



Operating Manual BACnet Router Start-up Guide



Revision: 3.C

Document No.: T18625

Print Spec: 10000005389 (F)



fieldserver

MSA Safety
1991 Tarob Court
Milpitas, CA 95035

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

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

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

Contents

1	BACnet Router Description	5
2	Equipment Setup	6
2.1	Mounting	6
2.2	Physical Dimensions	7
3	Installation	8
3.1	Connecting the R1 & R2 Ports	8
3.1.1	Wiring	8
3.2	10/100 Ethernet Connection Port	9
4	Power up the Gateway	10
5	Connecting to the BACnet Router	11
5.1	Using the FieldServer Toolbox to Discover and Connect to the BACnet Router	11
5.2	Using a Web Browser	11
6	Setup Web Server Security	12
6.1	Login to the FieldServer	12
6.2	Select the Security Mode	14
6.2.1	HTTPS with Own Trusted TLS Certificate	15
6.2.2	HTTPS with Default Untrusted Self-Signed TLS Certificate or HTTP with Built-in Payload Encryption	15
7	Setup Network	16
7.1	Ethernet 1	16
7.2	Routing Settings	17
8	Configuring the BACnet Router	18
8.1	Navigate to the BACnet Router Settings	18
8.2	BACnet Router Settings	19
8.2.1	Button Functions	19
8.2.2	Multiple Connections	20
8.2.3	BACnet Device	20
8.2.4	BACnet/IP	21
8.2.5	BACnet MS/TP, BACnet Ethernet and BACnet Explorer	22
8.3	Router Diagnostics	23
9	BACnet Explorer	24
9.1	Discover the Device List	25
9.2	View Device Details and Explore Points/Parameters	26
9.2.1	Edit the Present Value Field	29
10	MSA Grid - FieldSever Manager Setup	31
10.1	Create a New FieldServer Manager Account	31
10.2	Login to the FieldServer Manager	38
11	Troubleshooting	40
11.1	Tooltips	40
11.2	Taking a FieldServer Diagnostic Capture	41
11.3	Factory Reset Instructions	42

11.4	Internet Browser Software Support	42
12	Additional Information	43
12.1	Change Web Server Security Settings After Initial Setup	43
12.1.1	Change Security Mode	44
12.1.2	Edit the Certificate Loaded onto the FieldServer	45
12.2	Change User Management Settings	46
12.2.1	Create Users	47
12.2.2	Edit Users	48
12.2.3	Delete Users	49
12.2.4	Change FieldServer Password	50
12.3	Specifications	51
13	Limited 2 Year Warranty	52

1 BACnet Router Description

The BACnet Router provides stand-alone routing between BACnet networks such as BACnet/IP, BACnet Ethernet, and BACnet MS/TP – thereby allowing the system integrator to mix BACnet network technologies within a single BACnet internetwork. There are three physical communication ports on the BAS Router. One is a 10/100 Mbps Ethernet port and the other two are RS-485 MS/TP ports. Configuration is accomplished via a web page.

The BACnet Router is cloud ready and connects with the Grid MSA Safety's FieldServer cloud platform.

NOTE: For MSA Grid – FieldServer Manager information, refer to the [MSA Grid - FieldServer Manager Start-up Guide](#) online through the MSA website.

NOTE: The latest versions of instruction manuals, driver manuals, configuration manuals and support utilities are available online through the [MSA FieldServer webpage](#).

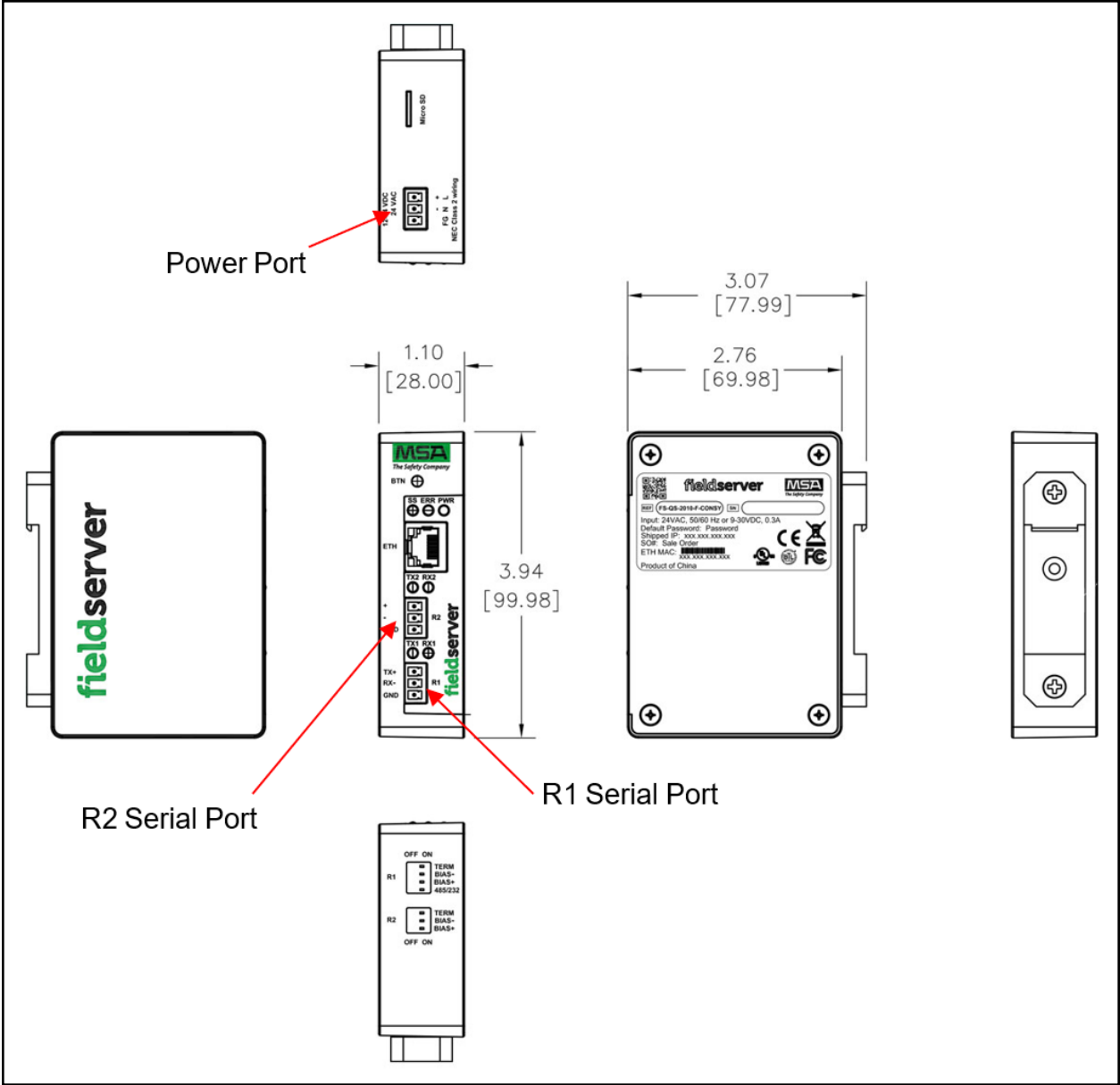
2 Equipment Setup

2.1 Mounting

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



2.2 Physical Dimensions



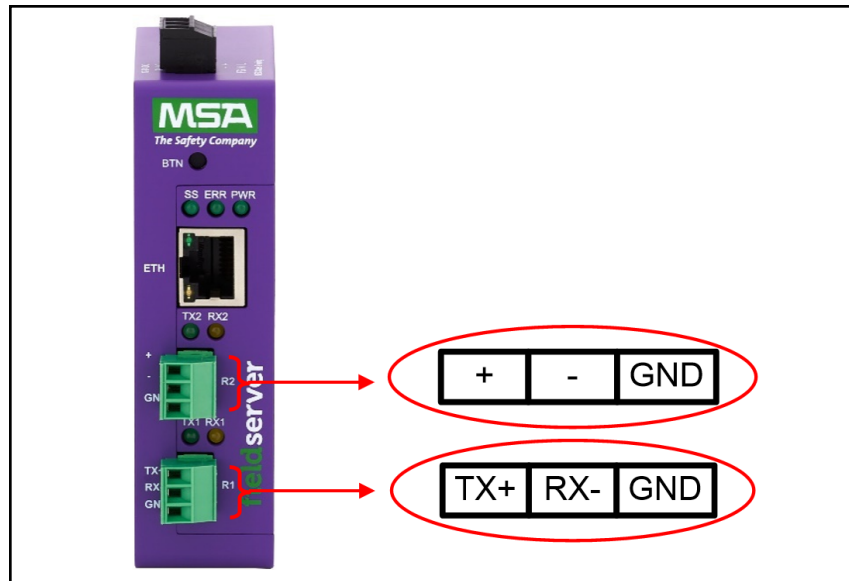
3 Installation

3.1 Connecting the R1 & R2 Ports

The R1 and R2 Ports are RS-485.

NOTE: For the R1 Port, 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(s) as shown below.



The following baud rates are supported:

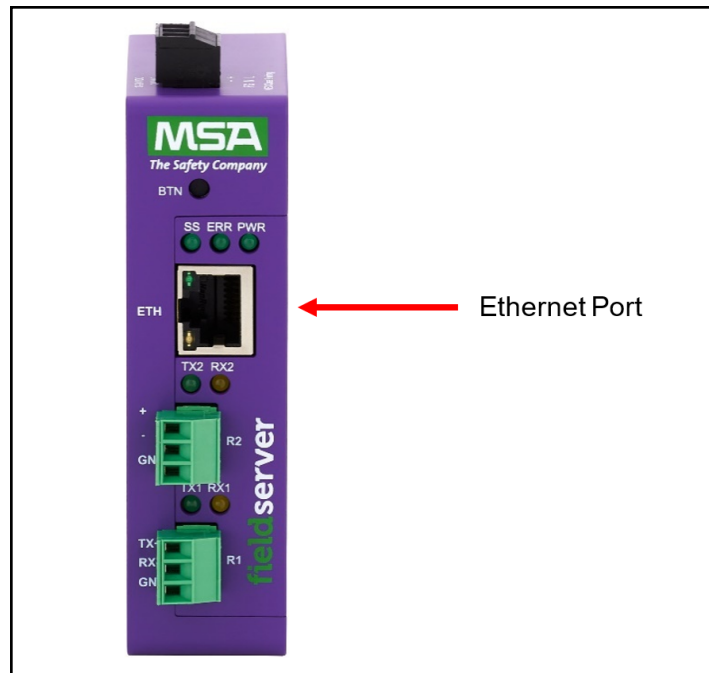
9600, 19200, 38400, 76800

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 10/100 Ethernet Connection Port



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

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

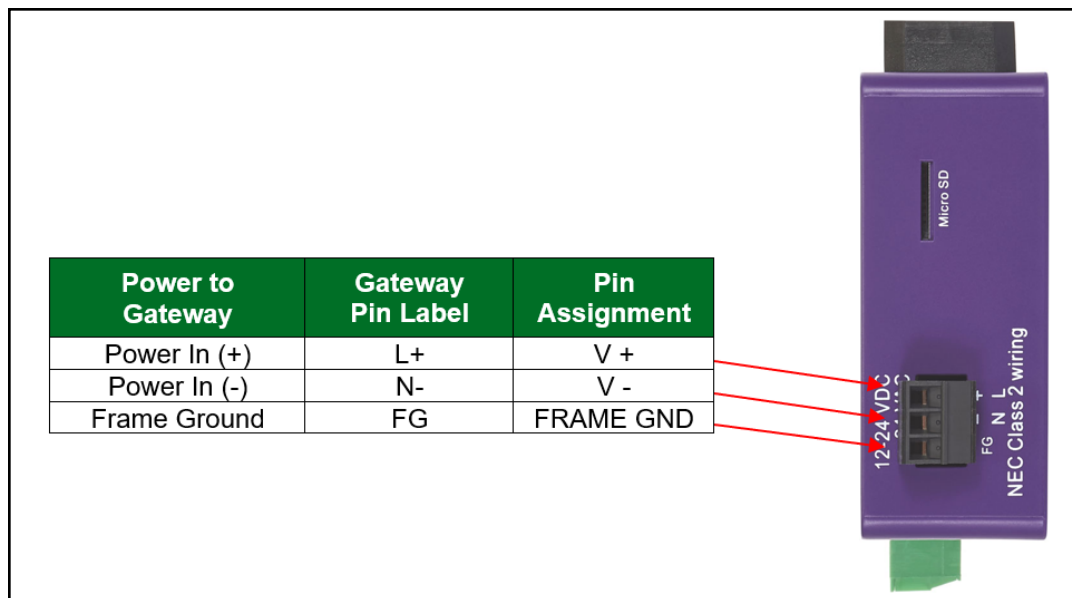
4 Power up the Gateway

Check power requirements in the table below:

Power Requirement for BACnet Router External Gateway		
	Current Draw Type	
BACnet Router Family	12VDC	24VDC/AC
FS-EXPLORER-BAC2 (Typical)	250mA	125mA
NOTE: These values are 'nominal' and a safety margin should be added to the power supply of the host system. A safety margin of 25% is recommended.		

Apply power to the BACnet Router as shown below. Ensure that the power supply used complies with the specifications provided in **Section** .

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

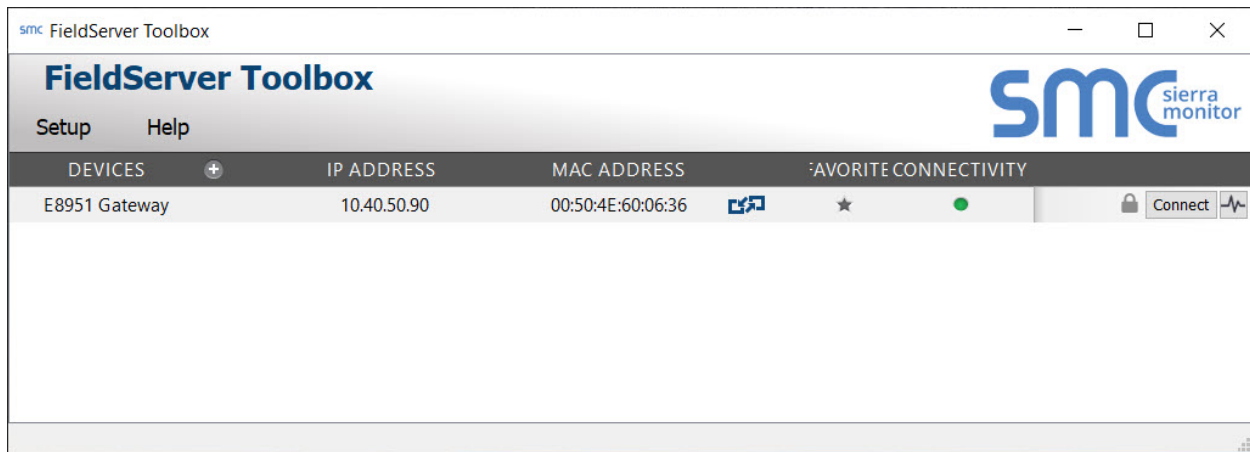


5 Connecting to the BACnet Router

5.1 Using the FieldServer Toolbox to Discover and Connect to the BACnet Router

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

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



5.2 Using a Web Browser

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

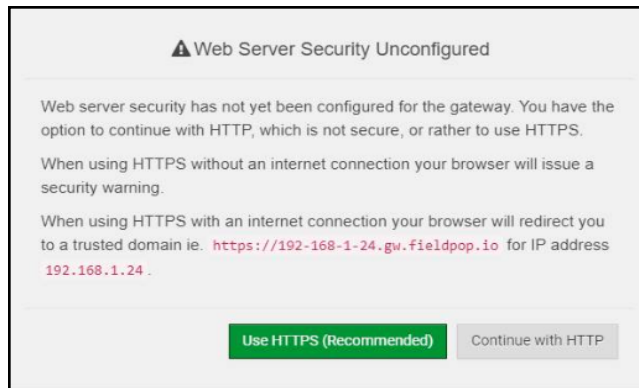
NOTE: Check Section [11.4 Internet Browser Software Support](#) for supported browsers.

6 Setup Web Server Security

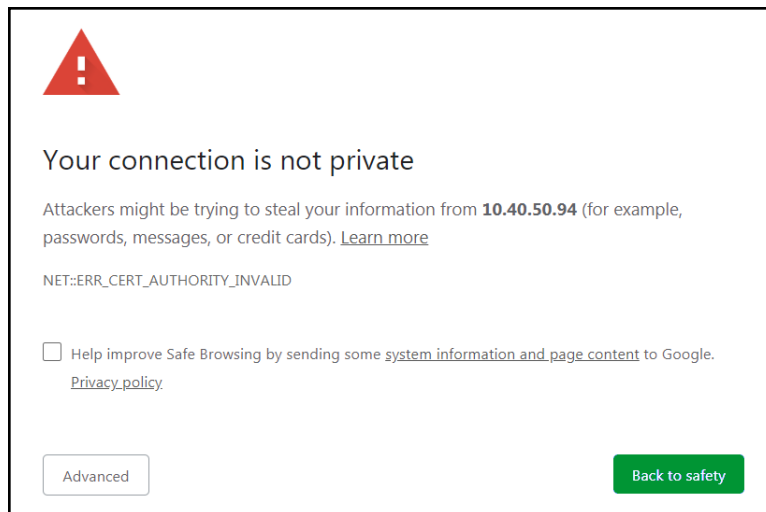
6.1 Login to the FieldServer

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

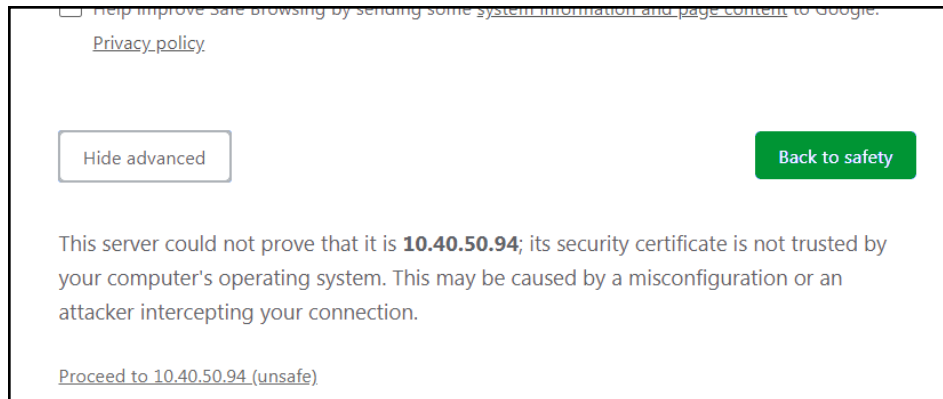
- When the Web Server Security Unconfigured window appears, read the text and choose whether to move forward with HTTPS or HTTP.



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

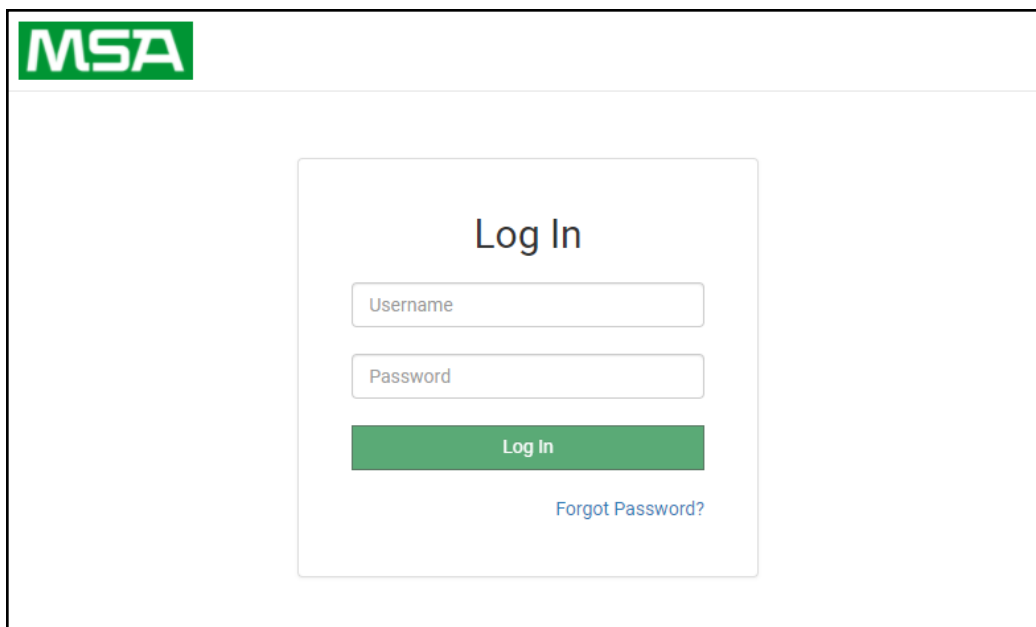


- Additional text will expand below the warning, click the underlined text to go to the IP Address. In the example below this text is “[Proceed to 10.40.50.94 \(unsafe\)](#)”.



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

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




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

NOTE: To create individual user logins, go to Section [12.2 Change User Management Settings](#).

6.2 Select the Security Mode

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



Web server security is not configured

Please select the web security profile from the options below.

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

Mode

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

Save

NOTE: Cookies are used for authentication.

NOTE: To change the web server security mode after initial setup, go to [Section 12.1 Change Web Server Security Settings After Initial Setup](#).

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

6.2.1 HTTPS with Own Trusted TLS Certificate

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

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

Certificate

```
XzyMbQZFIRuJZJPe7CTHLcHOrHlOwoUFoVTaBMYd4d6VGdNklKazByWKcNOL7mrX
A4lBAQBfM+IPvOx3T/47VEmaiXqE3bx3zEuBFJ6pWPlw7LHf2r2ZoHw+9xb+aNMU
dVYAelhBMTMsn2ERvQVp0xj3psSv2EJyKXS1bOYNRLsq7UzpwuAdT/Wy3o6vUM5
K+Cwf9qEoQ0LuxDZTIECt67MkcHMiuFi5pk7TRicHnQF/sfOAYOulduHOy9exlk9
FmHfVDIZt/cJUaF+e74EuSph+qEr0lQo2wvmhyc7L22UXse1NoOfU2Zg0Eu1VWtu
JRryaMWIRFEWuuzMGZtKFWVC+8q2JQsVcgiRWM7naoblEhOCMH+sKHJMCxDoXGt
vtZjpZUoAL51YXxWSVcyZdGiAP5e
-----END CERTIFICATE-----
```

Private Key

```
sHB0zZoHr4YQSDk2BbYVzbl0LDuKtc8+JiO3ooGjoTuHnqkeAj/fKfbTAsKeAzw
gKQe+H5UQNk0bdvZfOJrm6daDK2vVDmR5k+jUUhEj5N49uplroB97MQgYotzqfT+
THlbpq5t1SIK617k04ObKmHF5l8fck+ru545sVmpeeZh0m5j5SURYAZMvbq5daCu
J4l5NIihbEvxRF4UK41ZDMCvujopCkUWrb1a/3XXnDnM2K9xyz2wze998D6Wk46
+7aOFY9F+7j5lJmnkoS3GYtwCyH5jP+mPP1K6RnuiD019wvGPb4dtN/RTnfd0eF
GYeVSkI9fxkxDOFtdWRZbM/rPjn4tmO1Xf8HqONVN1x/iaMynOXG4cukoi4+VO
u0rZaUESlI2zNkfrn7fAASm5NBWg202Cy9lAYnuujs3aALl5uGBEEKa62oTMxlzx
-----END RSA PRIVATE KEY-----
```

Private Key Passphrase

Save

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

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

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

7 Setup Network

7.1 Ethernet 1

To change the IP Settings, follow these instructions:

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

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

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

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


The screenshot displays the MSA FieldServer Manager web interface. On the left is a dark sidebar with the MSA logo at the top and a menu containing: Bacnet Router, Bacnet Explorer, Network Settings, Router Diagnostics, FieldServer Manager (highlighted with a green icon), About, and Logout. The main content area is titled 'ETH 1' and 'Routing'. It features a checkbox for 'Enable DHCP' which is currently unchecked. Below this are input fields for 'IP Address' (10.40.50.74), 'Netmask' (255.255.255.0), 'Gateway' (10.40.50.1), 'Domain Name Server 1 (Optional)' (8.8.8.8), and 'Domain Name Server 2 (Optional)' (8.8.4.4). At the bottom of this section are 'Cancel' and 'Save' buttons. To the right of the configuration fields is a 'Network Status' panel showing: Connection Status (Connected with a green checkmark), MAC Address (00:50:4e:60:16:49), Ethernet Tx Msgs (49,920), Ethernet Rx Msgs (109,161), Ethernet Tx Msgs Dropped (0), and Ethernet Rx Msgs Dropped (0). The footer of the interface contains the text 'Copyright © MSA Safety - Diagnostics' and the 'fieldserver' logo.

7.2 Routing Settings

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





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

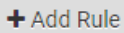
ETH 1

Routing 

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

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

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



Cancel

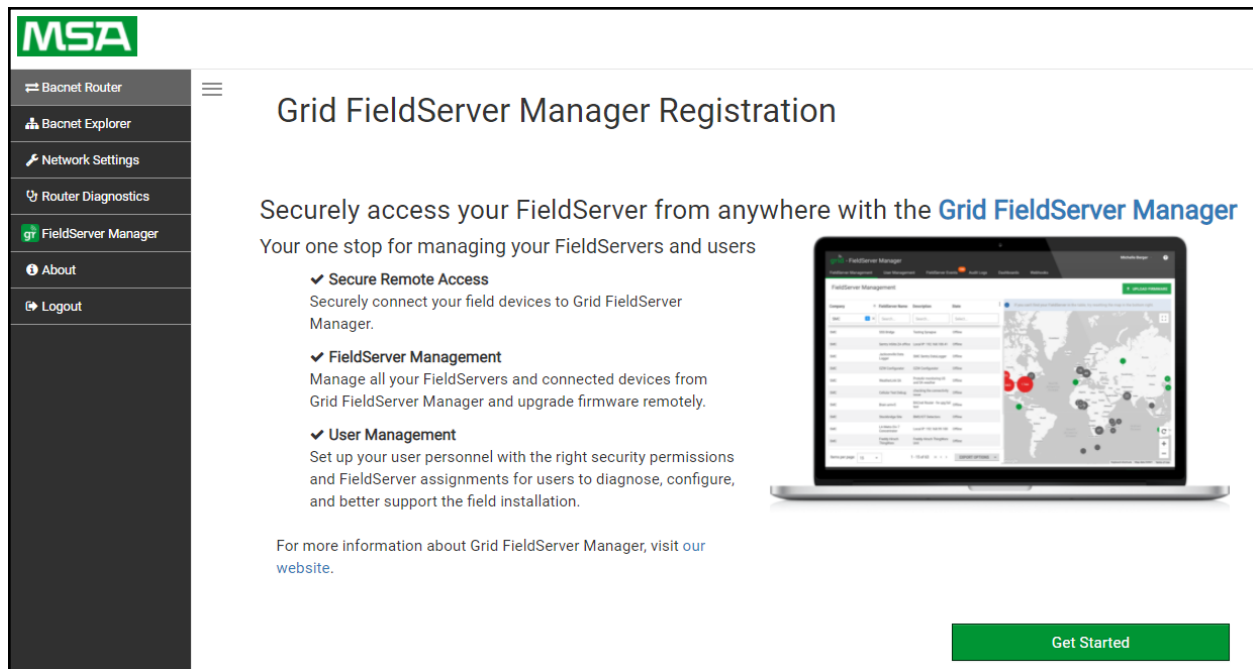
Save

There are unsaved settings

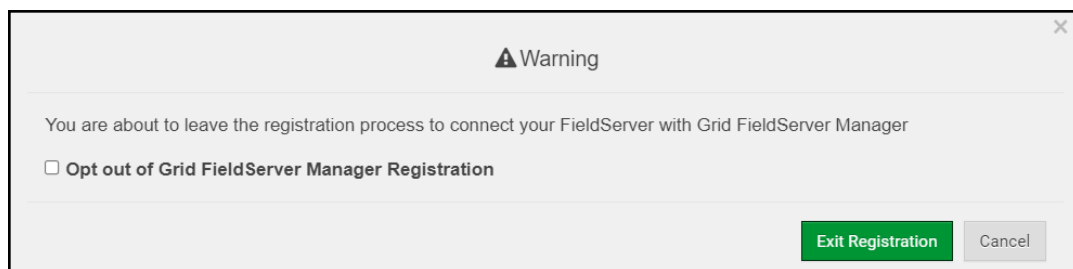
8 Configuring the BACnet Router

8.1 Navigate to the BACnet Router Settings

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



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



8.2 BACnet Router Settings

MSA

BACnet Router

BACnet Explorer

Network Settings

Router Diagnostics

FieldServer Manager

About

Logout

BACnet Device

Device Name: BACnet Router

Device Instance: 1000

Device Location: -

Device Connection: BACnet IP Wired 1

BACnet Ethernet

Enable: ☐

Network Number: 3

BACnet MSTP Settings

Max Info Frames: 50

Max Master: 127

BACnet MSTP R1

Enable: ☐

Network Number: 4

MAC Address: 0

Baud Rate: 38400

Token Usage Timeout (ms): 50

BACnet MSTP R2

Enable: ☐

BACnet IP Wired 1

Enable: ☒

Network Number: 1

IP Port: 47808

BACnet IP Wired 2

Enable: ☐

Network Number: 2

IP Port: 47809

BACnet IP BBMD

Save

Restart

Reload

Defaults

Status

Router is online

Log

Copyright © MSA Safety - Diagnostics

fieldserver

8.2.1 Button Functions

Save

Restart

Reload

Defaults

- **Save** – write the currently displayed settings to the device. A restart will be required to apply the updated settings.
- **Reload** – discard the currently displayed settings and reload the settings stored on the device. This will undo any unsaved edits.
- **Defaults** – discard the currently displayed settings and load default settings. This must still be saved and the device must be restarted for the default settings to be applied.
- **Restart** – restarts the device.

8.2.2 Multiple Connections

- **Network Number** – set up the BACnet network number for the connection. Legal values are 1-65534. Each network number must be unique across the entire BACnet internetwork. . All devices that are interconnected by the same IP network and that can reach one another through local IP broadcasts (including local IP broadcasts forwarded by BBMD) should be treated as a single BACnet network segment, and hence all routing ports connected to this segment should have the same globally unique network number.

NOTE: Each BACnet network segment, regardless of technology, must have a unique network number. For example, a single RS-485 MS/TP segment or BACnet/IP subnet, can each be regarded as a BACnet network segment. All routing ports that connect directly to the same segment should also assign the same globally unique network number to that segment.

- **Enable** – enable or disable the connection; note that BACnet/IP Primary is always enabled.

8.2.3 BACnet Device

BACnet Device

Device Name	<input type="text" value="BACnet Router"/>
Device Instance	<input type="text" value="1000"/>
Device Location	<input type="text" value="-"/>
Device Connection	<input type="text" value="BACnet IP Wired 1"/>

- **Device Instance** and **Device Name** – a BACnet Router must provide a Device Object. Configure its name and Instance Number here. Take care to select a Device Instance Number that is unique across the entire BACnet internetwork.
- **Device Location** – enter a location for the Device. The location may not contain any commas.
- **Device Connection** – select which connection to bond the BACnet device settings.

8.2.4 BACnet/IP

BACnet IP Wired 1

Enable ☒

Network Number

IP Port

BACnet IP Wired 2

Enable ☐

Network Number

IP Port

BACnet IP BBMD

Enable ☐

BBMD Connection

Public IP Address

Public IP Port

[Edit BDT](#)

- **IP Port** – the BACnet/IP default is 47808 (0xBAC0), but a different port number may be specified here.
- **IP Port** – this MUST be different to the IP Port used on the BACnet/IP Primary connection. Default is 47809 (0xBAC1).
- **BBMD Connection** – select which connection to bond the BACnet/IP BBMD settings.
- **Public IP Address** and **Port** – if the BBMD is being accessed across a NAT Router, then these values must be configured with the public IP Address and Port by which the BBMD can be reached from across the NAT Router. The Public IP Address and Port would also be used in the BDT of remote BBMD's that need to reach this BBMD across the NAT Router. If no NAT Router is being used, these fields can be left blank. For example, type into a Google browser "my IP Address" to see the local PC's Public IP Address.

8.2.5 BACnet MS/TP, BACnet Ethernet and BACnet Explorer

BACnet Ethernet

Enable ☐

Network Number

BACnet MSTP Settings

Max Info Frames

Max Master

BACnet MSTP R1

Enable ☐

Network Number

MAC Address

Baud Rate

Token Usage Timeout (ms)

BACnet MSTP R2

Enable ☐

Network Number

MAC Address

Baud Rate

Token Usage Timeout (ms)


BACnet Explorer

Network Number

- **Max Info Frames** – the number of transactions the Router may initiate while it has the MS/TP token. Default is 50.
- **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.
- **MAC Address** – legal values are 0 to 127, must be unique on the physical network.
- **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.

8.3 Router Diagnostics

By clicking on the Router Diagnostics tab all the connection communication details can be viewed to ensure the BACnet Router is working correctly.



Bacnet Router

Bacnet Explorer

Network Settings

Router Diagnostics

FieldServer Manager

About

Logout

ETH1 - BACnet IP Wired 1

Network Number	1	
Info Statistics	Messages Sent	270
	Messages Received	280
Error Statistics	Total Errors	0

Routing Table

DNET	MAC Address	Status
5	10.40.51.113:47808	Available
6	10.40.50.80:47808	Available
50	10.40.50.103:47808	Available
181	10.40.50.181:47808	Available
1100	10.40.50.73:47808	Available
1200	10.40.50.73:47808	Available
50001	10.40.50.88:47808	Available
50003	10.40.50.88:47808	Available
60003	10.40.50.116:47808	Available

ETH1 - BACnet Explorer 47800

Network Number	7	
Info Statistics	Messages Sent	258
	Messages Received	246
Error Statistics	Total Errors	0

Routing Table is empty

Copyright © MSA Safety - Diagnostics

fieldserver

9 BACnet Explorer

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

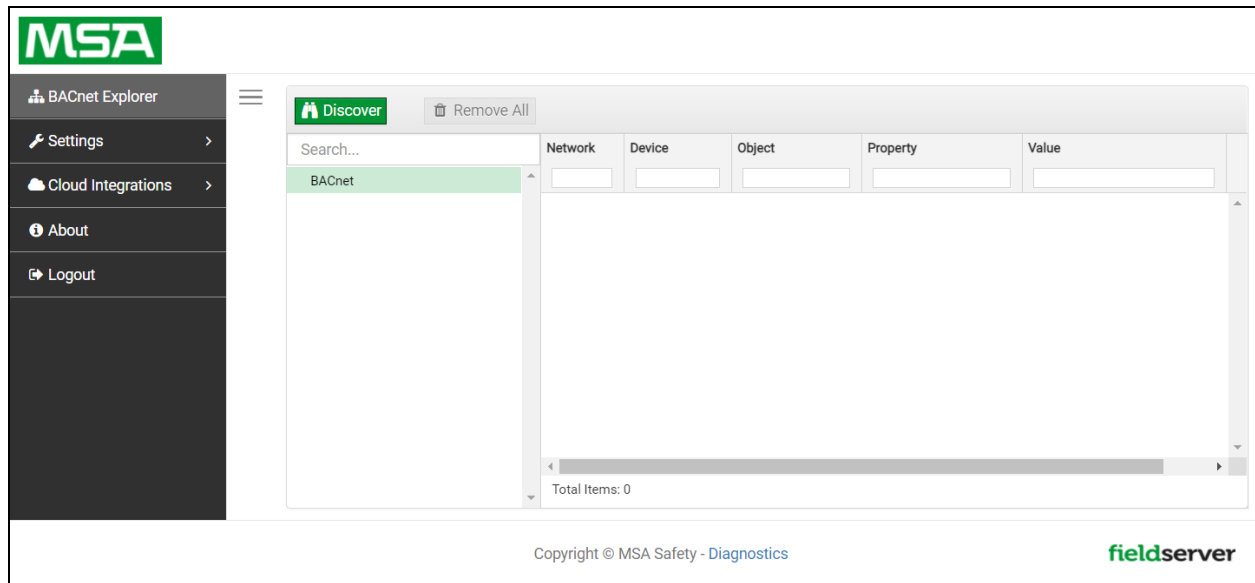
- To access the embedded BACnet Explorer click the BACnet Explorer tab.


The screenshot displays the MSA BACnet Explorer configuration interface. On the left is a dark sidebar with the MSA logo at the top and a menu containing: BACnet Router, BACnet Explorer (selected), Network Settings, Router Diagnostics, FieldServer Manager, About, and Logout. The main content area is divided into several sections:
1. **BACnet Device**: Fields for Device Name (BACnet Router), Device Instance (1000), Device Location (-), and Device Connection (BACnet IP Wired 1).
2. **BACnet IP Wired 1**: Includes an 'Enable' checkbox (checked), Network Number (1), and IP Port (47808).
3. **BACnet IP Wired 2**: Includes an 'Enable' checkbox (unchecked), Network Number (2), and IP Port (47809).
4. **BACnet IP BBMD**: A section header with no visible fields.
5. **BACnet Ethernet**: Includes an 'Enable' checkbox (unchecked) and Network Number (3).
6. **BACnet MSTP Settings**: Includes Max Info Frames (50) and Max Master (127).
7. **BACnet MSTP R1**: Includes an 'Enable' checkbox (unchecked), Network Number (4), MAC Address (0), Baud Rate (38400), and Token Usage Timeout (50).
8. **BACnet MSTP R2**: Includes an 'Enable' checkbox (unchecked).
On the right side of the interface, there are control buttons: 'Save' and 'Restart' in green, and 'Reload' and 'Defaults' in grey. Below these is a 'Status' box showing 'Router is online' and a 'Log' box. The footer contains the copyright notice 'Copyright © MSA Safety - Diagnostics' and the 'fieldserver' logo.

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

9.1 Discover the Device List

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



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

The 'Discover' window is a modal dialog with a title bar containing a binocular icon and the word 'Discover'. It is divided into two sections: 'Devices' and 'Networks'. In the 'Devices' section, there is an unchecked checkbox for 'Discover All Devices' and two input fields labeled 'From device' (containing '0') and 'to device' (containing '4194303'). In the 'Networks' section, there is an unchecked checkbox for 'Discover All Networks' and an input field labeled 'Discover Specific Network' (containing '0'). At the bottom right are 'Cancel' and 'Discover' buttons.

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

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

Search...	Device	Object	Property	Value	Monitor
+ 1400					
- network:6					
+ 101 (New_BACnet_Node)	1 (FAP_1)	device:1 (FAP_1)	max-apdu-length-accepted	1458	Off
- 102 (temp)	1 (FAP_1)	device:1 (FAP_1)	object-name	FAP_1	Off
device:102 (temp)	1 (FAP_1)	device:1 (FAP_1)	vendor-identifier	37	Off
- network:50	18100 (BASRTLX-B-01C6AF)	device:18100 (BASRTLX-B-01C...	max-apdu-length-accepted	1476	Off
+ 50002	18100 (BASRTLX-B-01C6AF)	device:18100 (BASRTLX-B-01C...	object-name	BASRTLX-B-01C6AF	Off
+ 50022 (1020_22)	18100 (BASRTLX-B-01C6AF)	device:18100 (BASRTLX-B-01C...	vendor-identifier	245	Off
+ 50033 (6020_33)	50001	device:50001	max-apdu-length-accepted	1458	Off
- network:50001	50001	device:50001	vendor-identifier	37	Off
+ 50000 (Dev_IP)	54321 (SENTRY_BAC_11)	device:54321 (SENTRY_BAC_11)	max-apdu-length-accepted	1458	Off
- network:60001	54321 (SENTRY_BAC_11)	device:54321 (SENTRY_BAC_11)	object-name	SENTRY_BAC_11	Off
+ 1 (FAP_1)	54321 (SENTRY_BAC_11)	device:54321 (SENTRY_BAC_11)	vendor-identifier	37	Off
+ 18100 (BASRTLX-B-01C6AF)	259645 (WeatherLink_1)	device:259645 (WeatherLink_1)	max-apdu-length-accepted	1458	Off
+ 50001	259645 (WeatherLink_1)	device:259645 (WeatherLink_1)	object-name	WeatherLink_1	Off
+ 54321 (SENTRY_BAC_11)	259645 (WeatherLink_1)	device:259645 (WeatherLink_1)	vendor-identifier	37	Off
+ 259645 (WeatherLink_1)					


Total Items: 42 (Showing Items: 14)

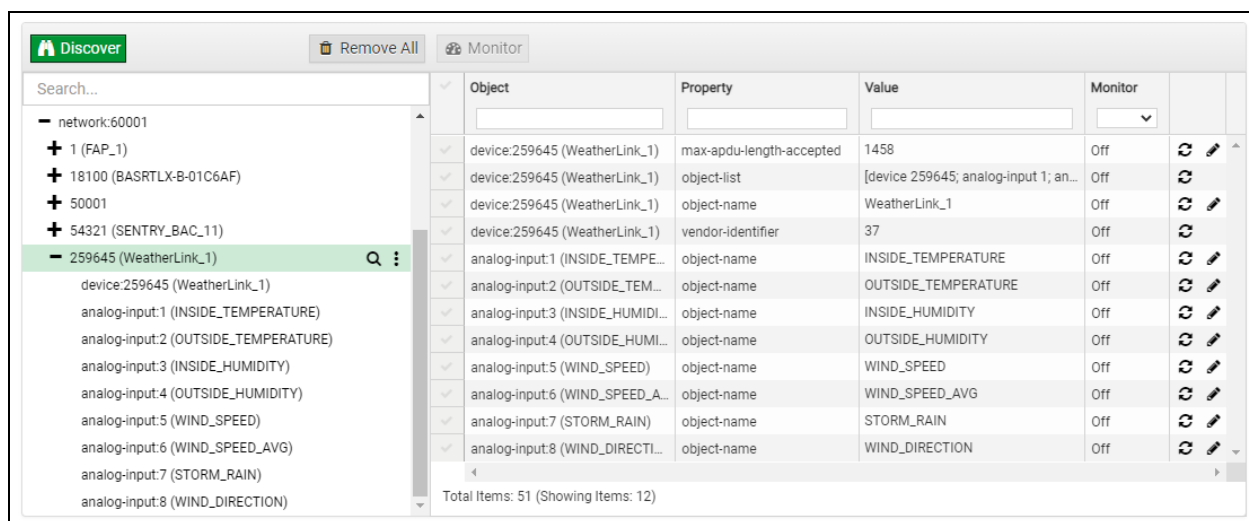
9.2 View Device Details and Explore Points/Parameters

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

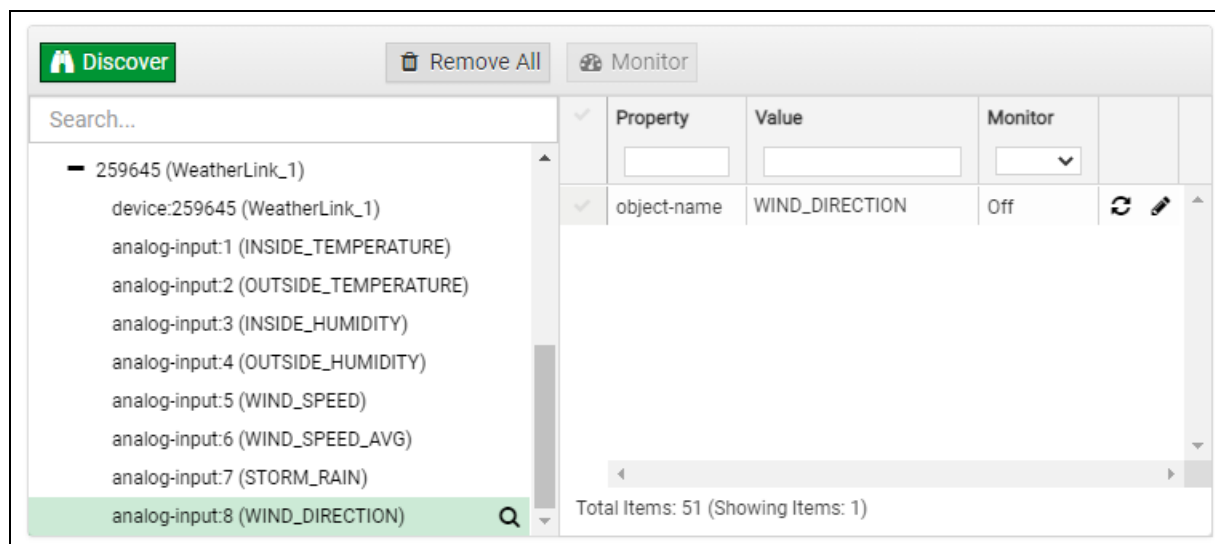
Search...	Object	Property	Value	Monitor
- BACnet				
+ network:4	device:259645 (WeatherLink_1)	max-apdu-length-accepted	1458	Off
+ network:5	device:259645 (WeatherLink_1)	object-name	WeatherLink_1	Off
+ network:6	device:259645 (WeatherLink_1)	vendor-identifier	37	Off
+ network:50				
+ network:50001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

Total Items: 42 (Showing Items: 3)

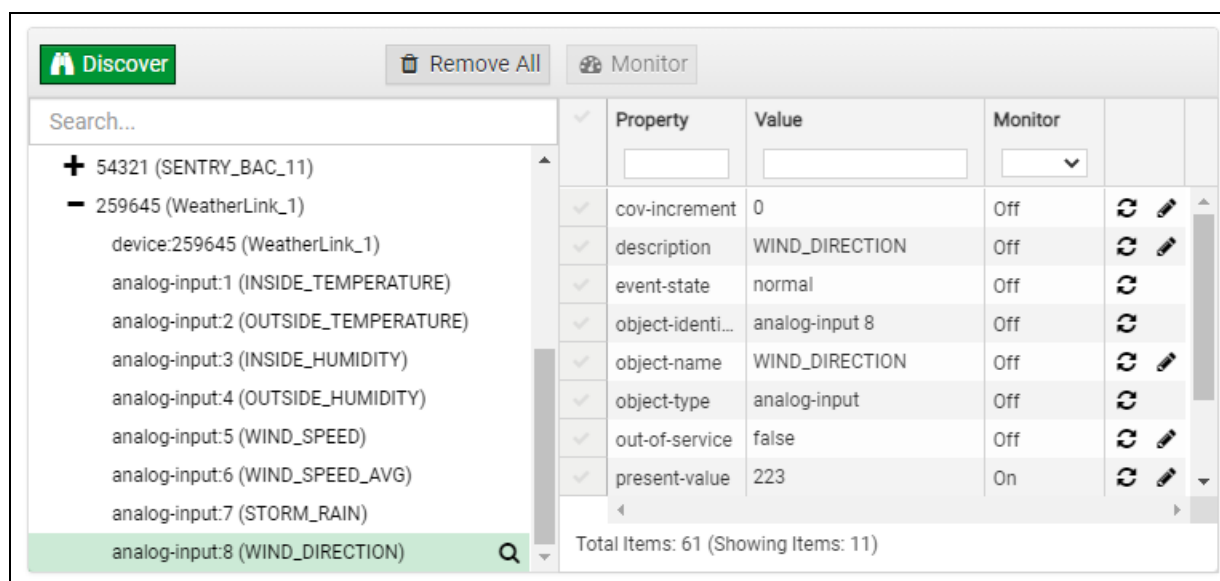
- To view the full details of a device, highlight the device directly (in the image below – “1991 WeatherLink_1”) and click the Explore button () that appears to the right of the highlighted device as a magnifying glass icon or double-click the highlighted device.



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



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



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

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

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

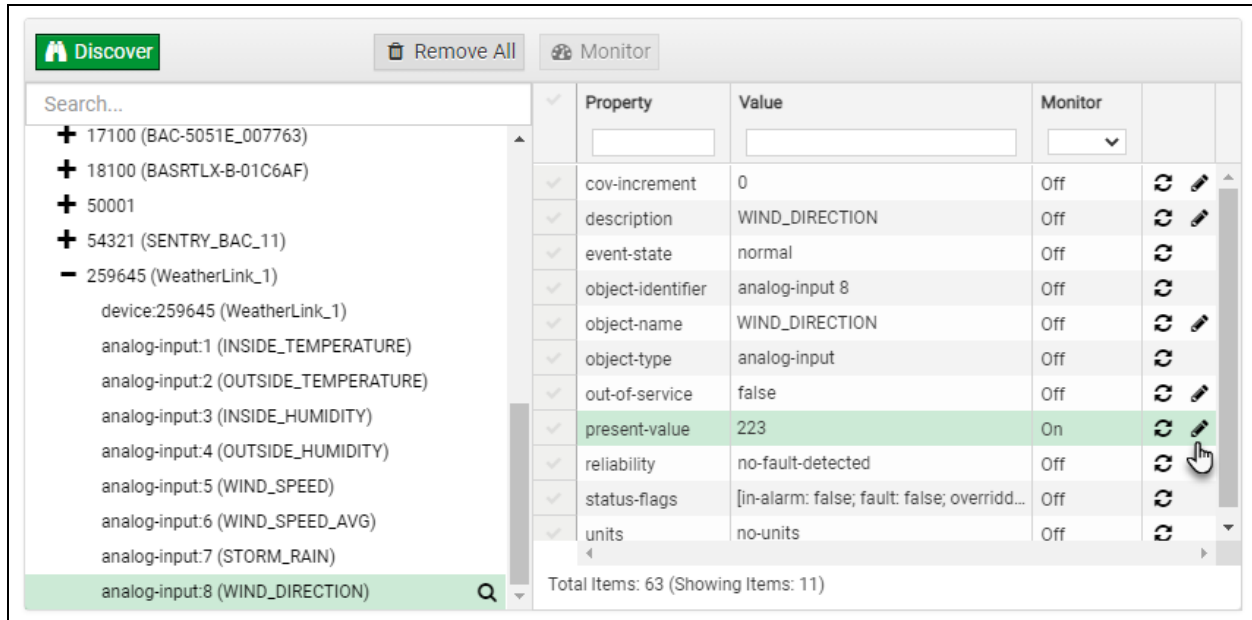
- Network number
 - Device
 - Device object

9.2.1 Edit the Present Value Field

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

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

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

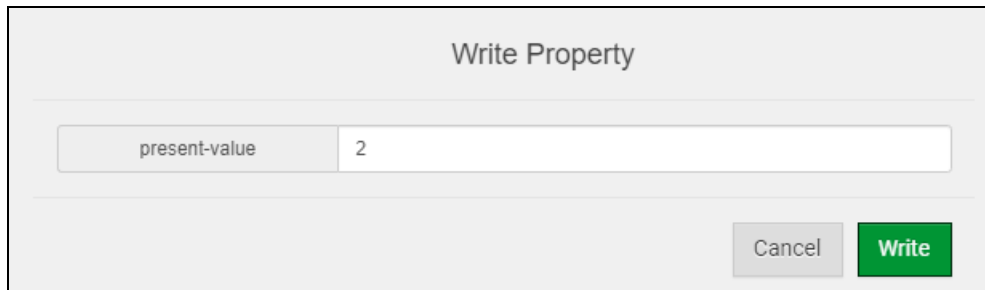


The screenshot shows the 'Discover' tab of the BACnet Router interface. On the left, a search bar and a list of discovered objects are visible. On the right, a table lists properties for the selected object. The 'present-value' property is highlighted in green, and its value is 223. A hand icon is clicking the edit button (pencil) for the 'present-value' property.

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

Total Items: 63 (Showing Items: 11)

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



The 'Write Property' window is shown. It has a title bar 'Write Property'. Below the title bar, there is a text input field with the label 'present-value' and the value '2'. At the bottom right, there are two buttons: 'Cancel' and 'Write' (highlighted in green).

- 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.

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

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)

30

BACnet Router Start-up Guide

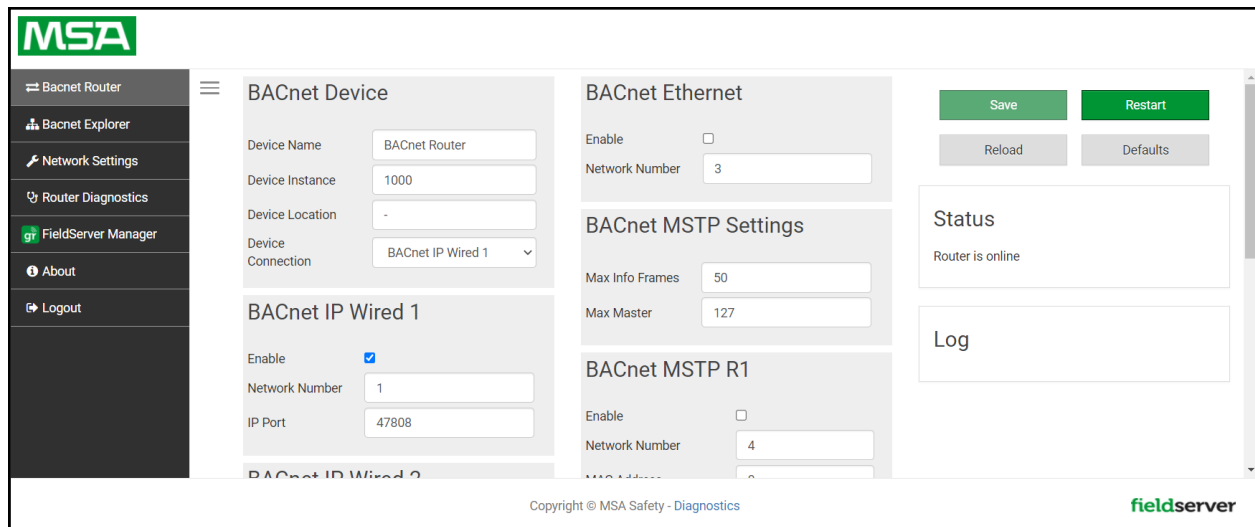
10 MSA Grid - FieldServer Manager Setup

The Grid is MSA Safety's device cloud solution for IIoT. Integration with the MSA Grid - FieldServer Manager enables the a secure remote connection to field devices through a FieldServer and hosts local applications for device configuration, management, as well as maintenance. For more information about the FieldServer Manager, refer to the [MSA Grid - FieldServer Manager Start-up Guide](#).

10.1 Create a New FieldServer Manager Account

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

- Click on the FieldServer Manager tab.



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

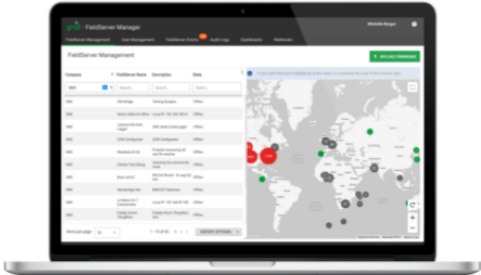
Grid FieldServer Manager Registration

Securely access your FieldServer from anywhere with the **Grid FieldServer Manager**

Your one stop for managing your FieldServers and users

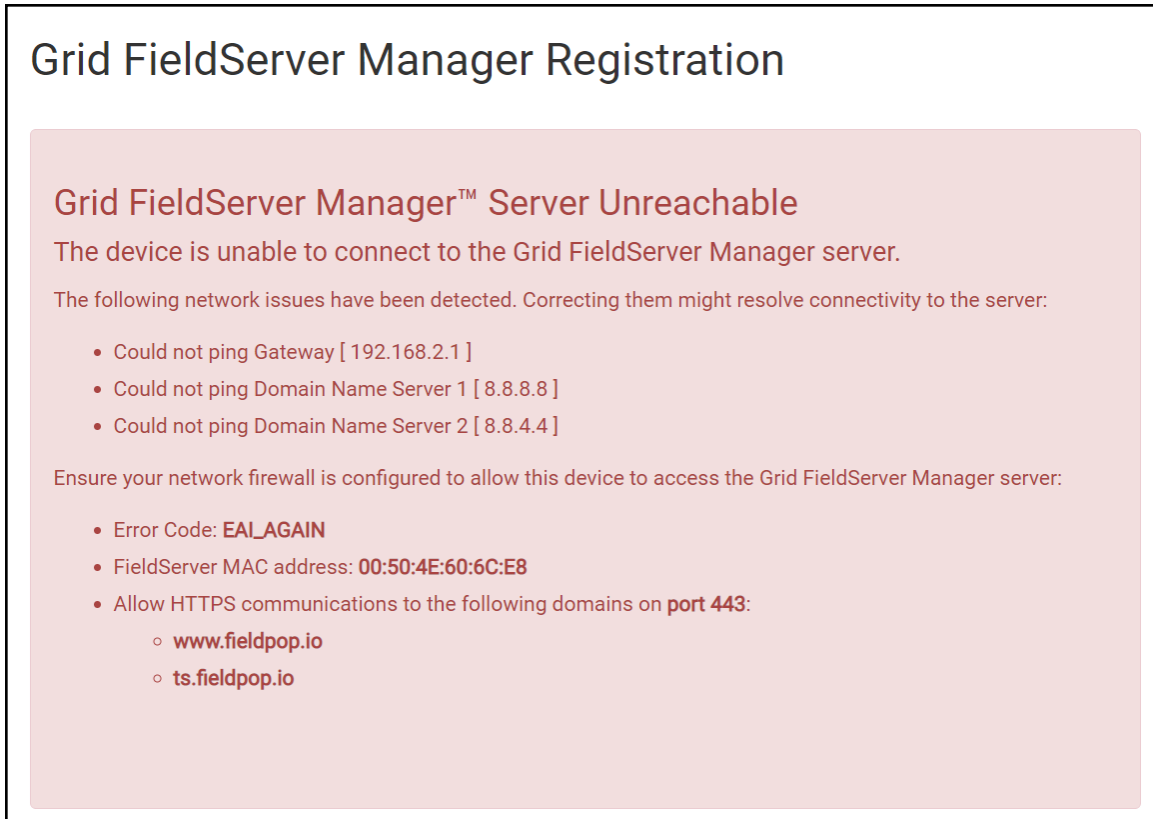
- ✓ **Secure Remote Access**
Securely connect your field devices to Grid FieldServer Manager.
- ✓ **FieldServer Management**
Manage all your FieldServers and connected devices from Grid FieldServer Manager and upgrade firmware remotely.
- ✓ **User Management**
Set up your user personnel with the right 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](#).



Get Started

- If a warning message appears instead of the splash page, follow the suggestion that appears on screen.
- If the BACnet Router cannot reach the Grid FieldServer Manager server, the following message will appear.



- 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 Router is properly connected to the Internet

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

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

- Enter user details and click Next

The screenshot shows the 'Installer Details' step, which is the first of four steps in the registration process. The steps are: 1. Installer Details, 2. Installation Site, 3. FieldServer Details, and 4. Account Details. The 'Installer Details' section contains the following fields:

- Installer Name
- Company
- Telephone
- Email
- Installation Date (with a calendar icon)

At the bottom right, there are 'Cancel' and 'Next' buttons.

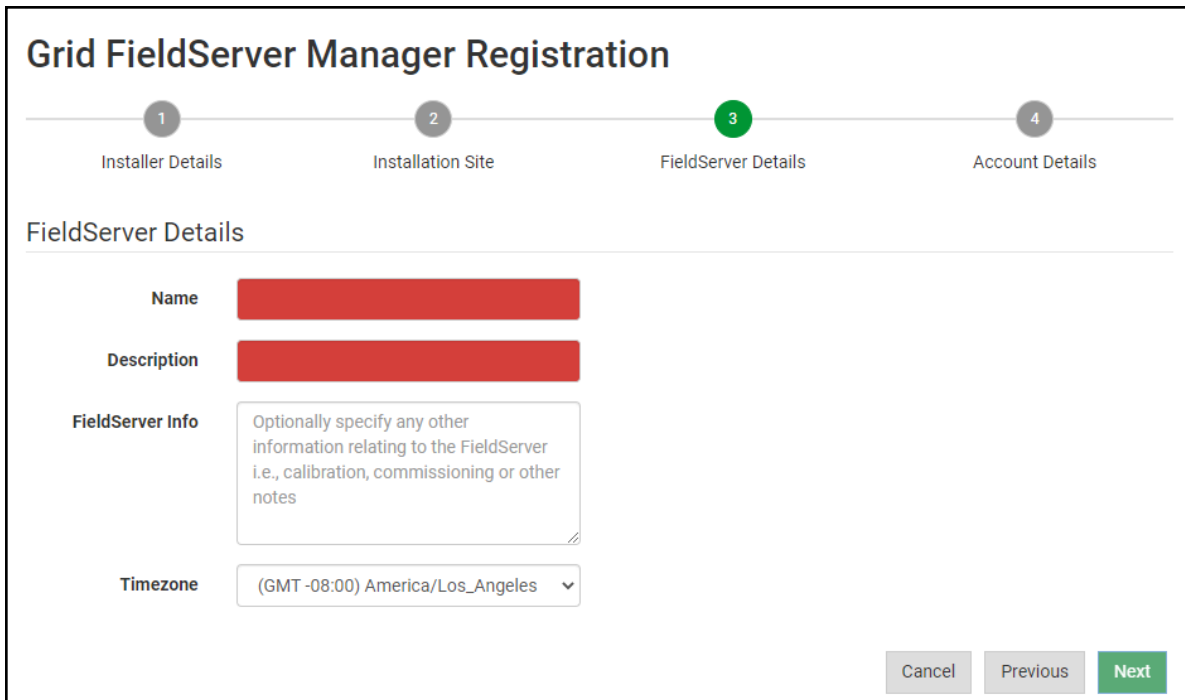
- Enter the site details by entering the physical address fields or the latitude and longitude then click Next

The screenshot shows the 'Installation Site Details' step, which is the second of four steps in the registration process. The steps are: 1. Installer Details, 2. Installation Site, 3. FieldServer Details, and 4. Account Details. The 'Installation Site Details' section contains the following fields:

- Search (Search Google Maps)
- Site Name (with a red placeholder: 'Enter a name for this location')
- Building
- Street Address (with a placeholder: 'Enter street address')
- Suburb
- City
- State
- Country
- Postal Code
- Latitude (with a red placeholder: 'Enter latitude')
- Longitude (with a red placeholder: 'Enter longitude')

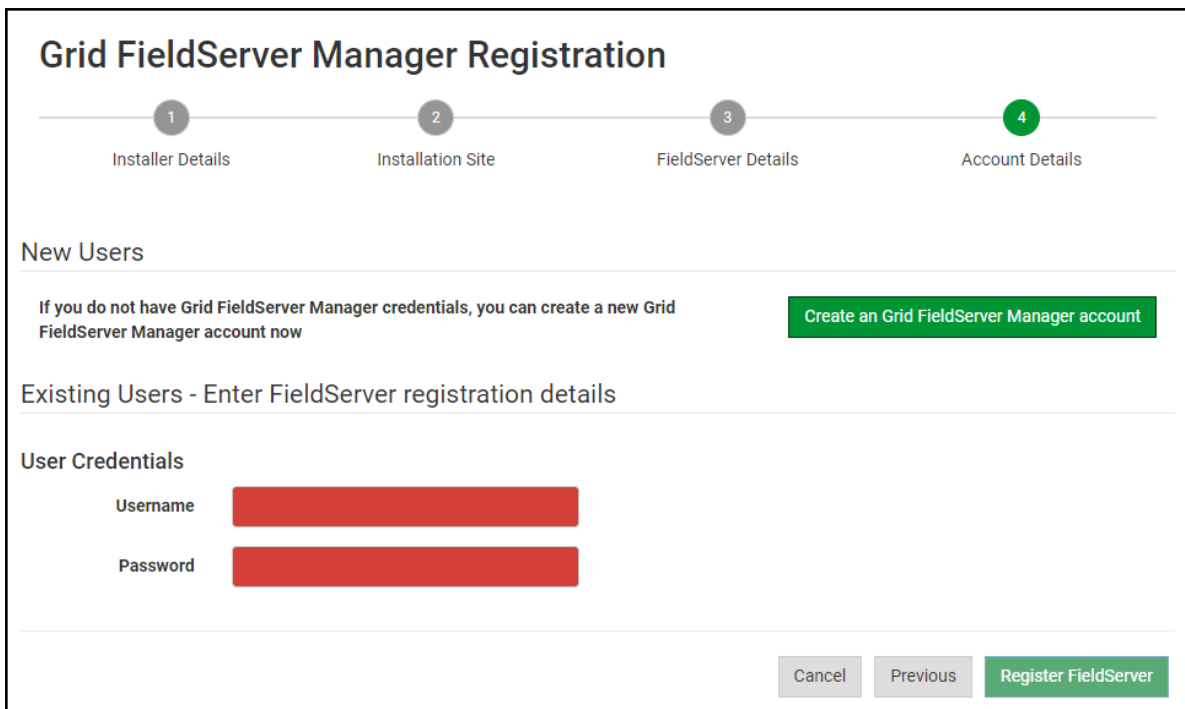
On the right side of the form, there is a Google Map showing the location. At the bottom right, there are 'Cancel', 'Previous', and 'Next' buttons.

- Enter Name and Description (required) then click Next



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

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



The screenshot shows the 'Grid FieldServer Manager Registration' wizard at step 4, 'Account Details'. The progress bar at the top indicates four steps: 1. Installer Details, 2. Installation Site, 3. FieldServer Details, and 4. Account Details (current). The 'Account Details' section is divided into two parts. The first part, 'New Users', contains the text 'If you do not have Grid FieldServer Manager credentials, you can create a new Grid FieldServer Manager account now' and a green button labeled 'Create an Grid FieldServer Manager account'. The second part, 'Existing Users - Enter FieldServer registration details', contains a section titled 'User Credentials' with two red text input fields: 'Username' and 'Password'. At the bottom right, there are three buttons: 'Cancel', 'Previous', and 'Register FieldServer'.

- Once the device has successfully been registered, a confirmation window will appear. Click the Close button and the following screen will appear listing the device details and additional information auto-populated by the BACnet Router.

Grid FieldServer Manager Registration

FieldServer Registered

FieldServer Details
Name: Test1
Description: FS Test
FieldServer Info:
Timezone: America/Los_Angeles
MAC Address: 00:50:4E:60:13:FE
Tunnel Server URL: tunnel.fieldpop.io
FieldServer ID: treedancer_KrgPKmLRY
Product Name: Core Application - Default
Product Version: 5.2.0


Installer Details
Installer Name: Test
Company: MSA Safety
Telephone: (408) 444-4444
Email: contactus@msasafety.com
Installation Date: Sep 20, 2021

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

Update FieldServer Details

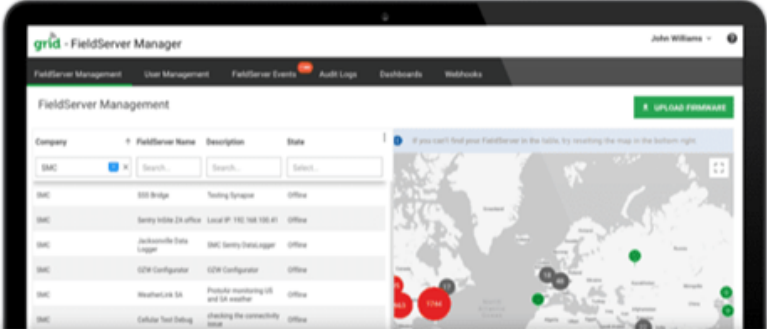
NOTE: Update these details at any time by going to the FieldServer Manager tab and clicking the Update FieldServer Details button.

- Open the registered email account.
- The “Welcome to SMC Cloud” email will appear as shown below.



Fieldserver Manager

Welcome to FieldServer Manager



Your one stop for managing your FieldServers and users

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

COMPLETE REGISTRATION

Contact Us

+1 408 262-6611

smc-support@msasafety.com

www.msasafety.com

© copyright 2021 MSA . All rights reserved.

MSA | fieldserver

NOTE: If no Grid 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

First Name

Last Name

Mobile Phone Number

New Password

Confirm Password

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

Cancel

Save

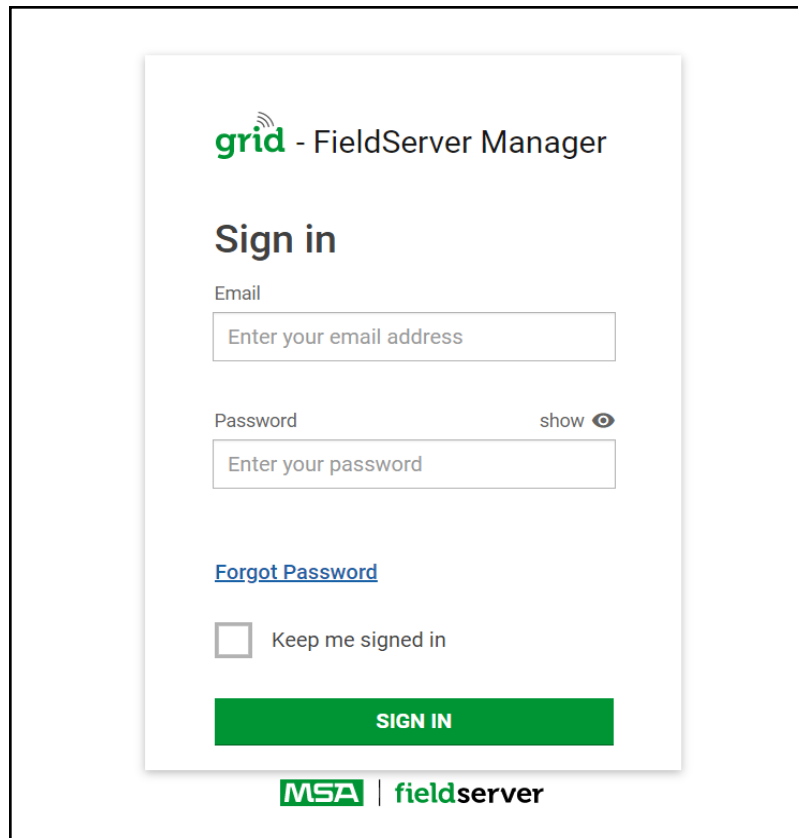
- Fill in the name, phone number, password fields and click the checkbox to agree to the privacy policy and terms of service.

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

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

10.2 Login to the FieldServer Manager

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



The screenshot shows the login interface for the FieldServer Manager. At the top, the logo 'grid' (in green) is followed by the text '- FieldServer Manager'. Below this is the heading 'Sign in'. There are two input fields: 'Email' with the placeholder text 'Enter your email address' and 'Password' with the placeholder text 'Enter your password'. To the right of the password field is a 'show' label with an eye icon. Below the password field is a blue link labeled 'Forgot Password'. Underneath is a checkbox labeled 'Keep me signed in'. At the bottom of the form is a large green button labeled 'SIGN IN'. At the very bottom of the page, there is a logo for 'MSA | fieldserver'.

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

NOTE: For additional FieldServer Manager instructions see the [MSA Grid - FieldServer Manager Start-up Guide](#).

grid - FieldServer Manager

User A

FieldServer Management

User Management

FieldServer Events

Audit Logs

Dashboards

Webhooks

FieldServer Management

UPLOAD FIRMWARE

Company

FieldServer Name

Description

State

Select...

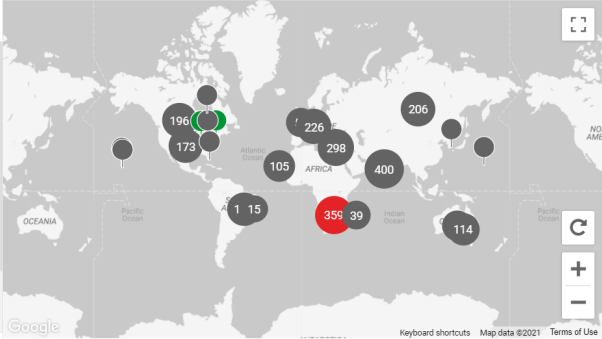
Search...

Search...

Select...

Eggers OEM	Jens's Brain 31	192.168.1.31	Offline
Eggers OEM	Jens MBP Core App	~/git/smc-core-application	Offline
Eggers OEM	Jens's Dell Profile View	~/git/profile-view	Offline
Eggers OEM	hd_test_log_to_fpop	testing_modbus	Offline
Eggers OEM	Mbus demo	testing registration	Offline
SMC	TestWall-PA2port 97	Testwall pa 2 97	Offline
SMC	TestWall-Lon152	Testwall unit	Offline

If you can't find your FieldServer in the table, try resetting the map in the bottom right.



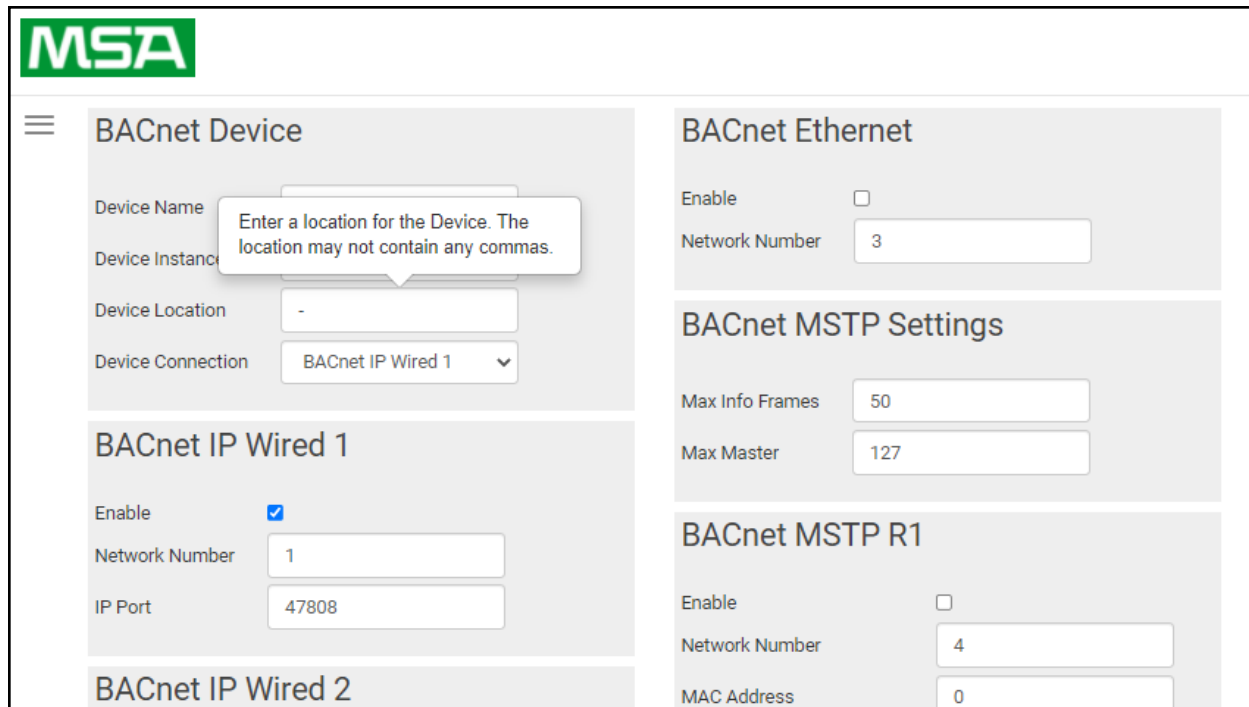
© 2021 MSA. All rights reserved.

MSA | fieldserver

11 Troubleshooting

11.1 Tooltips

Tooltips appear when the mouse pointer hovers over the corresponding settings field. A balloon will appear giving a description of that input field. This applies to all input fields.




The screenshot displays the MSA BACnet configuration interface. At the top left is the MSA logo. A hamburger menu icon is located to the left of the 'BACnet Device' panel. The interface is divided into several sections:

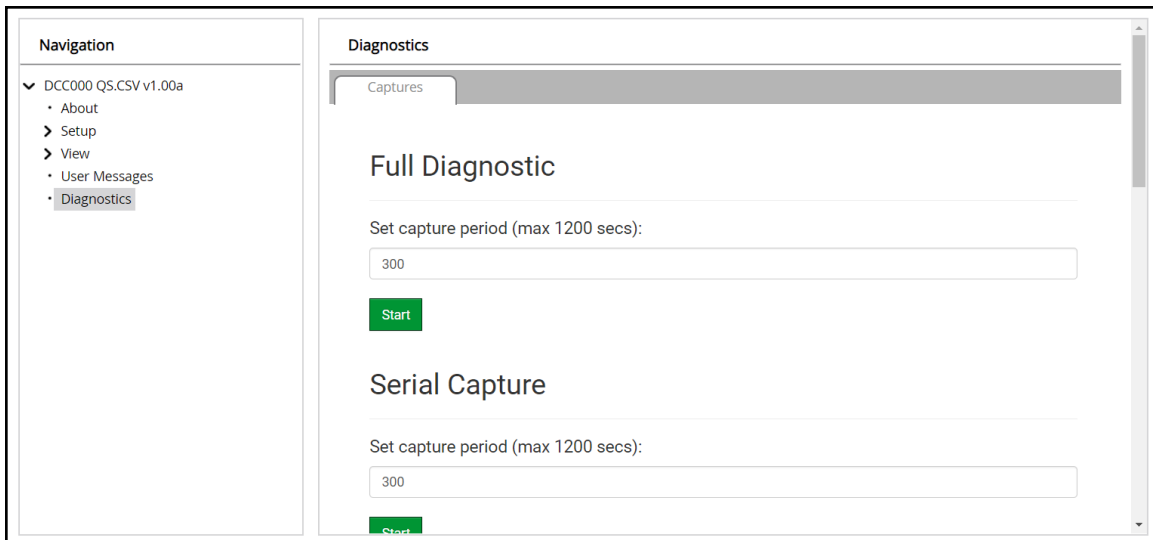
- BACnet Device**: Contains fields for 'Device Name', 'Device Instance', 'Device Location' (with a tooltip), and 'Device Connection' (set to 'BACnet IP Wired 1').
- BACnet IP Wired 1**: Contains 'Enable' (checked), 'Network Number' (1), and 'IP Port' (47808).
- BACnet IP Wired 2**: A header for the second IP wired section.
- BACnet Ethernet**: Contains 'Enable' (unchecked) and 'Network Number' (3).
- BACnet MSTP Settings**: Contains 'Max Info Frames' (50) and 'Max Master' (127).
- BACnet MSTP R1**: Contains 'Enable' (unchecked), 'Network Number' (4), and 'MAC Address' (0).

A tooltip is visible over the 'Device Location' field, stating: "Enter a location for the Device. The location may not contain any commas."

11.2 Taking a FieldServer Diagnostic Capture

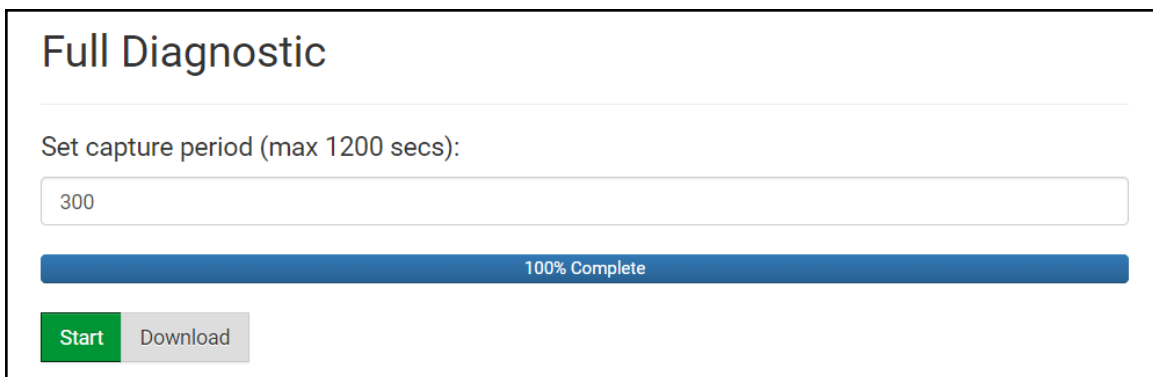
When there is a problem on-site that cannot easily be resolved, perform a Diagnostic Capture before contacting support. Once the Diagnostic Capture is complete, email it to technical support. The Diagnostic Capture will accelerate diagnosis of the problem.

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



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

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



This screenshot is a close-up of the 'Full Diagnostic' section. It shows the 'Set capture period (max 1200 secs):' label and the input field with '300'. Below the input field is a blue progress bar that is completely filled and labeled '100% Complete'. At the bottom of this section, there are two buttons: a green 'Start' button and a grey 'Download' button.

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

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

11.3 Factory Reset Instructions

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

11.4 Internet Browser Software Support

The following web browsers are supported:

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

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

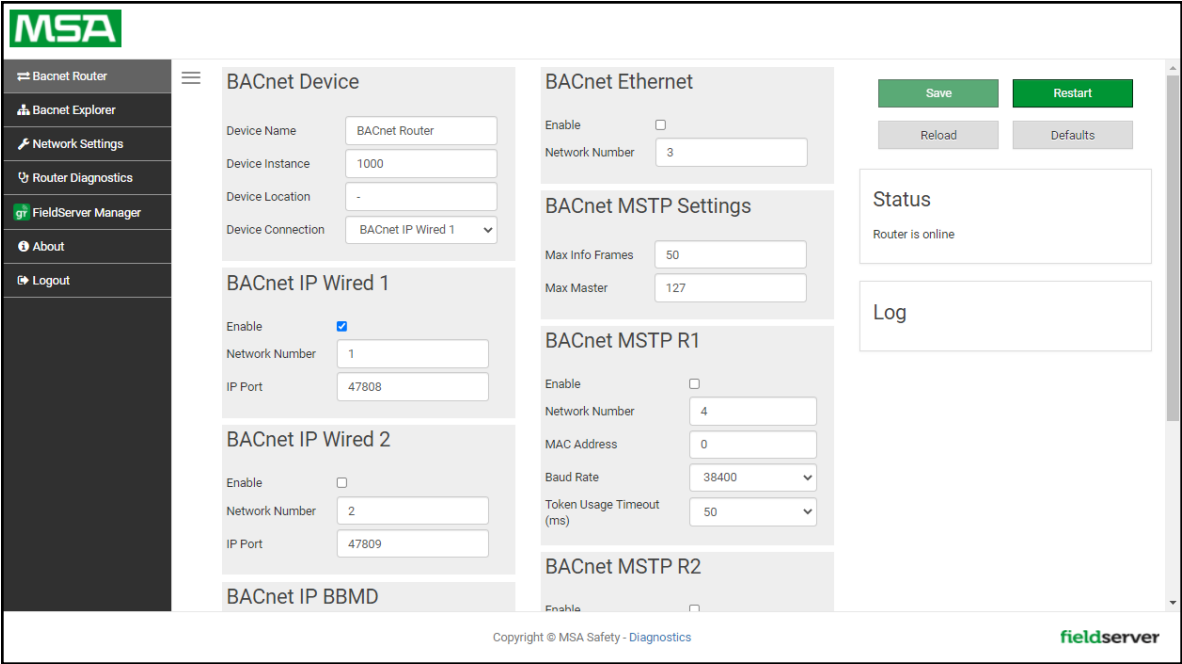
NOTE: Computer and network firewalls must be opened for Port 80 to allow FieldServer GUI to function.

12 Additional Information

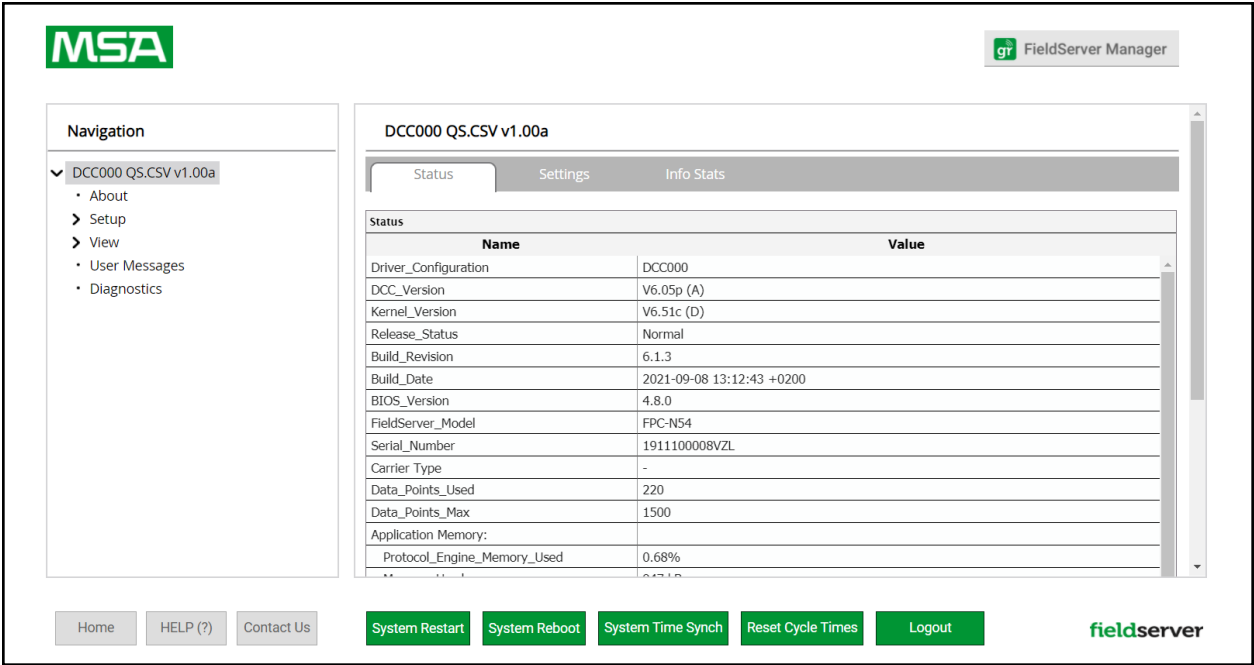
12.1 Change Web Server Security Settings After Initial Setup

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

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

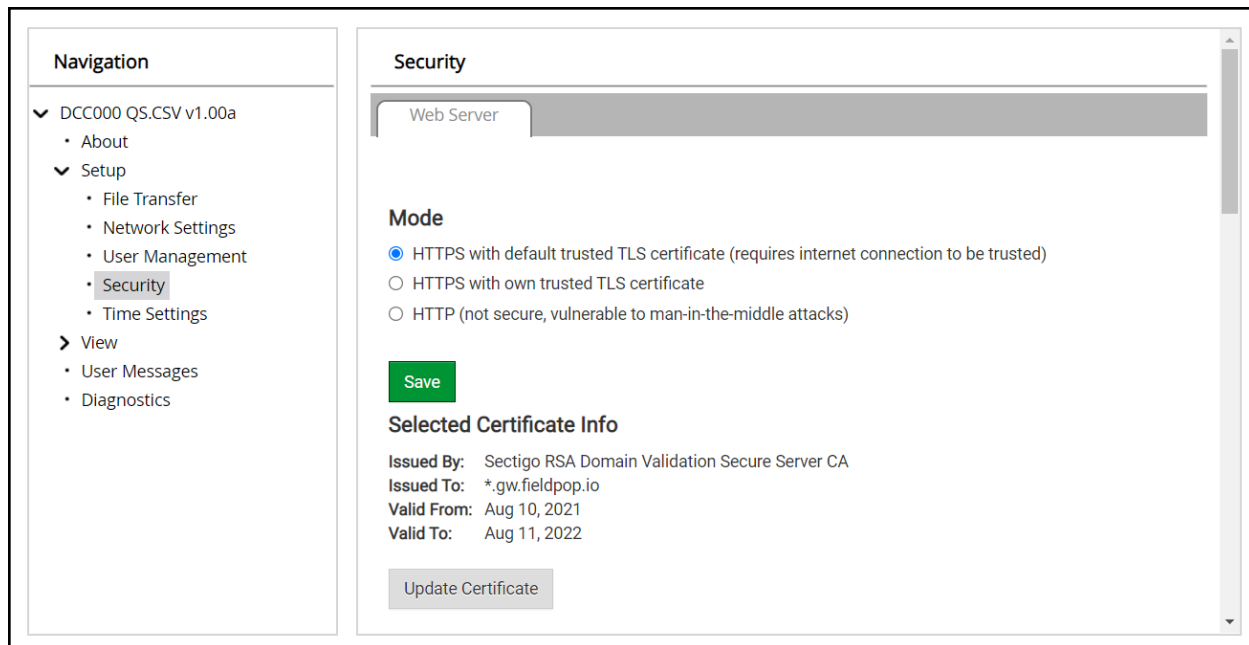


- Click Setup in the Navigation panel.



12.1.1 Change Security Mode

- Click Security in the Navigation panel.



The screenshot shows a web interface with a left-hand navigation panel and a main content area. The navigation panel, titled 'Navigation', contains a tree structure with 'DCC000 QS.CSV v1.00a' expanded, showing sub-items: 'About', 'Setup', 'Security' (highlighted), 'View', 'User Messages', and 'Diagnostics'. The main content area, titled 'Security', has a 'Web Server' tab selected. Under the 'Mode' section, three radio buttons are present: 'HTTPS with default trusted TLS certificate (requires internet connection to be trusted)' (selected), 'HTTPS with own trusted TLS certificate', and 'HTTP (not secure, vulnerable to man-in-the-middle attacks)'. Below the radio buttons is a green 'Save' button. Under the 'Selected Certificate Info' section, the following details are displayed: 'Issued By: Sectigo RSA Domain Validation Secure Server CA', 'Issued To: *.gw.fieldpop.io', 'Valid From: Aug 10, 2021', and 'Valid To: Aug 11, 2022'. At the bottom of this section is a grey 'Update Certificate' button.

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

12.1.2 Edit the Certificate Loaded onto the FieldServer

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

- Click Security in the Navigation panel.

The screenshot shows the 'Security' configuration page. On the left is a 'Navigation' panel with a tree structure: 'DCC000 QS.CSV v1.00a' (expanded) contains 'About', 'Setup' (expanded), 'View', 'User Messages', and 'Diagnostics'. Under 'Setup', 'Security' is highlighted. The main content area is titled 'Security' and has a 'Web Server' tab selected. Under the 'Mode' section, three radio buttons are present: 'HTTPS with default trusted TLS certificate (requires internet connection to be trusted)' (selected), 'HTTPS with own trusted TLS certificate', and 'HTTP (not secure, vulnerable to man-in-the-middle attacks)'. Below the modes is a green 'Save' button. The 'Selected Certificate Info' section displays: 'Issued By: Sectigo RSA Domain Validation Secure Server CA', 'Issued To: *.gw.fieldpop.io', 'Valid From: Aug 10, 2021', and 'Valid To: Aug 11, 2022'. At the bottom of this section is a grey 'Update Certificate' button.

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

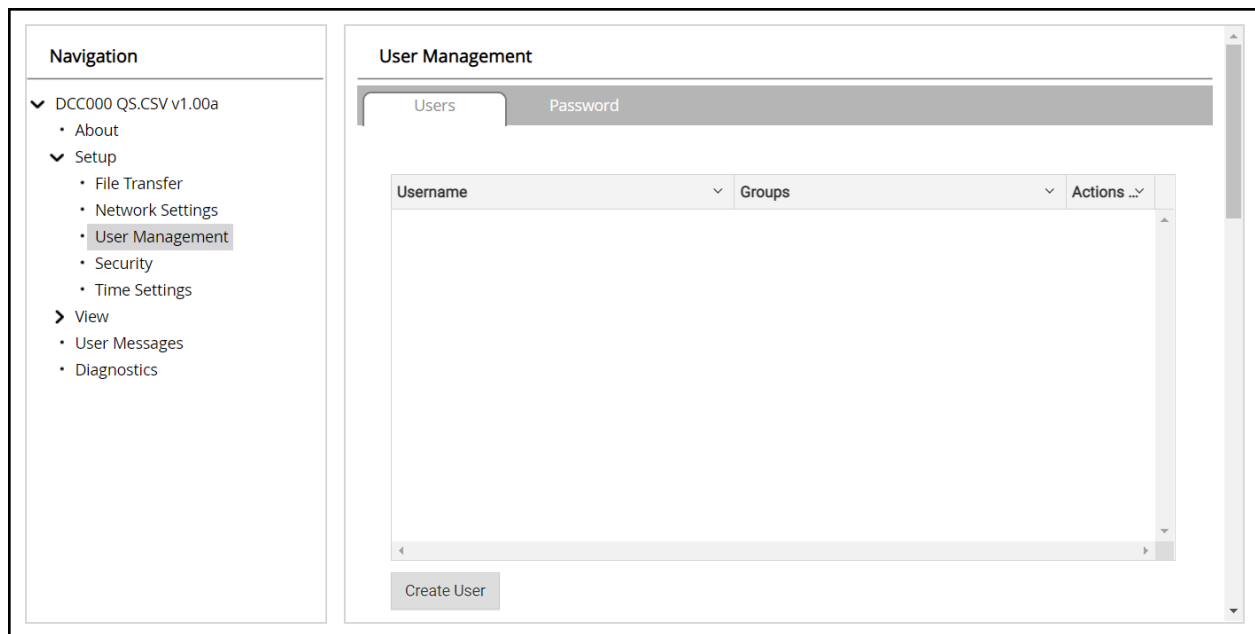
12.2 Change User Management Settings

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

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

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

- Check that the Users tab is selected.



User Types:

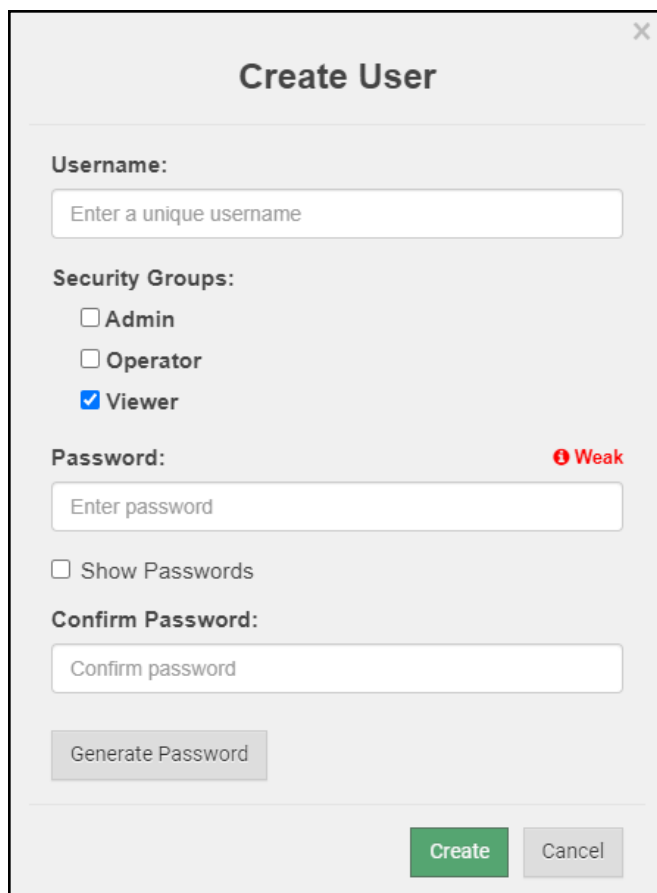
Admin – Can modify and view any settings on the FieldServer.

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

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

12.2.1 Create Users

- Click the Create User button.



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

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

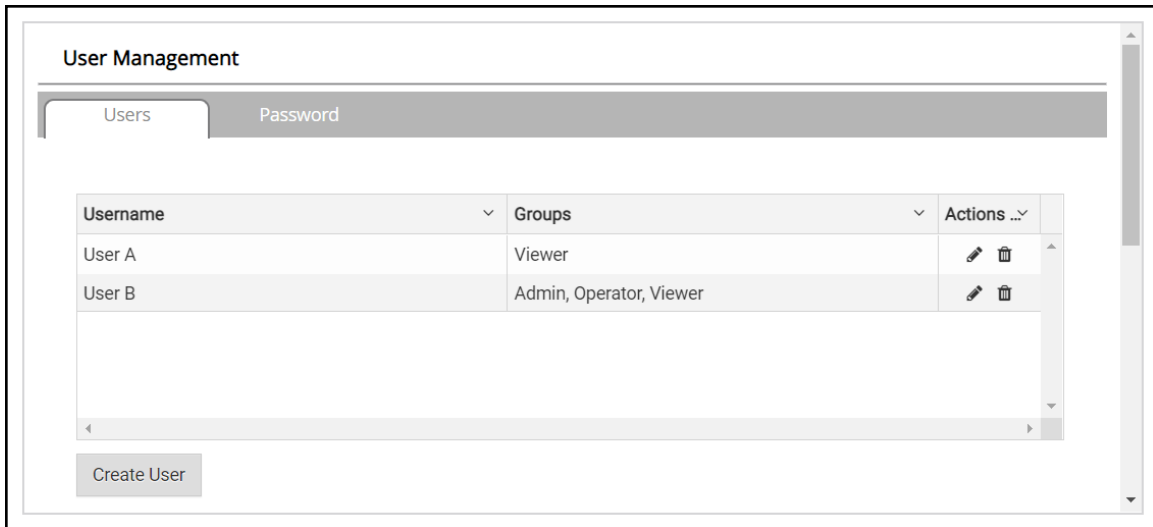
- Enter the new User fields: Name, Security Group and Password.
 - User details are hashed and salted**

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

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

12.2.2 Edit Users

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

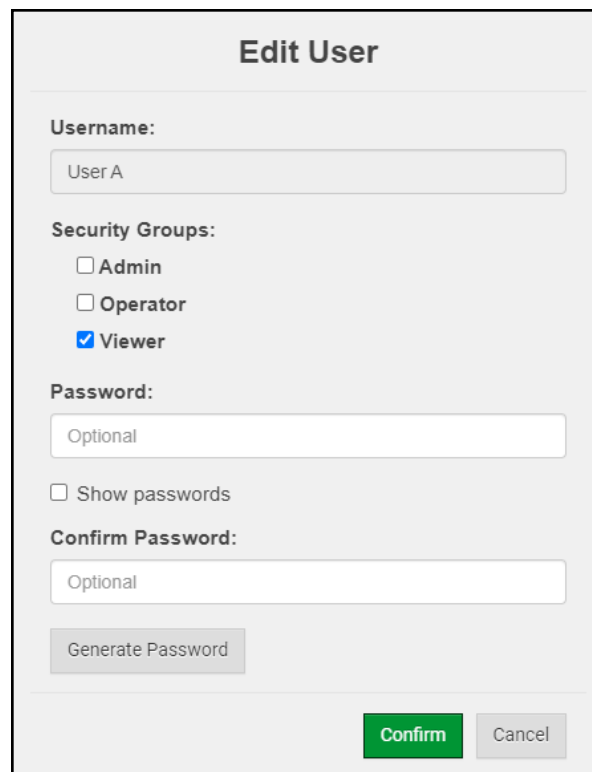


The 'User Management' window has two tabs: 'Users' (selected) and 'Password'. It contains a table with the following data:

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

Below the table is a 'Create User' button.

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



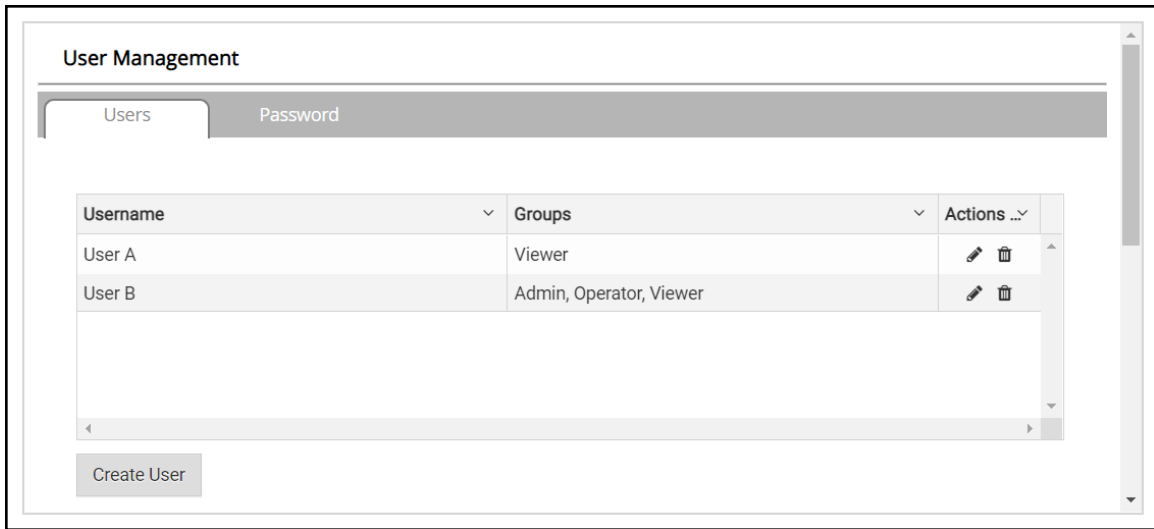
The 'Edit User' window contains the following fields and controls:

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

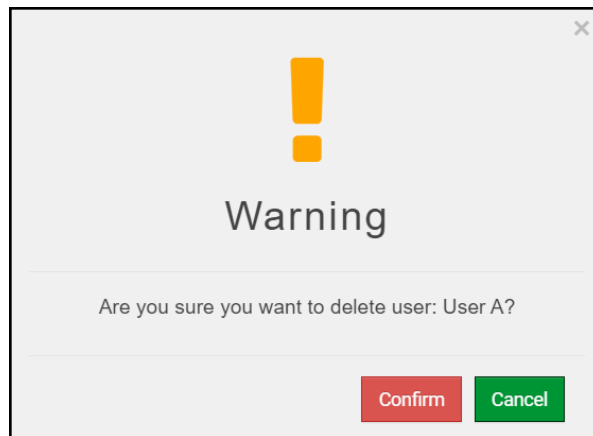
- Click Confirm.
- Once the Success message appears, click OK.

12.2.3 Delete Users

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



- When the warning message appears, click Confirm.



12.2.4 Change FieldServer Password

- Click the Password tab.

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

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

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

12.3 Specifications



	FS-ROUTER-BAC2
Electrical Connections	One 3-pin Phoenix connector with: RS-485/RS-232 (Tx+ / Rx- / gnd) One 3-pin Phoenix connector with: RS-485 (+ / - / gnd) One 3-pin Phoenix connector with: Power port (+ / - / Frame-gnd) One Ethernet 10/100 BaseT port
Power Requirements	<i>Input Voltage:</i> 9-30VDC or 24VAC <i>Max Power:</i> 3 Watts <i>Current draw:</i> 24VAC 0.125A 9-30VDC 0.25A @12VDC
Approvals	CE and FCC Class B & C Part 15, UL 60950-1, WEEE compliant, IC Canada, RoHS3 compliant, REACH compliant, UKCA compliant
Physical Dimensions	4 x 1.1 x 2.7 in (10.16 x 2.8 x 6.8 cm)
Weight	0.4 lbs (0.2 Kg)
Operating Temperature	-20°C to 70°C (-4°F to 158°F)
Humidity	10-95% RH non-condensing

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

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

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

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

NOTE: Specifications subject to change without notice.

13 Limited 2 Year Warranty

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

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

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

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