

# Field Server

Automation Gateway  
OWNER'S MANUAL

FS-3000 and FS-1000



# CONTENTS

<b>About the Field Servers</b> .....	3	<b>Configuring the Field Server</b> .....	13
Certification .....	3	Retrieving the Sample Configuration File .....	13
Supplied Equipment .....	3	Changing the Configuration File to Meet the Application .....	13
<b>Equipment Setup</b> .....	3	Loading the Updated Configuration File .....	13
Mounting .....	3	Using FS-GUI to Input Load a Configuration File .....	13
Physical Dimensions .....	4	Retrieving the Configuration File for Modification or Backup .....	14
<b>Installation</b> .....	5	Testing and Commissioning the Field Server ..	14
DIP Switch Settings .....	5	Accessing the Field Server Manager .....	14
Bias Resistors .....	5	<b>Troubleshooting</b> .....	15
Termination Resistor.....	6	Lost or Incorrect IP Address.....	15
Connecting the R1 and R2 Ports.....	6	Viewing Diagnostic Information.....	15
Wiring.....	6	Checking Wiring and Settings.....	15
Supported RS-485 Baud Rates by Protocol.....	7	Taking a Field Server Diagnostic Capture.....	16
10/100 Ethernet Connection Port .....	7	LED Functions.....	17
<b>Powering up the Gateway</b> .....	7	Factory Reset Instructions.....	17
<b>Connecting the PC to the Gateway</b> .....	8	Internet Browser Software Support .....	17
Connecting to the Gateway via Ethernet .....	8	<b>Additional Information</b> .....	17
Changing the Subnet of the Connected PC....	8	Changing the Web Server Security Settings After Initial Setup.....	17
<b>Setting Up Web Server Security</b> .....	9	Changing the Security Mode .....	18
Logging In to the Field Server .....	9	Editing the Certificate Loaded onto the Field Server.....	18
Selecting the Security Mode .....	10	Changing the User Management Settings .....	18
HTTPS with Own Trusted TLS Certificate .....	10	Creating Users .....	19
HTTPS with Default Untrusted Self-Signed TLS Certificate or HTTP with Built-in Payload Encryption.....	10	Editing Users .....	19
<b>Setting Up the Network</b> .....	11	Deleting Users .....	19
Using FS-GUI to Input Network Settings .....	11	Changing the Field Server Password.....	20
Routing Settings.....	11	Specifications.....	20
Eth1 and Eth2		Warnings .....	20
Network Settings - LAN Mode.....	12	Complying with EN IEC 62368-1.....	20
Ethernet 2 Network Settings - WAN Mode.....	12	<b>Limited 2-Year Warranty</b> .....	21



## ABOUT THE FIELD SERVERS

The Field Server 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 the [Troubleshooting](#) section or any of the troubleshooting appendices in the related driver supplements. Check the Hunter Industries website for technical support resources and documentation that may be of assistance.

The Field Server is cloud-ready and connects with Hunter Industries's Grid. See the section on [Accessing the Field Server Manager](#) for more information.

### Certification

BTL Mark – BACnet™  
Testing Laboratory



The BTL Mark on the Field Server is a symbol indicating that a product has passed a series of rigorous tests conducted by an independent laboratory. This 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](http://www.BACnetInternational.net) for more information about the BACnet Testing Laboratory. You can view the BACnet Protocol Implementation Conformance Statement (PICS) at [bacnet.org/conformance-pics/](http://bacnet.org/conformance-pics/). BACnet is a registered trademark of ASHRAE.

### Supplied Equipment

#### Field Server Gateway

- Preloaded with two selected drivers and a sample configuration file.

fieldserver operating manual

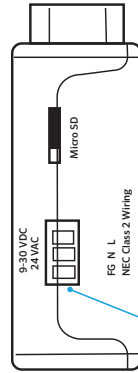
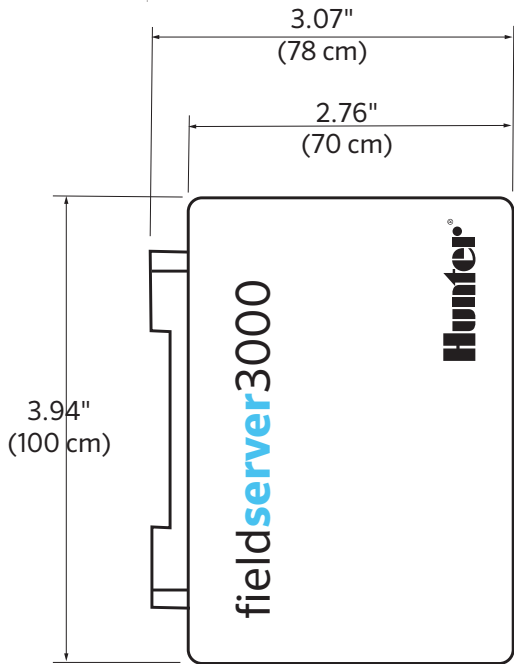
## EQUIPMENT SETUP

### Mounting

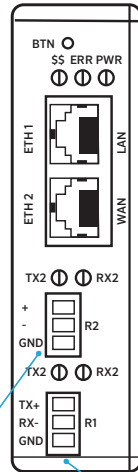
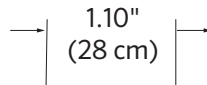
The gateway can be mounted using the DIN rail mounting bracket on the back of the unit.



# Physical Dimensions

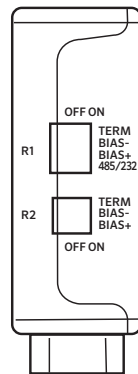
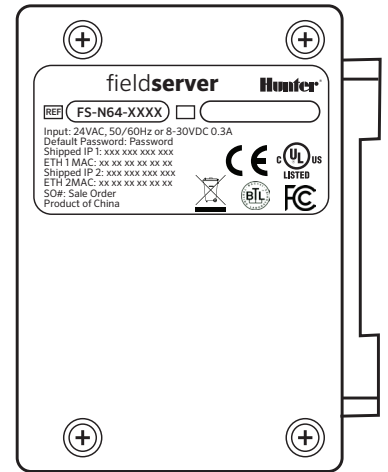


Power Port



R2 Serial Port

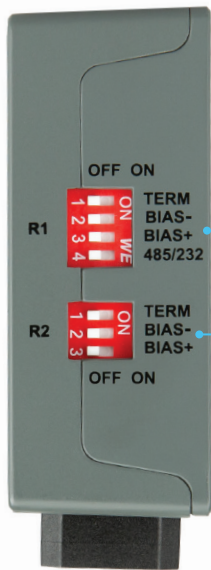
R1 Serial Port



## INSTALLATION

### DIP Switch Settings

#### Bias Resistors



R1 Bias Resistor DIP switches (2 and 3)

R2 Bias Resistor DIP switches (2 and 3)

**NOTE:** See [ni.com/support/serial/resinfo.htm](http://ni.com/support/serial/resinfo.htm) for additional information.

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

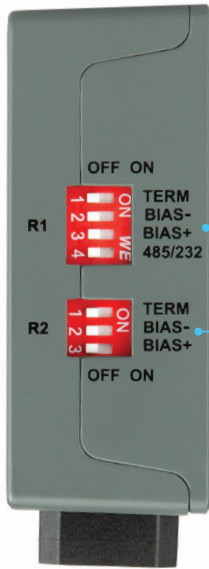
**NOTE:** If the gateway is already powered on, DIP switch settings will not take effect unless the unit is power cycled.

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 Field Servers can be put on the network without running into the bias resistor limit, which is < 500 ohms.

## Termination Resistor



R1 Bias Resistor DIP switches (2 and 3)

R2 Bias Resistor DIP switches (2 and 3)

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 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.

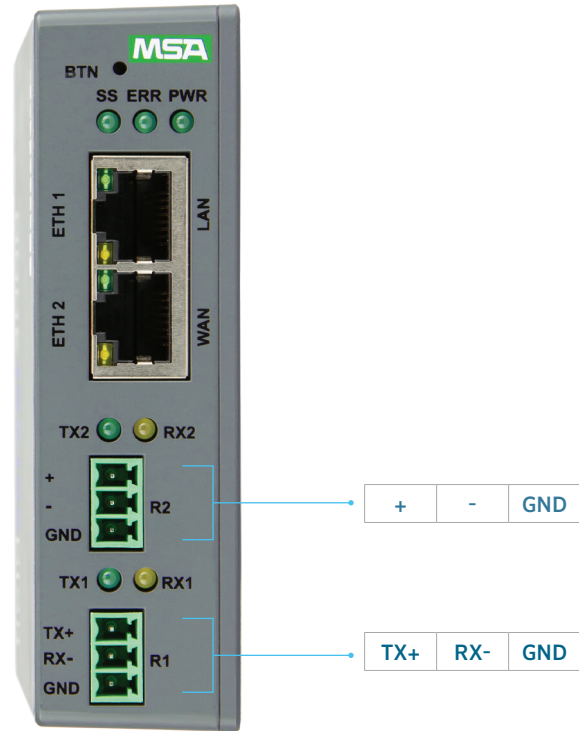
**NOTE:** If the gateway is already powered on, DIP switch settings will not take effect unless the unit is power cycled.

### 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 [DIP Switch Setting](#) section).

The R2 port is RS-485.

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



### 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:** The RS-485/RS-232 is part of the RS-485/RS-232 interface and must be connected to the corresponding terminal on the BMS. If the cable is shielded, the shield must be connected only at one end and to earth ground. This will help suppress the electromagnetic field interference. (Connecting the shield at both ends will likely produce current loops, which could produce noise or interference that the shield was intended to block).



## Supported RS-485 Baud Rates by Protocol

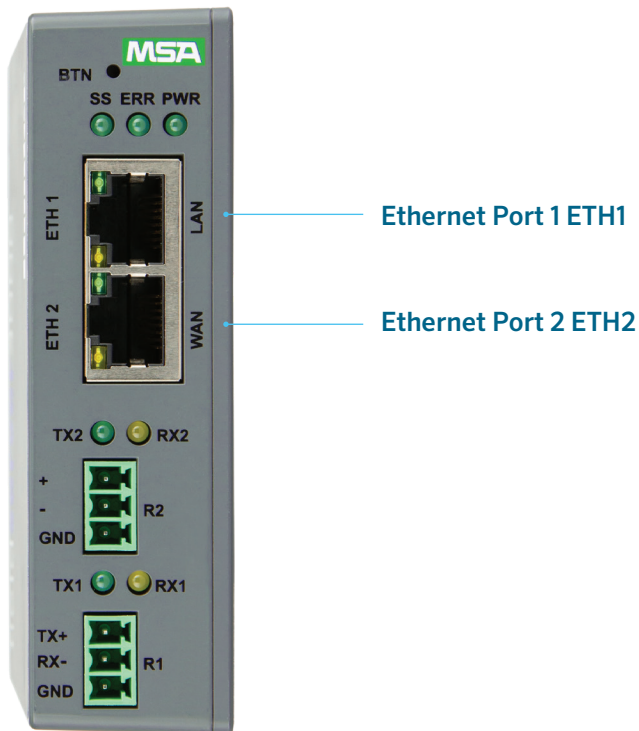
The supported baud rates for either port is based on the protocol of the connected devices. The following baud rates are supported for Modbus RTU:

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

The following baud rates are supported for BACnet MS/TP: 9600, 19200, 38400, 76800, 115200

## 10/100 Ethernet Connection Port

**NOTE:** Do not use shielded Ethernet cables.



Ethernet Port 1 ETH1

Ethernet Port 2 ETH2

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, and the Subnet Mask is 255.255.255.0.

**NOTE:** The ETH2 port can be set to WAN mode to limit Ethernet traffic. See the WAN Mode Settings for ETH2 section for details.

**NOTE:** ETH1 and ETH2 must be configured with IP Addresses on different IP subnets.

## POWERING UP THE GATEWAY

Check power requirements in the table below:

### Power Requirement for Field Server External Gateway

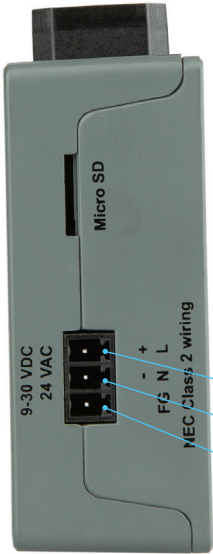
Field Server Family	Current Draw Type	
	12VDC	24vdc/ac
FS-QS-3X109-XXXX (typical)	250mA	125mA

**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 Field Server as shown on next page. Ensure that the power supply used complies with the specifications provided in the Specifications section.

- The gateway accepts 9 to 30 VDC or 24 VAC on pins L+ and N-.
  - Supports both Full-Wave and Half-Wave AC
- Frame GND should be connected to ensure personnel safety and to limit material damages due to electrical faults. Ground planes are susceptible to transient events that cause sudden surges in current. The frame ground connection provides a safe and effective path to divert the excess current from the equipment to earth ground.

**NOTE:** Floating AC power supplies are supported.

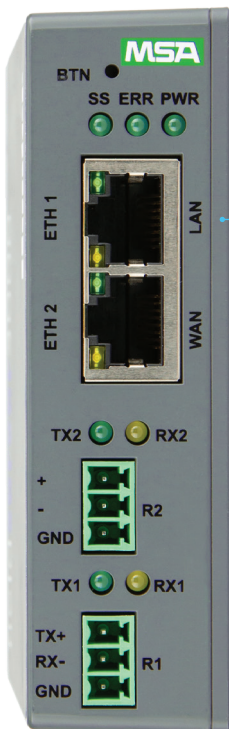


Power to Gateway	Gateway Pin Label	Pin Assignment
Power in (+)	L +	V +
Power In (-)	N-	V -
Frame GND	FG	Frame GND

## CONNECTING THE PC TO THE GATEWAY

### Connecting to the Gateway via Ethernet

Connect a Cat-5 Ethernet cable (straight through or cross-over) between the local PC and Field Server ETH1 (LAN port).



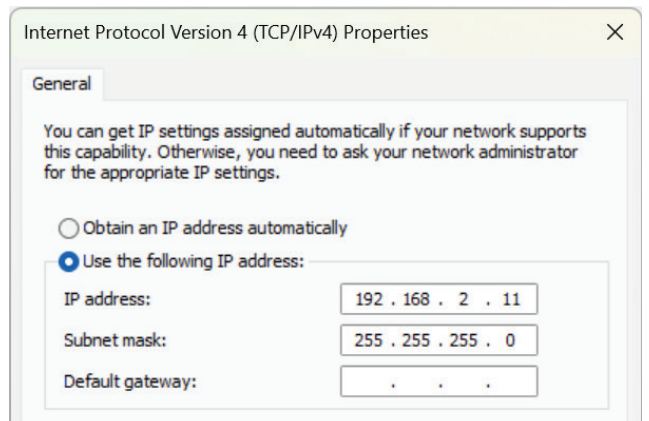
Ethernet Port

## Changing the Subnet of the Connected PC

The default IP address for the Field Server is 192.168.2.101, and the Subnet Mask is 255.255.255.0. If the PC and Field Server are on different IP networks, assign a static IP address to the PC on the 192.168.2.xxx network.

### For Windows 10:

- Find the search field in the local computer's taskbar (usually to the right of the Windows icon) and type in Control Panel.
- Click Control Panel, Network and Internet, then Network and Sharing Center in that order.
- 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 and then click the Properties button.
- Select and enter a static IP address on the same subnet. For example:



- Click the Okay button to close the Internet Protocol window. Next, select the Close button to close the Ethernet Properties window.

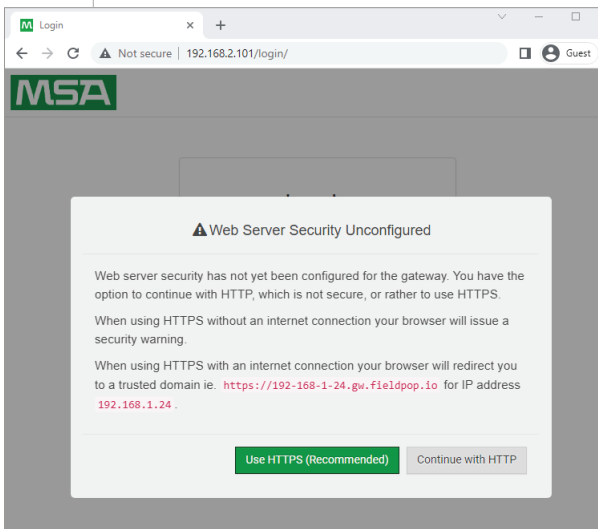


# SETTING UP WEB SERVER SECURITY

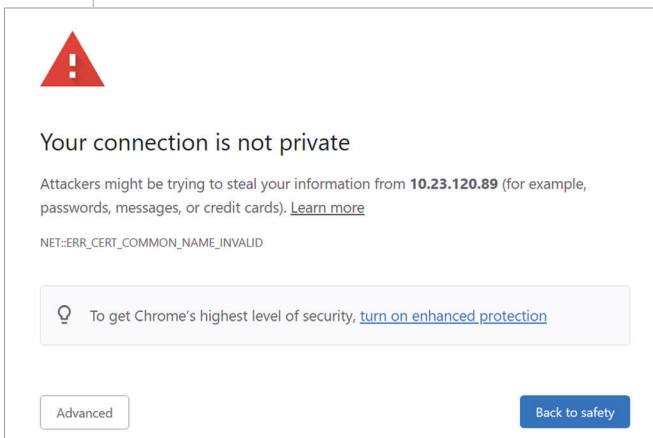
## Logging In to the Field Server

The first time the Field Server 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.

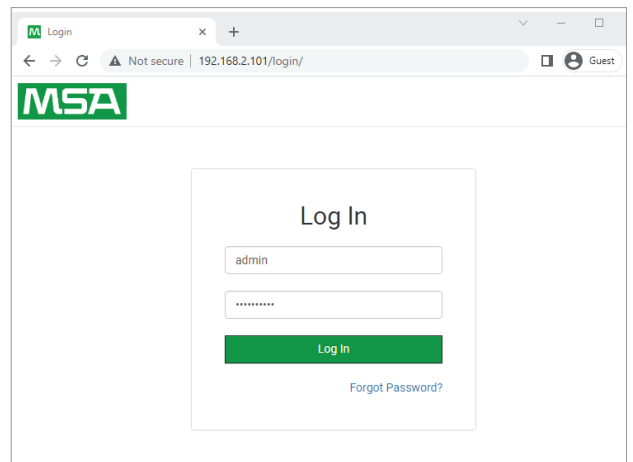


- Additional text will expand below the warning. Click the underlined text to go to the IP address. In the example below, this text is “Proceed to 10.40.50.94 (unsafe).”



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

**NOTE:** There is also a QR code in the top right corner of the Field Server label that shows the default unique password when scanned.



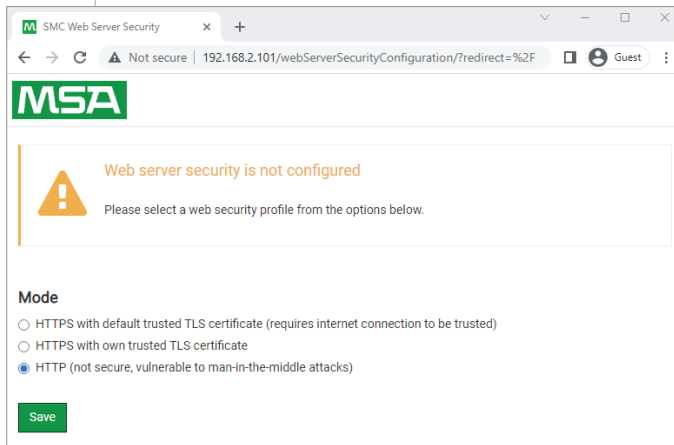
**NOTE:** A user has five attempts to log in. Afterward, there will be a 10-minute lockout. There is no timeout on the Field Server to enter a password.

**NOTE:** To create individual user logins, go to the [Change User Management Settings](#) section.



## Selecting the Security Mode

On the first login attempt to the Field Server, the following screen will appear. It allows the user to select the mode that the Field Server should use.



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

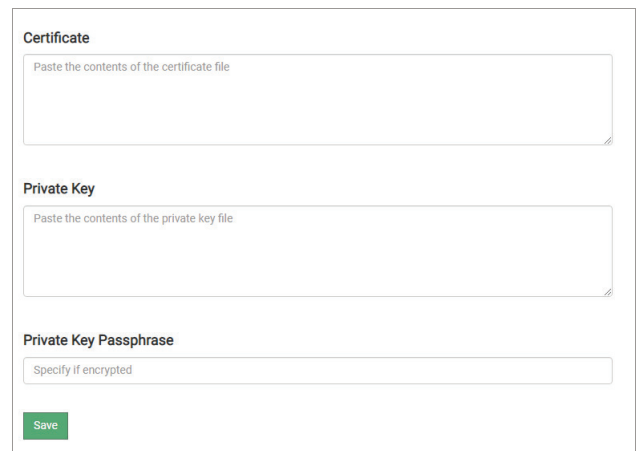
**NOTE:** To change the web server security mode after initial setup, go to the [Change Web Server Security Settings After Initial Setup](#) section.

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

### 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.



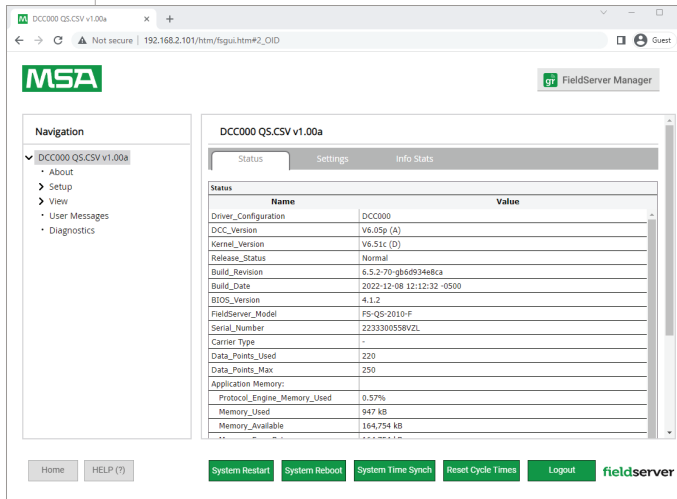
- Copy and paste the Certificate and Private Key text into their respective fields. If the Private Key is encrypted, type in the associated Passphrase.
- Click Save.
- A “Redirecting” message will appear. After a short time, the Field Server GUI will open.

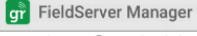
### HTTPS with Default Untrusted Self-Signed TLS Certificate or HTTP with Built-in Payload Encryption

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

# SETTING UP THE NETWORK

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

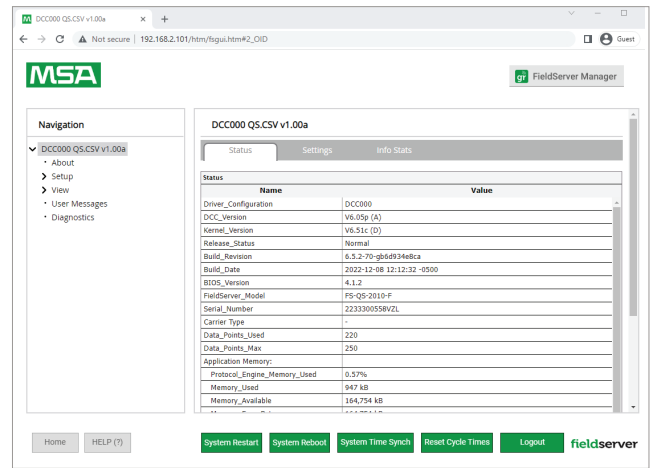


**NOTE:** The Field Server Manager tab  allows users to connect to the Grid, Hunter Industries’s device cloud solution for IIoT. The Field Server Manager enables secure remote connection to field devices through a Field Server and its local applications for configuration, management, and maintenance.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

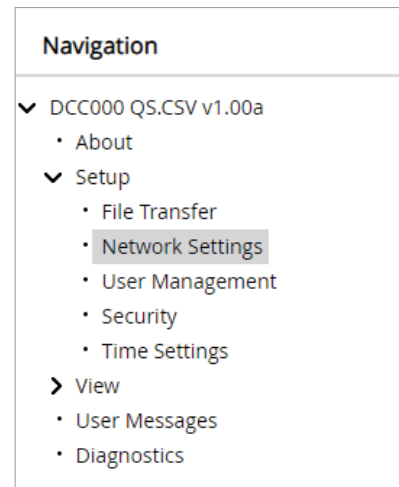
## Using FS-GUI to Input Network Settings

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

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



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



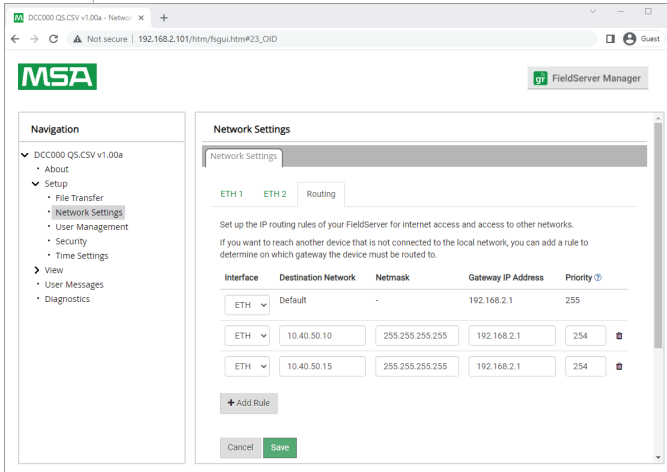
## Routing Settings

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

**NOTE:** The default connection is ETH1.

- Select the default connection in the first row as either ETH 1 or ETH 2.
- Click the Add Rule button to add a new row and set a new Destination Network, Netmask, and Gateway IP Address as needed.

- Set the Priority for each connection (1 to 255 with 1 as the highest priority and 255 as the lowest).
- Click the Save button to activate the new settings.



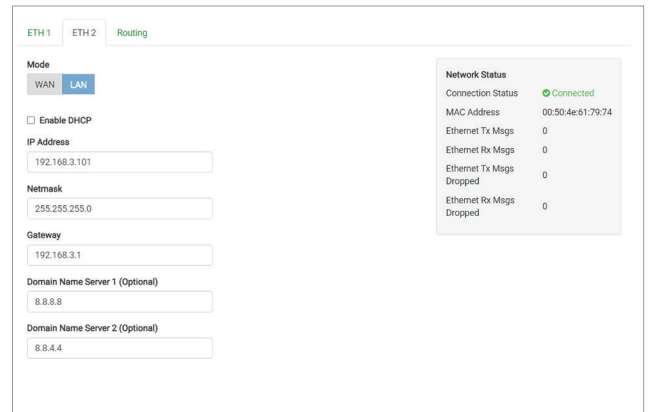
## Ethernet 1 and Ethernet 2 Network Settings – LAN Mode

- Check that the Mode is set to LAN. If not, click LAN to change the ETH 2 port to LAN mode.
- Enable DHCP to automatically assign IP settings or modify the IP settings manually as needed, via these fields: IP Address, Netmask, Gateway, and Domain Name Server1/2.

**NOTE:** *If connected to a router, set the gateway to the same IP address as the router.*

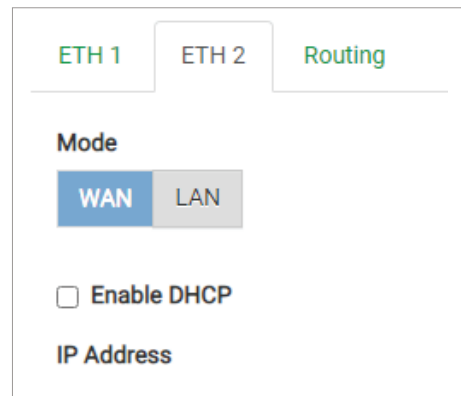
- Click Save to record and activate the new IP address.
- Connect the Field Server to the local network or router.

**NOTE:** *If the webpage was open in a browser, the browser will need to be pointed to the new IP address of the Field Server before the webpage will be accessible again.*



## Ethernet 2 Network Settings – WAN Mode

- Click the blue WAN box to change the ETH 2 port to WAN mode.
  - This grants access only to allowed incoming traffic on the ETH 2 port. It does allow a connection to the internet via port 80 and 443.



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

**Incoming Firewall (Optional)**  
All incoming network traffic is blocked by default. You can use the incoming firewall rules to allow specified traffic to the FieldServer from the WAN network.

Shorthand tips When you add rules, you can use the following symbols

IP Address	Netmask (Optional)	Port Range	Description (Optional)
*		80,443,1024	Webpage and FieldServer To

+ Add Rule

Cancel Save

**NOTE:** See the options below for setting firewall rules.

- Add 1023 to the Port Range field to allow Field Server Toolbox access.
- Add 47808 to the Port Range field for BACnet access.
- Add 80 and 443 to the Port Range field for web browser access.
- Use an asterisk (\*) as a wild card for the IP address.

## CONFIGURING THE FIELD SERVER

### Retrieving the Sample Configuration File

The configuration of the Field Server is provided to the Field Server's operating system via a comma-delimited file called config.csv.

If a custom configuration was ordered, the Field Server will be programmed with the relevant device registers in the config.csv file for the initial start-up. If not, the product will ship 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.

fieldserver operating manual

### Changing the Configuration File to Meet the Application

Refer to the Field Server Configuration Manual in conjunction with the driver supplements for information on configuring the Field Server.

### Loading the Updated Configuration File

#### Using 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 config.csv file, open, then click Submit.

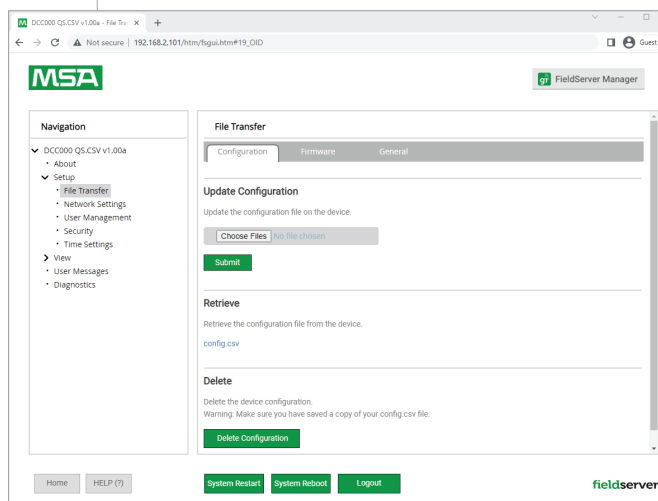
- Once the download is complete, a message bar will appear confirming that the configuration was updated successfully.
- Click the System Restart Button to put the new file into operation.

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

## Retrieving 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.

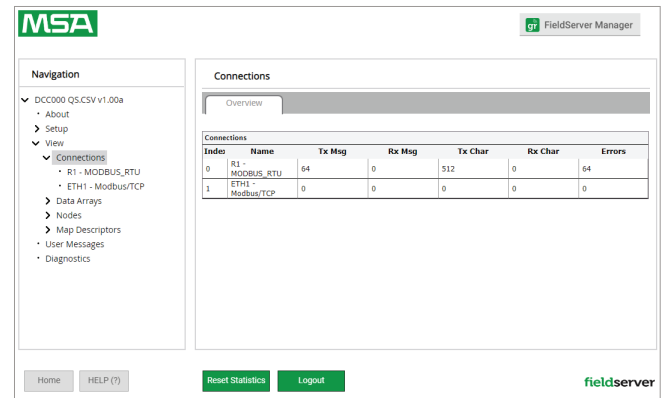


- Click the config.csv link under the Retrieve heading in the middle section of the screen.
  - The file will automatically download to the web browser's default download location.
- Edit or store the file as desired.

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

## Testing and Commission the Field Server

- Connect the field server 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 the Troubleshooting section or any of the troubleshooting appendices in the related driver supplements and configuration manual. Hunter Industries also offers a technical support section on the Hunter Industries website, which contains a significant number helpful resources and documentation.*

## Accessing the Field Server Manager

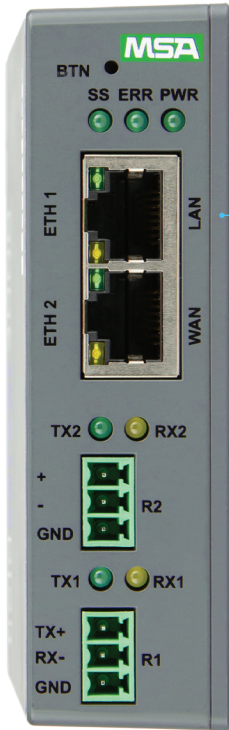
**NOTE:** *The Field Server Manager tab allows users to connect to the Grid, Hunter Industries's device cloud solution for IIoT. The Field Server Manager enables secure remote connection to field devices through a field server and its local applications for configuration, management, and maintenance. For more information about the Field Server Manager, refer to the MSA Grid - Field Server Manager Startup Guide.*



# TROUBLESHOOTING

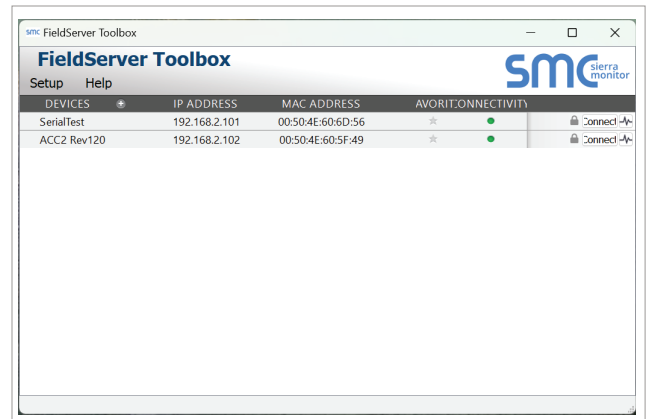
## Lost or Incorrect IP Address

- Ensure that the Field Server Toolbox is loaded onto the local PC. Otherwise, download the Field Server-Toolbox.zip file via the Hunter Industries website.
- Extract the executable file and complete the installation.



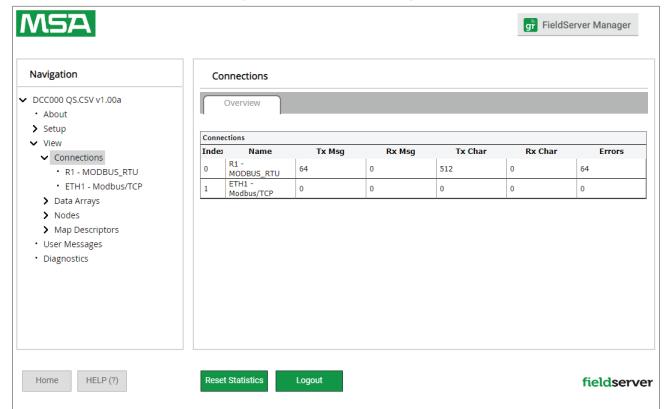
Ethernet Port

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



## Viewing Diagnostic Information

- Type the IP address of the Field Server into the web browser, or use the Field Server Toolbox to connect to the field server.
- Click on the Diagnostics and Debugging button, then click on View, and then on Connections.
- If there are any errors showing on the Connection page, refer to [Checking Wiring and Settings](#) section for the relevant wiring and settings.



## Checking Wiring and Settings

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

- Check the LEDs on the Field Server (LED Functions section).
- Check the baud rate, parity, data bits, and stop bits.
- Check the device address.
- Verify the wiring.
- Verify that the device is connected to the same subnet as the Field Server.

### Field COM Problems

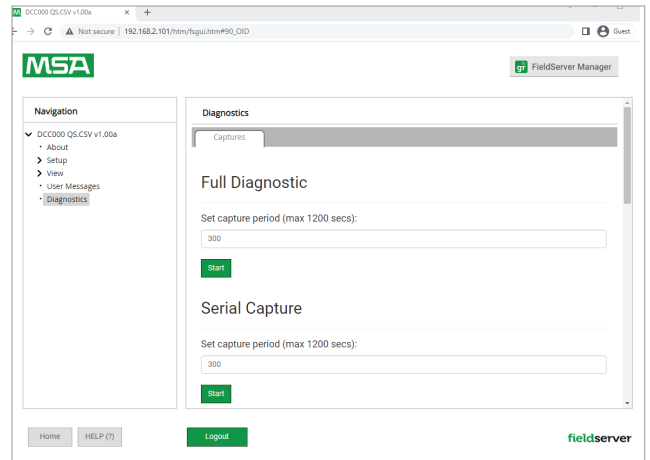
- Visual observations of LEDs on the Field Server (LED Functions section).
- Verify wiring.
- Verify IP Address setting.

**NOTE:** *If the problem still exists, a diagnostic capture needs to be taken and sent to Technical Support. See [Taking a Field Server Diagnostic Capture](#) section.*

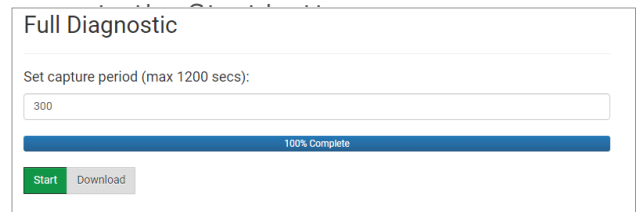
### Taking a Field Server Diagnostic Capture

**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 Field Server Diagnostics page via one of the following methods:
  - Open the Field Server GUI page, and click on Diagnostics in the Navigation panel.
  - Open the Field Server Toolbox software, and click the diagnose icon of the desired device.



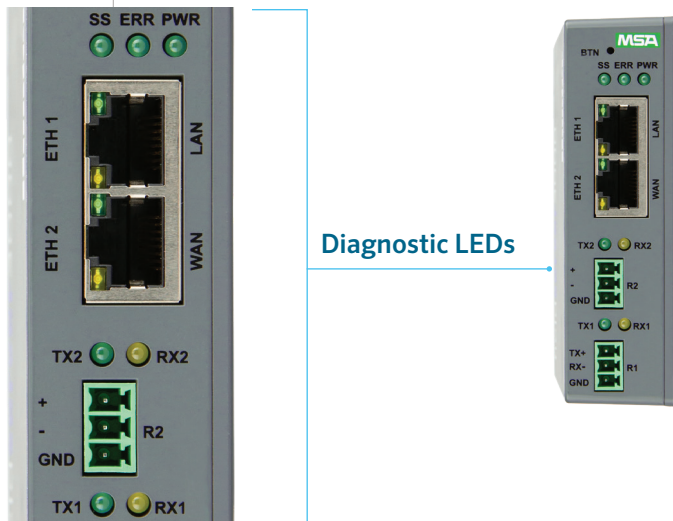
- Go to Full Diagnostic, and select the capture period.
- Click the Start button under the Full Diagnostic heading to start the capture.
  - When the capture is complete, a Download button will appear next to the Start button.



- Click Download for the capture to be downloaded to the local PC.
- Email the diagnostic zip file to Technical Support ([smc-support.emea@msasafety.com](mailto: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.*

## LED Functions



### TAG DESCRIPTION

<b>SS</b>	The SS LED will flash once a second to indicate that the bridge is in operation.
<b>ERR</b>	The SYS ERR LED will turn solid, indicating a system error. If this occurs, immediately report the related "system error" shown in the error screen of the Field Server GUI to Technical Support for evaluation.
<b>PWR</b>	The power light should always be a steady green when the unit is powered on.
<b>RX</b>	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.
<b>TX</b>	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.

## Factory Reset Instructions

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

## 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

fieldserver operating manual

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

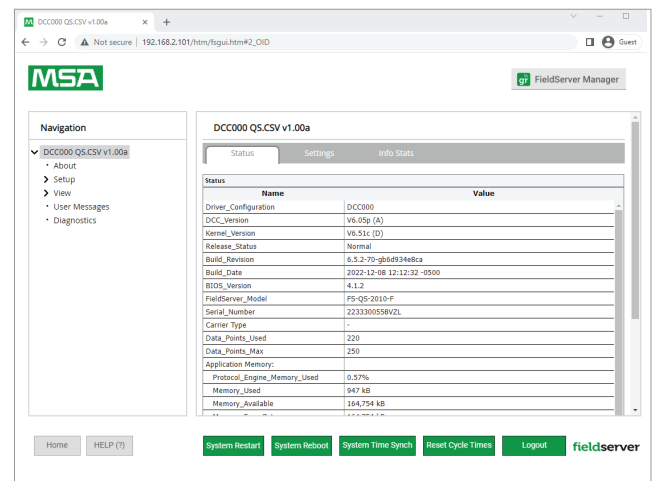
**NOTE:** Computer and network firewalls must be opened for Port 80 to allow the Field Server GUI to function.

## ADDITIONAL INFORMATION

### Changing Web Server Security Settings After Initial Setup

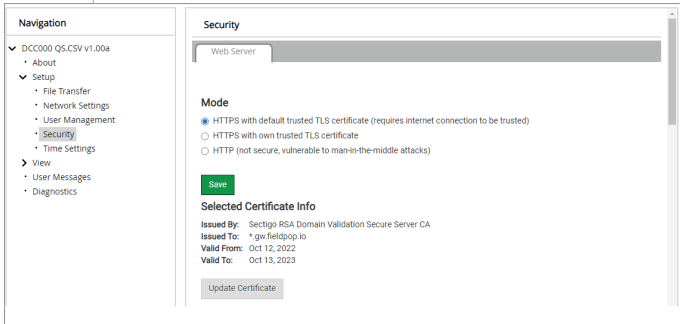
**NOTE:** Any changes will require a Field Server reboot to take effect.

- Navigate from the QuickServer landing page to the Field Server GUI by clicking the blue Diagnostics text on the bottom of the screen.
- The QuickServer landing page is the Field Server GUI.
- Click Setup in the Navigation panel.



## Changing Security Mode

- Click Security in the Navigation panel.

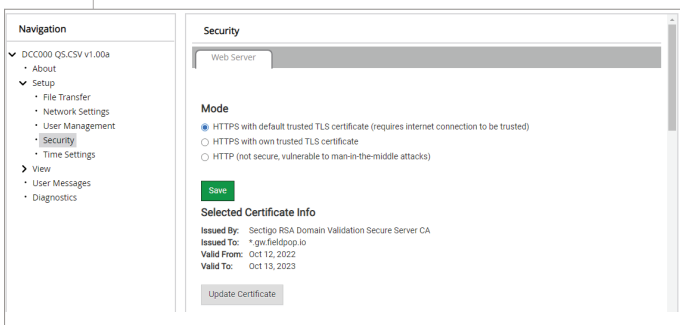


- Click the Mode desired.
  - If HTTPS with Own Trusted TLS Certificate is selected, follow instructions in the HTTPS with Own Trusted TLS Certificate section.
- Click the Save button.

## Editing the Certificate Loaded onto the Field Server

**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.



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

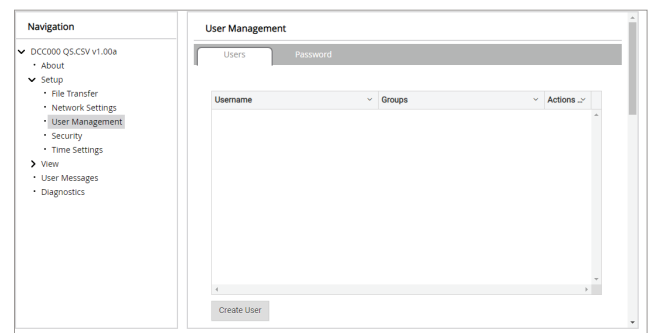
## Changing User Management Settings

- From the Field Server 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 *Field Server 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 Field Server reboot to take effect.

- Check that the Users tab is selected.



### User Types:

**Admin:** Can modify and view any settings on the Field Server.

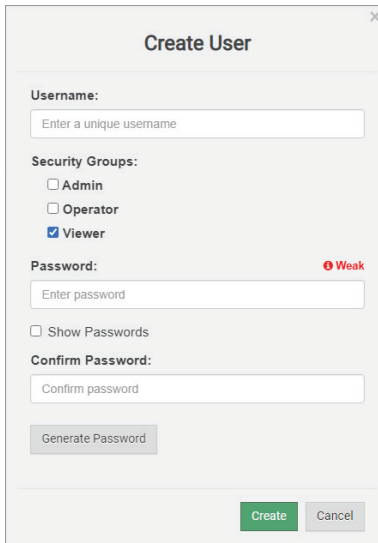
**Operator:** Can modify and view any data in the Field Server array(s).

**Viewer:** Can only view settings/readings on the Field Server.

- 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.

## Creating Users

- Click the Create User button.



The 'Create User' dialog box contains the following fields and controls:

- Username:** A text input field with the placeholder text 'Enter a unique username'.
- Security Groups:** Three radio button options: 'Admin', 'Operator', and 'Viewer'. The 'Viewer' option is selected.
- Password:** A text input field with the placeholder text 'Enter password'. A red 'Weak' indicator is visible to the right of the field.
- Show Passwords:** A checkbox that is currently unchecked.
- Confirm Password:** A text input field with the placeholder text 'Confirm password'.
- Generate Password:** A button located below the password fields.
- Create/Cancel:** Two buttons at the bottom right of the dialog.

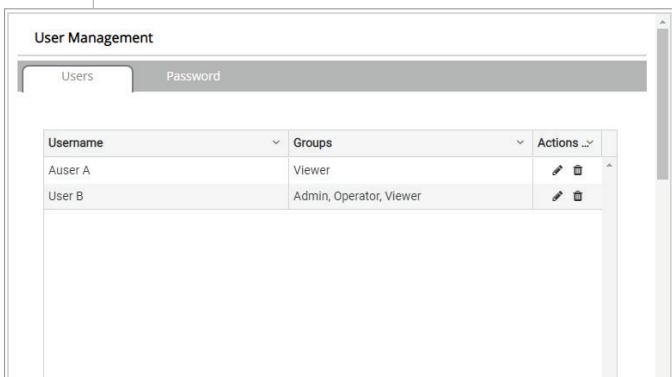
- Enter the new User fields: Name, Security Group, and Password.
  - User details are hashed and salted.

**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.

## Editing Users

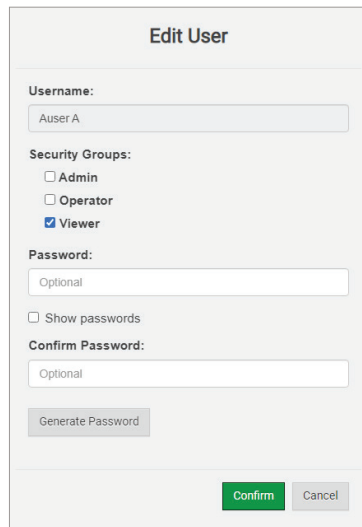
- Click the pencil icon next to the desired user to open the User Edit window.



The 'User Management' dialog box shows a table of users:

Username	Groups	Actions
Auser A	Viewer	[Pencil] [Trash]
User B	Admin, Operator, Viewer	[Pencil] [Trash]

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



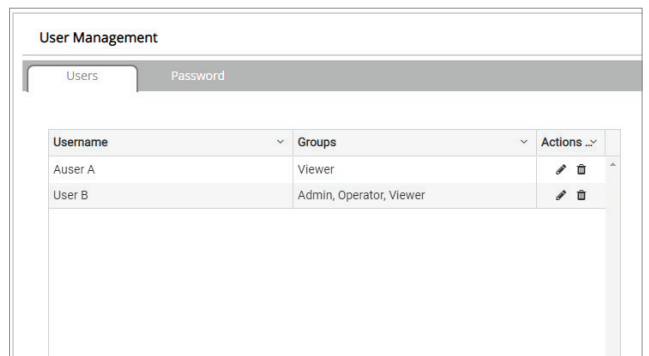
The 'Edit User' dialog box contains the following fields and controls:

- Username:** A text input field with the value 'Auser A'.
- Security Groups:** Three radio button options: 'Admin', 'Operator', and 'Viewer'. The 'Viewer' option is selected.
- Password:** A text input field with the placeholder text 'Optional'.
- Show Passwords:** A checkbox that is currently unchecked.
- Confirm Password:** A text input field with the placeholder text 'Optional'.
- Generate Password:** A button located below the password fields.
- Confirm/Cancel:** Two buttons at the bottom right of the dialog.

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

## Deleting Users

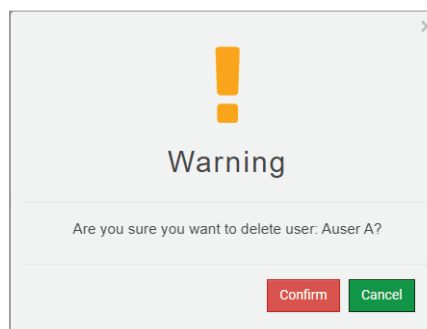
- Click the trash can icon next to the desired user to delete the entry.



The 'User Management' dialog box shows a table of users:

Username	Groups	Actions
Auser A	Viewer	[Pencil] [Trash]
User B	Admin, Operator, Viewer	[Pencil] [Trash]

- When the warning message appears, click Confirm.



The 'Warning' dialog box displays a large orange exclamation mark and the text:

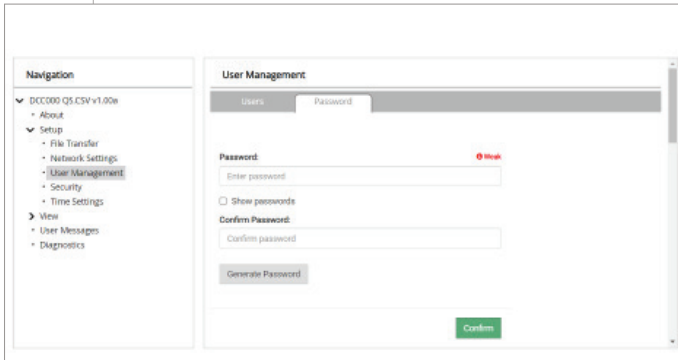
Warning

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

Buttons: Confirm (red), Cancel (green)

## Changing Field Server Password

- Click the Password tab.



- Change the general login password for the Field Server 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.

## Specifications



### FS-QS-3X10-F

#### Electrical Connections

One 3-pin Phoenix connector with: RS-485/RS-232 (Tx+ / Rx- / gnd)  
 One 3-pin Phoenix connector with: RS-485 (+ / - / gnd)  
 One 3-pin Phoenix connector with: Power port (+ / - / Frame-gnd)  
 Two Ethernet 10/100 BaseT port

#### Power Requirements

Input Voltage: 9 to 30 VDC or 24 VAC  
 Current draw: 24 VAC 0.125 A 9 to 30 VDC 0.25 A @12 VDC  
 Max Power: 3 W

#### Approvals

CE and FCC compliant, UL 62368-1, WEEE compliant ISED CAN ICES-003(B)/NBM-003(B), RoHS compliant, REACH compliant, UKCA compliant

#### Dimensions

4" x 1.1" x 2.7" (10.2 cm x 2.8 cm x 6.8 cm)

#### Weight

0.4 lb (0.2 kg)

#### Operating Temperature

-4°F to 158°F (-20°C to 70°C)

#### Humidity

10 to 95% RH non-condensing

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

## Warnings

### FCC Class B

**NOTE:** This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

### Compliance with EN IEC 62368-1

For EN IEC compliance, the following instructions must be met when operating the Field Server.



- The units shall be powered by a 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 Field Server
- Furthermore, the interconnecting power cable shall:
  - Be of length not exceeding 118.3" (3.1 m)
  - 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 149° F (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.

## LIMITED TWO-YEAR WARRANTY

Hunter Industries warrants its products to be free from defects in workmanship or material under normal use and service for two years after the date of shipment. Hunter Industries 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 Hunter Industries 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 Hunter Industries'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, Hunter Industries'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, Hunter Industries 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 Hunter Industries for damages including, but not limited to, consequential damages arising out of/or in connection with the use or performance of the product.

[hunterindustries.com/support/fs-3000-support](http://hunterindustries.com/support/fs-3000-support)



---

**HUNTER INDUSTRIES INCORPORATED** | *Built on Innovation*<sup>®</sup>  
1940 Diamond Street, San Marcos, California 92078 USA  
hunterindustries.com

© 2023 Hunter Industries Inc. Hunter, the Hunter logo, and all other trademarks are property of Hunter Industries, registered in the U.S. and other countries.