Operating Manual

# QuickServer FS-QS-2XX0 Start-up Guide

Revision: 2.I

Document No.:T18627

Print Spec: 10000005389 (F)

MSA

The Safety Company

fieldserver

MSA Safety
1991 Tarob Court
Milpitas, CA 95035

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

For your local MSA contacts, please go to our website www.MSAsafety.com

# Contents

# 1 About the QuickServer

The 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 10 Troubleshooting, 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 Grid. See **Section 9 MSA Grid - FieldSever Manager Setup** for further information.

**NOTE: The FS-QS-2XX0-F contains all Serial and Ethernet drivers.**

## 1.1 Certification

**BTL Mark – BACnet Testing Laboratory**

The BTL Mark on the FieldServer 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. *BACnet is a registered trademark of ASHRAE*.

## 1.2 Supplied Equipment

**FieldServer 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.

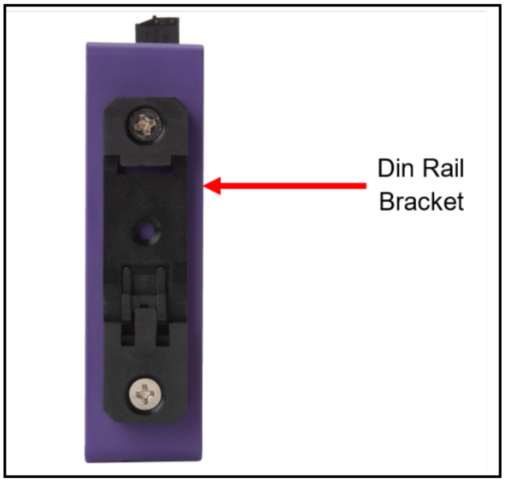
**Accessory kit (optional)** (Part # FS-8915-38-QS) includes:

- 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:
  - Start-up Guide
  - FieldServer Configuration Manual
  - All FieldServer Driver Manuals
  - Support Utilities
  - Any additional folders related to special files configured for a specific FieldServer
  - Additional components as required - see driver manual supplement for details

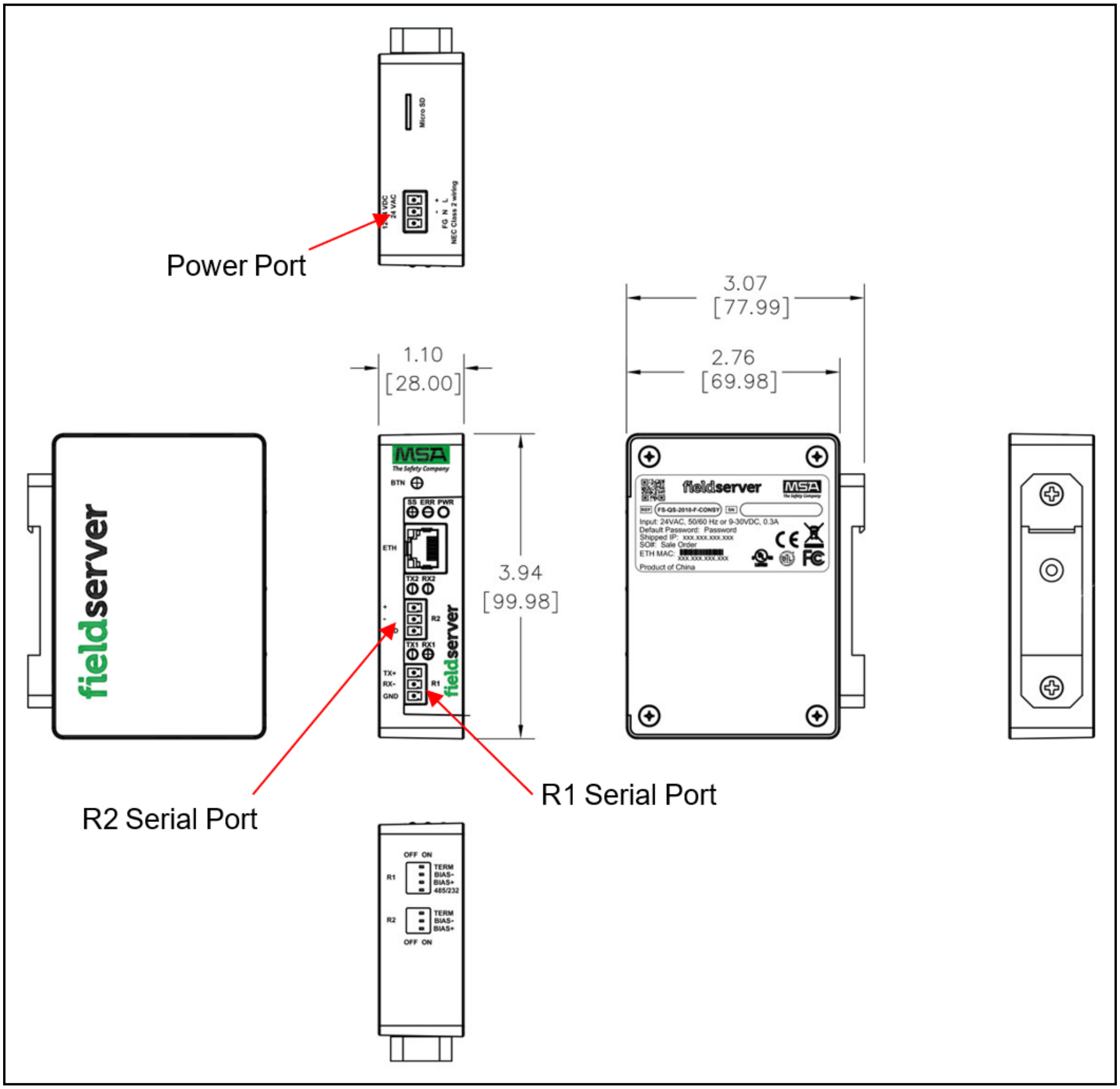
# 2 Equipment Setup

## 2.1 Mounting

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



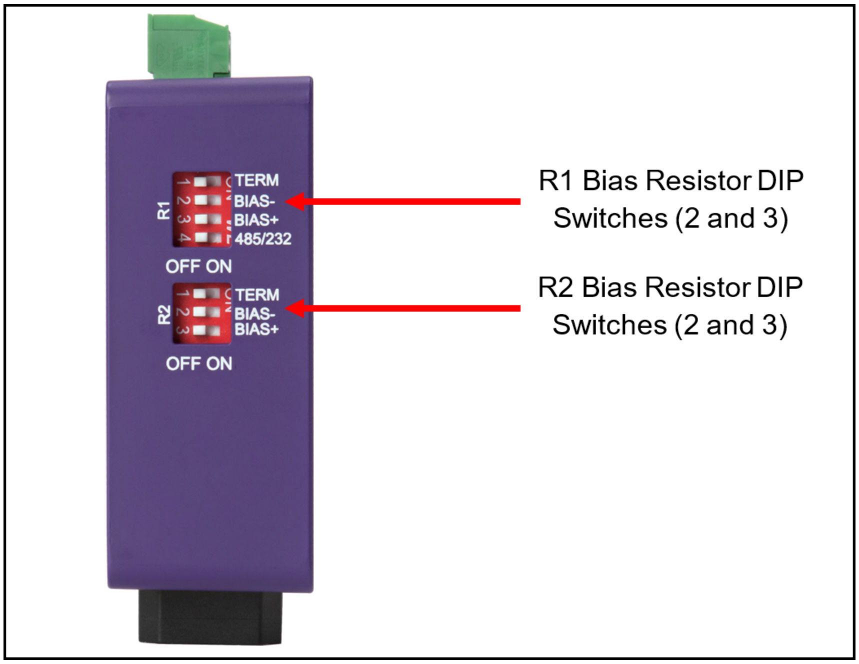
### 2.2 Physical Dimensions



# 3 Installation

## 3.1 DIP Switch Settings

### 3.1.1 Bias Resistors



R1 Bias Resistor DIP Switches (2 and 3)

R2 Bias Resistor DIP Switches (2 and 3)

**To enable Bias Resistors, move both the BIAS- and BIAS+ dip switches to the right in the orientation shown above**.

The bias resistors are used to keep the RS-485 bus to a known state, when there is no transmission on the line (bus is idling), to help prevent false bits of data from being detected. The bias resistors typically pull one line high and the other low - far away from the decision point of the logic.

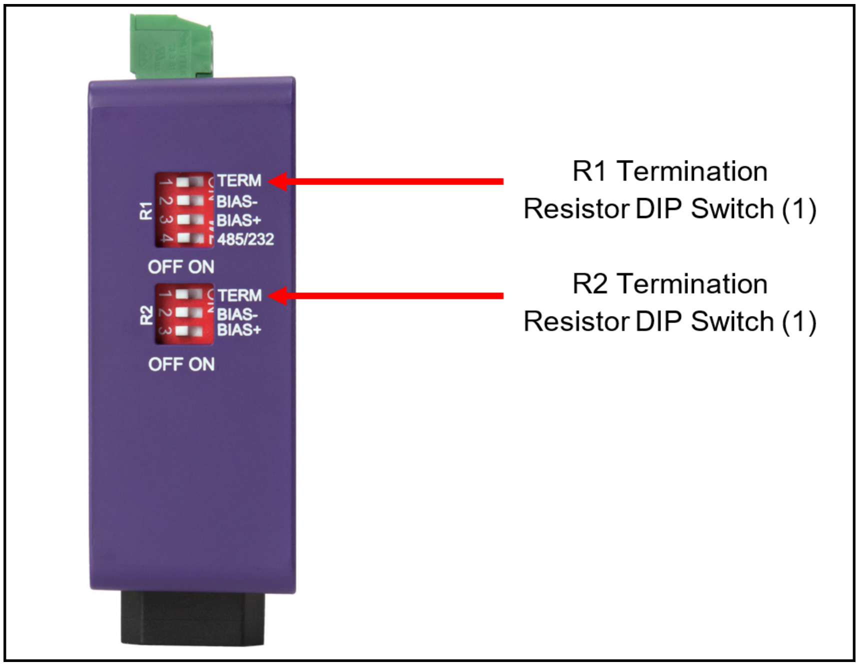
The bias resistor is 510 ohms which is in line with the BACnet spec. It should only be enabled at one point on the bus (for example, on the field port were there are very weak bias resistors of 100k). Since there are no jumpers, many QuickServers can be put on the network without running into the bias resistor limit which is < 500 ohms.

**NOTE: See [www.ni.com/support/serial/resinfo.htm](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


R1
1 2 3 4
TERM
BIAS-
BIAS+
485/232
OFF ON
R2
1 2 3
TERM
BIAS-
BIAS+
OFF ON
R1 Termination Resistor DIP Switch (1)
R2 Termination Resistor DIP Switch (1)

If the gateway is the last device on the serial trunk, then the End-Of-Line Termination Switch needs to be enabled**. To enable the Termination Resistor, move the TERM dip switch to the right in the orientation shown in above**.

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.**

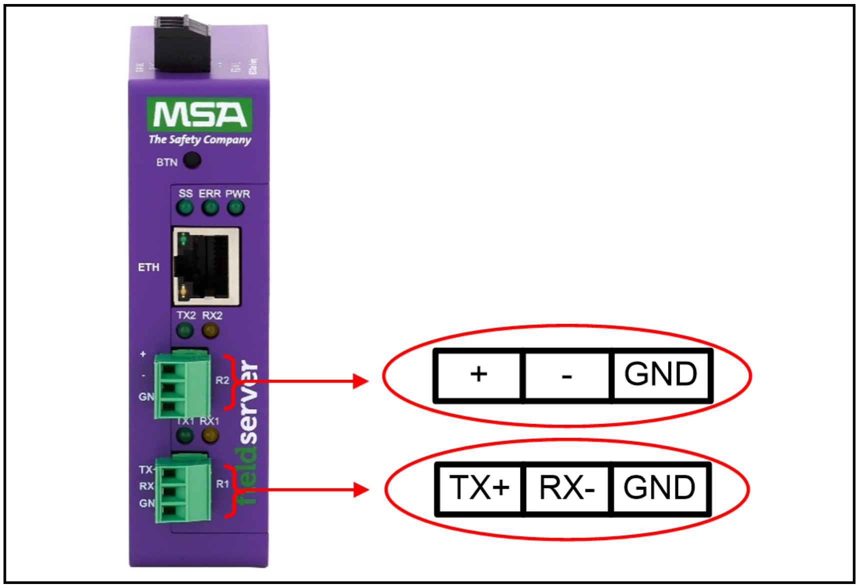
**NOTE: If the gateway is already powered on, DIP switch settings will not take effect unless the unit is power cycled.**

## 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 (see images in **Section 3.1 DIP Switch Settings**).

The R2 Port is RS-485.

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



### 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.**

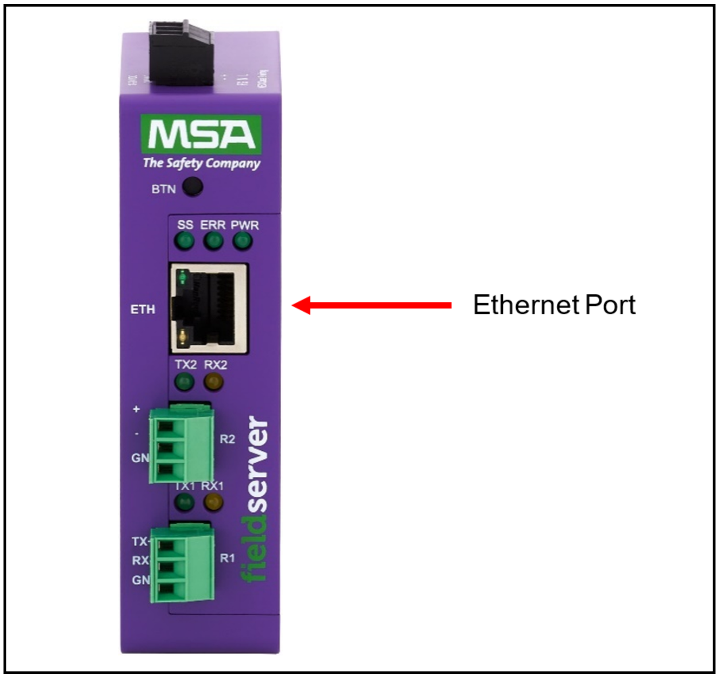
### 3.2.2 Supported RS-485 Baud Rates by Protocol

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, 115200

### 3.3 10/100 Ethernet Connection Port



The Ethernet Port is used both for BACnet/IP communications and for configuring the gateway via the Web App. To connect the gateway, 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 gateway is 192.168.2.101, Subnet Mask is 255.255.255.0.**

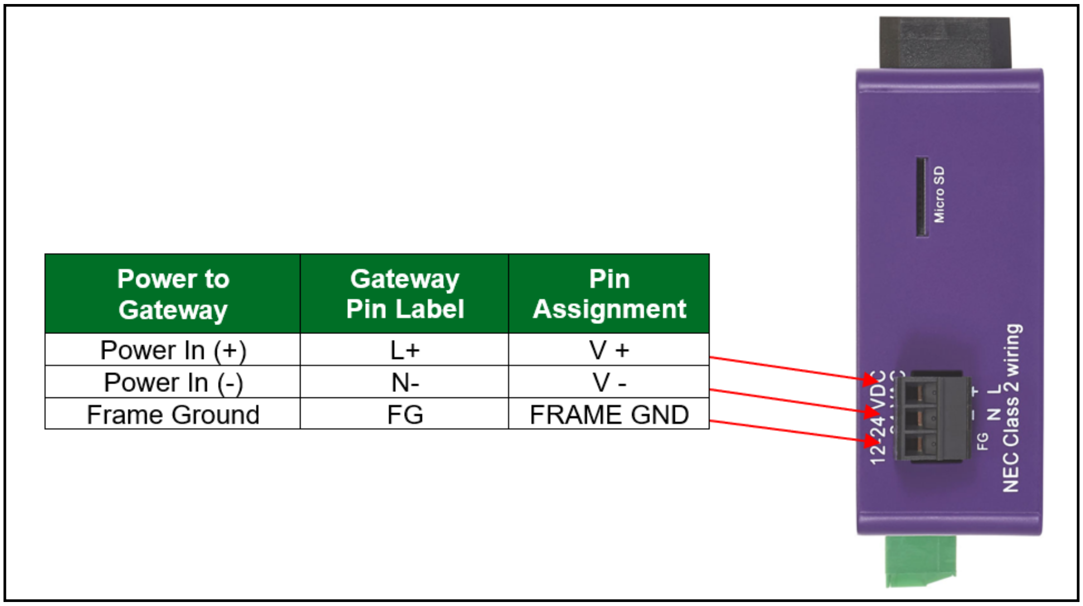
## 4 Power up the Gateway

Check power requirements in the table below:

| Power Requirement for QuickServer 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.** | | |

Apply power to the QuickServer as shown below. Ensure that the power supply used complies with the specifications provided in **Section 11.6 Specifications** .

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

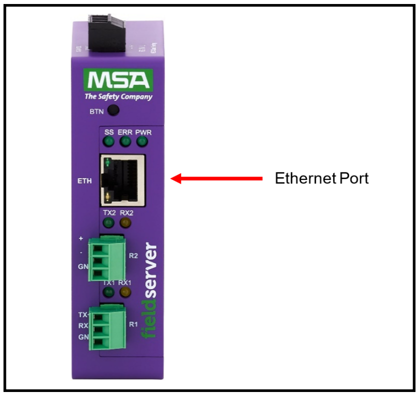


| Power to Gateway | Gateway Pin Label | Pin Assignment |
|---|---|---|
| Power In (+) | L+ | V + |
| Power In (-) | N- | V - |
| Frame Ground | FG | FRAME GND |

# 5 Connect the PC to the Gateway

## 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 .

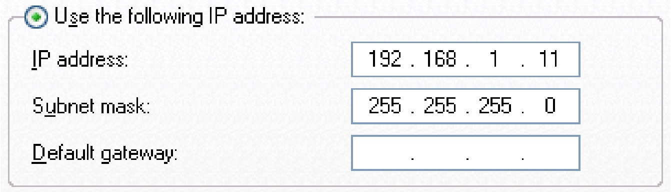


### 5.1.1 Changing the Subnet of the Connected PC

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 192.168.2.xxx network.

For Windows 10:

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



● 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 exit the Ethernet Properties window.

## 5.2 Navigate to the Login Page

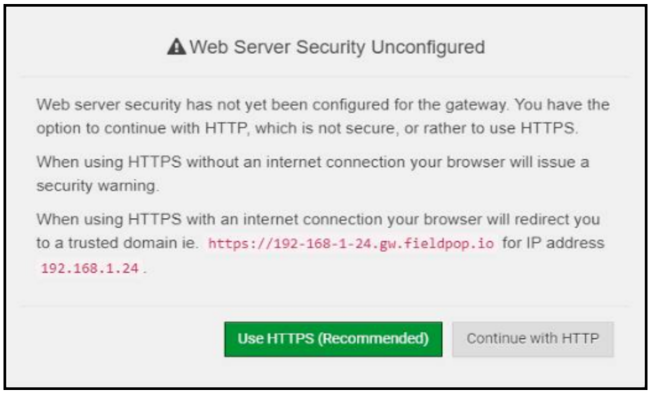
- Open a web browser and connect to the FieldServer's default IP Address. The default IP Address of the FieldServer is **192.168.2.101**, Subnet Mask is **255.255.255.0**.
- If the PC and the FieldServer are on different IP networks, assign a static IP Address to the PC on the 192.168.2.X network.

# 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.



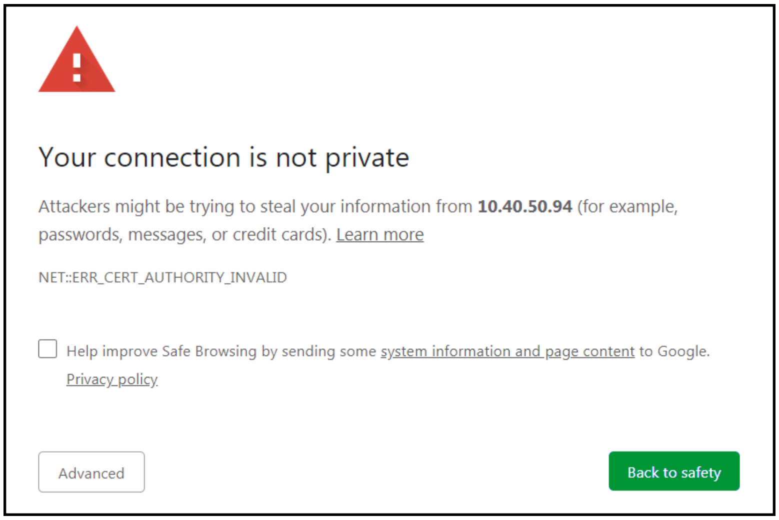
⚠ Web Server Security Unconfigured

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 to use HTTPS.

When using HTTPS without an internet connection your browser will issue a security warning.

When using HTTPS with an internet connection your browser will redirect you to a trusted domain ie. `https://192-168-1-24.gw.fieldpop.io` for IP address `192.168.1.24`.

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



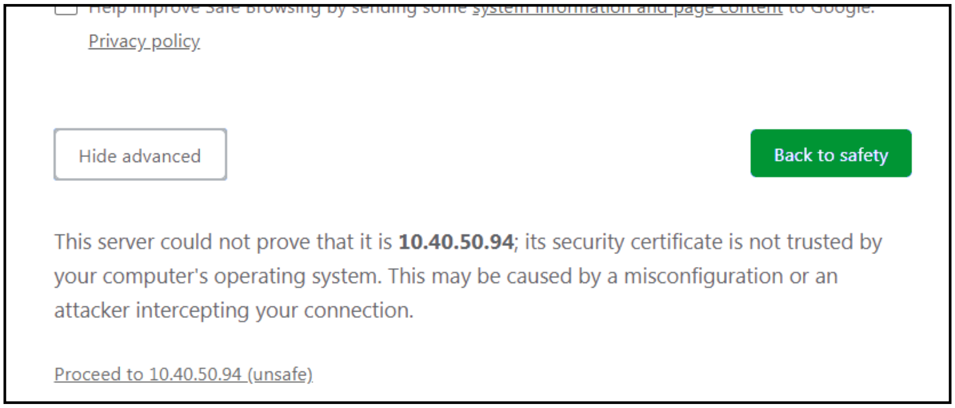
Your connection is not private

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

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



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

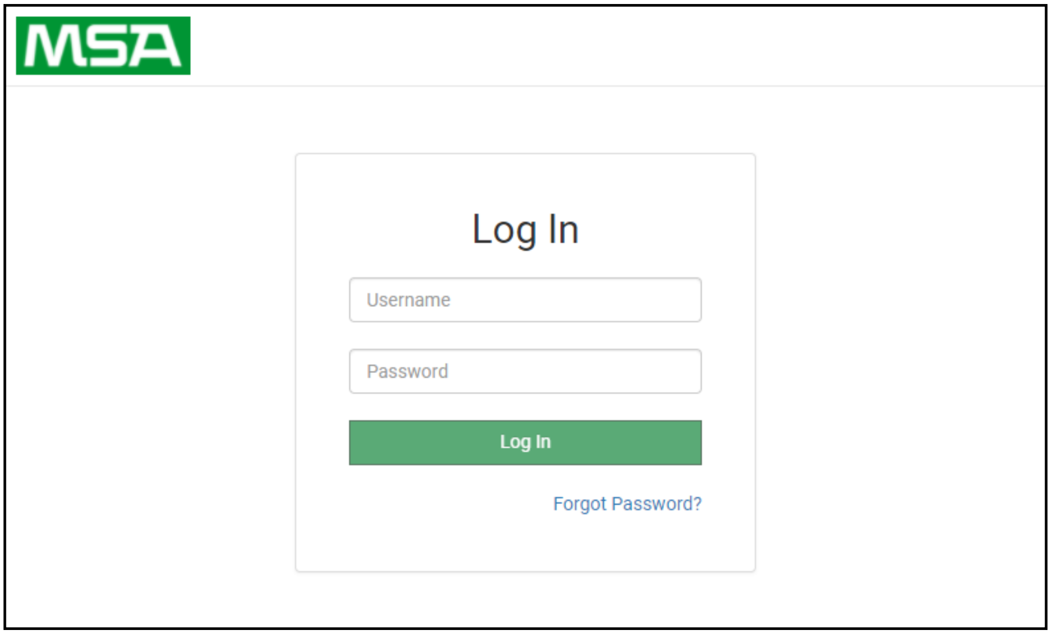
Privacy policy

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)

- 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.**

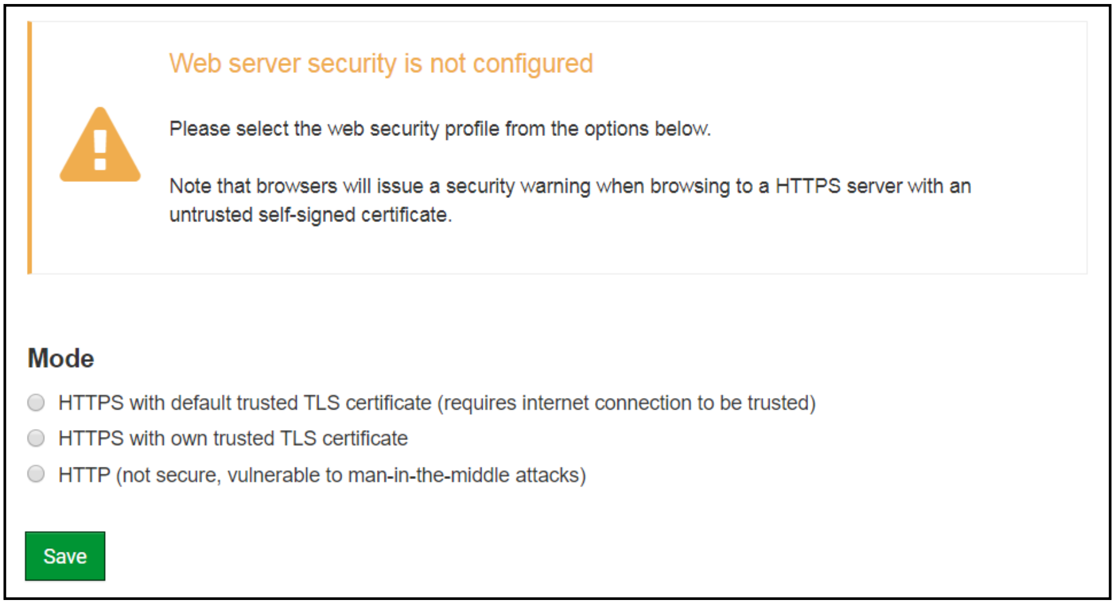


**NOTE: A user has 5 attempts to login then there will be a 10-minute lockout. There is no timeout on the FieldServer to enter a password.**

**NOTE: To create individual user logins, go to Section 11.3 Change User Management Settings.**

### 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)

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

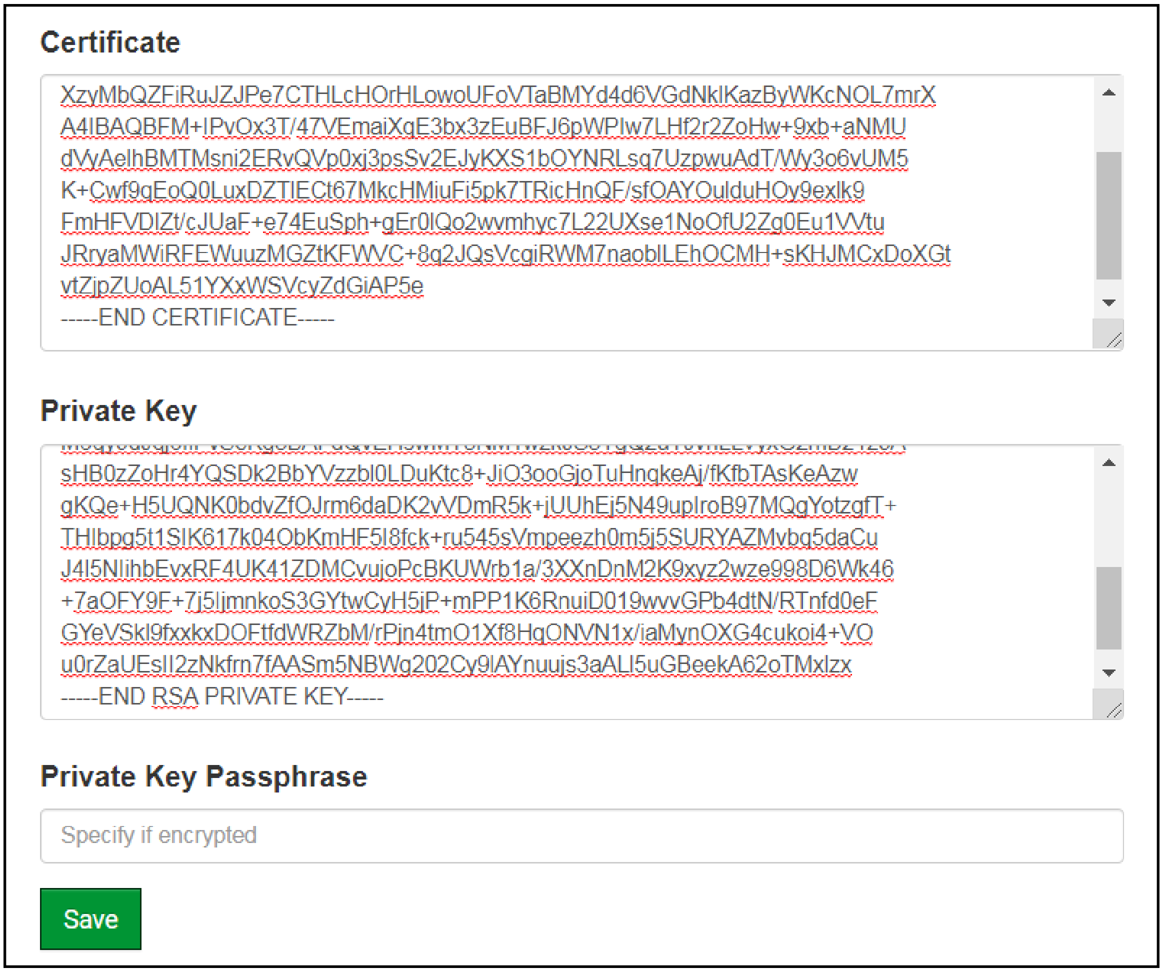
**NOTE: To change the web server security mode after initial setup, go to Section 11.2 Change Web Server Security Settings After Initial Setup.**

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.



Certificate

```
XzyMbQZFiRuJZJPe7CTHLcHOrHLowoUFoVTaBMYd4d6VGdNklKazByWKcNOL7mrX
A4IBAQBFM+IPvOx3T/47VEmaiXqE3bx3zEuBFJ6pWPlw7LHf2r2ZoHw+9xb+aNMU
dVyAelhBMTMsni2ERvQVp0xj3psSv2EJyKXS1bOYNRLsq7UzpwuAdT/Wy3o6vUM5
K+Cwf9qEoQ0LuxDZTlECt67MkcHMiuFi5pk7TRicHnQF/sfOAYOulduHOy9exlk9
FmHFVDlZt/cJUaF+e74EuSph+gEr0lQo2wvmhyc7L22UXse1NoOfU2Zg0Eu1VVtu
JRryaMWiRFEWuuzMGZtKFWVC+8q2JQsVcgiRWM7naoblLEhOCMH+sKHJMCxDoXGt
vtZjpZUoAL51YXxWSVcyZdGiAP5e
-----END CERTIFICATE-----
```

Private Key

```
sHB0zZoHr4YQSDk2BbYVzzbl0LDuKtc8+JiO3ooGjoTuHnqkeAj/fKfbTAsKeAzw
gKQe+H5UQNK0bdvZfOJrm6daDK2vVDmR5k+jUUhEj5N49upIroB97MQgYotzgfT+
THlbpg5t1SlK617k04ObKmHF5l8fck+ru545sVmpeezh0m5j5SURYAZMvbq5daCu
J4I5NIihbEvxRF4UK41ZDMCvujoPcBKUWrb1a/3XXnDnM2K9xyz2wze998D6Wk46
+7aOFY9F+7j5ljmnkoS3GYtwCyH5jP+mPP1K6RnuiD019wvvGPb4dtN/RTnfd0eF
GYeVSkl9fxxkxDOFtfdWRZbM/rPjn4tmO1Xf8HqONVN1x/iaMynOXG4cukoi4+VO
u0rZaUEsIl2zNkfrn7fAASm5NBWg202Cy9lAYnuujs3aALl5uGBeekA62oTMxlzx
-----END RSA PRIVATE KEY-----
```

Private Key Passphrase

Specify if encrypted

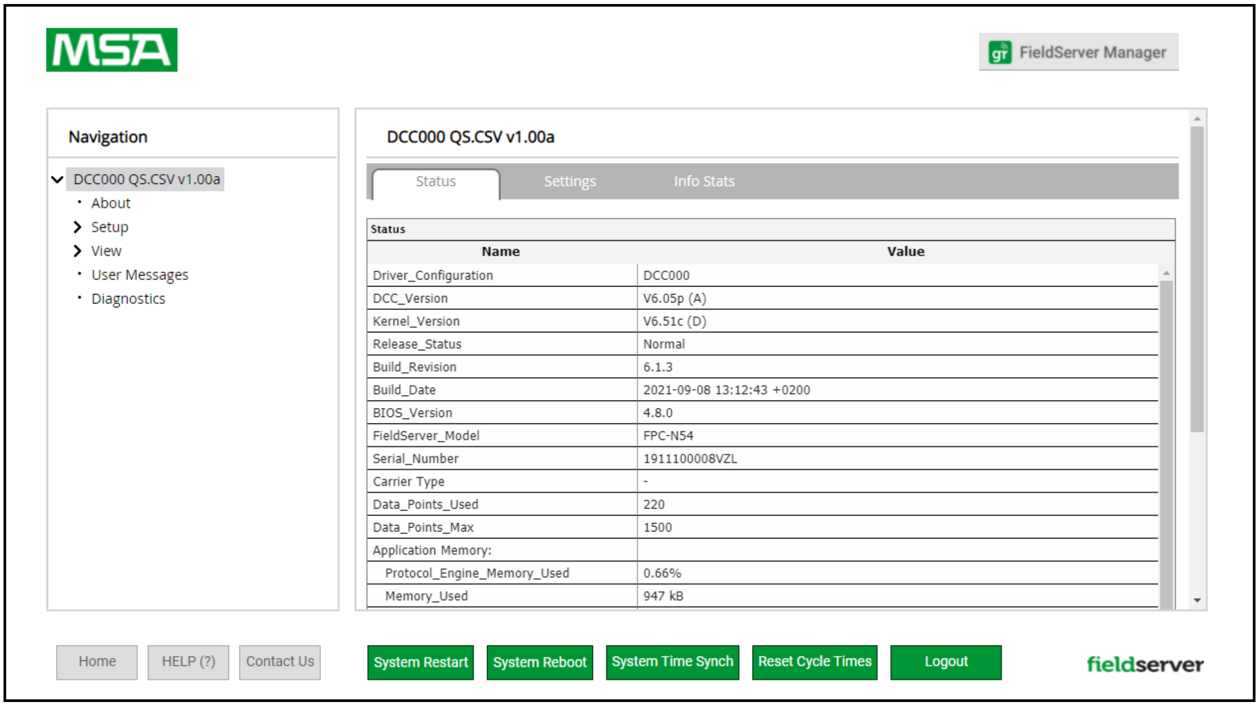
- Copy and paste the Certificate and Private Key text into their respective fields. If the Private Key is encrypted type in the associated Passphrase.
- Click Save.
- A “Redirecting” message will appear. After a short time, the FieldServer GUI will open.

### 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 Setup Network

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



Status

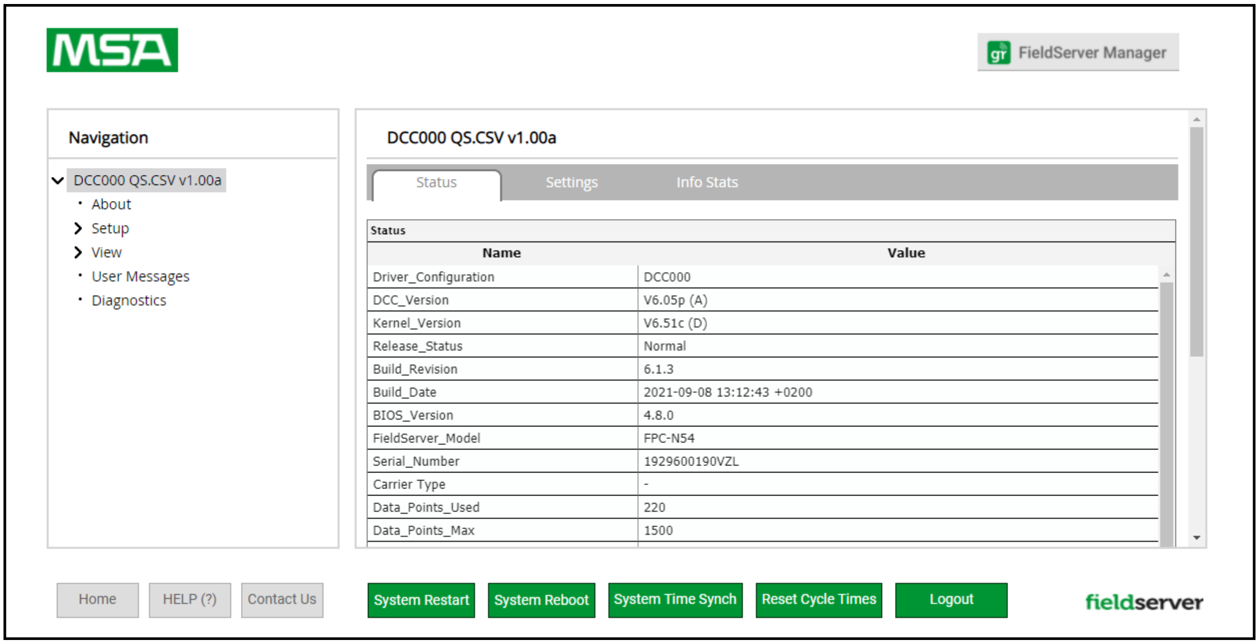
| Name | Value |
|---|---|
| Driver_Configuration | DCC000 |
| DCC_Version | V6.05p (A) |
| Kernel_Version | V6.51c (D) |
| Release_Status | Normal |
| Build_Revision | 6.1.3 |
| Build_Date | 2021-09-08 13:12:43 +0200 |
| BIOS_Version | 4.8.0 |
| FieldServer_Model | FPC-N54 |
| Serial_Number | 1911100008VZL |
| Carrier Type | - |
| Data_Points_Used | 220 |
| Data_Points_Max | 1500 |
| Application Memory: | |
| Protocol_Engine_Memory_Used | 0.66% |
| Memory_Used | 947 kB |

**NOTE: The FieldServer Manager tab FieldServer Manager (see image above) allows users to connect to the Grid, MSA Safety's device cloud solution for IIoT. The FieldServer Manager enables secure remote connection to field devices through a FieldServer and its local applications for configuration, management, maintenance. For more information about the FieldServer Manager, refer to the MSA Grid - FieldServer Manager Start-up Guide.**

### 7.1 Using FS-GUI to Input Network Settings

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

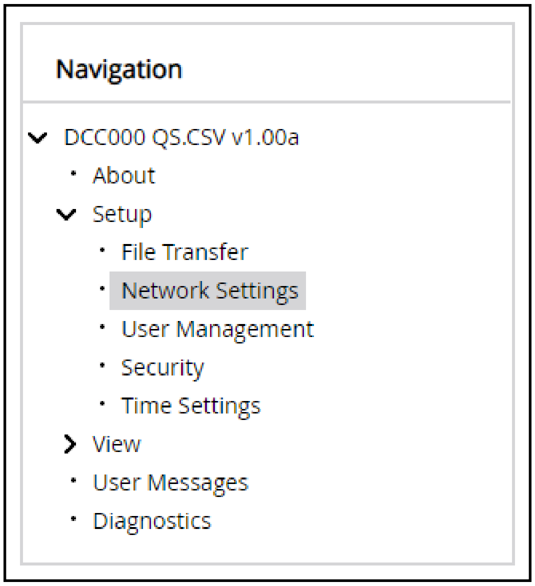
- Find the Navigation tree across the left side of the screen.
- Click the arrow next to the FieldServer title/CN number to expand the tree.



Status

| Name | Value |
|---|---|
| Driver_Configuration | DCC000 |
| DCC_Version | V6.05p (A) |
| Kernel_Version | V6.51c (D) |
| Release_Status | Normal |
| Build_Revision | 6.1.3 |
| Build_Date | 2021-09-08 13:12:43 +0200 |
| BIOS_Version | 4.8.0 |
| FieldServer_Model | FPC-N54 |
| Serial_Number | 1929600190VZL |
| Carrier Type | - |
| Data_Points_Used | 220 |
| Data_Points_Max | 1500 |

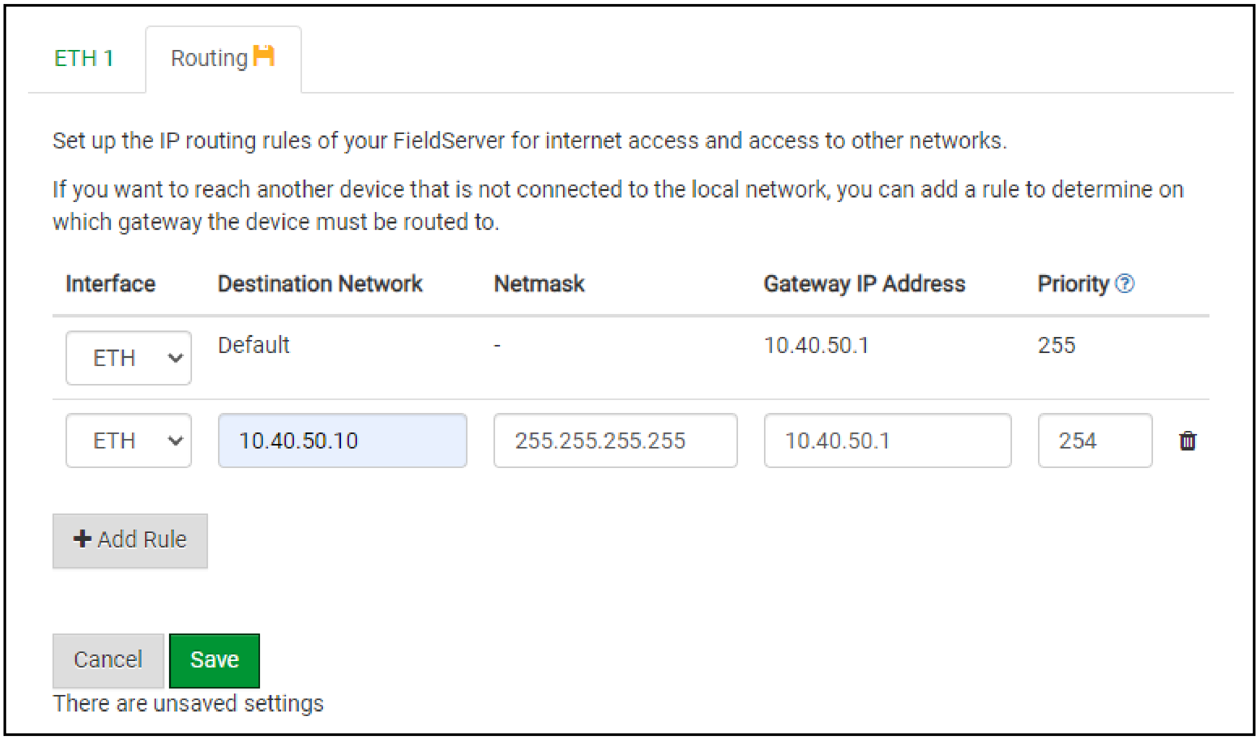
- Click on the arrow next to Setup to expand the tree.
- Click on Network Settings.



### 7.2 Routing Settings

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

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



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

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

| Interface | Destination Network | Netmask | Gateway IP Address | Priority |
|---|---|---|---|---|
| ETH | Default | - | 10.40.50.1 | 255 |
| ETH | 10.40.50.10 | 255.255.255.255 | 10.40.50.1 | 254 |

There are unsaved settings

### 7.3 Ethernet 1 Network Settings

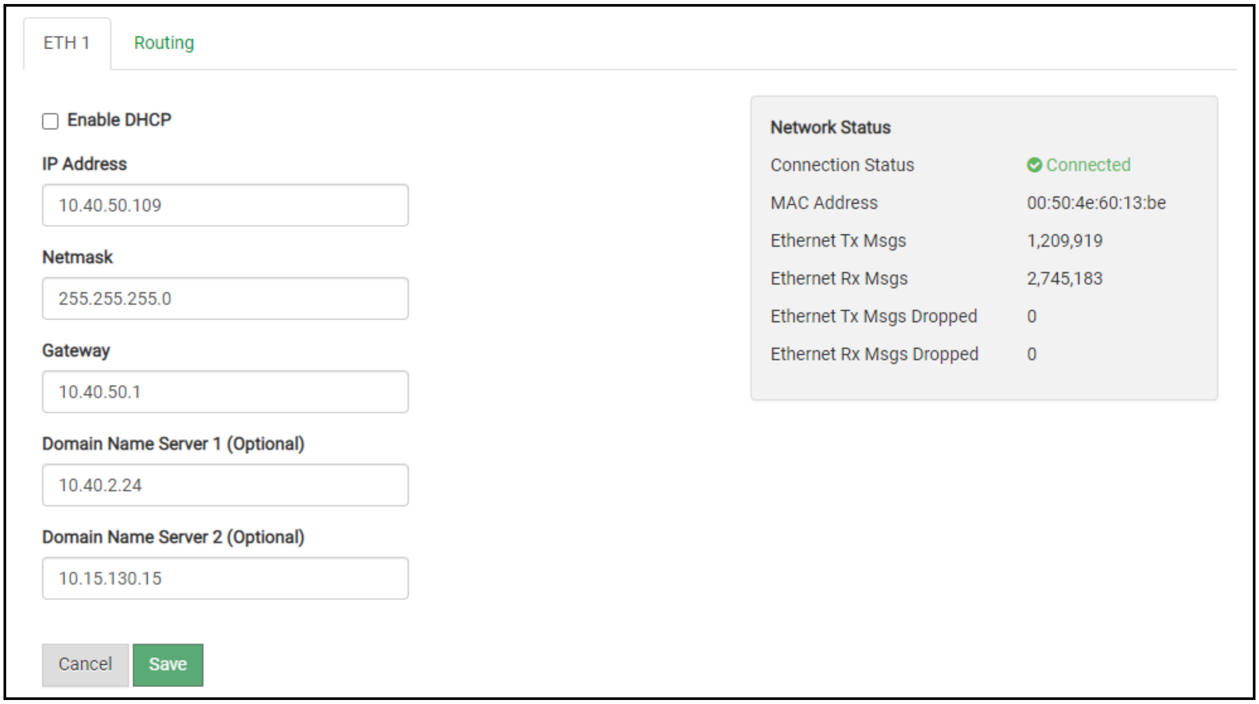
To change the IP Settings, follow these instructions:

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

**NOTE: If 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 Save to record and activate the new IP Address.
- Connect the FieldServer to the local network or router.

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



□ Enable DHCP

IP Address: 10.40.50.109

Netmask: 255.255.255.0

Gateway: 10.40.50.1

Domain Name Server 1 (Optional): 10.40.2.24

Domain Name Server 2 (Optional): 10.15.130.15

Network Status

| | |
|---|---|
| Connection Status | ✓ Connected |
| MAC Address | 00:50:4e:60:13:be |
| Ethernet Tx Msgs | 1,209,919 |
| Ethernet Rx Msgs | 2,745,183 |
| Ethernet Tx Msgs Dropped | 0 |
| Ethernet Rx Msgs Dropped | 0 |

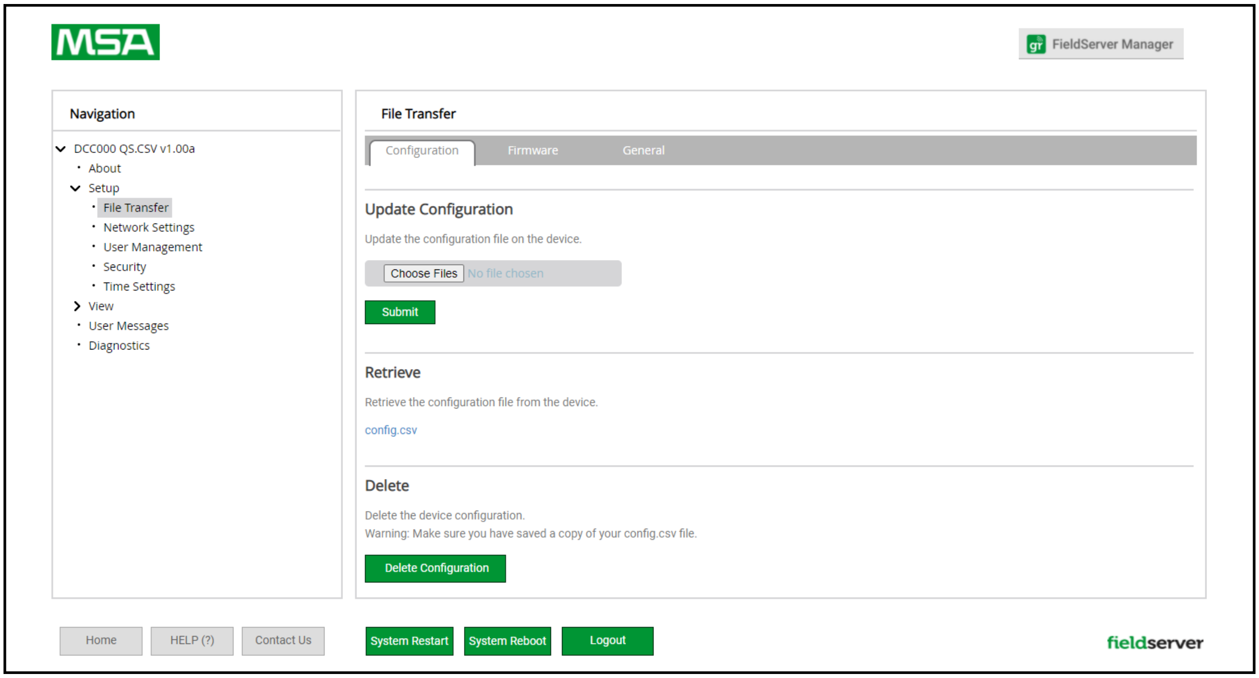
# 8 Configuring the QuickServer

## 8.1 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.

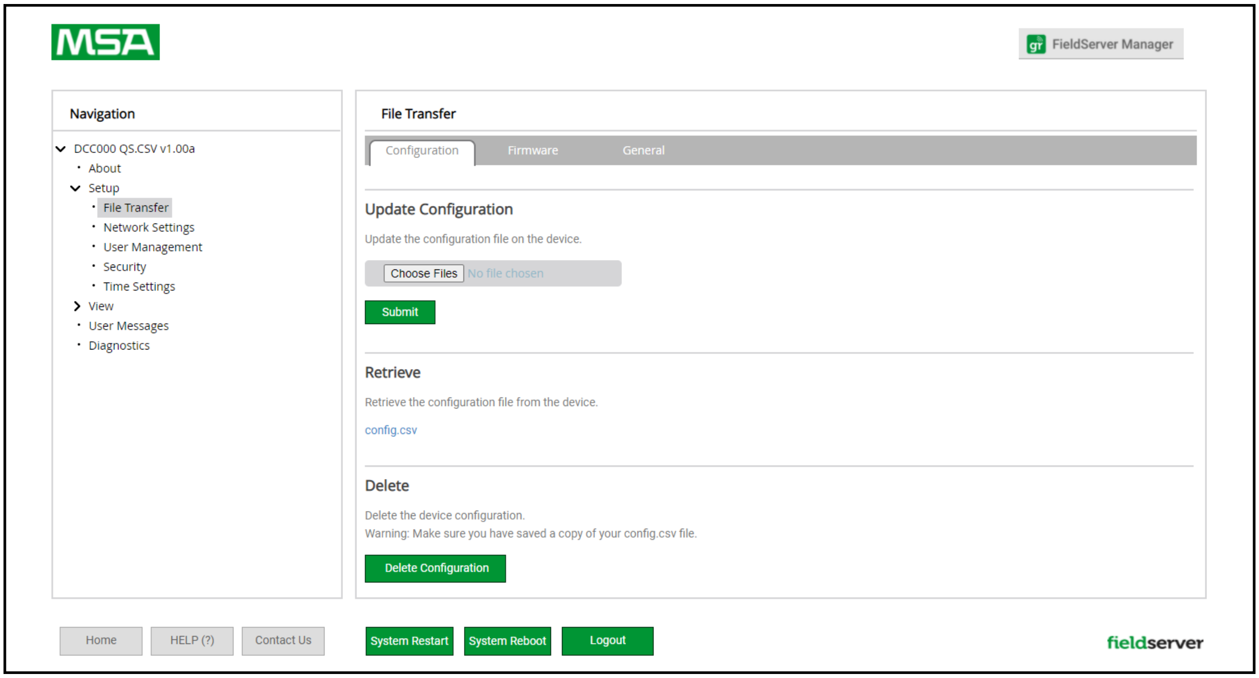
## 8.2 Change the Configuration File to Meet the Application

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

## 8.3 Load the Updated Configuration File

### 8.3.1 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.

config.csv

Delete

Delete the device configuration.

Warning: Make sure you have saved a copy of your config.csv file.

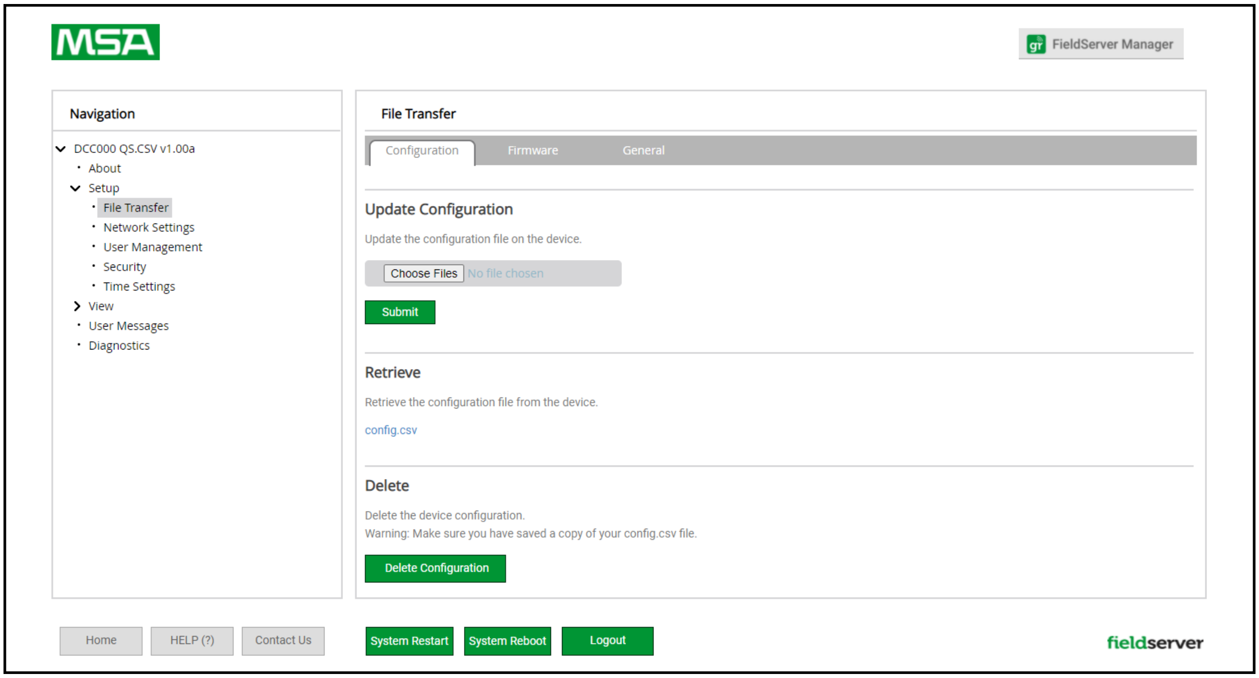
- Once download is complete, a message bar will appear confirming that the configuration was updated successfully.
- Click the System Restart Button to put the new file into operation.

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

### 8.3.2 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”.



Update Configuration

Update the configuration file on the device.

Retrieve

Retrieve the configuration file from the device.

Delete

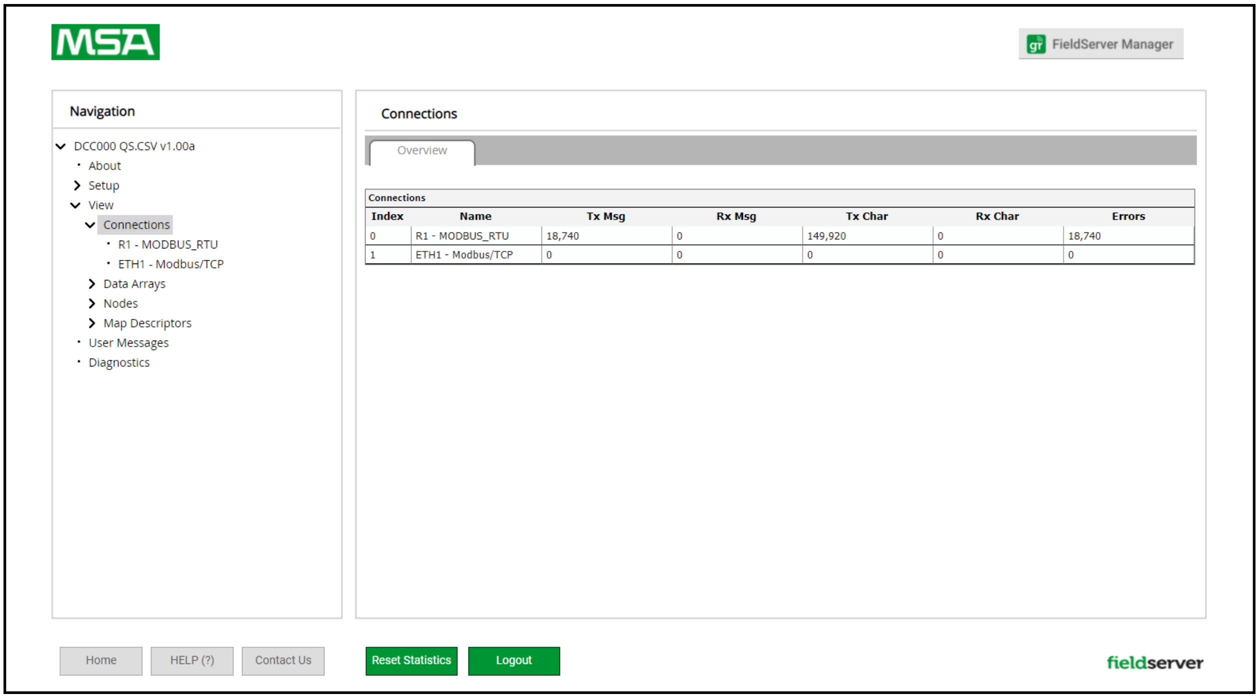
Delete the device configuration.
Warning: Make sure you have saved a copy of your config.csv file.

- 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.**

## 8.4 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 | R1 - MODBUS_RTU | 18,740 | 0 | 149,920 | 0 | 18,740 |
| 1 | ETH1 - Modbus/TCP | 0 | 0 | 0 | 0 | 0 |

**NOTE: For troubleshooting assistance refer to Section 10 Troubleshooting, 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.**

### 8.4.1 Accessing the FieldServer Manager

**NOTE: The FieldServer Manager tab FieldServer Manager (see image above) allows users to connect to the Grid, MSA Safety’s device cloud solution for IIoT. The FieldServer Manager enables secure remote connection to field devices through a FieldServer and its local applications for configuration, management, maintenance. For more information about the FieldServer Manager, refer to the MSA Grid - FieldServer Manager Start-up Guide.**

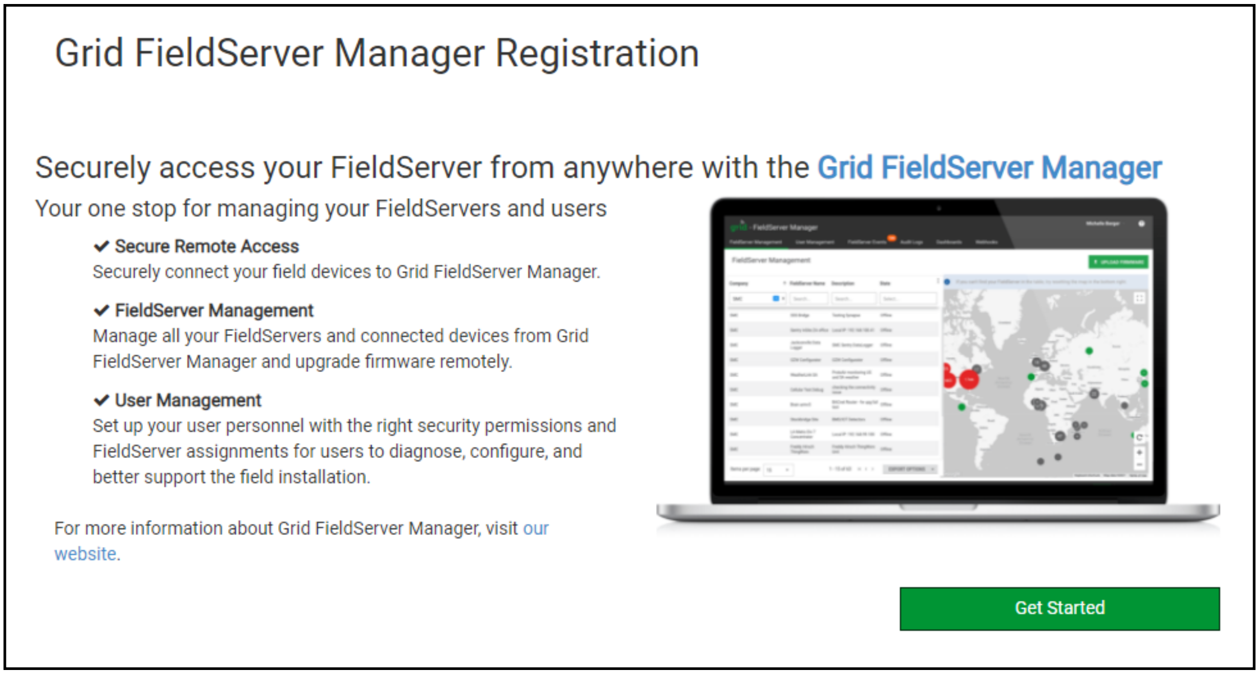
# 9 MSA Grid - FieldSever Manager Setup

**The Grid is MSA Safety's device cloud solution for IIoT. Integration with the MSA Grid - FieldServer Manager enables the a secure remote connection to field devices through a FieldServer and hosts local applications for device configuration, management, as well as maintenance. For more information about the FieldServer Manager, refer to the MSA Grid - FieldServer Manager Start-up Guide.**

## 9.1 Registration Process

- After logging onto the QuickServer, go to the FS-GUI webpage and click the FieldServer Manager button gr FieldServer Manager in the top right corner of the page.

**NOTE: If a warning message appears instead, go to Section 11.7 FieldServer Manager Connection Warning Message to resolve the connection issue.**



Grid FieldServer Manager Registration

Securely access your FieldServer from anywhere with the Grid FieldServer Manager

Your one stop for managing your FieldServers and users

✓ Secure Remote Access

Securely connect your field devices to Grid FieldServer Manager.

✓ FieldServer Management

Manage all your FieldServers and connected devices from Grid FieldServer Manager and upgrade firmware remotely.

✓ User Management

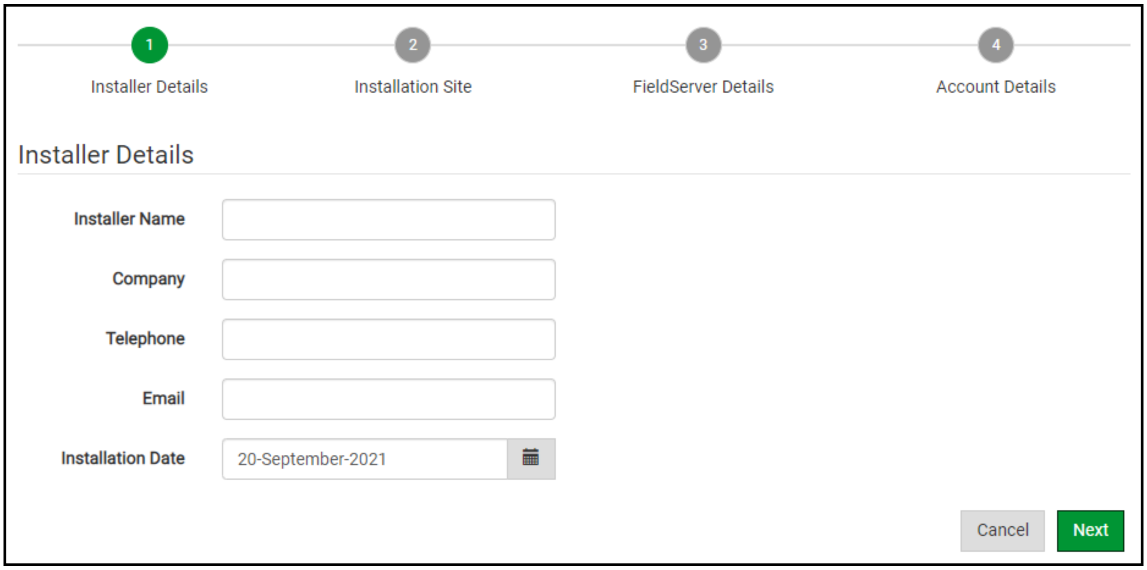
Set up your user personnel with the right security permissions and FieldServer assignments for users to diagnose, configure, and better support the field installation.

For more information about Grid FieldServer Manager, visit our website.

Get Started

- Click Get Started to view the Grid registration page.

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



1 Installer Details — 2 Installation Site — 3 FieldServer Details — 4 Account Details

Installer Details

Installer Name

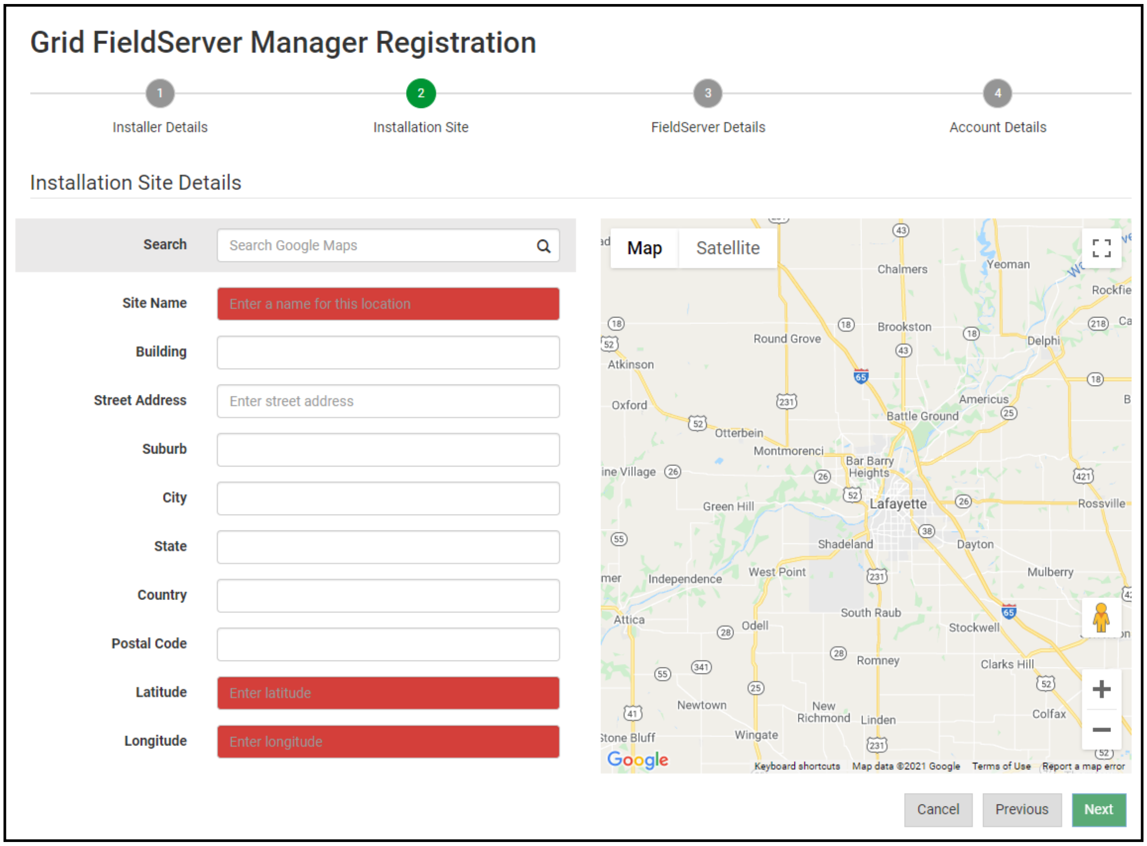
Company

Telephone

Email

Installation Date 20-September-2021

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



Grid FieldServer Manager Registration

1 Installer Details — 2 Installation Site — 3 FieldServer Details — 4 Account Details

Installation Site Details

Search: Search Google Maps

Site Name: Enter a name for this location

Building

Street Address: Enter street address

Suburb

City

State

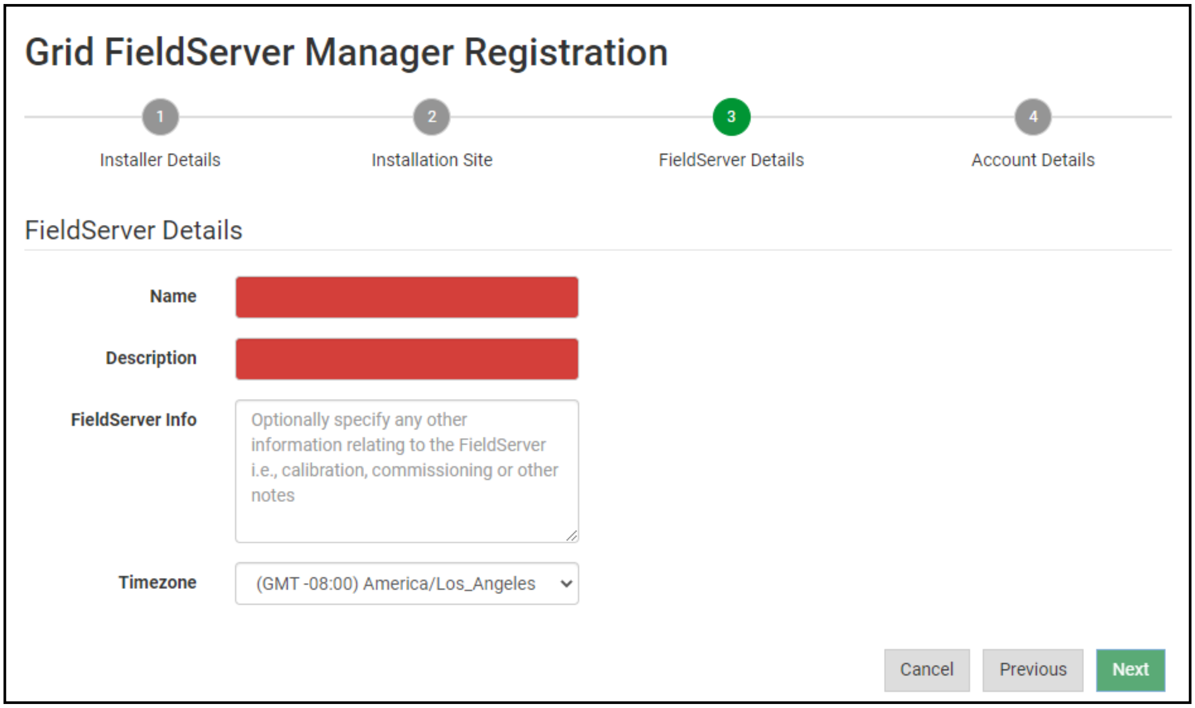
Country

Postal Code

Latitude: Enter latitude

Longitude: Enter longitude

- Enter Name and Description (required) then click Next

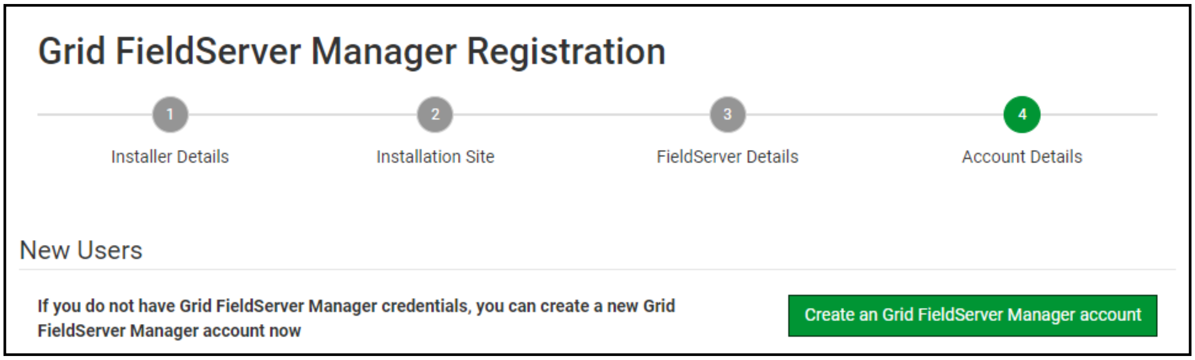


## Grid FieldServer Manager Registration

### FieldServer Details

| | |
|---|---|
| Name | [redacted] |
| Description | [redacted] |
| FieldServer Info | Optionally specify any other information relating to the FieldServer i.e., calibration, commissioning or other notes |
| Timezone | (GMT -08:00) America/Los_Angeles |

- Click the “Create an Grid FieldServer Manager account” button

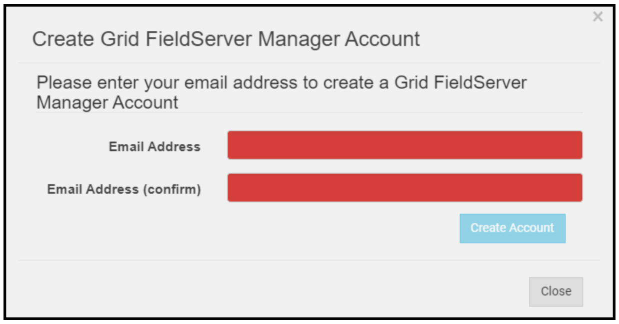


## Grid FieldServer Manager Registration

### New Users

If you do not have Grid FieldServer Manager credentials, you can create a new Grid FieldServer Manager account now

- Enter a valid email and click the Create Account button to send a “Welcome to the MSA Grid” invite to the email address entered



Create Grid FieldServer Manager Account

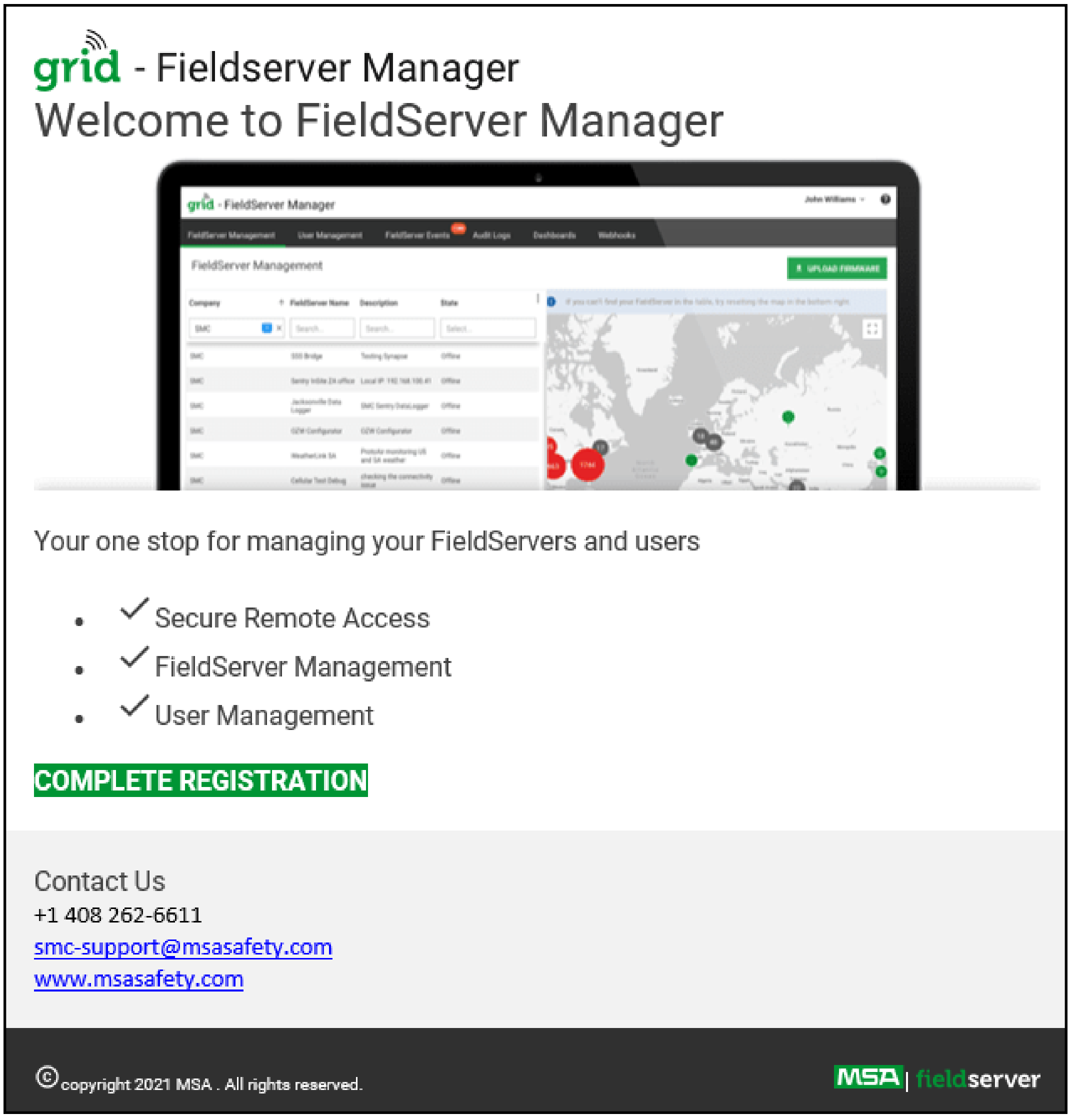
Please enter your email address to create a Grid FieldServer Manager Account

| | |
|---|---|
| Email Address | [redacted] |
| Email Address (confirm) | [redacted] |

### 9.2 User Setup

Before the gateway can be connected to the FieldServer Manager, a user account must be created. Request an invitation to the FieldServer Manager from the manufacturer's support team. Once an invitation has been requested (see **Section 9.1 Registration Process**), follow the instructions below to set up login details:

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



grid - Fieldserver Manager

Welcome to FieldServer Manager

Your one stop for managing your FieldServers and users

- ✓ Secure Remote Access
- ✓ FieldServer Management
- ✓ User Management

COMPLETE REGISTRATION

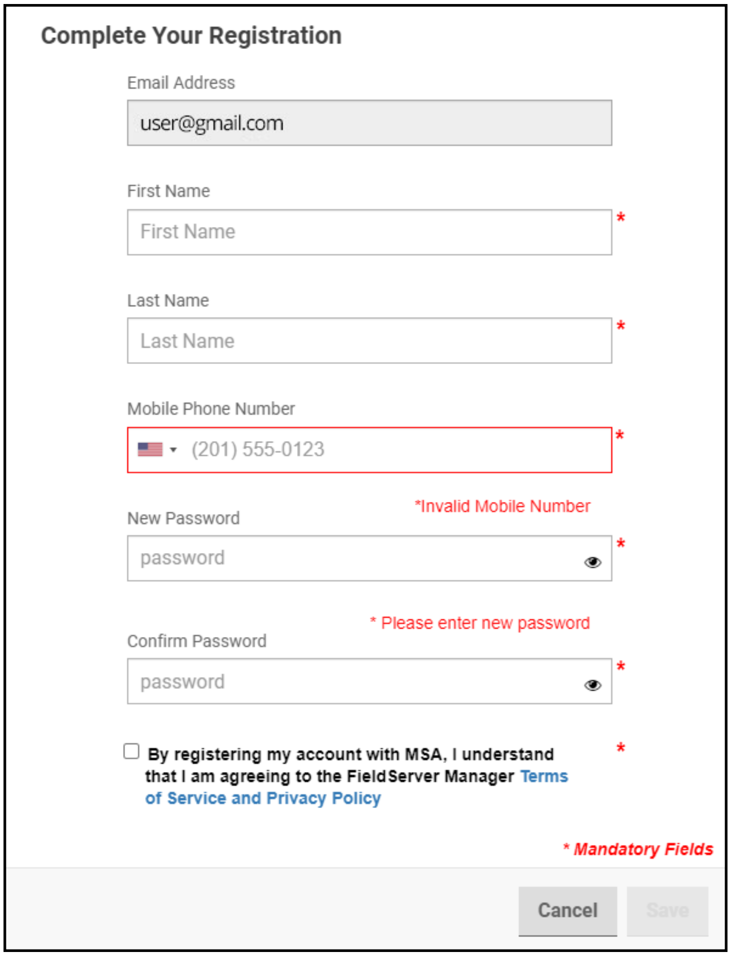
Contact Us
+1 408 262-6611
smc-support@msasafety.com
www.msasafety.com

©copyright 2021 MSA . All rights reserved.

MSA | fieldserver

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

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



Complete Your Registration

Email Address

user@gmail.com

First Name

First Name *

Last Name

Last Name *

Mobile Phone Number

(201) 555-0123 *

*Invalid Mobile Number

New Password

password *

* Please enter new password

Confirm Password

password *

□ By registering my account with MSA, I understand that I am agreeing to the FieldServer Manager Terms of Service and Privacy Policy *

*** Mandatory Fields***

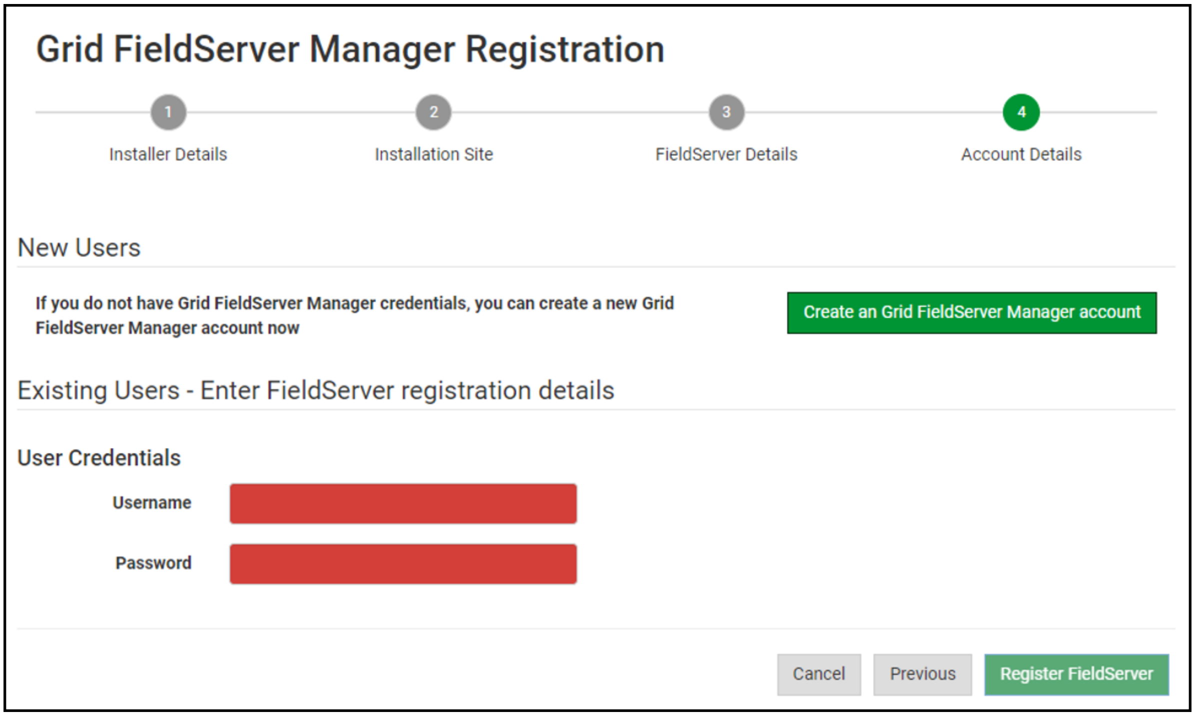
- Fill in the name, phone number, password fields and click the checkbox to agree to the privacy policy and terms of service.

**NOTE: If access to data logs using RESTful API is needed, do not include “#” in the password.**

- Click “Save” to save the user details.
- Click “OK” when the Success message appears.
- Record the email account used and password for future use.

### 9.3 Finish Registering the FieldServer

- Enter the new Username and Password set up in **Section 9.2 User Setup**.



Grid FieldServer Manager Registration

New Users

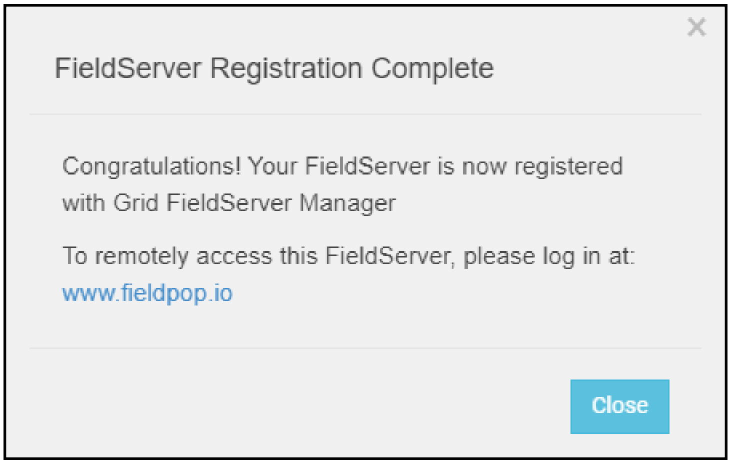
If you do not have Grid FieldServer Manager credentials, you can create a new Grid FieldServer Manager account now

Existing Users - Enter FieldServer registration details

User Credentials

Username [redacted]

Password [redacted]

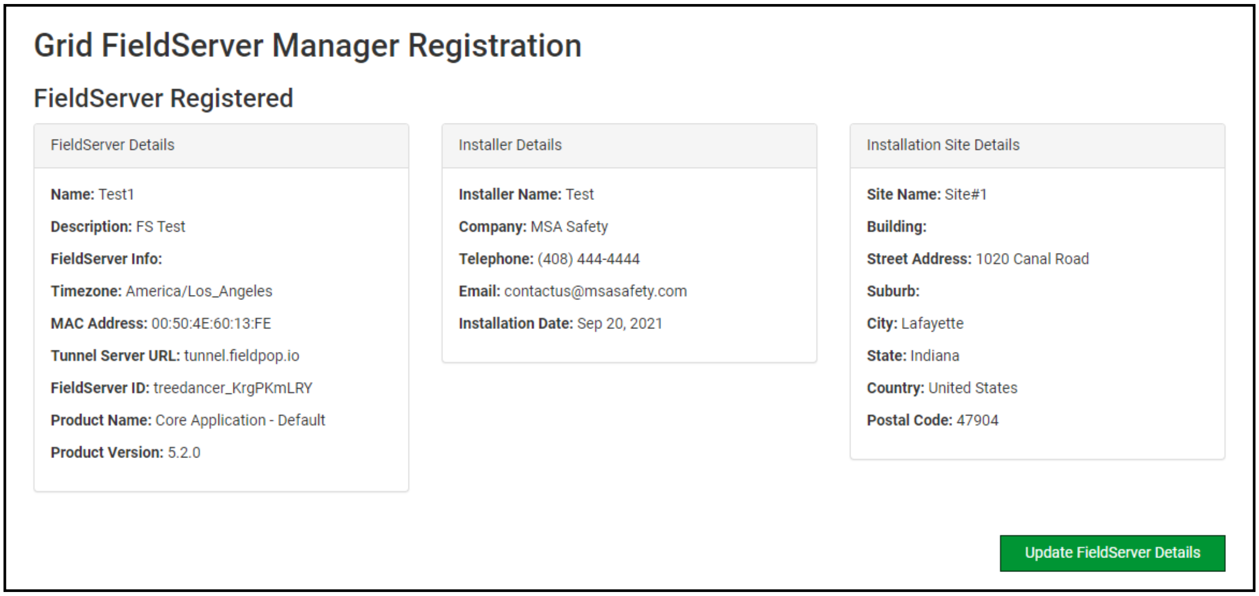


FieldServer Registration Complete

Congratulations! Your FieldServer is now registered with Grid FieldServer Manager

To remotely access this FieldServer, please log in at: www.fieldpop.io

- Once the device has successfully been registered, a confirmation window will appear. Click the Close button and the following screen will appear listing the device details and additional information auto-populated by the QuickServer.



Grid FieldServer Manager Registration

FieldServer Registered

FieldServer Details

**Name:** Test1

**Description:** FS Test

**FieldServer Info:**

**Timezone:** America/Los_Angeles

**MAC Address:** 00:50:4E:60:13:FE

**Tunnel Server URL:** tunnel.fieldpop.io

**FieldServer ID:** treedancer_KrgPKmLRY

**Product Name:** Core Application - Default

**Product Version:** 5.2.0

Installer Details

**Installer Name:** Test

**Company:** MSA Safety

**Telephone:** (408) 444-4444

**Email:** contactus@msasafety.com

**Installation Date:** Sep 20, 2021

Installation Site Details

**Site Name:** Site#1

**Building:**

**Street Address:** 1020 Canal Road

**Suburb:**

**City:** Lafayette

**State:** Indiana

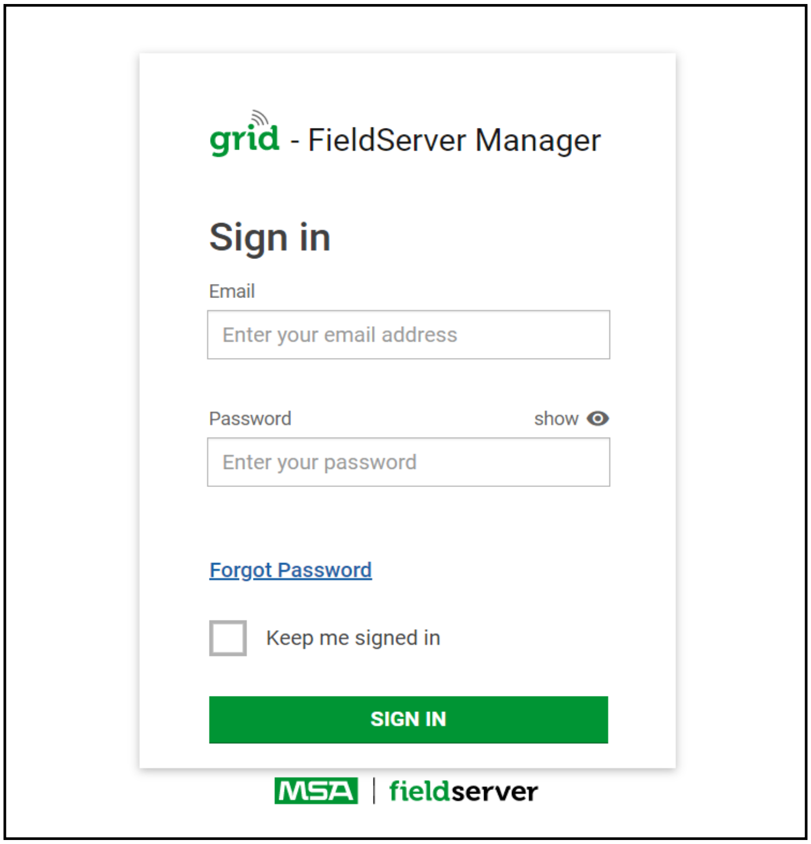
**Country:** United States

**Postal Code:** 47904

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

### 9.4 Login to the FieldServer Manager

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



grid - FieldServer Manager

Sign in

Email

Enter your email address

Password show

Enter your password

Forgot Password

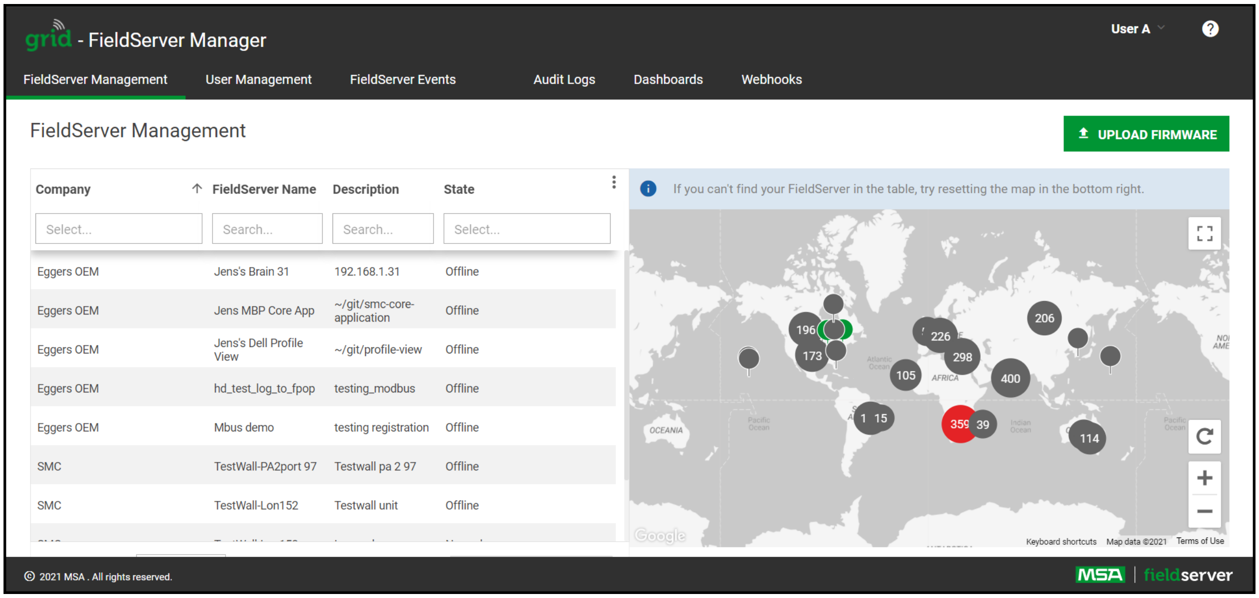
□ Keep me signed in

SIGN IN

MSA | fieldserver

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

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



grid - FieldServer Manager

FieldServer Management | User Management | FieldServer Events | Audit Logs | Dashboards | Webhooks

FieldServer Management

UPLOAD FIRMWARE

| Company | FieldServer Name | Description | State |
|---|---|---|---|
| Select... | Search... | Search... | Select... |
| Eggers OEM | Jens's Brain 31 | 192.168.1.31 | Offline |
| Eggers OEM | Jens MBP Core App | ~/git/smc-core-application | Offline |
| Eggers OEM | Jens's Dell Profile View | ~/git/profile-view | Offline |
| Eggers OEM | hd_test_log_to_fpop | testing_modbus | Offline |
| Eggers OEM | Mbus demo | testing registration | Offline |
| SMC | TestWall-PA2port 97 | Testwall pa 2 97 | Offline |
| SMC | TestWall-Lon152 | Testwall unit | Offline |

If you can't find your FieldServer in the table, try resetting the map in the bottom right.

© 2021 MSA . All rights reserved.

# 10 Troubleshooting

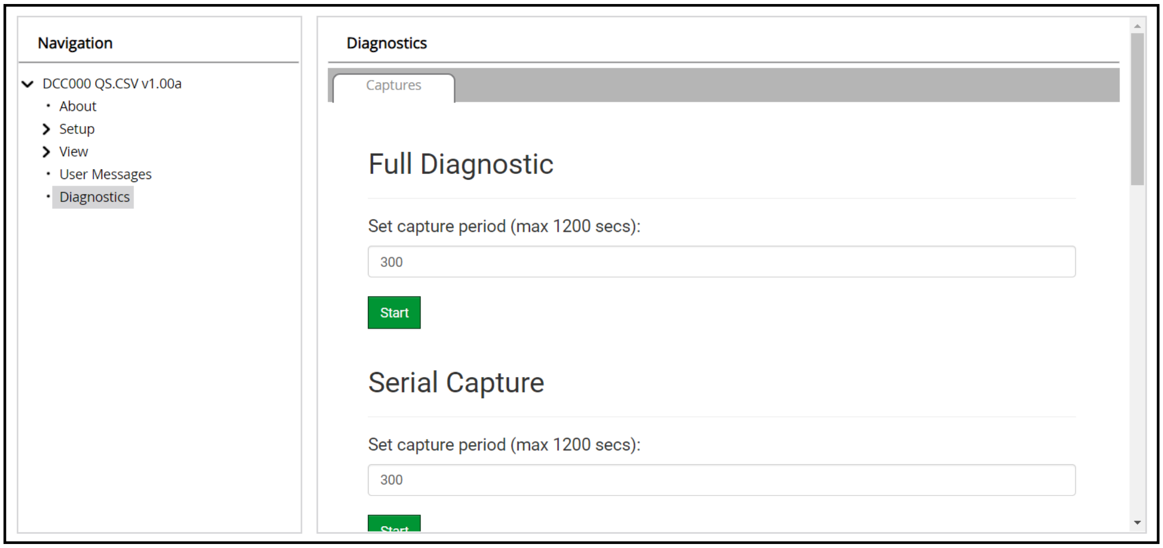
## 10.1 Communicating with the QuickServer Over the Network

- 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.X network.

## 10.2 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.**

- 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



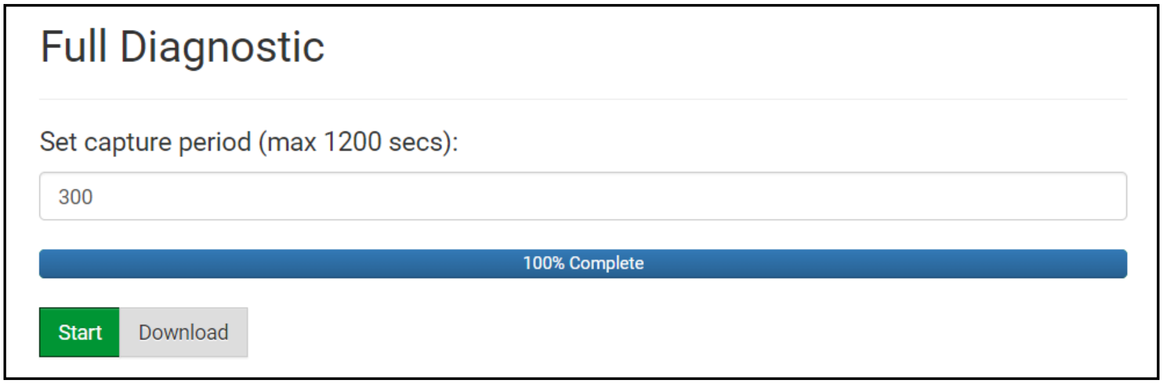
Full Diagnostic

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

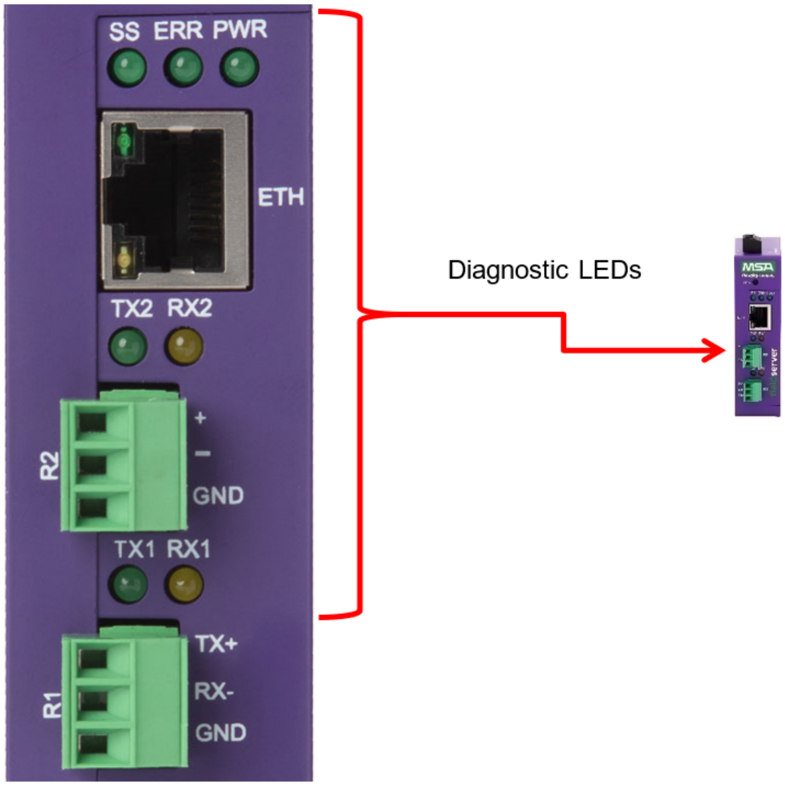
Set capture period (max 1200 secs): 300

100% Complete

- Click Download for the capture to be downloaded to the local PC.
- 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.**

### 10.3 LED Functions



| Tag | Description |
|---|---|
| **SS** | The SS LED will flash once a second to indicate that the bridge is in operation. |
| **ERR** | The SYS ERR LED will go on solid indicating there is a system error. If this occurs, immediately report the related "system error" shown in the error screen of the FS-GUI interface to support for evaluation. |
| **PWR** | 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. |

### 10.4 Factory Reset Instructions

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

### 10.5 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.**

# 11 Additional Information

## 11.1 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.

### 11.1.1 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
```

### 11.1.2 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 11.1.1 Configuring FieldServer as a SSL/TLS Server**.

**Certificate Validation Options**

Use the Check_Remote_Host element as described in **Section 11.1.1 Configuring FieldServer as a SSL/TLS Server**.

**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

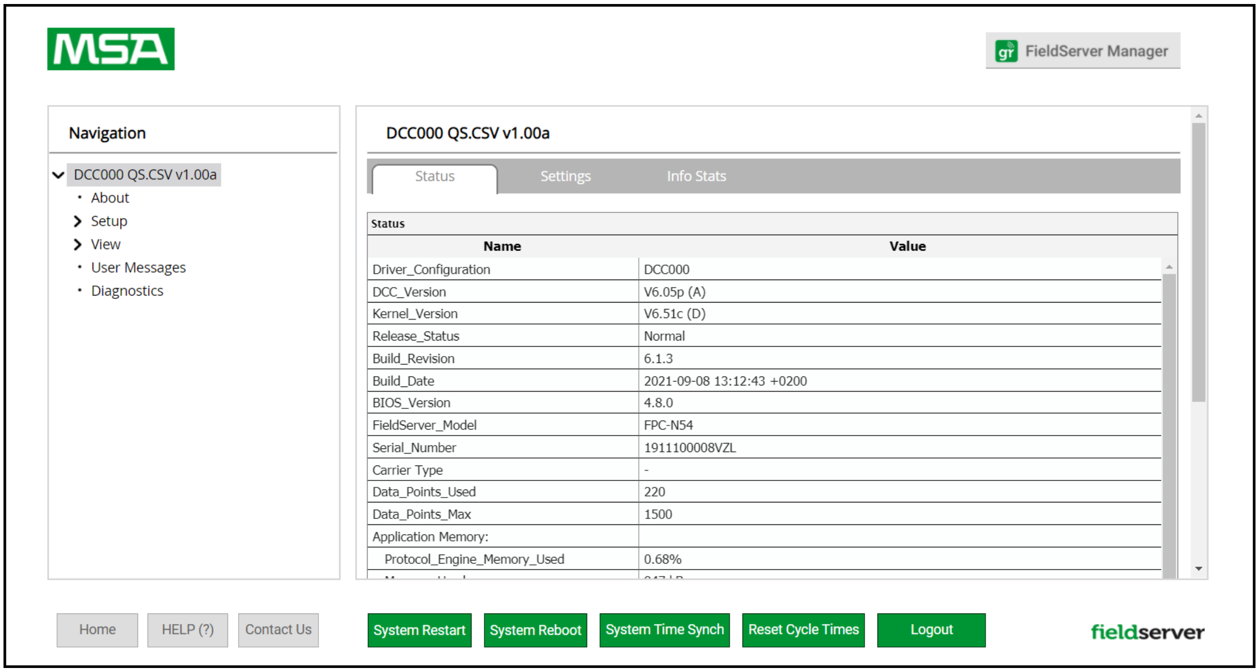
Configure the FieldServer to use a custom certificate as shown below:

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

## 11.2 Change Web Server Security Settings After Initial Setup

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

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



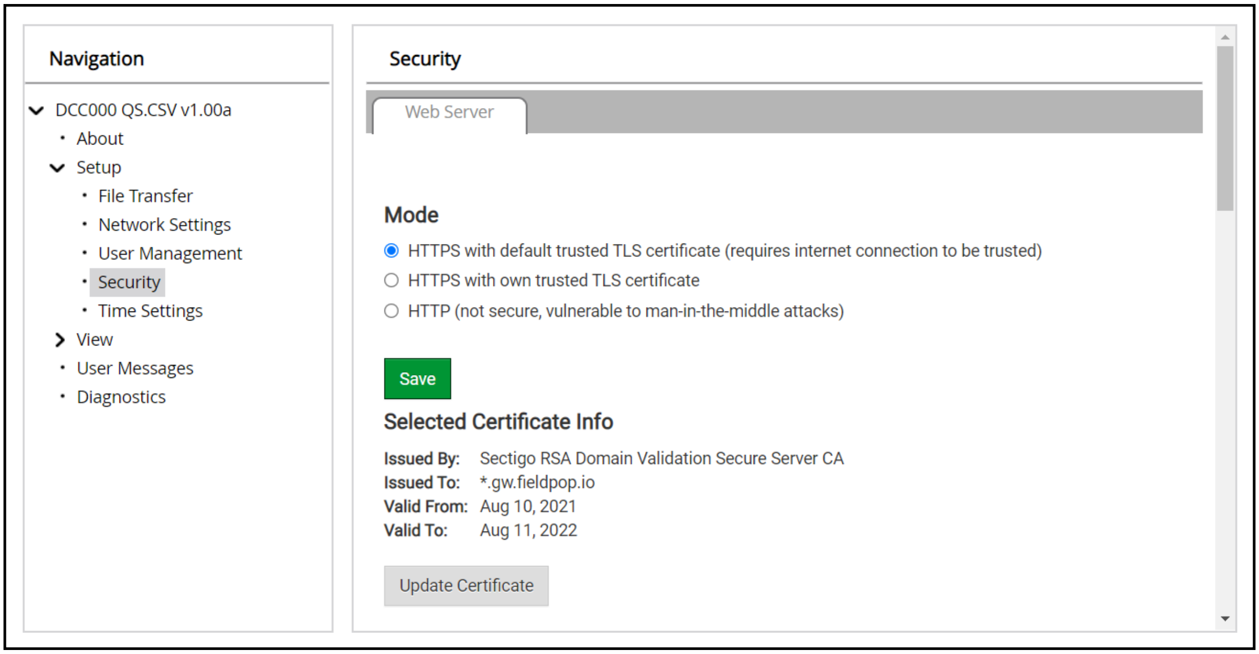
DCC000 QS.CSV v1.00a

Status

| Name | Value |
|---|---|
| Driver_Configuration | DCC000 |
| DCC_Version | V6.05p (A) |
| Kernel_Version | V6.51c (D) |
| Release_Status | Normal |
| Build_Revision | 6.1.3 |
| Build_Date | 2021-09-08 13:12:43 +0200 |
| BIOS_Version | 4.8.0 |
| FieldServer_Model | FPC-N54 |
| Serial_Number | 1911100008VZL |
| Carrier Type | - |
| Data_Points_Used | 220 |
| Data_Points_Max | 1500 |
| Application Memory: | |
| Protocol_Engine_Memory_Used | 0.68% |

### 11.2.1 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)

Selected Certificate Info

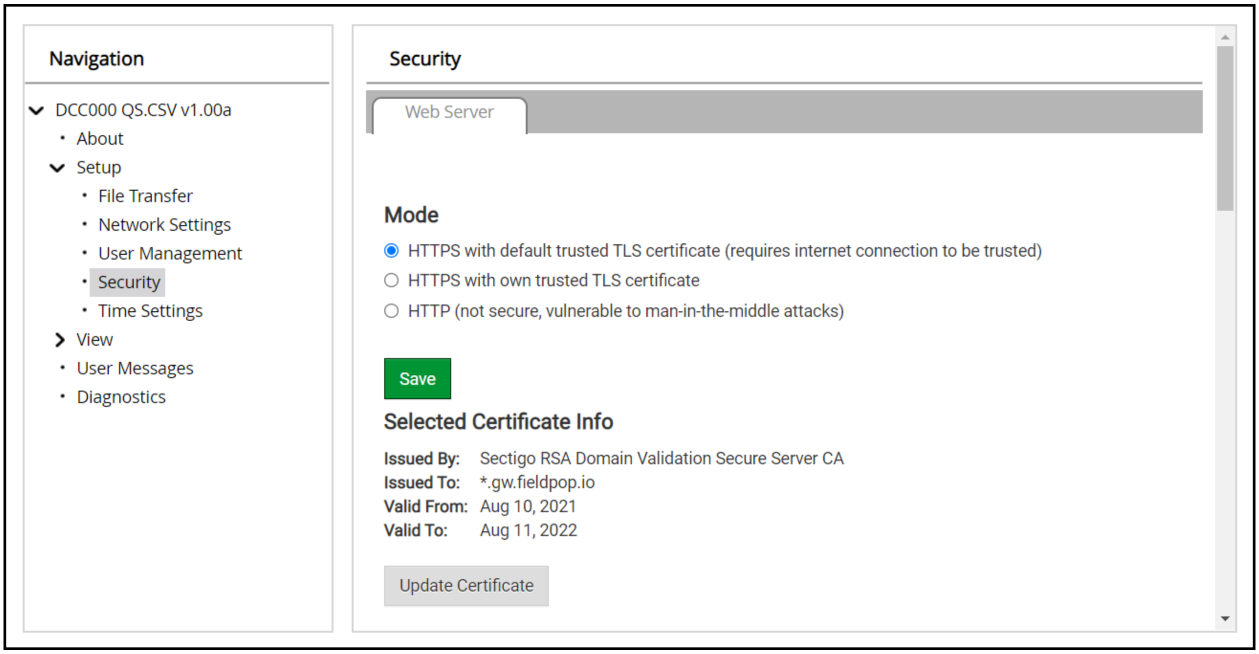
**Issued By:** Sectigo RSA Domain Validation Secure Server CA
**Issued To:** *.gw.fieldpop.io
**Valid From:** Aug 10, 2021
**Valid To:** Aug 11, 2022

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

### 11.2.2 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.



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)

Selected Certificate Info

**Issued By:** Sectigo RSA Domain Validation Secure Server CA
**Issued To:** *.gw.fieldpop.io
**Valid From:** Aug 10, 2021
**Valid To:** Aug 11, 2022

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

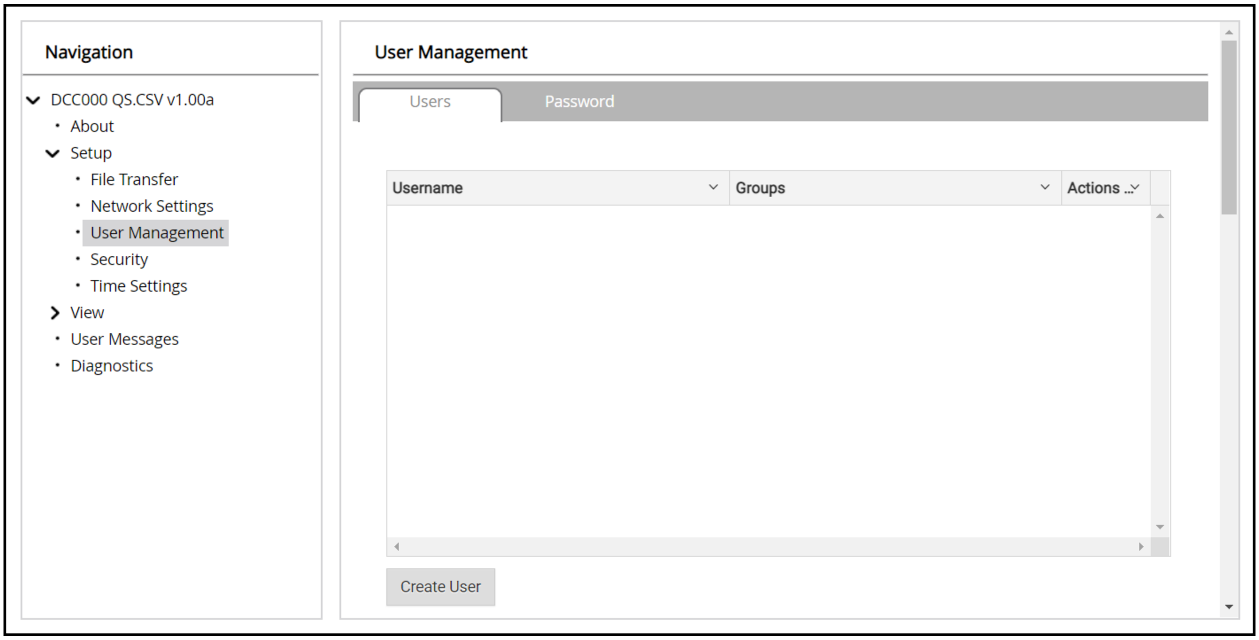
### 11.3 Change User Management Settings

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

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

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

- Check that the Users tab is selected.



User Types:

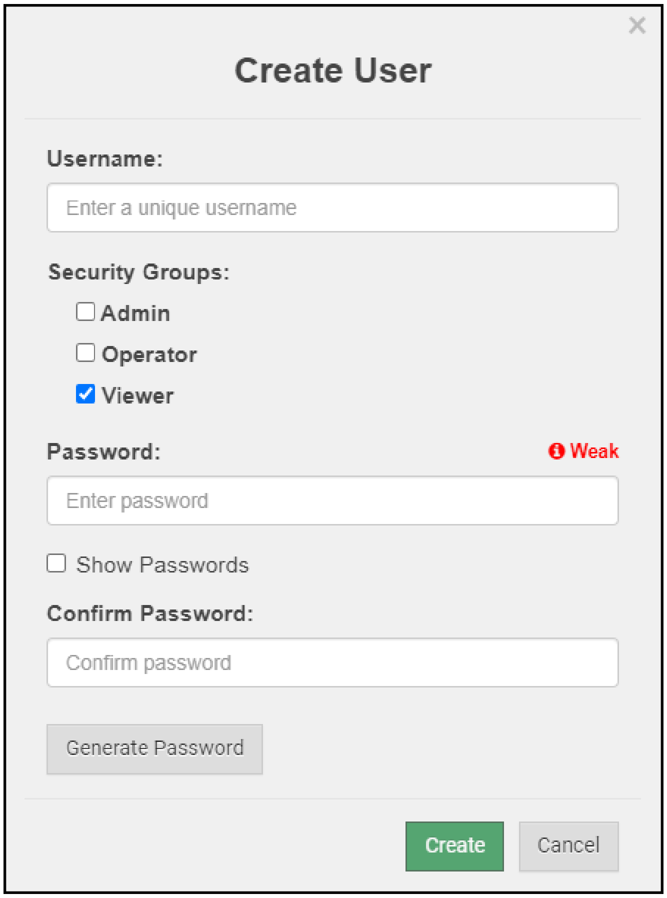
**Admin** – Can modify and view any settings on the FieldServer.

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

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

### 11.3.1 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

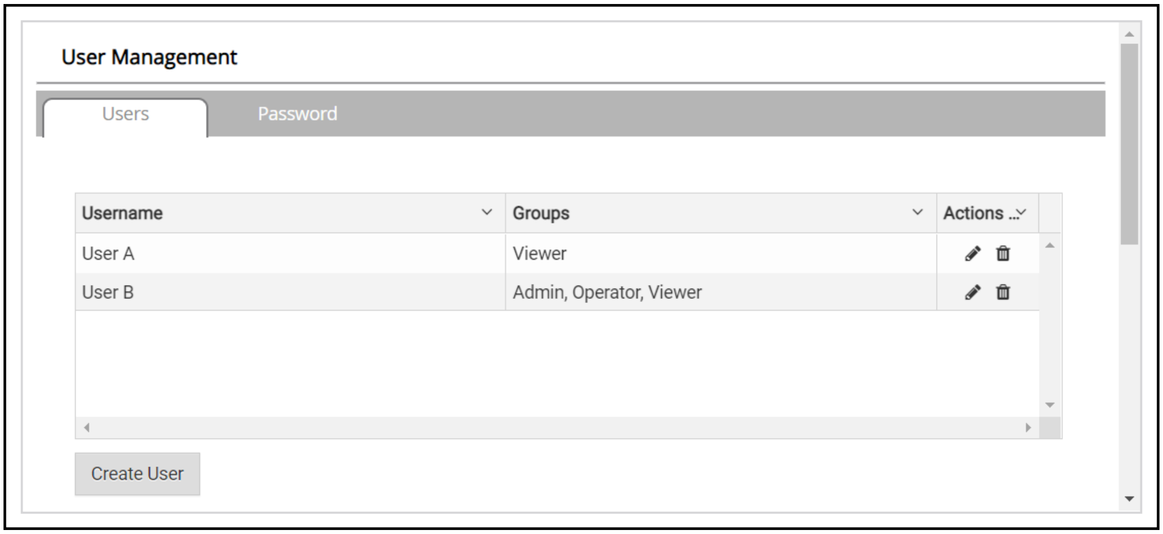
- Enter the new User fields: Name, Security Group and Password.
    - **User details are hashed and salted**

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

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

### 11.3.2 Edit Users

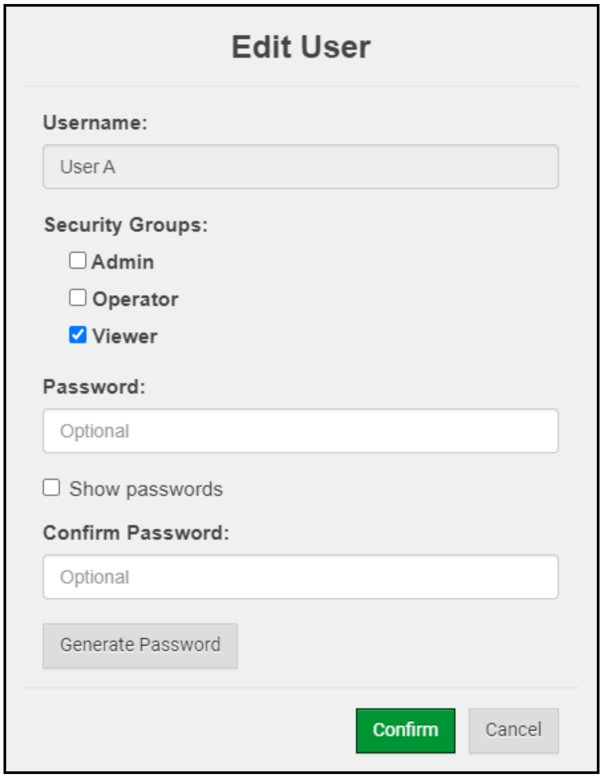
- Click the pencil icon next to the desired user to open the User Edit window.



User Management

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

- 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

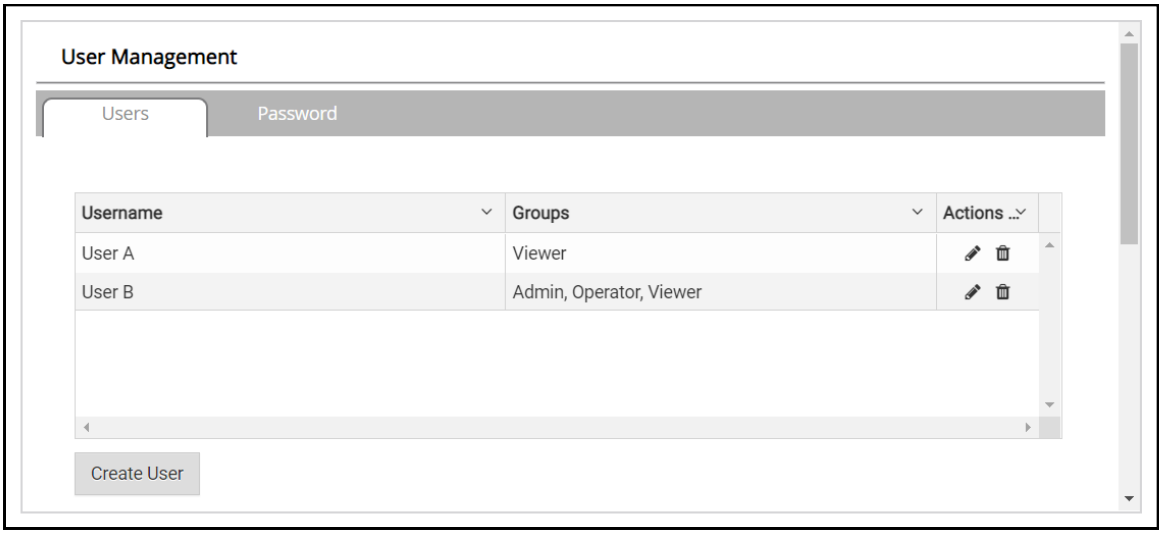
□ Show passwords

Confirm Password: Optional

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

### 11.3.3 Delete Users

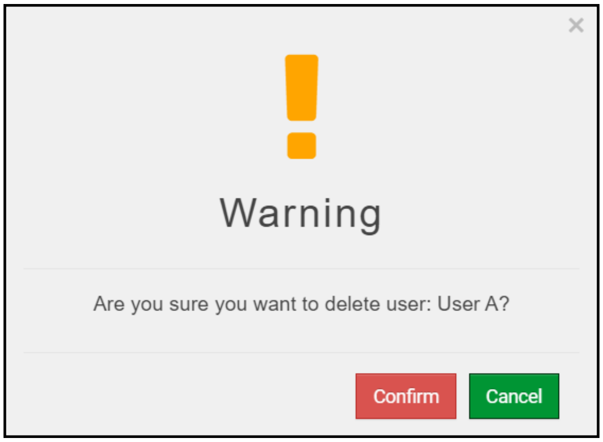
- Click the trash can icon next to the desired user to delete the entry.



User Management

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

- When the warning message appears, click Confirm.

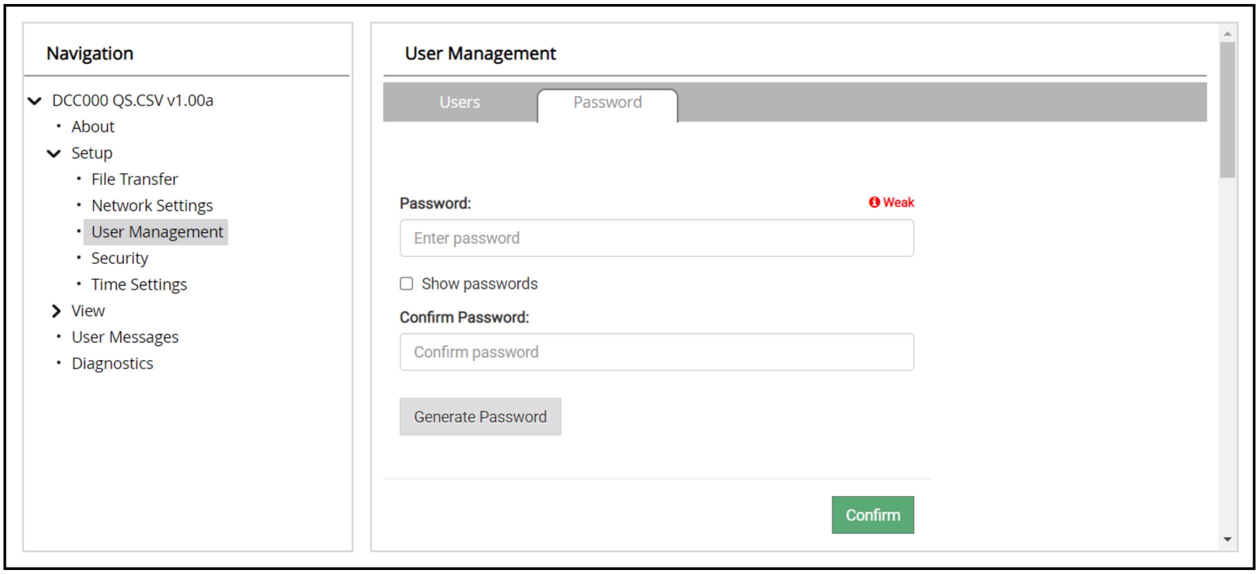


Warning

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

### 11.3.4 Change FieldServer Password

- Click the Password tab.



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

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

### 11.4 QuickServer Part Numbers

| QuickServer | Interface Connections | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | RS-232[1] | RS-485[2] | RS-422[3] | KNX[6] | RS-485 | M-Bus | Ethernet[4] | LonWorks[5] |
| 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.**

### 11.5 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 FieldServer
- Furthermore, the interconnecting power cable shall:
  - Be of length not exceeding 3.05m (118.3")
  - Be constructed of materials rated VW-1, FT-1 or better
- If the unit is to be installed in an operating environment with a temperature above 65 °C, it should be installed in a Restricted Access Area requiring a key or a special tool to gain access.
- This device must not be connected to a LAN segment with outdoor wiring.

### 11.6 Specifications

| | FS-QS-2XX0-XXXX |
|---|---|
| **Electrical Connections** | One 3-pin Phoenix connector with: RS-485/RS-232 (Tx+ / Rx- / gnd)<br>One 3-pin Phoenix connector with: RS-485 (+ / - / 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<br>*Max Power:* 3 Watts<br>*Current draw:* 24VAC 0.125A<br>9-30VDC 0.25A @12VDC |
| **Approvals** | CE and FCC Class B & C Part 15, UL 60950-1, WEEE compliant, IC Canada, RoHS3 compliant, REACH compliant, UKCA compliant |
| **Capacity Options** | FS-QS-20X0: 250 data points<br>FS-QS-22X0: 500 data points<br>FS-QS-21X0: 1,000 data points<br>FS-QS-23X0: 3,000 data points<br>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 |

“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.

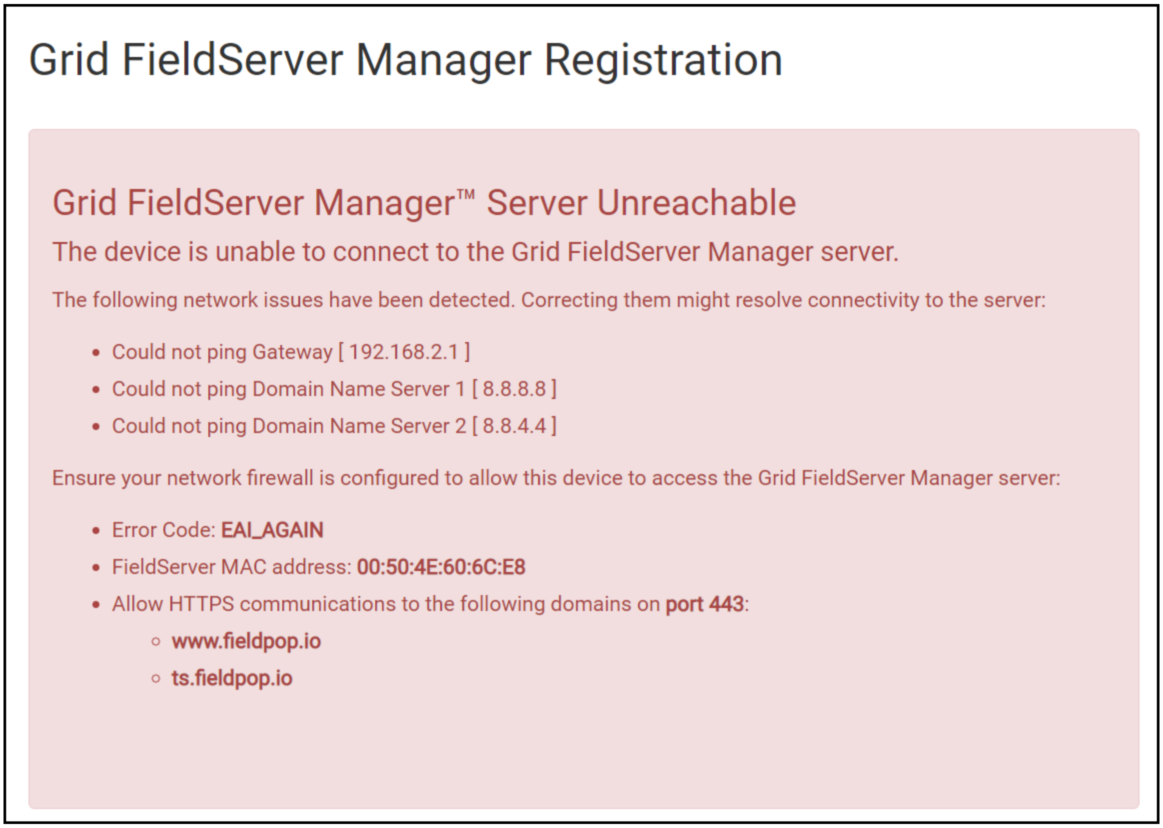
**NOTE:** This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment 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.”

**NOTE: Specifications subject to change without notice.**

### 11.7 FieldServer Manager Connection Warning Message

- If a warning message appears instead of the page as shown below, follow the suggestion that appears on screen.
  - If the FieldServer cannot reach the server, the following message will appear



Grid FieldServer Manager Registration

Grid FieldServer Manager™ Server Unreachable

The device is unable to connect to the Grid FieldServer Manager server.

The following network issues have been detected. Correcting them might resolve connectivity to the server:

- Could not ping Gateway [ 192.168.2.1 ]
- Could not ping Domain Name Server 1 [ 8.8.8.8 ]
- Could not ping Domain Name Server 2 [ 8.8.4.4 ]

Ensure your network firewall is configured to allow this device to access the Grid FieldServer Manager server:

- Error Code: **EAI_AGAIN**
- FieldServer MAC address: **00:50:4E:60:6C:E8**
- Allow HTTPS communications to the following domains on **port 443**:
  - **www.fieldpop.io**
  - **ts.fieldpop.io**

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

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

## 12 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.