



Operating Manual
BACnet Router Wi-Fi Start-up Guide
FS-Router-BACW



Revision: 3.M

Document No.: T18621

Print Spec: 10000005389 (EO)



The Safety Company

fieldserver

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.MSAafety.com

Contents

1	BACnet Router Description	5
2	Equipment Setup	5
2.1	Mounting	5
2.2	Attaching the Antenna(s)	6
2.3	Physical Dimensions	6
3	Installation	7
3.1	Connecting the R1 & R2 Ports	7
3.1.1	Wiring	7
3.2	DIP Switch Settings	8
3.2.1	Bias Resistors	8
3.2.2	Termination Resistor	9
3.3	10/100 Ethernet Connection Port	10
4	Power up the Gateway	11
5	Connecting to the BACnet Router	12
5.1	Using the FieldServer Toolbox to Discover and Connect to the BACnet Router	12
5.2	Using a Web Browser	12
6	Setup Web Server Security	13
6.1	Login to the FieldServer	13
6.2	Select the Security Mode	15
6.2.1	HTTPS with Own Trusted TLS Certificate	16
6.2.2	HTTPS with Default Untrusted Self-Signed TLS Certificate or HTTP with Built-in Payload Encryption	16
7	Setup Network	17
7.1	Change the BACnet Router IP Address	17
7.1.1	Routing Settings	18
7.1.2	Ethernet 1	19
7.1.3	Wi-Fi Client Settings	20
7.1.4	Wi-Fi Access Point Settings	21
8	Configuring the BACnet Router	22
8.1	Navigate to the BACnet Router Settings	22
8.2	BACnet Router Settings	23
8.2.1	Button Functions	23
8.2.2	Multiple Connections	24
8.2.3	BACnet Device	24
8.2.4	BACnet/IP	25
8.2.5	BACnet MS/TP, BACnet Ethernet and BACnet Explorer	26
8.3	Router Diagnostics	27
9	BACnet Explorer	28
9.1	Discover the Device List	28
9.2	View Device Details and Explore Points/Parameters	30
9.2.1	Edit the Present Value Field	32
10	MSA Grid - FieldServer Manager Setup	33
10.1	Create a New FieldServer Manager Account	33
10.2	Login to the FieldServer Manager	39
11	Troubleshooting	40
11.1	Tooltips	40
11.2	Taking a FieldServer Diagnostic Capture	41

11.3	Factory Reset Instructions	42
11.4	Internet Browser Software Support	42
11.5	Wi-Fi Signal Strength	42
12	Additional Information	43
12.1	Change Web Server Security Settings After Initial Setup	43
12.1.1	Change Security Mode	44
12.1.2	Edit the Certificate Loaded onto the FieldServer	44
12.2	Change User Management Settings	45
12.2.1	Create Users	46
12.2.2	Edit Users	47
12.2.3	Delete Users	48
12.2.4	Change FieldServer Password	48
12.3	Specifications	49
12.4	Warnings for FCC and IC	50
13	Limited 2 Year Warranty	53

1 BACnet Router Description

The BACnet Router provides stand-alone routing between BACnet networks such as BACnet/IP, BACnet Ethernet, and BACnet MS/TP – thereby allowing the system integrator to mix BACnet network technologies within a single BACnet internetwork. There are three physical communication ports on the BAS Router. One is a 10/100 Mbps Ethernet port and the other two are RS-485 MS/TP ports. Configuration is accomplished via a web page.

The BACnet Router with Wi-Fi (FS-ROUTER-BACW) model has one RS-485 port, one Ethernet 10/100 port and supports Wi-Fi network connection. Additionally, the Router acts as a Wi-Fi access point for modern web based configuration and remote access from any mobile device without user restrictions.

The BACnet Router is cloud ready and connects with the Grid MSA Safety's FieldServer cloud platform.

NOTE: A cellular version of the BACnet Router is not available.

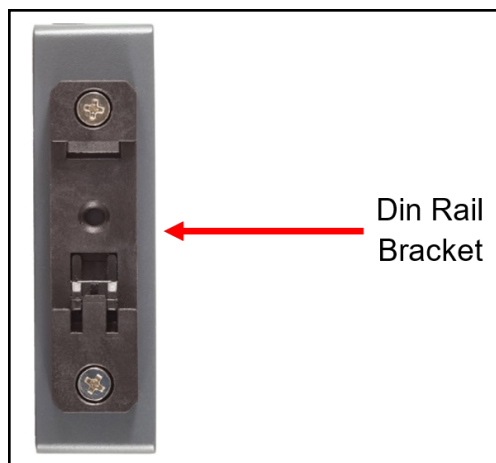
NOTE: For MSA Grid – FieldServer Manager information, refer to the [MSA Grid - FieldServer Manager Start-up Guide](#) online through the MSA website.

NOTE: The latest versions of instruction manuals, driver manuals, configuration manuals and support utilities are available online through the [MSA FieldServer webpage](#).

2 Equipment Setup

2.1 Mounting

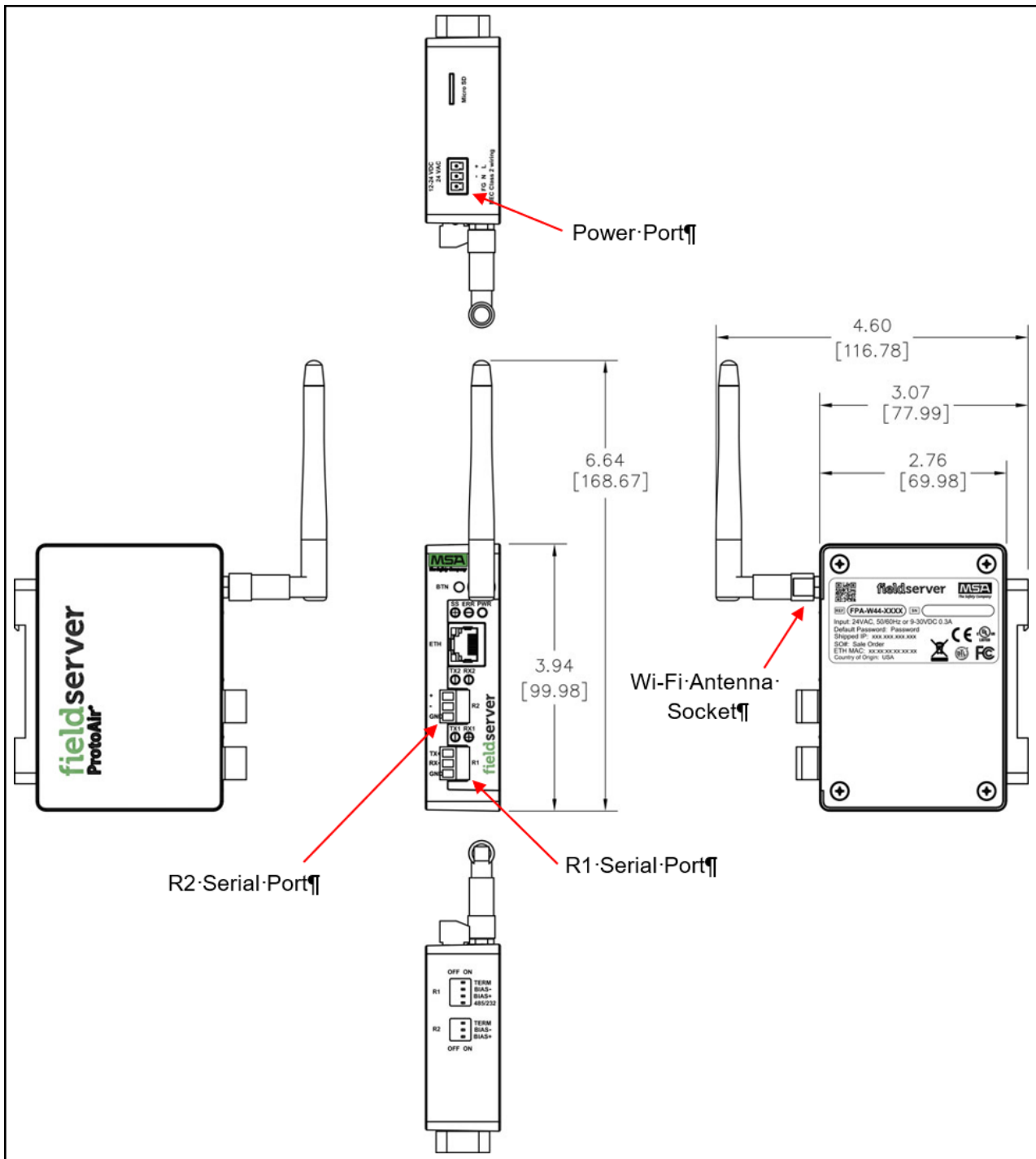
The gateway can be mounted using the DIN rail mounting bracket on the back of the unit.



2.2 Attaching the Antenna(s)

Screw in the Wi-Fi antenna to the front of the unit as shown in [Section 2.3 Physical Dimensions](#).

2.3 Physical Dimensions



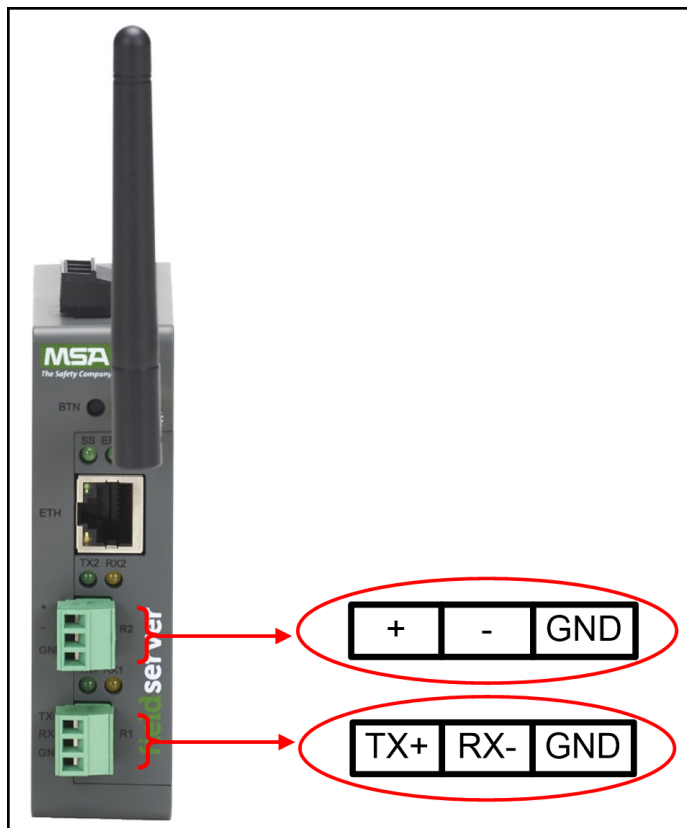
3 Installation

3.1 Connecting the R1 & R2 Ports

The R1 and R2 Ports are RS-485.

NOTE: For the R1 Port, ensure RS-485 is selected by checking the number 4 DIP Switch is set to the left side.

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



The following baud rates are supported:
9600, 19200, 38400, 76800

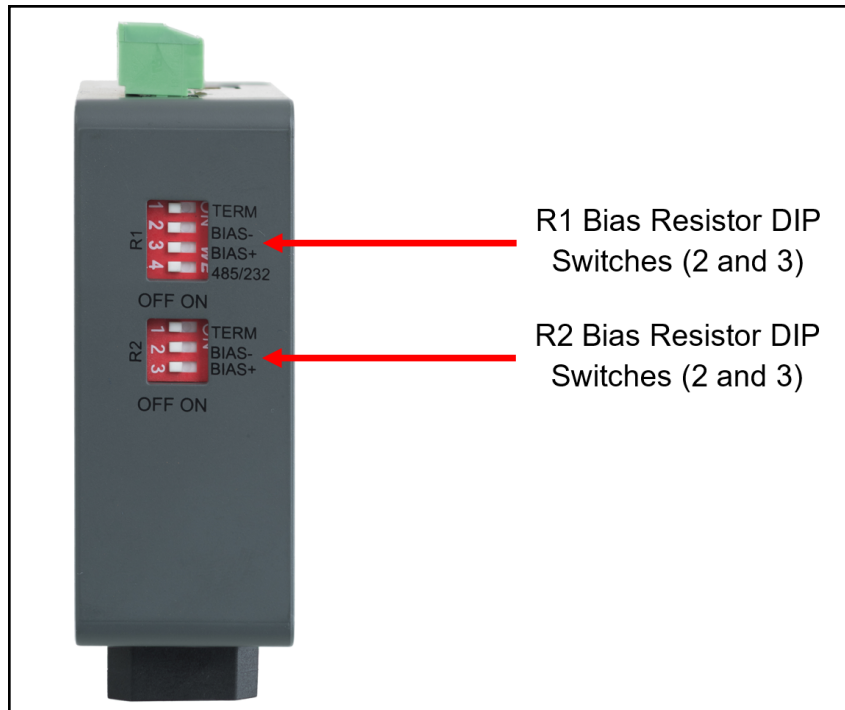
3.1.1 Wiring

RS-485	
BMS RS-485 Wiring	Gateway Pin Assignment
RS-485 +	TX +
RS-485 -	RX -
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 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).

3.2 DIP Switch Settings

3.2.1 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.

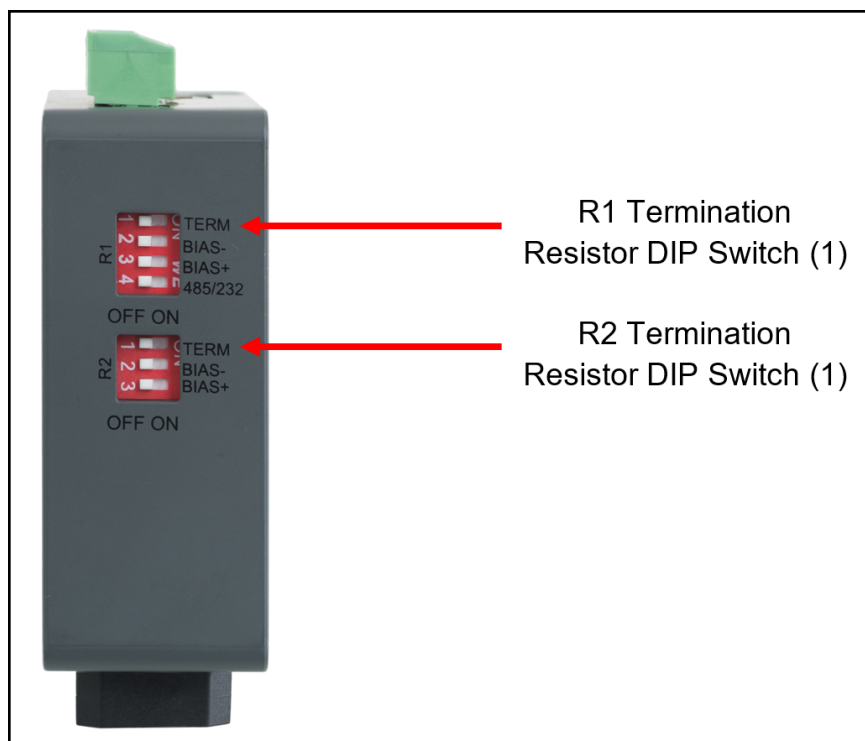
The bias resistor is 510 ohms which is in line with the BACnet spec. It should only be enabled at one point on the bus (for example, on the field port where there are very weak bias resistors of 100k). Since there are no jumpers, many BACnet Routers can be put on the network without running into the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

3.2.2 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.**

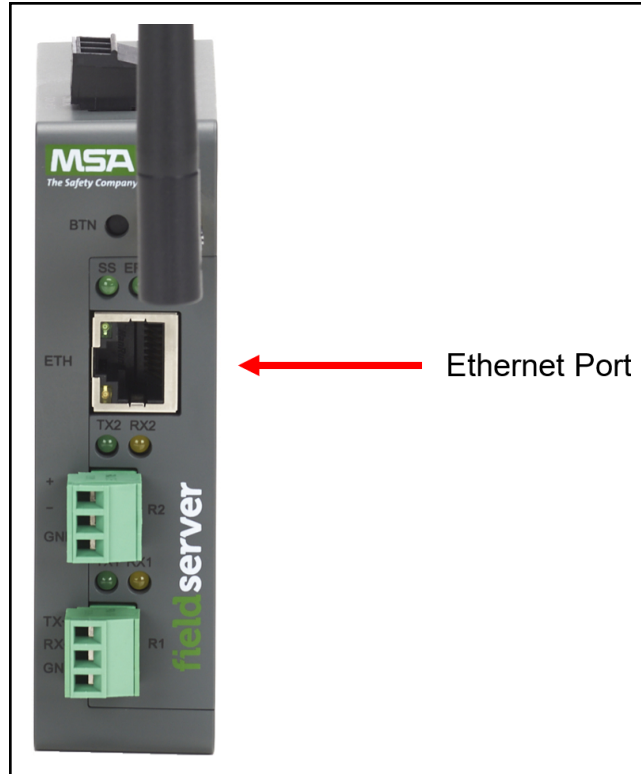
The termination resistor is also used to reduce noise. It pulls the two lines of an idle bus together. However, the resistor would override the effect of any bias resistors if connected. The R1 termination resistor is 120 Ohms.

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.

3.3 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 192.168.2.101, Subnet Mask is 255.255.255.0.

4 Power up the Gateway

Check power requirements in the table below:

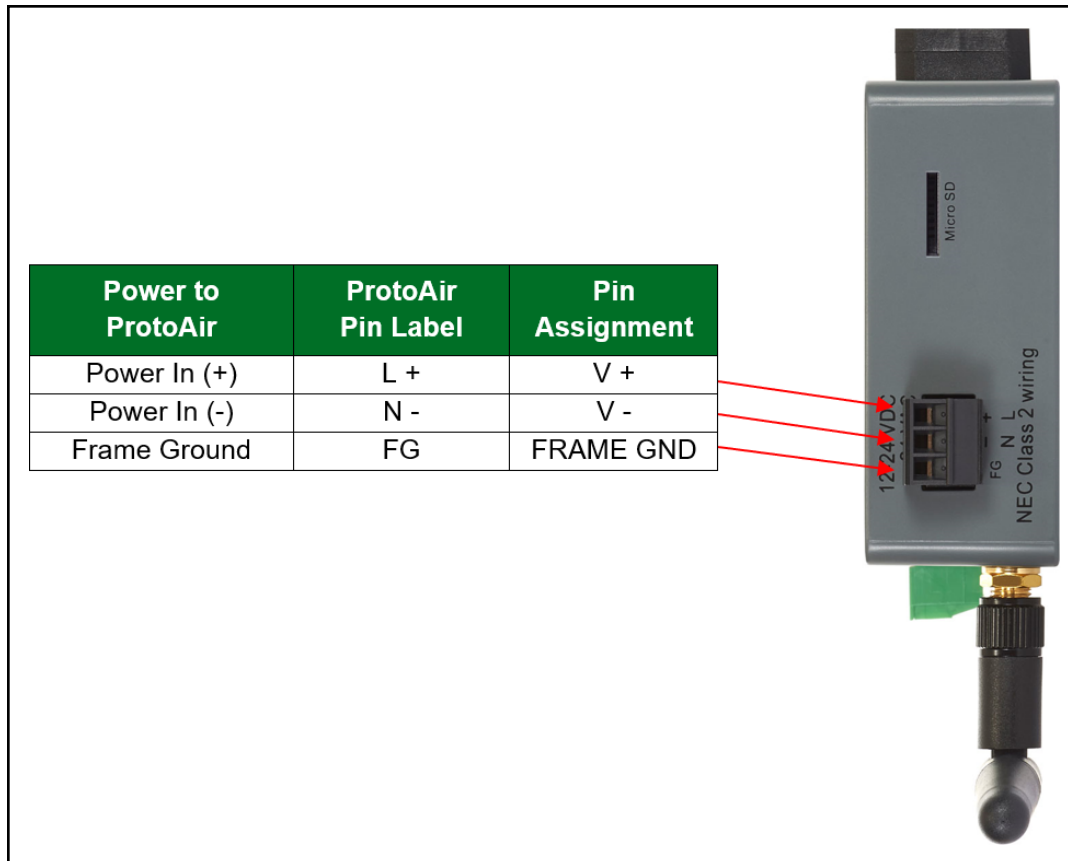
Power Requirement for BACnet Router External Gateway		
BACnet Router Family	Current Draw Type	
	12VDC	24VDC/AC
FS-ROUTER-BACW (Typical)	250mA	125mA

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 BACnet Router as shown below. Ensure that the power supply used complies with the specifications provided in [Section 12.3 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.



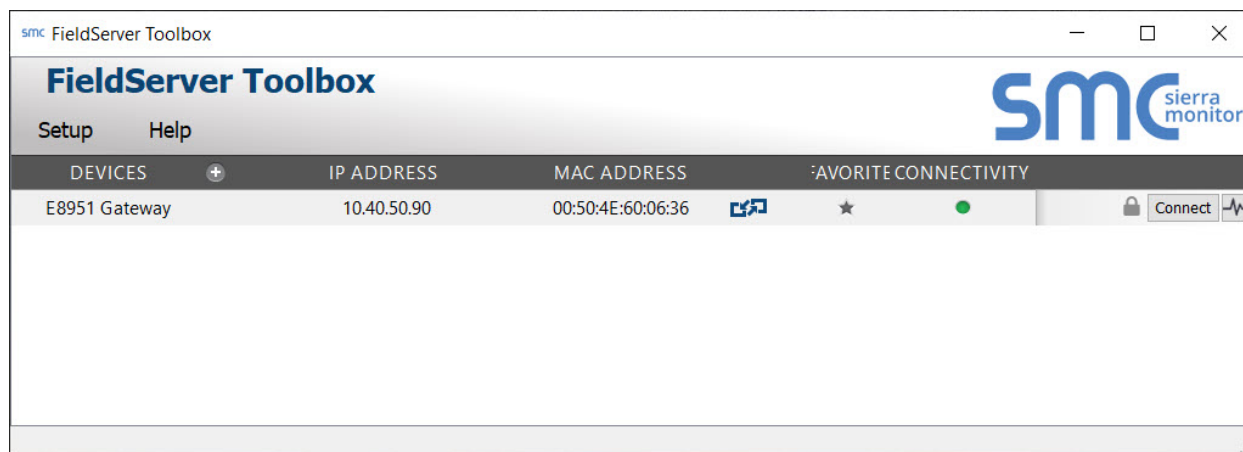
5 Connecting to the BACnet Router

The FieldServer Toolbox Application can be used to discover and connect to the BACnet Router on a local area network. To manually connect to the BACnet Router 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.

5.1 Using the FieldServer Toolbox to Discover and Connect to the BACnet Router

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

NOTE: If the connect button is grayed out, the BACnet Router's IP Address must be set to be on the same network as the PC. (Section [5.2 Using a Web Browser](#))



5.2 Using a Web Browser

- Open a web browser and connect to the BACnet Router's default IP Address. The default IP Address of the BACnet Router is **192.168.2.101**, Subnet Mask is **255.255.255.0**.
- If the PC and the BACnet Router are on different IP networks, assign a static IP Address to the PC on the 192.168.2.X network.

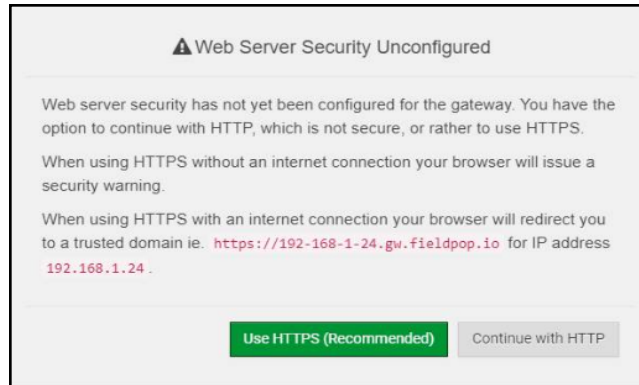
NOTE: Check Section [11.4 Internet Browser Software Support](#) for supported browsers.

6 Setup Web Server Security

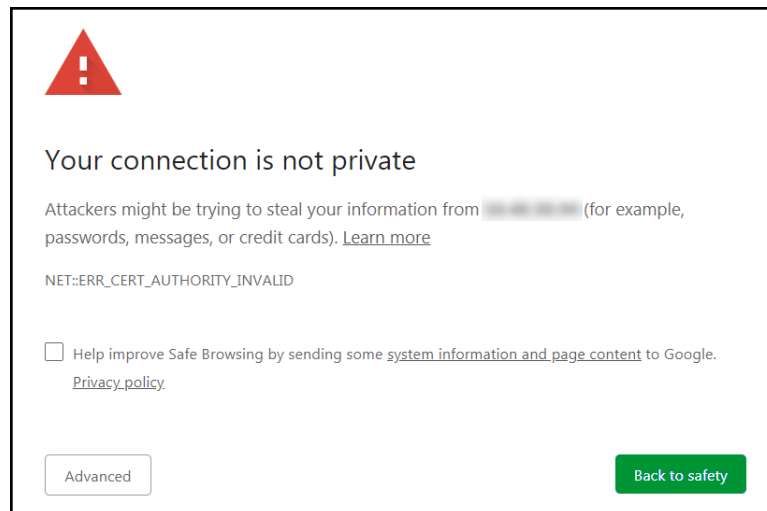
6.1 Login to the FieldServer

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.

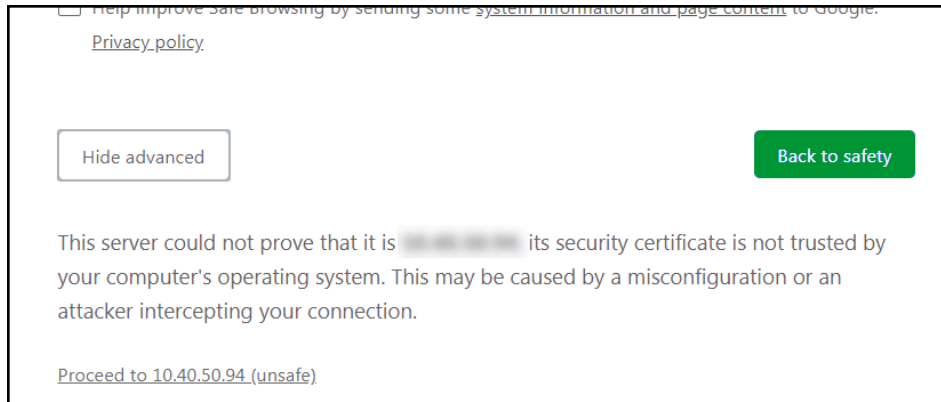
- When the Web Server Security Unconfigured window appears, read the text and choose whether to move forward with HTTPS or HTTP.



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

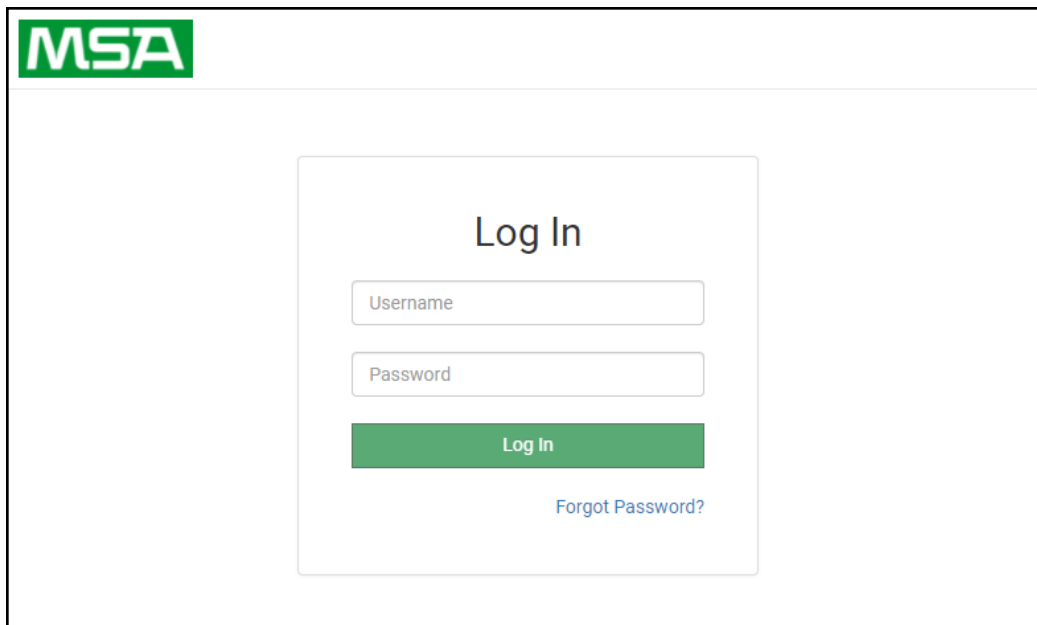


- Additional text will expand below the warning, click the underlined text to go to the IP Address. In the example below this text is “[Proceed to <FieldServer IP> \(unsafe\)](#)”.



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

6.2 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)

Save

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.

6.2.1 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

```
XzyMbQZFiRuJZJPe7CTHLcHOrHLowofUoVtaBMYd4d6VGdNklKazByWKcNOL7mrX
A4IBAQBfM+IPvOx3T/47VEmaiXqE3bx3zEuBFJ6pWPlw7LHf2r2ZoHw+9xb+aNMU
dVyAelhBMTMsnI2ERvQVp0xj3psSv2EJyKXS1bOYNRLsq7UzpwuAdT/Wy3o6vUM5
K+Cwf9qEoQ0LuxDZTIEct67MkcHMiuFi5pk7TRicHnQf/sfOAYOulduHOy9exlk9
FmHFVDIZt/cJUaF+e74EuSph+gEr0lQo2wmmhyc7L22UXse1NoOfu2Zg0Eu1VWtu
JRryaMwIRFEWuuzMGZtKFWVC+8q2JQsVcqiRWM7naoblEhOCMH+sKHJMCxDoXGt
vtZjpZUoAL51YXxWSVcyZdGiAP5e
-----END CERTIFICATE-----
```

Private Key

```
sHB0zZoHr4YQSDK2BbYVzzbl0LDuKtc8+JiO3ooGjoTuHnqkeAj/fkfbTAsKeAzw
gKQe+H5UQNK0bdvZfOJrm6daDK2vDmR5k+juUhej5N49uplroB97MQgYotzgf+
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.

6.2.2 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.

7 Setup Network

Navigate to the Network Settings tab and configure the settings as needed.

7.1 Change the BACnet Router IP Address

Configure the IP settings of the BACnet Router using the following sections of the Network page:

- If using the Ethernet port to connect to the local network, scroll to “ETH 1” ([Section 7.1.2 Ethernet 1](#)).
- If connecting the BACnet Router to a local wireless network, scroll to “WiFi Client Settings” ([Section 7.1.3 Wi-Fi Client Settings](#)).
- If updating Wi-Fi Access Point settings, scroll to “WiFi Access Point Settings” ([Section 7.1.4 Wi-Fi Access Point Settings](#)).

7.1.1 Routing Settings

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

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.

ETH 1 WiFi Client WiFi Access Point Routing

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

7.1.2 Ethernet 1

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 shows the network configuration page for 'ETH 1'. It features four tabs: 'ETH 1' (selected), 'WiFi Client', 'WiFi Access Point', and 'Routing'. The main configuration area includes a checkbox for 'Enable DHCP' which is unchecked. Below this are input fields for 'IP Address' (10.40.50.92), 'Netmask' (255.255.255.0), 'Gateway' (10.40.50.1), 'Domain Name Server 1 (Optional)' (10.40.2.24), and 'Domain Name Server 2 (Optional)' (10.15.130.15). At the bottom left are 'Cancel' and 'Save' buttons. On the right side, a 'Network Status' box displays 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

7.1.3 Wi-Fi Client Settings

- Set the Wi-Fi Status to ENABLED for the BACnet Router 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 7.1.1 Routing Settings](#)) to set the default connection to Wi-Fi Client.

The screenshot displays the 'WiFi Client' configuration page. At the top, there are tabs for 'ETH 1', 'WiFi Client', 'WiFi Access Point', and 'Routing'. The 'WiFi Client' tab is active.

Configuration Fields:

- Enable**
- SSID:** FieldSVR
- Password (Optional):** [Redacted]
- Enable DHCP**
- IP Address:** 10.40.50.37
- 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 Panel:

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

At the bottom left, there are 'Cancel' and 'Save' buttons.

7.1.4 Wi-Fi Access Point Settings

- Check the Enable tick box to allow connecting to the BACnet Router 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.

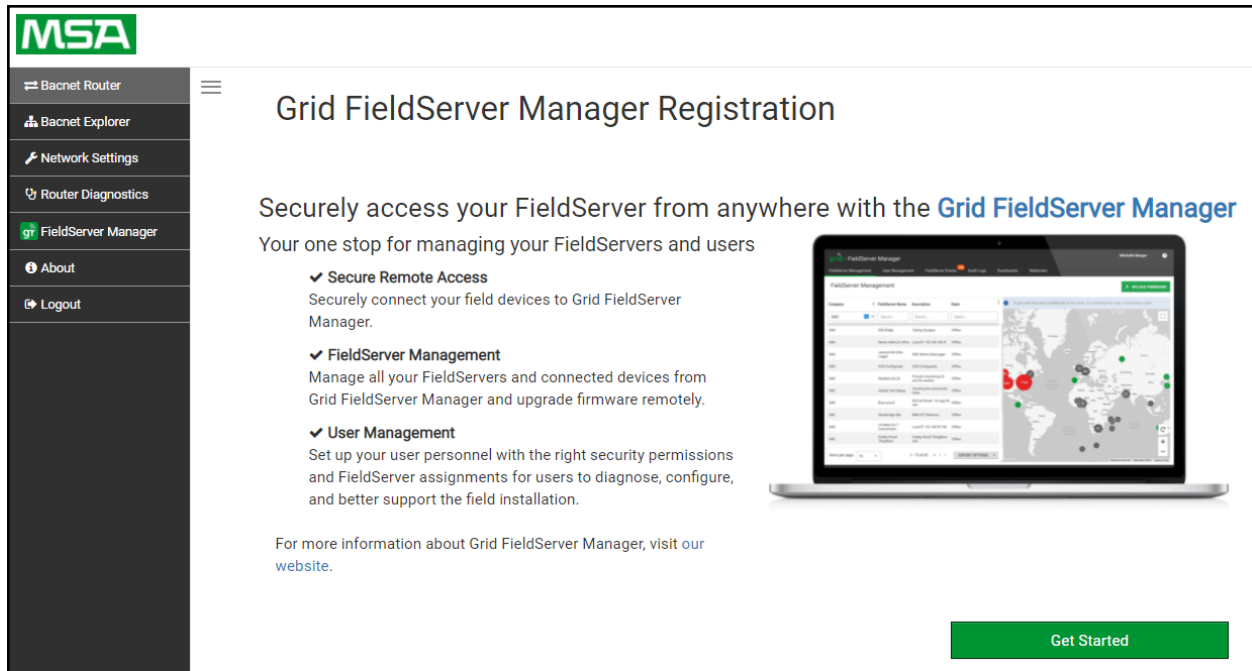
NOTE: If the webpage was open in a browser via Wi-Fi, the browser will need to be updated with the new Wi-Fi details before the webpage will be accessible again.

The screenshot displays the configuration page for the WiFi Access Point. The interface includes several tabs: 'ETH 1', 'WiFi Client', 'WiFi Access Point' (which is the active tab), and 'Routing'. Under the 'WiFi Access Point' tab, there is an 'Enable' checkbox. Below it, the 'SSID' is set to 'ProtoAir-6001FD', and the 'Password (Optional)' is masked with dots. The 'Channel' is set to 11. There are checkboxes for 'Allow others to find this network' (checked) and 'Enable hotspot'. The IP configuration section includes 'IP Address' (192.168.50.1), 'Netmask' (255.255.255.0), 'IP Pool Address Start' (192.168.50.120), and 'IP Pool Address End' (192.168.50.130). At the bottom left are 'Cancel' and 'Save' buttons. On the right side, a 'Network Status' box shows 'Connection Status' as 'Disabled', 'Access Point MAC Address' as 'a0:cc:2b:ff:ab:59', and various message counts (Tx/Rx Msgs and Dropped) all set to 0.

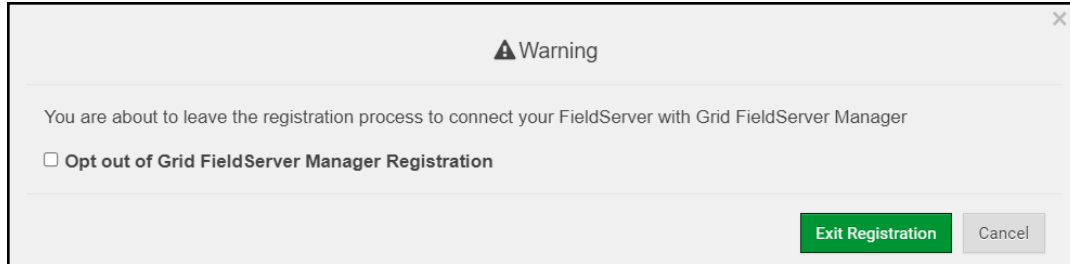
8 Configuring the BACnet Router

8.1 Navigate to the BACnet Router Settings

- From the Web App landing page, click the BACnet Router tab on the left side of the screen.



- A warning message will appear when performing the first-time setup, click the Exit Registration button to continue to the Settings page.



8.2 BACnet Router Settings

The screenshot shows the configuration page for a BACnet Router. The left sidebar contains navigation options: BACnet Router, BACnet Explorer, Network Settings, Router Diagnostics, FieldServer Manager, About, and Logout. The main content area is organized into several panels:

- BACnet Device:** Fields for Device Name (BACnet Router), Device Instance (1000), Device Location (-), and Device Connection (BACnet IP Wired 1).
- BACnet Ethernet:** Fields for Enable (checkbox), and Network Number (3).
- BACnet IP Wired 1:** Fields for Enable (checked), Network Number (1), and IP Port (47808).
- BACnet IP Wired 2:** Fields for Enable (checkbox), Network Number (2), and IP Port (47809).
- BACnet IP BBMD:** Field for Enable (checkbox).
- BACnet MSTP Settings:** Fields for Max Info Frames (50) and Max Master (127).
- BACnet MSTP R1:** Fields for Enable (checkbox), Network Number (4), MAC Address (0), Baud Rate (38400), and Token Usage Timeout (50).
- BACnet MSTP R2:** Field for Enable (checkbox).

On the right side, there are four buttons: Save (green), Restart (green), Reload (grey), and Defaults (grey). Below these is a Status box showing 'Router is online' and a Log box.

8.2.1 Button Functions



- **Save** – write the currently displayed settings to the device. A restart will be required to apply the updated settings.
- **Reload** – discard the currently displayed settings and reload the settings stored on the device. This will undo any unsaved edits.
- **Defaults** – discard the currently displayed settings and load default settings. This must still be saved and the device must be restarted for the default settings to be applied.
- **Restart** – restarts the device.

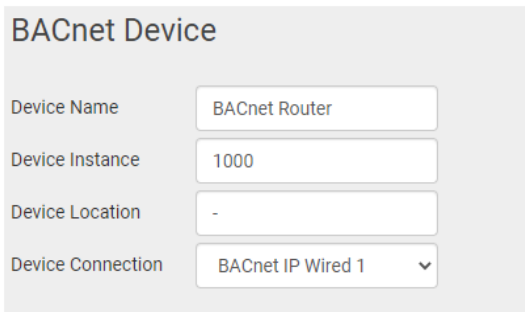
8.2.2 Multiple Connections

- **Network Number** – set up the BACnet network number for the connection. Legal values are 1-65534. Each network number must be unique across the entire BACnet internetwork. . All devices that are interconnected by the same IP network and that can reach one another through local IP broadcasts (including local IP broadcasts forwarded by BBMD) should be treated as a single BACnet network segment, and hence all routing ports connected to this segment should have the same globally unique network number.

NOTE: Each BACnet network segment, regardless of technology, must have a unique network number. For example, a single RS-485 MS/TP segment or BACnet/IP subnet, can each be regarded as a BACnet network segment. All routing ports that connect directly to the same segment should also assign the same globally unique network number to that segment.

- **Enable** – enable or disable the connection; note that BACnet/IP Primary is always enabled.

8.2.3 BACnet Device



The screenshot shows a configuration form titled "BACnet Device". It contains four fields:

- Device Name:** A text input field containing "BACnet Router".
- Device Instance:** A text input field containing "1000".
- Device Location:** A text input field containing "-".
- Device Connection:** A dropdown menu with "BACnet IP Wired 1" selected.

- **Device Instance** and **Device Name** – a BACnet Router must provide a Device Object. Configure its name and Instance Number here. Take care to select a Device Instance Number that is unique across the entire BACnet internetwork.
- **Device Location** – enter a location for the Device. The location may not contain any commas.
- **Device Connection** – select which connection to bond the BACnet device settings.

8.2.4 BACnet/IP

BACnet IP Wired 1

Enable

Network Number

IP Port

BACnet IP Wired 2

Enable

Network Number

IP Port

BACnet IP WiFi

Enable

Network Number

IP Port

BACnet IP BBMD

Enable

BBMD Connection

Public IP Address

Public IP Port

[Edit BDT](#)

- **IP Port** – the BACnet/IP default is 47808 (0xBAC0), but a different port number may be specified here.
- **IP Port** – this MUST be different to the IP Port used on the BACnet/IP Primary connection. Default is 47809 (0xBAC1).
- **BBMD Connection** – select which connection to bond the BACnet/IP BBMD settings.
- **Public IP Address and Port** – if the BBMD is being accessed across a NAT Router, then these values must be configured with the public IP Address and Port by which the BBMD can be reached from across the NAT Router. The Public IP Address and Port would also be used in the BDT of remote BBMD's that need to reach this BBMD across the NAT Router. If no NAT Router is being used, these fields can be left blank. For example, type into a Google browser “my IP Address” to see the local PC’s Public IP Address.

8.2.5 BACnet MS/TP, BACnet Ethernet and BACnet Explorer

BACnet Ethernet

Enable

Network Number

BACnet MSTP Settings

Max Info Frames

Max Master

BACnet MSTP R1

Enable

Network Number

MAC Address

Baud Rate

Token Usage Timeout (ms)

BACnet MSTP R2

Enable

Network Number

MAC Address

Baud Rate

Token Usage Timeout (ms)

BACnet Explorer

Network Number

- **Max Info Frames** – the number of transactions the Router may initiate while it has the MS/TP token. Default is 50.
- **Max Master** – the highest MAC address to scan for other MS/TP master devices. The default of 127 is guaranteed to discover all other MS/TP master devices on the network.
- **MAC Address** – legal values are 0 to 127, must be unique on the physical network.
- **Baud Rate** – the serial baud rate used on the network.
- **Token Usage Timeout (ms)** – the number of milliseconds the router will wait before deciding that another master has dropped the MS/TP token. This value must be between 20ms and 100ms. Choose a larger value to improve reliability when working with slow MS/TP devices that may not be able to meet strict timing specifications.

8.3 Router Diagnostics

By clicking on the Router Diagnostics tab all the connection communication details can be viewed to ensure the BACnet Router is working correctly.

The screenshot displays the MSA FieldServer Manager interface. On the left is a navigation menu with the following items: BACnet Router, BACnet Explorer, Network Settings, Router Diagnostics (highlighted), FieldServer Manager, About, and Logout. The main content area is divided into two sections.

ETH1 - BACnet IP Wired 1

Network Number	1	
Info Statistics	Messages Sent	270
	Messages Received	280
Error Statistics	Total Errors	0


Routing Table

DNET	MAC Address	Status
5	10.40.51.113:47808	Available
6	10.40.50.80:47808	Available
50	10.40.50.103:47808	Available
181	10.40.50.181:47808	Available
1100	10.40.50.73:47808	Available
1200	10.40.50.73:47808	Available
50001	10.40.50.88:47808	Available
50003	10.40.50.88:47808	Available
60003	10.40.50.116:47808	Available

ETH1 - BACnet Explorer 47800

Network Number	7	
Info Statistics	Messages Sent	258
	Messages Received	246
Error Statistics	Total Errors	0

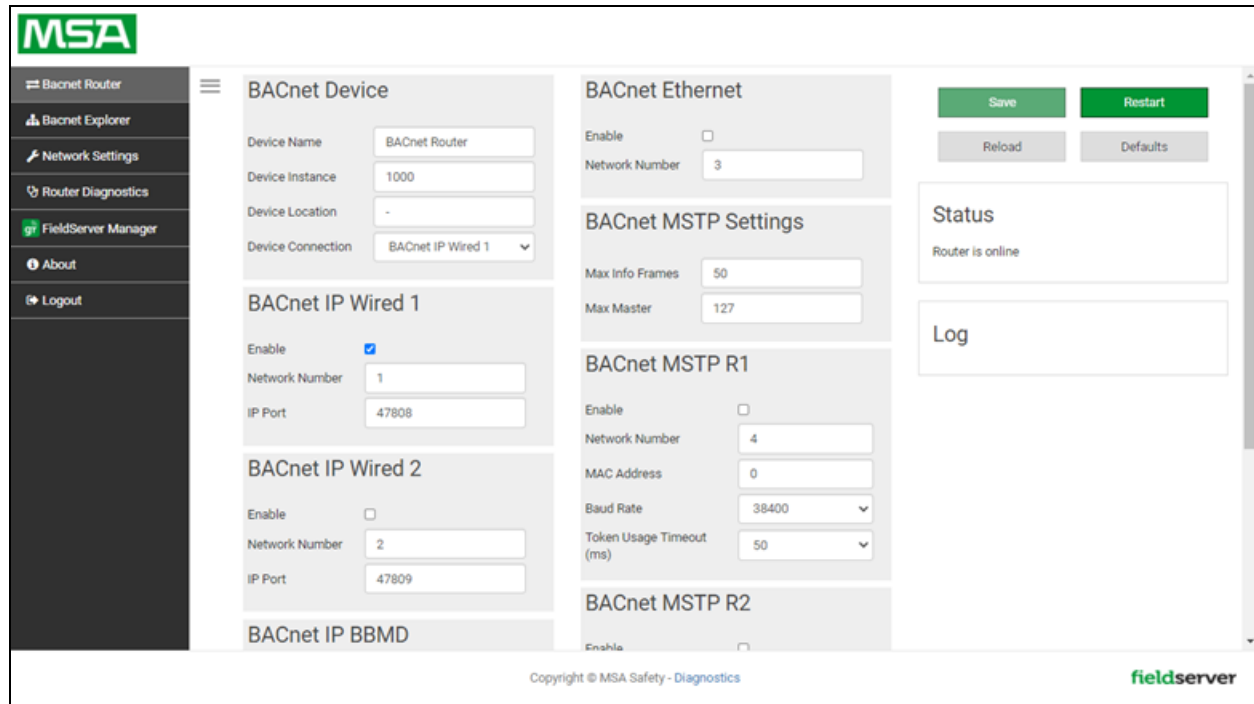
Routing Table is empty

Copyright © MSA Safety - Diagnostics 

9 BACnet Explorer

The embedded BACnet Explorer allows installers to validate that their equipment is working on BACnet without having to ask the BMS integrator to test the unit.

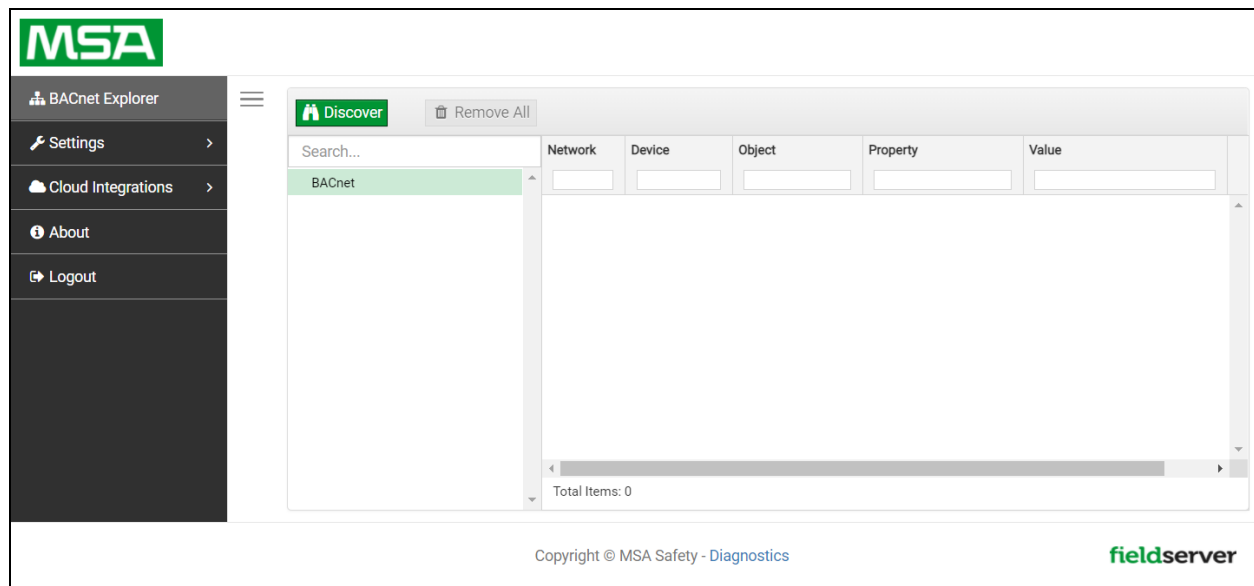
- To access the embedded BACnet Explorer, click the BACnet Explorer tab.




NOTE: For BACnet/IP, click on the Settings button on the left side of the landing page to ensure the BACnet Router is on the BACnet/IP network subnet to configure BBMD.


9.1 Discover the Device List

- From the BACnet Explorer landing page, click on the BACnet Explorer tab on the left side of the screen to go to the BACnet Explorer page.



- Find devices connected to the same subnet as the gateway by clicking the Discover button  (binocular icon).

- This opens the Discover window, click the checkboxes next to the desired settings and click Discover to start the search.

 Discover

Devices

Discover All Devices

From device to device


Networks

Discover All Networks

Discover Specific Network

NOTE: The “Discover All Devices” or “Discover All Networks” checkboxes must be unchecked to search for a specific device range or network.

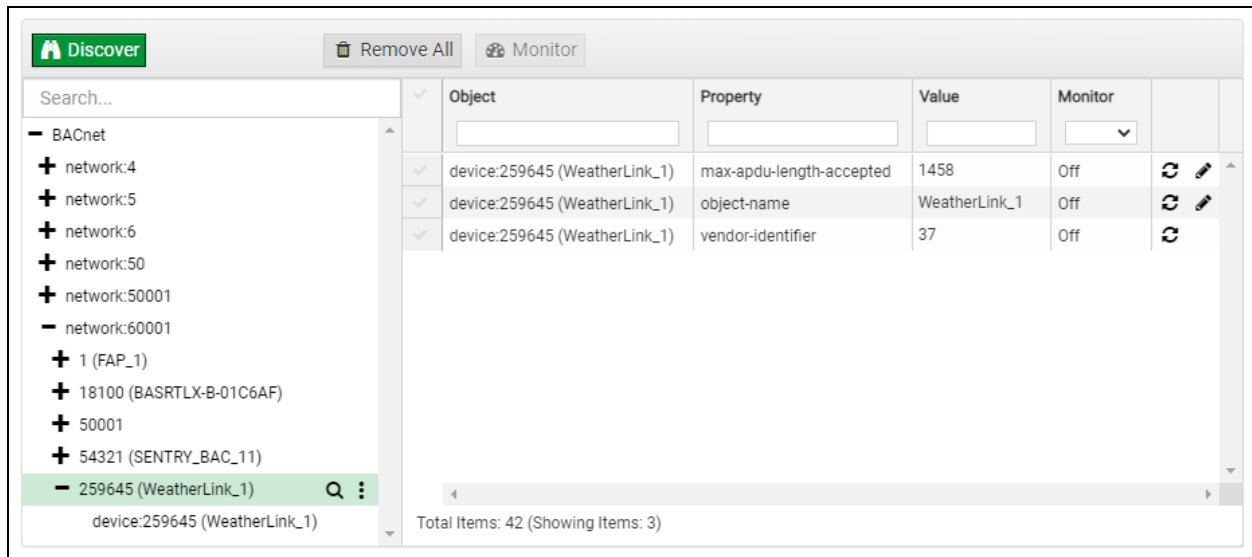
Allow the devices to populate before interacting with the device list for optimal performance. Any discovery or explore process will cause a green message to appear in the upper right corner of the browser to confirm that the action is complete.

 Discover

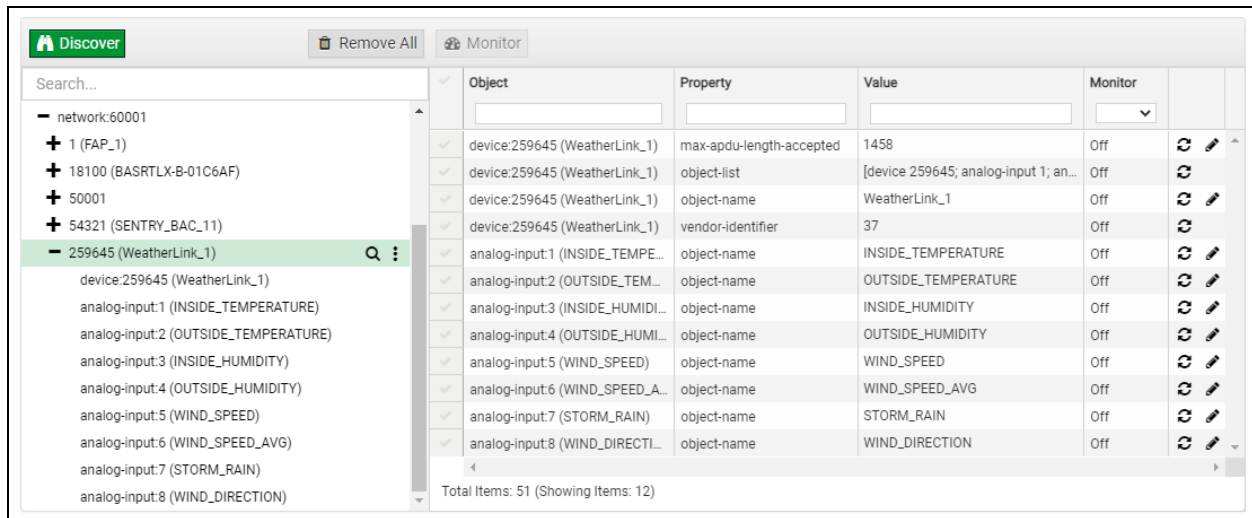
Search...	Device	Object	Property	Value	Monitor		
+ 1400	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Refresh"/>	<input type="button" value="Edit"/>
- network:6	1 (FAP_1)	device:1 (FAP_1)	max-apdu-length-accepted	1458	Off	<input type="button" value="Refresh"/>	<input type="button" value="Edit"/>
+ 101 (New_BACnet_Node)	1 (FAP_1)	device:1 (FAP_1)	object-name	FAP_1	Off	<input type="button" value="Refresh"/>	<input type="button" value="Edit"/>
- 102 (temp)	1 (FAP_1)	device:1 (FAP_1)	vendor-identifier	37	Off	<input type="button" value="Refresh"/>	<input type="button" value="Edit"/>
device:102 (temp)	18100 (BASRTLX-B-01C6AF)	device:18100 (BASRTLX-B-01C...	max-apdu-length-accepted	1476	Off	<input type="button" value="Refresh"/>	<input type="button" value="Edit"/>
- network:50	18100 (BASRTLX-B-01C6AF)	device:18100 (BASRTLX-B-01C...	object-name	BASRTLX-B-01C6AF	Off	<input type="button" value="Refresh"/>	<input type="button" value="Edit"/>
+ 50002	18100 (BASRTLX-B-01C6AF)	device:18100 (BASRTLX-B-01C...	vendor-identifier	245	Off	<input type="button" value="Refresh"/>	<input type="button" value="Edit"/>
+ 50022 (1020_22)	50001	device:50001	max-apdu-length-accepted	1458	Off	<input type="button" value="Refresh"/>	<input type="button" value="Edit"/>
+ 50033 (6020_33)	50001	device:50001	vendor-identifier	37	Off	<input type="button" value="Refresh"/>	<input type="button" value="Edit"/>
- network:50001	54321 (SENTRY_BAC_11)	device:54321 (SENTRY_BAC_11)	max-apdu-length-accepted	1458	Off	<input type="button" value="Refresh"/>	<input type="button" value="Edit"/>
+ 50000 (Dev_IP)	54321 (SENTRY_BAC_11)	device:54321 (SENTRY_BAC_11)	object-name	SENTRY_BAC_11	Off	<input type="button" value="Refresh"/>	<input type="button" value="Edit"/>
- network:60001	54321 (SENTRY_BAC_11)	device:54321 (SENTRY_BAC_11)	vendor-identifier	37	Off	<input type="button" value="Refresh"/>	<input type="button" value="Edit"/>
+ 1 (FAP_1)	259645 (WeatherLink_1)	device:259645 (WeatherLink_1)	max-apdu-length-accepted	1458	Off	<input type="button" value="Refresh"/>	<input type="button" value="Edit"/>
+ 18100 (BASRTLX-B-01C6AF)	259645 (WeatherLink_1)	device:259645 (WeatherLink_1)	object-name	WeatherLink_1	Off	<input type="button" value="Refresh"/>	<input type="button" value="Edit"/>
+ 50001	259645 (WeatherLink_1)	device:259645 (WeatherLink_1)	vendor-identifier	37	Off	<input type="button" value="Refresh"/>	<input type="button" value="Edit"/>
+ 54321 (SENTRY_BAC_11)							
+ 259645 (WeatherLink_1)							
Total Items: 42 (Showing Items: 14)							

9.2 View Device Details and Explore Points/Parameters

- To view the device details, click the blue plus sign (+) next to the desired device in the list.
 - This will show only some of the device properties for the selected aspect of a device

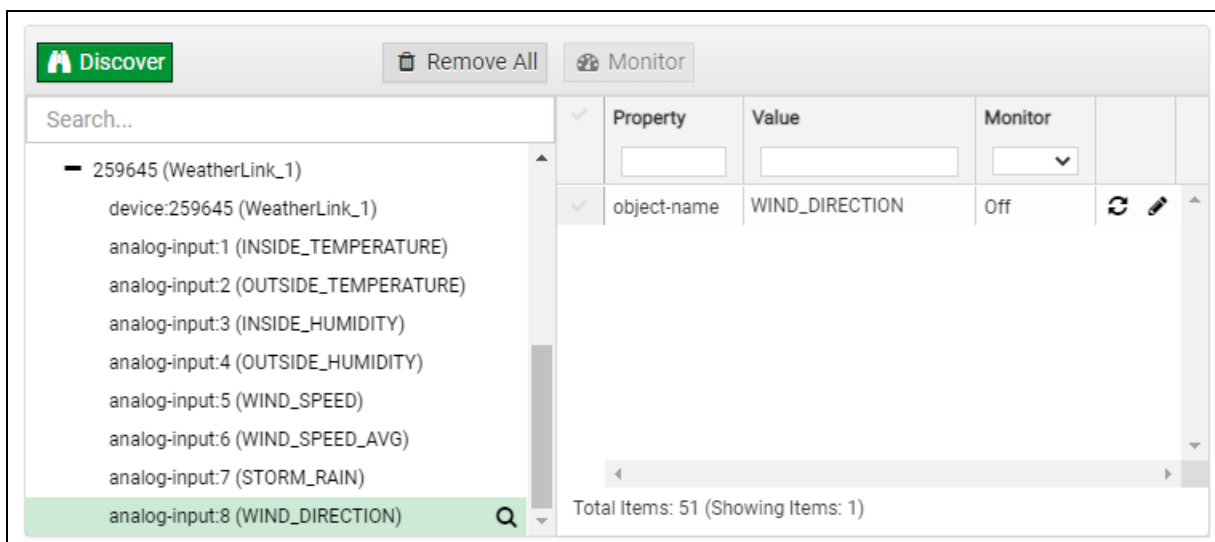


- To view the full details of a device, highlight the device directly (in the image below – “1991 WeatherLink_1”) and click the Explore button (🔍) that appears to the right of the highlighted device as a magnifying glass icon or double-click the highlighted device.

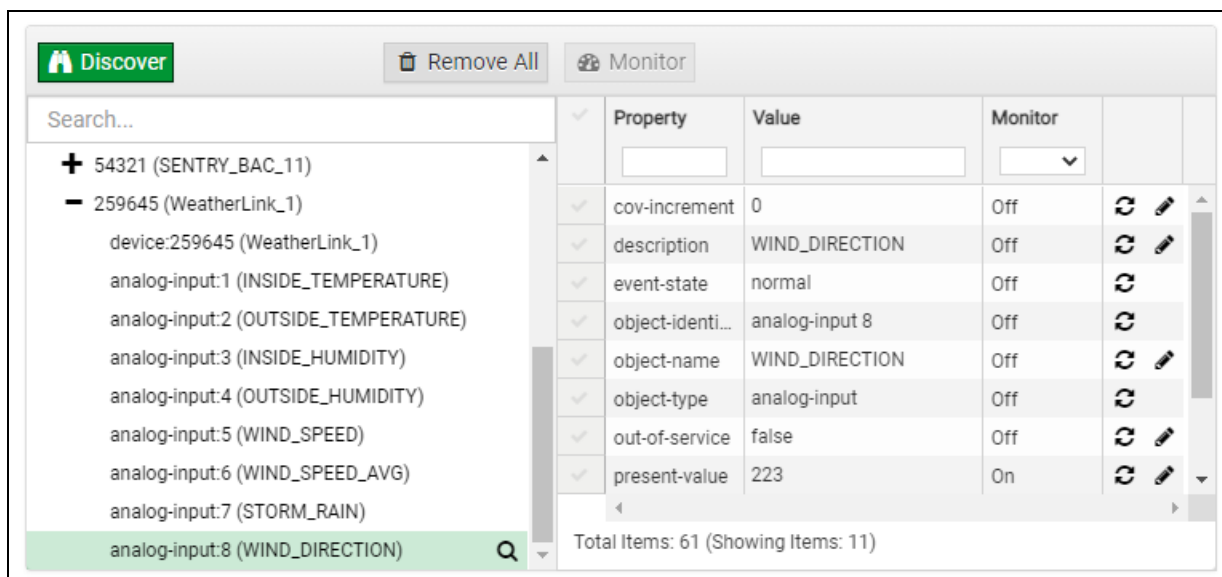


- Now additional device details are viewable; however, the device can be explored even further

- Click on one of the device details.



- Then click on the Explore button that appears or double-click the device object.



A full list of the device details will appear on the right side window. If changes are expected since the last explore, simply press the Refresh button (↻) that appears to right of individual properties to refresh.

NOTE: The Gateway Search Bar will find devices based on their Device ID.

NOTE: The Gateway Discovery Tree has 3 levels that correspond to the following.

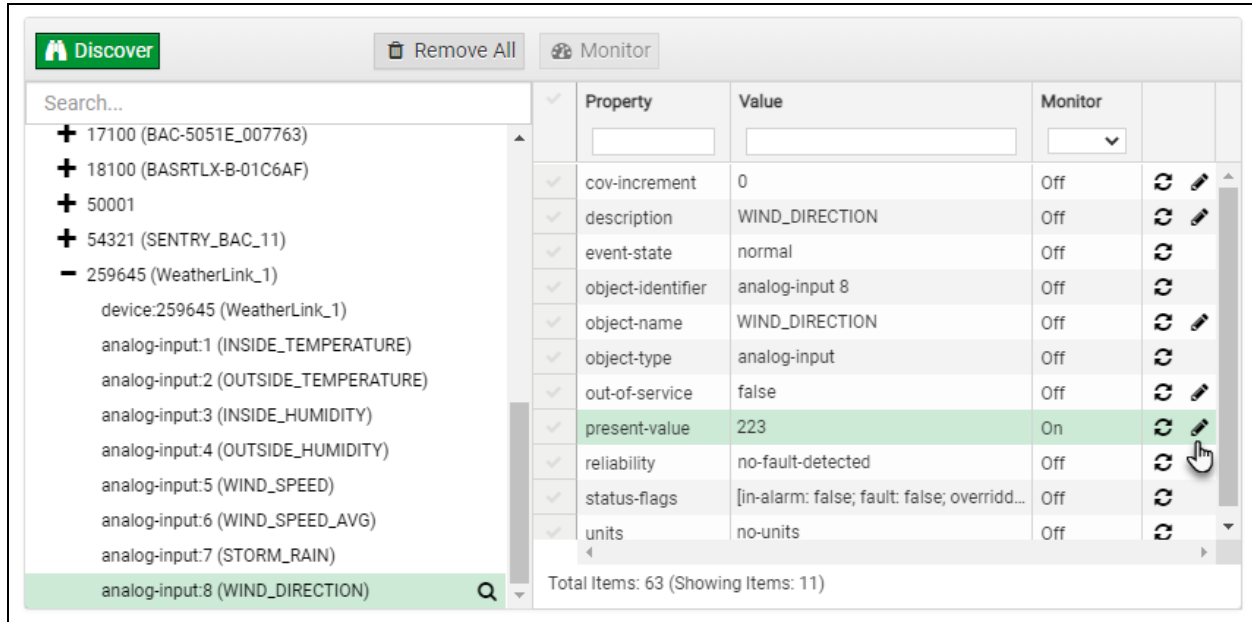
- Network number
 - Device
 - Device object

9.2.1 Edit the Present Value Field

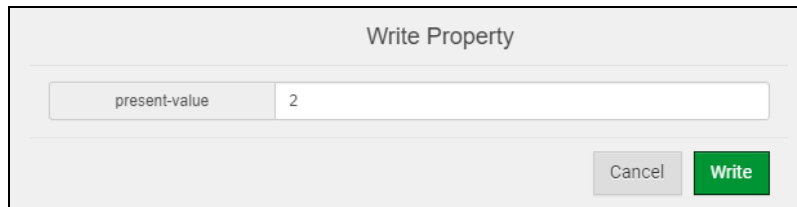
The only recommended field to edit is the device's present value field.

NOTE: Other BACnet properties are editable (such as object name, object description, etc.); however, this is not recommended because the gateway is not a Building Management System (BMS).

- To edit the present value, select it in the property listings.



- Then click the Write button (✎) on the right of the property to bring up the Write Property window.



- Enter the appropriate change and click the Write button.

The window will close. When the BACnet Explorer page appears, the present value will be changed as specified.

Property	Value	Monitor	
cov-increment	0	Off	🔄 ✎
description	WIND_DIRECTION	Off	🔄 ✎
event-state	normal	Off	🔄 ✎
object-identifier	analog-input 8	Off	🔄 ✎
object-name	WIND_DIRECTION	Off	🔄 ✎
object-type	analog-input	Off	🔄 ✎
out-of-service	false	Off	🔄 ✎
present-value	2	On	🔄 ✎
reliability	no-fault-detected	Off	🔄 ✎

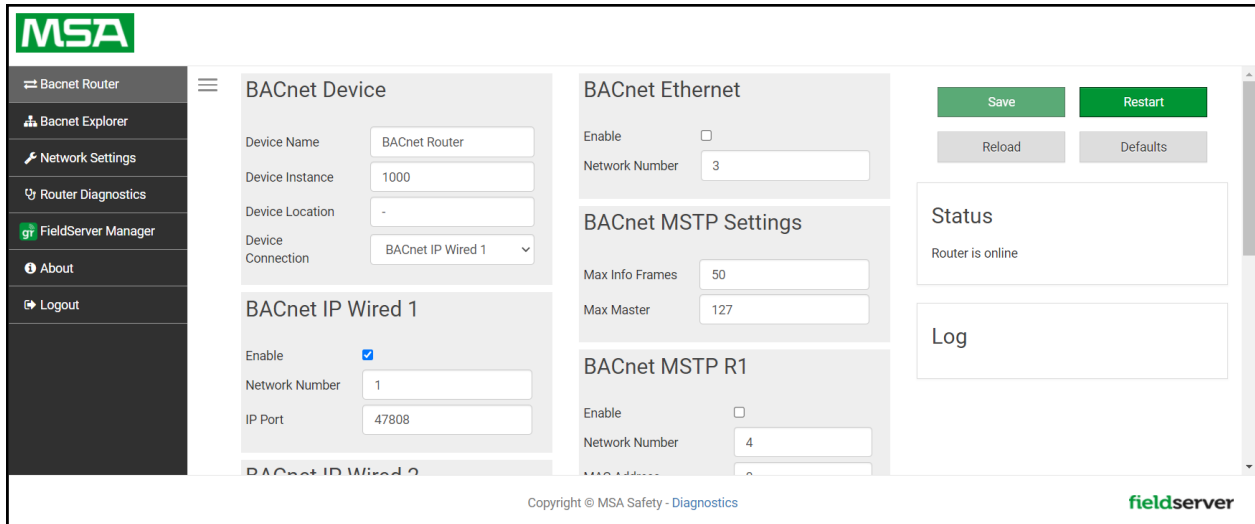
10 MSA Grid - FieldServer Manager Setup

The MSA Grid is MSA Safety's device cloud solution for IIoT. Integration with the MSA Grid - FieldServer Manager enables the a secure remote connection to field devices through a FieldServer and hosts local applications for device configuration, management, as well as maintenance. For more information about the FieldServer Manager, refer to the [MSA Grid - FieldServer Manager Start-up Guide](#).

10.1 Create a New FieldServer Manager Account

The first step to connecting to the FieldServer Manager is to create an account.

- Click on the FieldServer Manager tab.



- An informational splash page will appear, click the Close button to view the registration page.

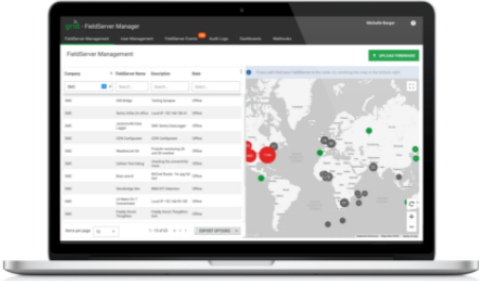
Grid FieldServer Manager Registration

Securely access your FieldServer from anywhere with the [Grid FieldServer Manager](#)

Your one stop for managing your FieldServers and users

- ✓ **Secure Remote Access**
Securely connect your field devices to Grid FieldServer Manager.
- ✓ **FieldServer Management**
Manage all your FieldServers and connected devices from Grid FieldServer Manager and upgrade firmware remotely.
- ✓ **User Management**
Set up your user personnel with the right security permissions and FieldServer assignments for users to diagnose, configure, and better support the field installation.

For more information about Grid FieldServer Manager, visit [our website](#).



[Get Started](#)

- If a warning message appears instead of the splash page, follow the suggestion that appears on screen.
- If the BACnet Router cannot reach the FieldServer Manager server, the following message will appear.

Grid FieldServer Manager Registration

Grid FieldServer Manager™ Server Unreachable

The device is unable to connect to the Grid FieldServer Manager server.

The following network issues have been detected. Correcting them might resolve connectivity to the server:

- Could not ping Gateway [192.168.2.1]
- Could not ping Domain Name Server 1 [8.8.8.8]
- Could not ping Domain Name Server 2 [8.8.4.4]

Ensure your network firewall is configured to allow this device to access the Grid FieldServer Manager server:

- Error Code: **EAI_AGAIN**
- FieldServer MAC address: **00:50:4E:60:6C:E8**
- Allow HTTPS communications to the following domains on **port 443**:
 - **www.fieldpop.io**
 - **ts.fieldpop.io**

- Follow the directions presented in the warning message and check that the DNS settings are set up with the following Domain Name Server (DNS) settings:
DNS1=8.8.8.8
DNS2=8.8.4.4
- Ensure that the BACnet Router is properly connected to the Internet

NOTE: If changes to the network settings are done, remember to save and then power cycle the BACnet Router to update the settings.

- Fill in the user details, site details, gateway details and create a new account.
 - Enter user details and click Next

The screenshot shows the 'Installer Details' step, which is the first of four steps in the registration process. The steps are: 1. Installer Details, 2. Installation Site, 3. FieldServer Details, and 4. Account Details. The 'Installer Details' section includes the following fields:

- Installer Name:
- Company:
- Telephone:
- Email:
- Installation Date:

At the bottom right, there are two buttons: 'Cancel' and 'Next'.

- Enter the site details by entering the physical address fields or the latitude and longitude then click Next

The screenshot shows the 'Installation Site Details' step, which is the second of four steps in the registration process. The steps are: 1. Installer Details, 2. Installation Site, 3. FieldServer Details, and 4. Account Details. The 'Installation Site Details' section includes the following fields:

- Search:
- Site Name:
- Building:
- Street Address:
- Suburb:
- City:
- State:
- Country:
- Postal Code:
- Latitude:
- Longitude:

On the right side of the form, there is a Google Maps interface with 'Map' and 'Satellite' tabs. The map shows a location in the Lafayette area. At the bottom right, there are three buttons: 'Cancel', 'Previous', and 'Next'.

- Enter Name and Description (required) then click Next

The screenshot shows the 'Grid FieldServer Manager Registration' wizard at step 3, 'FieldServer Details'. The progress bar at the top indicates four steps: 1. Installer Details, 2. Installation Site, 3. FieldServer Details (highlighted in green), and 4. Account Details. The main content area is titled 'FieldServer Details' and contains the following fields:

- Name:** A red rectangular input field.
- Description:** A red rectangular input field.
- FieldServer Info:** A text area with the placeholder text: 'Optionally specify any other information relating to the FieldServer i.e., calibration, commissioning or other notes'.
- Timezone:** A dropdown menu currently set to '(GMT -08:00) America/Los_Angeles'.

At the bottom right, there are three buttons: 'Cancel' (disabled), 'Previous' (disabled), and 'Next' (active).

- Click the "Create an Grid FieldServer Manager account" button and enter a valid email to send a "Welcome to FieldServer Manager" invite to the email address entered

The screenshot shows the 'Grid FieldServer Manager Registration' wizard at step 4, 'Account Details'. The progress bar at the top indicates four steps: 1. Installer Details, 2. Installation Site, 3. FieldServer Details, and 4. Account Details (highlighted in green). The main content area is titled 'New Users' and contains the following elements:

- A text prompt: 'If you do not have Grid FieldServer Manager credentials, you can create a new Grid FieldServer Manager account now'.
- A green button labeled 'Create an Grid FieldServer Manager account'.
- A section titled 'Existing Users - Enter FieldServer registration details'.
- A sub-section titled 'User Credentials' with two red rectangular input fields: 'Username' and 'Password'.

At the bottom right, there are three buttons: 'Cancel' (disabled), 'Previous' (disabled), and 'Register FieldServer' (active).

- Once the device is registered, a confirmation window will appear. Click the Close button and the following screen will appear listing the device details and additional information auto-populated by the BACnet Router.

Grid FieldServer Manager Registration


FieldServer Registered

FieldServer Details	Installer Details	Installation Site Details
<p>Name: Test1</p> <p>Description: FS Test</p> <p>FieldServer Info:</p> <p>Timezone: America/Los_Angeles</p> <p>MAC Address: 00:50:4E:60:13:FE</p> <p>Tunnel Server URL: tunnel.fieldpop.io</p> <p>FieldServer ID: treedancer_KrgPKmLRY</p> <p>Product Name: Core Application - Default</p> <p>Product Version: 5.2.0</p>	<p>Installer Name: Test</p> <p>Company: MSA Safety</p> <p>Telephone: (408) 444-4444</p> <p>Email: contactus@msasafety.com</p> <p>Installation Date: Sep 20, 2021</p>	<p>Site Name: Site#1</p> <p>Building:</p> <p>Street Address: 1020 Canal Road</p> <p>Suburb:</p> <p>City: Lafayette</p> <p>State: Indiana</p> <p>Country: United States</p> <p>Postal Code: 47904</p>

Update FieldServer Details

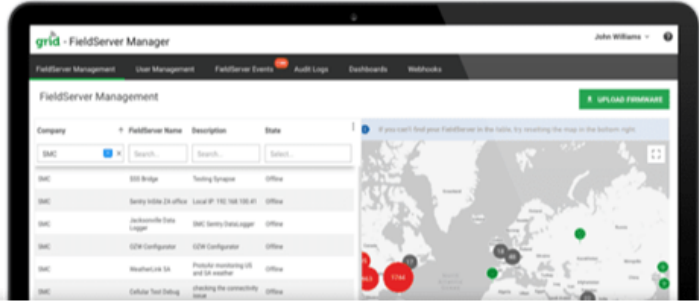
NOTE: Update these details at any time by going to the FieldServer Manager tab and clicking the Update FieldServer Details button.

- Open the registered email account.
- The “Welcome to FieldServer Manager” email will appear as shown below.



Fieldserver Manager

Welcome to FieldServer Manager



Your one stop for managing your FieldServers and users

- ✓ Secure Remote Access
- ✓ FieldServer Management
- ✓ User Management

COMPLETE REGISTRATION


Contact Us

+1 408 262-6611

smc-support@msasafety.com

www.msasafety.com

© copyright 2021 MSA . All rights reserved.



NOTE: If no email was received, check the spam/junk folder for an email from notification@fieldpop.io. Contact the FieldServer support team if the email cannot be found.

- Click the “Complete Registration” button and fill in user details accordingly.

Complete Your Registration

Email Address
user@gmail.com

First Name
First Name *

Last Name
Last Name *

Mobile Phone Number
🇺🇸 (201) 555-0123 *

New Password *Invalid Mobile Number
password *

Confirm Password * Please enter new password
password *

By registering my account with MSA, I understand that I am agreeing to the FieldServer Manager [Terms of Service and Privacy Policy](#) *

* Mandatory Fields

- Fill in the name, phone number, password fields and click the checkbox to agree to the privacy policy and terms of service.

NOTE: If access to data logs using RESTful API is needed, do not include “#” in the password.

- Click “Save” to save the user details.
- Click “OK” when the Success message appears.
- Record the email account used and password for future use.

10.2 Login to the FieldServer Manager

After the gateway is registered, go to www.smccloud.net and type in the appropriate login information as per registration credentials.

NOTE: If the login password is lost, see the [MSA Grid - FieldServer Manager Start-up Guide](#) for recovery instructions.

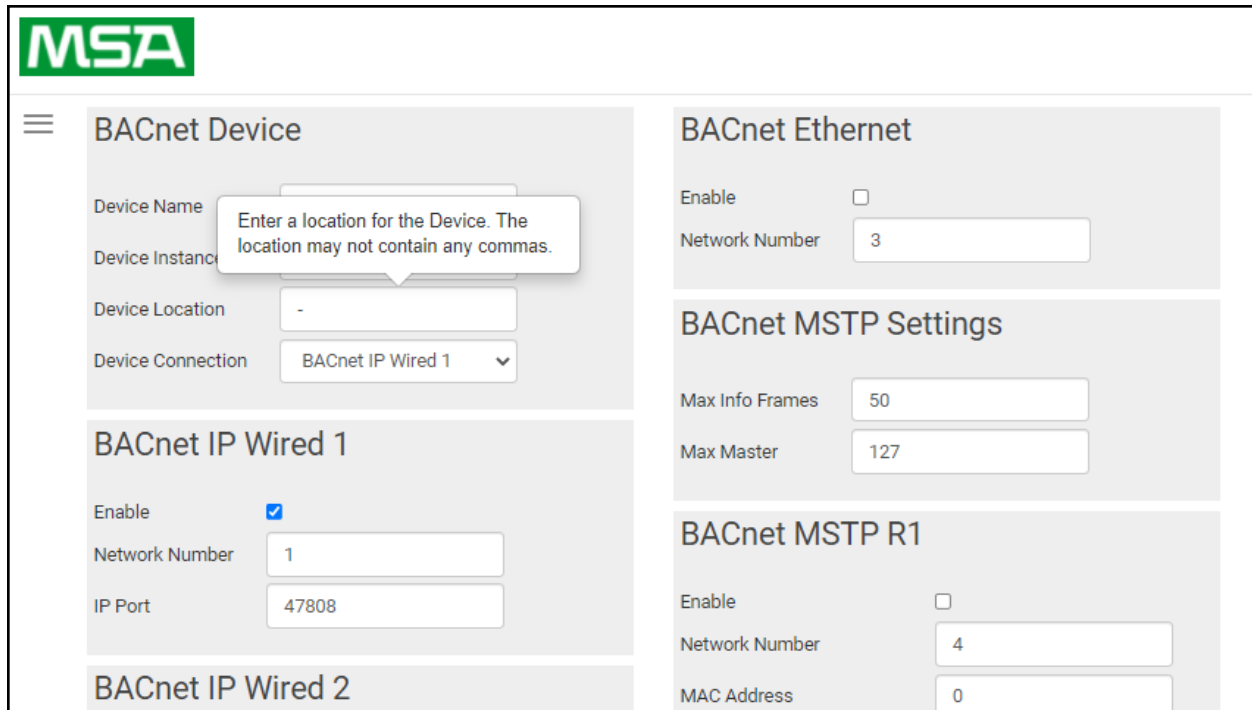
Company	FieldServer Name	Description	State
Eggers OEM	Jens's Brain 31	192.168.1.31	Offline
Eggers OEM	Jens MBP Core App	~/git/smc-core-application	Offline
Eggers OEM	Jens's Dell Profile View	~/git/profile-view	Offline
Eggers OEM	hd_test_log_to_fpop	testing_modbus	Offline
Eggers OEM	Mbus demo	testing registration	Offline
SMC	TestWall-PA2port 97	Testwall pa 2 97	Offline
SMC	TestWall-Lon152	Testwall unit	Offline

NOTE: For additional FieldServer Manager instructions see the [MSA Grid - FieldServer Manager Start-up Guide](#).

11 Troubleshooting


11.1 Tooltips

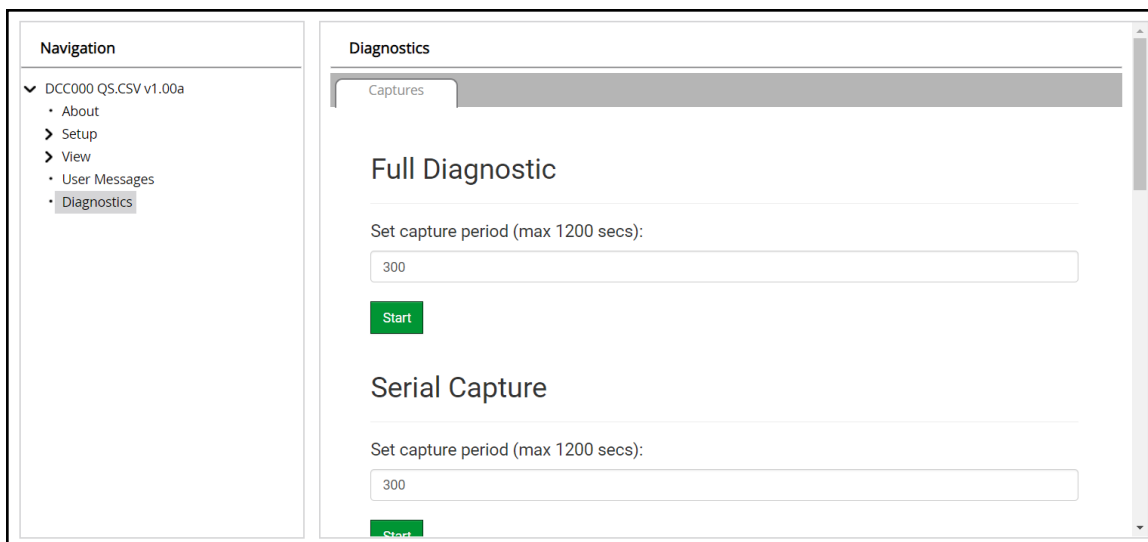
Tooltips appear when the mouse pointer hovers over the corresponding settings field. A balloon will appear giving a description of that input field. This applies to all input fields.



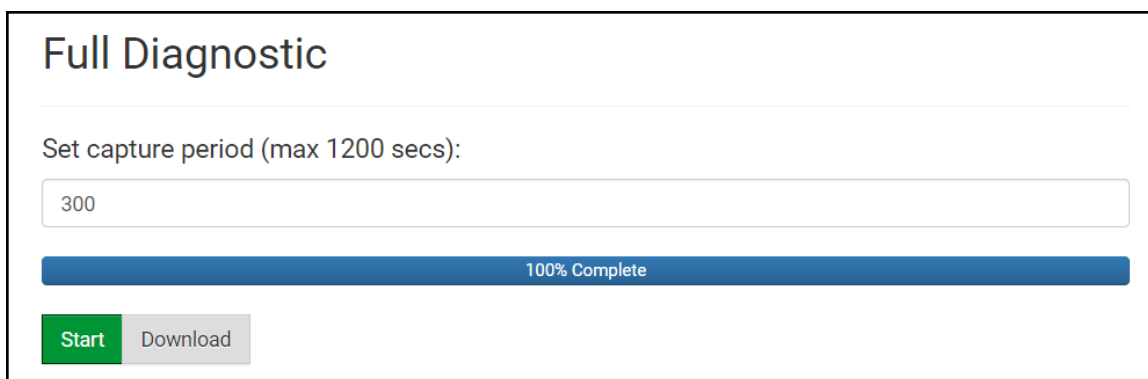
11.2 Taking a FieldServer Diagnostic Capture

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.

11.3 Factory Reset Instructions

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

11.4 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.

11.5 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.

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 from the BACnet Router landing page to the FS-GUI by clicking the blue “Diagnostics” text on the bottom of the screen.

The screenshot displays the BACnet Router configuration page. The left sidebar contains navigation options: BACnet Router, BACnet Explorer, Network Settings, Router Diagnostics, FieldServer Manager, About, and Logout. The main content area is divided into several sections:

- BACnet Device:** Fields for Device Name (BACnet Router), Device Instance (1000), Device Location (-), and Device Connection (BACnet IP Wired 1).
- BACnet Ethernet:** Enable checkbox, Network Number (3).
- BACnet MSTP Settings:** Max Info Frames (50), Max Master (127).
- BACnet IP Wired 1:** Enable checkbox, Network Number (1), IP Port (47808).
- BACnet IP Wired 2:** Enable checkbox, Network Number (2), IP Port (47809).
- BACnet IP BBMD:** Enable checkbox.
- BACnet MSTP R1:** Enable checkbox, Network Number (4), MAC Address (0), Baud Rate (38400), Token Usage Timeout (ms) (50).
- BACnet MSTP R2:** Enable checkbox.

On the right side, there are control buttons: Save, Restart, Reload, and Defaults. Below these is a Status section showing "Router is online" and a Log section.

At the bottom of the interface, it says "Copyright © MSA Safety - Diagnostics" and "fieldserver".

- Click Setup in the Navigation panel.

The screenshot shows the FieldServer Manager interface. The top right corner has the "FieldServer Manager" logo. The left sidebar contains a "Navigation" panel with the following items:

- ✓ DCC000 QS.CSV v1.00a
 - About
 - Setup
 - View
 - User Messages
 - Diagnostics

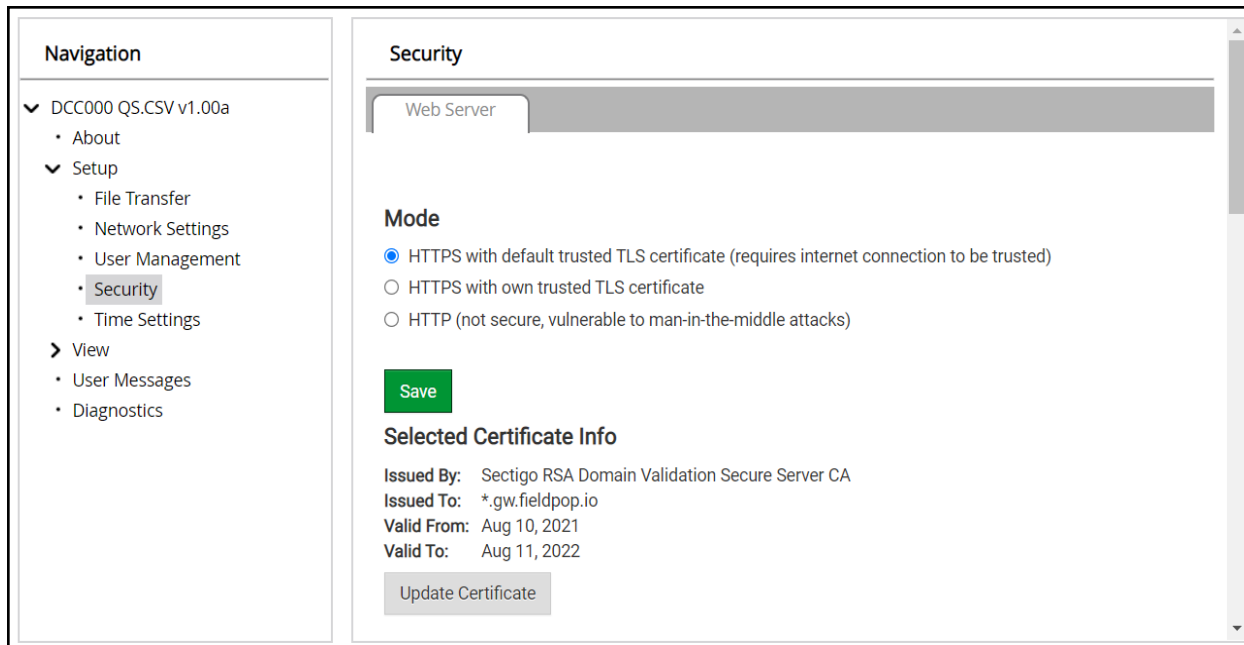
The main content area is titled "DCC000 QS.CSV v1.00a" and has tabs for "Status", "Settings", and "Info Stats". The "Status" tab is active, showing a table with the following data:

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

At the bottom of the interface, there are buttons for "Home", "HELP (?)", "Contact Us", "System Restart", "System Reboot", "System Time Synchron", "Reset Cycle Times", and "Logout". The "fieldserver" logo is also present in the bottom right corner.

12.1.1 Change Security Mode

- Click Security in the Navigation panel.

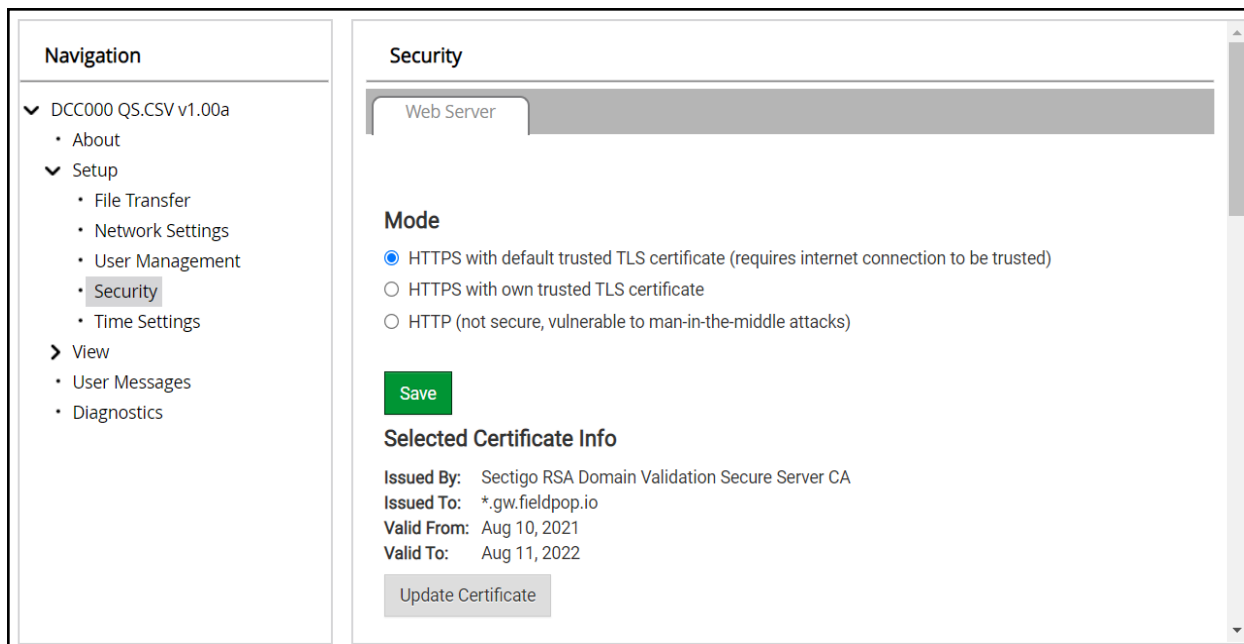


- Click the Mode desired.
 - If HTTPS with own trusted TLS certificate is selected, follow instructions in [Section 6.2.1 HTTPS with Own Trusted TLS Certificate](#)
- Click the Save button.

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.



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

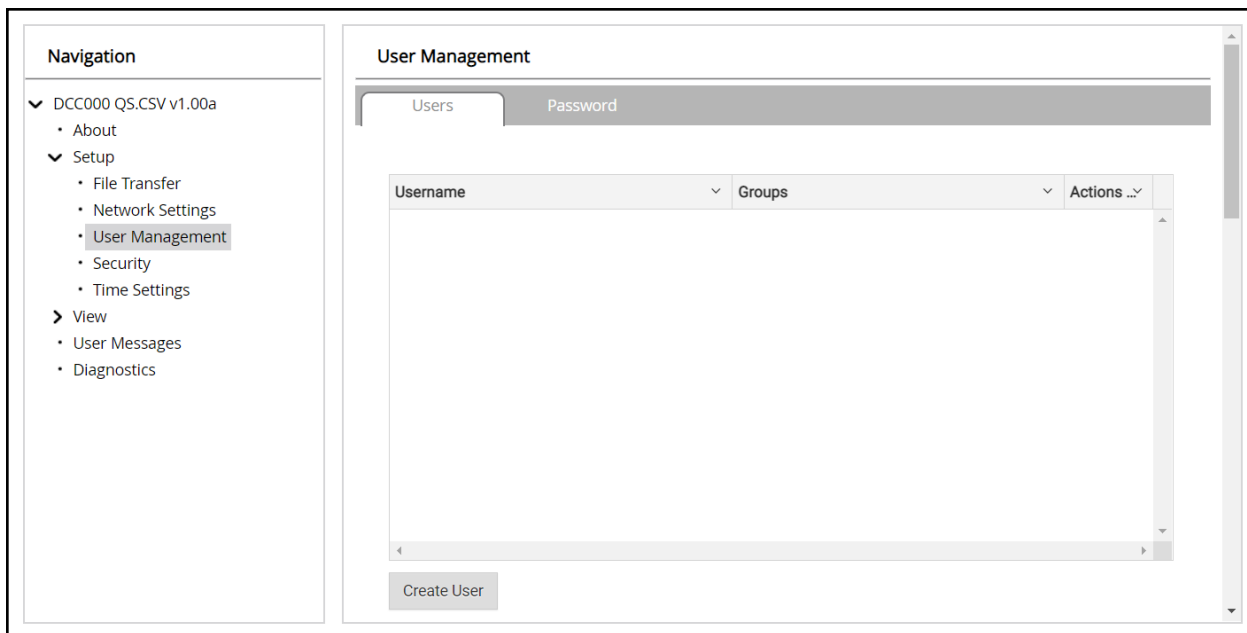
12.2 Change User Management Settings

- 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 . 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:

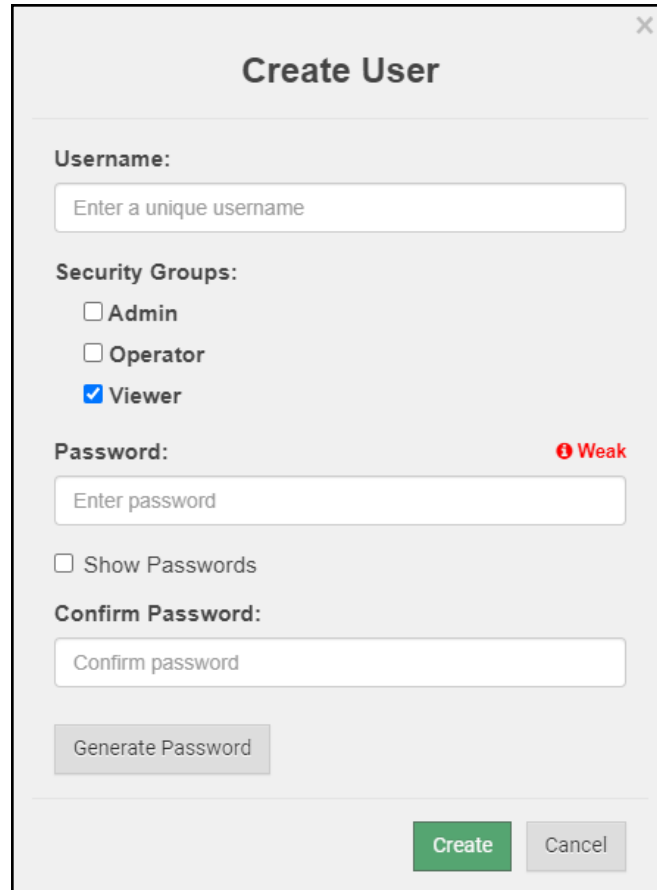
Admin – Can modify and view any settings on the FieldServer.

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

Generate Password

Create Cancel

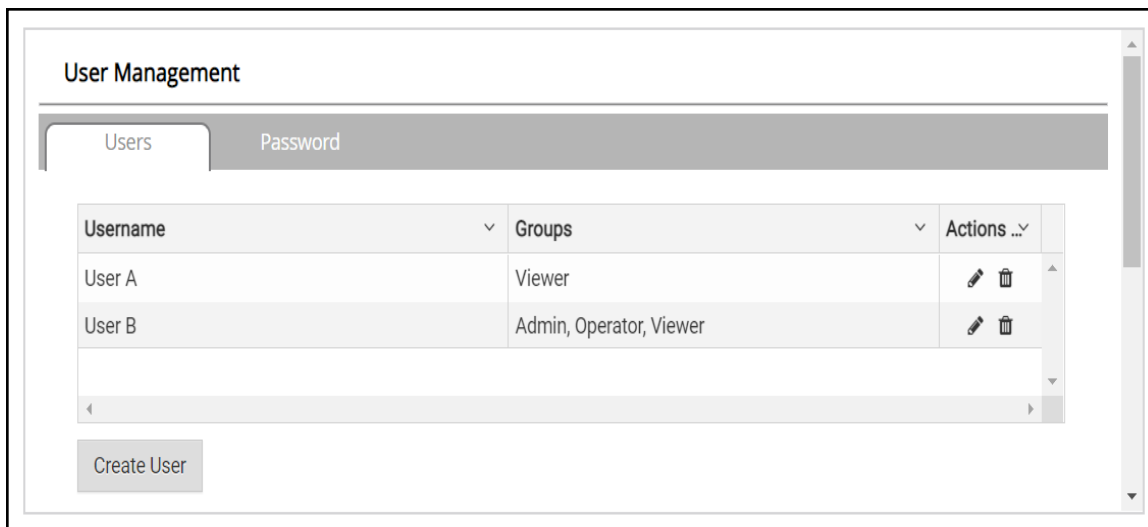
- Enter the new User fields: Name, Security Group and Password.
 - **User details are hashed and salted**

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.

12.2.2 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.

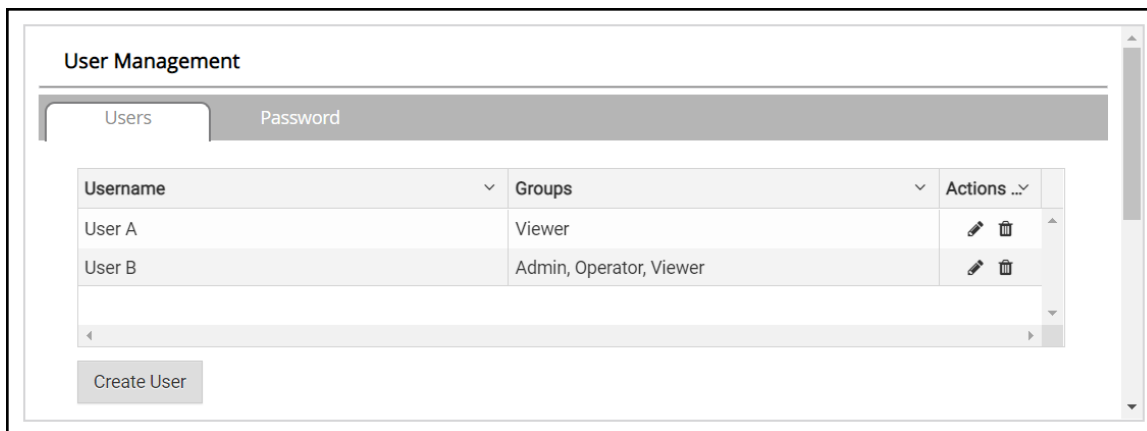
The 'Edit User' dialog box contains the following fields and options:

- Username:** Text field containing 'User A'.
- Security Groups:**
 - Admin
 - Operator
 - Viewer
- Password:** Text field containing 'Optional'.
- Show passwords
- Confirm Password:** Text field containing 'Optional'.
-
- (green)
-

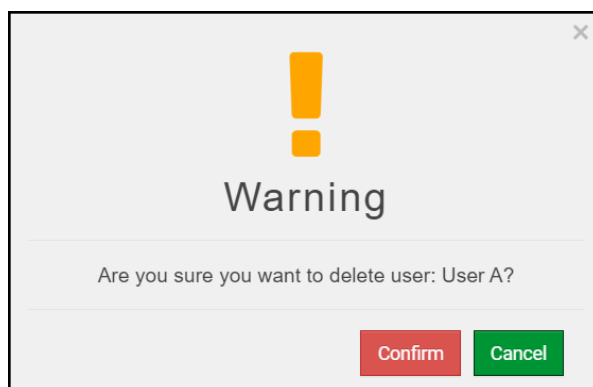
- Click Confirm.
- Once the Success message appears, click OK.

12.2.3 Delete Users

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

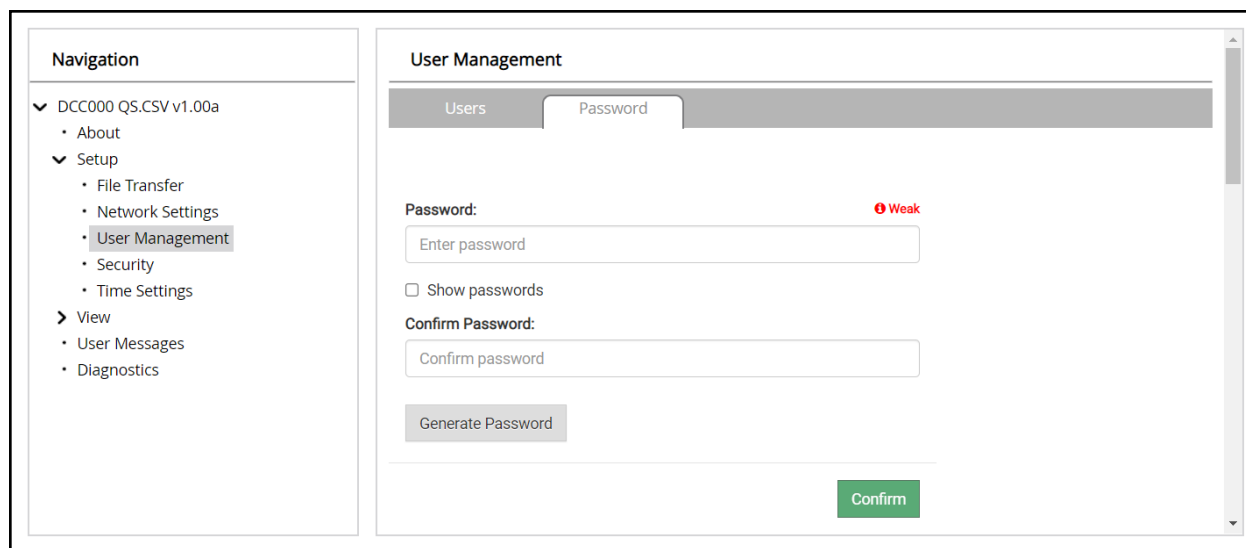


- When the warning message appears, click Confirm.



12.2.4 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.

12.3 Specifications



FS-ROUTER-BACW	
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>Current draw:</i> 24VAC 0.125A <i>Max Power:</i> 3 Watts 12-24VDC 0.25A @12VDC
Approvals	FCC Part 15, UL 60950-1, EN IEC 62368-1, WEEE compliant, RoHS compliant, DNP 3.0 and Modbus conformance tested, BTL marked, REACH compliant, UKCA and CE compliant, 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>Channels:</i> 1 to 11 (inclusive) <i>Antenna:</i> Omnidirectional SMA <i>Encryption:</i> TKIP, WPA2 & AES

NOTE: Specifications subject to change without notice.

12.4 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 BACnet Router.

BACnet Router 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.

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.