

Operating Manual

BACnet Router Start-up Guide

FS-Router-BAC2

Revision: 3.I

Document No.: T18625

Print Spec: 10000005389 (EO)

*MSA**safety**.com*

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

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

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

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

© MSA 2024. All rights reserved

Contents

1 BACnet Router Description 5

2 Equipment Setup 5
2.1 Mounting 5
2.2 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 Routing Settings 17
7.2 Ethernet 1 18

8 Configuring the BACnet Router 19
8.1 Navigate to the BACnet Router Settings 19
8.2 BACnet Router Settings 20
8.2.1 Button Functions 20
8.2.2 Multiple Connections 21
8.2.3 BACnet Device 21
8.2.4 BACnet/IP 21
8.2.5 BACnet MS/TP, BACnet Ethernet and BACnet Explorer 22
8.3 Router Diagnostics 23

9 BACnet Explorer 24
9.1 Discover the Device List 24
9.2 View Device Details and Explore Points/Parameters 26
9.2.1 Edit the Present Value Field 28

10 MSA Grid - FieldSever Manager Setup 29
10.1 Create a New FieldServer Manager Account 29
10.2 Login to the FieldServer Manager 35

11 Troubleshooting 36
11.1 Tooltips 36
11.2 Factory Reset Instructions 36
11.3 Internet Browser Software Support 36
11.4 Taking a FieldServer Diagnostic Capture 37

12 Additional Information 38

12.1 Change Web Server Security Settings After Initial Setup 38
12.1.1 Change Security Mode 39
12.1.2 Edit the Certificate Loaded onto the FieldServer 39
12.2 Change User Management Settings 40
12.2.1 Create Users 41
12.2.2 Edit Users 42
12.2.3 Delete Users 43
12.2.4 Change FieldServer Password 43
12.3 Specifications 44
12.4 Warnings 44
12.5 Compliance with EN IEC 62368-1 44

13 Limited 2 Year Warranty 45

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

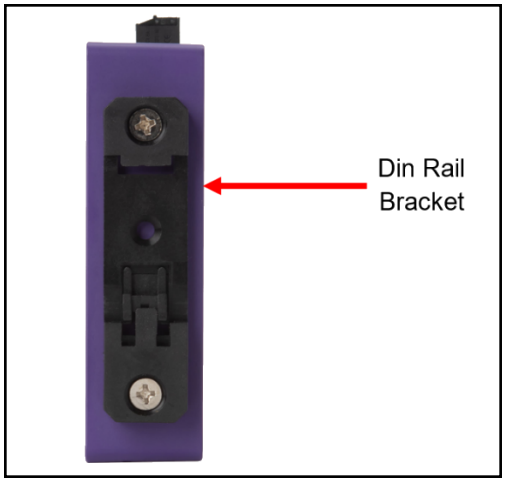
NOTE: For MSA Grid – FieldServer Manager information, refer to the MSA Grid - FieldServer Manager Start-up Guide online through the MSA website.

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

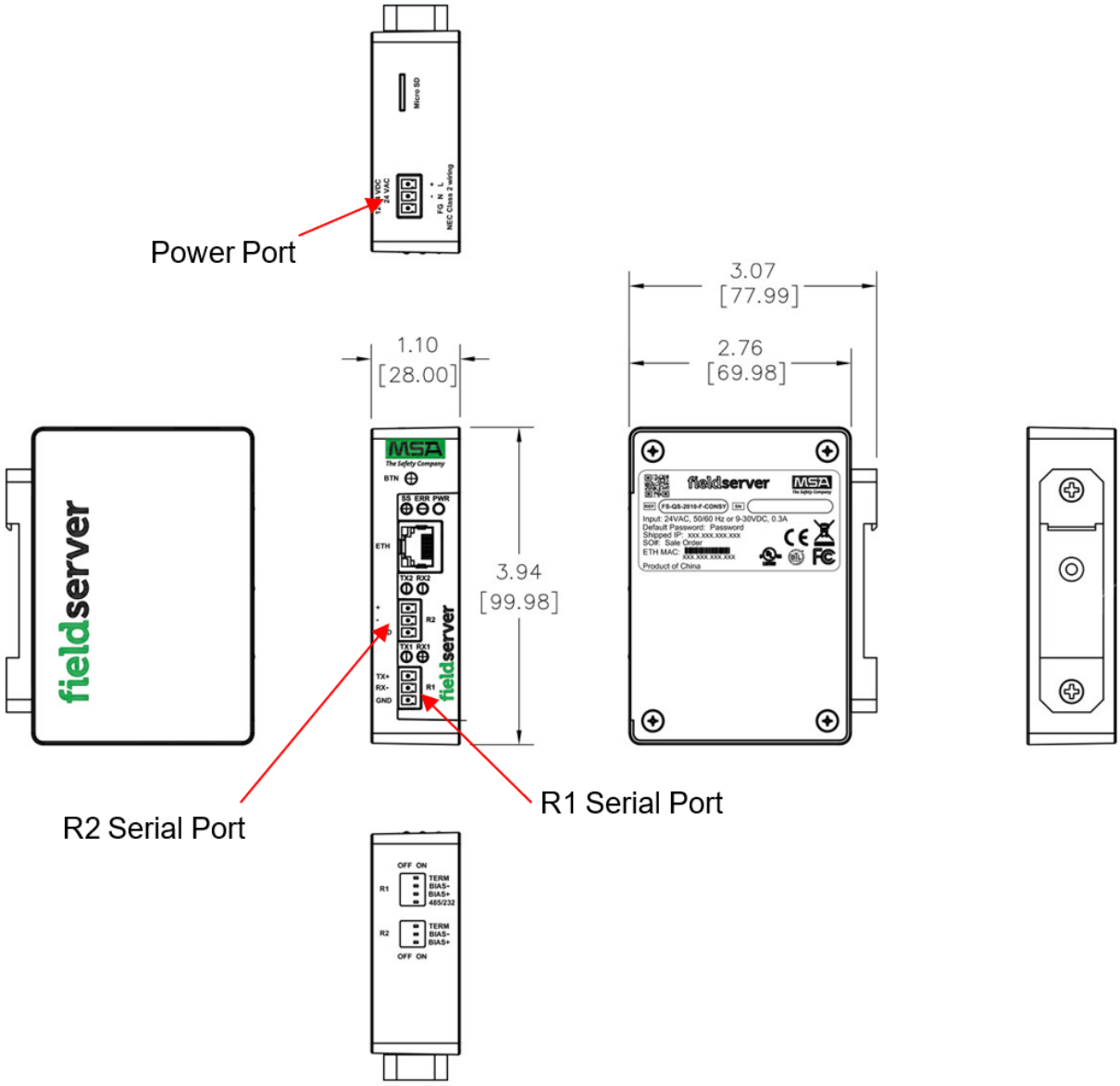
2 Equipment Setup

2.1 Mounting

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



2.2 Physical Dimensions



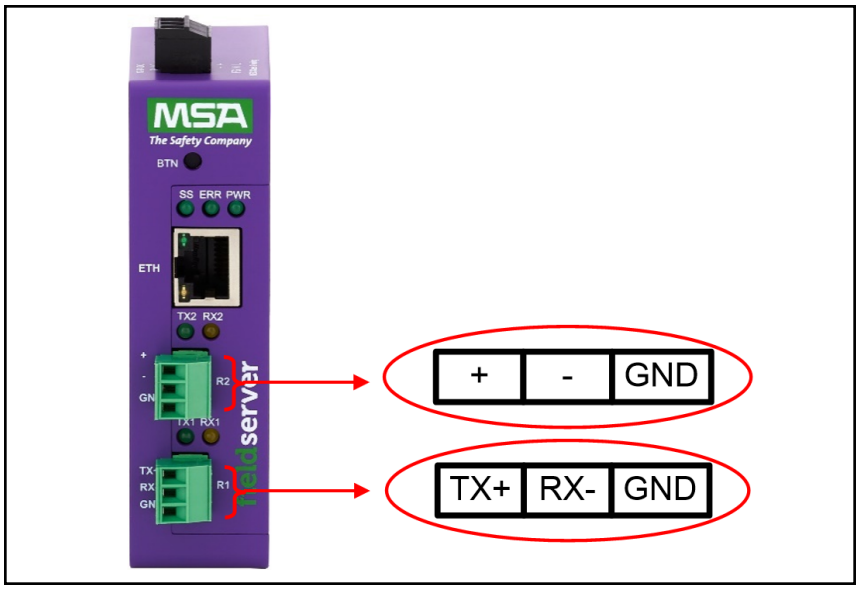
3 Installation

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

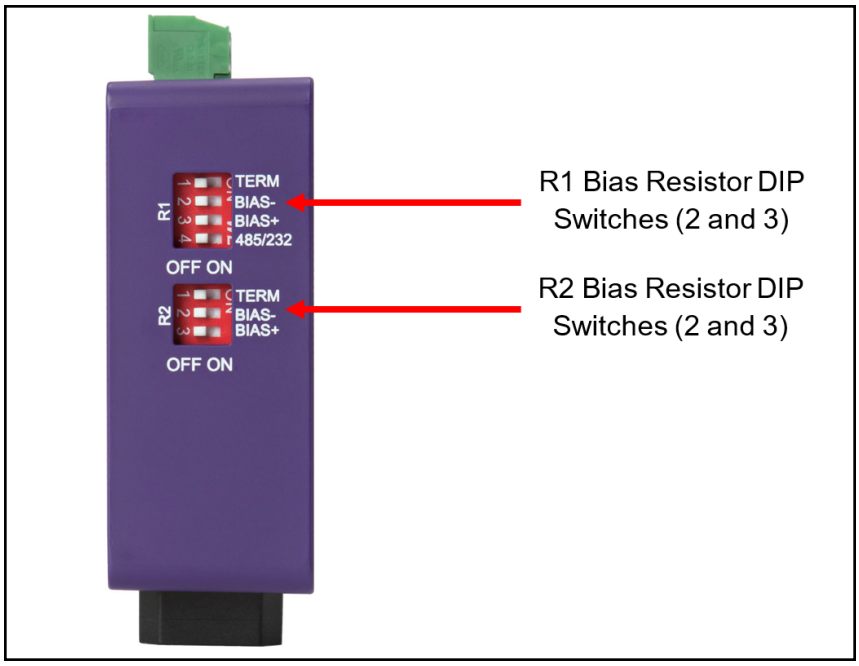
3.1.1 Wiring

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 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.

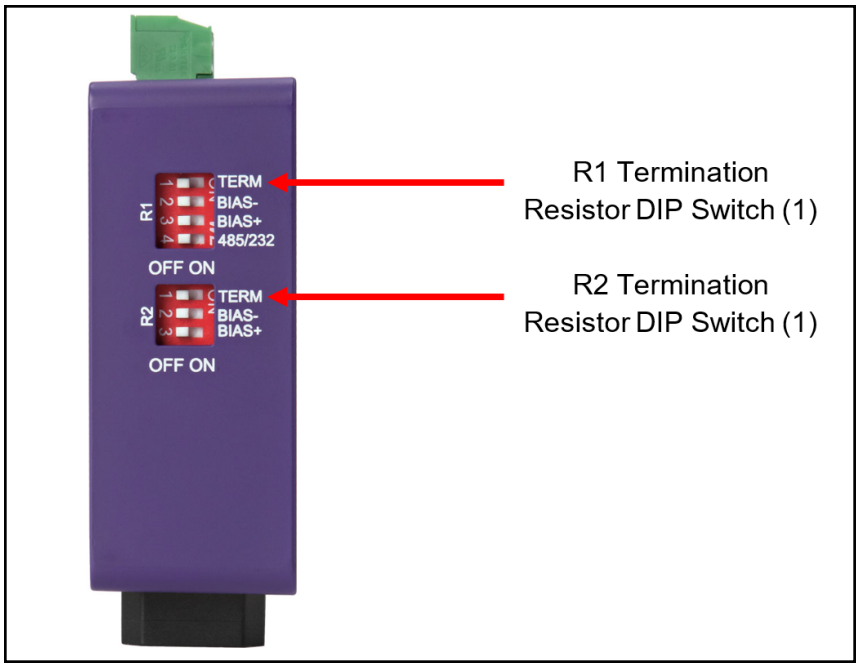
The bias resistor is 510 ohms which is in line with the BACnet spec. It should only be enabled at one point on the bus (for example, on the field port were there are very weak bias resistors of 100k). Since there are no jumpers, many BACnet Routers can be put on the network without running into the bias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

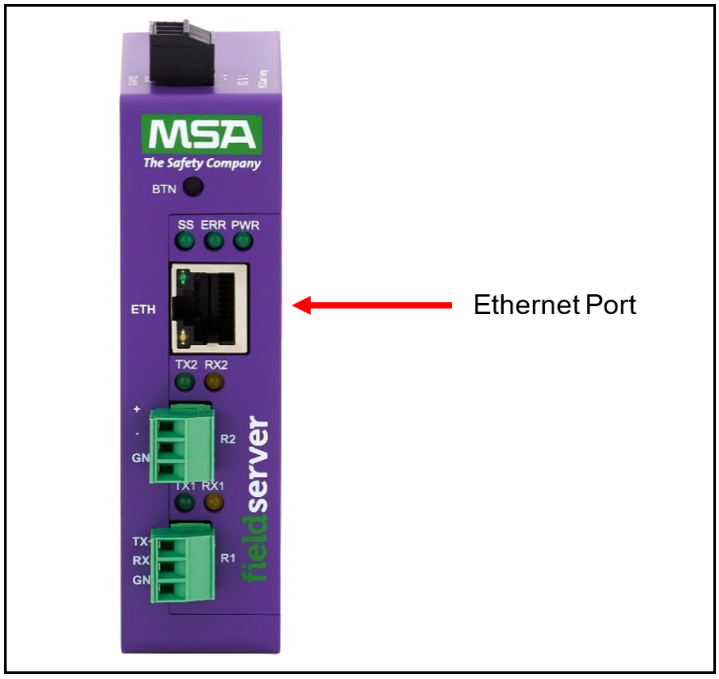
The termination resistor is also used to reduce noise. It pulls the two lines of an idle bus together. However, the resistor would override the effect of any bias resistors if connected. The R1 termination resistor is 120 Ohms.

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

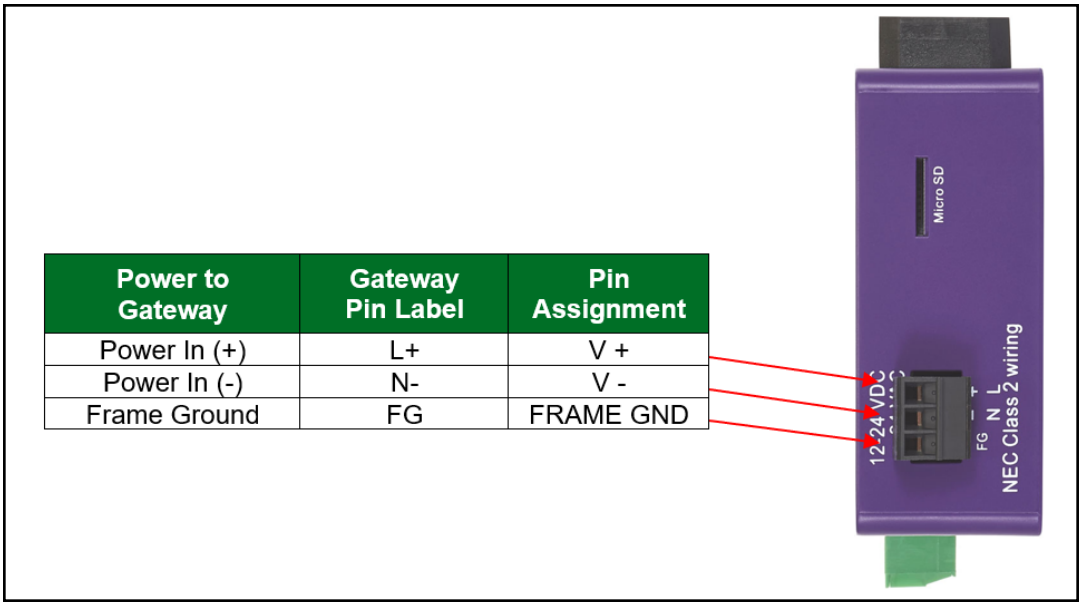
Check power requirements in the table below:

Power Requirement for BACnet Router External Gateway		
	Current Draw Type	
BACnet Router Family	12VDC	24VDC/AC
FS-EXPLORER-BAC2 (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-.
  - Supports both Full-Wave and Half-Wave AC
- 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.



Power to Gateway	Gateway Pin Label	Pin Assignment
Power In (+)	L+	V +
Power In (-)	N-	V -
Frame Ground	FG	FRAME GND

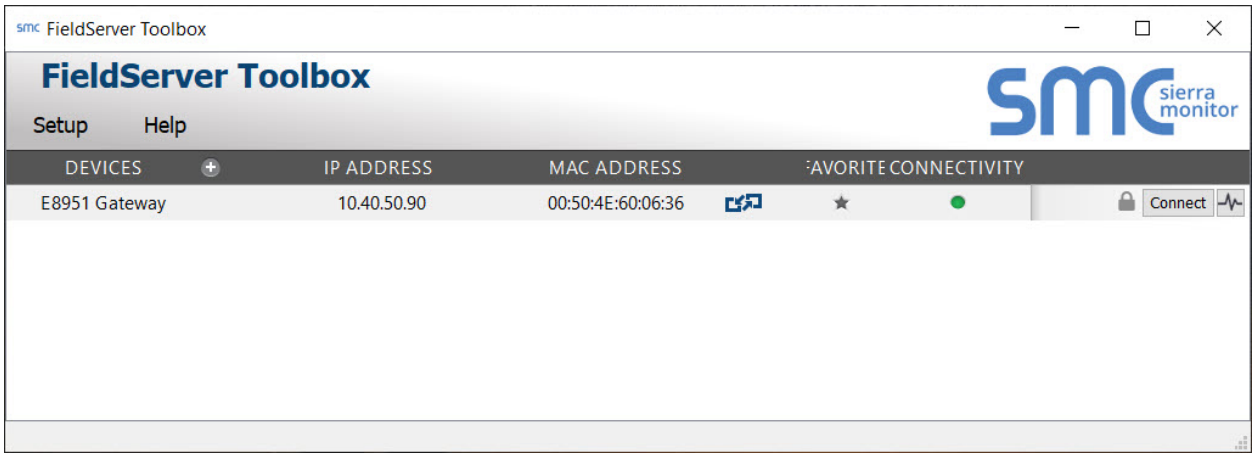
5 Connecting to the BACnet Router

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 11.3 Internet Browser Software Support for supported browsers.

6 Setup Web Server Security

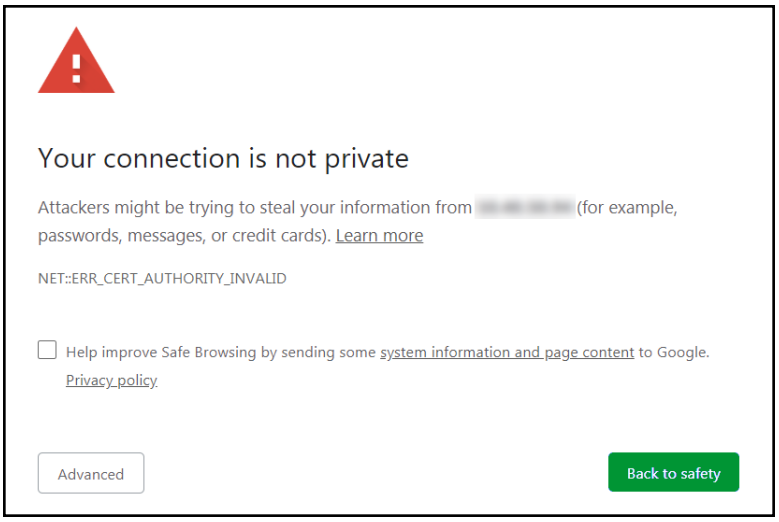
6.1 Login to the FieldServer

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.

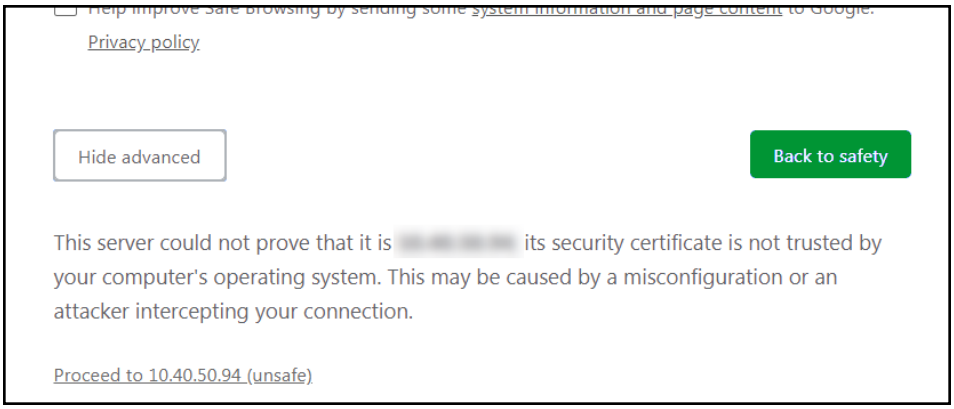
- When the Web Server Security Unconfigured window appears, read the text and choose whether to move forward with HTTPS or HTTP.



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

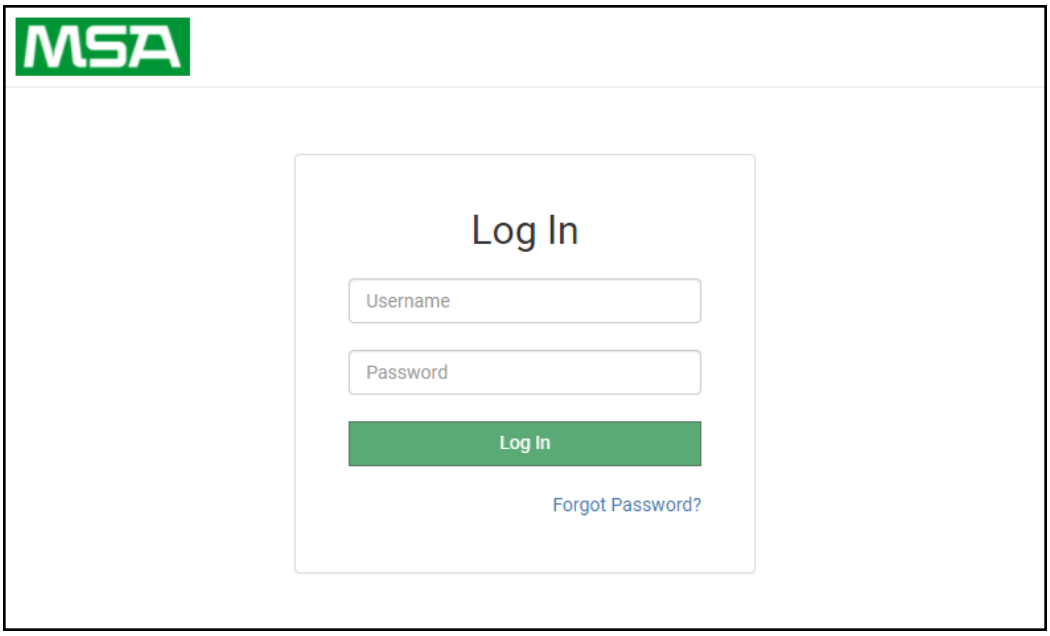


- Additional text will expand below the warning, click the underlined text to go to the IP Address. In the example below this text is "Proceed to <FieldServer IP> (unsafe)".



- 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.

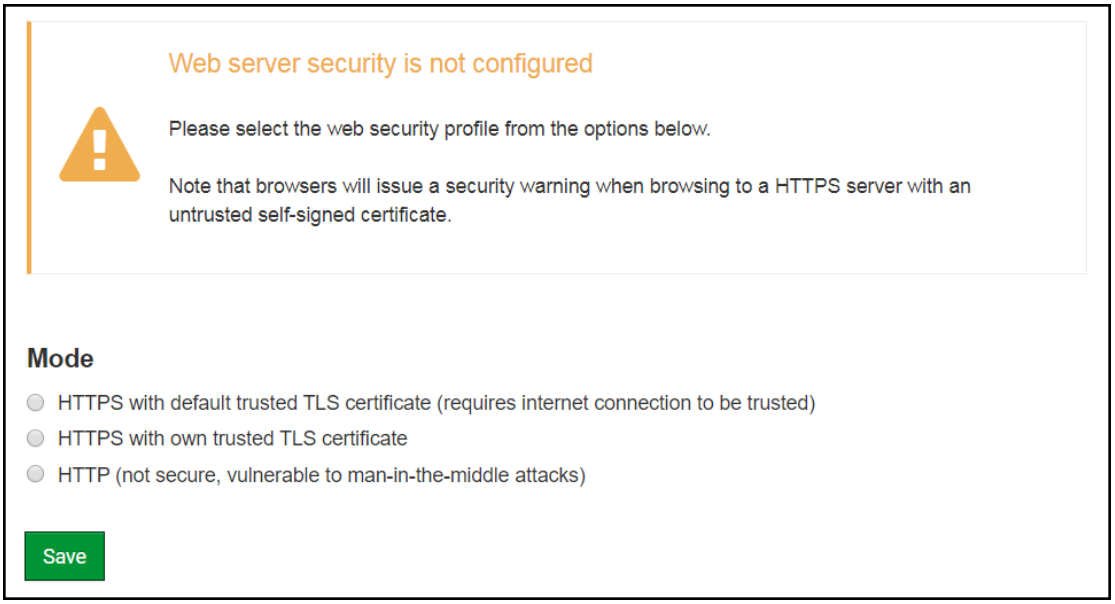


NOTE: A user has 5 attempts to login then there will be a 10-minute lockout. There is no timeout on the FieldServer to enter a password.

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.



NOTE: Cookies are used for authentication.

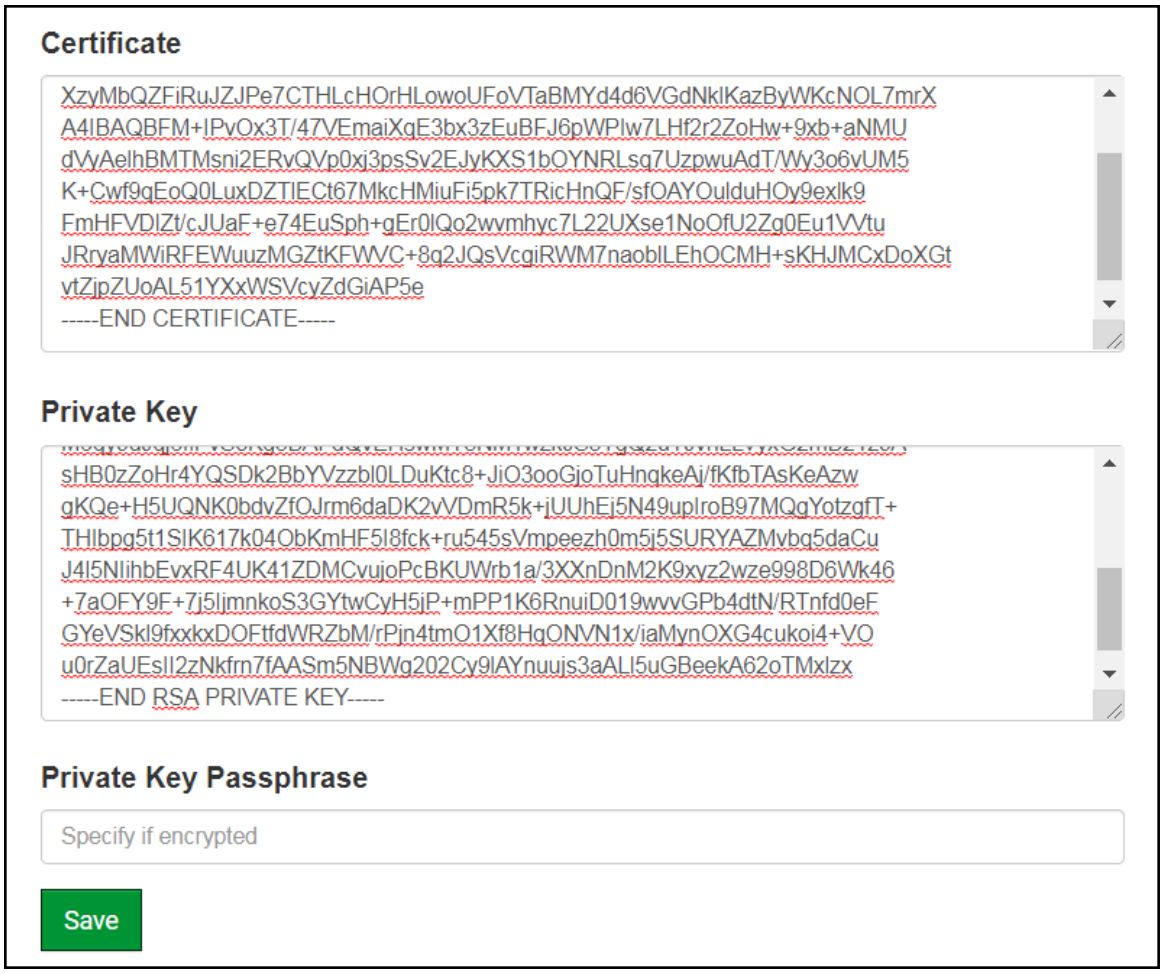
NOTE: To change the web server security mode after initial setup, go to Section 12.1 Change Web Server Security Settings After Initial Setup.

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.



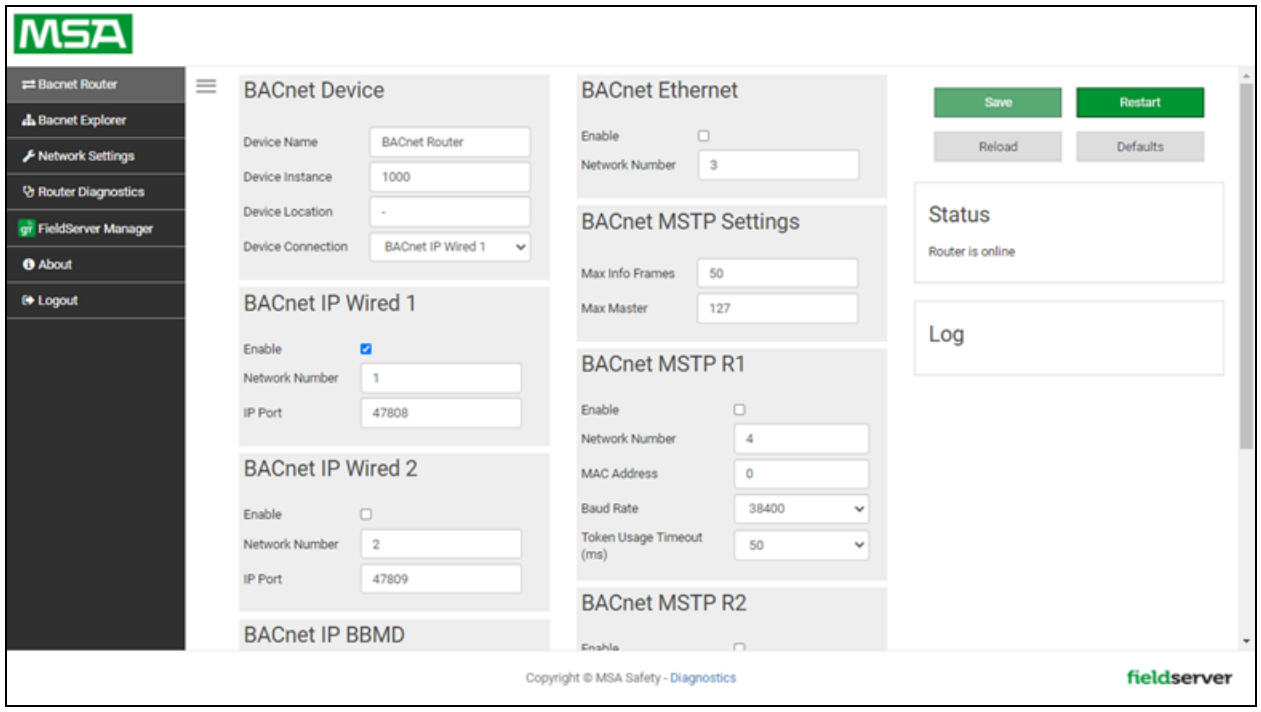
- Copy and paste the Certificate and Private Key text into their respective fields. If the Private Key is encrypted type in the associated Passphrase.
- Click Save.
- A “Redirecting” message will appear. After a short time, the FieldServer GUI will open.

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

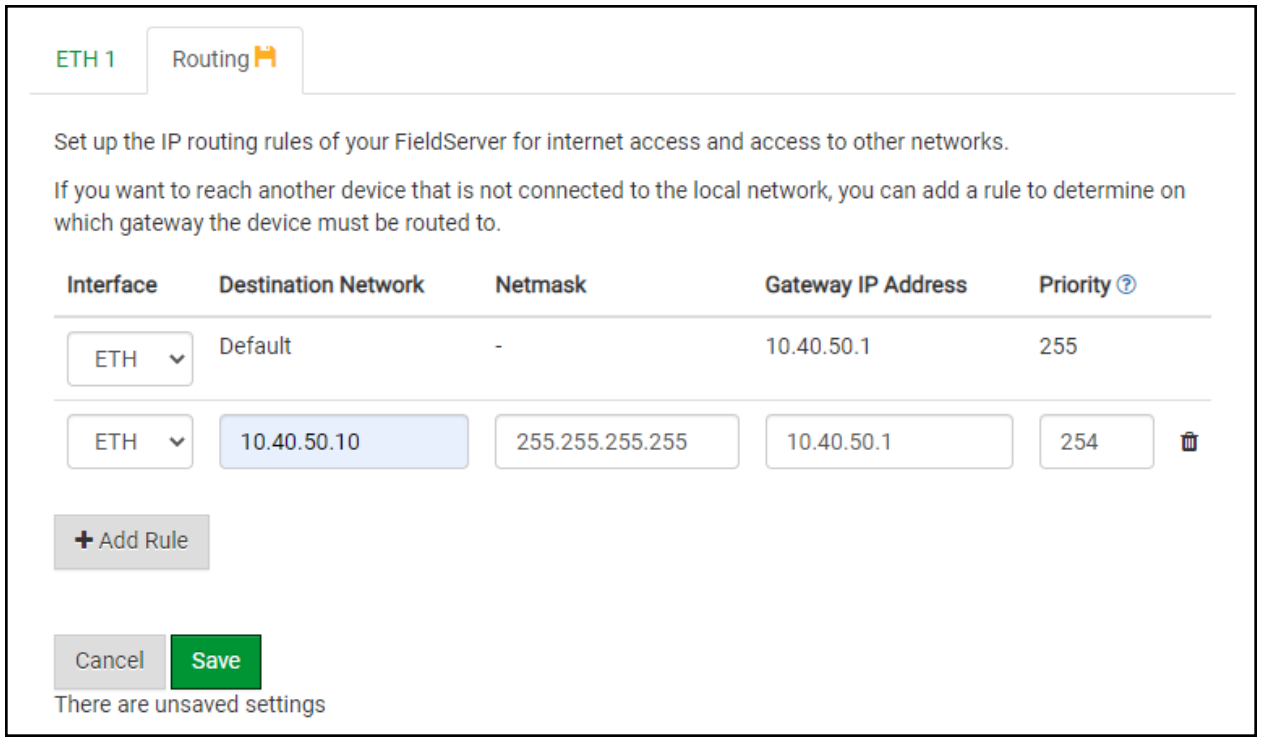
Navigate to the Network Settings tab and configure the settings as needed.



7.1 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.



7.2 Ethernet 1

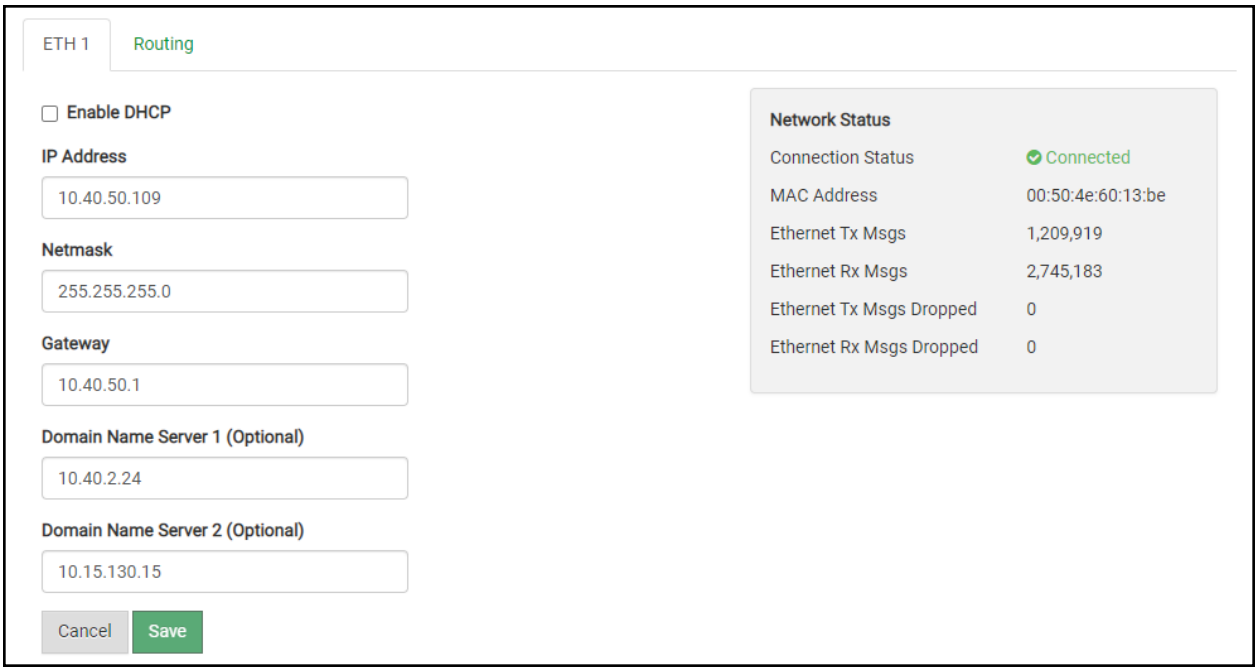
To change the FieldServer IP Settings, follow these instructions:

- 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.

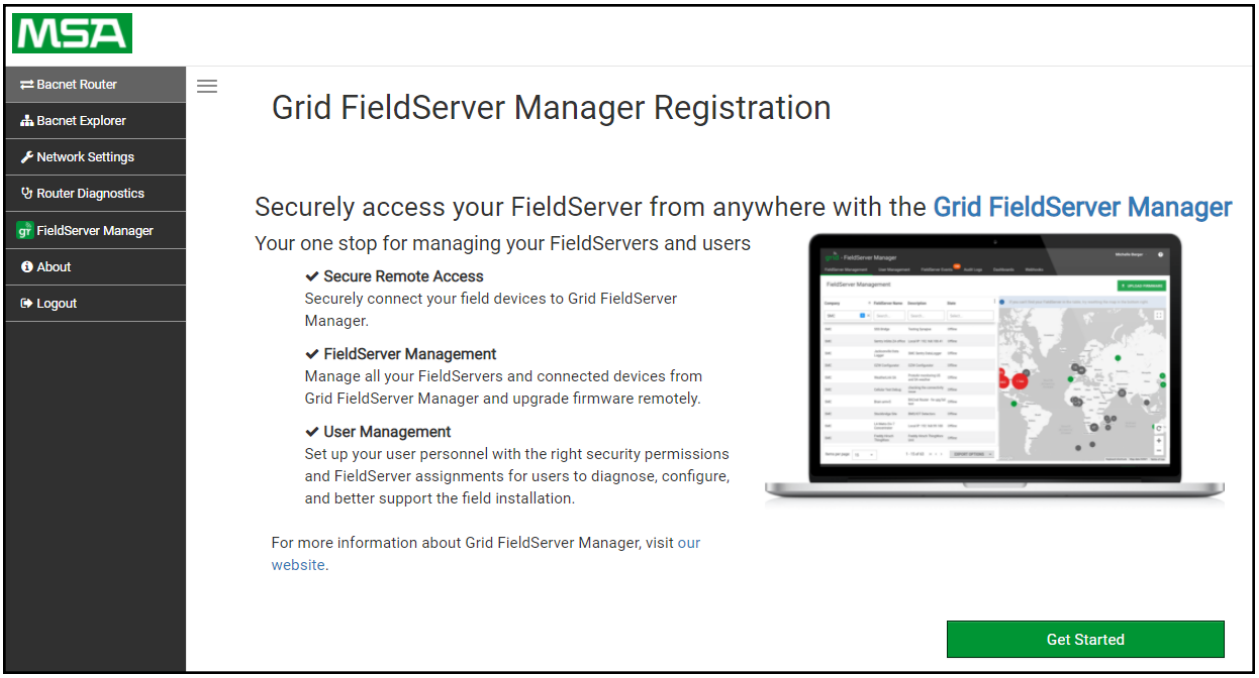
NOTE: The browser needs to be updated to the new IP Address of the FieldServer before the settings will be accessible again.



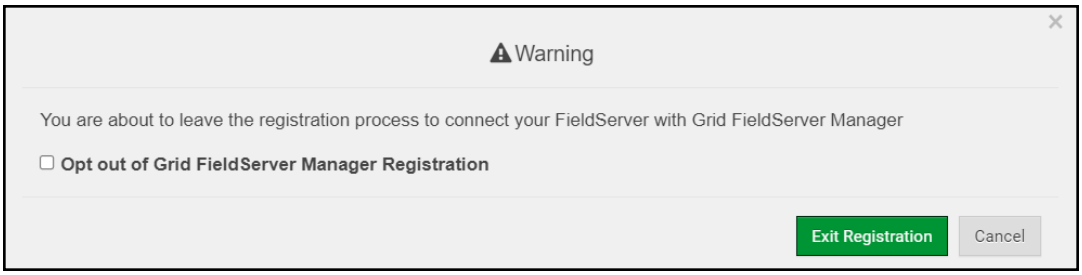
8 Configuring the BACnet Router

8.1 Navigate to the BACnet Router Settings

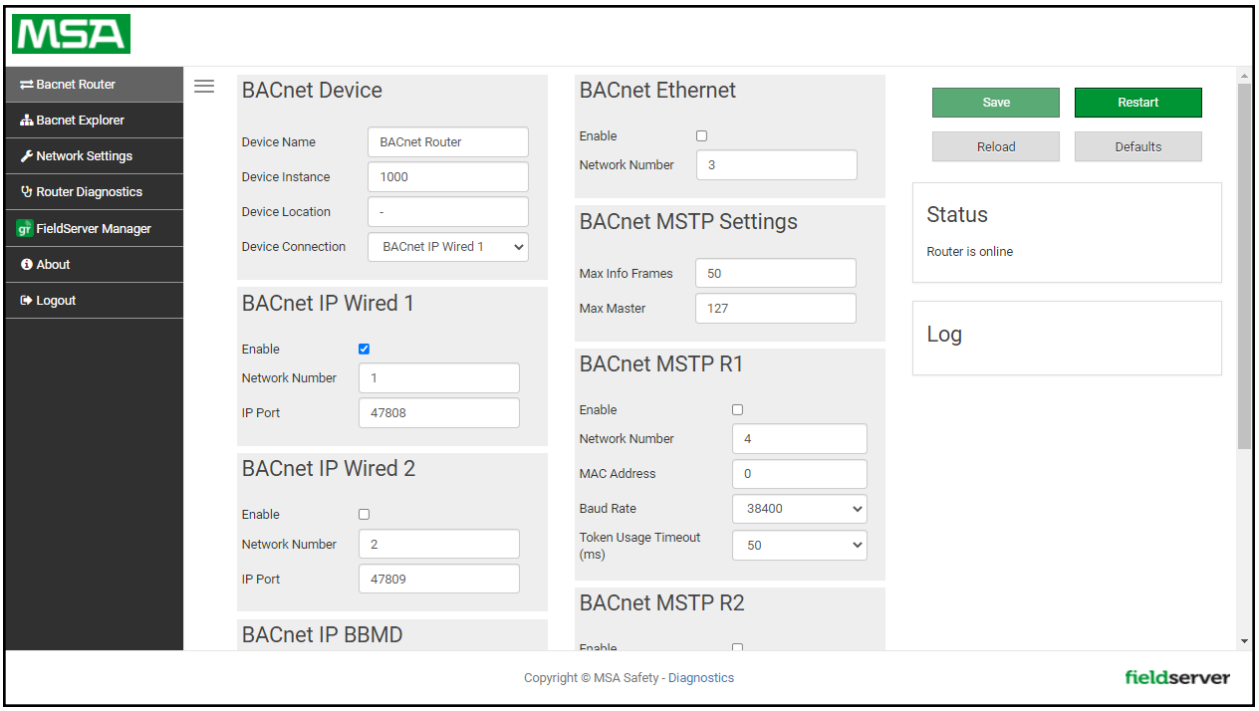
- From the Web App landing page, click the BACnet Router tab on the left side of the screen.



- 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



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.

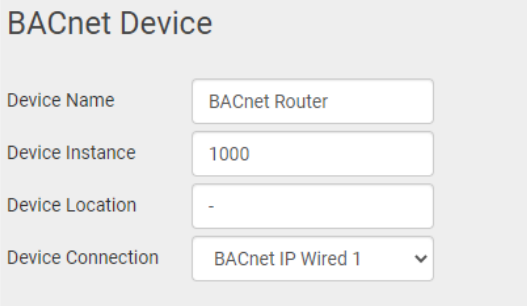
8.2.2 Multiple Connections

- **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.

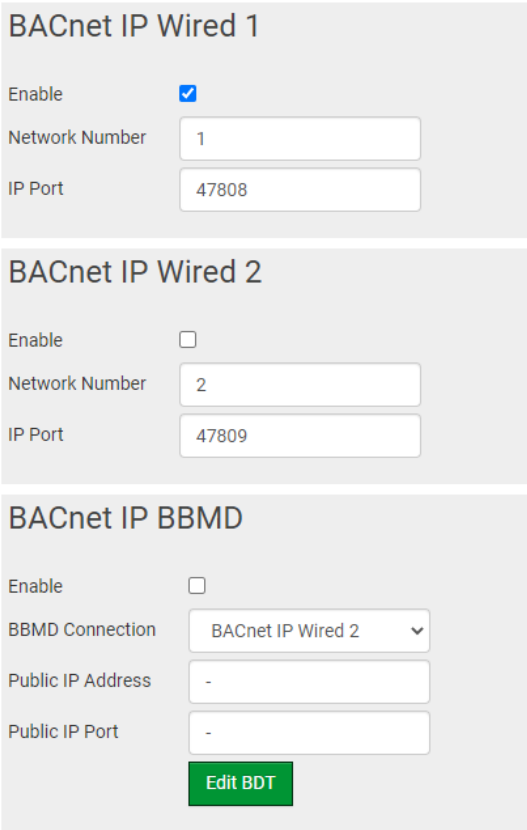
- **Enable** – enable or disable the connection; note that BACnet/IP Primary is always enabled.

8.2.3 BACnet Device



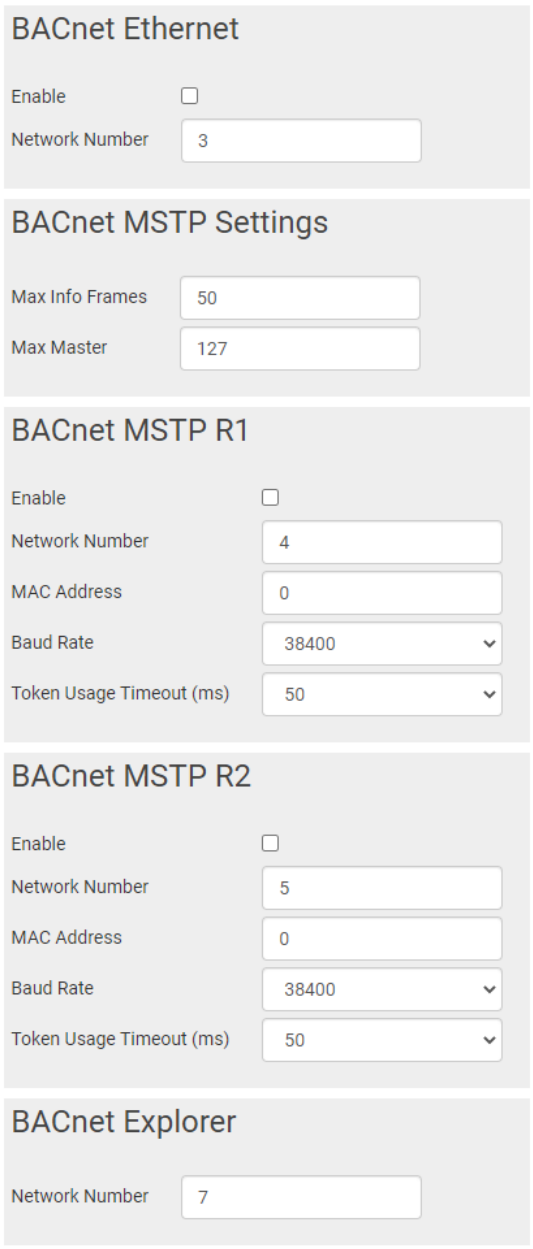
- **Device Instance** and **Device Name** – a BACnet Router must provide a Device Object. Configure its name and Instance Number here. Take care to select a Device Instance Number that is unique across the entire BACnet internetwork.
- **Device Location** – enter a location for the Device. The location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

8.2.4 BACnet/IP



- **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.

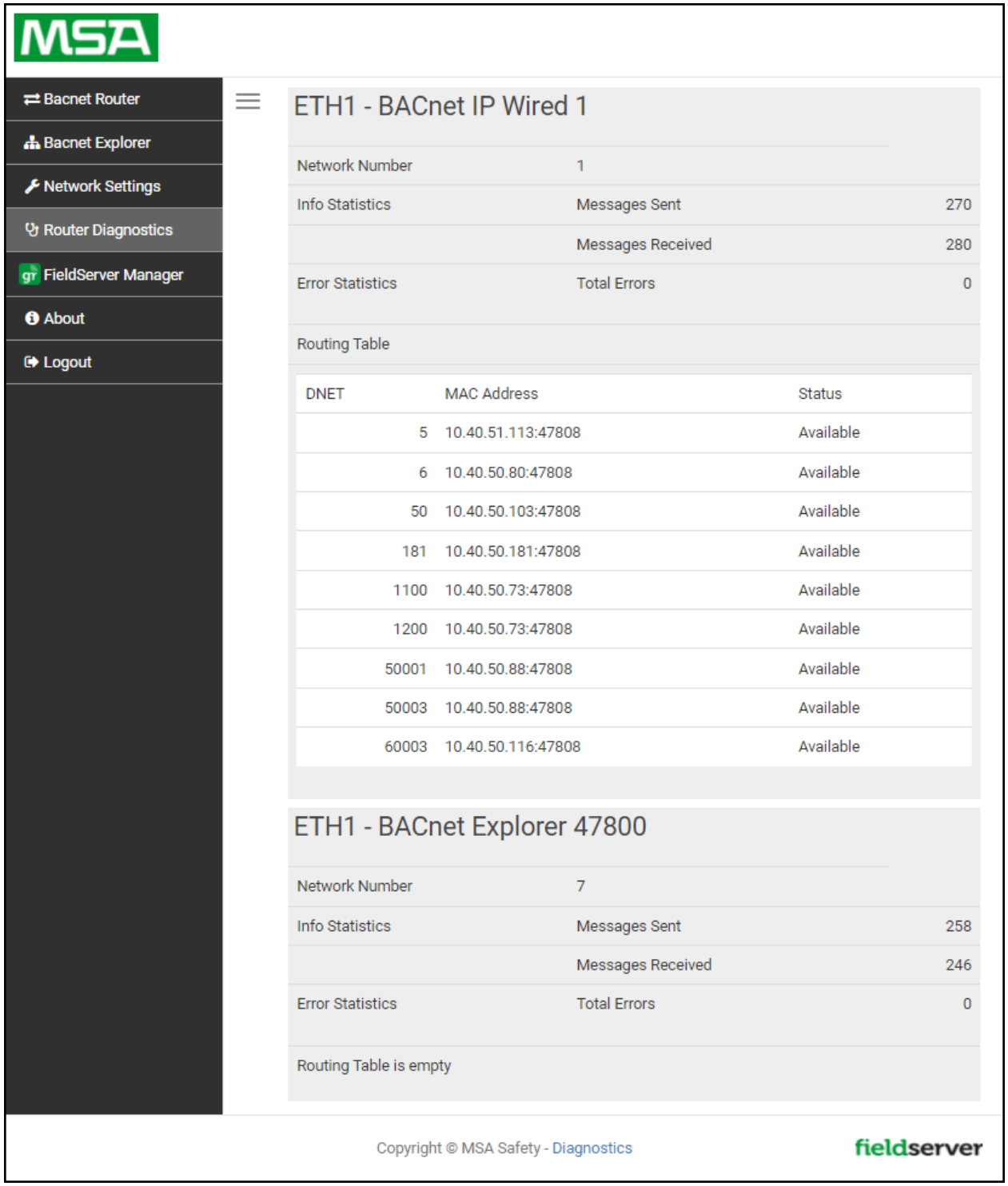
8.2.5 BACnet MS/TP, BACnet Ethernet and BACnet Explorer



- **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

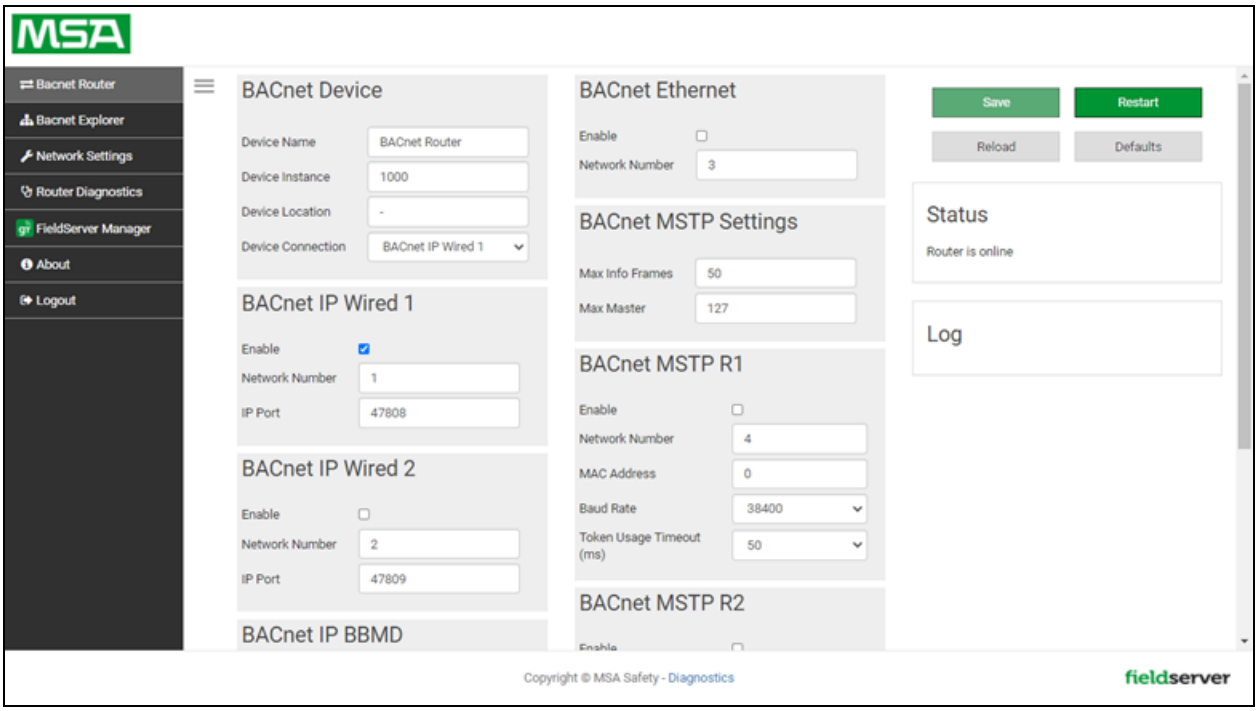
By clicking on the Router Diagnostics tab all the connection communication details can be viewed to ensure the BACnet Router is working correctly.



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.

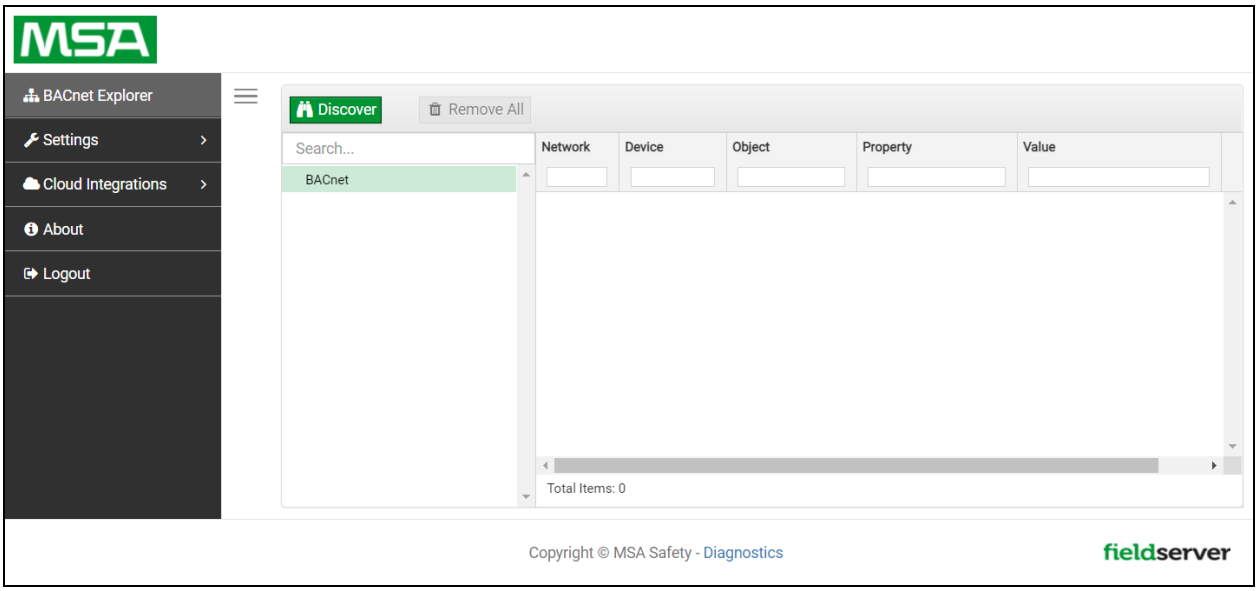
- To access the embedded BACnet Explorer, click the BACnet Explorer tab.



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.

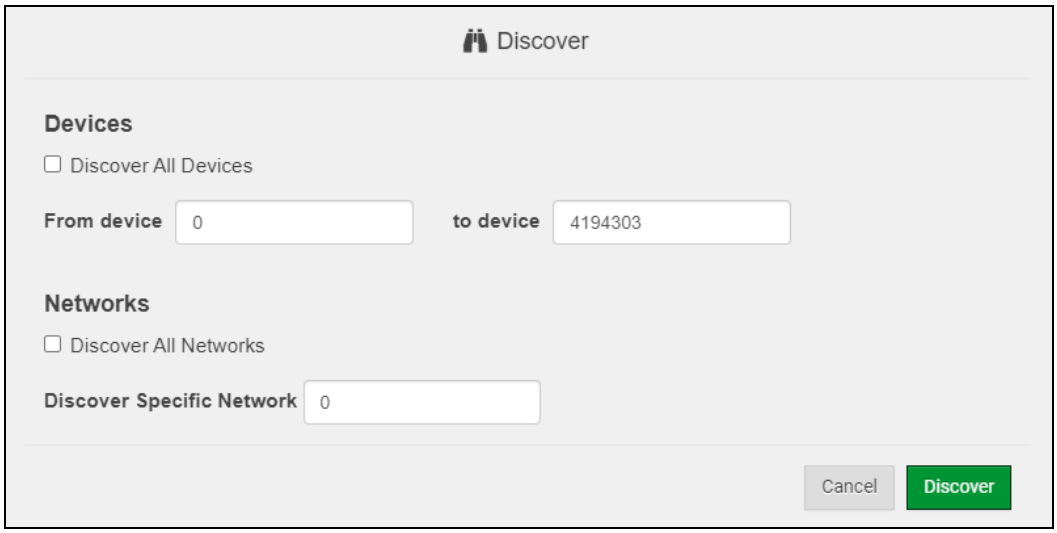
9.1 Discover the Device List

- 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.



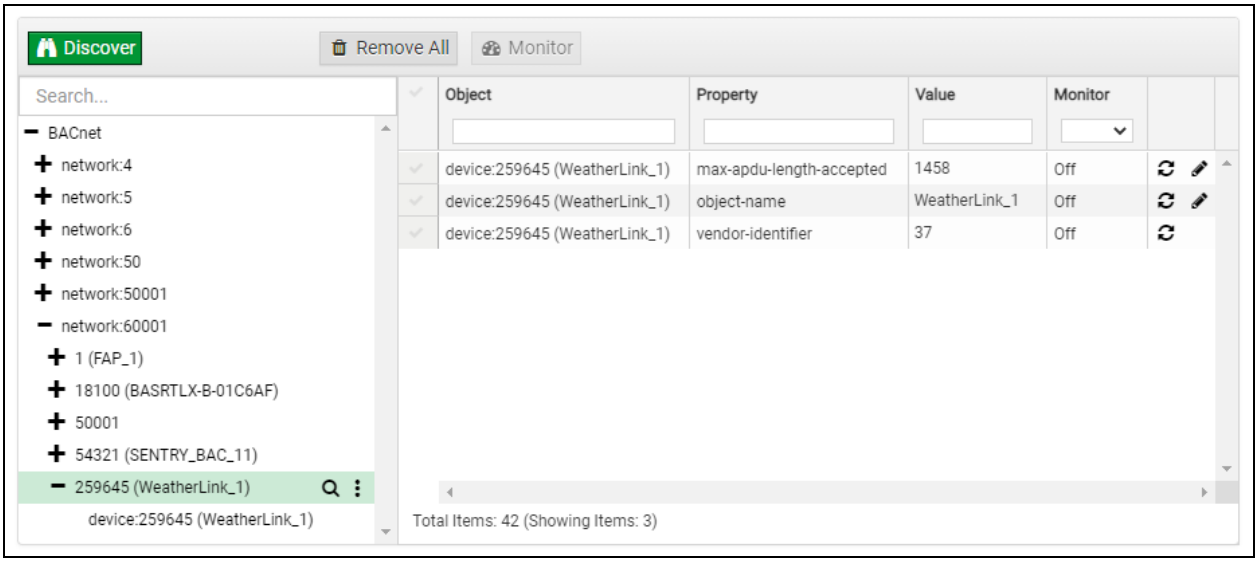
NOTE: The "Discover All Devices" or "Discover All Networks" checkboxes must be unchecked to search for a specific device range or network.

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.

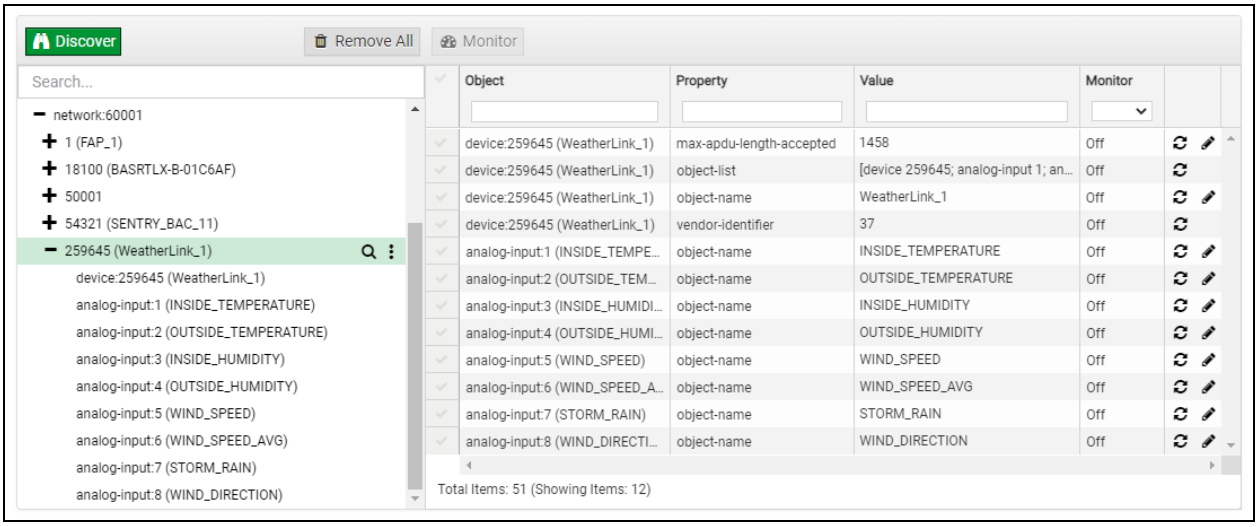


9.2 View Device Details and Explore Points/Parameters

- 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

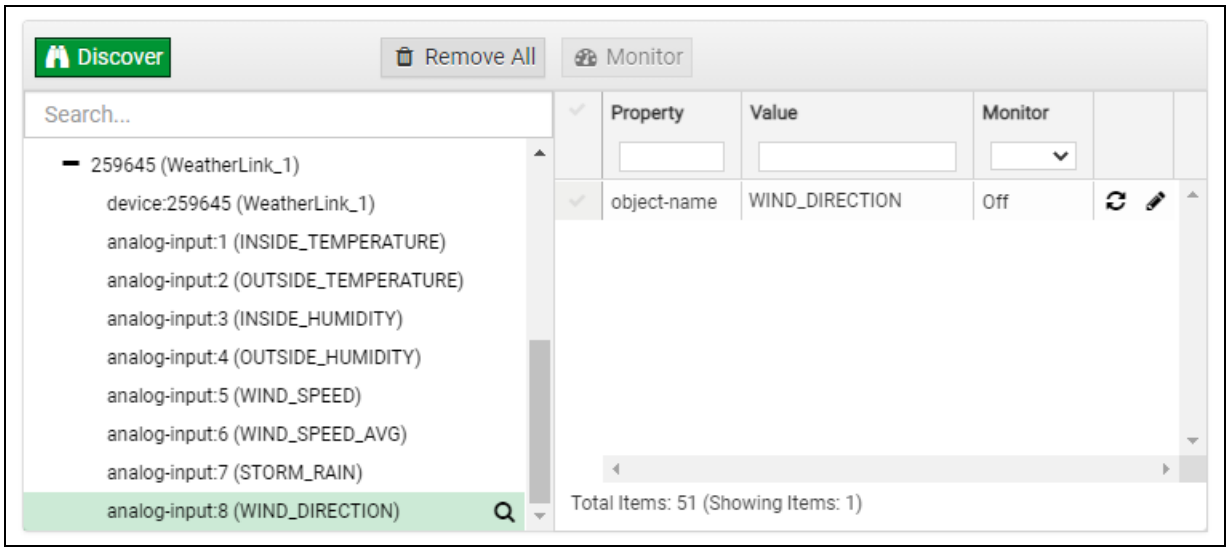


- To view the full details of a device, highlight the device directly (in the image below – "1991 WeatherLink_1") and click the Explore button (🔍) that appears to the right of the highlighted device as a magnifying glass icon or double-click the highlighted device.

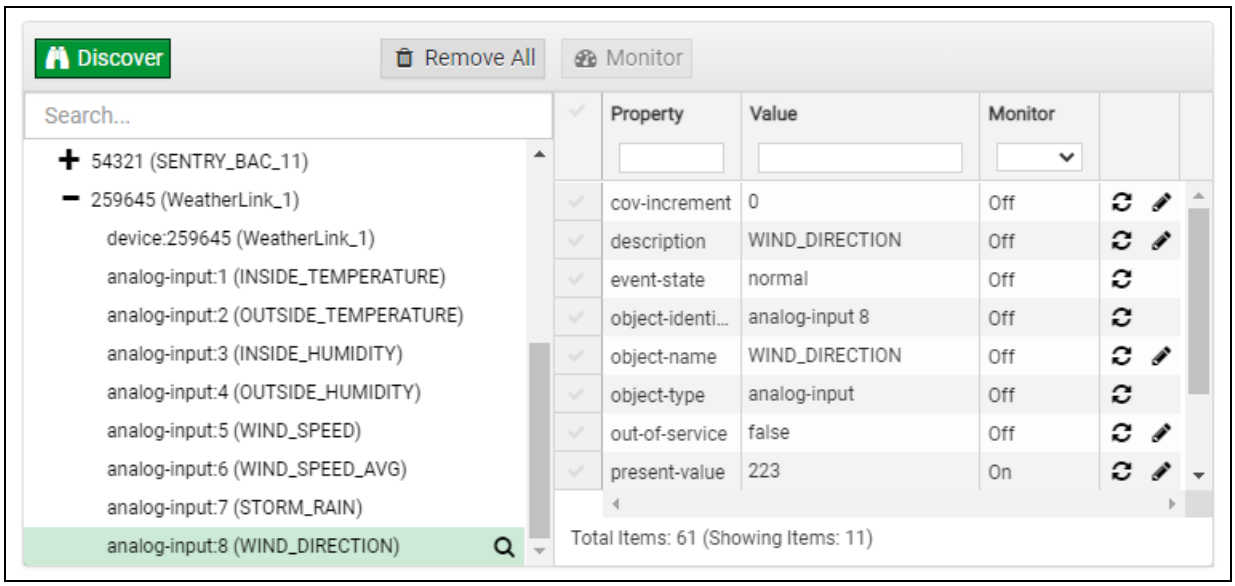


  - Now additional device details are viewable; however, the device can be explored even further

- 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.

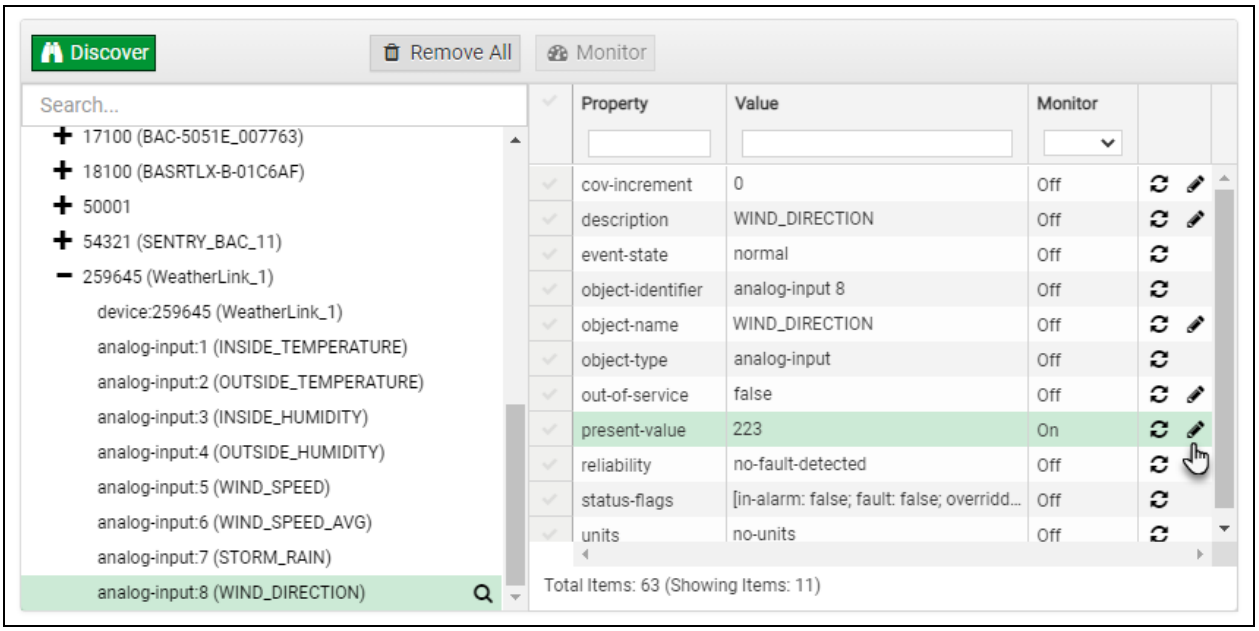
- Network number
  - Device
    - Device object

9.2.1 Edit the Present Value Field

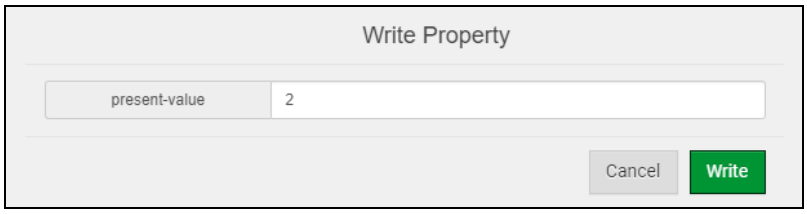
The only recommended field to edit is the device's present value field.

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.

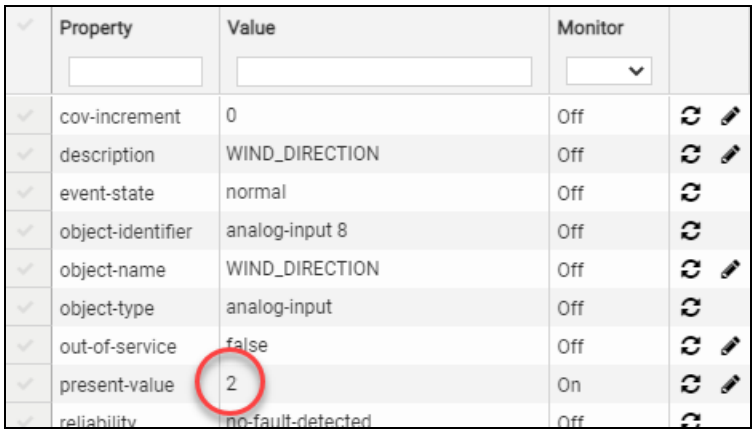


- Then click the Write button (✎) on the right of the property to bring up the Write Property window.



- 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.



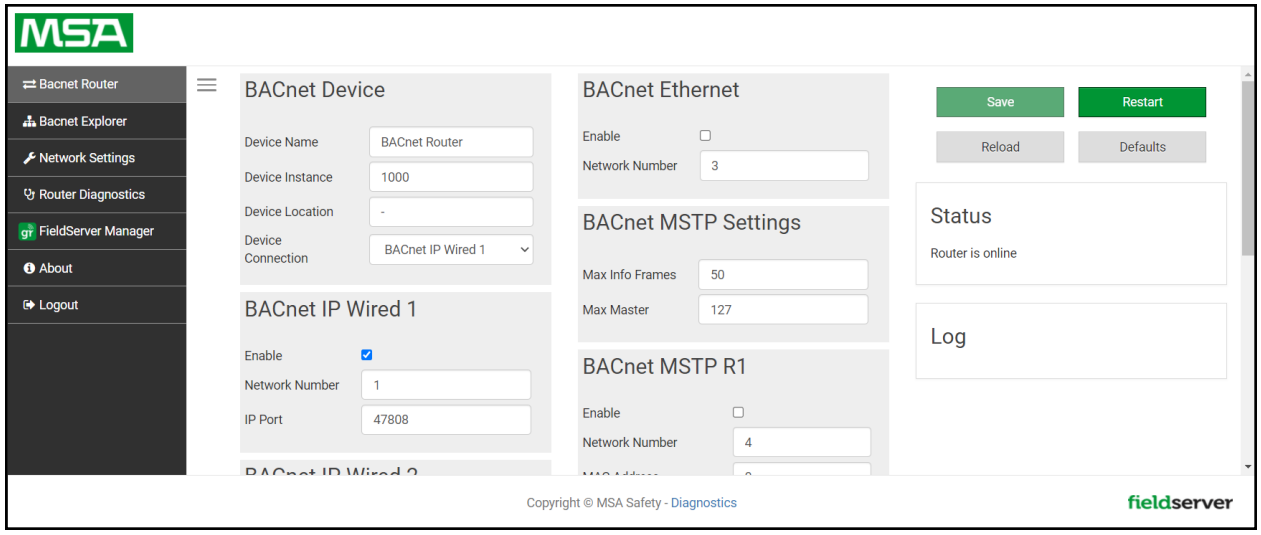
10 MSA Grid - FieldSever Manager Setup

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.

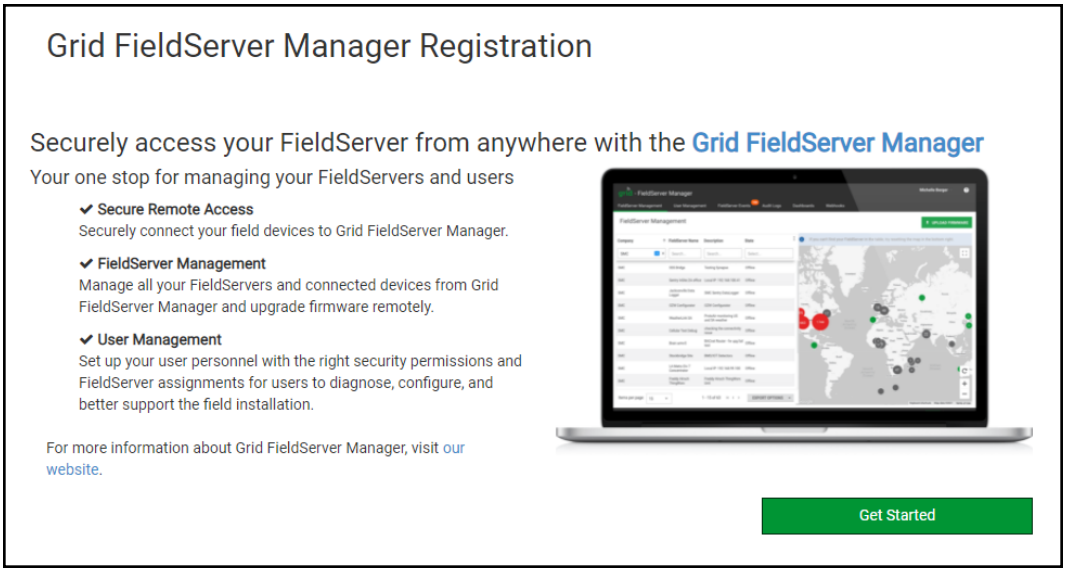
10.1 Create a New FieldServer Manager Account

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

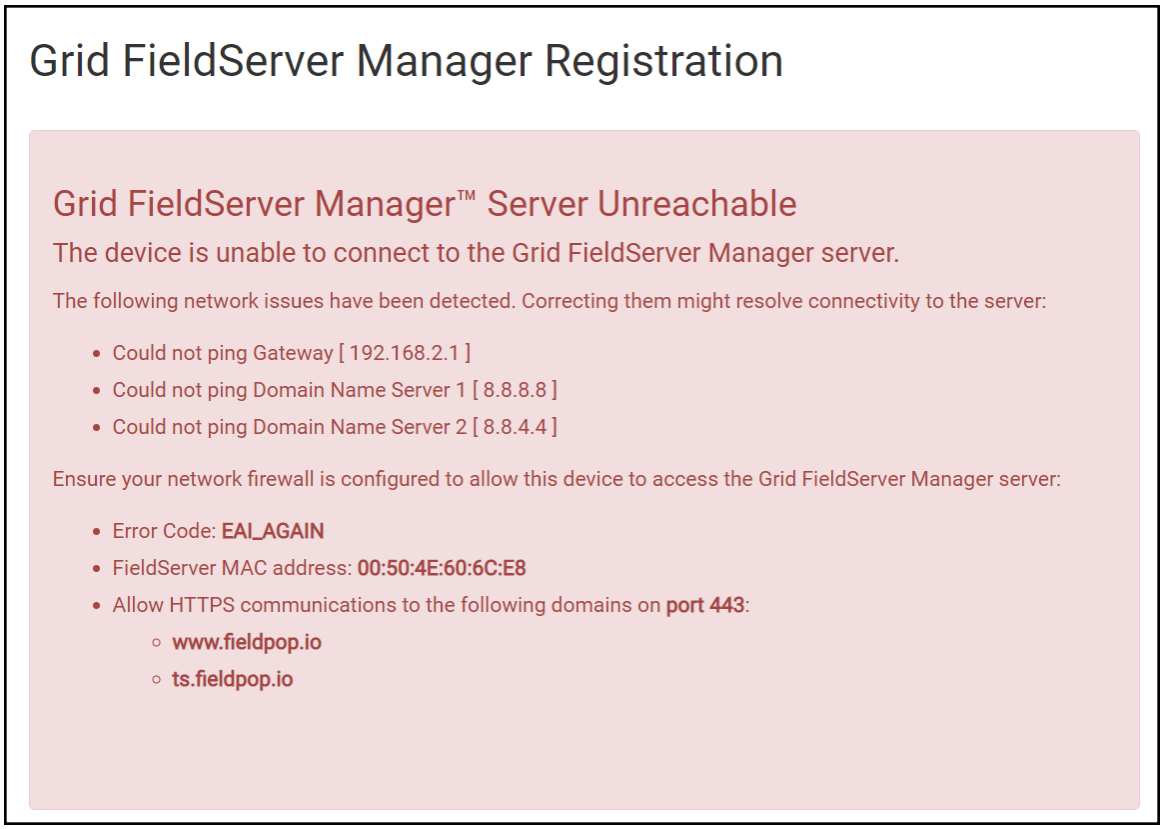
- Click on the FieldServer Manager tab.



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



- 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.



  - 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:

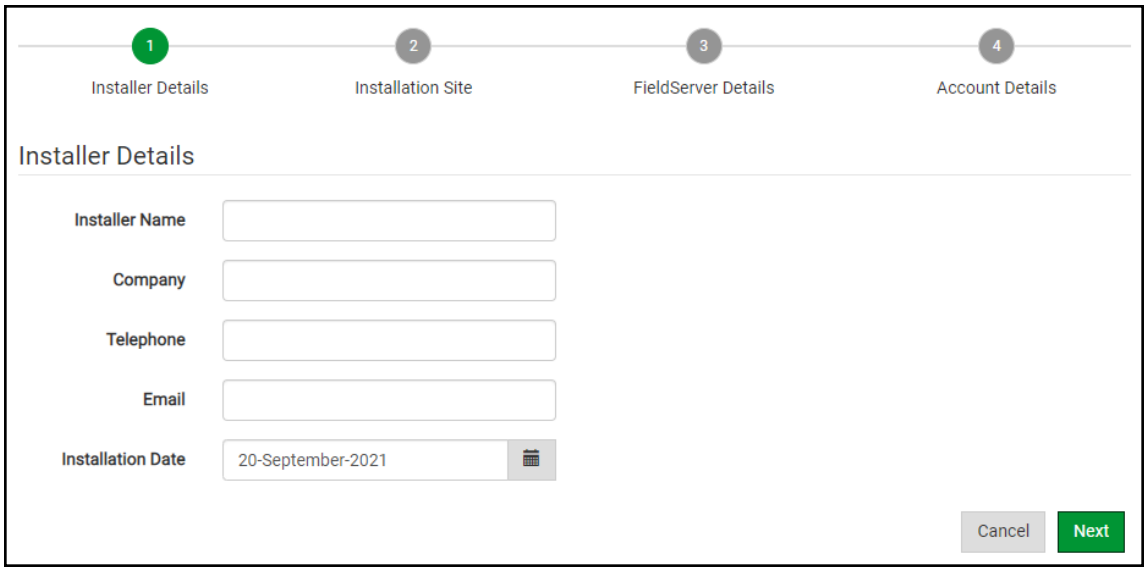
    DNS1=8.8.8.8

    DNS2=8.8.4.4

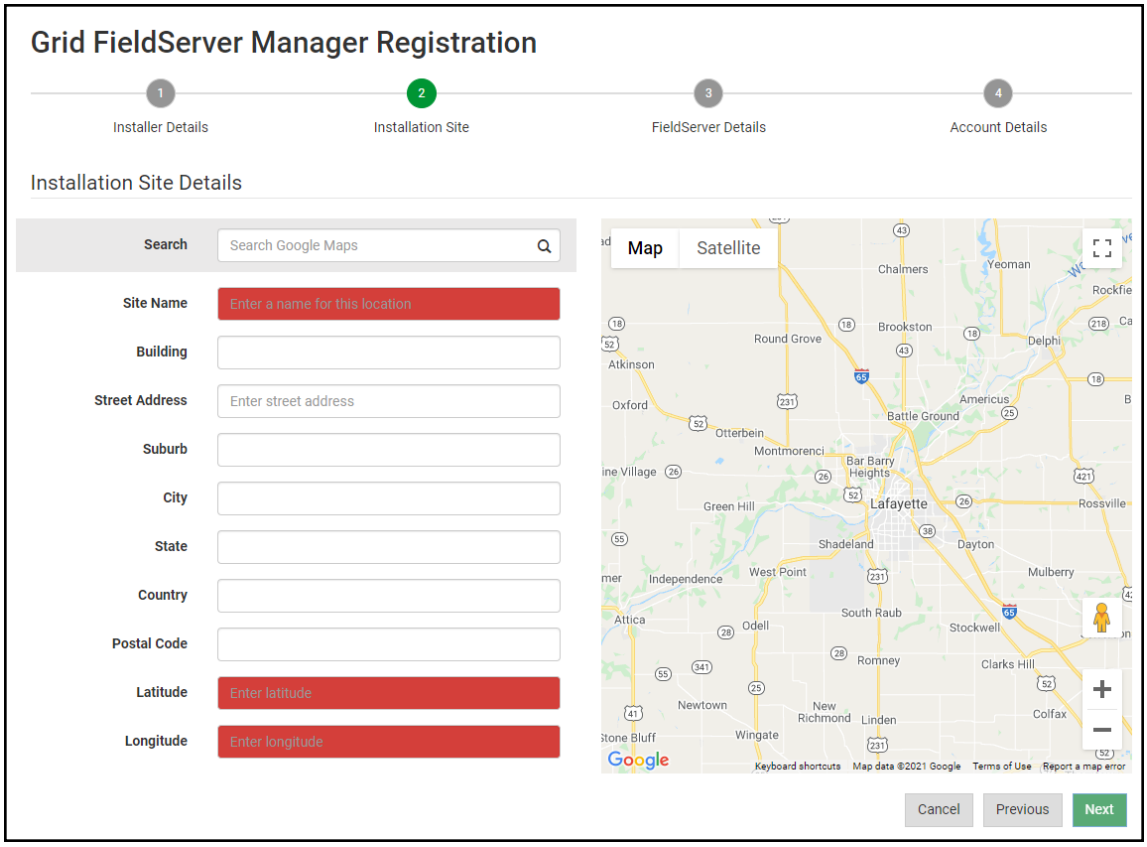
  - Ensure that the BACnet Router is properly connected to the Internet

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

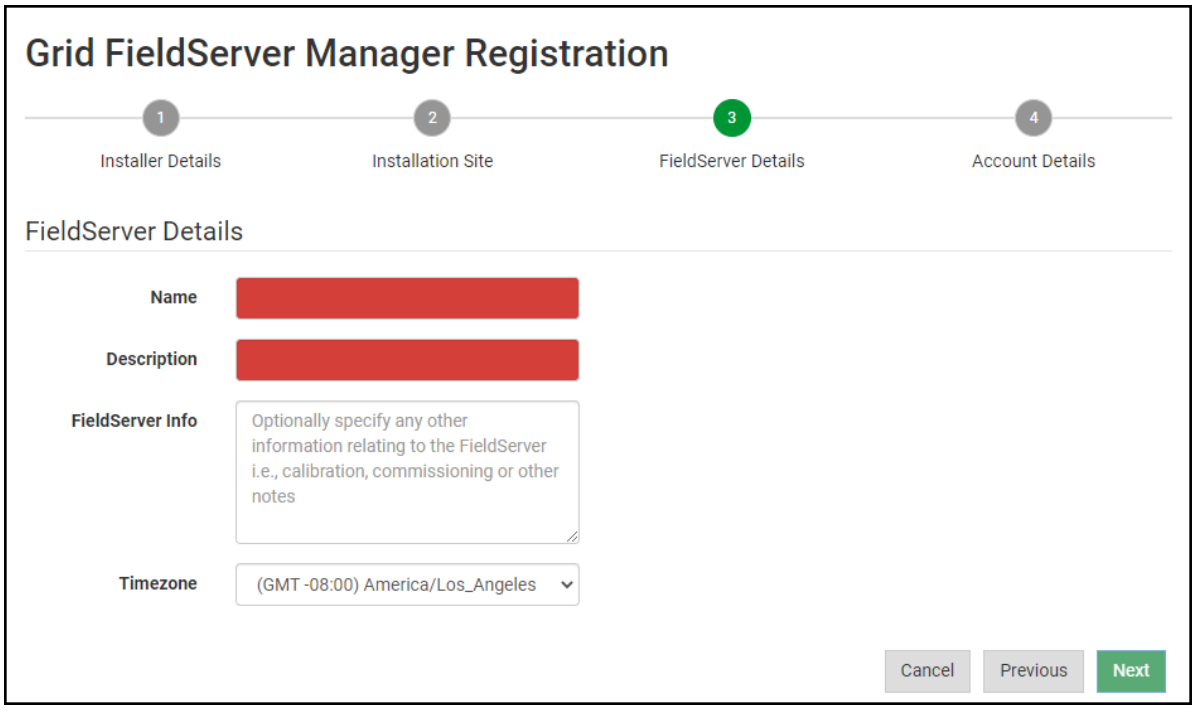
- Fill in the user details, site details, gateway details and create a new account.
  - Enter user details and click Next



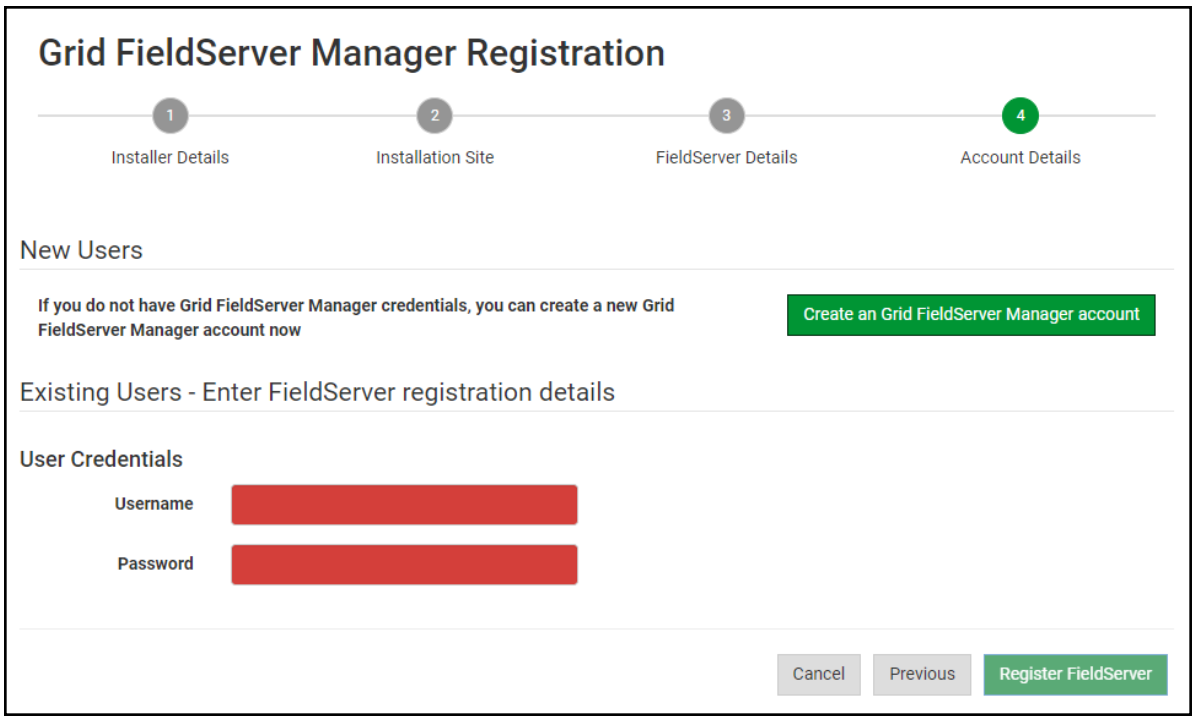
  - Enter the site details by entering the physical address fields or the latitude and longitude then click Next



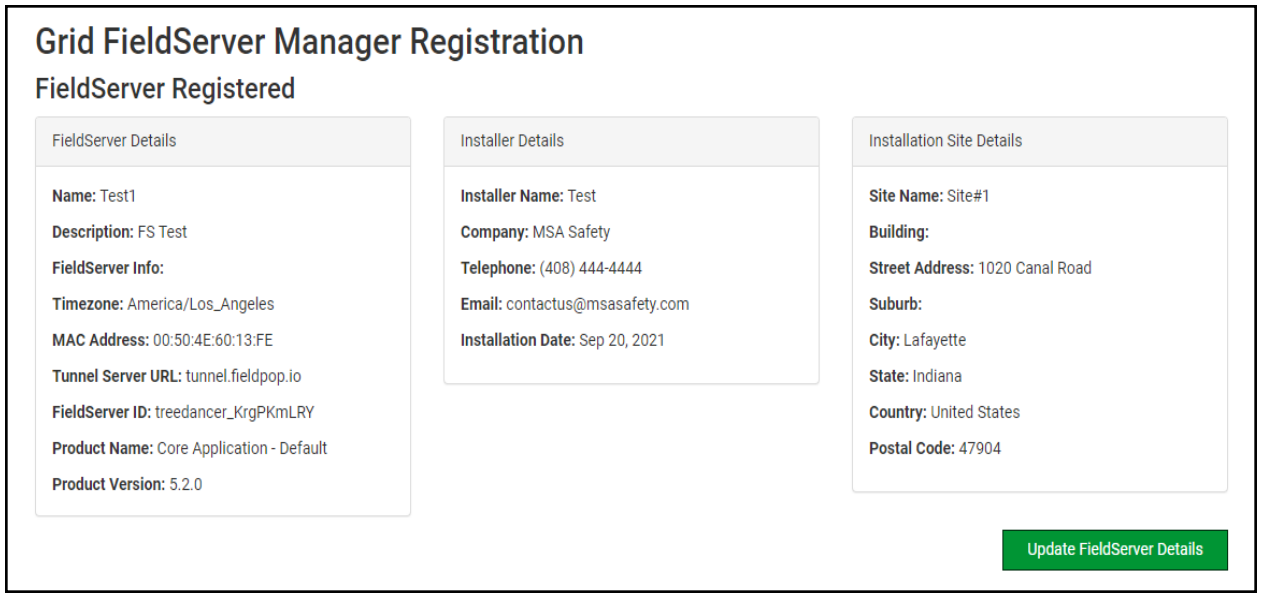
- Enter Name and Description (required) then click Next



- 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

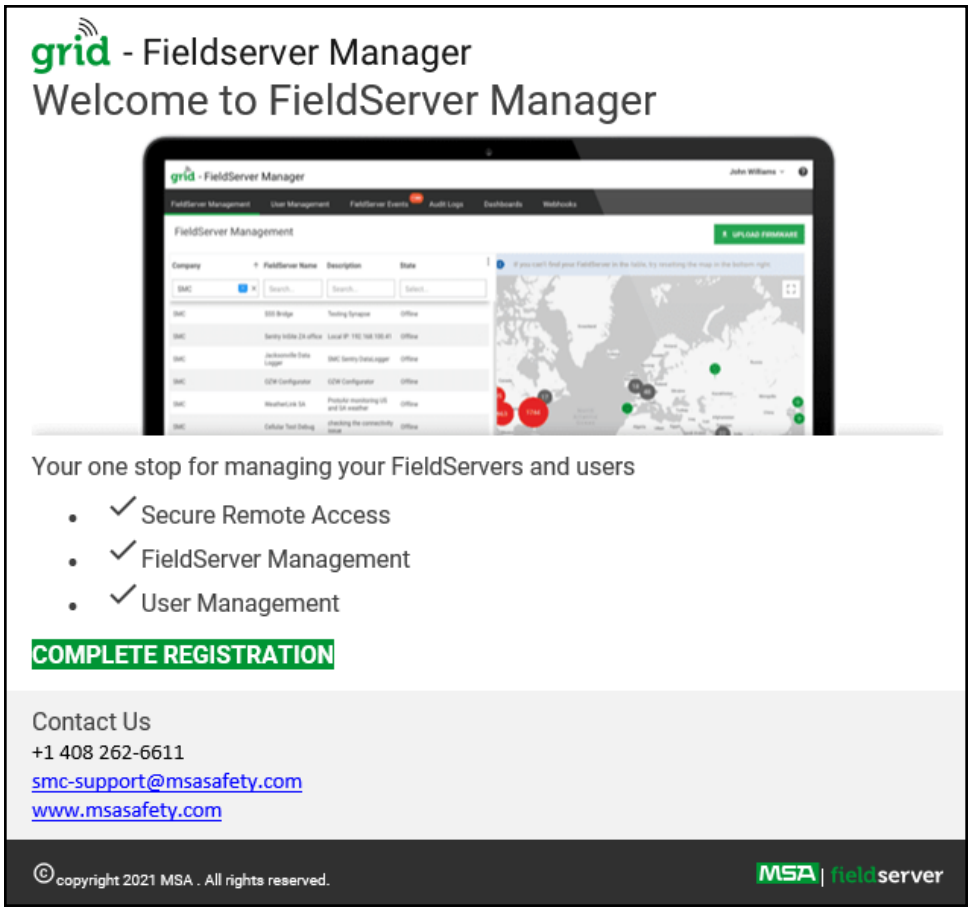


- Once the device is registered, a confirmation window will appear. Click the Close button and the following screen will appear listing the device details and additional information auto-populated by the BACnet Router.



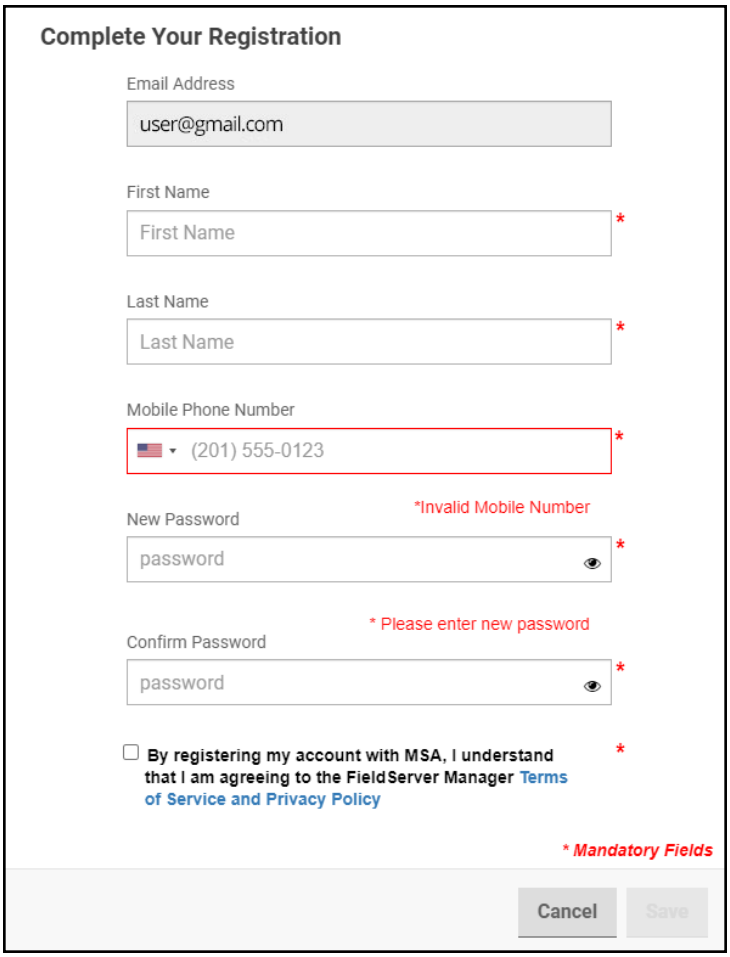
NOTE: Update these details at any time by going to the FieldServer Manager tab and clicking the Update FieldServer Details button.

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



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.



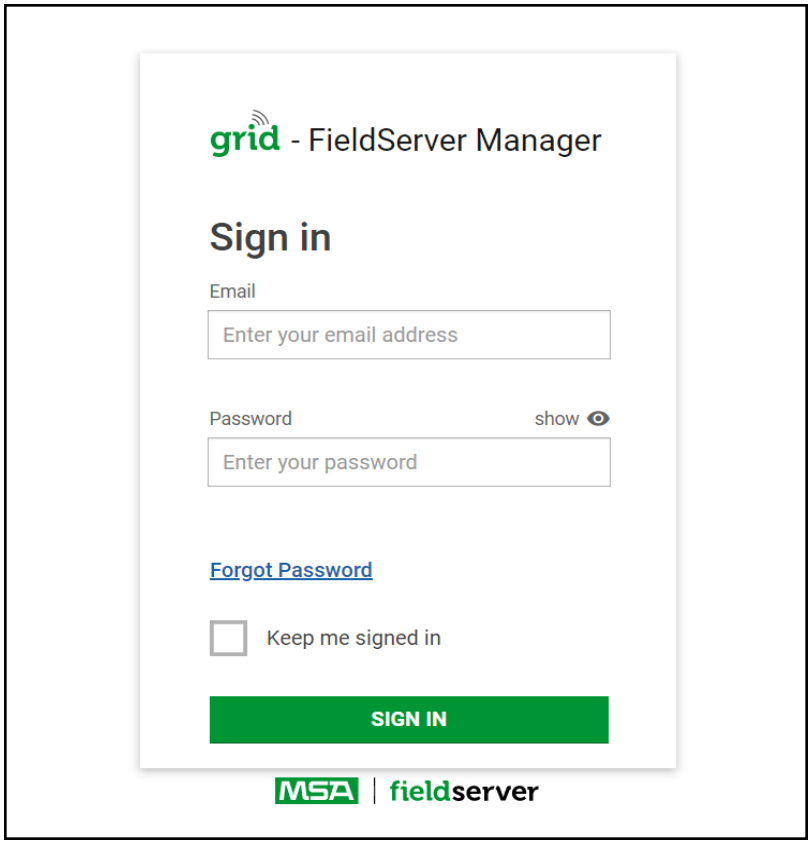
- Fill in the name, phone number, password fields and click the checkbox to agree to the privacy policy and terms of service.

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

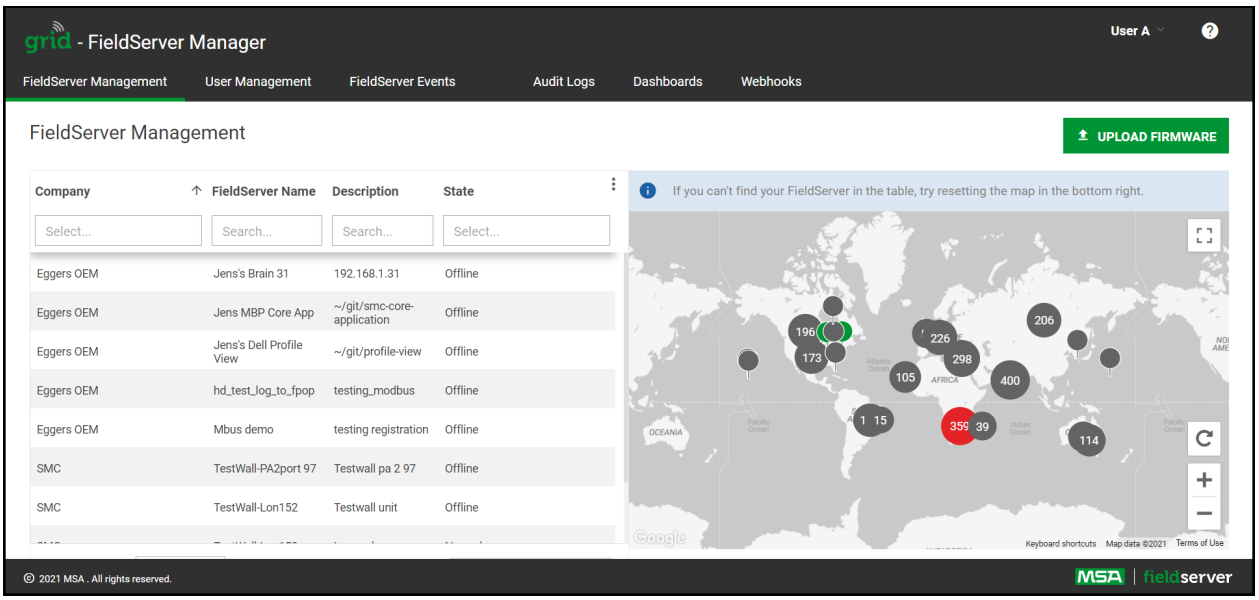
- Click “Save” to save the user details.
- Click “OK” when the Success message appears.
- Record the email account used and password for future use.

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.

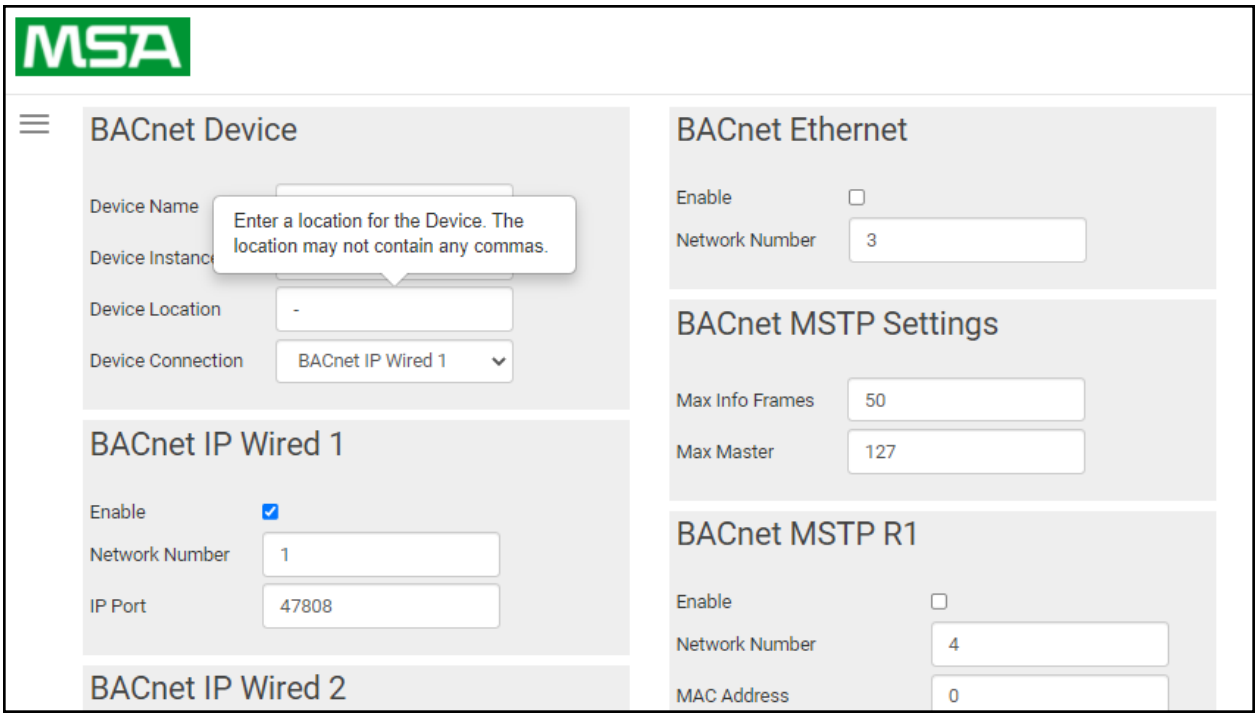


NOTE: For additional FieldServer Manager instructions see the MSA Grid - FieldServer Manager Start-up Guide.

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 Factory Reset Instructions

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

11.3 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

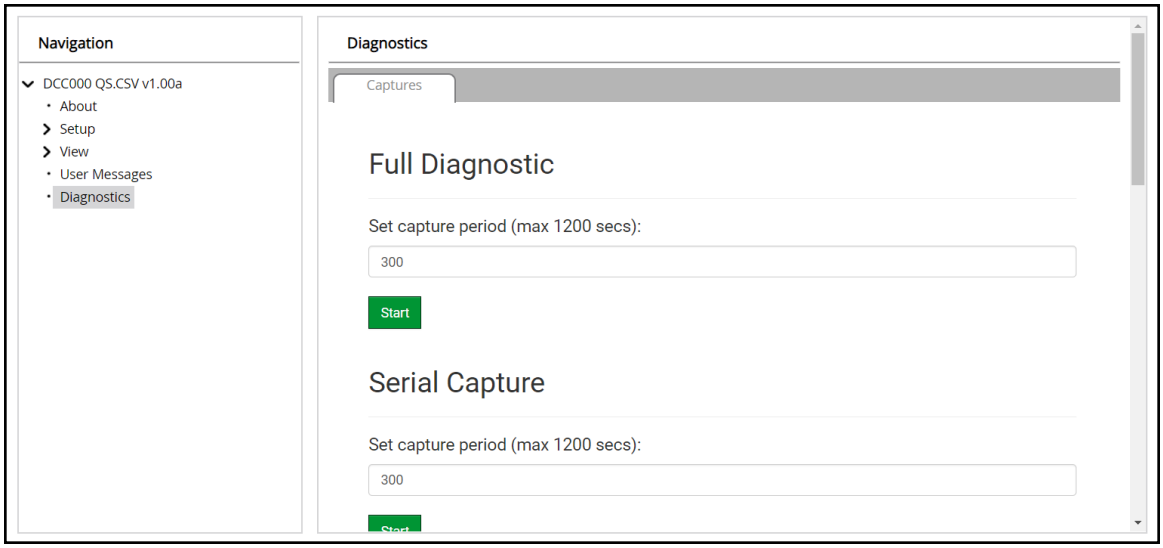
NOTE: Internet Explorer is no longer supported as recommended by Microsoft.

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

11.4 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).

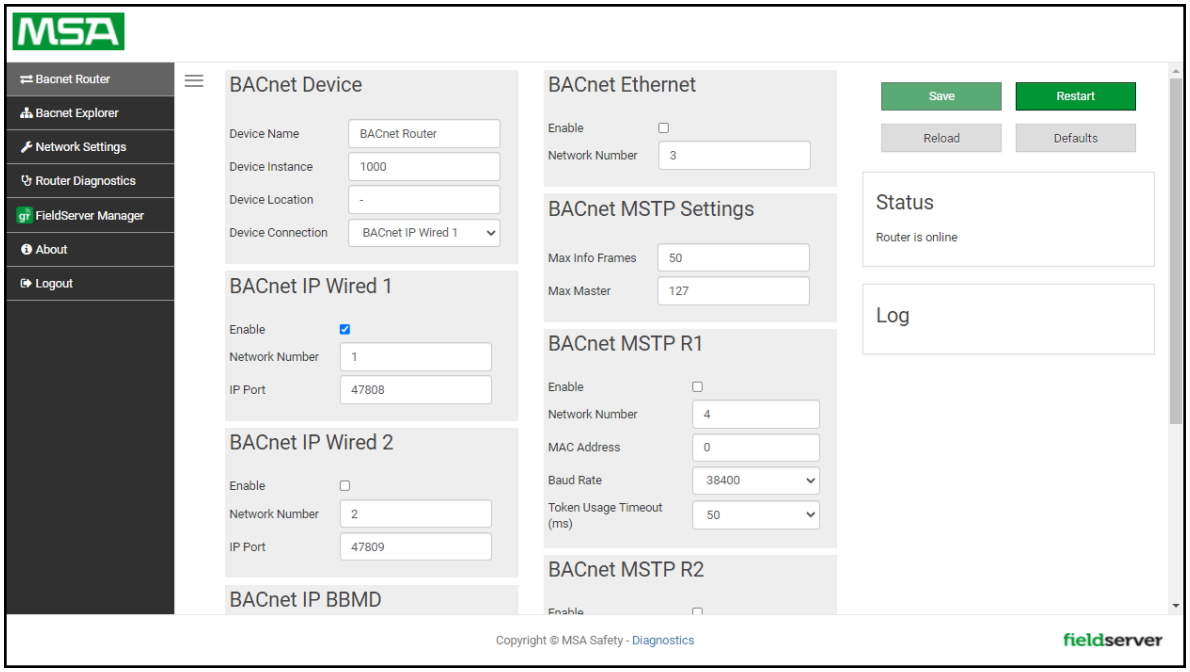
NOTE: Diagnostic captures of BACnet MS/TP communication are output in a ".PCAP" file extension which is compatible with Wireshark.

12 Additional Information

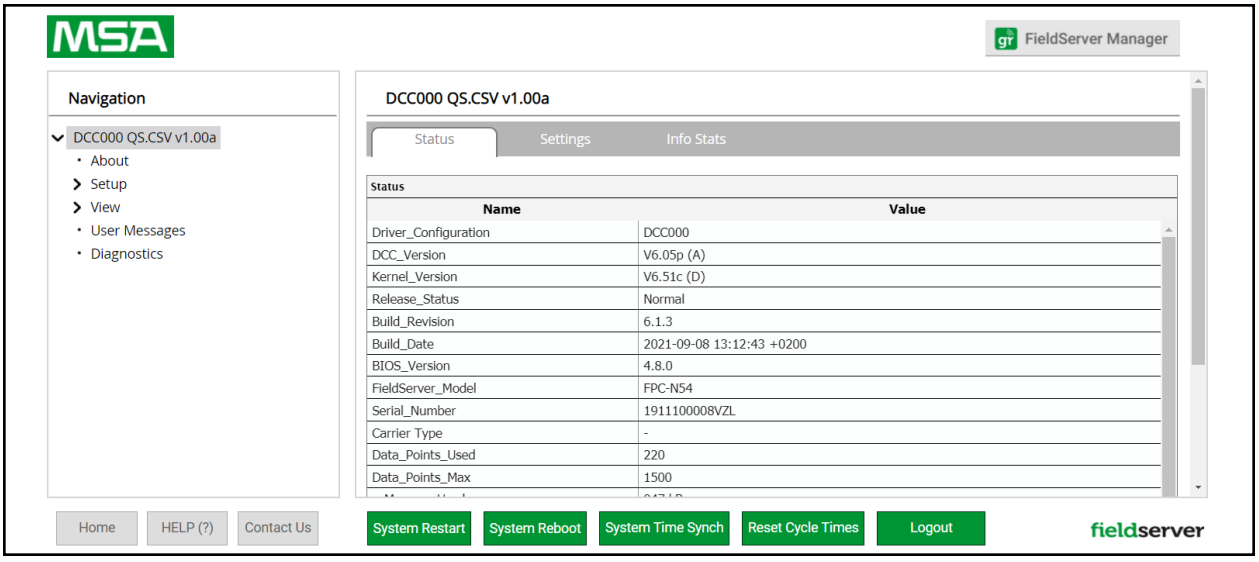
12.1 Change Web Server Security Settings After Initial Setup

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.

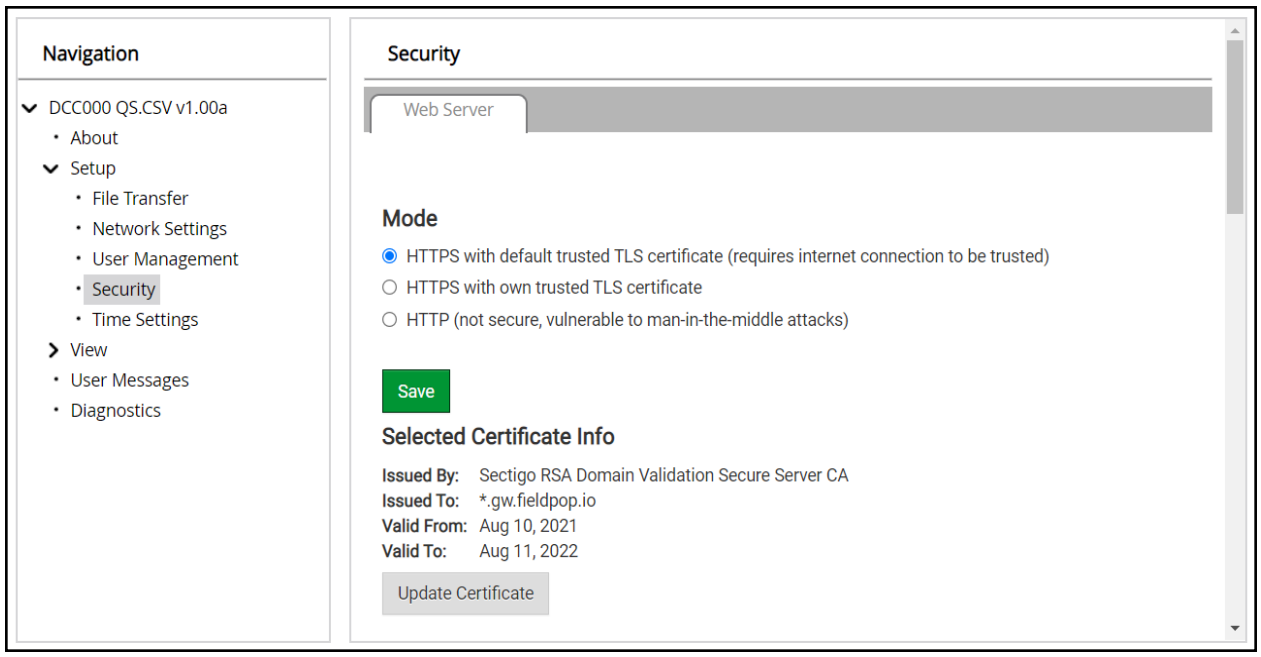


- Click Setup in the Navigation panel.



12.1.1 Change Security Mode

- Click Security in the Navigation panel.

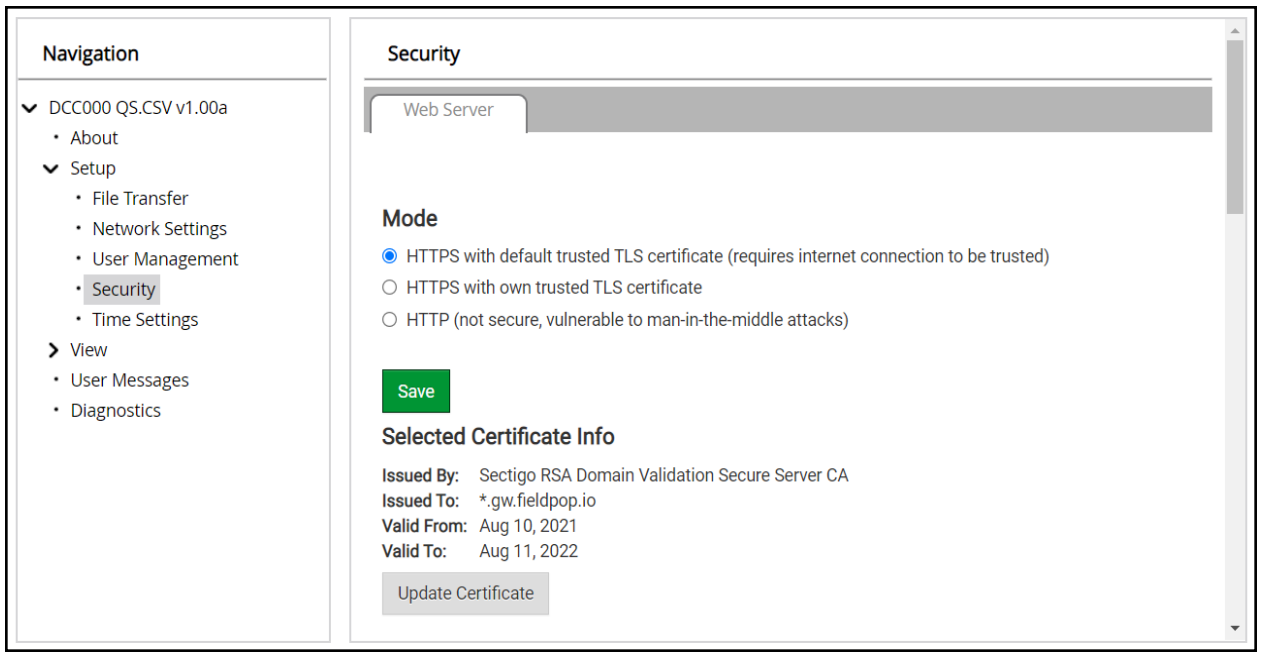


- Click the Mode desired.
  - If HTTPS with own trusted TLS certificate is selected, follow instructions in **Section 6.2.1 HTTPS with Own Trusted TLS Certificate**
- Click the Save button.

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.

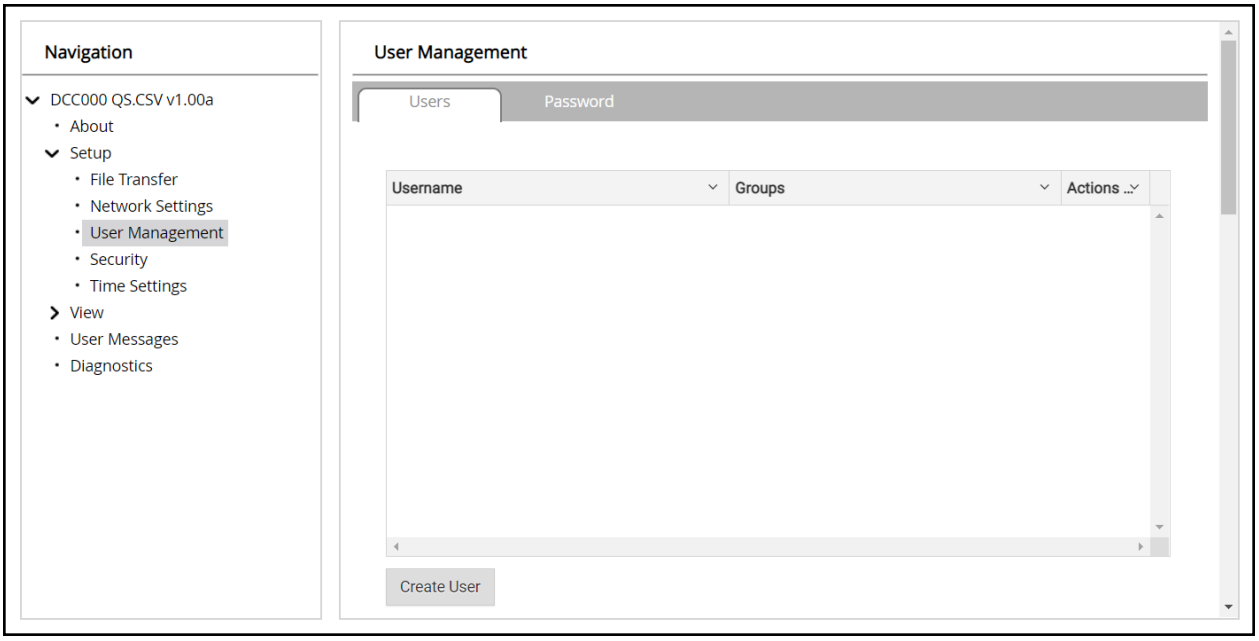
12.2 Change User Management Settings

- 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 FieldServer Next Gen Recovery document. If the default unique password is lost, then the unit must be mailed back to the factory.

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

- Check that the Users tab is selected.



User Types:

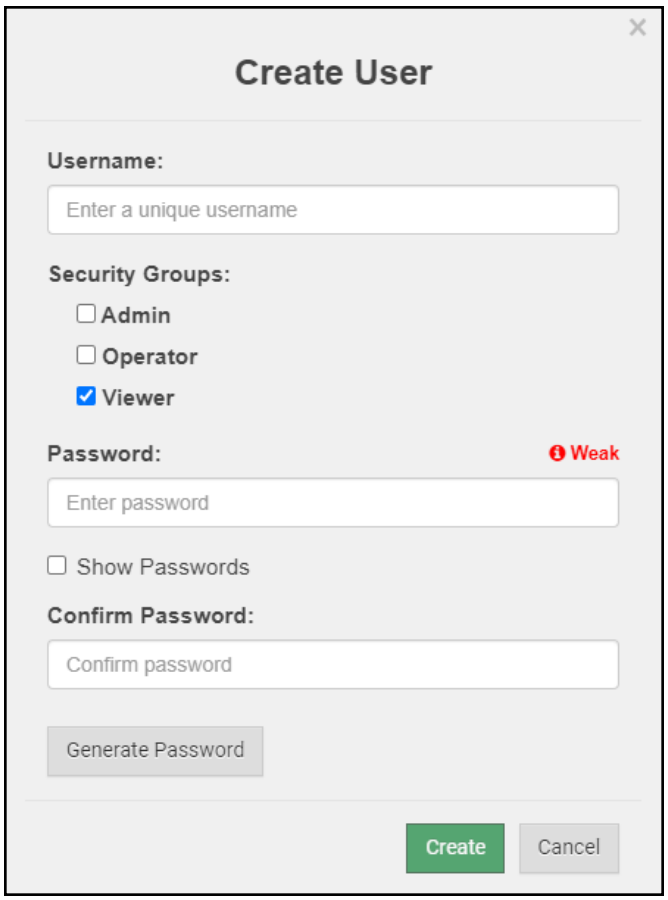
Admin – Can modify and view any settings on the FieldServer.

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

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

12.2.1 Create Users

- Click the Create User button.



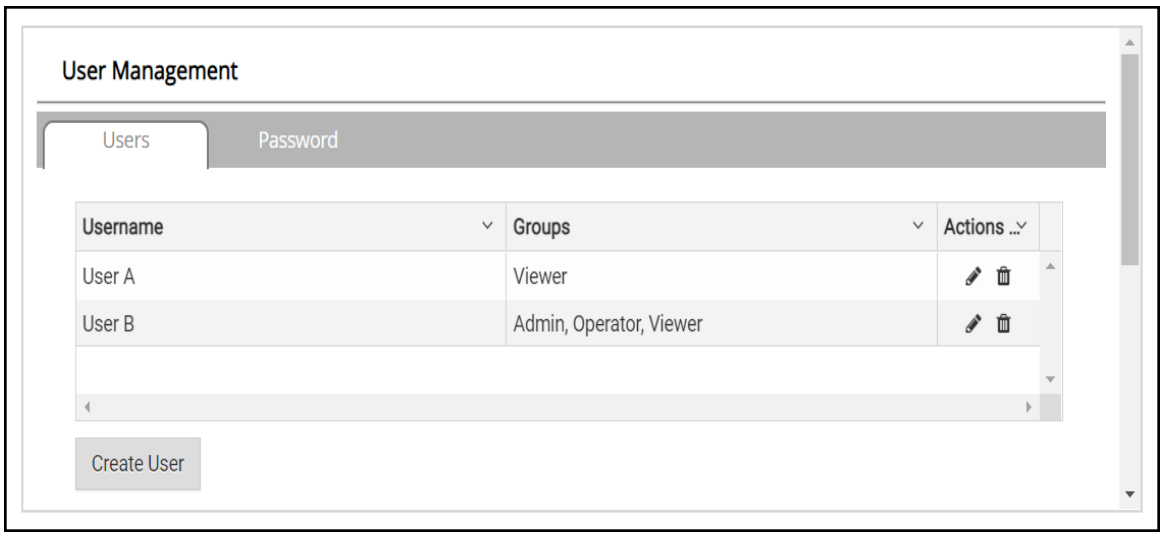
- Enter the new User fields: Name, Security Group and Password.
  - **User details are hashed and salted**

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.

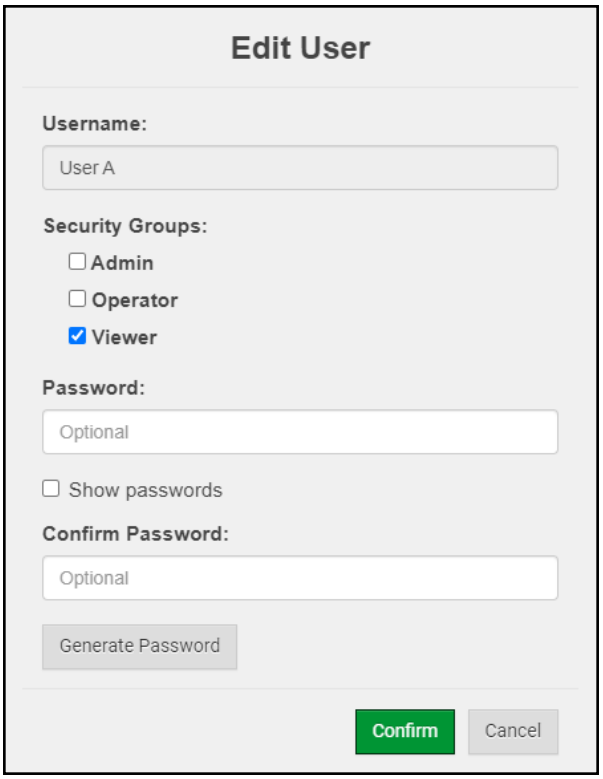
- Click the Create button.
- Once the Success message appears, click OK.

12.2.2 Edit Users

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



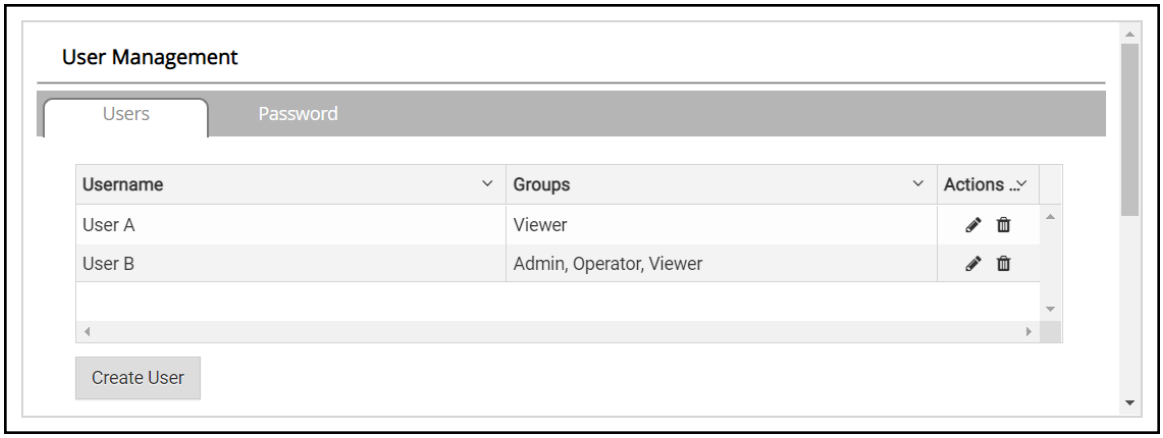
- Once the User Edit window opens, change the User Security Group and Password as needed.



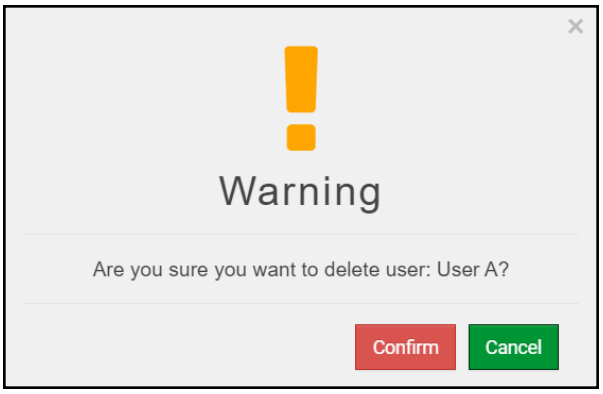
- Click Confirm.
- Once the Success message appears, click OK.

12.2.3 Delete Users

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

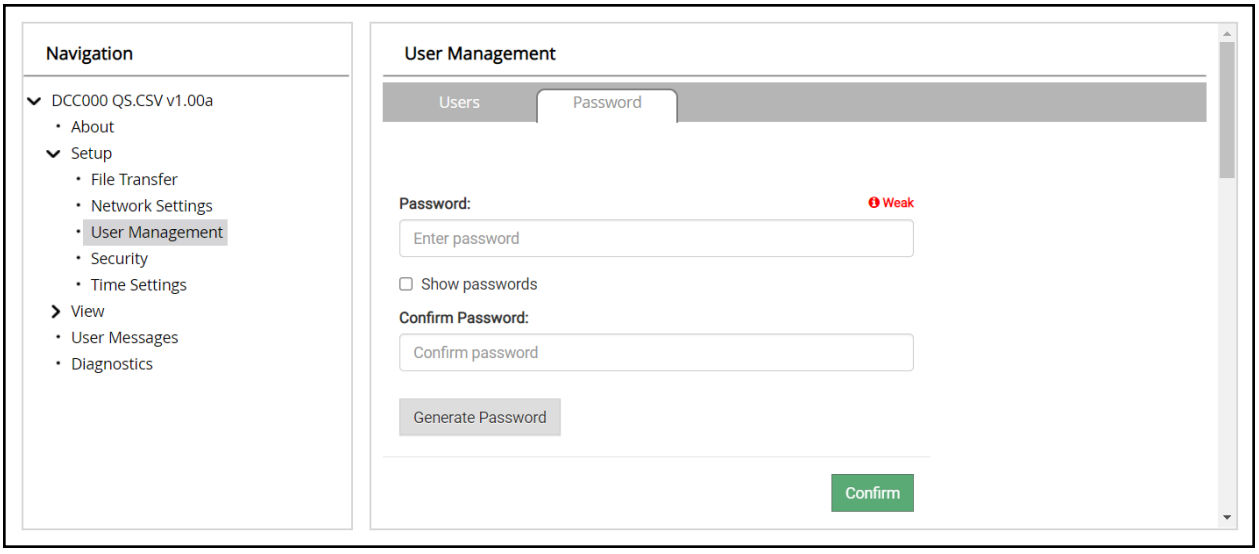


- When the warning message appears, click Confirm.



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-BAC2
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	*Input Voltage:* 12-24VDC or 24VAC *Max Power:* 3 Watts *Current draw:* 24VAC 0.125A 12-24VDC 0.25A @12VDC
Approvals	FCC Part 15, UL 60950-1 and CAN/CSA C22.2, 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 to158°F)
Humidity	10-95% RH non-condensing

NOTE: Specifications subject to change without notice.

12.4 Warnings

FCC Class B

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.

12.5 Compliance with EN IEC 62368-1

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

- 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.

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.