# FieldServer

# QuickServer Start-up Guide

# FS-QS-2XX0

## APPLICABILITY & EFFECTIVITY

Effective for all systems manufactured after July 2020.

Document Revision: 1.L
T18627

# Technical Support

Please call us for any technical support needs related to the FieldServer product.

MSA Safety
1991 Tarob Court
Milpitas, CA 95035

Website: www.sierramonitor.com

U.S. Support Information:

+1 408 964-4443
+1 800 727-4377

Email: smc-support@msasafety.com

EMEA Support Information:

+31 33 808 0590

Email: smc-support.emea@msasafety.com

# TABLE OF CONTENTS

## LIST OF FIGURES

# 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 – BACnet[1] Testing Laboratory

BACnet is a registered trademark of ASHRAE. ASHRAE does not endorse, approve or test products for compliance with ASHRAE standards. Compliance of listed 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 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.

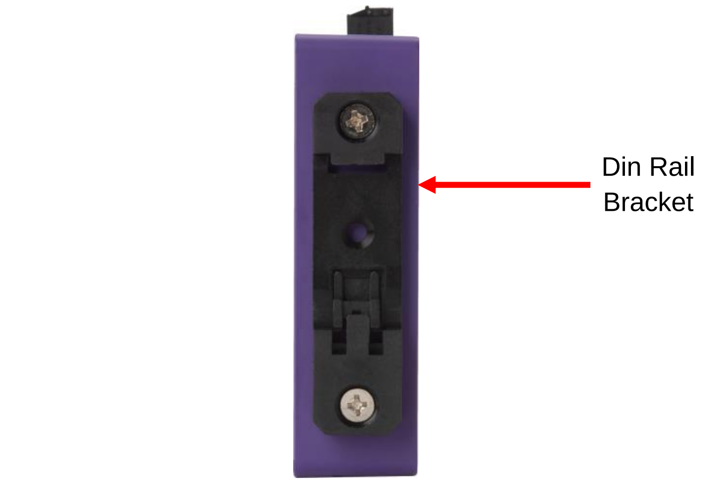


Figure 1: DIN Rail Bracket

**NOTE: For dimension details see Appendix C.4.**

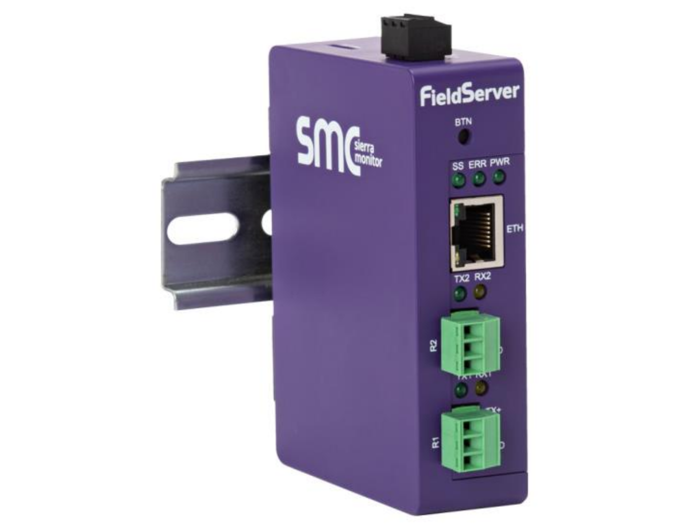


Figure 2: DIN Rail Mounted

## 4.2 DIP Switch Settings

### 4.2.1 Bias Resistors

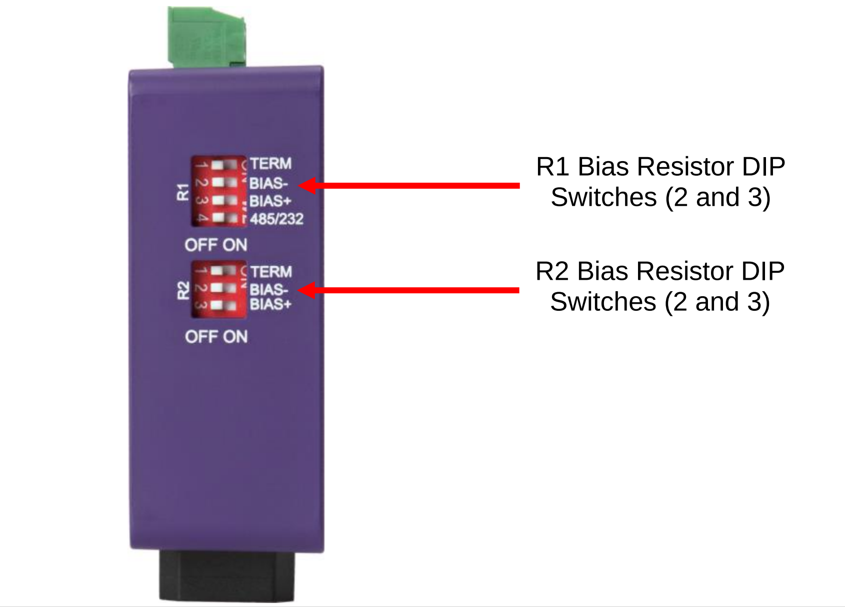

R1
TERM
BIAS-
BIAS+
485/232
OFF ON
R2
TERM
BIAS-
BIAS+
OFF ON
R1 Bias Resistor DIP Switches (2 and 3)
R2 Bias Resistor DIP Switches (2 and 3)

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

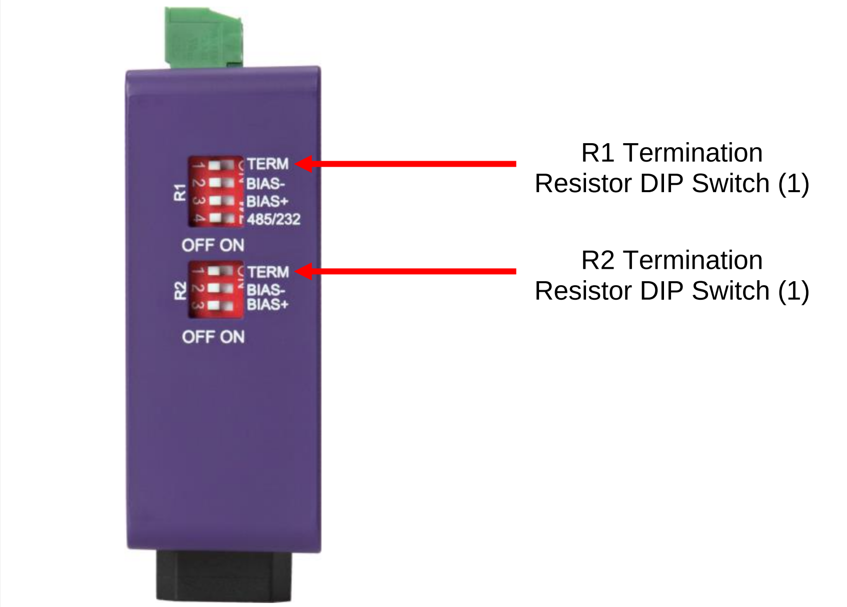

TERM
BIAS-
BIAS+
485/232
R1
OFF ON
TERM
BIAS-
BIAS+
R2
OFF ON
R1 Termination Resistor DIP Switch (1)
R2 Termination Resistor DIP Switch (1)

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.

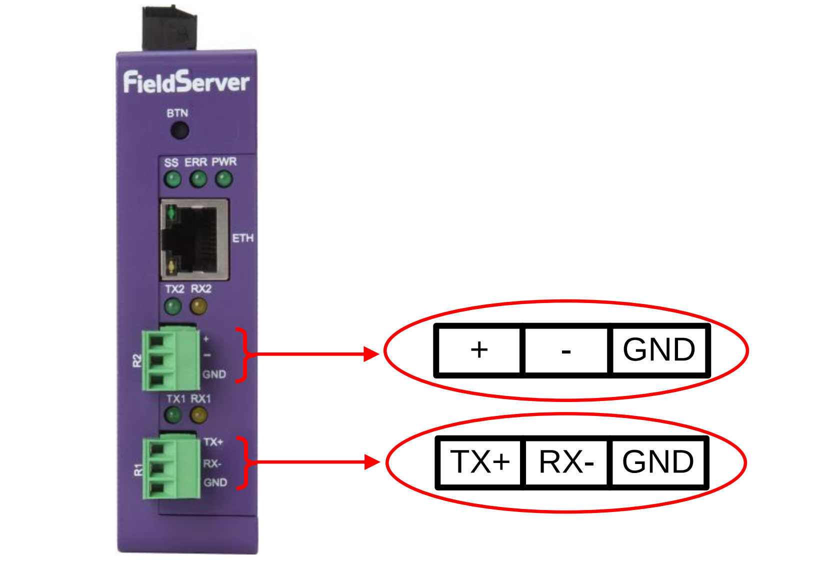


Figure 5: R1 & R2 Connection Ports

### 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.

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

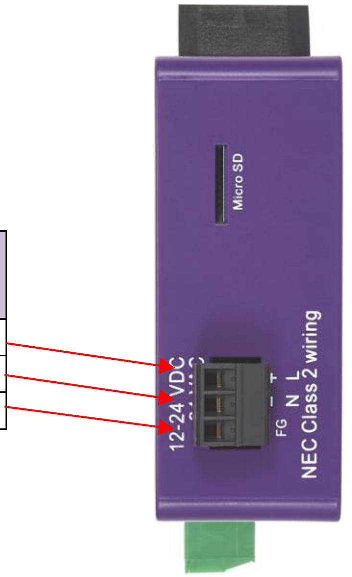


Figure 7: Power Connections

# 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.

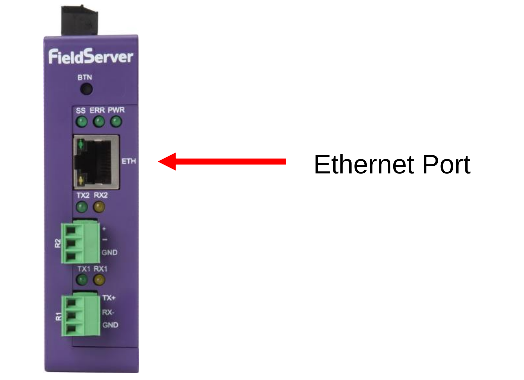


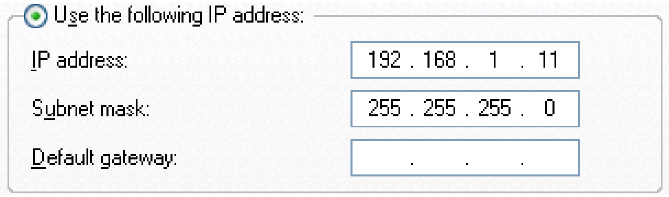
Figure 8: Ethernet Port Location

### 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

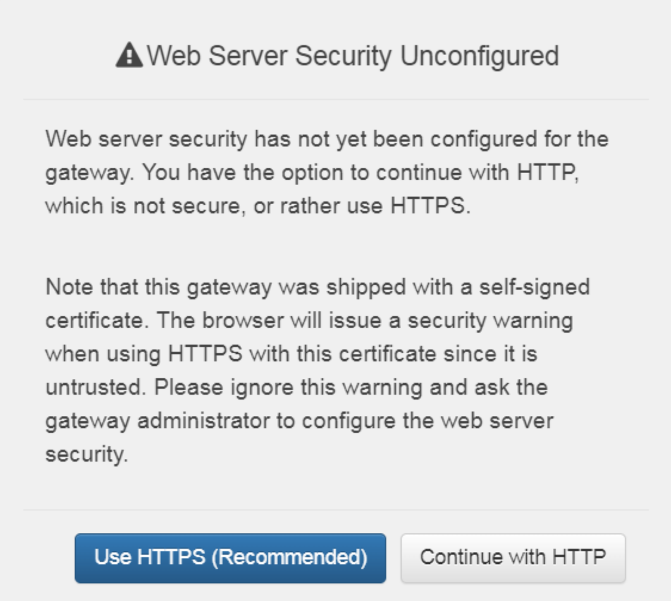
- Open a web browser and connect to the QuickServer's default IP Address. The default IP Address of the FieldServer is **192.168.2.101**, Subnet Mask is **255.255.255.0**.
- If the PC and the QuickServer are on different IP networks, assign a static IP Address to the PC on the 192.168.2.X network.

# 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.



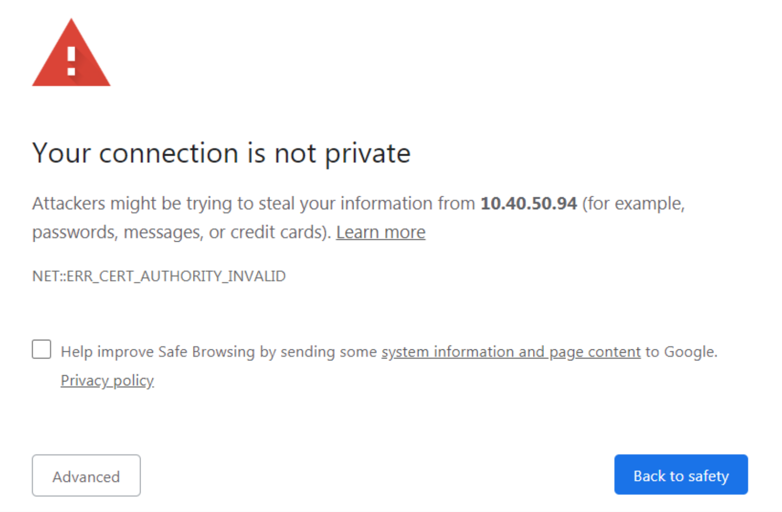
Web Server Security Unconfigured

Web server security has not yet been configured for the gateway. You have the option to continue with HTTP, which is not secure, or rather use HTTPS.

Note that this gateway was shipped with a self-signed certificate. The browser will issue a security warning when using HTTPS with this certificate since it is untrusted. Please ignore this warning and ask the gateway administrator to configure the web server security.

Figure 9: 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.



Your connection is not private

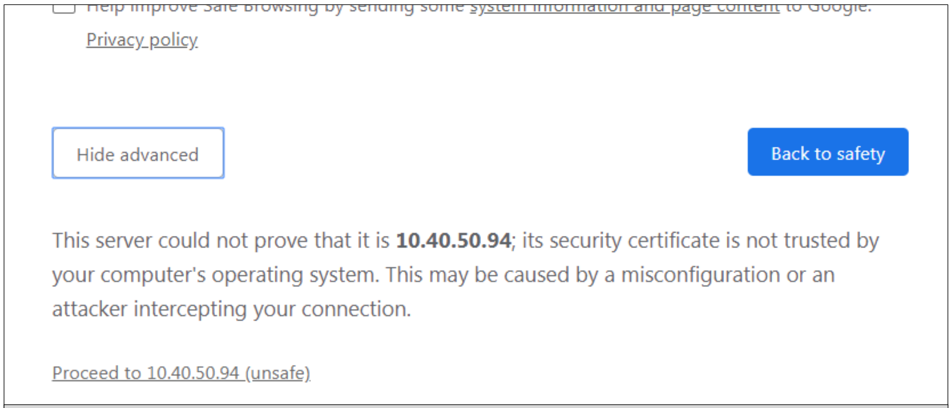
Attackers might be trying to steal your information from **10.40.50.94** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

☐ Help improve Safe Browsing by sending some system information and page content to Google. Privacy policy

Figure 10: Connection Not Private Warning

- 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)".



□ Help improve Safe Browsing by sending some system information and page content to Google. Privacy policy

This server could not prove that it is **10.40.50.94**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to 10.40.50.94 (unsafe)

**Figure 11: 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.**

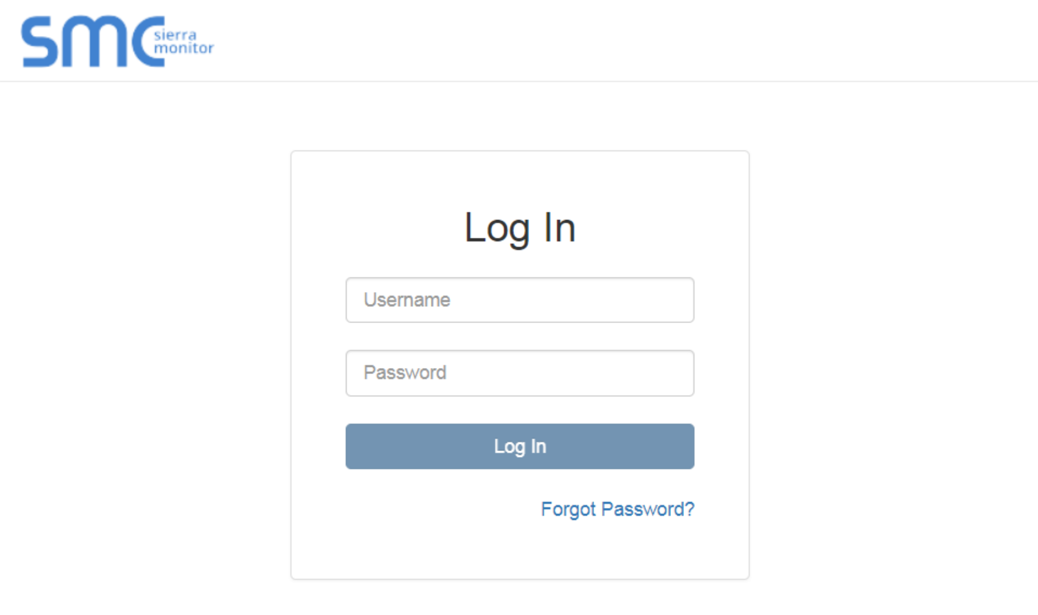


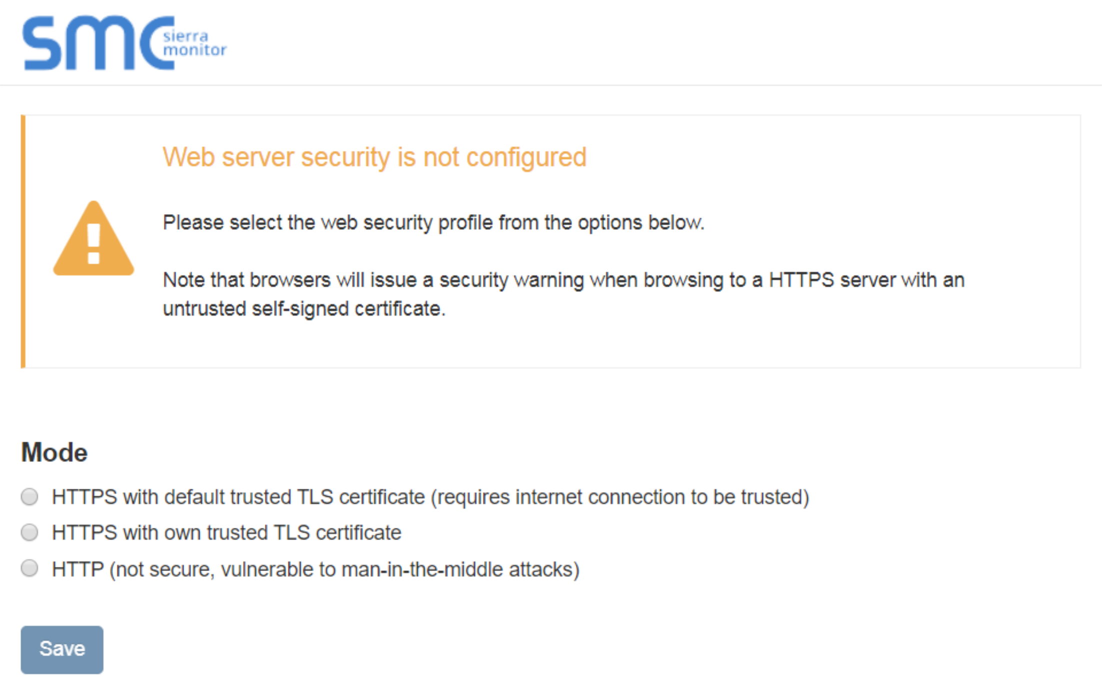
**Figure 12: FieldServer Login**

**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 Appendix B.7.**

## 6.2 Select the Security Mode

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



Web server security is not configured

Please select the web security profile from the options below.

Note that browsers will issue a security warning when browsing to a HTTPS server with an untrusted self-signed certificate.

**Mode**

○ HTTPS with default trusted TLS certificate (requires internet connection to be trusted)

○ HTTPS with own trusted TLS certificate

○ HTTP (not secure, vulnerable to man-in-the-middle attacks)

Figure 13: Security Mode Selection Screen

**NOTE: Cookies are used for authentication.**

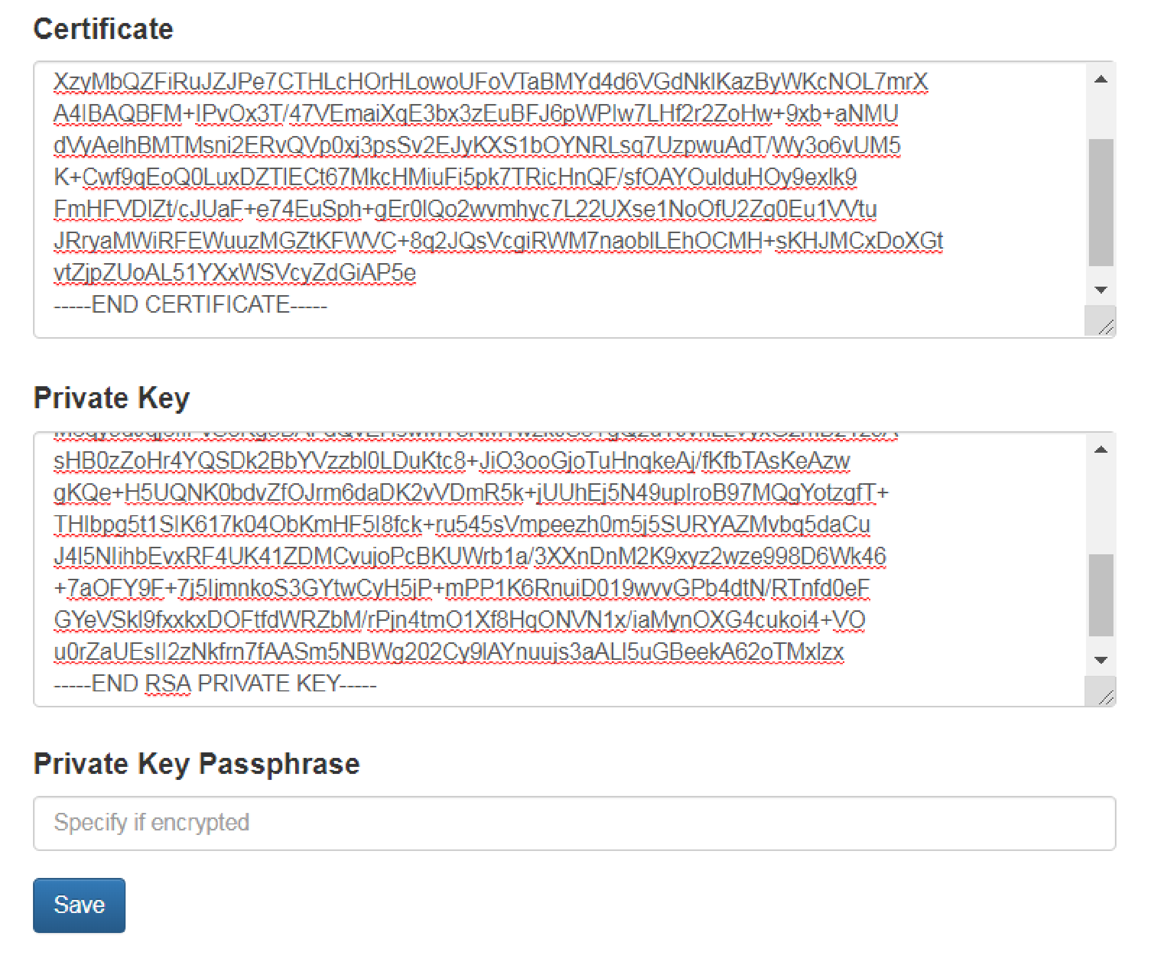
**NOTE: To change the web server security mode after initial setup, go to Appendix B.6.**

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.



**Certificate**

```
XzyMbQZFiRuJZJPe7CTHLcHOrHLowoUFoVTaBMYd4d6VGdNkIKazByWKcNOL7mrX
A4IBAQBFM+IPvOx3T/47VEmaiXqE3bx3zEuBFJ6pWPIw7LHf2r2ZoHw+9xb+aNMU
dVyAelhBMTMsni2ERvQVp0xj3psSv2EJyKXS1bOYNRLsq7UzpwuAdT/Wy3o6vUM5
K+Cwf9qEoQ0LuxDZTIECt67MkcHMiuFi5pk7TRicHnQF/sfOAYOuIduHOy9exIk9
FmHFVDIZt/cJUaF+e74EuSph+gEr0IQo2wvmhyc7L22UXse1NoOfU2Zg0Eu1VVtu
JRryaMWiRFEWuuzMGZtKFWVC+8q2JQsVcgiRWM7naobILEhOCMH+sKHJMCxDoXGt
vtZjpZUoAL51YXxWSVcyZdGiAP5e
-----END CERTIFICATE-----
```

**Private Key**

```
sHB0zZoHr4YQSDk2BbYVzzbl0LDuKtc8+JiO3ooGjoTuHnqkeAj/fKfbTAsKeAzw
gKQe+H5UQNK0bdvZfOJrm6daDK2vVDmR5k+jUUhEj5N49upIroB97MQgYotzgfT+
THIbpg5t1SIK617k04ObKmHF5I8fck+ru545sVmpeezh0m5j5SURYAZMvbq5daCu
J4I5NIihbEvxRF4UK41ZDMCvujoPcBKUWrb1a/3XXnDnM2K9xyz2wze998D6Wk46
+7aOFY9F+7j5IjmnkoS3GYtwCyH5jP+mPP1K6RnuiD019wvvGPb4dtN/RTnfd0eF
GYeVSkl9fxxkxDOFtfdWRZbM/rPjn4tmO1Xf8HqONVN1x/iaMynOXG4cukoi4+VO
u0rZaUEsII2zNkfrn7fAASm5NBWg202Cy9IAYnuujs3aALI5uGBeekA62oTMxlzx
-----END RSA PRIVATE KEY-----
```

**Private Key Passphrase**

Specify if encrypted

**Figure 14: Security Mode Selection Screen – Certificate & Private Key**

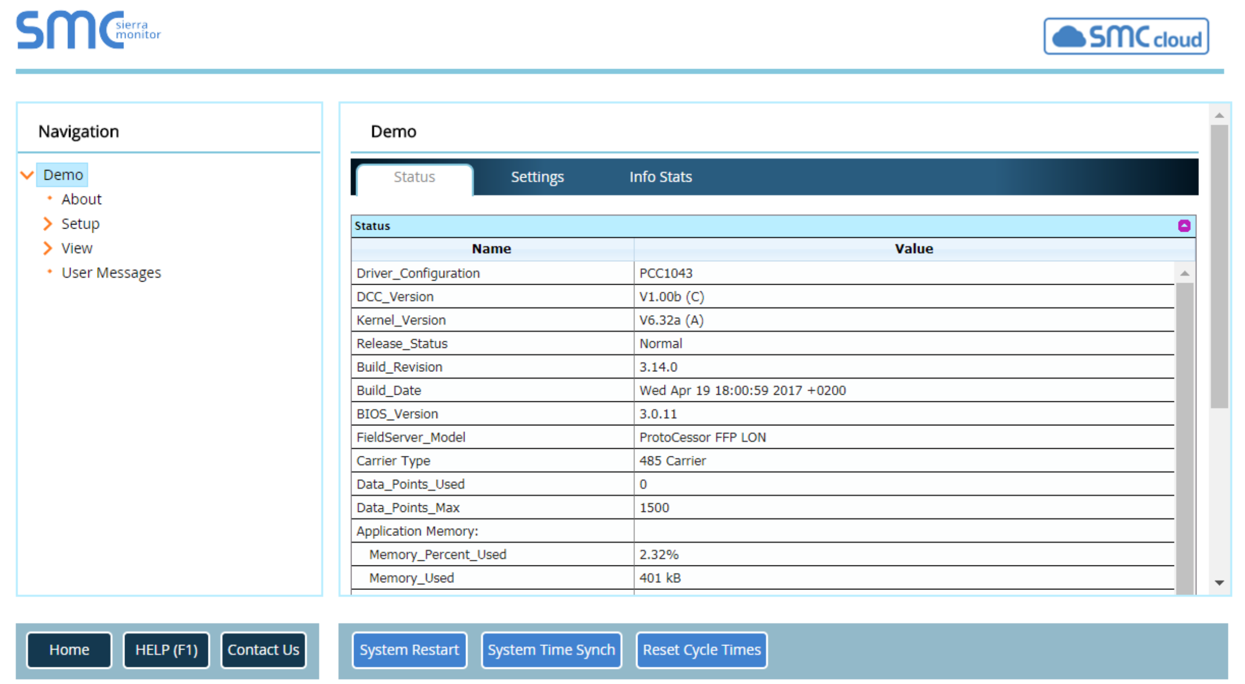
- Copy and paste the Certificate and Private Key text into their respective fields. If the Private Key is encrypted type in the associated Passphrase.
- Click Save.
- A "Redirecting" message will appear. After a short period of time the FieldServer GUI will open.

### 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 will appear. 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.



Status

| Name | Value |
|---|---|
| Driver_Configuration | PCC1043 |
| DCC_Version | V1.00b (C) |
| Kernel_Version | V6.32a (A) |
| Release_Status | Normal |
| Build_Revision | 3.14.0 |
| Build_Date | Wed Apr 19 18:00:59 2017 +0200 |
| BIOS_Version | 3.0.11 |
| FieldServer_Model | ProtoCessor FFP LON |
| Carrier Type | 485 Carrier |
| Data_Points_Used | 0 |
| Data_Points_Max | 1500 |
| Application Memory: | |
| Memory_Percent_Used | 2.32% |
| Memory_Used | 401 kB |

Figure 15: FS-GUI Landing Page

**NOTE: The SMC Cloud button SMC cloud (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.**

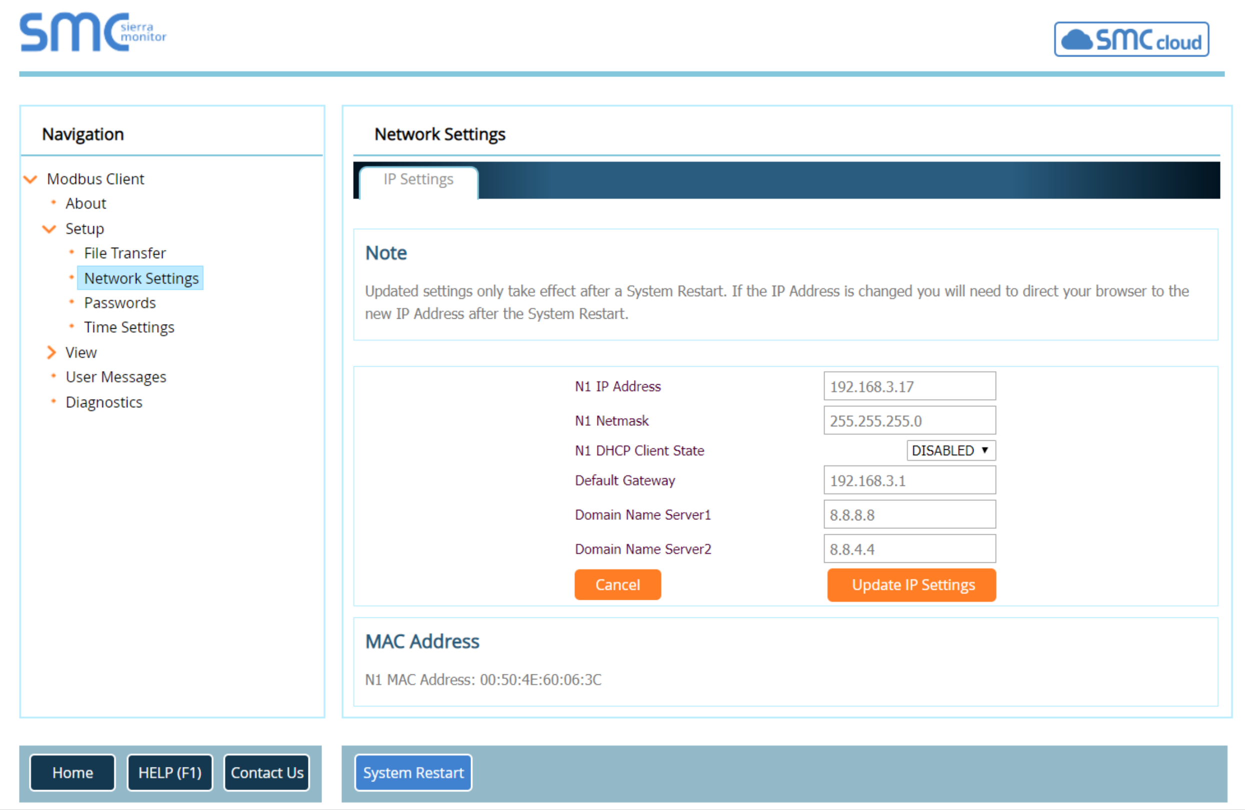
## 7.1 Set IP Address of the QuickServer Using FS-GUI

- 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.**



Note

Updated settings only take effect after a System Restart. If the IP Address is changed you will need to direct your browser to the new IP Address after the System Restart.

| | |
|---|---|
| N1 IP Address | 192.168.3.17 |
| N1 Netmask | 255.255.255.0 |
| N1 DHCP Client State | DISABLED ▾ |
| Default Gateway | 192.168.3.1 |
| Domain Name Server1 | 8.8.8.8 |
| Domain Name Server2 | 8.8.4.4 |

MAC Address

N1 MAC Address: 00:50:4E:60:06:3C

Figure 16: FS-GUI Network Settings

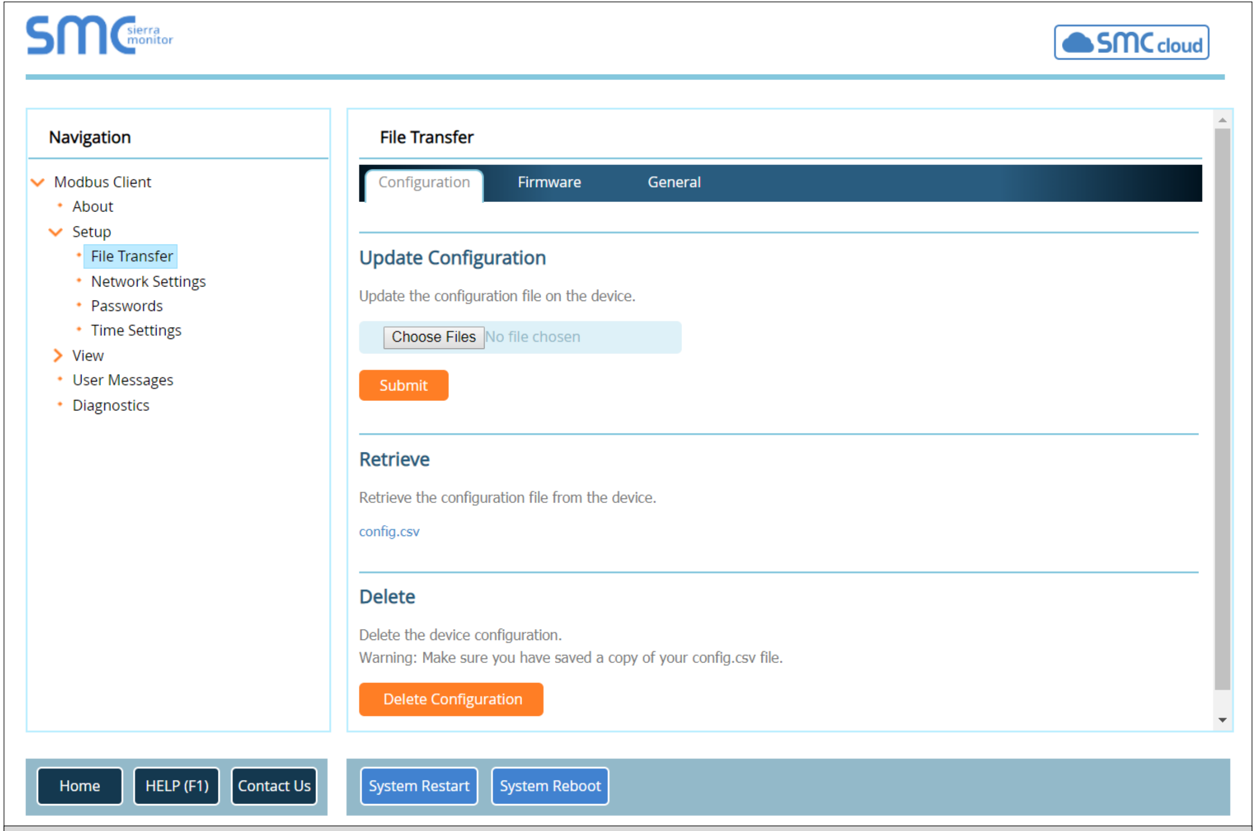
**NOTE: The SMC Cloud button SMC cloud (see Figure 16) allows users to connect to the SMC Cloud, MSA Safety's device cloud solution for IIoT. The SMC Cloud enables secure remote connection to field devices through a FieldServer and its local applications for configuration, management, maintenance. For 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.



Update Configuration

Update the configuration file on the device.

Retrieve

Retrieve the configuration file from the device.

Delete

Delete the device configuration.
Warning: Make sure you have saved a copy of your config.csv file.

Figure 17: FS-GUI File Transfer

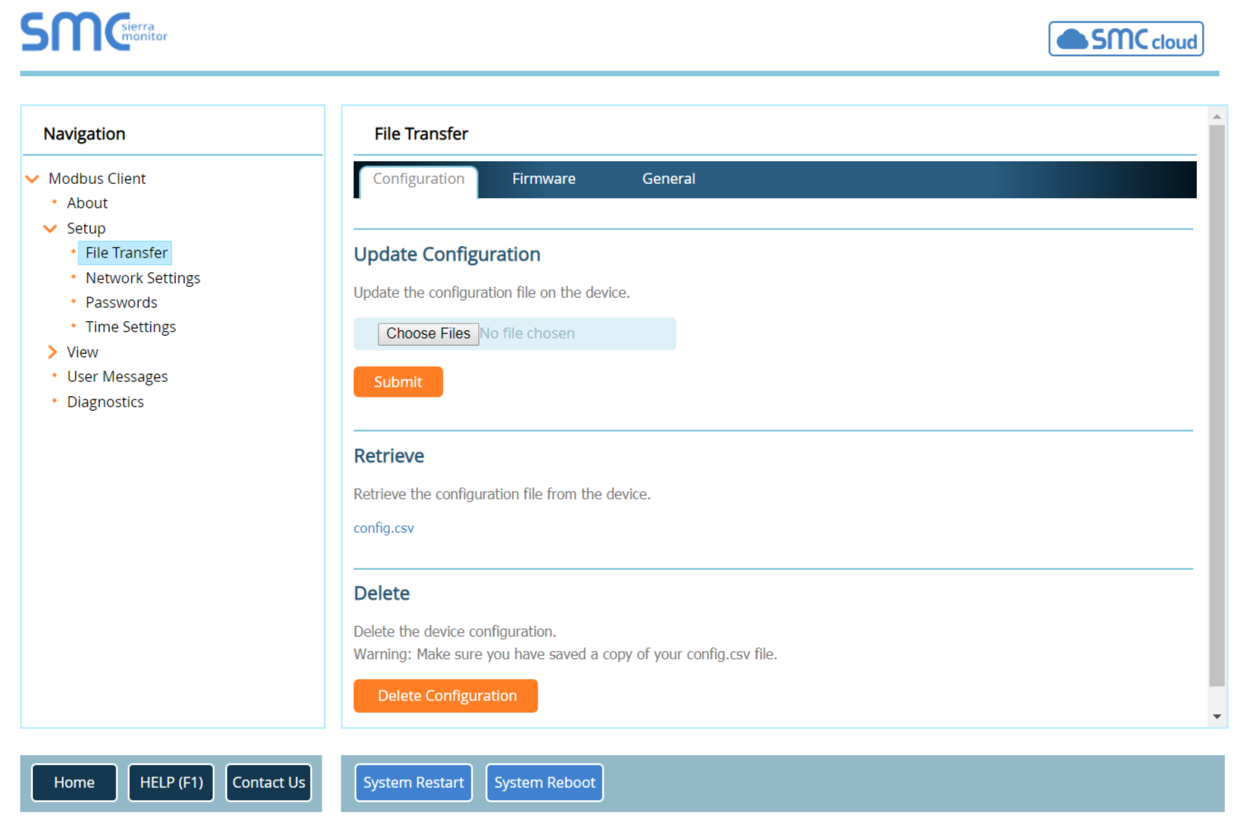
## 7.3 Change the Configuration File to Meet the Application

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”.



Update Configuration

Update the configuration file on the device.

Retrieve

Retrieve the configuration file from the device.

Delete

Delete the device configuration.
Warning: Make sure you have saved a copy of your config.csv file.

Figure 18: FS-GUI Loading Files

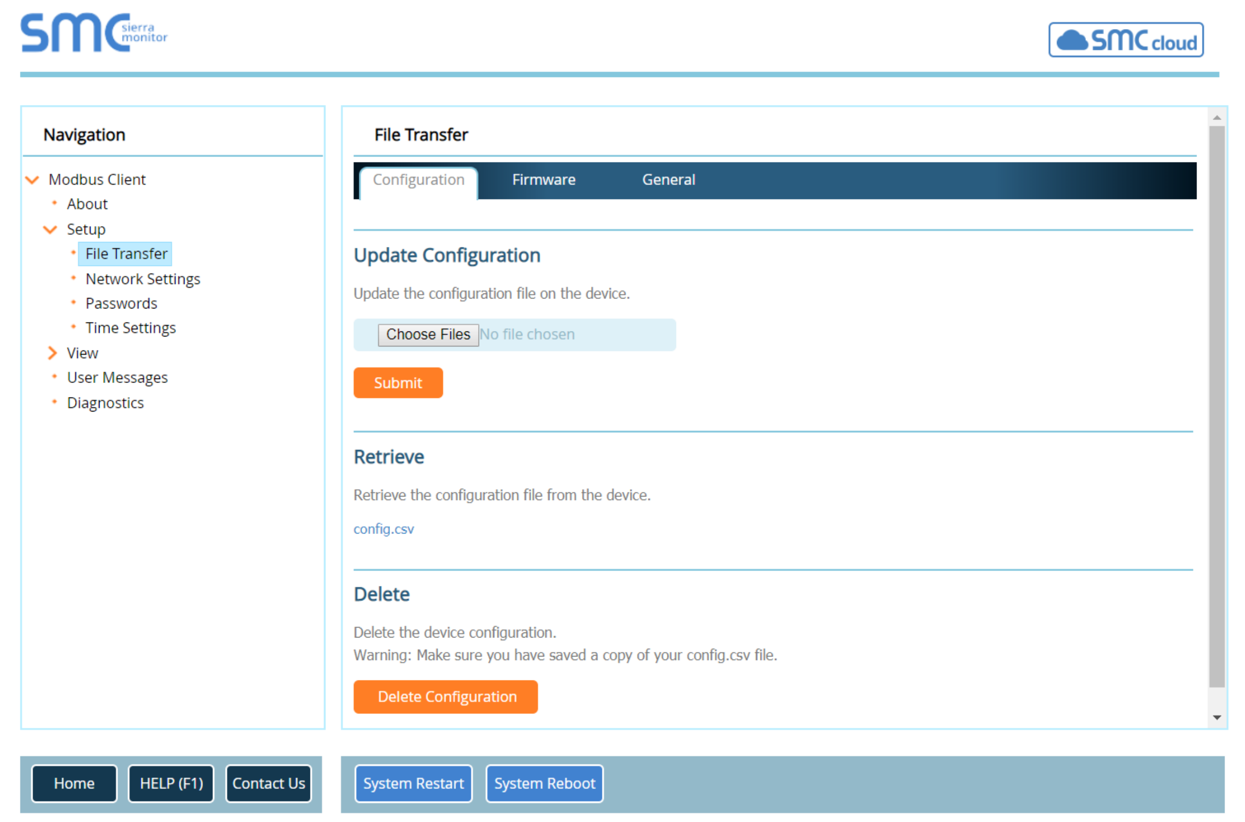
- Once download is complete, a message bar will appear confirming that the configuration was updated successfully.
- Click the System Restart Button to put the new file into operation.

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

### 7.4.2 Retrieve the Configuation 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”.



Update Configuration

Update the configuration file on the device.

Retrieve

Retrieve the configuration file from the device.

Delete

Delete the device configuration.
Warning: Make sure you have saved a copy of your config.csv file.

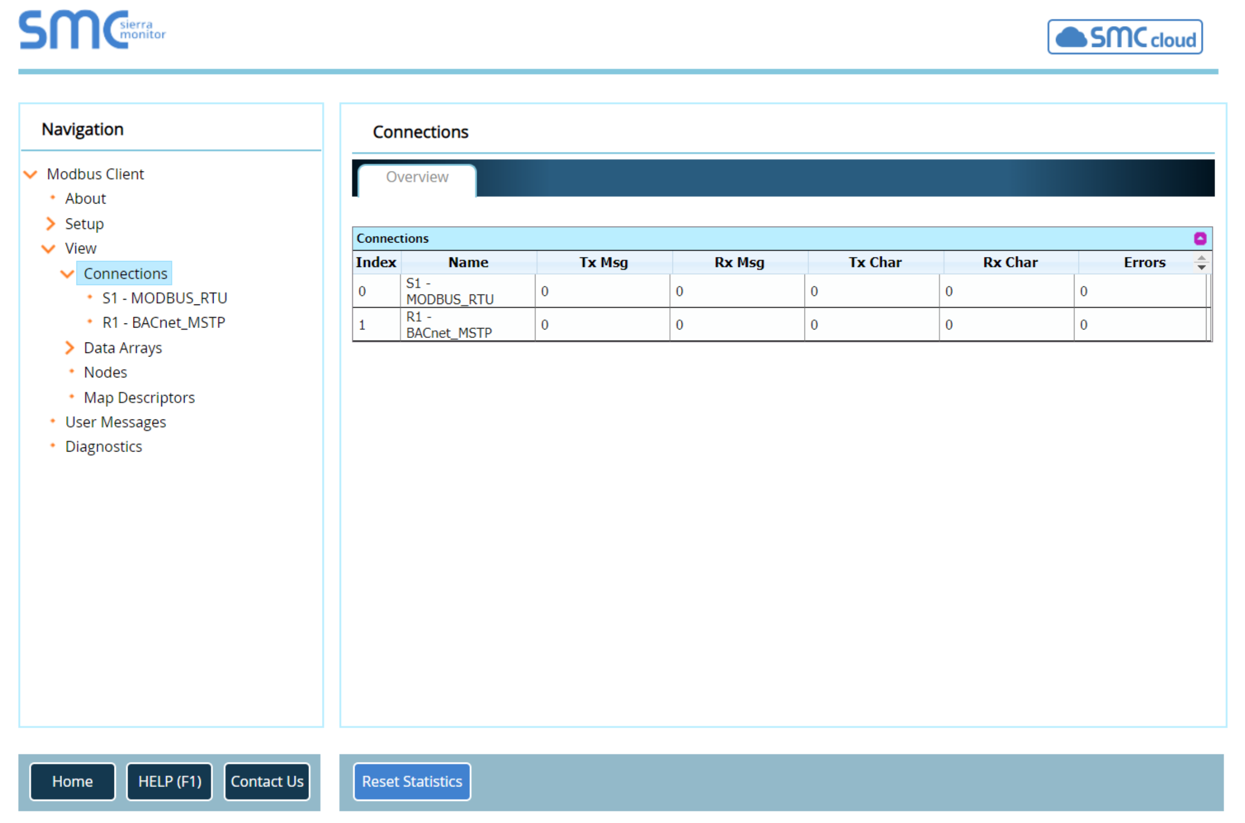
Figure 19: Retrieve Configuration File

- 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.



Connections

| Index | Name | Tx Msg | Rx Msg | Tx Char | Rx Char | Errors |
|---|---|---|---|---|---|---|
| 0 | S1 - MODBUS_RTU | 0 | 0 | 0 | 0 | 0 |
| 1 | R1 - BACnet_MSTP | 0 | 0 | 0 | 0 | 0 |

**Figure 20: FS-GUI Connections Page**

### 7.5.1 Accessing SMC Cloud

The SMC Cloud button SMC cloud (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

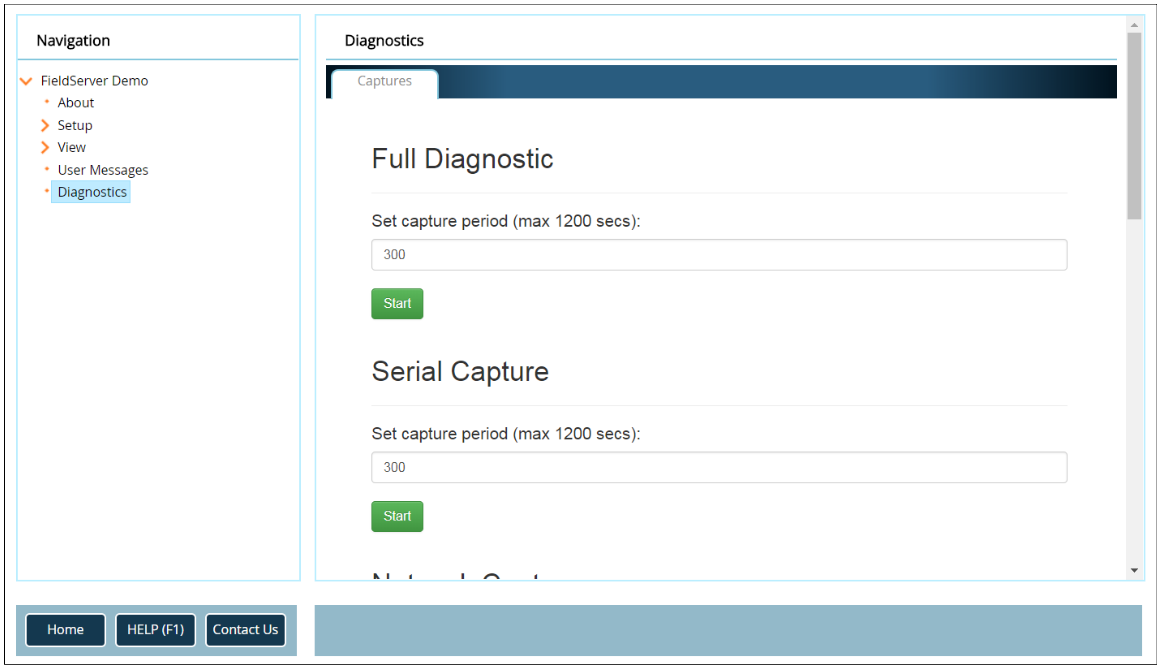
- Confirm that the network cabling is correct.
- Confirm that the computer network card is operational and correctly configured.
- Confirm that there is an Ethernet adapter installed in the PC's Device Manager List, and that it is configured to run the TCP/IP protocol.
- Check that the IP netmask of 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. 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



Diagnostics

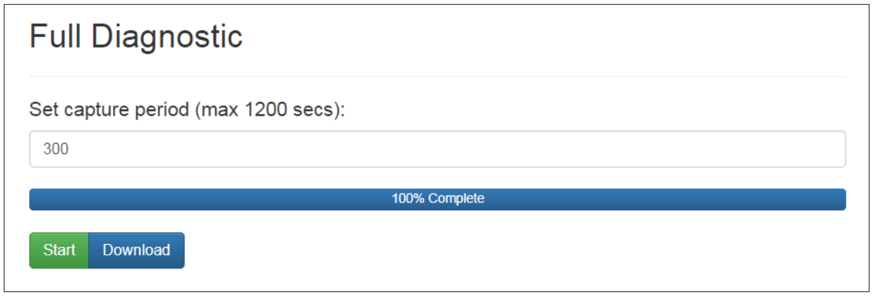
Full Diagnostic

Set capture period (max 1200 secs): 300

Serial Capture

Set capture period (max 1200 secs): 300

- 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



Full Diagnostic

Set capture period (max 1200 secs): 300

100% Complete

- Click Download for the capture to be downloaded to the local PC.
- Send the diagnostic zip file to technical support (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.2.1. 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.**

**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.

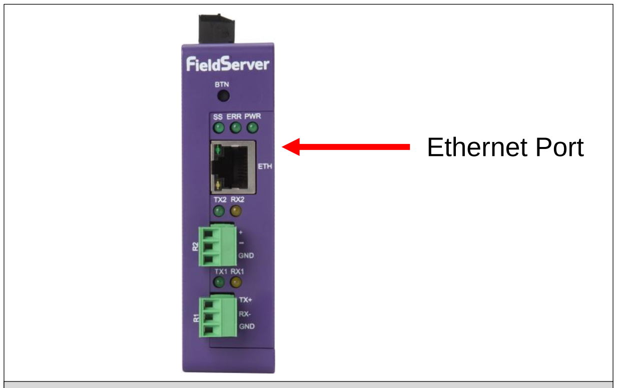
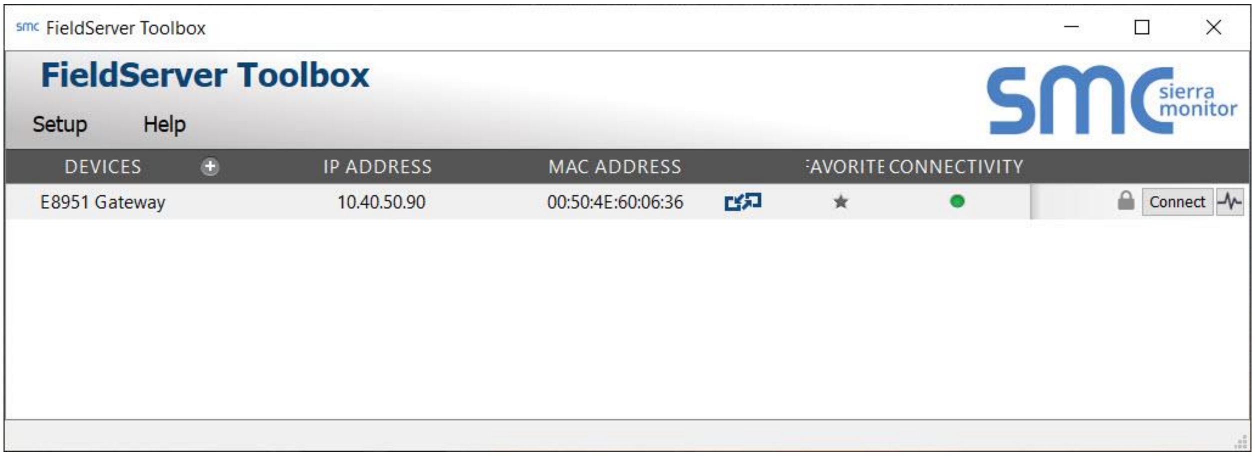


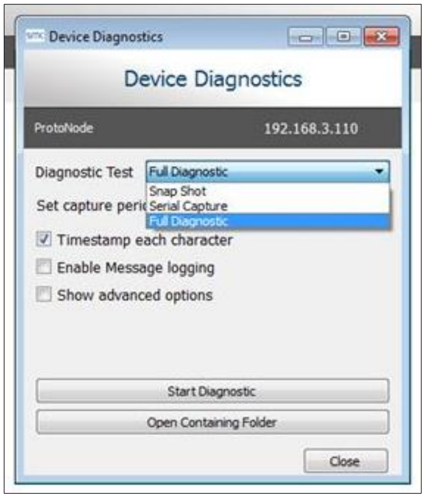
Figure 21: Ethernet Port Location

- 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



| DEVICES | IP ADDRESS | MAC ADDRESS | :AVORITE | CONNECTIVITY |
|---|---|---|---|---|
| E8951 Gateway | 10.40.50.90 | 00:50:4E:60:06:36 | ★ | ● |

- Select “Full Diagnostic" from the drop down menu



Diagnostic Test: Full Diagnostic

Set capture peri

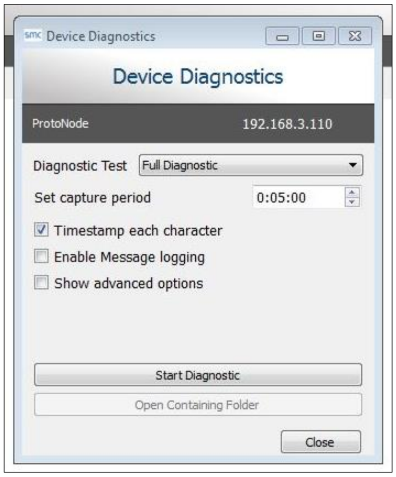
☑ Timestamp each character

☐ Enable Message logging

☐ Show advanced options

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

- Click on the Start Diagnostic button



Diagnostic Test: Full Diagnostic

Set capture period: 0:05:00

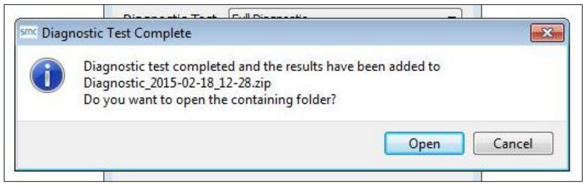
☑ Timestamp each character

☐ Enable Message logging

☐ Show advanced options

- 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

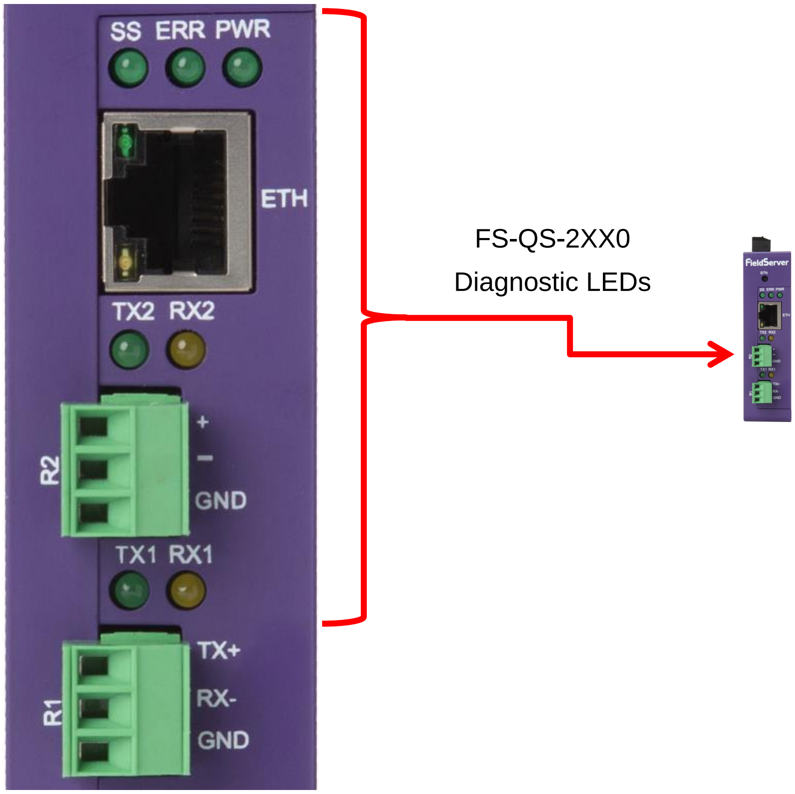


Diagnostic test completed and the results have been added to Diagnostic_2015-02-18_12-28.zip
Do you want to open the containing folder?

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

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

## Appendix B.3. LED Functions



FS-QS-2XX0
Diagnostic LEDs

| 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.<br>**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.<br>**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. Factory Reset Instructions

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

## Appendix B.5. 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

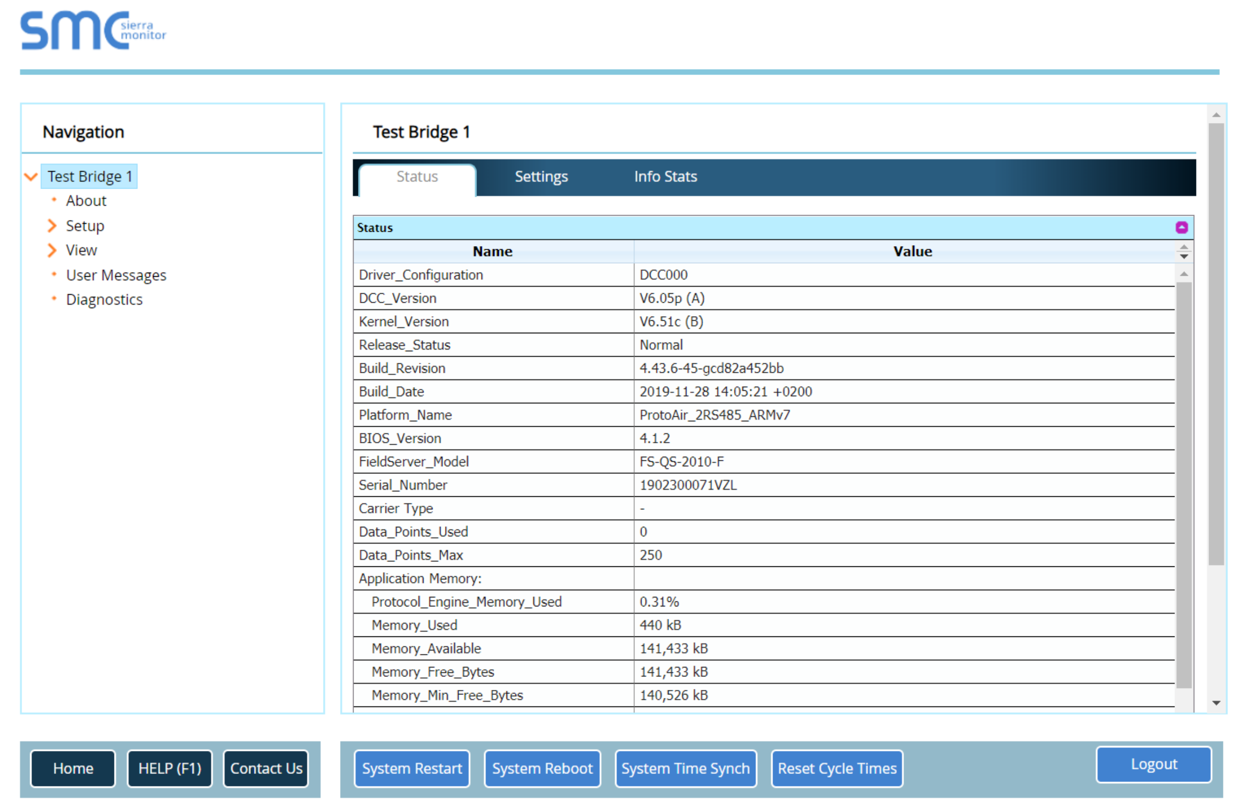
**NOTE: Internet Explorer is no longer supported as recommended by Microsoft.**

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

## Appendix B.6. 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.



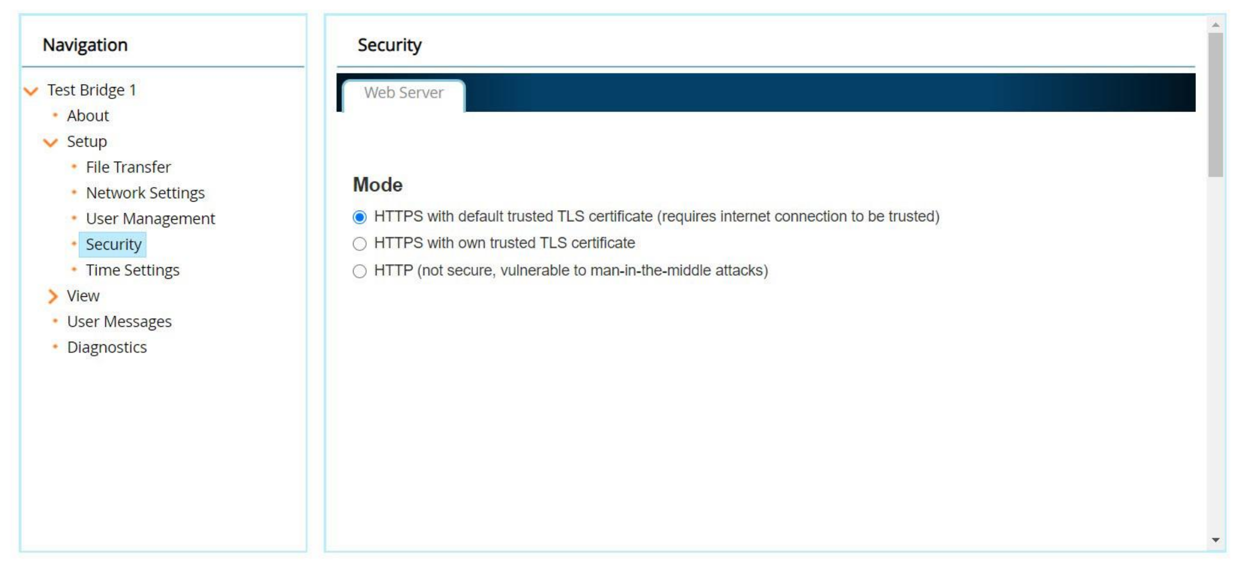
Status

| Name | Value |
|---|---|
| Driver_Configuration | DCC000 |
| DCC_Version | V6.05p (A) |
| Kernel_Version | V6.51c (B) |
| Release_Status | Normal |
| Build_Revision | 4.43.6-45-gcd82a452bb |
| Build_Date | 2019-11-28 14:05:21 +0200 |
| Platform_Name | ProtoAir_2RS485_ARMv7 |
| BIOS_Version | 4.1.2 |
| FieldServer_Model | FS-QS-2010-F |
| Serial_Number | 1902300071VZL |
| Carrier Type | - |
| Data_Points_Used | 0 |
| Data_Points_Max | 250 |
| Application Memory: | |
| Protocol_Engine_Memory_Used | 0.31% |
| Memory_Used | 440 kB |
| Memory_Available | 141,433 kB |
| Memory_Free_Bytes | 141,433 kB |
| Memory_Min_Free_Bytes | 140,526 kB |

Figure 23: FS-GUI Page

## Appendix B.6.1. Change Security Mode

- Click Security in the Navigation panel.



**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)

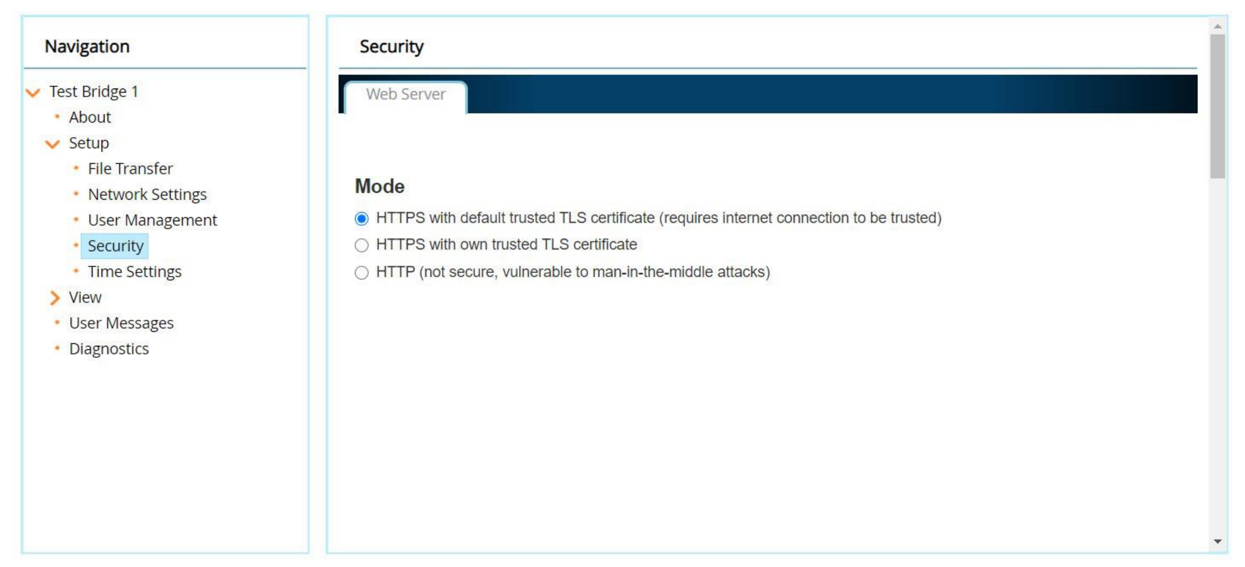
Figure 24: FS-GUI Security Setup

- 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.6.2. 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.



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)

Figure 25: 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.7. 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 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.**

### Appendix B.7.1. User Management

- Check that the Users tab is selected.

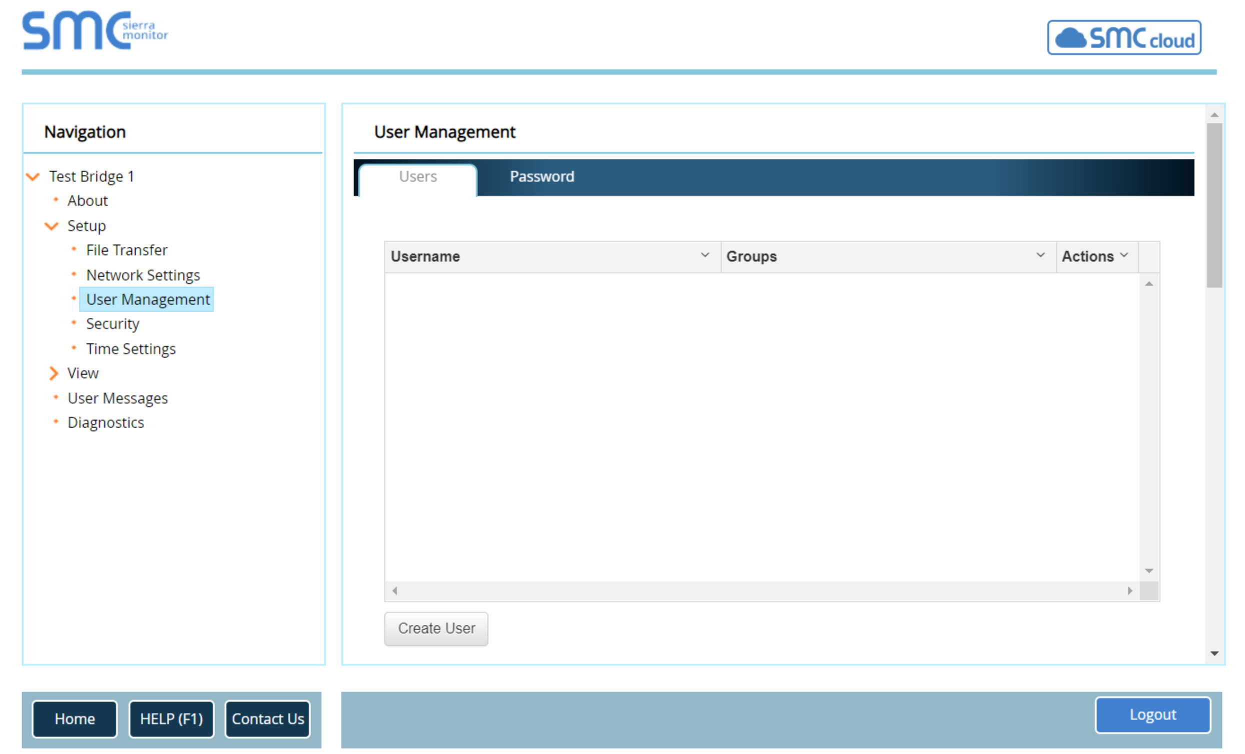


Figure 26: FS-GUI User Management

User Types:

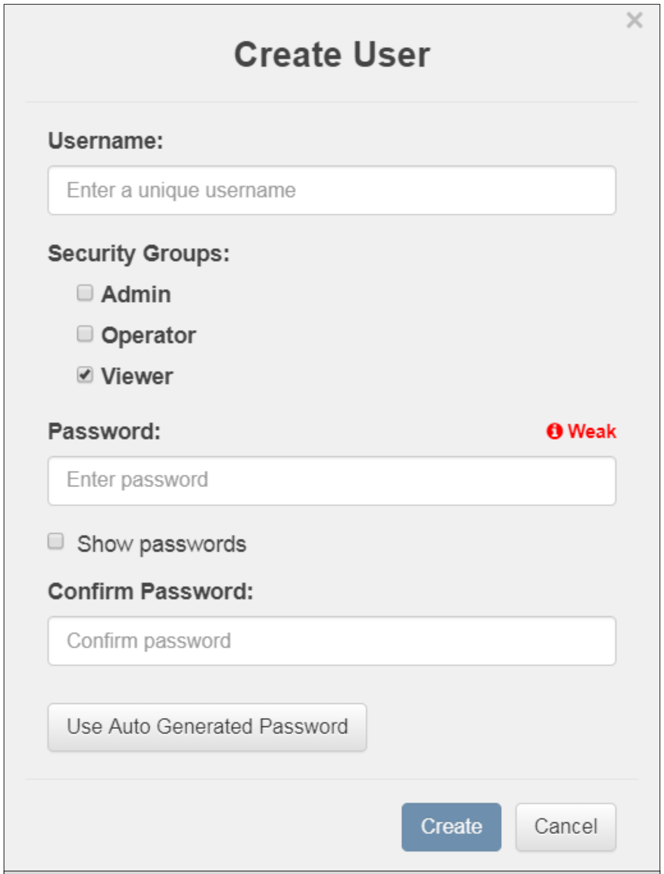
**Admin** – Can modify and view any settings on the FieldServer.

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

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

### Appendix B.7.1.1. Create Users

- Click the Create User button.



Create User

Username:

Enter a unique username

Security Groups:

□ Admin

□ Operator

☑ Viewer

Password: Weak

Enter password

□ Show passwords

Confirm Password:

Confirm password

Figure 27: Create User Window

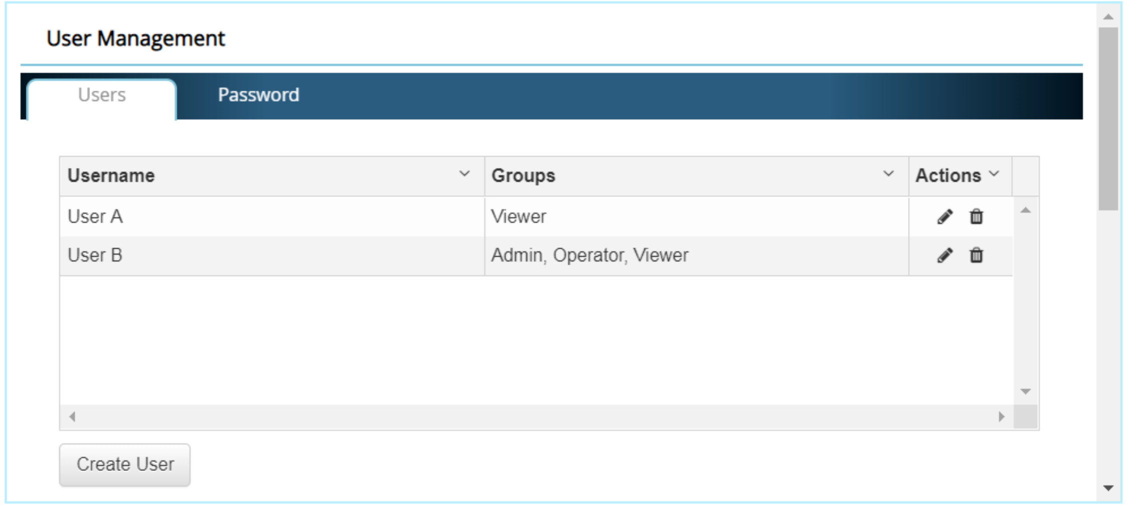
- Enter the new User fields: Name, Security Group and Password.
  - **User details are hashed and salted**

**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.

### Appendix B.7.1.2. Edit Users

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

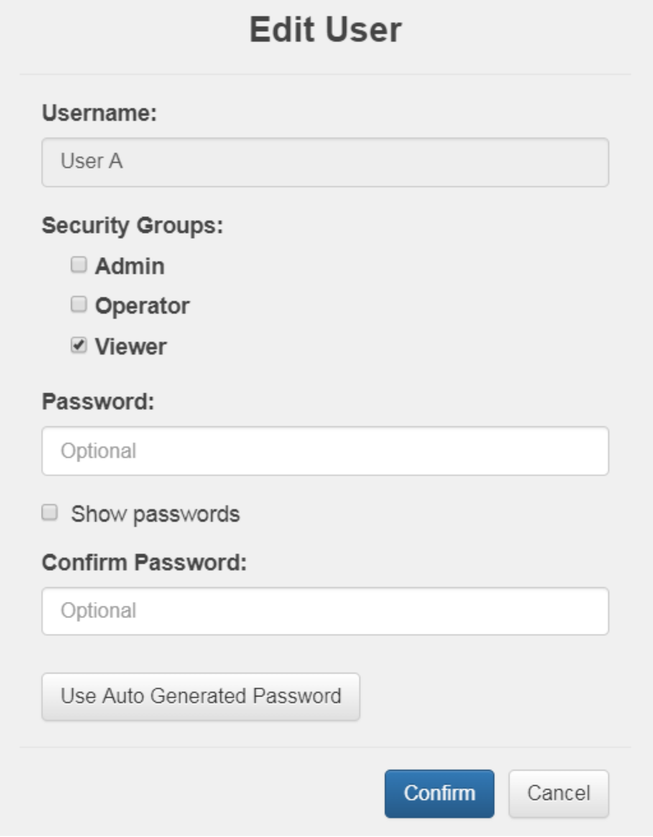


User Management

| Username | Groups | Actions |
|---|---|---|
| User A | Viewer | ✎ 🗑 |
| User B | Admin, Operator, Viewer | ✎ 🗑 |

Figure 28: Setup Users

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



Edit User

Username: User A

Security Groups:

□ Admin
□ Operator
☑ Viewer

Password: Optional

□ Show passwords

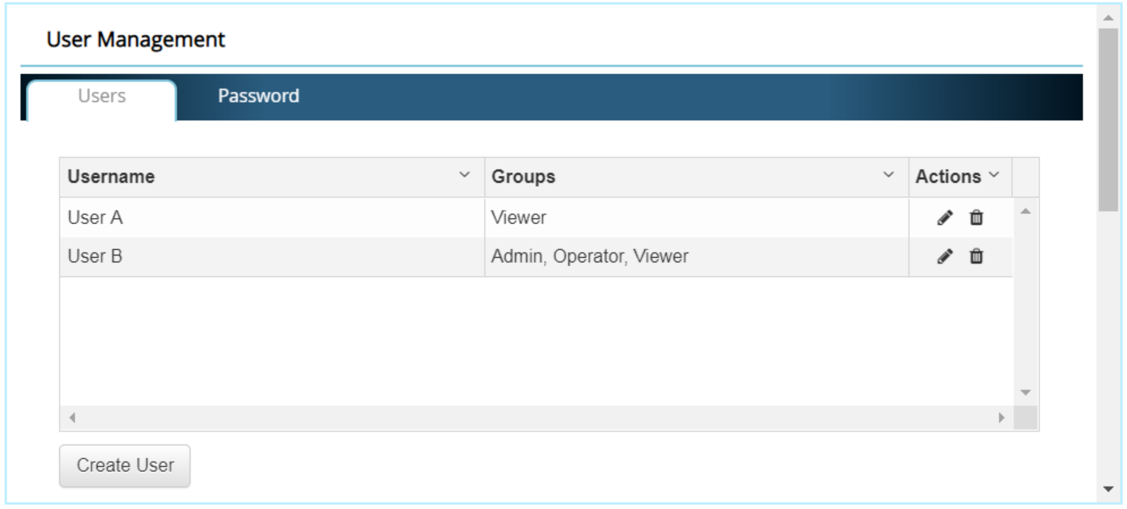
Confirm Password: Optional

Figure 29: Edit User Window

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

### Appendix B.7.1.3. Delete Users

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

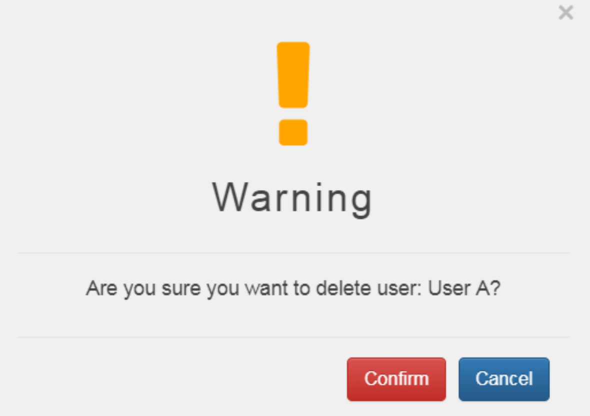


User Management

| Username | Groups | Actions |
|---|---|---|
| User A | Viewer | |
| User B | Admin, Operator, Viewer | |

Figure 30: Setup Users

- When the warning message appears, click Confirm.



Warning

Are you sure you want to delete user: User A?

Figure 31: User Delete Warning

## Appendix B.7.2. Change FieldServer Password

- Click the Password tab.

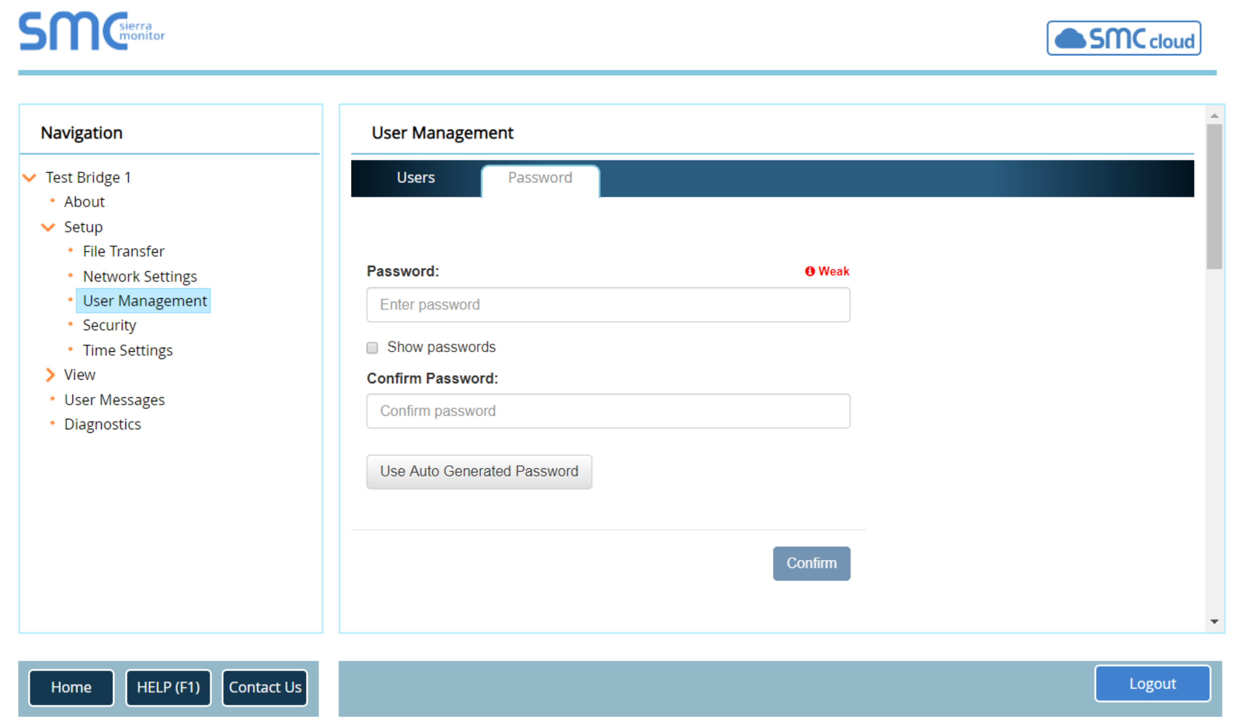


Figure 32: FieldServer Password Update via FS-GUI

- Change the 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.**

**NOTE: If a gateway in the field is updated to a secure gateway, the password will change to "admin". This change will still occur if the gateway was already setup with a unique password that was loaded in the factory and printed on the label.**

# 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 | | | 1 | |
| | FS-QS-1241 | | | | 1 | | | 1 | 1 |
| | FS-QS-1A50 | | | | | 1 | 1 | 1 | |
| | FS-QS-1A51 | | | | | | 1 | 1 | 1 |
| | FS-QS-1B50 | | | | | 1 | 1 | 1 | |
| | FS-QS-1B51 | | | | | | 1 | 1 | 1 |
| | FS-QS-1C50 | | | | | 1 | 1 | 1 | |
| | FS-QS-1C51 | | | | | | 1 | 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

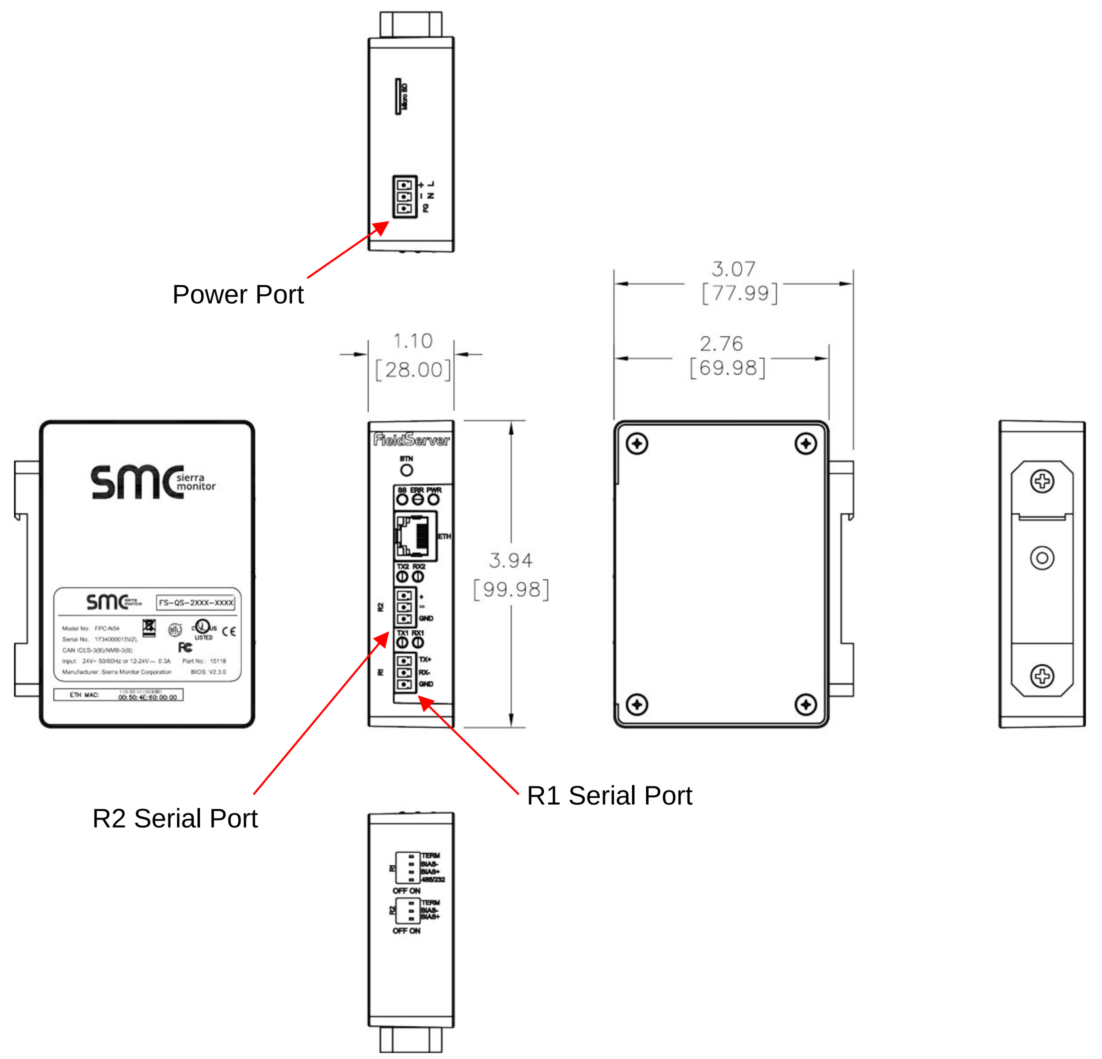


Figure 33: QuickServer Dimension Drawing

## Appendix C.5. Specifications

| | FS-QS-2XX0-XXXX [2] |
|---|---|
| **Electrical Connections** | One 3-pin Phoenix connector with: RS-485/RS-232 (Tx+ / Rx- / gnd)<br>One 3-pin Phoenix connector with: RS-485 (Tx+ / Rx- / gnd)<br>One 3-pin Phoenix connector with: Power port (+ / - / Frame-gnd)<br>One Ethernet 10/100 BaseT port |
| **Power Requirements** | *Input Voltage:* 9-30VDC or 24VAC *Current draw:* 24VAC 0.125A<br>*Max Power:* 3 Watts 9-30VDC 0.25A @12VDC |
| **Approvals** | CE and FCC Class B & C Part 15, UL 60950-1, WEEE compliant,<br>IC Canada, RoHS3 compliant |
| **Capacity Options** | FS-QS-20X0: 250 data points FS-QS-22X0: 3,000 data points<br>FS-QS-23X0: 500 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 to158°F) |
| **Humidity** | 10-95% RH non-condensing |

**Figure 34: 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.