Gateway E2425800
Installation and Operating Manual

H2435500-

Revision: 2.O

Document No.: T18630

Print Spec: 10000005389 (EO)

LAARS® Heating Systems Company

Customer Service and Product Support: **800.900.9276 • Fax 800.559.1583**
Headquarters: **20 Industrial Way, Rochester, NH, USA 03867 • 603.335.6300 • Fax 603.335.3355**
9 Brigden Gate, Halton Hills, Ontario, Canada L7G 0A3 • 905.203.0600 • Fax 905.636.0666
www.Laars.com

Contents

Technical Support

Thank You for purchasing this Product.

Support Contact Information &
Customer Service:

603-335-6300

info@laars.com

www.laars.com

Quick Start Guide

1. Record the information about the unit. (**Section 2.1**)
2. Check that the Gateway and customer device COM settings match. (**Section 2.3**)
3. **If connecting to a serial device:**
   Connect the Gateway 3 pin RS-485 R1 port to the RS-485 network connected to each of the devices. (**Section 3.1)**
4. **If using a serial field protocol:**
   Connect the Gateway 3 pin RS-485 R2 port to the field protocol cabling. (**Section 3.2**)
5. Connect a PC to the Gateway via Ethernet cable. (**Section 4**)
6. Setup Web Server Security and login via web browser. (**Section 5**)
7. Configure the Gateway to connect to the local network. (**Section 6**)
8. Integrate the Gateway with the FieldServer Manager or opt out. (**Section 7**)
9. Use a web browser to access the Gateway Web Configurator page to select the profile of the device attached to the Gateway and enter any necessary device information. Once the device is selected, the Gateway automatically builds and loads the appropriate configuration. (**Section 8.3**)

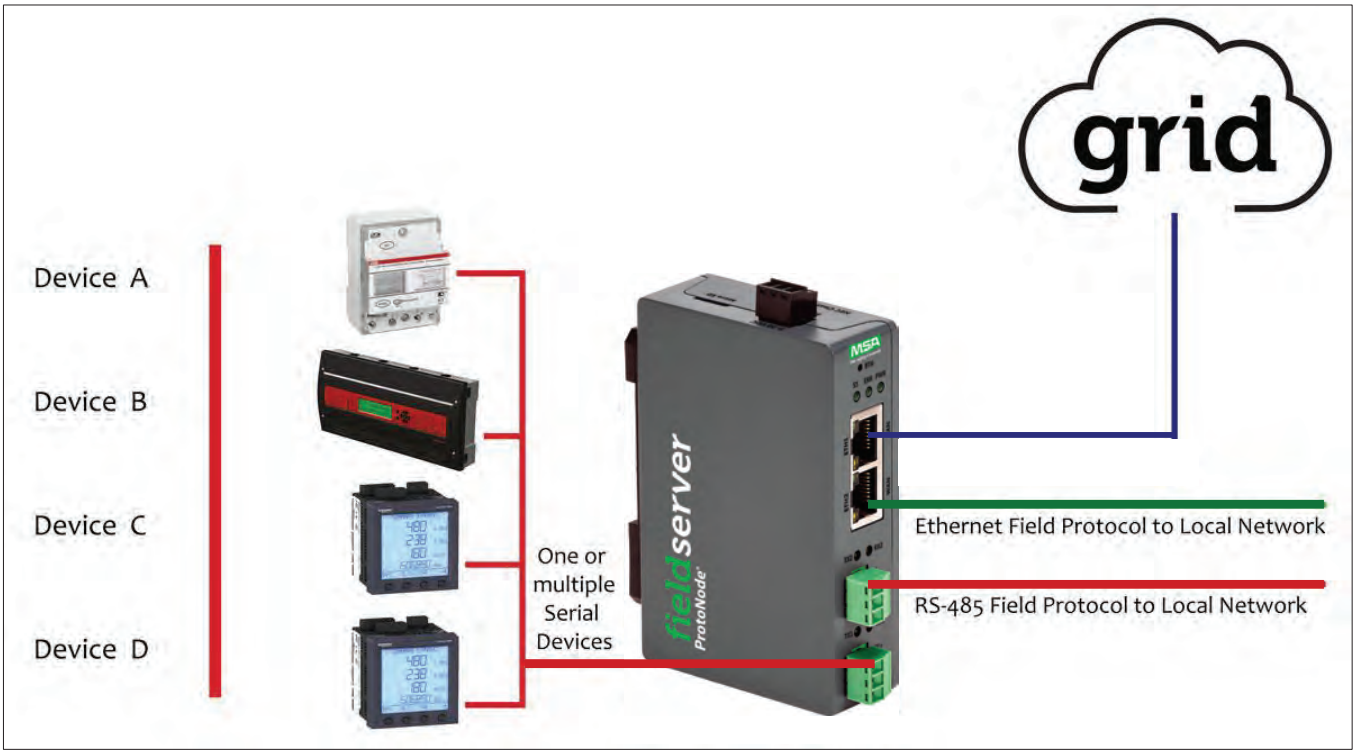
1 Introduction

1.1 About the Gateway

The Gateway wireless is an external, high performance building automation multi-protocol gateway that is preconfigured to automatically communicate between LAARS' devices (hereafter simply called "device") connected to the Gateway and automatically configures them for BACnet/IP, BACnet MS/TP, Modbus TCP/IP and Modbus RTU

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

E2425800 Connectivity Diagram:



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

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

For more information on the FieldServer Manager, see the MSA Grid - FieldServer Manager Start-up Guide.

2 Set Up for Gateway

2.1 Record Identification Data

Each Gateway has a unique part numbe. This number should be recorded, as it may be required for technical support. The numbers are as follows:

Model	Part Number
Gateway	E2425800

Figure 1: Gateway part numbers

- Each Gateway has the following 4 ports: RS -485 + Ethernet x2 + RS-485/RS-232

2.2 Point Count Capacity and Registers per Device

The total number of registers presented to the device(s) attached to the Gateway cannot exceed 1500.

Devices	Point Count Per Device
E-Therm	110
Tank System Conrol	130

Figure 3: Points per Device

2.3 Configuring Device Communications

2.3.1 Confirm the Device and Gateway COM Settings Match

- **Any connected serial devices MUST have the same baud rate, data bits, stop bits, and parity settings as the Gateway.**
- **Figure 4** specifies the device serial port settings required to communicate with the Gateway.

Port Setting	Device
Protocol	Modbus RTU
Baud Rate	38400
Parity	None
Data Bits	8
Stop Bits	1

Figure 4: COM Settings

2.3.2 Set Node-ID for Any Device Attached to the Gateway

- Set Node-ID for any device attached to Gateway. The Node-ID needs to be uniquely assigned between 1 and 255.
- Document the Node-ID that is assigned. The Node-ID assigned is used for deriving the Device Instance for BACnet/IP and BACnet MS/TP. (**Section 8.3**)

NOTE: The Metasys N2 and Modbus TCP/IP field protocol Node-ID is automatically set to be the same value as the Node-ID of the device.

3 Interfacing Gateway to Devices

3.1 Device Connections to Gateway

The Gateway has a 3-pin Phoenix connector for connecting RS-485 devices on the R1 port.

NOTE: Use standard grounding principles for RS-485 GND.

Device Pins	Gateway Pin Label	Pin Assignment
RS-485 +	TX +	RS-485 +
RS-485 -	RX -	RS-485 -
RS-485 GND	GND	RS-485 GND

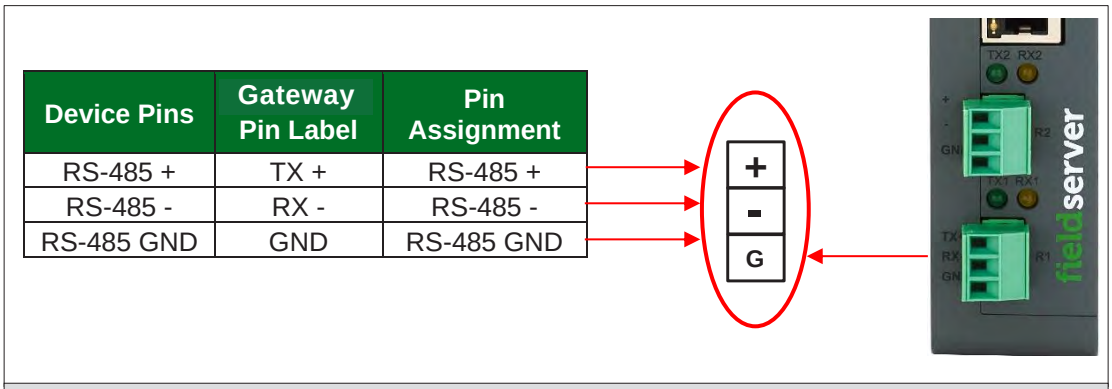


Figure 5: RS-485 Connections from Devices to the ProtoNode

3.2 Wiring Field Port to RS-485 Serial Network

- Connect the RS-485 network wires to the 3-pin RS-485 connector on the R2 port. (**Figure 6**)
  - Use standard grounding principles for RS-485 GND
- See **Section 4** for information on connecting to an Ethernet network.

BMS Wiring	ProtoNode Pin Label	Pin Assignment
RS-485 +	+	RS-485 +
RS-485 -	-	RS-485 -
-	GND	RS-485 GND

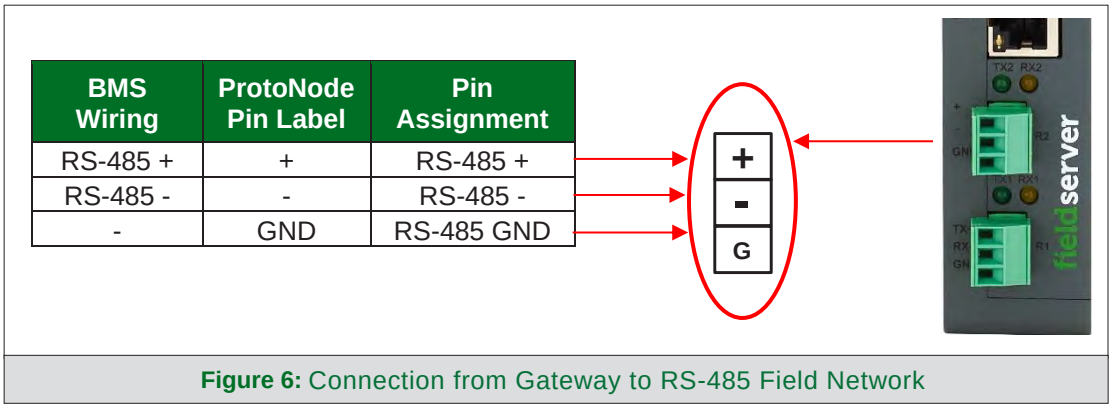
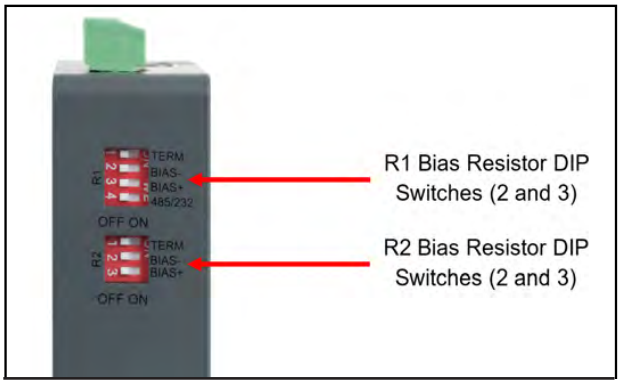


Figure 6: Connection from Gateway to RS-485 Field Network

3.3 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 Gateways can be put on the network without running into the bias resistor limit which is < 500 ohms.

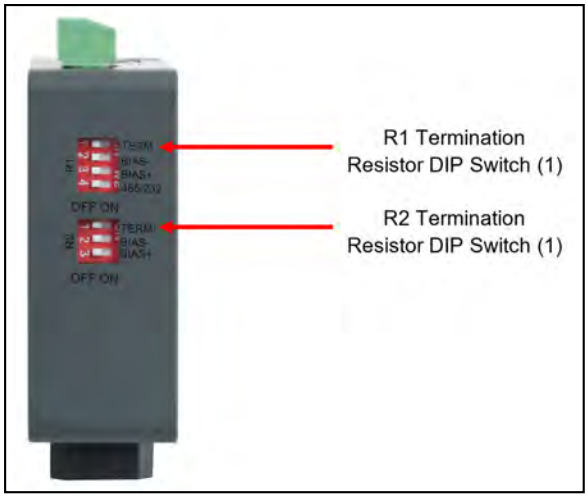
NOTE: See the Termination and Bias Resistance Enote for additional information.

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.

Interfacing Gateway to Devices (continued)

3.4 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.

3.5 Power Up the Gateway

NOTE: The Gateway E2425800 is pre-installed to the Heat Pump.

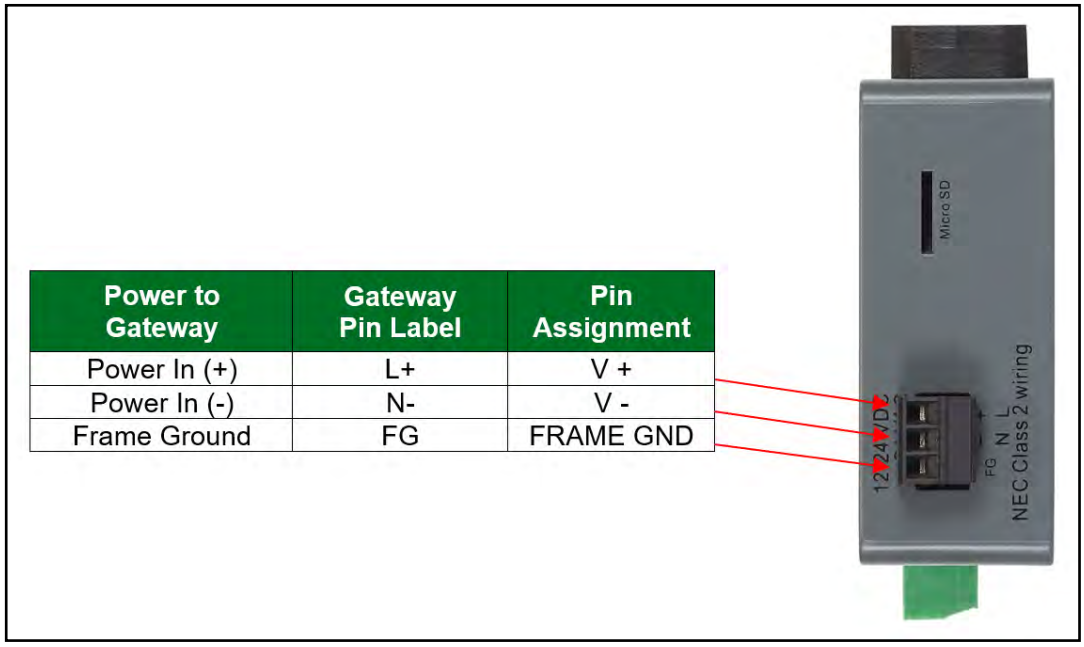
Section 4 of this manual is retained as a reference to the Power Requirements and Current Draw Type of the Heat Pump.

Check power requirements in the table below:

Power Requirement for I Gateway External Gateway		
	Current Draw Type	
Gateway Family	12VDC	24VDC/AC
FPC – N64 (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.		

- 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 can be used to power FieldServers

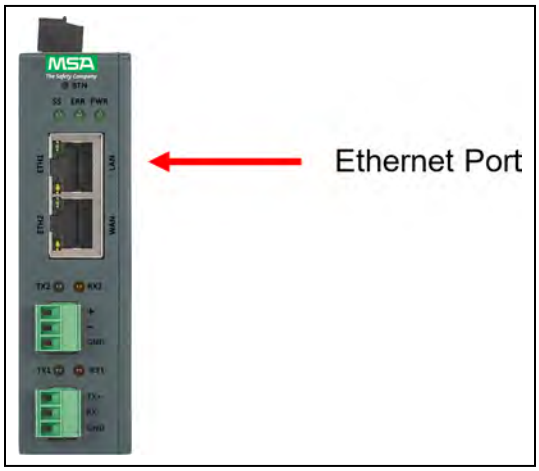


Power to Gateway	Gateway Pin Label	Pin Assignment
Power In (+)	L+	V +
Power In (-)	N-	V -
Frame Ground	FG	FRAME GND

4 Connect the PC to the Gateway

4.1 Connecting to the Gateway via Ethernet

Connect a Cat-5 Ethernet cable (straight through or cross-over) between the local PC and Gateway ETH1 (LAN Port).

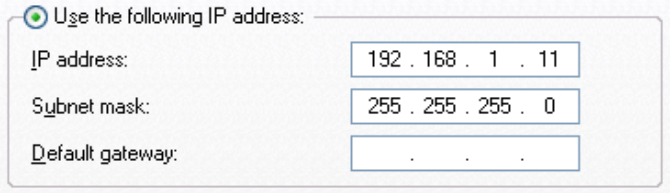


4.1.1 Changing the Subnet of the Connected PC

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

For Windows 10:

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



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

4.2 Navigate to the Login Page

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

NOTE: If the IP Address of the Gateway has been changed, the IP Address can be discovered using the FS Toolbox utility. See Section 9.1 Lost or Incorrect IP Address for instructions.

5 Setup Web Server Security

Navigate to the IP Address of the Gateway on the local PC by opening a web browser and entering the IP Address of the ProtoNode; the default Ethernet address is 192.168.1.24.

NOTE: If the IP Address of the Gateway has been changed, the assigned IP Address can be discovered using the FS Toolbox utility. See Section 9.1 for instructions.

5.1 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.

Figure 12: Web Server Security Window

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

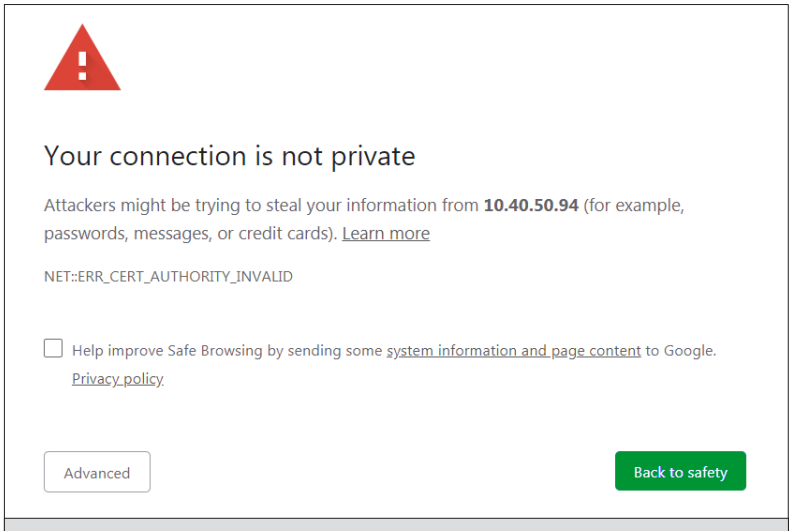


Figure 13: Connection Not Private Warning

Setup Web Server Security (continued)

- Additional text will expand below the warning, click the underlined text to go to the IP Address. In the **Figure 14** example this text is "Proceed to 10.40.50.94 (unsafe)".

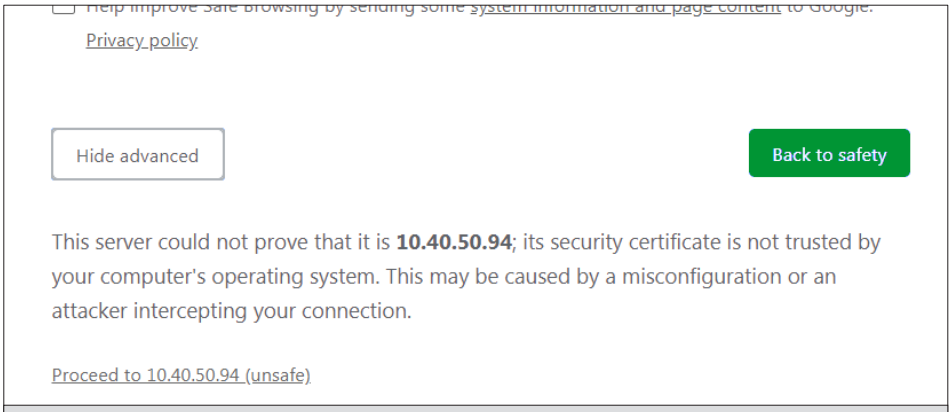


Figure 14: Warning Expanded Text

- 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.

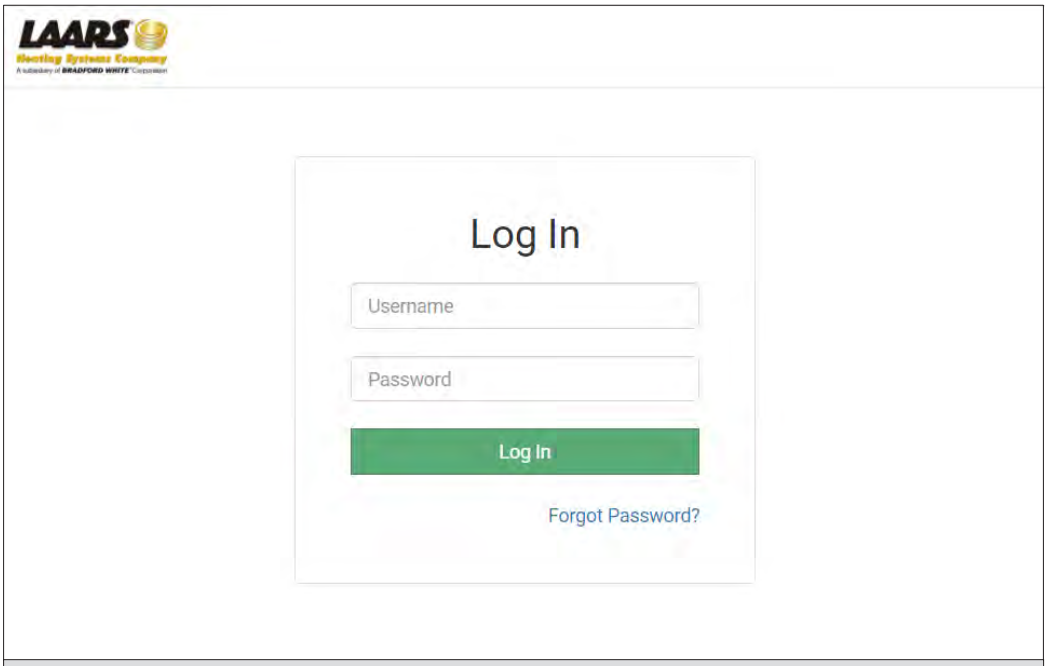


Figure 15: FieldServer Login

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 10.7.

5.2 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.

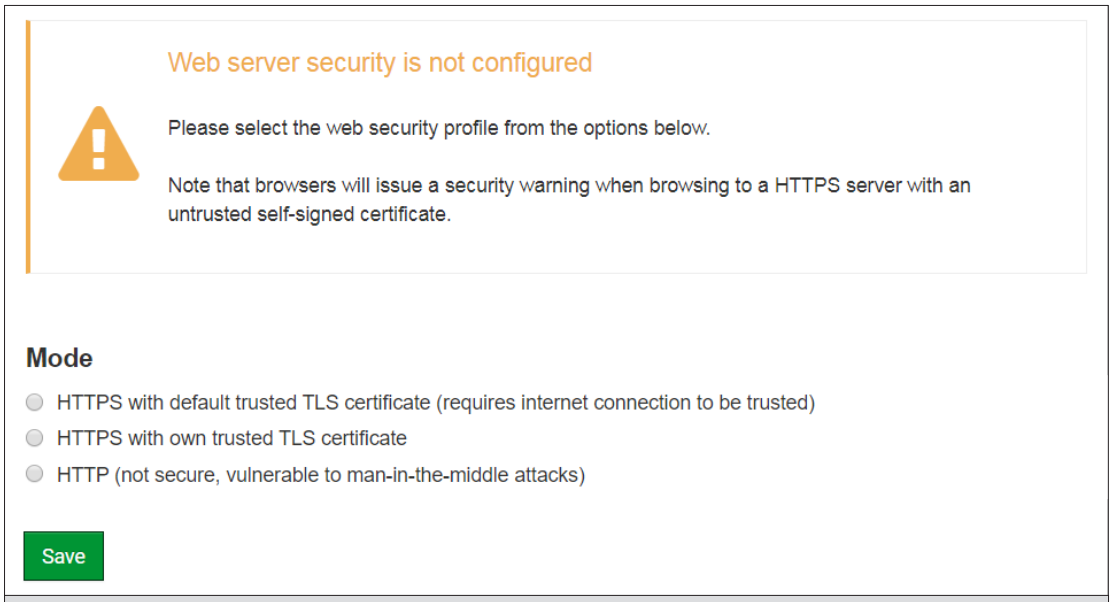


Figure 16: Security Mode Selection Screen

NOTE: Cookies are used for authentication.

NOTE: To change the web server security mode after initial setup, go to Section 10.1.

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

Setup Web Server Security (continued)

5.2.1 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.

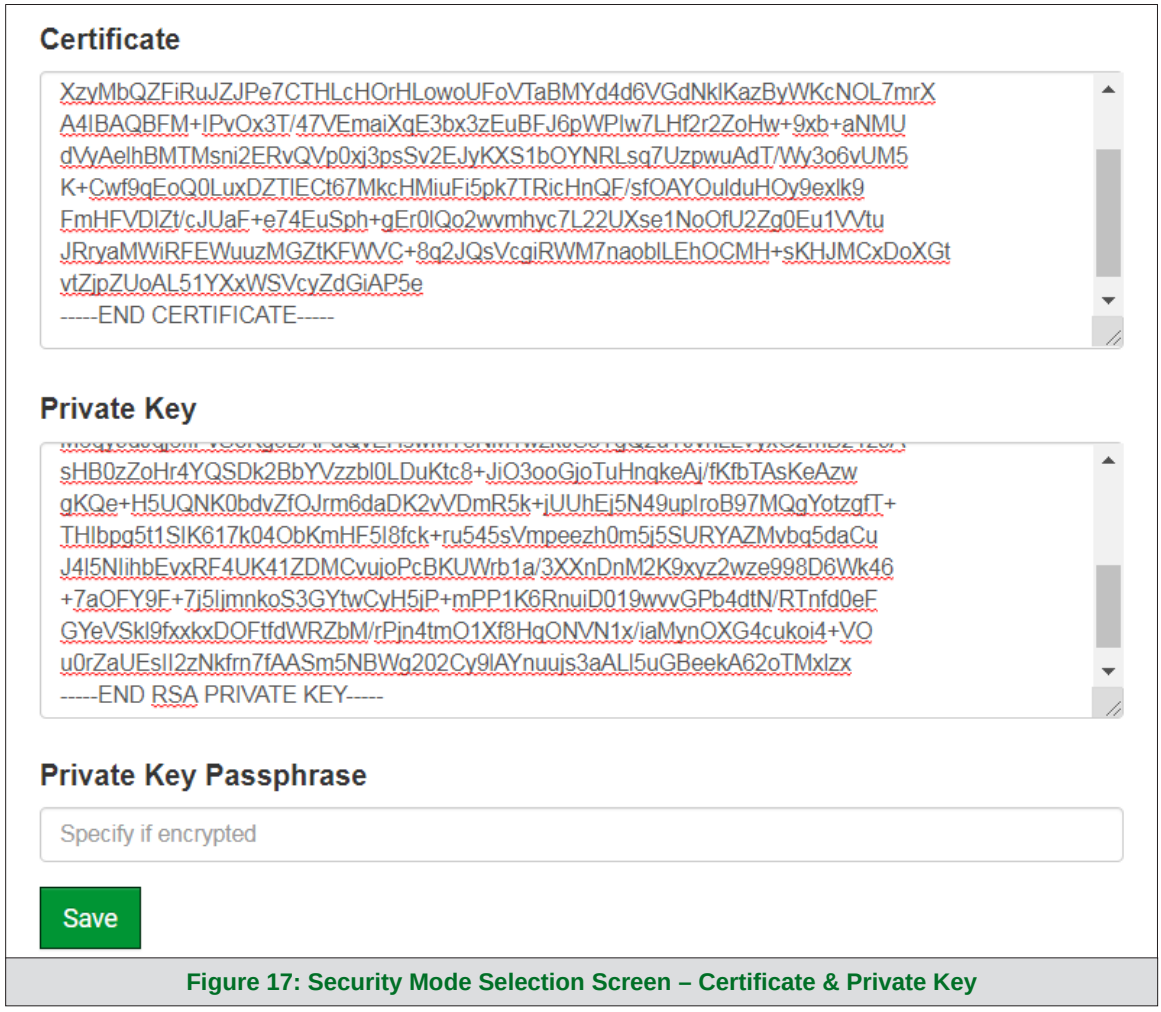


Figure 17: Security Mode Selection Screen – Certificate & Private Key

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

5.2.2 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.

6 Configure Network Settings

6.1 Navigate to the Settings

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

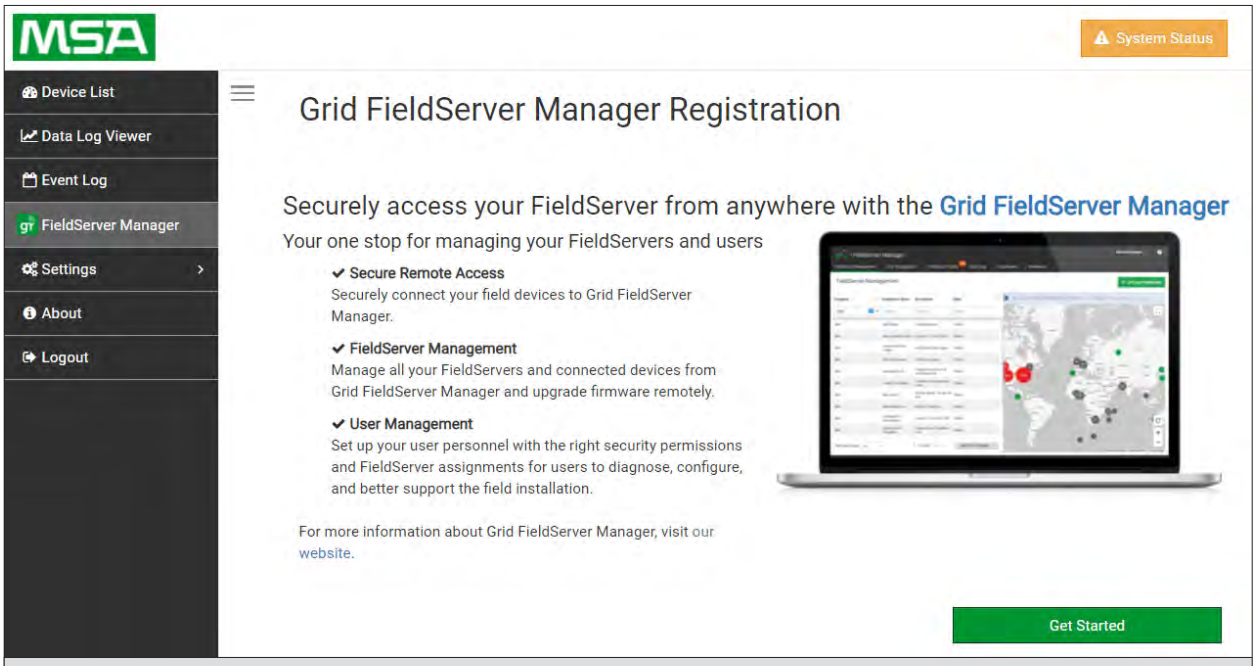


Figure 18: Generic Web App Landing Page

- Click the Network tab that appears to open the Network Settings page.

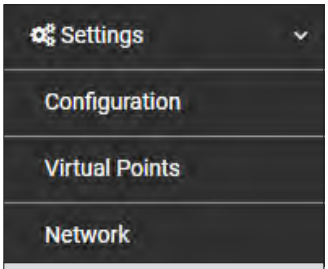


Figure 19: Settings Tabs

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

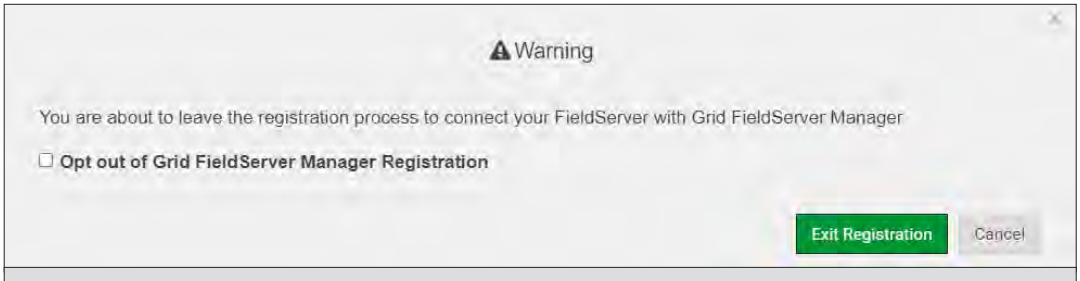


Figure 20: Registration Warning Window

Configure Network Settings (continued)

6.2 Change the Gateway IP Address

The IP Settings section updates the wired network configuration. To update, 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 connected to a router, set the Gateway to the same IP Address as the router.

- Click the Save button to activate the new settings.

NOTE: If the webpage was open in a browser, the browser will need to be pointed to the new IP Address before the webpage will be accessible again.

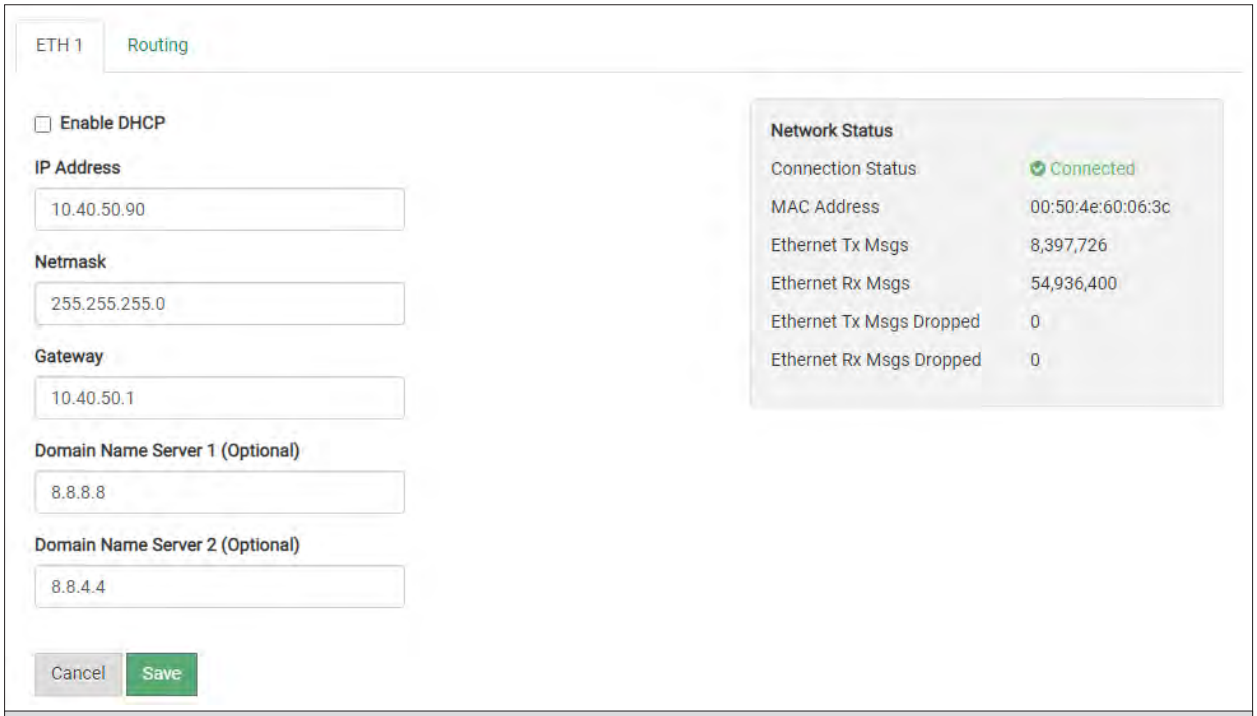


Figure 21: ETH 1 Port Network Settings

6.3 Routing

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.

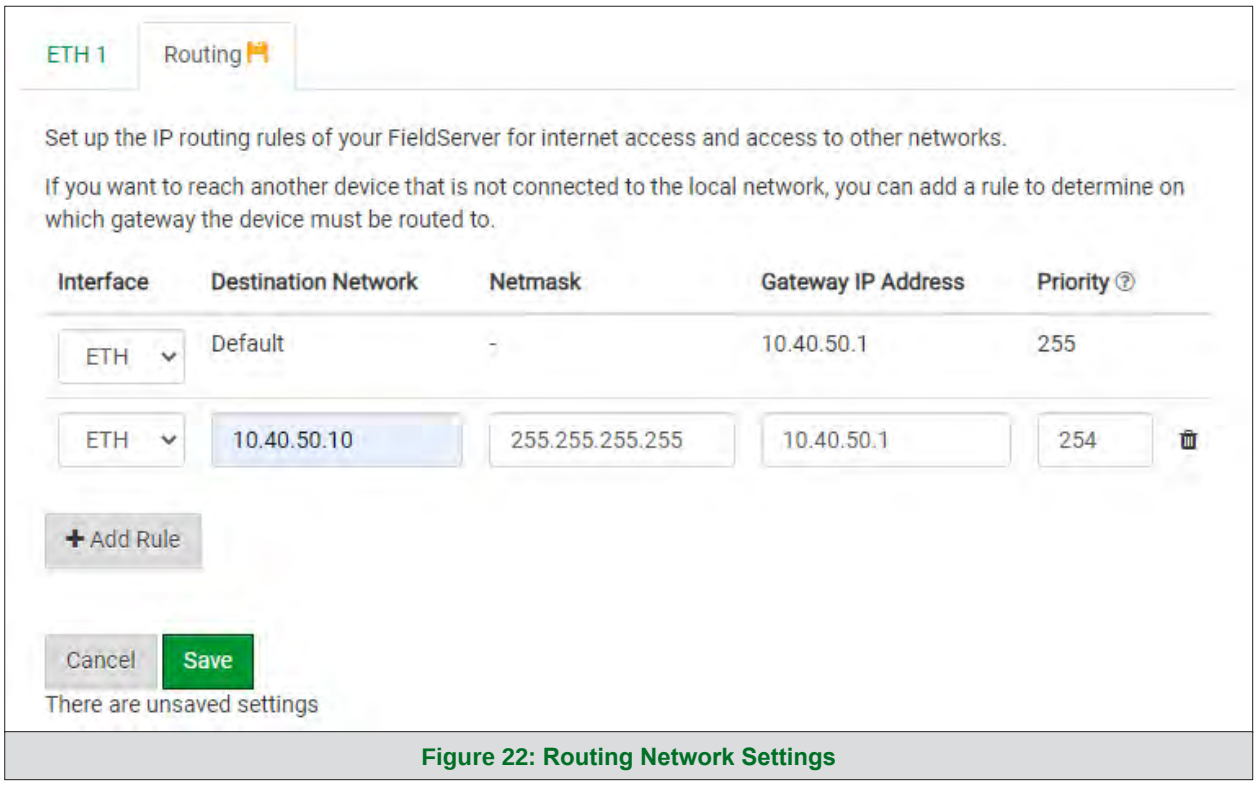


Figure 22: Routing Network Settings

7 FieldServer Manager User Setup, Registration and Login

The Grid is MSA Safety's device cloud solution for IIoT. Integration with the MSA Grid – FieldServer Manager enables 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 Start-up Guide.

7.1 Choose Whether to Integrate the FieldServer Manager

When first logging onto the Gateway, the Web App will open on the Grid FieldServer Manager page.

NOTE: If a warning message appears instead, go to Section 10.8 to resolve the connection issue.

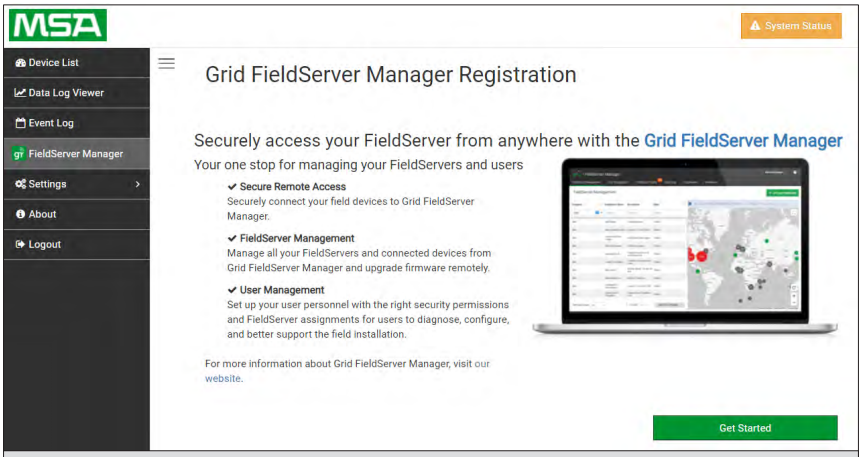


Figure 23: Generic Web App Page – First Login

- Either go through the FieldServer Manager setup to integrate cloud functionality to the FieldServer or optout of FieldServer Manager setup.
  - For FieldServer Manager setup, continue with instructions in the following sections
  - To opt out, click on a tab other than the Grid FieldServer Manger tab, click the checkbox next to "Opt out of Grid FieldServer Manager Registration" in the Warning window that appears and click the Exit Registration button (skip to **Section 8** to continue FieldServer configuration)
  - To ignore setup until the next time the FieldServer Web App is opened, click a tab other than Grid FieldServer Manager and then click the Exit Registration button with the "Opt out" checkbox unchecked (skip to **Section 8** to continue FieldServer configuration)

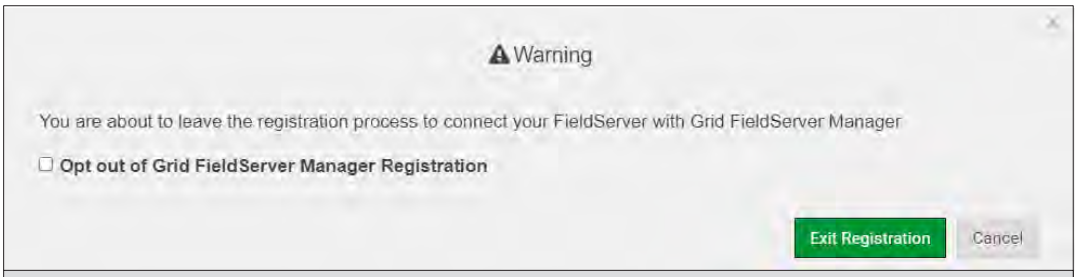


Figure 24: FieldServer Manager Opt Out Warning Window

NOTE: If FieldServer Manager integration with the Gateway is not desired, skip to Section 8 to continue gateway setup. If user setup is already complete go to Section 7.3.

7.2 User Setup

Before the Gateway can be connected to the FieldServer Manager, a user account must be created. Request an invitation to the FieldServer Manager from the manufacturer's support team and follow the instructions below to set up login details:

- The "Welcome to the MSA Grid – FieldServer Manager" email will appear as shown below.

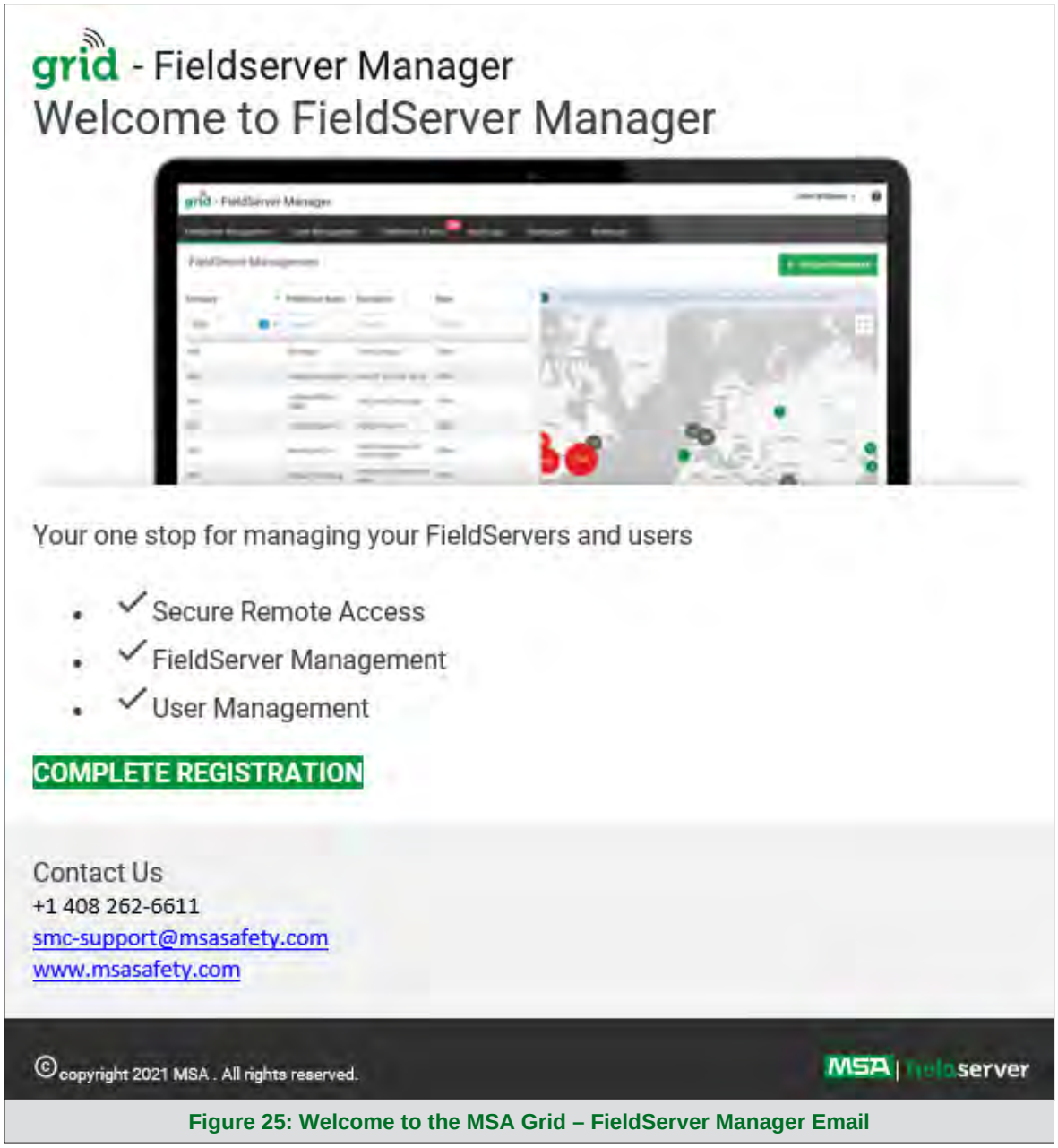


Figure 25: Welcome to the MSA Grid – FieldServer Manager Email

NOTE: If no email was received, check the spam/junk folder for an email from notification@fieldpop.io. Contact the manufacturer's support team if no email is found.

FieldServer Manager User Setup (continued)

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

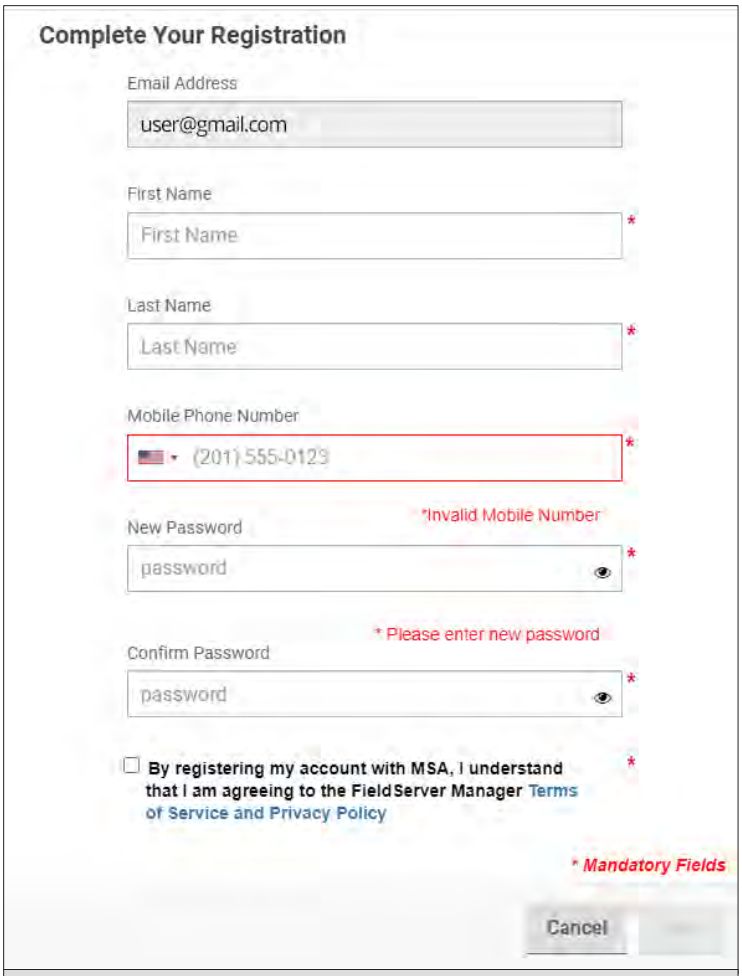


Figure 26: Setting User Details

- 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.

7.3 Registration Process

Once FieldServer Manager user credentials have been generated, the Gateway can be registered onto the server.

- When first logging onto the Gateway, the Web App will open on the Grid Fieldserver Manager page.

NOTE: If a warning message appears instead, go to Section 10.8 to resolve the connection issue.

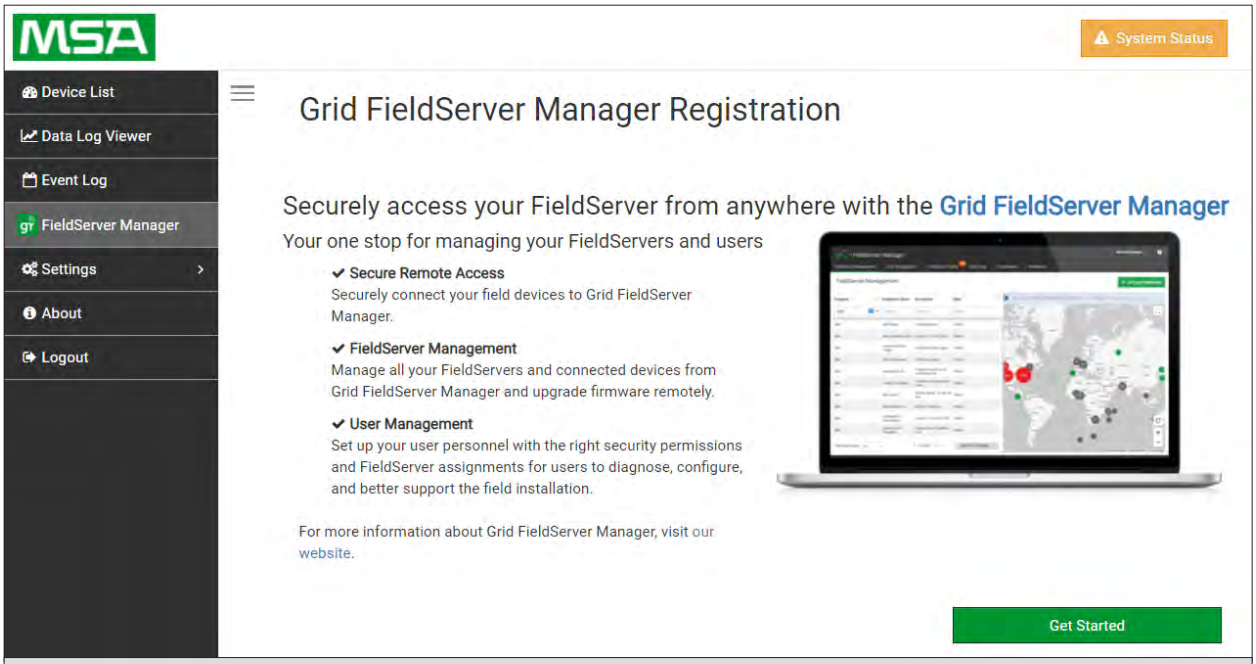


Figure 27: FieldServer Manager Registration Message

- Click Get Started to view the registration page.

NOTE: For information on the System Status button, go to Section 10.9.

FieldServer Manager User Setup (continued)

- To register, fill in the user details, site details, gateway details and account credentials.
  - Enter user details and click Next

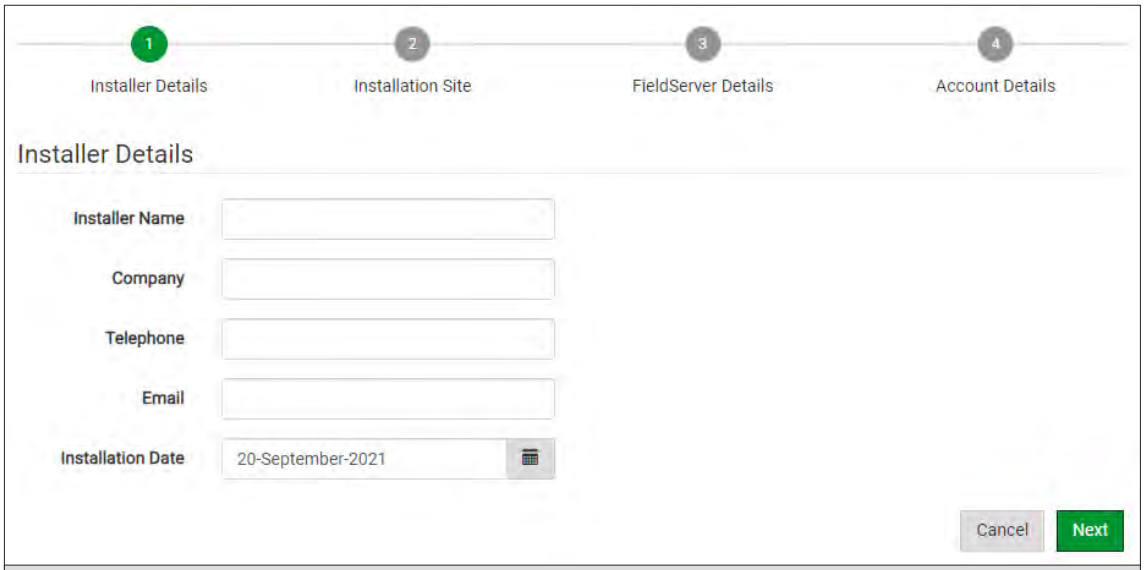


Figure 28: FieldServer Manager Registration – Installer Details

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

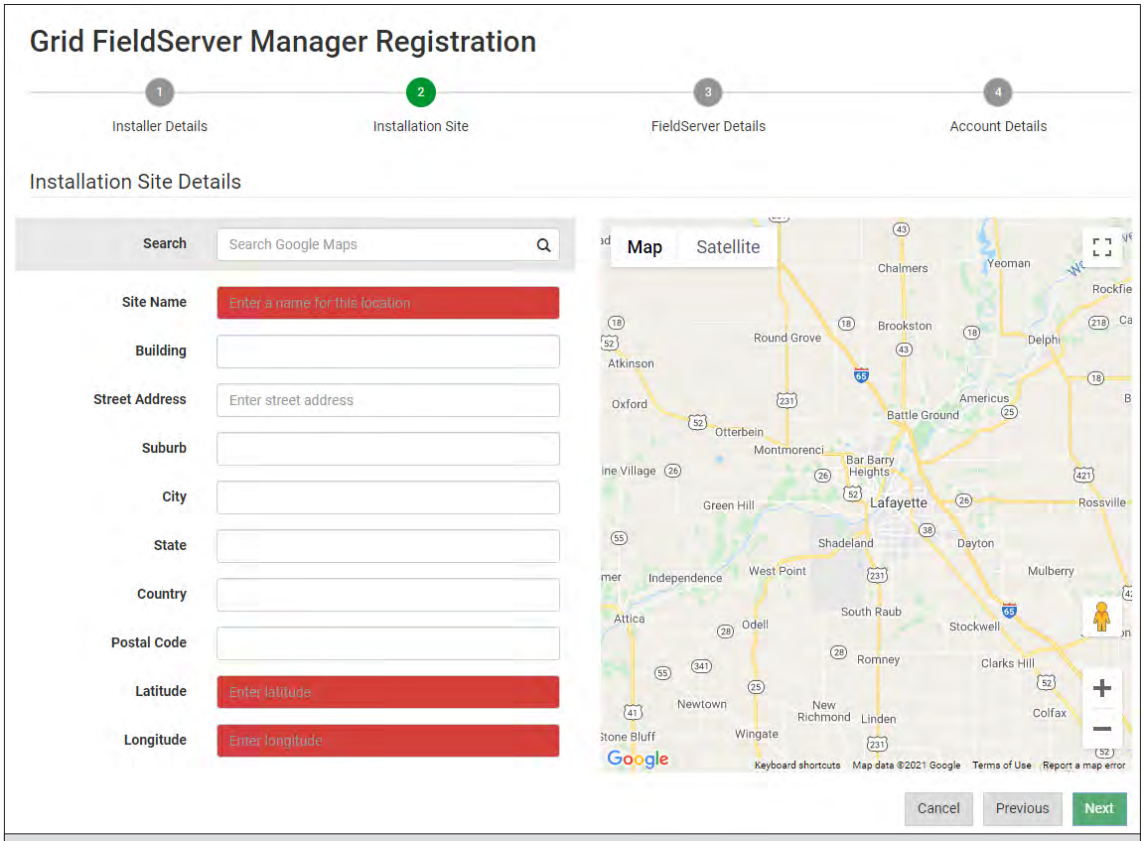


Figure 29: FieldServer Manager Registration – Site Details

- Enter Name and Description (required) then click Next

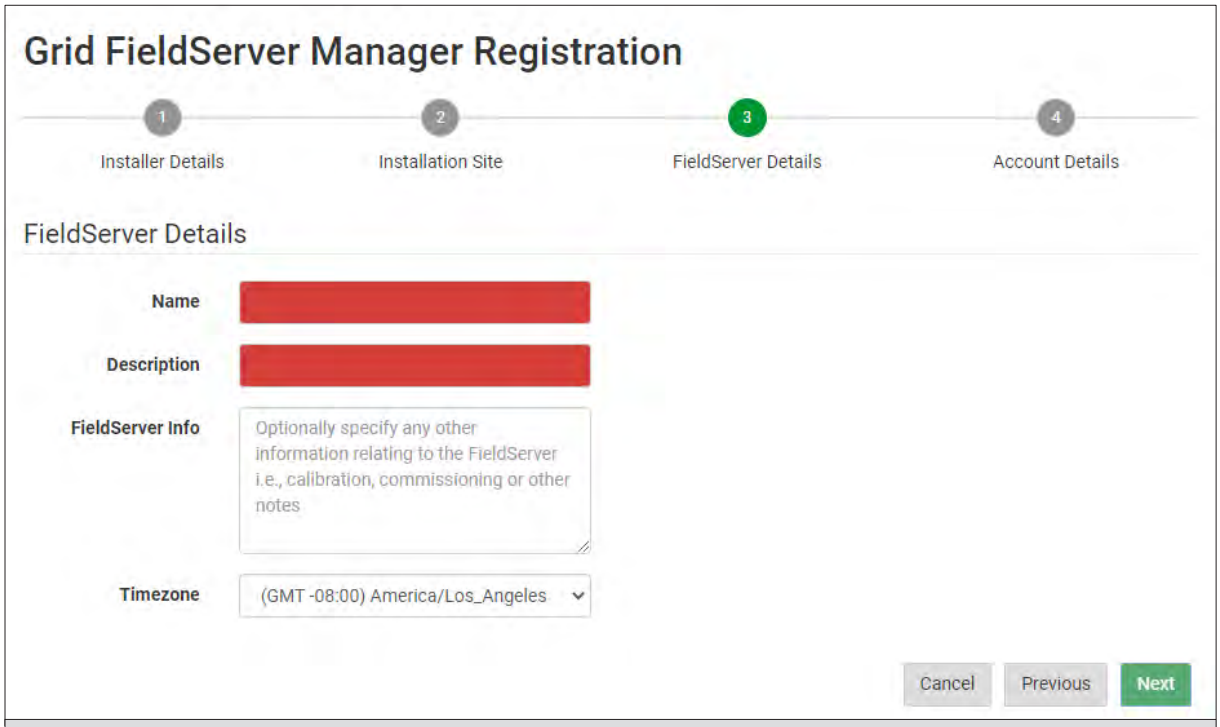


Figure 30: FieldServer Manager Registration – Gateway Details

- Enter user credentials and click Register Device

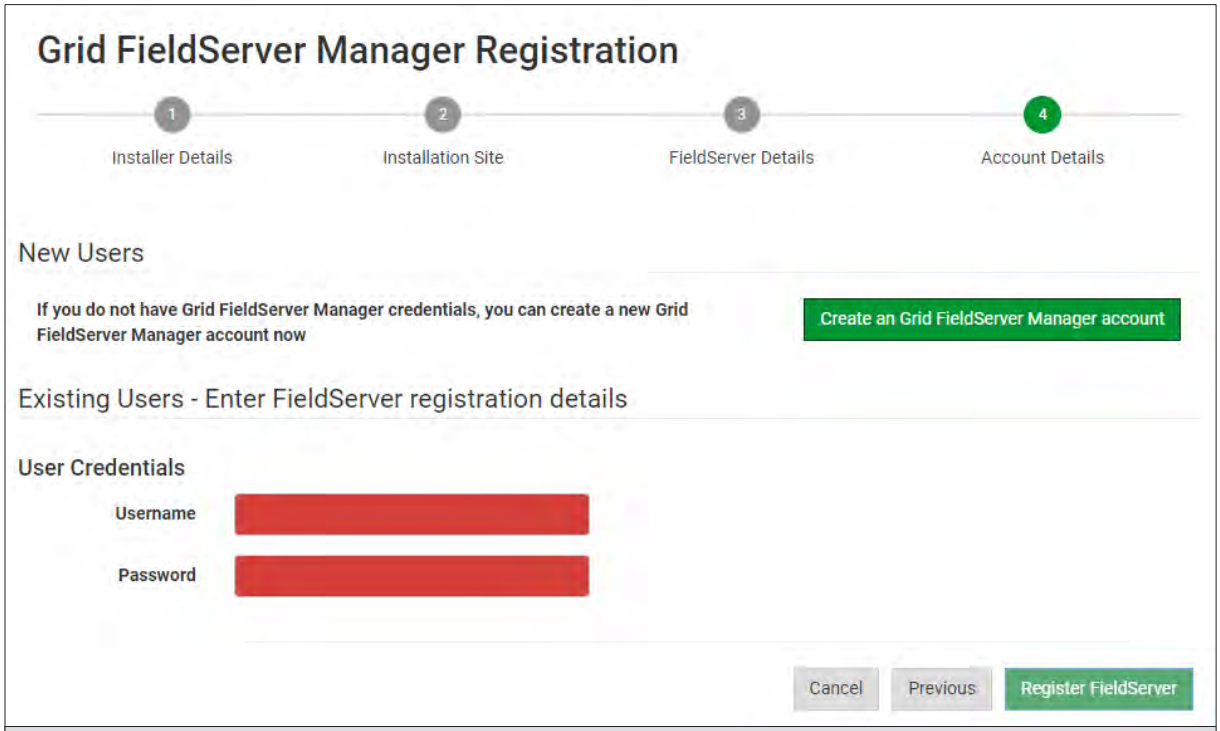


Figure 31: FieldServer Manager Registration – Account

FieldServer Manager User Setup (continued)

- Once the device has successfully been 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 Gateway.

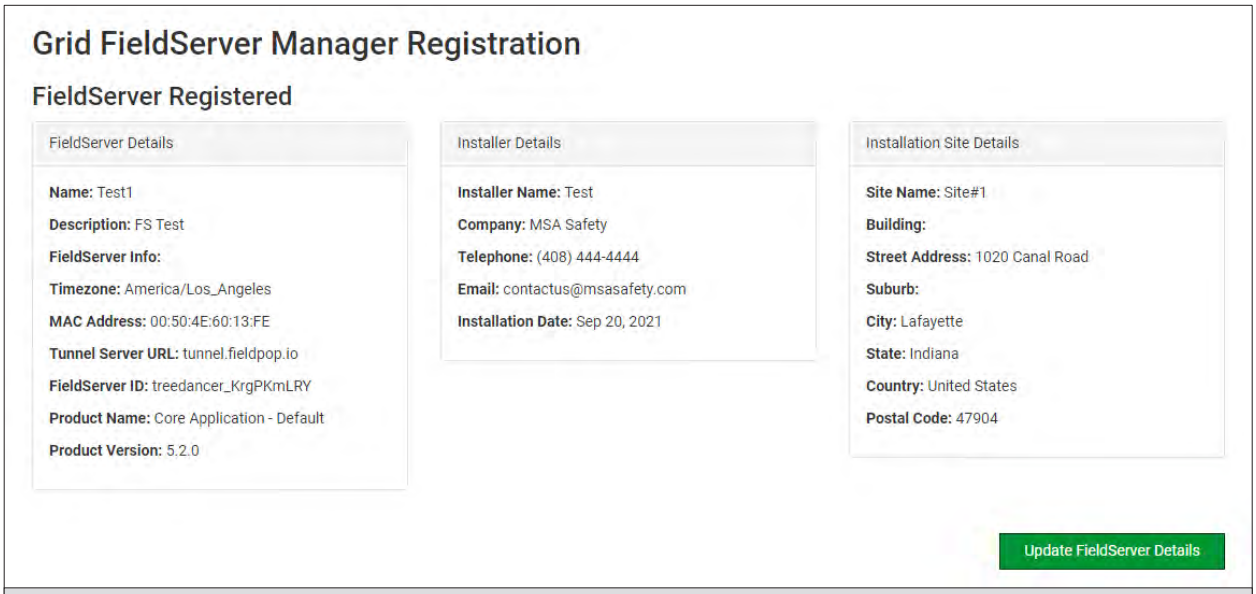


Figure 32: Device Registered for the FieldServer Manager

NOTE: Update these details at any time by going to the device's FS-GUI webpage, clicking the FieldServer Manager button and then clicking the Update FieldServer Details button.

7.4 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.

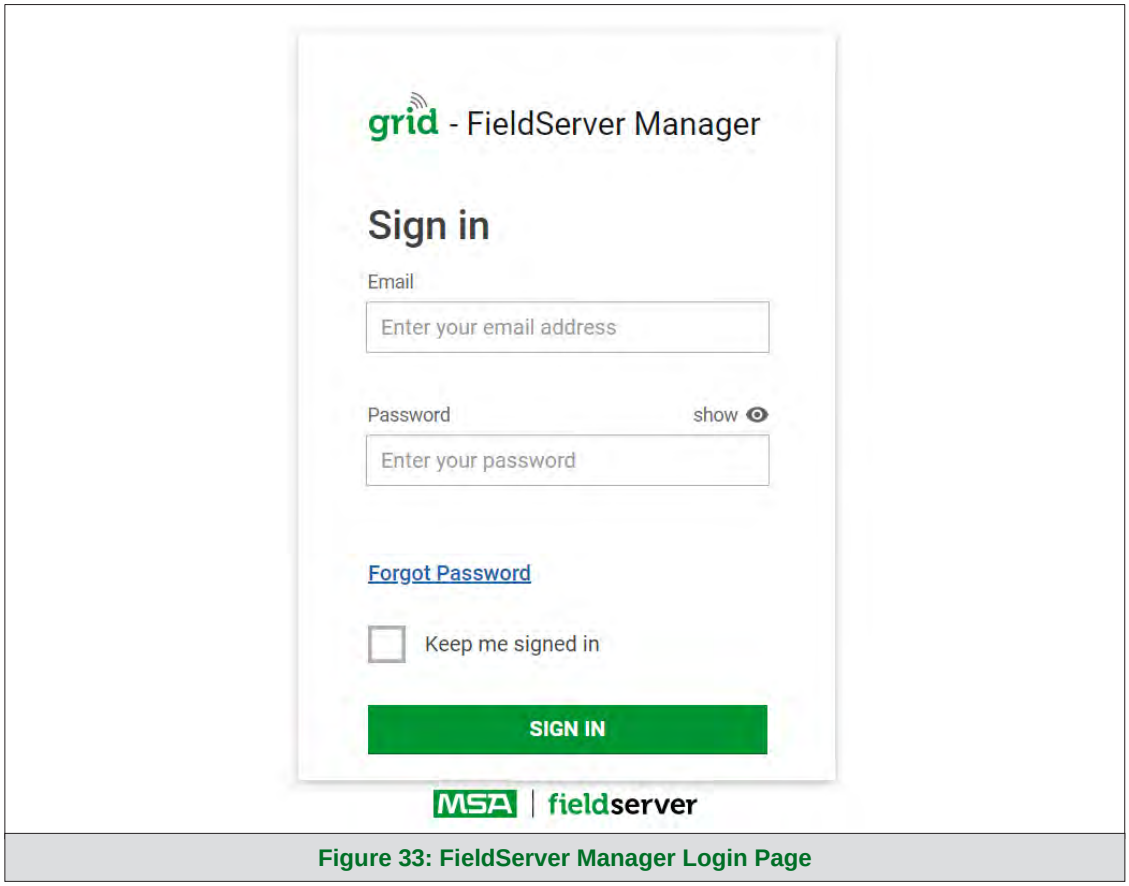


Figure 33: FieldServer Manager Login Page

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

FieldServer Manager User Setup (continued)

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

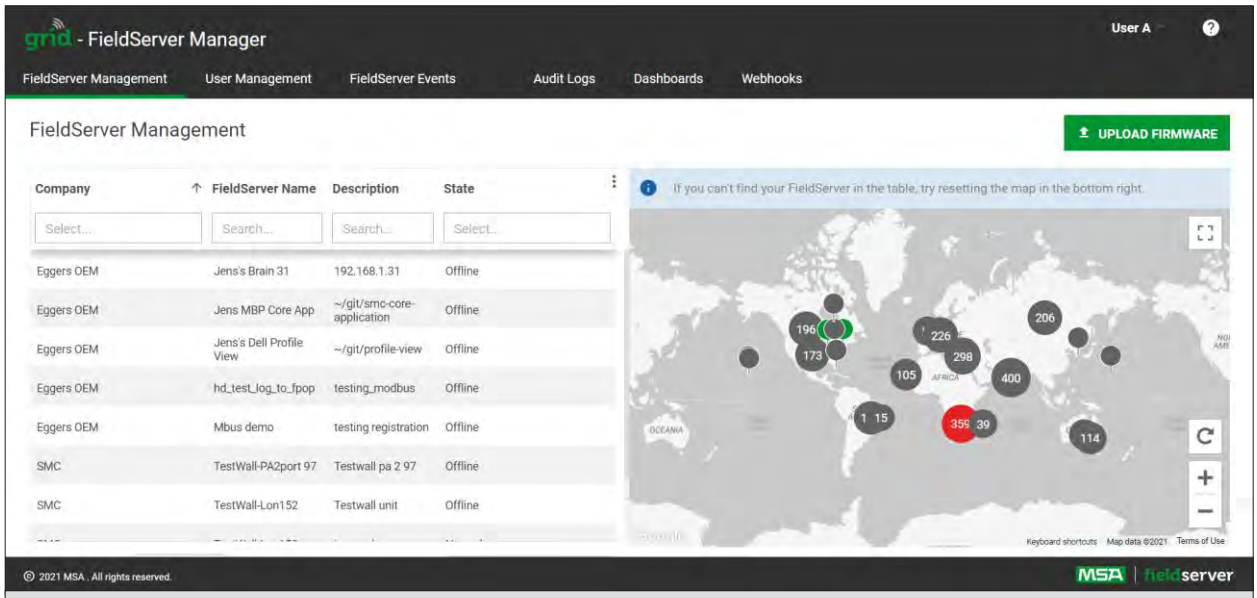


Figure 34: FieldServer Manager Landing Page

8 Configure the Gateway

8.1 Navigate to the Gateway Web Configurator

- From the Web App landing page (**Figure 35**), click the Settings tab and then click Configuration.

Figure 35: Web App Landing Page

NOTE: For information on the System Status button, go to Section 10.9.

- Then click the Profiles Configuration button to go to the Web Configurator page.

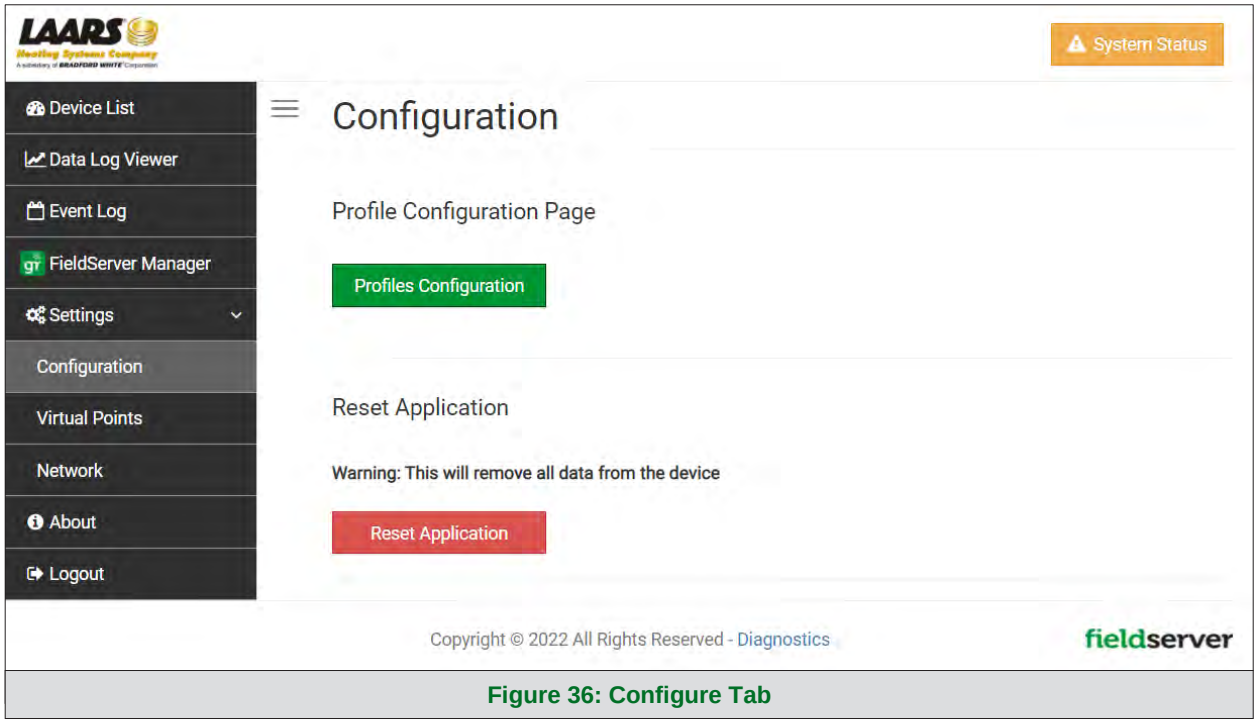


Figure 36: Configure Tab

NOTE: For Web App instructions to the System View, Data Log Viewer, Event Logger and Virtual Points functions, see the MSA Grid - FieldServer Manager Start-up Guide.

Configure the Gateway (continued)

8.2 Select Field Protocol and Set Configuration Parameters

- On the Web Configurator page, the first configuration parameter is the Protocol Selector.

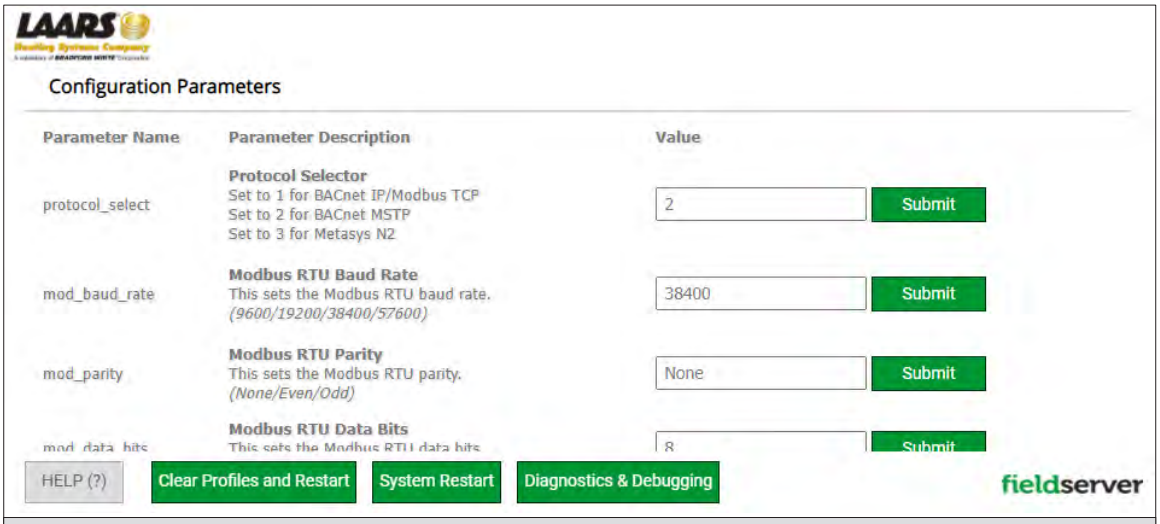


Figure 37: Web Configurator Showing Configuration Parameters

- Select the field protocol by entering the appropriate number into the Protocol Selector Value. Click the Submit button. Click the System Restart button to save the updated configuration.

NOTE: Protocol specific parameters are only visible when the associated protocol is selected.

- Ensure that all parameters are entered for successful operation of the gateway. Find the legal value options for each parameter under the Parameter Description in parentheses.

NOTE: If multiple devices are connected to the Gateway, set the BACnet Virtual Server Nodes field to "Yes"; otherwise leave the field on the default "No" setting.

8.3 Setting Gateway Active Profiles

- In the Web Configurator, the Active Profiles are shown below the configuration parameters. The Active Profiles section lists the currently active device profiles, including previous Web Configurator additions. This list is empty for new installations, or after clearing all configurations. (**Figure 38**)

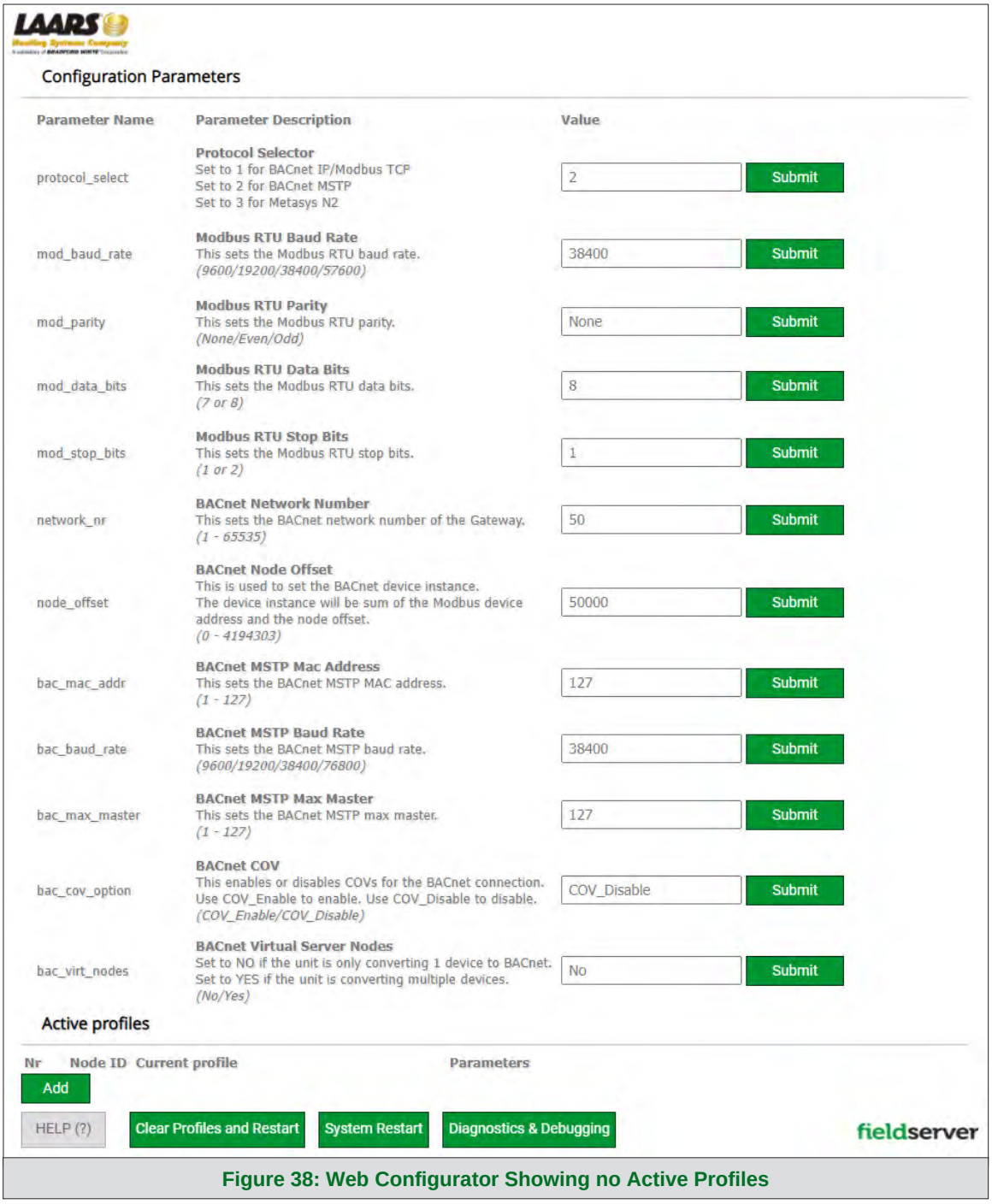


Figure 38: Web Configurator Showing no Active Profiles

Configure the Gateway (continued)

- To add an active profile to support a device, click the Add button under the Active Profiles heading. This will present a profile drop-down menu underneath the Current profile column.
- Once the Profile for the device has been selected from the drop-down list, enter the value of the device's Node-ID which was assigned in **Section 2.3.2**.
- Then press the "Submit" button to add the Profile to the list of devices to be configured.
- Repeat this process until all the devices have been added.
- Completed additions are listed under "Active profiles" as shown in **Figure 39**.

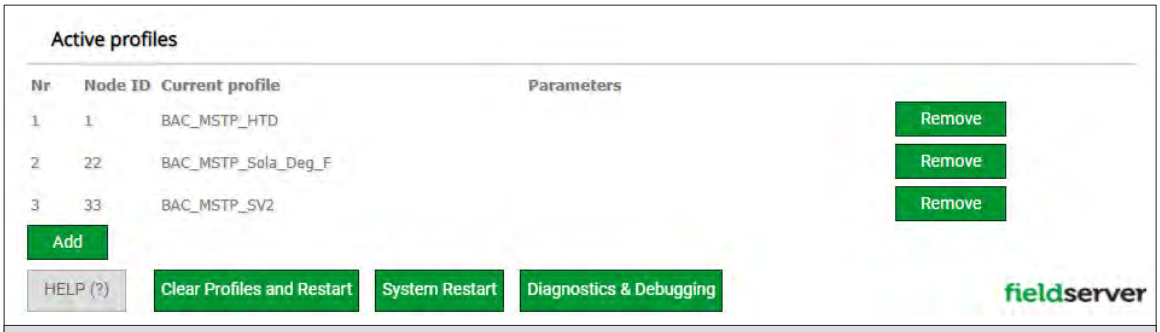


Figure 39: Web Configurator Showing Active Profile Additions

8.5 Verify Device Communications

- **Check that the port R1 TX1 and RX1 LEDs are rapidly flashing**. See **Section 9.4** for additional LED information and images.
- Confirm the software shows good communications without errors (**Section 9.2**).

8.4 BACnet: Setting Node_Offset to Assign Specific Device Instances

- Follow the steps outlined in **Section 5.1** to access the Gateway Web Configurator.
- Node_Offset field shows the current value (default = 50,000).
  - The values allowed for a BACnet Device Instance can range from 1 to 4,194,303
- To assign a specific Device Instance (or range); change the Node_Offset value as needed using the calculation below:

  Device Instance (desired) = Node_Offset + Node_ID

  For example, if the desired Device Instance for the device 1 is 50,001 and the following is true:
  - Device 1 has a Node-ID of 1
  - Device 2 has a Node-ID of 22
  - Device 3 has a Node-ID of 33

  Then plug the device 1's information into the formula to find the desired Node_Offset:

  50,001 = Node_Offset + 1

  ➢ **50,000 = Node_Offset**

Once the Node_Offset value is input, it will be applied as shown below:

- Device 1 Instance = 50,000 + Node_ID = 50,000 + 1 = 50,001
- Device 2 Instance = 50,000 + Node_ID = 50,000 + 22 = 50,022
- Device 3 Instance = 50,000 + Node_ID = 50,000 + 33 = 50,033

- Click “Submit” once the desired value is entered.

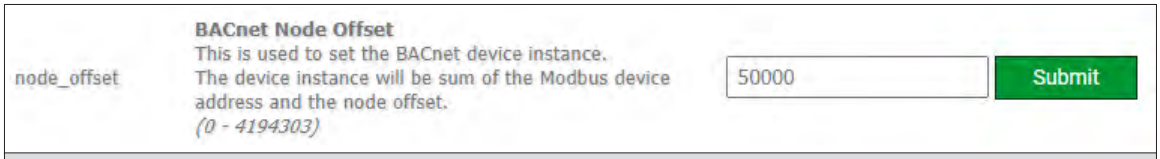


Figure 40: Web Configurator Node Offset Field

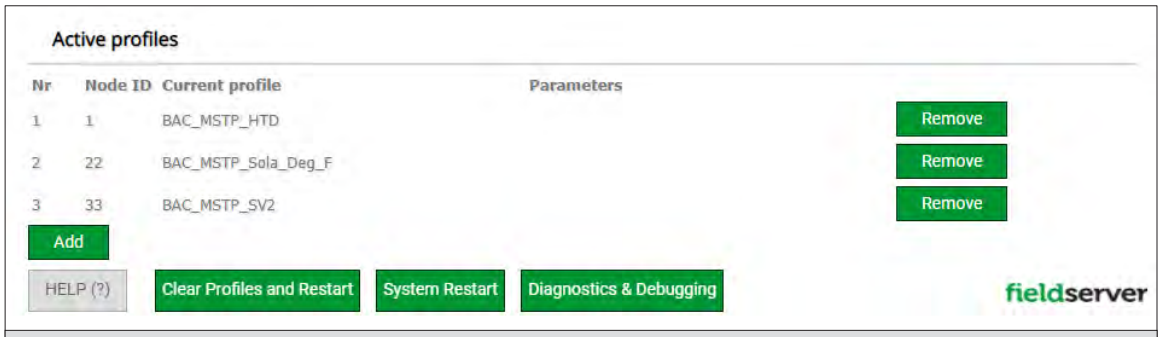


Figure 41: Active Profiles

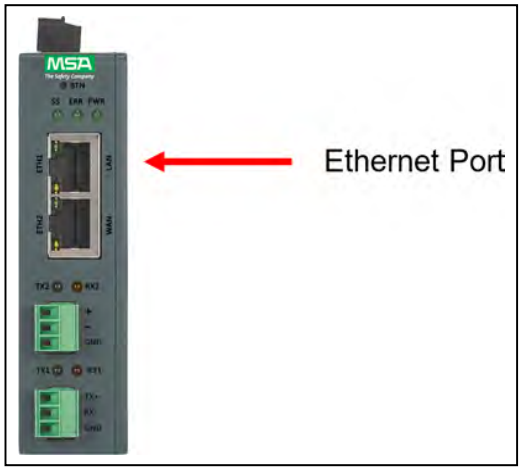
8.6 How to Start the Installation Over: Clearing Profiles

- Follow the steps outlined in **Section 5.1** to access the Gateway Web Configurator.
- At the bottom-left of the page, click the “Clear Profiles and Restart” button.
- Once restart is complete, all past profiles discovered and/or added via Web configurator are deleted. The unit can now be reinstalled.

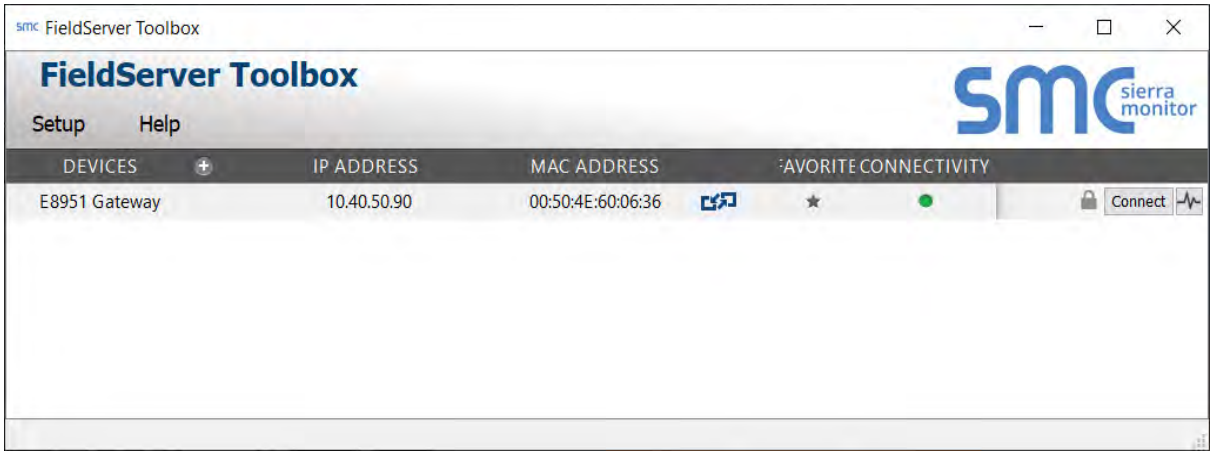
9 Troubleshooting

9.1 Lost or Incorrect IP Address

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

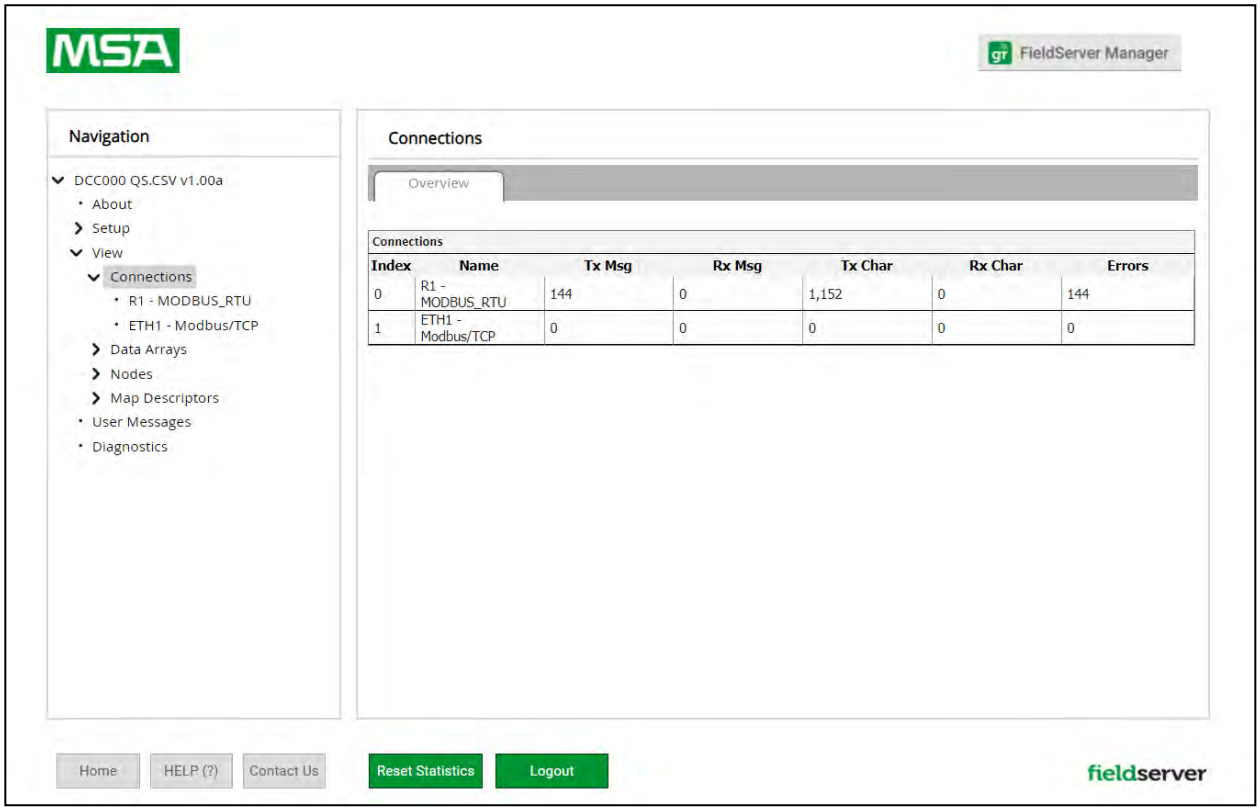


- Connect a standard Cat-5 Ethernet cable between the user's PC and Gateway.
- Double click on the FS Toolbox Utility and click Discover Now on the splash page.
- Check for the IP Address of the desired gateway.



9.2 Viewing Diagnostic Information

- Type the IP Address of the FieldServer into the web browser or use the FieldServer Toolbox to connect to the FieldServer.
- Click on Diagnostics and Debugging Button, then click on view, and then on connections.
- If there are any errors showing on the Connection page, refer to **Section 9.3 Checking Wiring and Settings** for the relevant wiring and settings.



9.3 Checking Wiring and Settings

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

- Visual observations of LEDs on the Gateway. . (**Section 9.5 LED Functions**)
- Check baud rate, parity, data bits, stop bits.
- Check device address.
- Verify wiring.
- Verify the device is connected to the same subnet as the Gateway.

Field COM problems:

- Visual observations of LEDs on the Gateway. . (**Section 9.5 LED Functions**)
- Verify wiring.
- Verify IP Address setting.

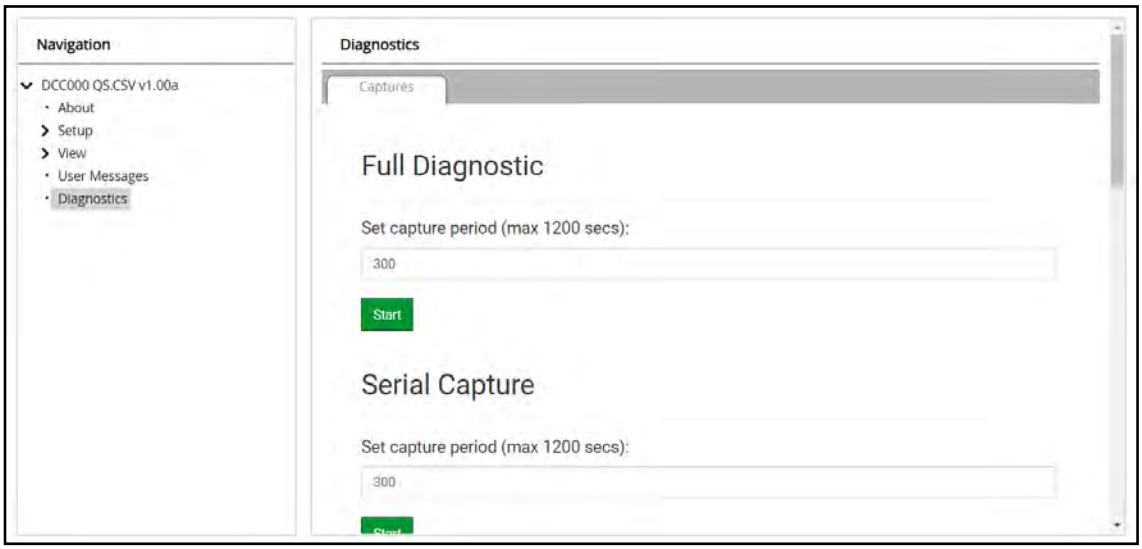
NOTE: If the problem still exists, a Diagnostic Capture needs to be taken and sent to support. (Section 9.4 Taking a FieldServer Diagnostic Capture)

Troubleshooting (continued)

9.4 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

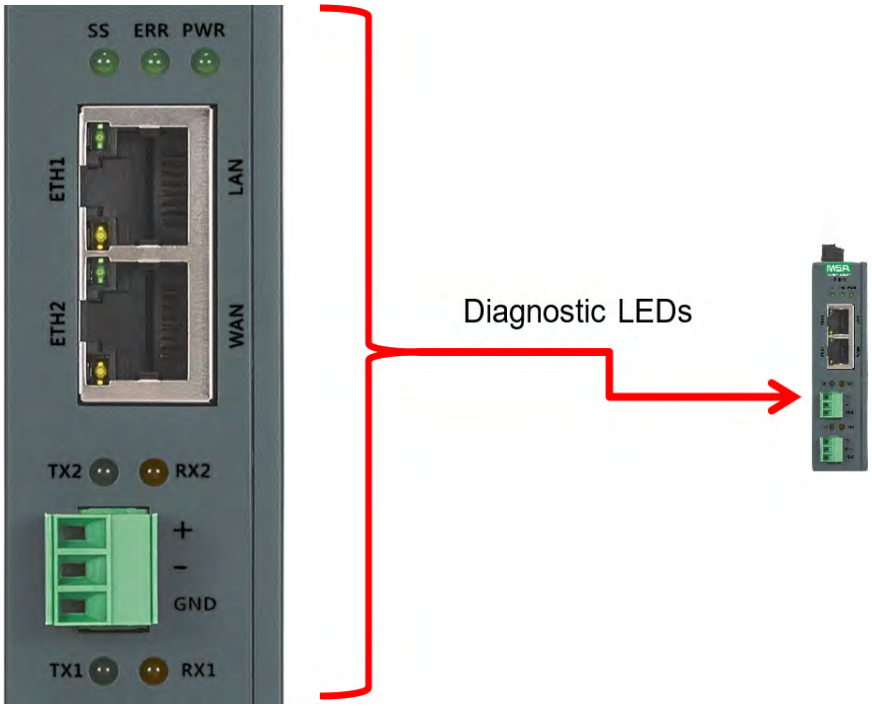


- Go to Full Diagnostic and select the capture period.
- Click the Start button under the Full Diagnostic heading to start the capture.
  - When the capture period is finished, a Download button will appear next to the Start button

- 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.

9.5 LED Functions



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

9.6 Factory Reset Instructions

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

9.7 Internet Browser Software Support

The following web browsers are supported:

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

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

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

10 Additional Information

10.1 Update Firmware

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

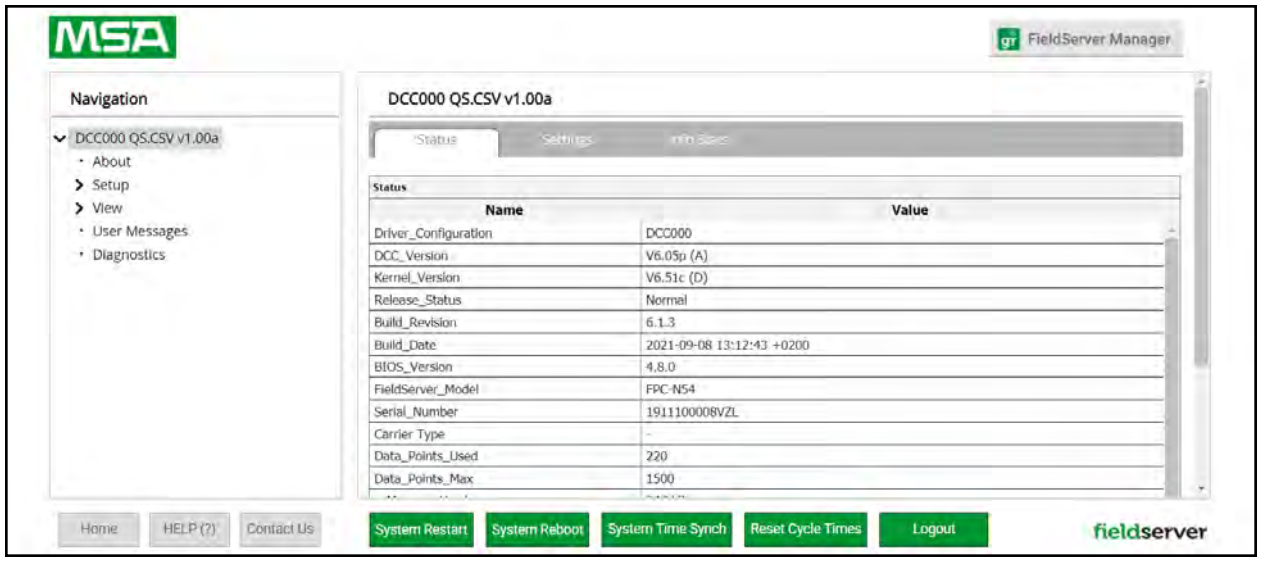
1. Extract and save the new file onto the local PC.
2. Open a web browser and type the IP Address of the FieldServer in the address bar.
   - Default IP Address is **192.168.1.24**
   - Use the FS Toolbox utility if the IP Address is unknown (**Section 9.1 Lost or Incorrect IP Address**)
3. Click on the “Diagnostics & Debugging” button.
4. In the Navigation Tree on the left hand side, do the following:
   a. Click on “Setup”
   b. Click on “File Transfer”
   c. Click on the “General” tab
5. In the General tab, click on “Choose Files” and select the web.img file extracted in step 1.
6. Click on the orange “Submit” button.
7. When the download is complete, click on the “System Restart” button.

NOTE: Contact to receive any firmware updates.

10.2 Change Web Server Security Settings After Initial Setup

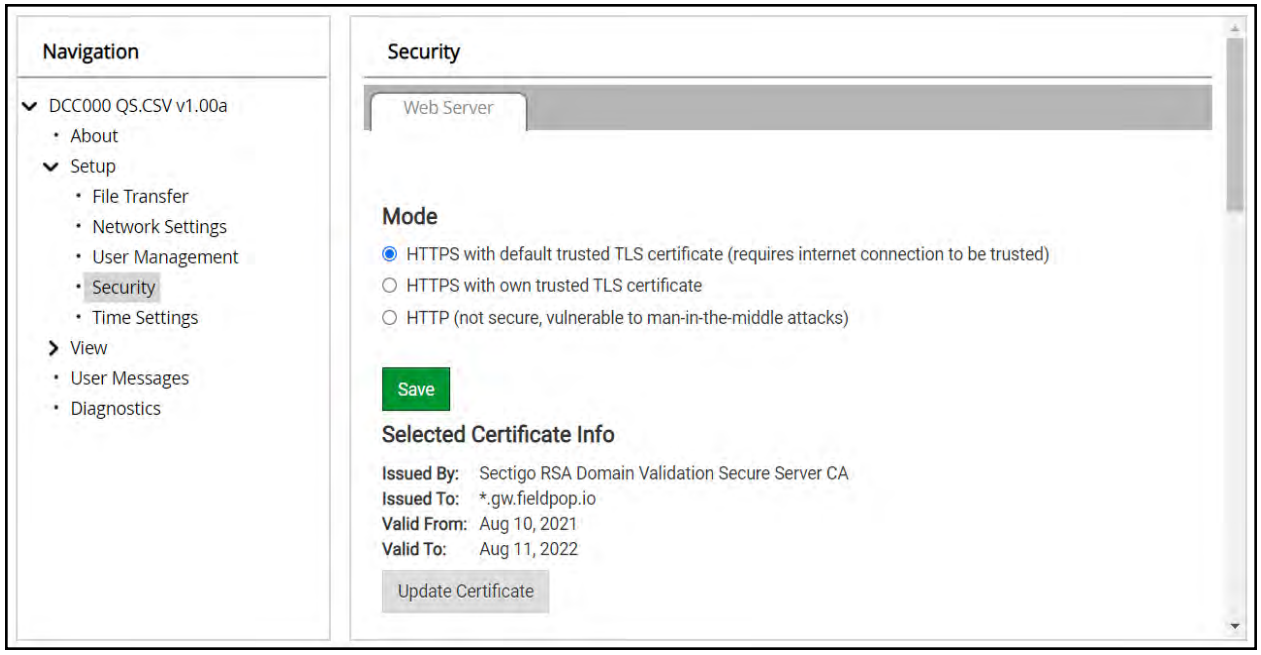
NOTE: Any changes will require a FieldServer reboot to take effect.

- Navigate from the Gateway landing page to the FS-GUI by clicking the blue "Diagnostics" text on the bottom of the screen.
- The Gateway landing page is the FS-GUI.
- Click Setup in the Navigation panel.



10.2.1 Change Security Mode

- Click Security in the Navigation panel.



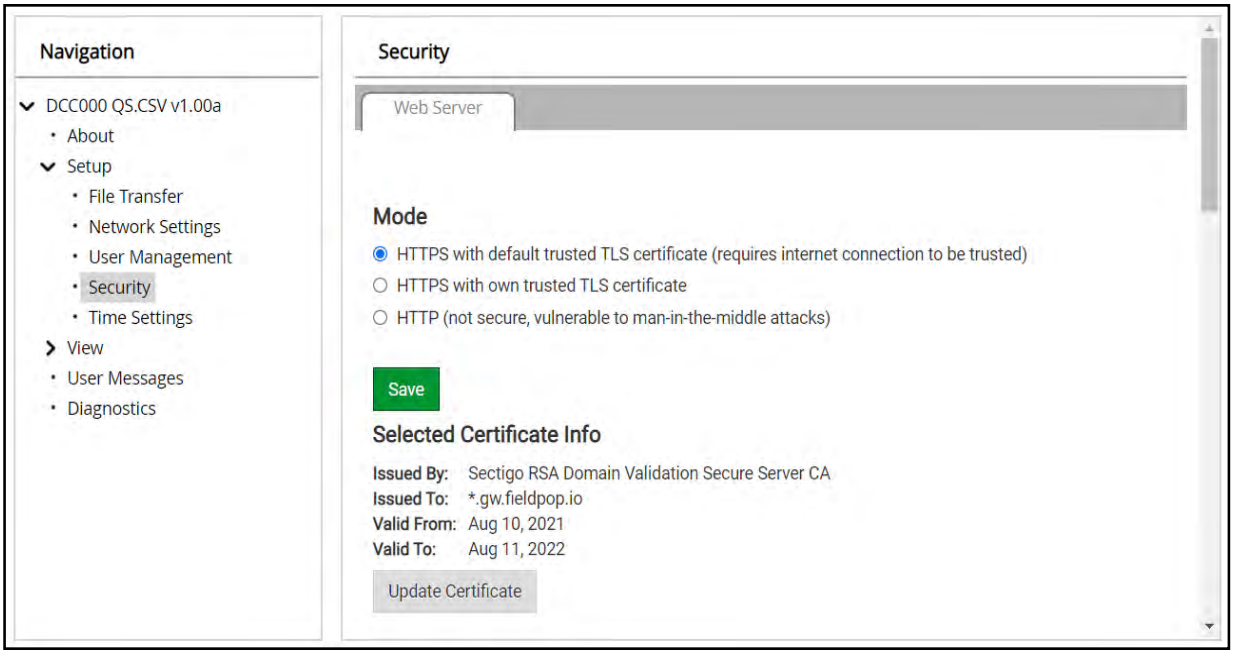
- Click the Mode desired.
  - If HTTPS with own trusted TLS certificate is selected, follow instructions in **Section 6.2.1 HTTPS with Own Trusted TLS Certificate**

Additional Information (continued)

10.2.2 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.

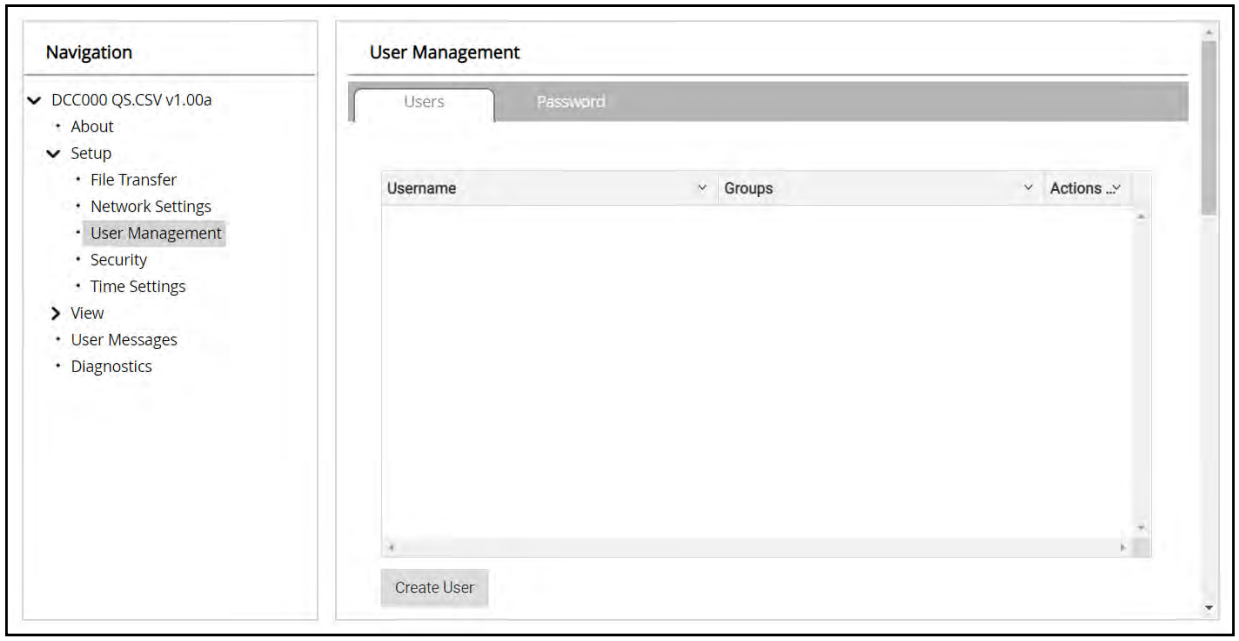
10.3 Change User Management Settings

- 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.

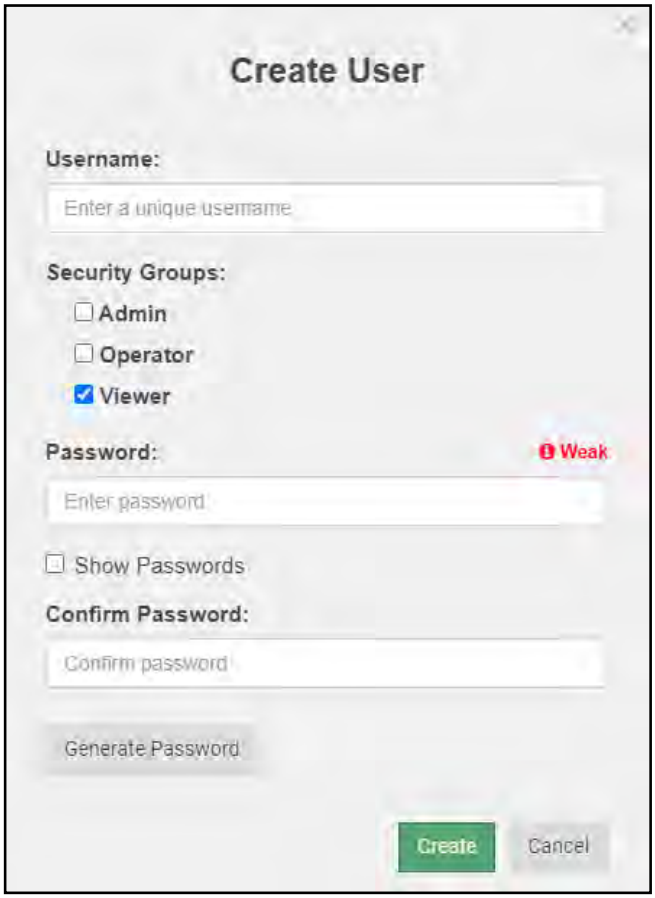
Operator – Can modify and view any data in the FieldServer array(s).

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

Additional Information (continued)

10.3.1 Create Users

- Click the Create User button.



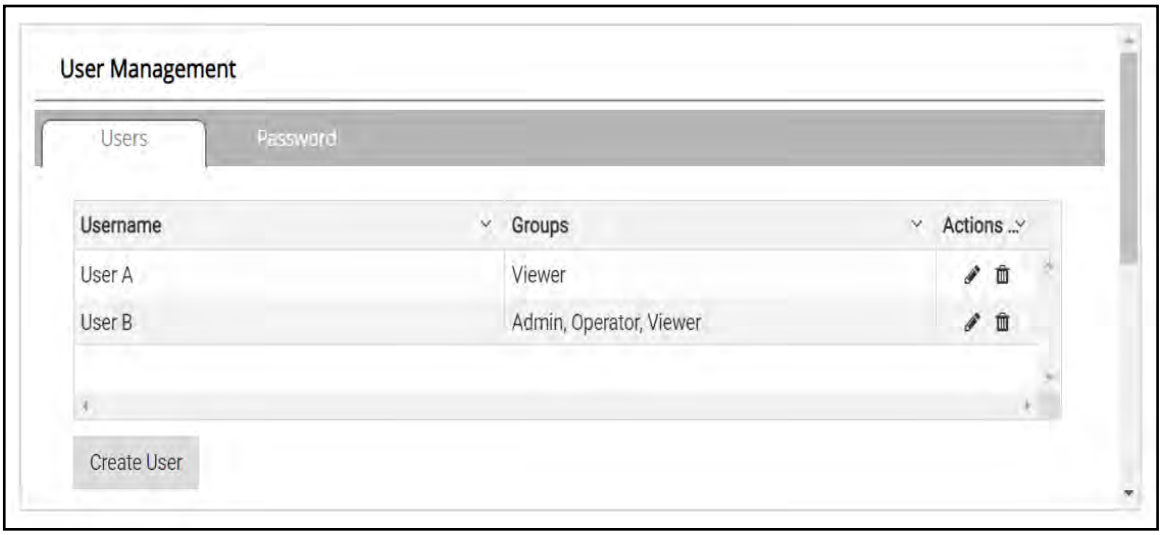
- Enter the new User fields: Name, Security Group and Password.
  - **User details are hashed and salted**

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.

10.3.2 Edit Users

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



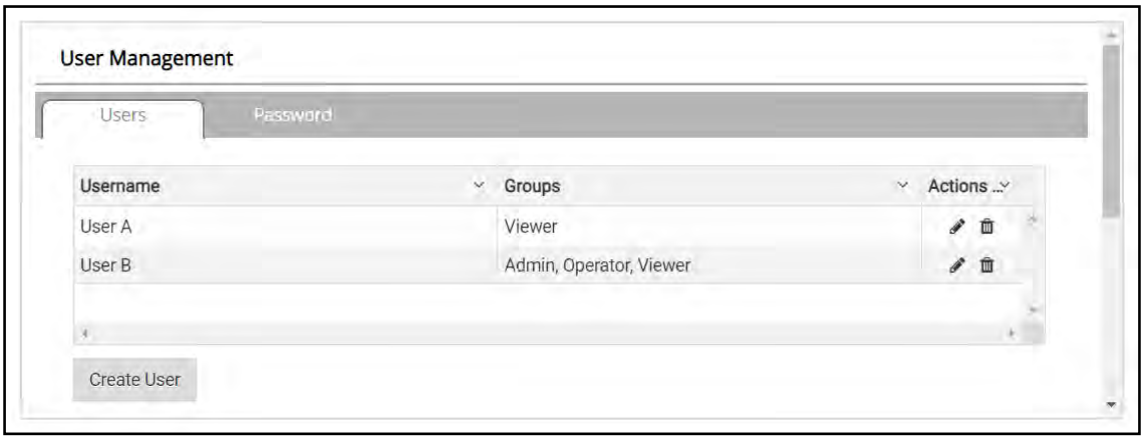
- Once the User Edit window opens, change the User Security Group and Password as needed.

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

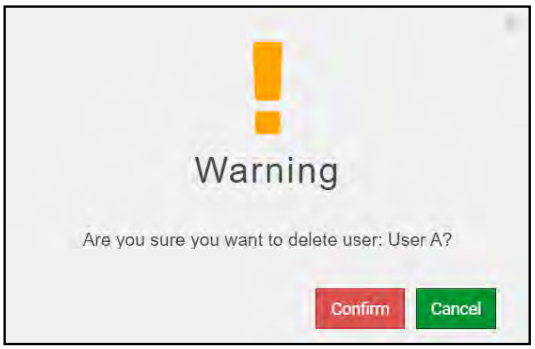
Additional Information (continued)

10.3.3 Delete Users

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

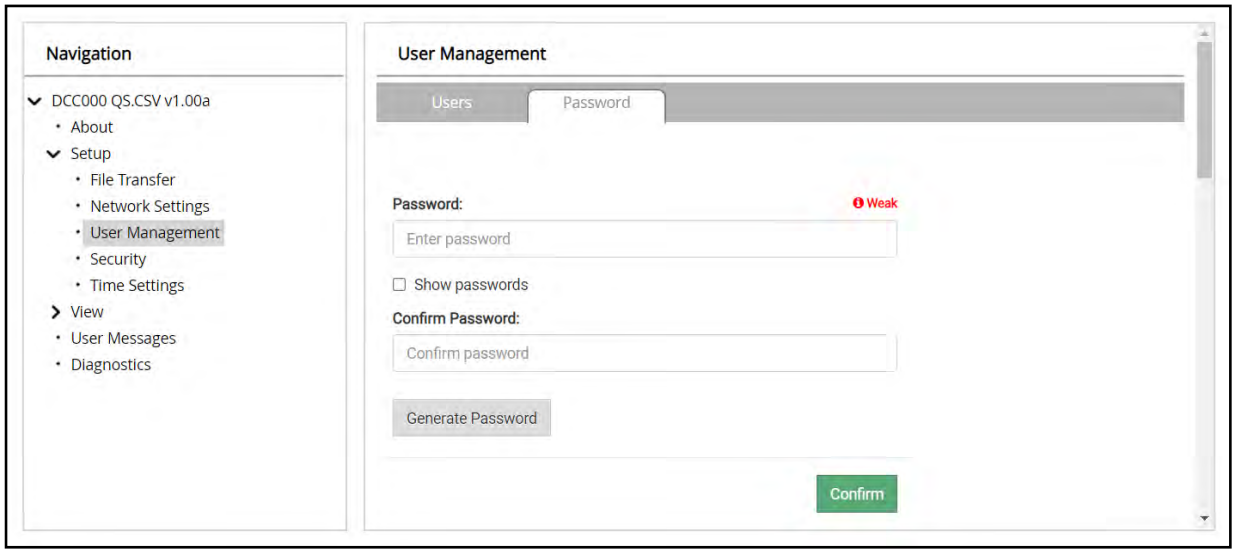


- When the warning message appears, click Confirm.



10.3.4 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.

10.4 Specifications

	ProtoNode FPC-N64
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) Two 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 C, UL 62368-1, CAN/CSA C22.2 No. 62368-1, EN IEC 62368-1, DNP 3.0 and Modbus conformance tested, BTL Marked, WEEE compliant, RoHS compliant, REACH compliant, UKCA and CE compliant, ODVA conformant, CAN ICES-003(B) / NMB-003(B)
Physical Dimensions	4 x 1.1 x 2.7 in (10.16 x 2.8 x 6.8 cm)
Weight	0.4 lbs (0.2 Kg)
Operating Temperature	-20°C to 70°C (-4°F to158°F)
Humidity	10-95% RH non-condensing

NOTE: Specifications subject to change without notice.

10.5 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.

10.6 Compliance with EN IEC 62368-1

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

- 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.

11 Limited 2 Year Warranty

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

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

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

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

Notes:

H2435500-