Operating Manual

ProtoAir Start-up Guide

FPA-W44, FPA-C41, FPA-C42, FPA-C43

Revision: 3.M

Document No.: T18622

Print Spec: 10000005389 (F)

MSA Safety
1000 Cranberry Woods Drive
Cranberry Township, PA 16066 USA

U.S. Support Information:
+1 408 964-4443
+1 800 727-4377
Email: smc-support@msasafety.com

EMEA Support Information:
+31 33 808 0590
Email:
smc-support.emea@msasafety.com

For your local MSA contacts, please go to our website www.MSAsafety.com

Contents

1 About the ProtoAir

The ProtoAir is a high performance,high-performance, multi-protocol IIoT gateway providing manufacturers Wi-Fi and cellular connectivity into the cloud and instant multi-protocol deployment of field protocols, enabling new or legacy devices to easily interface with other protocols.

It is not necessary to download any configuration files to support the required applications. The ProtoAir is pre-loaded with tested profiles/configurations for the supported devices.

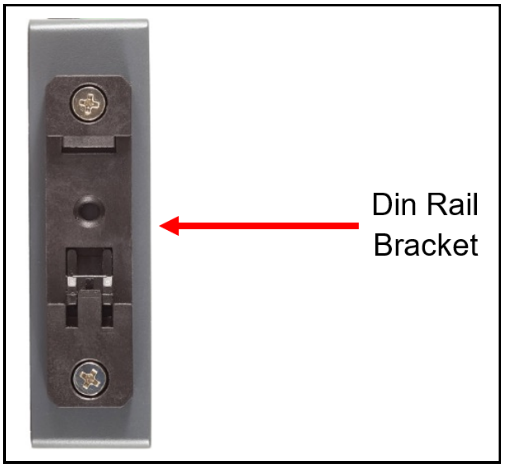
NOTE: For troubleshooting assistance refer to Section 11 Troubleshooting, or any of the troubleshooting appendices in the related driver supplements. Check the MSA Safety website for technical support resources and documentation that may be of assistance.

The ProtoAir is cloud ready and connects with MSA Safety's Grid. See **Section 9.4.1 Accessing the FieldServer Manager** for further information.

2 Equipment Setup

2.1 Mounting

The gateway can be mounted using the DIN rail mounting bracket on the back of the unit.



2.2 Attaching the Antenna(s)

Wi-Fi Antenna:

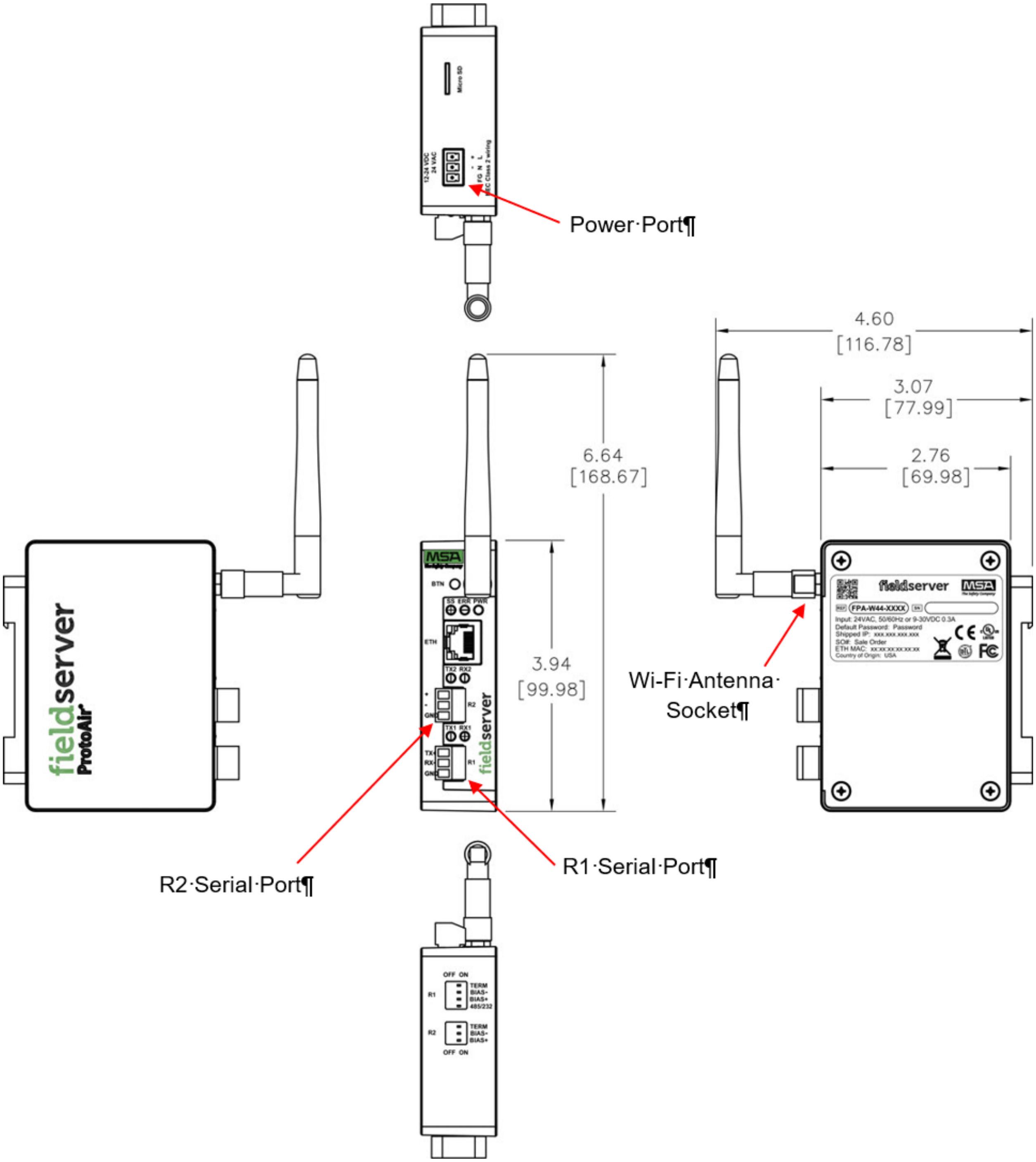
If using the FPA-W44 model, screw in the Wi-Fi antenna to the front of the unit as shown in **Section 2.3.1 FPA-W44 Drawing**.

Cellular Antenna:

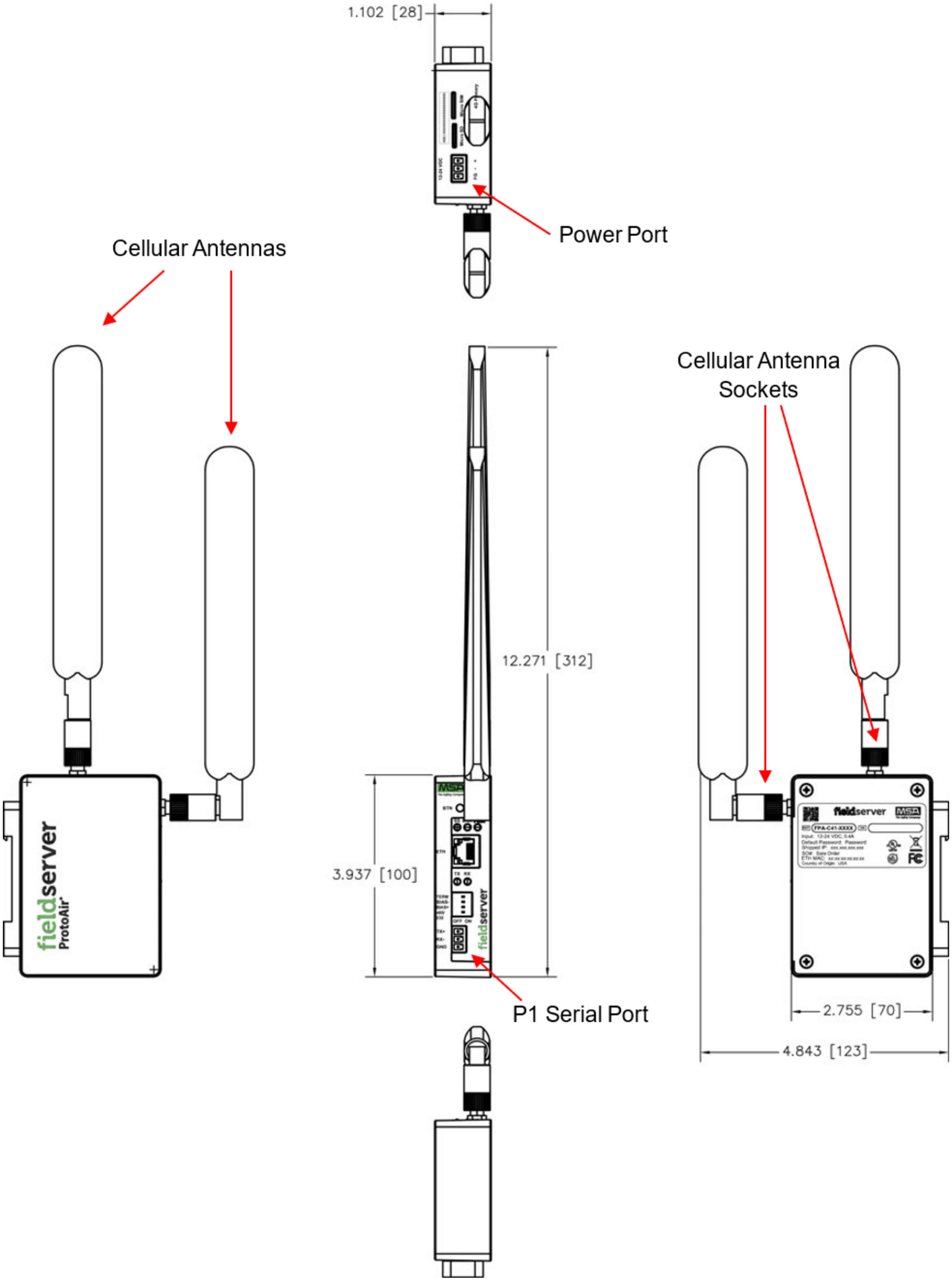
If using the FPA-C4X model, screw in the two cellular antennas. One antenna is screwed into the socket on the top of the unit and one is screwed into the socket on the side as shown in **Section 2.3.2 FPA-C4X Drawing**.

2.3 Physical Dimensions

2.3.1 FPA-W44 Drawing



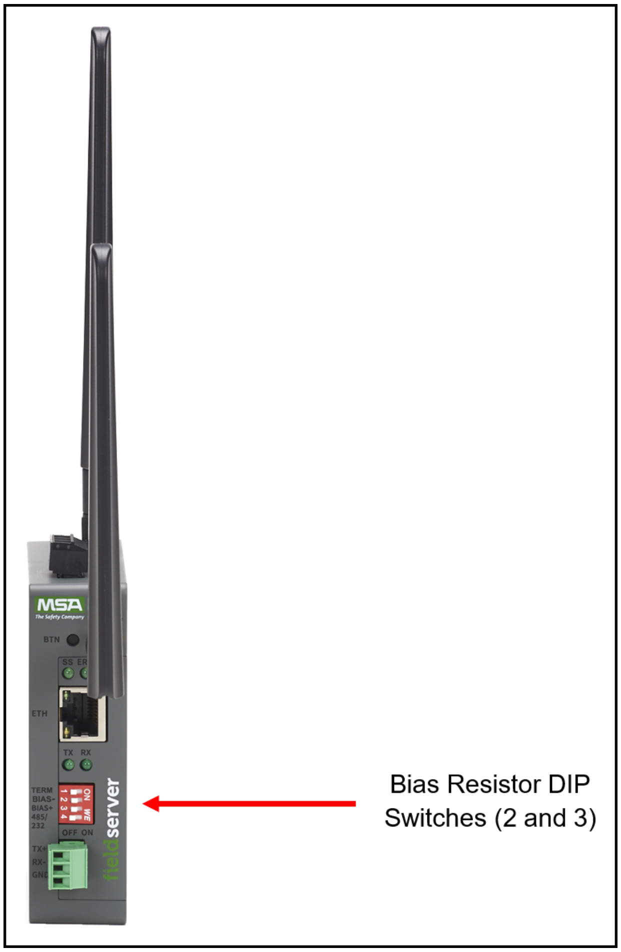
2.3.2 FPA-C4X Drawing



3 Installation

3.1 DIP Switch Settings for FPA-C4X

3.1.1 Bias Resistors



Bias Resistor DIP Switches (2 and 3)

To enable Bias Resistors, move both the BIAS- and BIAS+ dip switches to the right in the orientation shown above.

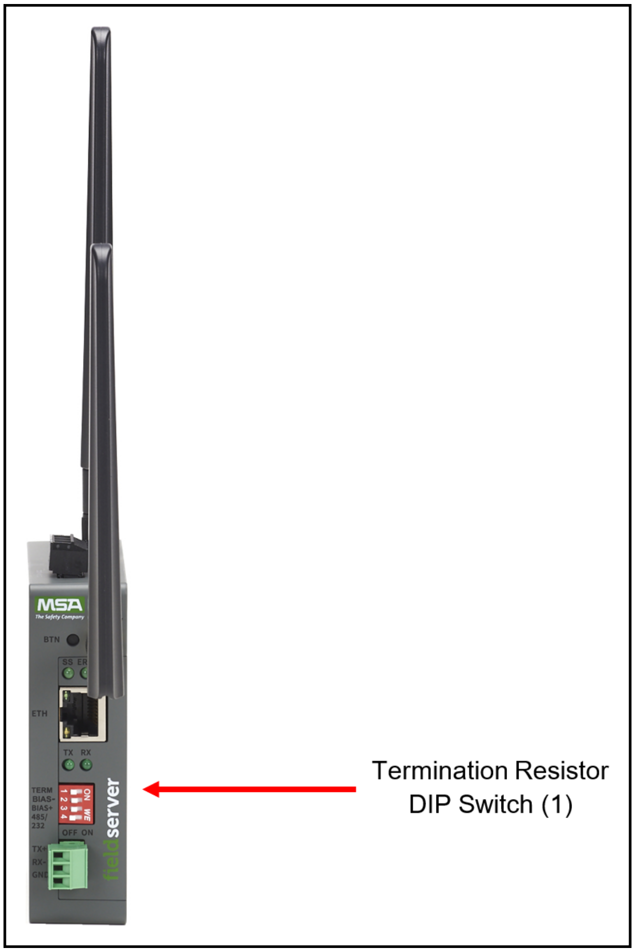
The bias resistors are used to keep the RS-485 bus to a known state, when there is no transmission on the line (bus is idling), to help prevent false bits of data from being detected. The bias resistors typically pull one line high and the other low - far away from the decision point of the logic.

The bias resistor is 510 ohms which is in line with the BACnet spec. It should only be enabled at one point on the bus (for example, on the field port were there are very weak bias resistors of 100k). Since there are no jumpers, many ProtoAirs can be put on the network without running into the bias resistor limit which is < 500 ohms.

NOTE: See the Termination and Bias Resistance Enote for additional information.

NOTE: If the gateway is already powered on, DIP switch settings will not take effect unless the unit is power cycled.

3.1.2 Termination Resistor



Termination Resistor
DIP Switch (1)

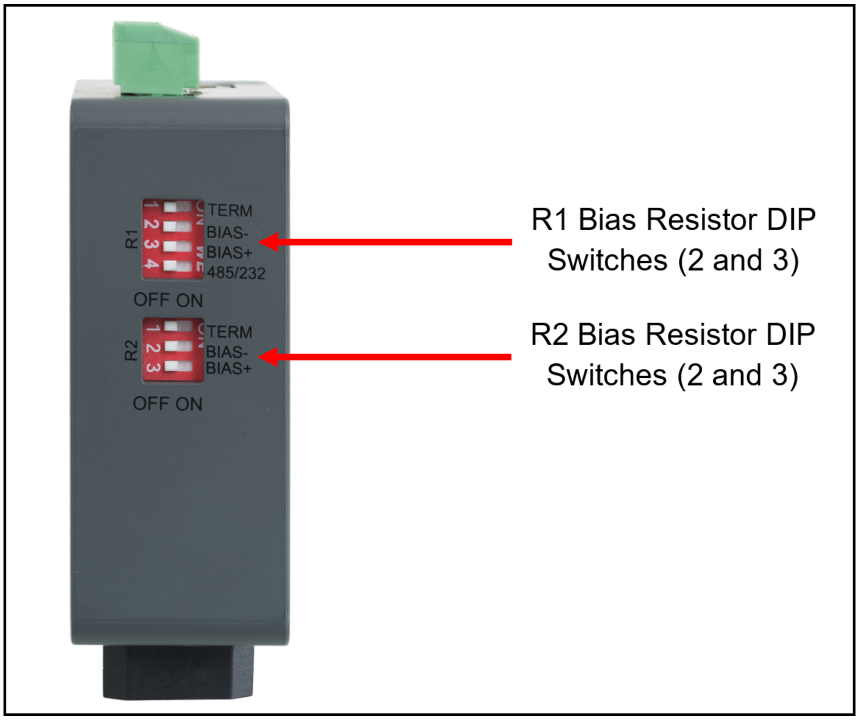
If the gateway is the last device on the serial trunk, then the End-Of-Line Termination Switch needs to be enabled**. To enable the Termination Resistor, move the TERM dip switch to the right in the orientation shown in above**.

Termination resistor is also used to reduce noise. It pulls the two lines of an idle bus together. However, the resistor would override the effect of any bias resistors if connected.

NOTE: If the gateway is already powered on, DIP switch settings will not take effect unless the unit is power cycled.

3.2 DIP Switch Settings for FPA-W44

3.2.1 Bias Resistors



R1 Bias Resistor DIP Switches (2 and 3)

R2 Bias Resistor DIP Switches (2 and 3)

To enable Bias Resistors, move both the BIAS- and BIAS+ dip switches to the right in the orientation shown above.

The bias resistors are used to keep the RS-485 bus to a known state, when there is no transmission on the line (bus is idling), to help prevent false bits of data from being detected. The bias resistors typically pull one line high and the other low - far away from the decision point of the logic.

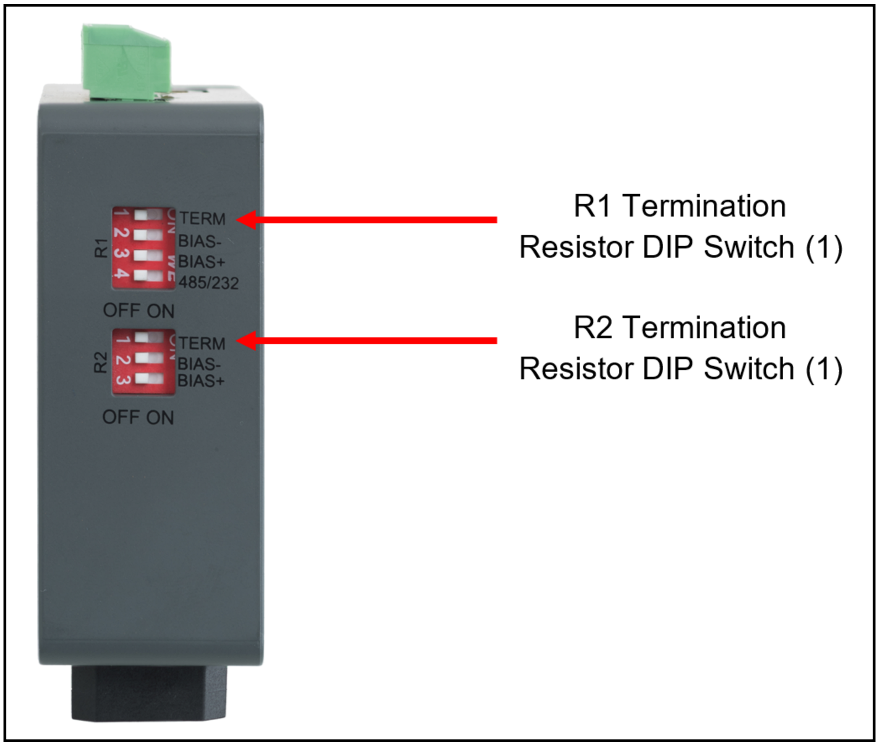
The bias resistor is 510 ohms which is in line with the BACnet spec. It should only be enabled at one point on the bus (for example, on the field port were there are very weak bias resistors of 100k). Since there are no jumpers, many ProtoAirs can be put on the network without running into the bias resistor limit which is < 500 ohms.

NOTE: See the Termination and Bias Resistance Enote for additional information.

NOTE: The R1 and R2 DIP Switches apply settings to the respective serial port.

NOTE: If the gateway is already powered on, DIP switch settings will not take effect unless the unit is power cycled.

3.2.2 Termination Resistor


R1
1 2 3 4
ON
TERM
BIAS-
BIAS+
485/232
OFF ON
R2
1 2 3
ON
TERM
BIAS-
BIAS+
OFF ON
R1 Termination Resistor DIP Switch (1)
R2 Termination Resistor DIP Switch (1)

If the gateway is the last device on the serial trunk, then the End-Of-Line Termination Switch needs to be enabled**. To enable the Termination Resistor, move the TERM dip switch to the right in the orientation shown in above**.

Termination resistor is also used to reduce noise. It pulls the two lines of an idle bus together. However, the resistor would override the effect of any bias resistors if connected.

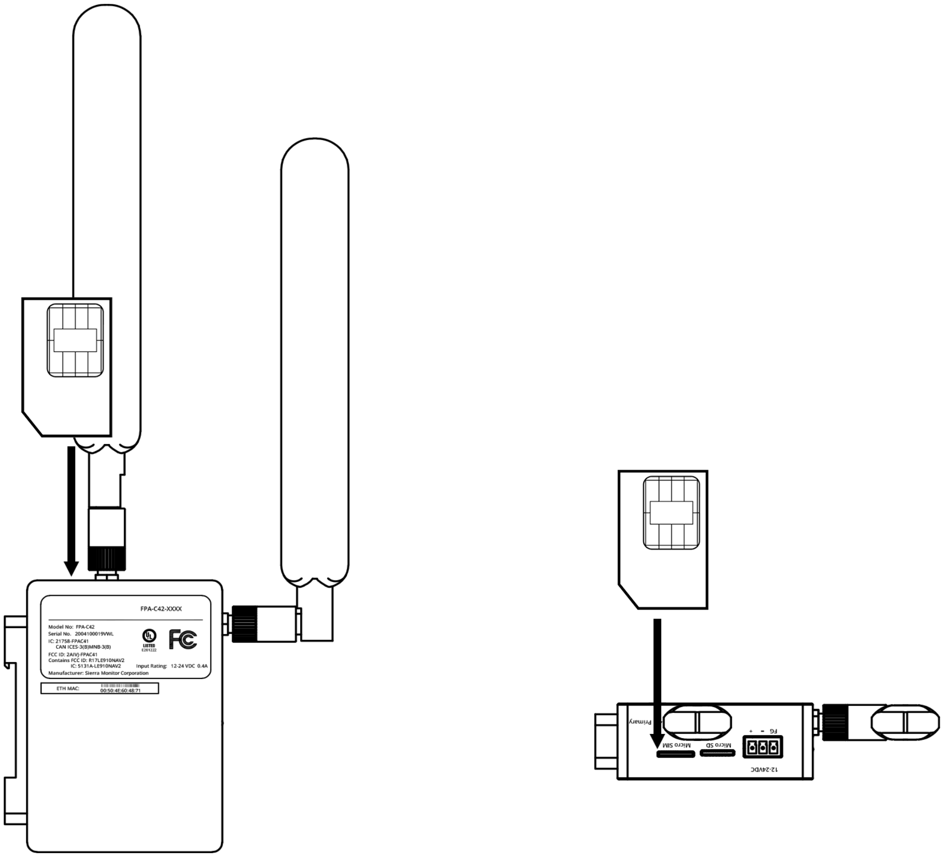
NOTE: The R1 and R2 DIP Switches apply settings to the respective serial port.

NOTE: If the gateway is already powered on, DIP switch settings will not take effect unless the unit is power cycled.

3.3 FPA-C4X: Inserting the SIM Card

NOTE: A micro 4G SIM card must be purchased from an AT&T or Verizon cellular provider to set up cellular functionality and create a data plan for the FieldServer. SIM card vendor contact information is available at the end of the section.

Insert the SIM card into the Micro SIM card slot with the chip on the SIM card facing away from the cellular antenna as shown below.



See **Section 8.1.5 FPA-C4X: Cellular Settings** to complete cellular setting configuration.

The table below shows cellular usage examples to forecast data usage on the chosen cellular plan.

Number of Data Points	Logging Frequency	Data Usage per Hour	Data Usage per Month
10	40 sec	0.75 Mb	547 Mb
10	900 sec	0.55 Mb	400 Mb
50	40 sec	1.24 Mb	900 Mb
50	900 sec	0.90 Mb	657 Mb
100	40 sec	3.00 Mb	2.2 Gb
100	900 sec	1.26 Mb	900 Mb
500	40 sec	10.86 Mb	7.8 Gb
500	900 sec	0.55 Mb	1.5 Gb

SIM Card Vendor Contact Information:

Verizon

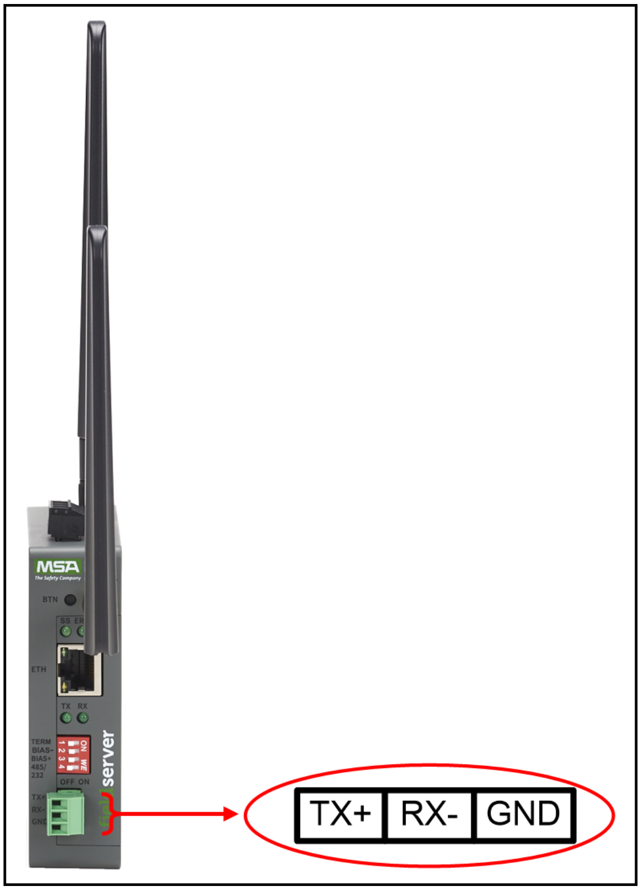
A business contract is required to purchase a Verizon SIM card. The IMEI of the ProtoAir is required to purchase the Verizon SIM card.

AT&T

Please call AT&T Customer Service at 800.331.0500 or find the nearest AT&T store.

3.4 FPA-C4X: Connecting the P1 Port

Switch between RS-485 and RS-232 by moving the number 4 DIP Switch left for RS-485 and right for RS-232. Connect to the 3-pin connector as shown below.



The following baud rates are supported on the P1 Port:
9600, 19200, 38400, 57600, 76800, 115000

NOTE: Not all baud rates listed are supported by all protocols. Check the specific protocol driver manual for a list of the supported baud rates.

3.4.1 Wiring

RS-485		RS-232	
OEM Device orBMS RS-485 Wiring	**Gateway Pin Assignment**	**OEM Device orBMS RS-485 Wiring**	**Gateway Pin Assignment**
RS-485 +	TX +	RS-232 -	TX +
RS-485 -	RX -	RS-232 +	RX -
GND	GND	GND	GND

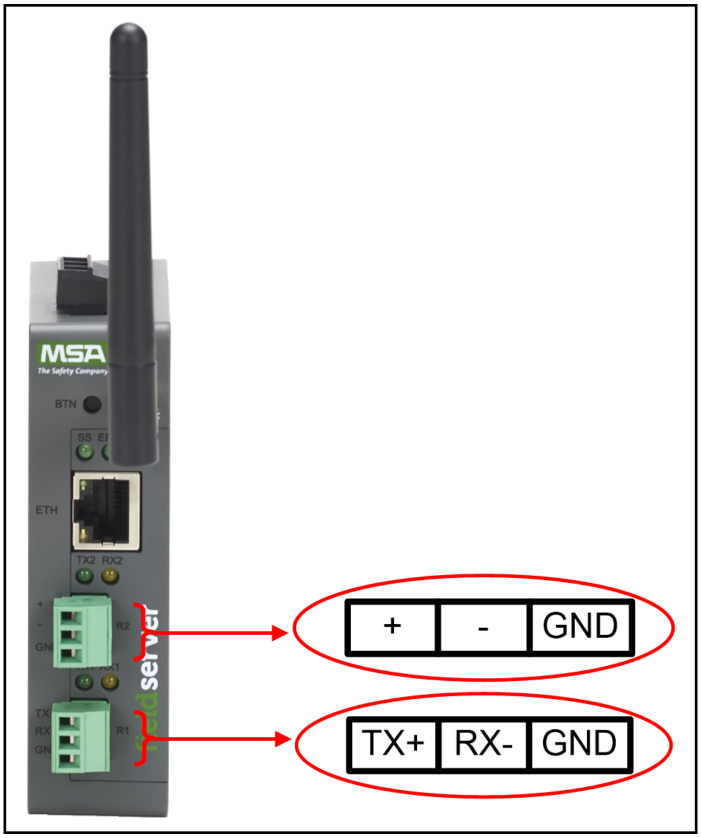
NOTE: The RS-485/RS-232 is part of the RS-485/RS-232 interface and must be connected to the corresponding terminal on the BMS. If the cable is shielded, the shield must connected only at one end and to earth ground – it will help suppress the electromagnetic field interference. (Connecting the shield at both ends will likely produce current loops, which could produce noise or interference that the shield was intended to block).

3.5 FPA-W44: Connecting the R1 & R2 Ports

For the R1 Port only: Switch between RS-485 and RS-232 by moving the number 4 DIP Switch left for RS-485 and right for RS-232 (see images in **Section 3.2 DIP Switch Settings for FPA-W44**).

The R2 Port is RS-485.

Connect to the 3-pin connector(s) as shown below.



The following baud rates are supported on the R1 and R2 Ports:
9600, 19200, 38400, 57600, 76800, 115000

NOTE: Not all baud rates listed are supported by all protocols. Check the specific protocol driver manual for a list of the supported baud rates.

3.5.1 Wiring

RS-485		RS-232	
OEM Device orBMS RS-485 Wiring	Gateway Pin Assignment	OEM Device orBMS RS-485 Wiring	Gateway Pin Assignment
RS-485 +	TX +	RS-232 -	TX +
RS-485 -	RX -	RS-232 +	RX -
GND	GND	GND	GND

NOTE: The RS-485/RS-232 is part of the RS-485/RS-232 interface and must be connected to the corresponding terminal on the BMS. If the cable is shielded, the shield must connected only at one end and to earth ground – it will help suppress the electromagnetic field interference. (Connecting the shield at both ends will likely produce current loops, which could produce noise or interference that the shield was intended to block).

4 Power up the Gateway

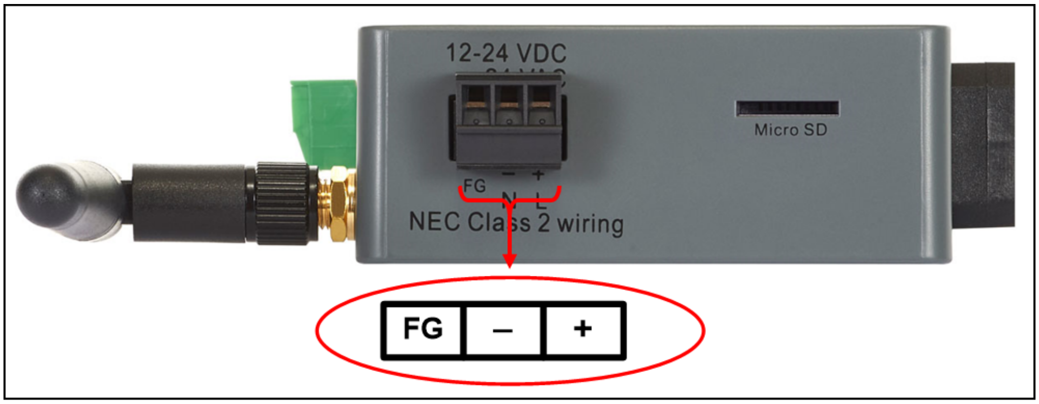
Check power requirements in the table below:

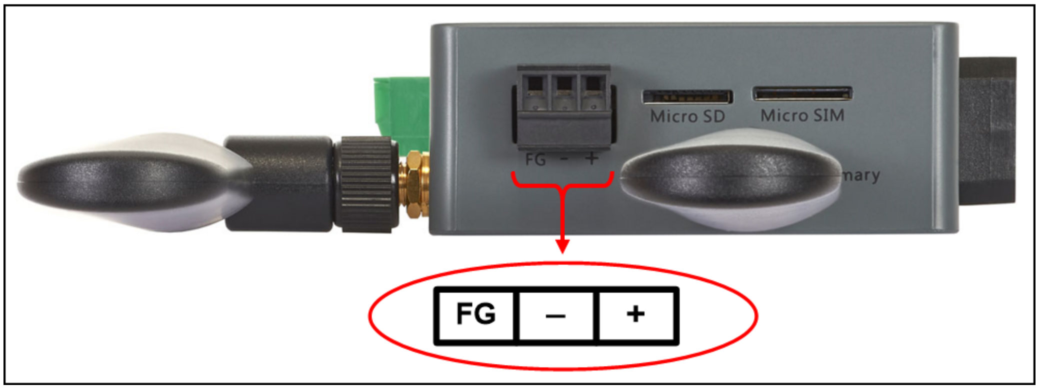
Power Requirement for ProtoAir External Gateway		
	Current Draw Type	
ProtoAir Family	**12VDC**	**24VDC/AC**
FPA –W44 (Typical)	250mA	125mA
ProtoAir Family	**12VDC**	**24VDC**
FPA –C4X (Typical)	320mA	185mA
FPA –C4X (Maximum)	670mA	390mA
NOTE: These values are 'nominal' and a safety margin should be added to the power supply of the host system. A safety margin of 25% is recommended.		

Apply power to the ProtoAir as shown below. Ensure that the power supply used complies with the specifications provided in **Section 12.7 Specifications** . Ensure that the cable is grounded using the FG or "Frame GND" terminal.

- The ProtoAir FPA-W44 is powered by 9-30VDC or 24VAC.
  - Supports both Full-Wave and Half-Wave AC
- The ProtoAir FPA-C4X is powered by 12-24VDC.
- Frame GND should be connected to ensure personnel safety and to limit material damages due to electrical faults. Ground planes are susceptible to transient events that cause sudden surges in current. The frame ground connection provides a safe and effective path to divert the excess current from the equipment to earth ground.

NOTE: Floating AC Power Supplies are supported.

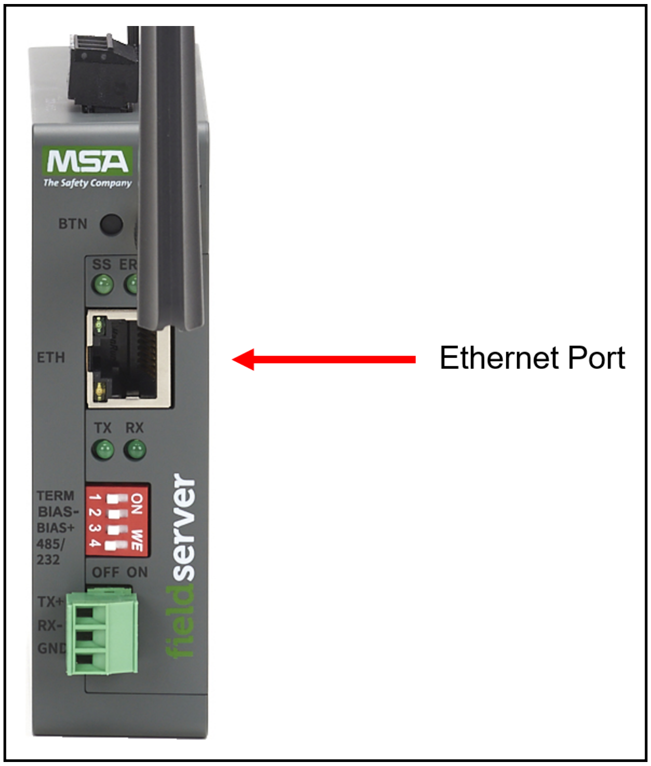




5 Connect the PC to the Gateway

5.1 10/100 Ethernet Connection Port

NOTE: Do not use shielded Ethernet cables.



The Ethernet Port is used both for Ethernet protocol communications and for configuring the gateway via the Web App. To connect the gateway, either connect the PC to the router's Ethernet port or connect the router and PC to an Ethernet switch. Use Cat-5 cables for the connection.

NOTE: The Default IP Address of the gateway is 192.168.1.24, Subnet Mask is 255.255.255.0.

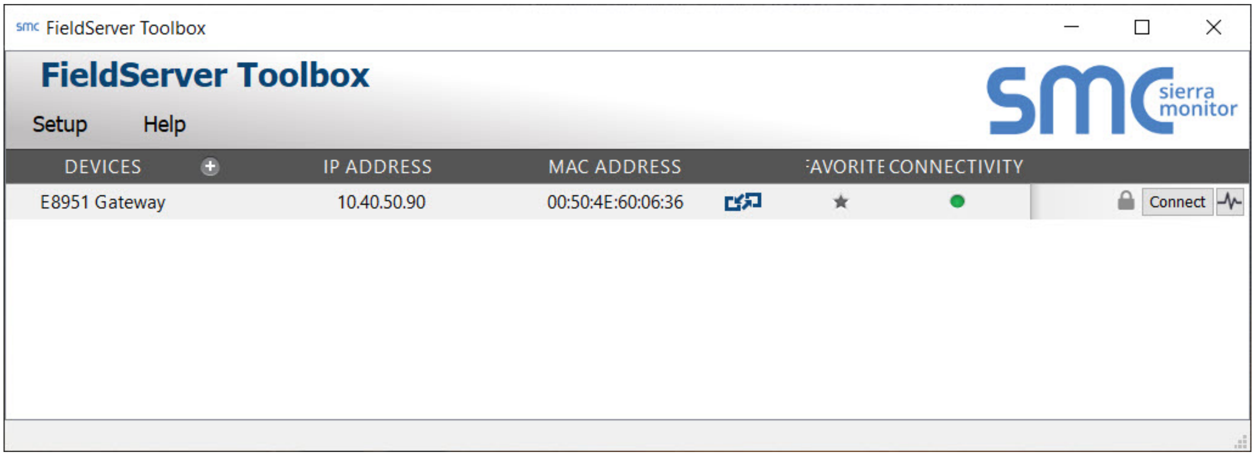
6 Connecting to the ProtoAir

The FieldServer Toolbox Application can be used to discover and connect to the ProtoAir on a local area network. To manually connect to the ProtoAir using the Toolbox, click on the plus icon next to the "Devices" header and enter the IP Address, or enter the Internet IP Address into a web browser.

6.1 Using the FieldServer Toolbox to Discover and Connect to the ProtoAir

- Install the Toolbox application from the USB drive or download it from the MSA Safety website.
- Use the FS Toolbox application to find the ProtoAir and connect to the ProtoAir.

NOTE: If the connect button is grayed out, the ProtoAir's IP Address must be set to be on the same network as the PC. (Section 6.2 Using a Web Browser)



DEVICES	IP ADDRESS	MAC ADDRESS	:AVORITE	CONNECTIVITY
E8951 Gateway	10.40.50.90	00:50:4E:60:06:36	★	●

6.2 Using a Web Browser

- Open a web browser and connect to the ProtoAir's default IP Address. The default IP Address of the ProtoAir is **192.168.1.24**, Subnet Mask is **255.255.255.0**.
- If the PC and the ProtoAir are on different IP networks, assign a static IP Address to the PC on the 192.168.1.X network.

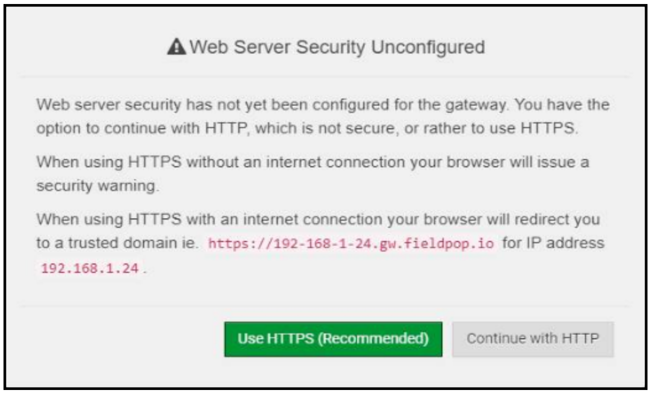
NOTE: Check Section 11.8 Internet Browser Software Support for supported browsers.

7 Setup Web Server Security

7.1 Login to the FieldServer

The first time the FieldServer GUI is opened in a browser, the IP Address for the gateway will appear as untrusted. This will cause the following pop-up windows to appear.

- When the Web Server Security Unconfigured window appears, read the text and choose whether to move forward with HTTPS or HTTP.



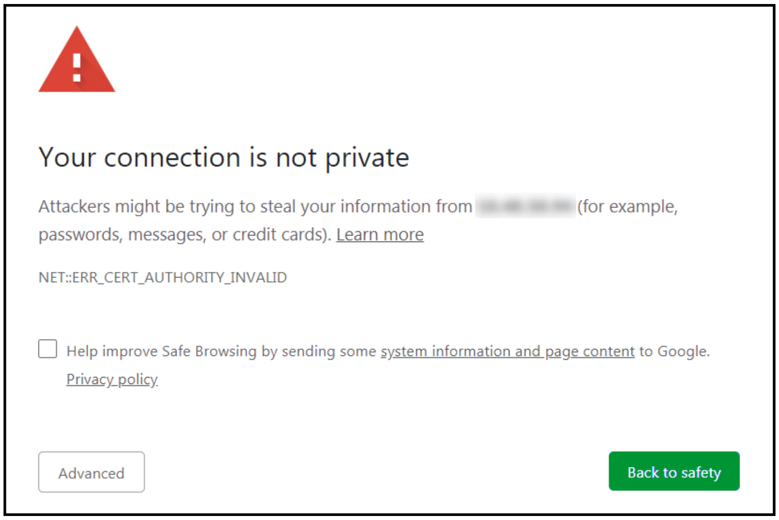
⚠ Web Server Security Unconfigured

Web server security has not yet been configured for the gateway. You have the option to continue with HTTP, which is not secure, or rather to use HTTPS.

When using HTTPS without an internet connection your browser will issue a security warning.

When using HTTPS with an internet connection your browser will redirect you to a trusted domain ie. `https://192-168-1-24.gw.fieldpop.io` for IP address `192.168.1.24`.

- When the warning that "Your connection is not private" appears, click the advanced button on the bottom left corner of the screen.



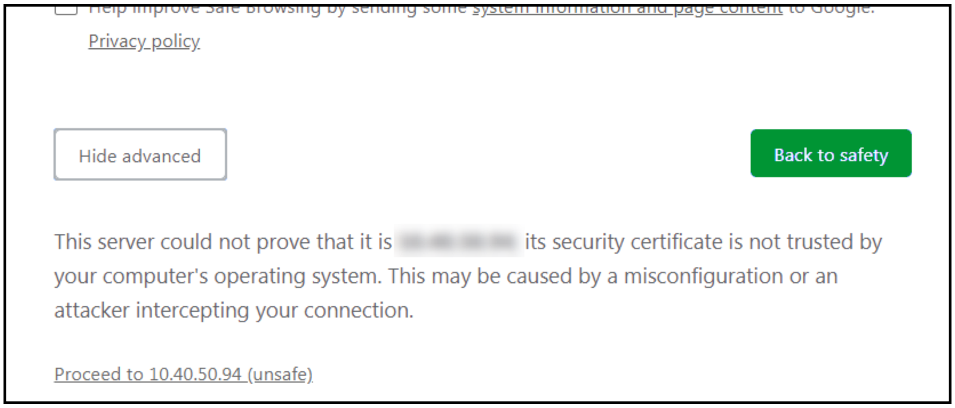
Your connection is not private

Attackers might be trying to steal your information from [redacted] (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

□ Help improve Safe Browsing by sending some system information and page content to Google. Privacy policy

- Additional text will expand below the warning, click the underlined text to go to the IP Address. In the example below this text is "Proceed to <FieldServer IP> (unsafe)".



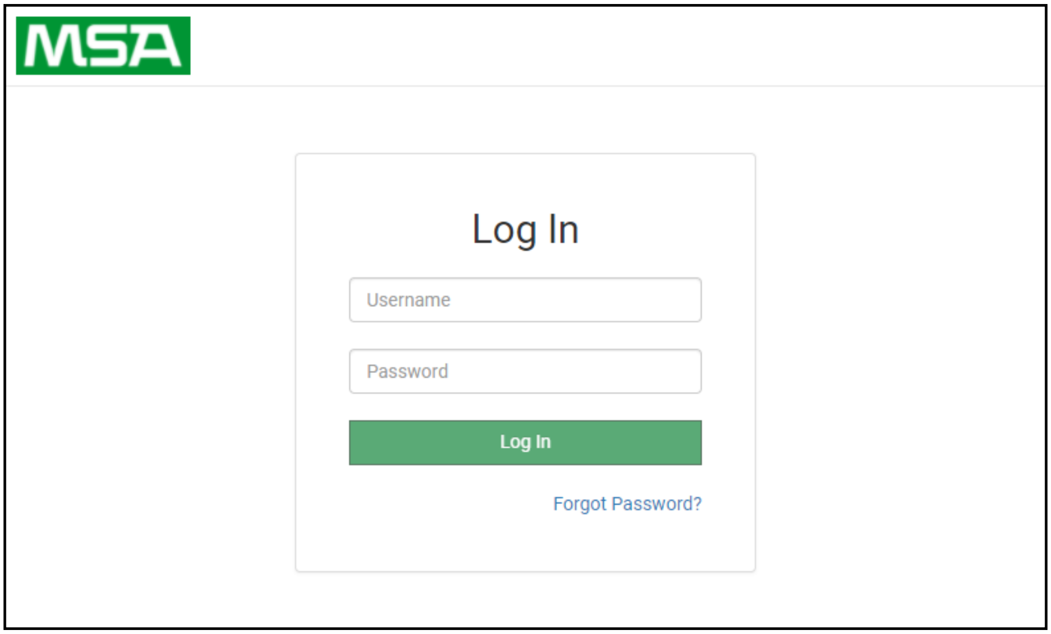
□ Help improve Safe Browsing by sending some system information and page content to Google.
Privacy policy

This server could not prove that it is [redacted] 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.

Proceed to 10.40.50.94 (unsafe)

- When the login screen appears, put in the Username (default is "admin") and the Password (found on the label of the FieldServer).

NOTE: There is also a QR code in the top right corner of the FieldServer label that shows the default unique password when scanned.

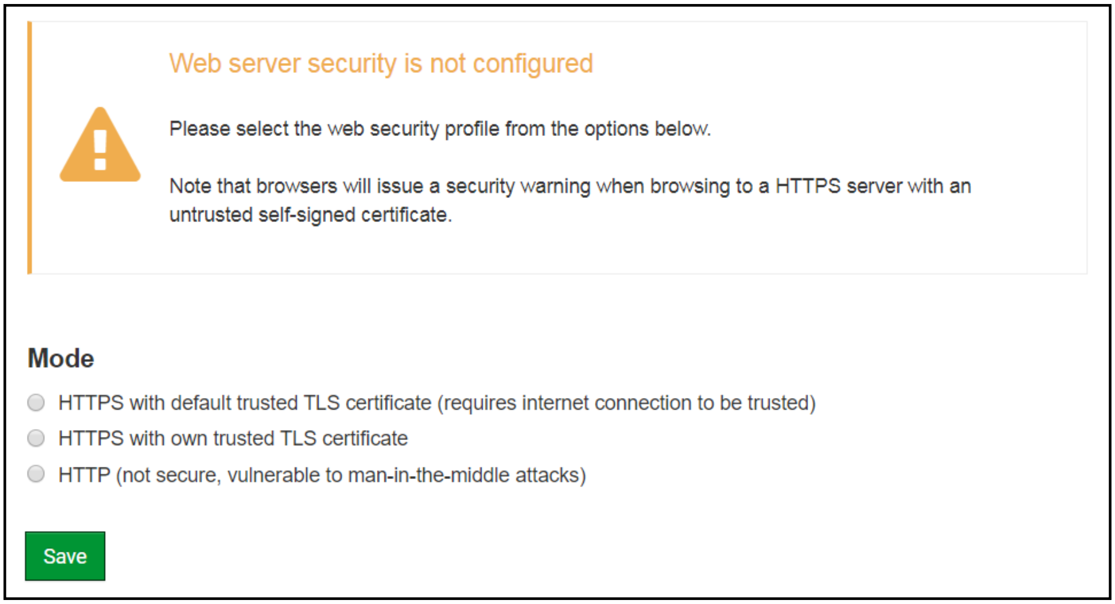


NOTE: A user has 5 attempts to login then there will be a 10-minute lockout. There is no timeout on the FieldServer to enter a password.

NOTE: To create individual user logins, go to Section 12.2 Change User Management Settings.

7.2 Select the Security Mode

On the first login to the FieldServer, the following screen will appear that allows the user to select which mode the FieldServer should use.



Web server security is not configured

Please select the web security profile from the options below.

Note that browsers will issue a security warning when browsing to a HTTPS server with an untrusted self-signed certificate.

Mode

○ HTTPS with default trusted TLS certificate (requires internet connection to be trusted)

○ HTTPS with own trusted TLS certificate

○ HTTP (not secure, vulnerable to man-in-the-middle attacks)

NOTE: Cookies are used for authentication.

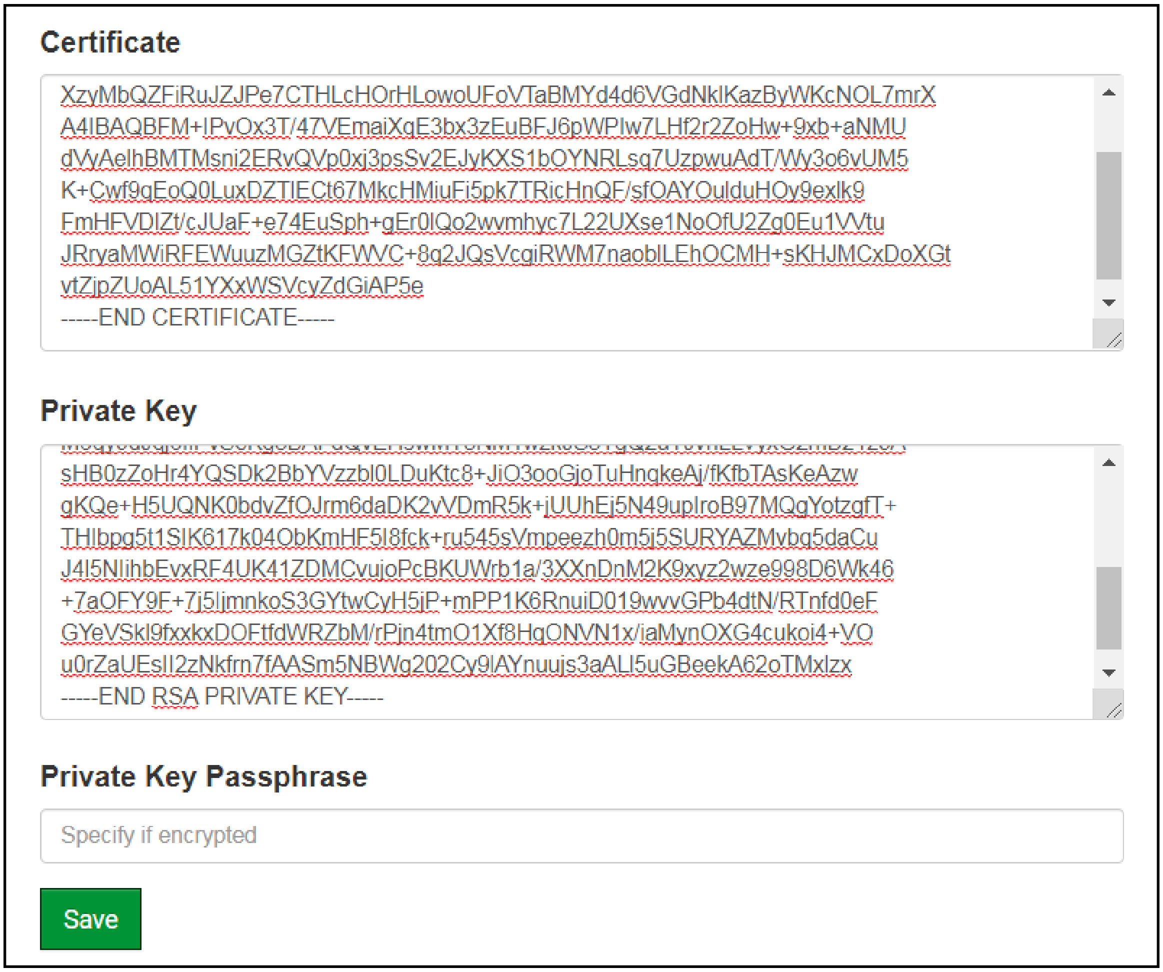
NOTE: To change the web server security mode after initial setup, go to Section 12.1 Change Web Server Security Settings After Initial Setup.

The sections that follow include instructions for assigning the different security modes.

7.2.1 HTTPS with Own Trusted TLS Certificate

This is the recommended selection and the most secure. **Please contact your IT department to find out if you can obtain a TLS certificate from your company before proceeding with the Own Trusted TLS Certificate option.**

- Once this option is selected, the Certificate, Private Key and Private Key Passphrase fields will appear under the mode selection.



Certificate

```
XzyMbQZFiRuJZJPe7CTHLcHOrHLowoUFoVTaBMYd4d6VGdNklKazByWKcNOL7mrX
A4IBAQBFM+IPvOx3T/47VEmaiXqE3bx3zEuBFJ6pWPIw7LHf2r2ZoHw+9xb+aNMU
dVyAelhBMTMsni2ERvQVp0xj3psSv2EJyKXS1bOYNRLsq7UzpwuAdT/Wy3o6vUM5
K+Cwf9qEoQ0LuxDZTIECt67MkcHMiuFi5pk7TRicHnQF/sfOAYOulduHOy9exlk9
FmHFVDIZt/cJUaF+e74EuSph+gEr0lQo2wvmhyc7L22UXse1NoOfU2Zg0Eu1VVtu
JRryaMWiRFEWuuzMGZtKFWVC+8q2JQsVcgiRWM7naoblLEhOCMH+sKHJMCxDoXGt
vtZjpZUoAL51YXxWSVcyZdGiAP5e
-----END CERTIFICATE-----
```

Private Key

```
sHB0zZoHr4YQSDk2BbYVzzbl0LDuKtc8+JiO3ooGjoTuHnqkeAj/fKfbTAsKeAzw
gKQe+H5UQNK0bdvZfOJrm6daDK2vVDmR5k+jUUhEj5N49upIroB97MQgYotzgfT+
THIbpg5t1SIK617k04ObKmHF5l8fck+ru545sVmpeezh0m5j5SURYAZMvbq5daCu
J4I5NIihbEvxRF4UK41ZDMCvujoPcBKUWrb1a/3XXnDnM2K9xyz2wze998D6Wk46
+7aOFY9F+7j5ljmnkoS3GYtwCyH5jP+mPP1K6RnuiD019wvvGPb4dtN/RTnfd0eF
GYeVSkl9fxxkxDOFtfdWRZbM/rPjn4tmO1Xf8HqONVN1x/iaMynOXG4cukoi4+VO
u0rZaUEsII2zNkfrn7fAASm5NBWg202Cy9lAYnuujs3aALI5uGBeekA62oTMxlzx
-----END RSA PRIVATE KEY-----
```

Private Key Passphrase

Specify if encrypted

- Copy and paste the Certificate and Private Key text into their respective fields. If the Private Key is encrypted type in the associated Passphrase.
- Click Save.
- A “Redirecting” message will appear. After a short time, the FieldServer GUI will open.

7.2.2 HTTPS with Default Untrusted Self-Signed TLS Certificate or HTTP with Built-in Payload Encryption

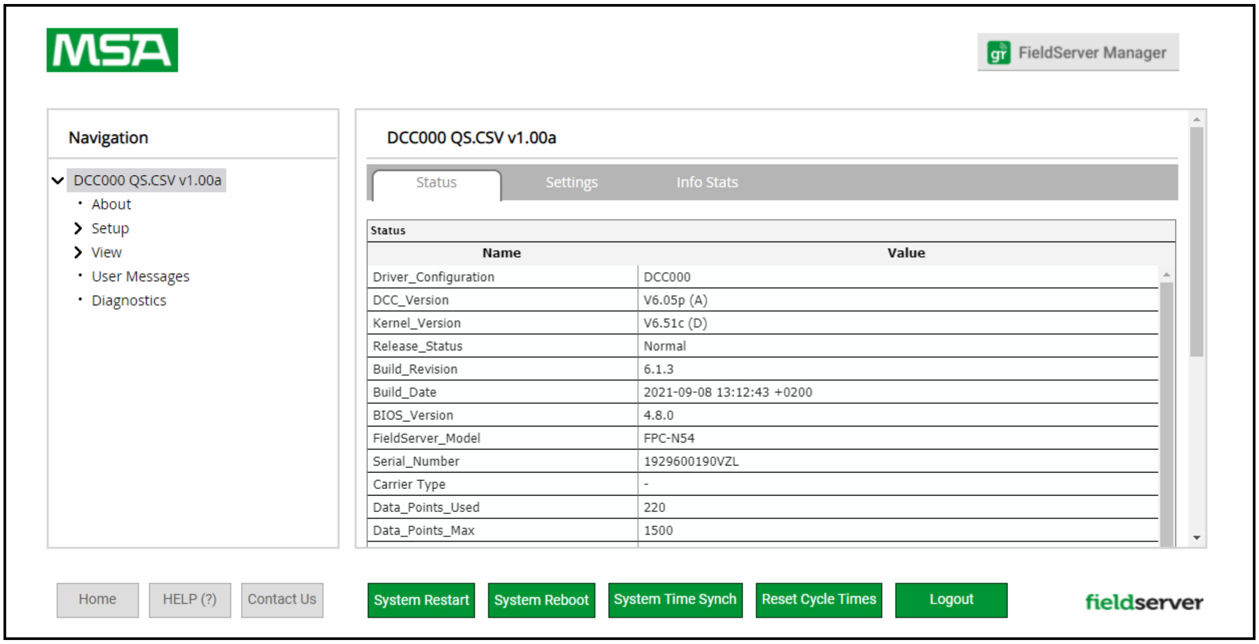
- Select one of these options and click the Save button.
- A “Redirecting” message will appear. After a short time, the FieldServer GUI will open.

8 Setup Network

8.1 Using FS-GUI to Input Network Settings

To navigate from the FS-GUI page to the Network Settings page follow the below instructions:

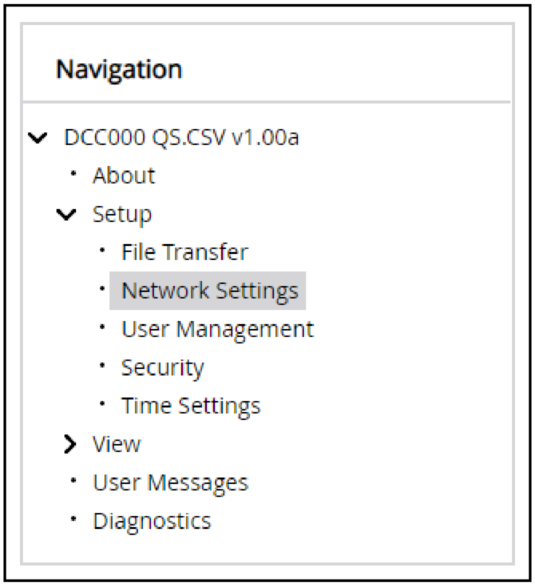
- Find the Navigation tree across the left side of the screen.
- Click the arrow next to the FieldServer title/CN number to expand the tree.



Status

Name	Value
Driver_Configuration	DCC000
DCC_Version	V6.05p (A)
Kernel_Version	V6.51c (D)
Release_Status	Normal
Build_Revision	6.1.3
Build_Date	2021-09-08 13:12:43 +0200
BIOS_Version	4.8.0
FieldServer_Model	FPC-N54
Serial_Number	1929600190VZL
Carrier Type	-
Data_Points_Used	220
Data_Points_Max	1500

- Click on the arrow next to Setup to expand the tree.
- Click on Network Settings.



8.1.1 Ethernet 1

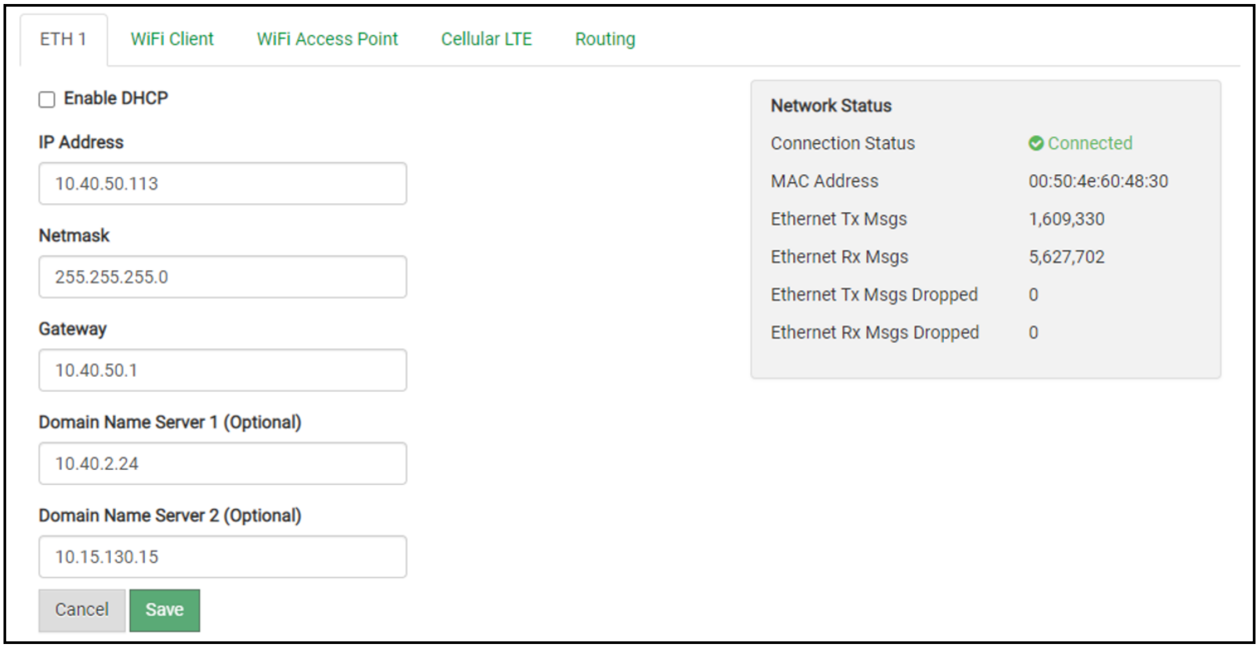
The ETH 1 section contains the wired network settings. To change the FieldServe IP Settings, follow these instructions:

- Enable DHCP to automatically assign IP Settings or modify the IP Settings manually as needed, via these fields: IP Address, Netmask, Default Gateway, and Domain Name Server1/2.

NOTE: If the FieldServer is connected to a router, the IP Gateway of the FieldServer should be set to the same IP Address of the router.

- Click Save to record and activate the new IP Address.
- Connect the FieldServer to the local network or router.

NOTE: The browser needs to be updated to the new IP Address of the FieldServer before the settings will be accessible again.



☐ Enable DHCP

IP Address
10.40.50.113

Netmask
255.255.255.0

Gateway
10.40.50.1

Domain Name Server 1 (Optional)
10.40.2.24

Domain Name Server 2 (Optional)
10.15.130.15

Network Status

Connection Status	✓ Connected
MAC Address	00:50:4e:60:48:30
Ethernet Tx Msgs	1,609,330
Ethernet Rx Msgs	5,627,702
Ethernet Tx Msgs Dropped	0
Ethernet Rx Msgs Dropped	0

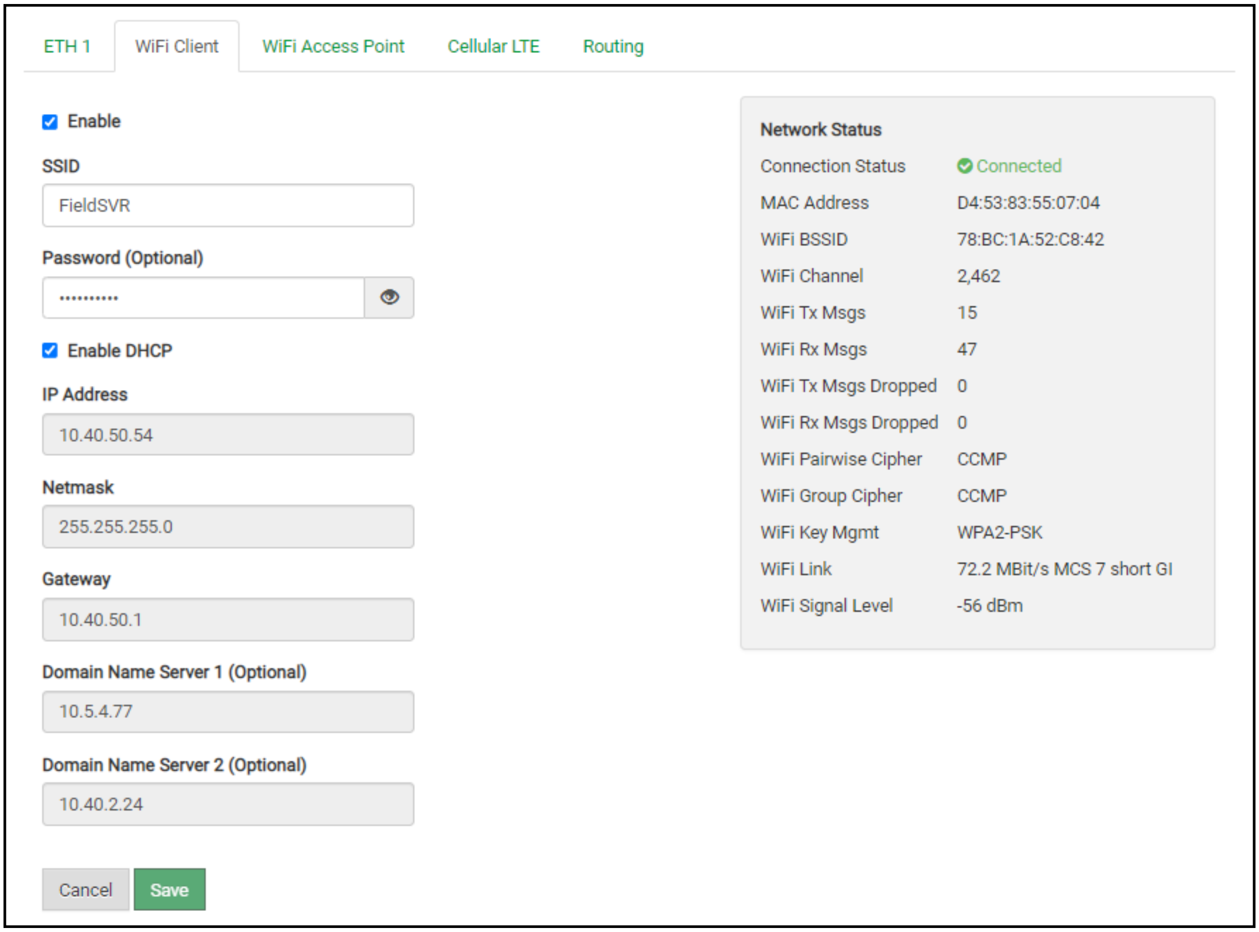
IP Setting Fields	Definition
Connection Status	Status of connection
MAC Address	Ethernet MAC Address
Tx/Rx Msgs	Number of transmitted and received messages
Tx/Rx Msgs Dropped	Number of unanswered Tx or Rx messages

8.1.2 Wi-Fi Client Settings

- Set the Wi-Fi Status to ENABLED for the ProtoAir to communicate with other devices via Wi-Fi.
- Enter the Wi-Fi SSID and Wi-Fi Password for the local wireless access point.
- Enable DHCP to automatically assign all Wi-Fi Client Settings fields or modify the Settings manually, via the fields immediately below the note (IP Address, Network, etc.).

NOTE: If connected to a router, set the IP gateway to the same IP Address as the router.

- Click the Save button to activate the new settings.
- Go to Routing (**Section 8.1.4 Routing Settings**) to set the default connection to Wi-Fi Client.



☑ Enable

SSID: FieldSVR

Password (Optional): ••••••••••

☑ Enable DHCP

IP Address: 10.40.50.54

Netmask: 255.255.255.0

Gateway: 10.40.50.1

Domain Name Server 1 (Optional): 10.5.4.77

Domain Name Server 2 (Optional): 10.40.2.24

Network Status

Connection Status	✓ Connected
MAC Address	D4:53:83:55:07:04
WiFi BSSID	78:BC:1A:52:C8:42
WiFi Channel	2,462
WiFi Tx Msgs	15
WiFi Rx Msgs	47
WiFi Tx Msgs Dropped	0
WiFi Rx Msgs Dropped	0
WiFi Pairwise Cipher	CCMP
WiFi Group Cipher	CCMP
WiFi Key Mgmt	WPA2-PSK
WiFi Link	72.2 MBit/s MCS 7 short GI
WiFi Signal Level	-56 dBm

Wi-Fi Client Fields	Definition
Connection Status	Status of connection
MAC Address, BSSID, Channel	Wi-Fi Client MAC Address, BSSID, and Channel
Tx/Rx Msgs	Number of transmitted and received messages
Tx/Rx Msgs Dropped	Number of unanswered Tx or Rx messages
Pairwise Cipher	Type of encryption used for unicast traffic
Group Cipher	Identifies the type of encryption used for multicast / broadcast traffic
Key Mgmt	Encryption type
Link	Connection speed
Signal Level	Signal level in dBm (see **Section 11.9 Wi-Fi and Cellular Signal Strength**)

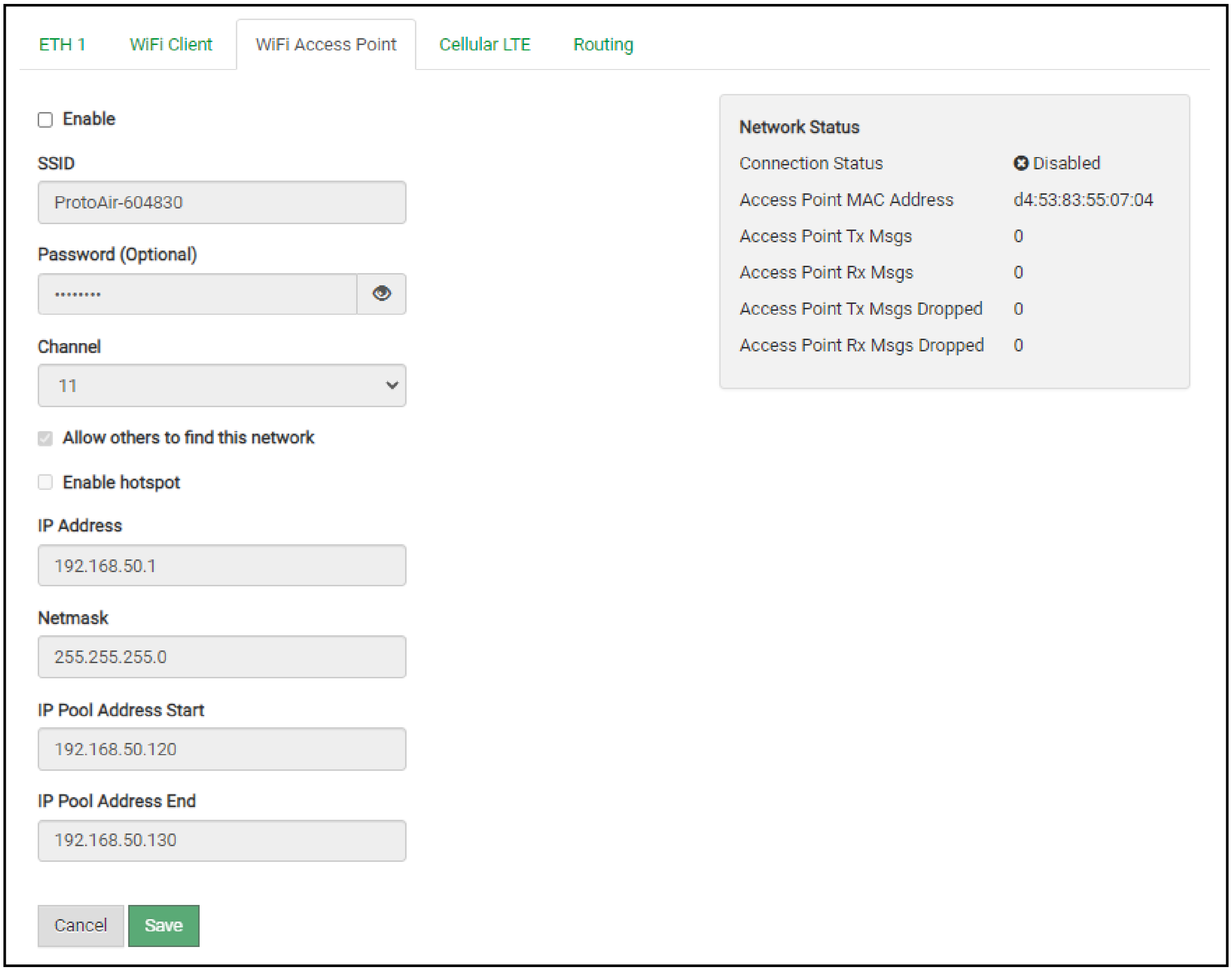
8.1.3 Wi-Fi Access Point Settings

- Check the Enable tick box to allow connecting to the ProtoAir via Wi-Fi Access Point.
- Modify the Settings manually as needed, via these fields: SSID, Password, Channel, IP Address, Netmask, IP Pool Address Start, and IP Pool Address End.

NOTE: The default channel is 11. The default IP Address is 192.168.50.1.

- Click the Save button to activate the new settings.

NOTE: If the webpage was open in a browser via Wi-Fi, the browser will need to be updated with the new Wi-Fi details before the webpage will be accessible again.



☐ Enable

SSID: ProtoAir-604830

Password (Optional): ••••••••

Channel: 11

☑ Allow others to find this network

☐ Enable hotspot

IP Address: 192.168.50.1

Netmask: 255.255.255.0

IP Pool Address Start: 192.168.50.120

IP Pool Address End: 192.168.50.130

Network Status

Connection Status	☒ Disabled
Access Point MAC Address	d4:53:83:55:07:04
Access Point Tx Msgs	0
Access Point Rx Msgs	0
Access Point Tx Msgs Dropped	0
Access Point Rx Msgs Dropped	0

Wi-Fi AP Fields	Definition
Connection Status	Status of connection
MAC Address	Access Point's MAC Address
Tx/Rx Msgs	Number of transmitted and received messages
Tx/Rx Msgs Dropped	Number of unanswered Tx or Rx messages

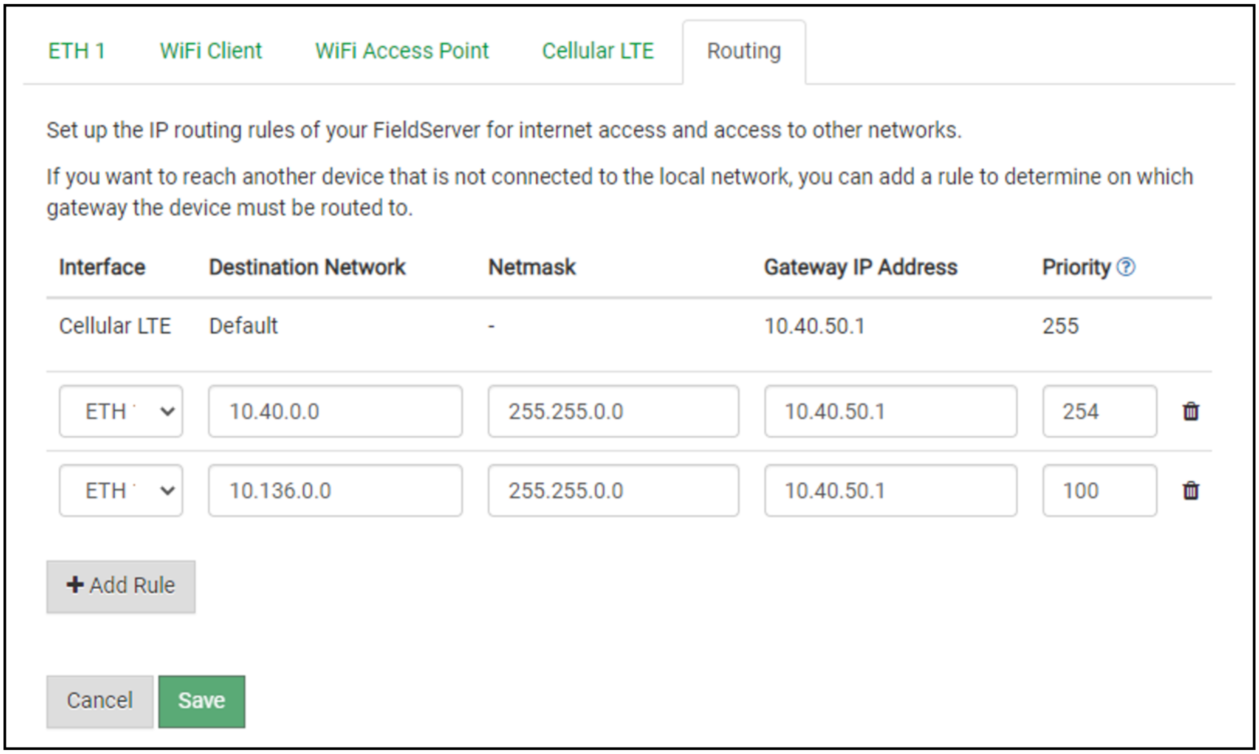
8.1.4 Routing Settings

The Routing settings make it possible to set up the IP routing rules for the FieldServer's internet and network connections.

NOTE: The default connection is ETH1.

- Select the default connection in the first row.
- Click the Add Rule button to add a new row and set a new Destination Network, Netmask and Gateway IP Address as needed.
- Set the Priority for each connection (1-255 with 1 as the highest priority and 255 as the lowest).
- Click the Save button to activate the new settings.

NOTE: If using Wi-Fi Client and not Ethernet, make the top priority rule a Wi-Fi Client connection.



Set up the IP routing rules of your FieldServer for internet access and access to other networks.

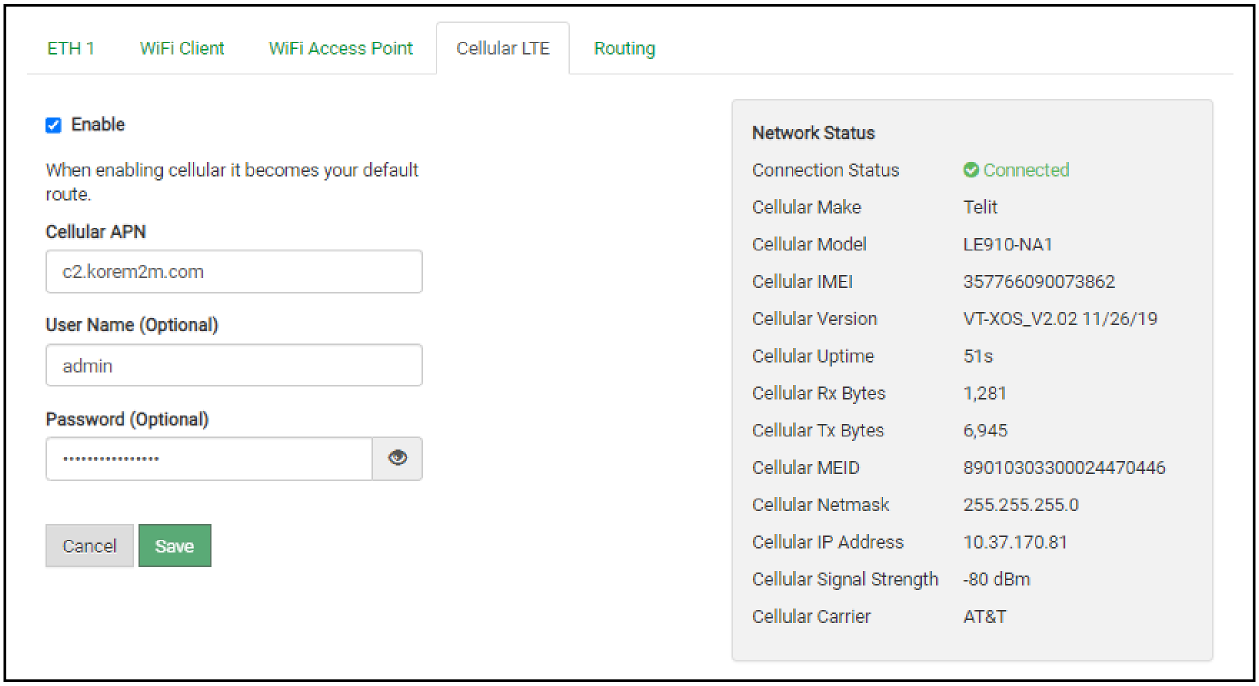
If you want to reach another device that is not connected to the local network, you can add a rule to determine on which gateway the device must be routed to.

Interface	Destination Network	Netmask	Gateway IP Address	Priority ?	
Cellular LTE	Default	-	10.40.50.1	255	
ETH	10.40.0.0	255.255.0.0	10.40.50.1	254	🗑
ETH	10.136.0.0	255.255.0.0	10.40.50.1	100	🗑

8.1.5 FPA-C4X: Cellular Settings

To change the Cellular settings, follow these instructions:

- Check the Enable tick box to allow connecting to the ProtoAir through the Grid.
- Modify the Settings manually as needed, via these fields: Cellular APN (see **Section 12.5 APN Table**), User Name, and Password.
- Click the Save button to activate the new settings.
- Power cycle the ProtoAir to update settings.



☑ Enable

When enabling cellular it becomes your default route.

Cellular APN: c2.korem2m.com

User Name (Optional): admin

Password (Optional): ••••••••••••••••

Network Status

Connection Status	✓ Connected
Cellular Make	Telit
Cellular Model	LE910-NA1
Cellular IMEI	357766090073862
Cellular Version	VT-XOS_V2.02 11/26/19
Cellular Uptime	51s
Cellular Rx Bytes	1,281
Cellular Tx Bytes	6,945
Cellular MEID	89010303300024470446
Cellular Netmask	255.255.255.0
Cellular IP Address	10.37.170.81
Cellular Signal Strength	-80 dBm
Cellular Carrier	AT&T

Cellular Fields	Definition
Connection Status	Status of connection
Make/Model/Version	Vendor, model and software version of the internal cellular chip
Uptime	Length of time connected
Tx/Rx Bytes	Receive and transmit bytes
MEID	Mobile Equipment ID; unique id for a device
IP Address/Netmask	Identifies the type of encryption used for multicast / broadcast traffic
Signal Strength	Strength of signal in dBm (see **Section 11.9 Wi-Fi and Cellular Signal Strength**)
Carrier	Cellular carrier provider

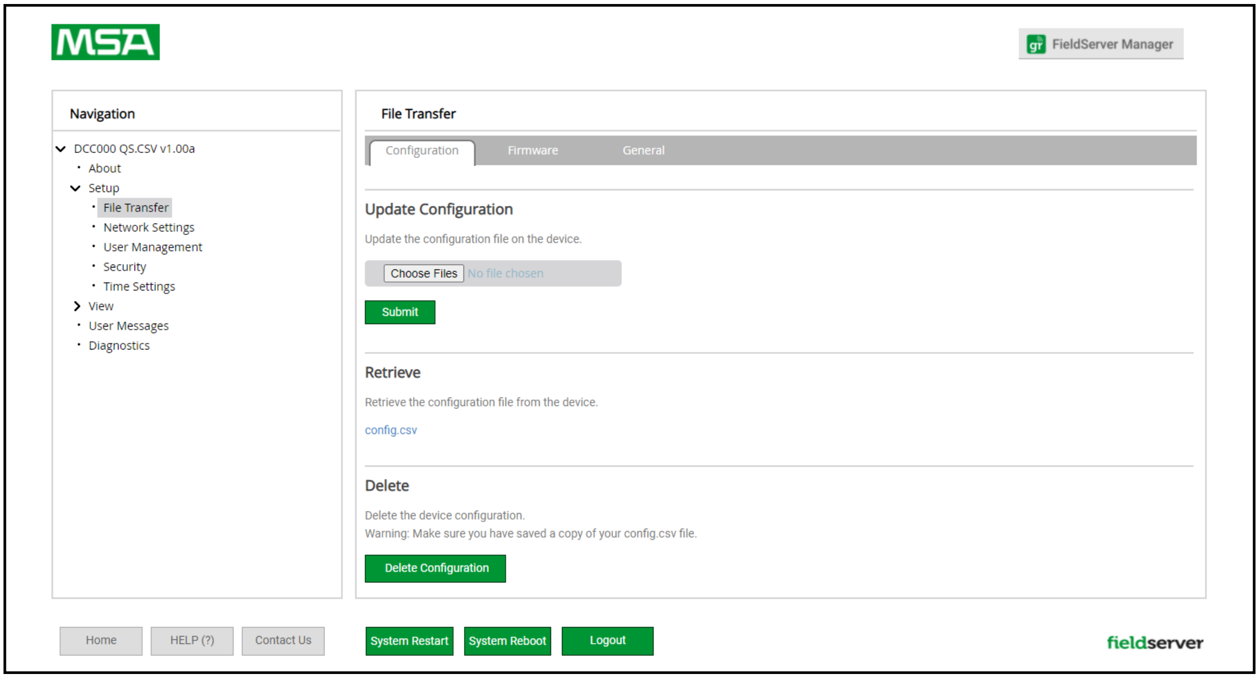
9 Configuring the ProtoAir

9.1 Retrieve the Sample Configuration File

The configuration of the ProtoAir is provided to the ProtoAir's operating system via a comma-delimited file called "CONFIG.CSV".

If a custom configuration was ordered, the ProtoAir will be programmed with the relevant device registers in the Config.csv file for the initial start-up. If not, the product is shipped with a sample config.csv that shows an example of the drivers ordered.

- In the main menu of the FS-GUI screen, go to "Setup", then "File Transfer", and finally "Retrieve".
- Click on "config.csv", and open or save the file.



Update Configuration

Update the configuration file on the device.

Retrieve

Retrieve the configuration file from the device.

Delete

Delete the device configuration.
Warning: Make sure you have saved a copy of your config.csv file.

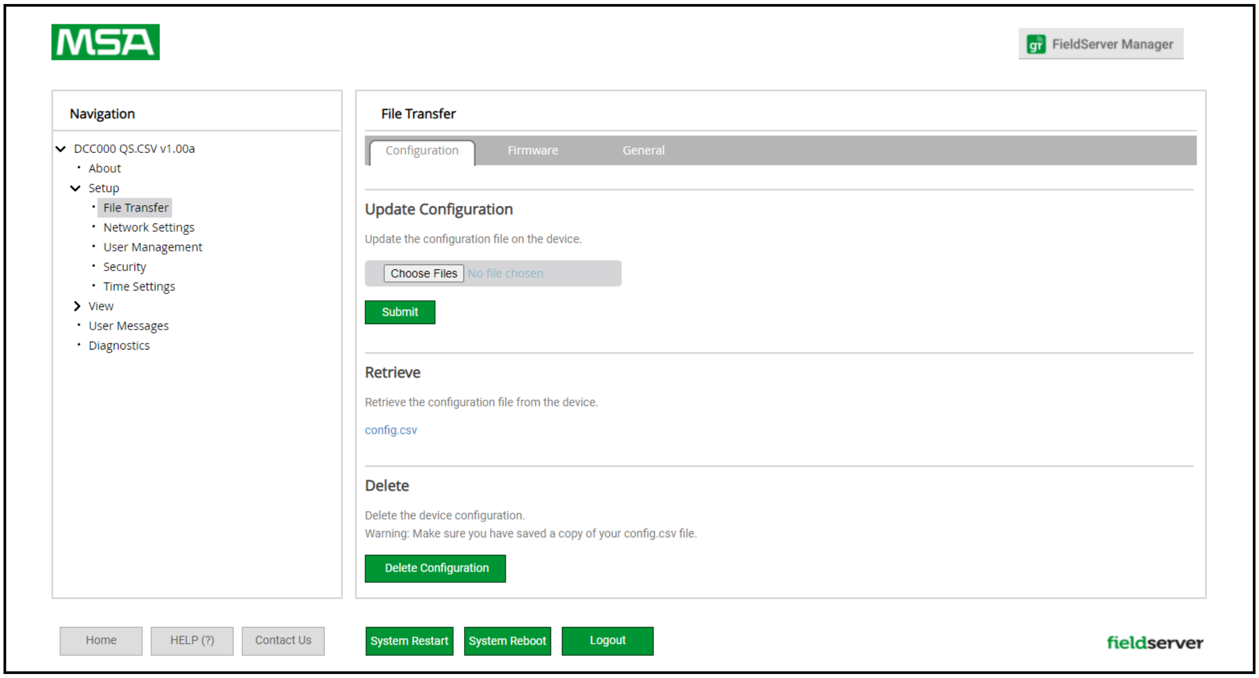
9.2 Change the Configuration File to Meet the Application

Refer to the FieldServer Configuration Manual in conjunction with the Driver supplements for information on configuring the ProtoAir.

9.3 Load the Updated Configuration File

9.3.1 Using the FS-GUI to Load a Configuration File

- In the main menu of the FS-GUI screen, click “Setup”, then “File Transfer” and finally “Update”.
- Browse and select the .csv file, open, then click “Submit”.



Update Configuration

Update the configuration file on the device.

Retrieve

Retrieve the configuration file from the device.

Delete

Delete the device configuration.

Warning: Make sure you have saved a copy of your config.csv file.

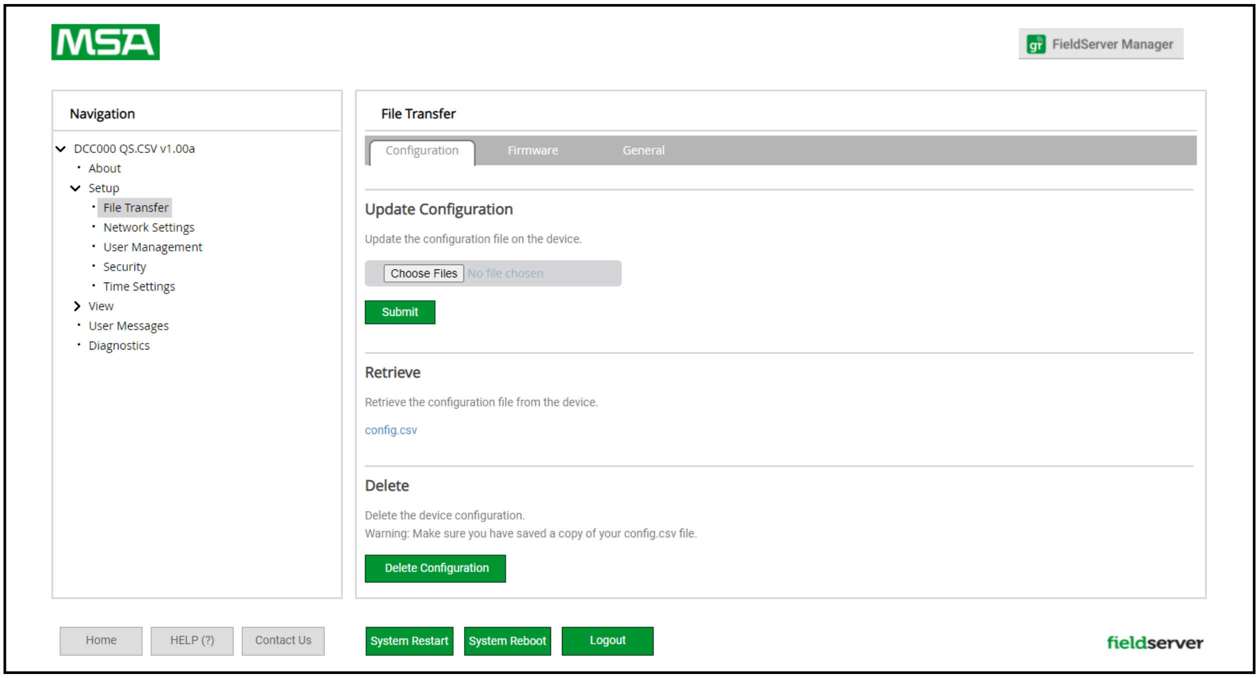
- Once download is complete, a message bar will appear confirming that the configuration was updated successfully.
- Click the System Restart Button to put the new file into operation.

NOTE: It is possible to do multiple downloads to the ProtoAir before resetting it.

9.3.2 Retrieve the Configuration File for Modification or Backup

To get a copy of the configuration file for modifying or backing up a configuration on a local computer, do the following:

- In the main menu of the FS-GUI screen, click “Setup”, then “File Transfer”.



Update Configuration

Update the configuration file on the device.

Retrieve

Retrieve the configuration file from the device.

Delete

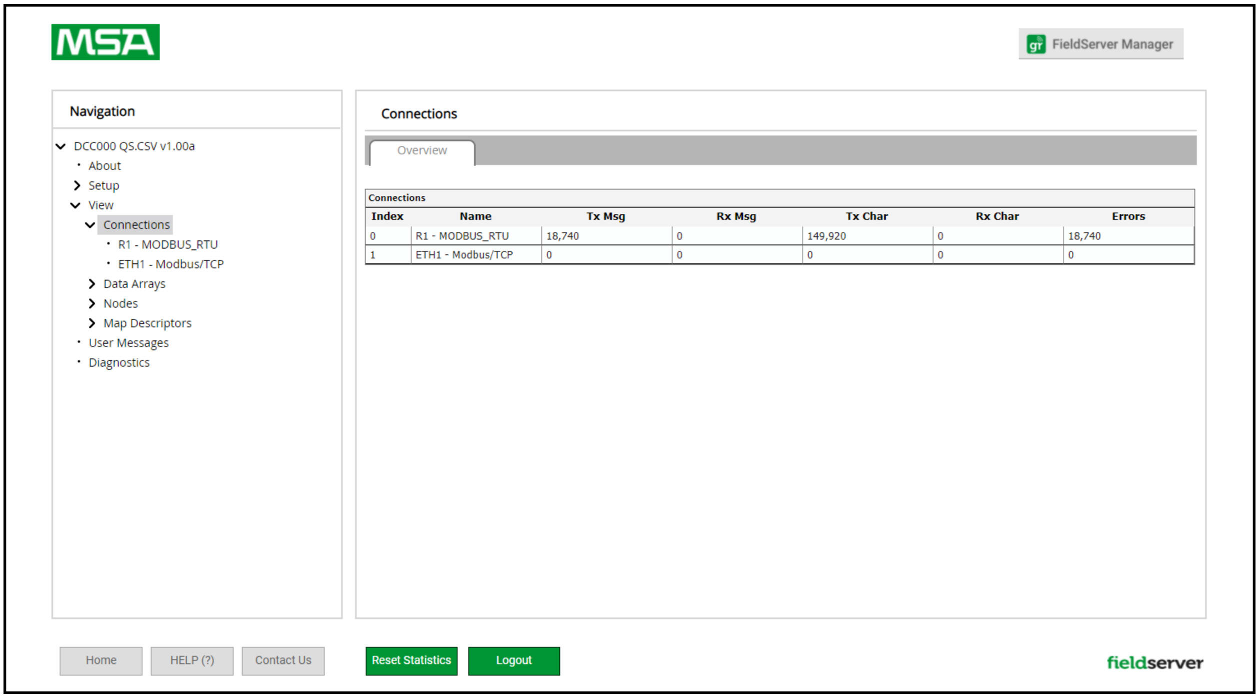
Delete the device configuration.
Warning: Make sure you have saved a copy of your config.csv file.

- Click the “config.csv” link under the “Retrieve” heading in the middle section of the screen.
  - The file will automatically download to the web browser’s default download location.
- Edit or store the file as desired.

NOTE: Before using any backup configuration file to reset the configuration settings, check that the backup file is not an old version.

9.4 Test and Commission the ProtoAir

- Connect the ProtoAir to the third party device(s), and test the application.
- From the landing page of the FS-GUI click on "View" in the navigation tree, then "Connections" to see the number of messages on each protocol.



Connections

Index	Name	Tx Msg	Rx Msg	Tx Char	Rx Char	Errors
0	R1 - MODBUS_RTU	18,740	0	149,920	0	18,740
1	ETH1 - Modbus/TCP	0	0	0	0	0

NOTE: For troubleshooting assistance refer to Section 11 Troubleshooting, or any of the troubleshooting appendices in the related driver supplements and configuration manual. MSA Safety also offers a technical support on the MSA Safety website, which contains a significant number of resources and documentation that may be of assistance.

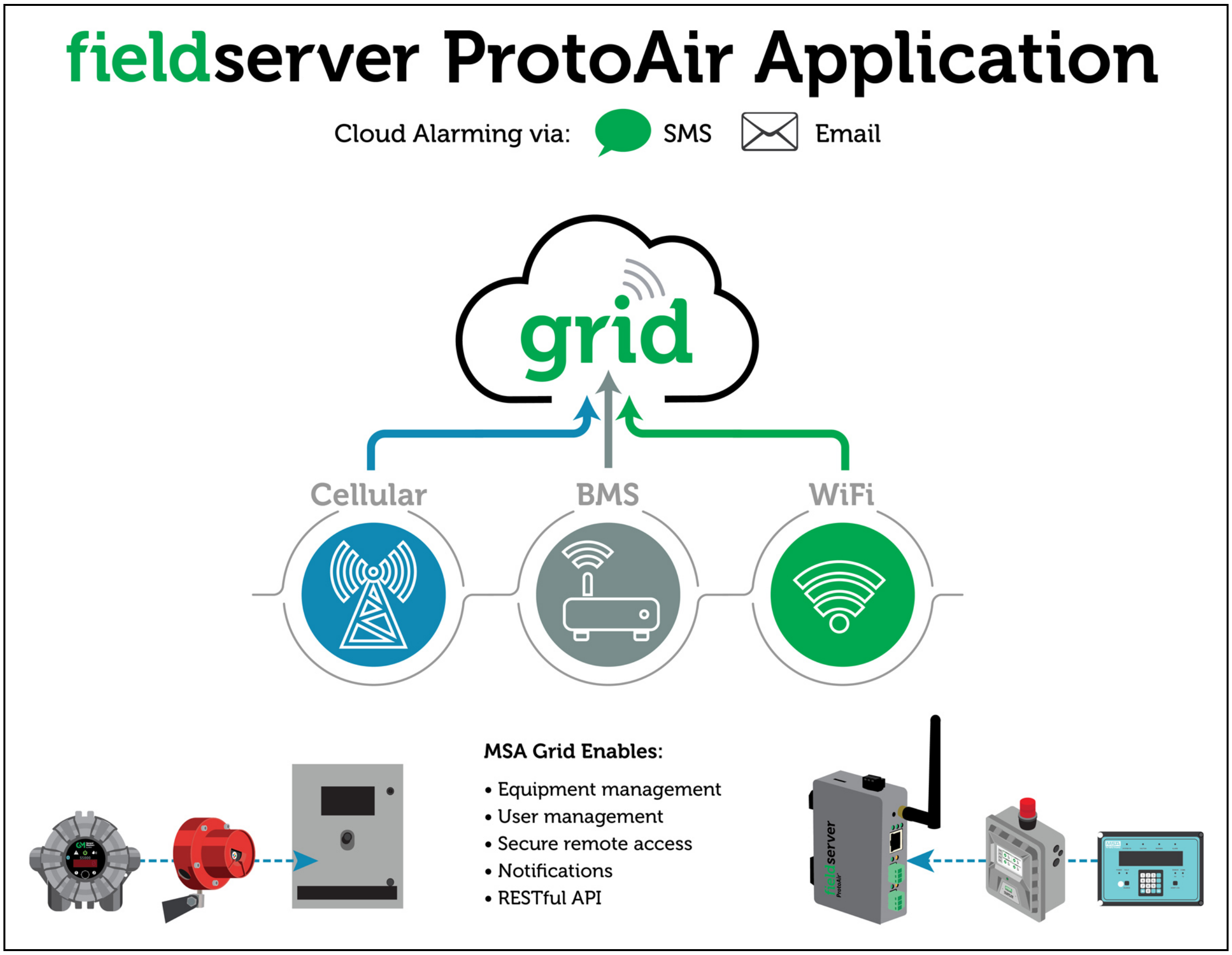
9.4.1 Accessing the FieldServer Manager

NOTE: The FieldServer Manager tab FieldServer Manager **(see image above) allows users to connect to the Grid, MSA Safety's device cloud solution for IIoT. The FieldServer Manager enables secure remote connection to field devices through a FieldServer and its local applications for configuration, management, maintenance. For more information about the FieldServer Manager, refer to the MSA Grid - FieldServer Manager Start-up Guide.**

10 Applications

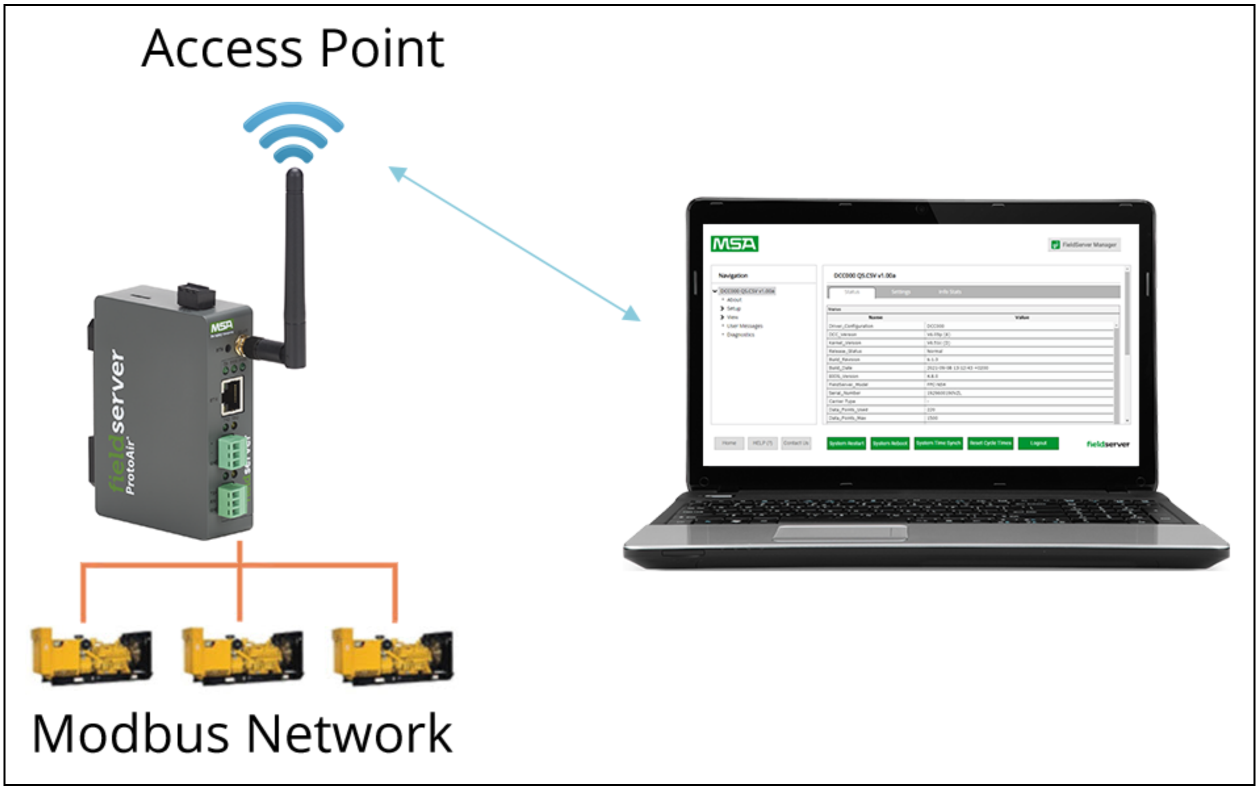
10.1 Connecting to the Network Through Wi-Fi

The ProtoAir can connect customer devices to the local Ethernet Network via Wi-Fi signal and connect customer devices to the cloud via cellular for remote accessibility.



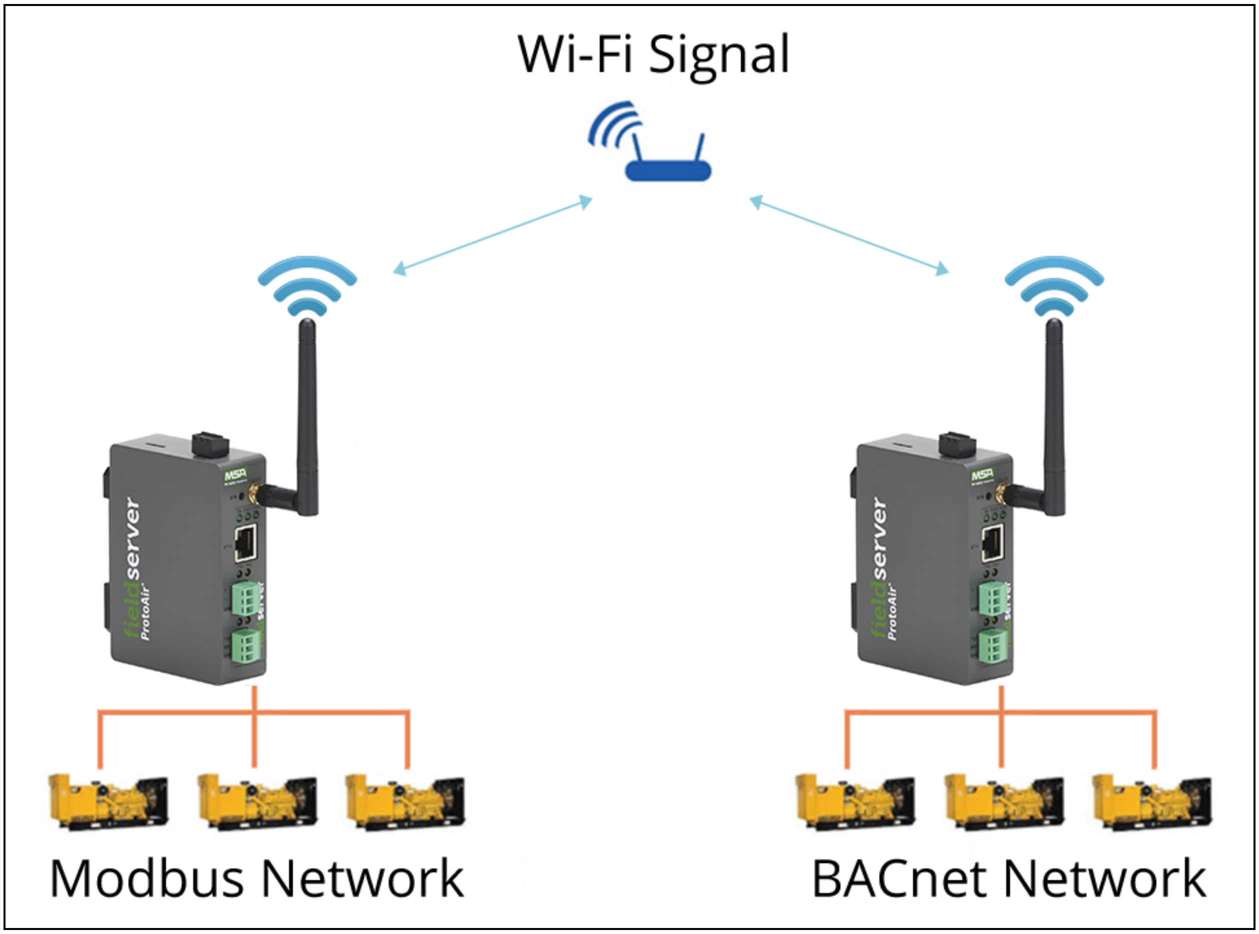
10.2 Connecting to Devices via Access Point

Customer devices setup on the ProtoAir can be connected to via the ProtoAir’s dedicated Access Point.



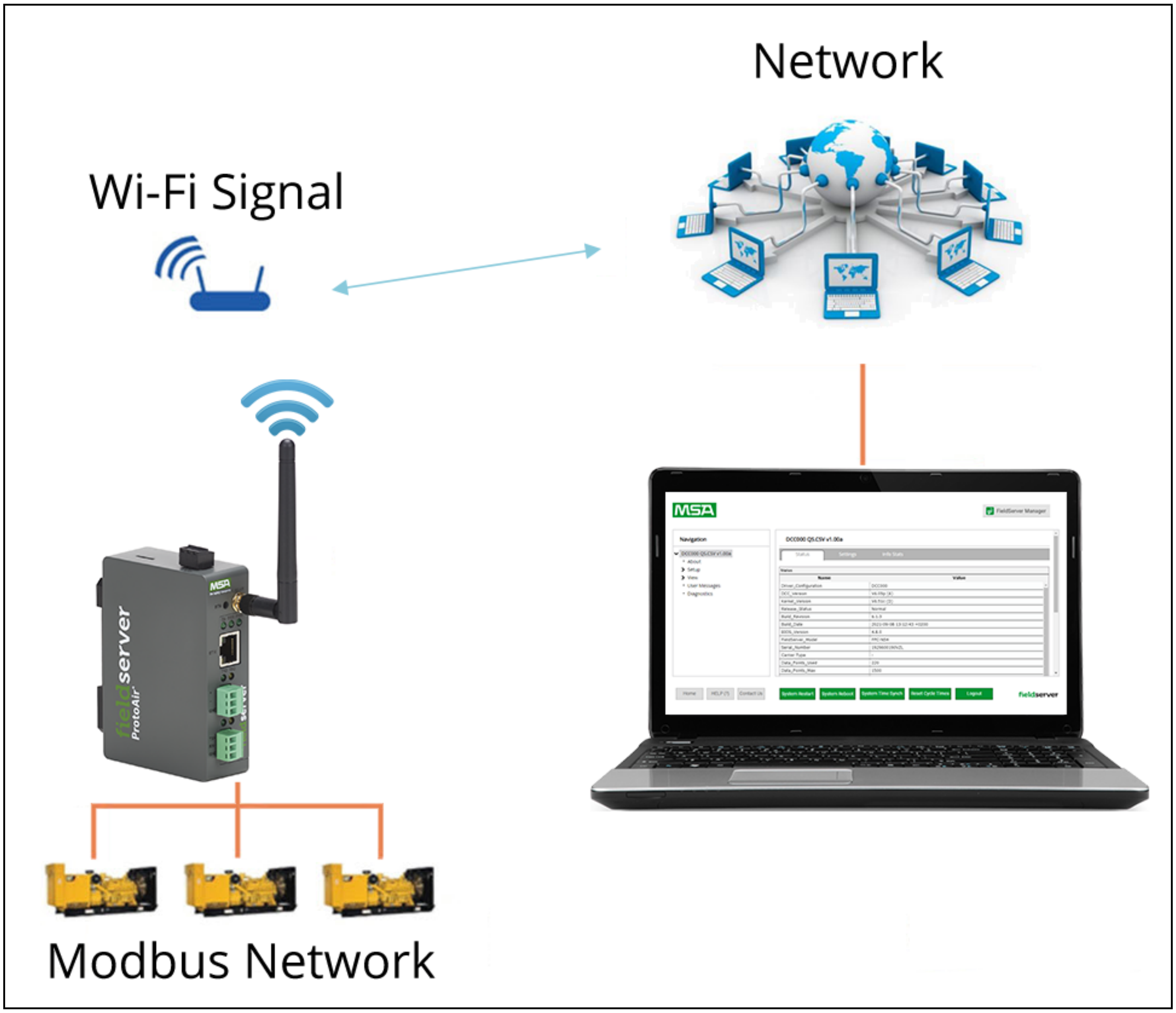
10.3 Device Communications via Wi-Fi

The ProtoAir can connect multiple customer devices via Wi-Fi.



10.4 Connecting Devices to the Network

The ProtoAir can connect devices to the local Network via Wi-Fi.



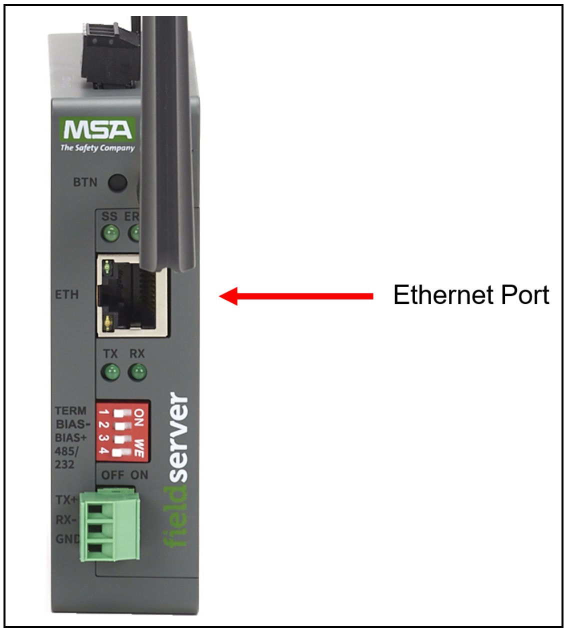
11 Troubleshooting

11.1 Communicating with the ProtoAir Over the Network

- Confirm that the network cabling is correct.
- Confirm that the computer network card is operational and correctly configured.
- Confirm that there is an Ethernet adapter installed in the PC's Device Manager List, and that it is configured to run the TCP/IP protocol.
- Check that the IP netmask of the PC matches the ProtoAir. The Default IP Address of the ProtoAir is 192.168.1.X, Subnet Mask is 255.255.255.0.
  - Go to Start|Run
  - Type in "ipconfig"
  - The account settings should be displayed
  - Ensure that the IP Address is 102.168.1.X and the netmask 255.255.255.0
- Ensure that the PC and ProtoAir are on the same IP Network, or assign a Static IP Address to the PC on the 192.168.1.X network.

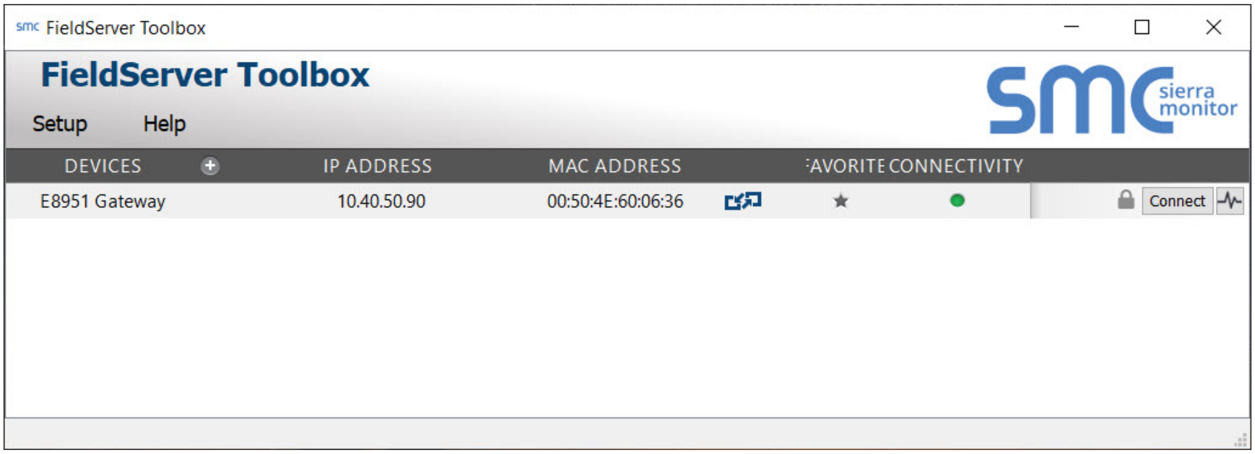
11.2 Lost or Incorrect IP Address

- Ensure that FieldServer Toolbox is loaded onto the local PC. Otherwise, download the FieldServer-Toolbox.zip via the MSA Safety website.
- Extract the executable file and complete the installation.



Ethernet Port

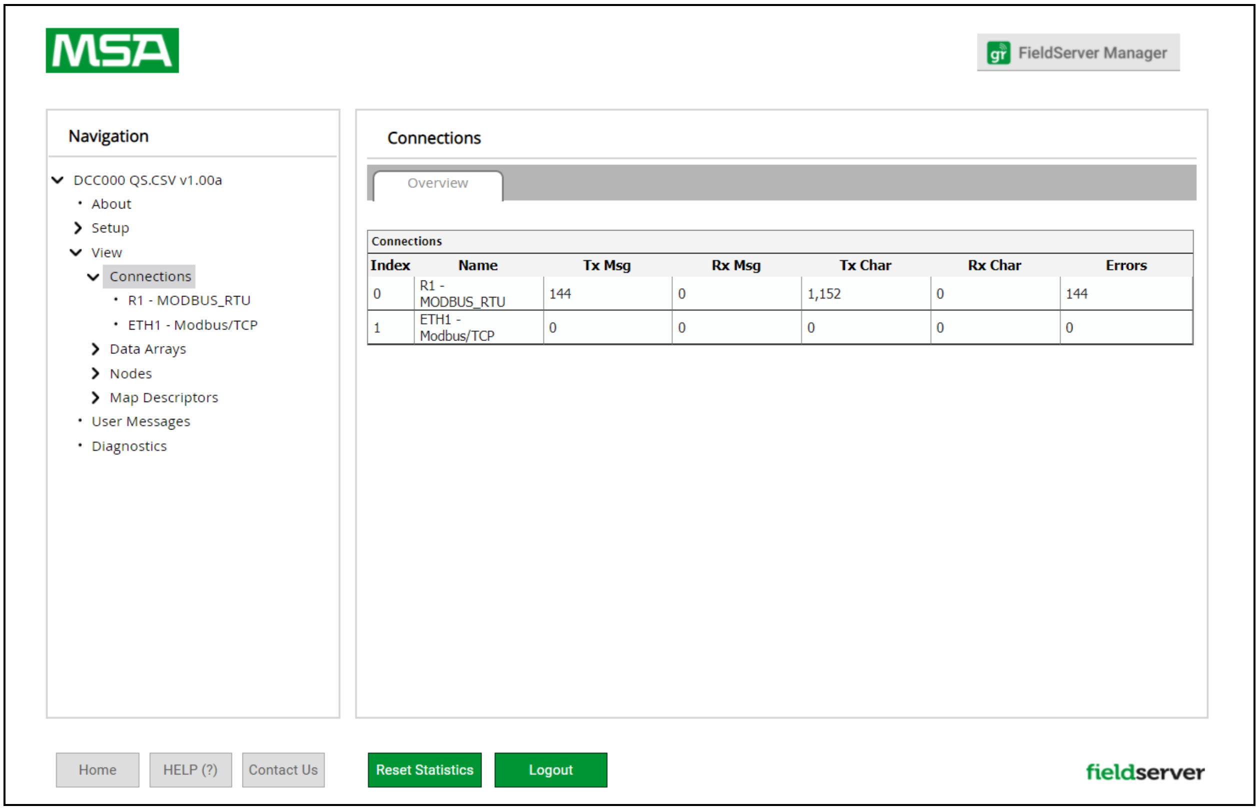
- Connect a standard Cat-5 Ethernet cable between the user's PC and ProtoAir.
- Double click on the FS Toolbox Utility and click Discover Now on the splash page.
- Check for the IP Address of the desired gateway.



DEVICES	IP ADDRESS	MAC ADDRESS	:AVORITE	CONNECTIVITY	
E8951 Gateway	10.40.50.90	00:50:4E:60:06:36	★	●	Connect

11.3 Viewing Diagnostic Information

- Type the IP Address of the FieldServer into the web browser or use the FieldServer Toolbox to connect to the FieldServer.
- Click on Diagnostics and Debugging Button, then click on view, and then on connections.
- If there are any errors showing on the Connection page, refer to **Section 11.4 Checking Wiring and Settings** for the relevant wiring and settings.



Connections

Index	Name	Tx Msg	Rx Msg	Tx Char	Rx Char	Errors
0	R1 - MODBUS_RTU	144	0	1,152	0	144
1	ETH1 - Modbus/TCP	0	0	0	0	0

11.4 Checking Wiring and Settings

No COMS on the Serial side. If the Tx/Rx LEDs are not flashing rapidly then there is a COM issue. To fix this problem, check the following:

- Visual observations of LEDs on the ProtoAir. (**Section 11.6 LED Functions**)
- Check baud rate, parity, data bits, stop bits.
- Check device address.
- Verify wiring.
- Verify the device is connected to the same subnet as the ProtoAir.

Field COM problems:

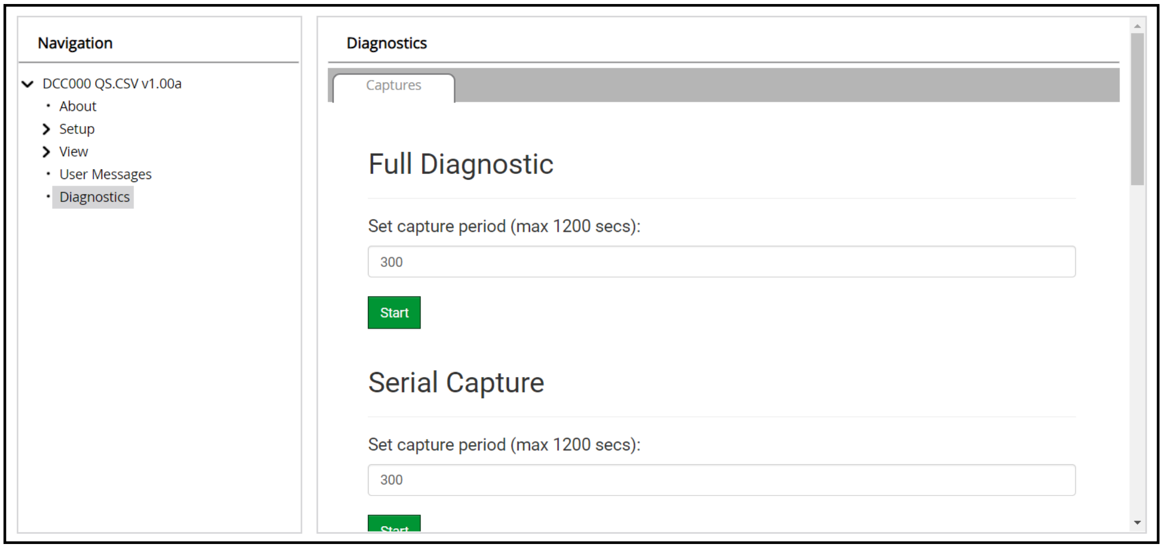
- Visual observations of LEDs on the ProtoAir. (**Section 11.6 LED Functions**)
- Verify wiring.
- Verify IP Address setting.

NOTE: If the problem still exists, a Diagnostic Capture needs to be taken and sent to support. (Section 11.5 Taking a FieldServer Diagnostic Capture)

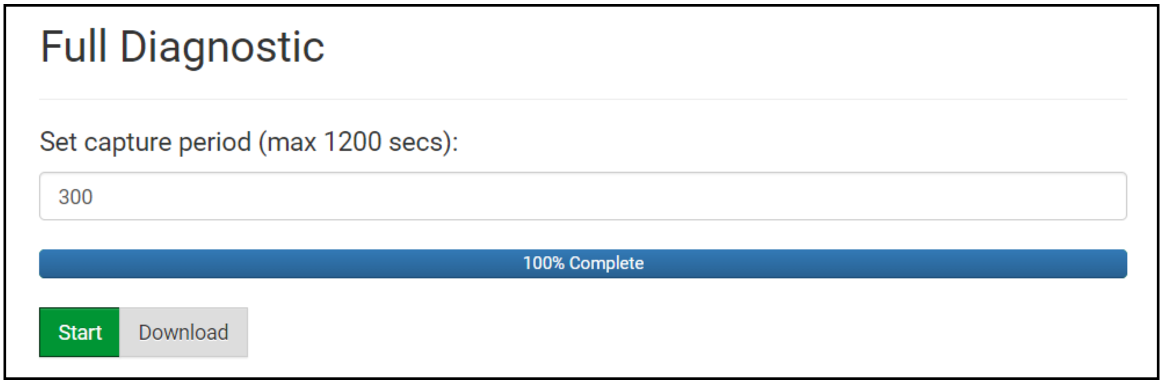
11.5 Taking a FieldServer Diagnostic Capture

When there is a problem on-site that cannot easily be resolved, perform a Diagnostic Capture before contacting support. Once the Diagnostic Capture is complete, email it to technical support. The Diagnostic Capture will accelerate diagnosis of the problem.

- Access the FieldServer Diagnostics page via one of the following methods:
  - Open the FieldServer FS-GUI page and click on Diagnostics in the Navigation panel
  - Open the FieldServer Toolbox software and click the diagnose icon ⚕ of the desired device



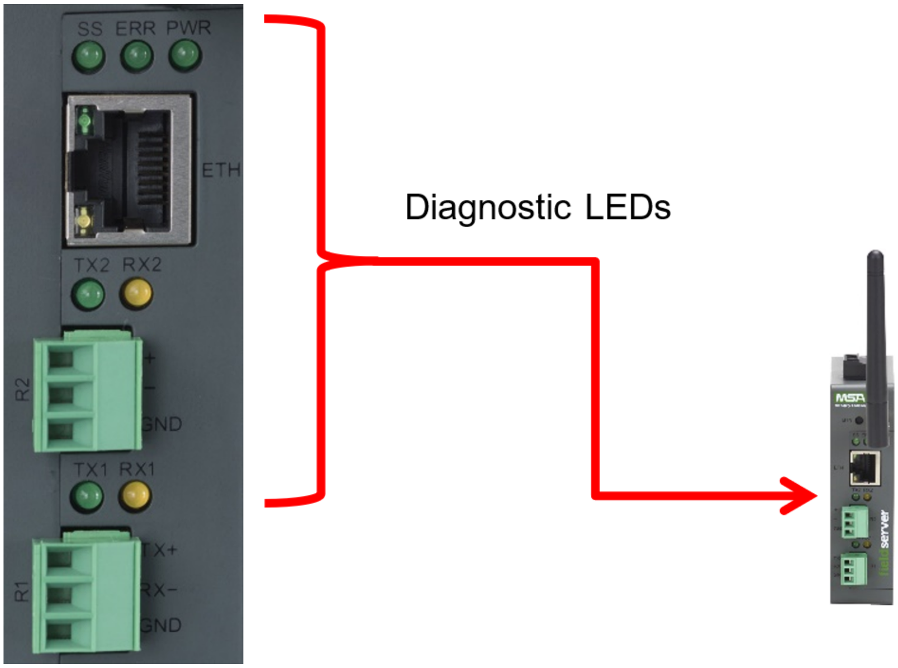
- Go to Full Diagnostic and select the capture period.
- Click the Start button under the Full Diagnostic heading to start the capture.
  - When the capture period is finished, a Download button will appear next to the Start button

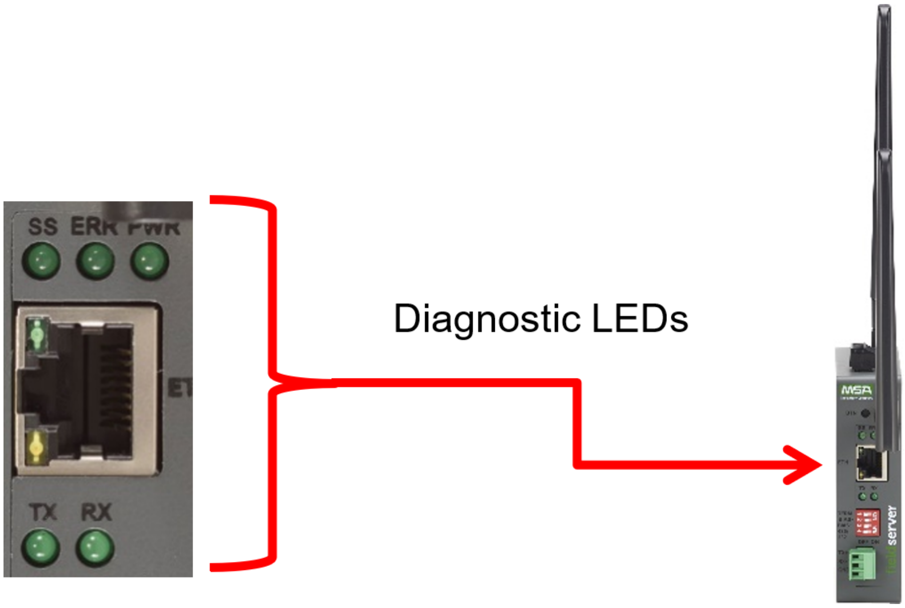


- Click Download for the capture to be downloaded to the local PC.
- Email the diagnostic zip file to technical support (smc-support.emea@msasafety.com).

NOTE: Diagnostic captures of BACnet MS/TP communication are output in a ".PCAP" file extension which is compatible with Wireshark.

11.6 LED Functions





Tag	Description
SS	The SS LED will flash once a second to indicate that the bridge is in operation.
ERR	The SYS ERR LED will go on solid indicating there is a system error. If this occurs, immediately report the related "system error" shown in the error screen of the FS-GUI interface to support for evaluation.
PWR	This is the power light and should always be steady green when the unit is powered.
RX	The RX LED will flash when a message is received on the serial port on the 3-pin connector. If the serial port is not used, this LED is non-operational. **For the FPA-W44**, RX1 applies to the R1 connection while RX2 applies to the R2 connection.
TX	The TX LED will flash when a message is sent on the serial port on the 3-pin connector. If the serial port is not used, this LED is non-operational. **For the FPA-W44**, TX1 applies to the R1 connection while TX2 applies to the R2 connection.

11.7 Factory Reset Instructions

For instructions on how to reset a FieldServer back to its factory released state, see ENOTE FieldServer Next Gen Recovery.

11.8 Internet Browser Software Support

The following web browsers are supported:

- Chrome Rev. 57 and higher
- Firefox Rev. 35 and higher
- Microsoft Edge Rev. 41 and higher
- Safari Rev. 3 and higher

NOTE: Internet Explorer is no longer supported as recommended by Microsoft.

NOTE: Computer and network firewalls must be opened for Port 80 to allow FieldServer GUI to function.

11.9 Wi-Fi and Cellular Signal Strength

Wi-Fi	Cellular
<60dBm – Excellent	< 60dBm – Excellent
<70dBm – Very good	<70dBm – Very good
<80dBm – Good	<80dBm – Good
>80dBm – Weak	<90dBm – Weak
	>90dBm – Spotty; not good for data

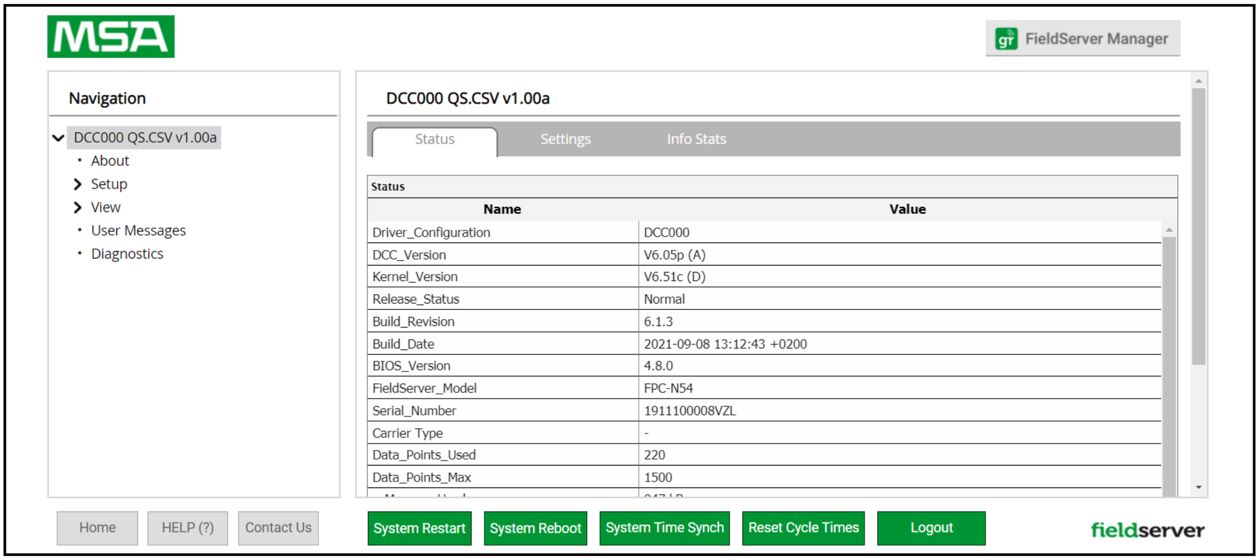
NOTE: If the signal is weak or spotty, try to improve the signal strength by checking the antenna and the FieldServer position.

12 Additional Information

12.1 Change Web Server Security Settings After Initial Setup

NOTE: Any changes will require a FieldServer reboot to take effect.

- Navigate to the FS-GUI page.
- Click Setup in the Navigation panel.

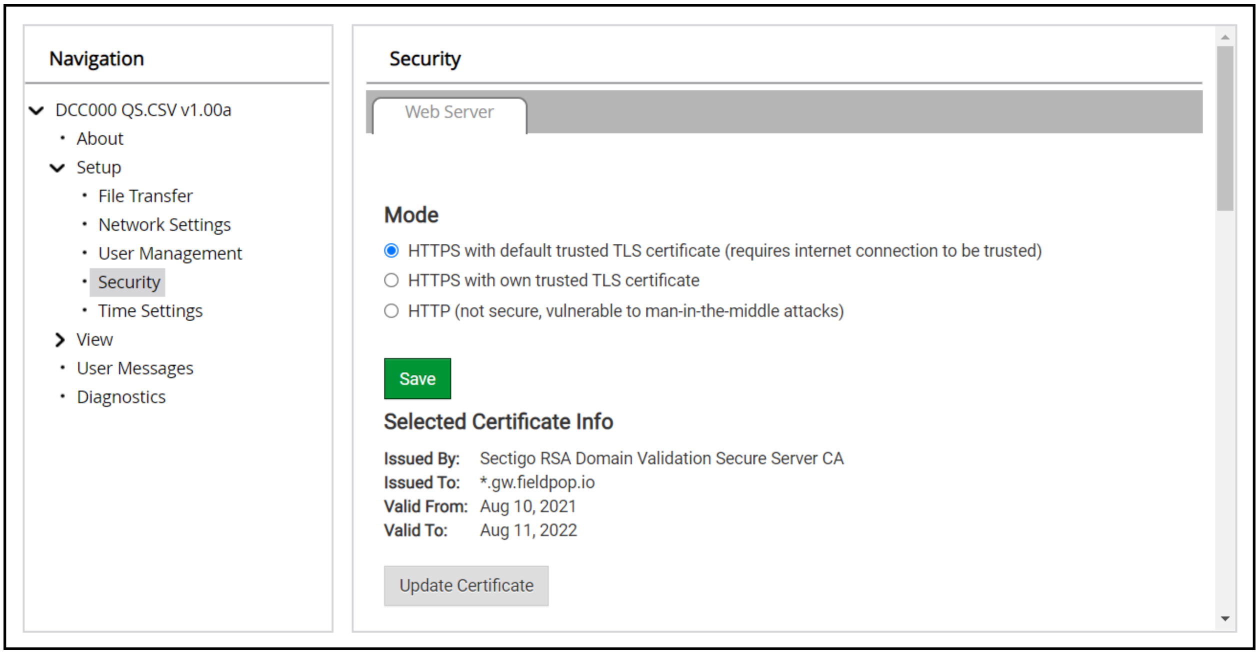


Status

Name	Value
Driver_Configuration	DCC000
DCC_Version	V6.05p (A)
Kernel_Version	V6.51c (D)
Release_Status	Normal
Build_Revision	6.1.3
Build_Date	2021-09-08 13:12:43 +0200
BIOS_Version	4.8.0
FieldServer_Model	FPC-N54
Serial_Number	1911100008VZL
Carrier Type	-
Data_Points_Used	220
Data_Points_Max	1500

12.1.1 Change Security Mode

- Click Security in the Navigation panel.



Mode

● HTTPS with default trusted TLS certificate (requires internet connection to be trusted)

○ HTTPS with own trusted TLS certificate

○ HTTP (not secure, vulnerable to man-in-the-middle attacks)

Selected Certificate Info

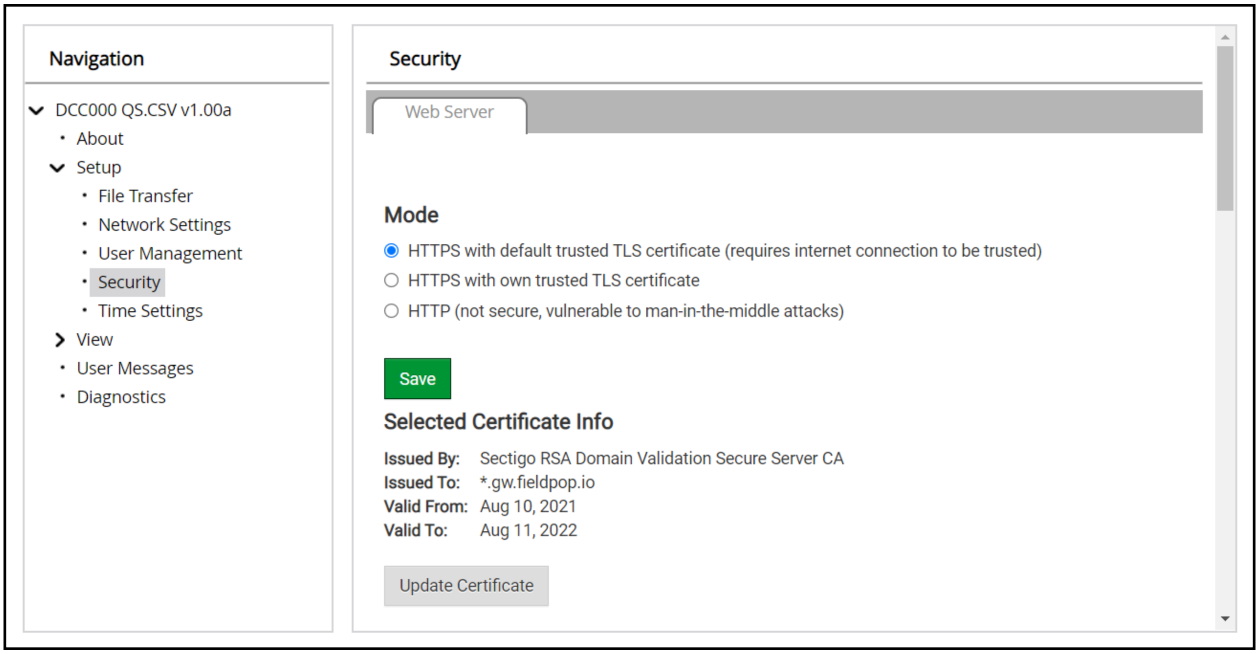
Issued By:	Sectigo RSA Domain Validation Secure Server CA
Issued To:	*.gw.fieldpop.io
Valid From:	Aug 10, 2021
Valid To:	Aug 11, 2022

- Click the Mode desired.
  - If HTTPS with own trusted TLS certificate is selected, follow instructions in **Section 7.2.1 HTTPS with Own Trusted TLS Certificate**
- Click the Save button.

12.1.2 Edit the Certificate Loaded onto the FieldServer

NOTE: A loaded certificate will only be available if the security mode was previously setup as HTTPS with own trusted TLS certificate.

- Click Security in the Navigation panel.



Mode

● HTTPS with default trusted TLS certificate (requires internet connection to be trusted)
○ HTTPS with own trusted TLS certificate
○ HTTP (not secure, vulnerable to man-in-the-middle attacks)

Selected Certificate Info

Issued By: Sectigo RSA Domain Validation Secure Server CA
Issued To: *.gw.fieldpop.io
Valid From: Aug 10, 2021
Valid To: Aug 11, 2022

- Click the Edit Certificate button to open the certificate and key fields.
- Edit the loaded certificate or key text as needed.
- Click Save.

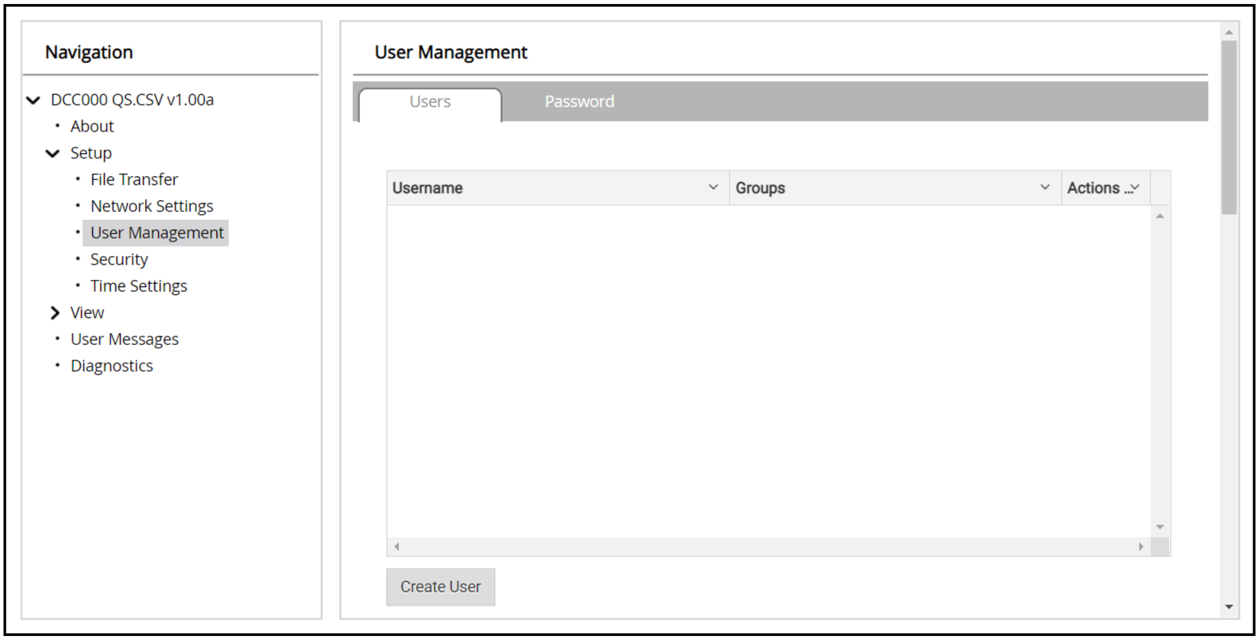
12.2 Change User Management Settings

- From the FS-GUI page, click Setup in the Navigation panel.
- Click User Management in the navigation panel.

NOTE: If the passwords are lost, the unit can be reset to factory settings to reinstate the default unique password on the label. For recovery instructions, see the FieldServer Next Gen Recovery document. If the default unique password is lost, then the unit must be mailed back to the factory.

NOTE: Any changes will require a FieldServer reboot to take effect.

- Check that the Users tab is selected.



User Types:

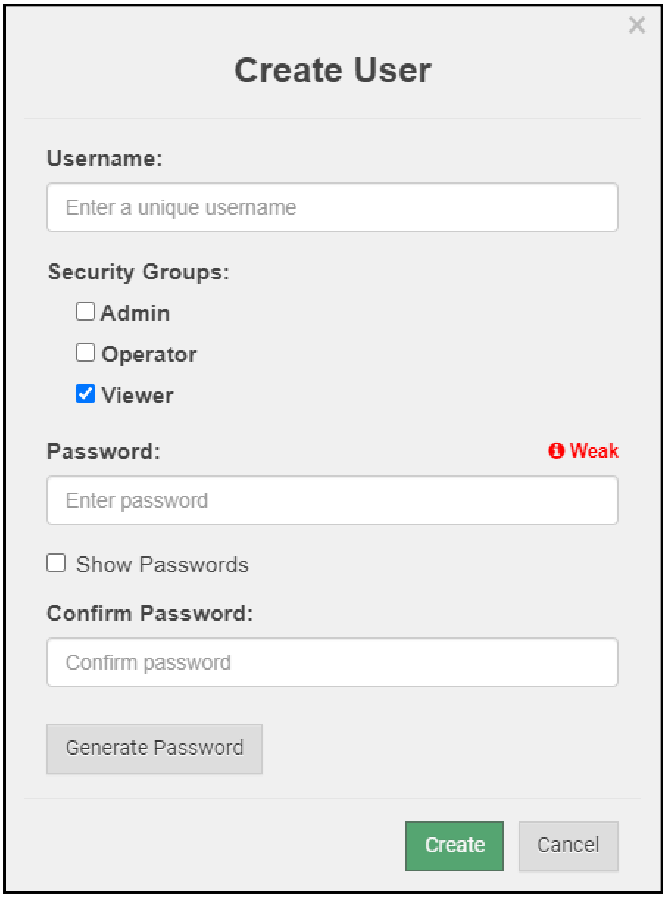
Admin – Can modify and view any settings on the FieldServer.

Operator – Can modify and view any data in the FieldServer array(s).

Viewer – Can only view settings/readings on the FieldServer.

12.2.1 Create Users

- Click the Create User button.



Create User

Username:

Enter a unique username

Security Groups:

☐ Admin

☐ Operator

☑ Viewer

Password: Weak

Enter password

☐ Show Passwords

Confirm Password:

Confirm password

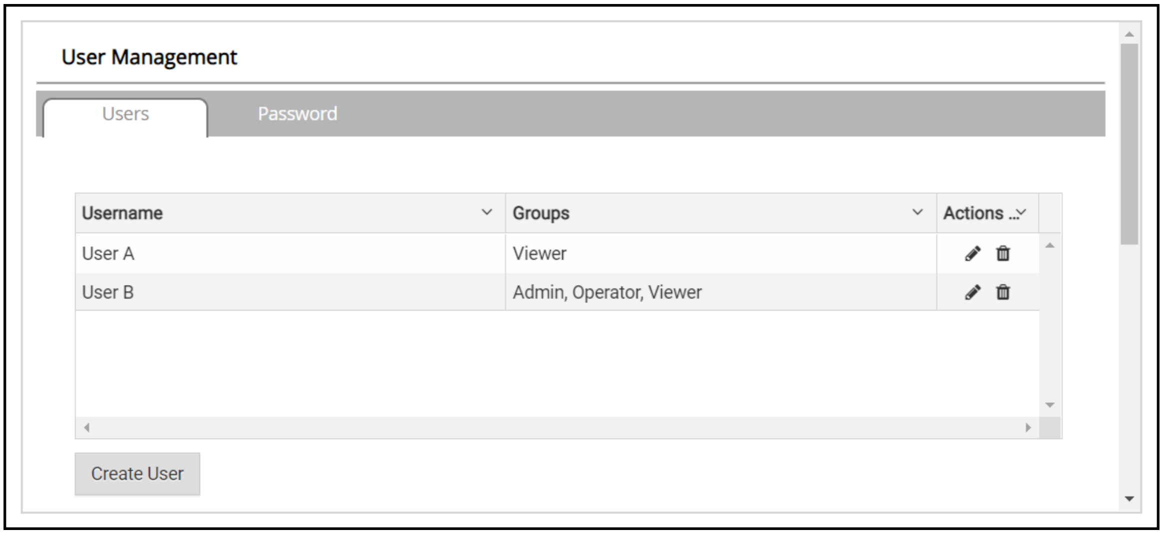
- Enter the new User fields: Name, Security Group and Password.
  - **User details are hashed and salted**

NOTE: The password must meet the minimum complexity requirements. An algorithm automatically checks the password entered and notes the level of strength on the top right of the Password text field.

- Click the Create button.
- Once the Success message appears, click OK.

12.2.2 Edit Users

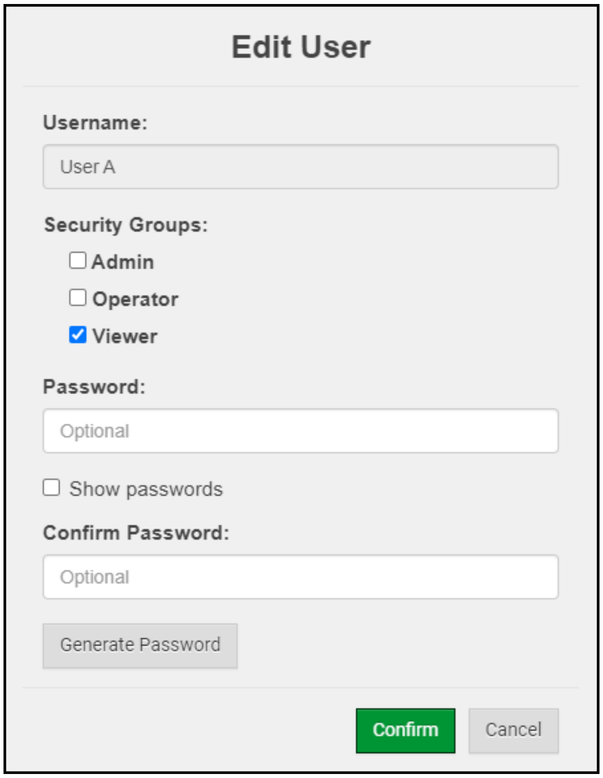
- Click the pencil icon next to the desired user to open the User Edit window.



User Management

Username	Groups	Actions
User A	Viewer	✎ 🗑
User B	Admin, Operator, Viewer	✎ 🗑

- Once the User Edit window opens, change the User Security Group and Password as needed.



Edit User

Username: User A

Security Groups:

☐ Admin
☐ Operator
☑ Viewer

Password: Optional

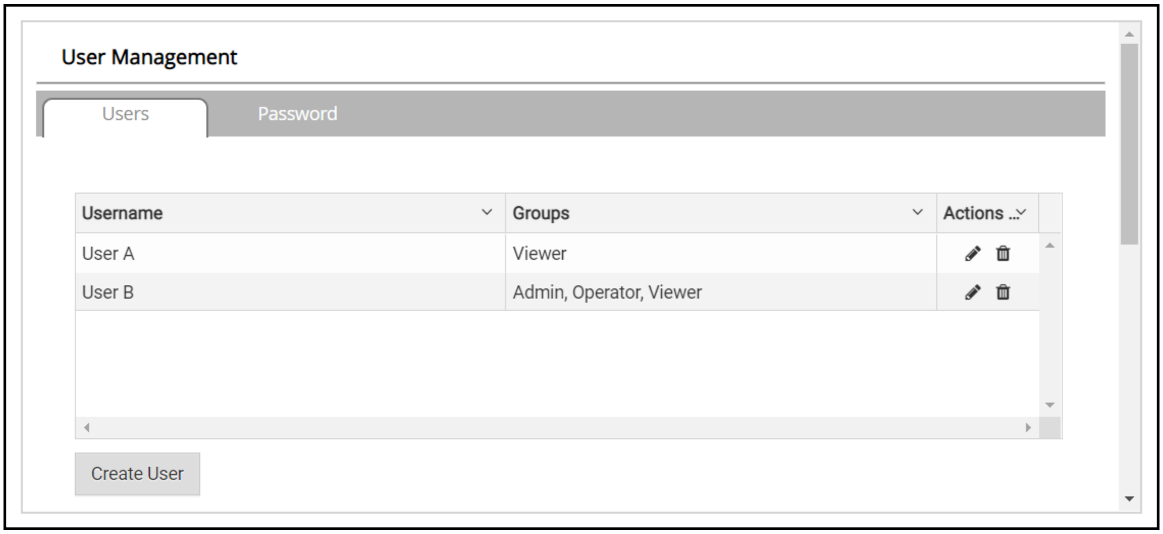
☐ Show passwords

Confirm Password: Optional

- Click Confirm.
- Once the Success message appears, click OK.

12.2.3 Delete Users

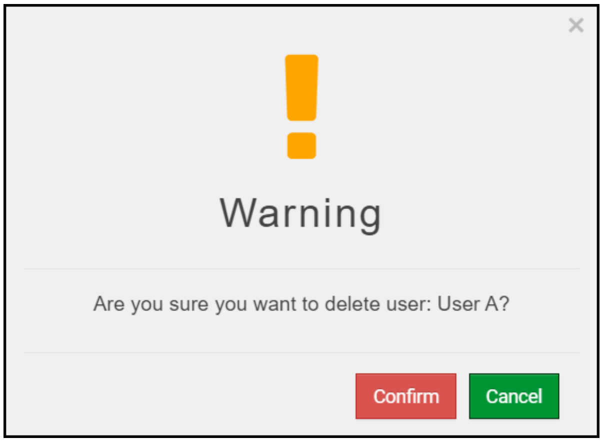
- Click the trash can icon next to the desired user to delete the entry.



User Management

Username	Groups	Actions ...
User A	Viewer	✎ 🗑
User B	Admin, Operator, Viewer	✎ 🗑

- When the warning message appears, click Confirm.

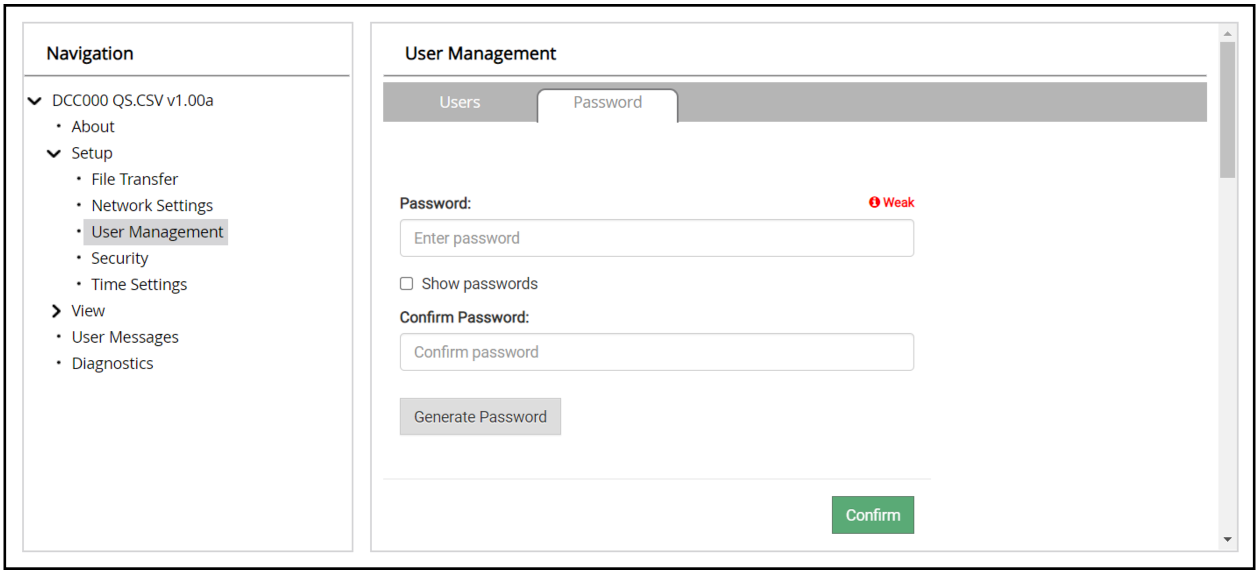


Warning

Are you sure you want to delete user: User A?

12.2.4 Change FieldServer Password

- Click the Password tab.



Password:

Enter password

□ Show passwords

Confirm Password:

Confirm password

- Change the general login password for the FieldServer as needed.

NOTE: The password must meet the minimum complexity requirements. An algorithm automatically checks the password entered and notes the level of strength on the top right of the Password text field.

12.3 Update Firmware

To load a new version of the firmware, follow these instructions:

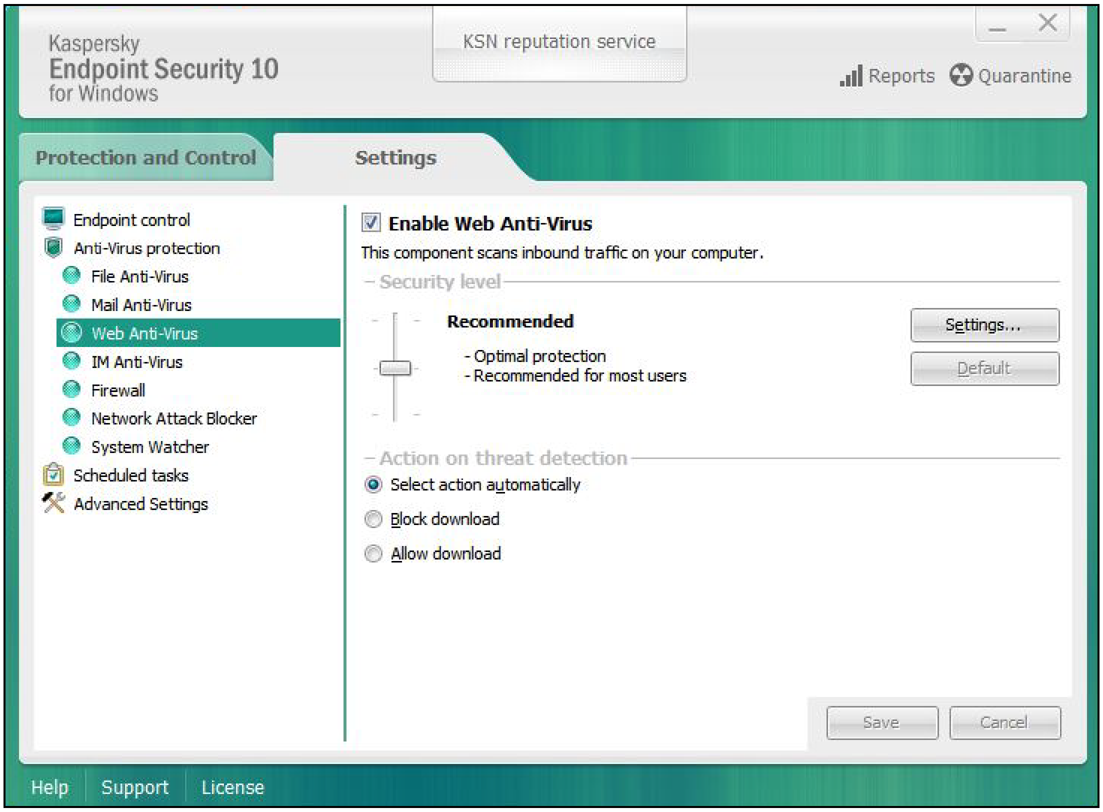
1. Extract and save the new file onto the local PC.
2. Open a web browser and type the IP Address of the FieldServer in the address bar.
   - Default IP Address is 192.168.1.24
   - Use the FS Toolbox utility if the IP Address is unknown (**Section 11.2 Lost or Incorrect IP Address**)
3. Click on the "Diagnostics & Debugging" button.
4. In the Navigation Tree on the left hand side, do the following:
   a. Click on "Setup"
   b. Click on "File Transfer"
   c. Click on the "General" tab
5. In the General tab, click on "Choose Files" and select the web.img file extracted in step 1.
6. Click on the orange "Submit" button.
7. When the download is complete, click on the "System Restart" button.

12.4 Kaspersky Endpoint Security 10

If Kaspersky Endpoint Security 10 is installed on the user's PC, the software needs to be modified to allow the PC to register bridges on the FieldServer Manager.

NOTE: This problem is specific to KES10, Kaspersky 2017 does not have this problem.

To fix the problem, the ProtoAir (see http://192.168.100.85/* in the 2nd image below) must be set as a trusted URL to the "Web Anti-Virus"->"Settings" as shown below.



☑ **Enable Web Anti-Virus**

This component scans inbound traffic on your computer.

Security level

Recommended

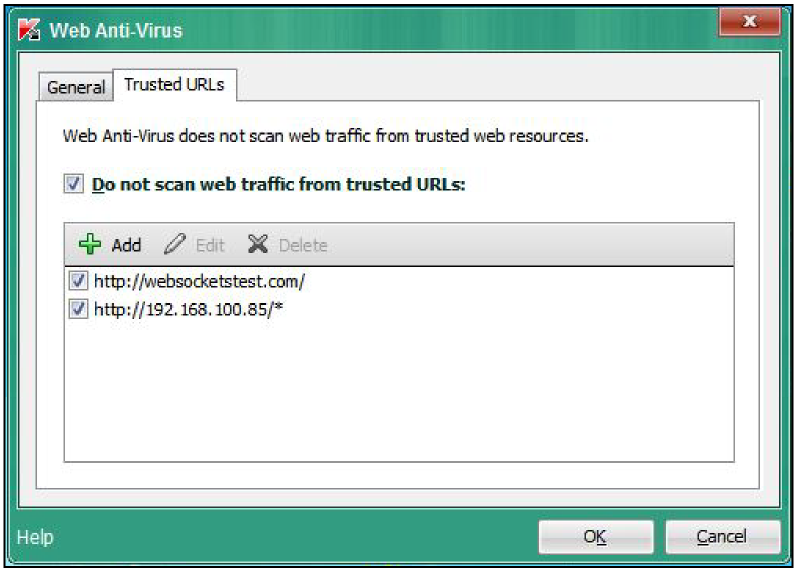
- Optimal protection
- Recommended for most users

Action on threat detection

● Select action automatically

○ Block download

○ Allow download



Web Anti-Virus does not scan web traffic from trusted web resources.

☑ **Do not scan web traffic from trusted URLs:**

☑ http://websockettest.com/

☑ http://192.168.100.85/*

12.5 APN Table

Use the table below to enter one of the correct APNs for your sim card:

Cellular Provider	APN
AT&T	broadband NXTGENPHONE
Verizon	Vzwinternet internet
Kore	c2.korem2m.com

12.6 ProtoAir Part Number by Carrier

- FPA-C41-XXXX: Serial, Ethernet, AT&T Cellular and Wi-Fi
- FPA-C42-XXXX: Serial, Ethernet, Verizon Cellular and Wi-Fi
- FPA-C43-XXXX: Serial, Ethernet, Vodafone Cellular and Wi-Fi

12.7 Specifications

	ProtoAir FPA-W44 & FPA-C4X
Electrical Connections	One 3-pin Phoenix connector with: RS-485/RS-232 (Tx+ / Rx- / gnd) One 3-pin Phoenix connector with: Power port (+ / - / Frame-gnd) One Ethernet 10/100 BaseT port **W44 includes an additional:** One 3-pin Phoenix connector with: RS-485 (+ / - / gnd)
W44 Power Requirements	*Input Voltage:* 9-30VDC or 24VAC *Current draw:* 24VAC 0.125A *Max Power:* 3 Watts 9-30VDC 0.25A @12VDC
C4X Power Requirements	*Input Voltage:* 12-24VDC *Current draw:* @ 12V, 0.67A *Max Power:* 8 Watts
Approvals	FCC Part 15 C, UL 60950-1 and CAN/CSA C22.2 No. 60950-1 (**W44**), EN IEC 62368-1:2020+A11:2020, WEEE compliant, RoHS compliant, DNP 3.0 and Modbus conformance tested, PTCRB compliant, BTL marked, REACH compliant, UKCA and CE compliant, ODVA conformant, CAN ICES-003(B) / NMB-003(B) (**W44, C41, C42**)
FCC ID	**FPA-W44:** 2AIVJ-FPAW44 **FPA-C4X:** 2AIVJ-FPAC41
Physical Dimensions	4 x 1.1 x 2.7 in (10.16 x 2.8 x 6.8 cm)
Weight	0.4 lbs (0.2 Kg)
Operating Temperature	-20°C to 70°C (-4°F to158°F)
Humidity	10-95% RH non-condensing
Wi-Fi 802.11 b/g/n	*Frequency:* 2.4 GHz *Channels:* 1 to 11 (inclusive) *Antenna:* Omnidirectional SMA *Encryption:* TKIP, WPA2 & AES
Cellular (C4X only)	*Features:* LTE Cat 4 *Antenna:* Omnidirectional 4G/LTE SMA *Uplink:* Up to 50 Mbps *Downlink:* Up to 150 Mbps *IMEI:* 357178070517852

NOTE: Specifications subject to change without notice.

12.8 Compliance with EN IEC 62368-1

For EN IEC compliance, the following instructions must be met when operating the ProtoAir.

- The units shall be powered by listed LPS or Class 2 power supply suited to the expected operating temperature range.
- The interconnecting power connector and power cable shall:
  - Comply with local electrical code
  - Be suited to the expected operating temperature range
  - Meet the current and voltage rating for the FieldServer
- Furthermore, the interconnecting power cable shall:
  - Be of length not exceeding 3.05m (118.3")
  - Be constructed of materials rated VW-1, FT-1 or better
- If the unit is to be installed in an operating environment with a temperature above 65 °C, it should be installed in a Restricted Access Area requiring a key or a special tool to gain access.
- This device must not be connected to a LAN segment with outdoor wiring.

12.9 Warnings for FCC and IC

Waste Disposal

It is recommended to disassemble the device before abandoning it in conformity with local regulations. Please ensure that the abandoned batteries are disposed according to local regulations on waste disposal. Do not throw batteries into fire (explosive) or put in common waste canister. Products or product packages with the sign of “explosive” should not be disposed like household waste but delivered to specialized electrical & electronic waste recycling/disposal center. Proper disposal of this sort of waste helps avoiding harm and adverse effect upon surroundings and people’s health. Please contact local organizations or recycling/disposal center for more recycling/disposal methods of related products.

Comply with the following safety tips:

Do Not use in Combustible and Explosive Environment

Keep away from combustible and explosive environment for fear of danger.

Keep away from all energized circuits.

Operators should not remove enclosure from the device. Only the group or person with factory certification is permitted to open the enclosure to adjust and replace the structure and components of the device. Do not change components unless the power cord is removed. In some cases, the device may still have residual voltage even if the power cord is removed. Therefore, it is a must to remove and fully discharge the device before contact so as to avoid injury.

Unauthorized Changes to this Product or its Components are Prohibited

In the aim of avoiding accidents as far as possible, it is not allowed to replace the system or change components unless with permission and certification. Please contact the technical department of Vantron or local branches for help.

Pay Attention to Caution Signs

Caution signs in this manual remind of possible danger. Please comply with relevant safety tips below each sign. Meanwhile, you should strictly conform to all safety tips for operation environment.

Notice

Considering that reasonable efforts have been made to assure accuracy of this manual, Vantron assumes no responsibility of possible missing contents and information, errors in contents, citations, examples, and source programs.

Vantron reserves the right to make necessary changes to this manual without prior notice. No part of this manual may be reprinted or publicly released.

FCC Warning (-W44, -C41, -C42)

This device complies with FCC Rules. Operation is subject to the following conditions.

This device may not cause harmful interference.

This device must accept any interference received, including interference that may cause undesired operation.

This device complies with Part 15C of the FCC Rules

For FPA-C41/C42, this device complies with Part 22H, Part 24E and Part 27 of the FCC Rules.

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Any modification to the product is not permitted unless authorized by MSA Safety. It’s not allowed to disassemble the product; it is not allowed to replace the system or change components unless with permission and certification. Please contact the FieldServer technical support department or local branches for help.

IC Statement

This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions:

- This device may not cause interference, and
- This device must accept any interference, including interference that may cause undesired operation of the device.

Warning! This class B digital apparatus complies with Canadian ICES-003.

Industry Canada ICES-003 Compliance Label:

CAN ICES-3 (B)/NMB-3(B)

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts.

L'exploitation est autorisée aux deux conditions suivantes:

- l'appareil ne doit pas produire de brouillage, et
- l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

RF Exposure Warning

This equipment must be installed and operated in accordance with provide instructions and the antenna used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operation in conjunction with any other antenna or transmitter. End-users and installers must be provided with antenna installation instructions and transmitter operating conditions for satisfying RF exposure compliance.

For product compliance test FCC and IC, all the technical documentation is submitted by MSA Safety, who is the customer or importer of the ProtoAir.

ProtoAir radios have been approved to be used with antennas that have a maximum gain of 3 dBi. Any antennas with a gain greater than 3 dBi are strictly prohibited for use with this device.

Power Output

Frequency Range Output Power:

Wi-Fi *(applies to all models)*
2402.0 – 2480 MHz 0.004 W

2412.0 – 2462.0 MHz 0.0258 W

LTE *(FPA-C4X models only)*
Supported Bands:
FPA-C41/FPA-C42 – B2, B4, B5, B12, B13 & B17 (0.25 W)
FPA-C43 – B1, B3, B7, B8, B20 (0.25 W)

The Output Power listed is conducted. The device should be professionally installed to ensure compliance with power requirements. The antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and not be co-located with any other transmitters except in accordance with multi-transmitter product procedures. This device supports 20MHz and 40MHz bandwidth.

13 Limited 2 Year Warranty

MSA Safety warrants its products to be free from defects in workmanship or material under normal use and service for two years after date of shipment. MSA Safety will repair or replace any equipment found to be defective during the warranty period. Final determination of the nature and responsibility for defective or damaged equipment will be made by MSA Safety personnel.

All warranties hereunder are contingent upon proper use in the application for which the product was intended and do not cover products which have been modified or repaired without MSA Safety’s approval or which have been subjected to accident, improper maintenance, installation or application; or on which original identification marks have been removed or altered. This Limited Warranty also will not apply to interconnecting cables or wires, consumables or to any damage resulting from battery leakage.

In all cases MSA Safety’s responsibility and liability under this warranty shall be limited to the cost of the equipment. The purchaser must obtain shipping instructions for the prepaid return of any item under this warranty provision and compliance with such instruction shall be a condition of this warranty.

Except for the express warranty stated above, MSA Safety disclaims all warranties with regard to the products sold hereunder including all implied warranties of merchantability and fitness and the express warranties stated herein are in lieu of all obligations or liabilities on the part of MSA Safety for damages including, but not limited to, consequential damages arising out of/or in connection with the use or performance of the product.