



Operating Manual

QuickServer FS-QS-1XXX Start-up Guide



Revision: 3.G

Document No.: T18600

Print Spec: 10000005389 (F)



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.MSAafety.com

Contents

1	About the QuickServer	5
1.1	Certification	5
1.2	Supplied Equipment	5
2	Equipment Setup	6
2.1	Mounting	6
2.2	Physical Dimensions	7
2.2.1	Dimension Drawing FS-QS-1X10-XXXX	7
2.2.2	Dimension Drawing FS-QS-1XX1-XXXX	8
2.2.3	Dimension Drawing FS-QS-123X Models with RS-422	9
2.3	R2 Port Jumper Settings	10
2.3.1	RS-485 Port	10
2.3.2	M-Bus Port: Master/Slave Jumper	13
2.4	R1 Port Small DIP Switches	14
2.4.1	RS-485 Port	14
3	Installing the QuickServer	15
3.1	RS-485	15
3.1.1	RS-485 Connection R2 Port	15
3.1.2	RS-485 Connection R1 Port	15
3.2	QuickServer LonWorks (FS-QS-1XX1-XXXX)	16
3.3	QuickServer KNX (FS-QS-124X-XXXX)	16
3.4	RS-232 Connection R2 Port (Only Available on FS-QS-122X Models)	17
4	Operation	18
4.1	Power Up the Device	18
4.2	Connect the PC to the QuickServer Over the Ethernet Port	18
5	Connecting to the QuickServer	19
5.1	Using the FieldServer Toolbox to Discover and Connect to the QuickServer	19
5.2	Using a Web Browser	19
6	Setup Web Server Security	20
6.1	Login to the FieldServer	20
6.2	Select the Security Mode	22
6.2.1	HTTPS with Own Trusted TLS Certificate	23
6.2.2	HTTPS with Default Untrusted Self-Signed TLS Certificate or HTTP with Built-in Payload Encryption	23
7	Setup Network	24
7.1	Using FS-GUI to Input Network Settings	25
7.2	Routing Settings	26
7.3	Ethernet 1 Network Settings	27
8	Configuring the QuickServer	28
8.1	Retrieve the Sample Configuration File	28
8.2	Change the Configuration File to Meet the Application	28
8.3	Load the Updated Configuration File	29
8.3.1	Using the FS-GUI to Load a Configuration File	29

8.3.2	Retrieve the Configuration File for Modification or Backup	30
8.4	Test and Commission the QuickServer	31
8.4.1	Accessing the FieldServer Manager	31
9	MSA Grid - FieldSever Manager Setup	32
9.1	Registration Process	32
9.2	User Setup	35
9.3	Finish Registering the FieldServer	37
9.4	Login to the FieldServer Manager	39
10	Additional Model Connection Ports	41
10.1	RS-422 Connection R2 Port	41
10.1.1	Connection and Operation via the RS-422 Port	42
10.2	KNX Connection R2 Port	43
10.3	M-Bus Connection R2 Port	44
11	Troubleshooting	45
11.1	Communicating with the QuickServer Over the Network	45
11.2	Taking a FieldServer Diagnostic Capture	46
11.3	LED Functions	47
11.4	Internet Browser Software Support	48
12	Additional Information	49
12.1	SSL/TLS for Secure Connection	49
12.1.1	Configuring FieldServer as a SSL/TLS Server	49
12.1.2	Configuring FieldServer as SSL/TLS Client	52
12.2	Change Web Server Security Settings After Initial Setup	53
12.2.1	Change Security Mode	54
12.2.2	Edit the Certificate Loaded onto the FieldServer	55
12.3	Change User Management Settings	56
12.3.1	Create Users	57
12.3.2	Edit Users	58
12.3.3	Delete Users	59
12.3.4	Change FieldServer Password	60
12.4	QuickServer FS-QS-101X DCC	61
12.5	QuickServer Part Numbers	62
12.6	Compliance with UL Regulations	63
12.7	Specifications	64
12.8	FieldServer Manager Connection Warning Message	65
13	Limited 2 Year Warranty	66

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 11 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 - FieldServer Manager Setup** for further information.

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.*

LonMark Certification



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

1.2 Supplied Equipment

FieldServer Gateway

- Preloaded with two selected drivers. A sample configuration file is also loaded.

NOTE: On the FS-QS-1X11 and FS-QS-12X1 one of those drivers is LonWorks.

- 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 following mounting options are available:

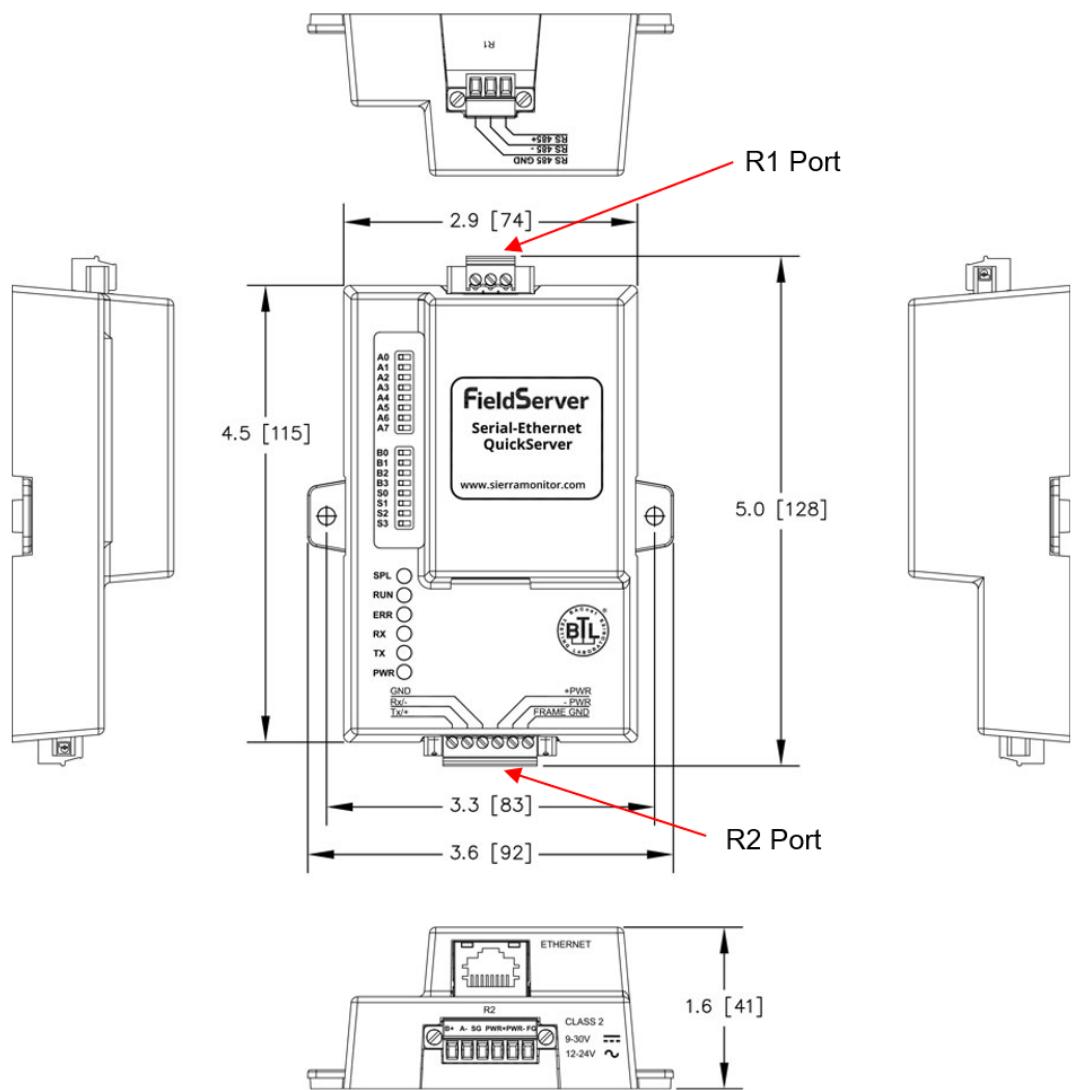
- Product comes with tabs for wall or surface mount. These can be snapped off if not required.
- DIN rail mounting bracket – Included in the accessory kit or ordered separately (part # FS-8915-35-QS).



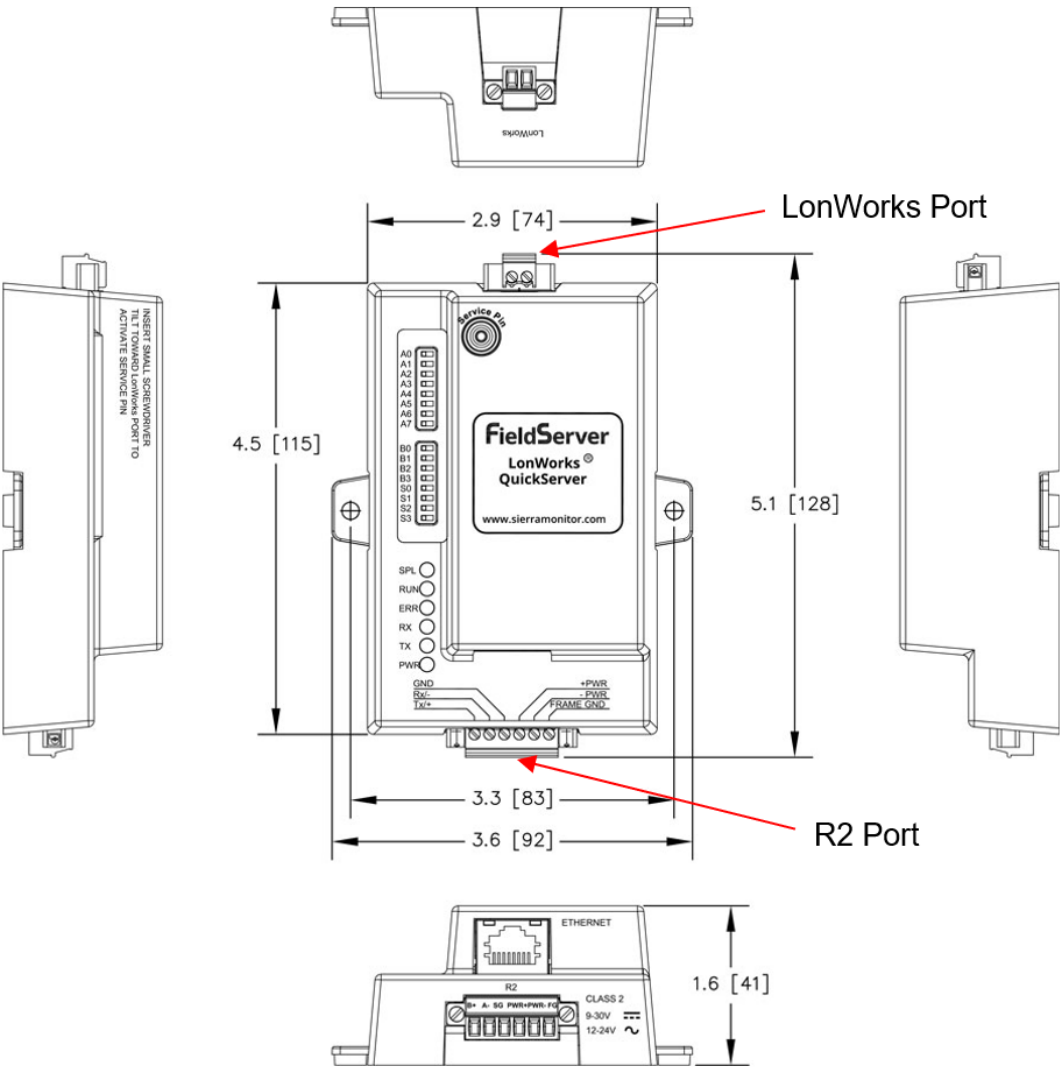
WARNING: Install only as instructed, failure to follow the installation guidelines or using screws without the DIN rail mounting bracket could result in permanent damage to the product. If the FieldServer is removed from the DIN rail, use the original screws to reattach. Only screws supplied by MSA Safety should be used in the holes found on the back of the unit when attaching the optional DIN Rail bracket. **USE OF ANY OTHER SCREWS MAY DAMAGE THE UNIT.**

2.2 Physical Dimensions

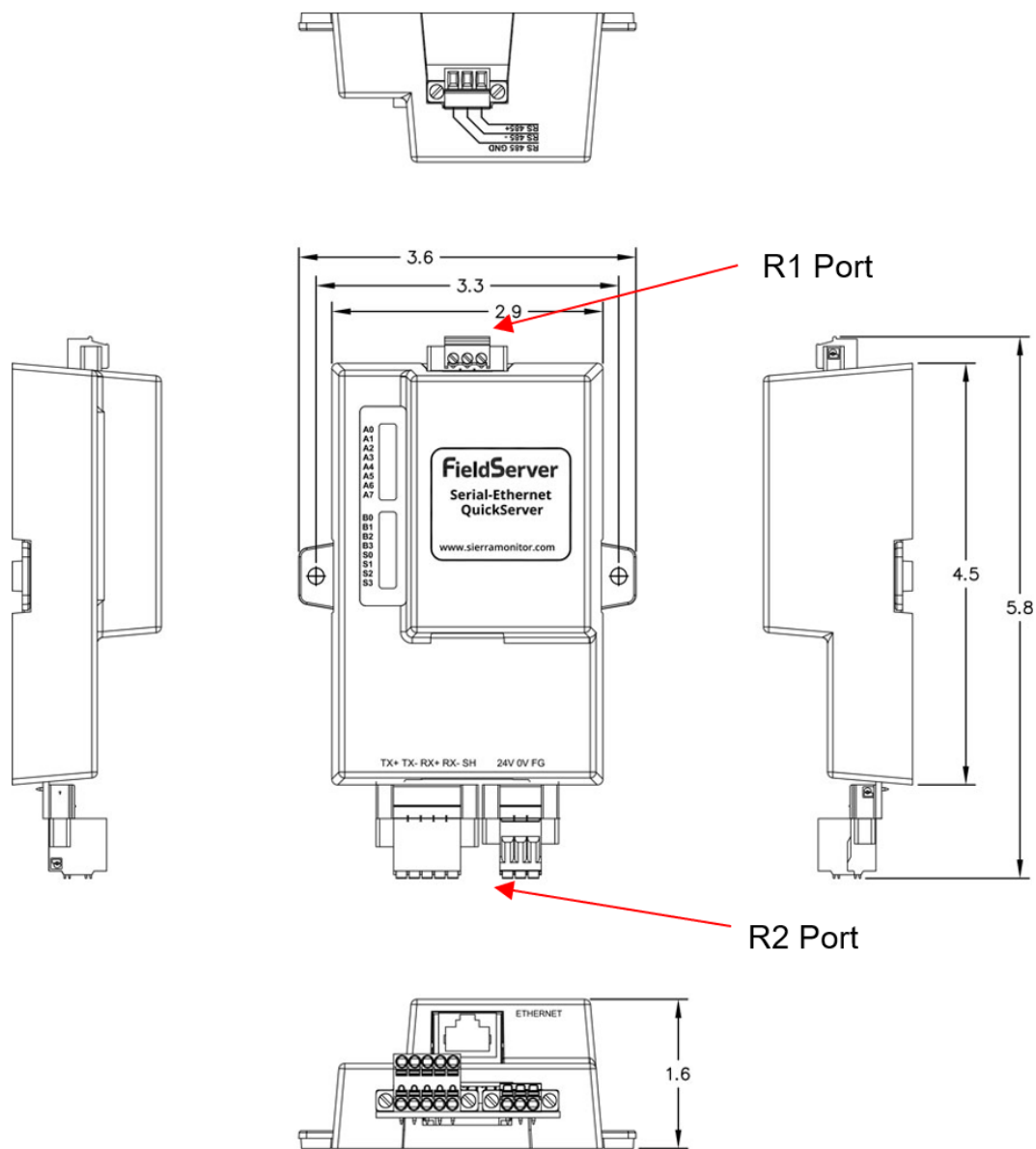
2.2.1 Dimension Drawing FS-QS-1X10-XXXX



2.2.2 Dimension Drawing FS-QS-1XX1-XXXX



2.2.3 Dimension Drawing FS-QS-123X Models with RS-422



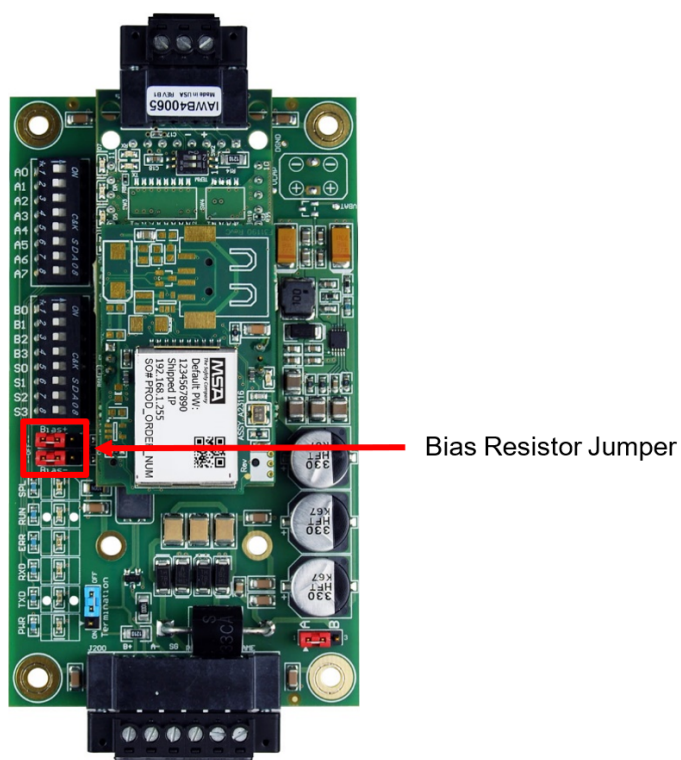
2.3 R2 Port Jumper Settings

Gently remove the QuickServer enclosure to access the jumpers on the unit.

2.3.1 RS-485 Port

NOTE: The following Sections only apply to QuickServer models: FS-QS-1011 and FS-QS-1211.

Bias Resistors

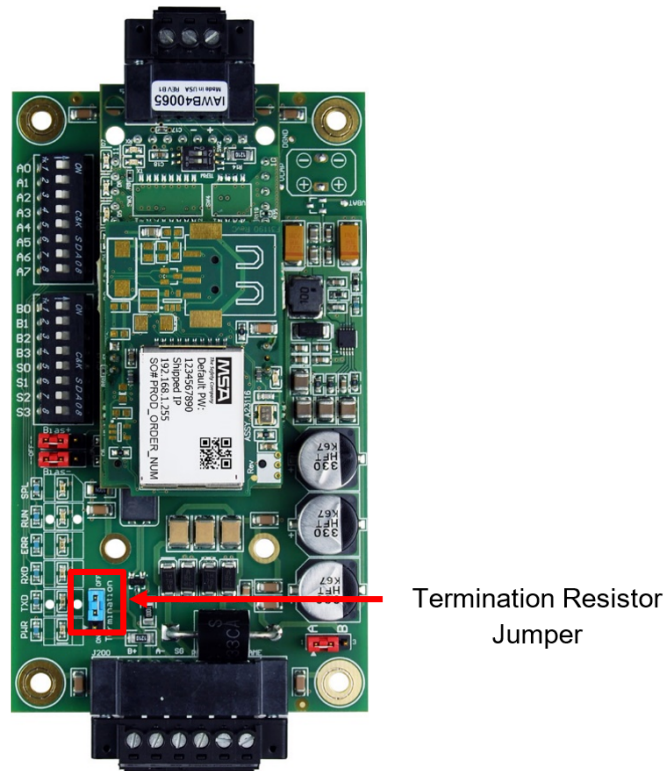


The QuickServer bias resistors are used to keep the RS-485 bus to a known state, when there is no transmission on the line (bus is idling), to help prevent false bits of data from being detected. The bias resistors typically pull one line high and the other low - far away from the decision point of the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

In the RS-485 carrier, 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 (on the field port where there are very weak bias resistors of 100k). Since there are no jumpers, many FieldServers can be put on network without running into the bias resistor limit which is < 500 ohms.

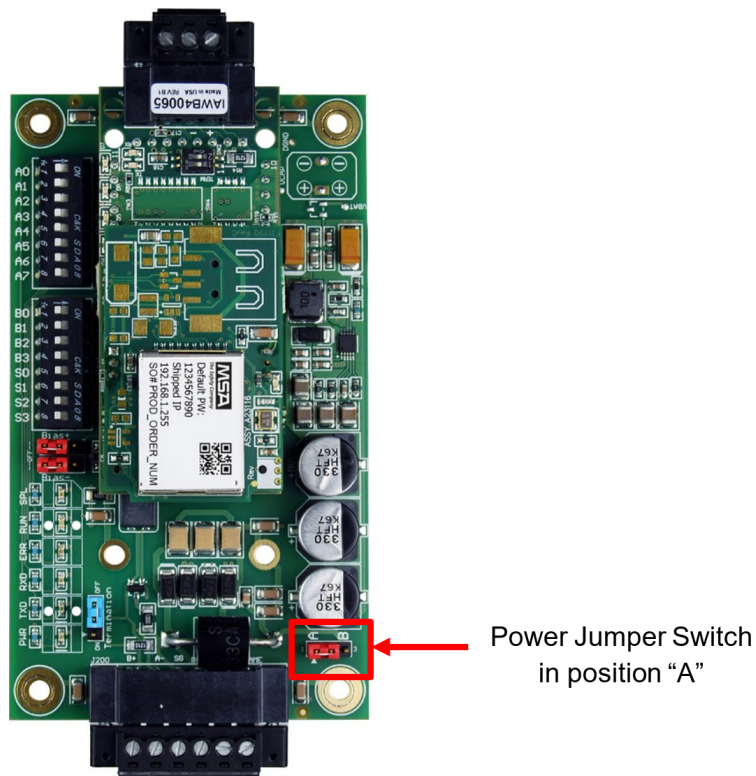
NOTE: See www.ni.com/support/serial/resinfo.htm for additional pictures and notes.

Termination Resistor



Termination resistors are also used to reduce noise. These pull the two lines of an idle bus together. However, they would override the effect of any bias resistors, if connected.

Power Jumper Settings



The QuickServer Carrier Board power jumper is set to position A by default but can be changed to position B for other power supply requirements.

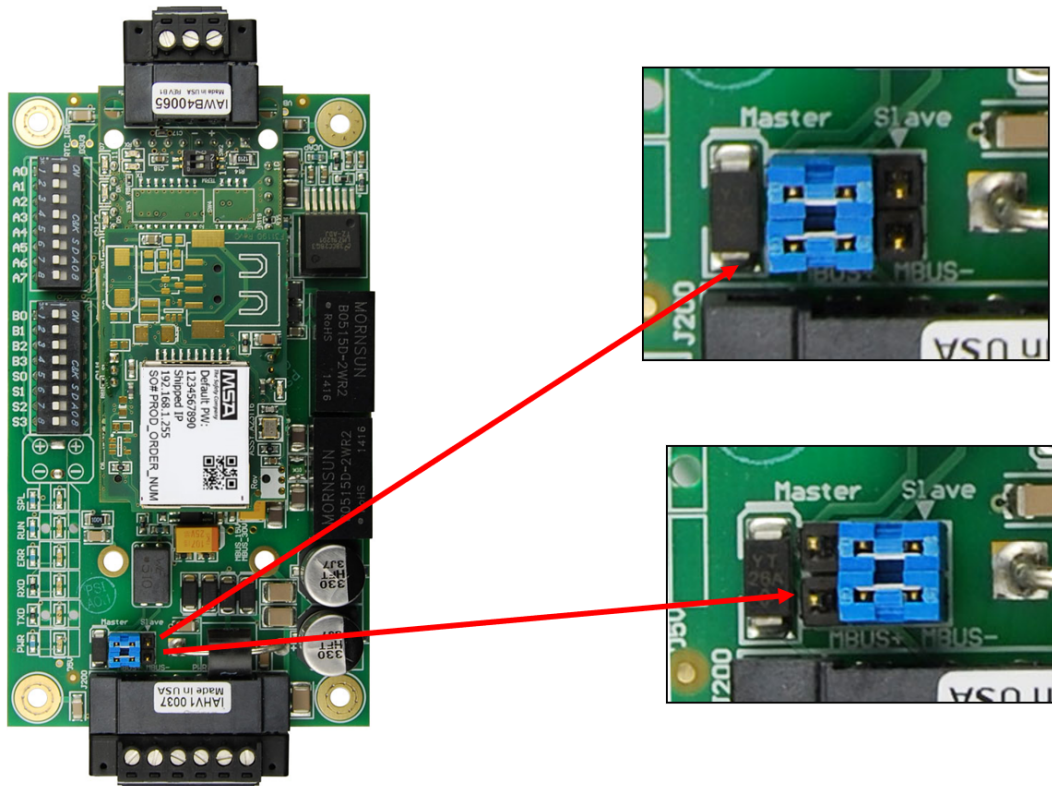
Position A: The Carrier makes use of a full-wave rectifying bridge. Can be used for 12-24VAC input or 9 – 30VDC input. At 9VDC this becomes marginal.

Position B: The Carrier makes use of a half-wave rectifying bridge. Best position for grounded AC transformers and for using DC voltage down to 9VDC.

2.3.2 M-Bus Port: Master/Slave Jumper

NOTE: The following only applies to models: FS-QS-1A50, FS-QS-1A51, FS-QS-1B51, FS-QS-1B51, FS-QS-1C51 and FS-QS-1C51.

The Master/Slave jumper is used to set the M-Bus hardware as a Master or Slave device (indicated by the labels on the board).

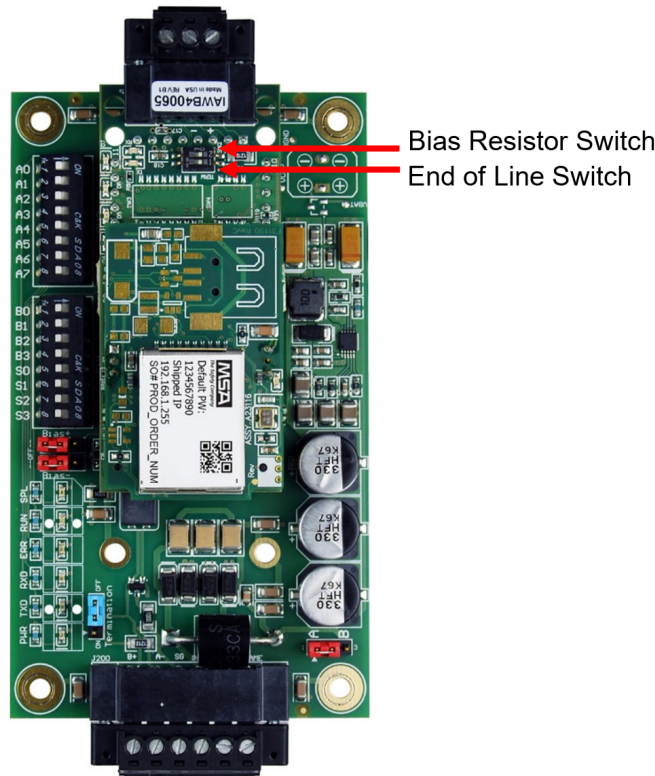


2.4 R1 Port Small DIP Switches

Gently remove the QuickServer enclosure to access the small DIP switches for the R1 Port.

2.4.1 RS-485 Port

NOTE: The following only applies to QuickServer models FS-QS-1XX0 or all non-LonWorks models.



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

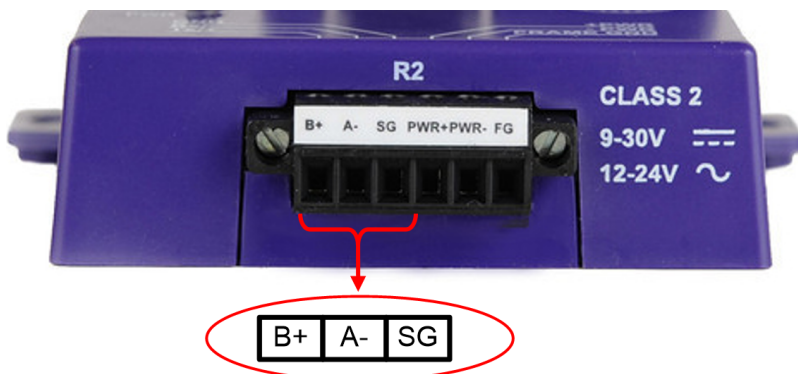
NOTE: Biasing only needs to be enabled on one device. The QuickServer has 510-ohm resistors that are used to set the biasing.

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

3 Installing the QuickServer

3.1 RS-485

3.1.1 RS-485 Connection R2 Port



Connect to the 3 pins on the left-hand-side of the 6-pin connector as shown.

The following Baud Rates are supported on the R2 Port:

4800, 9600, 19200, 38400, 57600, 115200

For connection details to RS-232 or RS-422, refer to **Section 10.1 RS-422 Connection R2 Port**.

3.1.2 RS-485 Connection R1 Port

NOTE: The following only applies to non-LonWorks QuickServers with an RS-485 R1 port.

Connect to the 3-pin connector as shown.

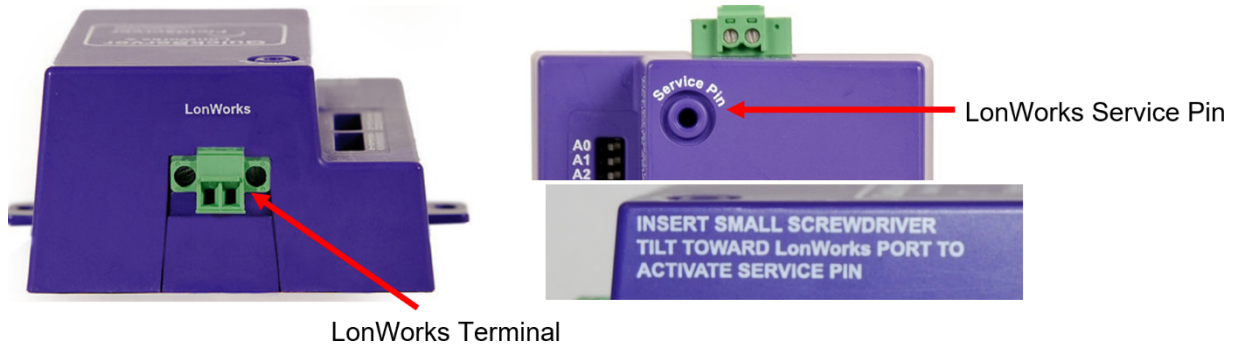


The following Baud Rates are supported on the R1 Port:

110, 300, 600, 1200, 2400, 4800, 9600, 19200, 20833, 28800, 38400, 57600, 76800, 115200

3.2 QuickServer LonWorks (FS-QS-1XX1-XXXX)

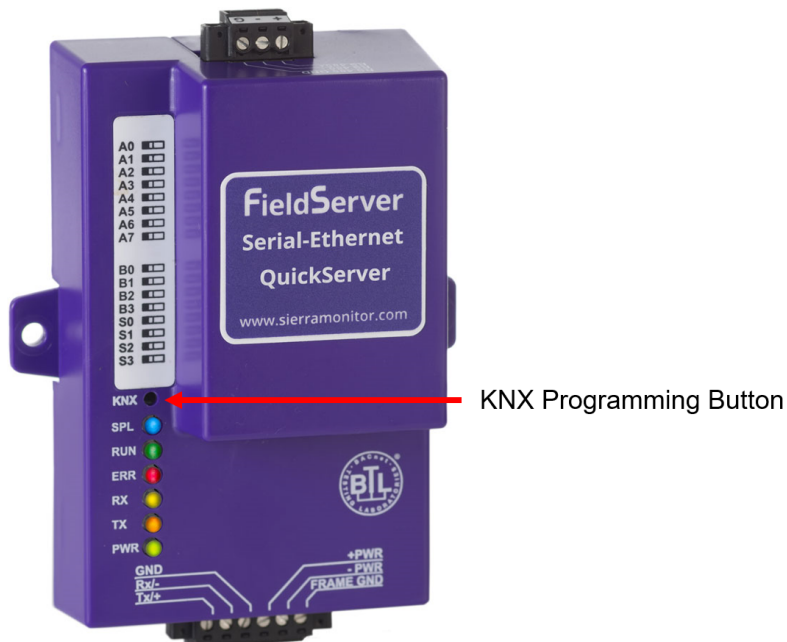
Connect the QuickServer to the LonWorks terminal using a twisted pair non-shielded cable.



To commission the QuickServer LonWorks port, insert a small screwdriver in the commissioning hole on the face of the QuickServer's enclosure to access the Service Pin. See the instructions on the QuickServer as to which way to toggle the screwdriver during commissioning.

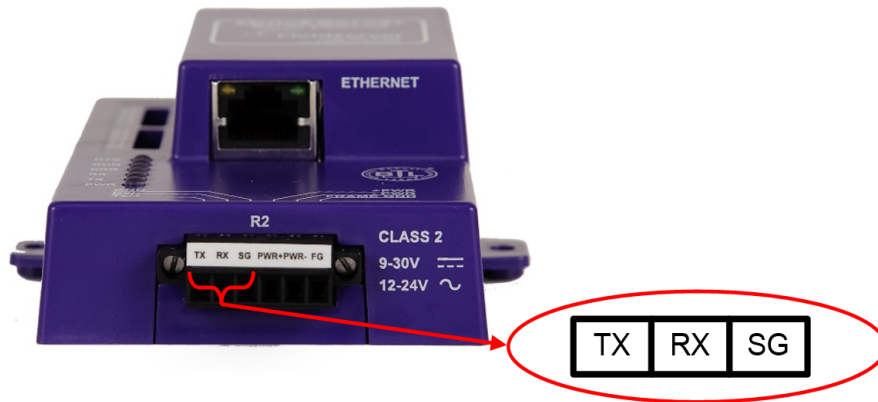
3.3 QuickServer KNX (FS-QS-124X-XXXX)

Connect the QuickServer to the KNX bus using the standard KNX twisted pair cable.



To commission the QuickServer as a KNX device in ETS Software, insert a small pin into the KNX commissioning hole on the face of the QuickServer to access the button.

3.4 RS-232 Connection R2 Port (Only Available on FS-QS-122X Models)



Refer to **Section 10 Additional Model Connection Ports** for further hardware connection options.

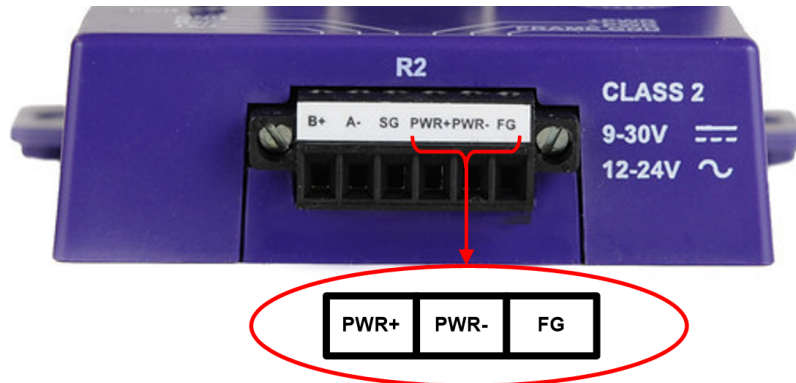
The following Baud Rates are supported on the R2 Port:

4800, 9600, 19200, 38400, 57600, 115200

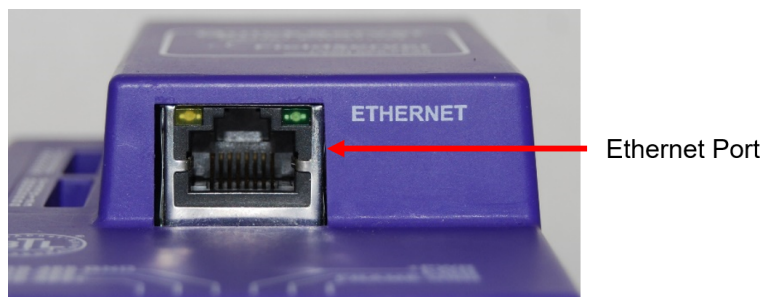
4 Operation

4.1 Power Up the Device

Apply power to the device. Ensure that the power supply used complies with the specifications provided. Ensure that the cable is grounded using the “Frame GND” terminal. The QuickServer is factory set for 9-30V DC or 12-24V AC.



4.2 Connect the PC to the QuickServer Over the Ethernet Port



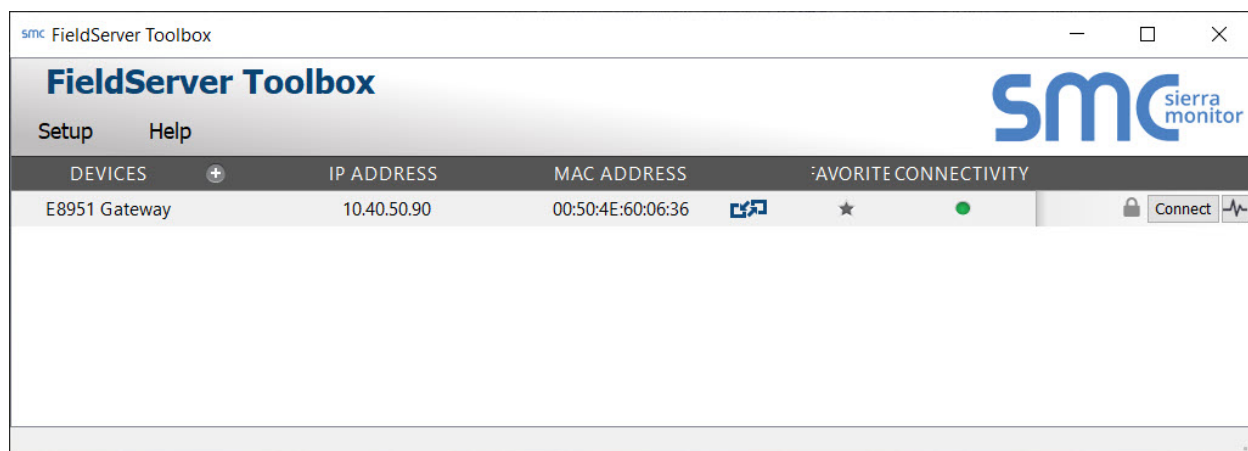
- Connect an Ethernet cable between the PC and QuickServer or connect the QuickServer and the PC to the switch using a straight Cat-5 cable.
- The Default IP Address of the QuickServer is **192.168.2.101**, Subnet Mask is **255.255.255.0**.

5 Connecting to the QuickServer

5.1 Using the FieldServer Toolbox to Discover and Connect to the QuickServer

- Install the Toolbox application from the USB drive or download it from the MSA Safety website.
- Use the FS Toolbox application to find the QuickServer and launch the FS-GUI.

NOTE: If the connect button is greyed out, the QuickServer's IP Address must be set to be on the same network as the PC. (Section [5.2 Using a Web Browser](#))



5.2 Using a Web Browser

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

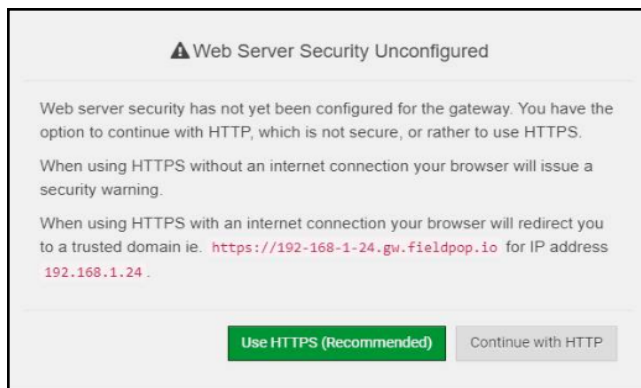
NOTE: Check Section [11.4 Internet Browser Software Support](#) for supported browsers.

6 Setup Web Server Security

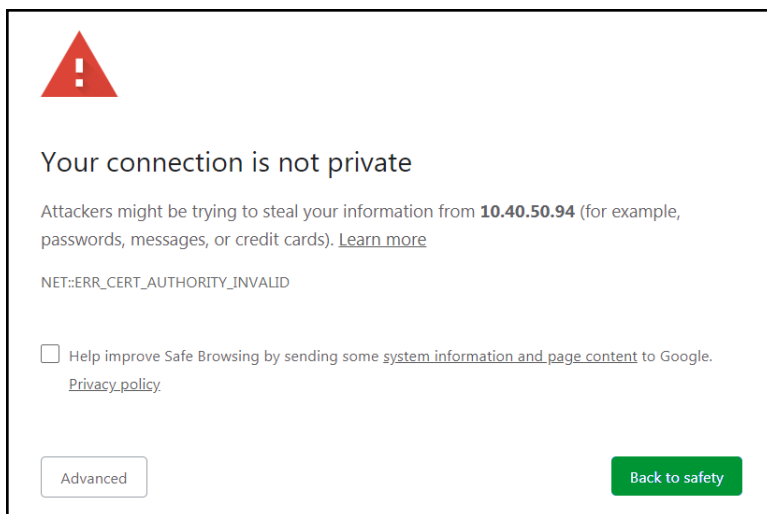
6.1 Login to the FieldServer

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

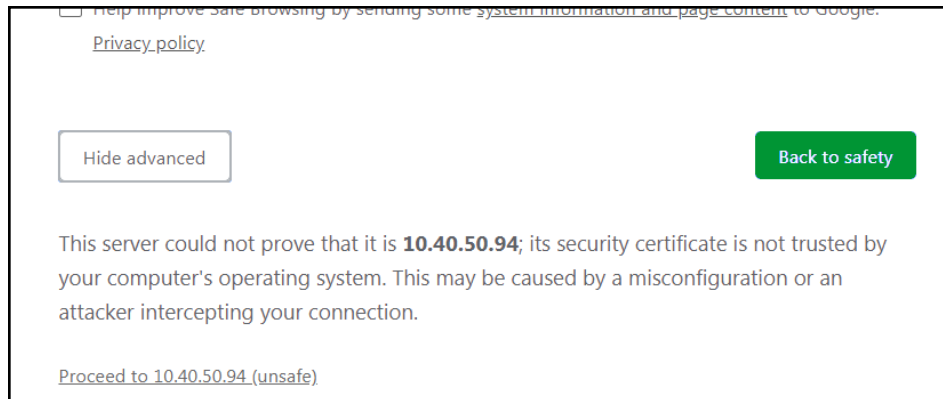
- When the Web Server Security Unconfigured window appears, read the text and choose whether to move forward with HTTPS or HTTP.



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

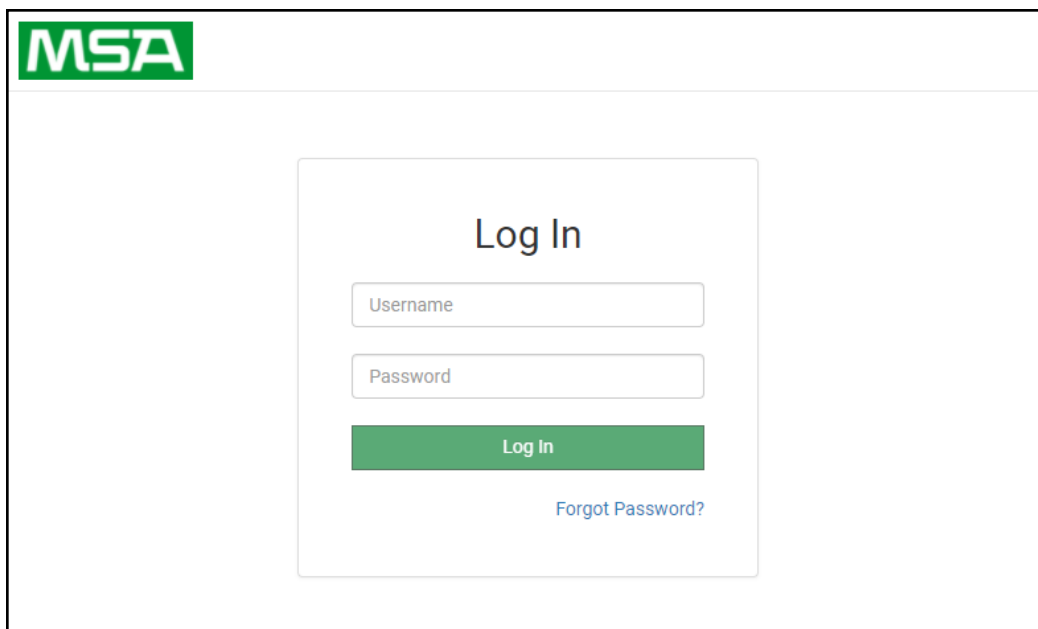


- Additional text will expand below the warning, click the underlined text to go to the IP Address. In the example below this text is “[Proceed to 10.40.50.94 \(unsafe\)](#)”.



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

NOTE: 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 [12.3 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)

Save

NOTE: Cookies are used for authentication.

NOTE: To change the web server security mode after initial setup, go to [Section 12.2 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
A4lBAQBFM+IPvOx3T/47VEmaiXqE3bx3zEuBFJ6pWPlw7LHf2r2ZoHw+9xb+aNMU
dVYAelhBMTMsn2ERvQVp0xj3psSv2EJyKXS1bOYNRLsq7UzpwuAdT/Wy3o6vUM5
K+Cwf9qEoQ0LuxDZTIECt67MkcHMiuFi5pk7TRicHnQF/sfOAYOulduHOy9exlk9
FmHfVDIZt/cJUaF+e74EuSph+qEr0lQo2wvmhyc7L22UXse1NoOfU2Zg0Eu1VWtu
JRryaMWIRFEWuuzMGZtKFWVC+8q2JQsVcgrWm7naoblEhOCMH+sKHJMCxDoXGt
vtZjpZUoAL51YXxWSVcyZdGiAP5e
-----END CERTIFICATE-----
```

Private Key

```
sHB0zZoHr4YQSDk2BbYVzbl0LDuKtc8+JiO3ooGjoTuHnqkeAj/fKfbTAsKeAzW
gKQe+H5UQNk0bdvZfOJrm6daDK2vVDmR5k+jUUhEj5N49uplroB97MQgYotzqfT+
THlbpq5t1SIK617k04ObKmHF5l8fck+ru545sVmpeeZh0m5j5SURYAZMvbq5daCu
J4l5NIihbEvxRF4UK41ZDMCvujopCbkUWrb1a/3XXnDnM2K9xyz2wze998D6Wk46
+7aOFY9F+7j5lmmkoS3GYtwCyH5jP+mPP1K6RnuiD019wvGPb4dtN/RTnfd0eF
GYeVSkI9fxkxDOFtdWRZbM/rPin4tmO1Xf8HqONVN1x/iaMynOXG4cukoi4+VO
u0rZaUESlI2zNkfrn7fAASm5NBWg202Cy9lAYnuujs3aALl5uGBEEKa62oTMxlzx
-----END RSA PRIVATE KEY-----
```

Private Key Passphrase

Save

- 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.

The screenshot displays the MSA FieldServer Manager web interface. The top left features the MSA logo. The top right shows the 'gr FieldServer Manager' header. On the left, a 'Navigation' sidebar lists options: 'DCC000 QS.CSV v1.00a' (selected), 'About', 'Setup', 'View', 'User Messages', and 'Diagnostics'. The main content area is titled 'DCC000 QS.CSV v1.00a' and has tabs for 'Status', 'Settings', and 'Info Stats'. The 'Status' tab is active, showing a table of system parameters.

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

At the bottom of the interface, there are buttons for 'Home', 'HELP (?)', 'Contact Us', 'System Restart', 'System Reboot', 'System Time Synchron', 'Reset Cycle Times', and 'Logout'. The 'fieldserver' logo is also present in the bottom right corner.

NOTE: The FieldServer Manager tab  (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.

The screenshot shows the MSA FieldServer Manager interface. On the left is a 'Navigation' tree with 'DCC000 QS.CSV v1.00a' expanded, showing sub-items: About, Setup, View, User Messages, and Diagnostics. The main area displays the 'Status' tab for 'DCC000 QS.CSV v1.00a'. Below the tabs is a table with system information.

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

At the bottom, there are buttons for 'Home', 'HELP (?)', 'Contact Us', 'System Restart', 'System Reboot', 'System Time Synch', 'Reset Cycle Times', and 'Logout'. The 'fieldserver' logo is in the bottom right corner.

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


This is a close-up of the 'Navigation' tree. The 'Setup' item is expanded, and 'Network Settings' is highlighted with a grey background. Other items in the tree include 'DCC000 QS.CSV v1.00a', 'About', 'File Transfer', 'User Management', 'Security', 'Time Settings', 'View', 'User Messages', and 'Diagnostics'.

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.

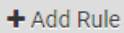
ETH 1

Routing 

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

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

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



Cancel

Save

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.

ETH 1

Routing

☐ 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

Cancel

Save

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

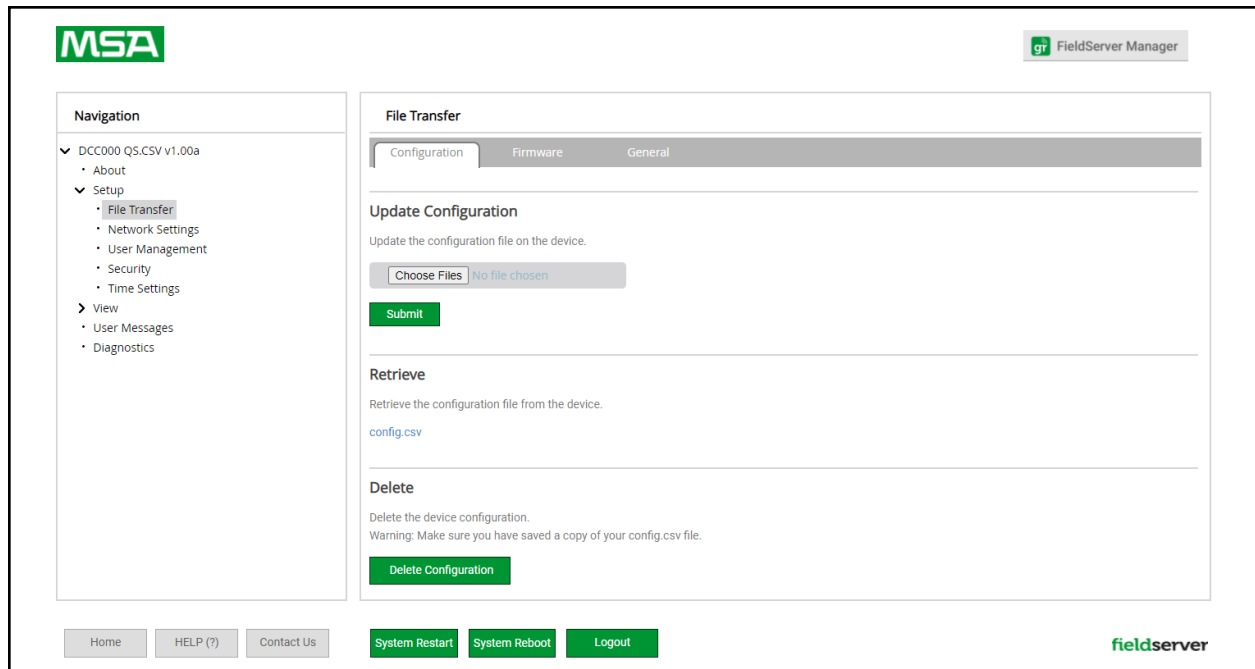
8 Configuring the QuickServer

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.



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”.

The screenshot displays the MSA FieldServer Manager web interface. On the left is a navigation menu with a tree structure: 'DCC000 QS.CSV v1.00a' (expanded) contains 'About', 'Setup', and 'View'. 'Setup' is further expanded to show 'File Transfer' (highlighted), 'Network Settings', 'User Management', 'Security', and 'Time Settings'. 'View' contains 'User Messages' and 'Diagnostics'. At the bottom of the navigation menu are links for 'Home', 'HELP (?)', and 'Contact Us'. The main content area is titled 'File Transfer' and has three tabs: 'Configuration' (active), 'Firmware', and 'General'. Under the 'Configuration' tab, there are three sections: 1. 'Update Configuration' with the instruction 'Update the configuration file on the device.', a 'Choose Files' button (disabled), a 'No file chosen' status, and a green 'Submit' button. 2. 'Retrieve' with the instruction 'Retrieve the configuration file from the device.' and a blue 'config.csv' link. 3. 'Delete' with the instruction 'Delete the device configuration.' and a warning 'Warning: Make sure you have saved a copy of your config.csv file.', followed by a green 'Delete Configuration' button. At the bottom of the page are buttons for 'System Restart', 'System Reboot', and 'Logout', along with the 'fieldserver' logo.

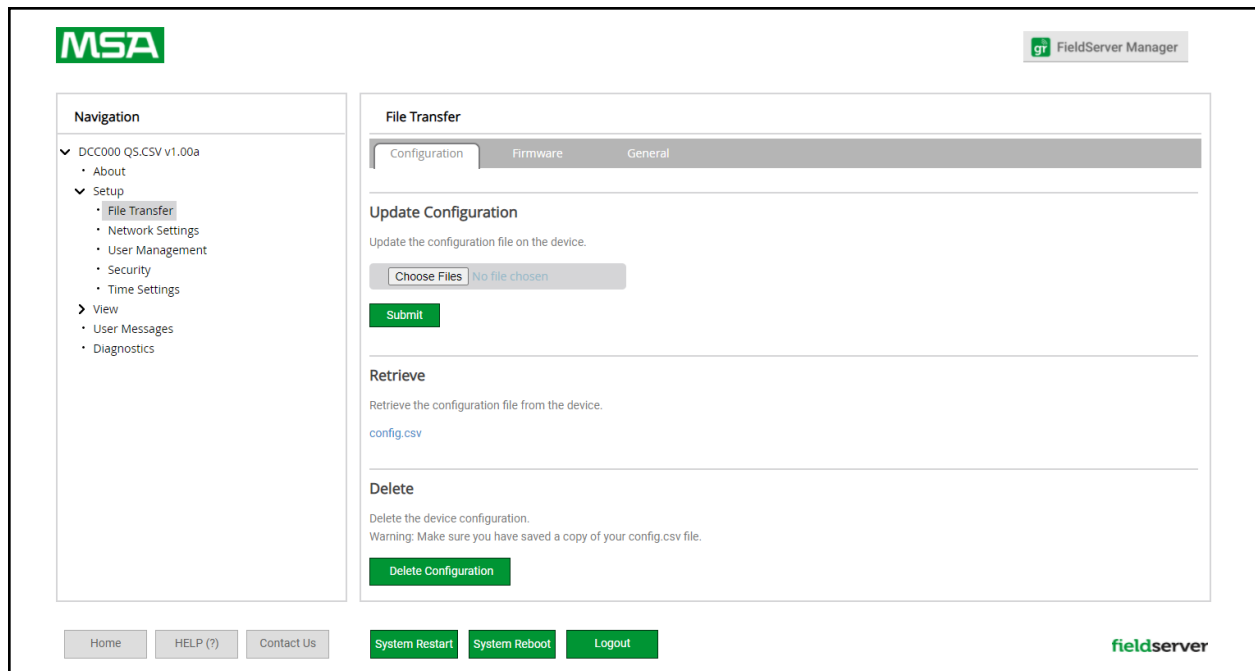
- Once download is complete, a message bar will appear confirming that the configuration was updated successfully.
- Click the System Restart Button to put the new file into operation.

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”.

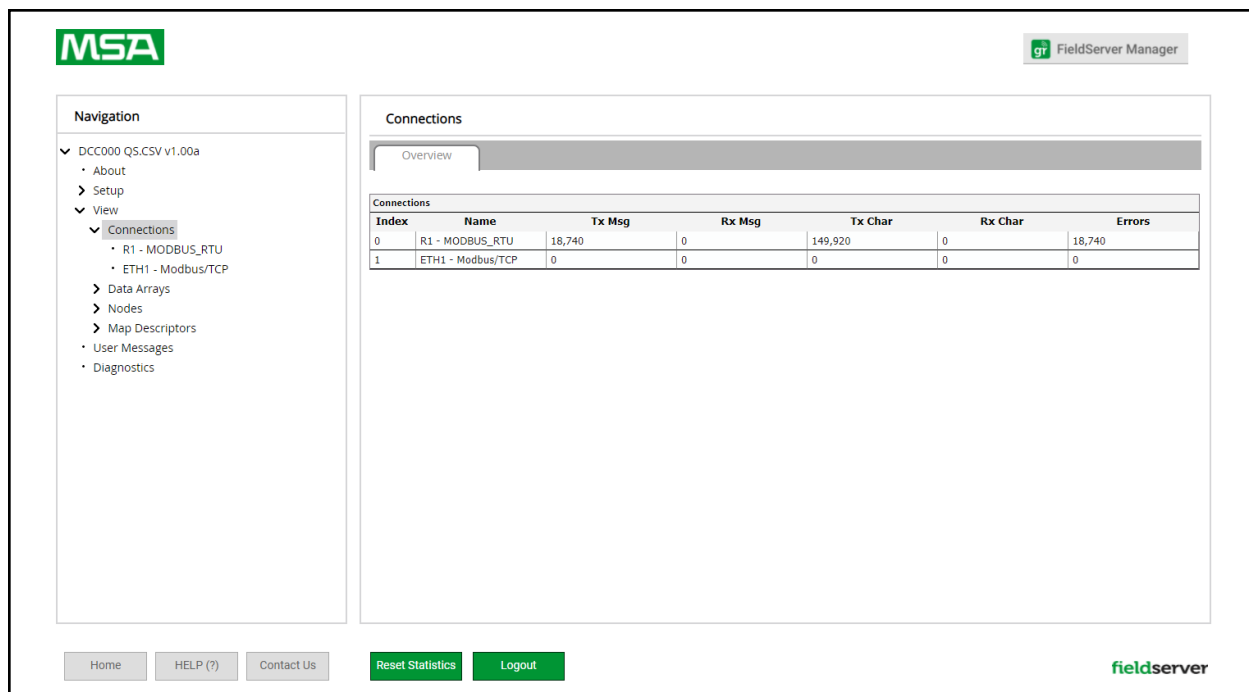


- Click the “config.csv” link under the “Retrieve” heading in the middle section of the screen.
 - The file will automatically download to the web browser’s default download location.
- Edit or store the file as desired.

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

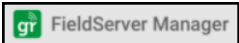
8.4 Test and Commission the QuickServer

- 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.



NOTE: For troubleshooting assistance refer to Section [11 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

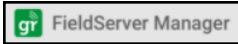
NOTE: The FieldServer Manager tab  (see image above) allows users to connect to the Grid, MSA Safety's device cloud solution for IIoT. The FieldServer Manager enables secure remote connection to field devices through a FieldServer and its local applications for configuration, management, maintenance.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

9 MSA Grid - FieldServer 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



in the top right corner of the page.

NOTE: If a warning message appears instead, go to Section [12.8 FieldServer Manager Connection Warning Message](#) to resolve the connection issue.

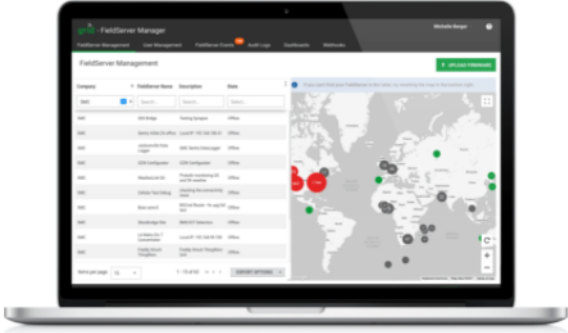
Grid FieldServer Manager Registration

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.

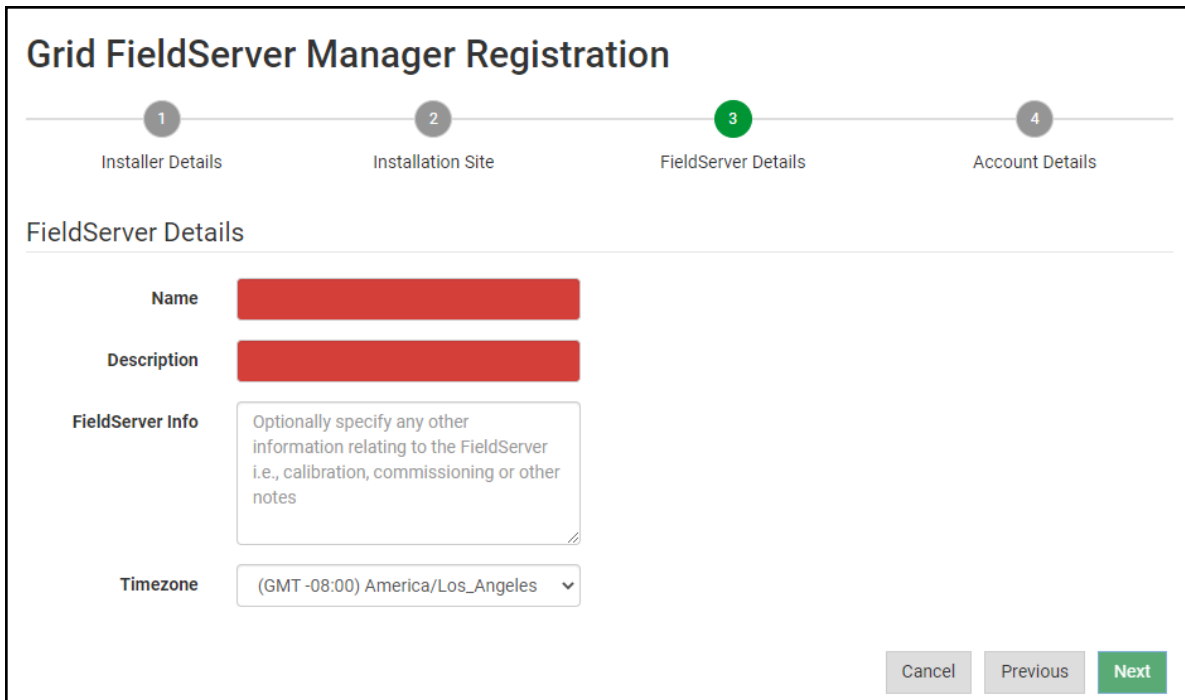
- Enter user details and click Next

The screenshot shows the 'Installer Details' step in a four-part registration process. The progress bar at the top indicates steps 1 (Installer Details), 2 (Installation Site), 3 (FieldServer Details), and 4 (Account Details). The 'Installer Details' section includes input fields for 'Installer Name', 'Company', 'Telephone', and 'Email'. The 'Installation Date' is set to '20-September-2021' with a calendar icon. At the bottom right, there are 'Cancel' and 'Next' buttons.

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

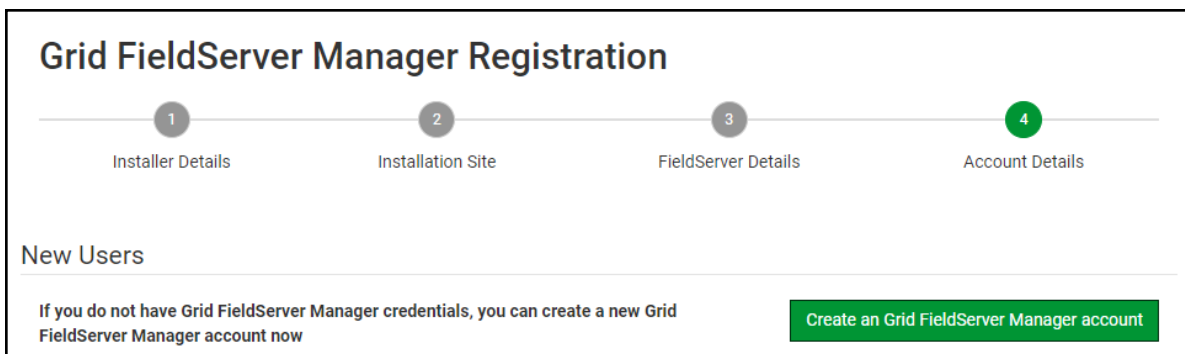
The screenshot shows the 'Installation Site Details' step in the 'Grid FieldServer Manager Registration' process. The progress bar at the top indicates steps 1 (Installer Details), 2 (Installation Site), 3 (FieldServer Details), and 4 (Account Details). The 'Installation Site Details' section includes a 'Search' bar with the text 'Search Google Maps'. Below this are input fields for 'Site Name', 'Building', 'Street Address', 'Suburb', 'City', 'State', 'Country', and 'Postal Code'. There are also red input fields for 'Latitude' and 'Longitude'. To the right of the form is a Google Map showing the area around Lafayette, Louisiana. At the bottom right, there are 'Cancel', 'Previous', and 'Next' buttons.

- Enter Name and Description (required) then click Next



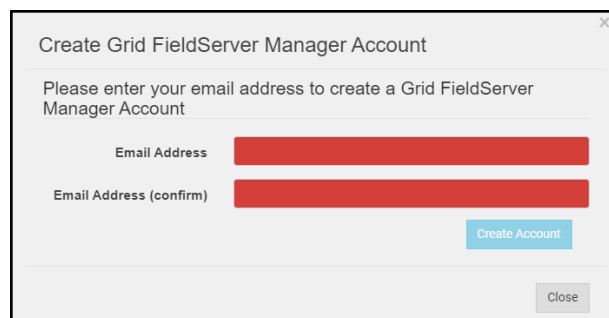
The screenshot shows the 'Grid FieldServer Manager Registration' window at step 3, 'FieldServer Details'. A progress bar at the top indicates four steps: 1. Installer Details, 2. Installation Site, 3. FieldServer Details (highlighted with a green circle), and 4. Account Details. The 'FieldServer Details' section contains four fields: 'Name' and 'Description' (both redacted with red bars), 'FieldServer Info' (a text area with placeholder text: 'Optionally specify any other information relating to the FieldServer i.e., calibration, commissioning or other notes'), and 'Timezone' (a dropdown menu showing '(GMT -08:00) America/Los_Angeles'). At the bottom right, there are three buttons: 'Cancel', 'Previous', and 'Next' (highlighted in green).

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



The screenshot shows the 'Grid FieldServer Manager Registration' window at step 4, 'Account Details'. The progress bar at the top shows step 4 highlighted with a green circle. The 'Account Details' section is titled 'New Users' and contains the text: 'If you do not have Grid FieldServer Manager credentials, you can create a new Grid FieldServer Manager account now'. To the right of this text is a green button labeled 'Create an Grid FieldServer Manager account'.

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

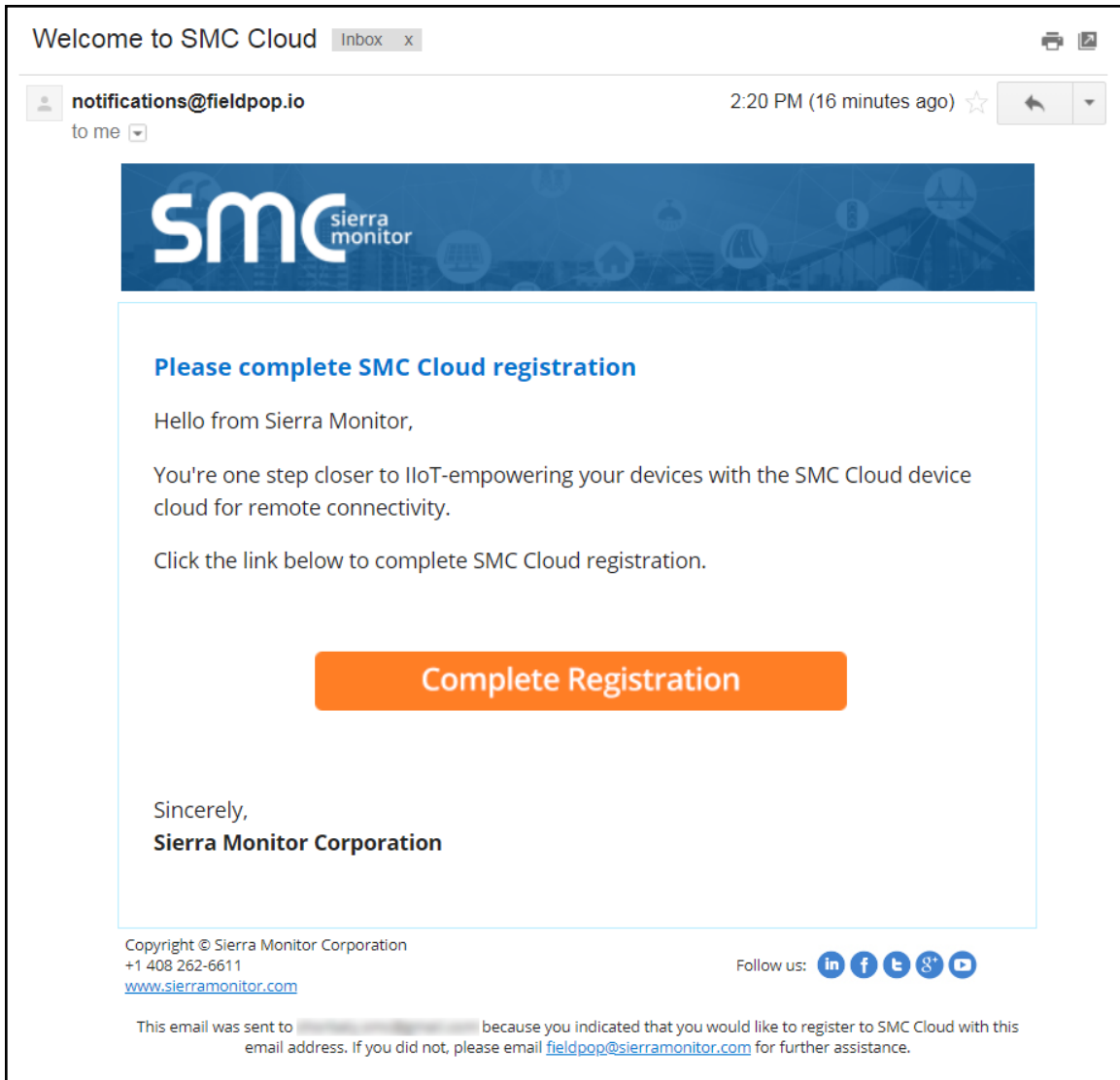


The screenshot shows a dialog box titled 'Create Grid FieldServer Manager Account'. It contains the text: 'Please enter your email address to create a Grid FieldServer Manager Account'. Below this text are two redacted input fields: 'Email Address' and 'Email Address (confirm)'. To the right of the second field is a blue button labeled 'Create Account'. At the bottom right of the dialog is a 'Close' button.

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.



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

First Name

Last Name

Mobile Phone Number

New Password

Confirm Password

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

Cancel

Save

- 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

1

2

3

4

Installer Details

Installation Site

FieldServer Details

Account Details

New Users

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

Create an Grid FieldServer Manager account

Existing Users - Enter FieldServer registration details

User Credentials

Username

Password

Cancel

Previous

Register FieldServer

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

Close

- 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

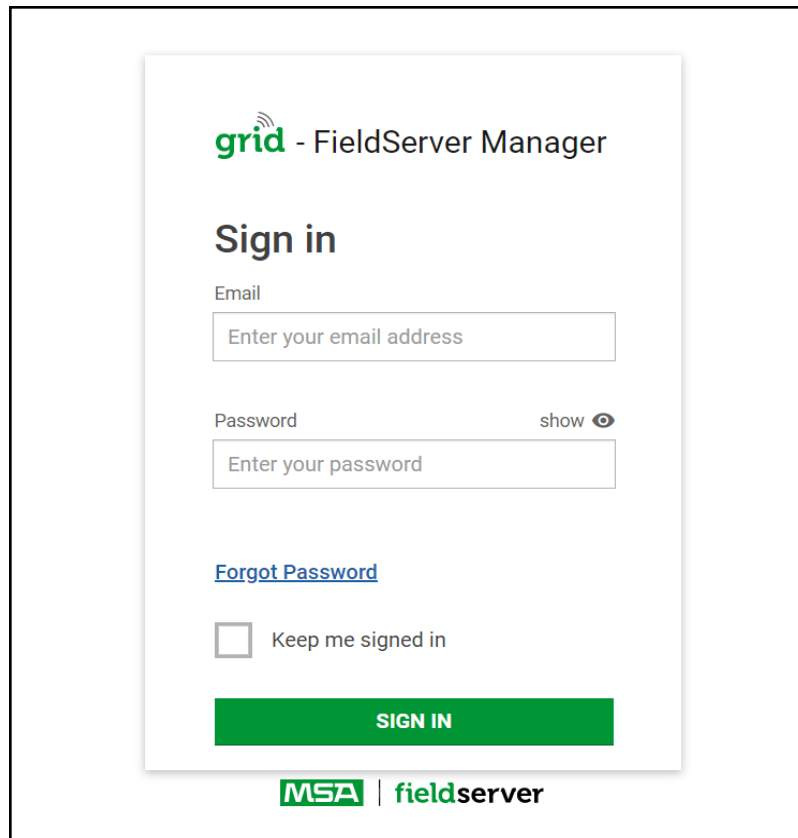
Installation Site Details
Site Name: Site#1
Building:
Street Address: 1020 Canal Road
Suburb:
City: Lafayette
State: Indiana
Country: United States
Postal Code: 47904

Update FieldServer Details

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.



The screenshot shows the 'grid - FieldServer Manager' login interface. It features a 'Sign in' heading, an 'Email' field with the placeholder 'Enter your email address', and a 'Password' field with the placeholder 'Enter your password'. A 'show' link with an eye icon is next to the password field. Below the password field is a '[Forgot Password](#)' link. There is a checkbox labeled 'Keep me signed in'. A green 'SIGN IN' button is at the bottom of the form. The footer displays the 'MSA | fieldserver' logo.

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

User A

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.

Keyboard shortcuts Map data ©2021 Terms of Use

© 2021 MSA. All rights reserved.

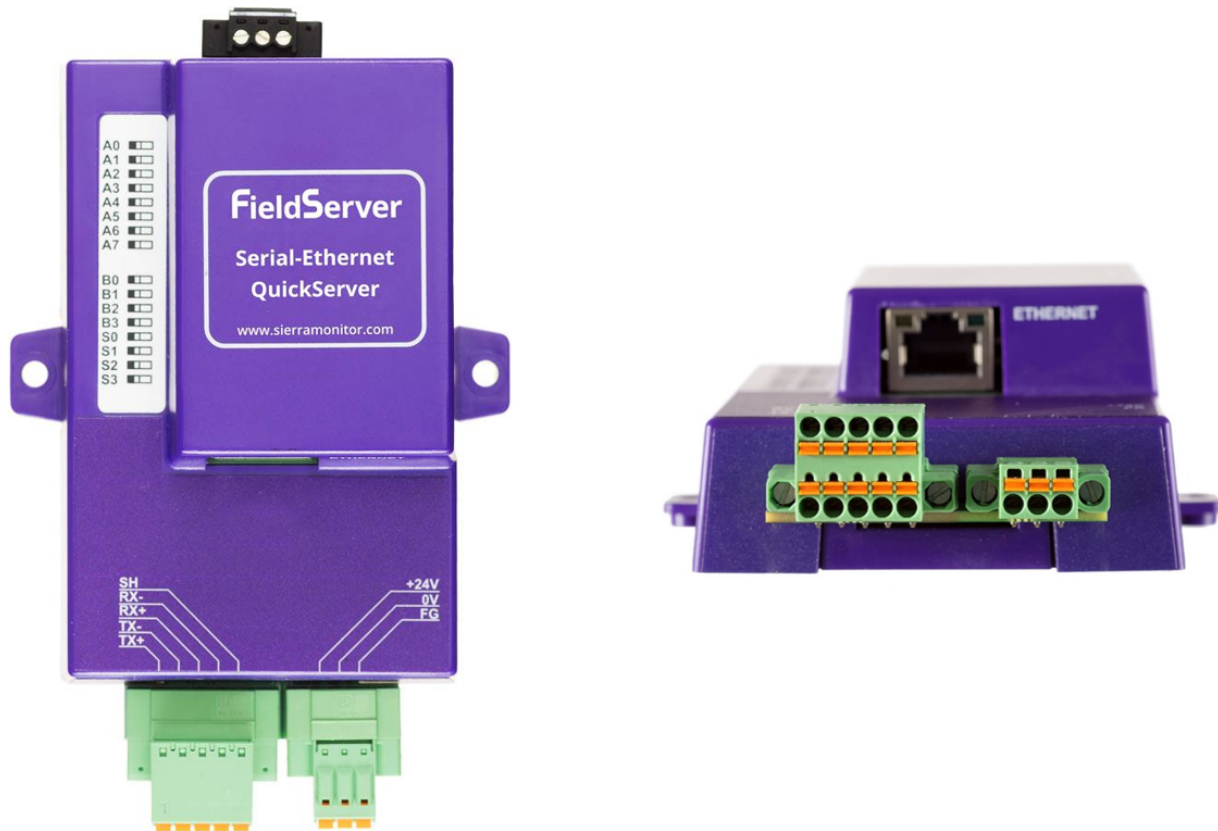
MSA | fieldserver

10 Additional Model Connection Ports

10.1 RS-422 Connection R2 Port

NOTE: The following only applies to models: FS-QS-1230 and FS-QS-1231.

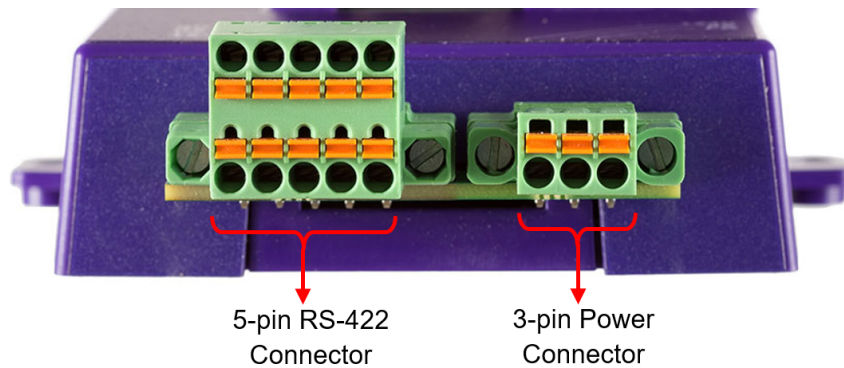
RS-422 is a full duplex multi-drop multi-master differential bus. It can be wired to conform to a RS-485 network when less wiring/cabling is used (due to being less expensive to install), but then it becomes a half-duplex multi-drop multi-master differential bus. RS-422 is used for dedicated peer to peer high speed communication when low bus latency is required (very few devices on the bus). Its usage is very specific to client installations/requirements.



NOTE:

- The RS-232 looks similar to the RS-485 but does not have the blue jumper. The blue jumper is used to enable the termination resistor for the RX signals (120 ohms), while the red jumpers are used to enable the bias resistors for RX signals (510 ohms). In the case of Rockwell/Tetrapak, all jumpers are always required to be in default position (not enabled). For other clients, the bias resistors should always be in the “on” state.
- The part number on the back of the box will identify the port.

10.1.1 Connection and Operation via the RS-422 Port



RS-422 Connector

Pin 1-2: TX +/- (Differential TX outputs: All + signals must be connected to each other, and same applies to - signals; no +/- signals may be crossed)

Pin 3-4: RX +/- (Differential RX inputs: All + signals must be connected to each other, and same applies to - signals, no +/- signals may be crossed)

Pin 5: SHD (Shield connection, must be connected on at least one side of the bus, but not necessarily on both sides)

POWER Connector

Please note that AC voltage is not supported on the RS-422 carrier, and that DC voltage range is ~20VDC to ~28VDC.

Pin 1: +24V (DC power requires this pin be used for the positive voltage)

Pin 2: 0V (DC power requires this pin is used for ground / return voltage)

Pin 3: FG (this pin needs to be connected to EARTH or noise free reference point - CHASSIS)

10.2 KNX Connection R2 Port

NOTE: The following only applies to models: FS-QS-1240 and FS-QS-1241.

The KNX QuickServer is used to transfer data to and from devices using KNX protocol. The KNX driver enables data access from KNX networks to other FieldServer protocols. Most KNX data-point types are supported, allowing communication to almost any kind of KNX device in an installation, such as temperature sensors, shutters, light switches, actuators, alarms, etc. This allows BMS systems to access a KNX network using direct read and write or with KNX configured groups. This setup does not require the use of ETS4 to configure the QuickServer KNX gateway. The KNX protocol is a connectionless protocol and therefore supports multiple clients and multiple servers. The QuickServer is intended to act as a Passive Client on the KNX bus and makes information available to other protocols.



The KNX Connector consist of a KNX + and KNX- terminal. Each terminal corresponds to the red KNX+ and gray KNX- bus connections on a KNX bus.

The following Baud Rates are supported on the R2 Port:

4800, 9600, 19200, 38400, 57600, 115200

10.3 M-Bus Connection R2 Port

NOTE: The following only applies to models: FS-QS-1A50, FS-QS-1A51, FS-QS-1B50, FS-QS-1B51, FS-QS-1C50 and FS-QS-1C51.

The M-Bus driver allows the FieldServer to transfer data to and from devices using M-Bus protocol. The Fieldbus connection is included with the FieldServer. The M-Bus QuickServer Gateway is configurable to act as both a Master and a Slave M-Bus device.

The M-Bus Connector consist of a + and – terminal. Most M-Bus Devices are not polarity sensitive, although the polarity of the M-Bus Connector is indicated on the device diagram, should it be a requirement. The M-Bus devices to communicate with the FieldServer must be configured according to the manufacturer's instructions (for example primary address and readout data).



The following baud rates are supported on the R2 Port:

300, 600, 1200, 2400, 4800, 9600, 19200, 38400


11 Troubleshooting

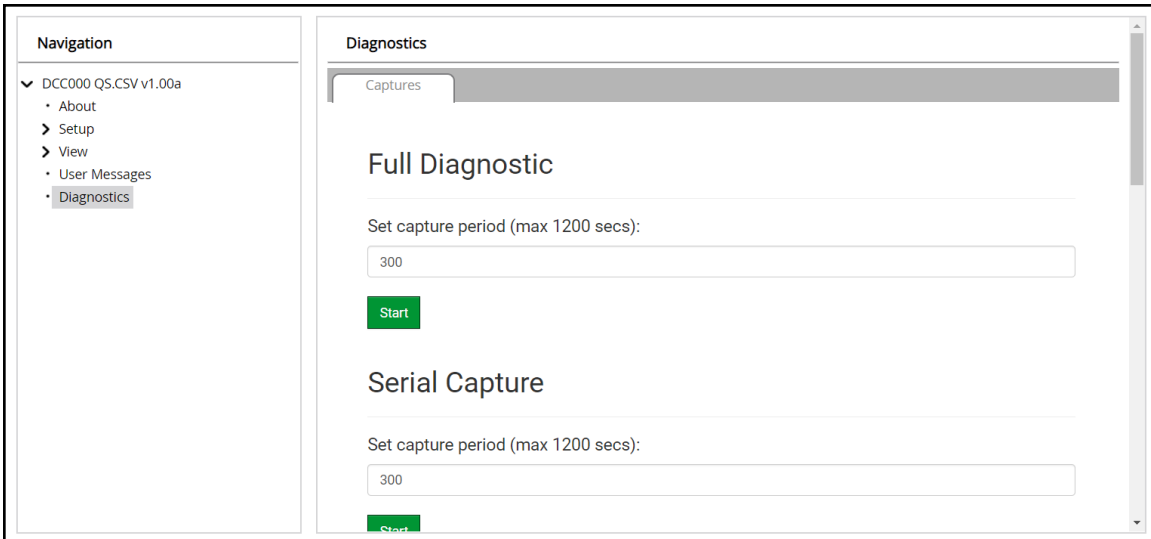
11.1 Communicating with the QuickServer Over the Network

- 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.

11.2 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



The screenshot shows the 'Diagnostics' page in the FieldServer FS-GUI. On the left is a 'Navigation' panel with a tree view containing 'DCC000 QS.CSV v1.00a', 'About', 'Setup', 'View', 'User Messages', and 'Diagnostics' (which is selected). The main content area is titled 'Diagnostics' and has a 'Captures' tab. Under this tab, there are two sections: 'Full Diagnostic' and 'Serial Capture'. Each section has a 'Set capture period (max 1200 secs):' label and a text input field containing '300'. Below each input field is a green 'Start' button.

- 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



This screenshot shows the 'Full Diagnostic' section after the capture is complete. The 'Set capture period (max 1200 secs):' label is followed by a text input field containing '300'. Below the input field is a blue progress bar that is 100% full, with the text '100% Complete' centered on it. At the bottom, there are two buttons: a green 'Start' button and a grey 'Download' 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.

11.3 LED Functions



Light	Description
SPL	SPL LED will be on when a configured node in the QuickServer is detected as being offline. See Node overview screen of the FS-GUI for further details. For LonWorks units , LED will light until the unit is commissioned on the LonWorks network.
RUN	RUN LED will flash 20 seconds after power up, signifying normal operation. The QuickServer will be able to access FS-GUI (refer to Section 5 Connecting to the QuickServer for more information) once this LED starts flashing. During the first 20 seconds, the LED should be off.
ERR	The ERR LED will go on solid 15 seconds after power up. It will turn off after 5 seconds. A steady red light will indicate there is a system error on the FieldServer. If this occurs, immediately report the related “system error” shown in the error screen of the FS-GUI interface to the FieldServer for evaluation.
RX	On normal operation of FS-QS-1XXX, the RX LED will flash when a message is received on the field port of the QuickServer.
TX	On normal operation of FS-QS-1XXX, the TX LED will flash when a message is sent on the field port of the QuickServer.
PWR	This is the power light. It should always show a steady green light when powered.

11.4 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.

12 Additional Information

12.1 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.

These functions are supported on the following:

FS-QS-1011 or **FS-QS-1211** with a serial number starting with 15 or later (indicating the year it shipped).

Minimum BIOS requirement: 2.6.1

12.1.1 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
```

12.1.2 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 12.1.1 Configuring FieldServer as a SSL/TLS Server**.

Certificate Validation Options

Use the Check_Remote_Host element as described in **Section 12.1.1 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.ssi.com/Knowledgebase/Article

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

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


12.2 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.

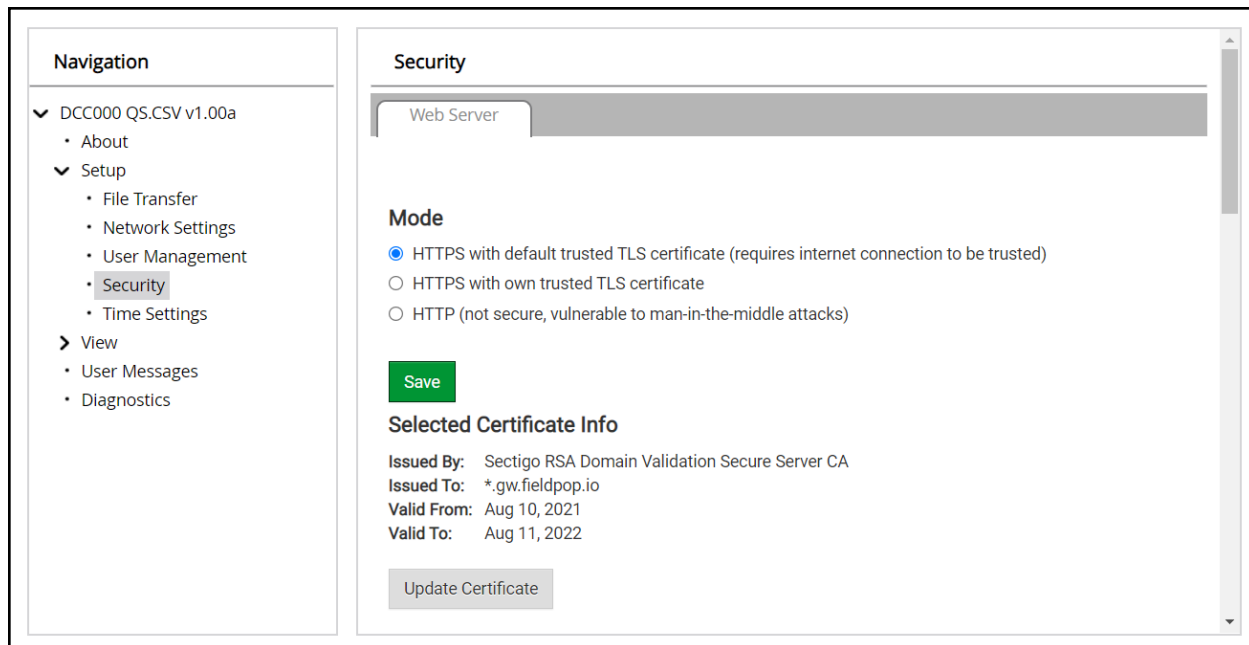
The screenshot displays the MSA FieldServer Manager web interface. The top left features the MSA logo, and the top right shows the 'gr FieldServer Manager' header. A left-hand navigation panel is titled 'Navigation' and contains a tree view with 'DCC000 QS.CSV v1.00a' selected, which has sub-items: 'About', 'Setup', 'View', 'User Messages', and 'Diagnostics'. The main content area is titled 'DCC000 QS.CSV v1.00a' and has three tabs: 'Status' (active), 'Settings', and 'Info Stats'. Below the tabs is a table with the following data:

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%

At the bottom of the interface, there is a row of buttons: 'Home', 'HELP (?)', 'Contact Us', 'System Restart', 'System Reboot', 'System Time Synch', 'Reset Cycle Times', and 'Logout'. The 'fieldserver' logo is located in the bottom right corner.

12.2.1 Change Security Mode

- Click Security in the Navigation panel.



- 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.

12.2.2 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.

The screenshot displays the 'Security' configuration interface. On the left, the 'Navigation' panel lists various settings, with 'Security' highlighted under the 'Setup' section. The main 'Security' panel features a 'Web Server' tab. The 'Mode' section offers three radio button options, with the first option, 'HTTPS with default trusted TLS certificate (requires internet connection to be trusted)', being selected. A prominent green 'Save' button is located below the mode selection. The 'Selected Certificate Info' section provides details about the current certificate, including the issuer (Sectigo RSA Domain Validation Secure Server CA), the domain (*.gw.fieldpop.io), and the validity period (August 10, 2021 to August 11, 2022). An 'Update Certificate' button is positioned at the bottom of this section.

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

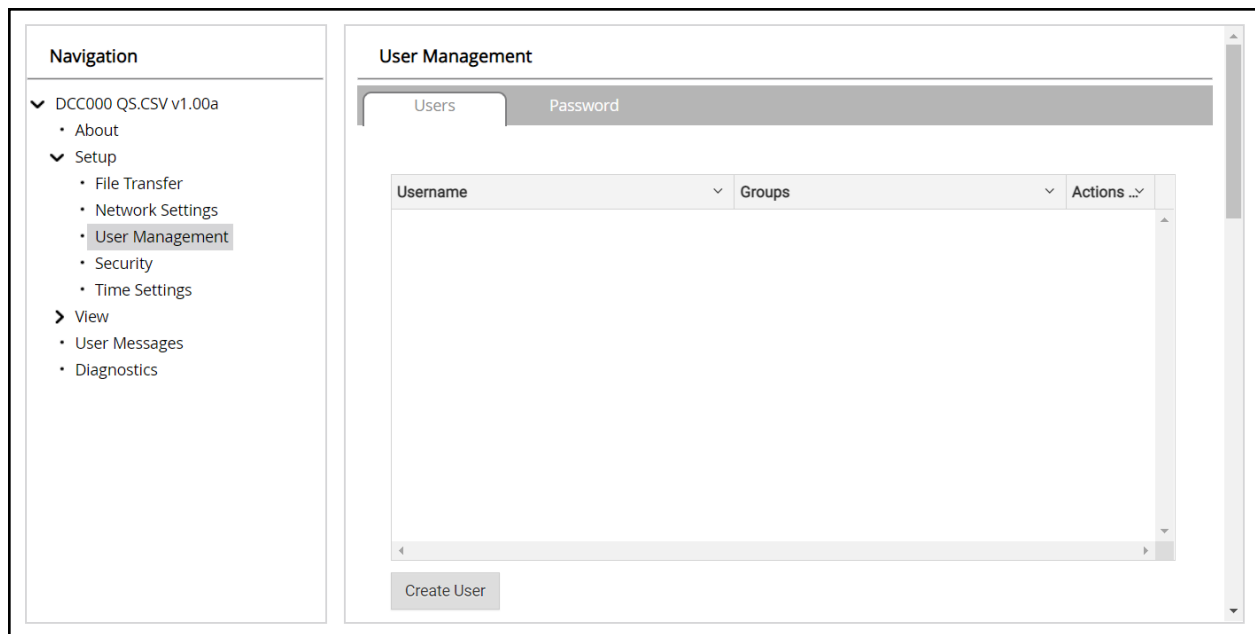
12.3 Change User Management Settings

- 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 Recovery Instructions 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:

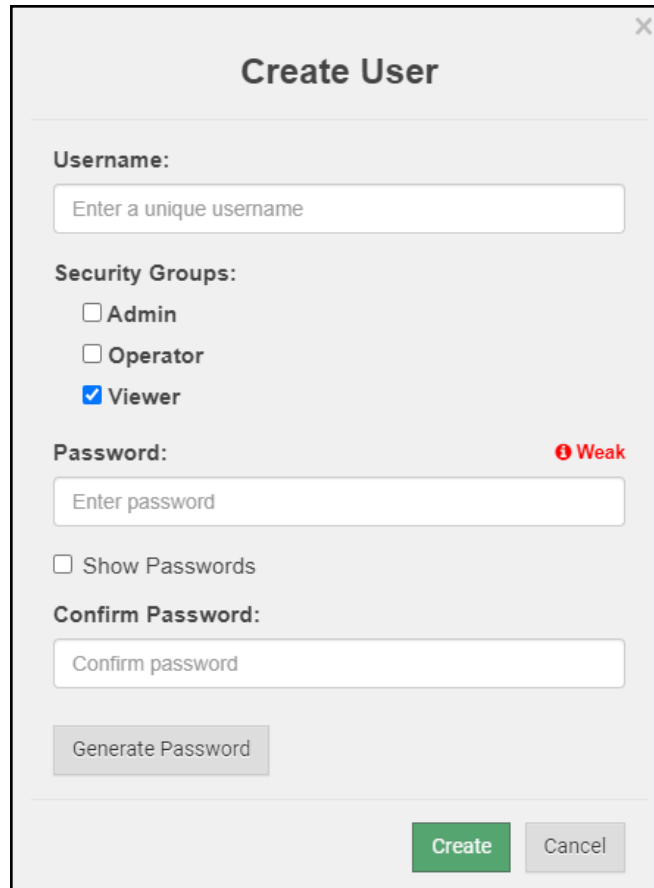
Admin – Can modify and view any settings on the FieldServer.

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

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

12.3.1 Create Users

- Click the Create User button.



The image shows a 'Create User' dialog box with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- Username:** A text input field with the placeholder text 'Enter a unique username'.
- Security Groups:** Three checkboxes: 'Admin' (unchecked), 'Operator' (unchecked), and 'Viewer' (checked).
- Password:** A text input field with the placeholder text 'Enter password'. To the right of the field is a red indicator icon and the text 'Weak'.
- Show Passwords:** An unchecked checkbox.
- Confirm Password:** A text input field with the placeholder text 'Confirm password'.
- Generate Password:** A button located below the Confirm Password field.
- Create and Cancel buttons:** Two buttons at the bottom right, 'Create' (green) and 'Cancel' (gray).

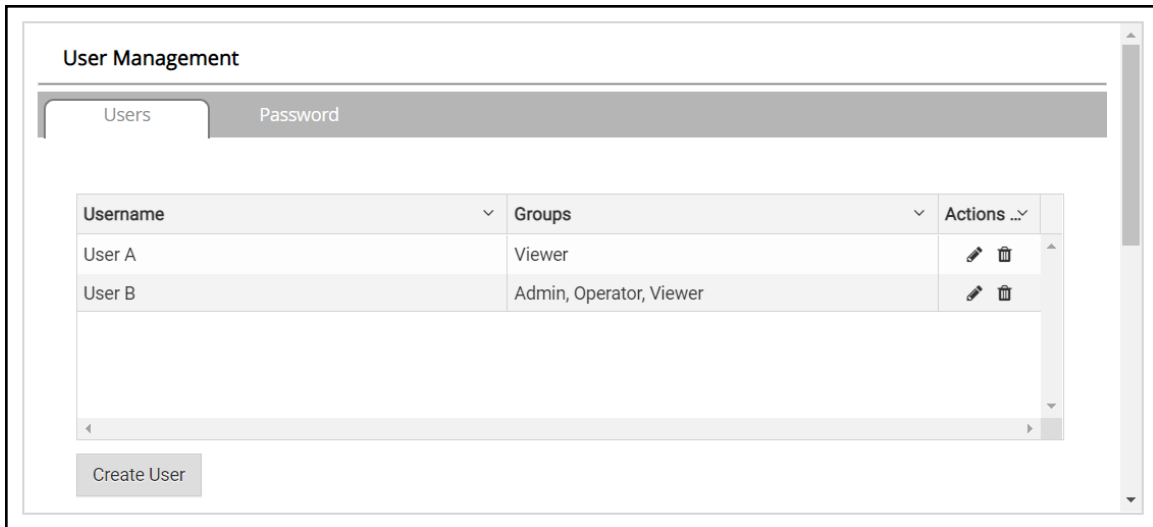
- Enter the new User fields: Name, Security Group and Password.
 - User details are hashed and salted**

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.

12.3.2 Edit Users

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

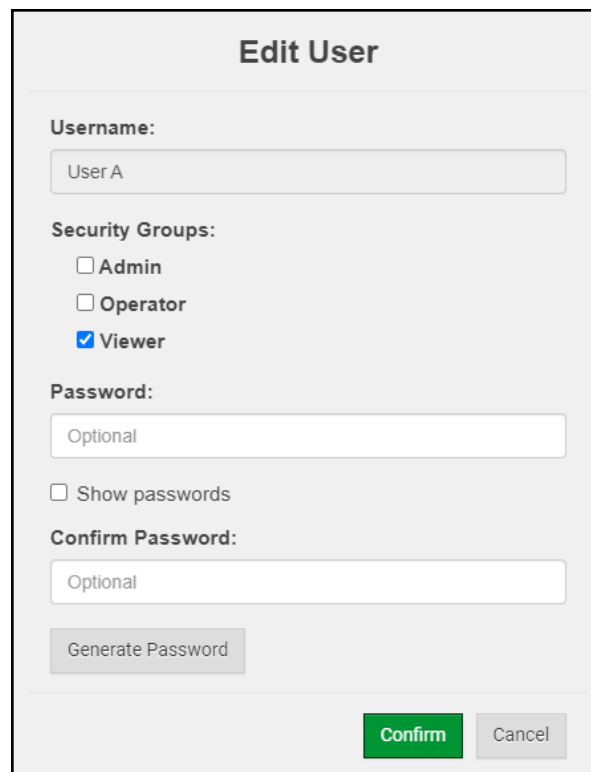


The 'User Management' window has two tabs: 'Users' and 'Password'. The 'Users' tab is active, displaying a table with the following data:

Username	Groups	Actions ...
User A	Viewer	
User B	Admin, Operator, Viewer	

Below the table is a 'Create User' button.

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



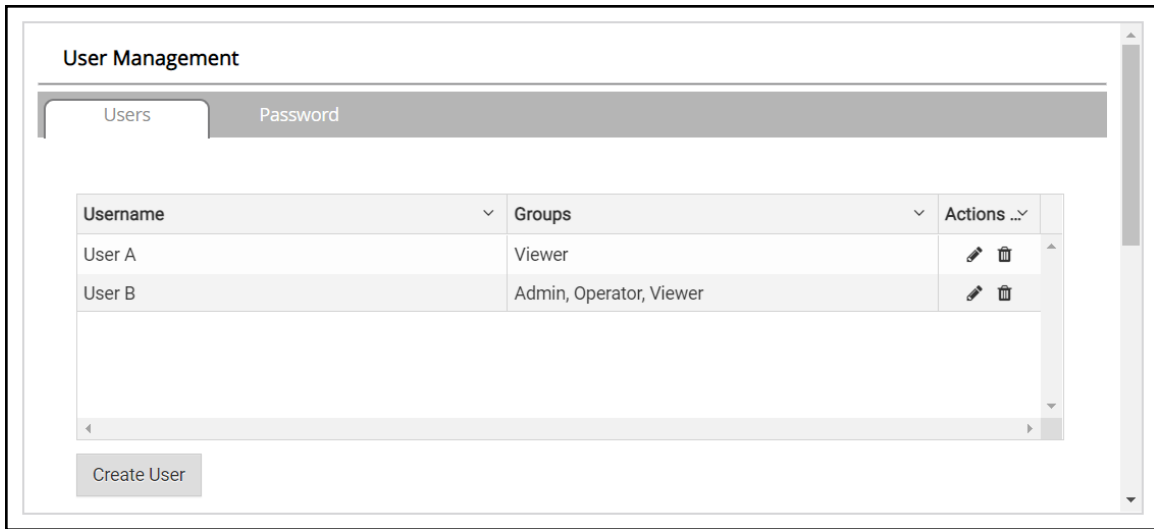
The 'Edit User' window contains the following fields and controls:

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

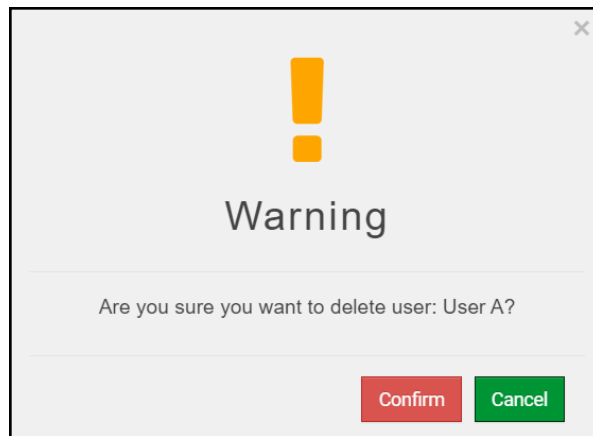
- Click Confirm.
- Once the Success message appears, click OK.

12.3.3 Delete Users

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



- When the warning message appears, click Confirm.



12.3.4 Change FieldServer Password

- Click the Password tab.

The screenshot shows the 'User Management' section of a web interface. On the left is a 'Navigation' sidebar with a tree structure: 'DCC000 QS.CSV v1.00a' (expanded), 'About', 'Setup' (expanded), 'File Transfer', 'Network Settings', 'User Management' (highlighted), 'Security', 'Time Settings', 'View' (expanded), 'User Messages', and 'Diagnostics'. The main area is titled 'User Management' and has two tabs: 'Users' and 'Password'. The 'Password' tab is active. It contains a 'Password:' label with a red 'Weak' indicator, a text input field with the placeholder 'Enter password', a checkbox for 'Show passwords', a 'Confirm Password:' label, another text input field with the placeholder 'Confirm password', a 'Generate Password' button, and a green 'Confirm' button at the bottom right.

- 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.

12.4 QuickServer FS-QS-101X DCC

Driver	Code
BACnet/IP – BACnet MS/TP	0285
BACnet/IP – LonWorks	0131
JCI Metasys N2 – LonWorks	0097
JCI Metasys N2– BACnet MS/TP	0309
JCI Metasys N2– BACnet/IP	0122
Modbus RTU – BACnet MS/TP	0367
Modbus RTU – BACnet/IP	0104
Modbus RTU – JCI Metasys N2	0038
Modbus RTU – LonWorks	0085
Modbus TCP/IP – BACnet/IP	0237
Modbus TCP/IP – LonWorks	0154
Modbus TCP/IP – BACnet MS/TP	0419
Modbus TCP/IP – JCI Metasys N2	0117
SNMP – BACnet/IP	1047
SNMP – LonWorks	1178
SNMP – JCI Metasys N2	1154
SNMP – BACnet MS/TP	1200
BACnet MS/TP - LonWorks	0345

12.5 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-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

12.6 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.

12.7 Specifications



	FS-QS-12X0-XXXX/ FS-QS-1X50-XXXX	FS-QS-1011-XXXX/FS-QS-12X1-XXXX/ FS QS-1X51-XXXX
Electrical Connections	6-pin Phoenix connector: RS-485 or RS 232 or RS-422 +/- ground port, power +/- frame ground port 3-pin RS-485 Phoenix connector: RS-485 +/- ground port Ethernet-10/100 port	6-pin Phoenix connector: RS-485 or RS-232 or RS-422 +/- ground port, power +/- frame ground port 2-pin FTT-10 LonWorks port Ethernet-10/100 port
Power Requirements	Input Voltage: 9-30VDC or 12-24VAC Input Power Frequency: 50/60 Hz. Power Rating: 2.5 Watts Current Draw: @ 12V, 150 mA	Input Voltage: 9-30VDC or 12-24VAC Input Power Frequency: 50/60 Hz. Power Rating: 2.5 Watts Current Draw: @ 12V, 279 mA
Approvals	UL 916 approved RoHS3 compliant FCC part 15 compliant DNP compliant CE certified BTL certified WEEE compliant UKCA compliant	UL 916 approved, RoHS compliant, FCC part 15 compliant, DNP compliant, LonMark certification, WEEE compliant, UKCA compliant SPID: 80:00:95:46:00:84:04:01 Profiles: 0000 - Node object (1) 0001 - Open Loop Sensor Object (5) 0003 - Open Loop Actuator Object (5)
Physical Dimensions	5.05 x 2.91 x 1.6 in. (12.82 x 7.39 x 4.06 cm)	
Weight	0.4 lbs (0.2 Kg)	
Operating Temperature	-40°C to 75°C (-40°F to 167°F)	
Surge Suppression	EN61000-4-2 ESD EN61000-4-3 EMC EN61000-4-4 EFT	
Humidity	5-90% RH non-condensing	

"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.

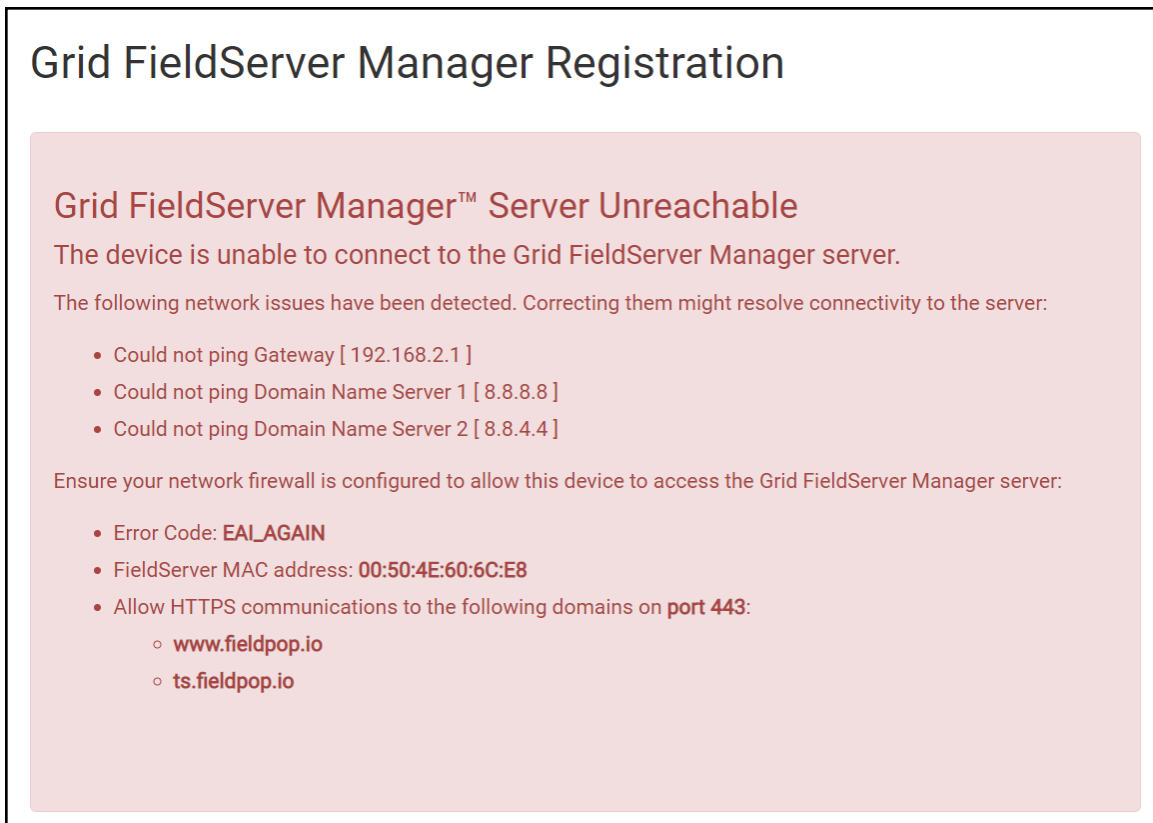
Modifications not expressly approved by FieldServer could void the user's authority to operate the equipment under FCC rules."

NOTE: Specifications subject to change without notice.

NOTE: XXXX at the end of the part number identifies the code for the specific drivers included in the QuickServer. (Section "QS DCC topic")

12.8 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



- 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.

13 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.