



FieldServer
BACnet Router FS-ROUTER-BAC2
Start-up Guide
BAS Router (BACnet Multi-Network Router)



APPLICABILITY & EFFECTIVITY

The instructions are effective for the above as of September 2020.

Document Revision: 2.A
T18625

Technical Support

Please call us for any technical support needs related to the FieldServer product.

MSA Safety
1991 Tarob Court
Milpitas, CA 95035

Website: www.sierramonitor.com

U.S. Support Information:

+1 408 964-4443
+1 800 727-4377

Email: smc-support@msasafety.com

EMEA Support Information:

+31 33 808 0590

Email: smc-support.emea@msasafety.com

TABLE OF CONTENTS

1	BACnet Router Description	5
2	Equipment Setup	6
2.1	Mounting	6
3	Installing the BACnet Router	7
3.1	Connecting the R1 and R2 Ports	7
3.1.1	Wiring	7
3.2	10/100 Ethernet Connection Port	8
4	Power Up the Device	9
5	Connecting to the BACnet Router	10
5.1	Using the FieldServer Toolbox	10
5.2	Using a Web Browser Directly	10
6	Setup Web Server Security	11
6.1	Login to the FieldServer	11
6.2	Select the Security Mode	13
6.2.1	HTTPS with Own Trusted TLS Certificate	14
6.2.2	HTTPS with Default Untrusted Self-Signed TLS Certificate or HTTP with Built-in Payload Encryption	14
7	Configuring the BACnet Router	15
7.1	Navigate to the BACnet Router Settings	15
7.2	BACnet Router Settings	16
7.2.1	Button Functions	16
7.2.2	Multiple Connections	17
7.2.3	BACnet Device	17
7.2.4	BACnet/IP	18
7.2.5	BACnet MS/TP, BACnet Ethernet and BACnet Explorer	19
7.3	Network Settings	20
7.4	Router Diagnostics	21
8	BACnet Explorer	22
8.1	Discover Device List	23
8.2	View Device Details and Explore Points/Parameters	24
8.2.1	Edit the Present Value Field	27
9	SMC Cloud Setup	29
9.1	Create a New SMC Cloud Account	29
9.2	Login to SMC Cloud	36
Appendix A	Useful Features	38
Appendix A.1	Tooltips	38
Appendix A.2	Taking a FieldServer Diagnostic Capture	39
Appendix A.3	Factory Reset Instructions	40
Appendix A.4	Internet Browser Software Support	40
Appendix A.5	Change Web Server Security Settings After Initial Setup	41
Appendix A.5.1	Change Security Mode	42
Appendix A.5.2	Edit the Certificate Loaded onto the FieldServer	43
Appendix A.6	Change User Management Settings	44
Appendix A.6.1	User Management	44
Appendix A.6.1.1	Create Users	45
Appendix A.6.1.2	Edit Users	46
Appendix A.6.1.3	Delete Users	47
Appendix A.6.2	Change FieldServer Password	48
Appendix B	Reference	49
Appendix B.1	Specifications	49
Appendix B.2	FS-ROUTER-BAC2 Dimension Drawing	50
Appendix C	Limited 2 Year Warranty	51

LIST OF FIGURES

Figure 1: DIN Rail Bracket	6
Figure 2: DIN Rail Mounted.....	6
Figure 3: R1 & R2 Connection Ports.....	7
Figure 4: Ethernet Connection	8
Figure 5: Required Current Draw for the Gateway	9
Figure 6: Power Connections.....	9
Figure 7: Web Server Security Unconfigured Window	11
Figure 8: Connection Not Private Warning	11
Figure 9: Warning Expanded Text	12
Figure 10: FieldServer Login.....	12
Figure 11: Security Mode Selection Screen.....	13
Figure 12: Security Mode Selection Screen.....	14
Figure 13: BACnet Router Landing Page	15
Figure 14: Opt Out Warning Message	15
Figure 15: BACnet Router Settings Page	16
Figure 16: Network Settings.....	20
Figure 17: BACnet Router Diagnostics Page.....	21
Figure 18: FS-GUI BACnet Explorer Button	22
Figure 19: BACnet Explorer Page.....	23
Figure 20: Discover Window	23
Figure 21: Device List	24
Figure 22: Device Sub-items.....	24
Figure 23: Full Device Sub-items.....	25
Figure 24: Simplified Device Details	25
Figure 25: Additional Device Details	26
Figure 26: Highlighted Present Value	27
Figure 27: Write Property Window	27
Figure 28: Updated Present Value.....	28
Figure 29: BACnet Router Landing Page – SMC Cloud Tab.....	29
Figure 30: Registration Information Page	29
Figure 31: SMC Cloud Connection Problems Message	30
Figure 32: SMC Cloud Registration – Installer Details	31
Figure 33: SMC Cloud Registration – Site Details.....	31
Figure 34: SMC Cloud Registration – Gateway Details.....	32
Figure 35: SMC Cloud Registration – SMC Cloud Account.....	32
Figure 36: Device Registered for SMC Cloud.....	33
Figure 37: Welcome to SMC Cloud Email	34
Figure 38: Setting User Details	35
Figure 39: SMC Cloud Login Page	36
Figure 40: SMC Cloud Privacy Policy	36
Figure 41: SMC Cloud Landing Page	37
Figure 42: Settings Tooltips	38
Figure 43: BACnet Router Landing Page	41
Figure 44: FS-GUI Landing Screen	41
Figure 45: FS-GUI Security Setup	42
Figure 46: FS-GUI Security Setup – Certificate Loaded.....	43
Figure 47: FS-GUI User Management.....	44
Figure 48: Create User Window.....	45
Figure 49: Setup Users	46
Figure 50: Edit User Window	46
Figure 51: Setup Users	47
Figure 52: User Delete Warning	47
Figure 53: FieldServer Password Update via FS-GUI	48
Figure 54: Specifications.....	49
Figure 55: BACnet Router Dimensions.....	50

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 MSA Safety's SMC Cloud.

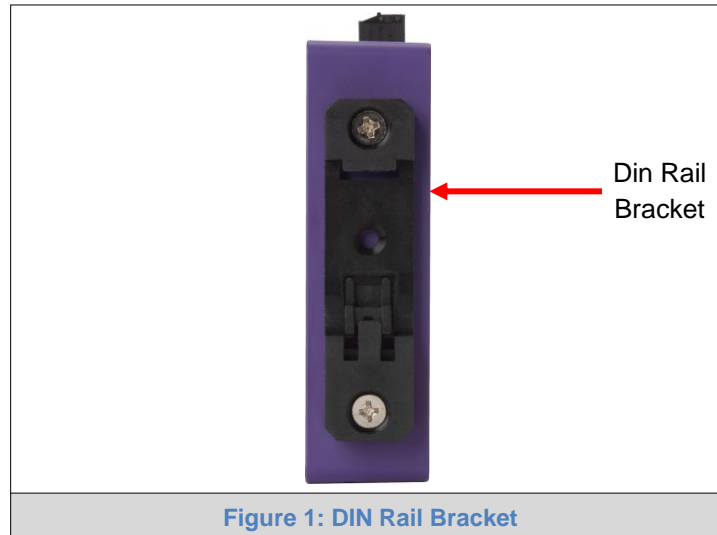
NOTE: For SMC Cloud information, refer to the [SMC Cloud Start-up Guide](#) online at the **Sierra Monitor website**.

NOTE: The latest versions of instruction manuals, driver manuals, configuration manuals and support utilities are available online at the [Sierra Monitor website](#).

2 EQUIPMENT SETUP

2.1 Mounting

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



NOTE: For dimension details see [Appendix B.2](#).



3 INSTALLING THE BACNET ROUTER

3.1 Connecting the R1 and 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.

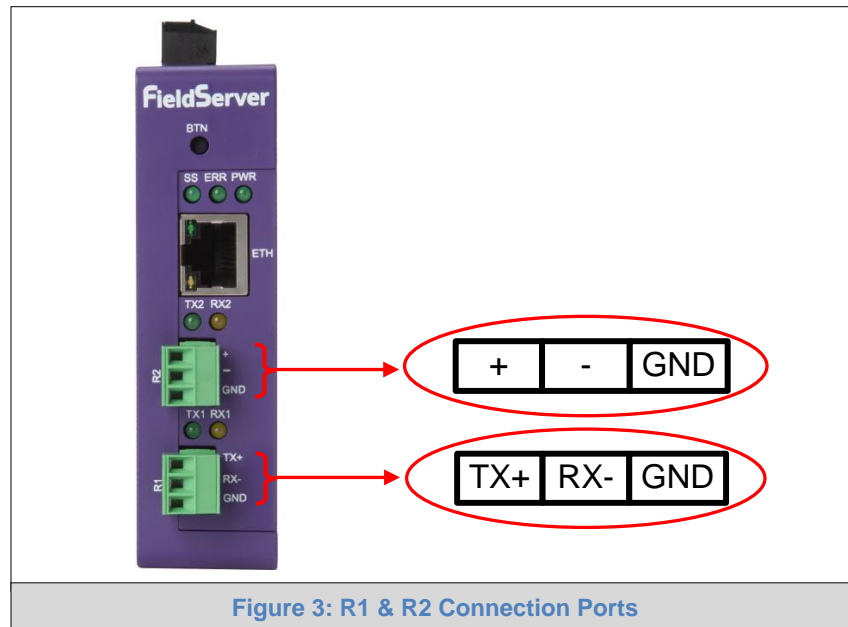


Figure 3: R1 & R2 Connection Ports

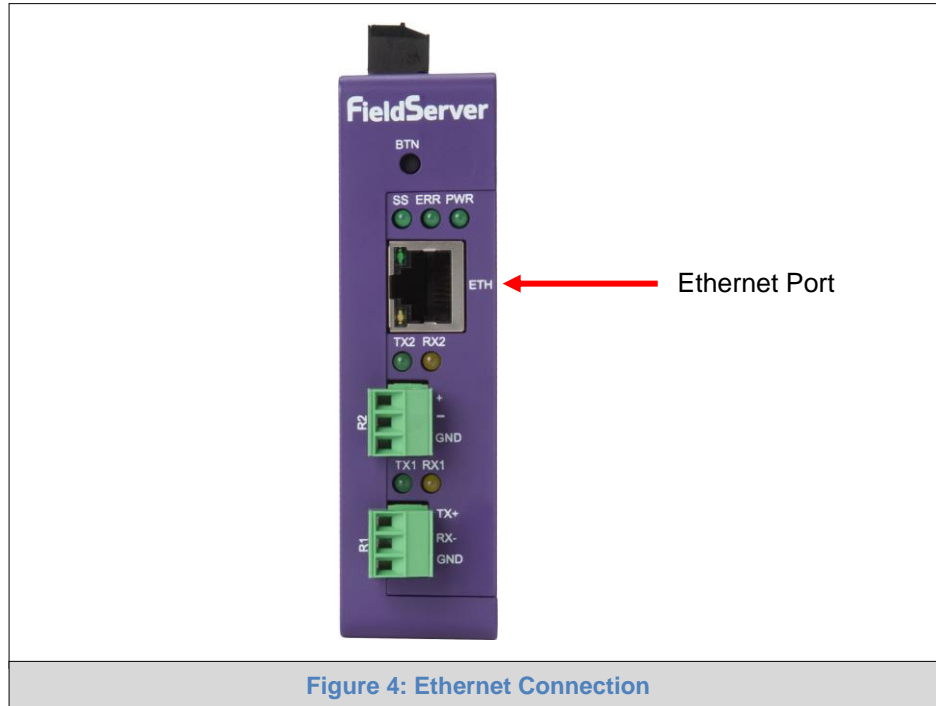
The following baud rates are supported:
9600, 19200, 38400, 76800

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 BACnet Router via the Web App. To connect the BACnet Router, 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 BACnet Router is 192.168.2.101, Subnet Mask is 255.255.255.0.

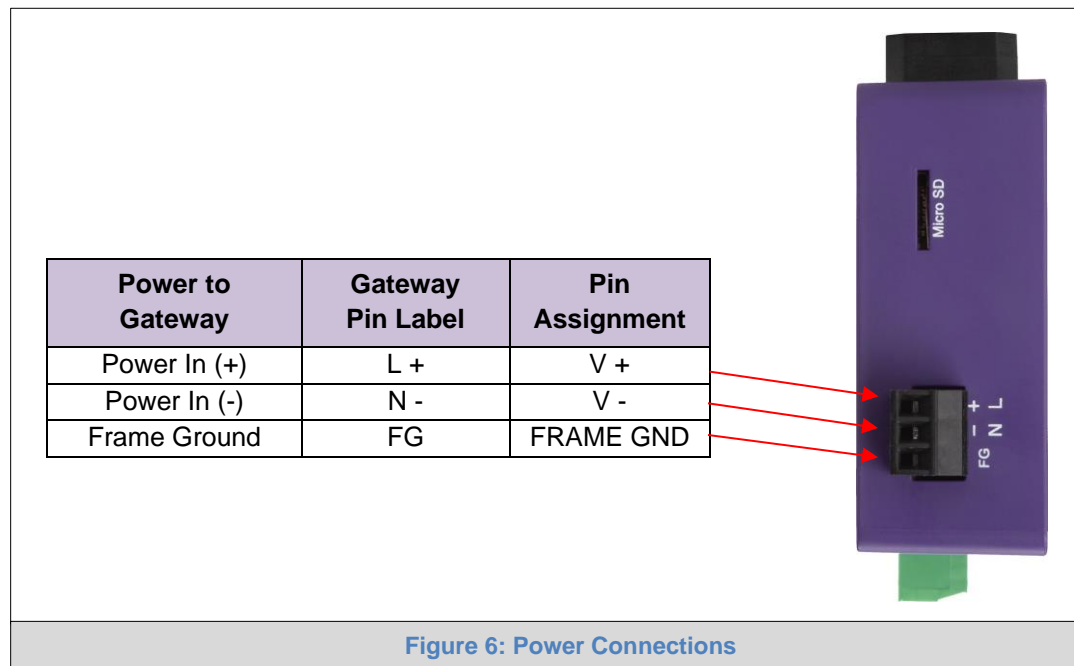
4 POWER UP THE DEVICE

Check power requirements in the table below:


Power Requirement for 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.		
Figure 5: Required Current Draw for the Gateway		

Apply power to the BACnet Router as shown below in [Figure 6](#). Ensure that the power supply used complies with the specifications provided in [Appendix B.1](#).

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

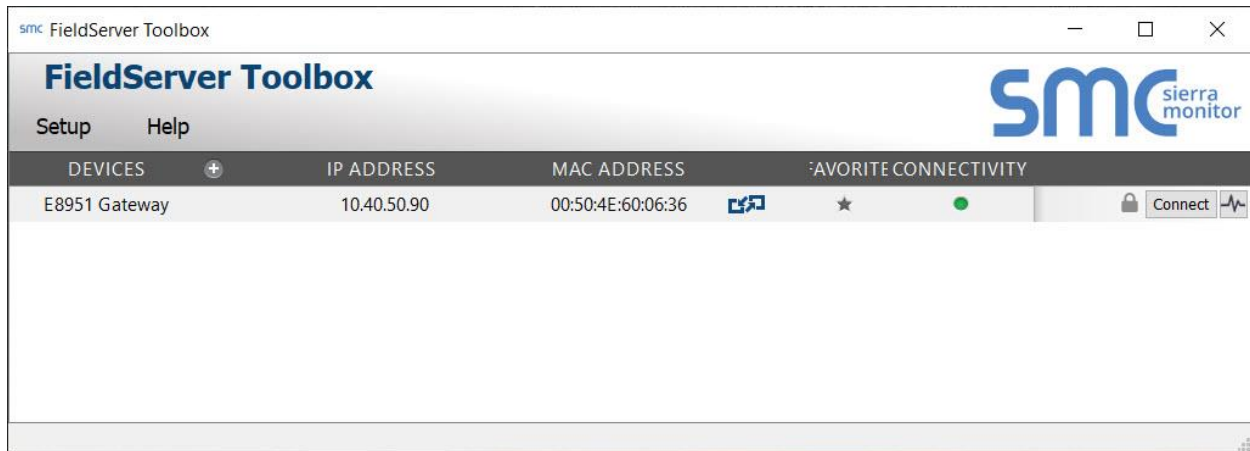


5 CONNECTING TO THE BACNET ROUTER

The FieldServer Toolbox Application can be used to discover and connect to the BACnet Router on a local area network. To connect to the BACnet Router over the Internet using Toolbox, add the Internet exposed IP Address of the Router by clicking on the  button, or alternatively enter the Internet exposed IP Address in a web browser directly.

5.1 Using the FieldServer Toolbox

- Install the FS Toolbox application from the USB drive or download it from the [Sierra Monitor website](#).
- Use the FS Toolbox application to find the BACnet Router and launch the Web App (by clicking the Connect button).



5.2 Using a Web Browser Directly

Open a Web Browser and input the BACnet Router's IP Address. The Default IP Address of the BACnet Router 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.

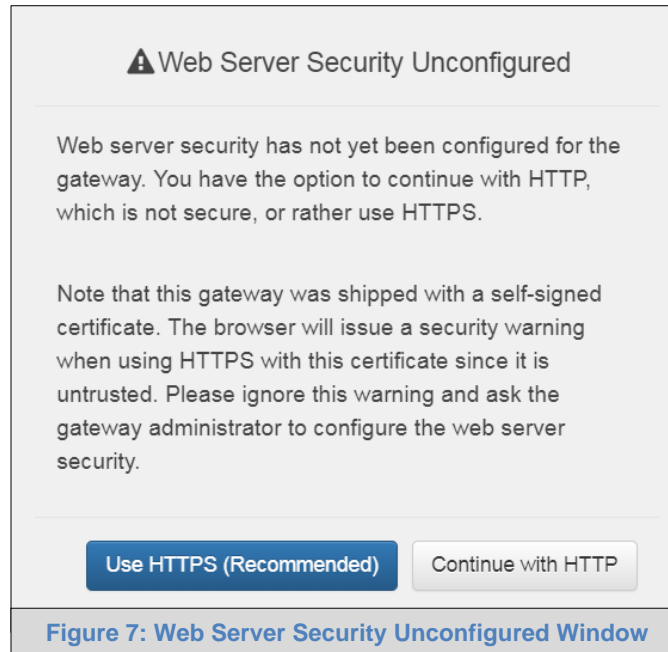
NOTE: Check [Appendix A.4](#) for supported browsers.

6 SETUP WEB SERVER SECURITY

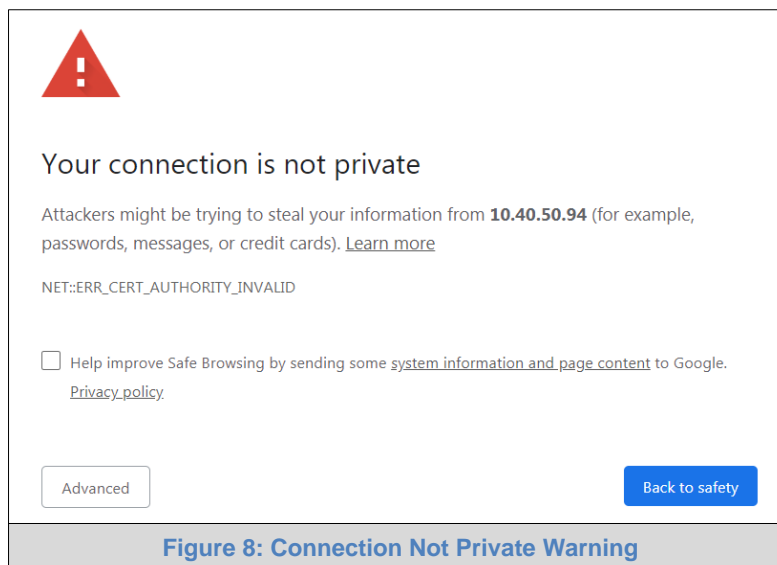
6.1 Login to the FieldServer

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.

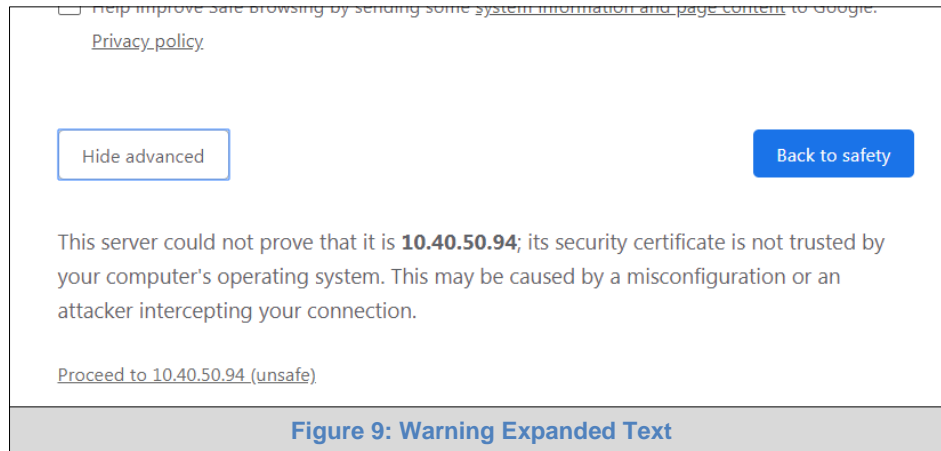
- When the Web Server Security Unconfigured window appears, read the text and choose whether to move forward with HTTPS or HTTP.



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

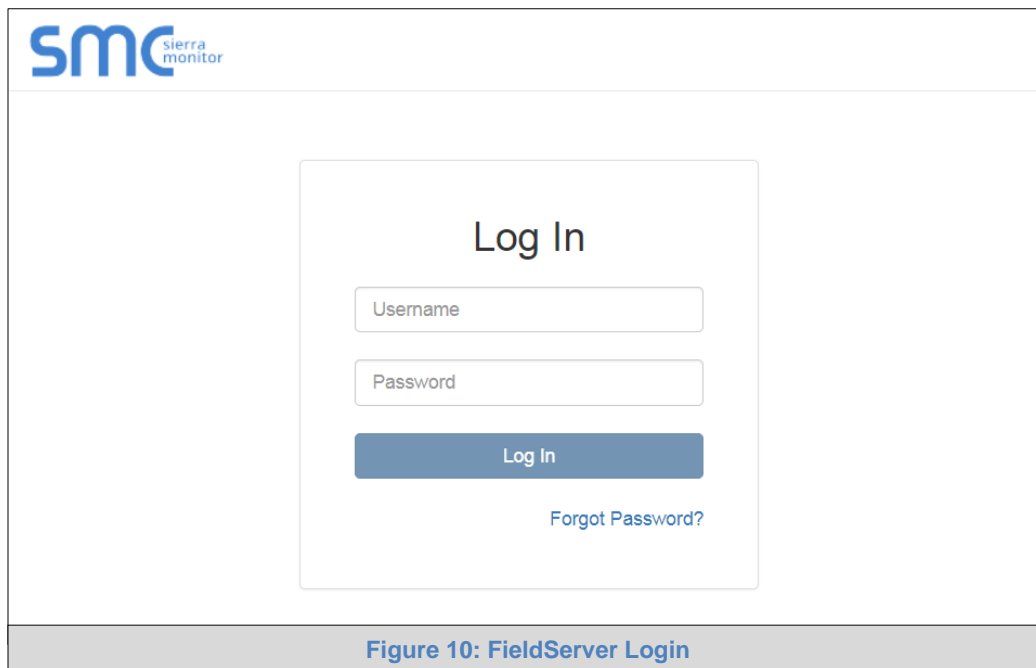


- Additional text will expand below the warning, click the underlined text to go to the IP Address. In the **Figure 9** example this text is “[Proceed to 10.40.50.94 \(unsafe\)](#)”.



- 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.

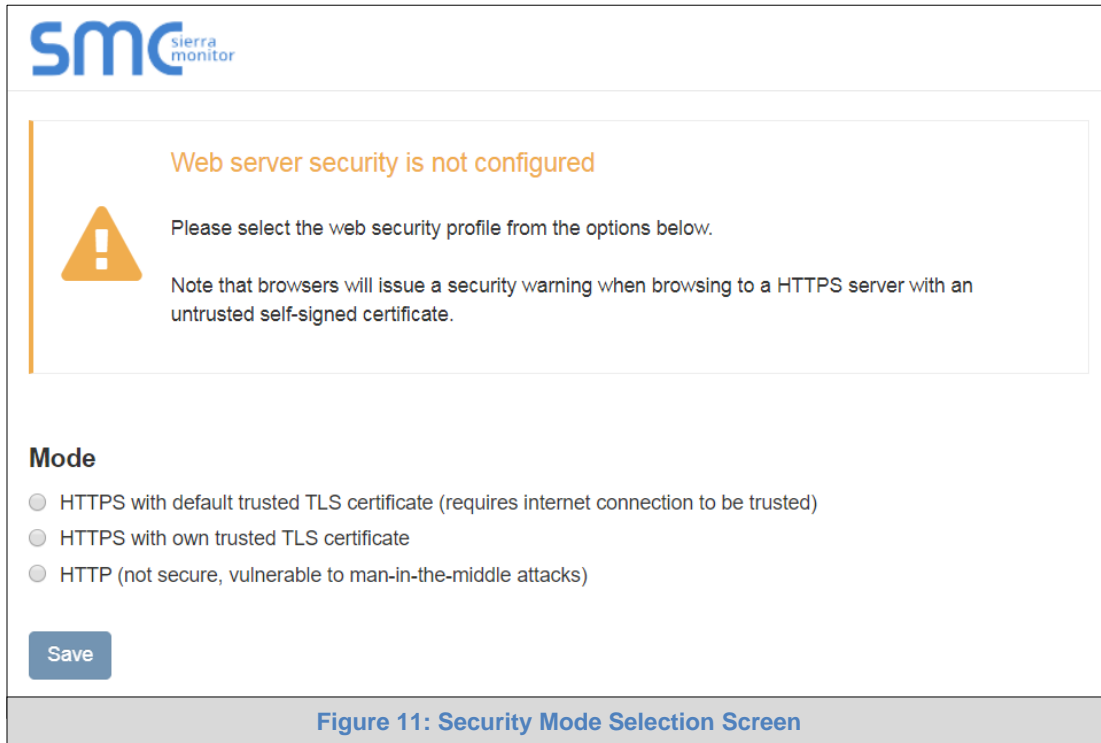


NOTE: A user has 5 attempts to login then there will be a 10-minute lockout. There is no timeout on the FieldServer to enter a password.

NOTE: To create individual user logins, go to [Appendix A.6](#).

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.



The screenshot shows the 'Web server security is not configured' warning screen. It features the smc logo at the top left. A yellow warning triangle icon is on the left side of a light gray box. The text inside the box reads: 'Web server security is not configured', 'Please select the web security profile from the options below.', and 'Note that browsers will issue a security warning when browsing to a HTTPS server with an untrusted self-signed certificate.' Below this box, under the heading 'Mode', there are three radio button options: 'HTTPS with default trusted TLS certificate (requires internet connection to be trusted)', 'HTTPS with own trusted TLS certificate', and 'HTTP (not secure, vulnerable to man-in-the-middle attacks)'. A blue 'Save' button is located at the bottom left of the form area.

Figure 11: Security Mode Selection Screen

NOTE: Cookies are used for authentication.

NOTE: To change the web server security mode after initial setup, go to [Appendix A.5](#).

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.

- 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
dVvAelhBMTmsni2ERvQVp0xj3psSv2EJyKXS1bOYNRLsq7UzpwuAdT/Wy3o6vUM5
K+Cwf9qEoQ0LuxDZTIECt67MkcHMiuFi5pk7TRicHnQF/sfOAYOulduHOy9exlk9
FmHFVDIZt/cJUaF+e74EuSph+qEr0IQo2wvmhyc7L22UXse1NoOfU2Zq0Eu1VVtu
JRryaMWiRFEWuuzMGZtKFWVC+8q2JQsVcqiRWM7naoblEhOCMH+sKHJMCxDoXGt
vtZpZUoAL51YXxWSVcyZdGiAP5e
-----END CERTIFICATE-----

Private Key

-----BEGIN RSA PRIVATE KEY-----
sHB0zZoHr4YQSDk2BbYVzzbl0LDuKtc8+JiO3ooGjoTuHnqkeAj/fkfbTAsKeAzw
gKQe+H5UQNK0bdvZfOJrm6daDK2vDmR5k+juUhej5N49uplroB97MQgYotzqfT+
THlbpq5t1SIK617k04ObKmHF5l8fck+ru545sVmpeezh0m5j5SURYAZMvbq5daCu
J4l5NlihbEvxRF4UK41ZDMCvujopCbkUWrb1a/3XXnDnM2K9xyz2wze998D6Wk46
+7aOFY9F+7j5ljmkoS3GYtwCyH5iP+mPP1K6RnuiD019wvGPb4dtN/RTnfd0eF
GYeVSk9fxxkxDOftfdWRZbM/rPin4tmO1Xf8HqONVN1x/iaMynOXG4cukoi4+VO
u0rZaUEsII2zNkfrn7fAASm5NBWg202Cy9IAYnuujs3aALl5uGBeekA62oTMxlzx
-----END RSA PRIVATE KEY-----

Private Key Passphrase

Specify if encrypted

Save

Figure 12: Security Mode Selection Screen

- 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

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

7 CONFIGURING THE BACNET ROUTER

7.1 Navigate to the BACnet Router Settings

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

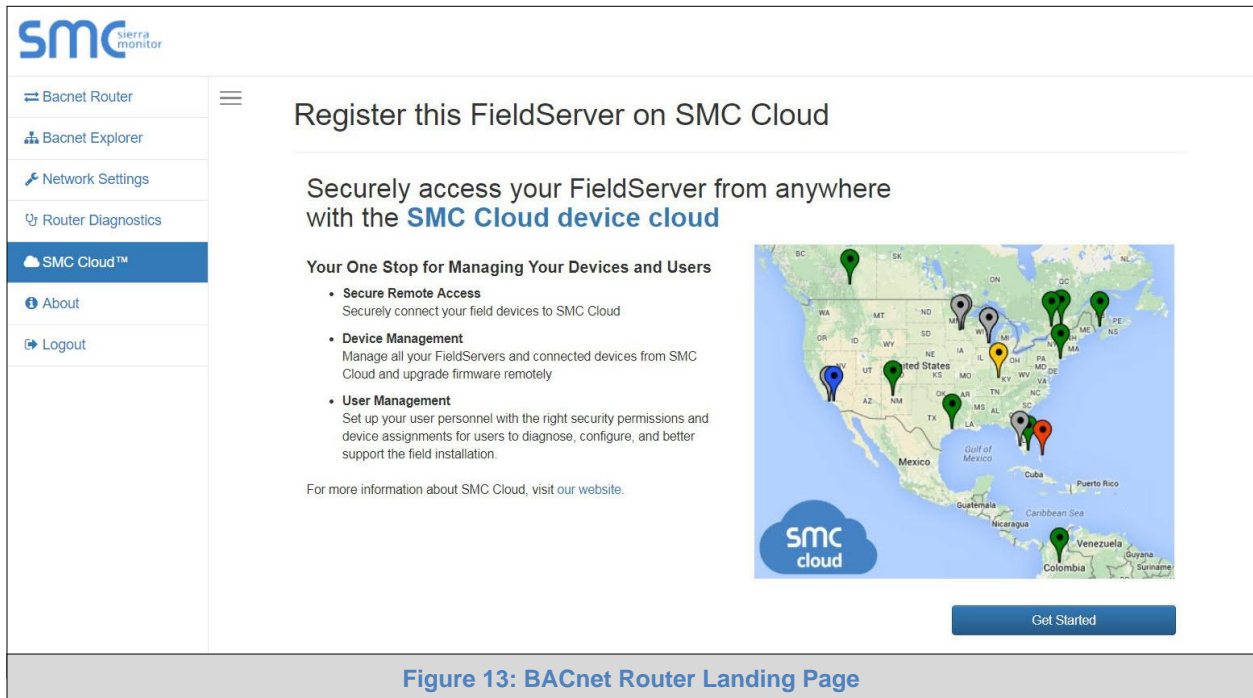


Figure 13: BACnet Router Landing Page

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

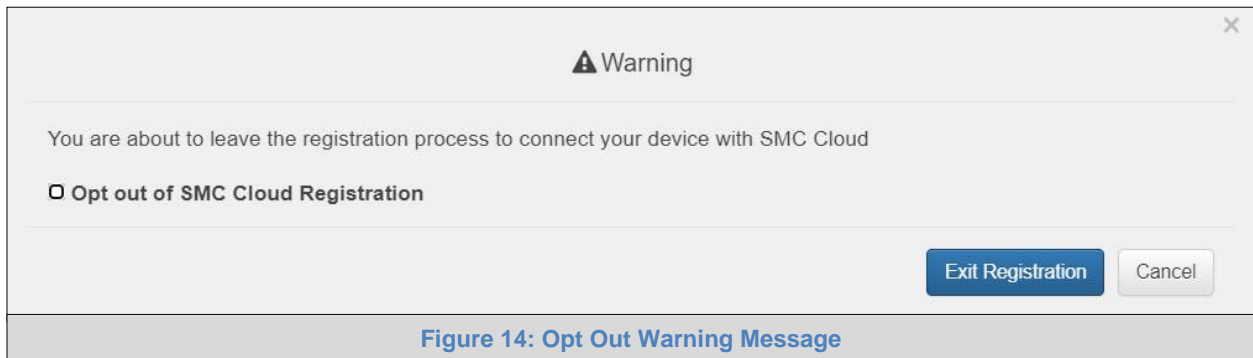


Figure 14: Opt Out Warning Message

7.2 BACnet Router Settings

The screenshot displays the BACnet Router Settings page. On the left is a navigation menu with options: BACnet Router, BACnet Explorer, Network Settings, Router Diagnostics, SMC Cloud™, About, and Logout. The main content area is divided into several panels:

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

Copyright © Sierra Monitor Corporation - Diagnostics

Figure 15: BACnet Router Settings Page

7.2.1 Button Functions

The Controls section contains four buttons arranged in a 2x2 grid:

- 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.
- Save:** Write the currently displayed settings to the device. A restart will be required to apply the updated settings.
- Restart:** Restarts the device.

- **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.

7.2.2 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.

7.2.3 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.

7.2.4 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.

7.2.5 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)

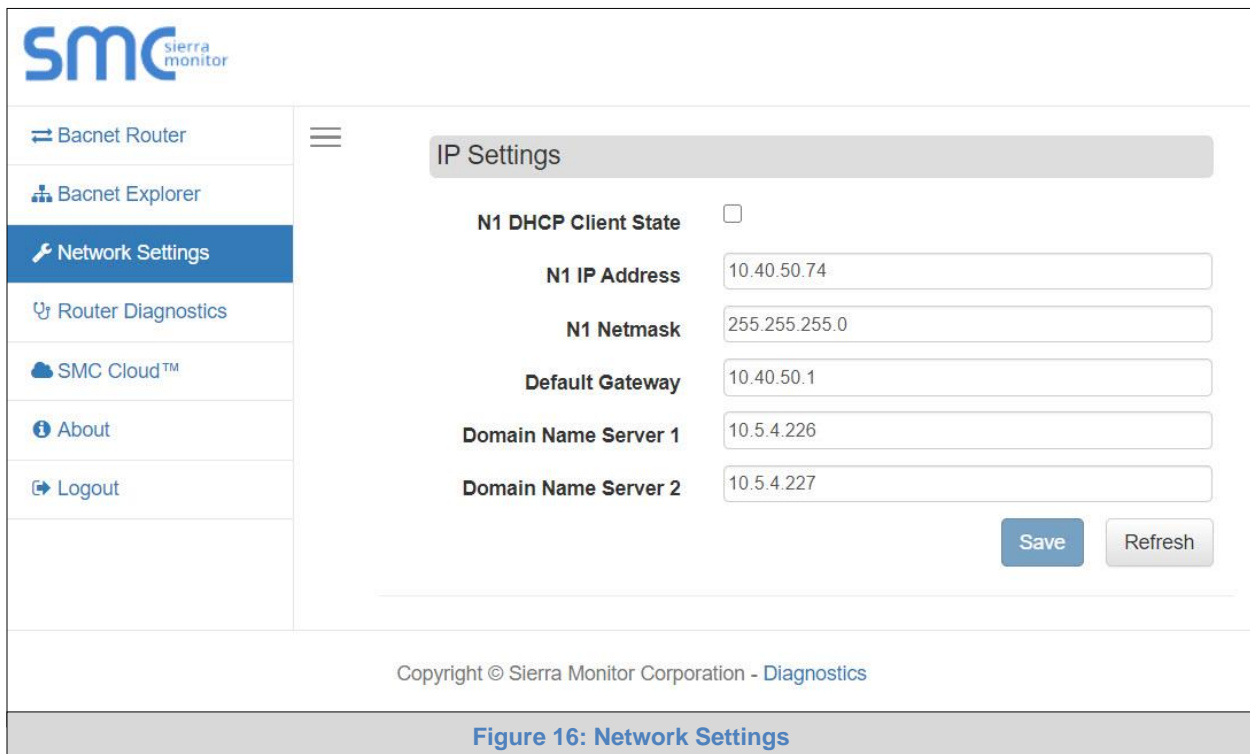
BACnet Explorer

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.

7.3 Network Settings

The IP Settings for the BACnet Router are used by BACnet/IP. The IP Settings can be edited in the Network Settings section as shown.



The screenshot shows the SMC Network Settings web interface. On the left is a navigation menu with the following items: BACnet Router, BACnet Explorer, Network Settings (highlighted), Router Diagnostics, SMC Cloud™, About, and Logout. The main content area is titled 'IP Settings' and contains the following configuration options:

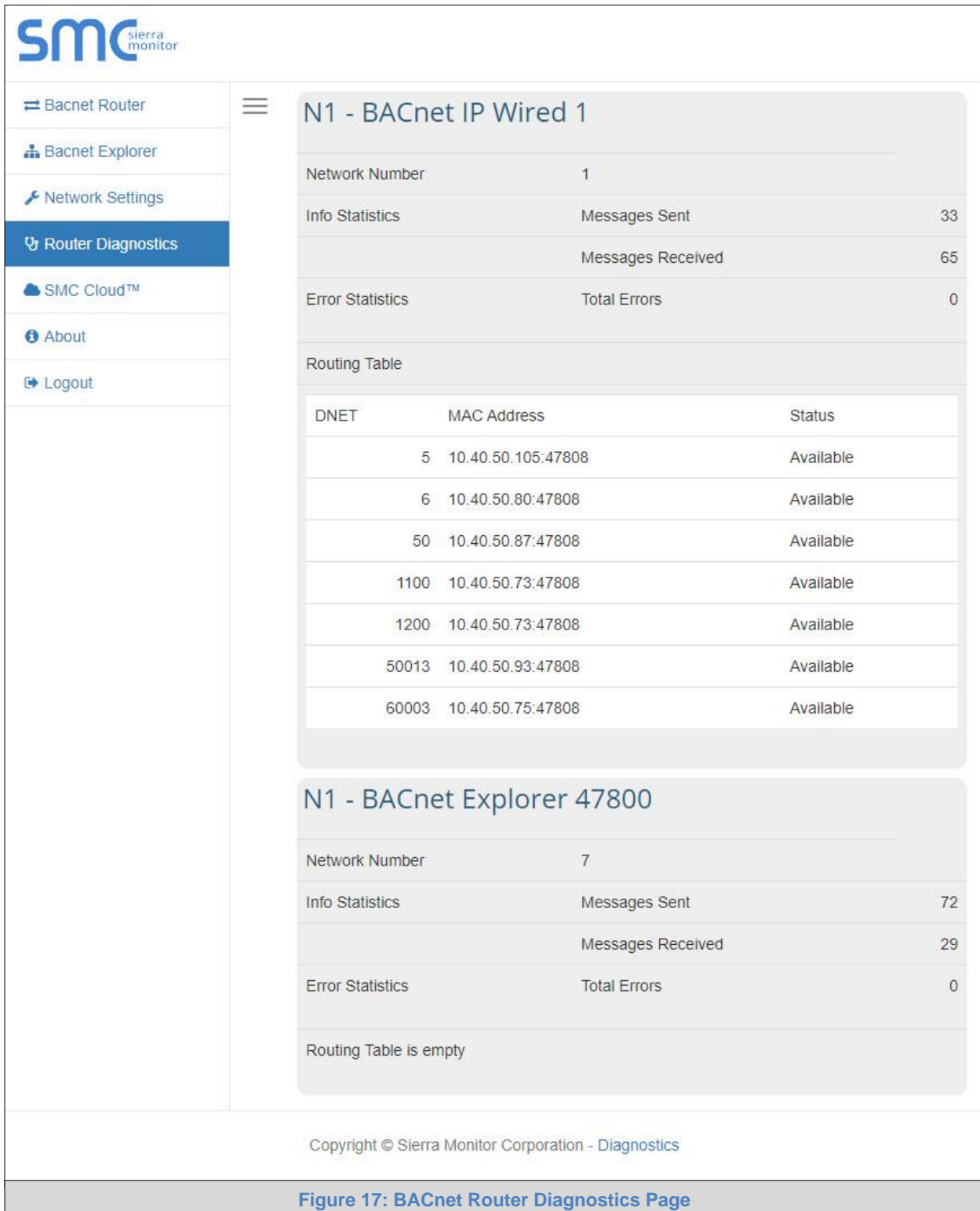
- N1 DHCP Client State**: A checkbox that is currently unchecked.
- N1 IP Address**: A text input field containing the value 10.40.50.74.
- N1 Netmask**: A text input field containing the value 255.255.255.0.
- Default Gateway**: A text input field containing the value 10.40.50.1.
- Domain Name Server 1**: A text input field containing the value 10.5.4.226.
- Domain Name Server 2**: A text input field containing the value 10.5.4.227.

At the bottom right of the settings area are two buttons: 'Save' and 'Refresh'. Below the settings area, there is a copyright notice: 'Copyright © Sierra Monitor Corporation - Diagnostics'.

Figure 16: Network Settings

7.4 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 SMC Router Diagnostics interface. On the left is a navigation menu with options: BACnet Router, BACnet Explorer, Network Settings, Router Diagnostics (selected), SMC Cloud™, About, and Logout. The main content area is divided into two sections:

N1 - BACnet IP Wired 1

Network Number	1	
Info Statistics	Messages Sent	33
	Messages Received	65
Error Statistics	Total Errors	0

Routing Table

DNET	MAC Address	Status
5	10.40.50.105:47808	Available
6	10.40.50.80:47808	Available
50	10.40.50.87:47808	Available
1100	10.40.50.73:47808	Available
1200	10.40.50.73:47808	Available
50013	10.40.50.93:47808	Available
60003	10.40.50.75:47808	Available

N1 - BACnet Explorer 47800

Network Number	7	
Info Statistics	Messages Sent	72
	Messages Received	29
Error Statistics	Total Errors	0

Routing Table is empty

Copyright © Sierra Monitor Corporation - Diagnostics

Figure 17: BACnet Router Diagnostics Page

8 BACNET EXPLORER

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

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

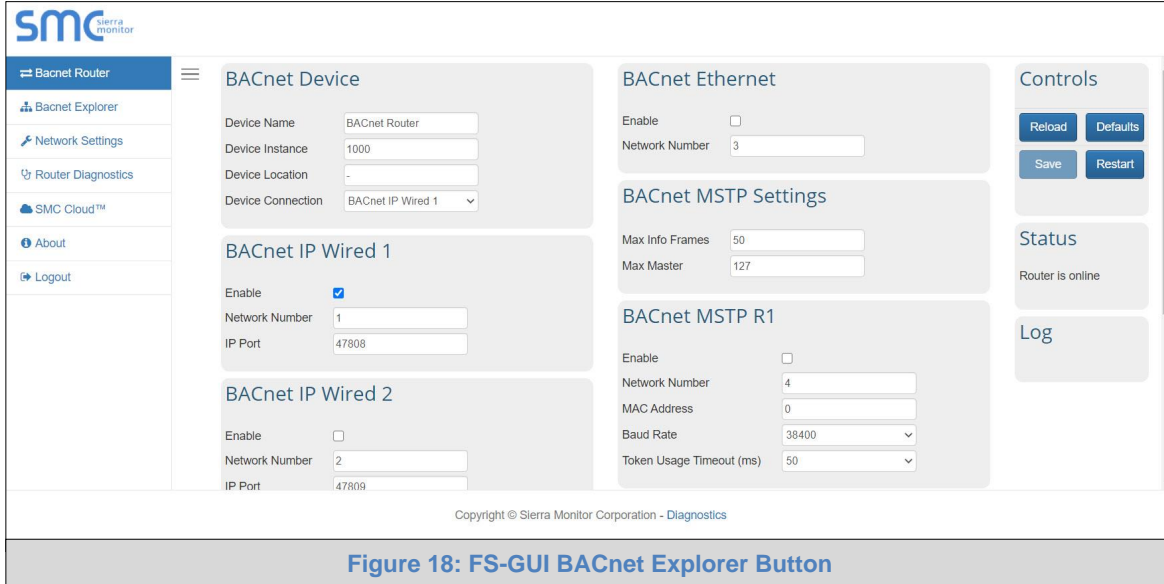


Figure 18: FS-GUI BACnet Explorer Button

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.

8.1 Discover Device List

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

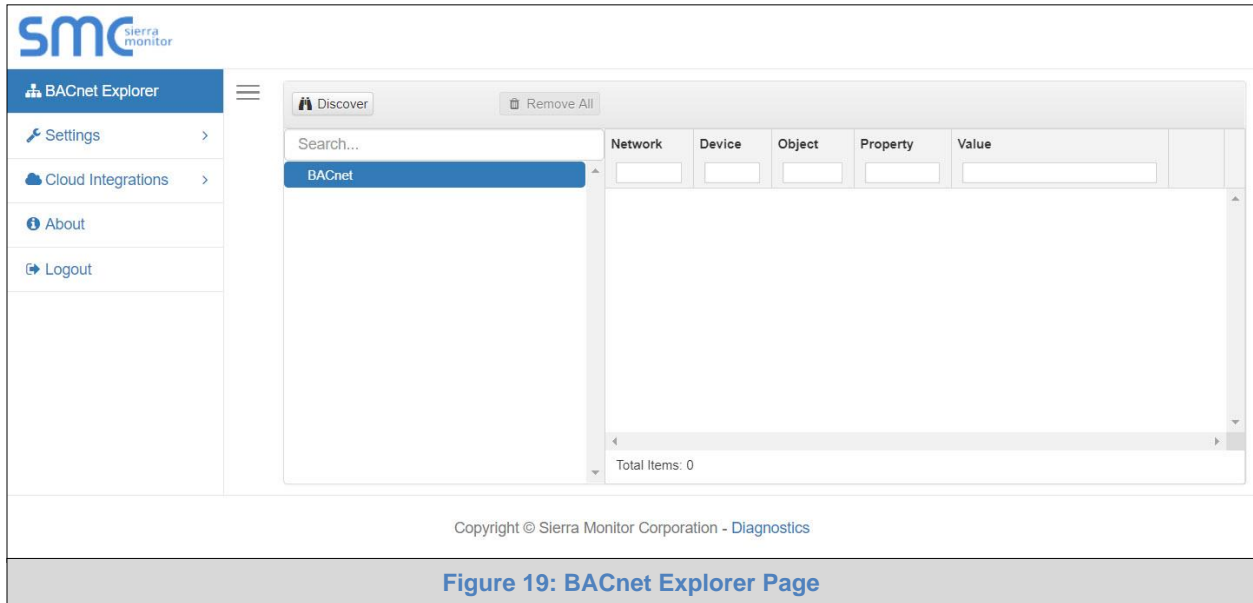



Figure 19: BACnet Explorer Page

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

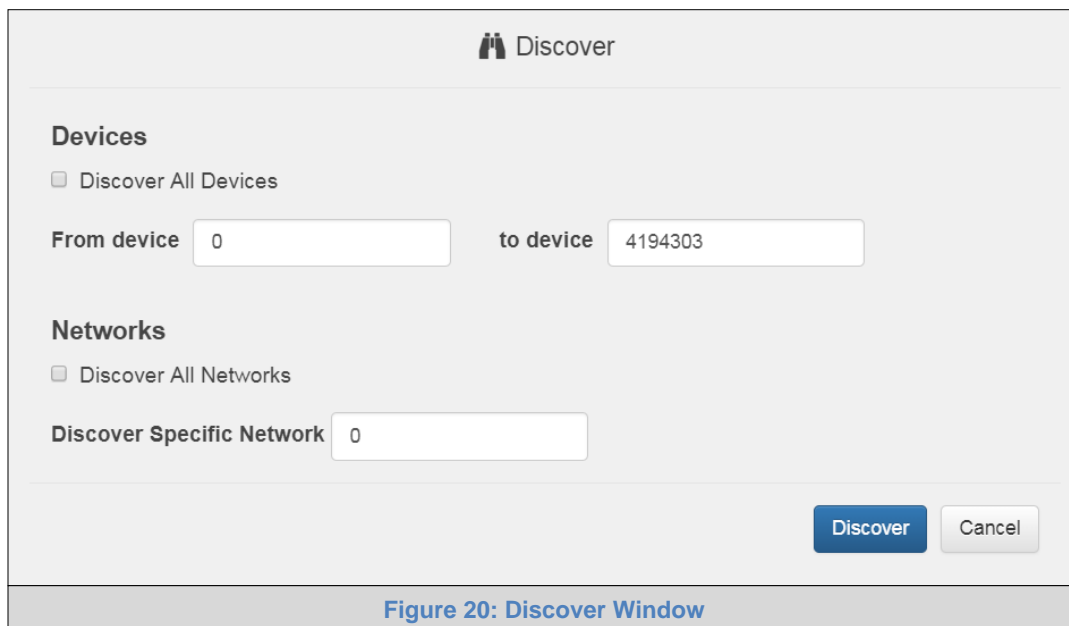


Figure 20: Discover Window

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.

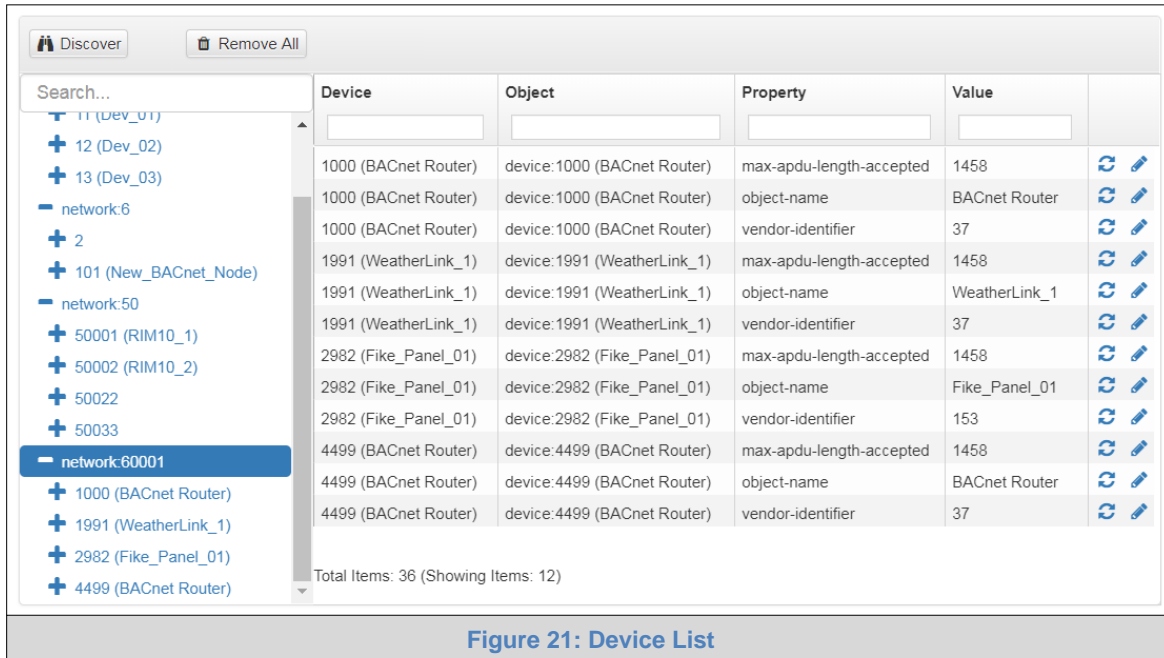


Figure 21: Device List

8.2 View Device Details and Explore Points/Parameters

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

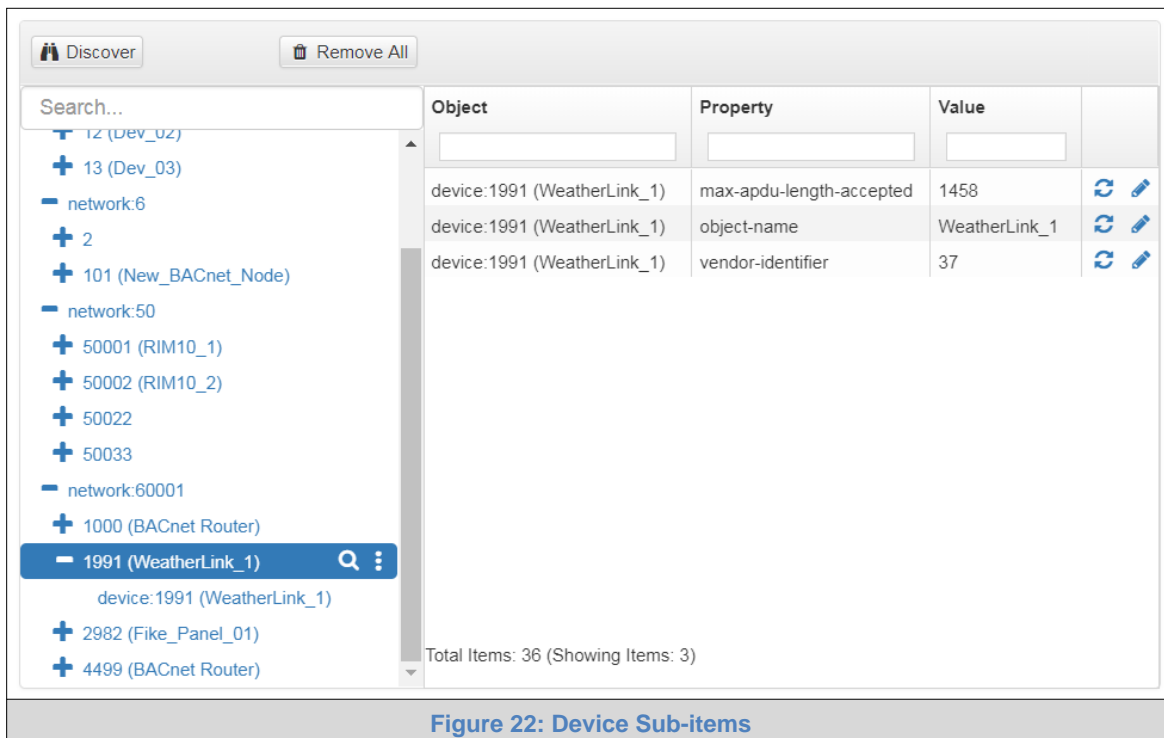


Figure 22: Device Sub-items

- To view the full details of a device, go back to highlighting the device directly (in [Figure 23](#) “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.

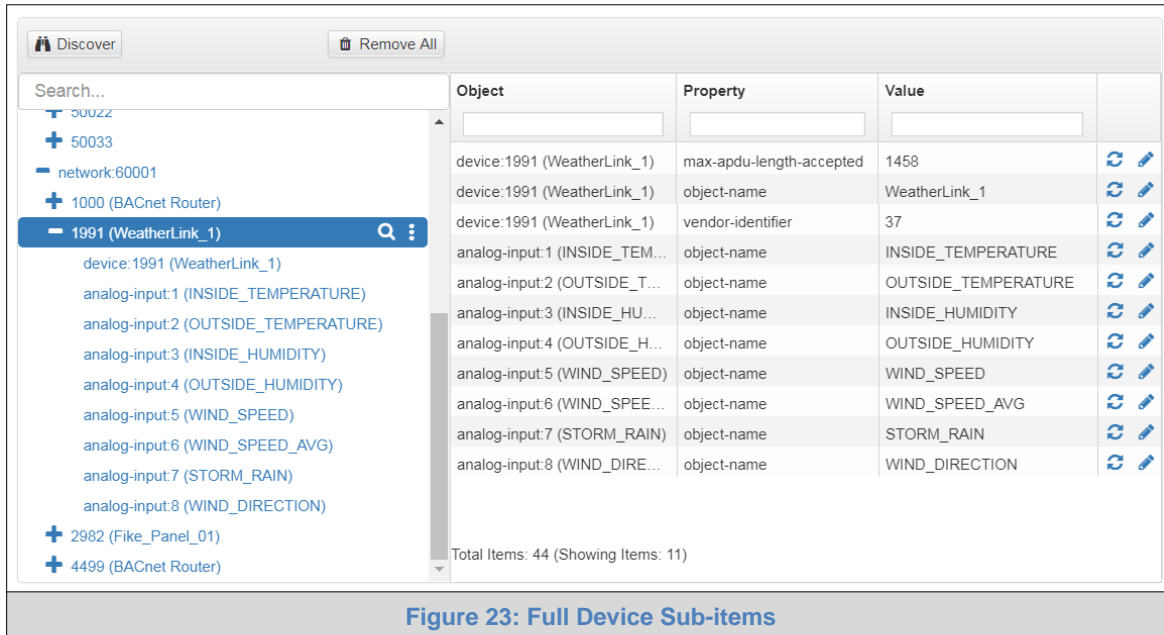


Figure 23: Full Device Sub-items

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

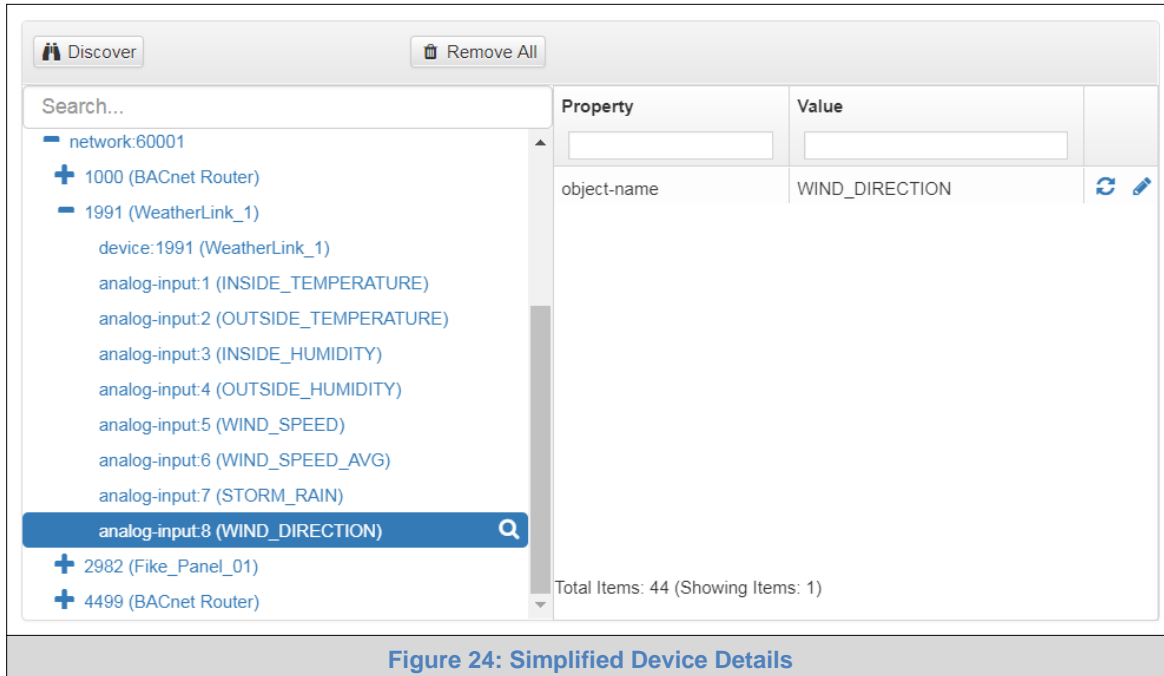
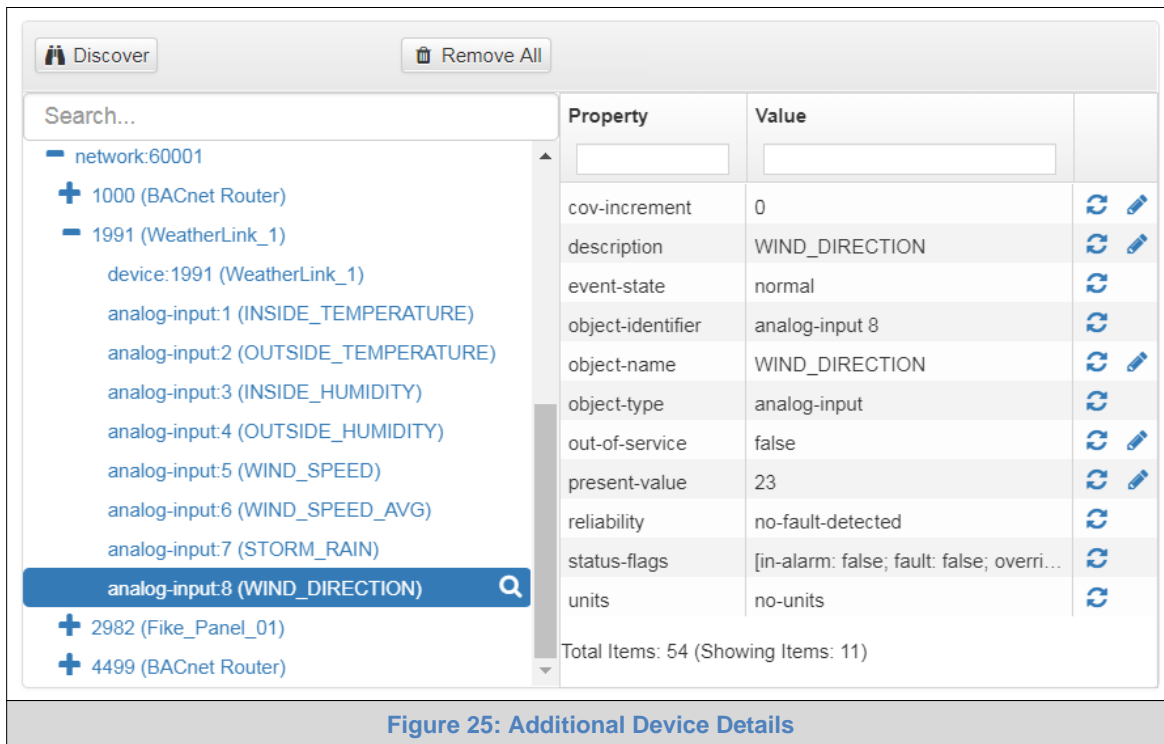



Figure 24: Simplified Device Details

- Then click on the Explore button 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 the value.

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

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

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

8.2.1 Edit the Present Value Field

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

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

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

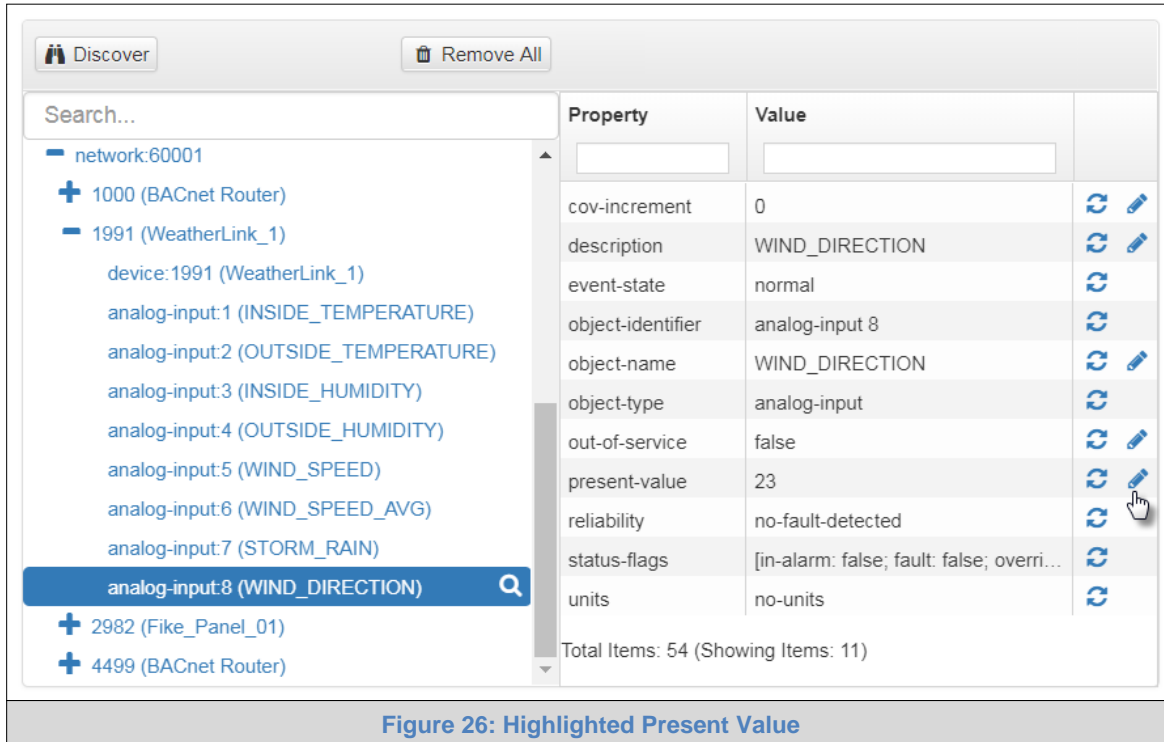



Figure 26: Highlighted Present Value

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

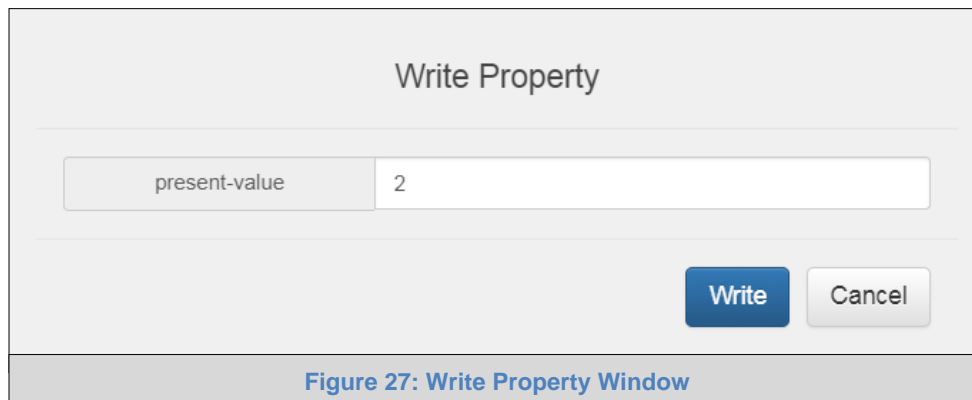
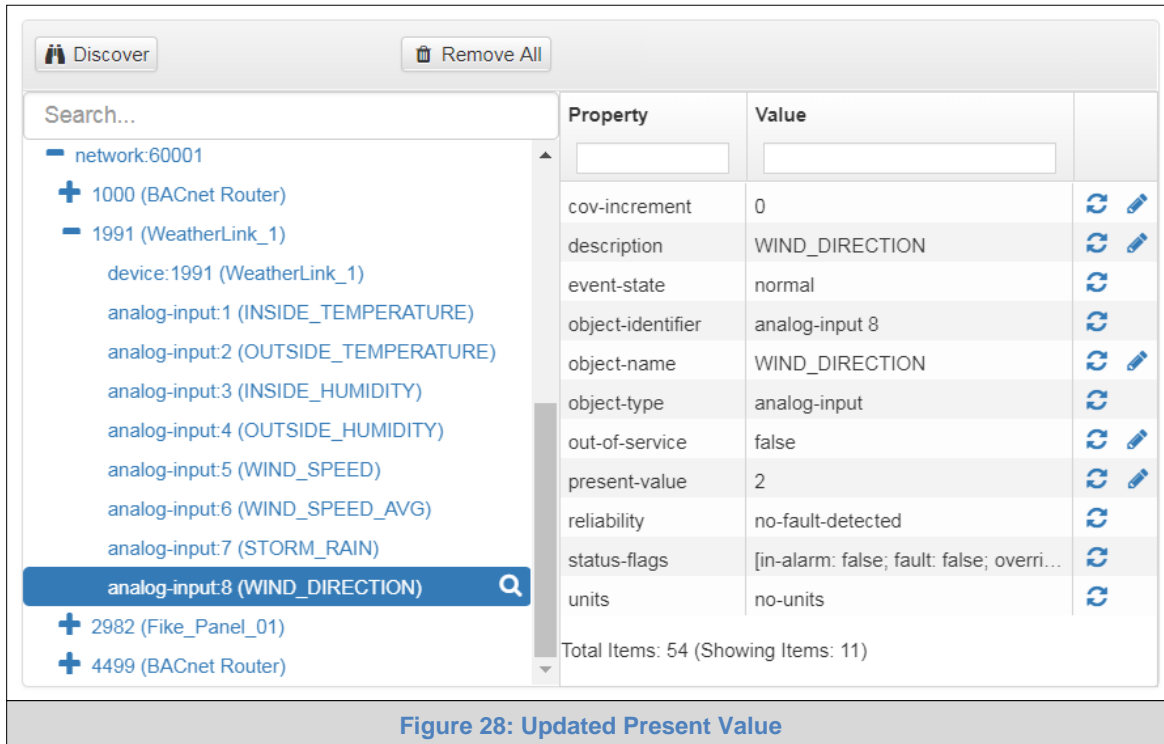


Figure 27: Write Property Window

- Enter the appropriate change and click write.

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



9 SMC CLOUD SETUP

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

9.1 Create a New SMC Cloud Account

The first step to connecting to the SMC Cloud is to create an account.

- Click on the Cloud Integrations tab, then click the SMC Cloud™ tab.

The screenshot displays the SMC Cloud configuration interface for a BACnet Router. The left sidebar lists navigation options. The main content area is divided into several sections for configuring different BACnet protocols. The 'BACnet Device' section includes fields for Device Name, Instance, Location, and Connection. 'BACnet Ethernet' has Enable, Network Number, and MAC Address settings. 'BACnet IP Wired 1' and '2' have Enable, Network Number, and IP Port settings. 'BACnet MSTP Settings' includes Max Info Frames and Max Master. 'BACnet MSTP R1' has Enable, Network Number, MAC Address, Baud Rate, and Token Usage Timeout settings. The right sidebar contains 'Controls' with Reload, Defaults, Save, and Restart buttons, and a 'Status' section indicating the router is online with a Log button.

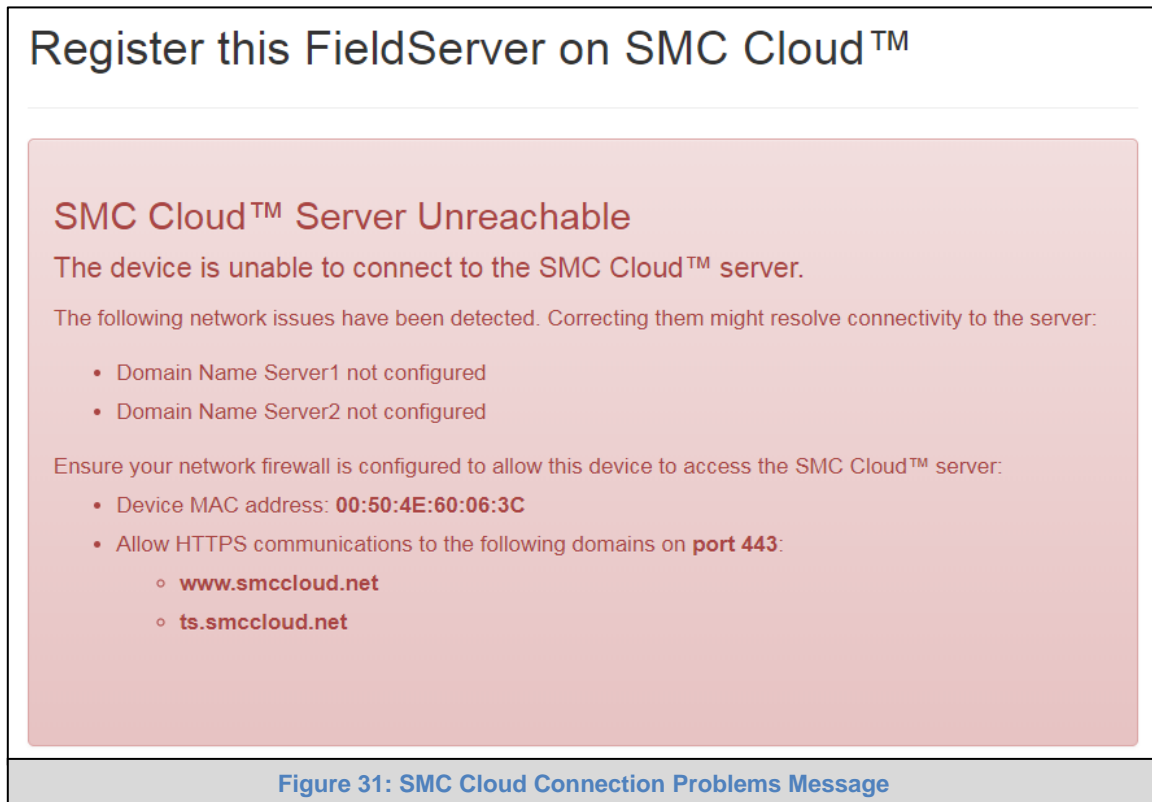
Figure 29: BACnet Router Landing Page – SMC Cloud Tab

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

The registration page provides information on how to securely access the FieldServer from anywhere using the SMC Cloud device cloud. It highlights the benefits of having a one-stop solution for managing devices and users. The page includes a list of features: Secure Remote Access (securely connecting field devices to SMC Cloud), Device Management (managing FieldServers and devices remotely), and User Management (setting up user personnel with security permissions). A map of the United States and surrounding regions shows various locations marked with pins, indicating the global reach of the SMC Cloud. A 'Get Started' button is located at the bottom right.

Figure 30: Registration Information Page

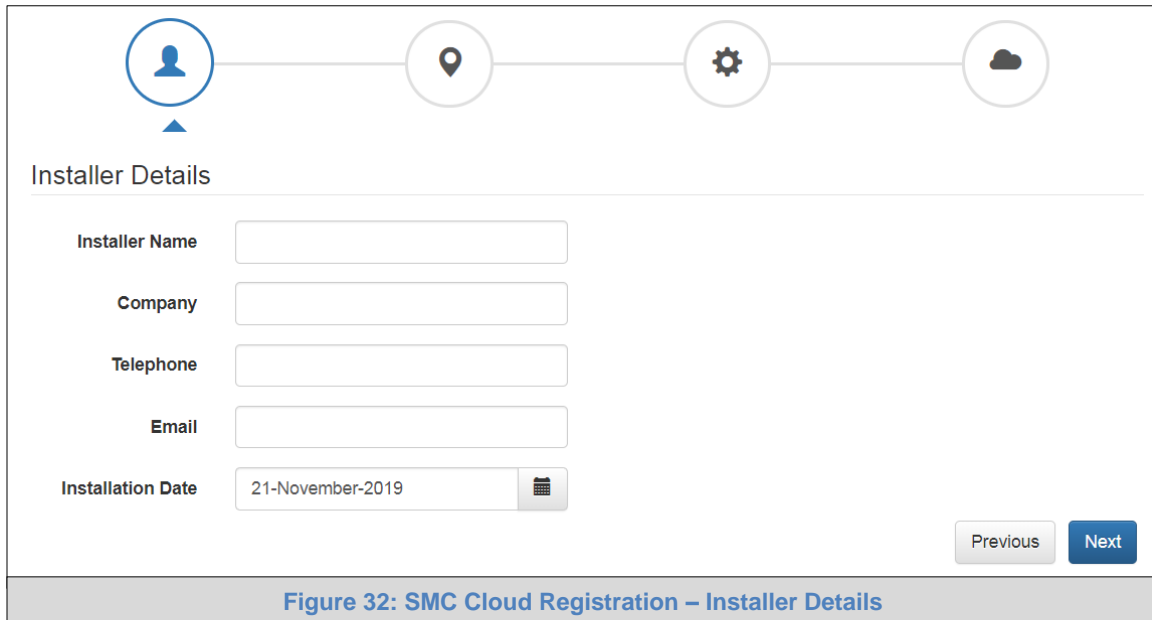
- If a warning message appears instead of the splash page, follow the suggestion that appears on screen.
- If the BACnet Router cannot reach the SMC Cloud server, the following message will appear.




- 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



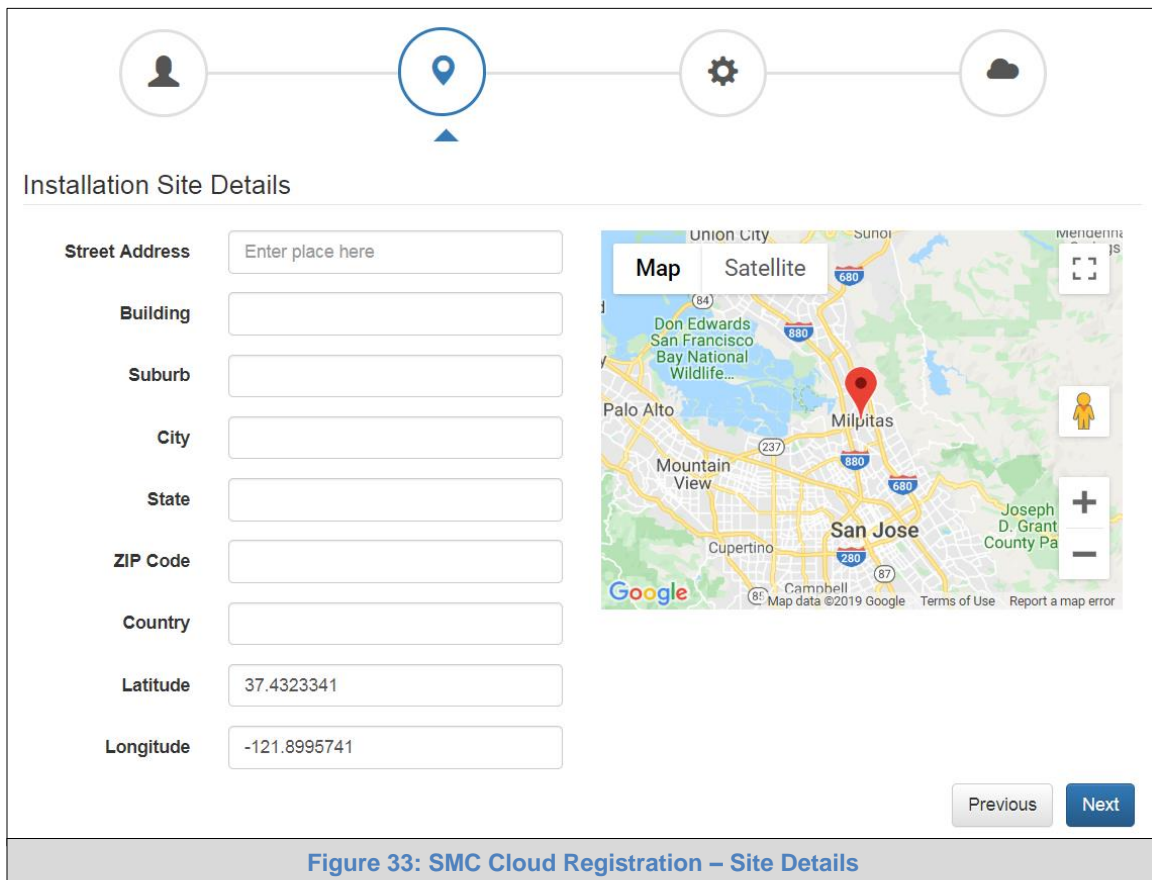
The screenshot shows the 'Installer Details' step in the SMC Cloud Registration process. At the top, there is a progress bar with four icons: a person (selected), a location pin, a gear, and a cloud. Below the progress bar, the title 'Installer Details' is followed by a form with the following fields:

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

At the bottom right of the form are two buttons: 'Previous' and 'Next'.

Figure 32: SMC Cloud Registration – Installer Details

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



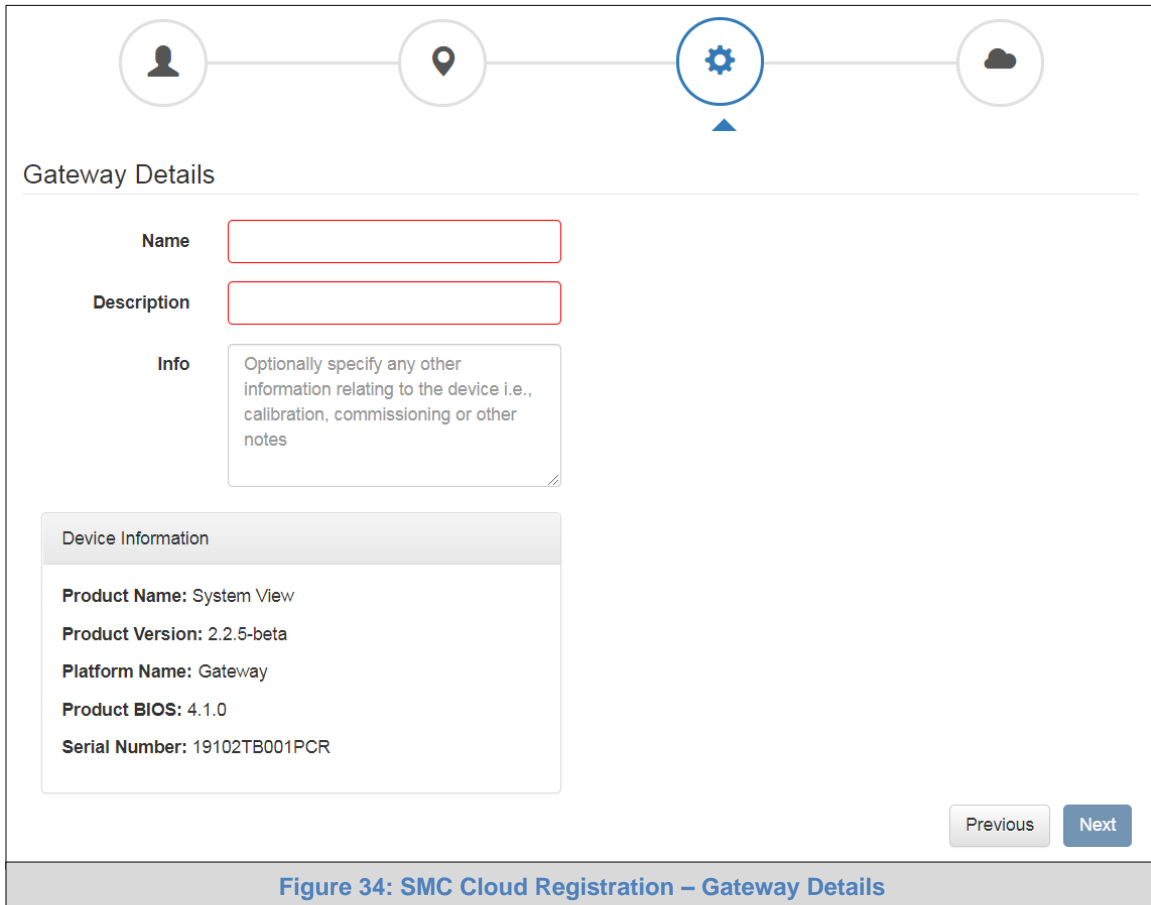
The screenshot shows the 'Installation Site Details' step in the SMC Cloud Registration process. At the top, there is a progress bar with four icons: a person, a location pin (selected), a gear, and a cloud. Below the progress bar, the title 'Installation Site Details' is followed by a form with the following fields:

- Street Address:
- Building:
- Suburb:
- City:
- State:
- ZIP Code:
- Country:
- Latitude:
- Longitude:

To the right of the form is a Google Map showing the San Jose area with a red location pin. Below the map are zoom controls and a person icon. At the bottom right of the form are two buttons: 'Previous' and 'Next'.

Figure 33: SMC Cloud Registration – Site Details

- Enter Name and Description (required) then click Next



Gateway Details

Name

Description

Info

Device Information

Product Name: System View

Product Version: 2.2.5-beta

Platform Name: Gateway

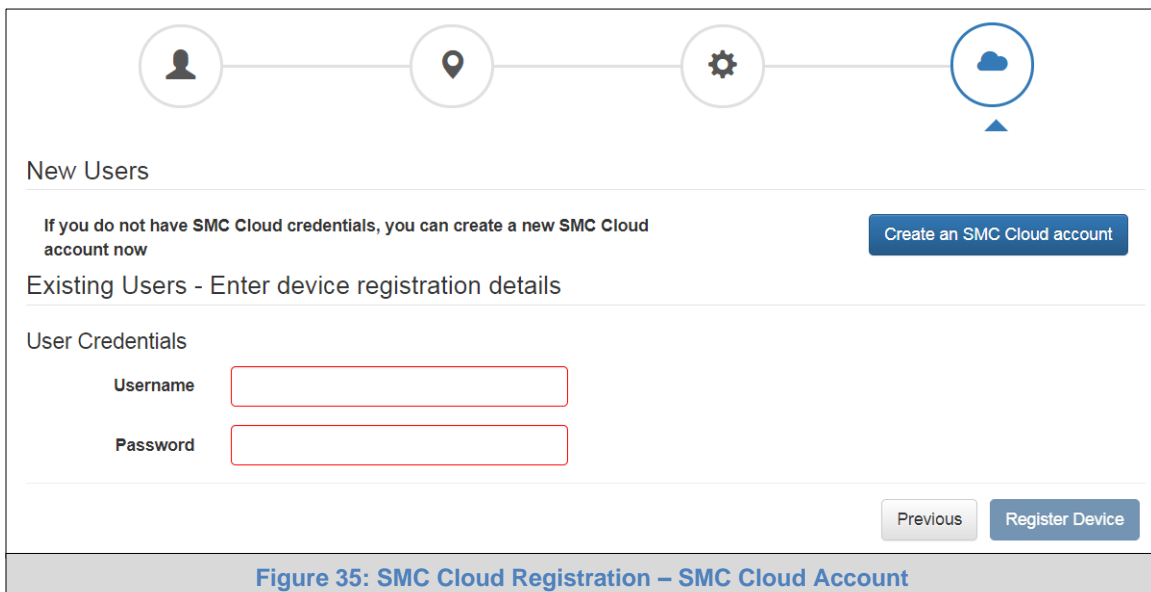
Product BIOS: 4.1.0

Serial Number: 19102TB001PCR

[Previous](#) [Next](#)

Figure 34: SMC Cloud Registration – Gateway Details

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



New Users

If you do not have **SMC Cloud** credentials, you can create a new **SMC Cloud** account now [Create an SMC Cloud account](#)

Existing Users - Enter device registration details

User Credentials

Username

Password

[Previous](#) [Register Device](#)

Figure 35: SMC Cloud Registration – SMC Cloud Account

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

Device Registered

Gateway Details

Name: FieldServer

Description: Gateway

Device Info:

MAC Address: 00:50:4E:60:06:3C

Tunnel Server URL: tunnel.fieldpop.io

Device ID: daffodilsentry_ylb4Xr5bQ

Product Name: CN1853-System View

Product Version: 2.2.5-beta

Installer Details

Installer Name: User

Company: Sierra Monitor Corp

Telephone:

Email:

Installation Date: Nov 21, 2019

Site Installation Details

Street Address: 1991 Tarob Court

Building Info: SMC Build #1

City: Milpitas

Suburb: Milpitas

State: CA

Country: United States

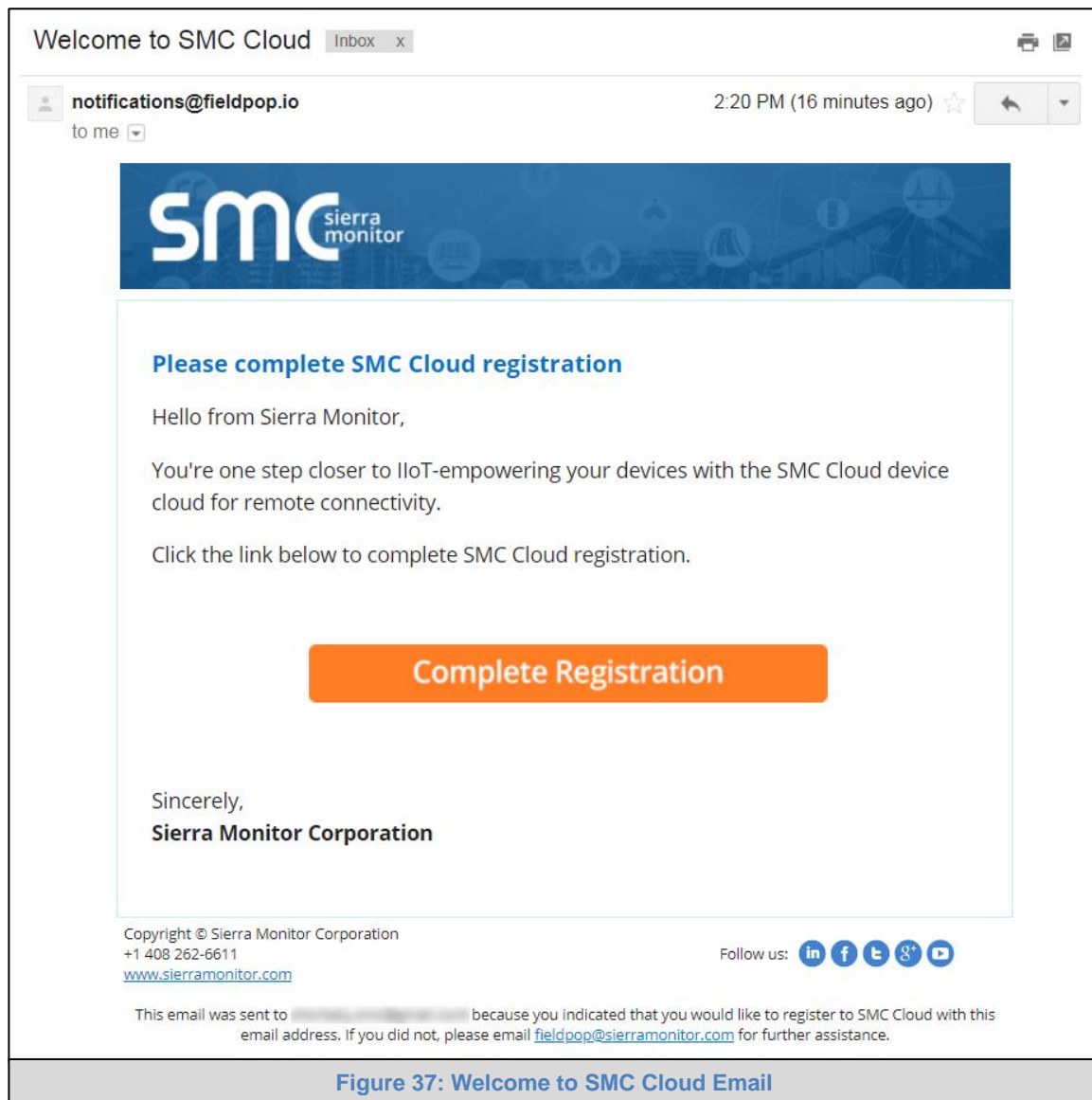
ZIP Code: 95035

Update Device Details

Figure 36: Device Registered for SMC Cloud

NOTE: Update these details at any time by going to the SMC Cloud™ tab and clicking the Update Device Details button.

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



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

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

Complete Your Registration

Email Address
user@gmail.com

First Name *

Last Name *

Phone Number *

(201) 555-5555

New Password *

password

Confirm Password *

password

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

* Mandatory Fields

Save Cancel

Figure 38: Setting User Details

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

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

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

9.2 Login to SMC Cloud

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

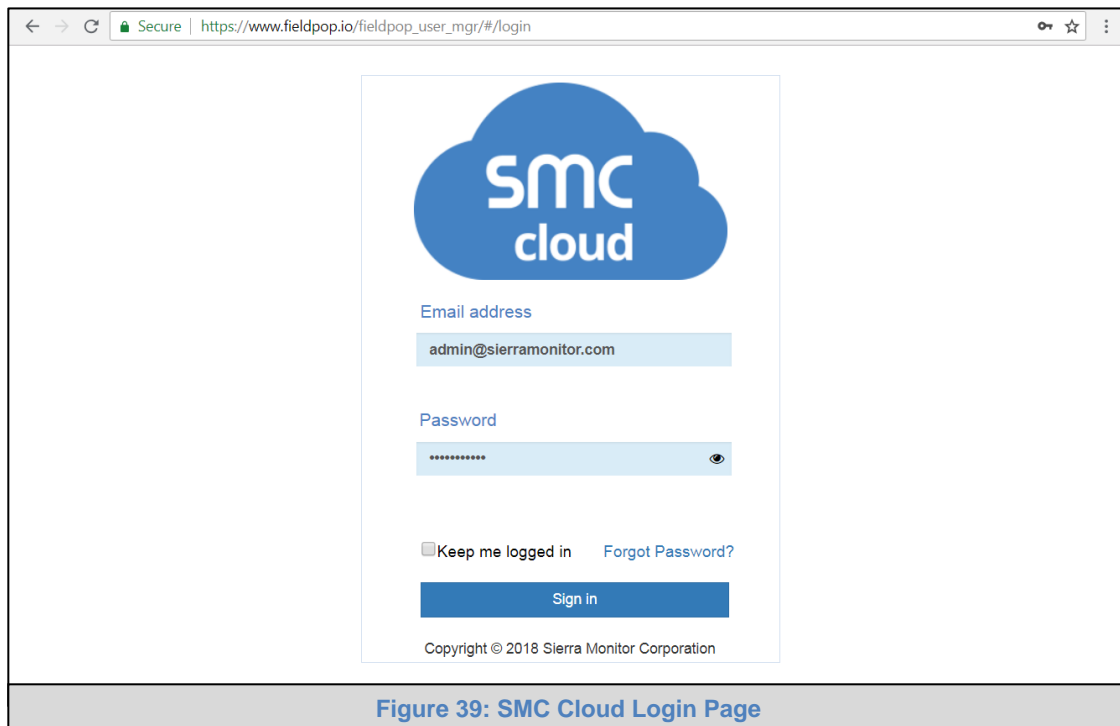


Figure 39: SMC Cloud Login Page

NOTE: If the login password is lost, see the [SMC Cloud Start-up Guide](#) for recovery instructions.

On first login, the Privacy Policy window will appear. Read the Terms of Service, click the checkbox to accept the terms and then click the Continue button to access SMC Cloud.

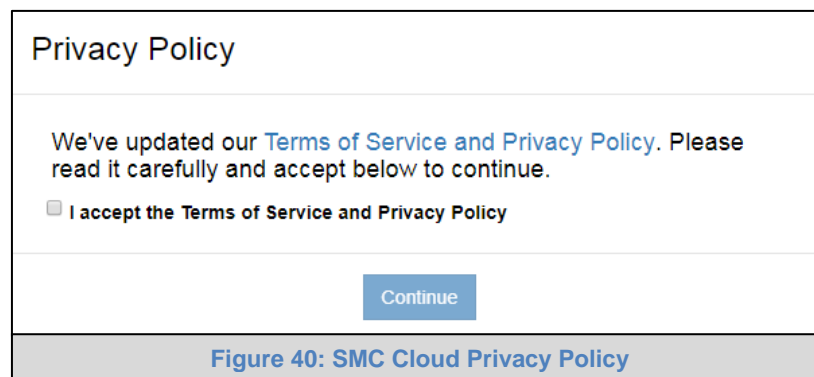


Figure 40: SMC Cloud Privacy Policy

NOTE: For additional SMC Cloud instructions see the [SMC Cloud Start-up Guide](#).

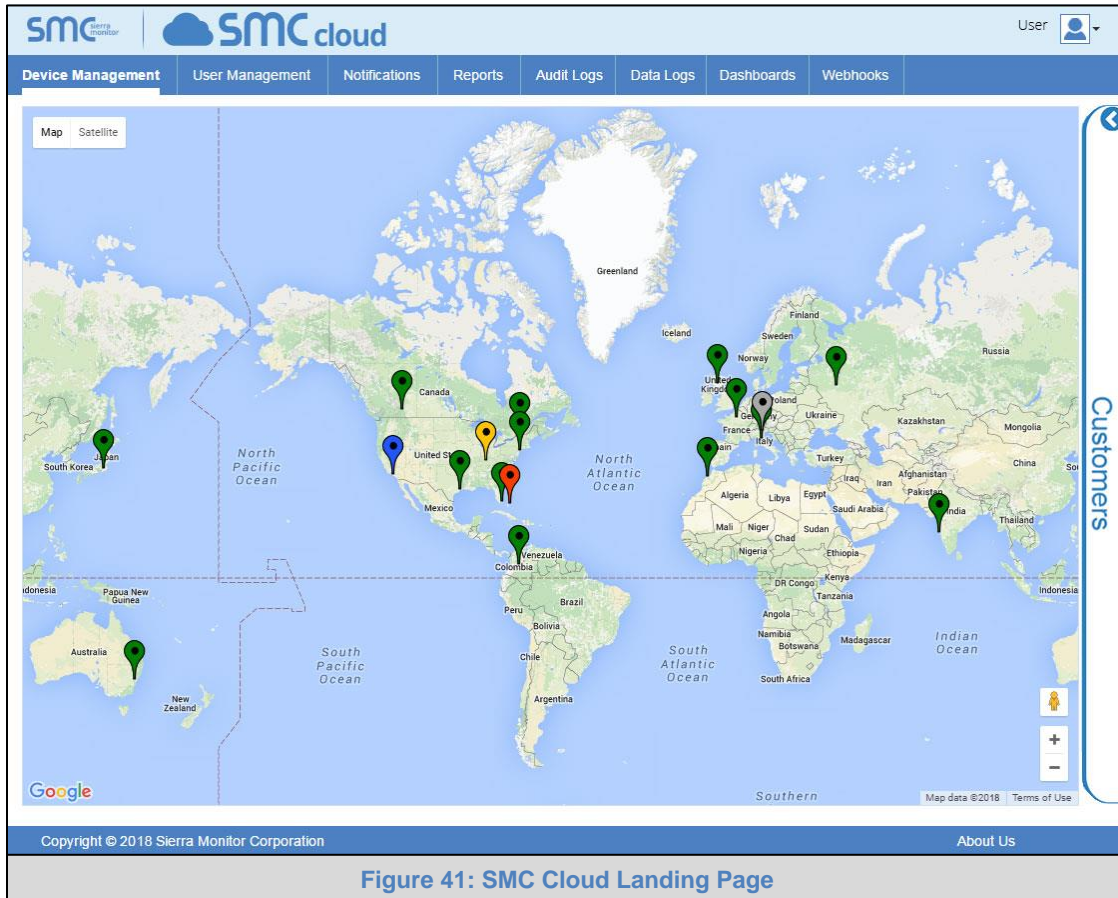


Figure 41: SMC Cloud Landing Page

APPENDIX A. USEFUL FEATURES

Appendix A.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.

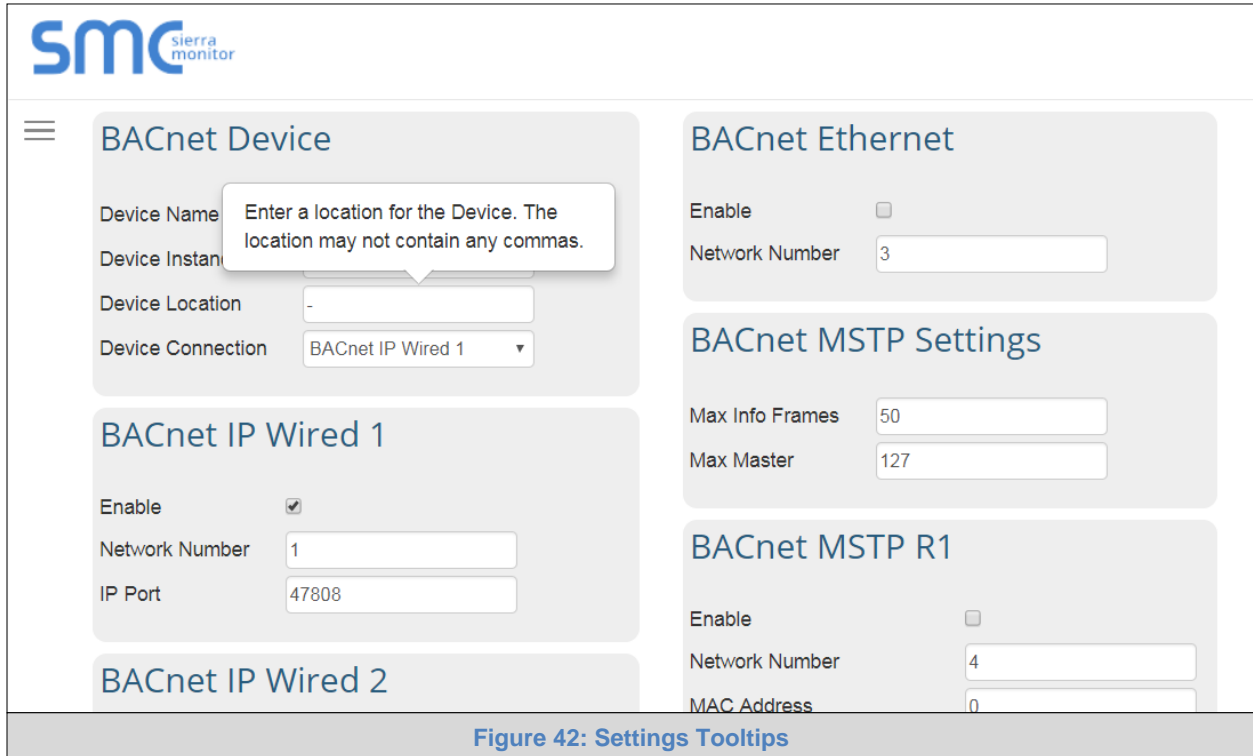

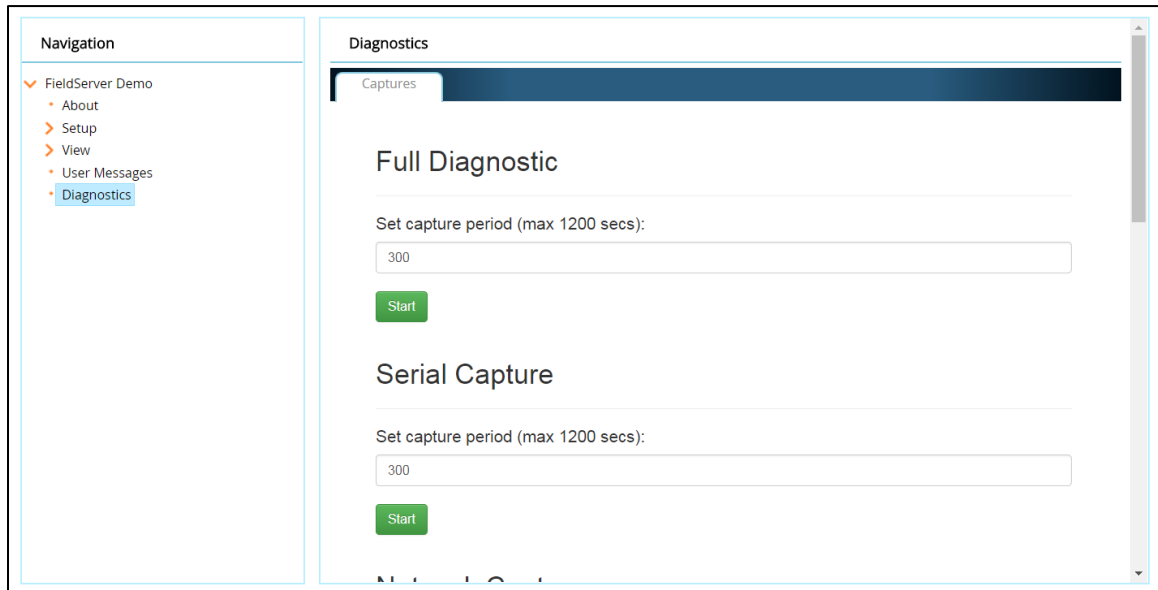


Figure 42: Settings Tooltips

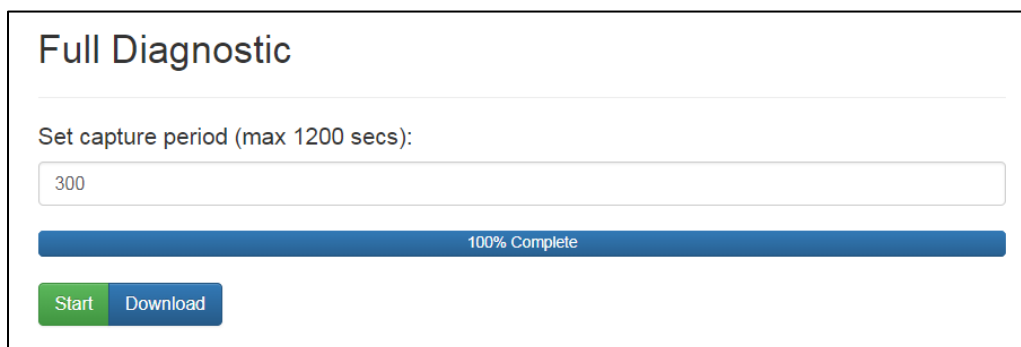
Appendix A.2. Taking a FieldServer Diagnostic Capture

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).

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

Appendix A.3. Factory Reset Instructions

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

Appendix A.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.

Appendix A.5. 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.

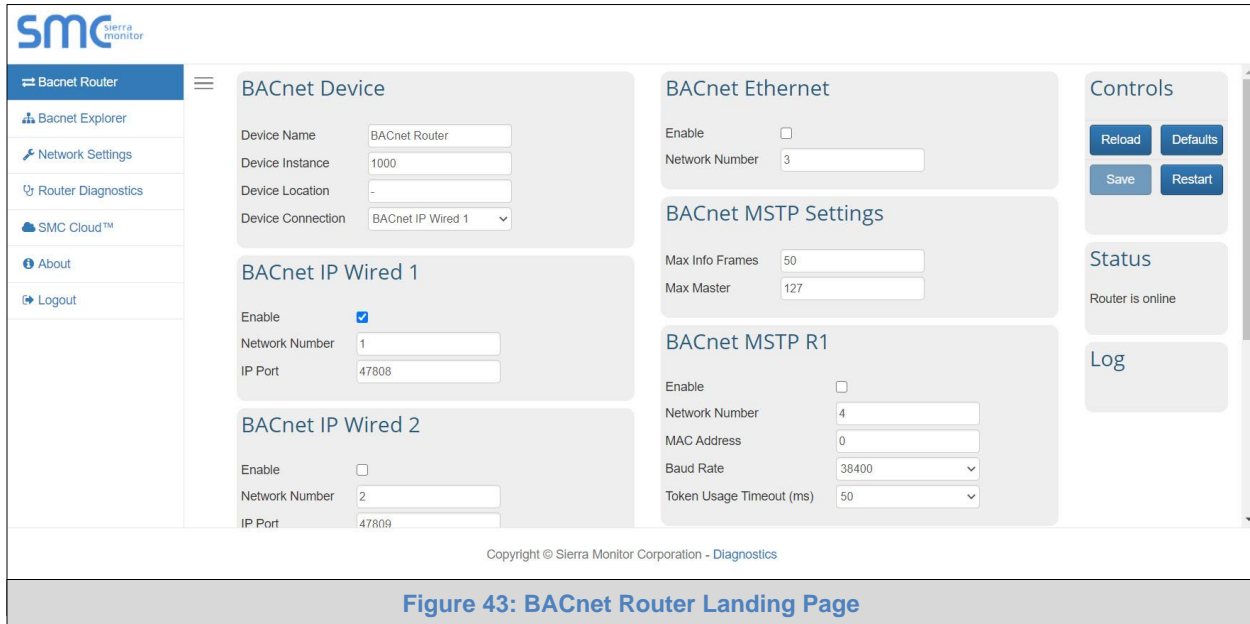


Figure 43: BACnet Router Landing Page

- Click Setup in the Navigation panel.

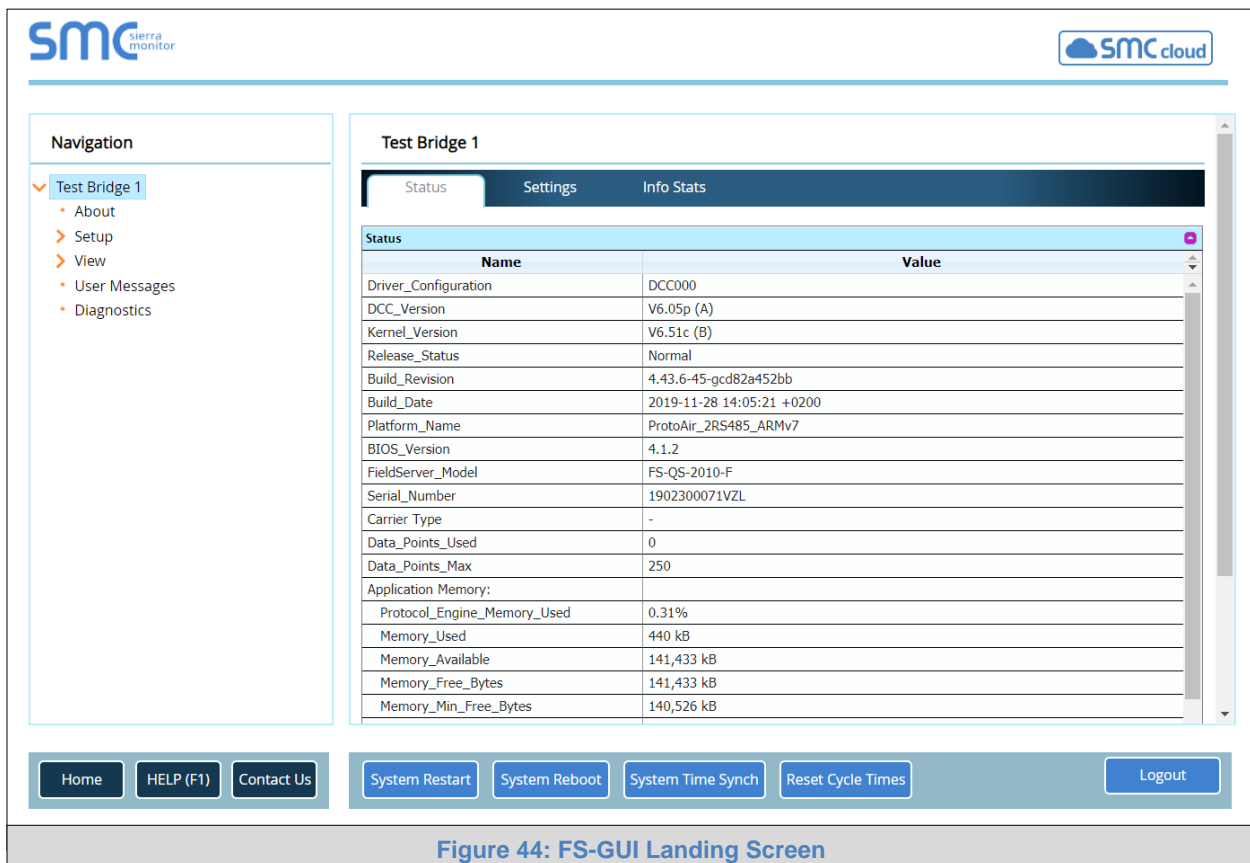


Figure 44: FS-GUI Landing Screen

Appendix A.5.1. Change Security Mode

- Click Security in the Navigation panel.

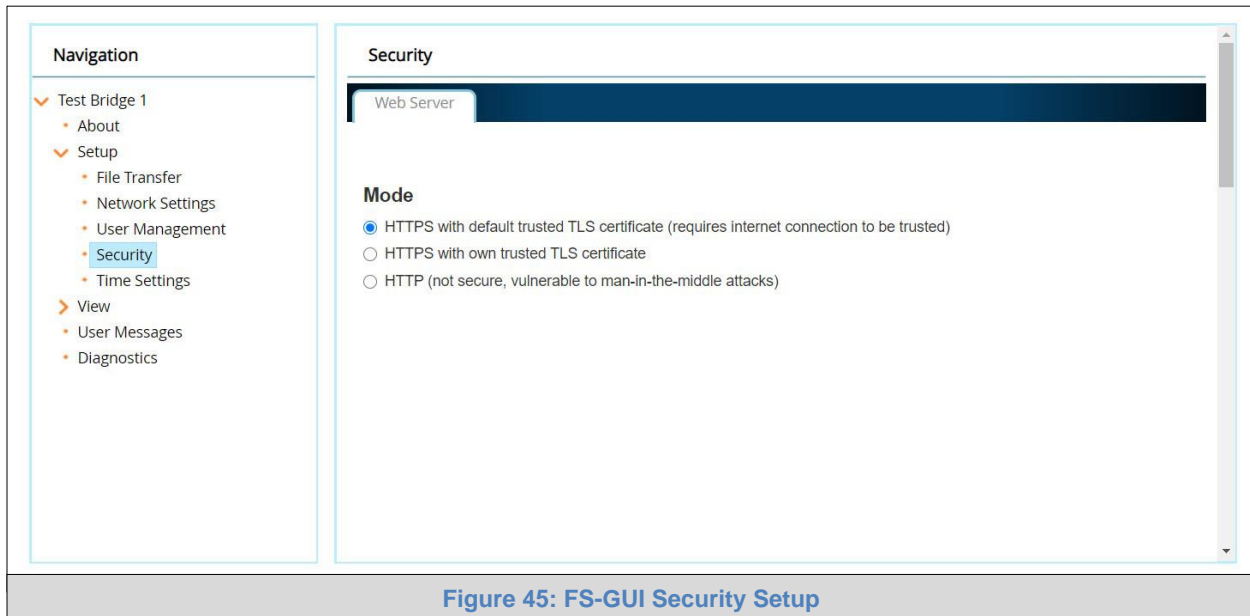


Figure 45: FS-GUI Security Setup

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

Appendix A.5.2. 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.

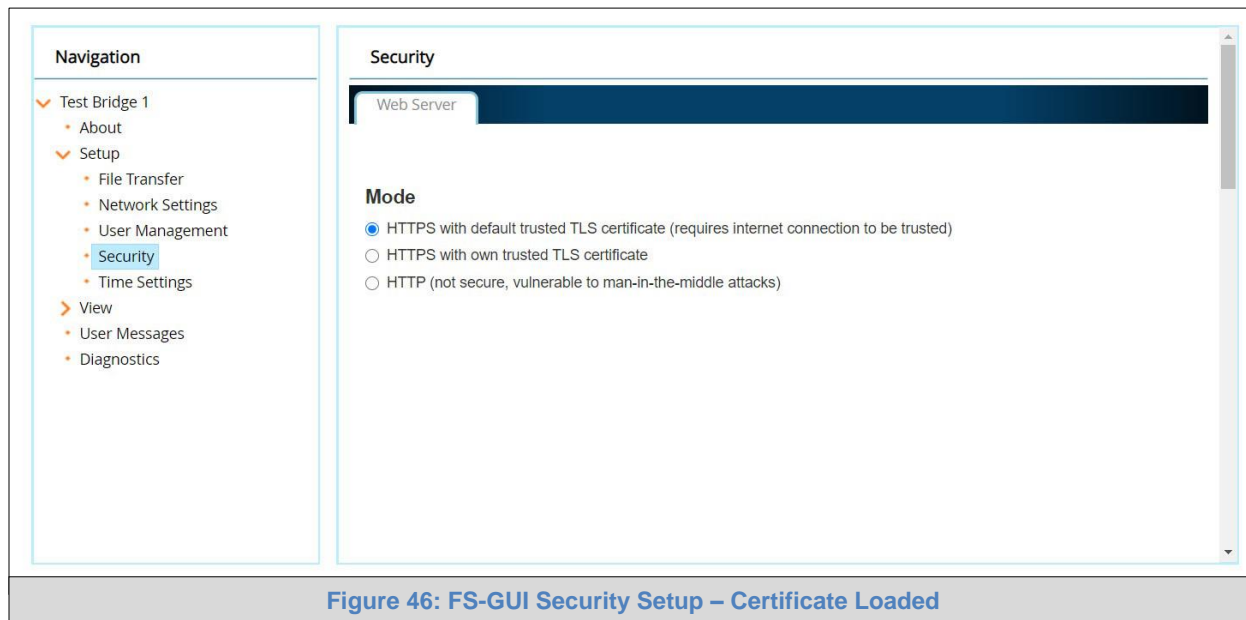


Figure 46: FS-GUI Security Setup – Certificate Loaded

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

Appendix A.6. 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.

Appendix A.6.1. User Management

- Check that the Users tab is selected.

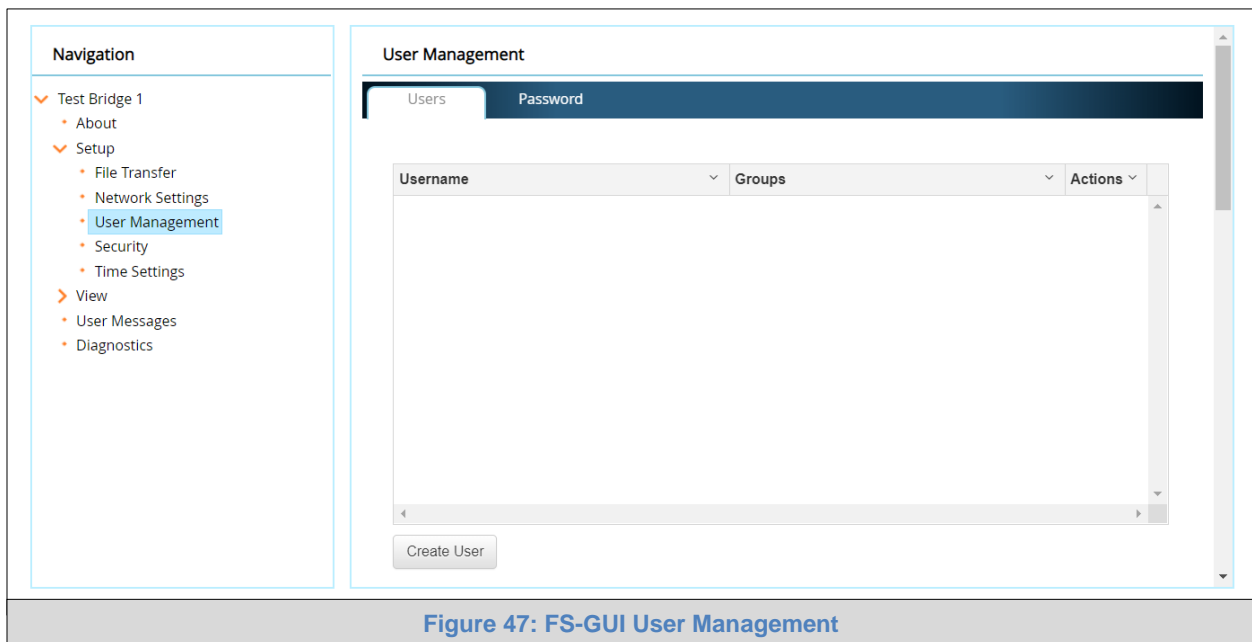


Figure 47: FS-GUI User Management

User Types:

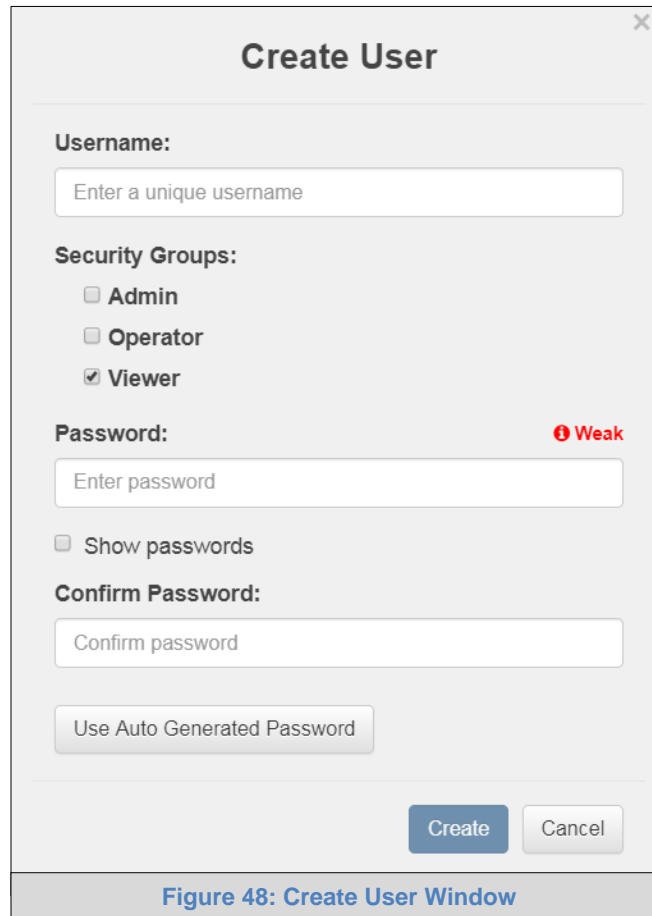
Admin – Can modify any settings on the FieldServer.

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

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

Appendix A.6.1.1. Create Users

- Click the Create User button.

A screenshot of the 'Create User' window. The window has a title bar with a close button (X). The main content area is light gray. It contains the following fields and controls:

- Username:** A text input field with the placeholder text 'Enter a unique username'.
- Security Groups:** A section with three checkboxes: 'Admin' (unchecked), 'Operator' (unchecked), and 'Viewer' (checked).
- Password:** A text input field with the placeholder text 'Enter password'. To the right of the field is a red indicator 'Weak'.
- Show passwords:** A checkbox that is currently unchecked.
- Confirm Password:** A text input field with the placeholder text 'Confirm password'.
- Use Auto Generated Password:** A button located below the Confirm Password field.
- Create and Cancel buttons:** Two buttons at the bottom right of the window.

Figure 48: Create User Window

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

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

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

Appendix A.6.1.2. Edit Users

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

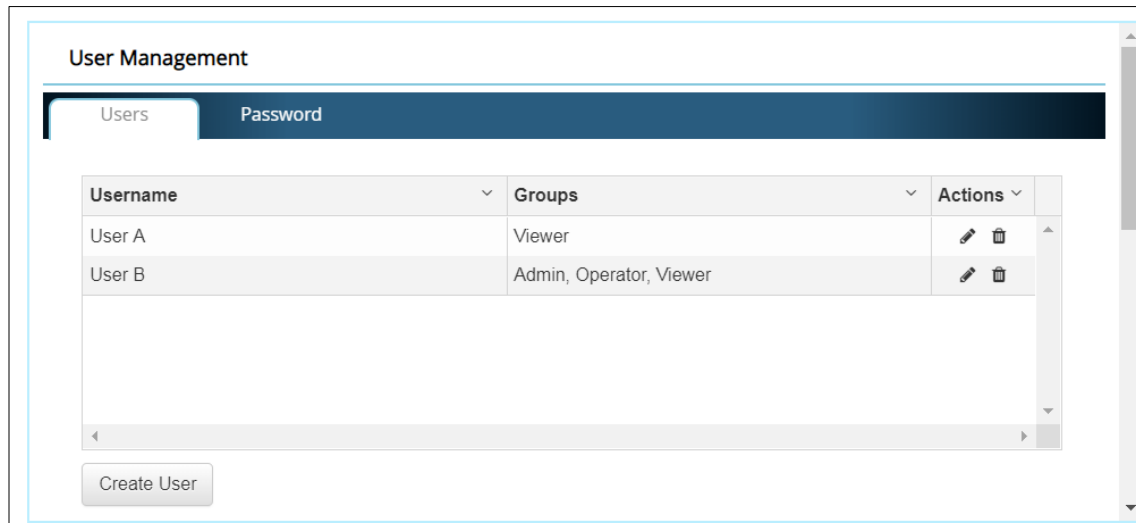
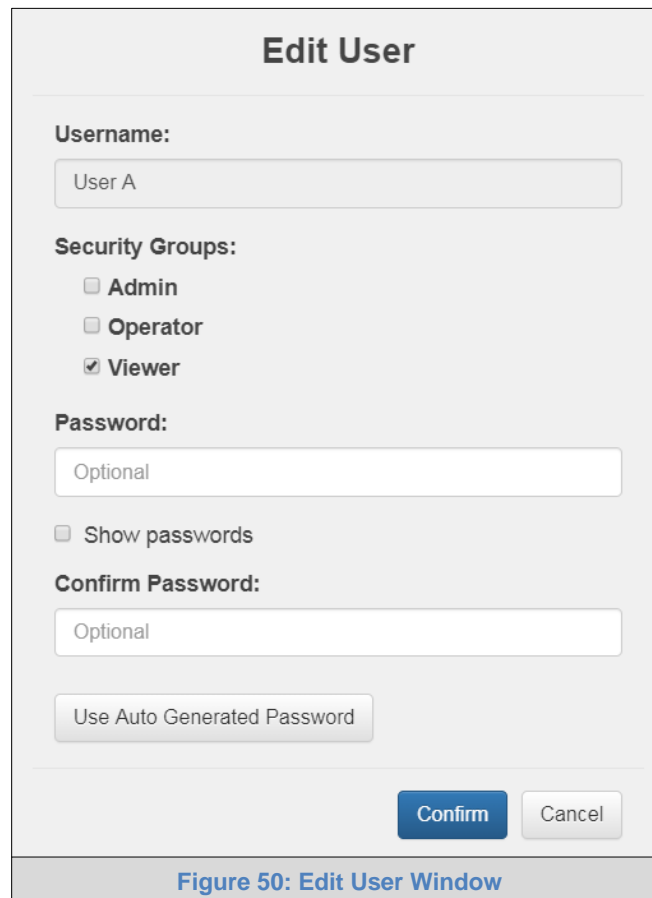


Figure 49: Setup Users

- 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:
 - ☐ Admin
 - ☐ Operator
 - ☒ Viewer
- Password:** A text field containing 'Optional'.
- ☐ Show passwords
- Confirm Password:** A text field containing 'Optional'.
-
-

Figure 50: Edit User Window

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

Appendix A.6.1.3. Delete Users

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

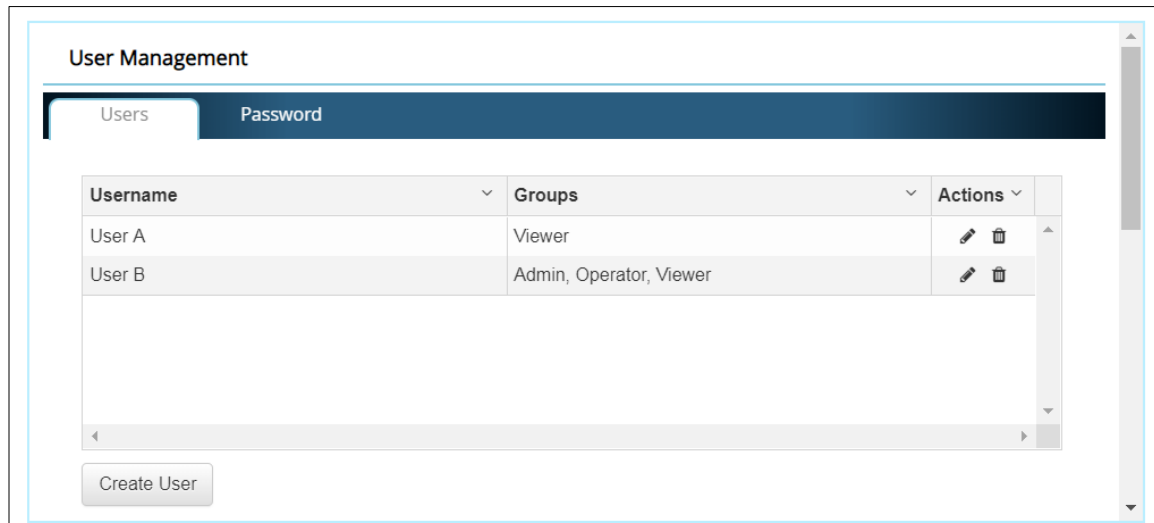


Figure 51: Setup Users

- When the warning message appears, click Confirm.

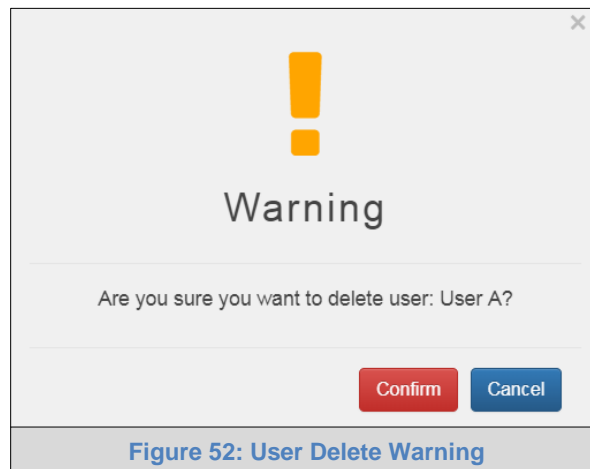


Figure 52: User Delete Warning

Appendix A.6.2. Change FieldServer Password

- Click the Password tab.

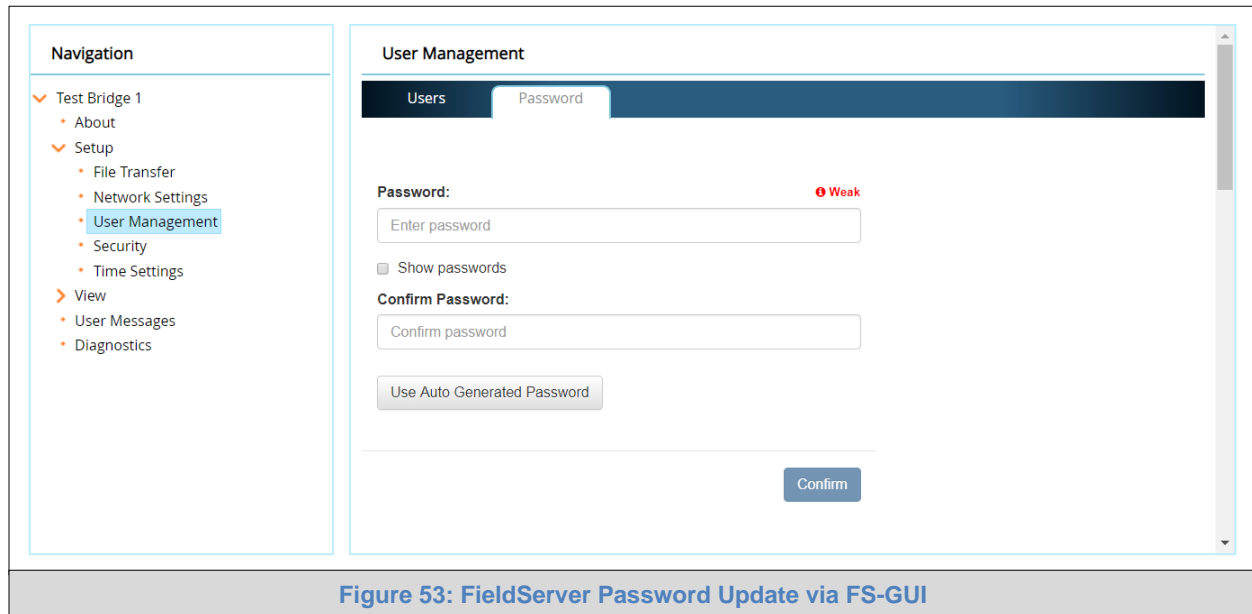


Figure 53: FieldServer Password Update via FS-GUI

- Change the 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.

NOTE: If a gateway in the field is updated to a secure gateway, the password will change to "admin". This change will still occur if the gateway was already setup with a unique password that was loaded in the factory and printed on the label.

APPENDIX B. REFERENCE

Appendix B.1. Specifications



	FS-ROUTER-BAC2 ¹
Electrical Connections	One 3-pin Phoenix connector with: RS-485 (Tx+ / Rx- / gnd) One 3-pin Phoenix connector with: RS-485 (Tx+ / Rx- / 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>Current draw:</i> 24VAC 0.125A <i>Max Power:</i> 3 Watts 9-30VDC 0.25A @12VDC
Approvals	CE and FCC Class B & C Part 15, UL 60950-1, WEEE compliant, IC Canada, RoHS compliant, BTL approved
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

Figure 54: Specifications

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

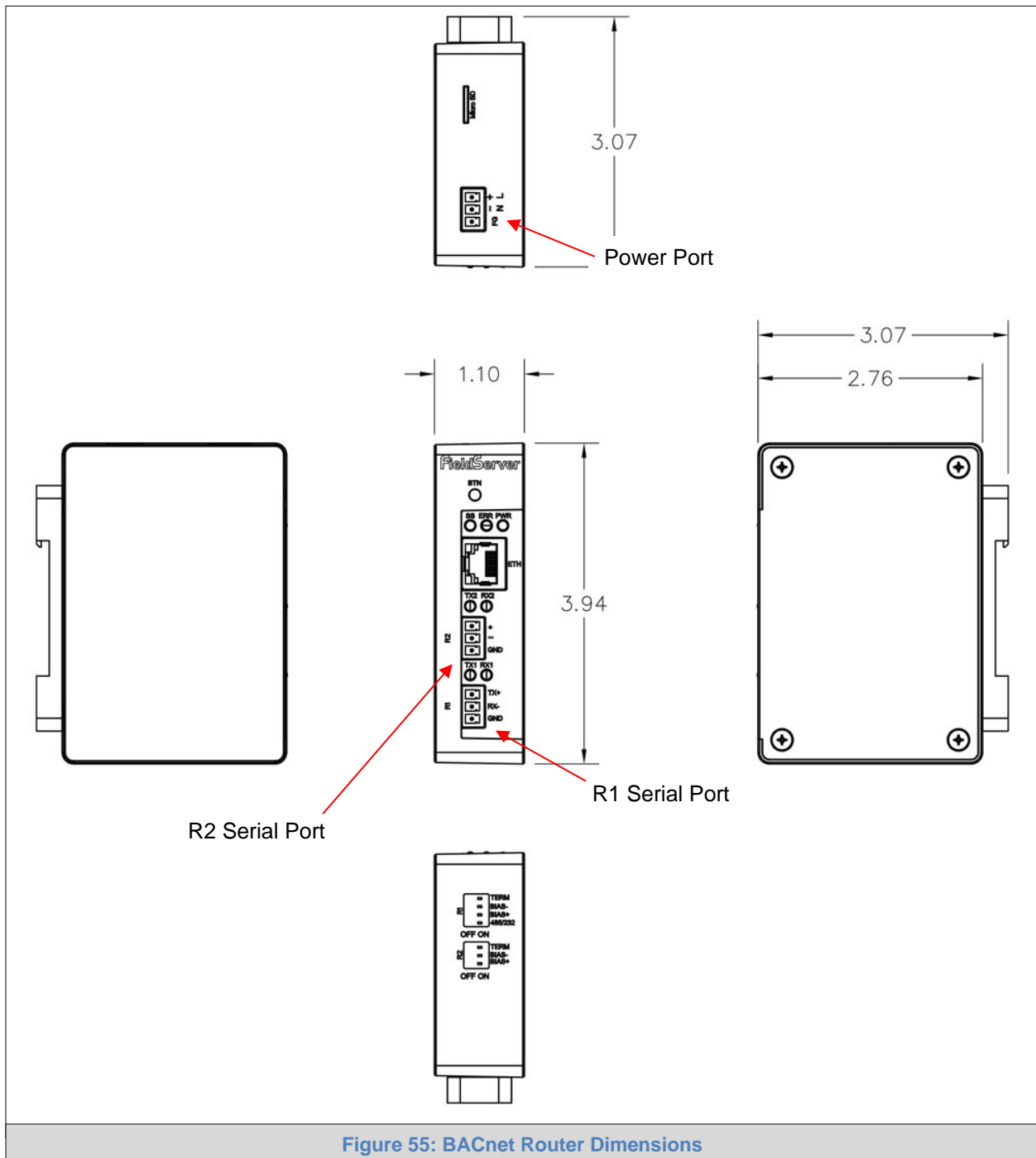
- This device may not cause harmful interference
- This device must accept any interference received, including interference that may cause undesired operation.

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

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

¹ Specifications subject to change without notice.

Appendix B.2. FS-ROUTER-BAC2 Dimension Drawing



APPENDIX C. 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.