FieldServer
BACnet Router Wi-Fi FS-ROUTER-BACW
Start-up Guide
BAS Router (BACnet Multi-Network Router)

APPLICABILITY & EFFECTIVITY
The instructions are effective for the above as of June 2020.
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
   2.2 Attaching the Wi-Fi Antenna ........................................................................................................ 6
3. Installing the BACnet Router ........................................................................................................... 7
   3.1 RS-485 ........................................................................................................................................... 7
      3.1.1 Connecting to the R1 & R2 Port .............................................................................................. 7
      3.1.1.1 Wiring ............................................................................................................................... 7
   3.2 10/100 Ethernet Connection Port .............................................................................................. 8
4. Operation ........................................................................................................................................... 9
   4.1 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
   6.1 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 Settings ....................................................................................................................................... 16
      7.1.1 Button Functions .................................................................................................................. 16
      7.1.2 Multiple Connections .......................................................................................................... 16
      7.1.3 BACnet Device ................................................................................................................... 16
      7.1.4 BACnet/IP ........................................................................................................................... 17
      7.1.5 BACnet MS/TP, BACnet Ethernet and BACnet Explorer .................................................... 18
   7.2 Network Settings ....................................................................................................................... 19
   7.3 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
Appendix A. Useful Features ................................................................................................................. 29
   Appendix A.1. Tooltips ..................................................................................................................... 29
   Appendix A.2. Take a Diagnostic Capture .......................................................................................... 30
      Appendix A.2.1. Using the FieldServer Toolbox .......................................................................... 30
      Appendix A.2.2. Using FS-GUI ..................................................................................................... 33
   Appendix A.3. Securing FieldServer with Passwords ......................................................................... 34
   Appendix A.4. Wi-Fi Signal Strength .................................................................................................. 35
   Appendix A.5. Factory Reset Instructions .......................................................................................... 35
   Appendix A.6. Internet Browsers Not Supported ................................................................................. 35
   Appendix A.7. Change Web Server Security Settings After Initial Setup ........................................... 36
      Appendix A.7.1. Change Security Mode ....................................................................................... 37
      Appendix A.7.2. Edit the Certificate Loaded onto the FieldServer .................................................. 38
   Appendix A.8. Change User Management Settings ............................................................................ 39
      Appendix A.8.1. User Management ............................................................................................... 39
         Appendix A.8.1.1. Create Users .................................................................................................. 40
         Appendix A.8.1.2. Edit Users ..................................................................................................... 41
         Appendix A.8.1.3. Delete Users .................................................................................................. 42
      Appendix A.8.2. Change FieldServer Password .............................................................................. 43
Appendix B. Reference .......................................................................................................................... 44
   Appendix B.1. Specifications .............................................................................................................. 44
   Appendix B.2. FS-ROUTER-BACW Dimension Drawing ................................................................. 45
Appendix C. Limited 2 Year Warranty .................................................................................................. 46
<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>DIN Rail</td>
<td>6</td>
</tr>
<tr>
<td>2</td>
<td>RS-485 R2 Connection Port</td>
<td>7</td>
</tr>
<tr>
<td>3</td>
<td>Ethernet Connection</td>
<td>8</td>
</tr>
<tr>
<td>4</td>
<td>Required Current Draw for the BACnet Router</td>
<td>9</td>
</tr>
<tr>
<td>5</td>
<td>Power Connections</td>
<td>9</td>
</tr>
<tr>
<td>6</td>
<td>Web Server Security Unconfigured Window</td>
<td>11</td>
</tr>
<tr>
<td>7</td>
<td>Connection Not Private Warning</td>
<td>11</td>
</tr>
<tr>
<td>8</td>
<td>Warning Expanded Text</td>
<td>12</td>
</tr>
<tr>
<td>9</td>
<td>FieldServer Login</td>
<td>12</td>
</tr>
<tr>
<td>10</td>
<td>Security Mode Selection Screen</td>
<td>13</td>
</tr>
<tr>
<td>11</td>
<td>Security Mode Selection Screen</td>
<td>14</td>
</tr>
<tr>
<td>12</td>
<td>BACnet Router Settings Page</td>
<td>15</td>
</tr>
<tr>
<td>13</td>
<td>Network Settings – IP Settings</td>
<td>19</td>
</tr>
<tr>
<td>14</td>
<td>Network Settings – Wi-Fi Client and Wi-Fi Access Point Settings</td>
<td>20</td>
</tr>
<tr>
<td>15</td>
<td>BACnet Router Diagnostics Page</td>
<td>21</td>
</tr>
<tr>
<td>16</td>
<td>FS-GUI BACnet Explorer Button</td>
<td>22</td>
</tr>
<tr>
<td>17</td>
<td>BACnet Explorer Login Page</td>
<td>22</td>
</tr>
<tr>
<td>18</td>
<td>BACnet Explorer Page</td>
<td>23</td>
</tr>
<tr>
<td>19</td>
<td>Discover Window</td>
<td>23</td>
</tr>
<tr>
<td>20</td>
<td>Device List</td>
<td>24</td>
</tr>
<tr>
<td>21</td>
<td>Device Sub-items</td>
<td>24</td>
</tr>
<tr>
<td>22</td>
<td>Full Device Sub-items</td>
<td>25</td>
</tr>
<tr>
<td>23</td>
<td>Simplified Device Details</td>
<td>25</td>
</tr>
<tr>
<td>24</td>
<td>Additional Device Details</td>
<td>26</td>
</tr>
<tr>
<td>25</td>
<td>Highlighted Present Value</td>
<td>27</td>
</tr>
<tr>
<td>26</td>
<td>Write Property Window</td>
<td>27</td>
</tr>
<tr>
<td>27</td>
<td>Updated Present Value</td>
<td>28</td>
</tr>
<tr>
<td>28</td>
<td>Settings Tooltips</td>
<td>29</td>
</tr>
<tr>
<td>29</td>
<td>Ethernet Port Location</td>
<td>30</td>
</tr>
<tr>
<td>30</td>
<td>FS-GUI Passwords Page</td>
<td>34</td>
</tr>
<tr>
<td>31</td>
<td>Password Recovery Page</td>
<td>34</td>
</tr>
<tr>
<td>32</td>
<td>Wi-Fi Signal Strength Listing</td>
<td>35</td>
</tr>
<tr>
<td>33</td>
<td>BACnet Router Landing Page</td>
<td>36</td>
</tr>
<tr>
<td>34</td>
<td>FS-GUI Landing Screen</td>
<td>36</td>
</tr>
<tr>
<td>35</td>
<td>FS-GUI Security Setup</td>
<td>37</td>
</tr>
<tr>
<td>36</td>
<td>FS-GUI Security Setup – Certificate Loaded</td>
<td>38</td>
</tr>
<tr>
<td>37</td>
<td>FS-GUI User Management</td>
<td>39</td>
</tr>
<tr>
<td>38</td>
<td>Create User Window</td>
<td>40</td>
</tr>
<tr>
<td>39</td>
<td>Setup Users</td>
<td>41</td>
</tr>
<tr>
<td>40</td>
<td>Edit User Window</td>
<td>41</td>
</tr>
<tr>
<td>41</td>
<td>Setup Users</td>
<td>42</td>
</tr>
<tr>
<td>42</td>
<td>User Delete Warning</td>
<td>42</td>
</tr>
<tr>
<td>43</td>
<td>FieldServer Password Update via FS-GUI</td>
<td>43</td>
</tr>
<tr>
<td>44</td>
<td>Specifications</td>
<td>44</td>
</tr>
<tr>
<td>45</td>
<td>BACnet Router Dimensions</td>
<td>45</td>
</tr>
</tbody>
</table>
1 BACNET ROUTER DESCRIPTION

The BACnet Router provides stand-alone routing between BACnet networks such as BACnet/IP, BACnet Ethernet, and BACnet MS/TP – 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 with Wi-Fi (FS-ROUTER-BACW) model has one RS-485 port, one Ethernet 10/100 port and supports Wi-Fi network connection. Additionally, the Router acts as a Wi-Fi access point for modern web based configuration and remote access from any mobile device without user restrictions.

The BACnet Router is cloud ready and connects with MSA Safety’s SMC Cloud.

NOTE: A cellular version of the BACnet Router is not available.

NOTE: For SMC Cloud information, refer to the SMC Cloud Start-up Guide online.

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.

2.2 Attaching the Wi-Fi Antenna

Screw in the Wi-Fi antenna to the front of the unit as shown in Appendix B.2.
3 INSTALLING THE BACNET ROUTER

3.1 RS-485

3.1.1 Connecting to the R1 & R2 Port

**For the R1 Port only:** Switch between RS-485 and RS-232 by moving the number 4 DIP Switch left for RS-485 and right for RS-232 (Figure 2).

The R2 Port is RS-485.

Connect to the 3-pin connector as shown below.

![Figure 2: RS-485 R2 Connection Port](image)

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

3.1.1.1 Wiring

<table>
<thead>
<tr>
<th>BMS RS-485 Wiring</th>
<th>BACnet Router Pin Assignment</th>
</tr>
</thead>
<tbody>
<tr>
<td>RS-485 +</td>
<td>TX +</td>
</tr>
<tr>
<td>RS-485 -</td>
<td>RX -</td>
</tr>
<tr>
<td>GND</td>
<td>GND</td>
</tr>
</tbody>
</table>

**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 OPERATION

4.1 Power Up the Device

Check power requirements in the table below:

<table>
<thead>
<tr>
<th>Current Draw Type</th>
<th>Power Requirement for BACnet Router External Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>12VDC</td>
<td>BACnet Router Family 25mA 125mA</td>
</tr>
<tr>
<td>24VDC/AC</td>
<td>FS-ROUTER-BACW (Typical) 250mA 125mA</td>
</tr>
</tbody>
</table>

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 4: Required Current Draw for the BACnet Router

Apply power to the device as show below in Figure 5. 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.

![Power Connections Diagram]

Figure 5: Power Connections
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 connect to the BACnet Router’s Default 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.
6 SETUP WEB SERVER SECURITY

6.1 Login to the FieldServer

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

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

![Web Server Security Unconfigured Window](image)

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

![Connection Not Private Warning](image)
• Additional text will expand below the warning, click the underlined text to go to the IP Address. In the Figure 8 example this text is “Proceed to 10.40.50.94 (unsafe)

![Figure 8: Warning Expanded Text](image)

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

![Figure 9: FieldServer Login](image)

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.8.
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.

![Security Mode Selection Screen](image)

**Figure 10: Security Mode Selection Screen**

**NOTE:** To change the web server security mode after initial setup, go to Appendix A.7.

**NOTE:** Cookies are used for authentication.

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.

![Security Mode Selection Screen](image)

- 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 appears and after a short period of 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 appears and after a short period of time the FieldServer GUI will open.
7 CONFIGURING THE BACNET ROUTER

Once the web server is set up, the BACnet Router landing page will appear.

NOTE: The SMC Cloud™ tab (see Figure 12) allows users to connect to the SMC Cloud, MSA Safety’s device cloud solution for IIoT. The SMC Cloud enables secure remote connection to field devices through a FieldServer and its local applications for configuration, management, maintenance. For more information about the SMC Cloud, refer to the SMC Cloud Start-up Guide.
7.1 Settings

7.1.1 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.

7.1.2 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.

7.1.3 BACnet Device

- **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.
7.1.4 BACnet/IP

- **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.
7.1.5 BACnet MS/TP, BACnet Ethernet and BACnet Explorer

- **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.
7.2 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.

![Network Settings](image)

**Figure 13: Network Settings – IP Settings**

**NOTE:** Common Settings make it possible to choose the primary connection when both Ethernet and Wi-Fi Client connections are available.
Scroll down to view and edit the Wi-Fi Client or Wi-Fi Access Point Settings.

Figure 14: Network Settings – Wi-Fi Client and Wi-Fi Access Point Settings
7.3 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.

Figure 15: 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.

- Then login to the BACnet Explorer page using the supplied username and password.

**NOTE:** The default user name is “admin” and the default password is “admin”.

**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 18: BACnet Explorer Page](image)

- 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 19: Discover Window](image)

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.

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.
• To view the full details of a device, go back to highlighting the device directly (in Figure 22 “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 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 25: Highlighted Present Value](image)

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

![Figure 26: Write Property Window](image)
• 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.
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 28: Settings Tooltips]
Appendix A.2. Take a Diagnostic Capture

When there is a problem on-site that cannot easily be resolved, perform a diagnostic capture before contacting support so that support can quickly solve the problem. There are two methods for taking diagnostic captures:

- **FieldServer Toolbox:**
  This method requires installation of the FS Toolbox program. A FS Toolbox diagnostic capture takes a snapshot of the loaded configuration files and a log of all the communications on the serial ports over a specified period of time. If the problem occurs over an Ethernet connection, then take a Wire Shark capture.

- **Gateway's FS-GUI Page:**
  This method doesn’t require downloading software. The diagnostic capture utilities are embedded in the FS-GUI web interface. Starting a diagnostic capture takes a snapshot of the loaded configuration files and a log of all the communications over a specified period of time. This works for both serial and Ethernet connections.

**NOTE:** The information in the zipped files contains everything support needs to quickly resolve problems that occur on-site.

Appendix A.2.1. Using the FieldServer Toolbox

Once the Diagnostic Capture is complete, email it to technical support. The Diagnostic Capture will accelerate diagnosis of the problem.

**NOTE:** While all necessary documentation is shipped with the FieldServer on the USB flash drive, these documents are updated regularly. New versions may be available on the Sierra Monitor website.

- Ensure that FieldServer Toolbox is loaded onto the local PC. Otherwise, download the FieldServer-Toolbox.zip via the Sierra Monitor website’s Software Downloads.

- Extract the executable file and complete the installation.

- Connect a standard Cat-5 Ethernet cable between the PC and QuickServer.

- Double click on the FS Toolbox Utility.
• **Step 1: Take a Log**
  - Click on the diagnose icon of the desired device
  - Ensure “Full Diagnostic” is selected (this is the default)

NOTE: If desired, the default capture period can be changed.
- Click on “Start Diagnostic”

- When the capture period is finished, the “Diagnostic Test Complete” window will appear

  **Step 2: Send Log**

  - Once the diagnostic test is complete, a .zip file will be saved on the PC

    - Click “Open” to launch explorer and have it point directly at the correct folder

    - Email the diagnostic zip file to **smc-support@msasafety.com**

    ![Diagnostic_test_complete_message.png](image-url)
Appendix A.2.2. Using FS-GUI

Diagnostic Capture with FS-GUI is only available on FieldServers with a bios updated/released on November 2017 or later. Completing a Diagnostic Capture through the FieldServer allows network connections (such as Ethernet and Wi-Fi) to be captured.

Once the Diagnostic Capture is complete, email it to technical support. The Diagnostic Capture will accelerate diagnosis of the problem.

- Open the FieldServer FS-GUI page.
- Click on Diagnostics in the Navigation panel.

- 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.
- Send the diagnostic zip file to smc-support@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. Securing FieldServer with Passwords

Access to the FieldServer can be restricted by enabling a password on the FS-GUI Passwords page – click Setup and then Passwords in the navigation panel. There are 2 access levels defined by 2 account names: Admin and User.

- The Admin account has unrestricted access to the FieldServer.
- The User account can view any FieldServer information but cannot make any changes or restart the FieldServer.

The password needs to be a minimum of eight characters and is case sensitive.

If the password is lost, click cancel on the password authentication popup window, and email the password recovery token to technical support to receive a temporary password from the support team. Access the FieldServer to set a new password.

![Figure 30: FS-GUI Passwords Page](image1)

Unauthorized

If you are the authorized administrator of this device and need to recover password access, you may contact support@sierramonitor.com and send them the Password Recovery Token shown below:

You will be given a recovery password to enable you to log in as Admin and create a new password.

Password Recovery Token: zMtywSDf4A==

LOGIN

www.ssierramonitor.com

![Figure 31: Password Recovery Page](image2)
Appendix A.4. Wi-Fi Signal Strength

<table>
<thead>
<tr>
<th>Wi-Fi</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;60dBm</td>
<td>Excellent</td>
</tr>
<tr>
<td>&lt;70dBm</td>
<td>Very good</td>
</tr>
<tr>
<td>&lt;80dBm</td>
<td>Good</td>
</tr>
<tr>
<td>&gt;80dBm</td>
<td>Weak</td>
</tr>
</tbody>
</table>

Figure 32: Wi-Fi Signal Strength Listing

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

Appendix A.5. 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.6. Internet Browsers Not Supported

- Internet Explorer 11

NOTE: Internet Explorer is no longer supported as recommended by Microsoft. Please use the latest version of Chrome, Firefox or Edge.
Appendix A.7. Change Web Server Security Settings After Initial Setup

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

![Figure 33: BACnet Router Landing Page](image)

- Click Setup in the Navigation panel.

![Figure 34: FS-GUI Landing Screen](image)
Appendix A.7.1. 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

- Click the Save button.
Appendix A.7.2. 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.
Appendix A.8. Change User Management Settings

- 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. If the default unique password is lost then the unit must be mailed back to the factory.

Appendix A.8.1. User Management

- Check that the Users tab is selected.

![User Management Screen](image)

**Figure 37: FS-GUI User Management**

User Types:

**Admin** – Can modify any settings on the FieldServer.

**Operator** – Can only make changes to the FieldServer Device Configuration.

**Viewer** – Can only view settings/reads on the FieldServer.
Appendix A.8.1.1. Create Users

- Click the Create User button.

![Create User Window]

- Enter the new User fields: Name, Security Group and Password.

**NOTE:** Passwords must be at least 10 characters long. 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.8.1.2. Edit Users

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

![User Management](image)

**Figure 39: Setup Users**

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

![Edit User Window](image)

**Figure 40: Edit User Window**

- Click Confirm.
- Once the Success message appears, click OK.
Appendix A.8.1.3. Delete Users

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

When the warning message appears, click Confirm.
Appendix A.8.2. Change FieldServer Password

- Click the Password tab.

**NOTE:** Passwords must be at least 10 characters long. An algorithm automatically checks the password entered and notes the level of strength on the top right of the Password text field.
Appendix B. Reference

Appendix B.1. Specifications

<table>
<thead>
<tr>
<th>FS-ROUTER-BACW ¹</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Available Ports</strong></td>
<td></td>
</tr>
<tr>
<td>One 3-pin Phoenix connector with: RS-485 port (TX+/RX-/gnd)</td>
<td></td>
</tr>
<tr>
<td>One 3-pin Phoenix connector with: RS-485 port (TX+/RX-/gnd)</td>
<td></td>
</tr>
<tr>
<td>One 3-pin Phoenix connector with: Power port (+/-/Frame-gnd)</td>
<td></td>
</tr>
<tr>
<td>One Ethernet 10/100 BaseT port</td>
<td></td>
</tr>
<tr>
<td><strong>Power Requirements</strong></td>
<td></td>
</tr>
<tr>
<td>Input Voltage: 9-30VDC or 24VAC</td>
<td>Current draw: 24VAC 0.125A</td>
</tr>
<tr>
<td>Max Power: 3 Watts</td>
<td>9-30VDC 0.25A @12VDC</td>
</tr>
<tr>
<td><strong>Approvals</strong></td>
<td></td>
</tr>
<tr>
<td>CE and FCC Class B &amp; C Part 15, UL 60950-1, WEEE compliant, IC Canada, RoHS compliant</td>
<td></td>
</tr>
<tr>
<td><strong>Dimensions (WxDxH)</strong></td>
<td></td>
</tr>
<tr>
<td>4 x 1.1 x 2.7 in (10.16 x 2.8 x 6.8 cm)</td>
<td></td>
</tr>
<tr>
<td><strong>Weight</strong></td>
<td></td>
</tr>
<tr>
<td>0.4 lbs (0.2 Kg)</td>
<td></td>
</tr>
<tr>
<td><strong>Operating Temperature</strong></td>
<td></td>
</tr>
<tr>
<td>-20 to 70°C (-4 to 158°F)</td>
<td></td>
</tr>
<tr>
<td><strong>Humidity</strong></td>
<td></td>
</tr>
<tr>
<td>10-95% RH non-condensing</td>
<td></td>
</tr>
<tr>
<td><strong>Wi-Fi 802.11 b/g/n</strong></td>
<td></td>
</tr>
<tr>
<td>Frequency: 2.4 GHz</td>
<td>Channels: 1 to 11 (inclusive)</td>
</tr>
<tr>
<td>Antenna Type: SMA</td>
<td>Encryption: TKIP, WPA &amp; AES</td>
</tr>
</tbody>
</table>

"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-BACW Dimension Drawing

Figure 45: BACnet Router Dimensions
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.