can choose your language. “English (United States)” is the default. Additional supported languages include Spanish, Portuguese, French, German, Italian, Russian, and Japanese. You can add up to four languages, which will then be listed on-screen.

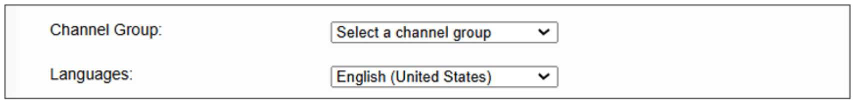


Fig. 10.27 **Selecting Channel Group and Language**

Transcriptions will now automatically be generated in the background.

10.5.2. Manual Transcriptions

Alternatively, if you are not running Scheduled (automatic) Evaluations, you can configure or generate transcriptions manually.

To generate manual transcriptions:

1. In the CIAI user interface, select a call.
2. Right-select the call and choose Generate Transcription.

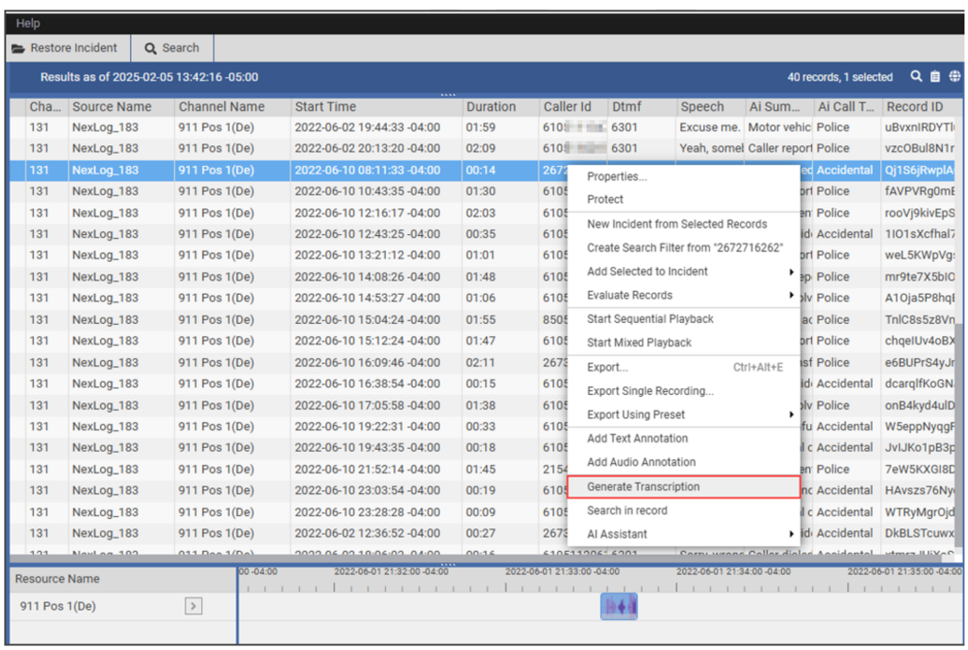


Fig. 10.28 **Generating Manual Transcriptions**

The call transcription is now generated and displayed in the Call Properties dialog on the Transcription tab.

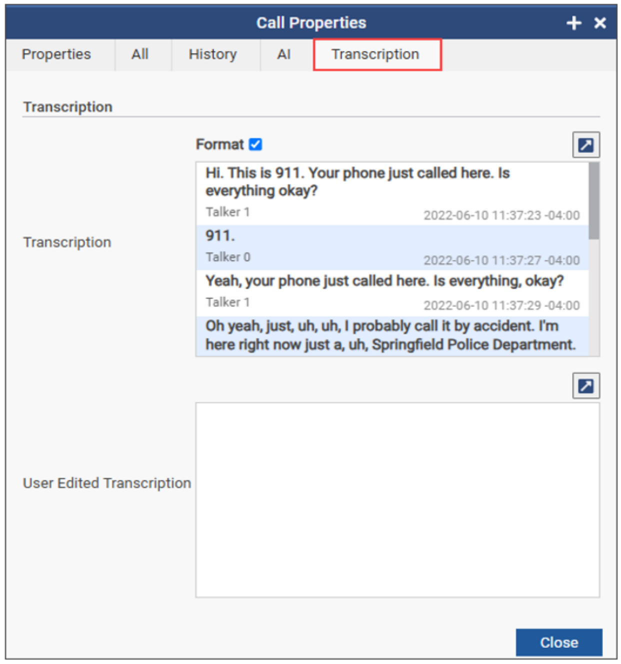


Fig. 10.29 **Manual Transcriptions**

> **Note**
>
> By default, only configure the '911 Positions' Channel Group for transcriptions.

10.5.3. Configuring Boost

The "boost" feature provides ways to correct words or multi-word phrases that AI may mis-transcribe. Mistranscriptions occur either because AI interprets a word or phrase as very similar to one found in its dictionary, or because it is not found in AI's dictionary.

The boost feature increases the likelihood that AI will correctlytranscribe a word or phrase. The best strategy to have AI correct its transcription depends on whether it is found in AI's dictionary. Here,trial-and-error is required because we have no way of knowing this.

10.5.3.1. Before Configuring Boost

Before configuring the boost figure for the customer, Eventide Communications suggests monitoring how transcription is working in the real world, looking at 911 calls. Boost is only required if issues exist to be resolved. As an important example, is the Agency Name being correctly transcribed? Is there a specific pattern of mis-transcribed words or phrases? If not, configuring boost may be deemed unnecessary at this time. If a specific transcription problem(s) exists, set up Boost, then monitor again.

Using the “boost” feature requires explanation. Three examples of using it are now presented. The first two assume that a word or phrase is found in AI’s dictionary.

Example 1:

Suppose you have two similar or identical-sounding valid words, where both are found in AI’s dictionary, such as “whether” and “weather”. If you wanted “whether” to be the more frequently-transcribed word, you can assign it a greater weight.

To boost a word or phrase:

1. In the Boost Phrase field, enter the desired word, “whether”.
2. In the Boost Value field to the right, from the drop-down menu, select the highest weight value ‘20 (Very Likely)’.
3. To the immediate right in the Boost Value field, from the following drop-down menu options, choose ‘20 (Very likely)’.
   - 0 (Very Unlikely)
   - 5 (Unlikely)
   - 15 (Likely)
   - 20 (Very likely)
4. Select the Add Boost button.

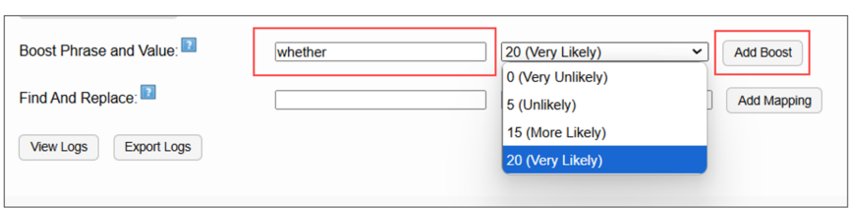


Fig. 10.30 **Boosting a Word or Phrase for Transcriptions**

Following this procedure maximizes the probability that AI will choose “whether” over “weather”, the greatest percentage of the time.

Example 2:

Similarly, suppose your agency name is ‘Barton County’, but AI mis-transcribes it as ‘Pardon County’. The assumption is that this is because although the phrase ‘Barton County’ *is* found in AI’s dictionary, it is not at the top of the list of AI’s phrases. In this case, you can boost ‘Barton County’ so that it is correctly transcribed.

1. In the Boost Phrase field, enter the (correct) phrase, ‘Barton County’.

2. In the Boost Value field, select the greatest value “20 (Very Likely)”.

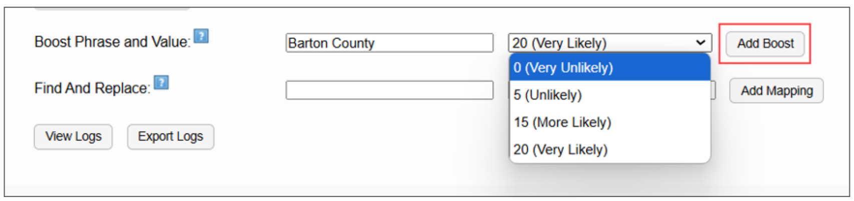


Fig. 10.31 **Configuring the Boost Value Field**

3. Select the Add Boost button. ‘Barton County’ is now likely to be transcribed the greatest percentage of the time.

4. Similarly, add additional words or phrases as per customer requirement. CIAI Service Provider technicians should boost the end customer’s Agency Name. Each added boost phrase becomes listedon-screen with its corresponding boost value.

   Conversely, had you assigned the lowest weight of “0 Very Unlikely” to ‘Barton County’, this would minimize the likelihood of ‘Barton County’ being transcribed, as opposed to similar-sounding phrases in AI’s dictionary. If this strategy fails, likely, the word or phrase is not found in AI’s dictionary.

   Example 3:

   In this example, the assumption is that a mis-transcribed word or phrase is *not* in the AI’s dictionary. This scenario requires a different strategy consisting of just two steps. Continuing with the “Barton County” example, again, suppose that phrase is mis-transcribed as ‘Pardon County’. In this case, ‘Barton County’ is unknown to AI.

To remedy this is a two-step procedure. In step one, what we can do is boost 'Pardon County'—the mis-transcribed word —which *is* in the dictionary. (The reason for this will be made clear in step two). This gives 'Pardon County' the highest weight among similar phrases known to AI. The result is to increase the likelihood that the AI will transcribe that phrase.

Now, in step two, we can use Search and Replace to create a fixed, one-to-one mapping between the mis-transcribed phrase, 'Pardon County' and 'Barton County', so that AI is now highly likely to transcribe 'Barton County' over any other phrase the greatest percentage of the time. The following steps illustrate this procedure.

To map a boosted word or phrase to another using find and replace:

1. In the Boost Phrase field, enter 'Pardon County', the mis-transcribed phrase.
2. In the Boost Phrase Value field, from the drop-down menu select "20 (Very likely)".

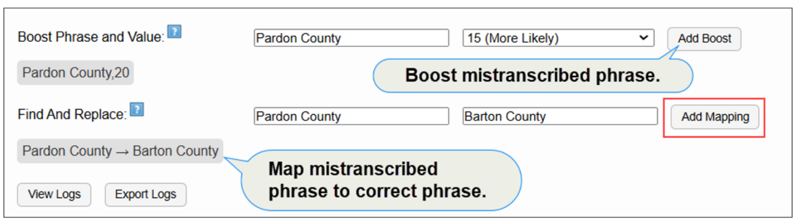


Fig. 10.32 **Boosting a Word or Phrase Using Find and Replace**

3. Select Add Boost.
4. In the Find field, enter 'Pardon County'.
5. In the Replace field, enter 'Barton County'.
6. Select the Add Mapping button.

   This mapping now maximizes the likelihood that AI will correctly transcribe 'Barton County' instead of 'Pardon County'.

7. Repeat this process to configure replacement words for unknown names, adding word or phrase mappings as required. Each new mapped pair will appear on-screen across the page.
8. Leave the Service Account Key section as-is. The Service Account Key will have been uploaded earlier already by an Eventide Communications technician, as indicated by the green check mark in the next screenshot.

By default, only configure the ‘911 Positions’ Resource Group for transcriptions.

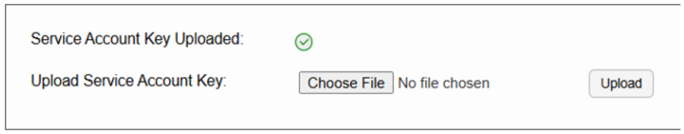


Fig. 10.33 **Service Account Key**

9. Select Save.

10.6. Configuring Retention Settings

The Retention Settings tab allows you to configure rules that determine how long recordings are stored on the NexLog DX-Series recorder for auditing, after which you can free up space.

To configure retention settings:

1. Select Recording → Retention Settings. The Retention Settings tab opens.

> **Note**
>
> The following screenshots show *sample values only*. Values entered here should be exclusively as per customer requirements.

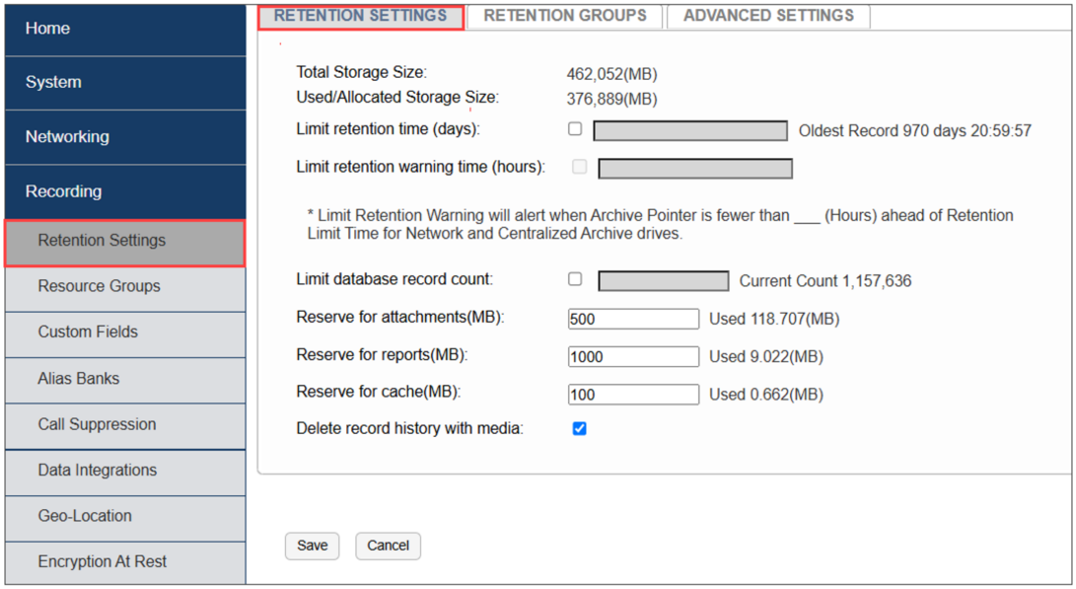


Fig. 10.34 **Retention Settings Tab**

2. Select the following checkboxes:

- **Limit retention time (days):** *<Enter value per customer request>*.
- **Limit retention warning time (hours):** *<Enter value per customer request>*.
- **Limit database record count checkboxes:** *<Enter value per customer request>*.

3. Type values for each of these settings as required.

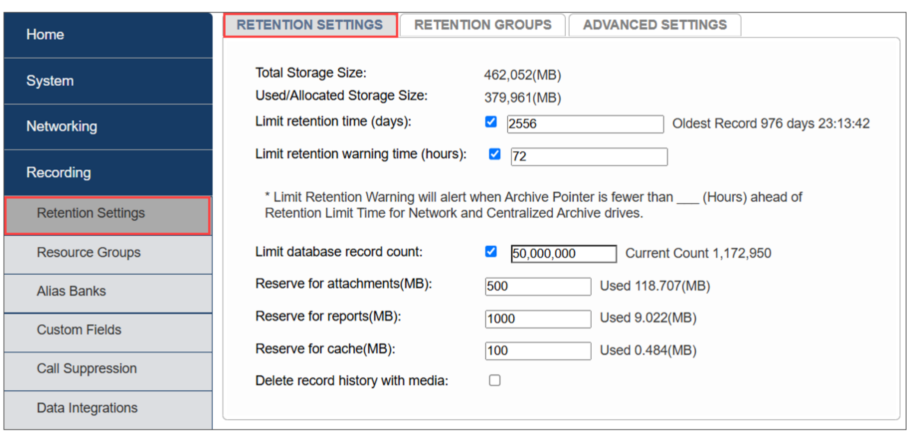


Fig. 10.35 **Setting the Retention Time**

4. Enter values for the following settings in the corresponding fields as per customer requirements.

- **Reserve for attachments (MB):** *<Space in MB to reserve for attachments>*.
- **Reserve for reports (MB):** *<Space in MB to reserve for reports>*.
- **Reserve for cache (MB):** *<Space in MB to reserve for cache>*.
- **Delete record history with media:** *<Space in MB to reserve for media record history>*. *Leave this setting blank by default*.

> **⚠ Caution**
>
> The setting **Delete record history with media** will delete *all* recordings and can be potentially dangerous. Enable this setting *only* if your intention is to delete *all recordings*. Otherwise, leave this setting blank.

The reserve space values shown in Fig. 10.35 are only suggestions for reserving storage for attachment, cache, reports.

10.7. Configuring Custom Fields

The CIAI Service Provider should configure all specified custom fields, as per customer request. Specifically, technicians should configure new custom field groups.

To configure custom fields and custom field groups:

1. In the left navigation menu, go to Recording → Custom Fields. All existing custom fields are listed here.

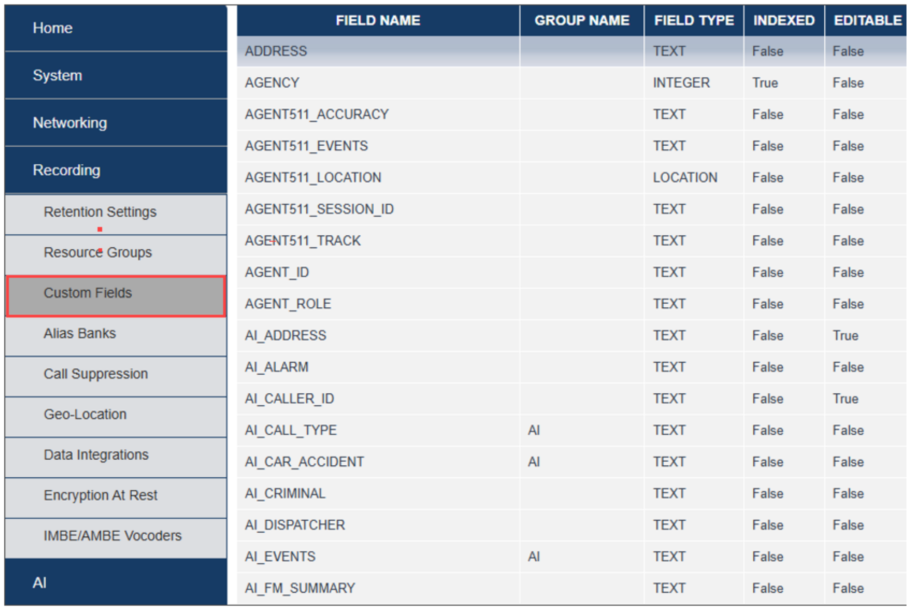


Fig. 10.36 **Configuring Custom Fields**

2. At the bottom of the page, select **Add Field**.

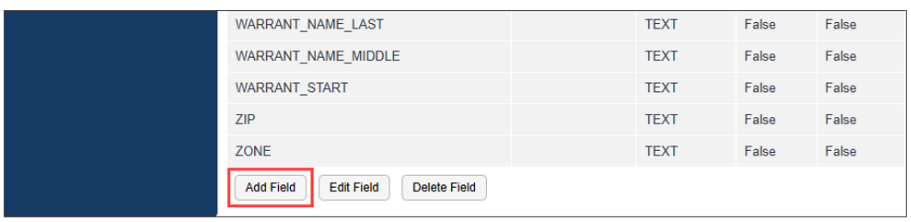


Fig. 10.37 **Adding Custom Fields**

The **New Custom Field** page opens.

3. In the Field Name field, type a name for the new field.

4. In the Group Name drop-down menu, type the group name to which the custom field should belong. This optional field is used to group custom fields together in CIAI search filters. Default options are ‘AI’ and ‘Transcription’.

   You can also create new custom field groups here.

5. For CIAI, Service Provider technicians should create the following Custom Field Groups:

    - CAD
    - TELEPHONY
    - RADIO
    - LOCATION

6. Create a new Group Name by selecting the New checkbox and then typing a name in the Group Name field.

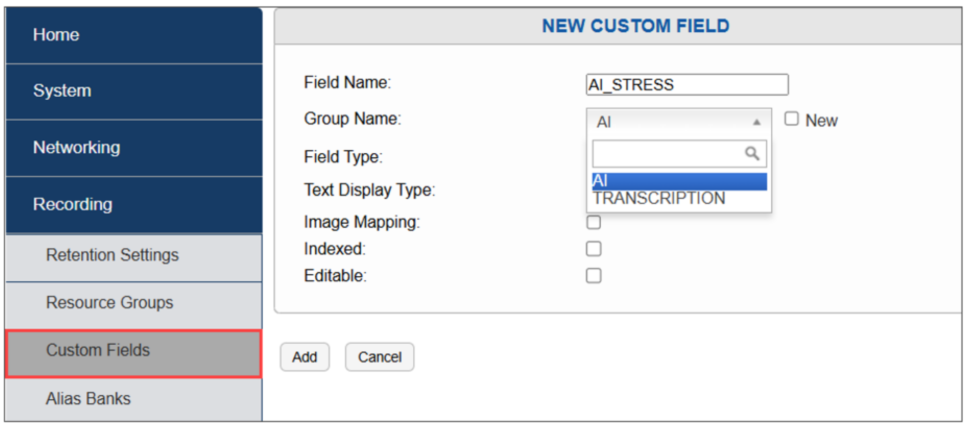


Fig. 10.38 **Creating a Group Name**

7. From the Field Type drop-down menu, select a Field Type, e.g. 'Text'.

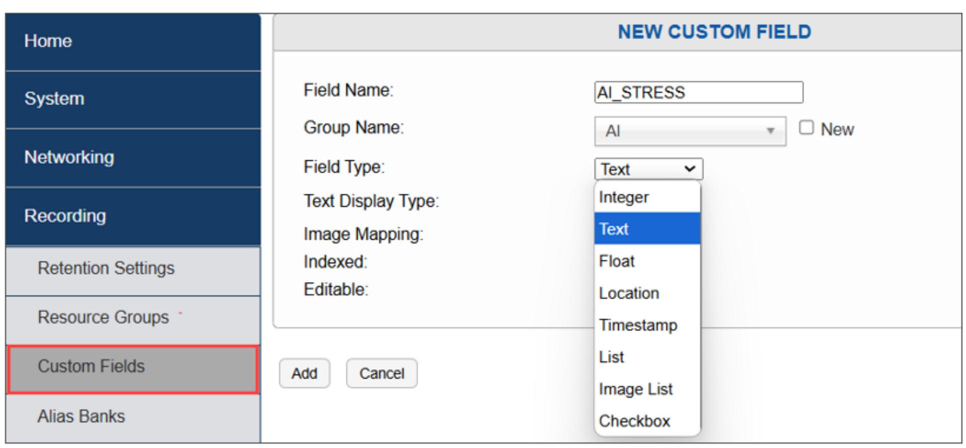


Fig. 10.39 **Selecting a Field Type**

8. From the Text Display Type drop-down menu, select the Text Display Type. For standard text display, choose ‘Standard’.

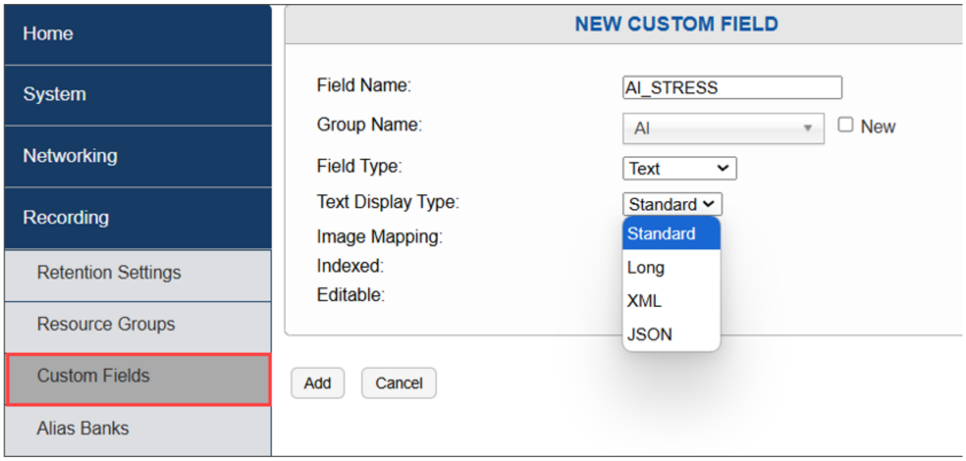


Fig. 10.40 **Selecting the Text Display Type**

9. To add an image icon, select an icon from among the various displayed icons. The icon now appears to the right of the Value field.

10. In the Value field, type a text-based value.

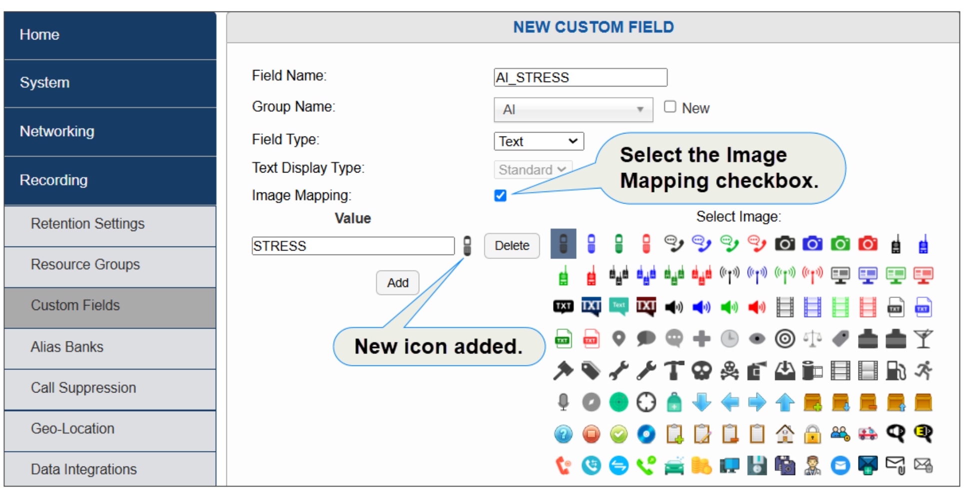


Fig. 10.41 **Adding an Image Icon**

11. If you select Indexed, the recorder database will maintain an index on metadata in CIAI (and the Front Panel). This yields faster search and retrieval, at the expense of added server CPU load. Select the field if commonly searched.

12. To make the custom field editable, select the Editable checkbox. If selected, users can edit the value of this field in CIAI; otherwise, only the CIAI Service can control the value of the custom field for a call.

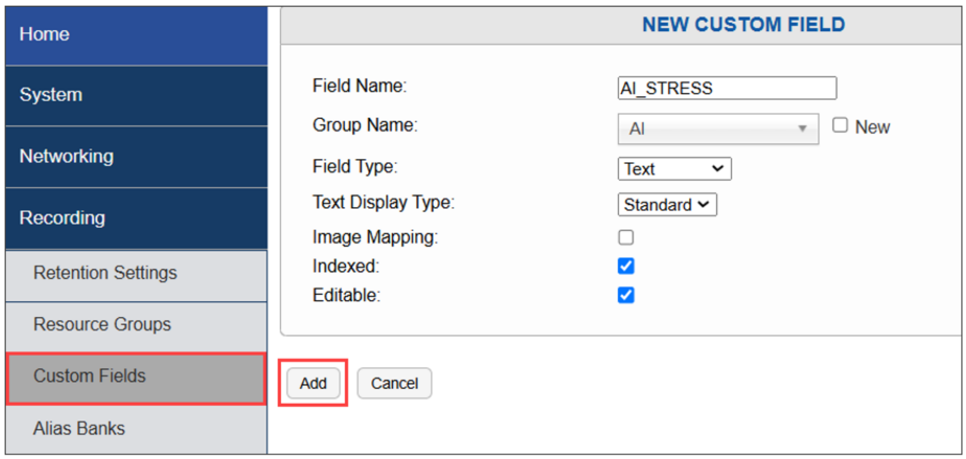


Fig. 10.42 **Saving Custom Fields**

13. Finally, select the Add button to save your new custom field. For more information on custom fields, see the NexLog DX-Series User Manual, *Section 7.3.6. "Custom Fields"*.

10.8. Configuring NexLog Reports

CIAI Service Providers are responsible for setting up NexLog reports for the customer, namely, choosing which reports to enable, running those reports and specifying report recipients.

Report types include:

- Basic Reports
- Advanced Analytics Reports
- 911 Call Handling Report

For further information on setting up and running NexLog Reports, refer to the *Enhanced Reports* Manual.

For any requests concerning custom reports, the customer should contact Eventide Communications.

10.9. Configuring CIAI User Interface Default Settings

- Once the prior steps are complete, configure the default settings for the CIAI user interface.

10.9.1. Adding Default Header Columns

To add default header columns

- In the top right pane, first right-select the header columns menu and then select your preferred AI header columns. Recommended minimum default fields:
  - Channel Name
  - Start Time
  - Duration
  - Caller ID
  - DTMF
  - Call Direction
  - AI Stress
  - AI Call Type
  - AI Subject
  - AI Summary

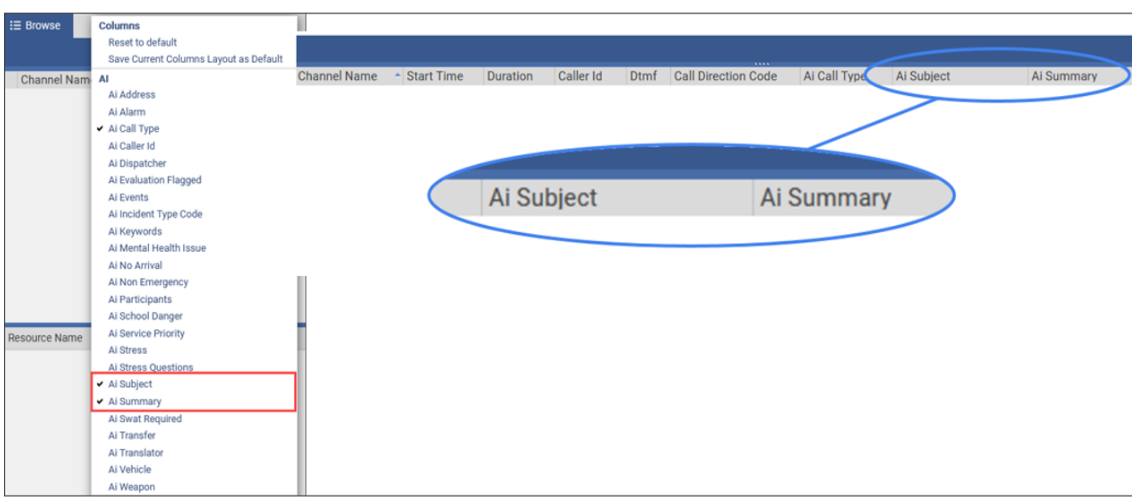


Fig. 10.43 **Selecting AI Column Headers**

These header columns represent basic defaults. Customers can further customize these defaults to their preference.

10.9.2. Displaying and Docking the Call Properties Pane

The Call Properties pane should be displayed and docked. It is not displayed by default.

To display and dock the call properties pane:

1. From search results, right-select a call and then select Properties.

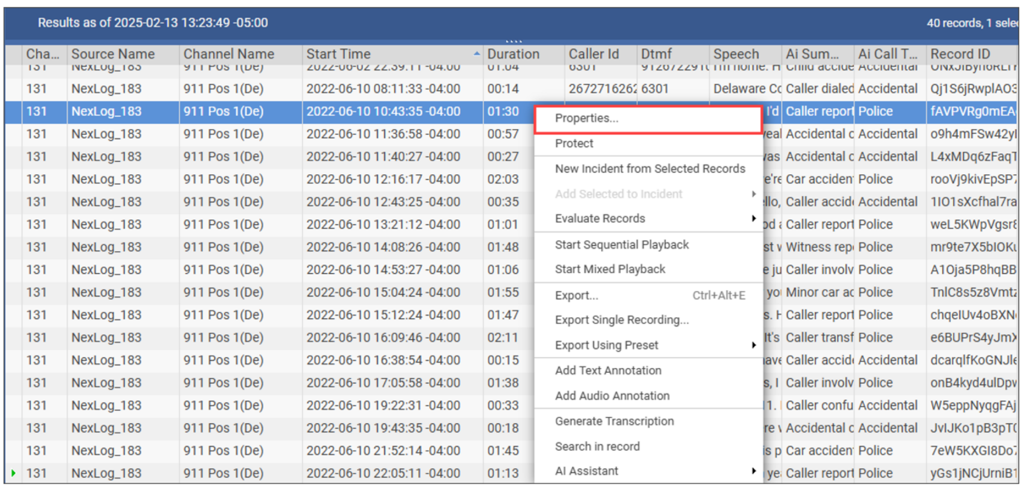


Fig. 10.44 **The Call Properties Pane**

The Call Properties dialog opens.

1. Select the “-” sign in the top right corner of the dialog to dock it on the right (if the Call Properties dialog open floating on-screen).

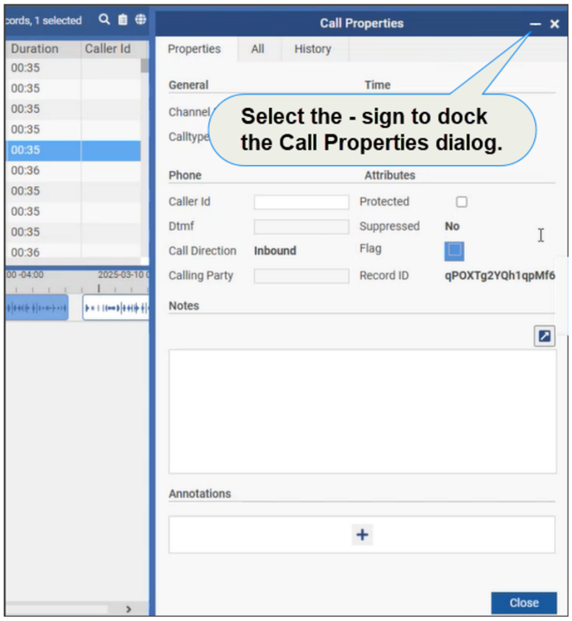


Fig. 10.45 **Docking the Call Properties Pane**

10.9.3. Displaying Default Tabs

To display default tabs:

- Go to File → New tab and select the following tabs to open them:
  - Browse
  - Search
  - Evaluations

10.9.4. Displaying the Transcriptions Tab

The following Call Properties tabs are displayed by default:

- Properties
- All
- History

To display the transcriptions tab:

1. In the main menu bar, right-select the Tools menu and select Edit Call Properties.

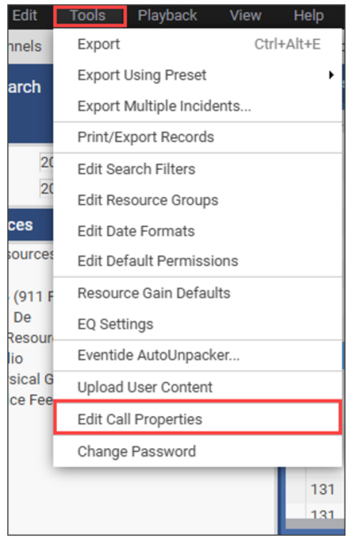


Fig. 10.46 **Edit Call Properties**

This latter action adds two buttons to the Call Properties menu, a plus (+) sign and a cog icon.

2. In the top right of the Call Properties dialog, select the cog icon.

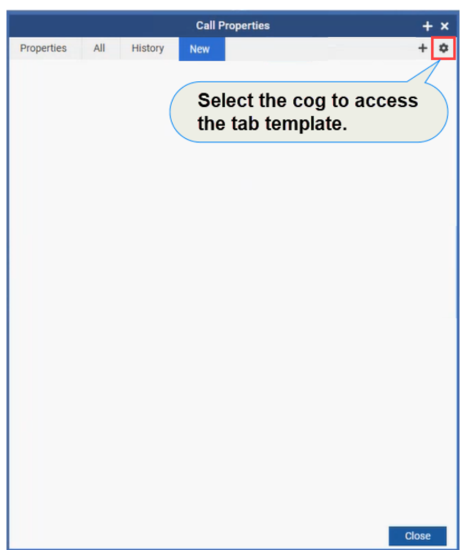


Fig. 10.47 **The Tab Template**

3. Select the template you want. You can now create a tab layout. You can select a blank layout or use an existing template. For setup purposes, we will select an existing saved layout.

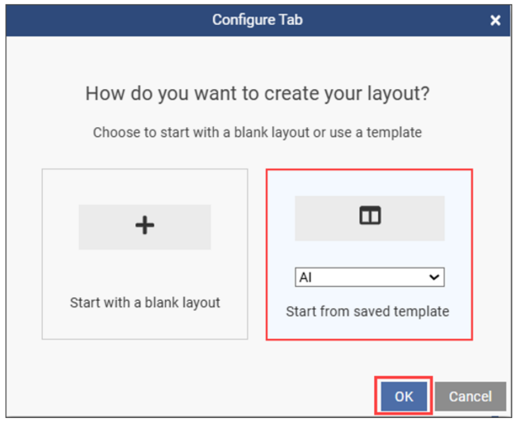


Fig. 10.48 **Tab Layout**

4. Select OK.
5. From the Configure Tab dialog, in the Tab Name field, type a unique name.
6. Select New Section.
7. Select the Edit pencil icon.
8. In the drop-down menu that appears, from the available field options, select Transcription.
9. Select the Add Field button to add the new Transcription field.
10. Select OK.

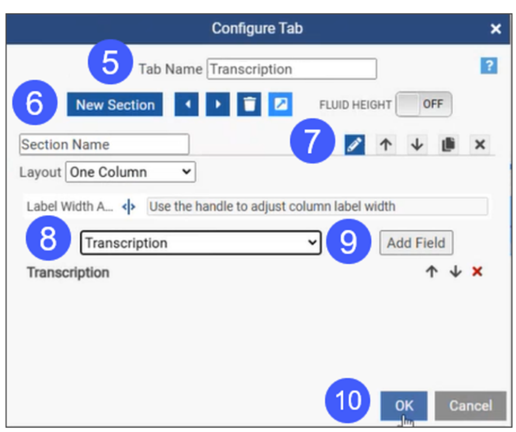


Fig. 10.49 **Adding the Transcription Tab**

The Transcription tab is now added.

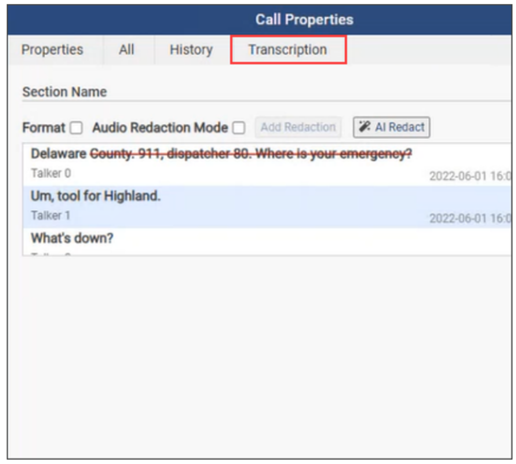


Fig. 10.50 **The Transcription Tab Successfully Added**

11. Optionally, add a user-edited transcription pane to the Transcriptions pane by following the same procedure shown in this section by selecting User-Edited Transcription, as in step 8.

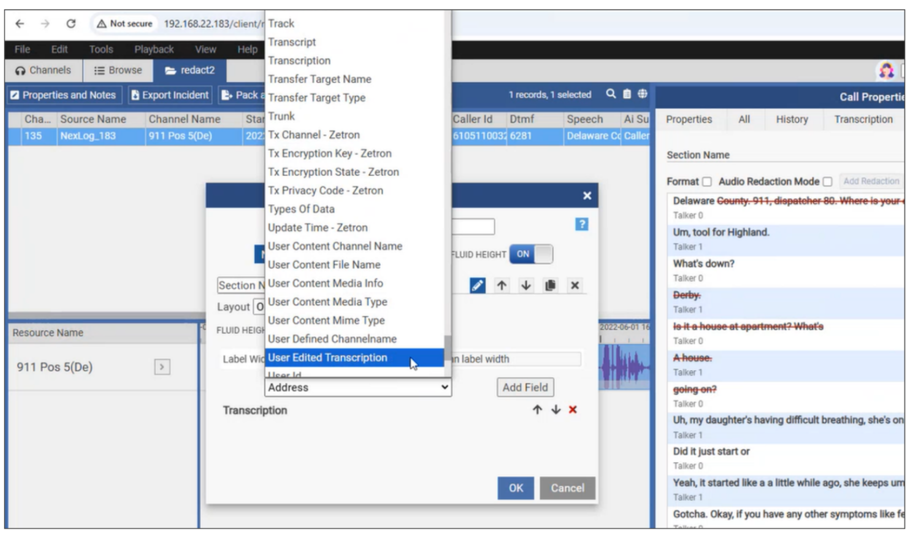


Fig. 10.51 **Adding the User-Edited Transcription Tab**

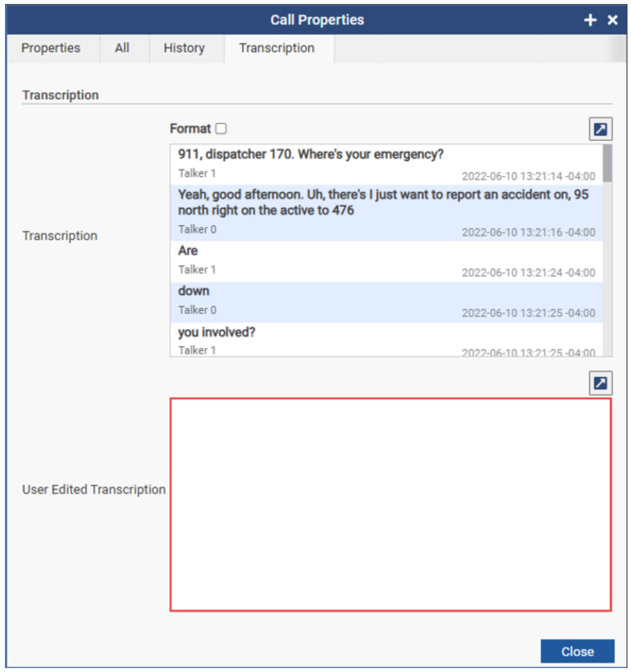


Fig. 10.52 **User-Edited Transcription Tab Successfully Added**

10.9.5. Displaying Transcriptions in the Timeline

Call transcriptions are not shown on the timeline by default.

To display transcriptions in the timeline:

1. In the main menu, select View –> Icons and Markers.
2. From the fly-out menu, select Show Transcription in Timeline.
3. Also select Show Calltype Icons.

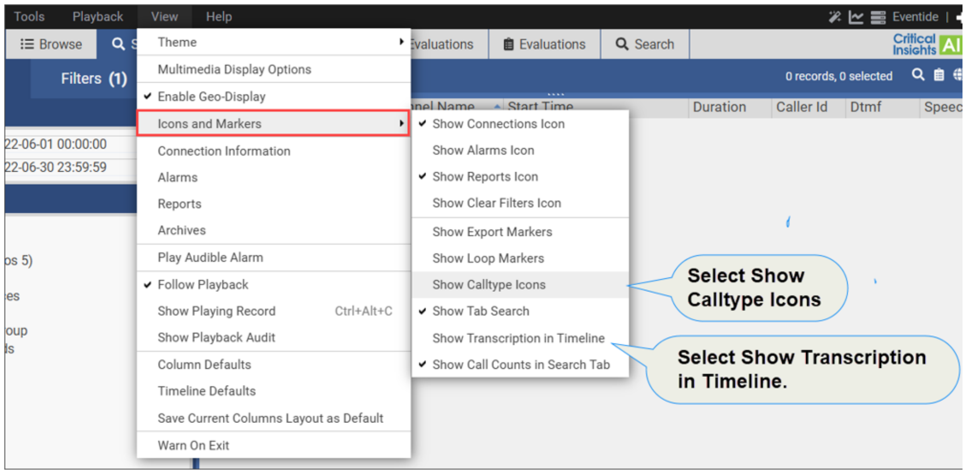


Fig. 10.53 **Displaying Transcriptions in the Timeline**

4. Right-select a call and then select Generate Transcription.

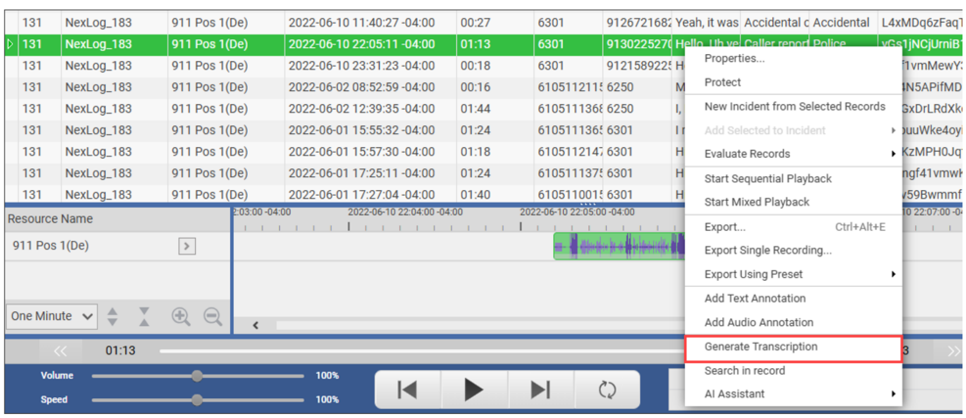


Fig. 10.54 **Generating a Transcription**

Transcriptions are now displayed for calls in the timeline.

10.9.6. Saving the Current Header Columns Layout as Default

You can save your most recent configuration changes to the CIAI header columns.

To save the current header columns layout as default:

- Right-select anywhere in the header column section (grey bar) and select Save Current Columns Layout as Default. This action sets the UI back to its default settings. Now you can configure the user interface.

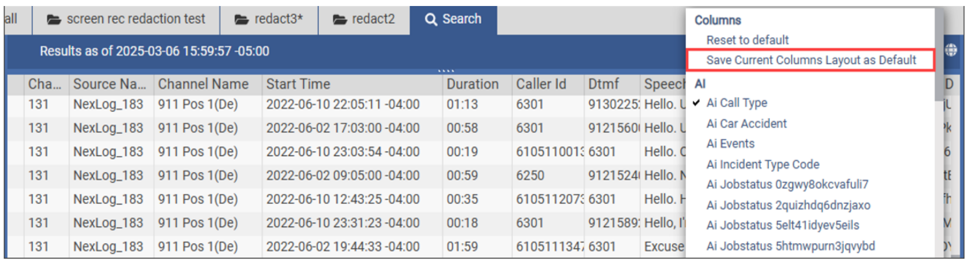


Fig. 10.55 **Saving the Current Columns Layout as Default**

10.9.7. Running Queries with AI Research Assistant

You should run queries with the AI Research Assistant to verify that it is working properly. This includes its voice-activated modes.

To run queries with AI Research Assistant

1. At the top right of the CIAI main menu bar, select the AI Research Assistant icon to the left of the customer's username.

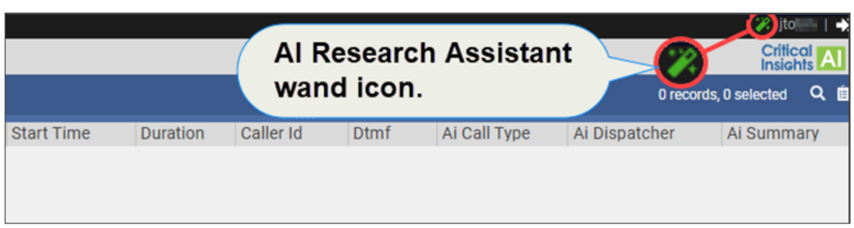


Fig. 10.56 **AI Research Assistant Icon**

The AI Research Assistant pop-up dialog opens.

2. Verify that AI Research Assistant is working properly by running a query.

3. In the text field provided, enter a search query, e.g., “Show me all calls from last week containing the word “accident”. (Include the agency name in the query to test for accuracy of transcription).

4. Confirm that search results are returned. If not, try using a specific date/date range, or include the channel name, and/or a different search keyword.

5. Test voice-activated search functionality by activating it and running a vocal search query (using a headset).

6. Similarly, test the ‘Hey Assistant’ voice-activated function by speaking the phrase, ‘Hey Assistant’ into a headset to automatically run a search query.

7. Confirm in each case that search results are returned.

   For instructions on how to run voice-activated queries, refer to the *AI Research Assistant Quickstart Guide.*

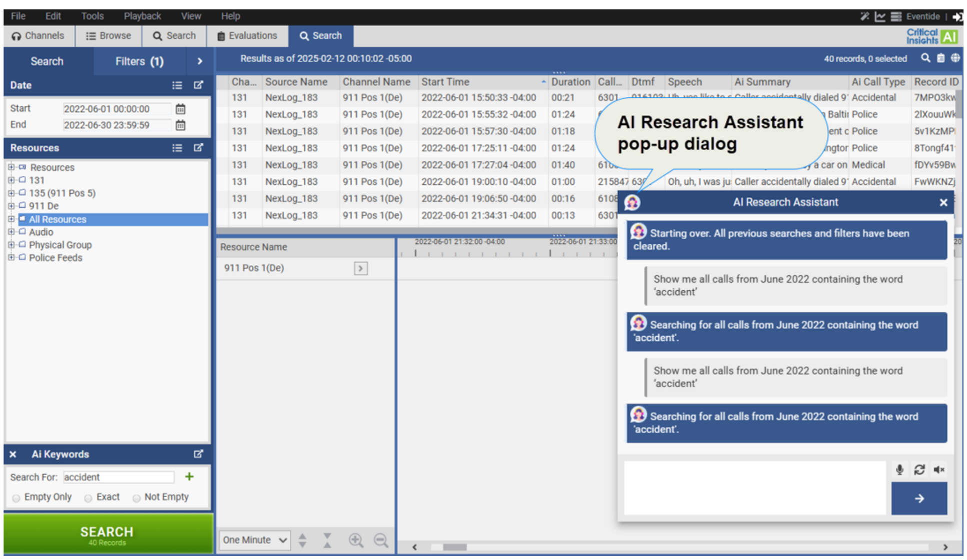


Fig. 10.57 **AI Research Assistant**

Note

Mozilla Firefox browser does not support voice-activated search queries for CIAI. Use Google Chrome or Microsoft Edge instead.

8. From the call results displayed, right-select a call and choose Properties to inspect the call properties.

10.9.8. Verifying Resource Groups

To verify Resource Groups:

1. Confirm that all previously-configured Resource Groups and their corresponding channels successfully show up in the left pane of the UI. If not, you should check the Group Rules for that Resource Group. To do so:
2. Sign in to Web Configuration Manager.
3. Go to Recording → Resource Groups.
4. Select a Resource Group, e.g. ‘911 Positions’ and then select the Group Rules button.
5. Make sure that Search Rules and Permissions Rules are selected for that Resource Group.

Before completing the configuration of the CIAI user interface, one additional task remains.

10.9.9. Adding Call Type Icons

Call type icons (shown in the following screenshot in the Resource name pane of the CIAI timeline) are not automatically transferred to CIAI and so do not show up by default.

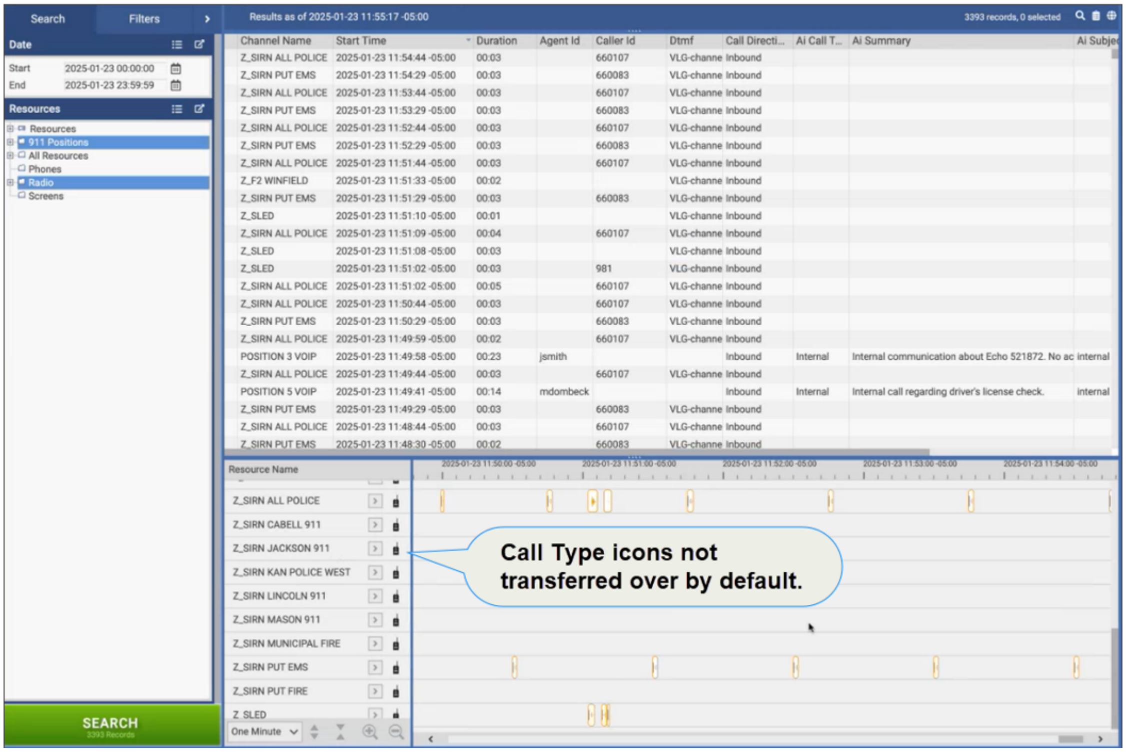


Fig. 10.58 **Adding Call Type Icons**

To add or transfer these icons to the CIAI user interface, they must be configured from the CIAI Web Configuration Manager.

To add calltype icons to the CIAI user interface:

1. Sign out of CIAI and sign in to the CIAI Web Configuration Manager by selecting the cog on the lower right of the page.

2. Go to Recording –> Resource Groups.

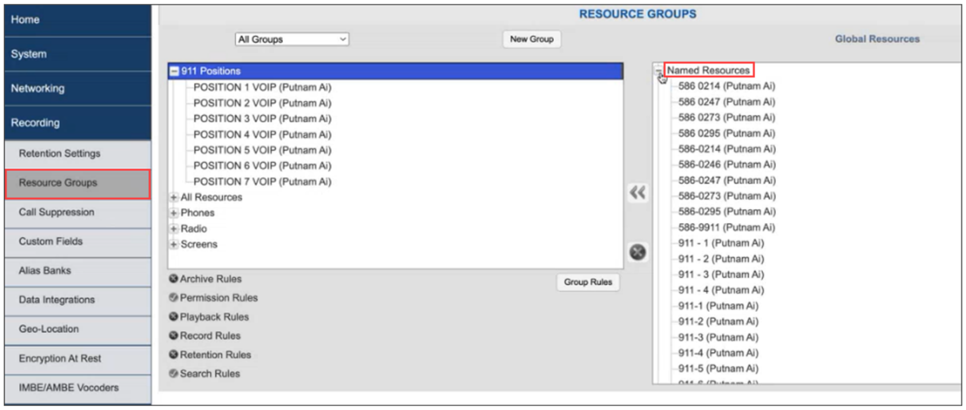


Fig. 10.59 **Named Resources**

3. In the Global Resources pane on the right, under Named Resources, select the group of channels for which you want Call Type icons to appear.

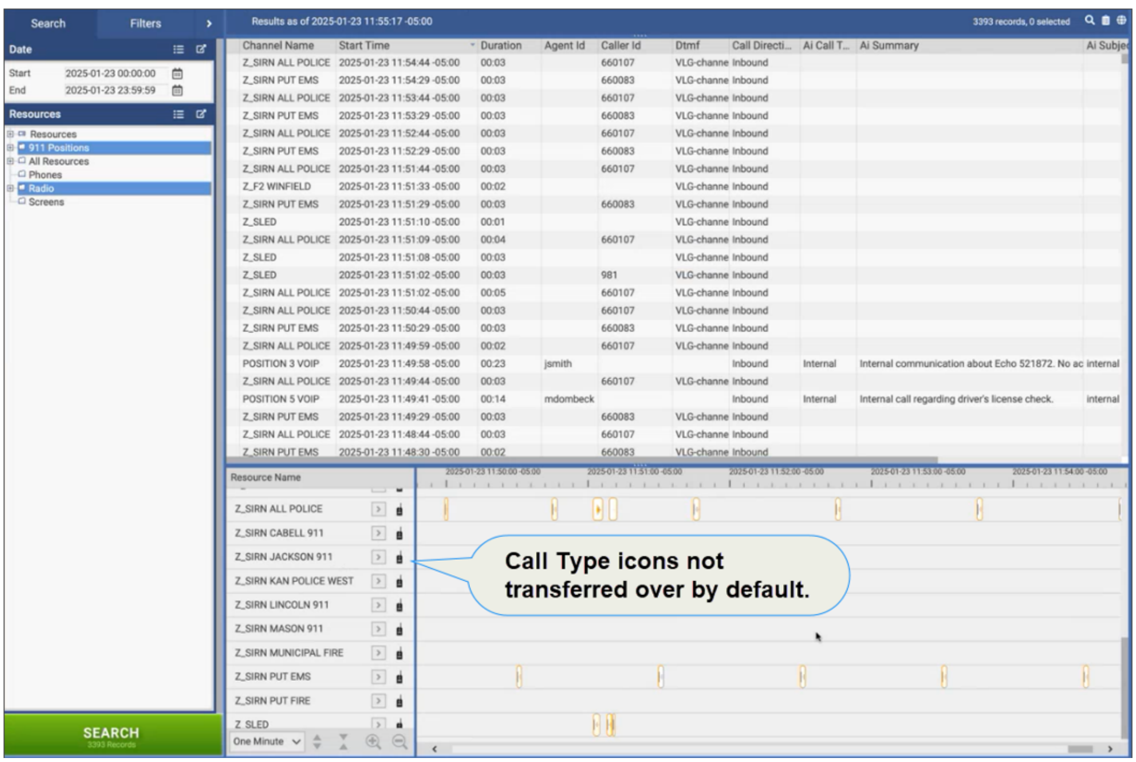


Fig. 10.60 **Selecting Channels**

4. Right-select a group of channels and from the menu, select Edit Resource Type.

5. From the Resource Type menu, select Phone.

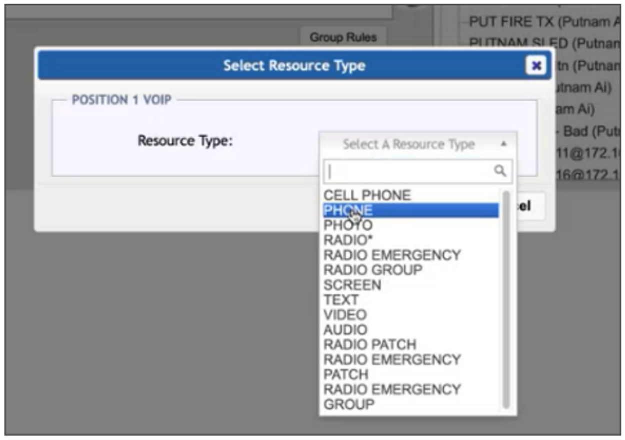


Fig. 10.61 **Selecting a Resource Type**

6. Select OK.

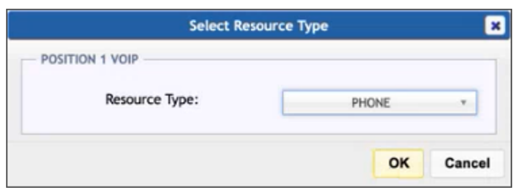


Fig. 10.62 **Adding Channels for a Resource Type**

A popup confirms that the Call Type icons were successfully added.

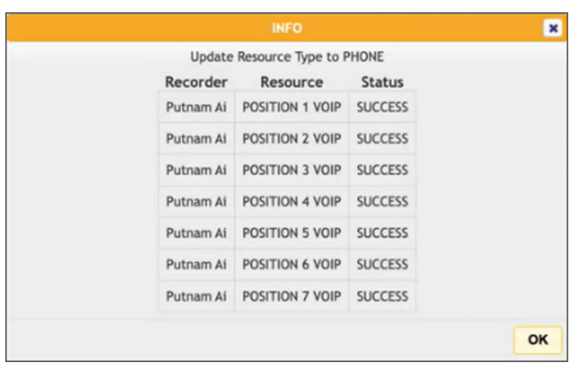


Fig. 10.63 **Call Type Icons Successfully Added**

10.9.10. Applying the Default Configuration to New Users

To apply the default configuration to new users:

1. Go to Users and Security –> Users.
2. First, right-select the account for the currently signed-in user (e.g., admin) and then select Use selected user as new user configuration.

Fig. 10.64 **Applying the Default Configuration to New Users**

Now, if you create a new user, the user will have all your configured defaults.

10.9.11. Applying the Default Configuration to Selected Users

You can also replicate the new configuration defaults to selected users at once.

To apply the default configuration to selected users:

1. On the Users page, press CTRL then click, to successively select all specific users for whom you want to replicate the configuration.

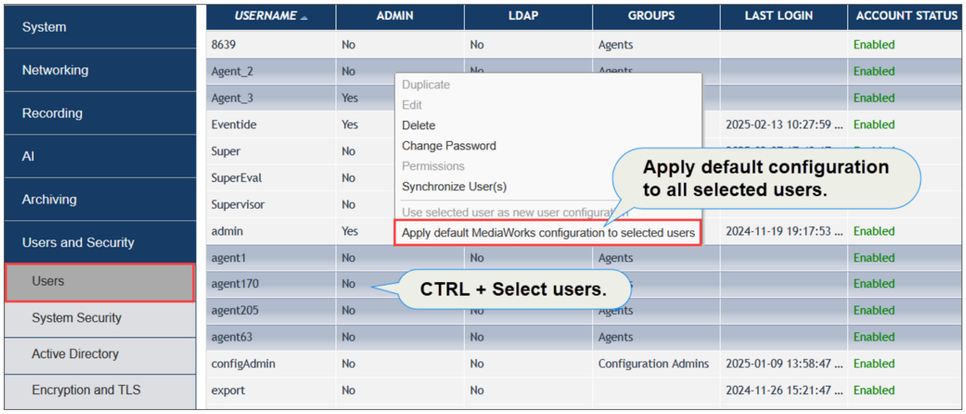


Fig. 10.65 **Applying the Default Configuration to Selected Users**

2. Right-select anywhere in your selections and from the menu select Apply default MediaWorks configuration to selected users. All selected users will now receive the same configuration in the CIAI user interface.

3. Confirm for each of the user accounts you configured earlier that the default configuration has taken.

10.10. Monitoring and Alerts

Monitoring is very important. CIAI Service Provider techniciansshould set up recorder alerts, a higher severity or impact that require attention and a response. They should also set up an email address to notify their service department about alerts, so that end users are notified in case of connectivity or other issues (low remaining storage, etc.).

- Verify that alerts are properly sent out if the connection to CIAI is lost. If there is an outage, then CIAI will not immediately have calls available.

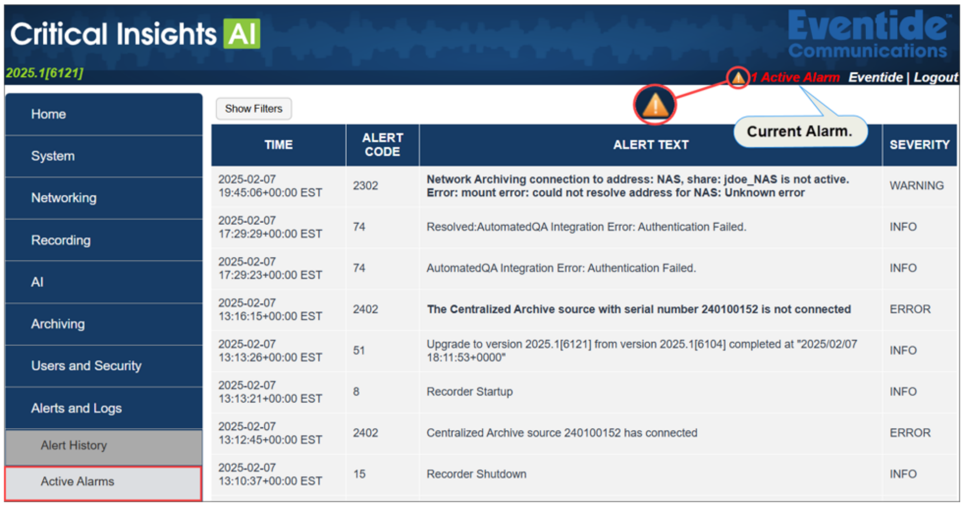
10.10.1. Configuring Email Alerts

This section deals with configuring specific alerts to be sent to an email recipient.

To configure email alerts:

1. In the left navigation menu, select Alert Codes. The Alert Codes page opens. Active alarms are displayed at the top right (in red text) accompanied by an orange Warning! icon.

2. Select the active alarm.



TIME	ALERT CODE	ALERT TEXT	SEVERITY
2025-02-07 19:45:06+00:00 EST	2302	Network Archiving connection to address: NAS, share: jdoe_NAS is not active. Error: mount error: could not resolve address for NAS: Unknown error	WARNING
2025-02-07 17:29:29+00:00 EST	74	Resolved:AutomatedQA Integration Error: Authentication Failed.	INFO
2025-02-07 17:29:23+00:00 EST	74	AutomatedQA Integration Error: Authentication Failed.	INFO
2025-02-07 13:16:15+00:00 EST	2402	The Centralized Archive source with serial number 240100152 is not connected	ERROR
2025-02-07 13:13:26+00:00 EST	51	Upgrade to version 2025.1[6121] from version 2025.1[6104] completed at "2025/02/07 18:11:53+0000"	INFO
2025-02-07 13:13:21+00:00 EST	8	Recorder Startup	INFO
2025-02-07 13:12:45+00:00 EST	2402	Centralized Archive source 240100152 has connected	ERROR
2025-02-07 13:10:37+00:00 EST	15	Recorder Shutdown	INFO

Fig. 10.66 **Active Alarms**

An alarm pop-up dialog opens.

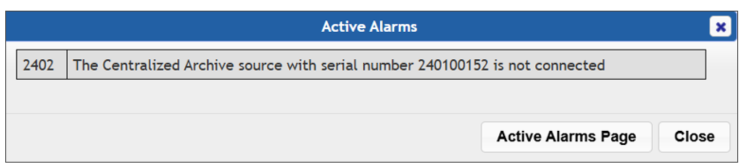


Fig. 10.67 **Pop-up Dialog Displaying Alarm Message**

3. Note the alarm number and then close the dialog.

4. Select Show Filters.

Fig. 10.68 **Show Filters**

5. Search for the alarm number.

Alert Search method 1:

- In the **Alert Code** field, type the alarm number to search for and then select Go.

Fig. 10.69 **Alert Search method 1**

Alert Search method 2:

1. Scroll to the bottom of the page and select the Next and Previous buttons (or enter the page number (estimated)) and select Go. The error message now displays on-screen.

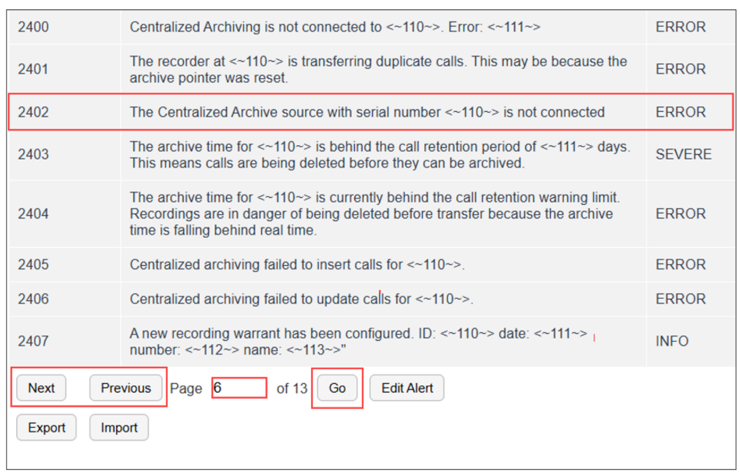


Fig. 10.70 **Alert Search method 2**

2. Select the line that contains the error message number and note the alarm type and its severity.

3. Select Edit Alert.

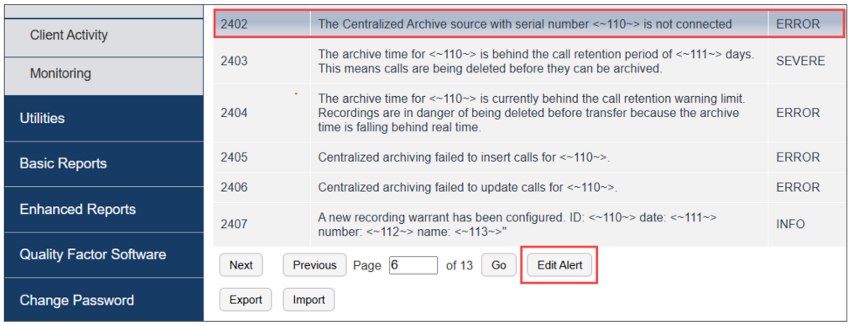


Fig. 10.71 **Editing an Alert**

4. At the bottom of the Edit Alert Code page, select the Send Email checkbox.

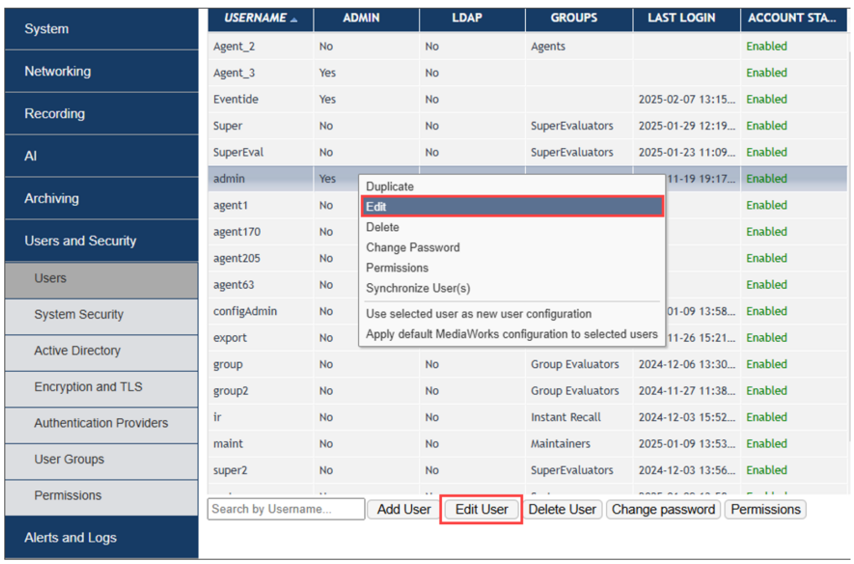


Fig. 10.72 **Setting up Email Alerts**

5. Select Save. As the final steps, you will configure the email address of the alert recipient.

6. Go to Users and Security –> Users.

7. Right-select the user to whom alerts will be sent, and then select Edit from the combo box menu (or alternatively, select Edit User at the bottom of the page).

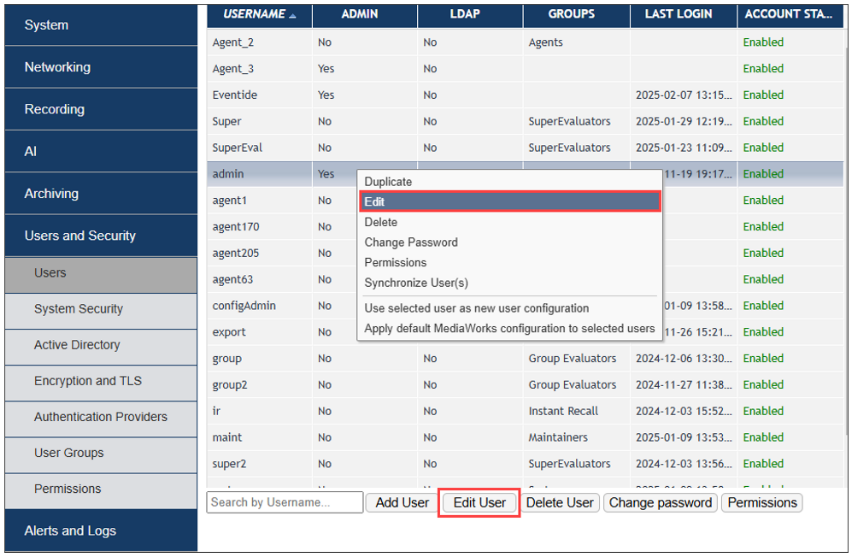


Fig. 10.73 **Edit User**

8. On the User Info tab, in the Email field, enter the recipient's email address.

9. Select Save.

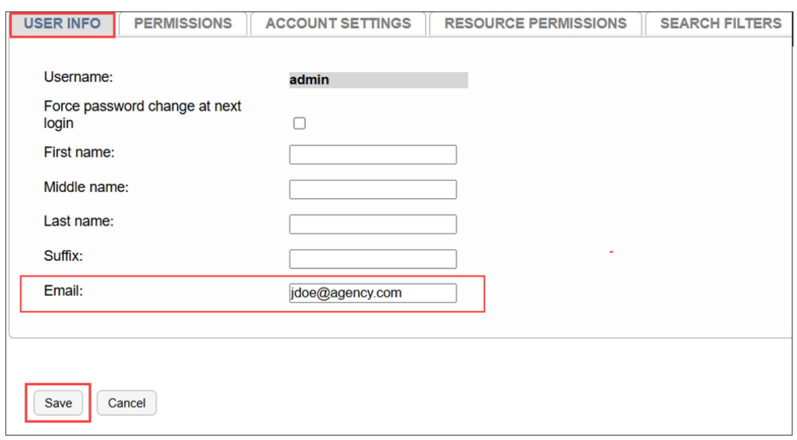


Fig. 10.74 **Selecting an Email Recipient for Alarms**

For all configured alerts, the recipient (e.g., jdoe@agency.com) will now receive an email.

Note

You *cannot* set up email for *all* alerts at once. Alerts must each be set up individually.

10.10.2. Exporting and Importing Alerts

You can also export and import alerts.

To export or Import alerts:

1. Go to Alerts and Logs → Alert Codes. Select Export to export alerts.

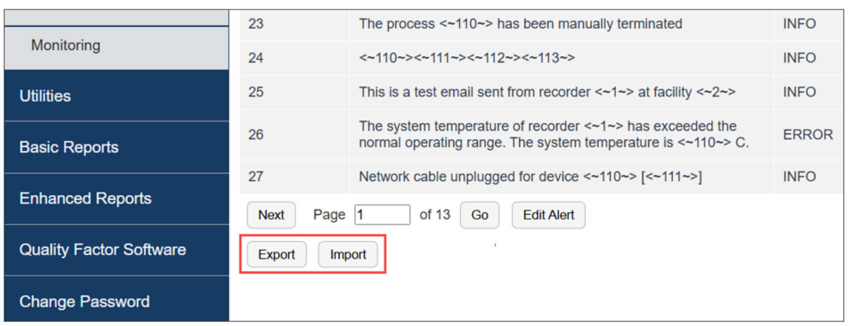


Fig. 10.75 **Exporting and Importing Alerts**

2. Similarly, select Import to import alerts.

10.10.3. Exporting Logs

You can also export logs from the Alerts and Logs → Logging menu.

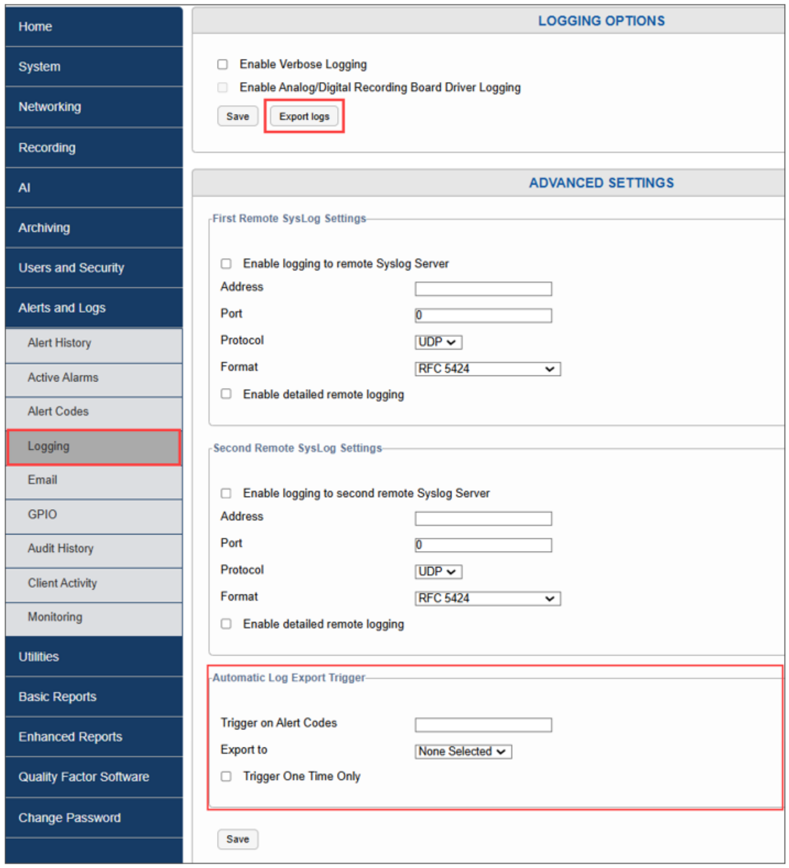


Fig. 10.76 **Logging Options Main Menu**

To export logs:

1. Go to Alerts and Logs → Logging.

2. In the top Logging Options section, select the Export logs button.

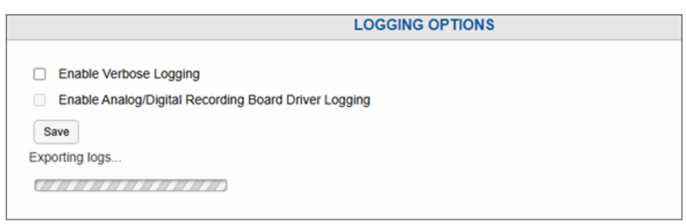


Fig. 10.77 **Exporting Logs**

Step 2 zips the recorder's log files and allows you to download them to your PC to send to the CIAI Service Provider or to Eventide Communications personnel. If running from the front panel, rather than a web browser, you can optionally write the logs to a plugged-in USB Keychain drive or other archive medium rather than downloading them.

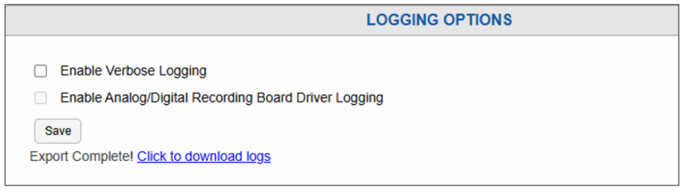


Fig. 10.78 **Logging Options**

3. Leave the other checkboxes at their default settings, un-selected.

   You can also export recorder logs when a specific alert code is triggered, which may indicate an issue. Recorder logs can be exported to available archive drives, ensuring they are saved before getting overwritten.

4. Under Alerts and Logs → Logging, in the Advanced Settings section, scroll to the bottom to Automatic Log Export Trigger.

5. In the Trigger on Alert Codes field, enter the alert code that will prompt the recorder to export its logs.

6. In the Export to drop-down menu, select the archive drive to which you want the logs exported.

   Regarding the Syslog settings in the Advanced Settings section of the page, refer to the NexLog DX User Manual, *Section 7.6.4.1. "Remote Syslog Settings"*.

10.10.4. Monitoring with NMS

Eventide Communications is responsible for basic infrastructure monitoring (i.e. AWS). However, if the customer has purchased NexLog Monitoring Server (NMS) license, which is optional, CIAI Service Providers will be responsible for monitoring the CIAI Service for alerts through NMS. The Service Provider will be notified of alarms and will take appropriate actions to notify Eventide.

NexLog Monitoring Server (NMS) is an HTTPS-based monitoring application for NexLog DX-Series products. NMS requires the following license.

- DX930 - NexLog Monitoring Subscription

If the customer has purchased an NMS license for their recorder, CIAI Service Provider technicians must add the license to it, following the procedure shown in Section 9.5.2 - Adding the CloudSync License.

Once the license is added, CIAI Service Provider technicians can sign in to NMS using their email address and password to monitor the customer's recorder(s) and view, acknowledge, and close all active alarms from a single console.

Fig. 10.79 **NMS Sign-in screen**

NMS provides a dashboard to users upon sign-in, where they can view the health status of their NexLog DX-Series recorders. The NMS dashboard offers the following features:

- **Health Dashboard**: A real-time 24x7 dashboard to view all the customer's NexLog DX recorders and their health.
- **Alarm Filtering**: Create custom re-usable alarm filters for each recorder.
- **Contact Groups**: You can group technicians together and assign them to specific recorders.
- **Recorder Groups**: Group your NexLog DX-Series recorders together for easy access and organization.

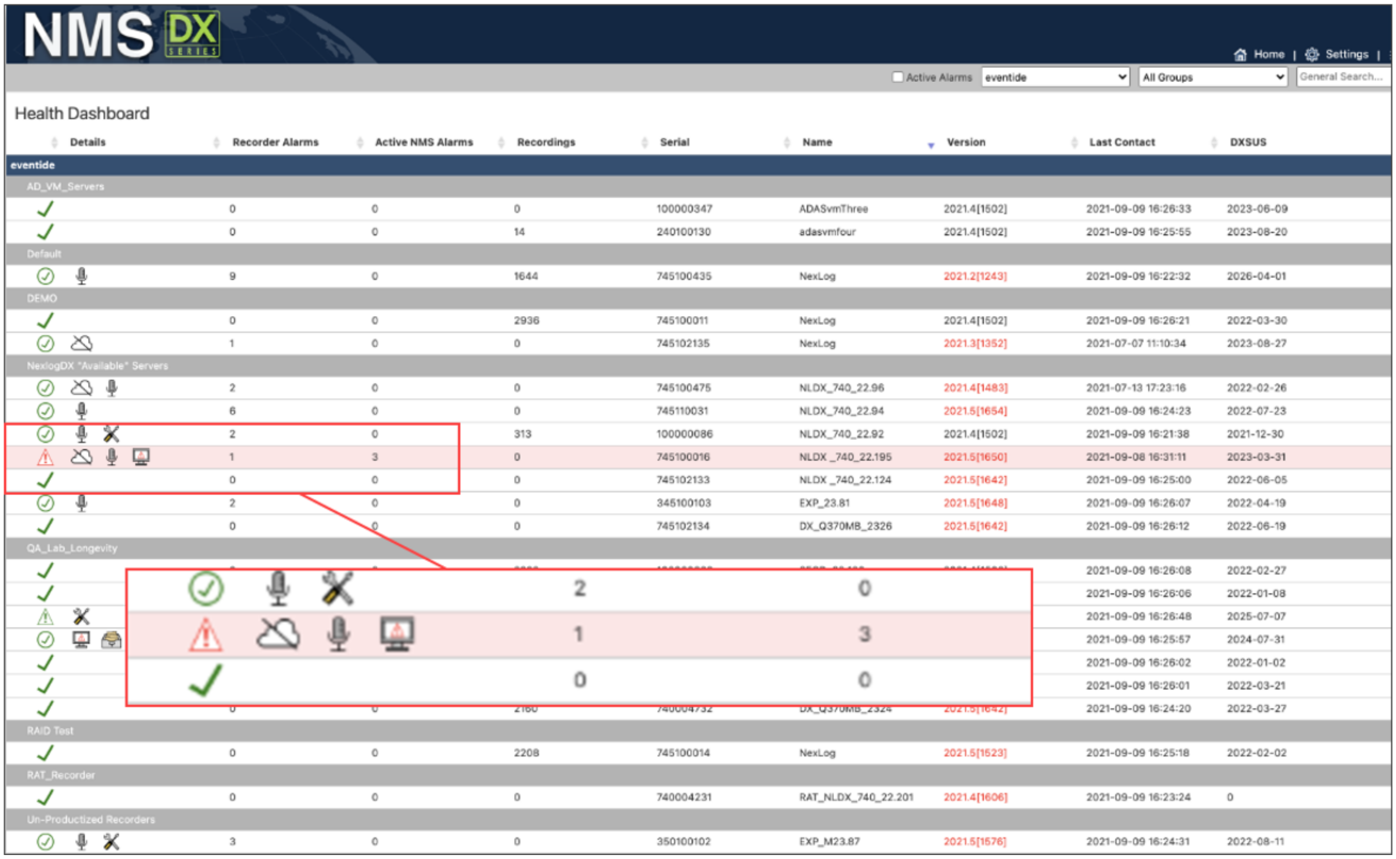


Fig. 10.80 **NMS Monitoring Dashboard**

For more information on NMS, see the NexLog DX-Series User Manual, *Section 7.6.9, “NexLog Monitoring”*.

10.10.5. Setting Up NMS Monitoring

You can set up NMS Monitoring by following these steps:

To set up NMS Monitoring:

1. In the left navigation menu, select Alerts and Logs → Monitoring.
2. On the NexLog Monitoring Server page, enter the following NMS URL:
   `https://monitor.nexlogdx.host/api`
3. Select Save.

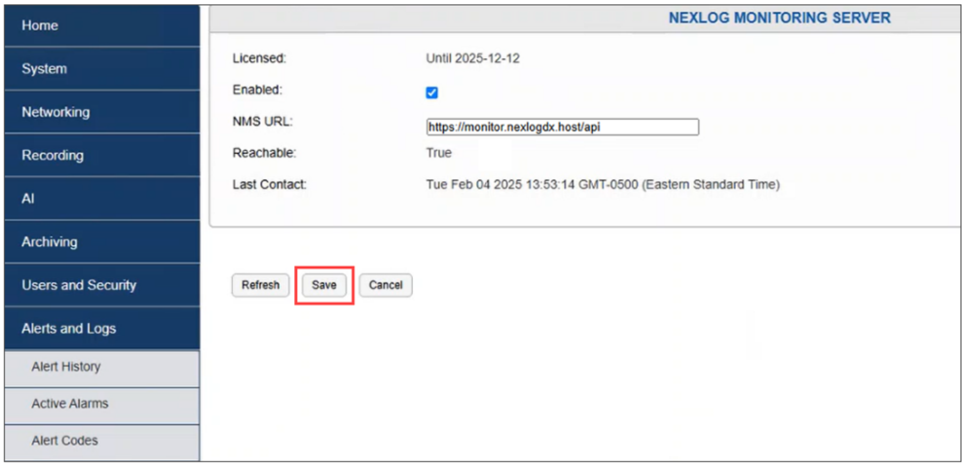


Fig. 10.81 **Saving the NMS Monitoring Configuration**

Alternatively, you can set up an SNMP monitoring console to monitor the recorder. SNMP provides a standard mechanism for System Administrators to manage devices over an IP Network. This is set up from Web Configuration Manager under System → Configuration Files.

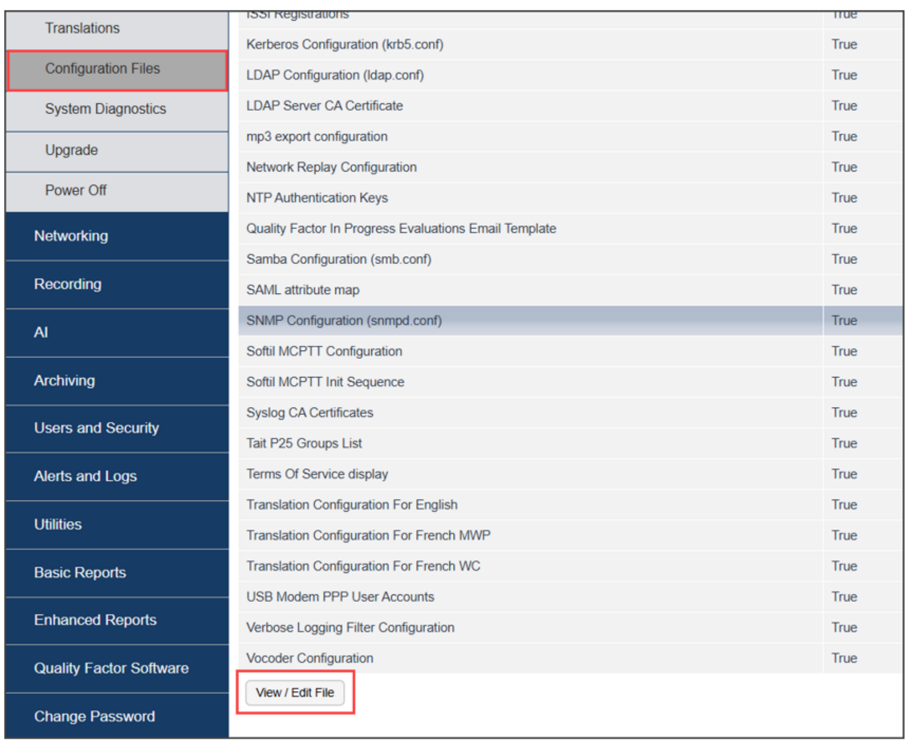


Fig. 10.82 **Setting up an SNMP Monitoring Console**

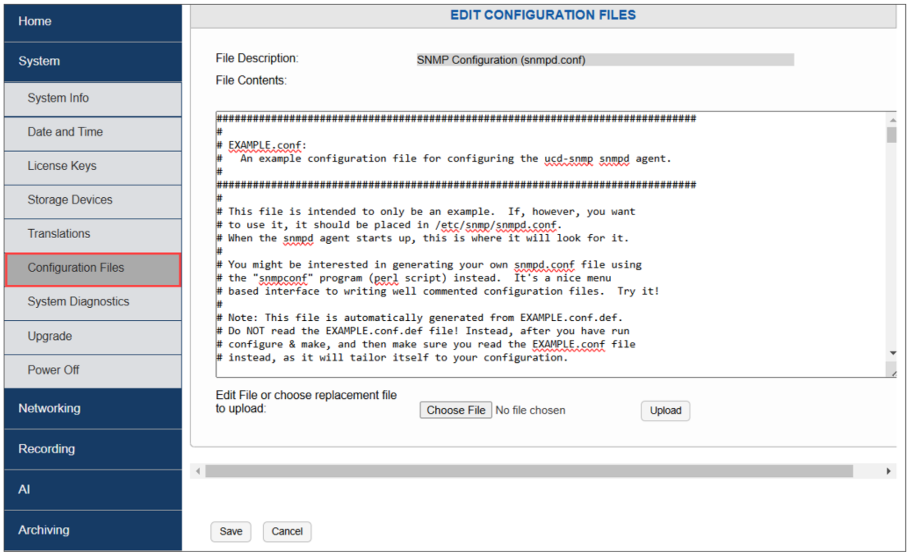


Fig. 10.83 **Configuring SNMP**

For more information, refer to the NexLog DX User Manual, *Section 7.2.5. “SNMP Settings”.*

11. ONBOARDING CUSTOMERS AND END USERS

Onboarding in this context refers to educating CIAI customers on the features, uses, and benefits of CIAI, for example, how to use the AI Assistants. EC could potentially be involved in this step, to process or schedule any customer customization requests regarding AI, QA, or reporting.

To assist in customer education, refer to the CIAI features overview in Section 6.1 - CIAI Feature Overview and to the supplemental documentation listed in Section 5 - Related Documentation

> **Note**
>
> When accessing and viewing CIAI, for optimal viewing performance, Eventide Communications makes the following recommendation for customers:

- Monitor screen size of 27” (minimum) with 2K resolution (i.e., typically (2560 x 1440) *a.k.a* QHD)

This page was intentionally left 99.88% blank.

12. TROUBLESHOOTING

This section deals with troubleshooting connectivity and other issues.

Issue: Cannot connect to CIAI. Error message: "Add Error: Failed to contact destination".

Action: Verify whether the recorder can access CIAI on port 4024.

1. Navigate to Web Configuration Manager on the source recorder, and under **Utilities** ▸ **Network Utilities**,

2. From the Command drop-down menu, select Netcat.

3. Enter the relevant values for the following fields:

   - **IP Address**: <*Enter the customer's domain address*>. (EC provides the customer with a domain name rather than an IP).
   - **Netcat Protocol:** Select TCP.
   - **Netcat Port:** <*The server port accepting the TCP Connection*>. Type 4024.
   - **Netcat Hello String:** <*Optional field. Leave blank*>.

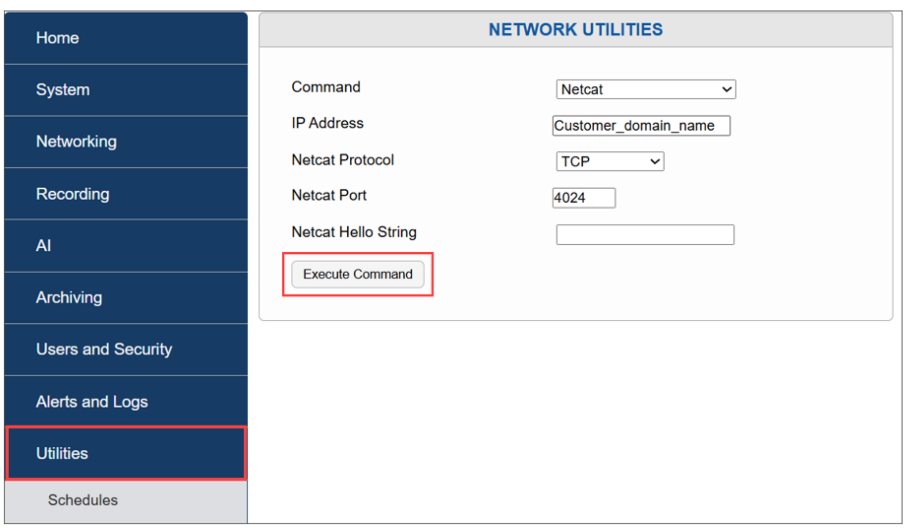


Fig. 12.1 **Executing the Netcat Command**

4. Select Execute Command.

   - If the source recorder can successfully reach port 4024, a success message is returned with a return code of 143.

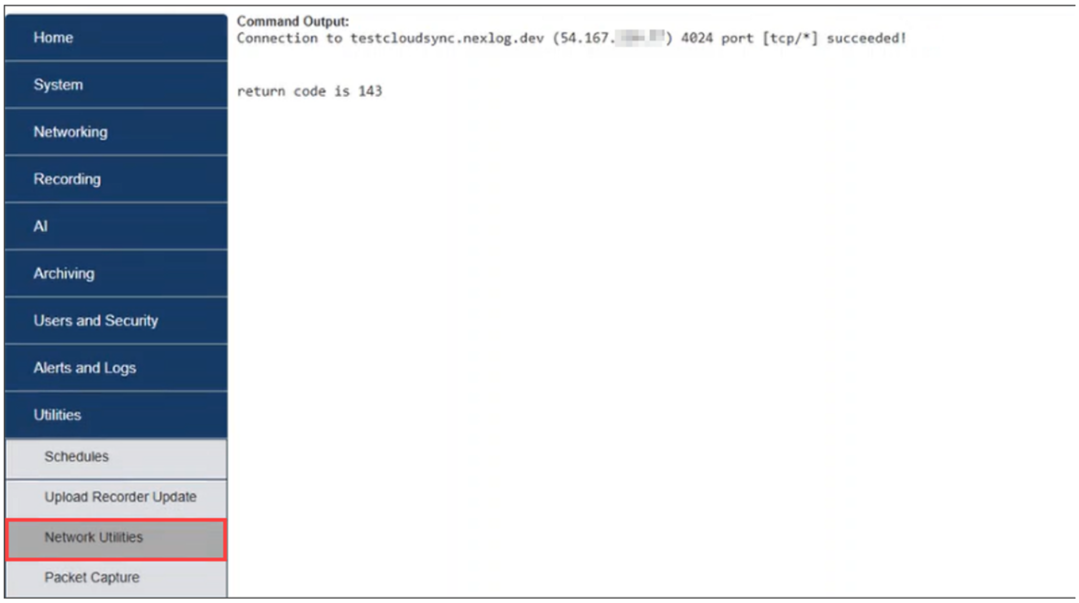


Fig. 12.2 **Success Return Code**

- If no connectivity exists, the page gives a return code of 1.

Fig. 12.3 **Failure Return Code**

If the recorder cannot reach the CIAI service on port 4024, verify that the IP address returned from Network Utilities matches the IP the customer has provided, by following these steps:

1. From the Command drop-down menu, select Get Recorder's Public IP and then select Execute Command.

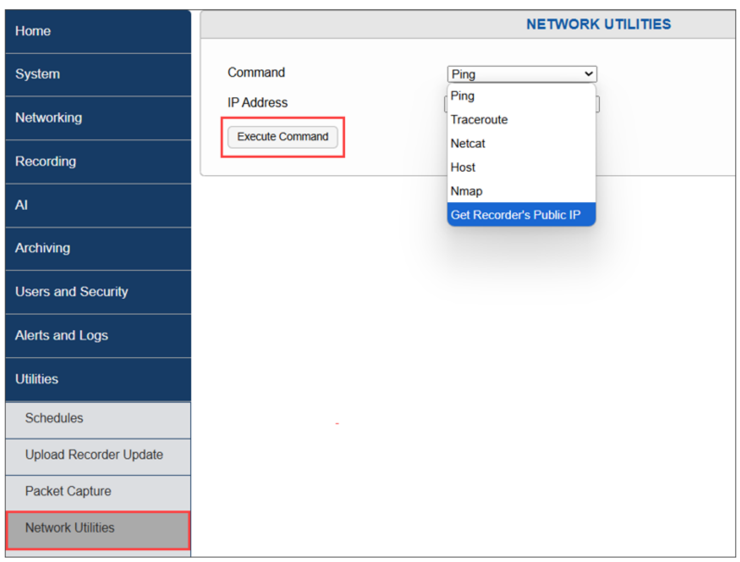


Fig. 12.4 **Getting the Recorder's Public IP**

The results will return the recorder's IP address just above the return code.

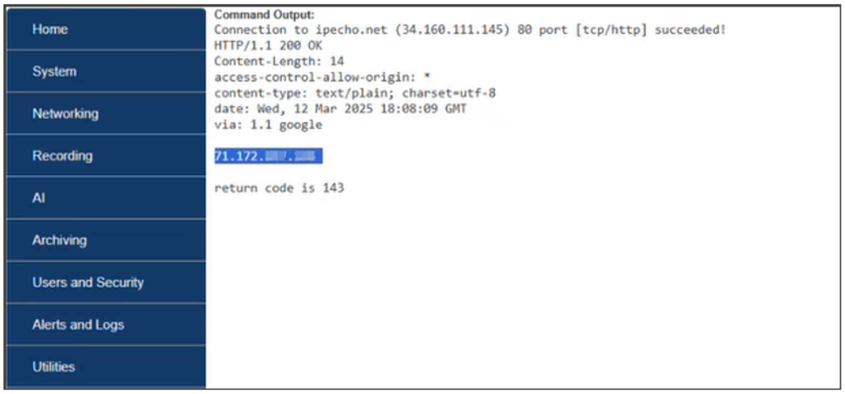


Fig. 12.5 **Displaying the Recorder's Public IP**

If the provided IP address does not match:

1. Have the customer provide the correct IP address and then contact Eventide Communications to have them whitelist it in AWS.
2. Once EC confirms (by email) that the IP has been whitelisted, again select Get Recorder's Public IP, and then select Execute Command to confirm that the correct recorder IP is now updated and displayed.
3. Try to re-connect.

If the provided IP address and other configuration settings are correct, troubleshoot internet connectivity, i.e., cables and networking devices.

Issue: Connectivity to CIAI is established, but the source recorder is not transferring recordings.

Action: If the CloudSync connection indicates that the recorder is processing the call transfer, but no calls are being transferred:

1. Check the time on both the source recorder and the CIAI machine.
2. Make sure they both display the same time and/or time zone.
3. If the time and/or time zone do not match, correct the time and/or date on the source recorder to match that of the CIAI machine and attempt to re-connect. If the time and time zone match, initiate a packet capture from the source recorder.

To initiate a packet capture:

1. From Utilities → Network Utilities, select :guilabel:Packet Capture`.

2. On the Packet Capture page, in the Ethernet Device field, select the correct Ethernet device that will be listening on the network from which the recorder will be sending traffic.

3. To start a packet capture of all traffic being received on the device, leave the Packet Filter (BPF) field blank and select Start Capturing.

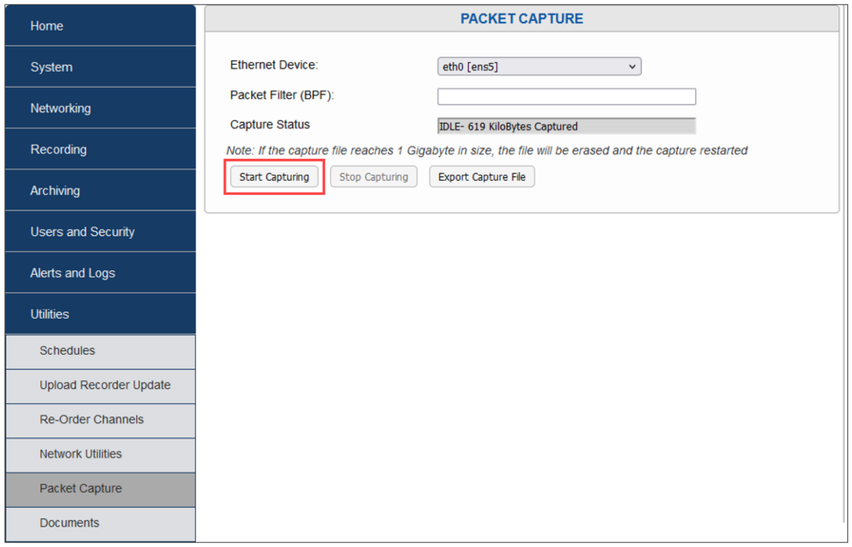


Fig. 12.6 **Performing a Packet Capture**

4. After some time, select Stop Capturing.

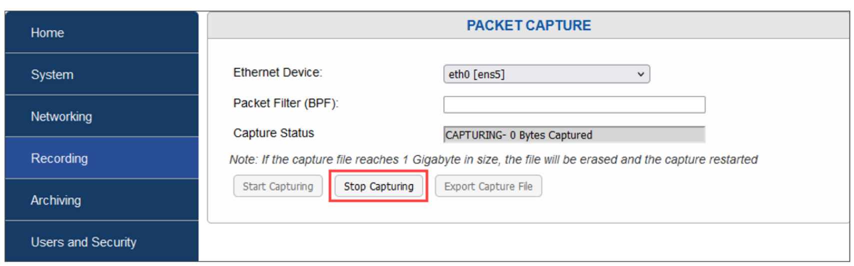


Fig. 12.7 **Stopping the Packet Capture**

5. Select Export Capture File. This action will download the capture file (extension .pcap) to your Downloads folder.

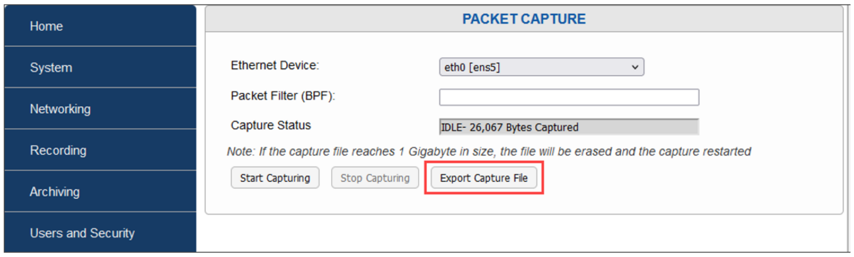


Fig. 12.8 **Exporting the Packet Capture**

6. Open the capture file in a packet capture program (e.g. Wireshark) and inspect the capture output for packet issues.
7. Optionally, in the Packet Filter (BPF) field, you can enter specific commands using advanced filtering options to filter the packet capture based on traffic type.

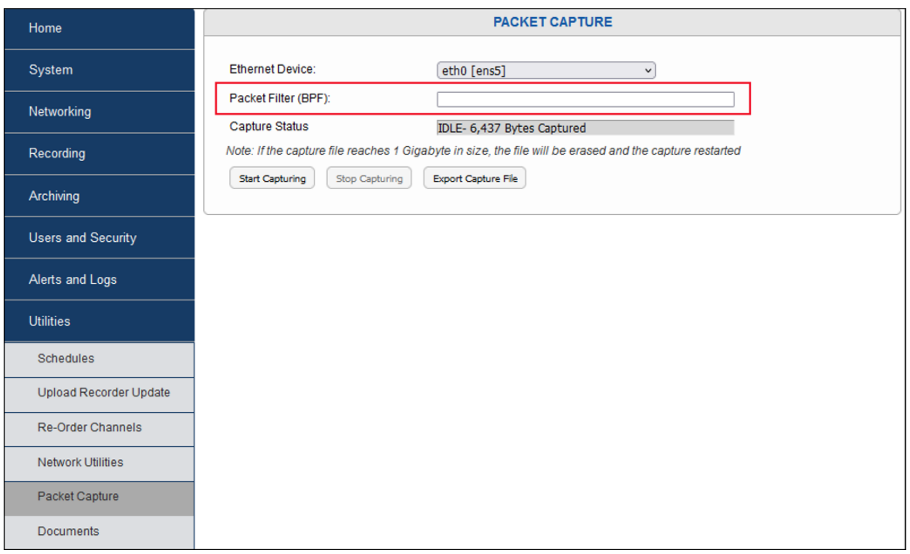


Fig. 12.9 **Entering Commands in the Packet Filter (BPF) Field**

If these steps do not resolve the issue, you may need to contact your IT support for further troubleshooting steps. If required, report any error messages to Eventide Communications.

13. CONTACT INFORMATION

Technical Support

Email: service@eventidecommunications.com
Phone: 1-201-641-1200, (Dial 6, then 2) between the hours of 7:00 A.M. and 7:00 P.M. EST Monday through Friday, except Eventide Communications business holidays.

Sales:

E-Mail: loggers@eventidecommunications.com Phone: 1-201-641-1200