Operating Manual

BACnet IoT Gateway Start-up Guide

Revision: 7.H

Document No.: T18620

Print Spec: 10000005389 (EO)

MSA Safety
1000 Cranberry Woods Drive
Cranberry Township, PA 16066 USA

U.S. Support Information:
+1 408 964-4443
+1 800 727-4377
Email: smc-support@msasafety.com

EMEA Support Information:
+31 33 808 0590
Email:
smc-support.emea@msasafety.com

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

Contents

1 BACnet IoT Gateway Description

The BACnet IoT Gateway provides a connection from BACnet devices and networks to the cloud. This is achieved via a discovery tool built into the hardware for any BACnet/IP or BACnet MS/TP network without any additional dongles or installations needed. BBMD BACnet network discovery is also supported.

The BACnet IoT Gateway comes in four model types. The FS-IOT-BAC model offers two RS-485 ports and one Ethernet 10/100 port. The FS-IOT-BAC2 model offers two RS-485 ports and two Ethernet 10/100 ports with WAN firewall options. The FS-IOT-BACW model has two RS-485 ports, one Ethernet 10/100 port and supports Wi-Fi network connection. The FS-IOT-BACA, FS-IOT-BACV and FS-IOT-BACF models offer cellular connections for the chosen carrier (AT&T, Verizon or Vodafone), one RS-485 port, one Ethernet 10/100 port and supports Wi-Fi network connection.

Additionally, Wi-Fi models act as a Wi-Fi access point for modern web-based configuration and remote access from any mobile device without user restrictions.

The BACnet IoT Gateway also includes Monitor View, Data Log Viewer, Virtual Points and Event Log data analysis features that allow tracking and logging of individual device data points across the connected network in real-time.

The BACnet IoT Gateway is cloud ready and connects with MSA Safety’s Grid FieldServer Manager.

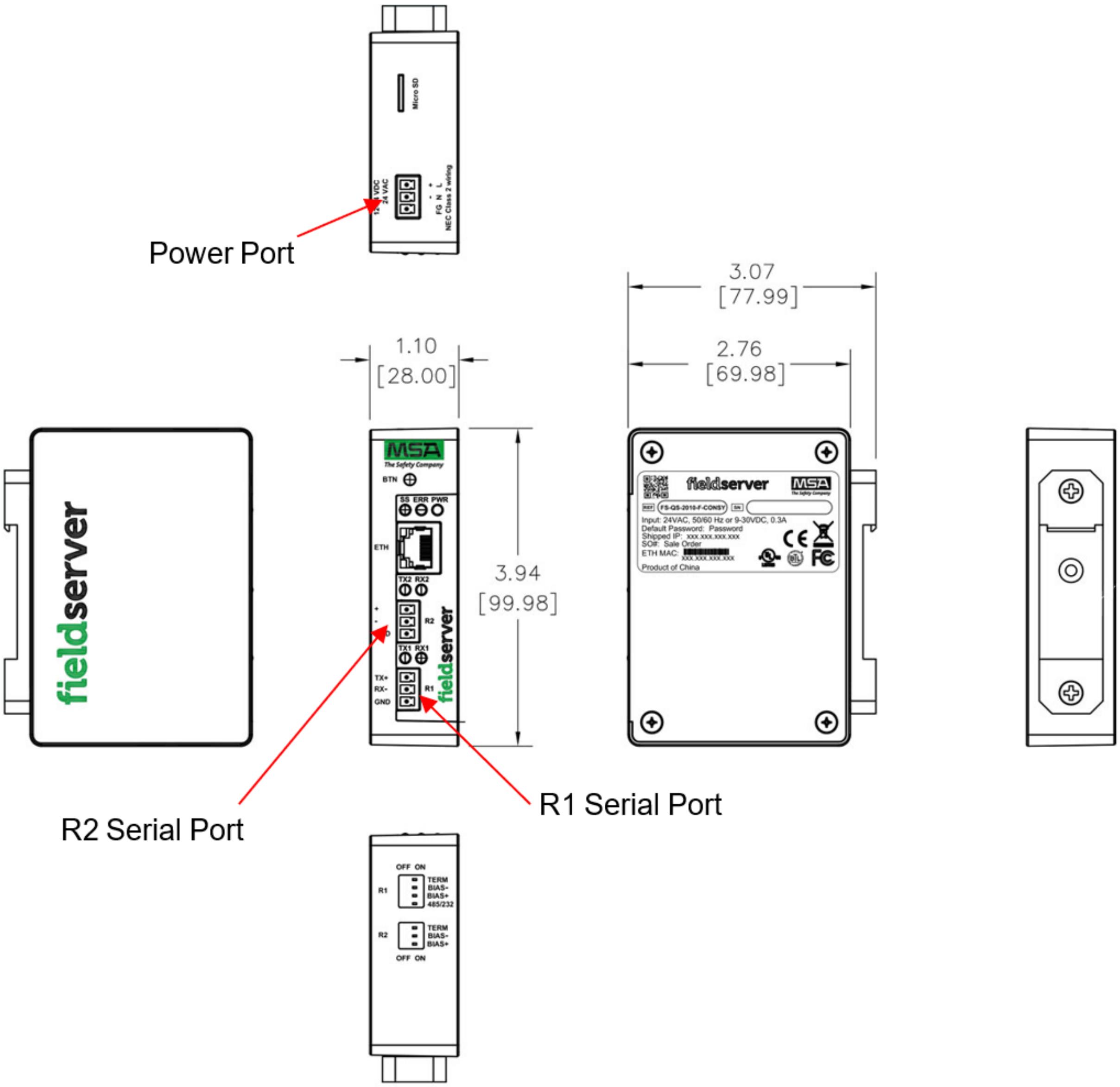
NOTE: For cloud information, refer to the MSA Grid - FieldServer Manager Start-up Guide online through the MSA Safety website.

NOTE: The latest versions of instruction manuals, driver manuals, configuration manuals and support utilities are available online through the MSA Safety website.

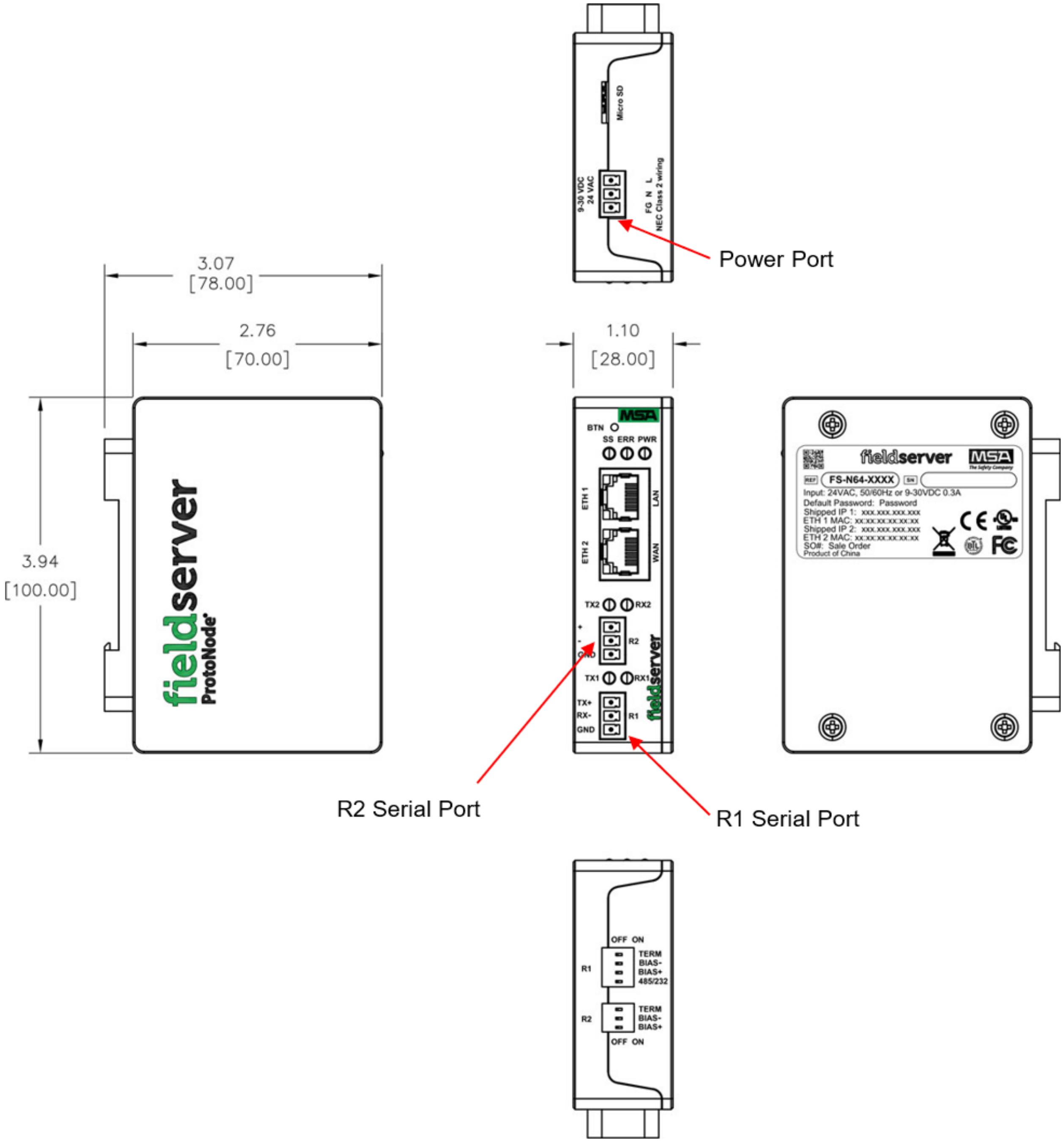
2 Equipment Setup

2.1 Physical Dimensions

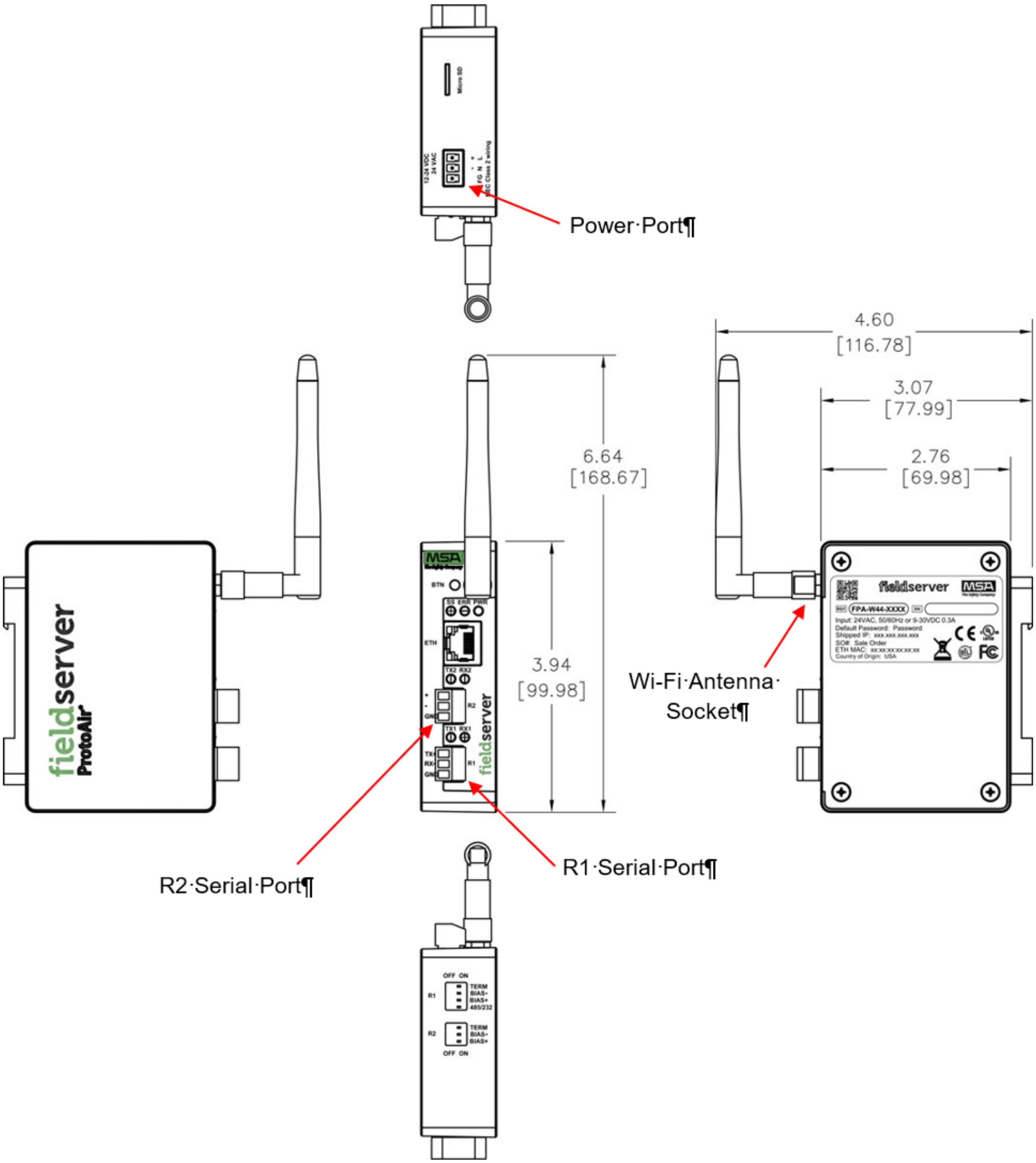
2.1.1 FS-IOT-BAC Drawing



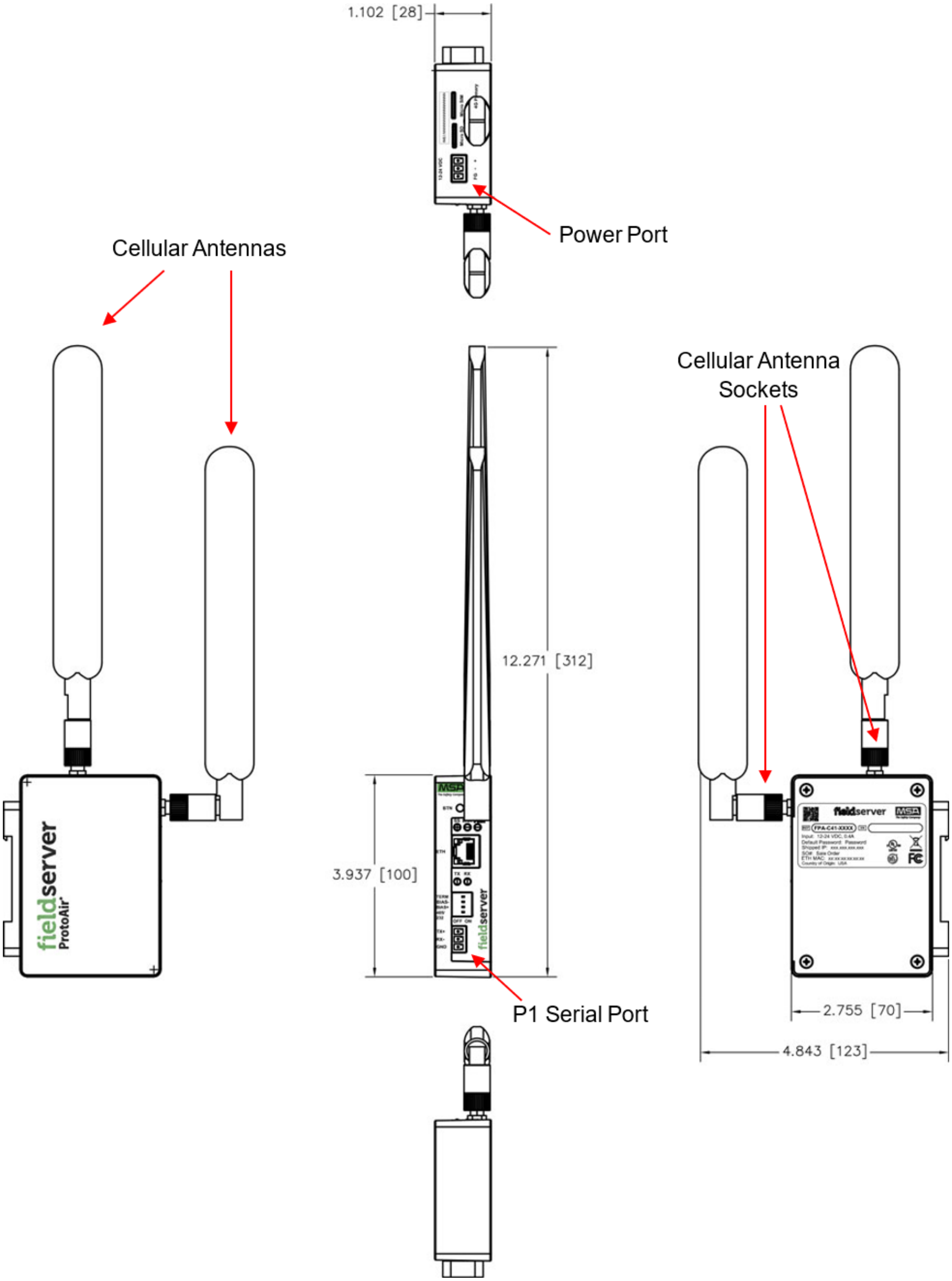
2.1.2 FS-IOT-BAC2 Drawing



2.1.3 FS-IOT-BACW Drawing

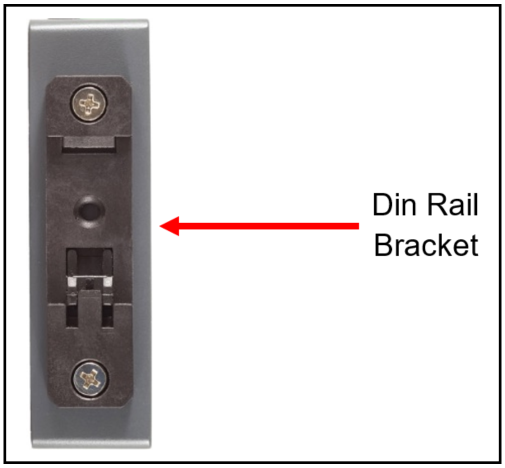


2.1.4 FS-IOT-BACA/V/F Drawing



2.2 Mounting

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



2.3 Attaching the Antenna(s)

NOTE: This section does not apply to the FS-IOT-BAC model BACnet IoT Gateway.

Wi-Fi Antenna:

If using the FS-IOT-BACW (Wi-Fi) model, screw in the Wi-Fi antenna to the front of the unit as shown in **Section 2.1.3 FS-IOT-BACW Drawing**.

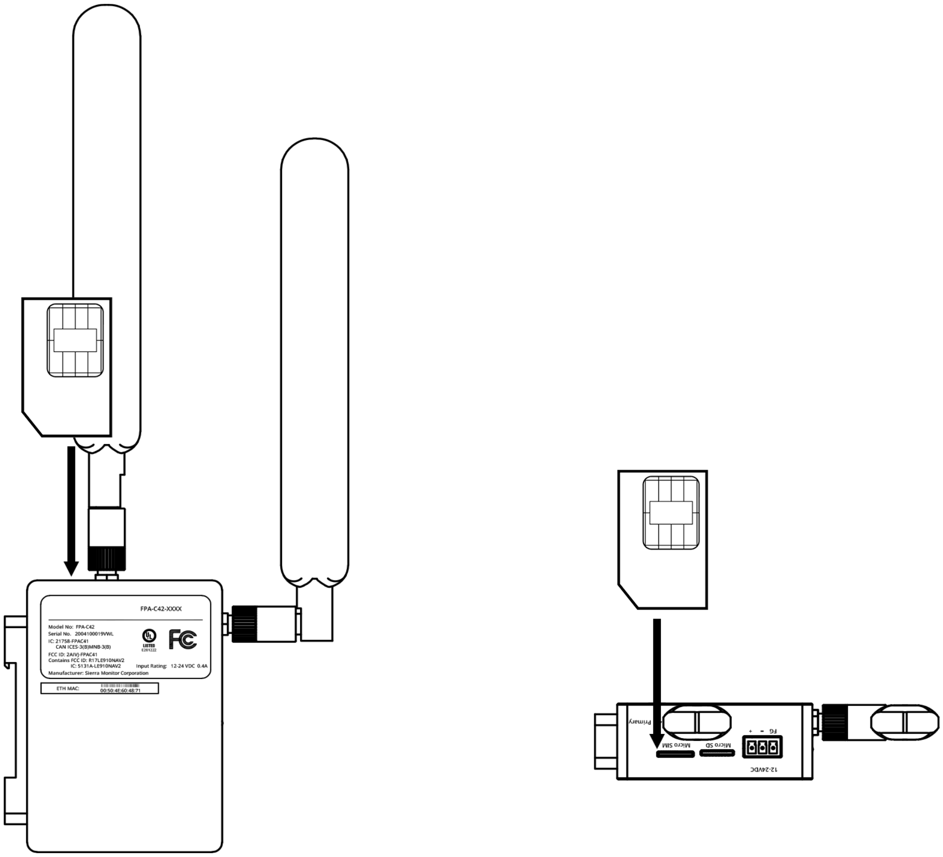
Cellular Antenna:

If using theFS-IOT-BACA/V/F models, screw in the two cellular antennas. One antenna is screwed into the socket on the top of the unit and one is screwed into the socket on the side as shown in **Section 2.1.4 FS-IOT-BACA/V/F Drawing**.

2.4 FS-IOT-BACA/V/F: Inserting the SIM Card

NOTE: A micro 4G SIM card must be purchased from an AT&T or Verizon cellular provider to set up cellular functionality and create a data plan for the FieldServer. SIM card vendor contact information is available at the end of the section. The IMEI can be found by accessing the FieldServer FS-GUI page and checking the Cellular network tab under “cellular model”.

Insert the SIM card into the Micro SIM card slot with the chip on the SIM card facing away from the cellular antenna as shown below.



See **Section 6.1.5 FS-IOT-BACA/V/F: Cellular Settings** to complete cellular setting configuration.

The table below shows cellular usage examples to forecast data usage on the chosen cellular plan.

Number of Data Points	Logging Frequency	Data Usage per Hour	Data Usage per Month
10	40 sec	0.75 Mb	547 Mb
10	900 sec	0.55 Mb	400 Mb
50	40 sec	1.24 Mb	900 Mb
50	900 sec	0.90 Mb	657 Mb
100	40 sec	3.00 Mb	2.2 Gb
100	900 sec	1.26 Mb	900 Mb
500	40 sec	10.86 Mb	7.8 Gb
500	900 sec	0.55 Mb	1.5 Gb

SIM Card Vendor Contact Information:

Verizon

A business contract is required to purchase a Verizon SIM card. The IMEI of the BACnet IoT Gateway is required to purchase the Verizon SIM card.

AT&T

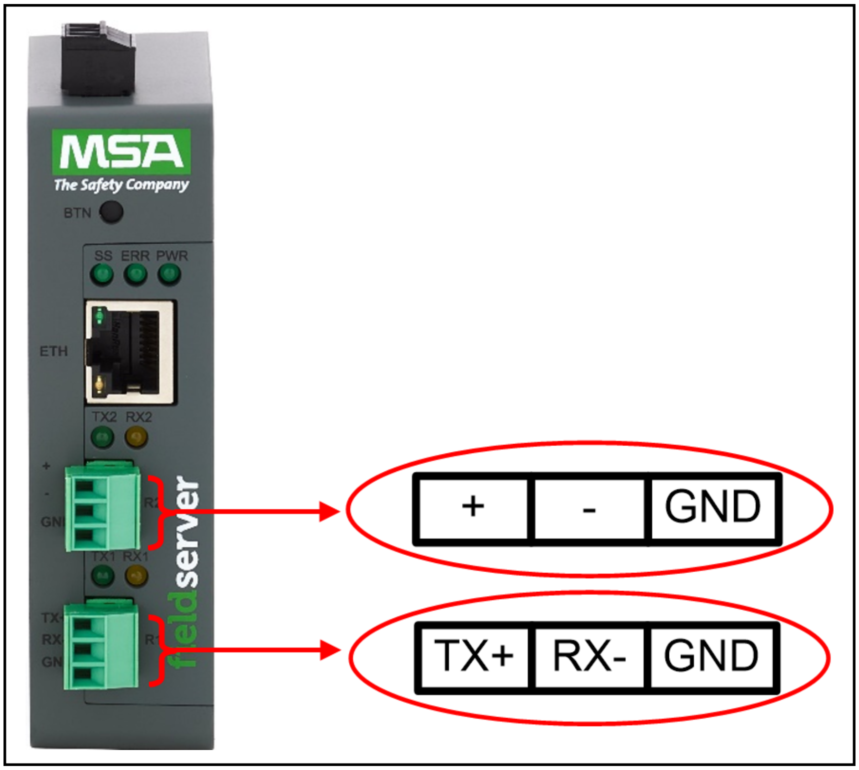
Please call AT&T Customer Service at 800.331.0500 or find the nearest AT&T store.

3 Installation

3.1 FS-IOT- BAC/BACW/BAC2: Connecting the R1 & R2 Ports

NOTE: For the R1 Port, ensure RS-485 is selected by checking the number 4 DIP Switch is set to the left side.

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



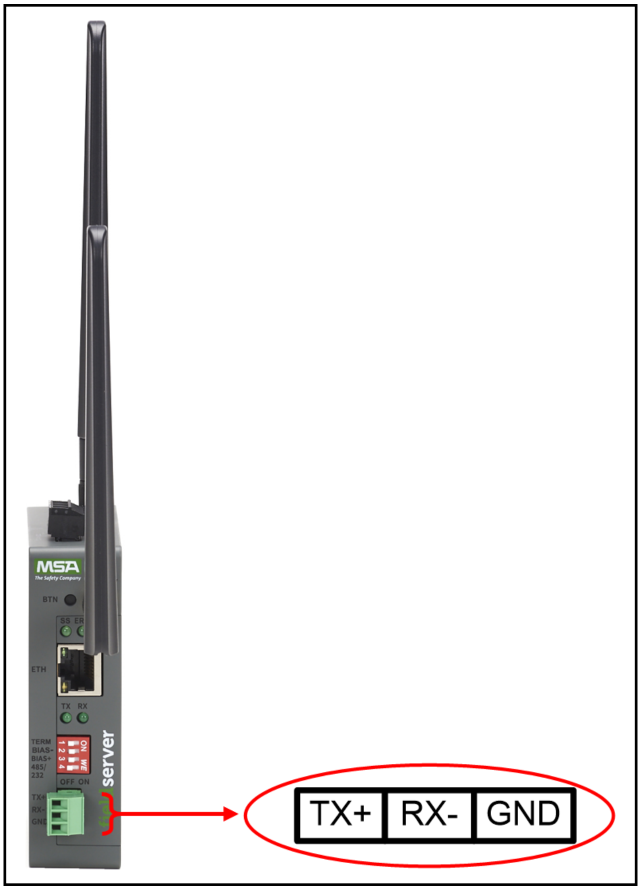
3.1.1 Wiring

RS-485	
BMS RS-485 Wiring	Gateway Pin Assignment
RS-485 +	TX +
RS-485 -	RX -
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 connected only at one end and to earth ground – it 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).

3.2 FS-IOT-BACA/V/F: Connecting the P1 Port

Switch between RS-485 and RS-232 by moving the number 4 DIP Switch left for RS-485 and right for RS-232. Connect to the 3-pin connector as shown below.



The following baud rates are supported on the P1 Port:
9600, 19200, 38400, 57600, 76800, 115000

NOTE: Not all baud rates listed are supported by all protocols. Check the specific protocol driver manual for a list of the supported baud rates.

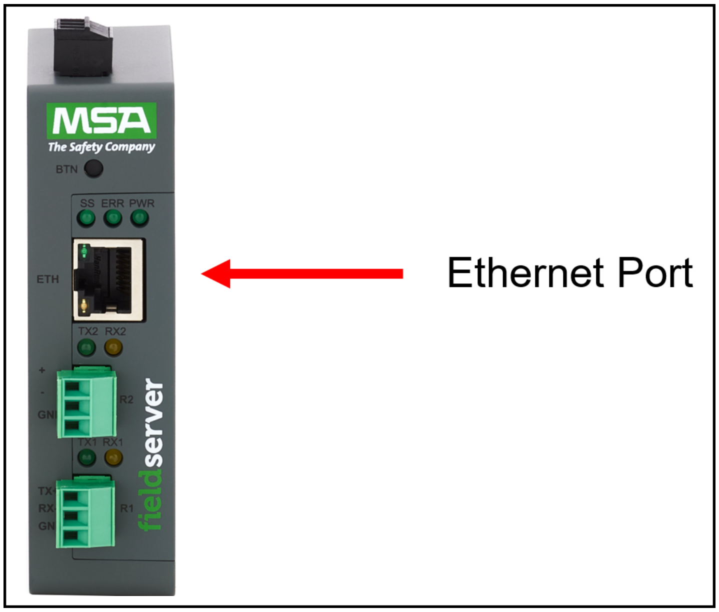
3.2.1 Wiring

RS-485	
BMS RS-485 Wiring	Gateway Pin Assignment
RS-485 +	TX +
RS-485 -	RX -
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 connected only at one end and to earth ground – it 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).

3.3 10/100 Ethernet Connection Port

NOTE: Do not use shielded Ethernet cables.



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.

3.4 Access BACnet IoT Gateway Using a Web Browser

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

NOTE: Check Section 11.9 Internet Browser Software Support for supported browsers.

4 Power up the Gateway

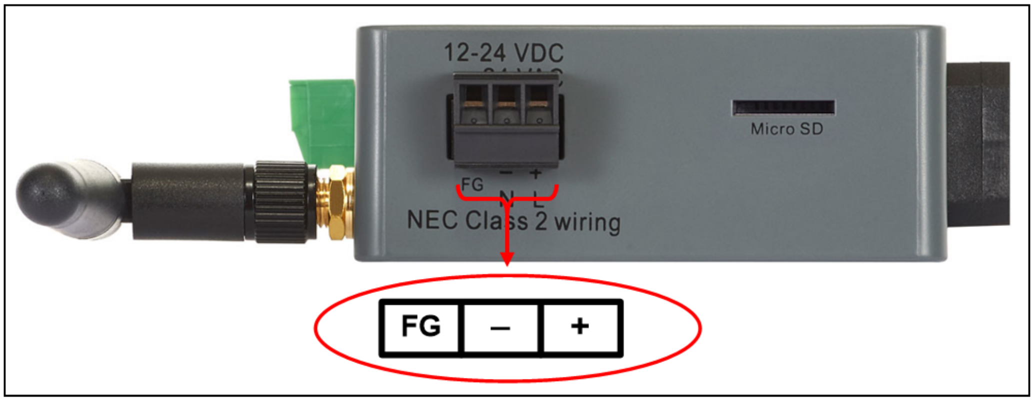
Check power requirements in the table below:

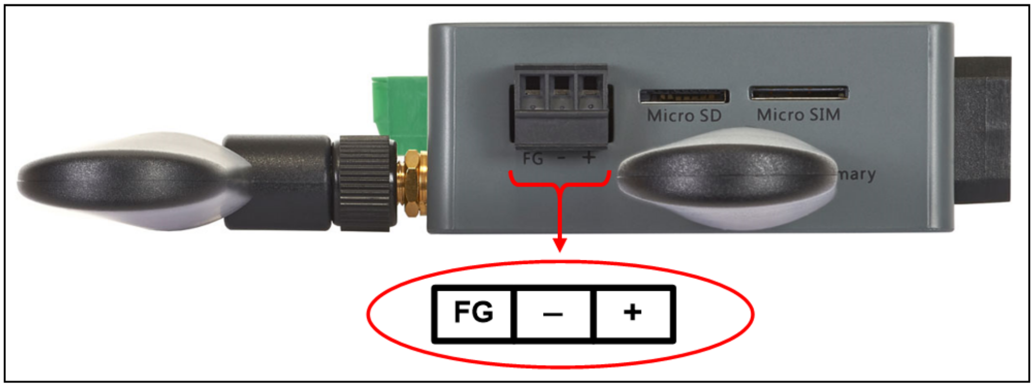
Power Requirement for BACnet IoT Gateway External Gateway			
	Current Draw Type		
BACnet IoT Gateway Family	12VDC	24VDC	24VAC
FS-IOT-BAC/BACW/BAC2 (Typical)	250mA	125mA	125mA
FS-IOT-BACA/V/F (Typical)	320mA	185mA	N/A
FS-IOT-BACA/V/F (Maximum)	670mA	390mA	N/A
NOTE: These values are 'nominal' and a safety margin should be added to the power supply of the host system. A safety margin of 25% is recommended.			

Apply power to the BACnet IoT Gateway as shown below. Ensure that the power supply used complies with the specifications provided . Ensure that the cable is grounded using the FG or "Frame GND" terminal.

- The FS-IOT-BAC/BACW/BAC2 BACnet IoT Gateway accepts 12-24VDC or 24VAC.
- The FS-IOT-BACA/V/F BACnet IoT Gateways accept 12-24VDC.
- 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: Only Class 2 PSU's must be used to power FieldServers.



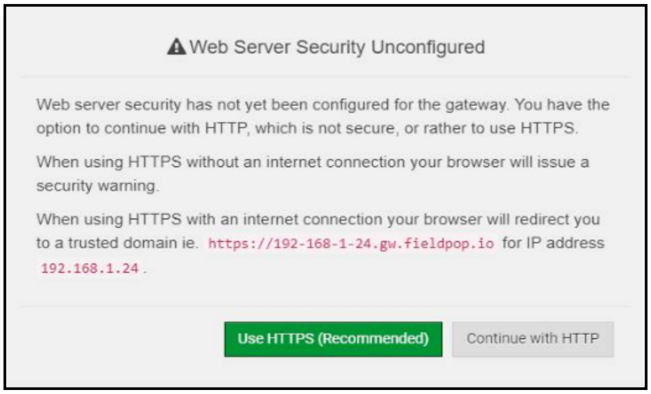


5 Setup Web Server Security

5.1 Login to the FieldServer

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

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



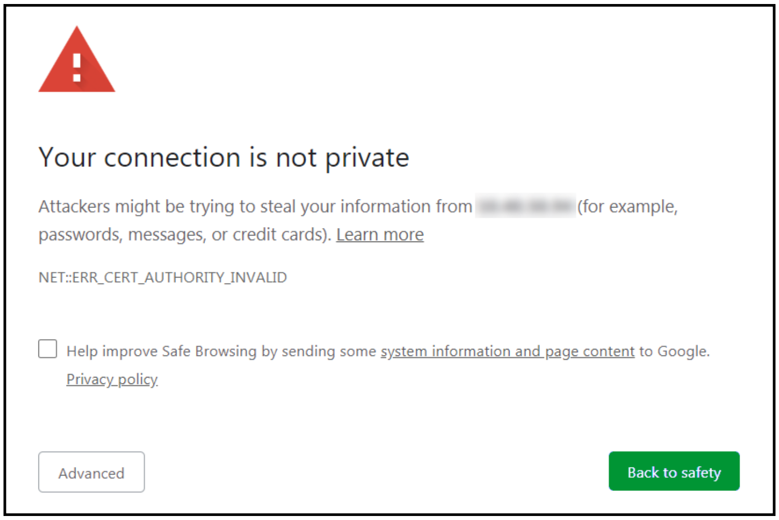
Web Server Security Unconfigured

Web server security has not yet been configured for the gateway. You have the option to continue with HTTP, which is not secure, or rather to use HTTPS.

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

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

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



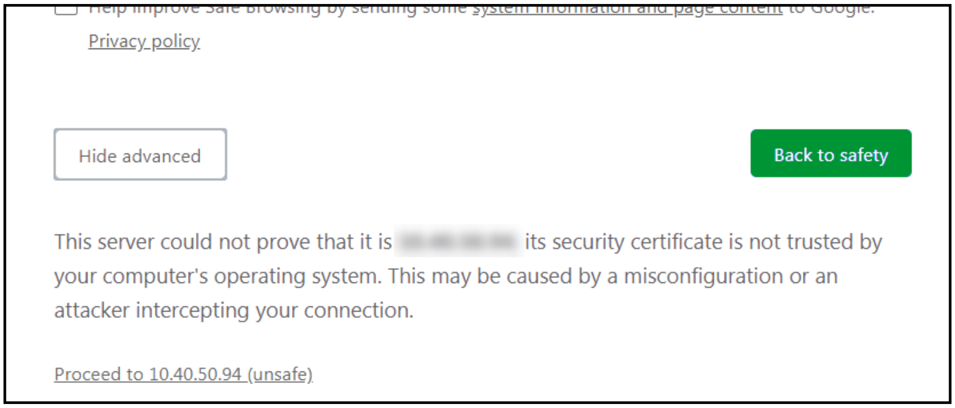
Your connection is not private

Attackers might be trying to steal your information from [redacted] (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

□ Help improve Safe Browsing by sending some system information and page content to Google. Privacy policy

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



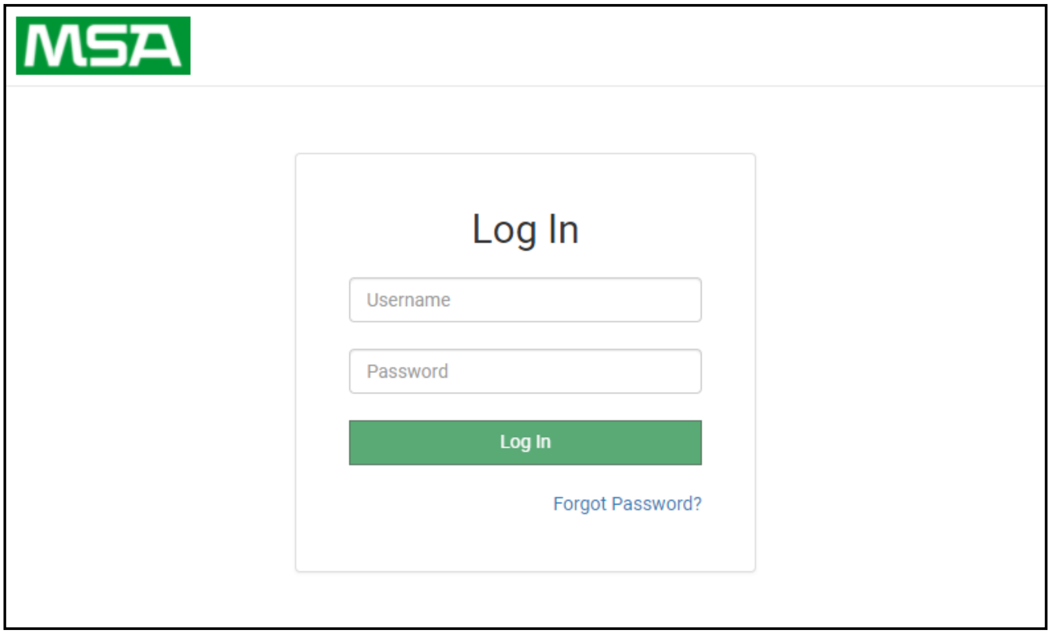
□ Help improve Safe Browsing by sending some system information and page content to Google.
Privacy policy

This server could not prove that it is [redacted] its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to 10.40.50.94 (unsafe)

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

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

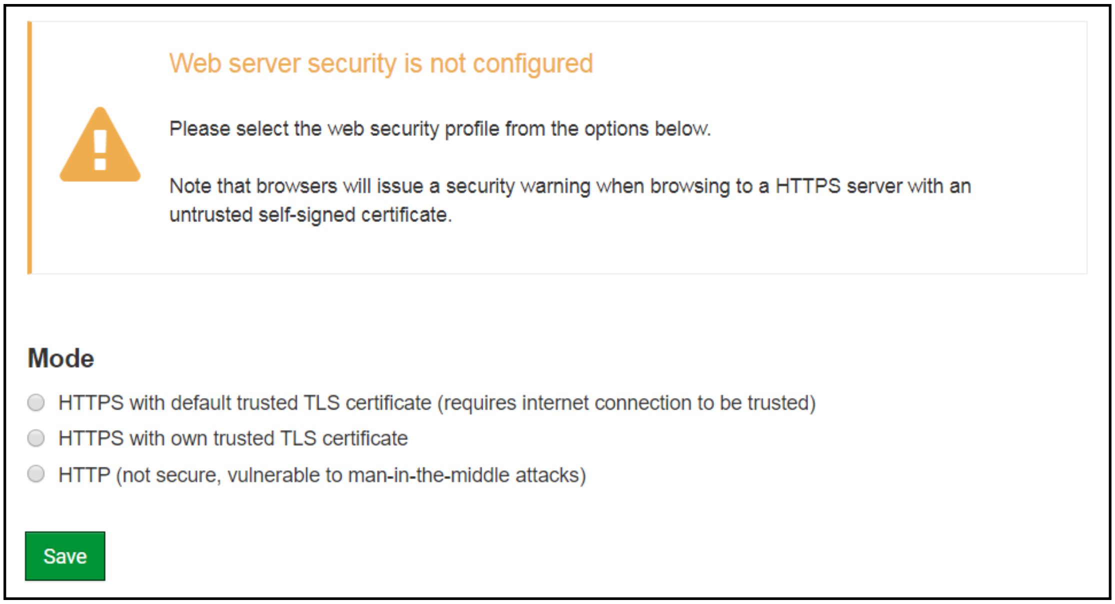


NOTE: A user has 5 attempts to login then there will be a 10-minute lockout. There is no timeout on the FieldServer to enter a password.

NOTE: To create individual user logins, go to Section 12.4 Change User Management Settings.

5.2 Select the Security Mode

On the first login to the FieldServer, the following screen will appear that allows the user to select which mode the FieldServer should use.



Web server security is not configured

Please select the web security profile from the options below.

Note that browsers will issue a security warning when browsing to a HTTPS server with an untrusted self-signed certificate.

Mode

○ HTTPS with default trusted TLS certificate (requires internet connection to be trusted)

○ HTTPS with own trusted TLS certificate

○ HTTP (not secure, vulnerable to man-in-the-middle attacks)

NOTE: Cookies are used for authentication.

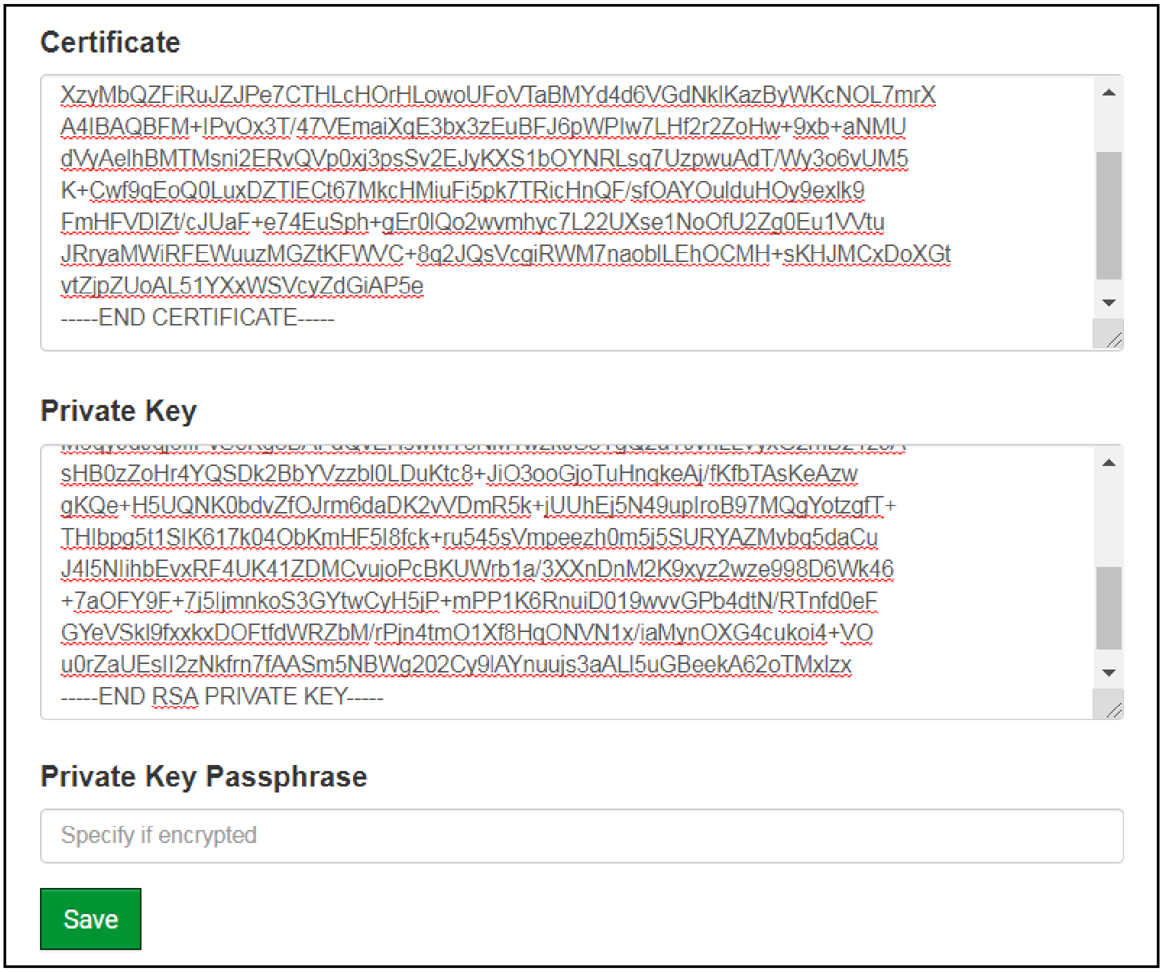
NOTE: To change the web server security mode after initial setup, go to Section 12.3 Change Web Server Security Settings After Initial Setup.

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

5.2.1 HTTPS with Own Trusted TLS Certificate

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

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



Certificate

```
XzyMbQZFiRuJZJPe7CTHLcHOrHLowoUFoVTaBMYd4d6VGdNklKazByWKcNOL7mrX
A4IBAQBFM+IPvOx3T/47VEmaiXqE3bx3zEuBFJ6pWPIw7LHf2r2ZoHw+9xb+aNMU
dVyAelhBMTMsni2ERvQVp0xj3psSv2EJyKXS1bOYNRLsq7UzpwuAdT/Wy3o6vUM5
K+Cwf9qEoQ0LuxDZTIECt67MkcHMiuFi5pk7TRicHnQF/sfOAYOulduHOy9exlk9
FmHFVDlZt/cJUaF+e74EuSph+gEr0lQo2wvmhyc7L22UXse1NoOfU2Zg0Eu1VVtu
JRryaMWiRFEWuuzMGZtKFWVC+8q2JQsVcgiRWM7naoblLEhOCMH+sKHJMCxDoXGt
vtZjpZUoAL51YXxWSVcyZdGiAP5e
-----END CERTIFICATE-----
```

Private Key

```
sHB0zZoHr4YQSDk2BbYVzzbl0LDuKtc8+JiO3ooGjoTuHnqkeAj/fKfbTAsKeAzw
gKQe+H5UQNK0bdvZfOJrm6daDK2vVDmR5k+jUUhEj5N49upIroB97MQgYotzgfT+
THIbpg5t1SIK617k04ObKmHF5l8fck+ru545sVmpeezh0m5j5SURYAZMvbq5daCu
J4I5NlihbEvxRF4UK41ZDMCvujoPcBKUWrb1a/3XXnDnM2K9xyz2wze998D6Wk46
+7aOFY9F+7j5IjmnkoS3GYtwCyH5jP+mPP1K6RnuiD019wvvGPb4dtN/RTnfd0eF
GYeVSkl9fxxkxDOFtfdWRZbM/rPjn4tmO1Xf8HqONVN1x/iaMynOXG4cukoi4+VO
u0rZaUEsII2zNkfrn7fAASm5NBWg202Cy9lAYnuujs3aALI5uGBeekA62oTMxlzx
-----END RSA PRIVATE KEY-----
```

Private Key Passphrase

Specify if encrypted

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

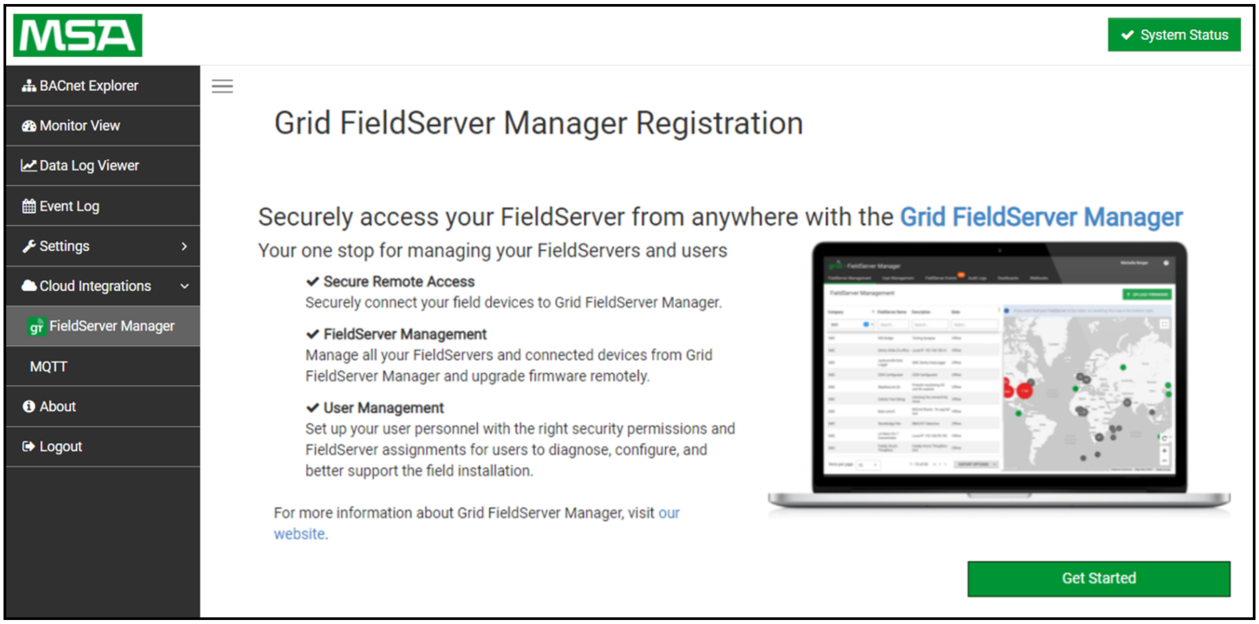
5.2.2 HTTPS with Default Untrusted Self-Signed TLS Certificate or HTTP with Built-in Payload Encryption

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

6 Setup Network

6.1 Navigate to the Network Settings

- From the Web App landing page, click the Settings tab on the left side of the screen.



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

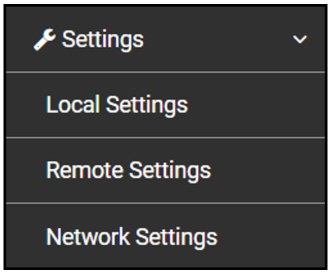
Manage all your FieldServers and connected devices from Grid FieldServer Manager and upgrade firmware remotely.

✓ User Management

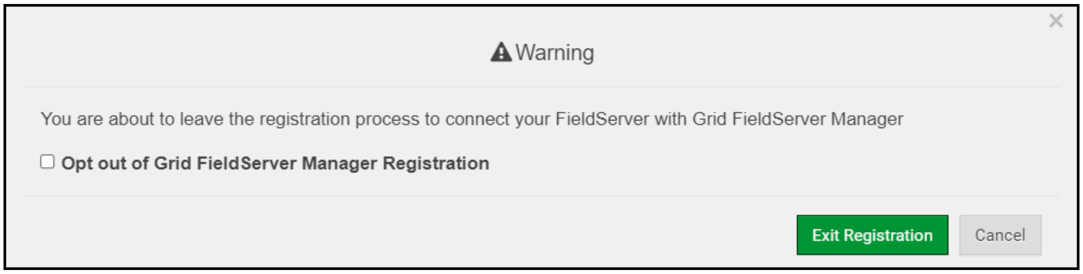
Set up your user personnel with the right security permissions and FieldServer assignments for users to diagnose, configure, and better support the field installation.

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

- The BACnet IoT Gateway settings are split up into three types: Local Settings, Remote Settings and Network Settings.



- A warning message will appear when performing the first-time setup, click the Exit Registration button to continue to the Settings page.



⚠ Warning

You are about to leave the registration process to connect your FieldServer with Grid FieldServer Manager

☐ Opt out of Grid FieldServer Manager Registration

The following sections explain the setting parameters by type for BACnet IoT Gateway configuration.The table below describes how the buttons at the bottom of each page function.

Button	Definition
Save	Click to save settings. Saving will require the device to be restarted.
Refresh	Click to clear the current settings before saving; if current settings are saved the Refresh button is unavailable.
Defaults	Click to change settings back to factory defaults.

6.1.1 Ethernet 1

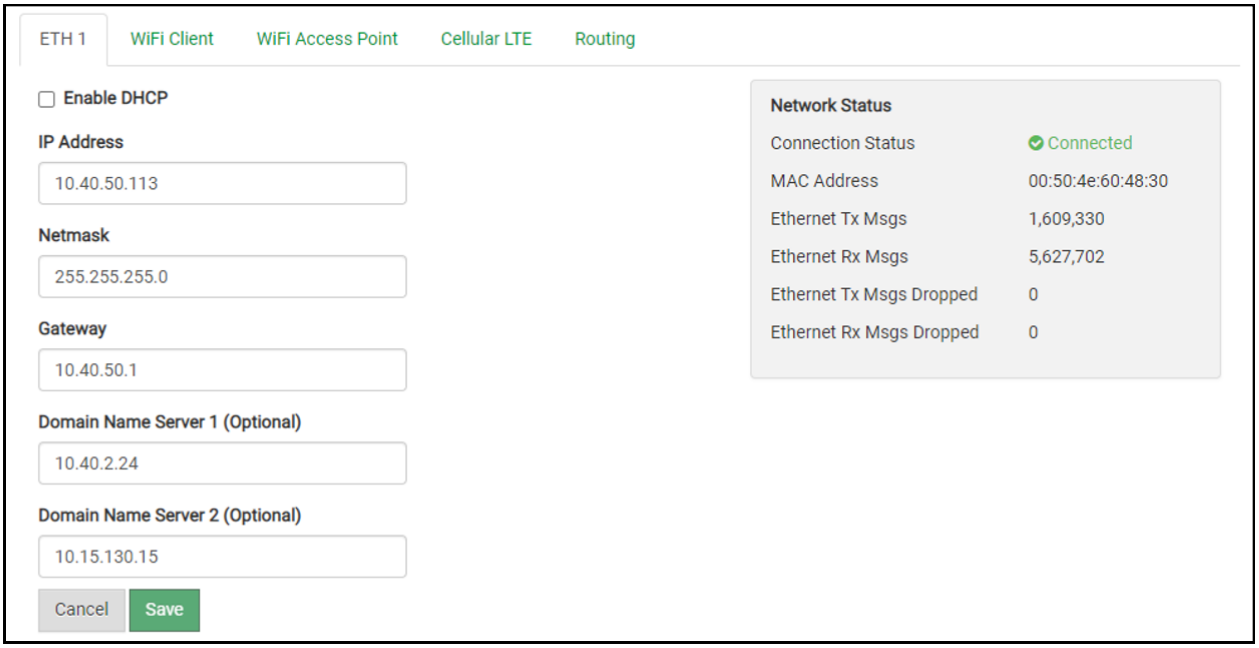
The ETH 1 tab is the landing page when selecting Network Settings. To change the FieldServer IP Settings, follow these instructions:

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

NOTE: If the FieldServer is connected to a router, the IP Gateway of the FieldServer should be set to the same IP Address of the router.

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

NOTE: The browser needs to be updated to the new IP Address of the FieldServer before the settings will be accessible again.



☐ Enable DHCP

IP Address: 10.40.50.113

Netmask: 255.255.255.0

Gateway: 10.40.50.1

Domain Name Server 1 (Optional): 10.40.2.24

Domain Name Server 2 (Optional): 10.15.130.15

Network Status

Connection Status	✓ Connected
MAC Address	00:50:4e:60:48:30
Ethernet Tx Msgs	1,609,330
Ethernet Rx Msgs	5,627,702
Ethernet Tx Msgs Dropped	0
Ethernet Rx Msgs Dropped	0

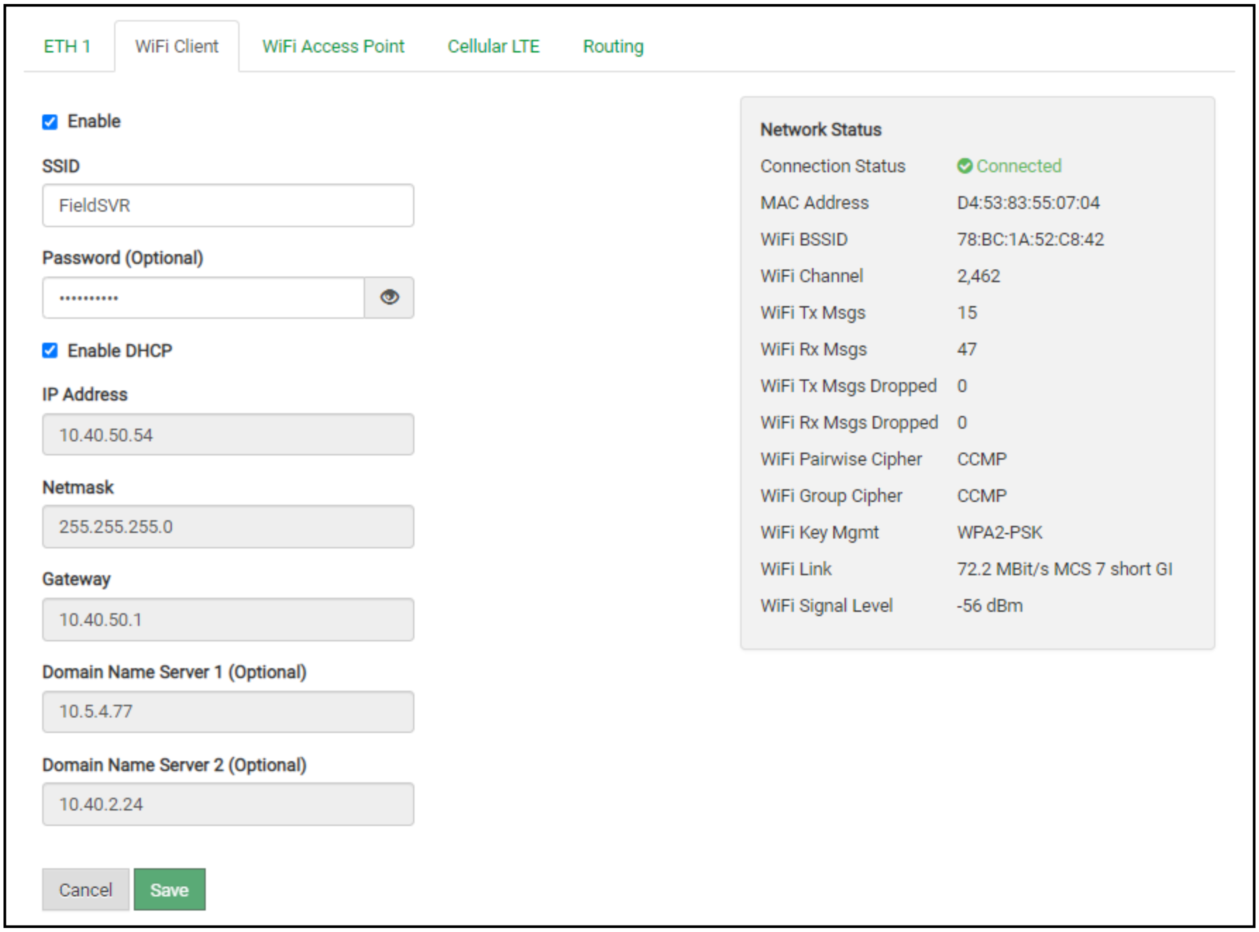
IP Setting Fields	Definition
Connection Status	Status of connection
MAC Address	Ethernet MAC Address
Tx/Rx Msgs	Number of transmitted and received messages
Tx/Rx Msgs Dropped	Number of unanswered Tx or Rx messages

6.1.2 Wi-Fi Client Settings

- Set the Wi-Fi Status to ENABLED for the BACnet IoT Gateway to communicate with other devices via Wi-Fi.
- Enter the Wi-Fi SSID and Wi-Fi Password for the local wireless access point.
- Enable DHCP to automatically assign all Wi-Fi Client Settings fields or modify the Settings manually, via the fields immediately below the note (IP Address, Network, etc.).

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

- Click the Save button to activate the new settings.
- Go to Routing (**Section 6.1.4 Routing Settings**) to set the default connection to Wi-Fi Client.



☑ Enable

SSID: FieldSVR

Password (Optional): ••••••••••

☑ Enable DHCP

IP Address: 10.40.50.54

Netmask: 255.255.255.0

Gateway: 10.40.50.1

Domain Name Server 1 (Optional): 10.5.4.77

Domain Name Server 2 (Optional): 10.40.2.24

Network Status

Connection Status	✓ Connected
MAC Address	D4:53:83:55:07:04
WiFi BSSID	78:BC:1A:52:C8:42
WiFi Channel	2,462
WiFi Tx Msgs	15
WiFi Rx Msgs	47
WiFi Tx Msgs Dropped	0
WiFi Rx Msgs Dropped	0
WiFi Pairwise Cipher	CCMP
WiFi Group Cipher	CCMP
WiFi Key Mgmt	WPA2-PSK
WiFi Link	72.2 MBit/s MCS 7 short GI
WiFi Signal Level	-56 dBm

Wi-Fi Client Fields	Definition
Connection Status	Status of connection
MAC Address, BSSID, Channel	Wi-Fi Client MAC Address, BSSID, and Channel
Tx/Rx Msgs	Number of transmitted and received messages
Tx/Rx Msgs Dropped	Number of unanswered Tx or Rx messages
Pairwise Cipher	Type of encryption used for unicast traffic
Group Cipher	Identifies the type of encryption used for multicast / broadcast traffic
Key Mgmt	Encryption type
Link	Connection speed
Signal Level	Signal level in dBm (see **Section 11.7 Wi-Fi and Cellular Signal Strength**)

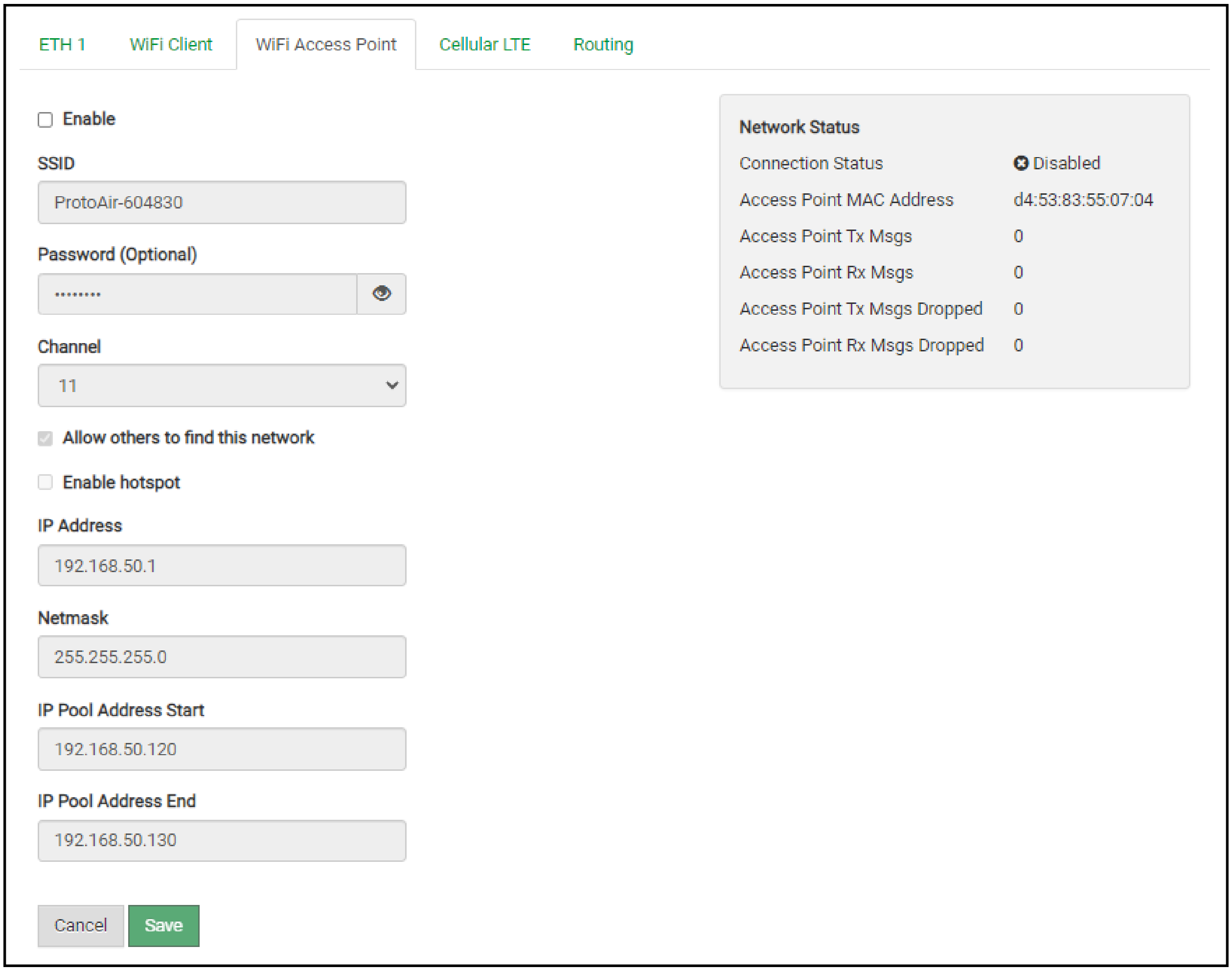
6.1.3 Wi-Fi Access Point Settings

- Check the Enable tick box to allow connecting to the BACnet IoT Gateway via Wi-Fi Access Point.
- Modify the Settings manually as needed, via these fields: SSID, Password, Channel, IP Address, Netmask, IP Pool Address Start, and IP Pool Address End.

NOTE: The default channel is 11. The default IP Address is 192.168.50.1. See the rest of the default settings listed in the screenshot below.

- Click the Save button to activate the new settings.

NOTE: If the webpage was open in a browser via Wi-Fi, the browser will need to be updated with the new Wi-Fi details before the webpage will be accessible again.



□ Enable

SSID: ProtoAir-604830

Password (Optional): ••••••••

Channel: 11

☑ Allow others to find this network

□ Enable hotspot

IP Address: 192.168.50.1

Netmask: 255.255.255.0

IP Pool Address Start: 192.168.50.120

IP Pool Address End: 192.168.50.130

Network Status

Connection Status	☒ Disabled
Access Point MAC Address	d4:53:83:55:07:04
Access Point Tx Msgs	0
Access Point Rx Msgs	0
Access Point Tx Msgs Dropped	0
Access Point Rx Msgs Dropped	0

Wi-Fi AP Fields	Definition
Connection Status	Status of connection
MAC Address	Access Point's MAC Address
Tx/Rx Msgs	Number of transmitted and received messages
Tx/Rx Msgs Dropped	Number of unanswered Tx or Rx messages

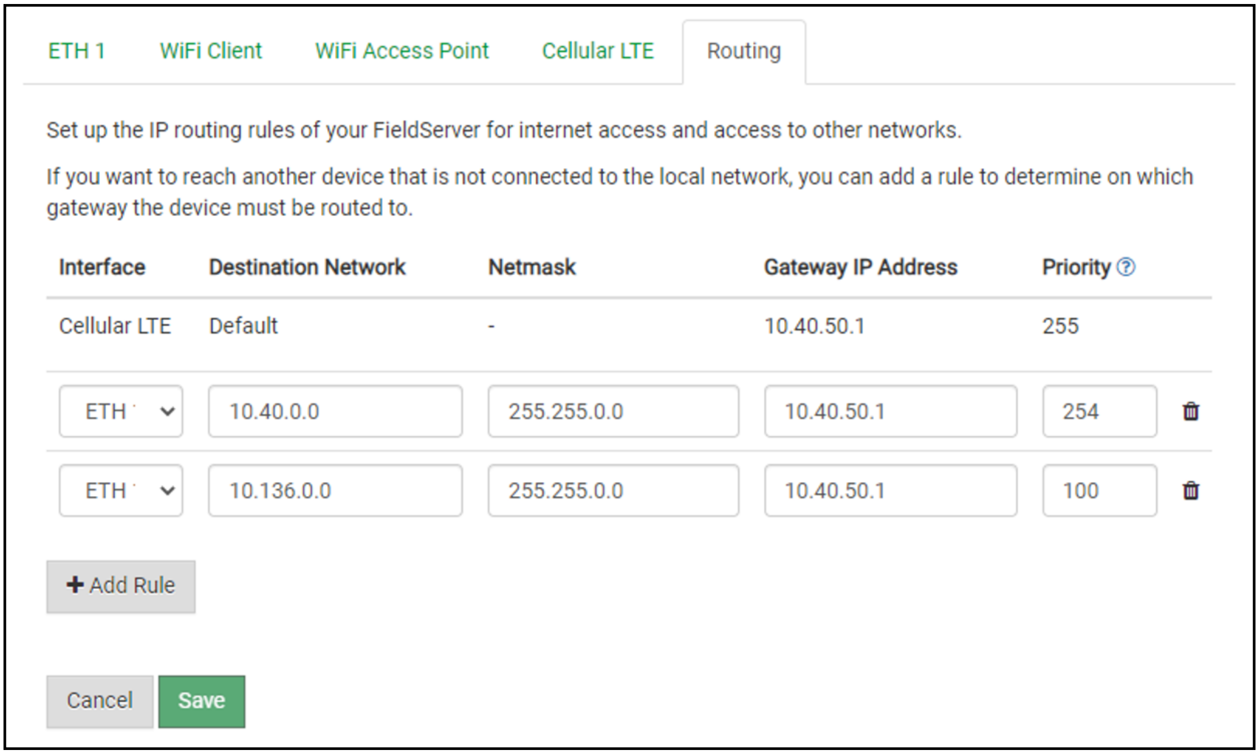
6.1.4 Routing Settings

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

NOTE: The default connection is ETH1.

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

NOTE: If using Wi-Fi Client and not Ethernet, make the top priority rule a Wi-Fi Client connection.



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

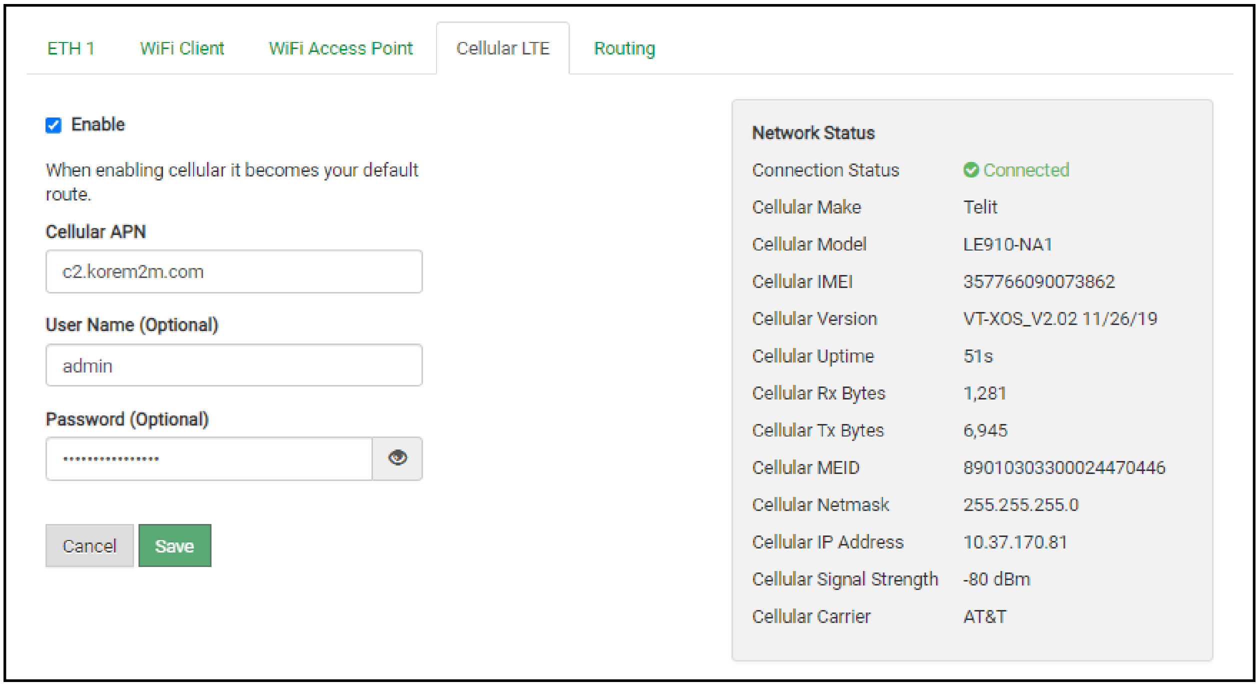
If you want to reach another device that is not connected to the local network, you can add a rule to determine on which gateway the device must be routed to.

Interface	Destination Network	Netmask	Gateway IP Address	Priority ?
Cellular LTE	Default	-	10.40.50.1	255
ETH	10.40.0.0	255.255.0.0	10.40.50.1	254
ETH	10.136.0.0	255.255.0.0	10.40.50.1	100

6.1.5 FS-IOT-BACA/V/F: Cellular Settings

To change the Cellular settings, follow these instructions:

- Check the Enable tick box to allow connecting to the BACnet IoT Gateway through the Grid.
- Modify the Settings manually as needed, via these fields: Cellular APN (see **Section 12.2 APN Table**), User Name, and Password.
- Click the Save button to activate the new settings.
- Power cycle the BACnet IoT Gateway to update settings.



☑ Enable

When enabling cellular it becomes your default route.

Cellular APN

c2.korem2m.com

User Name (Optional)

admin

Password (Optional)

••••••••••••••••

Network Status	
Connection Status	✓ Connected
Cellular Make	Telit
Cellular Model	LE910-NA1
Cellular IMEI	357766090073862
Cellular Version	VT-XOS_V2.02 11/26/19
Cellular Uptime	51s
Cellular Rx Bytes	1,281
Cellular Tx Bytes	6,945
Cellular MEID	89010303300024470446
Cellular Netmask	255.255.255.0
Cellular IP Address	10.37.170.81
Cellular Signal Strength	-80 dBm
Cellular Carrier	AT&T

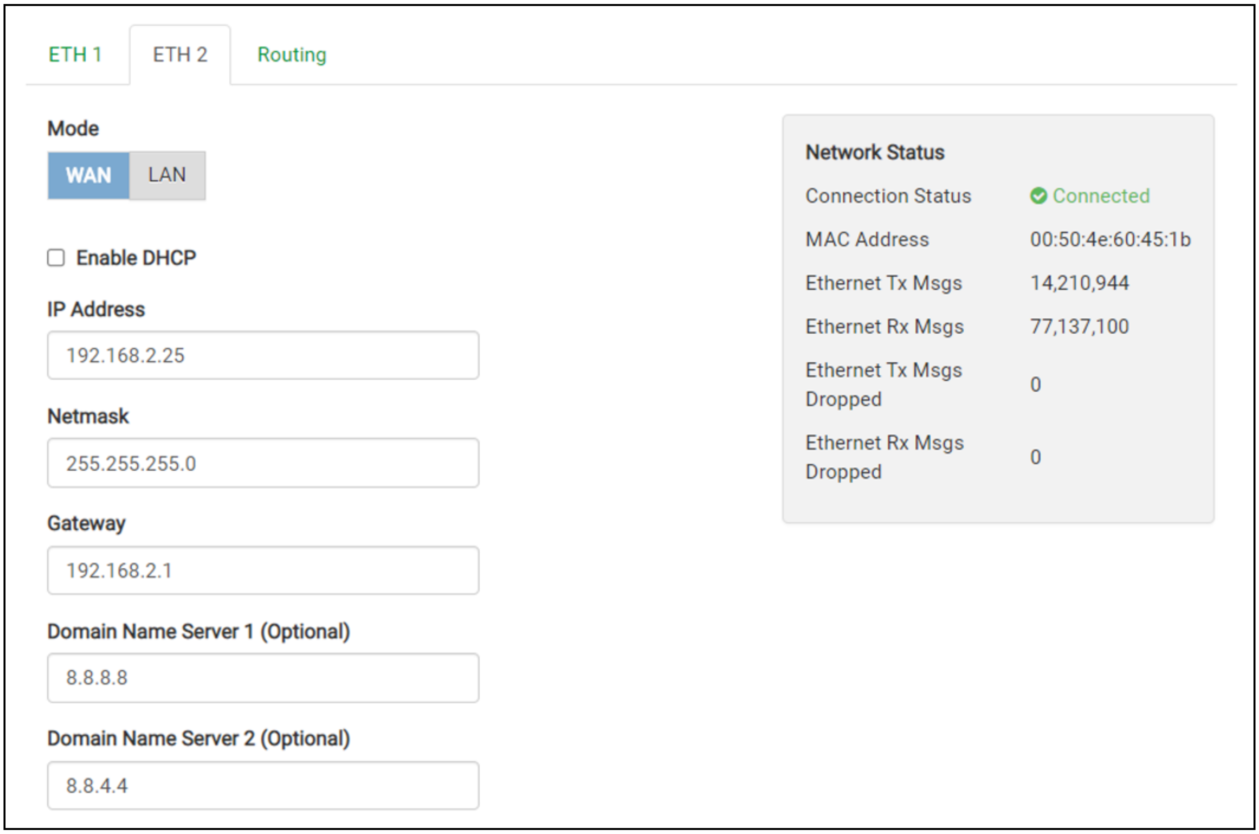
6.1.6 FS-IOT-BAC2: Ethernet 1 and Ethernet 2 Network Settings – LAN Mode

- 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 FieldServer to the local network or router.

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



Mode

☐ Enable DHCP

IP Address
192.168.2.25

Netmask
255.255.255.0

Gateway
192.168.2.1

Domain Name Server 1 (Optional)
8.8.8.8

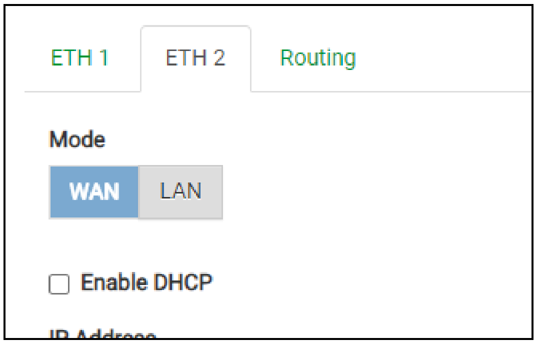
Domain Name Server 2 (Optional)
8.8.4.4

Network Status

Connection Status	✓ Connected
MAC Address	00:50:4e:60:45:1b
Ethernet Tx Msgs	14,210,944
Ethernet Rx Msgs	77,137,100
Ethernet Tx Msgs Dropped	0
Ethernet Rx Msgs Dropped	0

6.1.7 FS-IOT-BAC2: Ethernet 2 Network Settings – WAN Mode

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



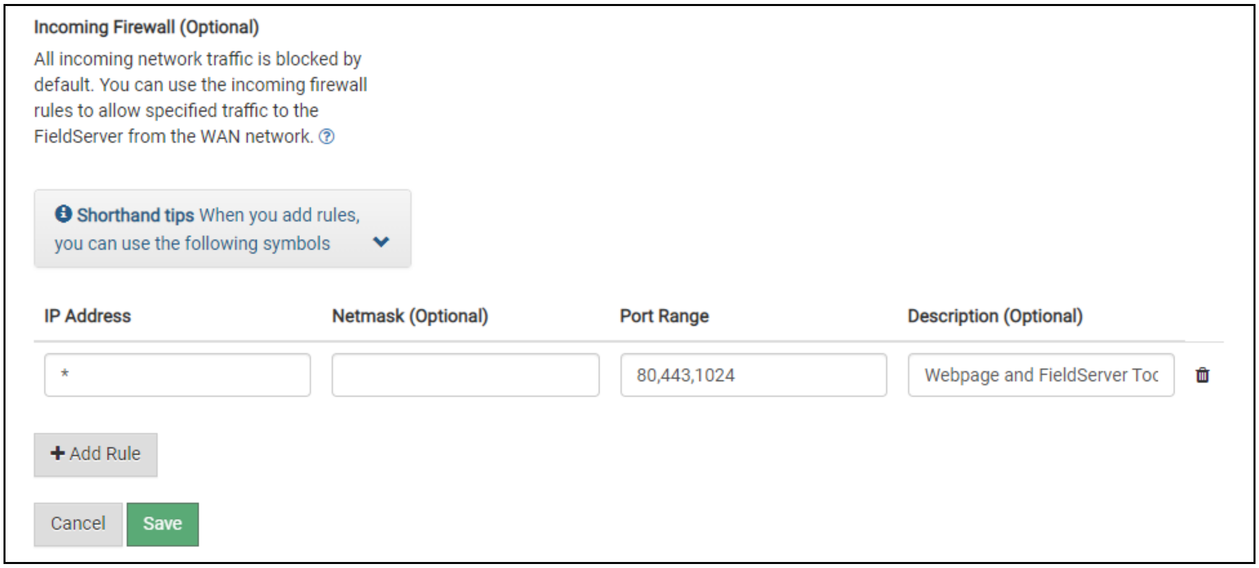
Mode

WAN | LAN

□ Enable DHCP

IP Address

- 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

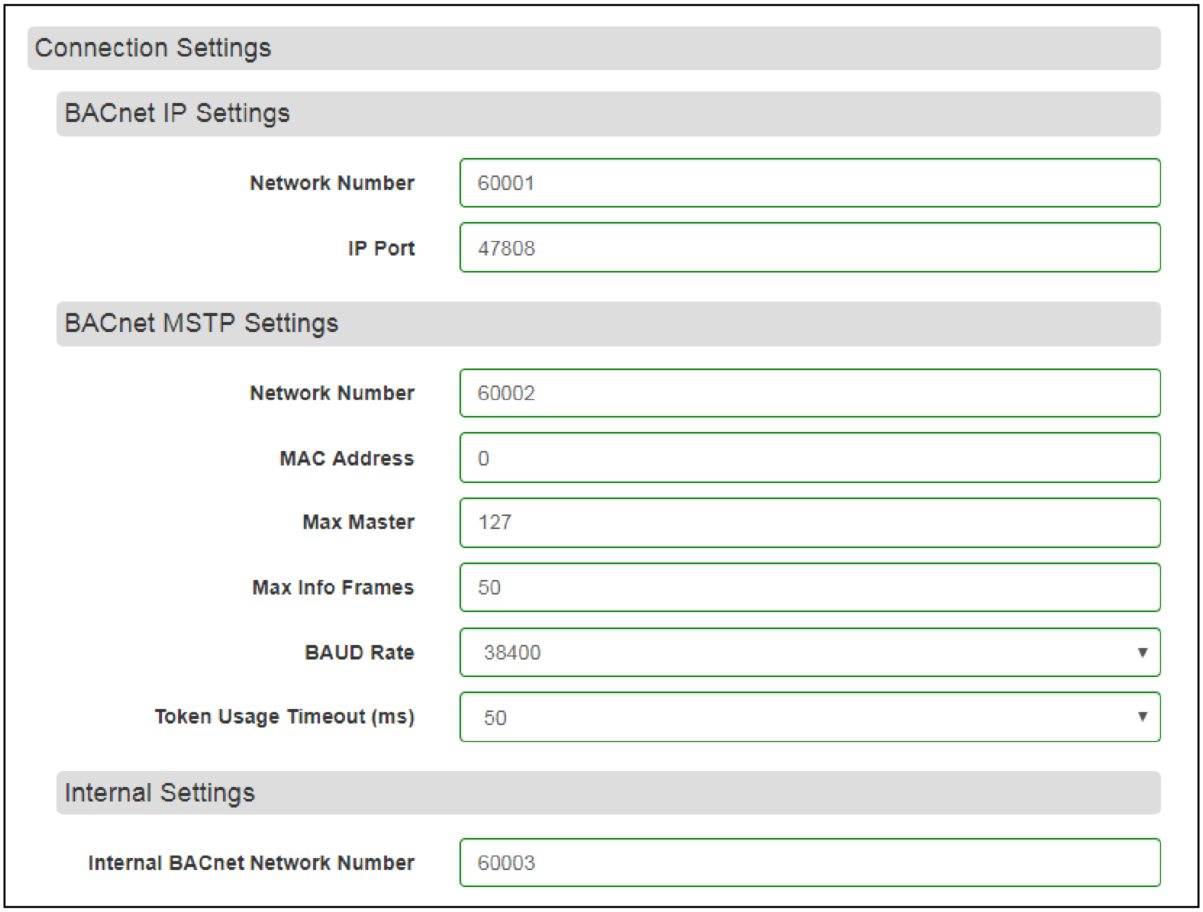
IP Address	Netmask (Optional)	Port Range	Description (Optional)
*		80,443,1024	Webpage and FieldServer Toc

NOTE the following options for setting firewall rules:

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

6.2 Local Settings – BACnet

Enter the fields for the settings described below as needed:



Connection Settings

BACnet IP Settings

Network Number: 60001

IP Port: 47808

BACnet MSTP Settings

Network Number: 60002

MAC Address: 0

Max Master: 127

Max Info Frames: 50

BAUD Rate: 38400

Token Usage Timeout (ms): 50

Internal Settings

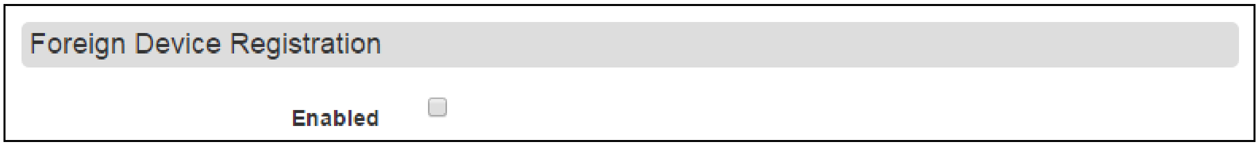
Internal BACnet Network Number: 60003

Parameter	Definition
All Connections	
Network Number	The BACnet network number for the connection. Legal values are 1-65534. Each network number must be unique across the entire BACnet network. The Internal Network Number is used for internal BACnet traffic and has to be unique across the BACnet network.
BACnet/IP Settings	
IP Port	The BACnet/IP default is 47808 (0xBAC0), but other port numbers can be specified.
BACnet MS/TP Settings	
MAC Address	Legal values are 0-127, must be unique on the physical network.
Max Master	The highest MAC address to scan for other MS/TP master devices. The default of 127 is guaranteed to discover all other MS/TP master devices on the network.
Max Info Frames	Transactions the BACnet IoT Gateway may initiate while it has the MS/TP token. Default is 50.
BAUD Rate	The serial baud rate used on the network.
Token Usage Timeout (ms)	Milliseconds the router waits before deciding that another master has dropped the MS/TP token. This value must be between 20ms and 100ms. Choose a larger value to improve reliability when working with slow MS/TP devices that may not be able to meet strict timing specifications.

6.3 Remote Settings – Foreign Device Registration for BBMD Support

The BACnet IoT Gateway uses “Foreign Device Registration” or “FDR” to communicate to BACnet/IP devices on another network. Follow the instructions below to enable FDR between the BACnet IoT Gateway and a remote network:

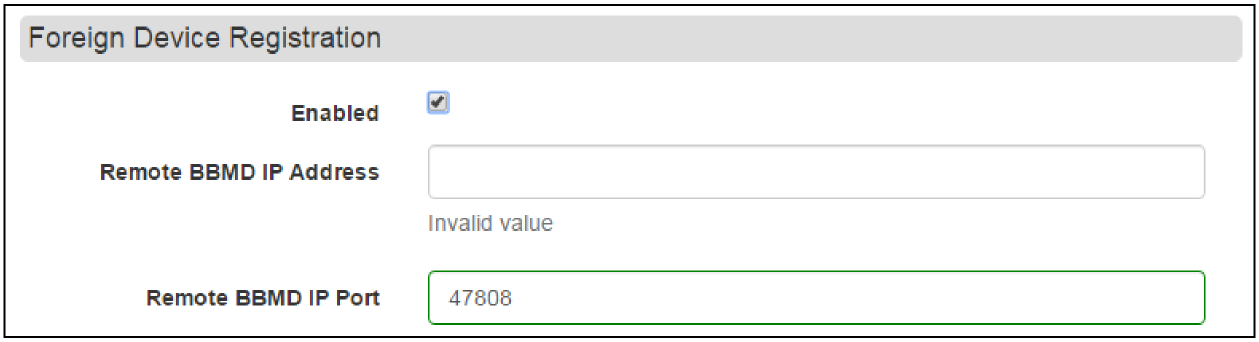
- Click the “Enabled” checkbox under the Foreign Device Registration section of the BACnet Settings.



Foreign Device Registration

Enabled □

- Enter the Remote BACnet Router’s externally mapped IP Address and BACnet/IP Port to the appropriate Foreign Device Registration fields. This allows the BACnet IoT Gateway to discover BACnet devices on the remote network.



Foreign Device Registration

Enabled ☑

Remote BBMD IP Address

Invalid value

Remote BBMD IP Port 47808

NOTE: The user must uncheck the “Enabled” checkbox to allow the BACnet IoT Gateway to discover on the local network.

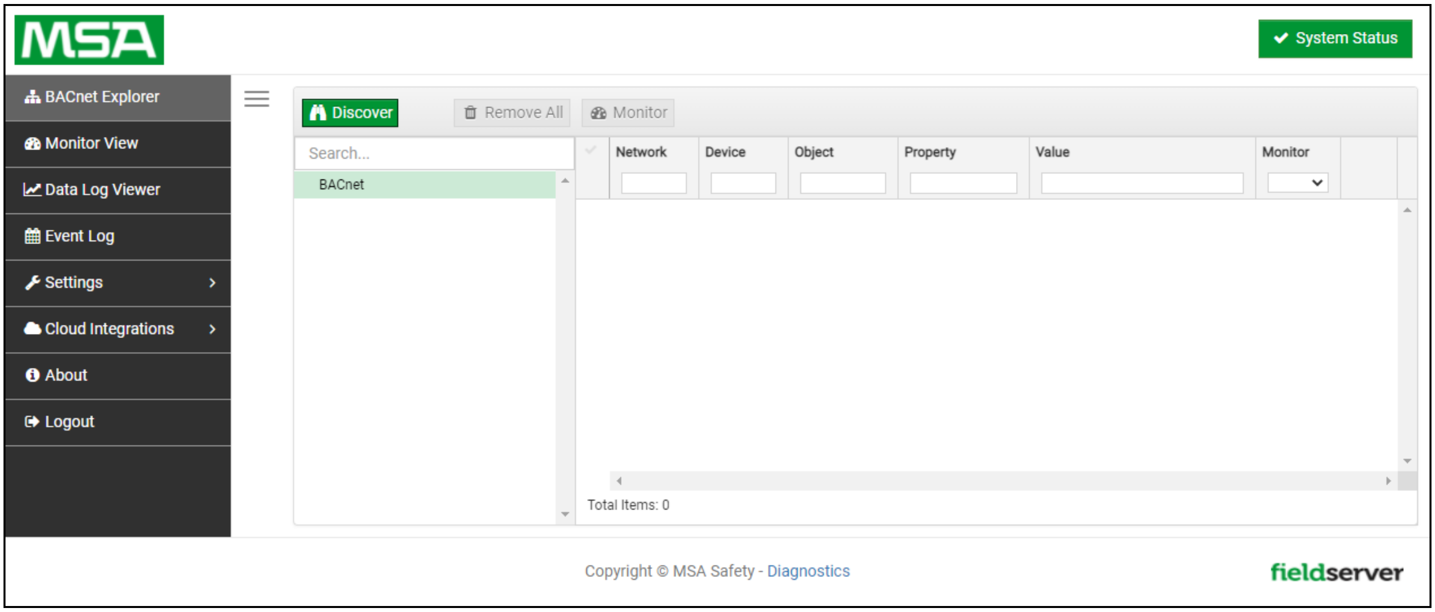
NOTE: See Section 10 References for additional details concerning FDR and BBMD.

7 Using the BACnet IoT Gateway

Sections 7.1 – 7.4 represent each of the first four tabs that appear across the left side of the page once logged into the BACnet IoT Gateway and describe their functions.

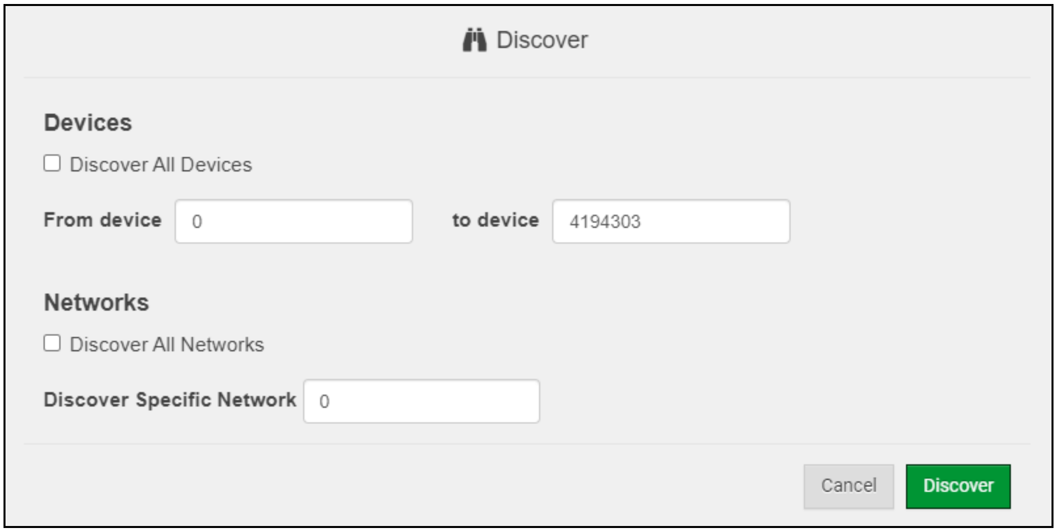
7.1 BACnet Explorer

Click on the BACnet Explorer tab on the left side of the page to open the BACnet Explorer page.



7.1.1 Discover Device List

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



Discover

Devices

☐ Discover All Devices

From device 0 to device 4194303

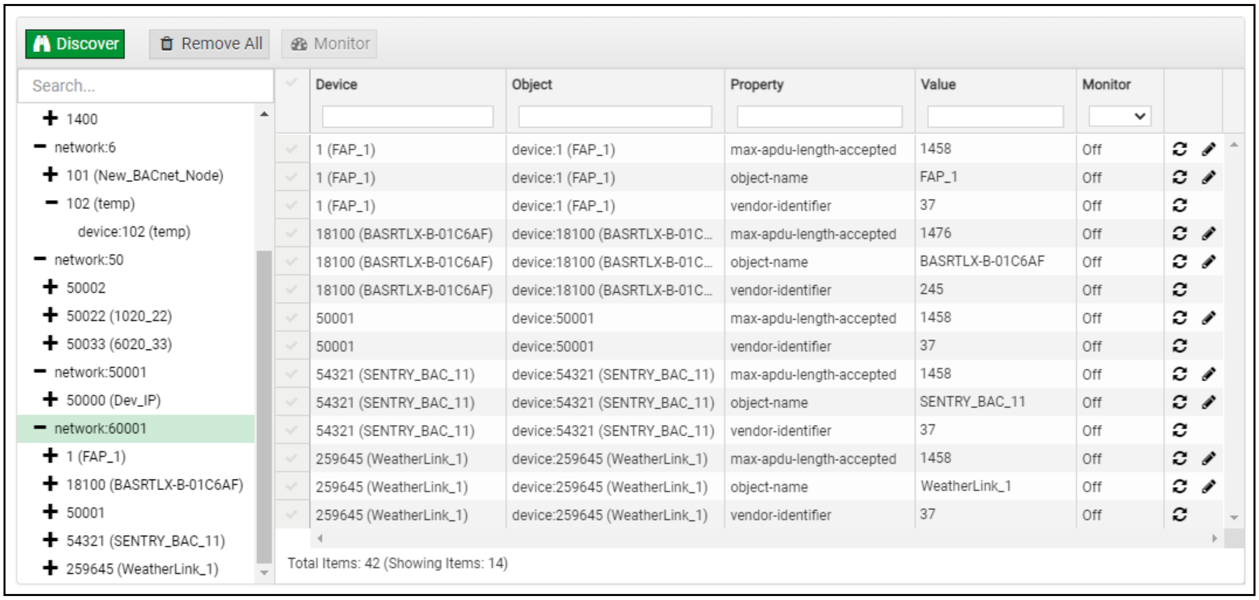
Networks

☐ Discover All Networks

Discover Specific Network 0

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

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.

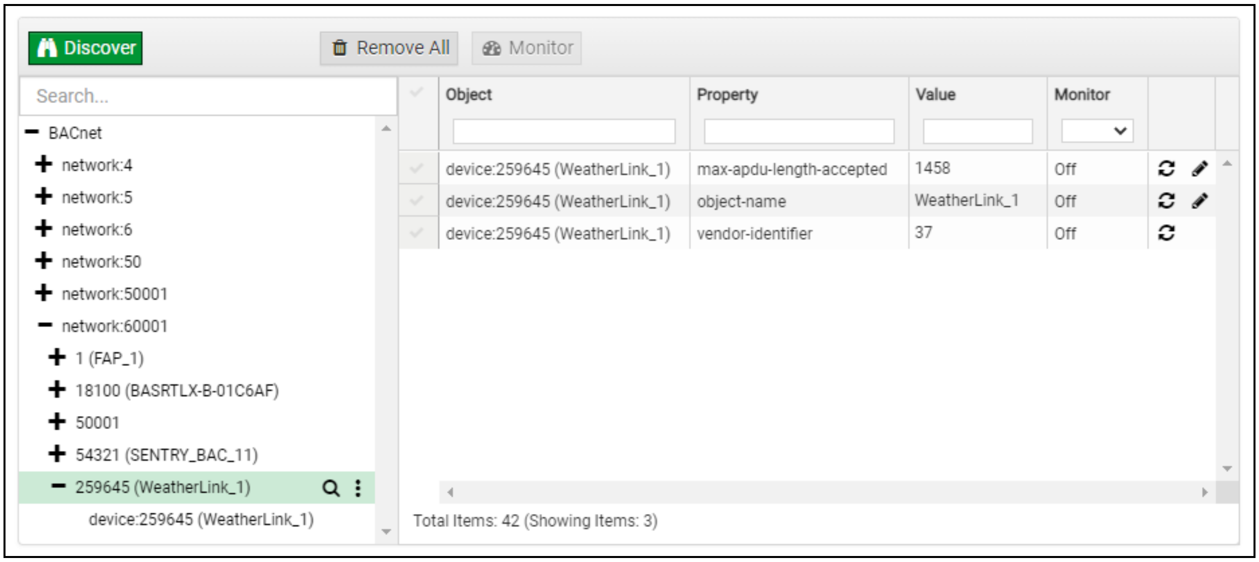


Device	Object	Property	Value	Monitor
1 (FAP_1)	device:1 (FAP_1)	max-apdu-length-accepted	1458	Off
1 (FAP_1)	device:1 (FAP_1)	object-name	FAP_1	Off
1 (FAP_1)	device:1 (FAP_1)	vendor-identifier	37	Off
18100 (BASRTLX-B-01C6AF)	device:18100 (BASRTLX-B-01C...	max-apdu-length-accepted	1476	Off
18100 (BASRTLX-B-01C6AF)	device:18100 (BASRTLX-B-01C...	object-name	BASRTLX-B-01C6AF	Off
18100 (BASRTLX-B-01C6AF)	device:18100 (BASRTLX-B-01C...	vendor-identifier	245	Off
50001	device:50001	max-apdu-length-accepted	1458	Off
50001	device:50001	vendor-identifier	37	Off
54321 (SENTRY_BAC_11)	device:54321 (SENTRY_BAC_11)	max-apdu-length-accepted	1458	Off
54321 (SENTRY_BAC_11)	device:54321 (SENTRY_BAC_11)	object-name	SENTRY_BAC_11	Off
54321 (SENTRY_BAC_11)	device:54321 (SENTRY_BAC_11)	vendor-identifier	37	Off
259645 (WeatherLink_1)	device:259645 (WeatherLink_1)	max-apdu-length-accepted	1458	Off
259645 (WeatherLink_1)	device:259645 (WeatherLink_1)	object-name	WeatherLink_1	Off
259645 (WeatherLink_1)	device:259645 (WeatherLink_1)	vendor-identifier	37	Off

Total Items: 42 (Showing Items: 14)

7.1.2 View Device Details and Explore Points/Parameters

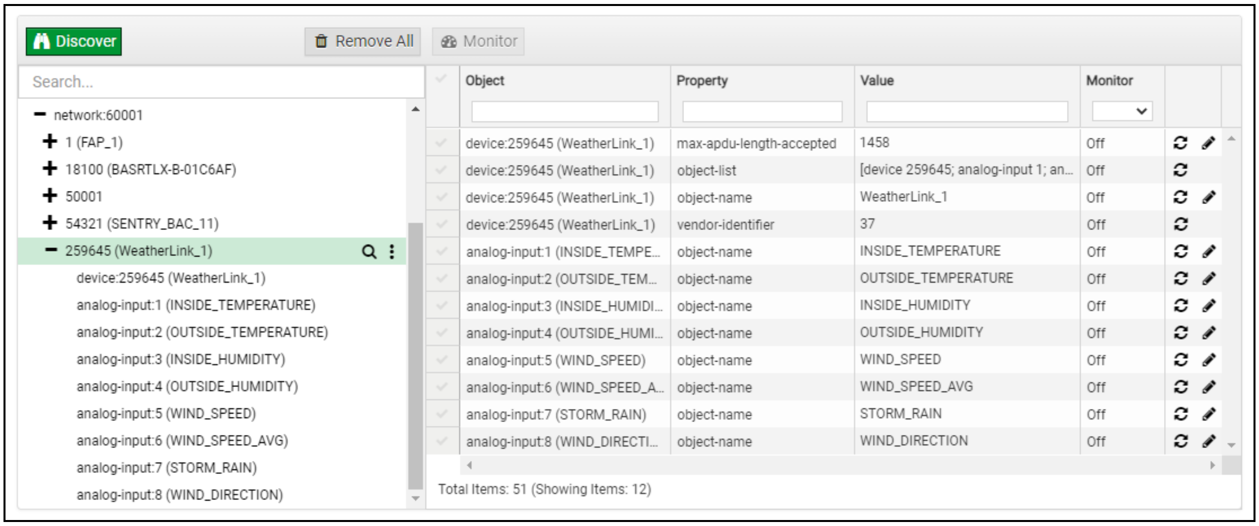
- To view the device details, click the blue plus sign (✚) next to the desired device in the list.
  - This will show only some of the device properties for the selected aspect of a device



Object	Property	Value	Monitor
device:259645 (WeatherLink_1)	max-apdu-length-accepted	1458	Off
device:259645 (WeatherLink_1)	object-name	WeatherLink_1	Off
device:259645 (WeatherLink_1)	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.



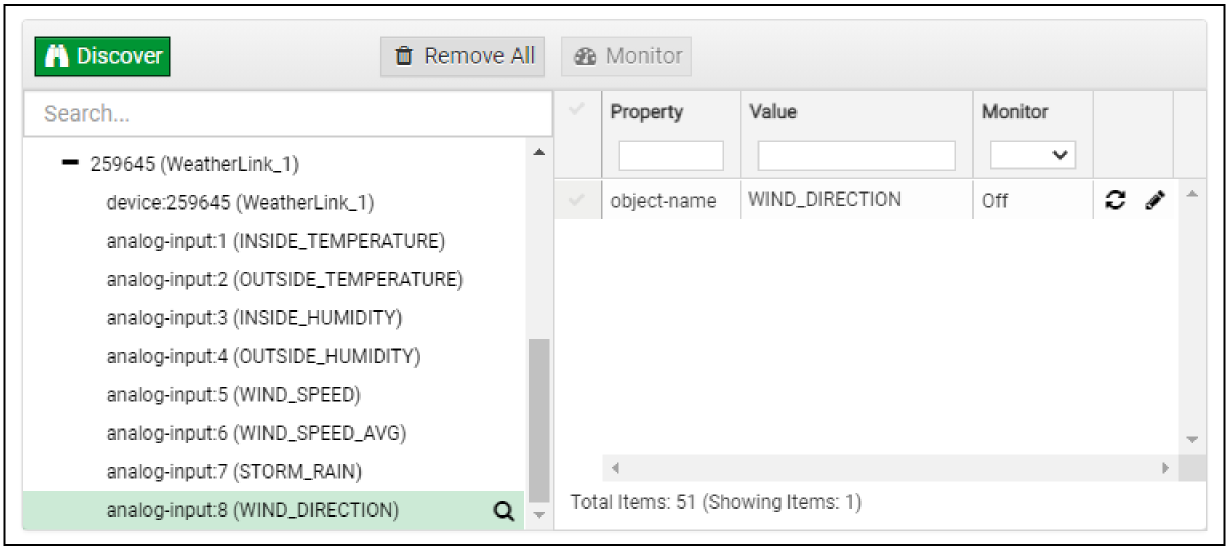
- network:60001
  - 1 (FAP_1)
  - 18100 (BASRTLX-B-01C6AF)
  - 50001
  - 54321 (SENTRY_BAC_11)
  - 259645 (WeatherLink_1)
    - device:259645 (WeatherLink_1)
    - analog-input:1 (INSIDE_TEMPERATURE)
    - analog-input:2 (OUTSIDE_TEMPERATURE)
    - analog-input:3 (INSIDE_HUMIDITY)
    - analog-input:4 (OUTSIDE_HUMIDITY)
    - analog-input:5 (WIND_SPEED)
    - analog-input:6 (WIND_SPEED_AVG)
    - analog-input:7 (STORM_RAIN)
    - analog-input:8 (WIND_DIRECTION)

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.

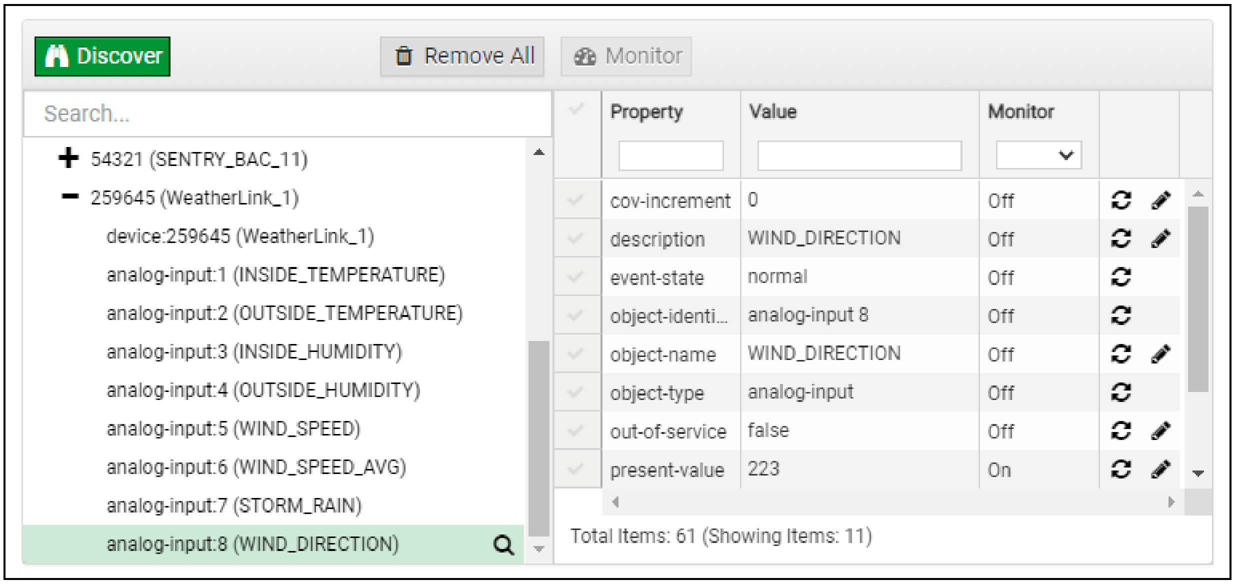


- 259645 (WeatherLink_1)
  - device:259645 (WeatherLink_1)
  - analog-input:1 (INSIDE_TEMPERATURE)
  - analog-input:2 (OUTSIDE_TEMPERATURE)
  - analog-input:3 (INSIDE_HUMIDITY)
  - analog-input:4 (OUTSIDE_HUMIDITY)
  - analog-input:5 (WIND_SPEED)
  - analog-input:6 (WIND_SPEED_AVG)
  - analog-input:7 (STORM_RAIN)
  - analog-input:8 (WIND_DIRECTION)

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.



- ✚ 54321 (SENTRY_BAC_11)
- ━ 259645 (WeatherLink_1)
  - device:259645 (WeatherLink_1)
  - analog-input:1 (INSIDE_TEMPERATURE)
  - analog-input:2 (OUTSIDE_TEMPERATURE)
  - analog-input:3 (INSIDE_HUMIDITY)
  - analog-input:4 (OUTSIDE_HUMIDITY)
  - analog-input:5 (WIND_SPEED)
  - analog-input:6 (WIND_SPEED_AVG)
  - analog-input:7 (STORM_RAIN)
  - analog-input:8 (WIND_DIRECTION)

Property	Value	Monitor
cov-increment	0	Off
description	WIND_DIRECTION	Off
event-state	normal	Off
object-identi...	analog-input 8	Off
object-name	WIND_DIRECTION	Off
object-type	analog-input	Off
out-of-service	false	Off
present-value	223	On

Total Items: 61 (Showing Items: 11)

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.

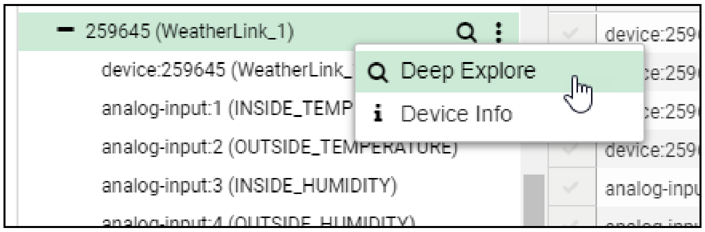
NOTE: The Gateway Search Bar will find devices based on their Device ID.

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

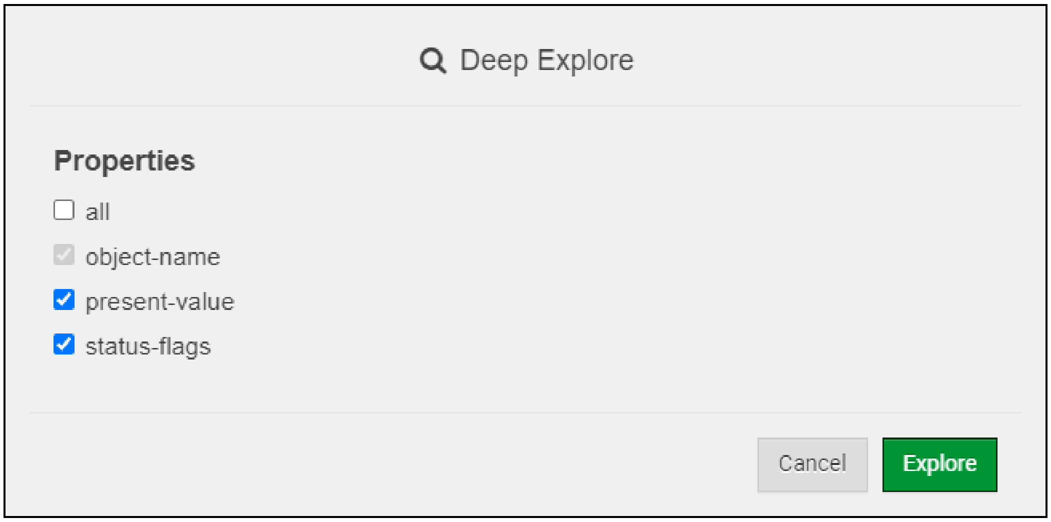
- Network number
  - Device
    - Device object

7.1.3 Explore All of a Device’s Points – Deep Explore

- To explore all device objects under a specific device with one search, click the desired device to highlight it.
- Then click the three white dots (⋮) that appear to the right of the highlighted device to open a dropdown menu.


259645 (WeatherLink_1)
device:259645 (WeatherLink_
analog-input:1 (INSIDE_TEMP
analog-input:2 (OUTSIDE_TEMPERATURE)
analog-input:3 (INSIDE_HUMIDITY)
analog-input:4 (OUTSIDE_HUMIDITY)
Deep Explore
Device Info
device:259
ce:259
ce:259
device:259
analog-inpu

- Click Deep Explore to open the Deep Explore window.



Properties

☐ all
☑ object-name
☑ present-value
☑ status-flags

- Select which property types to find in the search.

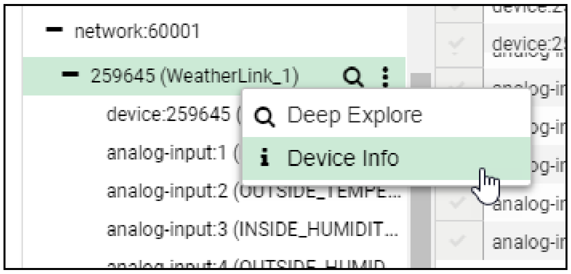
NOTE: The “all” selection must be unchecked to show object-name, present-value and status-flags as options.

NOTE: Object-name will always be checked in a Deep Explore search.

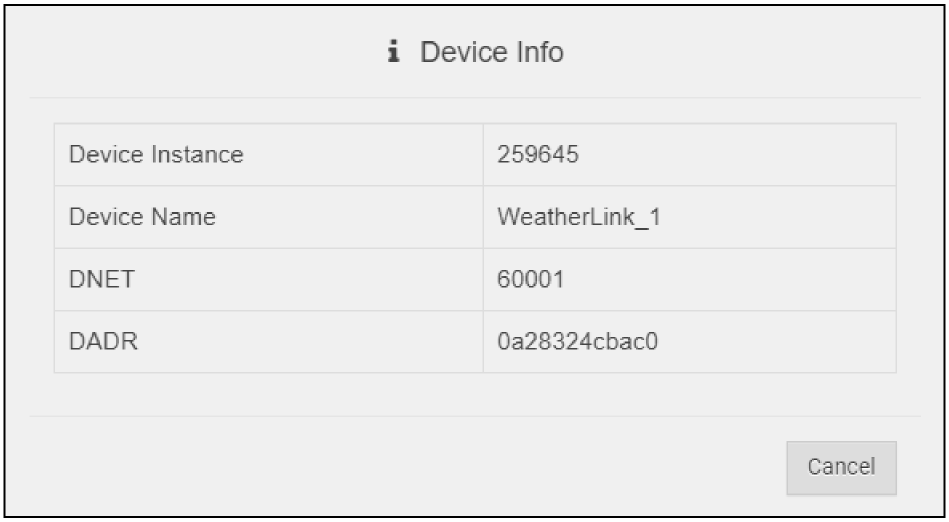
- Click the Explore button and wait for the green explore complete message to confirm all points have been discovered.

7.1.4 Checking Device Information – Device Info

- To check a device’s properties/information, click the desired device to highlight it.
- Then click the three black dots (⋮) that appear to the right of the highlighted device to open a dropdown menu.



- Click Device Info to open the Device Info window and get the device information needed.



Device Info

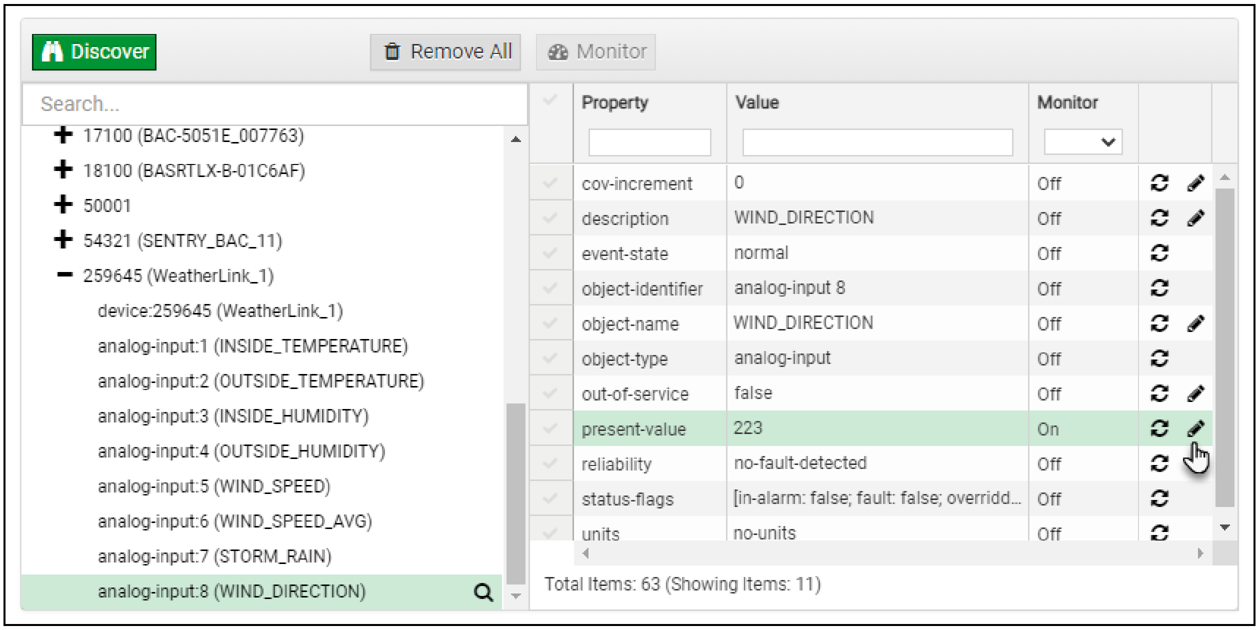
Device Instance	259645
Device Name	WeatherLink_1
DNET	60001
DADR	0a28324cbac0

7.1.5 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.

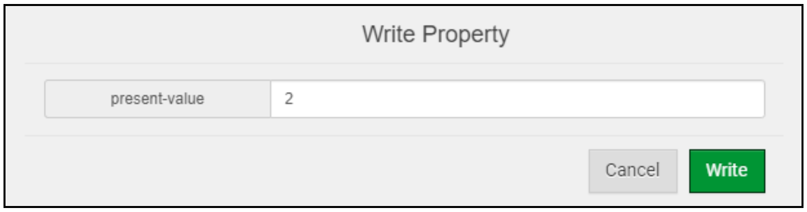


- 17100 (BAC-5051E_007763)
- 18100 (BASRTLX-B-01C6AF)
- 50001
- 54321 (SENTRY_BAC_11)
- 259645 (WeatherLink_1)
  - device:259645 (WeatherLink_1)
  - analog-input:1 (INSIDE_TEMPERATURE)
  - analog-input:2 (OUTSIDE_TEMPERATURE)
  - analog-input:3 (INSIDE_HUMIDITY)
  - analog-input:4 (OUTSIDE_HUMIDITY)
  - analog-input:5 (WIND_SPEED)
  - analog-input:6 (WIND_SPEED_AVG)
  - analog-input:7 (STORM_RAIN)
  - analog-input:8 (WIND_DIRECTION)

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; overridd...	Off
units	no-units	Off

Total Items: 63 (Showing Items: 11)

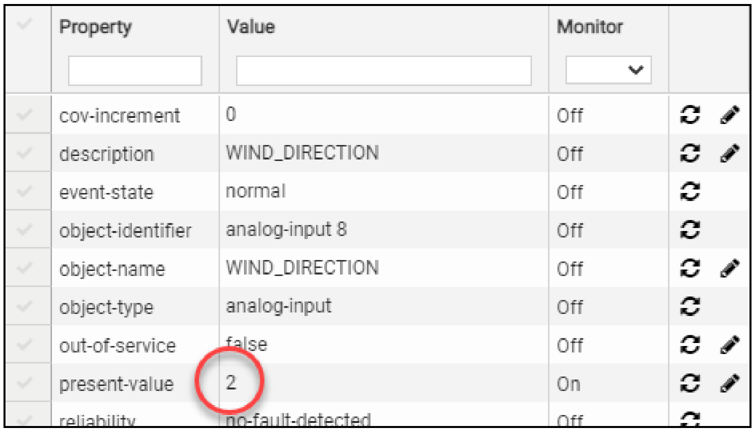
- Then click the Write button (✎) on the right of the property to bring up the Write Property window.



present-value: 2

- Enter the appropriate change and click the Write button.

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



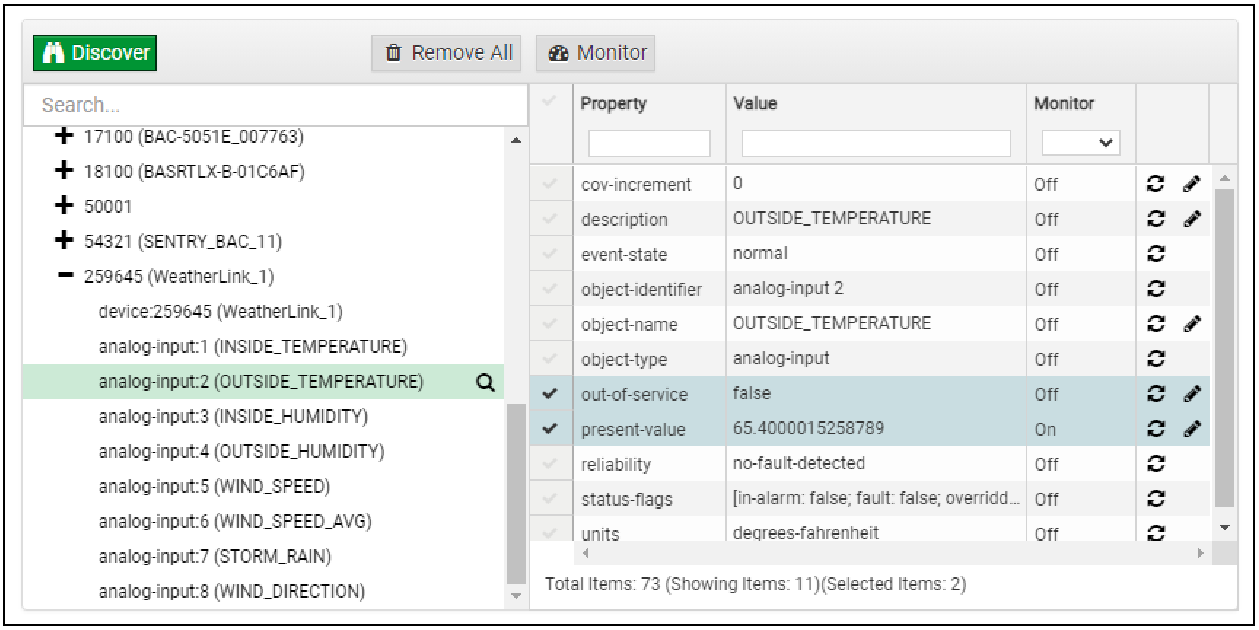
Property	Value	Monitor
cov-increment	0	Off
description	WIND_DIRECTION	Off
event-state	normal	Off
object-identifier	analog-input 8	Off
object-name	WIND_DIRECTION	Off
object-type	analog-input	Off
out-of-service	false	Off
present-value	2	On
reliability	no-fault-detected	Off

7.2 Monitor View

7.2.1 Set Devices to Track

Before using the Monitor View page, device properties must be selected to be monitored for analysis and testing in the BACnet Explorer page. To do so follow the instructions below:

- When viewing the expanded device properties on the BACnet Explorer page, click the checkbox to the left of any property to track.



- 17100 (BAC-5051E_007763)
- 18100 (BASRTLX-B-01C6AF)
- 50001
- 54321 (SENTRY_BAC_11)
- 259645 (WeatherLink_1)
  - device:259645 (WeatherLink_1)
  - analog-input:1 (INSIDE_TEMPERATURE)
  - analog-input:2 (OUTSIDE_TEMPERATURE)
  - analog-input:3 (INSIDE_HUMIDITY)
  - analog-input:4 (OUTSIDE_HUMIDITY)
  - analog-input:5 (WIND_SPEED)
  - analog-input:6 (WIND_SPEED_AVG)
  - analog-input:7 (STORM_RAIN)
  - analog-input:8 (WIND_DIRECTION)

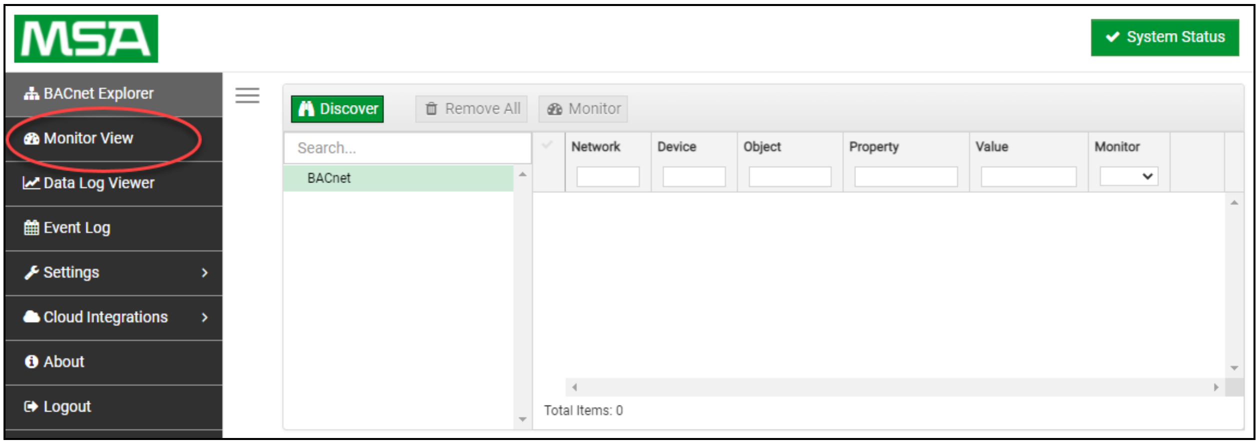
	Property	Value	Monitor
	cov-increment	0	Off
	description	OUTSIDE_TEMPERATURE	Off
	event-state	normal	Off
	object-identifier	analog-input 2	Off
	object-name	OUTSIDE_TEMPERATURE	Off
	object-type	analog-input	Off
✓	out-of-service	false	Off
✓	present-value	65.4000015258789	On
	reliability	no-fault-detected	Off
	status-flags	[in-alarm: false; fault: false; overridd...	Off
	units	degrees-fahrenheit	Off

Total Items: 73 (Showing Items: 11)(Selected Items: 2)

- Once all properties are selected for that data type, click the monitor button Monitor to set the selected properties to be monitored.
  - The Monitor column in the selected property row will change from “Off” to “On”

NOTE: A maximum of 1,000 data points can be monitored.

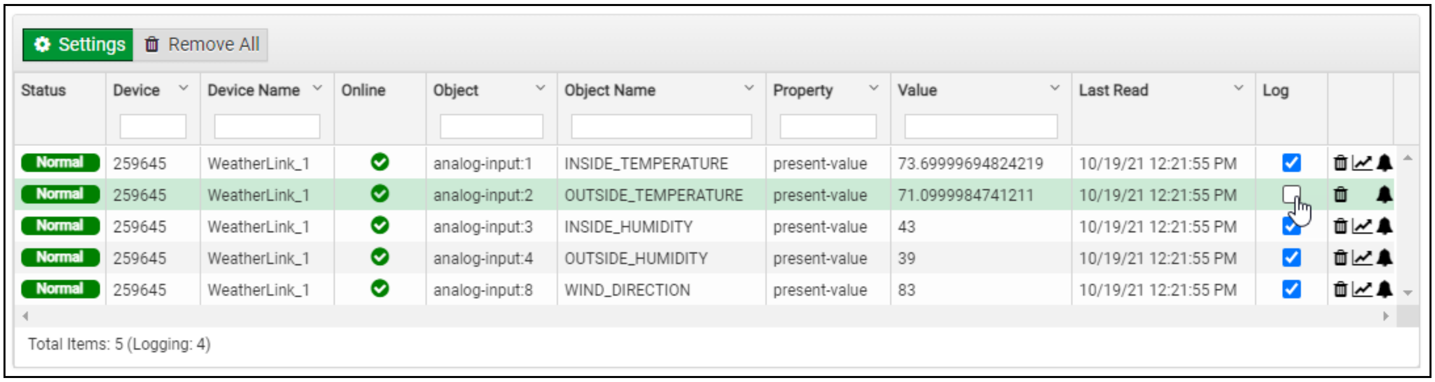
- Wait for the configuration to complete, then click on the Monitor View tab.



Total Items: 0

7.2.2 Logging Data

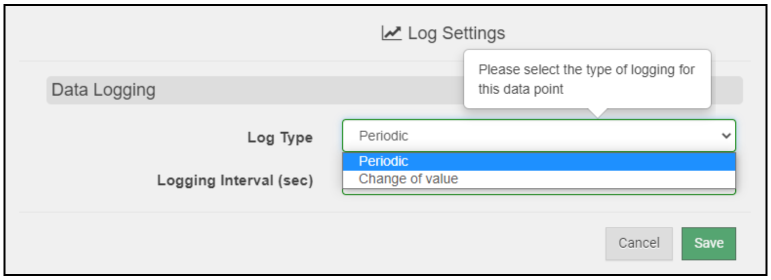
- For the Data Log Viewer, Event Log and the FieldServer Manager, click the checkbox under the Log column to add data points.



Status	Device	Device Name	Online	Object	Object Name	Property	Value	Last Read	Log
Normal	259645	WeatherLink_1	✓	analog-input:1	INSIDE_TEMPERATURE	present-value	73.69999694824219	10/19/21 12:21:55 PM	☑
Normal	259645	WeatherLink_1	✓	analog-input:2	OUTSIDE_TEMPERATURE	present-value	71.0999984741211	10/19/21 12:21:55 PM	☐
Normal	259645	WeatherLink_1	✓	analog-input:3	INSIDE_HUMIDITY	present-value	43	10/19/21 12:21:55 PM	☑
Normal	259645	WeatherLink_1	✓	analog-input:4	OUTSIDE_HUMIDITY	present-value	39	10/19/21 12:21:55 PM	☑
Normal	259645	WeatherLink_1	✓	analog-input:8	WIND_DIRECTION	present-value	83	10/19/21 12:21:55 PM	☑

Total Items: 5 (Logging: 4)

- Click on the graph icon (📈) to the right of the data elements to open the Data Logging window.



Log Settings

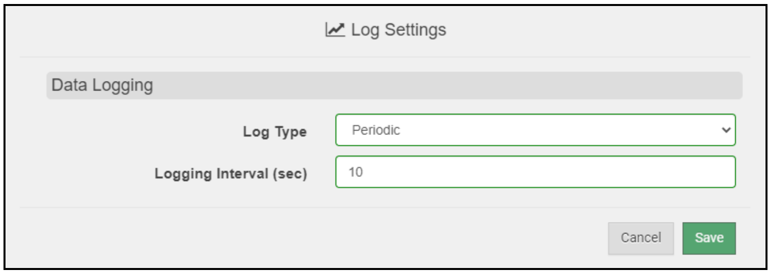
Data Logging

Please select the type of logging for this data point

Log Type: Periodic

Logging Interval (sec)

- Select the type of logging for the data point and set the logging interval, COV threshold value or COV max scan time as they apply then click the Save button to save the settings.

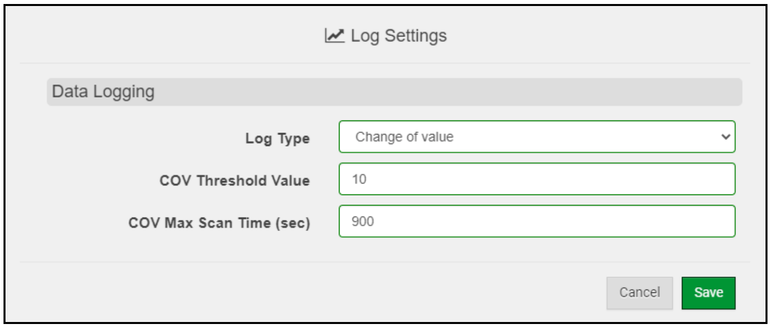


Log Settings

Data Logging

Log Type: Periodic

Logging Interval (sec): 10



Log Settings

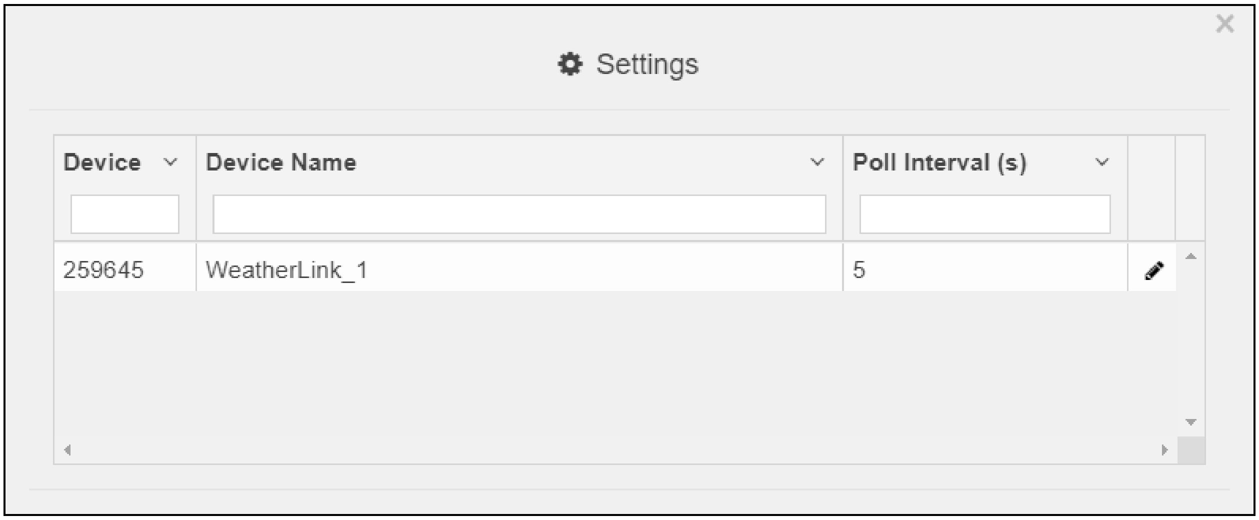
Data Logging

Log Type: Change of value

COV Threshold Value: 10

COV Max Scan Time (sec): 900

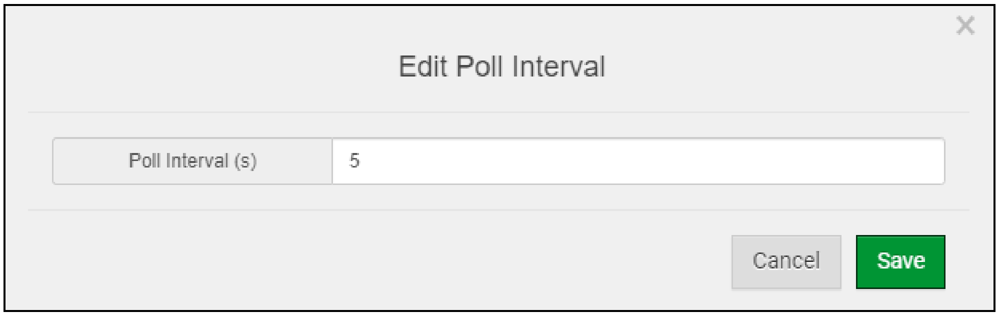
- To change the poll interval of a device, click the Settings button above the data elements to monitor to open the Settings window.



Settings

Device	Device Name	Poll Interval (s)
259645	WeatherLink_1	5

- Click the Edit icon to open the Edit Poll Interval window.



Edit Poll Interval

Poll Interval (s): 5

- Make desired changes and click Save.

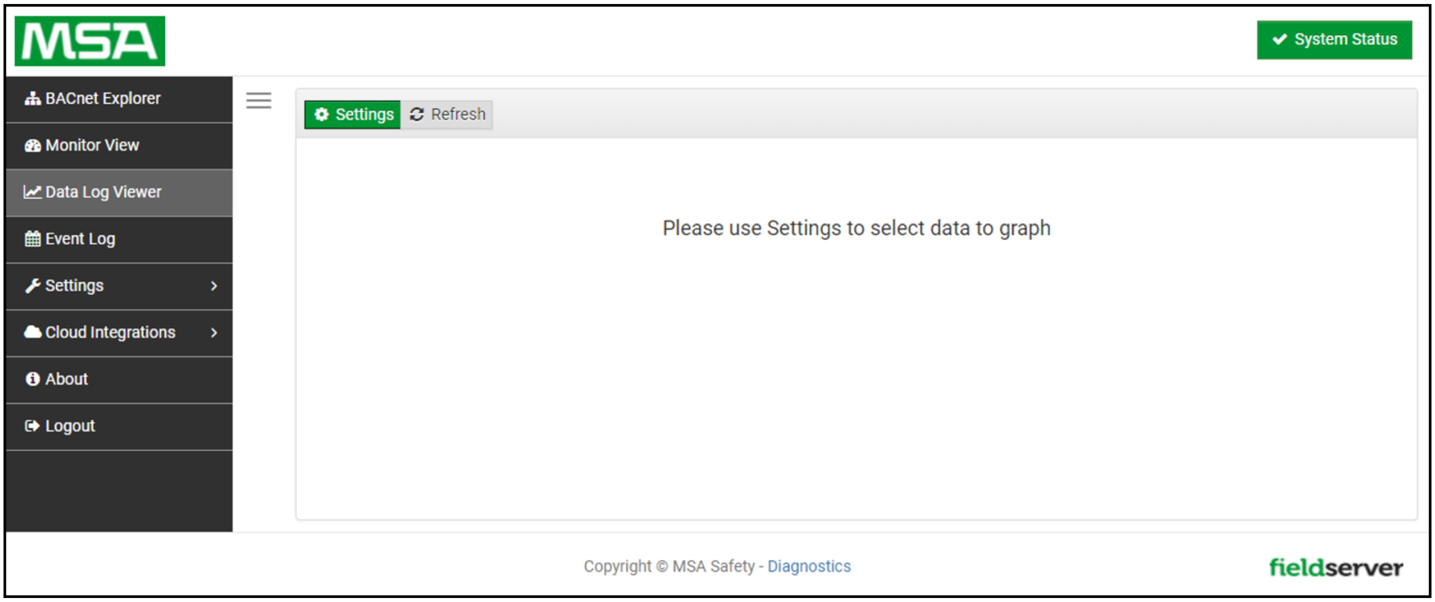
NOTE: Up to 30 days of data can be recorded and stored.

NOTE: Click the Trash icon (🗑) to the right of any logged property to remove it from Monitor View.

7.3 Data Log Viewer

NOTE: The Data Log Viewer can store up to 1,000 data points.

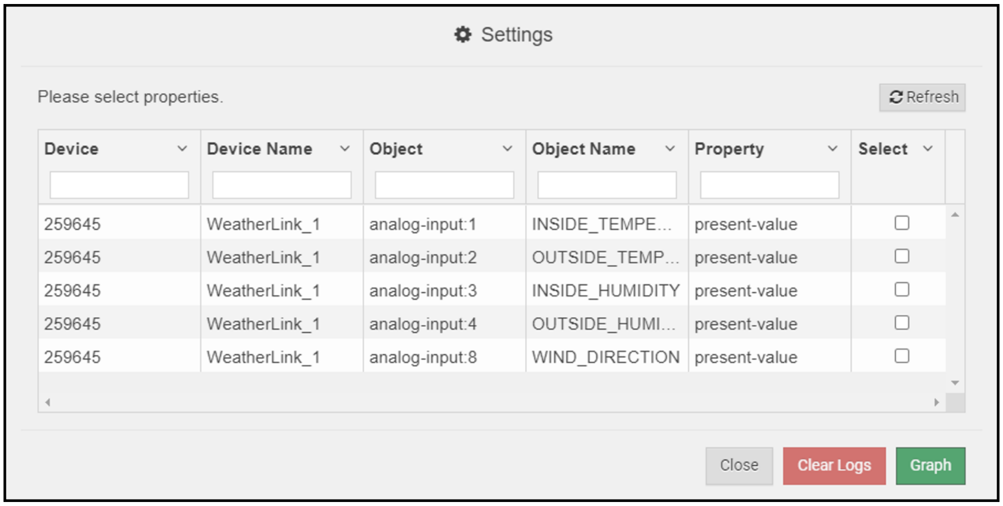
- Click the Data Log Viewer tab on the left side of the page.



Please use Settings to select data to graph

7.3.1 Graph Data Logging Information

- Click on the Settings button (⚙ Settings) to set up data to graph.



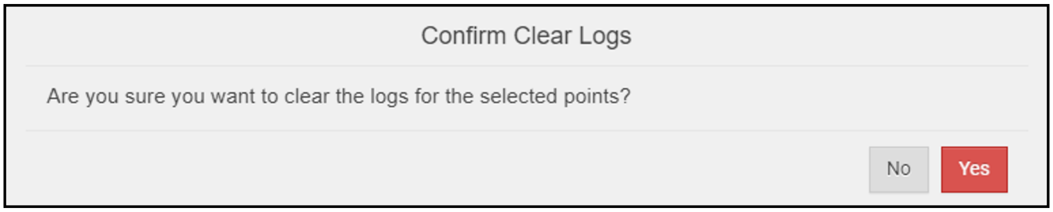
Please select properties.

Device	Device Name	Object	Object Name	Property	Select
259645	WeatherLink_1	analog-input:1	INSIDE_TEMPE...	present-value	☐
259645	WeatherLink_1	analog-input:2	OUTSIDE_TEMP...	present-value	☐
259645	WeatherLink_1	analog-input:3	INSIDE_HUMIDITY	present-value	☐
259645	WeatherLink_1	analog-input:4	OUTSIDE_HUMI...	present-value	☐
259645	WeatherLink_1	analog-input:8	WIND_DIRECTION	present-value	☐

- Click the checkbox next to the data element to graph.
  - Any combination of elements can be selected

NOTE: A data element is only visible when it is set for data logging as shown in Section 7.2 Monitor View.

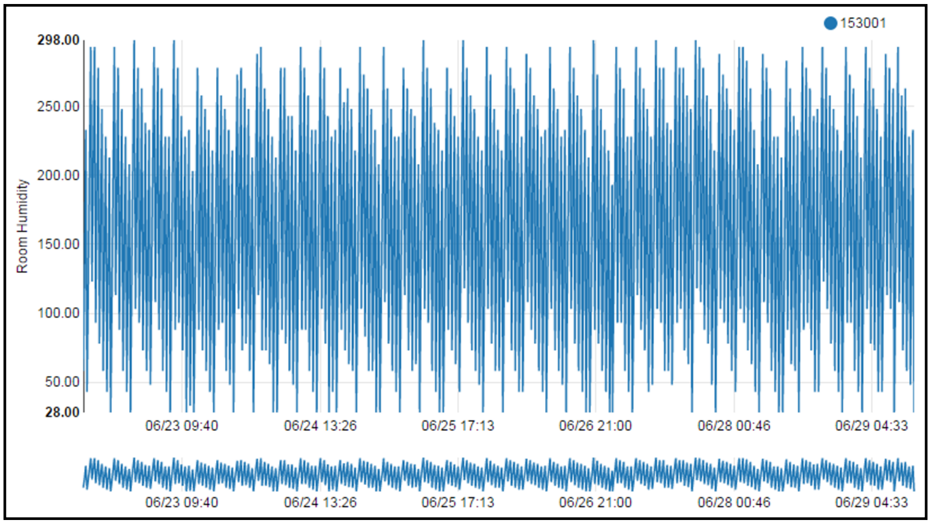
- Click Submit to generate a graph for each element selected.
  - To delete a log, check the boxes next to the properties to delete and click the Clear Logs button; then click "Yes" to confirm



Confirm Clear Logs

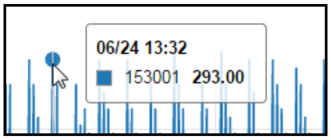
Are you sure you want to clear the logs for the selected points?

  - After a few seconds, the graph should appear

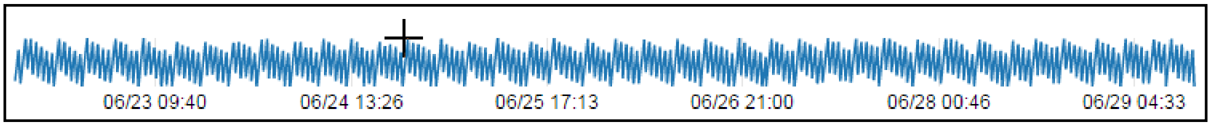


- See below for instructions on controlling graphs:

To view individual values of data, scroll across the graph to show a text box that states each exact point and the location of that point on the graph via a blue dot.

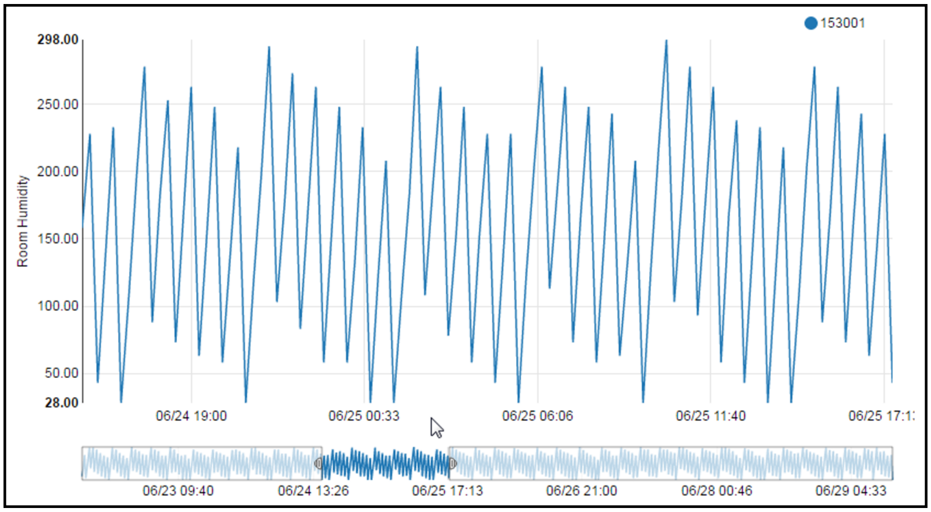


To view a graph of only select dates/time frames, move the cursor towards the miniature version of the graph that is shown just below the full size graph. Hover the cursor over the miniature graph so that the cursor becomes a crosshair (+).

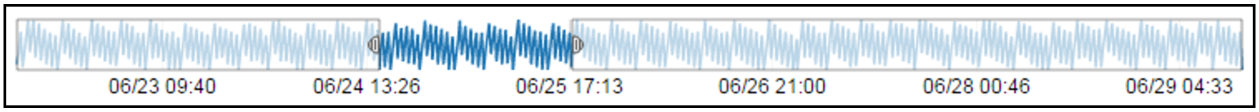


Click and hold near the beginning or ending time frame desired, then drag the crosshair towards the ending or beginning time frame; all within the confines of the miniature graph.

The full size version of the graph will populate accordingly.



Any additional edits to the time frame can be adjusted by clicking and dragging the wedge markers on either side of the highlighted portion of the miniature graph.

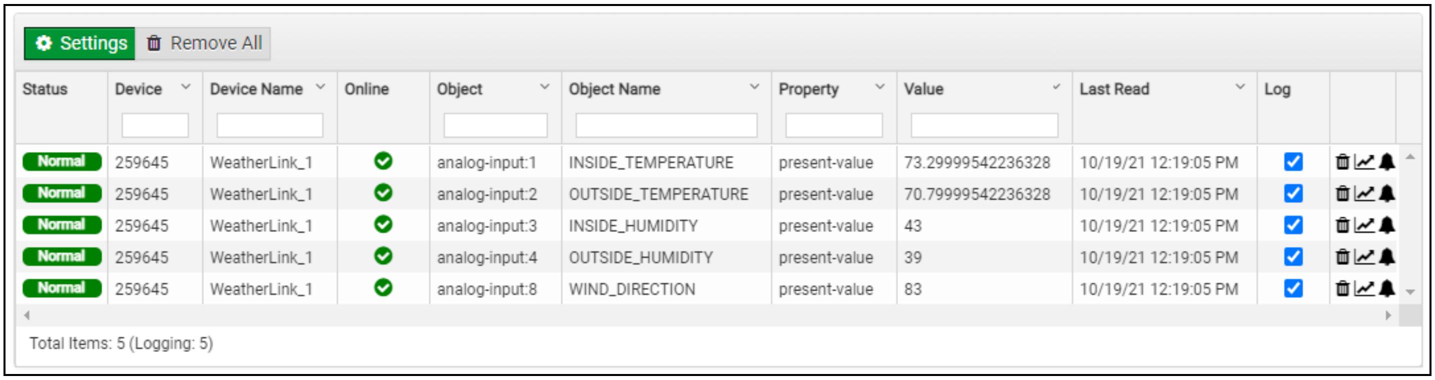


To go back to the full graph, click on any faded portion of the miniature graph.

NOTE: The data selected in the Data Log Viewer is also available via the RESTful API, contact FieldServer Technical Support for a copy of the RESTful API Start-up Guide.

7.3.2 Creating an Event Log

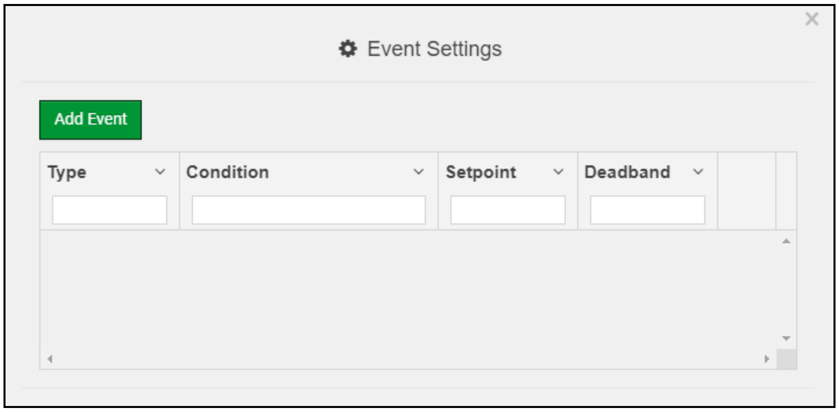
- To create an event log for a property, click on the Monitor View tab to go to the Monitor View page.



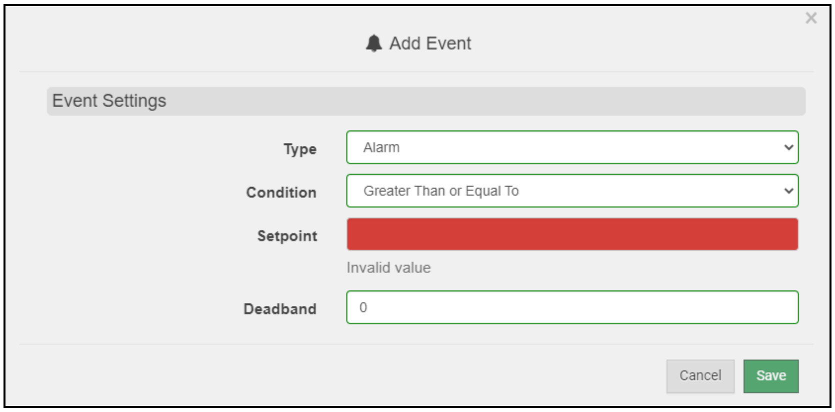
Status	Device	Device Name	Online	Object	Object Name	Property	Value	Last Read	Log	
Normal	259645	WeatherLink_1	✓	analog-input:1	INSIDE_TEMPERATURE	present-value	73.29999542236328	10/19/21 12:19:05 PM	☑	🗑 📈 🔔
Normal	259645	WeatherLink_1	✓	analog-input:2	OUTSIDE_TEMPERATURE	present-value	70.79999542236328	10/19/21 12:19:05 PM	☑	🗑 📈 🔔
Normal	259645	WeatherLink_1	✓	analog-input:3	INSIDE_HUMIDITY	present-value	43	10/19/21 12:19:05 PM	☑	🗑 📈 🔔
Normal	259645	WeatherLink_1	✓	analog-input:4	OUTSIDE_HUMIDITY	present-value	39	10/19/21 12:19:05 PM	☑	🗑 📈 🔔
Normal	259645	WeatherLink_1	✓	analog-input:8	WIND_DIRECTION	present-value	83	10/19/21 12:19:05 PM	☑	🗑 📈 🔔

Total Items: 5 (Logging: 5)

- Click the bell icon (🔔) to the right of the property to log and the Event Settings window will open.



- Click on the Add Event button to change the event settings.



Event Settings

Type: Alarm

Condition: Greater Than or Equal To

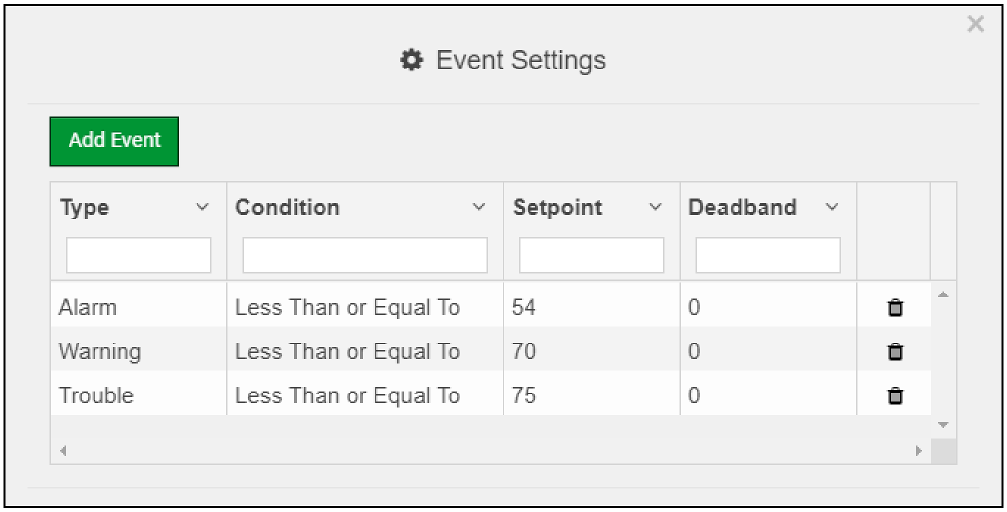
Setpoint:

Invalid value

Deadband: 0

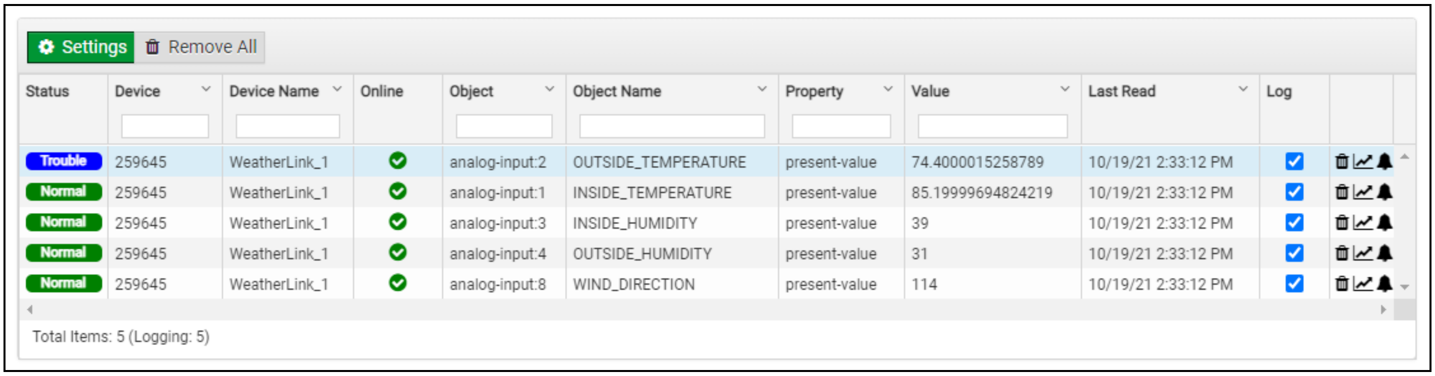
- Set the event as needed and click Save.
- Repeat this process to create more events as needed.

NOTE: Click the Trash icon (🗑) to the right of any event to remove it.



Type	Condition	Setpoint	Deadband	
Alarm	Less Than or Equal To	54	0	🗑
Warning	Less Than or Equal To	70	0	🗑
Trouble	Less Than or Equal To	75	0	🗑

- Click the “x” in the top right corner of the Event Settings window to close it.
  - The Monitor View page will now update the status column as events take place

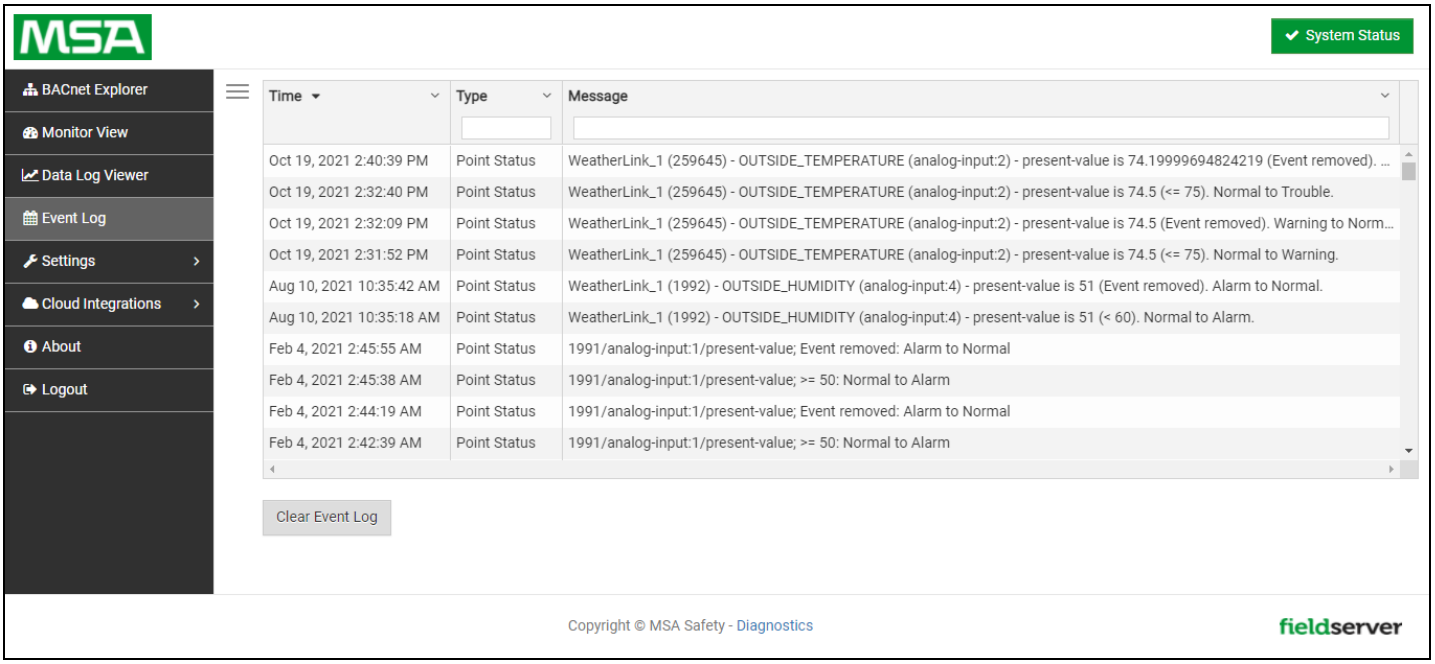


Status	Device	Device Name	Online	Object	Object Name	Property	Value	Last Read	Log	
Trouble	259645	WeatherLink_1	✓	analog-input:2	OUTSIDE_TEMPERATURE	present-value	74.4000015258789	10/19/21 2:33:12 PM	☑	🗑 📈 🔔
Normal	259645	WeatherLink_1	✓	analog-input:1	INSIDE_TEMPERATURE	present-value	85.19999694824219	10/19/21 2:33:12 PM	☑	🗑 📈 🔔
Normal	259645	WeatherLink_1	✓	analog-input:3	INSIDE_HUMIDITY	present-value	39	10/19/21 2:33:12 PM	☑	🗑 📈 🔔
Normal	259645	WeatherLink_1	✓	analog-input:4	OUTSIDE_HUMIDITY	present-value	31	10/19/21 2:33:12 PM	☑	🗑 📈 🔔
Normal	259645	WeatherLink_1	✓	analog-input:8	WIND_DIRECTION	present-value	114	10/19/21 2:33:12 PM	☑	🗑 📈 🔔

Total Items: 5 (Logging: 5)

7.4 Event Log

Click the Event Log tab on the left side of the page to open the Event Logger and view the events that have been set to track in **Section 7.3.2 Creating an Event Log** (by time and type with a descriptive message).



Time	Type	Message
Oct 19, 2021 2:40:39 PM	Point Status	WeatherLink_1 (259645) - OUTSIDE_TEMPERATURE (analog-input:2) - present-value is 74.19999694824219 (Event removed). ...
Oct 19, 2021 2:32:40 PM	Point Status	WeatherLink_1 (259645) - OUTSIDE_TEMPERATURE (analog-input:2) - present-value is 74.5 (<= 75). Normal to Trouble.
Oct 19, 2021 2:32:09 PM	Point Status	WeatherLink_1 (259645) - OUTSIDE_TEMPERATURE (analog-input:2) - present-value is 74.5 (Event removed). Warning to Norm...
Oct 19, 2021 2:31:52 PM	Point Status	WeatherLink_1 (259645) - OUTSIDE_TEMPERATURE (analog-input:2) - present-value is 74.5 (<= 75). Normal to Warning.
Aug 10, 2021 10:35:42 AM	Point Status	WeatherLink_1 (1992) - OUTSIDE_HUMIDITY (analog-input:4) - present-value is 51 (Event removed). Alarm to Normal.
Aug 10, 2021 10:35:18 AM	Point Status	WeatherLink_1 (1992) - OUTSIDE_HUMIDITY (analog-input:4) - present-value is 51 (< 60). Normal to Alarm.
Feb 4, 2021 2:45:55 AM	Point Status	1991/analog-input:1/present-value; Event removed: Alarm to Normal
Feb 4, 2021 2:45:38 AM	Point Status	1991/analog-input:1/present-value; >= 50: Normal to Alarm
Feb 4, 2021 2:44:19 AM	Point Status	1991/analog-input:1/present-value; Event removed: Alarm to Normal
Feb 4, 2021 2:42:39 AM	Point Status	1991/analog-input:1/present-value; >= 50: Normal to Alarm

Copyright © MSA Safety - Diagnostics

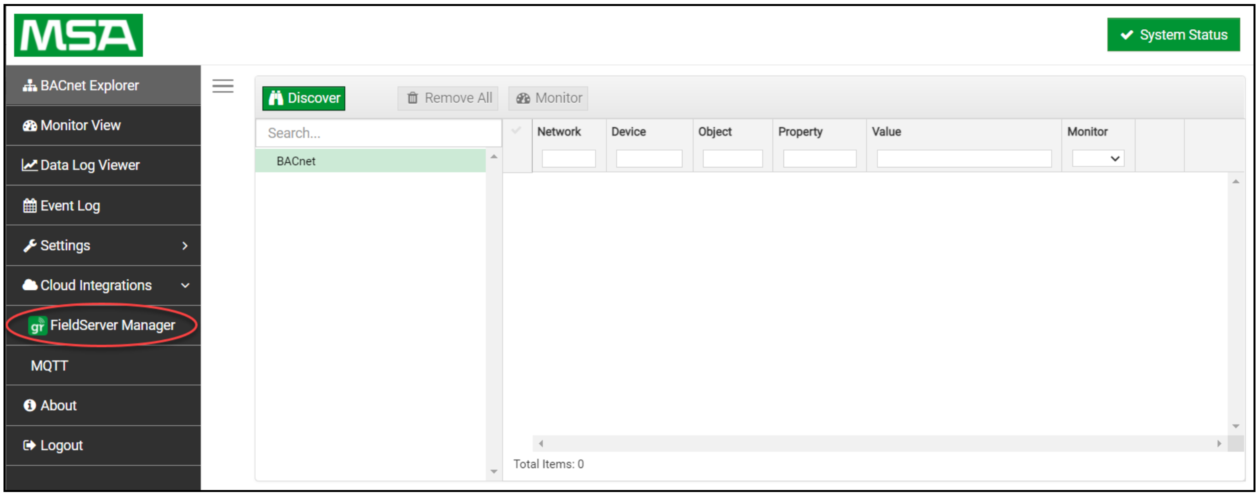
8 MSA Grid - FieldSever Manager Setup

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.

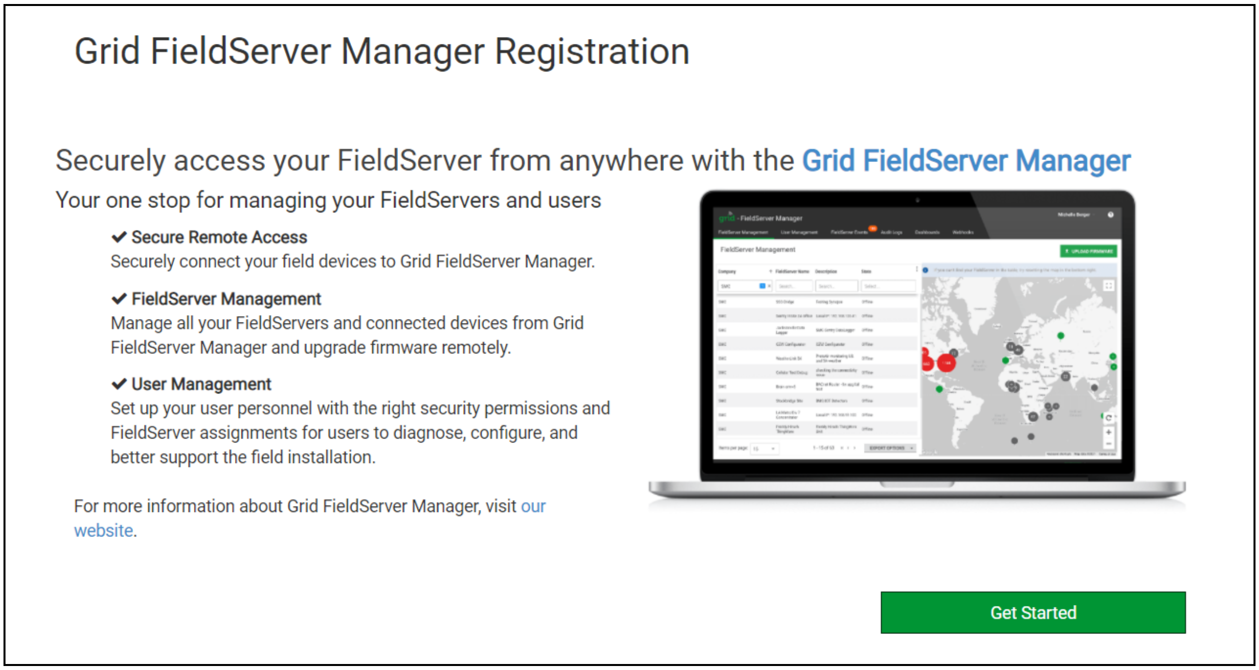
8.1 Create a New FieldServer Manager Account

The first step to connecting to the FieldServer Manager is to create an account.

- Click on the Cloud Integrations tab, then click the FieldServer Manager tab.



NOTE: If a warning message appears instead, go to Section 12.6 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.

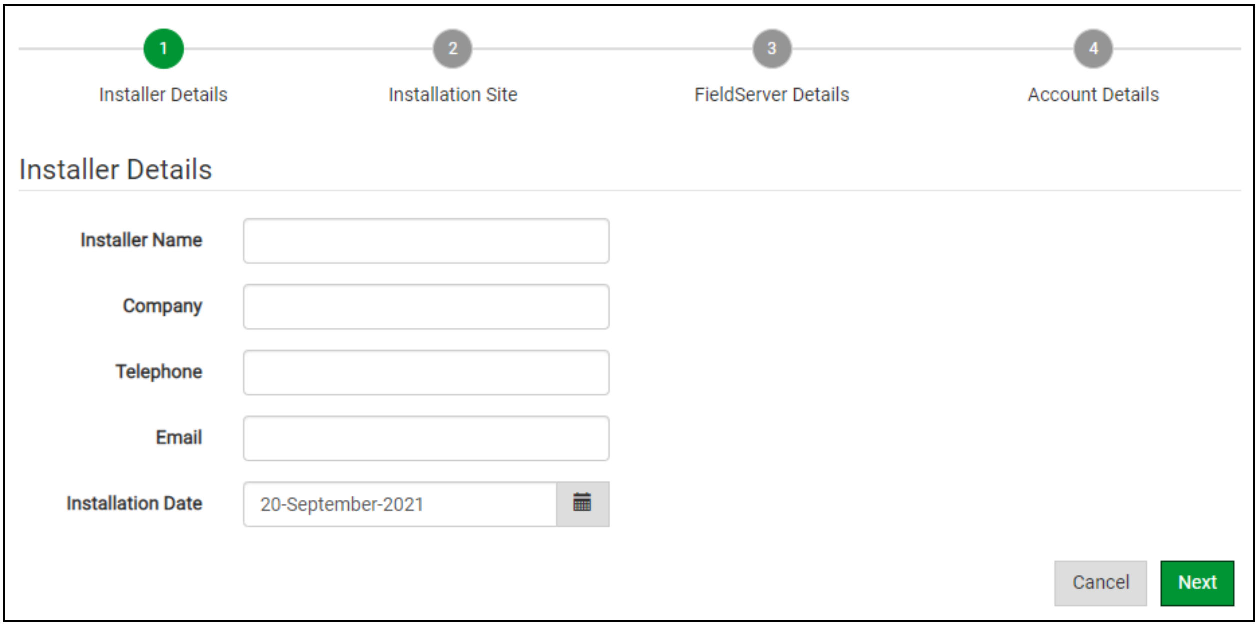
✓ User Management
Set up your user personnel with the right security permissions and FieldServer assignments for users to diagnose, configure, and better support the field installation.

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

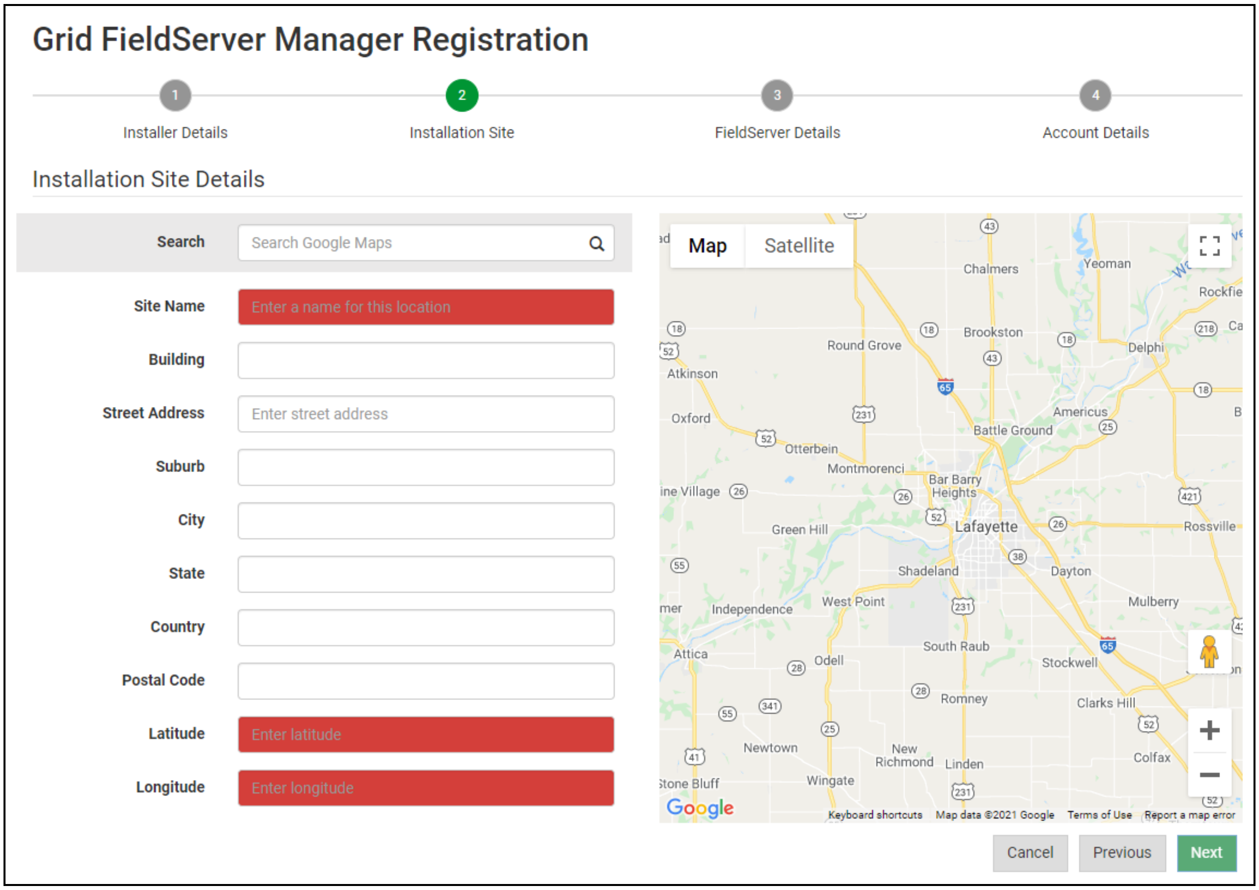


1 Installer Details — 2 Installation Site — 3 FieldServer Details — 4 Account Details

Installer Details

Installer Name	
Company	
Telephone	
Email	
Installation Date	20-September-2021

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



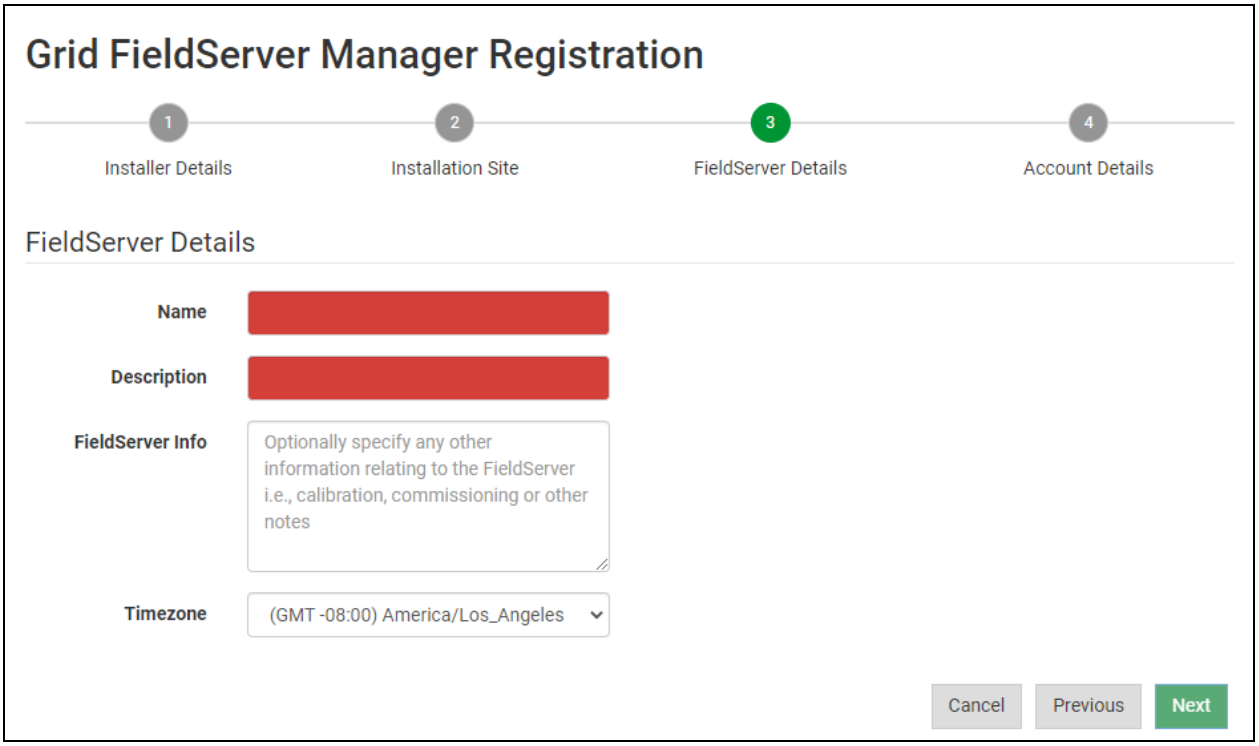
Grid FieldServer Manager Registration

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

Installation Site Details

Search	Search Google Maps
Site Name	Enter a name for this location
Building	
Street Address	Enter street address
Suburb	
City	
State	
Country	
Postal Code	
Latitude	Enter latitude
Longitude	Enter longitude

- Enter Name and Description (required) then click Next



Grid FieldServer Manager Registration

FieldServer Details

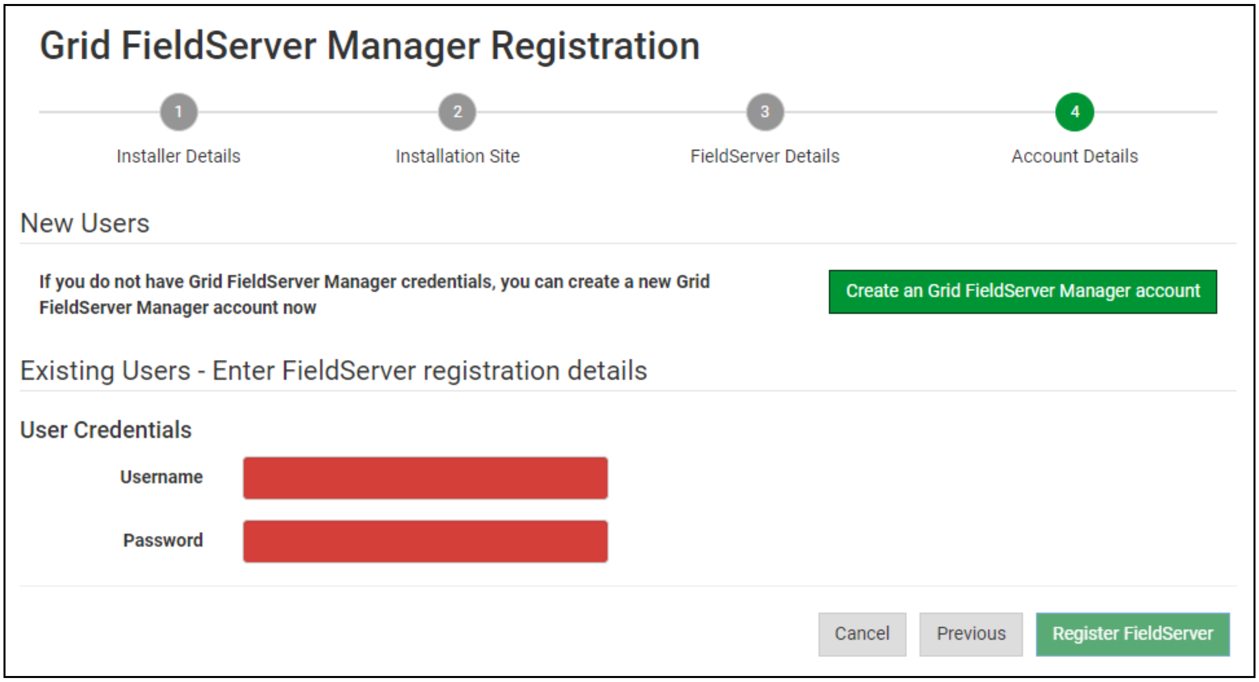
Name

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

- 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

New Users

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

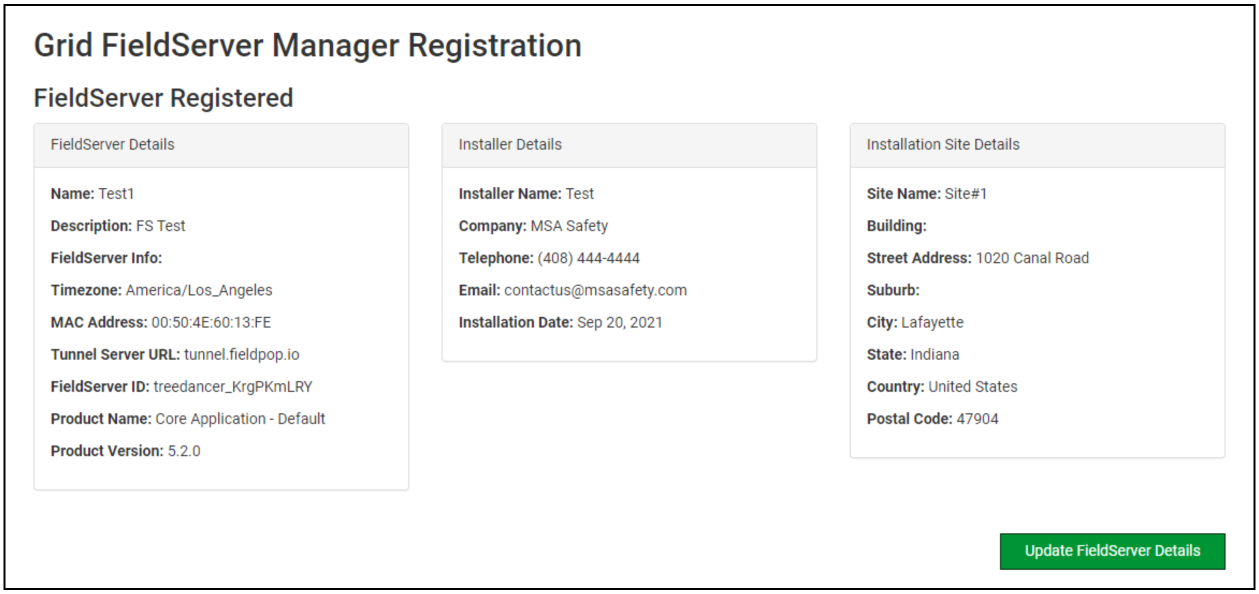
Existing Users - Enter FieldServer registration details

User Credentials

Username

Password

- 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 BACnet IoT 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

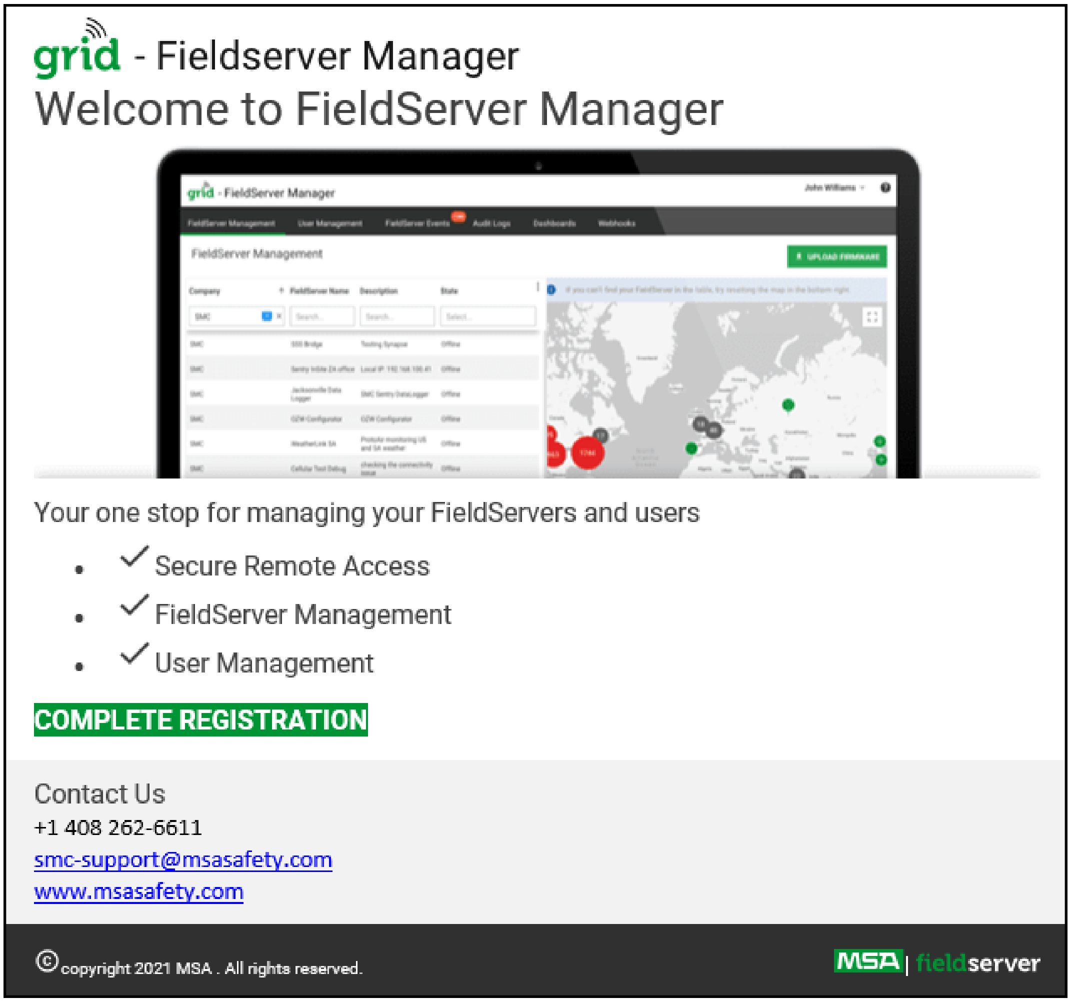
Country: United States

Postal Code: 47904

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

8.2 User Setup

- Open the registered email account.
- The “Welcome to the MSA Grid - FieldServer Manager” email will appear as shown below.



grid - Fieldserver Manager

Welcome to FieldServer Manager

Your one stop for managing your FieldServers and users

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

COMPLETE REGISTRATION

Contact Us

+1 408 262-6611

smc-support@msasafety.com

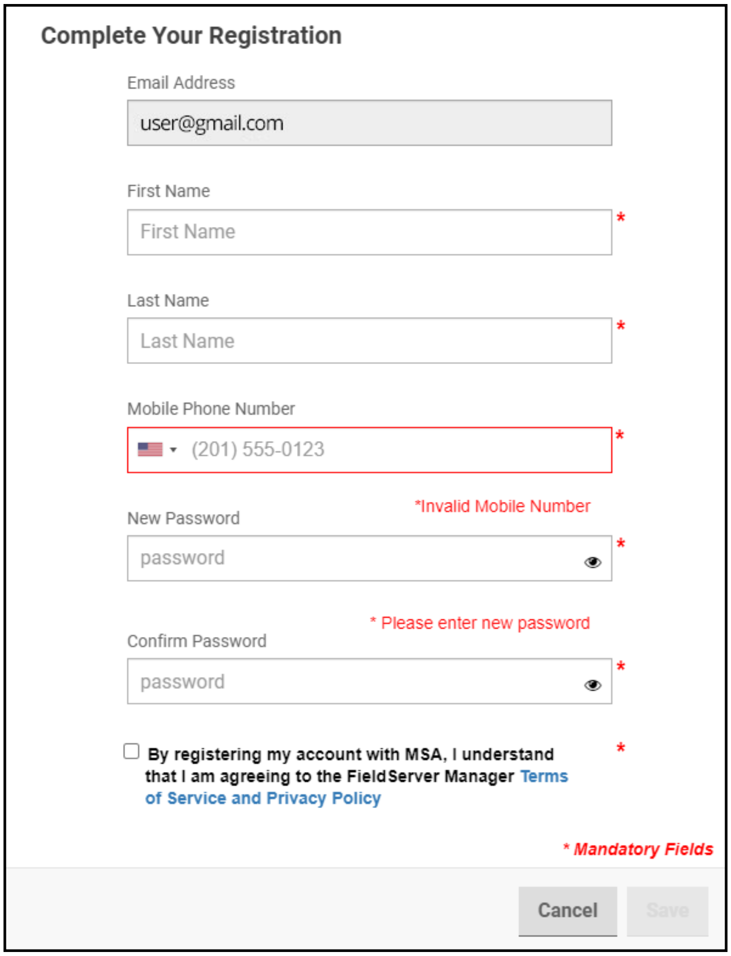
www.msasafety.com

©copyright 2021 MSA . All rights reserved.

MSA | fieldserver

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

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



Complete Your Registration

Email Address: user@gmail.com

First Name: First Name *

Last Name: Last Name *

Mobile Phone Number: (201) 555-0123 *

*Invalid Mobile Number

New Password: password *

* Please enter new password

Confirm Password: password *

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

* Mandatory Fields

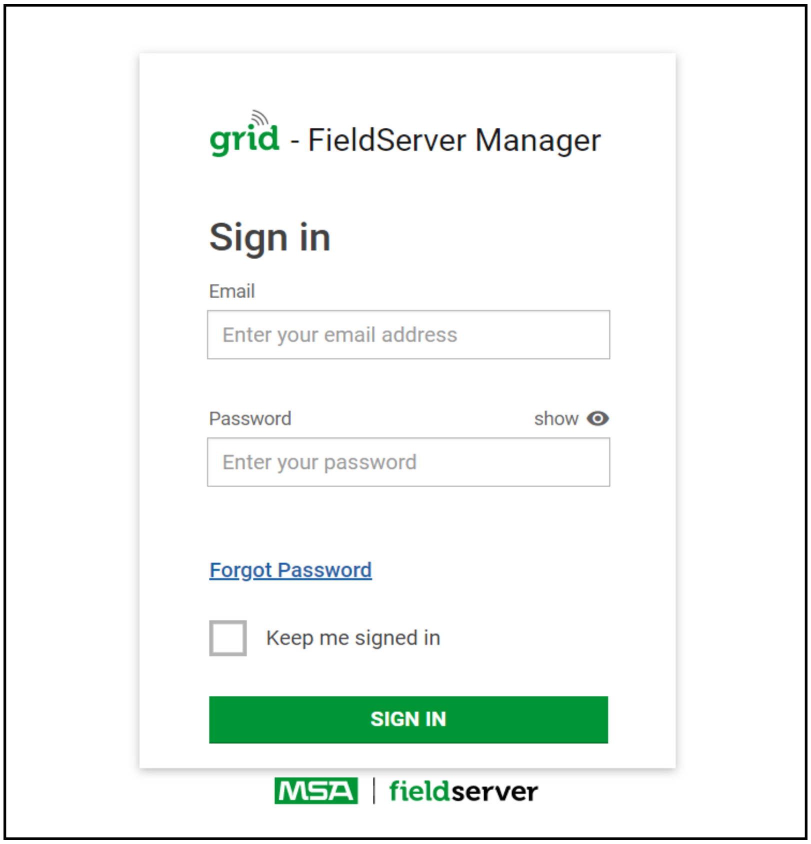
- Fill in the name, phone number, password fields and click the checkbox to agree to the privacy policy and terms of service.

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

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

8.3 Login to the FieldServer Manager

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



grid - FieldServer Manager

Sign in

Email

Enter your email address

Password show

Enter your password

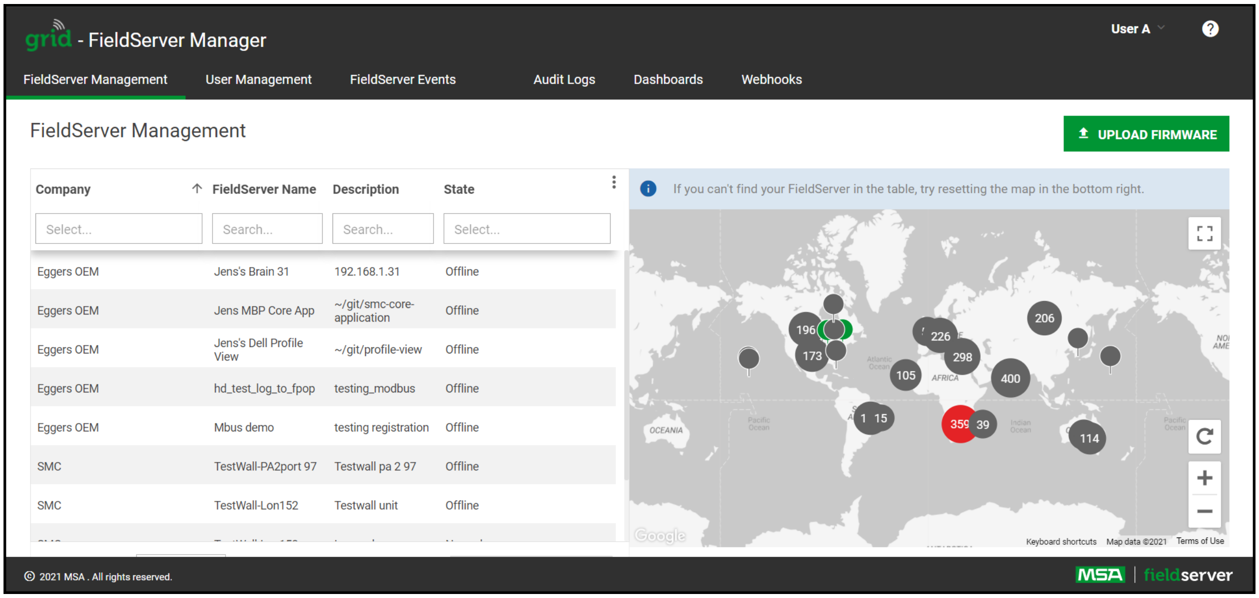
Forgot Password

□ Keep me signed in

SIGN IN

MSA | fieldserver

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



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

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

9 MQTT Integration

9.1 MQTT Published Messages

The BACnet IoT Gateway uses a single connection to the Broker URL. Communication via MQTT is “topic” based, meaning each data point is defined via an arbitrarily long and unique “topic” string which is usually in the following format: [(unique gateway identifier)/(unique node identifier)/(unique data point identifier)].

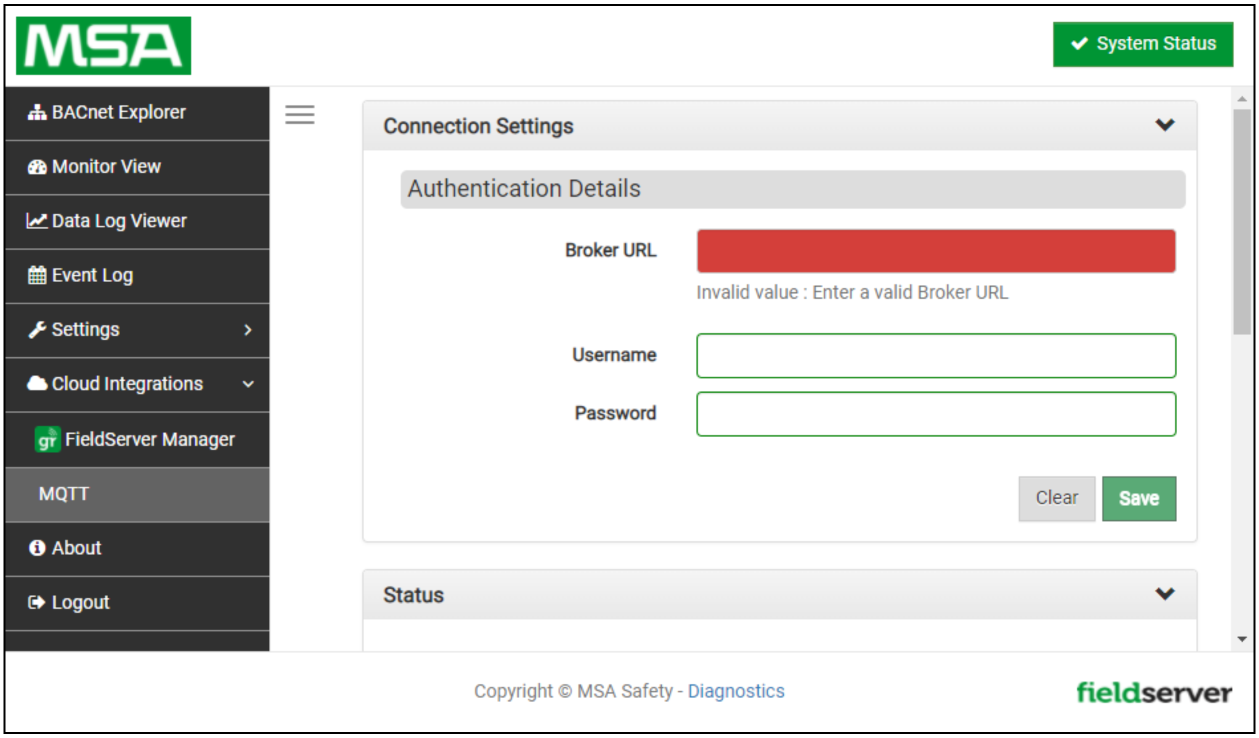
These topics are published via the logging method that was set up for the data points in Monitor View. Refer to **Section 7.2 Monitor View** and **Section 7.3 Data Log Viewer** for logging instructions.

The payload for each topic is in JSON format, containing the properties ‘value’ and ‘timestamp’.

NOTE: For message structure information see the MQTT Message Structure ENOTE on the MSA Safety website.

9.2 Connect to MQTT

- After setup and initial configuration of the BACnet IoT Gateway is complete, click the Cloud Integrations tab.
- Then click the MQTT tab.

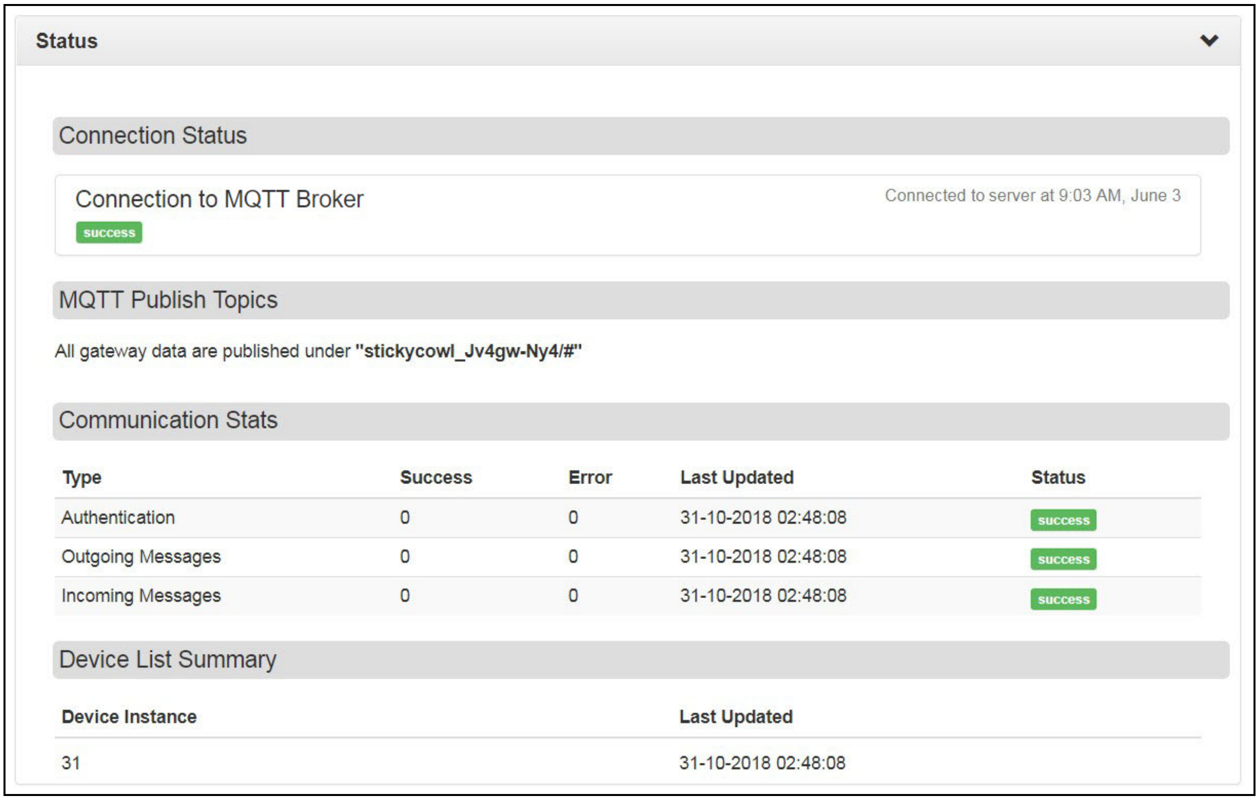


Invalid value : Enter a valid Broker URL

- Enter Authentication Details gathered from the MQTT Platform into the Connection Settings Window.
- Click Save to record the information and allow MQTT integration to your account.

9.3 Check the Status Window

- Scroll down from the Settings Window until the Status Window is visible.



Status

Connection Status

Connection to MQTT Broker

success

Connected to server at 9:03 AM, June 3

MQTT Publish Topics

All gateway data are published under **"stickycowl_Jv4gw-Ny4/#"**

Communication Stats

Type	Success	Error	Last Updated	Status
Authentication	0	0	31-10-2018 02:48:08	success
Outgoing Messages	0	0	31-10-2018 02:48:08	success
Incoming Messages	0	0	31-10-2018 02:48:08	success

Device List Summary

Device Instance	Last Updated
31	31-10-2018 02:48:08

- The Connection Status Section shows the state of connection to the MQTT Broker with the date and time of connection listed.
- The Communication Stats Section lists the communication statistics of the connected devices.
- The Device List Summary lists the device instances and the last time they were updated.

9.4 Specifications

	FS-IOT-BAC, FS-IOT-BACW & FS-IOT-BACA/V/F
Electrical Connections	One 3-pin Phoenix connector with: RS-485/RS-232 (Tx+ / Rx- / gnd) One 3-pin Phoenix connector with: Power port (+ / - / Frame-gnd) One Ethernet 10/100 BaseT port **BAC & BACW include an additional:** RS-485 port (TX+ / RX- / gnd) **BAC2 includes an additional:** One Ethernet 10/100 BaseT port
BAC/BACW/BAC2 Power Requirements	*Input Voltage:* 12-24VDC or 24VAC *Current draw:* 24VAC 0.125A *Max Power:* 3 Watts 12-24VDC 0.25A @12VDC
BACA/V/F Power Requirements	*Input Voltage:* 12-24VDC *Current draw:* @ 12V, 0.67A *Max Power:* 8 Watts
Approvals	FCC Part 15, UL 60950-1 and CAN/CSA C22.2 No. 60950-1 (**BACW**), EN IEC 62368-1:2020+A11:2020, WEEE compliant, RoHS compliant, DNP 3.0 and Modbus conformance tested, PTCRB compliant (**BACA/V/F**), BTL marked, REACH compliant, UKCA and CE compliant, CAN ICES-003(B) / NMB-003(B) (**BACW/A/V/2**)
Physical Dimensions	4 x 1.1 x 2.7 in (10.16 x 2.8 x 6.8 cm)
Weight	0.4 lbs (0.2 Kg)
Operating Temperature	-20°C to 70°C (-4°F to158°F)
Humidity	10-95% RH non-condensing
FS-IOT-BACW/A/V/F Wi-Fi 802.11 b/g/n	*Frequency:* 2.4 GHz *Channels:* 1 to 11 (inclusive) *Antenna:* Omnidirectional SMA *Encryption:* TKIP, WPA2 & AES
FS-IOT-BACA/V/F Cellular	*Features:* LTE Cat 4 *Antenna:* Omnidirectional 4G/LTE SMA *Uplink:* Up to 50 Mbps *Downlink:* Up to 150 Mbps

NOTE: Specifications subject to change without notice.

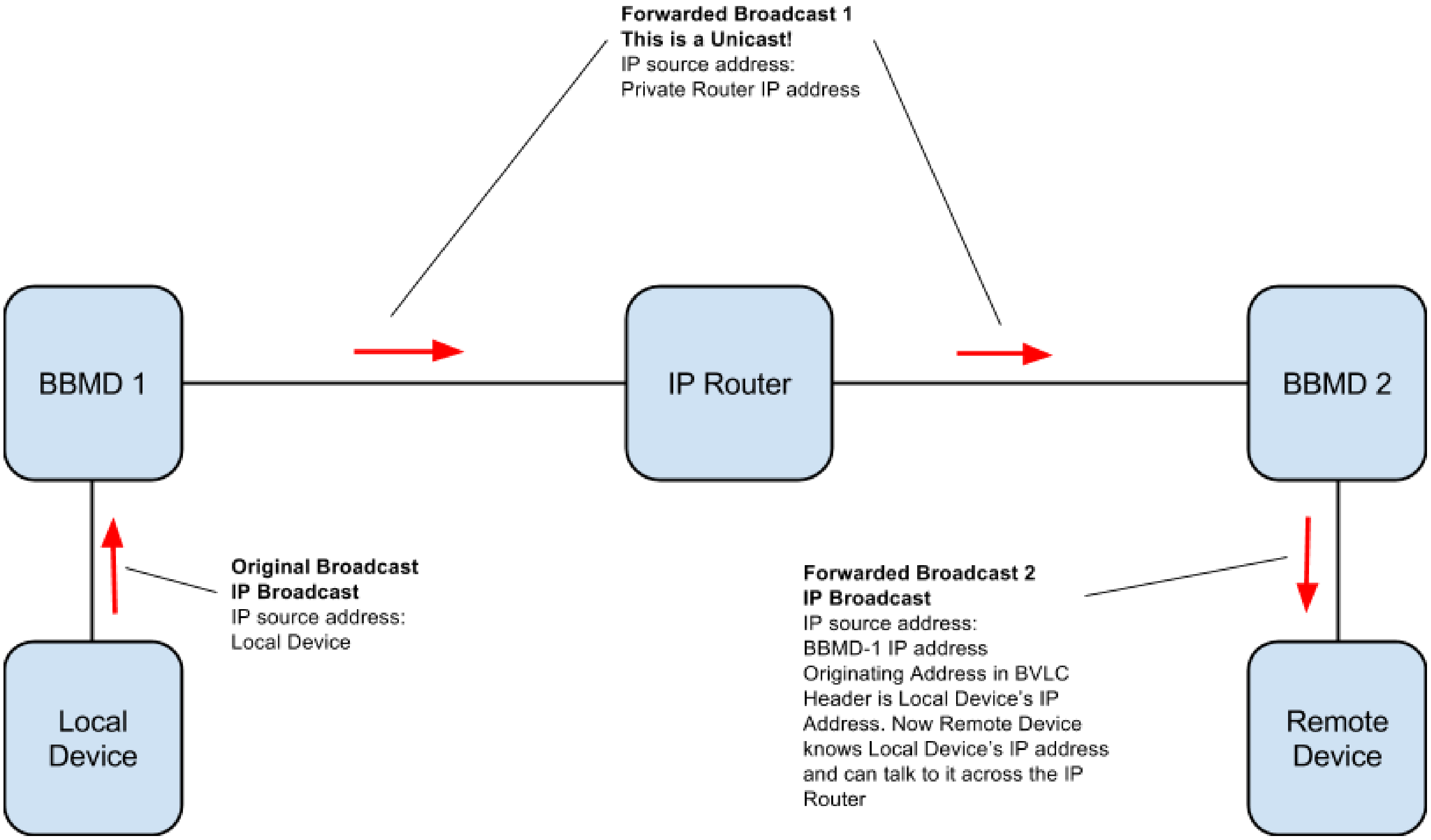
10 References

10.1 Understanding FDR

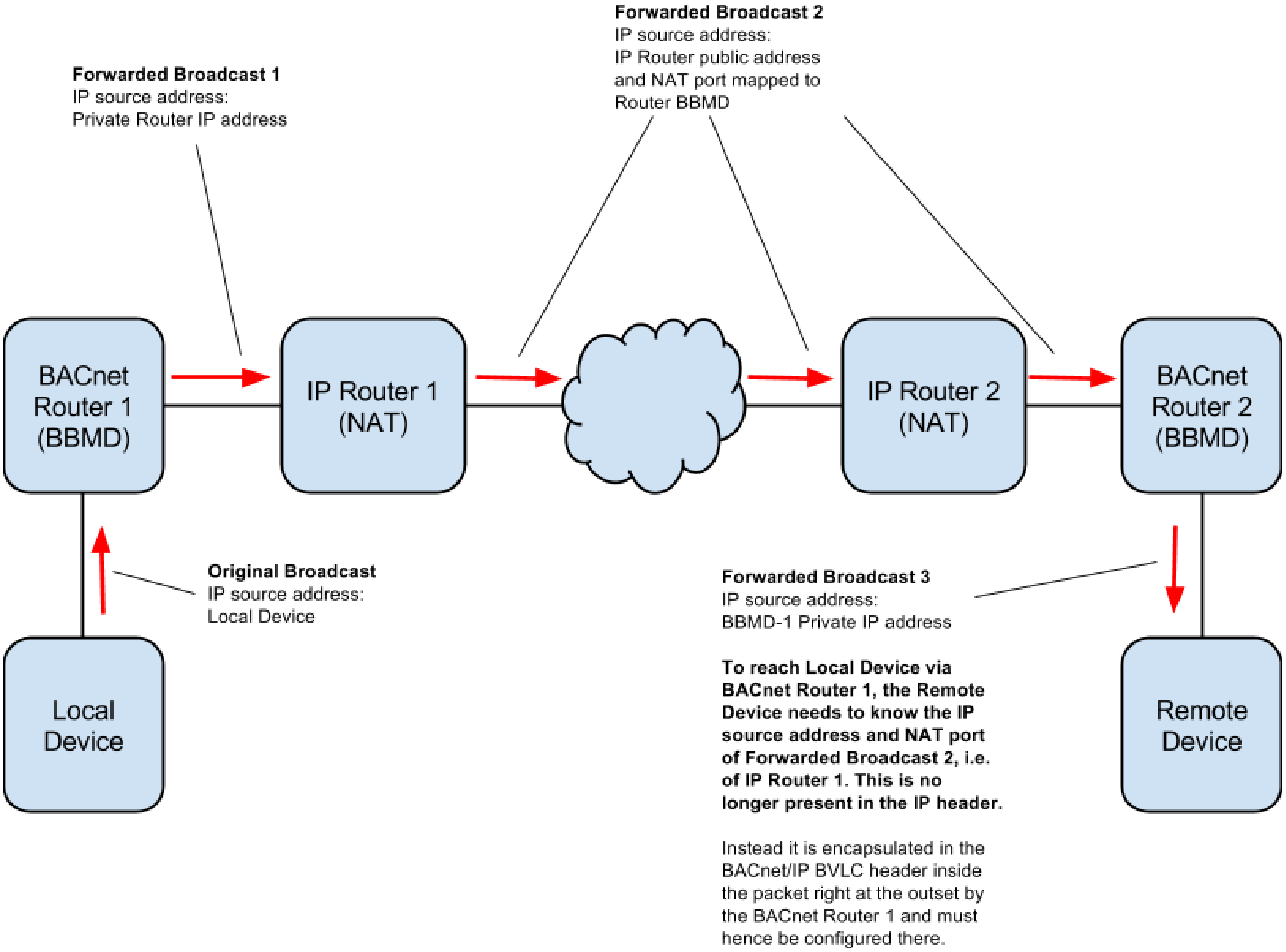
The BACnet IoT Gateway doesn't allow FDR, local IP and BACnet MS/TP to co-exist because there is no guarantee that two distinct BACnet networks will have unique Device Instances or Network Numbers. (Unique Device Instances and Network Numbers are a requirement for BACnet to function properly). If local and remote options were allowed concurrently, the BACnet IoT Gateway would connect two networks that are probably not designed to work together. Forcing this situation would create extremely difficult to diagnose problems.

10.2 Understanding BACnet BBMD and NAT Routing

The BACnet IoT Gateway does not support NAT routing. However, the BACnet IoT Gateway must have the external IP Address and IP Port that the NAT router assigns to it, because these are inserted into the BACnet/IP BVLC header as the source IP Address which a remote recipient can use to reach the BBMD (BACnet Broadcast Management Device). This is necessary because the messages are distributed again by a remote BBMD, and the remote recipient of a distributed broadcast needs to reach the originator of the broadcast.



With NAT Routing, BBMD alone does not work because the Devices cannot reach each other's IP Addresses even if they know them. The only reachable address is the BBMD itself, so this must also act as a BACnet IoT Gateway to forward traffic to the intended device. When this is done, the destination device's IP Address and Port are encoded as the DADR in the network header, so that the Router can forward messages to the correct device.



Forwarded Broadcast 1
IP source address:
Private Router IP address

Forwarded Broadcast 2
IP source address:
IP Router public address
and NAT port mapped to
Router BBMD

Original Broadcast
IP source address:
Local Device

Forwarded Broadcast 3
IP source address:
BBMD-1 Private IP address

To reach Local Device via BACnet Router 1, the Remote Device needs to know the IP source address and NAT port of Forwarded Broadcast 2, i.e. of IP Router 1. This is no longer present in the IP header.

Instead it is encapsulated in the BACnet/IP BVLC header inside the packet right at the outset by the BACnet Router 1 and must hence be configured there.

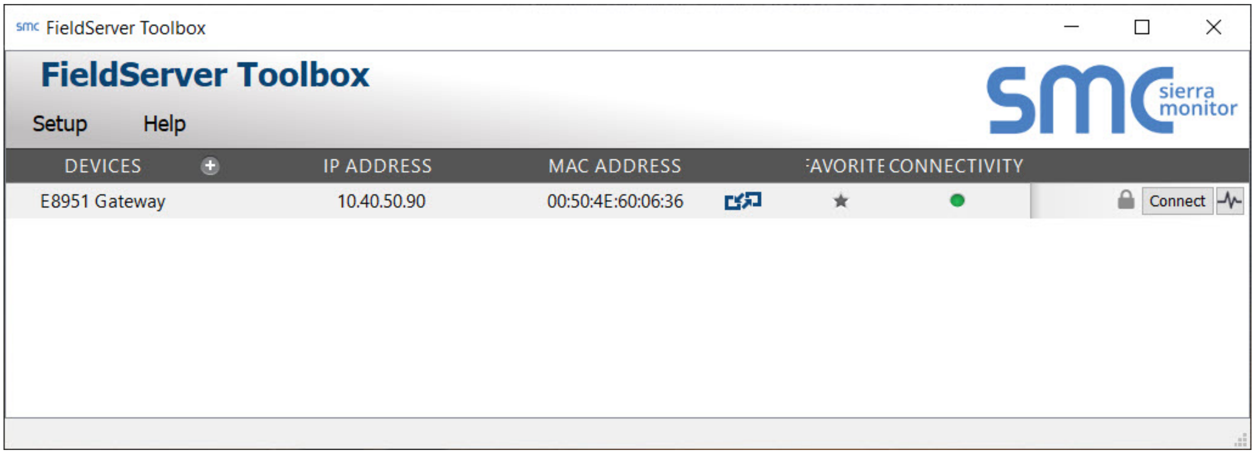
11 Troubleshooting

11.1 Communicating with the BACnet IoT 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 BACnet IoT Gateway. The Default IP Address of the BACnet IoT 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 BACnet IoT Gateway are on the same IP Network, or assign a Static IP Address to the PC on the 192.168.2.X network.

11.2 Lost or Incorrect IP Address

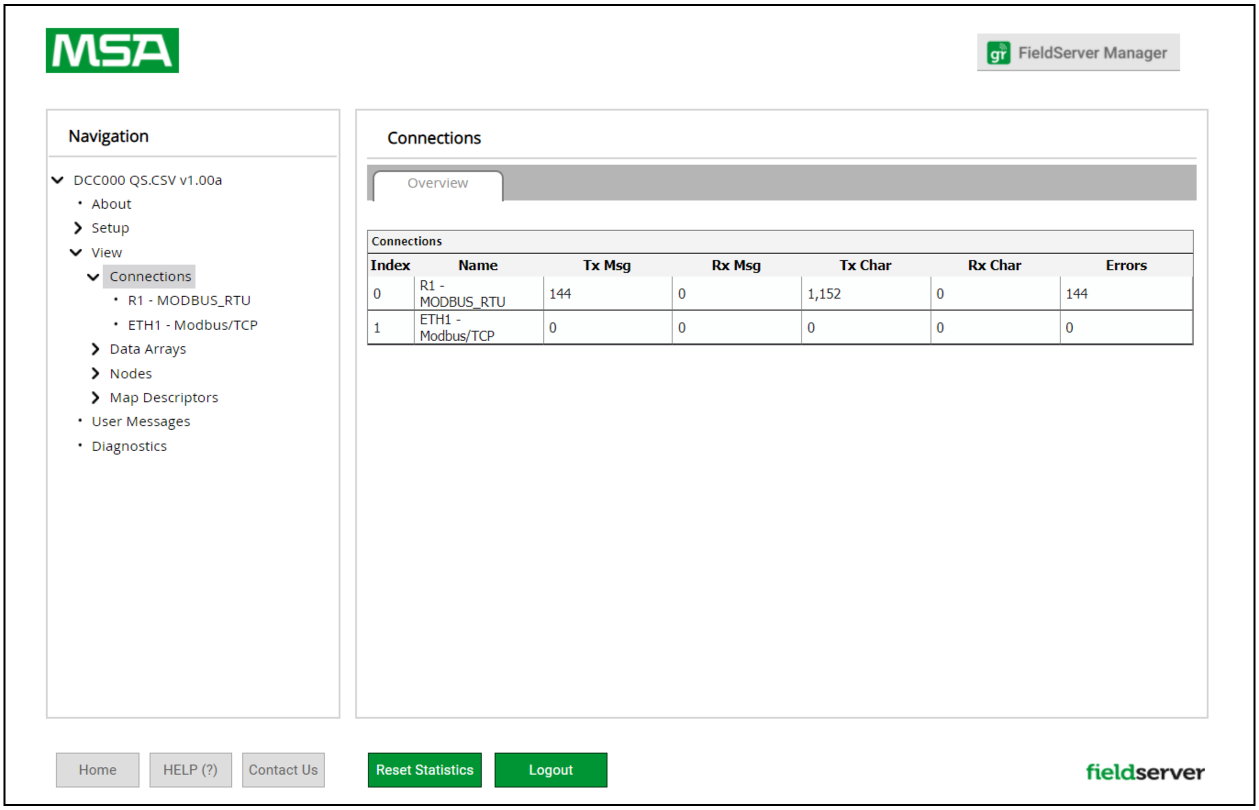
- Ensure that FieldServer Toolbox is loaded onto the local PC. Otherwise, download the FieldServer-Toolbox.zip via the MSA Safety website.
- Extract the executable file and complete the installation.
- Connect a standard Cat-5 Ethernet cable between the user’s PC and BACnet IoT Gateway.
- Double click on the FS Toolbox Utility and click Discover Now on the splash page.
- Check for the IP Address of the desired gateway.



DEVICES	IP ADDRESS	MAC ADDRESS	AVORITE	CONNECTIVITY
E8951 Gateway	10.40.50.90	00:50:4E:60:06:36	★	●

11.3 Viewing Diagnostic Information

- Type the IP Address of the FieldServer into the web browser or use the FieldServer Toolbox to connect to the FieldServer.
- Click on Diagnostics and Debugging Button, then click on view, and then on connections.
- If there are any errors showing on the Connection page, refer to **Section 11.4 Checking Wiring and Settings** for the relevant wiring and settings.



Connections

Connections

Index	Name	Tx Msg	Rx Msg	Tx Char	Rx Char	Errors
0	R1 - MODBUS_RTU	144	0	1,152	0	144
1	ETH1 - Modbus/TCP	0	0	0	0	0

11.4 Checking Wiring and Settings

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

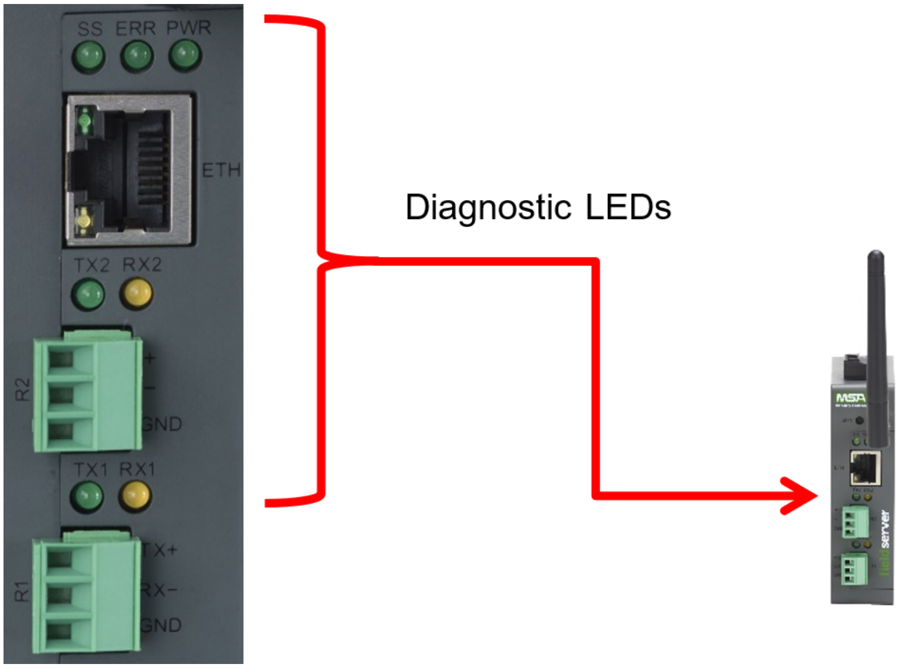
- Visual observations of LEDs on the BACnet IoT Gateway. (**Section 11.5 LED Functions**)
- Check baud rate, parity, data bits, stop bits.
- Check device address.
- Verify wiring.
- Verify the device is connected to the same subnet as the BACnet IoT Gateway.

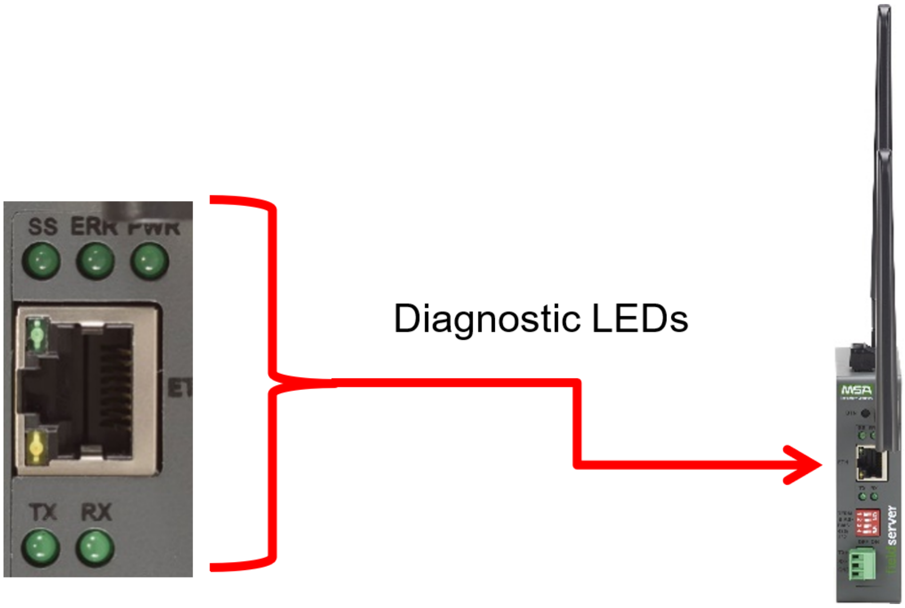
Field COM problems:

- Visual observations of LEDs on the BACnet IoT Gateway. (**Section 11.5 LED Functions**)
- Verify wiring.
- Verify IP Address setting.

NOTE: If the problem still exists, a Diagnostic Capture needs to be taken and sent to support. (Section 11.6 Taking a FieldServer Diagnostic Capture)

11.5 LED Functions



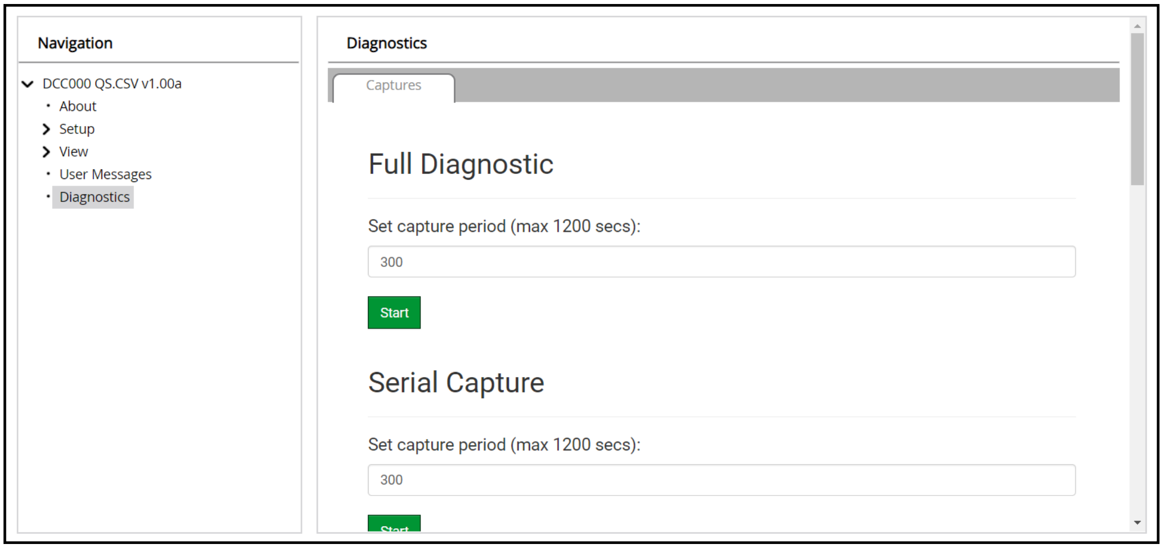


Tag	Description
SS	The SS LED will flash once a second to indicate that the bridge is in operation.
ERR	The SYS ERR LED will go on solid indicating there is a system error. If this occurs, immediately report the related “system error” shown in the error screen of the FS-GUI interface to support for evaluation.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

11.6 Taking a FieldServer Diagnostic Capture

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

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



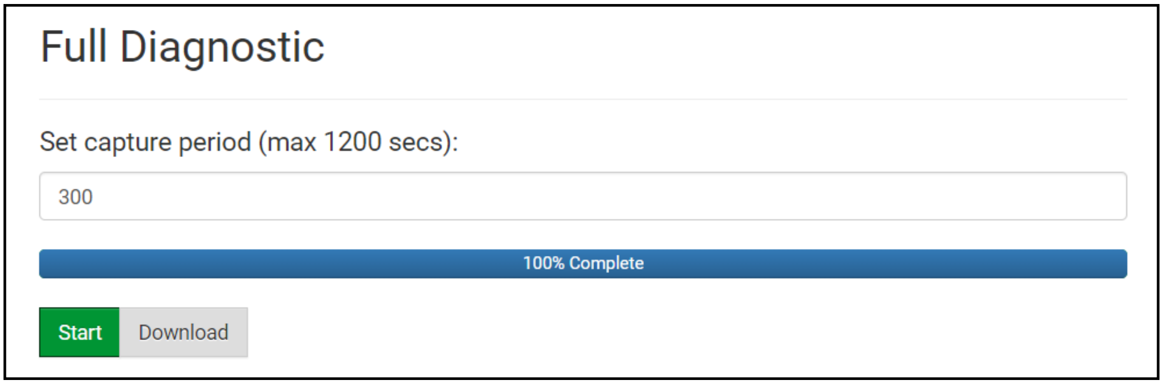
Full Diagnostic

Set capture period (max 1200 secs): 300

Serial Capture

Set capture period (max 1200 secs): 300

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



Full Diagnostic

Set capture period (max 1200 secs): 300

100% Complete

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

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

11.7 Wi-Fi and Cellular Signal Strength

Wi-Fi	Cellular
<60dBm – Excellent	< 60dBm – Excellent
<70dBm – Very good	<70dBm – Very good
<80dBm – Good	<80dBm – Good
>80dBm – Weak	<90dBm – Weak
	>90dBm – Spotty; not good for data

NOTE: If the signal is weak or spotty, try to improve the signal strength by checking the antenna and the FieldServer position.

11.8 Factory Reset Instructions

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

11.9 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.

11.10 Two Ethernet Port IP Subnets

If the user has one of the two Ethernet port units, the Eth1 and Eth2 ports need to be configured on different IP Subnets, otherwise the BACnet IOT Gateway will not be able to discover any BACnet IP or BACnet Ethernet devices on the network.

For example, if the ETH1 port is configured at 192.168.2.101, then the Eth 2 port cannot be configured with the same 192.168.2.XXX settings.

11.11 Data Missing on RESTful API and/or the Grid

If a RESTful API call for data fails and the BACnet IoT Gateway is not listed as a Device Name in the Data Logs found on the Grid, please ensure the following:

1. Check that the BACnet IoT Gateway has been registered to the Grid. (**Section 8.1 Create a New FieldServer Manager Account**)
2. Check that the Monitor View has saved data. (**Section 7.2 Monitor View**)
3. Check that the Log checkbox has been enabled. (**Section 7.2.2 Logging Data**)

12 Additional Information

12.1 Update Firmware

To load a new version of the firmware, follow these instructions:

1. Extract and save the new file onto the local PC.
2. Open a web browser and type the IP Address of the FieldServer in the address bar.
   - Default IP Address is **192.168.**
   - Use the FS Toolbox utility if the IP Address is unknown (**Section 11.2 Lost or Incorrect IP Address**)
3. Click on the “Diagnostics & Debugging” button.
4. In the Navigation Tree on the left hand side, do the following:
   a. Click on “Setup”
   b. Click on “File Transfer”
   c. Click on the “General” tab
5. In the General tab, click on “Choose Files” and select the web.img file extracted in step 1.
6. Click on the orange “Submit” button.
7. When the download is complete, click on the “System Restart” button.

NOTE: Contact to receive any firmware updates.

12.2 APN Table

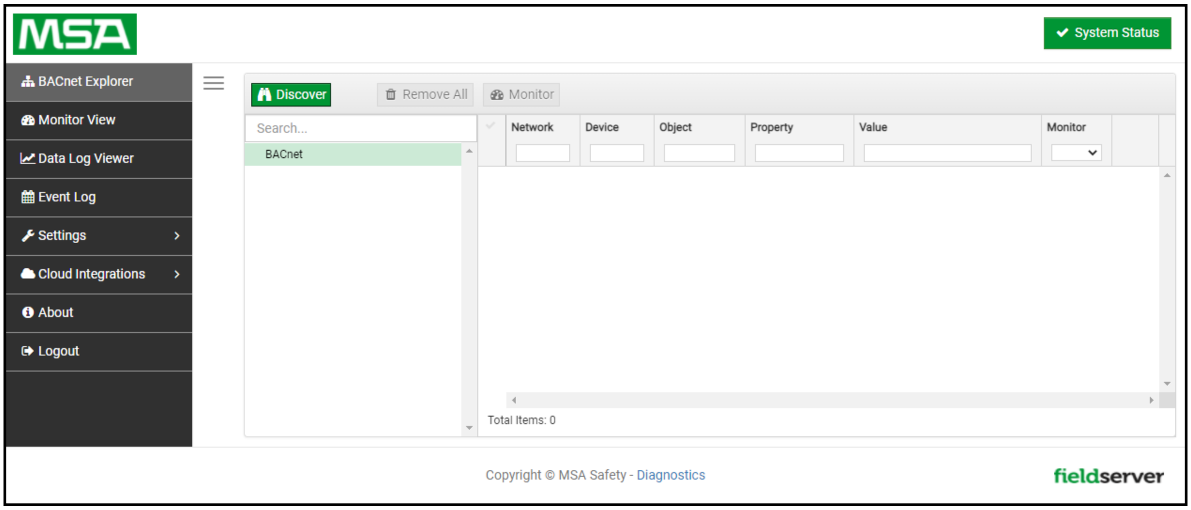
Use the table below to enter one of the correct APNs for your sim card:

Cellular Provider	APN
AT&T	broadband NXTGENPHONE
Verizon	Vzwinternet internet
Kore	c2.korem2m.com

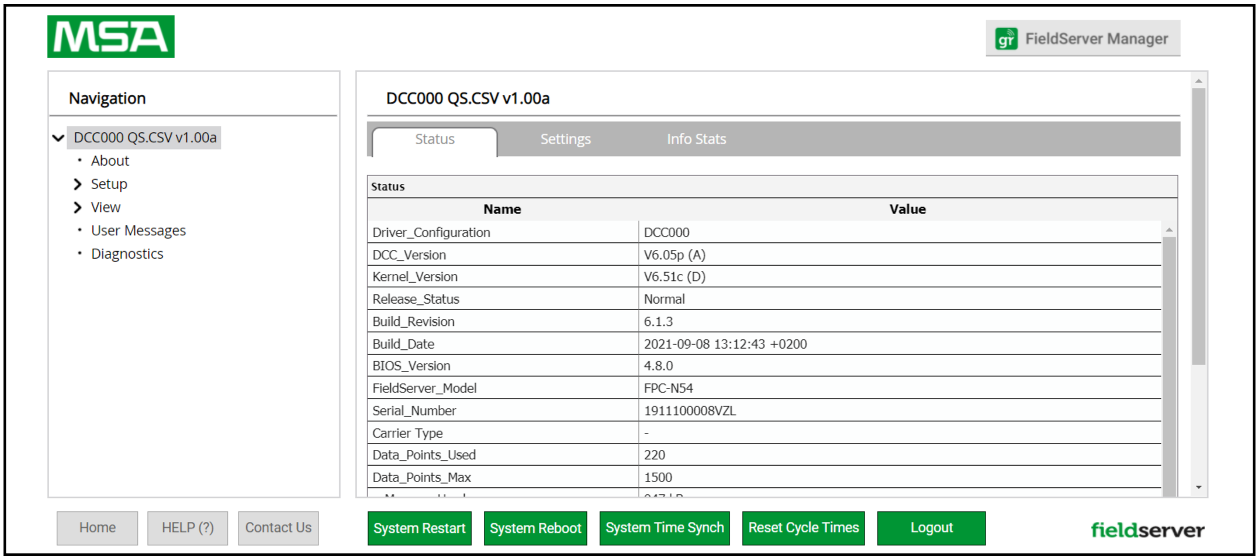
12.3 Change Web Server Security Settings After Initial Setup

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

- Navigate from the BACnet IoT Gateway landing page to the FS-GUI by clicking the blue “Diagnostics” text on the bottom of the screen.



- Click Setup in the Navigation panel.



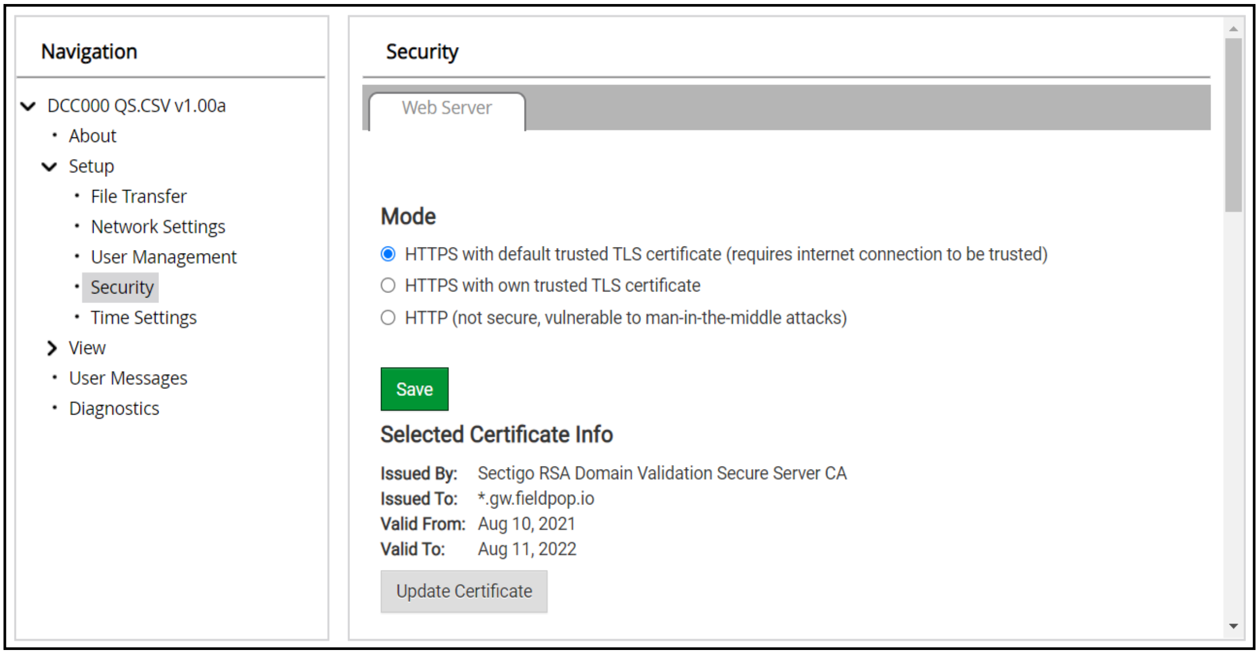
DCC000 QS.CSV v1.00a

Status

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

12.3.1 Change Security Mode

- Click Security in the Navigation panel.



Mode

● HTTPS with default trusted TLS certificate (requires internet connection to be trusted)
○ HTTPS with own trusted TLS certificate
○ HTTP (not secure, vulnerable to man-in-the-middle attacks)

Selected Certificate Info

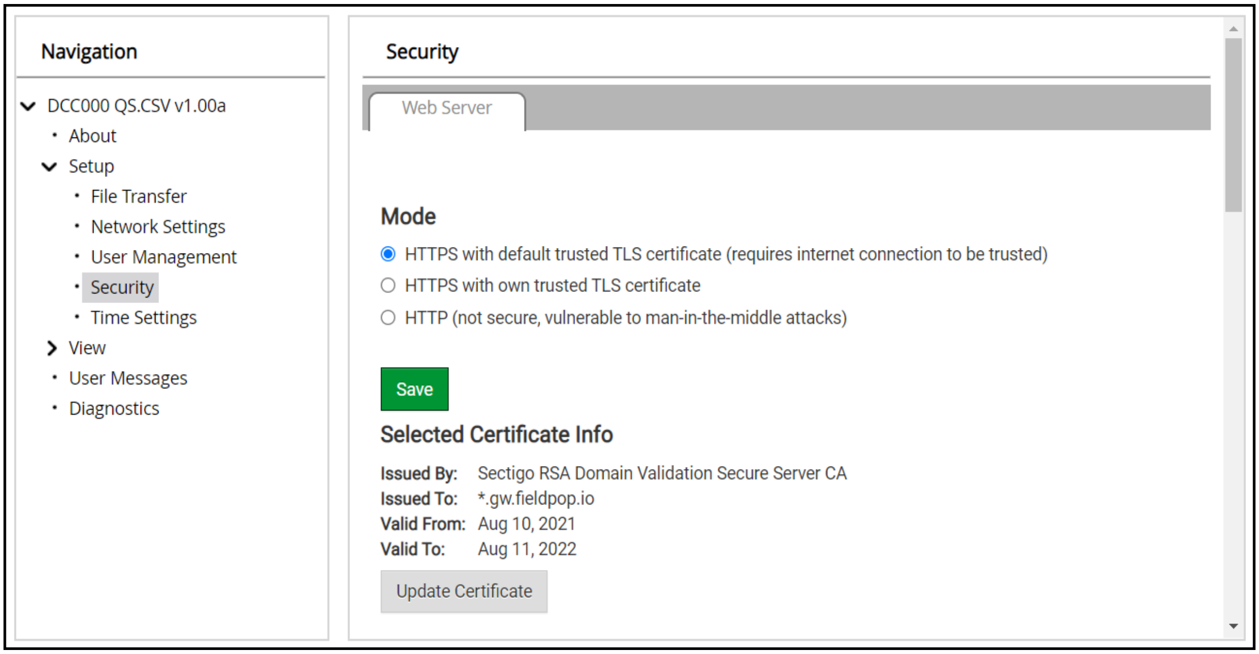
Issued By:	Sectigo RSA Domain Validation Secure Server CA
Issued To:	*.gw.fieldpop.io
Valid From:	Aug 10, 2021
Valid To:	Aug 11, 2022

- Click the Mode desired.
    - If HTTPS with own trusted TLS certificate is selected, follow instructions in **Section 5.2.1 HTTPS with Own Trusted TLS Certificate**
- Click the Save button.

12.3.2 Edit the Certificate Loaded onto the FieldServer

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

- Click Security in the Navigation panel.



Mode

● HTTPS with default trusted TLS certificate (requires internet connection to be trusted)
○ HTTPS with own trusted TLS certificate
○ HTTP (not secure, vulnerable to man-in-the-middle attacks)

Selected Certificate Info

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

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

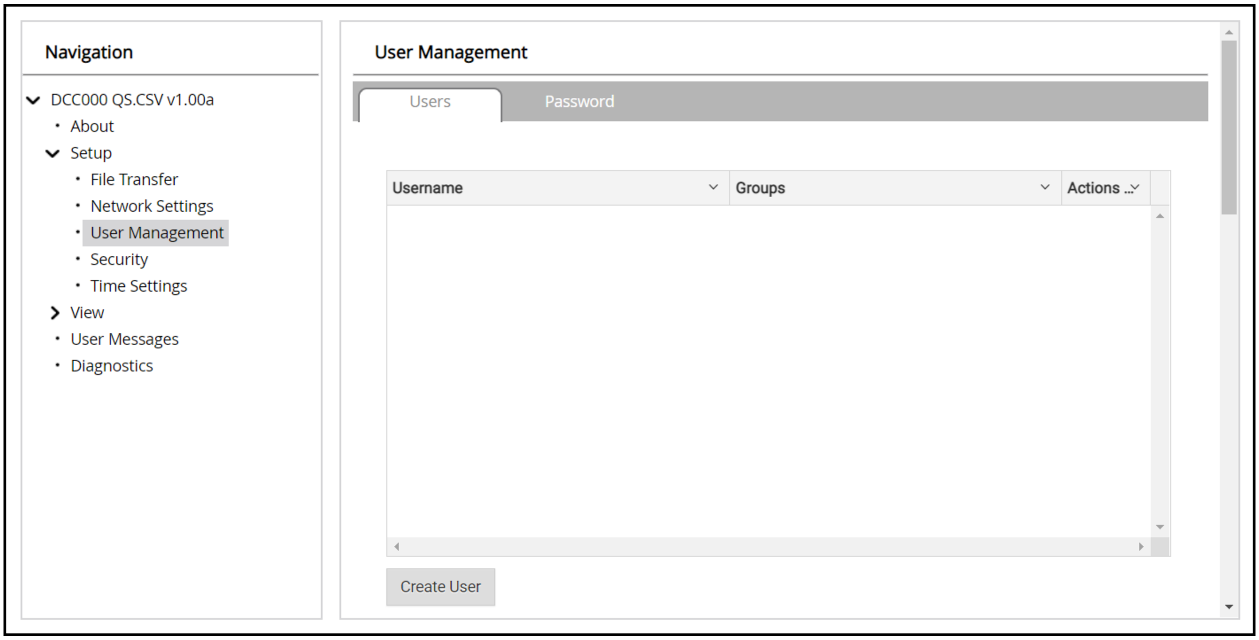
12.4 Change User Management Settings

- 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:

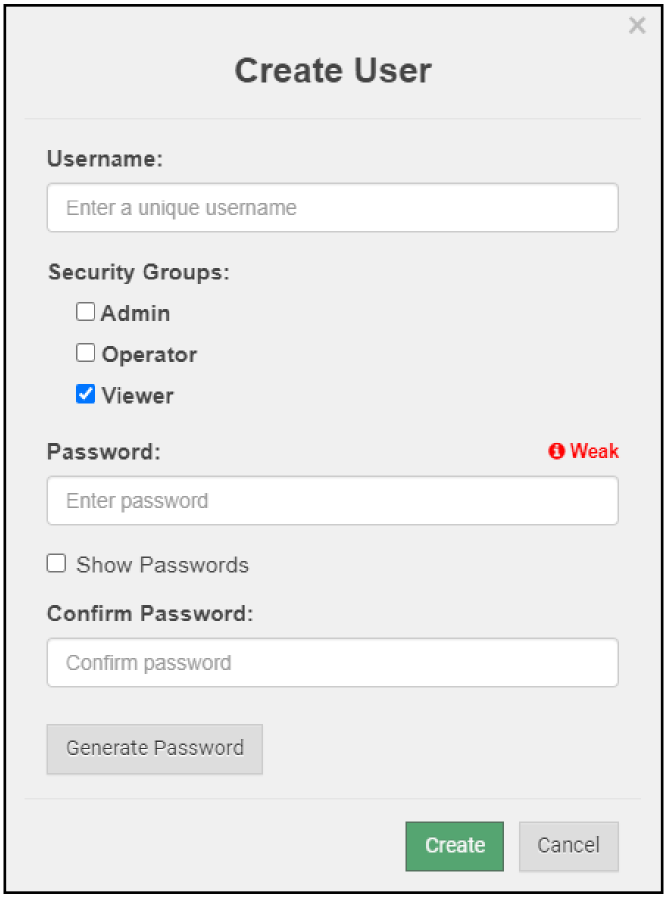
Admin – Can modify and view any settings on the FieldServer.

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

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

12.4.1 Create Users

- Click the Create User button.



Create User

Username:

Enter a unique username

Security Groups:

□ Admin

□ Operator

☑ Viewer

Password: Weak

Enter password

□ Show Passwords

Confirm Password:

Confirm password

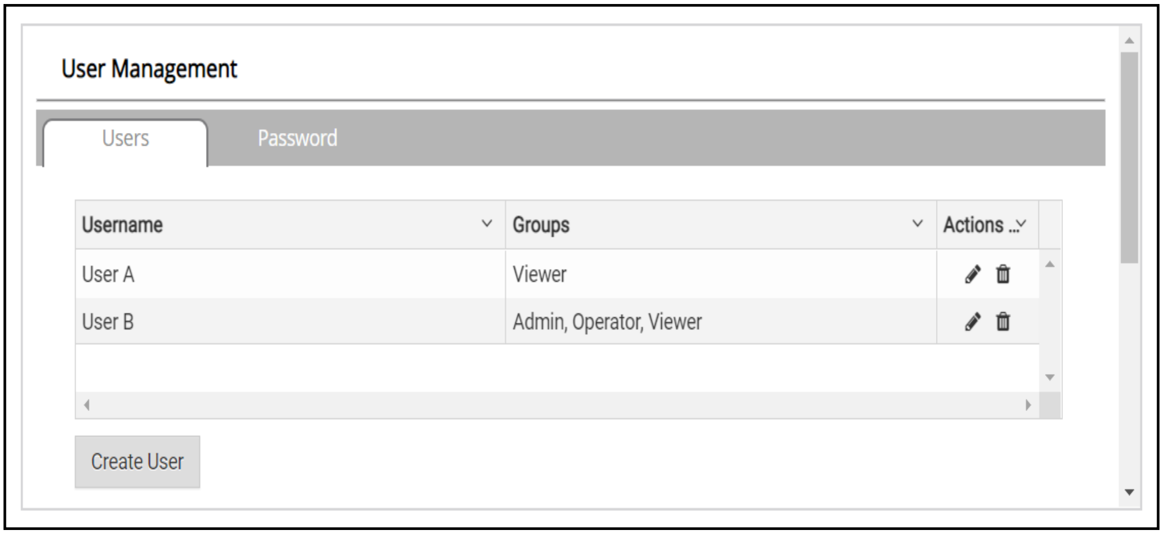
- Enter the new User fields: Name, Security Group and Password.
  - **User details are hashed and salted**

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

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

12.4.2 Edit Users

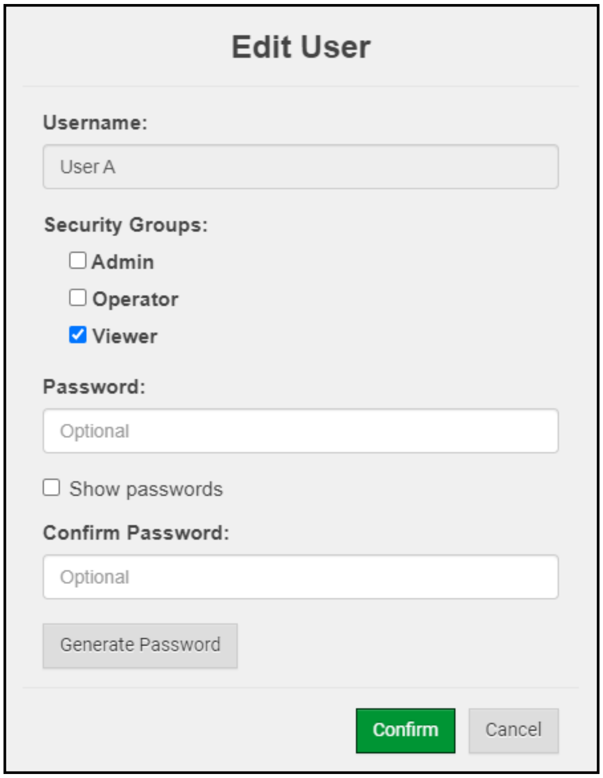
- Click the pencil icon next to the desired user to open the User Edit window.



User Management

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

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



Edit User

Username: User A

Security Groups:

□ Admin

□ Operator

☑ Viewer

Password: Optional

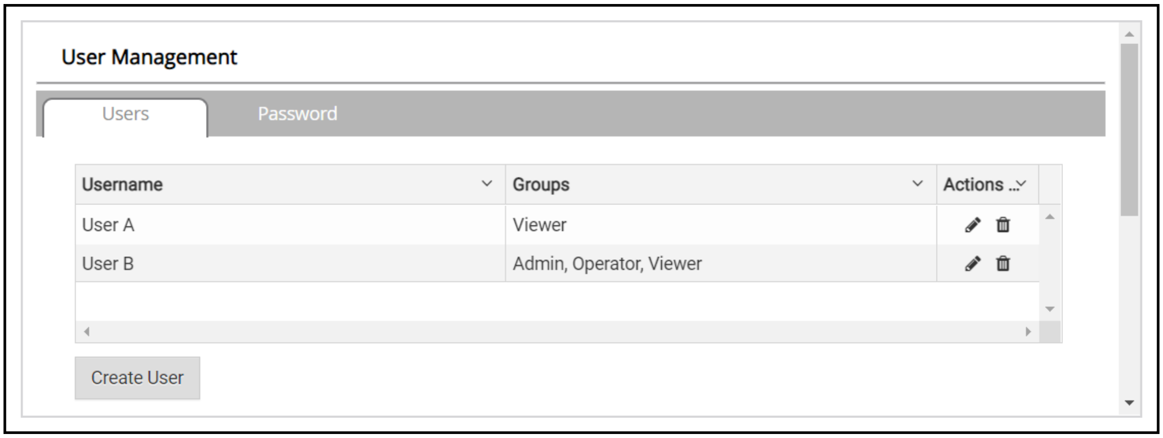
□ Show passwords

Confirm Password: Optional

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

12.4.3 Delete Users

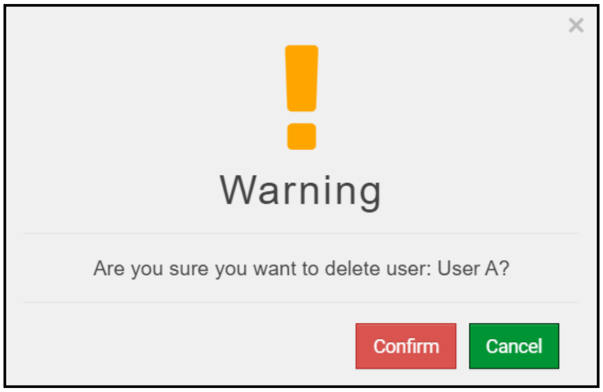
- Click the trash can icon next to the desired user to delete the entry.



User Management

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

- When the warning message appears, click Confirm.

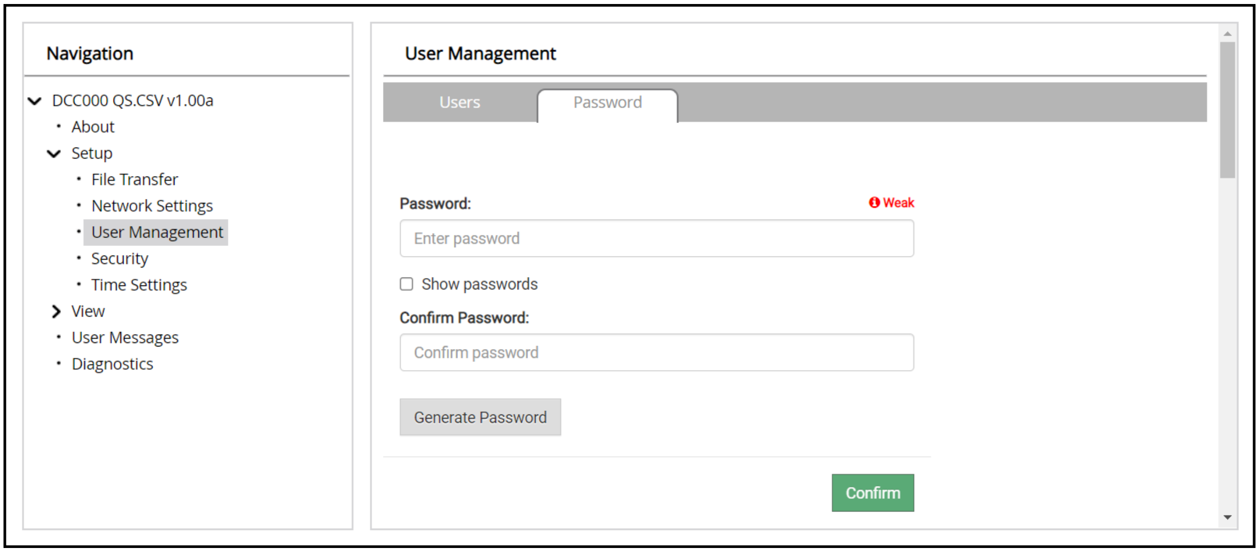


Warning

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

12.4.4 Change FieldServer Password

- Click the Password tab.



User Management

Password: ❶ Weak

Enter password

□ Show passwords

Confirm Password:

Confirm password

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

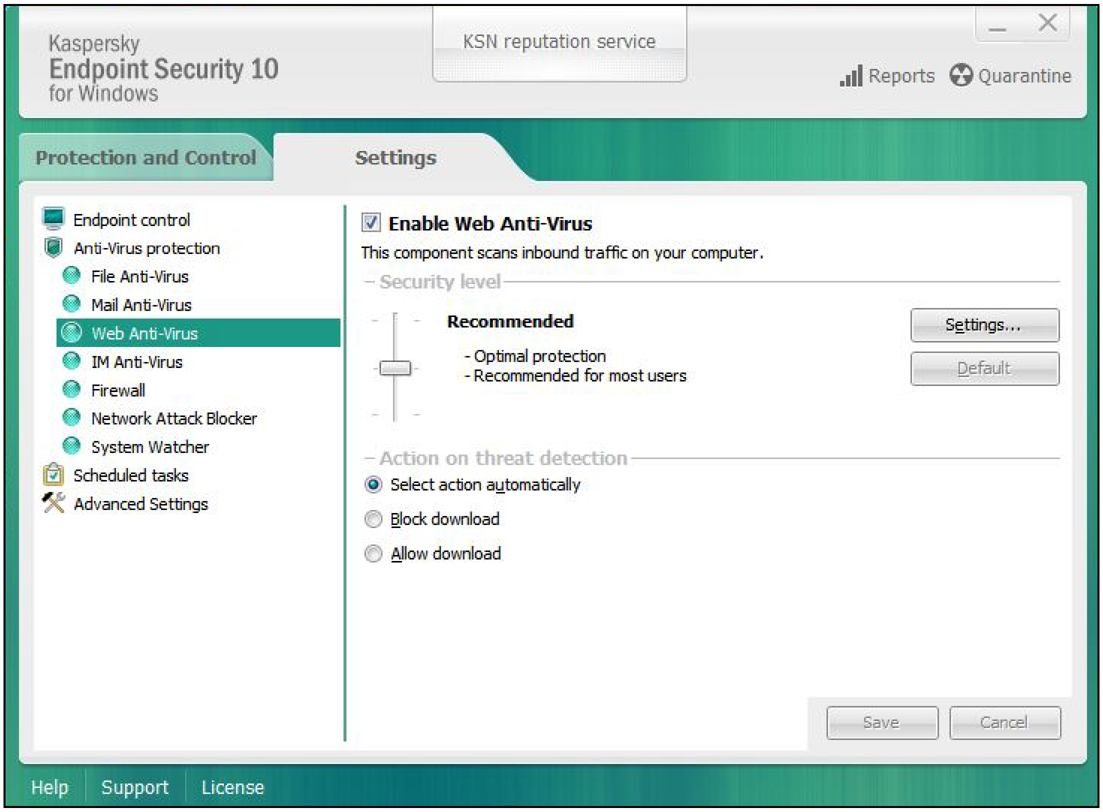
NOTE: The password must meet the minimum complexity requirements. An algorithm automatically checks the password entered and notes the level of strength on the top right of the Password text field.

12.5 Kaspersky Endpoint Security 10

If Kaspersky Endpoint Security 10 is installed on the user's PC, the software needs to be modified to allow the PC to register bridges on the FieldServer Manager.

NOTE: This problem is specific to KES10, Kaspersky 2017 does not have this problem.

To fix the problem, the BACnet IoT Gateway (see http://192.168.100.85/* in the 2nd image below) must be set as a trusted URL to the "Web Anti-Virus"->"Settings" as shown below.



☑ **Enable Web Anti-Virus**

This component scans inbound traffic on your computer.

Security level

Recommended

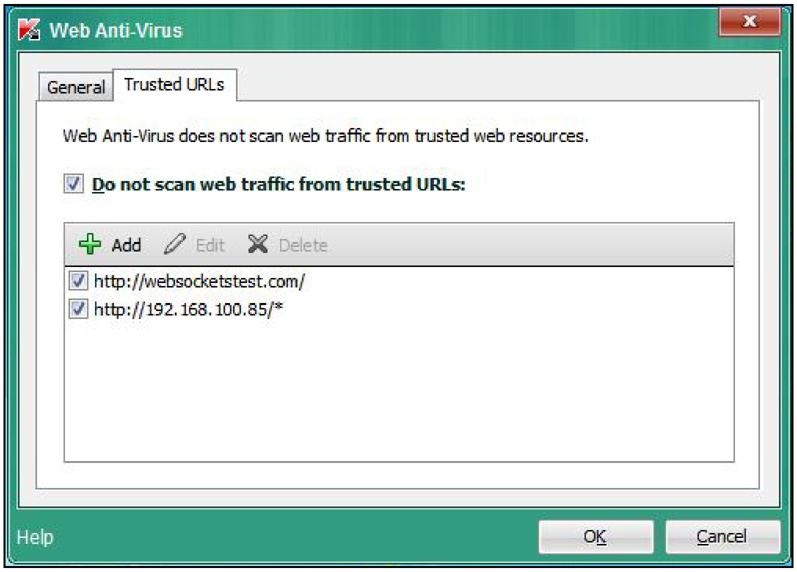
- Optimal protection
- Recommended for most users

Action on threat detection

● Select action automatically

○ Block download

○ Allow download



Web Anti-Virus does not scan web traffic from trusted web resources.

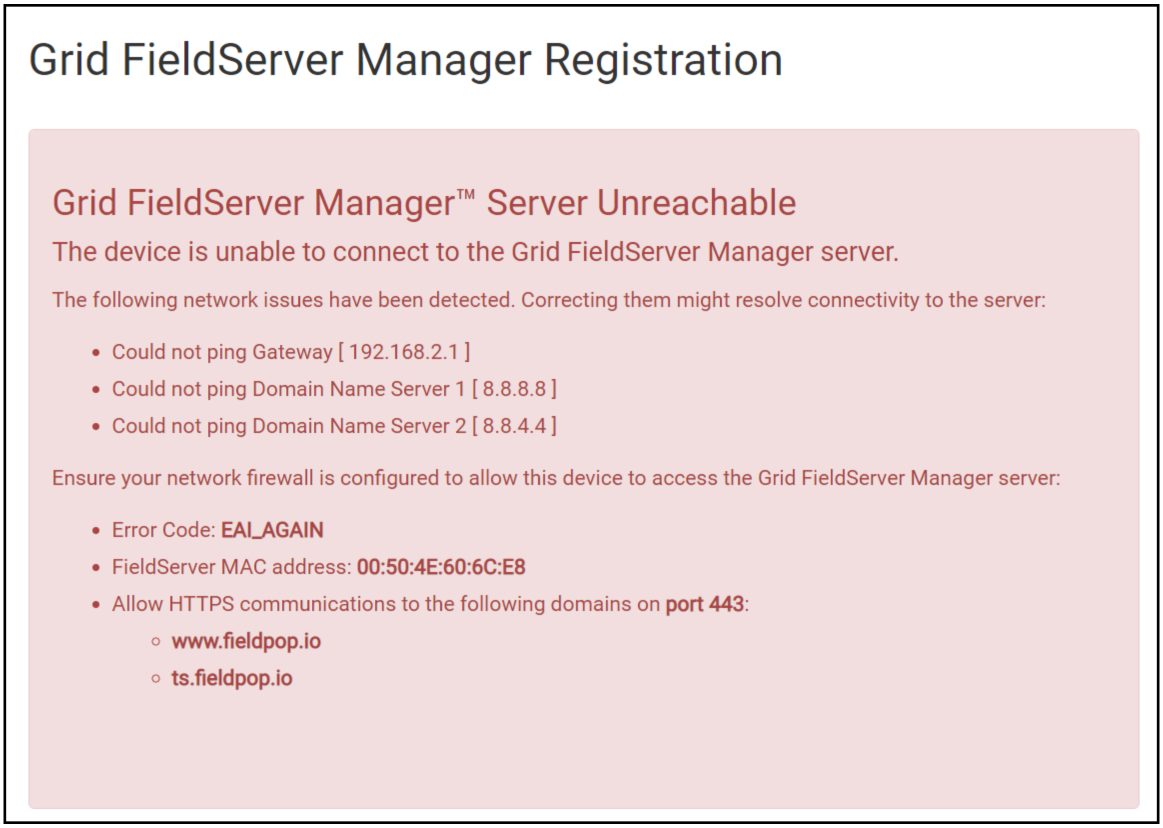
☑ **Do not scan web traffic from trusted URLs:**

☑ http://websocketstest.com/

☑ http://192.168.100.85/*

12.6 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



Grid FieldServer Manager Registration

Grid FieldServer Manager™ Server Unreachable

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

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

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

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

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

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

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

12.7 Warnings for FCC and IC

Waste Disposal

It is recommended to disassemble the device before abandoning it in conformity with local regulations. Please ensure that the abandoned batteries are disposed according to local regulations on waste disposal. Do not throw batteries into fire (explosive) or put in common waste canister. Products or product packages with the sign of “explosive” should not be disposed like household waste but delivered to specialized electrical & electronic waste recycling/disposal center. Proper disposal of this sort of waste helps avoiding harm and adverse effect upon surroundings and people’s health. Please contact local organizations or recycling/disposal center for more recycling/disposal methods of related products.

Comply with the following safety tips:

Do Not use in Combustible and Explosive Environment

Keep away from combustible and explosive environment for fear of danger.

Keep away from all energized circuits.

Operators should not remove enclosure from the device. Only the group or person with factory certification is permitted to open the enclosure to adjust and replace the structure and components of the device. Do not change components unless the power cord is removed. In some cases, the device may still have residual voltage even if the power cord is removed. Therefore, it is a must to remove and fully discharge the device before contact so as to avoid injury.

Unauthorized Changes to this Product or its Components are Prohibited

In the aim of avoiding accidents as far as possible, it is not allowed to replace the system or change components unless with permission and certification. Please contact the technical department of Vantron or local branches for help.

Pay Attention to Caution Signs

Caution signs in this manual remind of possible danger. Please comply with relevant safety tips below each sign. Meanwhile, you should strictly conform to all safety tips for operation environment.

Notice

Considering that reasonable efforts have been made to assure accuracy of this manual, Vantron assumes no responsibility of possible missing contents and information, errors in contents, citations, examples, and source programs.

Vantron reserves the right to make necessary changes to this manual without prior notice. No part of this manual may be reprinted or publicly released.

FCC Warning (BACW, -BACA, -BACV, -BAC2)

This device complies with FCC Rules. Operation is subject to the following conditions.

This device may not cause harmful interference.

This device must accept any interference received, including interference that may cause undesired operation.

This device complies with Part 15C of the FCC Rules

For FS-IOT-BACA/V, this device complies with Part 22H, Part 24E and Part 27 of the FCC Rules.

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.

Any modification to the product is not permitted unless authorized by MSA Safety. It’s not allowed to disassemble the product; it is not allowed to replace the system or change components unless with permission and certification. Please contact the FieldServer technical support department or local branches for help.

IC Statement

This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions:

- This device may not cause interference, and
- This device must accept any interference, including interference that may cause undesired operation of the device.

Warning! This class B digital apparatus complies with Canadian ICES-003.

Industry Canada ICES-003 Compliance Label:

CAN ICES-3 (B)/NMB-3(B)

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts.

L'exploitation est autorisée aux deux conditions suivantes:

- l'appareil ne doit pas produire de brouillage, et
- l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

RF Exposure Warning

This equipment must be installed and operated in accordance with provide instructions and the antenna used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operation in conjunction with any other antenna or transmitter. End-users and installers must be provided with antenna installation instructions and transmitter operating conditions for satisfying RF exposure compliance.

For product compliance test FCC and IC, all the technical documentation is submitted by MSA Safety, who is the customer or importer of the BACnet IoT Gateway.

BACnet IoT Gateway radios have been approved to be used with antennas that have a maximum gain of 3 dBi. Any antennas with a gain greater than 3 dBi are strictly prohibited for use with this device.

Power Output

Frequency Range Output Power:

Wi-Fi *(BACW, -BACA, -BACV, -BACF only)*
2402.0 – 2480 MHz 0.004 W

2412.0 – 2462.0 MHz 0.0258 W

LTE *(-BACA, -BACV, -BACF only)*
Supported Bands:
FS-IOT-BACA/V – B2, B4, B5, B12, B13 & B17 (0.25 W)
FS-IOT-BACF – B1, B3, B7, B8, B20 (0.25 W)

The Output Power listed is conducted. The device should be professionally installed to ensure compliance with power requirements. The antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and not be co-located with any other transmitters except in accordance with multi-transmitter product procedures. This device supports 20MHz and 40MHz bandwidth.

13 Limited 2 Year Warranty

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

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

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

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