



Operating Manual

EZ Gateway Modbus to BACnet Start-up Guide



Revision: 3.D

Document No.:T18626

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 EZ Gateway	5
1.1	Certification	5
1.2	Supplied Equipment	5
2	Equipment Setup	6
2.1	Mounting	6
2.2	Physical Dimensions	7
3	Installation	8
3.1	DIP Switch Settings	8
3.1.1	Bias Resistors	8
3.1.2	Termination Resistor	9
3.2	Connecting the R1 & R2 Ports	10
3.2.1	Wiring	10
3.2.2	Supported RS-485 Baud Rates by Protocol	10
3.3	10/100 Ethernet Connection Port	11
4	Power up the Gateway	12
5	Connect the PC to the Gateway	13
5.1	Connecting to the Gateway via Ethernet	13
5.1.1	Changing the Subnet of the Connected PC	13
5.2	Navigate to the Login Page	13
6	Setup Web Server Security	14
6.1	Login to the FieldServer	14
6.2	Select the Security Mode	16
6.2.1	HTTPS with Own Trusted TLS Certificate	17
6.2.2	HTTPS with Default Untrusted Self-Signed TLS Certificate or HTTP with Built-in Payload Encryption	17
7	Configuring the EZ Gateway	18
7.1	Controls, Status and Log Functions	18
7.2	Setting up the Connections	19
7.3	Creating Device EZ Profiles	20
7.3.1	Using the Device Web Interface to Map BACnet Objects	21
7.3.2	Using Excel Profile Generator to Map BACnet Objects	23
7.3.3	Completing Device Profile Setup	24
7.3.4	Export Profile for Backup or Future Use	25
7.4	Importing a Device Profile	26
7.5	Mapping BACnet Output with Device EZ Profiles	27
7.6	Test and Commission the EZ Gateway	28
7.6.1	Accessing the FieldServer Manager	28
8	BACnet Explorer	29
8.1	Discover the Device List	30
8.2	View Device Details and Explore Points/Parameters	31
8.2.1	Edit the Present Value Field	34
9	MSA Grid - FieldSever Manager Setup	36

9.1	Choose Whether to Integrate the FieldServer Manager	36
9.2	User Setup	37
9.3	Registration Process	39
9.4	Login to the FieldServer Manager	43
10	Troubleshooting	45
10.1	Communicating with the EZ Gateway Over the Network	45
10.2	Taking a FieldServer Diagnostic Capture	46
10.3	LED Functions	47
10.4	Factory Reset Instructions	48
10.5	Internet Browser Software Support	48
11	Additional Information	49
11.1	Change Web Server Security Settings After Initial Setup	49
11.1.1	Change Security Mode	50
11.1.2	Edit the Certificate Loaded onto the FieldServer	51
11.2	Change User Management Settings	52
11.2.1	Create Users	53
11.2.2	Edit Users	54
11.2.3	Delete Users	55
11.2.4	Change FieldServer Password	56
11.3	Specifications	57
11.4	Compliance with UL Regulations	58
11.5	Address Types and Data Types	59
11.6	FieldServer Manager Connection Warning Message	60
12	Limited 2 Year Warranty	61

1 About the EZ Gateway

EZ Gateway is a high performance, cost effective building and industrial automation multi-protocol gateway providing protocol translation between serial and Ethernet, devices and networks.

NOTE: For troubleshooting assistance refer to **Section 10 Troubleshooting**, or any of the troubleshooting appendices in the related driver supplements. Check the **MSA Safety website** for technical support resources and documentation that may be of assistance.

The EZ Gateway is cloud ready and connects with MSA Safety's Grid FieldServer Manager. See **Section 7.6.1 Accessing the FieldServer Manager** 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.*

1.2 Supplied Equipment

FieldServer Gateway

- Preloaded with the Modbus and BACnet drivers.
- All instruction manuals, driver manuals, support utilities are available on the USB drive provided in the optional accessory kit, or on the MSA website.

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

- 7-ft Cat-5 cable with RJ45 connectors at both ends
- Power Supply -110/220V (p/n 69196)
- Screwdriver for connecting to terminals
- USB Flash drive loaded with:
 - Start-up Guide
 - FieldServer Configuration Manual
 - All FieldServer Driver Manuals
 - Support Utilities
 - Any additional folders related to special files configured for a specific FieldServer
 - Additional components as required - see driver manual supplement for details

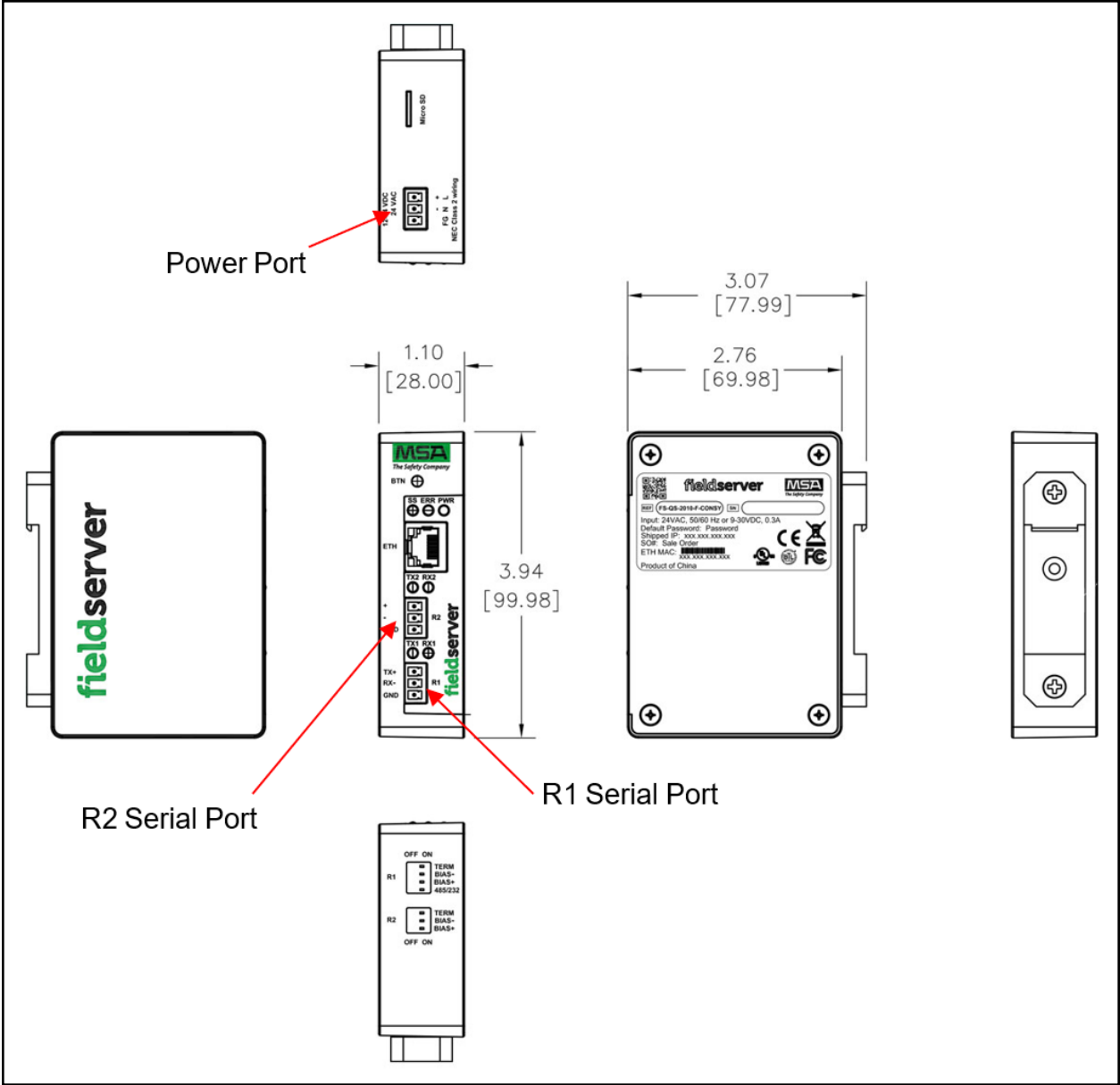
2 Equipment Setup

2.1 Mounting

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



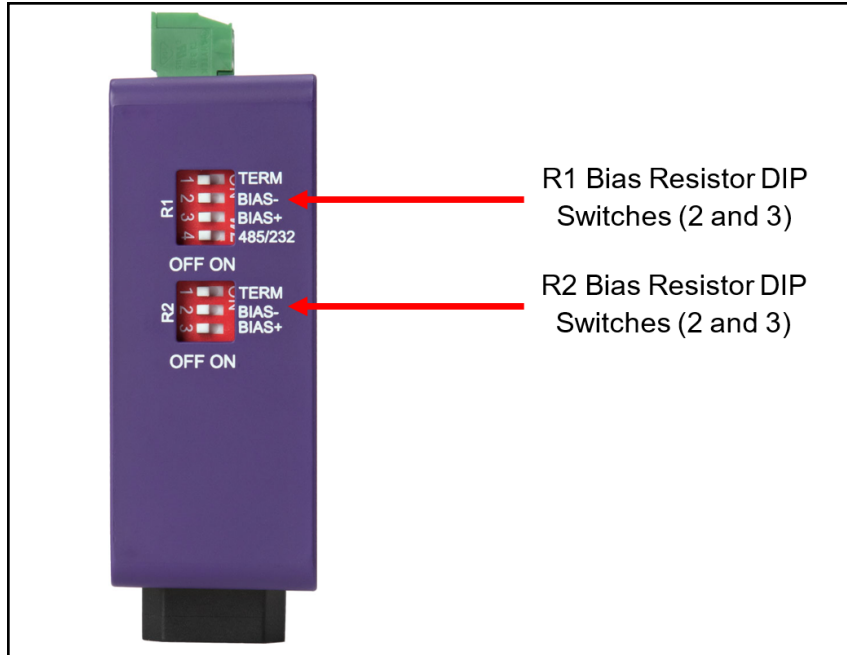
2.2 Physical Dimensions



3 Installation

3.1 DIP Switch Settings

3.1.1 Bias Resistors



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.

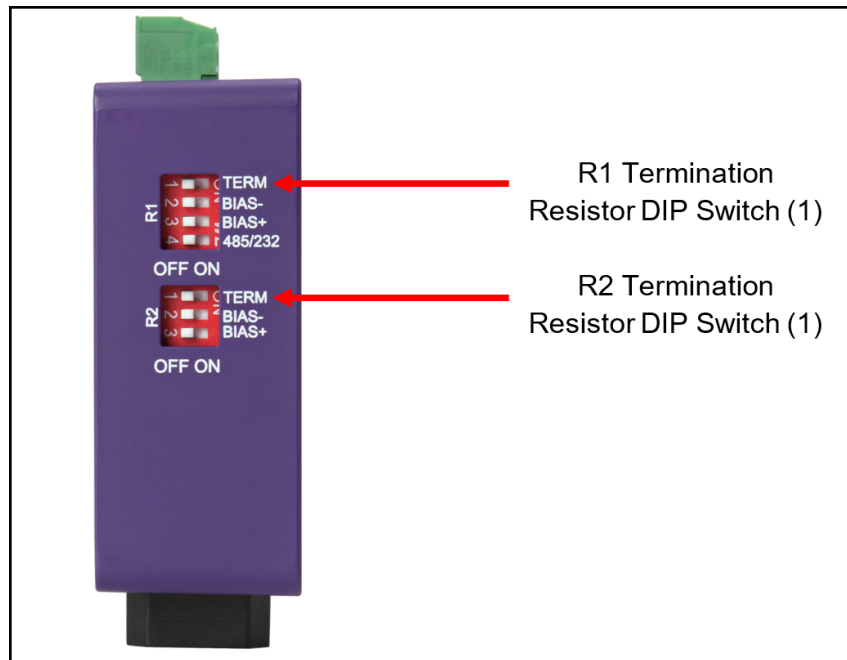
The bias resistor is 510 ohms which is in line with the BACnet spec. It should only be enabled at one point on the bus (for example, on the field port where there are very weak bias resistors of 100k). Since there are no jumpers, many EZ Gateways can be put on the network without running into the bias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

NOTE: See the [Termination and Bias Resistance Enote](#) 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.

3.1.2 Termination Resistor



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

Termination resistor is also used to reduce noise. It pulls the two lines of an idle bus together. However, the resistor would override the effect of any bias resistors if connected.

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

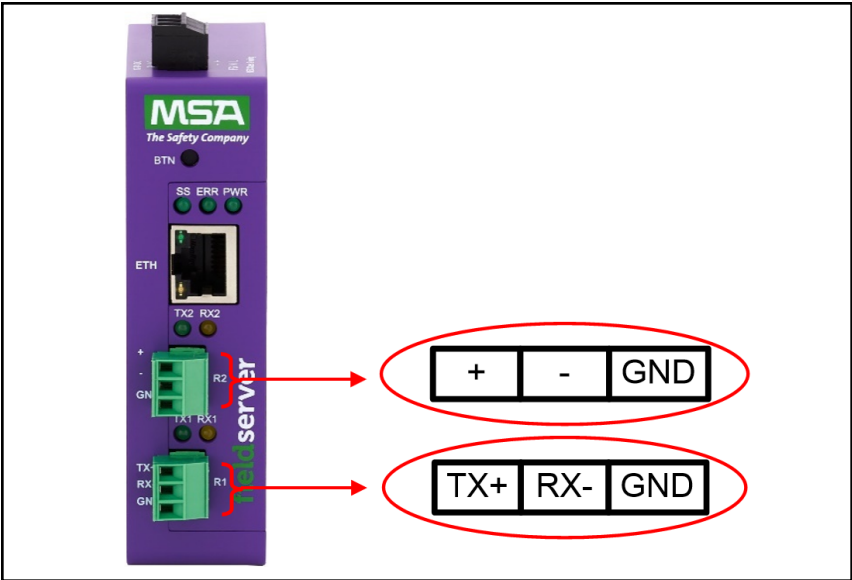
NOTE: If the gateway is already powered on, DIP switch settings will not take effect unless the unit is power cycled.

3.2 Connecting the R1 & R2 Ports

For the R1 Port only: Switch between RS-485 and RS-232 by moving the number 4 DIP Switch left for RS-485 and right for RS-232 (see images in **Section 3.1 DIP Switch Settings**).

The R2 Port is RS-485.

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



3.2.1 Wiring

RS-485		RS-232	
BMS RS-485 Wiring	Gateway Pin Assignment	BMS RS-485 Wiring	Gateway Pin Assignment
RS-485 +	TX +	RS-232 -	TX +
RS-485 -	RX -	RS-232 +	RX -
GND	GND	GND	GND

NOTE: Use standard grounding principles for GND.

3.2.2 Supported RS-485 Baud Rates by Protocol

The supported baud rates for either port is based on the protocol of the connected devices.

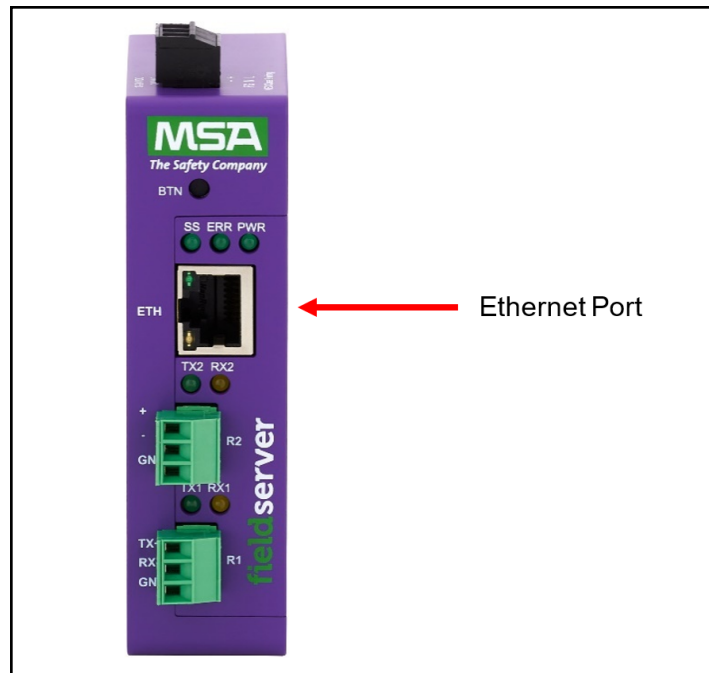
The following baud rates are supported for Modbus RTU:

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

The following baud rates are supported for BACnet MS/TP:

9600, 19200, 38400, 76800, 115200

3.3 10/100 Ethernet Connection Port



The Ethernet Port is used both for Ethernet protocol communications and for configuring the gateway via the Web App. To connect the gateway, either connect the PC to the router's Ethernet port or connect the router and PC to an Ethernet switch. Use Cat-5 cables for the connection.

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

4 Power up the Gateway

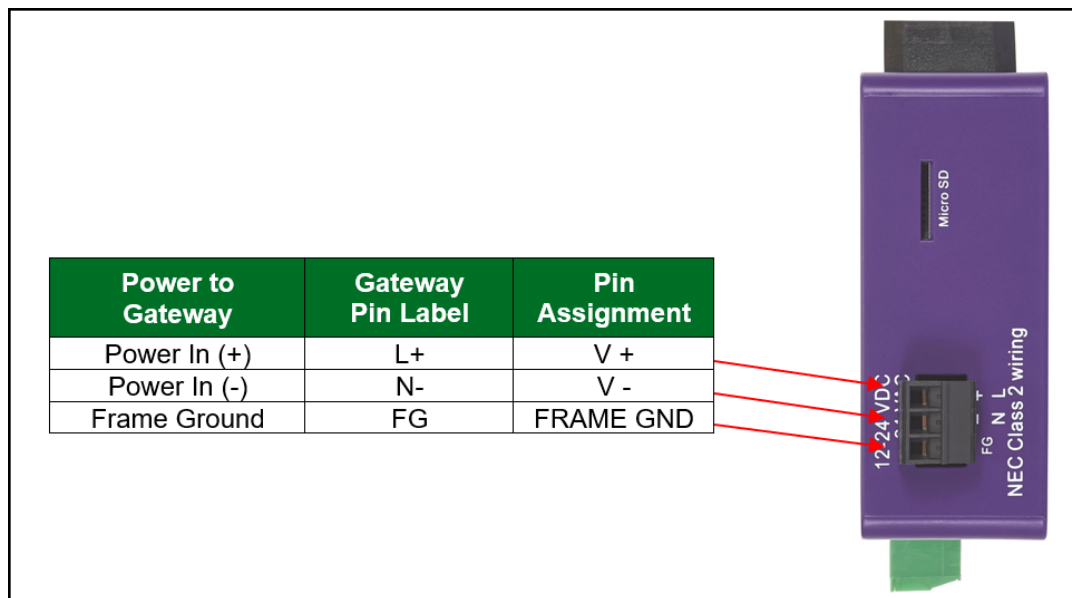
Check power requirements in the table below:

Power Requirement for EZ Gateway External Gateway		
EZ Gateway Family	Current Draw Type	
	12VDC	24VDC/AC
FS-EZ3-MOD-BAC (Typical)	250mA	125mA
FS-EZ4-MOD-BAC (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 EZ Gateway as shown below. Ensure that the power supply used complies with the specifications provided in **Section 11.3 Specifications**.

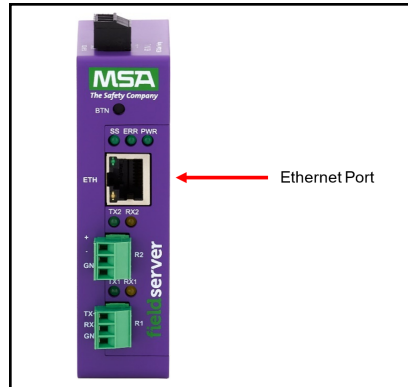
- The gateway accepts 9-30VDC or 24VAC on pins L+ and N-.
- Frame GND should be connected.



5 Connect the PC to the Gateway

5.1 Connecting to the Gateway via Ethernet


Connect a Cat-5 Ethernet cable (straight through or cross-over) between the local PC and EZ Gateway .

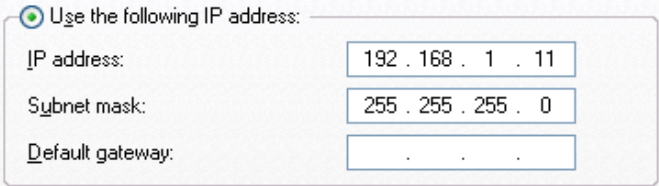


5.1.1 Changing the Subnet of the Connected PC

The default IP Address for the EZ Gateway is **192.168.2.101**, Subnet Mask is **255.255.255.0**. If the PC and EZ Gateway are on different IP networks, assign a static IP Address to the PC on the 192.168.2.xxx network.

For Windows 10:

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



Use the following IP address:	
IP address:	192 . 168 . 1 . 11
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	. . .

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

5.2 Navigate to the Login Page

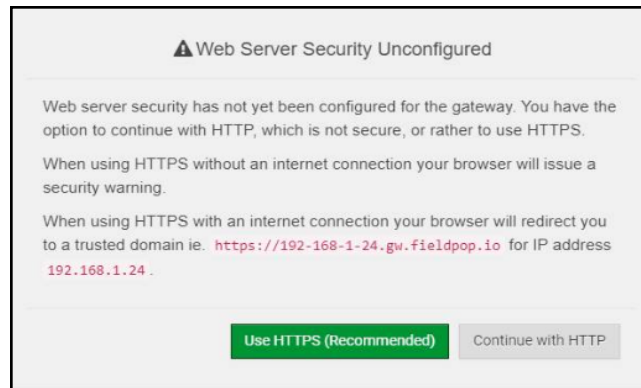
- Open a web browser and connect to the FieldServer's default IP Address. The default IP Address of the FieldServer is **192.168.2.101**, Subnet Mask is **255.255.255.0**.
- If the PC and the FieldServer are on different IP networks, assign a static IP Address to the PC on the 192.168.2.X network.

6 Setup Web Server Security

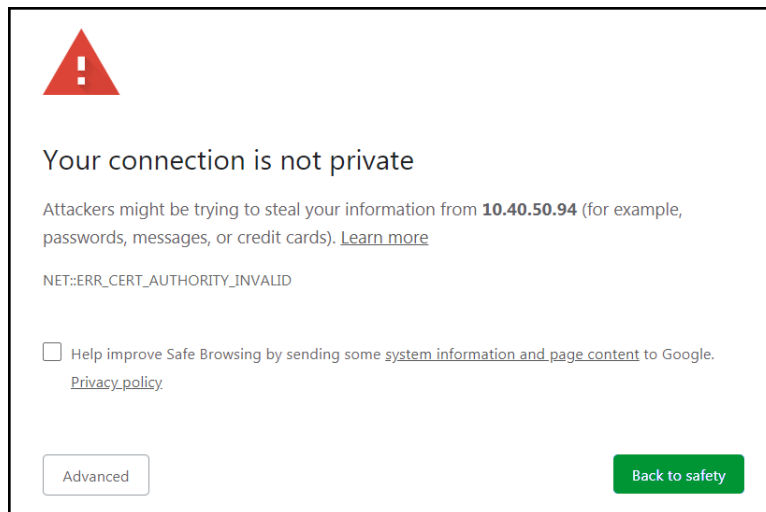
6.1 Login to the FieldServer

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

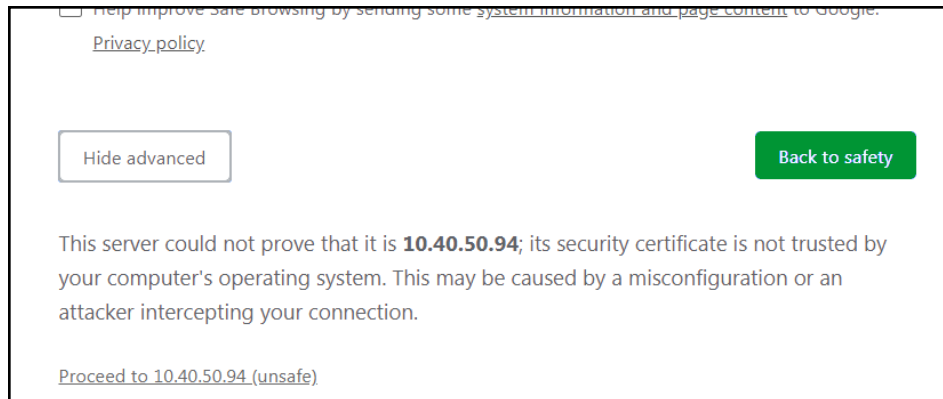
- When the Web Server Security Unconfigured window appears, read the text and choose whether to move forward with HTTPS or HTTP.



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

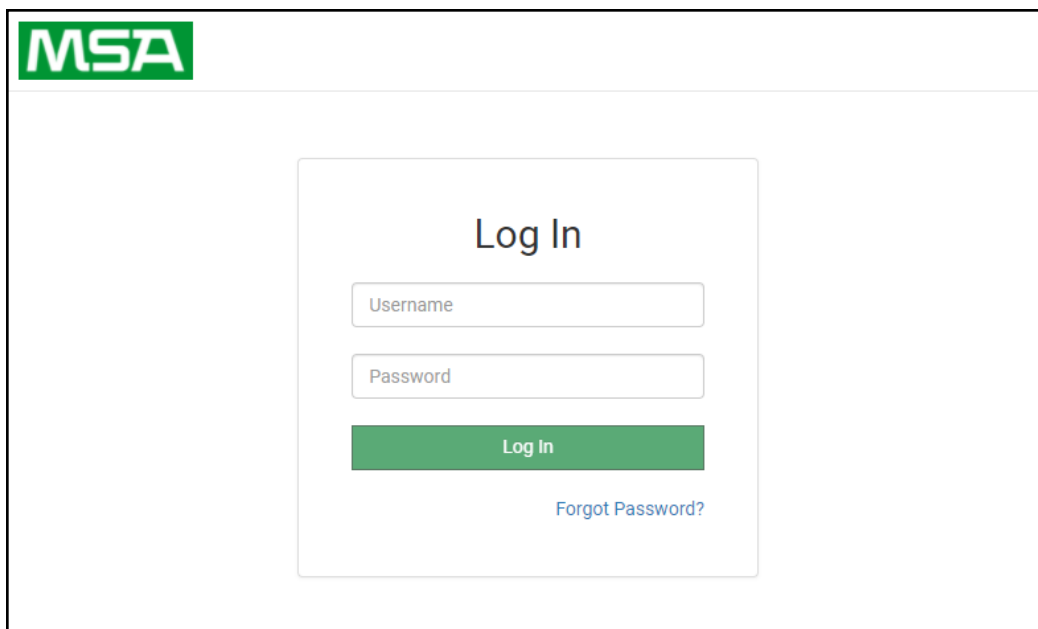


- Additional text will expand below the warning, click the underlined text to go to the IP Address. In the example below this text is “[Proceed to 10.40.50.94 \(unsafe\)](#)”.



- 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 [11.2 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 11.1 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+qEr0lQo2wvmhyc7L22UXse1NoOfU2Zg0Eu1Vtu
JRryaMWIRFEWuuzMGZtKFWVC+8q2JQsVcgrWm7naoblEhOCMH+sKHJMCxDoXGt
vtZjpZUoAL51YXxWSVcyZdGiAP5e
-----END CERTIFICATE-----
```

Private Key

```
sHB0zZoHr4YQSDk2BbYVzbl0LDuKtc8+JiO3ooGjoTuHnqkeAj/fKfbTAsKeAzw
gKQe+H5UQNk0bdvZfOJrm6daDK2vVDmR5k+jUUhEj5N49uplroB97MQgYotzqfT+
THlbp5t1SIK617k04ObKmHF5l8fck+ru545sVmpeeZh0m5j5SURYAZMvbq5daCu
J4l5NIihbEvxRF4UK41ZDMCvujopCbkUWrb1a/3XXnDnM2K9xyz2wze998D6Wk46
+7aOFY9F+7j5jmnkoS3GYtwCyH5jP+mPP1K6RnuiD019wvGPb4dtN/RTnfd0eF
GYeVSkI9fxkxDOFtdWRZbM/rPin4tmO1Xf8HqONVN1x/iaMynOXG4cukoi4+VO
u0rZaUESlI2zNkfrn7fAASm5NBWg202Cy9lAYnuujs3aALl5uGBEEK62oTMxlzx
-----END RSA PRIVATE KEY-----
```

Private Key Passphrase

Save

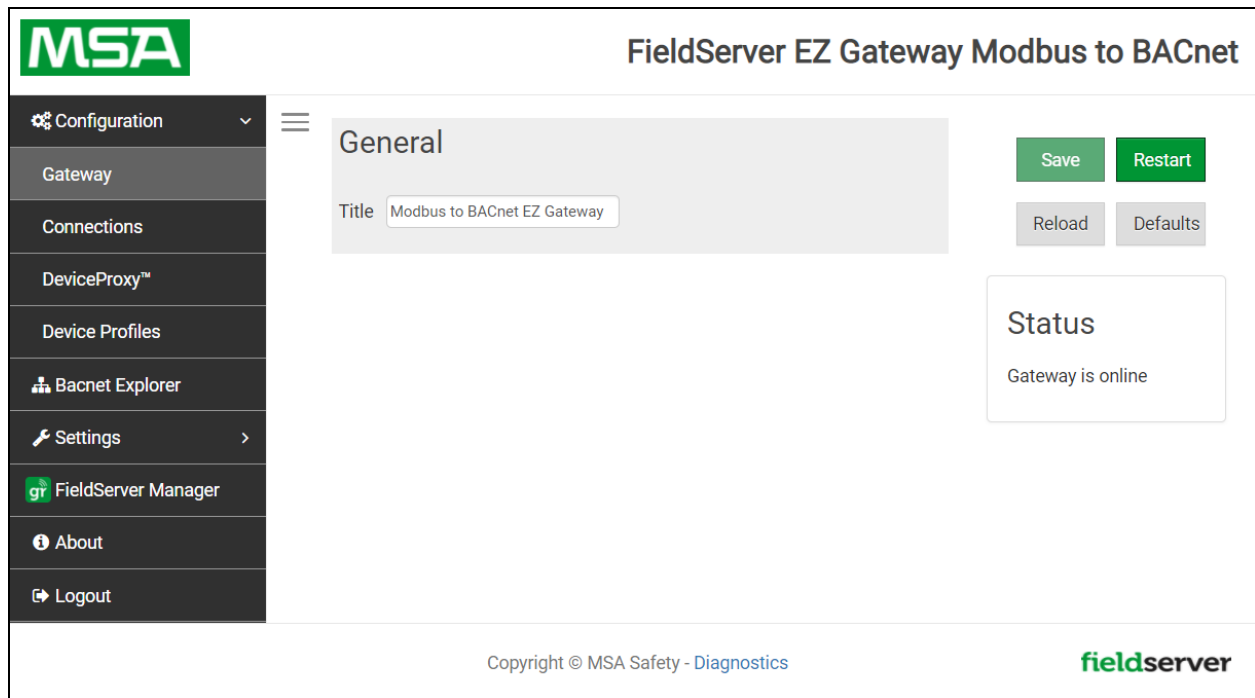
- Copy and paste the Certificate and Private Key text into their respective fields. If the Private Key is encrypted type in the associated Passphrase.
- Click Save.
- A “Redirecting” message will appear. After a short time, the FieldServer GUI will open.

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 Configuring the EZ Gateway

Once the web server setup is complete, the EZ Gateway landing page will appear.



NOTE: The FieldServer Manager tab  FieldServer Manager (see screenshot 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 Controls, Status and Log Functions

Along the right side of every Web Configurator GUI page is a column of buttons and event generated messages.

- Controls Panel – Contains the following four buttons:
 - Reload – Resets all settings to the last saved configuration
 - Defaults – Resets all settings to the default configuration
 - Save – Records all settings
 - Restart – Reboots the Gateway
- Status Information – Shows Gateway messages such as whether the Gateway is online, element validation status, unsaved settings, etc.

7.2 Setting up the Connections

- Open the Connections page to configure the connection ports and parameters.

MSA FieldServer EZ Gateway Modbus to BACnet

Configuration **Gateway** **Connections** **DeviceProxy™** **Device Profiles** **Bacnet Explorer** **Settings** **FieldServer Manager** **About** **Logout**

Modbus RTU R1

Enable ☒

Baud Rate 9600

Parity None

Data Bits 8

Stop Bits 1

Poll Delay 0.1

Modbus RTU R2

Enable ☐

Baud Rate 9600

Parity None

Data Bits 8

Stop Bits 1

Poll Delay 0.1

Modbus TCP

Enable ☒

Poll Delay 0.1

Max Concurrent Messages 1

BACnet IP

Enable ☒

IP Port 47808

Enable BBMD ☐

Public IP Address -

Public IP Port -

BACnet IP Settings

Virtual Network Number 1100

Internal Network Number 1 1200

Internal Network Number 2 1201

BACnet MSTP R1

Enable ☐

Baud Rate 38400

Parity None

Data Bits 8

Stop Bits 1

Mode Master

Max Master 127

Max Info Frames 1

MAC Address 1

BACnet MSTP R2

Enable ☒

Baud Rate 38400

Parity None

Data Bits 8

Stop Bits 1

Mode Master

Max Master 127

Max Info Frames 1

MAC Address 2

Save **Restart**

Reload **Defaults**

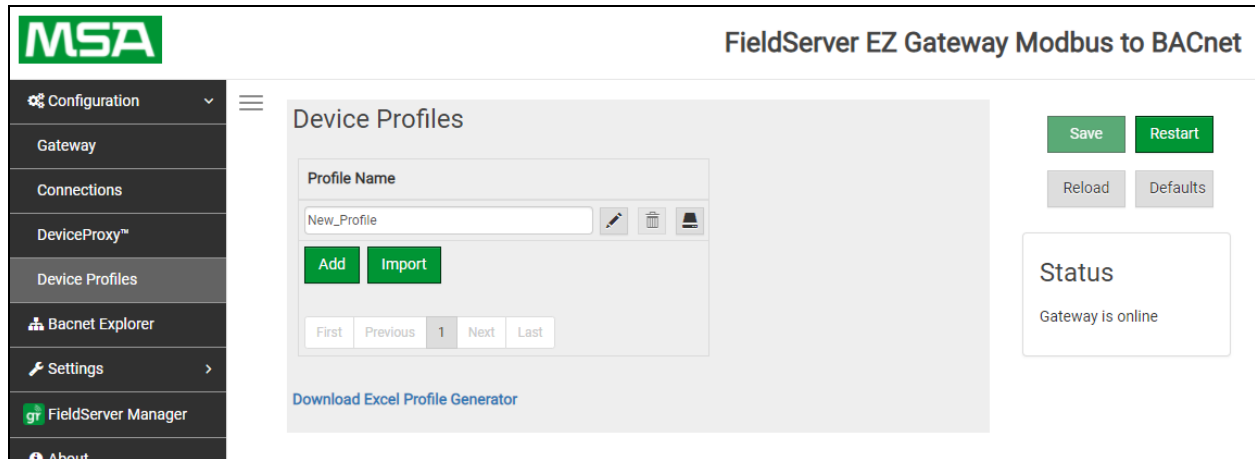
Status

Gateway is online

- Click the Save button in the Controls section once completed.
- Then click Restart to implement the new settings.

7.3 Creating Device EZ Profiles

- Open the Device Profiles page to create a new profile.



- Create a data map using one of two methods:
 - Create Modbus to BACnet mapping using the Web Interface ([Section 7.3.1 Using the Device Web Interface to Map BACnet Objects](#))
 - Create Modbus to BACnet mapping using Excel Profile Generator ([Section 7.3.2 Using Excel Profile Generator to Map BACnet Objects](#))
- After saving the data map, complete the profile setup by updating State Tables and Notification Classes as needed. ([Section 7.3.3 Completing Device Profile Setup](#))

7.3.1 Using the Device Web Interface to Map BACnet Objects

NOTE: The Add button creates another blank profile that must be mapped using the Web Interface.

- Click on the Edit button (pencil icon) next to the name of the profile to map.
- Enter the Modbus and BACnet parameters.

NOTE: See Section 11.5 [Address Types and Data Types](#) for additional information on Address Type.

The 'Edit Profile' dialog box is shown with the 'Device Settings' tab selected. The 'Data Map' tab is also visible. The 'Modbus' section includes 'Address Type' (Application Data Unit), 'Enable Write Multiple' (unchecked), and 'Write Length' (1). The 'BACnet' section includes 'Enable COV' (checked). At the bottom are 'Cancel', 'Reload', and 'Save' buttons.

Modbus
Address Type: Application Data Unit
Enable Write Multiple: <input type="checkbox"/>
Write Length: 1

BACnet
Enable COV: <input checked="" type="checkbox"/>

- Click on the Data Map tab and add the first Modbus address range.

The 'Edit Profile' dialog box is shown with the 'Data Map' tab selected. A table with columns: Address, Data Type, Function, Length, Scan Interval, and Signed Value is displayed. The first row contains: 1, Holding Register, Read Continuously, 1, 1, and an unchecked checkbox. Below the table is an 'Add' button and a pagination bar (First, Previous, 1, Next, Last). At the bottom are 'Cancel', 'Reload', and 'Save' buttons.

Address	Data Type	Function	Length	Scan Interval	Signed Value
1	Holding Register	Read Continuously	1	1	<input type="checkbox"/>

NOTE: Check the Signed Value checkbox (right of the data map entry) if signed values are needed.

- Click on the blue plus sign icon on the left side of the Address to map the BACnet Addresses to the Modbus Registers.

Edit Profile

Device Settings

Data Map

State Tables

Notification Classes

Address	Data Type	Function	Length	Scan Interval	Signed Value
+ 1	Holding Register	Read Continuously	1	1	<input type="checkbox"/>
- 2	Holding Register	Read Continuously	4	.01	<input type="checkbox"/>

Data Offset	Object Name	Object Type	Object Instance	Units	Description	Advanced
1	Device 1	Analog Input	1	-	-	
2	Device 2	Analog Value	2	-	-	
3	Device 3	Binary Value	3	-	-	

Add

First

Previous

1

Next

Last

Add

First

Previous

1

Next

Last

Cancel

Reload

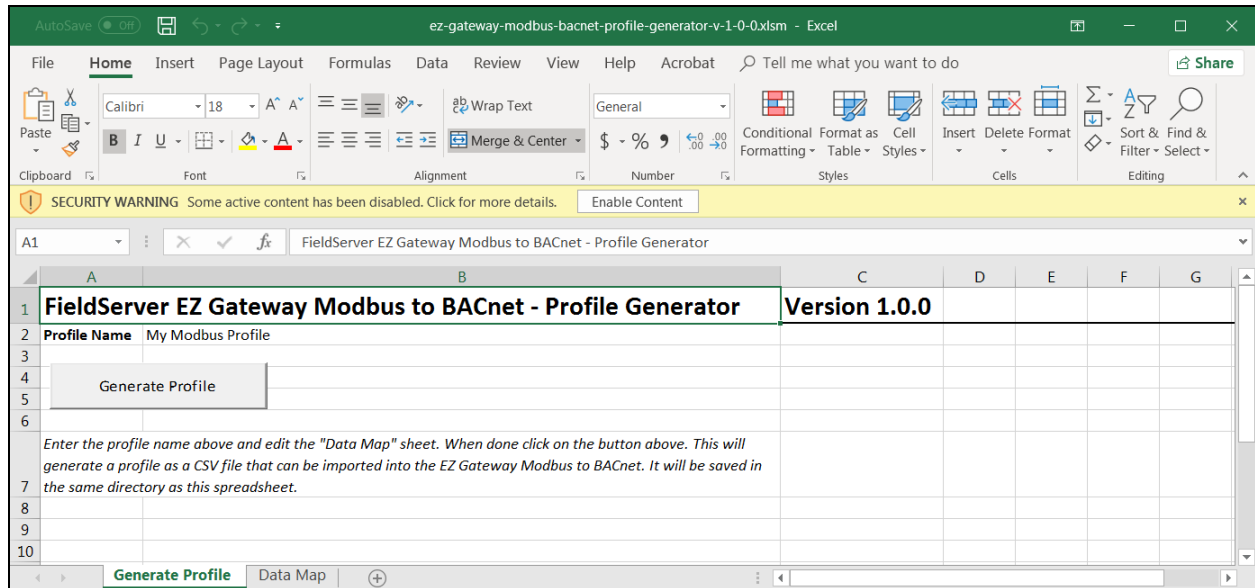
Save

NOTE: The Advanced button (eye icon) allows additional settings, including: Intrinsic Reporting, Bit Extraction, scaling and more.

- Repeat for all of the Modbus registers.
- Once all mappings are defined, click the Save button in the bottom left corner of the window to record the Profile.

7.3.2 Using Excel Profile Generator to Map BACnet Objects

- From the Device Profiles page ([Section 7.3 Creating Device EZ Profiles](#)), click on the “Download Excel Profile Generator” link to download the Excel spreadsheet used to create the profile to the default download folder on the local PC.
- Open the downloaded Excel spreadsheet and ensure that the content is not disabled by security settings (yellow security warning bar across the top of the spread sheet).



NOTE: If the security warning is present simply click the **Enable Content** button found at the end of the warning.

- Click the Data Map tab (near the bottom of the Excel spreadsheet).
- Edit or copy in Modbus registers as needed.
- Once all the point mappings are complete, switch back to the Generate Profile tab.
- Click the Generate Profile button to create a new Excel .csv file titled “My Modbus Profile”.
- Go back to the EZ Gateway Device Profiles page ([Section 7.3 Creating Device EZ Profiles](#)) and click the Import button.
- Select the Excel .csv file and click the checkbox to load the mapping.
- Once all mappings are loaded, click Save in the Controls section.

7.3.3 Completing Device Profile Setup

- Click on the Edit button (pencil icon) next to the name of the profile to complete setup.
- If a data map was loaded from a file created from the “Excel Profile Generator”, go to the Device Settings tab to enter the Modbus and BACnet parameters.

NOTE: See Section 11.5 [Address Types and Data Types](#) for additional information on Address Type.

The 'Edit Profile' dialog box is shown with the 'Device Settings' tab selected. The 'Modbus' section includes 'Address Type' (Application Data Unit), 'Enable Write Multiple' (unchecked), and 'Write Length' (1). The 'BACnet' section includes 'Enable COV' (checked). Buttons for 'Cancel', 'Reload', and 'Save' are at the bottom right.

Modbus
Address Type: Application Data Unit
Enable Write Multiple: <input type="checkbox"/>
Write Length: 1

BACnet
Enable COV: <input checked="" type="checkbox"/>

- If using a BACnet State Table, click on the “State Table” tab to define the table and its variables.

The 'Edit Profile' dialog box is shown with the 'State Tables' tab selected. It displays a list of table names ('New_Table', 'New_Table2') and a table with columns 'State Value', 'State Text', and 'State Class'. The table contains three rows: (1, State1, Normal), (2, State2, Alarm), and (3, State3, Fault). Buttons for 'Add', 'First', 'Previous', 'Next', 'Last', 'Cancel', 'Reload', and 'Save' are present.

Table Name
+ New_Table
- New_Table2

State Value	State Text	State Class
1	State1	Normal
2	State2	Alarm
3	State3	Fault

NOTE: The Table Name field must be 14 characters or less. No commas allowed. The State Text field must be 50 characters or less. No commas allowed.

- To define a Notification Class, click the “Notification Class” tab and define the parameters as needed.

Edit Profile

Device Settings | Data Map | State Tables | **Notification Classes**

Address	Data Type	Function	Length	Scan Interval	Signed Value
+ 1	Holding Register	Read Continuously	1	1	<input type="checkbox"/>
- 2	Holding Register	Read Continuously	4	.01	<input type="checkbox"/>

Data Offset	Object Name	Object Type	Object Instance	Units	Description	Advanced
1	Device 1	Analog Input	1	-	-	<input type="checkbox"/>
2	Device 2	Analog Value	2	-	-	<input type="checkbox"/>
3	Device 3	Binary Value	3	-	-	<input type="checkbox"/>

Add

First Previous **1** Next Last

Add

First Previous **1** Next Last

Cancel Reload **Save**

- Once all settings are defined, click the Save button.

7.3.4 Export Profile for Backup or Future Use

- Back on the Device Profiles page, the profile can be exported for backup or future use by hitting the Export Profile button (hard drive icon).

Device Profiles

Profile Name

New_Profile

Add **Import**

First Previous **1** Next Last

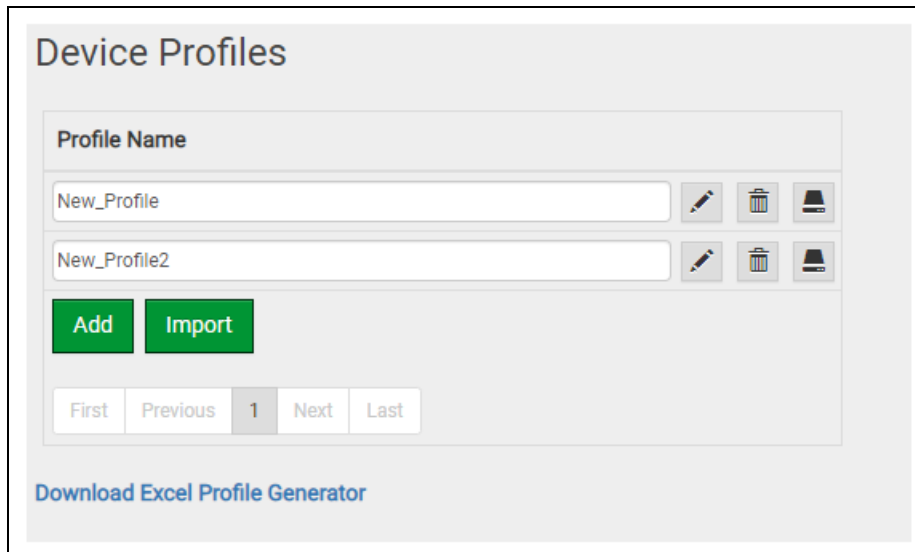
[Download Excel Profile Generator](#)

Export profile

- The profile downloads to the local computer in the format: <Profile Name>.profile.

7.4 Importing a Device Profile

- Profiles on the local computer can be imported to the EZ Gateway by going to the Device Profiles page and clicking the Import button.



The screenshot shows the 'Device Profiles' page. At the top, there's a title 'Device Profiles'. Below it, there's a section titled 'Profile Name' containing two input fields. The first field contains 'New_Profile' and the second contains 'New_Profile2'. To the right of each input field are three icons: a pencil (edit), a trash can (delete), and a document with a plus sign (add). Below the input fields are two green buttons: 'Add' and 'Import'. At the bottom of the section, there's a pagination bar with buttons: 'First', 'Previous', '1' (selected), 'Next', and 'Last'. Below the entire section is a blue link that says 'Download Excel Profile Generator'.

NOTE: All profiles will need to be created or imported to the EZ Gateway before proceeding.

NOTE: There are two types of files that can be imported. The Excel spreadsheet generated files (Section [7.3.2 Using Excel Profile Generator to Map BACnet Objects](#)) or an exported profile (Section [7.3.4 Export Profile for Backup or Future Use](#)). Files generated from the downloaded “Excel Profile Generator” only include Data Map information and must be completed by going through the steps found in Section [7.3.3 Completing Device Profile Setup](#) after being loaded. However, exported profiles include complete profile information and can be used immediately after load up.

7.5 Mapping BACnet Output with Device EZ Profiles

- Open the DeviceProxy™ page.
- Choose the Device Profile to load from the drop down menu.

MSA FieldServer EZ Gateway Modbus to BACnet

DeviceProxy™

Device Profile	Modbus Connection	BACnet Connection	Modbus Node ID	Modbus Node IP Address	Modbus Node IP Port	BACnet Device Instance	BACnet Device Name	Advanced
New_Profil	N1 (Modbi	N1 (BACne	1	192.168.1.1	502	34293	Meter_1	
New_Profil	N1 (Modbi	N1 (BACne	1	192.168.1.2	502	32494	Meter_2	

Add

First Previous 1 Next Last

Save Restart

Reload Defaults

Status

Gateway is online

Configuration update complete. Please restart the system to load the new Configuration. There are unsaved changes

NOTE: If required, click the Advanced Settings button (eye icon) to enter the Device Description and Device Location.

Advanced

BACnet Device

Device Description Device1

Device Location Milpitas, CA

Apply

- Choose the appropriate connection and Node ID/BACnet Device Instance for both the incoming Modbus device and the mapped BACnet output.
- Click Add to include additional device profiles in the Configuration.
- Repeat for all Modbus devices intended to connect to the EZ Gateway.
- Click the Save button on the right side of the screen once all device EZ Profiles are added and then click the Restart button to reset the system.

Save Restart

Reload Defaults

7.6 Test and Commission the EZ Gateway

- Connect the EZ Gateway to the third party device(s), and test the application.
- Click on the Diagnostic button to view to get to the FS-GUI.
- 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.

The screenshot displays the MSA FieldServer Manager web interface. On the left is a navigation tree under 'Modbus to BACnet EZ Gateway' with options like About, Setup, View, and Connections (selected). The main area shows the 'Connections' tab with a table of connection statistics.

Index	Name	Tx Msg	Rx Msg	Tx Char	Rx Char	Errors
0	R1 - MODBUS_RTU	9,134	0	73,072	0	9,134
1	ETH1 - Modbus/TCP	0	0	0	0	0
2	ETH1 - BACnet_IP 47800	7,831	3	14	28	0
3	ETH1 - BACnet_IP	333	4,568	0	122	0
4	R2 - BACnet_MSTP	12	0	0	0	0

At the bottom of the interface are buttons for Home, HELP (?), Contact Us, Reset Statistics, and Logout, along with the fieldserver logo.

NOTE: For troubleshooting assistance refer to [Section 10 Troubleshooting](#), or any of the troubleshooting appendices in the related driver supplements and configuration manual. MSA Safety also offers a technical support on the MSA Safety website, which contains a significant number of resources and documentation that may be of assistance.

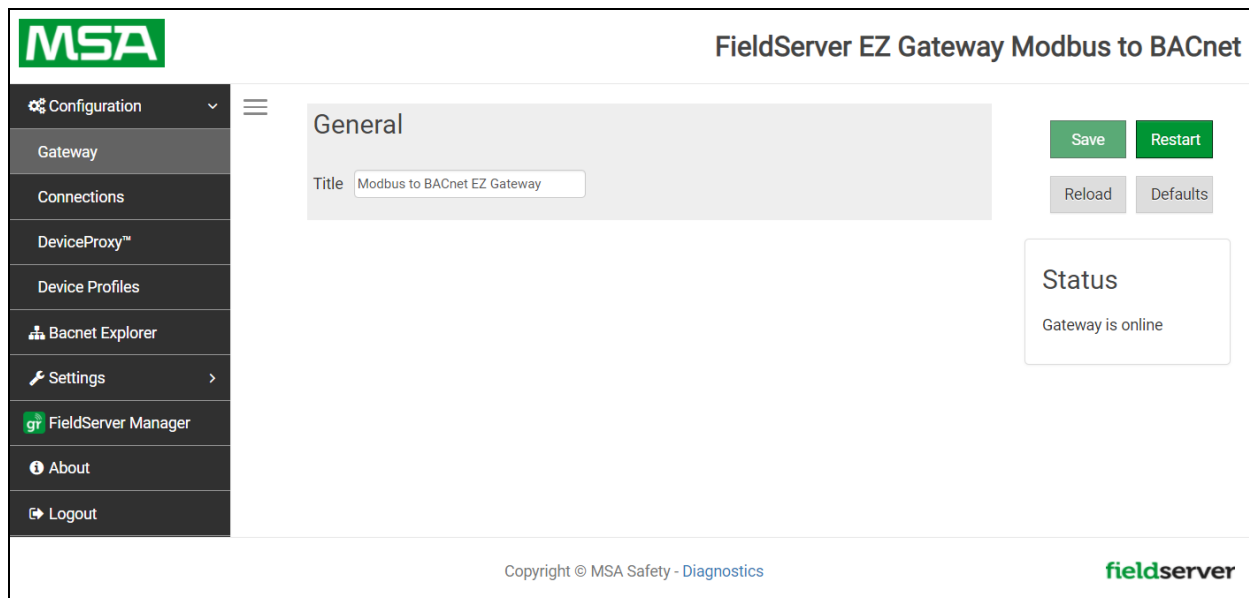
7.6.1 Accessing the FieldServer Manager

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](#).

8 BACnet Explorer

The BACnet Explorer tab allows installers to validate that their equipment is working on BACnet without having to ask the BMS integrator to test the unit.

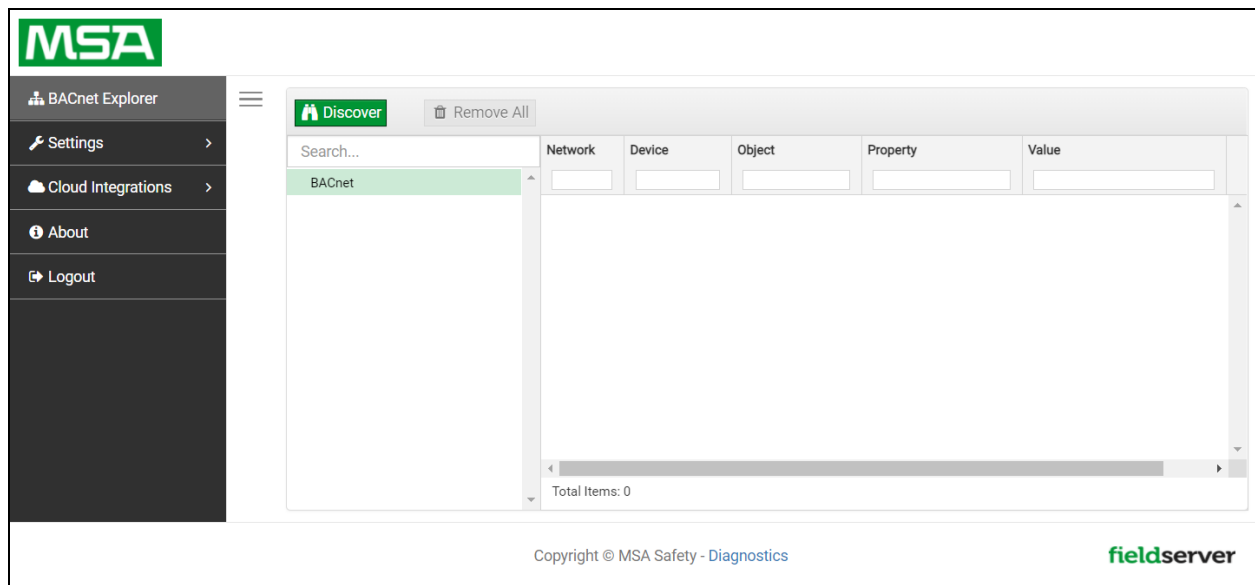
- To access the embedded BACnet Explorer click the BACnet Explorer tab.




NOTE: For BACnet/IP, click on the Connections tab to ensure the gateway is on the BACnet/IP network subnet to configure BBMD.

8.1 Discover the Device List

- From the BACnet Explorer landing page, click on the BACnet Explorer tab on the left side of the screen to go to the BACnet Explorer page.



- Find devices connected to the same subnet as the gateway by clicking the Discover button  (binocular icon).
- This opens the Discover window, click the checkboxes next to the desired settings and click Discover to start the search.

The Discover window is titled 'Discover' with a binocular icon. It contains two main sections: 'Devices' and 'Networks'. Under 'Devices', there is a checkbox for 'Discover All Devices' and input fields for 'From device' (0) and 'to device' (4194303). Under 'Networks', there is a checkbox for 'Discover All Networks' and an input field for 'Discover Specific Network' (0). At the bottom right are 'Cancel' and 'Discover' buttons.

NOTE: The “Discover All Devices” or “Discover All Networks” checkboxes must be unchecked to search for a specific device range or network.

NOTE: Allow the devices to populate before interacting with the device list for optimal performance. Any discovery or explore process will cause a green message to appear in the upper right corner of the browser to confirm that the action is complete.

Search...	Device	Object	Property	Value	Monitor		
+ 1400							
- network:6							
+ 101 (New_BACnet_Node)							
- 102 (temp)							
device:102 (temp)							
- network:50							
+ 50002							
+ 50022 (1020_22)							
+ 50033 (6020_33)							
- network:50001							
+ 50000 (Dev_IP)							
- network:60001							
+ 1 (FAP_1)	1 (FAP_1)	device:1 (FAP_1)	max-apdu-length-accepted	1458	Off		
+ 18100 (BASRTLX-B-01C6AF)	18100 (BASRTLX-B-01C6AF)	device:18100 (BASRTLX-B-01C6AF)	object-name	FAP_1	Off		
+ 50001	50001	device:50001	max-apdu-length-accepted	1458	Off		
+ 54321 (SENTRY_BAC_11)	54321 (SENTRY_BAC_11)	device:54321 (SENTRY_BAC_11)	object-name	SENTRY_BAC_11	Off		
+ 259645 (WeatherLink_1)	259645 (WeatherLink_1)	device:259645 (WeatherLink_1)	max-apdu-length-accepted	1458	Off		
			object-name	WeatherLink_1	Off		
			vendor-identifier	37	Off		


Total Items: 42 (Showing Items: 14)

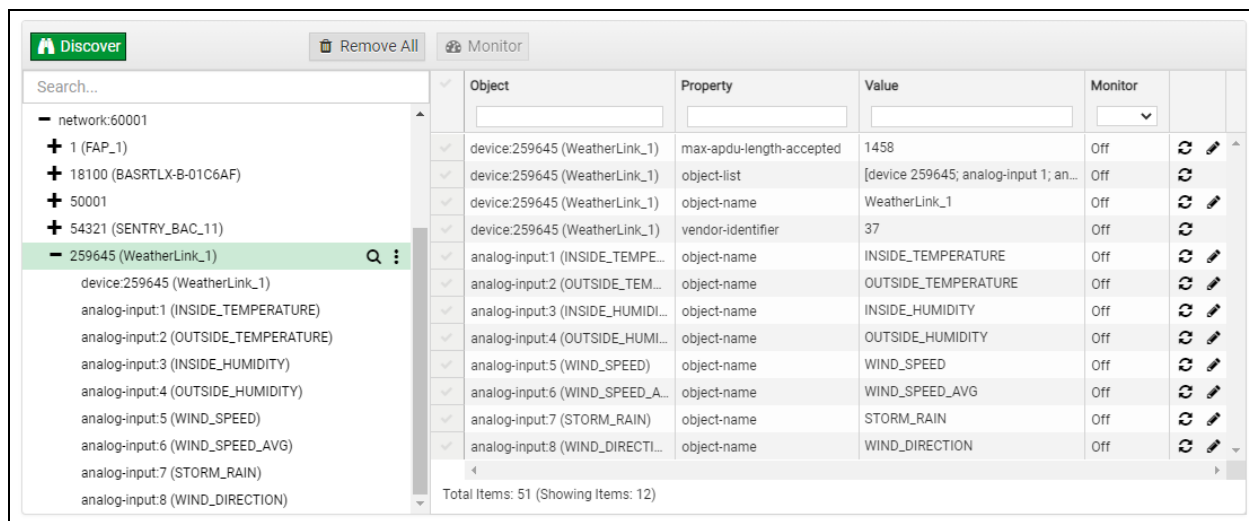
8.2 View Device Details and Explore Points/Parameters

- To view the device details, click the blue plus sign (+) next to the desired device in the list.
 - This will show only some of the device properties for the selected aspect of a device

























Search...	Object	Property	Value	Monitor		
- BACnet						
+ network:4						
+ network:5						
+ network:6						
+ network:50						
+ network:50001						
- network:60001						
+ 1 (FAP_1)						
+ 18100 (BASRTLX-B-01C6AF)						
+ 50001						
+ 54321 (SENTRY_BAC_11)						
- 259645 (WeatherLink_1)	device:259645 (WeatherLink_1)	max-apdu-length-accepted	1458	Off		
		object-name	WeatherLink_1	Off		
		vendor-identifier	37	Off		

Total Items: 42 (Showing Items: 3)

- To view the full details of a device, highlight the device directly (in the image below – “1991 WeatherLink_1”) and click the Explore button () that appears to the right of the highlighted device as a magnifying glass icon or double-click the highlighted device.

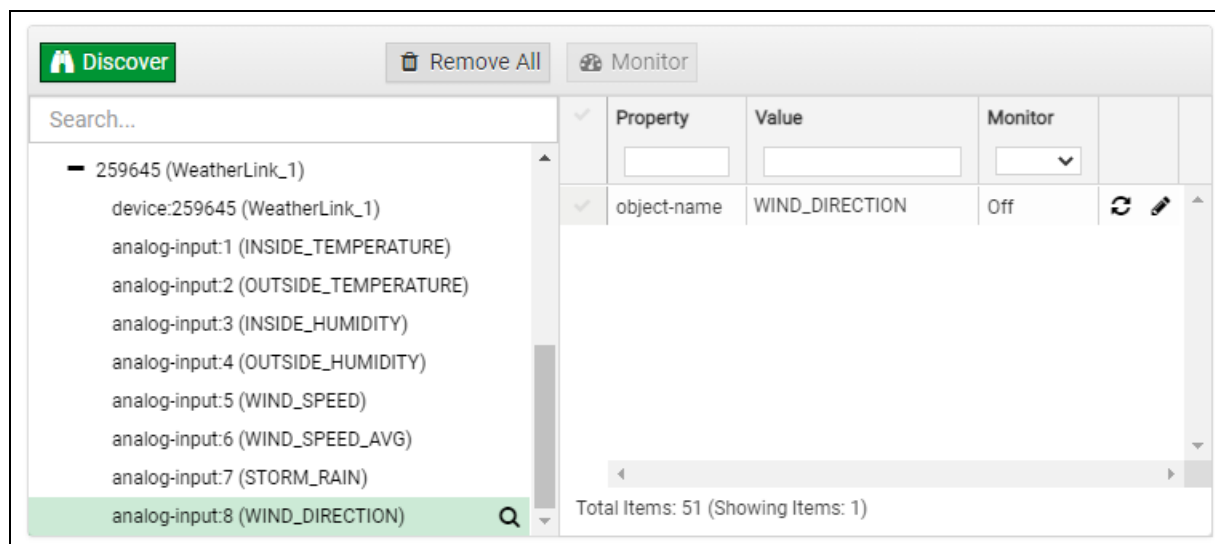


The screenshot shows the 'Discover' window with a search bar and a list of devices. The device '259645 (WeatherLink_1)' is highlighted. To its right, a magnifying glass icon is visible. Below the list, a table displays the properties of the selected device.



Object	Property	Value	Monitor	
device:259645 (WeatherLink_1)	max-apdu-length-accepted	1458	Off	 
device:259645 (WeatherLink_1)	object-list	[device 259645; analog-input 1; an...	Off	 
device:259645 (WeatherLink_1)	object-name	WeatherLink_1	Off	 
device:259645 (WeatherLink_1)	vendor-identifier	37	Off	 
analog-input:1 (INSIDE_TEMPE...	object-name	INSIDE_TEMPERATURE	Off	 
analog-input:2 (OUTSIDE_TEM...	object-name	OUTSIDE_TEMPERATURE	Off	 
analog-input:3 (INSIDE_HUMIDI...	object-name	INSIDE_HUMIDITY	Off	 
analog-input:4 (OUTSIDE_HUMI...	object-name	OUTSIDE_HUMIDITY	Off	 
analog-input:5 (WIND_SPEED)	object-name	WIND_SPEED	Off	 
analog-input:6 (WIND_SPEED_A...	object-name	WIND_SPEED_AVG	Off	 
analog-input:7 (STORM_RAIN)	object-name	STORM_RAIN	Off	 
analog-input:8 (WIND_DIRECTI...	object-name	WIND_DIRECTION	Off	 

Total Items: 51 (Showing Items: 12)

- Now additional device details are viewable; however, the device can be explored even further
- Click on one of the device details.

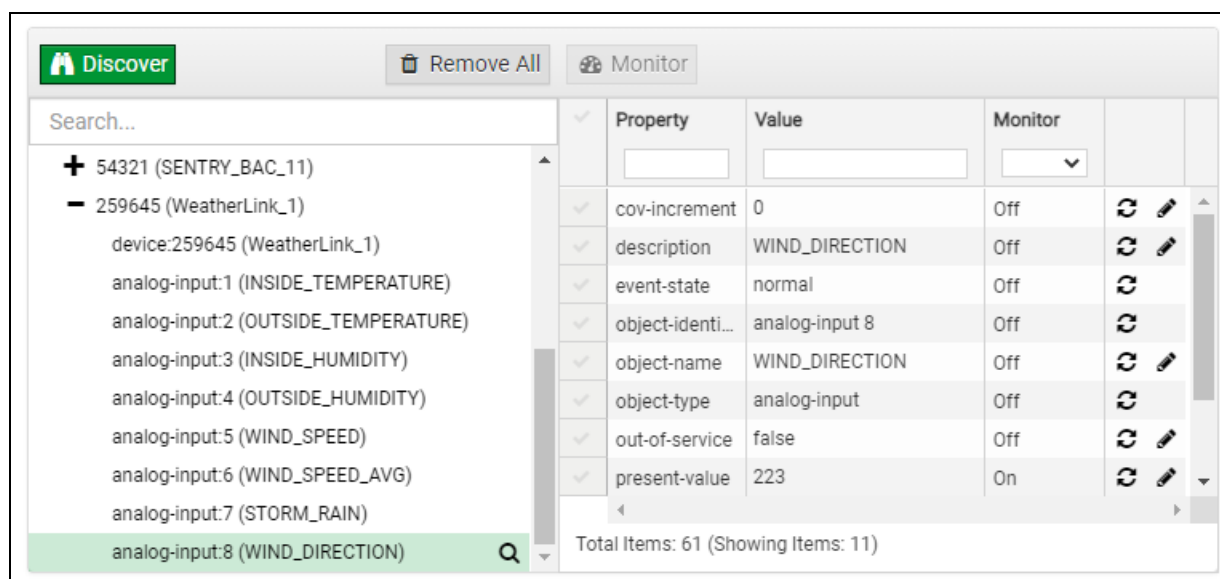


The screenshot shows the 'Discover' window with the device '259645 (WeatherLink_1)' selected. The details of the selected device are displayed in a table.

Property	Value	Monitor	
object-name	WIND_DIRECTION	Off	 

Total Items: 51 (Showing Items: 1)

- Then click on the Explore button that appears or double-click the device object.



A full list of the device details will appear on the right side window. If changes are expected since the last explore, simply press the Refresh button (↻) that appears to right of individual properties to refresh.

NOTE: The Gateway Search Bar will find devices based on their Device ID.

NOTE: The Gateway Discovery Tree has 3 levels that correspond to the following.

- Network number
 - Device
 - Device object

8.2.1 Edit the Present Value Field

The only recommended field to edit is the device's present value field.

NOTE: Other BACnet properties are editable (such as object name, object description, etc.); however, this is not recommended because the gateway is not a Building Management System (BMS).

- To edit the present value, select it in the property listings.

The screenshot shows a software interface for managing BACnet properties. At the top, there are buttons for 'Discover', 'Remove All', and 'Monitor'. Below these is a search bar and a list of properties. The 'present-value' property is highlighted in green. To the right of the list is a table with columns for 'Property', 'Value', and 'Monitor'. The 'present-value' row shows a value of 223 and is monitored. A hand icon is pointing to the edit button (pencil icon) for the 'present-value' property.

Property	Value	Monitor
cov-increment	0	Off
description	WIND_DIRECTION	Off
event-state	normal	Off
object-identifier	analog-input 8	Off
object-name	WIND_DIRECTION	Off
object-type	analog-input	Off
out-of-service	false	Off
present-value	223	On
reliability	no-fault-detected	Off
status-flags	[in-alarm: false; fault: false; overrid...	Off
units	no-units	Off

- Then click the Write button () on the right of the property to bring up the Write Property window.

The 'Write Property' dialog box is shown. It has a title bar 'Write Property'. Inside, there is a text input field with 'present-value' on the left and '2' on the right. At the bottom right, there are two buttons: 'Cancel' and 'Write'.

- The window will close. When the BACnet Explorer page appears, the present value will be changed as specified.



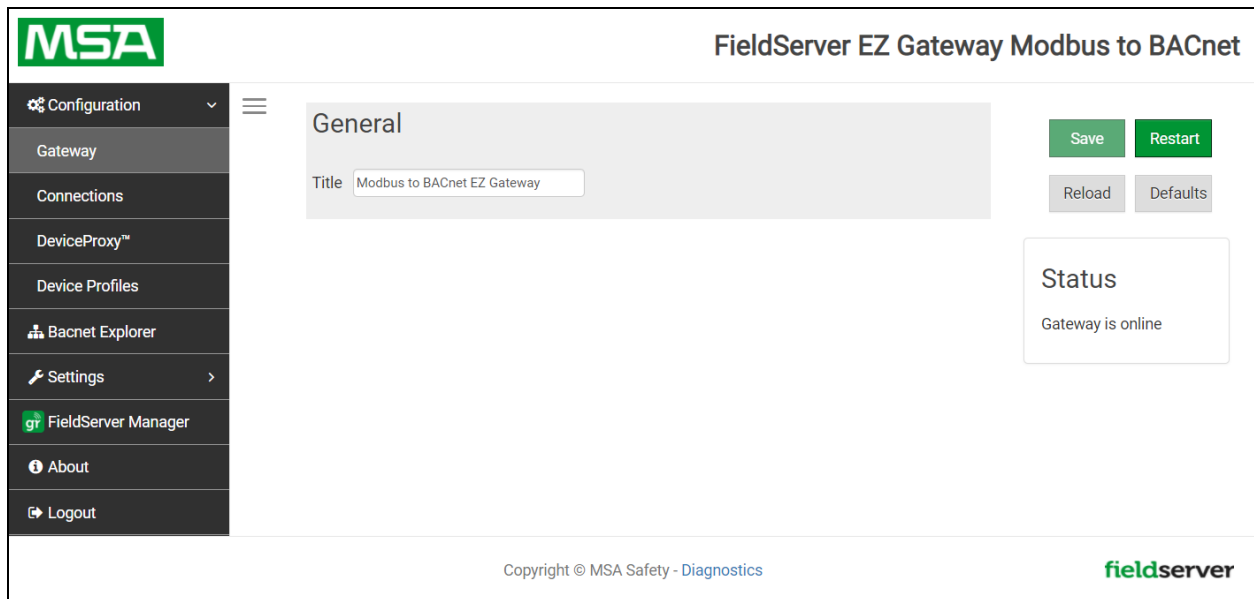
9 MSA Grid - FieldServer Manager Setup

The MSA 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](#).

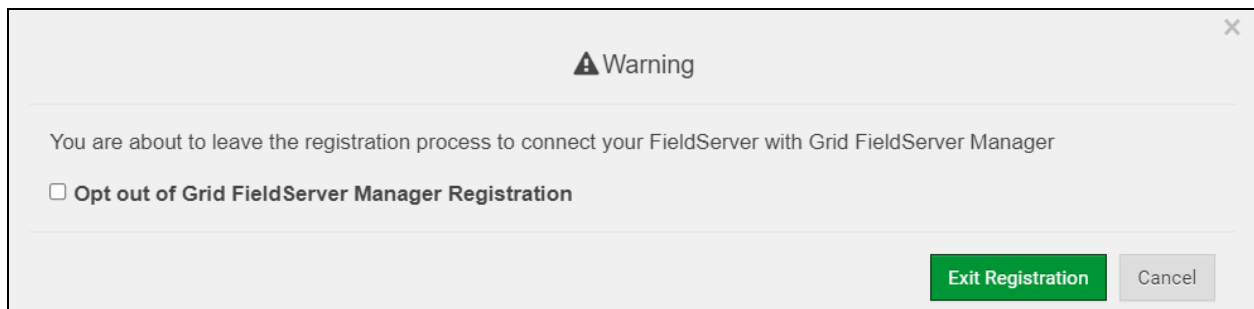
9.1 Choose Whether to Integrate the FieldServer Manager

When first logging onto the EZ Gateway, the Web App will open on the FieldServer Manager page.

NOTE: If a warning message appears instead, go to [Section 11.6 FieldServer Manager Connection Warning Message](#) to resolve the connection issue.



- Either go through the FieldServer Manager setup to integrate cloud functionality to the FieldServer or opt out.
 - For FieldServer Manager setup, continue with instructions in the following sections
 - To opt out of the FieldServer Manager, click on a tab other than the Grid FieldServer Manager tab, click the checkbox next to “Opt out of Grid FieldServer Manager Registration” in the Warning window that appears and click the Exit Registration button
 - To ignore FieldServer Manager setup until the next time the Web App is opened, click a tab other than Grid FieldServer Manager and then click the Exit Registration button with the “Opt out” checkbox unchecked

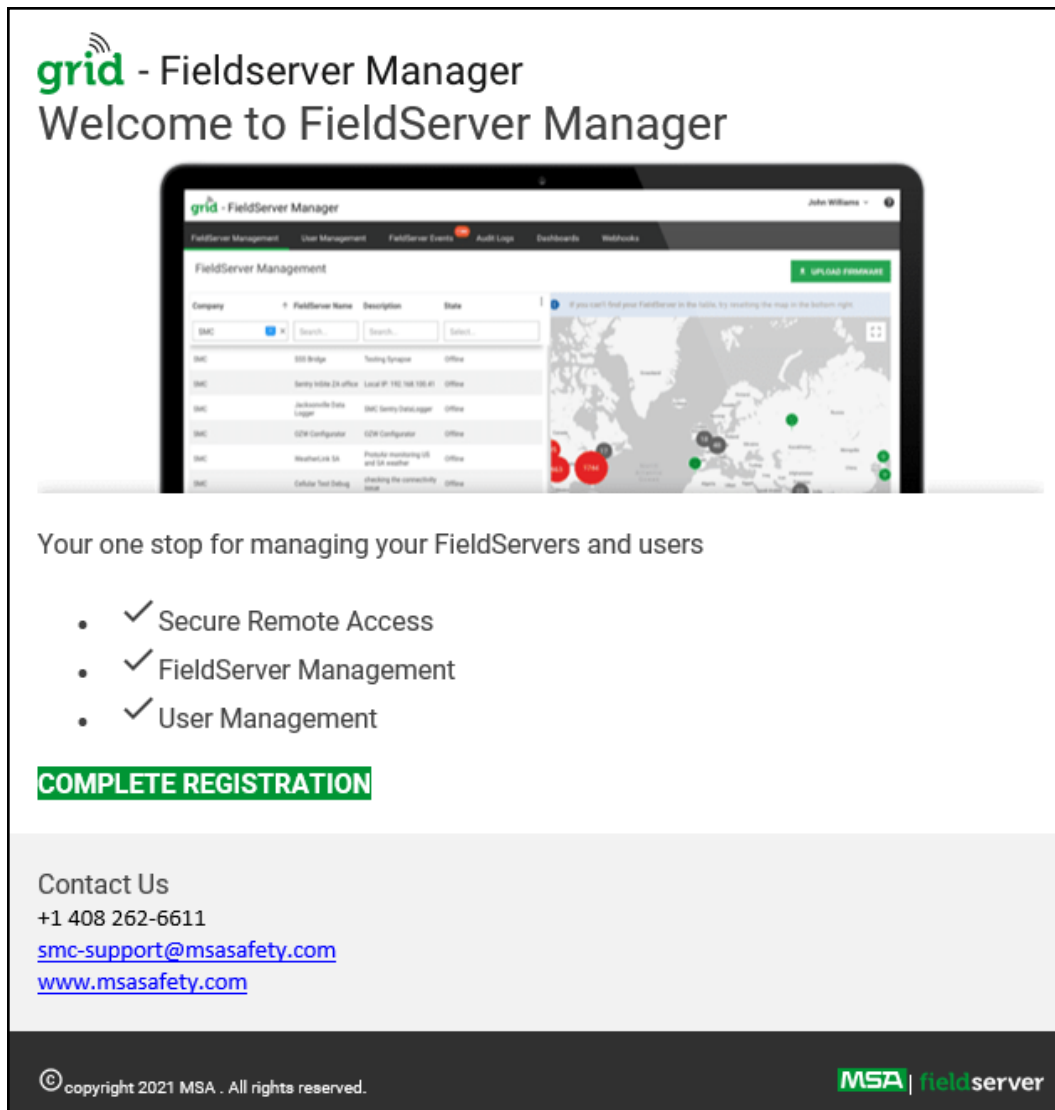


NOTE: If user setup is already complete go to [Section 9.3 Registration Process](#).

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, 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

*

*Invalid Mobile 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](#)

*

* Mandatory Fields

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 Registration Process

Once the FieldServer Manager user credentials have been generated, the EZ Gateway can be registered onto the server.

- Click the FieldServer Manager tab.

NOTE: If a warning message appears instead, go to [Section 11.6 FieldServer Manager Connection Warning Message](#) to resolve the connection issue.

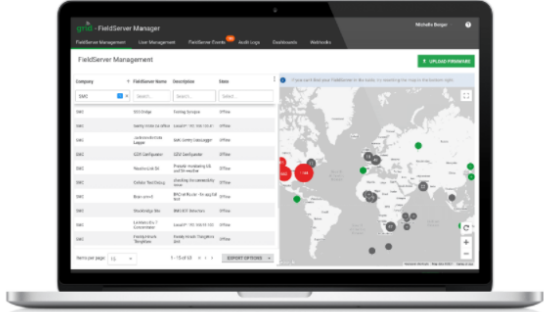
Grid FieldServer Manager Registration

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 FieldServer Manager registration page.

- To register, fill in the user details, site details, gateway details and FieldServer Manager account credentials.

- Enter user details and click Next

The screenshot shows the 'Installer Details' step (Step 1) of the registration process. At the top, there are four numbered steps: 1 (Installer Details), 2 (Installation Site), 3 (FieldServer Details), and 4 (Account Details). The 'Installer Details' section contains the following fields:

- Installer Name:** A text input field.
- Company:** A text input field.
- Telephone:** A text input field.
- Email:** A text input field.
- Installation Date:** A date picker showing '20-September-2021'.

At the bottom right, there are two buttons: 'Cancel' (grey) and 'Next' (green).

- 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 (Step 2) of the registration process. At the top, there are four numbered steps: 1 (Installer Details), 2 (Installation Site), 3 (FieldServer Details), and 4 (Account Details). The 'Installation Site Details' section contains the following fields:

- Search:** A search bar with the placeholder text 'Search Google Maps' and a magnifying glass icon.
- Site Name:** A red text input field with the placeholder text 'Enter a name for this location'.
- Building:** A text input field.
- Street Address:** A text input field with the placeholder text 'Enter street address'.
- Suburb:** A text input field.
- City:** A text input field.
- State:** A text input field.
- Country:** A text input field.
- Postal Code:** A text input field.
- Latitude:** A red text input field with the placeholder text 'Enter latitude'.
- Longitude:** A red text input field with the placeholder text 'Enter longitude'.

On the right side of the form, there is a map interface showing a map of Lafayette, Louisiana, with various locations marked. The map includes a search bar, a 'Map' button, a 'Satellite' button, and a person icon. At the bottom right, there are three buttons: 'Cancel' (grey), 'Previous' (grey), and 'Next' (green).

- Enter Name and Description (required) then click Next

Grid FieldServer Manager Registration

1
2
3
4

Installer Details
Installation Site
FieldServer Details
Account Details

FieldServer Details

Name

Description

FieldServer Info

Optionally specify any other information relating to the FieldServer i.e., calibration, commissioning or other notes

Timezone

(GMT -08:00) America/Los_Angeles

Cancel
Previous
Next

- Click the “Create an Grid FieldServer Manager account” button and enter a valid email to send a “Welcome to MSA Grid – FieldServer Manager” invite to the email address entered

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

- 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 EZ Gateway.

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

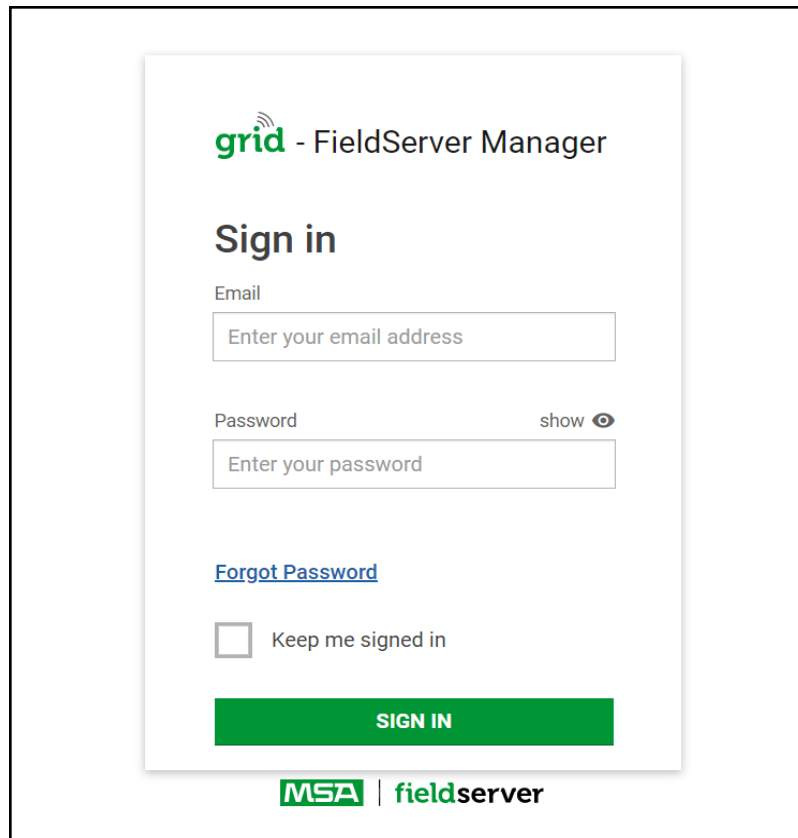
Site Name: Site#1
Building:
Street Address: 1020 Canal Road
Suburb:
City: Lafayette
State: Indiana
Country: United States
Postal Code: 47904

[Update FieldServer Details](#)

NOTE: Update these details at any time by going to the FieldServer Manager tab and clicking the Update FieldServer 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 large 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.

© 2021 MSA. All rights reserved.

MSA | fieldserver


10 Troubleshooting

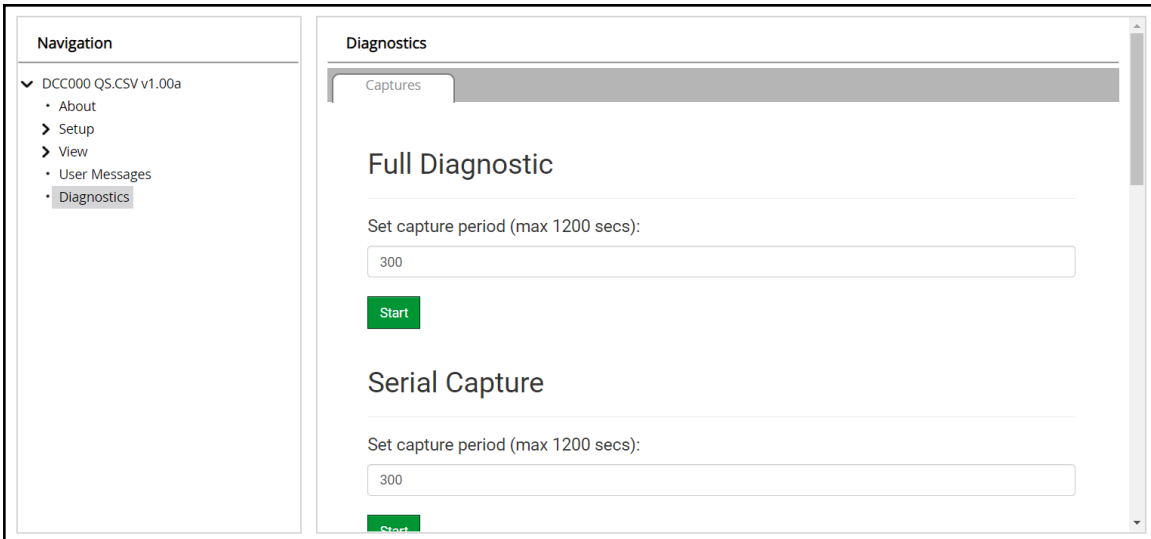
10.1 Communicating with the EZ Gateway Over the Network

- 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 EZ Gateway. The Default IP Address of the EZ Gateway 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 EZ Gateway are on the same IP Network, or assign a Static IP Address to the PC on the 192.168.2.X network.

10.2 Taking a FieldServer Diagnostic Capture

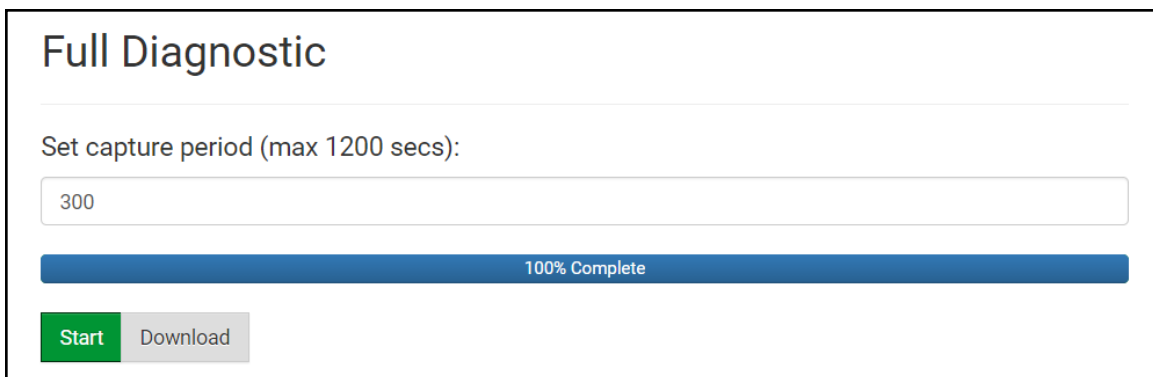
When there is a problem on-site that cannot easily be resolved, perform a Diagnostic Capture before contacting support. Once the Diagnostic Capture is complete, email it to technical support. The Diagnostic Capture will accelerate diagnosis of the problem.

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



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

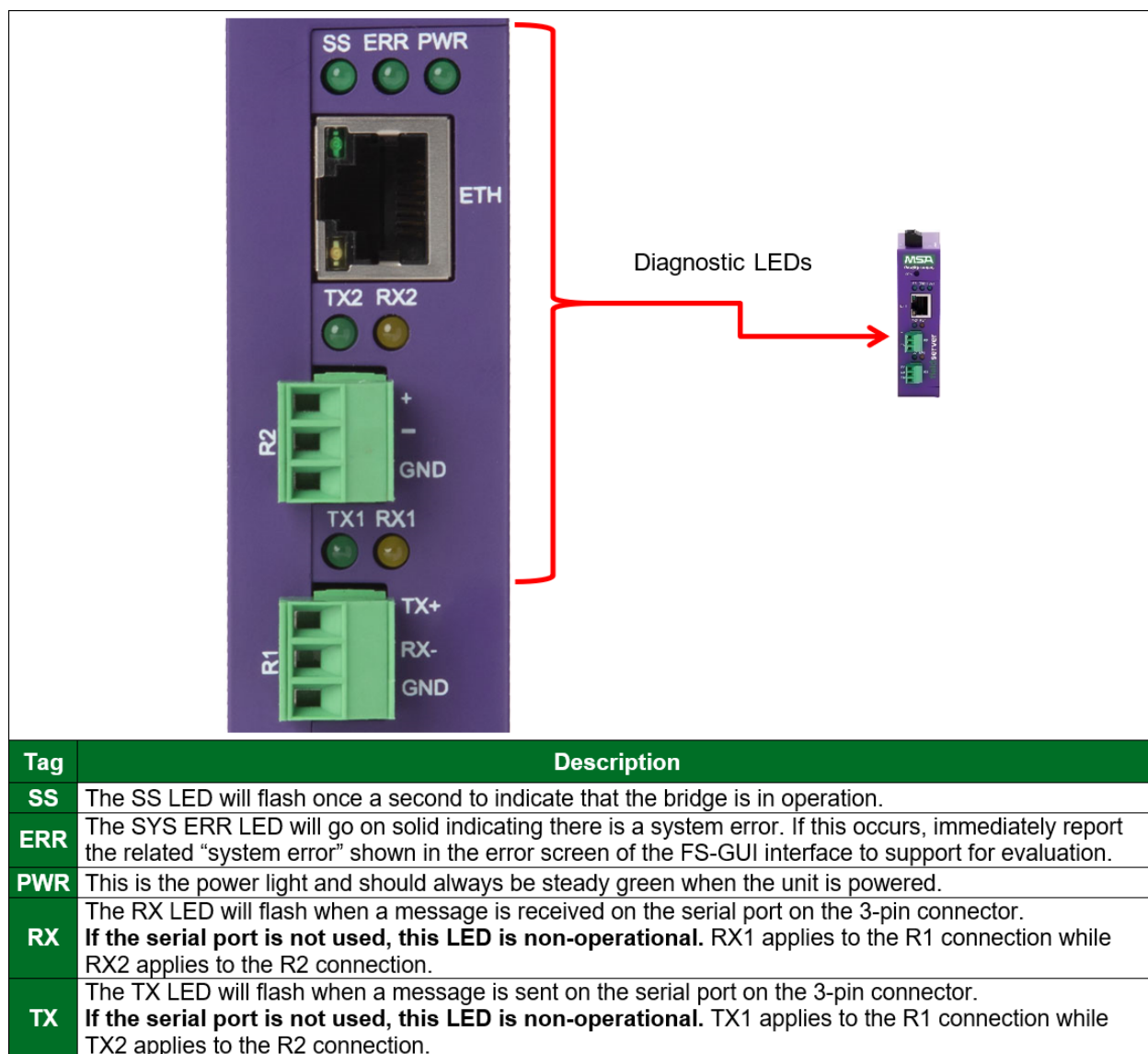


This screenshot shows the 'Full Diagnostic' section after the capture is complete. The 'Set capture period (max 1200 secs):' label is followed by a text input field containing '300'. Below the input field is a blue progress bar that is 100% full, with the text '100% Complete' centered on it. At the bottom,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

10.3 LED Functions



10.4 Factory Reset Instructions

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

10.5 Internet Browser Software Support

The following web browsers are supported:

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

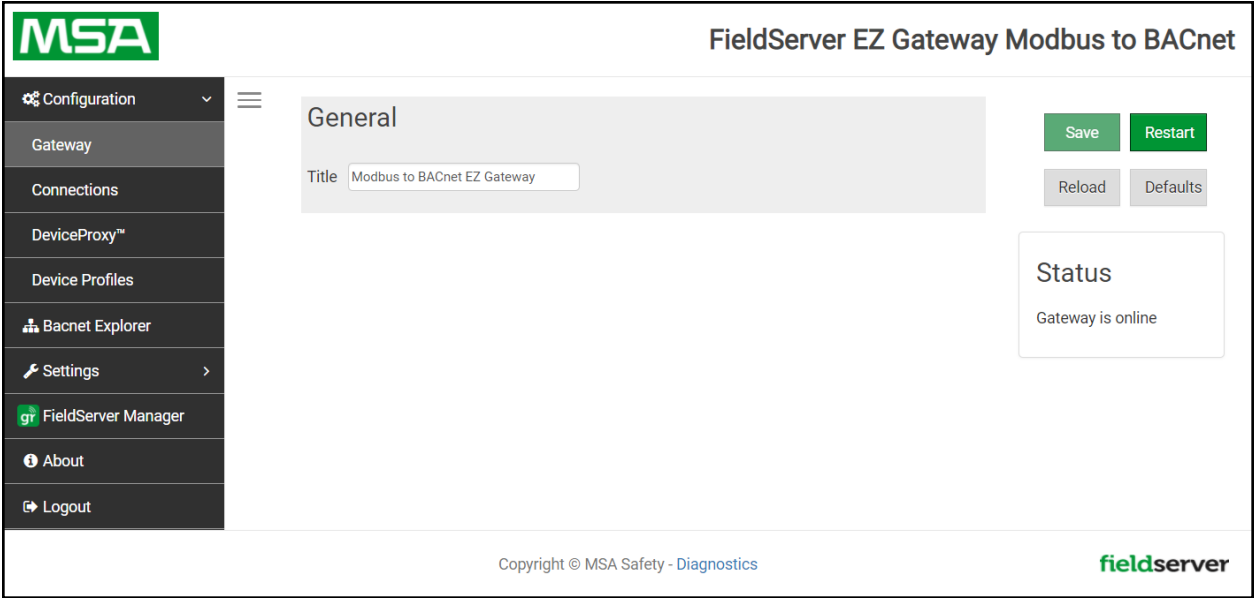
NOTE: Internet Explorer is no longer supported as recommended by Microsoft.

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

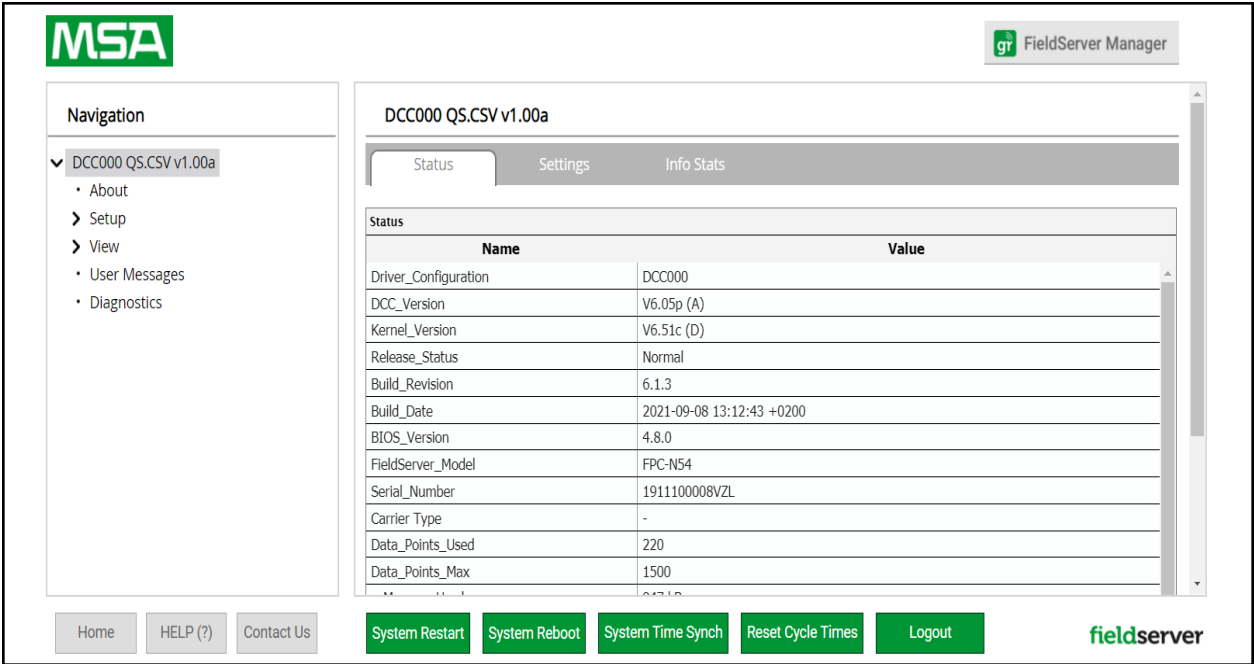
11 Additional Information

11.1 Change Web Server Security Settings After Initial Setup

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

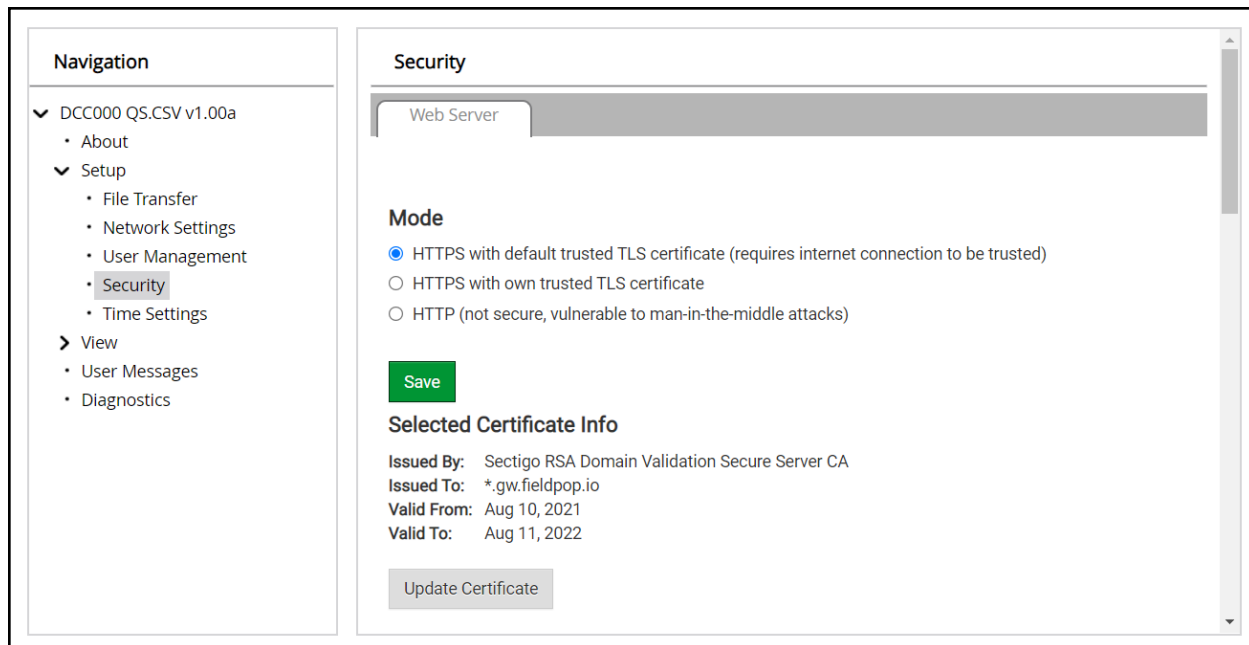


- Click Setup in the Navigation panel.



11.1.1 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.

11.1.2 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 shows the 'Security' configuration page. On the left is a 'Navigation' panel with a tree structure. The 'Security' option is highlighted. The main content area is titled 'Security' and has a 'Web Server' tab selected. Under the 'Mode' section, three radio buttons are present: 'HTTPS with default trusted TLS certificate (requires internet connection to be trusted)' (selected), 'HTTPS with own trusted TLS certificate', and 'HTTP (not secure, vulnerable to man-in-the-middle attacks)'. Below the modes is a green 'Save' button. Under the 'Selected Certificate Info' section, the following details are displayed: 'Issued By: Sectigo RSA Domain Validation Secure Server CA', 'Issued To: *.gw.fieldpop.io', 'Valid From: Aug 10, 2021', and 'Valid To: Aug 11, 2022'. At the bottom of this section is a grey 'Update Certificate' button.

Navigation

- ▼ DCC000 QS.CSV v1.00a
 - About
- ▼ Setup
 - File Transfer
 - Network Settings
 - User Management
 - **Security**
 - Time Settings
- View
 - User Messages
 - Diagnostics

Security

Web Server

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

Selected Certificate Info

Issued By: Sectigo RSA Domain Validation Secure Server CA

Issued To: *.gw.fieldpop.io

Valid From: Aug 10, 2021

Valid To: Aug 11, 2022

Update Certificate

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

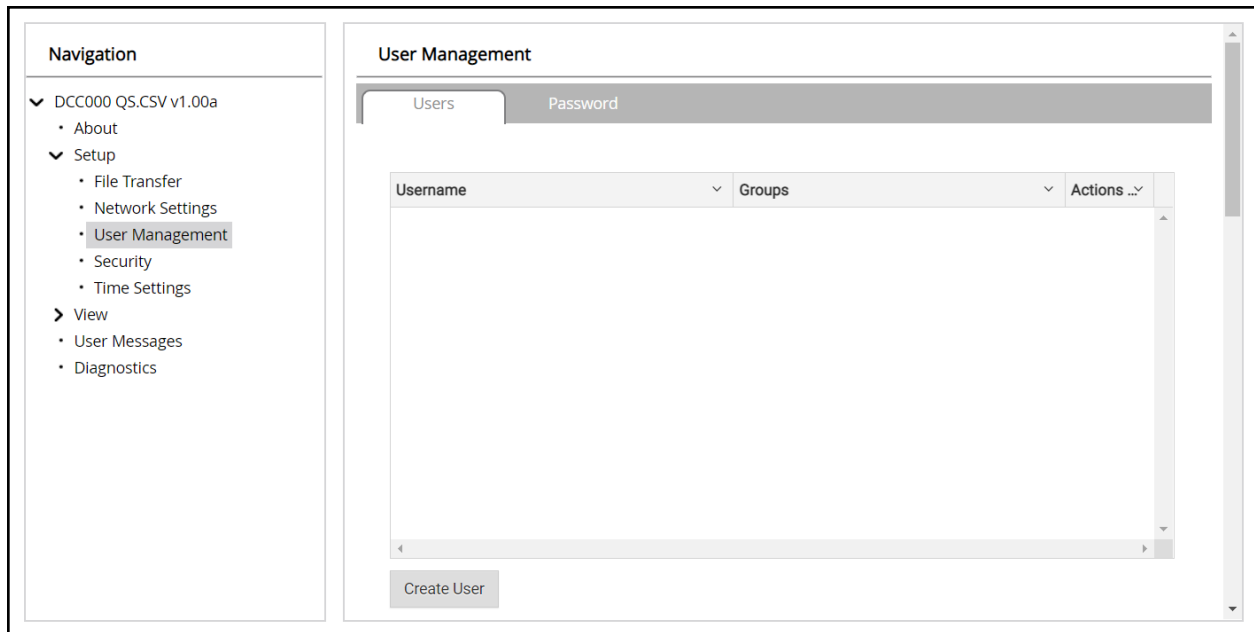
11.2 Change User Management Settings

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

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

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

- Check that the Users tab is selected.



User Types:

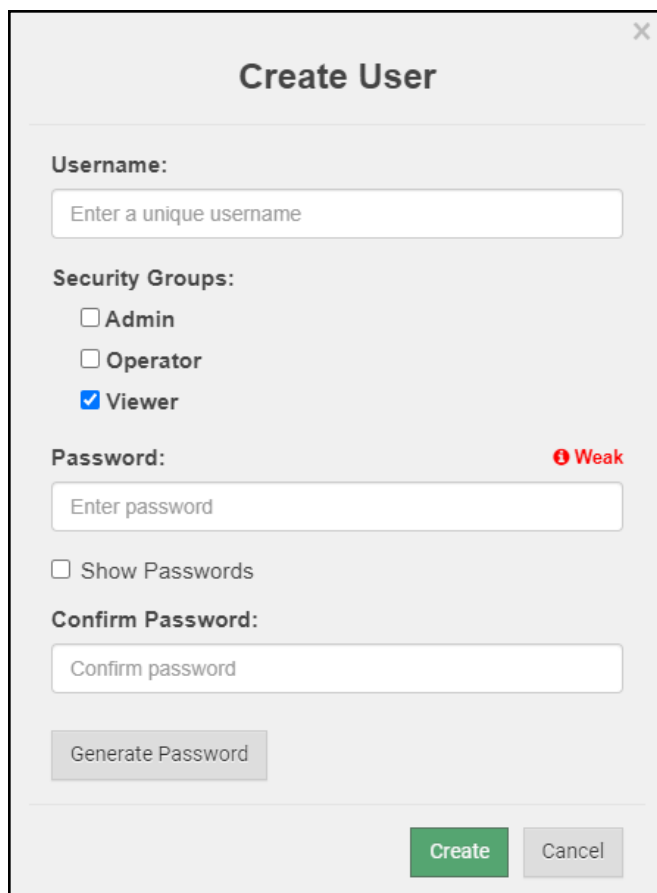
Admin – Can modify and view any settings on the FieldServer.

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

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

11.2.1 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 'Weak'.
- 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 Confirm Password field.
- Create and Cancel:** Two buttons at the bottom right, 'Create' (green) and 'Cancel' (grey).

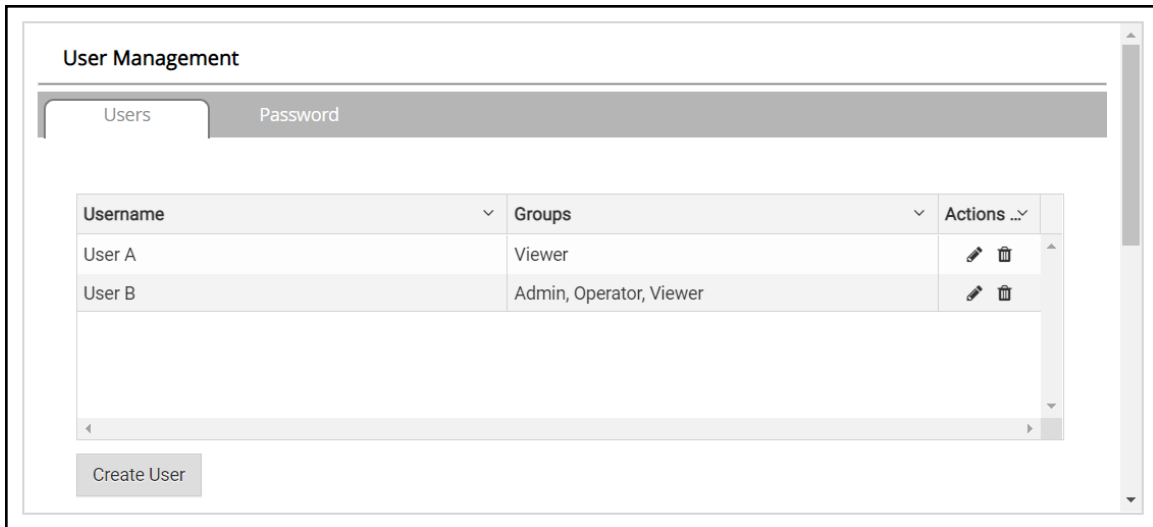
- Enter the new User fields: Name, Security Group and Password.
 - User details are hashed and salted**

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

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

11.2.2 Edit Users

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

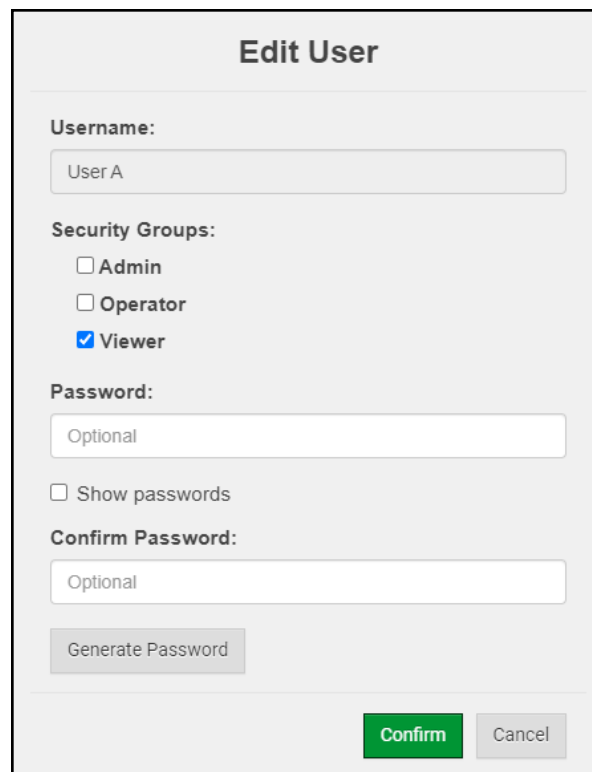


The 'User Management' window has two tabs: 'Users' and 'Password'. The 'Users' tab is active, displaying a table with the following data:

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.



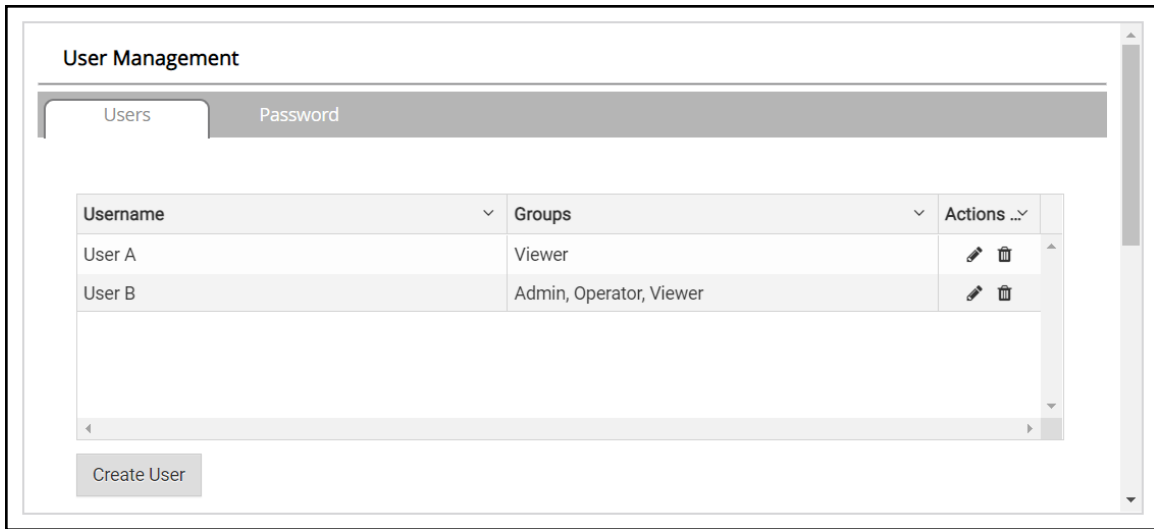
The 'Edit User' window contains the following fields and controls:

- 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.

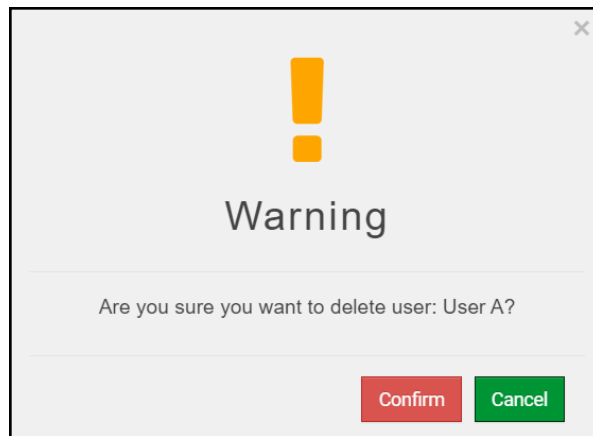
- Click Confirm.
- Once the Success message appears, click OK.

11.2.3 Delete Users

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



- When the warning message appears, click Confirm.



11.2.4 Change FieldServer Password

- Click the Password tab.

The screenshot shows a web interface for 'User Management'. On the left is a 'Navigation' sidebar with a tree structure: 'DCC000 Q5.CSV v1.00a' (expanded) contains 'About', 'Setup' (expanded), and 'View'. 'Setup' contains 'File Transfer', 'Network Settings', 'User Management' (highlighted), 'Security', and 'Time Settings'. 'View' contains 'User Messages' and 'Diagnostics'. The main area is titled 'User Management' and has two tabs: 'Users' and 'Password' (selected). The 'Password' tab contains a 'Password:' label with a red 'Weak' indicator, a text input field with placeholder 'Enter password', a checkbox for 'Show passwords', a 'Confirm Password:' label, another text input field with 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.

11.3 Specifications



	FS-EZ3-MOD-BAC & FS-EZ4-MOD-BAC	
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) One Ethernet 10/100 BaseT port	
Power Requirements	<i>Input Voltage:</i> 9-30VDC or 24VAC <i>Max Power:</i> 3 Watts	<i>Current draw:</i> 24VAC 0.125A 9-30VDC 0.25A @12VDC
Approvals	CE and FCC , UL 60950-1 and CAN/CSA C22.2, WEEE compliant, RoHS3 compliant, REACH compliant, UKCA compliant	
Physical Dimensions	4 x 1.1 x 2.7 in (10.16 x 2.8 x 6.8 cm)	
Weight	0.4 lbs (0.2 Kg)	
Operating Temperature	-20°C to 70°C (-4°F to 158°F)	
Humidity	10-95% RH non-condensing	

“This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference
- This device must accept any interference received, including interference that may cause undesired operation.

NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his expense.

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

NOTE: Specifications subject to change without notice.

11.4 Compliance with UL Regulations

For UL compliance, the following instructions must be met when operating the EZ Gateway.

- The units shall be powered by listed LPS or Class 2 power supply suited to the expected operating temperature range.
- The interconnecting power connector and power cable shall:
 - Comply with local electrical code
 - Be suited to the expected operating temperature range
 - Meet the current and voltage rating for the FieldServer
- Furthermore, the interconnecting power cable shall:
 - Be of length not exceeding 3.05m (118.3")
 - Be constructed of materials rated VW-1, FT-1 or better
- If the unit is to be installed in an operating environment with a temperature above 65 °C, it should be installed in a Restricted Access Area requiring a key or a special tool to gain access.
- This device must not be connected to a LAN segment with outdoor wiring.

11.5 Address Types and Data Types

If the node parameter Address_Type is set as ADU or PDU, then Data_Type must be specified as follows.

For Address_Type ADU

Address range	Data_Type	Function Code (Write)	Function Code (Read)
1 – 65536	Coil	15	1
1 – 65536	Discrete_Input	n/a.	2
1 – 65536	Input_Register	n/a.	4
1 – 65536	Holding_Register	16	3

For Address_Type PDU:

Address range	Data_Type	Function Code (Write)	Function Code (Read)
0 – 65535	Coil	15	1
0 – 65535	Discrete_Input	n/a.	2
0 – 65535	Input_Register	n/a.	4
0 – 65535	Holding_Register	16	3

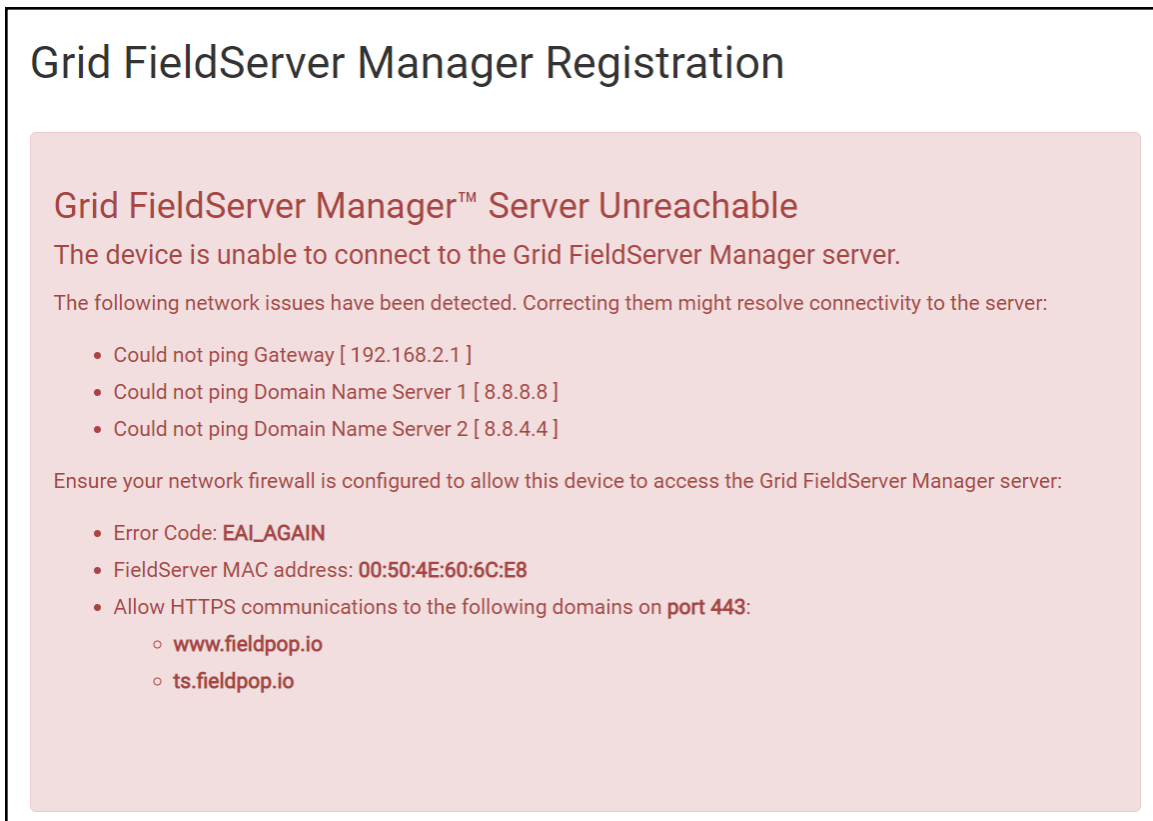
For Address_Type Modicon_5digit:

When a Modbus address range is specified, a particular Data Type is implied. The defaults are shown below.

Address Range	Data_Type	Function Code (Write)	Function Code (Read)
00001 - 09999	Coil	5,15	1
10001 - 19999	Discrete_Input	n/a.	2
30001 - 39999	Input_Register	n/a.	4
40001 - 49999	Holding_Register	6,16	3

11.6 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.

12 Limited 2 Year Warranty

MSA Safety warrants its products to be free from defects in workmanship or material under normal use and service for two years after date of shipment. MSA Safety will repair or replace any equipment found to be defective during the warranty period. Final determination of the nature and responsibility for defective or damaged equipment will be made by MSA Safety personnel.

All warranties hereunder are contingent upon proper use in the application for which the product was intended and do not cover products which have been modified or repaired without MSA Safety's approval or which have been subjected to accident, improper maintenance, installation or application; or on which original identification marks have been removed or altered. This Limited Warranty also will not apply to interconnecting cables or wires, consumables or to any damage resulting from battery leakage.

In all cases MSA Safety's responsibility and liability under this warranty shall be limited to the cost of the equipment. The purchaser must obtain shipping instructions for the prepaid return of any item under this warranty provision and compliance with such instruction shall be a condition of this warranty.

Except for the express warranty stated above, MSA Safety disclaims all warranties with regard to the products sold hereunder including all implied warranties of merchantability and fitness and the express warranties stated herein are in lieu of all obligations or liabilities on the part of MSA Safety for damages including, but not limited to, consequential damages arising out of or in connection with the use or performance of the product.