APPLICABILITY & EFFECTIVITY

Effective for all systems manufactured after March 2020.
Technical Support

Thank you for purchasing the BACnet IoT Gateway from MSA Safety.

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 IoT Gateway Description ............................................................................. 7

2 Equipment Setup ........................................................................................................ 8
   2.1 Physical Dimensions .......................................................................................... 8
   2.1.1 FS-IoT-BAC Drawing .................................................................................. 8
   2.1.2 FS-IoT-BACW Drawing .............................................................................. 9
   2.1.3 FS-IoT-BACC Drawing .............................................................................. 10
   2.2 Mounting .......................................................................................................... 11
   2.3 Attaching the Antenna(s) .................................................................................. 11
   2.4 FS-IoT-BACC: Inserting the SIM Card ............................................................. 12

3 Installing the BACnet IoT Gateway .......................................................................... 13
   3.1 FS-IoT-BAC/BACW: Connecting the R1 & R2 Ports ........................................... 13
   3.1.1 Wiring ......................................................................................................... 13
   3.2 FS-IoT-BACC: Connecting the P1 Port .............................................................. 14
   3.2.1 Wiring ......................................................................................................... 14
   3.3 10/100 Ethernet Connection Port ................................................................... 15

4 Operation .................................................................................................................... 16
   4.1 Power up the Device .......................................................................................... 16

5 Connecting to the BACnet IoT Gateway ................................................................... 17
   5.1 Using the FieldServer Toolbox ....................................................................... 17
   5.2 Connect Using a Web Browser ......................................................................... 18
   5.3 Logging into BACnet IoT Gateway ................................................................... 19
   5.3.1 Change Password ....................................................................................... 20
   5.4 Add Additional Users ...................................................................................... 20
   5.5 Manage Users .................................................................................................. 20

6 Configuring the BACnet IoT Gateway ..................................................................... 22
   6.1 Settings ............................................................................................................ 22
   6.1.1 Network Settings ....................................................................................... 22
   6.1.2 Local Settings – BACnet ............................................................................ 24
   6.1.3 Remote Settings – Foreign Device Registration for BBMD Support .............. 25

7 Using the BACnet IoT Gateway ............................................................................... 26
   7.1 BACnet Explorer ............................................................................................. 26
   7.1.1 Discover the Device List ............................................................................. 27
   7.1.2 View Device Details and Explore Points/Parameters ................................. 28
   7.1.3 Explore All of a Device’s Points – Deep Explore ....................................... 30
   7.1.4 Checking Device Information – Device Info .............................................. 31
   7.1.5 Edit the Present Value Field ....................................................................... 32
   7.2 Monitor View .................................................................................................... 34
   7.2.1 Set Devices to Track .................................................................................. 34
   7.2.2 Logging Data .............................................................................................. 35
   7.3 Historian ........................................................................................................... 37
   7.3.1 Graph Data Logging Information ............................................................... 37
   7.3.2 Creating an Event Log ............................................................................... 40
   7.4 Event Log .......................................................................................................... 42

8 Connecting to the SMC Cloud ................................................................................. 43
   8.1 Create a New SMC Cloud Account .................................................................. 43
   8.2 Registration Process ......................................................................................... 48
   8.3 Login to SMC Cloud ......................................................................................... 50
# Table of Contents

9  Integrating with the ThingWorx Platform ................................................................. 52
   9.1  ThingWorx General Overview ................................................................. 52
   9.2  Connect to ThingWorx ........................................................................... 53
   9.3  Configure the Thing Settings on Discovered Devices ......................... 54
   9.4  Check the Status Window ........................................................................ 55

10  Integrating with Cisco Kinetic............................................................... 56
   10.1  Cisco Kinetic General Overview ............................................................ 56
   10.2  Connect to Cisco Kinetic ........................................................................ 57
   10.3  Check the Status Window ........................................................................ 58

Appendix A Specifications.................................................................................. 59

Appendix B References...................................................................................... 60
   Appendix B.1. Understanding FDR ................................................................. 60
   Appendix B.2. Understanding BACnet BBMD and NAT Routing ................. 60

Appendix C Troubleshooting............................................................................. 62
   Appendix C.1. Communicating with the BACnet IoT Gateway Over the Network ................................................................. 62
   Appendix C.2. Lost or Incorrect IP Address .................................................... 63
   Appendix C.3. Viewing Diagnostic Information .............................................. 64
   Appendix C.4. Checking Wiring and Settings .................................................. 64
   Appendix C.5. LED Diagnostics for Communications Between BACnet IoT Gateway and Devices .................................................. 65
   Appendix C.6. Before Contacting Technical Support Take a Diagnostic Capture ................................................................. 66
   Appendix C.7. Updating Firmware ................................................................... 67
   Appendix C.8. Securing BACnet IoT Gateway with Passwords .................... 68
   Appendix C.9. Kaspersky Endpoint Security 10 ............................................... 69
   Appendix C.10. Wi-Fi and Cellular Signal Strength ........................................ 70
   Appendix C.11. Factory Reset Instructions ...................................................... 70
   Appendix C.12. Internet Browsers Not Supported .......................................... 70

Appendix D Limited 2 Year Warranty................................................................. 71
<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>BACnet IoT Gateway FS-IOT-BAC Dimensions</td>
<td>8</td>
</tr>
<tr>
<td>2</td>
<td>BACnet IoT Gateway FS-IOT-BACW Dimensions</td>
<td>9</td>
</tr>
<tr>
<td>3</td>
<td>BACnet IoT Gateway FS-IOT-BACC Dimensions</td>
<td>10</td>
</tr>
<tr>
<td>4</td>
<td>DIN Rail</td>
<td>11</td>
</tr>
<tr>
<td>5</td>
<td>Insert SIM Card into the Micro SIM Card Slot – Label Side View (Left) and Top Down View (Right)</td>
<td>12</td>
</tr>
<tr>
<td>6</td>
<td>R1 &amp; R2 Connection Ports</td>
<td>13</td>
</tr>
<tr>
<td>7</td>
<td>RS-485 R2 Connection Port</td>
<td>14</td>
</tr>
<tr>
<td>8</td>
<td>Ethernet Connection</td>
<td>15</td>
</tr>
<tr>
<td>9</td>
<td>Required Current Draw for the BACnet IoT Gateway</td>
<td>16</td>
</tr>
<tr>
<td>10</td>
<td>Connecting Power for FS-IOT-BAC</td>
<td>16</td>
</tr>
<tr>
<td>11</td>
<td>Connecting Power for FS-IOT-BACC</td>
<td>16</td>
</tr>
<tr>
<td>12</td>
<td>BACnet IoT Gateway Login Page</td>
<td>18</td>
</tr>
<tr>
<td>13</td>
<td>Login Window</td>
<td>19</td>
</tr>
<tr>
<td>14</td>
<td>BACnet IoT Gateway Landing Page</td>
<td>19</td>
</tr>
<tr>
<td>15</td>
<td>Profile Settings Window</td>
<td>20</td>
</tr>
<tr>
<td>16</td>
<td>Manage Users Settings</td>
<td>20</td>
</tr>
<tr>
<td>17</td>
<td>Select User</td>
<td>21</td>
</tr>
<tr>
<td>18</td>
<td>Edit User Information</td>
<td>21</td>
</tr>
<tr>
<td>19</td>
<td>Configuration Button Functions</td>
<td>22</td>
</tr>
<tr>
<td>20</td>
<td>Network Settings – Common and IP Settings</td>
<td>22</td>
</tr>
<tr>
<td>21</td>
<td>Network Settings – Wi-Fi Client, Wi-Fi AP, and Cellular Settings</td>
<td>23</td>
</tr>
<tr>
<td>22</td>
<td>Connection Settings</td>
<td>24</td>
</tr>
<tr>
<td>23</td>
<td>Connection Parameters</td>
<td>24</td>
</tr>
<tr>
<td>24</td>
<td>FDR Enabled Checkbox</td>
<td>25</td>
</tr>
<tr>
<td>25</td>
<td>FDR IP Fields</td>
<td>25</td>
</tr>
<tr>
<td>26</td>
<td>BACnet Explorer Page</td>
<td>26</td>
</tr>
<tr>
<td>27</td>
<td>Discovery Window</td>
<td>27</td>
</tr>
<tr>
<td>28</td>
<td>Device List</td>
<td>27</td>
</tr>
<tr>
<td>29</td>
<td>Device Sub-Items</td>
<td>28</td>
</tr>
<tr>
<td>30</td>
<td>Full Device Sub-items</td>
<td>28</td>
</tr>
<tr>
<td>31</td>
<td>Simplified Device Details</td>
<td>29</td>
</tr>
<tr>
<td>32</td>
<td>Additional Device Details</td>
<td>29</td>
</tr>
<tr>
<td>33</td>
<td>Highlighted Present Value</td>
<td>32</td>
</tr>
<tr>
<td>34</td>
<td>Write Property Window</td>
<td>32</td>
</tr>
<tr>
<td>35</td>
<td>Updated Present Value</td>
<td>33</td>
</tr>
<tr>
<td>36</td>
<td>Selected Device Properties for Monitor View</td>
<td>34</td>
</tr>
<tr>
<td>37</td>
<td>Highlighted Monitor View Tab</td>
<td>34</td>
</tr>
<tr>
<td>38</td>
<td>Monitor View Showing Tracked Device Properties</td>
<td>35</td>
</tr>
<tr>
<td>39</td>
<td>Data Logging Window</td>
<td>35</td>
</tr>
<tr>
<td>40</td>
<td>Change of Value Log Type</td>
<td>35</td>
</tr>
<tr>
<td>41</td>
<td>Periodic Log Type</td>
<td>35</td>
</tr>
<tr>
<td>42</td>
<td>Settings Window</td>
<td>36</td>
</tr>
<tr>
<td>43</td>
<td>Poll Interval Window</td>
<td>36</td>
</tr>
<tr>
<td>44</td>
<td>Historian Page</td>
<td>37</td>
</tr>
<tr>
<td>45</td>
<td>Historian Settings Window</td>
<td>37</td>
</tr>
<tr>
<td>46</td>
<td>Confirm Clear Logs Window</td>
<td>38</td>
</tr>
<tr>
<td>47</td>
<td>Historian Graph</td>
<td>38</td>
</tr>
<tr>
<td>48</td>
<td>Selected Portion of Historian Graph</td>
<td>39</td>
</tr>
<tr>
<td>49</td>
<td>Monitor View Device Properties</td>
<td>40</td>
</tr>
<tr>
<td>50</td>
<td>Event Settings Window</td>
<td>40</td>
</tr>
<tr>
<td>51</td>
<td>Add Event Settings</td>
<td>40</td>
</tr>
<tr>
<td>52</td>
<td>Event Settings Window with Added Events</td>
<td>41</td>
</tr>
<tr>
<td>53</td>
<td>Monitor View Device Properties with Updated Status</td>
<td>41</td>
</tr>
<tr>
<td>54</td>
<td>Event Log Page Showing Added Events</td>
<td>42</td>
</tr>
<tr>
<td>55</td>
<td>BACnet IoT Gateway Landing Page – SMC Cloud Tab</td>
<td>43</td>
</tr>
</tbody>
</table>
Figure 56: Registration Information Page ................................................................. 43
Figure 57: SMC Cloud Connection Problems Message ............................................ 44
Figure 58: SMC Cloud Registration Page ................................................................. 45
Figure 59: Welcome to SMC Cloud Email ............................................................... 46
Figure 60: Setting User Details ................................................................................ 47
Figure 61: Register the Gateway on SMC Cloud ....................................................... 48
Figure 62: Device Registered for SMC Cloud .......................................................... 49
Figure 63: SMC Cloud Login Page .......................................................................... 50
Figure 64: SMC Cloud Privacy Policy ..................................................................... 50
Figure 65: SMC Cloud Landing Page ....................................................................... 51
Figure 66: Specifications .......................................................................................... 59
Figure 67: BBMD Scenario 1 – Interconnected IP Network ..................................... 60
Figure 68: BBMD Scenario 2 – NAT Routing ............................................................ 61
Figure 69: Ethernet Port Location ............................................................................ 63
Figure 70: Error Messages Screen .......................................................................... 64
Figure 71: Diagnostic LEDs .................................................................................... 65
Figure 72: FS-GUI Passwords Page ......................................................................... 68
Figure 73: Password Recovery Page ....................................................................... 68
Figure 74: Kaspersky ES10 Settings ....................................................................... 69
Figure 75: Web Anti-Virus Trusted URLs ............................................................... 69
Figure 76: Wi-Fi & Cellular Signal Strength Listing ............................................... 70
1 BACNET IOT GATEWAY DESCRIPTION

The BACnet IoT Gateway provides a connection from BACnet devices and networks to the cloud. This is achieved via a discovery tool built into the hardware for any BACnet/IP or BACnet MS/TP network without any additional dongles or installations needed. BBMD BACnet network discovery is also supported.

The BACnet IoT Gateway comes in three models. The FS-IOT-BAC model offers two RS-485 ports and one Ethernet 10/100 port. The FS-IOT-BACW model has two RS-485 ports, one Ethernet 10/100 port and supports Wi-Fi network connection. The FS-IOT-BACC model only supports one RS-485 port but has cellular connections as well as other ports and support offered by the FS-IOT-BACW model.

Additionally, Wi-Fi models act as a Wi-Fi access point for modern web-based configuration and remote access from any mobile device without user restrictions.

The BACnet IoT Gateway also includes Monitor View, Historian, Virtual Points and Event Log data analysis features that allow tracking and logging of individual device data points across the connected network in real-time.

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

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

NOTE: The latest versions of instruction manuals, driver manuals, configuration manuals and support utilities are available online through the Sierra Monitor website.
2 EQUIPMENT SETUP

2.1 Physical Dimensions

2.1.1 FS-IOT-BAC Drawing

![BACnet IoT Gateway FS-IOT-BAC Dimensions](image)

Figure 1: BACnet IoT Gateway FS-IOT-BAC Dimensions
2.1.2 FS-IOT-BACW Drawing

Figure 2: BACnet IoT Gateway FS-IOT-BACW Dimensions
2.1.3 FS-IOT-BACC Drawing

Figure 3: BACnet IoT Gateway FS-IOT-BACC Dimensions
2.2 Mounting

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

![DIN Rail Bracket](image)

**Figure 4: DIN Rail**

2.3 Attaching the Antenna(s)

**NOTE:** This Section does not apply to the FS-IOT-BAC model BACnet IoT Gateway.

**Wi-Fi Antenna:**
If using the FS-IOT-BACW (Wi-Fi) or FS-IOT-BACC (Cellular & Wi-Fi) models, screw in the Wi-Fi antenna to the front of the unit as shown in **Figure 2**.

**Cellular Antenna:**
If using the FS-IOT-BACC model, screw in the long cellular antenna on the top of the unit as shown in **Figure 3**.
2.4 FS-IOT-BACC: Inserting the SIM Card

NOTE: A micro 3G SIM card (data only for commercial products IMEI 357178070517852) must be purchased from an AT&T, Kore Telematics or Vodafone cellular provider to set up cellular functionality and create a data plan for the ProtoAir. SIM card vendor contact information is available at the end of the section.

Insert the SIM card into the Micro SIM card slot with the chip on the SIM card facing away from the cellular antenna as shown below.

See Section 6 to complete cellular setting configuration.

SIM Card Vendor Contact Information:
Kore Telematics
Joao Freitas
KORE Wireless
Office: (669) 600-5360
jfreitas@korewireless.com
www.koretelematics.com

AT&T
Please call AT&T Customer Service at 800.331.0500 or find the nearest AT&T store.
3 INSTALLING THE BACNET IOT GATEWAY

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

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

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

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

3.1.1 Wiring

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

**NOTE:** Use standard grounding principles for GND.
3.2 FS-IOT-BACC: Connecting the P1 Port

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

Connect to the 3-pin connector as shown below.

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

### 3.2.1 Wiring

<table>
<thead>
<tr>
<th>BMS RS-485 Wiring</th>
<th>BACnet IoT Gateway 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.
3.3 10/100 Ethernet Connection Port

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

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

4.1 Power up the Device

Check power requirements in the table below:

<table>
<thead>
<tr>
<th>BACnet IoT Gateway Family</th>
<th>Current Draw Type</th>
<th>12VDC</th>
<th>24VDC</th>
<th>24VAC</th>
</tr>
</thead>
<tbody>
<tr>
<td>FS-IOT-BAC/BACW (Typical)</td>
<td>250mA</td>
<td>125mA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FS-IOT-BACC (Typical)</td>
<td>320mA</td>
<td>185mA</td>
<td></td>
<td>N/A</td>
</tr>
<tr>
<td>FS-IOT-BACC (Maximum)</td>
<td>670mA</td>
<td>390mA</td>
<td></td>
<td>N/A</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.

Apply power to the BACnet IoT Gateway as shown below. Ensure that the power supply used complies with the specifications provided. Ensure that the cable is grounded using the FG or “Frame GND” terminal, except when using 24VAC.

- The **FS-IOT-BAC/BACW** BACnet IoT Gateway accepts 9-30VDC or 24VAC.
- The **FS-IOT-BACC** BACnet IoT Gateways accept 12-24VDC.
5 CONNECTING TO THE BACNET IOT GATEWAY

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

5.1 Using the FieldServer Toolbox

- Install the Toolbox application from the USB drive or get it from the Sierra Monitor website.
- Use the Toolbox application to find the BACnet IoT Gateway IP Address and launch the Web App (by clicking the Connect button).
5.2 Connect Using a Web Browser

- Open a Web Browser and input the BACnet IoT Gateway’s IP Address. The Default IP Address of the BACnet IoT Gateway is **192.168.2.101**, Subnet Mask is **255.255.255.0**.

- If the PC and the BACnet IoT Gateway are on different IP Networks, assign a Static IP Address to the PC on the 192.168.2.X network.

![BACnet IoT Gateway Login Page](image)

*Figure 12: BACnet IoT Gateway Login Page*
5.3 Logging into BACnet IoT Gateway

- Click the orange “Login” button and enter user name and password information into the Login Window.

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

![Login Window](image)

**Figure 13: Login Window**

- The BACnet IoT Gateway landing page will open once valid user information has been entered and the “Log In” button is clicked.

![Landing Page](image)

**Figure 14: BACnet IoT Gateway Landing Page**
5.3.1 Change Password

- Once logged in, click on the profile dropdown menu (Profile) in the top right corner of any page.
- Then click on Settings (Settings) to open the Profile Settings window.

- Fill in the old password and the two new password fields, then click the change password button.
- A successful password update message will appear, click the “x” in the upper right corner of the window to exit the Profile Settings window.

5.4 Add Additional Users

- Once in the Profile Settings window, fill in the username, the two password and role fields.

**NOTE:** An administrator role has full access to the BACnet IoT Gateway and user management, while a user role does not have user management capability.
- Click the Add User button to save the new user.

5.5 Manage Users

- When more than one user is generated for the BACnet IoT Gateway, the Manage Users field will appear in the Profile Settings window.
NOTE: Only administrators are able to see and edit the Manage User fields.

- To edit a user entry, select a specific user from the dropdown menu.

  Figure 17: Select User

  ![Select User](image)

- This opens up multiple fields that allow editing of user information.

  Figure 18: Edit User Information

  ![Edit User Information](image)

- Select the action to perform:
  - Reset user password – Fill in the two password fields and click the Reset Password button
  - Change user role – Select the desired role in the dropdown menu and click the Change Role button
  - Delete user – Simply click the Delete User button and the user entry will be deleted
6 CONFIGURING THE BACNET IOT GATEWAY

6.1 Settings

By default, the BACnet IoT Gateway will open up on the BACnet Explorer page (Figure 14). Navigate to the settings by clicking on the Settings button, found along the left side of the page. The BACnet IoT Gateway settings are split up into three types: Local Settings, Remote Settings and Network Settings.

The table below describes how the buttons at the bottom of each page function.

<table>
<thead>
<tr>
<th>Button</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Save</td>
<td>Click to save settings. Saving will require the device to be restarted.</td>
</tr>
<tr>
<td>Refresh</td>
<td>Click to clear the current settings before saving; if settings have been saved the Refresh button is unavailable.</td>
</tr>
<tr>
<td>Defaults</td>
<td>Click to change settings back to factory defaults.</td>
</tr>
</tbody>
</table>

Figure 19: Configuration Button Functions

The following sections explain the setting parameters by type for BACnet IoT Gateway configuration.

6.1.1 Network Settings

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

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, Wi-Fi Access Point, and Cellular Settings.

**NOTE:** Cellular Settings are only available on FS-IOT-BACC models.
6.1.2 Local Settings – BACnet

Enter the fields for the settings described below as needed:

![Connection Settings](image)

**Figure 22: Connection Settings**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>All Connections</strong></td>
<td></td>
</tr>
<tr>
<td>Network Number</td>
<td>The BACnet network number for the connection. Legal values are 1-65534. Each network number must be unique across the entire BACnet internetwork. The <strong>Internal Network Number</strong> is used for internal BACnet traffic and has to be unique across the BACnet network.</td>
</tr>
<tr>
<td><strong>BACnet/IP Settings</strong></td>
<td></td>
</tr>
<tr>
<td>IP Port</td>
<td>The BACnet/IP default is 47808 (0xBAC0), but other port numbers can may be specified.</td>
</tr>
<tr>
<td><strong>BACnet MS/TP Settings</strong></td>
<td></td>
</tr>
<tr>
<td>MAC Address</td>
<td>Legal values are 0-127, must be unique on the physical network.</td>
</tr>
<tr>
<td>Max Master</td>
<td>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.</td>
</tr>
<tr>
<td>Max Info Frames</td>
<td>The number of transactions the BACnet IoT Gateway may initiate while it has the MS/TP token. Default is 50.</td>
</tr>
<tr>
<td>BAUD Rate</td>
<td>The serial baud rate used on the network.</td>
</tr>
<tr>
<td>Token Usage Timeout (ms)</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Figure 23: Connection Parameters**
6.1.3 Remote Settings – Foreign Device Registration for BBMD Support

The BACnet IoT Gateway uses “Foreign Device Registration” or “FDR” to communicate to BACnet/IP devices on another network. Follow the instructions below to enable FDR between the BACnet IoT Gateway and a remote network:

- Click the “Enabled” checkbox under the Foreign Device Registration section of the BACnet Settings.

![Figure 24: FDR Enabled Checkbox](image)

- Enter the Remote BACnet Router’s externally mapped IP Address and BACnet/IP Port to the appropriate Foreign Device Registration fields. This allows the BACnet IoT Gateway to discover BACnet devices on the remote network.

![Figure 25: FDR IP Fields](image)

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

NOTE: See Appendix B for additional details concerning FDR and BBMD.
7 USING THE BACNET IOT GATEWAY

Sections 7.1 – 7.4 represent each of the first four tabs that appear across the left side of the page once logged into the BACnet IoT Gateway and describe their functions.

7.1 BACnet Explorer

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

[Figure 26: BACnet Explorer Page]
7.1.1 Discover the Device List

- To discover the devices connected to the same subnet as the BACnet IoT Gateway, click the Discover button (binocular icon).
- This will open the Discovery window, click the checkboxes next to the desired discovery 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.
7.1.2 View Device Details and Explore Points/Parameters

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

- To view the full details of a device, highlight the device directly (in Figure 30 “1991 WeatherLink_1”) and click the Explore button (🔍) that appears to the right of the highlighted device.
  - Now additional device details are viewable; however, the device can be explored even further.
• Click on one of the device details.

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

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
  o Device
    ▪ Device object
7.1.3 Explore All of a Device’s Points – Deep Explore

- To explore all device objects under a specific device with one search, click the desired device to highlight it.

- Then click the three white dots (≡) that appear to the right of the highlighted device to open a dropdown menu.

- Click Deep Explore to open the Deep Explore window.

- Select which property types to find in the search.

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

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

- Click the Explore button and wait for the green explore complete message to confirm all points have been discovered.
7.1.4 Checking Device Information – Device Info

- To check a device’s properties/information, click the desired device to highlight it.
- Then click the three white dots ( ) that appear to the right of the highlighted device to open a dropdown menu.
- Click Device Info to open the Device Info window and get the device information needed.
7.1.5 Edit the Present Value Field

The only recommended field to edit via BACnet IoT Gateway is the device’s present value field.

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

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

![Figure 33: Highlighted Present Value](image)

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

![Figure 34: Write Property Window](image)
• 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.

![Updated Present Value](image)

**Figure 35: Updated Present Value**
7.2 Monitor View

7.2.1 Set Devices to Track

Before using the Monitor View page, device properties must be selected to be monitored for analysis and testing in the BACnet Explorer page. To do so follow the instructions below:

- When viewing the expanded device properties on the BACnet Explorer page, click the checkbox to the left of any property to track.

- Once all properties are selected for that data type, click the monitor button to set the selected properties to be monitored.
  - The Monitor column in the selected property row will change from “Off” to “On”

**NOTE:** A maximum of 1,000 data points can be monitored.

- Wait for the configuration to complete, then click on the Monitor View tab.
7.2.2 Logging Data

- To log data for Historian, Event Log and SMC Cloud, click the checkbox under the Log column.

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

- Select the type of logging for the data point and set the logging interval, COV threshold value or COV max scan time as they apply then click the Save button to save the settings.
To change the poll interval of a device, click the Settings button (see Figure 38) to open the Settings window.

```
+-------------------+-------------------+-------------------+
| Device            | Device Name       | Poll Interval (s) |
+-------------------+-------------------+-------------------+
| 1991              | WeatherLink_1     | 5                 |
+-------------------+-------------------+-------------------+
```

**Figure 42: Settings Window**

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

```
Poll Interval (s) 5
```

**Figure 43: Edit Poll Interval Window**

Make desired changes and click Save.

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

**NOTE:** Click the Trash icon (trash can) to the right of any logged property to remove it from Monitor View.
7.3 Historian

NOTE: The Historian can log up to 1,000 data points.

- Click the Historian tab on the left side of the page.

![Figure 44: Historian Page]

7.3.1 Graph Data Logging Information

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

![Figure 45: Historian Settings Window]

- Click the checkbox next to the data element to graph.
  - Any combination of elements can be selected

NOTE: A data element is only visible when it is set for data logging as shown in Section 7.2.
• Click Submit to generate a graph for each element selected.
  
  o To delete a log, check the boxes next to the properties to delete and click the delete button; then click “Yes” to confirm

![Confirm Clear Logs Window](image)

**Figure 46: Confirm Clear Logs Window**

• After a few seconds the graph should appear.

![Historian Graph](image)

**Figure 47: Historian Graph**

To view individual values of data, scroll across the graph to show a text box that states each exact point and the location of that point on the graph via a blue dot.

![Text Box](image)

To view a graph of only select dates/time frames, move the cursor towards the miniature version of the graph that is shown just below the full size graph. Hover the cursor over the miniature graph so that the cursor becomes a crosshair (＋).

![Miniature Graph](image)

Click and hold near the beginning or ending time frame desired, then drag the crosshair towards the ending or beginning time frame; all within the confines of the miniature graph.
The full-size version of the graph will populate accordingly.

![Selected Portion of Historian Graph](image)

Any additional edits to the time frame can be adjusted by clicking and dragging the wedge markers on either side of the highlighted portion of the miniature graph.

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

**NOTE:** The data selected in Historian is also available via SMC Cloud RESTful API, contact FieldServer Technical Support for a copy of the RESTful API Start-up Guide.
7.3.2 Creating an Event Log

- To create an event log for a property, click on the Monitor View tab to go to the Monitor View page.

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

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

- Set the event as needed and click Save.
• Repeat this process to create more events as needed.

![Event Settings Window with Added Events](image)

**Figure 52: Event Settings Window with Added Events**

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

• Click the “x” in the top right corner of the Event Settings window to close it.
  o The Monitor View page will now update the status column as events take place

![Monitor View Device Properties with Updated Status](image)

**Figure 53: Monitor View Device Properties with Updated Status**
7.4 Event Log

Click the Event Log tab on the left side of the page to open the Event Logger and view the events that have been set to track in Section 7.3.2 (by time and type with a descriptive message).

![Event Logger][1]

**Figure 54: Event Log Page Showing Added Events**
8 CONNECTING TO THE SMC CLOUD

8.1 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.

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

Securely access your FieldServer from anywhere with the SMC Cloud™ device cloud

Your One Stop for Managing Your Devices and Users

- Secure Remote Access
  Securely connect your field devices SMC Cloud™

- Device Management
  Manage all your FieldServers and connected devices from SMC Cloud™ and upgrade firmware remotely

- User Management
  Set up your user personnel with the right security permissions and device assignments for users to diagnose, configure, and better support the field installation.

For more information about SMC Cloud™, visit our website.
If a warning message appears instead of the splash page, follow the suggestion that appears on screen.

If the BACnet IoT Gateway cannot reach the SMC Cloud server, the following message will appear.

Register this FieldServer on SMC Cloud™

SMC Cloud™ Server Unreachable
The device is unable to connect to the SMC Cloud™ server.

The following network issues have been detected. Correcting them might resolve connectivity to the server:

- Domain Name Server 1 not configured
- Domain Name Server 2 not configured

Ensure your network firewall is configured to allow this device to access the SMC Cloud™ server:

- Device MAC address: 00:50:4E:60:06:3C
- Allow HTTPS communications to the following domains on port 443:
  - www.smccloud.net
  - ts.smccloud.net

Figure 57: SMC Cloud Connection Problems Message

- Follow the directions presented in the warning message and check that the DNS settings are set up with the following Domain Name Server (DNS) settings:
  
  DNS1=8.8.8.8
  
  DNS2=8.8.4.4

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

NOTE: If changes to the network settings are done, remember to click “Update IP Settings” and then power cycle the BACnet IoT Gateway.
On the registration page, click the “Create a SMC Cloud account” button and enter a valid email.

This will send a “Welcome to SMC Cloud” invite to the email address entered.
• The “Welcome to SMC Cloud” email will appear as shown below.

![Figure 59: Welcome to SMC Cloud Email]

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](image)

**Figure 60: 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.
8.2 Registration Process

Once SMC Cloud user credentials have been generated, the BACnet IoT Gateway can be registered onto the SMC Cloud server.

- On the registration page, fill in user credentials and all other device information fields for registration of each individual BACnet IoT Gateway in the field.

![Figure 61: Register the Gateway on SMC Cloud](image)

- To input the device location, do one of the following:
  - Enter the address in the address field
  - Click the “Get Current Location” button to auto-populate

**NOTE:** This button will only work if location services have been enabled on the local browser. If using the Chrome browser and connected via LAN, this method will not work.

  - Drop a location directly on the Google map
  - Enter the latitude and longitude manually

- Click Register Device.
Once the device has successfully been registered, the following screen will appear listing the device details and additional information auto-populated by the BACnet IoT Gateway.

![Device Registered](image)

**Figure 62: Device Registered for SMC Cloud™**
8.3 Login to SMC Cloud

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

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.
NOTE: For additional SMC Cloud instructions see the [SMC Cloud Start-up Guide](#).
9 INTEGRATING WITH THE THINGWORX PLATFORM

9.1 ThingWorx General Overview

MSA Safety’s BACnet IoT Gateway with ThingWorx Adapter provides a connection path between field devices and the ThingWorx cloud. ThingWorx is an enterprise-ready technology platform that enables innovators to develop and deploy smart, connected solutions for the Industrial Internet of Things (IIoT).

ThingWorx is an object oriented platform which allows the integrator to define re-usable components and then use those components to define “Things”, which represent real world devices. “ThingTemplates” contain pre-defined properties which are inherited into every Thing Instance created from the template.

<table>
<thead>
<tr>
<th>FieldServer</th>
<th>ThingWorx</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile</td>
<td>ThingTemplate</td>
<td>Provides base functionality, including properties for the device.</td>
</tr>
<tr>
<td>Profile Instance</td>
<td>Thing</td>
<td>Modeled representation of a physical device that has properties.</td>
</tr>
<tr>
<td>Data Point</td>
<td>Thing Property</td>
<td>Representation of a parameter or variable in the device.</td>
</tr>
</tbody>
</table>

The diagrams below show how the FieldServer Profiles translate into Things (left) and the communications between the FieldServer and cloud applications (right).

Follow the sections below to seamlessly integrate any discovered and logged devices to the ThingWorx platform. The gateway allows easy configuration of devices and maps them into ThingWorx “things”.

9.2 Connect to ThingWorx

- After setup and initial configuration of the BACnet IoT Gateway is complete, click the Cloud Integrations tab.

- Then click the ThingWorx tab to open the ThingWorx page.

- Enter Authentication information gathered from the ThingWorx Platform into the ThingWorx Settings Window.
  - A key must be generated via ThingWorx

- Click Save to record the information and allow ThingWorx integration to your account.
9.3 Configure the Thing Settings on Discovered Devices

- Click the Thing Settings tab.

**NOTE:** Only devices that have been discovered via the BACnet Explorer function (Section 7.1), set to Monitor View (Section 7.2.1) and then configured to be logged (Section 7.2.2) will appear in the Thing Settings tab.

- Enter the Thing Name, Thing Template and Thing Description as needed.
  - Double click on a field to edit it
- Click the Save button.

**NOTE:** Until a new Thing has been configured and saved (see Thing Setting Status column), the corresponding data will not be sent to the ThingWorx Platform.
9.4 Check the Status Window

- On either ThingWorx page, scroll down from the Settings Window until the Status Window is visible.

![Status Window Image]

- The Connection Status Section shows the state of connection to the ThingWorx Server and ThingWorx REST Server with the date and time of connection listed.

- The Communication Stats Section lists the communication status of each Thing.
  - Click “View” under the Properties column to see a list of the properties for that Thing.

![Properties Image]
10 INTEGRATING WITH CISCO KINETIC

10.1 Cisco Kinetic General Overview

The MSA Safety BACnet IoT Gateway facilitates BACnet data to easily and securely be moved to the Cisco Kinetic Data Control Module (DCM). The DCM enforces policy by, both seamlessly and timelessly, moving data to the relevant apps attached to Cisco Kinetic.
10.2 Connect to Cisco Kinetic

- After setup and initial configuration of the BACnet IoT Gateway is complete, click the Cloud Integrations tab.
- Then click the Cisco Kinetic tab to open the Cisco Kinetic page.

- Enter Authentication Details gathered from the Cisco Kinetic Platform into the Connection Settings Window.
- Click Save to record the information and allow Cisco Kinetic integration to your account.
10.3 Check the Status Window

- Scroll down from the Settings Window until the Status Window is visible.

- The Connection Status Section shows the state of connection to the Kinetic Server with the date and time of connection listed.
- The Communication Stats Section lists the communication statistics of the connected devices.
- The Device List Summary lists the device instances and the last time they were updated.
### Available Ports
- One 3-pin Phoenix connector with:
  - RS-485/RS-232 port (TX+ / RX- / gnd)
- One 3-pin Phoenix connector with:
  - Power port (+ / - / Frame-gnd)
- One Ethernet 10/100 BaseT port

**BAC/BACW Power Requirements**
- Input Voltage: 9-30VDC or 24VAC
- Max Power: 3 Watts
- Current draw: 24VAC 0.125A
- 9-30VDC 0.25A @12VDC

**BACC Power Requirements**
- Input Voltage: 12-24V DC
- Power Rating: 8 Watts
- Current draw: @ 12V, 0.67A

### Approvals
- CE and FCC Class B & C Part 15, UL 60950-1 TUV approved, UL 916 approved, IC Canada, RoHS Compliant, PTCRB and CTIA

### Dimensions (WxDxH)
- 4 x 1.1 x 2.7 in (10.16 x 2.8 x 6.8 cm)

### Weight
- 0.4 lbs (0.2 Kg)

### Operating Temperature
- -20 to 70°C (-4 to 158°F)

### Humidity
- 10-95% RH non-condensing

### Wi-Fi 802.11 b/g/n
- Frequency: 2.4 GHz
- Antenna Type: SMA
- Channels: 1 to 11 (inclusive)
- Encryption: TKIP, WPA & AES

### Cellular
- Features: 3G & GPS
- HSUPA: Up to 21.0 Mbps
- IMEI: 357178070517852
- Antenna Type: SMA
- HSUPA: Up to 5.76 Mbps

---

**Figure 66: Specifications**

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

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

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

Modifications not expressly approved by MSA Safety could void the user's authority to operate the equipment under FCC rules."
Appendix B.1. Understanding FDR

The BACnet IoT Gateway doesn't allow FDR, local IP and BACnet MS/TP to co-exist because there is no guarantee that two distinct BACnet networks will have unique Device Instances or Network Numbers. (Unique Device Instances and Network Numbers are a requirement for BACnet to function properly). If local and remote options were allowed concurrently, the BACnet IoT Gateway would connect two networks that are probably not designed to work together. Forcing this situation would create extremely difficult to diagnose problems.

Appendix B.2. Understanding BACnet BBMD and NAT Routing

The BACnet IoT Gateway does not support NAT routing. However, the BACnet IoT Gateway must have the external IP Address and IP Port that the NAT router assigns to it, because these are inserted into the BACnet/IP BVLC header as the source IP Address which a remote recipient can use to reach the BBMD (BACnet Broadcast Management Device). This is necessary because the messages are distributed again by a remote BBMD, and the remote recipient of a distributed broadcast needs to reach the originator of the broadcast.

Figure 67: BBMD Scenario 1 – Interconnected IP Network
With NAT Routing, BBMD alone does not work because the Devices cannot reach each other’s IP Addresses even if they know them. The only reachable address is the BBMD itself, so this must also act as a BACnet IoT Gateway to forward traffic to the intended device. When this is done, the destination device’s IP Address and Port are encoded as the DADR in the network header, so that the Router can forward messages to the correct device.

**Figure 68: BBMD Scenario 2 – NAT Routing**
APPENDIX C TROUBLESHOOTING

Appendix C.1. Communicating with the BACnet IoT Gateway Over the Network

- Confirm that the network cabling is correct.
- Confirm that the computer network card is operational and correctly configured.
- Confirm that there is an Ethernet adapter installed in the PC’s Device Manager List, and that it is configured to run the TCP/IP protocol.
- Check that the IP netmask of the PC matches the BACnet IoT Gateway. The Default IP Address of the BACnet IoT Gateway is 192.168.2.101, Subnet Mask is 255.255.255.0.
  - Go to Start|Run
  - Type in “ipconfig”
  - The account settings should be displayed.
  - Ensure that the IP Address is 192.168.1.X and the netmask 255.255.255.0
- Ensure that the PC and BACnet IoT Gateway are on the same IP Network, or assign a Static IP Address to the PC on the 192.168.1.X network.
Appendix C.2. Lost or Incorrect IP Address

- 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.

![](image)

- Connect a standard Cat-5 Ethernet cable between the user’s PC and BACnet IoT Gateway.
- Double click on the FS Toolbox Utility and click Discover Now on the splash page.
- Check for the IP Address of the desired gateway.

![](image)

- If correcting the IP Address of the gateway: click the settings icon on the same row as the gateway, then click Network Settings, change the IP Address and click Update IP Settings to save.
Appendix C.3. Viewing Diagnostic Information

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

NOTE: If there are any errors showing on the Connection page, refer to Appendix C.4 for the relevant wiring and settings.

Appendix C.4. Checking Wiring and Settings

No COMS on the Serial side. If the Tx/Rx LEDs are not flashing rapidly then there is a COM issue. To fix this problem, check the following:

- Visual observations of LEDs on the BACnet IoT Gateway (Appendix C.5)
- Check baud rate, parity, data bits, stop bits
- Check Serial device address
- Verify wiring
- Verify device is connected to the same subnet as the BACnet IoT Gateway

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

- Visual observations of LEDs on the BACnet IoT Gateway (Appendix C.5)
- Check device address
- Verify wiring
- Verify device is connected to the same subnet as the BACnet IoT Gateway
- Verify IP Address setting

NOTE: If the problem still exists, a Diagnostic Capture needs to be taken and sent to support. (Appendix C.6)
Appendix C.5. LED Diagnostics for Communications Between BACnet IoT Gateway and Devices

See the diagram below for BACnet IoT Gateway LED locations.

<table>
<thead>
<tr>
<th>Tag</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SS</td>
<td>The SS LED will flash once a second to indicate that the bridge is in operation.</td>
</tr>
<tr>
<td>ERR</td>
<td>The SYS ERR LED will go on solid indicating there is a system error on unit. If this occurs, immediately report the related “system error” shown on the error screen of the FS-GUI to support for evaluation.</td>
</tr>
<tr>
<td>PWR</td>
<td>The power light should always show steady green when connected to a functioning power source.</td>
</tr>
<tr>
<td>RX</td>
<td>The RX LED will flash when a message is received on the serial port on the 3-pin connector. <strong>If the serial port is not used, this LED is non-operational.</strong> For FS-IOT-BAC/BACW, RX1 applies to the R1 connection while RX2 applies to the R2 connection.</td>
</tr>
<tr>
<td>TX</td>
<td>The TX LED will flash when a message is sent on the serial port on the 3-pin connector. <strong>If the serial port is not used, this LED is non-operational.</strong> For FS-IOT-BAC/BACW, TX1 applies to the R1 connection while TX2 applies to the R2 connection.</td>
</tr>
</tbody>
</table>

*Figure 71: Diagnostic LEDs*
Appendix C.6. Before Contacting Technical Support Take a Diagnostic Capture

When a problem occurs that cannot be resolved with regular troubleshooting, take a log via the FieldServer FS-GUI. Send this log together with a detailed description of the problem to technical support for evaluation. 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.
- 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 C.7. Updating Firmware

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

1. Extract and save the new file onto the local PC.
2. Open a web browser and type the IP Address of the FieldServer in the address bar.
   o Default IP Address is 192.168.2.101
   o Use the FS Toolbox utility if the IP Address is unknown (Appendix C.2)
3. Click on the “Diagnostics & Debugging” button.
4. In the Navigation Tree on the left-hand side, do the following:
   a. Click on “Setup”
   b. Click on “File Transfer”
   c. Click on the “General” tab
5. In the General tab, click on “Choose Files” and select the firmware file extracted in step 1.
6. Click on the orange “Submit” button.
7. When the download is complete, click on the “System Restart” button.
Appendix C.8. Securing BACnet IoT Gateway with Passwords

Access to the BACnet IoT Gateway 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 BACnet IoT Gateway.
- The User account can view any BACnet IoT Gateway information but cannot make any changes or restart the BACnet IoT Gateway.

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 smc-support.emea@msasafety.com to receive a temporary password from the support team. Access the BACnet IoT Gateway to set a new password.

Figure 72: FS-GUI Passwords Page

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: zMtvwSdf4A—

LOGIN
www.sierramonitor.com

Figure 73: Password Recovery Page
Appendix C.9. Kaspersky Endpoint Security 10

If Kaspersky Endpoint Security 10 is installed on the user’s PC, the software needs to be modified to allow the PC to register bridges on SMC Cloud.

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

To fix the problem, the BACnet IoT Gateway (http://192.168.100.85/ in Figure 75) must be set as a trusted URL to the "Web Anti-Virus"->"Settings" as shown below.
Appendix C.10. Wi-Fi and Cellular Signal Strength

<table>
<thead>
<tr>
<th>Wi-Fi</th>
<th>Cellular</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;60dBm</td>
<td>&lt;60dBm – Excellent</td>
</tr>
<tr>
<td>&lt;70dBm</td>
<td>&lt;70dBm – Very good</td>
</tr>
<tr>
<td>&lt;80dBm</td>
<td>&lt;80dBm – Good</td>
</tr>
<tr>
<td>&gt;80dBm</td>
<td>&lt;90dBm – Weak</td>
</tr>
<tr>
<td>&gt;90dBm</td>
<td>&gt;90dBm – Spotty; not good for data</td>
</tr>
</tbody>
</table>

*Figure 76: Wi-Fi & Cellular Signal Strength Listing*

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

Appendix C.11. Factory Reset Instructions

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

Appendix C.12. Internet Browsers Not Supported

- Internet Explorer

NOTE: Internet Explorer is no longer supported as recommended by Microsoft. Please use the latest version of Chrome, Firefox or Edge.
APPENDIX D 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.