



FieldServer

QuickServer Start-up Guide

FS-QS-2XX0-F



APPLICABILITY & EFFECTIVITY

Effective for all systems manufactured after May 2020.

Document Revision: 1.K
T18627

Technical Support

ProSoft Technology, Inc. is a provider of FieldServer QuickServers.

For Technical Support call

+1 661.716.5100

TABLE OF CONTENTS

- 1 QuickServer Description..... 6**
- 2 Certifications 6**
 - 2.1 BTL Mark – BACnet Testing Laboratory 6
- 3 Supplied Equipment 6**
- 4 QuickServer Setup..... 7**
 - 4.1 Mounting..... 7
 - 4.2 DIP Switch Settings 8
 - 4.2.1 Bias Resistors..... 8
 - 4.2.2 Termination Resistor 9
 - 4.3 Connecting the R1 Port 10
 - 4.3.1 Wiring 10
 - 4.3.2 Supported RS-485 Baud Rates by Protocol..... 10
 - 4.4 Power Up the Device..... 11
- 5 Connect the PC to the QuickServer 12**
 - 5.1 Connecting to the Gateway via Ethernet..... 12
 - 5.1.1 Changing the Subnet of the Connected PC 12
 - 5.2 Navigate to the EZ Gateway Login Page 12
- 6 Setup Web Server Security 13**
 - 6.1 Login to the FieldServer 13
 - 6.2 Select the Security Mode..... 15
 - 6.2.1 HTTPS with Own Trusted TLS Certificate..... 16
 - 6.2.2 HTTPS with Default Untrusted Self-Signed TLS Certificate or HTTP with Built-in Payload Encryption 16
- 7 Configuring the QuickServer 17**
 - 7.1 Set IP Address of the QuickServer Using FS-GUI 18
 - 7.2 Retrieve the Sample Configuration File..... 19
 - 7.3 Change the Configuration File to Meet the Application 19
 - 7.4 Load the Updated Configuration File..... 20
 - 7.4.1 Using the FS-GUI to Load a Configuration File..... 20
 - 7.4.2 Retrieve the Configuration File for Modification or Backup 21
 - 7.5 Test and Commission the QuickServer 22
 - 7.5.1 Accessing SMC Cloud..... 22
- Appendix A Useful Features 23**
 - Appendix A.1. SSL/TLS for Secure Connection..... 23
 - Appendix A.1.1. Configuring FieldServer as a SSL/TLS Server 23
 - Appendix A.1.1.1. Simple Secure Server Configuration 23
 - Appendix A.1.1.2. Limiting Client Access 24
 - Appendix A.1.1.3. To Upload the Authority File to the FieldServer 24
 - Appendix A.1.1.4. Certificate Validation Options 25
 - Appendix A.1.1.5. Set up Server Certificate 25
 - Appendix A.1.2. Configuring FieldServer as SSL/TLS Client..... 26
 - Appendix A.1.2.1. Simple Secure Client Configuration 26
 - Appendix A.1.2.2. Limit Server Access..... 26
 - Appendix A.1.2.3. Certificate Validation Options 26
 - Appendix A.1.2.4. Set up Client Certificate..... 26
- Appendix B Troubleshooting 27**
 - Appendix B.1. Communicating with the QuickServer Over the Network 27
 - Appendix B.2. Before Contacting Technical Support Take a Diagnostic Capture 28
 - Appendix B.2.1. Using the FieldServer Toolbox..... 28
 - Appendix B.2.2. Using FS-GUI 31
 - Appendix B.3. LED Functions 32
 - Appendix B.4. Securing QuickServer with Password..... 33

Appendix B.5. Factory Reset Instructions	33
Appendix B.6. Internet Browser Software Support.....	34
Appendix B.7. Change Web Server Security Settings After Initial Setup.....	34
Appendix B.7.1. Change Security Mode.....	35
Appendix B.7.2. Edit the Certificate Loaded onto the FieldServer	36
Appendix B.8. Change User Management Settings.....	37
Appendix B.8.1. User Management.....	37
Appendix B.8.1.1. Create Users.....	38
Appendix B.8.1.2. Edit Users	39
Appendix B.8.1.3. Delete Users	40
Appendix B.8.2. Change FieldServer Password	41
Appendix C Reference.....	42
Appendix C.1. QuickServer FS-QS-2XX0-XXXX DCC	42
Appendix C.2. QuickServer Part Numbers.....	42
Appendix C.3. Compliance with UL Regulations.....	43
Appendix C.4. Dimension Drawing FS-QS-2XX0-XXXX.....	43
Appendix C.5. Specifications.....	44
Appendix D Limited 2 Year Warranty.....	45

LIST OF FIGURES

Figure 1: DIN Rail Bracket 10

Figure 2: DIN Rail Mounted..... 7

Figure 3: Bias Resistor DIP Switches 8

Figure 4: Termination Resistor DIP Switch 9

Figure 5: R1 & R2 Connection Ports..... 10

Figure 6: Required Current Draw for the Gateway 11

Figure 7: Power Connections..... 11

Figure 8: Ethernet Port Location 12

Figure 9: Web Server Security Unconfigured Window 13

Figure 10: Connection Not Private Warning 13

Figure 11: Warning Expanded Text 14

Figure 12: FieldServer Login..... 14

Figure 13: Security Mode Selection Screen..... 15

Figure 14: Security Mode Selection Screen..... 16

Figure 15: FS-GUI Landing Page 17

Figure 16: FS-GUI Network Settings 18

Figure 17: FS-GUI File Transfer 19

Figure 18: FS-GUI Loading Files 20

Figure 19: Retrieve Configuration File 21

Figure 20: FS-GUI Connections Page 22

Figure 21: Ethernet Port Location 28

Figure 22: Diagnostic LEDs 32

Figure 23: FS-GUI Passwords Page..... 33

Figure 24: Password Recovery Page 33

Figure 25: FS-GUI Landing Screen 34

Figure 26: FS-GUI Security Setup 35

Figure 27: FS-GUI Security Setup – Certificate Loaded..... 36

Figure 28: FS-GUI User Management..... 37

Figure 29: Create User Window..... 38

Figure 30: Setup Users 39

Figure 31: Edit User Window 39

Figure 32: Setup Users 40

Figure 33: User Delete Warning 40

Figure 34: FieldServer Password Update via FS-GUI 41

Figure 35: QuickServer Dimension Drawing..... 43

Figure 36: Specifications..... 44

1 QUICKSERVER DESCRIPTION

QuickServer is a high performance, cost effective Building and Industrial Automation multi-protocol gateway providing protocol translation between serial/Ethernet devices and networks.

NOTE: For troubleshooting assistance refer to Appendix B, or any of the troubleshooting appendices in the related driver supplements. Check the [Sierra Monitor website](#) for technical support resources and documentation that may be of assistance.

The QuickServer is cloud ready and connects with MSA Safety’s SMC Cloud. See **Section 7.5.1** for further information.

2 CERTIFICATIONS

2.1 BTL Mark – BACnet¹ Testing Laboratory



The BTL Mark 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.

3 SUPPLIED EQUIPMENT

QuickServer Gateway

- Preloaded with two selected drivers. A sample configuration file is also loaded.
- All instruction manuals, driver manuals, support utilities are available on the USB drive provided in the optional accessory kit, or on the [Sierra Monitor website](#).

Accessory kit (optional) (Part # FS-8915-38-QS) includes:

- 7-ft Cat-5 cable with RJ45 connectors at both ends
- Power Supply -110/220V (p/n 69196)
- Screwdriver for connecting to terminals
- USB Flash drive loaded with:
 - QuickServer 2XX0 Start-up Guide
 - FieldServer Configuration Manual
 - All FieldServer Driver Manuals
 - Support Utilities
 - Any additional folders related to special files configured for a specific QuickServer
 - Additional components as required - see driver manual supplement for details



¹ BACnet is a registered trademark of ASHRAE.

4 QUICKSERVER SETUP

4.1 Mounting

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

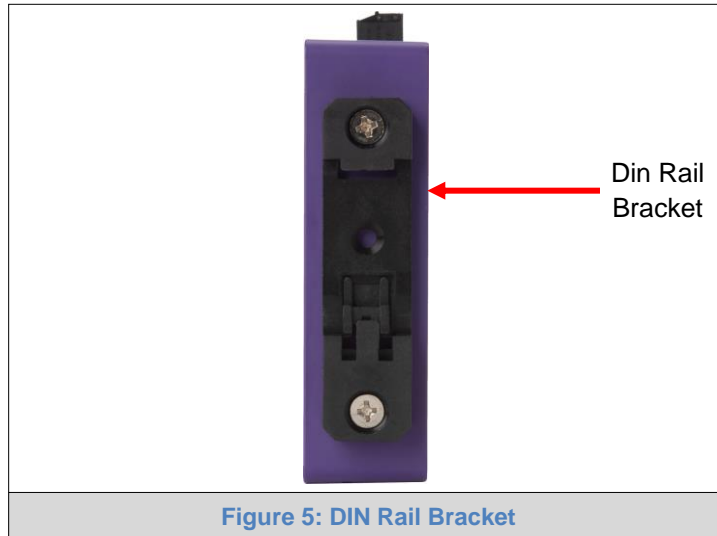


Figure 5: DIN Rail Bracket

NOTE: For dimension details see [Appendix C.4](#).



Figure 2: DIN Rail Mounted

4.2 DIP Switch Settings

4.2.1 Bias Resistors

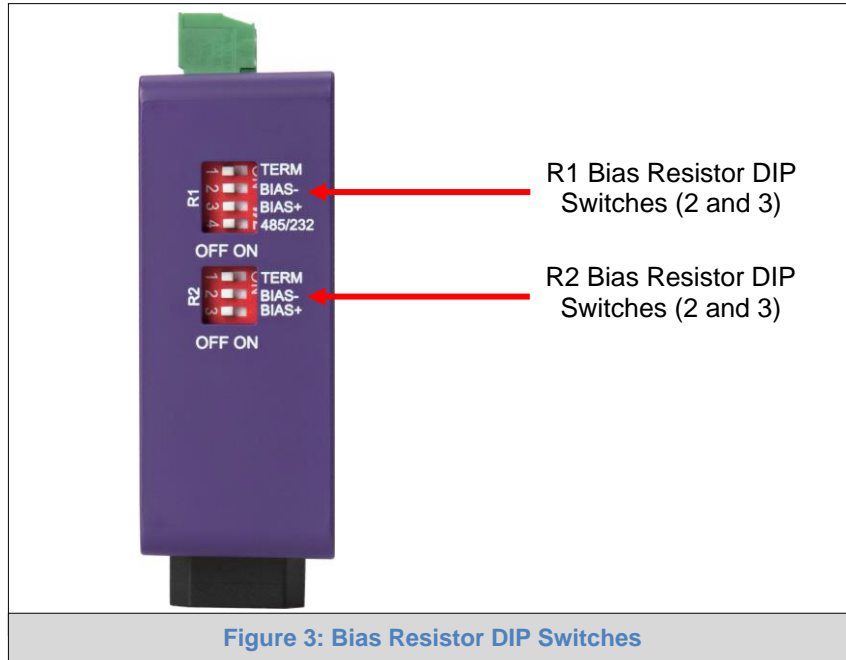


Figure 3: Bias Resistor DIP Switches

To enable Bias Resistors, move both the BIAS- and BIAS+ dip switches to the right in the orientation shown in [Figure 3](#).

The QuickServer 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 QuickServers can be put on the network without running into the bias resistor limit which is < 500 ohms.

NOTE: See www.ni.com/support/serial/resinfo.htm for additional pictures and notes.

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

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

4.2.2 Termination Resistor

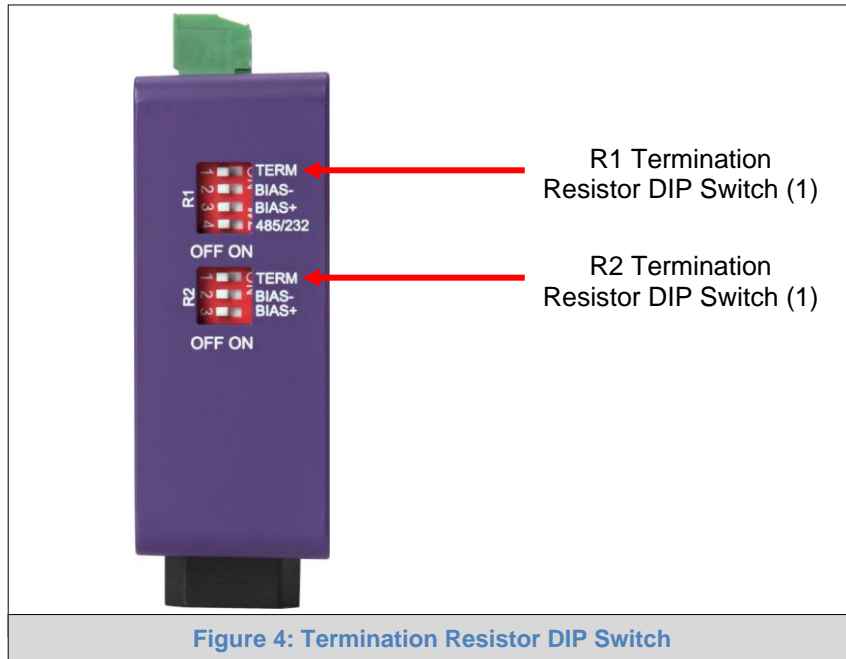


Figure 4: Termination Resistor DIP Switch

If the QuickServer 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 Figure 4.**

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.

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

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

4.3 Connecting the R1 Port

For the R1 Port only: Switch between RS-485 and RS-232 by moving the number 4 DIP Switch left for RS-485 and right for RS-232 (**Figure 4**).

The R2 Port is RS-485.

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

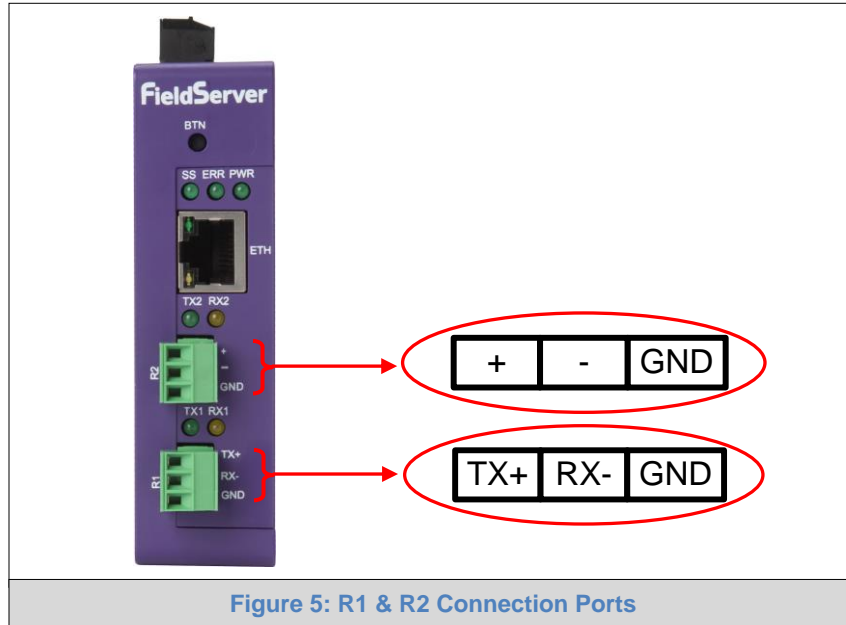


Figure 5: R1 & R2 Connection Ports

4.3.1 Wiring

RS-485		RS-232	
BMS RS-485 Wiring	Gateway Pin Assignment	BMS RS-232 Wiring	Gateway Pin Assignment
RS-485 +	TX +	RS-232 -	TX +
RS-485 -	RX -	RS-232 +	RX -
GND	GND	GND	GND

NOTE: Use standard grounding principles for GND.

4.3.2 Supported RS-485 Baud Rates by Protocol

The supported baud rates for either port is based on the protocol of the connected devices.

The following baud rates are supported for Modbus RTU:

2400, 4800, 9600, 19200, 38400, 57600, 76800, 115200

The following baud rates are supported for BACnet MS/TP:

9600, 19200, 38400, 76800

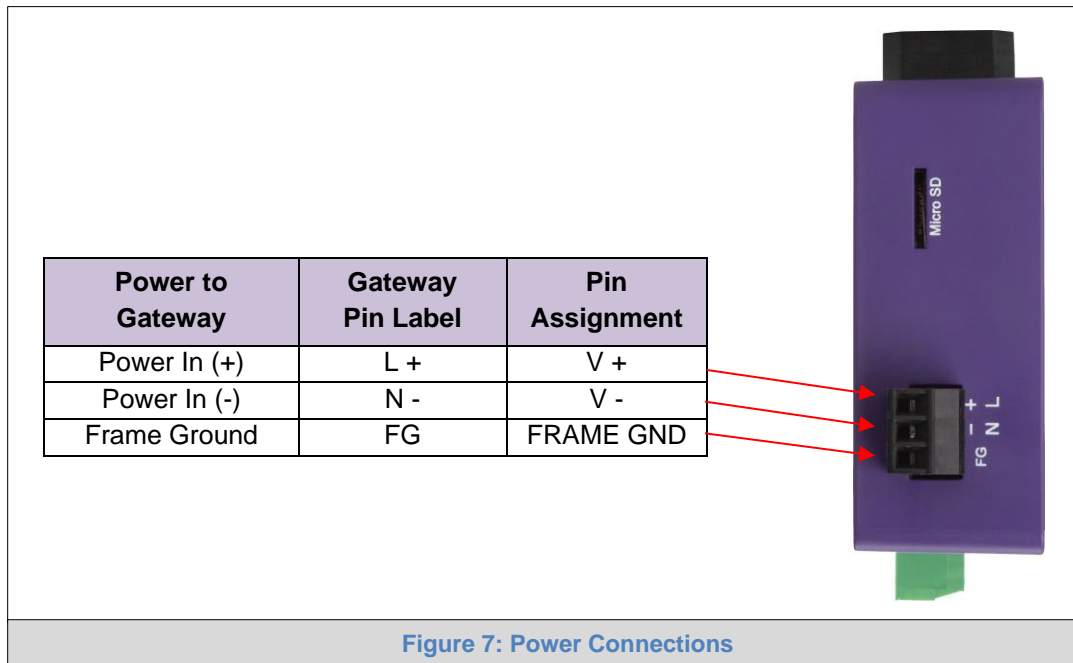
4.4 Power Up the Device

Check power requirements in the table below:

Power Requirement for External Gateway		
	Current Draw Type	
QuickServer Family	12VDC	24VDC/AC
FS-QS-2XX0-XXXX (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.		
Figure 6: Required Current Draw for the Gateway		

Apply power to the QuickServer as shown below in [Figure 7](#). Ensure that the power supply used complies with the specifications provided in [Appendix C.5](#).

- The QuickServer accepts 9-30VDC or 24VAC on pins L+ and N-.
- Frame GND should be connected.



5 CONNECT THE PC TO THE QUICKSERVER

5.1 Connecting to the Gateway via Ethernet

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

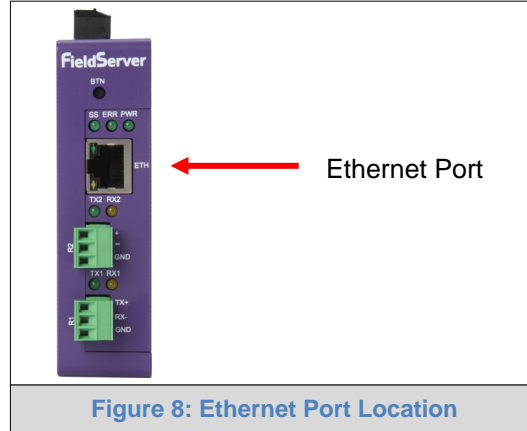



Figure 8: Ethernet Port Location

5.1.1 Changing the Subnet of the Connected PC

The default IP Address for the QuickServer is **192.168.2.101**, Subnet Mask is **255.255.255.0**. If the PC and QuickServer 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.

5.2 Navigate to the EZ Gateway Login Page

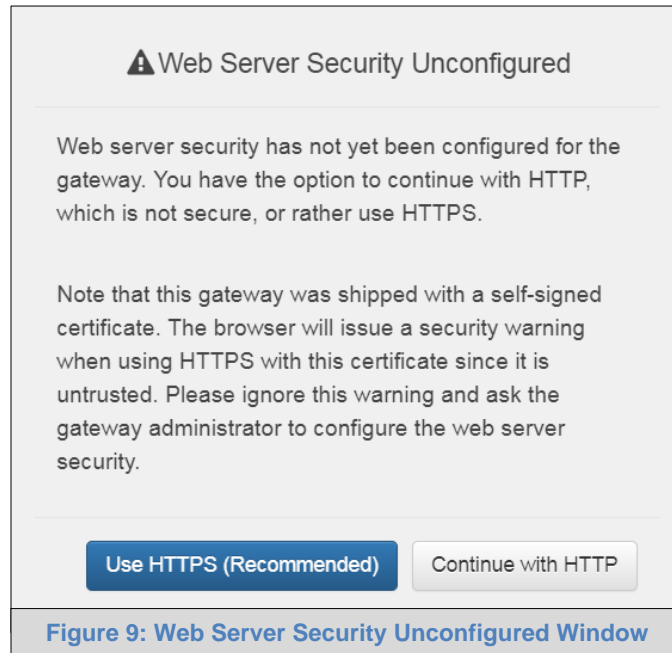
- Open a web browser and connect to the QuickServer's default IP Address. The default IP Address of the FieldServer is **192.168.2.101**, Subnet Mask is **255.255.255.0**.
- If the PC and the QuickServer are on different IP networks, assign a static IP Address to the PC on the 192.168.2.X network.

6 SETUP WEB SERVER SECURITY

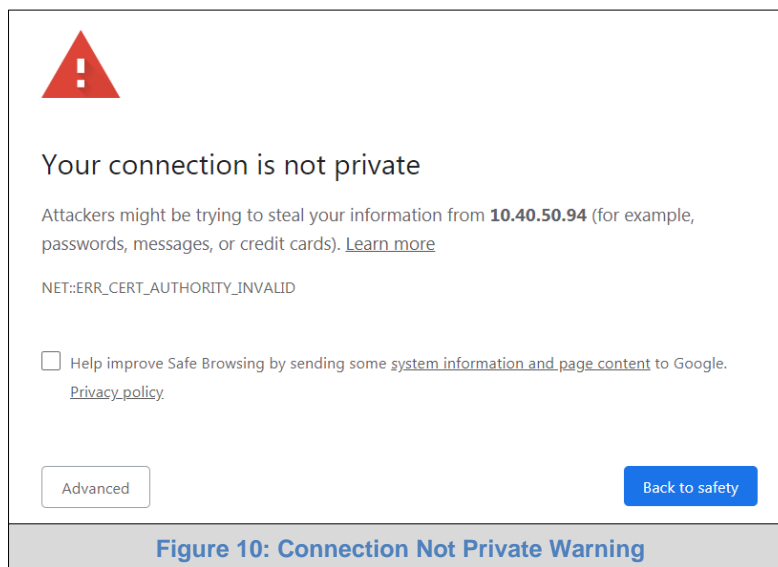
6.1 Login to the FieldServer

The first time the FieldServer GUI is opened in a browser, the IP Address for the gateway will appear as untrusted. This will cause the following pop-up windows to appear.

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



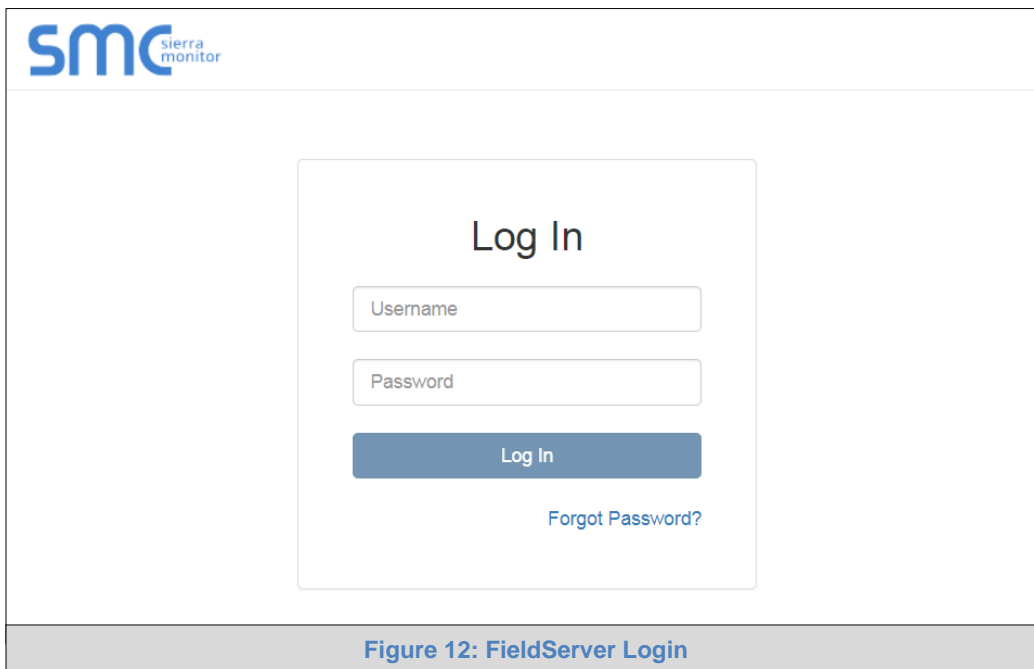
- When the warning that “Your connection is not private” appears, click the advanced button on the bottom left corner of the screen.



- Additional text will expand below the warning, click the underlined text to go to the IP Address. In the **Figure 11** example this text is “[Proceed to 10.40.50.94 \(unsafe\)](#)”.



- When the login screen appears, put in the Username (default is “admin”) and the Password (found on the label of the FieldServer).



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 [Appendix B.8](#).

6.2 Select the Security Mode

- On the first login to the FieldServer, the following screen will appear that allows the user to select which mode the FieldServer should use.

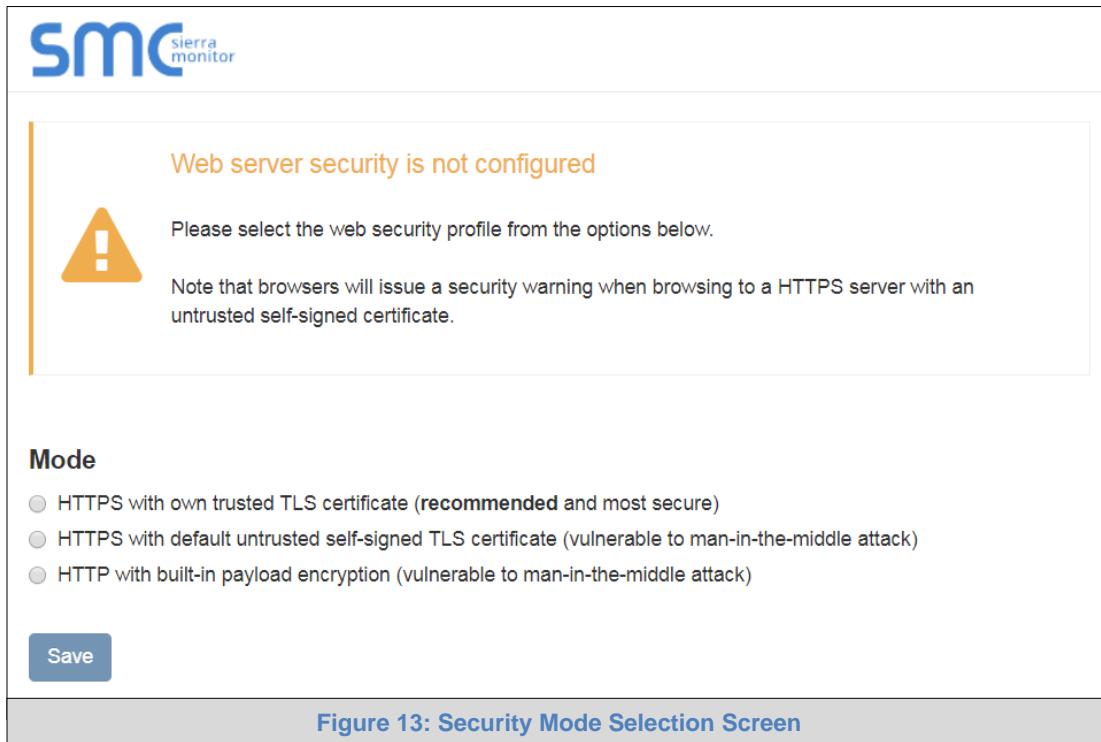


Figure 13: Security Mode Selection Screen

NOTE: To change the web server security mode after initial setup, go to 0.

NOTE: Cookies are used for authentication.

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

6.2.1 HTTPS with Own Trusted TLS Certificate

This is the recommended selection and the most secure.

- Once this option is selected, the Certificate, Private Key and Private Key Passphrase fields will appear under the mode selection.

Mode

HTTPS with own trusted TLS certificate (**recommended** and most secure)
 HTTPS with default untrusted self-signed TLS certificate (vulnerable to man-in-the-middle attack)
 HTTP with built-in payload encryption (vulnerable to man-in-the-middle attack)

Certificate

```
XzyMbQZFIRuJZJPe7CTHLcHOrHLowoUFoVTaBMYd4d6VGdNklKazByWKcNOL7mrX
A4IBAQBfM+IPvOx3T/47VEmaiXqE3bx3zEuBFJ6pWPlw7LHf2r2ZoHw+9xb+aNMU
dVyAelhBMTmsni2ERvQVp0xj3psSv2EJyKXS1bOYNRLsq7UzpwuAdT/Wy3o6vUM5
K+Cwf9qEoQ0LuxDZTIECt67MkcHMiuFi5pk7TRicHnQF/sfOAYOulduHOy9exlk9
FmHFVDIZt/cJUaF+e74EuSph+gEr0lQo2wmmhyc7L22UXse1NoOfU2Zq0Eu1VVtu
JRryaMWiRFEWuuzMGZtKFWWC+8q2JQsVcgiRWM7naoblEhOCMH+sKHJMCxDoXGt
vtZjpZUoAL51YXxWSVcyZdGiAP5e
-----END CERTIFICATE-----
```

Private Key

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAQGAQIhB0zZoHr4YQSDk2BbYVzzbl0LDuKtc8+JiO3ooGjoTuHngkeAj/fKfbTAsKeAzw
gKQe+H5UQNk0bdvZfOJrm6daDK2vDmR5k+iUUhEi5N49upIroB97MQgYotzqfT+
THlBpg5t1SIK617k04ObKmHF5l8fck+ru545sVmpeeZh0m5j5SURYAZMvbq5daCu
J4l5NlihbEvxRF4UK41ZDMCvuj0PcBKUwrb1a/3XXnDnM2K9xyz2wze998D6Wk46
+7aOFY9F+7j5ljmkoS3GYtwCyH5jP+mPP1K6RnuiD019wvGPb4dtN/RTnfd0eF
GYeVSkI9fxxkxDOFtdWRZbM/rPjn4tmO1Xf8HqONVN1x/iaMynOXG4cukoi4+VO
u0rZaUEsIl2zNkfm7fAASm5NBWq202Cy9IAYnuujs3aALi5uGBeekA62oTMxlzx
-----END RSA PRIVATE KEY-----
```

Private Key Passphrase

Specify if encrypted

Save

Figure 14: Security Mode Selection Screen

- 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 appears and after a short period of time the FieldServer GUI will open.

6.2.2 HTTPS with Default Untrusted Self-Signed TLS Certificate or HTTP with Built-in Payload Encryption

- Simply select one of these options and click the Save button.
- A “Redirecting” message appears and after a short period of time the FieldServer GUI will open.

7 CONFIGURING THE QUICKSERVER

Once the web server setup is complete, the FS-GUI landing page will appear.

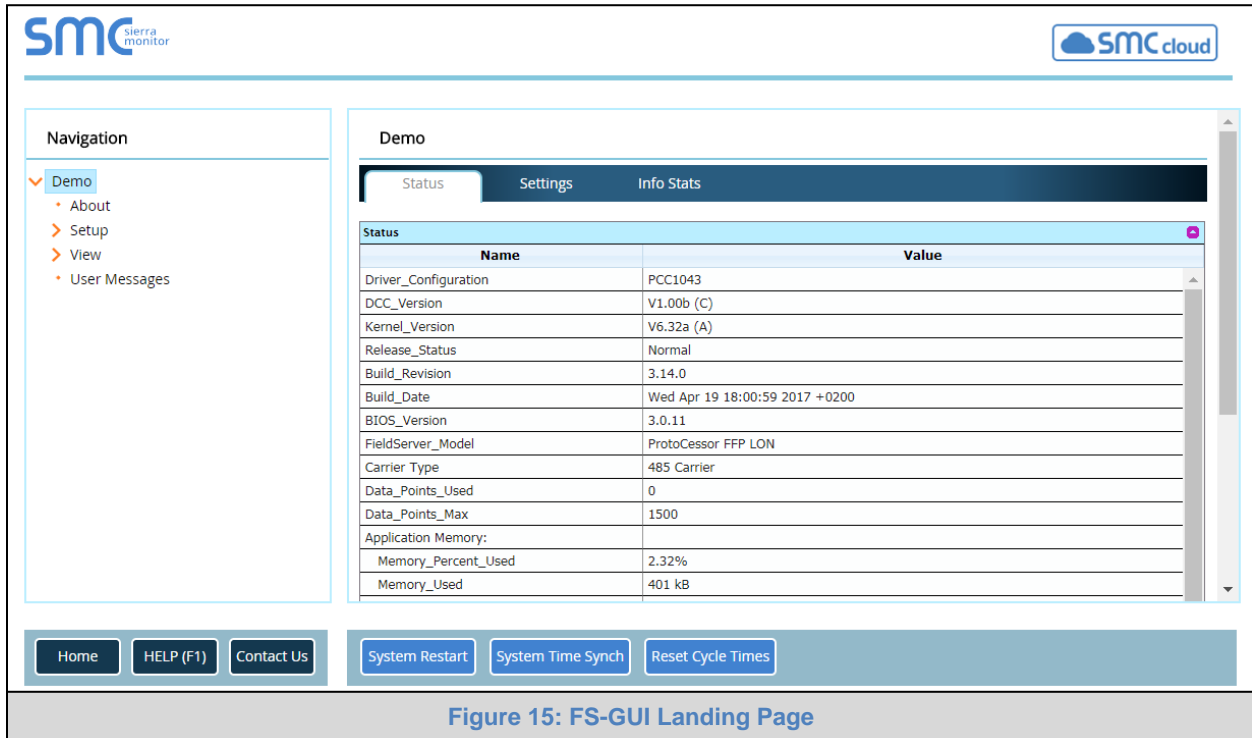



Figure 15: FS-GUI Landing Page

NOTE: The SMC Cloud button  (see [Figure 15](#)) allows users to connect to the SMC Cloud, MSA Safety’s device cloud solution for IIoT. The SMC Cloud enables secure remote connection to field devices through a FieldServer and its local applications for configuration, management, maintenance. For more information about the SMC Cloud, refer to the [SMC Cloud Start-up Guide](#).

7.1 Set IP Address of the QuickServer Using FS-GUI

- From the FS-GUI main home page, click on setup and then Network Settings to enter the Edit IP Address Settings menu.
- Modify the IP Address (N1 IP Address field) of the QuickServer Ethernet port.
- If necessary, change the Netmask (N1 Netmask field).
- Type in a new Subnet Mask.
- If necessary, change the IP Gateway (Default Gateway field).
- Type in a new IP Gateway.

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 Update IP Settings, then click on the System Restart to restart the Gateway and activate the new IP Address.

NOTE: If the FS-GUI was open in a browser, the browser will need to be pointed to the new IP Address of the QuickServer before the FS-GUI will be accessible again.

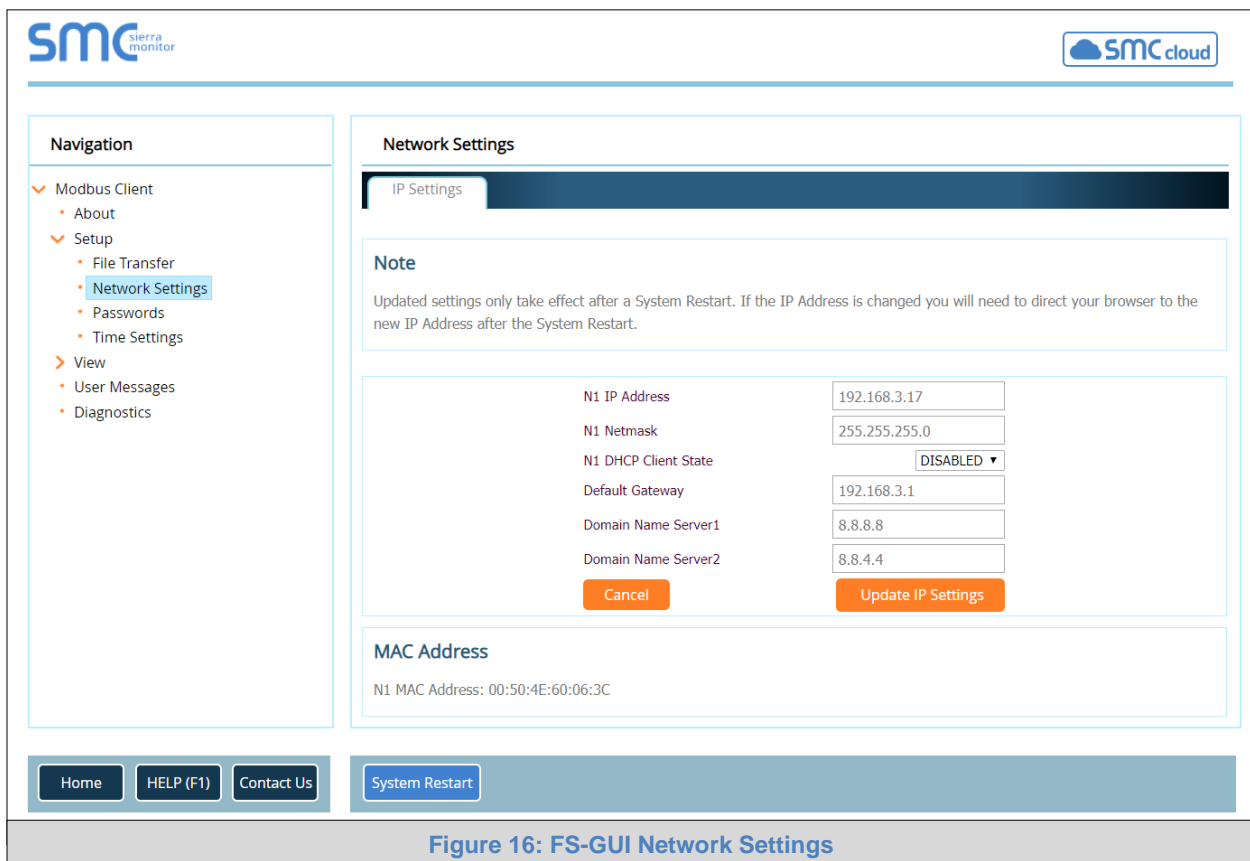



Figure 16: FS-GUI Network Settings

NOTE: The SMC Cloud button  (see Figure 16) allows users to connect to the SMC Cloud, MSA Safety’s device cloud solution for IIoT. The SMC Cloud enables secure remote connection to field devices through a FieldServer and its local applications for configuration, management, maintenance. For more information about the SMC Cloud, refer to the [SMC Cloud Start-up Guide](#).

7.2 Retrieve the Sample Configuration File

The configuration of the QuickServer is provided to the QuickServer’s operating system via a comma-delimited file called “CONFIG.CSV”.

If a custom configuration was ordered, the QuickServer will be programmed with the relevant device registers in the Config.csv file for the initial start-up. If not, the product is shipped with a sample config.csv that shows an example of the drivers ordered.

- In the main menu of the FS-GUI screen, go to “Setup”, then “File Transfer”, and finally “Retrieve”.
- Click on “config.csv”, and open or save the file.

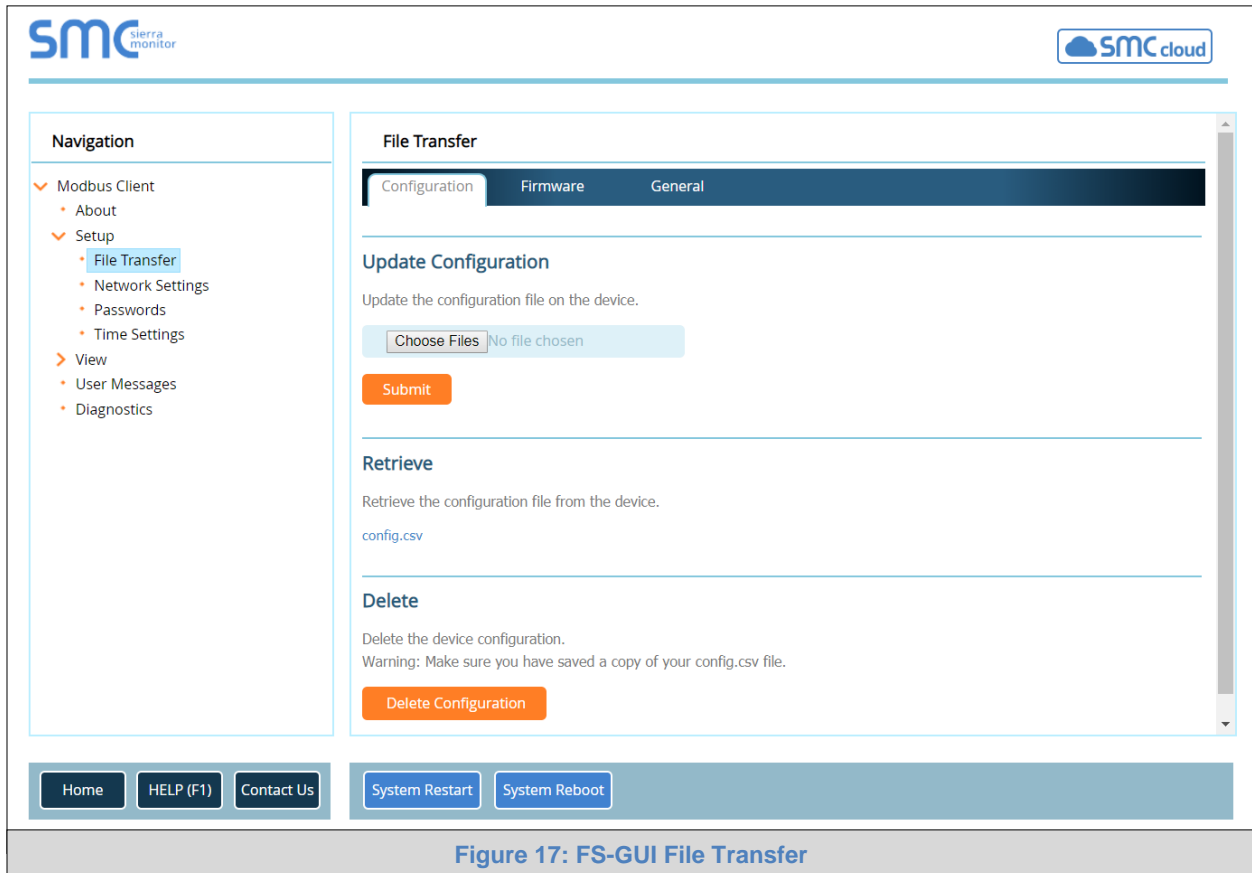


Figure 17: FS-GUI File Transfer

7.3 Change the Configuration File to Meet the Application

Refer to the FieldServer Configuration Manual in conjunction with the Driver supplements for information on configuring the QuickServer.

7.4 Load the Updated Configuration File

7.4.1 Using the FS-GUI to Load a Configuration File

- In the main menu of the FS-GUI screen, click “Setup”, then “File Transfer” and finally “Update”.
- Browse and select the .csv file, open, then click “Submit”.

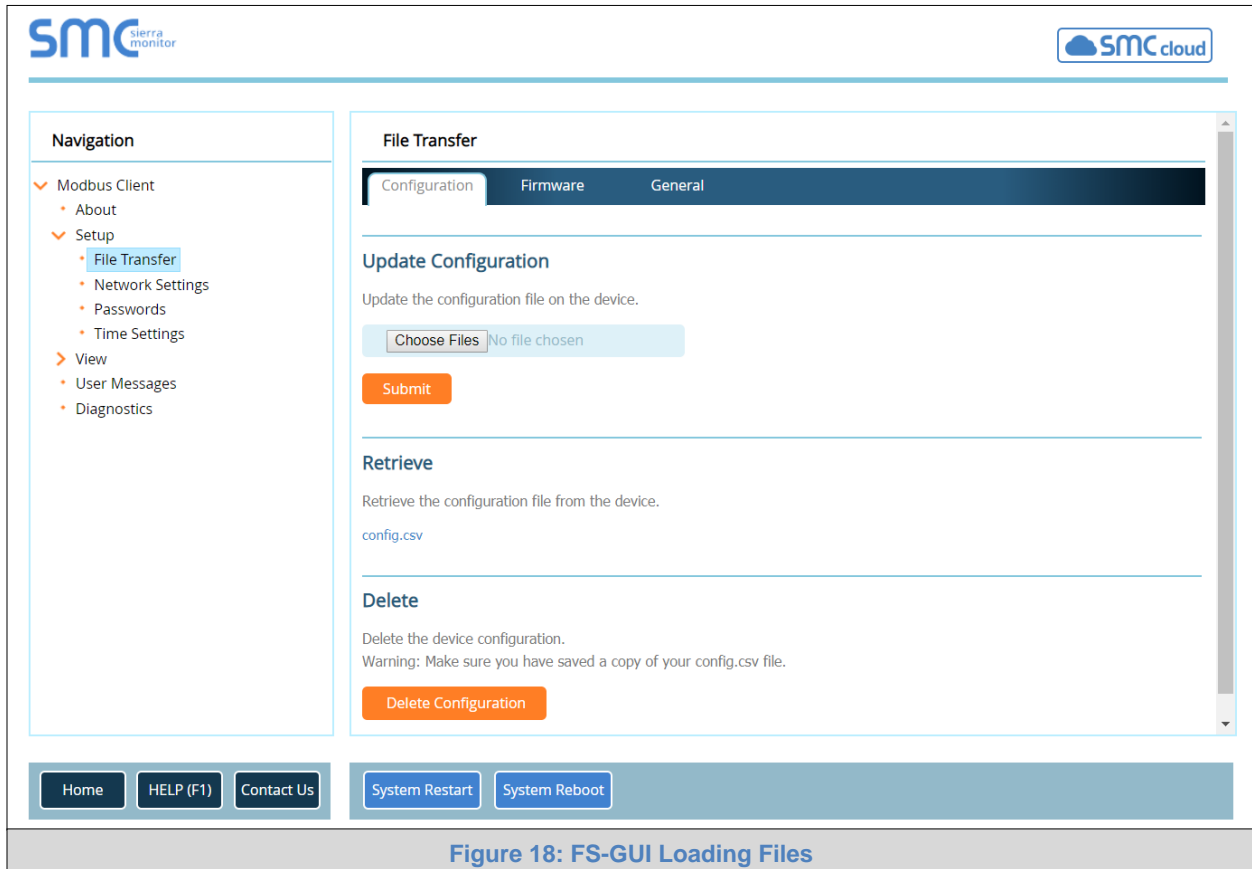


Figure 18: FS-GUI Loading Files

- Once download is complete, a message bar will appear confirming that the configuration was updated successfully.
- Click the System Restart Button to put the new file into operation.

NOTE: It is possible to do multiple downloads to the QuickServer before resetting it.

7.4.2 Retrieve the Configuration File for Modification or Backup

To get a copy of the configuration file for modifying or backing up a configuration on a local computer, do the following:

- In the main menu of the FS-GUI screen, click “Setup”, then “File Transfer”.

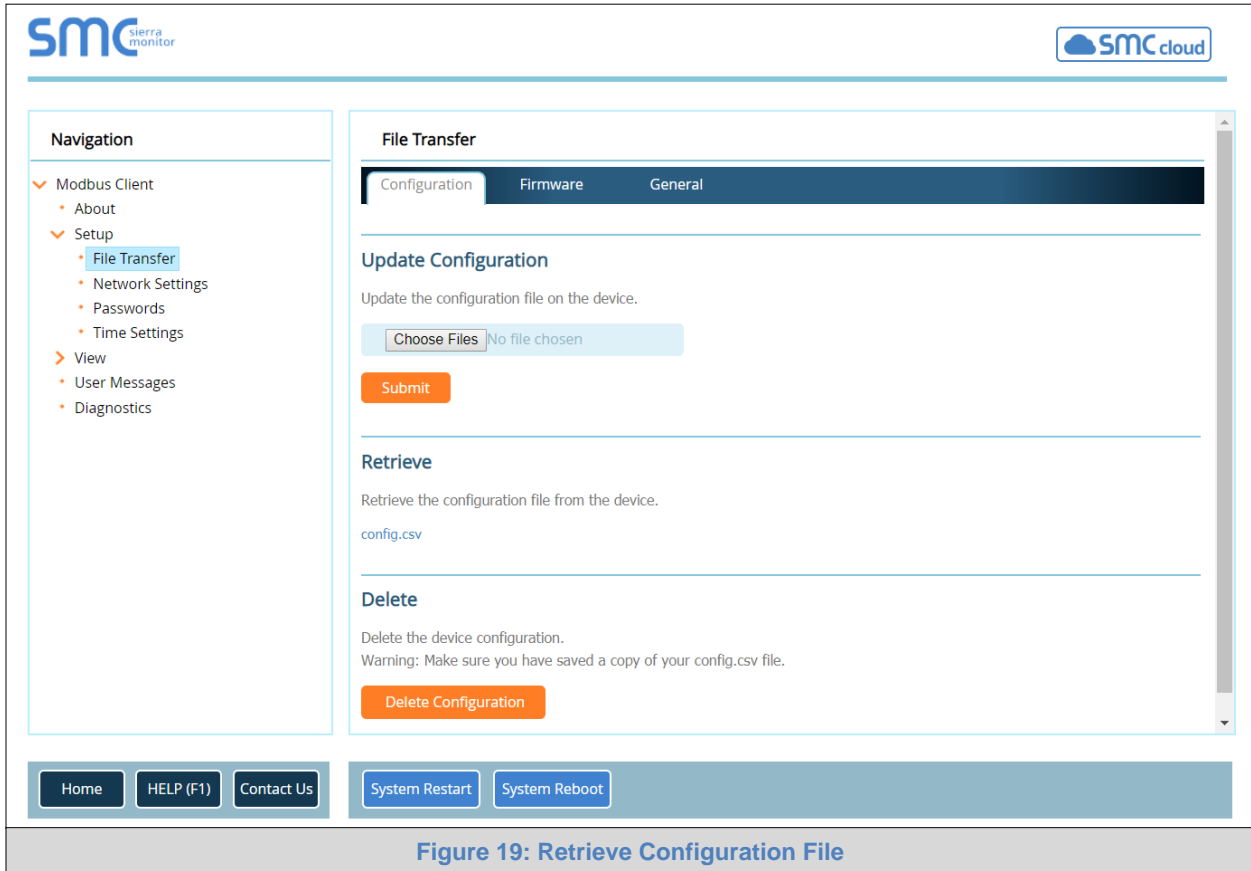


Figure 19: Retrieve Configuration File

- Click the “config.csv” link under the “Retrieve” heading in the middle section of the screen.
 - The file will automatically download to the web browser’s default download location.
- Edit or store the file as desired.

NOTE: Before using any backup configuration file to reset the configuration settings, check that the backup file is not an old version.

7.5 Test and Commission the QuickServer

- Connect the QuickServer to the third party device(s), and test the application.
- From the landing page of the FS-GUI click on “View” in the navigation tree, then “Connections” to see the number of messages on each protocol.

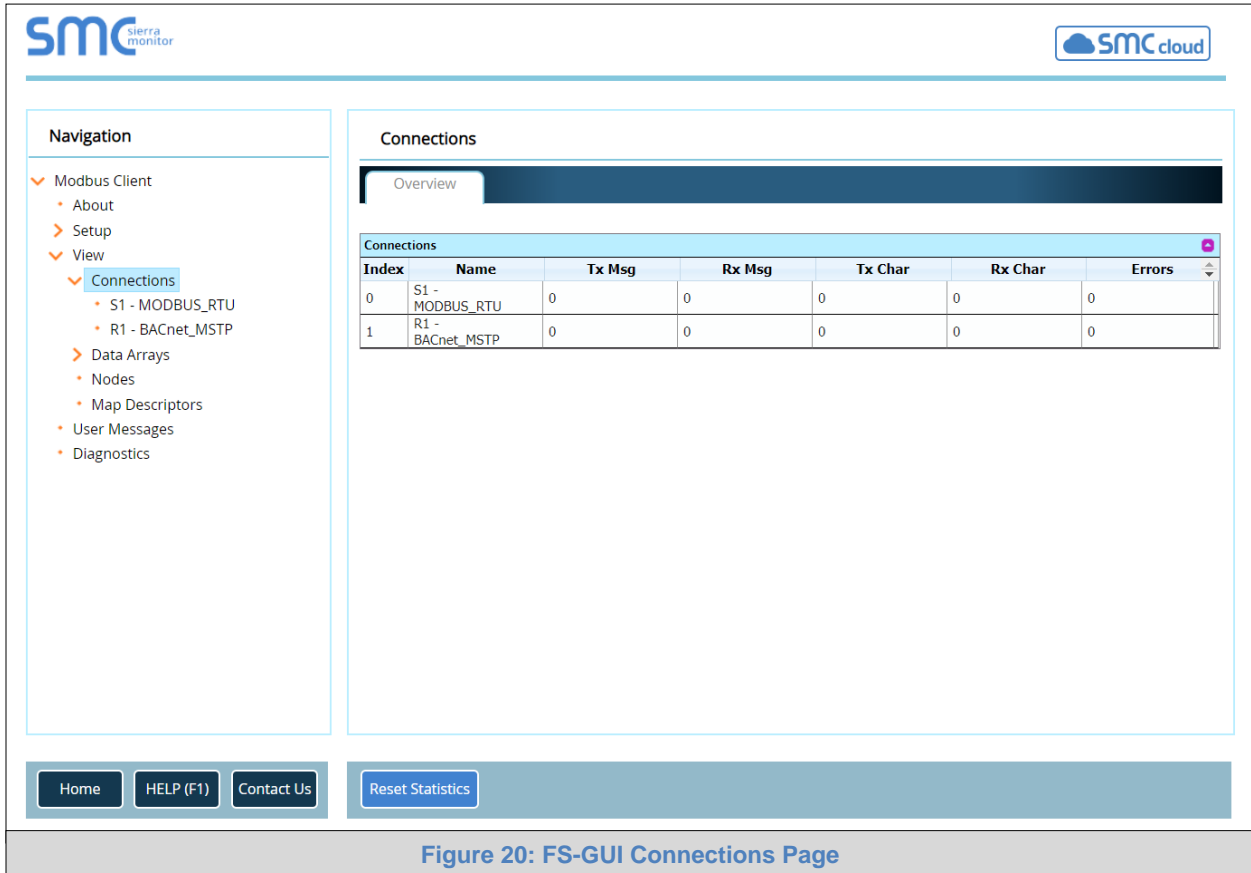


Figure 20: FS-GUI Connections Page

7.5.1 Accessing SMC Cloud

The SMC Cloud button (see Figure 16) allows users to connect to the SMC Cloud, MSA Safety’s device cloud solution for IIoT. The SMC Cloud enables secure remote connection to field devices through a FieldServer and its local applications for configuration, management, maintenance. For more information about the SMC Cloud, refer to the [SMC Cloud Start-up Guide](#).

APPENDIX A USEFUL FEATURES

Appendix A.1. SSL/TLS for Secure Connection

SSL/TLS (Secure Sockets Layer/Transport Layer Security) is a security technology for establishing an encrypted connection between a server and a client. This allows the secure transfer of data across untrusted networks.

Appendix A.1.1. Configuring FieldServer as a SSL/TLS Server

The following example sets the FieldServer to accept a secure Modbus/TCP connection on port 1502.

Appendix A.1.1.1. Simple Secure Server Configuration

Add TLS_Port parameter in the connections section of the configuration file and set to a port number between 1 – 65535.

```
Connections
Adapter , Protocol , TLS_Port
N1 , Modbus/TCP , 1502
```

This configuration sets the FieldServer to accept any incoming connection but will not request a client's certificate for verification. This means that the FieldServer end point communication will be encrypted but not authenticated.

The FieldServer will send an embedded self-signed certificate if one is requested by a connecting client.

NOTE: If a remote client requires a certificate, then request the smc_cert.pem certificate from FieldServer Technical Support and update the remote client's authority as per vendor instructions.

Appendix A.1.1.2. Limiting Client Access

In addition to TLS_Port parameter also add Validate_Client_Cert in the connections section of the configuration file and set it to “Yes”.

Connections				
Adapter	Protocol	TLS_Port	Validate_Client_Cert	
N1	Modbus/TCP	1502	Yes	

The configuration above sets the FieldServer to request and verify a client’s certificate against its internal authority file before accepting connection. By default, this means the FieldServer will only accept connections from other FieldServers.

In order to load an authority file so that the FieldServer will accept connections from a chosen list of remote clients, configure the FieldServer with the following connection settings:

Connections					
Adapter	Protocol	TLS_Port	Validate_Client_Cert	Cert_Authority_File	
N1	Modbus/TCP	1502	Yes	my_authorized_clients.pem	

This configuration has the FieldServer accept connections from clients who have the correct certificate. The authority file is a collection of client certificates in PEM format. This file can be edited using any text file editor.

NOTE: Cert_Authority_File is useful only if Validate_Client_Cert is set to ‘Yes’.

Appendix A.1.1.3. To Upload the Authority File to the FieldServer

1. Enter the IP address of the FieldServer into a web browser.
2. Choose the ‘Setup’ option in the Navigation Tree and Select ‘File Transfer’.
3. Choose the ‘General’ tab.
4. Click on the ‘Browse’ button and select the PEM file you want to upload.
5. Click on ‘Submit’.
6. When the message, “The file was uploaded successfully” appears, click on the ‘System Restart’ button.

Appendix A.1.1.4. Certificate Validation Options

If connections must be limited to only a particular domain (vendor devices), include Check_Remote_Host to specify the domain/host name.

```
Connections
Adapter , Protocol , TLS_Port , Validate_Client_Cert , Cert_Authority_File , Check_Remote_Host
N1 , Modbus/TCP , 1502 , Yes , my_authorized_clients.pem , SMC
```

The configuration above tells the FieldServer to only accept connections that have the correct certification and is coming from the specified host.

The Check_Remote_Host value is synonymously known as common name, host name or domain etc. The common name can be obtained by the following methods:

- Ask the certificate issuer for the host name.
- Use online tools to decode the certificate (for example: <https://www.sslshopper.com/certificate-decoder.html>).
- If the program openssl is installed on the local PC, then run the following command to get the common name: `openssl x509 -in certificate.pem -text -noout`

Appendix A.1.1.5. Set up Server Certificate

Make sure the certificate is in PEM format. Otherwise, convert it to PEM format (reference the link below). support.ssl.com/Knowledgebase/Article

Configure the FieldServer to use a custom certificate as shown below:

```
Connections
Adapter , Protocol , TLS_Port , Server_Cert_File
N1 , Modbus/TCP , 1502 , my_server_cert.pem
```

Appendix A.1.2. Configuring FieldServer as SSL/TLS Client

The following Node configurations set the FieldServer to open a secure Modbus/TCP connection to Server at IP Address 10.11.12.13 on port 1502.

Appendix A.1.2.1. Simple Secure Client Configuration

Add Remote_Node_TLS_Port parameter in the nodes section of the configuration file and set to a port number between 1 – 65535.

```
Nodes
Node_Name , Node_ID , Protocol , Adapter , IP_Address , Remote_Node_TLS_Port
PLC_11 , 11 , Modbus/TCP , N1 , 10.11.12.13 , 1502
```

The above configuration sets the FieldServer to connect to a remote server but does not request a server’s certificate for verification. This means that the FieldServer end point communication will be encrypted but not authenticated.

If requested by a remote server, the FieldServer will send an embedded self-signed certificate.

Appendix A.1.2.2. Limit Server Access

Add the Validate_Server_Cert parameter to the client node section of the configuration.

```
..... , Remote_Node_TLS_Port , Validate_Server_Cert
..... , 1502 , Yes
```

The above configuration sets the FieldServer to request and verify the server’s certificate against its own internal authority file before finalizing the connection. By default, this means the FieldServer will only establish connections to other FieldServers.

```
..... , Remote_Node_TLS_Port , Validate_Server_Cert , Cert_Authority_File
..... , 1502 , Yes , my_authorized_servers.pem
```

The above configuration sets the FieldServer to use a specified PEM file to allow custom server connections.

The authority file is a collection of server certificates in PEM format. This file can be edited using any text file editor (such as notepad). When the file has all required certificates, paste it into the PEM formatted server certificate. Now the FieldServer will connect to a server if it can find the server’s certificate in the authority file.

NOTE: Cert_Authority_File is useful only if Validate_Client_Cert is set to ‘Yes’.

To upload the Certificate to the FieldServer follow the directions for the authority file in [Appendix A.1.1.3](#).

Appendix A.1.2.3. Certificate Validation Options

Use the Check_Remote_Host element as described in [Appendix A.1.1.4](#).

Appendix A.1.2.4. Set up Client Certificate

Make sure the certificate is in PEM format. Otherwise, convert it to PEM format (reference the link below). support.ssl.com/Knowledgebase/Article

Configure the FieldServer to use a custom certificate as shown below:

```
..... , Client_Cert_File
..... , my_client_cert.pem
```

APPENDIX B TROUBLESHOOTING**Appendix B.1. Communicating with the QuickServer Over the Network**

- Confirm that the network cabling is correct.
- Confirm that the computer network card is operational and correctly configured.
- Confirm that there is an Ethernet adapter installed in the PC's Device Manager List, and that it is configured to run the TCP/IP protocol.
- Check that the IP netmask of the PC matches the QuickServer. The Default IP Address of the QuickServer is 192.168.2.X, Subnet Mask is 255.255.255.0.
 - Go to Start|Run
 - Type in "ipconfig"
 - The account settings should be displayed.
 - Ensure that the IP Address is 102.168.2.X and the netmask 255.255.255.0
- Ensure that the PC and QuickServer are on the same IP Network, or assign a Static IP Address to the PC on the 192.168.2.0 network.

Appendix B.2. Before Contacting Technical Support Take a Diagnostic Capture

When there is a problem on-site that cannot easily be resolved, perform a diagnostic capture before contacting support so that support can quickly solve the problem. There are two methods for taking diagnostic captures:

- FieldServer Toolbox:**
 This method requires installation of the FS Toolbox program. A FS Toolbox diagnostic capture takes a snapshot of the loaded configuration files and a log of all the communications on the serial ports over a specified period of time. If the problem occurs over an Ethernet connection, then take a Wire Shark capture.
- Gateway's FS-GUI Page:**
 This method doesn't require downloading software. The diagnostic capture utilities are embedded in the FS-GUI web interface. Starting a diagnostic capture takes a snapshot of the loaded configuration files and a log of all the communications over a specified period of time. This works for both serial and Ethernet connections.

NOTE: The information in the zipped files contains everything support needs to quickly resolve problems that occur on-site.

Appendix B.2.1. Using the FieldServer Toolbox

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

NOTE: While all necessary documentation is shipped with the FieldServer on the USB flash drive, these documents are constantly being updated. Newer versions may be available on the [Sierra Monitor website](#).

- Ensure that FieldServer Toolbox is loaded onto the local PC. Otherwise, download the FieldServer-Toolbox.zip via the Sierra Monitor website's [Software Downloads](#).
- Extract the executable file and complete the installation.

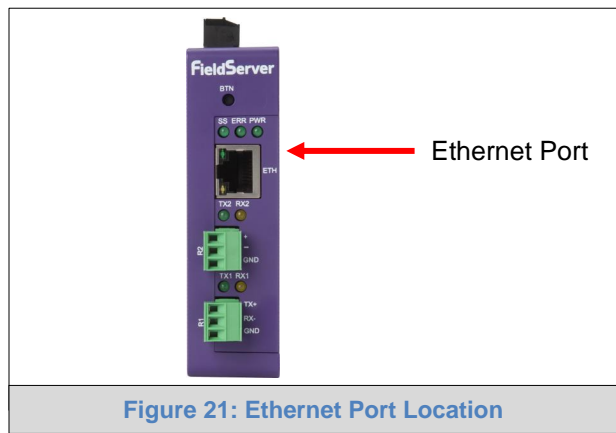

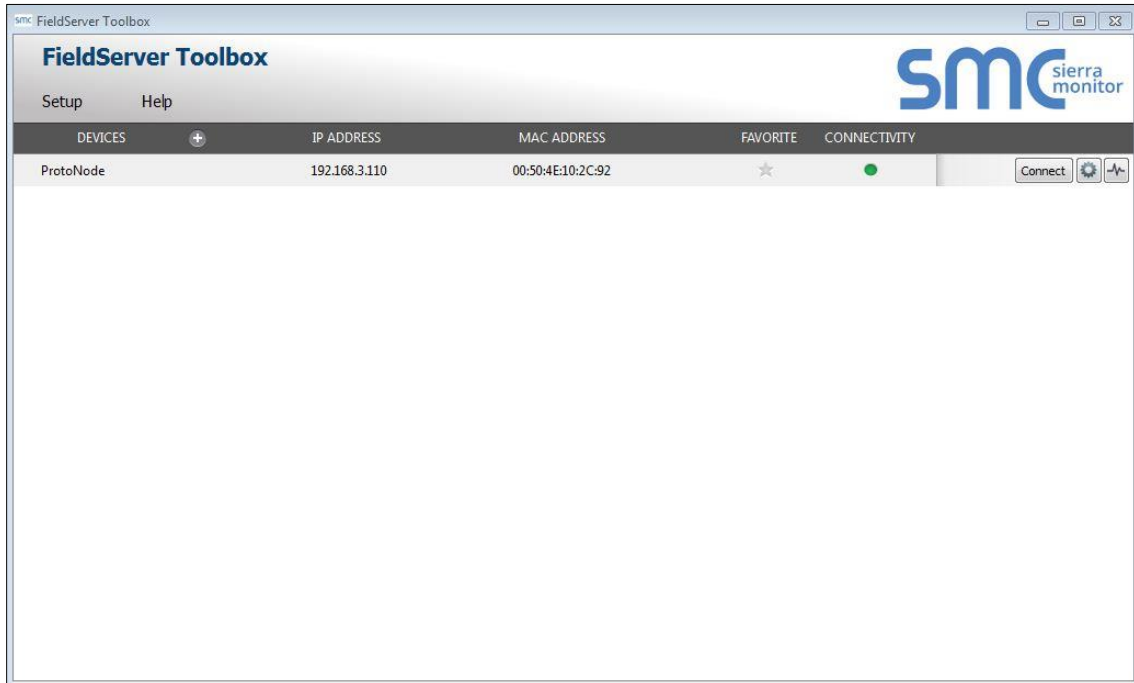


Figure 21: Ethernet Port Location

- Connect a standard Cat-5 Ethernet cable between the PC and QuickServer.
- Double click on the FS Toolbox Utility.

Step 1: Take a Log

- Click on the diagnose icon  of the desired device

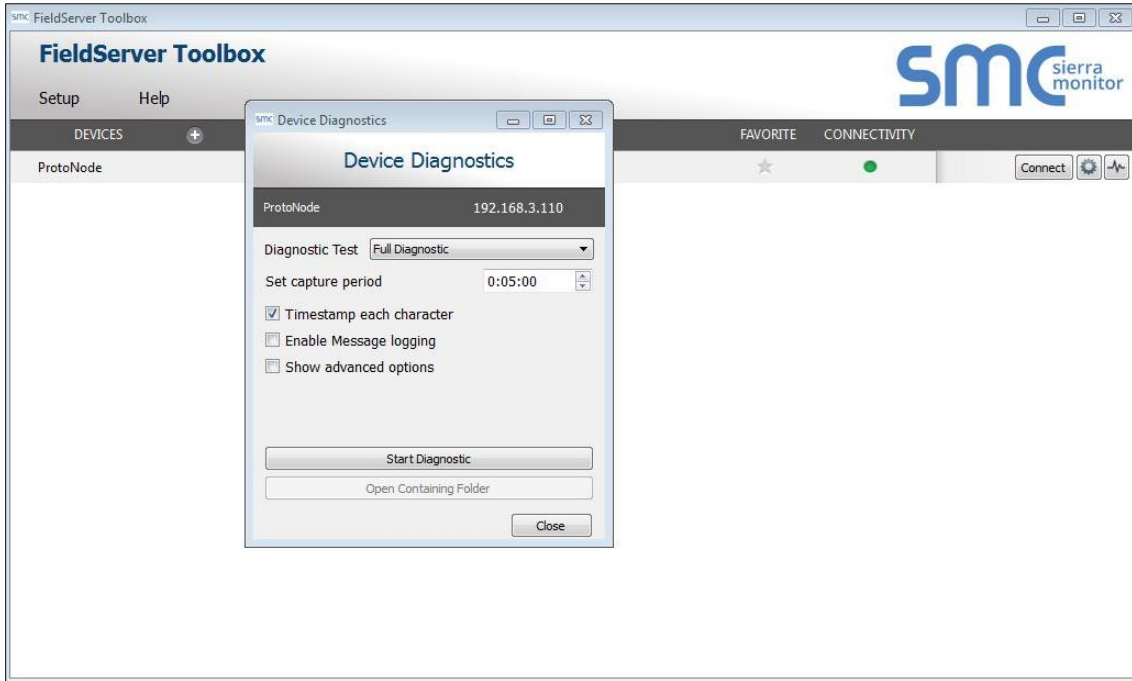


- Ensure "Full Diagnostic" is selected (this is the default)



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

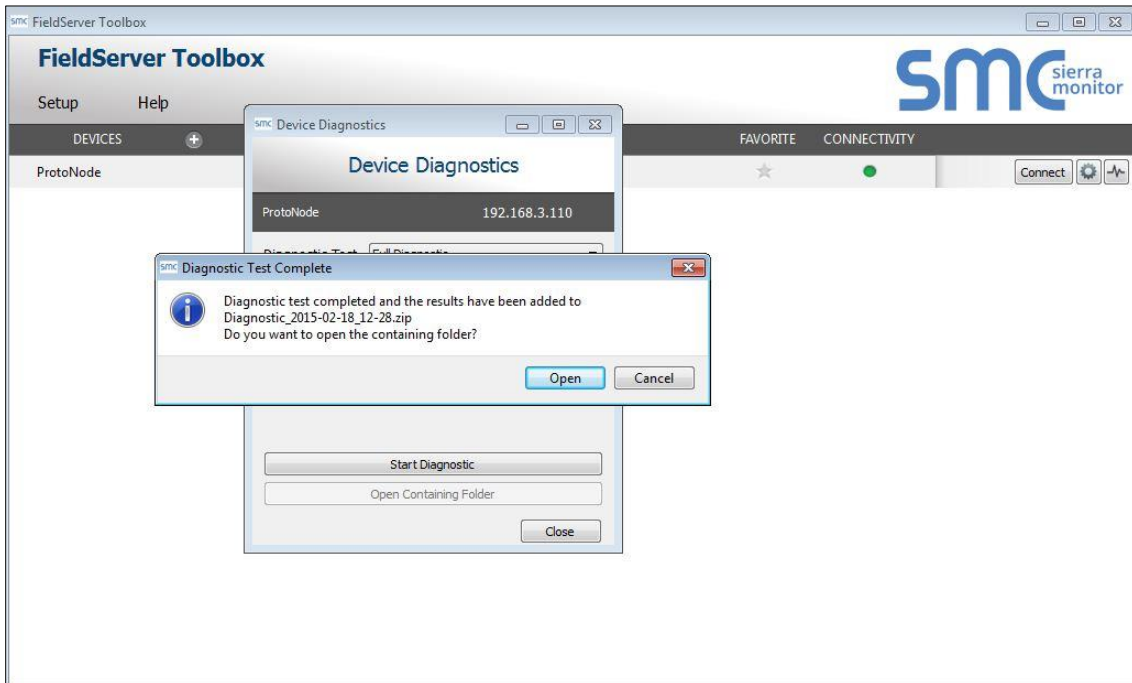
- Click on “Start Diagnostic”



- When the capture period is finished, the “Diagnostic Test Complete” window will appear

Step 2: Send Log

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



- Click “Open” to launch explorer and have it point directly at the correct folder
- Email the diagnostic zip file to smc-support@msasafety.com

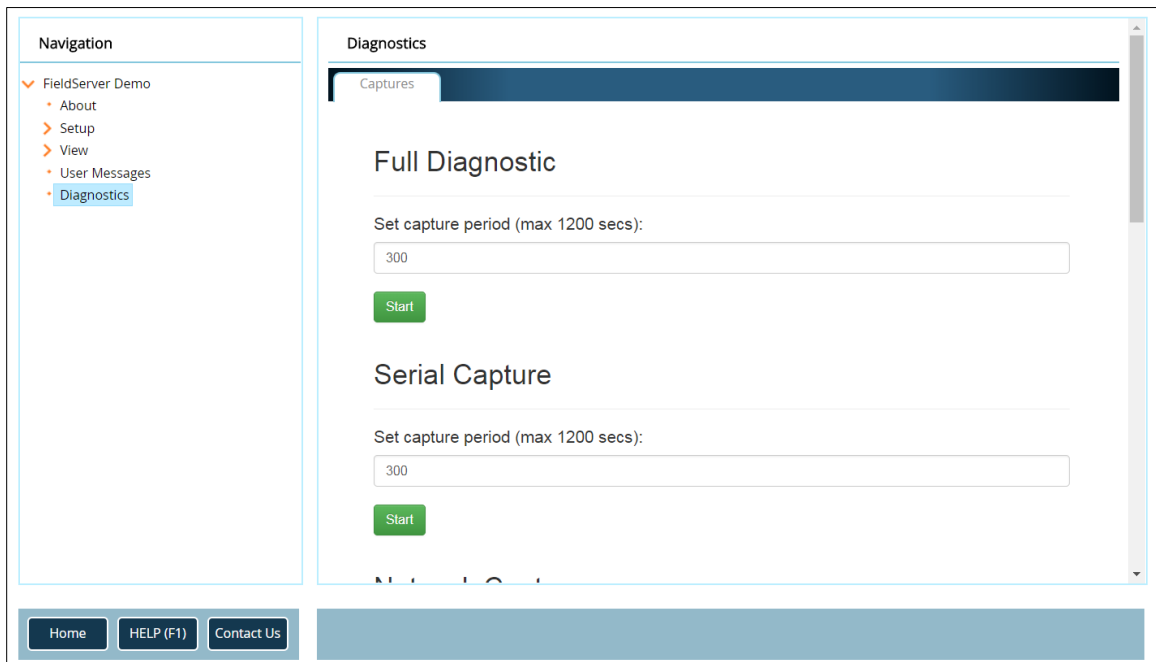


Appendix B.2.2. Using FS-GUI

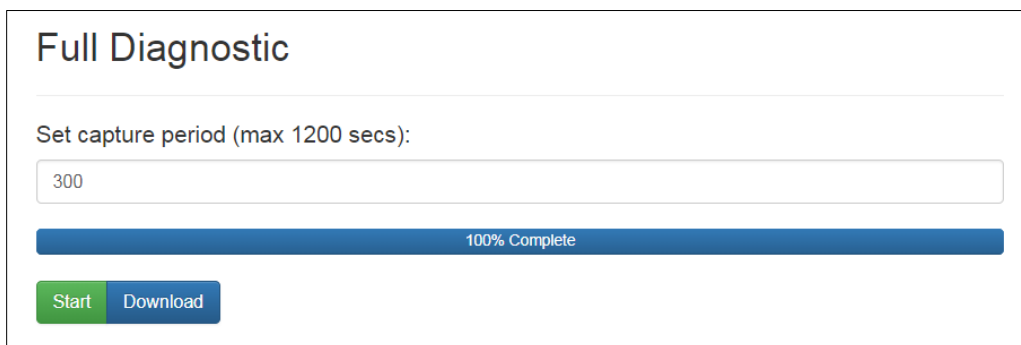
Diagnostic Capture with FS-GUI is only available on FieldServers with a bios updated/released on November 2017 or later. Completing a Diagnostic Capture through the FieldServer allows network connections (such as Ethernet and Wi-Fi) to be captured.

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

- Open the FieldServer FS-GUI page.
- Click on Diagnostics in the Navigation panel.



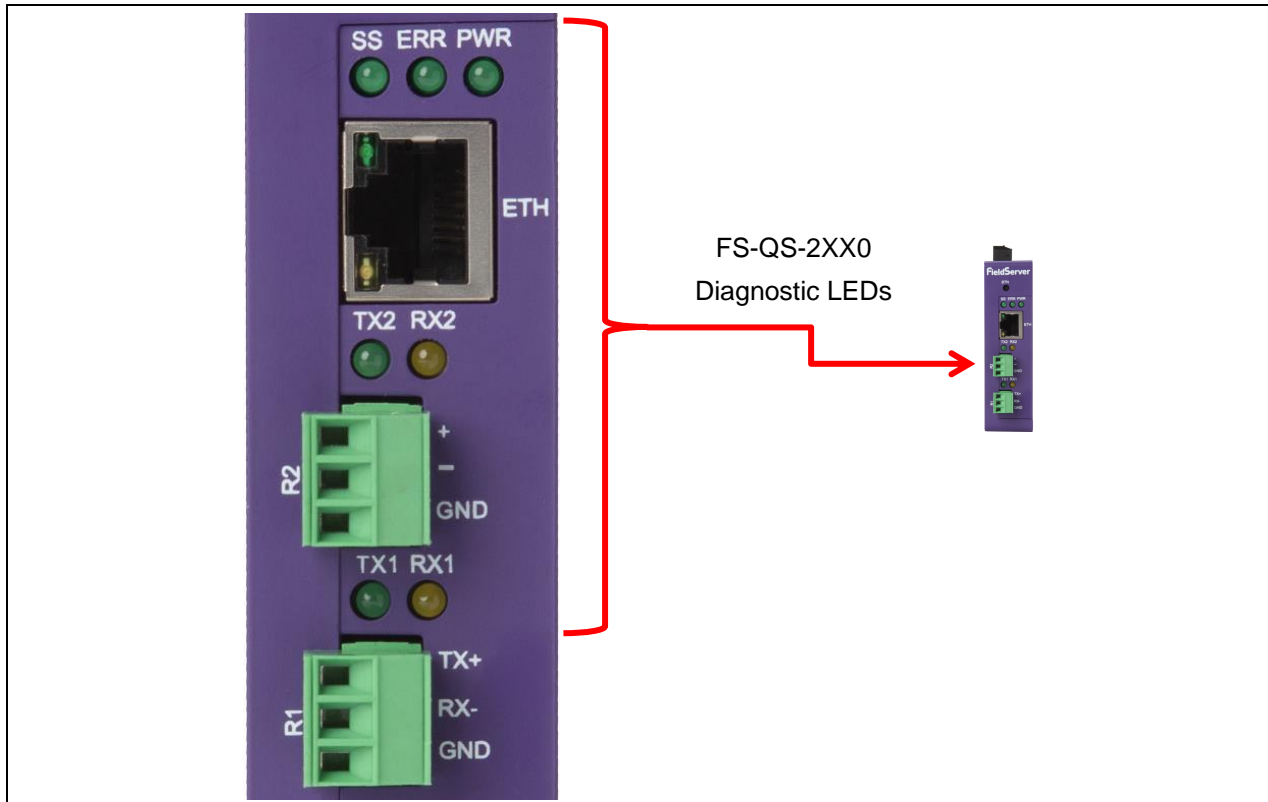
- Go to Full Diagnostic and select the capture period.
- Click the Start button under the Full Diagnostic heading to start the capture.
 - When the capture period is finished, a Download button will appear next to the Start button



- Click Download for the capture to be downloaded to the local PC.
- Send the diagnostic zip file to smc-support@msasafety.com.

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

Appendix B.3. 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	The power light should always show steady green when connected to a functioning power source.
TX	The TX 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. TX1 applies to the R1 connection while TX2 applies to the R2 connection.
RX	The RX 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. RX1 applies to the R1 connection while RX2 applies to the R2 connection.

Figure 22: Diagnostic LEDs

Appendix B.4. Securing QuickServer with Password

Access to the FieldServer can be restricted by enabling a password on the FS-GUI Passwords page – click Setup and then Passwords in the navigation panel. There are 2 access levels defined by 2 account names: Admin and User.

- The Admin account has unrestricted access to the FieldServer.
- The User account can view FieldServer information but can't make changes or restart the unit.

The password needs to be a minimum of eight characters and is **case sensitive**. If the password is lost, click cancel on the password authentication popup window, and e-mail the password recovery token to smc-support@msasafety.com to receive a temporary password from the FieldServer support team. This will allow access to the FieldServer in order to set a new password.

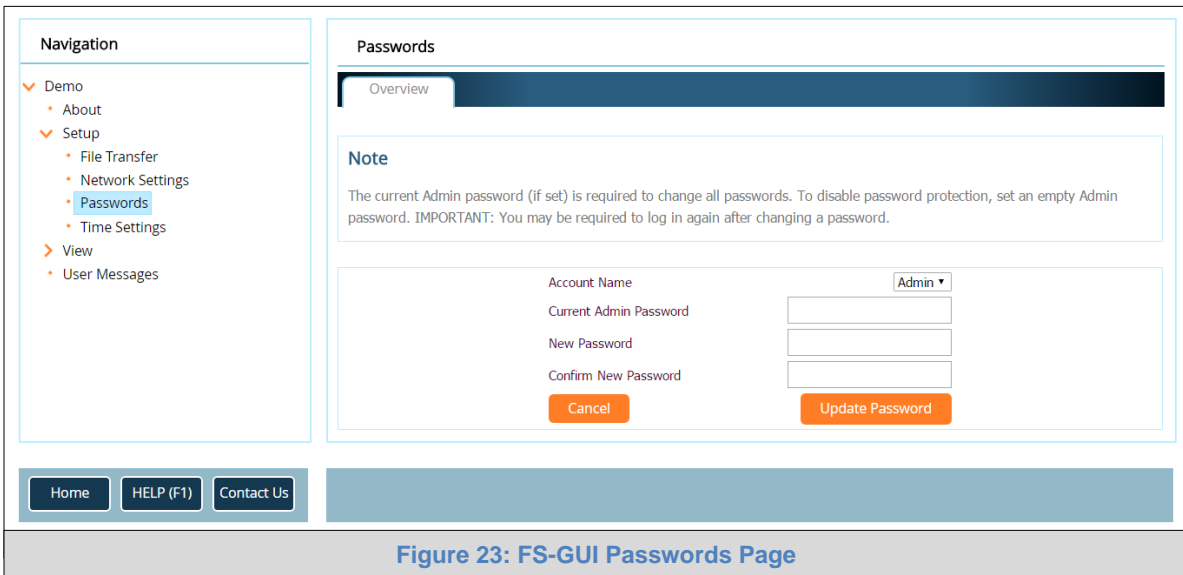


Figure 23: FS-GUI Passwords Page

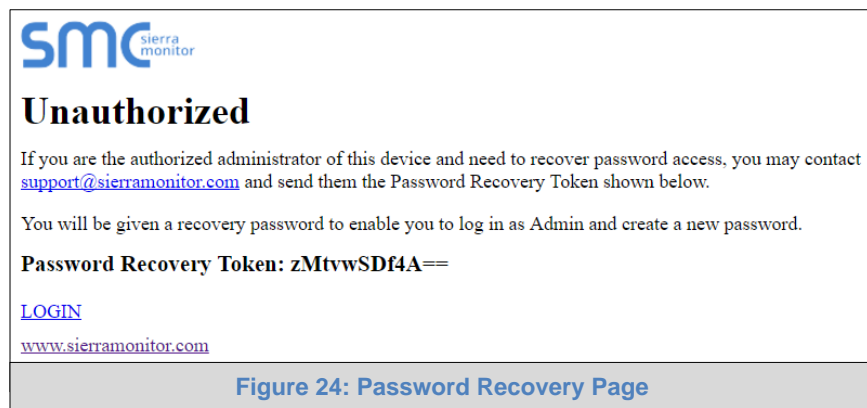


Figure 24: Password Recovery Page

Appendix B.5. Factory Reset Instructions

For FieldServer factory reset instructions, see [ENOTE - FieldServer Next Gen Recovery](#).

Appendix B.6. 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.

Appendix B.7. Change Web Server Security Settings After Initial Setup

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

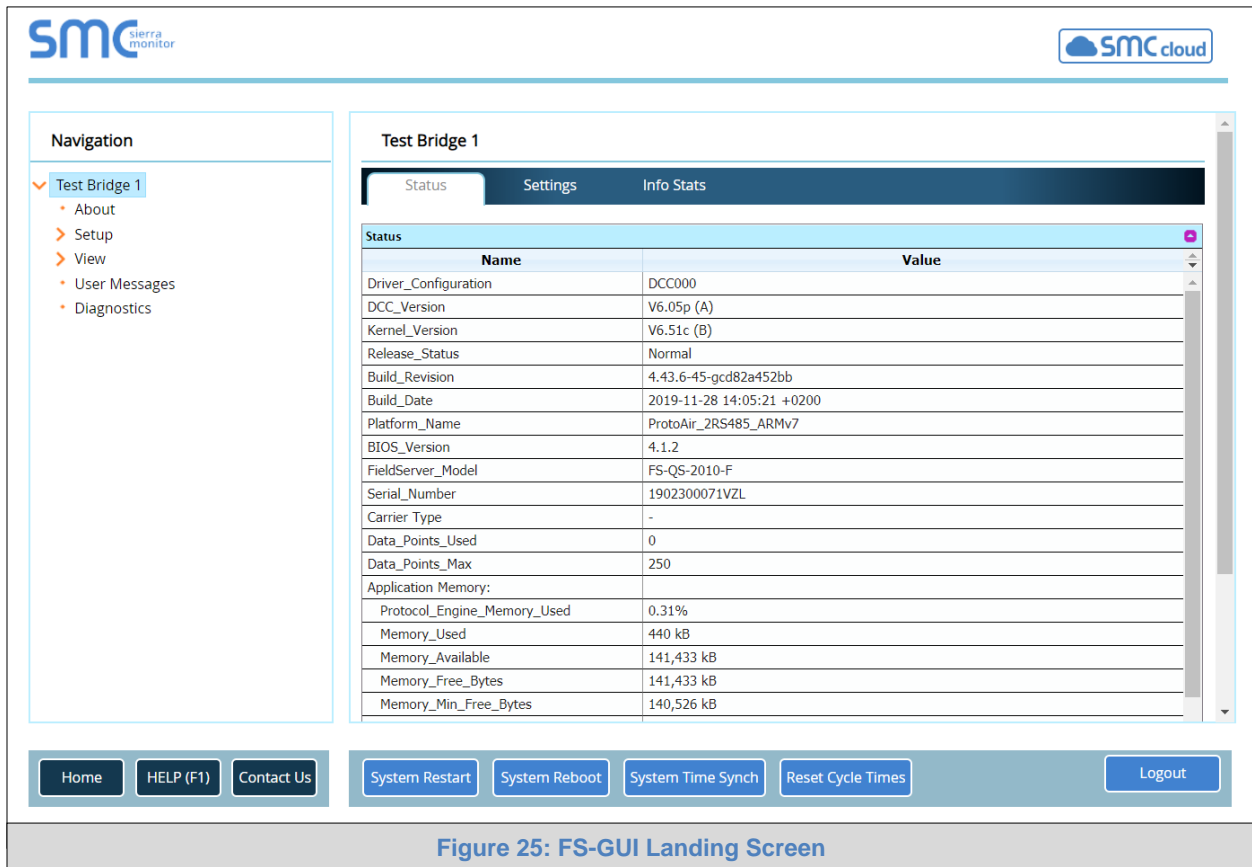


Figure 25: FS-GUI Landing Screen

Appendix B.7.1. Change Security Mode

- Click Security in the Navigation panel.

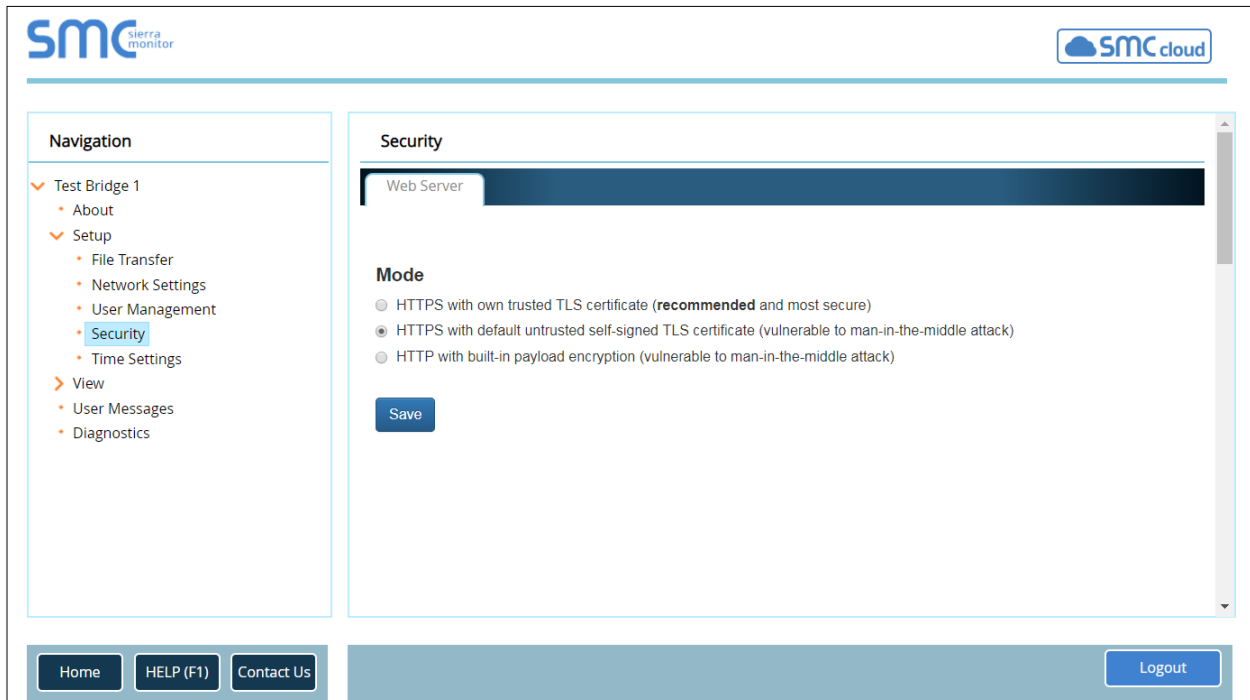


Figure 26: FS-GUI Security Setup

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

Appendix B.7.2. 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.

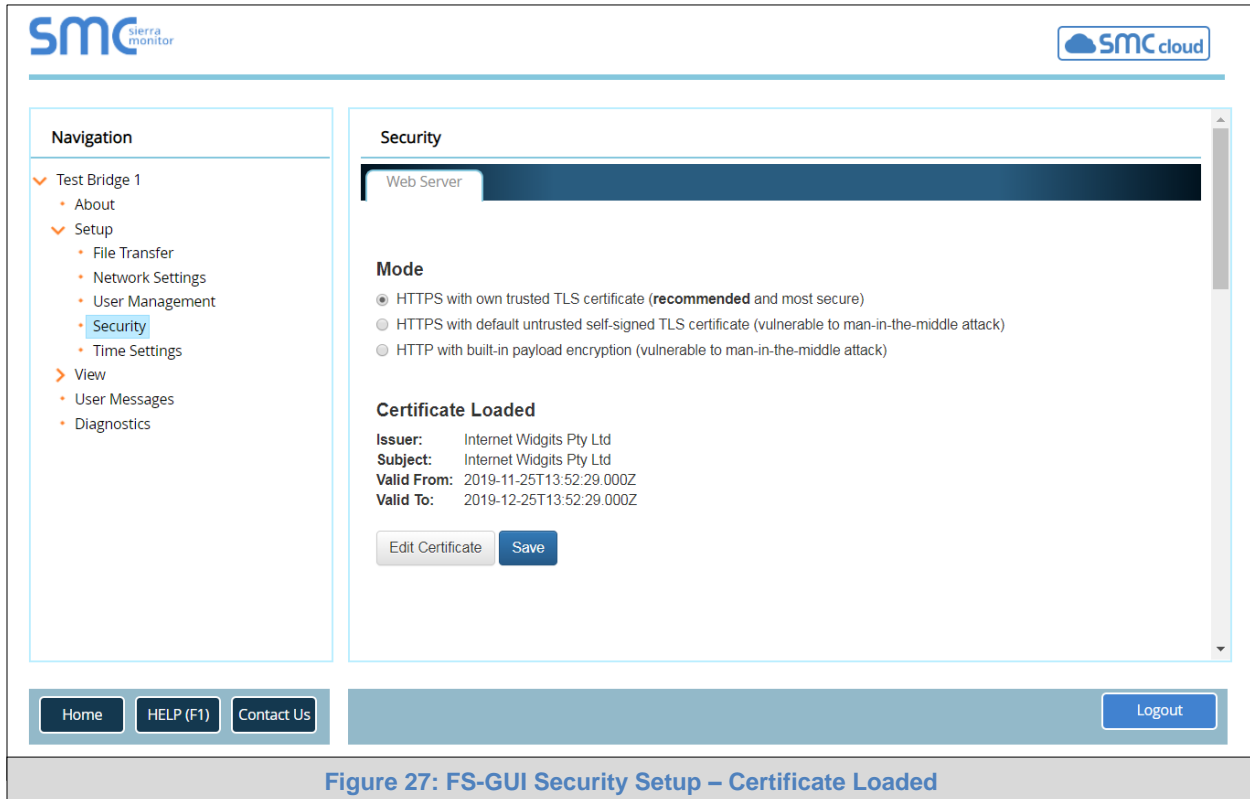


Figure 27: FS-GUI Security Setup – Certificate Loaded

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

Appendix B.8. Change User Management Settings

- 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. If the default unique password is lost, then the unit must be mailed back to the factory.

Appendix B.8.1. User Management

- Check that the Users tab is selected.

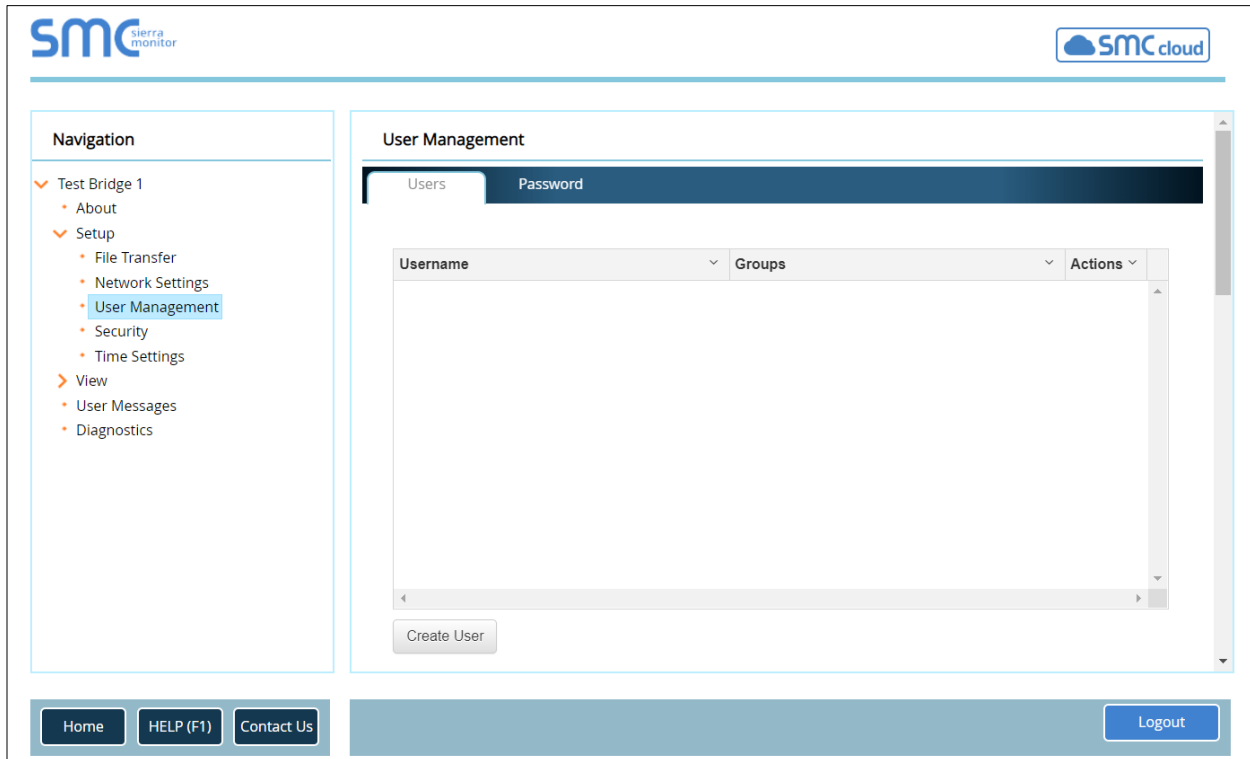


Figure 28: FS-GUI User Management

User Types:

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

Operator – Can only make changes to the writable device points on the FieldServer.

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

Appendix B.8.1.1. Create Users

- Click the Create User button.

- Enter the new User fields: Name, Security Group and Password.

NOTE: Passwords must be at least 10 characters long. An algorithm automatically checks the password entered and notes the level of strength on the top right of the Password text field.

NOTE: User details are hashed and salted.

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

Appendix B.8.1.2. Edit Users

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

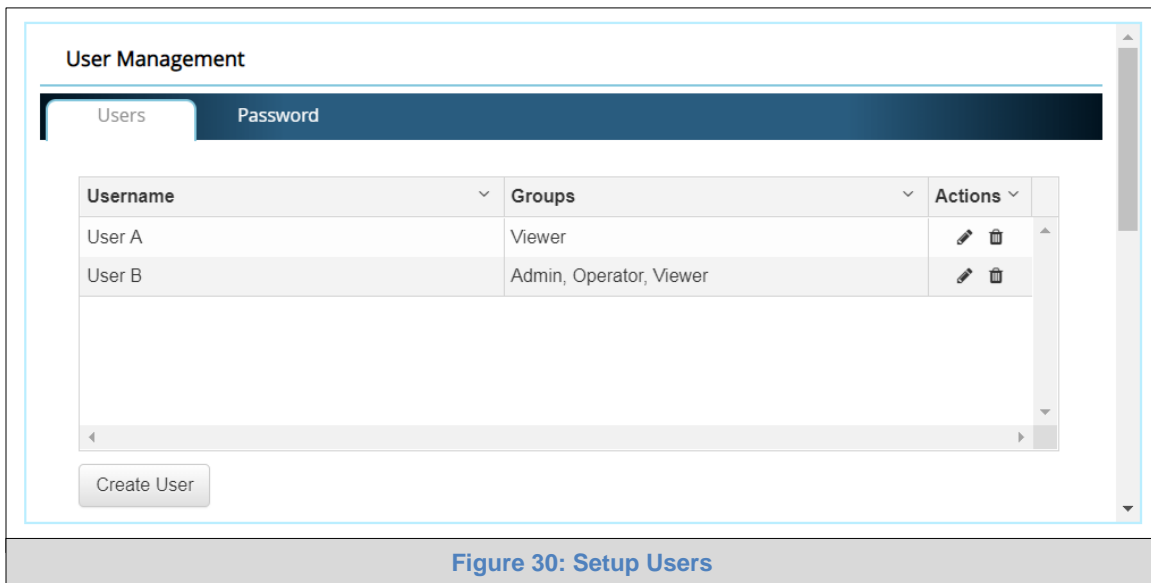


Figure 30: Setup Users

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

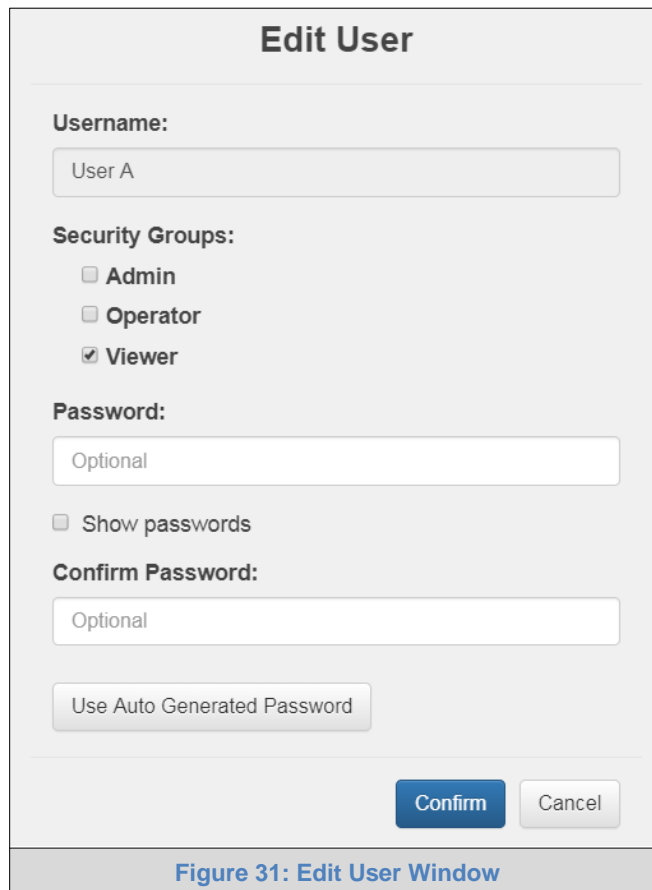


Figure 31: Edit User Window

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

Appendix B.8.1.3. Delete Users

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

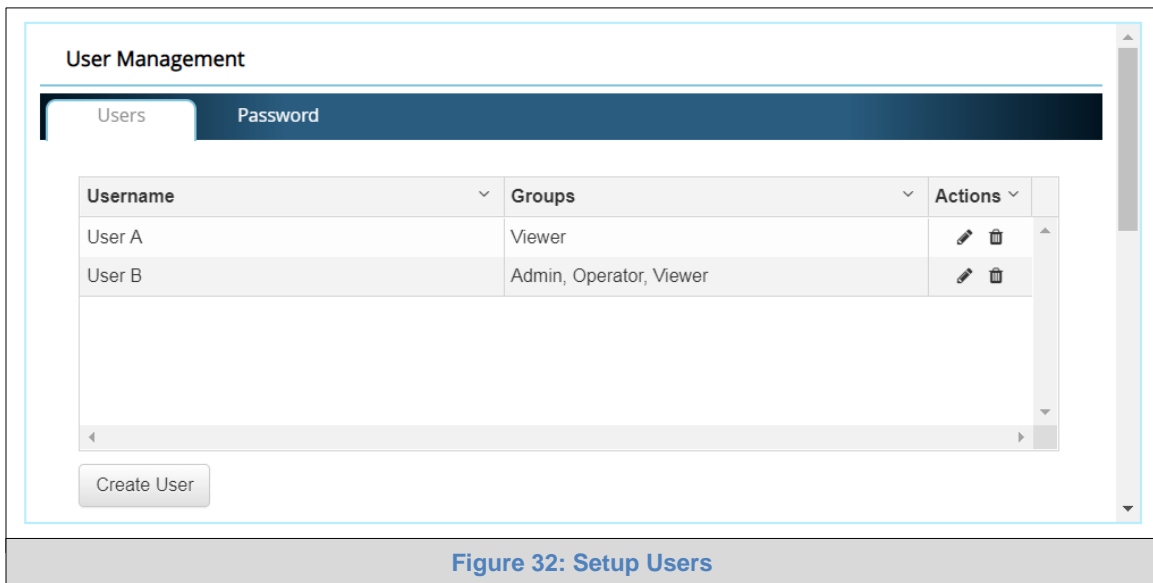


Figure 32: Setup Users

- When the warning message appears, click Confirm.

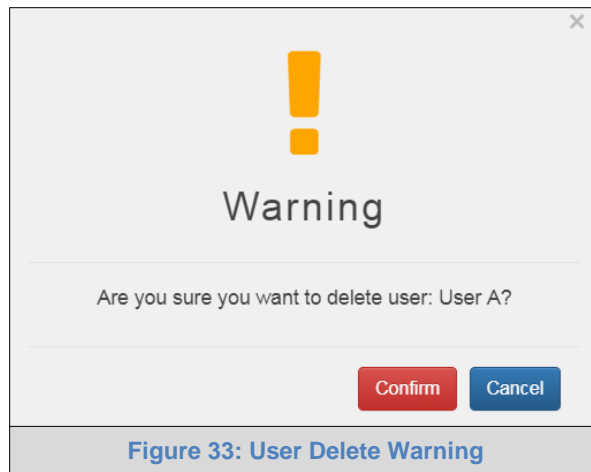


Figure 33: User Delete Warning

Appendix B.8.2. Change FieldServer Password

- Click the Password tab.

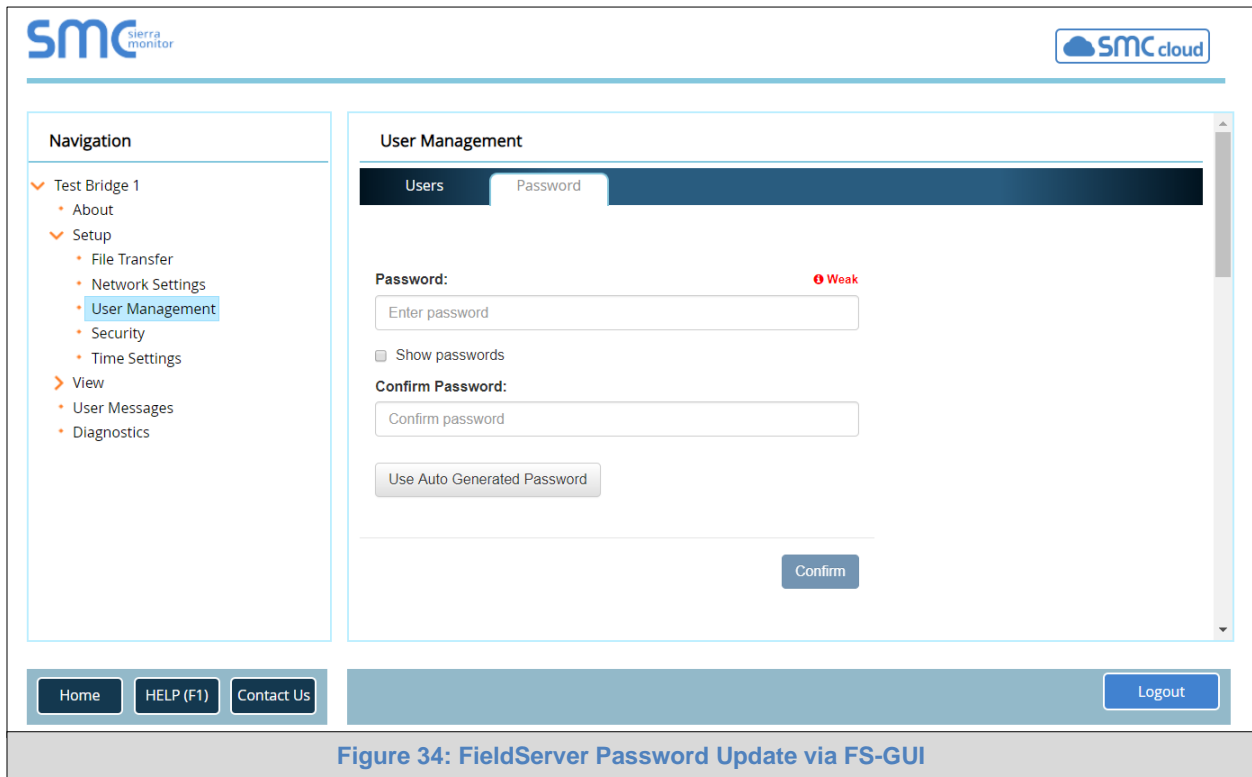


Figure 34: FieldServer Password Update via FS-GUI

- Change the login password for the FieldServer as needed.

NOTE: Passwords must be at least 10 characters long. An algorithm automatically checks the password entered and notes the level of strength on the top right of the Password text field.

APPENDIX C REFERENCE

Appendix C.1. QuickServer FS-QS-2XX0-XXXX DCC

Driver	Code
BACnet/IP – BACnet MS/TP	0285
JCI Metasys N2– BACnet MS/TP	0309
JCI Metasys N2– BACnet/IP	0122
Modbus RTU – BACnet MS/TP	0367
Modbus RTU – BACnet/IP	0104
Modbus RTU – JCI Metasys N2	0038
Modbus TCP/IP – BACnet/IP	0237
Modbus TCP/IP – BACnet MS/TP	0419
Modbus TCP/IP – JCI Metasys N2	0117
SNMP – BACnet/IP	1047
SNMP – JCI Metasys N2	1154
SNMP – BACnet MS/TP	1200

Appendix C.2. QuickServer Part Numbers

		Field Connections							
		Interface Connections							
		RS-232 ¹	RS-485 ²	RS-422 ³	KNX ⁶	RS-485	M-Bus	Ethernet ⁴	LonWorks ⁵
QuickServer	FS-QS-2X10	1	2					1	
	FS-QS-2X20	1	2					1	
	FS-QS-1011		1					1	1
	FS-QS-1211		1					1	1
	FS-QS-1221	1						1	1
	FS-QS-1230		1	1				1	
	FS-QS-1231			1				1	1
	FS-QS-1240		1					1	
	FS-QS-1241					1		1	1
	FS-QS-1A50						1	1	1
	FS-QS-1A51							1	1
	FS-QS-1B50						1	1	1
	FS-QS-1B51							1	1
	FS-QS-1C50						1	1	1
	FS-QS-1C51							1	1

¹ TX/Rx/GND ² +/-Frame Ground ³ See Manual ⁴ 10/100 Base T ⁵ FTT10 ⁶ KNX/EIB TP1

NOTE: The 2X10 and 2X20 are the same hardware model with 1 port that can be either RS-232 or RS-485. The 2X10 has a default setting of RS-485 while the 2X20 has a default setting of RS-232.

Appendix C.3. Compliance with UL Regulations

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

- 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 QuickServer/Net
- 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.

Appendix C.4. Dimension Drawing FS-QS-2XX0-XXXX

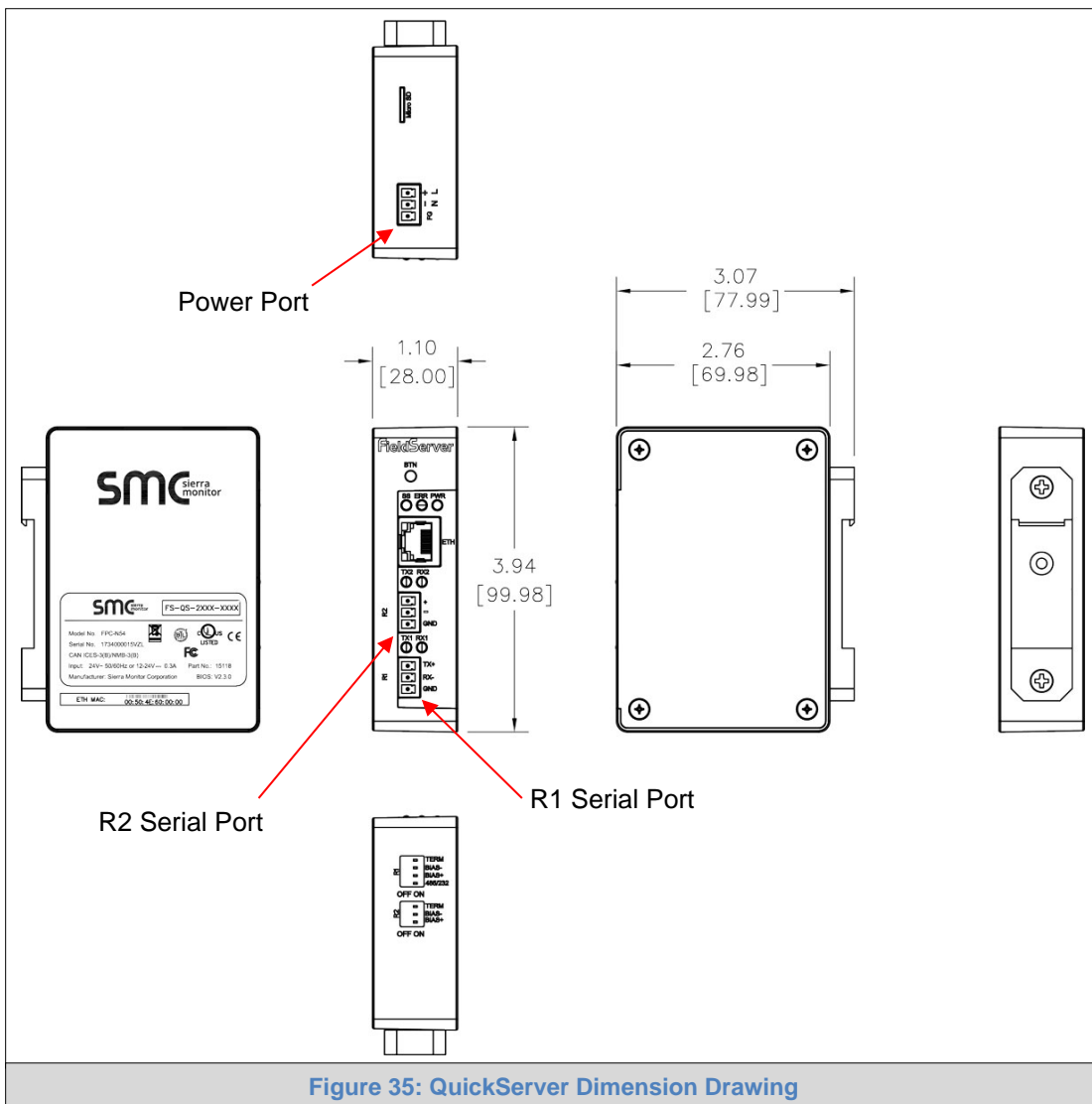


Figure 35: QuickServer Dimension Drawing

Appendix C.5. Specifications



	FS-QS-2XX0-XXXX ²	
Electrical Connections	One 3-pin Phoenix connector with: RS-485/RS-232 (Tx+ / Rx- / gnd) One 3-pin Phoenix connector with: RS-485 (Tx+ / Rx- / gnd) One 3-pin Phoenix connector with: Power port (+ / - / Frame-gnd) One Ethernet 10/100 BaseT port	
Power Requirements	Input Voltage: 9-30VDC or 24VAC Max Power: 3 Watts	Current draw: 24VAC 0.125A 9-30VDC 0.25A @12VDC
Approvals	CE and FCC Class B & C Part 15, UL 60950-1, WEEE compliant, IC Canada, RoHS3 compliant	
Capacity Options	FS-QS-20X0: 250 data points FS-QS-23X0: 500 data points	FS-QS-22X0: 3,000 data points FS-QS-24X0: 5,000 data points
Physical Dimensions	4 x 1.1 x 2.7 in (10.16 x 2.8 x 6.8 cm)	
Weight	0.4 lbs (0.2 Kg)	
Operating Temperature	-20°C to 70°C (-4°F to 158°F)	
Humidity	10-95% RH non-condensing	
Figure 36: Specifications		

“This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his expense. Modifications not expressly approved by FieldServer could void the user's authority to operate the equipment under FCC rules.”

² Specifications subject to change without notice.

APPENDIX D 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.