Start-up Guide

QuickServer FS-QS-3X10-F

APPLICABILITY & EFFECTIVITY
Effective for all systems manufactured after April 2021.

Document Revision: 1.A

T18627

MSA Safety
1991 Tarob Court
Milpitas, CA 95035
Website: www.MSAsafety.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 About the QuickServer

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 Section 8, or any of the troubleshooting appendices in the related driver supplements. Check the MSA Safety 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.

1.1 Certification

BTL Mark – BACnet Testing Laboratory[1]

The BTL Mark on QuickServer 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.

1.2 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 MSA 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.

2 Equipment Setup

2.1 Mounting

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

Figure 1: DIN Rail Bracket

2.2 Physical Dimensions

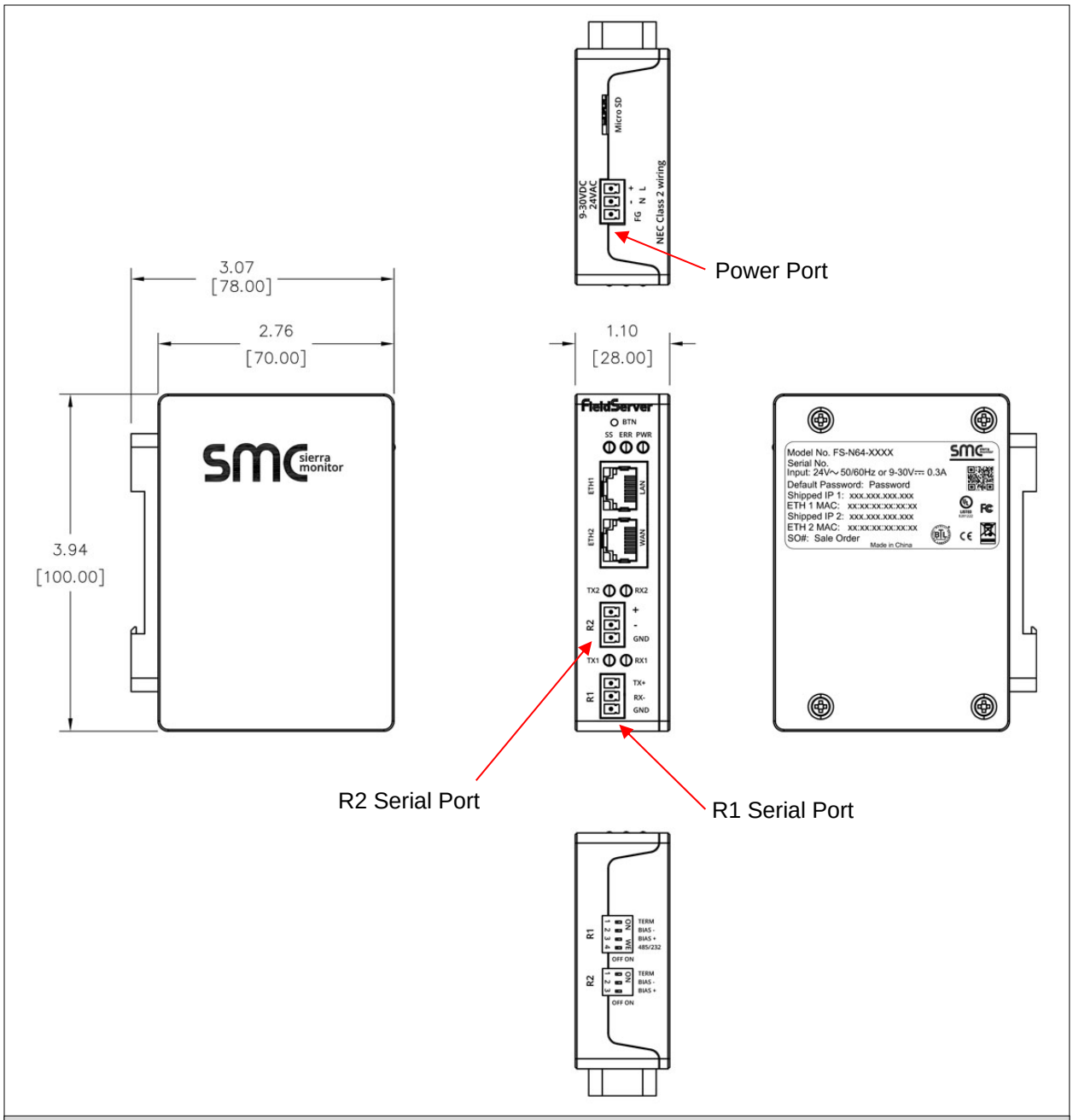


Figure 2: QuickServer 3X10-F Dimensions

3 Installing the QuickServer

3.1 DIP Switch Settings

3.1.1 Bias Resistors

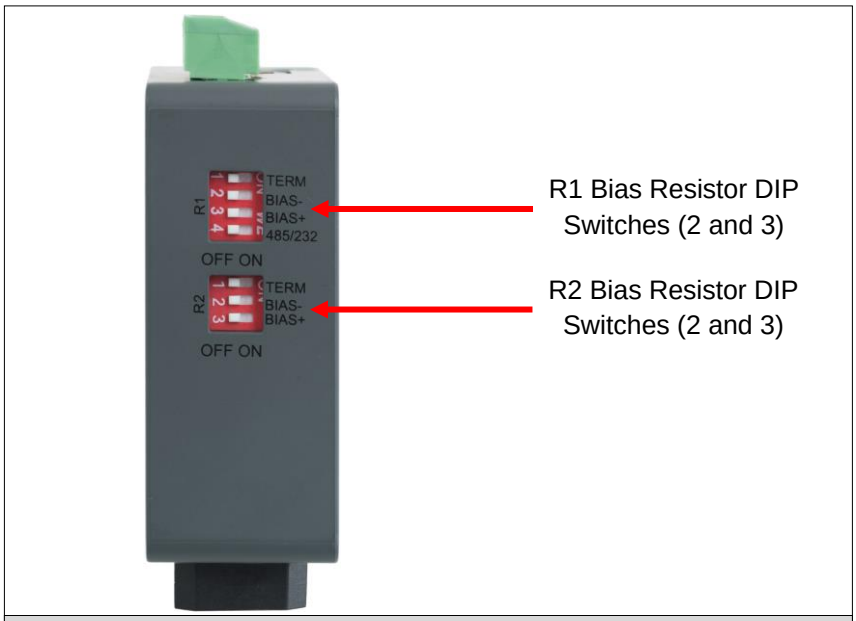


Figure 3: Bias Resistor DIP Switches

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.

3.1.2 Termination Resistor

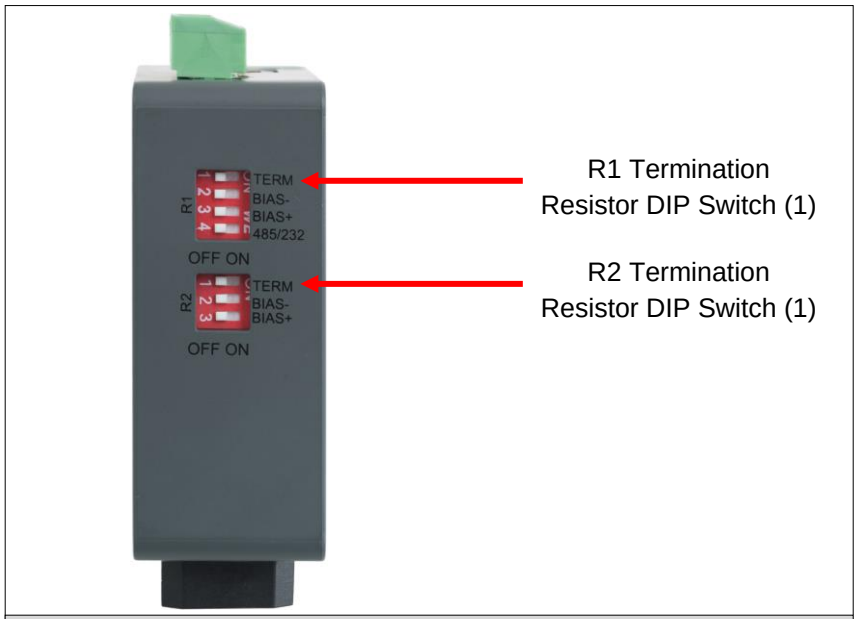


Figure 4: Termination Resistor DIP Switch

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.

3.2 Connecting the R1 & R2 Ports

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 5**).

The R2 Port is RS-485.

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

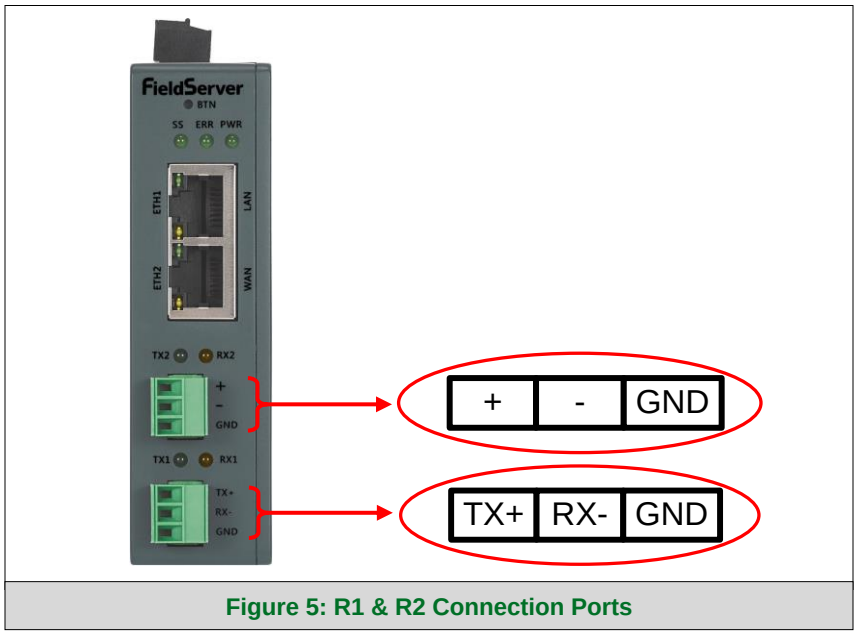


Figure 5: R1 & R2 Connection Ports

3.2.1 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.

3.2.2 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

3.3 10/100 Ethernet Connection Port

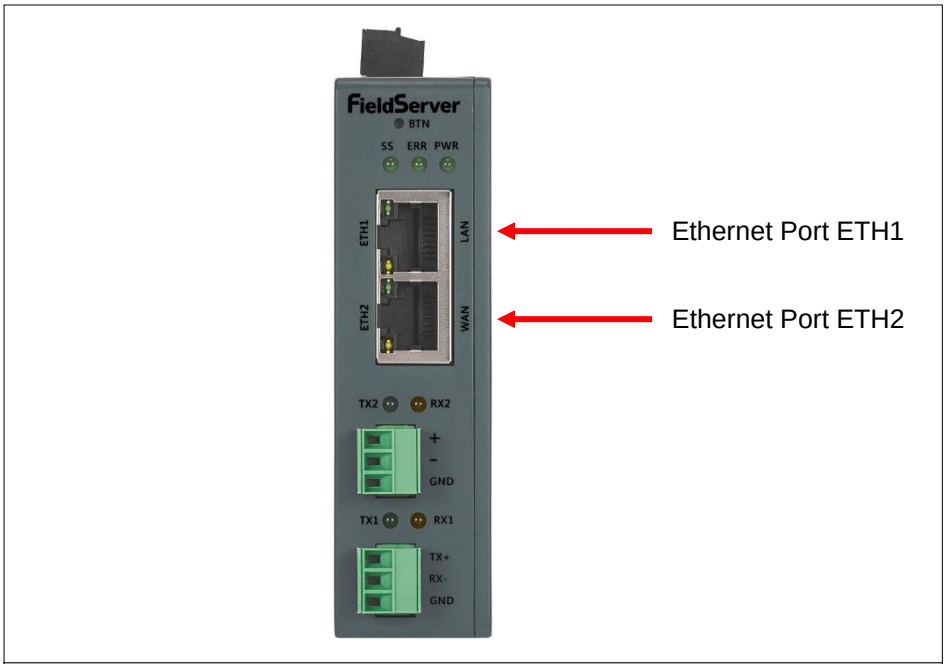


Figure 6: Ethernet Connection

The Ethernet Ports are used both for BACnet/IP communications and for configuring the QuickServer via the Web App. To connect the QuickServer, either connect the PC to the Router's Ethernet port or connect the Router and PC to an Ethernet switch. Use Cat-5 cables for the connection.

NOTE: The Default IP Address of the QuickServer is 192.168.2.101, Subnet Mask is 255.255.255.0.

NOTE: The ETH2 port can be set to WAN mode to limit ethernet traffic. See Section 7.1.4 for details.

4 Power up the QuickServer

Check power requirements in the table below:

Power Requirement for QuickServer External Gateway		
	Current Draw Type	
QuickServer Family	**12VDC**	**24VDC/AC**
FS-QS-3X10-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 7: Required Current Draw for the Gateway

Apply power to the QuickServer as shown below in **Figure 8.** Ensure that the power supply used complies with the specifications provided in **Section 9.4.**

- The gateway 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

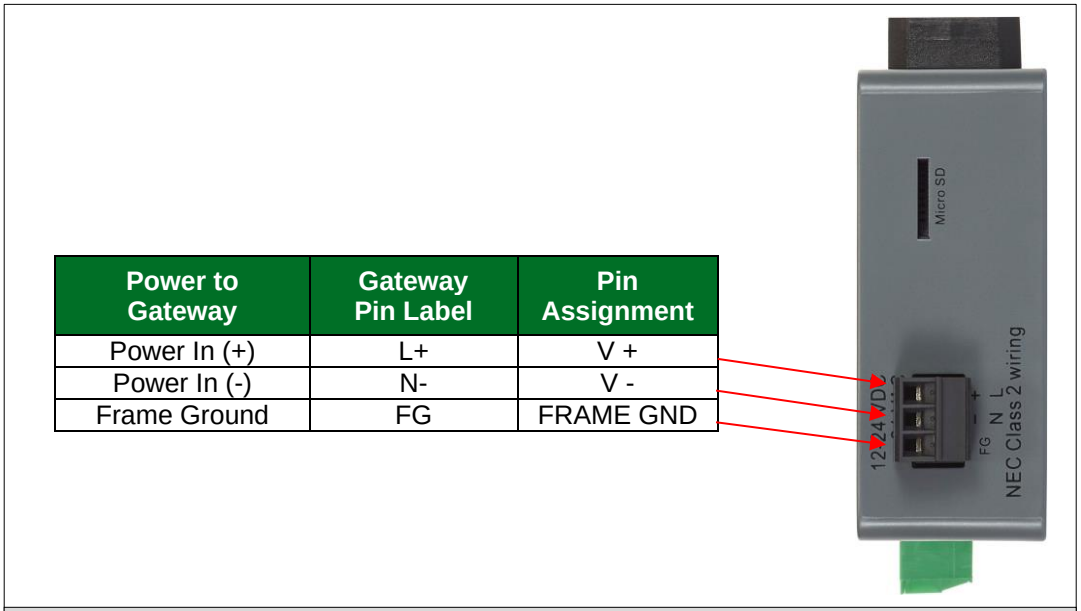


Figure 8: Power Connections

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 ETH1 (LAN Port).

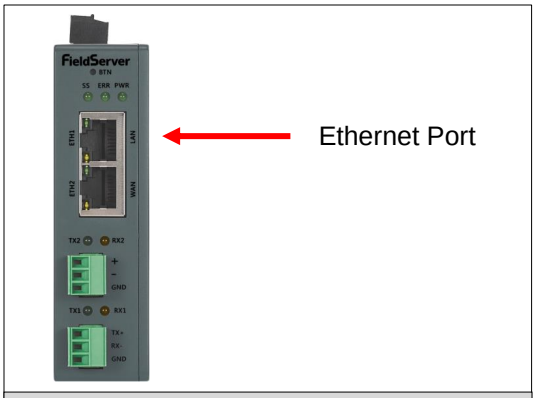


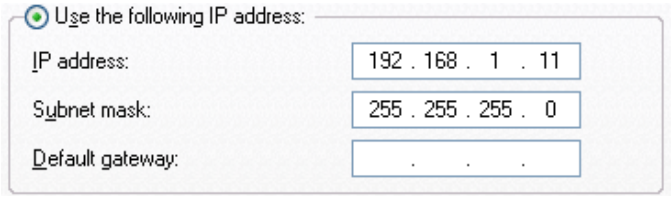
Figure 9: Ethernet Port Location

5.1.1 Changing the Subnet of the Connected PC

The default IP Address for the QuickServer is **192.168.1.24**, 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 192.168.2.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:



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

6 Setup Web Server Security

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

NOTE: If the IP Address of the QuickServer has been changed, the IP Address can be discovered using the FS Toolbox utility. See Section 8.1 for instructions.

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.

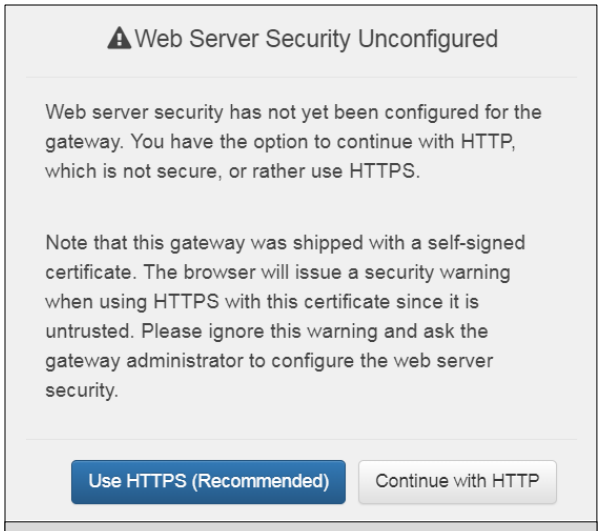


Figure 10: Web Server Security Window

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

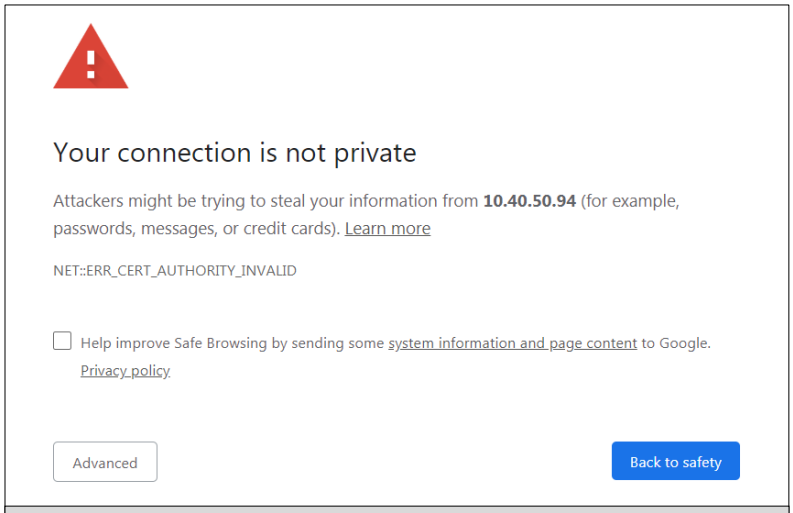


Figure 11: Connection Not Private Warning

- Additional text will expand below the warning, click the underlined text to go to the IP Address. In the **Figure 12** example this text is "Proceed to 10.40.50.94 (unsafe)".

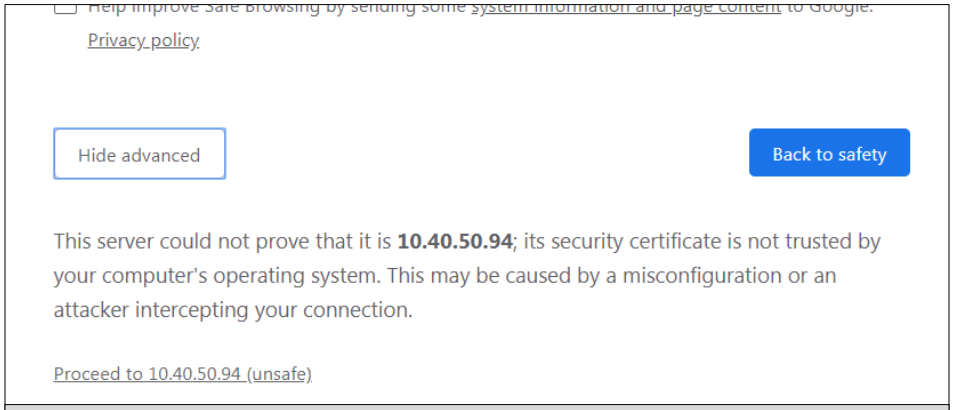


Figure 12: Warning Expanded Text

- 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.

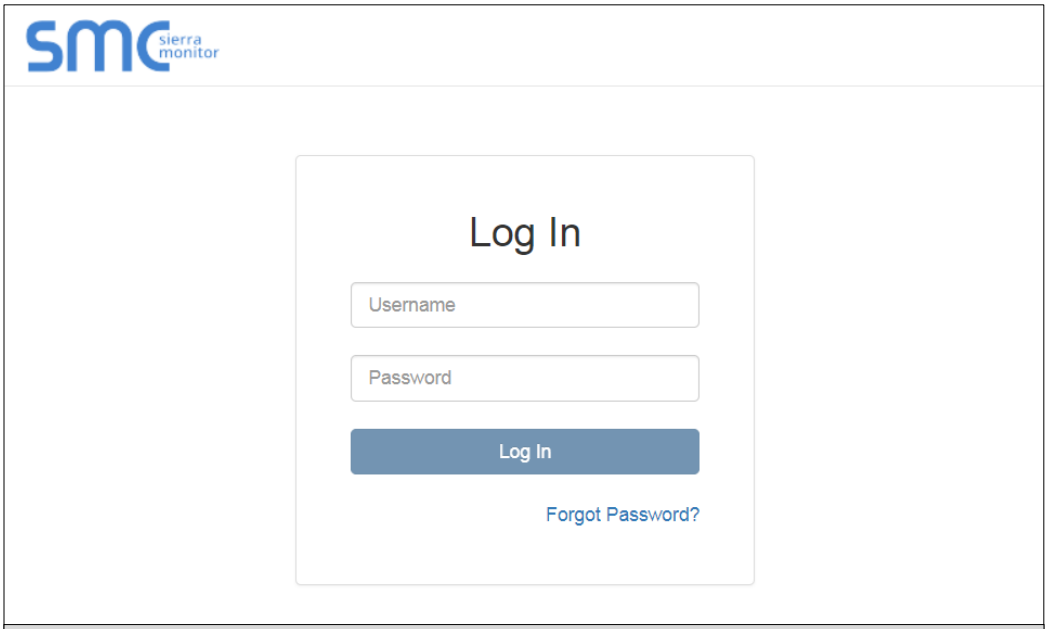


Figure 13: FieldServer Login

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 9.3.

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.

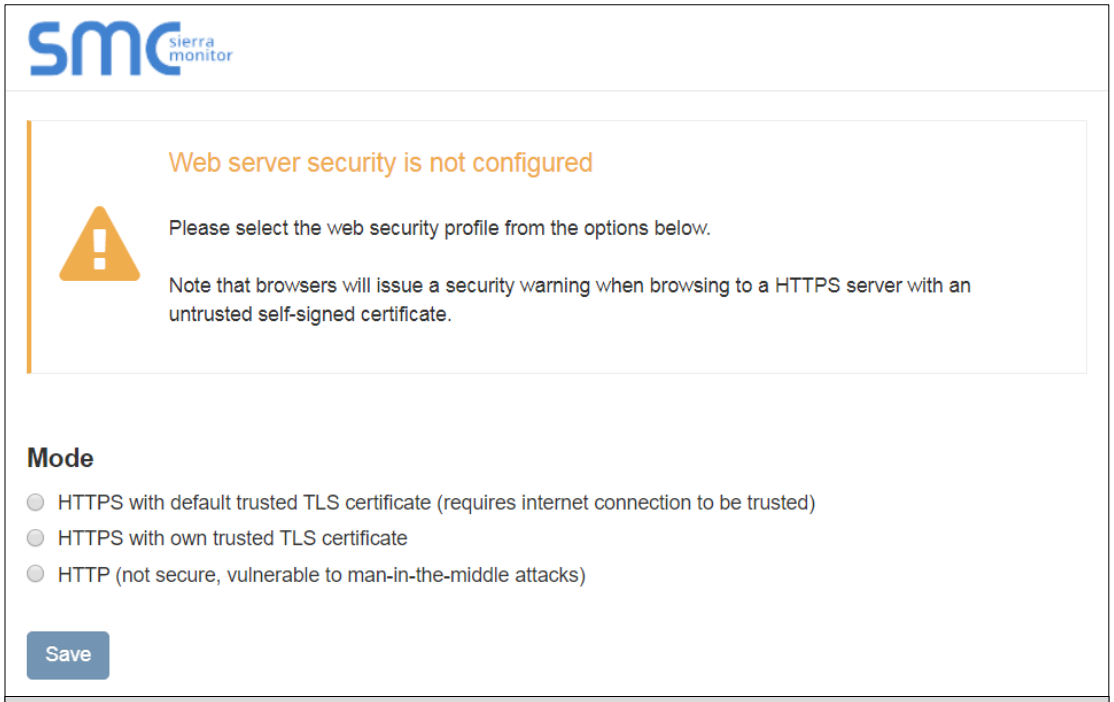


Figure 14: Security Mode Selection Screen

NOTE: Cookies are used for authentication.

NOTE: To change the web server security mode after initial setup, go to Section 9.2.

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

6.2.1 HTTPS with Own Trusted TLS Certificate

This is the recommended selection and the most secure. **Please contact your IT department to find out if you can obtain a TLS certificate from your company before proceeding with the Own Trusted TLS Certificate option.**

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

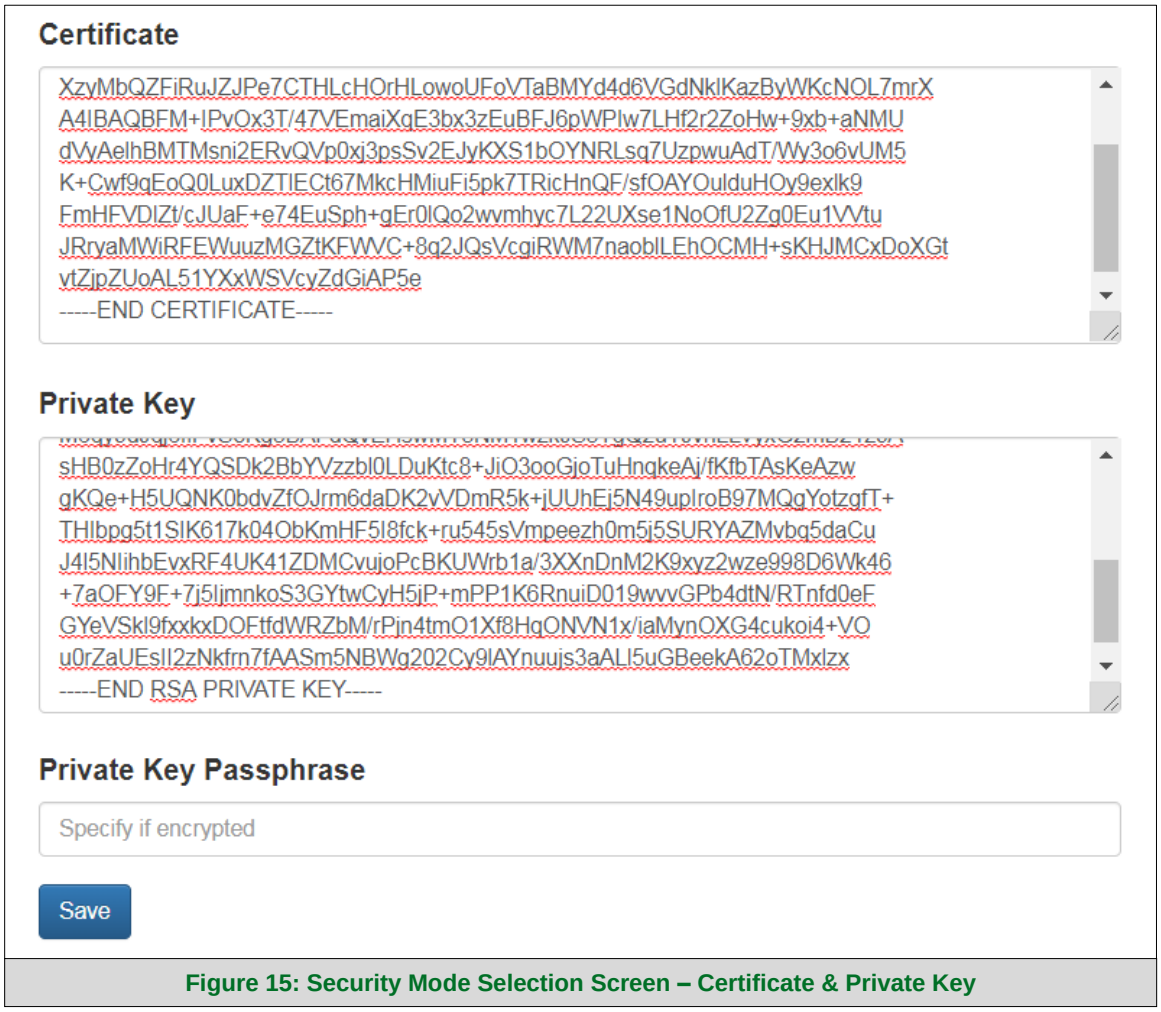


Figure 15: Security Mode Selection Screen – Certificate & Private Key

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

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

- Select one of these options and click the Save button.
- A “Redirecting” message will appear. After a short time, the FieldServer GUI will open.

7 Configuring the QuickServer

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

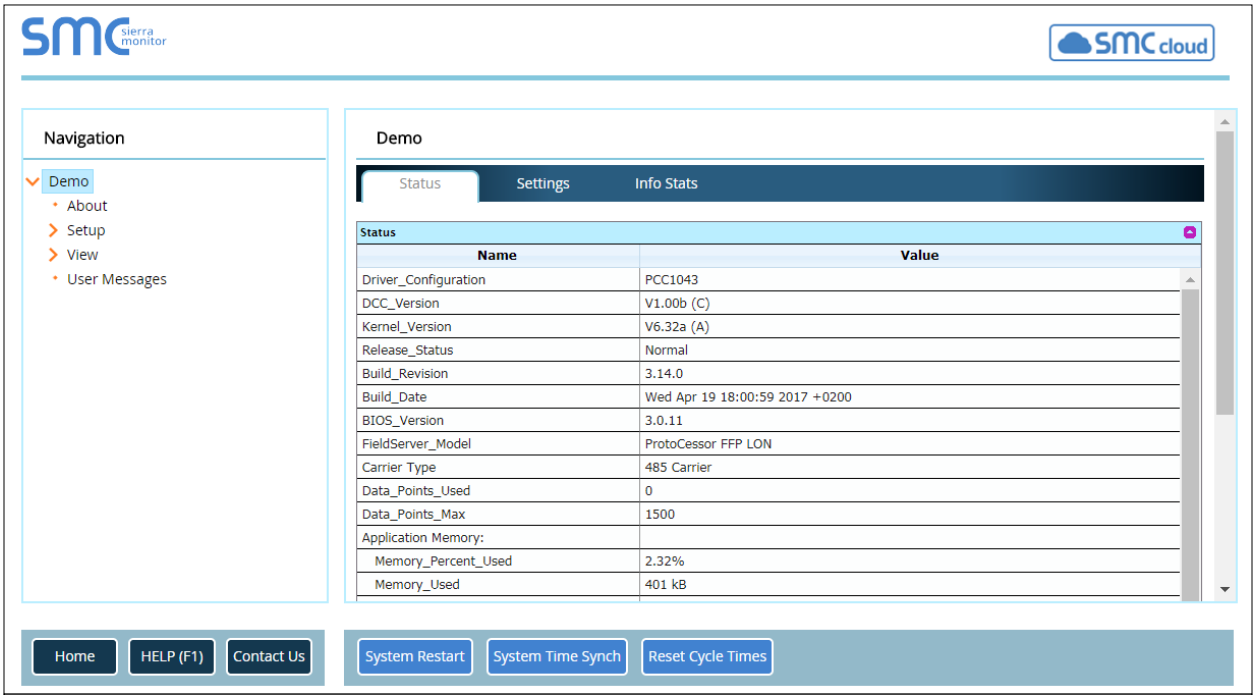


Figure 16: FS-GUI Landing Page

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.

7.1 Configure Network Settings

7.1.1 Using FS-GUI to Input Network Settings

To navigate from the FS-GUI page to the Network Settings page follow the below instructions:

- Find the Navigation tree across the left side of the screen.
- Click the orange arrow next to the QuickServer CN number and title to expand the tree.

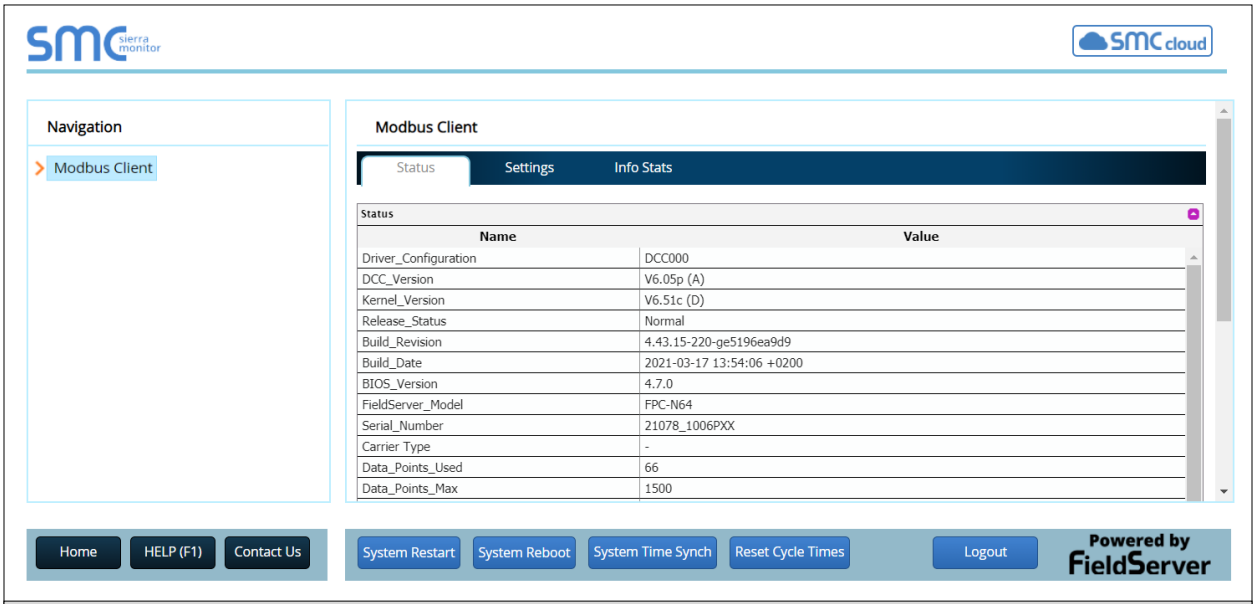


Figure 17: FS-GUI Page

- Click on the orange arrow next to Setup to expand the tree.
- Click on Network Settings.

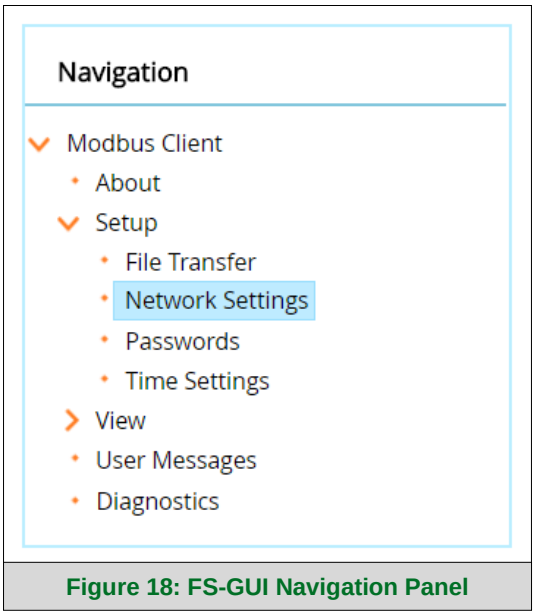


Figure 18: FS-GUI Navigation Panel

7.1.2 Routing Settings

The Routing settings make it possible to set up the IP routing rules for the FieldServer's internet and network connections.

NOTE: The default connection is ETH1.

- Select the default connection in the first row as either ETH 1 or ETH 2.
- Click the Add Rule button to add a new row and set a new Destination Network, Netmask and Gateway IP Address as needed.
- Set the Priority for each connection (1-255 with 1 as the highest priority and 255 as the lowest).
- Click the Save button to activate the new settings.

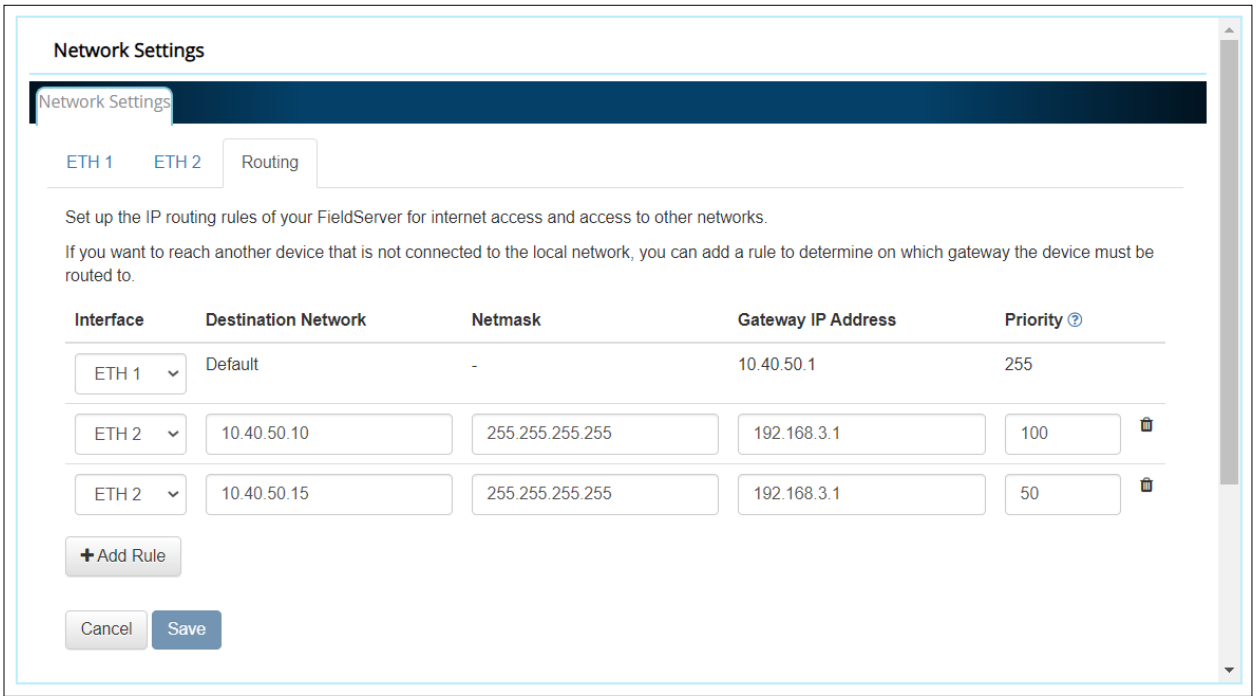


Figure 19: Routing Settings

7.1.3 Ethernet 1 and Ethernet 2 Network Settings

- Enable DHCP to automatically assign IP Settings or modify the IP Settings manually as needed, via these fields: IP Address, Netmask, Gateway, and Domain Name Server1/2.

NOTE: If connected to a router, set the Gateway to the same IP Address as the router.

- Click Save to record and activate the new IP Address.
- Connect the FieldServer to the local network or router.

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

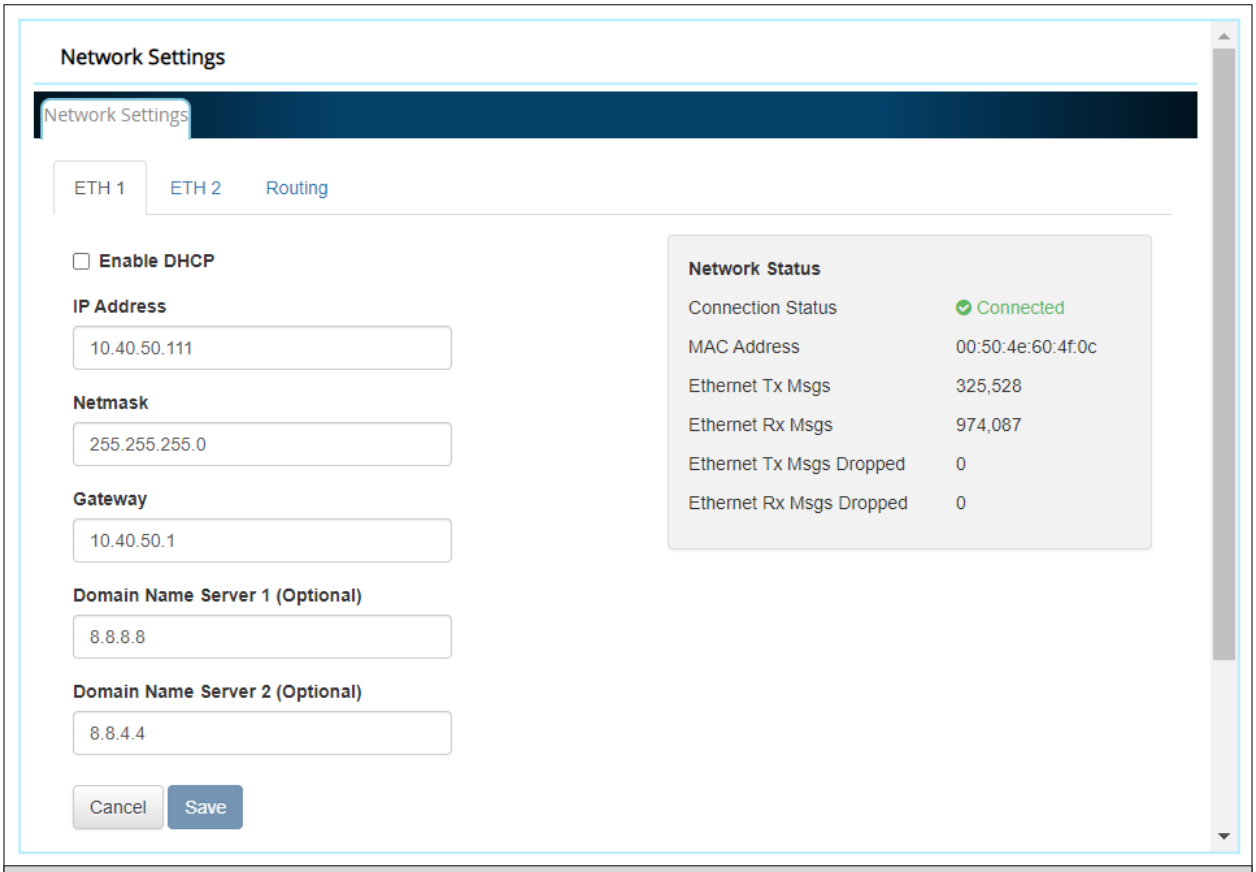
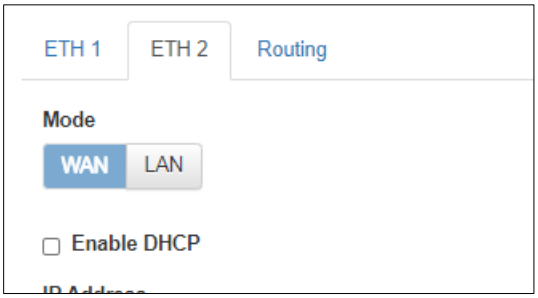


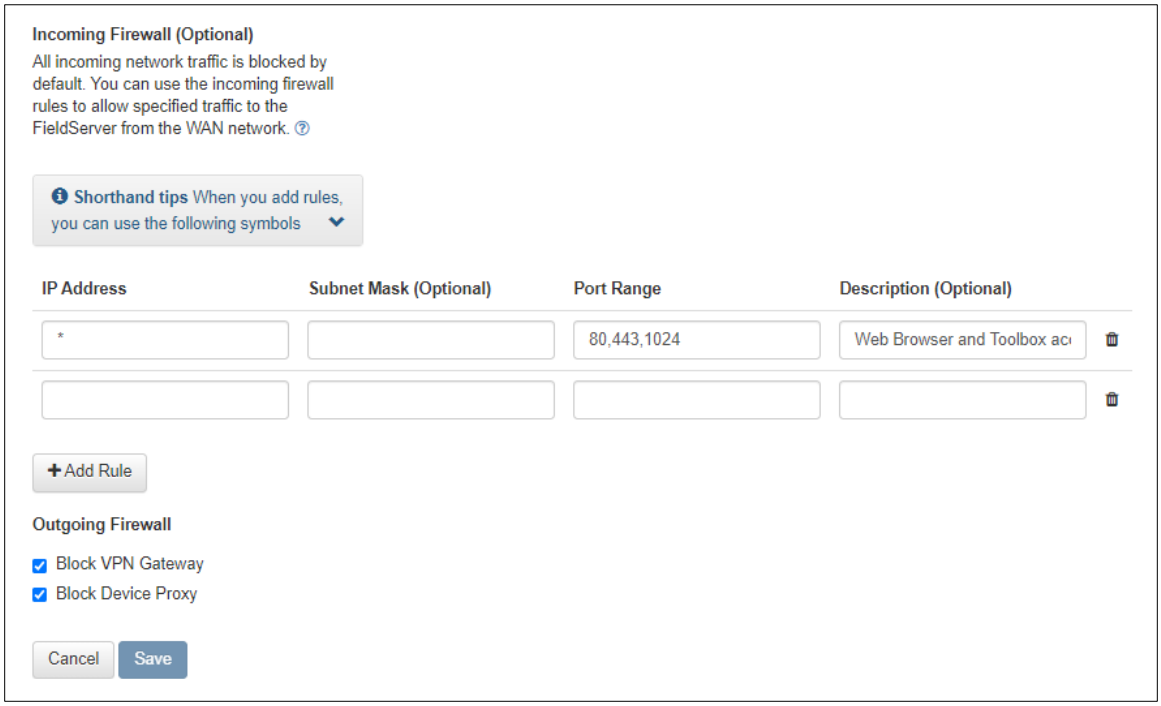
Figure 20: Ethernet Port Network Settings

7.1.4 WAN Mode Settings for ETH2

- Click the blue WAN box to change the ETH 2 port to WAN mode.
  - This prevents all but allowed incoming traffic on the ETH 2 port it does allow a connection to the internet via port 80 & 443



- Scroll below the network settings to get to the firewall options with rules that allow specific incoming traffic (through setting rules) and outgoing options.



NOTE the following options for setting firewall rules:

- Add 1023 to the Port Range field to allow the FieldServer Toolbox access.
- Add 47808 to the Port Range field for BACnet access.
- Add 80 & 443 to the Port Range field for web browser access.
- Use a "*" as a wild card for IP Address.

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.

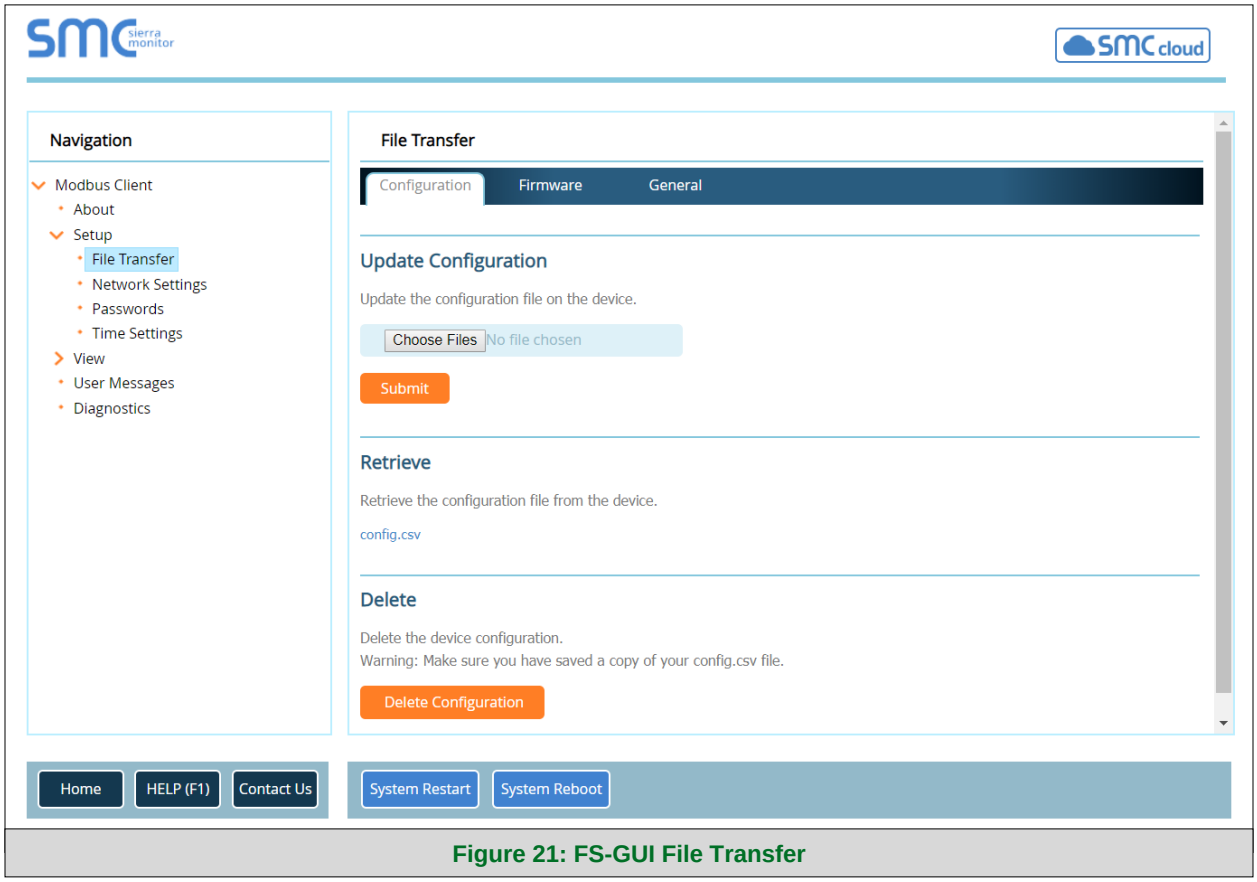


Figure 21: FS-GUI File Transfer

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”.

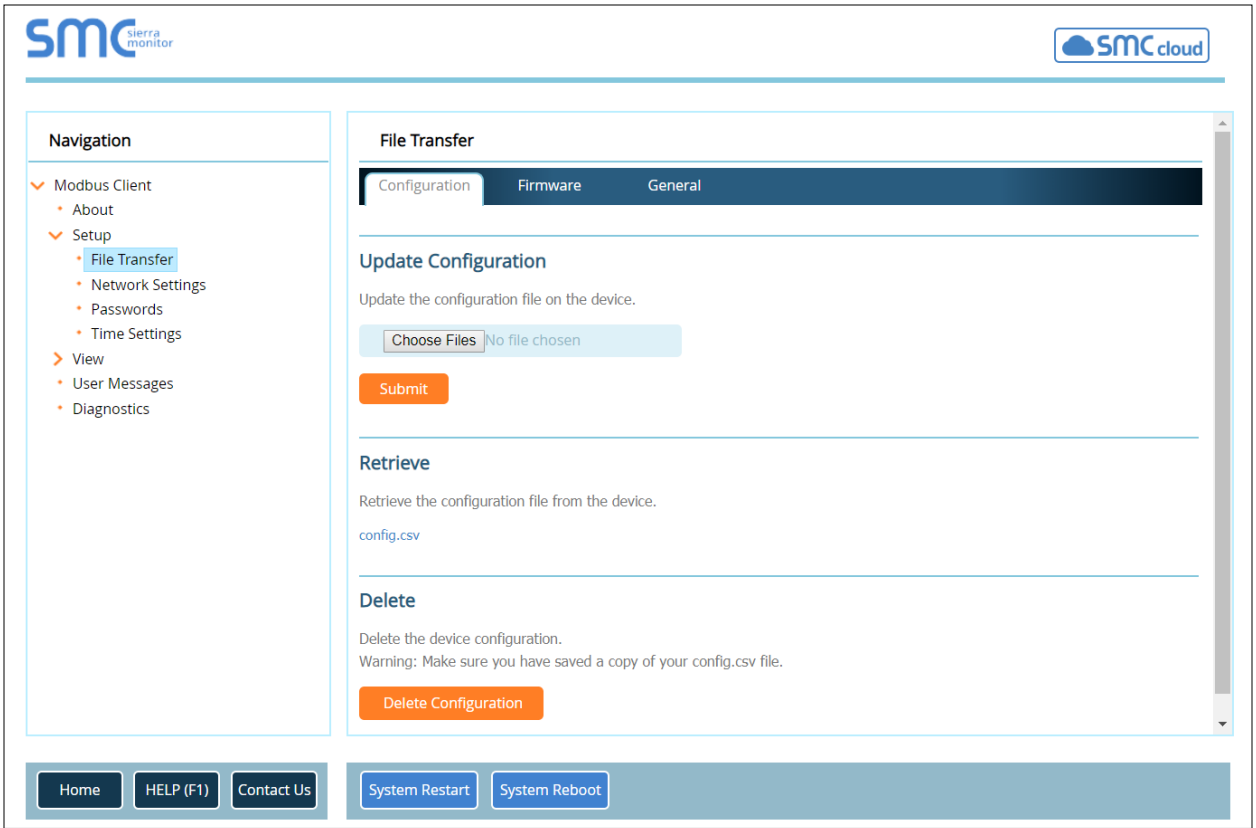


Figure 22: FS-GUI Loading Files

- 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”.

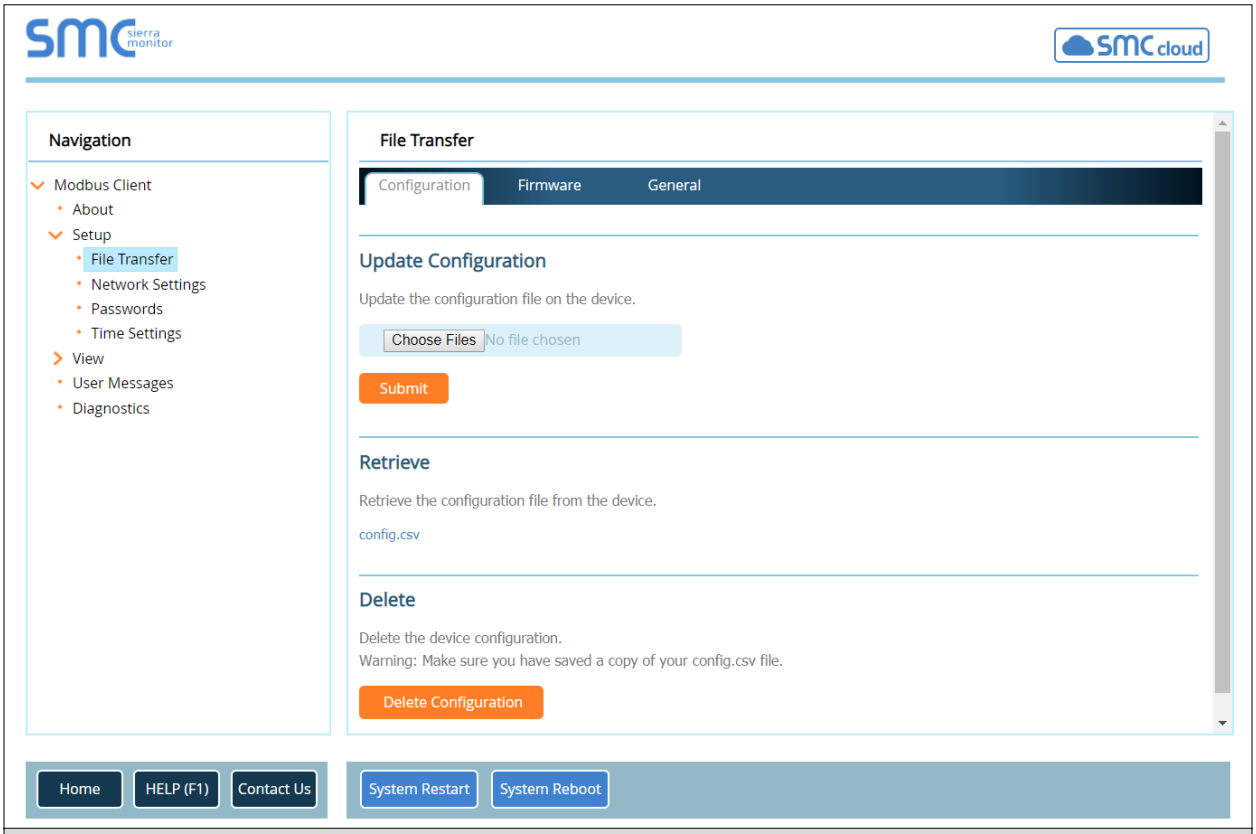


Figure 23: Retrieve Configuration File

- 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.

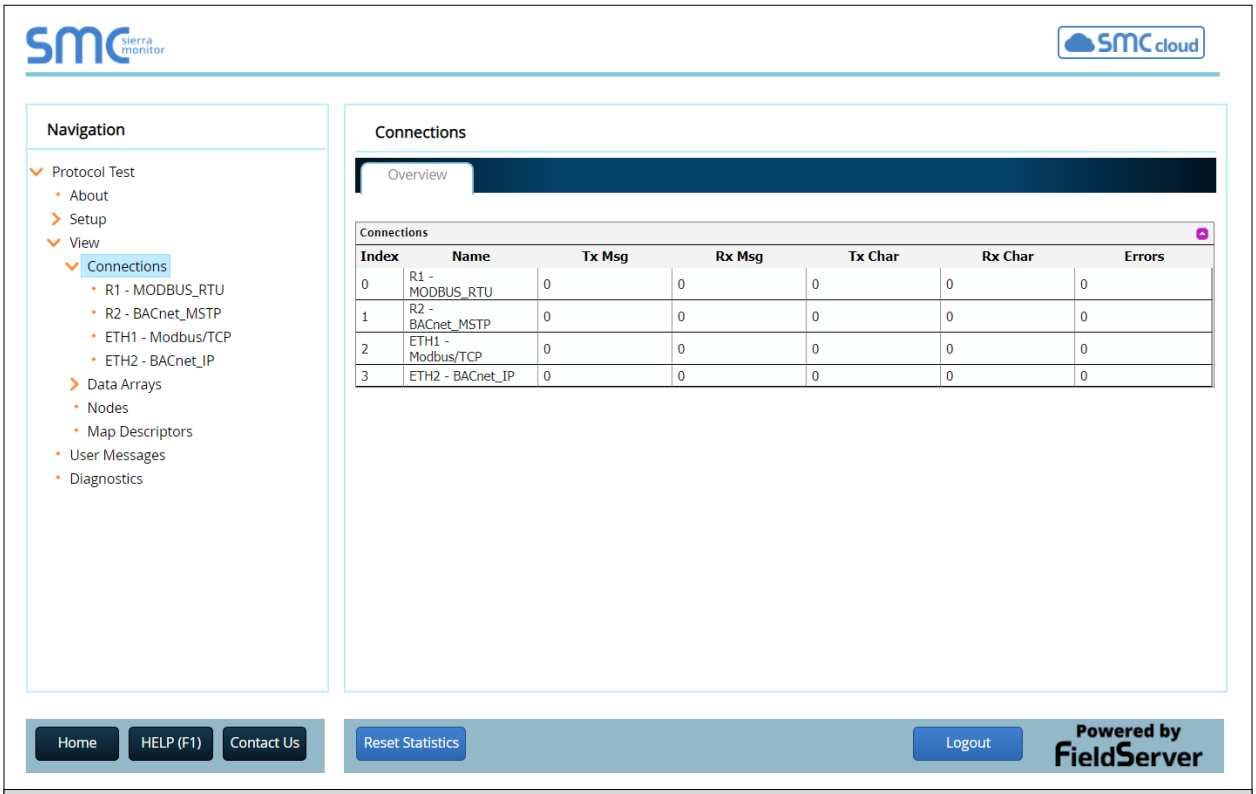


Figure 24: FS-GUI Connections Screen

NOTE: For troubleshooting assistance refer to Section 8, or any of the troubleshooting appendices in the related driver supplements and configuration manual. MSA Safety also offers a technical support on the MSA Safety website, which contains a significant number of resources and documentation that may be of assistance.

7.5.1 Accessing SMC Cloud

NOTE: The SMC Cloud button SMC cloud (see Figure 24) 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.

8 Troubleshooting

8.1 Lost or Incorrect IP Address

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

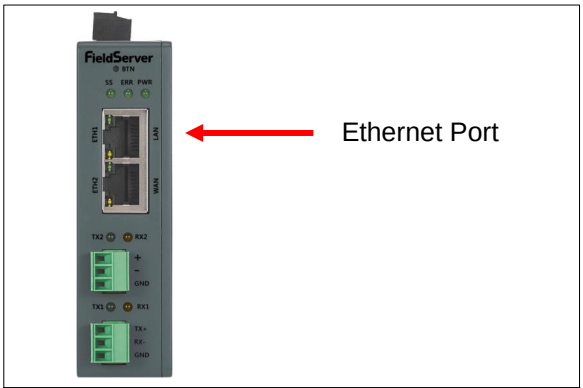
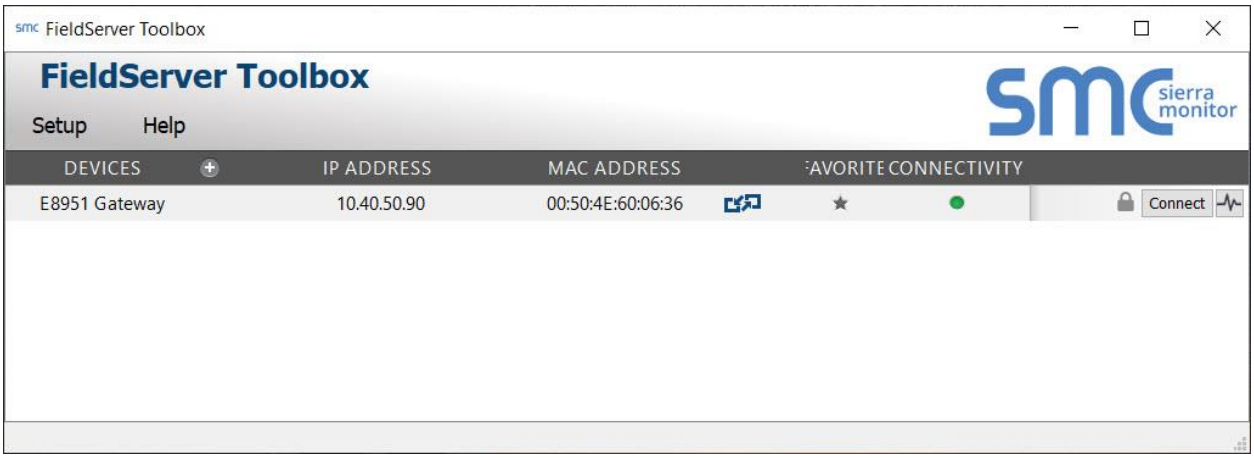


Figure 25: Ethernet Port Location

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



8.2 Viewing Diagnostic Information

- Type the IP Address of the QuickServer into the web browser or use the FieldServer Toolbox to connect to the QuickServer.
- Click on Diagnostics and Debugging Button, then click on view, and then on connections.
- If there are any errors showing on the Connection page, refer to **Section 8.3** for the relevant wiring and settings.

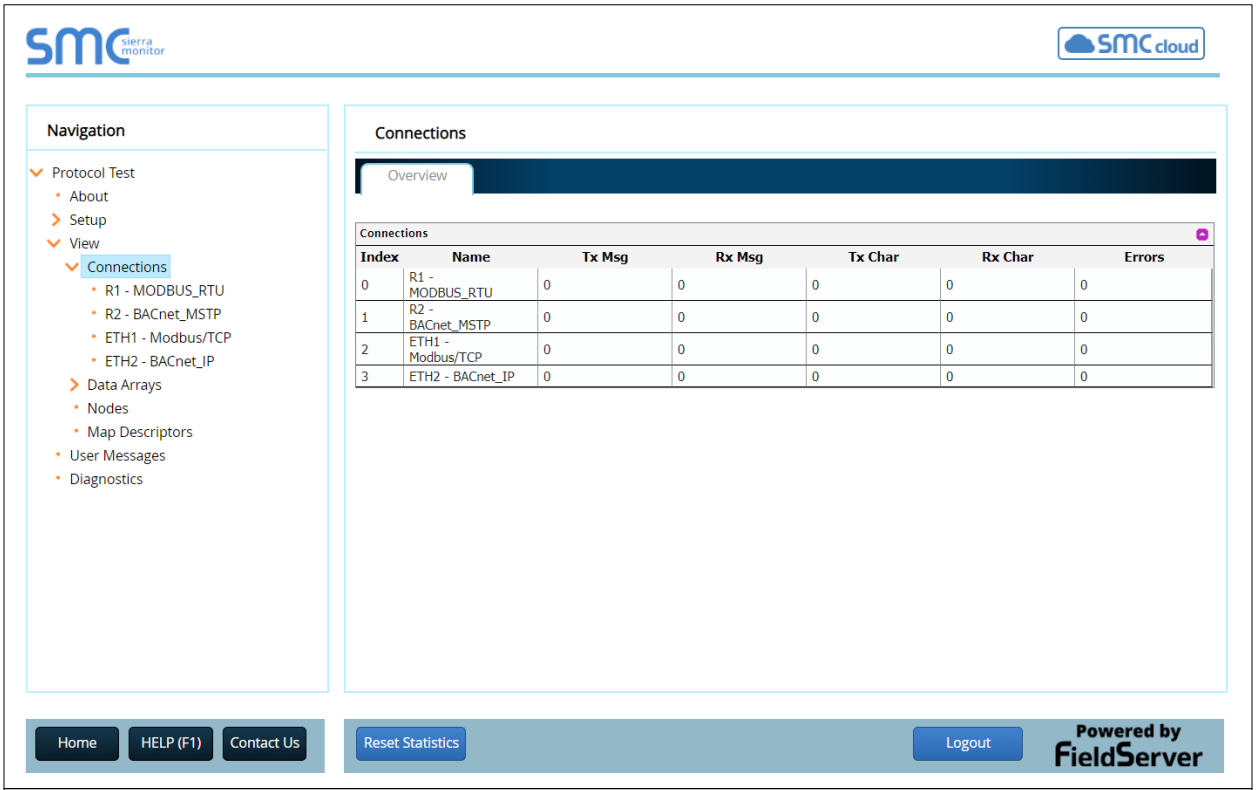


Figure 26: Error Messages Screen

8.3 Checking Wiring and Settings

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

- Visual observations of LEDs on the QuickServer. (**Section 8.5**)
- Check baud rate, parity, data bits, stop bits.
- Check Serial device address.
- Verify wiring.
- Verify device is connected to the same subnet as the QuickServer.

No COMS on the Ethernet protocol. To fix this, check the following:

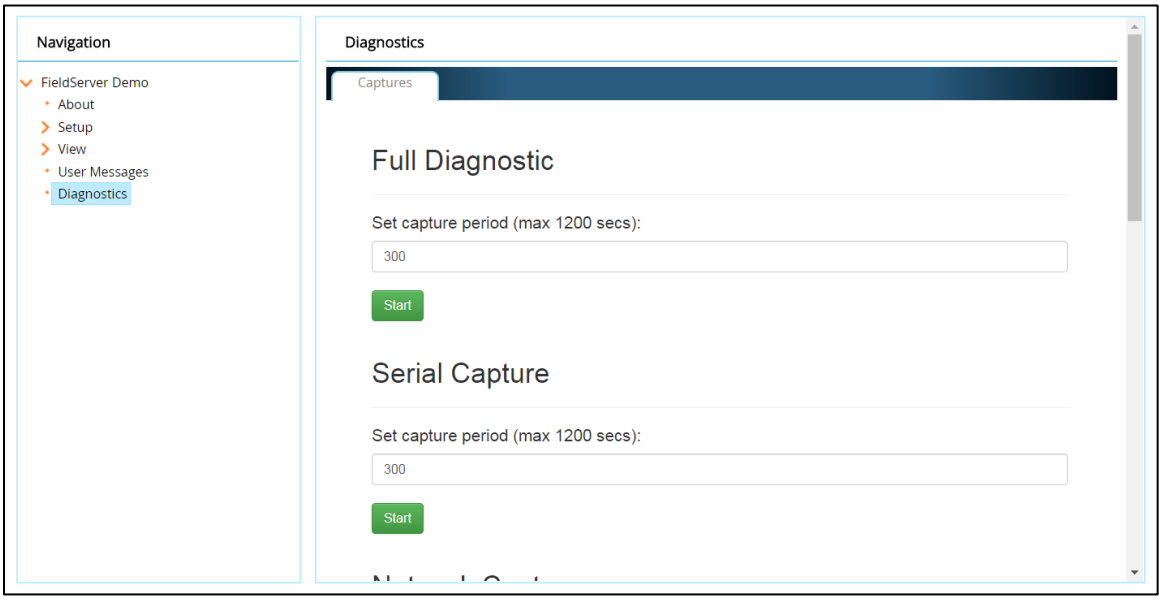
- Visual observations of LEDs on the QuickServer. (**Section 8.5**)
- Check device address.
- Verify wiring.
- Verify device is connected to the same subnet as the QuickServer.
- Verify IP Address setting.

NOTE: If the problem still exists, a Diagnostic Capture needs to be taken and sent to support. (Section 8.4)

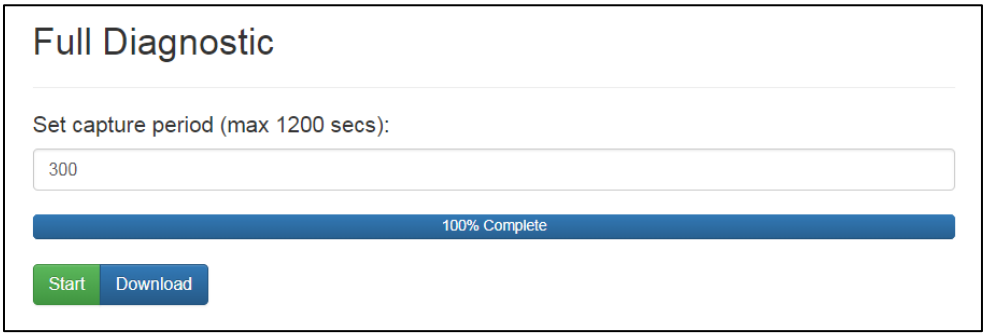
8.4 Taking a FieldServer Diagnostic Capture

When there is a problem on-site that cannot easily be resolved, perform a Diagnostic Capture before contacting support. Once the Diagnostic Capture is complete, email it to technical support. The Diagnostic Capture will accelerate diagnosis of the problem. If the FieldServer bios is updated/released on November 2017 or later then the Diagnostic Capture is performed via the gateway's on-board system.

- Access the FieldServer Diagnostics page via one of the following methods:
  - Open the FieldServer FS-GUI page and click on Diagnostics in the Navigation panel
  - Open the FieldServer Toolbox software and click the diagnose icon of the desired device



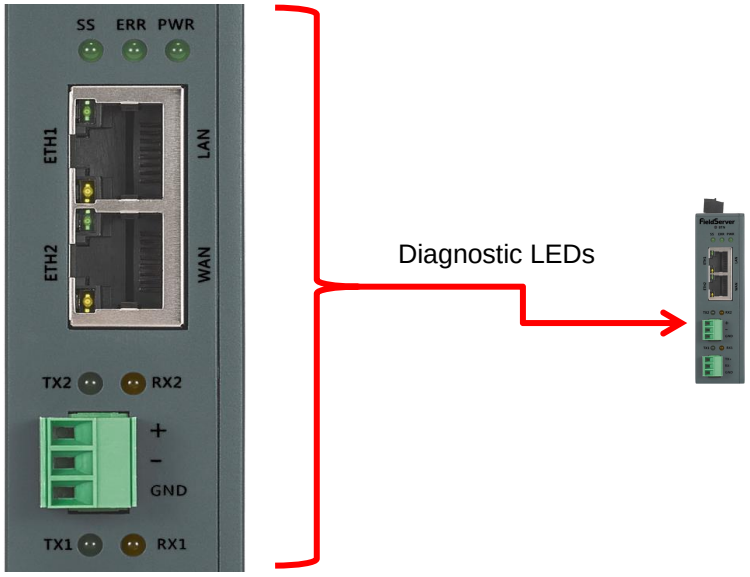
- Go to Full Diagnostic and select the capture period.
- Click the Start button under the Full Diagnostic heading to start the capture.
  - When the capture period is finished, a Download button will appear next to the Start button



- Click Download for the capture to be downloaded to the local PC.
- Email the diagnostic zip file to technical support (smc-support.emea@msasafety.com).

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

8.5 LED Functions



Tag	Description
SS	The SS LED will flash once a second to indicate that the bridge is in operation.
ERR	The SYS ERR LED will go on solid indicating there is a system error. If this occurs, immediately report the related “system error” shown in the error screen of the FS-GUI interface to support for evaluation.
PWR	This is the power light and should always be steady green when the unit is powered.
RX	The RX LED will flash when a message is received on the serial port on the 3-pin connector. **If the serial port is not used, this LED is non-operational.** RX1 applies to the R1 connection while RX2 applies to the R2 connection.
TX	The TX LED will flash when a message is sent on the serial port on the 3-pin connector. **If the serial port is not used, this LED is non-operational.** TX1 applies to the R1 connection while TX2 applies to the R2 connection.

Figure 27: Diagnostic LEDs

8.6 Factory Reset Instructions

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

8.7 Internet Browser Software Support

The following web browsers are supported:

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

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

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

9 Additional Information

9.1 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.

9.1.1 Configuring FieldServer as a SSL/TLS Server

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

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.

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’.

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.

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

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
```

9.1.2 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.

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.

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 **Section 9.2.1**.

Certificate Validation Options

Use the Check_Remote_Host element as described in **Section 9.2.1**.

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
```

9.2 Change Web Server Security Settings After Initial Setup

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

- The FieldServer landing page is the FS-GUI.
- Click Setup in the Navigation panel.

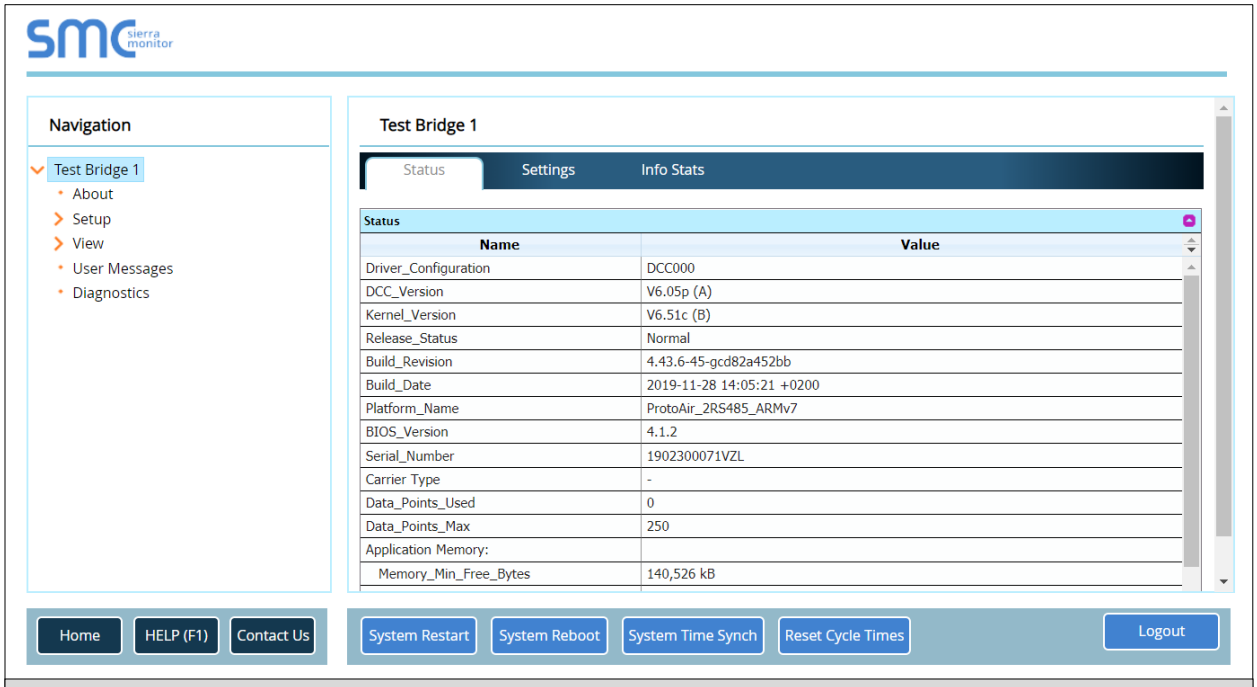


Figure 28: FS-GUI Page

9.2.1 Change Security Mode

- Click Security in the Navigation panel.

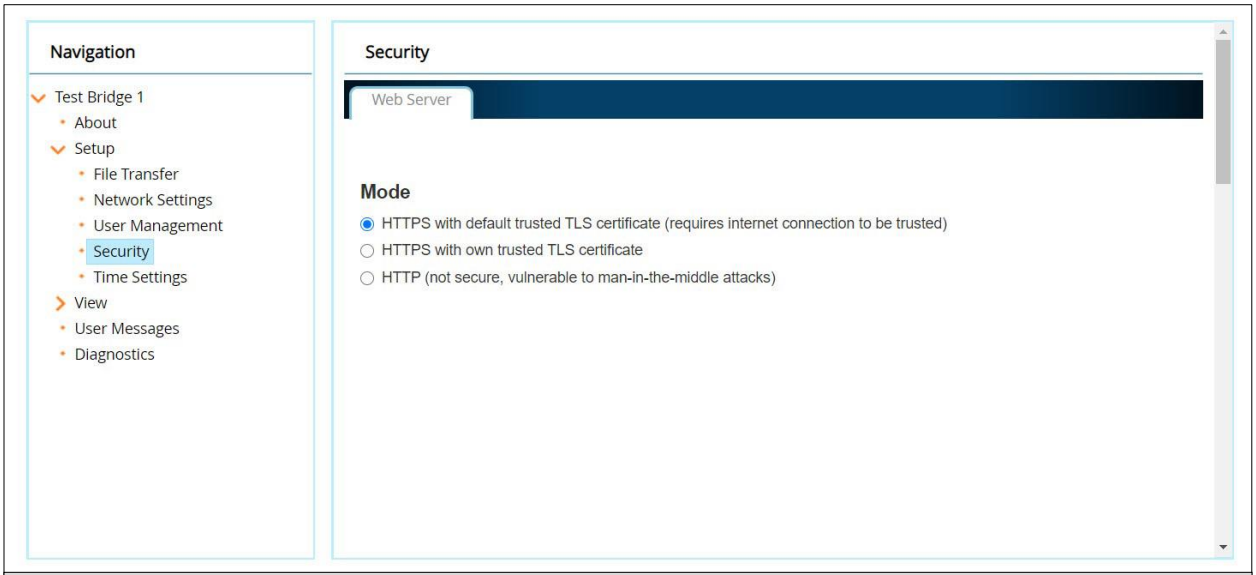


Figure 29: FS-GUI Security Setup

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

9.2.2 Edit the Certificate Loaded onto the FieldServer

NOTE: A loaded certificate will only be available if the security mode was previously setup as HTTPS with own trusted TLS certificate.

- Click Security in the Navigation panel.

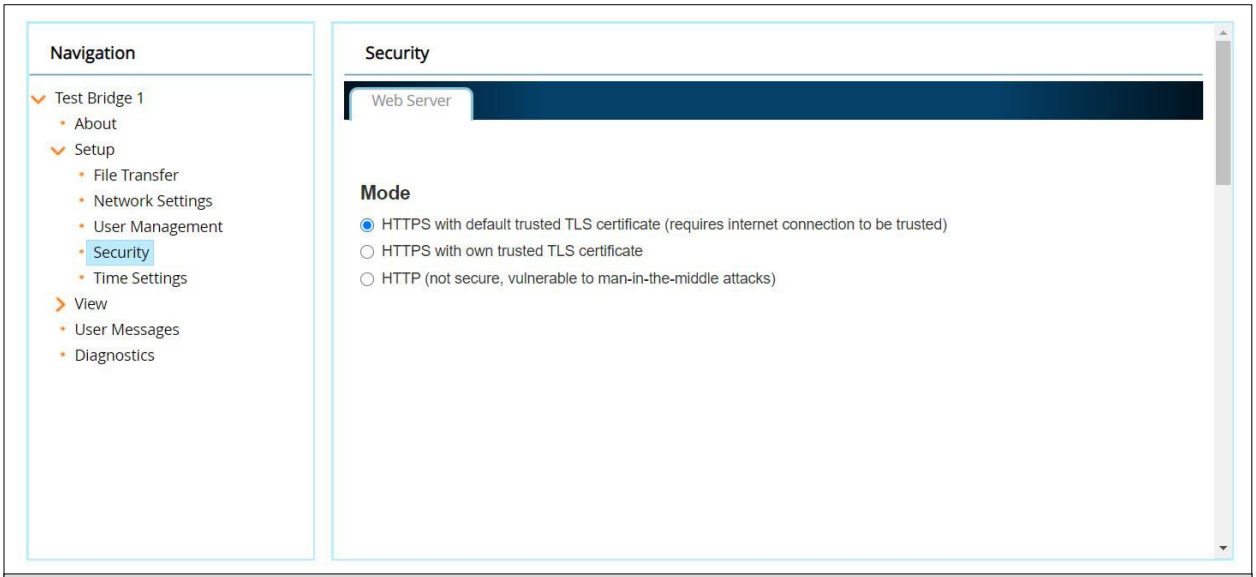


Figure 30: FS-GUI Security Setup – Certificate Loaded

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

9.3 Change User Management Settings

- From the FS-GUI page, click Setup in the Navigation panel.
- Click User Management in the navigation panel.

NOTE: If the passwords are lost, the unit can be reset to factory settings to reinstate the default unique password on the label. For recovery instructions, see the FieldServer Next Gen Recovery document. If the default unique password is lost, then the unit must be mailed back to the factory.

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

- Check that the Users tab is selected.

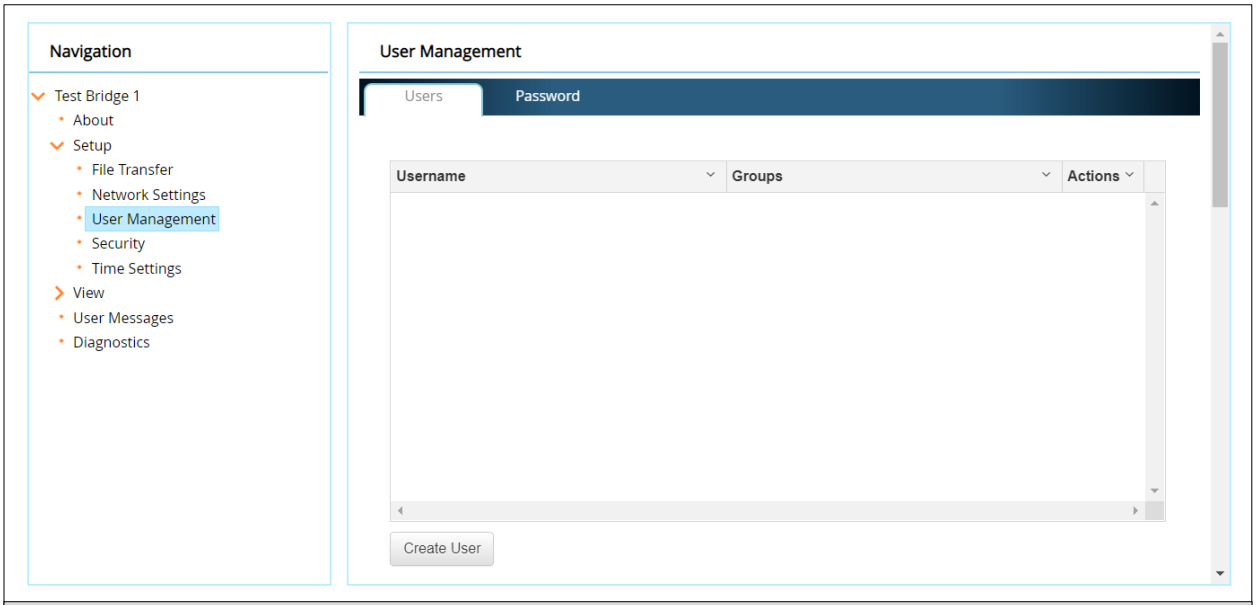


Figure 31: FS-GUI User Management

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.

9.3.1 Create Users

- Click the Create User button.

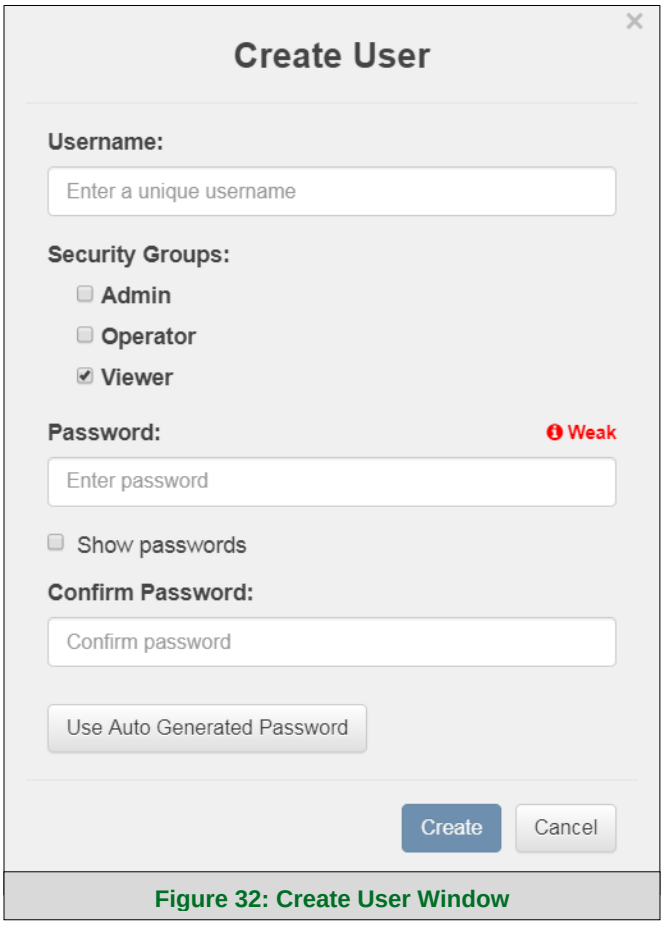


Figure 32: Create User Window

- 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.

9.3.2 Edit Users

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

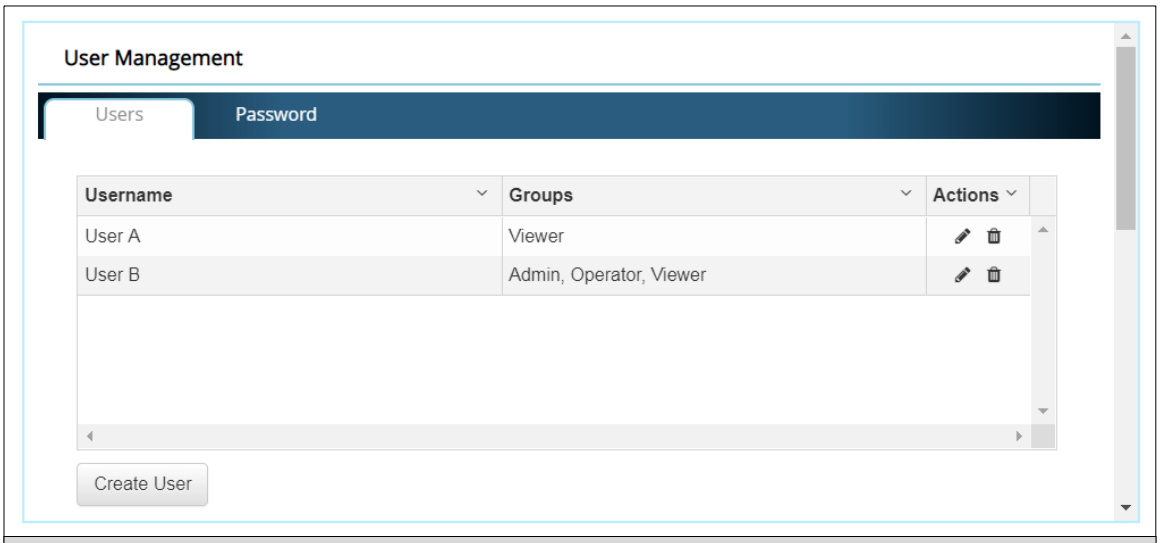


Figure 33: Setup Users

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

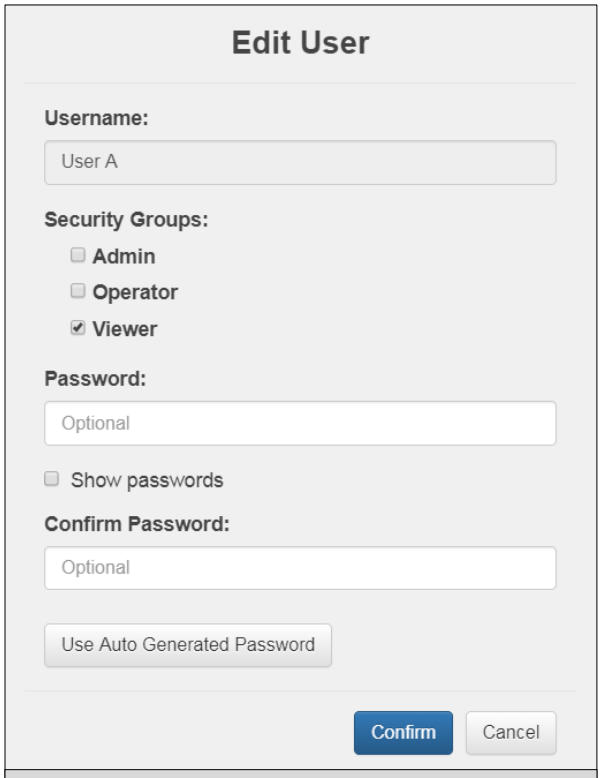


Figure 34: Edit User Window

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

9.3.3 Delete Users

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

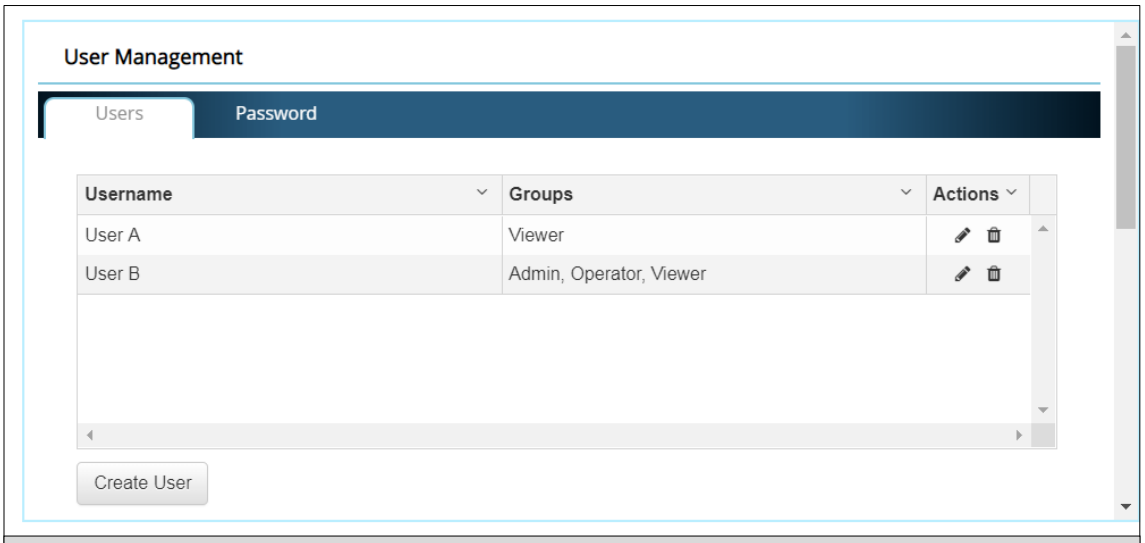


Figure 35: Setup Users

- When the warning message appears, click Confirm.

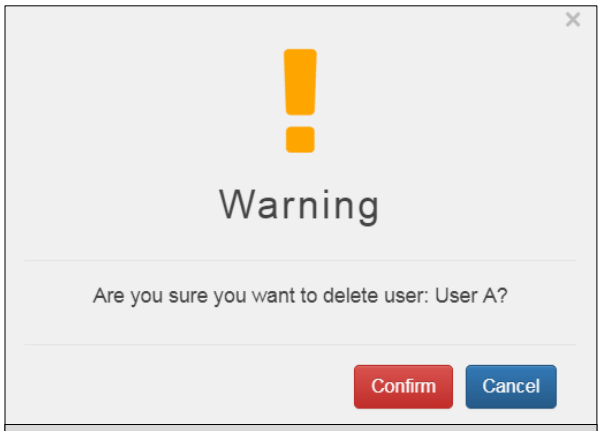


Figure 36: User Delete Warning

9.3.4 Change FieldServer Password

- Click the Password tab.

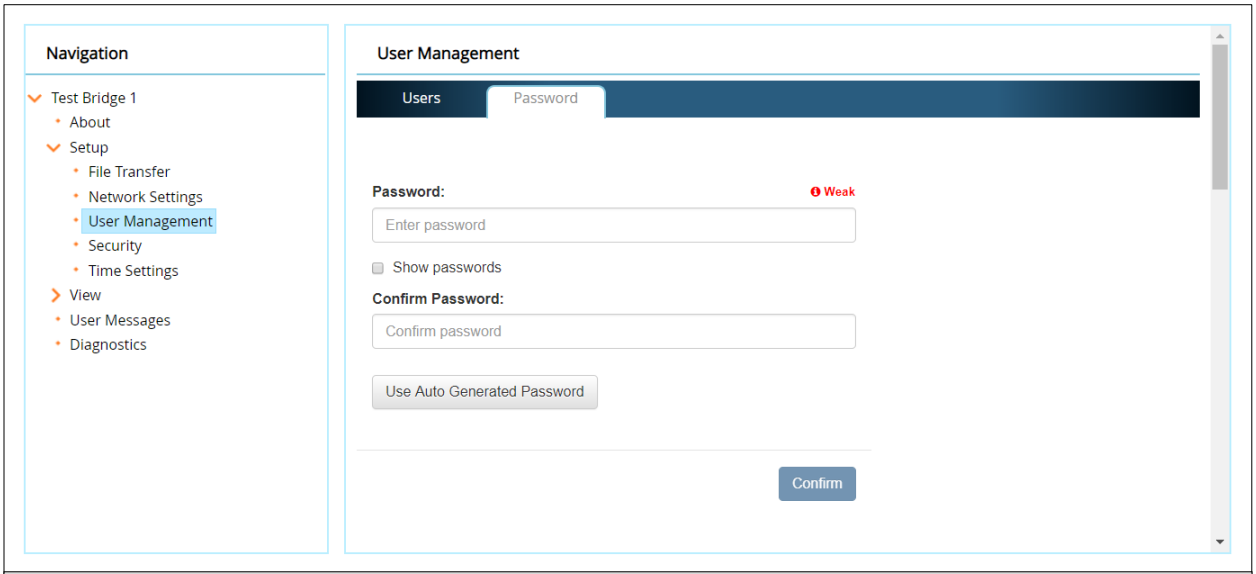


Figure 37: FieldServer Password Update via FS-GUI

- Change the general login password for the FieldServer as needed.

NOTE: The password must meet the minimum complexity requirements. An algorithm automatically checks the password entered and notes the level of strength on the top right of the Password text field.

9.4 Specifications

	FS-QS-3X10-F[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) Two Ethernet 10/100 BaseT ports
Power Requirements	*Input Voltage:* 9-30VDC or 24VAC *Current draw:* 24VAC 0.125A *Max Power:* 3 Watts 9-30VDC 0.25A @12VDC
Approvals	CE and FCC Class B & C Part 15, UL 62368-1, WEEE compliant, IC Canada, RoHS3 compliant, REACH compliant
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 38: 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.

9.5 Compliance with UL Regulations

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