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 4-22-2024, 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.

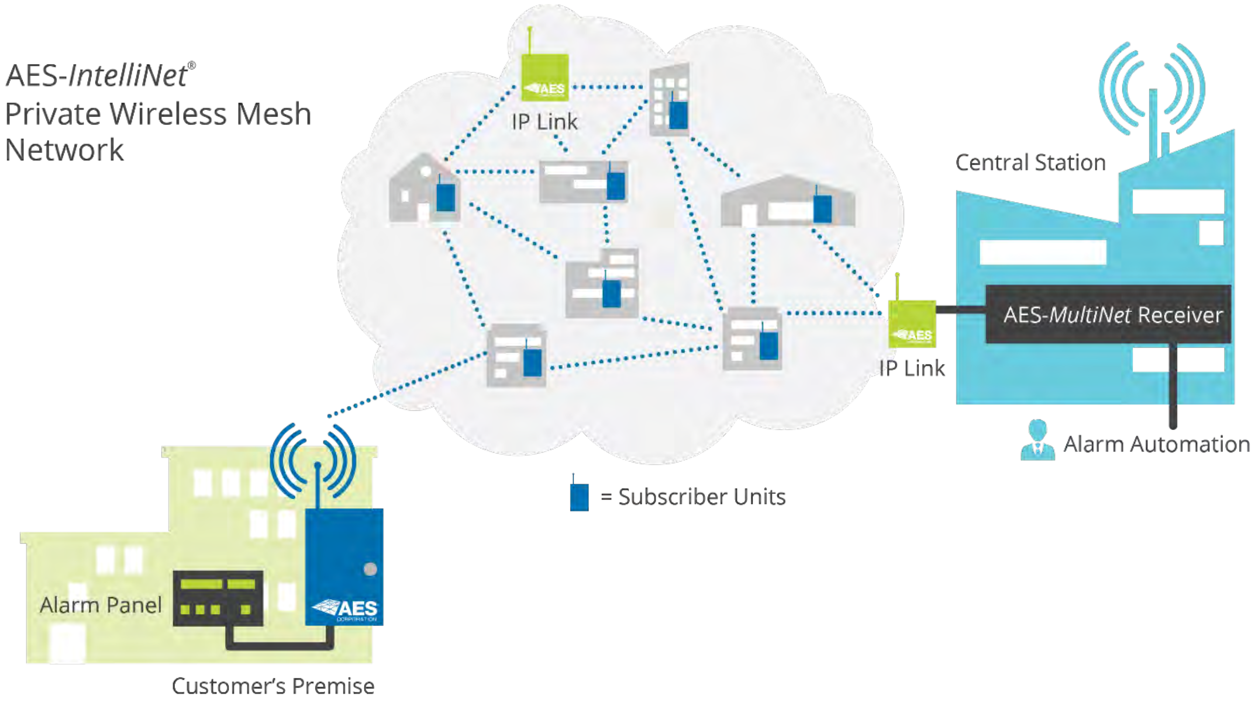
Notes

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	7300-1516:0505
City of New York Fire Department Certificate of Acceptance Number (COA)	2023-TMCOAP-002520-CERT

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 (64 bit) ***Note newer versions will not work**

Other requirements that must be considered for the installation:

- Primary and secondary servers are redundant machines.
- All servers must be operating at all times, 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.

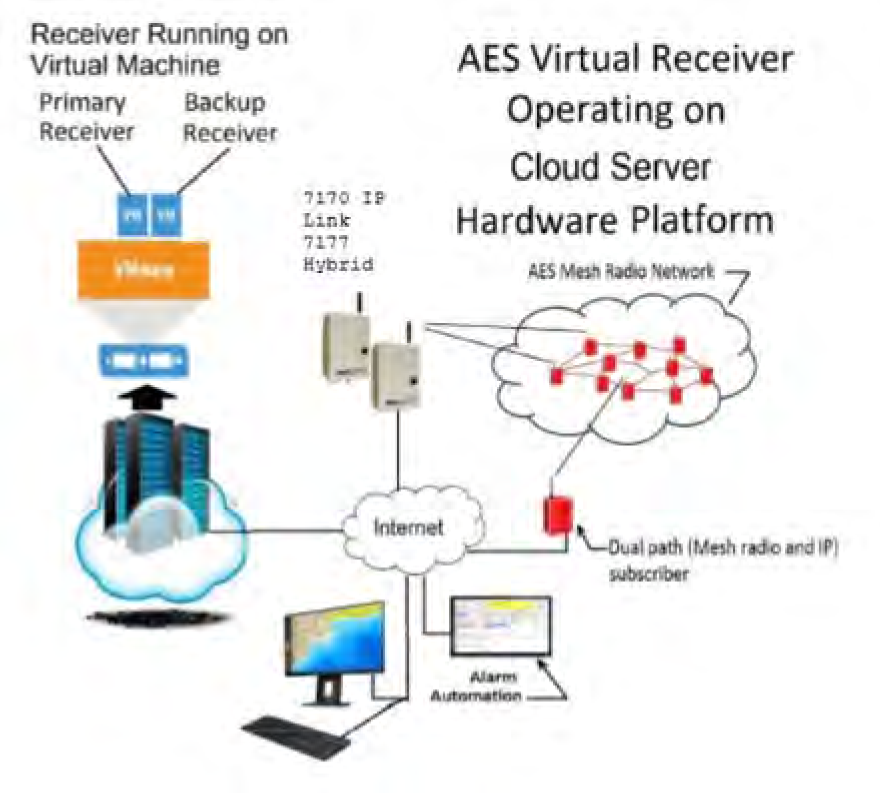
Software Requirements

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.


Receiver Running on Virtual Machine
Primary Receiver
Backup Receiver
VM
VM
VMware
AES Virtual Receiver Operating on Cloud Server Hardware Platform
7170 IP Link
7177 Hybrid
AES Mesh Radio Network
Internet
Dual path (Mesh radio and IP) subscriber
Alarm Automation

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)
- Compatible software alarm automation system for signal processing
- Web-enabled device for browser access to the AES software receiver

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 in 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 provide ability 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.
- In order to perform 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 operating system. Need to allocate all space to root partition. When checking LVM group is when you will modify this allocation. (Let's add screen shot of this process)

When changing IP address for INCC, please check IP addresses are not being used currently and inside your network scope

Prerequisites

Software Distribution Media

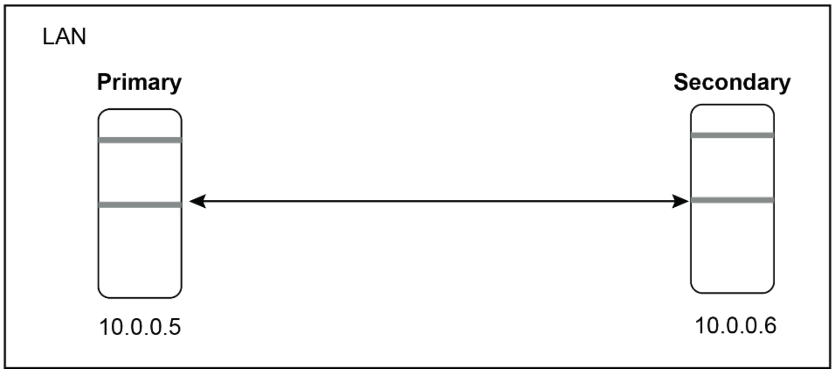
NOTE: The INCC software is available from AES as a web download or USB.

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,
2. Hardware and Software Requirements are met from above criteria
3. Configure static IP addresses for both the primary and secondary servers, then run both servers (https://en.wikipedia.org/wiki/Private_network).

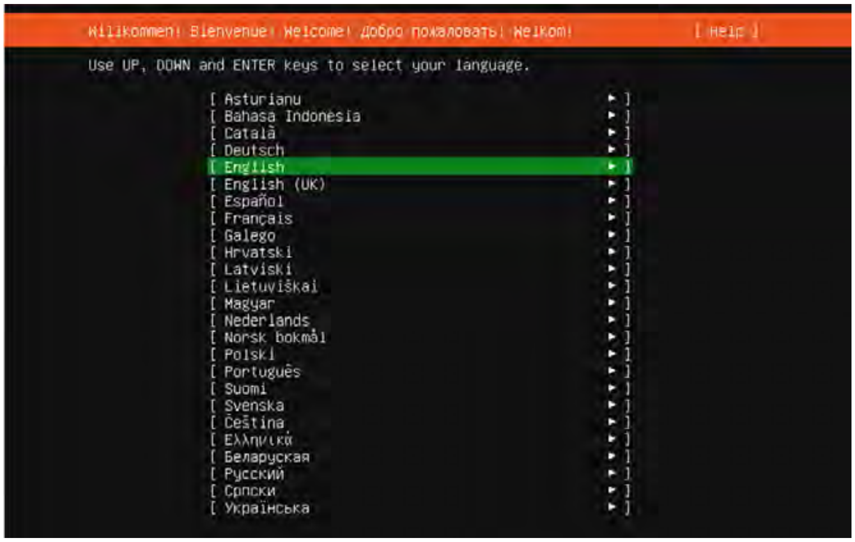
4. Network connectivity between VMs must be configured.



5. INCC Software Installation

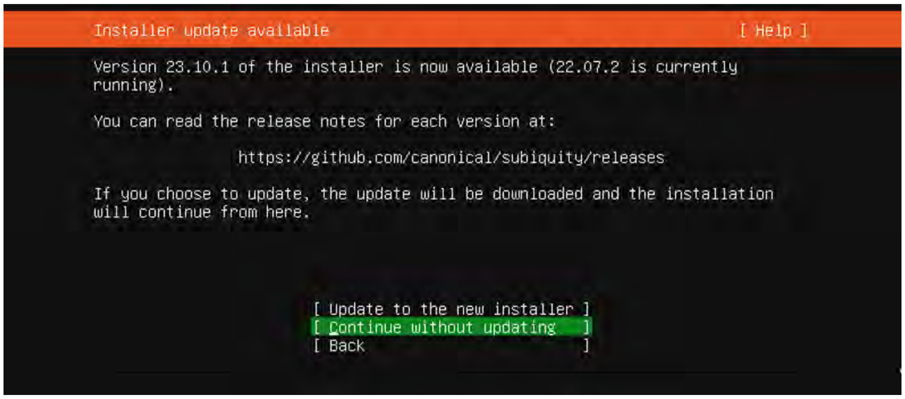
Installing Ubuntu Operation System

1. Please select a language of your choice:



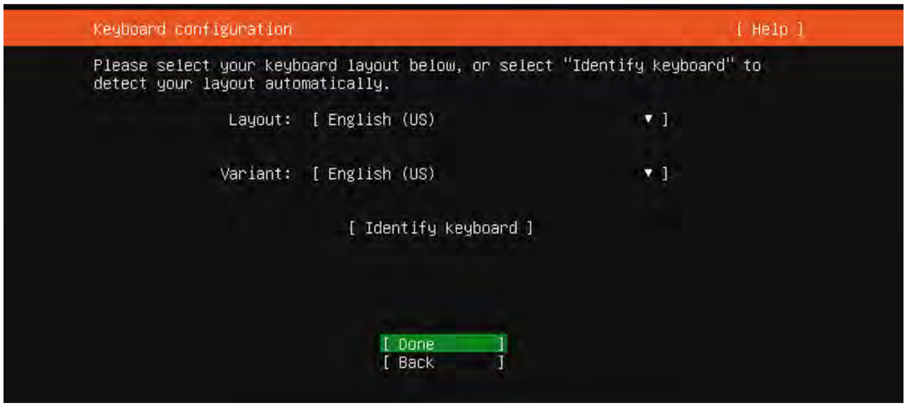
```
Willkommen! Bienvenue! Welcome! Добро пожаловать! Welkom!            [ Help ]
Use UP, DOWN and ENTER keys to select your language.

              [ Asturianu                                  ▸ ]
              [ Bahasa Indonesia                           ▸ ]
              [ Català                                     ▸ ]
              [ Deutsch                                    ▸ ]
              [ English                                    ▸ ]
              [ English (UK)                               ▸ ]
              [ Español                                    ▸ ]
              [ Français                                   ▸ ]
              [ Galego                                     ▸ ]
              [ Hrvatski                                   ▸ ]
              [ Latviski                                   ▸ ]
              [ Lietuviškai                                ▸ ]
              [ Magyar                                     ▸ ]
              [ Nederlands                                 ▸ ]
              [ Norsk bokmål                               ▸ ]
              [ Polski                                     ▸ ]
              [ Português                                  ▸ ]
              [ Suomi                                      ▸ ]
              [ Svenska                                    ▸ ]
              [ Čeština                                    ▸ ]
              [ Ελληνικά                                   ▸ ]
              [ Беларуская                                 ▸ ]
              [ Русский                                    ▸ ]
              [ Српски                                     ▸ ]
              [ Українська                                 ▸ ]
```

It is recommended that you continue without updating:



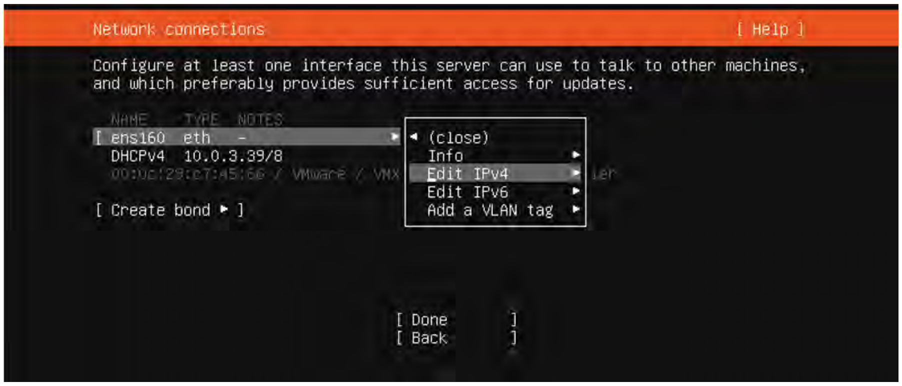
```
Installer update available                                      [ Help ]
Version 23.10.1 of the installer is now available (22.07.2 is currently
running).

You can read the release notes for each version at:

            https://github.com/canonical/subiquity/releases

If you choose to update, the update will be downloaded and the installation
will continue from here.


                    [ Update to the new installer ]
                    [ Continue without updating   ]
                    [ Back                        ]
```

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



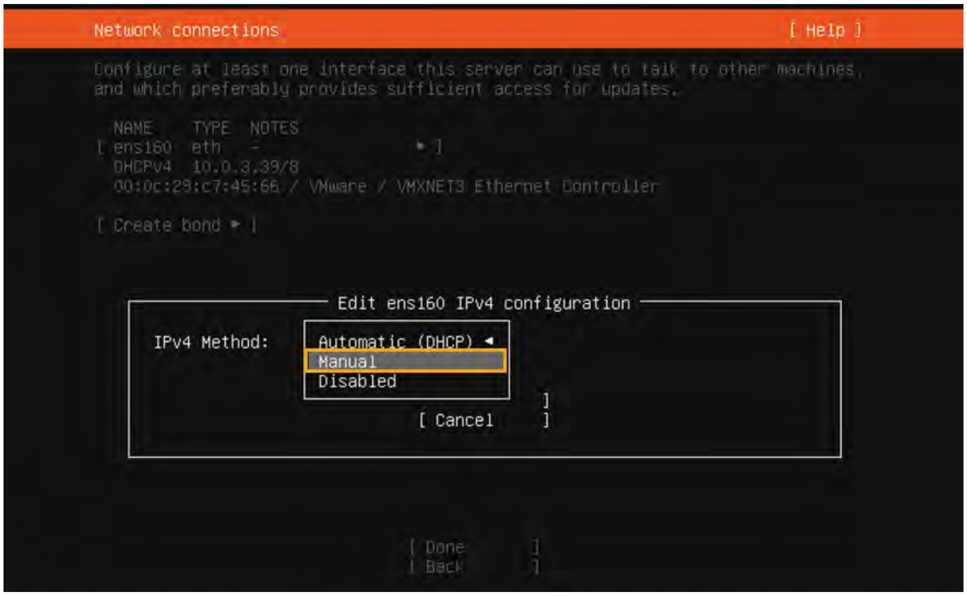
```
Keyboard configuration                                             [ Help ]

Please select your keyboard layout below, or select "Identify keyboard" to
detect your layout automatically.

               Layout:  [ English (US)                        ▾ ]

              Variant:  [ English (US)                        ▾ ]

                            [ Identify keyboard ]



                                [ Done       ]
                                [ Back       ]
```

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



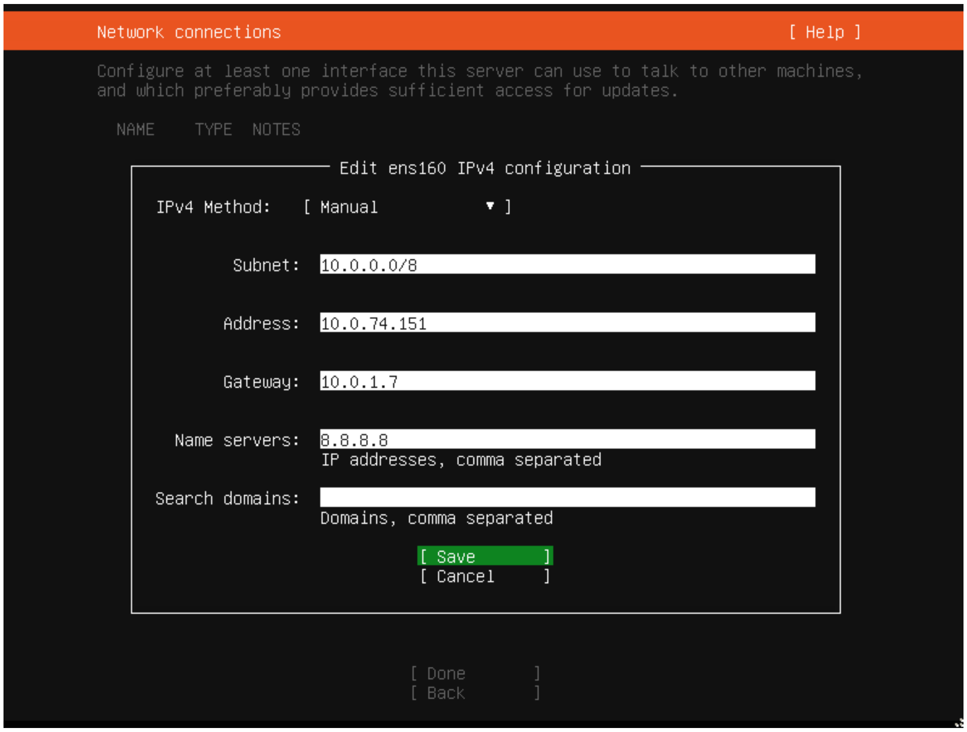
```
Network connections                                                [ Help ]

Configure at least one interface this server can use to talk to other machines,
and which preferably provides sufficient access for updates.

  NAME    TYPE  NOTES
[ ens160  eth   -                  ▸ ◂ (close)
  DHCPv4  10.0.3.39/8                  Info              ▸
  00:0c:29:c7:45:66 / VMware / VMX     Edit IPv4         ▸ ler
                                       Edit IPv6         ▸
[ Create bond ▸ ]                      Add a VLAN tag    ▸



                                 [ Done       ]
                                 [ Back       ]
```

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



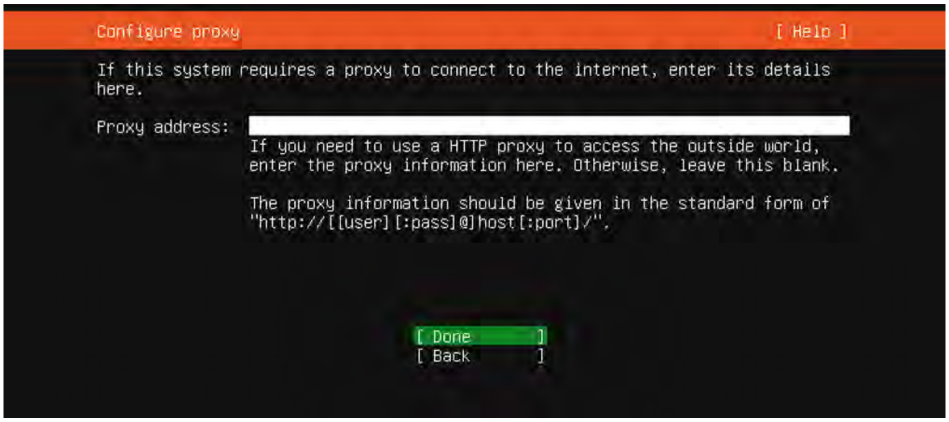
```
Network connections                                                [ Help ]
Configure at least one interface this server can use to talk to other machines,
and which preferably provides sufficient access for updates.

  NAME    TYPE  NOTES
[ ens160  eth   -                  ▸ ]
  DHCPv4  10.0.3.39/8
  00:0c:29:c7:45:66 / VMware / VMXNET3 Ethernet Controller

[ Create bond ▸ ]


     ┌──────────────── Edit ens160 IPv4 configuration ────────────────┐
     │ IPv4 Method:  ┌──────────────────┐                              │
     │               │ Automatic (DHCP) ◂                              │
     │               │ Manual           │                              │
     │               │ Disabled         │                              │
     │               └──────────────────┘  ]                           │
     │                         [ Cancel    ]                           │
     └─────────────────────────────────────────────────────────────────┘


                               [ Done       ]
                               [ Back       ]
```

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



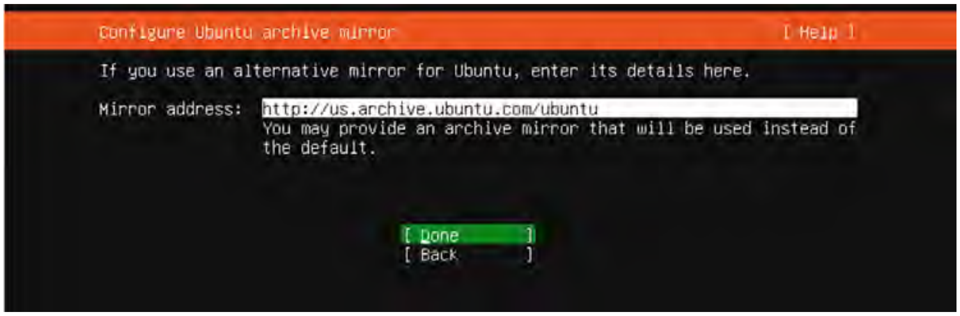
```
Network connections                                                [ Help ]
Configure at least one interface this server can use to talk to other machines,
and which preferably provides sufficient access for updates.

  NAME    TYPE  NOTES
     ┌──────────────── Edit ens160 IPv4 configuration ────────────────┐
     │ IPv4 Method:   [ Manual           ▾ ]                          │
     │                                                                 │
     │        Subnet: 10.0.0.0/8                                       │
     │                                                                 │
     │       Address: 10.0.74.151                                      │
     │                                                                 │
     │       Gateway: 10.0.1.7                                         │
     │                                                                 │
     │  Name servers: 8.8.8.8                                          │
     │                IP addresses, comma separated                    │
     │                                                                 │
     │ Search domains:                                                 │
     │                Domains, comma separated                         │
     │                                                                 │
     │                          [ Save      ]                          │
     │                          [ Cancel    ]                          │
     └─────────────────────────────────────────────────────────────────┘

                               [ Done       ]
                               [ Back       ]
```

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



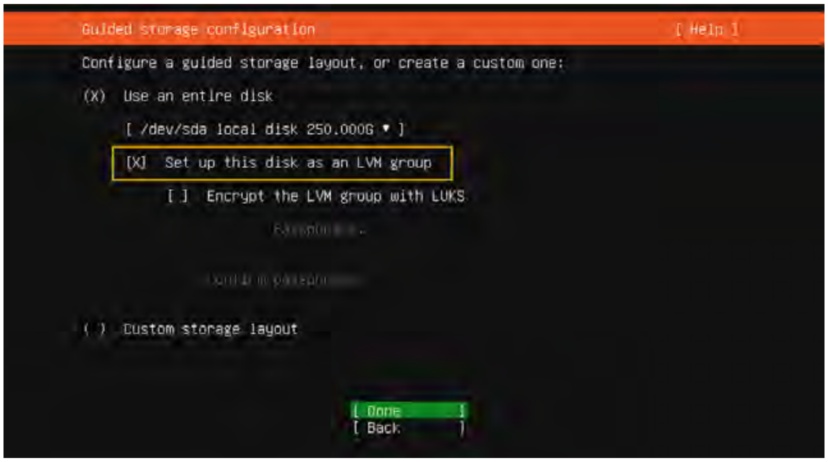
```
Configure proxy                                                  [ Help ]

If this system requires a proxy to connect to the internet, enter its details
here.

Proxy address: [                                                          ]
               If you need to use a HTTP proxy to access the outside world,
               enter the proxy information here. Otherwise, leave this blank.

               The proxy information should be given in the standard form of
               "http://[[user][:pass]@]host[:port]/".
```

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



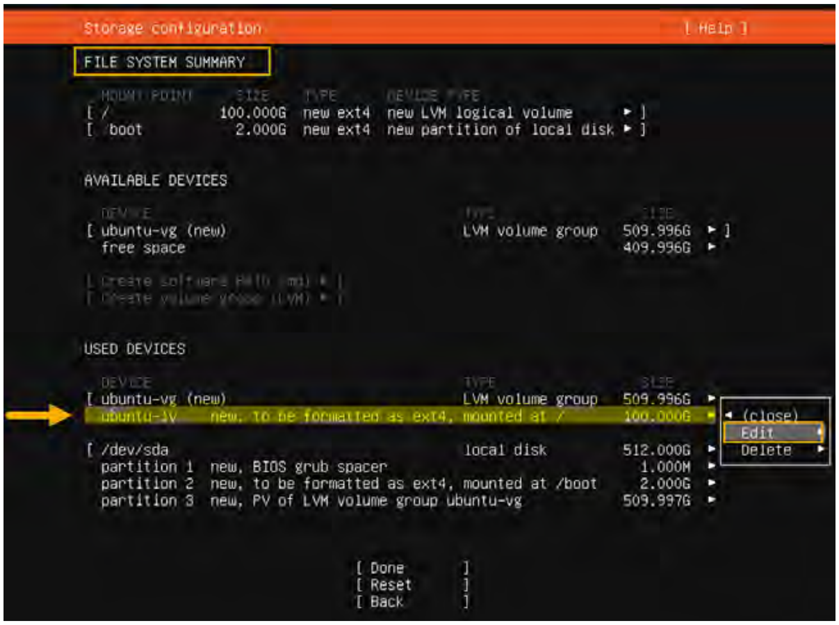
```
Configure Ubuntu archive mirror                                  [ Help ]

If you use an alternative mirror for Ubuntu, enter its details here.

Mirror address: http://us.archive.ubuntu.com/ubuntu
                You may provide an archive mirror that will be used instead of
                the default.
```

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



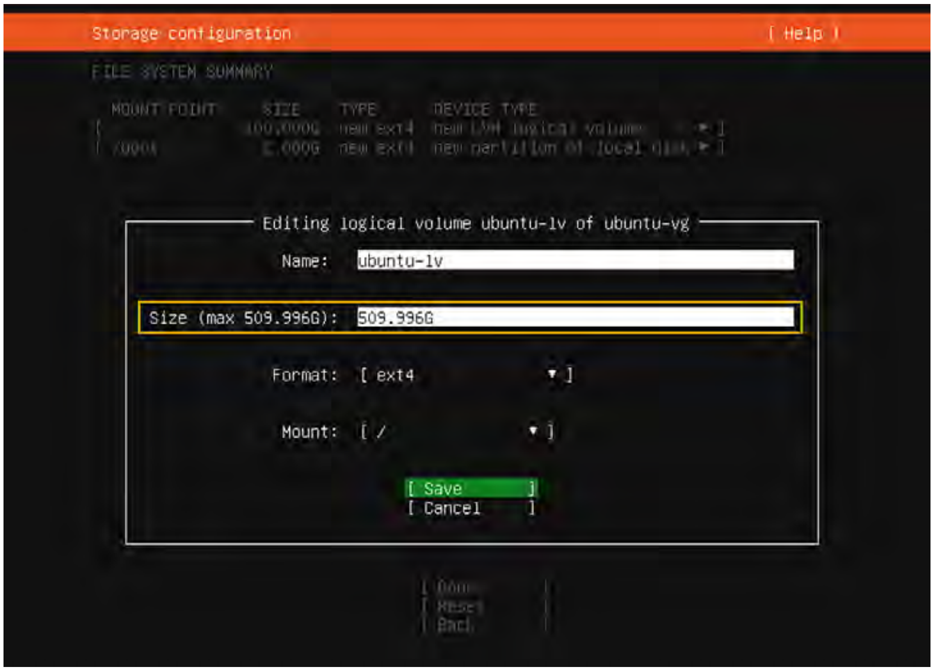
```
Guided storage configuration                                   [ Help ]

Configure a guided storage layout, or create a custom one:

(X)  Use an entire disk

     [ /dev/sda local disk 250.000G ▾ ]

     [X]  Set up this disk as an LVM group

          [ ]  Encrypt the LVM group with LUKS

                   Passphrase:


               Confirm passphrase:


( )  Custom storage layout
```

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**.



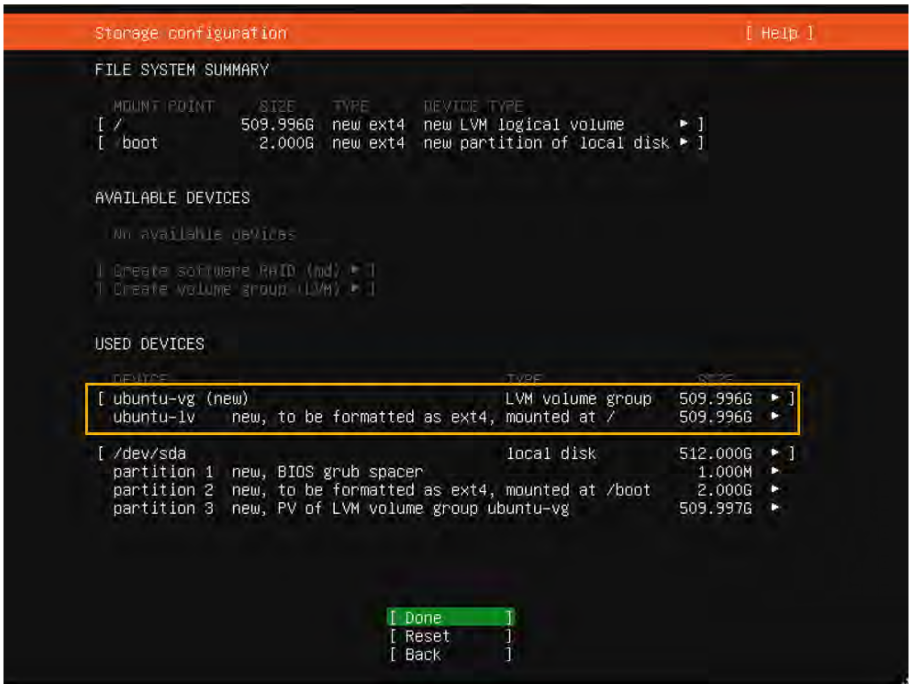
```
  Storage configuration                                                 [ Help ]
  FILE SYSTEM SUMMARY

    MOUNT POINT      SIZE     TYPE       DEVICE TYPE
  [ /             100.000G   new ext4   new LVM logical volume        ▸ ]
  [ /boot           2.000G   new ext4   new partition of local disk   ▸ ]

  AVAILABLE DEVICES

    DEVICE                                         TYPE                SIZE
  [ ubuntu-vg (new)                                LVM volume group    509.996G  ▸ ]
    free space                                                         409.996G  ▸

  [ Create software RAID (md) ▸ ]
  [ Create volume group (LVM) ▸ ]

  USED DEVICES

    DEVICE                                         TYPE                SIZE
  [ ubuntu-vg (new)                                LVM volume group    509.996G  ▸
    ubuntu-lv    new, to be formatted as ext4, mounted at /            100.000G  ▸  ◂ (close)
                                                                                      Edit
  [ /dev/sda                                       local disk          512.000G  ▸    Delete ▸
    partition 1  new, BIOS grub spacer                                   1.000M  ▸
    partition 2  new, to be formatted as ext4, mounted at /boot          2.000G  ▸
    partition 3  new, PV of LVM volume group ubuntu-vg                 509.997G  ▸

                              [ Done      ]
                              [ Reset     ]
                              [ Back      ]
```

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



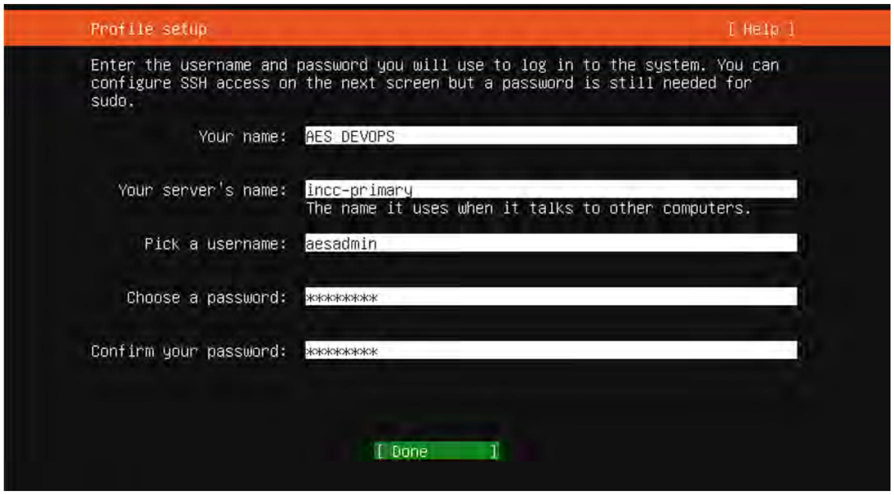
```
  Storage configuration                                                 [ Help ]
  FILE SYSTEM SUMMARY

    MOUNT POINT     SIZE      TYPE       DEVICE TYPE
  [ /             100.000G   new ext4   new LVM logical volume       ▸ ]
  [ /boot           2.000G   new ext4   new partition of local disk  ▸ ]

      ┌──────── Editing logical volume ubuntu-lv of ubuntu-vg ────────┐
      │            Name:  ubuntu-lv                                    │
      │                                                                │
      │ Size (max 509.996G):  509.996G                                 │
      │                                                                │
      │          Format:  [ ext4             ▾ ]                       │
      │                                                                │
      │           Mount:  [ /              ▾ ]                         │
      │                                                                │
      │                     [ Save      ]                              │
      │                     [ Cancel    ]                              │
      └────────────────────────────────────────────────────────────────┘

                              [ Done      ]
                              [ Reset     ]
                              [ Back      ]
```

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



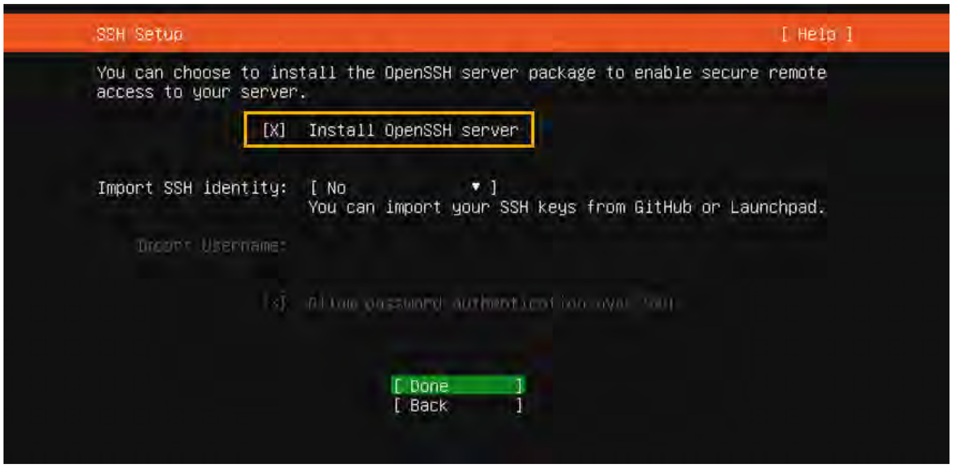
```
Storage configuration                                                  [ Help ]

FILE SYSTEM SUMMARY

  MOUNT POINT     SIZE    TYPE     DEVICE TYPE
[ /             509.996G  new ext4  new LVM logical volume     ▸ ]
[ /boot           2.000G  new ext4  new partition of local disk ▸ ]

AVAILABLE DEVICES

  No available devices

[ Create software RAID (md) ▸ ]
[ Create volume group (LVM) ▸ ]

USED DEVICES

  DEVICE                                       TYPE               SIZE
[ ubuntu-vg (new)                              LVM volume group   509.996G  ▸ ]
  ubuntu-lv    new, to be formatted as ext4, mounted at /         509.996G  ▸

[ /dev/sda                                     local disk         512.000G  ▸ ]
  partition 1  new, BIOS grub spacer                                1.000M  ▸
  partition 2  new, to be formatted as ext4, mounted at /boot       2.000G  ▸
  partition 3  new, PV of LVM volume group ubuntu-vg              509.997G  ▸


                              [ Done       ]
                              [ Reset      ]
                              [ Back       ]
```

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



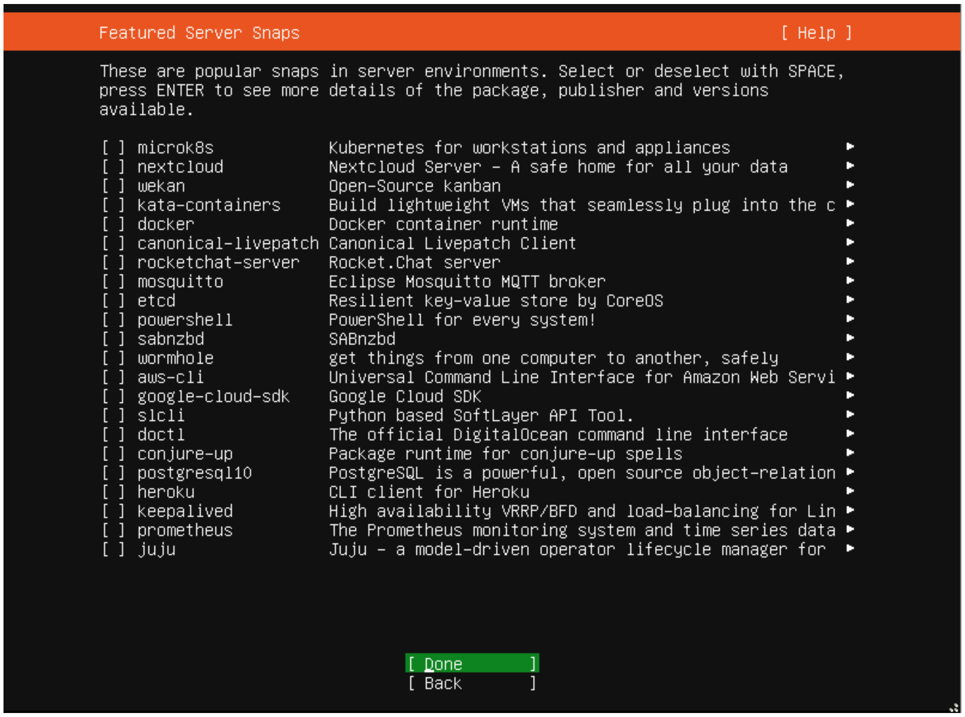
```
Profile setup                                                          [ Help ]

Enter the username and password you will use to log in to the system. You can
configure SSH access on the next screen but a password is still needed for
sudo.

            Your name:  AES DEVOPS

     Your server's name:  incc-primary
                        The name it uses when it talks to other computers.

       Pick a username:  aesadmin

     Choose a password:  *********

   Confirm your password:  *********


                          [ Done       ]
```

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



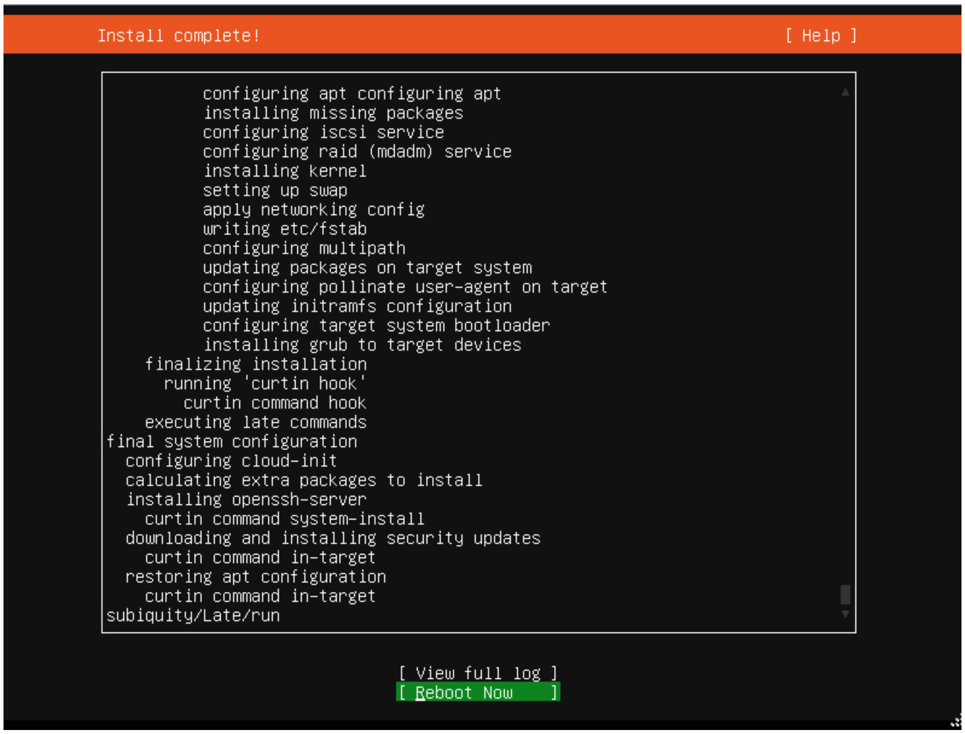
```
SSH Setup                                                    [ Help ]

You can choose to install the OpenSSH server package to enable secure remote
access to your server.

                   [X]  Install OpenSSH server

Import SSH identity:  [ No              ▾ ]
                      You can import your SSH keys from GitHub or Launchpad.

    Import Username:

                   [X]  Allow password authentication over SSH


                              [ Done       ]
                              [ Back       ]
```

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



```
Featured Server Snaps                                        [ Help ]

These are popular snaps in server environments. Select or deselect with SPACE,
press ENTER to see more details of the package, publisher and versions
available.

[ ] microk8s            Kubernetes for workstations and appliances          ▸
[ ] nextcloud           Nextcloud Server - A safe home for all your data    ▸
[ ] wekan               Open-Source kanban                                  ▸
[ ] kata-containers     Build lightweight VMs that seamlessly plug into the c ▸
[ ] docker              Docker container runtime                            ▸
[ ] canonical-livepatch Canonical Livepatch Client                          ▸
[ ] rocketchat-server   Rocket.Chat server                                  ▸
[ ] mosquitto           Eclipse Mosquitto MQTT broker                       ▸
[ ] etcd                Resilient key-value store by CoreOS                 ▸
[ ] powershell          PowerShell for every system!                        ▸
[ ] sabnzbd             SABnzbd                                             ▸
[ ] wormhole            get things from one computer to another, safely     ▸
[ ] aws-cli             Universal Command Line Interface for Amazon Web Servi ▸
[ ] google-cloud-sdk    Google Cloud SDK                                    ▸
[ ] slcli               Python based SoftLayer API Tool.                    ▸
[ ] doctl               The official DigitalOcean command line interface    ▸
[ ] conjure-up          Package runtime for conjure-up spells               ▸
[ ] postgresql10        PostgreSQL is a powerful, open source object-relation ▸
[ ] heroku              CLI client for Heroku                               ▸
[ ] keepalived          High availability VRRP/BFD and load-balancing for Lin ▸
[ ] prometheus          The Prometheus monitoring system and time series data ▸
[ ] juju                Juju - a model-driven operator lifecycle manager for  ▸


                              [ Done       ]
                              [ Back       ]
```

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



```
Install complete!                                              [ Help ]

          configuring apt configuring apt
          installing missing packages
          configuring iscsi service
          configuring raid (mdadm) service
          installing kernel
          setting up swap
          apply networking config
          writing etc/fstab
          configuring multipath
          updating packages on target system
          configuring pollinate user-agent on target
          updating initramfs configuration
          configuring target system bootloader
          installing grub to target devices
    finalizing installation
      running 'curtin hook'
        curtin command hook
    executing late commands
final system configuration
  configuring cloud-init
  calculating extra packages to install
  installing openssh-server
    curtin command system-install
  downloading and installing security updates
    curtin command in-target
  restoring apt configuration
    curtin command in-target
subiquity/Late/run
```

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):

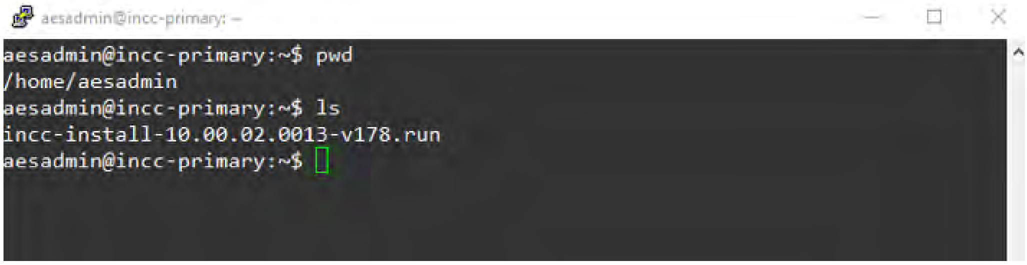
  USERNAME=**aesadmin** && sudo useradd -m -d /home/${USERNAME} ${USERNAME} && sudo usermod -aG sudo ${USERNAME} && sudo usermod -s /bin/bash ${USERNAME} && sudo passwd ${USERNAME}

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).



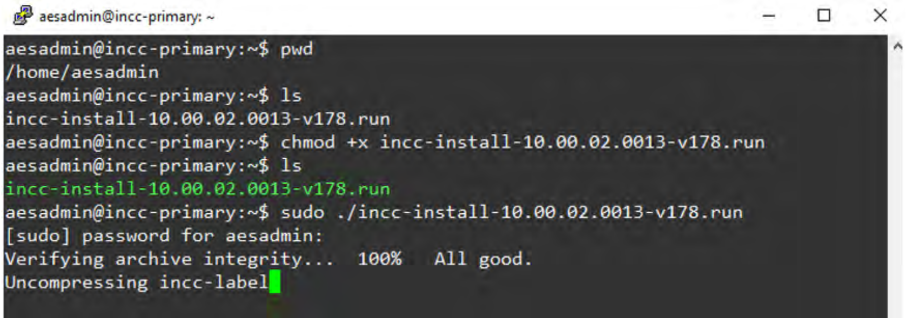
```
aesadmin@incc-primary:~$ pwd
/home/aesadmin
aesadmin@incc-primary:~$ ls
incc-install-10.00.02.0013-v178.run
aesadmin@incc-primary:~$ 
```

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



```
aesadmin@incc-primary:~$ pwd
/home/aesadmin
aesadmin@incc-primary:~$ ls
incc-install-10.00.02.0013-v178.run
aesadmin@incc-primary:~$ chmod +x incc-install-10.00.02.0013-v178.run
aesadmin@incc-primary:~$ ls
incc-install-10.00.02.0013-v178.run
aesadmin@incc-primary:~$ sudo ./incc-install-10.00.02.0013-v178.run
[sudo] password for aesadmin:
Verifying archive integrity...  100%   All good.
Uncompressing incc-label
```

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.

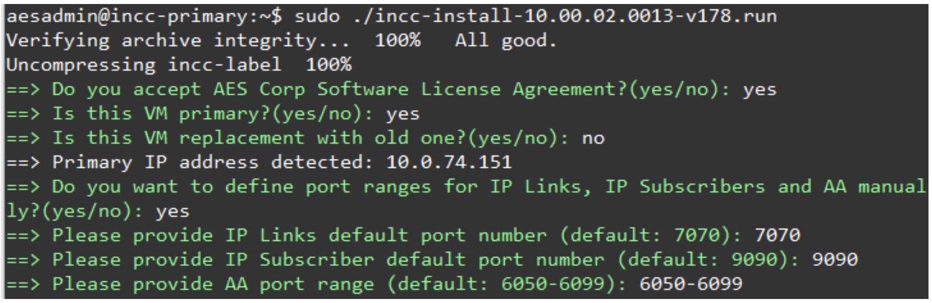
  IP Link default port: **7070**

  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
```

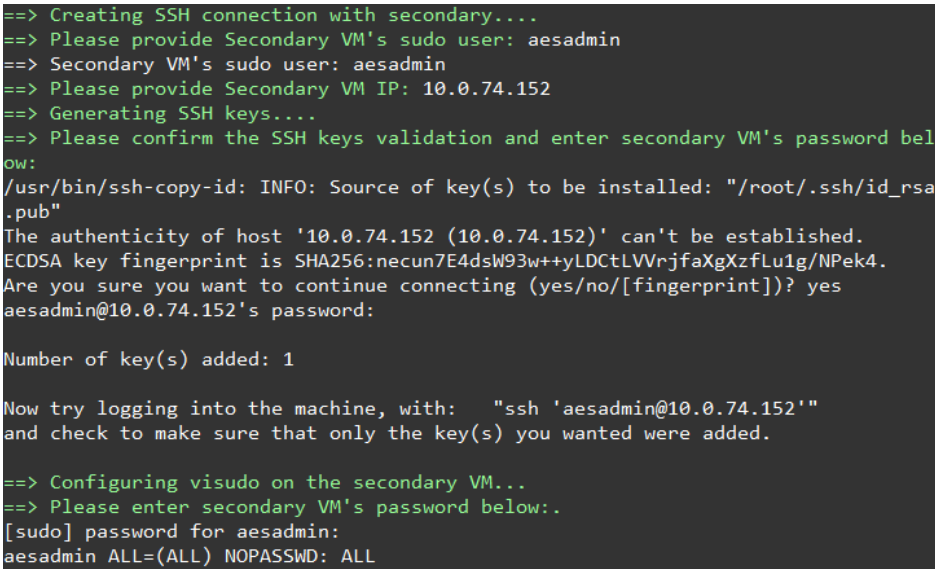
Note: Keep in mind that your firewall should allow ports 80, 443, and the ports that you defined above for IP Links, IP subscribers, and AA.

- Please provide Secondary VMs sudo user:

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

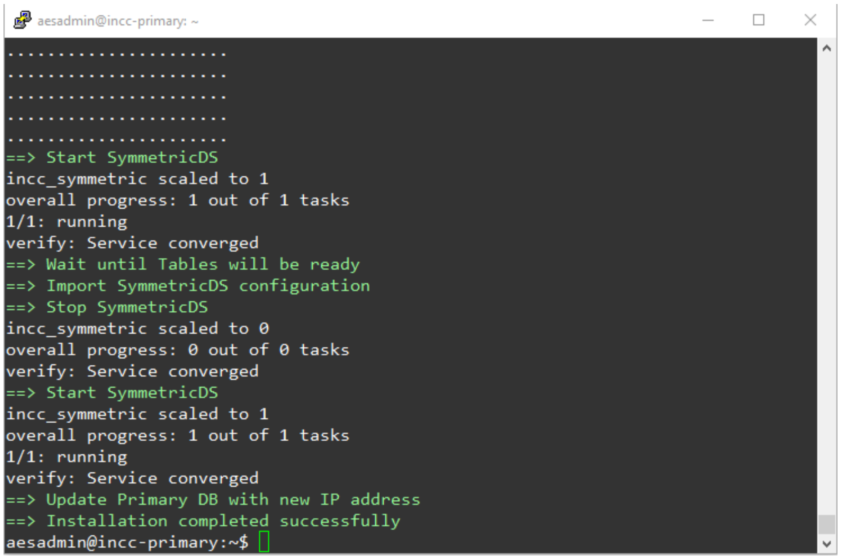
- Please provide Secondary VM IP:

  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:



```
......................
......................
......................
......................
......................
==> Start SymmetricDS
incc_symmetric scaled to 1
overall progress: 1 out of 1 tasks
1/1: running
verify: Service converged
==> Wait until Tables will be ready
==> Import SymmetricDS configuration
==> Stop SymmetricDS
incc_symmetric scaled to 0
overall progress: 0 out of 0 tasks
verify: Service converged
==> Start SymmetricDS
incc_symmetric scaled to 1
overall progress: 1 out of 1 tasks
1/1: running
verify: Service converged
==> Update Primary DB with new IP address
==> Installation completed successfully
aesadmin@incc-primary:~$
```

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.

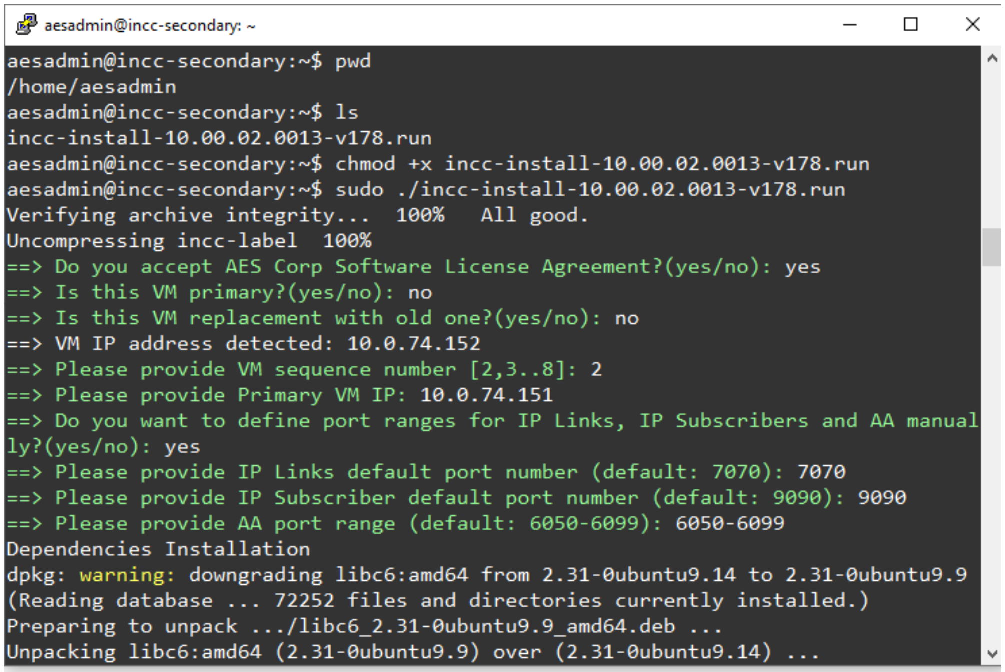
  IP Link default port: **7070**

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

  IP Subscriber default port: **9090**

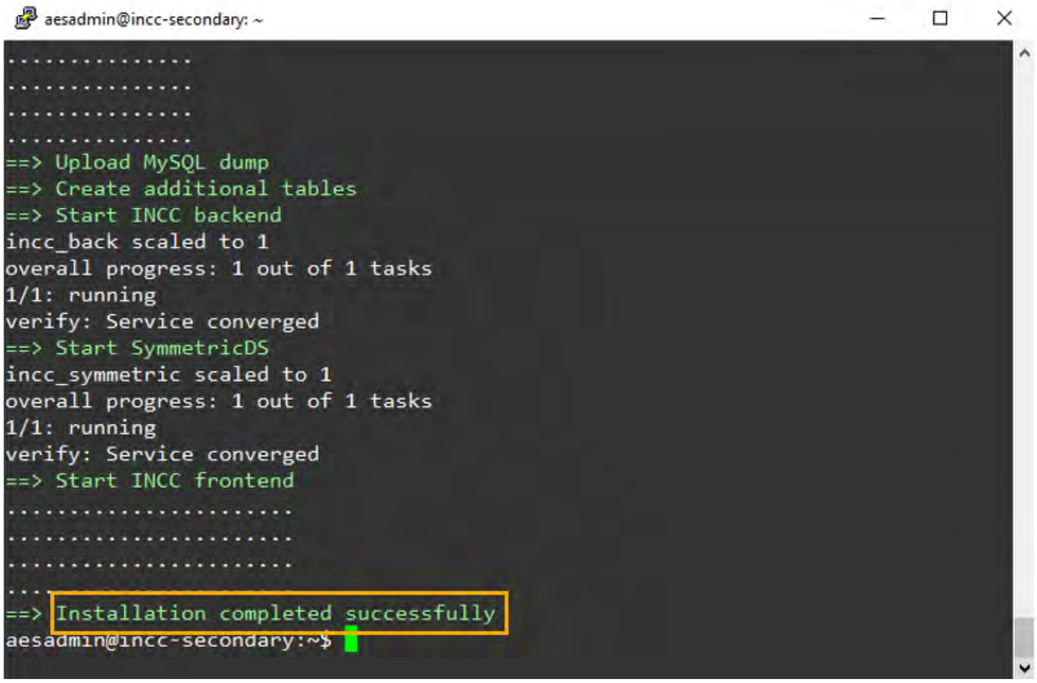
  IP Subscriber default port ranges: **9000-9099**

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



```
aesadmin@incc-secondary:~$ pwd
/home/aesadmin
aesadmin@incc-secondary:~$ ls
incc-install-10.00.02.0013-v178.run
aesadmin@incc-secondary:~$ chmod +x incc-install-10.00.02.0013-v178.run
aesadmin@incc-secondary:~$ 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): no
==> Is this VM replacement with old one?(yes/no): no
==> VM IP address detected: 10.0.74.152
==> Please provide VM sequence number [2,3..8]: 2
==> Please provide Primary VM IP: 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
Dependencies Installation
dpkg: warning: downgrading libc6:amd64 from 2.31-0ubuntu9.14 to 2.31-0ubuntu9.9
(Reading database ... 72252 files and directories currently installed.)
Preparing to unpack .../libc6_2.31-0ubuntu9.9_amd64.deb ...
Unpacking libc6:amd64 (2.31-0ubuntu9.9) over (2.31-0ubuntu9.14) ...
```

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



```
...............
...............
...............
...............
==> Upload MySQL dump
==> Create additional tables
==> Start INCC backend
incc_back scaled to 1
overall progress: 1 out of 1 tasks
1/1: running
verify: Service converged
==> Start SymmetricDS
incc_symmetric scaled to 1
overall progress: 1 out of 1 tasks
1/1: running
verify: Service converged
==> Start INCC frontend
.......................
.......................
.......................
...
==> Installation completed successfully
aesadmin@incc-secondary:~$
```

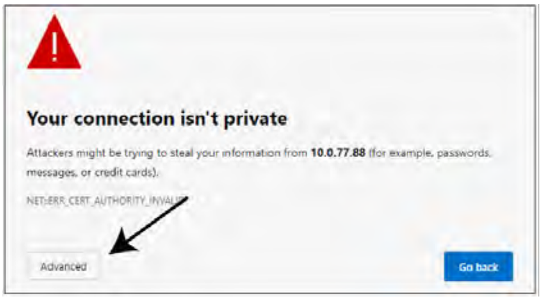
Logging in to the INCC Web Interface

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

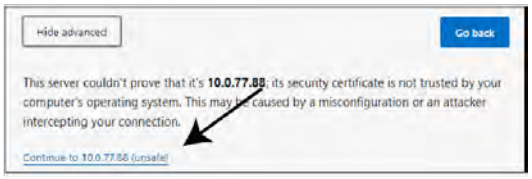
7. Click **Advanced**, then proceed to the IP address.



Your connection isn't private

Attackers might be trying to steal your information from **10.0.77.88** (for example, passwords, messages, or credit cards).

NET::ERR_CERT_AUTHORITY_INVALID



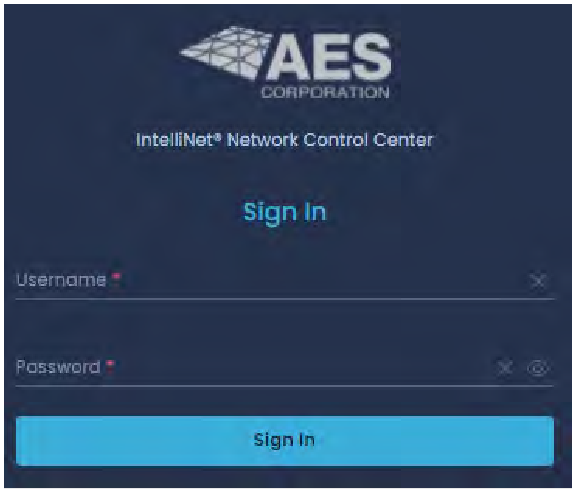
This server couldn't prove that it's **10.0.77.88**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Continue to 10.0.77.88 (unsafe)

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 (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 (i.e., if you created "01.01.2023" folder and you have a sudo user named "aesadmin" the folder will be home/aesadmin/01.01.2023).

Navigate to the new folder:

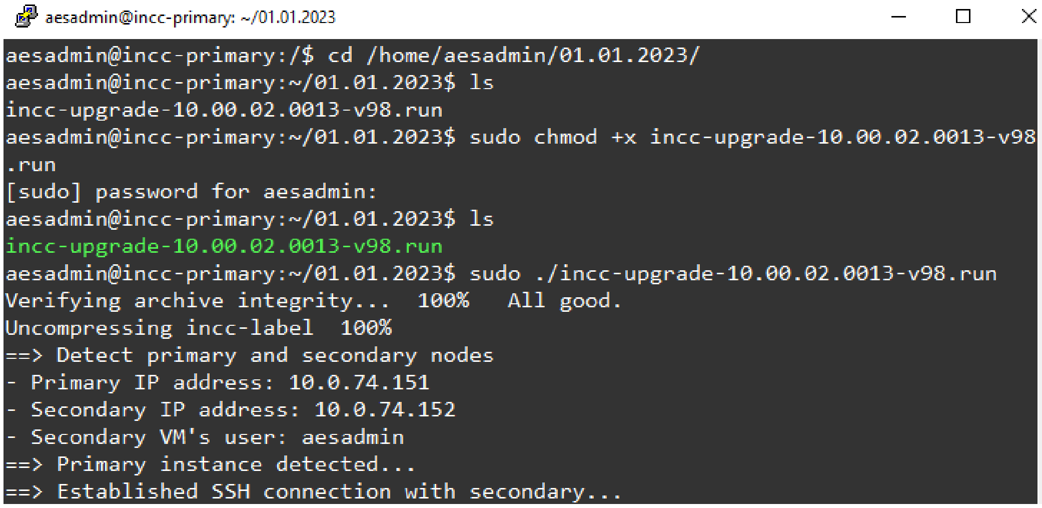
cd /home/aesadmin/01.01.2023

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**



```
aesadmin@incc-primary:/$ cd /home/aesadmin/01.01.2023/
aesadmin@incc-primary:~/01.01.2023$ ls
incc-upgrade-10.00.02.0013-v98.run
aesadmin@incc-primary:~/01.01.2023$ sudo chmod +x incc-upgrade-10.00.02.0013-v98
.run
[sudo] password for aesadmin:
aesadmin@incc-primary:~/01.01.2023$ ls
incc-upgrade-10.00.02.0013-v98.run
aesadmin@incc-primary:~/01.01.2023$ sudo ./incc-upgrade-10.00.02.0013-v98.run
Verifying archive integrity...  100%   All good.
Uncompressing incc-label  100%
==> Detect primary and secondary nodes
- Primary IP address: 10.0.74.151
- Secondary IP address: 10.0.74.152
- Secondary VM's user: aesadmin
==> Primary instance detected...
==> Established SSH connection with secondary...
```

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

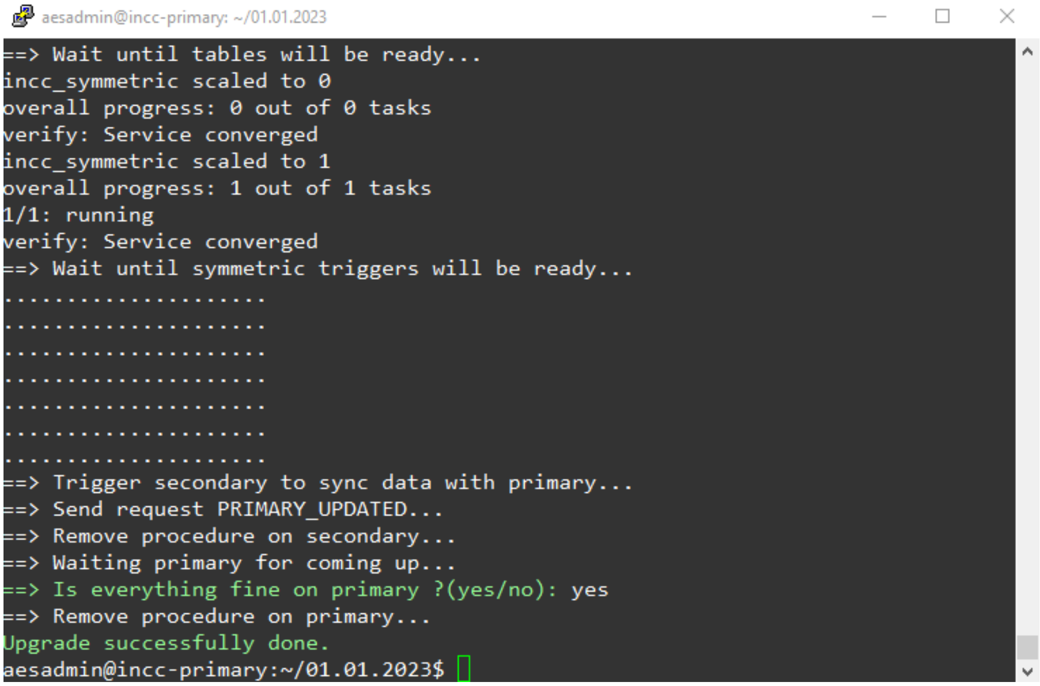
- Is everything fine on secondary? (yes/no):

  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 will be finished:



```
==> Wait until tables will be ready...
incc_symmetric scaled to 0
overall progress: 0 out of 0 tasks
verify: Service converged
incc_symmetric scaled to 1
overall progress: 1 out of 1 tasks
1/1: running
verify: Service converged
==> Wait until symmetric triggers will be ready...
.....................
.....................
.....................
.....................
.....................
.....................
.....................
==> Trigger secondary to sync data with primary...
==> Send request PRIMARY_UPDATED...
==> Remove procedure on secondary...
==> Waiting primary for coming up...
==> Is everything fine on primary ?(yes/no): yes
==> Remove procedure on primary...
Upgrade successfully done.
aesadmin@incc-primary:~/01.01.2023$
```

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:

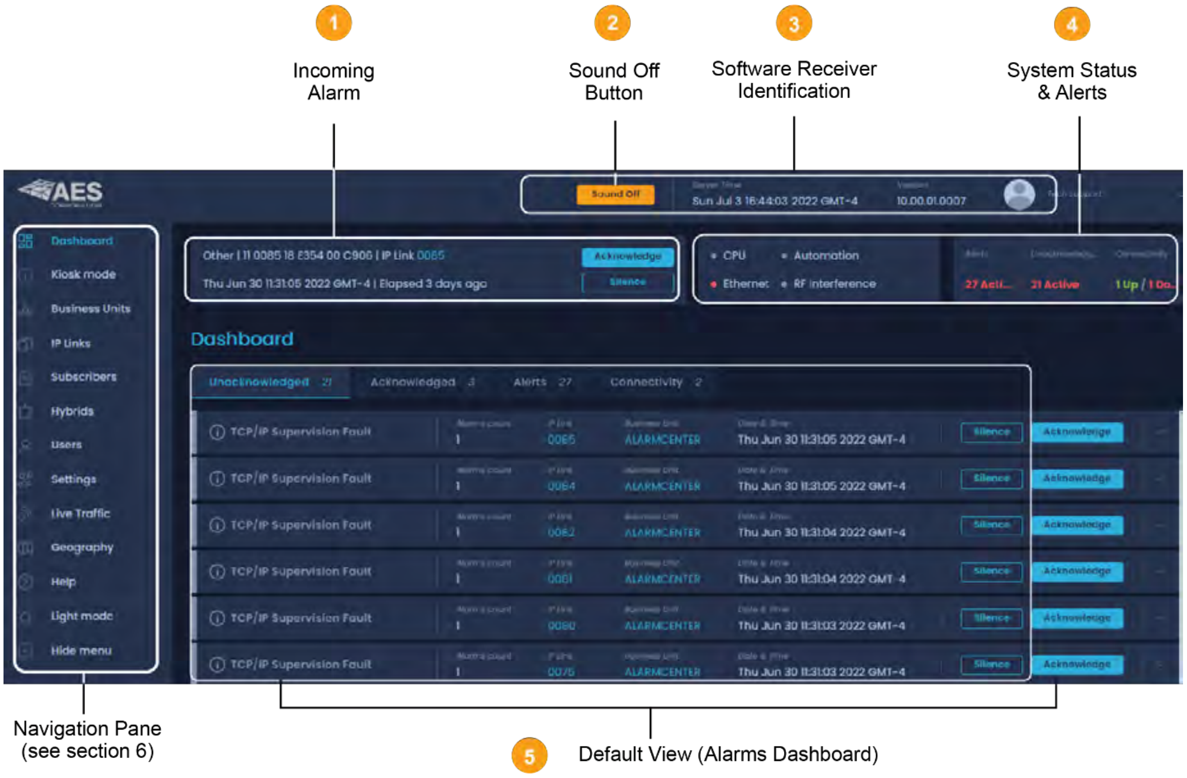
- 22 (SSH)
- 3306 (MySQL)
- 31415 (SymmetricDS)

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 allows you to configure the IntelliNet system, view information about the system, and process alarms.



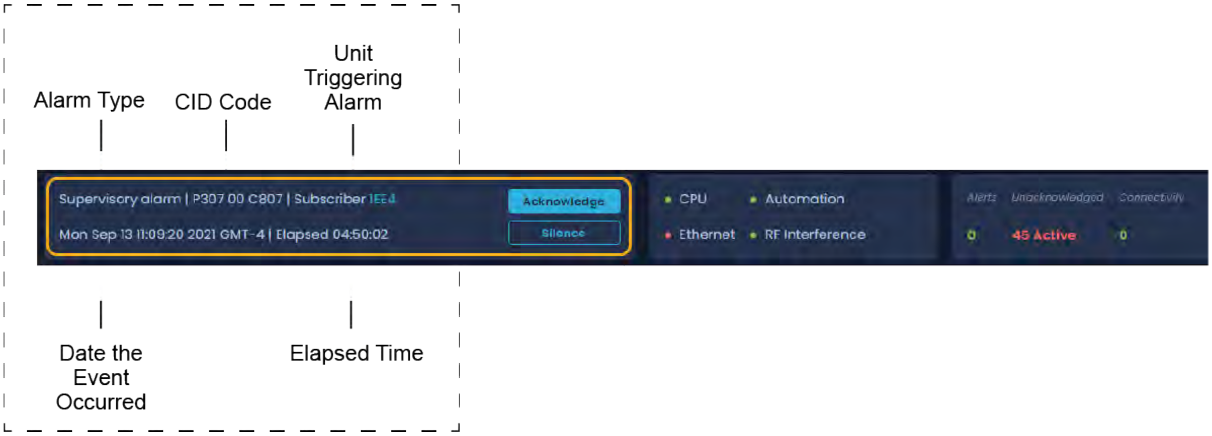
Sun Jul 3 16:44:03 2022 GMT-4 10.00.01.0007

Other | 11 0085 18 E354 00 C906 | IP Link 0085
Thu Jun 30 11:31:05 2022 GMT-4 | Elapsed 3 days ago

TCP/IP Supervision Fault	1	0085	ALARMCENTER	Thu Jun 30 11:31:05 2022 GMT-4	Silence	Acknowledge
TCP/IP Supervision Fault	1	0084	ALARMCENTER	Thu Jun 30 11:31:05 2022 GMT-4	Silence	Acknowledge
TCP/IP Supervision Fault	1	0082	ALARMCENTER	Thu Jun 30 11:31:04 2022 GMT-4	Silence	Acknowledge
TCP/IP Supervision Fault	1	0081	ALARMCENTER	Thu Jun 30 11:31:04 2022 GMT-4	Silence	Acknowledge
TCP/IP Supervision Fault	1	0080	ALARMCENTER	Thu Jun 30 11:31:03 2022 GMT-4	Silence	Acknowledge
TCP/IP Supervision Fault	1	0076	ALARMCENTER	Thu Jun 30 11:31:03 2022 GMT-4	Silence	Acknowledge

Incoming Alarm

Exploring the INCC Control Center Dashboard 1 **Incoming Alarm**



Supervisory alarm | P307 00 C807 | Subscriber 1EE4
Mon Sep 13 11:09:20 2021 GMT-4 | Elapsed 04:50:02

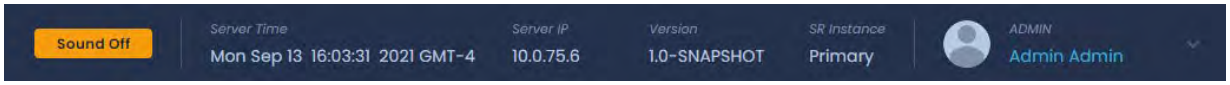
Alerts: 0 | Unacknowledged: 45 Active | Connectivity: 0

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

Exploring the INCC Control Center Dashboard **2** **Sound Off Button**

The **Sound Off** button allows you to silence every alarm for all subscribers on the system.

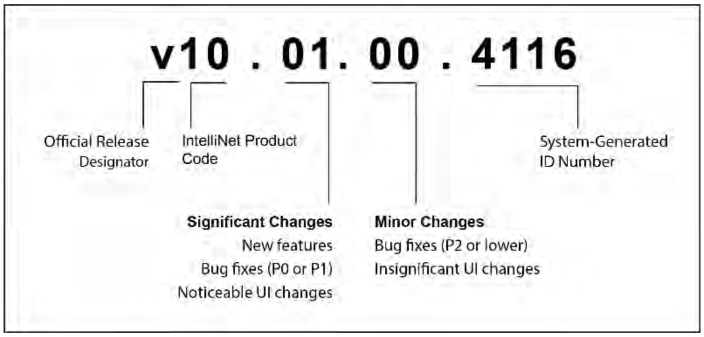


Server Time: Mon Sep 13 16:03:31 2021 GMT-4
Server IP: 10.0.75.6
Version: 1.0-SNAPSHOT
SR Instance: Primary
ADMIN: Admin Admin

Software Receiver Identification

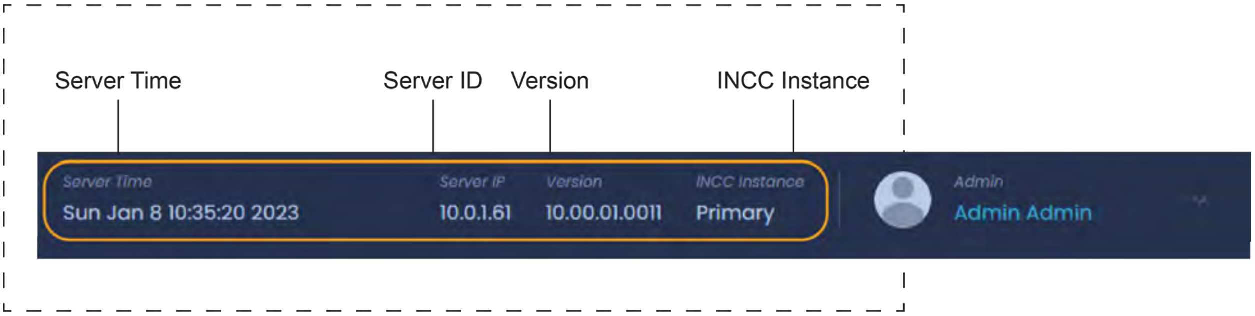
Exploring the INCC Control Center Dashboard **3** **Software Receiver Identification**

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 105 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.)



Server Time Sun Jan 8 10:35:20 2023

Server IP 10.0.1.61

Version 10.00.01.0011

INCC Instance Primary

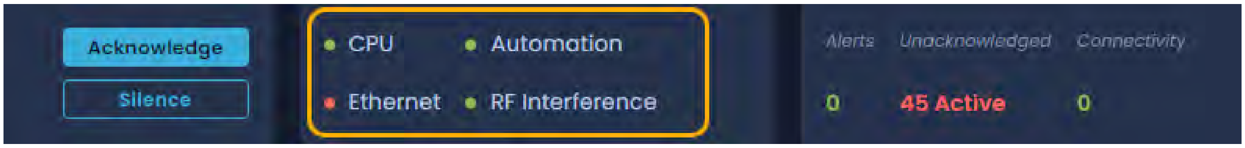
Admin Admin Admin

System Status & Alerts

Exploring the INCC Control Center Dashboard **4** **System Status and 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).



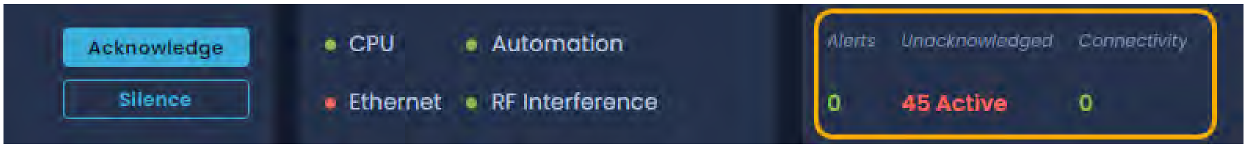
Alerts 0

Unacknowledged 45 Active

Connectivity 0

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	Unacknowledged	Connectivity
0	45 Active	0

- *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.
  - Alarms Dashboard

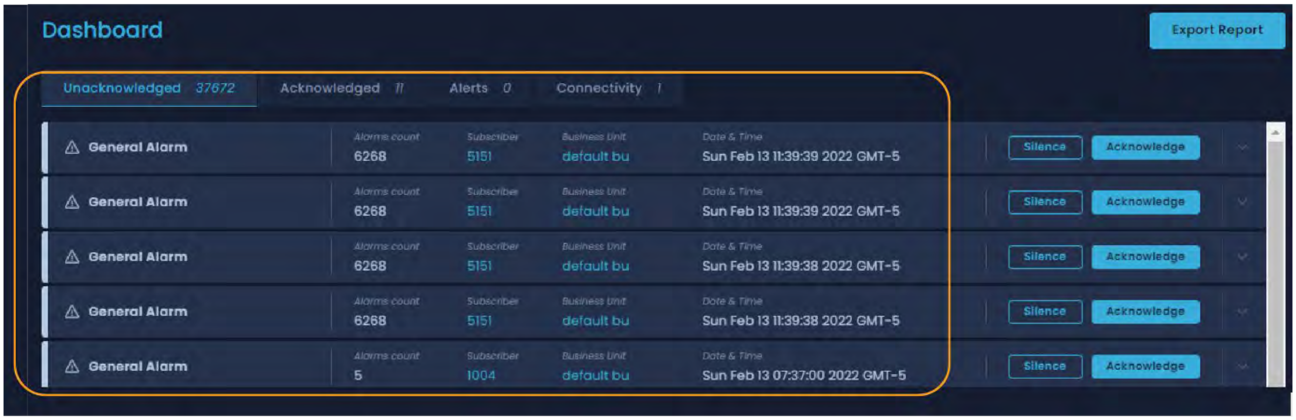
Exploring the INCC Control Center Dashboard

5 Default View (Alarms Dashboard)

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

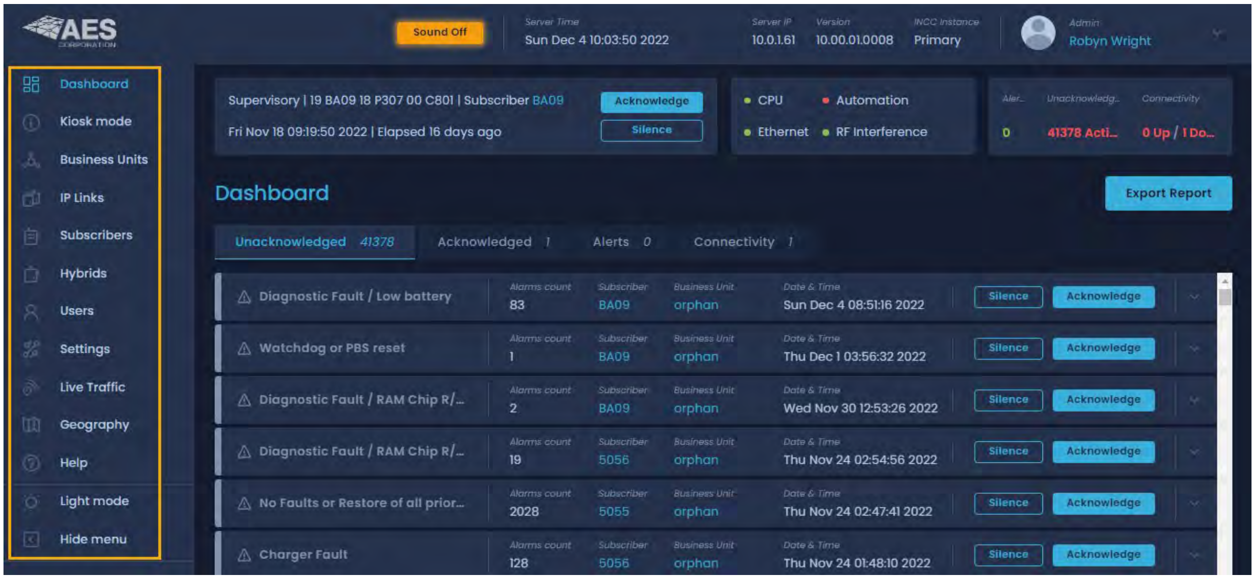
Alarms that haven't been processed due to a failure in alarm automation are displayed in the Alarms Dashboard. These alarms will remain active until they are acknowledged. Once alarm automation restarts, alarms will automatically be moved and cleared from the system and will be visible from the Acknowledged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

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



	Alarms count	Subscriber	Business Unit	Date & Time
General Alarm	6268	5151	default bu	Sun Feb 13 11:39:39 2022 GMT-5
General Alarm	6268	5151	default bu	Sun Feb 13 11:39:39 2022 GMT-5
General Alarm	6268	5151	default bu	Sun Feb 13 11:39:38 2022 GMT-5
General Alarm	6268	5151	default bu	Sun Feb 13 11:39:38 2022 GMT-5
General Alarm	5	1004	default bu	Sun Feb 13 07:37:00 2022 GMT-5

7. INCC Navigation Pane



Server Time	Server IP	Version	INCC Instance	Admin
Sun Dec 4 10:03:50 2022	10.0.1.61	10.00.01.0008	Primary	Robyn Wright

Supervisory | 19 BA09 18 P307 00 C801 | Subscriber BA09

Fri Nov 18 09:19:50 2022 | Elapsed 16 days ago

Aler...	Unacknowledg...	Connectivity
0	41378 Acti...	0 Up / 1 Do...

	Alarms count	Subscriber	Business Unit	Date & Time
Diagnostic Fault / Low battery	83	BA09	orphan	Sun Dec 4 08:51:16 2022
Watchdog or PBS reset	1	BA09	orphan	Thu Dec 1 03:56:32 2022
Diagnostic Fault / RAM Chip R/...	2	BA09	orphan	Wed Nov 30 12:53:26 2022
Diagnostic Fault / RAM Chip R/...	19	5056	orphan	Thu Nov 24 02:54:56 2022
No Faults or Restore of all prior...	2028	5055	orphan	Thu Nov 24 02:47:41 2022
Charger Fault	128	5056	orphan	Thu Nov 24 01:48:10 2022

Dashboard

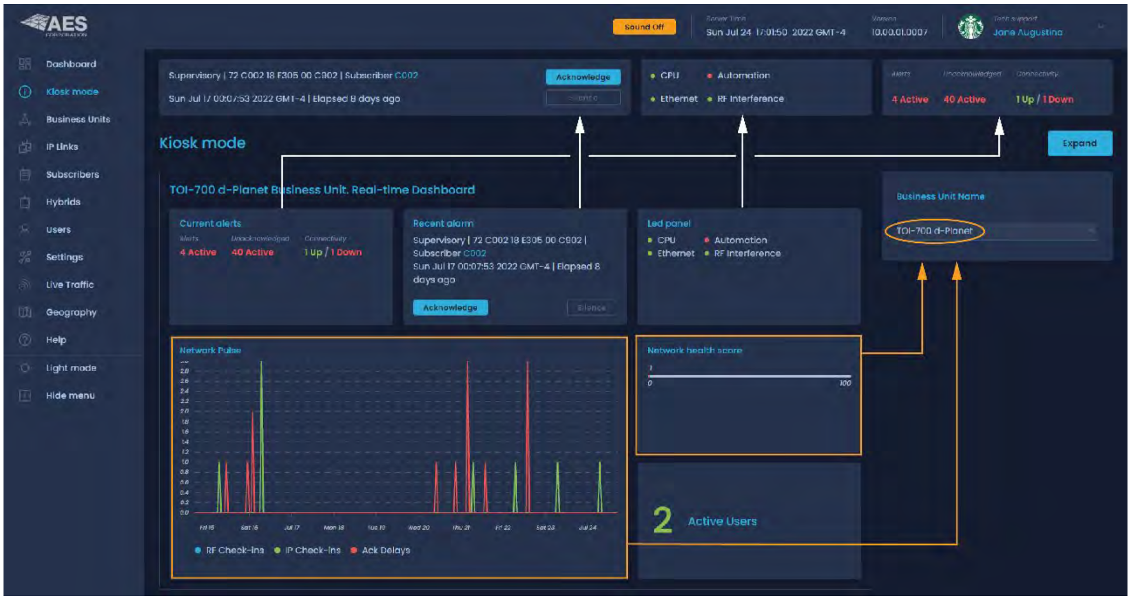
The Alarms Dashboard is the default view of the INCC Control Center dashboard (the alarms dashboard is described on page 37).

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.



Supervisory | 72 C002 18 E305 00 C902 | Subscriber C002

Sun Jul 17 00:07:53 2022 GMT-4 | Elapsed 8 days ago

Server Time Sun Jul 24 17:01:50 2022 GMT-4

Version 10.00.01.0007

Tech support Jane Augustino

Alerts 4 Active · Unacknowledged 40 Active · Connectivity 1 Up / 1 Down

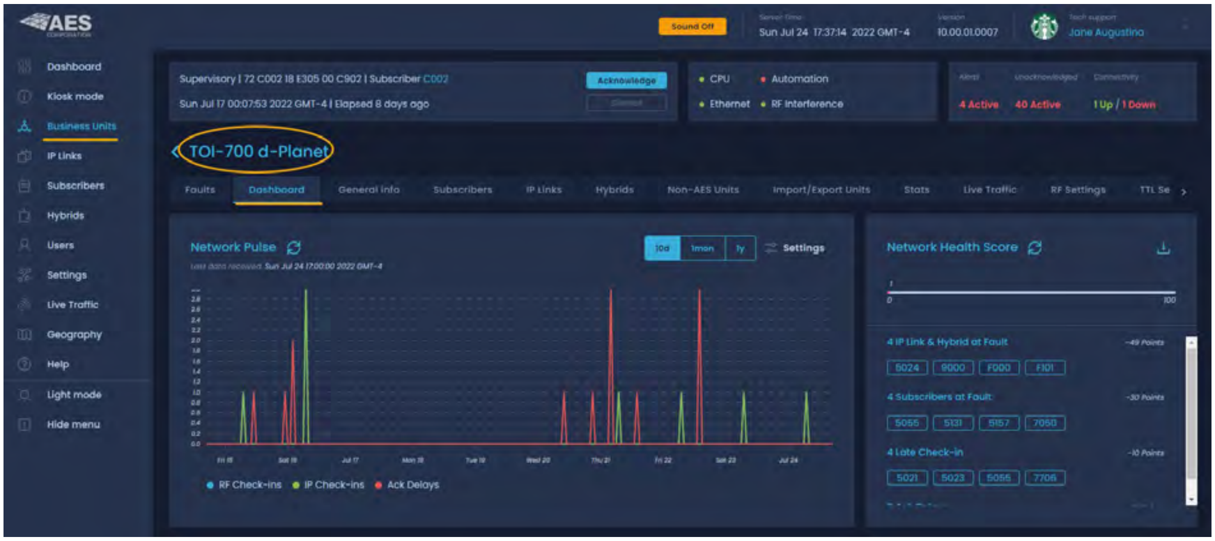
TOI-700 d-Planet Business Unit. Real-time Dashboard

Recent alarm: Supervisory | 72 C002 18 E305 00 C902 | Subscriber C002 Sun Jul 17 00:07:53 2022 GMT-4 | Elapsed 8 days ago

Business Unit Name: TOI-700 d-Planet

2 Active Users

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 (see also the **Error! Reference source not found.** on page **Error! Bookmark not defined.**).



Supervisory | 72 C002 18 E305 00 C902 | Subscriber C002

Sun Jul 17 00:07:53 2022 GMT-4 | Elapsed 8 days ago

Server Time Sun Jul 24 17:37:14 2022 GMT-4

Version 10.00.01.0007

Tech support Jane Augustino

Alerts 4 Active · Unacknowledged 40 Active · Connectivity 1 Up / 1 Down

TOI-700 d-Planet

Last data received: Sun Jul 24 17:00:00 2022 GMT-4

Network Health Score

4 IP Link & Hybrid at Fault −49 Points: 5024 · 9000 · F000 · F101

4 Subscribers at Fault −30 Points: 5055 · 5131 · 5157 · 7050

4 Late Check-in −10 Points: 5021 · 5023 · 5055 · 7706

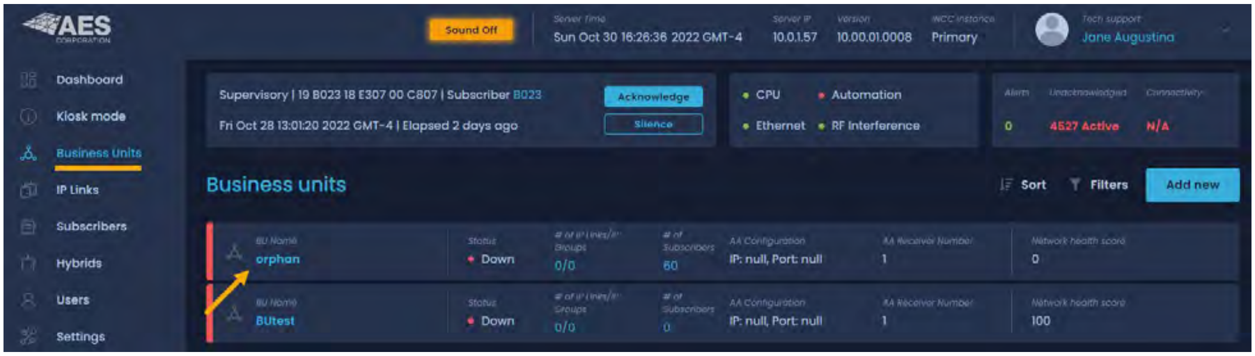
Business Units

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 **Error! Reference source not found.**.



Supervisory | 19 B023 18 E307 00 C807 | Subscriber B023
Fri Oct 28 13:01:20 2022 GMT-4 | Elapsed 2 days ago

Business units

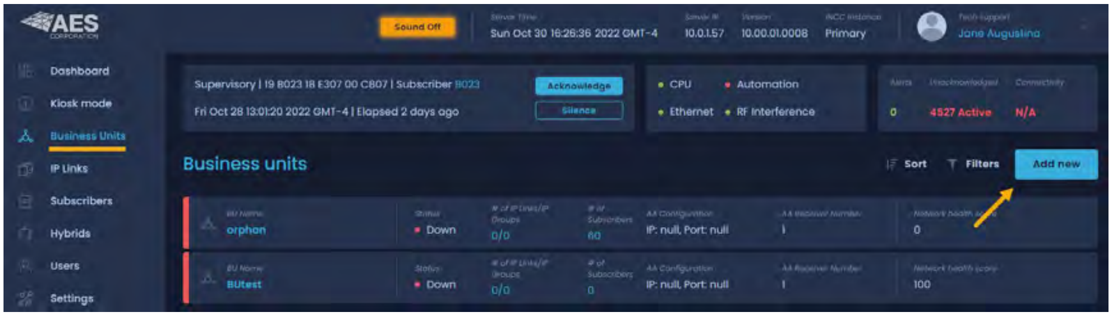
BU Name	Status	# of IP Lines/IP Groups	# of Subscribers	AA Configuration	AA Receiver Number	Network health score
orphan	Down	0/0	60	IP: null, Port: null	1	0
BUtest	Down	0/0	0	IP: null, Port: null	1	100

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**.

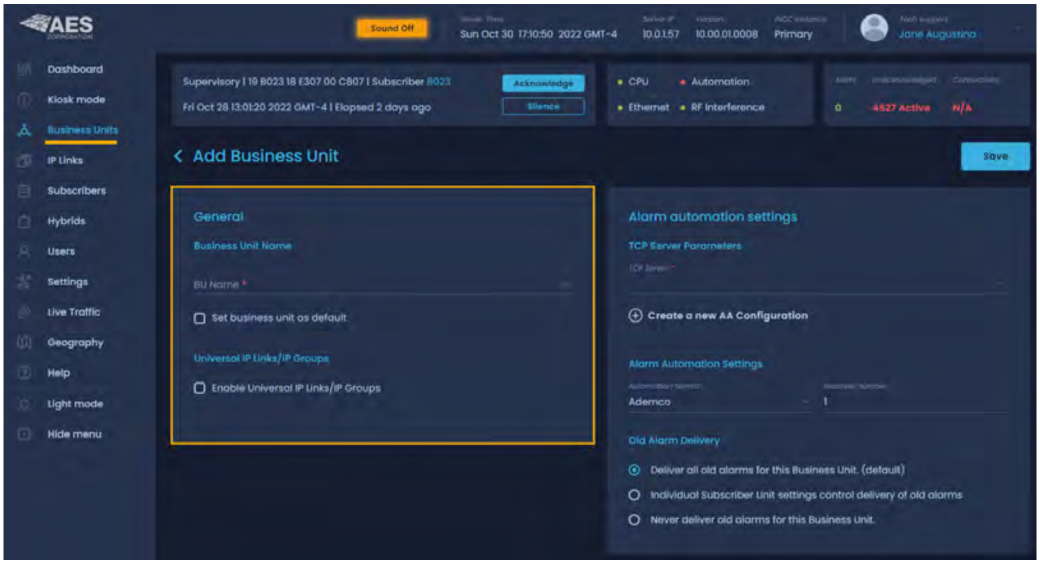

Supervisory | 19 B023 18 E307 00 C807 | Subscriber B023
Fri Oct 28 13:01:20 2022 GMT-4 | Elapsed 2 days ago

Business units

BU Name	Status	# of IP Lines/IP Groups	# of Subscribers	AA Configuration	AA Receiver Number	Network health score
orphan	Down	0/0	60	IP: null, Port: null	1	0
BUtest	Down	0/0	0	IP: null, Port: null	1	100

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).



Add Business Unit

General

Business Unit Name

BU Name *

□ Set business unit as default

Universal IP Links/IP Groups

□ Enable Universal IP Links/IP Groups

Alarm automation settings

TCP Server Parameters

TCP Server *

⊕ Create a new AA Configuration

Alarm Automation Settings

Adernco

1

Old Alarm Delivery

● Deliver all old alarms for this Business Unit. (default)

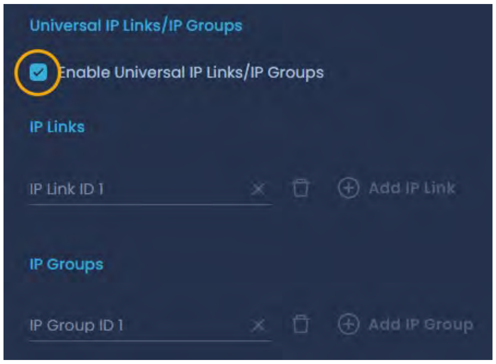
○ Individual Subscriber Unit settings control delivery of old alarms

○ Never deliver old alarms for this Business Unit.

- **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.



Universal IP Links/IP Groups

☑ Enable Universal IP Links/IP Groups

IP Links

IP Link ID 1

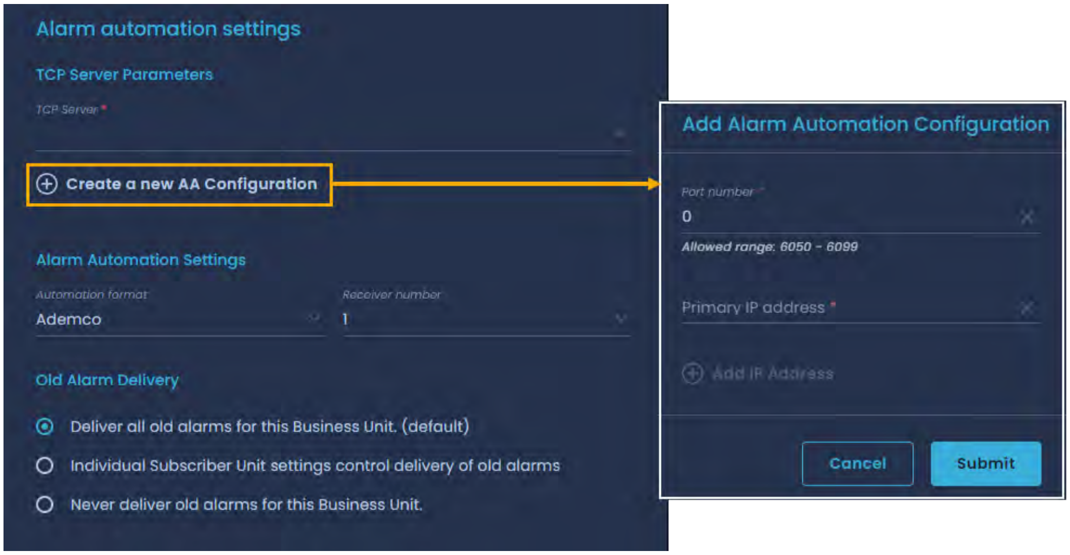
IP Groups

IP Group ID 1

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:



Alarm automation settings

TCP Server Parameters

TCP Server *

Alarm Automation Settings

Automation format: Ademco

Receiver number: 1

Old Alarm Delivery

◉ Deliver all old alarms for this Business Unit. (default)

○ Individual Subscriber Unit settings control delivery of old alarms

○ Never deliver old alarms for this Business Unit.

Add Alarm Automation Configuration

Port number *: 0

Allowed range: 6050 - 6099

Primary IP address *

- **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)

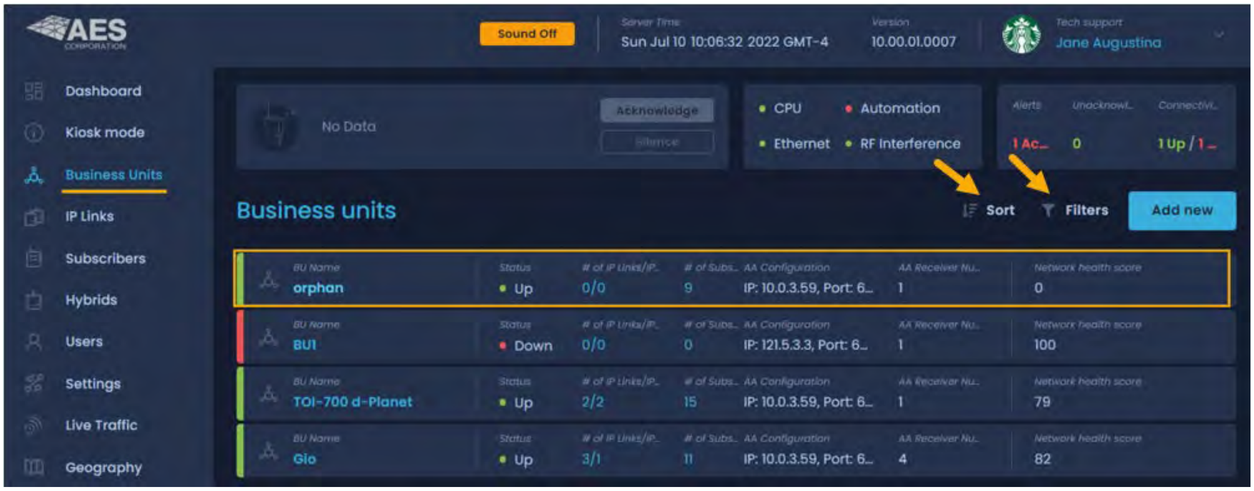
– Individual Subscriber Unit settings control delivery of old alarms (configuration for each subscriber set in the subscriber unit setting)

– 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



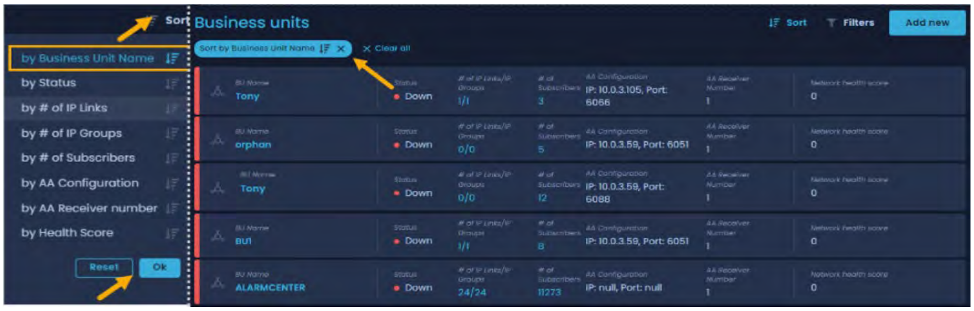
BU Name	Status	# of IP Links/IP...	# of Subs...	AA Configuration	AA Receiver Nu...	Network health score
orphan	● Up	0/0	9	IP: 10.0.3.59, Port: 6...	1	0
BU1	● Down	0/0	0	IP: 121.5.3.3, Port: 6...	1	100
TOI-700 d-Planet	● Up	2/2	15	IP: 10.0.3.59, Port: 6...	1	79
Gio	● Up	3/1	11	IP: 10.0.3.59, Port: 6...	4	82

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.

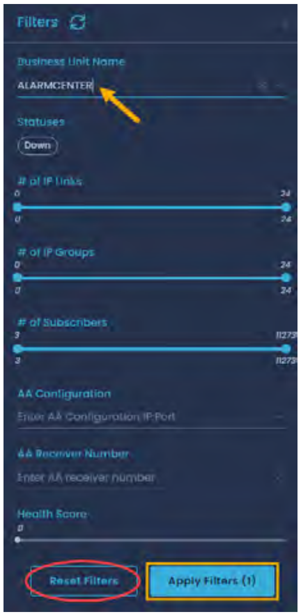
Sort selection *Result*



BU Name	Status	# of IP Links/IP Groups	# of Subscribers	AA Configuration	AA Receiver Number	Network health score
Tony	Down	1/1	3	IP: 10.0.3.105, Port: 6066	1	0
orphan	Down	0/0	5	IP: 10.0.3.59, Port: 6051	1	0
Tony	Down	0/0	12	IP: 10.0.3.59, Port: 6088	1	0
BU1	Down	1/1	8	IP: 10.0.3.59, Port: 6051	1	0
ALARMCENTER	Down	24/24	11273	IP: null, Port: null	1	0

- 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*



Business Unit Name: ALARMCENTER

Statuses: Down

# of IP Links: 0 – 24

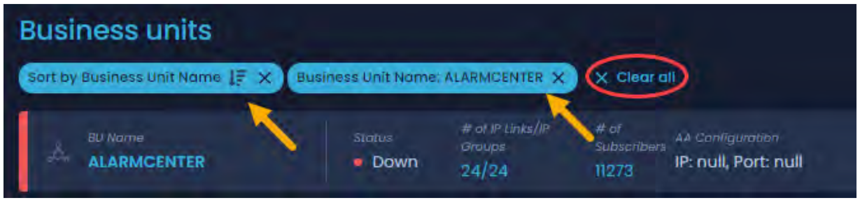
# of IP Groups: 0 – 24

# of Subscribers: 3 – 11273

AA Configuration: Enter AA Configuration IP:Port

AA Receiver Number: Enter AA receiver number

Health Score: 0

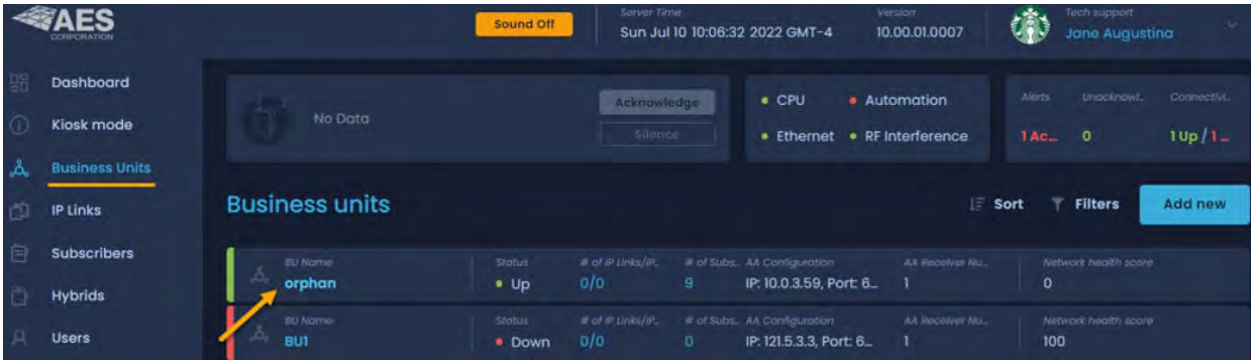


BU Name	Status	# of IP Links/IP Groups	# of Subscribers	AA Configuration
ALARMCENTER	Down	24/24	11273	IP: null, Port: null

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.

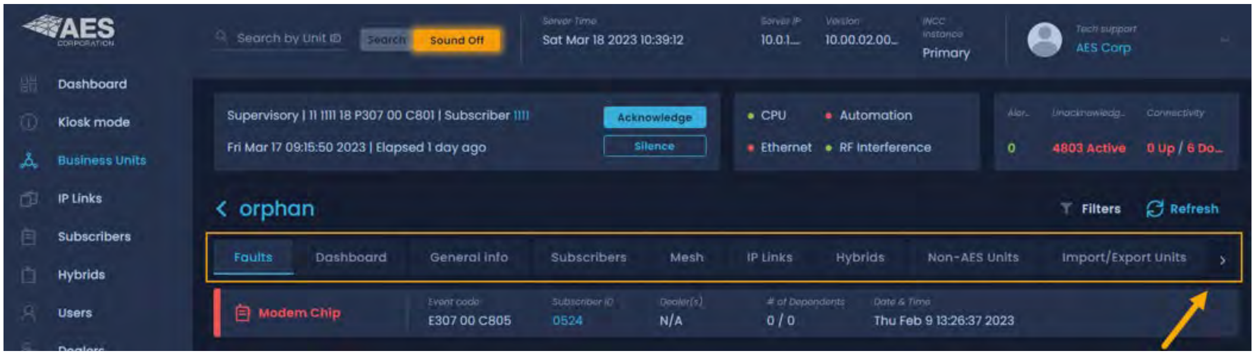


Server Time: Sun Jul 10 10:06:32 2022 GMT-4 | Version: 10.00.01.0007 | Tech support: Jane Augustina

Alerts: 1 Ac... | Unacknowl...: 0 | Connectivi...: 1 Up / 1...

BU Name	Status	# of IP Links/IP...	# of Subs...	AA Configuration	AA Receiver Nu...	Network health score
orphan	Up	0/0	9	IP: 10.0.3.59, Port: 6...	1	0
BU1	Down	0/0	0	IP: 121.5.3.3, Port: 6...	1	100

Each individual business unit has 14 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.)



Server Time: Sat Mar 18 2023 10:39:12 | Server IP: 10.0.1... | Version: 10.00.02.00... | INCC instance: Primary | Tech support: AES Corp

Supervisory | 11 1111 18 P307 00 C801 | Subscriber 1111
Fri Mar 17 09:15:50 2023 | Elapsed 1 day ago

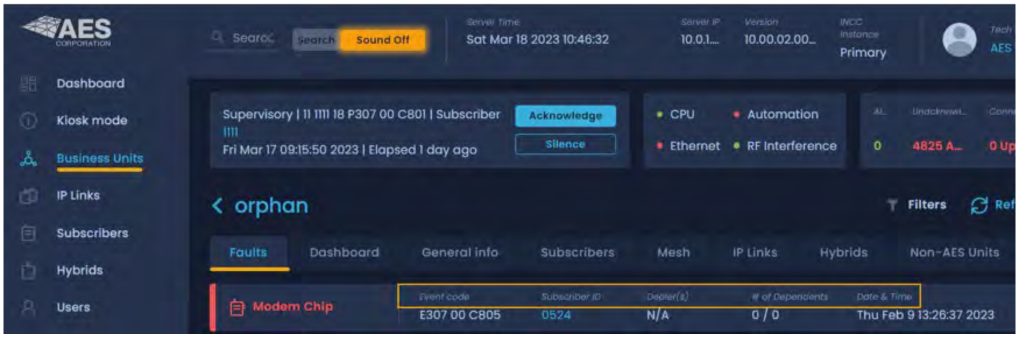
Aler...: 0 | Unacknowledg...: 4803 Active | Connectivity: 0 Up / 6 Do...

	Event code	Subscriber ID	Dealer(s)	# of Dependents	Date & Time
Modem Chip	E307 00 C805	0524	N/A	0 / 0	Thu Feb 9 13:26:37 2023

Faults Tab

The **Faults** tab provides a list of subscriber faults that are occurring.

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



Server Time: Sat Mar 18 2023 10:46:32 | Server IP: 10.0.1... | Version: 10.00.02.00... | INCC instance: Primary | Tech AES

Supervisory | 11 1111 18 P307 00 C801 | Subscriber 1111
Fri Mar 17 09:15:50 2023 | Elapsed 1 day ago

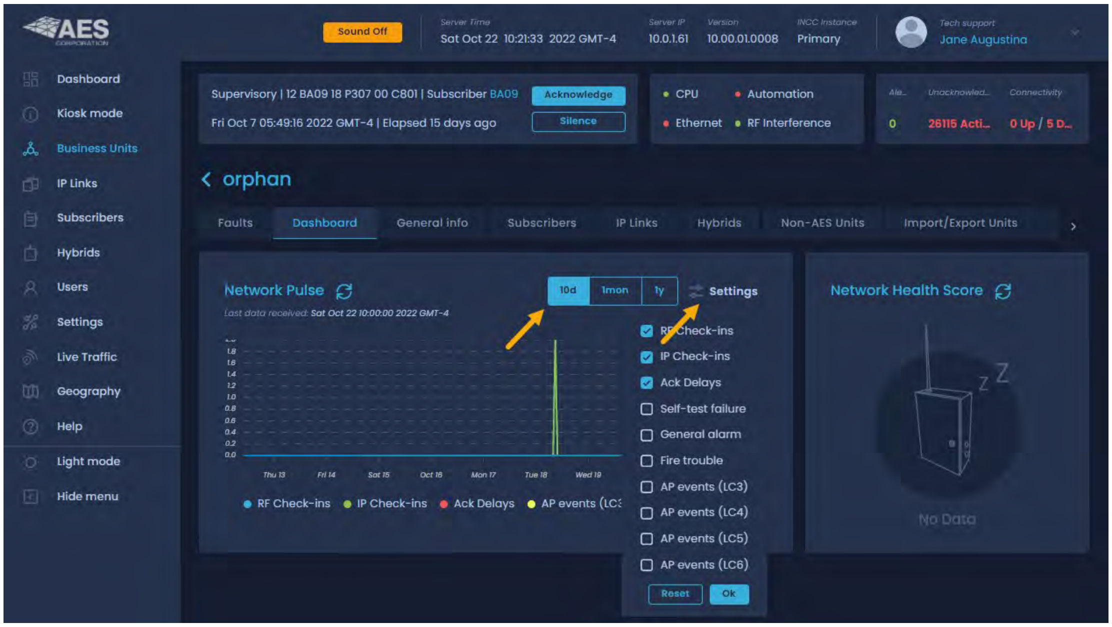
Al...: 0 | Unacknowl...: 4825 A... | Conn...: 0 Up

	Event code	Subscriber ID	Dealer(s)	# of Dependents	Date & Time
Modem Chip	E307 00 C805	0524	N/A	0 / 0	Thu Feb 9 13:26:37 2023

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



Server Time: Sat Oct 22 10:21:33 2022 GMT-4
Server IP: 10.0.1.61
Version: 10.00.01.0008
INCC Instance: Primary
Tech support: Jane Augustina

Supervisory | 12 BA09 18 P307 00 C801 | Subscriber BA09
Fri Oct 7 05:49:16 2022 GMT-4 | Elapsed 15 days ago

Ale… 0 | Unacknowled… 26115 Acti… | Connectivity 0 Up / 5 D…

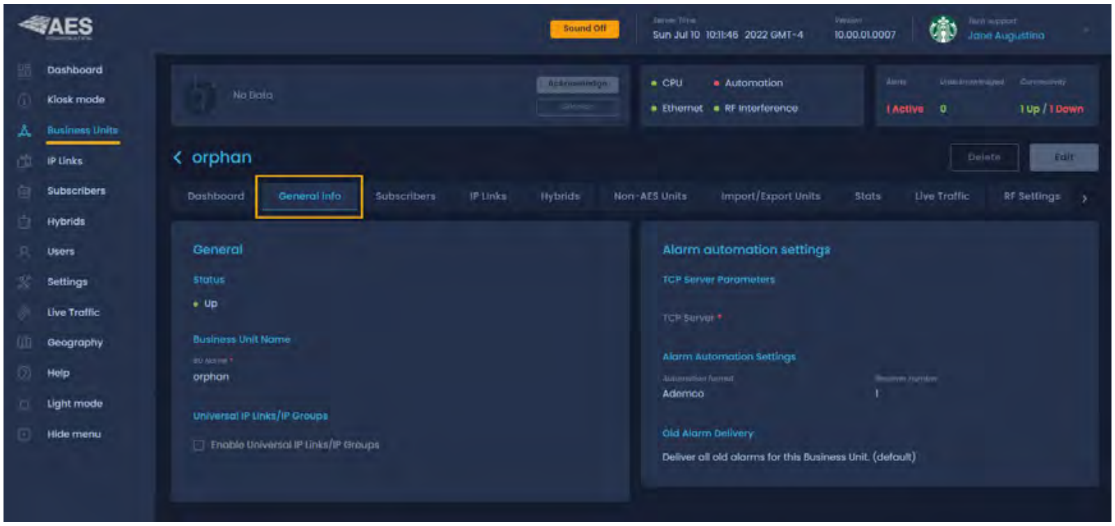
Network Pulse
Last data received: Sat Oct 22 10:00:00 2022 GMT-4

Settings
☑ RF Check-ins
☑ IP Check-ins
☑ Ack Delays
☐ Self-test failure
☐ General alarm
☐ Fire trouble
☐ AP events (LC3)
☐ AP events (LC4)
☐ AP events (LC5)
☐ AP events (LC6)

Network Health Score
No Data

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



General

Status

● Up

Business Unit Name

BU Name *

orphan

Universal IP Links/IP Groups

□ Enable Universal IP Links/IP Groups

Alarm automation settings

TCP Server Parameters

TCP Server *

Alarm Automation Settings

Automation format: Ademco

Receiver number: 1

Old Alarm Delivery

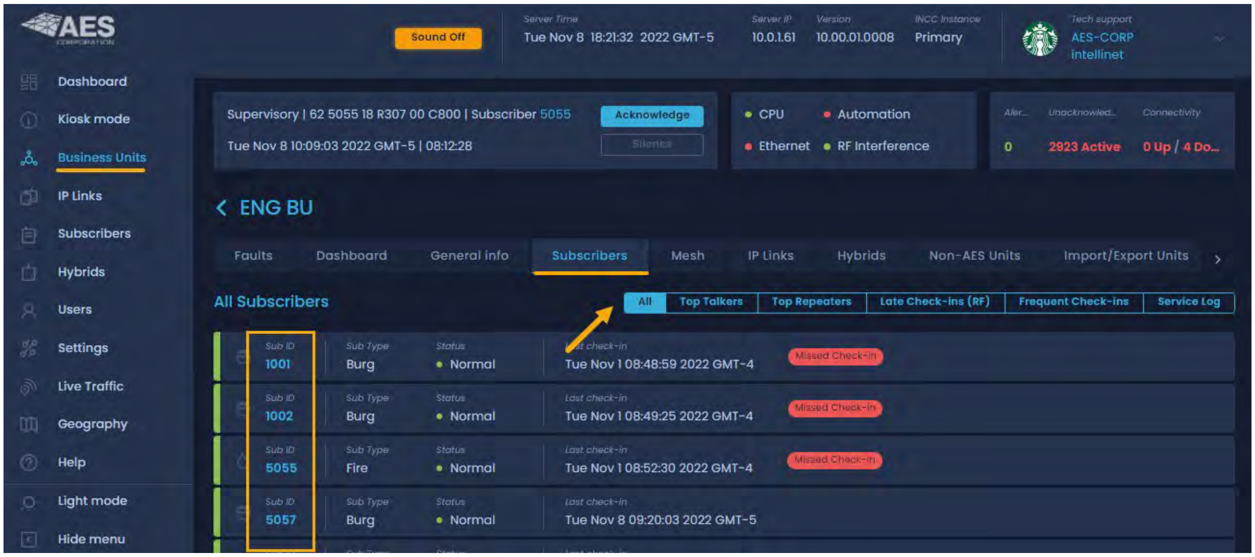
Deliver all old alarms for this Business Unit. (default)

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, as well as service log (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.

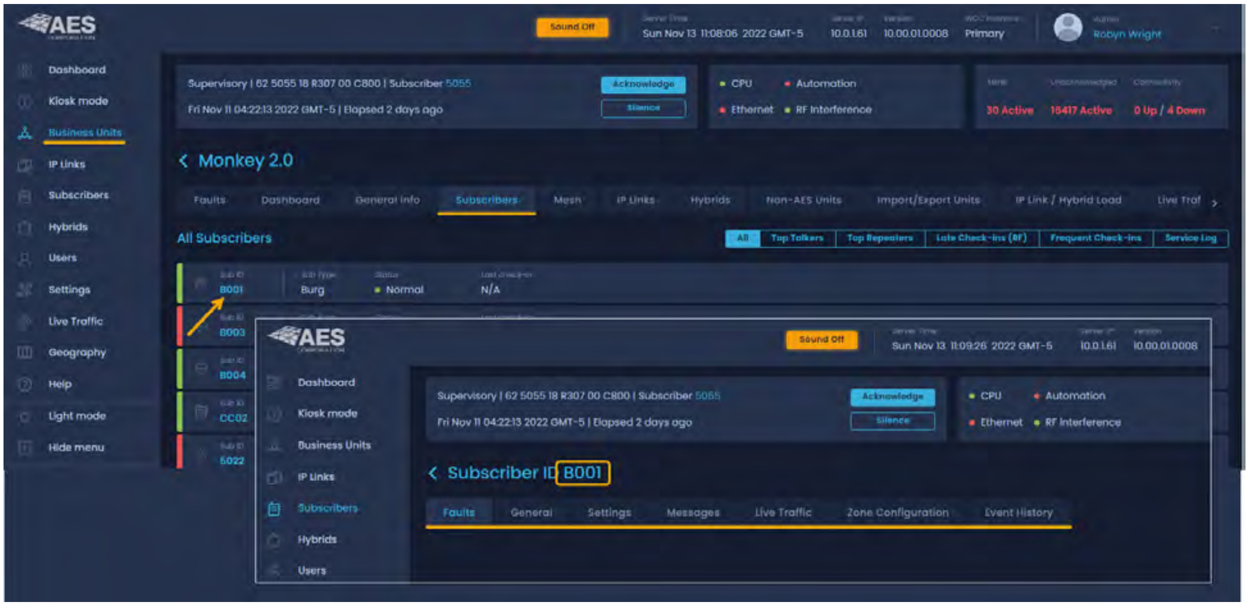


Supervisory | 62 5055 18 R307 00 C800 | Subscriber 5055

Tue Nov 8 10:09:03 2022 GMT-5 | 08:12:28

Sub ID	Sub Type	Status	Last check-in	
1001	Burg	● Normal	Tue Nov 1 08:48:59 2022 GMT-4	Missed Check-in
1002	Burg	● Normal	Tue Nov 1 08:49:25 2022 GMT-4	Missed Check-in
5055	Fire	● Normal	Tue Nov 1 08:52:30 2022 GMT-4	Missed Check-in
5057	Burg	● Normal	Tue Nov 8 09:20:03 2022 GMT-5	

To access a specific subscriber, click the subscriber from the list of subscribers. Subscribers are described in detail on page 62 (Subscribers).



Supervisory | 62 5055 18 R307 00 C800 | Subscriber 5055
Fri Nov 11 04:22:13 2022 GMT-5 | Elapsed 2 days ago

B001 Burg Normal N/A

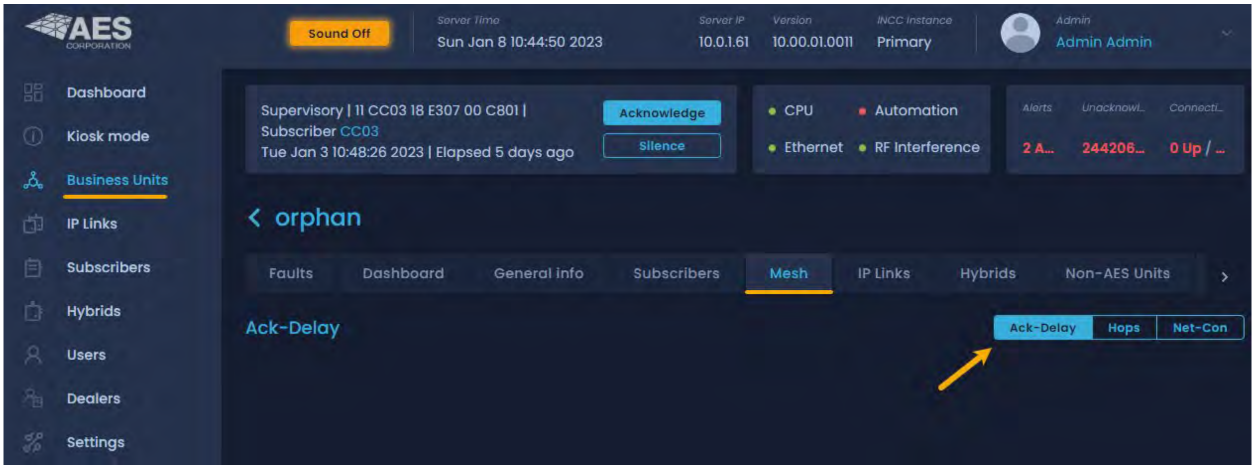
Table 1. Network Analysis Tools

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 that the subscriber is installed properly. • Ensure that the subscriber is free of faults. – Ensure that the alarm panel connected to the subscriber is configured and connected properly. – Ensure that the alarm panel connected to the subscriber is free of faults. – Ensure that 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.

Table 1. Network Analysis Tools

	• 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 that the subscriber is installed properly. • Ensure that the subscriber is free of faults. • Ensure that the subscriber is connected to the network by watching the LEDs on the subscriber PCB. • Ensure that the subscriber settings on page 67 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. 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 need service.

Mesh Tab



Supervisory | 11 CC03 18 E307 00 C801 |
Subscriber CC03
Tue Jan 3 10:48:26 2023 | Elapsed 5 days ago

- 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. 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. Only fire subscribers report their Net-Con statuses, as either high or low, in messages sent to the MultiNet/INCC receiver.

IP Links Tab

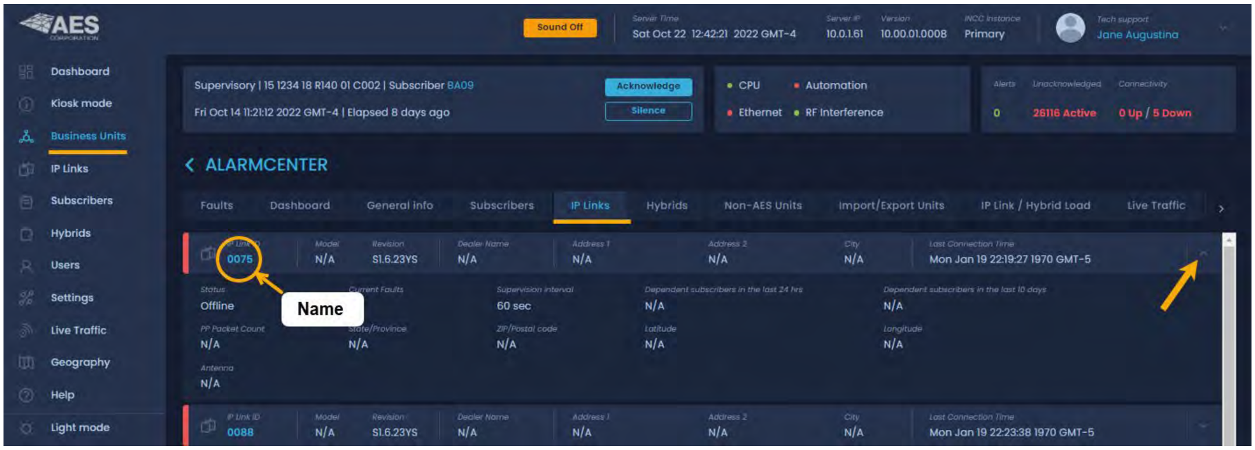
The IP Links tab displays a list of all IP Links associated with a subscriber. Each IP Link displays general information:

- 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).



Server Time: Sat Oct 22 12:42:21 2022 GMT-4 | Server IP: 10.0.1.61 | Version: 10.00.01.0008 | INCC Instance: Primary | Tech support: Jane Augustina

Supervisory | 15 1234 18 R140 01 C002 | Subscriber BA09
Fri Oct 14 11:21:12 2022 GMT-4 | Elapsed 8 days ago

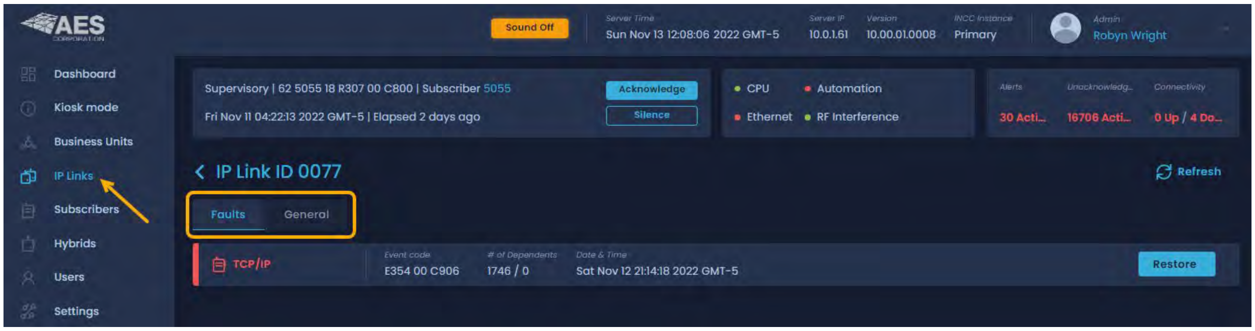
Alerts: 0 | Unacknowledged: 26116 Active | Connectivity: 0 Up / 5 Down

ALARMCENTER

IP Link ID	Model	Revision	Dealer Name	Address 1	Address 2	City	Last Connection Time
0075	N/A	S1.6.23YS	N/A	N/A	N/A	N/A	Mon Jan 19 22:19:27 1970 GMT-5
0088	N/A	S1.6.23YS	N/A	N/A	N/A	N/A	Mon Jan 19 22:23:38 1970 GMT-5

Status: Offline
Current Faults:
Supervision interval: 60 sec
Dependent subscribers in the last 24 hrs: N/A
Dependent subscribers in the last 10 days: N/A
PP Packet Count: N/A
State/Province: N/A
ZIP/Postal code: N/A
Latitude: N/A
Longitude: N/A
Antenna: N/A

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



Server Time: Sun Nov 13 12:08:06 2022 GMT-5 | Server IP: 10.0.1.61 | Version: 10.00.01.0008 | INCC Instance: Primary | Admin: Robyn Wright

Supervisory | 62 5055 18 R307 00 C800 | Subscriber 5055
Fri Nov 11 04:22:13 2022 GMT-5 | Elapsed 2 days ago

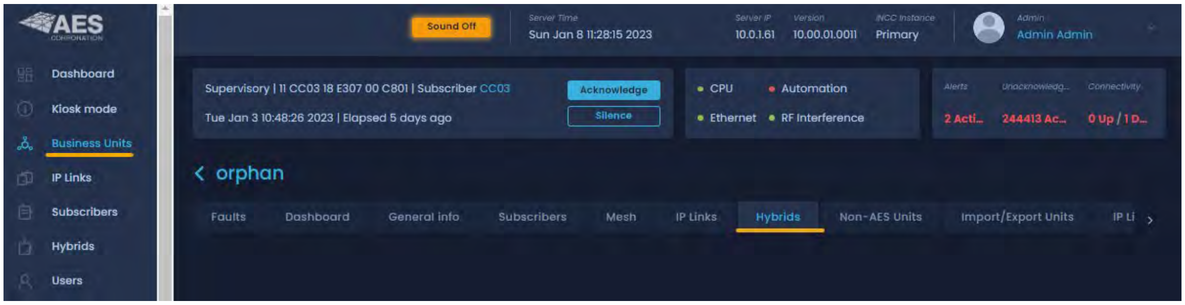
Alerts: 30 Acti... | Unacknowledg...: 16706 Acti... | Connectivity: 0 Up / 4 Do...

IP Link ID 0077

	Event code	# of Dependents	Date & Time
TCP/IP	E354 00 C906	1746 / 0	Sat Nov 12 21:14:18 2022 GMT-5

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.



Supervisory | 11 CC03 18 E307 00 C801 | Subscriber CC03

Tue Jan 3 10:48:26 2023 | Elapsed 5 days ago

Server Time: Sun Jan 8 11:28:15 2023

Server IP: 10.0.1.61

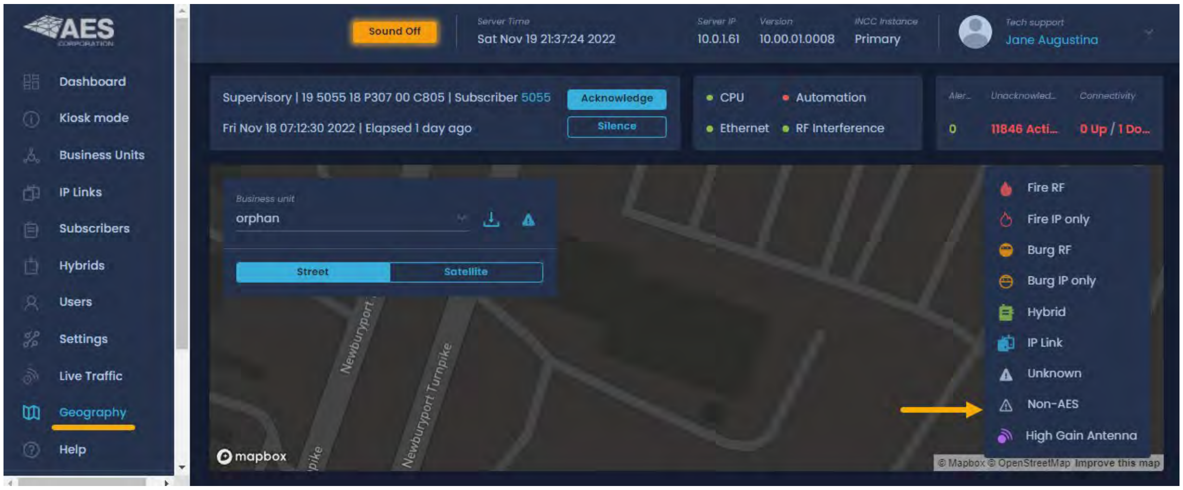
Version: 10.00.01.0011

INCC Instance: Primary

Admin: Admin Admin

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.



Supervisory | 19 5055 18 P307 00 C805 | Subscriber 5055

Fri Nov 18 07:12:30 2022 | Elapsed 1 day ago

Server Time: Sat Nov 19 21:37:24 2022

Server IP: 10.0.1.61

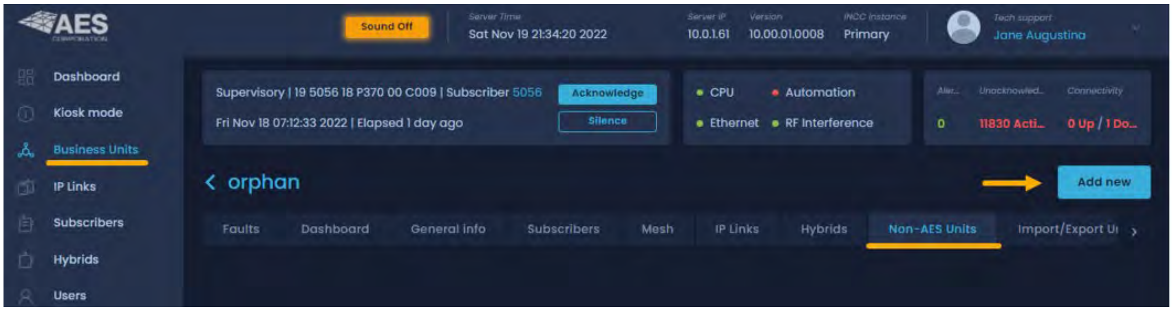
Version: 10.00.01.0008

INCC Instance: Primary

Tech support: Jane Augustina

Business unit: orphan

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



Supervisory | 19 5056 18 P370 00 C009 | Subscriber 5056

Fri Nov 18 07:12:33 2022 | Elapsed 1 day ago

Server Time: Sat Nov 19 21:34:20 2022

Server IP: 10.0.1.61

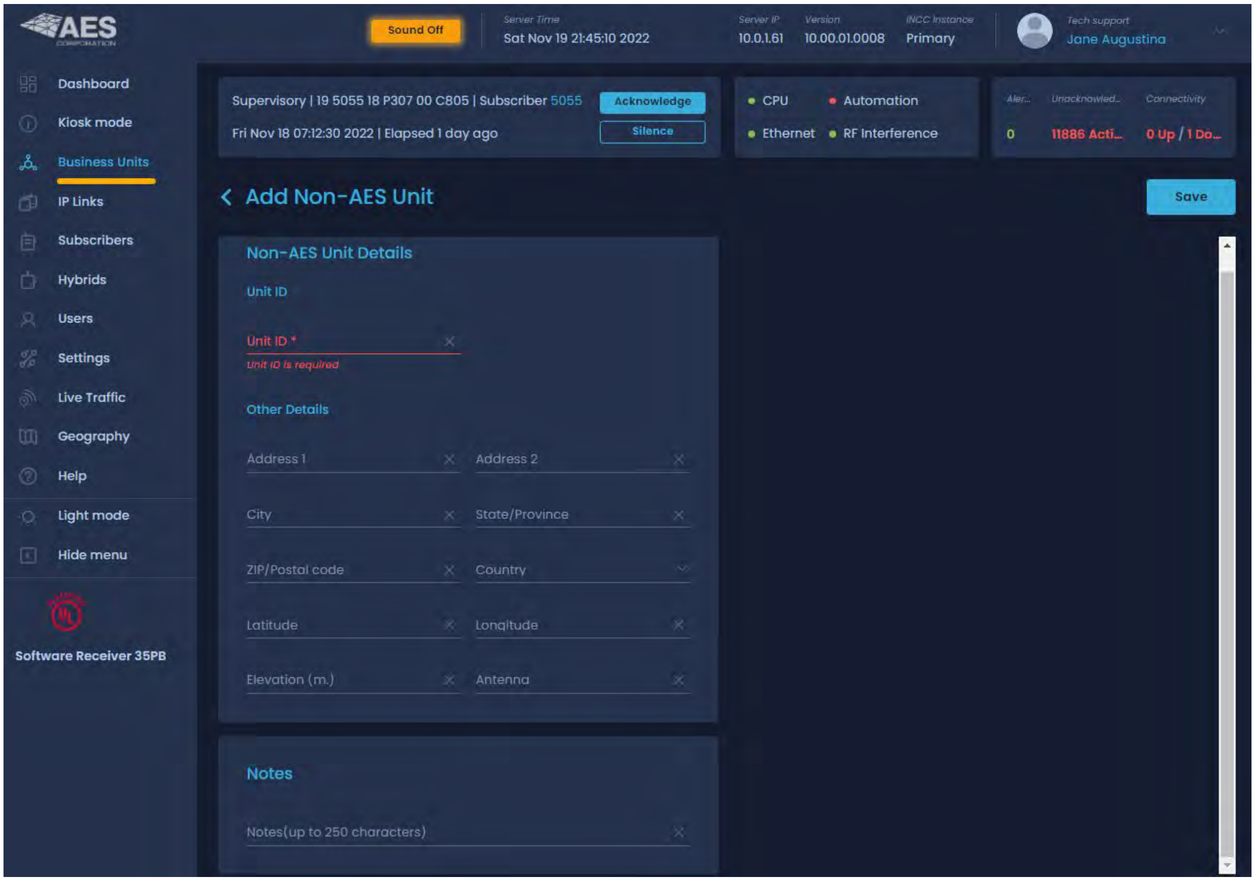
Version: 10.00.01.0008

INCC Instance: Primary

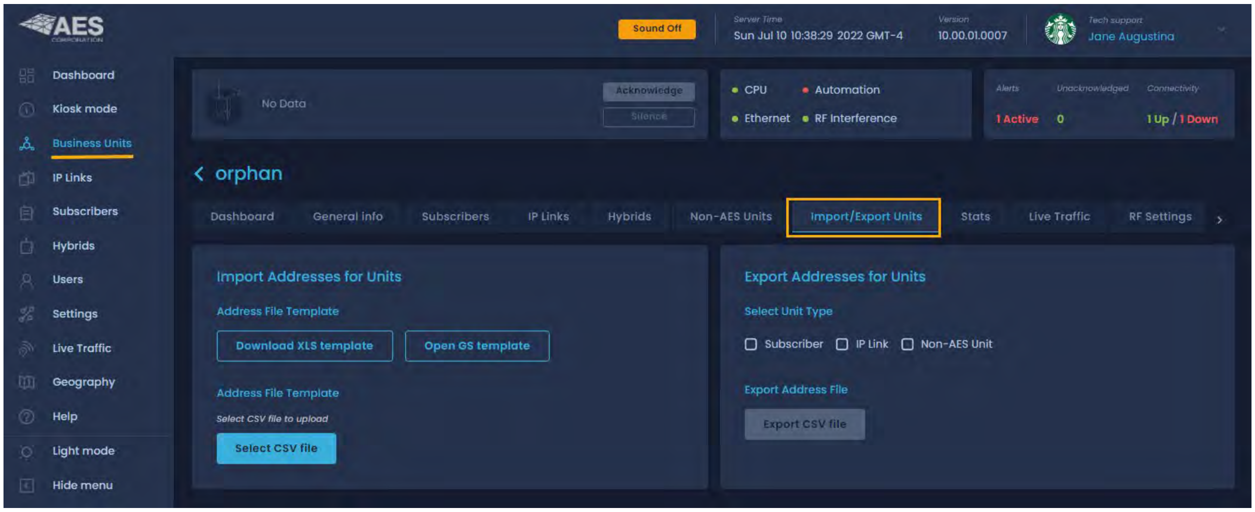
Tech support: Jane Augustina

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

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



Import/Export Units

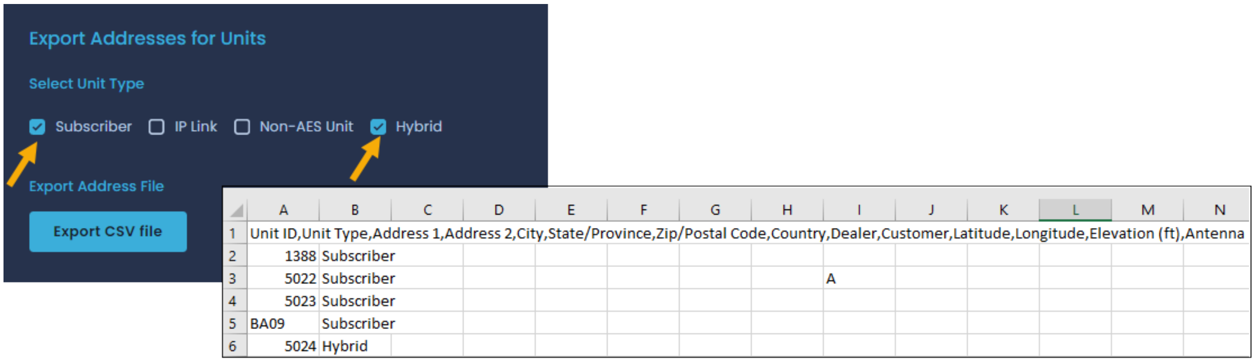


To import addresses for units:

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:



Export Addresses for Units

Select Unit Type

☑ Subscriber □ IP Link □ Non-AES Unit ☑ Hybrid

Export Address File

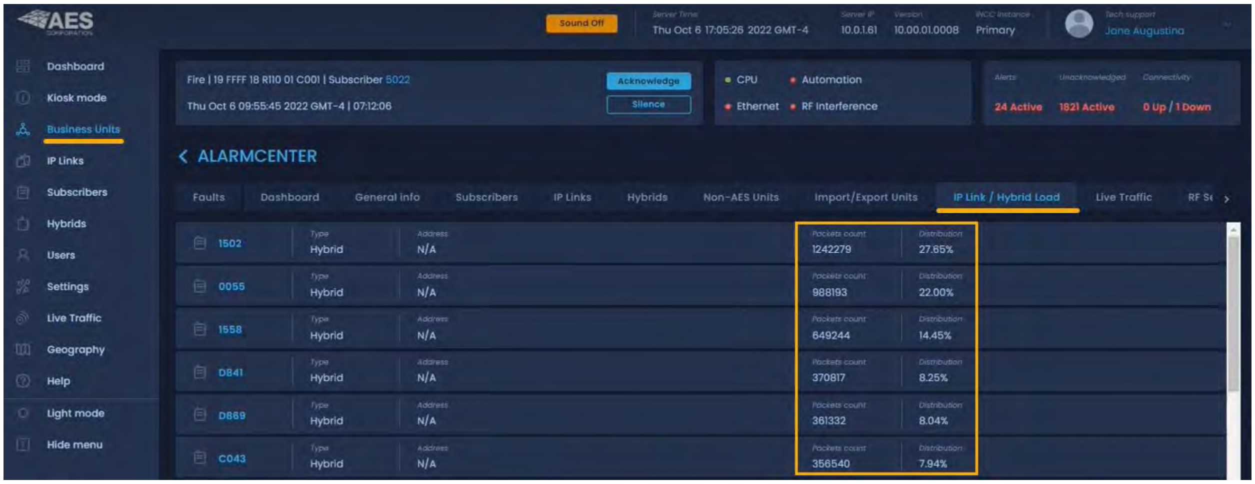
Export CSV file

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	Unit ID,Unit Type,Address 1,Address 2,City,State/Province,Zip/Postal Code,Country,Dealer,Customer,Latitude,Longitude,Elevation (ft),Antenna													
2	1388	Subscriber												
3	5022	Subscriber							A					
4	5023	Subscriber												
5	BA09	Subscriber												
6	5024	Hybrid												

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.

To increase RF traffic handled by an under-utilized IP Link, …



Server Time: Thu Oct 6 17:05:26 2022 GMT-4 | Server IP: 10.0.1.61 | Version: 10.00.01.0008 | INCC Instance: Primary | Tech support: Jane Augustina

Fire | 19 FFFF 18 R110 01 C001 | Subscriber 5022
Thu Oct 6 09:55:45 2022 GMT-4 | 07:12:06

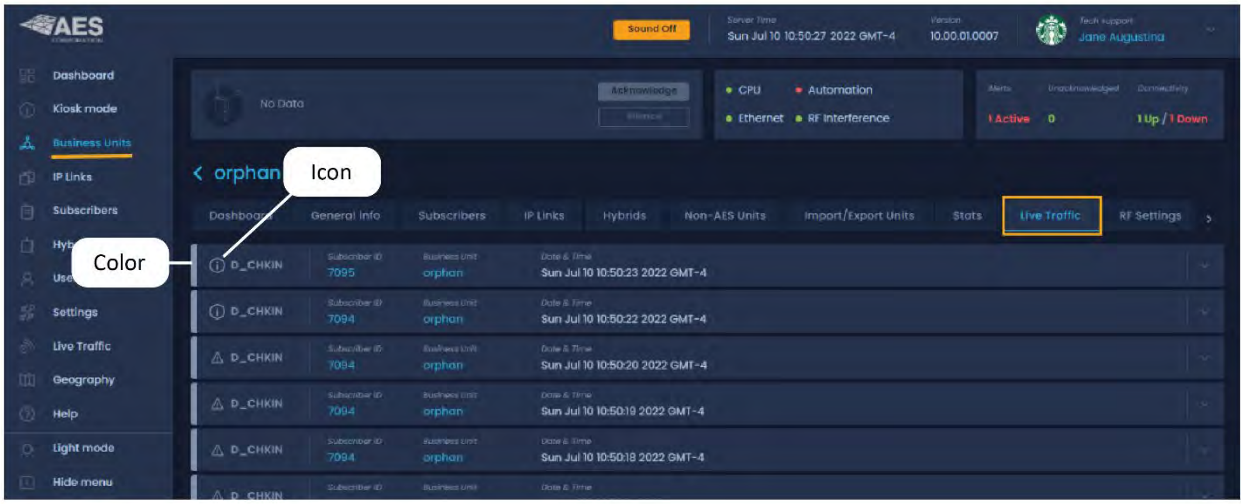
● CPU ● Automation ● Ethernet ● RF Interference

Alerts: 24 Active | Unacknowledged: 1821 Active | Connectivity: 0 Up / 1 Down

	Type	Address	Packets count	Distribution
1502	Hybrid	N/A	1242279	27.65%
0055	Hybrid	N/A	988193	22.00%
1558	Hybrid	N/A	649244	14.45%
D841	Hybrid	N/A	370817	8.25%
D869	Hybrid	N/A	361332	8.04%
C043	Hybrid	N/A	356540	7.94%

Live Traffic

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



Server Time: Sun Jul 10 10:50:27 2022 GMT-4 | Version: 10.00.01.0007 | Tech support: Jane Augustina

No Data

● CPU ● Automation ● Ethernet ● RF Interference

Alerts: 1 Active | Unacknowledged: 0 | Connectivity: 1 Up / 1 Down

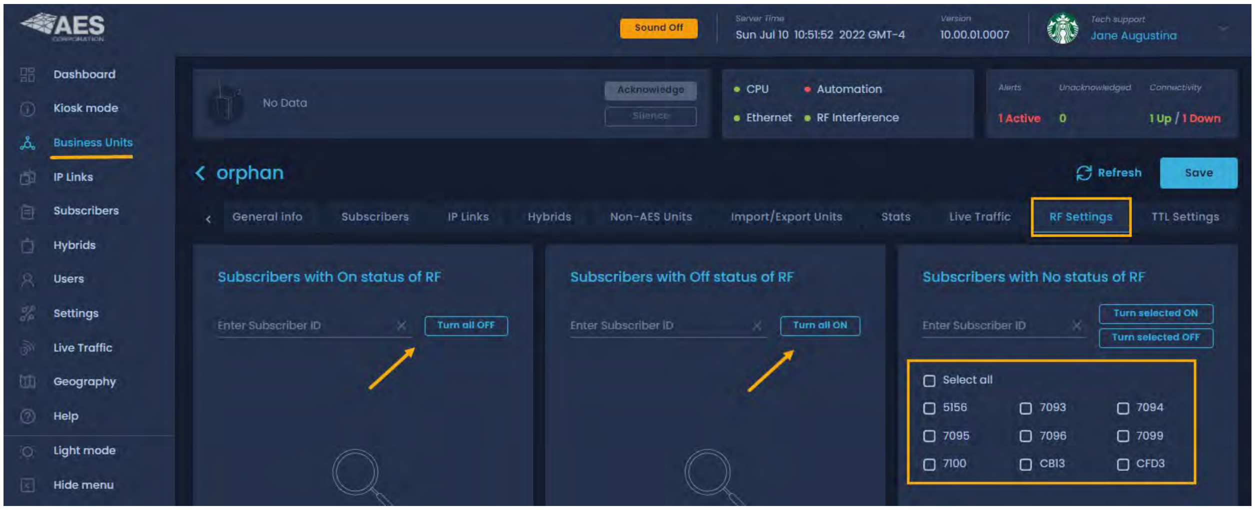
	Subscriber ID	Business Unit	Date & Time
D_CHKIN	7095	orphan	Sun Jul 10 10:50:23 2022 GMT-4
D_CHKIN	7094	orphan	Sun Jul 10 10:50:22 2022 GMT-4
D_CHKIN	7094	orphan	Sun Jul 10 10:50:20 2022 GMT-4
D_CHKIN	7094	orphan	Sun Jul 10 10:50:19 2022 GMT-4
D_CHKIN	7094	orphan	Sun Jul 10 10:50:18 2022 GMT-4
D_CHKIN			

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.

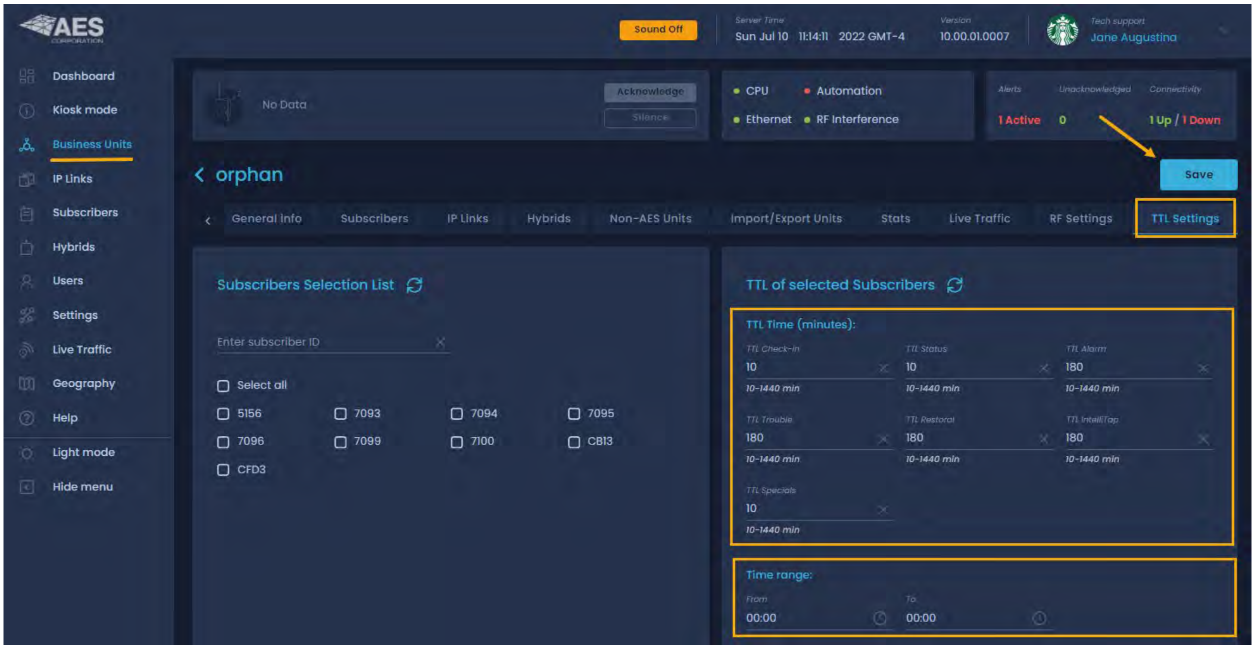


TTL Settings

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 message (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.



Server Time: Sun Jul 10 11:14:11 2022 GMT-4

Version: 10.00.01.0007

Tech support: Jane Augustina

Alerts: 1 Active

Unacknowledged: 0

Connectivity: 1 Up / 1 Down

orphan

□ Select all

□ 5156 □ 7093 □ 7094 □ 7095

□ 7096 □ 7099 □ 7100 □ CB13

□ CFD3

TTL Time (minutes):

TTL Check-in: 10 (10-1440 min)

TTL Status: 10 (10-1440 min)

TTL Alarm: 180 (10-1440 min)

TTL Trouble: 180 (10-1440 min)

TTL Restoral: 180 (10-1440 min)

TTL IntelliTap: 180 (10-1440 min)

TTL Specials: 10 (10-1440 min)

Time range:

From: 00:00

To: 00:00

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

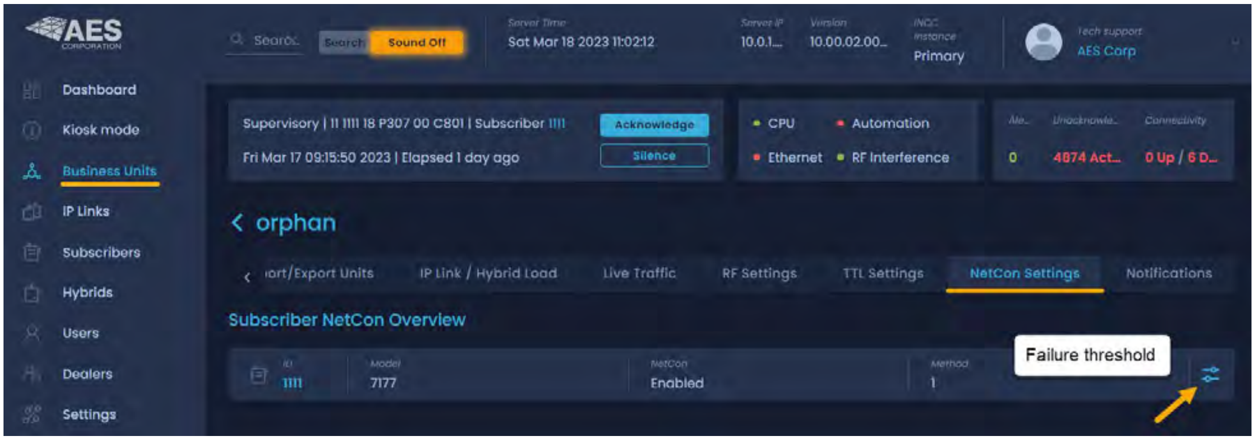
- TTL Check-in: Note that even when a check-in packet is deleted due to a delay, the objective of that message has already served its purpose: the late or missing signal should have been flagged at the central station (see Automatic Test Supervision section).

- 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 level of confidence that its transmissions will reach an IP Link. Only fire subscribers report NetCon status, as either high or low, in messages sent to the INCC.



Server Time: Sat Mar 18 2023 11:02:12
Server IP: 10.0.1...
Version: 10.00.02.00...
INCC Instance: Primary
Tech support: AES Corp

Supervisory | 11 1111 18 P307 00 C801 | Subscriber 1111
Fri Mar 17 09:15:50 2023 | Elapsed 1 day ago

CPU · Automation · Ethernet · RF Interference

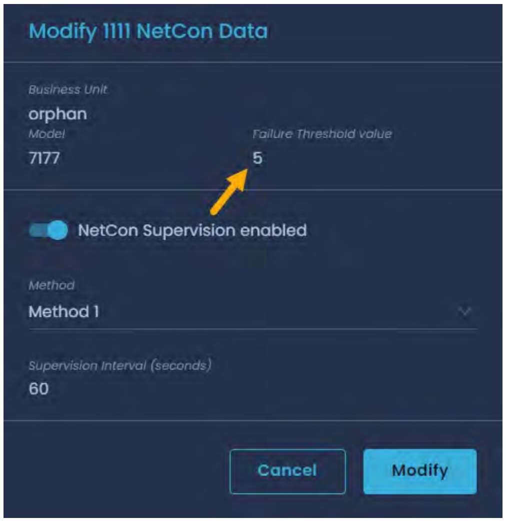
Ale...	Unacknowle...	Connectivity
0	4874 Act...	0 Up / 6 D...

orphan

Subscriber NetCon Overview

ID	Model	NetCon	Method
1111	7177	Enabled	1

When a fire subscriber reports low NetCon, 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.



Modify 1111 NetCon Data

Business Unit: orphan
Model: 7177
Failure Threshold value: 5

NetCon Supervision enabled

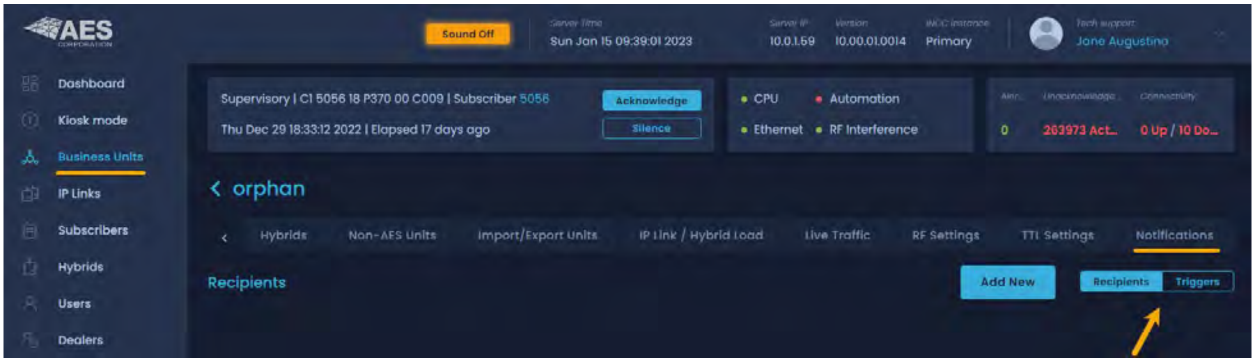
Method: Method 1

Supervision Interval (seconds): 60

Notifications

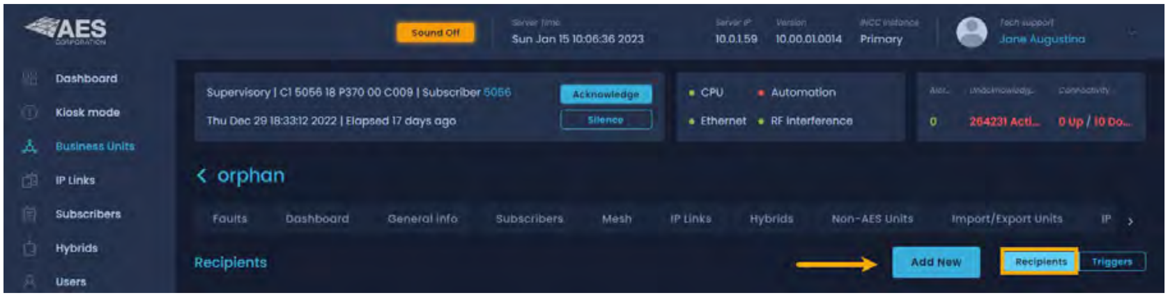
The Notification function enables users to monitor their AES-*IntelliNet* network from anywhere at any time. Users can configure automatic alerts based on a change to the network health score, a fault with any subscriber or IP links, or when traffic drops on IP links.

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.

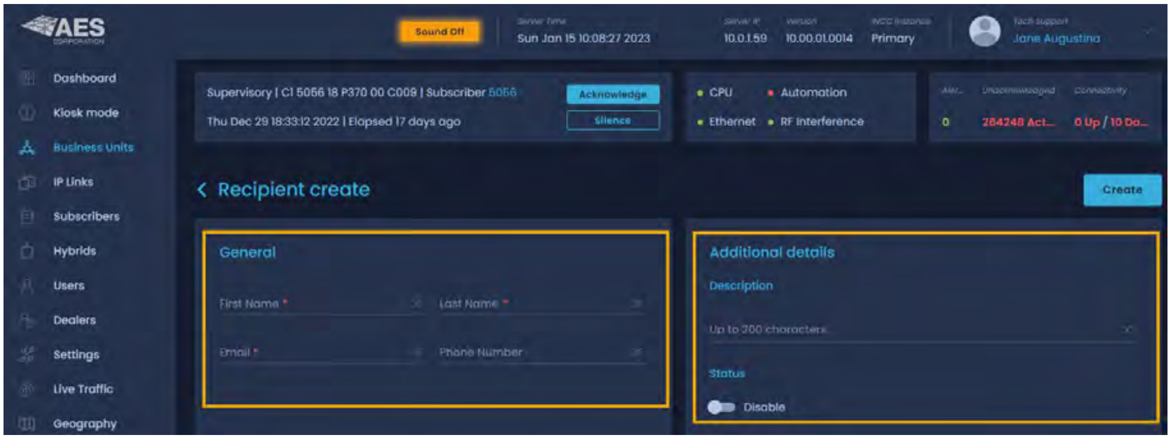


To create a list of Recipients:

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

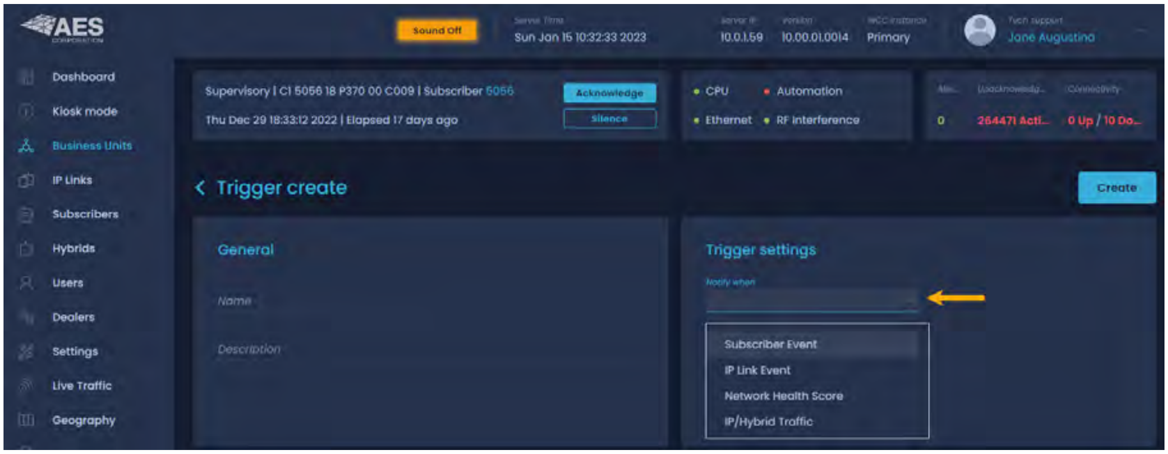


2. Enter the recipient's name and email address, then enter a description.



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.



Server Time Sun Jan 15 10:32:33 2023 | Server IP 10.0.1.59 | Version 10.00.01.0014 | INCC instance Primary | Tech support Jane Augustino

Supervisory | C1 5056 18 P370 00 C009 | Subscriber 5056

Thu Dec 29 18:33:12 2022 | Elapsed 17 days ago

0 | 264471 Acti... | 0 Up / 10 Do...

Trigger create

General

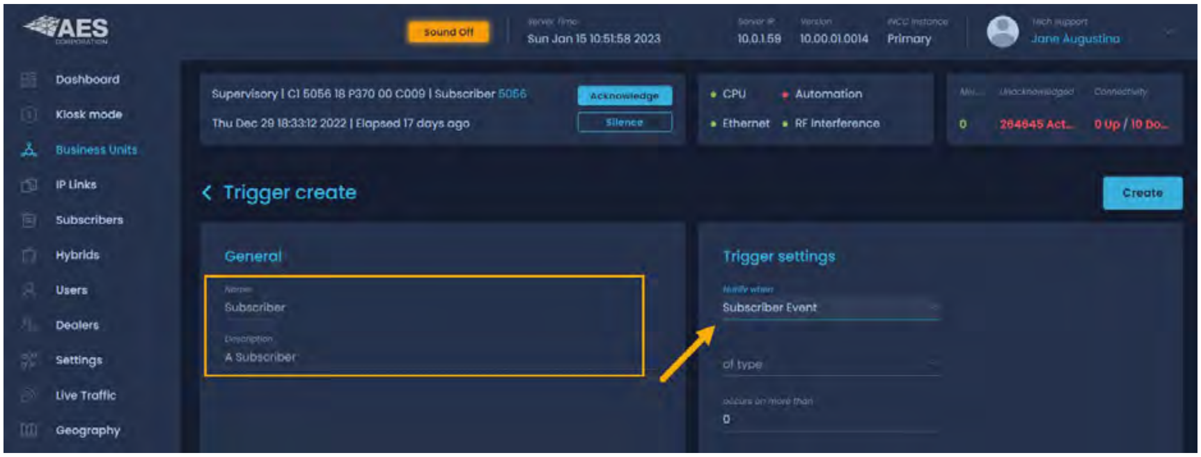
Name

Description

Trigger settings

Notify when

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



Server Time Sun Jan 15 10:51:58 2023 | Server IP 10.0.1.59 | Version 10.00.01.0014 | INCC instance Primary | Tech support Jane Augustino

Supervisory | C1 5056 18 P370 00 C009 | Subscriber 5056

Thu Dec 29 18:33:12 2022 | Elapsed 17 days ago

0 | 264645 Act... | 0 Up / 10 Do...

Trigger create

General

Name: Subscriber

Description: A Subscriber

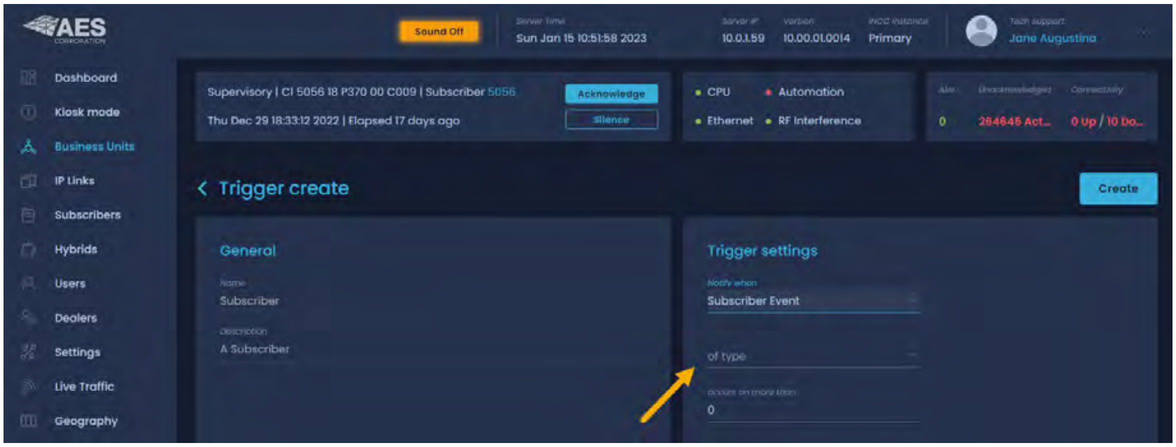
Trigger settings

Notify when: Subscriber Event

of type

occurs on more than: 0

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



Trigger create

General

Name: Subscriber

Description: A Subscriber

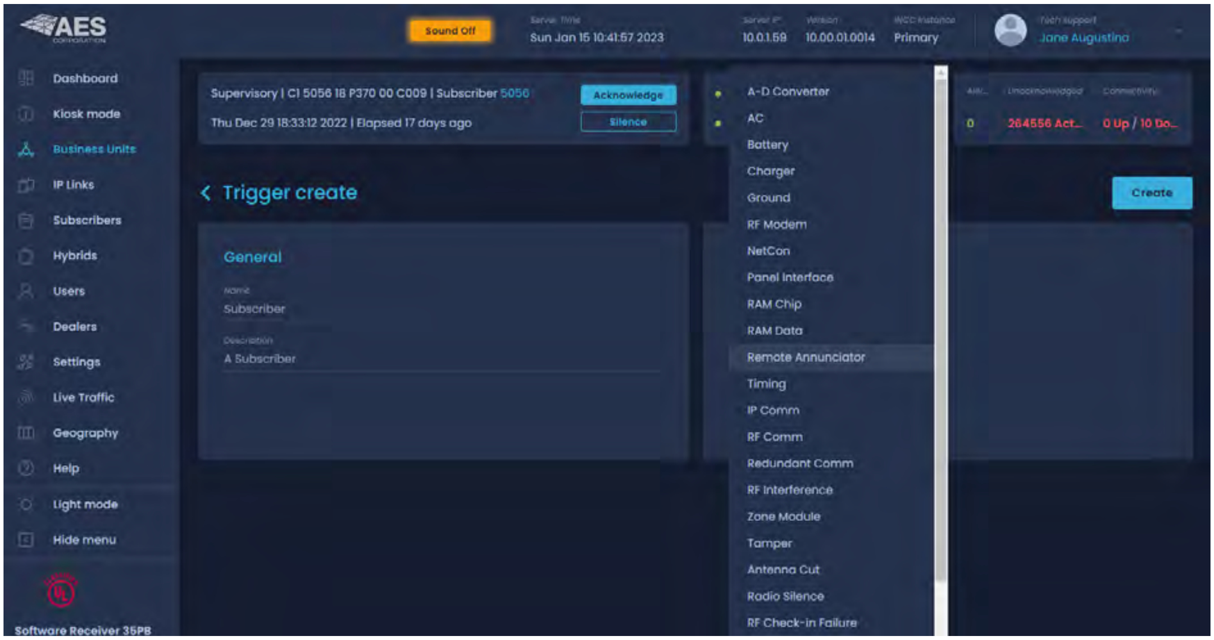
Trigger settings

Notify when: Subscriber Event

of type

0

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



Trigger create

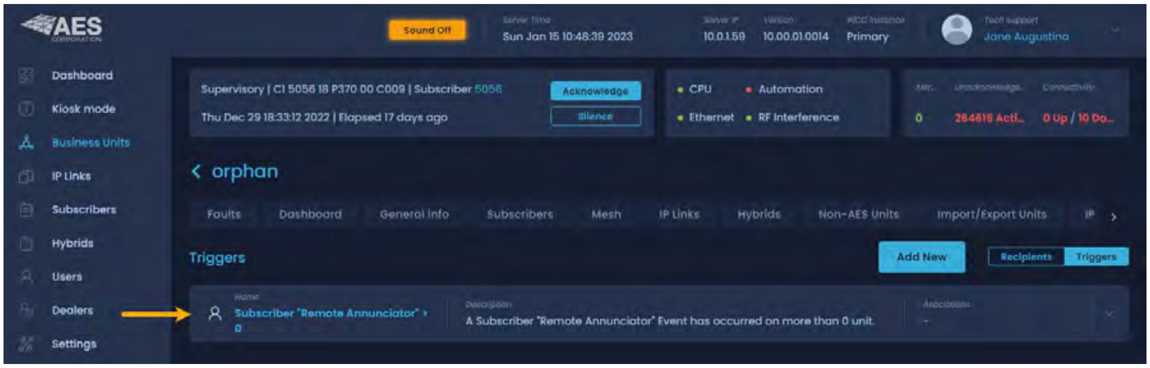
General

Name: Subscriber

Description: A Subscriber

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

   Triggers are listed on the Triggers page.



Server Time: Sun Jan 15 10:48:39 2023 | Server IP: 10.0.1.59 | Version: 10.00.01.0014 | INCC Instance: Primary | Tech support: Jane Augustina

Supervisory | C1 5056 18 P370 00 C009 | Subscriber 5056
Thu Dec 29 18:33:12 2022 | Elapsed 17 days ago

● CPU ● Automation
● Ethernet ● RF Interference

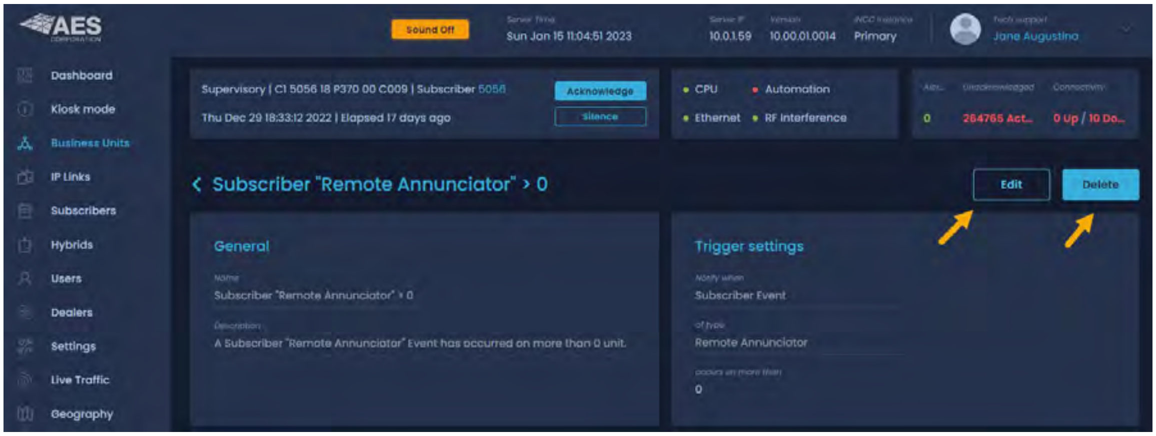
Aler...	Unacknowledge...	Connectivity
0	264615 Acti...	0 Up / 10 Do...

< orphan

Triggers

Name	Description	Associations
Subscriber "Remote Annunciator" > 0	A Subscriber "Remote Annunciator" Event has occurred on more than 0 unit.	-

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



Server Time: Sun Jan 15 11:04:51 2023 | Server IP: 10.0.1.59 | Version: 10.00.01.0014 | INCC Instance: Primary | Tech support: Jane Augustina

Supervisory | C1 5056 18 P370 00 C009 | Subscriber 5056
Thu Dec 29 18:33:12 2022 | Elapsed 17 days ago

● CPU ● Automation
● Ethernet ● RF Interference

Aler...	Unacknowledged	Connectivity
0	264765 Act...	0 Up / 10 Do...

< Subscriber "Remote Annunciator" > 0

General

Name: Subscriber "Remote Annunciator" > 0

Description: A Subscriber "Remote Annunciator" Event has occurred on more than 0 unit.

Trigger settings

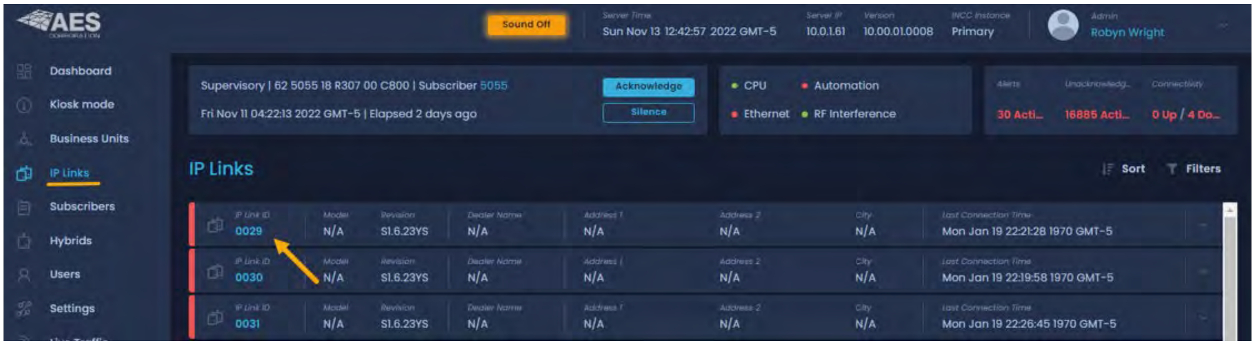
Notify when: Subscriber Event

of type: Remote Annunciator

occurs on more than: 0

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.



Server Time: Sun Nov 13 12:42:57 2022 GMT-5 | Server IP: 10.0.1.61 | Version: 10.00.01.0008 | INCC Instance: Primary | Admin: Robyn Wright

Supervisory | 62 5055 18 R307 00 C800 | Subscriber 5055
Fri Nov 11 04:22:13 2022 GMT-5 | Elapsed 2 days ago

● CPU ● Automation
● Ethernet ● RF Interference

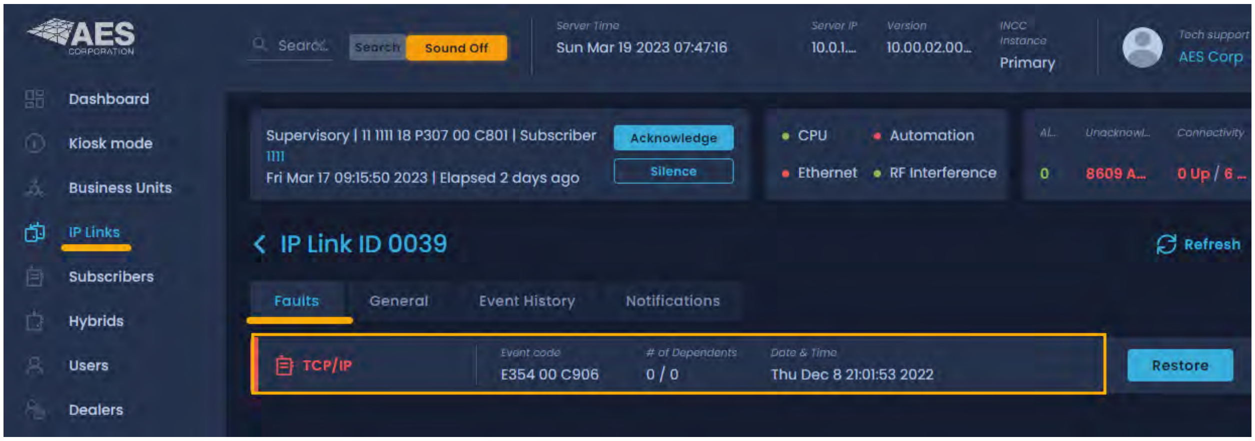
Alerts	Unacknowledg...	Connectivity
30 Acti...	16885 Acti...	0 Up / 4 Do...

IP Links

IP Link ID	Model	Revision	Dealer Name	Address 1	Address 2	City	Last Connection Time
0029	N/A	S1.6.23YS	N/A	N/A	N/A	N/A	Mon Jan 19 22:21:28 1970 GMT-5
0030	N/A	S1.6.23YS	N/A	N/A	N/A	N/A	Mon Jan 19 22:19:58 1970 GMT-5
0031	N/A	S1.6.23YS	N/A	N/A	N/A	N/A	Mon Jan 19 22:26:45 1970 GMT-5

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.



Server Time: Sun Mar 19 2023 07:47:16
Server IP: 10.0.1...
Version: 10.00.02.00...
INCC Instance: Primary
Tech support: AES Corp

Supervisory | 11 1111 18 P307 00 C801 | Subscriber 1111
Fri Mar 17 09:15:50 2023 | Elapsed 2 days ago

CPU · Automation · Ethernet · RF Interference

Al...	Unacknowl...	Connectivity
0	8609 A...	0 Up / 6 ...

IP Link ID 0039

	Event code	# of Dependents	Date & Time
TCP/IP	E354 00 C906	0 / 0	Thu Dec 8 21:01:53 2022

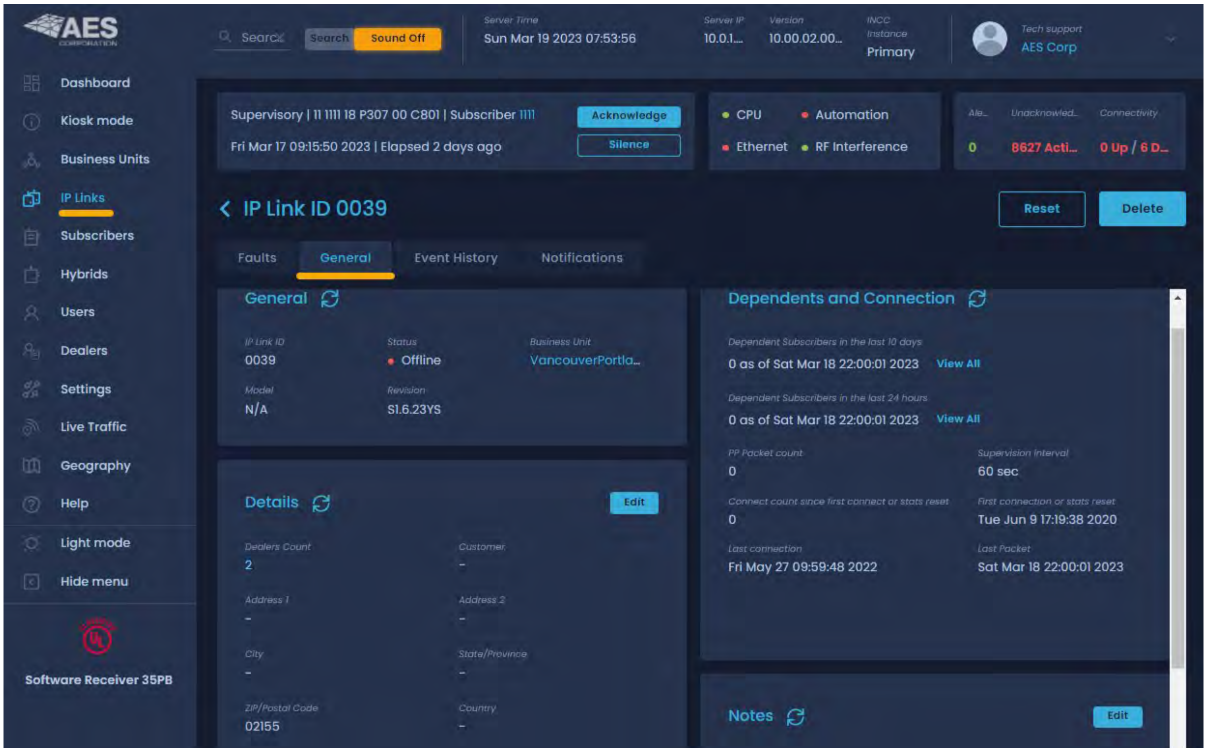
IP Link fault types include:

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.



Server Time: Sun Mar 19 2023 07:53:56
Server IP: 10.0.1...
Version: 10.00.02.00...
INCC Instance: Primary
Tech support: AES Corp

Supervisory | 11 1111 18 P307 00 C801 | Subscriber 1111
Fri Mar 17 09:15:50 2023 | Elapsed 2 days ago

CPU · Automation · Ethernet · RF Interference

Ale...	Unacknowled...	Connectivity
0	8627 Acti...	0 Up / 6 D...

IP Link ID 0039

General

IP Link ID	Status	Business Unit
0039	Offline	VancouverPortla...
Model	**Revision**	
N/A	S1.6.23YS	

Details

Dealers Count	Customer
2	-
Address 1	**Address 2**
-	-
City	**State/Province**
-	-
ZIP/Postal Code	**Country**
02155	-

Dependents and Connection

Dependent Subscribers in the last 10 days: 0 as of Sat Mar 18 22:00:01 2023

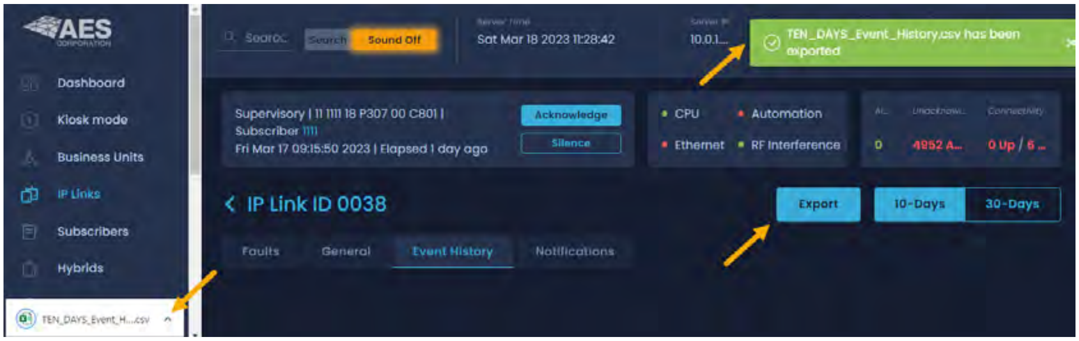
Dependent Subscribers in the last 24 hours: 0 as of Sat Mar 18 22:00:01 2023

PP Packet count	Supervision interval
0	60 sec
Connect count since first connect or stats reset	**First connection or stats reset**
0	Tue Jun 9 17:19:38 2020
Last connection	**Last Packet**
Fri May 27 09:59:48 2022	Sat Mar 18 22:00:01 2023

Notes

Events History Tab

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



Server Time: Sat Mar 18 2023 11:28:42
Server IP: 10.0.1...

TEN_DAYS_Event_History.csv has been exported

Supervisory | 11 1111 18 P307 00 C801 | Subscriber 1111
Fri Mar 17 09:15:50 2023 | Elapsed 1 day ago

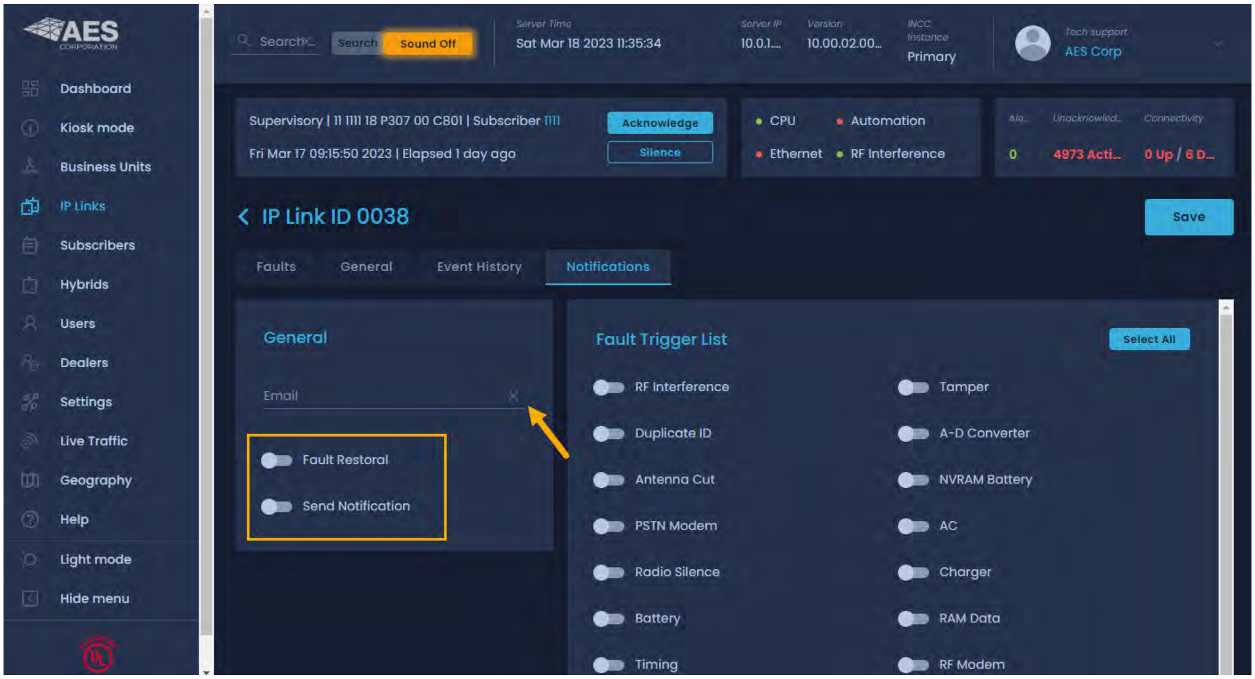
CPU · Automation · Ethernet · RF Interference

Al...	Unacknow...	Connectivity
0	4952 A...	0 Up / 6 ...

IP Link ID 0038

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.



Sat Mar 18 2023 11:35:34 | 10.0.1... | 10.00.02.00... | Primary | AES Corp

Supervisory | 11 1111 18 P307 00 C801 | Subscriber 1111

Fri Mar 17 09:15:50 2023 | Elapsed 1 day ago

0 | 4973 Acti... | 0 Up / 6 D...

IP Link ID 0038

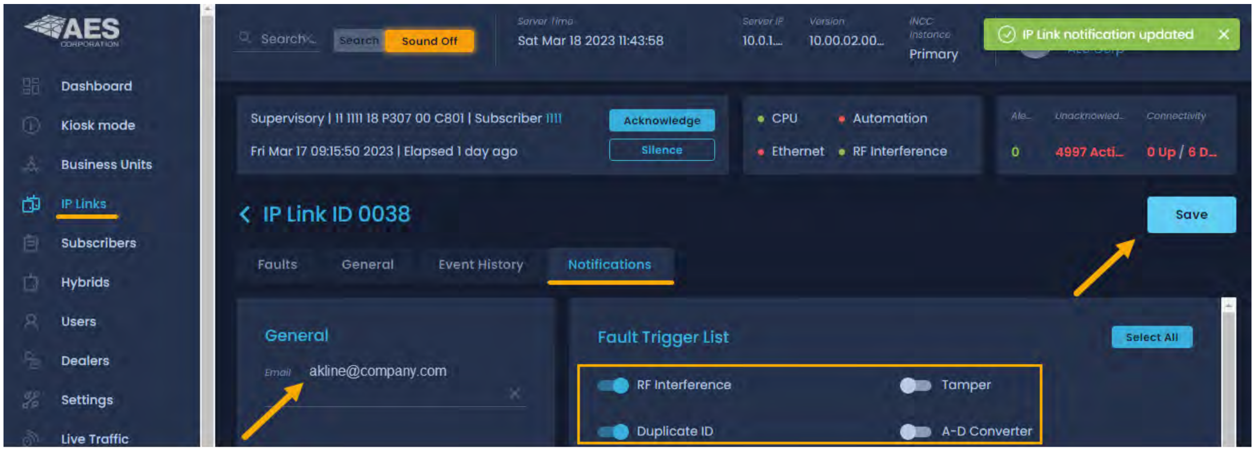
Fault Restoral

Send Notification

RF Interference | Tamper
Duplicate ID | A-D Converter
Antenna Cut | NVRAM Battery
PSTN Modem | AC
Radio Silence | Charger
Battery | RAM Data
Timing | RF Modem

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**.



Sat Mar 18 2023 11:43:58 | 10.0.1... | 10.00.02.00... | Primary

IP Link notification updated

Supervisory | 11 1111 18 P307 00 C801 | Subscriber 1111

Fri Mar 17 09:15:50 2023 | Elapsed 1 day ago

0 | 4997 Acti... | 0 Up / 6 D...

IP Link ID 0038

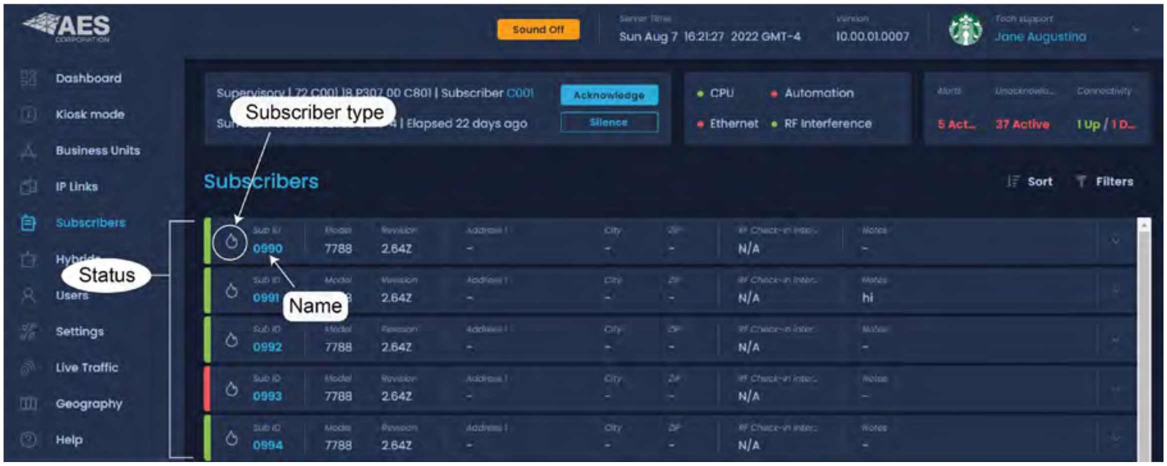
Email akline@company.com

RF Interference | Tamper
Duplicate ID | A-D Converter

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).



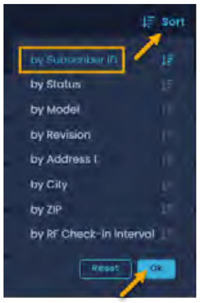
Sub ID	Model	Revision	Address I	City	ZIP	RF Check-in Inter...	Notes
0990	7788	2.64Z	–	–	–	N/A	–
0991	7788	2.64Z	–	–	–	N/A	hi
0992	7788	2.64Z	–	–	–	N/A	–
0993	7788	2.64Z	–	–	–	N/A	–
0994	7788	2.64Z	–	–	–	N/A	–

Sorting and Filtering

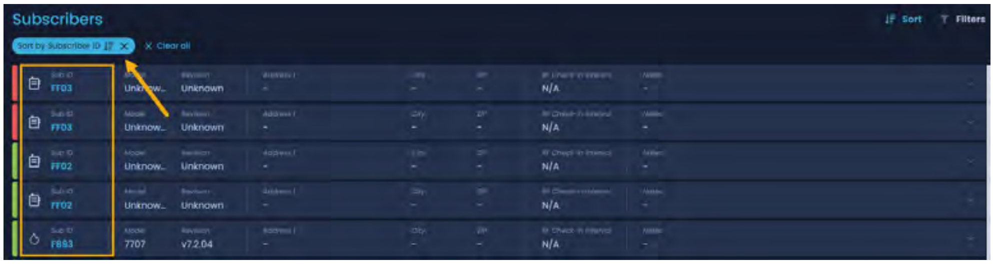
Subscribers can be sorted and filtered from the dashboard.

– 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



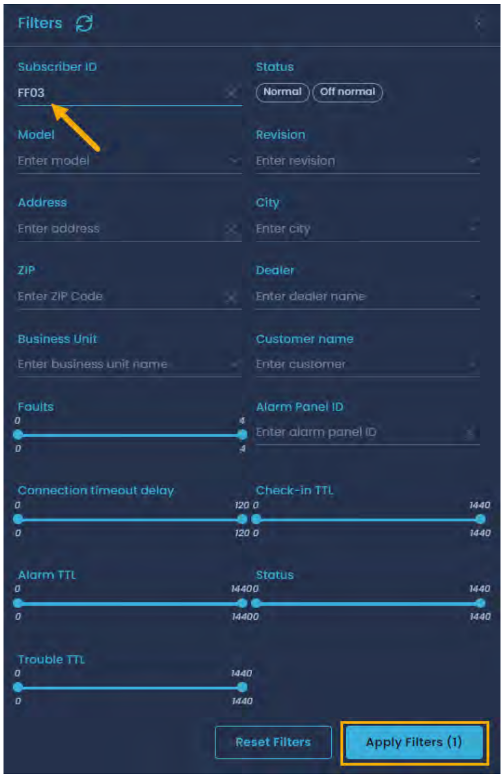
Result



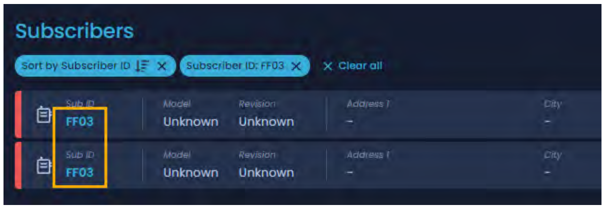
Sub ID	Model	Revision	Address I	City	ZIP	RF Check-in Interval	Notes
FF03	Unknow...	Unknown	–	–	–	N/A	–
FF03	Unknow...	Unknown	–	–	–	N/A	–
FF02	Unknow...	Unknown	–	–	–	N/A	–
FF02	Unknow...	Unknown	–	–	–	N/A	–
F883	7707	v7.2.04	–	–	–	N/A	–

– 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

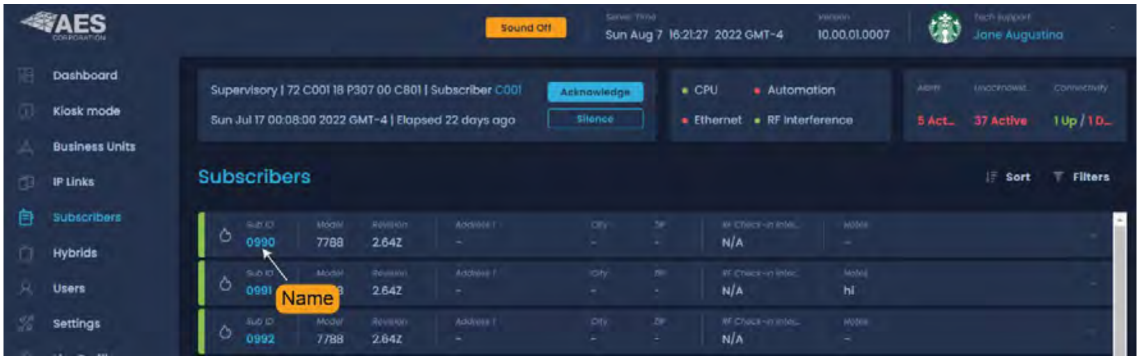


Sub ID	Model	Revision	Address 1	City
FF03	Unknown	Unknown	–	–
FF03	Unknown	Unknown	–	–

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

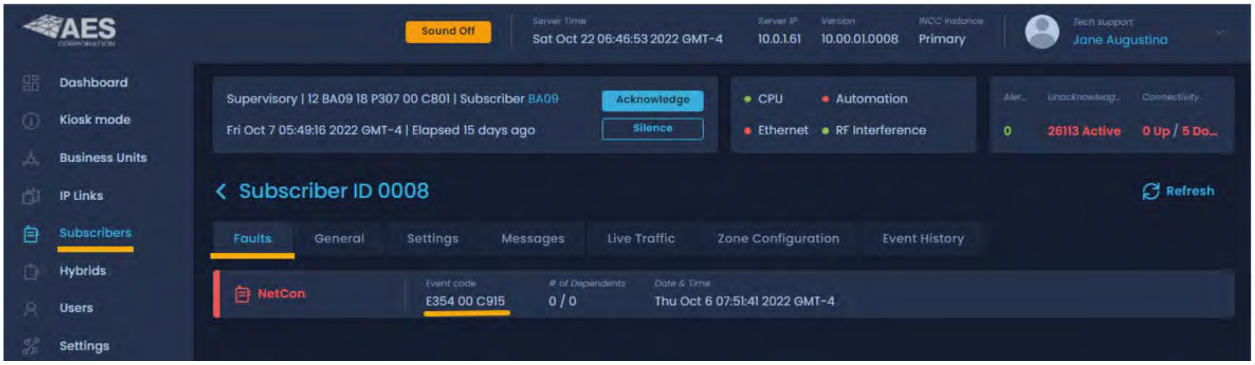
Click the name of the subscriber to view subscriber details (e.g., faults, general, settings, messages, live traffic, zone configuration, and event history).



Sub ID	Model	Revision	Address 1	City	ZIP	RF Check-in inte...	Mobile
0990	7788	2.64Z	–	–	–	N/A	–
0991	[illegible]	2.64Z	–	–	–	N/A	hi
0992	7788	2.64Z	–	–	–	N/A	–

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.



Server Time: Sat Oct 22 06:46:53 2022 GMT-4 | Server IP: 10.0.1.61 | Version: 10.00.01.0008 | INCC Instance: Primary | Tech support: Jane Augustina

Supervisory | 12 BA09 18 P307 00 C801 | Subscriber BA09
Fri Oct 7 05:49:16 2022 GMT-4 | Elapsed 15 days ago

● CPU ● Automation
● Ethernet ● RF Interference

Aler…	Unacknowledg…	Connectivity
0	26113 Active	0 Up / 5 Do…

Subscriber ID 0008

	Event code	# of Dependents	Date & Time
NetCon	E354 00 C915	0 / 0	Thu Oct 6 07:51:41 2022 GMT-4

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

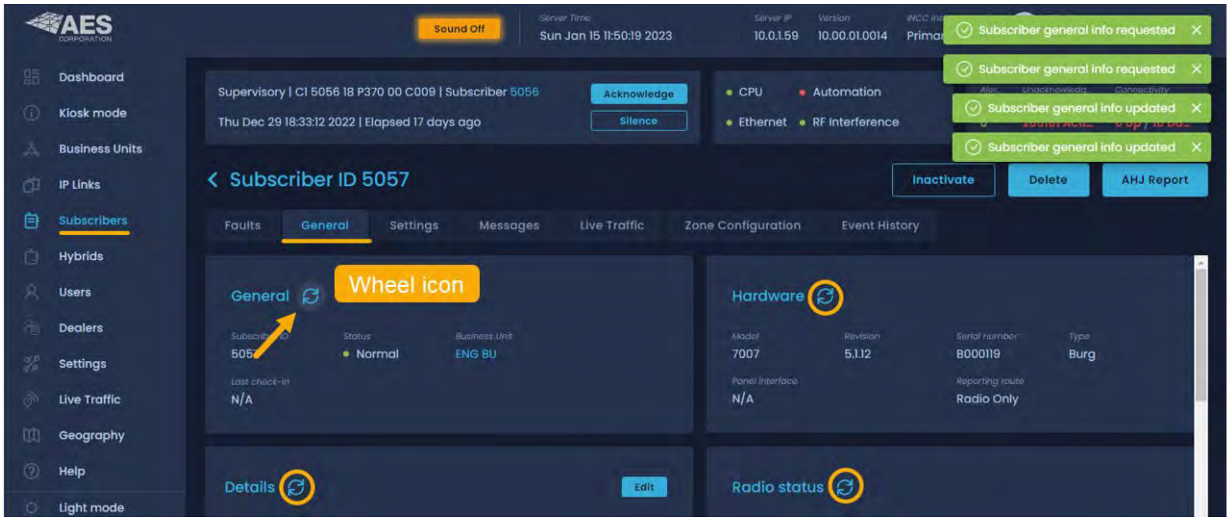
Fault Name	Event Code
RAM Chip	E307 00 C807
RAM Data	E307 00 C802
Redundant Comm	E350 00 C915
Remote Annunciator	E307 00 C813
RF Check-in Failure	E354 00 C906
RF Comm	E356 00 C903
RF Interference	E350 00 C906
RF Modem	E307 00 C805
Tamper	E145 00 C906
Timing	E307 00 C806
Zone Module	E307 00 C817

General Tab

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.
- Hardware – Subscriber model and panel interface information.
- Radio Status – Link layer and NetCon information.
- Zones – Zone and restoral status information.

- Refresh Icon – If the refresh icon is clicked, the INCC pings the subscriber with an outbound request to get the most recent information. In the example shown below, the General refresh icon was clicked. The green callouts at the top right indicate that the request has been acknowledged.



Server Time Sun Jan 15 11:50:19 2023
Server IP 10.0.1.59
Version 10.00.01.0014

Subscriber general info requested
Subscriber general info requested
Subscriber general info updated
Subscriber general info updated

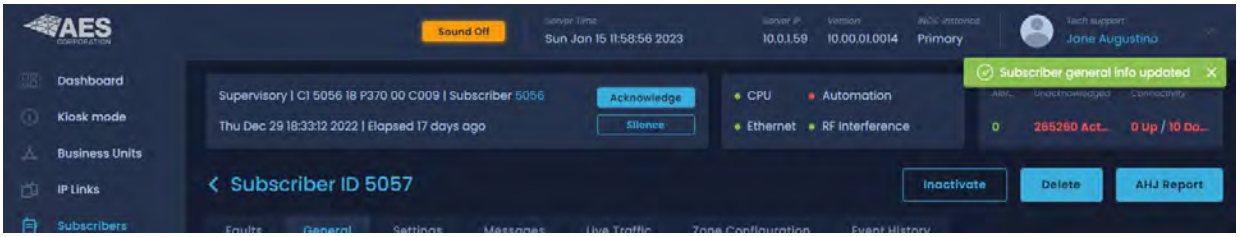
Supervisory | CI 5056 18 P370 00 C009 | Subscriber 5056
Thu Dec 29 18:33:12 2022 | Elapsed 17 days ago

Subscriber ID 5057

General
Subscriber ID 5057
Status Normal
Business Unit ENG BU
Last check-in N/A

Hardware
Model 7007
Revision 5.1.12
Serial number B000119
Type Burg
Panel interface N/A
Reporting route Radio Only

As the subscriber information is updated, notifications appear at the top right.



Server Time Sun Jan 15 11:58:56 2023
Server IP 10.0.1.59
Version 10.00.01.0014
INCC instance Primary
Tech support Jane Augustino

Subscriber general info updated

Supervisory | CI 5056 18 P370 00 C009 | Subscriber 5056
Thu Dec 29 18:33:12 2022 | Elapsed 17 days ago

Alar... 0
Unacknowledged 285260 Act...
Connectivity 0 Up / 10 Do...

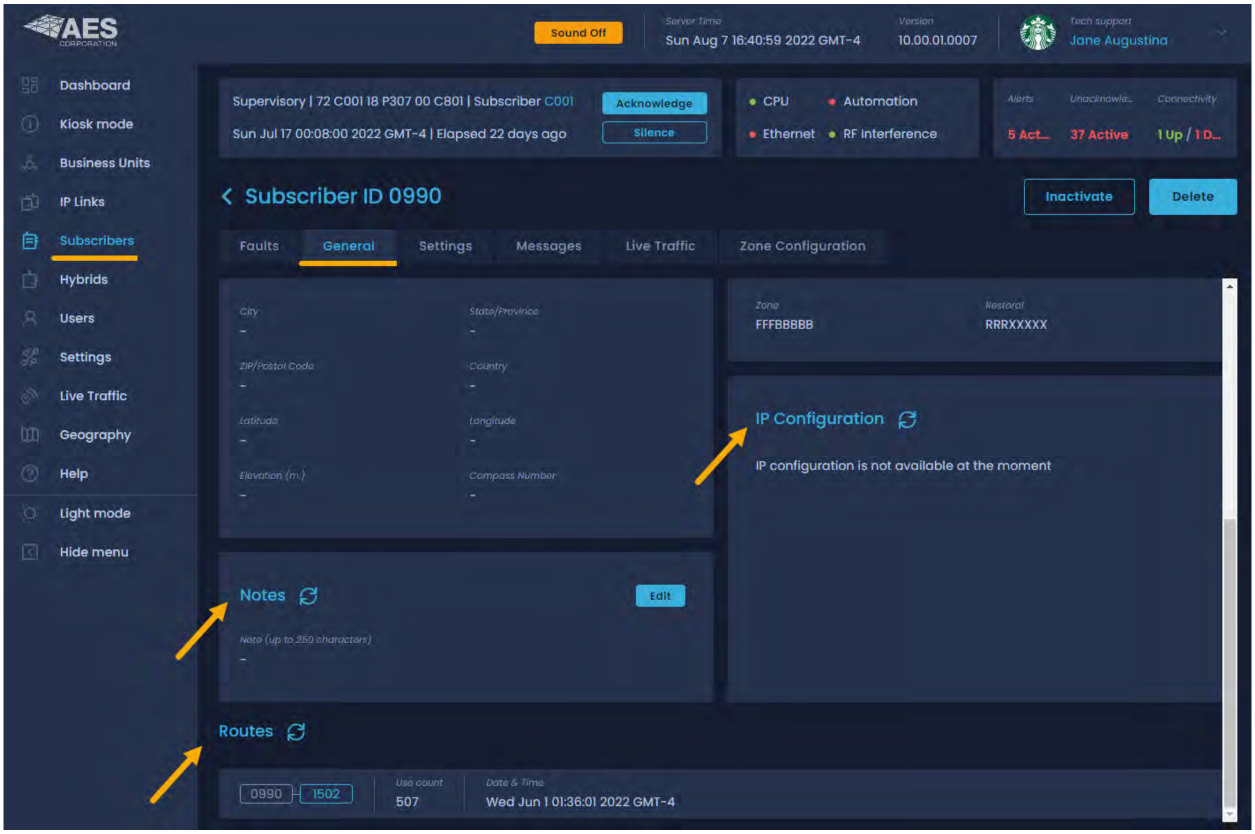
Subscriber ID 5057

Other subscriber settings in the General tab include:

- Notes – Free form text may be added for notes on the subscriber.
- Routes – Information on subscriber route paths.
- 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. It also includes the business unit group that the subscriber belongs to.

  For reporting routing, 2.0 subscribers can deliver signals using five different reporting options (all legacy subscribers do radio only).

  - Radio Only
  - Radio and Internet
  - Radio and Internet Backup
  - Internet and Radio Backup
  - Internet Only



Server Time: Sun Aug 7 16:40:59 2022 GMT-4
Version: 10.00.01.0007
Tech support: Jane Augustina

Supervisory | 72 C001 18 P307 00 C801 | Subscriber C001
Sun Jul 17 00:08:00 2022 GMT-4 | Elapsed 22 days ago

● CPU ● Automation
● Ethernet ● RF Interference

Alerts	Unacknowle...	Connectivity
5 Act...	37 Active	1 Up / 1 D...

Subscriber ID 0990

City -	State/Province -
ZIP/Postal Code -	Country -
Latitude -	Longitude -
Elevation (m.) -	Compass Number -

Zone: FFFBBBBB
Restoral: RRRXXXXX

IP Configuration

IP configuration is not available at the moment

Notes

Note (up to 250 characters)
-

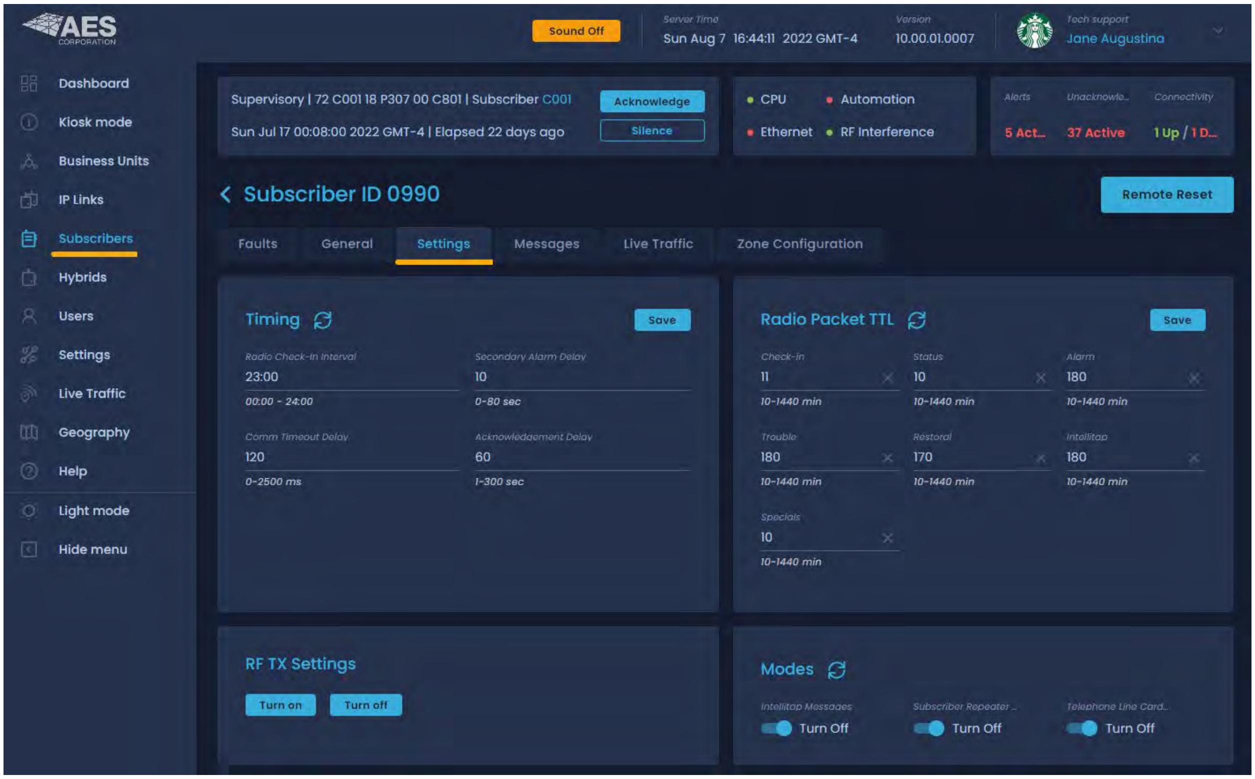
Routes

	Use count	Date & Time
0990 - 1502	507	Wed Jun 1 01:36:01 2022 GMT-4

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.



Server Time: Sun Aug 7 16:44:11 2022 GMT-4
Version: 10.00.01.0007
Tech support: Jane Augustina

Supervisory | 72 C001 18 P307 00 C801 | Subscriber C001
Sun Jul 17 00:08:00 2022 GMT-4 | Elapsed 22 days ago

● CPU ● Automation
● Ethernet ● RF Interference

Alerts	Unacknowle...	Connectivity
5 Act...	37 Active	1 Up / 1 D...

Subscriber ID 0990

Timing

Radio Check-In Interval: 23:00 (00:00 - 24:00)	Secondary Alarm Delay: 10 (0-80 sec)
Comm Timeout Delay: 120 (0-2500 ms)	Acknowledgement Delay: 60 (1-300 sec)

Radio Packet TTL

Check-in: 11 (10-1440 min)	Status: 10 (10-1440 min)	Alarm: 180 (10-1440 min)
Trouble: 180 (10-1440 min)	Restoral: 170 (10-1440 min)	Intellitap: 180 (10-1440 min)
Specials: 10 (10-1440 min)		

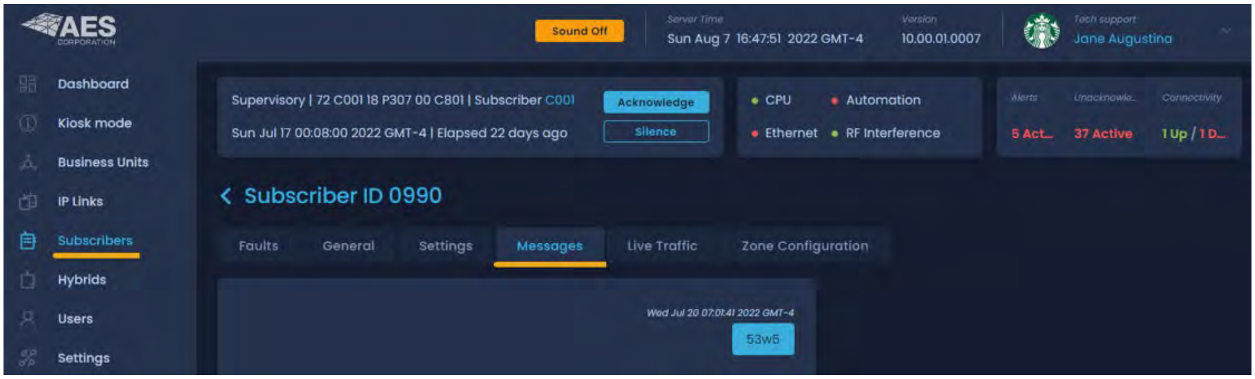
RF TX Settings

Modes

Intellitap Messages	Subscriber Repeater ...	Telephone Line Card...
Turn Off	Turn Off	Turn Off

Messages Tab

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

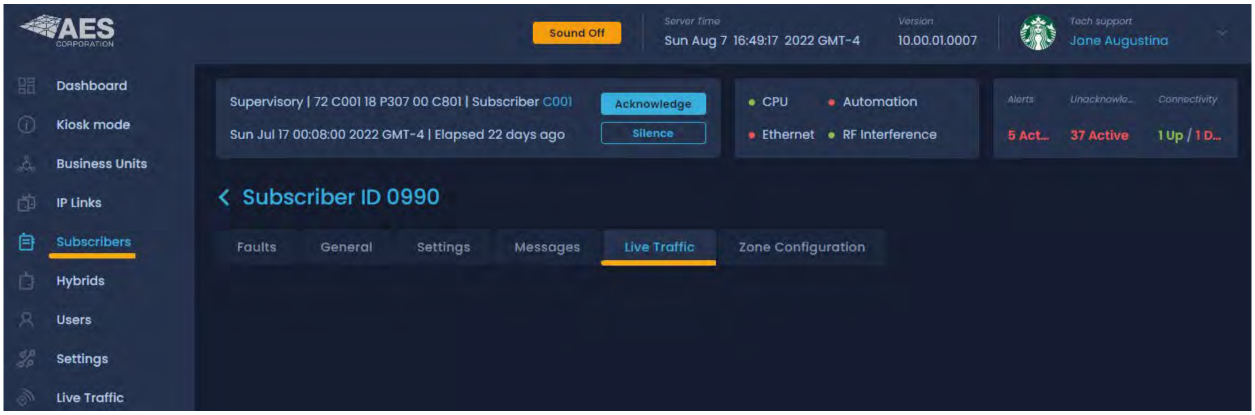


Supervisory | 72 C001 18 P307 00 C801 | Subscriber C001
Sun Jul 17 00:08:00 2022 GMT-4 | Elapsed 22 days ago

Wed Jul 20 07:01:41 2022 GMT-4
53w5

Live Traffic Tab

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



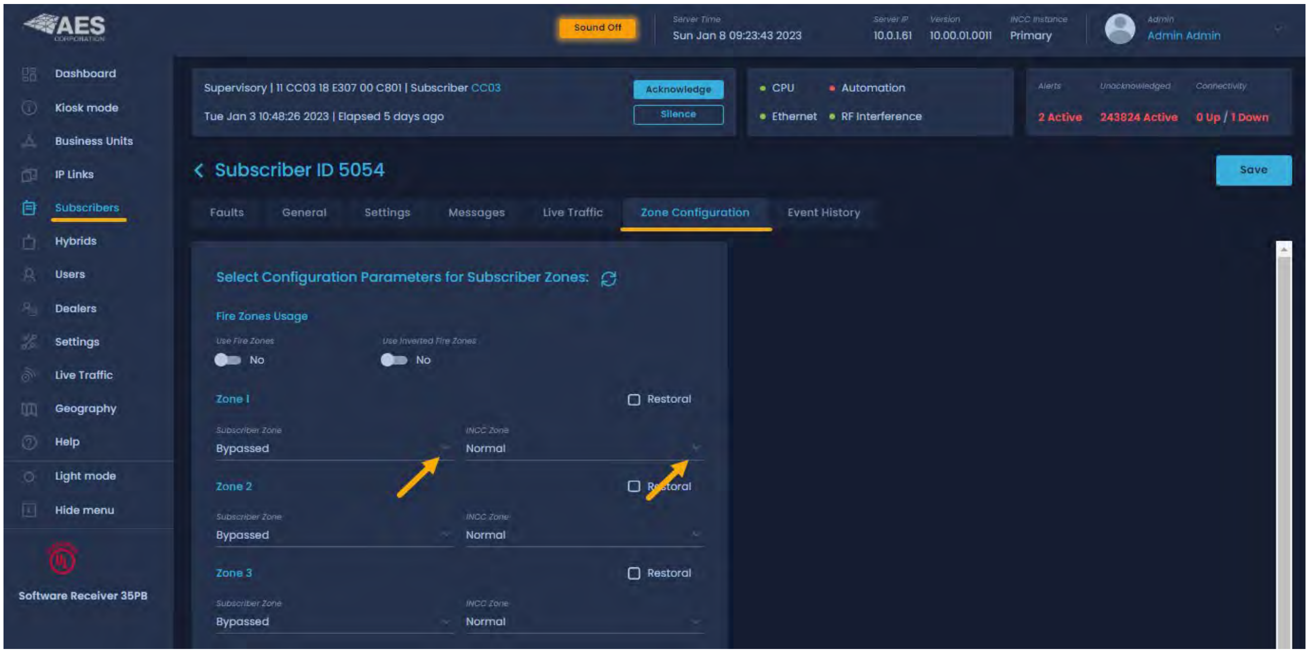
Supervisory | 72 C001 18 P307 00 C801 | Subscriber C001
Sun Jul 17 00:08:00 2022 GMT-4 | Elapsed 22 days ago

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 a message that was received. 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



Server Time: Sun Jan 8 09:23:43 2023 | Server IP: 10.0.1.61 | Version: 10.00.01.0011 | INCC Instance: Primary | Admin: Admin Admin

Supervisory | 11 CC03 18 E307 00 C801 | Subscriber CC03

Tue Jan 3 10:48:26 2023 | Elapsed 5 days ago

● CPU ● Automation ● Ethernet ● RF Interference

Alerts: 2 Active | Unacknowledged: 243824 Active | Connectivity: 0 Up / 1 Down

Subscriber ID 5054

Select Configuration Parameters for Subscriber Zones:

Fire Zones Usage

Use Fire Zones: No | Use Inverted Fire Zones: No

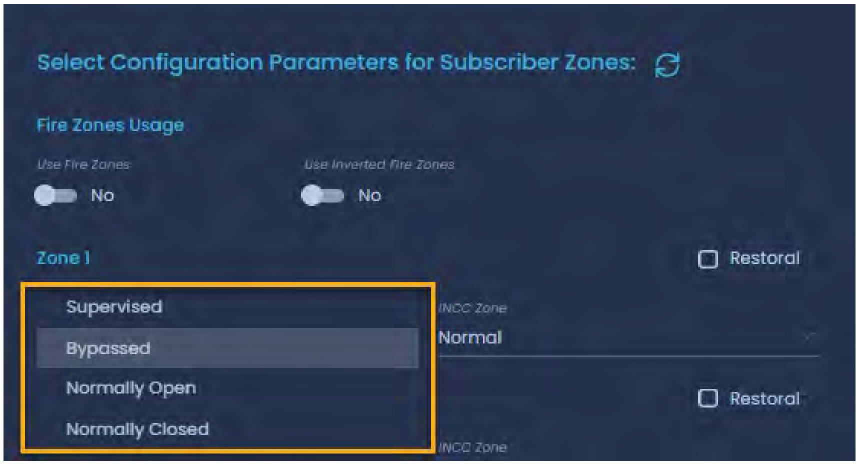
Zone 1 □ Restoral
Subscriber Zone: Bypassed | INCC Zone: Normal

Zone 2 □ Restoral
Subscriber Zone: Bypassed | INCC Zone: Normal

Zone 3 □ Restoral
Subscriber Zone: Bypassed | INCC Zone: Normal

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



Select Configuration Parameters for Subscriber Zones:

Fire Zones Usage

Use Fire Zones: No

Use Inverted Fire Zones: No

Zone 1

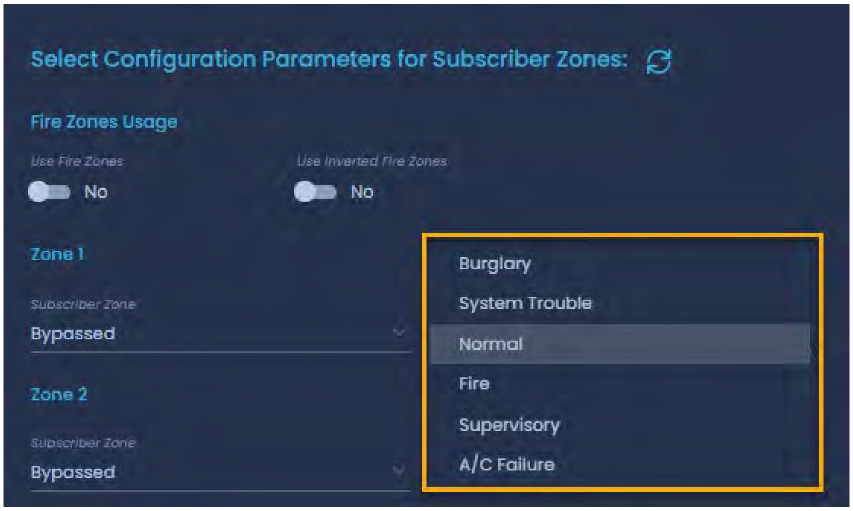
□ Restoral

INCC Zone: Normal

□ Restoral

INCC Zone

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



Select Configuration Parameters for Subscriber Zones:

Fire Zones Usage

Use Fire Zones: No

Use Inverted Fire Zones: No

Zone 1

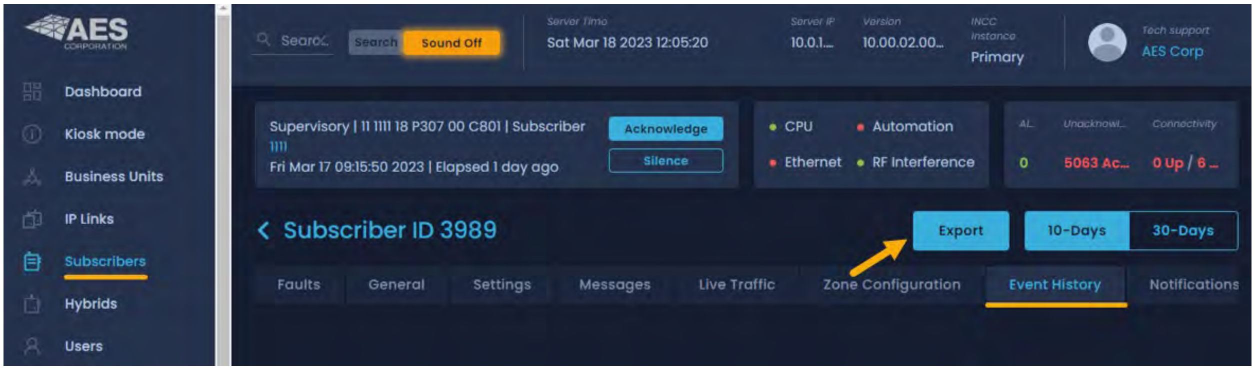
Subscriber Zone: Bypassed

Zone 2

Subscriber Zone: Bypassed

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.



Sat Mar 18 2023 12:05:20 | 10.0.1... | 10.00.02.00... | Primary

Supervisory | 11 1111 18 P307 00 C801 | Subscriber 1111
Fri Mar 17 09:15:50 2023 | Elapsed 1 day ago

0 | 5063 Ac... | 0 Up / 6 ...

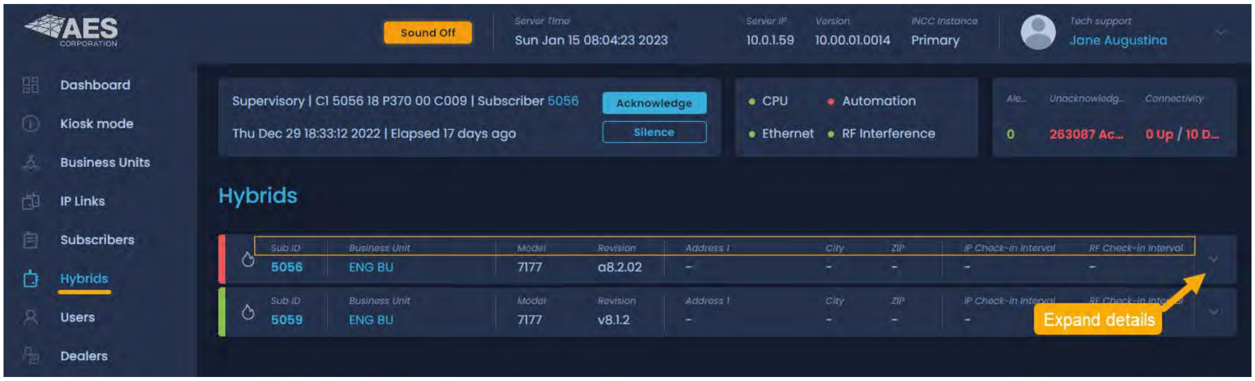
Subscriber ID 3989

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)

ℹ 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.



Sun Jan 15 08:04:23 2023 | 10.0.1.59 | 10.00.01.0014 | Primary

Supervisory | C1 5056 18 P370 00 C009 | Subscriber 5056
Thu Dec 29 18:33:12 2022 | Elapsed 17 days ago

0 | 263087 Ac... | 0 Up / 10 D...

Hybrids

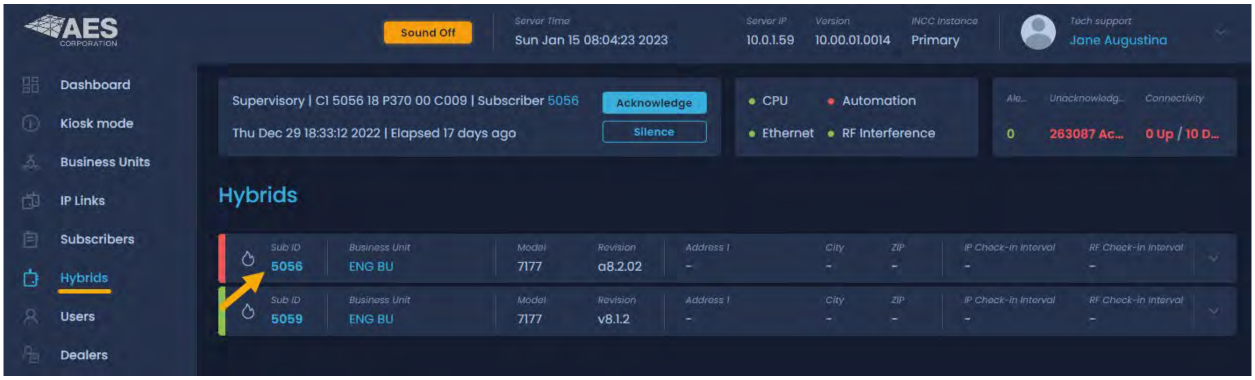
Sub ID	Business Unit	Model	Revision	Address 1	City	ZIP	IP Check-in Interval	RF Check-in Interval
5056	ENG BU	7177	a8.2.02	-	-	-	-	-
5059	ENG BU	7177	v8.1.2	-	-	-	-	

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

- Status
- Business unit
- Current faults
- Customer
- Comm timeout delay
- Check-in TTL

- Last check-in
- Alarm panel ID
- Dealer name
- Status TTL
- Alarm TTL
- Trouble TTL

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



Server Time: Sun Jan 15 08:04:23 2023 | Server IP: 10.0.1.59 | Version: 10.00.01.0014 | INCC Instance: Primary | Tech support: Jane Augustina

Supervisory | C1 5056 18 P370 00 C009 | Subscriber 5056

Thu Dec 29 18:33:12 2022 | Elapsed 17 days ago

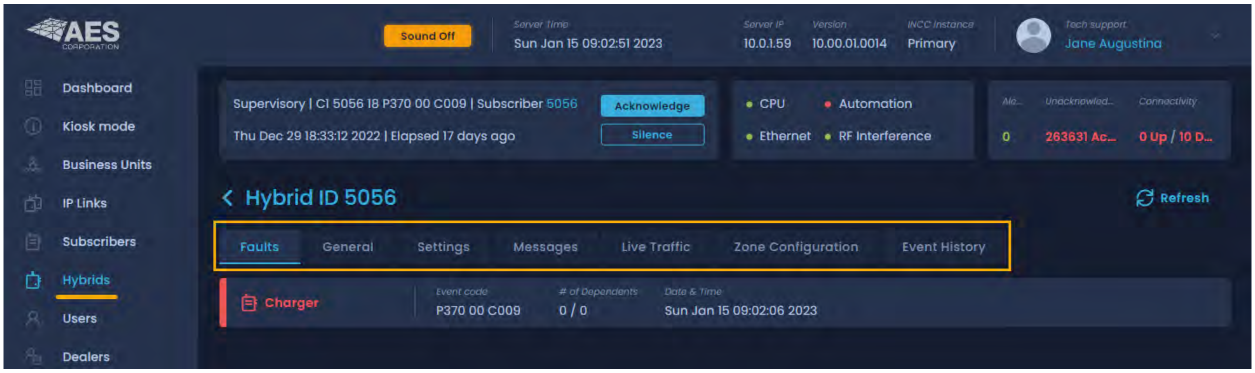
● CPU ● Automation ● Ethernet ● RF Interference

Ale...	Unacknowledg...	Connectivity
0	263087 Ac...	0 Up / 10 D...

Hybrids

Sub ID	Business Unit	Model	Revision	Address 1	City	ZIP	IP Check-in Interval	RF Check-in Interval
5056	ENG BU	7177	a8.2.02	-	-	-	-	-
5059	ENG BU	7177	v8.1.2	-	-	-	-	-

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



Server Time: Sun Jan 15 09:02:51 2023 | Server IP: 10.0.1.59 | Version: 10.00.01.0014 | INCC Instance: Primary | Tech support: Jane Augustina

Supervisory | C1 5056 18 P370 00 C009 | Subscriber 5056

Thu Dec 29 18:33:12 2022 | Elapsed 17 days ago

● CPU ● Automation ● Ethernet ● RF Interference

Ale...	Unacknowled...	Connectivity
0	263631 Ac...	0 Up / 10 D...

Hybrid ID 5056

	Event code	# of Dependents	Date & Time
Charger	P370 00 C009	0 / 0	Sun Jan 15 09:02:06 2023

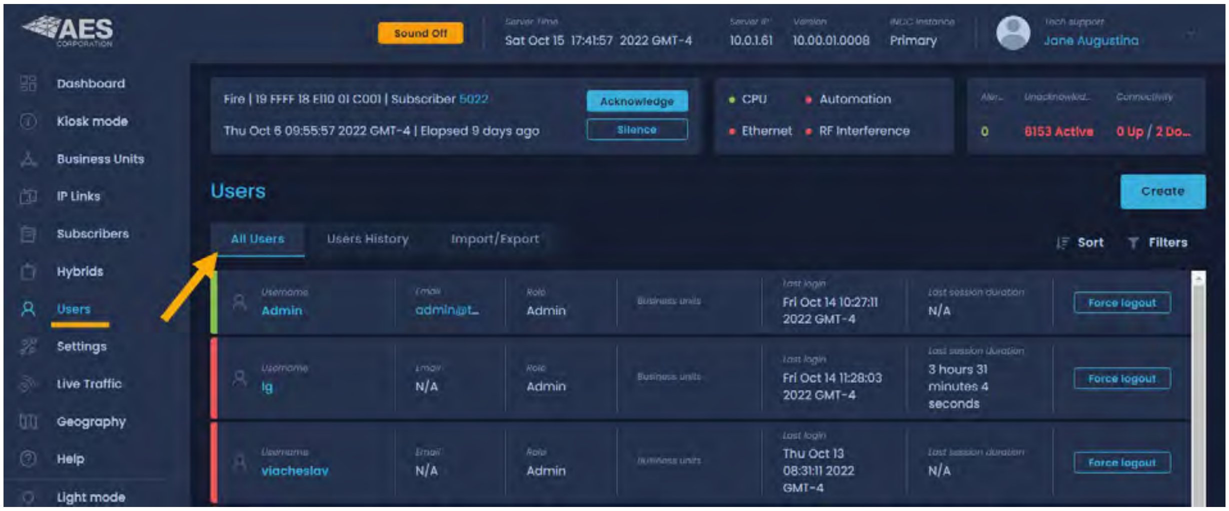
Users

All Users Tab

The **All Users** tab displays general information about users who have access to the INCC software. You can also see 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.

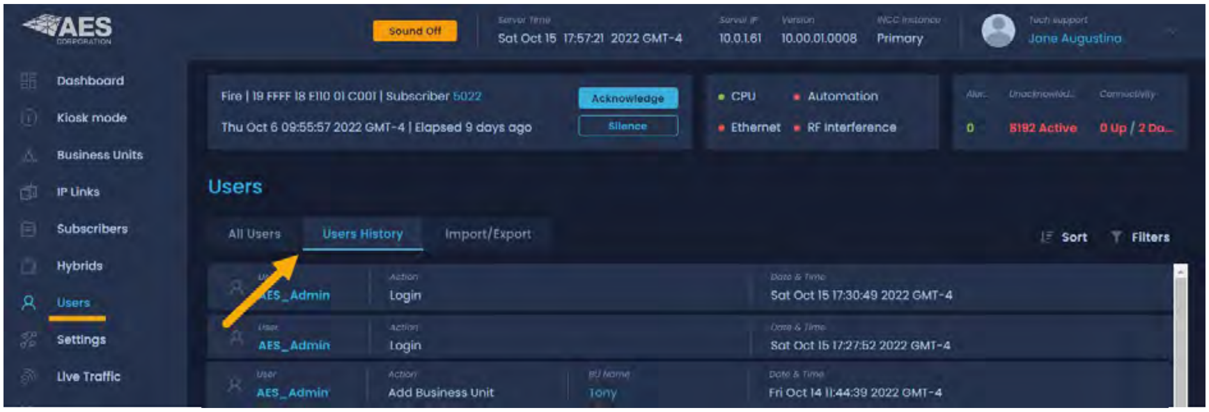
- To log a user out of the INCC software, click **Force logout**.



Username	Email	Role	Business units	Last login	Last session duration	
Admin	admin@t...	Admin		Fri Oct 14 10:27:11 2022 GMT-4	N/A	Force logout
lg	N/A	Admin		Fri Oct 14 11:28:03 2022 GMT-4	3 hours 31 minutes 4 seconds	Force logout
viacheslav	N/A	Admin		Thu Oct 13 08:31:11 2022 GMT-4	N/A	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.

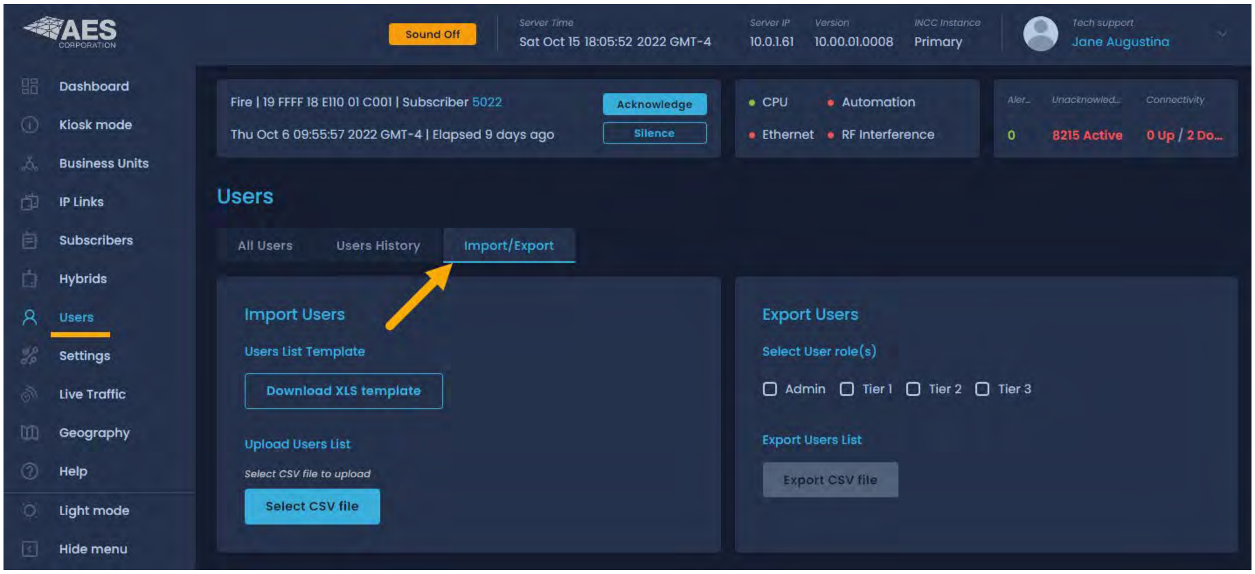


User	Action	BU Name	Date & Time
AES_Admin	Login		Sat Oct 15 17:30:49 2022 GMT-4
AES_Admin	Login		Sat Oct 15 17:27:52 2022 GMT-4
AES_Admin	Add Business Unit	Tony	Fri Oct 14 11:44:39 2022 GMT-4

Import/Export Tab

To import a list of users:

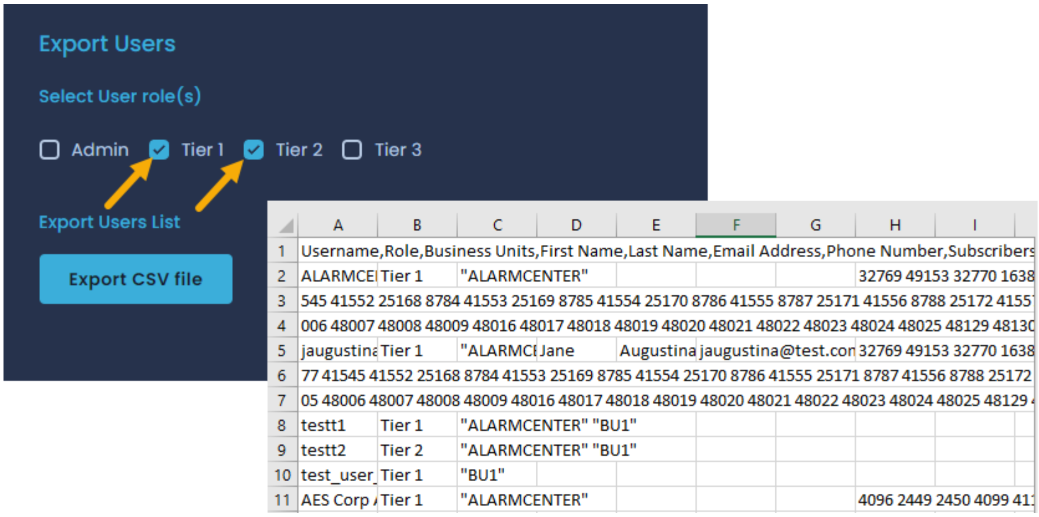
1. Click **Download XLS template** to download the template.
2. Populate columns A through N in the template. Save the file.
3. Export the Excel file to CSV.
4. Upload the CSV file by clicking **Select CSV file**.



Export Users

To export user data:

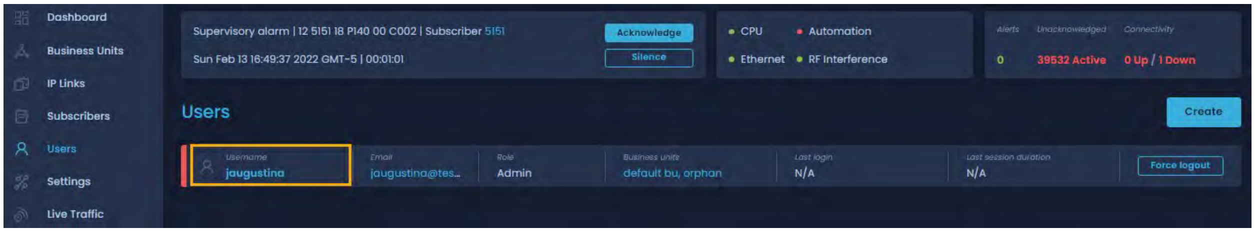
1. Check each box next to the roles you would like to collect data for.
2. Click the **Export CSV file** button to download the file. The Excel file consists of the data that was selected:



	A	B	C	D	E	F	G	H	I
1	Username,Role,Business Units,First Name,Last Name,Email Address,Phone Number,Subscribers								
2	ALARMCEI	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 48130								
5	jaugustina	Tier 1	"ALARMCI	Jane	Augustina	jaugustina@test.con		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.



Supervisory alarm | 12 5151 18 P140 00 C002 | Subscriber 5151
Sun Feb 13 16:49:37 2022 GMT-5 | 00:01:01

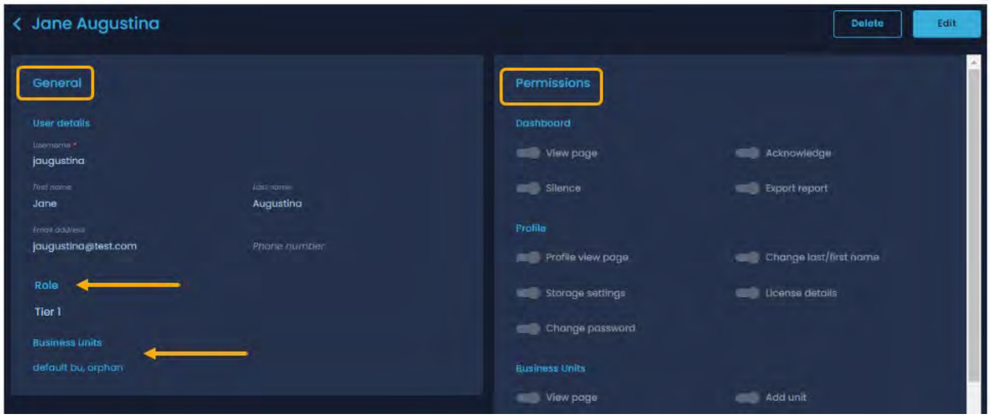
Alerts	Unacknowledged	Connectivity
0	39532 Active	0 Up / 1 Down

Users

Username	Email	Role	Business units	Last login	Last session duration
jaugustina	jaugustina@tes...	Admin	default bu, orphan	N/A	N/A

- 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.

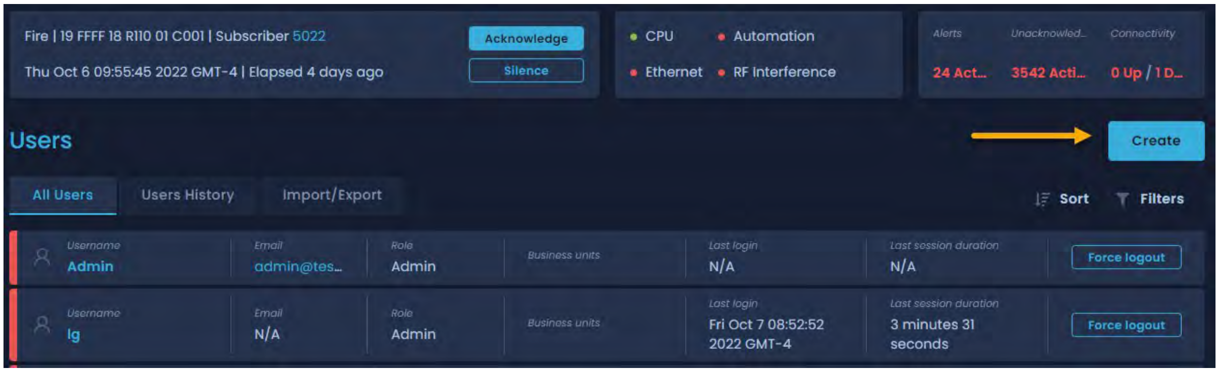


Jane Augustina

User details
Username *: jaugustina
First name: Jane
Last name: Augustina
Email address: jaugustina@test.com
Phone number
Role: Tier 1
Business units: default bu, orphan

Create a User Account

1. Click the **Create** button.



Fire | 19 FFFF 18 R110 01 C001 | Subscriber 5022
Thu Oct 6 09:55:45 2022 GMT-4 | Elapsed 4 days ago

Alerts	Unacknowled...	Connectivity
24 Act...	3542 Acti...	0 Up / 1 D...

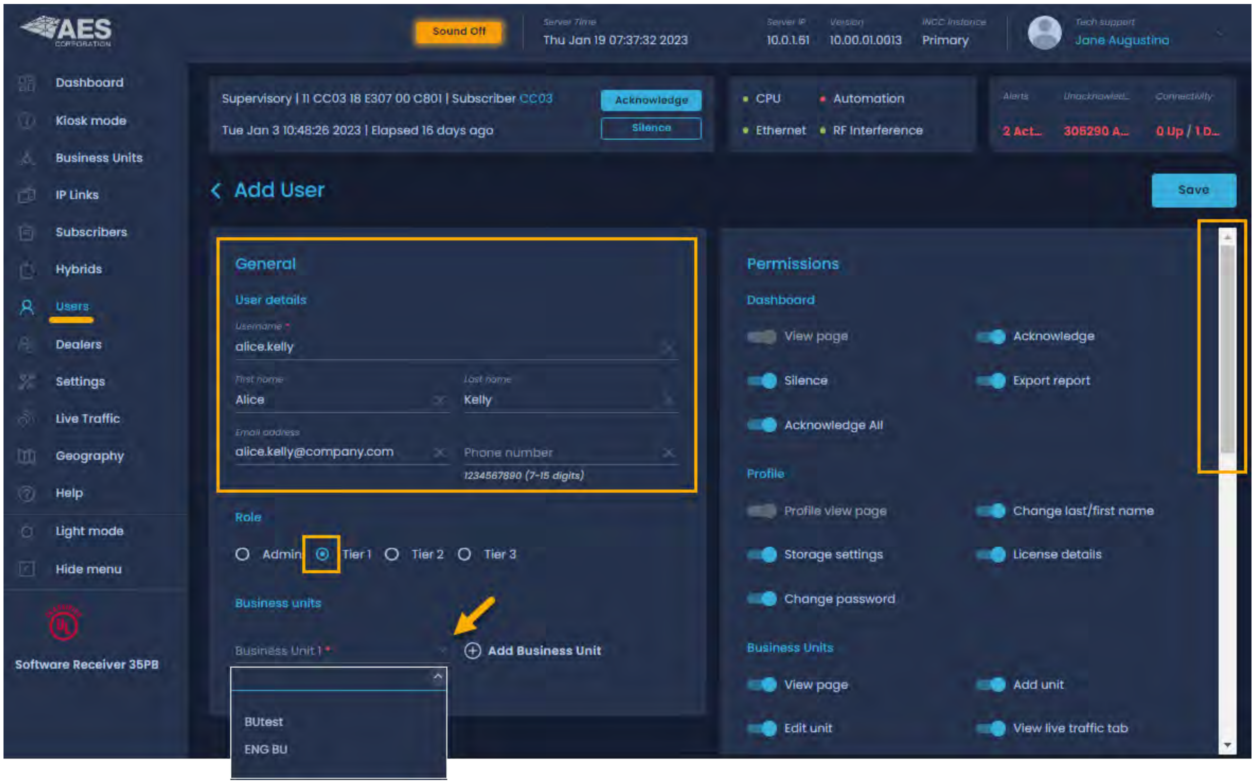
Users

Username	Email	Role	Business units	Last login	Last session duration
Admin	admin@tes...	Admin		N/A	N/A
lg	N/A	Admin		Fri Oct 7 08:52:52 2022 GMT-4	3 minutes 31 seconds

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

   Note: Different permissions are assigned different tier levels. Use the scrollbar at the right to view the permissions for each role.

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.



Server Time: Thu Jan 19 07:37:32 2023 | Server IP: 10.0.1.61 | Version: 10.00.01.0013 | INCC Instance: Primary | Tech support: Jane Augustina

Supervisory | 11 CC03 18 E307 00 C801 | Subscriber CC03
Tue Jan 3 10:48:26 2023 | Elapsed 16 days ago

Add User

General
User details
Username *: alice.kelly
First name: Alice
Last name: Kelly
Email address: alice.kelly@company.com
Phone number: 1234567890 (7-15 digits)

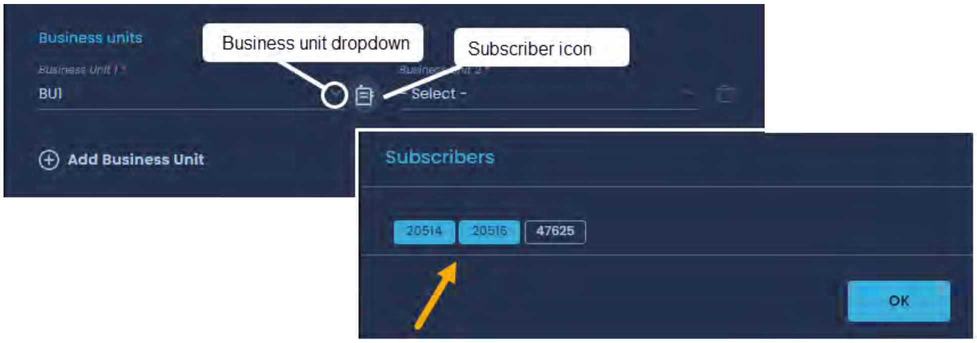
Role
○ Admin ● Tier 1 ○ Tier 2 ○ Tier 3

Business units
Business Unit 1 *
BUtest
ENG BU

Permissions
Dashboard
View page | Acknowledge
Silence | Export report
Acknowledge All
Profile
Profile view page | Change last/first name
Storage settings | License details
Change password
Business Units
View page | Add unit
Edit unit | View live traffic tab

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**.



Business units
Business Unit 1 *: BU1
Business Unit 2 *: - Select -

Subscribers
20514 20516 47625

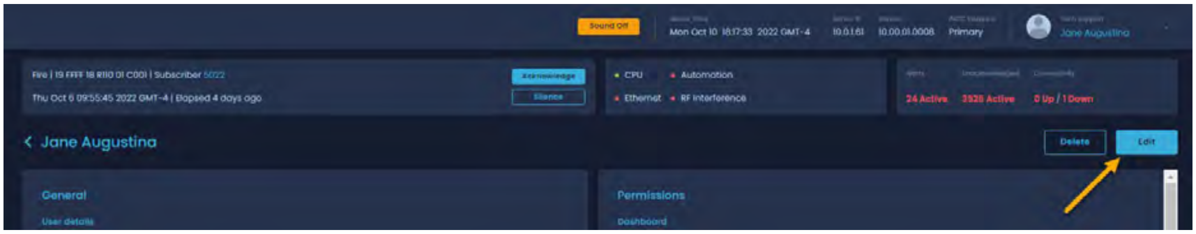
6. When you are finished setting up the user account, click **Save** (top right).

7. Upon Initial login, the user is prompted to change the password.

Note: Default password for initial login: INCC#2023

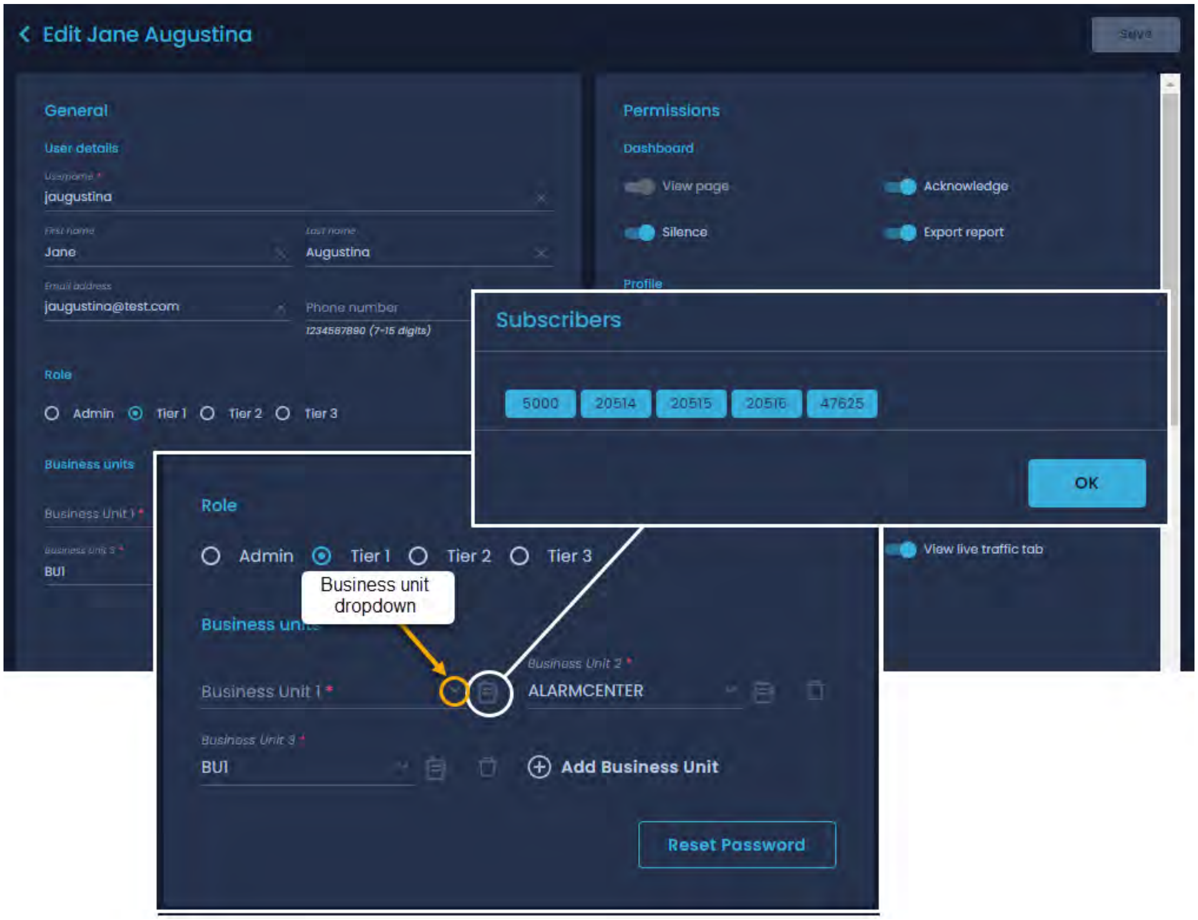
Edit a User Account

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



You can restrict the user’s access to specific business units and subscribers to prevent usesrs from viewing other business units and subscribers.

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**.


Edit Jane Augustina

Username * jaugustina

First name Jane

Last name Augustina

Email address jaugustina@test.com

Phone number 1234567890 (7-15 digits)

Role ○ Admin ● Tier 1 ○ Tier 2 ○ Tier 3

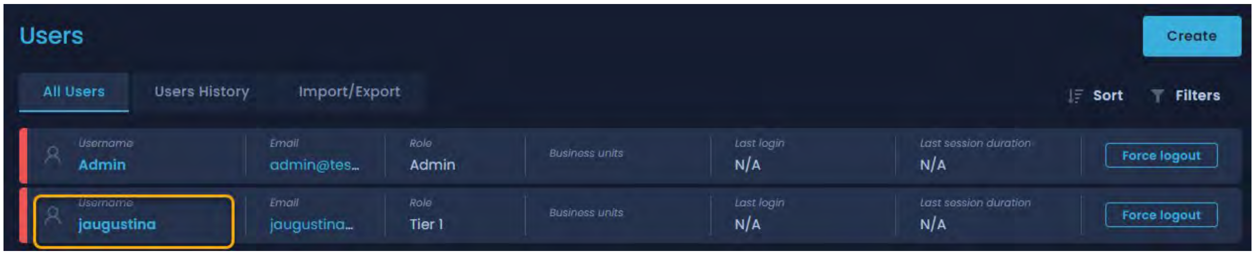
Business Unit 1 *

Business Unit 2 * ALARMCENTER

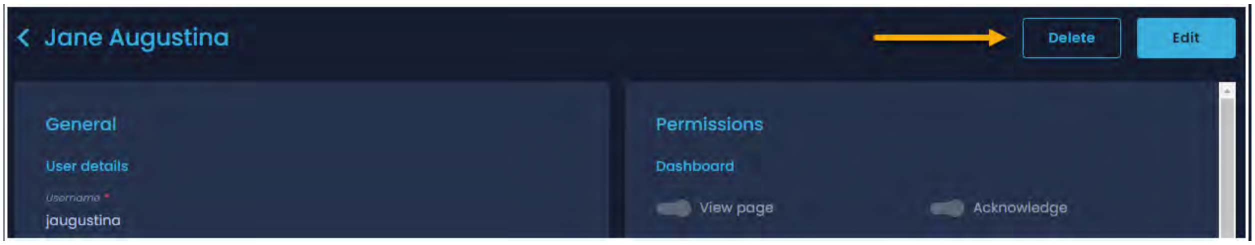
Business Unit 3 * BU1

Delete a User Account

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



Username	Email	Role	Business units	Last login	Last session duration
Admin	admin@tes...	Admin		N/A	N/A
jaugustina	jaugustina...	Tier 1		N/A	N/A



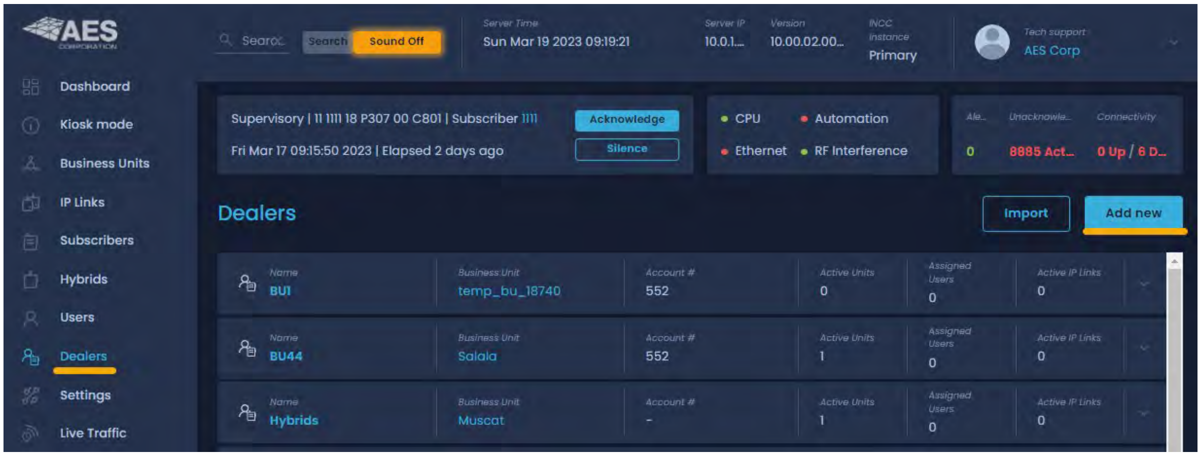
Username * jaugustina

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**.



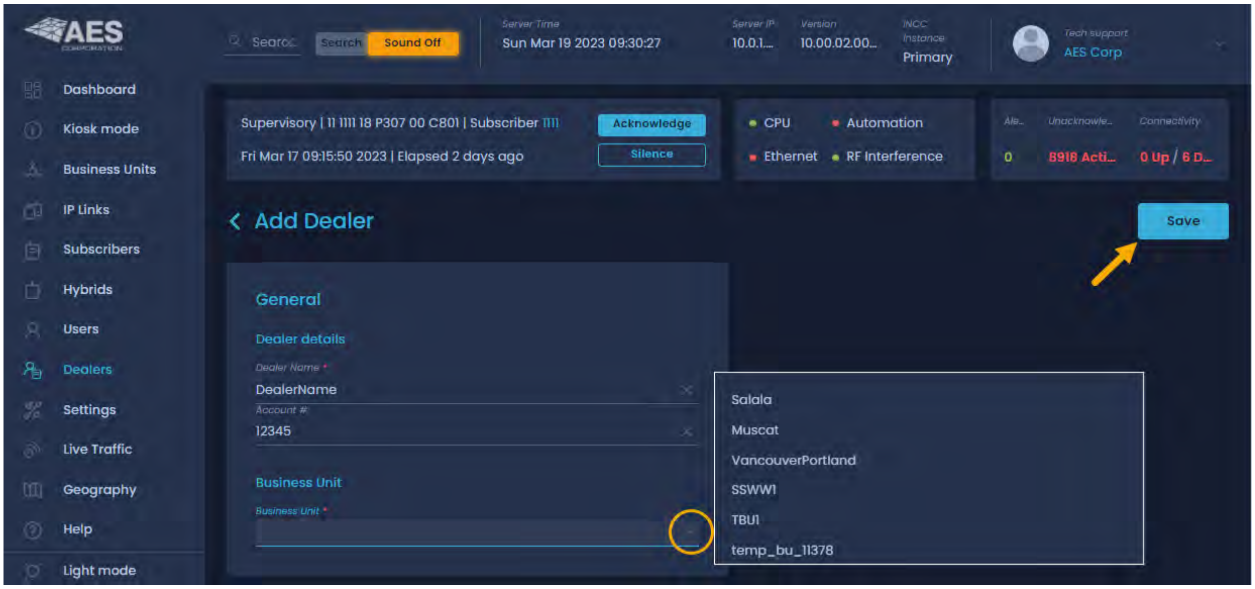
Server Time Sun Mar 19 2023 09:19:21 | Server IP 10.0.1... | Version 10.00.02.00... | INCC instance Primary | Tech support AES Corp

Supervisory | 11 1111 18 P307 00 C801 | Subscriber 1111
Fri Mar 17 09:15:50 2023 | Elapsed 2 days ago

Ale... 0 | Unacknowle... 8885 Act... | Connectivity 0 Up / 6 D...

Name	Business Unit	Account #	Active Units	Assigned Users	Active IP Links
BU1	temp_bu_18740	552	0	0	0
BU44	Salala	552	1	0	0
Hybrids	Muscat	-	1	0	0

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



Server Time: Sun Mar 19 2023 09:30:27 | Server IP: 10.0.1... | Version: 10.00.02.00... | INCC Instance: Primary | Tech support: AES Corp

Supervisory | 11 1111 18 P307 00 C801 | Subscriber 1111
Fri Mar 17 09:15:50 2023 | Elapsed 2 days ago

Ale...: 0 | Unacknowle...: 8918 Acti... | Connectivity: 0 Up / 6 D...

Add Dealer

General

Dealer details

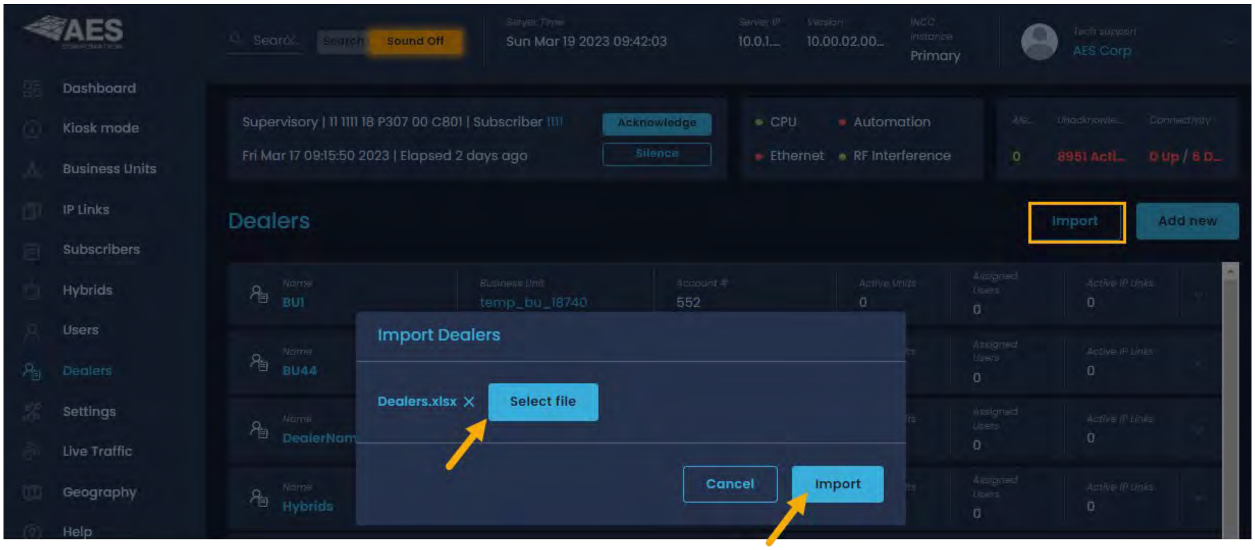
Dealer Name *: DealerName
Account #: 12345

Business Unit

Business Unit *

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.



Server Time: Sun Mar 19 2023 09:42:03 | Server IP: 10.0.1... | Version: 10.00.02.00... | INCC Instance: Primary | Tech support: AES Corp

Supervisory | 11 1111 18 P307 00 C801 | Subscriber 1111
Fri Mar 17 09:15:50 2023 | Elapsed 2 days ago

Ale...: 0 | Unacknowle...: 8951 Acti... | Connectivity: 0 Up / 6 D...

Dealers

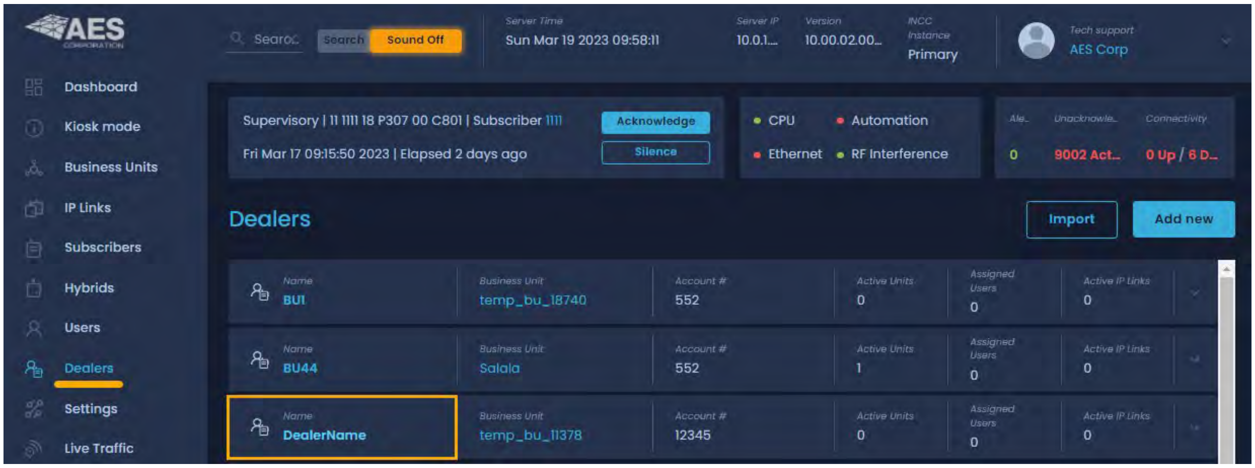
Name	Business Unit	Account #	Active Units	Assigned Users	Active IP Links
BU1	temp_bu_18740	552	0	0	0
BU44				0	0
DealerNam...				0	0
Hybrids				0	0

Import Dealers

Dealers.xlsx

To Add Subscribers to the Dealer

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



Server Time: Sun Mar 19 2023 09:58:11 | Server IP: 10.0.1... | Version: 10.00.02.00... | INCC Instance: Primary | Tech support: AES Corp

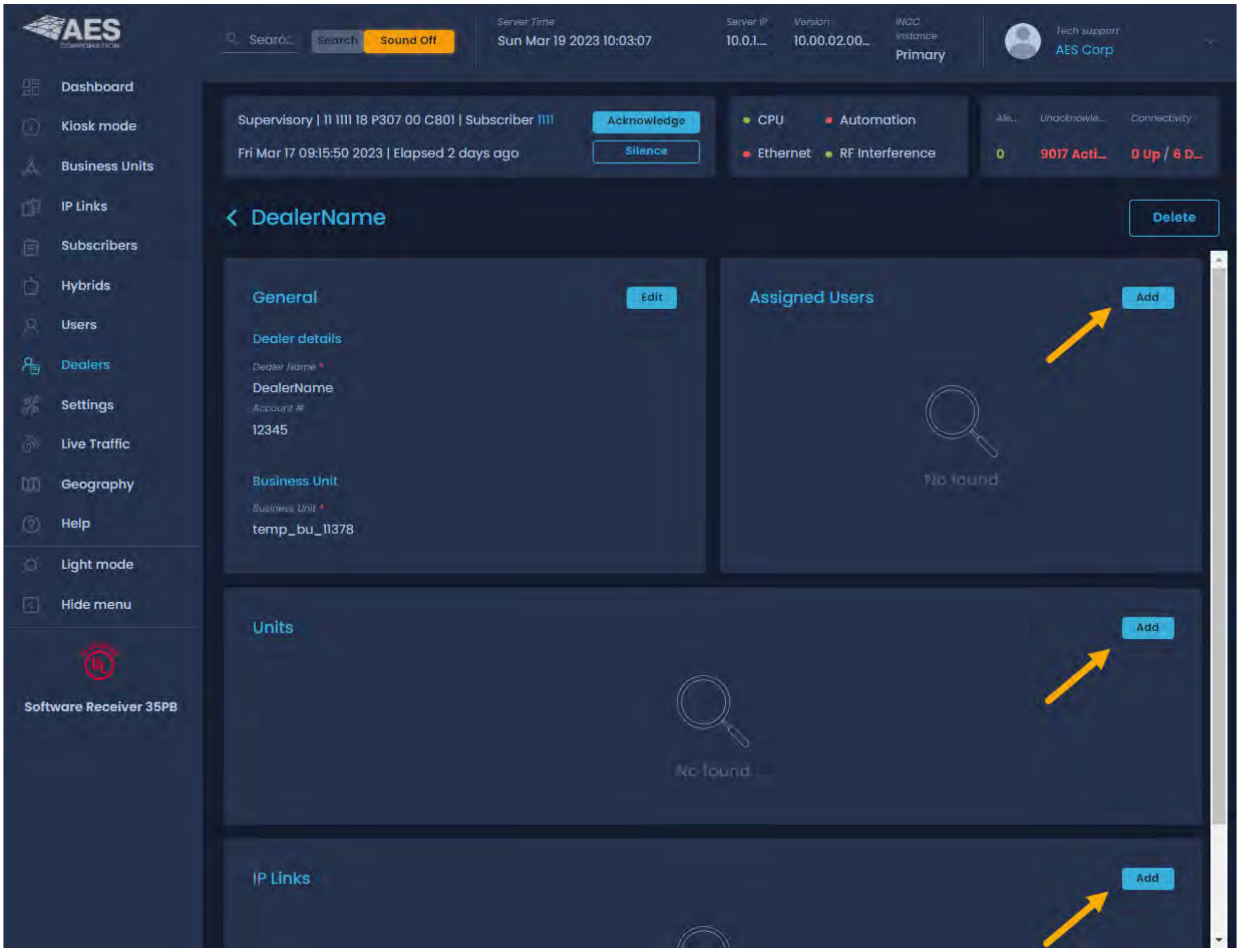
Supervisory | 11 1111 18 P307 00 C801 | Subscriber 1111
Fri Mar 17 09:15:50 2023 | Elapsed 2 days ago

Ale...	Unacknowle...	Connectivity
0	9002 Act...	0 Up / 6 D...

Dealers

Name	Business Unit	Account #	Active Units	Assigned Users	Active IP Links
BU1	temp_bu_18740	552	0	0	0
BU44	Salala	552	1	0	0
DealerName	temp_bu_11378	12345	0	0	0

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



Server Time: Sun Mar 19 2023 10:03:07 | Server IP: 10.0.1... | Version: 10.00.02.00... | INCC Instance: Primary | Tech support: AES Corp

Supervisory | 11 1111 18 P307 00 C801 | Subscriber 1111
Fri Mar 17 09:15:50 2023 | Elapsed 2 days ago

Ale...	Unacknowle...	Connectivity
0	9017 Acti...	0 Up / 6 D...

DealerName

General

Dealer details
Dealer Name *: DealerName
Account #: 12345

Business Unit
Business Unit *: temp_bu_11378

Assigned Users

Units

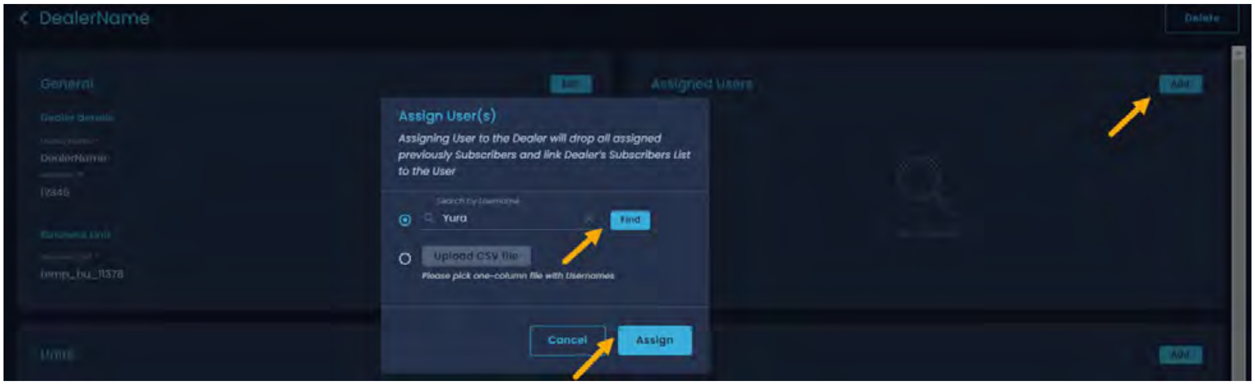
IP Links

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**.

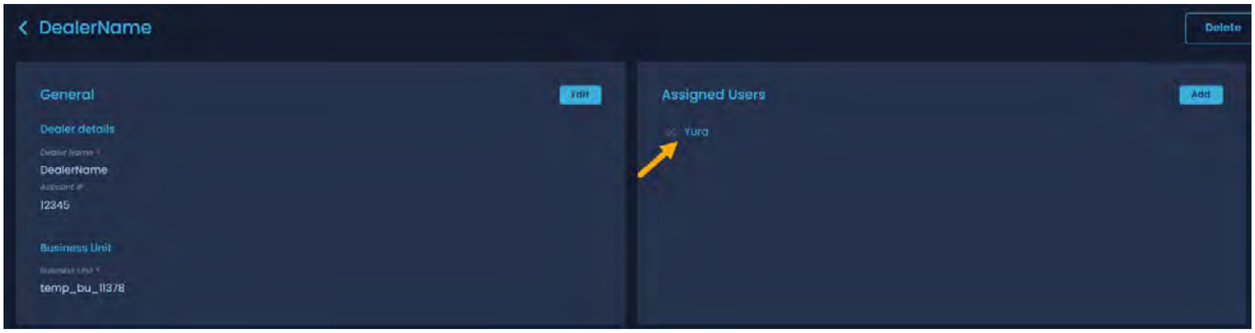
Note: You can also add users via a CSV file.



Assigning User to the Dealer will drop all assigned previously Subscribers and link Dealer's Subscribers List to the User

○ Upload CSV file *Please pick one-column file with Usernames*

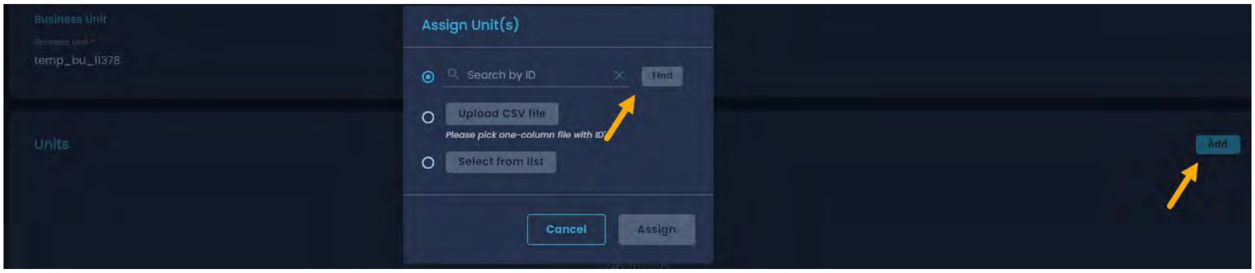
The user appears is the **Assigned Users** list.



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.

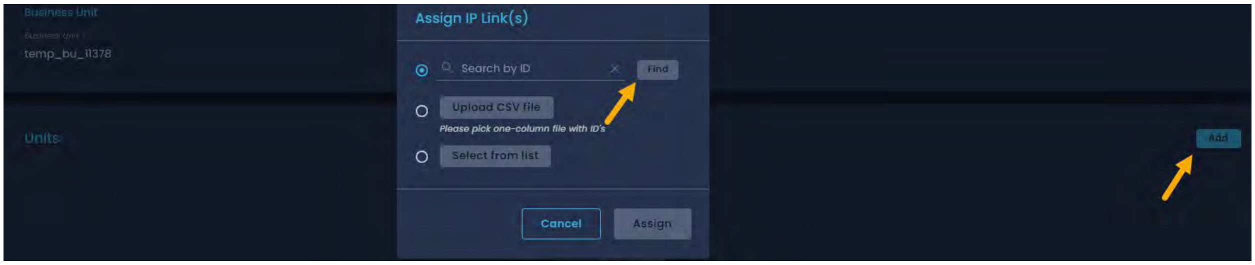


○ Upload CSV file *Please pick one-column file with ID*

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.



Business Unit
Business Unit: temp_bu_11378

Units

Assign IP Link(s)

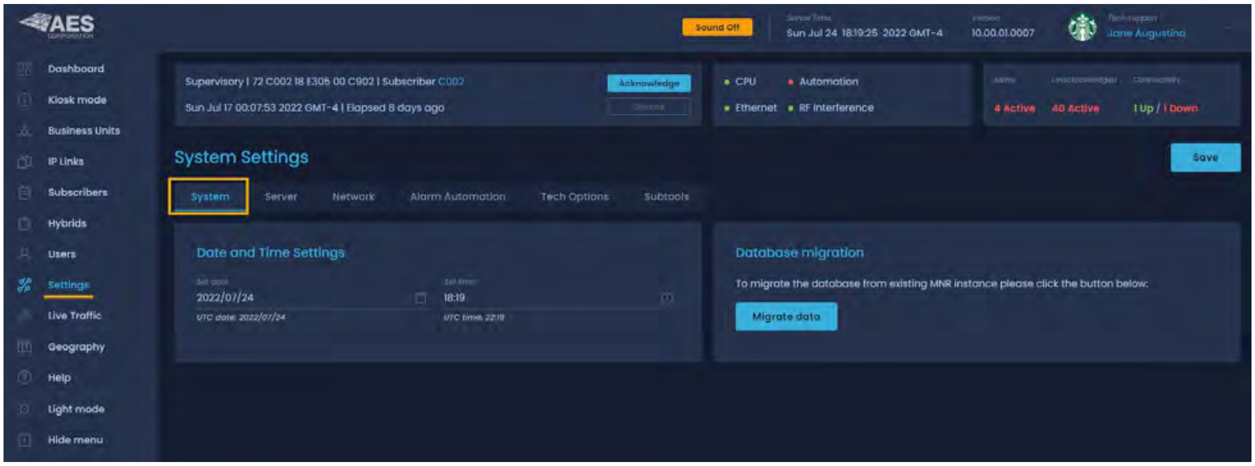
● Search by ID ✕ Find
○ Upload CSV file
Please pick one-column file with ID's
○ Select from list

Cancel Assign

Settings

System Tab

System Settings allows you to change the date and time for the INCC server.



Server Time: Sun Jul 24 18:19:25 2022 GMT-4
Version: 10.00.01.0007
Tech support: Jane Augustino

Supervisory | 72 C002 18 E305 00 C902 | Subscriber C002
Sun Jul 17 00:07:53 2022 GMT-4 | Elapsed 8 days ago

4 Active 40 Active 1 Up / 1 Down

System Settings

Date and Time Settings
Set date: 2022/07/24
UTC date: 2022/07/24
Set time: 18:19
UTC time: 22:19

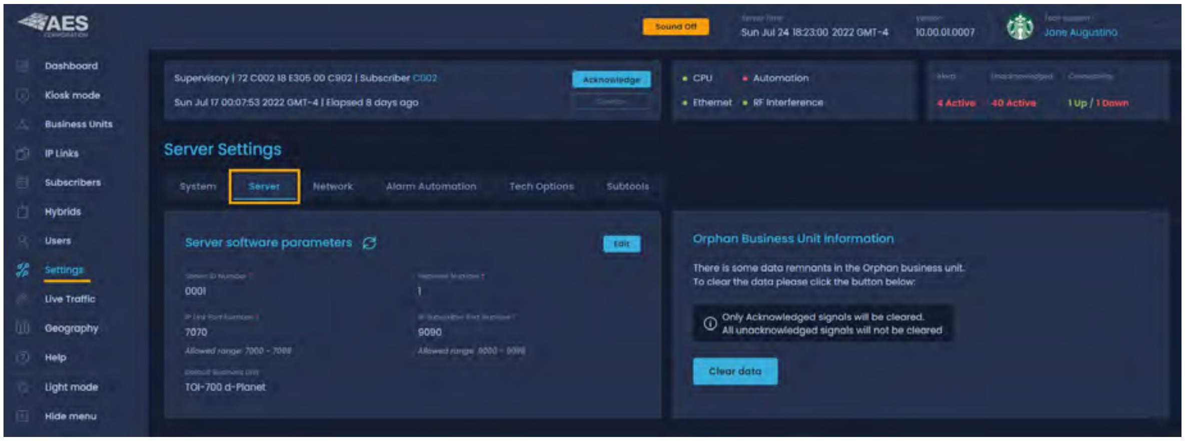
Database migration
To migrate the database from existing MNR instance please click the button below:

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.



Sun Jul 24 18:23:00 2022 GMT-4

10.00.01.0007

Jane Augustino

Supervisory | 72 C002 18 E305 00 C902 | Subscriber C002

Sun Jul 17 00:07:53 2022 GMT-4 | Elapsed 8 days ago

4 Active 40 Active 1 Up / 1 Down

Server Settings

Server software parameters

Server ID Number: 0001

Network Number: 1

IP Link Port Number: 7070

Allowed range: 7000 - 7099

IP Subscriber Port Number: 9090

Allowed range: 9000 - 9099

Default Business Unit: TOI-700 d-Planet

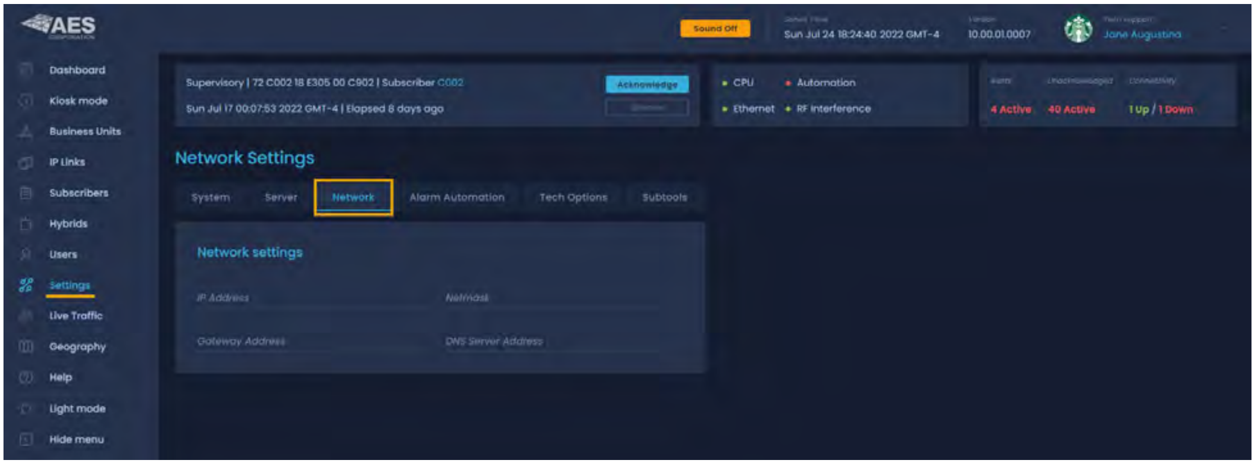
Orphan Business Unit Information

There is some data remnants in the Orphan business unit.
To clear the data please click the button below:

Only Acknowledged signals will be cleared.
All unacknowledged signals will not be cleared

Network Tab

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



Sun Jul 24 18:24:40 2022 GMT-4

10.00.01.0007

Jane Augustino

Supervisory | 72 C002 18 E305 00 C902 | Subscriber C002

Sun Jul 17 00:07:53 2022 GMT-4 | Elapsed 8 days ago

4 Active 40 Active 1 Up / 1 Down

Network Settings

Network settings

IP Address

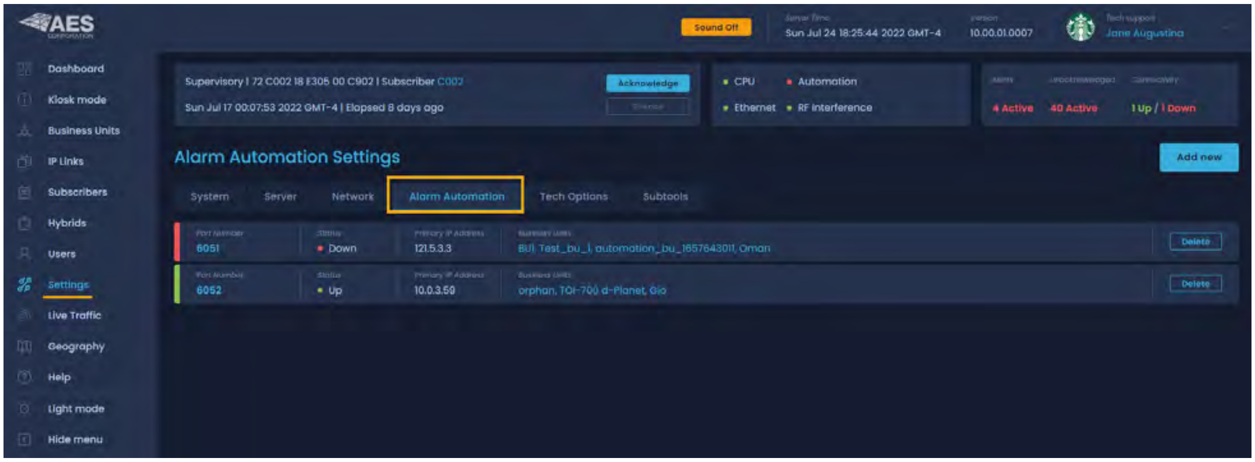
Netmask

Gateway Address

DNS Server Address

Alarm Automation Tab

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



Sun Jul 24 18:25:44 2022 GMT-4

10.00.01.0007

Jane Augustina

Supervisory | 72 C002 18 E305 00 C902 | Subscriber C002

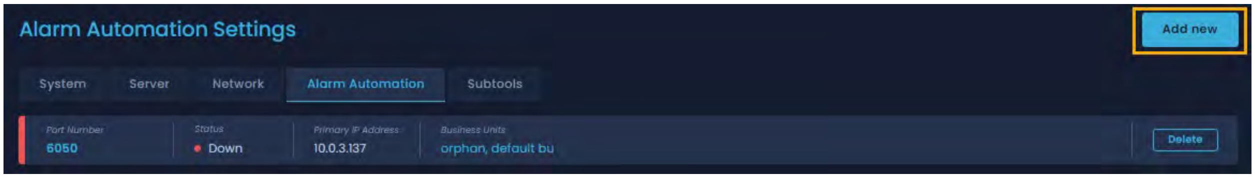
Sun Jul 17 00:07:53 2022 GMT-4 | Elapsed 8 days ago

4 Active 40 Active 1 Up / 1 Down

Alarm Automation Settings

Port Number	Status	Primary IP Address	Business Units
6051	Down	121.5.3.3	BU1, Test_bu_1, automation_bu_1657643011, Oman
6052	Up	10.0.3.59	orphan, TOI-700 d-Planet, Gio

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

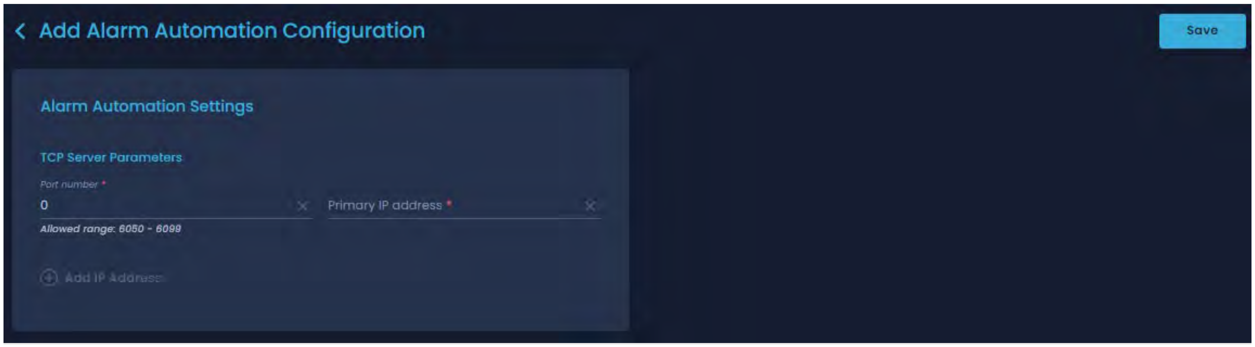


Alarm Automation Settings

Port Number	Status	Primary IP Address	Business Units
6050	Down	10.0.3.137	orphan, default bu

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.



Add Alarm Automation Configuration

Alarm Automation Settings

TCP Server Parameters

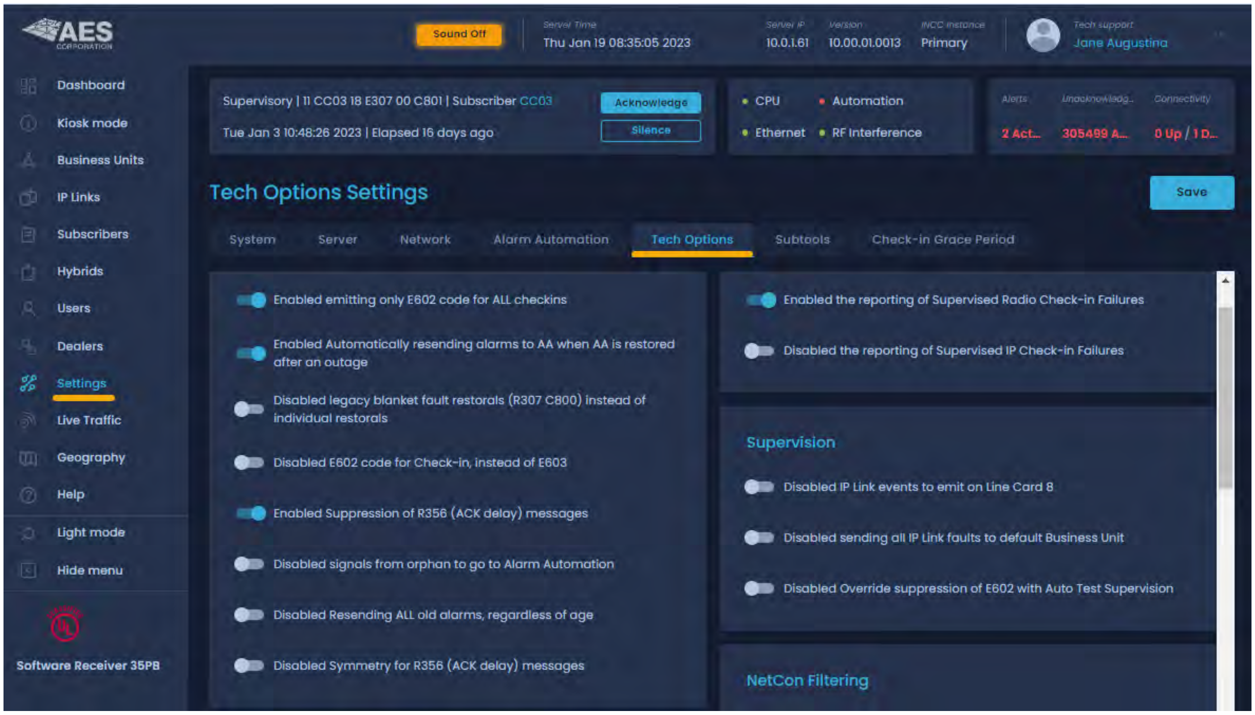
Port number * 0

Allowed range: 6050 - 6099

Primary IP address *

Tech Options Tab

Listed below are all the options available on the …



Server Time: Thu Jan 19 08:35:05 2023
Server IP: 10.0.1.61
Version: 10.00.01.0013
INCC Instance: Primary
Tech support: Jane Augustina

Supervisory | 11 CC03 18 E307 00 C801 | Subscriber CC03
Tue Jan 3 10:48:26 2023 | Elapsed 16 days ago

Alerts: 2 Act…
Unacknowledg…: 305499 A…
Connectivity: 0 Up / 1 D…

Tech Options Settings

- Enabled emitting only E602 code for ALL checkins
- Enabled Automatically resending alarms to AA when AA is restored after an outage
- Disabled legacy blanket fault restorals (R307 C800) instead of individual restorals
- Disabled E602 code for Check-in, instead of E603
- Enabled Suppression of R356 (ACK delay) messages
- Disabled signals from orphan to go to Alarm Automation
- Disabled Resending ALL old alarms, regardless of age
- Disabled Symmetry for R356 (ACK delay) messages
- Enabled the reporting of Supervised Radio Check-in Failures
- Disabled the reporting of Supervised IP Check-in Failures

Supervision

- Disabled IP Link events to emit on Line Card 8
- Disabled sending all IP Link faults to default Business Unit
- Disabled Override suppression of E602 with Auto Test Supervision

NetCon Filtering

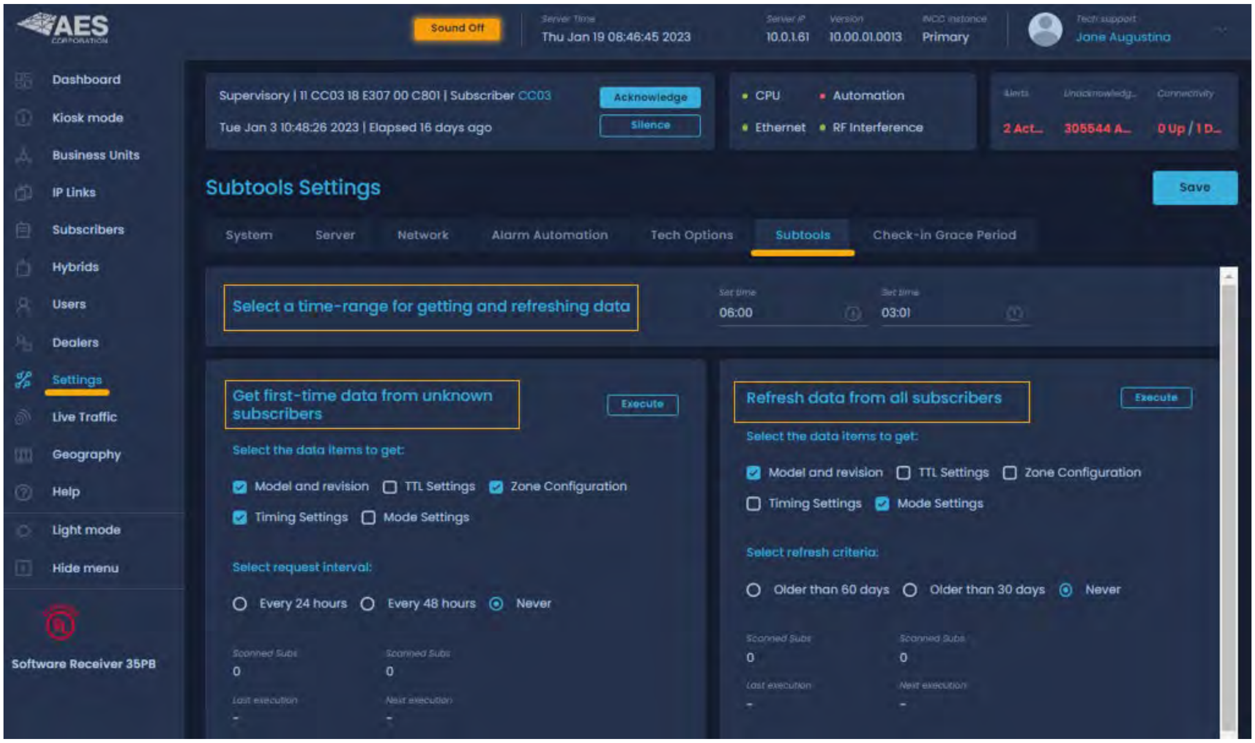
Options	Enable?
Enabled emitting only E602 *code for ALL checkins* This feature will eliminate E603 & E608 and combine to only #E602	
Enabled Automatically resending alarms to AA when AA is restored after an outage This feature allows the INCC/MultiNet Receiver to automatically resend messages to Automation 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

Options	Enable?
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 be 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 *E*nable and Disable Feature E/R. By default system will only generate R, this feature will add E	
Deduplication	
Enabled *IP packet deduplication* 2.0 MCT Subscribers will receive RF and IP packets. Enable/Disable receiving single or dual packets	Yes/No
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	No

Options	Enable?
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.	
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 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.	No

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.



Server Time: Thu Jan 19 08:46:45 2023
Server IP: 10.0.1.61
Version: 10.00.01.0013
INCC instance: Primary
Tech support: Jane Augustina

Supervisory | 11 CC03 18 E307 00 C801 | Subscriber CC03
Tue Jan 3 10:48:26 2023 | Elapsed 16 days ago

● CPU ● Automation
● Ethernet ● RF Interference

Alerts	Unacknowledg...	Connectivity
2 Act...	305544 A...	0 Up / 1 D...

Subtools Settings

Select a time-range for getting and refreshing data
Set time: 06:00
Set time: 03:01

Get first-time data from unknown subscribers
Select the data items to get:
☑ Model and revision ☐ TTL Settings ☑ Zone Configuration
☑ Timing Settings ☐ Mode Settings
Select request interval:
○ Every 24 hours ○ Every 48 hours ● Never
Scanned Subs: 0
Scanned Subs: 0
Last execution: -
Next execution: -

Refresh data from all subscribers
Select the data items to get:
☑ Model and revision ☐ TTL Settings ☐ Zone Configuration
☐ Timing Settings ☑ Mode Settings
Select refresh criteria:
○ Older than 60 days ○ Older than 30 days ● Never
Scanned Subs: 0
Scanned Subs: 0
Last execution: -
Next execution: -

Configuring first-time data from unknown subscribers

These settings are associated with subscribers that come onto 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**.

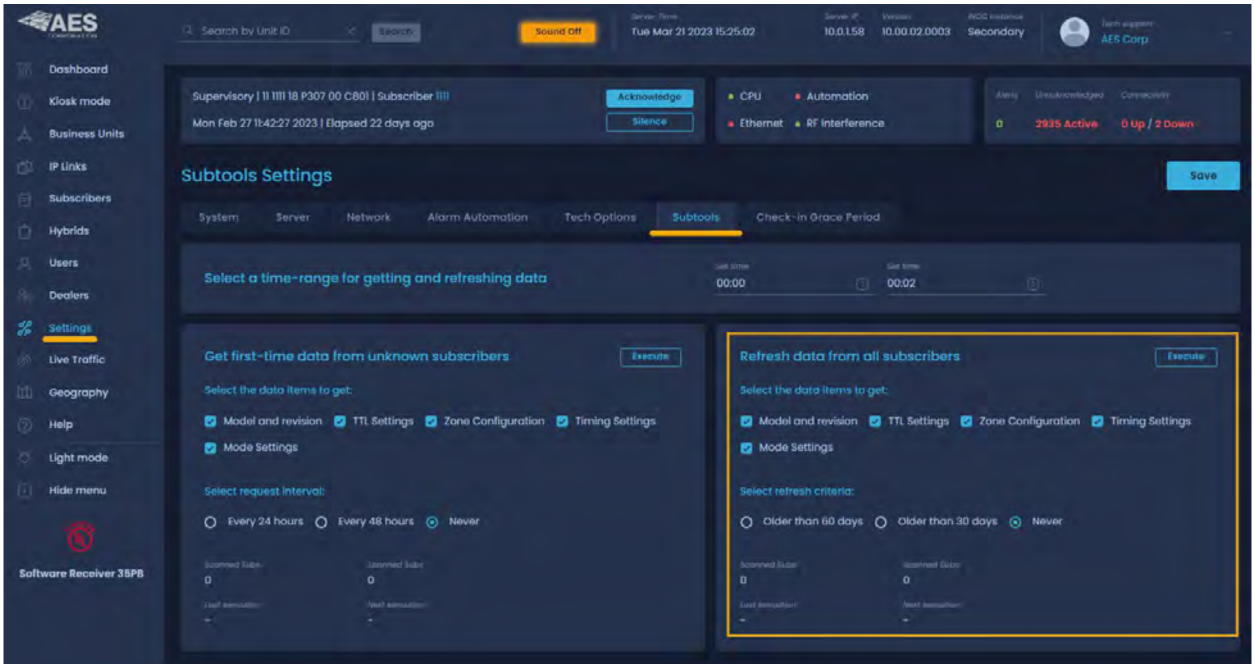
Refresh data from all subscribers

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.



Tue Mar 21 2023 15:25:02 | 10.0.1.58 | 10.00.02.0003 | Secondary | AES Corp

Supervisory | 11 1111 18 P307 00 C801 | Subscriber 1111
Mon Feb 27 11:42:27 2023 | Elapsed 22 days ago

CPU · Automation · Ethernet · RF Interference

0 | 2935 Active | 0 Up / 2 Down

Subtools Settings

Select a time-range for getting and refreshing data: 00:00 – 00:02

Get first-time data from unknown subscribers

Select the data items to get:
☑ Model and revision ☑ TTL Settings ☑ Zone Configuration ☑ Timing Settings
☑ Mode Settings

Select request interval:
○ Every 24 hours ○ Every 48 hours ◉ Never

Scanned Subs: 0 | Scanned Subs: 0
Last execution: - | Next execution: -

Refresh data from all subscribers

Select the data items to get:
☑ Model and revision ☑ TTL Settings ☑ Zone Configuration ☑ Timing Settings
☑ Mode Settings

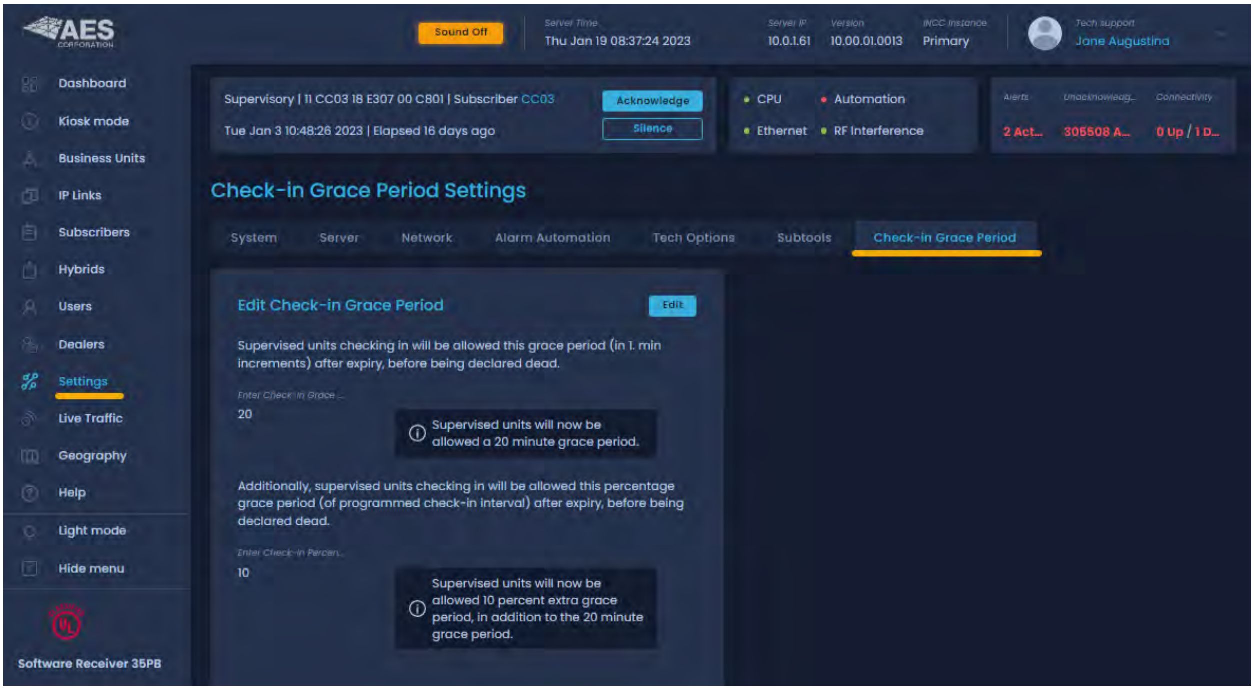
Select refresh criteria:
○ Older than 60 days ○ Older than 30 days ◉ Never

Scanned Subs: 0 | Scanned Subs: 0
Last execution: - | Next execution: -

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.



Server Time: Thu Jan 19 08:37:24 2023 | Server IP: 10.0.1.61 | Version: 10.00.01.0013 | INCC Instance: Primary | Tech support: Jane Augustina

Supervisory | 11 CC03 18 E307 00 C801 | Subscriber CC03

Tue Jan 3 10:48:26 2023 | Elapsed 16 days ago

● CPU ● Automation ● Ethernet ● RF Interference

Alerts: 2 Act... | Unacknowledg...: 305508 A... | Connectivity: 0 Up / 1 D...

Check-in Grace Period Settings

Edit Check-in Grace Period

Supervised units checking in will be allowed this grace period (in 1. min increments) after expiry, before being declared dead.

Enter Check-in Grace ...: 20

ⓘ Supervised units will now be allowed a 20 minute grace period.

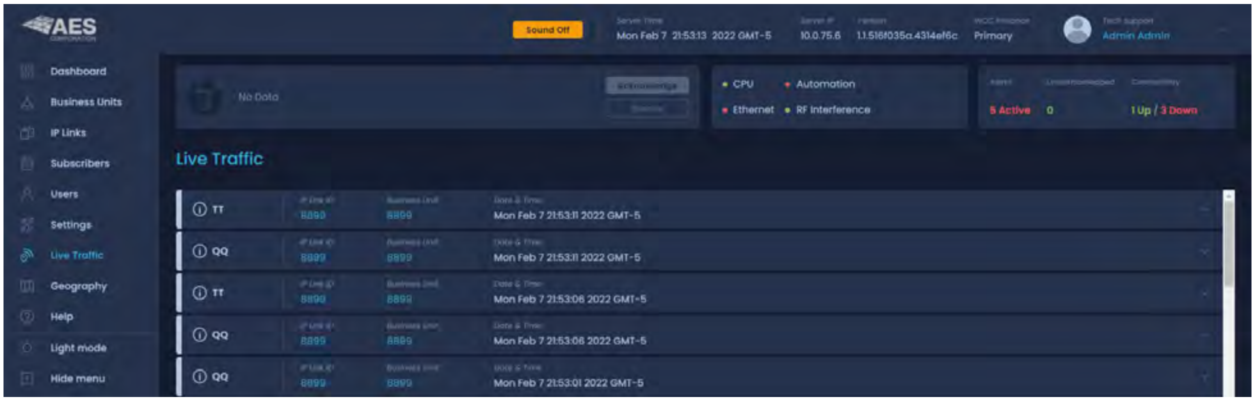
Additionally, supervised units checking in will be allowed this percentage grace period (of programmed check-in interval) after expiry, before being declared dead.

Enter Check-in Percen...: 10

ⓘ Supervised units will now be allowed 10 percent extra grace period, in addition to the 20 minute grace period.

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.



Server Time: Mon Feb 7 21:53:13 2022 GMT-5 | Server IP: 10.0.75.6 | Version: 1.1.516f035a.4314ef6c | INCC Instance: Primary | Tech support: Admin Admin

No Data

● CPU ● Automation ● Ethernet ● RF Interference

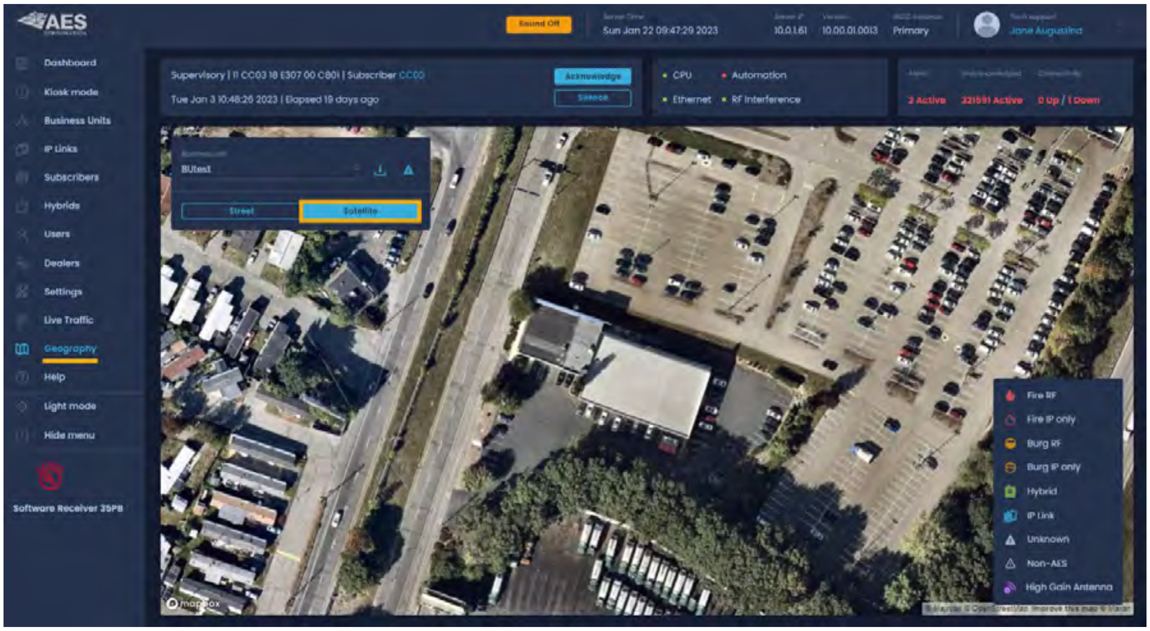
Alert: 5 Active | Unacknowledged: 0 | Connectivity: 1 Up / 3 Down

Live Traffic

	IP Link ID	Business Unit	Date & Time
ⓘ TT	8890	8899	Mon Feb 7 21:53:11 2022 GMT-5
ⓘ QQ	8899	8899	Mon Feb 7 21:53:11 2022 GMT-5
ⓘ TT	8890	8899	Mon Feb 7 21:53:06 2022 GMT-5
ⓘ QQ	8899	8899	Mon Feb 7 21:53:06 2022 GMT-5
ⓘ QQ	8899	8899	Mon Feb 7 21:53:01 2022 GMT-5

Geography

The **Geography** tab has the option for Earth or satellite view.



Server Time: Sun Jan 22 09:47:29 2023
Server IP: 10.0.1.61
Version: 10.00.01.0013
INCC Instance: Primary
Tech support: Jane Augustina

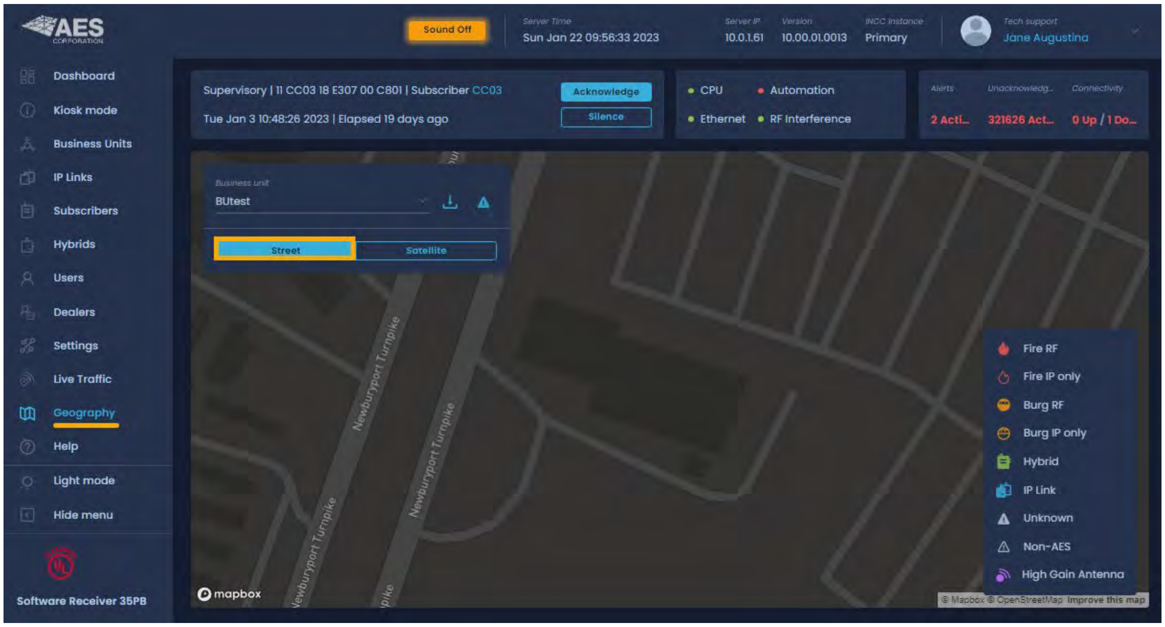
Supervisory | 11 CC03 18 E307 00 C801 | Subscriber CC03
Tue Jan 3 10:48:26 2023 | Elapsed 19 days ago

● CPU ● Automation
● Ethernet ● RF Interference

Alerts: 2 Active
Unacknowledged: 321591 Active
Connectivity: 0 Up / 1 Down

Business unit: BUtest

The **Street** view enables you to view and navigate through 360 degree horizontal and 290 degree vertical panoramic street level images.



Server Time: Sun Jan 22 09:56:33 2023
Server IP: 10.0.1.61
Version: 10.00.01.0013
INCC Instance: Primary
Tech support: Jane Augustina

Supervisory | 11 CC03 18 E307 00 C801 | Subscriber CC03
Tue Jan 3 10:48:26 2023 | Elapsed 19 days ago

● CPU ● Automation
● Ethernet ● RF Interference

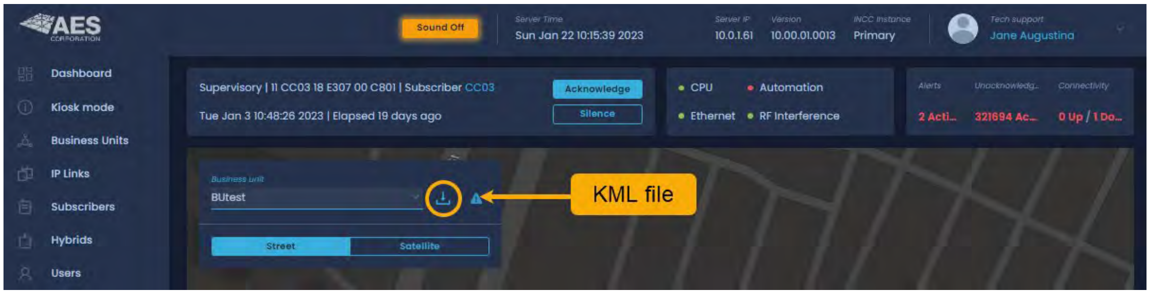
Alerts: 2 Acti...
Unacknowledg...: 321626 Act...
Connectivity: 0 Up / 1 Do...

Business unit: BUtest

Configuration

In order to view the Visualization feature of the INCC on Google Earth you have to first load the addresses of the Subscribers and IP Links (Step 1 below).

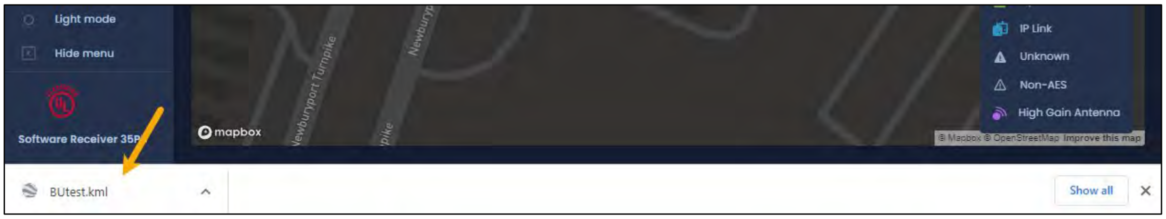
1. This step is done during migration process.
2. Click the download icon to download the .klm file with the Business Unit map information. (KML is a file format used to display geographic data in an Earth browser such as Google Earth.)



Supervisory | 11 CC03 18 E307 00 C801 | Subscriber CC03

Tue Jan 3 10:48:26 2023 | Elapsed 19 days ago

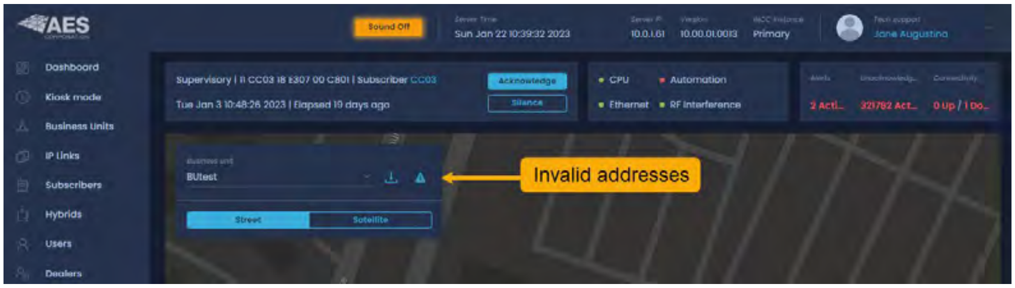
3. Click the business unit .klm file at the bottom left of the screen.



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 used for the *Operator Dashboard* password for that Business Unit.

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

   a. Invalid Addresses – Will list addresses that are not in correct format and need to be adjusted



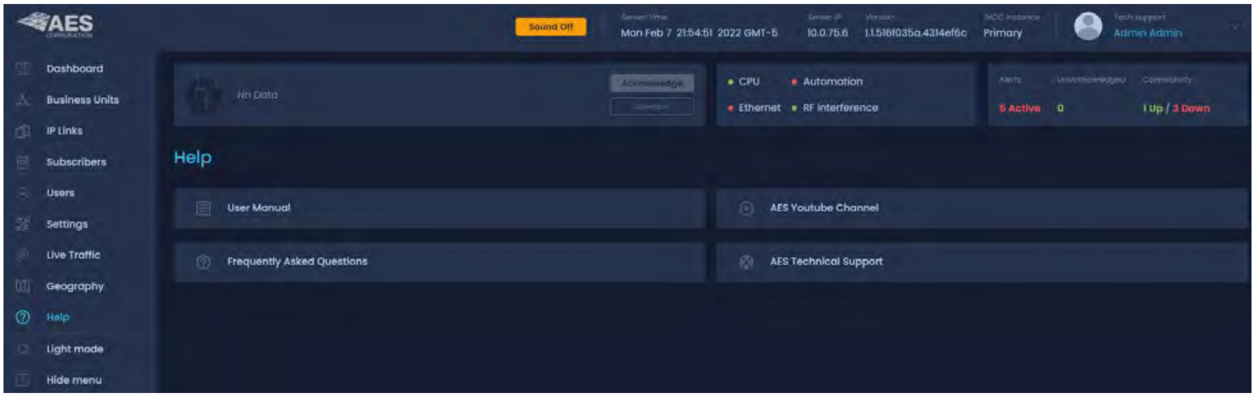
Supervisory | 11 CC03 18 E307 00 C801 | Subscriber CC03

Tue Jan 3 10:48:26 2023 | Elapsed 19 days ago

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.



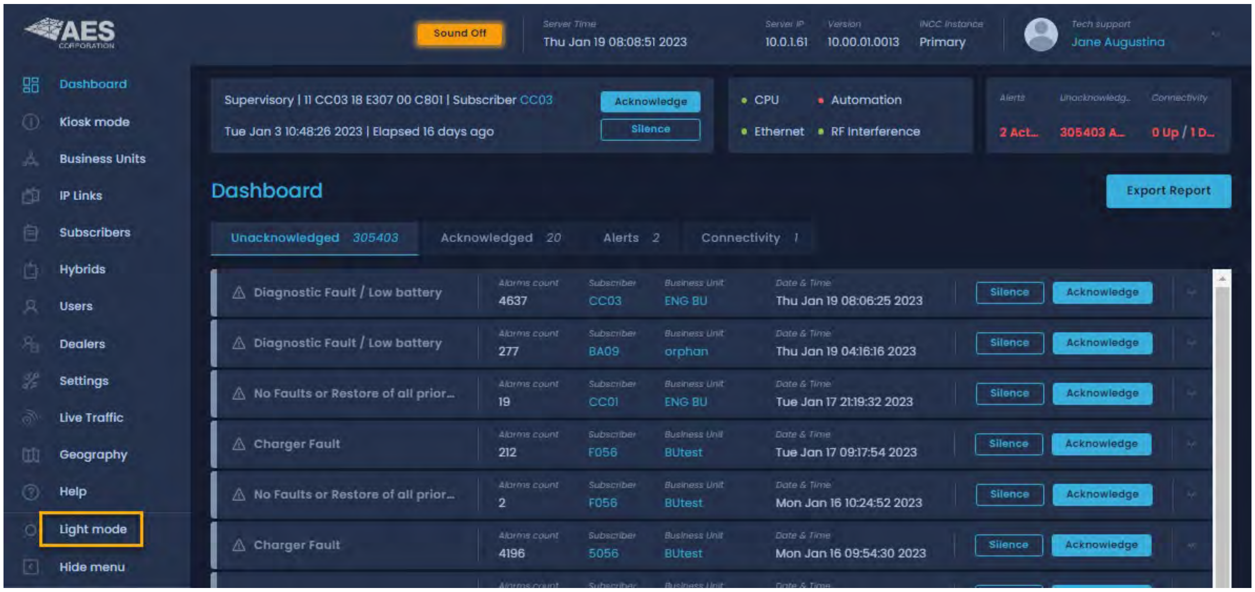
Server Time: Mon Feb 7 21:54:51 2022 GMT-5
Server IP: 10.0.75.6
Version: 1.1.516f035a.4314ef6c
INCC Instance: Primary
Tech support: Admin Admin

No Data

Alerts: 5 Active
Unacknowledged: 0
Connectivity: 1 Up / 3 Down

Light mode

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



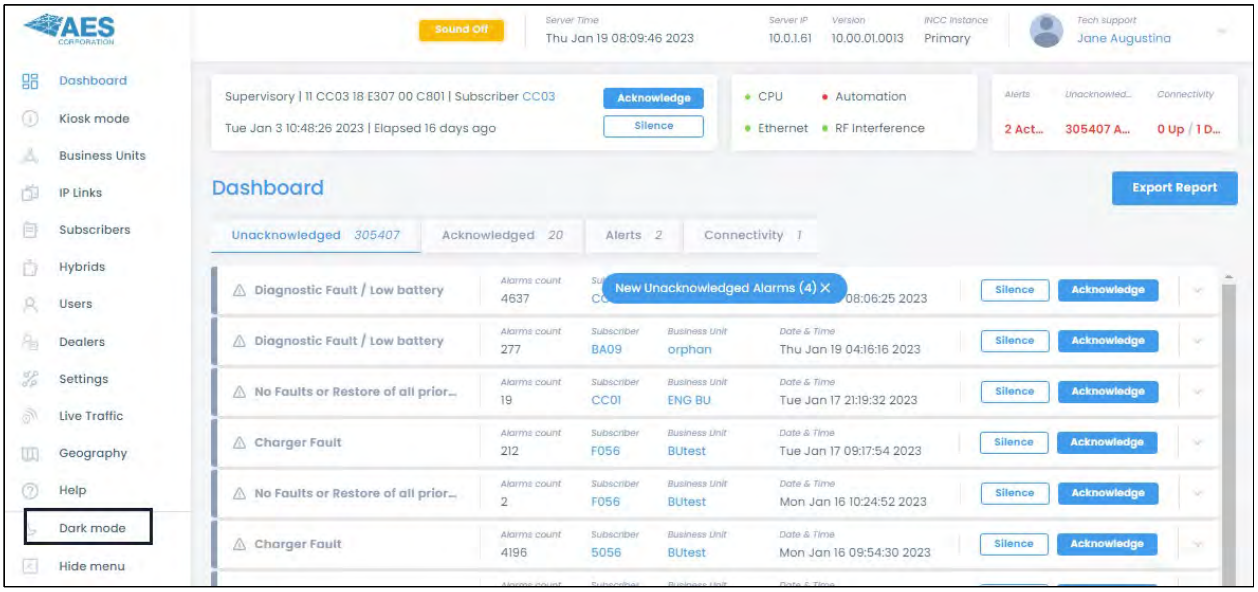
Server Time: Thu Jan 19 08:08:51 2023
Server IP: 10.0.1.61
Version: 10.00.01.0013
INCC Instance: Primary
Tech support: Jane Augustina

Supervisory | 11 CC03 18 E307 00 C801 | Subscriber CC03
Tue Jan 3 10:48:26 2023 | Elapsed 16 days ago

Alerts: 2 Act...
Unacknowledg...: 305403 A...
Connectivity: 0 Up / 1 D...

Unacknowledged 305403 | Acknowledged 20 | Alerts 2 | Connectivity 1

	Alarms count	Subscriber	Business Unit	Date & Time
Diagnostic Fault / Low battery	4637	CC03	ENG BU	Thu Jan 19 08:06:25 2023
Diagnostic Fault / Low battery	277	BA09	orphan	Thu Jan 19 04:16:16 2023
No Faults or Restore of all prior...	19	CC01	ENG BU	Tue Jan 17 21:19:32 2023
Charger Fault	212	F056	BUtest	Tue Jan 17 09:17:54 2023
No Faults or Restore of all prior...	2	F056	BUtest	Mon Jan 16 10:24:52 2023
Charger Fault	4196	5056	BUtest	Mon Jan 16 09:54:30 2023



Server Time Thu Jan 19 08:09:46 2023 | Server IP 10.0.1.61 | Version 10.00.01.0013 | INCC Instance Primary | Tech support Jane Augustina

Supervisory | 11 CC03 18 E307 00 C801 | Subscriber CC03
Tue Jan 3 10:48:26 2023 | Elapsed 16 days ago

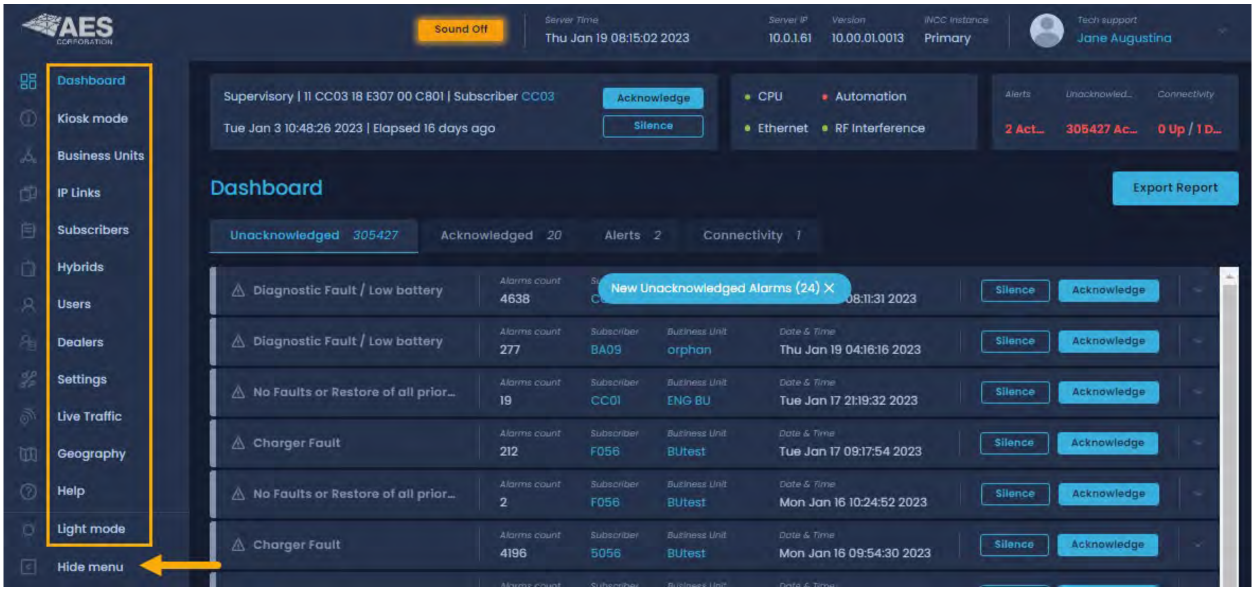
● CPU ● Automation ● Ethernet ● RF Interference

Alerts	Unacknowledged...	Connectivity
2 Act...	305407 A...	0 Up / 1 D...

	Alarms count	Subscriber	Business Unit	Date & Time
⚠ Diagnostic Fault / Low battery	4637	CC		08:06:25 2023
⚠ Diagnostic Fault / Low battery	277	BA09	orphan	Thu Jan 19 04:16:16 2023
⚠ No Faults or Restore of all prior...	19	CC01	ENG BU	Tue Jan 17 21:19:32 2023
⚠ Charger Fault	212	F056	BUtest	Tue Jan 17 09:17:54 2023
⚠ No Faults or Restore of all prior...	2	F056	BUtest	Mon Jan 16 10:24:52 2023
⚠ Charger Fault	4196	5056	BUtest	Mon Jan 16 09:54:30 2023

Hide menu

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



Server Time Thu Jan 19 08:15:02 2023 | Server IP 10.0.1.61 | Version 10.00.01.0013 | INCC Instance Primary | Tech support Jane Augustina

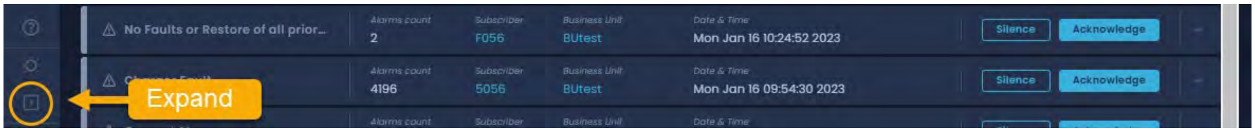
Supervisory | 11 CC03 18 E307 00 C801 | Subscriber CC03
Tue Jan 3 10:48:26 2023 | Elapsed 16 days ago

● CPU ● Automation ● Ethernet ● RF Interference

Alerts	Unacknowledged...	Connectivity
2 Act...	305427 Ac...	0 Up / 1 D...

	Alarms count	Subscriber	Business Unit	Date & Time
⚠ Diagnostic Fault / Low battery	4638	C		08:11:31 2023
⚠ Diagnostic Fault / Low battery	277	BA09	orphan	Thu Jan 19 04:16:16 2023
⚠ No Faults or Restore of all prior...	19	CC01	ENG BU	Tue Jan 17 21:19:32 2023
⚠ Charger Fault	212	F056	BUtest	Tue Jan 17 09:17:54 2023
⚠ No Faults or Restore of all prior...	2	F056	BUtest	Mon Jan 16 10:24:52 2023
⚠ Charger Fault	4196	5056	BUtest	Mon Jan 16 09:54:30 2023

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



	Alarms count	Subscriber	Business Unit	Date & Time
⚠ No Faults or Restore of all prior...	2	F056	BUtest	Mon Jan 16 10:24:52 2023
⚠	4196	5056	BUtest	Mon Jan 16 09:54:30 2023

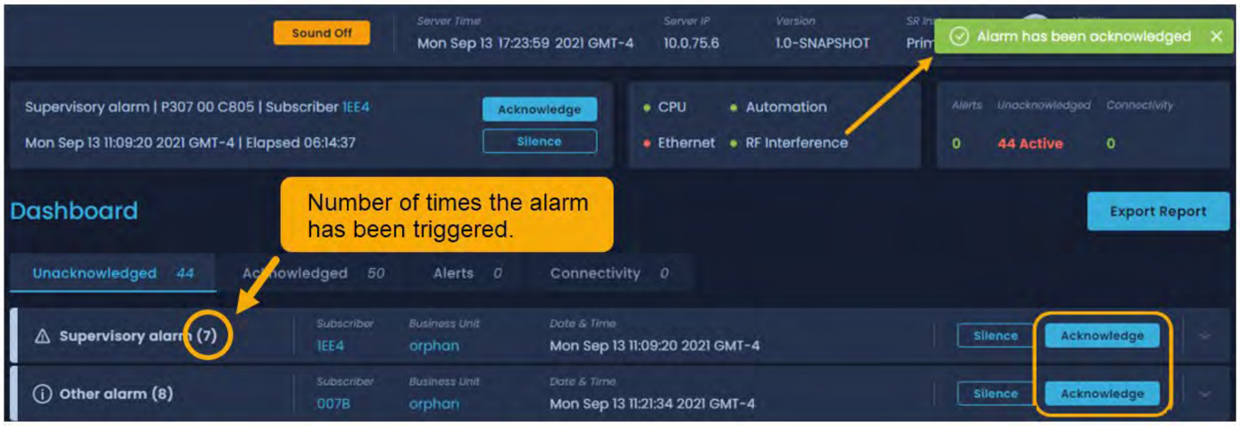
8. Processing Alarms

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.



Sound Off | Server Time Mon Sep 13 17:23:59 2021 GMT-4 | Server IP 10.0.75.6 | Version 1.0-SNAPSHOT | SR In Prim

Alarm has been acknowledged ✕

Supervisory alarm | P307 00 C805 | Subscriber 1EE4 — Acknowledge

Mon Sep 13 11:09:20 2021 GMT-4 | Elapsed 06:14:37 — Silence

● CPU ● Automation

● Ethernet ● RF Interference

Alerts	Unacknowledged	Connectivity
0	44 Active	0

Dashboard

Number of times the alarm has been triggered.

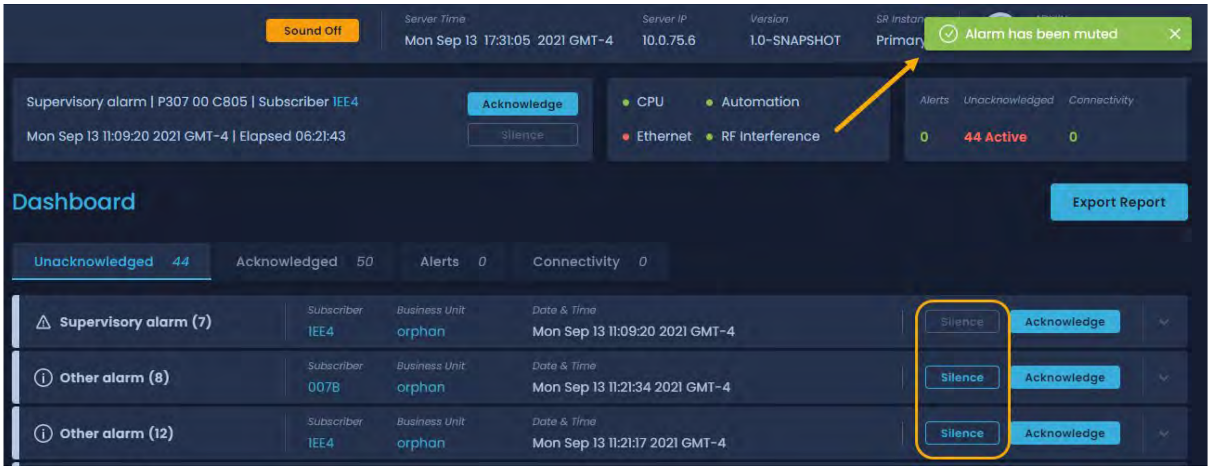
Export Report

Unacknowledged 44 | Acknowledged 50 | Alerts 0 | Connectivity 0

Alarm	Subscriber	Business Unit	Date & Time		
⚠ Supervisory alarm (7)	1EE4	orphan	Mon Sep 13 11:09:20 2021 GMT-4	Silence	Acknowledge
ⓘ Other alarm (8)	007B	orphan	Mon Sep 13 11:21:34 2021 GMT-4	Silence	Acknowledge

Silencing Alarms

To silence an alarm, click the **Silence** button. Once an alarm has been silenced, a green pop-up displays “Alarm has been muted” as confirmation.



Sound Off | Server Time Mon Sep 13 17:31:05 2021 GMT-4 | Server IP 10.0.75.6 | Version 1.0-SNAPSHOT | SR Instan Primary

Alarm has been muted ✕

Supervisory alarm | P307 00 C805 | Subscriber 1EE4 — Acknowledge

Mon Sep 13 11:09:20 2021 GMT-4 | Elapsed 06:21:43 — Silence

● CPU ● Automation

● Ethernet ● RF Interference

Alerts	Unacknowledged	Connectivity
0	44 Active	0

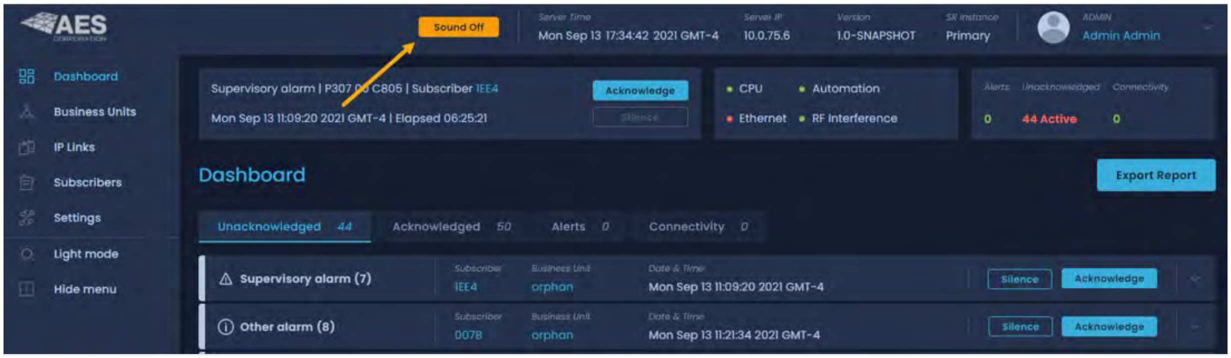
Dashboard

Export Report

Unacknowledged 44 | Acknowledged 50 | Alerts 0 | Connectivity 0

Alarm	Subscriber	Business Unit	Date & Time		
⚠ Supervisory alarm (7)	1EE4	orphan	Mon Sep 13 11:09:20 2021 GMT-4	Silence	Acknowledge
ⓘ Other alarm (8)	007B	orphan	Mon Sep 13 11:21:34 2021 GMT-4	Silence	Acknowledge
ⓘ Other alarm (12)	1EE4	orphan	Mon Sep 13 11:21:17 2021 GMT-4	Silence	Acknowledge

To silence all alarms, click the **Sound Off** button at the top of the screen. The button is replaced with a new button: **Sound On**.



Server Time: Mon Sep 13 17:34:42 2021 GMT-4 | Server IP: 10.0.75.6 | Version: 1.0-SNAPSHOT | SR Instance: Primary | ADMIN: Admin Admin

Supervisory alarm | P307 00 C805 | Subscriber IEE4
Mon Sep 13 11:09:20 2021 GMT-4 | Elapsed 06:25:21

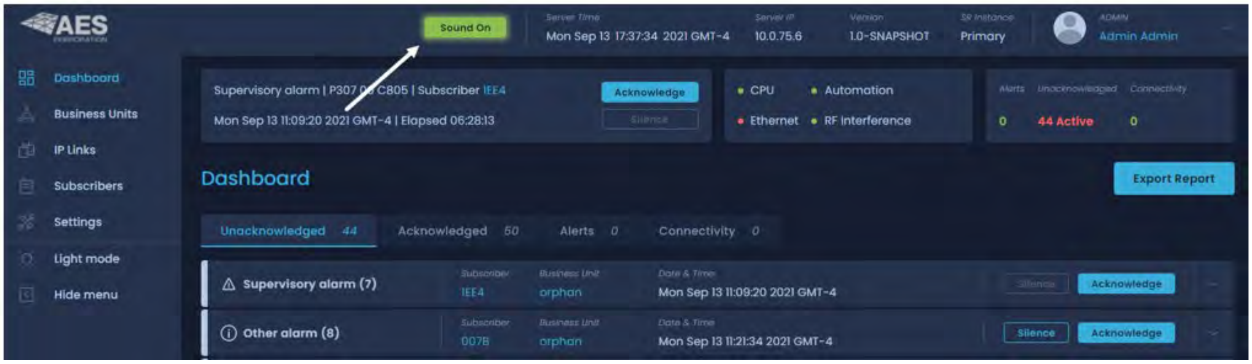
● CPU ● Automation ● Ethernet ● RF Interference

Alerts 0 | Unacknowledged 44 Active | Connectivity 0

Dashboard

	Subscriber	Business Unit	Date & Time
Supervisory alarm (7)	IEE4	orphan	Mon Sep 13 11:09:20 2021 GMT-4
Other alarm (8)	0078	orphan	Mon Sep 13 11:21:34 2021 GMT-4

To re-activate the sound, click the **Sound On** button.



Server Time: Mon Sep 13 17:37:34 2021 GMT-4 | Server IP: 10.0.75.6 | Version: 1.0-SNAPSHOT | SR Instance: Primary | ADMIN: Admin Admin

Supervisory alarm | P307 00 C805 | Subscriber IEE4
Mon Sep 13 11:09:20 2021 GMT-4 | Elapsed 06:28:13

● CPU ● Automation ● Ethernet ● RF Interference

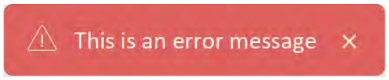
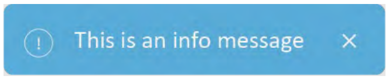
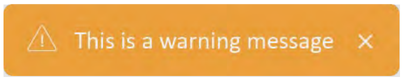
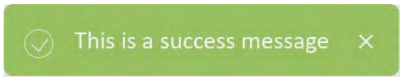
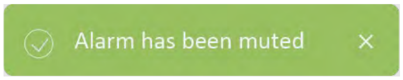
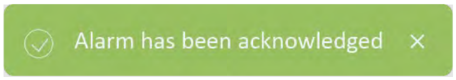
Alerts 0 | Unacknowledged 44 Active | Connectivity 0

Dashboard

	Subscriber	Business Unit	Date & Time
Supervisory alarm (7)	IEE4	orphan	Mon Sep 13 11:09:20 2021 GMT-4
Other alarm (8)	0078	orphan	Mon Sep 13 11:21:34 2021 GMT-4

Onscreen Messages

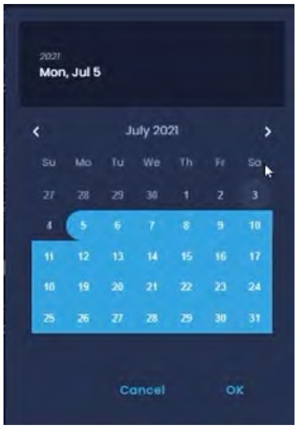
While using the INCC application, the following messages may be displayed. These messages will help you understand the software operating status and the actions you can take.

 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.

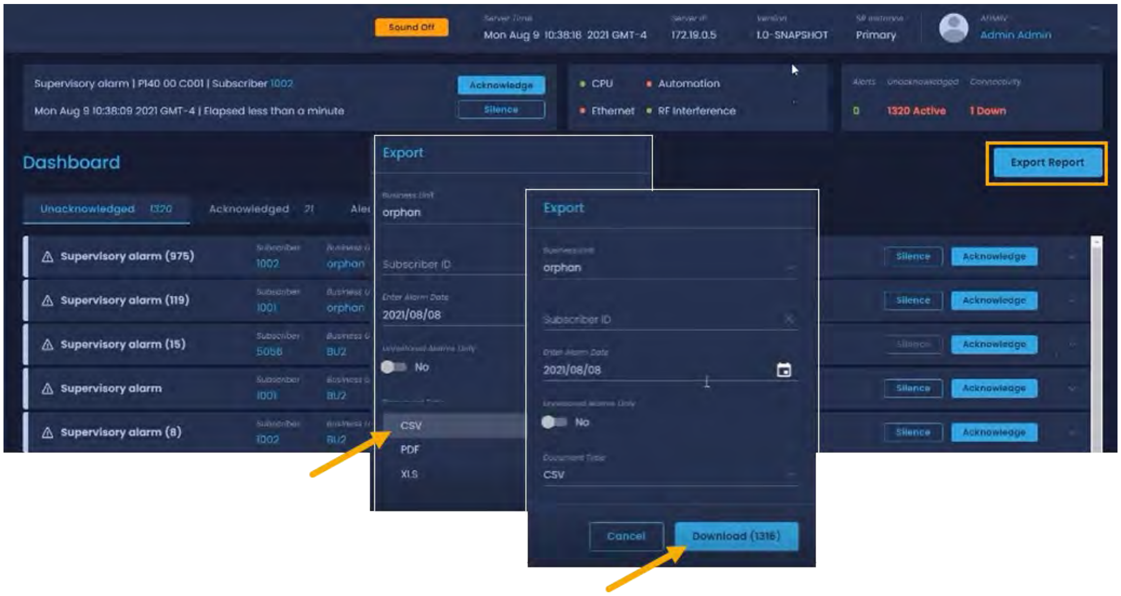
Exporting Reports

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.


Server Time: Mon Aug 9 10:38:18 2021 GMT-4
Server IP: 172.19.0.5
Version: 1.0-SNAPSHOT
SR instance: Primary
Admin Admin

Supervisory alarm | P140 00 C001 | Subscriber 1002
Mon Aug 9 10:38:09 2021 GMT-4 | Elapsed less than a minute

Alerts: 0 Unacknowledged: 1320 Active Connectivity: 1 Down

Export
Business Unit: orphan
Subscriber ID
Enter Alarm Date: 2021/08/08
Unresolved Alarms Only: No
Document Type: CSV

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 displayed on the Alerts tab of Dashboard.
BU Statistics	Analysis tools under a particular business unit: • Total Signals Received • Subscribers over time • IP Link and Hybrid Subscriber Load
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 Net-Con	NetCon is a measurement calculated by a subscriber to determine the level of confidence that its transmissions will reach an IP Link. Only fire

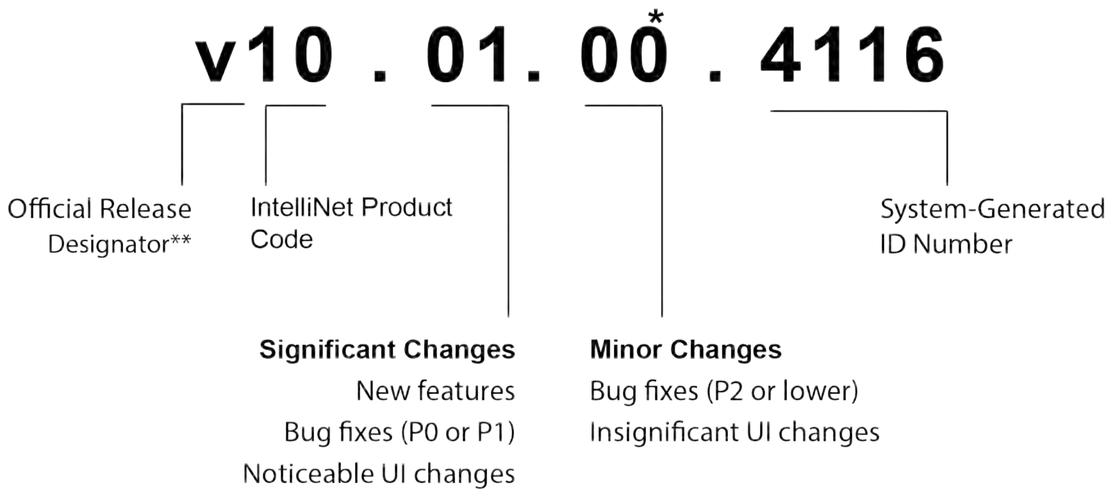
Name	Definition
	subscribers report their NetCon statuses, as either high or low, in messages sent to the INCC/MultiNet receiver. In general, NetCon is an abbreviation for Network Connectivity. It is a rating of the number of radio frequency (RF) paths from a subscriber to other subscribers installed 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.