

ProtoNode FPC-N34 and ProtoNode FPC-N35 Installation and Operating Manual

For Interfacing LAARS Products:

Sola, Multiburner, SV2, HTD, OmniTherm, MagnaTherm, NeoTherm XTR

To Building Automation Systems:

BACnet MS/TP, BACnet/IP, Modbus TCP/IP, Metasys N2, LonWorks and
SMC Cloud

APPLICABILITY & EFFECTIVITY

Explains ProtoNode hardware and how to install it.

The instructions are effective for the above as of March 2024



Document Revision: 14.B

Web Configurator

H2354400L

Technical Support

Thank you for purchasing the ProtoNode for LAARS.

Please call LAARS for technical support of the ProtoNode product.

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

Support Contact Information:

LAARS
20 Industrial Way,
Rochester, NH 03867

Customer Service:
(603) 335-6300

Email: info@LAARS.com

Website: www.laars.com

Quick Start Guide

1. Record the information about the unit. (**Section 2.1**)
2. Check that the ProtoNode and customer device COM settings match. (**Section 2.3**)
3. Connect the ProtoNode 6 pin RS-485 connector to the RS-485 network that is connected to each of the devices. (**Section 3.2**)
4. **If using a serial field protocol:**
Connect the ProtoNode FPC-N34 3 pin RS-485 port to the field protocol cabling, (Section 3.3**)**
or connect the ProtoNode FPC-N35 2 pin LonWorks port to the field protocol cabling. (Section 3.4**)**
5. Connect power to the ProtoNode 6 pin port. (**Section 3.5**)
6. Connect a PC to the ProtoNode via Ethernet cable. (**Section 4**)
7. Setup Web Server Security and login via web browser. (**Section 5**)
8. Use a web browser to access the ProtoNode Web Configurator page to select the profiles of the devices attached to the ProtoNode and enter any necessary device information. Once the devices are selected, the ProtoNode automatically builds and loads the appropriate configuration. (**Section 8**)
9. LonWorks (FPC-N35): The ProtoNode must be commissioned on the LonWorks Network. This needs to be done by the LonWorks administrator using a LonWorks commissioning tool. (**Section 9**)

Table of Contents

1	Introduction.....	8
1.1	ProtoNode Gateway	8
2	Setup for ProtoNode	10
2.1	Record Identification Data	10
2.2	Point Count Capacity	10
2.3	Configuring Device Communications	11
2.3.1	Confirm the Device and ProtoNode COM Settings Match	11
2.3.2	Set Node-ID for Any Device Attached to the ProtoNode	11
3	Interfacing ProtoNode to Devices	12
3.1	ProtoNode FPC-N34 and FPC-N35 Showing Connection Ports.....	12
3.2	Serial Device Connections to the ProtoNode	13
3.2.1	Biasing the RS-485 Device Network	14
3.2.2	End of Line Termination Switch for the RS-485 Device Network	15
3.3	Serial Network (FPC-N34): Wiring Field Port to RS-485 Network	16
3.4	LonWorks (FPC-N35): Wiring LonWorks Devices to the LonWorks Terminal	17
3.5	Power-Up ProtoNode	18
4	Connect the PC to the ProtoNode	19
4.1	Connecting to the Gateway via Ethernet.....	19
4.1.1	Changing the Subnet of the Connected PC	19
5	Setup Web Server Security	20
5.1	Login to the FieldServer	20
5.2	Select the Security Mode.....	22
5.2.1	HTTPS with Own Trusted TLS Certificate	23
5.2.2	HTTPS with Default Untrusted Self-Signed TLS Certificate or HTTP with Built-in Payload Encryption	23
6	Configure Network Settings.....	24
6.1	Navigate to the Network Settings	24
6.2	Change the ProtoNode IP Address	25
7	SMC Cloud User Setup, Registration and Login.....	26
7.1	Choose Whether to Integrate SMC Cloud.....	26
7.2	User Setup.....	28
7.3	Registration Process	30
7.4	Login to SMC Cloud	34
8	Configure the ProtoNode.....	36
8.1	Navigate to the ProtoNode Web Configurator	36
8.2	Select Field Protocol and Set Configuration Parameters	37
8.3	Setting ProtoNode Active Profiles	38
8.4	Verify Device Communications.....	39
8.5	BACnet: Setting Node_Offset to Assign Specific Device Instances.....	40
8.6	How to Start the Installation Over: Clearing Profiles	41
9	LonWorks (FPC-N35): Commissioning ProtoNode on a LonWorks Network	42
9.1	Commissioning ProtoNode FPC-N35 on a LonWorks Network	42
9.1.1	Instructions to Upload XIF File from ProtoNode FPC-N35 Using Browser.....	42
10	Troubleshooting	44
10.1	Lost or Incorrect IP Address	44
10.2	Viewing Diagnostic Information	45
10.3	Checking Wiring and Settings	46
10.4	LED Diagnostics for Communications Between ProtoNode and Devices	47
10.5	Taking a FieldServer Diagnostic Capture.....	48
10.5.1	Taking a Capture with Older Firmware	49

10.6	Factory Reset Instructions.....	51
10.7	Internet Browsers Not Supported	51
11	Additional Information	52
11.1	Update Firmware	52
11.2	BACnet: Setting Network_Number for More Than One ProtoNode on the Subnet	52
11.3	Certification.....	52
11.3.1	BTL Mark – BACnet® Testing Laboratory	52
11.3.2	LonMark Certification	53
11.4	Change Web Server Security Settings After Initial Setup	54
11.4.1	Change Security Mode.....	55
11.4.2	Edit the Certificate Loaded onto the FieldServer	56
11.5	Change User Management Settings	57
11.5.1	Create Users	58
11.5.2	Edit Users	59
11.5.3	Delete Users.....	60
11.5.4	Change FieldServer Password	61
11.6	SMC Cloud Connection Warning Message.....	62
11.7	System Status Button	63
11.8	Routing Settings	64
12	Vendor Information – LAARS.....	65
13	Specifications	66
13.1	Compliance with UL Regulations.....	66
14	Limited 2 Year Warranty	67

List of Figures

Figure 1: ProtoNode Part Numbers.....	10
Figure 2: Supported Point Count Capacity.....	10
Figure 3: Points per Device.....	10
Figure 4: COM Settings.....	11
Figure 5: ProtoNode FPC-N34 (Top) and ProtoNode FPC-N35 (Bottom)	12
Figure 6: Device and Power Connections.....	13
Figure 7: RS-485 Biasing Switch on the ProtoNode N34 (Left) and ProtoNode N35 (Right).....	14
Figure 8: RS-485 End-Of-Line Termination Switch on the ProtoNode N34 (Left) and.....	15
Figure 9: Connection from ProtoNode to RS-485 Field Network	16
Figure 10: RS-485 EOL & Bias Resistor Switches.....	16
Figure 11: LonWorks Terminal.....	17
Figure 12: Required Current Draw for the ProtoNode.....	18
Figure 13: Power Connections.....	18
Figure 14: Ethernet Port Location	19
Figure 15: Web Server Security Unconfigured Window.....	20
Figure 16: Connection Not Private Warning.....	20
Figure 17: Warning Expanded Text	21
Figure 18: FieldServer Login.....	21
Figure 19: Security Mode Selection Screen.....	22
Figure 20: Security Mode Selection Screen – Certificate & Private Key	23
Figure 21: Generic Web App Landing Page	24
Figure 22: Settings Tabs	24
Figure 23: FS-GUI Landing Page.....	24
Figure 24: Ethernet Port Network Settings.....	25
Figure 25: Generic Web App Page – First Login	26
Figure 26: SMC Cloud Opt Out Warning Window	27
Figure 27: Welcome to SMC Cloud Email.....	28
Figure 28: Setting User Details	29
Figure 29: SMC Cloud Registration Message.....	30
Figure 30: SMC Cloud Registration – Installer Details.....	31
Figure 31: SMC Cloud Registration – Site Details	31
Figure 32: SMC Cloud Registration – Gateway Details	32
Figure 33: SMC Cloud Registration – SMC Cloud Account	32
Figure 34: Device Registered for SMC Cloud	33
Figure 35: SMC Cloud Login Page	34
Figure 36: SMC Cloud Privacy Policy	34
Figure 37: SMC Cloud Landing Page	35
Figure 38: Web App Landing Page	36
Figure 39: Configure Tab	36
Figure 40: Web Configurator Showing Configuration Parameters	37
Figure 41: Web Configurator Showing no Active Profiles	38
Figure 42: Profile Selection Menu	39
Figure 43: Web Configurator Showing Active Profile Additions	39
Figure 44: Web Configurator Node Offset Field	40
Figure 45: Active Profiles	40
Figure 46: LonWorks Service Pin Location	42
Figure 47: Sample of Fserver.XIF File Generated	43
Figure 48: Ethernet Port Location	44
Figure 49: Error Messages Screen	45
Figure 50: Diagnostic LEDs	47
Figure 51: Ethernet Port Location	49
Figure 52: Web Configurator – Network Number Field	52
Figure 53: FS-GUI Page	54
Figure 54: FS-GUI Security Setup	55
Figure 55: FS-GUI Security Setup – Certificate Loaded	56
Figure 56: FS-GUI User Management	57
Figure 57: Create User Window	58

Figure 58: Setup Users59

Figure 59: Edit User Window59

Figure 60: Setup Users60

Figure 61: User Delete Warning.....60

Figure 62: FieldServer Password Update via FS-GUI61

Figure 63: SMC Cloud Connection Problems Message.....62

Figure 64: Routing Settings.....64

Figure 65: Specifications66

1 Introduction

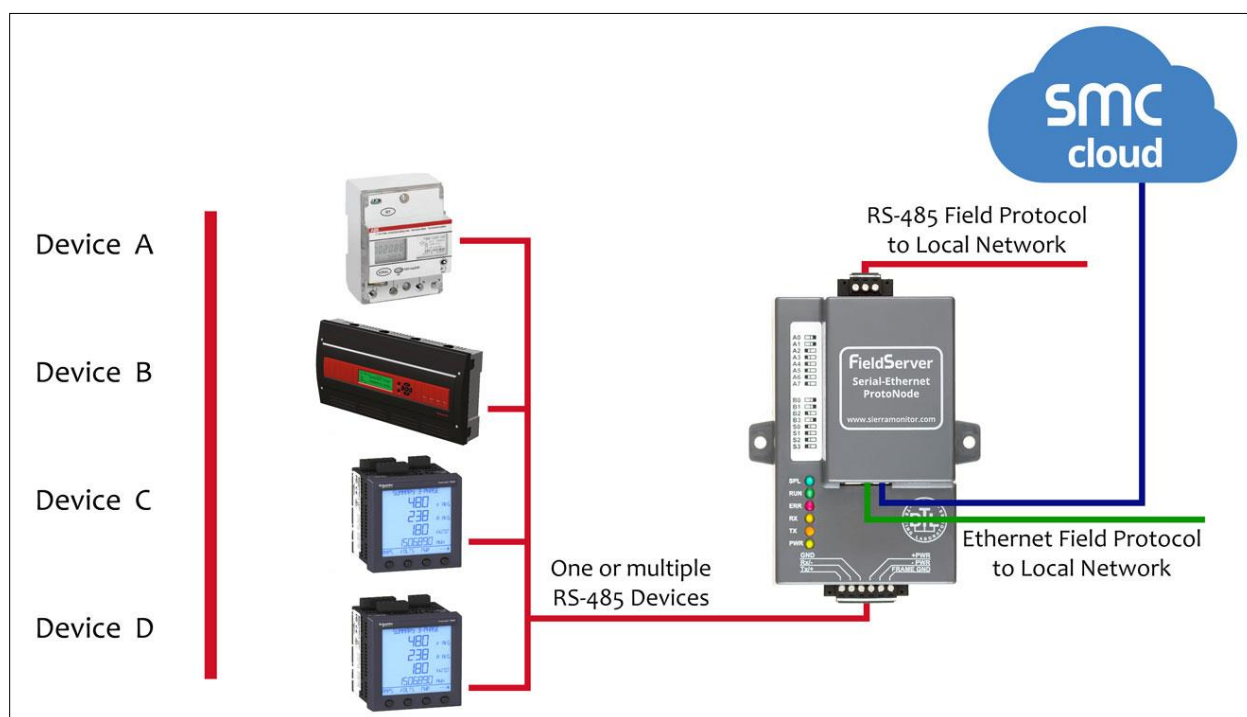
1.1 ProtoNode Gateway

The ProtoNode 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 ProtoNode and automatically configures them for BACnet MS/TP, BACnet/IP, Modbus TCP/IP or LonWorks®¹.

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

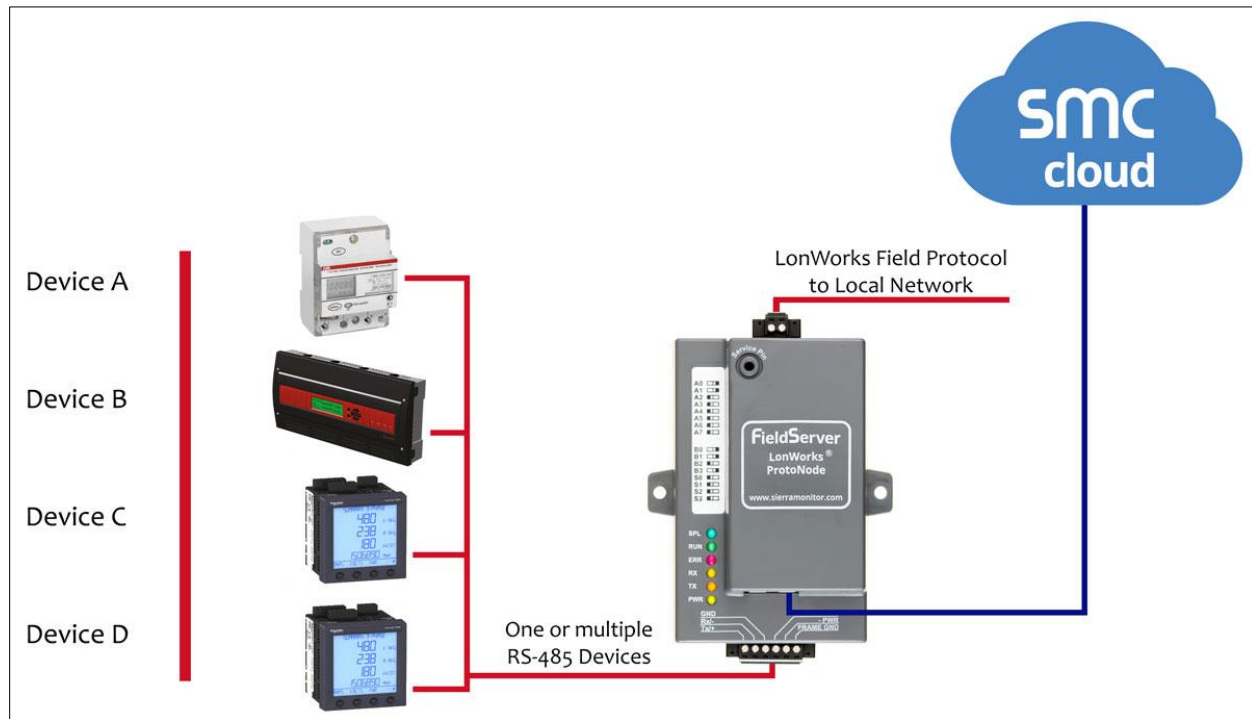
WARNING: Only use screws supplied by MSA Safety in the holes found on the back of the unit when attaching the optional DIN rail bracket. Use of any other screws may damage the unit.

FPC-N34 Connectivity Diagram:



¹ LonWorks is a registered trademark of Echelon Corporation

FPC-N35 Connectivity Diagram:



The ProtoNode can connect with the SMC Cloud. The SMC Cloud allows technicians, the OEM's support team and MSA Safety's support team to remotely connect to the ProtoNode. The SMC Cloud provides the following capabilities for any registered devices in the field:

- Remotely monitor and control devices.
- Collect device data and view it on the SMC Cloud Dashboard and the SMC 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 about the SMC Cloud, refer to the [SMC Cloud Start-up Guide](#).

2 Setup for ProtoNode

2.1 Record Identification Data

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

Model	Part Number
ProtoNode FPC-N34	FPC-N34-0701
ProtoNode FPC-N35	FPC-N35-0702
Figure 1: ProtoNode Part Numbers	

FPC-N34 units have the following 3 ports: RS-485 + Ethernet + RS-485

FPC-N35 units have the following 3 ports: LonWorks + Ethernet + RS-485

2.2 Point Count Capacity

The total number of registers presented the device(s) attached to the ProtoNode cannot exceed:

Part number	Total Registers
FPC-N34-0701	1,500
FPC-N35-0702	1,500
Figure 2: Supported Point Count Capacity	

Devices	Point Count Per Device
Sola	88
Multiburner	149
SV2	82
HTD	254
OmniTherm	174
MagnaTherm	174
NeoTherm XTR	102
Figure 3: Points per Device	

2.3 Configuring Device Communications

2.3.1 Confirm the Device and ProtoNode COM Settings Match

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

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 ProtoNode

- Set Node-ID for any device attached to ProtoNode. 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 8.5**)

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

3 Interfacing ProtoNode to Devices

3.1 ProtoNode FPC-N34 and FPC-N35 Showing Connection Ports

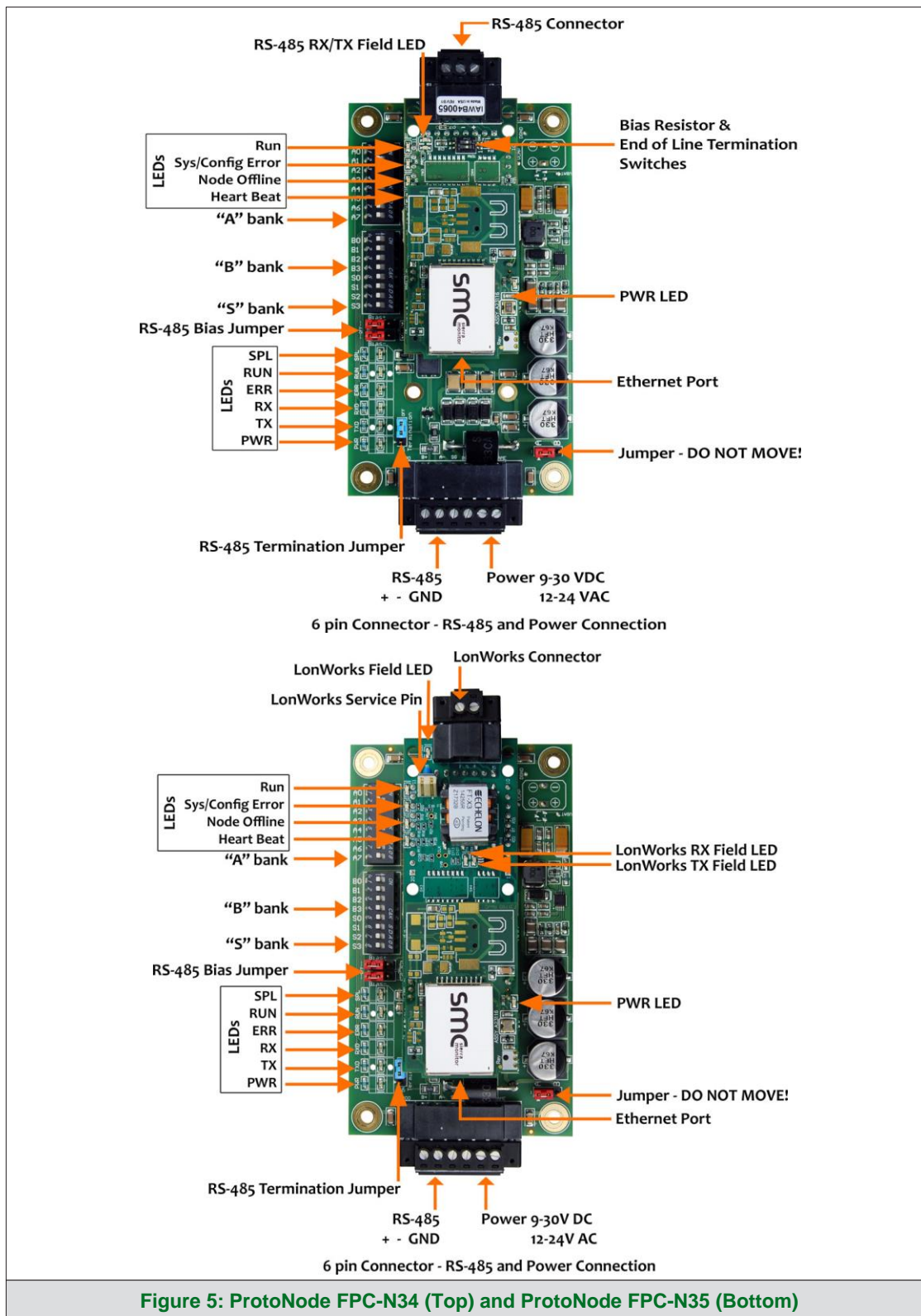
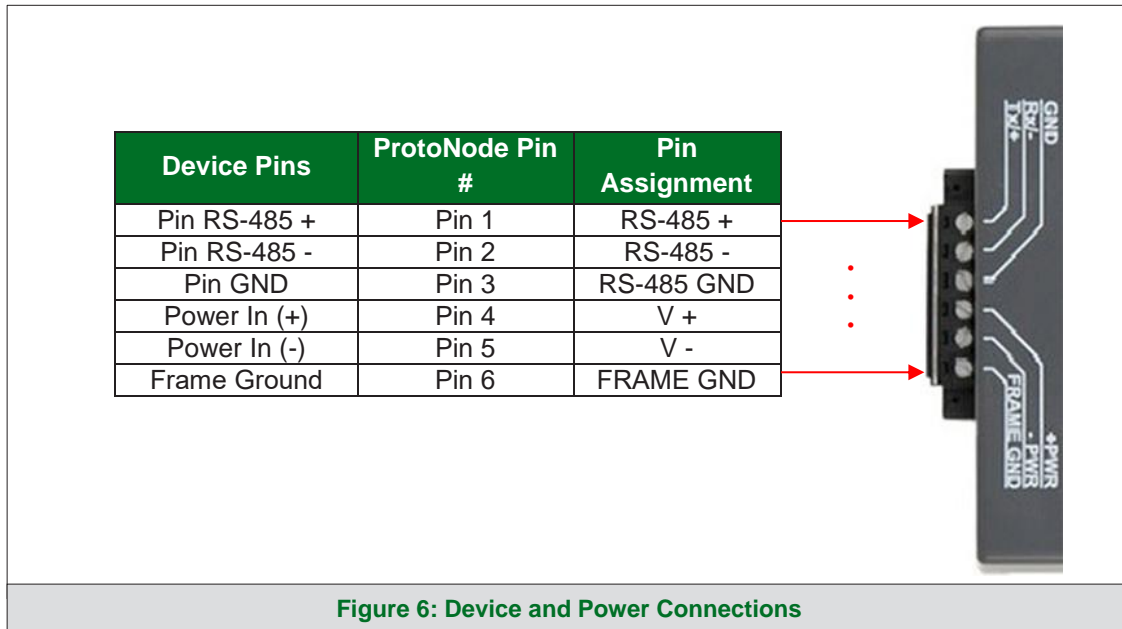


Figure 5: ProtoNode FPC-N34 (Top) and ProtoNode FPC-N35 (Bottom)

3.2 Serial Device Connections to the ProtoNode

ProtoNode 6 Pin Phoenix connector:

- The 6 pin Phoenix connector is the same for ProtoNode FPC-N34 and FPC-N35 (LonWorks).
- Pins 1 through 3 are for RS-485 devices.
 - Use standard grounding principles for RS-485 GND
- Pins 4 through 6 are for power. **Do not connect power until Section 3.5.**



3.2.1 Biasing the RS-485 Device Network

- An RS-485 network with more than one device needs to have biasing to ensure proper communication. The biasing only needs to be done on one device.
- The ProtoNode has 510 ohm resistors that can be used to set the biasing. The ProtoNode's default positions from the factory for the biasing jumpers are OFF.
- The OFF position is when the 2 red biasing jumpers straddle the 4 pins closest to the outside of the board of the ProtoNode. (**Figure 7**)
- **Only turn biasing ON:**
 - **IF the BMS cannot see more than one device connected to the ProtoNode**
 - **AND all the settings (COM settings, wiring, and DIP switches) have been checked**
- To turn biasing ON, move the 2 red biasing jumpers to straddle the 4 pins closest to the inside of the board of the ProtoNode.

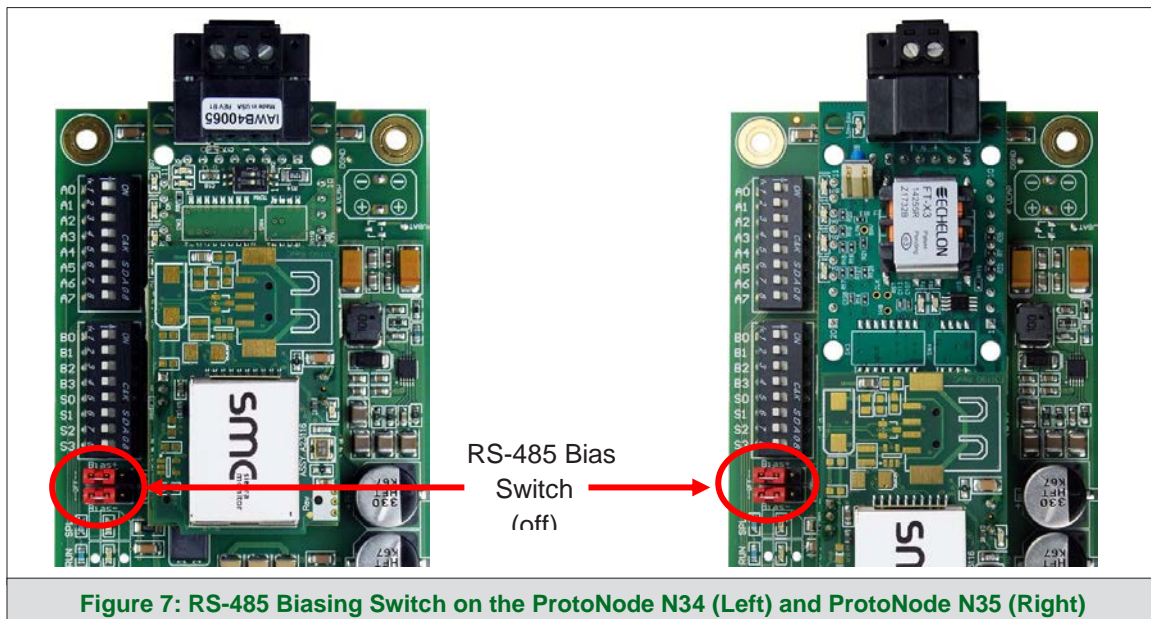
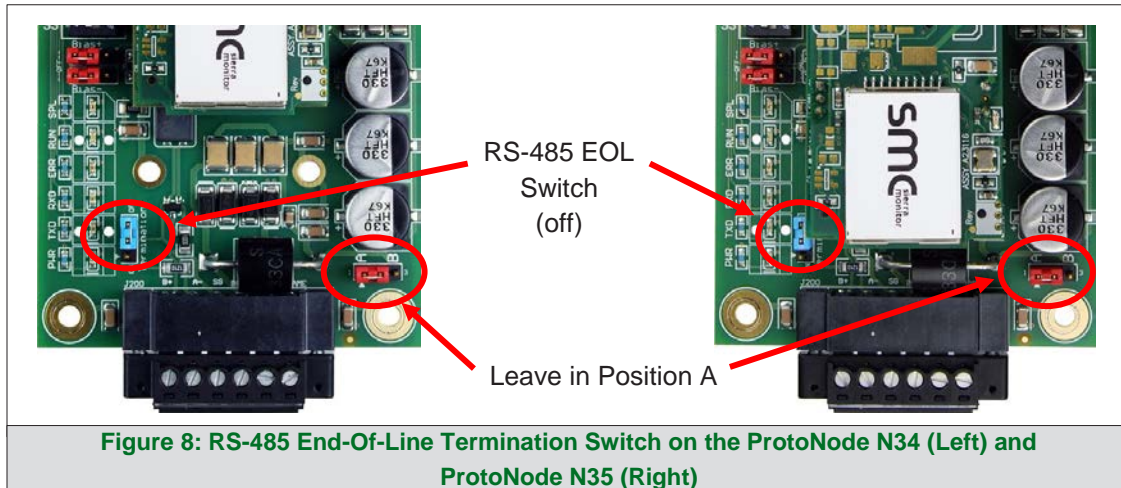


Figure 7: RS-485 Biasing Switch on the ProtoNode N34 (Left) and ProtoNode N35 (Right)

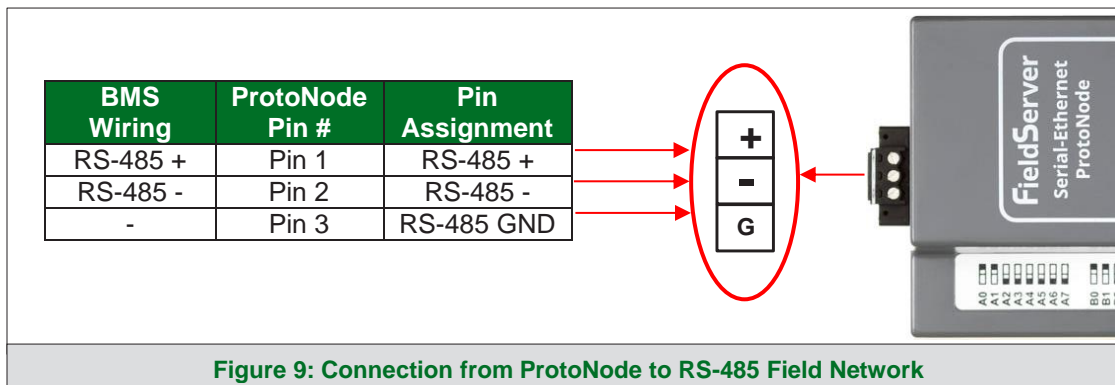
3.2.2 End of Line Termination Switch for the RS-485 Device Network

- On long RS-485 cabling runs, the RS-485 trunk must be properly terminated at each end.
- The ProtoNode has an end of line (EOL) blue jumper. The default setting for this blue EOL switch is OFF with the jumper straddling the pins closest to the inside of the board of the ProtoNode.
 - On short cabling runs the EOL switch does not need to be turned ON
- **If the ProtoNode is placed at one of the ends of the trunk, set the blue EOL jumper to the ON position straddling the pins closest to the outside of the board of the ProtoNode.**
- **Always leave the single red jumper in the A position (default factory setting).**



3.3 Serial Network (FPC-N34): Wiring Field Port to RS-485 Network

- Connect the RS-485 network wires to the 3-pin RS-485 connector on ProtoNode as shown below in **Figure 9**.
 - Use standard grounding principles for RS-485 GND
- See **Section 7** for information on connecting to an Ethernet network.



- If the ProtoNode is the last device on the trunk, then the end of line (EOL) termination switch needs to be enabled. See **Figure 10** for the orientation of switch positions referenced below.
 - The default setting from the factory is OFF (switch position = right side)
 - To enable the EOL termination, turn the EOL switch ON (switch position = left side)



- If more than one RS-485 device is connected to the network, then the field bias resistor switch needs to be enabled to ensure proper communication. See **Figure 10** for the orientation of switch positions referenced below.
 - The default factory setting is OFF (switch position = right side)
 - To enable biasing, turn the bias switch ON (switch position = left side)

NOTE: Biasing only needs to be enabled on one device. The ProtoNode has 510 ohm resistors that are used to set the biasing.

3.4 LonWorks (FPC-N35): Wiring LonWorks Devices to the LonWorks Terminal

- Wire the LonWorks device network to the ProtoNode LonWorks Terminal.
 - Use approved cable per the FT-10 installation guidelines
 - LonWorks has no polarity.



Figure 11: LonWorks Terminal

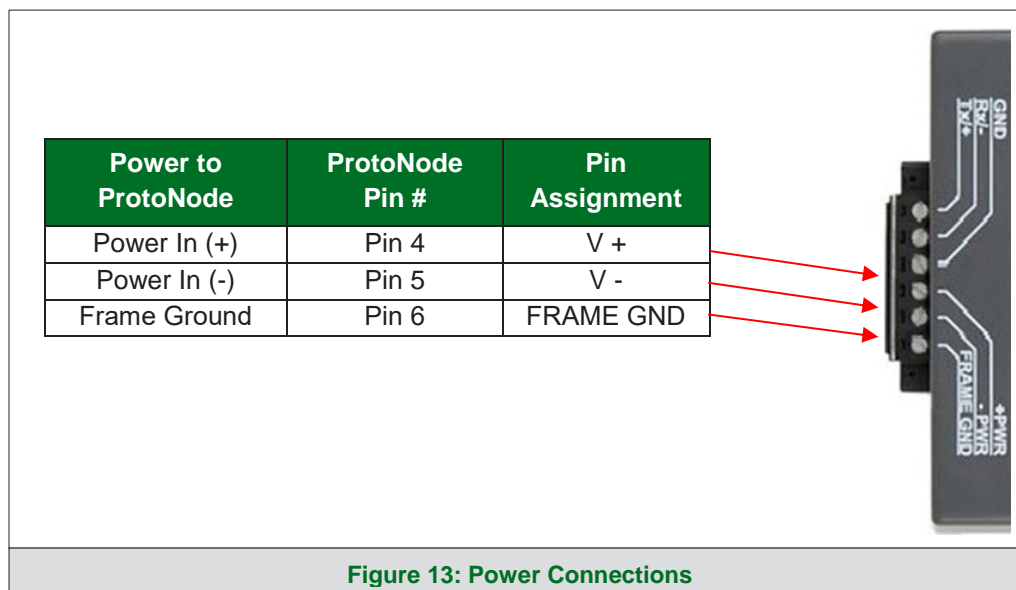
3.5 Power-Up ProtoNode

Check power requirements in the table below:

Power Requirement for ProtoNode External Gateway			
ProtoNode Family	Current Draw Type		
	12VDC/AC	24VDC/AC	30VDC
FPC – N34 (Typical)	170mA	100mA	80mA
FPC – N34 (Maximum)	240mA	140mA	100mA
FPC – N35 (Typical)	210mA	130mA	90mA
FPC – N35 (Maximum)	250mA	170mA	110mA
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.			
Figure 12: Required Current Draw for the ProtoNode			

Apply power to the ProtoNode as shown below in **Figure 13**. Ensure that the power supply used complies with the specifications provided in **Section 13**.

- ProtoNode accepts either 9-30VDC or 12-24VAC on pins 4 and 5.
- Frame GND should be connected.



4 Connect the PC to the ProtoNode

4.1 Connecting to the Gateway via Ethernet

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

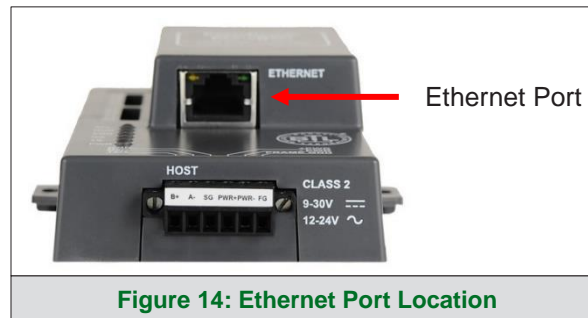



Figure 14: Ethernet Port Location

4.1.1 Changing the Subnet of the Connected PC

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

For Windows 10:

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

☒ Use the following IP address:

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

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

5 Setup Web Server Security

Navigate to the IP Address of the ProtoNode 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 ProtoNode has been changed, the assigned IP Address can be discovered using the FS Toolbox utility. See Section 10.1 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.

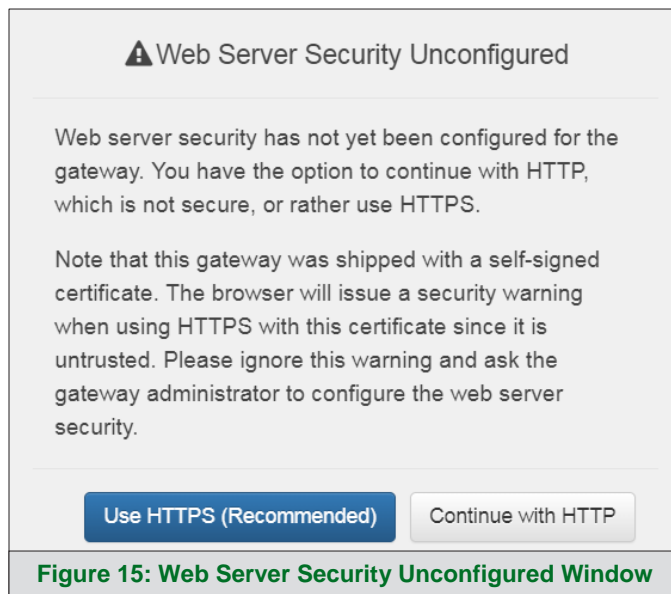


Figure 15: Web Server Security Unconfigured Window

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

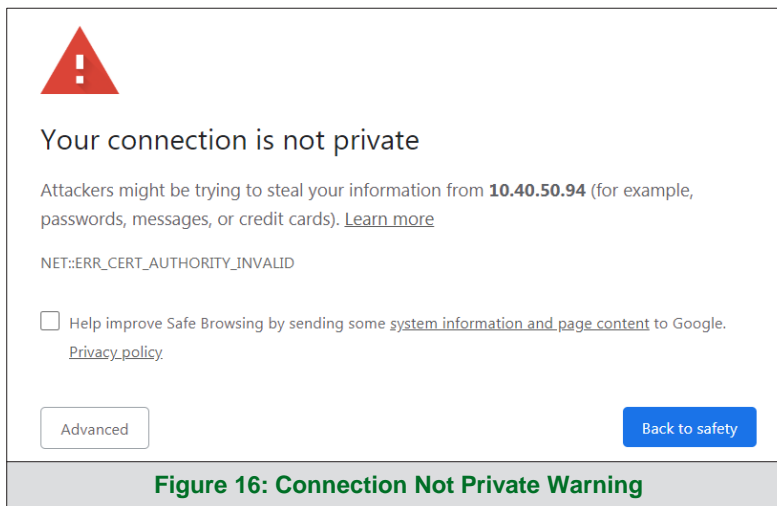


Figure 16: Connection Not Private Warning

- Additional text will expand below the warning, click the underlined text to go to the IP Address. In the **Figure 17** example this text is “[Proceed to 10.40.50.94 \(unsafe\)](#)”.

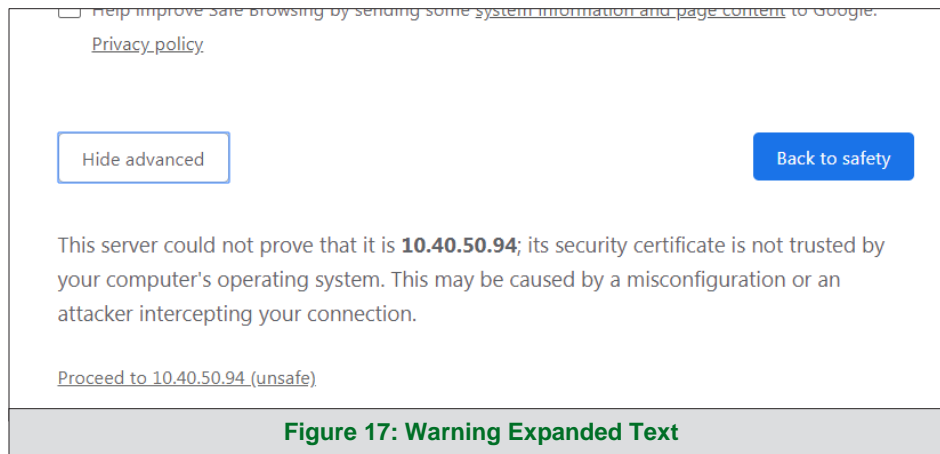


Figure 17: Warning Expanded Text

- 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.

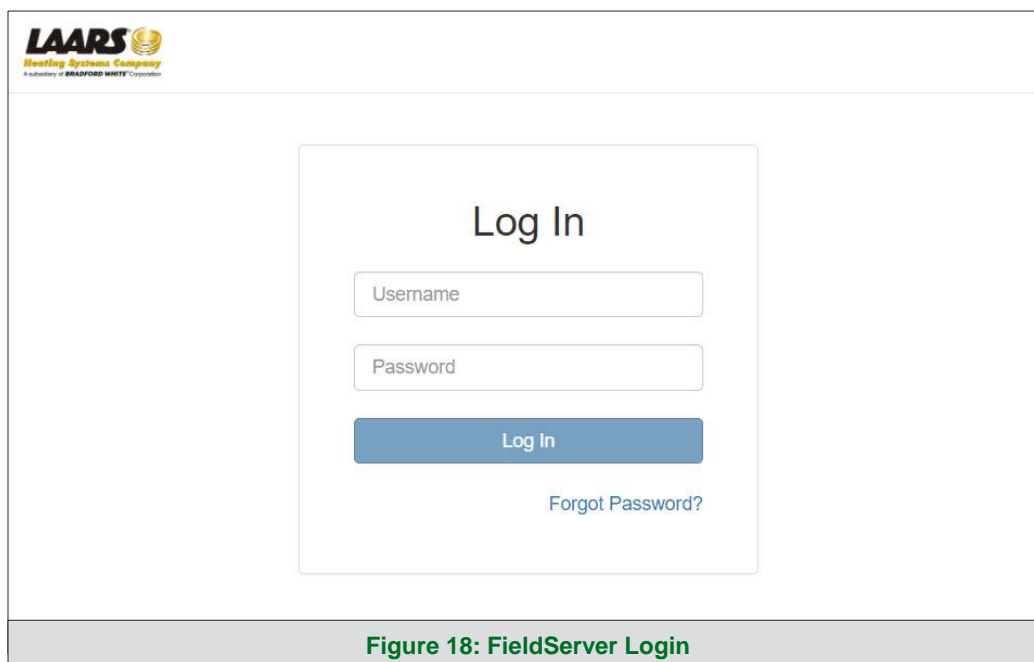


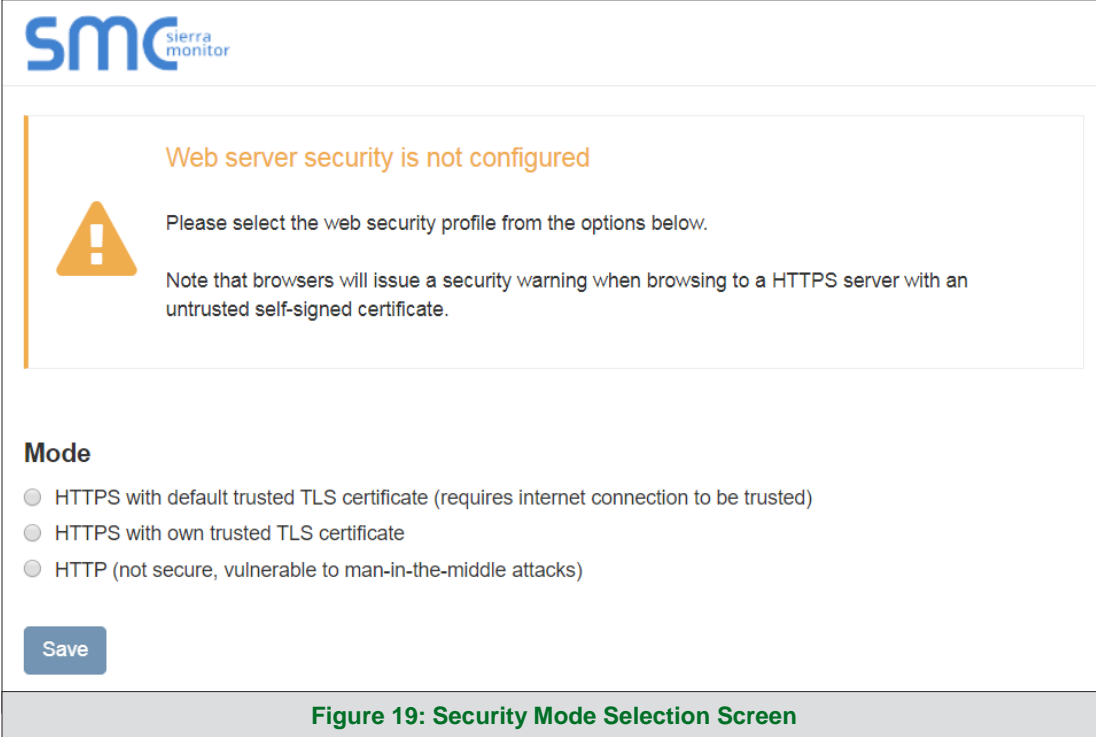
Figure 18: FieldServer Login

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 11.5.

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.



The screenshot shows the SMC Sierra Monitor web interface. At the top left is the SMC logo. A central warning box with an orange triangle icon contains the text: "Web server security is not configured", "Please select the web security profile from the options below.", and "Note that browsers will issue a security warning when browsing to a HTTPS server with an untrusted self-signed certificate." Below this, under the heading "Mode", are three radio button options: "HTTPS with default trusted TLS certificate (requires internet connection to be trusted)", "HTTPS with own trusted TLS certificate", and "HTTP (not secure, vulnerable to man-in-the-middle attacks)". A blue "Save" button is located at the bottom left of the form area.

Mode

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

Save

Figure 19: Security Mode Selection Screen

NOTE: Cookies are used for authentication.

NOTE: To change the web server security mode after initial setup, go to **Section 11.1**.

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

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.

The screenshot shows a web interface for selecting a security mode. Under the 'Certificate' section, there is a text area containing a long base64-encoded string followed by '-----END CERTIFICATE-----'. Below this is the 'Private Key' section with another text area containing a long base64-encoded string followed by '-----END RSA PRIVATE KEY-----'. The 'Private Key Passphrase' section has a text input field with the placeholder 'Specify if encrypted' and a 'Save' button below it. At the bottom of the form, a green caption reads: 'Figure 20: 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 Network Settings

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

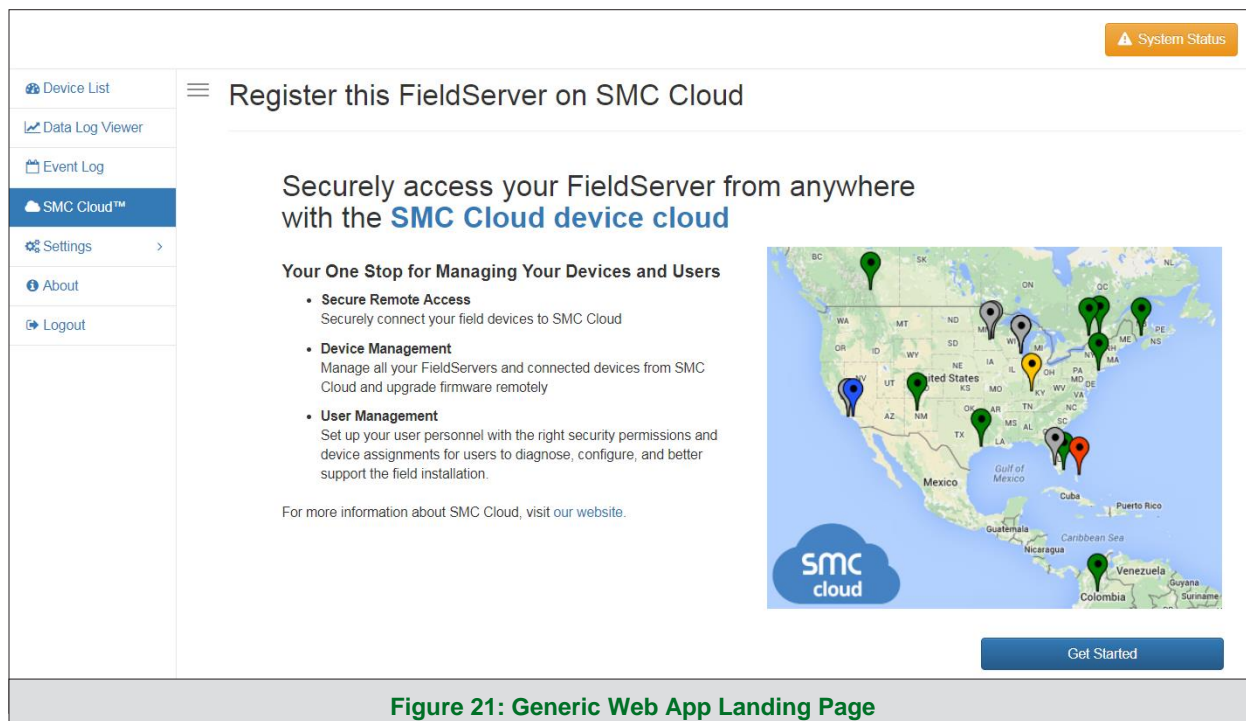


Figure 21: Generic Web App Landing Page

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

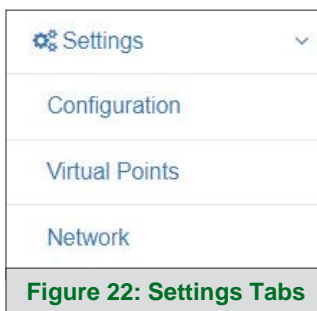


Figure 22: Settings Tabs

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

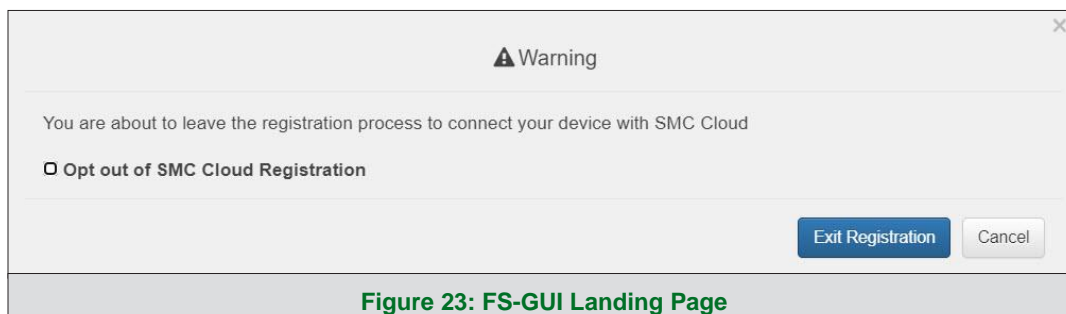


Figure 23: FS-GUI Landing Page

6.2 Change the ProtoNode IP Address

- Enable DHCP to automatically assign IP Settings or modify the IP Settings manually as needed, via these fields: IP Address, Netmask, 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 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 of the ProtoNode before the webpage will be accessible again.

ETH 1 Routing

☐ Enable DHCP

IP Address
10.40.50.111

Netmask
255.255.255.0

Gateway
10.40.50.1

Domain Name Server 1 (Optional)
8.8.8.8

Domain Name Server 2 (Optional)
8.8.4.4

Cancel Save

Network Status

Connection Status	✔ Connected
MAC Address	00:50:4e:60:4f:0c
Ethernet Tx Msgs	325,528
Ethernet Rx Msgs	974,087
Ethernet Tx Msgs Dropped	0
Ethernet Rx Msgs Dropped	0

Figure 24: Ethernet Port Network Settings

NOTE: For Router settings go to Section 11.8.

7 SMC Cloud User Setup, Registration and Login

The SMC Cloud is MSA Safety's device cloud solution for IIoT. Integration with the SMC Cloud 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 SMC Cloud, refer to the [SMC Cloud Start-up Guide](#).

7.1 Choose Whether to Integrate SMC Cloud

When first logging onto the ProtoNode, the Web App will open on the SMC Cloud™ page.

NOTE: If a warning message appears instead, go to Section 11.6 to resolve the connection issue.

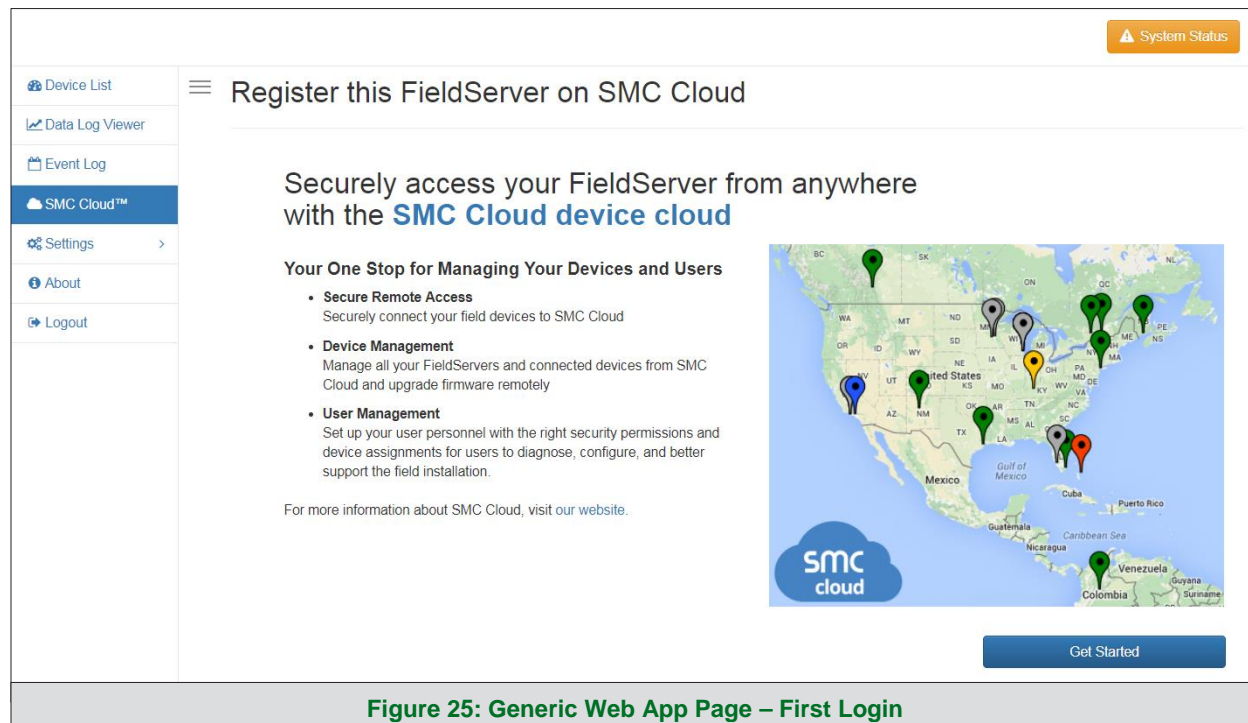



Figure 25: Generic Web App Page – First Login

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

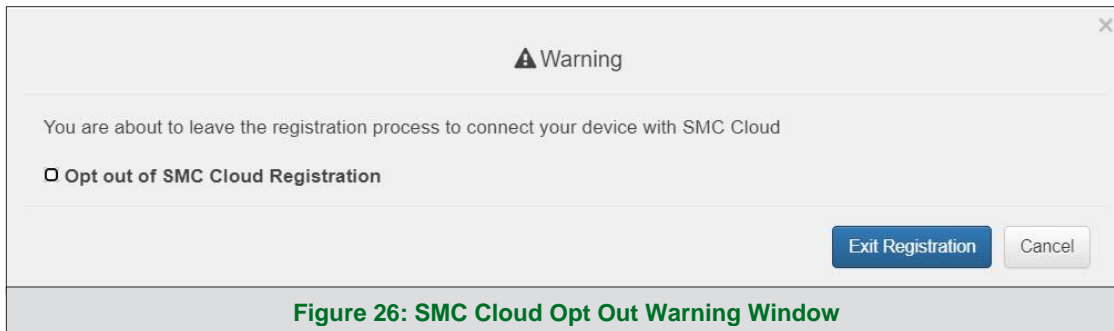


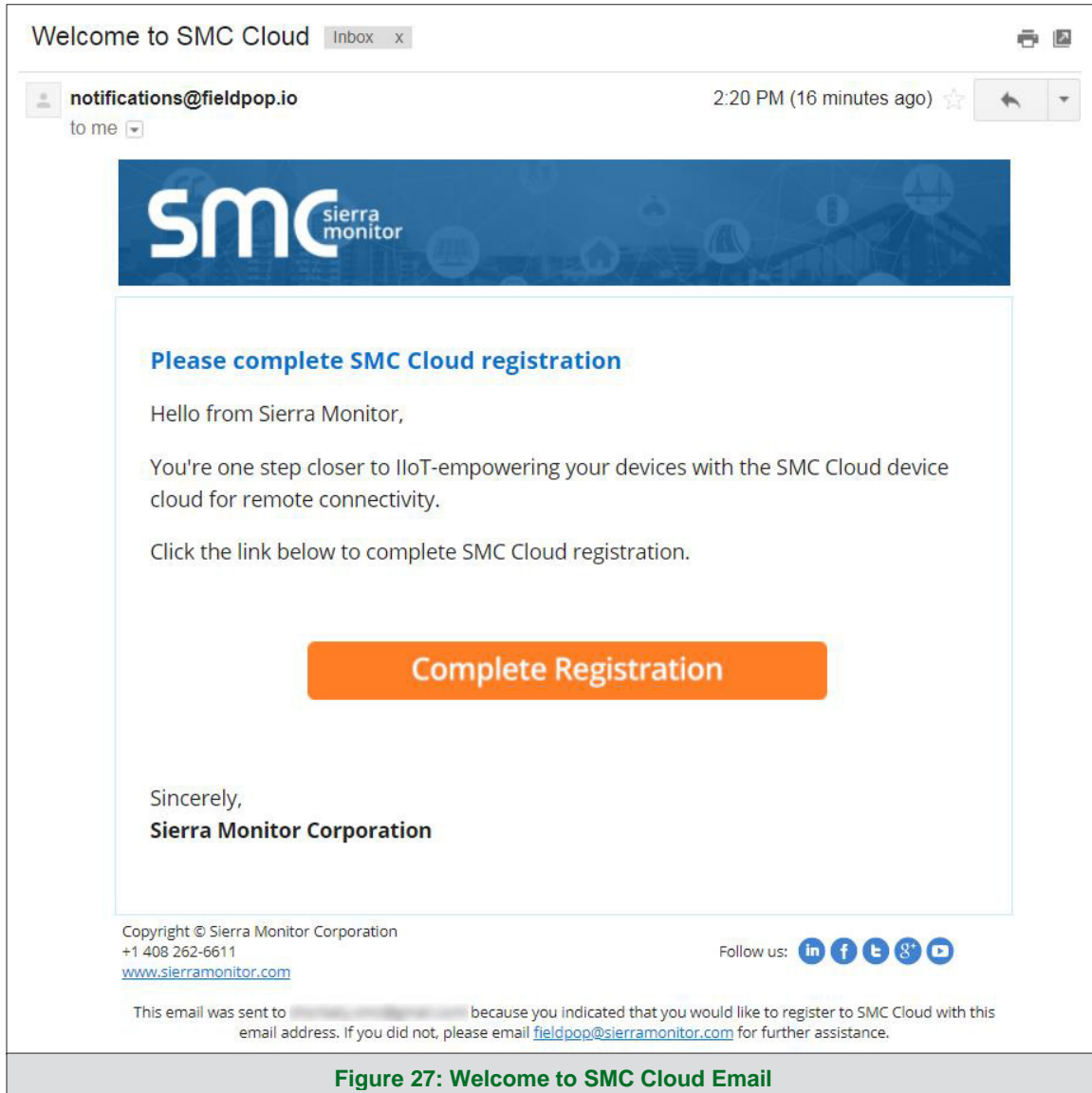
Figure 26: SMC Cloud Opt Out Warning Window

NOTE: If SMC Cloud integration with the ProtoNode 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 SMC Cloud a user account must be created. Request an invitation to SMC Cloud from the manufacturer's support team and follow the instructions below to set up login details:

- The "Welcome to SMC Cloud" email will appear as shown below.



NOTE: If no SMC Cloud 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.

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

Complete Your Registration

Email Address
user@gmail.com

First Name *

Last Name *

Phone Number *

New Password *

Confirm Password *

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

* Mandatory Fields

Save Cancel

Figure 28: 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 SMC Cloud user credentials have been generated, the ProtoNode can be registered onto the SMC Cloud server.

- When first logging onto the ProtoNode, the Web App will open on the SMC Cloud™ page.

NOTE: If a warning message appears instead, go to **Section 11.6** to resolve the connection issue.

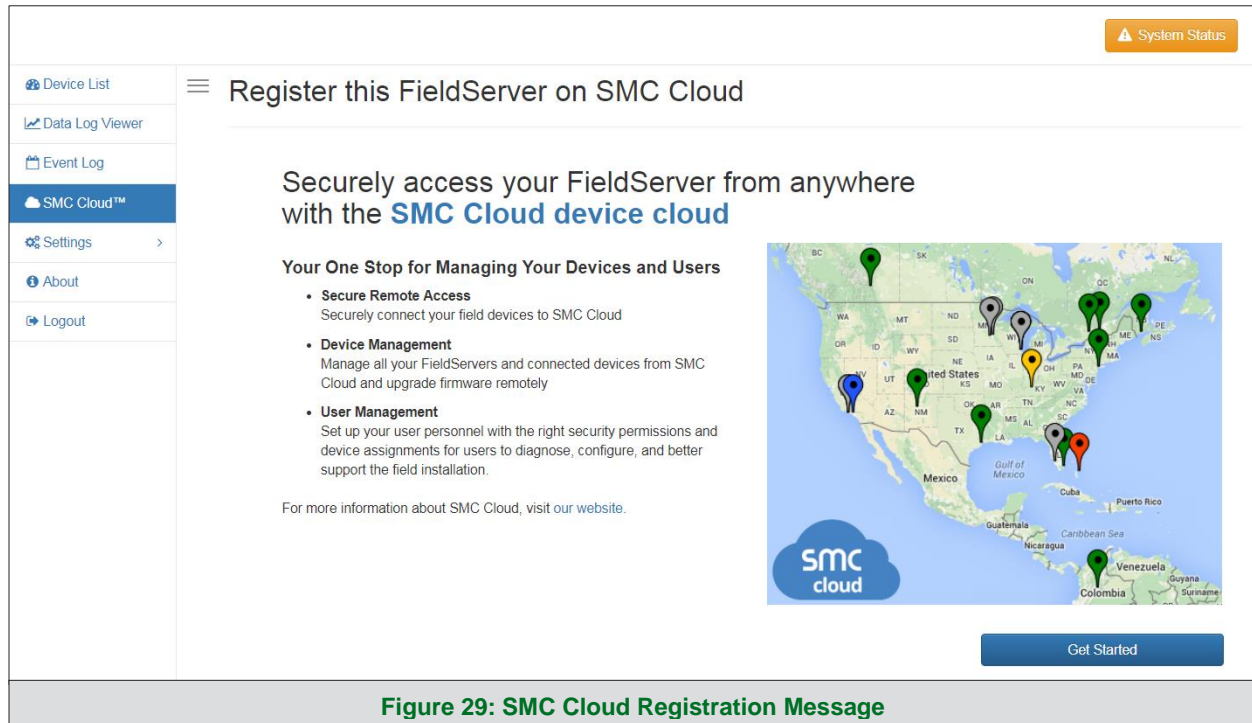
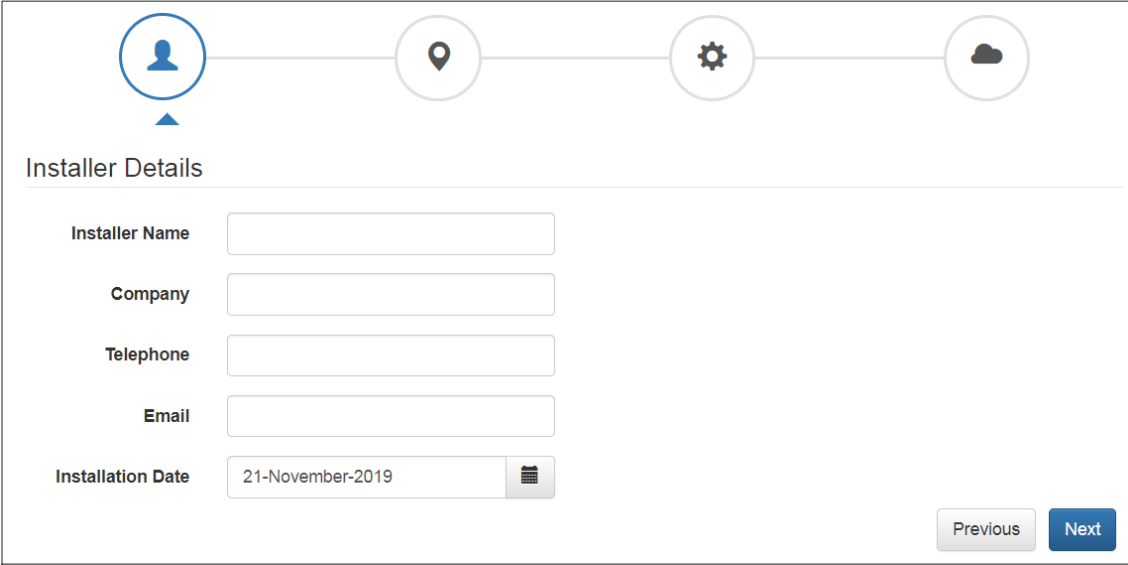


Figure 29: SMC Cloud Registration Message

- Click Get Started to view the SMC Cloud registration page.

NOTE: For information on the System Status button, go to **Section 11.7**.

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



Installer Details

Installer Name

Company

Telephone

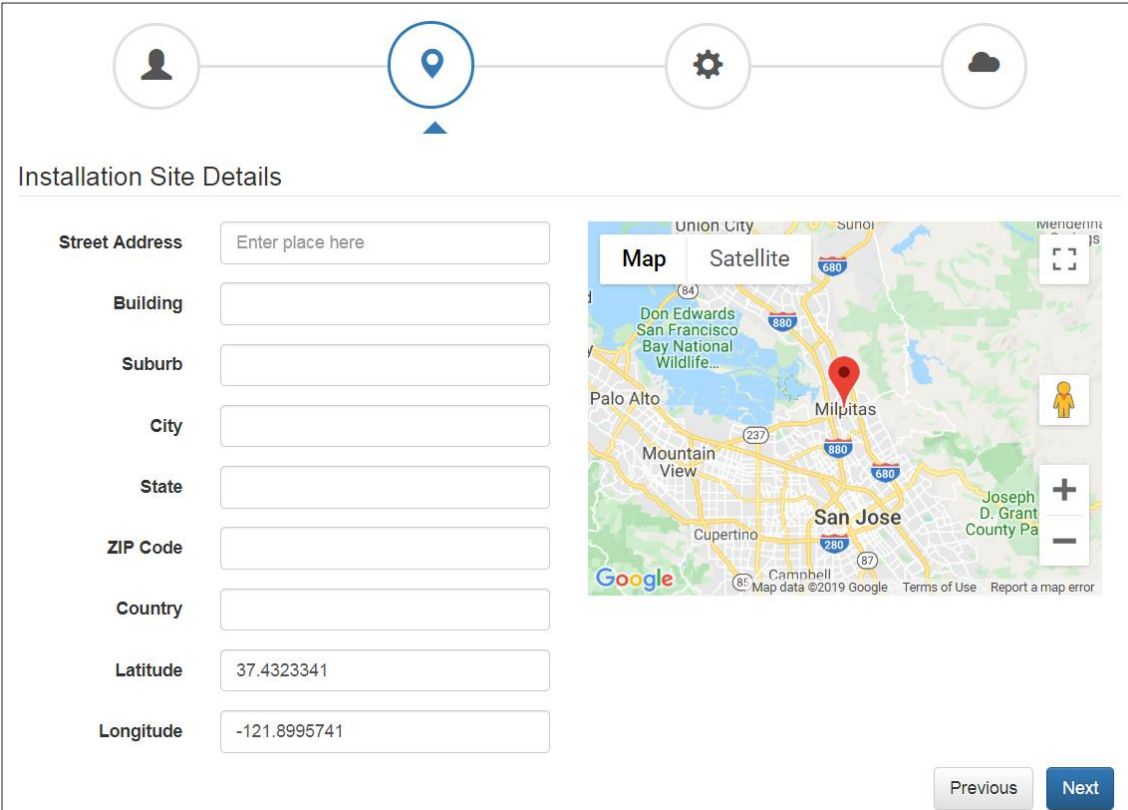
Email

Installation Date

[Previous](#) [Next](#)

Figure 30: SMC Cloud Registration – Installer Details

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



Installation Site Details

Street Address

Building

Suburb

City

State

ZIP Code

Country

Latitude

Longitude

[Previous](#) [Next](#)

Figure 31: SMC Cloud Registration – Site Details

- Enter Name and Description (required) then click Next

Gateway Details

Name

Description

Info Optionally specify any other information relating to the device i.e., calibration, commissioning or other notes

Device Information

Product Name: System View

Product Version: 2.2.5-beta

Platform Name: Gateway

Product BIOS: 4.1.0

Serial Number: 19102TB001PCR

Previous Next

Figure 32: SMC Cloud Registration – Gateway Details

- Enter user credentials and click Register Device

New Users

If you do not have SMC Cloud credentials, you can create a new SMC Cloud account now [Create an SMC Cloud account](#)

Existing Users - Enter device registration details

User Credentials

Username

Password

Previous Register Device

Figure 33: SMC Cloud Registration – SMC Cloud Account

- 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 ProtoNode.

Device Registered

Gateway Details

Name: FieldServer

Description: Gateway

Device Info:

MAC Address: 00:50:4E:60:06:3C

Tunnel Server URL: tunnel.fieldpop.io

Device ID: daffodilsentry_ylb4Xr5bQ

Product Name: CN1853-System View

Product Version: 2.2.5-beta

Installer Details

Installer Name: User

Company: Sierra Monitor Corp

Telephone:

Email:

Installation Date: Nov 21, 2019

Site Installation Details

Street Address: 1991 Tarob Court

Building Info: SMC Build #1

City: Milpitas

Suburb: Milpitas

State: CA

Country: United States

ZIP Code: 95035

Update Device Details

Figure 34: Device Registered for SMC Cloud

NOTE: Update these details at any time by going to the SMC Cloud™ tab and clicking the Update Device Details button.

7.4 Login to SMC Cloud

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

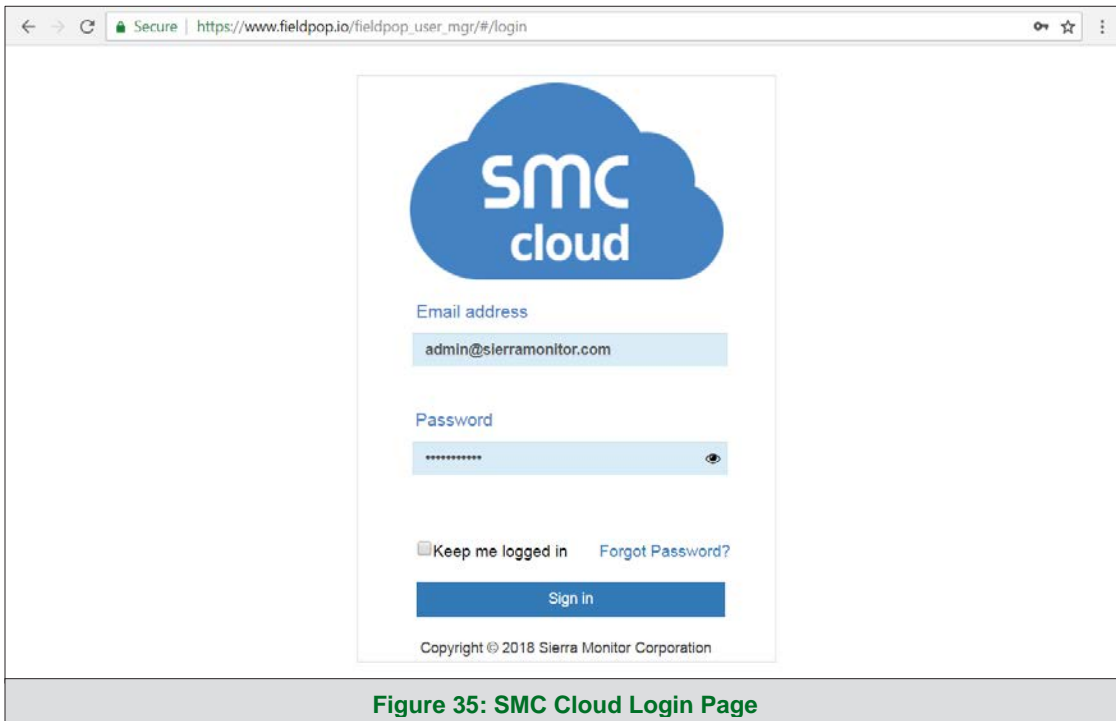


Figure 35: SMC Cloud Login Page

NOTE: If the login password is lost, see the [SMC Cloud Start-up Guide](#) for recovery instructions.

On first login, the Privacy Policy window will appear. Read the Terms of Service, click the checkbox to accept the terms and then click the Continue button to access SMC Cloud.

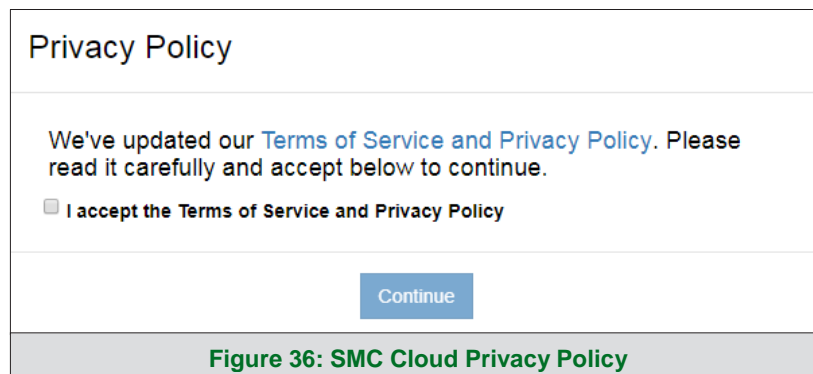


Figure 36: SMC Cloud Privacy Policy

NOTE: For additional SMC Cloud instructions see the [SMC Cloud Start-up Guide](#).



8 Configure the ProtoNode

8.1 Navigate to the ProtoNode Web Configurator

- From the Web App landing page (**Figure 38**), click the Settings tab and then click Configuration.

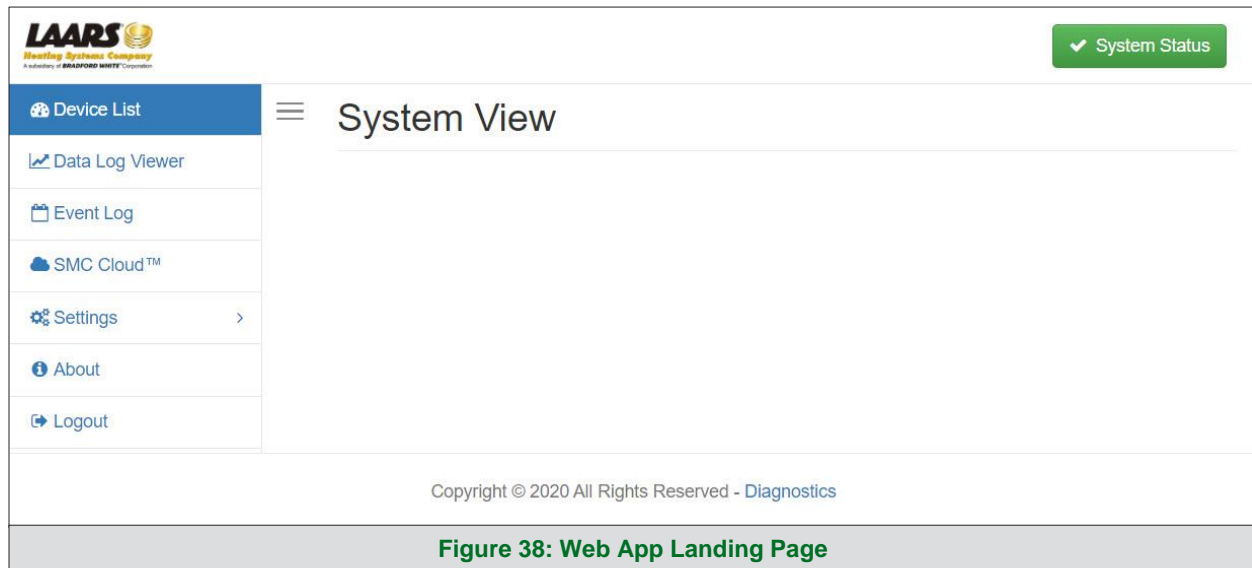


Figure 38: Web App Landing Page

NOTE: For information on the System Status button, go to Section 11.7.

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

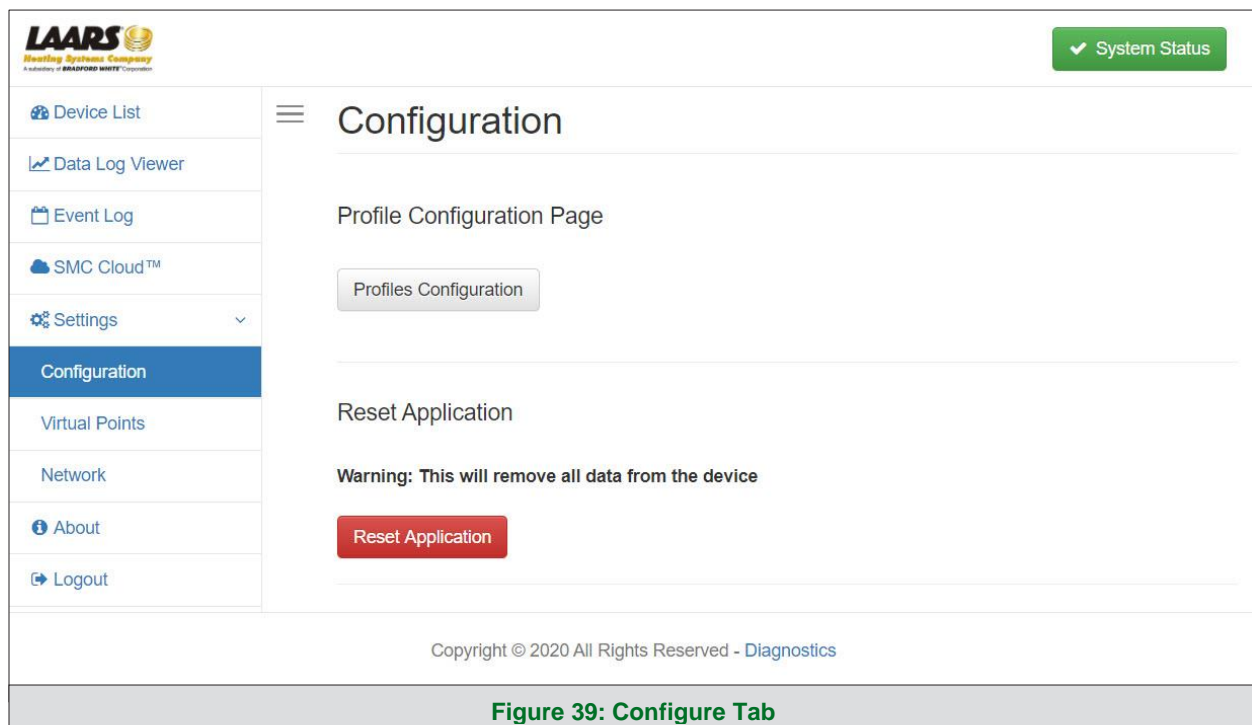
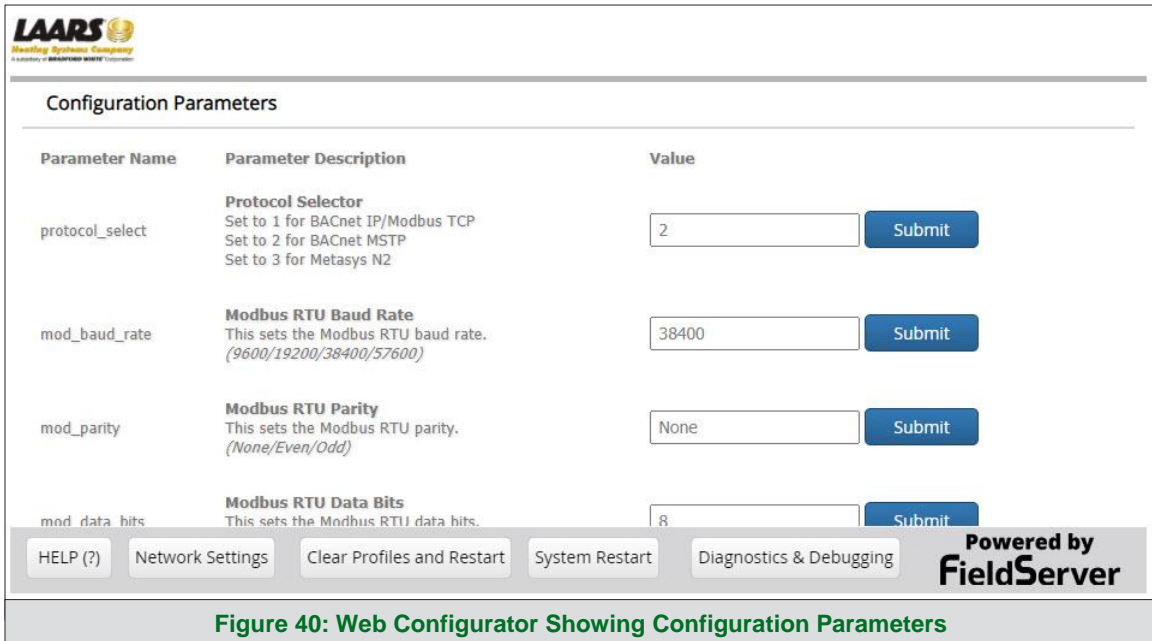


Figure 39: Configure Tab

NOTE: For Web App instructions to the System View, Data Log Viewer, Event Logger and Virtual Points functions, see the [SMC Cloud Start-up Guide](#).

8.2 Select Field Protocol and Set Configuration Parameters

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



The screenshot shows the LAARS Web Configurator interface. At the top left is the LAARS logo with the tagline 'Heating Systems Company'. Below it is a 'Configuration Parameters' section with a table of settings. Each row includes a parameter name, a description, a value input field, and a 'Submit' button. The parameters shown are: protocol_select (set to 2), mod_baud_rate (set to 38400), mod_parity (set to None), and mod_data_bits (set to 8). At the bottom of the configuration area are five buttons: 'HELP (?)', 'Network Settings', 'Clear Profiles and Restart', 'System Restart', and 'Diagnostics & Debugging'. To the right of these buttons is a 'Powered by FieldServer' logo.

Parameter Name	Parameter Description	Value
protocol_select	Protocol Selector Set to 1 for BACnet IP/Modbus TCP Set to 2 for BACnet MSTP Set to 3 for Metasys N2	2
mod_baud_rate	Modbus RTU Baud Rate This sets the Modbus RTU baud rate. (9600/19200/38400/57600)	38400
mod_parity	Modbus RTU Parity This sets the Modbus RTU parity. (None/Even/Odd)	None
mod_data_bits	Modbus RTU Data Bits This sets the Modbus RTU data bits.	8

Buttons: HELP (?), Network Settings, Clear Profiles and Restart, System Restart, Diagnostics & Debugging

Powered by FieldServer

Figure 40: 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.

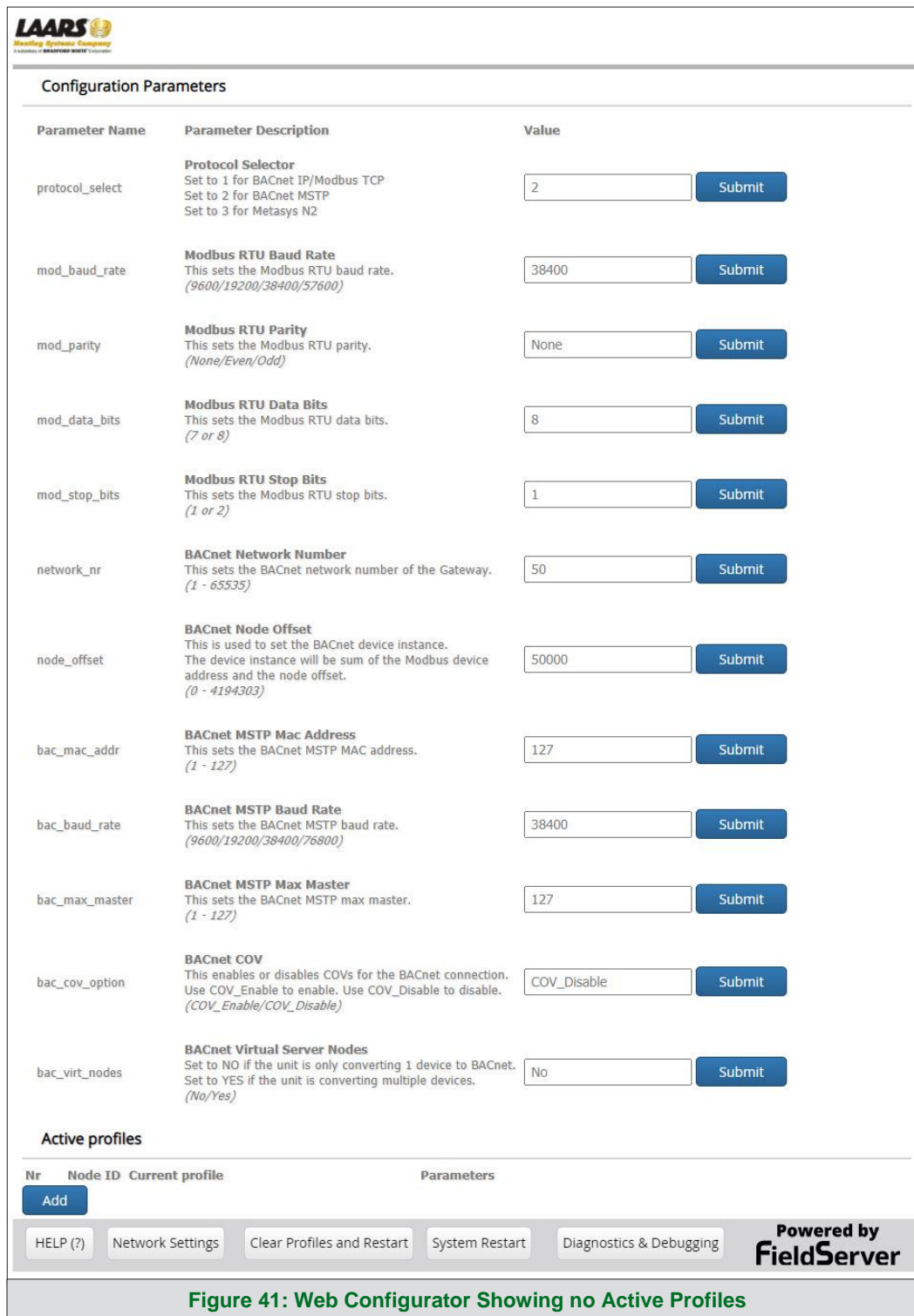
NOTE: If Modbus TCP/IP was selected and is used for the field protocol, skip Section 8.3. Device profiles are NOT used for Modbus TCP/IP.

- 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 ProtoNode, set the BACnet Virtual Server Nodes field to “Yes”; otherwise leave the field on the default “No” setting.

8.3 Setting ProtoNode 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 41)



LAARS
Heating Systems Company
A subsidiary of BRIDGEMOUNT WHITE Corporation

Configuration Parameters

Parameter Name	Parameter Description	Value
protocol_select	Protocol Selector Set to 1 for BACnet IP/Modbus TCP Set to 2 for BACnet MSTP Set to 3 for Metasys N2	2 <input type="button" value="Submit"/>
mod_baud_rate	Modbus RTU Baud Rate This sets the Modbus RTU baud rate. (9600/19200/38400/57600)	38400 <input type="button" value="Submit"/>
mod_parity	Modbus RTU Parity This sets the Modbus RTU parity. (None/Even/Odd)	None <input type="button" value="Submit"/>
mod_data_bits	Modbus RTU Data Bits This sets the Modbus RTU data bits. (7 or 8)	8 <input type="button" value="Submit"/>
mod_stop_bits	Modbus RTU Stop Bits This sets the Modbus RTU stop bits. (1 or 2)	1 <input type="button" value="Submit"/>
network_nr	BACnet Network Number This sets the BACnet network number of the Gateway. (1 - 65535)	50 <input type="button" value="Submit"/>
node_offset	BACnet Node Offset This is used to set the BACnet device instance. The device instance will be sum of the Modbus device address and the node offset. (0 - 4194303)	50000 <input type="button" value="Submit"/>
bac_mac_addr	BACnet MSTP Mac Address This sets the BACnet MSTP MAC address. (1 - 127)	127 <input type="button" value="Submit"/>
bac_baud_rate	BACnet MSTP Baud Rate This sets the BACnet MSTP baud rate. (9600/19200/38400/76800)	38400 <input type="button" value="Submit"/>
bac_max_master	BACnet MSTP Max Master This sets the BACnet MSTP max master. (1 - 127)	127 <input type="button" value="Submit"/>
bac_cov_option	BACnet COV This enables or disables COVs for the BACnet connection. Use COV_Enable to enable. Use COV_Disable to disable. (COV_Enable/COV_Disable)	COV_Disable <input type="button" value="Submit"/>
bac_virt_nodes	BACnet Virtual Server Nodes Set to NO if the unit is only converting 1 device to BACnet. Set to YES if the unit is converting multiple devices. (No/Yes)	No <input type="button" value="Submit"/>

Active profiles

Nr	Node ID	Current profile	Parameters
<input type="button" value="Add"/>			

Powered by FieldServer

Figure 41: Web Configurator Showing no Active Profiles

- 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.

Figure 42: Profile Selection Menu

- 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 43**.

Figure 43: Web Configurator Showing Active Profile Additions

8.4 Verify Device Communications

- Check that the port TX1 and RX1 LEDs are rapidly flashing. See **Section 10.4** for additional LED information and images.
- Confirm the software shows good communications without errors (**Section 10.2**).

8.5 BACnet: Setting Node_Offset to Assign Specific Device Instances

- Follow the steps outlined in **Section 5.1** to access the ProtoNode 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:

$$\text{Device Instance (desired)} = \text{Node_Offset} + \text{Node_ID}$$

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:

$$50,001 = \text{Node_Offset} + 1$$

$$\Rightarrow 50,000 = \text{Node_Offset}$$

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.

The screenshot shows a web form titled "BACnet Node Offset". It includes a label "node_offset", a descriptive text block stating "This is used to set the BACnet device instance. The device instance will be sum of the Modbus device address and the node offset. (0 - 4194303)", a text input field containing the value "50000", and a blue "Submit" button.

Figure 44: Web Configurator Node Offset Field

The screenshot shows the "Active profiles" section of the web configurator. It contains a table with three columns: "Nr", "Node ID", and "Current profile". There are three rows of active profiles, each with a "Remove" button. Below the table is an "Add" button. At the bottom, there is a navigation bar with buttons for "HELP (?)", "Network Settings", "Clear Profiles and Restart", "System Restart", and "Diagnostics & Debugging". The "Powered by FieldServer" logo is also present.

Nr	Node ID	Current profile	Parameters
1	1	BAC_MSTP_HTD	
2	22	BAC_MSTP_OmniTherm	
3	33	BAC_MSTP_Sola_Deg_F	

Figure 45: Active Profiles

8.6 How to Start the Installation Over: Clearing Profiles

- Follow the steps outlined in **Section 5.1** to access the ProtoNode 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 LonWorks (FPC-N35): Commissioning ProtoNode on a LonWorks Network

Commissioning may only be performed by the LonWorks administrator.

9.1 Commissioning ProtoNode FPC-N35 on a LonWorks Network

During the commissioning process, the LonWorks administrator may prompt the user to hit the service pin on the ProtoNode FPC-N35 at a specific point (this step occurs at different points of the commissioning process for each LonWorks network management tool).

- If an XIF file is required, see steps in **Section 9.1.1** to generate XIF.




Figure 46: LonWorks Service Pin Location

9.1.1 Instructions to Upload XIF File from ProtoNode FPC-N35 Using Browser

- Connect a Cat-5 Ethernet cable (straight through or cross-over) between the PC and ProtoNode.
- The default IP Address for the ProtoNode is **192.168.1.24**, Subnet Mask is **255.255.255.0**. If the PC and ProtoNode are on different IP networks, assign a static IP Address to the PC on the 192.168.1.xxx network.

For Windows 10:

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

☒ Use the following IP address:

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

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

- Open a web browser and go to the following address: [IP Address of ProtoNode]/fserver.xif
 - Example: 192.168.1.24/fserver.xif
- If the web browser prompts to save the file, save the file onto the PC. If the web browser displays the xif file as a web page, save the file onto the local PC as “fserver.xif”.

```

File: fserver.xif generated by LonDriver Revision 1.30(d), XIF Version 4.0
Copyright (c) 2000-2012 by FieldServer Technologies
All Rights Reserved. Run on Thu Jan 1 00:00:00 1970

90:00:95:47:1E:02:04:7C
2 15 1 4 0 14 11 3 3 12 14 11 11 11 11 3 0 16 63 0 1 11 4
32 5 19 13 28 0 0 15 5 3 109 63
1 7 1 0 4 4 4 15 200 0
78125 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 1 5 8 5 12 14 15
*
"FFP-Lon Demo

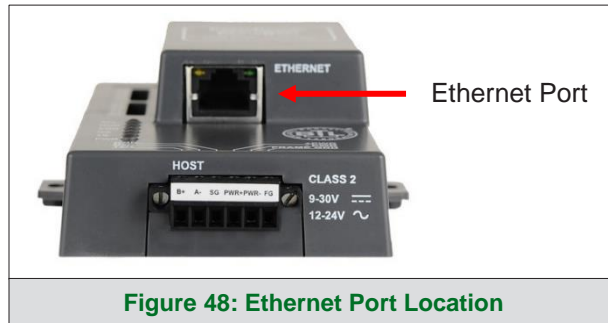
VAR nviAnalog_01 0 0 0 0
0 1 63 0 0 0 0 0 0 0 0 0 0
*
51 * 1
4 0 4 0 0
VAR nvoAnalog_01 1 0 0 0
0 1 63 1 0 0 0 0 0 0 0 0
*
51 * 1
4 0 4 0 0
VAR nviBinary_01 2 0 0 0
0 1 63 0 0 0 0 0 0 0 0 0
*
95 * 2
1 0 0 0 0
1 0 0 1 0
VAR nvoBinary_01 3 0 0 0
0 1 63 1 0 0 0 0 0 0 0 0
*
95 * 2
1 0 0 0 0
1 0 0 1 0
    
```

Figure 47: Sample of Fserver.XIF File Generated

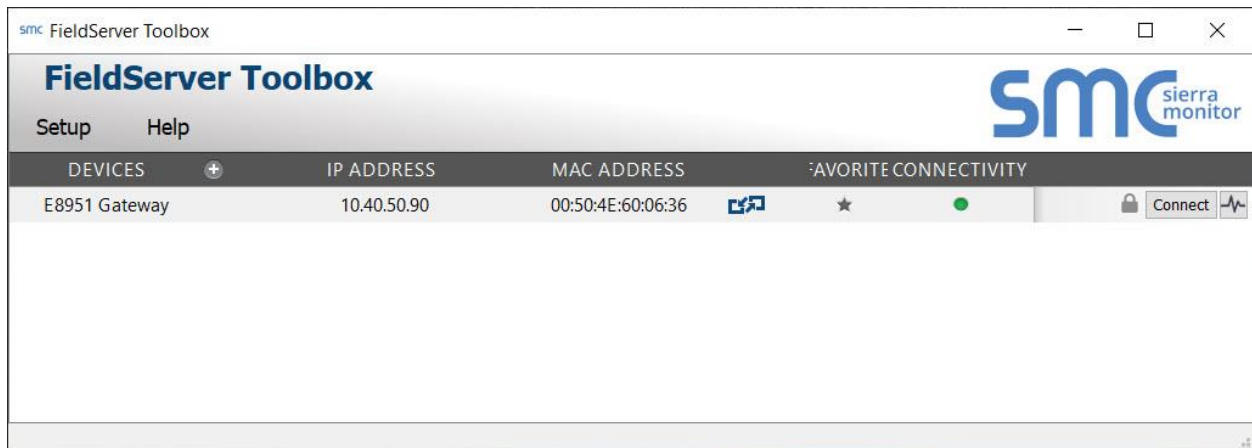
10 Troubleshooting

10.1 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 ProtoNode.
- Double click on the FS Toolbox Utility and click Discover Now on the splash page.
- Check for the IP Address of the desired gateway.



10.2 Viewing Diagnostic Information

- Type the IP Address of the ProtoNode into the web browser or use the FieldServer Toolbox to connect to the ProtoNode.
- 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 10.3** for the relevant wiring and settings.

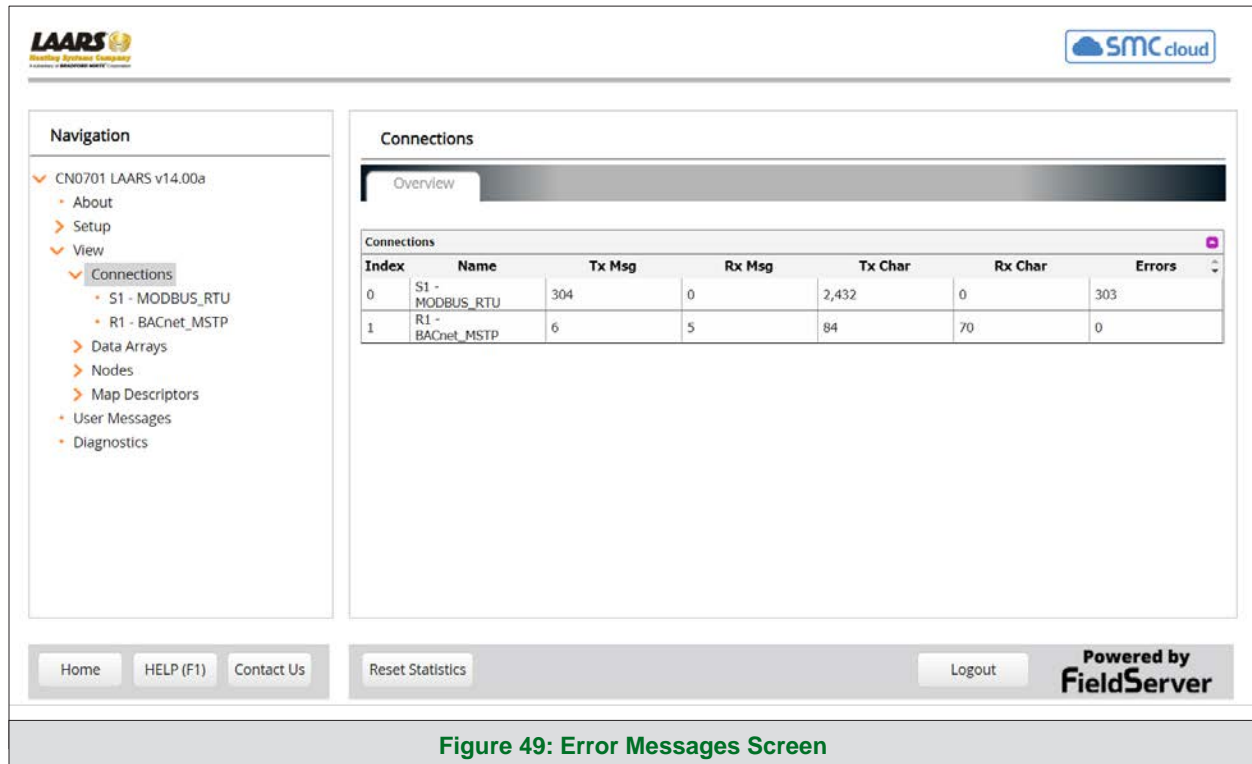


Figure 49: Error Messages Screen

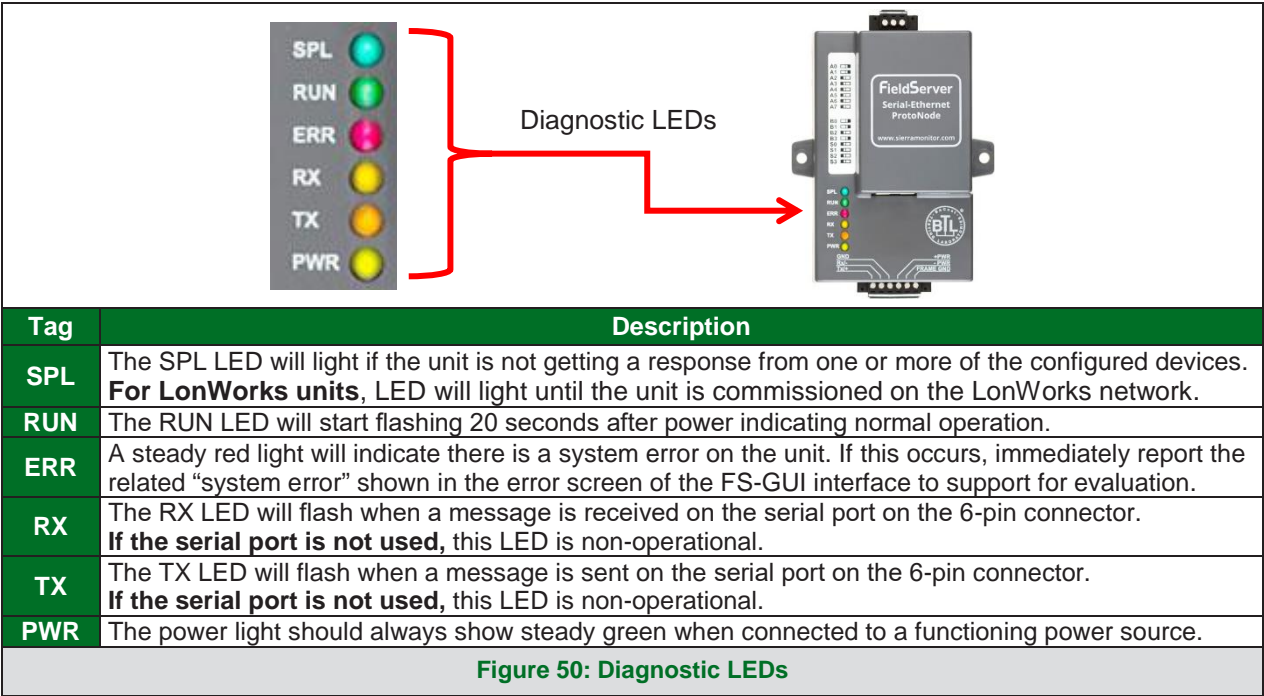
10.3 Checking Wiring and Settings

- No COMS on Modbus RTU side. If the Tx/Rx LEDs are not flashing rapidly then there is a COM issue. To fix this, check the following:
 - Visual observations of LEDs on ProtoNode (**Section 10.4**)
 - Check baud rate, parity, data bits, stop bits
 - Check device address
 - Verify wiring
 - Verify the device was listed in the Web Configurator (**Section 8.3**)
- Field COM problems:
 - Visual observations of LEDs on the ProtoNode (**Section 10.4**)
 - Verify IP Address setting
 - Verify wiring

NOTE: If the problem persists, a Diagnostic Capture needs to be taken and sent to support. (**Section 10.5**)

10.4 LED Diagnostics for Communications Between ProtoNode and Devices


See the diagram below for ProtoNode FPC-N34 and FPC-N35 LED Locations.

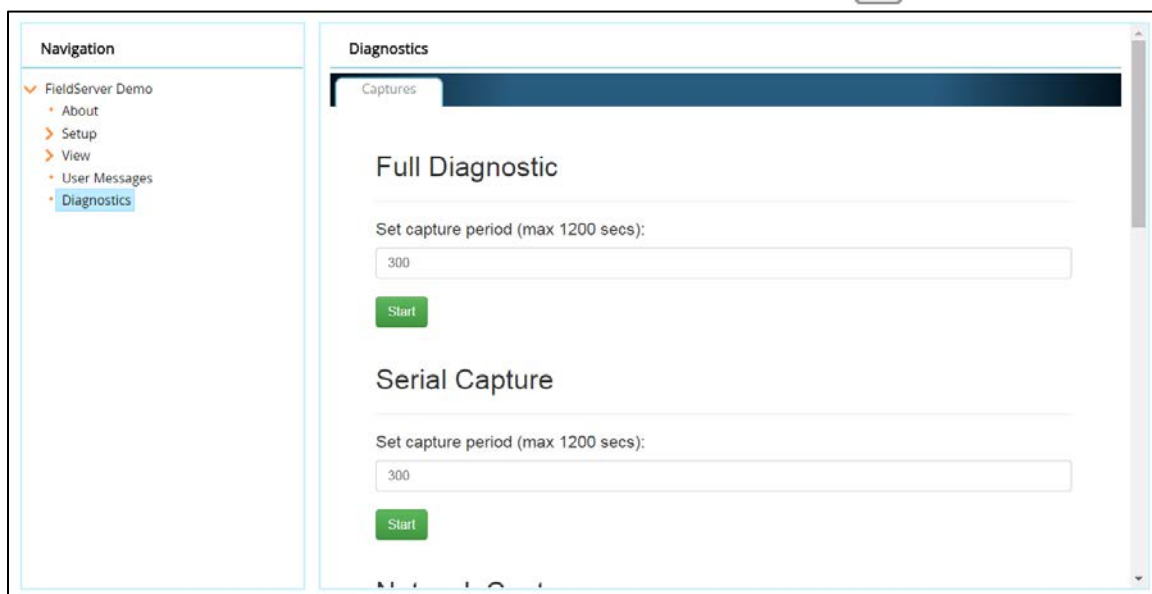


10.5 Taking a FieldServer Diagnostic Capture

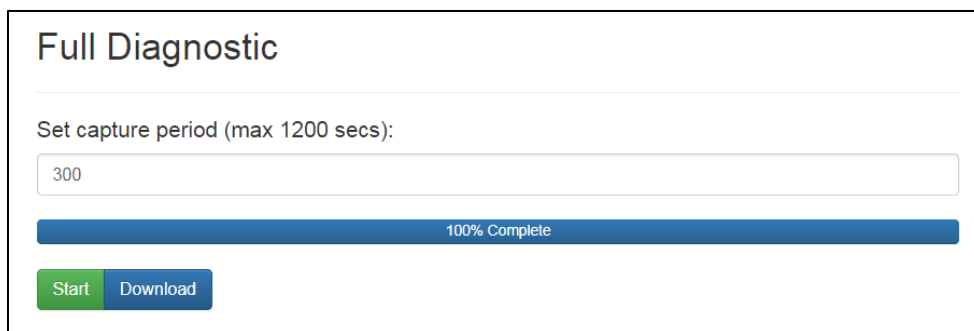
When there is a problem on-site that cannot easily be resolved, perform a Diagnostic Capture before contacting support. Once the Diagnostic Capture is complete, email it to technical support. The Diagnostic Capture will accelerate diagnosis of the problem.

If the FieldServer bios is updated/released on November 2017 or later then the Diagnostic Capture is performed via the gateway's on-board system.

- 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.

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

10.5.1 Taking a Capture with Older Firmware

If the FieldServer firmware is from before November 2017, the Diagnostic Capture can be done by downloading the FieldServer Toolbox software but network connections (such as Ethernet and Wi-Fi) cannot be captured (if a network diagnostic is needed take a Wire Shark capture).

Once the Diagnostic Capture is complete, email it to technical support. The Diagnostic Capture will accelerate diagnosis of the problem.

- 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.

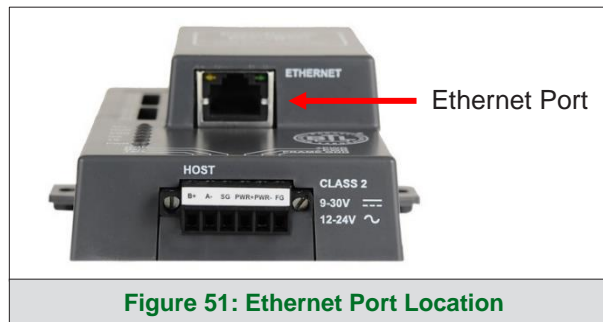

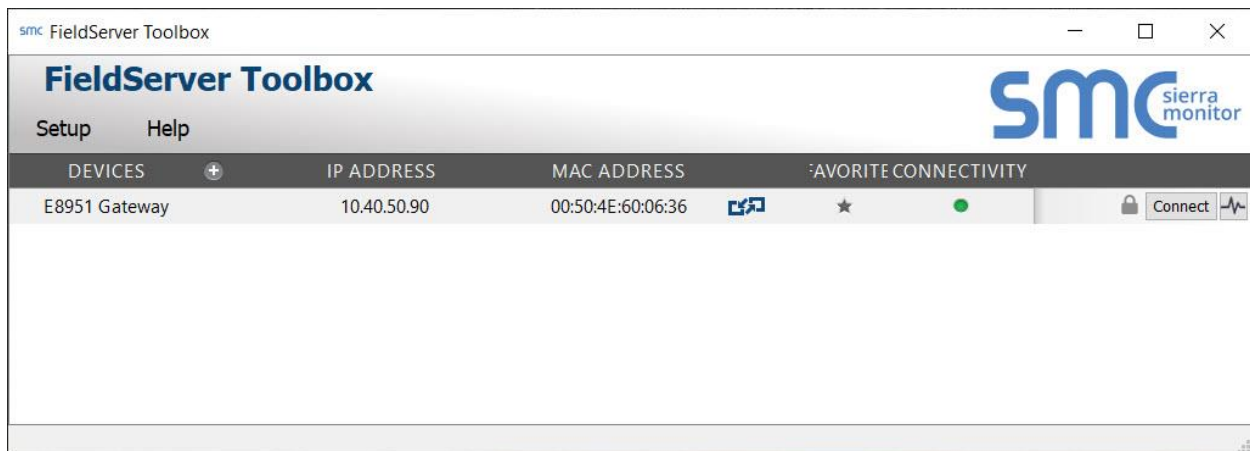


Figure 51: Ethernet Port Location

- Connect a standard Cat-5 Ethernet cable between the PC and ProtoNode.
- Double click on the FS Toolbox Utility.
- **Step 1: Take a Log**
 - Click on the diagnose icon  for the desired device



- Select "Full Diagnostic" from the drop down menu



NOTE: If desired, the default capture period can be changed.

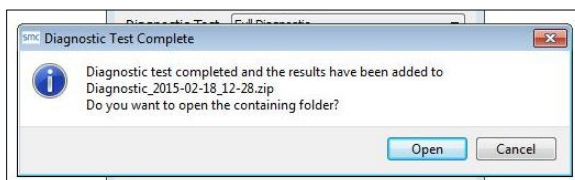
- Click on the Start Diagnostic button



- Wait for the capture period to finish and the Diagnostic Test Complete window will appear

- **Step 2: Send Log**

- Once the diagnostic test is complete, a .zip file is saved on the PC



- Choose "Open" to launch explorer and have it point directly at the correct folder
- Send the Diagnostic zip file to technical support

 Diagnostic_2014-07-17_20-15.zip	2014/07/17 20:16	zip Archive	676 KB
---	------------------	-------------	--------

10.6 Factory Reset Instructions

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

10.7 Internet Browsers Not Supported

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 Additional Information

11.1 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 10.1**)
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.

11.2 BACnet: Setting Network_Number for More Than One ProtoNode on the Subnet

For both BACnet MS/TP and BACnet/IP, if more than one ProtoNode is connected to the same subnet, they must be assigned unique Network_Number values.

On the main Web Configuration screen, update the BACnet Network Number field and click submit. The default value is 50.

network_nr	BACnet Network Number This sets the BACnet network number of the Gateway. (1 - 65535)	50	Submit
------------	--	----	--------

Figure 52: Web Configurator – Network Number Field

11.3 Certification

11.3.1 BTL Mark – BACnet® Testing Laboratory



BACnet is a registered trademark of ASHRAE. ASHRAE does not endorse, approve or test products for compliance with BACnet standards. Compliance of these products to requirements of ASHRAE Standard 135 is the responsibility of the BACnet International. BTL is a registered trademark of the BACnet International.

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

Go to www.BACnetInternational.net for more information about the BACnet Testing Laboratory. Click [here](#) for the BACnet PIC Statement.

NOTE: BACnet is a registered trademark of ASHRAE.

11.3.2 LonMark Certification

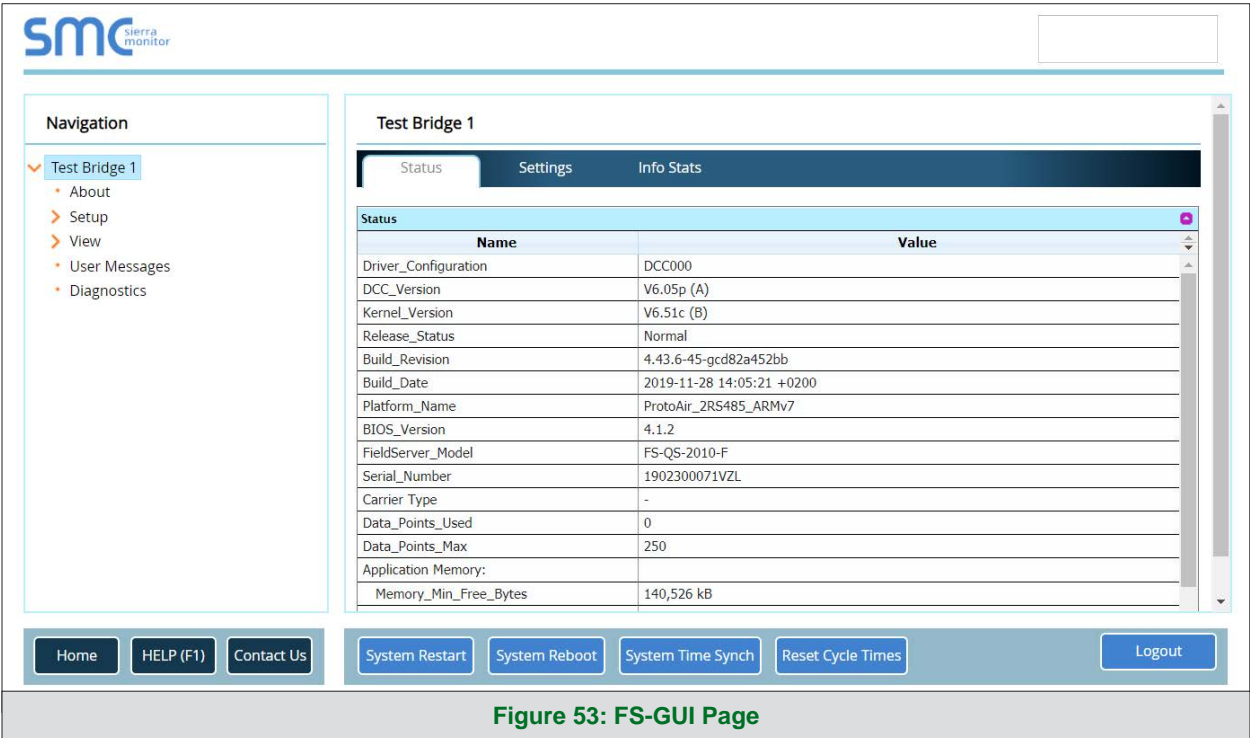


LonMark International is the recognized authority for certification, education, and promotion of interoperability standards for the benefit of manufacturers, integrators and end users. LonMark International has developed extensive product certification standards and tests to provide the integrator and user with confidence that products from multiple manufacturers utilizing LonMark devices work together. MSA Safety has more LonMark Certified gateways than any other gateway manufacturer, including the ProtoCessor, ProtoCarrier and ProtoNode for OEM applications and the full featured, configurable gateways.

11.4 Change Web Server Security Settings After Initial Setup

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

- From the FS-GUI page, click Setup in the Navigation panel.



11.4.1 Change Security Mode

- Click Security in the Navigation panel.

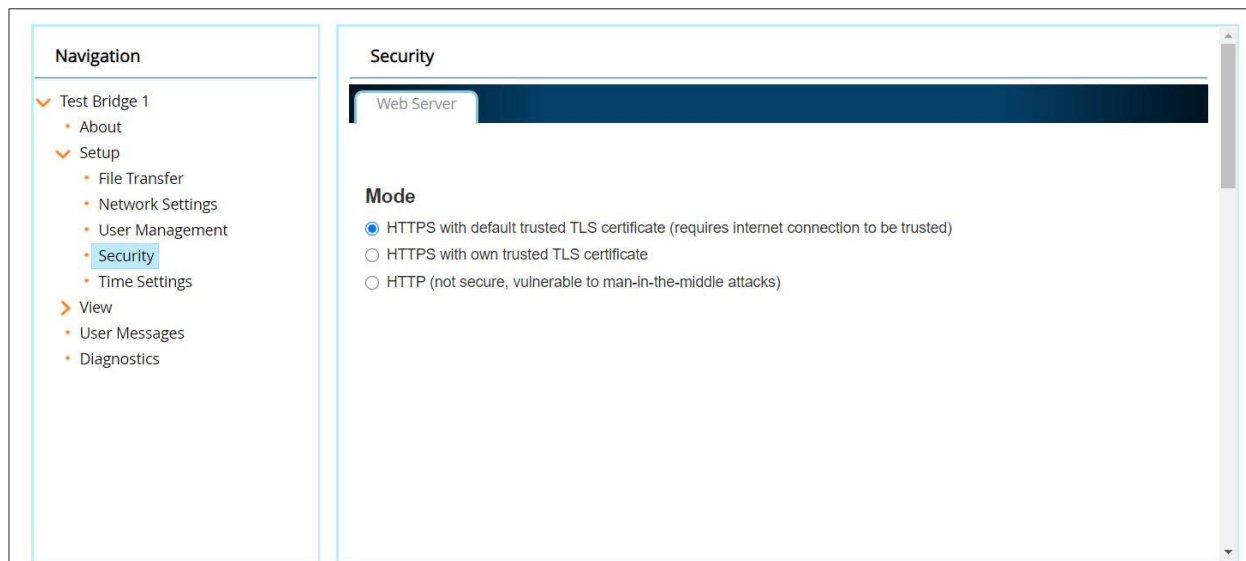


Figure 54: FS-GUI Security Setup

- Click the Mode desired.
 - If HTTPS with own trusted TLS certificate is selected, follow instructions in **Section 5.2.1**
- Click the Save button.

11.4.2 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.

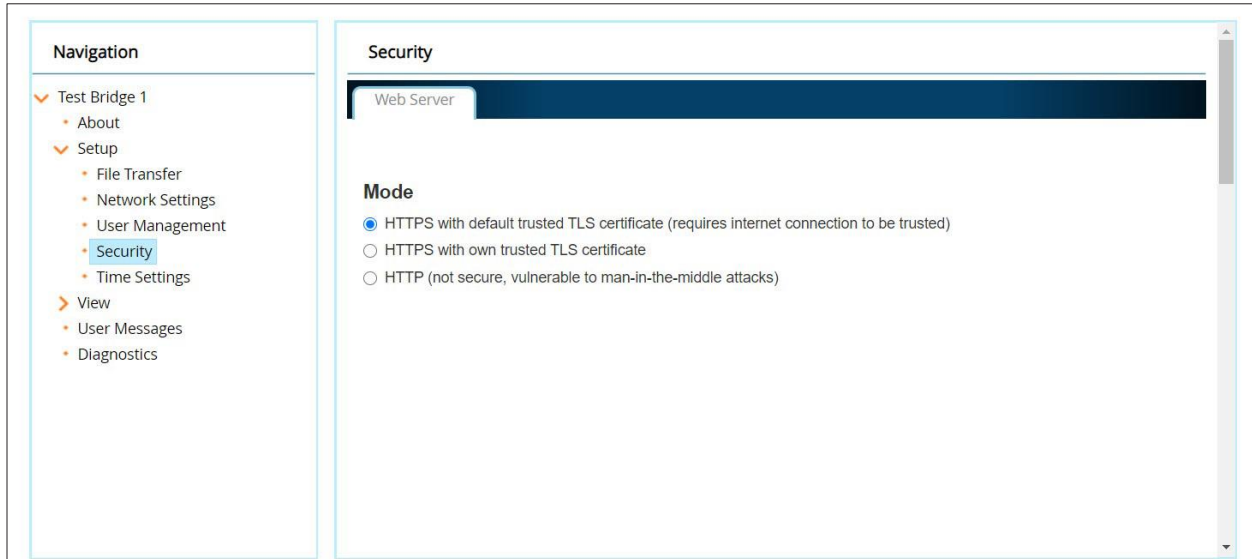


Figure 55: FS-GUI Security Setup – Certificate Loaded

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

11.5 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 ProtoNode, ProtoCessor or ProtoCarrier recovery instructions, see the [FieldServer Recovery Instructions document](#). For ProtoNode FPC-N54, ProtoNode FPC-N64 or ProtoAir 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.

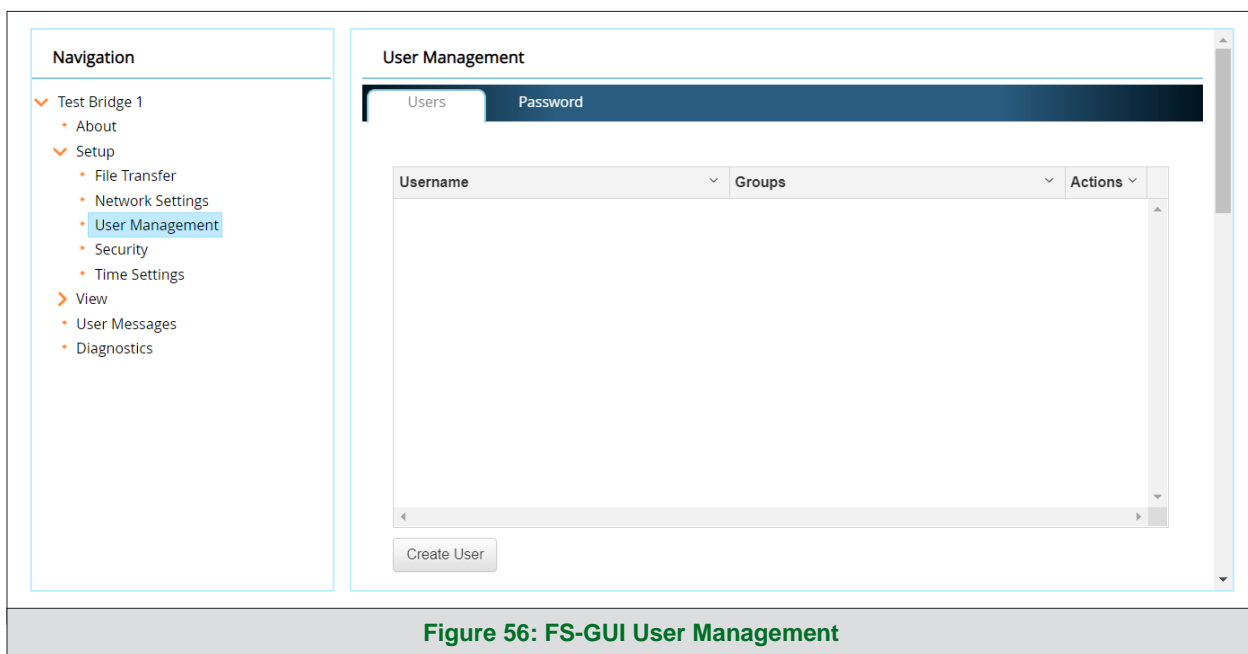


Figure 56: FS-GUI User Management

User Types:

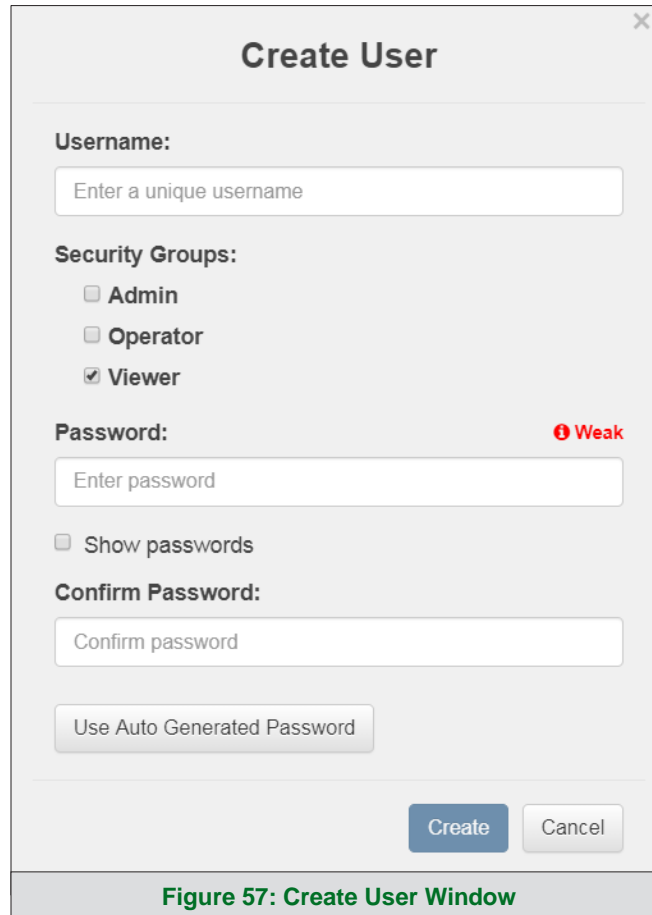
Admin – Can modify and view any settings on the FieldServer.

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

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

11.5.1 Create Users

- Click the Create User button.

A screenshot of the 'Create User' dialog box. The dialog has a title bar with a close button (X). Inside, the 'Username:' section has a text input field with the placeholder 'Enter a unique username'. The 'Security Groups:' section has three checkboxes: 'Admin' (unchecked), 'Operator' (unchecked), and 'Viewer' (checked). The 'Password:' section has a text input field with the placeholder 'Enter password' and a red indicator 'Weak' to its right. Below the password field is a checkbox for 'Show passwords' (unchecked). The 'Confirm Password:' section has a text input field with the placeholder 'Confirm password'. At the bottom left of the form area is a button labeled 'Use Auto Generated Password'. At the bottom right are two buttons: 'Create' (blue) and 'Cancel' (grey).

Create User

Username:

Enter a unique username

Security Groups:

☐ Admin

☐ Operator

☒ Viewer

Password: Weak

Enter password

☐ Show passwords

Confirm Password:

Confirm password

Use Auto Generated Password

Create Cancel

Figure 57: Create User Window

- 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.

11.5.2 Edit Users

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

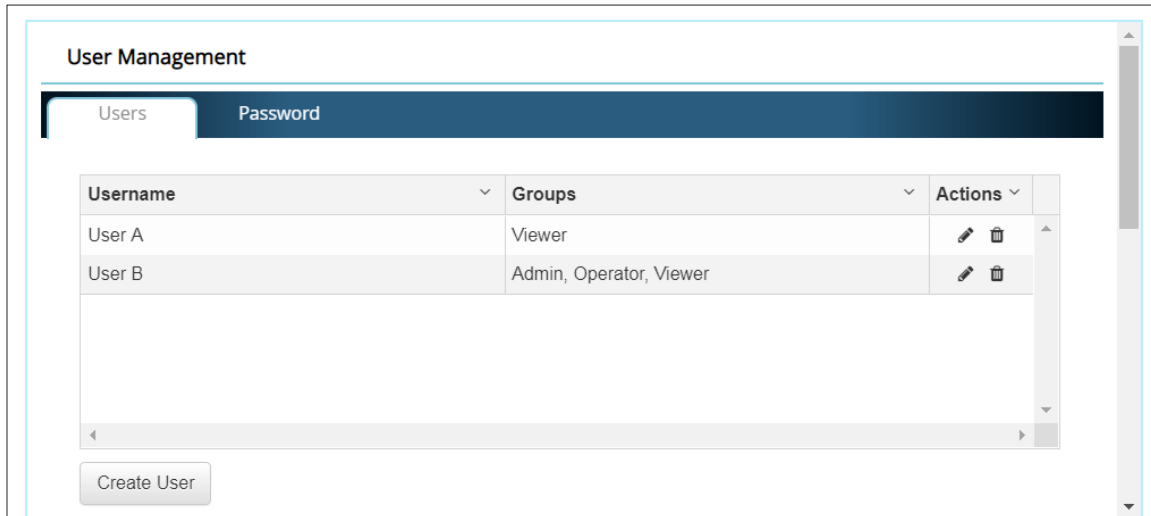


Figure 58: Setup Users

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

The 'Edit User' window contains the following fields and options:

- Username:** A text field containing 'User A'.
- Security Groups:** A list of checkboxes:
 - ☐ Admin
 - ☐ Operator
 - ☒ Viewer
- Password:** A text field containing 'Optional'.
- ☐ Show passwords
- Confirm Password:** A text field containing 'Optional'.
-
-

Figure 59: Edit User Window

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

11.5.3 Delete Users

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

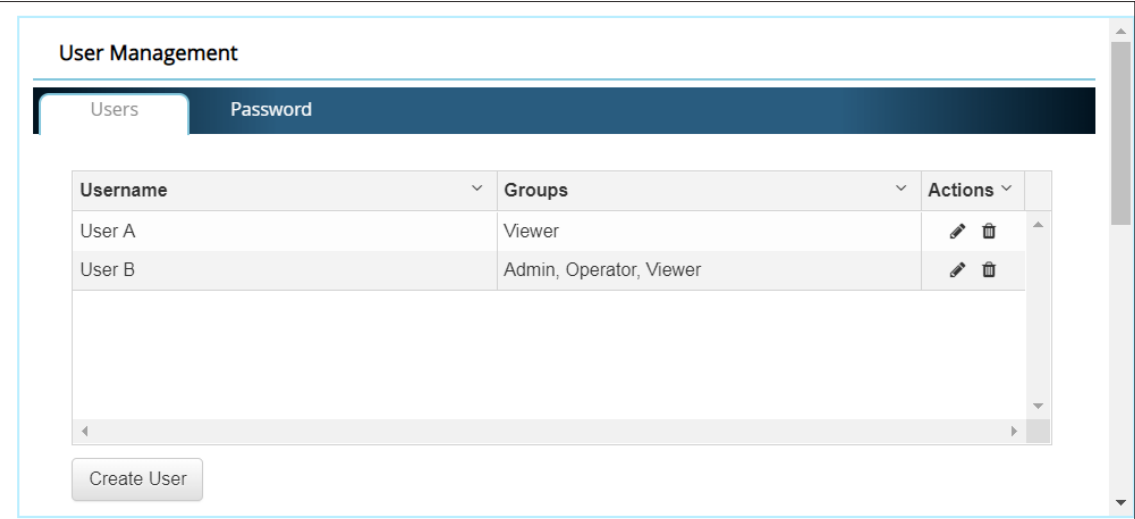


Figure 60: Setup Users

- When the warning message appears, click Confirm.

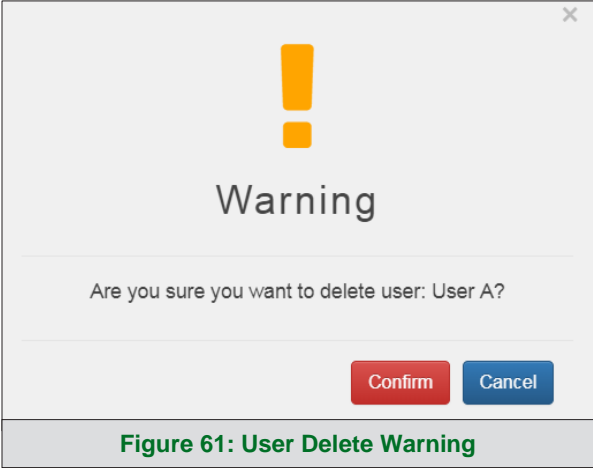


Figure 61: User Delete Warning

11.5.4 Change FieldServer Password

- Click the Password tab.

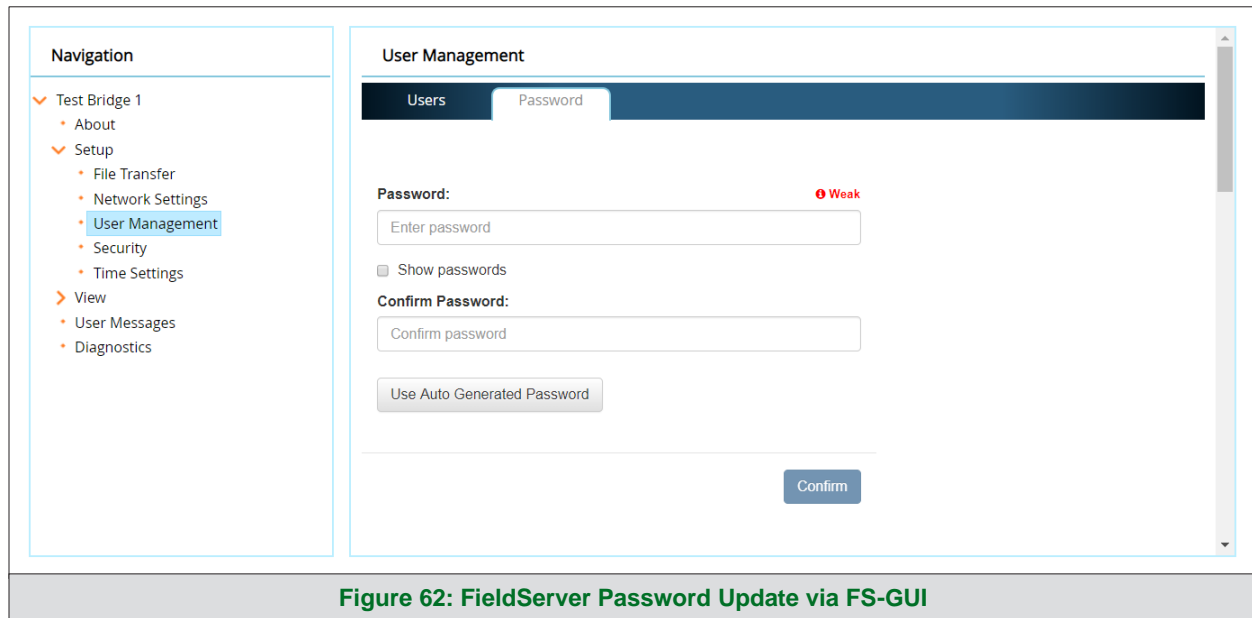


Figure 62: FieldServer Password Update via FS-GUI

- 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.

11.6 SMC Cloud Connection Warning Message

- If a warning message appears instead of the page as shown in **Figure 29**, follow the suggestion that appears on screen.
 - If the ProtoNode cannot reach the SMC Cloud server, the following message will appear

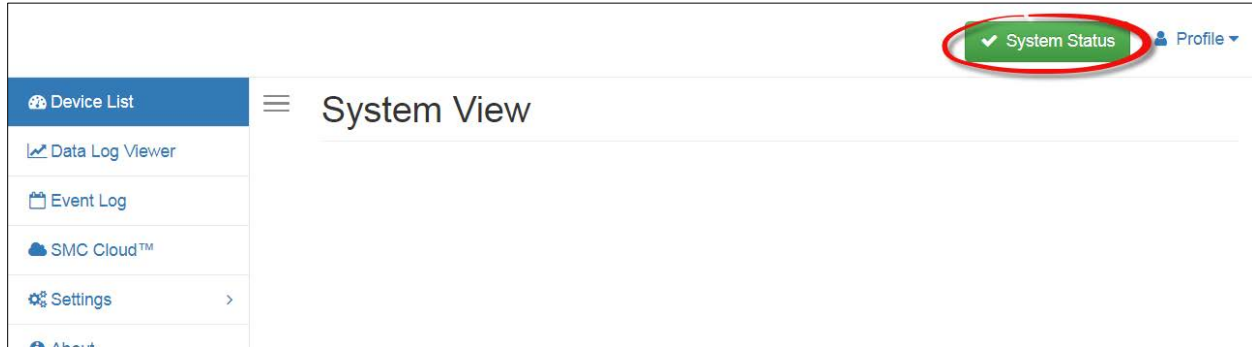


- Follow the directions presented in the warning message.
 - Go to the network settings by clicking the Settings tab and then click the Network tab
 - Check with the site's IT support that the DNS settings are setup correctly
 - Ensure that the ProtoNode is properly connected to the Internet

NOTE: If changes to the network settings are done, remember to click the **Save** button. Then power cycle the FieldServer by clicking on the **Confirm** button in the window and click on the bolded "Restart" text in the yellow pop-up box that appears in the upper right corner of the screen.

11.7 System Status Button

The System Status Button can be found on any page of the web apps. This shows the level of alert/functionality for the customer device. This is an aggregate of the Web App page's resource usage upon the local PC or mobile device, SMC Cloud connectivity and device alert level.



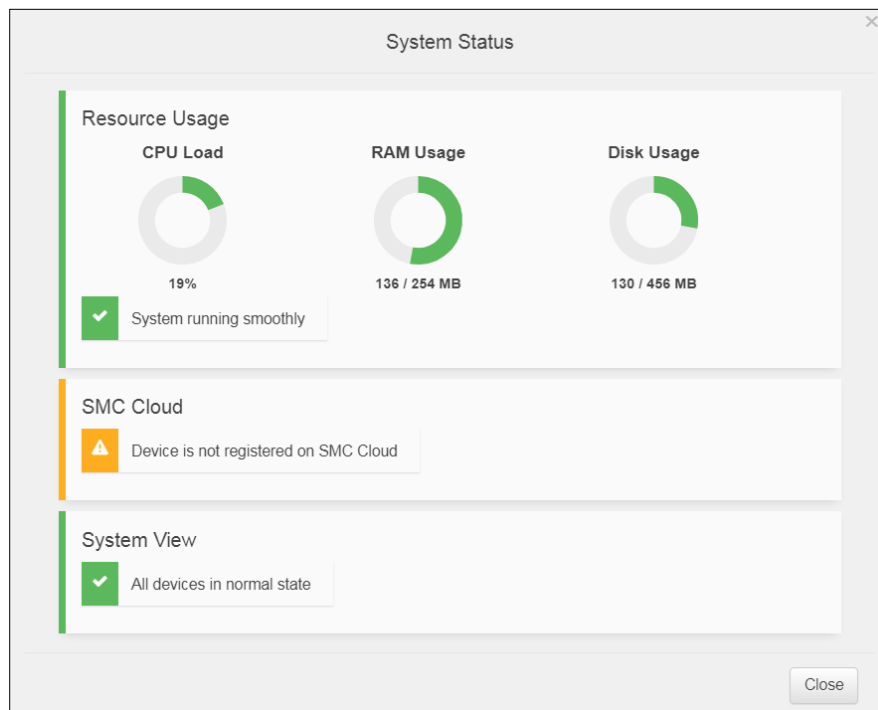
The color of the button represents the status of one to all three systems:

Green – Normal status

Yellow – Warning status

Red – Alarm status

Click on the System Status Button to open the System Status window, showing more details on the status of each system.




NOTE: If it was selected to opt out of SMC Cloud (Figure 26), the SMC Cloud status will not show in the System Status window. This means the status will show as green even if the gateway is not connected to SMC Cloud.

11.8 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.

ETH 1

Routing 

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

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

Interface	Destination Network	Netmask	Gateway IP Address	Priority 	
ETH 	Default	-	10.40.50.1	255	
ETH 	<input type="text" value="10.40.50.10"/>	<input type="text" value="255.255.255.255"/>	<input type="text" value="10.40.50.12"/>	<input type="text" value="100"/>	

+ Add Rule

Cancel

Save

There are unsaved settings

Figure 64: Routing Settings

12 Vendor Information – LAARS

See the document 'Vendor Protocol Mapping' in the document library on laars.com, for all the devices referenced in this manual. Only the protocols listed as supported for this FieldServer are supported (see Section 1.1). Ignore all points referring to unsupported protocols when using this FieldServer.

13 Specifications



	ProtoNode FPC-N34	ProtoNode FPC-N35
Electrical Connections	One 6-pin Phoenix connector with: RS-485 port (+ / - / gnd) Power port (+ / - / Frame-gnd) One 3-pin Phoenix connector with RS-485 port (+ / - / gnd) One Ethernet 10/100 BaseT port	One 6-pin Phoenix connector with: RS-485 port (+ / - / gnd) Power port (+ / - / Frame-gnd) One 2-pin Phoenix connector with: One FTT-10 LonWorks port One Ethernet 10/100 BaseT port
Approvals	CE certified; UL 916 approved; WEEE compliant; REACH compliant; EN 50491-3 and CSA C22-2 standards; FCC Class A Part 15; DNP 3.0 conformance tested; RoHS 3 compliant; CSA 205 approved	
	BTL Marked	LonMark Certified
Power Requirements	9-30VDC or 12-24VAC	
Physical Dimensions	11.5 cm L x 8.3 cm W x 4.1 cm H (4.5 x 3.2 x 1.6 in.)	
Weight	0.2 kg (0.4 lbs)	
Operating Temperature	-40°C to 75°C (-40°F to 167°F)	
Surge Suppression	EN61000-4-2 ESD EN61000-4-3 EMC EN61000-4-4 EFT	
Humidity	5-90% RH (non-condensing)	
(Specifications subject to change without notice)		
Figure 65: Specifications		

Warning: This equipment is compliant with Class A of CISPR 32. In a residential environment, this equipment may cause radio interference.

13.1 Compliance with UL Regulations

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

- The units shall be powered by listed LPS or Class 2 power supply suited to the expected operating temperature range.
- The interconnecting power connector and power cable shall:
 - Comply with local electrical code
 - Be suited to the expected operating temperature range
 - Meet the current and voltage rating for the ProtoNode
- 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.

14 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.

H2354400L