SAFE-COM Wireless

Public Safety Distributed Antenna System

Product Line Series
SAFE-1050

Class A Bidirectional Amplifier (passive)

and Class A Fiber DAS (active)

User Manual

Safe-Com Wireless
Holmdel, NJ 07733
www.safe-comwireless.com

WARNING. This is NOT a CONSUMER device. It is designed for installation by FCC LICENSEES and QUALIFIED INSTALLERS. You MUST have an FCC LICENSE or express consent of an FCC Licensee to operate this device. You MUST register Class A signal boosters (as defined in 47 CFR 90.219) online at
"http://www.fcc.gov/signal-boosters/registration" www.fcc.gov/signal-boosters/ registration.
Unauthorized use may result in significant forfeiture penalties, including penalties in excess of $100,000 for each continuing violation."

WARNING. This is NOT a CONSUMER device. It is designed for installation by FCC LICENSEES and QUALIFIED INSTALLERS.
You MUST have an FCC LICENSE or express consent of an FCC Licensee to operate this device.
Unauthorized use may result in significant forfeiture penalties, including penalties in excess of $100,000 for each continuing violation."

This device complies with part 15 of the FCC Rules.
Operation is subject to the following two conditions:
1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interference that may cause undesired operation.

Liability Disclaimer

The information contained in this document is assumed to be correct and current. The manufacturer is not responsible for errors or omissions and reserves the right to change specifications at any time without notice. Safe-Com Wireless assumes no responsibility for its use nor for any indirect, incidental damage or loss resulting from its use.

Under Industry Canada regulations, this radio frequency power amplifier may only be used with the transmitter with which the amplifier has been certified by Industry Canada. The certification number for the transmitter with which this amplifier is permitted to operate is IC:22303

Conformément à la réglementation d'Industrie Canada, le présent amplificateur de puissance radiofréquence peut être utilisé seulement avec un émetteur avec lequel il a été certifié par Industrie Canada. Le numéro d'identification d'Industrie Canada pour l'émetteur avec lequel l'amplificateur est autorisé à fonctionner est IC : 22303

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that necessary for successful communication.

Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peut fonctionner avec une antenne d'un type et d'un gain maximal (ou inférieur) approuvé pour l'émetteur par Industrie Canada. Dans le but de réduire les risques de brouillage radioélectrique à l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que la puissance isotrope rayonnée équivalente (p.i.r.e.) ne dépasse pas l'intensité nécessaire à l'établissement d'une communication satisfaisante.

This radio transmitter (identify the device by certification number, or model number if Category II) has been approved by Industry Canada to operate with the antenna types listed below with the maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

Le présent émetteur radio (identify the device by certification number, or model number if Category II) a été approuvé par Industrie Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal et l'impédance requise pour chaque type d'antenne. Les types d'antenne non inclus dans cette liste, ou dont le gain est supérieur au gain maximal indiqué, sont strictement interdits pour l'exploitation de l'émetteur.

Table of Contents

Introduction…… 5

Overview, Start-up, …….. 9

System Overview & Block Diagram…… 11

Theory of Operation Block Diagram…… 13

Specifications, Maximum RF Input …… 15

BDA and Front Panel…… 18
- Overview
- DC Power and Alarm Input
- Alarm Outputs
- LED Indicators
-

Card System…… 22

Network Management System
- Loading the software…….. 23
- Configuration…….. 24
- Overview…….. 25
- Fiber DAS …… 22, 26
- NMS Main Page Display …… 27
- Controls: Frequency…….. 30
- Controls: Setup – Alarm outputs…… 32, 33
- VSWR (testing for antenna monitor)…….. 32
- Controls: Configure – Attenuators…… 34
- Control: Squelch…… …… 35

Battery Installation, Maintenance and Testing…… 36
Installation /Wall Mounting……. 39

Introduction

Safe-Coms DASAssure™ SAFE-1050 is a CLASS A or CLASS B patent-pending Public Safety Bidirectional Amplifier (Booster) and Fiber Optic Distributed Antenna System utilizing an advanced architecture that addresses the challenges of designing, deploying and maintaining a Public Safety BDA over its life-time. This innovative approach utilizes channel and sub-band processing that assures the lowest noise and spurious interference to radio communications coverage enhancement available. The unique architecture allows band expansion on ANY frequency adding only the power and resources required. Yet the design is the most compact BDA available – Integrating for the first time a Class A BDA with a Lithium back-up battery system inside a 19 x 18 x 7 inch NEMA4 enclosure.

FCC certified and UL2524 listed, the SAFE-1050 is the most advanced ERCES coverage enhancement system available.

Safe-Com's high-quality manufacturing system and superior applications support assures your success and the public's safety.

FCC Antenna Requirements

The user must assure that the installation meets FCC RF exposure limits. Minimum distance between any person and the operating antenna must be 23 inches or 56 cm. The antenna must be mounted on a stable, permanent structure.

Maximum ERP is 5 watts per FCC regulations per rule part 90.219(e)(1). The FCC licensed and qualified installer user must calculate the total transmitted power, taking into account the losses of the cables and splitters etc, plus the gain of the antenna to assure compliance with the maximum exposure regulation.

Lightening protection is required on all antennas as loss or damage as a result of lightening is not covered by the warranty. Antennas must be connected prior to turning up power to the unit.

Frequency Bands of Operation and RF output power control

The authorized bands of use for the SAFE-1050 Series product line include:

700 MHz Band: Uplink 763-775 & Downlink 799-805 MHz
800 MHz Band : Uplink 806-816 & Downlink 851-861 MHz

The channelizer cards and the user control via the Network Management System (NMS) determine the frequency transmitted. The manufacturer factory-sets the general operating bands for each plug-in card. Each card can accommodate frequencies only within their designated band which is delineated in this user manual and further in the Graphical User Interface (GUI) of the web-based NMS. The operating bands can not be modified by the user, only the channelized frequency operating within the band can be added, deleted and set. Consult the manufacturers data sheet and this operating manual to confirm proper operation. RF Output is controlled automatically by an ALC (automatic level control) circuitry within the cards. The user can not set the output power to exceed the FCC limits. The user can set the output power lower than the designed maximum using the webNMS interface integrated into the unit.

An integrated software defined radio module offers a selection of Class A filters. Up to 68 filters are available when two Digital Filter Array (DFA) modules are installed at the factory.

Note: Only factory trained and certified systems integrators are authorized to configure and manage the SAFE-1050 Booster.

Startup - Power

The SAFE-1050 series products operate on 120 VAC 60 Hz.
An internal AC to DC power supply is installed within booster to provide power when AC is available.

Power sources which can be specified include:

- 120 VAC (2 amps max)

Connect the system to the appropriate power source (120VAC).
An AC power source requires 3 connections: Line, Neutral and Ground.
Earth grounding the NEMA case is required. This is done through the terminal strip provided in the unit.
Follow all local electrical codes and the NEC (National Electrical Code).

Power consumption is directly related to the number of channels or bands and therefore the number of plug-in cards integrated in the system. Safe-Com applications engineering can provide the exact power consumption of your unit especially related to the backup battery requirements – whether they are 12 or 24 hours. The Safe-Com Series 1050 has very low power consumption. Typical values range from 40 to 65 watts for a single BDA unit.

The SAFE-1050 series modular card system has a dedicated card per band or frequency (in the case of Class A). This is important to know as the power consumption depends on how many channels are implemented and how many are keyed up. When a channel is not keyed up, its internal power control circuitry reduces its power consumption to the minimum level.

There are a number of ways to estimate the power consumption over 12 of 24 hours and that depends on what assumption one makes of the key up time; i.e. how many channels key up and for how long. The estimate Safe-Com provides is based on a 50% duty cycle. This means that the power consumption is calculated assuming the half the channels are in use continuously for the 12 or 24 hours period. This is a conservative estimate. Consult with Safe-Com Wireless applications engineering for exact values.

The NEMA4 Unit case is grounded to the electrical ground terminals internally. The user must assure that the earth ground connection at the terminal strip or the grounding lug on the outside of the NEMA is properly connected to the external earth ground.

Model Numbers

SAFE-1050 : 700 & 800 MHz BAND BDA, CLASS A

SAFE-AN-1002 : REMOTE ANNUNCIATOR (SEE SEPARATE DATA SHEET)

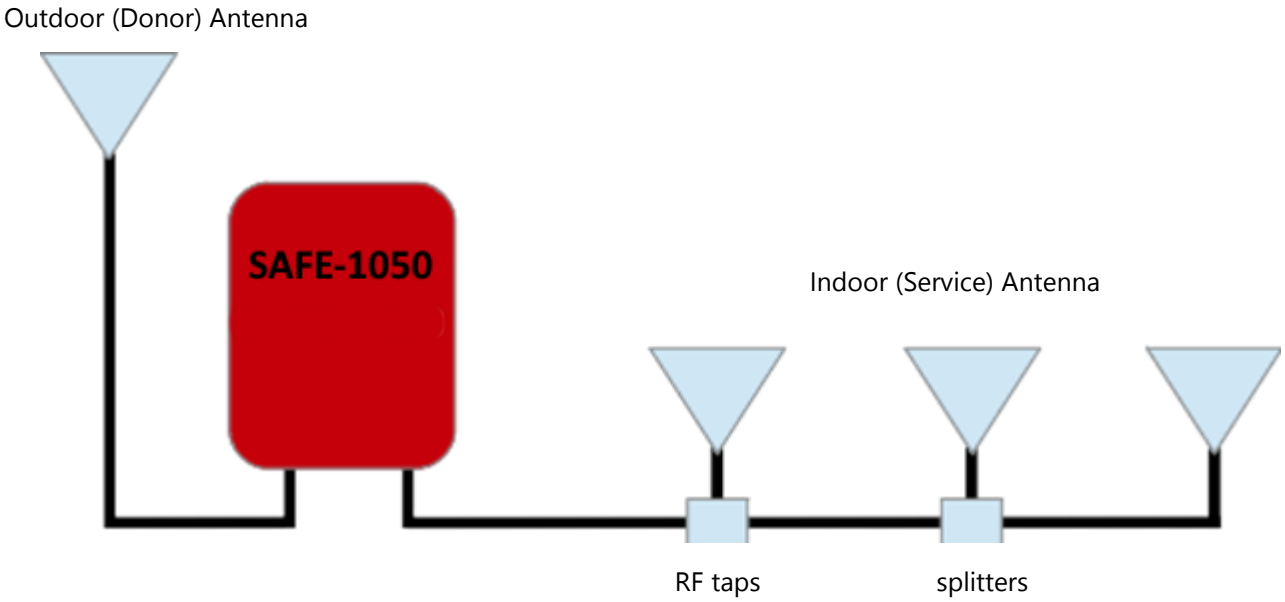
Options:

a. 700 MHz only
b. 800 MHz only
c. 32 digital filters
d. 64 digital filters
e. Single Service port
f. Dual service port (Each port is bidirectional and carries all the bands)

For the base model, the single-pack battery will provide up to 24hours battery back-up. Some options above may require a second battery pack to cover 24 hour requirements. Consult the sales department.

System Application Overview

Bidirectional Amplifier: Model 1050



An indoor coverage plan is implemented using RF coaxial cable, RF taps (couplers) of various proportions and splitters with antennas suited for the 700 and 800 MHz bands.

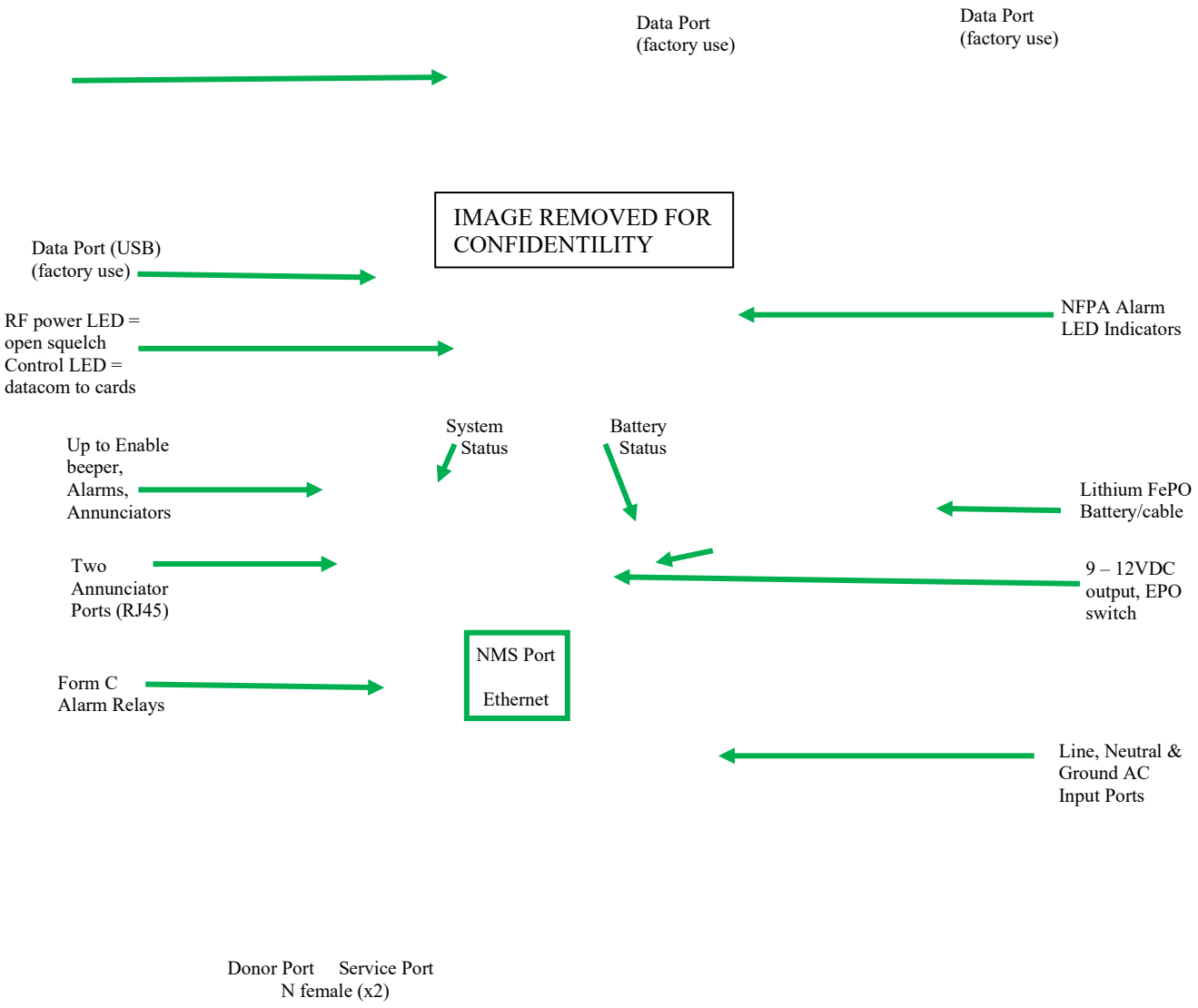
Theory of Operation

1. An antenna receives the signal off-air and it is passed through a pre-selector filter and low-noise amplifier.
2. The pre-selector filter limits the downlink pass-band to 769-775MHz bandwidth (for 700 MHZ systems) and 851-861MHz bandwidth (for 800 MHZ systems).
3. The low noise amplifier boosts the incoming preselected frequencies.
4. The downlink signal then passes into several linear gain stages in the “channel card” prior to a mixer stage tat translates the RF frequency to a lower intermediate frequency - typically below 60MHz.
5. AGC is deployed in this front-end receiver to assure the down conversion mixer operates in its liner region under all input RF levels.
6. The IF signal then passes through the digital filter array (DFA) which is a software defined radio. The DFA digitally can be set to configure multiple filters with bandwidths between 12 to 75kHz (Class A) and 100 to 1000MHz (Class B) frequencies signal.
7. Each filter can be individually set for Gain, Squelch level, bandwidth and maximum output level.
8. After conditioning with the DFA the signal is routed back to the “channel card” and is up-converted back to its original frequency (in the 700MHz or 800MHz bands).
9. A power amplifier located at the output of the channel card boosts the signal to the desired level.
10. The same process works in the reverse (uplink) direction.

Block Diagram (simplified)

IMAGE REMOVED FOR CONFIDENTILITY

SAFE-1050 Bidirectional Amplifier



Booster SPECIFICATIONS:

Power / Mechanical	
System Configuration	Single band: 700 MHz Single band: 800 MHz Dual band: 700/800 MHz
Power supply	120 VAC
Power consumption*	50 watts average
Output power per band*	700 MHz: 29 dBm 800 MHz: 29 dBm 700 & 800 MHz: 32 dBm
Backup duration	12 or 24 hours
Channel card input frequency range	700 Uplink: 799 to 805 MHz 700 Downlink: 769 to 775 MHz 800 Uplink: 806 to 816 MHz 800 Downlink: 851 to 861 MHz
Certifications	UL 2524 FCC ID: Pending
Associated products	Remote Alarm Annunciator: SAFE-AN-1002
Alarms	6 NFPA alarms plus an oscillation alarm, an alarm to indicate a lost data connection to the remote annunciator, and a door alarm

Additional Operating Features	
Class A and Class B filter latency	12.5 kHz: 60 µs 25 kHz: 35 µs 50 kHz: 25 µs 75 kHz: 15 µs 200 kHz: 10 µs 500 kHz: 8 µs
RF input **RF output***	0 dBm (max, no damage) 1 watt (2 watts with dual band)
Noise figure*	6 dB (typical)
Gain control **Gain range**	30 dB (+/- 1 dB steps) 80 dB standard (90 dB optional)
Squelch range	-85 to -50 dBm
AGC range	60 dB
Operating temperature	14 to 122°F (-10 to 50°C)
Size	19 x 18 x 6.7 inches
Weight	50 lbs
Enclosure	NEMA 4

* RF output power, output power per band, noise figure and power consumption depends on configuration. Other sub-bands are available. FirstNet available as required. RF Power +/- 2dB, Consult Customer Service for applications and quotations support.

WARNING. This is NOT a CONSUMER device. It is designed for installation by FCC LICENSEES and QUALIFIED INSTALLERS. You MUST have an FCC LICENSE or express consent of an FCC Licensee to operate this device. You MUST register Class B signal boosters (as defined in 47 CFR 90.219) online at www.fcc.gov/signal-boosters/registration. Unauthorized use may result in significant forfeiture penalties, including penalties in excess of $100,000 for each continuing violation.

Battery Back-Up SPECIFICATIONS:

BBU Startup

1. Connect AC power to the BBU "AC power input" terminals with three wires: line, neutral and ground. Maximum power is 200 watts so choose conductor size appropriately. (See image to the right.)

2. After the AC connections are secured, install the provided terminal block cover over the exposed contacts. Secure the AC cable to the black cable mount in the center of the panel. Note: The BBU requires AC power to turn on initially.

3. With the BBU system power switch in the off position, connect the provided 8-pin power cable from the BBU 12V power output port to the BDA 12V DC input port.

4. First turn the BBU power switch on, then turn the BDA power switch on. Follow this sequence any time the BBU system power switch is turned on.

5. The BBU LED status indicators should be in state 1 upon initial power-up. See "Led Indicators" below.

IMAGE REMOVED FOR CONFIDENTILITY

LED Indicators

STATE	1	2	3	4	5	6	7	8	9
AC POWER									
BATTERY									
STATUS									

- *Grey Circle indicates LED off.*
- *White Dotted Circle indicates LED may flash red or green depending on current state when alarm occurred.*
- *Dashed Circle indicates flashing LED.*

State Descriptions

1. AC on, battery charging/balancing.
2. AC on, battery charged.
3. AC off, battery powered.
4. AC on, charger failure (not connected).
5. AC off, low battery voltage: (slow red/green flash).
6. External AUX alarm active.
7. External EPO engaged.
8. Battery over current.
9. Battery error: fast flashing (battery and status LEDs indicate blown fuse or cell out of range).

Alarm Testing

1. Low Battery Voltage Level Alarm

Disconnect the 4-wire cable jumper that runs between the battery and the front panel. This will trigger a low battery level alarm. Reconnect to clear the alarm. If two battery packs are installed, both must be disconnected to trigger the alarm. Always keep the two batteries at a similar charge level. If connected, both should be connected. If disconnected, both should be disconnected. If the two batteries are at a different charge level, you can experience a larger surge of current between the two batteries upon connecting them. This is undesirable and dangerous. It could damage the equipment.

2. Battery Charger Alarm

Press "TEST" button on front panel (located under the LEDs). This will trigger the battery charger fail alarm. Press again to reset alarm.

3. AC Power Alarm:

Disconnect AC power source. This will trigger the AC alarm. Reconnect AC power to reset alarm.

Other Alarms

4. Power AMP

To test amp alarm, press black push-button on amplifiers modules mounted to inside wall of BDA. Alarm will trigger. Press again to clear.

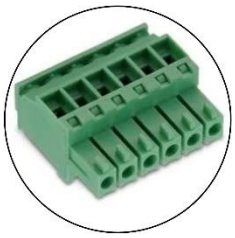
5. Antenna Monitor

Remove Donor antenna cable from Donor port. Alarm will trigger in 30 seconds (settable time-out). Replace cable with downlink signal present, alarm clears.

SAFE-1050 Series BDA and Fiber DAS

Relay Alarm Connector Pinouts – and NFPA Alarm TEST methods

The alarm output connector on the front panel of the BDA is comprised of 18 position (3 x 6) terminal blocks as shown. Insert an alarm wire and EOL resistor as required into one of three 6 pin plugs provided (as seen in the inset photo). Then using a small screwdriver tighten the wire into place. Each position accepts a wire size of 18 to 26 gauge with room for a EOL resistor.



Three plugs as shown here will be provided. Use them to connect alarm wire and end-of-line termination resistors for the fire panel. Once wired, press each plug into one of the jacks on the front panel shown below.

Each Alarm is a Form C Relay output.
The pinout provides 3 ports for each alarm:

- Normally Closed (NC)
- Common-
- Normally Open (NO)

Connect 2 wires to the Common and one of the other ports depending if the fire panel requires normally open or normally closed relay inputs. The pinout is as shown (left to right):

1-AC Loss NO
2-AC Loss Common
3-AC Loss NC
This requires an external alarm input into the 8 pin on front panel of BDA from external Safe-Com BBU

TEST: Disconnect AC Power
RESET: Reconnect AC Power

10-Power amp fail NO
11-Power amp Common
12-Power amp NC

TEST: Press black button on amplifier
RESET: Press again

16-BDA or System Alarm NO
17- BDA or System Alarm Common
18- BDA or System Alarm NC

This alarm triggers along with all other alarms. It can be used as a summary alarm.

IMAGE REMOVED FOR CONFIDENTILITY

4-Low Battery NO
5-Low Battery Common
6-Low Battery NC
This requires an external alarm input into the 8 pin on front panel of BDA from external Safe-Com BBU

TEST: Remove 4 wire battery cable from front panel in BBU.
RESET: Plug cable back into panel. Remove both cables if it's a 2 pack.

7-Battery Charger NO
8-Battery Common
9-Battery Charger NC
This requires an external alarm input into the 8 pin on front panel of BDA from external Safe-Com BBU

TEST: Press TEST button on BBU Panel (found under the LEDs)
RESET: Press TEST button again.

13-Donor Antenna Fail NO
14-Donor Antenna Common
15-Donor Antenna Fail NC

TEST: Disconnect Donor antenna. Wait timeout period.
RESET: Reconnect Donor, push reset on BDA or power cycle. Reset timeout period if required.

Note:
The BDA or System Alarm output relay is a catch-all summary alarm output that triggers along with any of the other alarm notifications. Therefore, it can be used as a single summary connection to the fire panel.
The “BDA or System” output relay is a catch-all alarm. It will trigger with the triggering of any of the other alarms.

Fiber DAS

Warning: Laser output from fiber ports.
Laser output from the green SC/APC connectors
Do not stare into fiber connectors or permanent eye damage may occur..
Class 3R Laser Diode

The fiber used is industry standard single mode fiber (9/125um)
The connectors used are industry standard SC/APC (typically green colored).
Maximum optical loss between Head-End and Remote is 5dB optical.

The Head-End unit polls the Remote units using a data channel operating on a subcarrier frequency of 915MHz. The system communicates over the fiber and the Remotes report their configuration and alarm data to the Head-End. The Head-end then annunciates these alarms via its NFPA Relay outputs and via the NMS software.

The Remotes also report their own alarms to the NFPA alarm outputs on its own Front Panel.

Network Management System Software

The Safe-Com Wireless (SCW) Web Network Management System (WNMS) interface provides an easy access portal to a remote BDA unit. Using a secure IP connection, full monitoring and control capabilities can be realized. Network management tools such as SNMP (Simple Network Monitoring Protocol) can be deployed along with Traps, if desired.

Connectivity can be provided by a direct, hard-wire connection to a router or via a Network Modem using 4G or 5G technology. Using a Network Modem will require a Static IP SIM card subscription, available from many carrier services (see addendum).

The WNMS server can utilize DDNS (Dynamic Domain Name System) to ensure reliable remote access or a static IP can also be used.
The entire system is configured using text-based configuration files. These files are stored locally on the DAS system but can be easily updated from a USB thumb drive.

QUICK START

An IP connection is required to login to WNMS. This can be a direct connection to a laptop Ethernet Port, Ethernet Router, Network Modem (5G for example), in all cases a static IP is programmed into the DAS control board. Contact your IT department for the required information

1. Switch off DAS system from IO panel switch
2. Require USB thumb drive formatted for Windows FAT32
3. Insert into computer USB connector and open file manager
4. Clink on New and select Folder
5. Name new folder DAS
6. Folder should appear in file manager, double click to enter folder
7. Clink on New and select Folder
8. Name New folder user
9. Folder should appear in file manager, double click to enter folder
10. Clink on New and select Text Document
11. When file appears in file manager, enter user
12. Double click the file to open it
13. Copy and paste the configuration lines shown in Table.1
14. Edit the IP and gateway IP addresses to suit your system
15. Save file, eject USB drive
16. Plug USB drive into the USB C connector on the DAS module
17. Turn ON the DAS system – this will automatically config the IP interface to the address specified in user.txt file
18. Open FireFox web browser and enter https://192.168.1.193
19. As this is the first connection you will receive a security warning, accept the risk as this is a known system. Never accept the risk if you do not know the system you are connecting to.
20. This will save the required SSL credentials
21. A login dialog box should now appear

Copy and paste these lines into \DAS\user\user.txt file and save file.

.name Welcome .iplocal 192.168.1.193 .netmask 255.255.255.0 .gateway

Table.1

Login Screen:

- Enter username: admin
- Enter password: scw@admin.

Fig.1

Note: Name/Location of system is that set in Admin dialog box
Home Page:

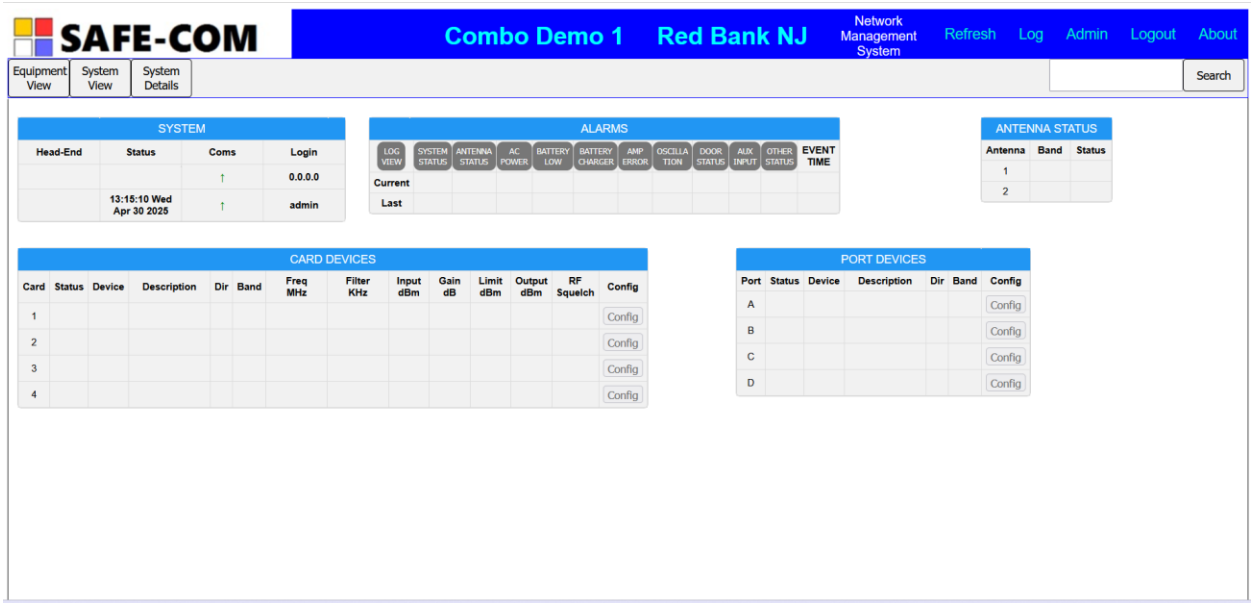


Fig.2

Note the following Dialog boxes can be moved to desired position by hovering over title line, left click, move and then release.

- **SYSTEM:**
  - Head-End Software Version
  - System voltage (AC/Battery)
  - Coms – rotating arrow to indicate connection between WNMS and System
  - Login – IP of remote and who

- **ALARMS:**
  - 1st Row shows active alarm condition(s):
    - RED = Alarm active
    - GREEN = Normal
    - EVENT TIME = time alarm occurred
  - 2nd Row shows past alarm condition(s):
    - RED = Alarm active
    - GREEN = Normal
    - EVENT TIME = time alarm went off
  - Hover mouse over Alarm Name to see history of Alarms.

- **CARD DEVICES:**
  - List of installed Cards 1 through 10

- **PORT DEVICES:**
  - List of installed Port connected boards A through J
- **ANTENNA STATUS:**
  - List of active Antenna's and status

Menu Options:

- **Refresh**
  - Restore dialog boxes to original/default positions.
  - Update all display parameters:
    - Note after 30 minutes the display will not auto-update.
    - Click Refresh to resume real-time updates.

- **About**
  - Contact information for Safe Com Wireless

- **Admin**
  - View/Edit Administration parameter.

- **Logout**
  - Exit WNMS and return to Login screen.

Admin:

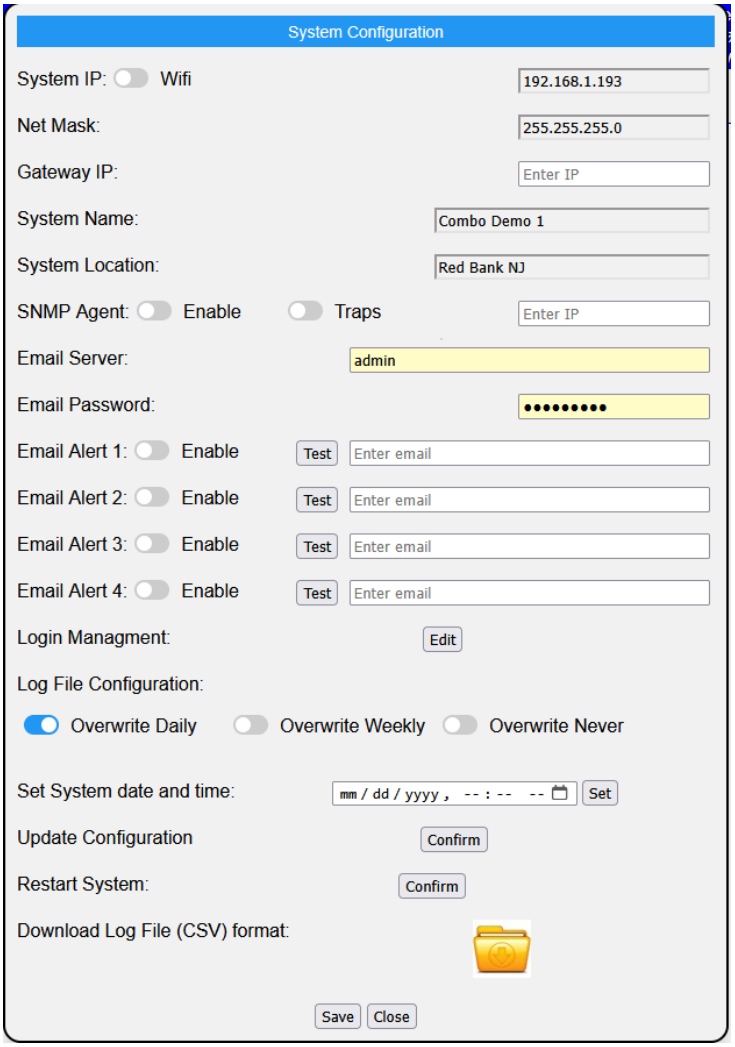


Fig.3

- **System IP:**
  - default 192.168.1.192
  - Enter required static IP – ethernet connection.
  - Wi-Fi mode (if accessible network available)

- **Net Mask:**
  - 255.155.255.0 (typical value)

- **Gateway IP:**
  - Leave blank if gateway not required
  - Include IP address if required

- **System Name:**
  - This will appear on WNMS title line and Login dialog box.
  - Included in email alerts.

- **System Location:**
    - This will appear on WNMS title line and Login dialog box.
    - Included in email alerts.

- **SNMP:**
    - Enter the IP address of SNMP server.
    - Check Enable to run SNMP Agent
    - Check Traps to enable alerts

- **Email Server:**
    - This is your email account name (myemail@mycompany.com)

- **Email Password:**
    - Password for your email account
    - Note, you will have to generate a unique password when using Yahoo/Google

- **Email Alert 1-4:**
    - Enable: click to enable email alert to this address
    - Enter a valid email address to receive Alarm Alert emails.

- **Login Management:**
    - Up to 10 logins can be configured
    - Click on required privileges for each login account

- **Log File Configuration:**
    - Log file over-write period selection.
    - Last log data will be archived, new/cleared log file will be created

- **Set System Time and Date:**
    - Network Time Protocol (NTP) required for auto-update
    - Use calendar/time fields to manually set time/date
    - Click Set to update

- **Update**
    - System can be updated via an external USB thumb drive

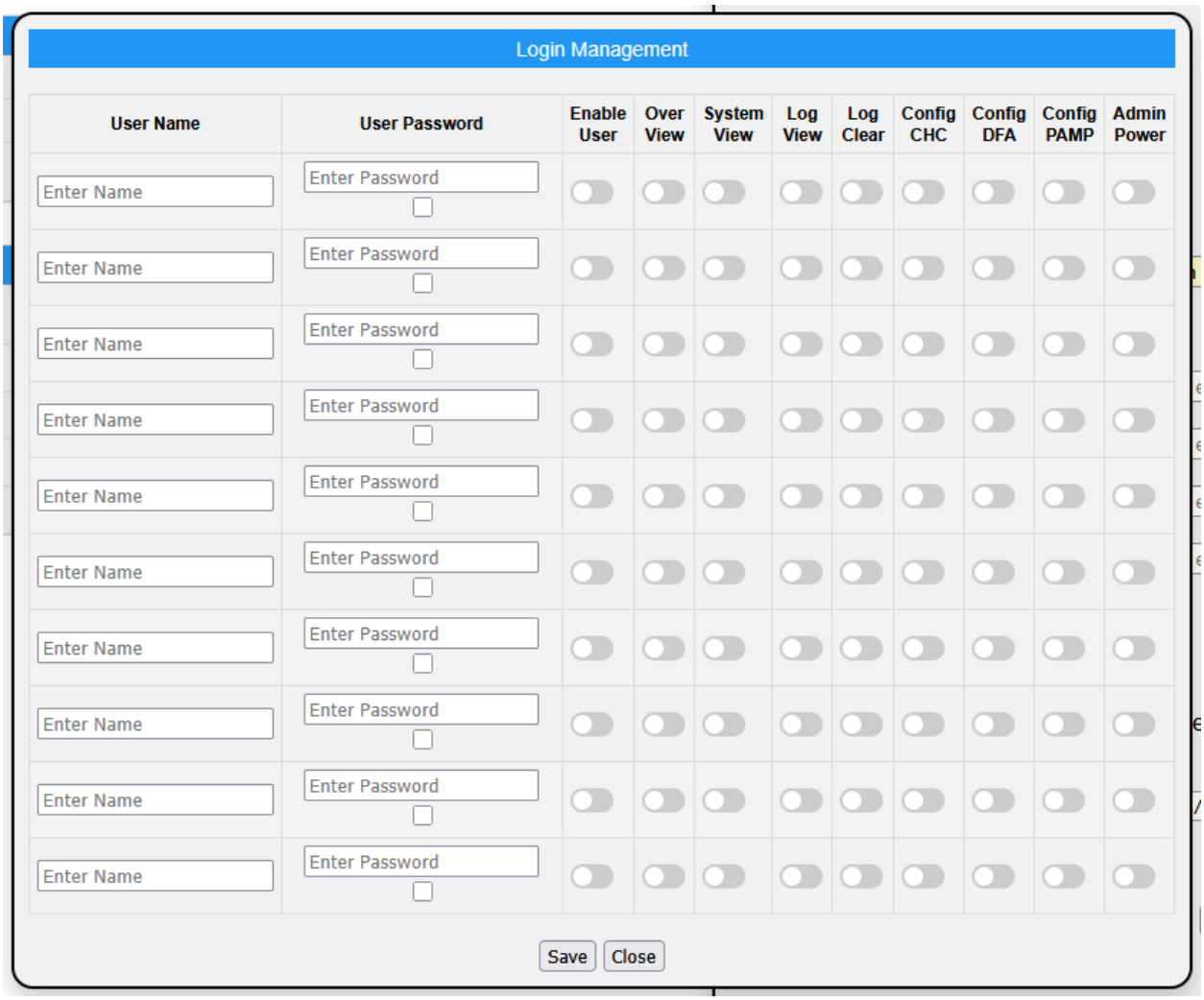
- **Restart:**
    - Reboot system. This will logout and close session

- **Download Log File:**
    - Click download folder icon
    - Files saved in download directory on local machine
    - CSV, comma delimited format.

- **Save:**
  - Click to update Admin database and take effect.

- **Close:**
  - Click to disregard any changes.

Password Management:
Enter user login and password details. Click box to right of password to view. Select options for each user.



Log:
A log file is updated for all network activity, the format of the log file is shown in Fig.4. Log data display is Last In, First Line (LIFO), chronologically descending order.

Log Entries — Filter: off Page: 1

Status	Device	Location	Date	Description	Action
Login		192.168.1.230	13:11:40 Mon Aug 12 2024	admin	
Login		192.168.1.230	11:26:48 Mon Aug 12 2024	admin	
Boot			11:18:01 Mon Aug 12 2024	System Reboot	
Boot			11:18:01 Mon Aug 12 2024	System Reboot	
Boot			11:18:01 Mon Aug 12 2024	System Reboot	
Boot			11:18:01 Mon Aug 12 2024	System Reboot	
Boot			11:18:01 Mon Aug 12 2024	System Reboot	
Alarm			13:30:40 Thu Dec 19 2024	alarm OFF - device	none
Boot			13:30:28 Thu Dec 19 2024	System Reboot	
Alarm			11:28:06 Mon Aug 12 2024	alarm OFF - device	none
Boot			11:18:01 Mon Aug 12 2024	System Reboot	
Alarm			13:07:42 Thu Dec 19 2024	alarm OFF - device	none
Boot			13:07:30 Thu Dec 19 2024	System Reboot	
Login		0.0.0.0	12:33:54 Thu Dec 19 2024	admin	
Boot			12:33:44 Thu Dec 19 2024	System Reboot	
Login		192.168.1.200	12:28:56 Thu Dec 19 2024	admin	
Login		192.168.1.200	12:27:54 Thu Dec 19 2024	admin	
Login		192.168.1.200	12:24:17 Thu Dec 19 2024	admin	
Login		192.168.1.200	12:04:56 Thu Dec 19 2024	admin	
Login		192.168.1.200	11:58:45 Thu Dec 19 2024	admin	

Home | Page Up | Page Down | Filter | Close

Fig.4

- Status – log entry type:
  - System = system messages/events such as Login, Boot
  - Alarms = any system/device alarm event
  - Devices = parameter changes made to any device(s)
- Device – which device was changed (Card, Port)
- Location – multi-purpose, system data or Card/Port/DFA slot/channel
- Date – Time and Date of log entry
- Description – description of event
- Action – action taken such as email sent, parameter value that was changed
- Filter:
  - On/Off annunciator for filtering
- Page:
  - Current log page being displayed, 20 entries per page

Navigation Buttons:

- **Home** – move display to first/home page. Top right display
- **Page Up** – scroll up 20 entries
- **Page Down** – scroll down 20 entries
- **Filter** – select filter mode
- **Close** – close log display

Log file entries can be filtered to reduce clutter, focus on specific log entries as shown in Fig.5.

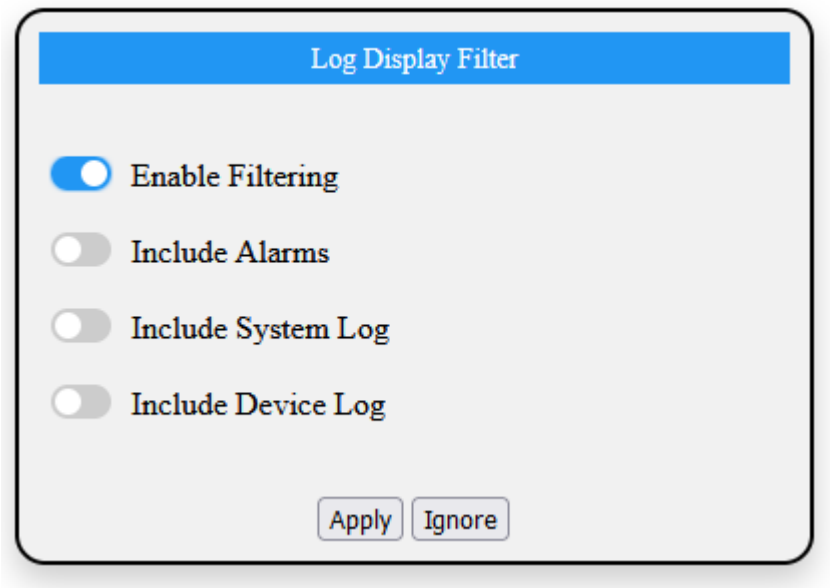


Fig.5

- Enable Filtering – must be enabled to filter log entries
- Include Alarms – Alarm entries
- Include System Log – system messages such as Login, Boot, etc
- Include Device Log – device parameter changes

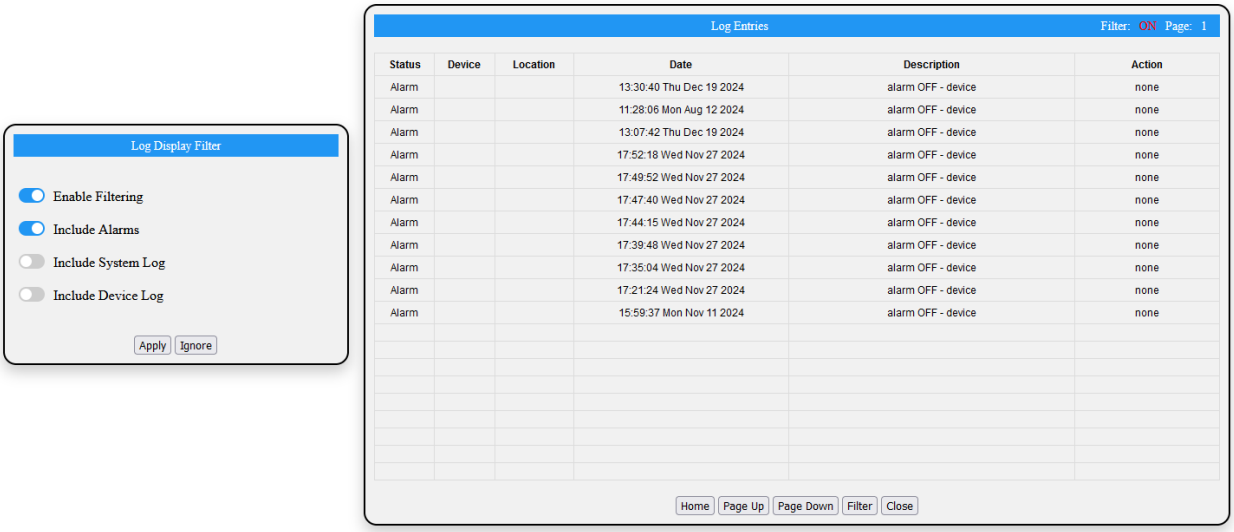


Fig.6

Fig.6 depicts a Filter setting of Alarms Only selection. Note that multiple filter options can be selected - default of none.

The Log display is live, a new log entry will be displayed as received and the display page scrolled down – this may not be the case if filtering is Enabled, and new log message does not match the criteria of selected log filtering.

Entire Log File can be downloaded to local host in Admin menu dialog. The file format is comma delimited CSV, Excel spreadsheet and saved in local Downloads directory. This file can be directly imported into a New spreadsheet.

About:
This dialog box displays contact information and software version running.

Fig.7

Logins:

The system supports three (3) login names as shown in Table.1. The passwords are fixed in http: (port 80) version, using https: (port 443) passwords can be changed . When using https: enter the new password required and save – this is effective at next login.

Name	Password	Privileges	Notes
user	safecom	View only	General usage, user login
tech	scw@tech	Change parameters	Only CHC/DFA parameters
admin	scw@admin	Change All	Card Parameters and Admin

Table.1

Directory Structure:

WEBNMS is Linux based and follows standard Linux practices for directory/file permissions. A System Service is started at boot time which will run WEBNMS automatically after boot. The directory structure is fixed, thus adding an extra layer of security, as shown in Table.2.

Directory/File	Purpose	Notes
/usr/html_web	Containing folder for WEBNMS	Scweb program, all HTML, .JPG, .CSS, .ICO files
/usr/html_web/data	Containing folder for data files	Generally, SCWEB update
/usr/html_web/admin.scw	Admin configuration Data	Encrypted file, not editable
/usr/html_web/user.scw	User Defined Parameters	Text file, user editable
/usr/html_web/bdadbase.scw	Device Data Base	Encrypted, not user editable

Table.2

User Configuration File:

This is a text file and editable in Notepad or similar. This allows the user to simply configure the IP settings of the system.

Location: /usr/html_web/data/user.scw

Command	Syntax	Notes
.name	.name Combo	Appears on main Web screen
.location Red+Bank	.location Red+Bank	Appears on main Web screen
.iplocal 192.168.1.193	.iplocal 192.168.1.193	Sets IP address of system - fixed
.netmask 255.255.255.0	.netmask 255.255.255.0	Required netmask - default
.gateway	.gateway 192.168.1.0	As required to reach outside network

Table.3

Note, changing this file will require a reboot of the WEBNMS. System can be rebooted from the Admin Dialog Box or using SSH and entering “sudo reboot” followed by password.

Windows Shared Folder Access:

WEBNMS has a Shared Folder process running that allows WEBNMS to be Mapped to a Windows Driver Letter. From File Explorer, right-click on This PC. Then select Map Network Drive, choose drive letter, enter the IP address of connected WEBNMS board and share folder. Also Check-box use different credentials. See Fig.4. for details

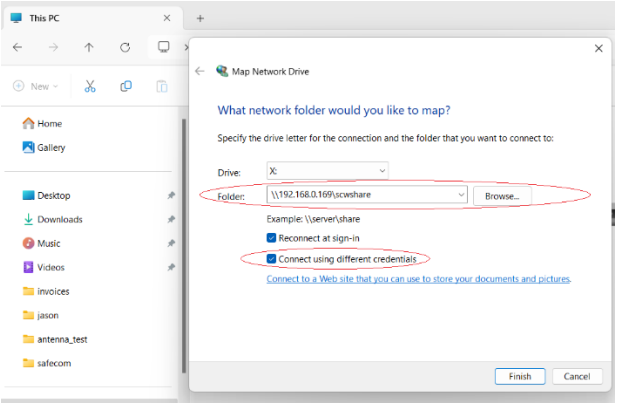


Fig.4

PW: safecom

Now, all the files in /usr/html_web will be accessible from the X: drive in this example. To update software, simply copy directly here and then reboot. Also, /usr/html_web/data/user.scw can be opened in WordPad and edited.

SSH Access:

The Linux board can be accessed via Secured Shell (SSH) protocol which connects via IP and Port 22. Using Putty or similar, enter the boards IP and connect using SSH (Port should already be set by default). Refer to Table.4 for details.

Step	Enter	Notes
1	Run Putty	Or similar Terminal Emulator (RealTerm)
2	IP address xxx.xxx.xxx.xxx	WEBNMS default is **192.168.1.192**
3	Set Port 22	Normally set by default
4	Connect	Connection return Login/Pw window
5	Login: rock Pw: rock	Connection will then be completed. A new Certificate may pop-up, accept it.
6	Sudo bash	Set login to root/sudo – high privileges
	Enter PW: rock	Enter password as requested
7	cd /usr/html_web/data	Change to WEBNMS data directory

Table.4

WIFI Setup:

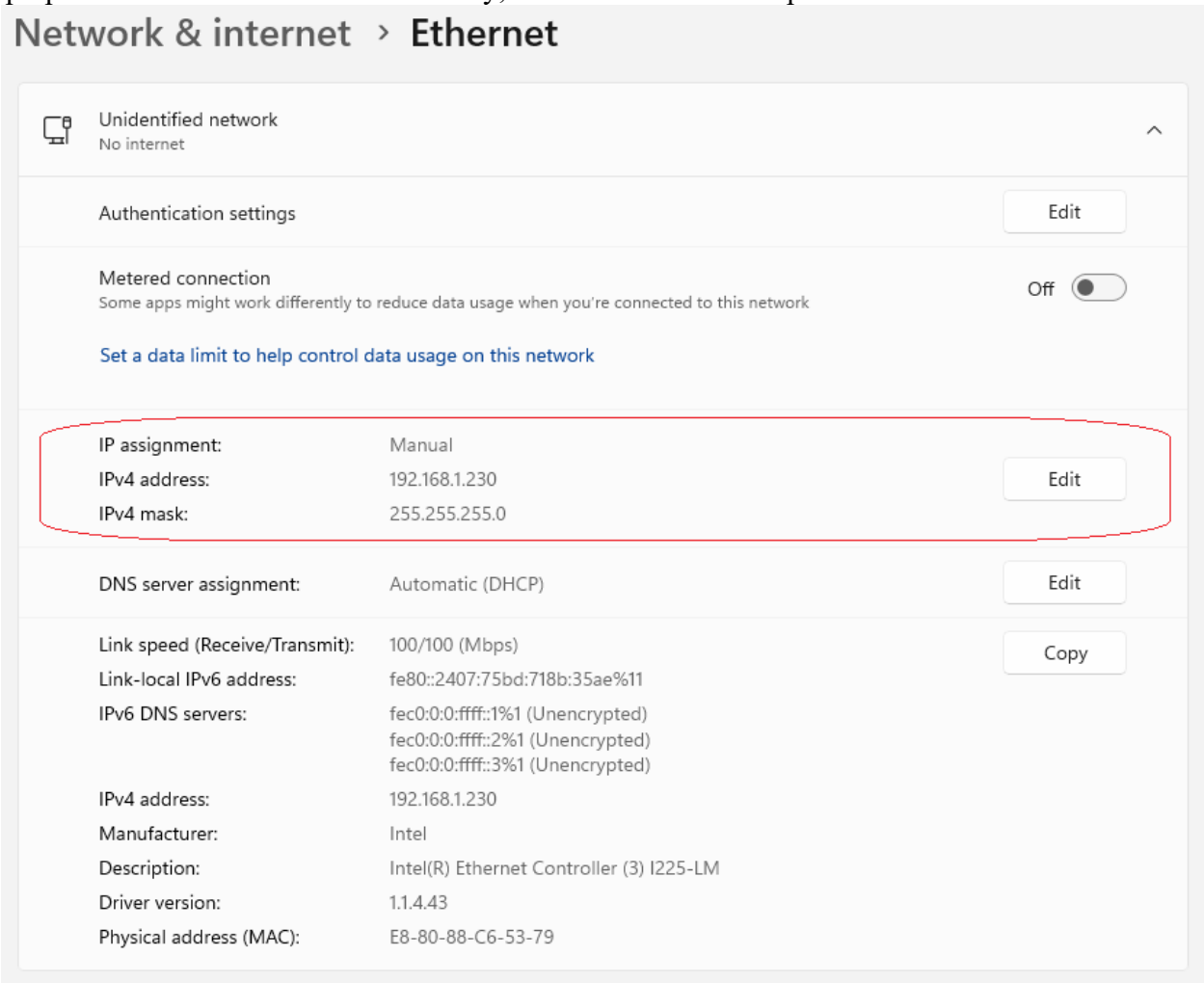
Some versions of RockPI S have Wifi capabilities. In order to setup the connection, run the following commands as shown in Table.5.

Command Line	Response	Notes
nmcli radio wifi	enabled	Check if Wifi running
nmcli radio wifi on	enabling	If disabled, enable with this
nmcli dev wifi list	List of available Wifi names	Use Space Bar to step, Enter for next page, Ctrl-C to exit
sudo nmcli dev wifi connect ssid password “pw”	Command prompt	Enter SSID/PW for your site
nmcli con show	Wifi connection details	Try ping google.com to test

Table.5

Appendix A

Setting up Lan connection to local PC/laptop allows for direct connection between DAS system and laptop via CAT cable. To do this directly, windows must be setup as follows:



- Connect the DAS system via CAT cable to laptop Ethernet port
- Open Network connections dialog box and select Ethernet port
- Click Edit:
  - IP assignment – Manual
  - IPV4 address – 192.168.1.230
  - IPv4 mask – 255.255.255.0

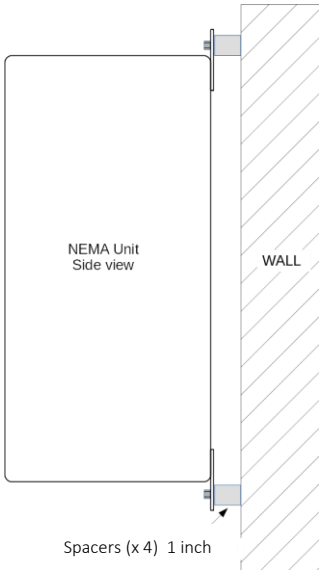
DAS can now be connected via https (port 433) or SSH (port 22)

Installation

NOTE: All wiring shall be performed by an authorized licensed contractor in accordance with the local jurisdictions code and compliant to NEC.

Wall Mounting

When mounting the BDA on the wall, it is critical to provide spacers between the unit and the wall. A one inch space is appropriate to allow for good air flow.



Four ¼ inch LAG Screws are to be used to mount the NEMA unit to ½ plywood.

One inch punched square tube can be used as a spacer between the NEMA unit and the wall.

Electrical Connections: For pluggable equipment, the socket-outlet shall be easily accessible. Proper strain relief is required on all electrical connections to the unit.

Copyright © 2025 Safe-Com. All Rights Reserved.

No part of this publication, or any software included with it may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, including photocopying, electronic, mechanical, recording or otherwise, without the prior written permission of the copyright holder.

Safe-Com provides this document as is, without any warranty of any kind either expressed or implied including, but not limited to, the implied warranties of merchantability and fitness of a particular purpose. Safe-Com may make changes or improvements in the equipment, software, or specifications described in this document at any time and without notice. These changes will be incorporated in new releases of this document.
This document may contain technical inaccuracies or typographical errors. Safe-Com waives responsibility for any labor, materials, or costs incurred by any person or party as a result of using this document. Safe-Com and any of its affiliates shall not be liable for any damages (including, but not limited to, consequential, indirect or incidental, special damages or loss of profits or date) even if they were foreseeable and Safe-Com has been informed of their potential occurrence, arising out of or in connection with this document or its use.