



## 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](mailto:smc-support@msasafety.com)

EMEA Support Information:  
+31 33 808 0590  
Email: [smc-support.emea@msasafety.com](mailto:smc-support.emea@msasafety.com)

For your local MSA contacts, please go to our website [www.MSAafety.com](http://www.MSAafety.com)

# Contents

<b>1</b>	<b>BACnet Router Description</b>	<b>5</b>
<b>2</b>	<b>Equipment Setup</b>	<b>6</b>
2.1	Mounting	6
2.2	Physical Dimensions	7
<b>3</b>	<b>Installation</b>	<b>8</b>
3.1	Connecting the R1 & R2 Ports	8
3.1.1	Wiring	8
3.2	10/100 Ethernet Connection Port	9
<b>4</b>	<b>Power up the Gateway</b>	<b>10</b>
<b>5</b>	<b>Connecting to the BACnet Router</b>	<b>11</b>
5.1	Using the FieldServer Toolbox to Discover and Connect to the BACnet Router	11
5.2	Using a Web Browser	11
<b>6</b>	<b>Setup Web Server Security</b>	<b>12</b>
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
<b>7</b>	<b>Setup Network</b>	<b>16</b>
7.1	Ethernet 1	17
7.2	Routing Settings	18
<b>8</b>	<b>Configuring the BACnet Router</b>	<b>19</b>
8.1	Navigate to the BACnet Router Settings	19
8.2	BACnet Router Settings	20
8.2.1	Button Functions	20
8.2.2	Multiple Connections	21
8.2.3	BACnet Device	21
8.2.4	BACnet/IP	22
8.2.5	BACnet MS/TP, BACnet Ethernet and BACnet Explorer	23
8.3	Router Diagnostics	24
<b>9</b>	<b>BACnet Explorer</b>	<b>25</b>
9.1	Discover the Device List	26
9.2	View Device Details and Explore Points/Parameters	27
9.2.1	Edit the Present Value Field	30
<b>10</b>	<b>MSA Grid - FieldServer Manager Setup</b>	<b>32</b>
10.1	Create a New FieldServer Manager Account	32
10.2	Login to the FieldServer Manager	39
<b>11</b>	<b>Troubleshooting</b>	<b>41</b>
11.1	Tooltips	41
11.2	Taking a FieldServer Diagnostic Capture	42
11.3	Factory Reset Instructions	43

11.4	Internet Browser Software Support .....	43
<b>12</b>	<b>Additional Information .....</b>	<b>44</b>
12.1	Change Web Server Security Settings After Initial Setup .....	44
12.1.1	Change Security Mode .....	45
12.1.2	Edit the Certificate Loaded onto the FieldServer .....	46
12.2	Change User Management Settings .....	47
12.2.1	Create Users .....	48
12.2.2	Edit Users .....	49
12.2.3	Delete Users .....	50
12.2.4	Change FieldServer Password .....	51
12.3	Specifications .....	52
<b>13</b>	<b>Limited 2 Year Warranty .....</b>	<b>53</b>

## 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](#).

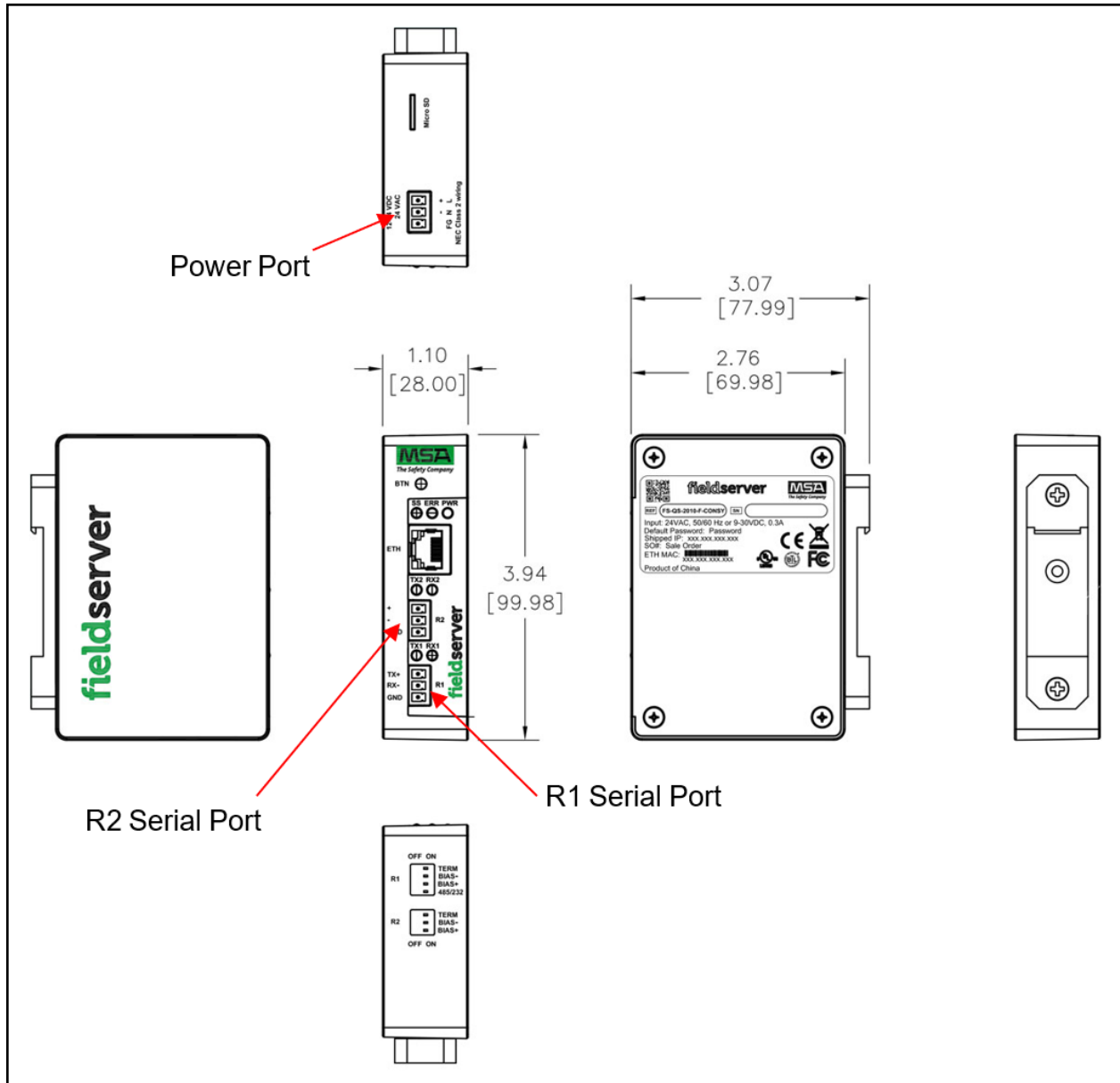
## 2 Equipment Setup

### 2.1 Mounting

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



## 2.2 Physical Dimensions



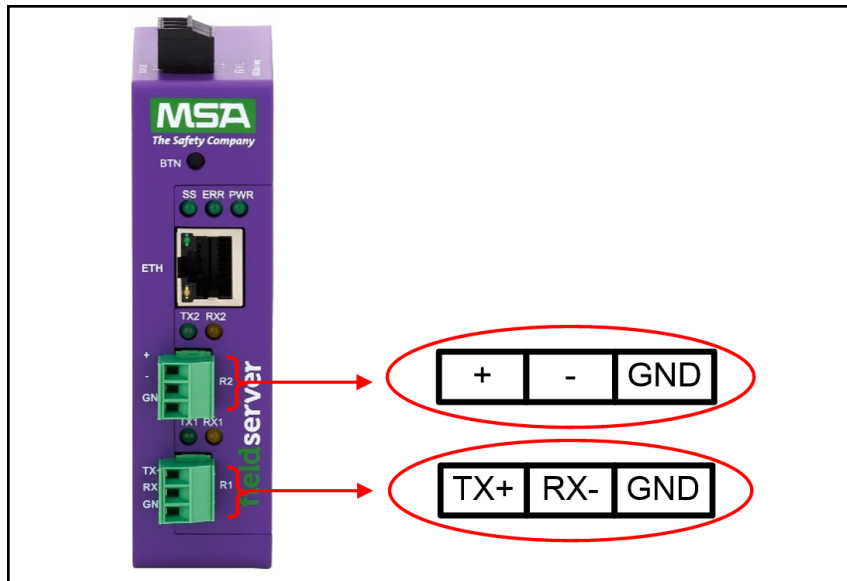
### 3 Installation

#### 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

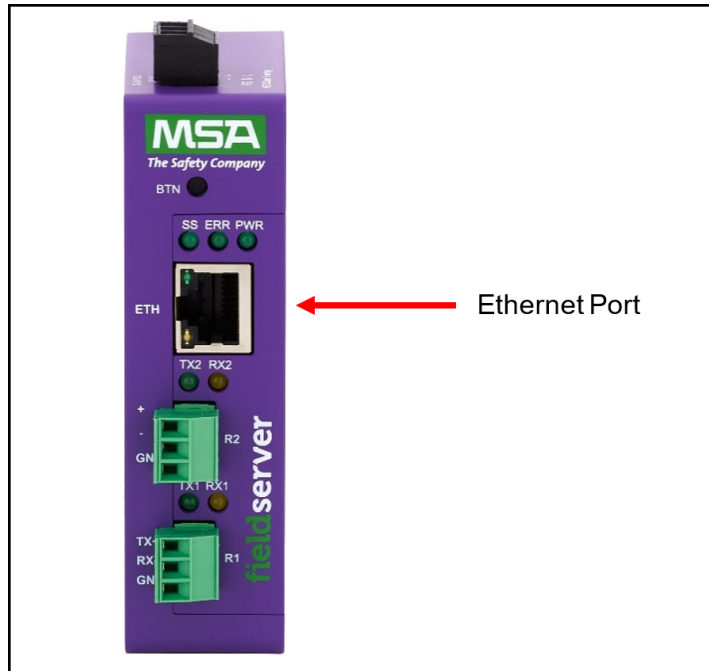
##### 3.1.1 Wiring

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.

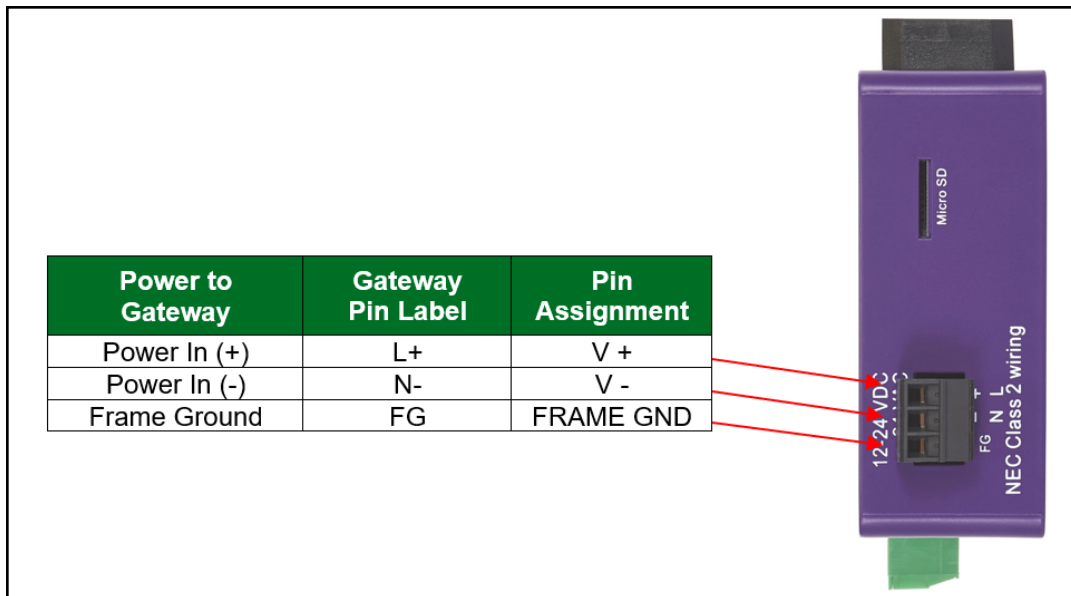
## 4 Power up the Gateway

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
<b>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.</b>		

Apply power to the BACnet Router as shown below. Ensure that the power supply used complies with the specifications provided in [Section 12.3 Specifications](#) .

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



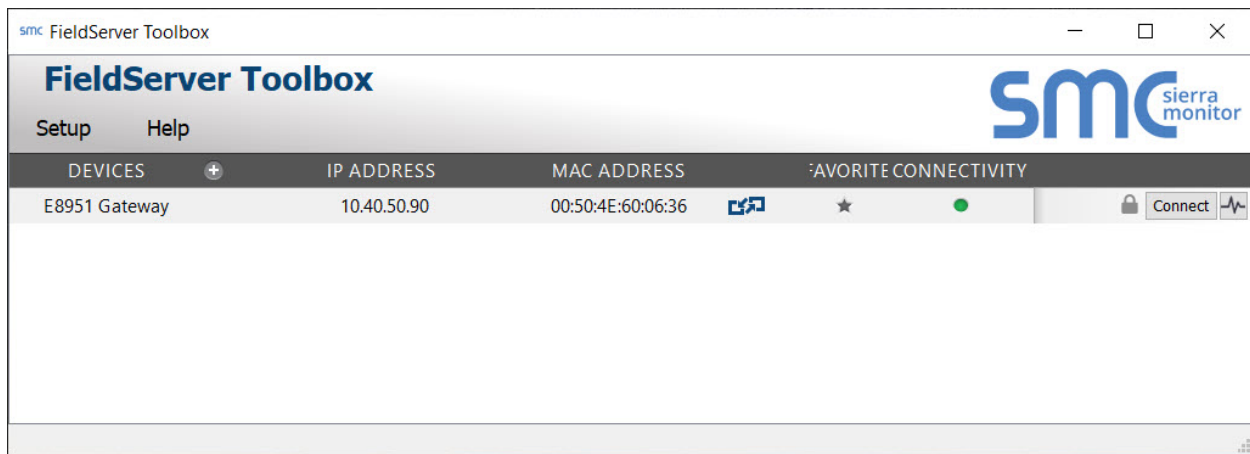
## 5 Connecting to the BACnet Router

The FieldServer Toolbox Application can be used to discover and connect to the BACnet Router on a local area network. To manually connect to the BACnet Router using the Toolbox, click on the plus icon next to the "Devices" header and enter the IP Address, or enter the Internet IP Address into a web browser.

### 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.

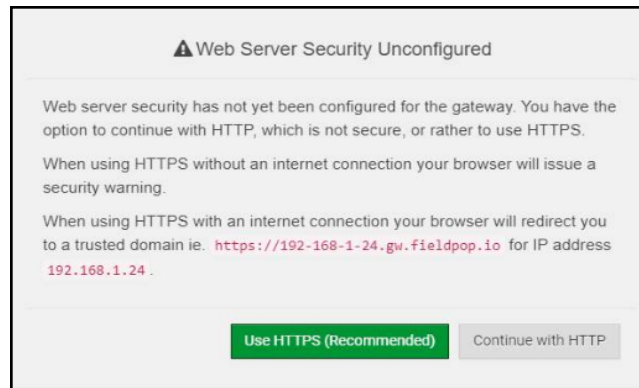
**NOTE:** Check Section [11.4 Internet Browser Software Support](#) for supported browsers.

## 6 Setup Web Server Security

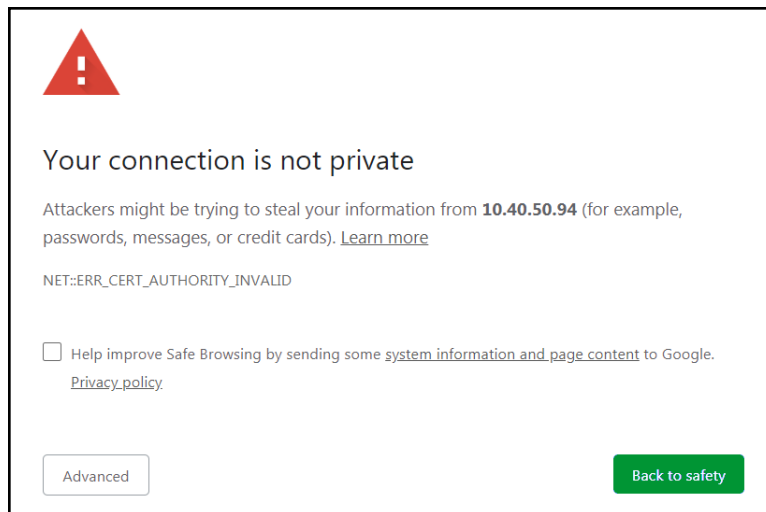
### 6.1 Login to the FieldServer

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.

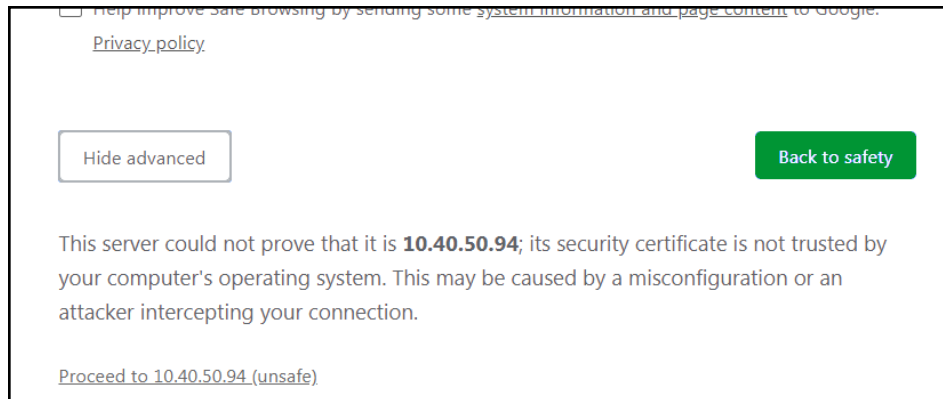
- When the Web Server Security Unconfigured window appears, read the text and choose whether to move forward with HTTPS or HTTP.



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

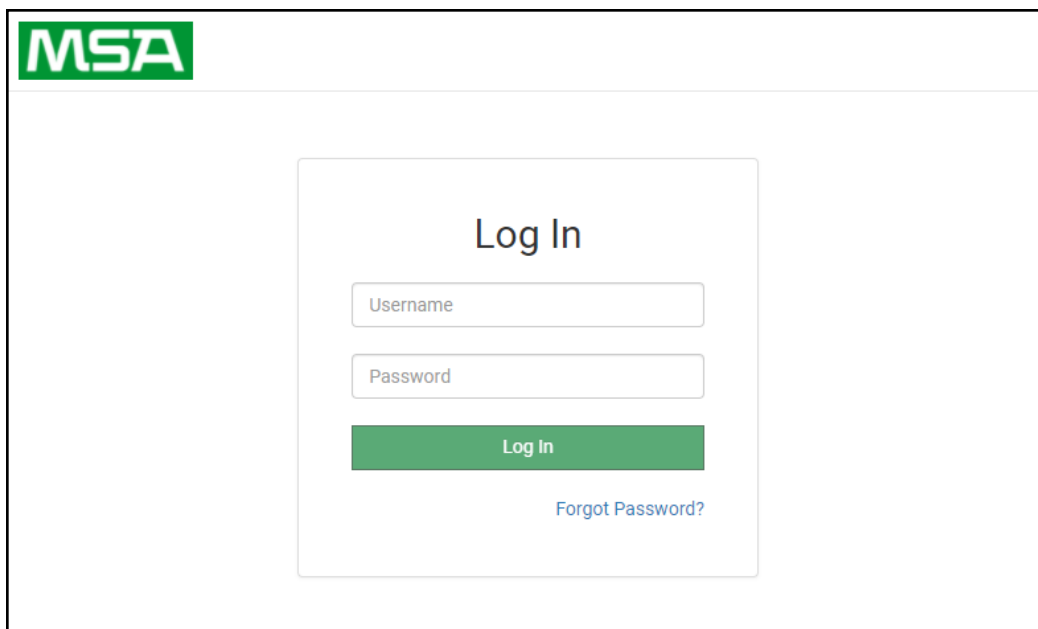


- Additional text will expand below the warning, click the underlined text to go to the IP Address. In the example below this text is “[Proceed to 10.40.50.94 \(unsafe\)](#)”.



- 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
A41BAQBFM+IPvOx3T/47VEmaiXqE3bx3zEuBFJ6pWPlw7LHf2r2ZoHw+9xb+aNMU
dVyAelhBMTMsnI2ERvQVp0xj3psSv2EJyKXS1bOYNRLsq7UzpwuAdT/Wy3o6vUM5
K+Cwf9qEoQ0LuxDZTIEct67MkcHMiuFi5pk7TRicHnQF/sfOAYOulduHOy9exlk9
FmHFVDIZt/cJUaF+e74EuSph+gEr0lQo2wvmhyc7L22UXse1NoOfUJ2Zq0Eu1Vvtu
JRryaMWIRFEWuuzMGZtKFWWC+8q2JQsVcqiRWM7naoblEhOCMH+sKHJMCxDoXGt
vtZjpZUoAL51YXxWSVcyZdGiAP5e
-----END CERTIFICATE-----
```

**Private Key**

```
sHB0zZoHr4YQSDK2BbYVzZbI0LDuKtc8+JiO3ooGjoTuHnqkeAj/fKfbTAsKeAzw
gKQe+H5UQNK0bdvZfOJrm6daDK2vVDMR5k+juUUhEj5N49uplroB97MQgYotzqfT+
THlbpq5t1SIK617k04ObKMHF5l8fck+ru545sVmpeeZh0m5j5SURYAZMvbq5daCu
J4l5NlIhbEvxRF4UK41ZDMCvujopCbkUWrb1a/3XXnDnM2K9xyz2wze998D6Wk46
+7aOFY9F+7j5lJmknkoS3GYtwCyH5iP+mPP1K6RnuiD019wvGpB4dtN/RTnfd0eF
GYeVskl9fxkxDOFtdWRZbM/rPin4tmO1Xf8HqONVN1x/iaMynOXG4cukoi4+VO
u0rZaUEsll2zNkfrn7fAASm5NBWg202Cy9IAYnuujs3aALl5uGBeekA62oTMxlzx
-----END RSA PRIVATE KEY-----
```

**Private Key Passphrase**

Specify if encrypted

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

Navigate to the Network Settings tab shown below and configure the settings as needed.

The screenshot displays the MSA FieldServer Manager interface for configuring network settings. The left sidebar contains navigation options: BACnet Router, BACnet Explorer, Network Settings (selected), Router Diagnostics, FieldServer Manager, About, and Logout. The main content area is divided into several sections:

- BACnet Device:** Fields for Device Name (BACnet Router), Device Instance (1000), Device Location (-), and Device Connection (BACnet IP Wired 1).
- BACnet IP Wired 1:** Fields for Enable (checked), Network Number (1), and IP Port (47808).
- BACnet IP Wired 2:** Fields for Enable (unchecked), Network Number (2), and IP Port (47809).
- BACnet IP BBMD:** Section header with no visible fields.
- BACnet Ethernet:** Fields for Enable (unchecked) and Network Number (3).
- BACnet MSTP Settings:** Fields for Max Info Frames (50) and Max Master (127).
- BACnet MSTP R1:** Fields for Enable (unchecked), Network Number (4), MAC Address (0), Baud Rate (38400), and Token Usage Timeout (50).
- BACnet MSTP R2:** Section header with no visible fields.

On the right side, there are control buttons: Save, Restart, Reload, and Defaults. Below these are two status boxes: "Status" showing "Router is online" and "Log".

At the bottom of the interface, the copyright notice "Copyright © MSA Safety - Diagnostics" and the "fieldserver" logo are visible.



## 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:** The browser will need to be pointed to the new IP Address of the FieldServer before the settings will be accessible again.


The screenshot shows the configuration interface for Ethernet 1. On the left, there are input fields for IP Address (10.40.50.109), Netmask (255.255.255.0), Gateway (10.40.50.1), Domain Name Server 1 (10.40.2.24), and Domain Name Server 2 (10.15.130.15). There is an unchecked checkbox for 'Enable DHCP'. At the bottom left are 'Cancel' and 'Save' buttons. On the right, a 'Network Status' box shows 'Connection Status' as 'Connected' with a green checkmark, and other statistics like MAC Address (00:50:4e:60:13:be), Ethernet Tx/Rx Msgs, and Dropped counts.

Network Status	
Connection Status	✔ Connected
MAC Address	00:50:4e:60:13:be
Ethernet Tx Msgs	1,209,919
Ethernet Rx Msgs	2,745,183
Ethernet Tx Msgs Dropped	0
Ethernet Rx Msgs Dropped	0

## 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.

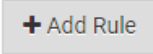
- Click the Add Rule button to add a new row and set a new Destination Network, Netmask and Gateway IP Address as needed.
- Set the Priority for each connection (1-255 with 1 as the highest priority and 255 as the lowest).
- Click the Save button to activate the new settings.

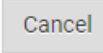

ETH 1 Routing 

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 

 + Add Rule

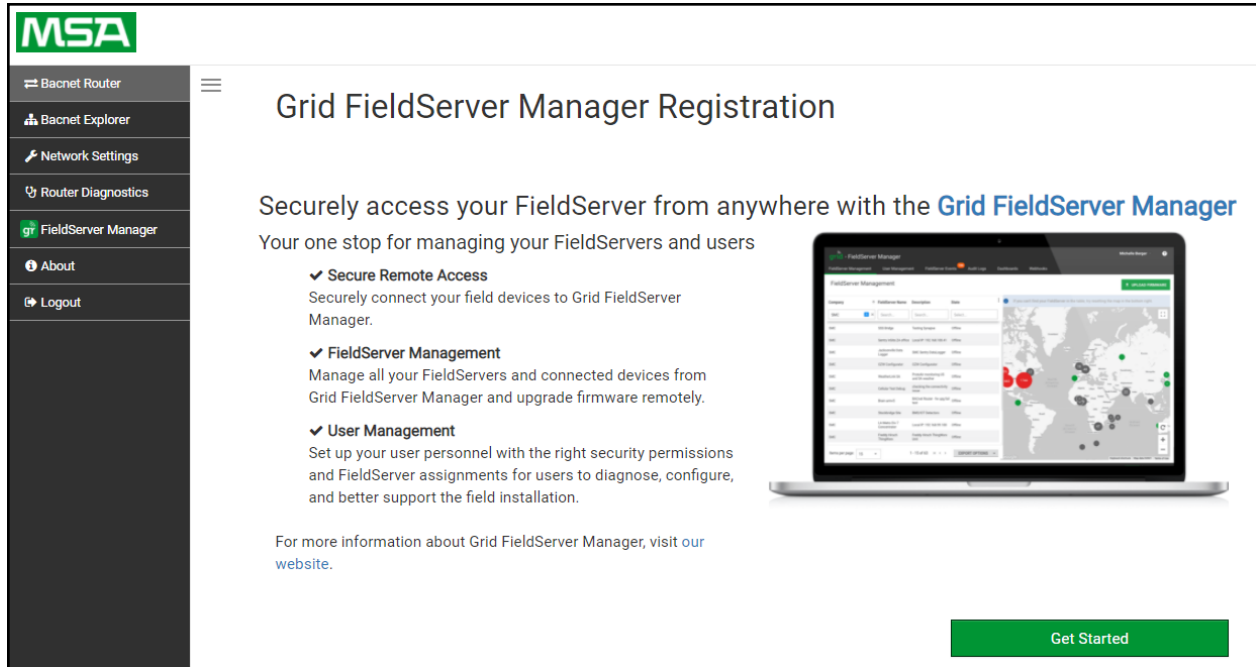
 

There are unsaved settings

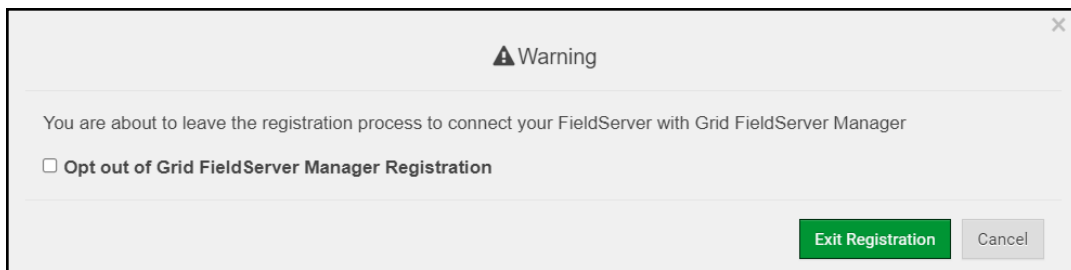
## 8 Configuring the BACnet Router

### 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

The screenshot shows the MSA BACnet Router Settings web interface. The interface is divided into several sections for configuration:

- BACnet Device:** Fields for Device Name (BACnet Router), Device Instance (1000), Device Location (-), and Device Connection (BACnet IP Wired 1).
- BACnet Ethernet:** Fields for Enable (checkbox), Network Number (3).
- BACnet IP Wired 1:** Fields for Enable (checked), Network Number (1), and IP Port (47808).
- BACnet IP Wired 2:** Fields for Enable (checkbox), Network Number (2), and IP Port (47809).
- BACnet IP BBMD:** Section header.
- BACnet MSTP Settings:** Fields for Max Info Frames (50) and Max Master (127).
- BACnet MSTP R1:** Fields for Enable (checkbox), Network Number (4), MAC Address (0), Baud Rate (38400), and Token Usage Timeout (50).
- BACnet MSTP R2:** Section header.

On the right side, there are buttons for **Save** and **Restart** (green), and **Reload** and **Defaults** (grey). Below these are sections for **Status** (Router is online) and **Log**.

Copyright © MSA Safety - Diagnostics fieldserver

### 8.2.1 Button Functions



- **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.

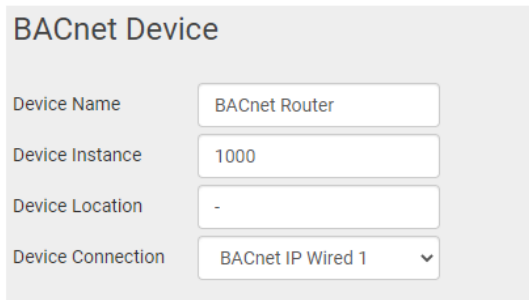
## 8.2.2 Multiple Connections

- **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



The screenshot shows a configuration form titled "BACnet Device" with the following fields:

Field	Value
Device Name	BACnet Router
Device Instance	1000
Device Location	-
Device Connection	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

- **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.

The screenshot displays the MSA FieldServer Manager interface. On the left is a dark sidebar with navigation options: Bacnet Router, Bacnet Explorer, Network Settings, Router Diagnostics (highlighted), FieldServer Manager, About, and Logout. The main content area is titled 'ETH1 - BACnet IP Wired 1'. It shows network statistics for Network Number 1: Messages Sent (270), Messages Received (280), and Total Errors (0). Below this is a 'Routing Table' with columns for DNET, MAC Address, and Status. The table lists ten entries, all with a status of 'Available'. The second network shown is 'ETH1 - BACnet Explorer 47800', with Network Number 7, Messages Sent (258), Messages Received (246), and Total Errors (0). Its routing table is empty. The footer contains the copyright notice 'Copyright © MSA Safety - Diagnostics' and the 'fieldserver' logo.

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

Network Number	Messages Sent	Messages Received	Total Errors
7	258	246	0



## 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.

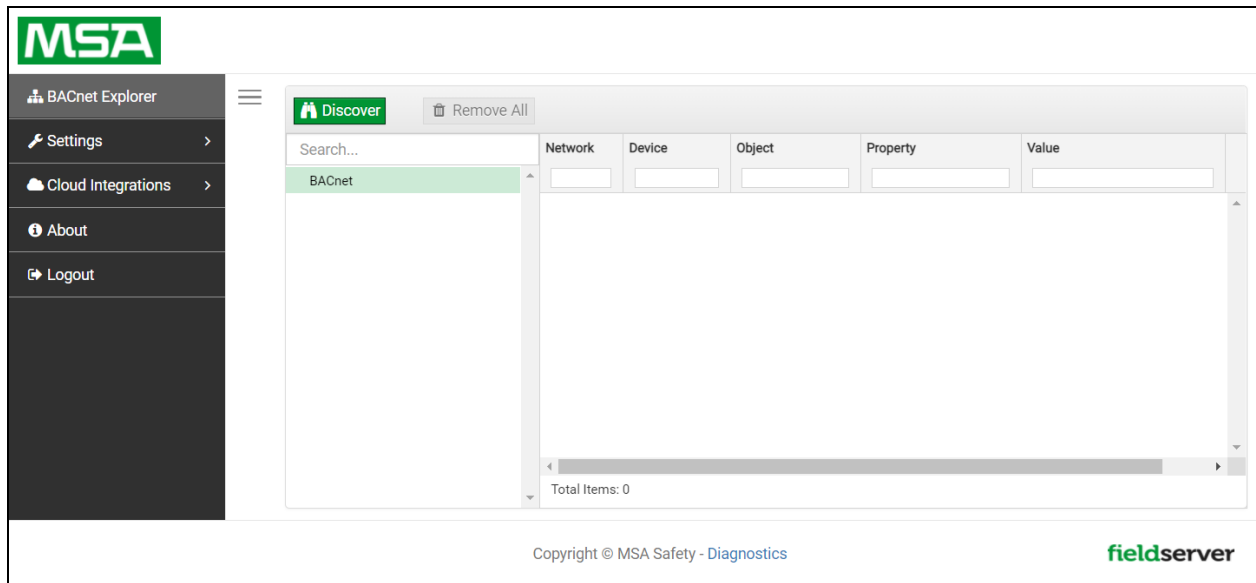
- To access the embedded BACnet Explorer click the BACnet Explorer tab.


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**: Fields for Enable (checked), Network Number (1), and IP Port (47808).   
3. **BACnet IP Wired 2**: Fields for Enable (unchecked), Network Number (2), and IP Port (47809).   
4. **BACnet IP BBMD**: A section header with no visible fields.   
5. **BACnet Ethernet**: Fields for Enable (unchecked) and Network Number (3).   
6. **BACnet MSTP Settings**: Fields for Max Info Frames (50) and Max Master (127).   
7. **BACnet MSTP R1**: Fields for Enable (unchecked), Network Number (4), MAC Address (0), Baud Rate (38400), and Token Usage Timeout (50).   
8. **BACnet MSTP R2**: Fields for Enable (unchecked).   
On the right side, there are control buttons: Save (green), Restart (green), Reload (grey), and Defaults (grey). Below these are two boxes: **Status** (Router is online) and **Log**. The footer contains 'Copyright © MSA Safety - Diagnostics' and the 'fieldserver' logo.

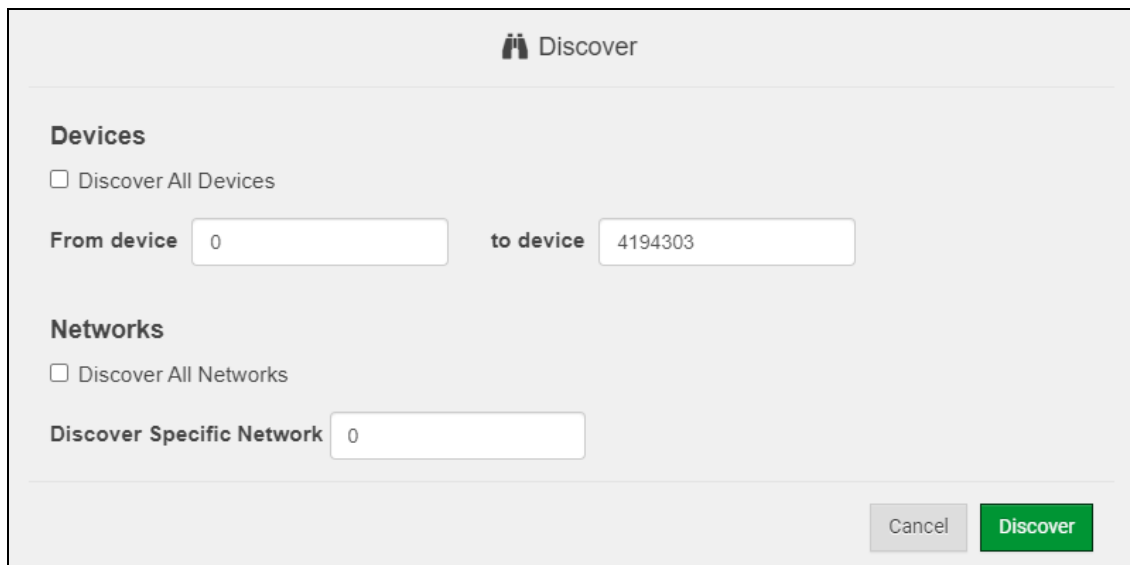
**NOTE:** For BACnet/IP, click on the Settings button on the left side of the landing page to ensure the BACnet Router is on the BACnet/IP network subnet or to configure BBMD.

## 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.



**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.

The screenshot shows the 'Discover' interface with a search bar and a list of devices. The table below represents the data shown in the interface.

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)


## 9.2 View Device Details and Explore Points/Parameters

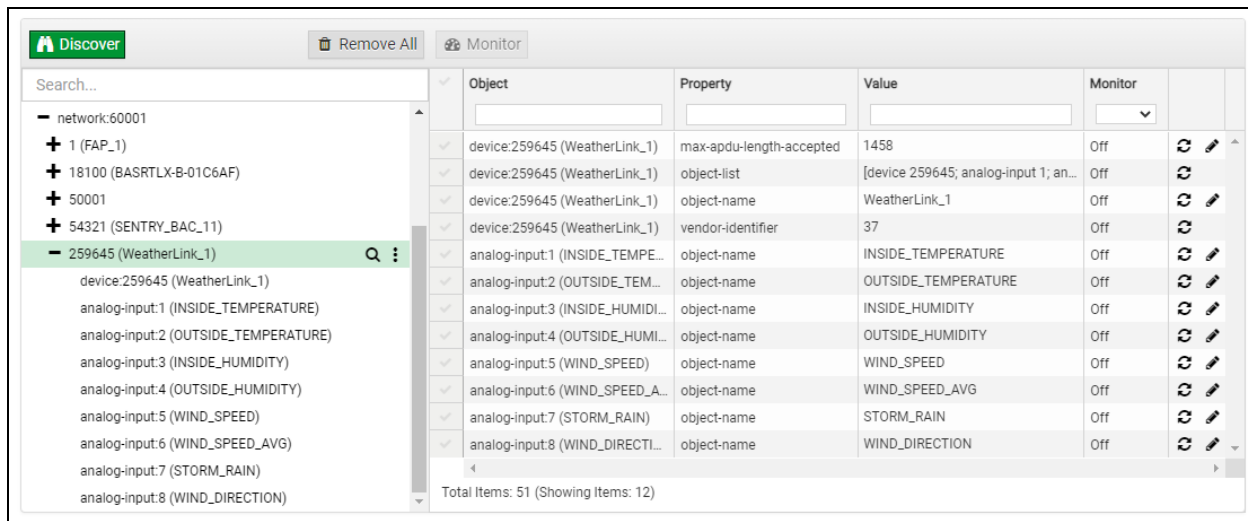
- To view the device details, click the blue plus sign (+) next to the desired device in the list.
  - This will show only some of the device properties for the selected aspect of a device

The screenshot shows the 'Discover' interface with the device '259645 (WeatherLink\_1)' selected. The table below represents the data shown in the interface.

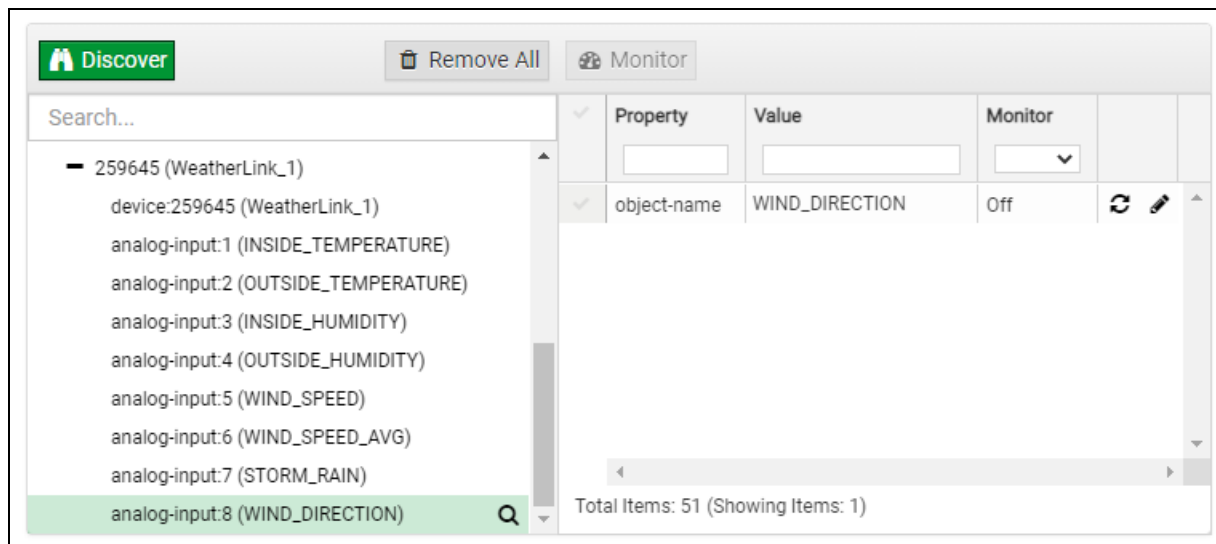
Object	Property	Value	Monitor
device:259645 (WeatherLink_1)	max-apdu-length-accepted	1458	Off
device:259645 (WeatherLink_1)	object-name	WeatherLink_1	Off
device:259645 (WeatherLink_1)	vendor-identifier	37	Off

Total Items: 42 (Showing Items: 3)

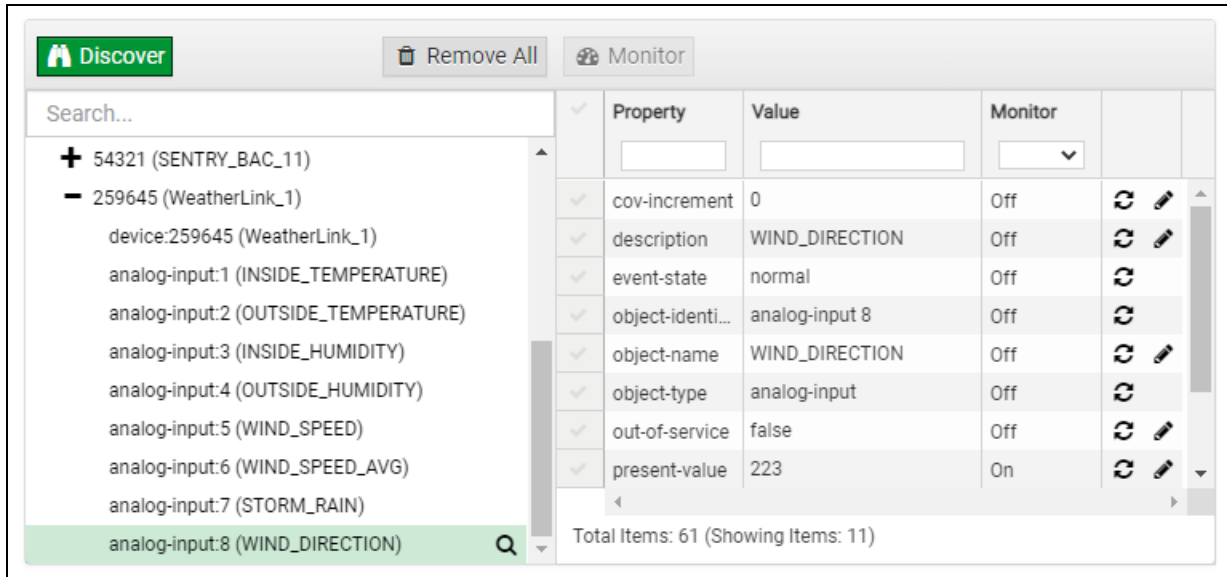
- To view the full details of a device, highlight the device directly (in the image below – “1991 WeatherLink\_1”) and click the Explore button (  ) that appears to the right of the highlighted device as a magnifying glass icon or double-click the highlighted device.



- 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.

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

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

Write Property

present-value 2

Cancel Write

- 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.

The screenshot displays the BACnet Explorer interface. On the left, a tree view shows a hierarchy of devices and analog inputs. The selected item is 'analog-input:8 (WIND\_DIRECTION)'. On the right, a table displays the properties of this selected object.

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)

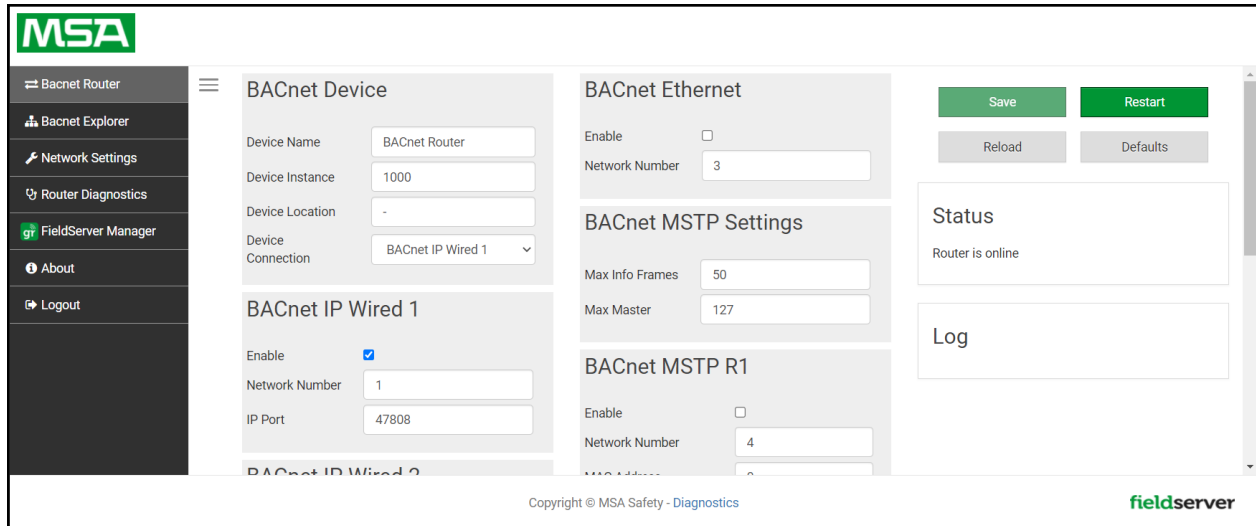
## 10 MSA Grid - FieldServer Manager Setup

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.

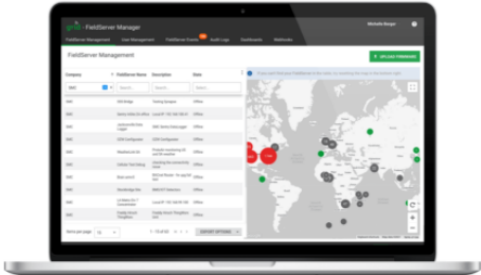
## Grid FieldServer Manager Registration

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 a progress bar at the top with four steps: 1 (Installer Details, highlighted in green), 2 (Installation Site), 3 (FieldServer Details), and 4 (Account Details). Below the progress bar, the 'Installer Details' form contains the following fields:

- Installer Name:
- Company:
- Telephone:
- Email:
- Installation Date:

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

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

The screenshot shows a progress bar at the top with four steps: 1 (Installer Details), 2 (Installation Site, highlighted in green), 3 (FieldServer Details), and 4 (Account Details). Below the progress bar, the 'Installation Site Details' form includes:

- Search:
- Site Name:
- Building:
- Street Address:
- Suburb:
- City:
- State:
- Country:
- Postal Code:
- Latitude:
- Longitude:

On the right side of the form is a Google Maps interface showing a map of the Lafayette area. At the bottom right, there are three buttons: 'Cancel' (grey), 'Previous' (grey), and 'Next' (green).

- Enter Name and Description (required) then click Next

**Grid FieldServer Manager Registration**

Progress: 1 Installer Details, 2 Installation Site, 3 **FieldServer Details**, 4 Account Details

**FieldServer Details**

Name: [Redacted]

Description: [Redacted]

FieldServer Info:

Timezone: (GMT -08:00) America/Los\_Angeles

Buttons: Cancel, Previous, Next

- 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**

Progress: 1 Installer Details, 2 Installation Site, 3 FieldServer Details, 4 **Account Details**

**New Users**

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

[Create an Grid FieldServer Manager account](#)

**Existing Users - Enter FieldServer registration details**

**User Credentials**

Username: [Redacted]

Password: [Redacted]

Buttons: Cancel, Previous, Register FieldServer

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

## Grid FieldServer Manager Registration

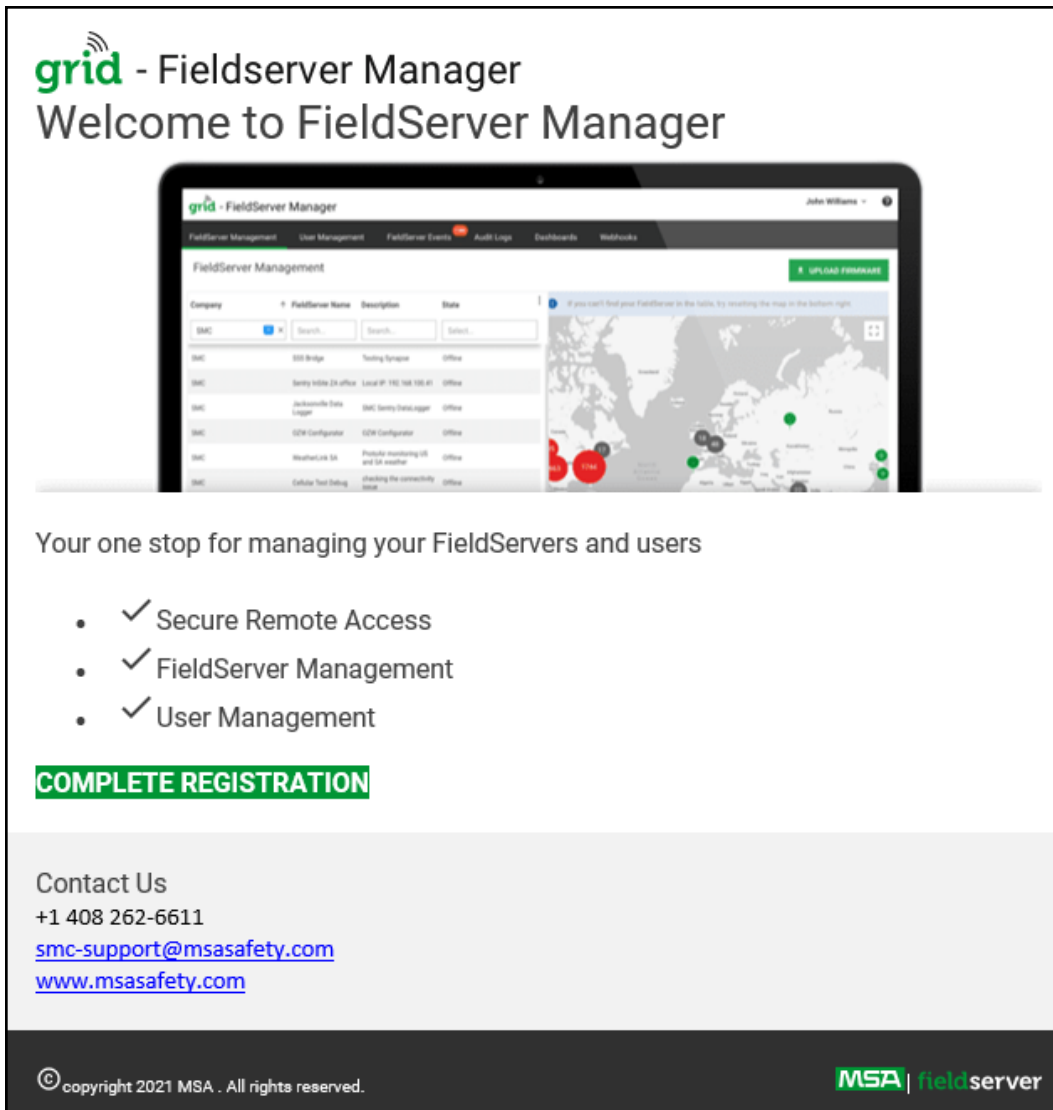
### FieldServer Registered

<b>FieldServer Details</b>	<b>Installer Details</b>	<b>Installation Site Details</b>
<b>Name:</b> Test1 <b>Description:</b> FS Test <b>FieldServer Info:</b> <b>Timezone:</b> America/Los_Angeles <b>MAC Address:</b> 00:50:4E:60:13:FE <b>Tunnel Server URL:</b> tunnel.fieldpop.io <b>FieldServer ID:</b> treedancer_KrgPKmLRY <b>Product Name:</b> Core Application - Default <b>Product Version:</b> 5.2.0	<b>Installer Name:</b> Test <b>Company:</b> MSA Safety <b>Telephone:</b> (408) 444-4444 <b>Email:</b> contactus@msasafety.com <b>Installation Date:</b> Sep 20, 2021	<b>Site Name:</b> Site#1 <b>Building:</b> <b>Street Address:</b> 1020 Canal Road <b>Suburb:</b> <b>City:</b> Lafayette <b>State:</b> Indiana <b>Country:</b> United States <b>Postal Code:</b> 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 FieldServer Manager” email will appear as shown below.



**NOTE:** If no Grid email was received, check the spam/junk folder for an email from [notification@fieldpop.io](mailto: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 \*Invalid Mobile Number  
 \*

Confirm Password \* Please enter new password  
 \*

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

\* Mandatory Fields

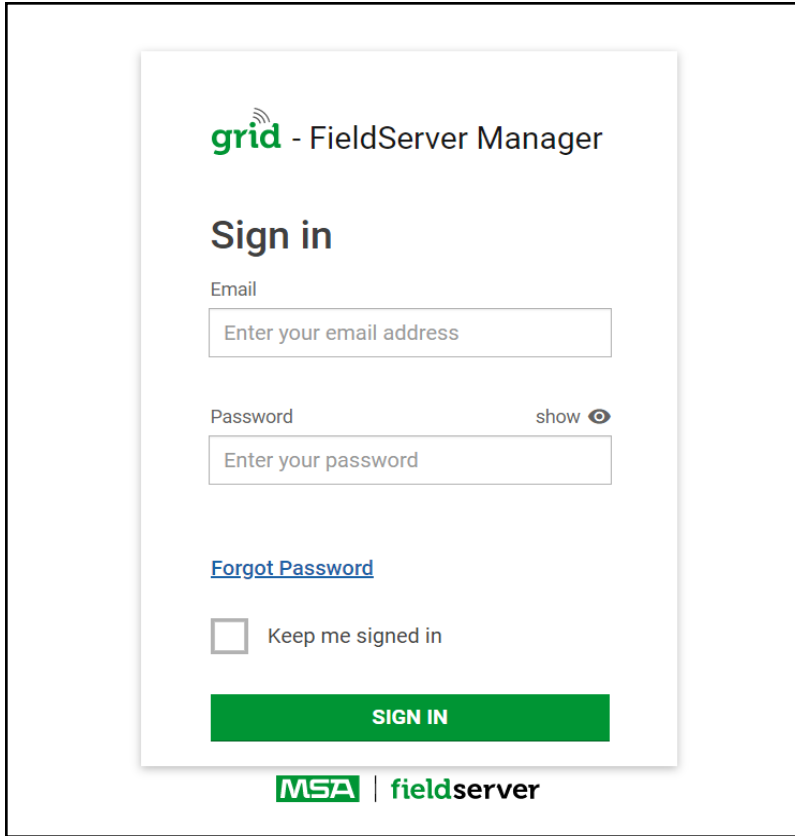
- Fill in the name, phone number, password fields and click the checkbox to agree to the privacy policy and terms of service.

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

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

## 10.2 Login to the FieldServer Manager

After the gateway is registered, go to [www.smccloud.net](http://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' is displayed in green, followed by the text '- FieldServer Manager'. Below this is the heading 'Sign in'. There are two input fields: one for 'Email' with the placeholder text 'Enter your email address', and one for 'Password' with the placeholder text 'Enter your password'. To the right of the password field is a 'show' button with an eye icon. Below the password field is a blue link for 'Forgot Password'. There is a checkbox labeled 'Keep me signed in'. At the bottom of the form is a green button labeled 'SIGN IN'. Below the form, the logos for 'MSA' and 'fieldserver' are displayed.

**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](#).

**FieldServer Management**

↑ **UPLOAD FIRMWARE**

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

Company	FieldServer Name	Description	State
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

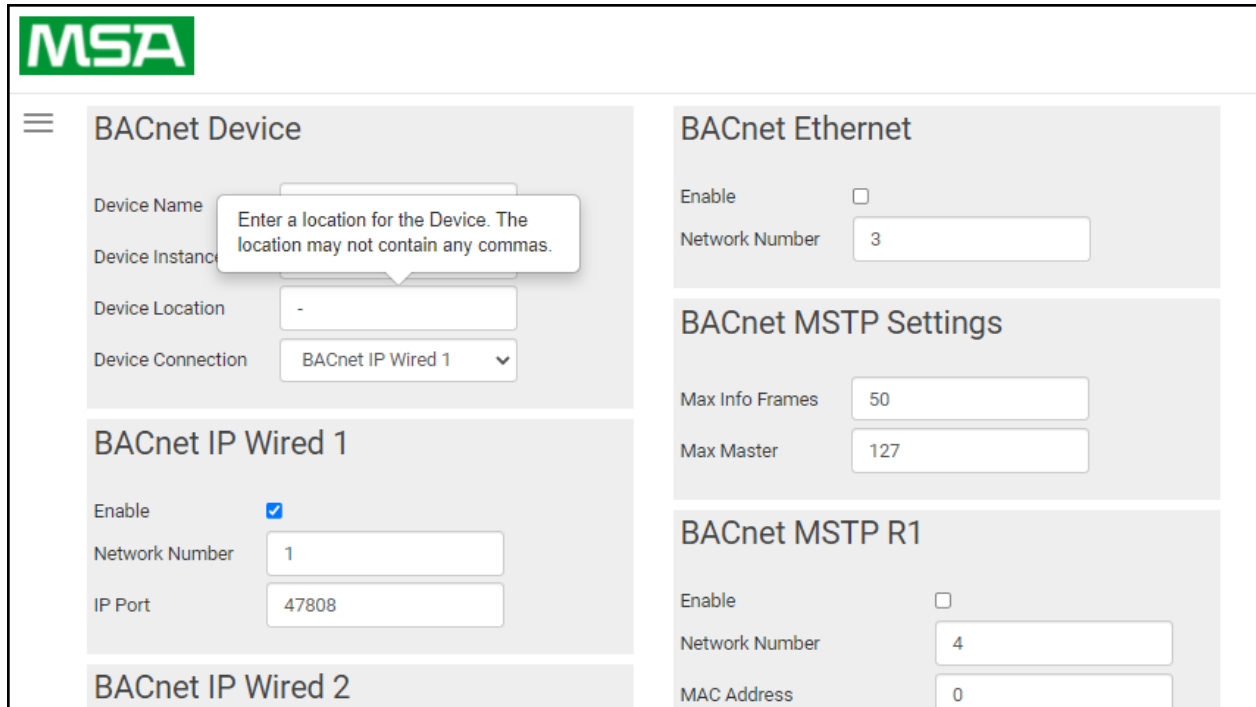
© 2021 MSA. All rights reserved. **MSA | fieldserver**



## 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 configuration interface for BACnet settings. The interface is organized into several sections:

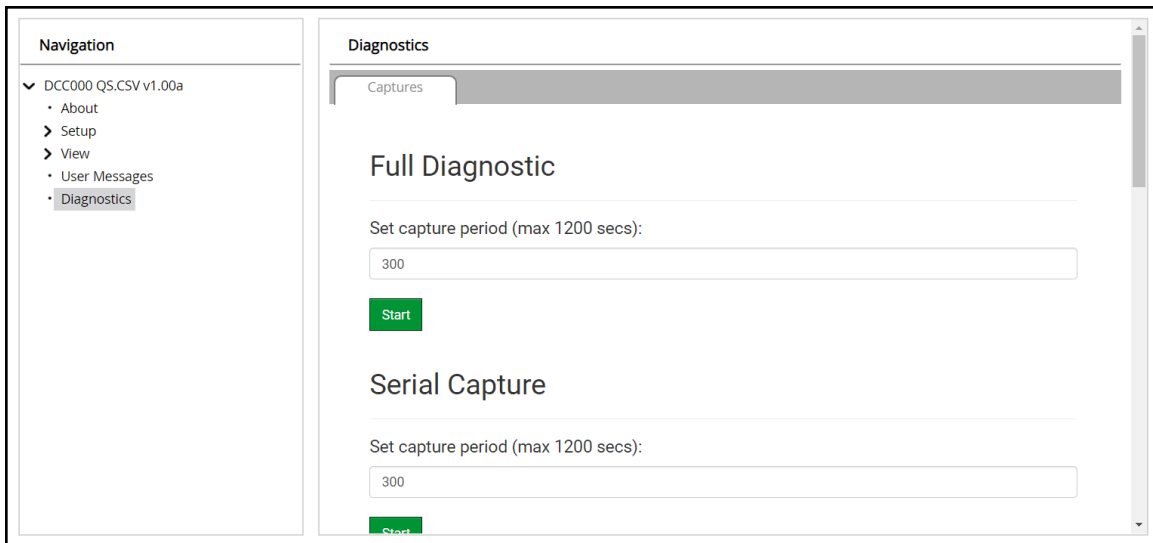
- BACnet Device:** Contains fields for Device Name, Device Instance, Device Location (with a tooltip), and Device Connection (set to BACnet IP Wired 1).
- BACnet IP Wired 1:** Contains fields for Enable (checked), Network Number (1), and IP Port (47808).
- BACnet IP Wired 2:** Section header.
- BACnet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

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

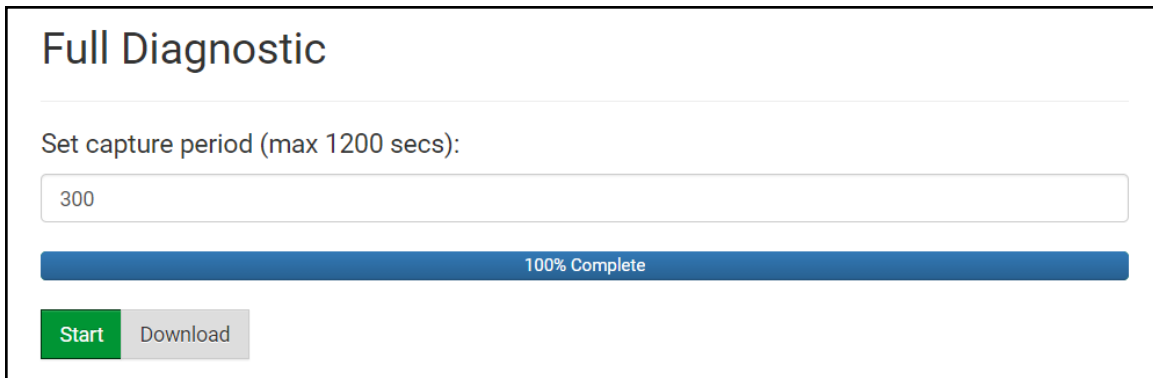
## 11.2 Taking a FieldServer Diagnostic Capture

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



- 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



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

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

### 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.

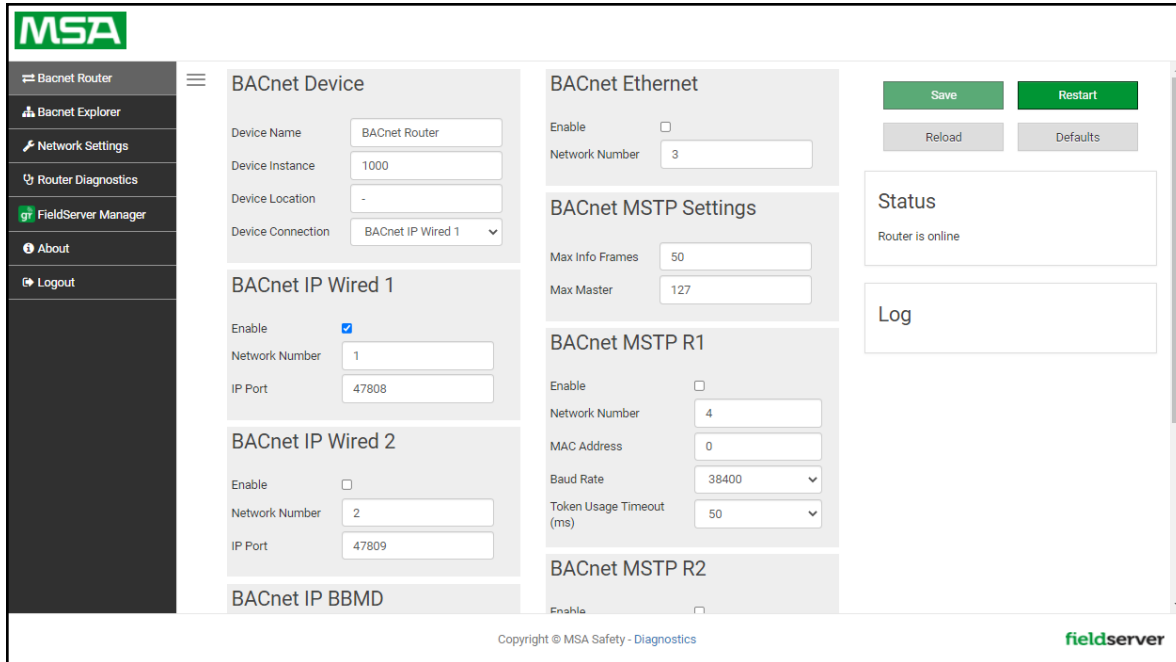
**NOTE:** Computer and network firewalls must be opened for Port 80 to allow FieldServer GUI to function.

## 12 Additional Information

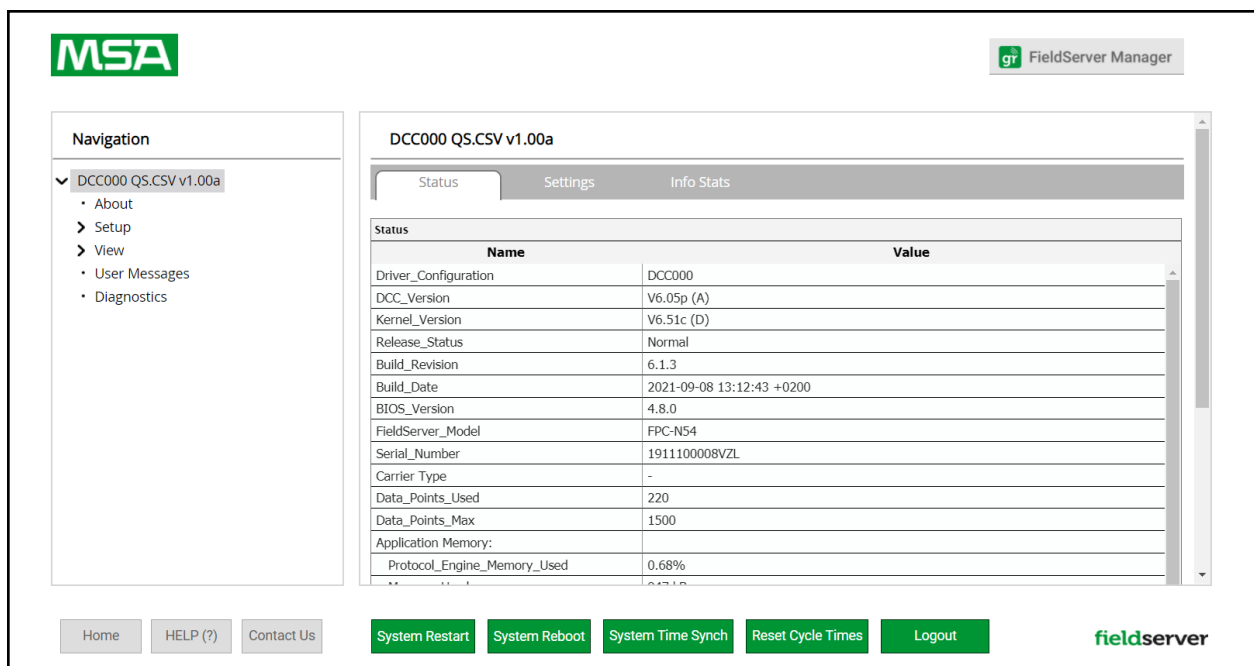
### 12.1 Change Web Server Security Settings After Initial Setup

**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.

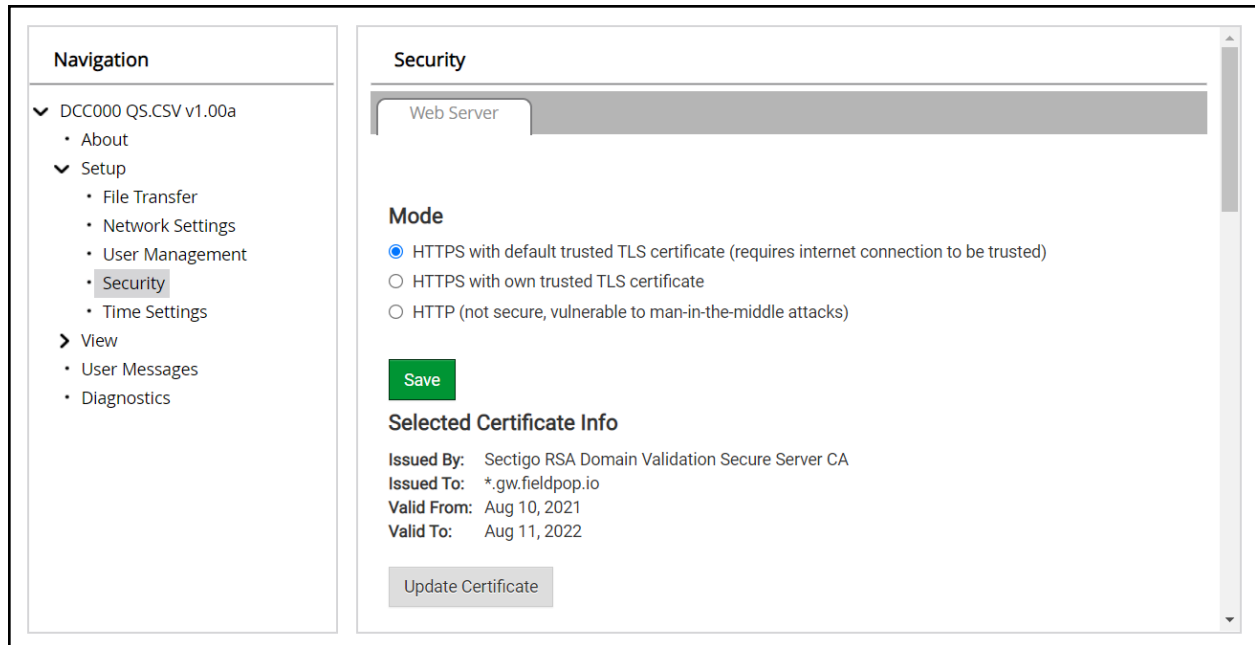


- Click Setup in the Navigation panel.



## 12.1.1 Change Security Mode

- Click Security in the Navigation panel.

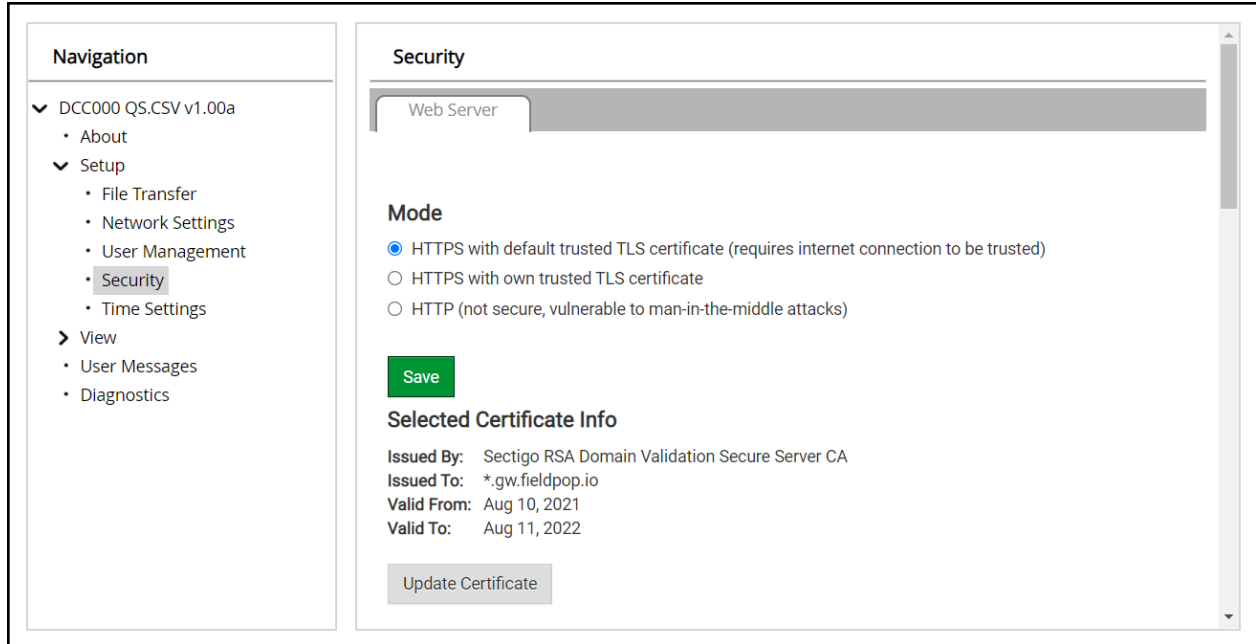


- Click the Mode desired.
  - If HTTPS with own trusted TLS certificate is selected, follow instructions in [Section 6.2.1 HTTPS with Own Trusted TLS Certificate](#)
- Click the Save button.

### 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.



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

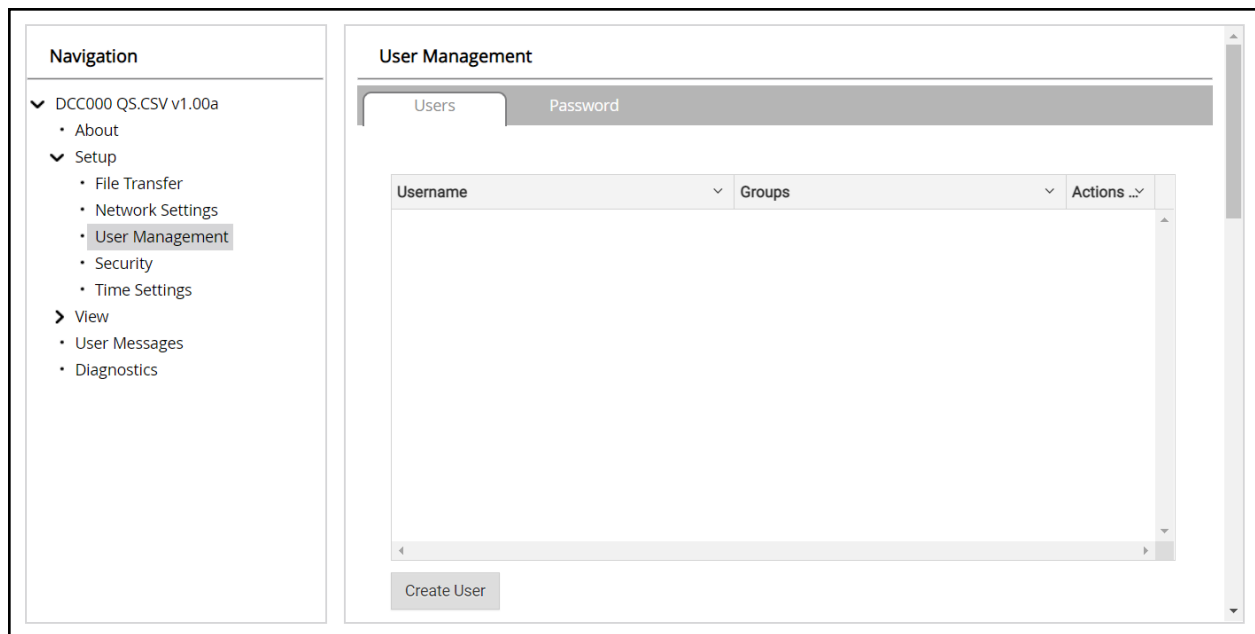
## 12.2 Change User Management Settings

- 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.

**Create User**

**Username:**  
Enter a unique username

**Security Groups:**

- Admin
- Operator
- Viewer

**Password:** Weak  
Enter password

Show Passwords

**Confirm Password:**  
Confirm password

Generate Password

Create Cancel

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

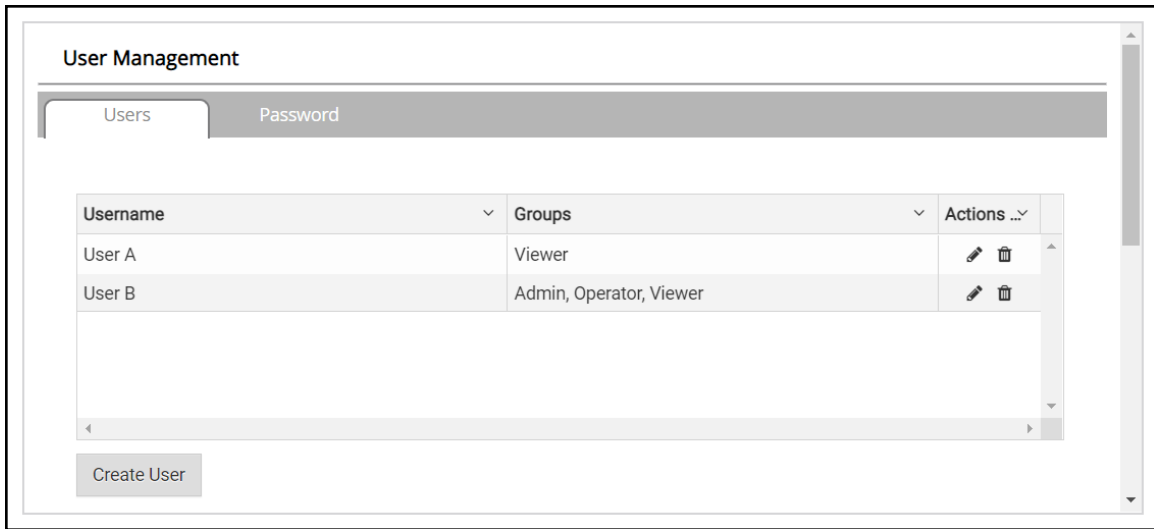
**NOTE:** The password must meet the minimum complexity requirements. An algorithm automatically checks the password entered and notes the level of strength on the top right of the Password text field.

- 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.



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

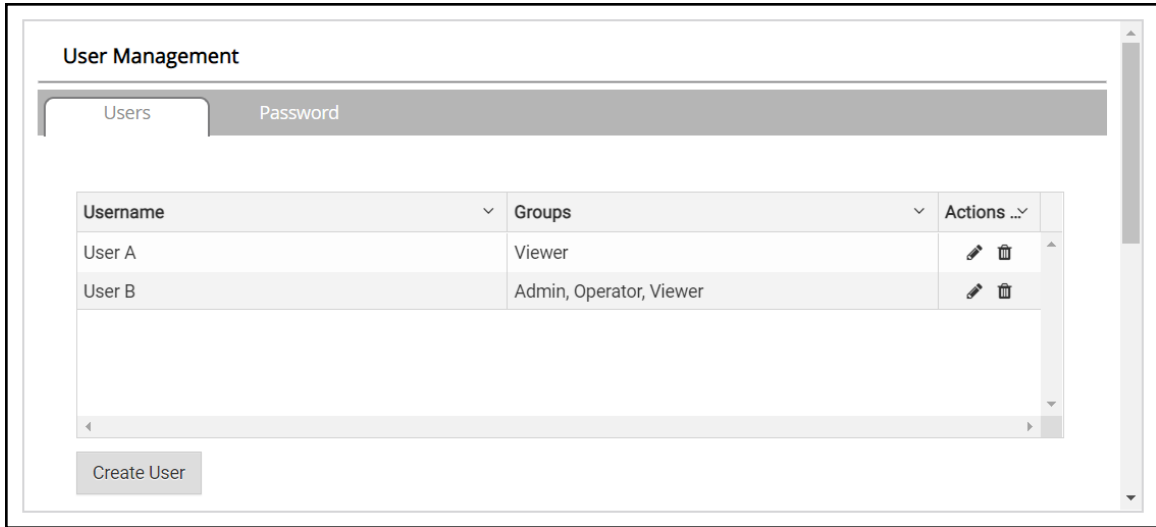
The 'Edit User' dialog box contains the following fields and options:

- Username:** A text input field containing 'User A'.
- Security Groups:** Three checkboxes:  Admin,  Operator, and  Viewer.
- Password:** A text input field containing 'Optional'.
- Show passwords
- Confirm Password:** A text input field containing 'Optional'.
- 
- (highlighted in green)
- 

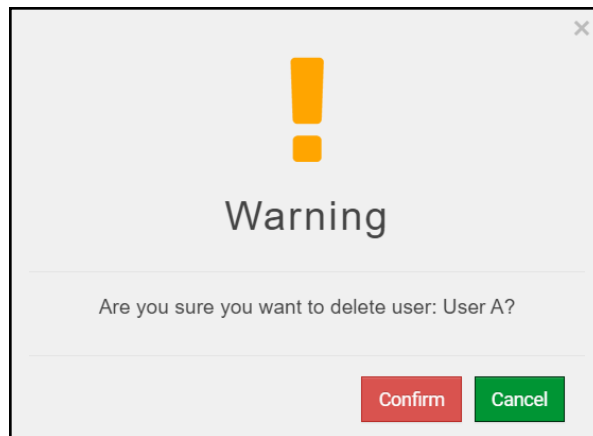
- Click Confirm.
- Once the Success message appears, click OK.

### 12.2.3 Delete Users

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

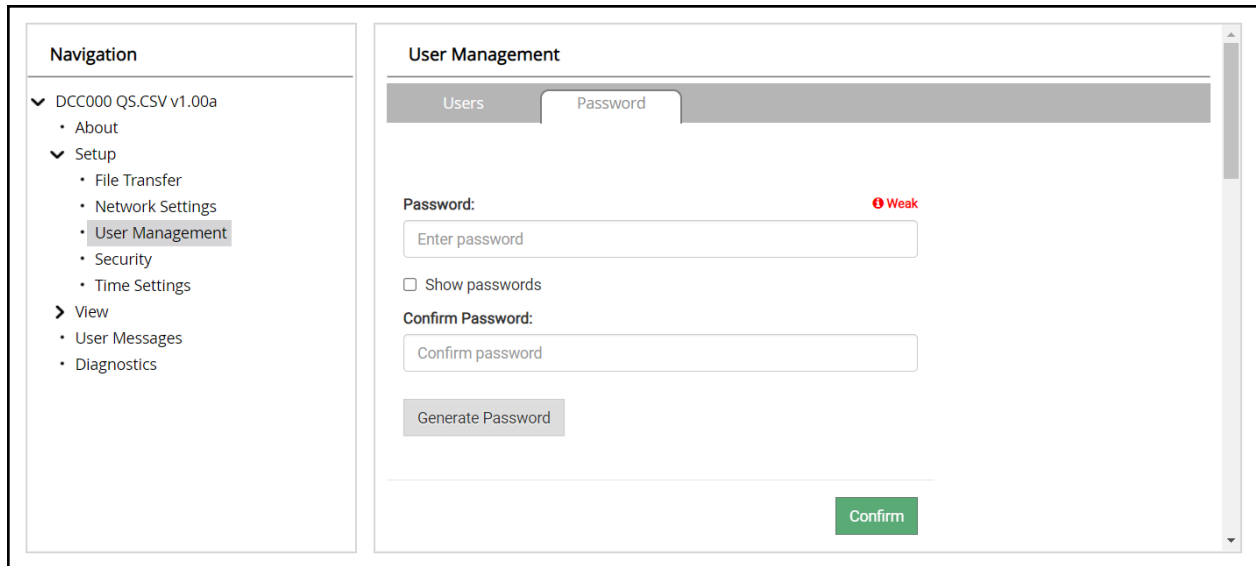


- When the warning message appears, click Confirm.



## 12.2.4 Change FieldServer Password

- Click the Password tab.



The screenshot shows a web interface for 'User Management' with two tabs: 'Users' and 'Password'. The 'Password' tab is active. On the left is a 'Navigation' sidebar with a tree structure: 'DCC000 QS.CSV v1.00a' (expanded) containing 'About', 'Setup' (expanded) containing 'File Transfer', 'Network Settings', 'User Management' (highlighted), 'Security', and 'Time Settings', and 'View' containing 'User Messages' and 'Diagnostics'. The main content area has a 'Password:' label with a red 'Weak' indicator and a password input field containing 'Enter password'. Below it is a 'Show passwords' checkbox. A 'Confirm Password:' label is followed by a 'Confirm password' input field. A 'Generate Password' button is located below the input fields. At the bottom right of the main area is a green 'Confirm' button.

- 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	
<b>Electrical Connections</b>	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
<b>Power Requirements</b>	<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
<b>Approvals</b>	CE and FCC Class B & C Part 15, UL 60950-1, WEEE compliant, IC Canada, RoHS3 compliant, REACH compliant, UKCA compliant
<b>Physical Dimensions</b>	4 x 1.1 x 2.7 in (10.16 x 2.8 x 6.8 cm)
<b>Weight</b>	0.4 lbs (0.2 Kg)
<b>Operating Temperature</b>	-20°C to 70°C (-4°F to 158°F)
<b>Humidity</b>	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.