Start-up Guide

BACnet IoT Gateway FS-IOT-BACX

APPLICABILITY & EFFECTIVITY
Effective for all systems manufactured after April 2022.

Document Revision: 6.E

T18620

MSA Safety
1991 Tarob Court
Milpitas, CA 95035
Website: www.MSAsafety.com

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

Table of Contents

List of Figures

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-BAC2E 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

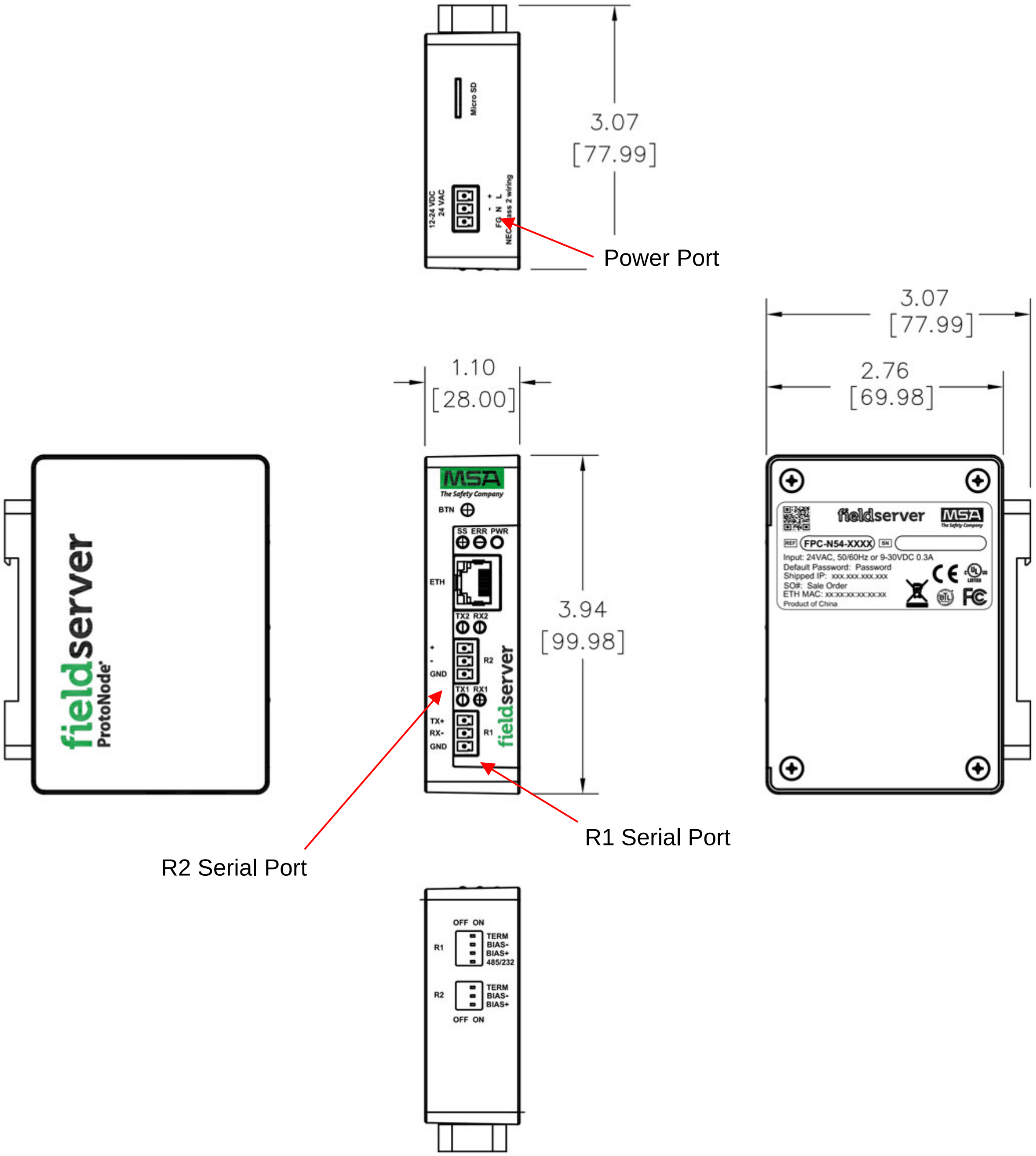


Figure 1: BACnet IoT Gateway FS-IOT-BAC Dimensions

2.1.2 FS-IOT-BAC2E Drawing

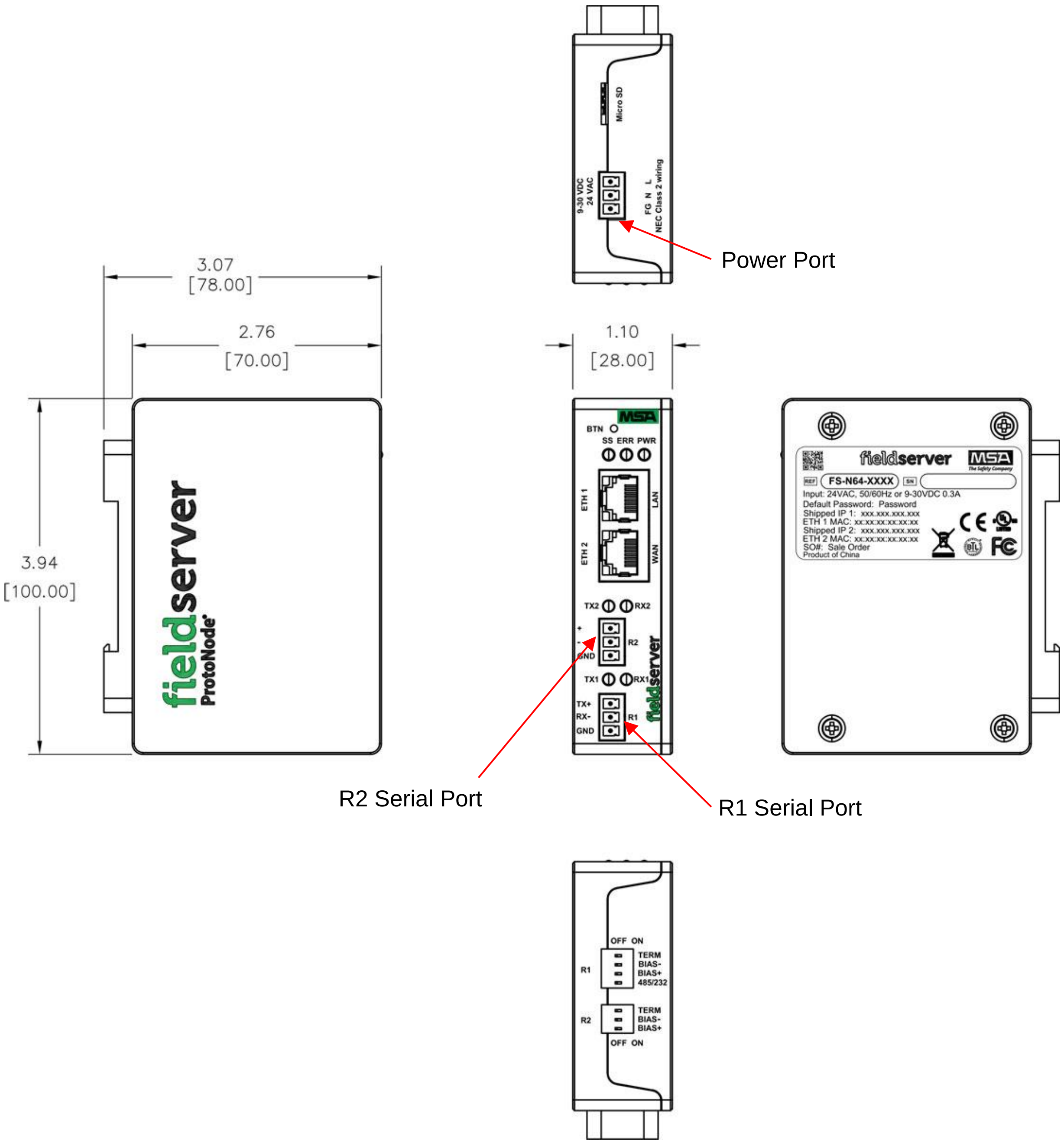


Figure 2: BACnet IoT Gateway FS-IOT-BAC2E Dimensions

2.1.3 FS-IOT-BACW Drawing

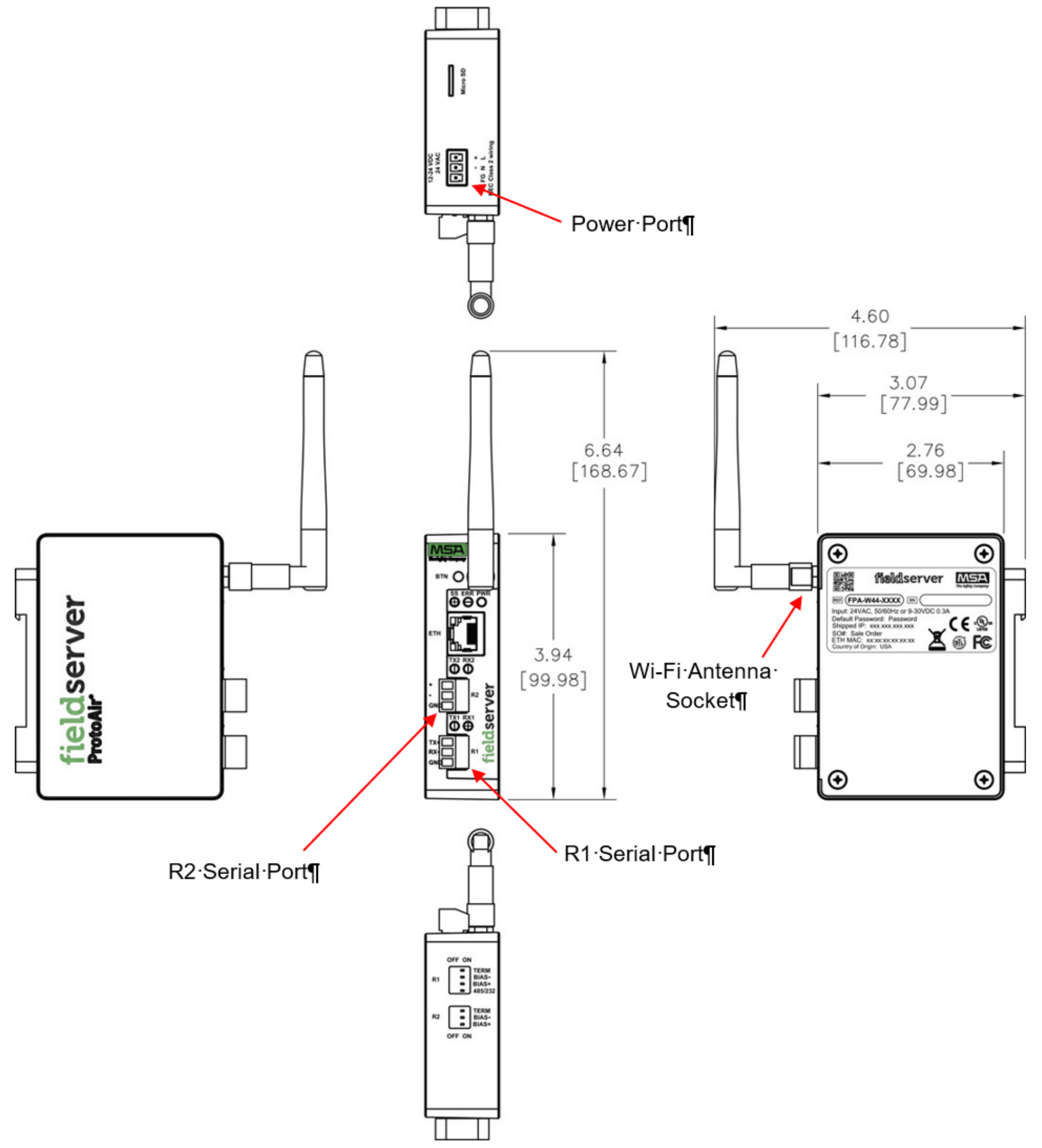


Figure 3: BACnet IoT Gateway FS-IOT-BACW Dimensions

2.1.4 FS-IOT-BACA/V/F Drawing

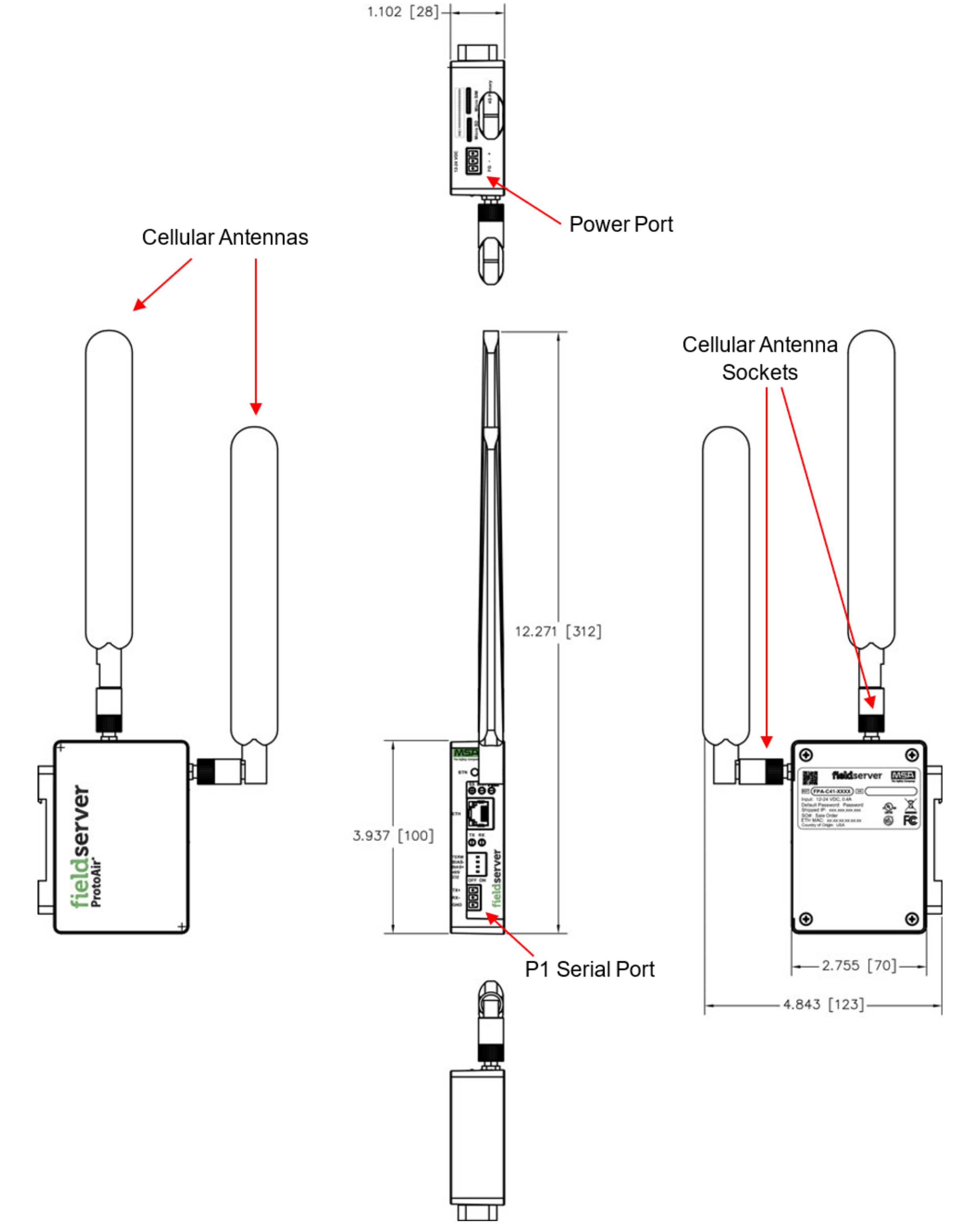


Figure 4: BACnet IoT Gateway FS-IOT-BAC/V/F Dimensions

2.2 Mounting

The BACnet IoT Gateway can be mounted using the DIN rail mounting bracket on the back of the unit.

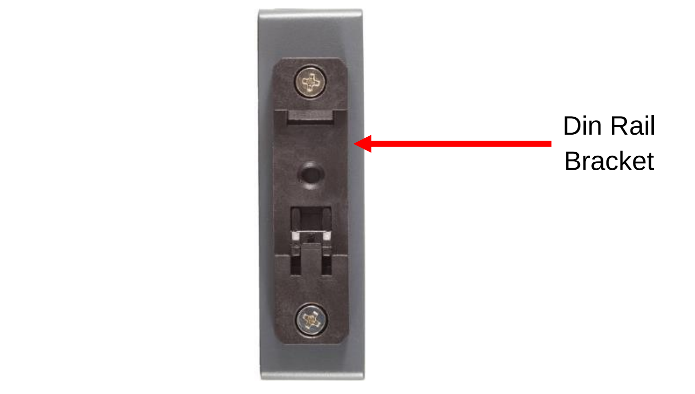


Figure 5: DIN Rail

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 socket on the front of the unit. For the location of the socket, see **Figure 3**.

Cellular Antennas:

If using the FS-IOT-BACA/V/F models, screw in the long cellular antennas into the sockets on the top and the front of the unit as shown in **Figure 4**.

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

NOTE: A micro 4G SIM card must be purchased from an AT&T, Verizon or Vodafone cellular provider to set up cellular functionality and create a data plan for the ProtoAir. 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.

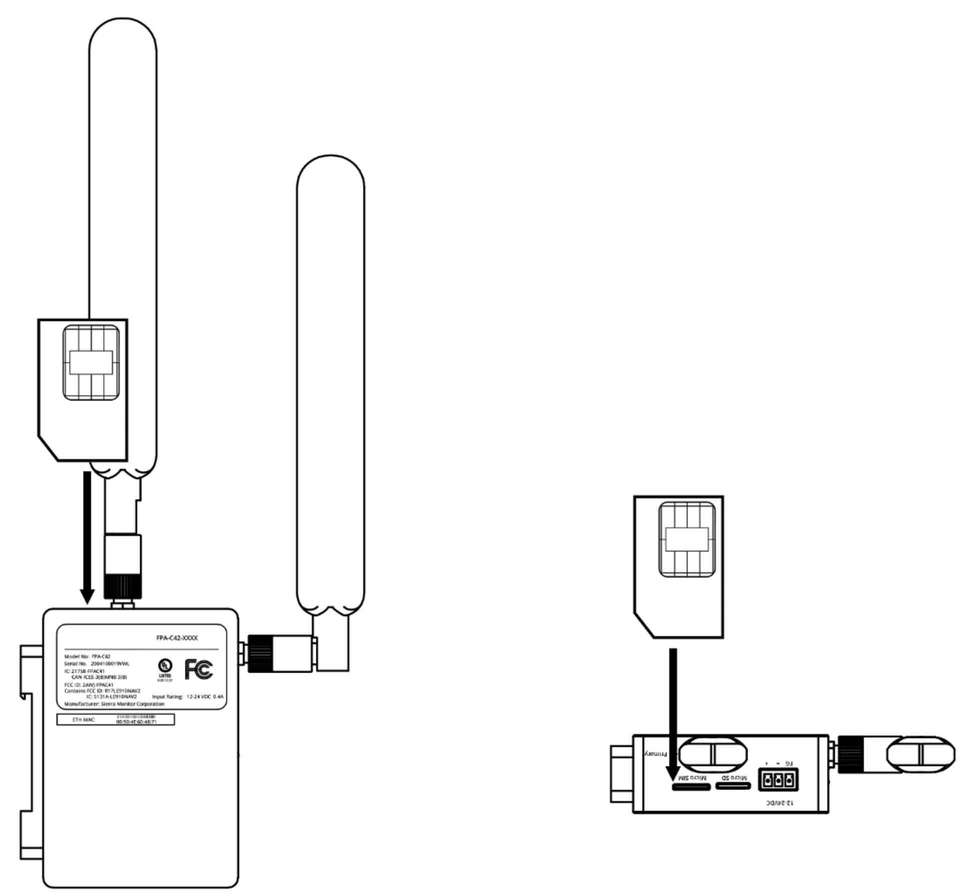


Figure 6: Insert SIM Card into the Micro SIM Card Slot – Label Side View (Left) and Top Down View (Right)

See **Section 7.1** 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

Figure 7: Cellular Data Usage Examples

SIM Card Vendor Contact Information:

Verizon

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

3.1 FS-IOT- BAC/BACW/BAC2E: Connecting the R1 & R2 Ports

NOTE: Ensure RS-485 is selected for R1 by checking that the number 4 DIP Switch is set to the left side.

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

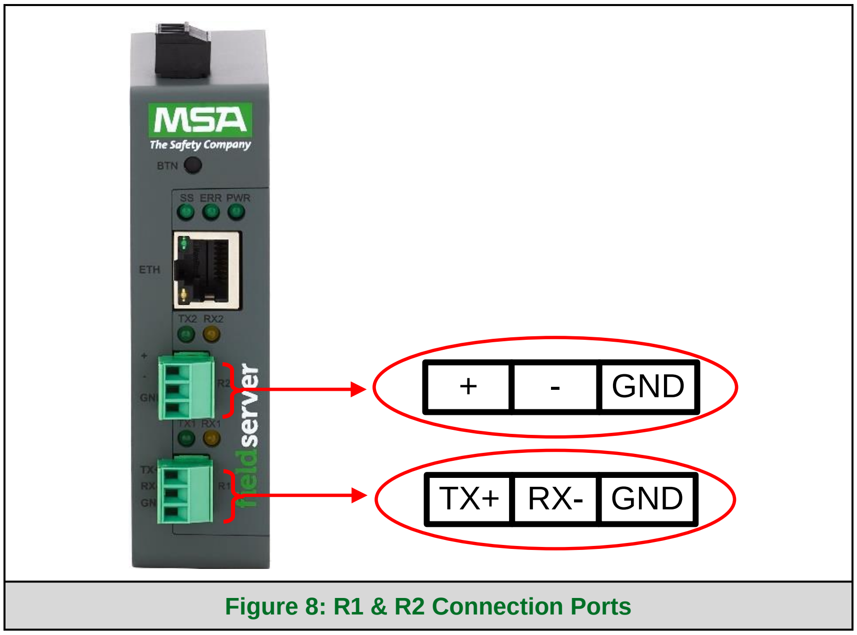


Figure 8: R1 & R2 Connection Ports

The following baud rates are supported for both ports:
9600, 19200, 38400, 76800

3.1.1 Wiring

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

NOTE: Use standard grounding principles for GND.

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

NOTE: Ensure RS-485 is selected by checking that the number 4 DIP Switch is set to the left side.

Connect to the 3-pin connector as shown below.

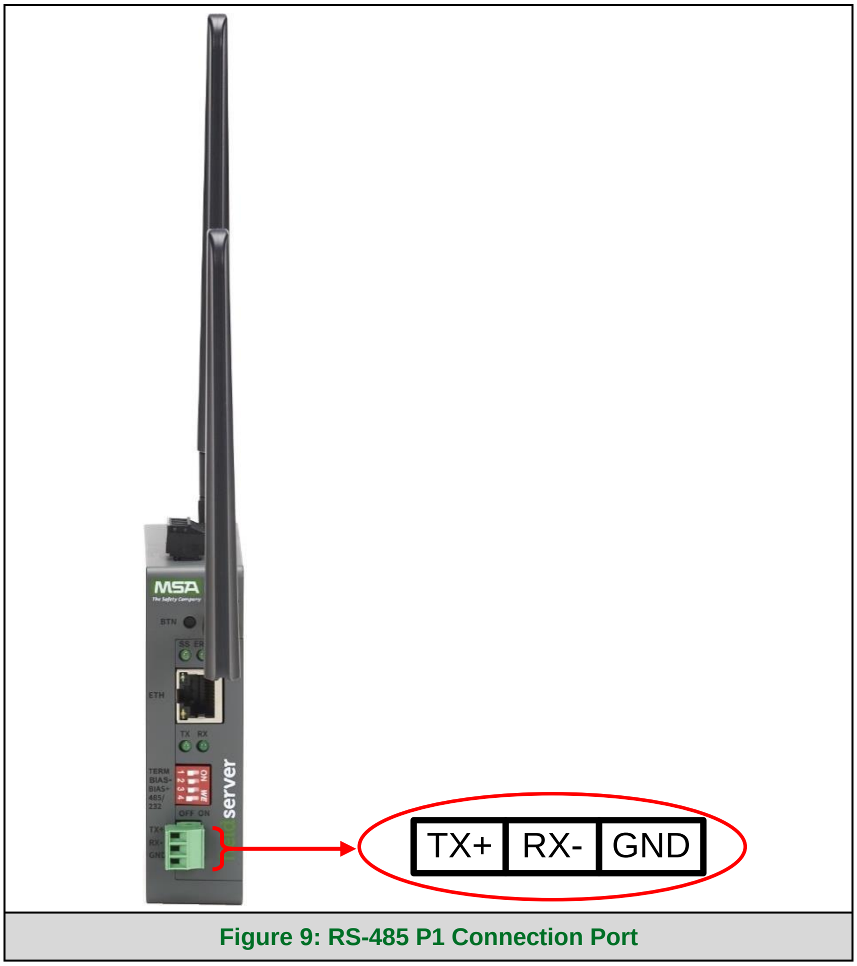


Figure 9: RS-485 P1 Connection Port

The following Baud Rates are supported on the P1 Port:
9600, 19200, 38400, 76800

3.2.1 Wiring

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

NOTE: Use standard grounding principles for GND.

3.3 10/100 Ethernet Connection Port

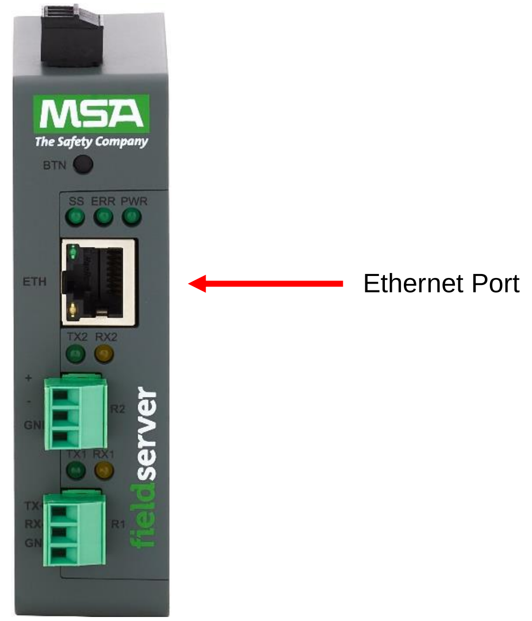


Figure 10: Ethernet Connection

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

NOTE: The Default IP Address of the BACnet IoT Gateway is 192.168.2.101, Subnet Mask is 255.255.255.0.

4 Power up the BACnet IoT 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/BAC2E (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.			

Figure 11: Required Current Draw for the BACnet IoT Gateway

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/BAC2E** BACnet IoT Gateway accepts 9-30VDC or 24VAC.
- The **FS-IOT-BACA/V/F** BACnet IoT Gateways accept 12-24VDC.

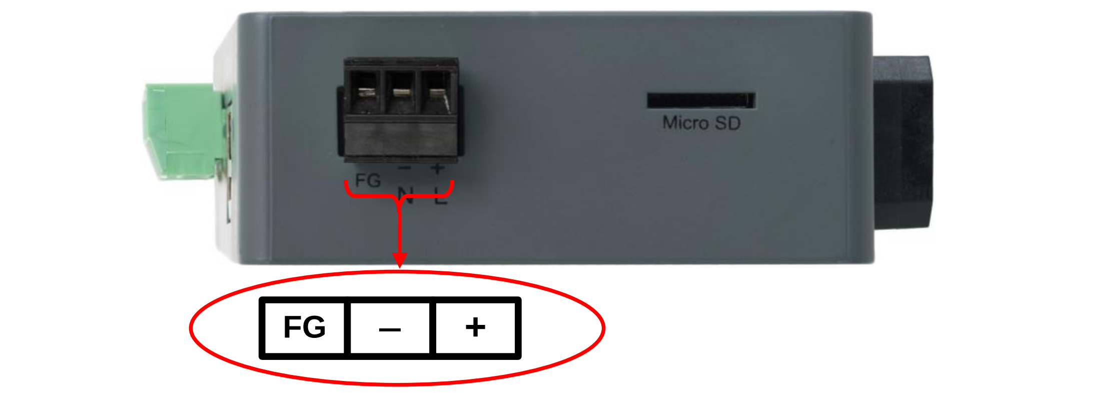


Figure 12: Connecting Power for FS-IOT- BAC/BACW/BAC2E

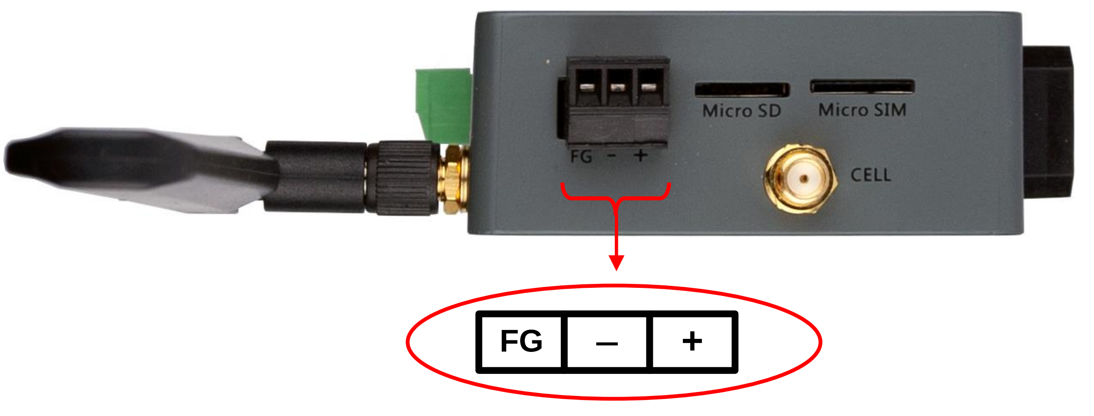


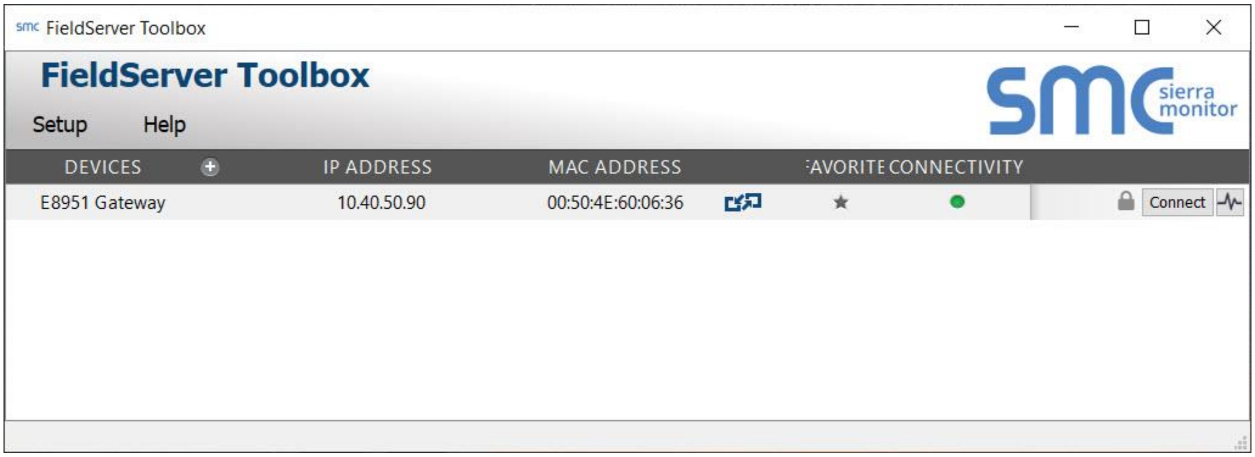
Figure 13: Connecting Power for FS-IOT-BACA/V/F

5 Connecting to the BACnet IoT Gateway

The FieldServer Toolbox Application can be used to discover and connect to the BACnet IoT Gateway on a local area network. To manually connect to the BACnet IoT Gateway using the Toolbox, click on the plus icon (+) and enter the IP Address, or enter the Internet IP Address into a web browser.

5.1 Using the FieldServer Toolbox

- Install the Toolbox application from the USB drive or get it from the MSA Safety website.
- Use the Toolbox application to find the BACnet IoT Gateway IP Address and launch the Web App (by clicking the Connect button).



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

5.2 Using a Web Browser

Open a Web Browser and input the BACnet IoT Gateway's 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.

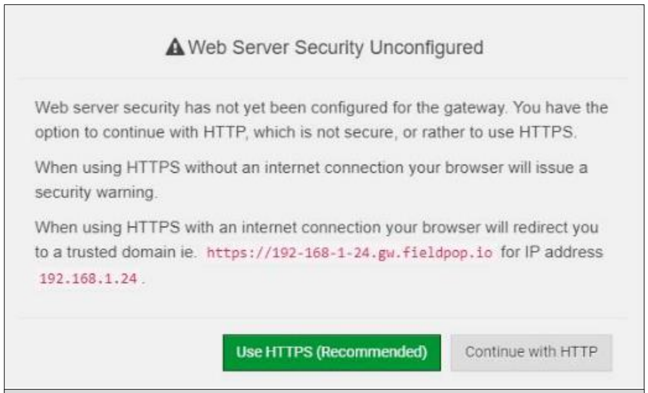
NOTE: Check Section 14.10 for supported browsers.

6 Setup Web Server Security

6.1 Login to the FieldServer

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

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



Web Server Security Unconfigured

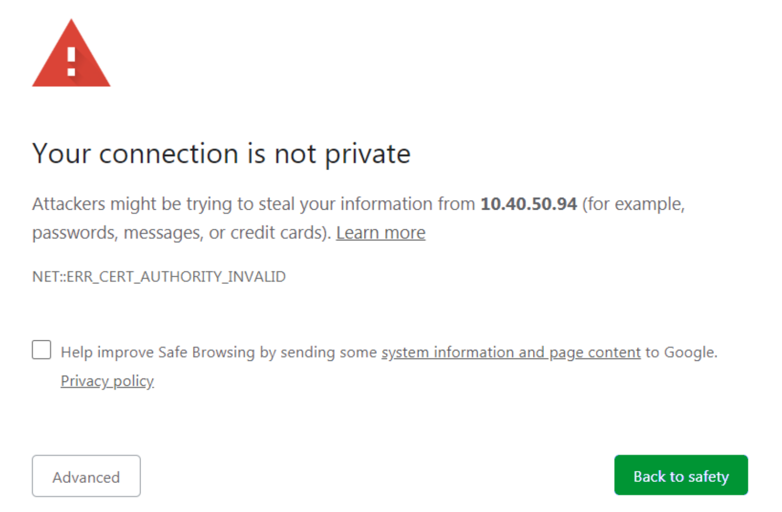
Web server security has not yet been configured for the gateway. You have the option to continue with HTTP, which is not secure, or rather to use HTTPS.

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`.

Figure 14: Web Server Security Window

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



Your connection is not private

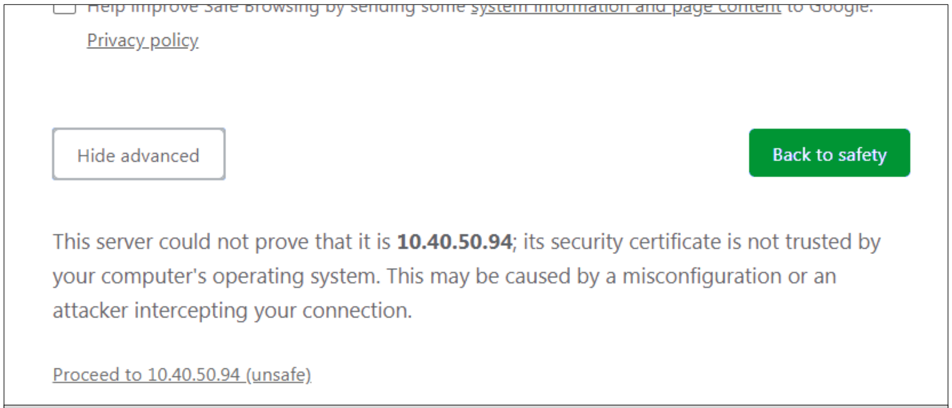
Attackers might be trying to steal your information from **10.40.50.94** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

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

Figure 15: Connection Not Private Warning

- Additional text will expand below the warning, click the underlined text to go to the IP Address. In the **Figure 16** example this text is "Proceed to 10.40.50.94 (unsafe)".


☐ Help improve Safe Browsing by sending some system information and page content to Google.
Privacy policy
Hide advanced
Back to safety

This server could not prove that it is **10.40.50.94**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to 10.40.50.94 (unsafe)

Figure 16: Warning Expanded Text

- 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.

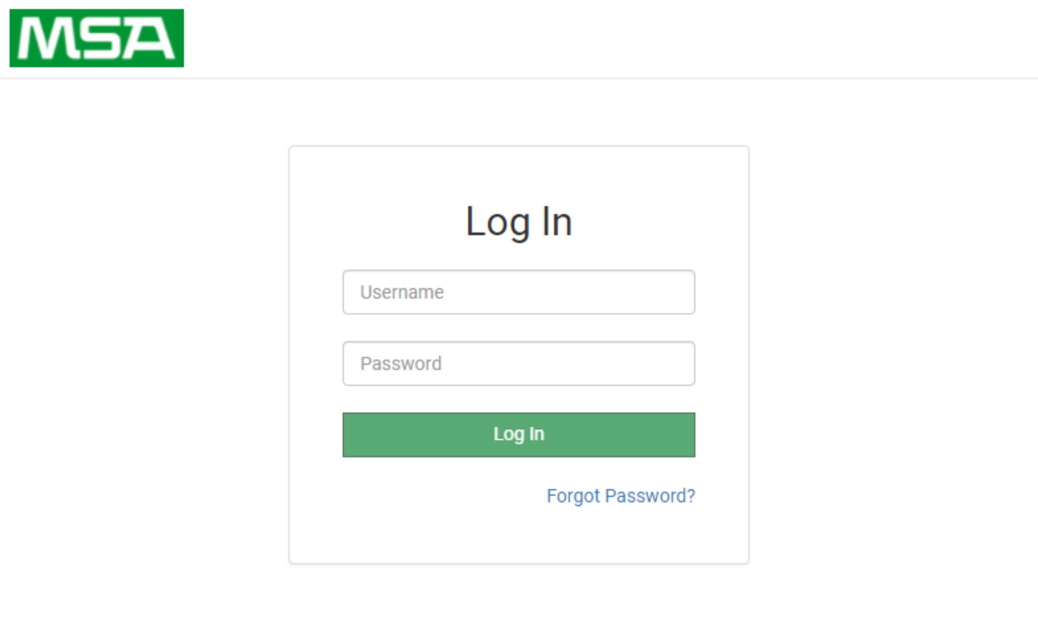


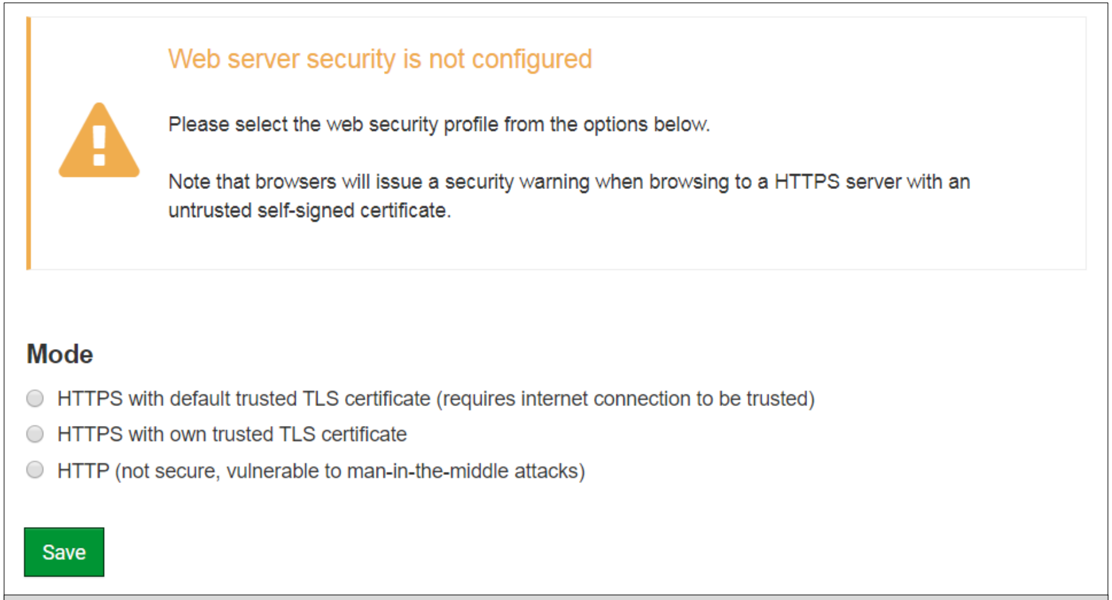
Figure 17: FieldServer Login

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 15.3.

6.2 Select the Security Mode

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



Web server security is not configured

Please select the web security profile from the options below.

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

Mode

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

Figure 18: Security Mode Selection Screen

NOTE: Cookies are used for authentication.

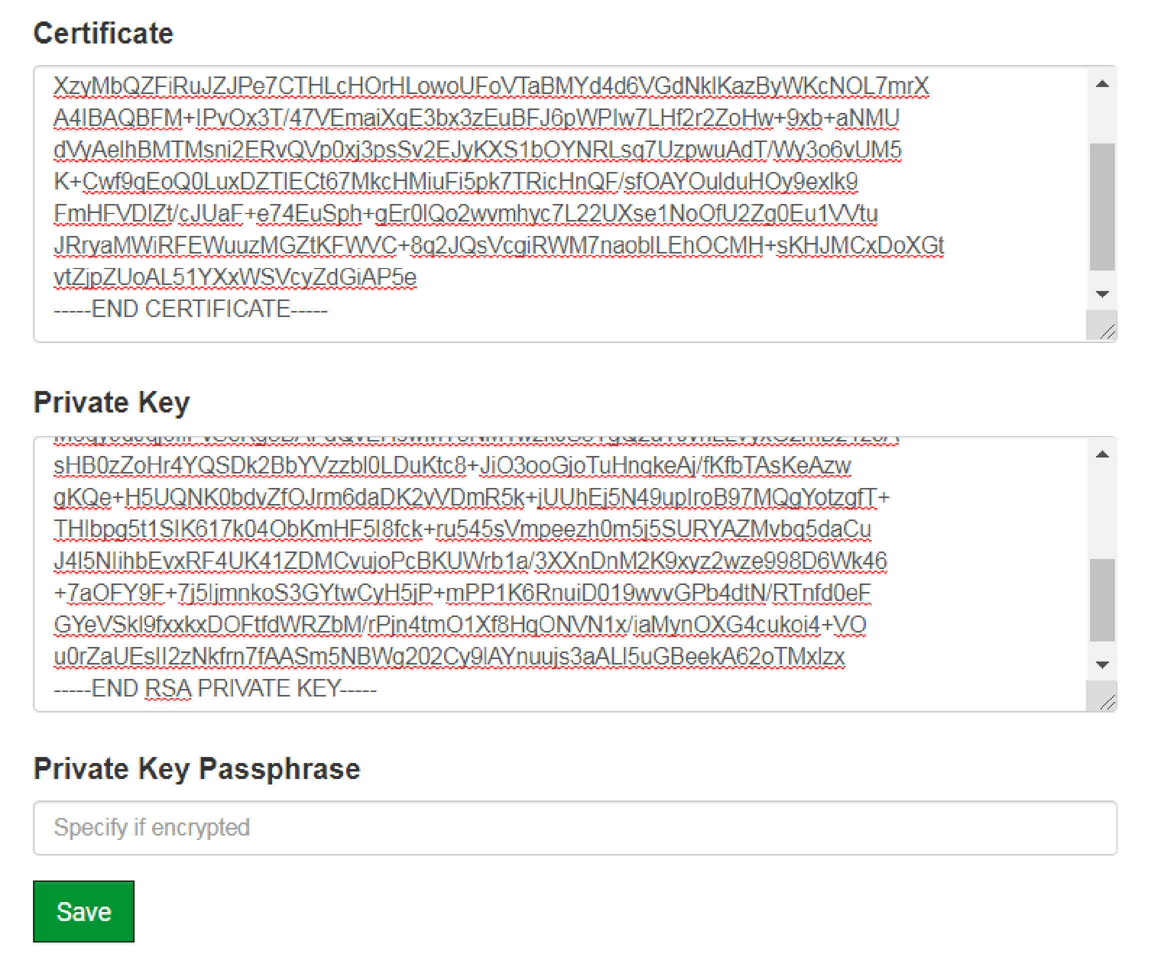
NOTE: To change the web server security mode after initial setup, go to Section 15.2.

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

6.2.1 HTTPS with Own Trusted TLS Certificate

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

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



Certificate

```
XzyMbQZFiRuJZJPe7CTHLcHOrHLowoUFoVTaBMYd4d6VGdNklKazByWKcNOL7mrX
A4IBAQBFM+lPvOx3T/47VEmaiXqE3bx3zEuBFJ6pWPlw7LHf2r2ZoHw+9xb+aNMU
dVyAelhBMTMsni2ERvQVp0xj3psSv2EJyKXS1bOYNRLsq7UzpwuAdT/Wy3o6vUM5
K+Cwf9qEoQ0LuxDZTlECt67MkcHMiuFi5pk7TRicHnQF/sfOAYOulduHOy9exlk9
FmHFVDlZt/cJUaF+e74EuSph+gEr0lQo2wvmhyc7L22UXse1NoOfU2Zg0Eu1VVtu
JRryaMWiRFEWuuzMGZtKFWVC+8q2JQsVcgiRWM7naoblLEhOCMH+sKHJMCxDoXGt
vtZjpZUoAL51YXxWSVcyZdGiAP5e
-----END CERTIFICATE-----
```

Private Key

```
sHB0zZoHr4YQSDk2BbYVzzbl0LDuKtc8+JiO3ooGjoTuHnqkeAj/fKfbTAsKeAzw
gKQe+H5UQNK0bdvZfOJrm6daDK2vVDmR5k+jUUhEj5N49upIroB97MQgYotzgfT+
THIbpg5t1SIK617k04ObKmHF5I8fck+ru545sVmpeezh0m5j5SURYAZMvbq5daCu
J4I5NIihbEvxRF4UK41ZDMCvujoPcBKUWrb1a/3XXnDnM2K9xyz2wze998D6Wk46
+7aOFY9F+7j5ljmnkoS3GYtwCyH5jP+mPP1K6RnuiD019wvvGPb4dtN/RTnfd0eF
GYeVSkl9fxxkxDOFtfdWRZbM/rPjn4tmO1Xf8HqONVN1x/iaMynOXG4cukoi4+VO
u0rZaUEsII2zNkfrn7fAASm5NBWg202Cy9lAYnuujs3aALI5uGBeekA62oTMxlzx
-----END RSA PRIVATE KEY-----
```

Private Key Passphrase

Specify if encrypted

Figure 19: Security Mode Selection Screen – Certificate & Private Key

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

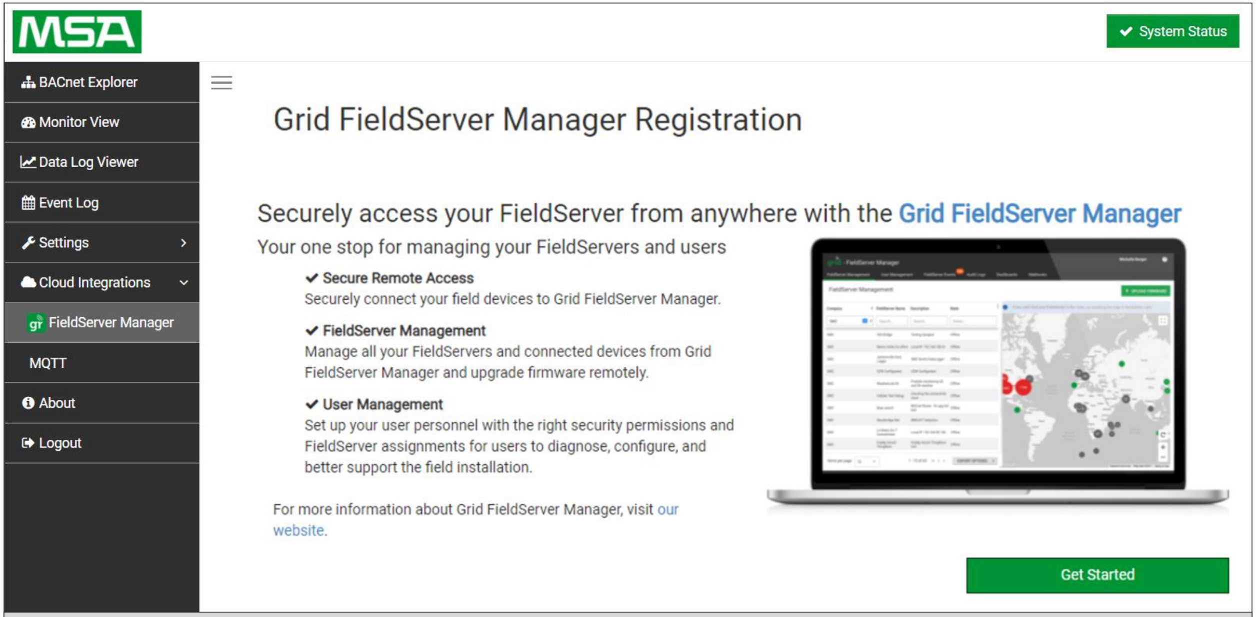
6.2.2 HTTPS with Default Untrusted Self-Signed TLS Certificate or HTTP with Built-in Payload Encryption

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

7 Gateway Settings

7.1 Navigate to the 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.

Figure 20: Web App Landing Page

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

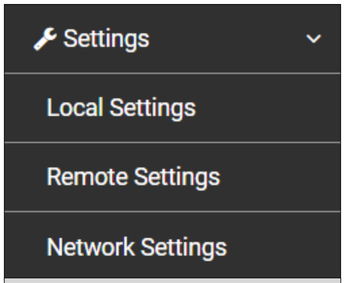
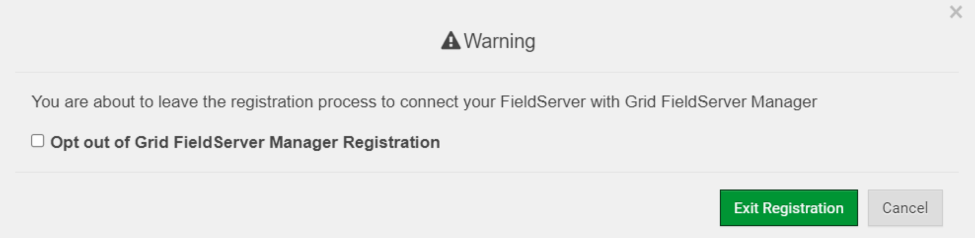


Figure 21: Settings Tabs

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



Warning

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

☐ Opt out of Grid FieldServer Manager Registration

Figure 22: Opt Out Warning Message

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 settings have been saved the Refresh button is unavailable.
Defaults	Click to change settings back to factory defaults.

Figure 23: Configuration Button Functions

7.1.1 ETH 1 IP Settings

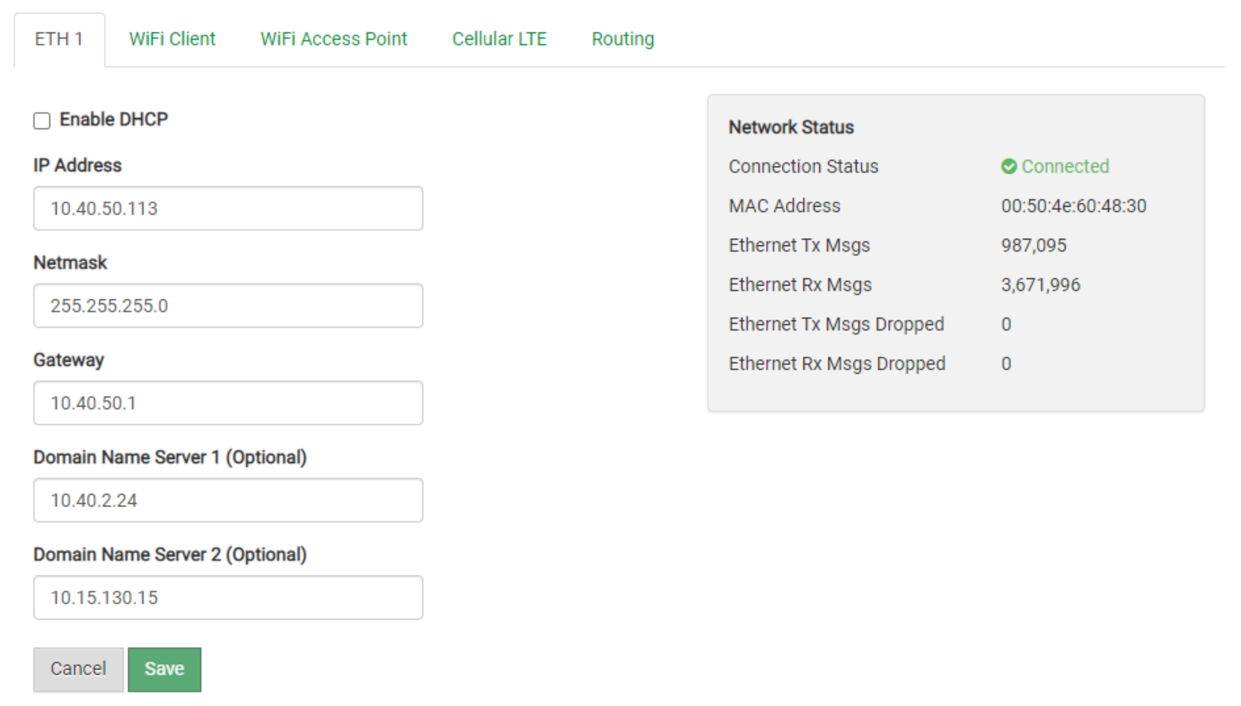
The ETH 1 tab is the landing page when selecting the Network Settings tab. To change the FieldServer IP Settings, follow these instructions:

- 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 connected to a router, set the Gateway to the same IP Address as the router.

- Click the Save button to activate the new settings.

NOTE: If the webpage was open in a browser, the browser will need to be pointed to the new IP Address before the webpage 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	987,095
Ethernet Rx Msgs	3,671,996
Ethernet Tx Msgs Dropped	0
Ethernet Rx Msgs Dropped	0

Figure 24: ETH 1 Port Network Settings

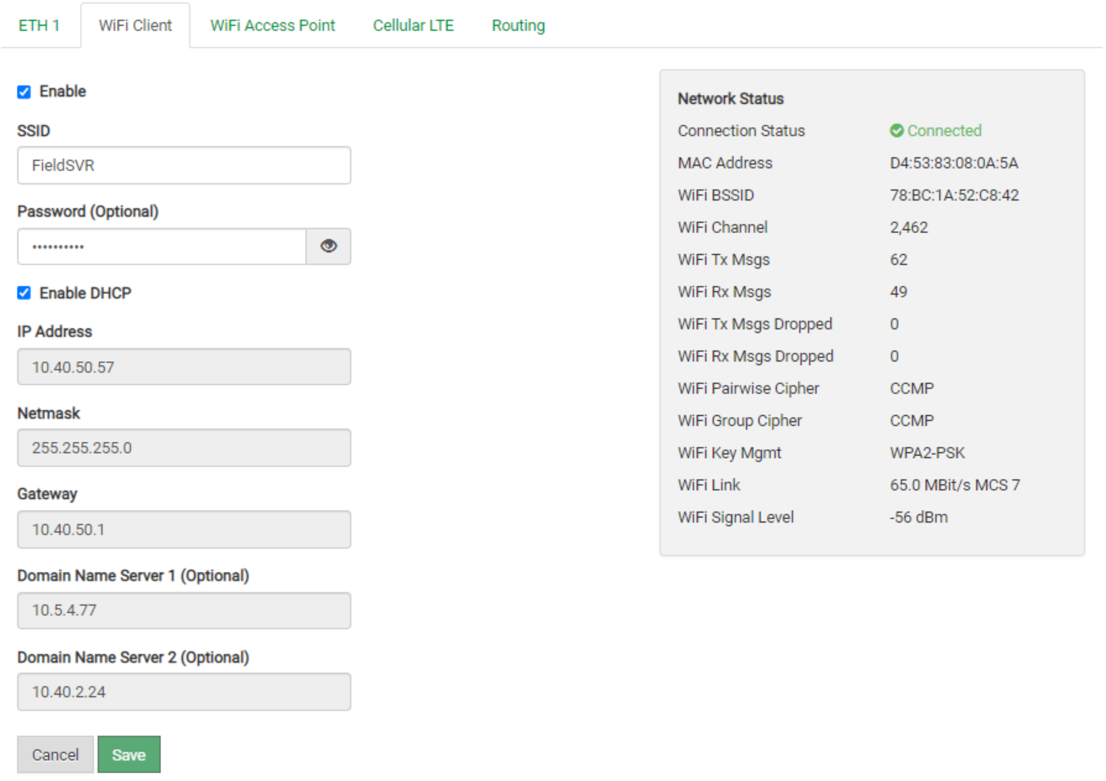
IP Setting Fields	Definition
Connection Status	Status of connection
MAC Address	Ethernet MAC Address
Tx/Rx Msgs	Number of transmitted and received messages
Tx/Rx Msgs Dropped	Number of unanswered Tx or Rx messages

7.1.2 Wi-Fi Client

- Set the Wi-Fi Status to ENABLED for the ProtoAir 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 Router settings (**Section 7.1.4**) to set the default connection to Wi-Fi Client.



☑ Enable

SSID: FieldSVR

Password (Optional): ••••••••••

☑ Enable DHCP

IP Address: 10.40.50.57

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	D4:53:83:08:0A:5A
WiFi BSSID	78:BC:1A:52:C8:42
WiFi Channel	2,462
WiFi Tx Msgs	62
WiFi Rx Msgs	49
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	65.0 MBit/s MCS 7
WiFi Signal Level	-56 dBm

Figure 25: Wi-Fi Client Network Settings

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 14.8**)

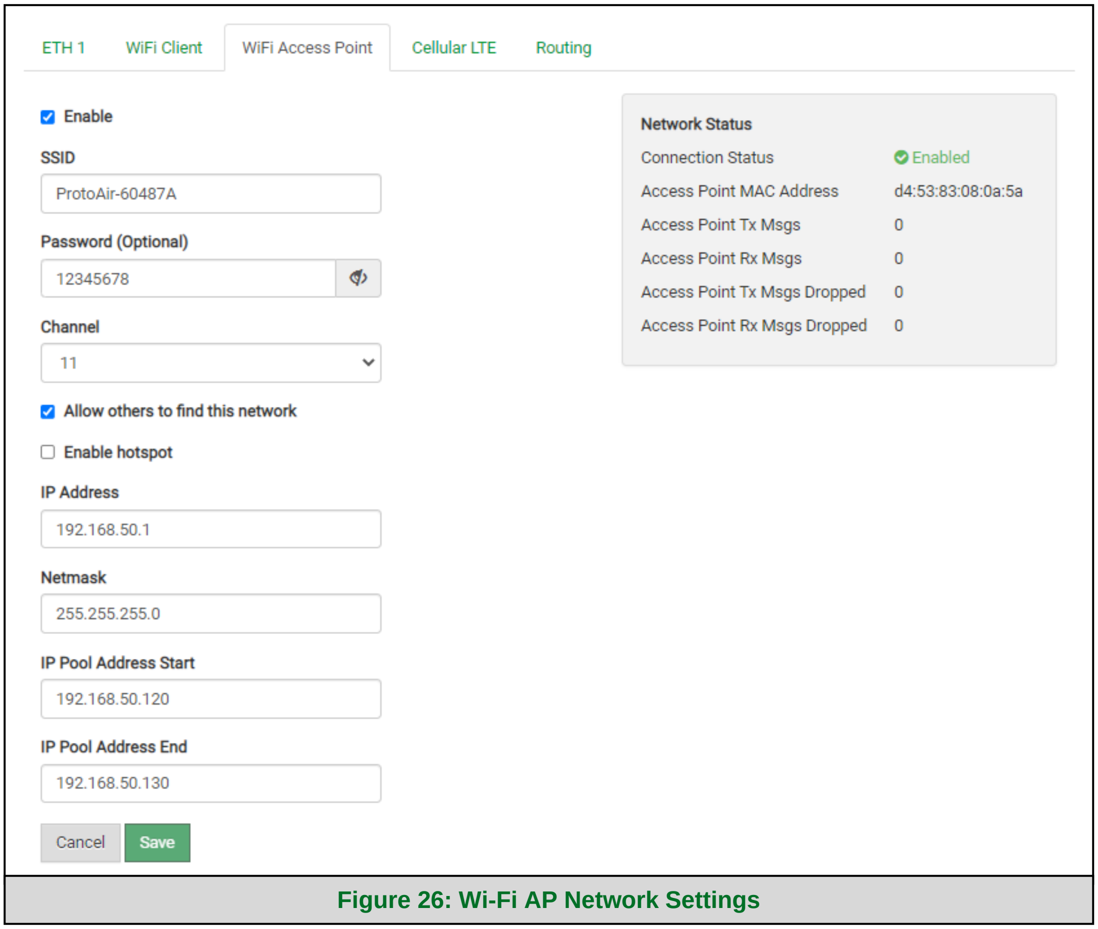
7.1.3 Wi-Fi Access Point

- Check the Enable tick box to allow connecting to the ProtoAir 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.

- 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-60487A

Password (Optional): 12345678

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	✓ Enabled
Access Point MAC Address	d4:53:83:08:0a:5a
Access Point Tx Msgs	0
Access Point Rx Msgs	0
Access Point Tx Msgs Dropped	0
Access Point Rx Msgs Dropped	0

Figure 26: Wi-Fi AP Network Settings

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

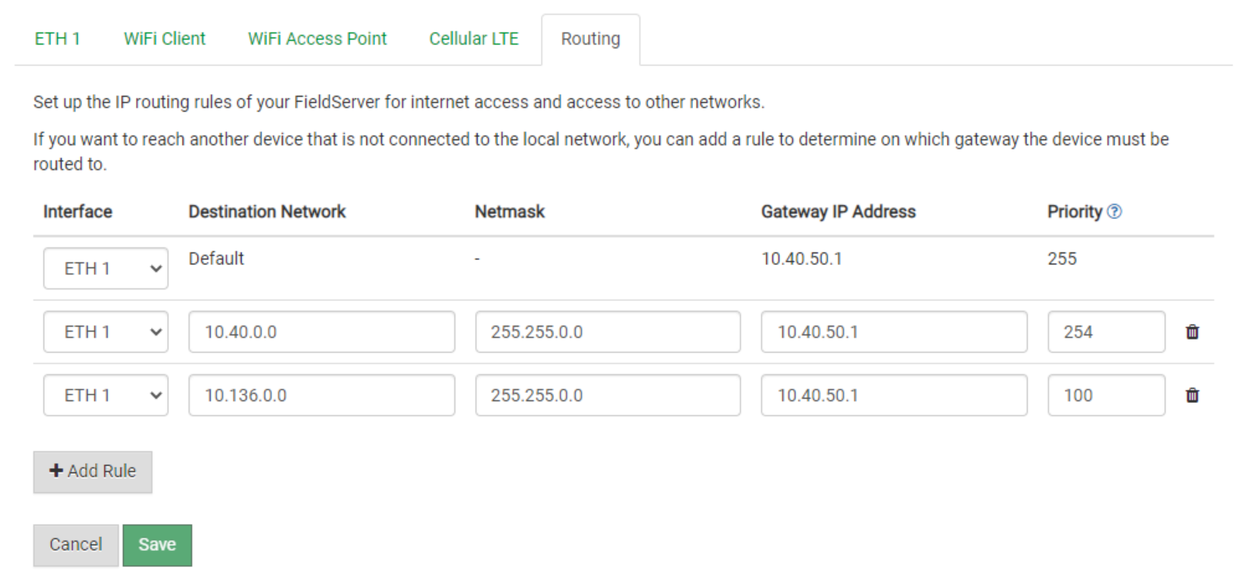
7.1.4 Routing

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.

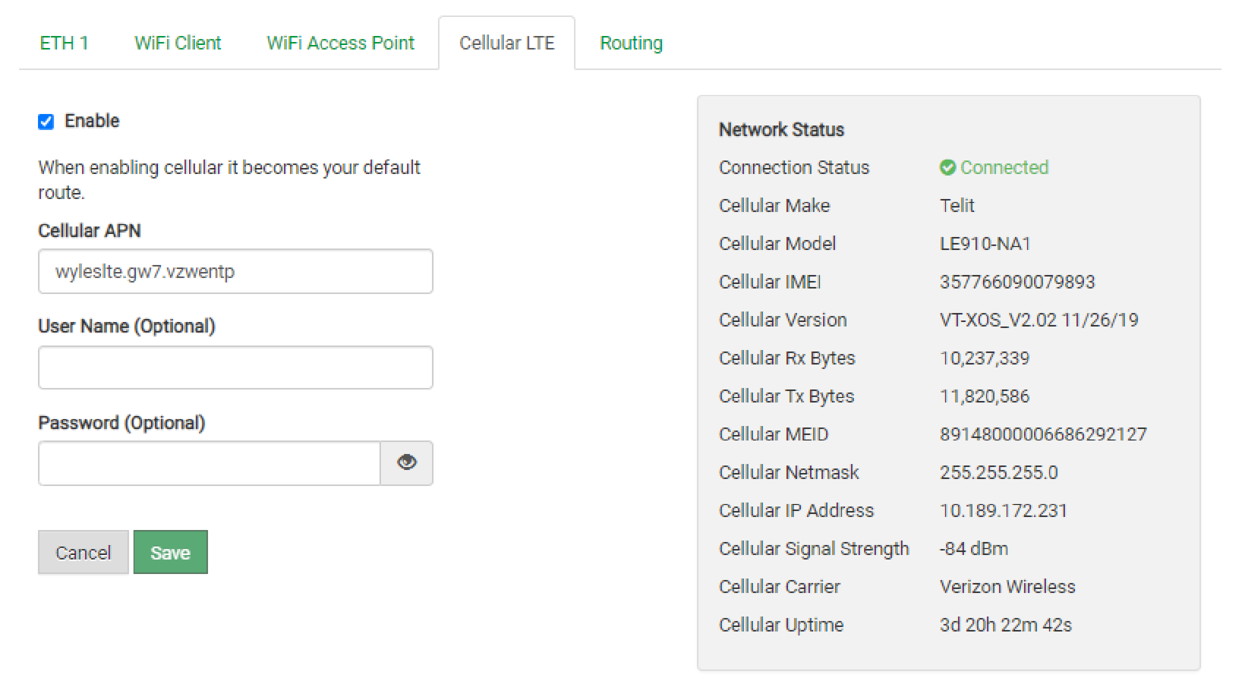
Interface	Destination Network	Netmask	Gateway IP Address	Priority
ETH 1	Default	-	10.40.50.1	255
ETH 1	10.40.0.0	255.255.0.0	10.40.50.1	254
ETH 1	10.136.0.0	255.255.0.0	10.40.50.1	100

Figure 27: Routing Network Settings

7.1.5 FS-IOT-BACA/V/F: Cellular LTE

To change the Cellular settings, follow these instructions:

- Check the Enable tick box to allow connecting to the ProtoAir through the Grid.
- Modify the Settings manually as needed, via these fields: Cellular APN (see **Section 14.11**), User Name, and Password.
- Click the Save button to activate the new settings.



☑ Enable

When enabling cellular it becomes your default route.

Cellular APN: wyleslte.gw7.vzwentp

User Name (Optional):

Password (Optional):

Network Status

Connection Status	✓ Connected
Cellular Make	Telit
Cellular Model	LE910-NA1
Cellular IMEI	357766090079893
Cellular Version	VT-XOS_V2.02 11/26/19
Cellular Rx Bytes	10,237,339
Cellular Tx Bytes	11,820,586
Cellular MEID	89148000006686292127
Cellular Netmask	255.255.255.0
Cellular IP Address	10.189.172.231
Cellular Signal Strength	-84 dBm
Cellular Carrier	Verizon Wireless
Cellular Uptime	3d 20h 22m 42s

Figure 28: Cellular Network Settings

Cellular Fields	Definition
Connection Status	Status of connection
Uptime	Length of time connected
Signal Strength	Strength of signal in dBm (see 14.8)
Signal Type	Type of Signal
Tx/Rx Bytes	Receive and transmit bytes
MEID	Mobile Equipment ID; unique id for a device
Carrier	Cellular carrier provider
IP Address/Netmask	IP Address and Netmask of the cellular connection
Make/Model/Version	Vendor, model and software version of the internal cellular chip

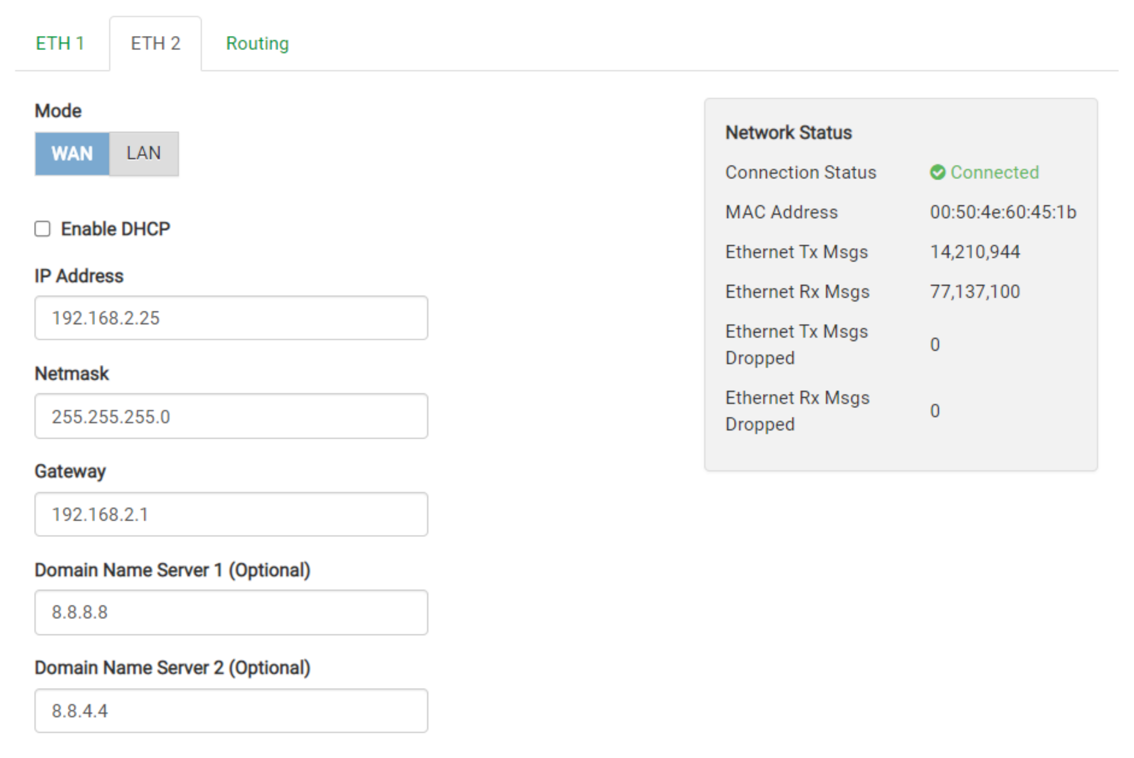
7.1.6 FS-IOT-BAC2E: Ethernet 2 Network Settings – LAN Mode

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

- Scroll down to the bottom of the page and click the Save button to activate the new settings.

NOTE: If the webpage was open in a browser, the browser will need to be pointed to the new IP Address 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

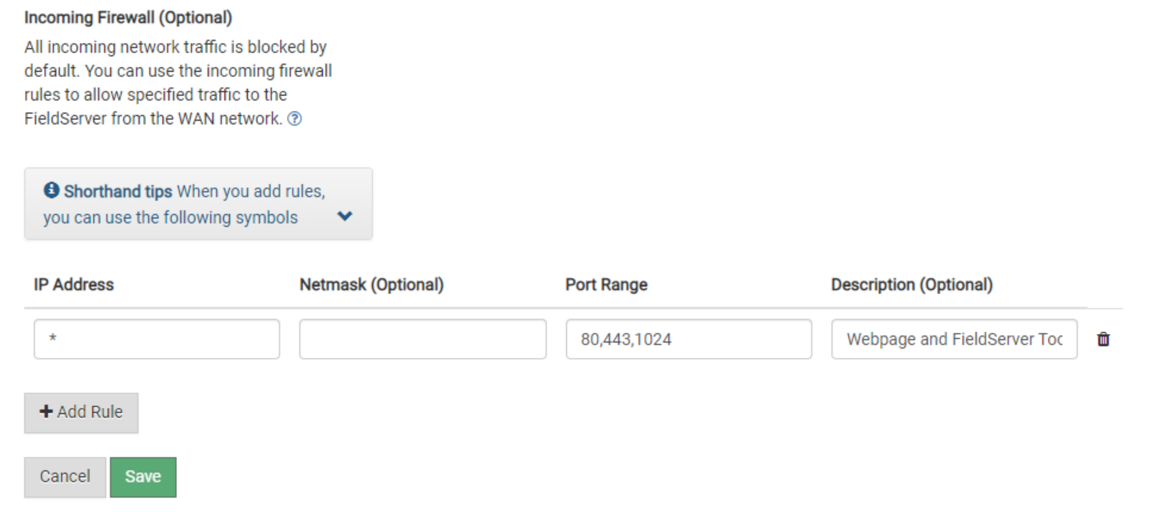
Network Status

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

Figure 29: Ethernet 2 Port Network Settings

7.1.7 FS-IOT-BAC2E: Ethernet 2 Network Settings – WAN Mode

- Click the WAN box to change the ETH 2 port to WAN mode.
  - This prevents all incoming traffic on the ETH 2 port but it allows a connection to the internet via port 80 & 443
- Scroll below the network settings to get to the firewall options with rules that allow specific incoming traffic (through setting rules) and outgoing options.



Incoming Firewall (Optional)

All incoming network traffic is blocked by default. You can use the incoming firewall rules to allow specified traffic to the FieldServer from the WAN network.

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

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

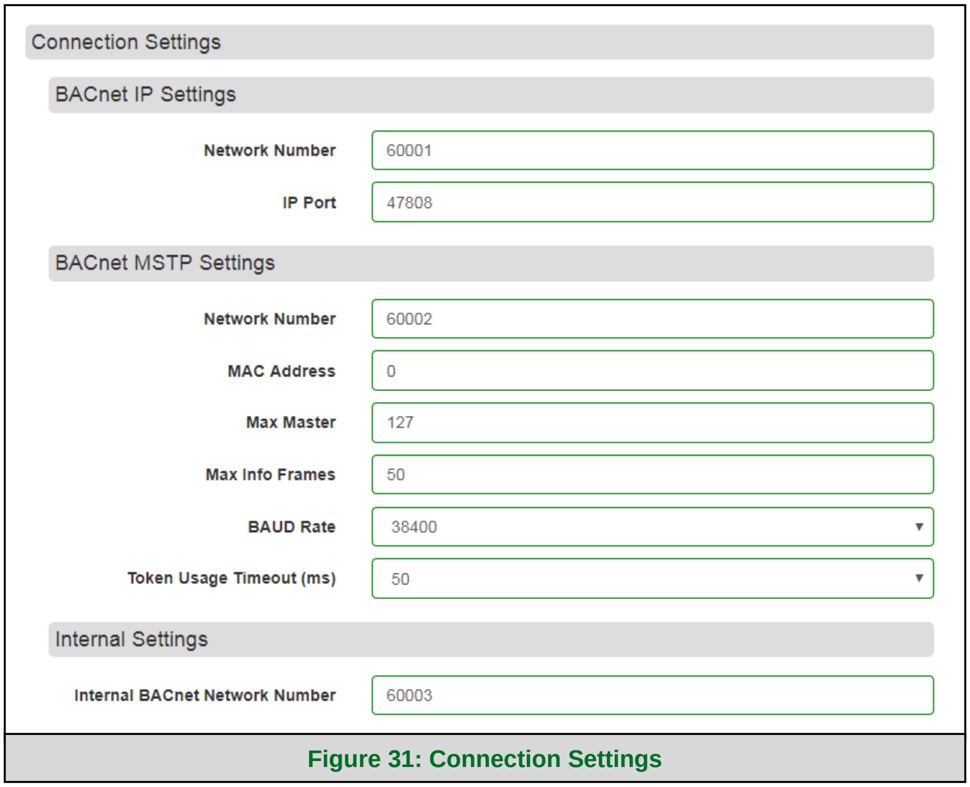
Figure 30: Ethernet 2 Port Firewall Settings

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.

7.2 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

Figure 31: Connection Settings

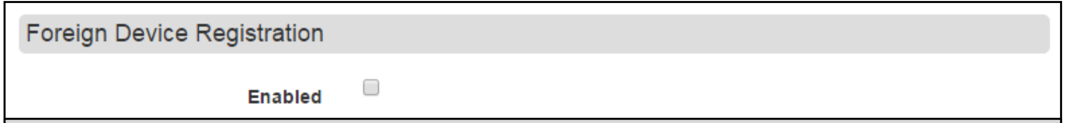
Parameter	Definition
All Connections	
Network Number	The BACnet network number for the connection. Legal values are 1-65534. Each network number must be unique across the entire BACnet internetwork. The **Internal Network Number** is used for internal BACnet traffic and has to be unique across the BACnet 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	The number of 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)	The number of milliseconds the router will wait 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.

Figure 32: Connection Parameters

7.3 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.

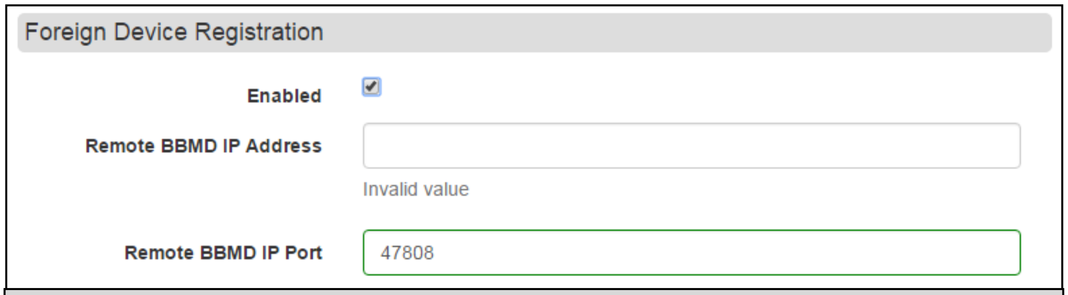


Foreign Device Registration

Enabled □

Figure 33: FDR Enabled Checkbox

- 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

Figure 34: FDR IP Fields

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

NOTE: See Section 13 for additional details concerning FDR and BBMD.

8 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.

8.1 BACnet Explorer

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

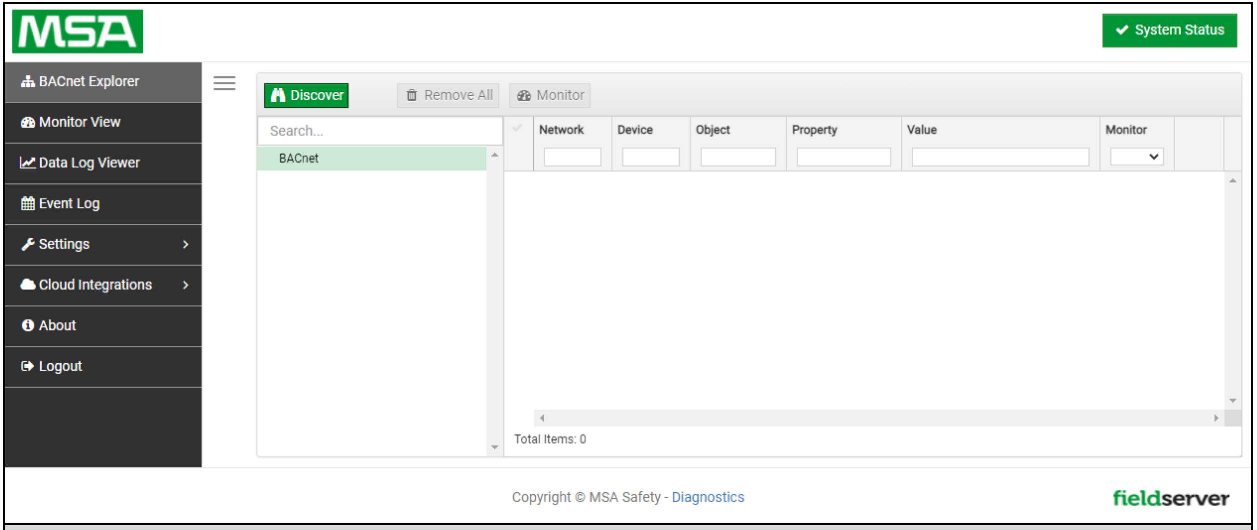
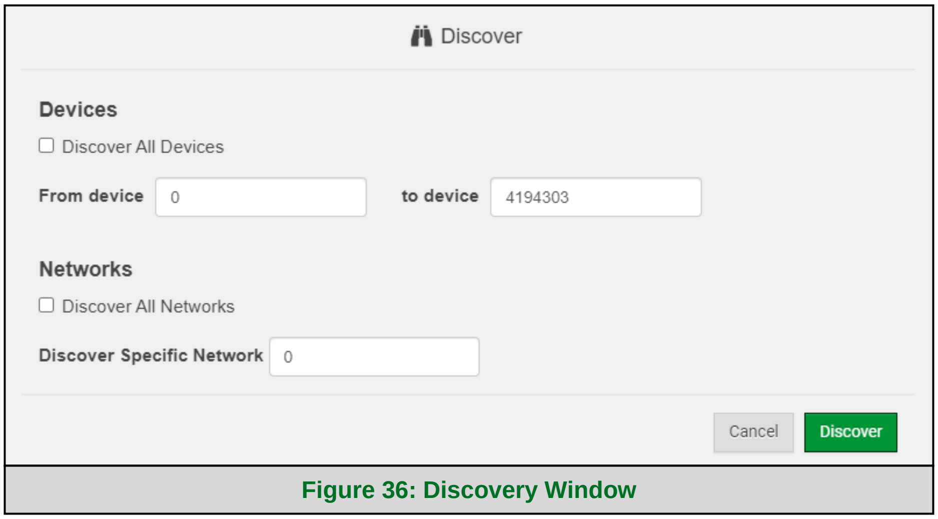


Figure 35: BACnet Explorer Page

8.1.1 Discover the Device List

- To discover the devices connected to the same subnet as the BACnet IoT Gateway, click the Discover button Discover (binocular icon).
- This will open the Discovery window, click the checkboxes next to the desired discovery settings and click Discover to start the search.



Discover

Devices

□ Discover All Devices

From device 0 to device 4194303

Networks

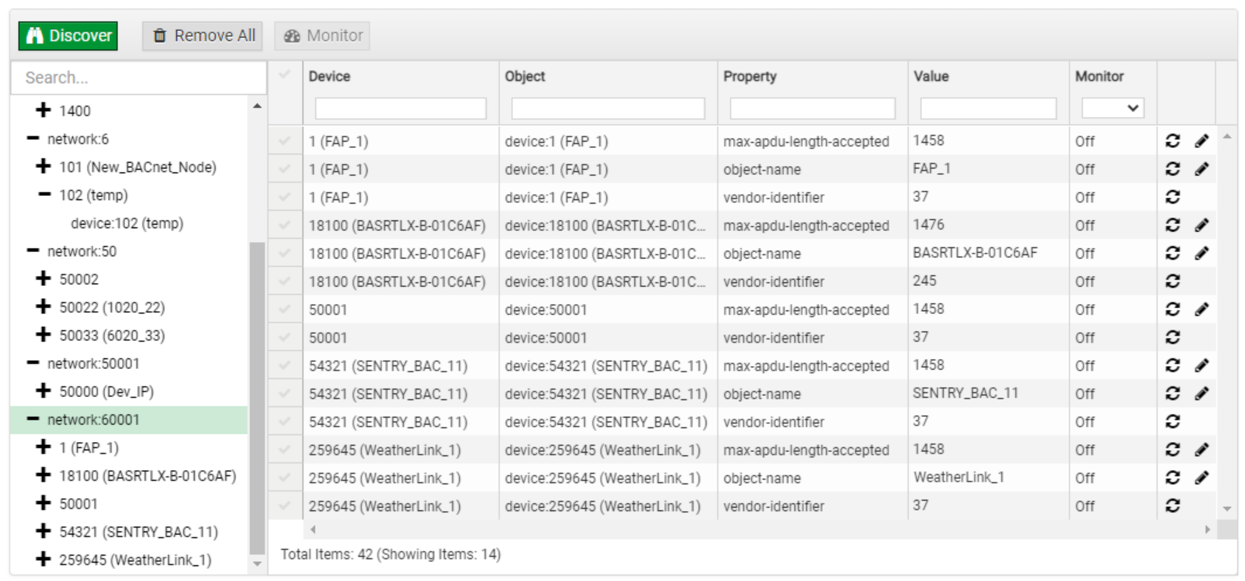
□ Discover All Networks

Discover Specific Network 0

Figure 36: Discovery Window

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.



- + 1400
- − network:6
  - + 101 (New_BACnet_Node)
  - − 102 (temp)
    - device:102 (temp)
- − network:50
  - + 50002
  - + 50022 (1020_22)
  - + 50033 (6020_33)
- − network:50001
  - + 50000 (Dev_IP)
- − network:60001
  - + 1 (FAP_1)
  - + 18100 (BASRTLX-B-01C6AF)
  - + 50001
  - + 54321 (SENTRY_BAC_11)
  - + 259645 (WeatherLink_1)

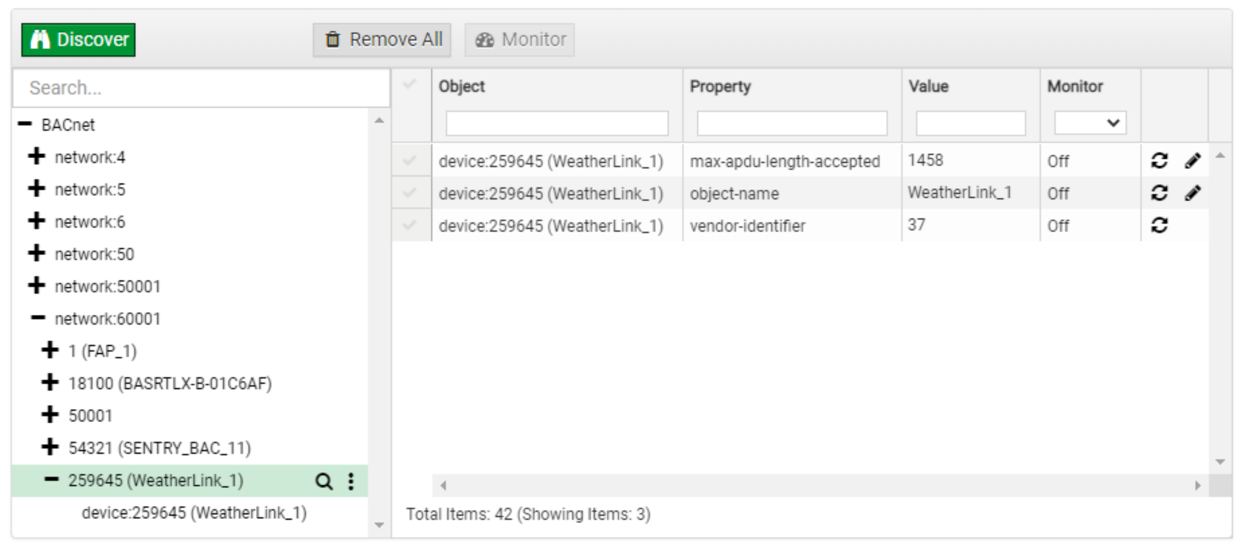
Device	Object	Property	Value	Monitor
1 (FAP_1)	device:1 (FAP_1)	max-apdu-length-accepted	1458	Off
1 (FAP_1)	device:1 (FAP_1)	object-name	FAP_1	Off
1 (FAP_1)	device:1 (FAP_1)	vendor-identifier	37	Off
18100 (BASRTLX-B-01C6AF)	device:18100 (BASRTLX-B-01C...	max-apdu-length-accepted	1476	Off
18100 (BASRTLX-B-01C6AF)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

Figure 37: Device List

8.1.2 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



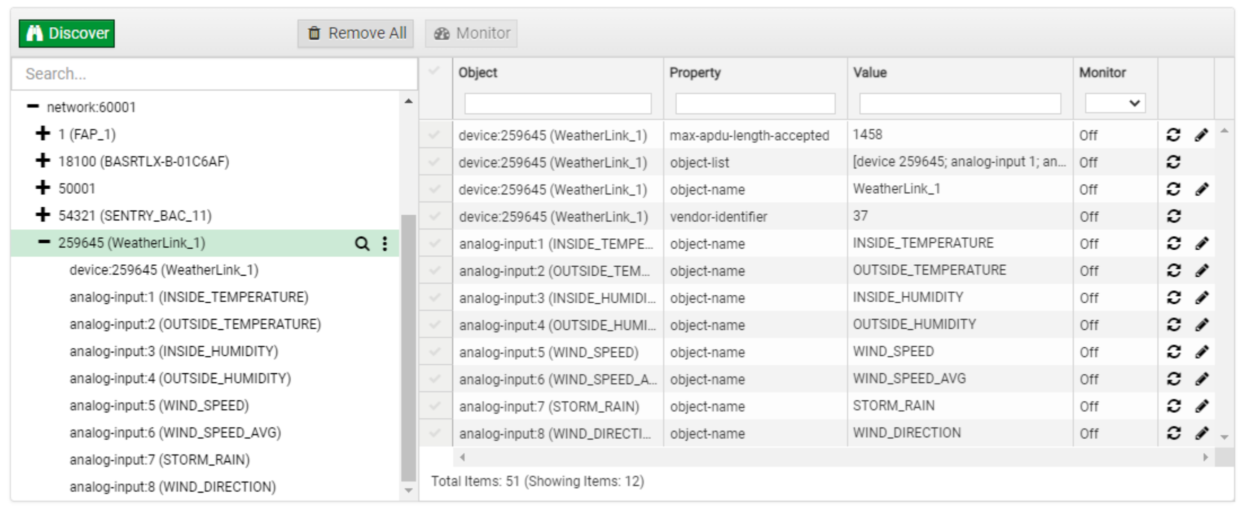
− BACnet
✚ network:4
✚ network:5
✚ network:6
✚ network:50
✚ network:50001
− network:60001
✚ 1 (FAP_1)
✚ 18100 (BASRTLX-B-01C6AF)
✚ 50001
✚ 54321 (SENTRY_BAC_11)
− 259645 (WeatherLink_1)
device:259645 (WeatherLink_1)

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)

Figure 38: Device Sub-items

- 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)

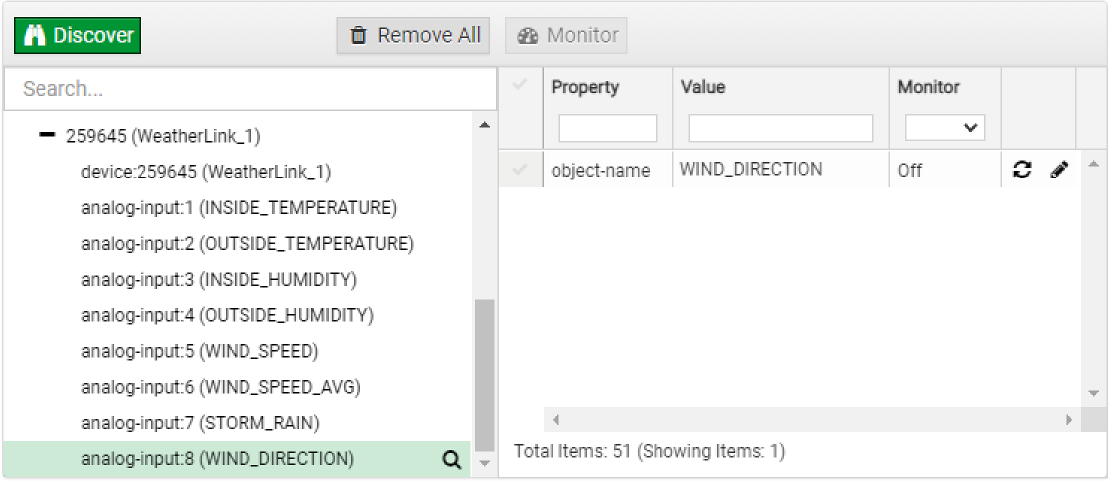
Object	Property	Value	Monitor
device:259645 (WeatherLink_1)	max-apdu-length-accepted	1458	Off
device:259645 (WeatherLink_1)	object-list	[device 259645; analog-input 1; an...	Off
device:259645 (WeatherLink_1)	object-name	WeatherLink_1	Off
device:259645 (WeatherLink_1)	vendor-identifier	37	Off
analog-input:1 (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)

Figure 39: Full Device Sub-items

  - Now additional device details are viewable; however, the device can be explored even further

- Click on one of the device details.

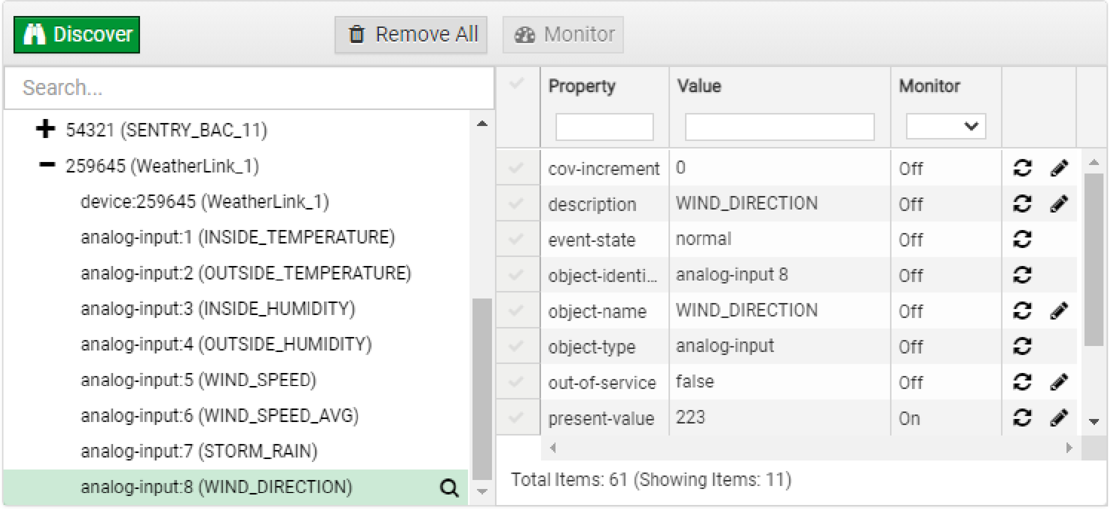

Discover
Remove All
Monitor
Search...
259645 (WeatherLink_1)
device:259645 (WeatherLink_1)
analog-input:1 (INSIDE_TEMPERATURE)
analog-input:2 (OUTSIDE_TEMPERATURE)
analog-input:3 (INSIDE_HUMIDITY)
analog-input:4 (OUTSIDE_HUMIDITY)
analog-input:5 (WIND_SPEED)
analog-input:6 (WIND_SPEED_AVG)
analog-input:7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

Property	Value	Monitor
object-name	WIND_DIRECTION	Off

Total Items: 51 (Showing Items: 1)

Figure 40: Simplified Device Details

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


Discover
Remove All
Monitor
Search...
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)

Figure 41: Additional Device Details

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

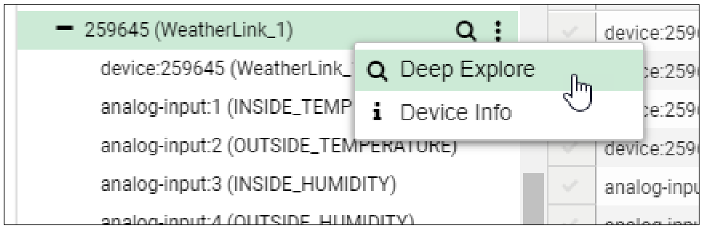
NOTE: The Gateway Search Bar will find devices based on their Device ID.

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

- **Network number**
  - **Device**
    - **Device object**

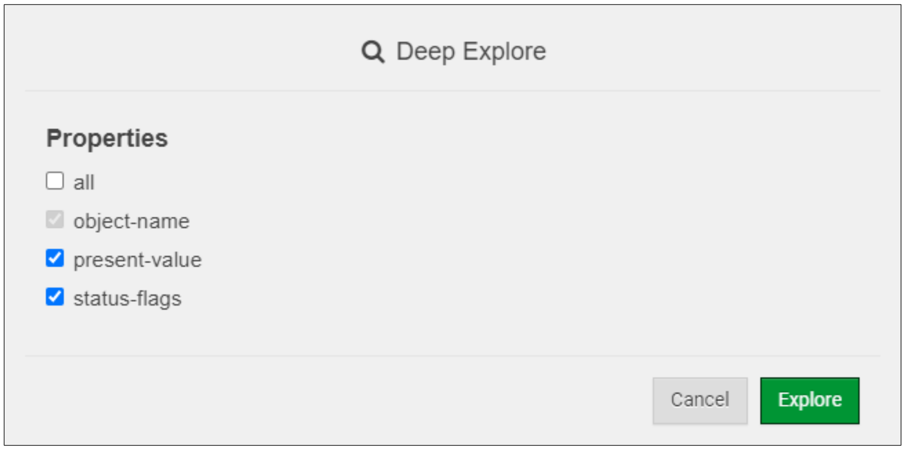
8.1.3 Explore All of a Device's Points – Deep Explore

- 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.



Deep Explore

Properties

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

- Select which property types to find in the search.

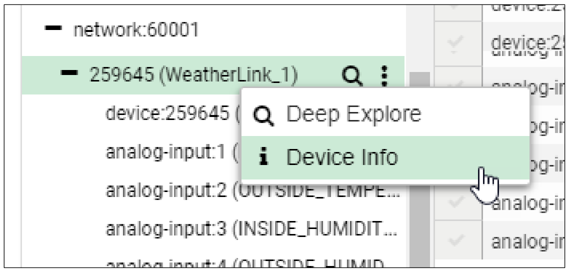
NOTE: The "all" selection must be unchecked to show object-name, present-value and status-flags as options.

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

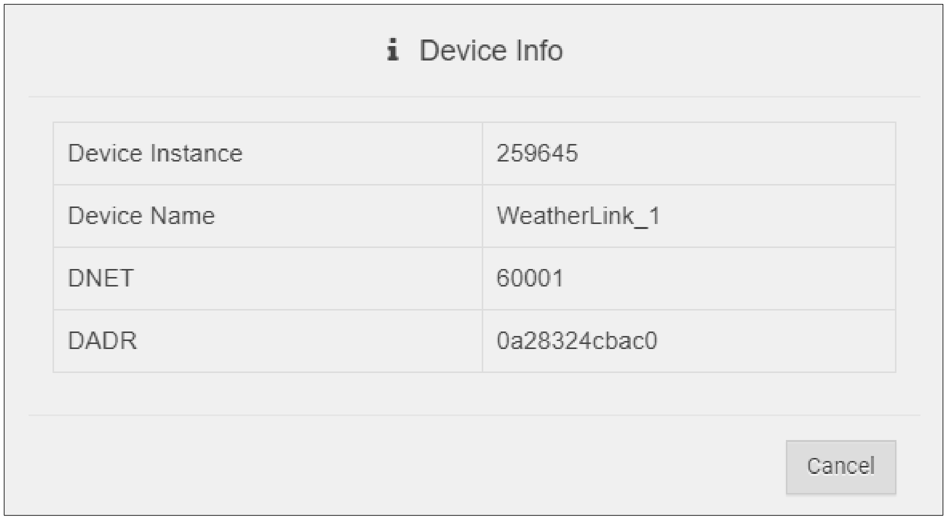
- Click the Explore button and wait for the green explore complete message to confirm all points have been discovered.

8.1.4 Checking Device Information – Device Info

- To check a device’s properties/information, click the desired device to highlight it.
- Then click the three white 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

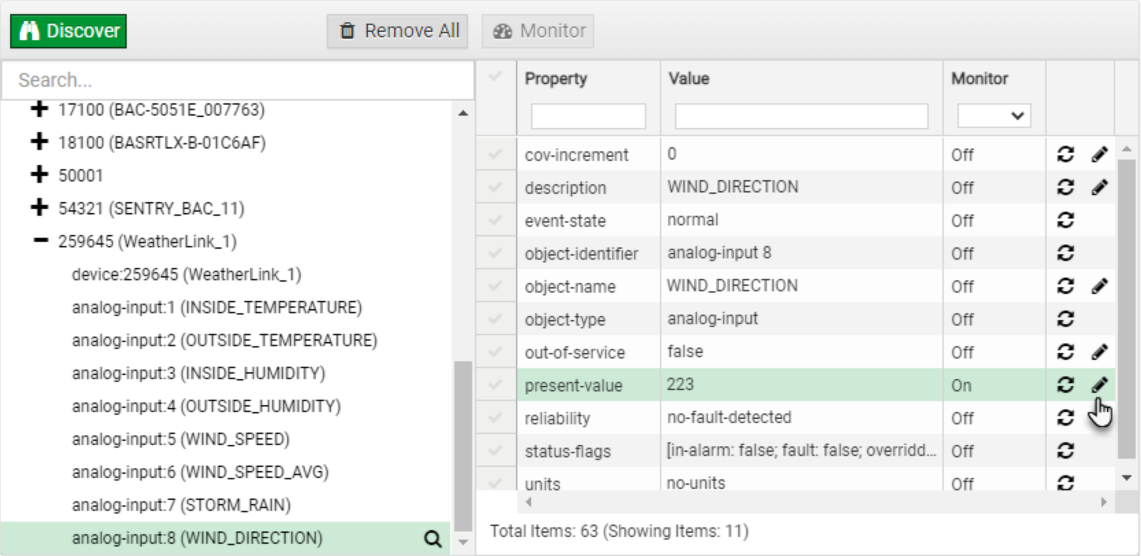
Device Instance	259645
Device Name	WeatherLink_1
DNET	60001
DADR	0a28324cbac0

8.1.5 Edit the Present Value Field

The only recommended field to edit via BACnet IoT Gateway 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 BACnet IoT Gateway is not a Building Management System (BMS).

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



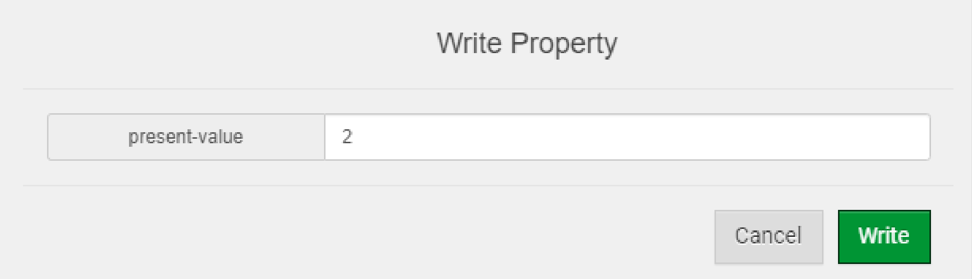
- 17100 (BAC-5051E_007763)
- 18100 (BASRTLX-B-01C6AF)
- 50001
- 54321 (SENTRY_BAC_11)
- 259645 (WeatherLink_1)
  - device:259645 (WeatherLink_1)
  - analog-input:1 (INSIDE_TEMPERATURE)
  - analog-input:2 (OUTSIDE_TEMPERATURE)
  - analog-input:3 (INSIDE_HUMIDITY)
  - analog-input:4 (OUTSIDE_HUMIDITY)
  - 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)

Figure 42: Highlighted Present Value

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

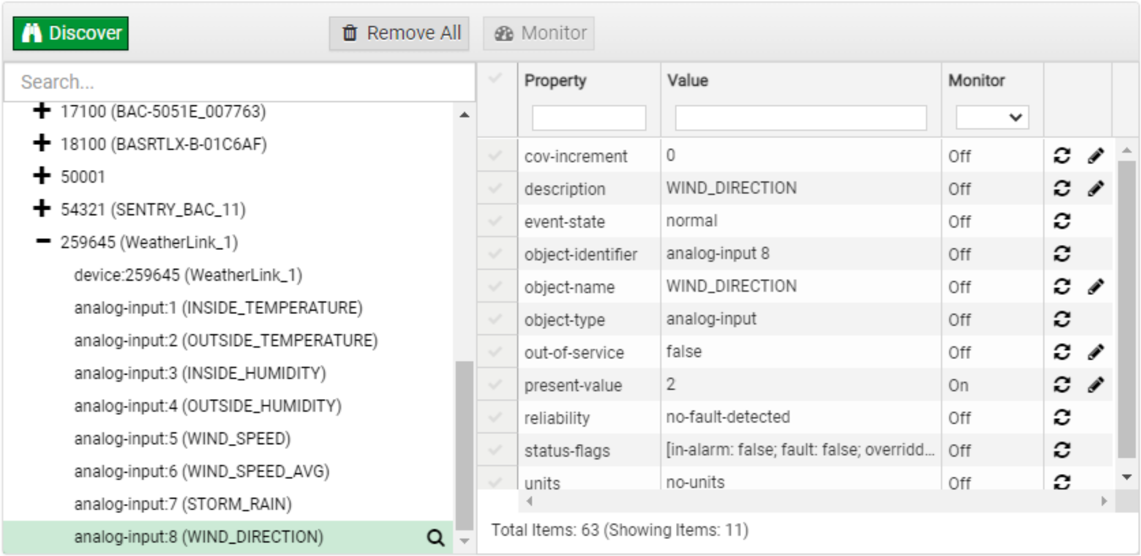

Write Property

present-value	2

Figure 43: Write Property Window

- 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.



- 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	2	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)

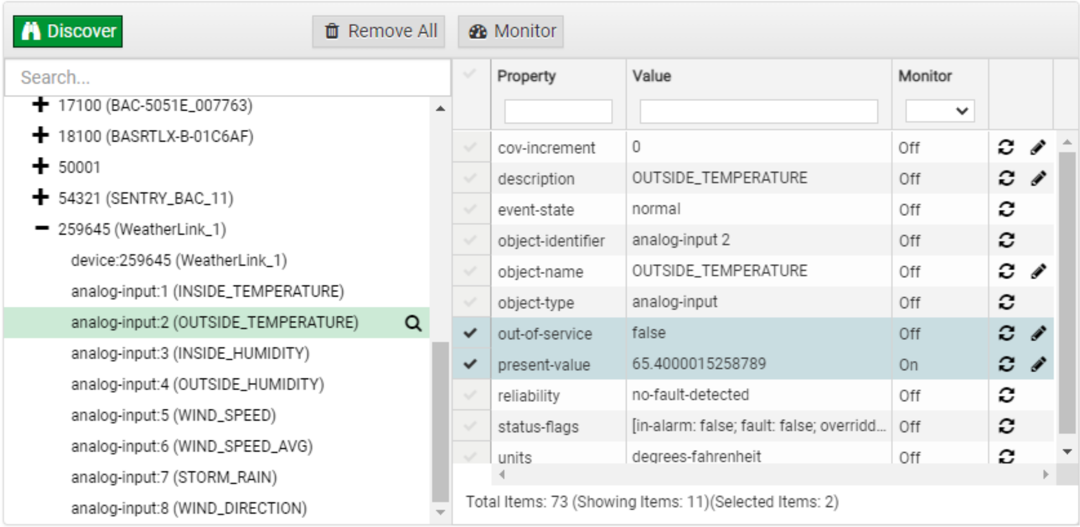
Figure 44: Updated Present Value

8.2 Monitor View

8.2.1 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.


Discover
Remove All
Monitor
Search...
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)

Figure 45: Selected Device Properties for Monitor View

- 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.

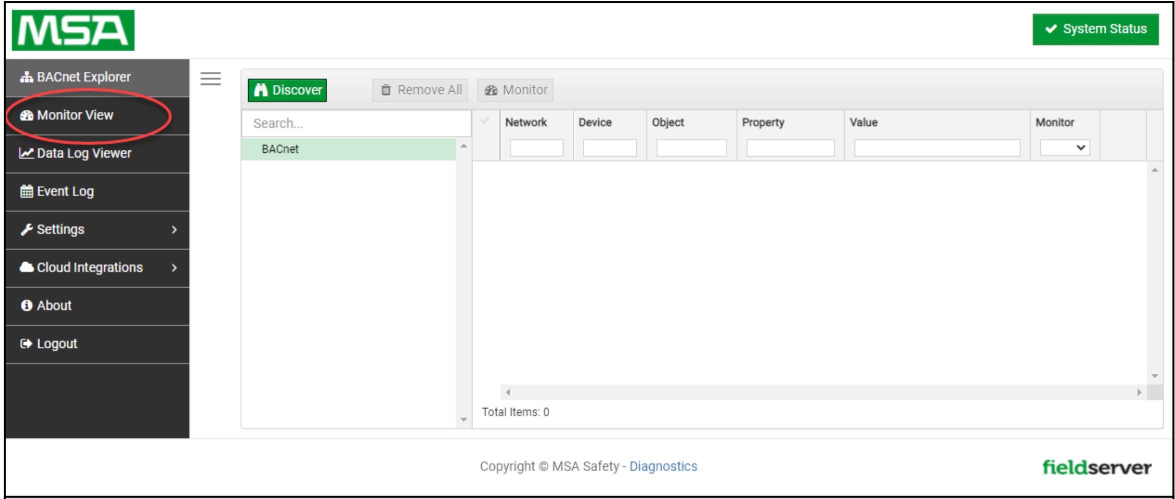
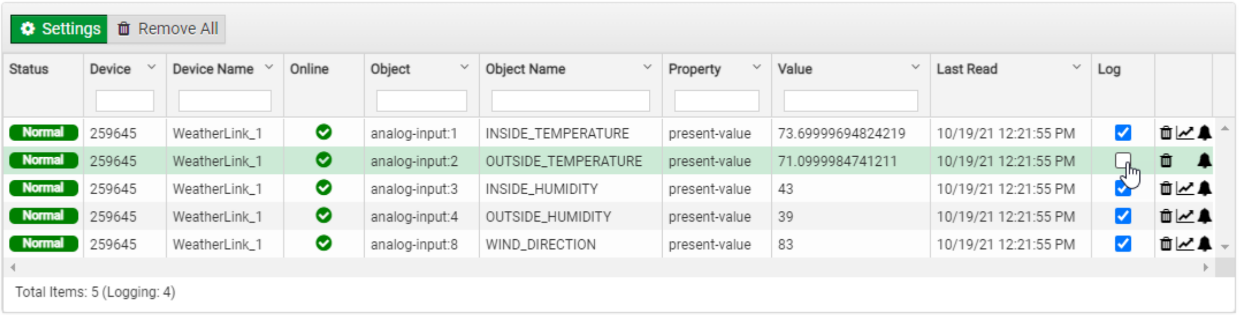


Figure 46: Highlighted Monitor View Tab

8.2.2 Logging Data

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

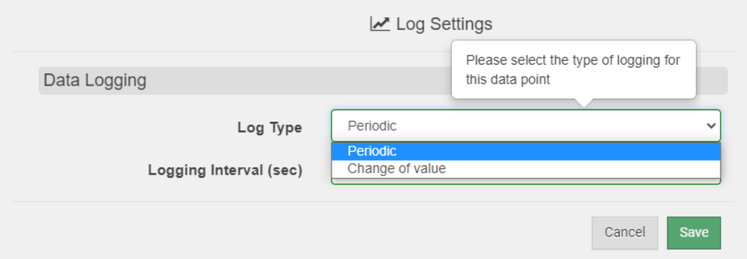


Status	Device	Device Name	Online	Object	Object Name	Property	Value	Last Read	Log
Normal	259645	WeatherLink_1	✓	analog-input:1	INSIDE_TEMPERATURE	present-value	73.69999694824219	10/19/21 12:21:55 PM	☑
Normal	259645	WeatherLink_1	✓	analog-input:2	OUTSIDE_TEMPERATURE	present-value	71.0999984741211	10/19/21 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)

Figure 47: Monitor View Showing Tracked Device Properties

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


Log Settings

Data Logging

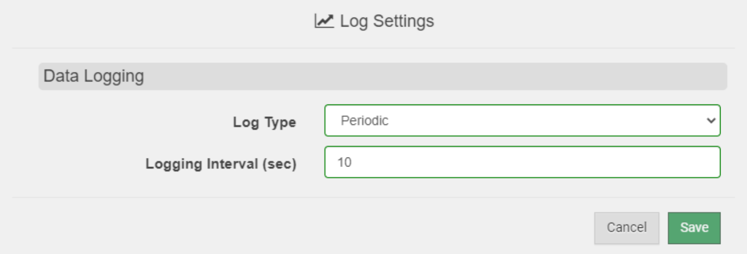
Please select the type of logging for this data point

Log Type: Periodic

Logging Interval (sec)

Figure 48: Data Logging Window

- 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.

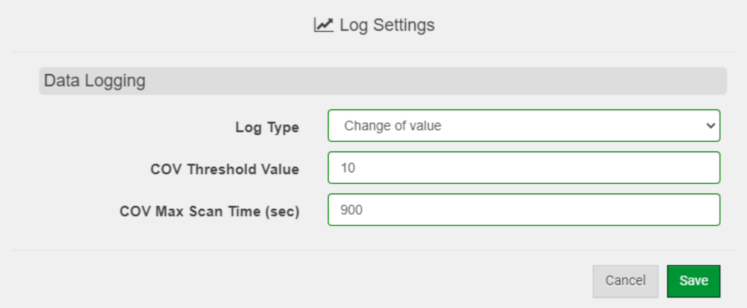

Log Settings

Data Logging

Log Type: Periodic

Logging Interval (sec): 10

Figure 50: Periodic Log Type


Log Settings

Data Logging

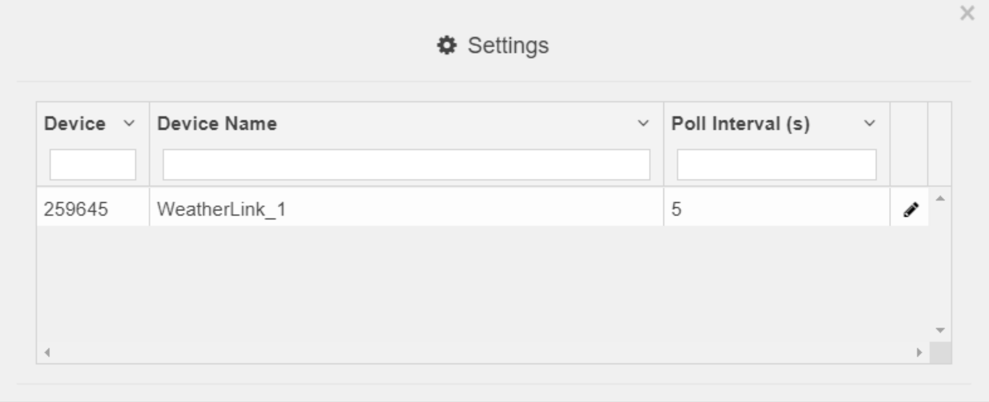
Log Type: Change of value

COV Threshold Value: 10

COV Max Scan Time (sec): 900

Figure 49: Change of Value Log Type

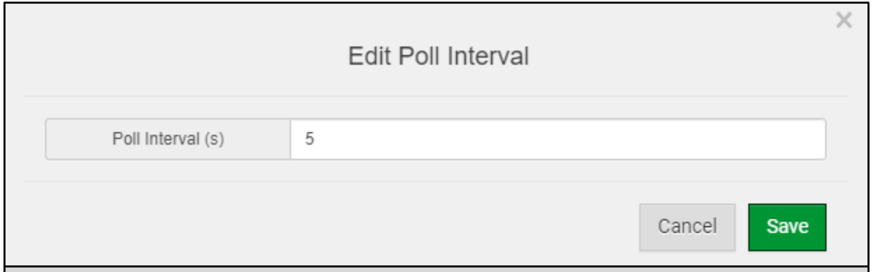
- To change the poll interval of a device, click the Settings button ⚙ Settings (see **Figure 47**) to open the Settings window.



Device	Device Name	Poll Interval (s)
259645	WeatherLink_1	5

Figure 51: Settings Window

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



Poll Interval (s) 5

Figure 52: Edit Poll Interval Window

- Make desired changes and click Save.

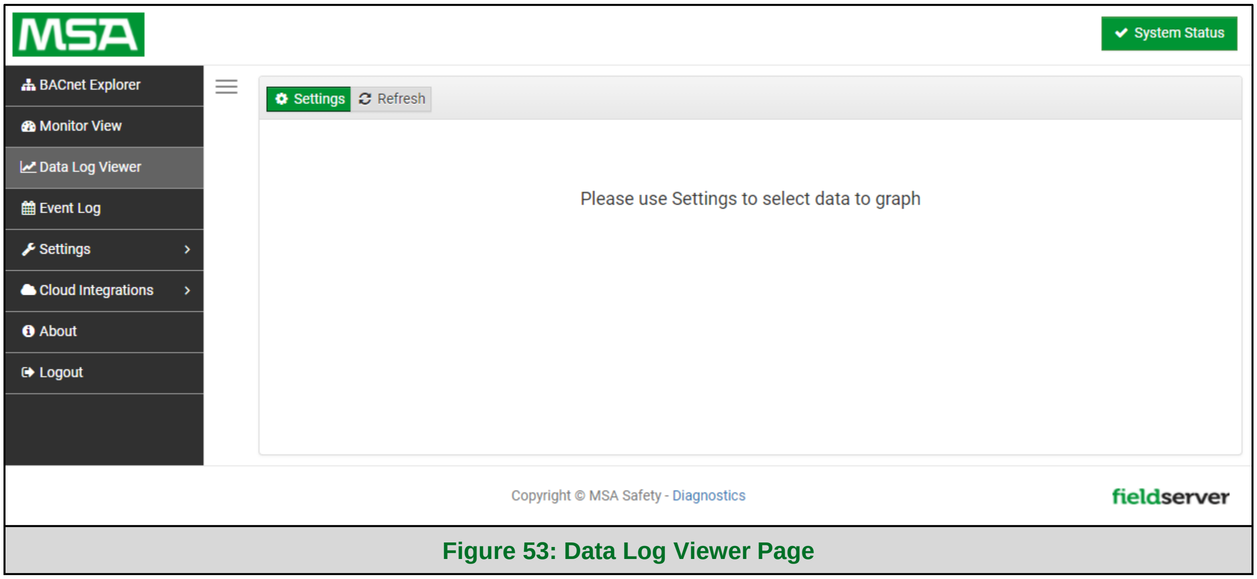
NOTE: Up to 30 days of data can be recorded and stored.

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

8.3 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.

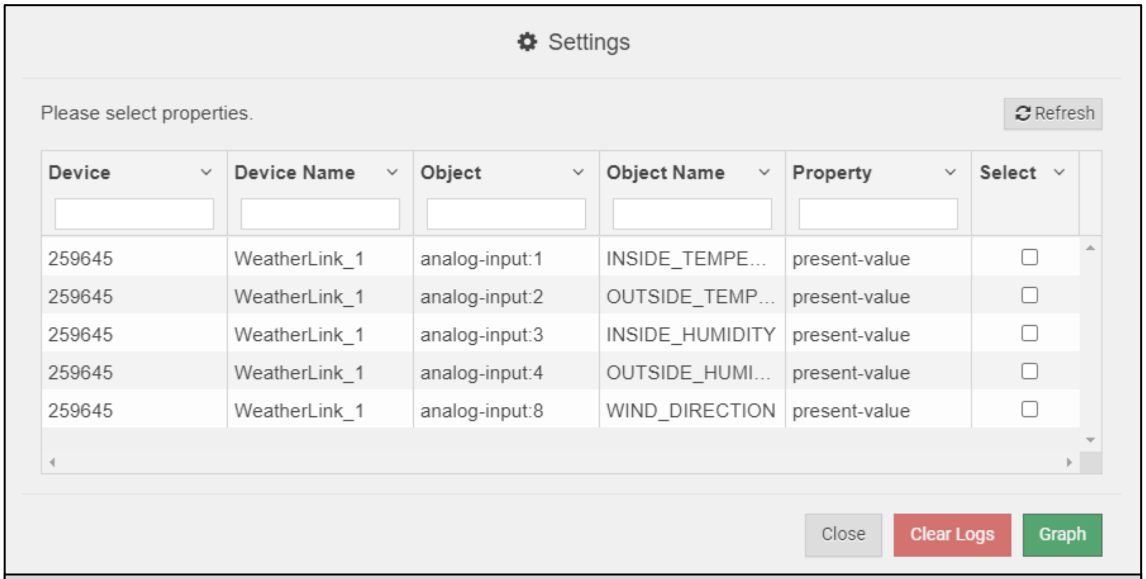


Please use Settings to select data to graph

Figure 53: Data Log Viewer Page

8.3.1 Graph Data Logging Information

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



Please select properties.

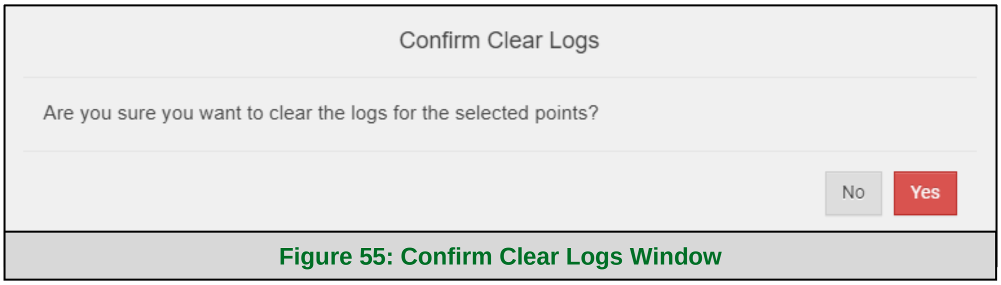
Device	Device Name	Object	Object Name	Property	Select
259645	WeatherLink_1	analog-input:1	INSIDE_TEMPE…	present-value	□
259645	WeatherLink_1	analog-input:2	OUTSIDE_TEMP…	present-value	□
259645	WeatherLink_1	analog-input:3	INSIDE_HUMIDITY	present-value	□
259645	WeatherLink_1	analog-input:4	OUTSIDE_HUMI…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

Figure 54: Data Log Viewer Settings Window

- 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 8.2.

- 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?

Figure 55: Confirm Clear Logs Window

- After a few seconds the graph should appear.

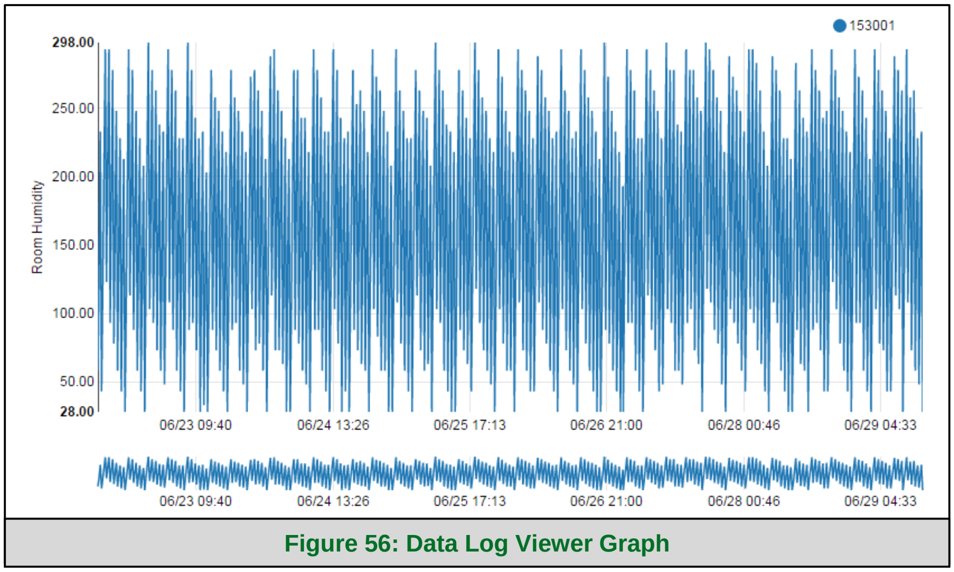
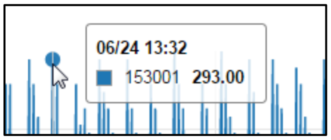
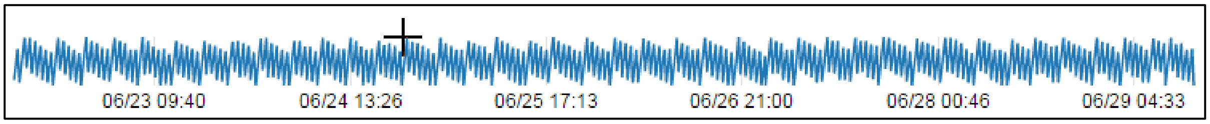


Figure 56: Data Log Viewer Graph

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.

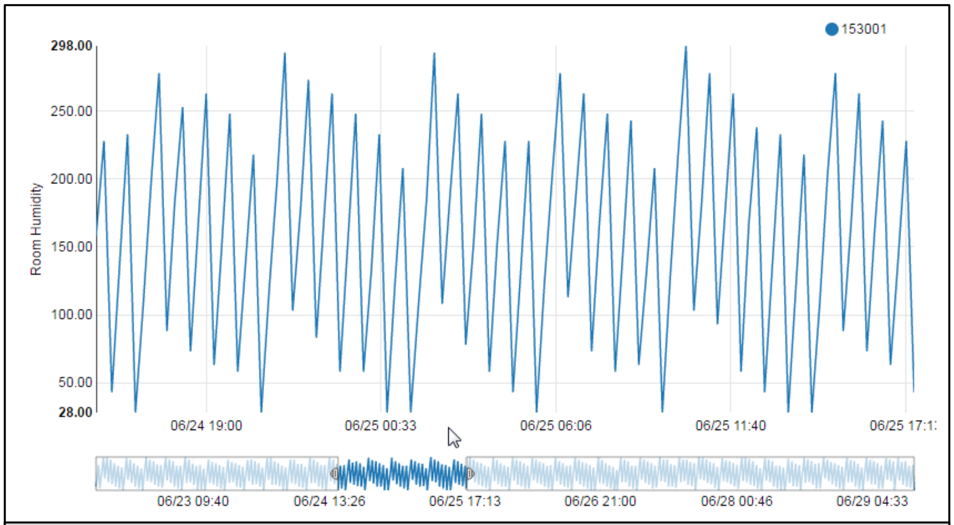
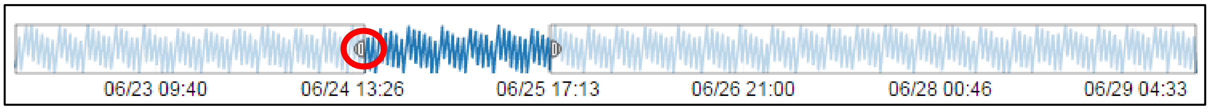


Figure 57: Selected Portion of Data Log Viewer Graph

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.

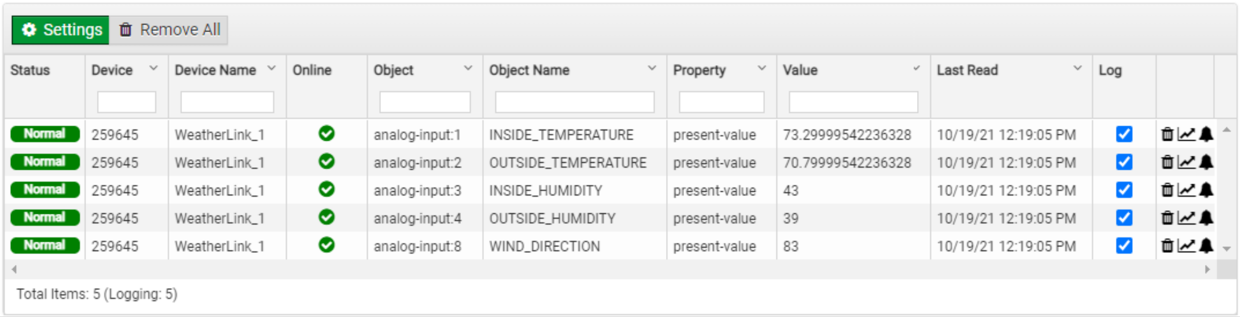


To go back to the full graph, click on any faded portion of the miniature graph.

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.

8.3.2 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.

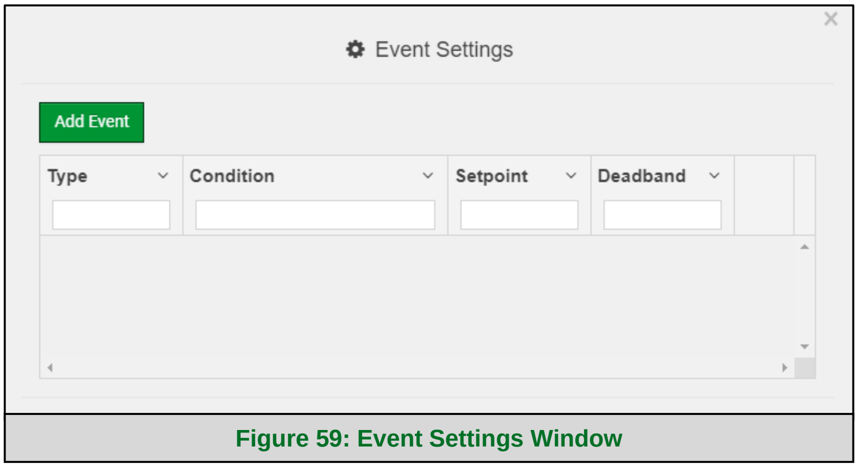


Status	Device	Device Name	Online	Object	Object Name	Property	Value	Last Read	Log	
Normal	259645	WeatherLink_1	✓	analog-input:1	INSIDE_TEMPERATURE	present-value	73.29999542236328	10/19/21 12:19:05 PM	☑	
Normal	259645	WeatherLink_1	✓	analog-input:2	OUTSIDE_TEMPERATURE	present-value	70.79999542236328	10/19/21 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)

Figure 58: Monitor View Device Properties

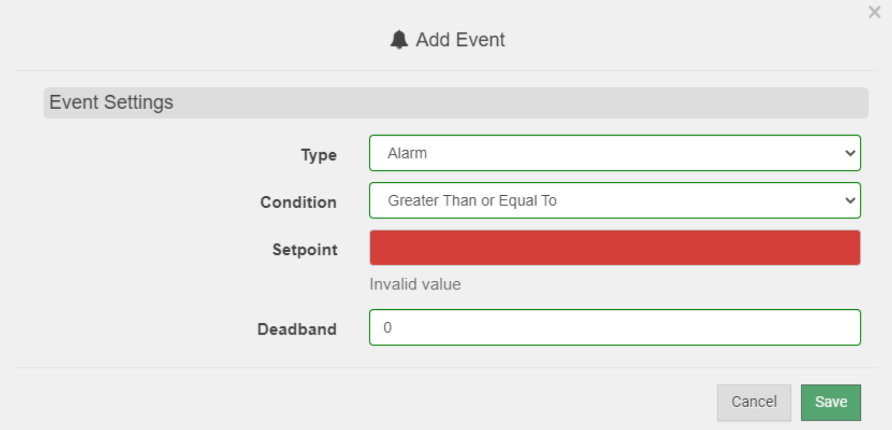
- Click the bell icon (🔔) to the right of the property to log and the Event Settings window will open.



Type	Condition	Setpoint	Deadband

Figure 59: Event Settings Window

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



Type: Alarm

Condition: Greater Than or Equal To

Setpoint:

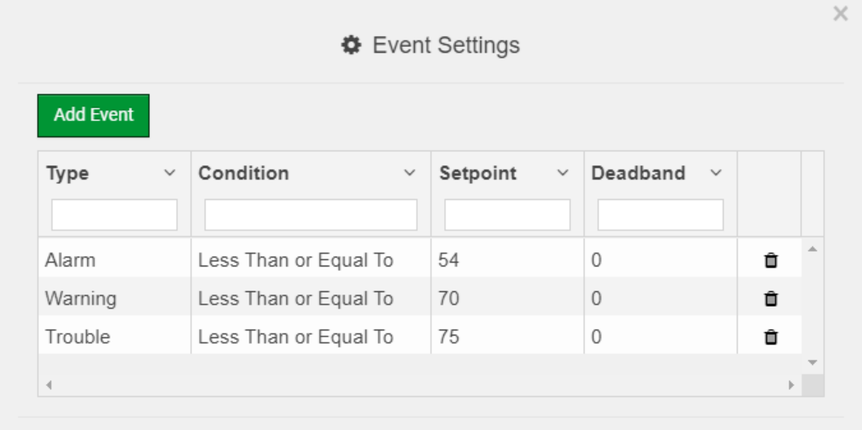
Invalid value

Deadband: 0

Figure 60: Add Event Settings

- Set the event as needed and click Save.

- Repeat this process to create more events as needed.

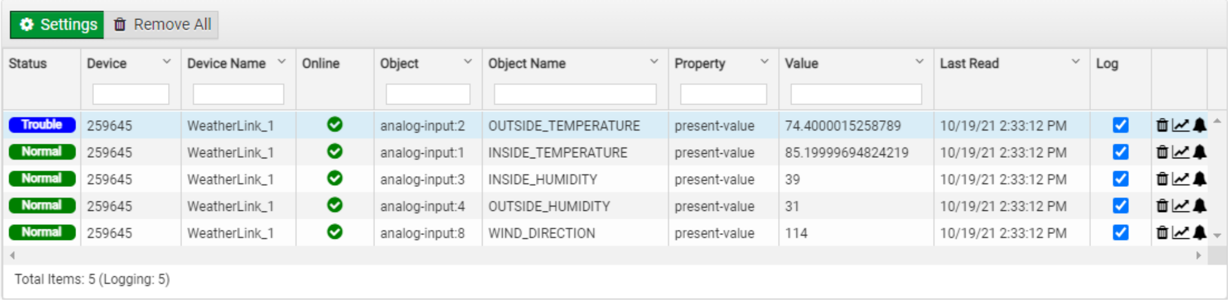


Type	Condition	Setpoint	Deadband	
Alarm	Less Than or Equal To	54	0	🗑
Warning	Less Than or Equal To	70	0	🗑
Trouble	Less Than or Equal To	75	0	🗑

Figure 61: Event Settings Window with Added Events

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

- 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



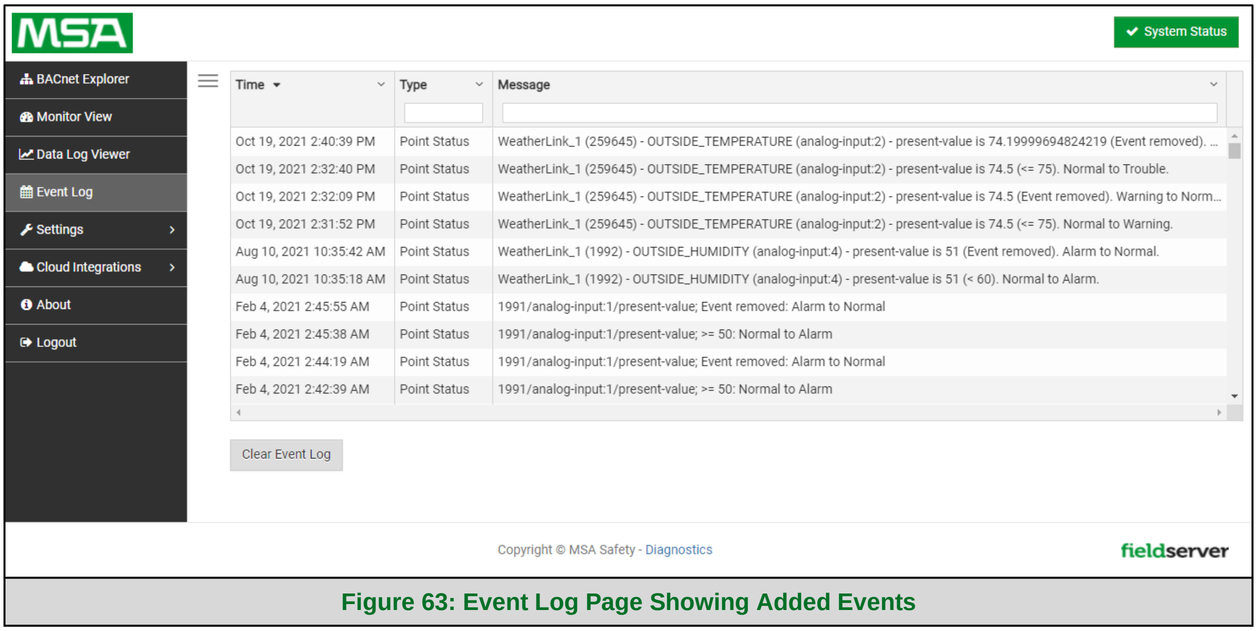
Status	Device	Device Name	Online	Object	Object Name	Property	Value	Last Read	Log	
Trouble	259645	WeatherLink_1	✓	analog-input:2	OUTSIDE_TEMPERATURE	present-value	74.4000015258789	10/19/21 2:33:12 PM	☑	🗑 📈 🔔
Normal	259645	WeatherLink_1	✓	analog-input:1	INSIDE_TEMPERATURE	present-value	85.19999694824219	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)

Figure 62: Monitor View Device Properties with Updated Status

8.4 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** 8.3.2 (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

Figure 63: Event Log Page Showing Added Events

9 FieldServer Manager Setup

The Grid is MSA Safety's device cloud solution for IIoT. Integration with the MSA Grid – FieldServer Manager enables 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 Manger, refer to the MSA Grid - FieldServer Manager Start-up Guide.

9.1 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.

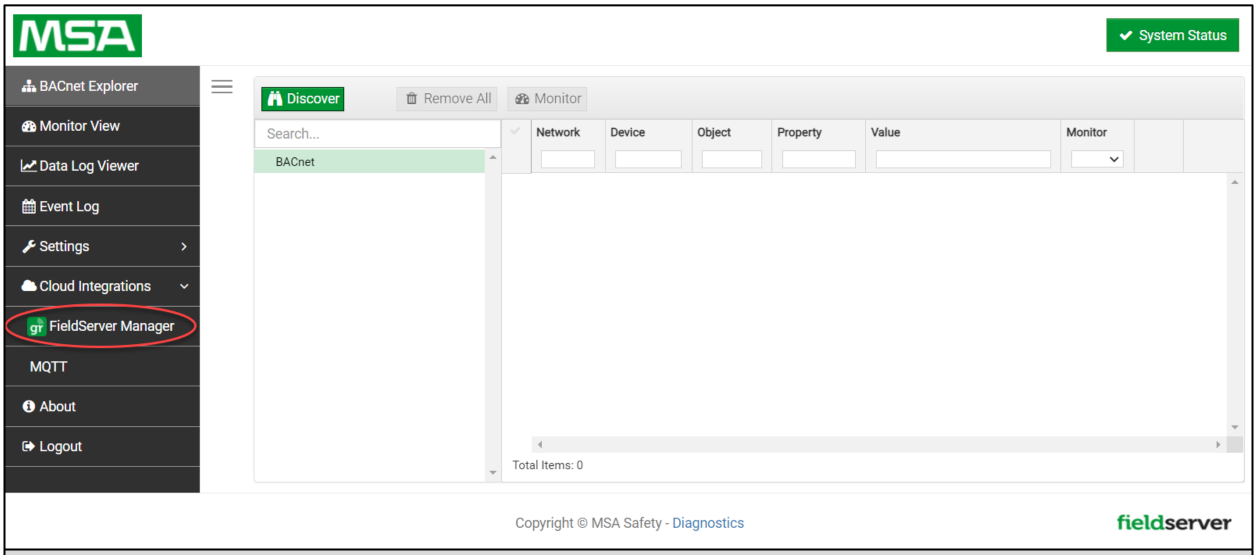
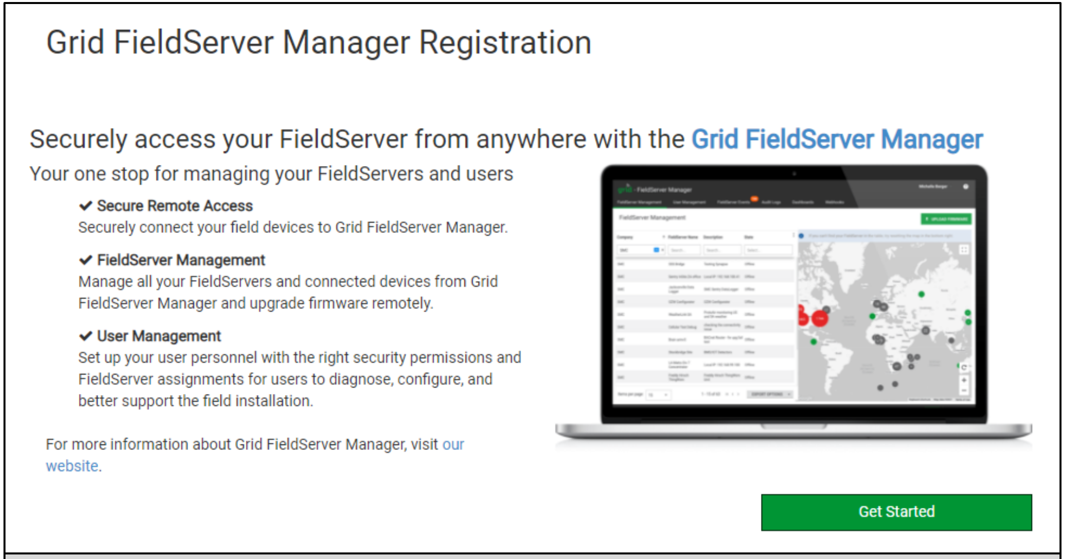


Figure 64: BACnet IoT Gateway Landing Page – FieldServer Manager Tab

- An informational splash page will appear, click the Close button to view the registration page.



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.

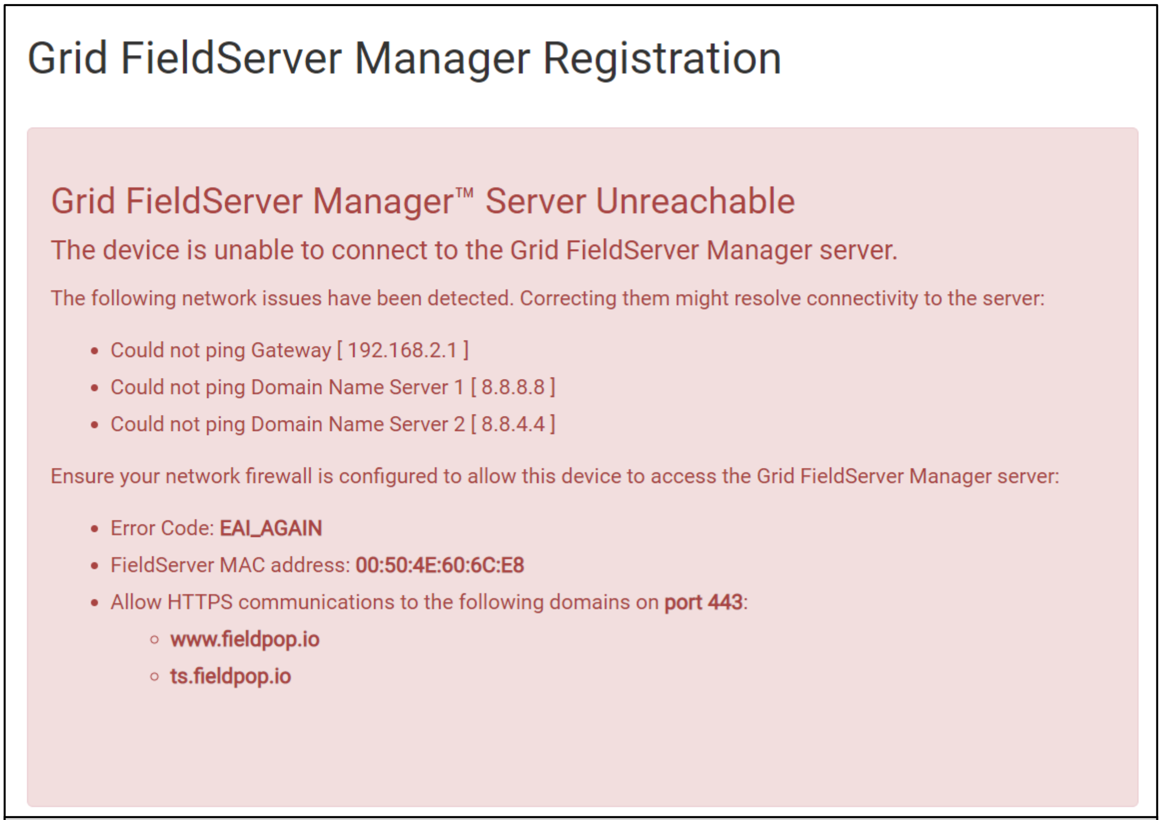
✓ FieldServer Management
Manage all your FieldServers and connected devices from Grid FieldServer Manager and upgrade firmware remotely.

✓ 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.

Figure 65: Registration Information Page

- If a warning message appears instead of the splash page, follow the suggestion that appears on screen.
- If the BACnet IoT Gateway cannot reach the Grid 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**

Figure 66: FieldServer Manager Connection Problems Message

  - Follow the directions presented in the warning message and check that the DNS settings are set up with the following Domain Name Server (DNS) settings:

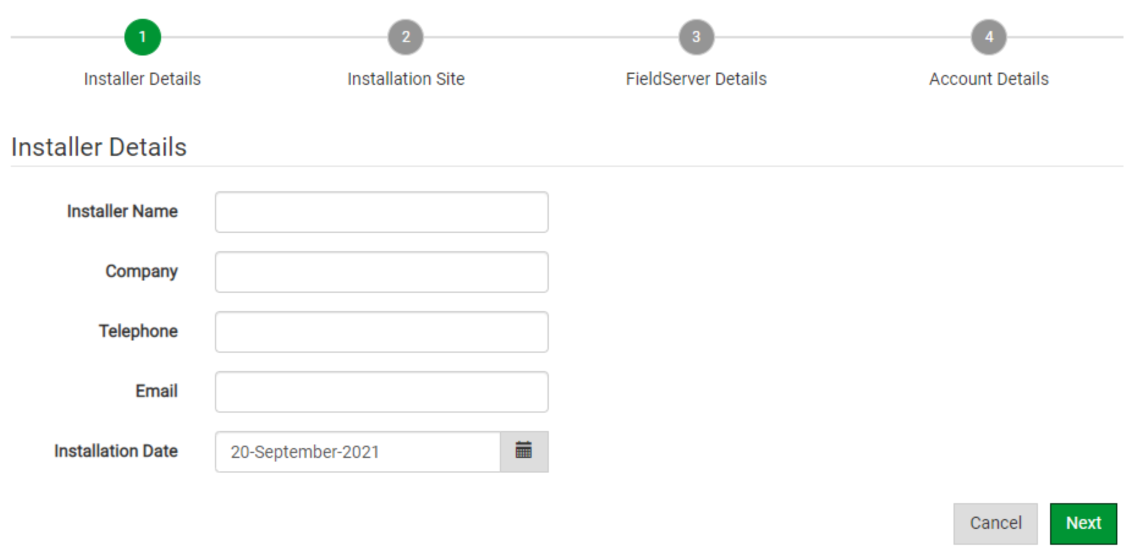
    DNS1=8.8.8.8

    DNS2=8.8.4.4

  - Ensure that the BACnet IoT Gateway is properly connected to the Internet

NOTE: If changes to the network settings are done, remember to save and then power cycle the BACnet IoT Gateway to update the settings.

- Fill in the user details, site details, gateway details and create a new account.
  - Enter user details and click Next

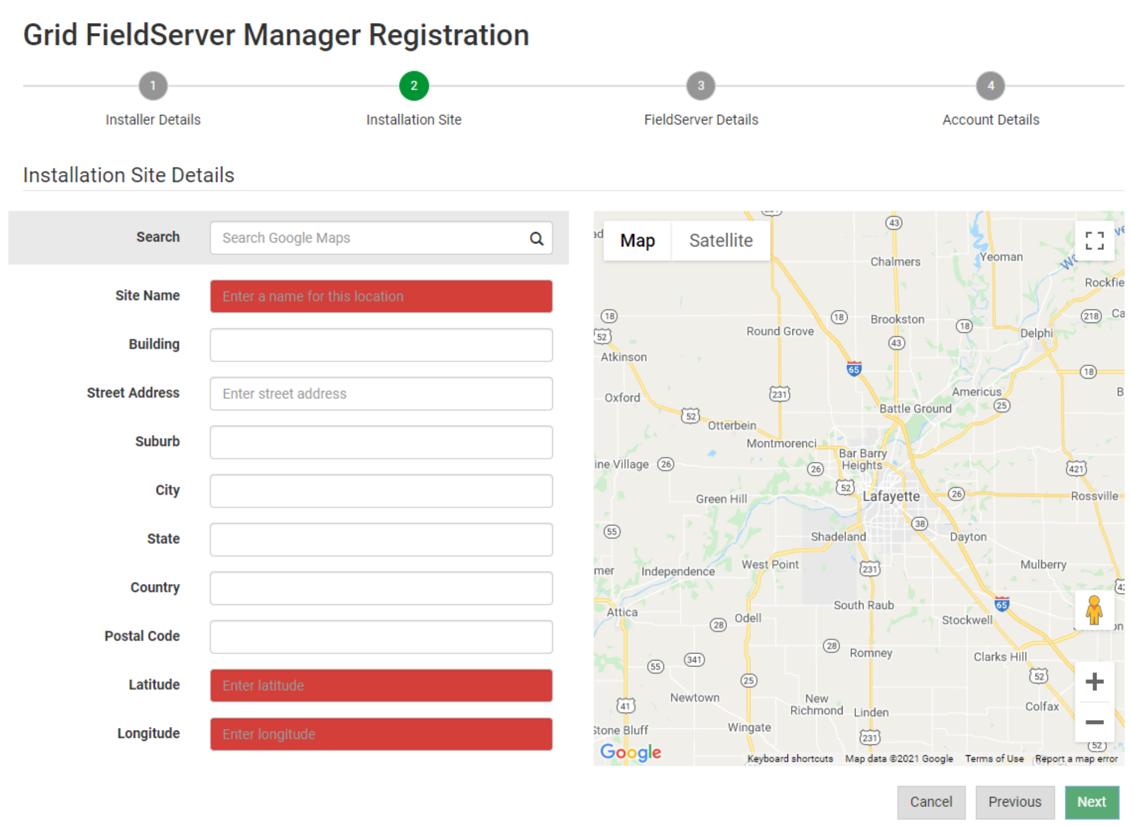


Installer Details

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

Figure 67: FieldServer Manager Registration – Installer Details

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



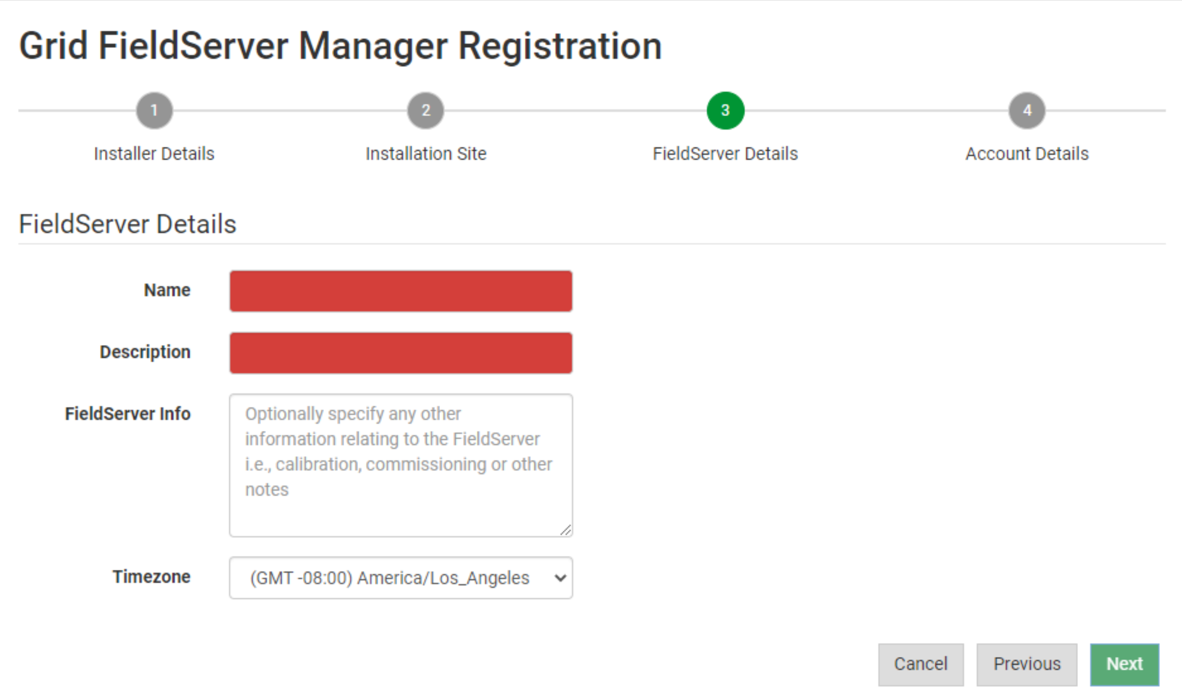
Grid FieldServer Manager Registration

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

Figure 68: FieldServer Manager Registration – Site Details

- Enter Name and Description (required) then click Next



Grid FieldServer Manager Registration

FieldServer Details

Name

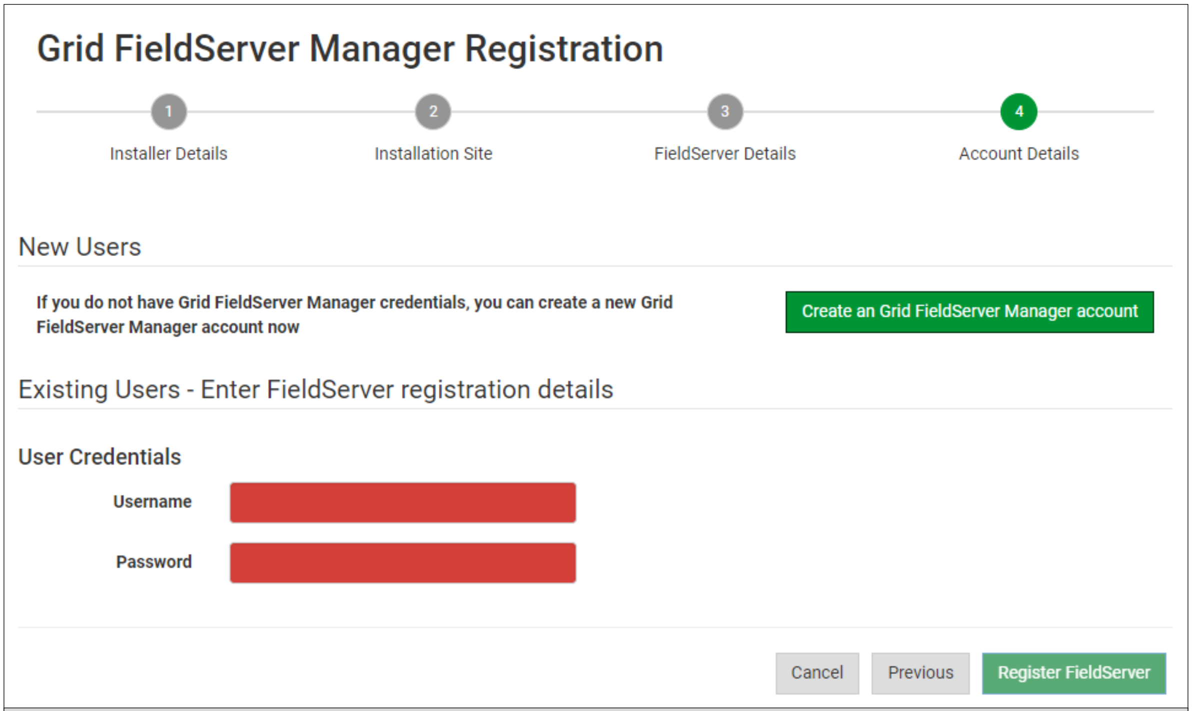
Description

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

Figure 69: FieldServer Manager Registration – Gateway Details

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

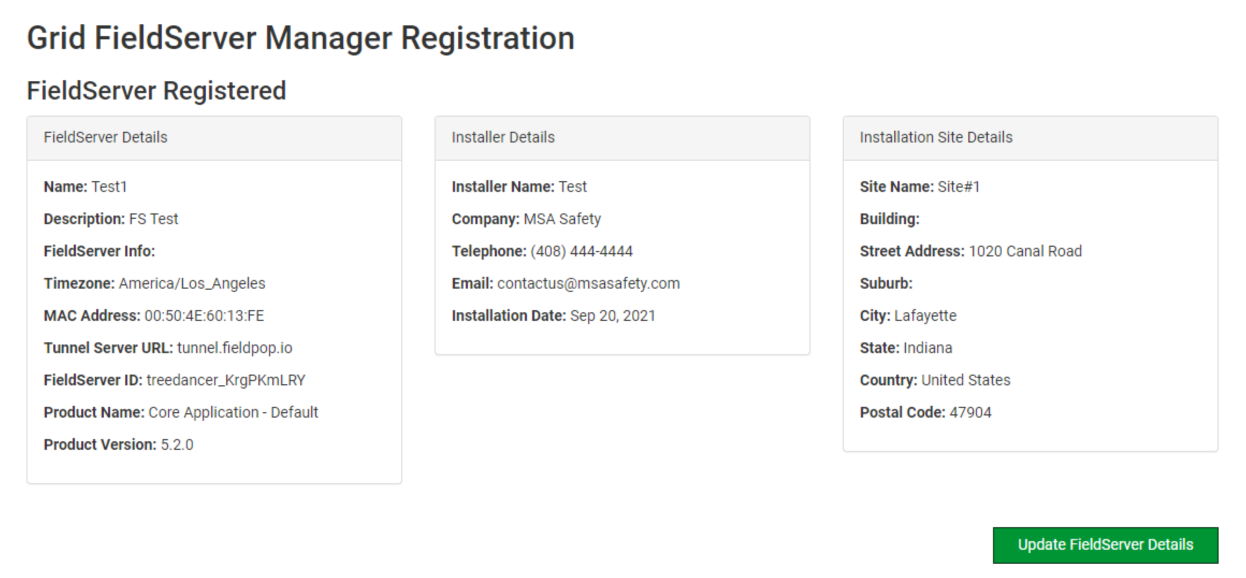
User Credentials

Username

Password

Figure 70: FieldServer Manager Registration – Account

- 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

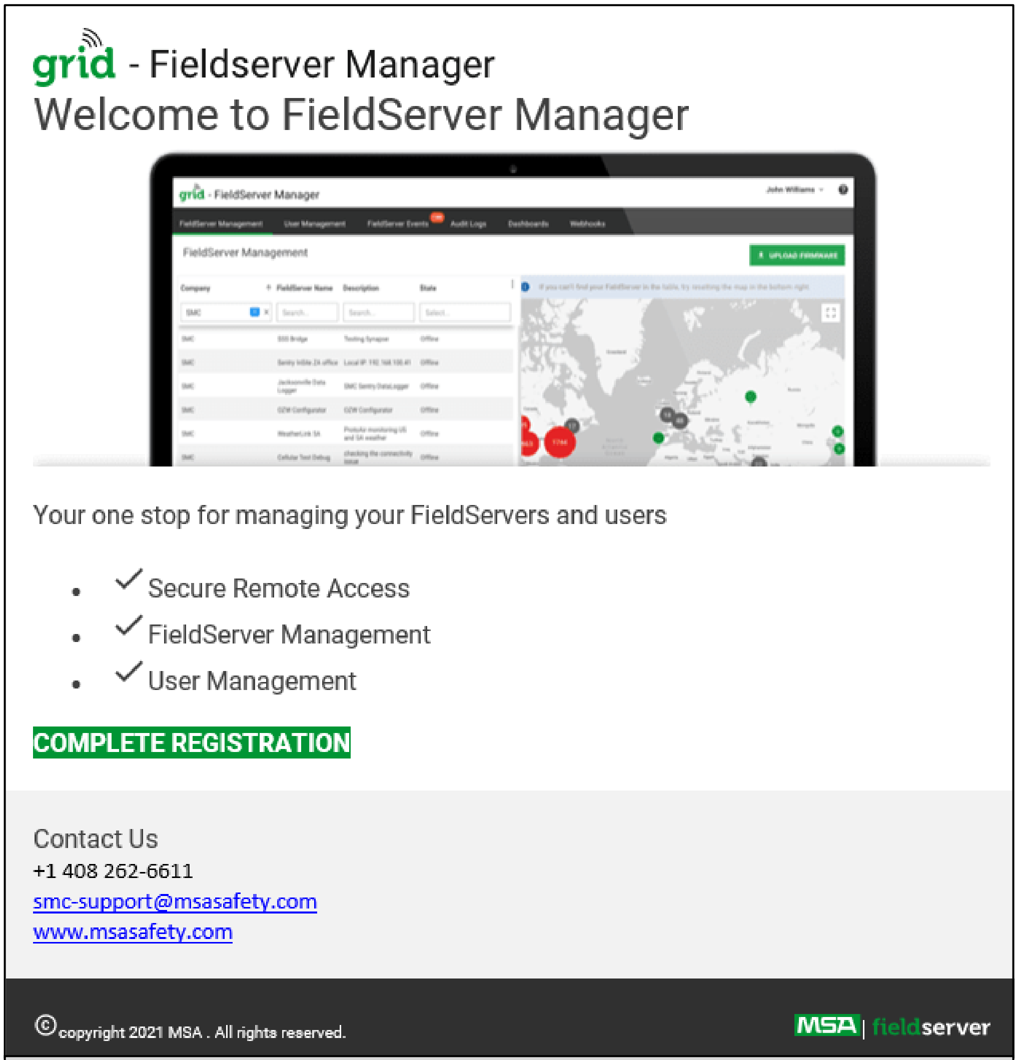
Installation Site Details

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

Figure 71: Device Registered for the FieldServer Manager

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

- Open the registered email account.
- The “Welcome to 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

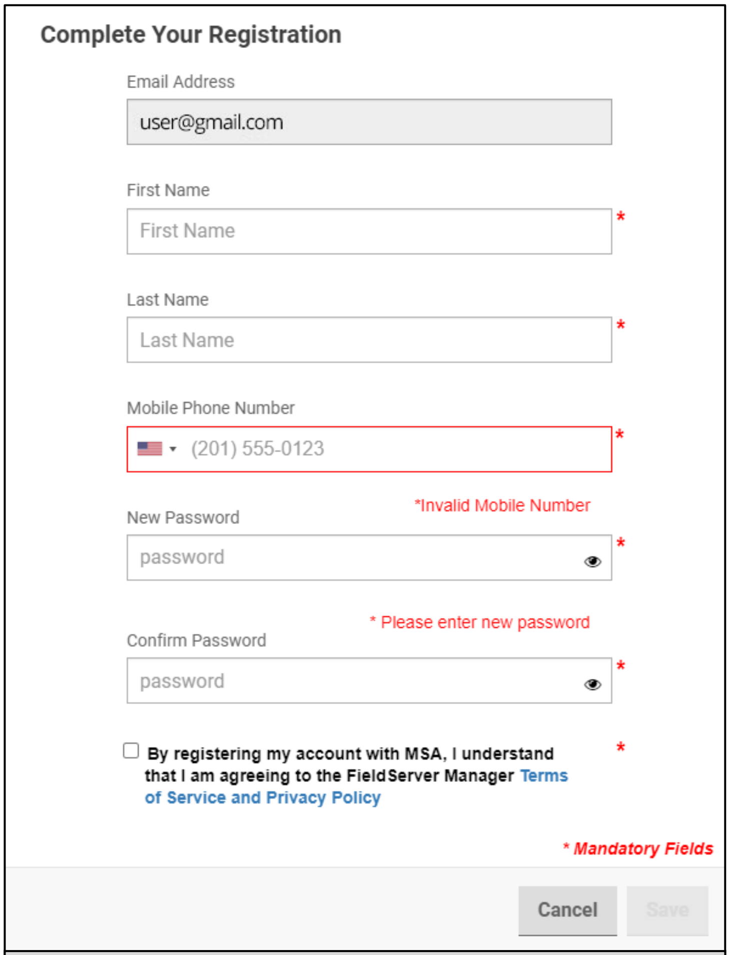
© copyright 2021 MSA . All rights reserved.

MSA | fieldserver

Figure 72: Welcome to FieldServer Manager Email

NOTE: If no email was received, check the spam/junk folder for an email from notification@fieldpop.io. Contact the FieldServer support team if the email cannot be 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*

Figure 73: Setting User Details

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

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

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

9.2 Login to the FieldServer Manager

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

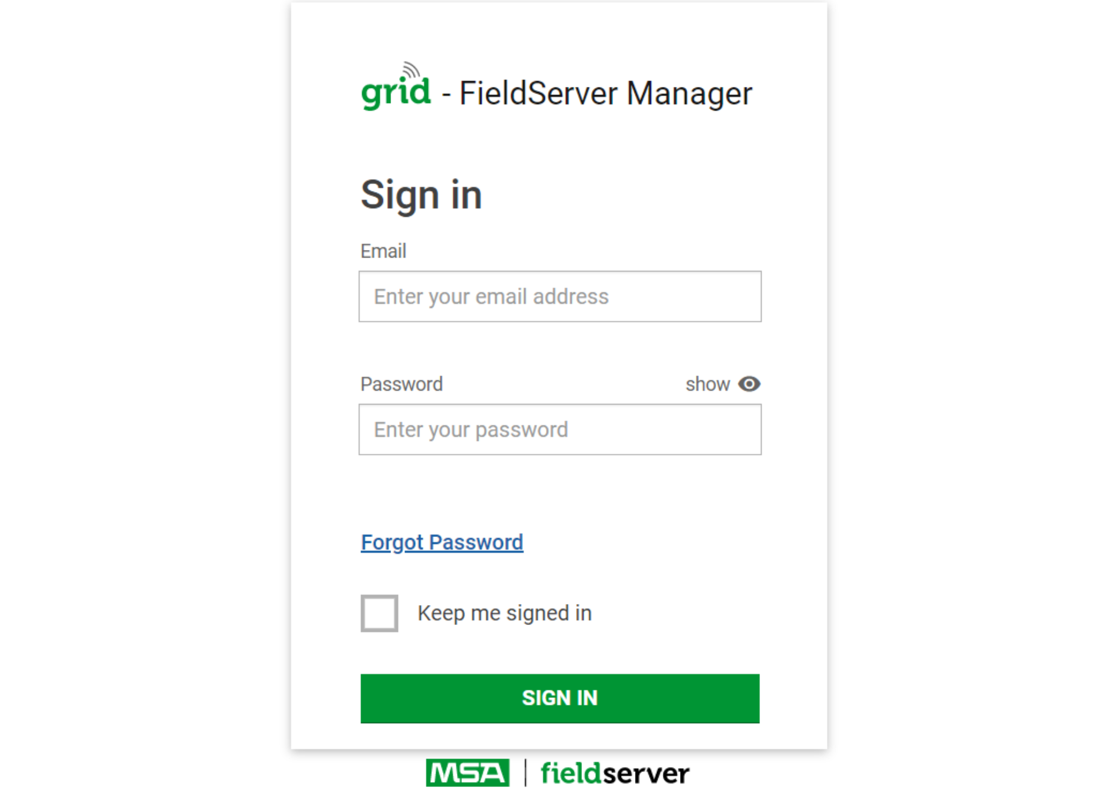
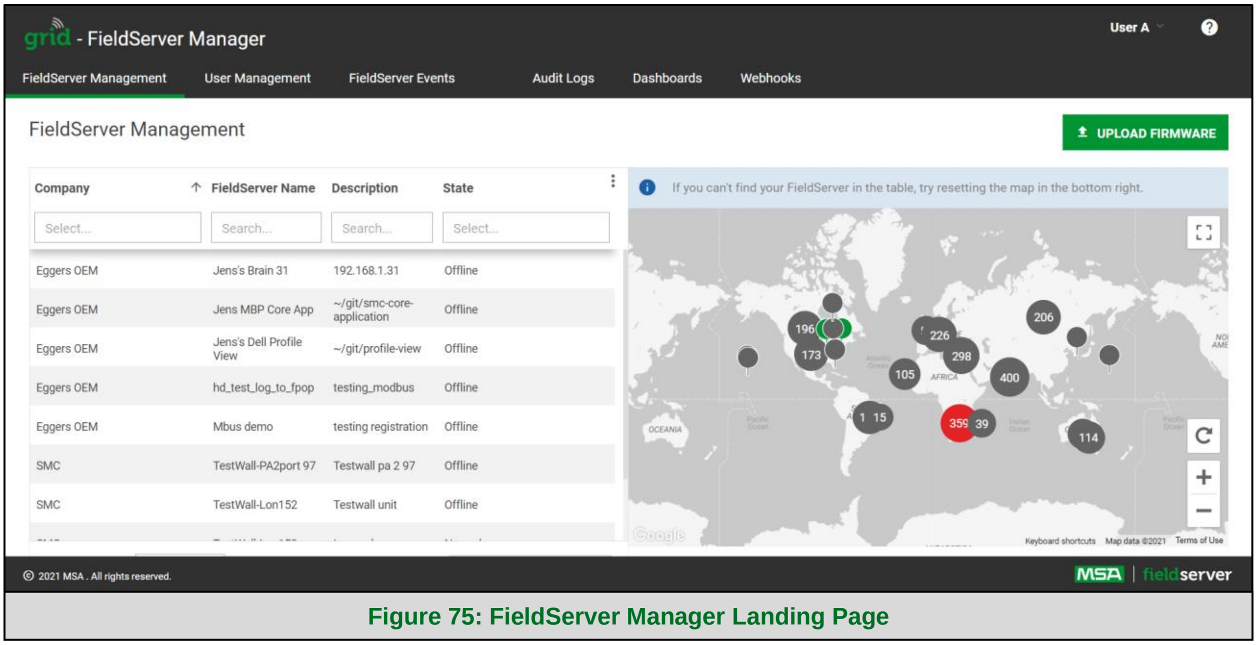


Figure 74: FieldServer Manager Login Page

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

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



FieldServer Management

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.

Figure 75: FieldServer Manager Landing Page

10 MQTT Integration

10.1 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)].

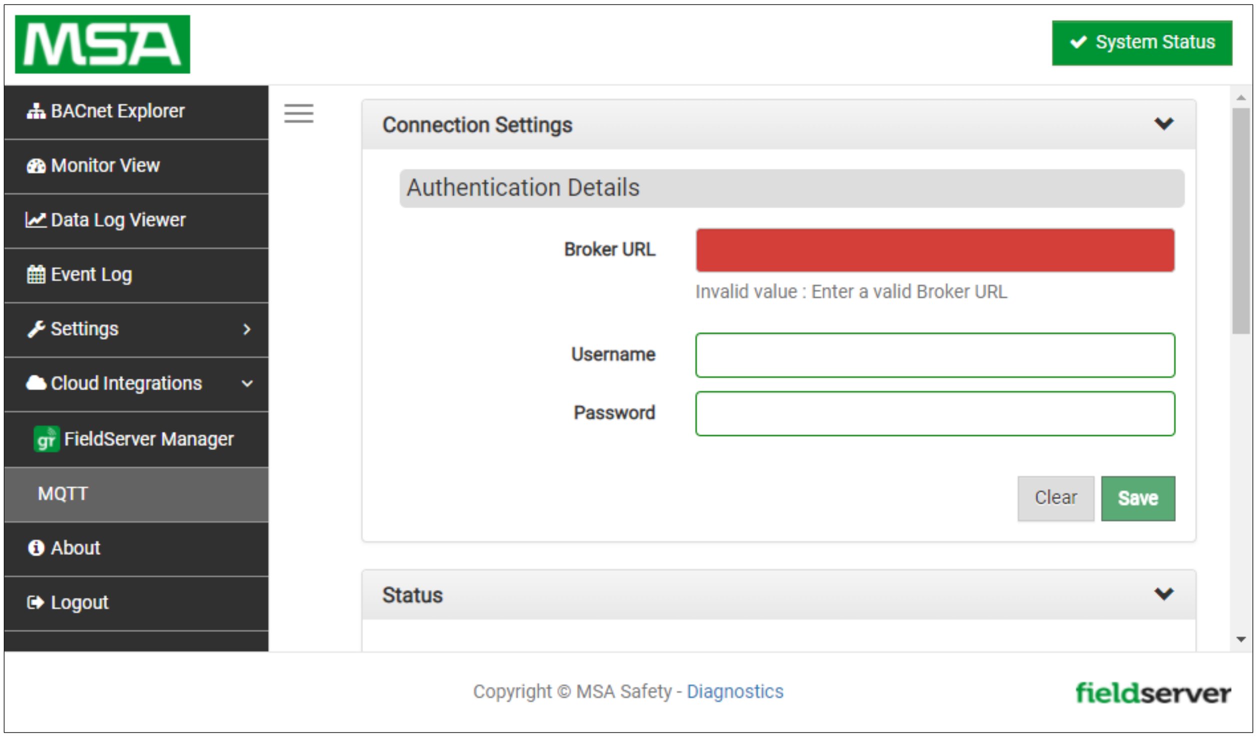
These topics are published via the logging method that was set up for the data points in Monitor View. Refer to **Section** 8.2 and **Section** 8.3 for logging instructions.

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.**

10.2 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.



Connection Settings

Authentication Details

Broker URL

Invalid value : Enter a valid Broker URL

Username

Password

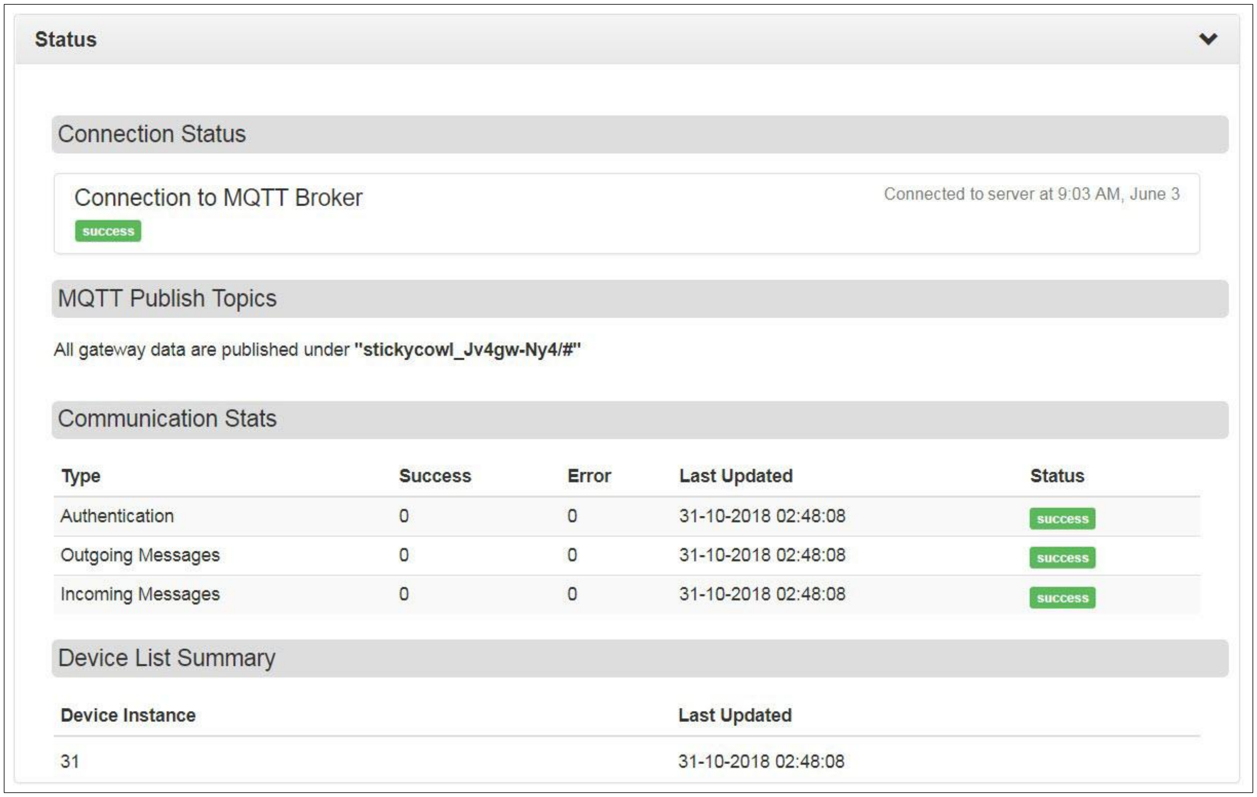
Status

Copyright © MSA Safety - Diagnostics

- 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.

10.3 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.

11 OpenVPN Setup

11.1 Setup Amazon AWS Server

It is recommended to use OpenVPN with Amazon AWS. Follow the linked guide to setup an Amazon AWS server: https://openvpn.net/amazon-cloud/

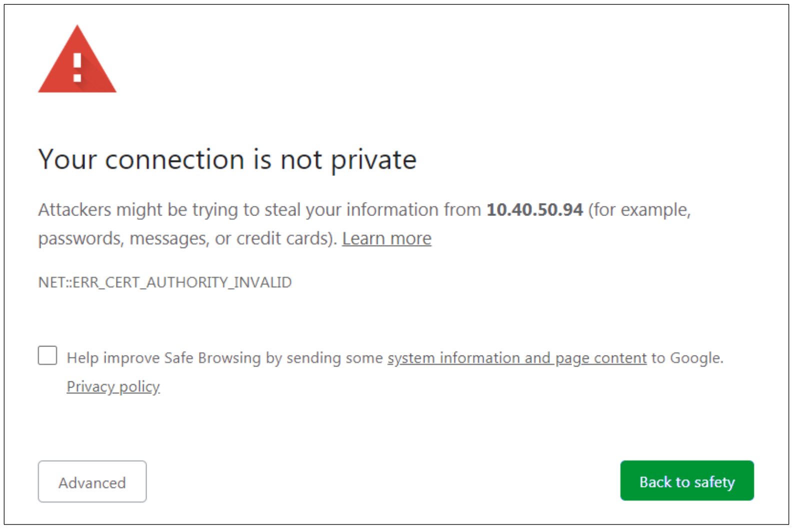
There are 2 options for running OpenVPN on Amazon:

- Purchase the license through Amazon and only pay for the time the OpenVPN is running. For a 5 device license the pricing is listed below:
  Starting from $0.07/hr or from $490.00/yr (20% savings) for software + AWS usage fees
- Bring your own License (BYOL): Amazon offers an unlicensed version of the EC2 instance. A license can be purchased from OpenVPN and entered into the instance. This option is cheaper for continuous usage.

11.2 Setup OpenVPN Cloud

11.2.1 Configure the OpenVPN Server

- Once the AWS server is configured, enter the server's IP Address/admin into the local device's web browser. Example: 35.163.72.29/admin
- This may generate a security warning as there is no certificate for HTTPS to verify. Click the Advanced button to proceed to the IP Address (unsafe). A domain with DNS entry can resolve this error.



Your connection is not private

Attackers might be trying to steal your information from **10.40.50.94** (for example, passwords, messages, or credit cards). Learn more

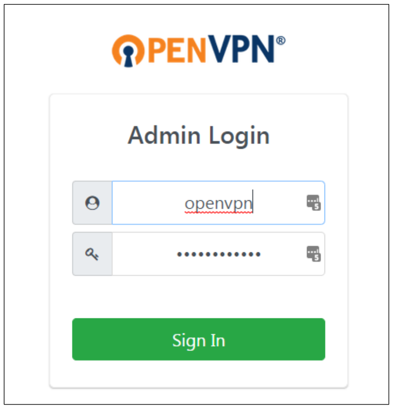
NET::ERR_CERT_AUTHORITY_INVALID

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

NOTE: Some browsers may require adding the IP Address to the trusted IP sites list.

11.2.2 Login to the Server

- Once on the website, use Admin credentials to login.



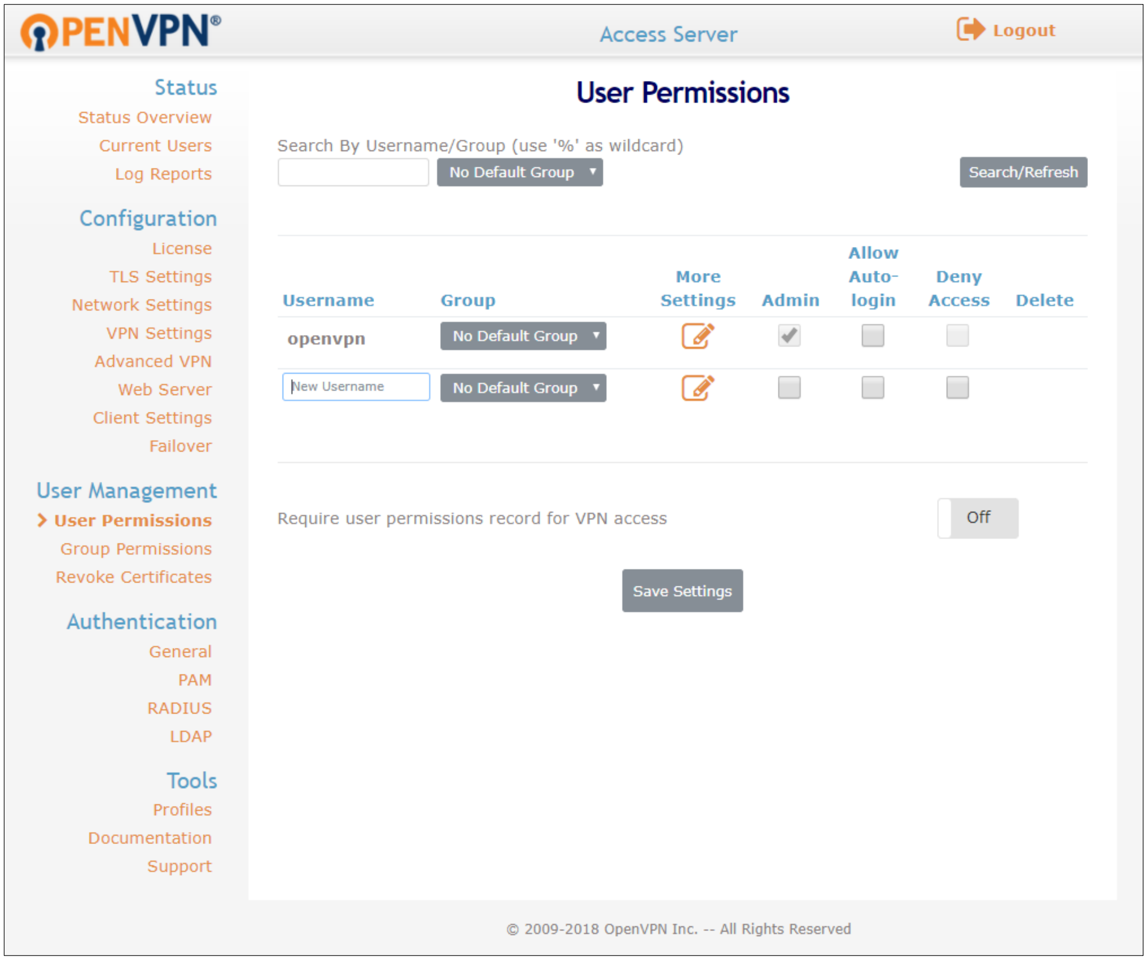
Admin Login

openvpn

••••••••••••

11.2.3 Create a New User for the PC Connection

- Find the User Management Section in the Navigation bar on the left side of the screen.
- Click on User Permissions.



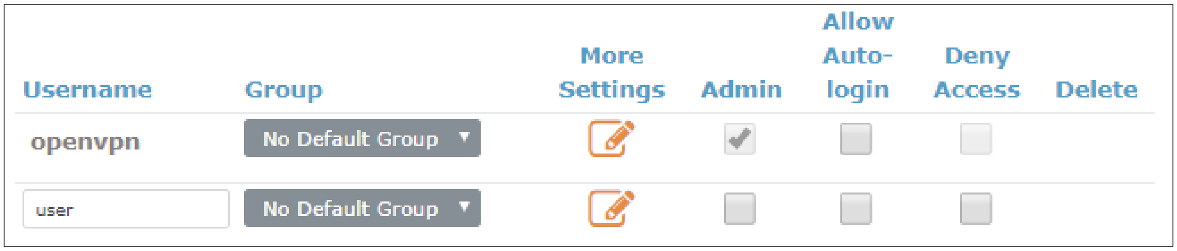
User Permissions

Search By Username/Group (use '%' as wildcard)

Username	Group	More Settings	Admin	Allow Auto-login	Deny Access	Delete
openvpn	No Default Group ▾	✎	☑	□	□	
New Username	No Default Group ▾	✎	□	□	□	

Require user permissions record for VPN access: Off

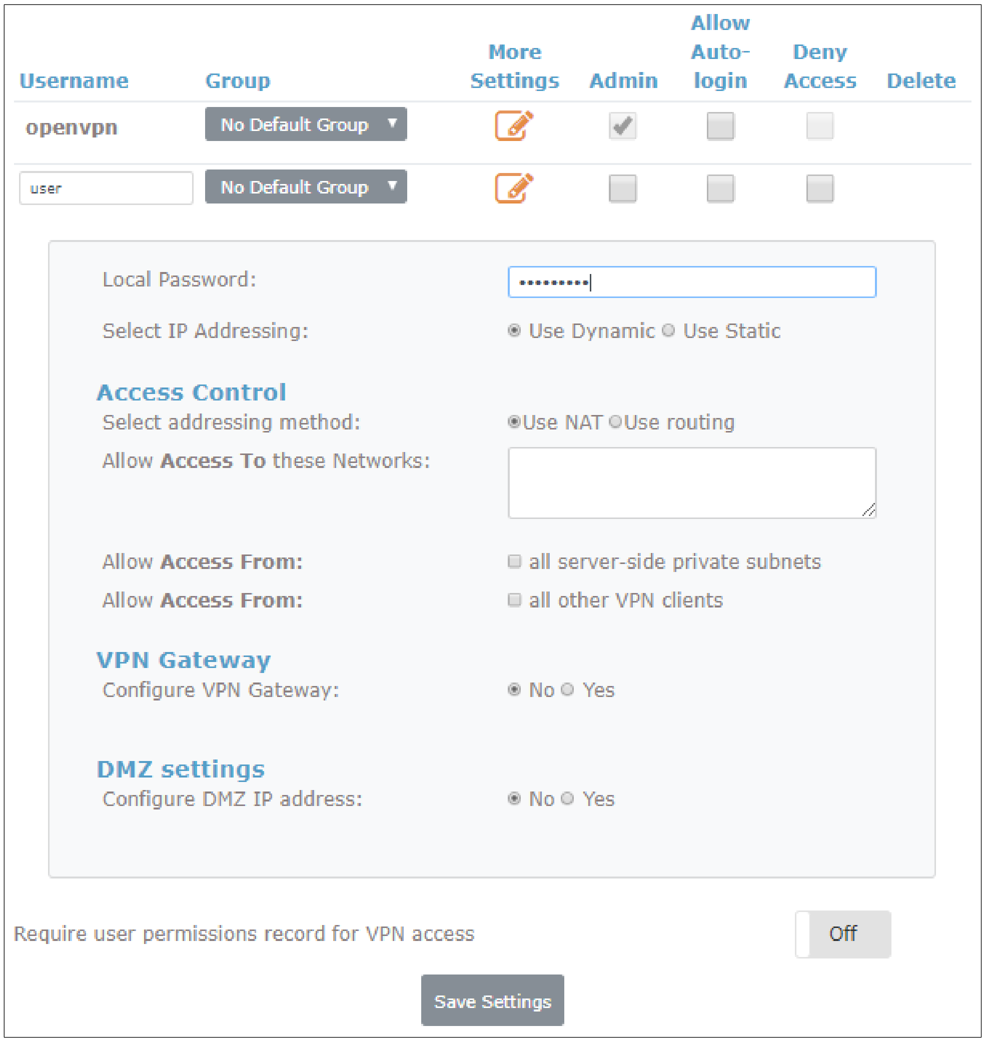
- Once the User Permissions page is open, type in a new username in the text field under the Username heading and make sure the Admin, Allow-Auto login, and Deny Access boxes are all unchecked.



Username	Group	More Settings	Admin	Allow Auto-login	Deny Access	Delete
openvpn	No Default Group ▾	✎	☑	□	□	
user	No Default Group ▾	✎	□	□	□	

- Click the configuration button (✎) under the More Settings heading to access more configuration options.

- Enter a password for the USER profile in the Local Password field and record for future use.



Username	Group	More Settings	Admin	Allow Auto-login	Deny Access	Delete
openvpn	No Default Group ▼	✎	☑	□	□	
user	No Default Group ▼	✎	□	□	□	

Local Password: •••••••••

Select IP Addressing: ● Use Dynamic ○ Use Static

Access Control

Select addressing method: ●Use NAT ○Use routing

Allow **Access To** these Networks:

Allow **Access From:** □ all server-side private subnets

Allow **Access From:** □ all other VPN clients

VPN Gateway

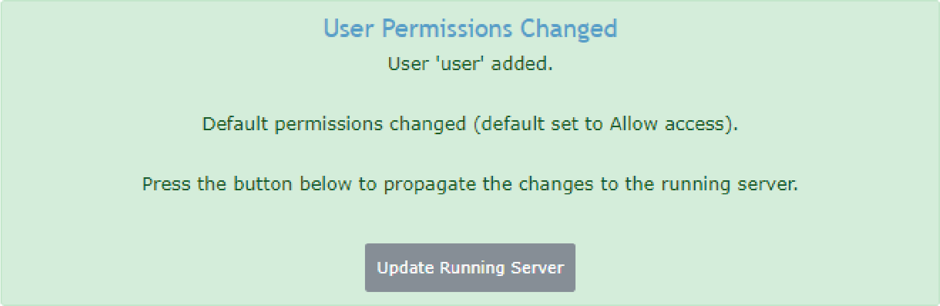
Configure VPN Gateway: ● No ○ Yes

DMZ settings

Configure DMZ IP address: ● No ○ Yes

Require user permissions record for VPN access Off

- Once configuration is complete, click the Save Settings button and then click the Update Running Server button.

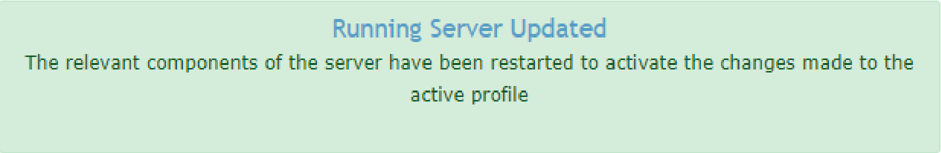


User Permissions Changed

User 'user' added.

Default permissions changed (default set to Allow access).

Press the button below to propagate the changes to the running server.

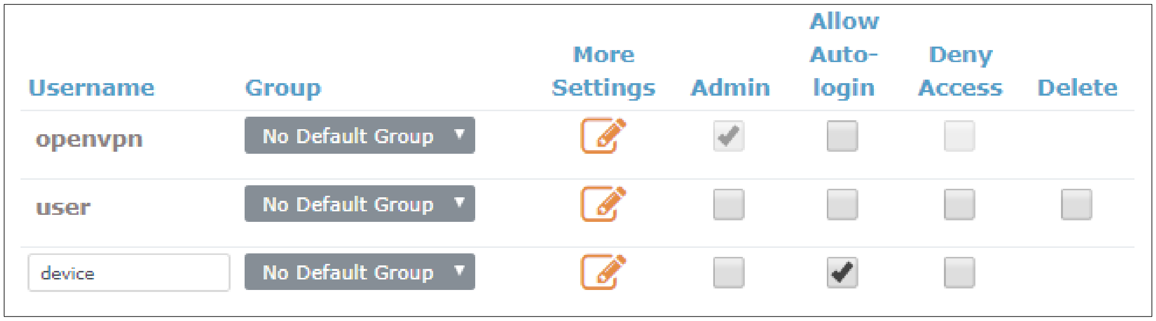


Running Server Updated

The relevant components of the server have been restarted to activate the changes made to the active profile

11.2.4 Create a New User for the Device Connection

- Once the User Permissions page is open, type in a new device name in the text field under the Username heading and make sure the Allow-Auto login box is checked, and the Admin and Deny Access boxes are all unchecked.



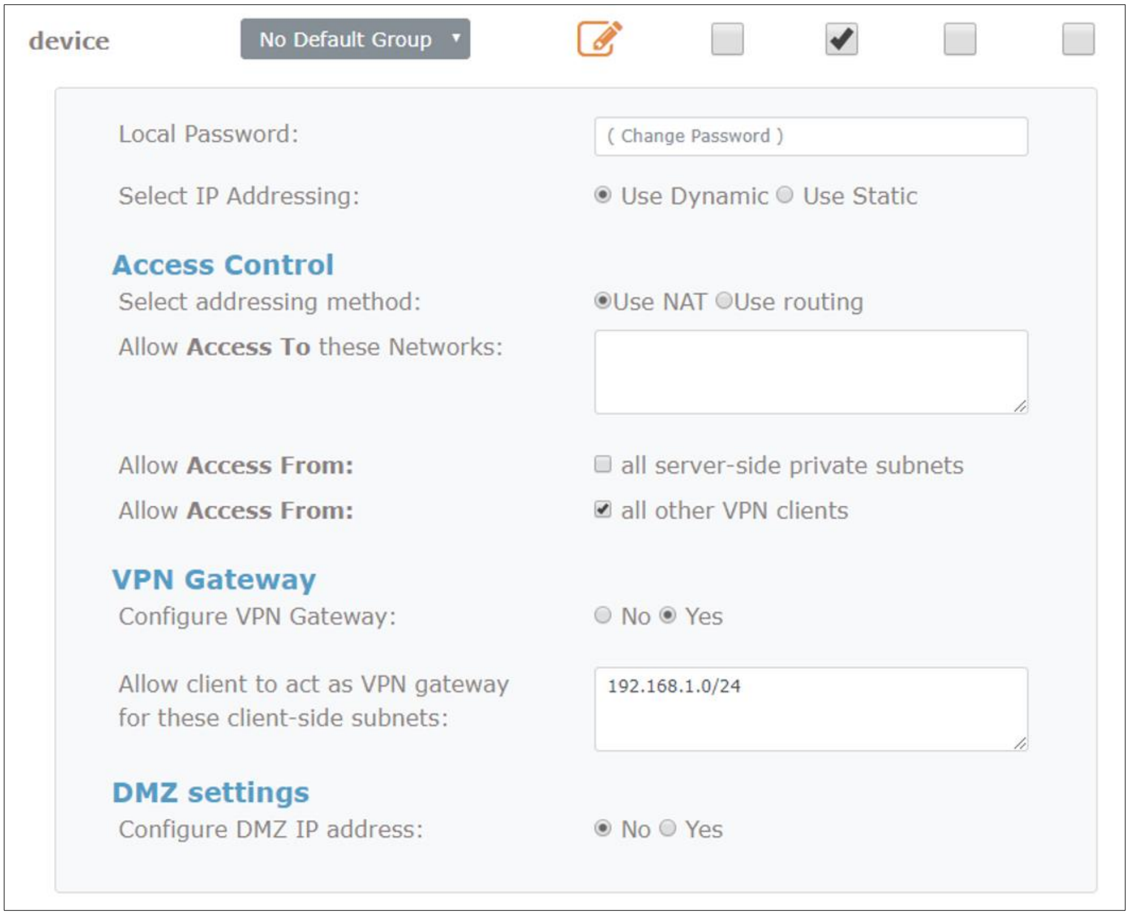
Username	Group	More Settings	Admin	Allow Auto-login	Deny Access	Delete
openvpn	No Default Group ▾	✎	☑	☐	☐	
user	No Default Group ▾	✎	☐	☐	☐	☐
device	No Default Group ▾	✎	☐	☑	☐	

- Click the configuration button (✎) under the More Settings heading to access more configuration options.
- Enter a password for the DEVICE profile in the Local Password field and record for future use.
- Set the Configure VPN Gateway to Yes.

- If the VPN needs to access the local network, configure the VPN Gateway section. This will allow traffic through the FieldServer to the IP Addresses on the local network.

  For example:

  - To allow access to all IP Address on 192.168.1.x subnet, type in “192.168.1.0/24”
  - To only allow access to 192.168.1.50, type in “192.168.1.50/32”



device No Default Group ▾ □ ☑ □ □

Local Password: (Change Password)

Select IP Addressing: ● Use Dynamic ○ Use Static

Access Control

Select addressing method: ●Use NAT ○Use routing

Allow **Access To** these Networks:

Allow **Access From:** □ all server-side private subnets

Allow **Access From:** ☑ all other VPN clients

VPN Gateway

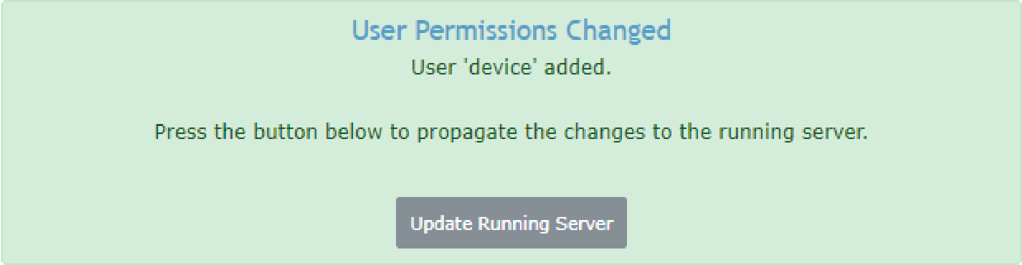
Configure VPN Gateway: ○ No ● Yes

Allow client to act as VPN gateway for these client-side subnets: 192.168.1.0/24

DMZ settings

Configure DMZ IP address: ● No ○ Yes

- Once configuration is complete, click the Save Settings button and then click the Update Running Server button.

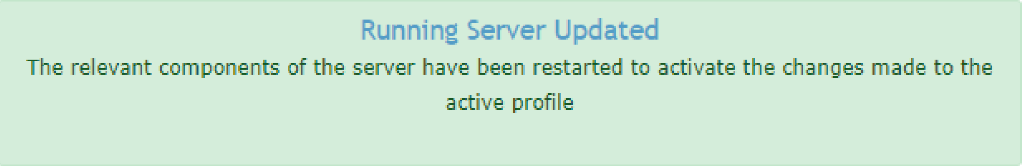


User Permissions Changed

User 'device' added.

Press the button below to propagate the changes to the running server.

Update Running Server



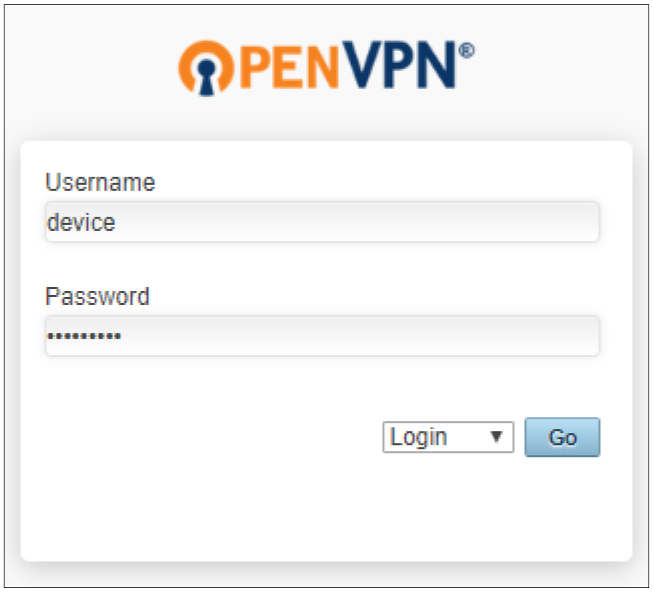
Running Server Updated

The relevant components of the server have been restarted to activate the changes made to the active profile

11.3 Configure BACnet IoT Gateway for OpenVPN

11.3.1 Download the DEVIC Configuration Profile

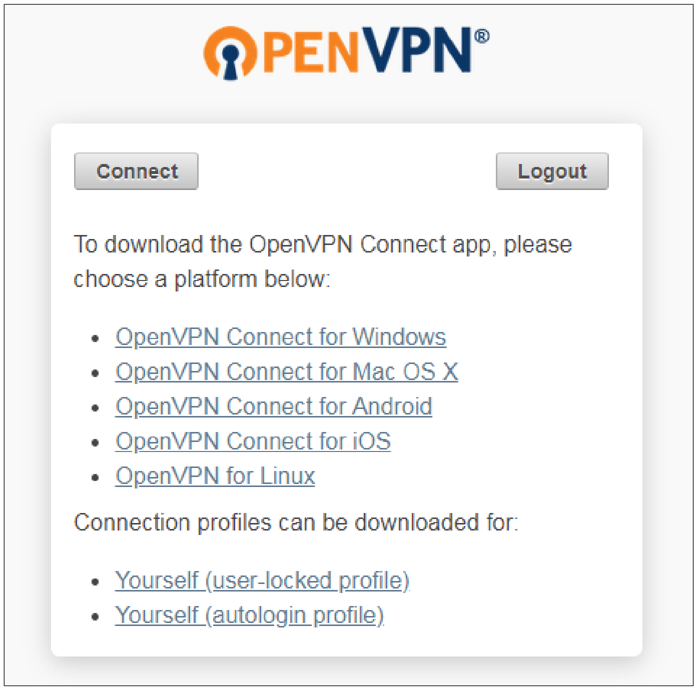
- Login with the DEVICE credentials that were created in **Section 11.2.4**.



Username
device

Password
•••••••••

- Click on "Yourself (autologin profile)".
  - The DEVICE .opvn file will download to the default folder on the PC



To download the OpenVPN Connect app, please choose a platform below:

- OpenVPN Connect for Windows
- OpenVPN Connect for Mac OS X
- OpenVPN Connect for Android
- OpenVPN Connect for iOS
- OpenVPN for Linux

Connection profiles can be downloaded for:

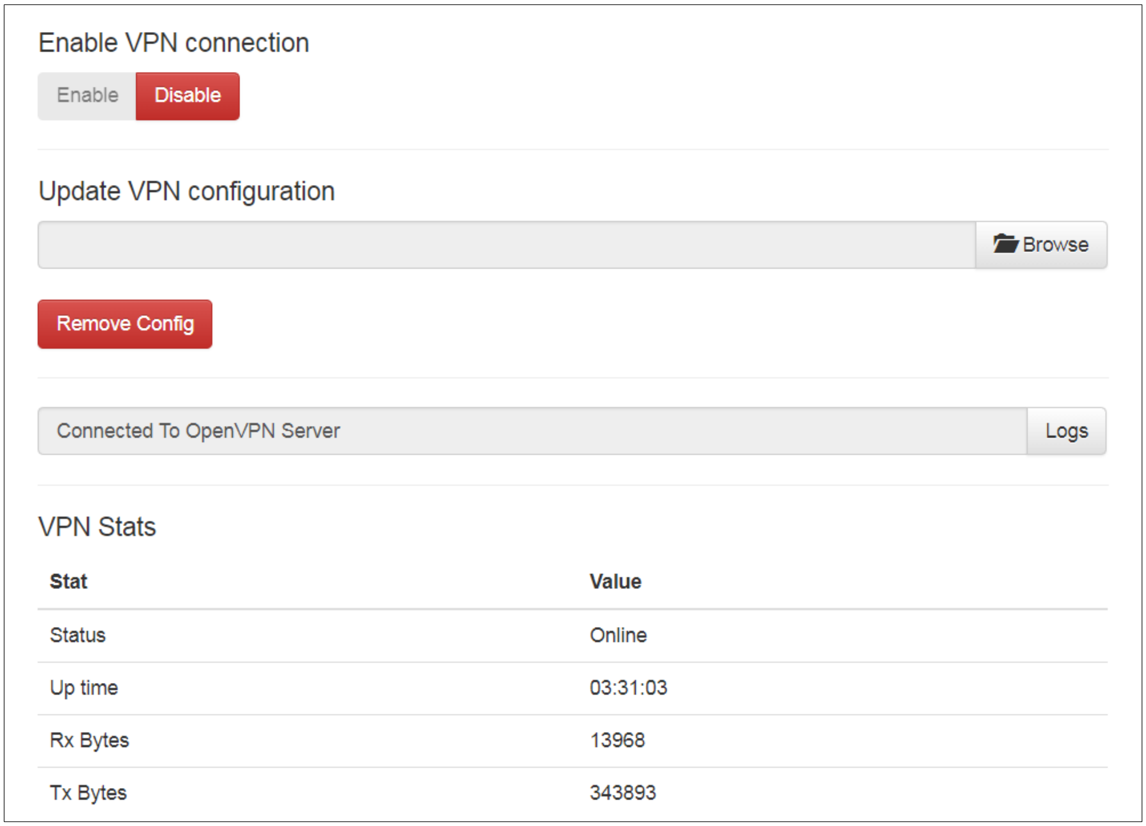
- Yourself (user-locked profile)
- Yourself (autologin profile)

- Click on Logout.

11.3.2 Load the DEVICE OpenVPN Connection Profile onto the BACnet IoT Gateway

The DEVICE .opvn file must be loaded onto the BACnet IoT Gateway for OpenVPN configuration.

- To do this, input the BACnet IoT's IP Address into the local browser and login.
- Click the Settings tab to show the configurable settings types.
- Then click on the OpenVPN tab that appears to bring up the following page:



Enable VPN connection

Update VPN configuration

Connected To OpenVPN Server

VPN Stats

Stat	Value
Status	Online
Up time	03:31:03
Rx Bytes	13968
Tx Bytes	343893

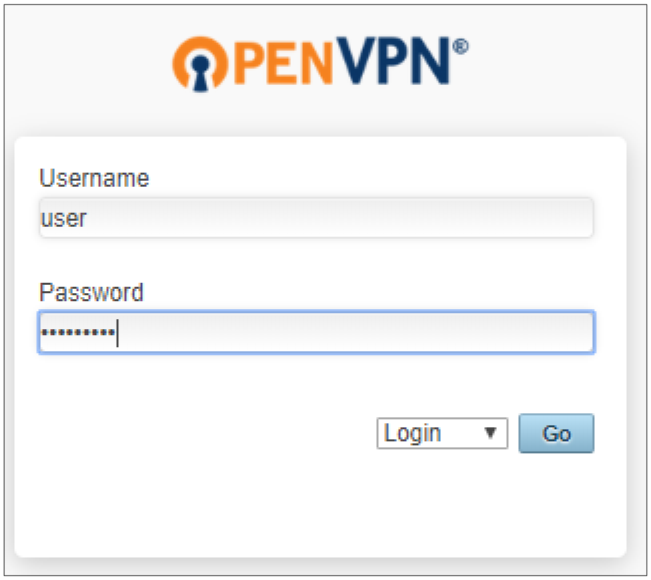
- Click the Browse button under the Update VPN configuration header and select the DEVICE .opvn file to load it for OpenVPN configuration.
- Change the Enable VPN connection to Enable.
  - Once OpenVPN is enabled on the FieldServer, it will connect to the OpenVPN server.

NOTE: The connection statistics will be displayed in the VPN Stats section.

11.4 Install the OpenVPN Client onto a Local PC

11.4.1 Download the USER Configuration Profile

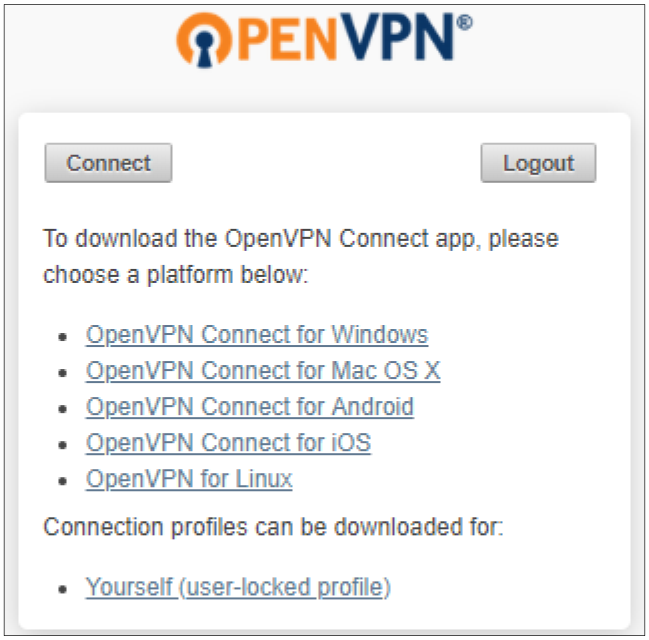
- Enter the server's IP Address into the local device's web browser.
- Go to the OpenVPN server and login with the USER credentials created in **Section 11.2.3**.



Username
user

Password
•••••••••

- Click on "Yourself (user-locked profile)".
  - The USER .opvn file will download to the default folder on the PC



To download the OpenVPN Connect app, please choose a platform below:

- OpenVPN Connect for Windows
- OpenVPN Connect for Mac OS X
- OpenVPN Connect for Android
- OpenVPN Connect for iOS
- OpenVPN for Linux

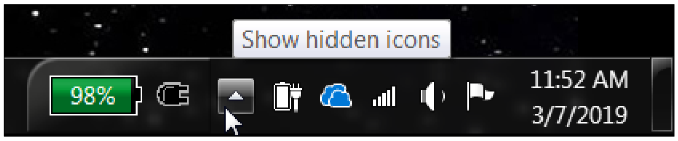
Connection profiles can be downloaded for:

- Yourself (user-locked profile)

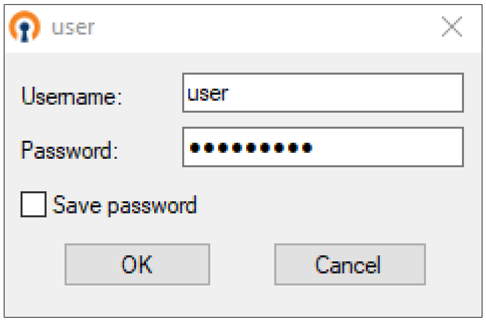
- Click on Logout.

11.4.2 Load the USER OpenVPN Connection Profile onto the PC

- Download and install the OpenVPN client at: https://swupdate.openvpn.org/community/releases/openvpn-install-2.4.6-I602.exe
- Start the OpenVPN software by double clicking the OpenVPN GUI shortcut on the desktop.
- Right click the OpenVPN icon (🖥) found in the system tray (on the right side of the taskbar).
    - If the icon isn’t visible, click the upwards arrow in the system tray to find it



- Select the "Import file …" option in the dropdown menu.
- Find and select the USER .opvn file on the local PC.
- Right click on the OpenVPN icon (🖥) again and click the new “Connect” option in the dropdown menu.
- When the login window appears, enter the USER credentials.



Username: user

Password: ●●●●●●●●●

☐ Save password

- A message will appear saying the OpenVPN connection has been established.

12 Specifications

	FS-IOT-BAC, FS-IOT-BACW & FS-IOT-BACA/V/F[1]
Available Ports	One 3-pin Phoenix connector with: RS-485/RS-232 port (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) **BAC2E includes an additional:** One Ethernet 10/100 BaseT port
BAC/BACW/BAC2E Power Requirements	*Input Voltage:* 9-30VDC or 24VAC *Current draw:* 24VAC 0.125A *Max Power:* 3 Watts 9-30VDC 0.25A @12VDC
BACA/V/F Power Requirements	*Input Voltage:* 12-24V DC *Current draw:* @ 12V, 0.67A *Power Rating:* 8 Watts
Approvals	CE and FCC Class B & C Part 15, UL 62368 approved[4], UL 916 approved[2], WEEE compliant, IC Canada, RoHS compliant, REACH compliant, UKCA compliant, PTCRB[3] and CTIA[3]
Dimensions (WxDxH)	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 to 70ºC (-4 to 158ºF)
Humidity	10-95% RH non-condensing
Wi-Fi 802.11 b/g/n [3]	*Frequency:* 2.4 GHz *Channels:* 1 to 11 (inclusive) *Antenna Type:* SMA *Encryption:* TKIP, WPA & AES
Cellular [4]	*Features:* LTE Cat.4 *Antenna Type:* SMA *Uplink:* Up to 50 Mbps *Downlink:* Up to 150 Mbps

Figure 76: Specifications

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

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

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

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

[1] Specifications subject to change without notice
[2] Only for FS-IOT-BAC & FS-IOT-BACW
[3] Only for FS-IOT-BACW & FS-IOT-BACA/V/F
[4] Only for FS-IOT-BACA/V/F

13 References

13.1 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.

13.2 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.

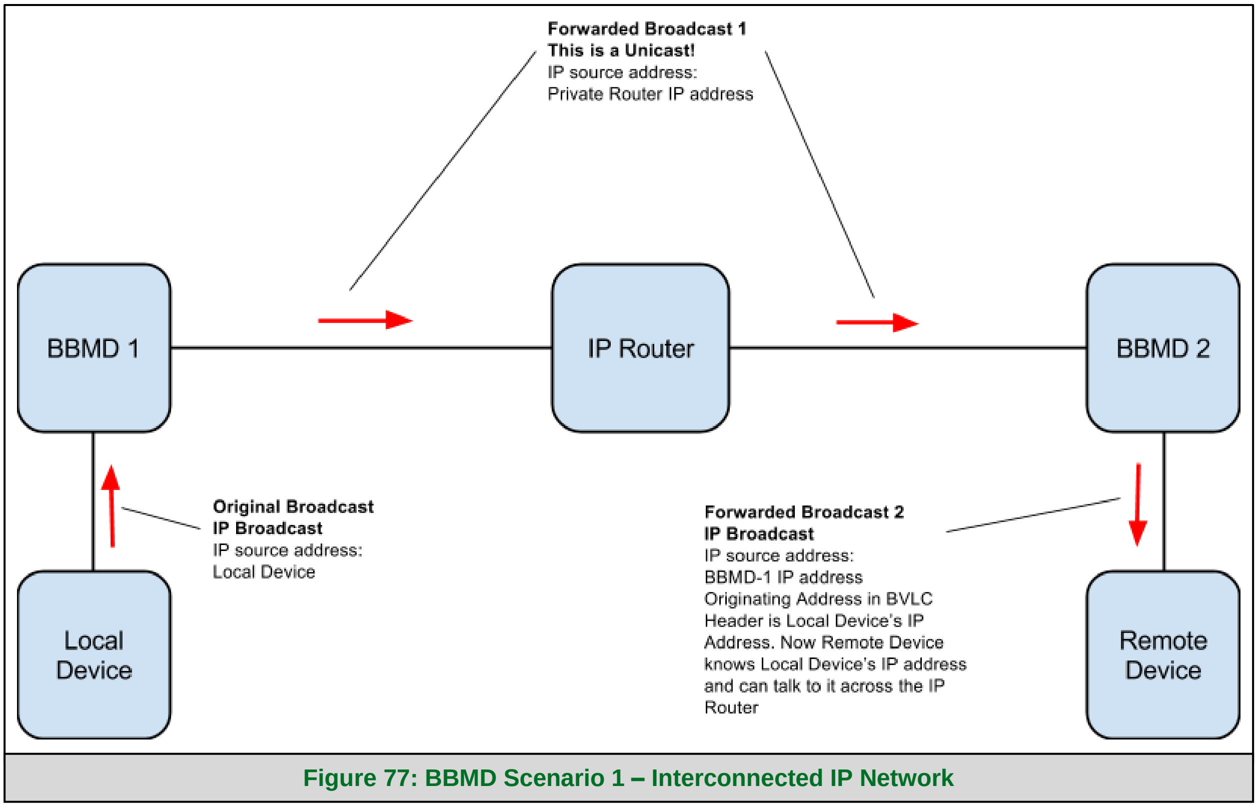
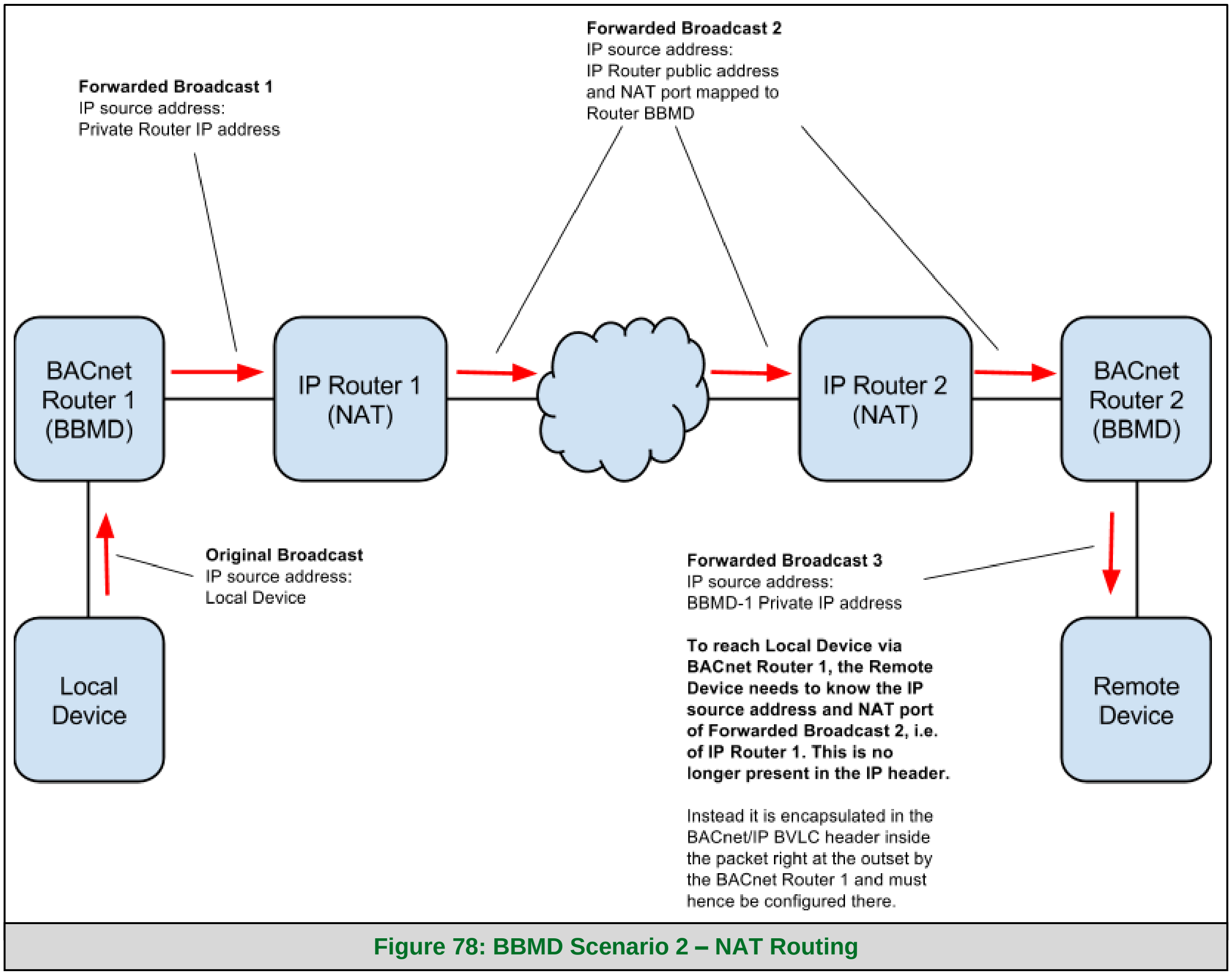

Forwarded Broadcast 1
This is a Unicast!
IP source address:
Private Router IP address
BBMD 1
IP Router
BBMD 2
Original Broadcast
IP Broadcast
IP source address:
Local Device
Forwarded Broadcast 2
IP Broadcast
IP source address:
BBMD-1 IP address
Originating Address in BVLC Header is Local Device's IP Address. Now Remote Device knows Local Device's IP address and can talk to it across the IP Router
Local Device
Remote Device

Figure 77: BBMD Scenario 1 – Interconnected IP Network

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.



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.

Figure 78: BBMD Scenario 2 – NAT Routing

14 Troubleshooting

14.1 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 192.168.2.101, 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 192.168.2.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.

14.2 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.

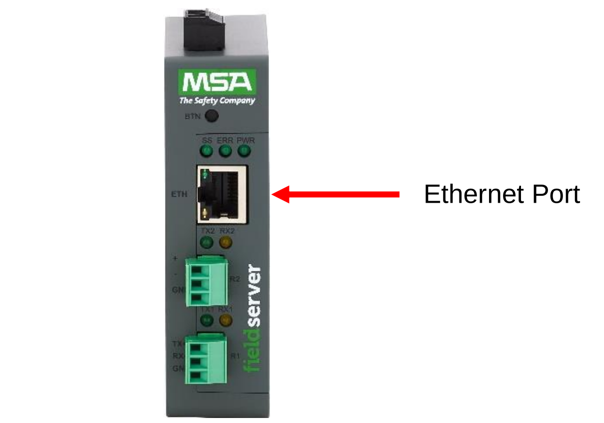
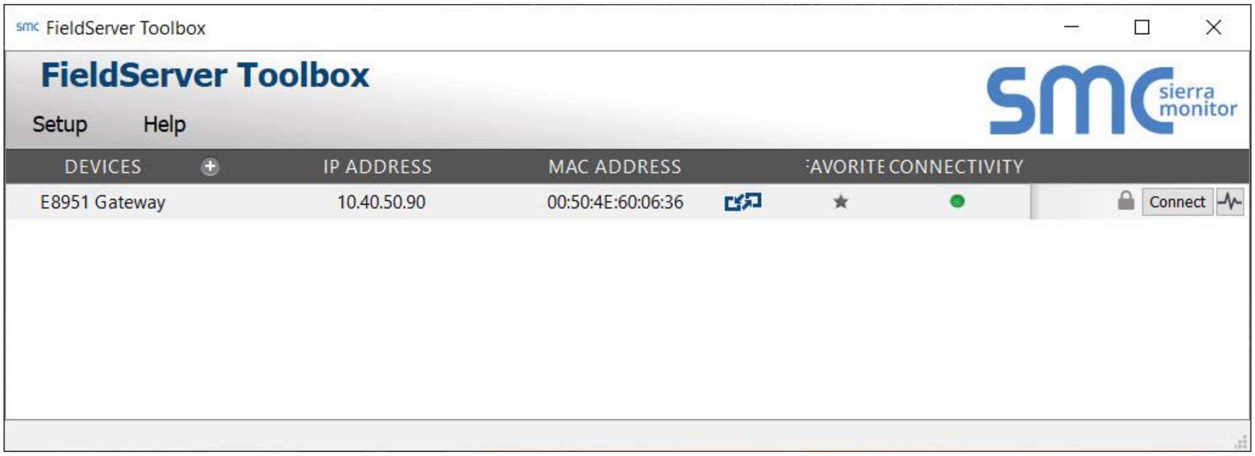


Figure 79: Ethernet Port Location

- 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.

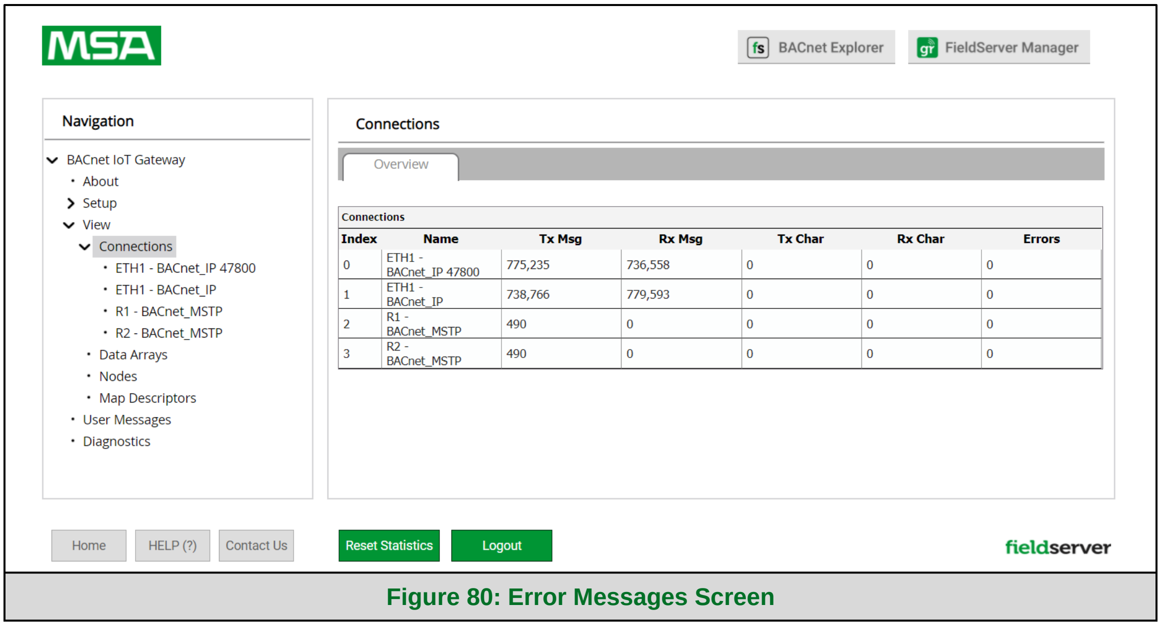


DEVICES	IP ADDRESS	MAC ADDRESS	FAVORITE	CONNECTIVITY
E8951 Gateway	10.40.50.90	00:50:4E:60:06:36	★	●

14.3 Viewing Diagnostic Information

- Type the IP Address of the BACnet IoT Gateway into the web browser or use the FieldServer Toolbox to connect to the BACnet IoT Gateway.
- Click on the blue “Diagnostics” text at the bottom of the page.
- Under the Navigation panel, click on view and then on connections.

NOTE: If there are any errors showing on the Connection page, refer to Section 14.4 for the relevant wiring and settings.



Connections

Connections

Index	Name	Tx Msg	Rx Msg	Tx Char	Rx Char	Errors
0	ETH1 - BACnet_IP 47800	775,235	736,558	0	0	0
1	ETH1 - BACnet_IP	738,766	779,593	0	0	0
2	R1 - BACnet_MSTP	490	0	0	0	0
3	R2 - BACnet_MSTP	490	0	0	0	0

Figure 80: Error Messages Screen

14.4 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** 14.5)
- Check baud rate, parity, data bits, stop bits
- Check Serial device address
- Verify wiring
- Verify device is connected to the same subnet as the BACnet IoT Gateway

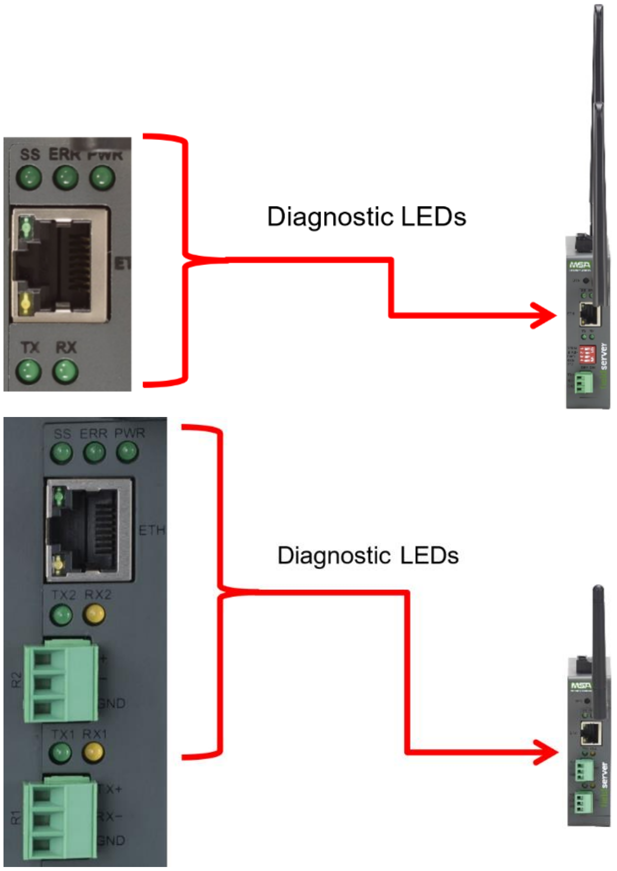
No COMS on the Ethernet protocol. To fix this, check the following:

- Visual observations of LEDs on the BACnet IoT Gateway (**Section** 14.5)
- Check device address
- Verify wiring
- Verify device is connected to the same subnet as the BACnet IoT Gateway
- Verify IP Address setting

NOTE: If the problem still exists, a Diagnostic Capture needs to be taken and sent to support. (Section 14.6)

14.5 LED Diagnostics for Communications Between BACnet IoT Gateway and Devices

See the diagram below for BACnet IoT Gateway LED locations.



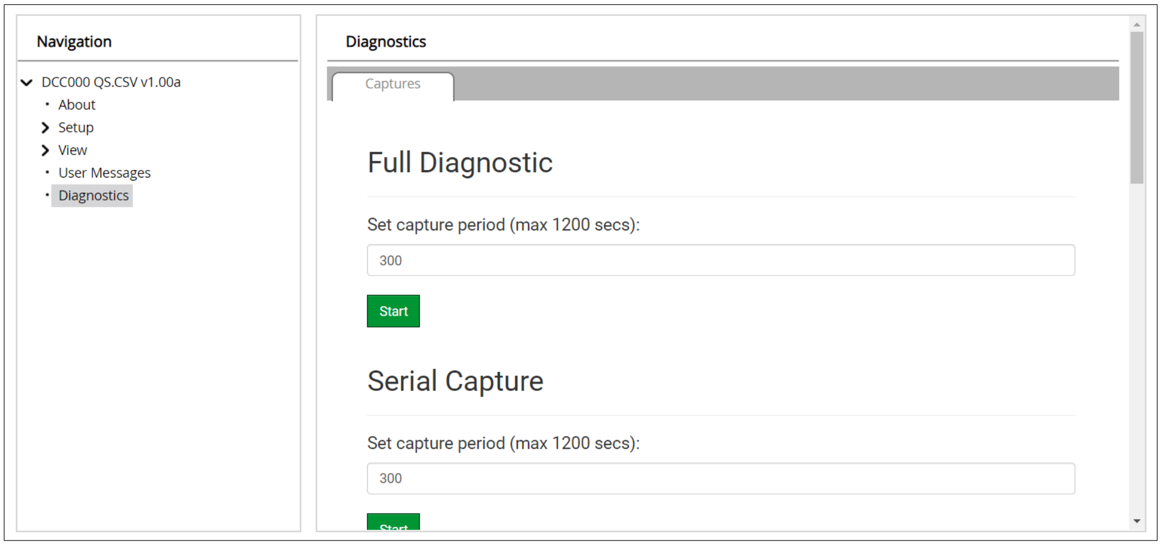
Tag	Description
SS	The SS LED will flash once a second to indicate that the bridge is in operation.
ERR	The SYS ERR LED will go on solid indicating there is a system error on unit. If this occurs, immediately report the related “system error” shown on the error screen of the FS-GUI to support for evaluation.
PWR	The power light should always show steady green when connected to a functioning power source.
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 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 FS-IOT-BAC/BACW**, TX1 applies to the R1 connection while TX2 applies to the R2 connection.

Figure 81: Diagnostic LEDs

14.6 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



Navigation

- DCC000 QS.CSV v1.00a
  - About
  - Setup
  - View
  - User Messages
  - Diagnostics

Diagnostics

Captures

Full Diagnostic

Set capture period (max 1200 secs):

300

Start

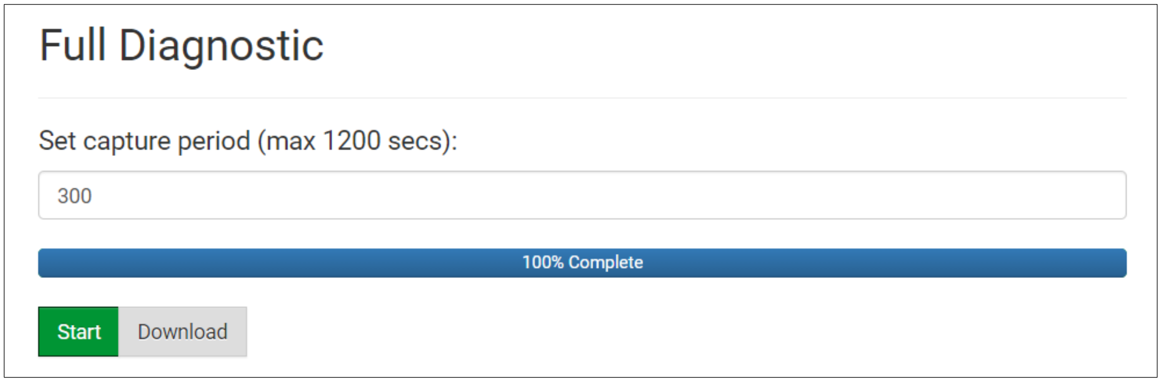
Serial Capture

Set capture period (max 1200 secs):

300

Start

- 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

Start Download

- 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).

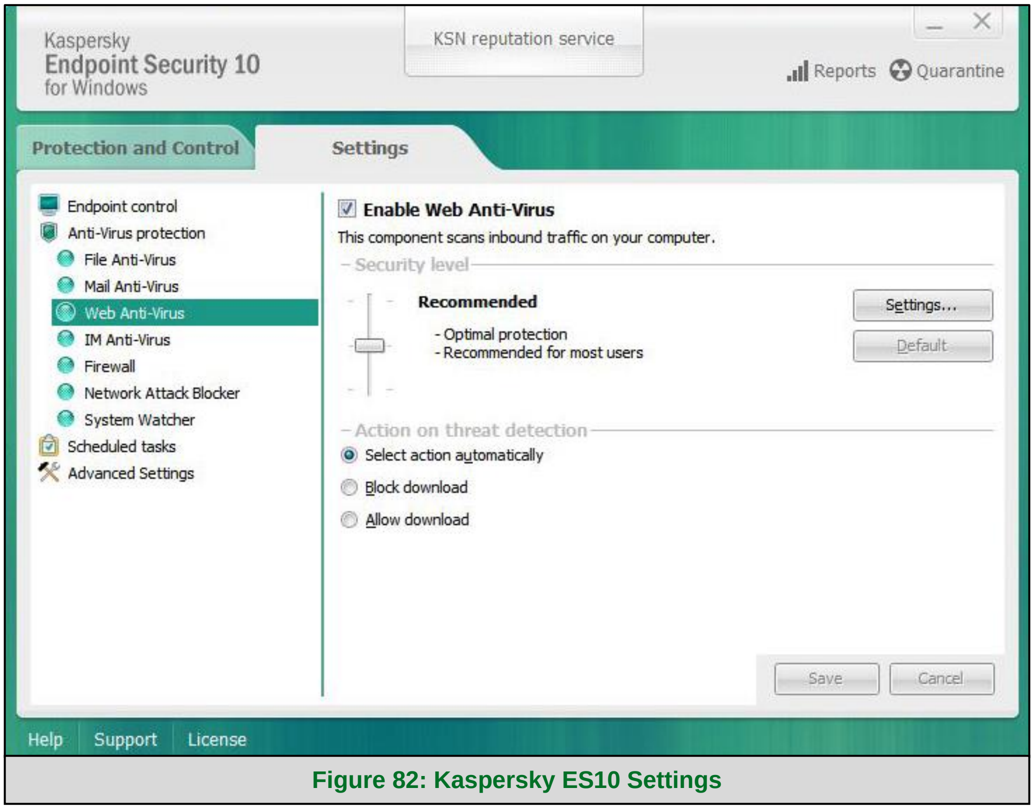
NOTE: Diagnostic captures of BACnet MS/TP communication are output in a ".PCAP" file extension which is compatible with Wireshark.

14.7 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 Grid.

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

To fix the problem, the BACnet IoT Gateway (http://192.168.100.85/* in **Figure 83**) 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

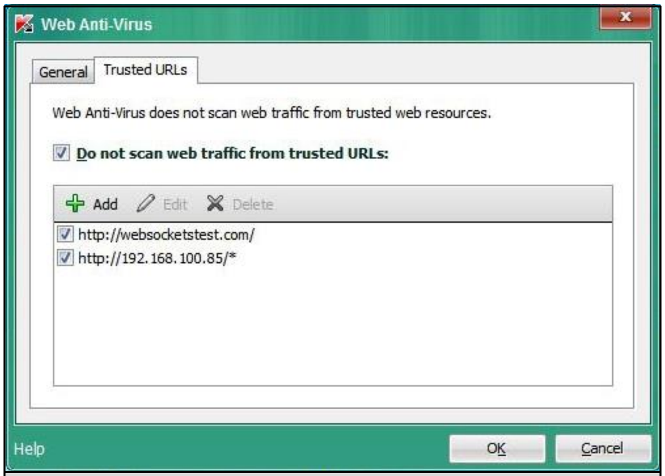
Action on threat detection

● Select action automatically

○ Block download

○ Allow download

Figure 82: Kaspersky ES10 Settings



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/*

Figure 83: Web Anti-Virus Trusted URLs

14.8 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

Figure 84: Wi-Fi & Cellular Signal Strength Listing

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

14.9 Factory Reset Instructions

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

14.10 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.

14.11 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

Figure 85: Cellular Provider APN

14.12 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.

14.13 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 9.1**)
2. Check that the Monitor View has saved data. (**Section 8.2**)
3. Check that the Log checkbox has been enabled. (**Section 8.2.2**)

15 Additional Information

15.1 Updating Firmware

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

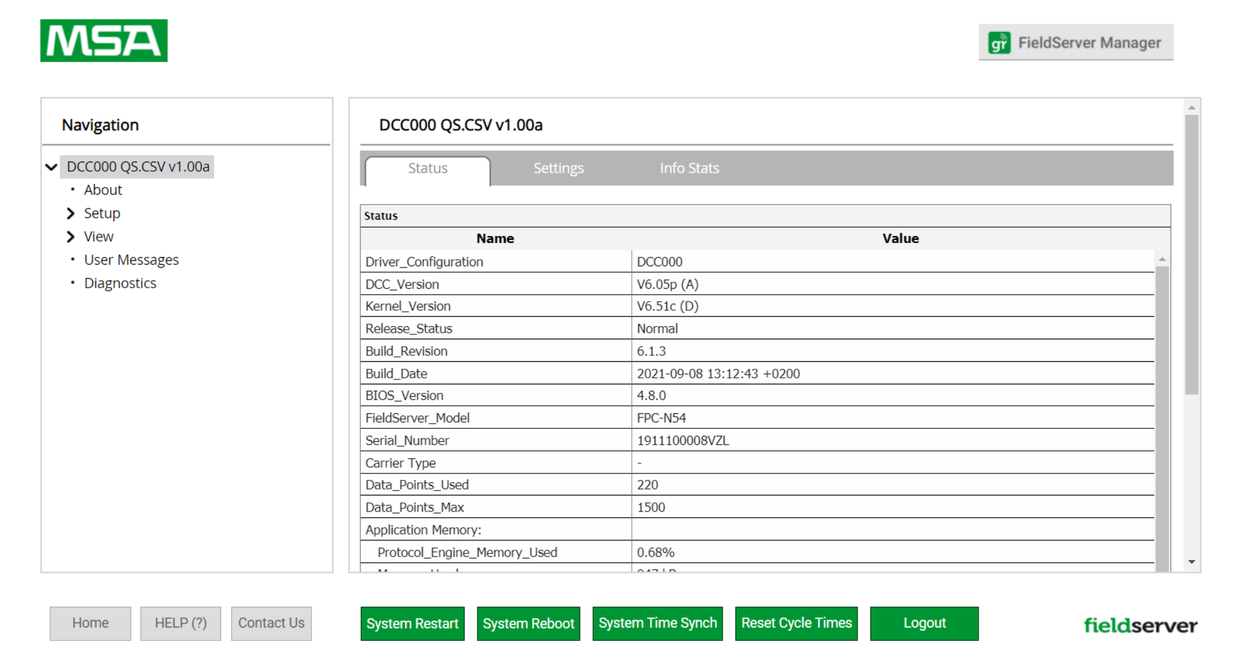
1. Extract and save the new file onto the local PC.
2. Open a web browser and type the IP Address of the FieldServer in the address bar.
   - Default IP Address is 192.168.2.101
   - Use the FS Toolbox utility if the IP Address is unknown (**Section** 14.2)
3. Click on the “Diagnostics & Debugging” button.
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 firmware file extracted in step 1.
6. Click on the orange “Submit” button.

   When the download is complete, click on the “System Restart” button.

15.2 Change Web Server Security Settings After Initial Setup

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

- From the FS-GUI page, click Setup in the Navigation panel.



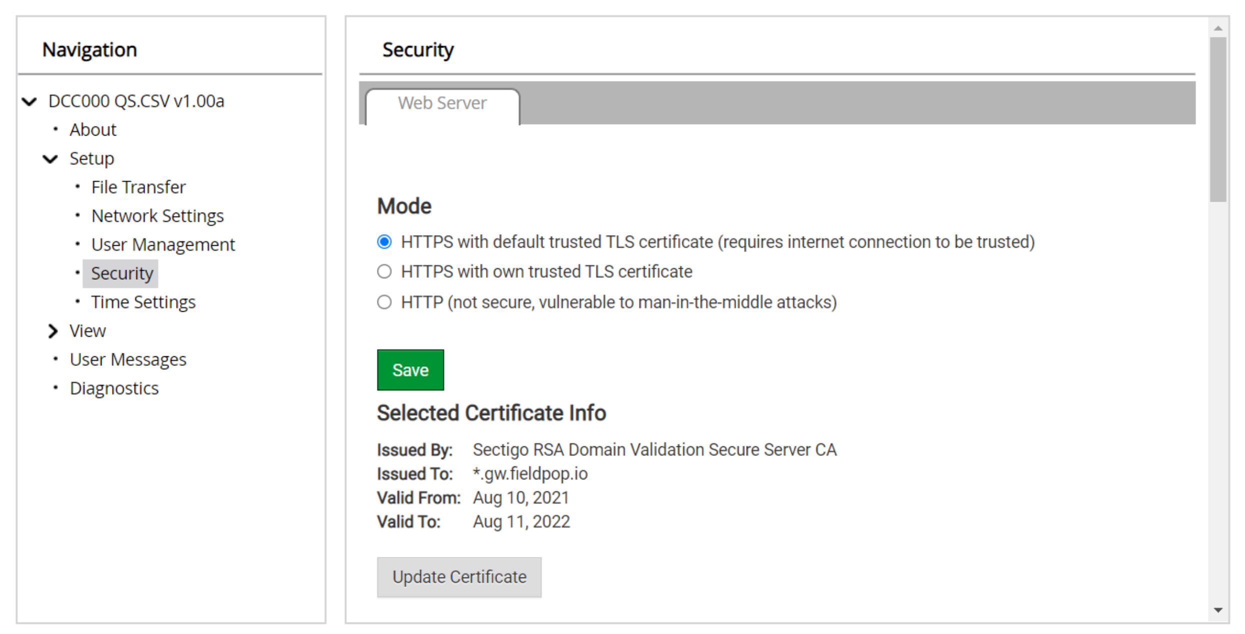
Status

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

Figure 86: FS-GUI Page

15.2.1 Change Security Mode

- Click Security in the Navigation panel.



Mode

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

○ HTTPS with own trusted TLS certificate

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

Selected Certificate Info

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

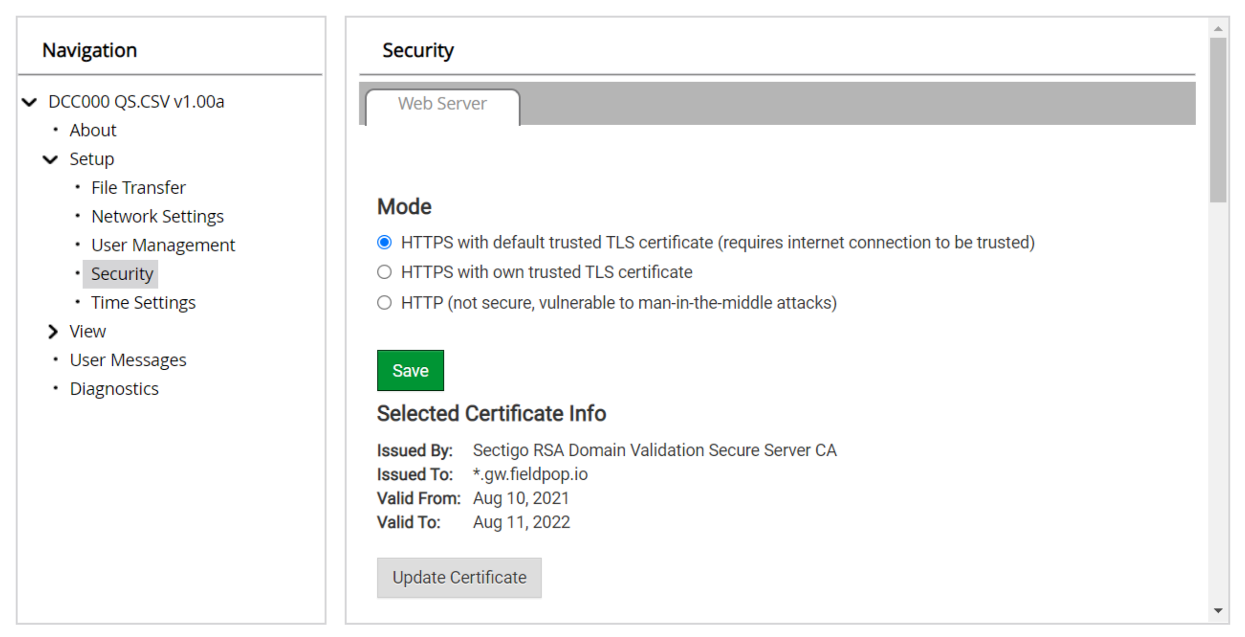
Figure 87: FS-GUI Security Setup

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

15.2.2 Edit the Certificate Loaded onto the FieldServer

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

- Click Security in the Navigation panel.



Mode

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

Selected Certificate Info

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

Figure 88: FS-GUI Security Setup – Certificate Loaded

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

15.3 Change User Management Settings

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

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

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

- Check that the Users tab is selected.

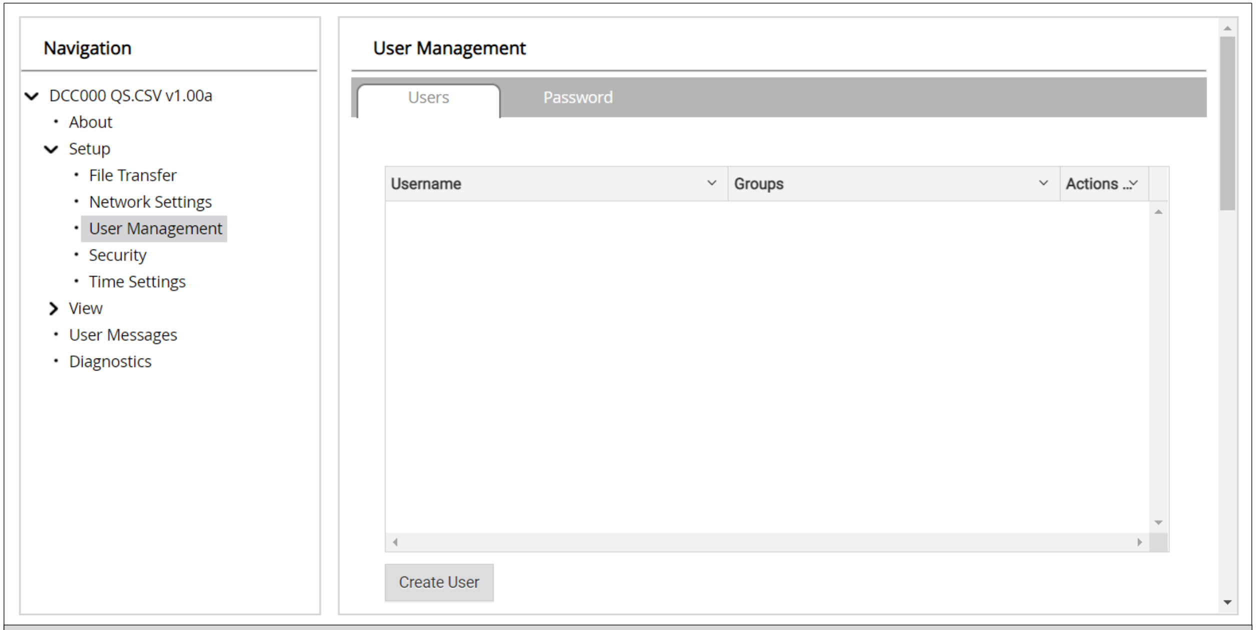


Figure 89: FS-GUI User Management

User Types:

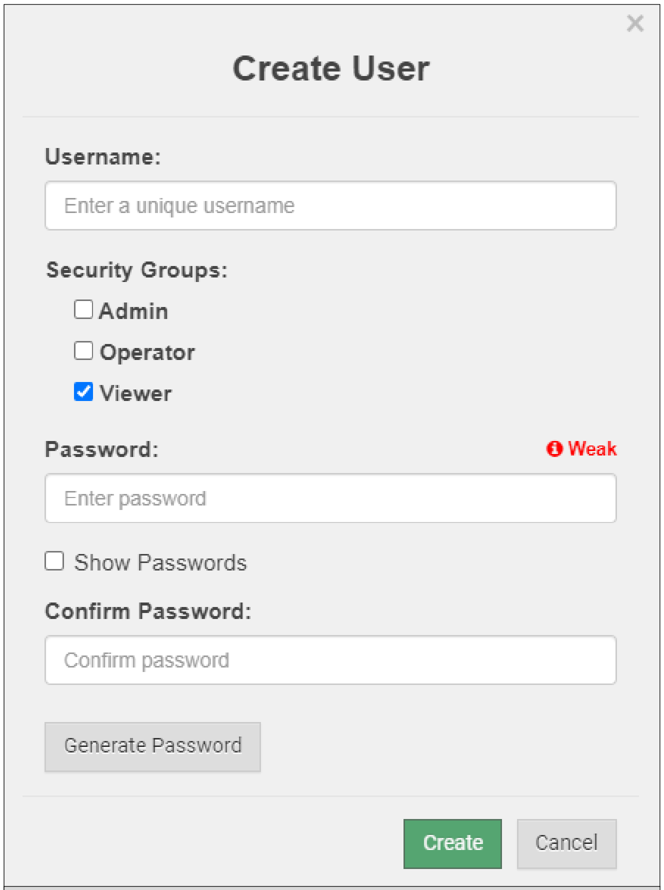
Admin – Can modify and view any settings on the FieldServer.

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

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

15.3.1 Create Users

- Click the Create User button.



Create User

Username:

Enter a unique username

Security Groups:

□ Admin

□ Operator

☑ Viewer

Password: Weak

Enter password

□ Show Passwords

Confirm Password:

Confirm password

Figure 90: Create User Window

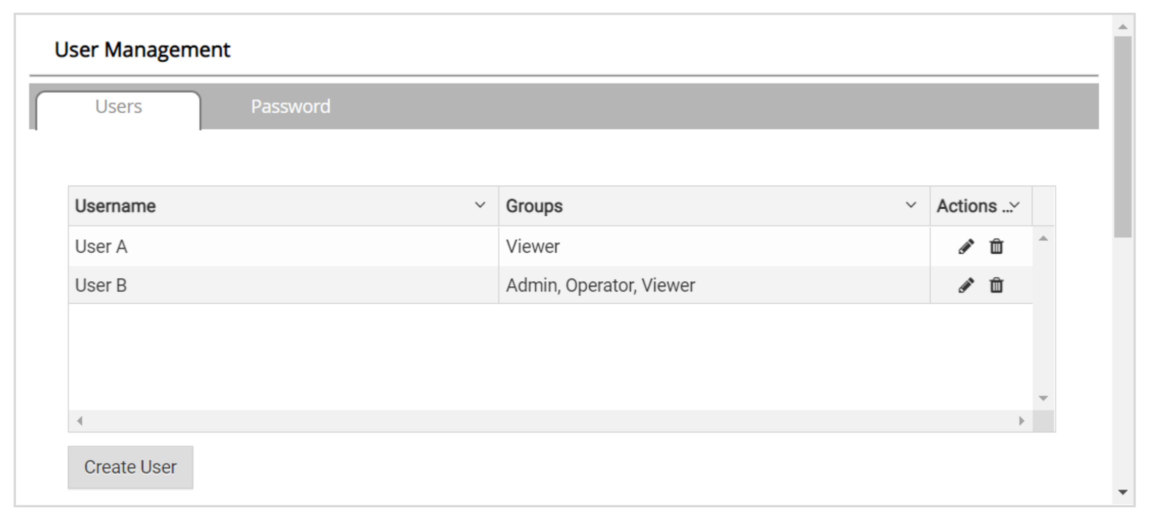
- Enter the new User fields: Name, Security Group and Password.
  - **User details are hashed and salted**

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.

15.3.2 Edit Users

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

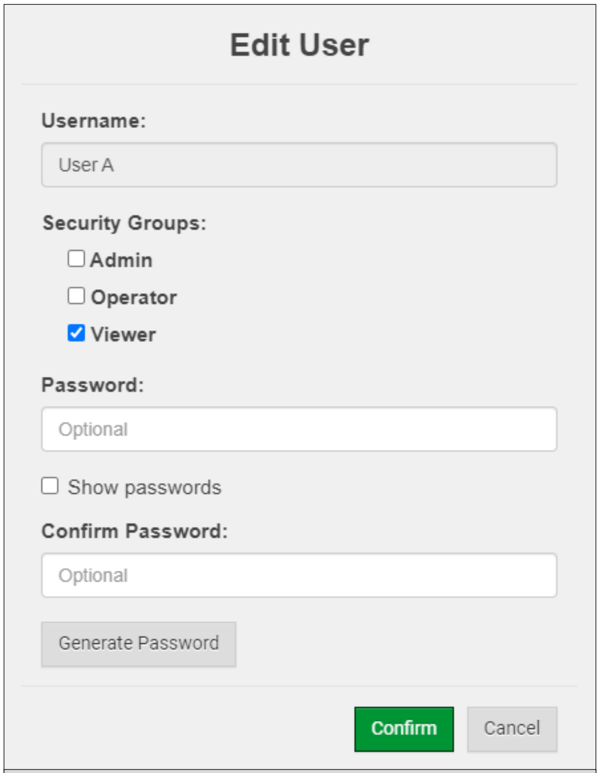


User Management

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

Figure 91: Setup Users

- 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

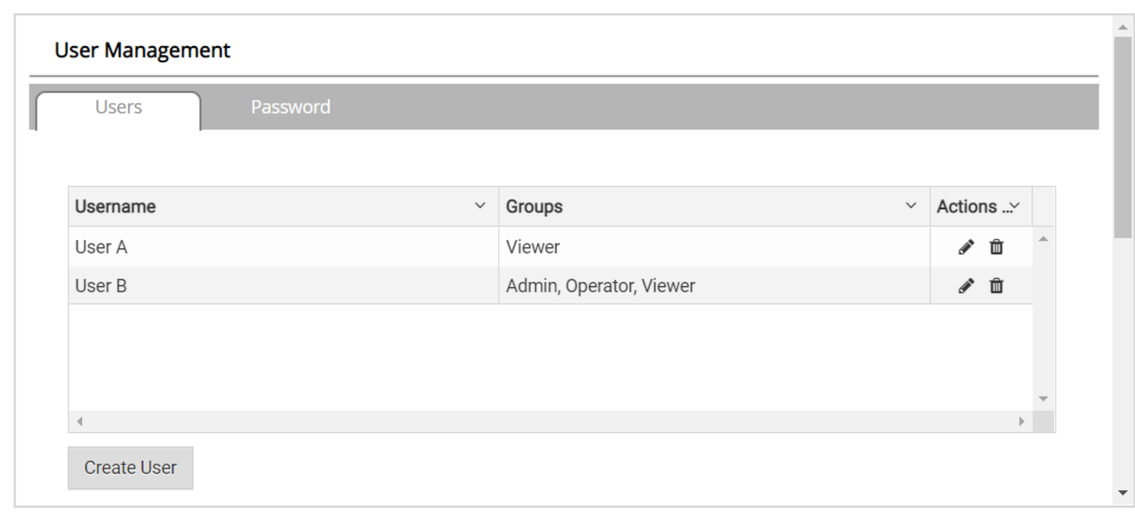
Confirm Password: Optional

Figure 92: Edit User Window

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

15.3.3 Delete Users

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

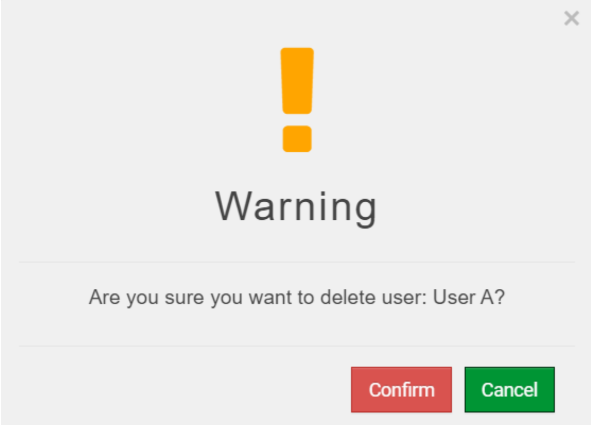


User Management

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

Figure 93: Setup Users

- When the warning message appears, click Confirm.



Warning

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

Figure 94: User Delete Warning

15.3.4 Change FieldServer Password

- Click the Password tab.

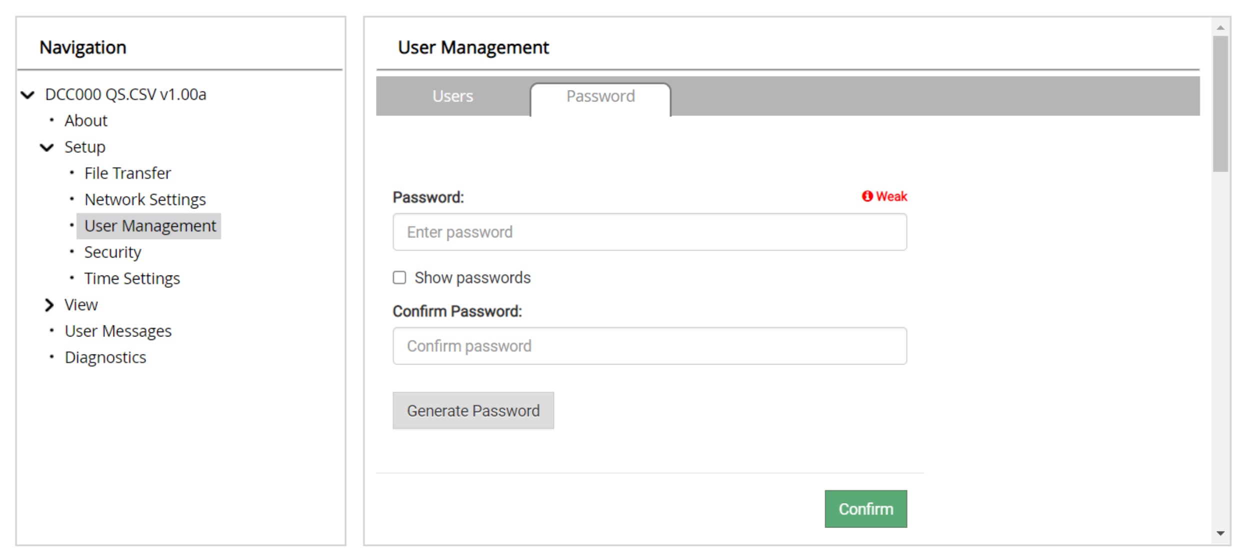


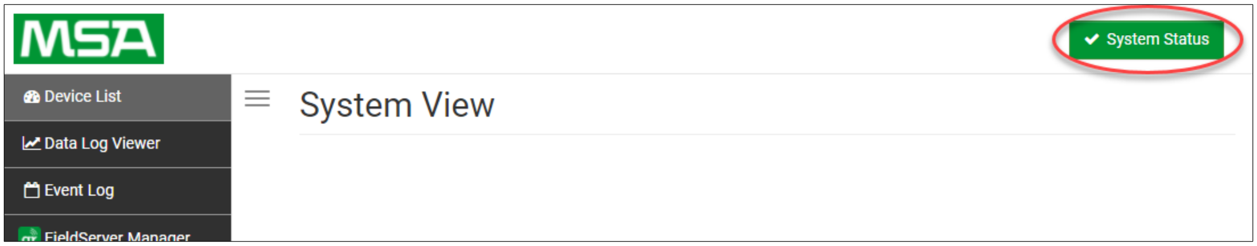
Figure 95: FieldServer Password Update via FS-GUI

- 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.

15.4 System Status Button

The System Status Button can be found on any page of the web apps. This shows the level of alert/functionality for the customer device. This is an agragate of the Web App page's resource usage upon the local PC or mobile device, the Grid connectivity and device alert level.



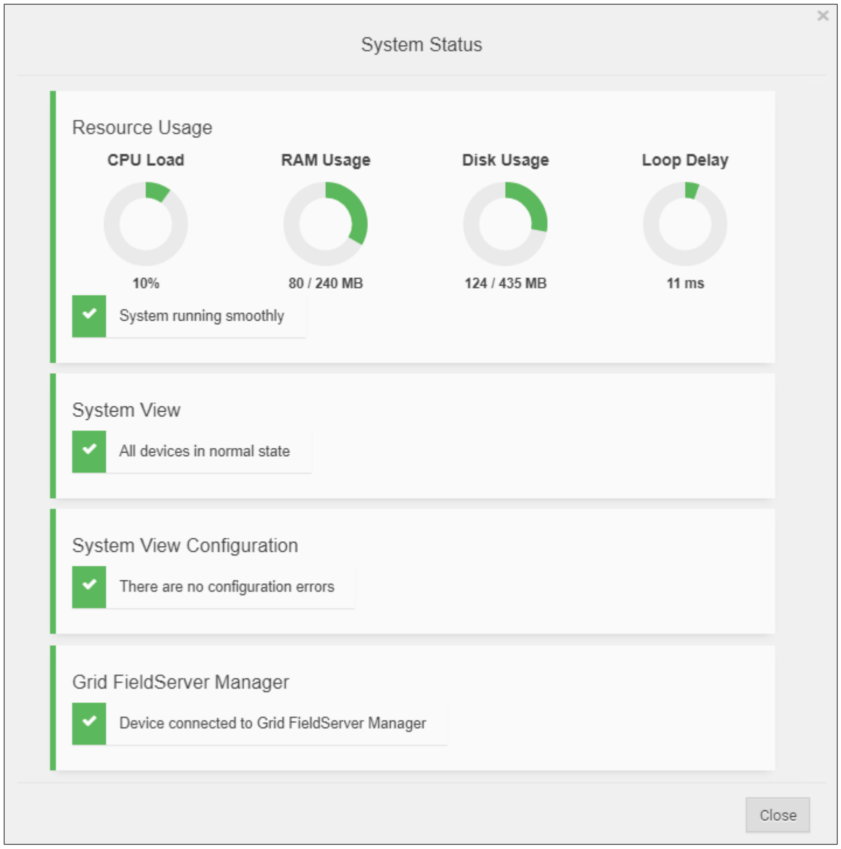
The color of the button represents the status of one to all three systems:

Green – Normal status

Yellow – Warning status

Red – Alarm status

Click on the System Status Button to open the System Status window, showing more details on the status of each system.



System Status

Resource Usage

CPU Load	RAM Usage	Disk Usage	Loop Delay
10%	80 / 240 MB	124 / 435 MB	11 ms

✓ System running smoothly

System View

✓ All devices in normal state

System View Configuration

✓ There are no configuration errors

Grid FieldServer Manager

✓ Device connected to Grid FieldServer Manager

NOTE: If it was selected to opt out of the Grid, the cloud status will not show in the System Status window. This means the status will show as green even if the gateway is not connected to the Grid.