IntelliNet® Network Control Center (INCC)

Installation, Configuration, and Operations Manual

285 Newbury Street

Peabody, Massachusetts 01960 USA
Telephone: 1-978-535-7310
Fax: 978-535-7313

www.aes-corp.com

Document Number: 40-8705 5-8-2024, Version 17.4

Contents

NOTICE TO USERS, INSTALLERS, AUTHORITIES HAVING JURISDICTION, AND OTHER INVOLVED PARTIES

This product incorporates field-programmable software. In order for the product to comply with the requirements in the Standard for Control Units and Accessories for Fire Alarm Systems, UL 864, certain programming features or options must be limited to specific values or not used at all as indicated below.

Program Feature or Option	Permitted in UL 864 (Y/N)	Possible Settings	Settings Permitted in UL 864
Alarm Automation (Heartbeat Signal Frequency: Serial or IP)	Y	0–90	As configured by UL 1981, Central-Station Automation Systems Requirements
Data Type	Y	Security, GPS, USDI (others in pull-down menu)	Security
Old Alarm Delivery Options	Y	All, Subscriber controlled, Never	All
Radio Packet Life	Y	0–99	0 (No Time Out for Alarm, Trouble or Restoral)

Software Version

The instructions in this manual correspond to version 10.00.01 of the INCC software. To verify which version of the software you have, go to Software Receiver Identification.

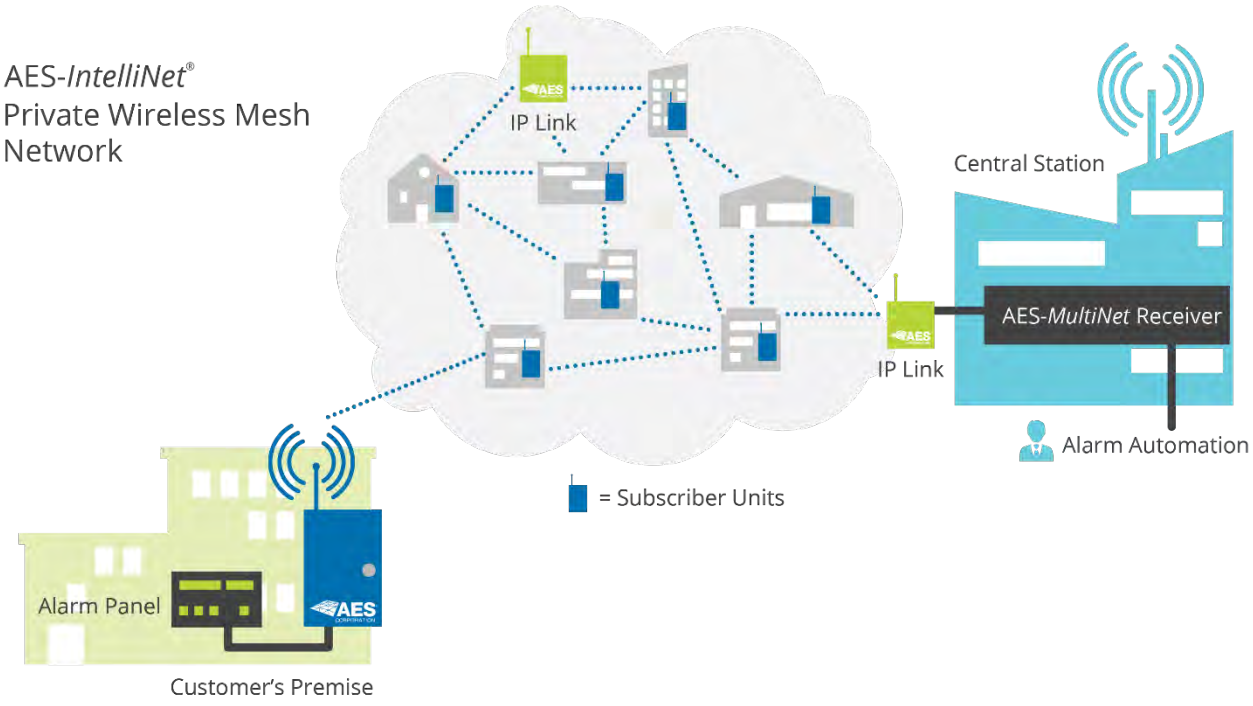
Notes

1. INCC operates with alarm mode and in manual mode.
2. For Alarm Automation references throughout this manual, Alarm Automation output must be connected to a UL 1981 Listed Alarm Automation System. Automation system must have a redundant system.
3. For UL Central Station Burglar Alarm applications, opening/closing signals shall be sent using an alternate communication means that provides for premises acknowledgement (ring back).
4. Alarm Automation is not allowed for proprietary monitoring centers, manual mode only. (According to UL 2610.)
5. This product shall be installed in accordance with NFPA 72, NEC (NFPA 70 National Electric Code), UL 827 and all applicable local codes.

6. For compliance with UL Central Station Fire/ Burglar Alarm applications, a computer workstation is required to be able to determine subscriber status. The workstation shall be UL-listed ITE equipment.

1. Introduction

The AES IntelliNet is a patented two-way data radio network used for monitoring alarms and transmitting specialized data packets. The system is faster and more reliable than telephone and cellular systems, both of which are subject to tampering and general failure. Phone lines may still be used for backup.



The system's unique "smart" radio communicators, called subscriber units, are each connected to an alarm panel or specialized data port. Alarm information or data is transmitted by radio to the central receiver. If a subscriber unit is too far away to reach the central station directly, its message is relayed by another subscriber unit closer to or in better communication with the central station or other closer units. This unique built-in "repeater" capability creates a highly rugged, adaptive security network. The system self-adjusts to ensure that messages are forwarded via the shortest and best available route. This "smart routing" capability is automated, requiring no special programming. Also, the AES system eliminates the need for dedicated repeaters and towers, significantly reducing setup and operating costs.

2. Product Compliance Statements

AES IntelliNet Network Control Center software, version 10.00.xx, meets UL 864 and UL 2610 when used with UL 60950 or UL 62368 listed ITE equipment, meeting the minimum hardware requirements.

California State Fire Marshall Listing Number	Please visit AES Website for latest listing #
City of New York Fire Department Certificate of Acceptance (COA) Number	Please visit AES website for latest certificate #

All AES products are compatible with the INCC receiver, but applications that have been tested to be compliant with UL 864 and UL 2610 are limited to the following:

Model Number	Type
7744F	Fire
7788F	Fire
7706 ULF	Fire
7707	Fire
7007	Burg
7177	Hybrid
7170	IP Link

3. Hardware and Software Requirements

Server

Minimum Hardware Requirements

The minimum hardware requirements for operating the AES software receiver system are as follows:

- 1 TB disk drive storage
- Intel® Xeon® quad core microprocessor with minimum speed of 2.4 GHz, or similar specification x64 Intel® compatible microprocessor
- 8 GB RAM
- USB Type-A or Type-C (USB 2.0/3.0)
- 100 Mb Ethernet connection
- Operating System Ubuntu 20.04,

Ubuntu 22.04, 23.04, 23.10, 24.04

Other requirements that must be considered for the installation:

- Primary and secondary servers are redundant machines.
- All servers must be operating non-stop, including monitors.
- Every workstation requires a keyboard, mouse, monitor, and network connected to the primary/secondary server.
- Do not use a screen saver on any INCC server.

All network switches, routers, hubs, and the like, shall be Listed Information Technology Equipment in accordance with UL 60950 and/or UL 62368.

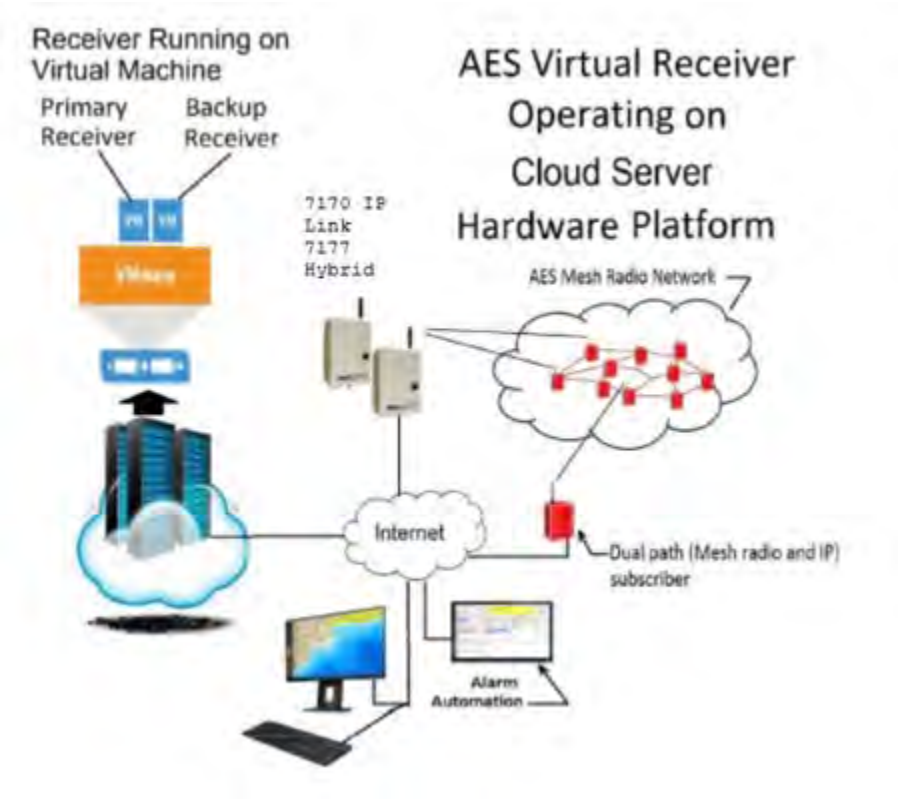
Software Requirements

The customer is responsible for installing Ubuntu on either a server or virtual machine.

Install Ubuntu 20.04 LTS (64 bit), which is available at https://releases.ubuntu.com/20.04/.

Important: No other software other than the operating system software and anti-virus/security protection software shall be installed on the primary and backup computer/servers.

Note: Customers can use a cloud server if it adheres to UL 872A, “Hosted Central Station Services,” as shown below.



Virtual Machine

The hardware requirements for each server installation are as follows:

- 8 GB RAM
- 512 GB Hard Drive
- 4 CPU's per VM
- Intel® Xeon® quad core microprocessor with minimum speed of 2.4 GHz, or similar specification x86 Intel® compatible microprocessor

The software requirements are as follows:

- Ubuntu server 20.04.4 (64 bit), 22.04, 23.04, 23.10, 24.04
- Compatible software alarm automation system for signal processing
- Web-enabled device for browser access to the AES software receiver

Note*:* The INCC does not support Internet Explorer.

Other Hardware Considerations

- Supply line transient protection is required that complies with the Standard for Surge Protective Devices, UL 1449, with a maximum marked rating of 330V. This applies to 120/220 V AC single-phase systems.

- The source of power for the equipment shall be within the rated voltage range of the signal processing equipment.
- Network (Ethernet) cabling requires transient protection complying with the Standard for Protectors for Data Communications and Fire Alarm Circuits, UL 497B, with a maximum marked rating of 50V.
- The communication circuits and network components connected to the telecommunications network must be protected by secondary protectors for communication circuits. These protectors must comply with the Standard for Secondary Protectors for Communications Circuits, UL 497A, with a marked rating of 150V or less. These protectors must be used only on the protected side of the telecommunications network.
- Supervising station processing control equipment or the enclosure housing the control equipment be provided with a permanent means for connection to the branch-circuit supply which shall include provision for installing the supply conductors in conduit.
- Any telecommunication interface lines must be protected by secondary protectors that comply with the Standard for Secondary Protectors for Communications Circuits, UL 497A, with a maximum marked rating of 150V.
- The equipment used must be installed in a temperature-controlled environment that can be maintained between 13–35°C (55–95°F) by the HVAC system. The monitoring station must have an HVAC maintenance contract for the equipment providing the controlled environment.
- Twenty-four hours of standby power must be provided for the HVAC system, which may be supplied by an engine-driven generator alone. A standby battery is not required to be used.
- In addition to the main power supply and secondary power supply (120V AC/240V AC), an uninterruptable power supply (UPS) with sufficient capacity to operate the computer equipment for a minimum of 15 minutes is required. If more than 15 minutes is required for the secondary power supply to supply the UPS input power, the additional UPS required must be capable of providing input power for at least that amount of time.
- The UPS used must comply with the Standard for Uninterruptible Power Systems, UL 1778, or the **Standard for Control Units and Accessories for Fire Alarm Systems**, UL 864.
- To allow for maintenance and repair service, a means for disconnecting the input to the UPS while maintaining continuity of power to the receiving equipment must be provided.
- If a power conditioner is used, the receiving equipment must comply with the applicable requirements in the Standard for Power Units Other Than Class 2, UL 1012.

- To allow for maintenance and repair service, a means for disconnecting the input to a power conditioner and output from a power conditioner while maintaining continuity of power to the automation system shall be provided.

4. INCC Software Installation

The following instructions describe how to install a new AES central station system. Upgrades and replacements are not covered in this document.

Important: AES customers are provided with a Linux installation package file **only** and are required to build and prepare a virtual machine prior to the installation.

Note: Please pay attention to partition allocation when installing the operating system. All space required to root a partition must be allocated. You will modify this allocation when checking the LVM group.

When changing the IP address for the INCC, please verify that the IP addresses are not currently being used inside your network scope.

Prerequisites

Software Distribution Media

: The INCC software is available from AES as a web download or USB.

Note: Estimated completion time to install a new AES central station system is approximately 20–30 minutes, depending on the Internet service provider (ISP).

Before installing the INCC software, complete the following steps so that the virtual machine can access the VNET PC transfer application:

1. Ensure that the software and hardware for the virtual machine meets the minimum requirements specified in Section 3, Hardware and Software Requirements.

Model Number	Type
7744F	Fire
7788F	Fire
7706 ULF	Fire
7707	Fire
7007	Burg
7177	Hybrid
7170	IP Link

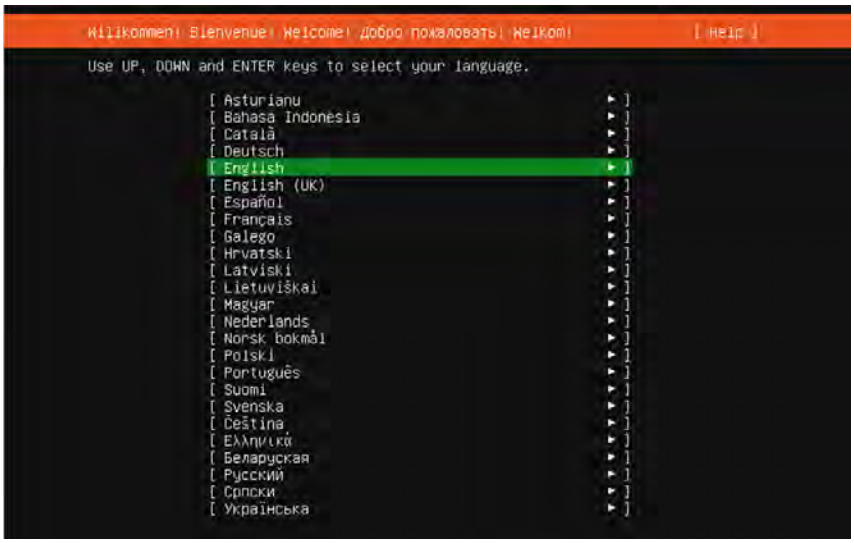
2. Configure static IP addresses for both the primary and secondary servers, then run both servers (https://en.wikipedia.org/wiki/Private_network).

3. Network connectivity between VMs must be configured.

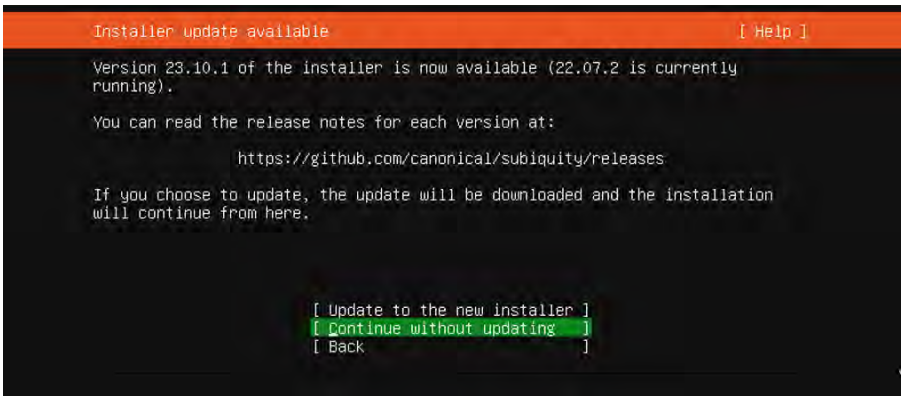
5. INCC Software Installation

Installing Ubuntu Operation System

1. Please select a language of your choice:

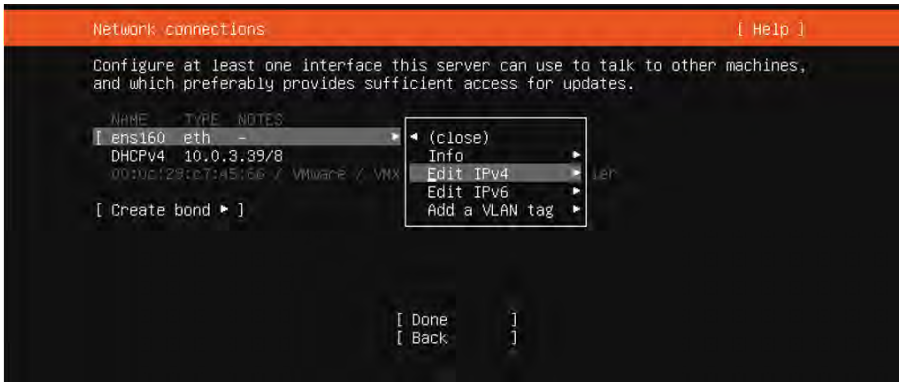


It is recommended that you continue without updating:

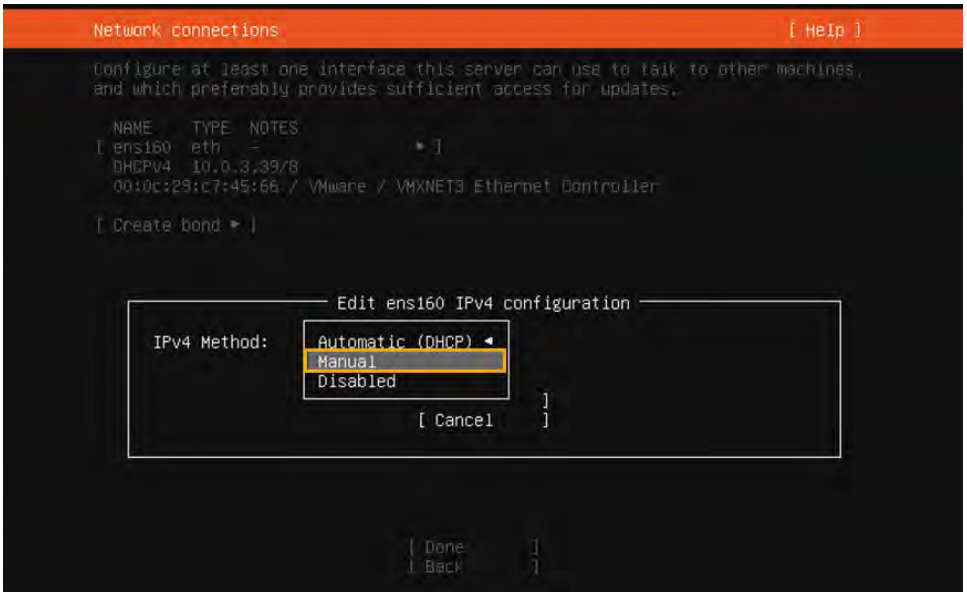


2. Select a keyboard language from the **Layout** and **Variant** dropdown lists:

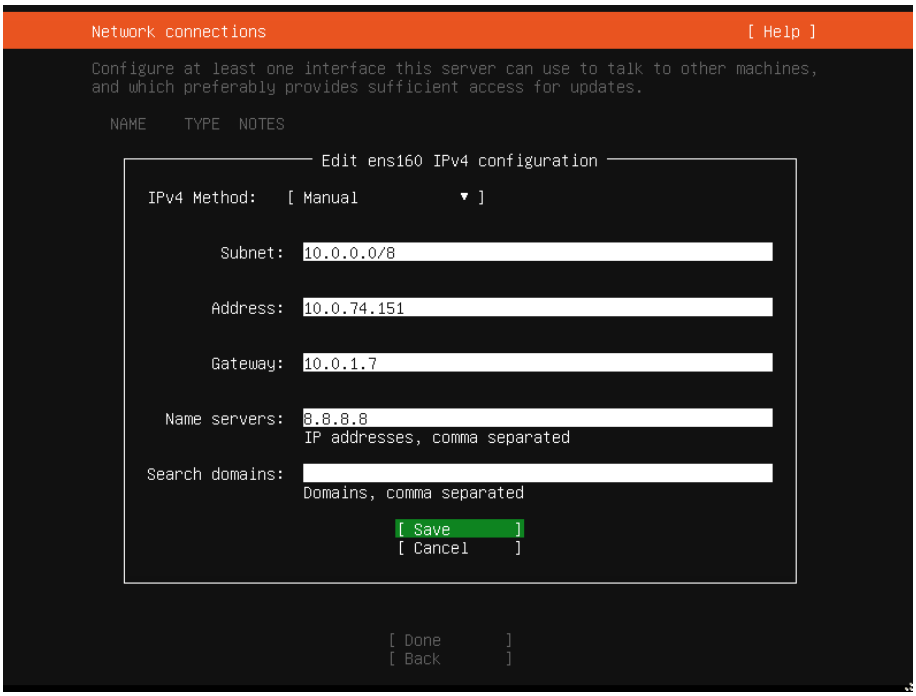
3. Configure at least one interface the server can use to communicate with other machines. Start by clicking **eth** > **Edit IPv4**.



4. Define the IP address by selecting **Manual**:



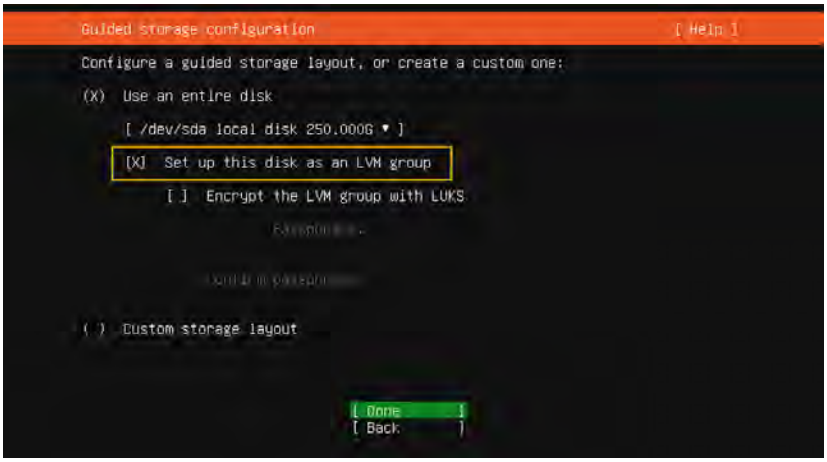
5. Add your static network values into the form, then click **Save** and **Done**:



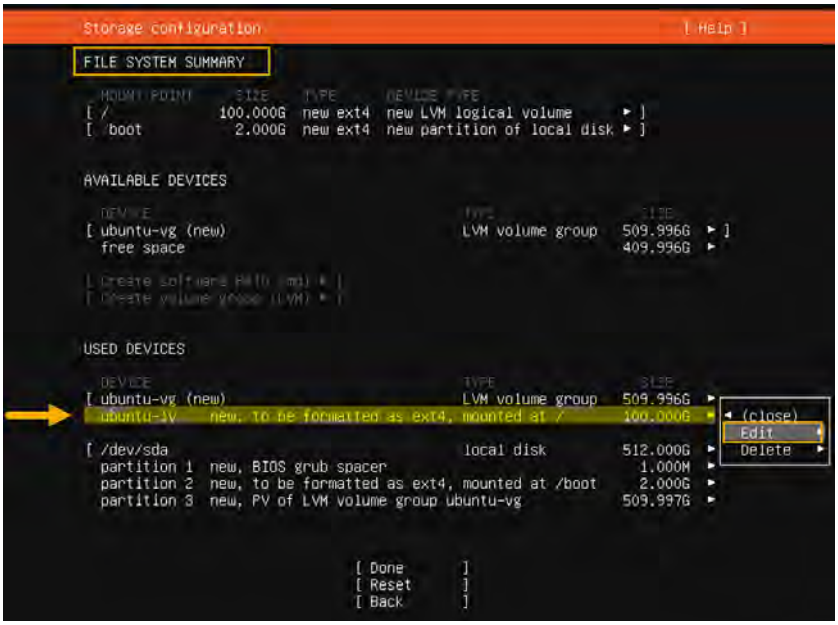
6. Keep the default proxy settings, then click **Done**:

7. Keep the default mirror values, then click **Done**:

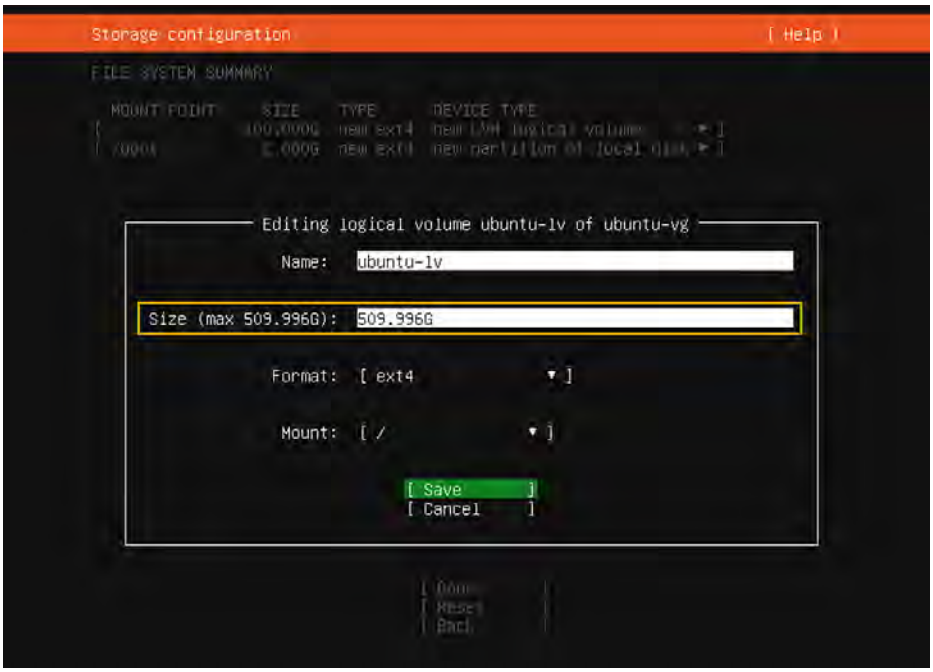
8. In the Guided Storage section, set up the disk as an LMV group. Keep all other settings in default mode.



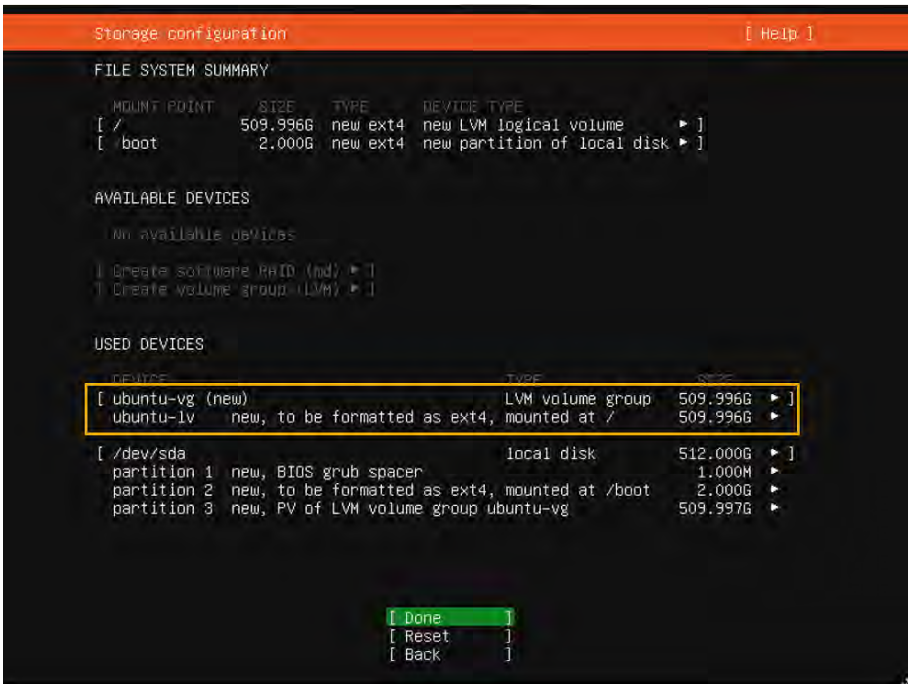
9. In the FILE SYSTEM SUMMARY section, you will need to define a maximum volume for the server. Begin by selecting **ubuntu-lv** under USED DEVICES, then click **Edit**.



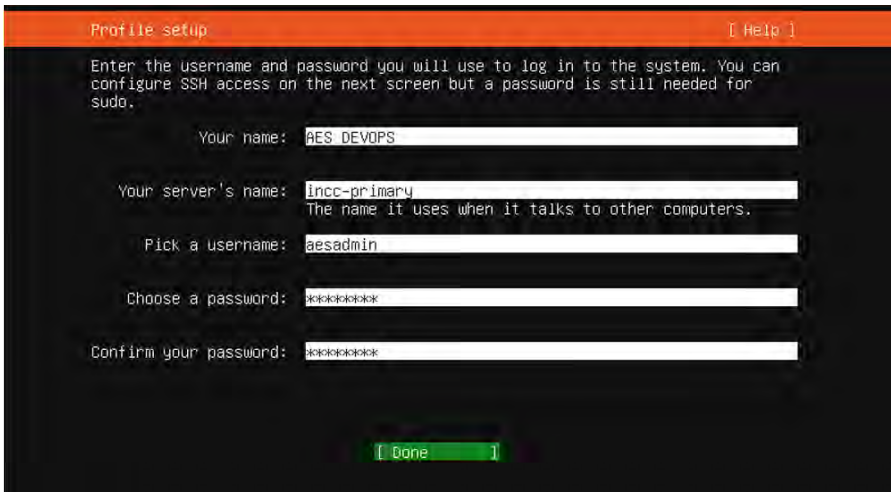
10. In the **Size** field, enter the maximum size, then click **Save**:



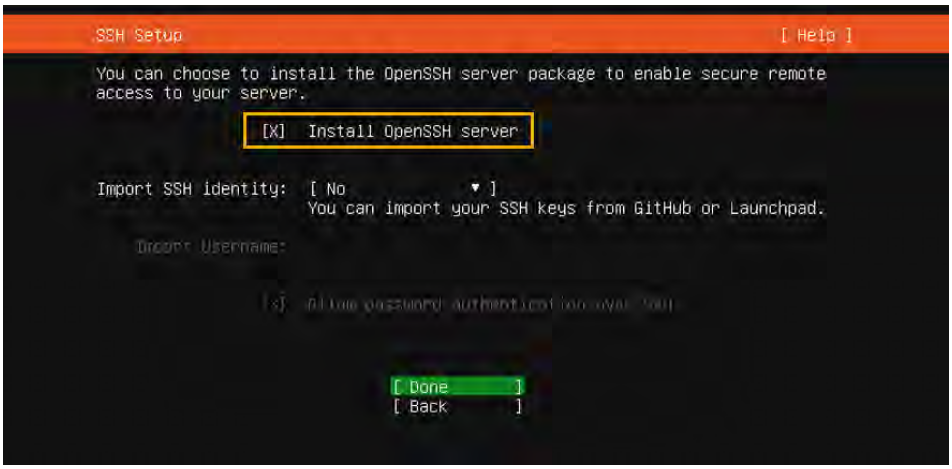
11. Confirm the storage space and click **Done**. Then approve the format and click **Continue**.



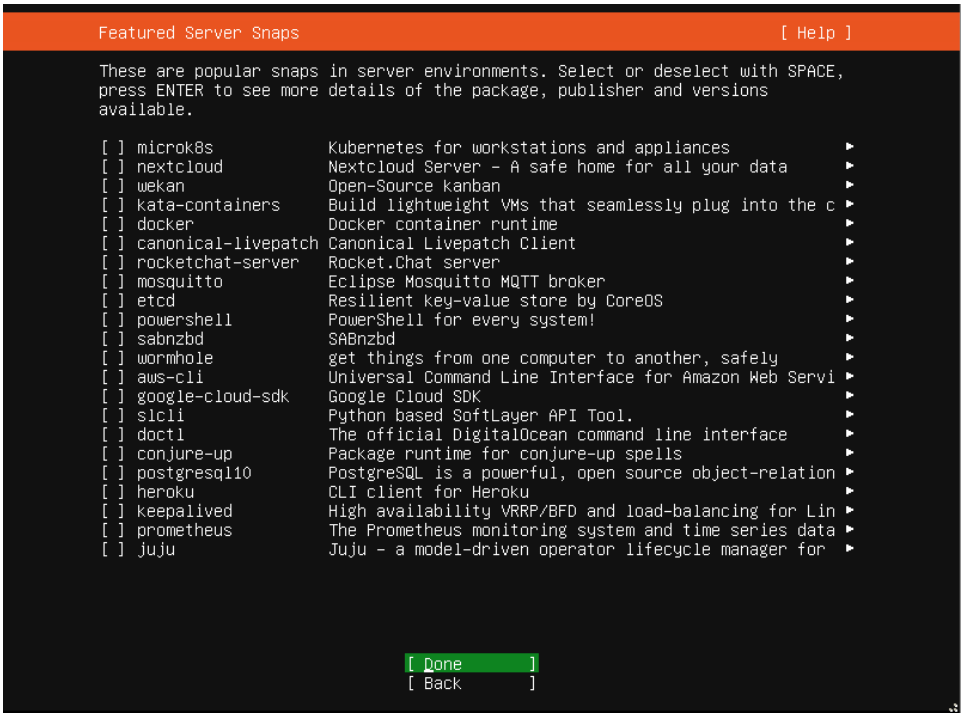
12. On the Profile page, enter your VM profile information:



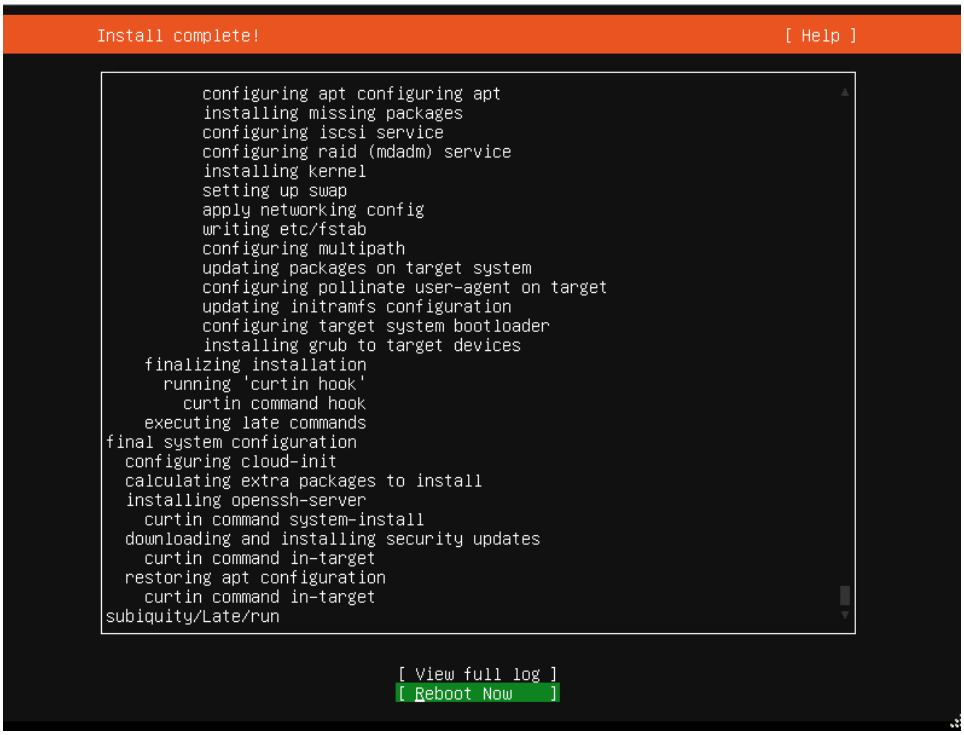
13. On the SSH Setup page, check **Install OpenSSH server** and click **Done**:



14. Click **Done** *without* making any selections (the INCC does not have any additional packages).



15. Once the installation and update are finished for the Ubuntu Operating System, the **Reboot Now** button will appear. When ready, click **Reboot Now**.



Installing the Package Files

Requirements for installing the INCC software are as follows:

- PuTTY or other third-party SSH client
- WinSCP or other file transfer client
- Install package file (File will be provided by AES in **`incc-instal-xx.xx.xx.xxxx-vxx.run`** format.)
- Sudo user in Ubuntu — The sudo user should be created while the operating system is installed, or you can create a new sudo user with the following command (you must replace the bold text — **`aesadmin`** — with your new user):

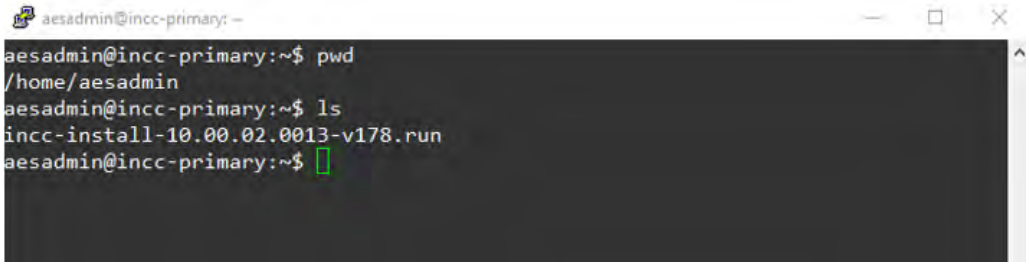
  USERNAME=**aesadmin** && sudo useradd -m -d /home/${USERNAME} ${USERNAME} && sudo usermod -aG sudo ${USERNAME} && sudo usermod -s /bin/bash ${USERNAME} && sudo passwd ${USERNAME}

Note: The INCC installation requires that the primary instance be installed first. Once the primary instance has been successfully installed, the secondary instance can be installed. Currently, the INCC supports only two instances—primary and secondary.

1. Before starting the installation, update and upgrade Ubuntu using the following commands on all Ubuntu operating systems:

   sudo apt-get update && sudo apt-get upgrade –y

2. Transfer the install package file with WinSCP (or other tools) to the home folder of sudo users for all instances (if you created **`aesadmin`** user, the folder will be /home/aesadmin).

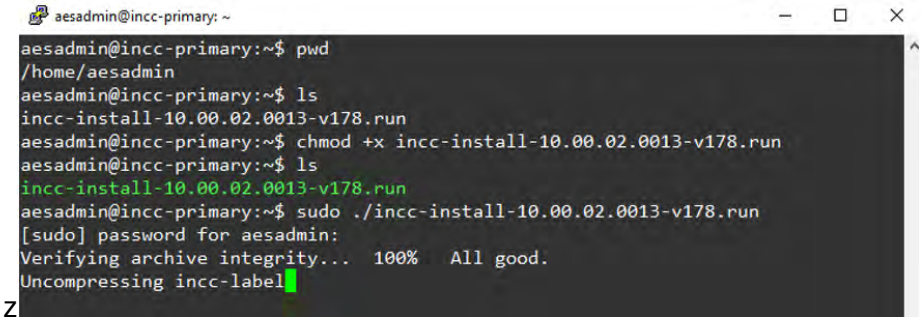


3. Make the install package file executable using the following command:

   sudo chmod +x instal-xx.xx.xx.xxxx-vxx.run

4. Install the primary instance using the following command:

   sudo ./ instal-xx.xx.xx.xxxx-vxx.run



Z

While installing the primary instance, you will be asked the following questions:

- Do you accept AES Corp Software License Agreement? (yes/no):

  Type **yes** and press the **Enter** key.

- Is this VM primary? (yes/no):

  Type **yes** and press the **Enter** key.

- Is this VM replacement with old one? (yes/no): (syntax needs to be adjusted)

  If you installed the INCC primary first, type **no**.

  If your INCC primary instance corrupted and you want to replace it with a new one, type **yes** and press the **Enter** key.

- Do you want to define port ranges for IP Links, IP Subscribers and AA manually? (yes/no):

  Default ports have been set for IP Links, IP Subscribers, and AA. If you wish to go with default ports, you can type **no**; otherwise, type **yes** to define it manually.

  IP Link default port: **7070**

  IP Link default port ranges: **7000-7099**

  IP Subscriber default port: **9090**

  IP Subscriber default port ranges: **9000-9099**

  AA default port ranges: **6050-6099**

```
aesadmin@incc-primary:~$ sudo ./incc-install-10.00.02.0013-v178.run
Verifying archive integrity...  100%   All good.
Uncompressing incc-label  100%
==> Do you accept AES Corp Software License Agreement?(yes/no): yes
==> Is this VM primary?(yes/no): yes
==> Is this VM replacement with old one?(yes/no): no
==> Primary IP address detected: 10.0.74.151
==> Do you want to define port ranges for IP Links, IP Subscribers and AA manual
ly?(yes/no): yes
==> Please provide IP Links default port number (default: 7070): 7070
==> Please provide IP Subscriber default port number (default: 9090): 9090
==> Please provide AA port range (default: 6050-6099): 6050-6099
```

Note: Keep in mind that your firewall should allow ports 80, 443, and the ports that you defined above for IP Links, IP subscribers, and AA.

- Please provide Secondary VMs sudo user:

  Enter **sudo user** that you created on secondary instance.

- Please provide Secondary VM IP:

  Enter the **IP address** of the secondary instance. Press the **Enter** key and accept the SSH connection, then enter the secondary instance sudo user's password.

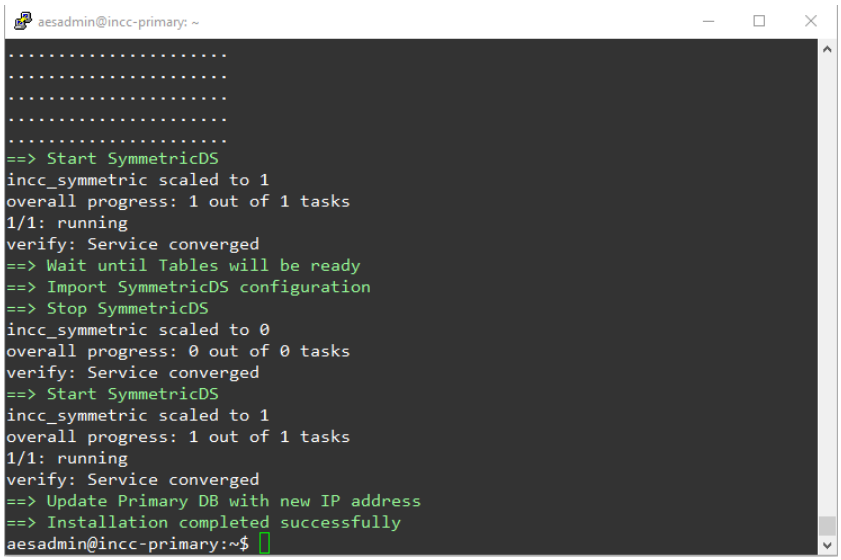
```
==> Creating SSH connection with secondary....
==> Please provide Secondary VM's sudo user: aesadmin
==> Secondary VM's sudo user: aesadmin
==> Please provide Secondary VM IP: 10.0.74.152
==> Generating SSH keys....
==> Please confirm the SSH keys validation and enter secondary VM's password bel
ow:
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa
.pub"
The authenticity of host '10.0.74.152 (10.0.74.152)' can't be established.
ECDSA key fingerprint is SHA256:necun7E4dsW93w++yLDCtLVVrjfaXgXzfLu1g/NPek4.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
aesadmin@10.0.74.152's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'aesadmin@10.0.74.152'"
and check to make sure that only the key(s) you wanted were added.

==> Configuring visudo on the secondary VM...
==> Please enter secondary VM's password below:.
[sudo] password for aesadmin:
aesadmin ALL=(ALL) NOPASSWD: ALL
```

Wait until you see the success message, as shown below:



Note: Installing package files may take time, depending on the speed of your host (VM) resources.

You are now ready to install the secondary instance. (Before running the install package file, you need to update and upgrade the Ubuntu operating system, as you did for the primary instance.) While installing the secondary instance, you will be asked the following questions:

- Do you accept AES Corp Software License Agreement? (yes/no):

  Type **yes** and press the **Enter** key.

- Is this VM primary? (yes/no):

  Type **no** and press the **Enter** key.

- Is this VM replacement with old one? (yes/no):

  If you installed the INCC secondary first, type **no** and press the **Enter** key.

  If your INCC secondary instance corrupted and you want to replace it with a new one, type **yes** and press the **Enter** key.

- Please provide VM sequence number [2,3..8]:

  Since the INCC supports only two instance at this time, type **2**

- Please provide a Primary VM IP:

  Provide the primary instance's IP address and press the **Enter** key.

- Do you want to define port ranges for IP Links, IP Subscribers and AA manually? (yes/no):

  We have set default ports for IP Links, IP Subscribers, and AA. If you wish to go with default ports, type **no**; otherwise, type **yes** to define it manually.

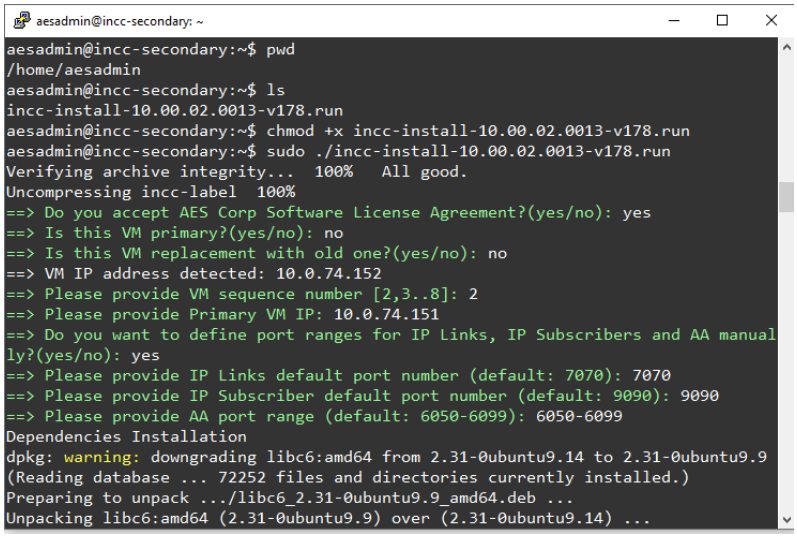
  IP Link default port: **7070**

  IP Link default port ranges: **7000-7099**

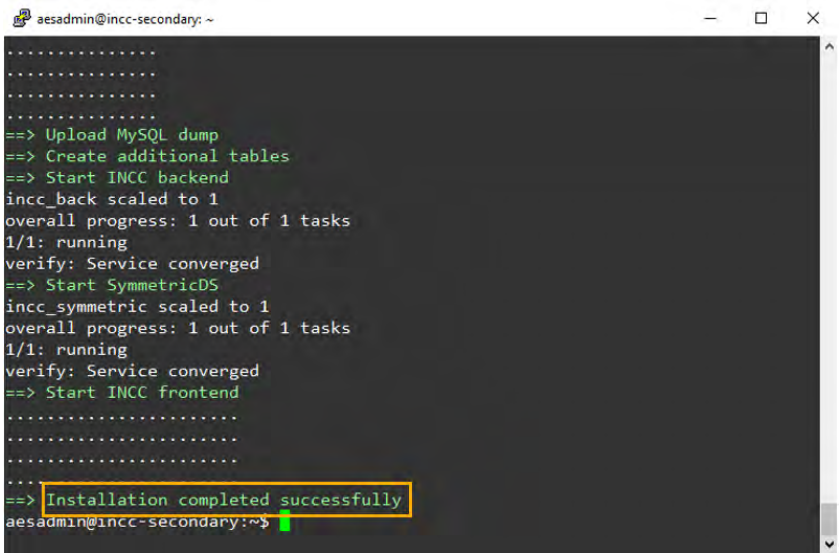
  IP Subscriber default port: **9090**

  IP Subscriber default port ranges: **9000-9099**

  AA default port ranges: **6050-6099**



Once the success message is displayed, as shown below, the installation is complete.



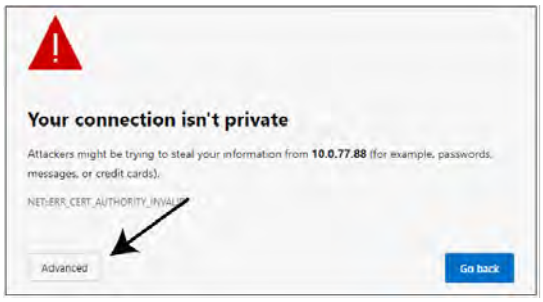
Logging in to the INCC Web Interface

Once the installation is complete, you can access the receiver's INCC web interface using HTTPS.

1. Enter the IP address of the primary server into a web browser.

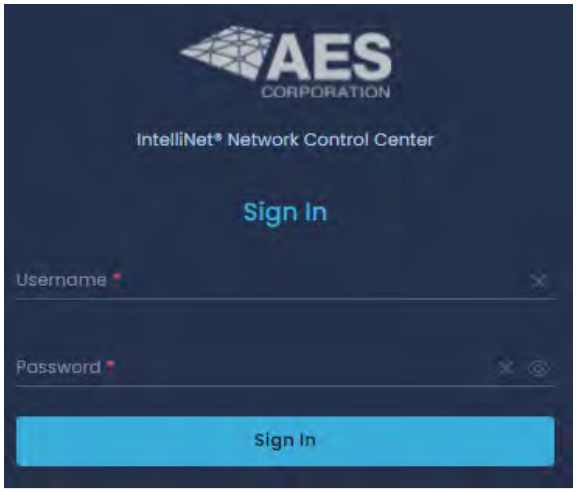
   Example: https://10.0.77.220

7. Click **Advanced**, then proceed to the IP address.



8. Enter the default credentials:

   - Username: Admin
   - Password: peabody



Upgrade/Rollback Procedure

Requirements for upgrading (rollback) the INCC software are as follows:

- PuTTY or other third-party SSH client
- WinSCP or other file transfer client
- Upgrade (rollback) package file (the file will be provided by AES in incc-upgrade-xx.xx.xx.xxxx-vxx.run format)

Note: Upgrade (rollback) package file must be run *only* from the primary instance, and it will upgrade (rollback) all instances.

Before starting the upgrade, go to the **sudo user's home folder** that was used during the INCC software installation. Create a new directory inside it (creating a directory name with the current date is recommended) using the following command:

mkdir 01.01.2023

Transfer the upgrade package file with WinSCP (or other tools) to the new folder of the primary instance's sudo user that was created (e.g., the folder will be home/aesadmin/01.01.2023 if you created a "01.01.2023" folder and you have a sudo user named **`aesadmin`**).

Navigate to the new folder:

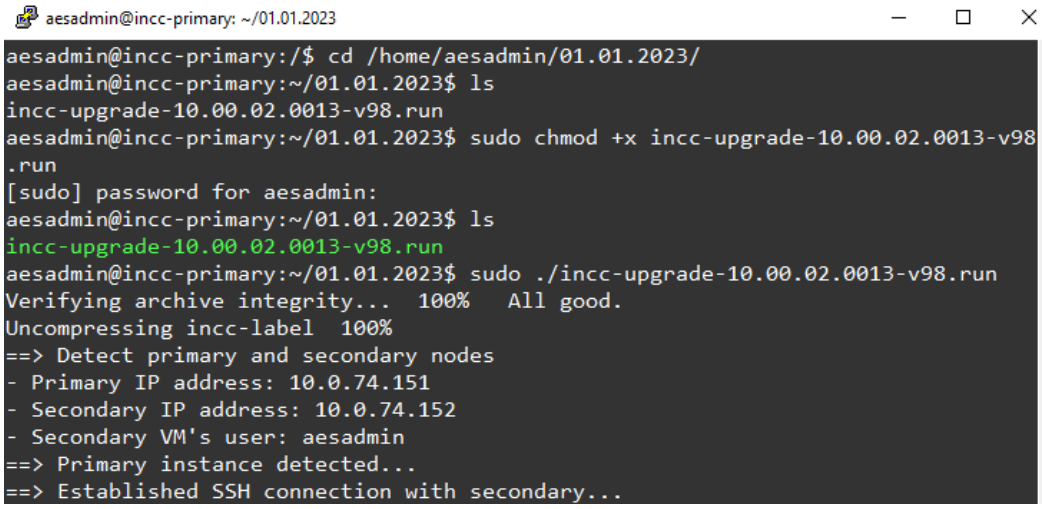
cd /home/aesadmin/01.01.2023

Make the upgrade package file executable using the following command:

sudo chmod +x **upgrade-xx.xx.xx.xxxx-vxx.run**

You are now ready to upgrade instances:

sudo ./ **upgrade-xx.xx.xx.xxxx-vxx.run**



After running the upgrade package file, you will be asked to perform several actions on the console to proceed:

- Please type **`start`** to start upgrade/rollback process:

  You must type **`start`** to start the process.

- Do you want to roll back? (yes/no):

For doing the upgrade, you must type **no** here. If you finish the upgrade process and see that the software doesn't work as expected, you will need to run the upgrade package file again and type **yes** in this section. It will roll back both instances.

- AA state is down on primary. Do you want to continue? (yes/no):

  You will be asked to confirm if AA is down.

- UnAcknowledged Events are present on primary. Do you want to continue? (yes/no):

  You will be asked to confirm if UnAcknowledged Events are present on primary

- AA state is down on secondary. Do you want to continue? (yes/no):

  You will be asked to confirm if AA is down

- UnAcknowledged Events are present on secondary. Do you want to continue? (yes/no):

  You will be asked to confirm if UnAcknowledged Events are present on secondary

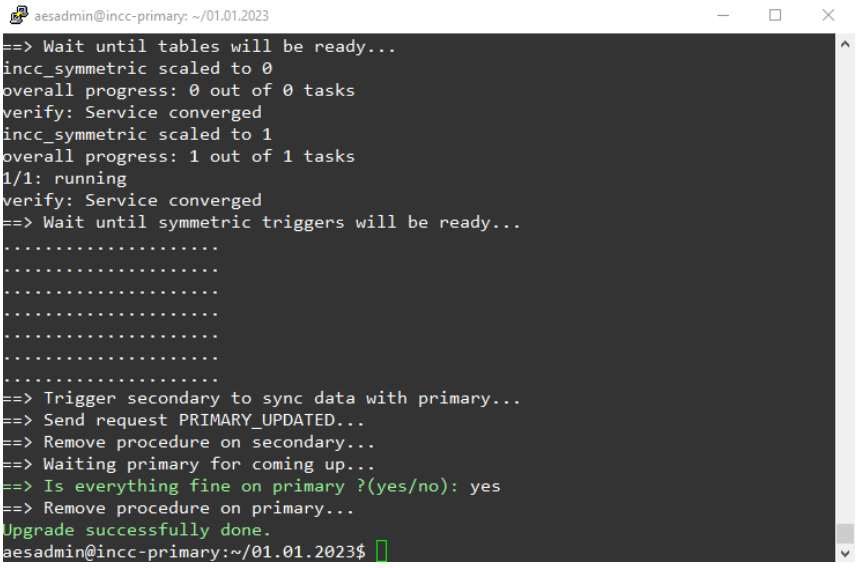
- Is everything fine on secondary? (yes/no):

  The upgrade package will upgrade secondary first and when upgrade on secondary completed, you will be asked to check the secondary instance and confirm the health. If you type **yes** here, it will continue the upgrade. If you type **no**, it will start the rollback process for the secondary instance

- Is everything fine on primary? ((yes/no):

The upgrade package will upgrade the primary after you confirm that everything is fine with secondary, and when the upgrade on the primary is completed, you will be asked to check the primary instance and confirm the health. If you type **yes** here, it will complete the upgrade process. If you type **no**, it will start the rollback process for all instances.

After you confirm that everything is fine with the primary, the upgrade process is finished:



Note: For keeping the INCC software up and running, the upgrade (rollback) package will upgrade the secondary instance first, then it will upgrade the primary. If you see any issues after the upgrade, you can run the package file again and go with the **rollback** step.

Troubleshooting

If you see any issue while doing installing INCC software, you can navigate to the install package file location and run the following script:

sudo ./clean.sh

This script will clear the corrupted install, and you may run the install package file to start the install process again.

Run this “clean.sh” file twice if you see any error.

While transferring package files through WinSCP (or other third-party tools), you may see some errors like “permission denied”. This means that you have lost the permission to the user’s home folder. To fix this issue, navigate to the home folder and correct the permissions:

cd /home

sudo chown –R aesadmin aesadmin/

The INCC software primary and other instances will communicate with each other with specific ports, so keep in mind that the following ports must be allowed between the instances from the firewall:

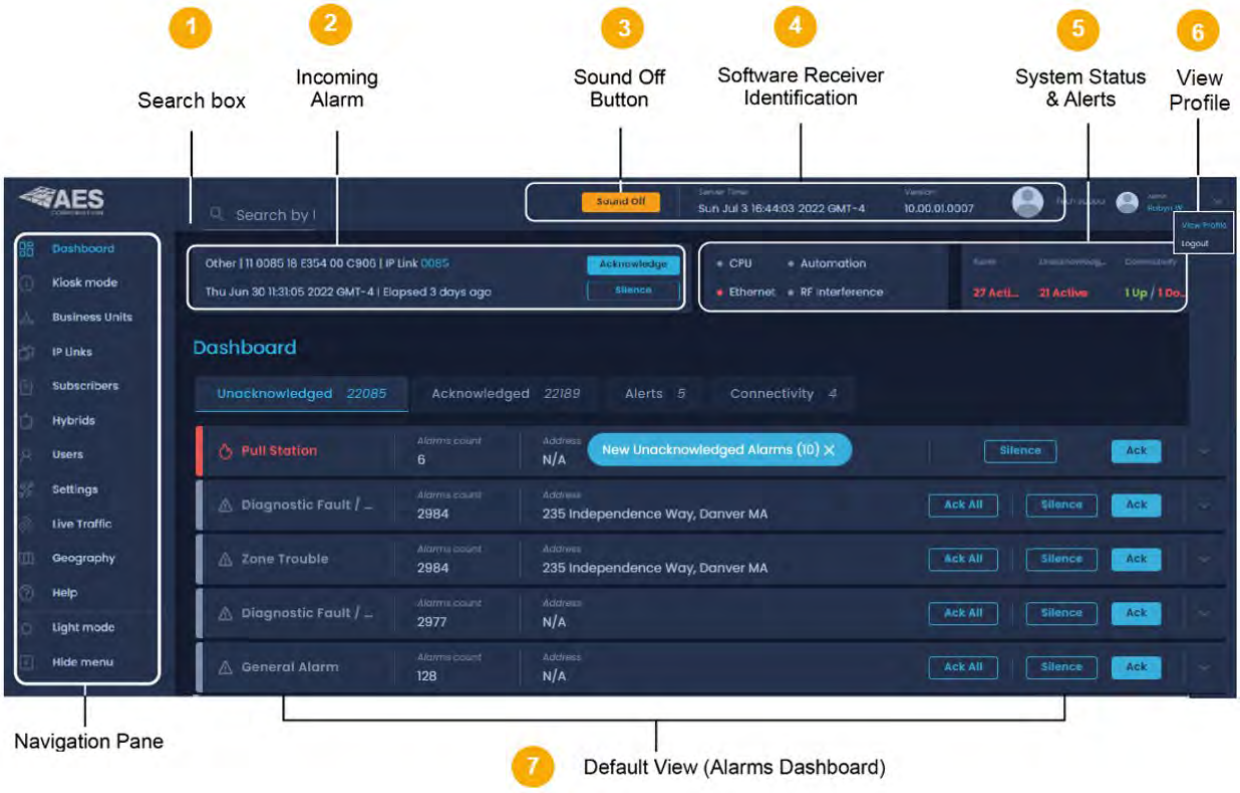
- 22 (SSH)
- 3306 (MySQL)
- 31415 (SymmetricDS)

Note: AES recommends the use of a firewall and that only the necessary ports be allowed.

6. Exploring the IntelliNet Control Center

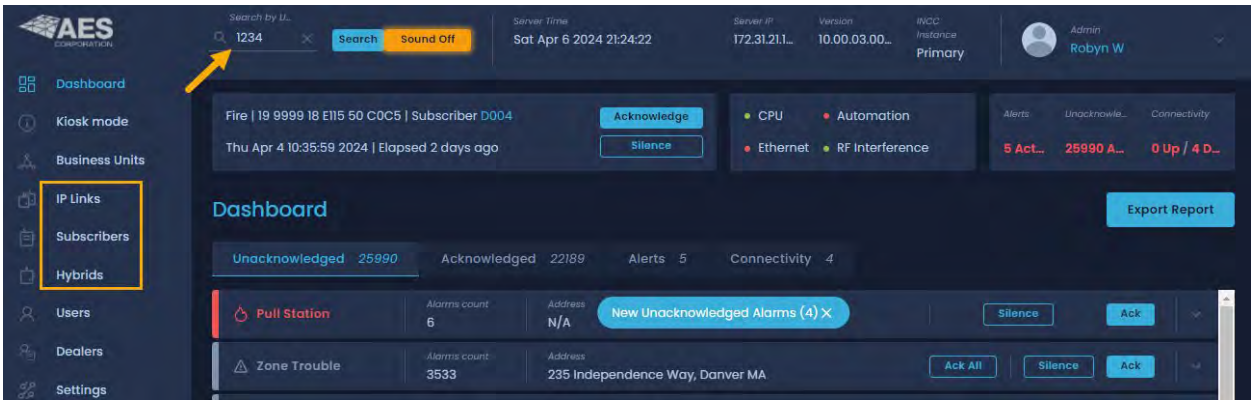
Overview

The Control Center dashboard is used for configuring the IntelliNet system, viewing information about the system, viewing your profile, and processing alarms. Detailed information about each component of the dashboard is described on the following pages.



Search by Unit

The search box at the top left can be used to search for IP links, subscribers, and hybrids across the system.



Incoming Alarm

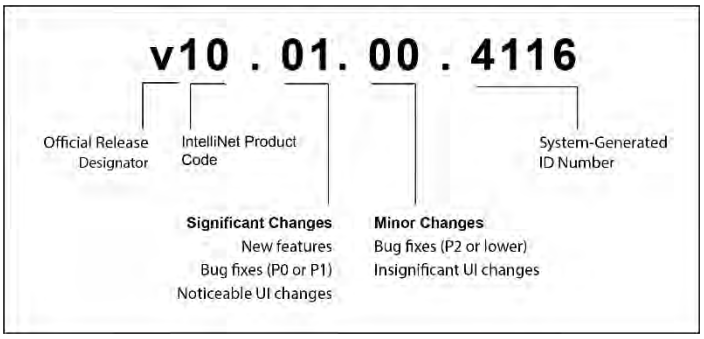
This panel provides detailed information about the most recent alarm, including the alarm type, the alarm ID code, and the subscriber associated with the alarm. The date and time zone of the subscriber, as well as how much time has elapsed, are also displayed. The **Acknowledge** and **Silence** buttons are used for processing incoming alarms manually.

Sound Off Button

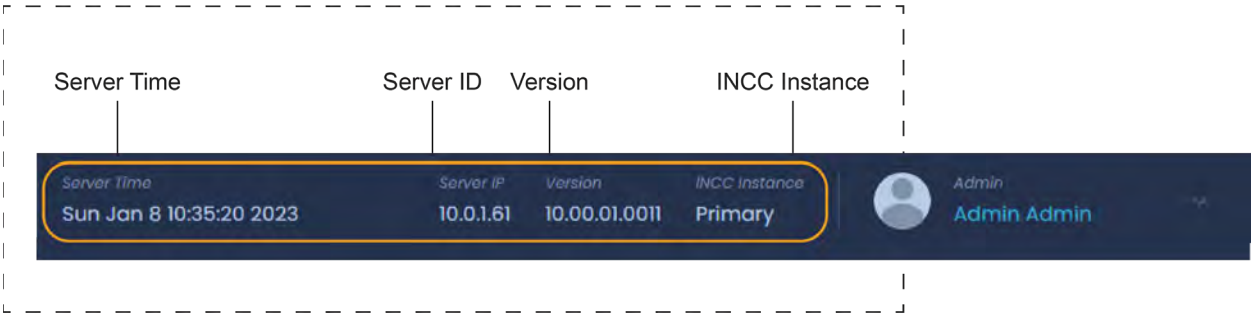
The **Sound Off** button is a visual indicator of the **System sound in OFF** (or ON) setting in the system settings. Refer to the description in the System Tab.

Software Receiver Identification

The Software Receiver Identification banner provides information about the software and the server.



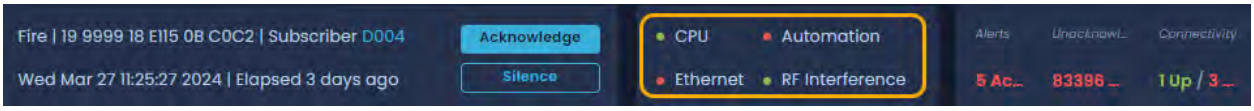
- Server Time: The current time and time zone of the location of the servers. (The server can be manually adjusted using the **Settings** option in the left navigation bar.)
- Server IP: The IP address for the primary instance of the server.
- Version: The current version of the software; see the Version Control Schema on page 119 for a detailed explanation on the versioning control syntax for the INCC software.
- INCC Instance: This field reflects the software receiver that is currently supporting the system. (If the primary receiver goes down, the secondary receiver automatically takes over.)



System Status & Alerts

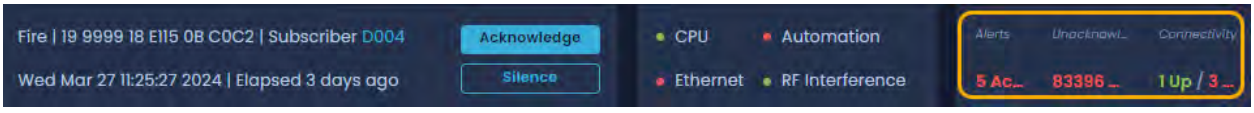
The four LED lights in the System Status & Alerts panel convey information about the status of the system. The alert indicators at the right of this panel provide information about alarm activity and connectivity issues.

Note: Status LEDs that turn red indicate a failure. Once the failure has been corrected, the LED returns to its normal state (green).



LED	Issues That Trigger Red	Result
CPU	Server issues (e.g., buffering issues, catastrophic failure with the server)	The INCC stops processing signals.
Ethernet	Missing check-in from a 7170 IP-Link	No connection between the INCC to the Model 7170 IP Link; the INCC will not receive subscriber signals. The time next to each issue indicates how long it will be before the LED is triggered. • Default IP Link: 60 seconds • Default IP Subscriber: 180 seconds • Default AA: 30 seconds
Automation	Unable to get Acknowledgements from a designated alarm monitoring system	Alarms must be processed in manual mode due to alarm automation not processing.
RF Interference	An RF interference condition exists	Signals may not be received.

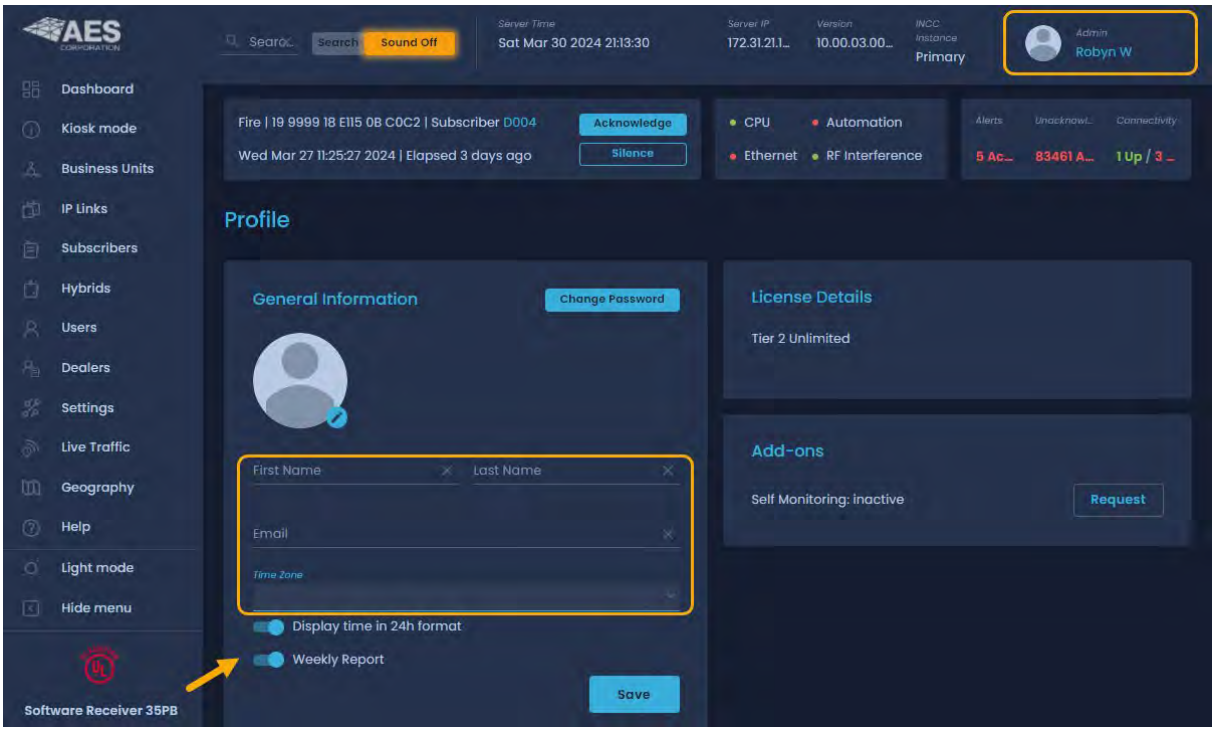
Alerts



- *Alerts* are incoming signals that require immediate attention.
- *Unacknowledged* refers to alerts that have not been acknowledged.
- *Connectivity* refers to IP Links that are not connected.

View Profile

Weekly reports can be enabled from within the profile page (click the top right corner at any time from within the INCC).



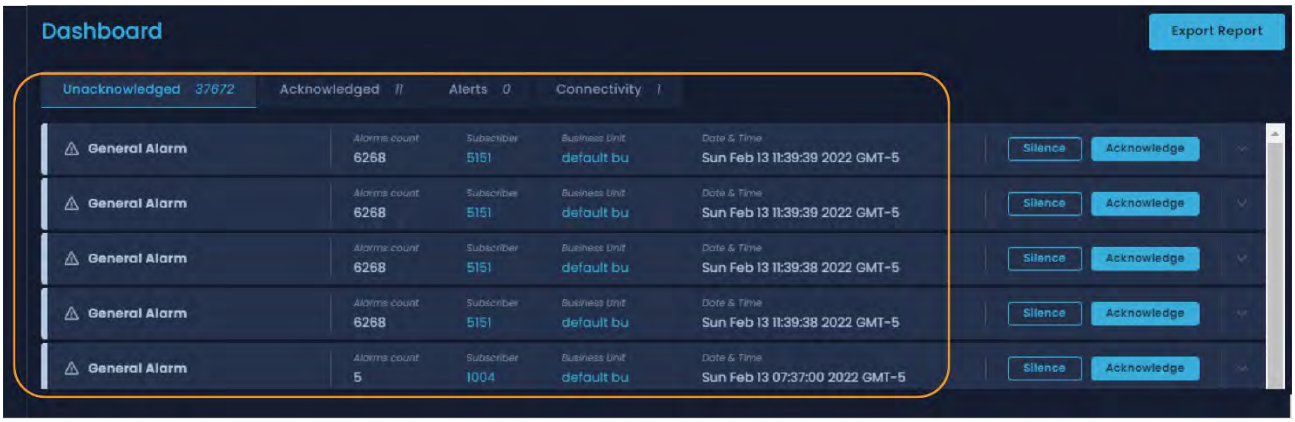
Provide the recipient's name and email address. The report will be sent as a CSV file to the provided email address.

Alarms Dashboard

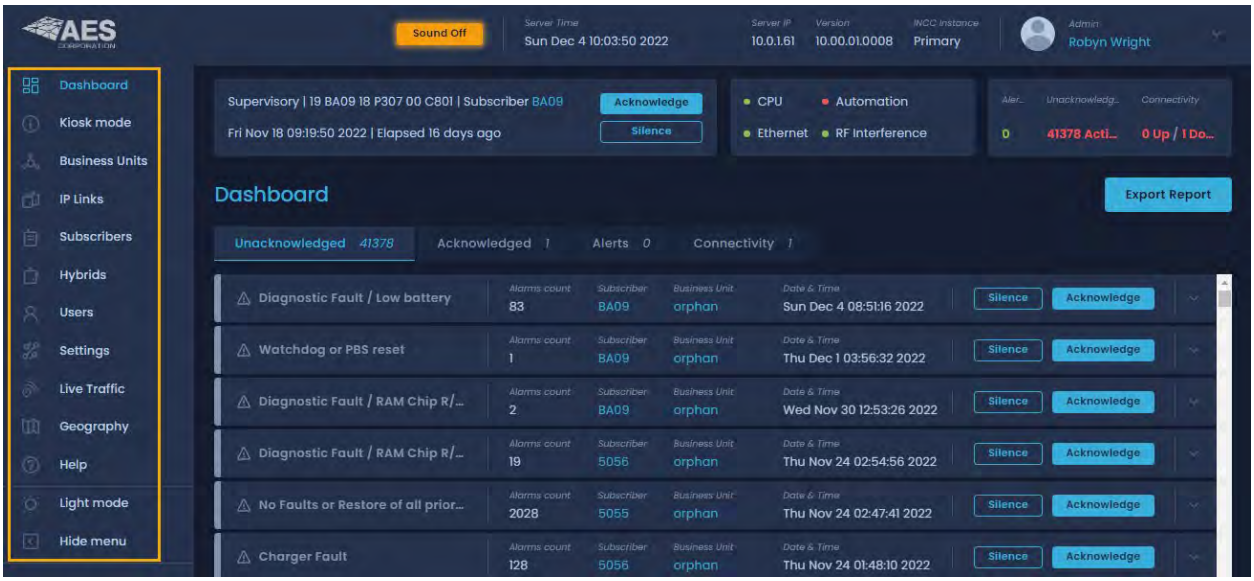
The Alarms Dashboard is the default view of the INCC Control Center dashboard (see image below).

Alarms that haven't been processed due to a failure in alarm automation are displayed in the Alarms Dashboard. These alarms will remain active until they are acknowledged. Once alarm automation restarts, alarms will automatically be moved and cleared from the system and will be visible from the Acknowledged tab. See Processing Alarms for more information on processing alarms.

Note: No alarms will be present on the Alarms Dashboard if alarm automation is active.



7. INCC Navigation Pane



Dashboard

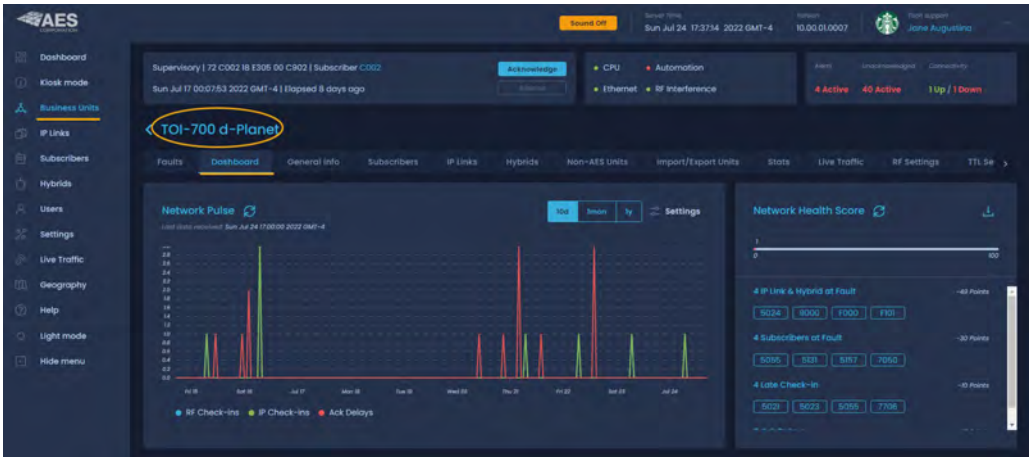
The Alarms Dashboard is the default view of the INCC Control Center dashboard (the alarms dashboard is described on page 39).

Kiosk mode

The information included on the kiosk is pulled from other areas of the INCC interface.

- The first three screens (Current alert, Recent alarm, and LED panel) are pulled from the top of the screen (the header).
- The Network Pulse and Network Health Score (yellow boxes below) are pulled from the business unit selected from the Business Unit Name dropdown.
  - The Network Health Score is a quick indicator of network performance. The score is calculated based on the number of Ack Delays, IP Link and subscriber faults, and the number of late check-in messages.
  - The Health Score range is a number from 1–100. A higher score suggests a healthy network, and a lower score suggests that improvements can be made to the network.

To view the network pulse and network health score for a business unit, navigate to Business Unit, select the business unit, then select the Dashboard tab.



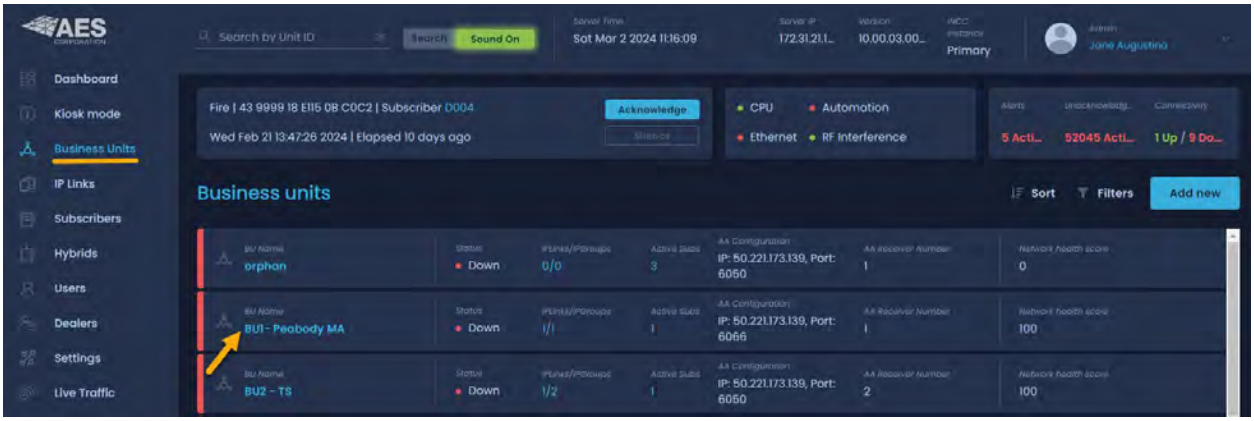
Business Units

Introduction

Business units are a collection of common subscribers grouped together for the purpose of controlling them via a specific cipher code access. Dealers and other people using the business unit can control the system and manage it through this interface.

Due to site-specific particulars, you will need to create at least one business unit to continue. The Multi-Net receiver does not come with business units from the factory.

Note: To view the details of a business that has already been created, click the business unit name. See Business Units for detailed information.



Note: Some systems have only one type of application data and one access point, and thus require only one business unit. If you have multiple types of data and need multiple remote access locations, define a business unit for each data type and/or remote user. For example, if you have subscriber units that send GPS data and subscriber units that send alarm data, define two business units.

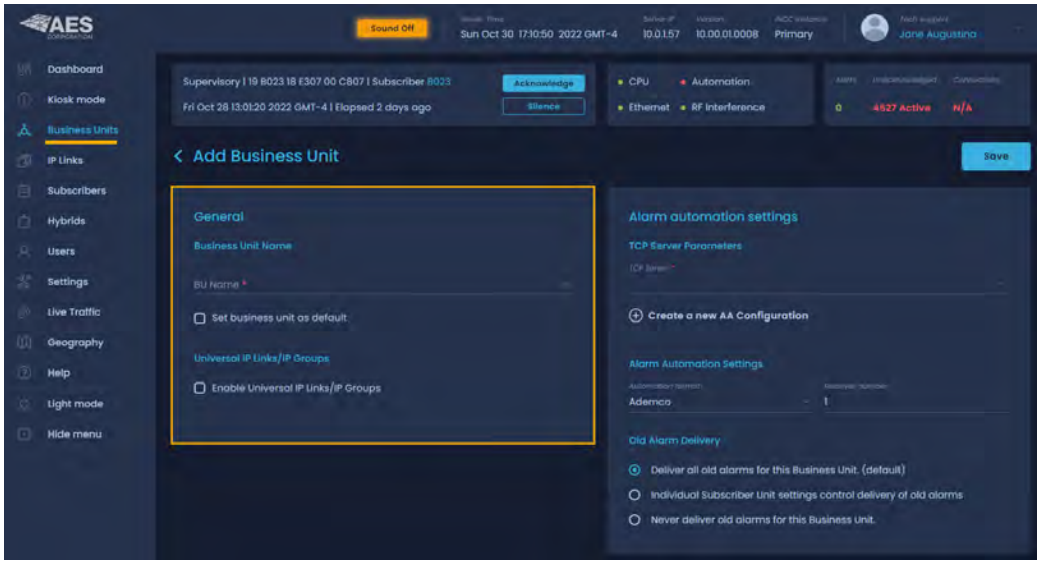
Note: Business units can also be used to separate elements of your operation. If you have networks that are independent, you may find it helpful to create separate business units for them.

Create a Business Unit

1. Click **Business Units** from the left navigation pane and select **Add new**.

2. Populate the General settings:

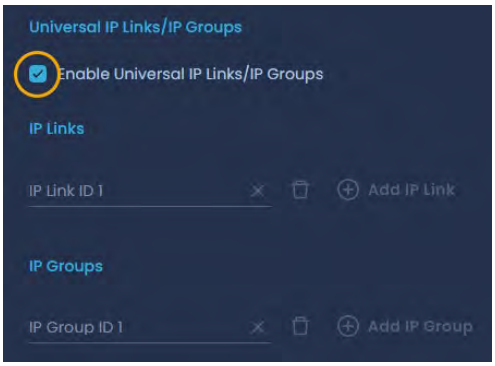
   - **Business Unit Name**: Create an alphanumeric string that you will use to refer to the business unit. The string must be less than 32 characters and can include spaces as well as characters that are considered invalid in Linux directory names (the string is casein sensitive).



   - **Enable Universal IP Links/IP Groups** (checkbox): Check this option if you have only one business unit and want all subscribers to be associated with this business unit (even if you do not manually add them to a subscriber database).

– If the checkbox is *not* checked, you will need to manually add each new subscriber to a subscriber database assigned to a business unit. Any signals received from a subscriber not in a database will force it to be handled by the pre-configured business unit named “orphan.”

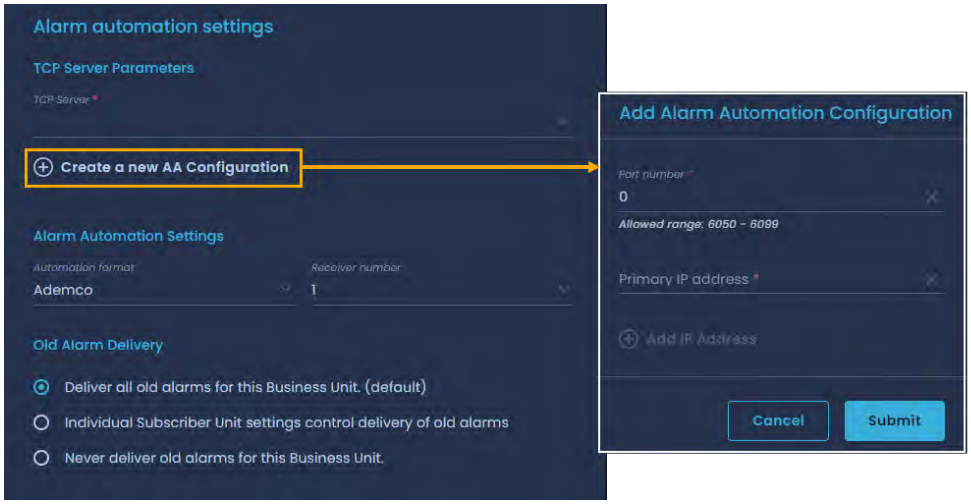
– If the checkbox *is* checked, any new subscriber not in a database that sends data will automatically use this business unit.



Note: Once the **Enable Universal IP Links/IP Groups** has been checked, the screen at the left is displayed.

Enter the ID of the IP-Link transceiver that will handle all subscribers.

3. Populate the Alarm Automation settings:



- **TCP Server Parameters**: For the TCP server, enter the IP address of the Alarm Automation system. The default is blank and should have an entry only if communication to Alarm Automation via TCP/IP is desired.

  Port Number: The IP port that the INCC receiver sends alarm automation messages on (default is blank).

- **Automation Format**: Select the emulation to use for messages using these settings. Select either Ademco or Radionics according to the configuration of the alarm monitoring system. See the AES website (AES-Corp.com) for a listing of generated messages.

Receiver Number: Select the number to place within the character(s) that represent the receiver number in the Alarm Automation message (default is 1). Range is Blank, 0 to 9 and A to F (0 and Blank are selectable options but may not be valid entries for all alarm Automation systems). Some Alarm Automation systems may ignore or be set to ignore this parameter.

Unless you know that you need or want something different, use the default and suggested value of 1.

Old Alarm Delivery

- Alarms are reported by AES subscribers when a zone that has gone into alarm in the past has not yet restored to its non-alarm condition at the time the subscriber is sending a Check-In or a Status report.

  Note: Compliant configuration to UL 864 requires the setting to be “Deliver all old alarms for this Business Unit.” See NOTICE TO USERS, INSTALLERS, AUTHORITIES HAVING JURISDICTION at the beginning of this document for details.

  Some Alarm Automation systems may not be configured to properly report these types of messages. There may be reasons not to send these signals to automation but be aware that these messages may indicate important conditions such as zone inputs that are possibly stuck, improperly configured, improperly wired, or in an alarm condition and may not be able to report a new event. Options are:

  – Deliver all old alarms for this Business Unit (default)

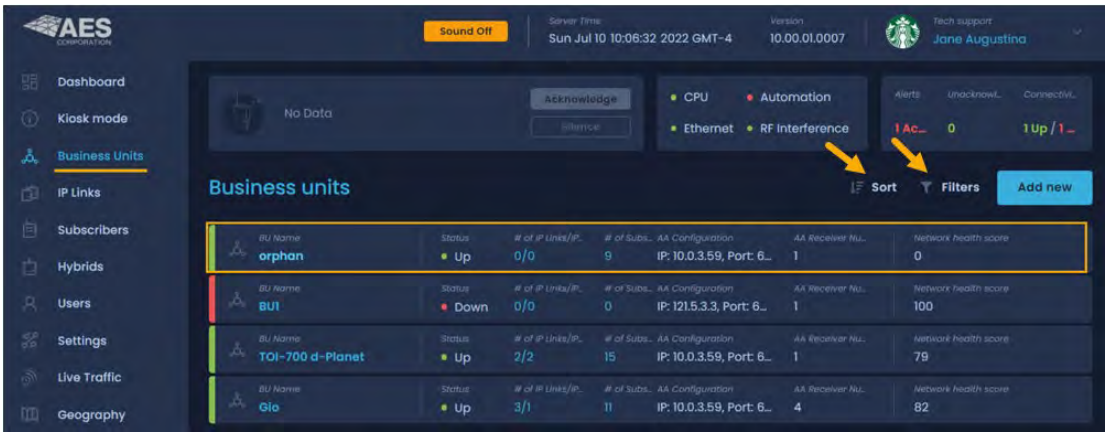
  – Individual Subscriber Unit settings control delivery of old alarms (configuration for each subscriber set in the subscriber unit setting)

  – Never deliver old alarms for this Business Unit (ignores subscriber configuration and will not report all old alarms to automation)

Business Units Dashboard

Business units that have been created on the system are displayed on the Business Units dashboard, along with a snapshot of information for each business unit, including:

- The status of the business unit
- Number of IP Links, IP groups, and subscribers associated with the business unit
- The business unit's alarm automation receiver number
- The network health score



Sorting and Filtering

Business units can be sorted and filtered from the dashboard.

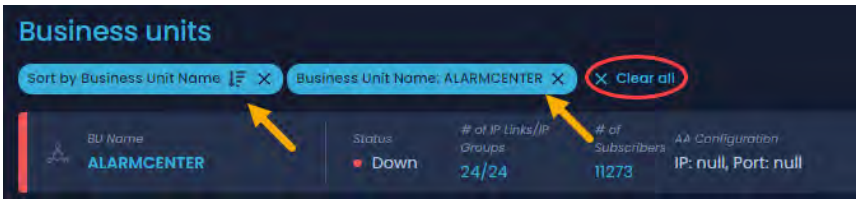
- To sort, click **Sort** to display the sorting options, then select your criteria and click **Ok**. The selected sort criteria are displayed at the top left of the list of business units.

Sort selection *Result*

- To filter out some of the business units, click **Filter**, then enter your data into the desired filtering fields. Click **Apply Filters** at the bottom right.

Filter selection

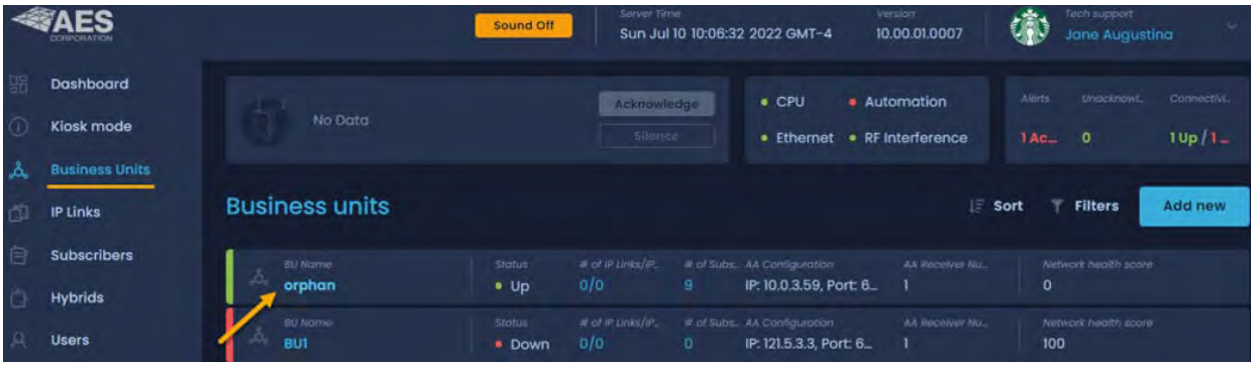
Result



Note: Filters can be cleared using either **Clear all** from the Business Units dashboard (shown above) or **Reset Filters** from the Filters dropdown (shown at left).

Viewing Individual Business Units

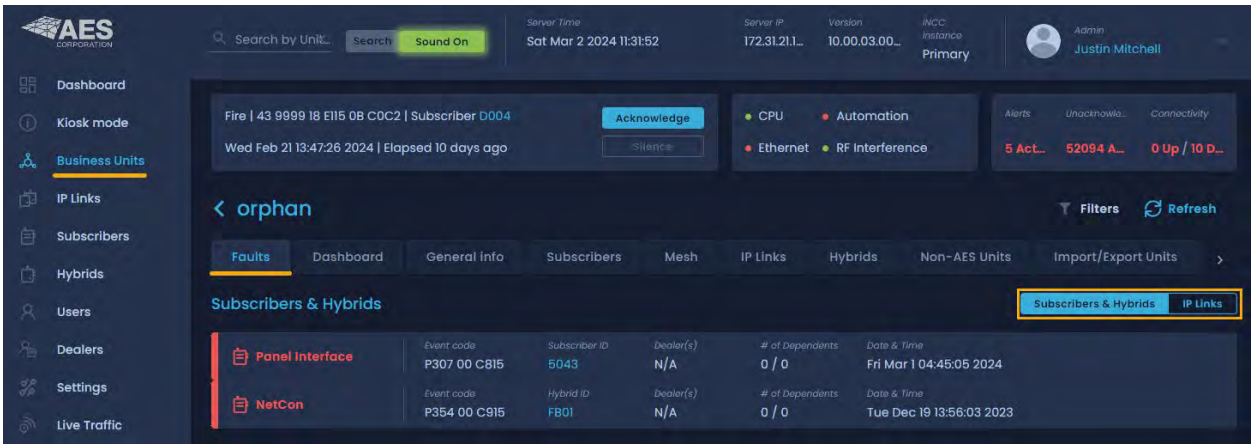
To view detailed information about a specific business unit, click the name of the business unit.



Each individual business unit has 17 tabs. (To view the tabs further to the right, click into any one of the other tabs and you will see an arrow icon at the right.)

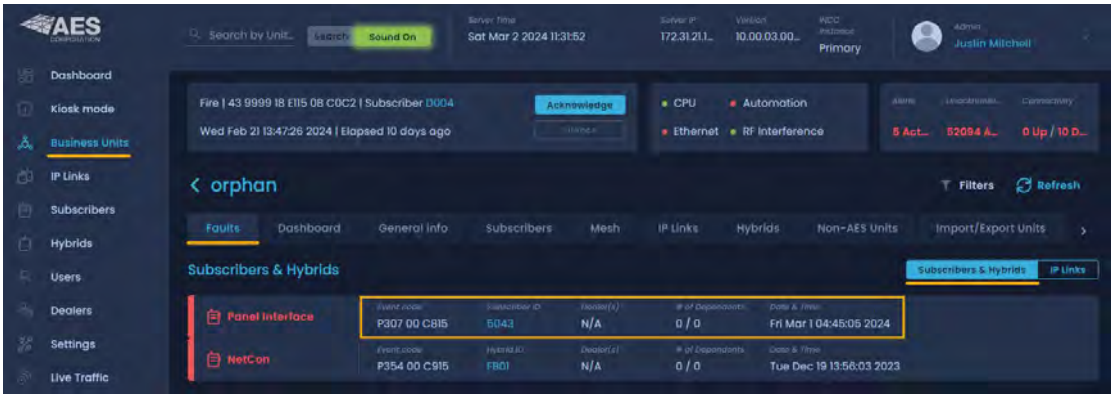
Faults Tab

The Faults screen allows you to view faults based on product type. Use the toggle buttons at the bottom right to switch between **Subscribers & Hybrids** and **IP Links**.



Both types of faults include the following information:

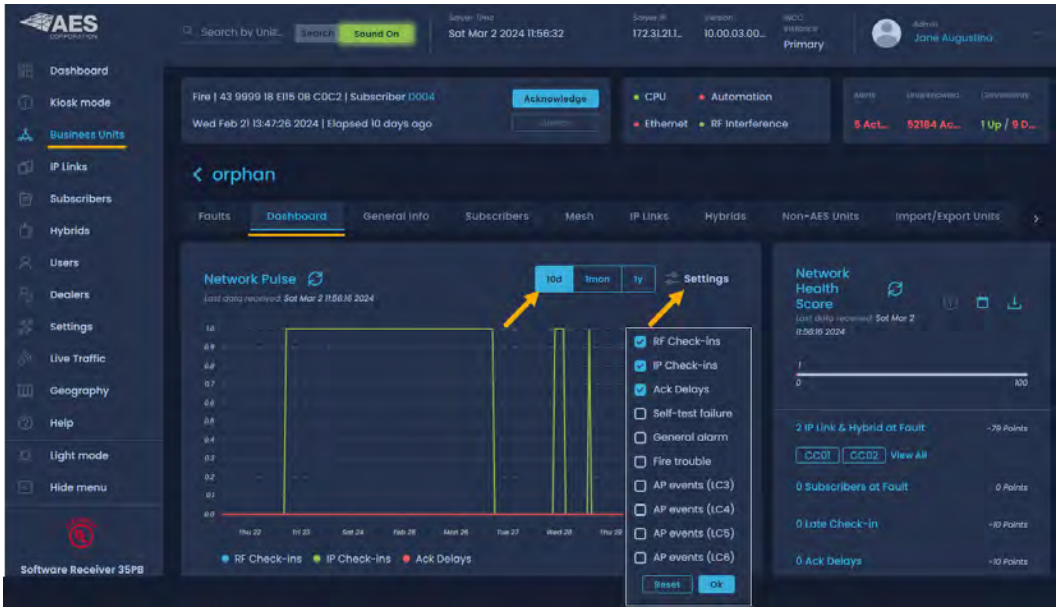
- Event code: Event code associated with each fault (the event code triggers the fault)
- Subscriber ID:
- Dealer(s):
- # of Dependents: The number of dependent subscribers
- Date & Time: The occurrence of the fault



Dashboard Tab

The **Dashboard** tab displays a color-coded line graph (i.e., the network pulse) that depicts network operation information, a network health score, and fault messages for subscribers.

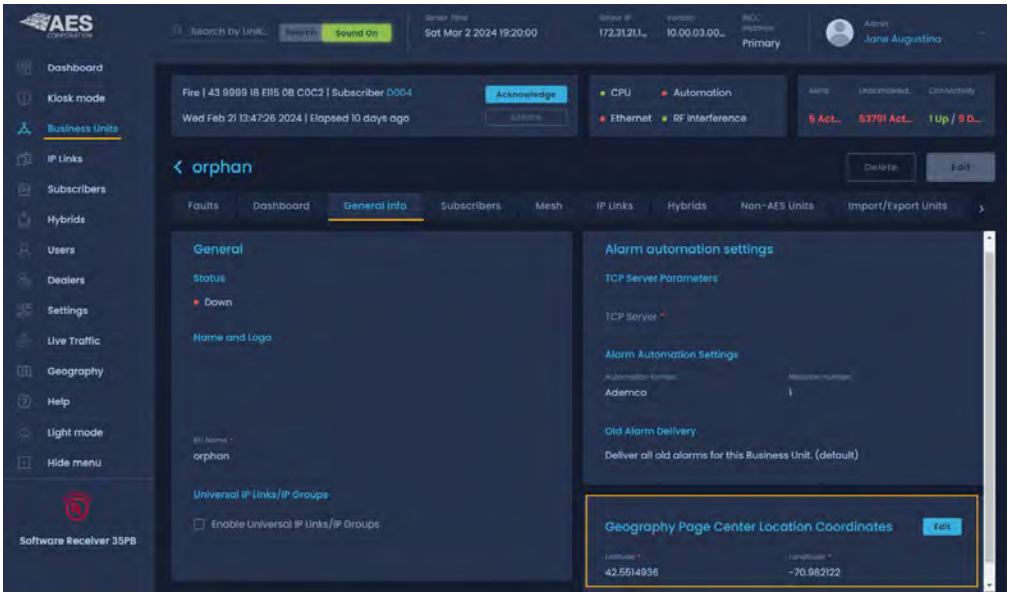
- To switch between daily, monthly, or yearly data for the network pulse history, toggle between **10d**, **1mon**, and **1y**.
- Use the **Settings** dropdown to select the data to include in the network pulse grapic.
- The network health score ranges from 0–100 and is based on four event categories. For more details on the network health score, please refer to the AES website.
  - IP Link/hybrid subscriber fault
  - Subscriber fault
  - Subscriber late check-in
  - Subscriber Ack delay



General Info Tab

The **General info** tab displays information that was populated at the time the business unit was created, including the status of the business unit, the name of the business unit, any IP Links and groups associated with the business unit, and alarm automation (refer to Alarm Automation

In addition, the Geography Page Center Location Coordinates setting (at the bottom right in the image below) allows you to specify where each BU is geographically located. For example, the coordinates for the BU shown below (QA BU1) correspond to those same coordinates on a map.

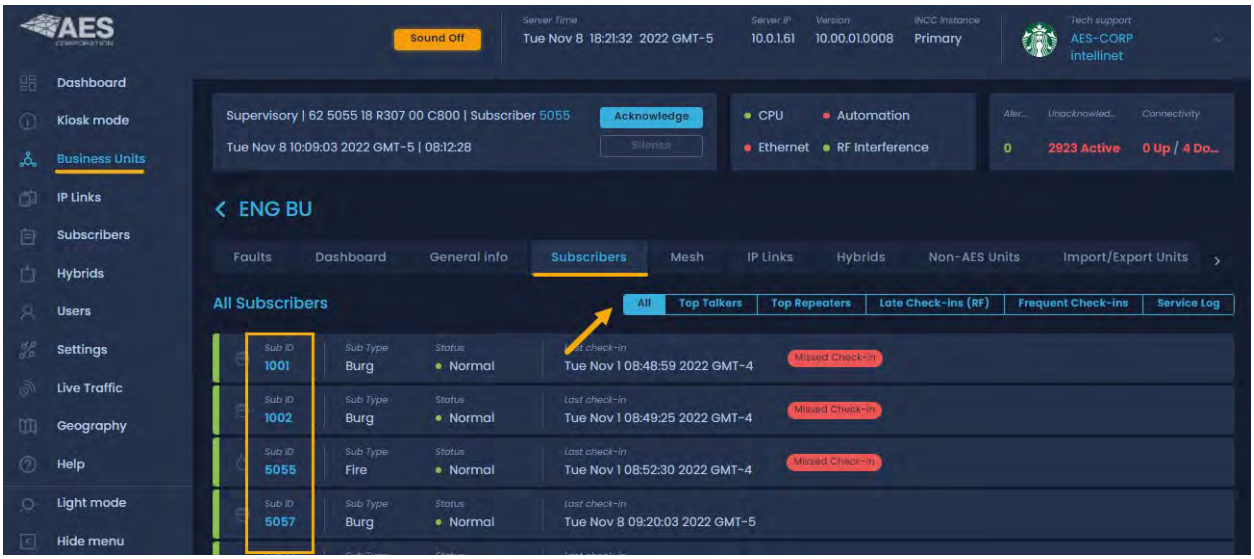


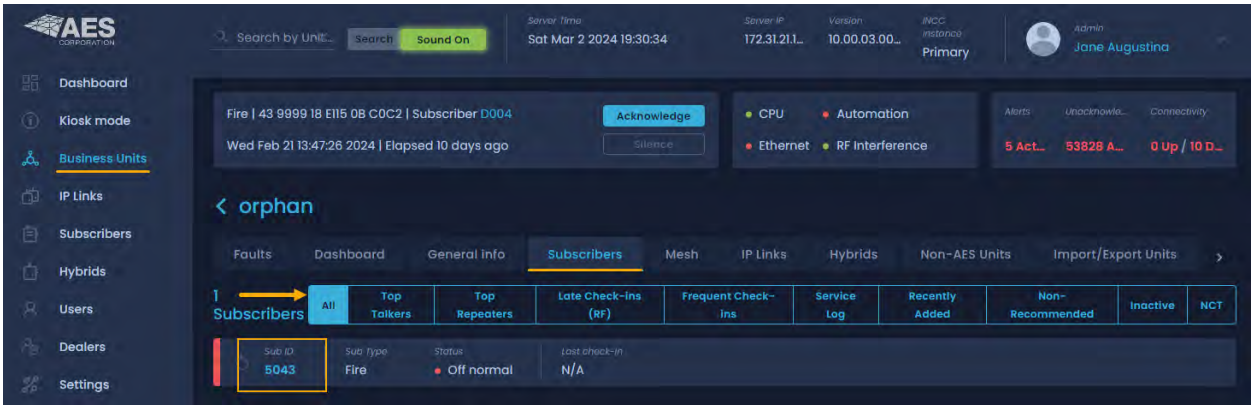
Subscribers Tab

The **Subscribers** tab displays a list of all subscribers associated with a business unit.

Subscribers can be filtered based on signal activity: top talkers, top repeaters, late check-ins, frequent check-ins, service log, and others (see Table 1, Network Analysis Tools for more details).

The **Subscribers** tab displays missed check-in alerts, which are notifications of faults on the subscribers. If subscribers don't check in at the set interval time, faults are triggered. Refer to the Radio Check-in Interval setting in the subscriber's Settings Tab to view the timing settings that impact faults.





To access a specific subscriber, click the subscriber from the list of subscribers. Subscribers are described in detail on page 68 (Subscribers).

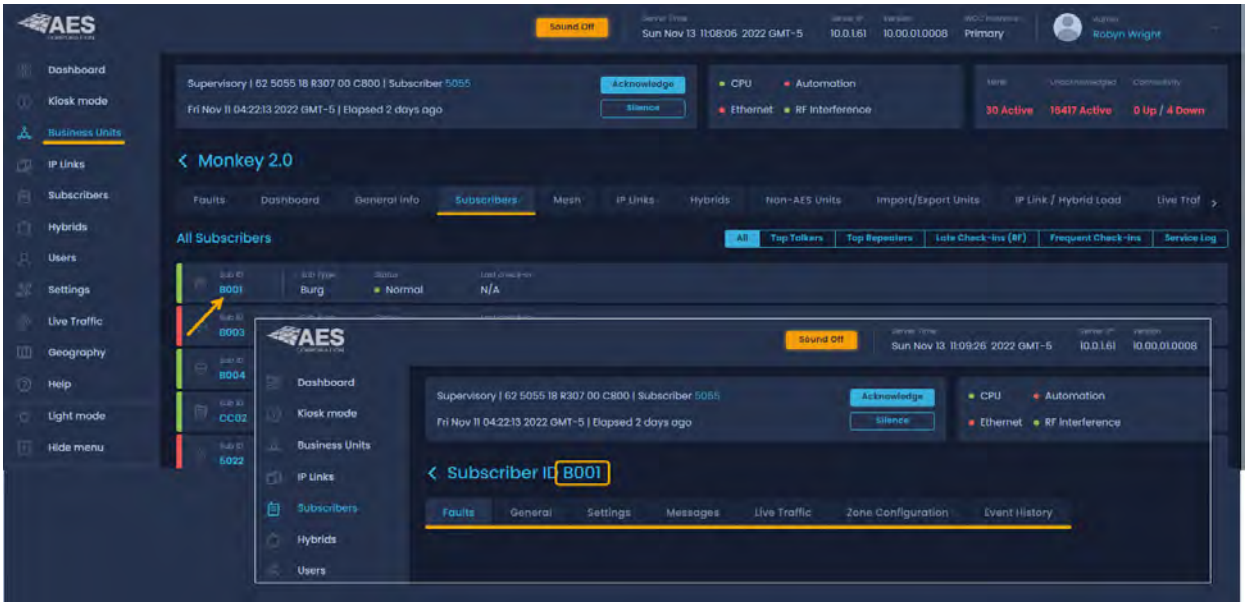
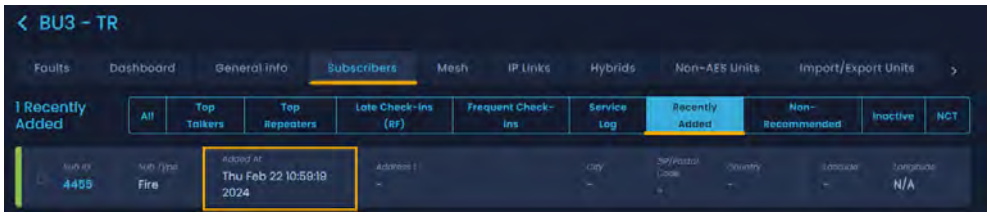
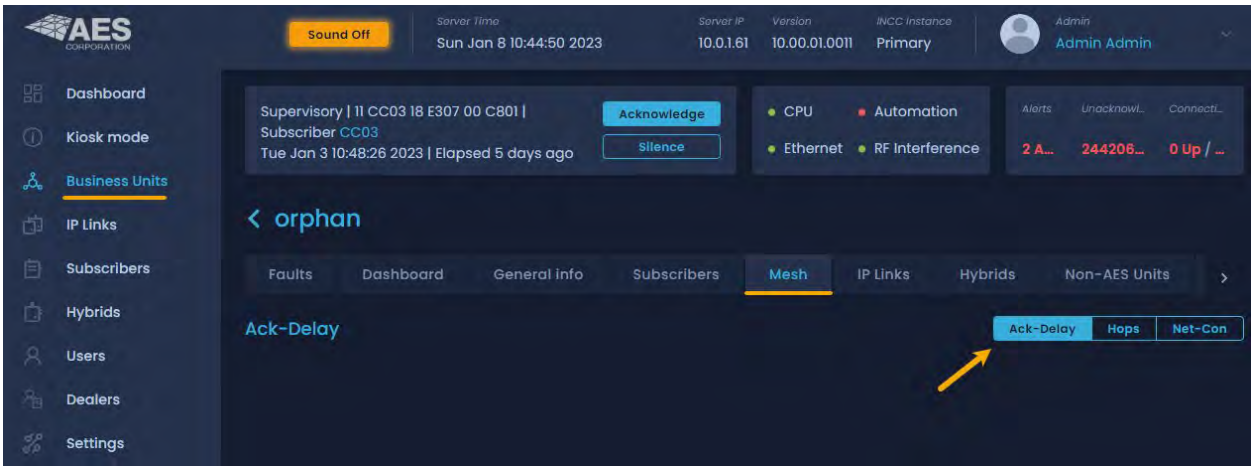


Table 1. Network Analysis Tools	
Top Talkers	Ideally, all subscribers in the network should generate roughly equal numbers of RF packets. Excess RF traffic from a single subscriber may reduce network efficiency by consuming airtime. To reduce excess activity on a subscriber: • Ensure the subscriber is installed properly. • Ensure the subscriber is free of faults.

Table 1. Network Analysis Tools	
	– Ensure the alarm panel connected to the subscriber is configured and connected properly. – Ensure the alarm panel connected to the subscriber is free of faults. – Ensure all zone, power, and communication wires are secured properly.
Top Repeaters	Repeating the packets of other subscribers is a normal function of the mesh network; however, excessive packet forwarding by a single subscriber may reduce network efficiency and cause delays, although unlikely. To improve efficiency: • Install an IP Link or a hybrid near any subscriber that repeats packets for many dependent subscribers. • Consider changing the antenna height or replacing with a higher or lower gain antenna.
Late Check-ins (RF)	Late Check-ins displays the list of subscribers currently late checking in, the length of time each is late, and the last time it checked in. Each subscriber normally transmits check-in messages at regular, pre-set intervals. If the INCC does not receive a check-in message at the expected time, there might be a problem with the subscriber; alternatively, there might be a problem with network performance, which may be explained by an environmental factor such as weather conditions. Once subscribers transmit three check-ins on schedule, they are removed from the Late Check-ins list. To improve network performance: • Ensure the subscriber is installed properly. • Ensure the subscriber is free of faults. • Ensure the subscriber is connected to the network by watching the LEDs on the subscriber PCB. • Ensure the subscriber settings on page 75 are up to date. • Consider changing the antenna height or replacing with a higher or lower gain antenna. • Consider installing an IP Link to improve network performance.
Frequent Check-ins	Frequent Check-ins displays the list of subscribers currently transmitting frequent check-ins and the number of check-ins per the recommended 24-hour period.

Table 1. Network Analysis Tools	
	Each subscriber normally transmits check-in messages at regular, pre-set intervals. The recommended number of check-ins per 24 hours is one; this meets the requirements of UL 864 for Commercial Fire and is appropriate for virtually all applications. A higher number of check-ins per 24-hour period can unnecessarily increase RF traffic on the network. AES recommends setting the subscriber Check-in interval to 23:45. A shorter time interval increases RF traffic in the network. To improve network performance: • Ensure that the subscriber is installed properly. • Ensure that no subscribers have mis-configured check-in intervals.
Service Log	Subscribers may occasionally require service; the service log identifies all subscribers that are currently in need of service.
Recently Added	Subscribers that have been added to the network within the last 10 days are displayed in the Recently Added list. 
Non-Recommended	Subscribers that fall outside the default TTL settings (referenced in the 7707 User Manual) are displayed in this list, triggering a notification so that customers are aware that these subscribers could potentially be harming the network.
Inactive	Subscribers are considered inactive if more than 10 days have lapsed since the subscriber's last check-in. This page is helpful for troubleshooting changes that have occurred on the network. These changes also appear on the Geography page, which can be used as confirmation.
NCT	NCT (an abbreviation for Network Connectivity Tool) is a diagnostic tool that lets you check whether a radio has two active paths at a particular site. This tool is used for setting up subscribers only. Customers use NCT when checking sites for NetCon 5. It does this by creating traffic by ID. If this option is enabled, it will block the ID from impacting health scores or run jobs. For example, late to check reports.

Mesh Tab



- Ack-Delay: When any subscriber transmits an RF packet, the subscriber recipient of the packet returns a message to the sender acknowledging receipt of the packet. An Ack Delay is triggered if a subscriber does not receive an acknowledgement message of a transmitted signal within the configured Communication Timeout Delay period. Ack Delays could indicate a service requirement for a subscriber or may be explained by some environmental factor such as the weather. It may be advisable to locate or install additional IP links near subscribers that remain on the list for extended periods.
- Hops: When a subscriber transmits an RF packet, that packet travels through the mesh network to an IP Link or a hybrid subscriber before reaching a MultiNet receiver. If the IP Link is within direct reach, the subscriber sends the packet to the IP Link; otherwise, it sends the packet to another subscriber along a route leading to the IP Link.

  Each step in the route from subscriber to IP Link or hybrid subscriber is called a hop. As network conditions evolve, the route, and consequently the number of hops from a given subscriber to an IP Link, can change.
- Net-Con: Net-Con is an abbreviation for Network Connectivity and is a rating of the number of radio frequency (RF) paths from a subscriber to other subscribers installed in the mesh network. The mesh refers to all the subscriber units on a network of the same frequency and cipher code. Only fire subscribers report their Net-Con statuses, as either high or low, in messages sent to the MultiNet/INCC receiver.

IP Links Tab

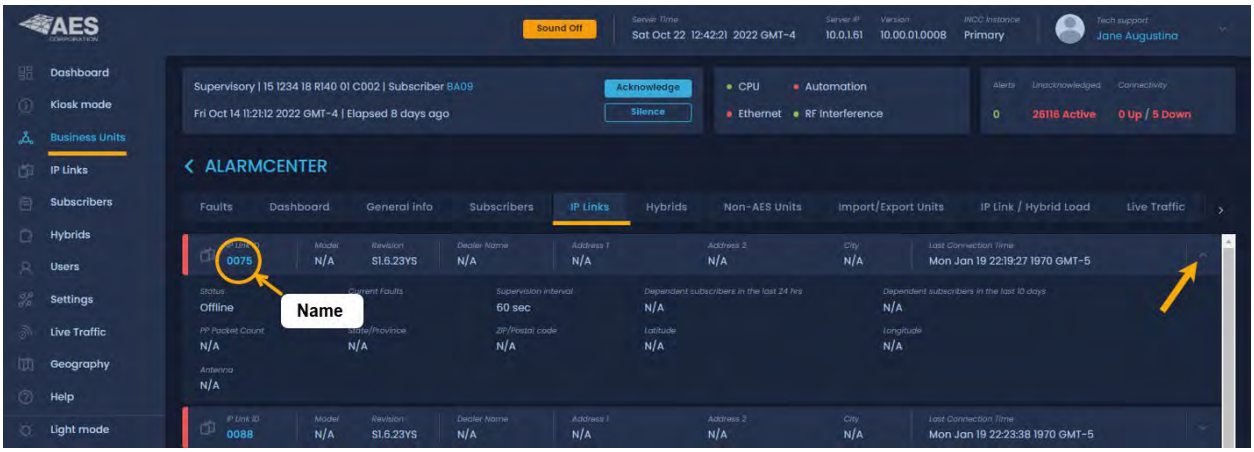
The IP Links tab displays a list of all IP Links associated with a subscriber. Each IP Link displays general information:

- IP Link ID
- Model
- Revision
- Dealer name
- Address
- Last connection time

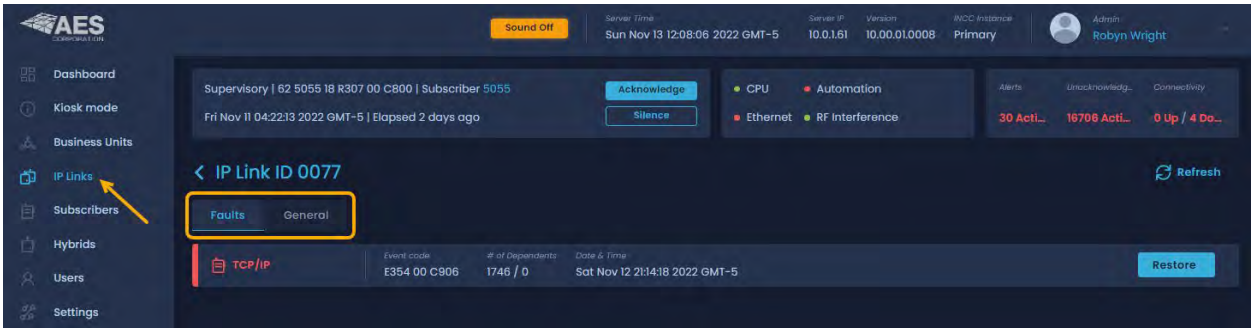
To expand the details for an IP Link, click the dropdown at the right. The additional information includes:

- Status
- The number of current faults
- Supervision interval
- Dependent subscribers in the last 24 hours
- Dependent subscribers in the last 10 days
- PP packet count
- State/province
- ZIP/postal code
- Latitude
- Longitude
- Antenna

To view further information about the IP Link, click the name of the IP Link (see Name below).

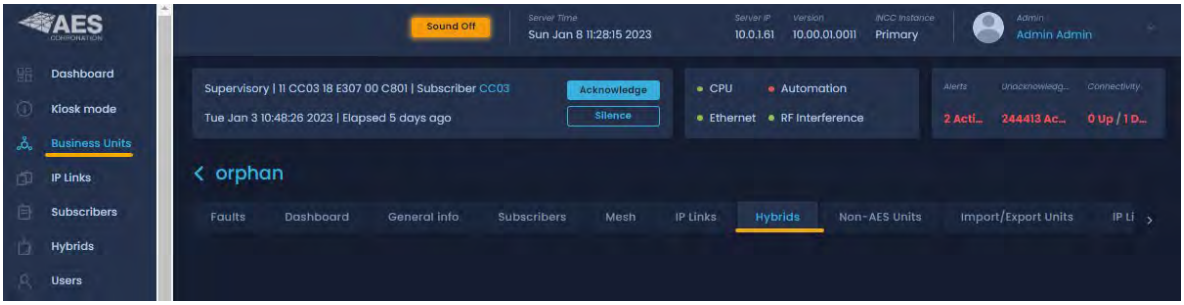


This takes you to the **IP Links** page, which is accessible from the navigation menu. See IP Links to view this information.



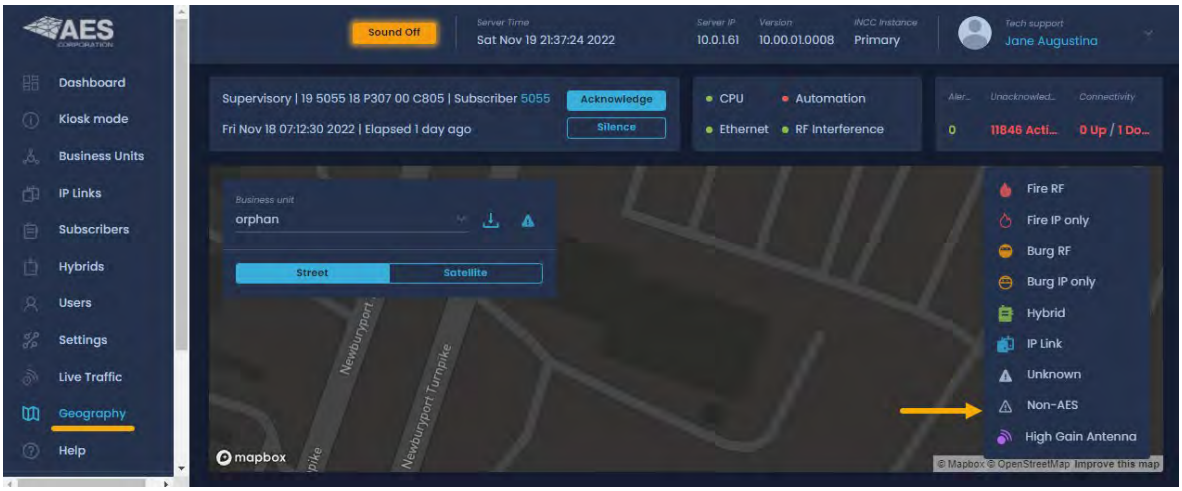
Hybrids

A hybrid fire subscriber offers dual functionality, combining full data module with IP Link. It also helps improve network health and makes it easy to expand and start a new network. See Hybrids section for detailed information on INCC configurations.

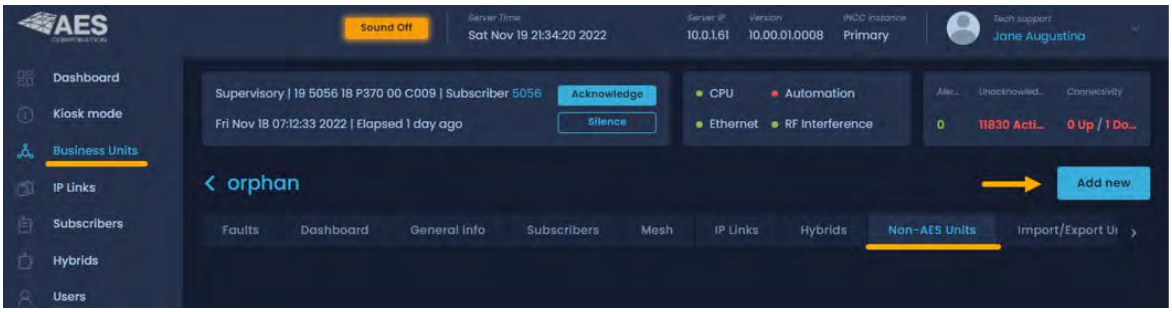


Non_AES Units

A non-AES unit is a unit that is not on the AES network. Adding your non-AES equipment gives you the ability to track the equipment from the **Geography** tab.

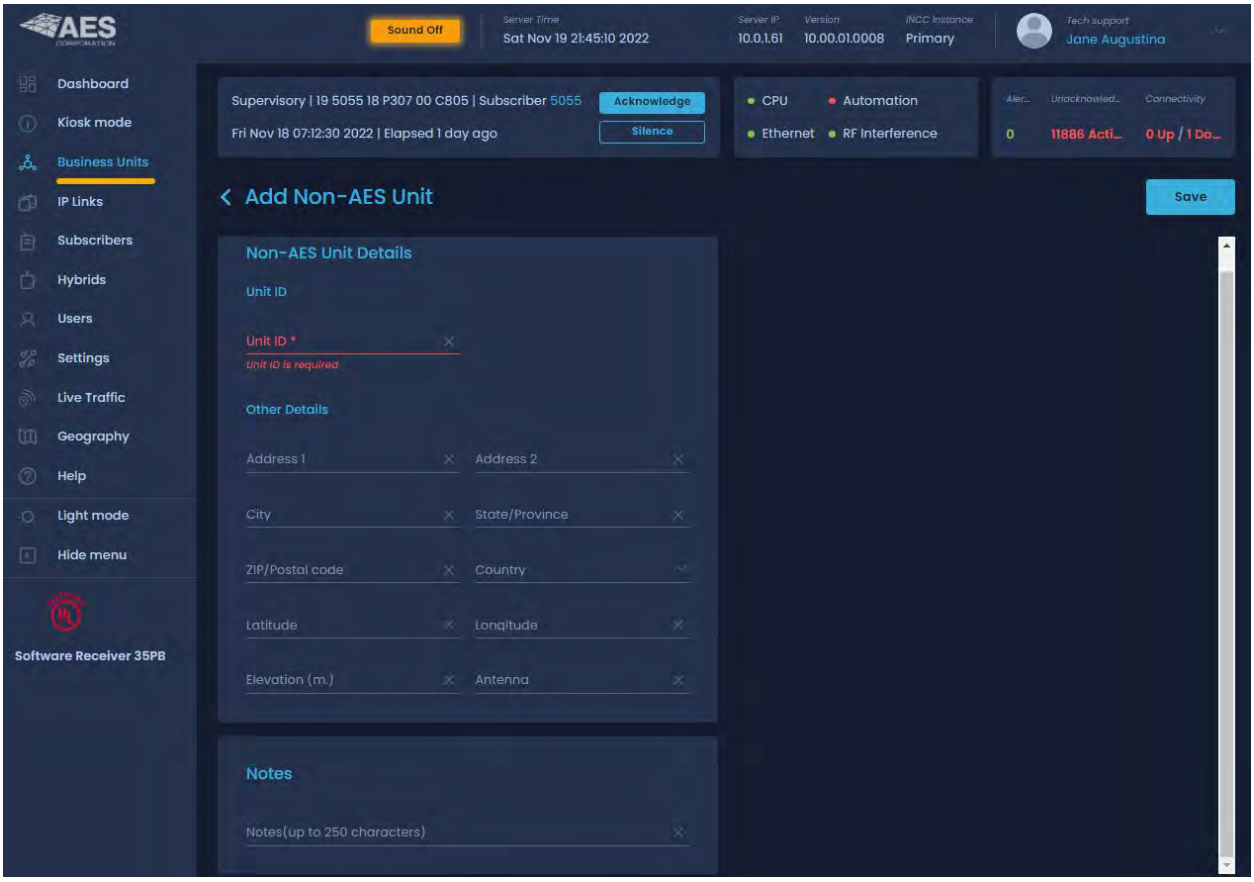


To add a non-AES piece of equipment, click **Add new**.



The information on this screen enables you to track where this unit is located.

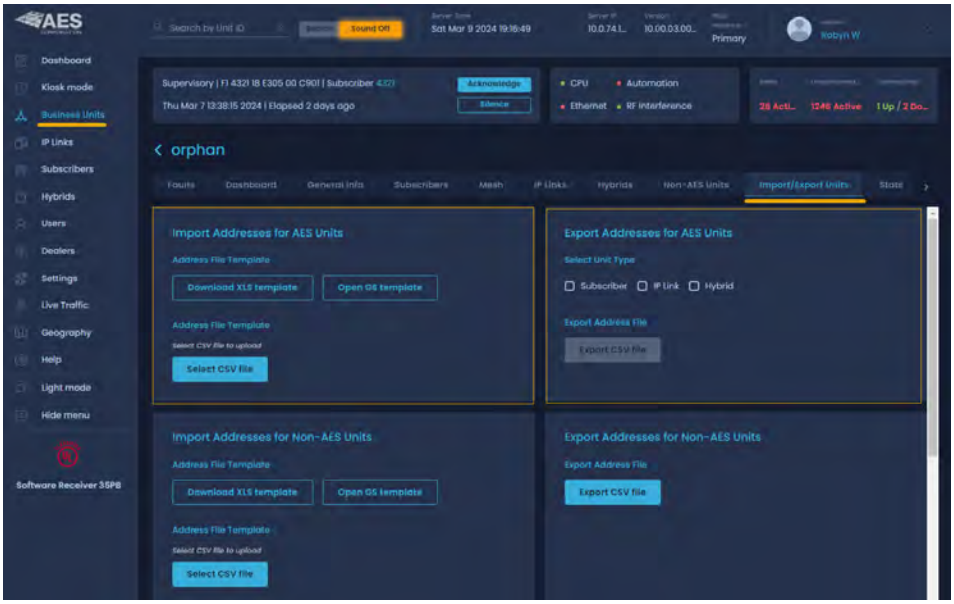
Note: A unit ID can consist of any character type (e.g., number, alpha, free text).



Import/Export Units

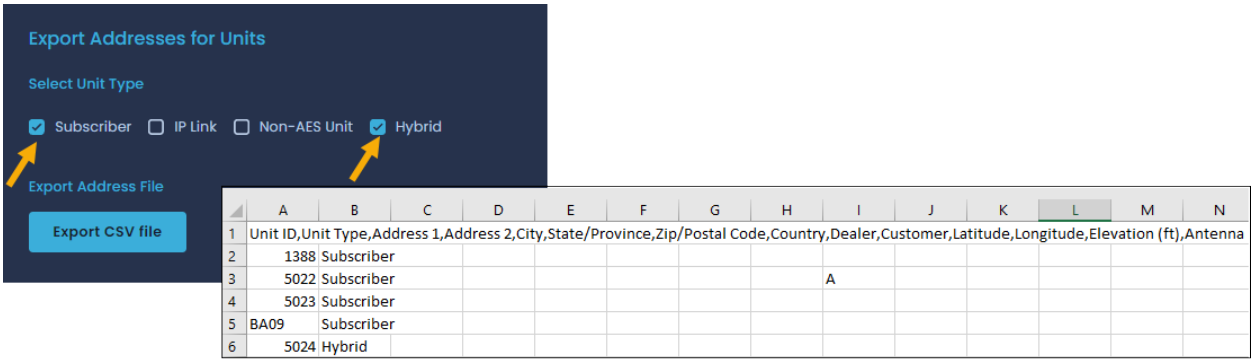
To import addresses for units:

1. Click **Download XLS template** to download the Address File template.
2. Populate columns A through N of the template. Save the file.
3. Export the Excel file to CSV.
4. Upload the CSV file by clicking **Select CSV file**.

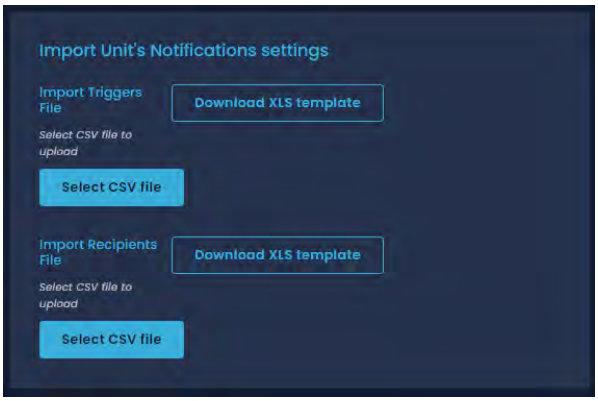


To export addresses for units:

1. Check each box next to the unit types you would like to export.
2. Click the **Export CSV file** button to download the file. The Excel file consists of the data that was selected:



The Import Unit's Notification settings allows you to pull the options that are available on the NMS and bring them into the INCC.

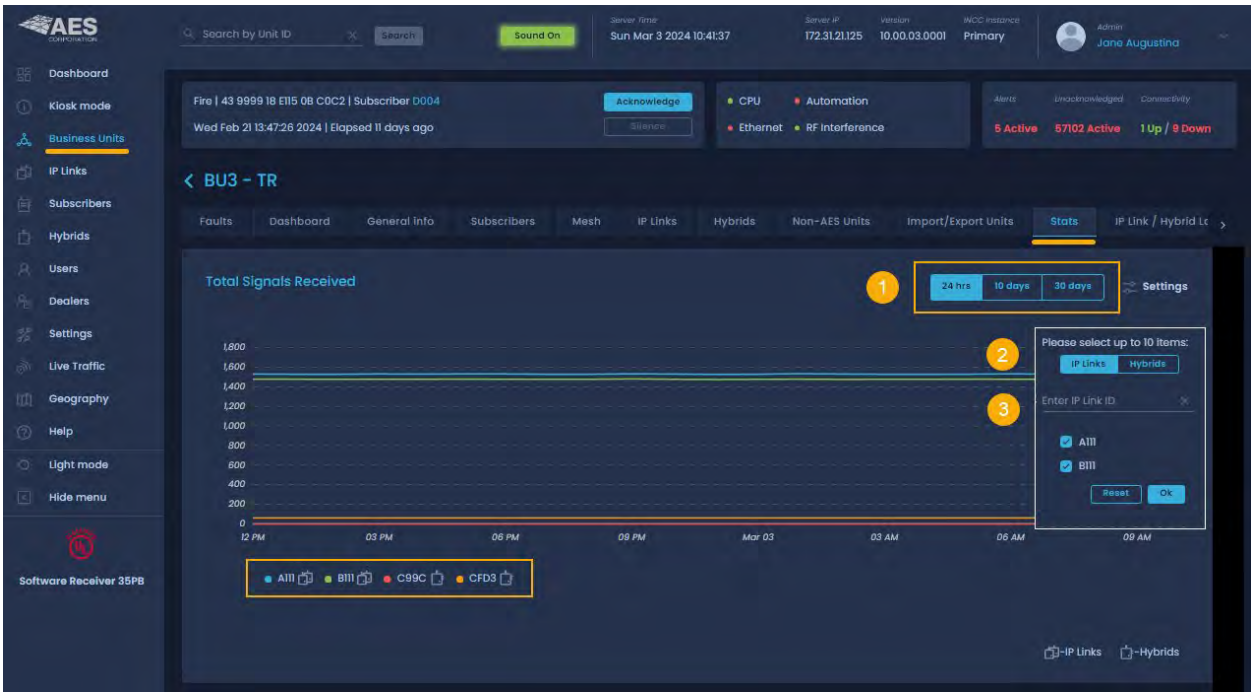


Stats

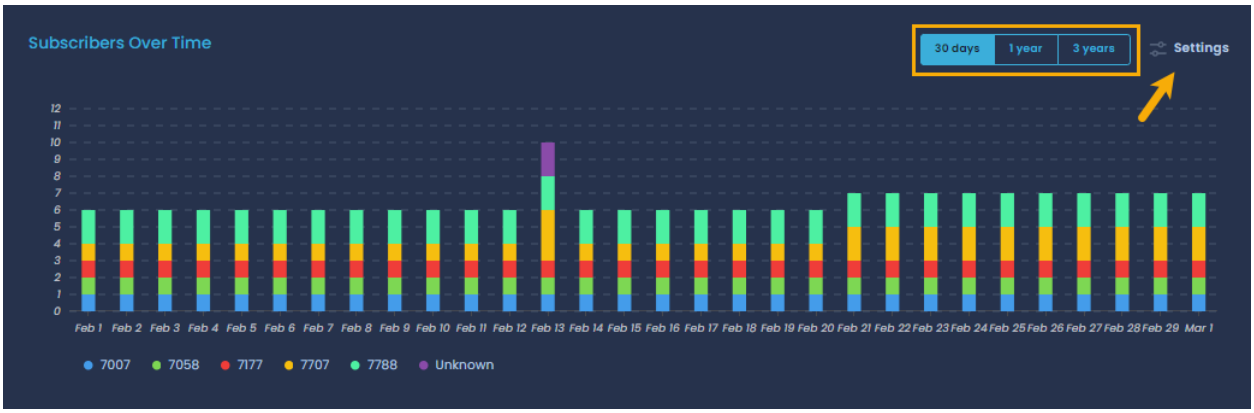
The Stats tab displays the total signals received based on filter selections:

1. To view the total signals received based on time period, select **24 hrs**., **15 days**, or **30 days**.
2. To limit the results to IP Links or hybrids, click **Settings** and check the appropriate option (IP Links or Hybrids).
3. To limit the results to specific IP Link(s), enter each IP Link ID into the search box.

The legend below the graph indicates which signals are being received by the IP Links and hybrids.

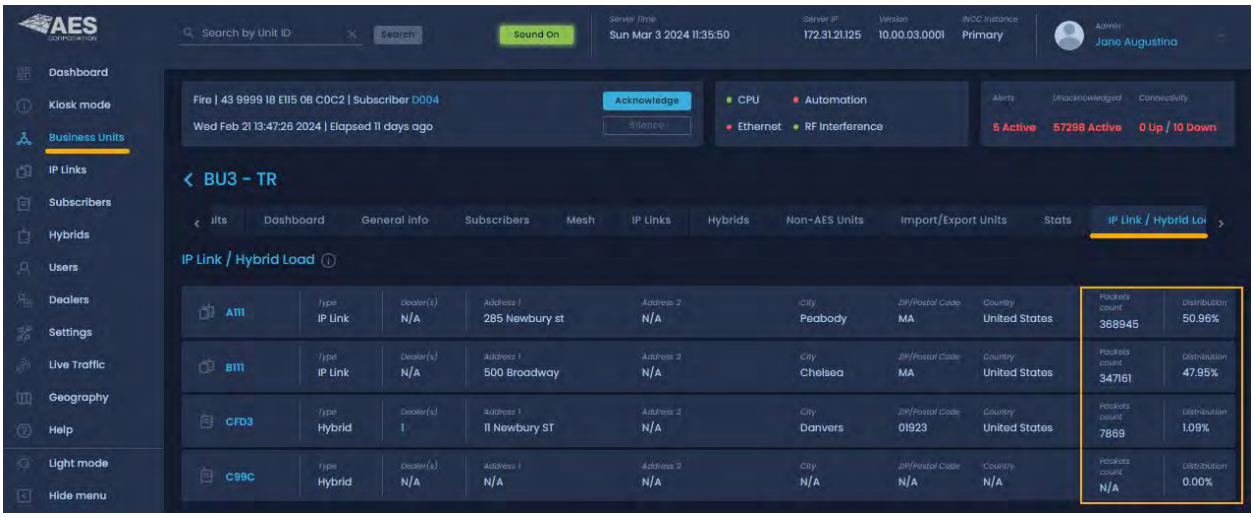


Subscriber activity can also be displayed based on different periods: 30 days, 1 year, and 3 years. Click **Settings** to limit the results to IP Links or hybrids**.**

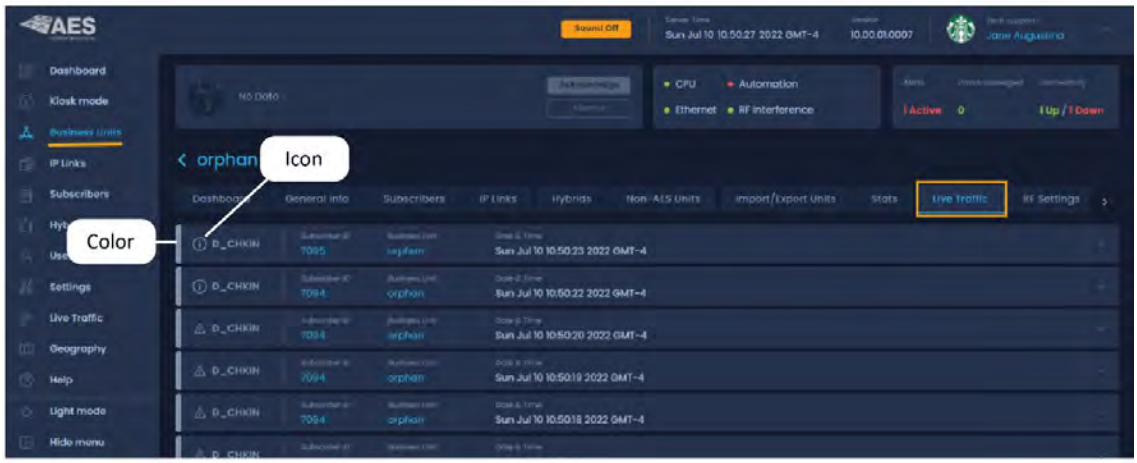


IP Link/Hybrid Load

The **IP Link/Hybrid Load** view displays a list of IP Links at the left. Analytical details include the number of packets received by each IP Link and the distribution of packets among all the IP Links on the network. Ideally, all IP Links in the network should handle roughly equal volumes of RF traffic. This generalization does not apply when the antennas of two IP Links are deliberately placed within RF range of each other such as at a Central Monitoring Station.



Live Traffic



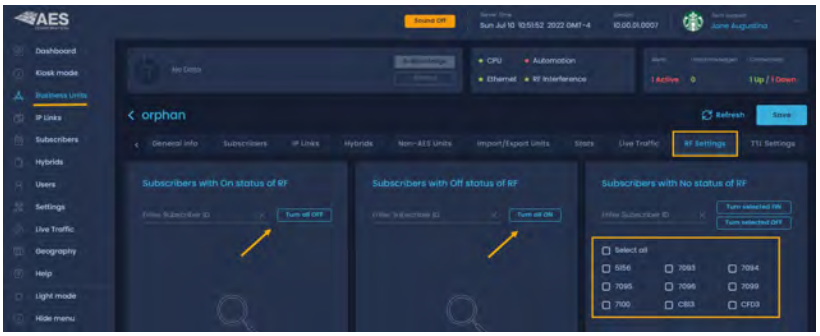
The **Live Traffic** tab provides a live visual representation of the traffic load across subscriber links.

Alarm indications (colors and icons) are shown below:

Color	Icon	Alarm/Event
Red		Fire alarm
Orange		Burglary alarm
Green		Restoral event from devices
Grey		All other cases

RF Settings

Subscribers can be turned on or off based on their RF status. Subscribers with no RF status can be changed via the checkboxes at the right.

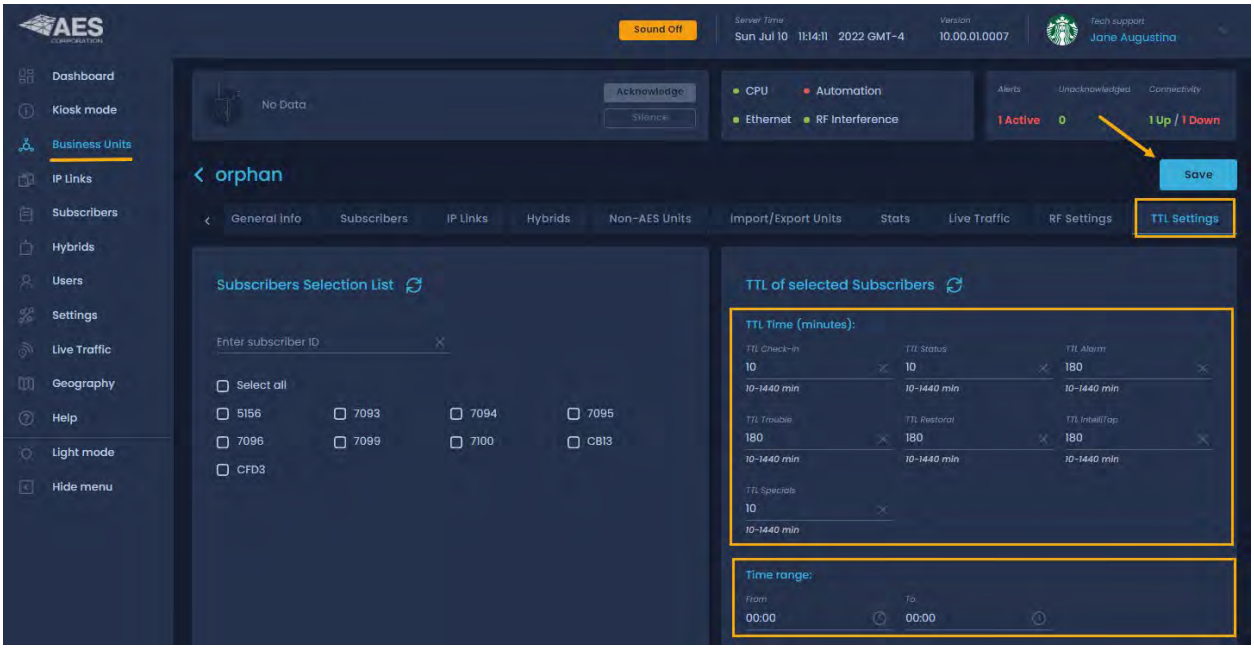


TTL Settings

Subscribers include the “Time-To-Live” (TTL) function. Like the Internet, AES IntelliNet uses a packet-based technology. The Time-to-Live concept in the Internet is based on the fact that all data has a useful life.

The benefits of TTL are best exhibited when the IP-Link goes off-line due to a lightning hit or some other unlikely, catastrophic event. While the IP-Link is off-line, messages traveling through the system are stored in the individual subscriber units for later delivery. Under the default TTL settings, unimportant test timer messages (typically 95+% of the traffic) are deleted from the subscriber unit memory after 30 minutes of being delayed in the network. Thus, the system will not have to handle the message when the IP-Link Receiver comes back on-line. All other messages, such as alarm, etc., speed their way to the IP-Link as they normally do.

Important: UL864 requires a setting of 0 for Alarm, Trouble, and Restoral.



The default Time-to-Live can be customized and assigned to specific subscriber(s). Defaults are shown in the TTL Time box at the right. To customize these settings, enter new values, then select the subscriber(s) you want to update from the subscribers list at the left. Once these settings have been saved, all subscribers will use the new time.

Notes

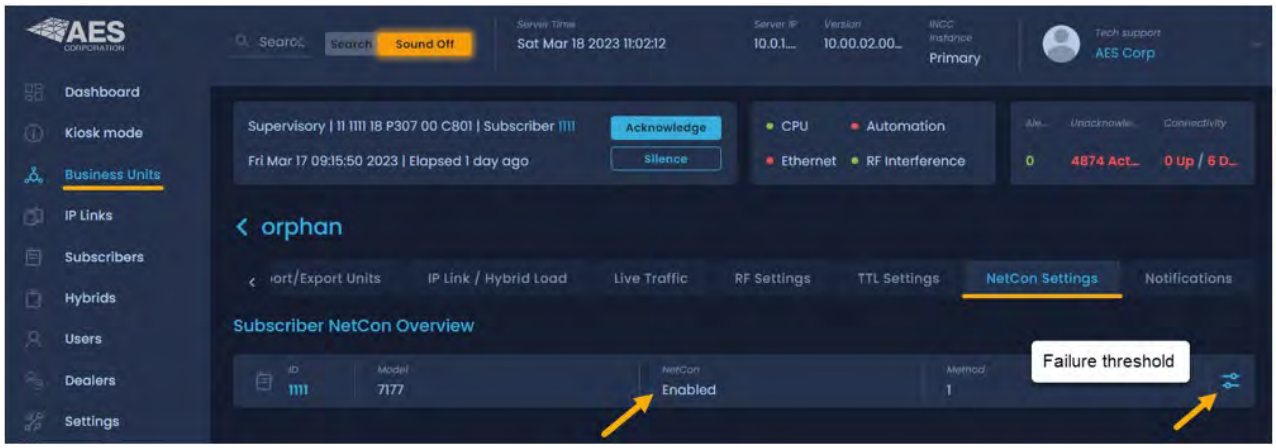
- TTL Check-in: Note that even when a check-in packet is deleted due to a delay, the objective of that message has already served its purpose: the late or missing signal should have been flagged at the central station (see Automatic Test Supervision section).

- Under the default (factory) settings, only test timer messages are subject to the TTL function. If you want TTL for other message types, YOU must activate it when you program the subscriber unit.
- The TTL time is included in packets generated by TTL capable subscribers. This feature is available in subscribers with firmware Version 2.1 and later which was first released in late 2000.
- The timeout function works when a packet is stored for forwarding in any subscriber with TTL capability, which will decrement the TTL time for the packet it is storing. When TTL time has expired, the packet is aborted. This function does not work with non-TTL (pre-Version 2.1) subscribers. The TTL feature works best when the majority of subscribers, or the subscribers that are most heavily used, have the feature in the firmware. Call your AES representative for upgrade information.
- Default time for Check-In Packets is 00 hours, 30 minutes. DO NOT enter a value greater than 24 hours 00 minutes. Entering a time of 00 hours and 00 minutes deactivates the time-to-live function for that packet type. The shortest allowed TTL time is 00 hours, 10 minutes. TTL can also be set for other packet types:
  - TTL Alarm
  - TTL Trouble
  - TTL Restoral
  - TTL IntelliTap
  - TTL Specials

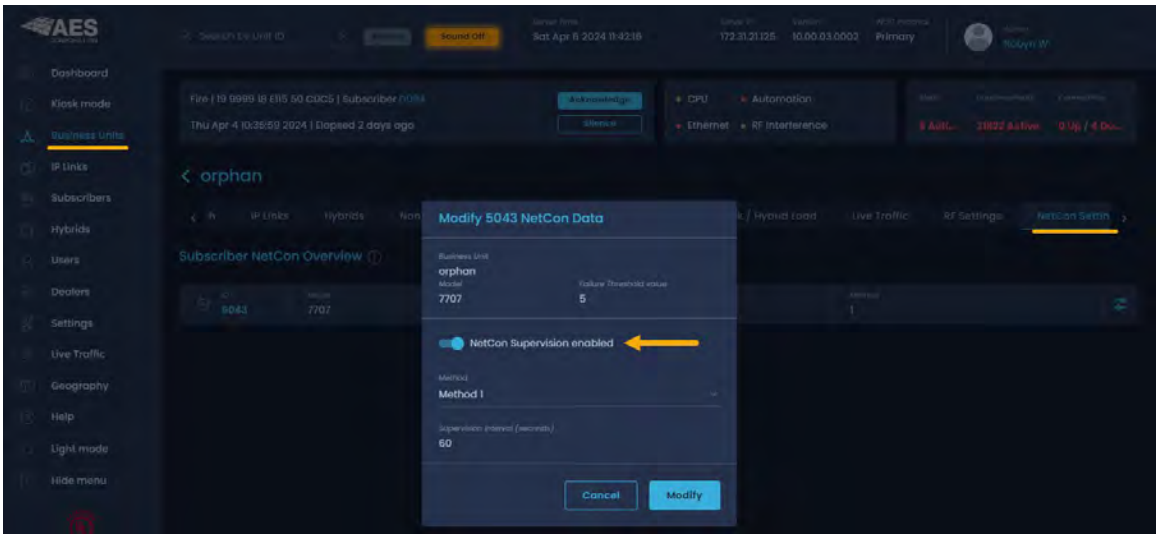
- The default time for the five packet types above is 00, i.e., the time-to-live function is deactivated for these packets. Entering anything greater than 00 hours and 10 minutes enables the Time-to-Live function. Enter the data for each type, then click **Save**.
- To confirm the data, press **<Alt>**+**<N>** to query the subscriber for Packet Life settings. Once the TTL parameters packet has been received back, check this screen again.

NetCon Settings

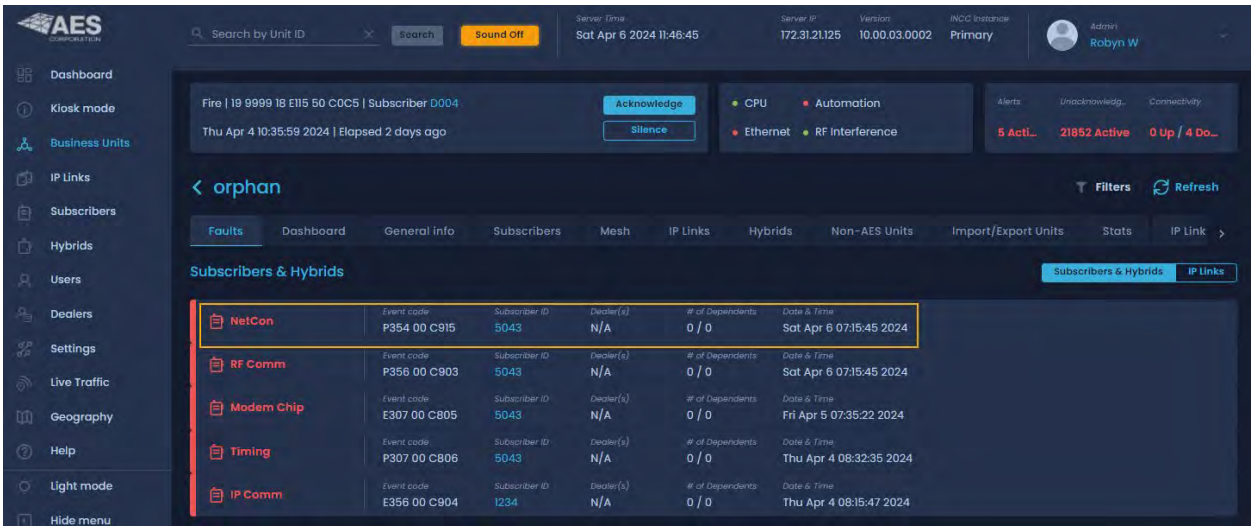
NetCon is a measurement calculated by a subscriber to determine the confidence level that transmissions will reach an IP Link. Only fire subscribers report NetCon status, as either high or low, in messages sent to the INCC. To modify the NetCon data, click the icon at the bottom right (see image below).



From here, you can enable or disable NetCon on a subscriber and make other adjustments.



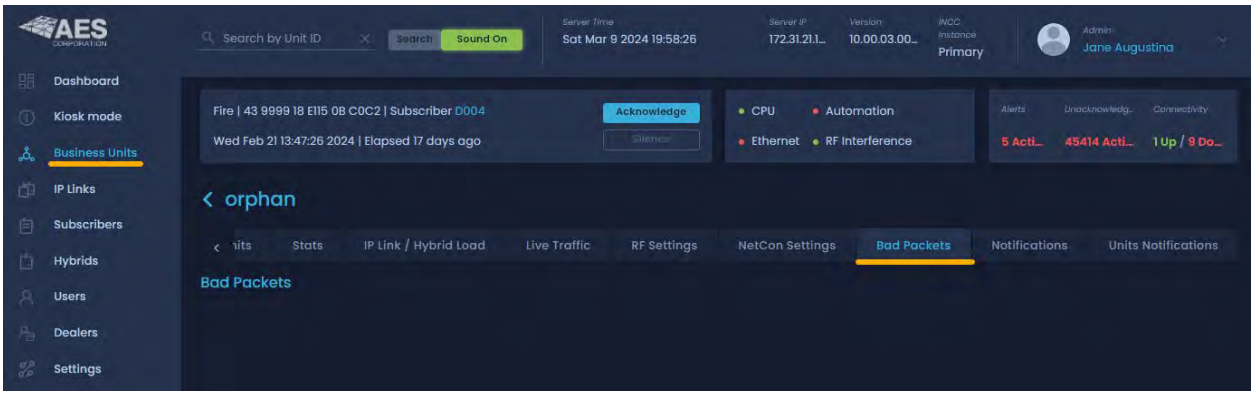
Subscribers with a NetCon value of 6 or higher are displayed in the **Faults** tab of the business unit.



Note: When a fire subscriber reports low NetCon, it's important to ensure that the other subscribers communicating with it are operating normally and are free of faults. In may be advisable to relocate the subscriber or to relocate or change its antenna.

Bad Packets

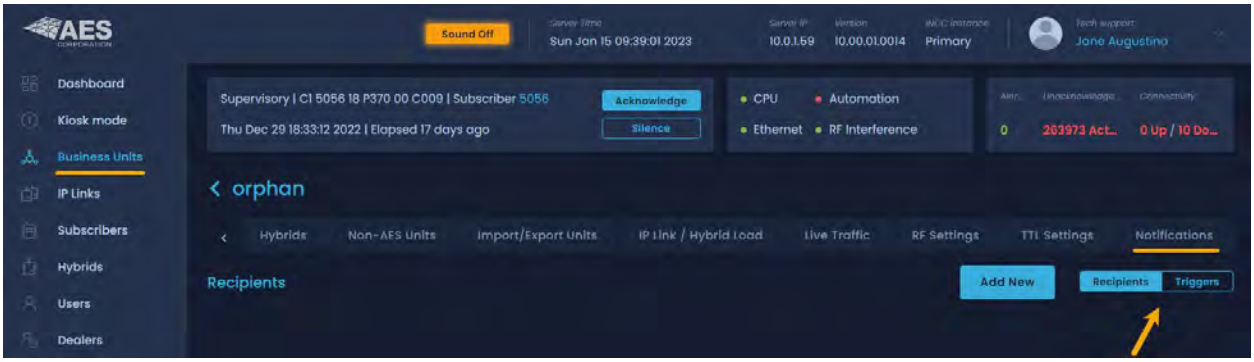
The Bad Packets tab displays events that involve the rejection of a bad packet (e.g., bad check stub, corrupt data, non-deciphering data).



Notifications

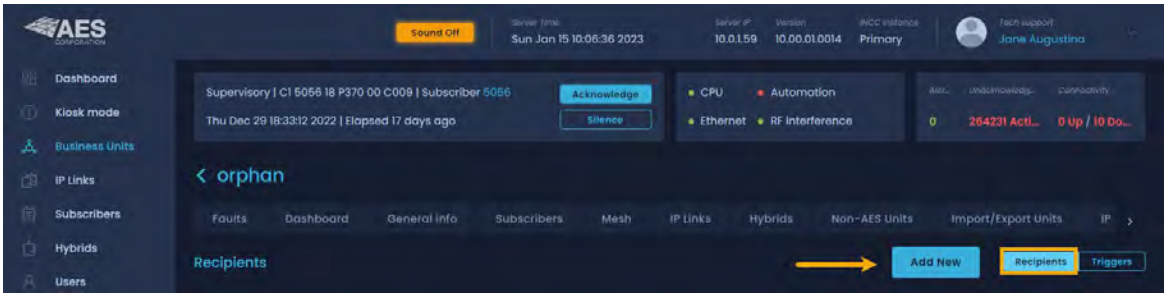
The Notification function enables users to monitor their AES-*IntelliNet* network from anywhere at any time. Users can configure automatic alerts based on a change to the network health score, a fault with any subscriber or IP links, or when traffic drops on IP links.

Separate dropdown menus enable users to easily create the list of personnel to be notified by both SMS and email, define the fault criteria to be reported, and create associations between the alert triggers and personnel to optimize response.

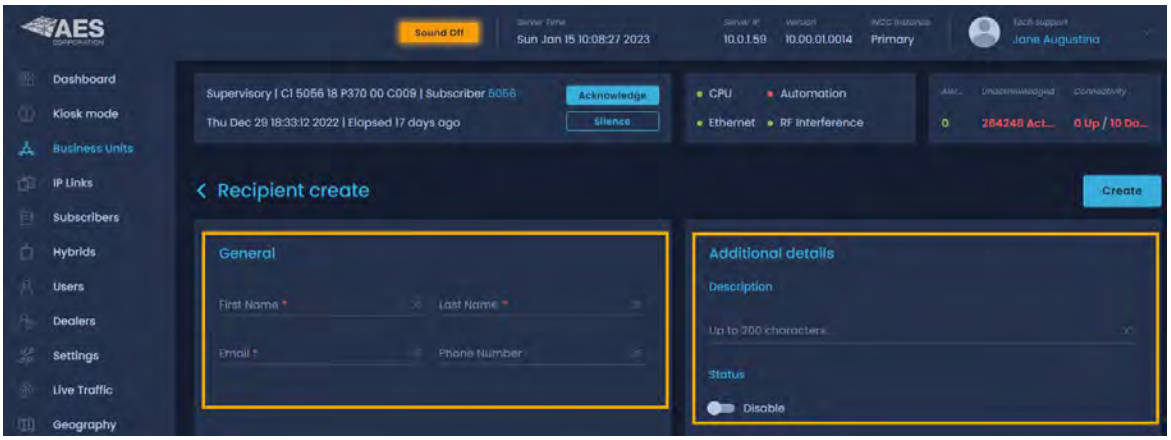


To create a list of Recipients:

1. Click the **Recipients** button, then click **Add New**.

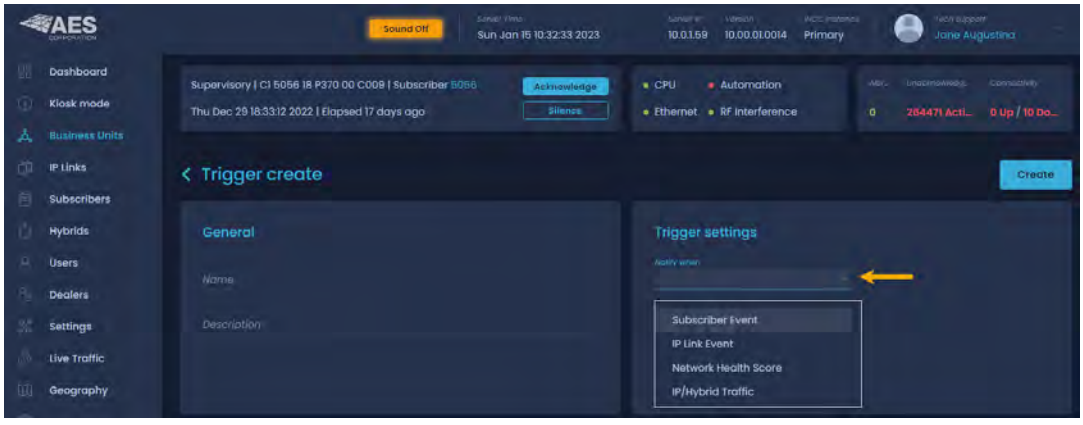


2. Enter the recipient's name and email address, then enter a description.

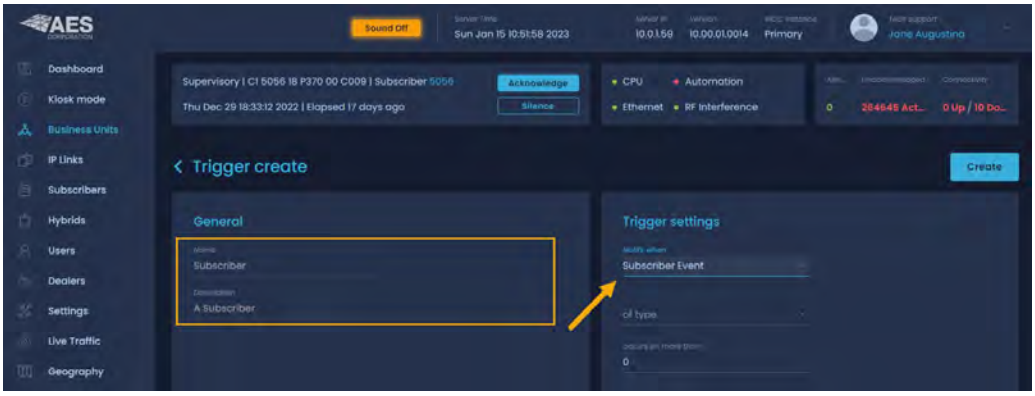


To define the fault criteria to be reported:

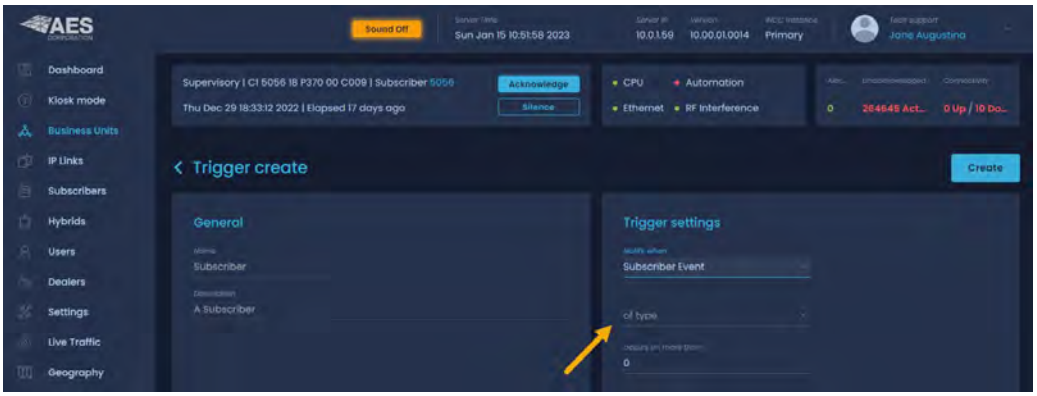
1. Click the **Triggers** button, then click **Add New**.
2. Click the **Notify when** dropdown at the right, then select a trigger from the list.



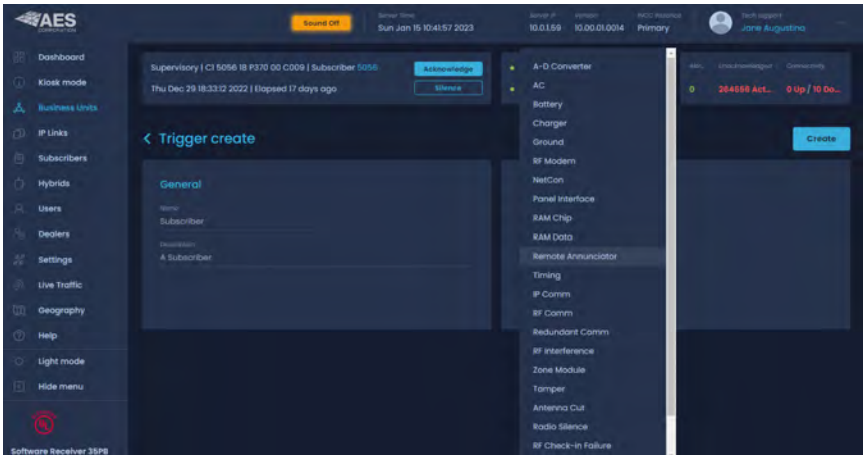
Once a trigger has been selected, the **Name** and **Description** fields on the left side of the screen automatically become populated.



3. From the **type** dropdown, select the fault criteria to be reported.

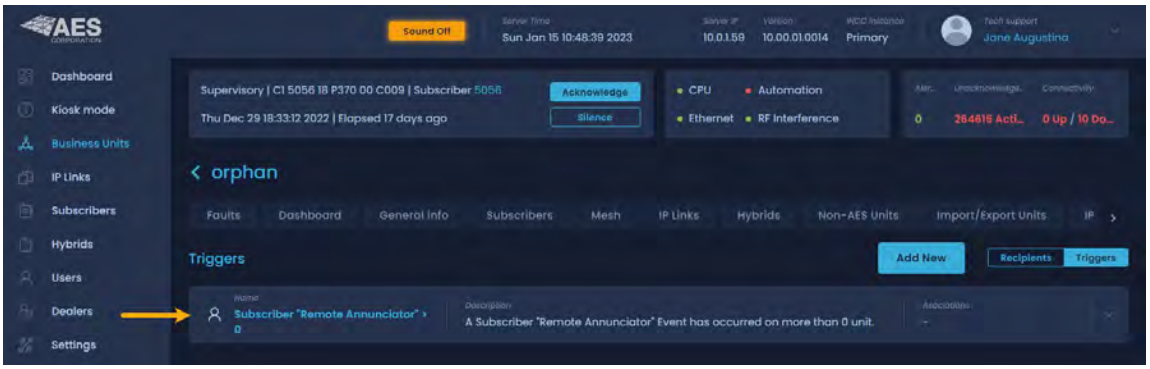


Important: Only the **Subscriber Event** and **IP Link Event** triggers have an additional dropdown. The triggers for **Network Health Score** and **IP/Hybrid Traffi**c do not rely on data associated with faults.

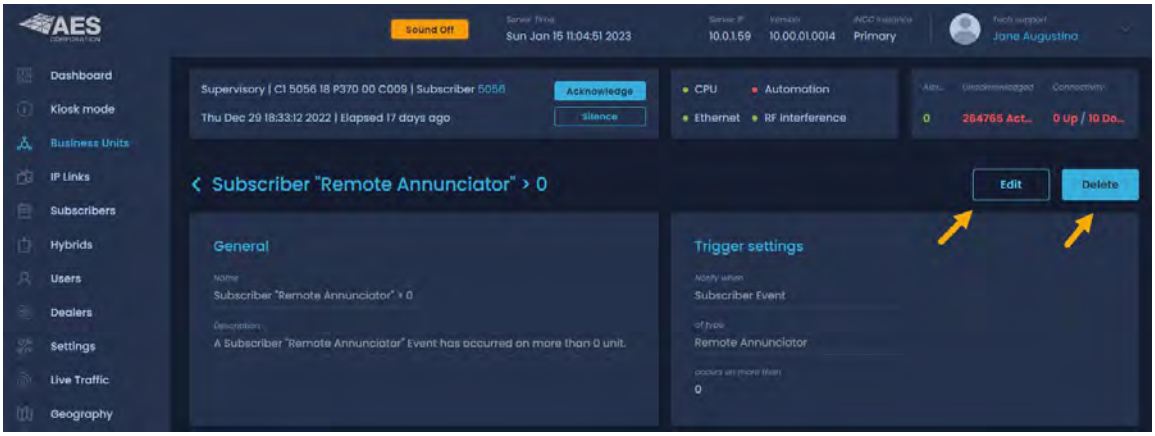


4. When finished, click **Create**.

   Triggers are listed on the Triggers page.

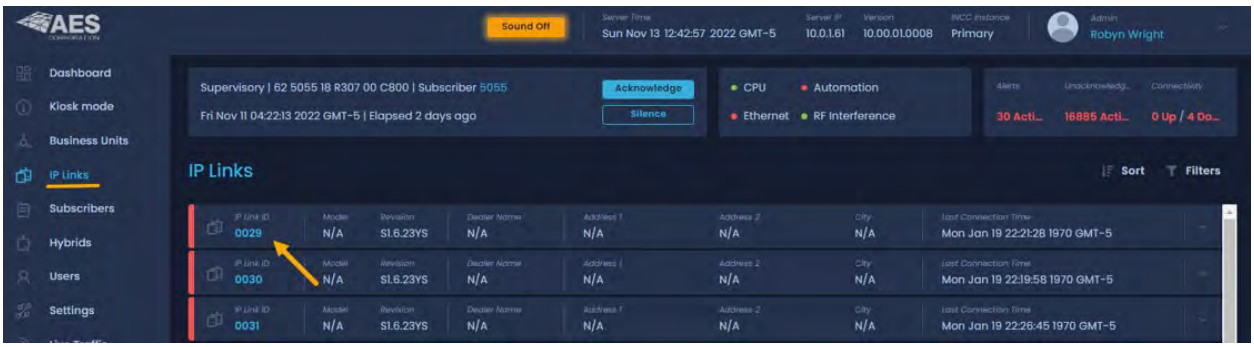


5. To edit or delete a trigger, click the trigger. The **Edit** and **Delete** butons are at the top right.



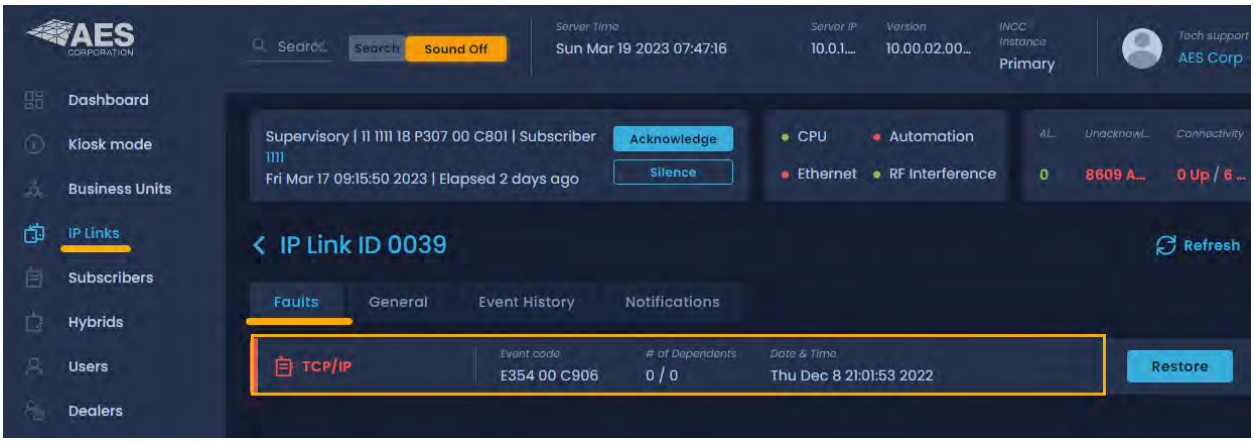
IP Links

IP Links displays a list of all IP Links on the system. Active links are marked by a green bar, and offline links are marked in red. To view faults and general information for an IP Link, click the name of the IP Link.



Faults Tab

The Faults screen shows the type of fault, the event code, the number of dependents, and the date and time the event occurred.



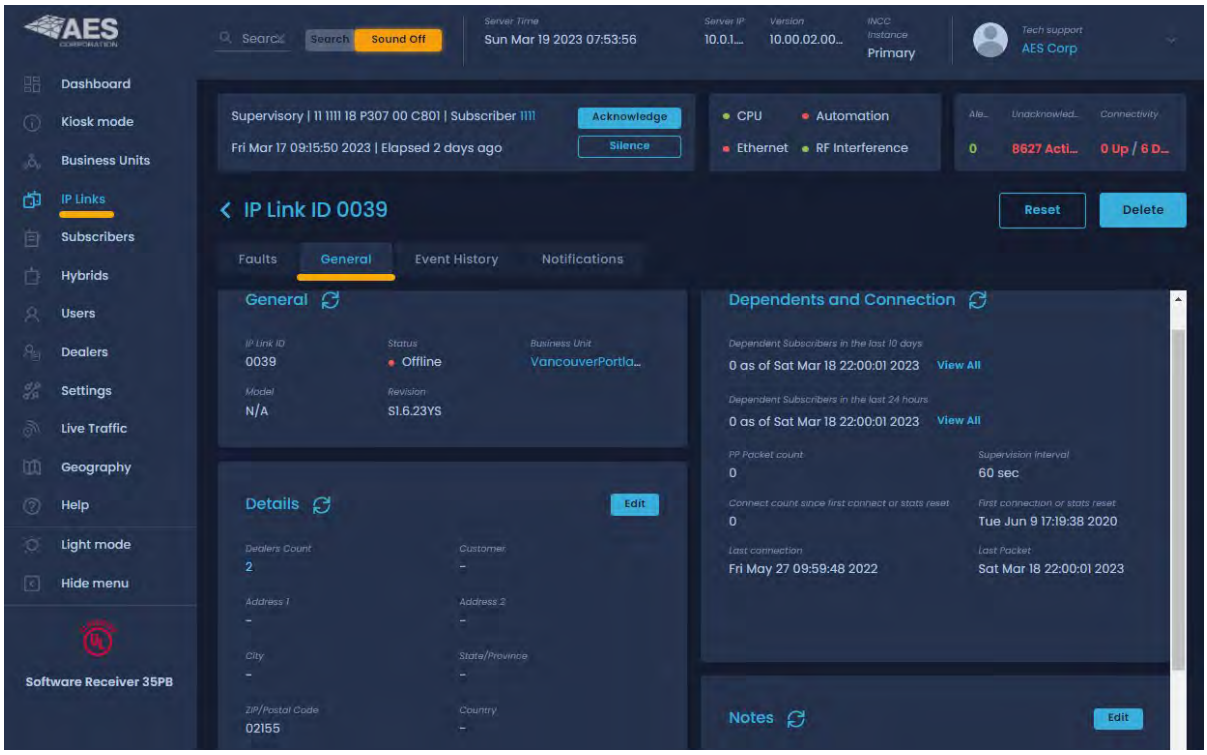
IP Link fault types include:

Fault Name	Event Code
A-D Converter	E307 00 C804
AC	E307 00 C912
Antenna Cut	E357 00 C916
Battery	E302 00 C911
Charger	E309 00 C910
Duplicate ID	E353 00 C906
Loopback	E307 00 C808
NVRAM Battery	E307 00 C803
PSTN Modem	E354 00 C908

Fault Name	Event Code	
Radio Silence	E355 00 C906	
RAM Clip	E307 00 C807	
RAM Data	E307 00 C802	
RF Interference	E350 00 C906	
RF Modem	E307 00 C805	
RF Offline	E354 00 C907	
Tamper	E145 00 C906	
TCP/IP	E354 00 C906	*See example above*
Timing	E307 00 C806	

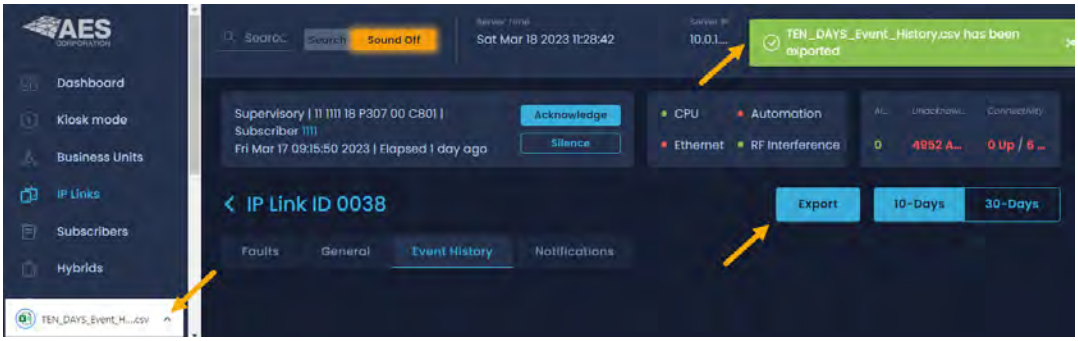
General Tab

- **General**: Displays the IP Link ID, status (online/offline), Business Unit affiliation, model, and software version.
- **Details**: Provides details on the IP Link dealer, geographic location, and installed antenna.
- **Dependents and Connection**: Displays IntelliNet subscribers that have used the IP Link. Other message packet-related statistics are also displayed.
- **Notes**: Information on the IP Link can be stored here in free form text.



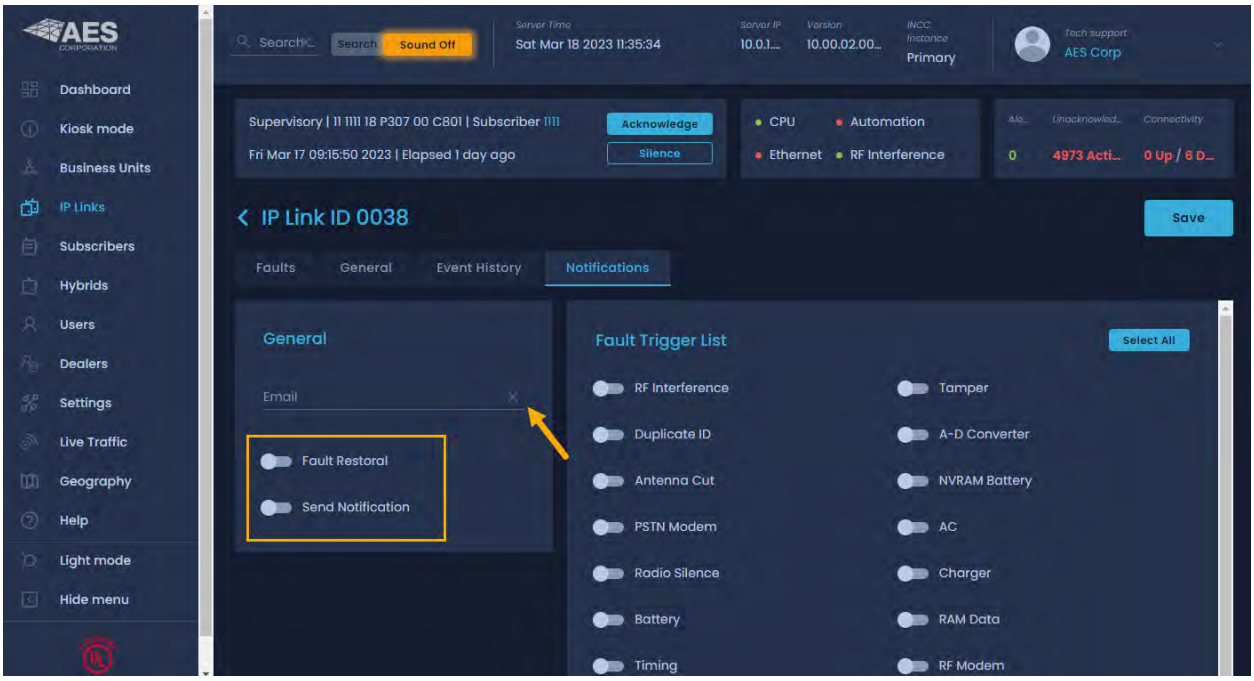
Events History Tab

Event history enables users to receive a 10- or 30-day event history. Click **Export** to download a CSV file.



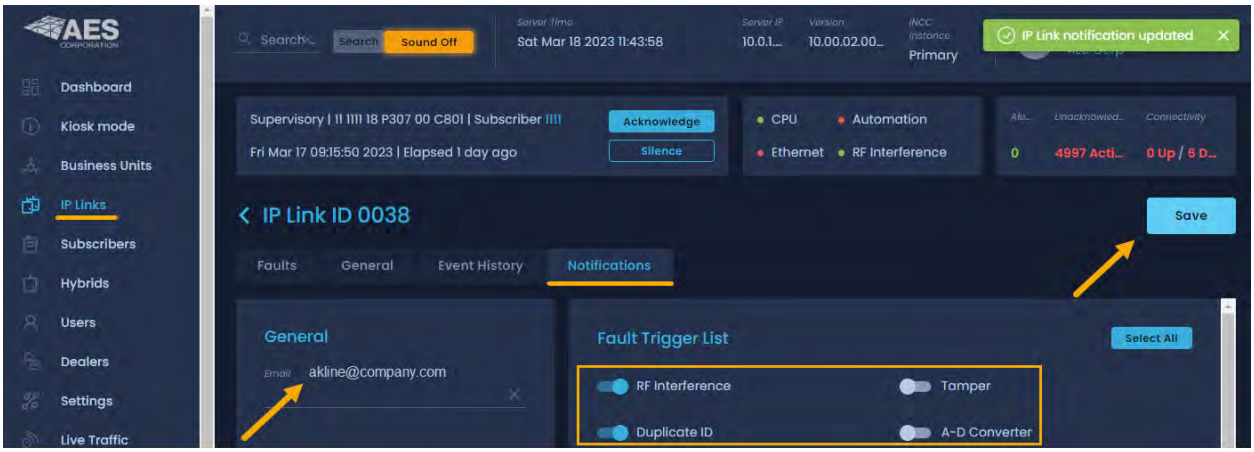
Notification Tab

The Notification function enables users to monitor their INCC network from anywhere, anytime. Users can configure automatic alerts based on a fault with any subscriber or IP Link.



Activating Notifications

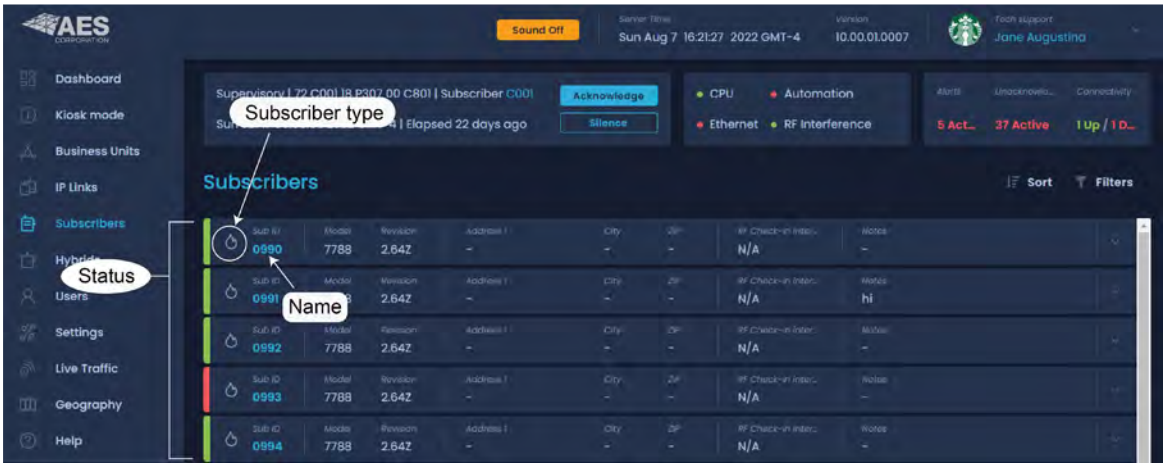
1. Define the fault criteria by clicking the fault(s) from the list of faults at the right.
2. Enter the email address of the user monitoring these triggers.
3. Click **Save**.



Subscribers

Subscribers automatically appear in the subscriber view once signals are sent to the AES IntelliNet network (subscribers do not need to be manually added).

- The status of a subscriber is indicated by the green and red vertical lines to the left of each row.
- Subscriber types include fire/burg products (please see the AES website for full list of AES supported products by the INCC).



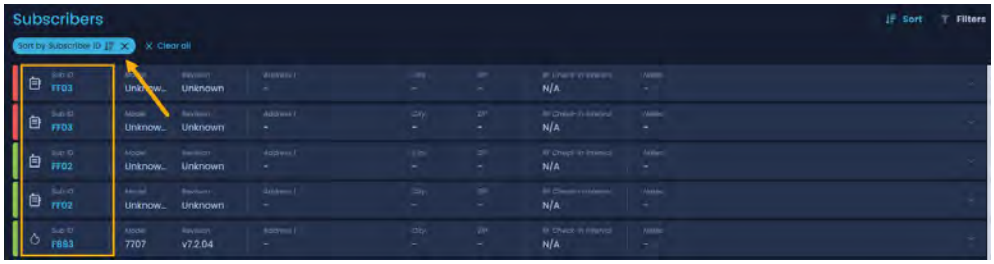
Sorting and Filtering

Subscribers can be sorted and filtered from the dashboard.

- To sort, click **Sort** to display the sorting options, then select your criteria and click **Ok**. The selected sort criteria is displayed at the top left of the list of subscribers.

Sort selection

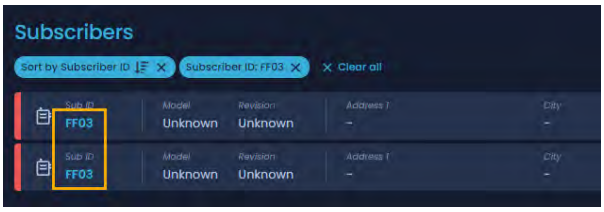
Result



- To filter out some of the subscribers, click **Filter**, then enter your data into the desired filtering fields. Click **Apply Filters** at the bottom right.

Filter selection

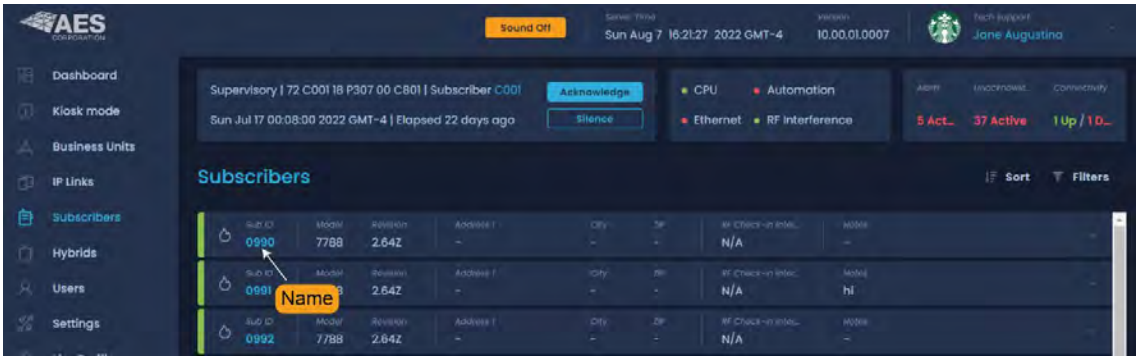
Result



Note: Filters can be cleared using either **Clear all** from the subscriber dashboard (shown above) or **Reset Filters** from the Filters dropdown (shown at left).

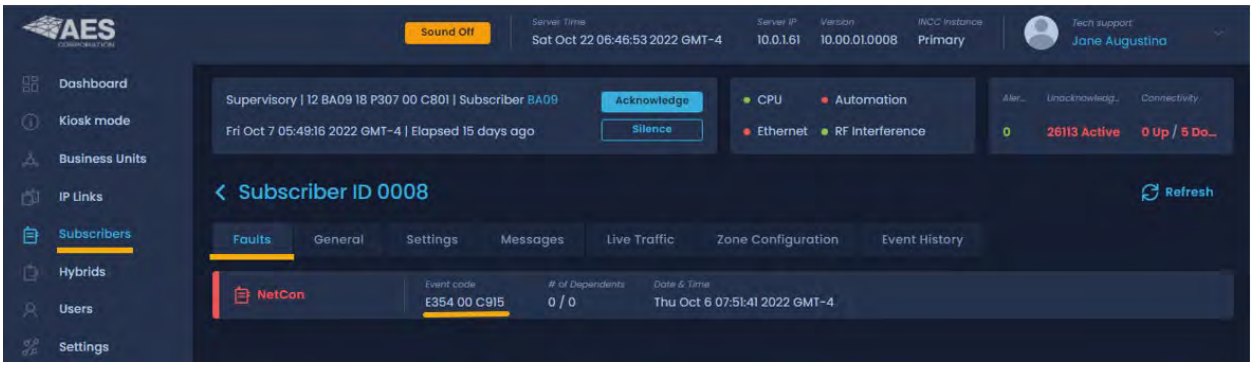
Viewing Subscriber Details

Click the name of the subscriber to view subscriber details (e.g., faults, general, settings, messages, live traffic, zone configuration, and event history).



Faults Tab

The Faults view shows the type of fault, the event code, the number of dependents, and the date and time the event occurred. The Faults view can simplify planning for routine service of subscribers, enabling it to be scheduled cost effectively within normal workflows.

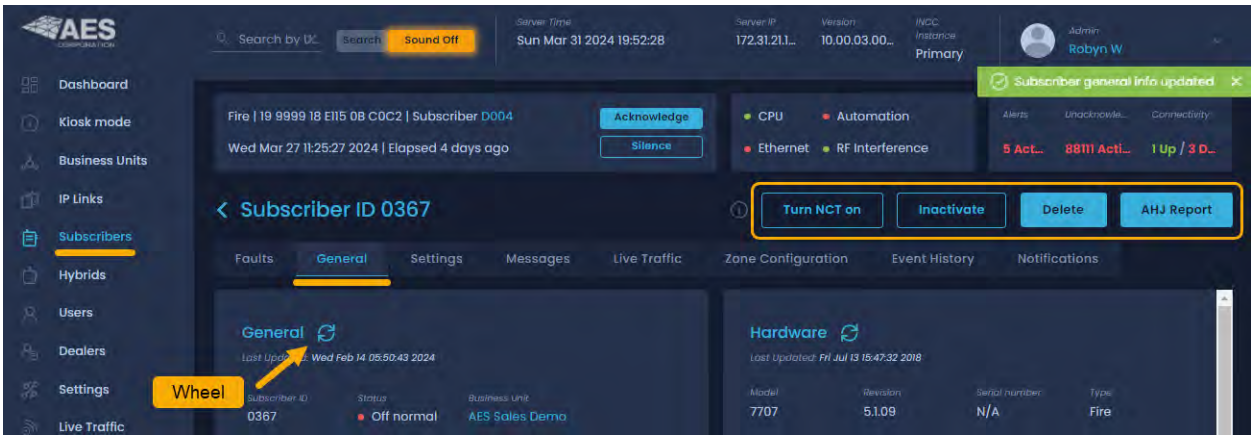


Subscriber fault types include:

Fault Name	Event Code
A-D Converter	E307 00 C804
AC	E307 00 C809
Antenna Cut	E357 00 C916
Battery	E307 00 C801
Charger	E370 00 C009
Ground	E370 00 C010
IP Check-in Failure	E354 00 C902
IP Comm	E356 00 C904
Loopback	E307 00 C808
NetCon	E354 00 C915
Panel Interface	E307 00 C815
Radio Silence	E355 00 C906

Fault Name	Event Code
RAM Chip	E307 00 C807
RAM Data	E307 00 C802
Redundant Comm	E350 00 C915
Remote Annunciator	E307 00 C813
RF Check-in Failure	E354 00 C906
RF Comm	E356 00 C903
RF Interference	E350 00 C906
RF Modem	E307 00 C805
Tamper	E145 00 C906
Timing	E307 00 C806
Zone Module	E307 00 C817

General Tab (Buttons and Icons)



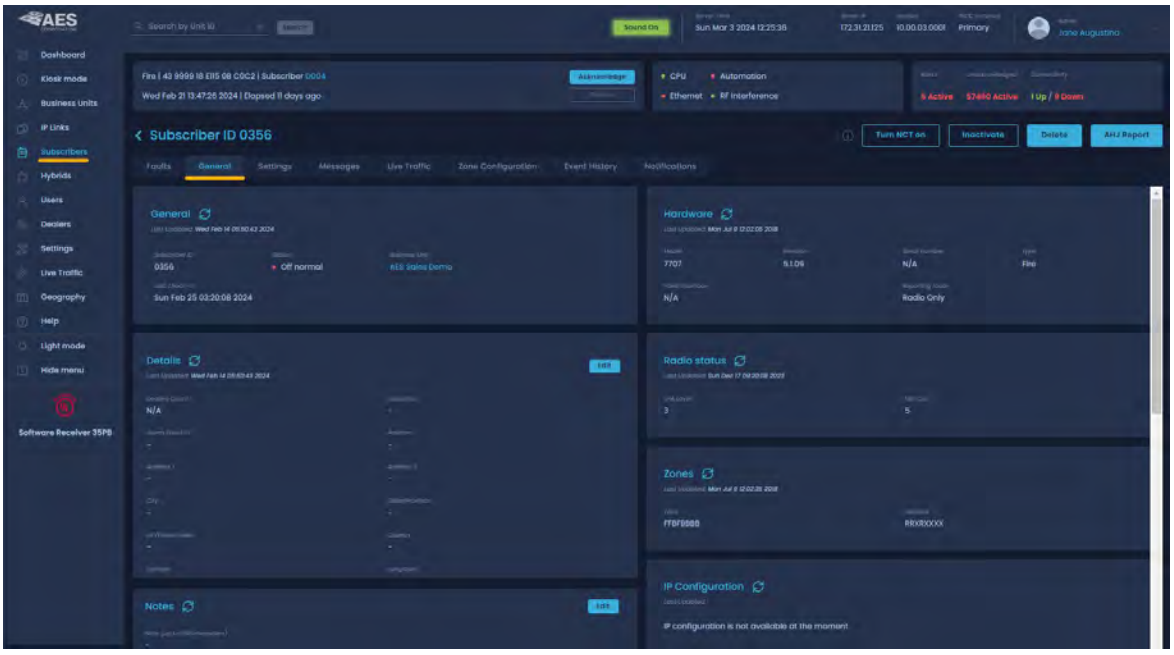
Descriptions of Buttons and Icons	
Refresh (wheel) icon	If the refresh icon is clicked, the INCC pings the subscriber with an outbound request for the most recent information. The green callouts at the top right indicate that the request has been acknowledged (first image). As the subscriber information is updated, notifications appear at the top right (second image).
Turn NCT on	Assigns a subscriber/hybrid as inactive to prevent impacting the network health score. Once **Turn NCT on** has been enabled, the subscriber ID is removed from all business unit dashboard calculations (e.g., signals and health score), and signals are no longer sent to the dashboard page or alarm automation. This tool is for setting up subscribers only.
Inactivate	Inactivates the subscriber ID.
Delete	Deletes the subscriber ID.
AHJ Report	Submits a request to receive an AHJ report via email within minutes. For a sample of the report, see Authority Having Jurisdiction (AHJ) Report.

As subscriber information is updated, notifications appear at the top right (green box).

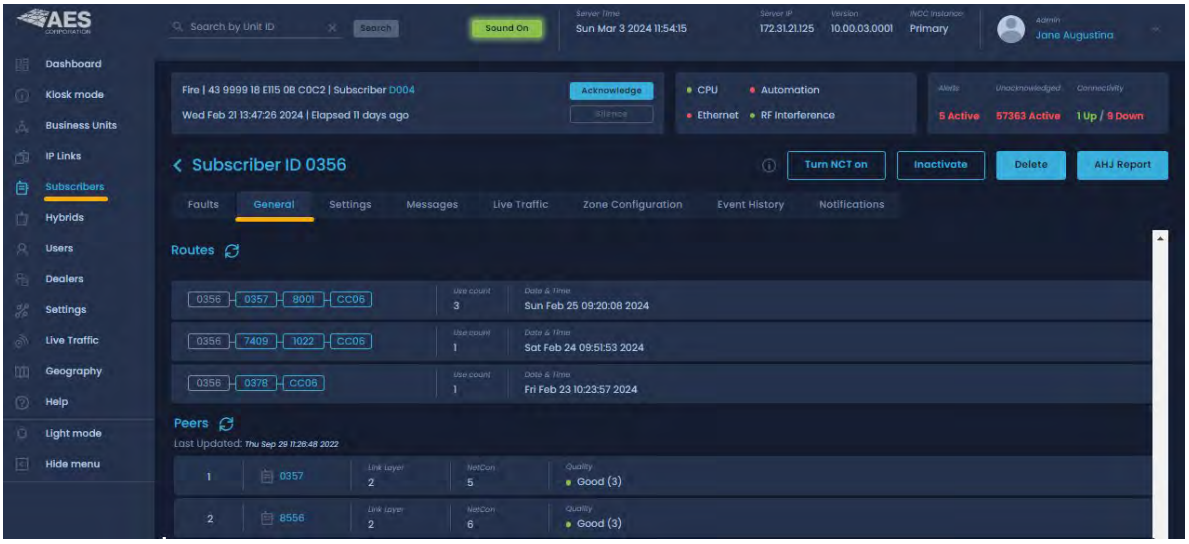
General Tab (Settings)

The General tab provides access to the following information:

- General – Subscriber ID and business unit affiliation.
- Details – Information on the dealer and location of the subscriber.
- Notes – A space for adding free-form text about the subscriber.
- Hardware – Subscriber model and panel interface information.
- Radio Status – Link layer and NetCon information.
- Zones – Zone and restoral status information.
- IP Configuration – Information on the IP configuration associated with the subscriber. The IP Configuration pane displays the IP addresses and ports for the primary and secondary receiver, as well as the MAC address of the primary server and the business unit group that the subscriber belongs to. For reporting routing, 2.0 subscribers can deliver signals using five different reporting options (legacy subscribers are limited to radio only).
  - Radio Only
  - Radio and Internet
  - Radio and Internet Backup
  - Internet and Radio Backup
  - Internet Only



- Routes – A total of four display screens are available to show the routing table. Up to eight peers, subscribers, or IP Links may be listed in the table. Each screen displays two subscribers. The total number of display screens varies depending on the total number of peers listed (a number from 1 to 8). Press the MENU button once to advance to the next routing table screen.



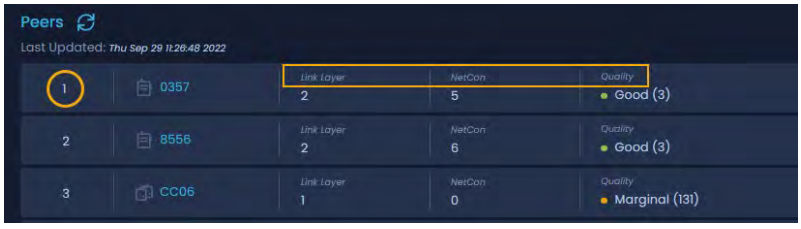
- Peers – Displays all subscribers in communication with the subscriber. Peers are pulled from the AES mesh packet structure. The INCC lists up to eight peers. A peer is any subscriber or IP Link that can communicate with a single path from a single subscriber.

  Routing Table ID#: A routing table lists up to eight other subscriber ID#'s or IP Links. The purpose of the list is to select a peer for passing off data packets. The table is sorted with the best quality subscriber placed at preference location 1 (see image below). Quality is a measure of the neighbor subscriber's ability to pass data packets.

  – L: Link Layer as reported by last transmission from the peer ID# shown.

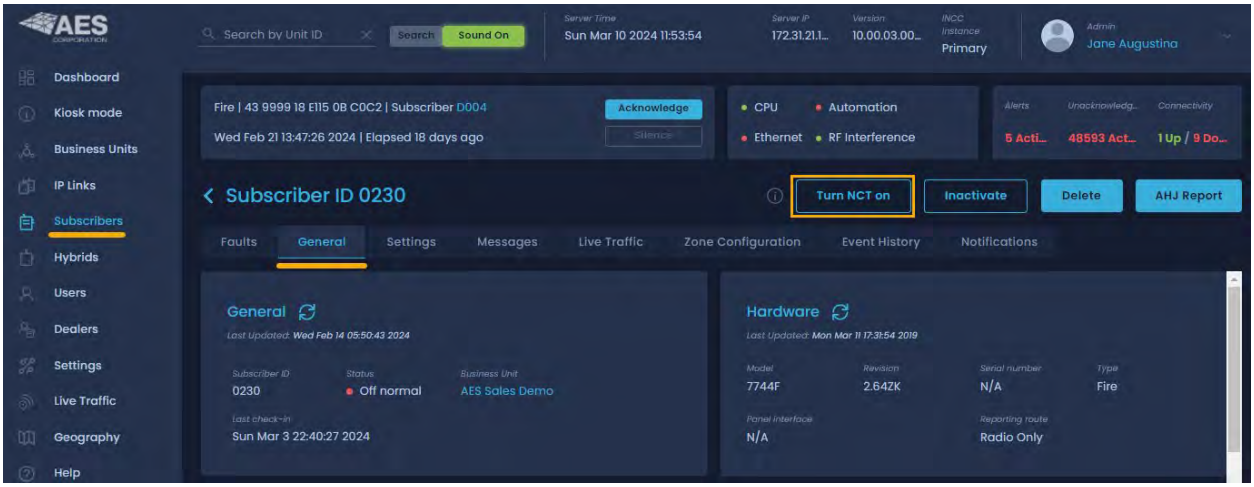
  – N: NetCon (NETwork CONnectivity) – An internal rating used in the automatic positioning of this unit in the network. A NetCon value of 5 is required for a subscriber that is compliant with UL-864, 10th Edition.

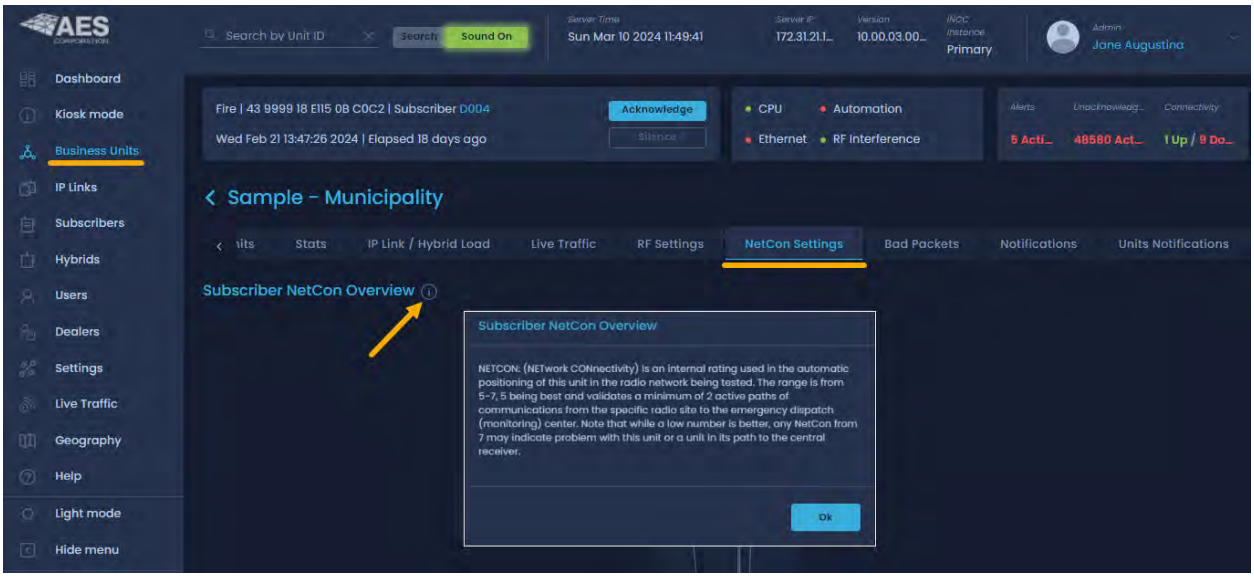
  – Q: Signal Quality – The first digit is either an 8 or a 0 (zero). The second digit is a measure of how old the data is (a 3 is assigned to the newest data; a 1 is assigned to older data). Routing preference is given to strong, recently heard subscribers (3) versus weaker subscribers heard a long time ago (131).



Turn NCT on

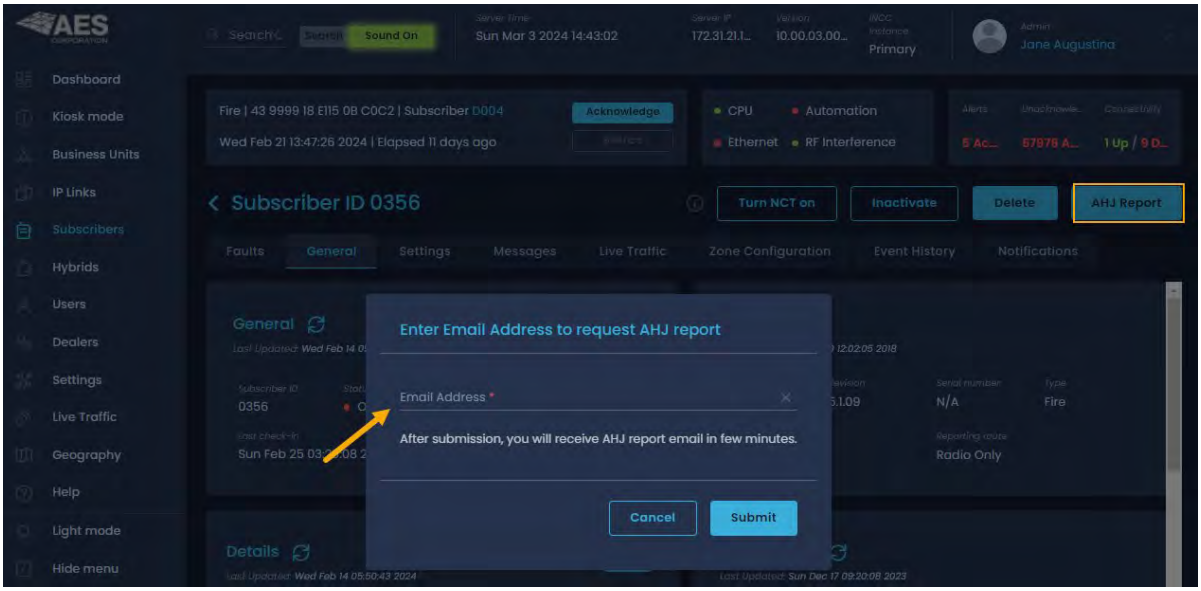
- Navigate to the subscriber page (General tab) and enable NCT mode.
- Once enabled, the subscriber ID will be removed from all business unit dashboard calculations (e.g., signals and health score), and signals will no longer be sent to the dashboard page or alarm automation.



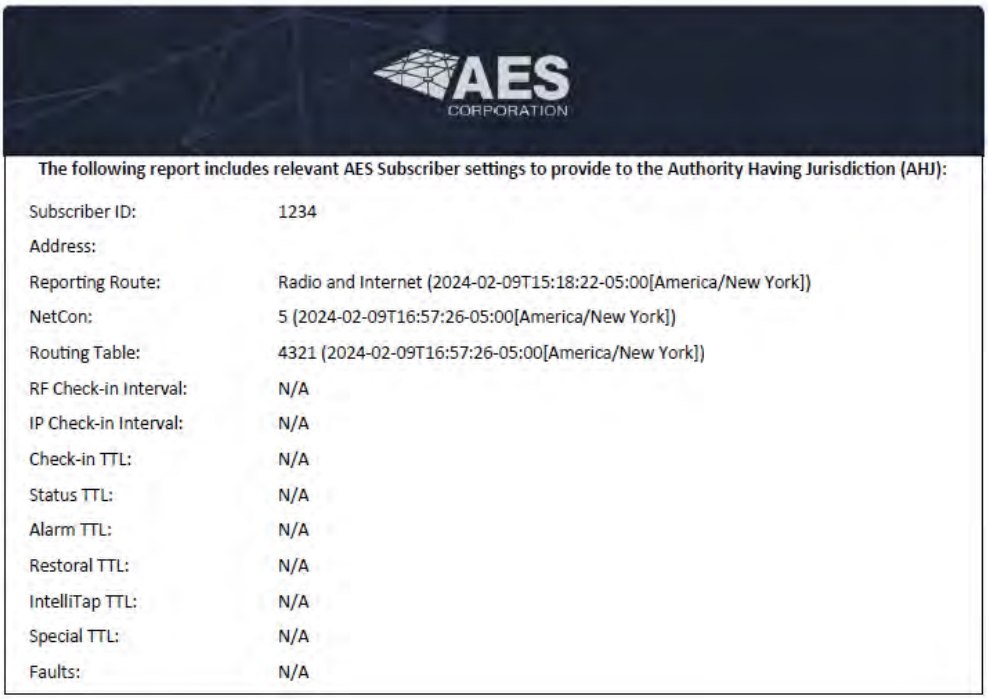


Authority Having Jurisdiction (AHJ) Report

The AHJ (Authority Having Jurisdiction) report includes relevant AES subscriber settings to provide to the AHJ. To request a copy of the report, navigate to the subscriber's General tab, click the **AHJ Report** button, then enter an email address.



A sample of the AHJ report is shown below:



The following report includes relevant AES Subscriber settings to provide to the Authority Having Jurisdiction (AHJ):

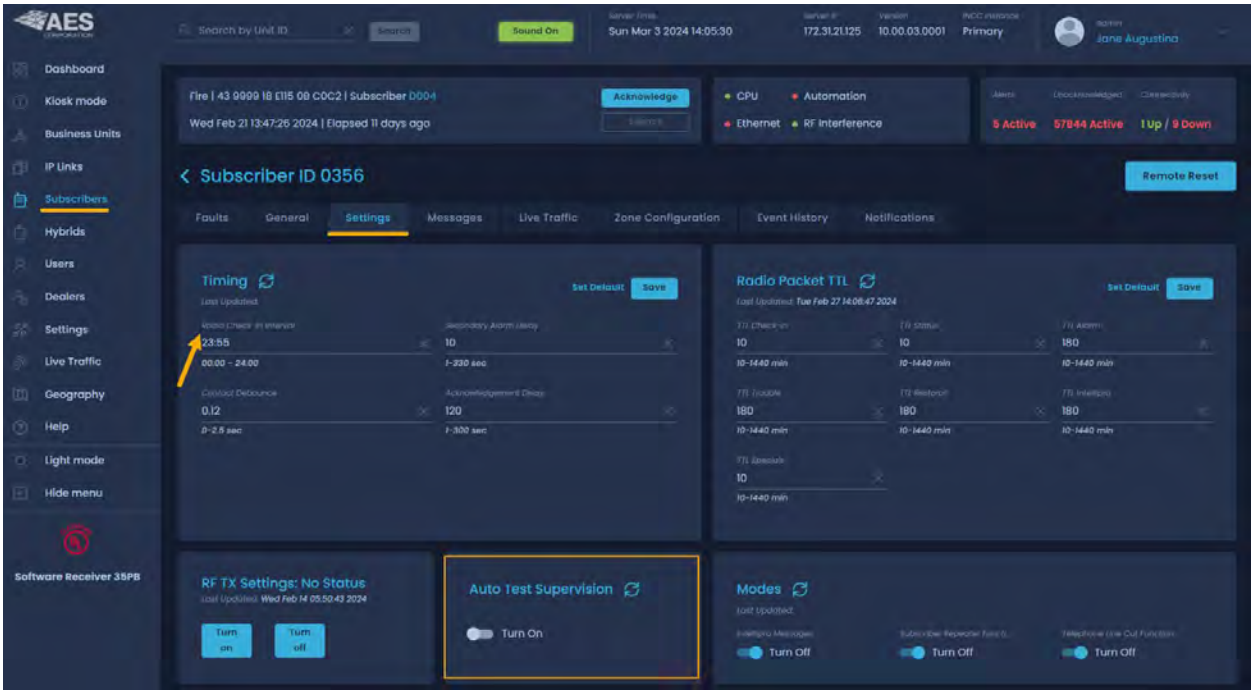
Subscriber ID:	1234
Address:	
Reporting Route:	Radio and Internet (2024-02-09T15:18:22-05:00[America/New York])
NetCon:	5 (2024-02-09T16:57:26-05:00[America/New York])
Routing Table:	4321 (2024-02-09T16:57:26-05:00[America/New York])
RF Check-in Interval:	N/A
IP Check-in Interval:	N/A
Check-in TTL:	N/A
Status TTL:	N/A
Alarm TTL:	N/A
Restoral TTL:	N/A
IntelliTap TTL:	N/A
Special TTL:	N/A
Faults:	N/A

Settings Tab

The **Settings** tab provides access to the following information:

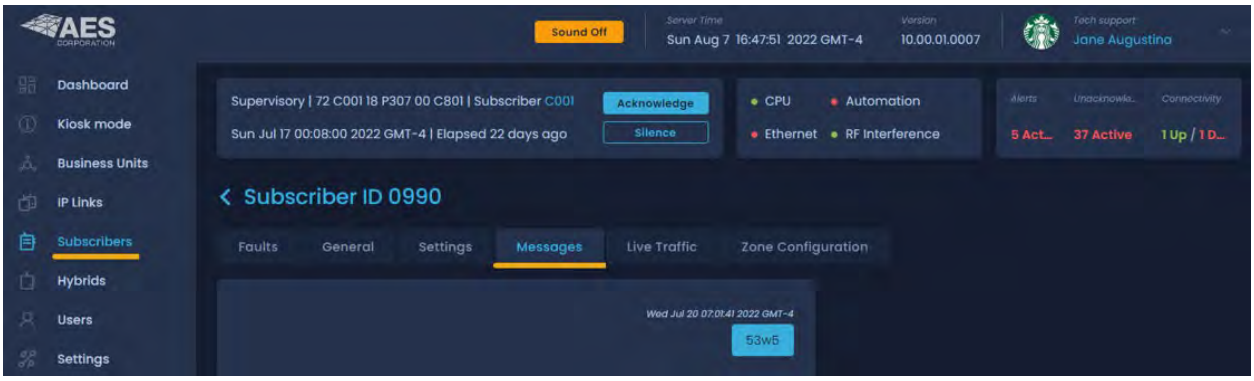
Timing	Radio check-in interval, communication timeout delay, secondary alarm delay, and acknowledgement delay settings
RF TX Settings	Allows RF transceiver turn on and off
Radio Packet TTL	Packet time to live settings
Modes	On/off status for IntelliTap messages, subscriber repeater function, and telephone line card function

The **Auto Test Supervision** setting enables the INCC to monitor automatic test timer check-ins. When enabled, it alerts an operator if a subscriber unit fails to check in within the programmed interval, plus 10% + 2 minutes as programmed in the subscriber's timing parameters function (see the **Radio Clock in interval** setting in the image below). A missed check-in is reported to alarm automation if the Auto Test Supervision is enabled.



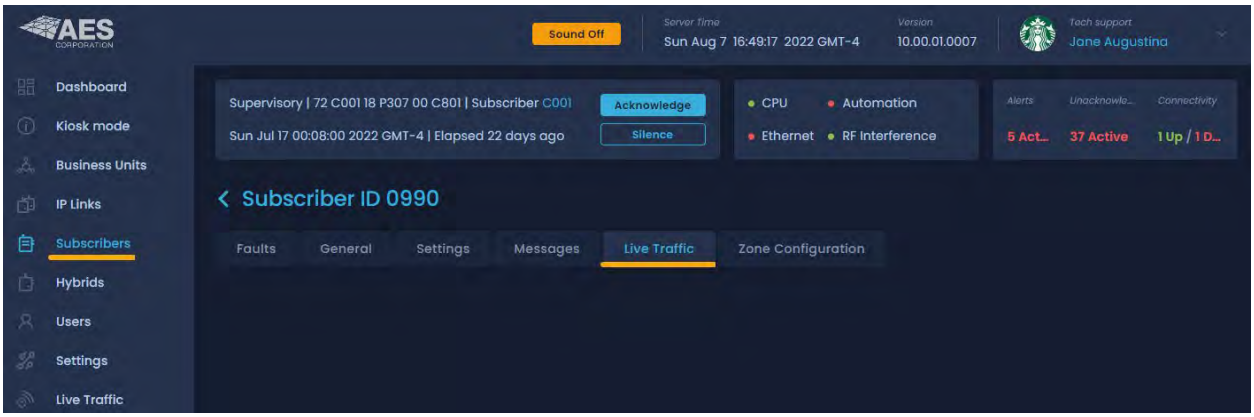
Messages Tab

The **Messages** tab provides an interface for sending a text message to a subscriber configured to receive text messages.



Live Traffic Tab

The **Live Traffic** tab provides information on the type of message traffic and details about the subscriber traffic.

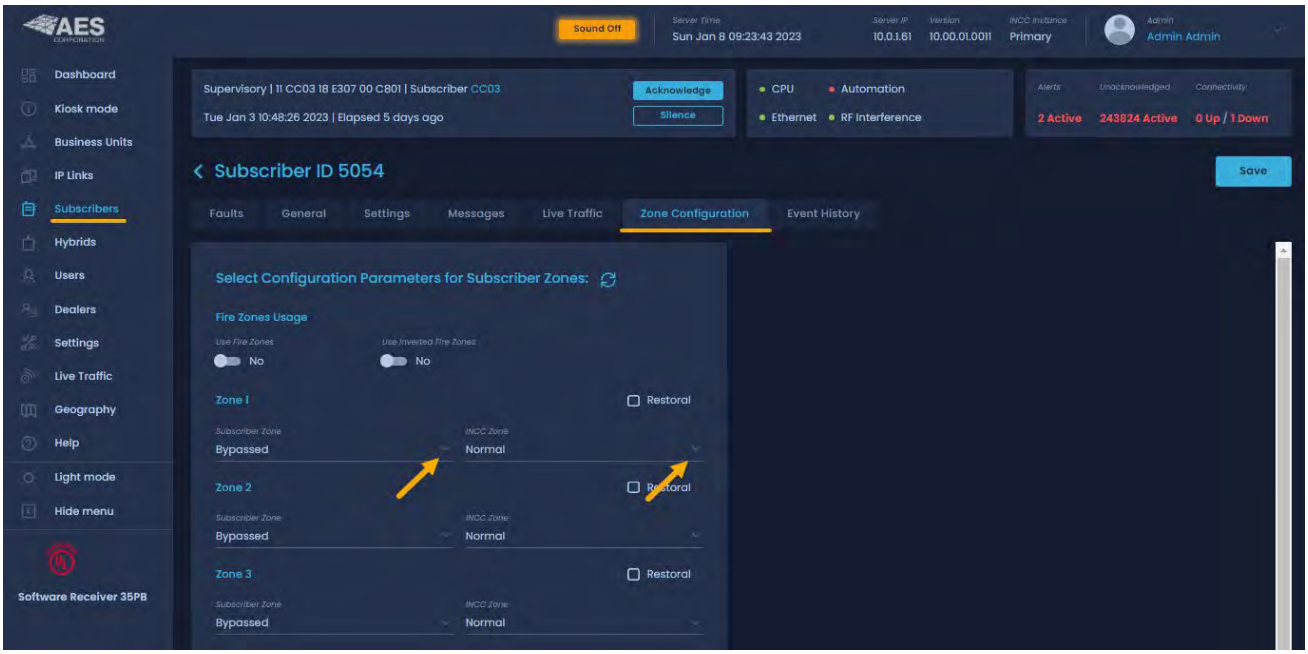


Zone Configuration Tab

The **Zone Configuration** tab allows for subscriber zone assignment. Zone usage is account or ID specific and enables users to receive a 10- or 30-day event history, including CID events that are set by a subscriber.

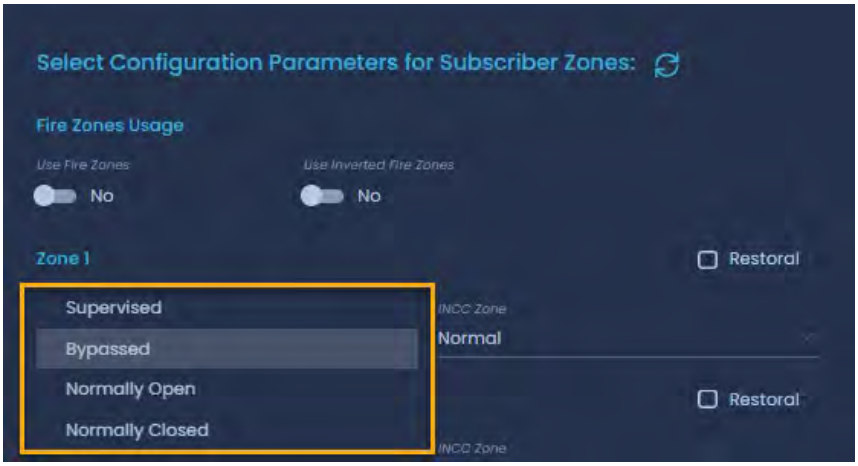
Following is a list of INCC fault statuses and trouble zone assignments that can be used during configuration. This information helps to explain or clarify received messages. You can also use this information to create templates in your alarm automation specifically for subscribers. (These AES custom codes can be found in the CID document on the AES website.)

Fault Statuses	Description	Event Code
918	Symmetric Failure Between Primary & Secondary.	E307
919	Hard-disk Full.	E623
920	IP Compromise, Duplicate IP Packets Detected.	E145
921	Peer IP Ping Failure.	E997
922	CPU Trouble	E307
923	Memory Issue.	E307

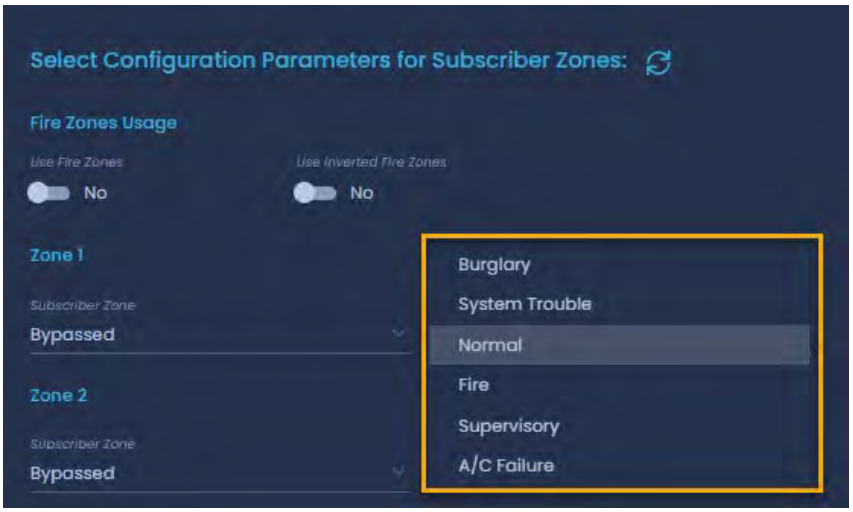


To configure the parameters for subscriber zones:

1. Click the **Subscriber Zone** dropdown and select from the following options:
    - Supervised
    - Bypassed
    - Normally Open
    - Normally Closed

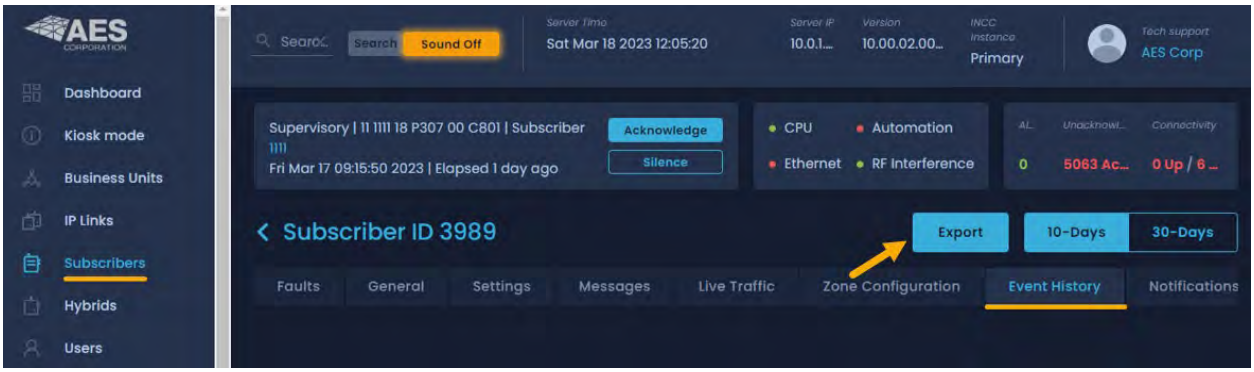


2. Click the **INCC Zone** dropdown, and select from the following options:
    - Burglary
    - System Trouble
    - Normal
    - Fire
    - Supervisory
    - A/C Failure



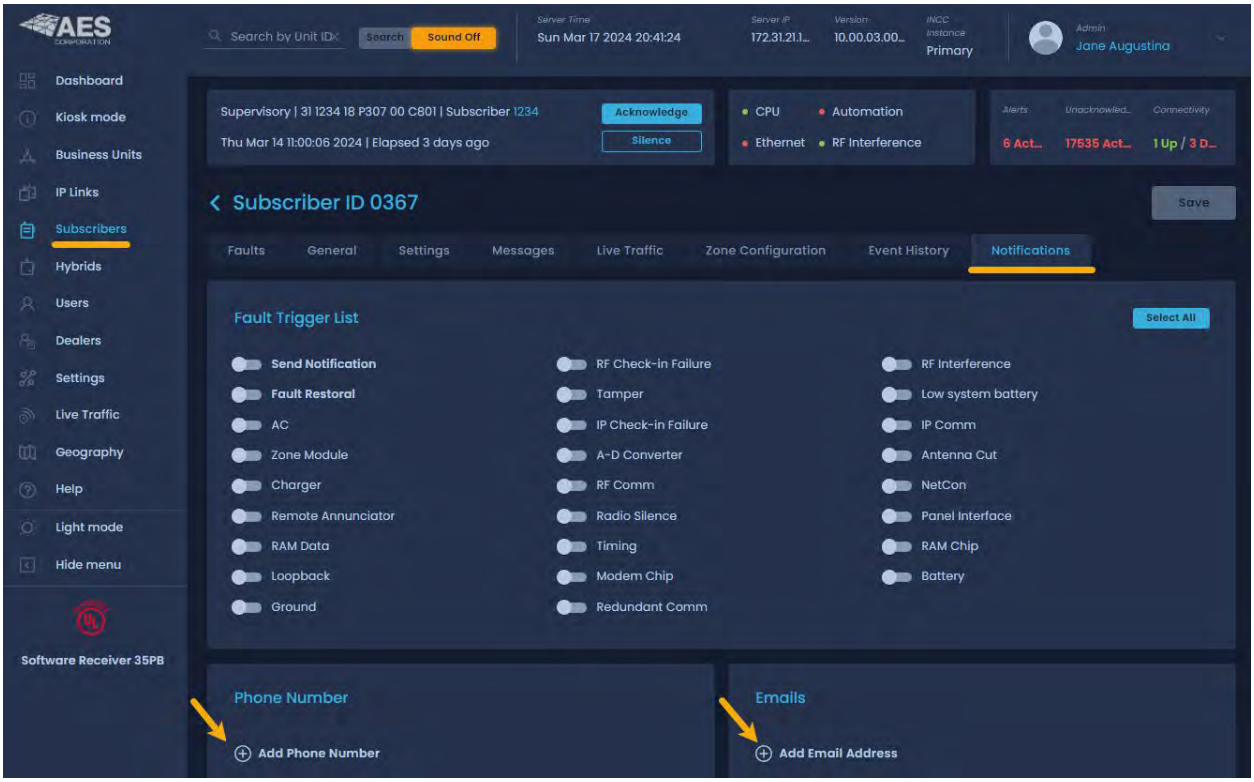
Event History

Event history enables users to receive a 10- or 30-day event history, including CID events that are set by a subscriber. Click **Export** to download a CSV file.



Notifications

The Notifications tab displays a list of fault triggers. To add a phone number, select the carrier (the carrier will depend on which server is used for sending messages to the phone), then enter a phone number.

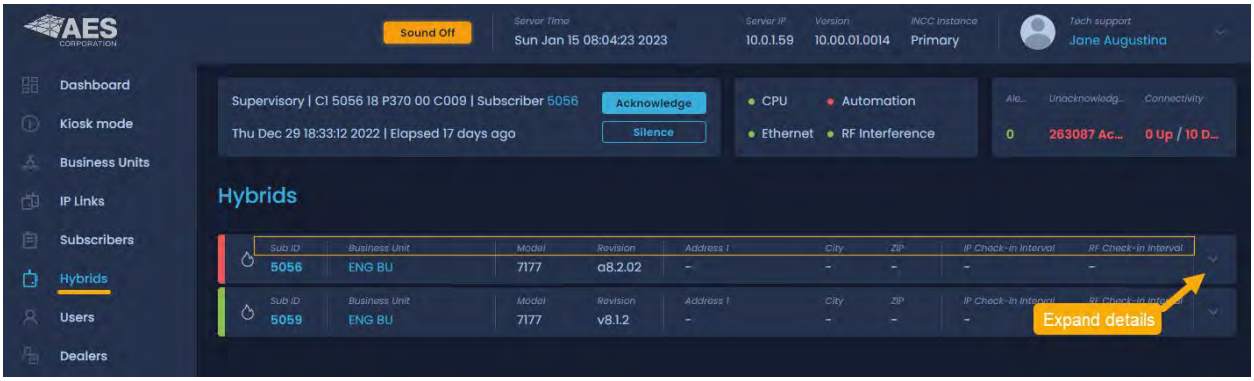


Hybrids

The Hybrids tab displays a list of all hybrid subscribers associated with a business unit. Each hybrid displays general information about the unit.

- Sub ID
- Model
- Revision
- Address
- RF check-in interval
- Notes (text entry)

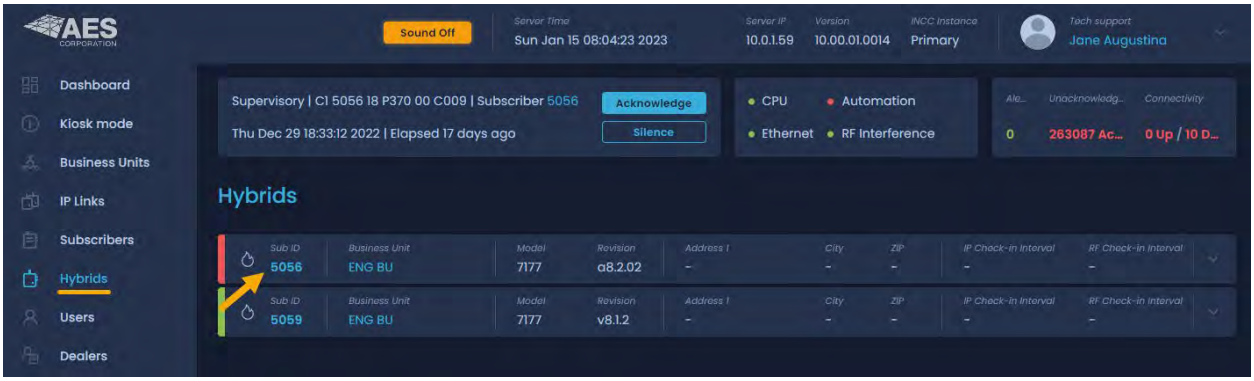
A hybrid is a fire unit with the ability to switch to IP and act as an IP Link, enabling the unit to send an alarm from the customer premises to the central monitoring station (CMS) via RF and/or IP and transmit peer signals via IP.



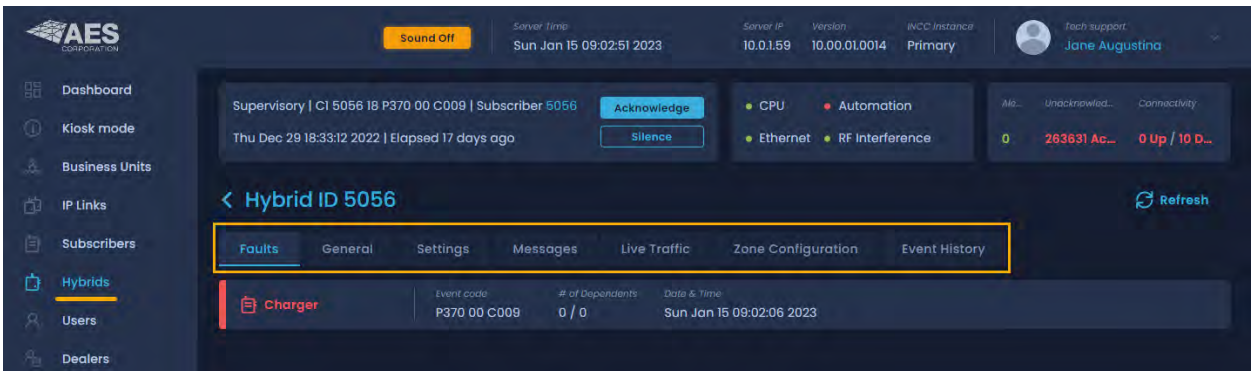
To expand the details for a hybrid, click the dropdown at the right. The additional information includes:

- Status
- Business unit
- Current faults
- Last check-in
- Alarm panel ID
- Dealer name
- Customer
- Comm timeout delay
- Check-in TTL
- Status TTL
- Alarm TTL
- Trouble TTL

To view the details about a specific unit, click the name of the hybrid.



Hybrid units share the same settings as subscribers. For configuration details, go to Viewing Subscriber Details.

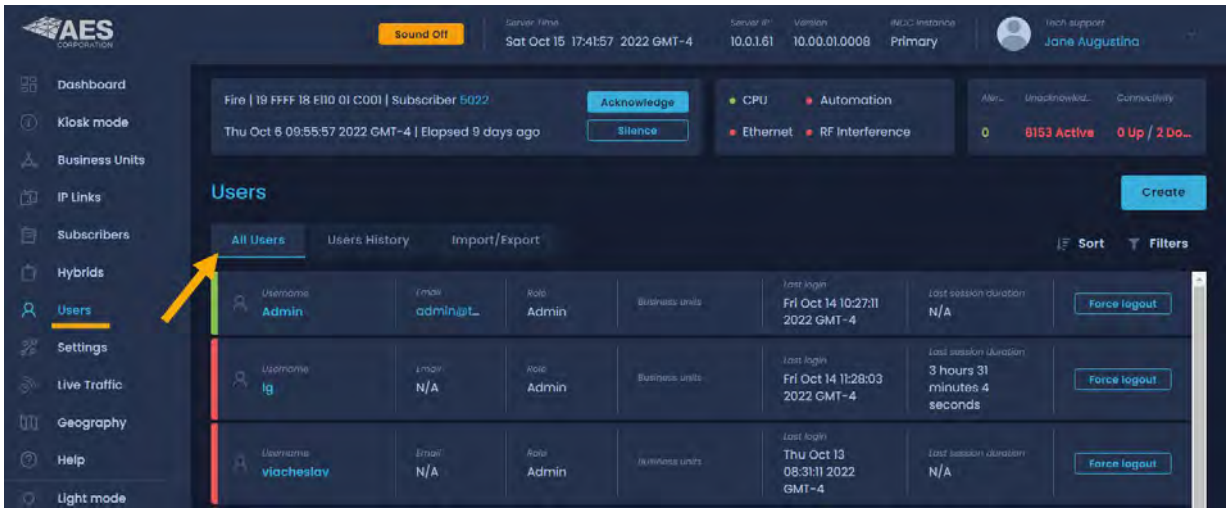


Users

All Users Tab

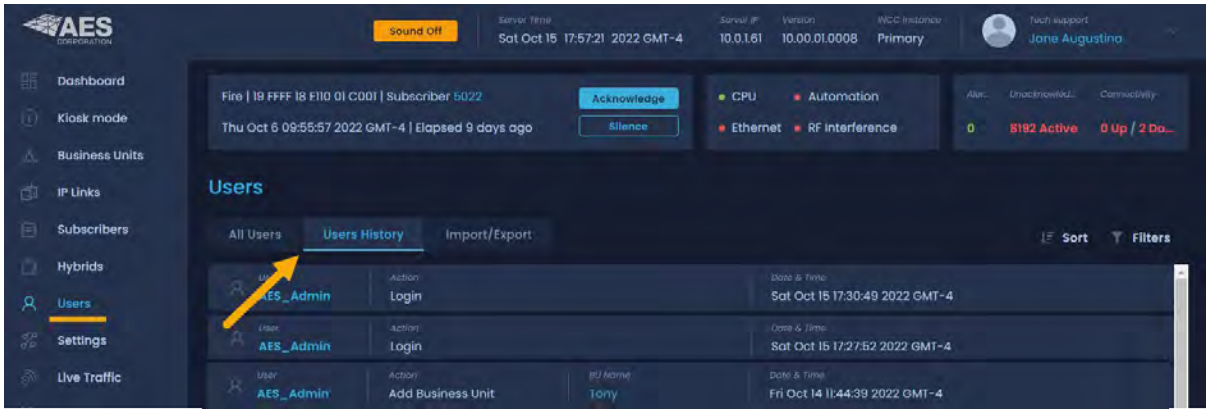
The **All Users** tab displays general information about users who have access to the INCC software. It also shows when a user last logged on and the length of the session. The **Force logout** button allows you to log a user out:

- *Username*: The red/green color coding to the left of the username indicates whether a user is logged on or off.
- *Email*: You can email a user by clicking the email link.
- *Role*: Tiers 1, 2, and 3.
- *Business units*: Indicates which business unit the user has access to.
- *Last login* and *Last session duration* provides login history.
- To log a user out of the INCC software, click **Force logout**.



Users History Tab

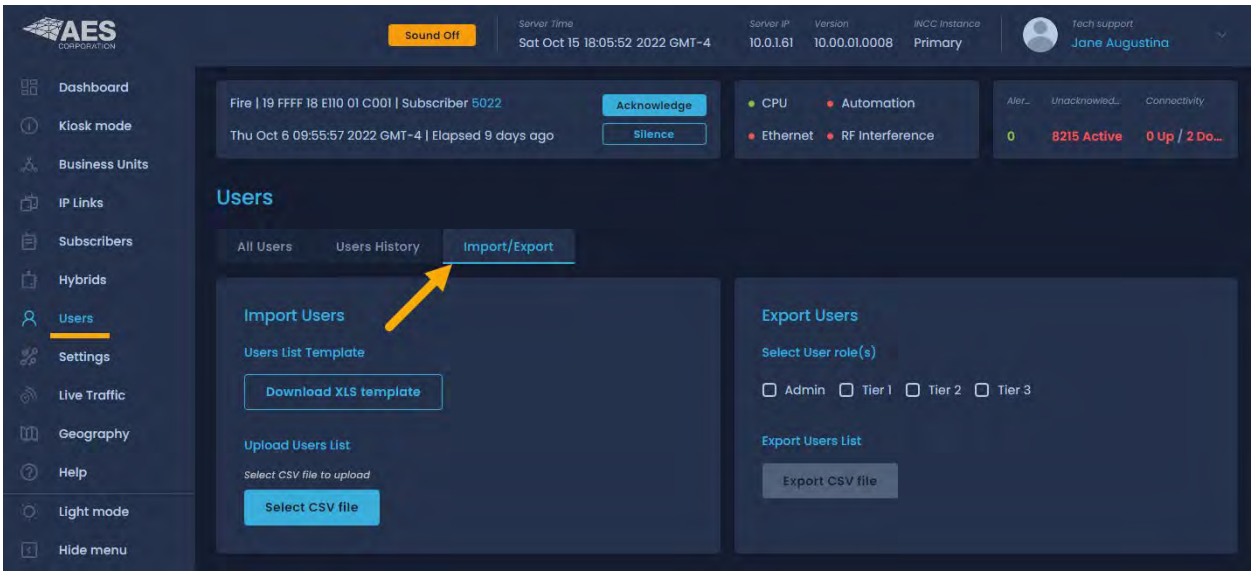
The **Users History** tab displays a list of actions the user performed (e.g., logging in, adding a business unit) and the date and time on which these actions occurred.



Import/Export Tab

To import a list of users:

1. Click **Download XLS template** to download the template.
2. Populate columns A through N in the template. Save the file.
3. Export the Excel file to CSV.
4. Upload the CSV file by clicking **Select CSV file**.



Export Users

To export user data:

1. Check each box next to the roles you would like to collect data for.
2. Click the **Export CSV file** button to download the file. The Excel file consists of the data that was selected:

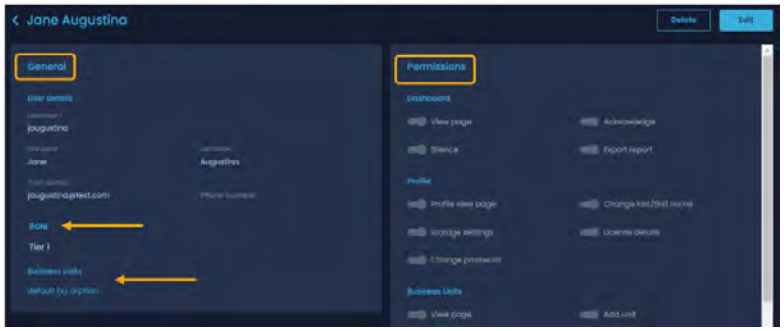
	A	B	C	D	E	F	G	H	I
1	Username,Role,Business Units,First Name,Last Name,Email Address,Phone Number,Subscribers								
2	ALARMCE	Tier 1	"ALARMCENTER"					32769 49153 32770 1638	
3	545 41552 25168 8784 41553 25169 8785 41554 25170 8786 41555 8787 25171 41556 8788 25172 4155								
4	006 48007 48008 48009 48016 48017 48018 48019 48020 48021 48022 48023 48024 48025 48129 4813								
5	jaugustina	Tier 1	"ALARMC	Jane	Augustina	jaugustina@test.cor		32769 49153 32770 1638	
6	77 41545 41552 25168 8784 41553 25169 8785 41554 25170 8786 41555 25171 8787 41556 8788 25172								
7	05 48006 48007 48008 48009 48016 48017 48018 48019 48020 48021 48022 48023 48024 48025 48129								
8	testt1	Tier 1	"ALARMCENTER" "BU1"						
9	testt2	Tier 2	"ALARMCENTER" "BU1"						
10	test_user	Tier 1	"BU1"						
11	AES Corp	Tier 1	"ALARMCENTER"					4096 2449 2450 4099 41	

View User Details

To view details about a specific user, click the username.

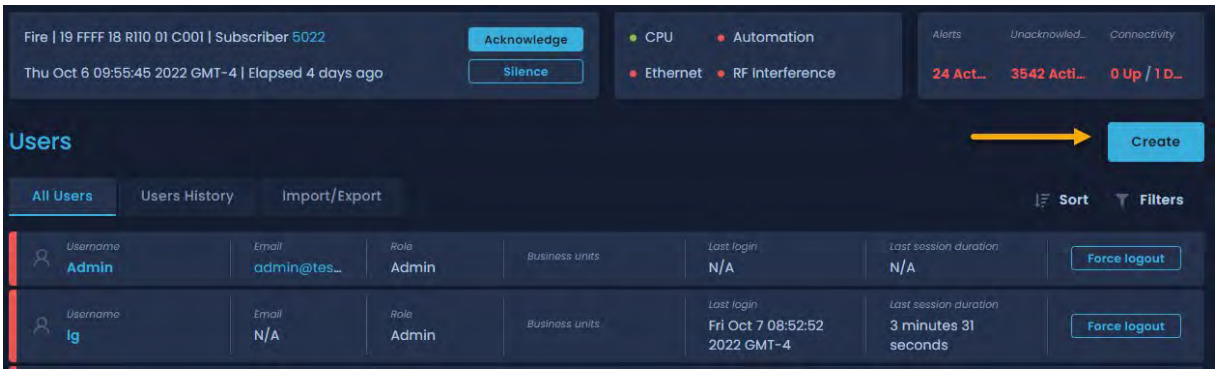
- General: Displays user details, the user's role, and the business units that the individual has access to.

1. Permissions: Contains a set of user-toggleable operations. Many of these operations are implemented as special permissions.



Create a User Account

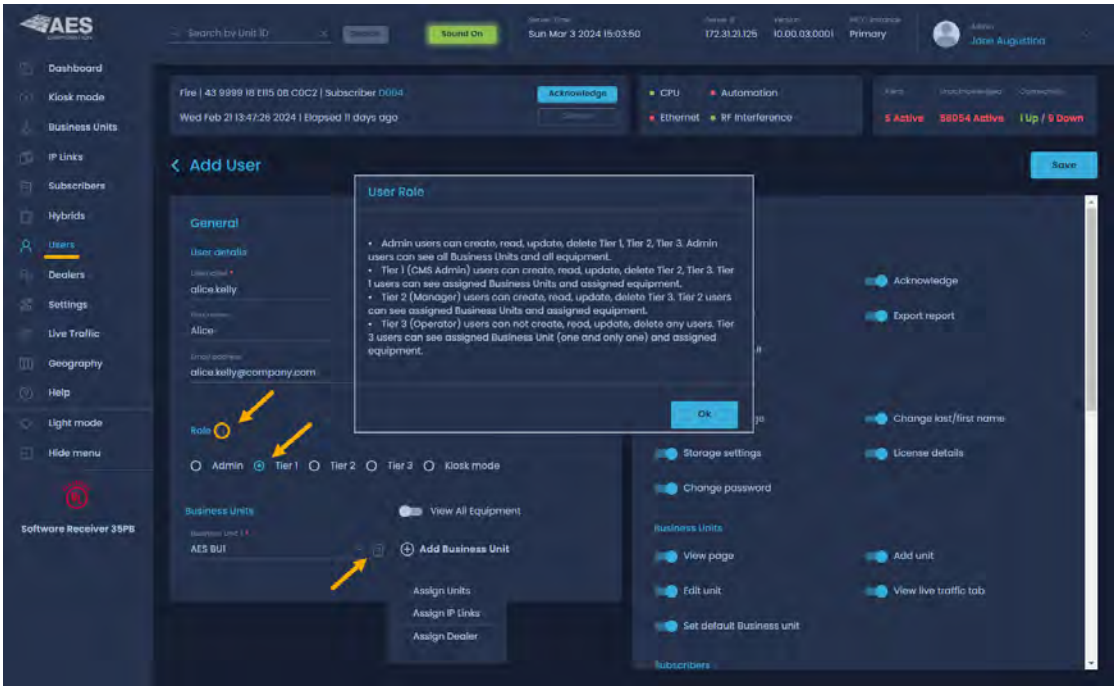
1. Click the **Create** button.



2. Fill out the user information and select a role.

   Note: Each user role provided by the INCC has a specific set of access. The actions associated with a user role were chosen to match the tasks that different team members may be responsible for. To view an overview of each role, click the **Role** icon.

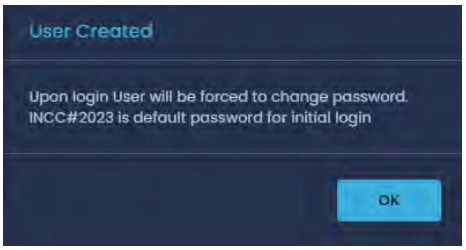
3. Add a business unit to the tier-level users by clicking **Add Business Unit** at the bottom left and selecting a business unit from the dropdown list.



4. To add subscriber(s) to the business unit, click the subscriber icon, as shown below, then select the subscribers that you would like to associate with this business unit.

5. When you are finished setting up the business unit, click **OK**.

6. When you're finished setting up the user account, click **Save** at the top right (see main image above). Once the user account has been saved, an onscreen message alerts you that the user will be forced to change the password upon initial login. INCC#2023 is the default password for the initial login.

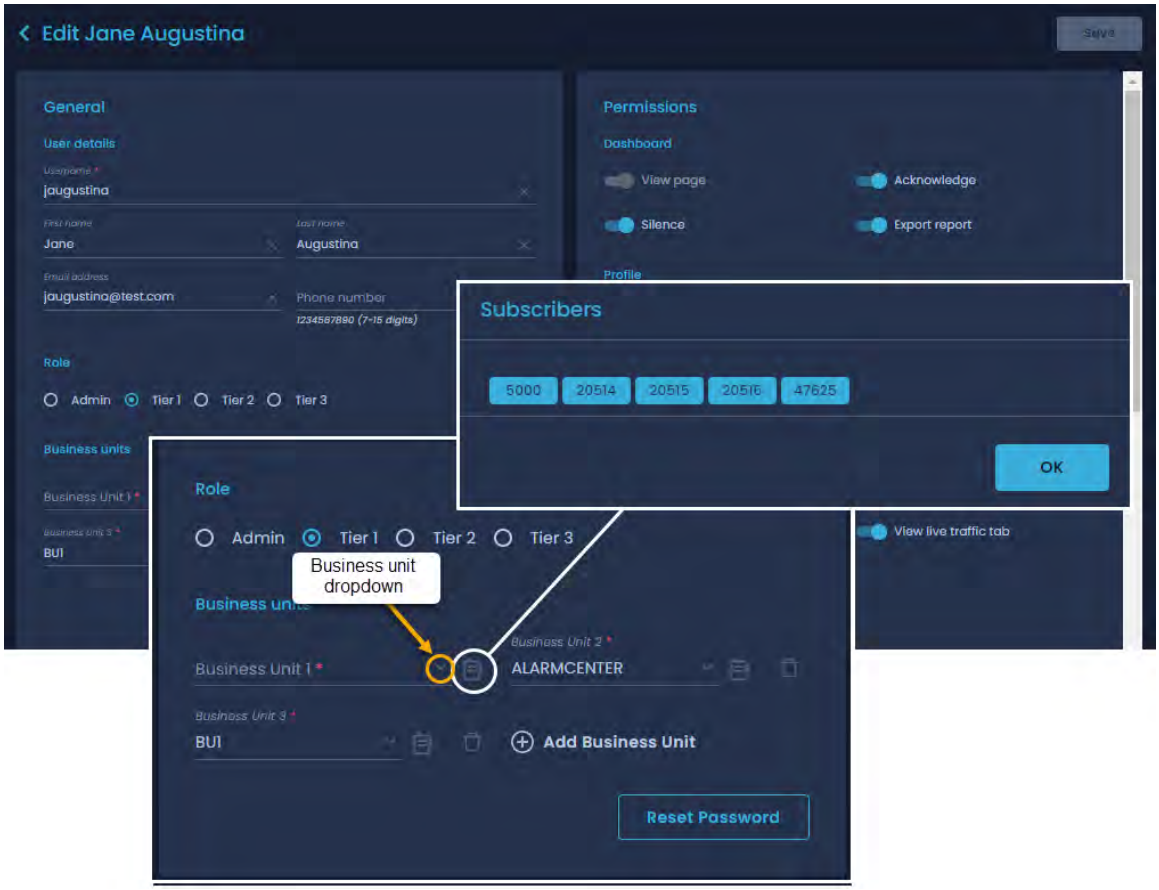


Edit a User Account

To edit the information in a user account, click the **Edit** button.

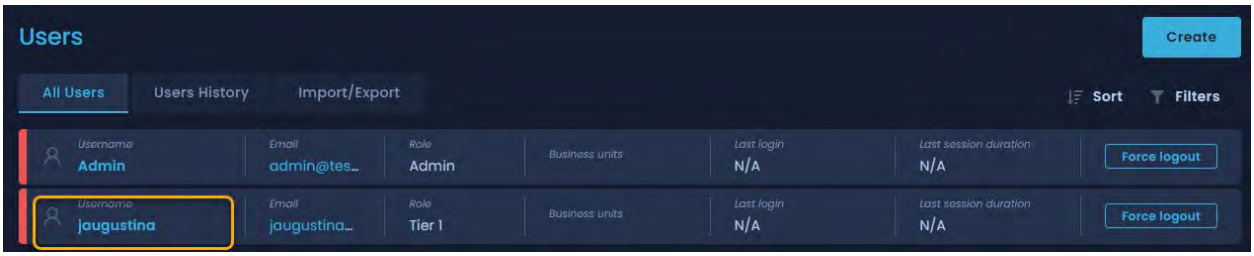
To restrict the user's access to specific business units and subscribers to prevent users from viewing other business units and subscribers, follow these steps:

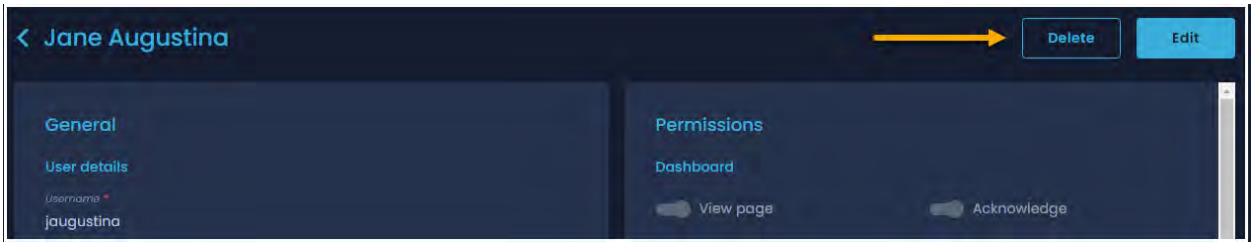
1. Click the business unit dropdown to view a list of business units.
2. Click the subscriber icon to view a set of subscribers. Click the subscribers you would like to add, then click **OK**.



Delete a User Account

Click the user from the list of users, then click the **Delete** button.



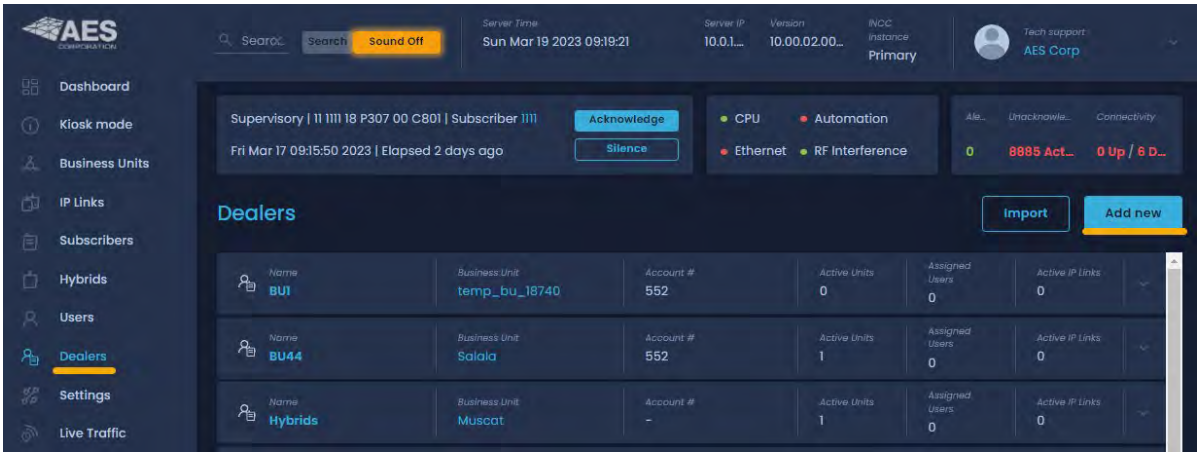


Dealers Page

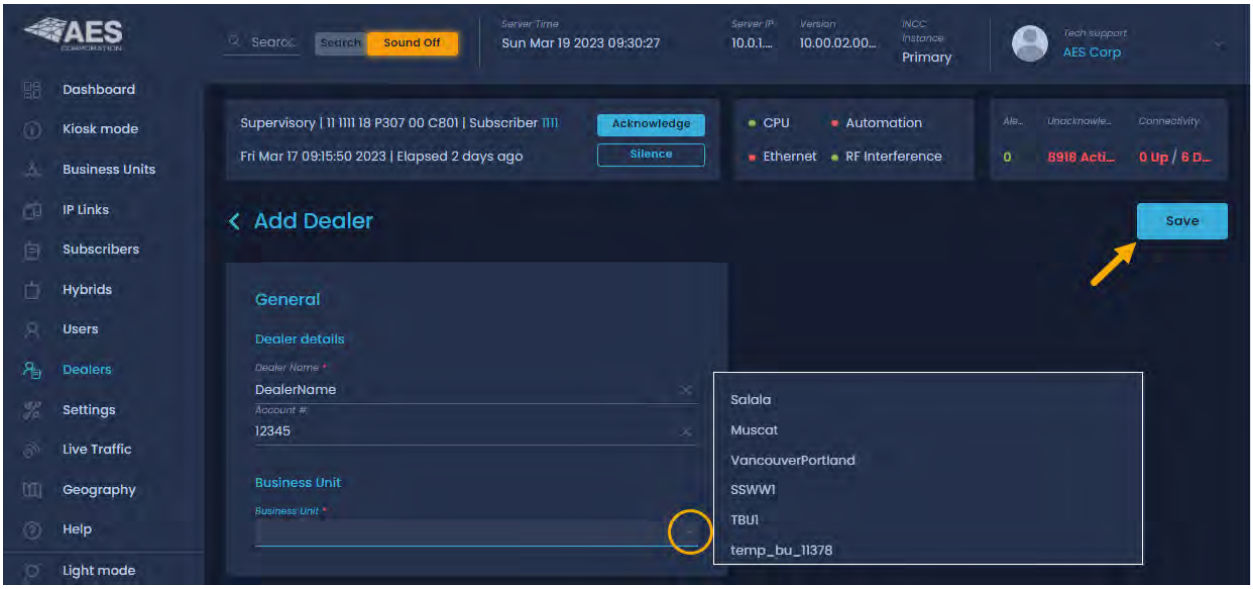
A dealer is an aggregation entity that consists of a set of subscribers. You can add dealers to the INCC either by importing them via a CSV file or by manually adding them to the system. The dealer can then be assigned to a user, in which case the user will be able to access all subscribers belonging to that dealer.

To Add a Dealer Manually

1. Click **Add new**.

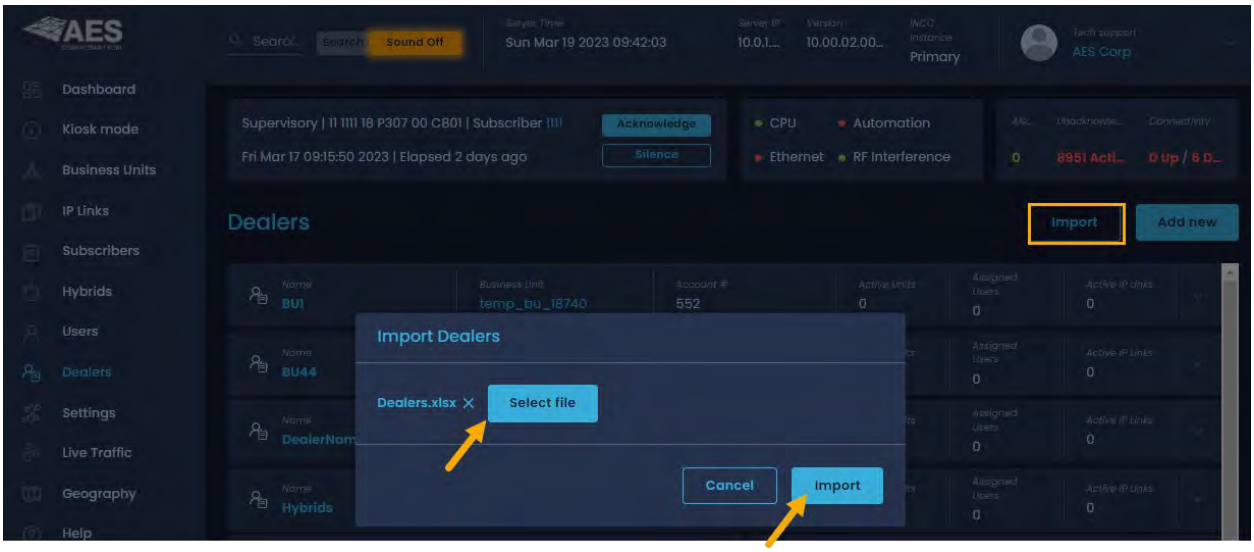


2. Enter the deal name and account number.
3. Click the **Business Unit** dropdown, and select a business unit.
4. Click **Save**.



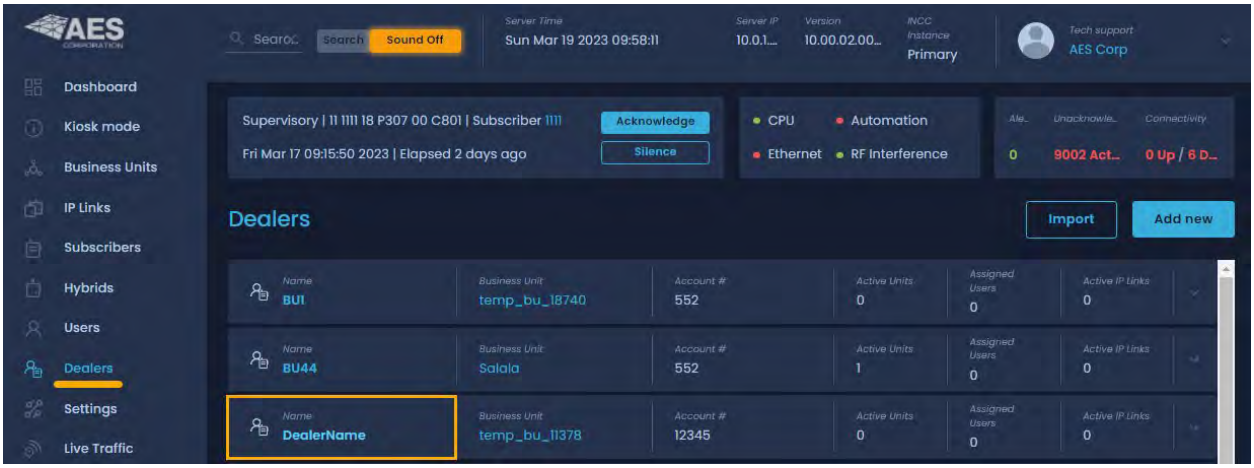
To Add a Dealer Using CSV

1. Click the **Import** button.
2. Click **Select file,** then navigate to the Excel file and double-click it.
3. Click **Import** to upload the file.



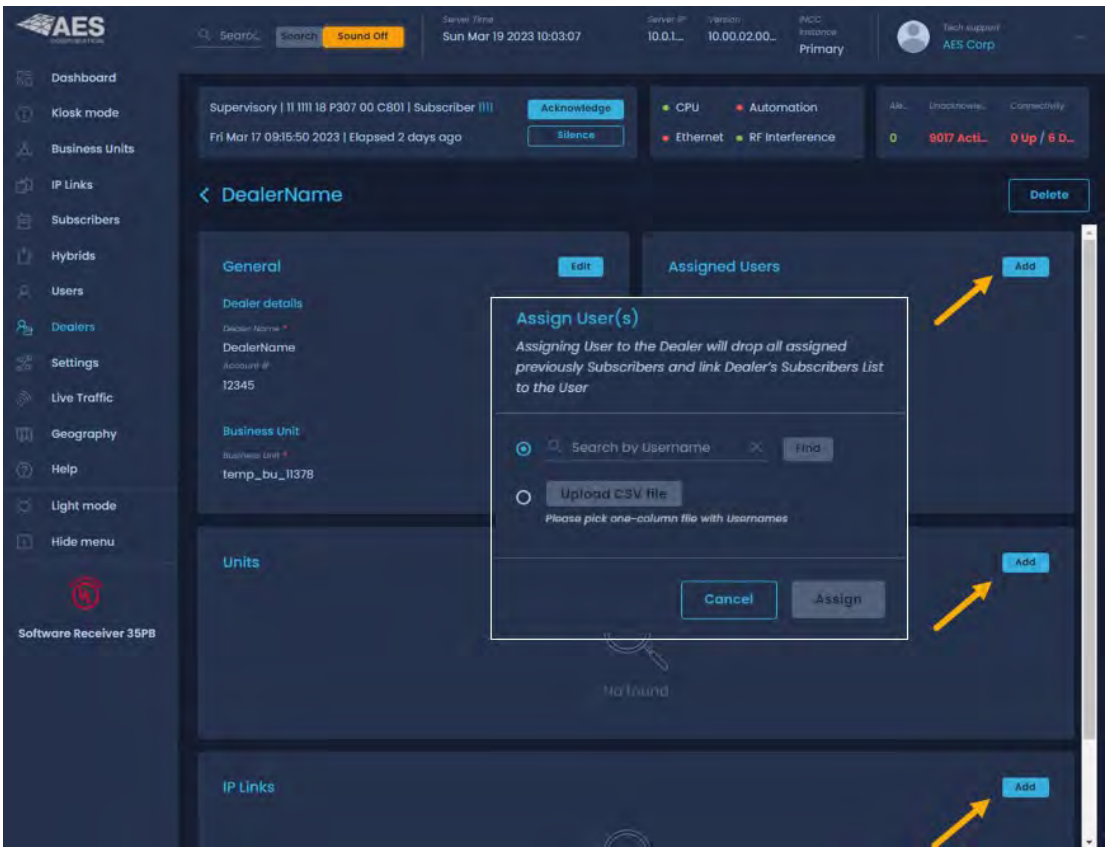
To Add Subscribers to the Dealer

1. From the **Dealer** page, click the name of the dealer.



From the dealer main page, you can add users, business units, and IP Links.

Note: Assigning a user to the dealer will drop all previously assigned subscribers and link the dealer's subscribers list to the user.

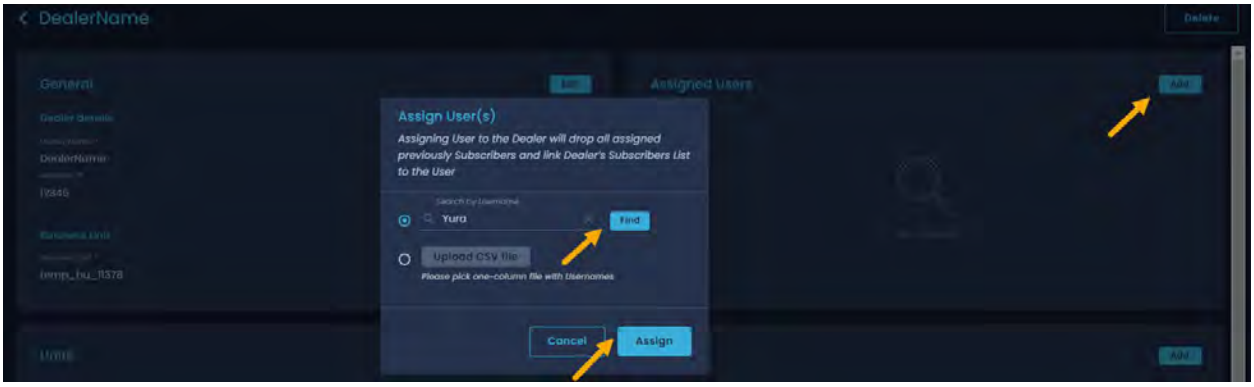


To Add Users

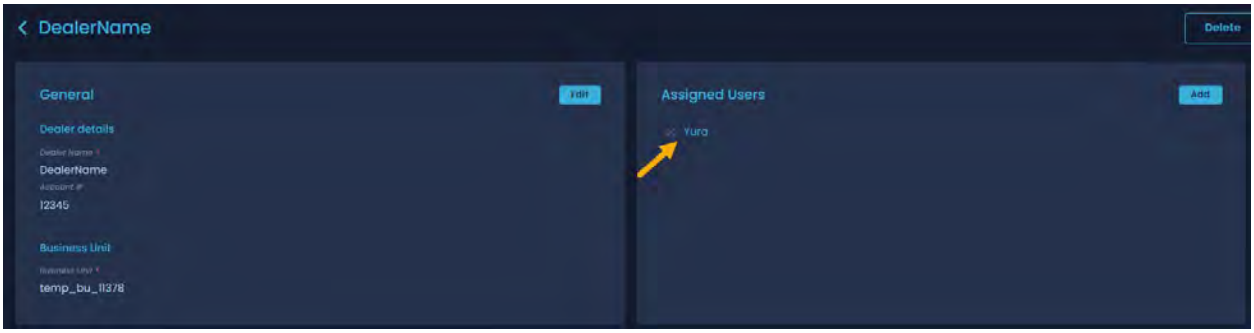
Assigning a user to a dealer drops all previously assigned subscribers and links the dealer's subscribers list to the user.

1. Click **Add**.
2. Click **Find** to locate the user (the user list is generated from the user list in the INCC), then click **Assign**.

Note: You can also add users via a CSV file.



The user appears in the **Assigned Users** list.



To Add Business Units

1. Click **Add**.
2. Click **Find** to locate the business unit, then click **Assign**.

Note: You can also add business units via a CSV file.

To Add IP Links

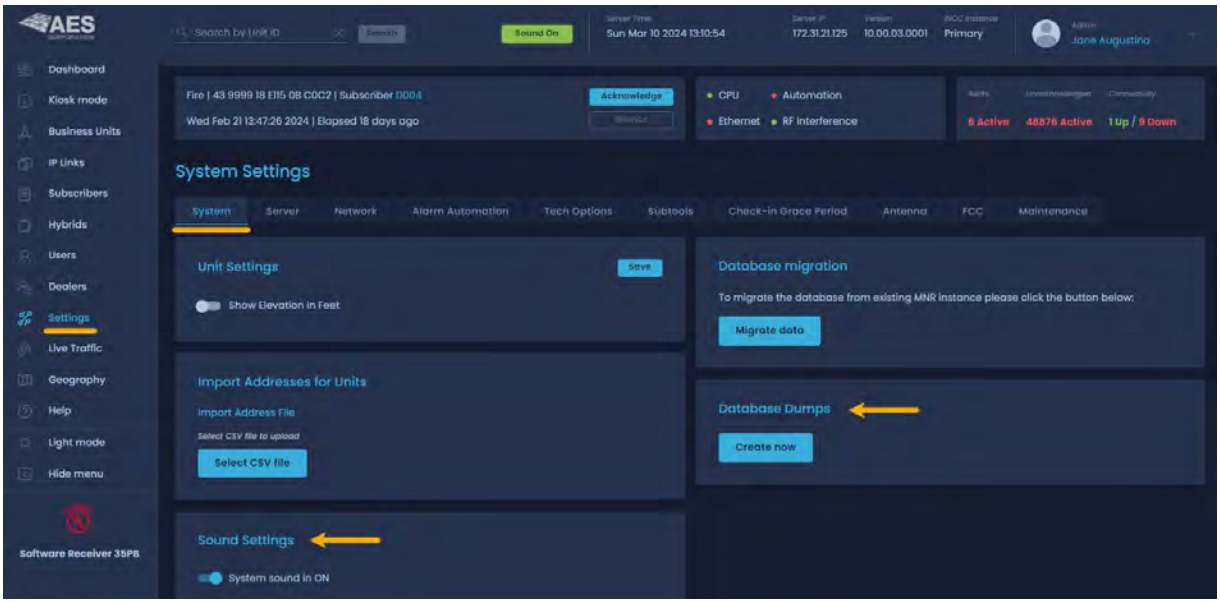
1. Click **Add**.
2. Click **Find** to locate the IP link, then click **Assign**.

Note: You can also add IP links via a CSV file.

Settings

System Tab

- Unit Settings: Toggle between metric and imperial.
- Import Addresses for Units: Data from the NMS will be imported into the INCC.
- Sound Settings: The **Sound off** button can no longer be used to control the sound of the INCC. The button is just a visual indicator of the **System sound in OFF** (or **ON**) setting (as shown below). This gives the admin full control and prevents other users from accidentally turning the sound off with a single click.



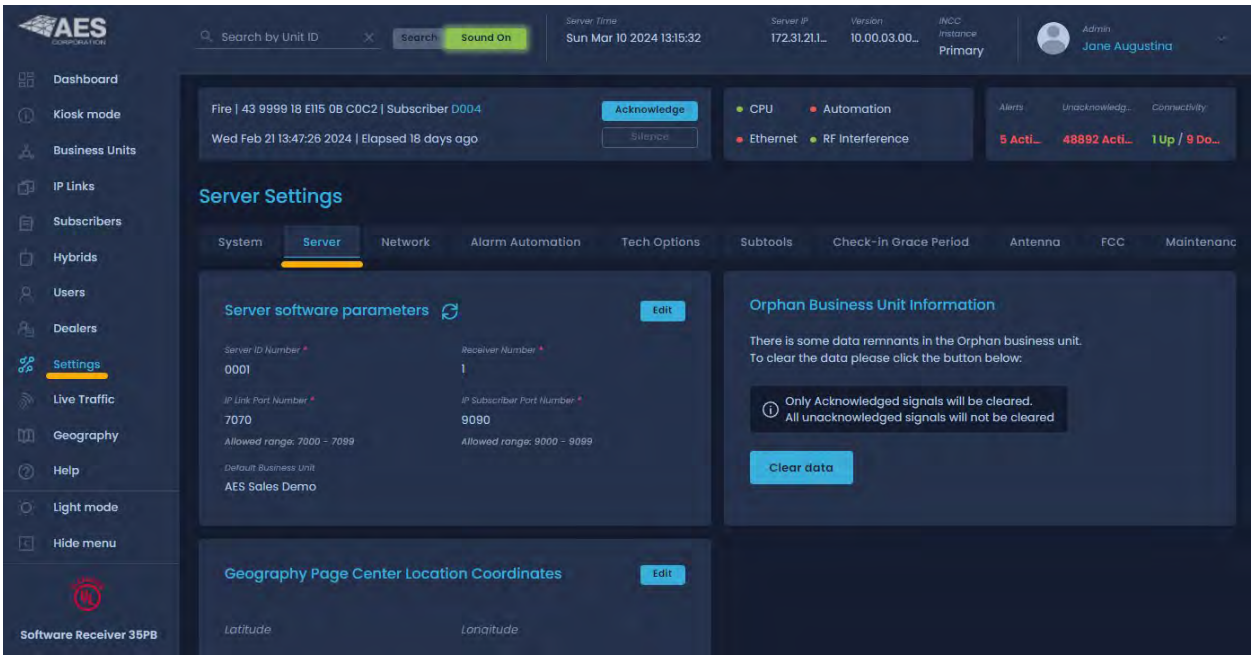
- Database Migration: Database migration allows a seamless transition from an existing MNR to the INCC. During migration, the MNR database dump data is transformed and entered into the INCC database.

- Database Dumps: A database dump can be shared with technical support to solve an issue. It can also be used to import the data to another VM by sharing the database dump with yourself.

Server Tab

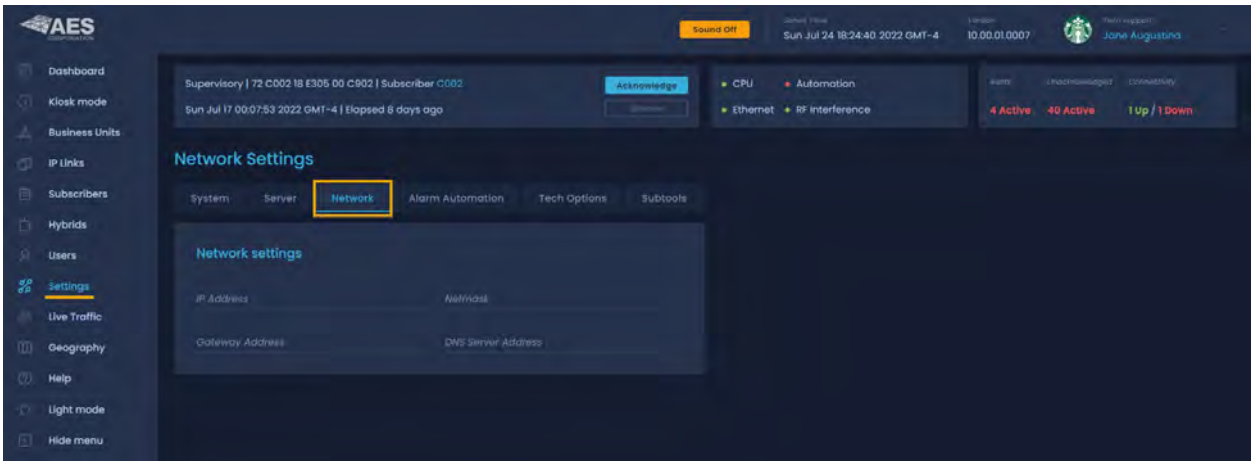
The Server tab contains server software parameters:

- Server ID number – the identification number for the server instance associated with the installation.
- Receiver number – the customer-defined identification number.
- IP Link port number – the port number for the INCC IP Link associated with the installation. This number must be within the 7000 – 7099 range.
- IP Subscriber port number – the port on the 2.0 Hybrid. This number must be within the 9000 – 9099 range.
- Default Business Unit – the name of the business unit orphan.



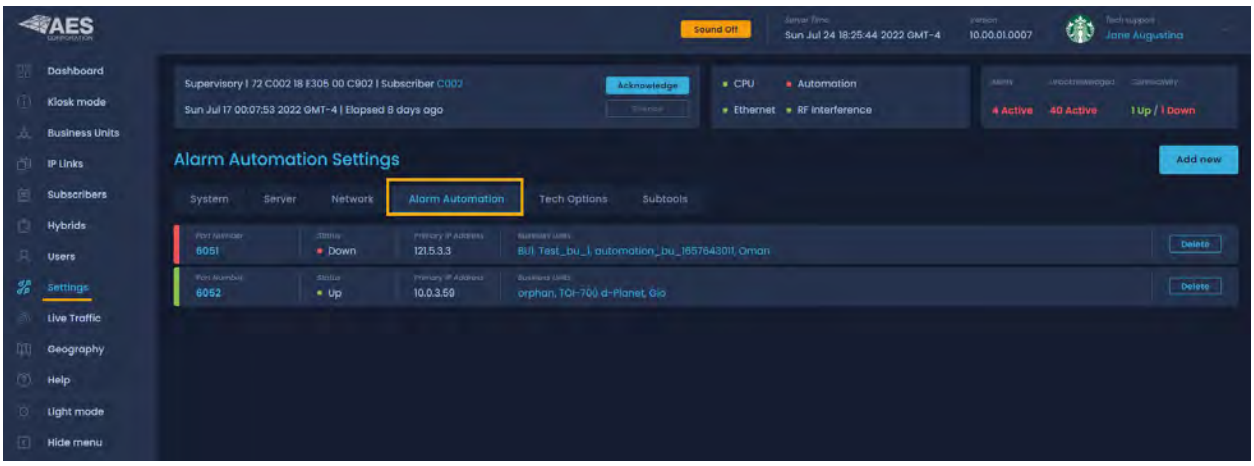
Network Tab

Network connectivity settings include the local IP Address, netmask, gateway address, and the DNS server address. This information is automatically populated.

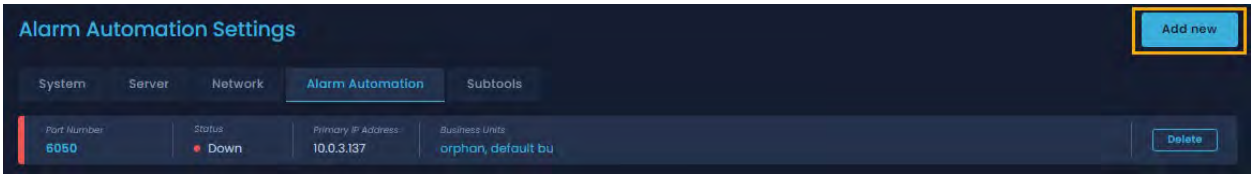


Alarm Automation Tab

This tab displays the status information for alarm automation software that the INCC is configured to use.

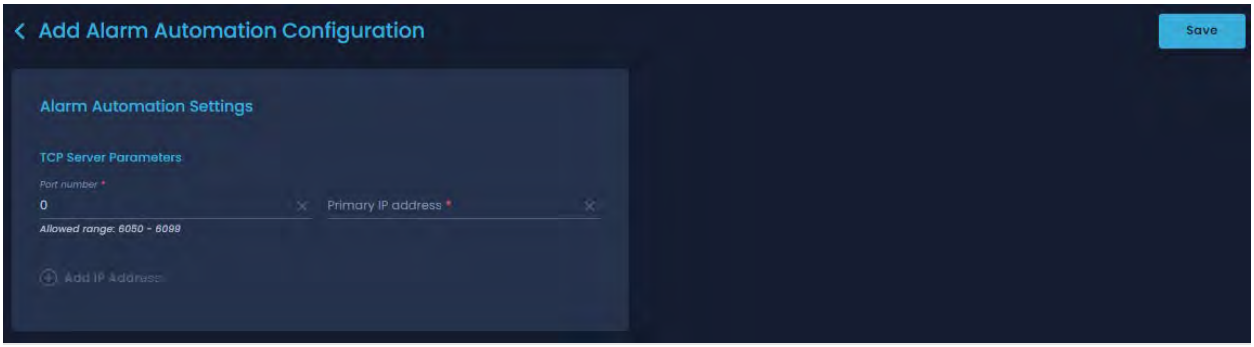


To enter information for configuration settings for an alarm automation system, click the **Add new** button.



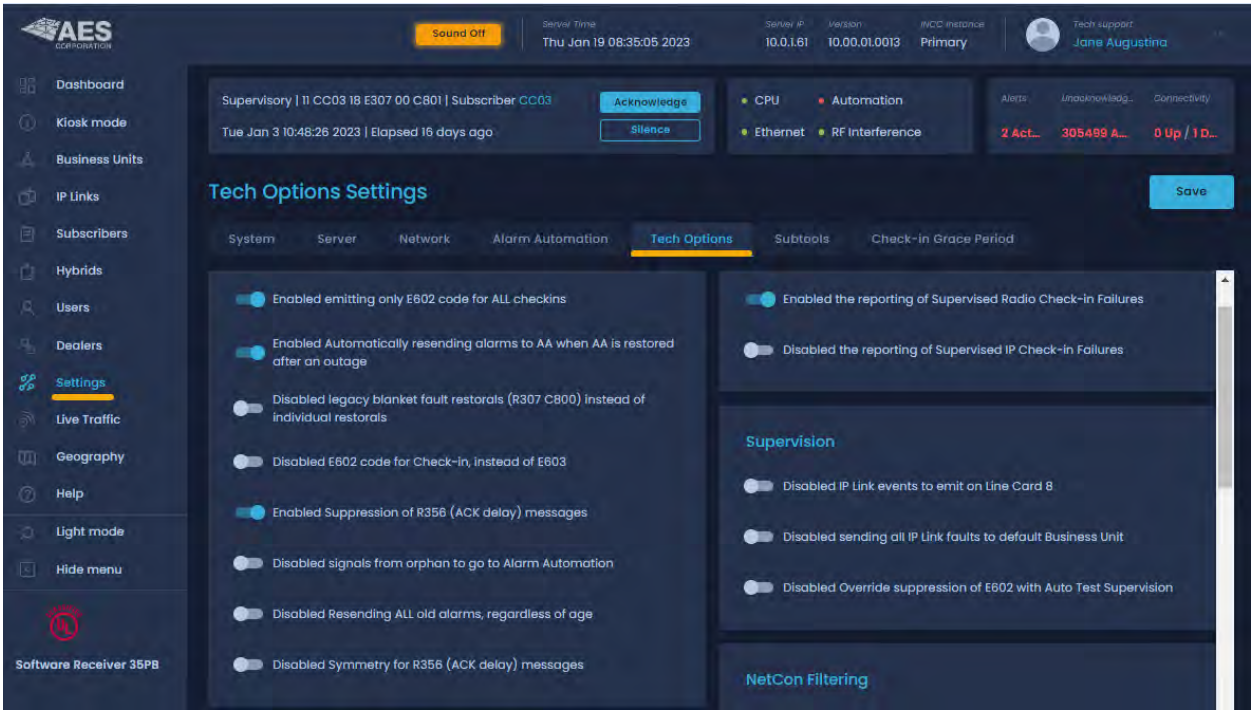
Enter the port number and primary IP address. Additional IP addresses may be entered if the automation software supports this. Use the **Add IP** address control. Click **Save** to store the information.

Important: The allowable range for port numbers is 6050–6099.



Tech Options Tab

Listed below are all the options available on the …



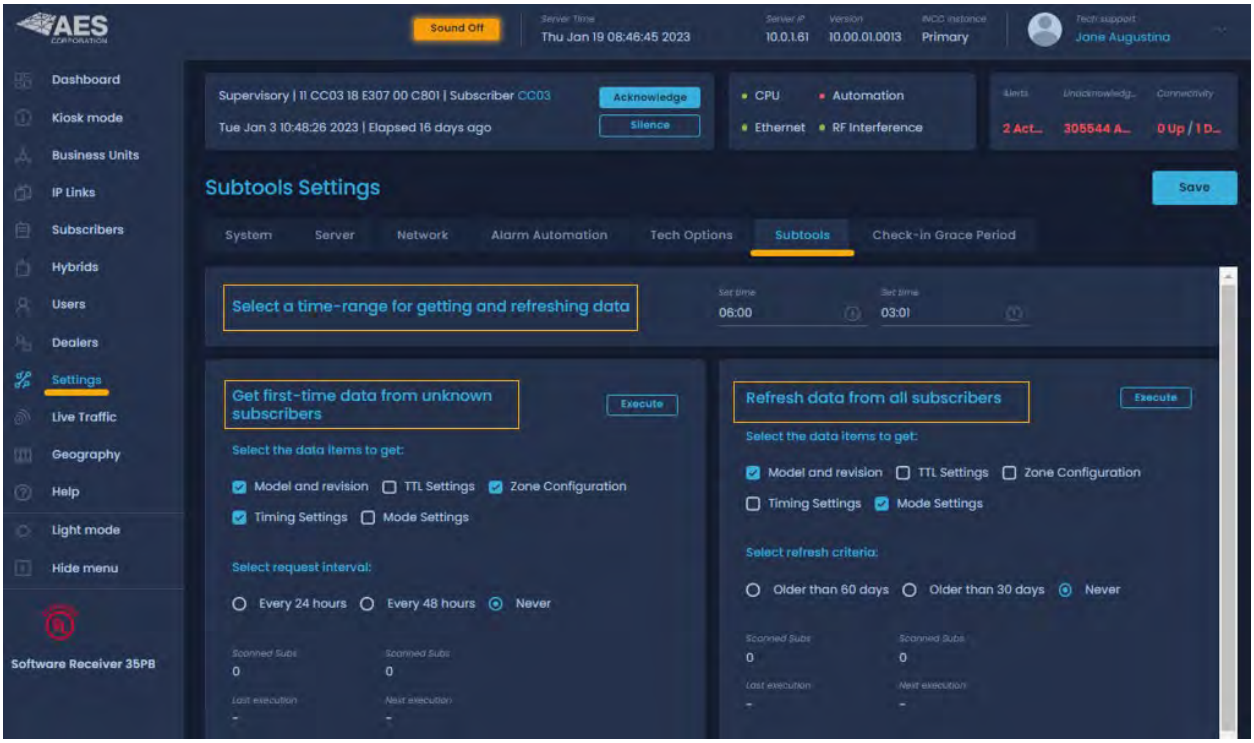
Options	Enable?
Enabled emitting only E602 *code for ALL checkins* This feature will eliminate E603 & E608 and combine to only #E602	
Enabled Automatically resending alarms to AA when AA is restored after an outage This feature allows the INCC/MultiNet Receiver to automatically resend messages to Automation when Automation is restored after a connection loss or outage. On previous INCC/MultiNet versions, all messages reported on the LCD screen were acknowledged manually one after the other and were never offered to Automation again. The Automation LED on the front panel of the MultiNet turns on if a message does not reach Automation. This indicates that Automation is down. The Automation LED turns off only when a new message is acknowledged by Automation after a connection has been restored. A new message coming in after automation is restored is required to recognize or test its return to operation. When this feature is set as Yes, any queued messages that are one day old (24 hrs.) or less are resent. All older queued messages are discarded. Messages are resent at a maximum rate of 30 messages per minute to help control a possible runaway condition.	Yes
Enabled legacy blanket fault restorals (R307 C800) instead of individual restorals This Feature will not send individual restoral. Enable and Disable this feature for subscriber faults	
Enabled E602 code for Check-in, instead of E603 By default E603 and this feature will enable E602	
Enabled Suppression of R356 (ACK delay) messages Suppress R356 ACK delay	
Enabled signals from orphan to go to Alarm Automation By default, the Orphan Business Unit (BU) does not deliver messages to automation or to the printer. Messages are only displayed in IPCtrl accessed using VNC Viewer for Orphan on Display :1. With this option set to Yes, the *Orphan Business Unit becomes a "catch all" and delivers any messages to automation. To allow a distinction between an Orphan Subscriber and a normal Main BU Subscriber, Orphan messages will b*e sent to automation, using the main BU number, using Line Card 9.	Optional Yes or No
Enabled Resending ALL old alarms, regardless of age With this Tech Option set to Yes, all old messages will be resent to automation, regardless of how old they are. Not recommended to use this option especially if resend to AA is enabled.	No
Enabled Symmetry for R356 (ACK delay) messages Enable and Disable Feature E/R. By default system will only generate R, this feature will add E	
Deduplication	
Enabled *IP packet deduplication*	Yes/No

Options	Enable?
2.0 MCT Subscribers will receive RF and IP packets. Enable/Disable receiving single or dual packets	
Line Card	
Enabled LC==1 for Tap message account takeovers Several versions of the INCC/MultiNet suite of software attempted to address the incorrect reporting of Line Card from IntelliTap/Pro generated messages. The primary issue is that when the IntelliPro/Tap reports that it detected a line cut, the Line Card should be reported as 1 because the detection is from an AES device or module but is reported as a 3 indicating that the AP is reporting the line cut. Setting this option to Yes corrects the Line Card for Line Cut from the Tap/Pro to 1. A message from the AP reports as 3 in suite 1067. Problem introduced is that using Account Override on an IntelliPro will cause all CID messages with the Account Override marker to also report on Line Card 1 instead of the correct Line Card 3. If Account Override is never used, this Option set to Yes will result in the IntelliPro Line Cut detection to be correctly reported. Since you can never for sure know that Account Override is used, the safest option is to leave this at No and understand that an IntelliPro Line Cut message will look like it is being reported by the alarm Panel.	No
Enabled IPSub packet using different receiver linecard group Setting this to Yes will result in different line cards being used for signals received by RF and TCP/IP. Default Line Card Assignments for origin of message. 1 = AES Device, Subscriber, IP-Link, Receiver 3 = Alarm Panel through IntelliTap Protocol in CID 4 = Alarm Panel through IntelliTap Protocol in 4+2 Selecting (Yes) will result in the following Line Card assignment for messages that are received from Subscribers directly over TCP/IP. 2 = AES Device, Subscriber, IP-Link, Receiver 5 = Alarm Panel through IntelliTap Protocol in CID 6 = Alarm Panel through IntelliTap Protocol in 4+2	
Supervision	
Enabled IP Link events to emit on Line Card 8 Will enable IP Link Faults to line card 8	
Enabled sending all IP Link faults to default Business Unit Enable all IP Links Faults to be sent to default Business Unit	
NetCon Filtering	
Enabled Bad NetCon Filtering for selected models and firmware revisions	No

Options	Enable?
The filtering of Bad or corrupted packets is on by default in versions that offer this feature. The filter examines IntelliTap Type I packet data. Packet data that fails the criteria of the filter is sent to the Bad Packet Log and not sent to Automation, Printer or IPCtrl. The filter is examining the CID or 4+2 Tap data strings. There are instances where legitimate IntelliTap Packets are being filtered. If after reviewing the Bad Packet Log, it is determined that legitimate data is filtered, the filter would need to be disabled or turned off to allow these through. This will expose the system to rare and real bad packets should they ever occur.	

Subtools Tab

The **Subtools** tab includes a set of subscriber maintenance tools for executing automated maintenance operations, allowing you to retrieve subscriber configuration information on all or select subscribers in an AES network. The information is reported back to the INCC through the IntelliNet network.



Configuring first-time data from unknown subscribers

These settings are associated with subscribers that come onto the network for the first time.

1. Select a time range for getting and refreshing data.
2. Select the data that you would like to get from the subscribers, all or single types of data.

   This tool queries every subscriber in all business units for the following data. This is useful for NMS since it displays the above data for each subscriber on the dashboard.

- Model and Revision
- Timing Settings
- TTL Settings
- Mode Settings
- Zone Configuration

3. Select how frequently you would like the query to run, every 24 or 48 hours.
   - Every 24 hours
   - Every 48 hours
   - Never

     Every 24 or 48 hours, outbound packets will be sent to subscribers with unknown data. During this process, there will be 2 packets sent out every 60 seconds. If there are no subscribers with unknown data, then no packets will be sent out.

4. Click **Execute**.

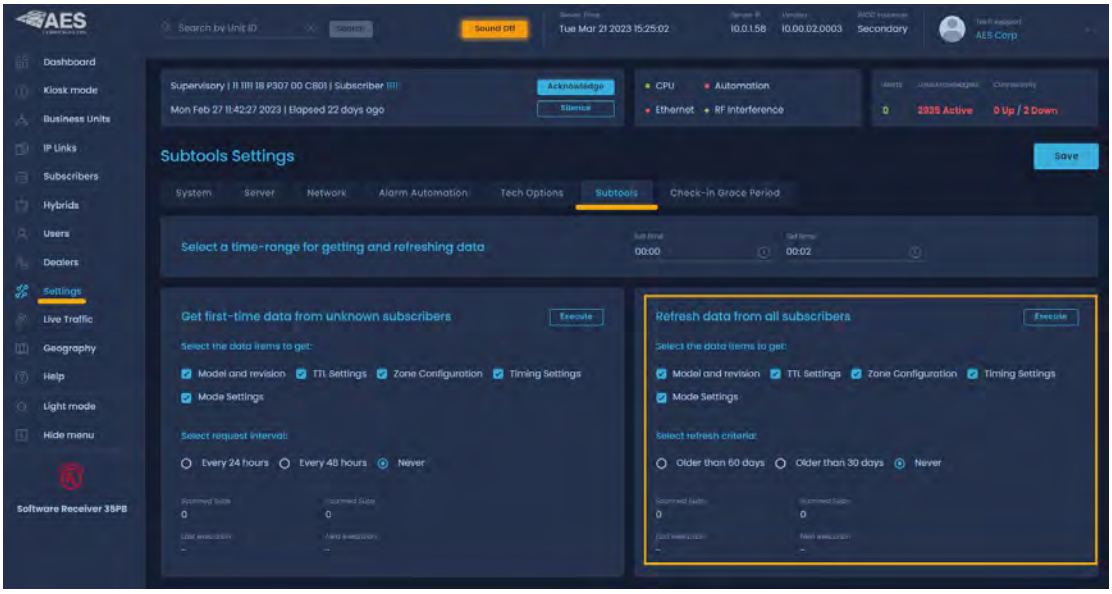
Refresh data from all subscribers

When a subscriber comes onto the network for the first time (refer to the configuration settings), the only details that are automatically populated from the alarm table are as follows:

- Unit ID
- BU

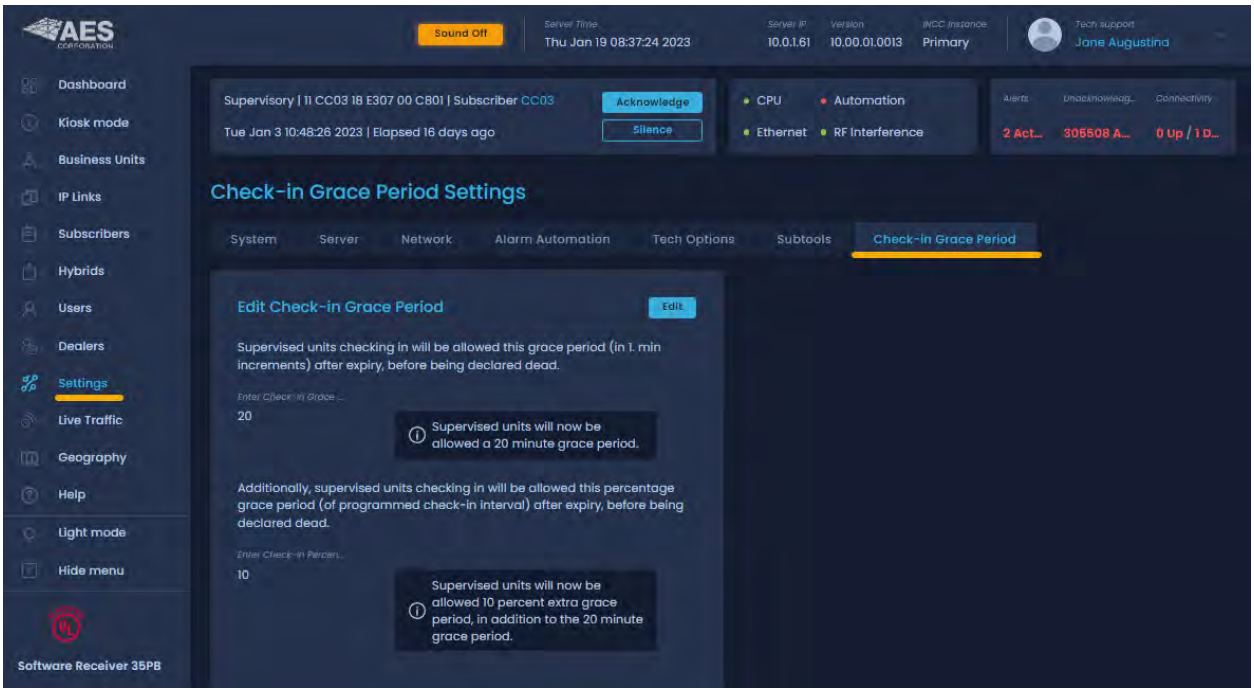
You can utilize the individual general settings under subpage to ping data for each unit.

The **Refresh data from all subscribers** option in the **Subtools** tab gives customers the ability to ping all subscribers to grab additional data.

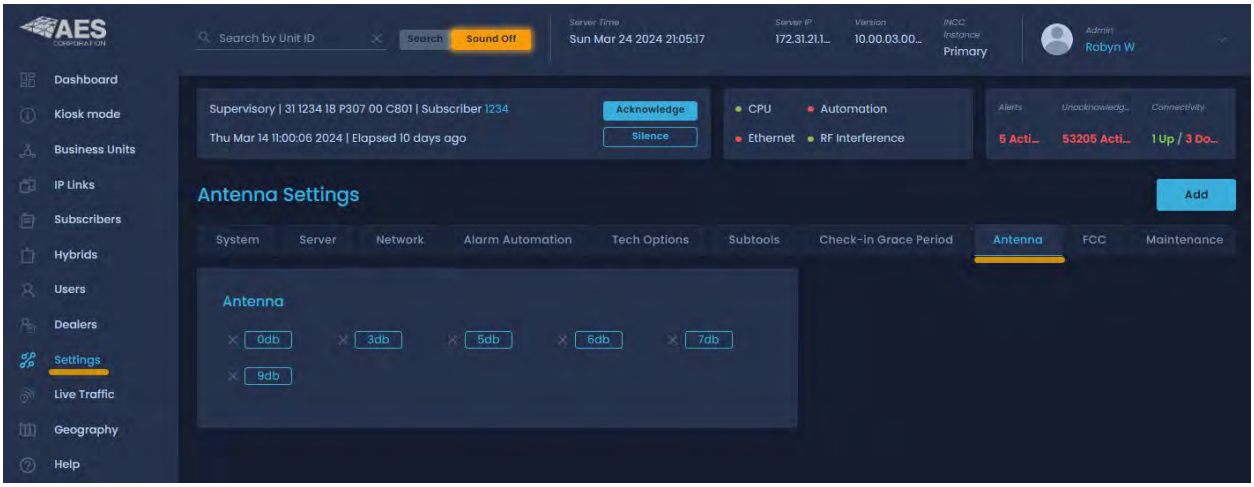


Check-in Grace Period

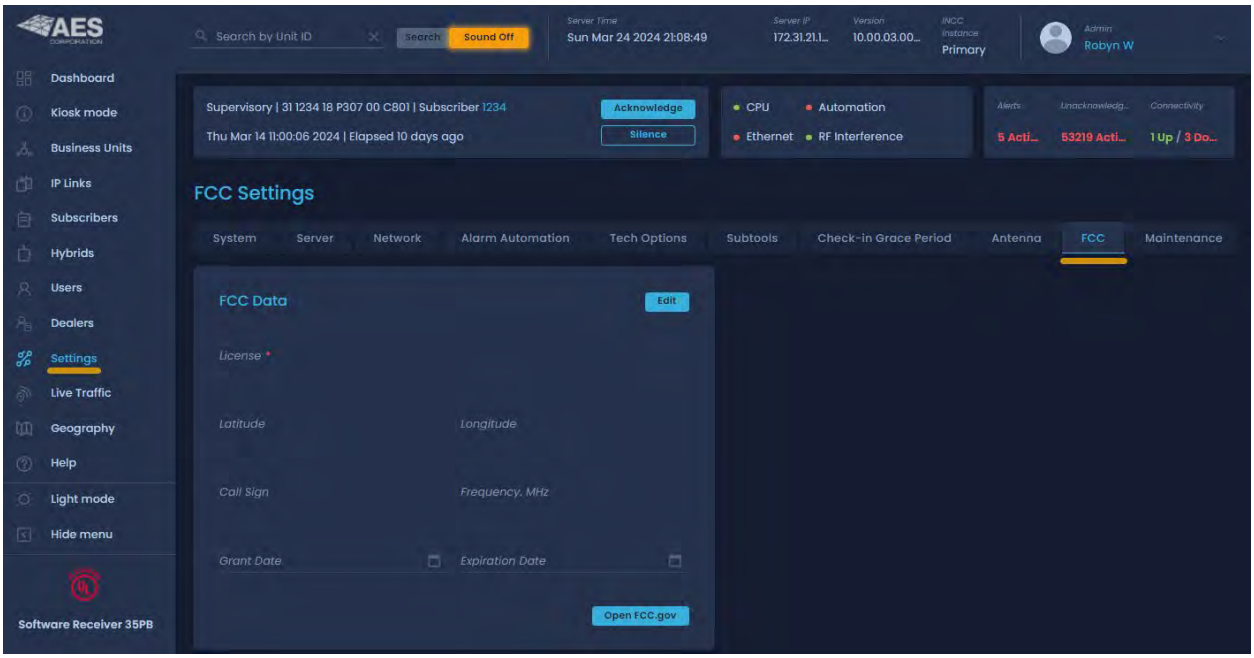
The **Check-in Grace Period** tab has two settings (minutes and percentage) that allow the user to set the grace period for supervising check-ins from the MultiNet receiver. Although the use of this feature is not recommended, if it is used, a grace period is needed. The suggested grace period is 20, which is 20 x 0.1 minutes (this equates to two minutes plus Check-In Percentage of 10%). The default is 20 and 0%, so this should be modified to 10% on any configuration unless the user has specific alternate needs.



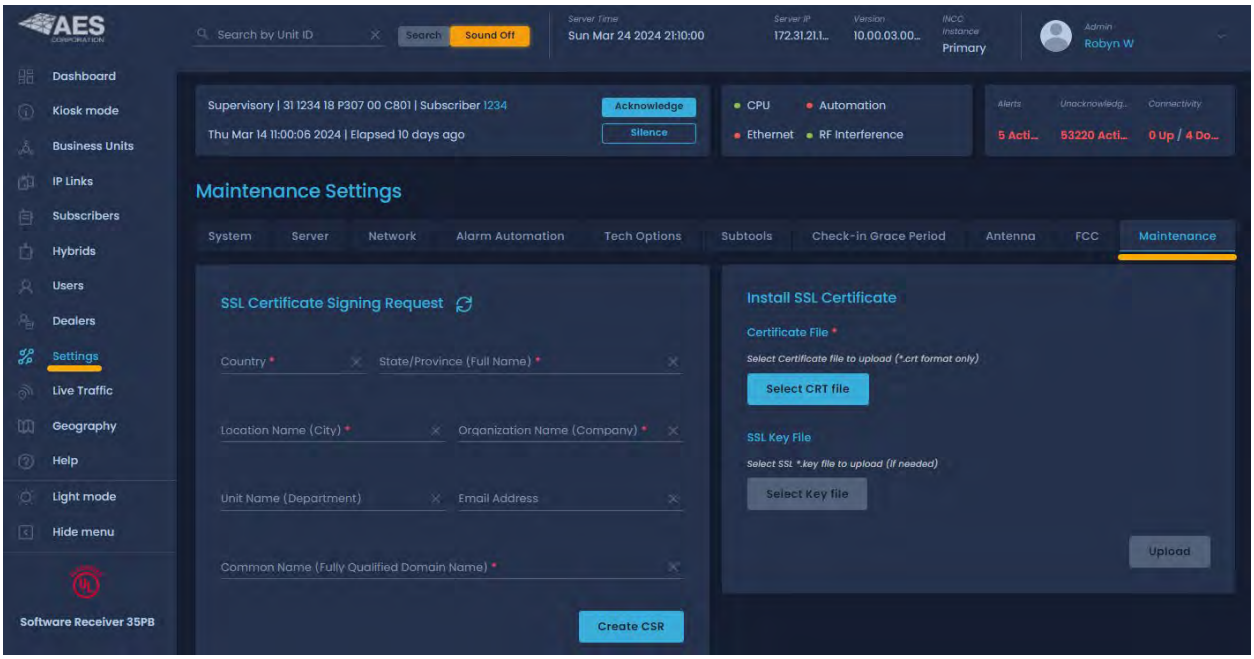
Antenna



FCC

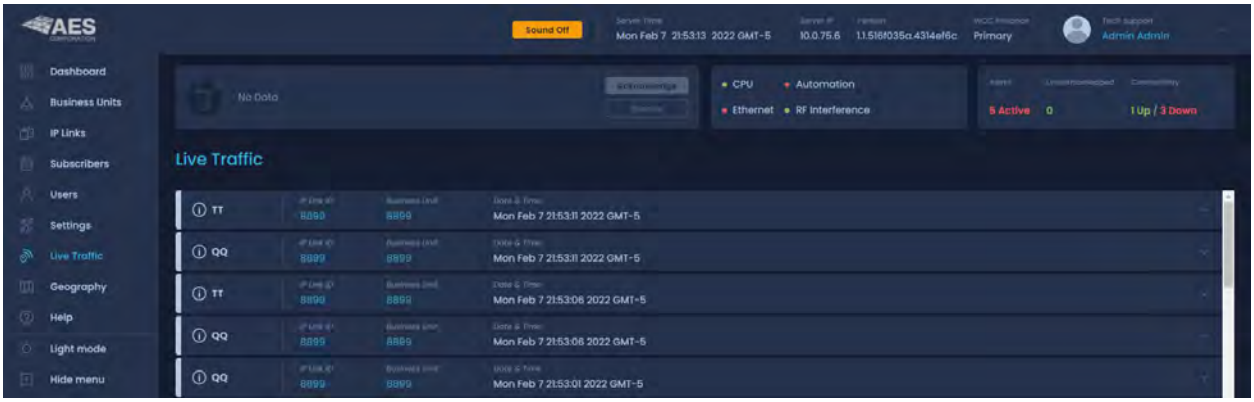


Maintenance



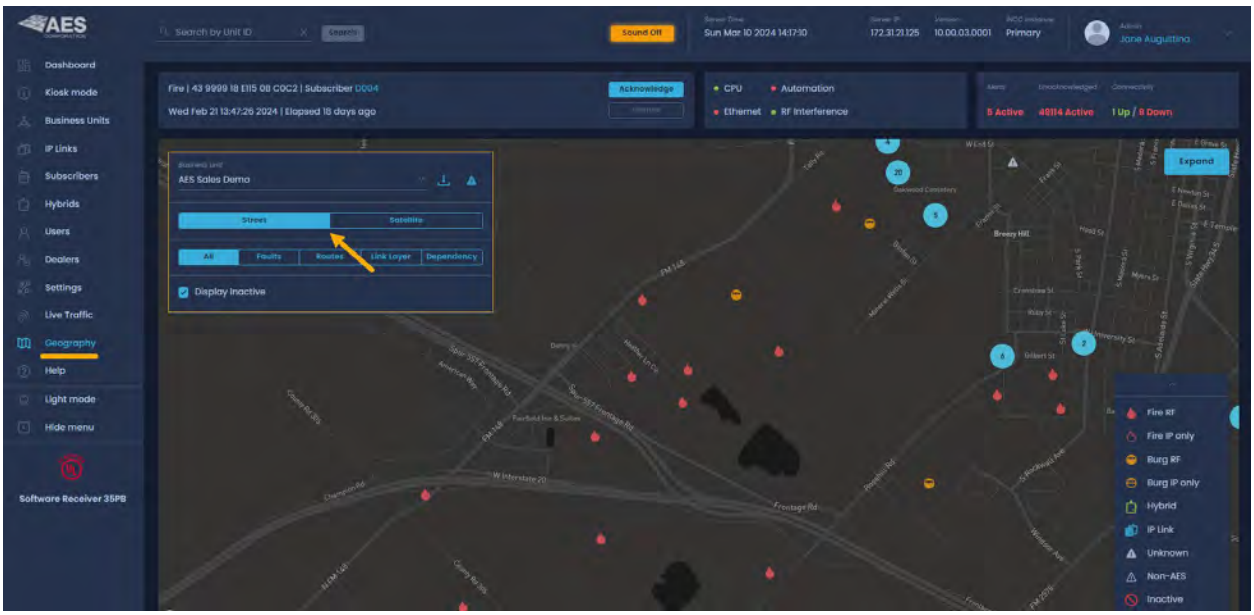
Live Traffic

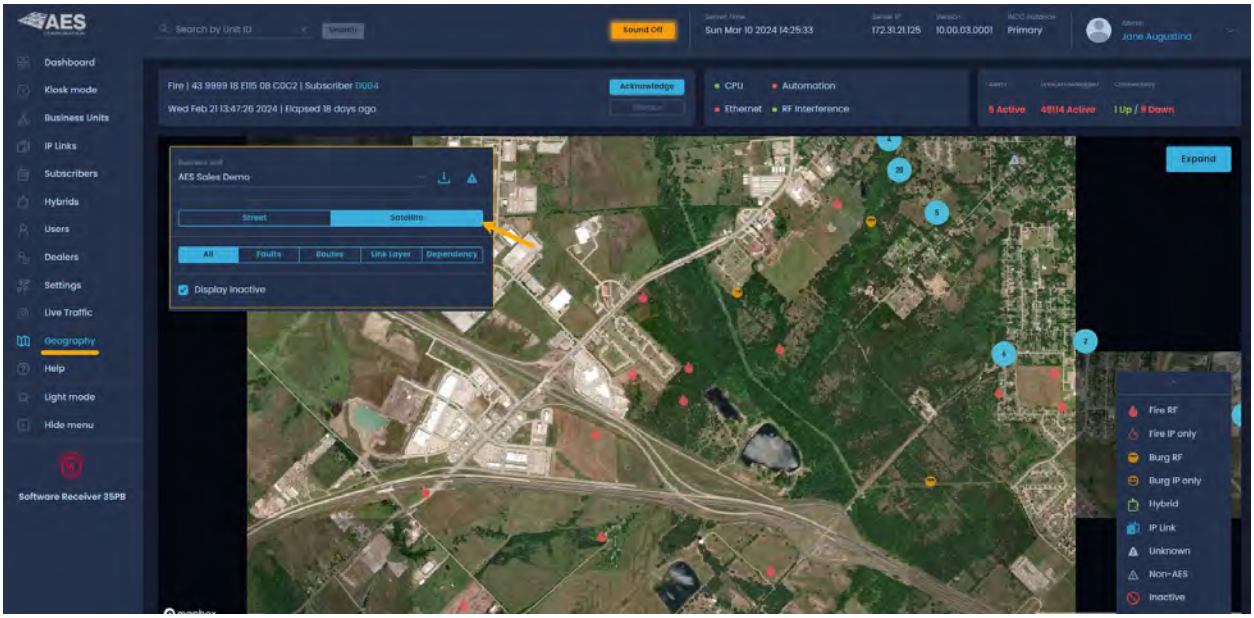
Live Traffic shows real-time information on communications between the INCC application and the installed AES subscribers. The traffic information and IP Link/Subscriber/Business Unit identification show where the traffic originated.



Geography

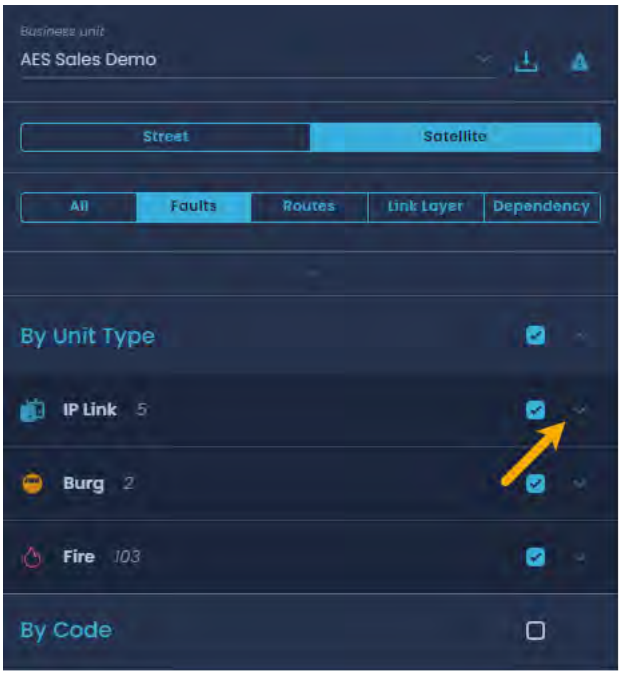
The **Geography** tab has the option for Earth or satellite view. The **Street** view enables you to view and navigate through 360 degree horizontal and 290 degree vertical panoramic street level images. You can also view the types of faults, the routes, the link layers involved, or the dependencies.

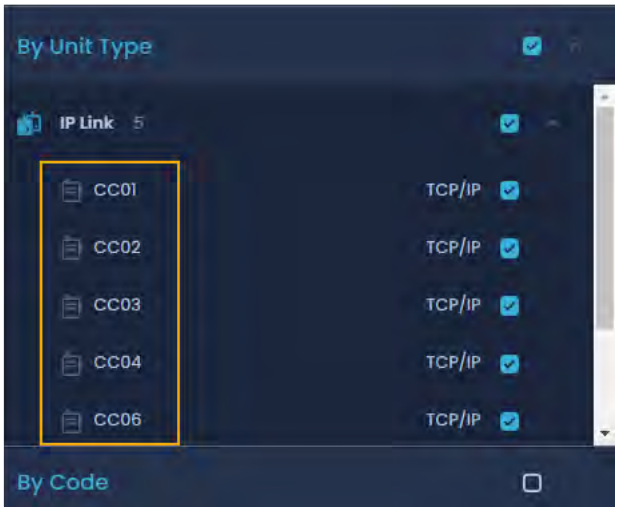




Faults

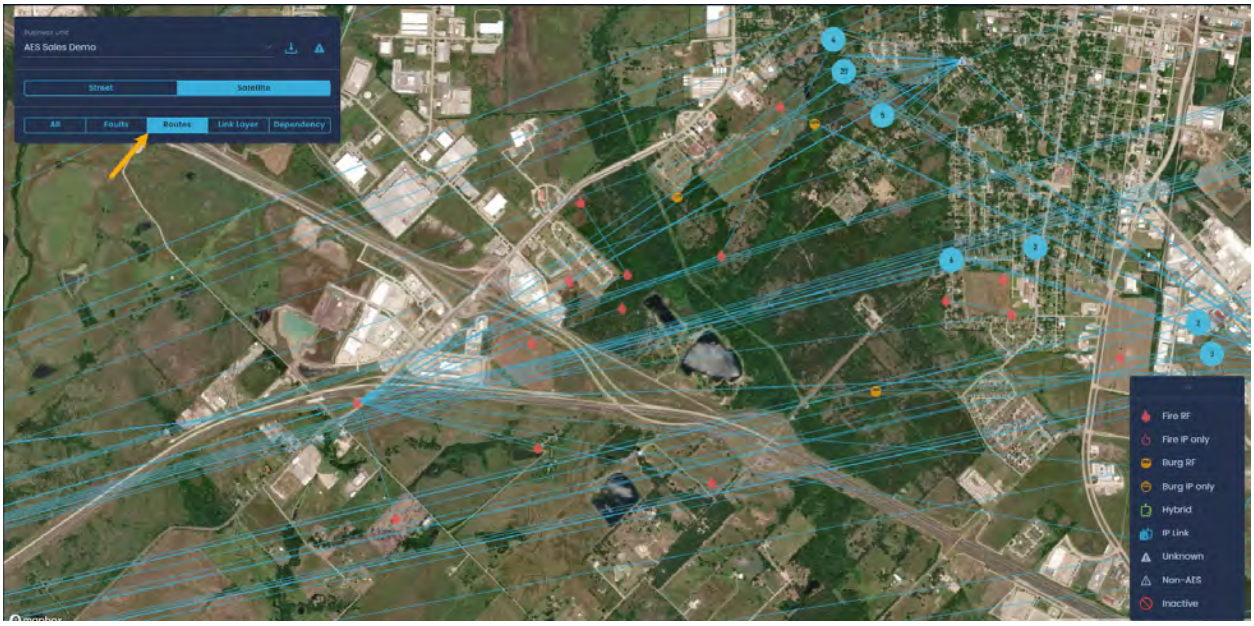
To view the active faults, click **Faults** then click the dropdown icon to view the codes.

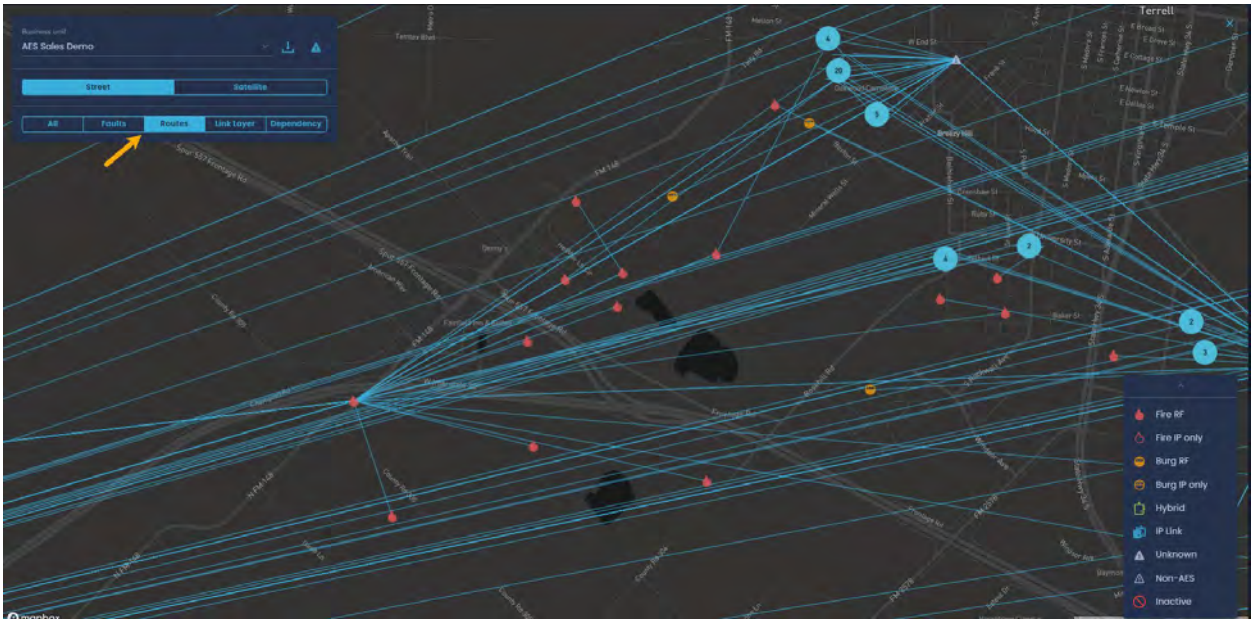




Routes

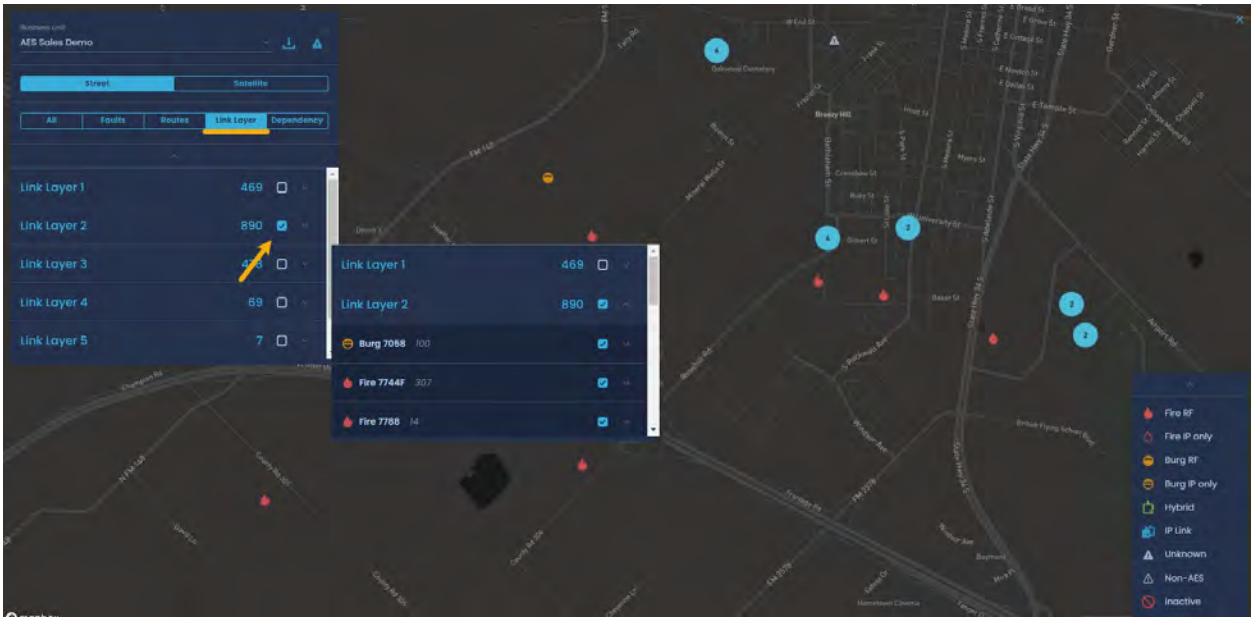
Click Routes to view the routes of the faults.





Link Layer

Link layer 2 indicates that it is directly connected. Link layers 3, 4, 5, and 6 refer to the number of hops required to get from the subscriber to the IP links.

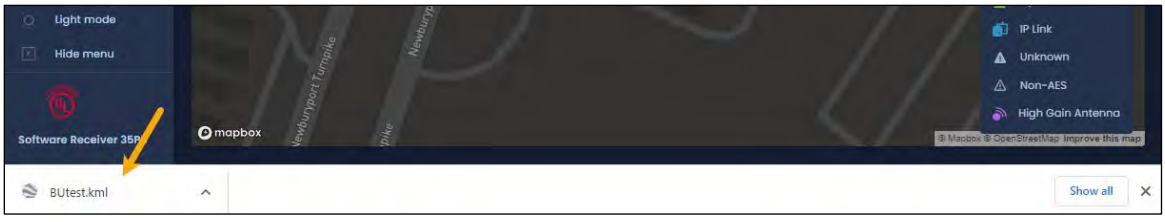


Configuration

To view the Visualization feature of the INCC on Google Earth, you must first load the addresses of the Subscribers and IP Links (see steps below).

1. This step is done during the migration process. Click the download icon to download the .klm file with the Business Unit map information. (KML is a file format used to display geographic data in an Earth browser such as Google Earth.)

2. Click the business unit .klm file at the bottom left of the screen.



As Google Earth begins to launch, you will be asked to enter a user name and password. The user name is the name of the business unit, and the password is the same password used for the *Operator Dashboard* password for that business unit.

3. Enter user name and password and click **Sign In.**

   Invalid addresses – When addresses are not in the correct format, they will need to be adjusted.

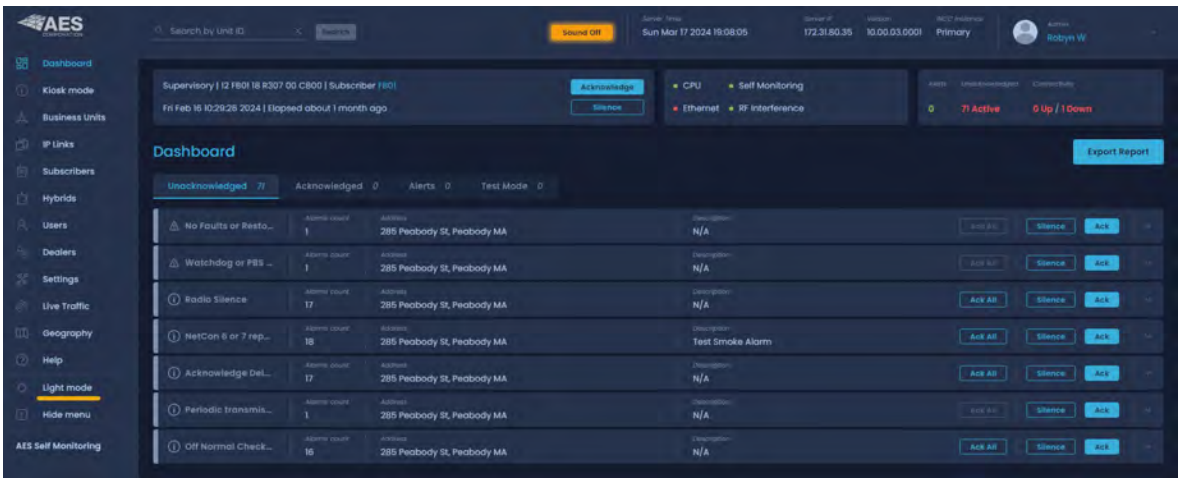
Help

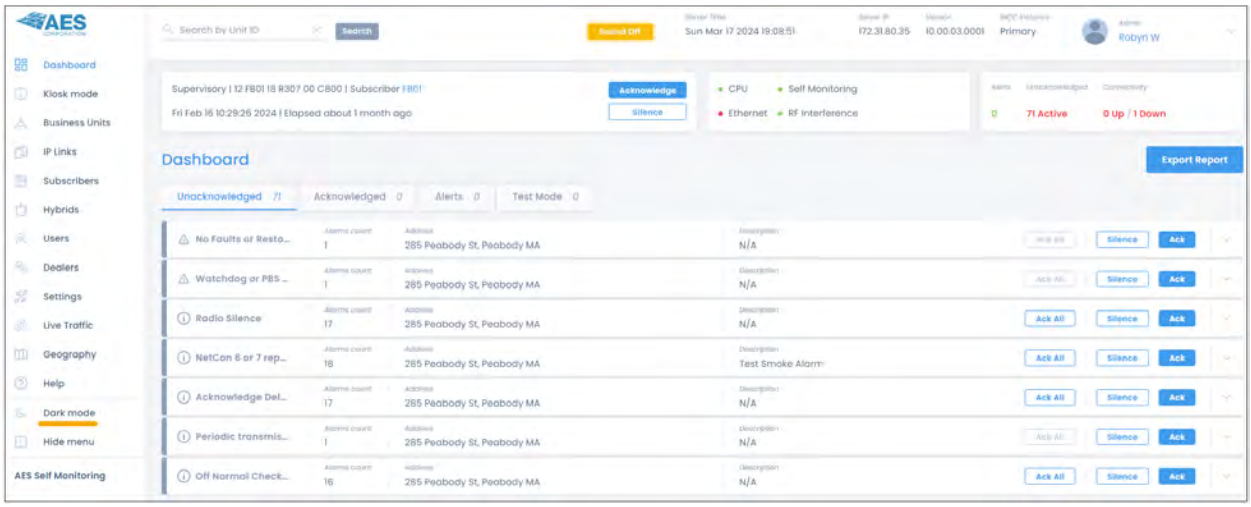
The Help page allows access to technical assistance resources.

- User Manual: online access to the INCC user manual
- Frequently Asked Questions: questions and answers about INCC and AES IntelliNet.
- AES YouTube Channel: videos on technical material and configuration of AES IntelliNet products
- AES Technical Support: contact information for AES support services.

Light mode

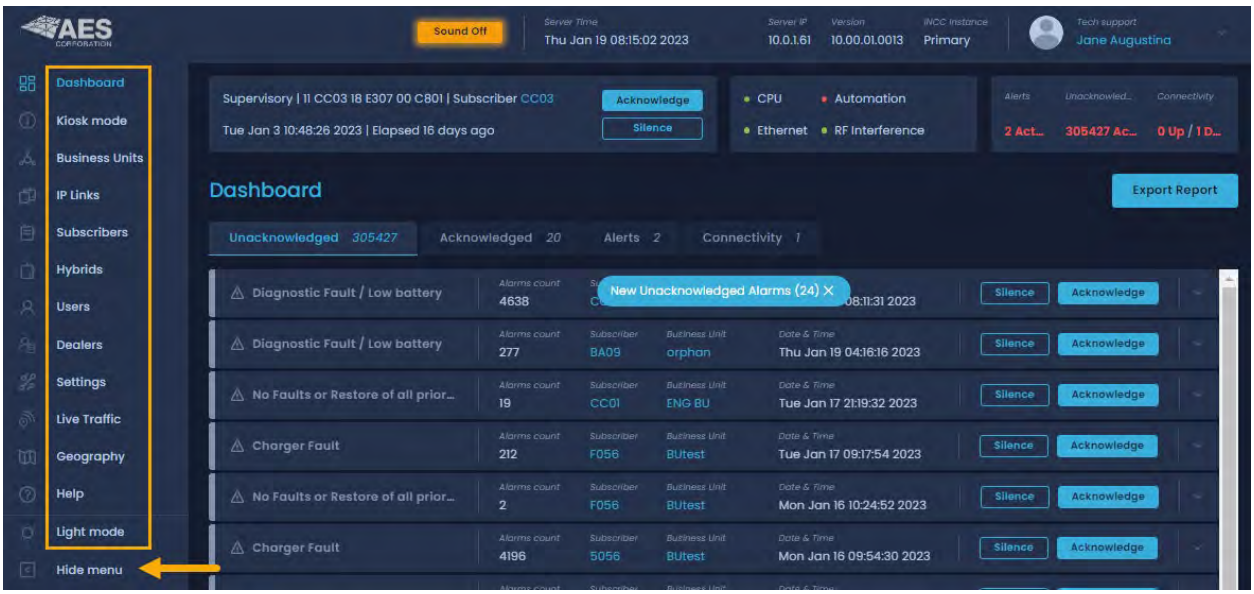
The INCC user interface can be viewed in either light or dark mode.





Hide menu

Clicking **Hide menu** hides the text portion of the navigation bar, leaving just the icons.



To expand the navigation bar to its default state, click the **Hide menu** icon.

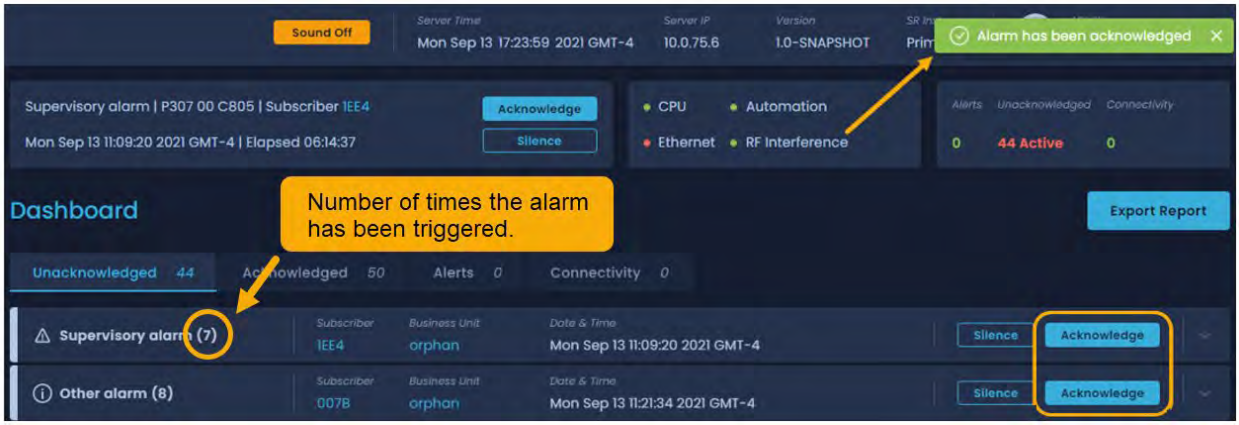
8. Processing Alarms

Clearing Alarms Manually

When alarm automation is enabled, no alarms display on the dashboard.

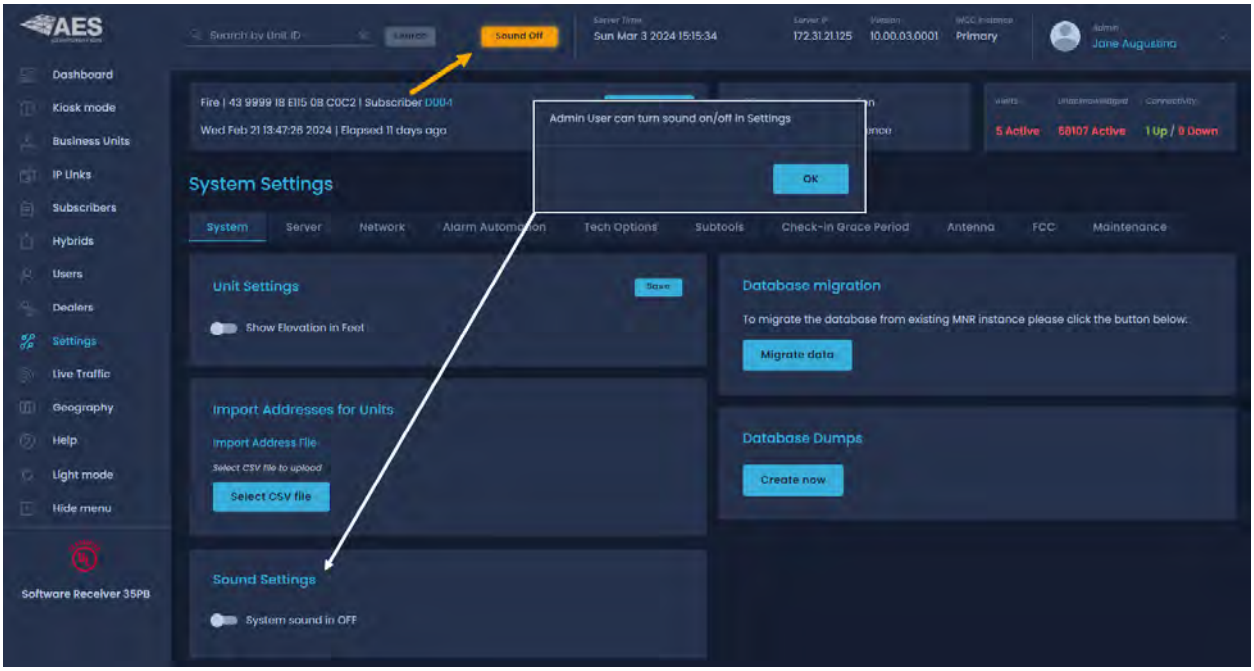
To clear an alarm manually, click the **Acknowledge** button. Once an alarm has been cleared, a green pop-up displays “Alarm has been acknowledged” as confirmation.

Note: The number next to the alarm indicates the number of times the alarm has been triggered.



Silencing Alarms

To silence an alarm, enable **System sound in OFF** (as shown below). Alarms can no longer be silenced by clicking **Sound Off**.



Onscreen Messages

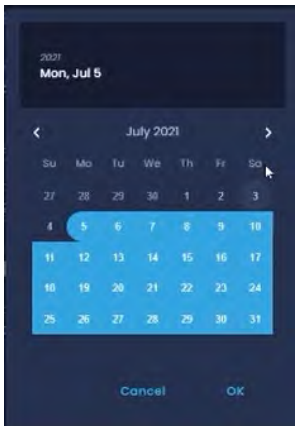
While using the INCC application, the following messages may be displayed. These messages will help you understand the software operating status and the actions you can take.

This is an error message ×	Application error has occurred.
This is an info message ×	A detail or additional information about an operation or feature is displayed.
This is a warning message ×	An action needs to be taken.
This is a success message ×	An action was successful.
Alarm has been muted ×	An alarm has been successfully silenced.
Alarm has been acknowledged ×	An alarm has been successfully cleared.

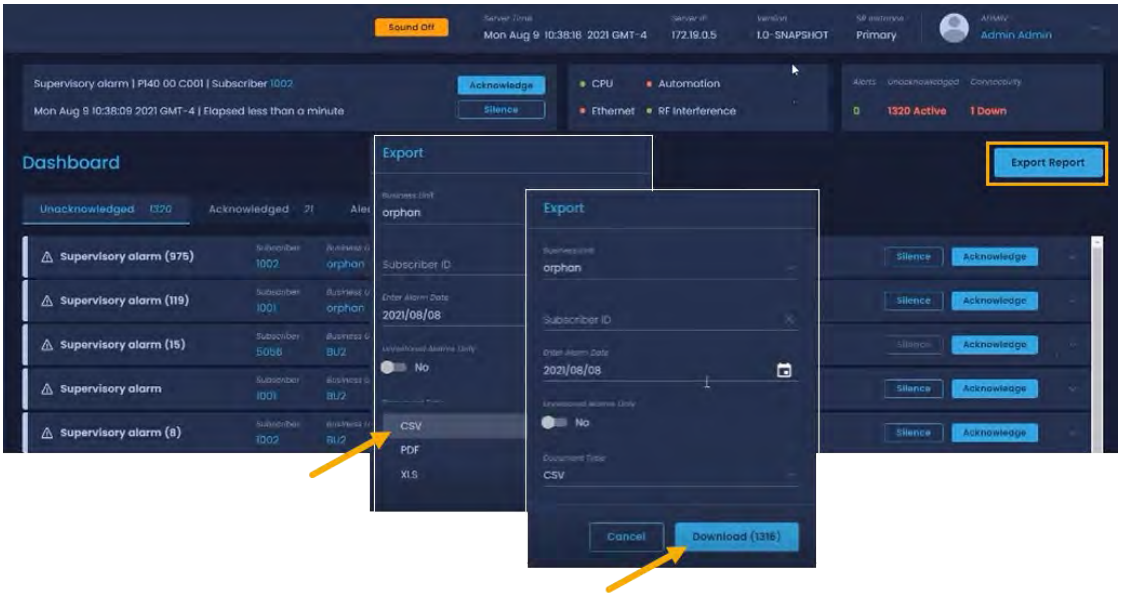
Exporting Reports

Reports can be exported to CSV, PDF, and XLS and can be customized based on the business unit and subscriber ID. A date range can also be set.

1. Click **Export Report**.
2. Use the **Business Unit** and **Subscriber ID** dropdown to specify what to include in the report.
3. Use the calendar icon to specify how far back the report should go. To make your selection, click any earlier date. The days between that date and the current date will be included in the report. Click **OK.**



4. Select a document type, then click **Download**. The download file displays at the top right of the browser.



9. Glossary

Name	Definition
Admin	Admin users can create, read, update, and delete Tier 1, Tier 2, and Tier 3. Admin users can see all data in all BUs.
AES Admin	AES Admin users can create, read, update, and delete Admin, Tier 1, Tier 2, and Tier 3. AES Admin users can see all data in all BUs.
Alarm	A signal from a subscriber or hybrid displayed on the Alarms tab of Dashboard. Can be either Acknowledged or Unacknowledged that splits Alarms between corresponding Dashboard tabs.
Alert	A signal from IP Link displays on the Alerts tab of Dashboard.
BU Statistics	Analysis tools under a particular business unit: • **Error! Hyperlink reference not valid.** • **Error! Hyperlink reference not valid.** • **Error! Hyperlink reference not valid.**
Business Unit	An aggregation entity that keeps and proceeds data for the set of assigned units: subscribers, IP Links, hybrids, and Non-AES.
Check-In	Each AES unit performs “check-ins” with the INCC at least once every 24 hours, which complies with the UL 864 standard for commercial alarm communications. The supervision check-in time can be set to as often as needed for the application.
CID Event Code	Unique code for every event received with Alarm/Alert. A CID code contains info about the unit ID, event type, zone configuration, and other data required for event recognition.
Connectivity	Dashboard tab that displays status of alarm automation.
Dashboard	Dashboard provides visibility into radio signal traffic and overall operation of business unit to ensure a high quality of service on a real-time basis. This dashboard displays critical business unit information in a dynamic and intuitive format to enable a quick assessment of the network’s performance and to quickly identify faults that could affect network operation and growth.
DB	Data Base that keeps all data for a particular INCC instance. DB data can be migrated from NMS/MNR.
Dealer	Aggregation entity that keeps a set of subscribers. The dealer can be assigned to a user, and then this user will have access to all subscribers belonging to that dealer.

Name	Definition
Default Business Unit	INCC instance should have at least two business units: Default to proceed data from assigned units, and Orphan to proceed data from unassigned units.
Check-in Grace Period	If set, supervised units checking in will be allowed the grace period after the expiry—before being declared dead.
Fault	Event sent by unit that has issues (antenna cut, battery, and so on).
Frequent Check-Ins	Each subscriber normally transmits check-in messages at regular, pre-set intervals. AES recommends setting the subscriber check-in interval to 23:45. A shorter time interval increases RF traffic in the network, which is why the INNC provides list of check-ins for all units.
Geo Page	Interactive map that displays all units that have coordinates. Geo Page can display data for one BU at a time.
Geocoding	INCC automatically checks and updates the units that have an address, but don't have latitude and longitude coordinates. Also, INCC can validate addresses (on demand).
Health Score	The Network Health Score quantifies overall network operational quality on a scale between 0–100.
Hybrid	An AES unit that can work as a subscriber and as an IP Link.
INCC	Intellinet Control Center. AES Application that can replace MNR and NMS both.
Installer	A software installation package that deploys INCC to a new instance.
IP Link	An AES unit that gets radio signals from subscribers and transmits them to the Internet.
IP Links / Hybrids Load	Ideally, all IP Links in the network should handle roughly equal volumes of RF traffic. (This generalization does not apply when the antennas of two IP Links are deliberately placed within RF range of each other; for example, at a Central Monitoring Station.) Tips for increasing RF traffic handled by an under-utilized IP Link are locate here.
IP Control	IP Control is an internal tool for viewing routing tables.
Kiosk Mode	A set of predefined widgets to visualize the current state of a business unit, usually on large screens.
Late Check-ins	Each subscriber normally transmits check-in messages at regular, pre-set intervals. If the MultiNet Receiver does not receive a check-in message at the expected time, there might be a problem with the

Name	Definition
	subscriber; alternatively, there might be a problem with network performance.
License	INCC license is provided for one instance (for both primary and secondary). A tier 1 license can keep up to 5000 units; a tier 2 license is unlimited.
Line Card	AES's Ademco 685 emulated output format can provide output using at least nine line cards. For example, the INCC can receive signals directly from subscribers via TCP/IP. This is referred to as MCT or Multiple Communication Technologies. To distinguish between messages that arrived via RF through an IP Link and directly through IP, a different line card is assigned.
Link Layer	The link layer defines how many hops a subscriber takes to reach an IP Link. A link layer of two indicates there is one subscriber between the subscriber the reading is being taken from and the IP Link.
Live Traffic	Live Traffic is a constantly updated list of all events produced by all units under an INCC instance. Also, every particular unit has a Live Traffic tab that displays its own events.
Mesh	Mesh networks built using patented AES-IntelliNet technology consist of many subscriber units installed in concentric rings around an IP Link, which is a major component.
Mesh Ack-Delay	Normally, after a subscriber transmits an RF packet, the recipient of the packet returns a message to the sender, acknowledging receipt of the packet. If the issuing subscriber does not receive the acknowledgement message within the configured Communication Timeout Delay period, then it indicates in a subsequent message that an Ack Delay has occurred.
Mesh Hops	When a subscriber transmits an RF packet, that packet travels through the mesh network to an IP Link or a hybrid subscriber before reaching a INCC/MultiNet receiver. If the IP Link is within direct reach, the subscriber sends the packet to the IP Link; otherwise, it sends the packet to another subscriber along a route leading to the IP Link. Each step in the route from subscriber to IP Link or hybrid subscriber is called a hop. As network conditions evolve, the route, and consequently the number of hops from a given subscriber to an IP Link, can change.
Mesh NetCon	NetCon is a measurement calculated by a subscriber to determine the level of confidence that its transmissions will reach an IP Link. Only fire

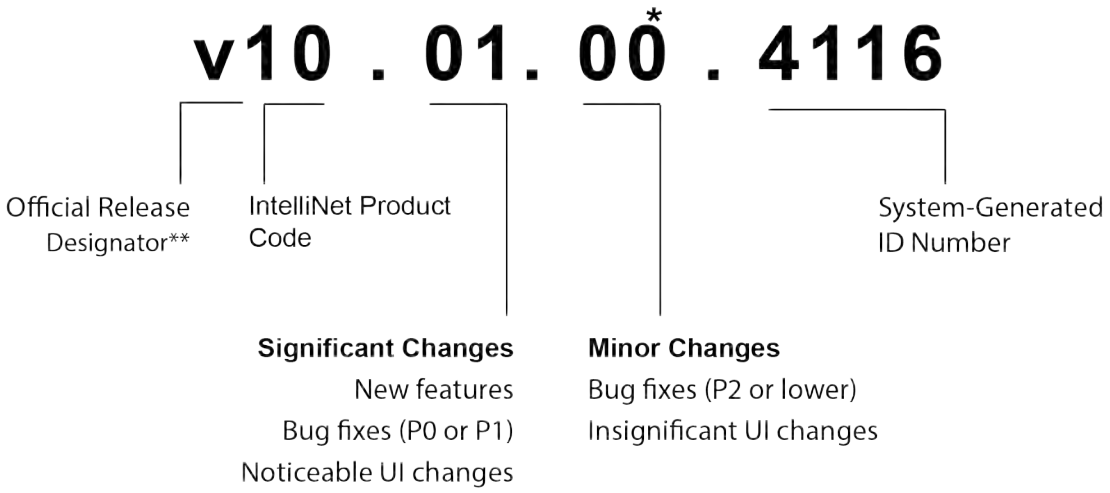
Name	Definition
	subscribers report their NetCon statuses, as either high or low, in messages sent to the INCC/MultiNet receiver. In general, NetCon is an abbreviation for Network Connectivity. It is a rating of the number of radio frequency (RF) paths from a subscriber to other subscribers installed in the mesh network. The mesh refers to all the subscriber units on a network of the same frequency and cipher code.
Migration	Database migration allows a seamless transition from an existing MNR to the INCC. During migration, MNR DB dump data is transformed and put into the INCC database.
MNR	AES MultiNet receivers are built to receive all alarm signals from the AES mesh network via IP Links, hybrid subscribers, and MCT subscribers. The receiver's robust hardware processes and forwards all alarm information to the central station alarm automation software.
Network Pulse	The Network Pulse dynamically tracks key performance indicators including subscriber check-ins and Acknowledgment delays over the most recent 10-day period.
NMS	Network Management System interfaces with the MNR to provide a complete end-to-end mesh radio network monitoring and management platform. Unlike other communication technologies, the NMS tool was developed to give users full visibility of a network and its performance via real-time dashboards, notification alerts, and map visualizations.
Non-AES Unit	Custom object that can be added under a particular business unit by the admin. Non-AES units can be displayed on Geo Page, but the INCC is not able to process any data from non-AES units.
Orphan	An INCC instance should have at least two BUs: Default to proceed data from assigned units, and Orphan to proceed data from unassigned units.
Path	Alarm signals transmitted from a subscriber will be repeated and acknowledged by other subscribers within its routing table. The signals will travel through the mesh network via the shortest path available to an IP Link. The IP Link receives and acknowledges the alarm signal.
Permission	All user roles have flexible permission settings that can be managed by admins.
Primary	Main INCC instance. All data is being constantly synced to the secondary.

Name	Definition
Recipient	The INCC supports sending notification to persons not registered as an INCC user. Notification is initialized by Trigger. A recipient can be added to BUs by the admin.
Restoral	Specific code that says the alarm/alert is fixed.
RF	Radio frequency—the main channel for radio subscribers.
RF Interference	Radio frequency interference is the conduction or radiation of radio frequency energy that causes an electronic or electrical device to produce noise that typically interferes with the function of an adjacent device.
Role	The set of permissions. The INCC has an AES admin role and four user roles: • Admin • Central Monitoring Station Admin (CMS Admin)/tier 1 • Manager/tier 2 • Operator/tier 3 A user can see other users and their data only if the other roles are lower.
Route	See Path.
Routing Table	A routing table exists for each subscriber on a network. It can contain up to eight viable transmission routes. The routing tables are visible only via a handheld programmer or through IP control. Routes, also known as paths, are what subscribers will depend on to deliver alarm signals back to the central monitoring station. This table is dynamic, meaning that as conditions change (i.e., other subscribers have troubles or are removed from the network), the table changes and other subscribers are entered into the list. The best route is always first on the list.
Secondary	Standby INCC instance to keep the system up if the primary is down.
Service Log	Occasionally, subscribers may require service, and this log identifies all the subscribers in need of service.
SMNR	Software MultiNet Receiver, another name for the INCC.
Subscriber	Hardware unit that monitors fire or burglary and sends signals to the INCC.

Name	Definition
Subscribers over time	This chart displays how many signals the INCC received from every model of connected subscribers.
Tier 1	Role: central monitoring station admin (CMS admin)
Tier 2	Role: manager
Tier 3	Role: operator (this role can access only one BU)
Top Repeater	To convey packets along their route toward an IP Link, it's normal for some subscribers to repeat RF packets originating from other subscribers. However, excessive packet repetition by a single subscriber may reduce network efficiency and cause delays.
Top Talker	Ideally, all subscribers in the network should generate roughly an equal numbers of RF packets. Excess RF traffic from a single subscriber may reduce network efficiency by consuming airtime. Tips for reducing excess activity on a subscriber are described here.
Total Signals Received	A business unit statistics chart that displays the number of signals received from all units.
Trigger	Trigger is a customizable event to send a notification to recipient.
TTL	Time to Live period that can be set for check-in, status, alarm, trouble, and restoral.
UL	The UL enterprise is a global safety science company that provides certification of safety standards.
Unit	AES/non-AES hardware module.
Updater	Software installation package that provides seamless update for an existing INCC.
User	A registered person who has access to the INCC.
Zone	Adjustable hardware part of subscriber/hybrid.

10. Version Control Schema

AES has established the following version control schema to align itself with contemporary software development practices and to provide greater consistency and visibility into software releases. The software recevier version number begins **v10**, followed by other digits. The details on version identification are described in the diagram below:



* The second, third, and fourth decimal places increment beginning with the number 1 and will always be represented as a whole number. The third decimal place has a leading zero, whereas the second and fourth decimal places do not have leading zeros.

** Other designators are used internally to distinquish between the alpha and beta releases ("a" versus "b"). Development releases, designated by an "x", are also used internally.

AES CORPORATION
TECHNOLOGY LICENSE

TECHNOLOGY LICENSE

Certain AES products include software, protocols and other proprietary and confidential technology and trade secrets of AES, which are incorporated in or provided with AES products solely for use in conjunction with and to operate AES products ("**Licensed Technology**"). AES grants the original recipient a non-exclusive license to use such Licensed Technology solely for the use and operation of AES Products and for no other purpose or use whatsoever. No title or ownership in or to any such Licensed Technology is conveyed by the sale or delivery of any AES products; all such rights are retained by AES.

AES SERVICE PROCEDURE

For warranty claims, a Return Material Authorization Number is required. Please contact AES by Phone (978) 535-7310, Fax (978) 535-7313 or Email rma@aes-corp.com, to receive a Return Material Authorization Number and have the AES part number and serial number ready.

Once you receive the Return Material Authorization Number, repack the equipment in its original or equivalent packaging. Inside the box, please include a contact name, telephone number, address and a brief description of the reason for return.

Ship items freight-prepaid to:

Repair Services, RMA#

AES Corporation,

285 Newbury Street

Peabody, MA 01960 USA

(Contact AES for Return Material Authorization number)

April 2019

2564727v1/7106-1