Appendix
IntelliNet® Network Control Center (INCC)
Installation, Configuration, and Operations Manual, 4th Release

Contents

Fourth Release INCC Features

Password Expiration Settings — Settings Page > System Tab

Security feature to force users to change their password. Configurable for 1–365 days.

Token — Settings Page > System Tab

Security feature to sign user out of INCC application. Configurable between 8–720 hours.

Two-Factor Authentication — Settings Page > System Tab

Two-factor authentication is an identify and access management security method that requires two forms of identification to log in. Google authenticator steps are as follows.

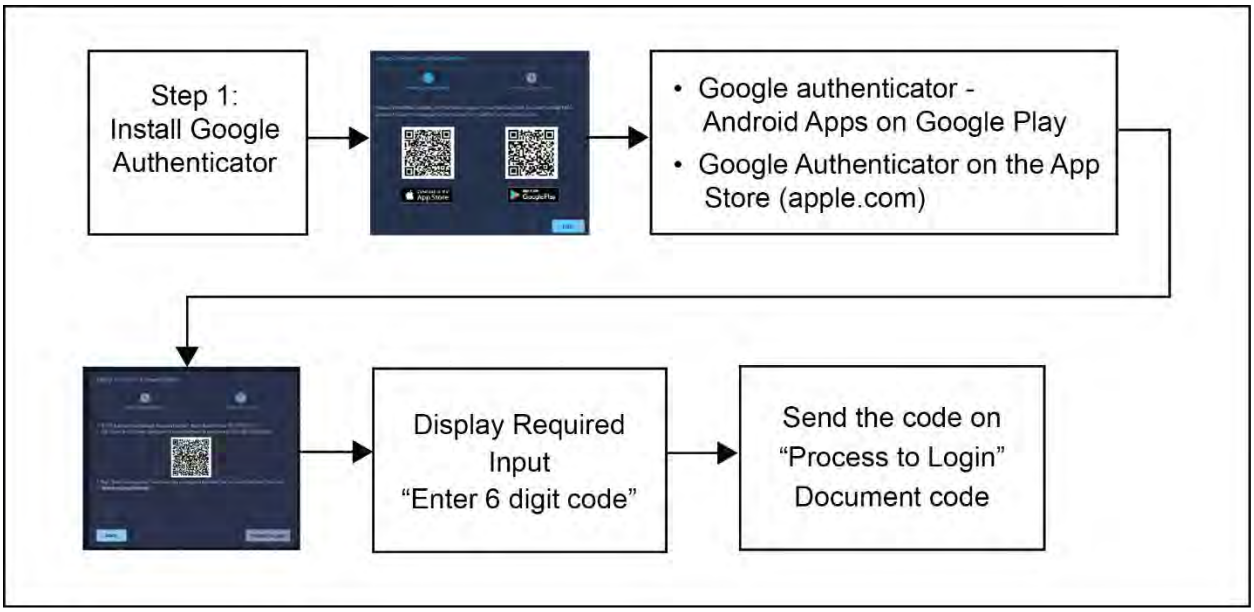
How to Install and Use Google Authenticator App on Android

1. Visit the Google Play Store and search for Google Authenticator to download the app.
2. Tap **Install**.
3. Open the app and tap the + to add a new account.
4. Scan the QR code provided by the service, or manually enter the setup key.
5. Open the app whenever you need a 2FA code.
6. Input the code displayed next to the account name when prompted during login.

How to Install and Use Google Authenticator App on iPhone

1. Visit the Apple App Store and search for Google Authenticator.
2. Tap **Get** to install.
3. Open the app and tap + to add accounts.
4. Choose **Scan QR code** or **Enter setup key**.
5. Scan the QR code or manually enter the setup key for the account.
6. The codes are displayed alongside your account names, and you can use them when required for 2FA.

Flow of Steps for 2FA



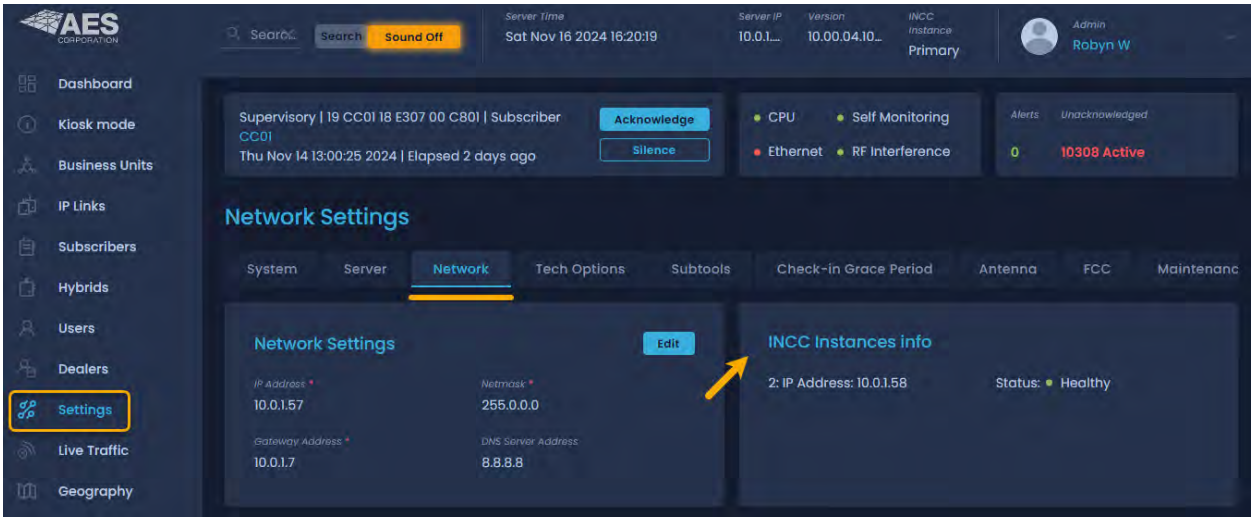
Primary Traffic Management — Settings Page > Network Tab

Manually push traffic to secondary. This will be used by AES technical support for upgrades and troubleshooting.

Third Instance — Settings Page

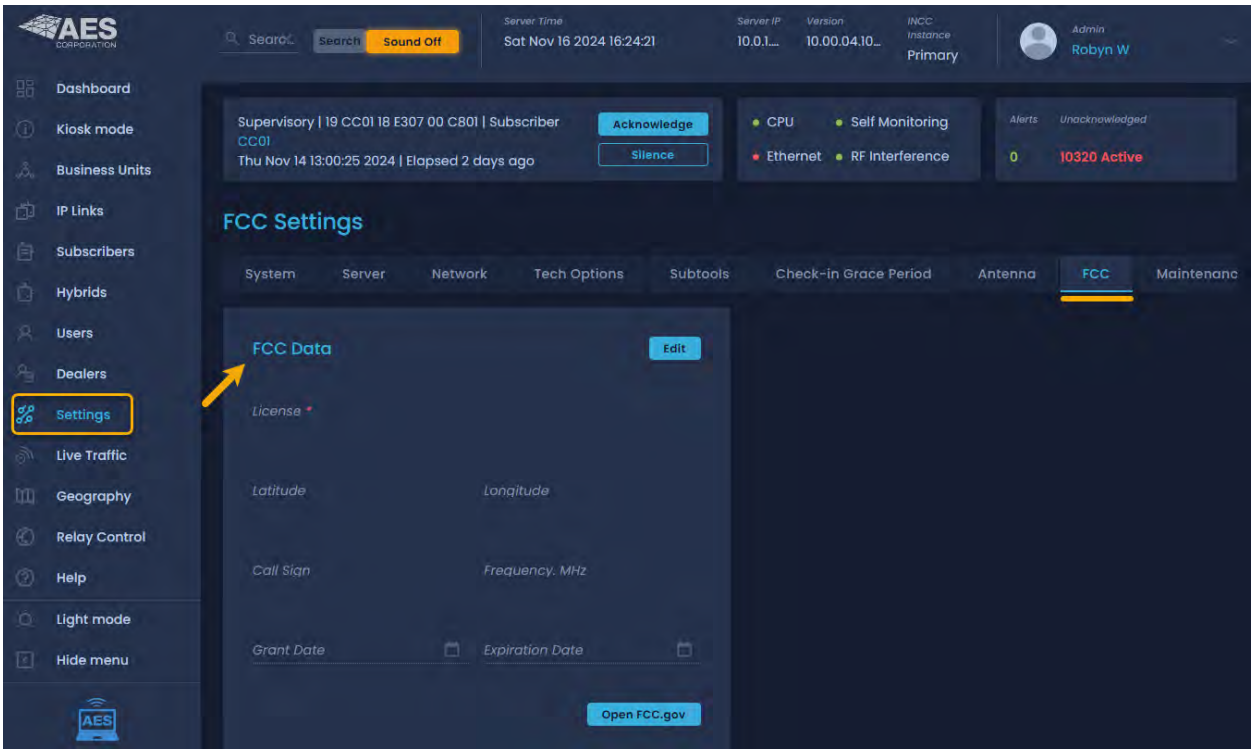
This is the disaster recovery instance that will be available if the customer has this feature enabled. To activate this feature, the customer must contact AES Sales to acquire a license and technical support.

If the third instance of the software has been installed and the license has been activated, the Network tab under Settings displays the third instance and the associated IP address.



FCC — Settings Page

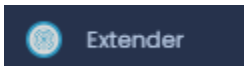
Placeholder to document FCC documentation, enabling customers to easily keep track of the FCC license.

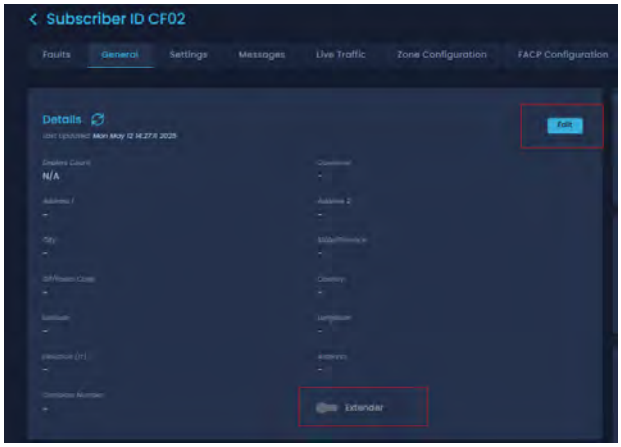


Extender Option to Add in GUI

Navigate to General page of subscriber. Click edit at top right and enable extender icon below.

Once enabled, this icon will show up on GEO page with this icon.



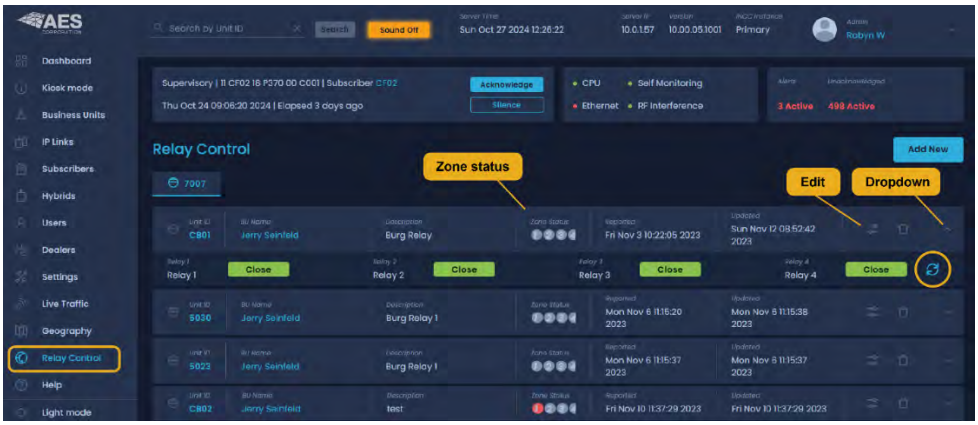


Relay Control — Tab on Left

This feature is used with AES Product 7007P-RB4. [AES 7007p-rb4]

Gives ability to control 4 zone relay board that enables sensors to control connected devices.

- Zone status shows active status of relay.
- Dropdown shows open, closed status, and refresh button.
- Edit configuration allows user to show red/green depending on if relay is triggered to open/close, etc.
- Setup of further relays is done in the RB4 GUI of the subscriber.



*Compatible with normally opened, normally closed sensors.

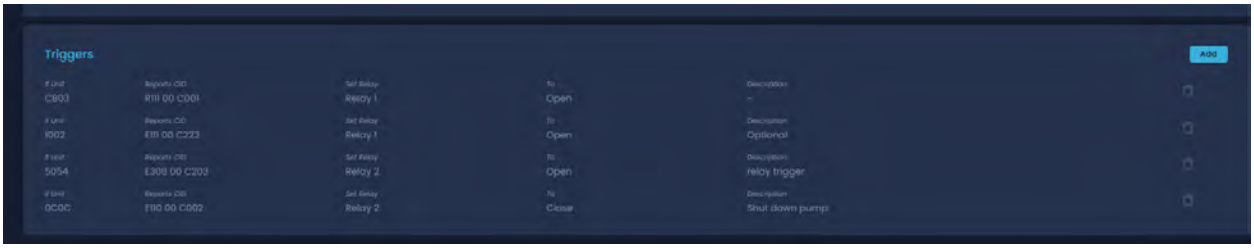
Relay Triggers

This feature allows configuration to trigger a relay to open or close state IF a specific fault is reported on another subscriber ID. Subscriber ID can be itself or another subscriber within same Business Unit.

Configure Following Fields:

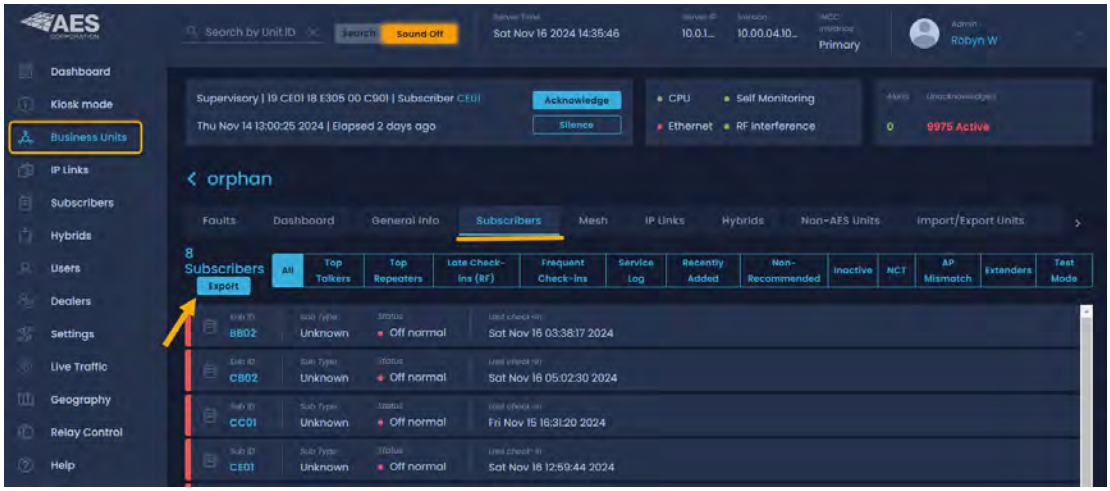
- CID Fault (Include E,R,P)
- Area (2 Digits)
- Zone (3 Digits)
- Set Relay (Select Relay 1-4)
- Set Position to Change (Open or Close)
- Description

Once you select save, will see list of Triggers below relays:



Business Unit Page — ability to export all reports

Exports as a CSV file for customer to download and view.



Dealer Import File

Dealer import file requires latest NMS version: 9.0.5.4729

Navigate to Tech Options on NMS click “Download File”

If not on the latest NMS, it will require AES Tech Support to login to run script to create download file.

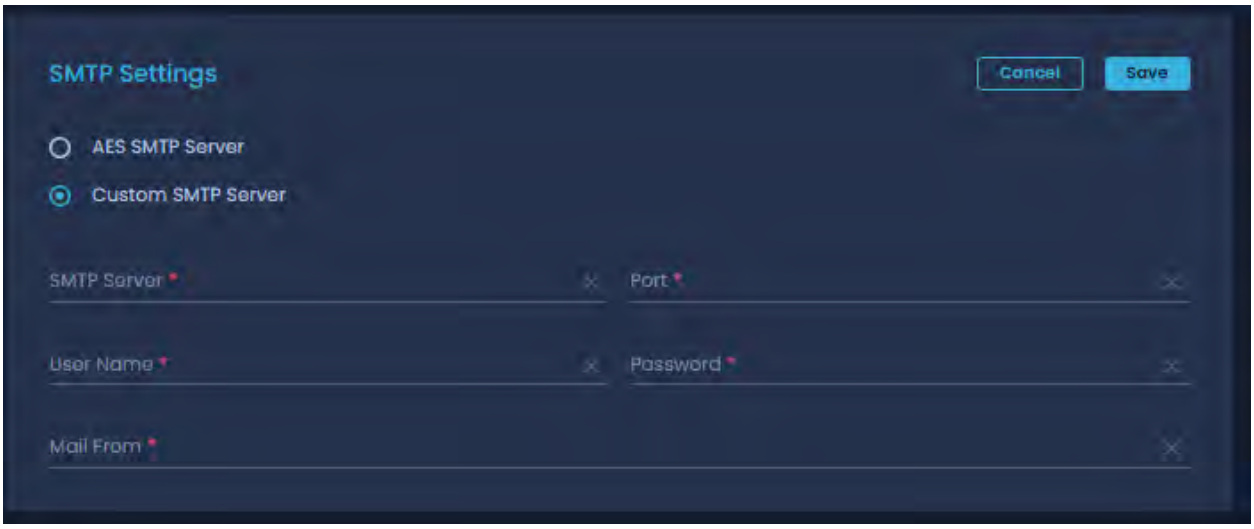
Global Top Talkers Top Repeaters for All BU’s

Added this feature under global subscribers to identify all top talkers/repeaters in single page below:

SMTP Settings

Ability to configure SMTP. By default, AES SMTP will be selected. Need to navigate to Settings > System > SMTP Settings to configure fields below:

- SMPT Server
- Port
- User Name
- Password
- Mail From



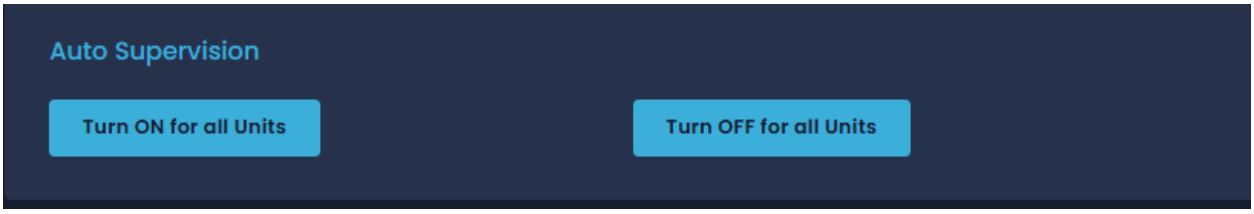
Auto Supervision

1. This section allows you to globally enable or disable the *Auto Supervision* feature for all units at once.

- **Turn ON for all Units**
  Click this button to activate Auto Supervision on all connected units simultaneously. This ensures each unit automatically monitors and reports its operational status as configured.
- **Turn OFF for all Units**
  Click this button to deactivate Auto Supervision on all units. This disables automatic status reporting and monitoring across all devices.

2. **Note:** Use this feature carefully, especially when disabling supervision, as it may affect unit status visibility and automated alerts.

Navigate to: “System Settings > System”



Replicate all data to Primary

This feature allows you to manually initiate a full data replication from the **Secondary** instance to the **Primary** database.

- **Start now**
  Pressing this button will immediately replicate all current data from the secondary instance and **overwrite the existing data** on the primary database.

  ⚠️ **Warning:**
  This operation will permanently overwrite all data on the Primary instance with the data from the Secondary instance. Ensure that the Secondary database contains the correct and intended data before proceeding.

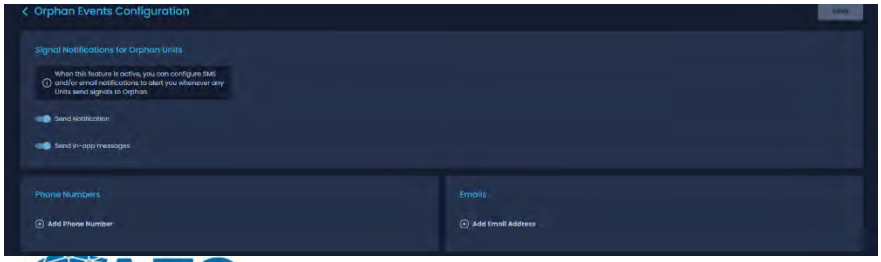
Use Cases:

- Recovery after primary database corruption
- Promoting a previously secondary instance to be the new source of truth
- Manual sync for troubleshooting or data alignment

Instance Level Notifications

Ability to create trigger if any traffic hits orphan. Orphan traffic is event traffic from subscribers that are not configured properly. They are not hitting specific BU and will not be mapped correctly in Alarm Automation. They should be addressed and resolved to not miss alarms.

Can configure phone number or email below to receive this notification:



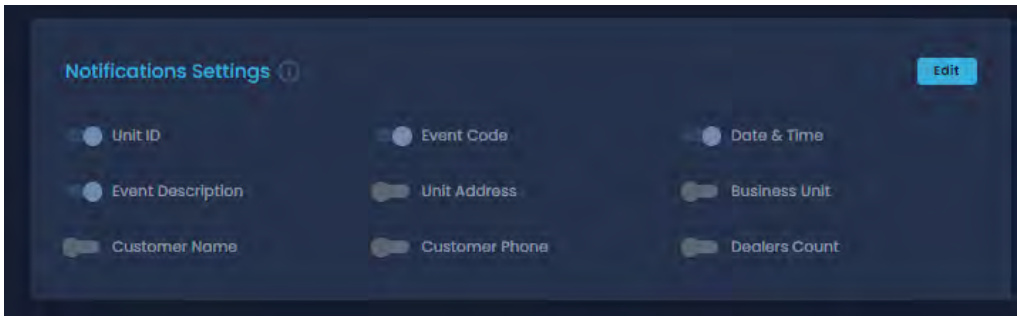
Protocol HTTPS to HTTP

Optional: Configure a manual redirect from HTTPS (port 443) to HTTP (port 80) by modifying your web server settings. This allows users accessing the secure URL to be redirected to an unencrypted connection. (Located under “Server Settings > Server”

Notification Settings

Ability to configure what information to show on email and or text notifications sent out.

- Unit ID, Event Code, Data/Time, Event Description, Unit Address, Business Unit, Customer Name, Customer Phone, Dealer Count

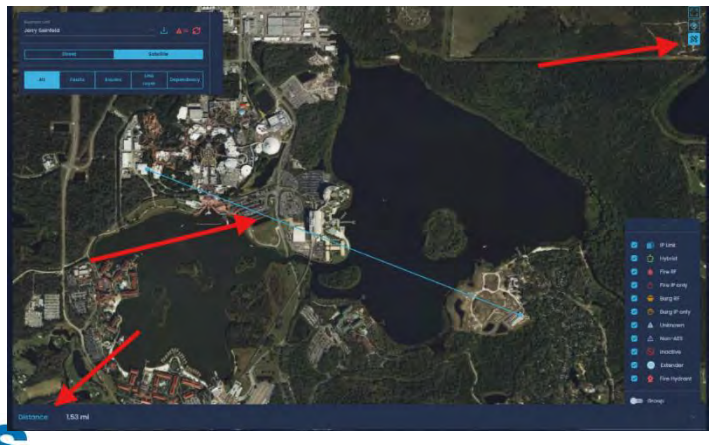


Geography Improvements

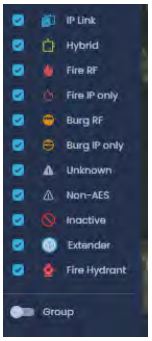
Page Ruler

Need to click ruler icon on top right of Geography Page.

Click two points and distance will show up on bottom tab.



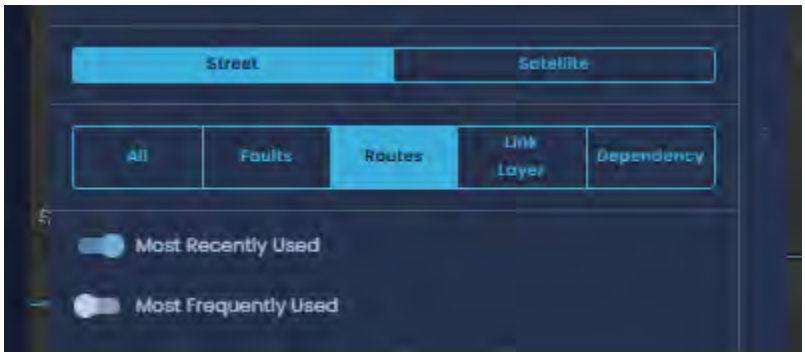
Updated Legend



- Extender – AES released new product 7207.
- Fire Hydrant – Ability to add equipment
- Group – Ability to enable/disable grouping of Subscribers

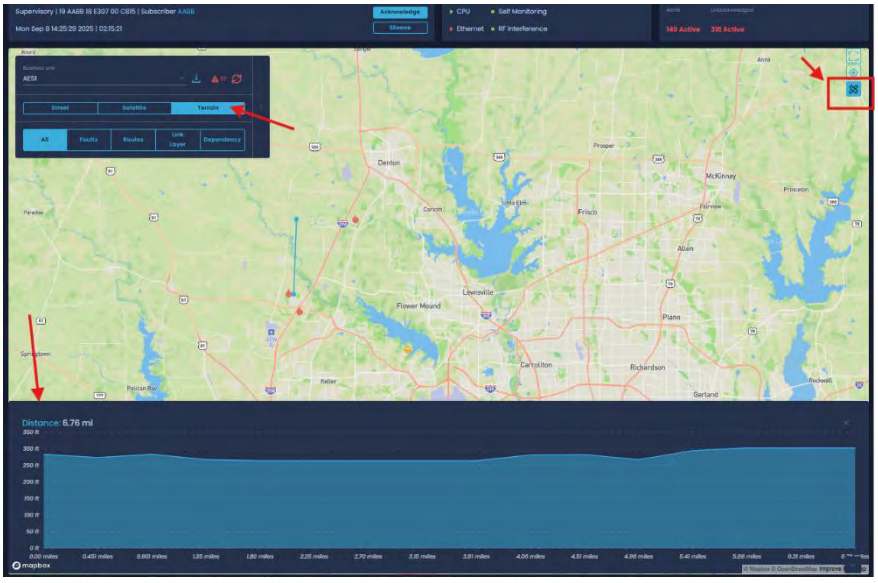
Routes

Ability to see most recently most recently used vs most frequently used



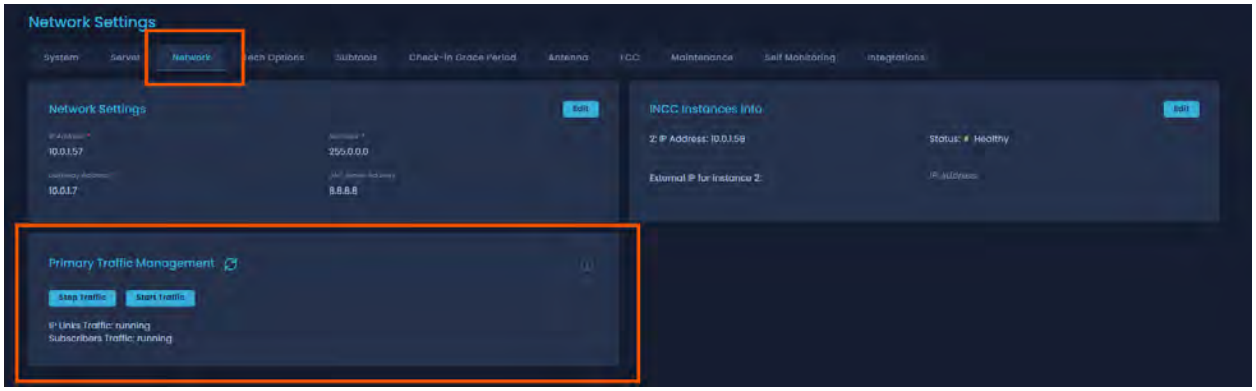
Elevation Profile

Ability to see elevation between points. Select terrain map and click ruler in upper right.



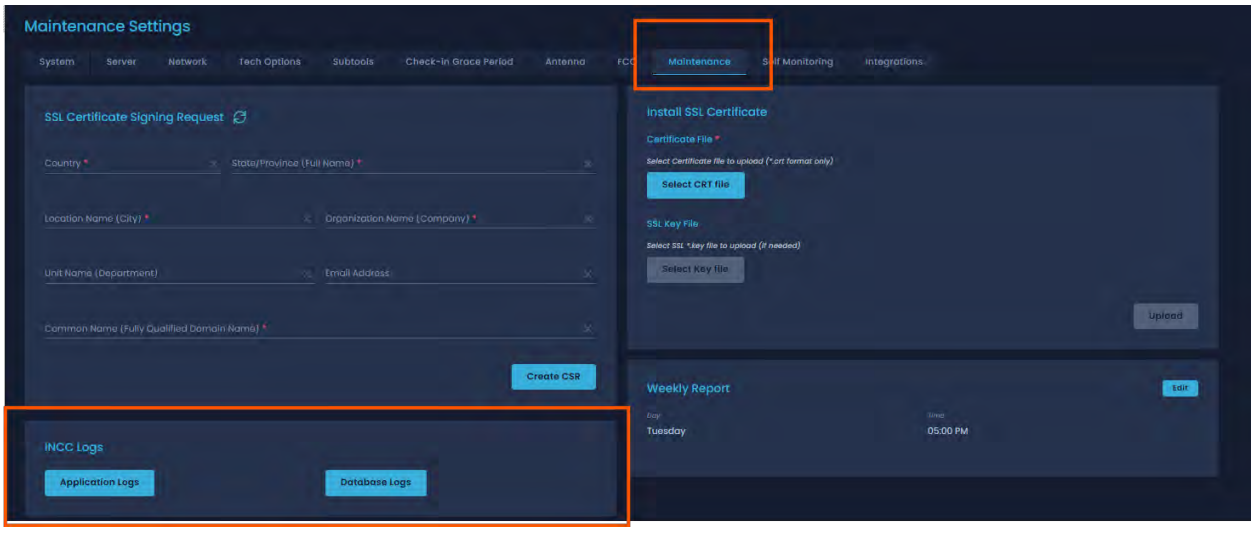
Primary Traffic Management

Ability to start & stop traffic gracefully from Primary to shut down INCC. Also can be used for testing purposes to validate secondary is Alarm Automation is working as expected upon install or changes to configuration.



INCC Logs

Ability to grab INCC logs from GUI. Used for Tech Support and Troubleshooting Purposes:



Integration Settings

Third party application to be added via http API. Configure Event Triggers to be sent to third party application.

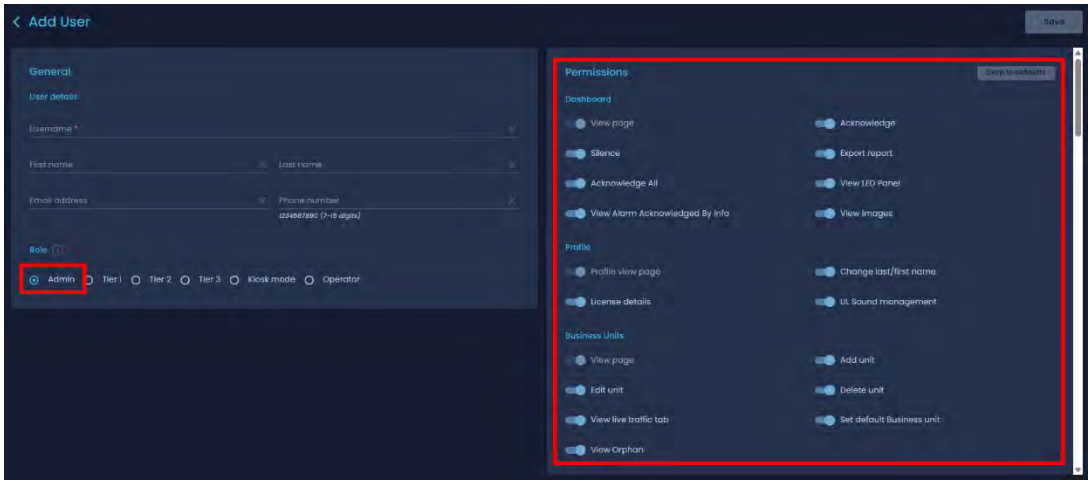
User Permissions

INCC has 6 user roles:

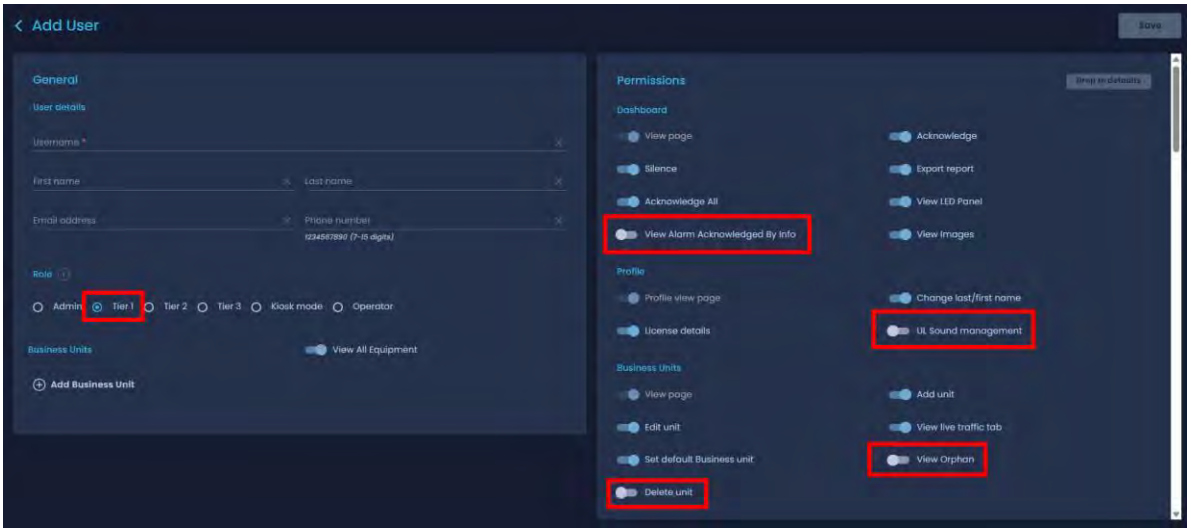
Admin, Operator, Tier 1-3, and Kiosk Mode

All permissions are available for every role; however, each role comes with a default set of permissions tailored to its specific function

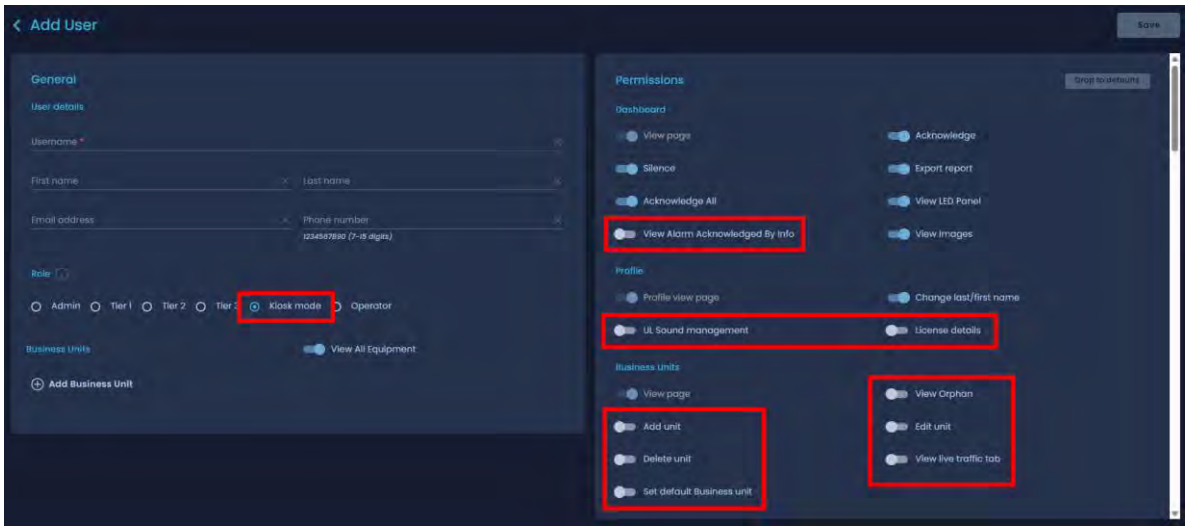
Admin:



Tier 1:



Kiosk:



SIA Support

Description: Customers requested SIA support. AES implemented SIA DC-03-2017. "SIA Format" Protocol for Alarm System Communications. (This standard includes SIA CD-07 & SIA DC-09)

SIA Level 1 was implemented and provides support for following compatibility:

Table 3 — Compatibility Levels

(SIA Level Information is not automated. Refer to the product documentation or inquire of the manufacturer.)

Level 1	*Level 2*	*Level 3*	*Function or Capability*	*TRANSMITTER[A]*	*RECEIVER[A]*
√	√	√	Support Tonal Acknowledgements	Required	Required
√	√	√	Support N Blocks with Zone Numbers Only	Required[B]	Required
√	√	√	Support Single Account Block per Call	Required	Required
√	√	√	Support O Blocks	(optional)[B]	Required
√	√	√	Support X Blocks	(optional)	Required

Future efforts will be made to address further support on Level 2 & 3 Items below:

√	√	√	Support 300 Baud (FAST)	(optional)	Required
	√	√	Support Configuration Block	required	Required
	√	√	Support Data Acknowledgements	required	Required
	√	√	Support Modifier Codes	(optional)	Required
	√	√	Support Multiple Account Blocks per Call	(optional)	Required
	√	√	Support E Blocks	(optional)	Required
	√	√	Support 1 (Wait) Block and 2 (Abort) Block	(optional)	Required
	√	√	Support Data Codes with Units Numbers	(optional)	Required
		√	Support RECEIVER call out and Access Passcode	required	Required
		√	Support Reverse Channel C Blocks	required	Required
		√	Support Reverse Channel P Blocks	required	(optional)
		√	Support Reverse Channel A Blocks	(optional)	Required
		√	Support Dynamic Block and Group Sizes	(optional)	Required
		√	Support Listen-in Block	(optional)	Required
		√	Support A Blocks to RECEIVER	(optional)	Required
		√	Support V-Channel Communications	(optional)	(optional)
		√	Support Video Block Communications	(optional)	(optional)

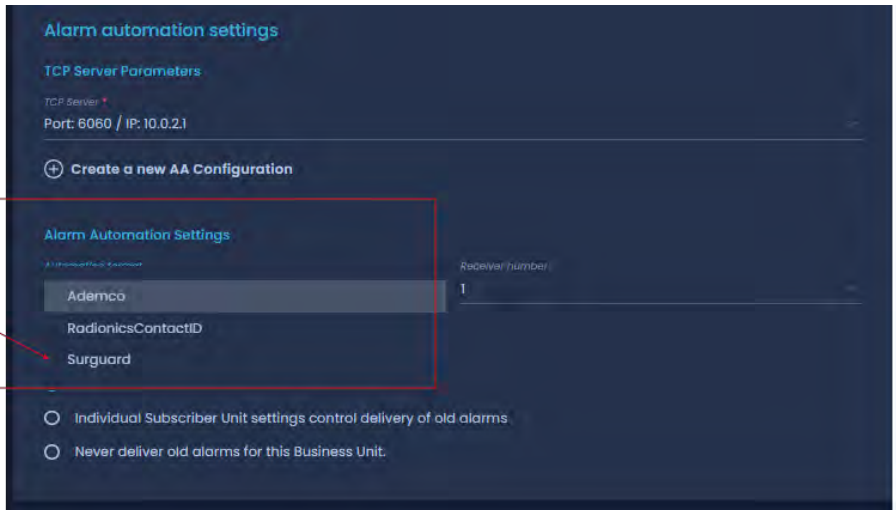
[A] For Reverse Channel, Receiver capabilities apply to transmitter

[B] Not all data code types need to be supported by TRANSMITTER. Individual subsets allowed.

Required to change automation output in INCC under Business Units > General Info > Alarm Automation Settings > Automation Format

INCC support 3 outputs:

1. Ademco CID
2. Radionics CID
3. Surgard



Once you select this format, required to notify Alarm Automation of this change. This will format output to match string below:

5RRLLLs18AAAAQXYZGGCCC[DC4]

Char values below:

5	: Protocol number.
	5 = CID
	S = SIA
	1= Basic Signal Protocol
	6 = Radionics
RR	: Virtual Receiver number.
LLL	: Virtual Line number.
s	: Space.
18	: Contact-ID format identifier. (98 can also be used)
AAAA	: Four digit account codes.
Q	: Qualifier, E= New event or opening,
	R= New restore or closing.
	P= Previous event
XYZ	: Class code and event codes.
GG	: Group Number
CCC	:Zone codes or user ID
[DC04]	:Terminator, 14 Hex

Self-Monitoring

Overview

The INCC can be utilized to acknowledge alarms from the dashboard page for self-monitoring applications. The Dashboard page is where all requisite data is brought together in one view to easily manage alarm types. Just click the icon at the end of each row to view the date and time, subscriber ID, event codes, tracking number, business unit, alarm type, and notes.

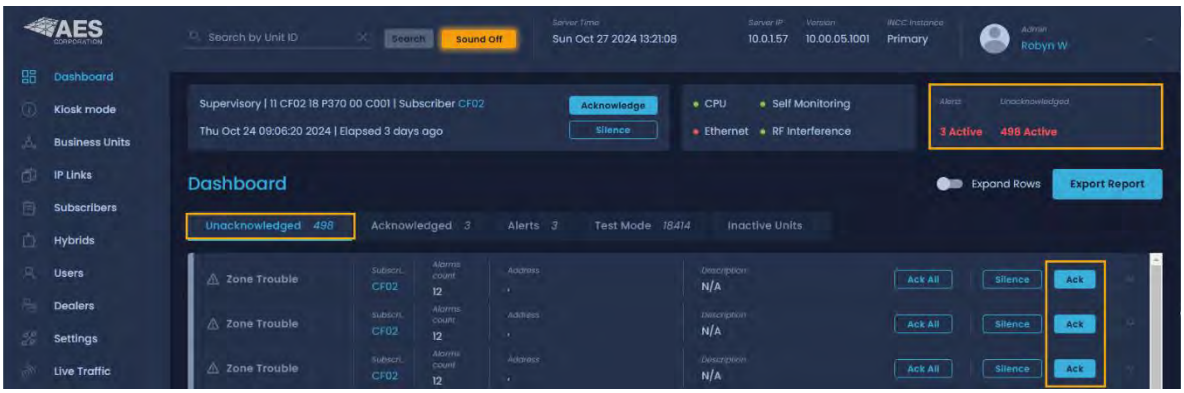
Dashboard

Acknowledging Alarms

To monitor alarms, use the **Ack** button from within the Unacknowledged tab. Alarm acknowledgement is indicated at the top right in red text.

Additional information on dashboard page:

1. Notes – Custom Notes that are added
2. Customer Info – Show Address, Name, Phone #, Email, Notes for Point of Contact
3. Geo Data – Navigates to Geo page to show locatin of subscriber on map

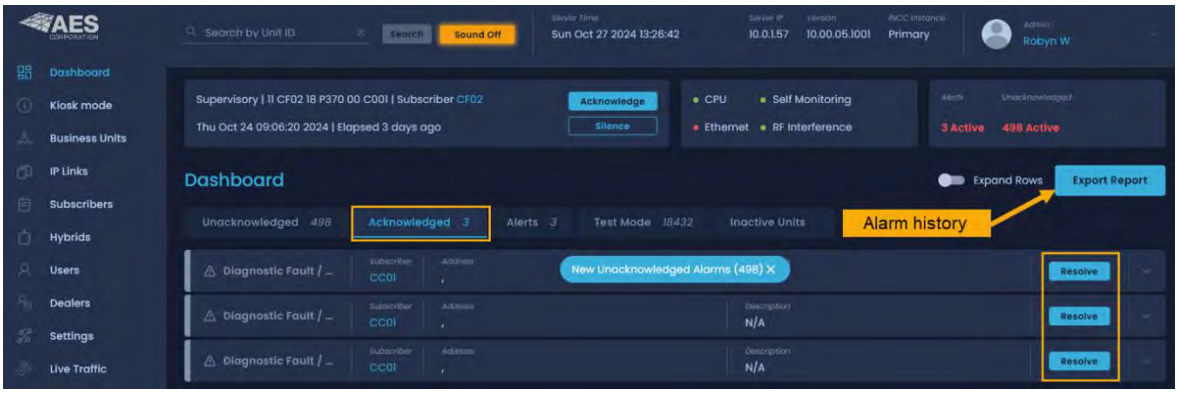


4. View Images – Show all associated images added

Unacknowledged Page

Once acknowledged, alarms go into the Acknowledged tab where the events stay for 24 hours before the INCC removes them. You can also go into this screen and click **Resolve** to remove them immediately.

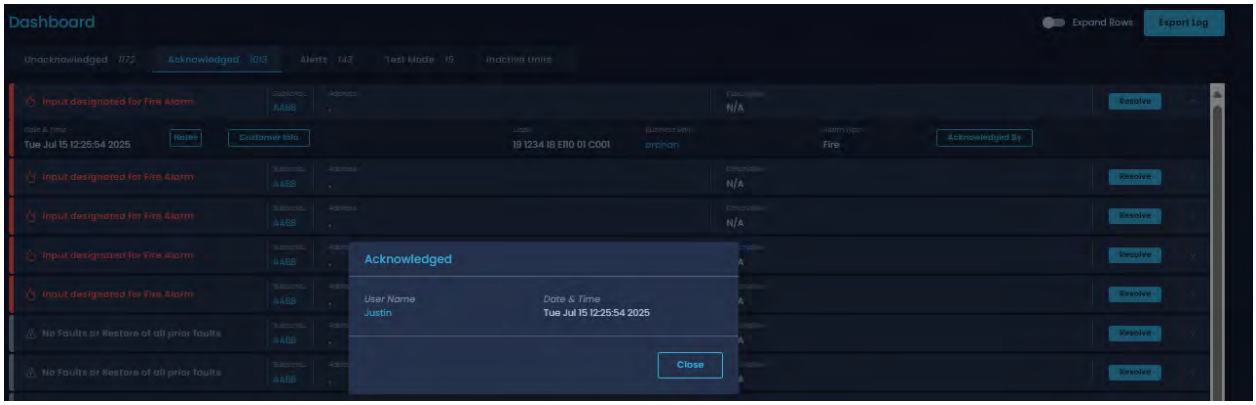
For alarm history, click **Export Report** or go to an individual subscriber to see event history.



Audit Trail for Acknowelded Events

Once events are acknowledged, they will go to acknowledge tab.

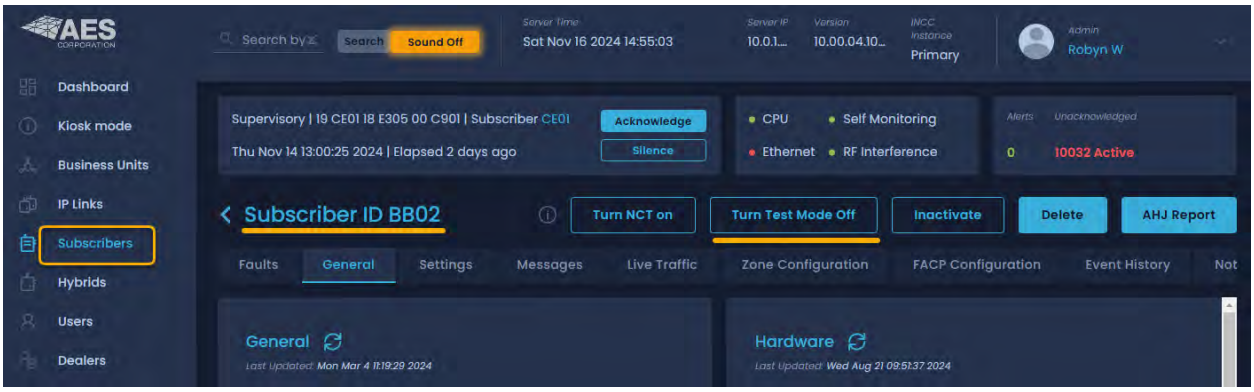
On this tab we will show acknowledged by tab below that will show stakeholder and time this event was acknowledged. **(Export available for past 30 days in top right corner)**



Test Mode

Subscribers or events that are configured to test mode are displayed on the Test Mode tab. **They will not show up on the Unacknowledged tab if test mode is enabled.**

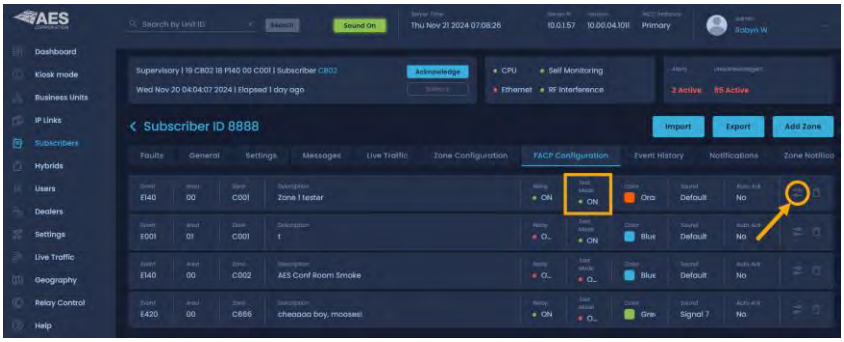
To access the list of all units under test, click **List Units** at the right.



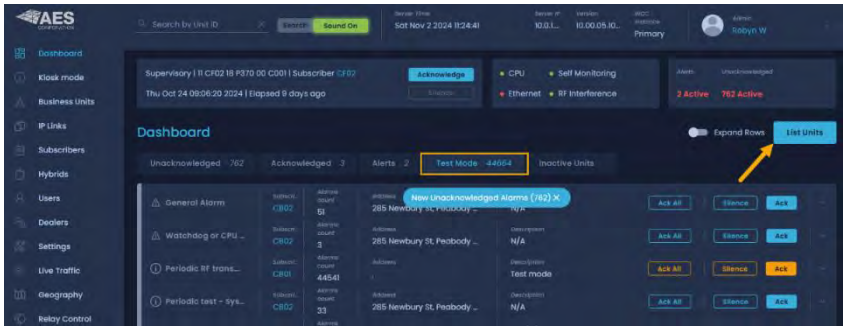
The subscribers under test mode are displayed:

Units must be disabled from test mode or the events must have test mode disabled.

Step 1



Step 2

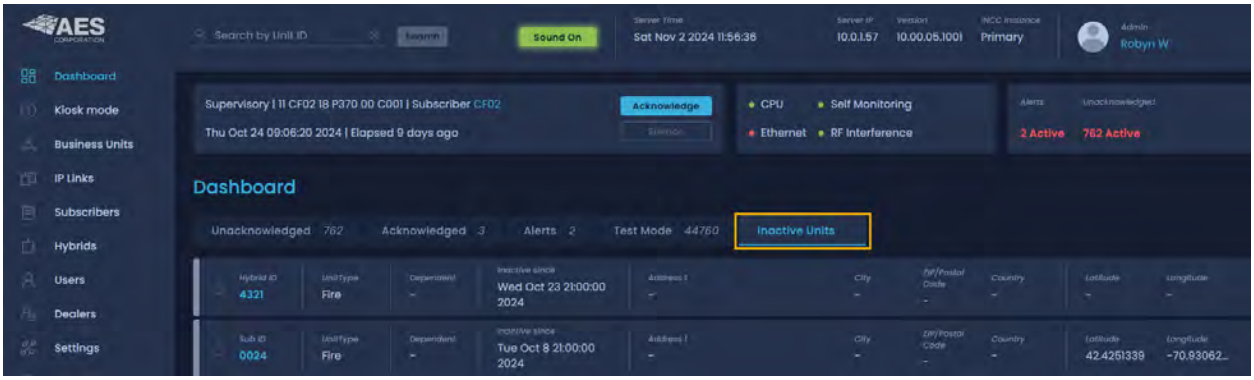


Step 3

Events are disabled by default when the zone is configured. Events that had been enabled can be disabled by navigating to the FACP Configuration tab and clicking the edit icon shown below, then toggling Test mode to off.

Inactive Units

The Inactive Units tab displays all inactive units. Inactive units can be manually pushed to inactive, or if a subscriber does not check in for 10 days, a unit is pushed to this table.

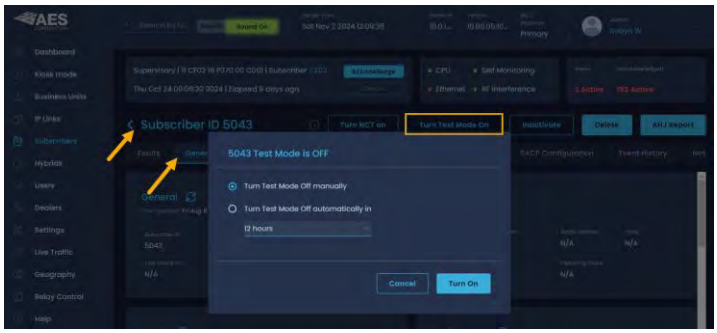


Subscriber Configuration

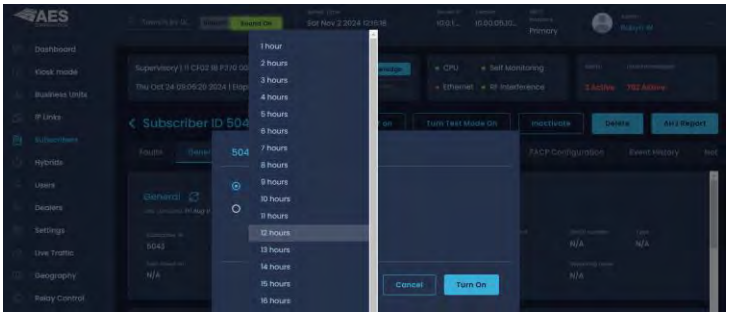
Test Mode

The Test Mode tab displays alarms for subscribers currently in test mode. To put a subscriber into test mode, click the **Turn Test Mode On** button from within the subscriber's General tab. This allows tests and system maintenance to be performed without having to worry about the police being dispatched. All events will be sent to the Test Mode tab on the dashboard if this is enabled.

Test mode can be configured so that it's turned off permanently, or it can be configured to turn off at a specified time between 1–24 hours:

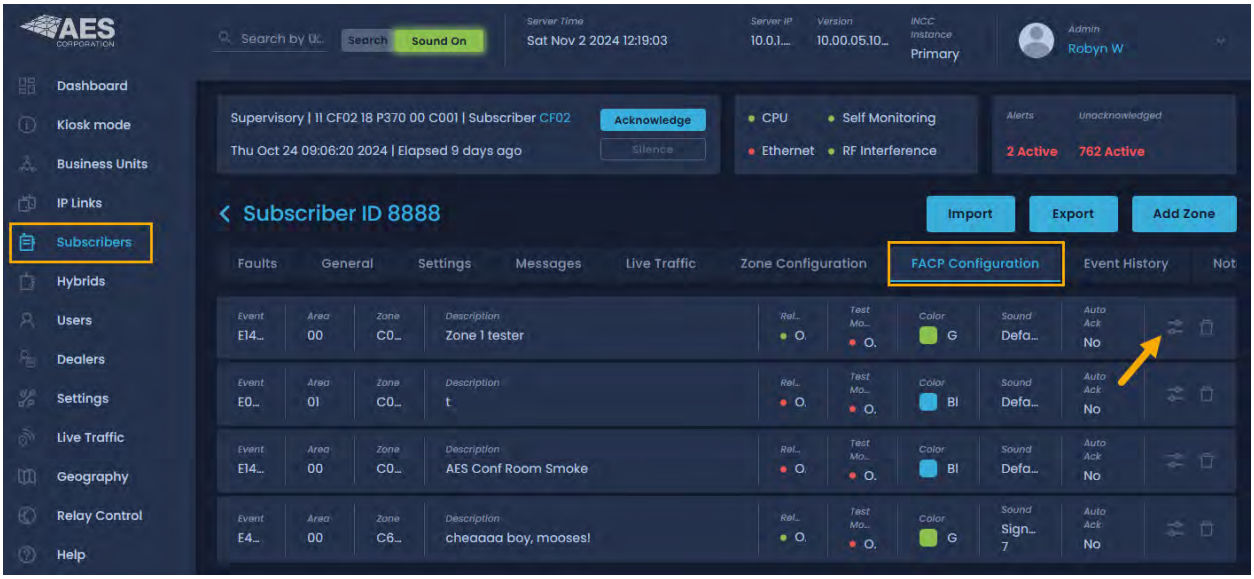


Configure Time:



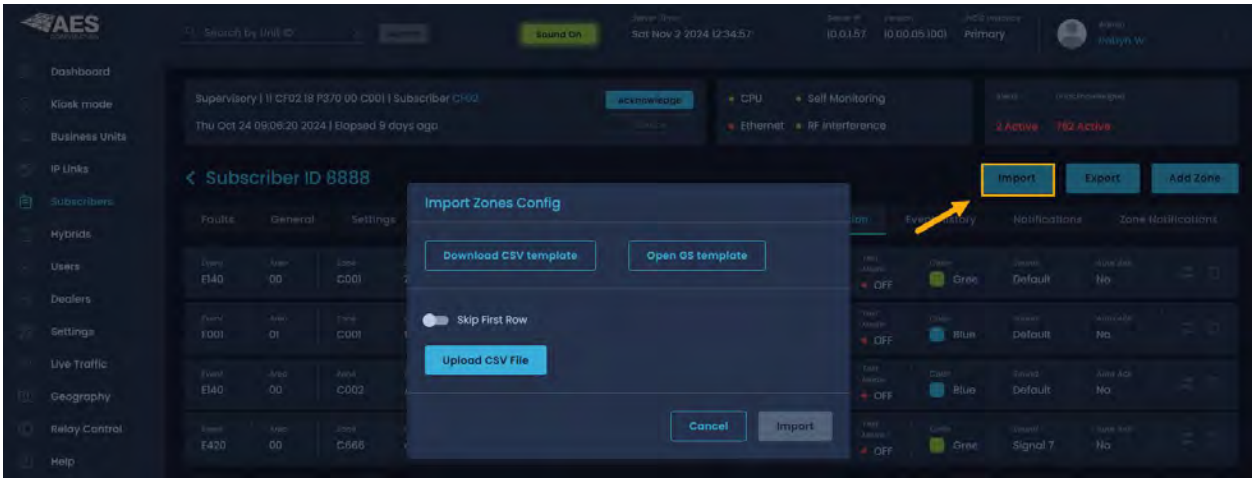
FACP Configuration

The FACP (fire alarm control panel) feature is used for defining zones and events. Any zone on the panel can be mapped for visibility from the dashboard.



Import Zone Configurations

Use this feature to import configurations of events per zone. The template is shown below, and a description for each item to import into the template follows.



Zone	Area	Event code	Color (From INCC selection)	Sound (From INCC Selection)	Test	Description	MCP	Autoack
C###	##	E###	0-3	0-15	Y or N	42 chars max	Y or N	Y or N or X
			0 = Blue, 1=Red, 2=Yellow, 3=Green					
Example:								
C001	00	E140	2	2	Y	Test for FACP	N	X

10.00.03.xxx Release Import Rules

- Zone – C followed by 3 alpha numerical characters
  - Required to have 3 digits for validation
  - Example C001 not C1
  - ***Required to have C or U in front of 3 digits for validation**
- Area – 00
  - ***Required to have 00 input. Need to change column B to "Text" in format cell to show 00**
- Event Code – E followed by 3 alpha numerical characters
- Color – Enter number 0–3
- Sound – Enter number 0–10
- Test – Enter Y or N
- Description – 42 characters maximum
- MCP – Enter Y or N

10.00.04.xxx Release Import Rules

- Zone – 3 Digits required for validation
  - Example C001 = 001

  - **Need to change column A to "Text" in format cell to show 001 instead of 1**
  - ***Required to remove C or U in front of 3 digits for validation**
- Area – 00
  - ***Required to have 00 input. Need to change column B to "Text" in format cell to show 00**
- Event Code – E followed by 3 alpha numerical characters
- Color – Enter number 0–3
- Sound – Enter number 0–10
- Test – Enter Y or N
- Description – 42 characters maximum
- MCP – Enter Y or N

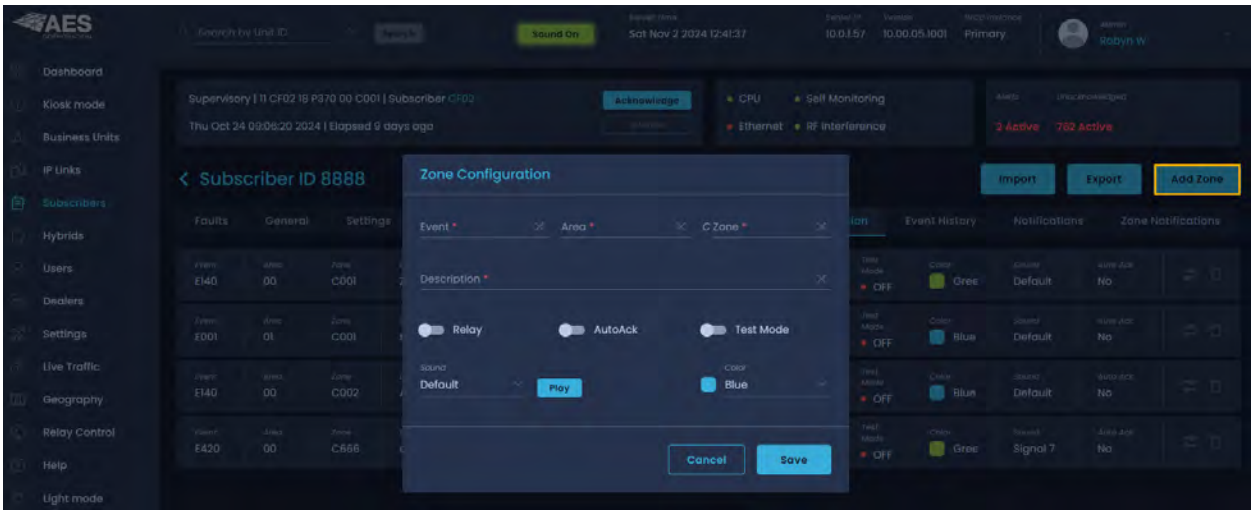
Export Zone Configurations

Export current configurations of zones.

Add Zone

To enter zones manually, click **Add Zone**.

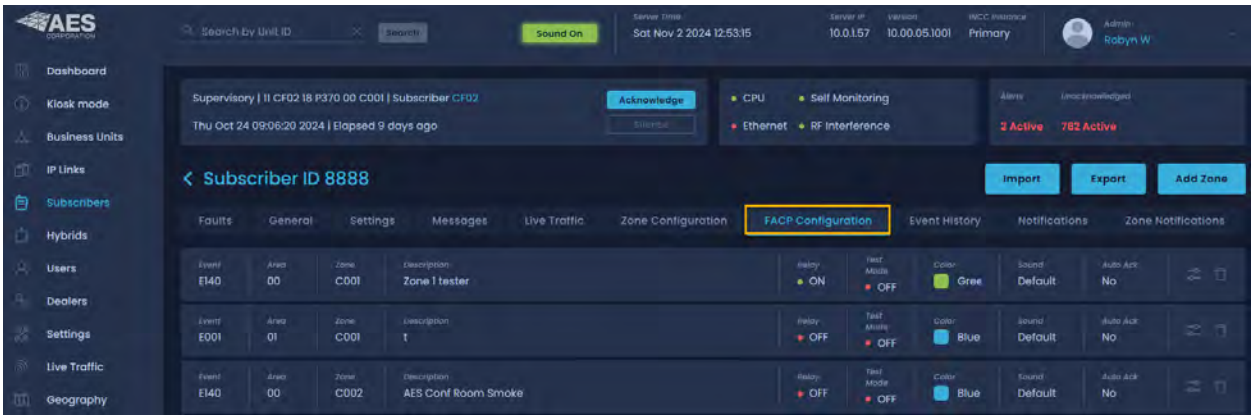
- Event – E/R/P followed by 3 digits
- Area – Partition 00 default



- Zone – Enter 3 digits
- Description – Describe zone or end point (maximum of 42 characters)
- MCP – Web Relay Device – triggers web relay if configured under Settings page. This is off by default.

- AutoAck – If enabled, events are pushed to the Acknowledged page on the dashboard (they do not go to the Unacknowledged page). This is off by default.
- Test Mode – If enabled, events are pushed to the Test Mode page on the dashboard (they do not go to the Unacknowledged or Acknowledged page). This is off by default.

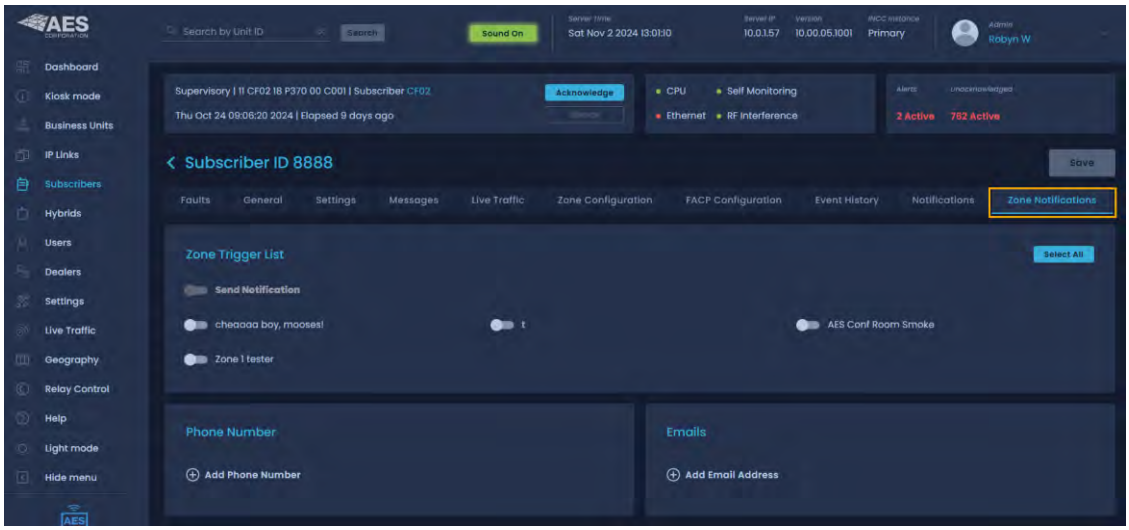
After the zone has been added, the list is displayed under the FACP Configuration tab:



Zone Notifications

All custom zones that have been created are displayed on the Zone Notifications page.

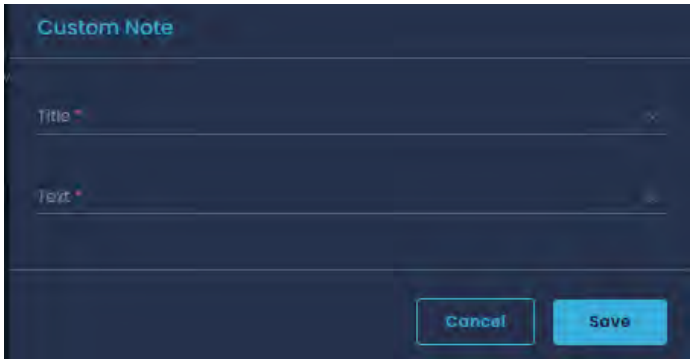
You can select the event for which you want to get notifications, as you can with the Notifications page.



The Notification function enables users to monitor their IntelliNet network from anyplace at any time. Using the page below, users can configure automatic alerts based on a change to any fault with any Subscriber or IP Link. Separate dropdown menus enable the user 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.

Custom Notes



Contact Persons

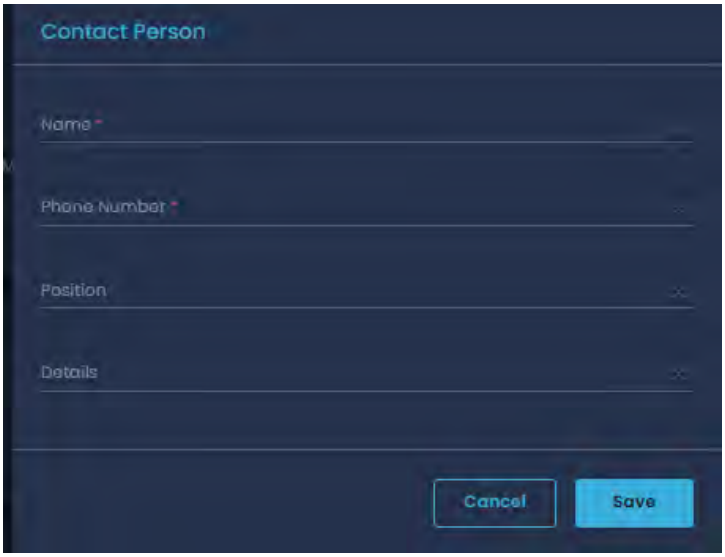
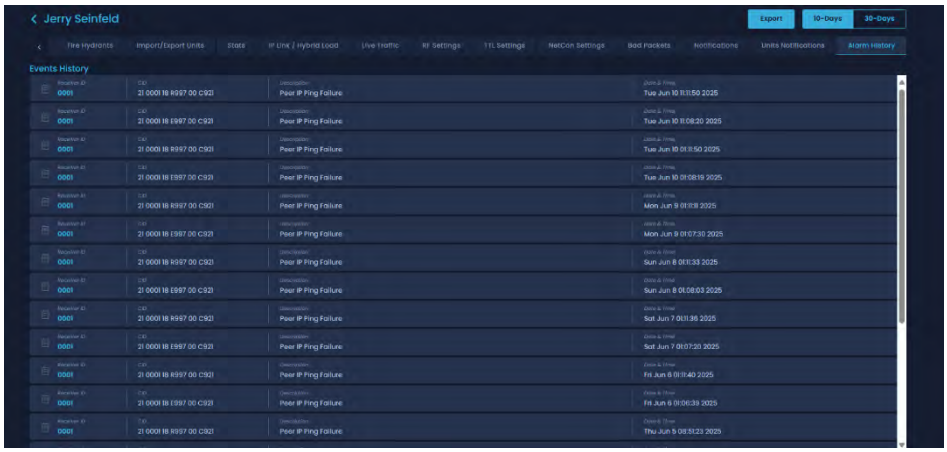


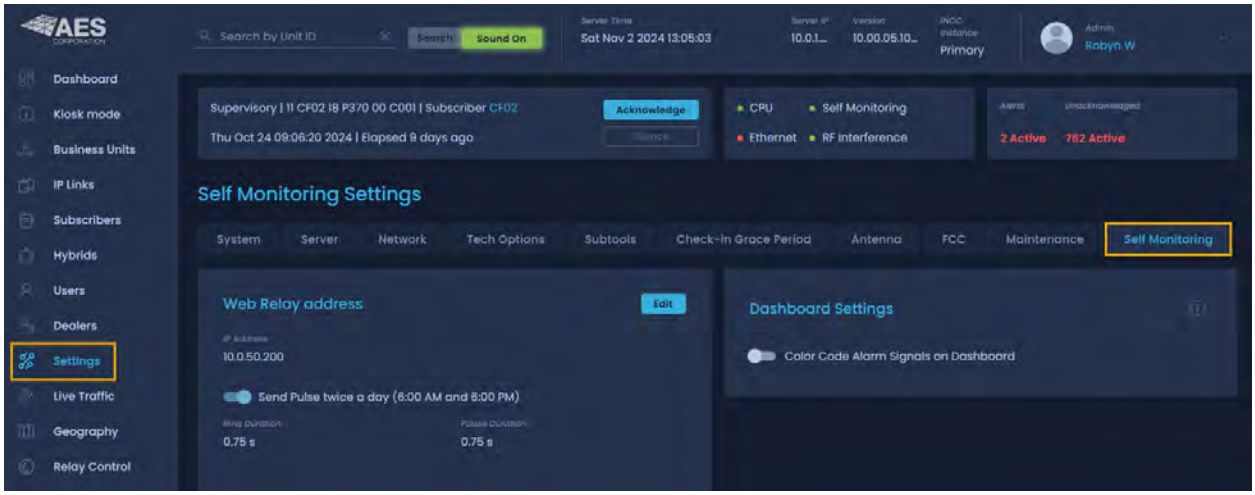
Image Associations

Alarm History

View alarm history of each BU under tab below: Can configure 10/30 days. Have ability to export list.



Self-Monitoring Settings

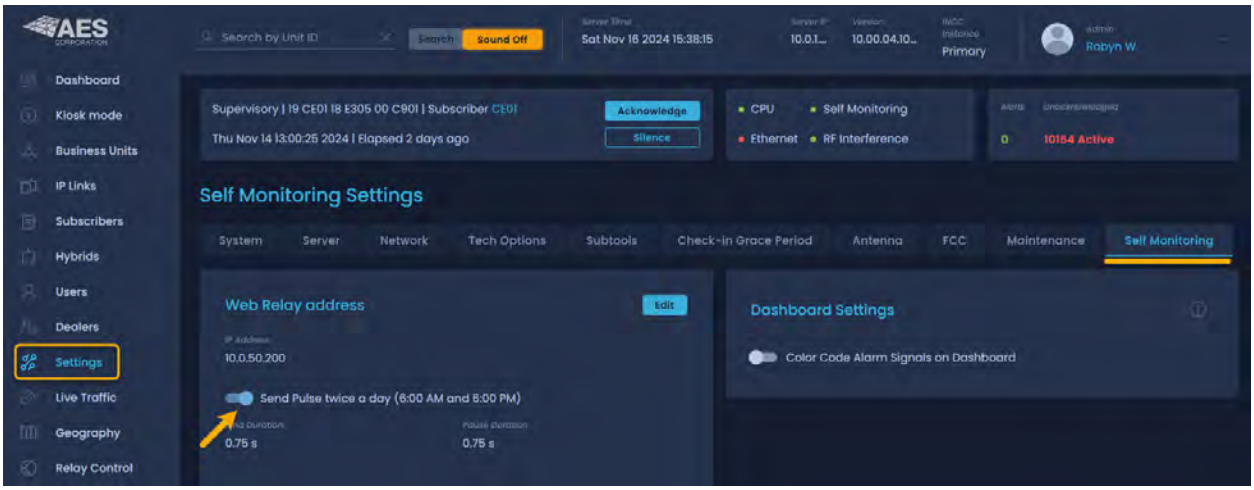


Web Relay Address (MCP)

This feature is used to control a web relay third party “single relay & input module”

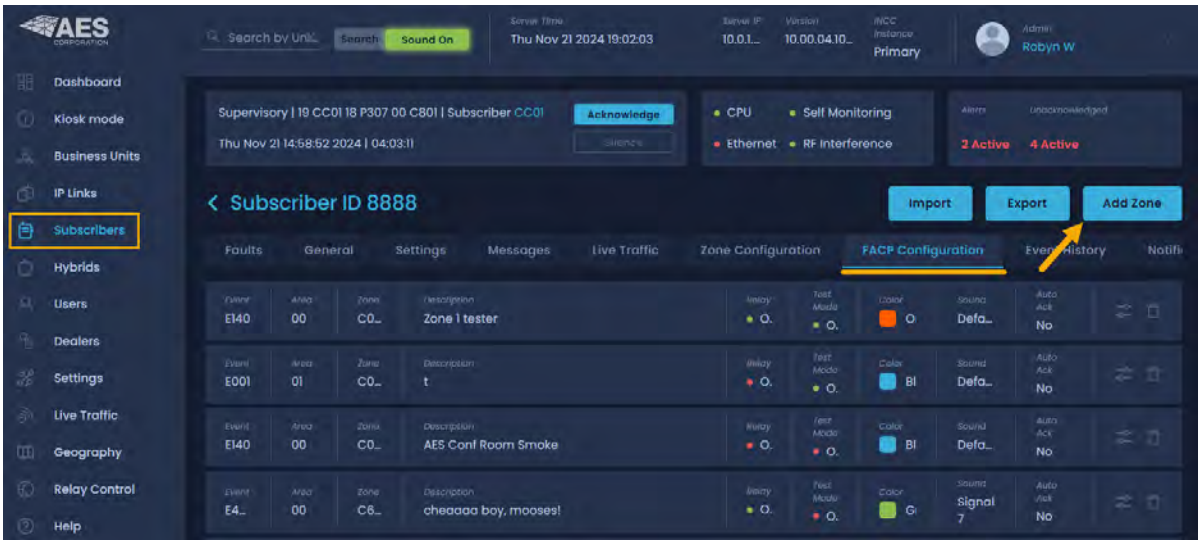
Recommended to use with Bell or Siren to conduct daily test. Can configure events in FACP zone configuration to trigger bell located below:

This area allows alarms received in the INCC to re-transmit signals to auxiliary circuits that control legacy devices, such as bells, lights, or other equipment using Web Relay model numbers X-WR-1R12 and X-WR-4R3.

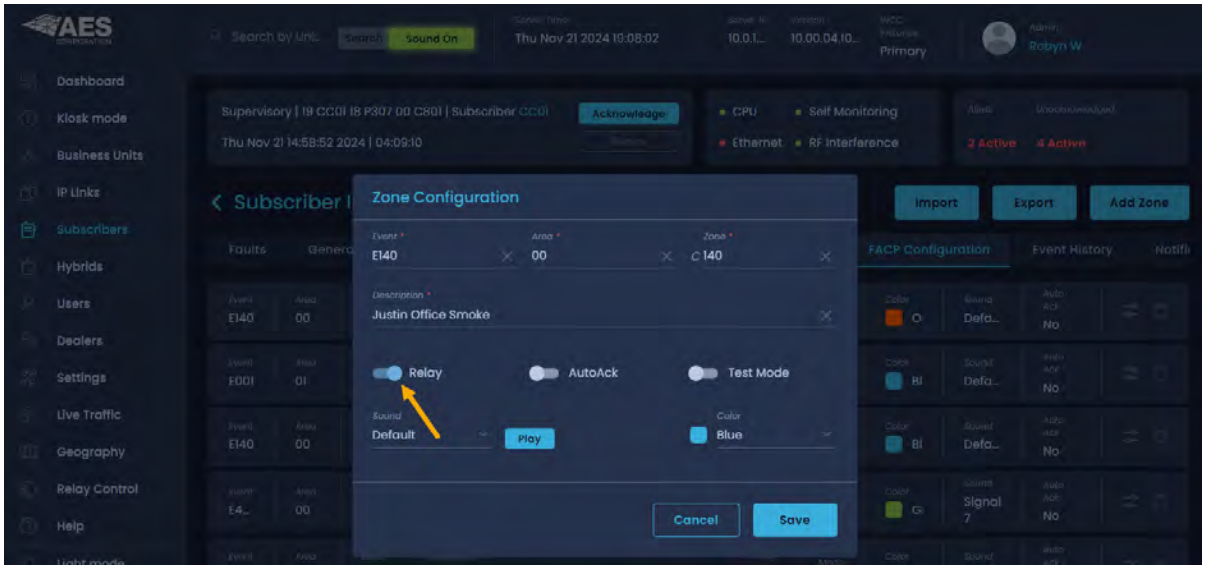


Configuration is needed on the Subscriber page to enable WebRelay.

1. Navigate to Subscribers > FACP Configuration and click **Add Zone**.



2. Enable **Relay**.



If Relay is enabled, when the INCC receives an alarm, a series of pulses are transmitted on the WebRelay, organized, and sequenced based on the ID number associated with the subscriber from which the signal originated.

Example: Subscriber 1234 is set to MCP for E140 00 C001 Event.

The event is displayed on the INCC dashboard page and simultaneously sends a group of pulses to the web relay organized as one pulse, then two pulses, then three pulses, then four pulses. The timing of the ring duration and the pause duration associated with each pulse can also be adjusted.

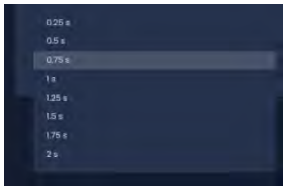
For example, when Ring Duration is set to 0.5 s and Pause Duration is set to 0.75 s, subscriber 1234 will be transmitted as:

- Ring Duration 0.5 s, Pause Duration 0.75 s (for number 1)
- Ring Duration 0.5 s, Pause Duration 0.75 s, Ring Duration 0.5 s, Pause Duration 0.75 s (for number 2)

The pattern continues.

Configuration of Web Relay

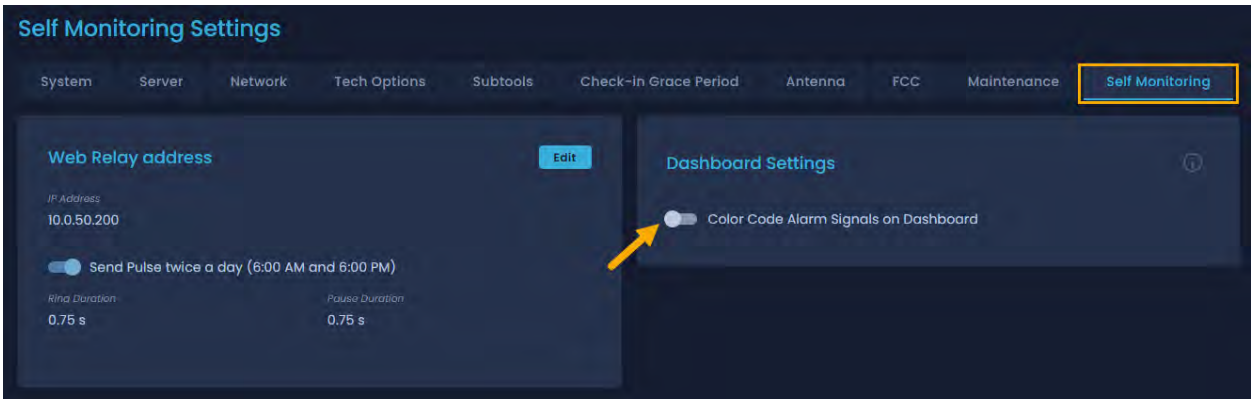
- Configure IP
- Ring Duration: Can be adjusted between 0.25 s – 2 s (.25 s intervals).



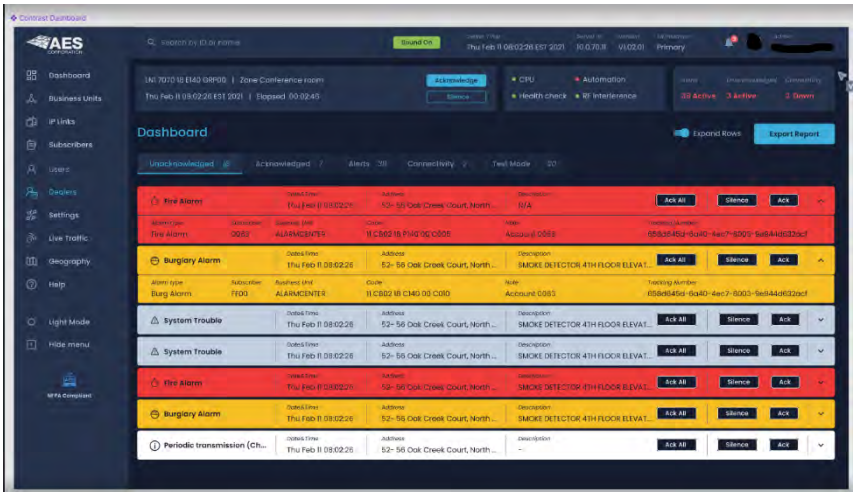
- Pause Duration: Can be adjusted between 0.25 s – 2 s (.25 s intervals).
- Configure time for Pulse 1 & Pulse 2

Dashboard Settings (High Contrast Coloring)

This mode is off by default.



Once enabled, it allows fuller contrast of coloring on the dashboard for all alarms as seen below:

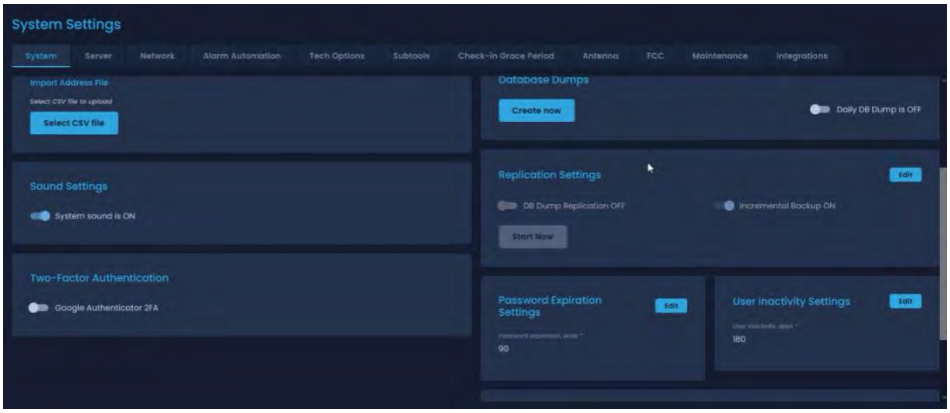


dB Dump Sync (Enable/Disable Cluster)

This feature was added to eliminate locking of tables due to customer networks. Our cluster configuration requires constant connection between instances. If this connection is unstable and goes down for more than 10 seconds, it will trigger a dump of database that will lock up secondary AA during this transfer period. This time depending on size of network and network bandwidth.

Navigate to “Settings” tab on left and then to “System” tab.

Screen below will open and navigate to “Replication Settings” below



By default, cluster will always be enabled. If you want to disable cluster and revert to dB dump please click edit button.

Upon this selection you have two options:

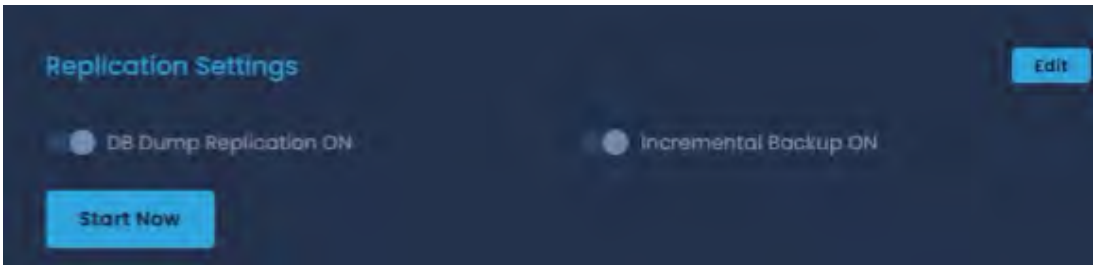
1. Enable/Disable dB Dump Replication
    a. Default is off
2. Enable Incremental Dump
    a. Default is full dump
        i. Incremental dump = Will only take events missing from time of last dB dump. This is recommended to keep files smaller for transfer
        ii. Full dump = Will take entire table from Primary (30 day history) and transfer to secondary

Once you finalize settings and click save, there will be a prompt to confirm password.

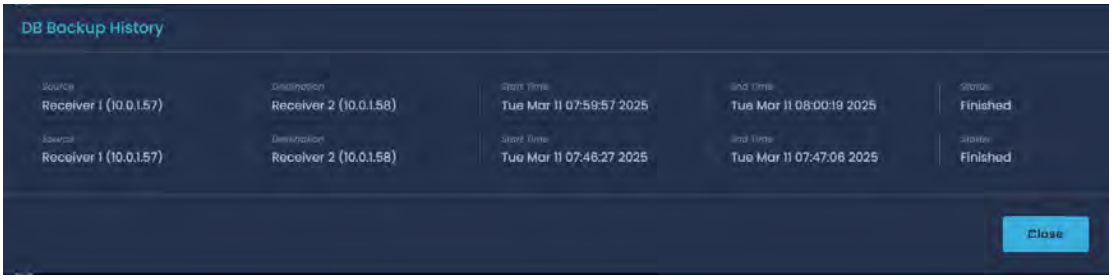
This setting is only available for Admin Users of INCC.

Upon enabling dB dump, will be triggered for following:

1. Daily dump at 2:00 AM
    a. If tertiary is present, will start with secondary instance, and push updates to tertiary upon completion of secondary
2. Can enable enable dump at anytime after enabling dB dump and navigating back to "Replication Settings" tab and selecting "Start Now"



To View dB History, please click history tab to see info below:



When dB Dump is enabled, the following screens on secondary will be unavailable due to data not being available in real time:

1. Dashboard page for BU
    a. Network Pulse
    b. Network Score
    c. IPL/Hybrid Link Loads
2. Other pages will be present but will potentially be missing events from the time of the last dump or default 12 AM EST. (2 AM UTC)

It is recommended to always trigger a dump if the following configurable items are added or changed:

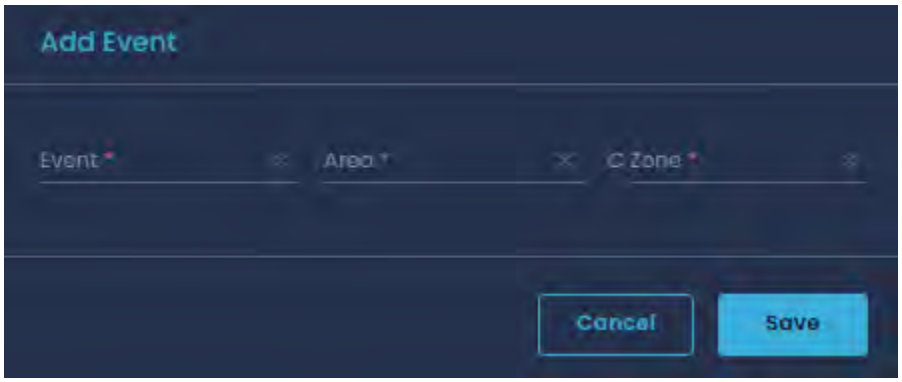
- License
- User
- Added BU
- Added IPL or IP Group
- Added Dealer

*Upon enabling dB dump mode, please wait 1 minute prior to starting dump.

Cluster will take a minute to shut down and restart database

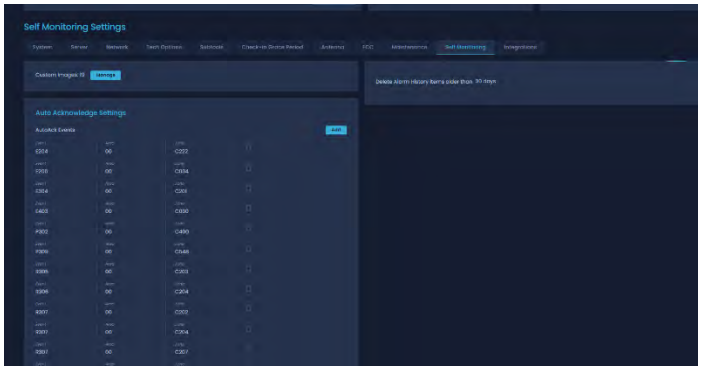
Global Auto Acknowledge Settings

This option allows user/operator to enter global CID event to auto ack across all subscribers:



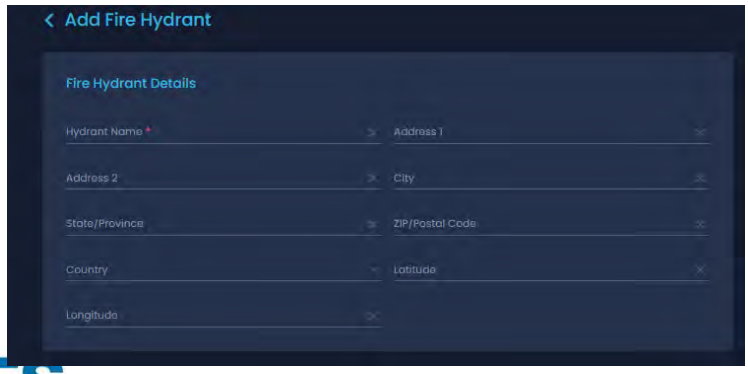
Event, Area, Zone all need to be entered.

List will be compiled below under Settings < Self-Monitoring < Auto Acknowledge Settings Tab below:

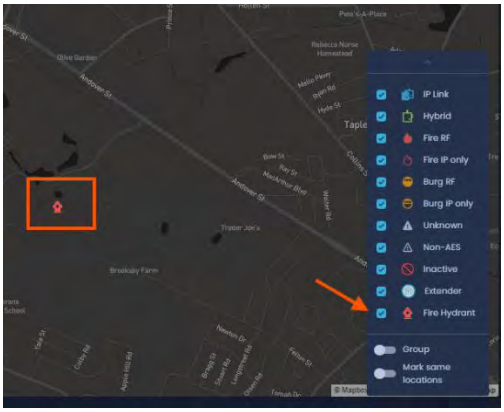


Fire Hydrant

Configure Fire Hydrants under BU page:



Show on Geography map with following Icon:



Assets (Add Images to associate with subscribers & installs)

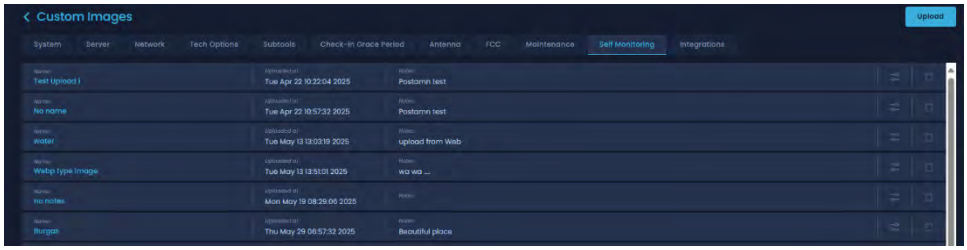
We have added ability to import pictures to apply to help review previous installs of subscribers and antenna locations for future troubleshooting.

This page maintains all pictures added to review.

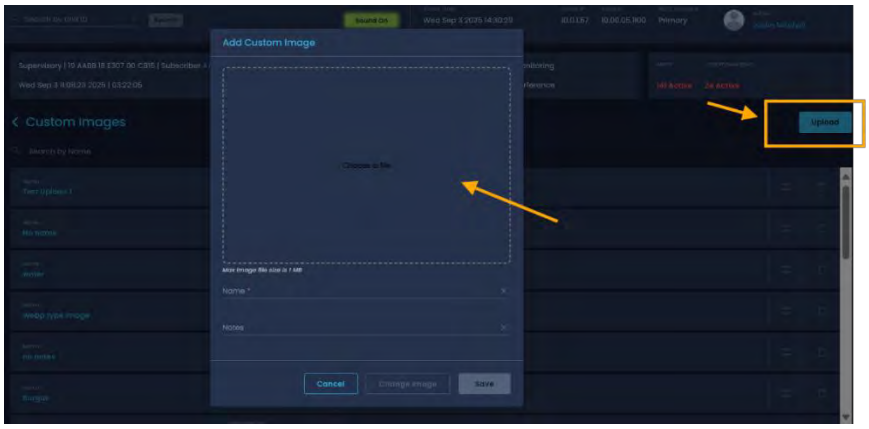
***Required to add image to this table to associate a FACP to an image.**

Step 1:

Step 2:



Step 3:



Bulk Import Options Under BU Page

Subscriber FACP Zones (Identical for Hybrid Section)

This section is used to import bulk FACP's from multiple Subscribers. (This template was taken from Digitize Output format below:

Zone # - Area - Event code – Type- Color- Sound – Show – Test – Description – MCP – Email – CAD - Auto Res – Complete - Wrk Grp

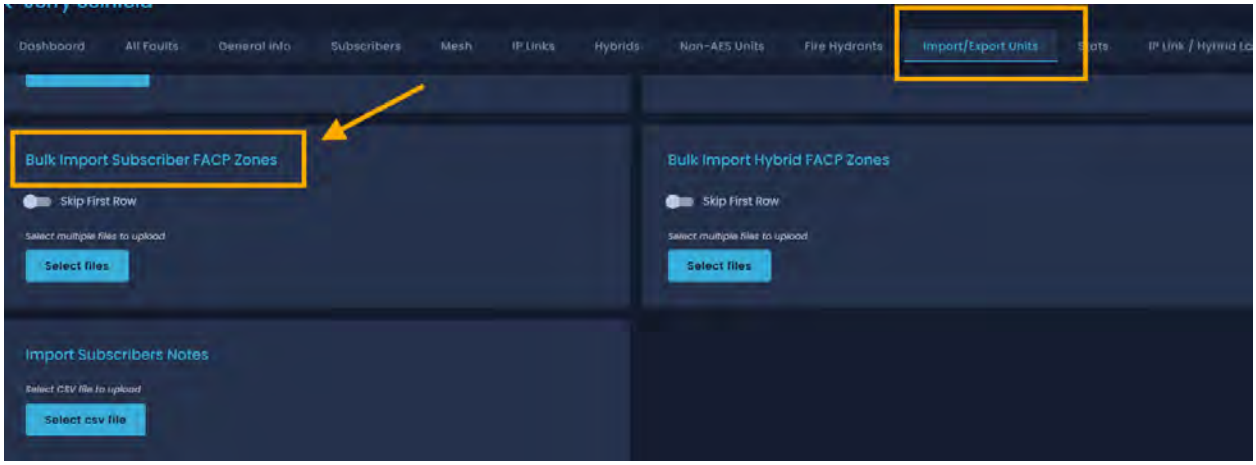
C000|00|E372|A|Y|4|Y|Y|SLC CIRCUIT TROUBLE|N|2|N|Y|Y|X|0|X

C000|00|E311|A|Y|4|Y|Y|TROUBLE - NO BATTERY|N|2|N|Y|Y|X|0|X

All fields are required for validation.
INCC will only map following fields:

- Zone
- Area
- Event Code
- Color
- Sound
- Test
- Description
- MCP

AES Internal Only - File can be found in sharepoint: Engineering Group - Documents - dB From Customers - All Documents



Import Subscriber Notes

Navigate to NMS to grab csv file from:

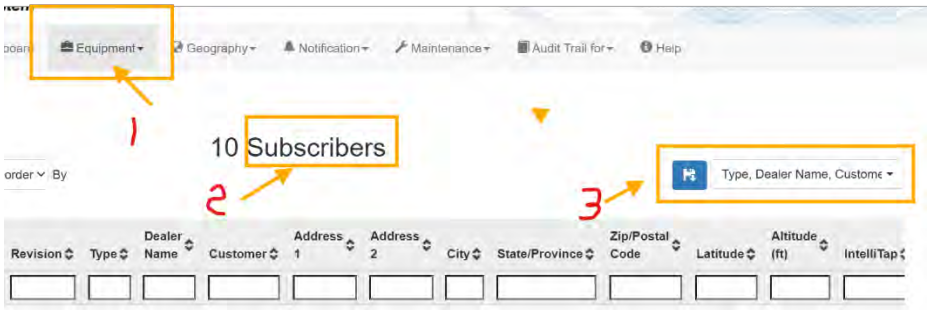
Business Unit > Equipment > Top right of table select following fields:

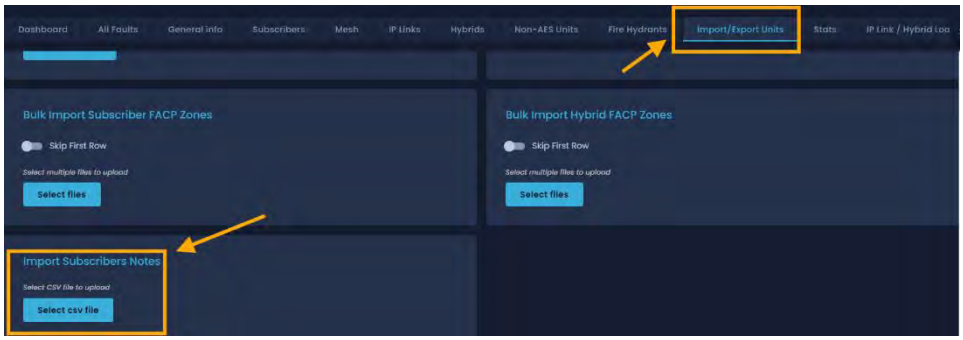
***All 28 fields are required in csv to pass validation**

Subscriber ID	Country
Model	Latitude
Revision	Elevation (ft)
Type	Antenna
AP ID	Report Delay
Reporting Route	Repeater
Dealer Name	Check-in TTL
Customer	Status TTL
Faults	Alarm TTL
Address 1	Trouble TTL
Address 2	Restoral TTL
City	IntelliTap TTL
State/Province	Special TTL
Zip/Postal Code	Notes

Select export csv and use this file to import on INCC

AES Internal Sample file can be found here: Subscriber Notes Template Import File 9.3.25.csv



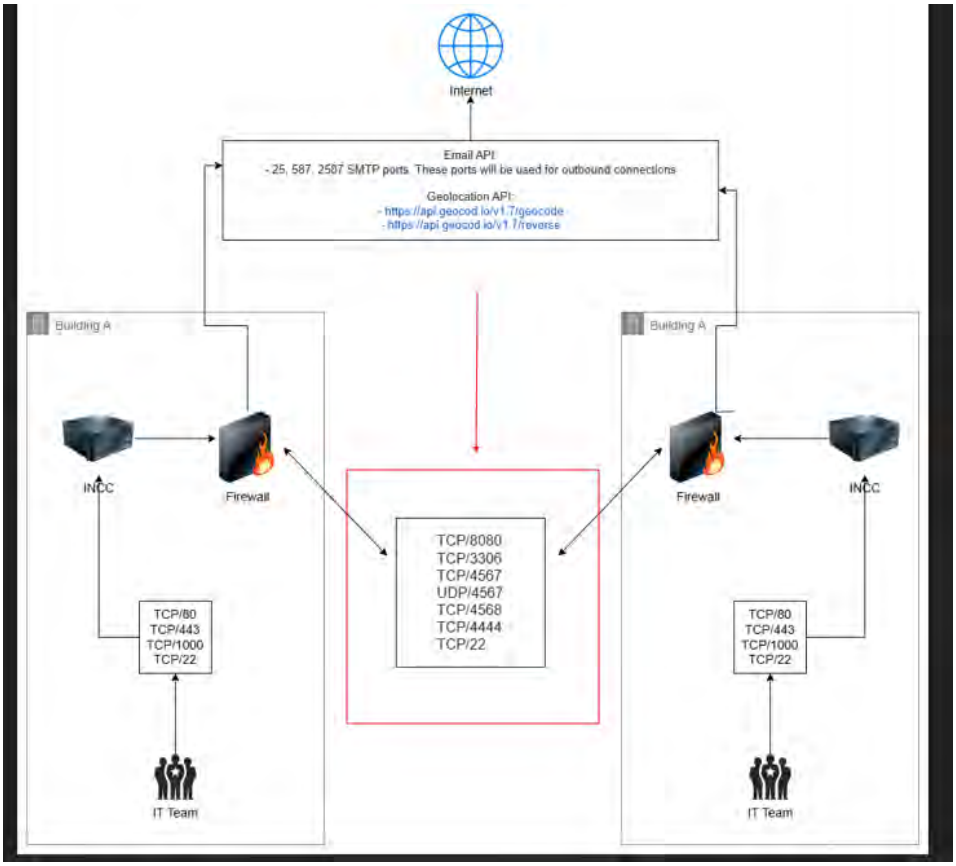


Glossary

IP Ports to Open

Application	Protocol	Port
SSH	TCP	22
Back End Health Check	TCP	8080
Database SST (State Snapshot Transfer)	TCP	4040
Database replication	TCP	4568
Database replication	TCP/UDP	4567
Database connection	TCP	3306
IP Link Default Port (Incoming Alarms)	TCP	7070
IP Subscribers Default Port (Incoming Alarms)	TCP	9090
Alarm Automation, if applicable Default Port	TCP	6050
Front End HTTP	TCP	80
Front End HTTPS	TCP	443
SMTP- simple mail transfer protocol (outbound only)	TCP	587/25
Geocodio- outbound/inbound	TCP	443

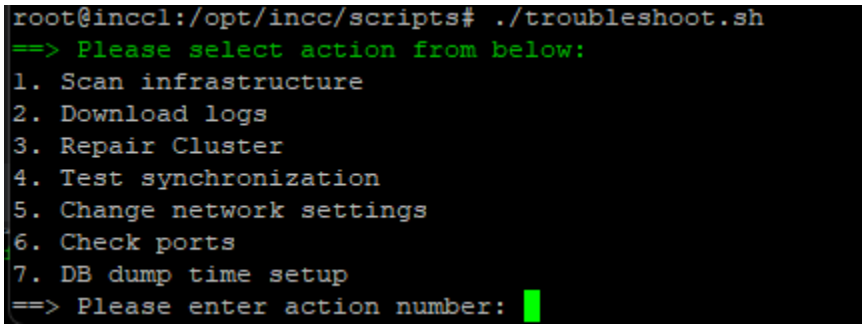
Network Diagram



INCC helper commands

There are following commands that helps gracefully start, stop and troubleshoot. These commands can be run in any folder directly:

- **incc stop**– gracefully stops all the containers. It is required before reboot and shutdown VMs
- **incc start** – gracefully starts all the containers. It is useful when containers are down or stopped.
- **incc troubleshoot** – opens troubleshooting options quickly.
    - cd /opt/incc/scripts (Need to run as ROOT user or with SUDO privileges)
        - ./troubleshoot.sh



Troubleshoot Options

- Scan infrastructure
    - Checking SSH connection availability
    - Checking if script running from Primary or not
    - Checking Primary DB IP configs
        - Suggesting fix
    - Checking Secondary DB IP configs
        - Suggesting fix
    - Checking Primary VM's Symmetric configs
        - Suggesting fix
    - Checking Secondary VM's Symmetric configs
        - Suggesting fix
- Download logs
    - it will generate web page to download logs from both Primary and Secondary instance in archive format at once.
- Reinstall Cluster
    - If there is any issue with Symmetric, you have an option to reinstall it.
- Test synchronization
    - It inserts record to Primary DB and waits it from Secondary DB

    - It inserts record to Secondary DB and waits it from Primary DB
- Change Network Settings
- Check Ports
    - INCC installed (prior to upgrade recommended)
    - INCC is not installed (prior to install recommended)
- dB dump time setup
    - Modify start time for dB dump (If enabled)

Revision History

INCC Appendix_ V1.1	1.27.25	JDM	Document Created to Support Added Features
INCC Appendix_V1.2	6.10.25	JDM	Added SIA, Surgard, 4th Release Features
INCC Appendix_V1.3	7.7.25	JDM	Updated 4th Release Items
INCC Appendix_V1.3	8.6.25	JDM	Updated Missing Features – Relays, User Permissions

Hard refresh- CTR F5 “empty cache and hard reload @Nijat Bayramov Add screen shot or fast key