



SYNAPSE

Operating Manual

BMS Gateway/ProtoAir (BMS-GW-002/FPA-W44)

for Interfacing the SimplySNAP Site Controller (SS420/450)



Revision: 4.A

Document No.: CN1913

Print Spec: 10000005389 (EO)

Technical Support

Thank you for purchasing the BMS Gateway/ProtoAir (BMS-GW-002/FPA-W44) from Synapse Wireless.

Please contact Synapse Wireless for technical support of the BMS Gateway/ProtoAir (BMS-GW-002/FPA-W44) product.

MSA Safety does not provide direct support. If Synapse Wireless needs to escalate the concern, they will contact MSA Safety for assistance.

Support Contact Information:

Synapse Wireless
351 Electronics Blvd, Suite D
Huntsville, Alabama 35824

Customer Service:

Phone: (877) 982-7888

Website: <http://www.synapsewireless.com>

A ticket can be opened at <https://support.synapsewireless.com>

Quick Start Guide

1. Record the information about the unit. ([Section 2.1 Record Identification Data](#))
2. Check that the BMS-GW/ProtoAir and customer device COM settings match. ([Section 2.2 Configuring Device Communications](#))
3. **If using a serial field protocol:**
Connect the BMS-GW/ProtoAir 3 pin RS-485 R2 port to the field protocol cabling ([Section 2.4 Wiring Field Port to RS-485 Serial Network](#)).
4. Connect power to BMS-GW/ProtoAir 3 pin power port. ([Section 3 Power up the Gateway](#))
5. Connect a PC to the BMS-GW/ProtoAir via Ethernet cable or by the unit's Wi-Fi Access Point. ([Section 4 Connect the PC to the Gateway](#))
6. Setup Web Server Security and login via web browser. ([Section 5 Setup Web Server Security](#))
7. Configure the BMS-GW/ProtoAir to connect to the local network. ([Section 6 Setup Network](#))
8. Enter the protocol settings via the BMS Settings window. ([Section 7.1 Select BMS Protocol and Configure Settings](#))
9. Use the Web Configurator Discovery function to configure the BMS-GW/ProtoAir and to find any connected devices. ([Section 7.2 Discover Devices Connected to the Gateway](#))

Contents

1	Introduction	6
1.1	ProtoAir Gateway	6
2	Setup for ProtoAir	7
2.1	Record Identification Data	7
2.2	Configuring Device Communications	7
2.3	Attaching the Antenna	7
2.4	Wiring Field Port to RS-485 Serial Network	7
2.5	Bias Resistors	8
2.6	Termination Resistor	9
3	Power up the Gateway	10
4	Connect the PC to the Gateway	11
4.1	Connecting to the Gateway via Ethernet	11
4.1.1	Changing the Subnet of the Connected PC	11
4.2	Connecting to the Gateway Over Wi-Fi Access Point	12
5	Setup Web Server Security	13
5.1	Navigate to the Login Page	13
5.2	Login to the FieldServer	13
5.3	Select the Security Mode	15
5.3.1	HTTPS with Own Trusted TLS Certificate	16
5.3.2	HTTPS with Default Untrusted Self-Signed TLS Certificate or HTTP with Built-in Payload Encryption	16
6	Setup Network	17
6.1	Change the ProtoAir IP Address	17
6.1.1	Routing Settings	17
6.1.2	Ethernet 1	18
6.1.3	Wi-Fi Client Settings	19
6.1.4	Wi-Fi Access Point Settings	20
7	Configure the ProtoAir	21
7.1	Select BMS Protocol and Configure Settings	21
7.1.1	BACnet Settings: Additional Information	22
7.1.2	BACnet MS/TP: Setting the MAC Address BACnet Network	22
7.1.3	BACnet Settings: Set the Device Instance	23
7.1.4	Modbus Settings: Additional Information	24
7.1.5	Setting the Modbus Slave ID	24
7.2	Discover Devices Connected to the Gateway	25
7.3	Configure Devices and Data Points	26
7.3.1	General Configuration Instructions	26
7.3.2	Data Map Window	28
7.4	Clearing Configuration	29
8	Troubleshooting	30
8.1	Lost or Incorrect IP Address	30
8.2	Viewing Diagnostic Information	31
8.3	Checking Wiring and Settings	31
8.4	LED Functions	32
8.5	Taking a FieldServer Diagnostic Capture	33
8.6	Factory Reset Instructions	33
8.7	Internet Browser Software Support	34
8.8	Wi-Fi Signal Strength	34

8.9	Kaspersky Endpoint Security 10	35
9	Additional Information	36
9.1	Update Firmware	36
9.2	Mounting	36
9.3	Certification	36
9.4	Physical Dimensions	37
9.5	Change Web Server Security Settings After Initial Setup	38
9.5.1	Change Security Mode	38
9.5.2	Edit the Certificate Loaded onto the FieldServer	39
9.6	Change User Management Settings	40
9.6.1	Create Users	41
9.6.2	Edit Users	42
9.6.3	Delete Users	43
9.6.4	Change FieldServer Password	43
9.7	Structure of the Device Tree	44
10	Specifications	45
10.1	Compliance with EN IEC 62368-1	45
10.2	Warnings for FCC and IC	46
11	Limited 2 Year Warranty	49

1 Introduction

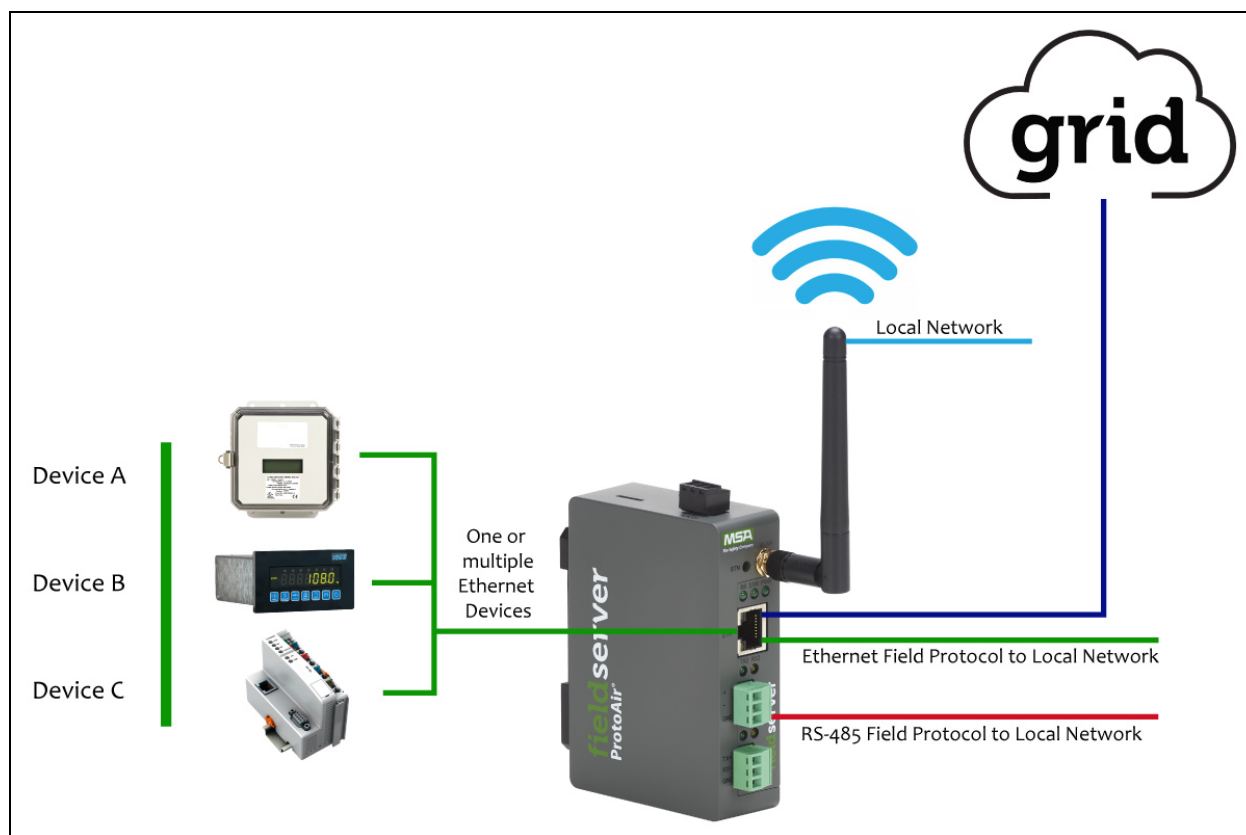
NOTE: The BMS Gateway (BMS-GW) is a co-branded hardware and software solution manufactured by MSA Safety. The Synaspe Wireless p/n for this product is BMS-GW. However, within this document, the BMS-GW will be referred to as the ProtoAir, which is the product name provided by MSA Safety.

1.1 ProtoAir Gateway

The ProtoAir wireless gateway is an external, high performance building automation multi-protocol gateway that is preconfigured to auto-discover the SimplySNAP site controller SS420/450 (hereafter simply called “device”) connected to the ProtoAir and automatically configures them for BACnet/IP, BACnet MS/TP, Modbus RTU and Modbus TCP/IP.

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.

FPA-W44 Connectivity Diagram:



The ProtoAir can connect with the MSA Grid – FieldServer Manager. The FieldServer Manager allows technicians, the OEM's support team and MSA Safety's support team to remotely connect to the ProtoAir. The FieldServer Manager provides the following capabilities for any registered devices in the field:

- Remotely monitor and control devices.
- Collect device data and view it on the Dashboard and the MSA Smart Phone App.
- Create user defined device notifications (alarm, trouble and warning) via SMS and/or Email.
- Generate diagnostic captures (as needed for troubleshooting) without going to the site.

For more information on the FieldServer Manager, see the [MSA Grid - FieldServer Manager Start-up Guide](#).

2 Setup for ProtoAir

2.1 Record Identification Data

Each ProtoAir has a unique part number located on the side or the back of the unit. This number should be recorded, as it may be required for technical support. The numbers are as follows:

Model	Part Number
ProtoAir	FPA-W44-1913

- FPA-W44 units have the following 4 ports: Ethernet + Wi-Fi + RS-485 + RS-485/RS-232

2.2 Configuring Device Communications

- The device needs to be on the same IP subnet as the ProtoAir and the configuration PC.
- Record the following device information to start the setup:
 - IP Address
 - IP port
 - Username
 - Password

NOTE: This information is required for [Section 7 Configure the ProtoAir](#).

2.3 Attaching the Antenna

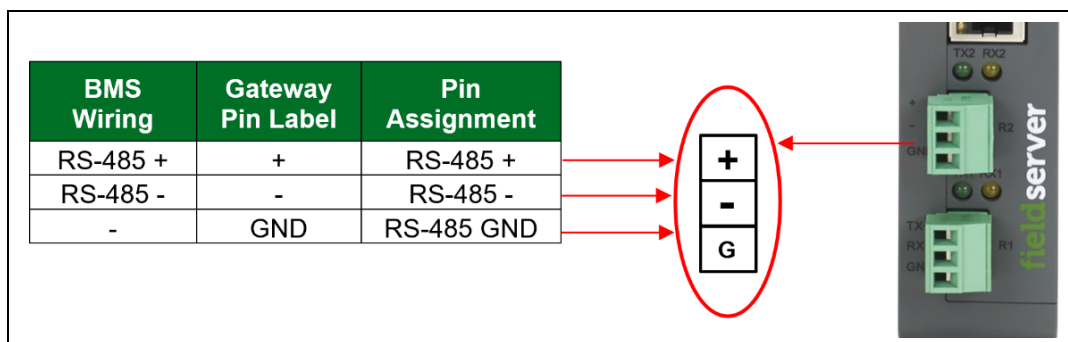
Wi-Fi Antenna:

Screw in the Wi-Fi antenna to the front of the unit as shown in [Section 9.4 Physical Dimensions](#).

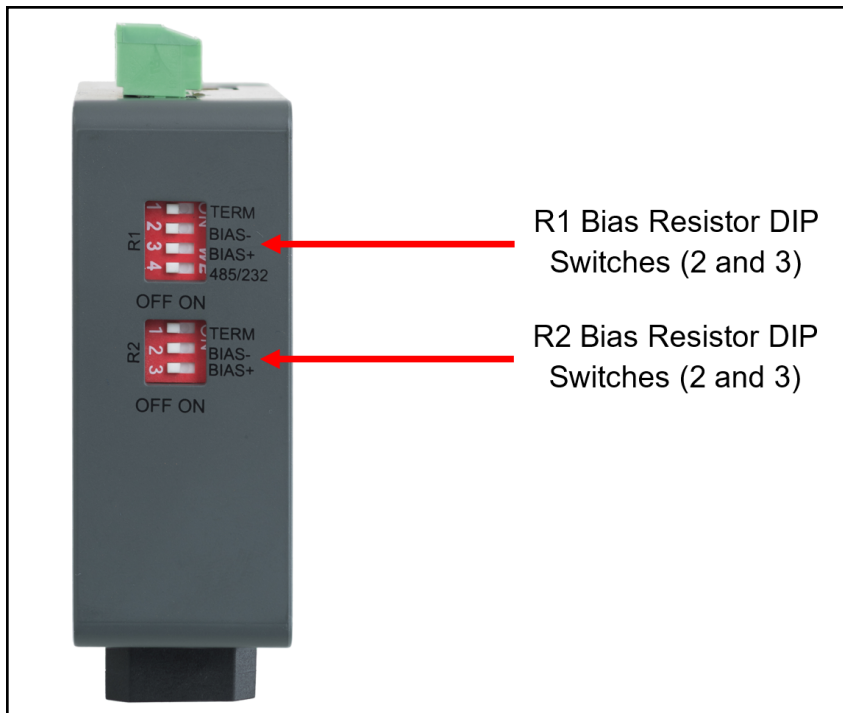
NOTE: Using an external antenna is also an option. An external antenna can be plugged into the SMA connector. The best antenna for the job depends on the range, topography and obstacles between the two radios.

2.4 Wiring Field Port to RS-485 Serial Network

- Connect the RS-485 network wires to the 3-pin RS-485 connector on the R2 port.
 - RS-485 is part of the RS-485 interface and must be connected to the corresponding terminal on the BMS. If the cable is shielded, the shield must be 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).
- See [Section 4.1 Connecting to the Gateway via Ethernet](#) for information on connecting to an Ethernet network.



2.5 Bias Resistors



To enable Bias Resistors, move 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.

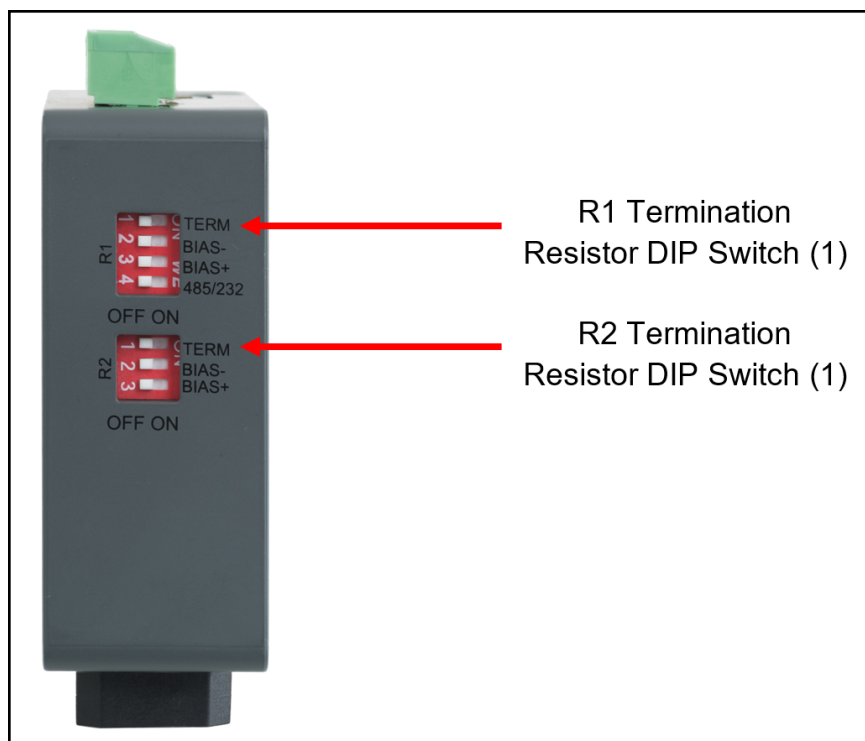
The bias resistor is 510 ohms which is in line with the BACnet spec. It should only be enabled at one point on the bus (for example, on the field port where there are very weak bias resistors of 100k). Since there are no jumpers, many ProtoAirs can be put on the network without running into the bias 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 powered on, DIP switch settings will not take effect unless the unit is power cycled.

2.6 Termination Resistor



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.**

The 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. The R1 termination resistor is 120 Ohms.

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

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

3 Power up the Gateway

Check power requirements in the table below:

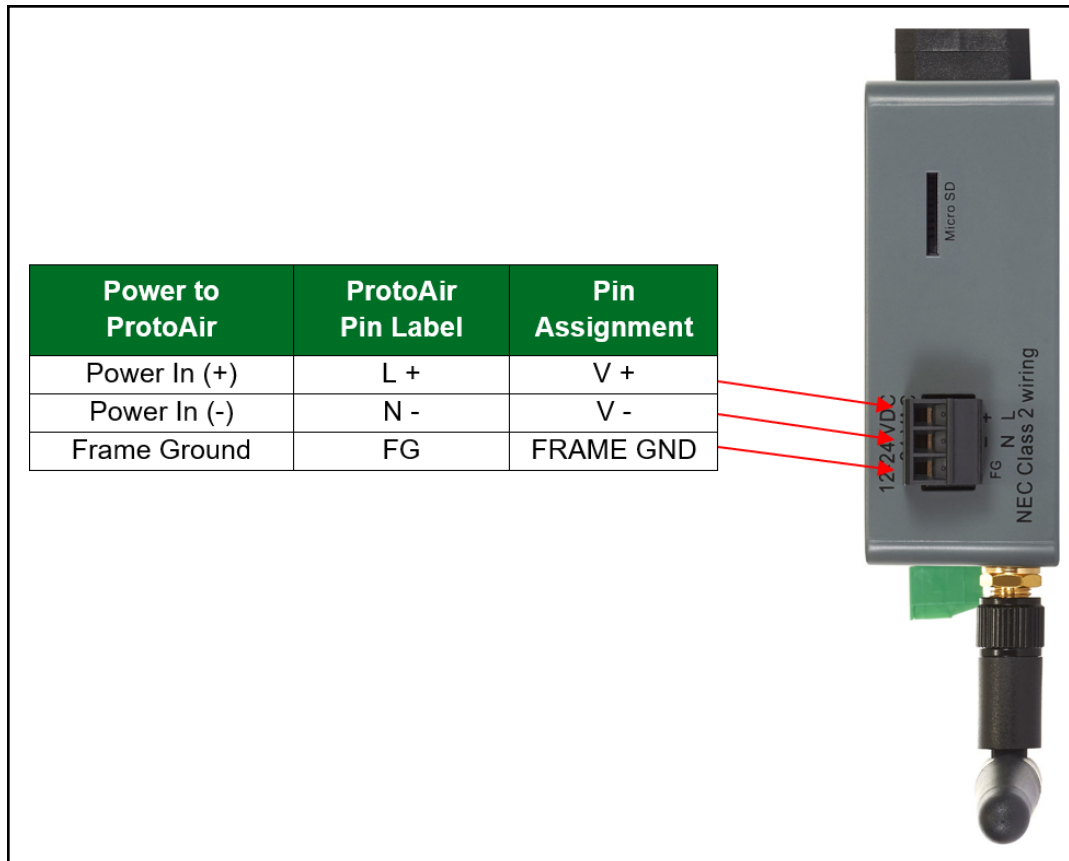
Power Requirement for ProtoAir External Gateway		
ProtoAir Family	Current Draw Type	
	12VDC	24VDC/AC
FPA –W44 (Typical)	250mA	125mA

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 10 Specifications](#).

- The gateway accepts 12-24VDC or 24VAC on pins L+ and N-.
- 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: Only Class 2 PSU's must be used to power FieldServers.

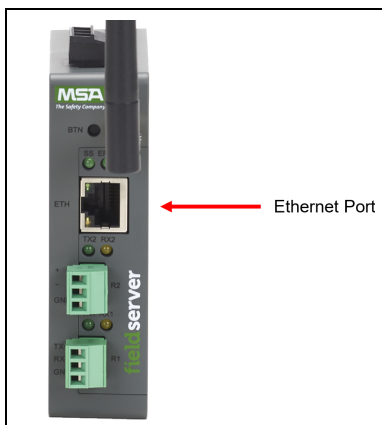


4 Connect the PC to the Gateway

There are two ways to connect the PC to the ProtoAir, either by Ethernet cable ([Section 4.1 Connecting to the Gateway via Ethernet](#)) or Wi-Fi Access Point ([Section 4.2 Connecting to the Gateway Over Wi-Fi Access Point](#)).

4.1 Connecting to the Gateway via Ethernet


Connect a Cat-5 Ethernet cable (straight through or cross-over) between the local PC and ProtoAir.



4.1.1 Changing the Subnet of the Connected PC

The default IP Address for the ProtoAir is **192.168.1.24**, Subnet Mask is **255.255.255.0**. If the PC and ProtoAir are on different IP networks, assign a static IP Address to the PC on the 192.168.1.xxx network.

For Windows 10:

- Use the search field in the local computer's taskbar (to the right of the windows icon ) and type in "Control Panel".
- Click "Control Panel", click "Network and Internet" and then click "Network and Sharing Center".
- Click "Change adapter settings" on the left side of the window.
- Right-click on "Local Area Connection" and select "Properties" from the dropdown menu.
- Highlight [Internet Protocol Version 4 \(TCP/IPv4\)](#) and then click the Properties button.
- Select and enter a static IP Address on the same subnet. For example:

Use the following IP address:

IP address:	192 . 168 . 1 . 11
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	. . .

- Click the Okay button to close the Internet Protocol window and click Close to exit the Ethernet Properties window.

4 Connect the PC to the Gateway

4.2 Connecting to the Gateway Over Wi-Fi Access Point

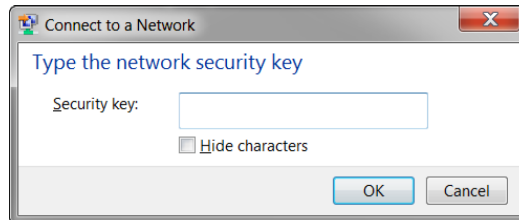
When the ProtoAir is first powered up, the Wi-Fi Access Point will be enabled allowing direct connection to the gateway with Wi-Fi.

To connect to the ProtoAir Wi-Fi Access Point:

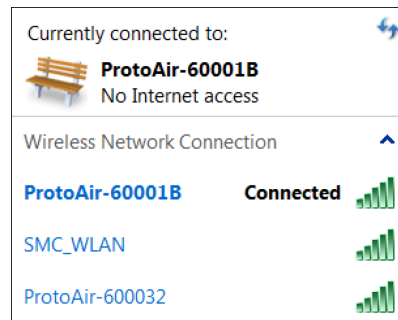
- Click the network icon (found in the bottom-right corner of the computer screen) to open the available Wireless Network Connections.
- Select the desired gateway and click Connect.



- Enter the Security key. The default is "12345678".



- The available Wireless Network Connection menu should now show that the computer is connected to the ProtoAir.



NOTE: For additional Wi-Fi AP settings information see [Section 6.1.4 Wi-Fi Access Point Settings](#).

5 Setup Web Server Security

5.1 Navigate to the Login Page

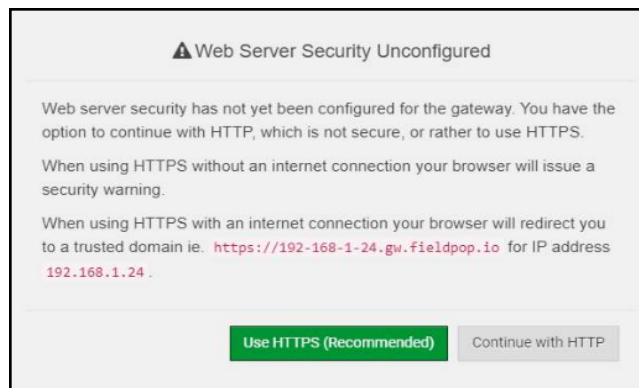
- Open a web browser and connect to the FieldServer's default IP Address. The default IP Address of the FieldServer is **192.168.1.24**, Subnet Mask is **255.255.255.0**.

NOTE: If the IP Address of the ProtoAir has been changed, the IP Address can be discovered using the FS Toolbox utility. See Section [8.1 Lost or Incorrect IP Address](#) for instructions.

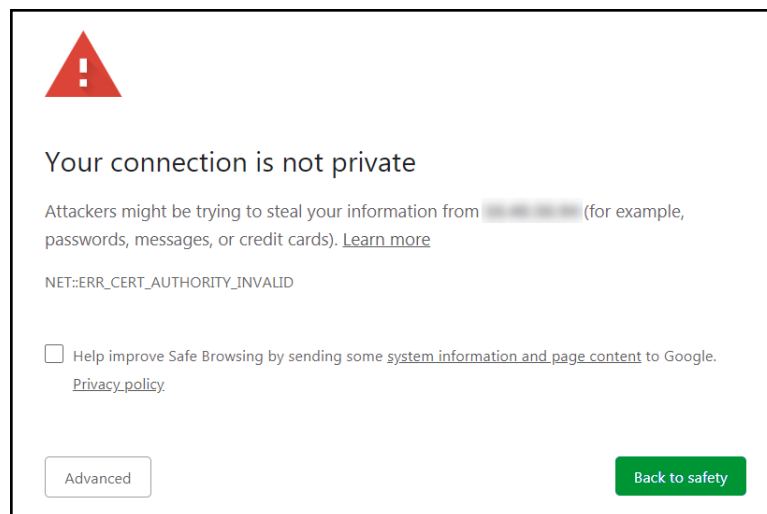
5.2 Login to the FieldServer

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.

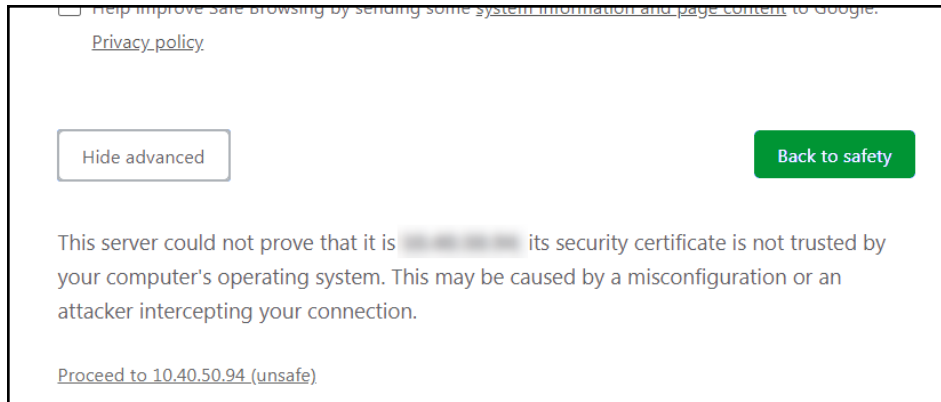


- When the warning that “Your connection is not private” appears, click the advanced button on the bottom left corner of the screen.



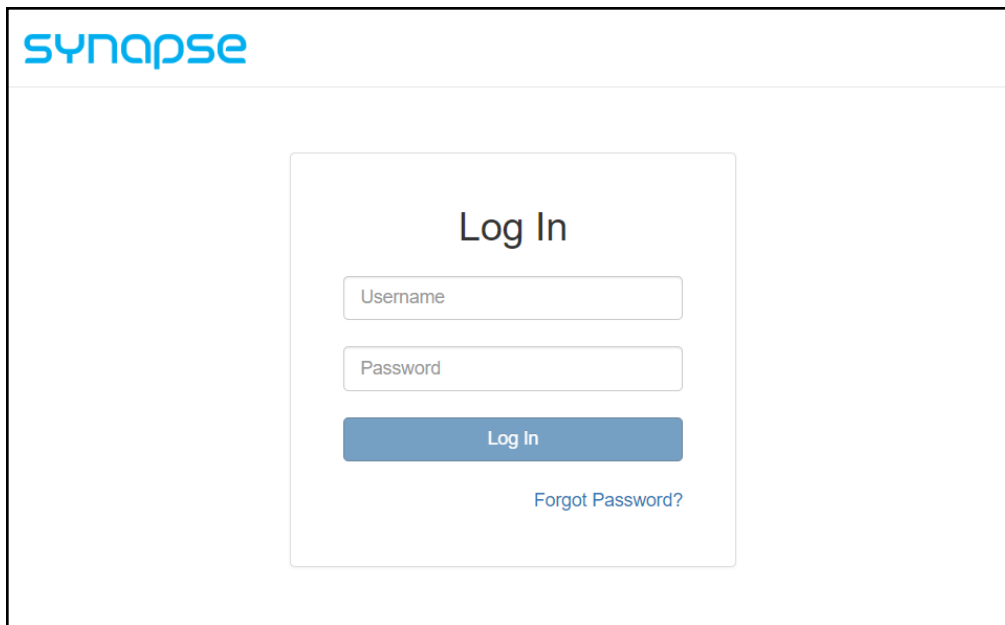
5 Setup Web Server Security

- 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> \(unsafe\)](#)”.



- 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 [9.6 Change User Management Settings](#).

5.3 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)

Save

NOTE: Cookies are used for authentication.

NOTE: To change the web server security mode after initial setup, go to [Section 9.5 Change Web Server Security Settings After Initial Setup](#).

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

5.3.1 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/47VEmaiXqE3bx3zEuBFJ6pWPlw7LHf2r2ZoHw+9xb+aNMU
dVyAelhBMTMsnI2ERvQVp0xj3psSv2EJyKXS1bOYNRLsq7UzpwuAdT/Wy3o6vUM5
K+Cwf9qEoQ0LluxDZTIEct67MkcHMiuFi5pk7TRicHnQf/sfOAYOulduHOy9exlk9
FmHFVDIZt/cJUaF+e74EuSph+gEr0IQo2wmmhyc7L22UXse1NoOfu2Zg0Eu1VWtu
JRryaMwIRFEWuuzMGZtKFWVC+8g2JQsVcqiRWM7naoblEhOCMH+sKHJMCxDoXGt
vtZjpZUoAL51YXxWSVcyZdGiAP5e
-----END CERTIFICATE-----
```

Private Key

```
sHB0zZoHr4YQSDK2BbYVzzbl0LDuKtc8+JiO3ooGjoTuHnqkeAj/fkfbTAsKeAzw
gKQe+H5UQNK0bdvZfOJrm6daDK2vDmR5k+juUhej5N49upIroB97MQgYotzgf+
THlbgp5t1SIK617k04ObKmHF5l8fck+ru545sVmpeezh0m5j5SURYAZMvbq5daCu
J4l5NlihbEvxRF4UK41ZDMCvujopCbkUWrb1a/3XXnDnM2K9xyz2wze998D6Wk46
+7aOFY9F+7j5ljmkoS3GYtwCyH5jP+mPP1K6RnuiD019wvGPb4dtN/RTnfd0eF
GYeVSkI9fxxkxDOFtdWRZbM/rPin4tmO1Xf8HqONVN1x/iaMynOXG4cukoi4+VO
u0rZaUEsII2zNkfrn7fAASm5NBWg202Cy9IAYnuujs3aALl5uGBEEK62oTMxlzx
-----END RSA PRIVATE KEY-----
```

Private Key Passphrase

Specify if encrypted

Save

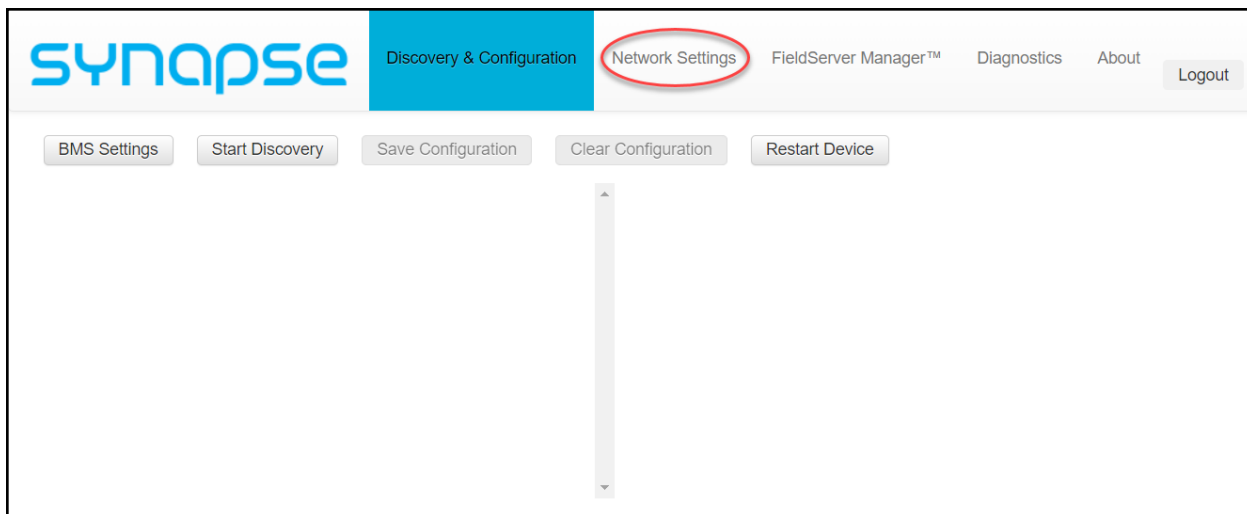
- Copy and paste the Certificate and Private Key text into their respective fields. If the Private Key is encrypted type in the associated Passphrase.
- Click Save.
- A “Redirecting” message will appear. After a short time, the FieldServer GUI will open.

5.3.2 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.

6 Setup Network

From the Web Configurator landing page, click the Network Settings tab to open the Network Settings page for the ProtoAir.



6.1 Change the ProtoAir IP Address

Configure the IP settings of the ProtoAir using the following sections of the Network page:

- If using the Ethernet port to connect to the local network, scroll to “ETH 1” ([Section 6.1.2 Ethernet 1](#)).
- If connecting the ProtoAir to a local wireless network, scroll to “WiFi Client Settings” ([Section 6.1.3 Wi-Fi Client Settings](#)).
- If updating Wi-Fi Access Point settings, scroll to “WiFi Access Point Settings” ([Section 6.1.4 Wi-Fi Access Point Settings](#)).

6.1.1 Routing Settings

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

- 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 ?
WiFi Client	Default	-	10.40.50.1	255
ETH 1	10.40.50.10	255.255.255.255	10.40.50.1	100

+ Add Rule

Cancel Save

6.1.2 Ethernet 1

The ETH 1 section contains the wired network settings. To change the FieldServer 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.

The screenshot displays the 'ETH 1' configuration page. At the top, there are tabs for 'ETH 1', 'WiFi Client', 'WiFi Access Point', and 'Routing'. The 'ETH 1' tab is active. Below the tabs, there is a checkbox for 'Enable DHCP' which is currently unchecked. The 'IP Address' field contains '10.40.50.92'. The 'Netmask' field contains '255.255.255.0'. The 'Gateway' field contains '10.40.50.1'. There are two optional 'Domain Name Server' fields: 'Domain Name Server 1 (Optional)' contains '10.40.2.24' and 'Domain Name Server 2 (Optional)' contains '10.15.130.15'. At the bottom left, there are 'Cancel' and 'Save' buttons. On the right side, there is a 'Network Status' panel with the following information:

Network Status	
Connection Status	✔ Connected
MAC Address	00:50:4e:60:01:fd
Ethernet Tx Msgs	498,827
Ethernet Rx Msgs	1,384,116
Ethernet Tx Msgs Dropped	0
Ethernet Rx Msgs Dropped	0

6.1.3 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 6.1.1 Routing Settings](#)) to set the default connection to Wi-Fi Client.

ETH 1
WiFi Client
WiFi Access Point
Routing

Enable

SSID

Password (Optional)

Enable DHCP

IP Address

Netmask

Gateway

Domain Name Server 1 (Optional)

Domain Name Server 2 (Optional)

Network Status

Connection Status	✔ Connected
MAC Address	A0:CC:2B:FF:AB:59
WiFi BSSID	78:BC:1A:52:C8:42
WiFi Channel	2,462
WiFi Tx Msgs	1,484
WiFi Rx Msgs	1,799
WiFi Tx Msgs Dropped	0
WiFi Rx Msgs Dropped	16
WiFi Pairwise Cipher	CCMP
WiFi Group Cipher	CCMP
WiFi Key Mgmt	WPA2-PSK
WiFi Link	19.5 MBit/s MCS 2
WiFi Signal Level	-86 dBm

6.1.4 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. See the rest of the default settings listed in the screenshot below.

- 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.

ETH 1 WiFi Client WiFi Access Point Routing

Enable

SSID
ProtoAir-6001FD

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

Cancel Save

Network Status

Connection Status	Disabled
Access Point MAC Address	a0:cc:2b:ff:ab:59
Access Point Tx Msgs	0
Access Point Rx Msgs	0
Access Point Tx Msgs Dropped	0
Access Point Rx Msgs Dropped	0

7 Configure the ProtoAir

7.1 Select BMS Protocol and Configure Settings

- Click back to the Discovery & Configuration tab, and click the BMS Settings button to view or edit the Building Management System (BMS) Settings.
- Select the appropriate protocol and edit the settings as needed.
- Once completed, click Save.
- Click Yes and then Restart to save and restart the ProtoNode.

BMS Settings

Select the BMS Protocol

BACnet IP

BACnet IP Settings

Device Name	SimplySNAPGateway
Device Location	-
Device Instance	11

Enable BBMD Edit Broadcast Distribution Table

IP Port	47808
Public IP Address	-
Public IP Port	47808

Communication with SimplySNAP

Scan Interval	30	s
---------------	----	---

Save Cancel

7.1.1 BACnet Settings: Additional Information

Enter the following details into the web configuration as seen in the following screenshot:

- Name – Enter a name for the ProtoAir.
- Location – Enter the location of the ProtoAir.
- Baud Rate (BACnet MS/TP only) – Select a value of 9600, 19200, 38400, or 76800.

The screenshot shows the 'BMS Settings' configuration page. At the top, there is a dropdown menu for 'Select the BMS Protocol' with 'BACnet MS/TP' selected. Below this is the 'BACnet MS/TP Settings' section, which contains several input fields:

Device Name	SimplySNAPGateway
Device Location	-
Device Instance	11
Max Masters	127
Max Info Frames	1
MAC address	1
Connection	
Baud Rate	9600

Below the BACnet settings is the 'Communication with SimplySNAP' section, which includes a 'Scan Interval' field set to 30 seconds.

At the bottom right of the form are 'Save' and 'Cancel' buttons.

7.1.2 BACnet MS/TP: Setting the MAC Address BACnet Network

NOTE: Only 1 MAC address is set for the ProtoAir regardless of how many devices are connected to the ProtoAir.

- Set the BACnet MS/TP MAC address of the ProtoAir to a value between 1 to 127 (MAC Master Addresses); this is so that the BMS Front End can find the ProtoAir via BACnet auto-discovery.

NOTE: Never set a BACnet MS/TP MAC Address from 128 to 255. Addresses from 128 to 255 are Slave Addresses and cannot be discovered by BMS Front Ends that support auto-discovery of BACnet MS/TP devices.

7.1.3 BACnet Settings: Set the Device Instance

NOTE: The Device Instance can be set independently of the site administrator.

- A Device Instance is a BACnet Node-ID which is obtained by the network administrator.
- All the devices connected to the ProtoAir will be under the same BACnet Device Instance.

NOTE: The default BACnet Device Instance is 11.

- The values allowed for a BACnet Device Instance can range from 1 to 4,194,303.
- To assign a specific Device Instance, change the Device Instance value as desired

BMS Settings

Select the BMS Protocol

BACnet IP

BACnet IP Settings

Device Name	SimplySNAPGateway
Device Location	-
Device Instance	11

Enable BBMD Edit Broadcast Distribution Table

IP Port	47808
Public IP Address	-
Public IP Port	47808

Communication with SimplySNAP

Scan Interval	30	s
---------------	----	---

Save Cancel

7.1.4 Modbus Settings: Additional Information

Enter the following details into the web configuration as seen in the following screenshot:

- Connection (Modbus RTU only) – Select the physical port to use.
- Partial Data Response (Modbus TCP/IP only) – If a partial data response is received on the SimplySNAP coms, select how the ProtoAir will respond to the Modbus front end.

The screenshot shows the 'BMS Settings' configuration window. At the top, 'Select the BMS Protocol' is set to 'Modbus RTU'. Below this, the 'Modbus RTU Settings' section contains a table of configuration options:

Field	Value
Connection	[Dropdown]
Slave ID	11
Baud Rate	9600
Parity	None
Data Bits	8
Stop Bits	1

Below the table, the 'Communication with SimplySNAP' section has a 'Scan Interval' field set to '30' with a unit indicator 's'. At the bottom right, there are 'Save' and 'Cancel' buttons.

7.1.5 Setting the Modbus Slave ID

When the Slave ID field is entered, the Slave ID Offset will not be used. In this setting, only one Modbus server node will be created.

The screenshot shows the 'BMS Settings' configuration window. At the top, 'Select the BMS Protocol' is set to 'Modbus TCP'. Below this, the 'Modbus TCP Settings' section contains a table of configuration options:

Field	Value
IP Port	502
Slave ID	11
Partial Data Response	Do Not Respond

Below the table, the 'Communication with SimplySNAP' section has a 'Scan Interval' field set to '30' with a unit indicator 's'. At the bottom right, there are 'Save' and 'Cancel' buttons.

If Slave ID is not used (input a dash [-] into the Slave ID field), the Slave ID Offset will be used to generate multiple Modbus server nodes.

7.2 Discover Devices Connected to the Gateway

- Click on the Start Discovery button to open the Discovery Window.
- Enter the appropriate network address, port, username and password for the SimplySNAP Site Controller. ([Section 2.2 Configuring Device Communications](#))

IP Address	Port	User	Password
127.0.0.1	443		

- After entering details, click on the Start Discovery button and the discovery progress bar will display.
 - Discovery may take a few minutes depending on the number of points to discover

- After the discovery process is complete, the device tree will appear (see [Section 9.7 Structure of the Device Tree](#) for device tree structure details).

7.3 Configure Devices and Data Points

7.3.1 General Configuration Instructions

- Click on the right facing arrows next to an item in the device tree to view the points or parameters underneath.

The screenshot shows the BMS configuration interface. At the top, there are buttons for "BMS Settings", "Start Discovery", "Save Configuration", "Clear Configuration", and "Restart Device". On the left, a device tree is displayed under the IP address 64.60.250.225. The tree includes "System", "Zones", "Scenes", and "Controllers". Under "Controllers", several controllers are listed, with "Dim10-100 B Controller 088f8d" selected and expanded to show a list of data points: "y", "x", "alarms", "active_power", "voltage", "current", "line_frequency", "power_factor", and "level". On the right, the "BACnet Instance Details" panel is shown, containing a table with the following information:

BACnet Instance	-
Name	Dim10-100 B Controller 088f8d
Description	Dim10-100 B Controller 088f8d
Location	-

NOTE: The device tree structure is detailed in [Section 9.7 Structure of the Device Tree](#).

- When viewing points or parameters containing points, click inside the checkbox to select or deselect items for protocol conversion.

NOTE: Clicking a checkbox will select all points nested under that item as well.

- Clicking on a point, the endpoint parameters for that point will be shown and, depending on the protocol, some fields may be editable

The screenshot shows the BMS configuration interface with the "Dim10-100 B Controller 088f8d" selected. The "BACnet Endpoint Parameters" panel is now displayed, showing a table with the following information:

BACnet Instance	-
Name	y
Description	latitude

NOTE: Items without BMS Protocol Details (see the screenshot at the bottom of the next page for a configured example) are not yet configured for protocol conversion.

- Once all the points for configuration are selected, click on the Save Configuration button. The save configuration progress bar will appear. This process may take several minutes.

The screenshot shows the BMS configuration interface with the following elements:

- Buttons: BMS Settings, Start Discovery, Save Configuration, Clear Configuration, Restart Device.
- Controllers list:
 - Dim10-250 Controller 07294b
 - Dim10-087 Controller 0816fb
 - Dim10-250 B Controller 072bab
 - Dim10-100 B Controller 088f8d** (selected)
 - y
 - x
 - alarms
 - active_power
 - voltage
 - current
 - line_frequency
 - power_factor
 - level
 - sssSensor Sensor Controller abcdef
- BACnet Instance Details panel:

BACnet Instance	-
Name	Dim10-100 B Controller 088f8d
Description	Dim10-100 B Controller 088f8d
Location	-

- When this process is complete click the Restart button.
 - Protocol specific reference fields (such as BACnet Instance and Modbus Node ID information) will populate for all configured points/devices
 - A BMS map of the configuration can now be viewed or downloaded as a CSV file

The screenshot shows the BMS configuration interface with the following elements:

- Buttons: BMS Settings, Start Discovery, Save Configuration, Clear Configuration, Restart Device.
- Controllers list:
 - Dim10-250 Controller 07294b
 - Dim10-087 Controller 0816fb
 - Dim10-250 B Controller 072bab
 - Dim10-100 B Controller 088f8d** (selected)
 - y
 - x
 - alarms
- BACnet Endpoint Parameters panel:

BACnet Instance	57
Name	y
Description	latitude

NOTE: This configuration method is the same for all protocols.

7.3.2 Data Map Window

NOTE: When configuring points, an option to view point details from a quick look up table or CSV file download is available.

- Click on the IP Address to view the Node details for the entire configuration or click on a specific device to view the map for just the selected device.

- To view or download the mapping click the “Download” or “View” links.
 - Click View to open a window that lists the data points

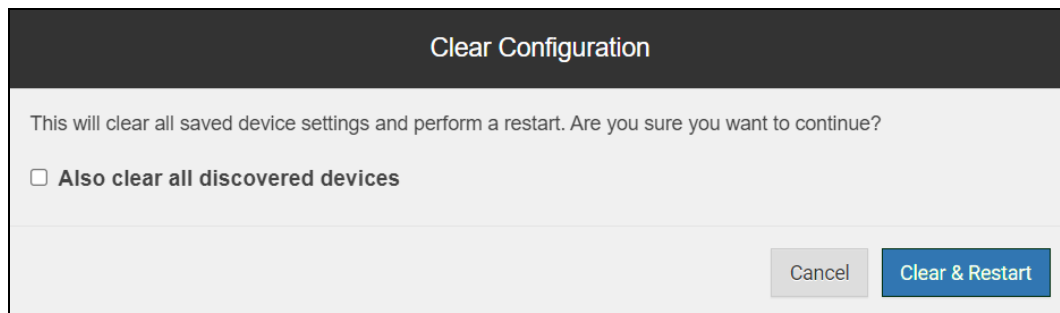
Device ID	Device Name	Point ID	Point Name	Modbus Node ID	Modbus Data Type	Modbus Register	Scaling
871	0.1 RVS68.663E/...	-	Device Fault Mon...	1	Input Register	0	1
871	0.1 RVS68.663E/...	877	Room Unit 1	1	Holding Register	0	1
871	0.1 RVS68.663E/...	878	Room Unit 2	1	Holding Register	1	1
871	0.1 RVS68.663E/...	879	Room Unit 3/P	1	Holding Register	2	1
871	0.1 RVS68.663E/...	880	Outside Sensor	1	Holding Register	3	1
871	0.1 RVS68.663E/...	881	Repeater	1	Holding Register	4	1
871	0.1 RVS68.663E/...	882	Operator unit 1	1	Holding Register	5	1
871	0.1 RVS68.663E/...	883	Operator unit 2	1	Holding Register	6	1
871	0.1 RVS68.663E/...	884	Operator unit 3/P	1	Holding Register	7	1
871	0.1 RVS68.663E/...	885	Service Unit	1	Holding Register	8	1

NOTE: Find specific points using the search bars above each data element.

- Click Download to download a CSV file of the data points to the local PC’s default download folder

7.4 Clearing Configuration

- To clear a configuration, click on the Clear Configuration button. An additional option to clear all device configurations is also available in the window that appears.

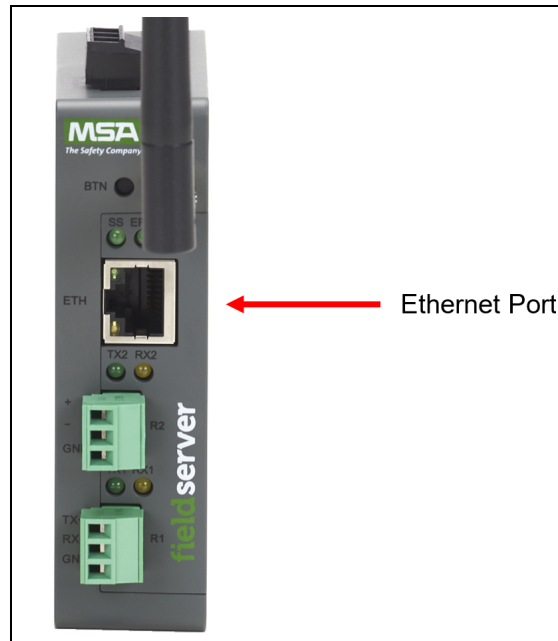


- After clicking on the Clear & Restart button the window will state "Configuration cleared. Restarting...".
- After this process is complete, the ProtoAir will automatically restart.

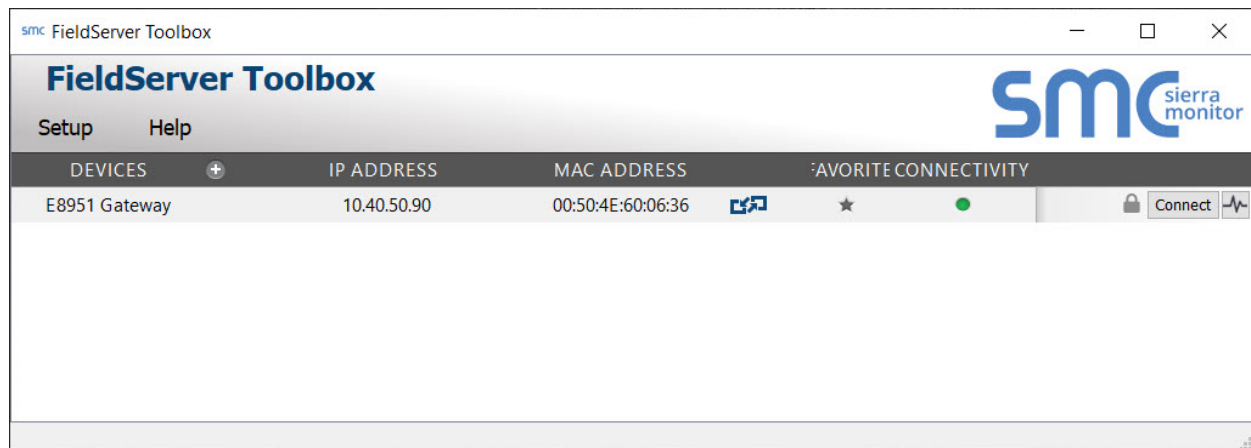
8 Troubleshooting

8.1 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.



- 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.



8.2 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 8.3 Checking Wiring and Settings** for the relevant wiring and settings.

The screenshot displays the MSA FieldServer Manager web interface. The top left features the MSA logo, and the top right shows the 'FieldServer Manager' title. A navigation menu on the left lists various system components, with 'Connections' selected. The main content area, titled 'Connections', contains a table with the following data:

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

At the bottom of the interface, there are buttons for 'Home', 'HELP (?)', 'Contact Us', 'Reset Statistics', and 'Logout'. The 'fieldserver' logo is visible in the bottom right corner.

8.3 Checking Wiring and Settings

No COMS on the Ethernet side. To fix this problem, check the following:

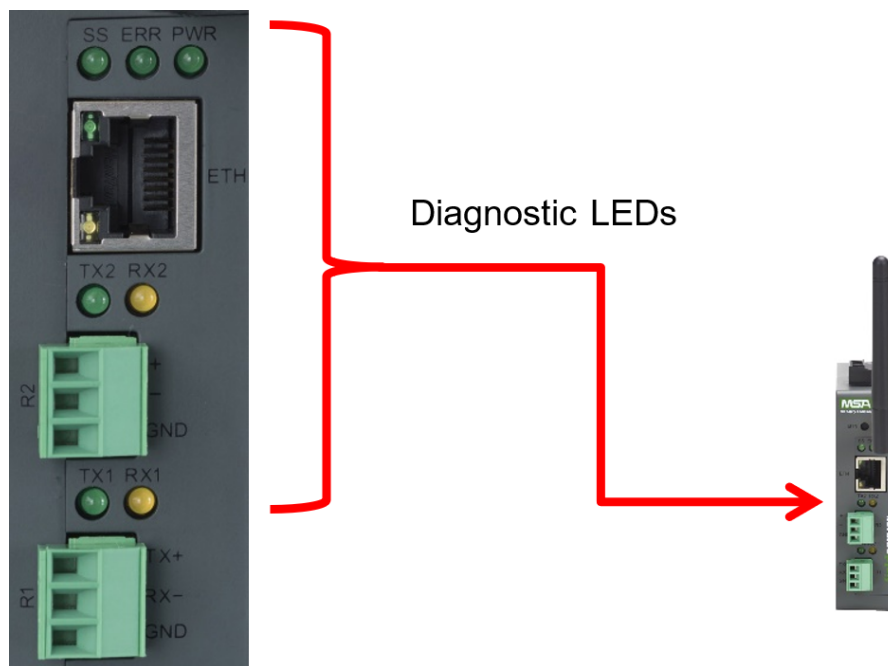
- Visual observations of LEDs on the ProtoAir. (**Section 8.4 LED Functions**)
- Check device address.
- Verify wiring.

Field COM problems:

- Visual observations of LEDs on the ProtoAir. (**Section 8.4 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 8.5 Taking a FieldServer Diagnostic Capture**)


8.4 LED Functions

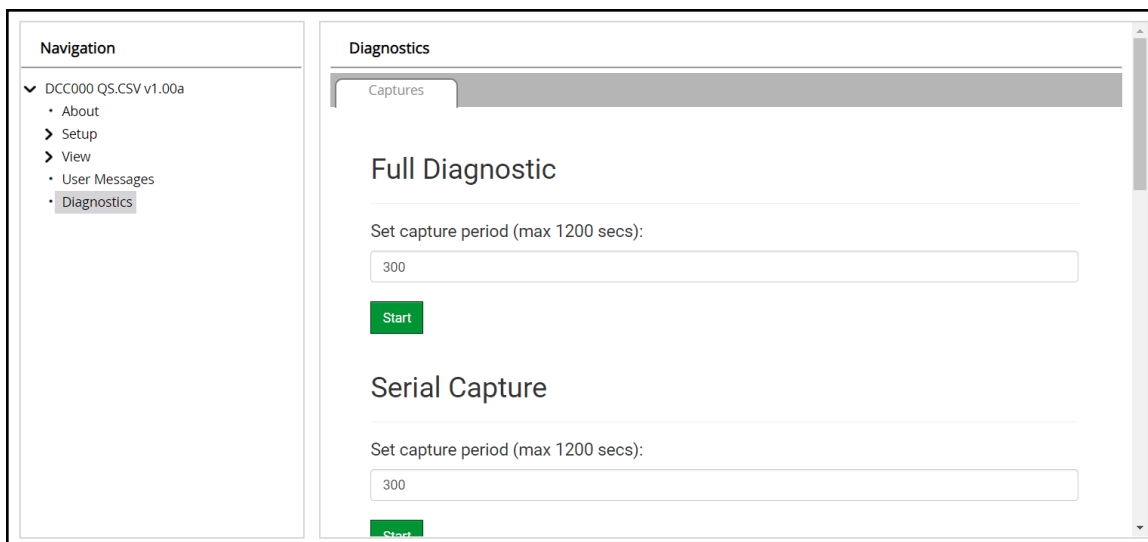


Tag	Description
SS	The SS LED will flash once a second to indicate that the bridge is in operation.
ERR	The SYS ERR LED will go on solid indicating there is a system error. If this occurs, immediately report the related "system error" shown in the error screen of the FS-GUI interface to support for evaluation.
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. 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. TX1 applies to the R1 connection while TX2 applies to the R2 connection.

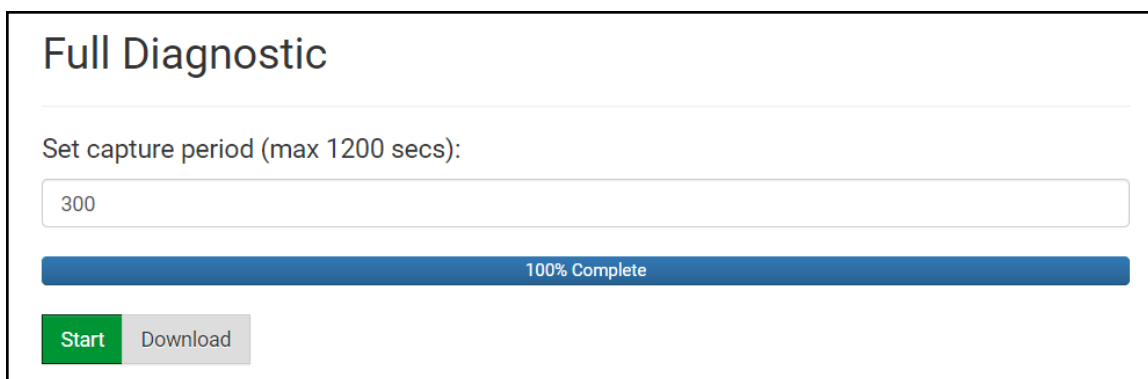
8.5 Taking a FieldServer Diagnostic Capture

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.

8.6 Factory Reset Instructions

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

8.7 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.

8.8 Wi-Fi Signal Strength

Wi-Fi
<60dBm – Excellent
<70dBm – Very good
<80dBm – Good
>80dBm – Weak

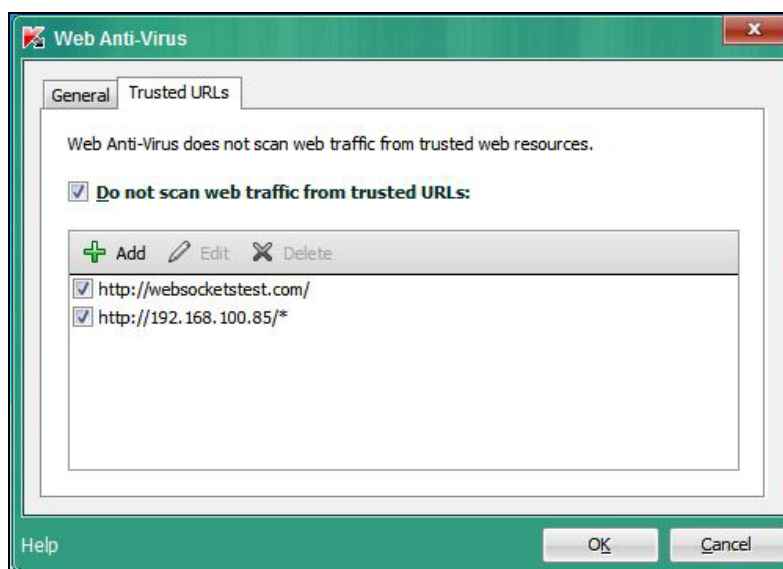
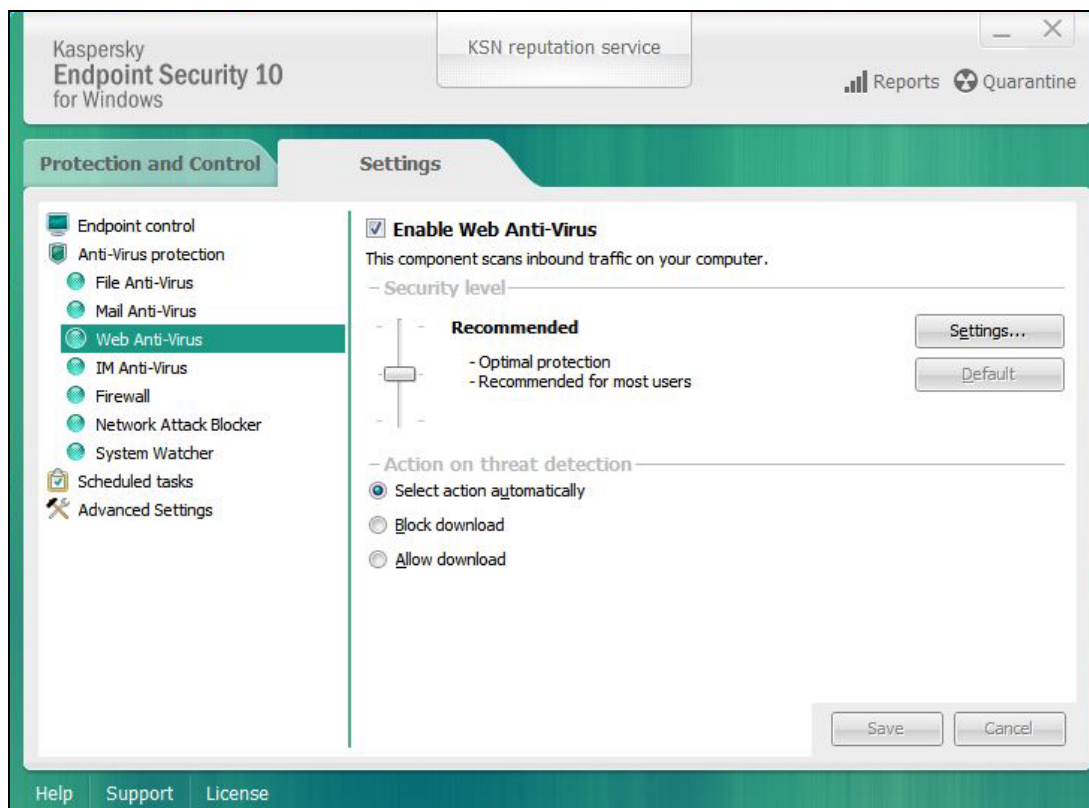
NOTE: If the signal is weak or spotty, try to improve the signal strength by checking the antenna and the FieldServer position.

8.9 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.



9 Additional Information

9.1 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 8.1 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.

NOTE: Contact Synapse Wireless to receive any firmware updates.

9.2 Mounting

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



9.3 Certification

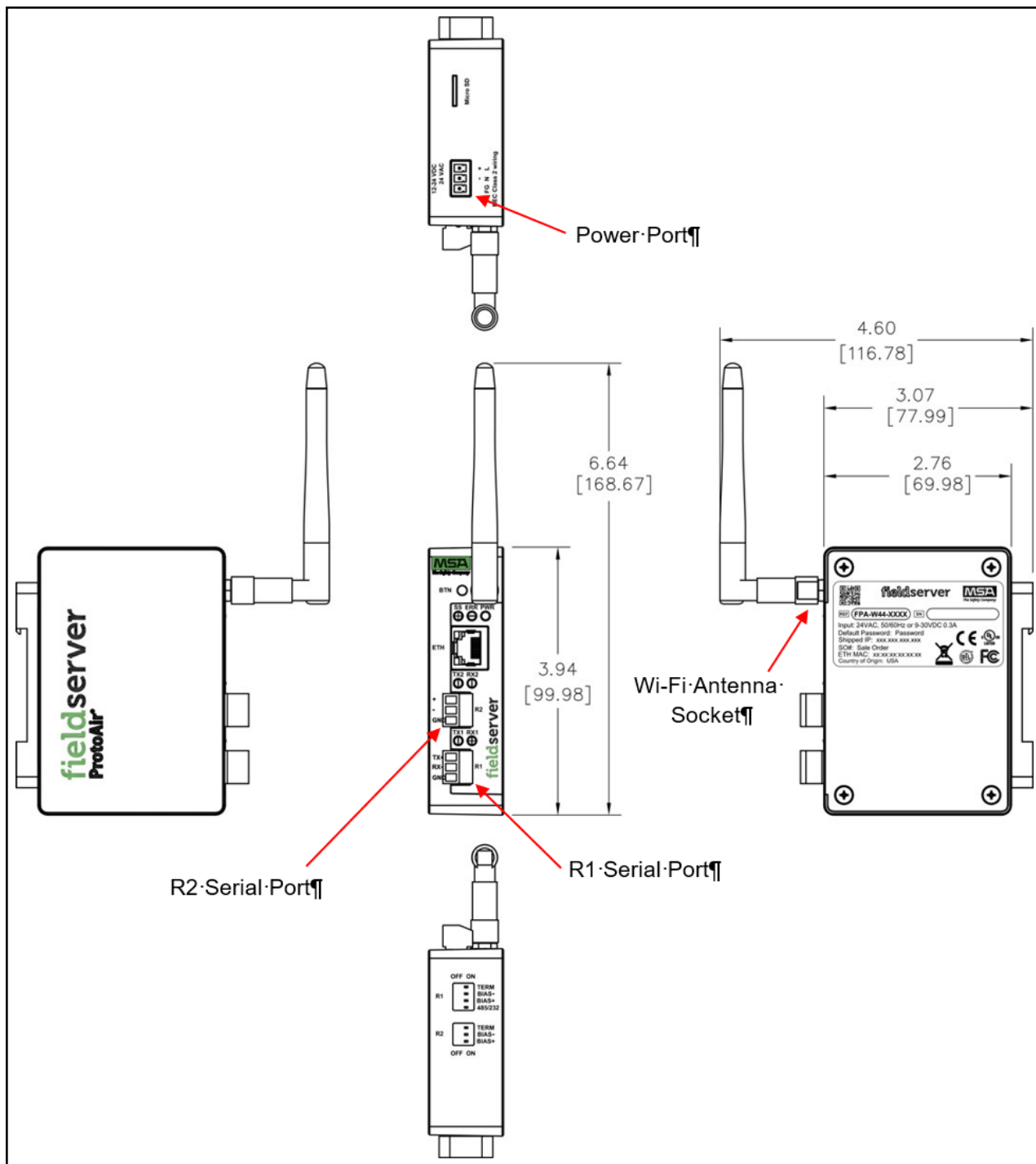


BTL Mark – BACnet Testing Laboratory

The BTL Mark on the FieldServer is a symbol that indicates that a product has passed a series of rigorous tests conducted by an independent laboratory which verifies that the product correctly implements the BACnet features claimed in the listing. The mark is a symbol of a high-quality BACnet product.

Go to www.BACnetInternational.net for more information about the BACnet Testing Laboratory. Click [here](#) for the BACnet PIC Statement. *BACnet is a registered trademark of ASHRAE.*

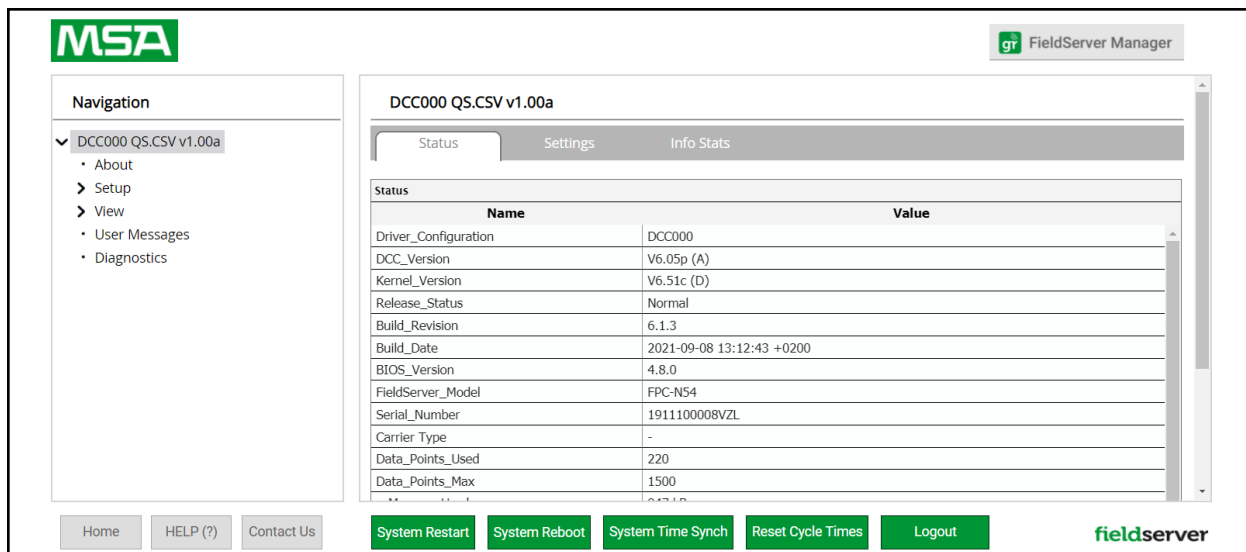
9.4 Physical Dimensions



9.5 Change Web Server Security Settings After Initial Setup

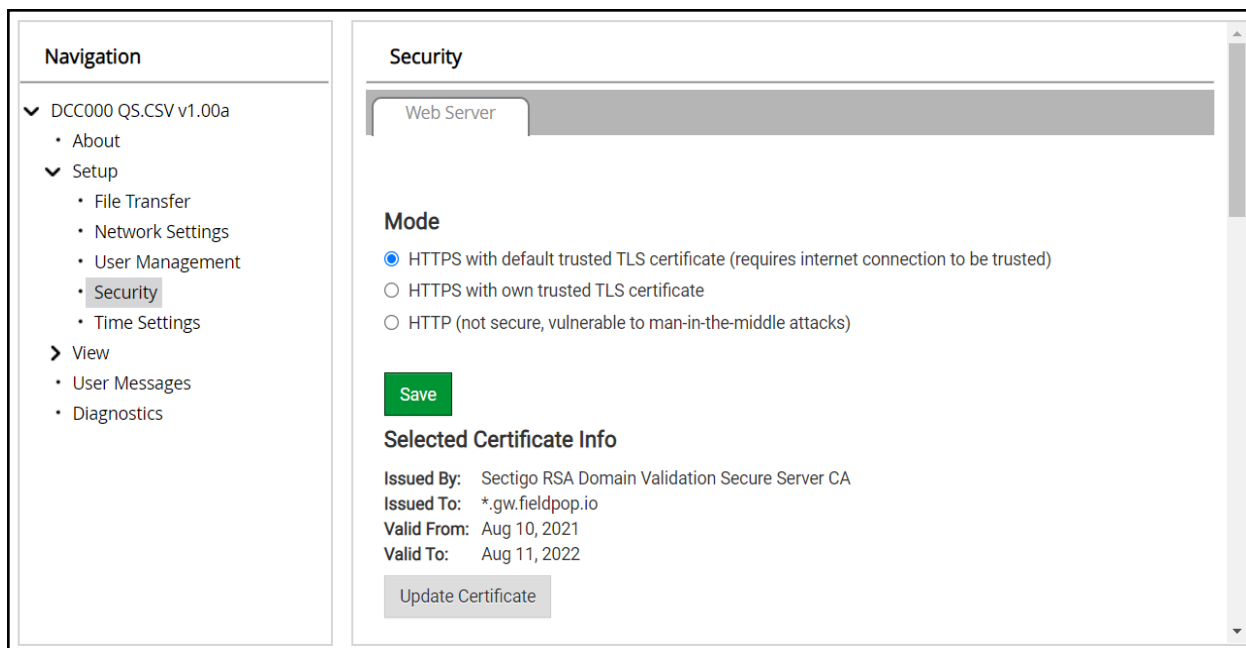
NOTE: Any changes will require a FieldServer reboot to take effect.

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



9.5.1 Change Security Mode

- Click Security in the Navigation panel.

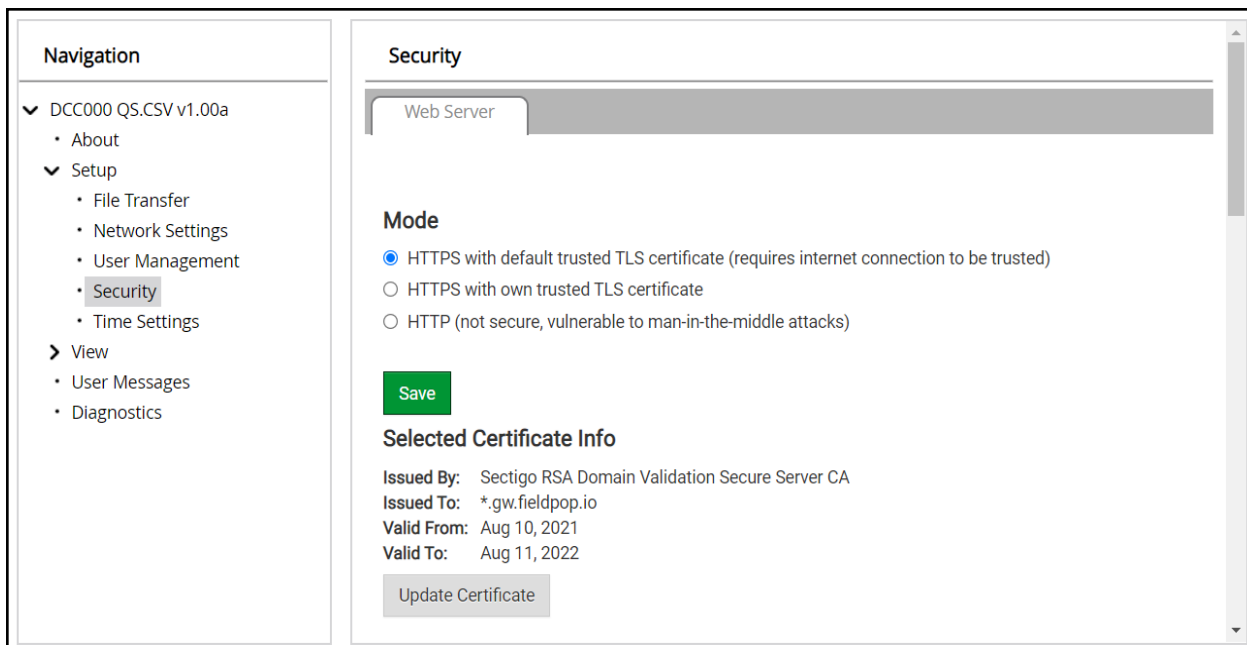


- Click the Mode desired.
 - If HTTPS with own trusted TLS certificate is selected, follow instructions in [Section 5.3.1 HTTPS with Own Trusted TLS Certificate](#)
- Click the Save button.

9.5.2 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.



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

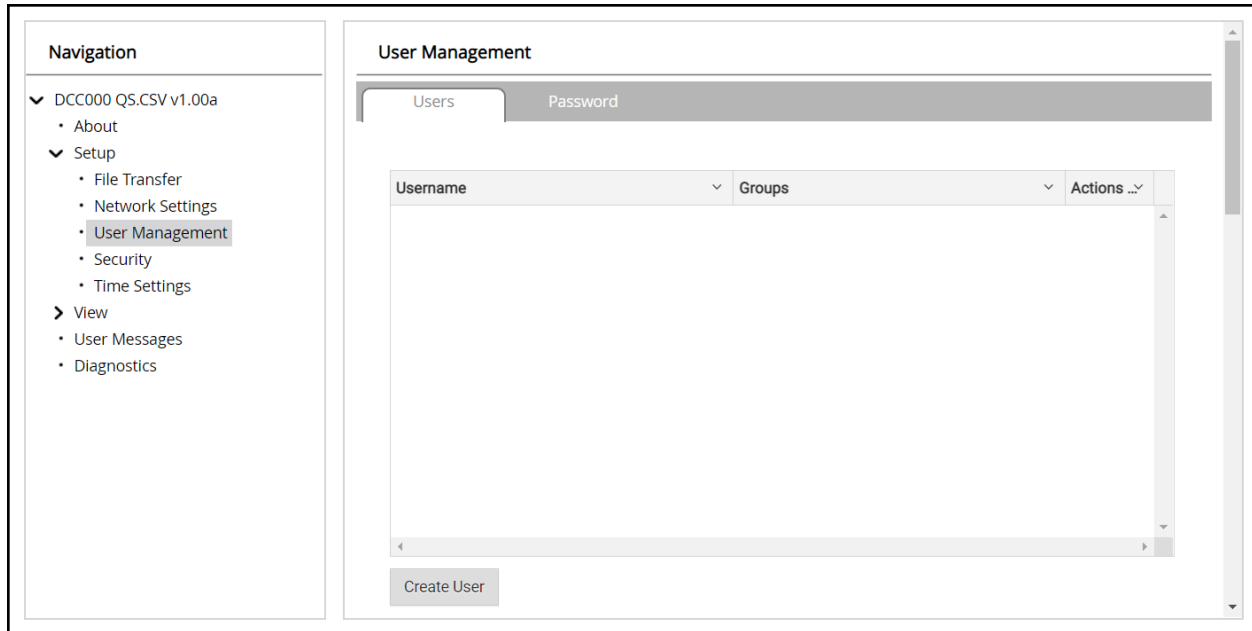
9.6 Change User Management Settings

- 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:

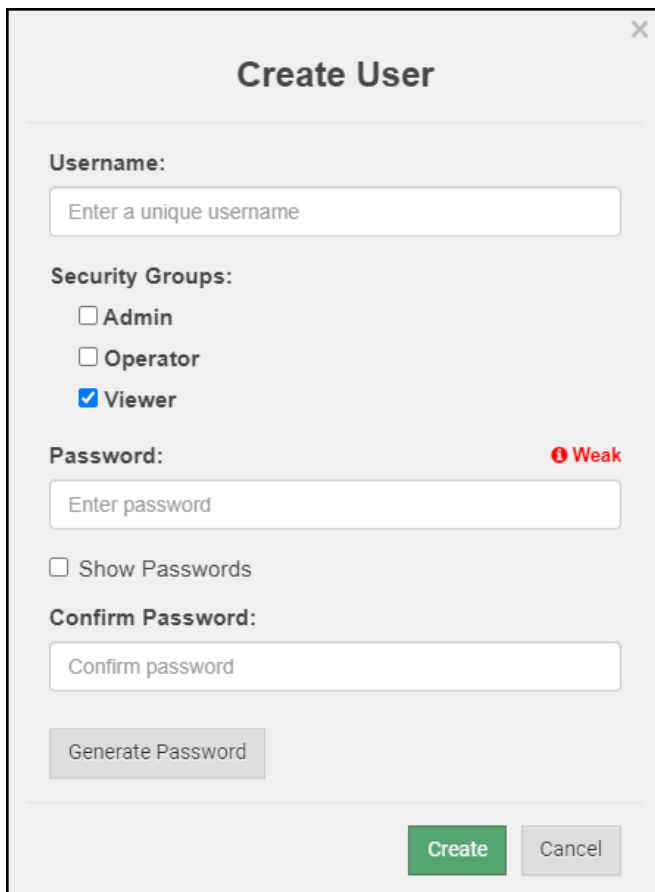
Admin – Can modify and view any settings on the FieldServer.

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

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

9.6.1 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

Generate Password

Create Cancel

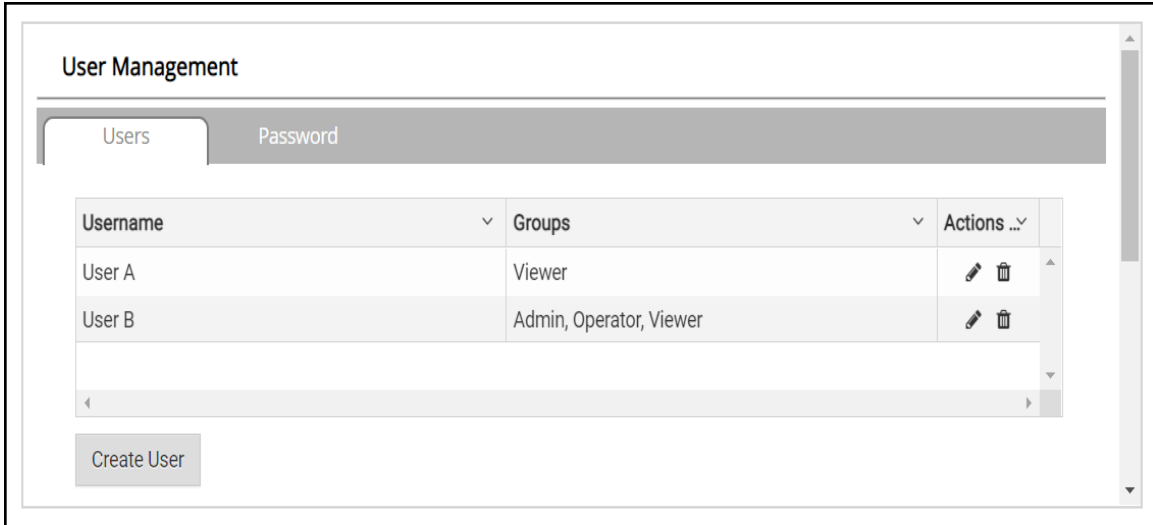
- Enter the new User fields: Name, Security Group and Password.
 - **User details are hashed and salted**

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.

9.6.2 Edit Users

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



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

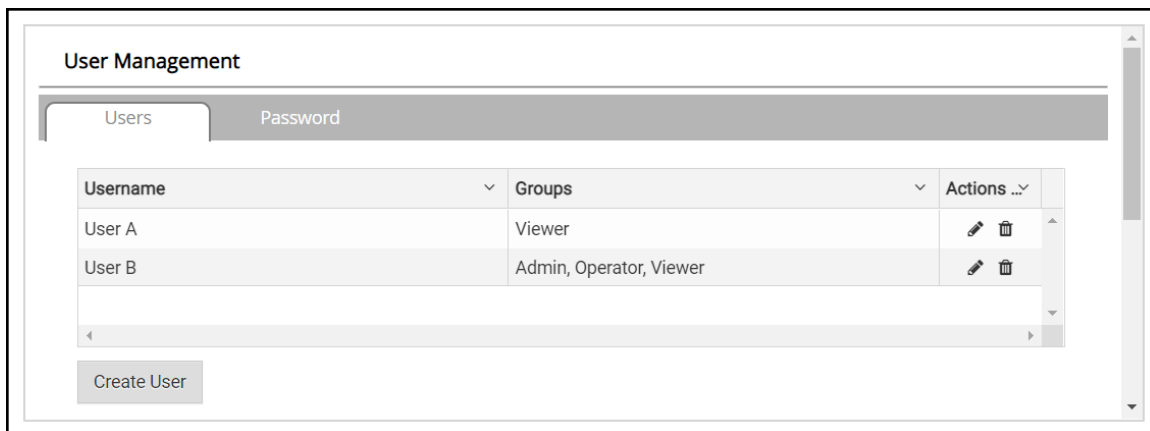
The 'Edit User' dialog box contains the following fields and options:

- Username:** A text input field containing 'User A'.
- Security Groups:** Three radio button options: Admin, Operator, and Viewer.
- Password:** A text input field containing 'Optional'.
- Show passwords
- Confirm Password:** A text input field containing 'Optional'.
-
- (green)
-

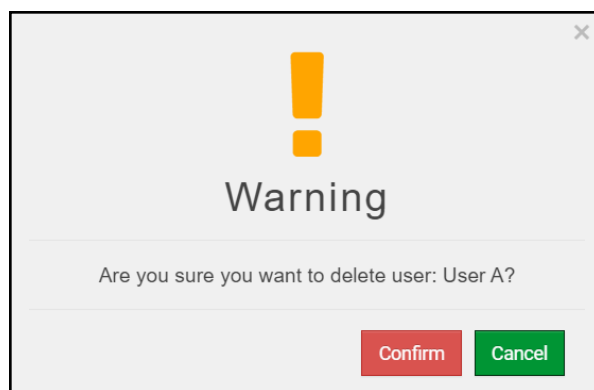
- Click Confirm.
- Once the Success message appears, click OK.

9.6.3 Delete Users

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

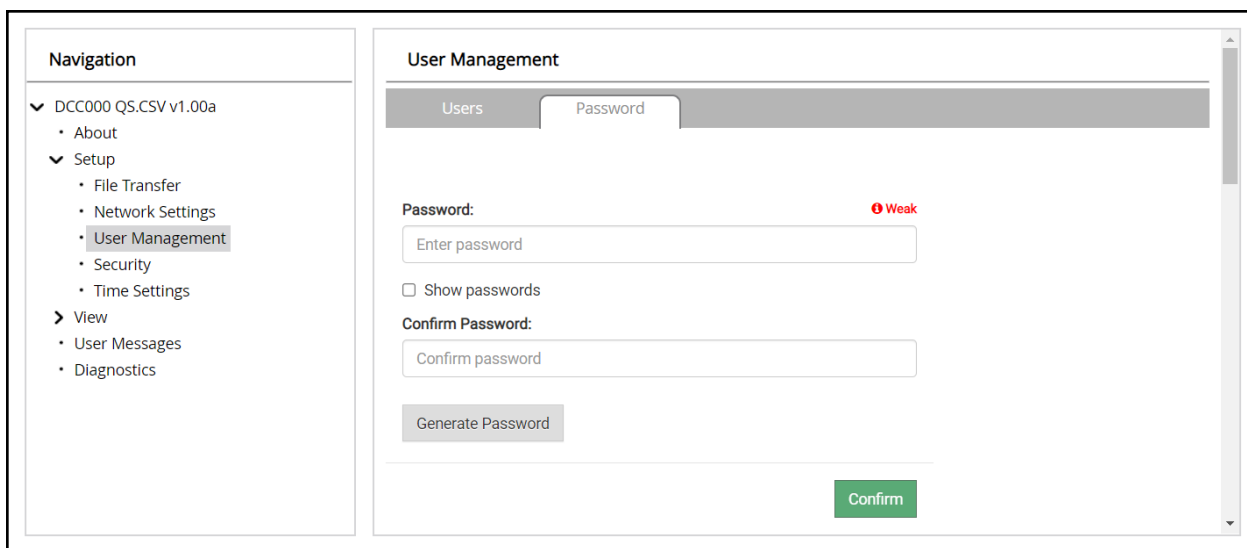


- When the warning message appears, click Confirm.



9.6.4 Change FieldServer Password

- Click the Password tab.



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

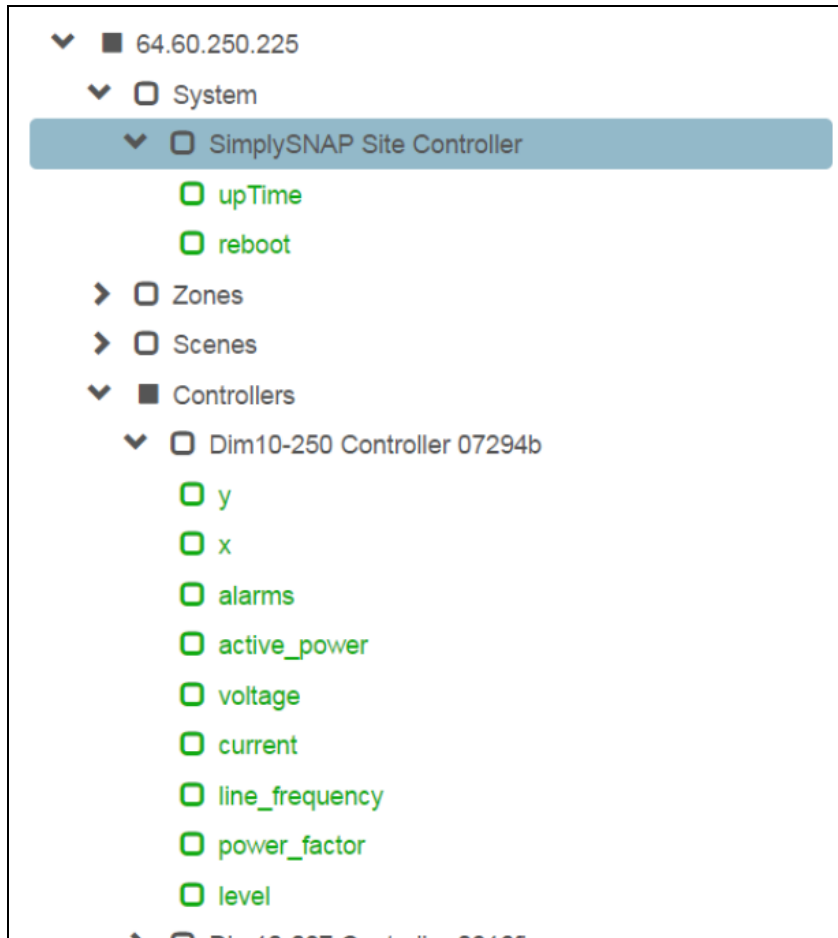
NOTE: The password must meet the minimum complexity requirements. An algorithm automatically checks the password entered and notes the level of strength on the top right of the Password text field.

9.7 Structure of the Device Tree

The Device Tree is in the following structure:

- ProtoAir IP Address
 - Device types
 - List of devices connected to this ProtoAir
 - List device parameters

For example:



10 Specifications



ProtoAir FPA-W44	
Electrical Connections	One 3-pin Phoenix connector with: RS-485/RS-232 (Tx+ / Rx- / gnd) One 3-pin Phoenix connector with: RS-485 (+ / - / gnd) One 3-pin Phoenix connector with: Power port (+ / - / Frame-gnd) One Ethernet 10/100 BaseT port
Power Requirements	<i>Input Voltage:</i> 12-24VDC or 24VAC <i>Max Power:</i> 3 Watts <i>Current draw:</i> 24VAC 0.125A 12-24VDC 0.25A @12VDC
Approvals	FCC Part 15 C, IEC 62368-1, CAN/CSA C22.2 No. 60950-1, EN IEC 62368-1:2020+A11:2020, DNP 3.0 and Modbus conformance tested, BTL marked, WEEE compliant, RoHS compliant, REACH compliant, UKCA and CE compliant, ODVA conformant, CAN ICES-003(B) / NMB-003(B)
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 to 158°F)
Humidity	10-95% RH non-condensing
Wi-Fi 802.11 b/g/n	<i>Frequency:</i> 2.4 GHz <i>Antenna Type:</i> SMA <i>Channels:</i> 1 to 11 (inclusive) <i>Encryption:</i> TKIP, WPA2 & AES

NOTE: Specifications subject to change without notice.

10.1 Compliance with EN IEC 62368-1

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

- 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.

10.2 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

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

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

2402.0 – 2480 MHz 0.004 W

2412.0 – 2462.0 MHz 0.0258 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.

11 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.