FieldServer – EZ Gateway

KNX to BACnet Start-up Guide

FS-EZX-KNX-BAC

APPLICABILITY & EFFECTIVITY

Effective for all systems manufactured after August 2020.

Document Revision: 7.H
T18605

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

LIST OF FIGURES

1 ABOUT THE EZ GATEWAY

EZ Gateway is a high performance, cost effective Building and Industrial Automation multi-protocol gateway providing protocol translation between serial and Ethernet, devices and networks.

NOTE: For troubleshooting assistance refer to Appendix A, or any of the troubleshooting appendices in the related driver supplements. Check the Sierra Monitor website for technical support resources and documentation that may be of assistance.

The EZ Gateway is cloud ready and connects with MSA Safety's SMC Cloud. See **Section 7.10.1** for further information.

2 CERTIFICATION

2.1 BTL Mark – BACnet Testing Laboratory[1]

The BTL Mark on the EZ Gateway is a symbol that indicates that a product has passed a series of rigorous tests conducted by an independent laboratory which verifies that the product correctly implements the BACnet features claimed in the listing. The mark is a symbol of a high-quality BACnet product.

Go to www.BACnetInternational.net for more information about the BACnet Testing Laboratory. Click here for the BACnet PIC Statement.

3 SUPPLIED EQUIPMENT

EZ Gateway

- Preloaded with the KNX and BACnet drivers.
- All instruction manuals, driver manuals, support utilities are available on the USB drive provided in the optional accessory kit, or on the Sierra Monitor website.

Accessory kit (optional) (Part # FS-8915-36-QS) includes:

- 7-ft Cat-5 cable with RJ45 connectors at both ends
- Power Supply -110/220V (p/n 69196)
- DIN Rail mounting bracket
- Screwdriver for connecting to terminals
- USB Flash drive loaded with:
  - KNX to BACnet Start-up Guide
  - FieldServer Configuration Manual
  - All FieldServer Driver Manuals
  - Support Utilities
  - Any additional folders related to special files configured for a specific EZ Gateway
  - Additional components as required - See Driver Manual Supplement for details

[1] BACnet is a registered trademark of ASHRAE.

4 INSTALLING THE EZ GATEWAY

4.1 Mounting

The following mounting options are available:

- Product comes with tabs for wall or surface mount. These can be snapped off if not required.
- DIN Rail Mounting Bracket – included in the accessory kit or ordered separately (part# FS-8915-35-QS).

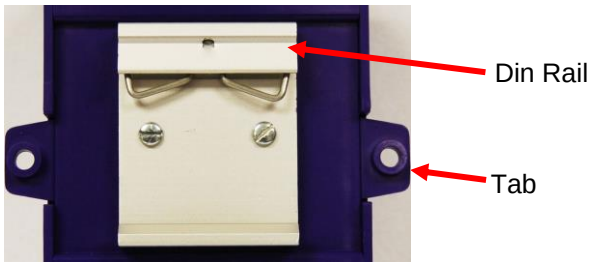


Figure 1: DIN Rail

WARNING: Install only as instructed, failure to follow the installation guidelines or using screws without the DIN rail mounting bracket could result in permanent damage to the product. If the FieldServer is removed from the DIN rail, use the original screws to reattach. Only screws supplied by MSA Safety should be used in the holes found on the back of the unit when attaching the optional DIN rail bracket. USE OF ANY OTHER SCREWS MAY DAMAGE THE UNIT.

NOTE: For dimension details see Appendix B.4.

4.2 KNX Connections

4.2.1 KNX Connection R2 Port

Connect to the 3 pins on the left side of the 6-pin connector as shown (pins labelled 6-4).

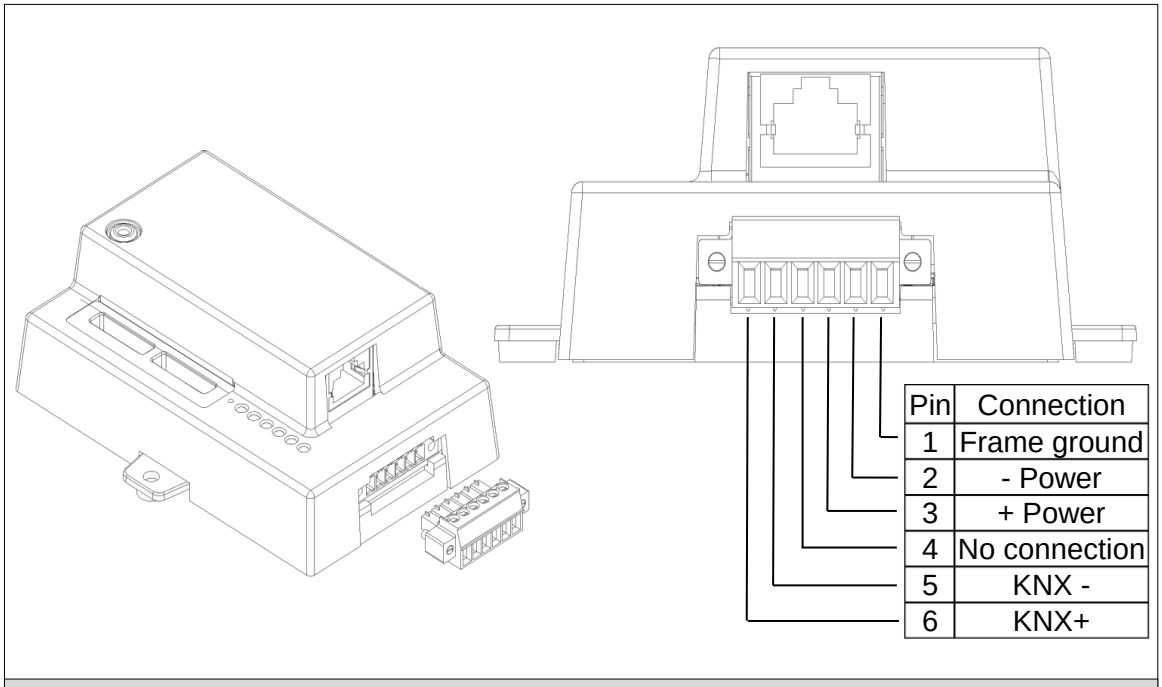


Figure 2: R2 Port Connection

4.2.2 RS-485 Connection R1 Port

Connect to the 3-pin connector as shown.

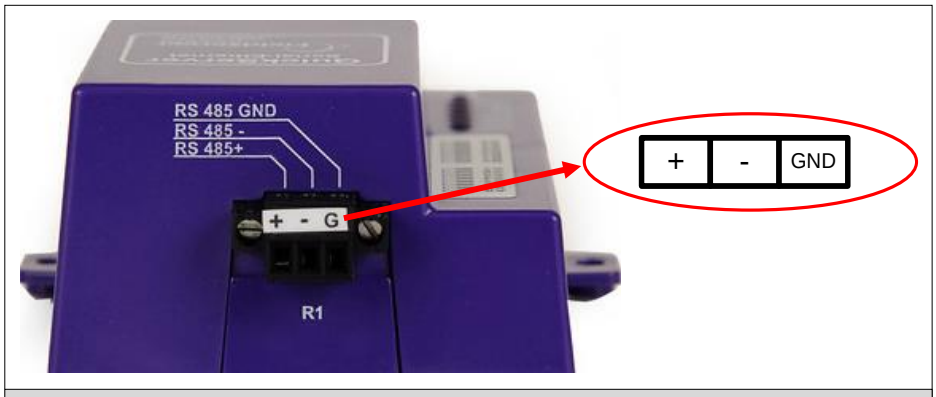


Figure 3: R1 Port Connection

The following baud rates are supported on the R1 Port for BACnet MS/TP:
9600, 19200, 38400, 76800

4.3 R1 Port Small DIP Switches

Gently remove the FieldServer enclosure to access the small DIP switches for the R1 Port.

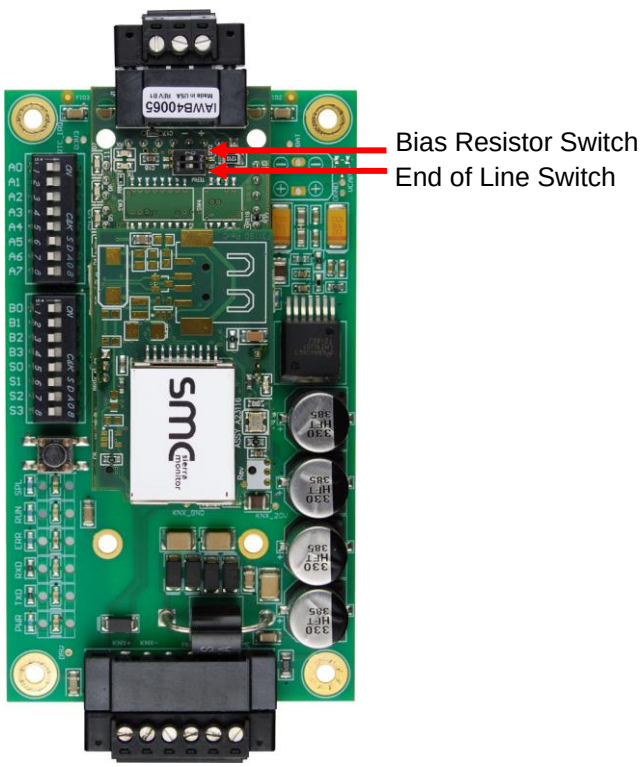


Figure 4: Bias Resistor DIP Switches & EOL

- If more than one RS-485 device is connected to the network, then the field bias resistor switch needs to be enabled to ensure proper communication. **See Figure 4 for the orientation of switch positions referenced below.**
  - The default factory setting is OFF (switch position = right side)
  - To enable biasing, turn the bias switch ON (switch position = left side)

NOTE: Biasing only needs to be enabled on one device. The FieldServer has 510 ohm resistors that are used to set the biasing.

- If the FieldServer is the last device on the trunk, then the end of line (EOL) termination switch needs to be enabled. **See Figure 4 for the orientation of switch positions referenced below.**
  - The default factory setting is OFF (switch position = right side)
  - To enable the EOL termination, turn the EOL switch ON (switch position = left side)

5 OPERATION

5.1 Power Up the Device

Apply power to the device. Ensure the power supply complies with the specifications provided in **Appendix B.1**. Ensure the cable is grounded using the "Frame GND" terminal. The EZ Gateway requires a power supply that provides 9-30V DC or 12-24V AC.

NOTE: A KNX compatible power supply is required on the KNX network.

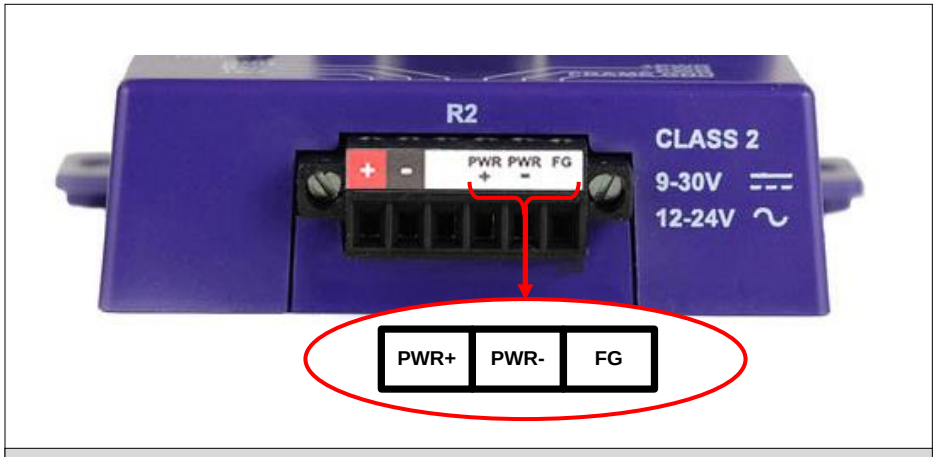


Figure 5: KNX Power Connection

5.2 Connect the PC to the EZ Gateway Over the Ethernet Port

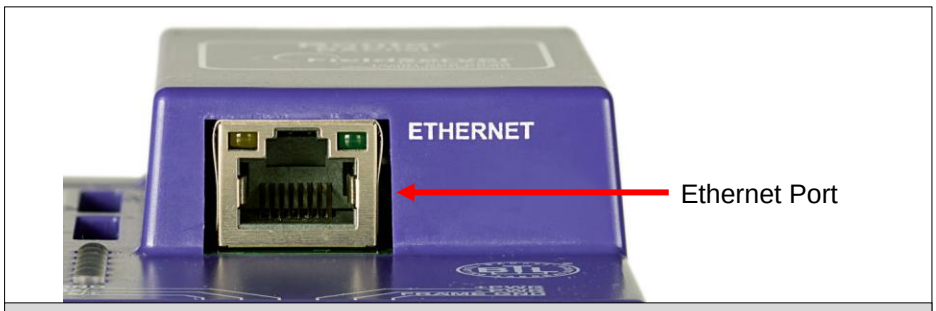


Figure 6: Ethernet Port

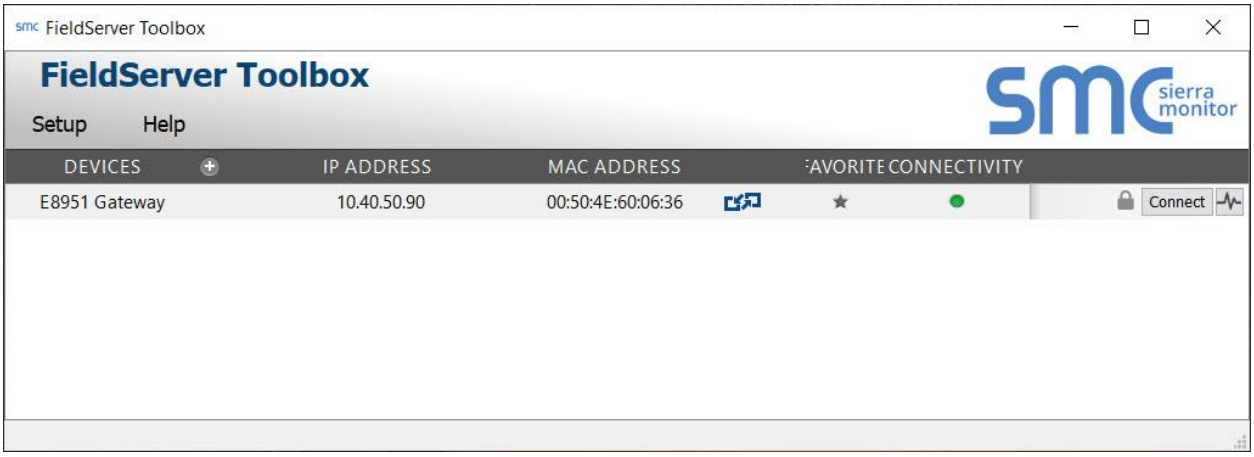
- Connect an Ethernet cable between the PC and EZ Gateway or connect the EZ Gateway and the PC to the Hub/switch using a straight Cat-5 cable.
- The Default IP Address of the EZ Gateway is **192.168.2.101**, Subnet Mask is **255.255.255.0**.

5.3 Connecting to the EZ Gateway

5.3.1 Using the FieldServer Toolbox to Discover and Connect to the EZ Gateway

- Install the FS Toolbox from the USB drive or download it from the Sierra Monitor website.
- Use FS Toolbox to find the EZ Gateway and launch the Web Configurator GUI.

NOTE: If the connect button is disabled, the EZ Gateway's IP Address must be set to be on the same network as the PC. (Section 6.3.2)



5.3.2 Using a Web Browser

- Open a web browser and connect to the EZ Gateway's default IP Address. The default IP Address of the EZ Gateway is **192.168.2.101**, Subnet Mask is **255.255.255.0**.
- If the PC and the EZ Gateway 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.

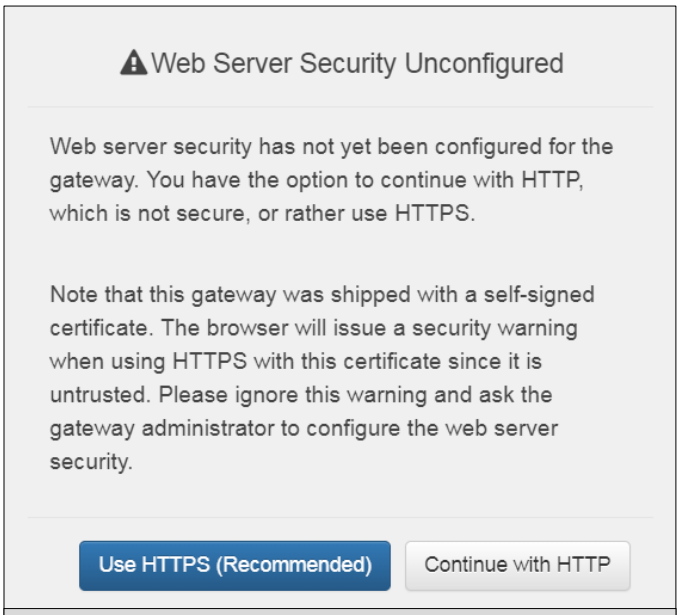


Figure 7: Web Server Security Unconfigured Window

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

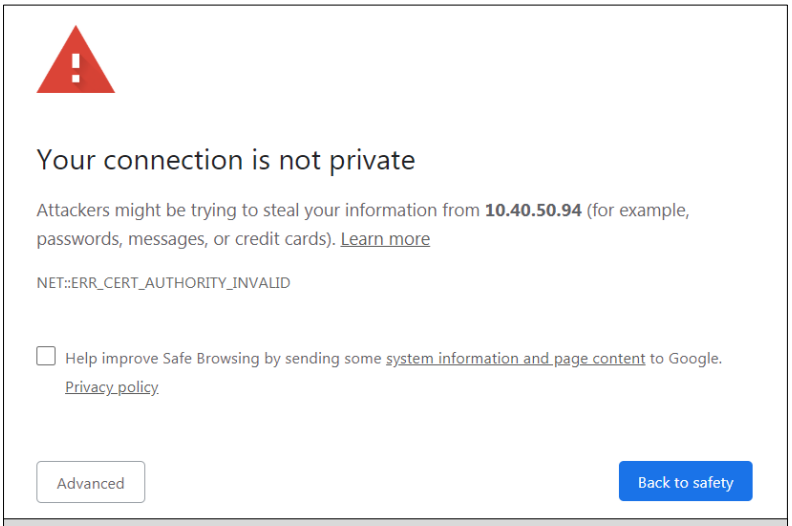


Figure 8: Connection Not Private Warning

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

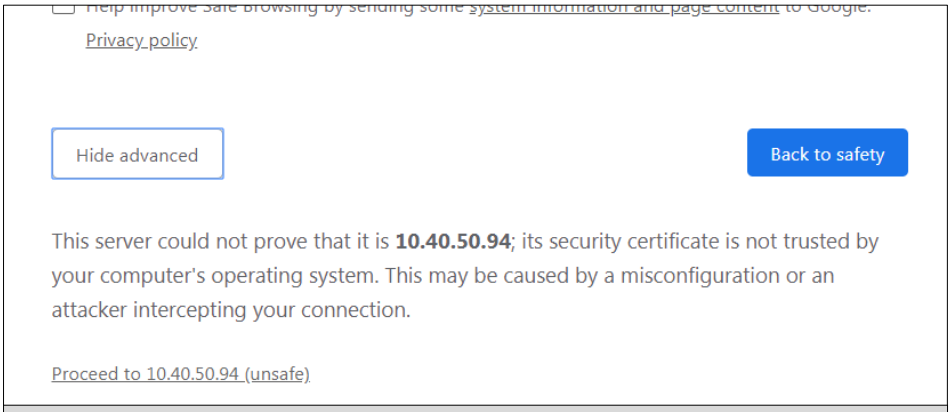


Figure 9: Warning Expanded Text

- When the login screen appears, put in the Username (default is "admin1991!") and the Password (found on the label of the FieldServer).

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

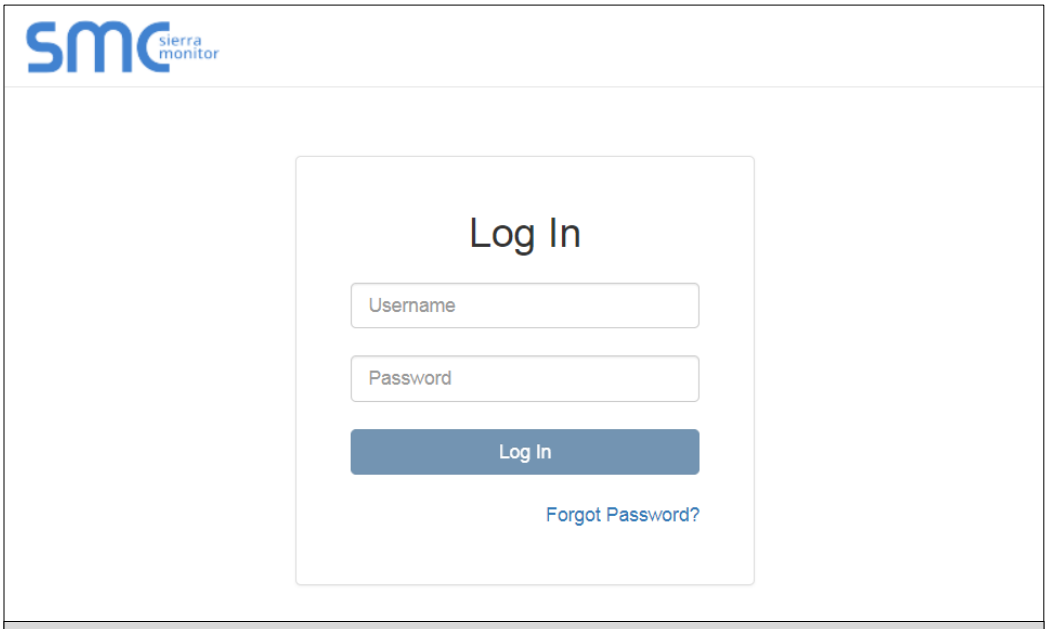


Figure 10: FieldServer Login

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.

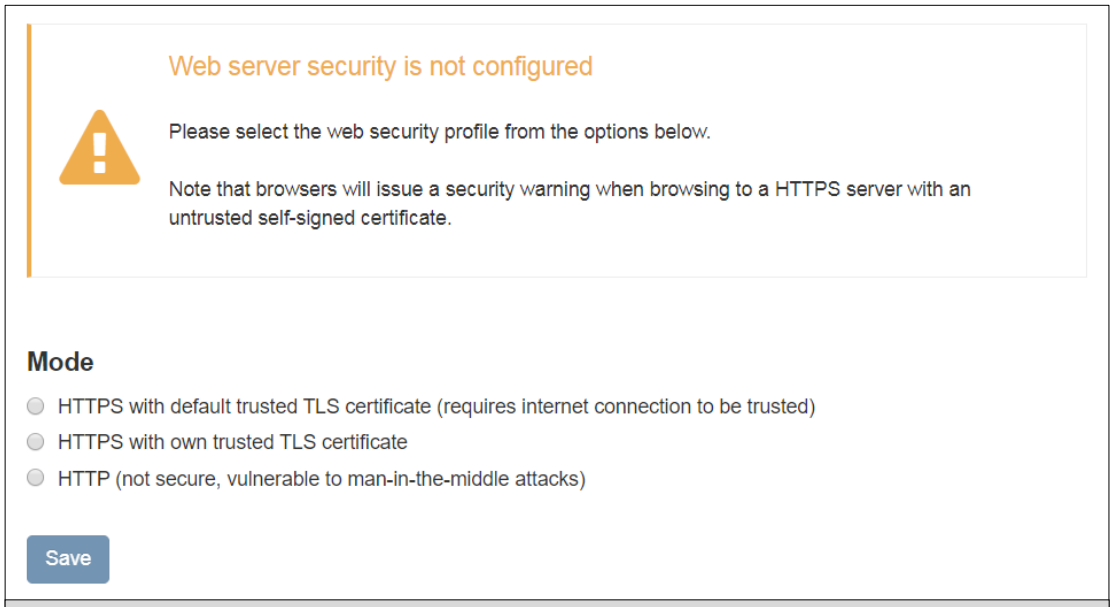


Figure 11: Security Mode Selection Screen

NOTE: Cookies are used for authentication.

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

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.

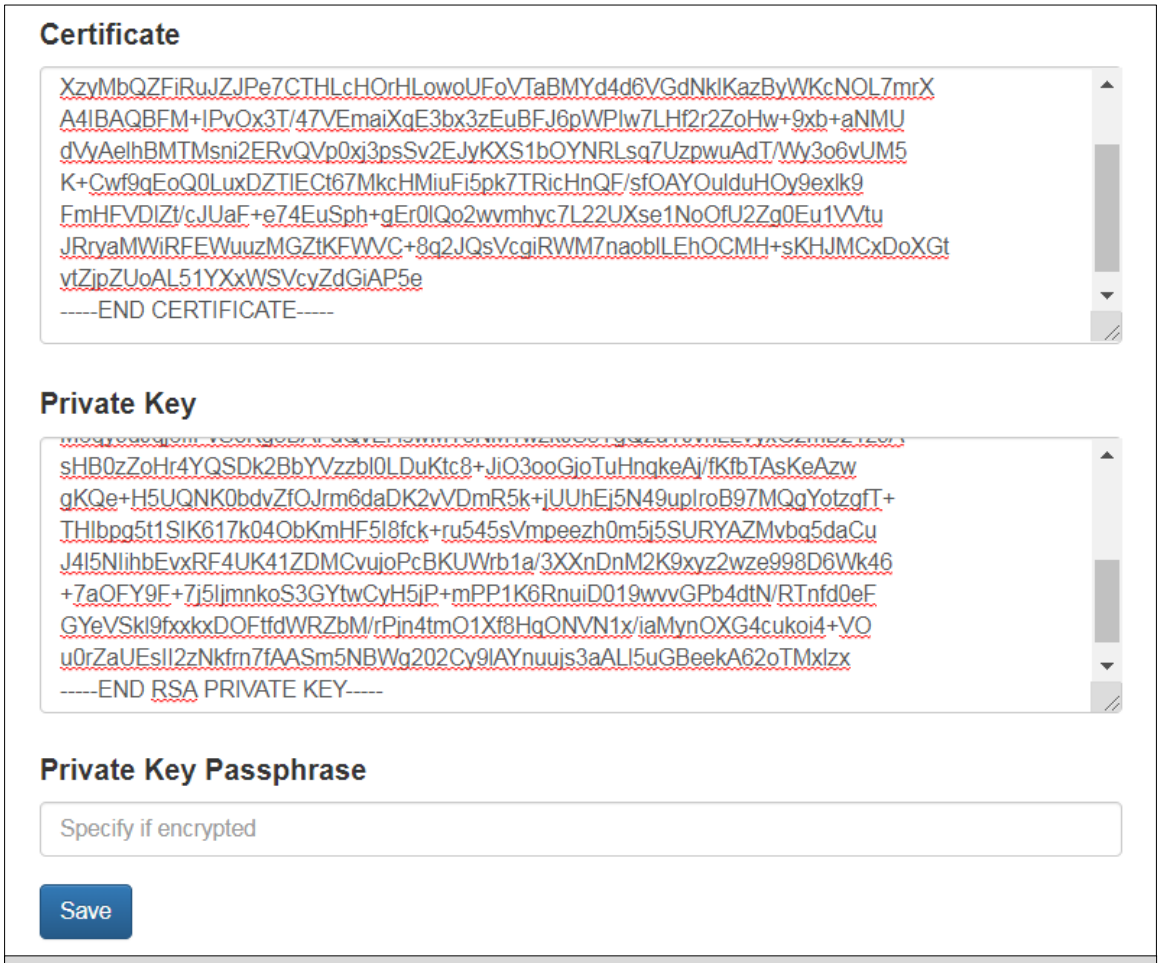


Figure 12: Security Mode Selection Screen – Certificate & Private Key

- 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 EZ GATEWAY

Once the web server setup is complete, the EZ Gateway landing page will appear.

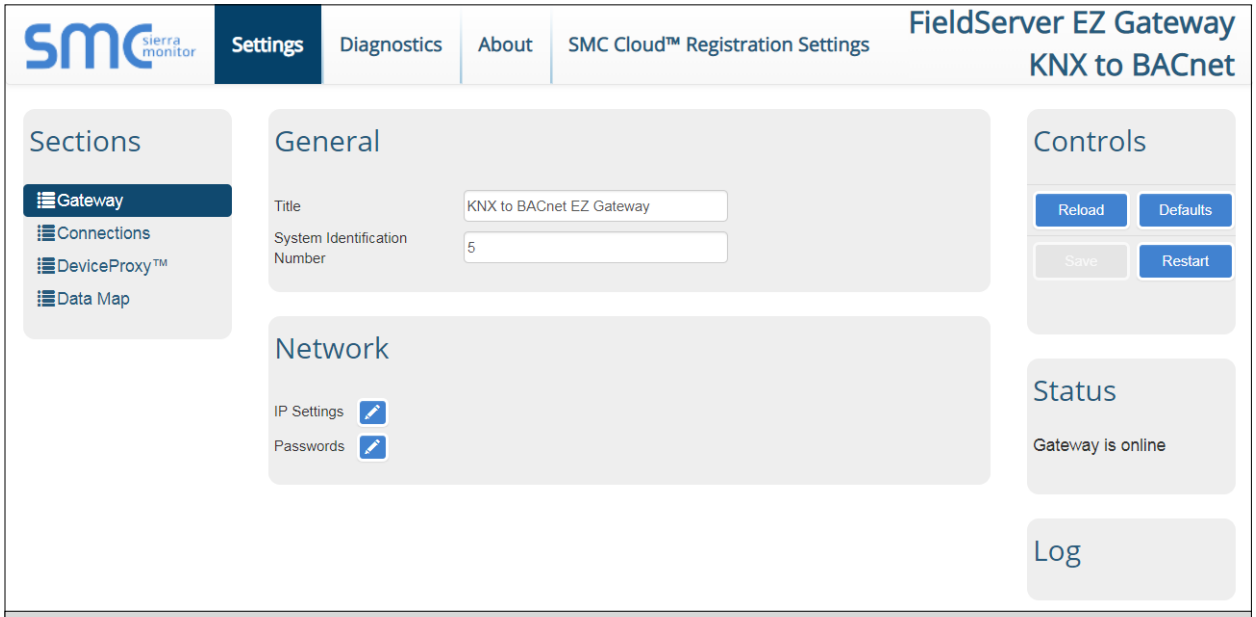


Figure 13: EZ Gateway Landing Page

NOTE: The SMC Cloud tab SMC Cloud™ (see Figure 13) 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 Controls, Status and Log Functions

Along the right side of every Web Configurator GUI page is a column of buttons and event generated messages.

- **Controls Panel** – Contains the following four buttons:
  - *Reload* – Resets all settings to the last saved configuration
  - *Defaults* – Resets all settings to the default configuration
  - *Save* – Records all settings
  - *Restart* – Reboots the Gateway
- **Status Information** – Shows Gateway messages such as whether the Gateway is online, element validation status, unsaved settings, etc.

  Log Messages – Lists last five events and when they were performed.

7.2 EZ Gateway Connection Setup

- Open the KNX EZ Gateway Web Configurator GUI in a local web browser (**Section 5.3.2**).

NOTE: The browser should open into the "Gateway" section, as shown in the Sections navigation map on the left side of the page (Figure 14). If navigating from another page in the Web Configurator GUI, click "Gateway" in the Sections navigation map.

- Specify the Gateway's Title and a System ID Number.
  - The System ID Number is a unique number to identify the EZ Gate way and is used as the default Device Instance if there are no nodes configured on the BACnet connection

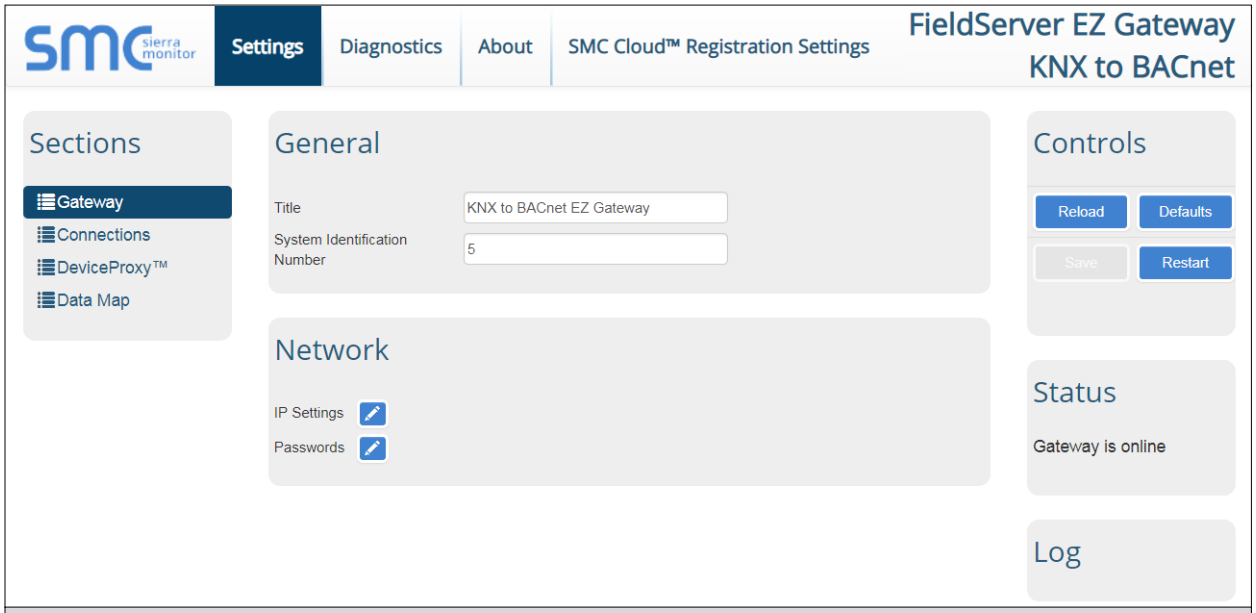
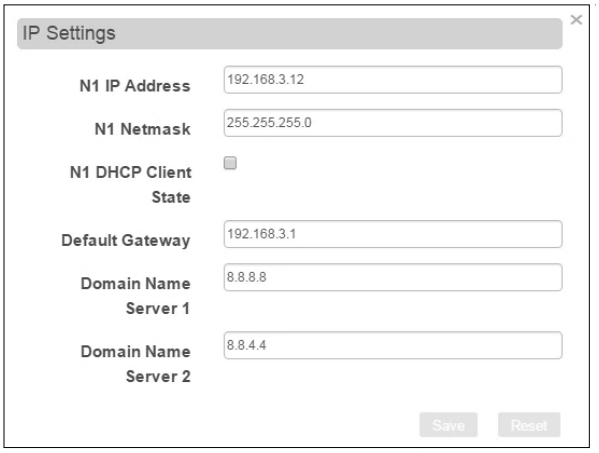


Figure 14: Gateway Network Settings

- Edit the IP Settings and Password Settings as needed by opening the respective settings windows via the edit buttons (pencil icons under "Network").



- Click Save button in the Controls Panel once edits are completed to record changes.

7.3 BACnet Connection Setup

- Click on the Enable checkbox under the 'BACnet/IP or BACnet MS/TP Connection' heading to configure the BACnet connections. The gateway has a BACnet MS/TP (R1) and BACnet/IP connection (N1).

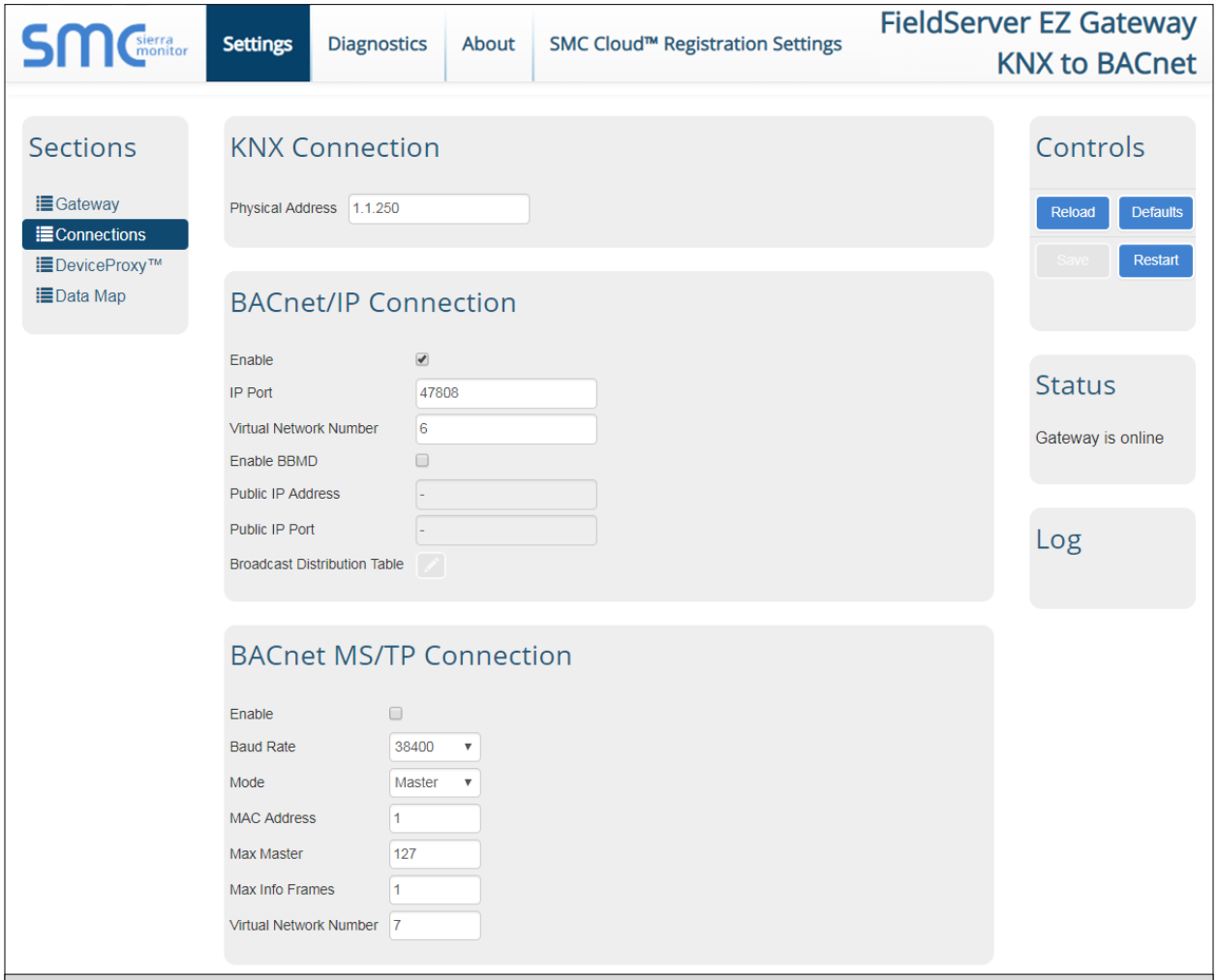


Figure 15: BACnet Connection Settings

- Enter the required BACnet/IP or BACnet MS/TP settings and **click the Save button in the Controls Panel once all edits are completed to record changes.**

7.3.1 All Connections Settings

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.

Enable – Enable or disable the connection.

7.3.2 BACnet/IP Connection Settings

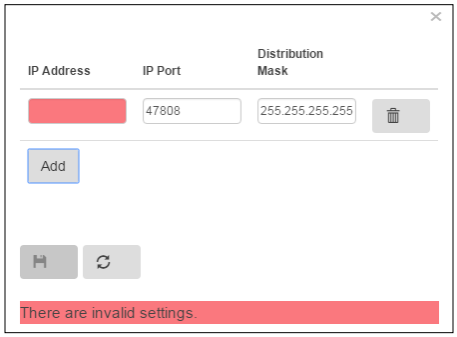
IP Port – The BACnet/IP default is 47808 (0xBAC0), but a different port may be specified.

Enable BBMD – Select this checkbox to enable the EZ Gateway to act as a BBMD.

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.

Broadcast Distribution Table – Click the edit button (pencil icon) to change the IP Address, IP Port and Distribution Mask. The following buttons are also available along the bottom of the window:

- Add Button - Add additional broadcasts, opening a new row of fields
- Save Button (floppy disk icon) - Save broadcast settings
- Reset Fields Button (cycle icon) - Clear fields



7.3.3 BACnet MS/TP Connection Settings

Baud Rate – The serial baud rate used on the network.

Mode – Select Master or Slave.

MAC Address – Legal values are 0 to 127. Address must be unique on the physical network.

Max Master – The highest MAC address to scan for other MSTP master devices. The default of 127 is guaranteed to discover all other MSTP master devices on the network.

Max Info Frames – The number of transactions the Router may initiate while it has the MSTP token. Default is 50.

7.4 BACnet Device Setup

- Click on the DeviceProxy™ section to configure the BACnet virtual nodes.

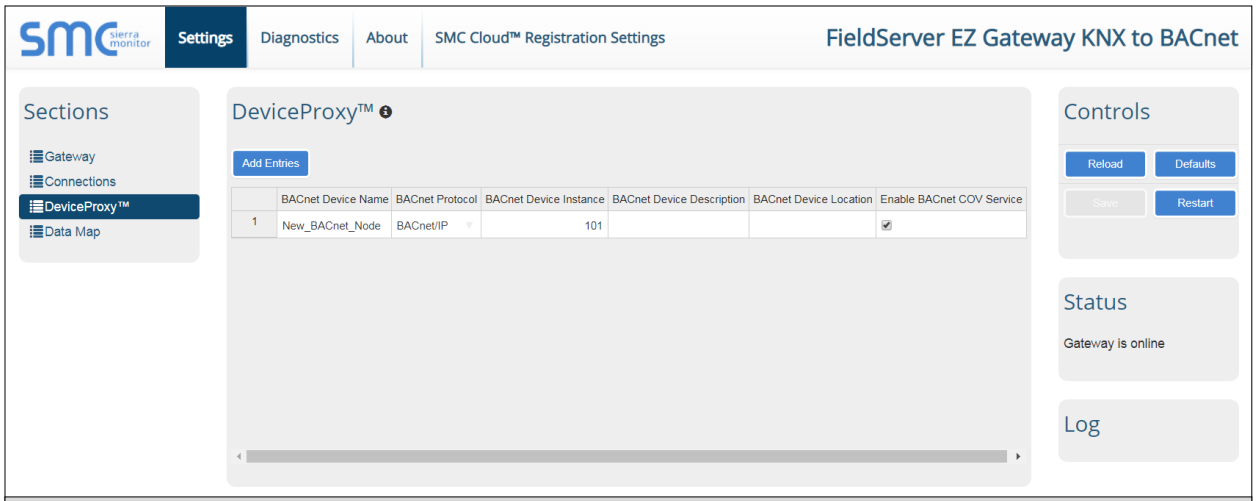


Figure 16: BACnet Device Settings

- Click the "Add Entries" button to reach the Add Node Map Entries window.

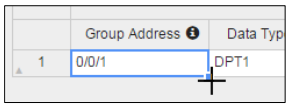
- Choose the number of devices to add and click the checkmark.
  - This will generate the requisite field inputs for each device
- Enter the appropriate information for each device.

NOTE: Click the ⓘ next to the DeviceProxy heading to see a list of all keyboard functions and shortcuts.

7.4.1 Table Editing Options

The DeviceProxy, Data Mapping and Notification tables allow special table editing options listed below:

- **Drag and drop** – When clicking on a field/cell in the table, a blue dot will appear in the bottom right corner of the field/cell. By scrolling over this dot, the arrow cursor will become a crosshair. By clicking this corner of the cell and dragging below the bottom of the table, additional rows are created. Release while highlighting cells below to populate with the same values as the originally highlighted cell.



- **Right click menu** – When right clicking on a field/cell, the following options will appear: inserting a row, removing a row, undo-ing the last edit and redo-ing the last undo.

7.5 KNX Network Mapping

There are two methods of mapping KNX Network to BACnet. ETS4 has the ability to export group addresses, which can then be imported into the KNX EZ Gateway (Section 7.5.1). The KNX mapping can also be set up manually in the Web Configurator GUI (Section 7.5.2).

7.5.1 KNX Mapping Method 1: Import Group Addresses

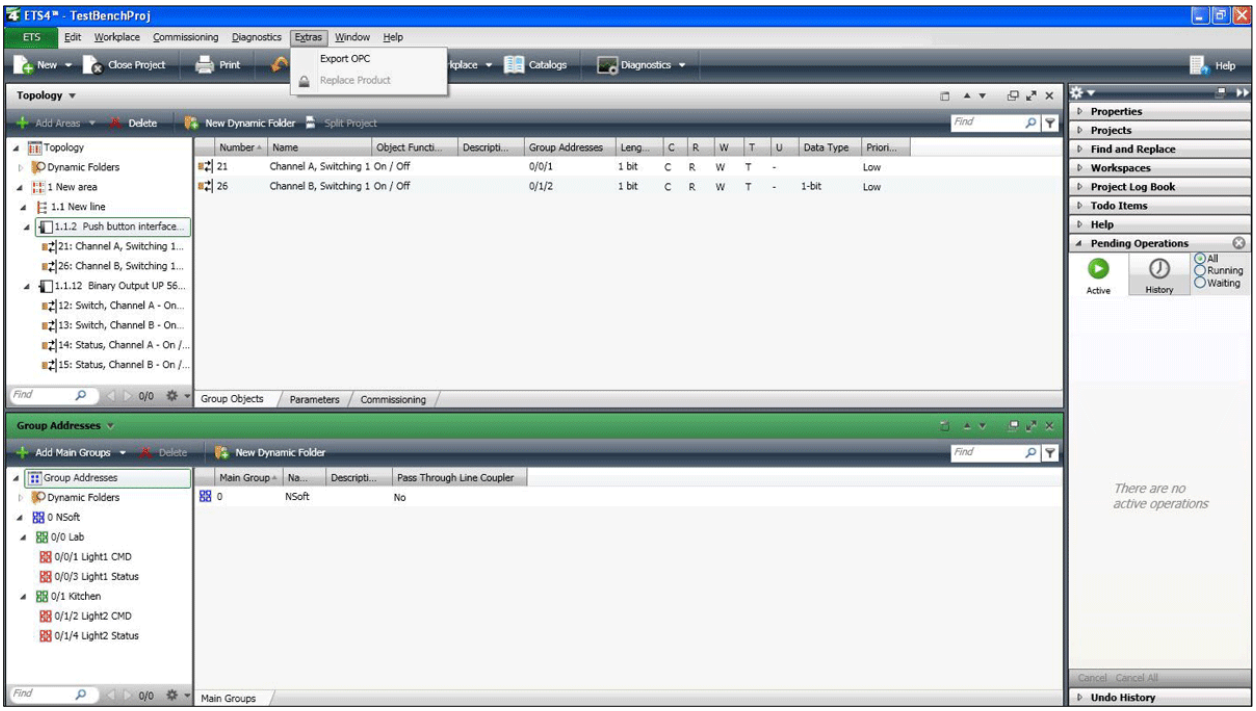
NOTE: This document assumes that a qualified ETS4 Operator will create the KNX Network in the ETS4 program. No direct instructions related to ETS4 (besides the file export instructions below) are present in this start up guide.

When the KNX Network is completed in ETS4, the group addresses can be exported. Follow the instructions below to complete this process.

NOTE: Both ESF and XML file types are supported for import by the EZ Gateway. However, ESF files are recommended as the saved data contains data type values while XML files do not.

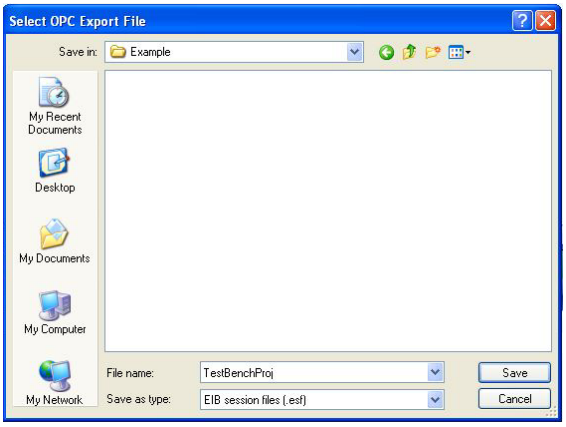
ESF File Export:

- In ETS, click the Extras drop down menu across the top of the page.



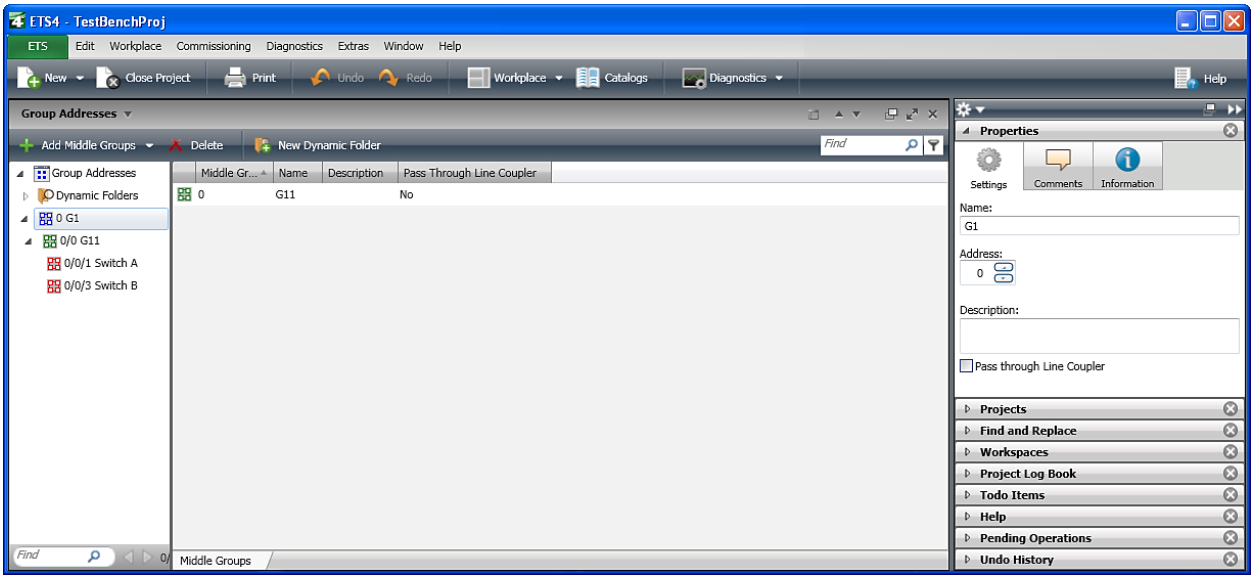
- Select “Export OPC”.

- Choose the location and name of the file then click Save.

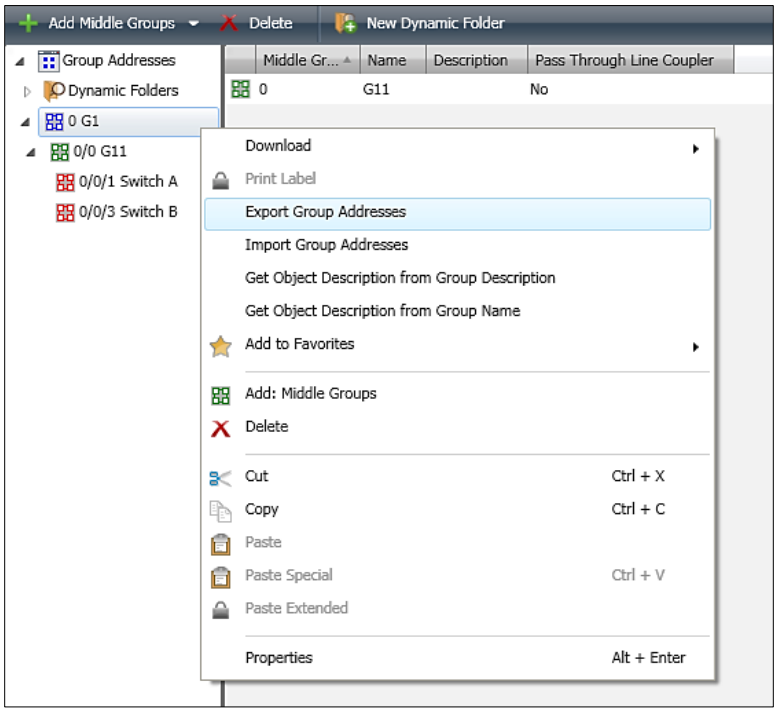


XML File Export:

- In ETS, select the Group Address window and navigate to the desired main group (at the highest level) to export all addresses contained within.



- Right-click on the main group and select “Export Group Addresses”.



- Select XML as the Output format type, enter the desired file location as well as file name in the Export file name field and save the file by clicking the “OK” button.

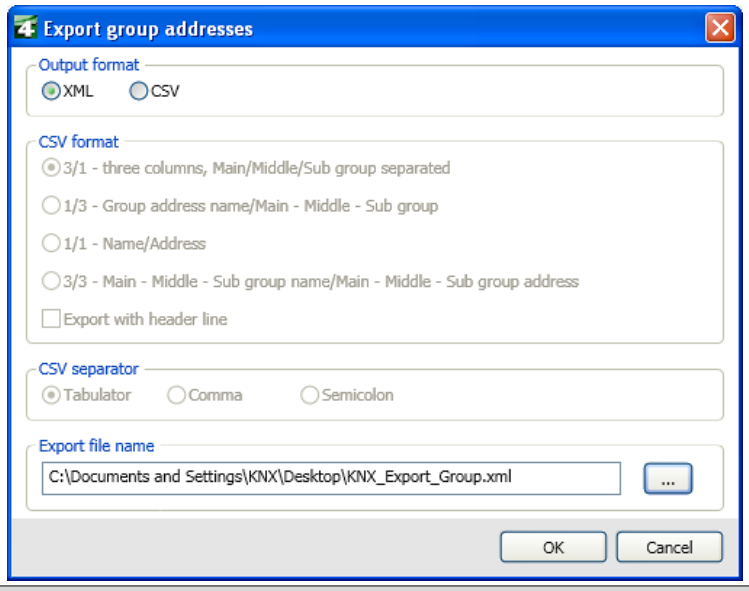


Figure 17: ETS4 Export Window

Import to EZ Gateway:

- Back on the Web Configurator GUI; click the “Data Map” section to configure the KNX to BACnet data point mapping.
- Click the “Import File” button to load the previously saved XML file.

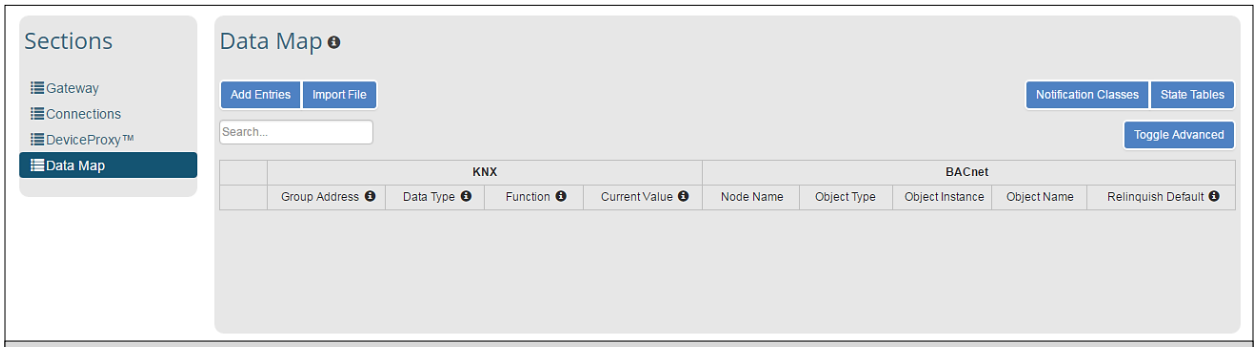
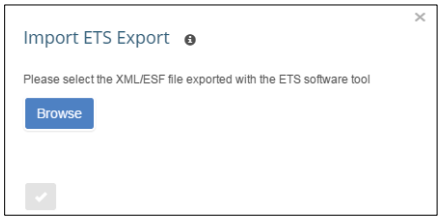


Figure 18: Data Map Page

- Click Browse to find and select the correct XML file.



- Click the checkmark to open the “Import ETS Export” window with the following import options:

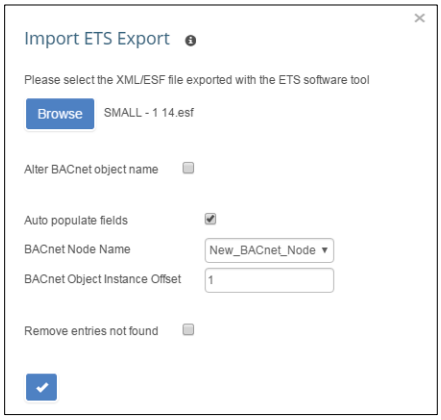
Alter the BACnet object name – Changes how the BACnet Object Name is generated by giving the option of inserting the group address, main group name and/or sub group name into the field.

Auto populate fields – Adds options to manipulate certain values generated for the imported data, specifically BACnet Node Name and BACnet Object Instance Offset.

BACnet Node Name – Select an already created BACnet Virtual Node to assign the imported data.

BACnet Object Instance Offset – Choose the starting number to assign BACnet Instances to the imported data.

Remove entries not found – Clears data map entries with group addresses not found in imported data.

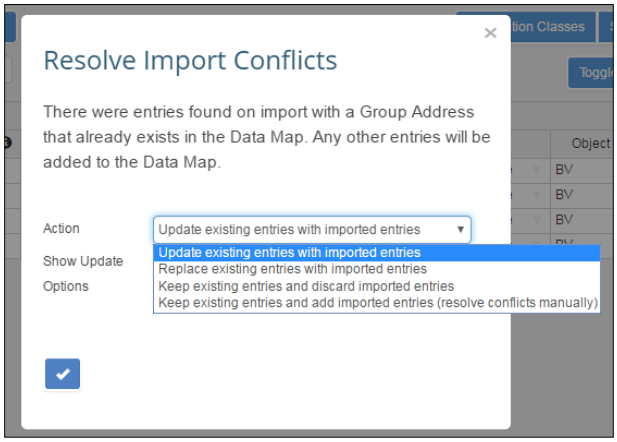


- Click the checkmark to confirm file selection and begin import.

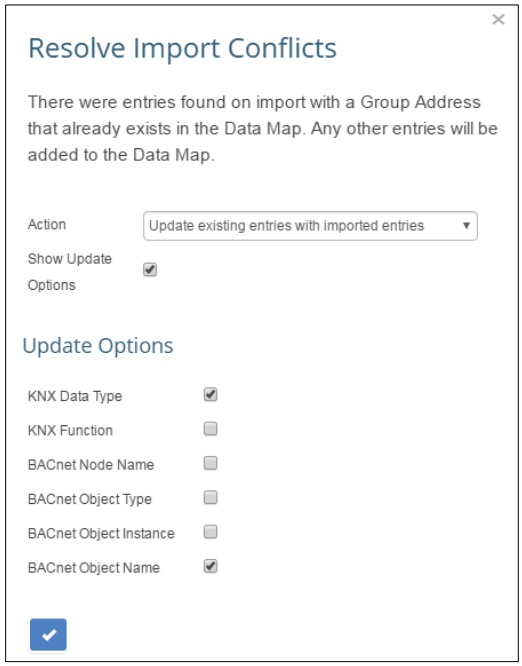
If there are problems with the import, one of two situations can occur.

Resolve Import Conflicts Window:

- If there are entries with the same group address on both the imported data and the existing data map the “Resolve Import Conflicts” window will appear



- Decide the appropriate action; if “Update existing entries with imported entries” is selected, the “Show Update Options” checkbox can be clicked to decide exactly which elements can be written over by the import

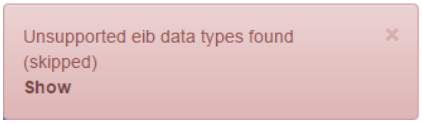


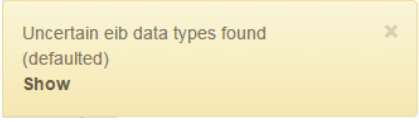
- Click the check mark in the bottom left corner of the window to begin import
- Once the XML file is imported, the data map screen will populate the appropriate group addresses and names

NOTE: If there are still conflicts, such as two entries on the same node using the same object instance, the offending fields are highlighted red and saving is unavailable until the conflict is resolved.

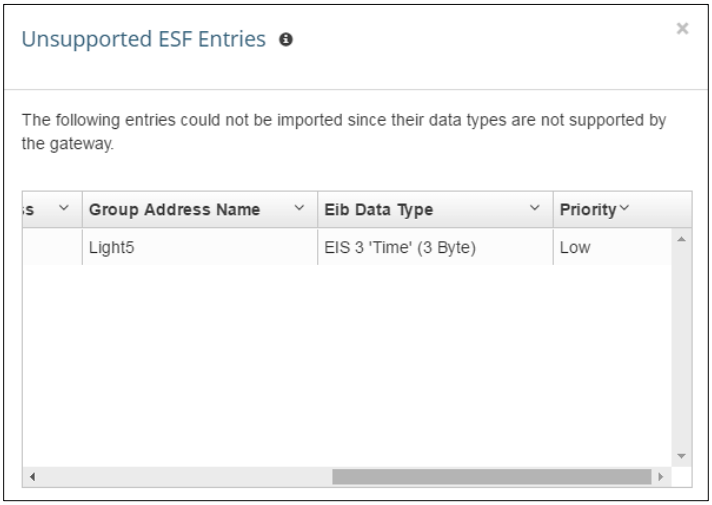
Unsupported or Uncertain eib Data Types Warning:

- If one or both of these warning pop-up messages appear after importing data, click the bolded “Show” text below the message



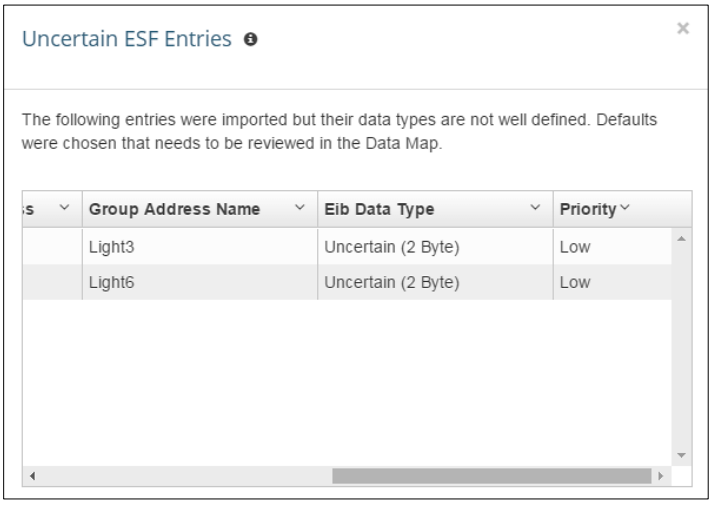


- The Unsupported ESF Entries Window lists which group addresses were not imported because the data type was not supported



NOTE: To fix an unsupported data type, the data type would have to be changed to a supported data type before exporting the KNX address data.

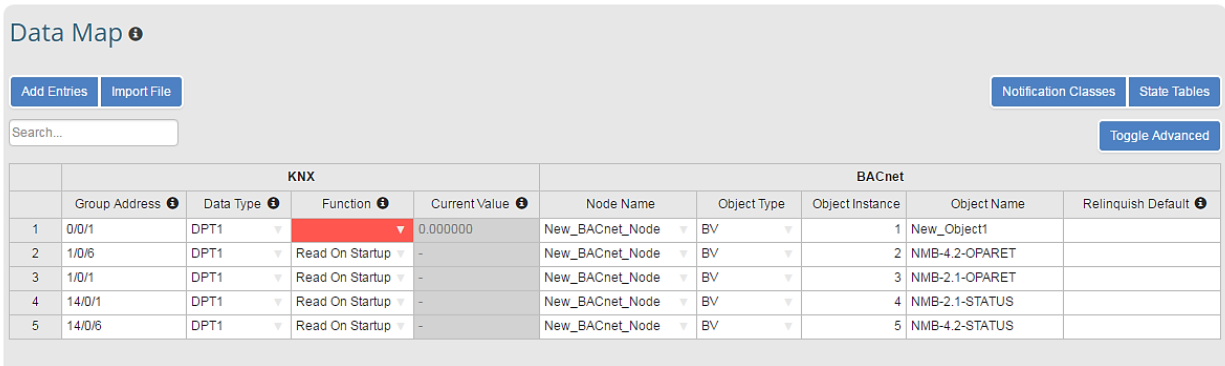
- On the other hand, the Uncertain ESF Entries Window shows which group addresses were imported with default data types because the data type was unclear



NOTE: Review the group address shown in the window and correct the data type if needed.

- Once review is complete, click the “X” in the upper right corner of the window and do the same to the original warning message to clear them from the screen

- After the import is complete the EZ Gateway will generate BACnet mapping data automatically, but if there are missing fields they must be defined for proper mapping (see **Section** 7.5.2 and **Section** 7.6 for additional information about KNX and BACnet fields).



	KNX				BACnet				
	Group Address	Data Type	Function	Current Value	Node Name	Object Type	Object Instance	Object Name	Relinquish Default
1	0/0/1	DPT1		0.000000	New_BACnet_Node	BV	1	New_Object1	
2	1/0/6	DPT1	Read On Startup	-	New_BACnet_Node	BV	2	NMB-4.2-OPARET	
3	1/0/1	DPT1	Read On Startup	-	New_BACnet_Node	BV	3	NMB-2.1-OPARET	
4	14/0/1	DPT1	Read On Startup	-	New_BACnet_Node	BV	4	NMB-2.1-STATUS	
5	14/0/6	DPT1	Read On Startup	-	New_BACnet_Node	BV	5	NMB-4.2-STATUS	

Figure 19: KNX Import Missing Fields

7.5.2 KNX Mapping Method 2: Setup on Web Configurator GUI

- In the Web Configurator GUI, click the “Data Map” section to configure the KNX data point mapping.

Figure 20: Mapping BACnet Addresses to the KNX Registers

- To bring in spreadsheet data, copy the appropriate cells and paste into the Data Map table.
  - The correct number of rows will automatically be added to the table
- Otherwise, click “Add Entries” and select the desired number of mappings (rows of the table).
  - For advanced table editing options, see **Section 7.6.1**

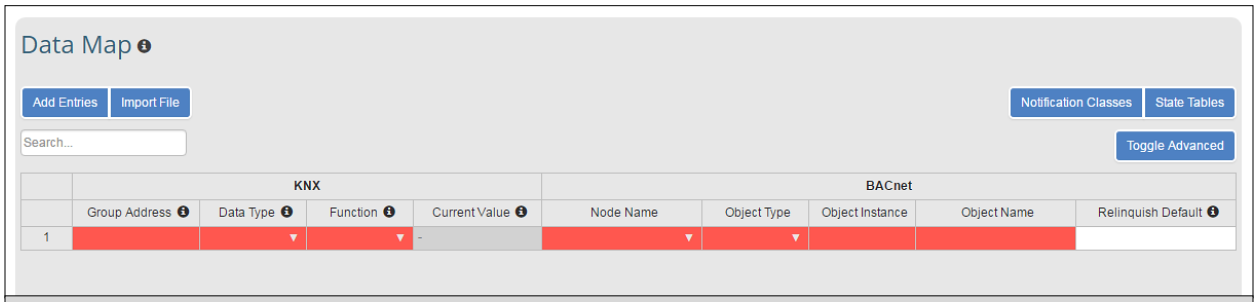


Figure 21: Creating an Item on the Data Map

- Fill in the necessary data entry fields under the KNX heading, including:
  - Group Address – KNX Group Address that will be served as a BACnet object
  - Data Type – The type of KNX data; click ⓘ to view a table describing the supported types (**Appendix B.3**)
  - Function – Read or write type; click ⓘ to view a table describing the supported types
  - Scan Interval – Seconds between poll requests; defaults at 2 if left blank

NOTE: Scan Interval is only available to edit when “Read Continuously” is selected in the function field.

  - Current Value – KNX data value read from ‘Group Address'
  - Write Group Address – Allows writing up to two KNX addresses from one BACnet object

NOTE: Click the Toggle Advanced button to see all KNX fields. Otherwise Scan Interval and Write Group Address will not appear.

NOTE: Certain fields show the information icon (ⓘ). Click on this icon to get additional information about the corresponding field.

7.6 BACnet Network Mapping

For every row of KNX parameters in the data map, a corresponding set of BACnet parameters must also be defined.

NOTE: Click Toggle Advanced button to see all BACnet fields. Otherwise some fields are hidden.

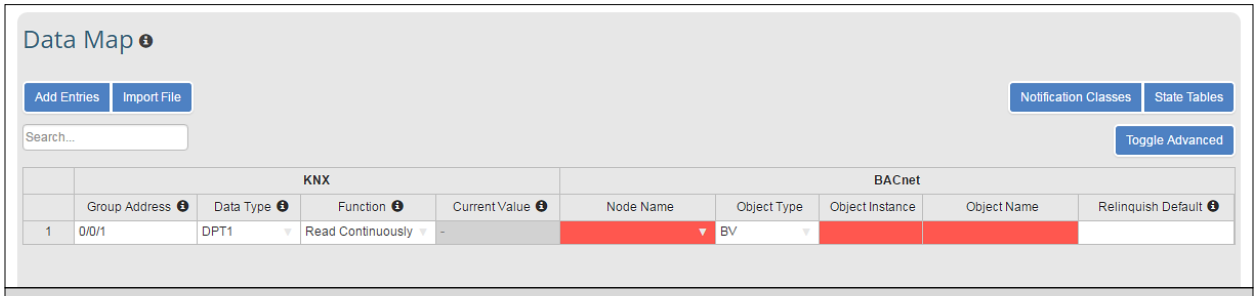


Figure 22: Mapping BACnet Fields

- Fill in the necessary data entry fields under the BACnet heading, including:
  - Node Name – Reference name for BACnet device
  - Object Type – Data structure for BACnet Object
  - Object Instance – Reference number for BACnet Object
  - Object Name – Name of each individual BACnet Object or point

NOTE: Certain fields show the information icon (ℹ). Click this icon to get additional informaiton on the corresponding field.

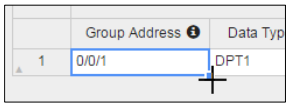
NOTE: Not all BACnet Fields are described in this manual. For additional information about any BACnet element, refer to the BACnet/IP or BACnet MS/TP driver manuals.

NOTE: Click the ℹ next to the Data Map heading to see a list of all keyboard functions.

7.6.1 Table Editing Options

The DeviceProxy™, Data Mapping and Notification tables allow special table editing options listed below:

- **Drag and drop** – When clicking on a field/cell in the table, a blue dot will appear in the bottom right corner of the field/cell. By scrolling over this dot, the arrow cursor will become a crosshair. By clicking this corner of the cell and dragging below the bottom of the table, additional rows are created. Release while highlighting cells below to populate with the same values as the originally highlighted cell.



- **Right click menu** – When right clicking on a field/cell the following menu will appear, allowing: inserting a row, removing a row, undo-ing the last edit and redo-ing the last undo.

NOTE: Click the ℹ next to the DeviceProxy and Data Map headings to see a list of all keyboard functions.

7.7 Alarm Settings

- Click the “Notification Classes” button to the upper right of the Data Map Table to enter the Notification Classes window.
- Fill in all fields.

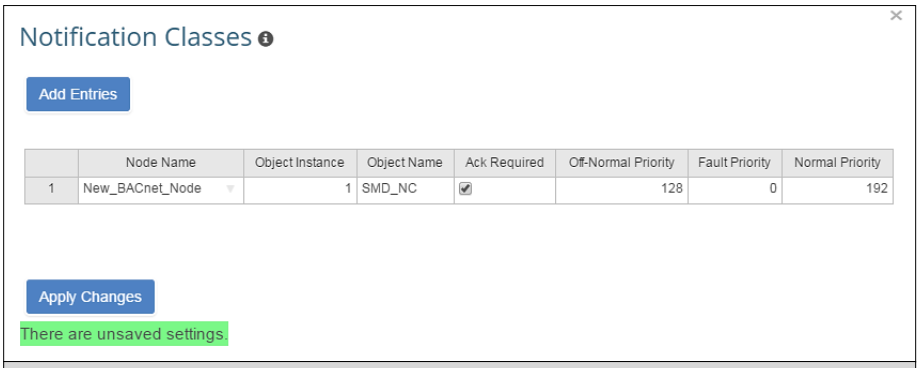


Figure 23: Defining Parameters of Notification Class

NOTE: Click the ℹ next to the Notification Classes heading to see a list of all keyboard functions and shortcuts.

- Click Apply Changes and click the “x” in the upper right corner to exit the window.
- Select Toggle Advanced button to make alarm elements visible.
- Fill in Notification Class, High Alarm, Low Alarm and Input Alarm State for each desired entry.

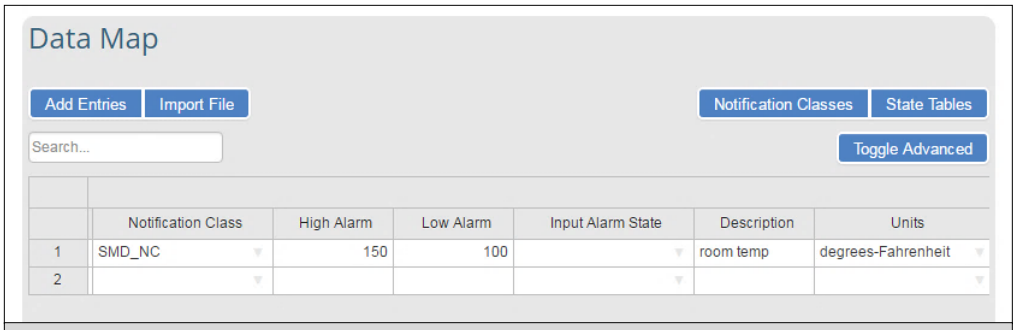


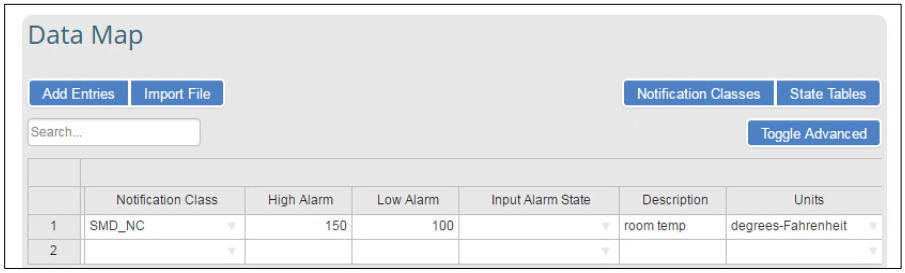
Figure 24: Setting Alarm Parameters

NOTE: For additional information about notification class elements, refer to the BACnet/IP or BACnet MS/TP driver manuals.

- Once finished, click Save in the Controls Panel.

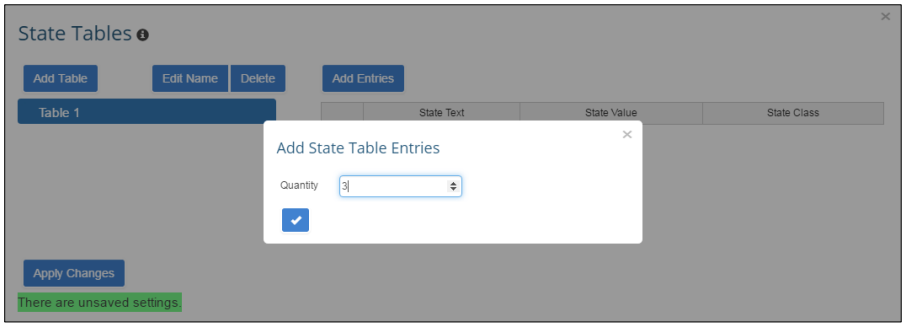
7.8 State Tables

- To setup state tables click the “State Tables” button in the upper right corner of the Data Map.



- Once the State Tables window is open, click the “Add Table” button.
- Name the table and click the check mark.

- Click on the new table entry, shown down the left side of the window.
- Click the “Add Entries” button to add the number of required entries (rows) for the table.



- Fill in the desired state values and repeat this process if additional tables are required.

- Once all needed tables are created, click the “Apply Changes” button in the bottom left corner of the State Tables window.

NOTE: The Apply Changes button will be disabled unless all state value fields are filled in with valid values.

7.9 Save KNX to BACnet Mapping

- Once the mappings and settings are defined, click Save to record information for later use.
- Click Restart to load the new configuration.

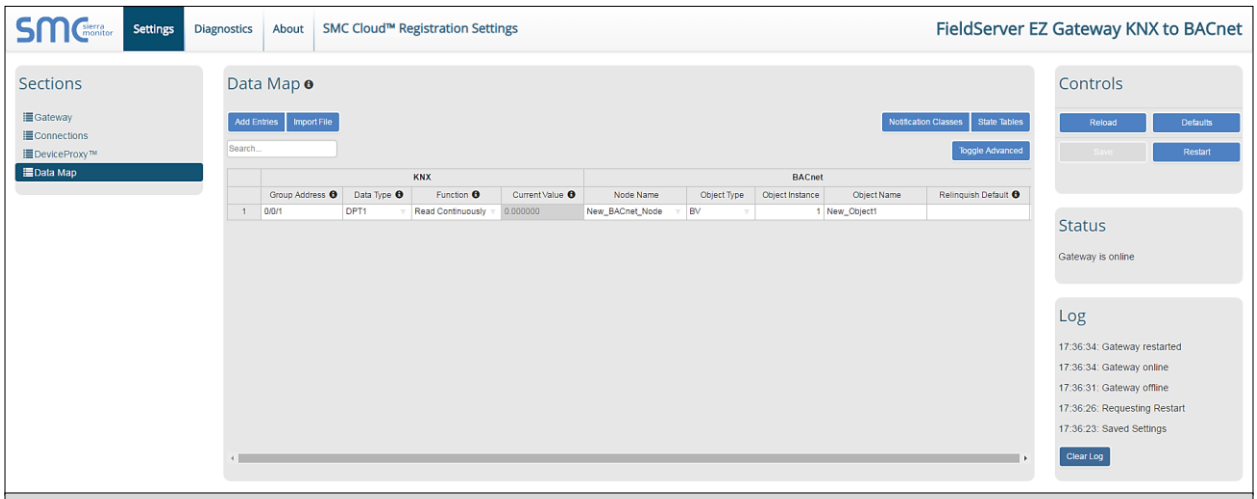


Figure 25: Saved Data Map

NOTE: Saving is prevented until all required fields in the table are validated. Highlighted fields go through validation and go from red to clear once a valid answer is entered. Once all highlighted data entry fields are clear, the status will change to allow saving. However, all fields should be filled out for accurate mapping.

7.10 Test and Commission the EZ Gateway

- Connect the EZ Gateway to the third party device(s), and test the application.
- Click on the “Diagnostic” tab to view the FS-GUI Diagnostic screen.
- From the main menu of the FS-GUI click on “View” under Navigation, then “Connections” to see the number of messages on each protocol.

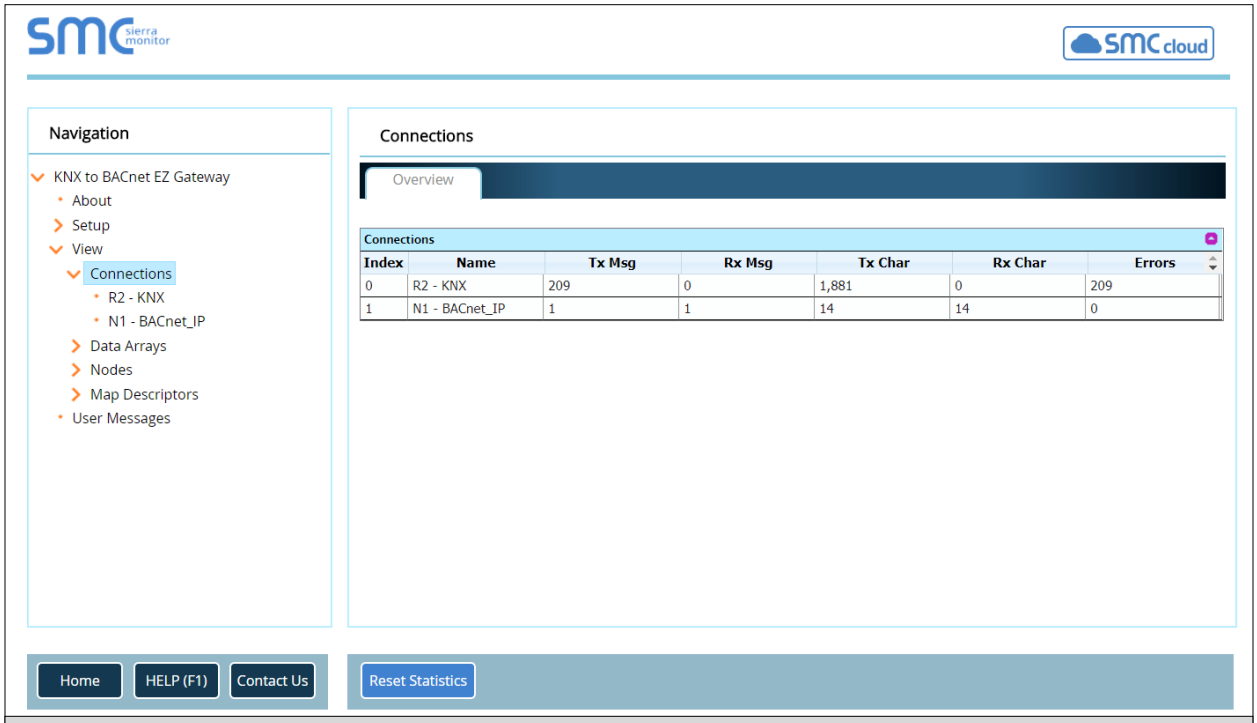


Figure 26: FS-GUI Connections Screen

NOTE: For troubleshooting assistance refer to Appendix A, or any of the troubleshooting Appendices in the related Driver Supplements and Configuration Manual. MSA Safety also offers a technical support page on the Sierra Monitor website, which contains a significant number of resources and documentation that may be of assistance.

7.10.1 Accessing SMC Cloud

The SMC Cloud button (see Figure 26) 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.

APPENDIX A. TROUBLESHOOTING

Appendix A.1. Communicating with the EZ Gateway over the Network

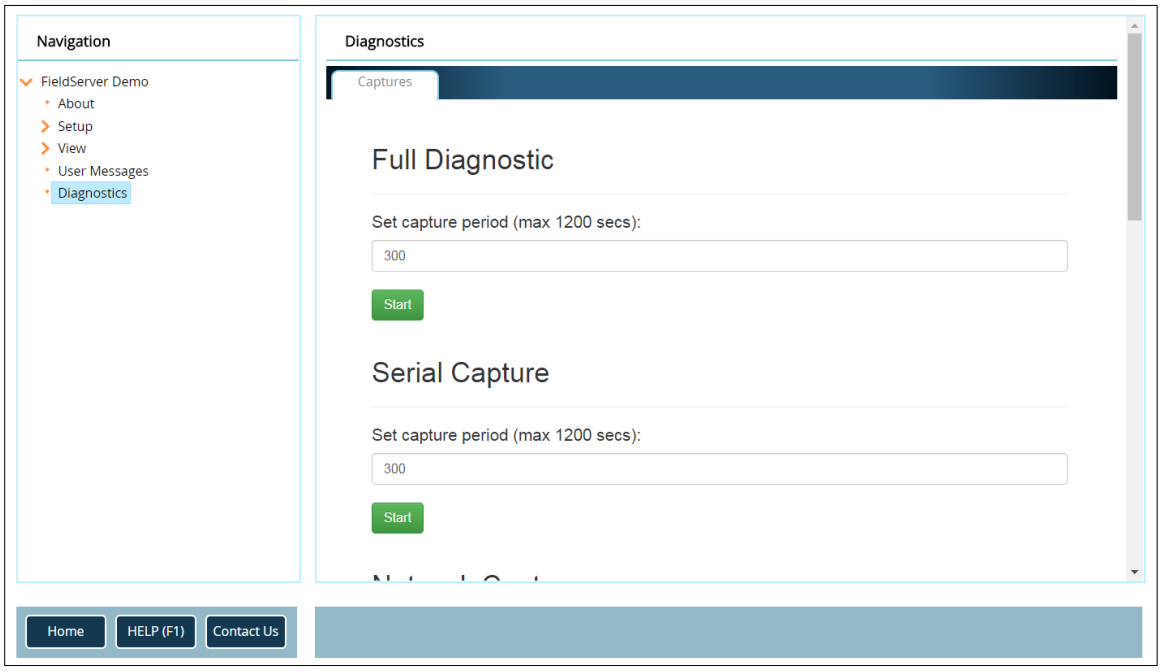
- Confirm that the network cabling is correct.
- Confirm that the computer network card is operational and correctly configured.
- Confirm that there is an Ethernet adapter installed in the PC's Device Manager List, and that it is configured to run the TCP/IP protocol.
- Check that the IP netmask of the PC matches the EZ Gateway. The Default IP Address of the EZ Gateway is 192.168.2.X, 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 102.168.2.X and the netmask 255.255.255.0
- Ensure that the PC and EZ Gateway are on the same IP Network, or assign a Static IP Address to the PC on the 192.168.2.X network.

Appendix A.2. Taking a FieldServer Diagnostic Capture

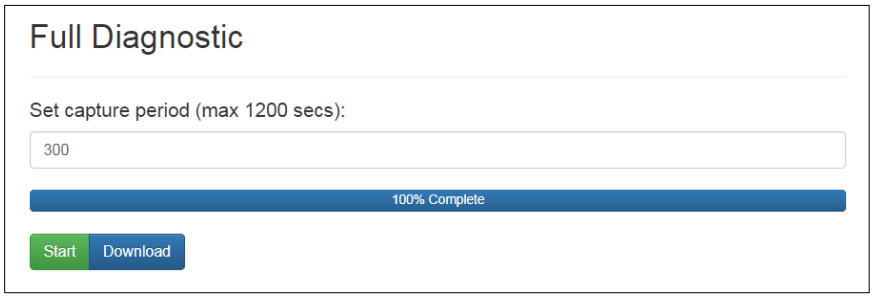
When there is a problem on-site that cannot easily be resolved, perform a Diagnostic Capture before contacting support. Once the Diagnostic Capture is complete, email it to technical support. The Diagnostic Capture will accelerate diagnosis of the problem.

If the FieldServer bios is updated/released on November 2017 or later then the Diagnostic Capture is performed via the gateway's on-board system.

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



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



- Click Download for the capture to be downloaded to the local PC.
- Send the diagnostic zip file to technical support.

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

Appendix A.2.1. Taking a Capture with Older Firmware

If the FieldServer firmware is from before November 2017, the Diagnostic Capture can be done by downloading the FieldServer Toolbox software but network connections (such as Ethernet and Wi-Fi) cannot be captured (if a network diagnostic is needed take a Wire Shark capture).

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 constantly being updated. Newer 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.

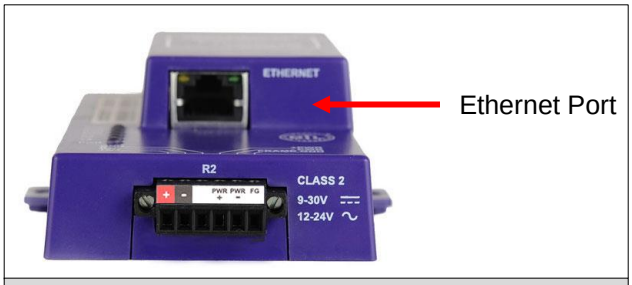
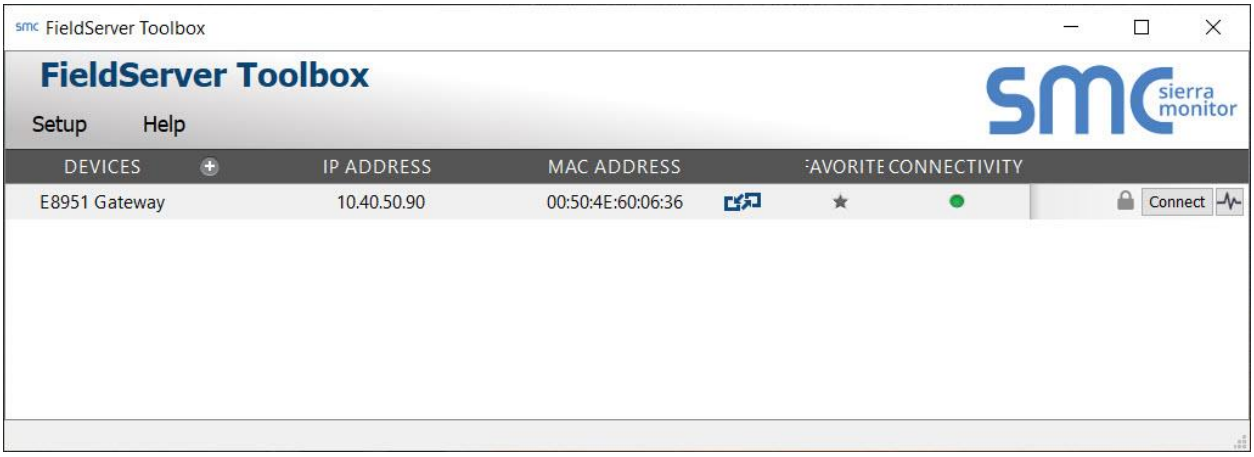


Figure 27: Ethernet Port Location

- Connect a standard Cat-5 Ethernet cable between the PC and FieldServer.
- Double click on the FS Toolbox Utility.
- **Step 1:** Take a Log
  - Click on the diagnose icon  of the desired device



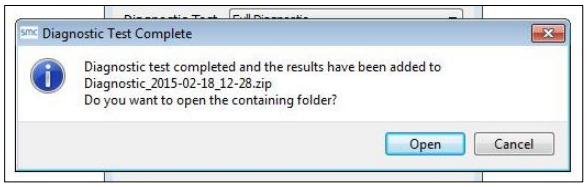
- Select “Full Diagnostic" from the drop down menu

NOTE: If desired, the default capture period can be changed.

- Click on the Start Diagnostic button

- Wait for the capture period to finish and the Diagnostic Test Complete window will appear

- **Step 2**: Send Log
  - Once the diagnostic test is complete, a .zip file is saved on the PC



- Choose “Open” to launch explorer and have it point directly at the correct folder
- Send the Diagnostic zip file to smc-support@msasafety.com

Appendix A.3. Notes Regarding Subnets and Subnet Masks

RFC standards allocate the IP Address range of 192.0.0.0 through to 223.255.255.255 to be used in Class-C subnetting (subnets listed as 255.255.255.xxx, where xxx can vary based on filtering required).

Consequently, the IP stack for this product will not allow any IP Addresses in this range to be allocated a subnet that does not fall within the Class C range.

Appendix A.4. LED Functions

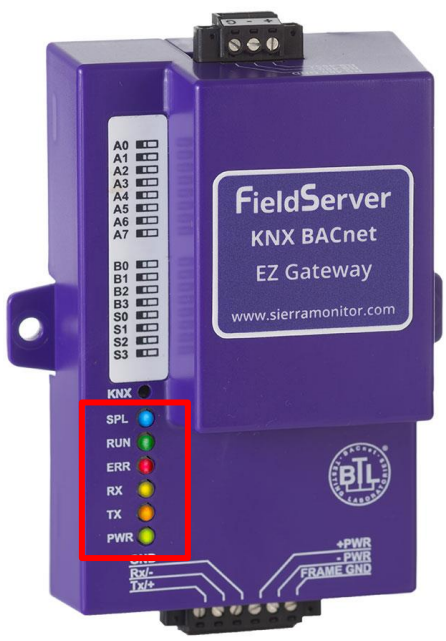


Figure 28: LED Location

Light	Description
SPL	SPL LED will be on when a configured node in the EZ Gateway is detected as being offline. For details, check the FS-GUI Node overview screen in FS-GUI (click “View” then “Nodes”).
RUN	RUN LED will flash 20 seconds after power up, signifying normal operation. The EZ Gateway will be able to access the Web Configurator GUI (**Section 5.3**) once this LED starts flashing. During the first 20 seconds, the LED should be off.
ERR	The ERR LED will go on solid 15 seconds after power up. It will turn off after 5 seconds. A steady red light will indicate there is a system error on the FieldServer. If this occurs, immediately report the related “system error” shown in the FS-GUI User Messages error screen to technical support for evaluation.
RX	On normal operation, the RX LED will flash when a message is received on the field port.
TX	On normal operation, the TX LED will flash when a message is sent on the field port.
PWR	The power light should always show steady green when connected to a functioning power source.

Appendix A.5. KNX Commissioning

Figure 29: KNX Port Location

The KNX Administrator will request that the installer hit the service pin at the correct step of the commissioning process. Insert a small screwdriver or other device into the KNX port to activate the service pin when prompted.

Appendix A.6. Internet Browser Software Support

The following web browsers are supported:

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

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

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

Appendix A.7. Change Web Server Security Settings After Initial Setup

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

- Navigate from the EZ Gateway landing page to the FS-GUI by clicking the Diagnostics tab at the top of the screen.

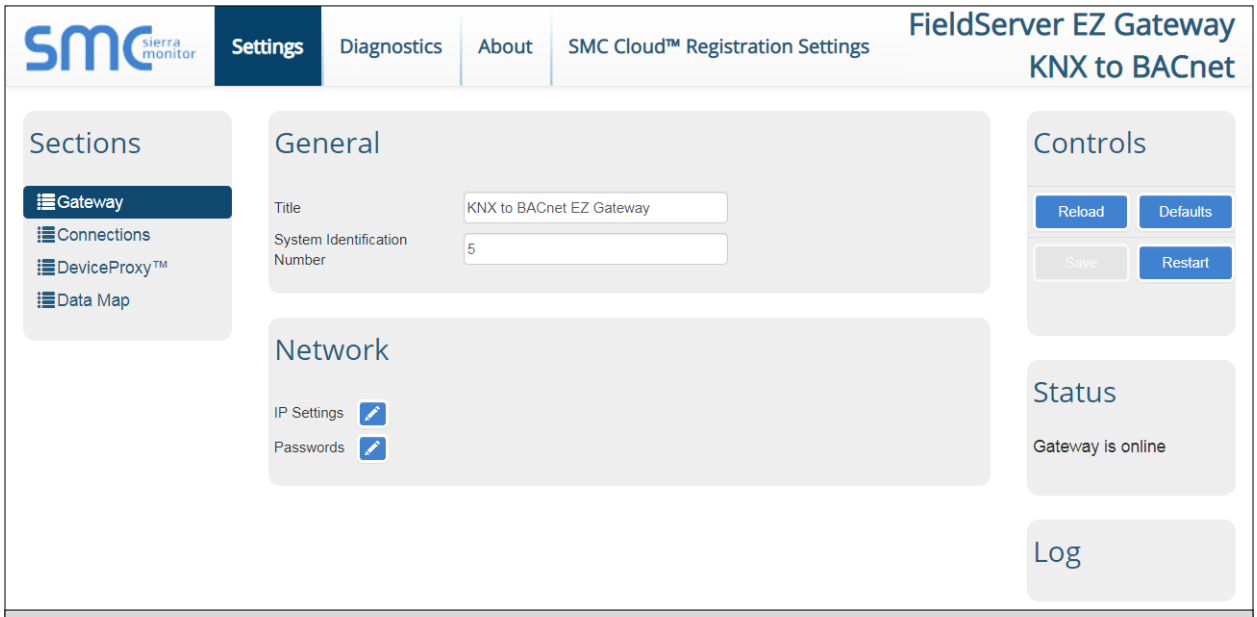


Figure 30: EZ Gateway Landing Page

- Click Setup in the Navigation panel.

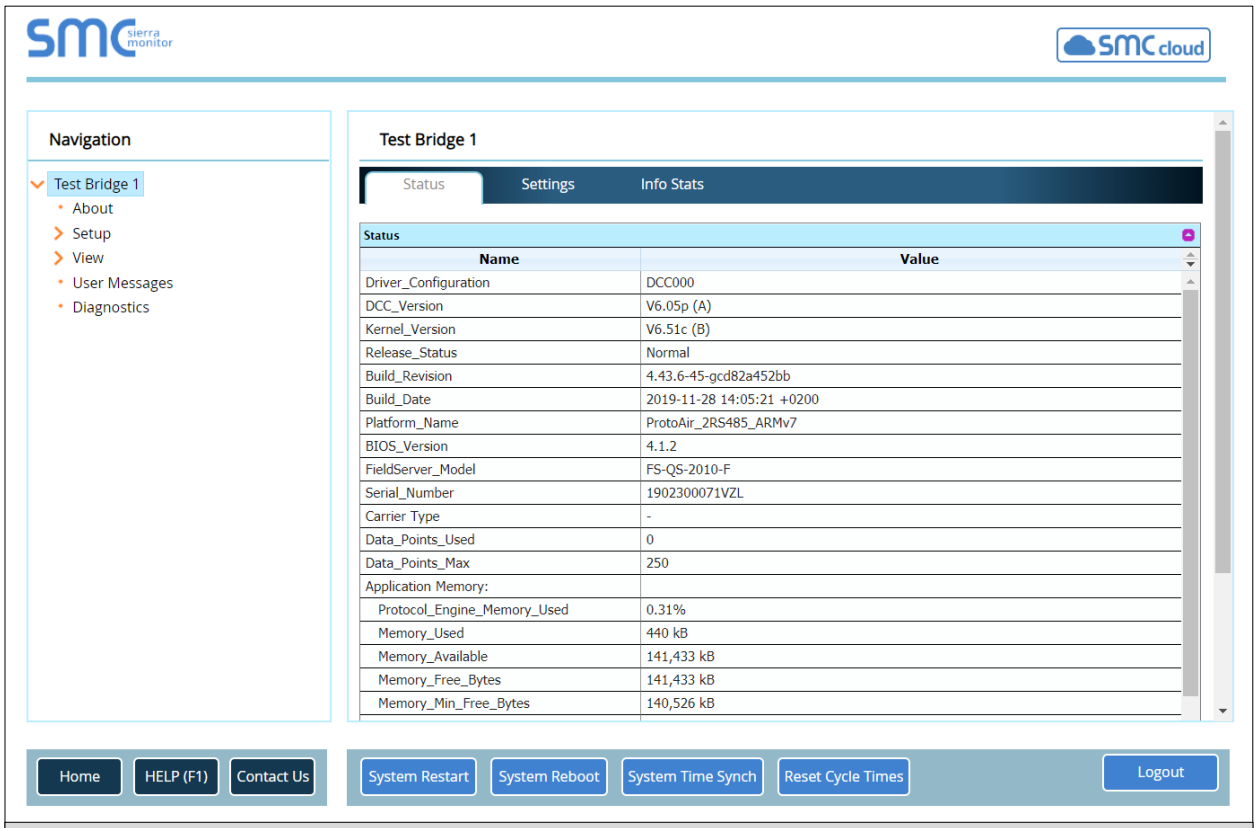


Figure 31: FS-GUI Landing Screen

Appendix A.7.1. Change Security Mode

- Click Security in the Navigation panel.

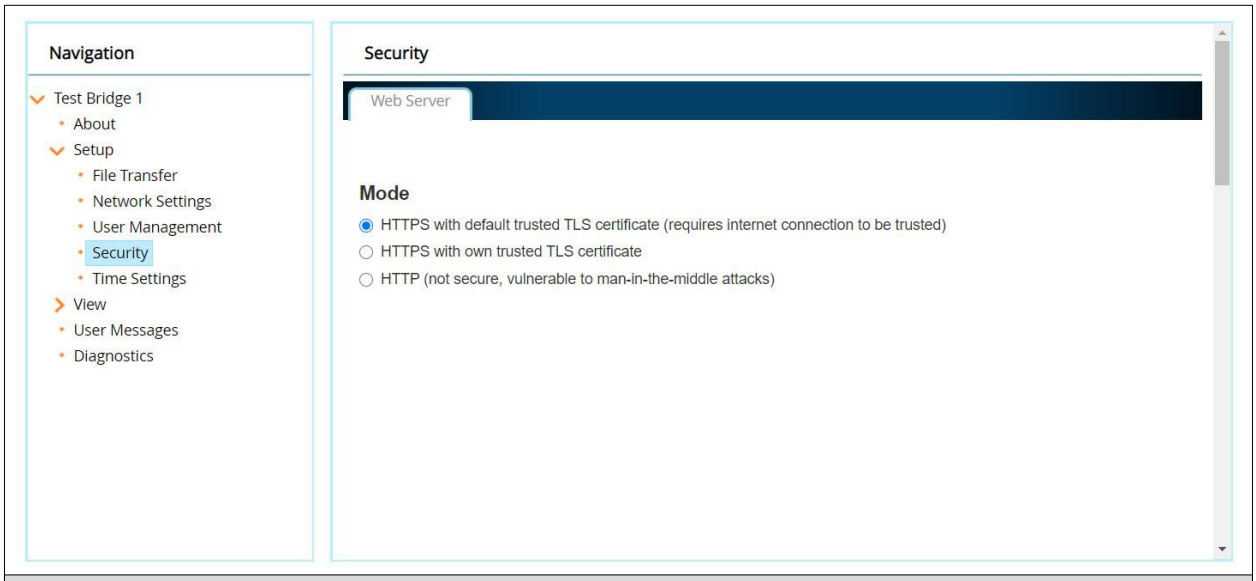


Figure 32: FS-GUI Security Setup

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

Appendix A.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.

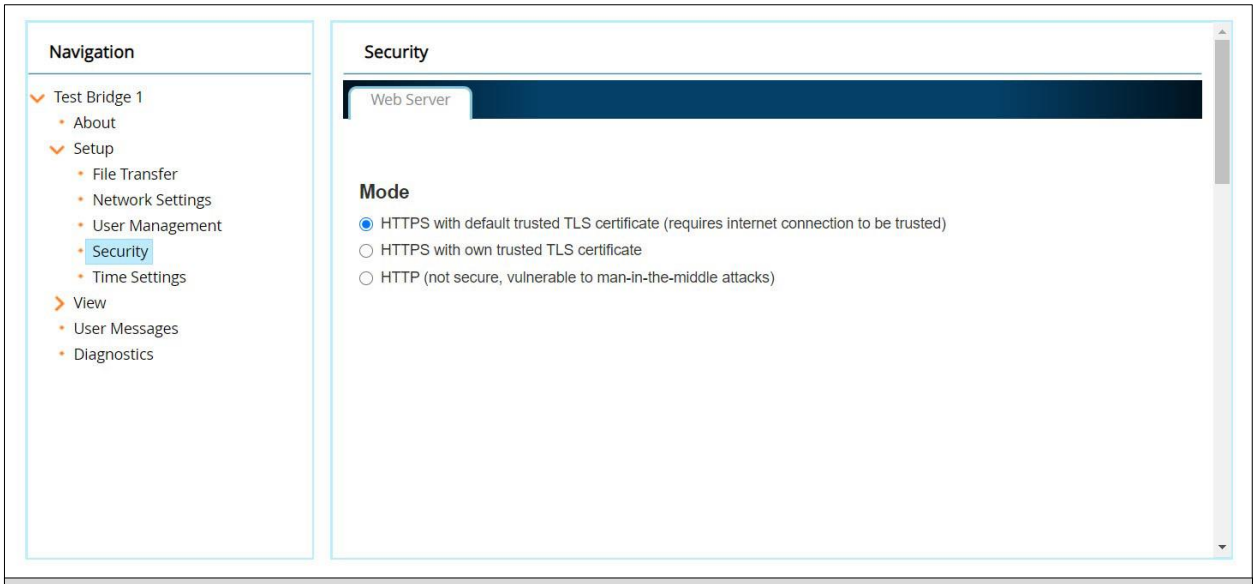


Figure 33: FS-GUI Security Setup – Certificate Loaded

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

Appendix A.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. For ProtoNode, ProtoCessor or ProtoCarrier recovery instructions, see the [FieldServer Recovery Instructions document]. 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.

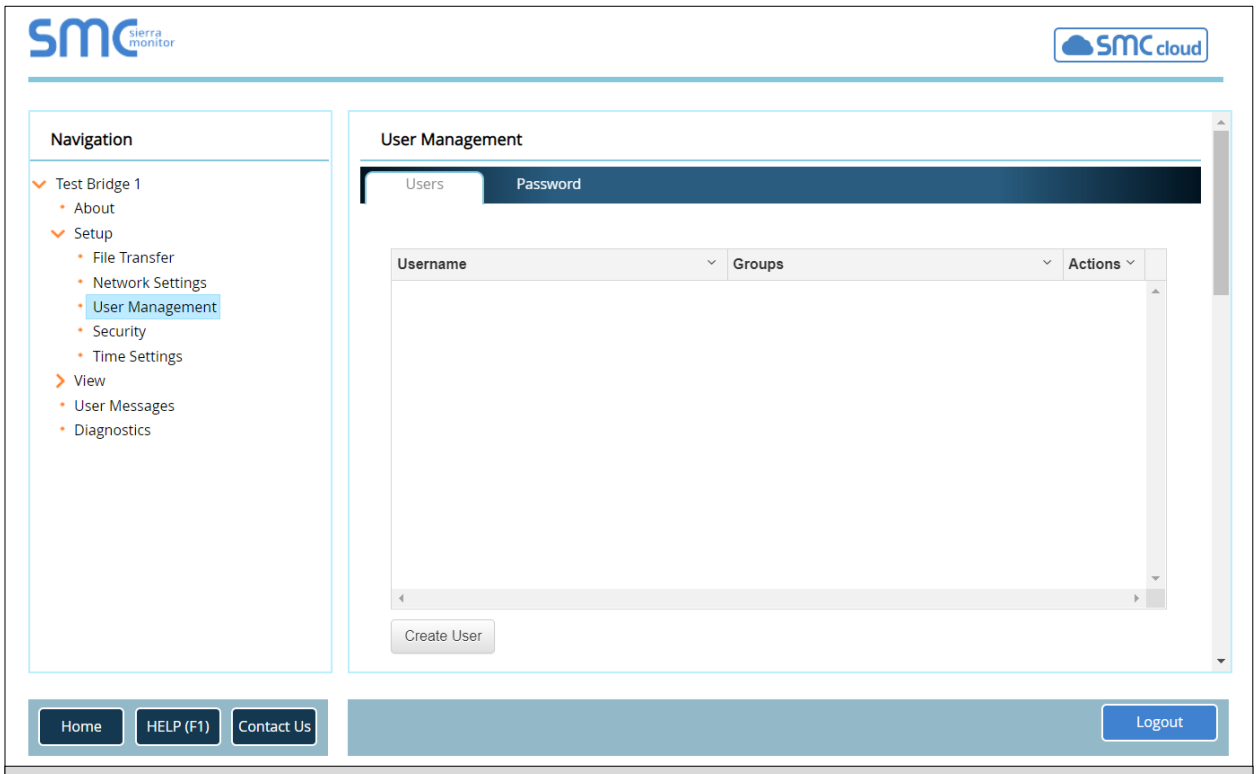


Figure 34: FS-GUI User Management

User Types:

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

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

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

Appendix A.8.1.1. Create Users

- Click the Create User button.

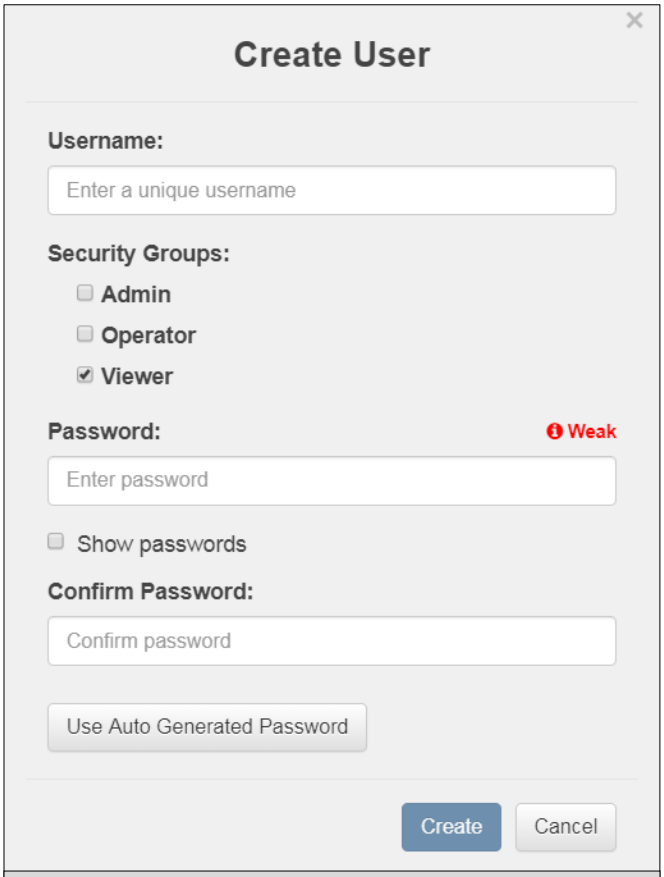


Figure 35: Create User Window

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

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

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

Appendix A.8.1.2. Edit Users

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

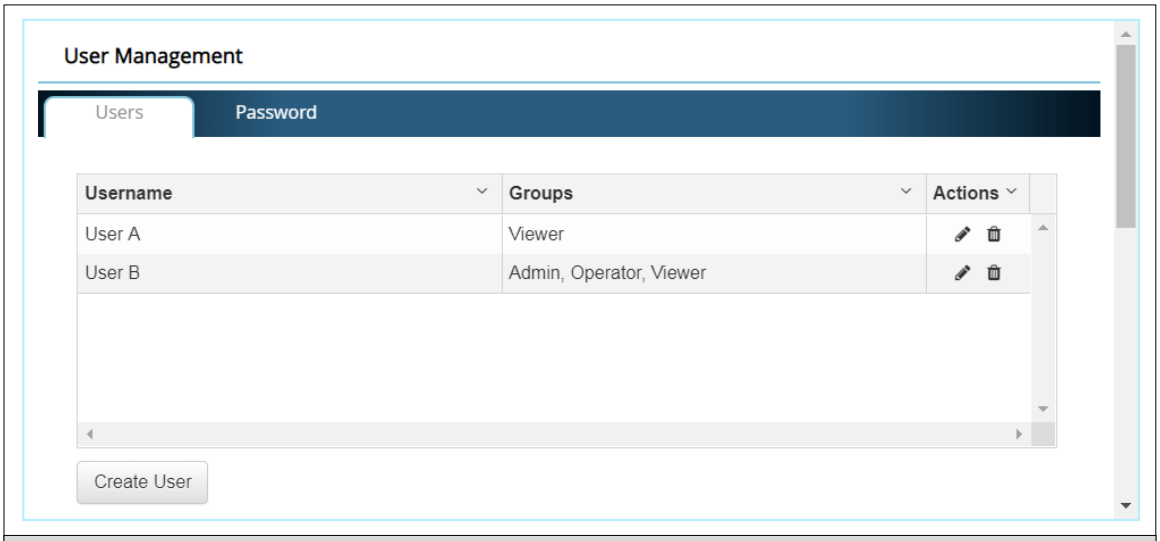


Figure 36: Setup Users

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

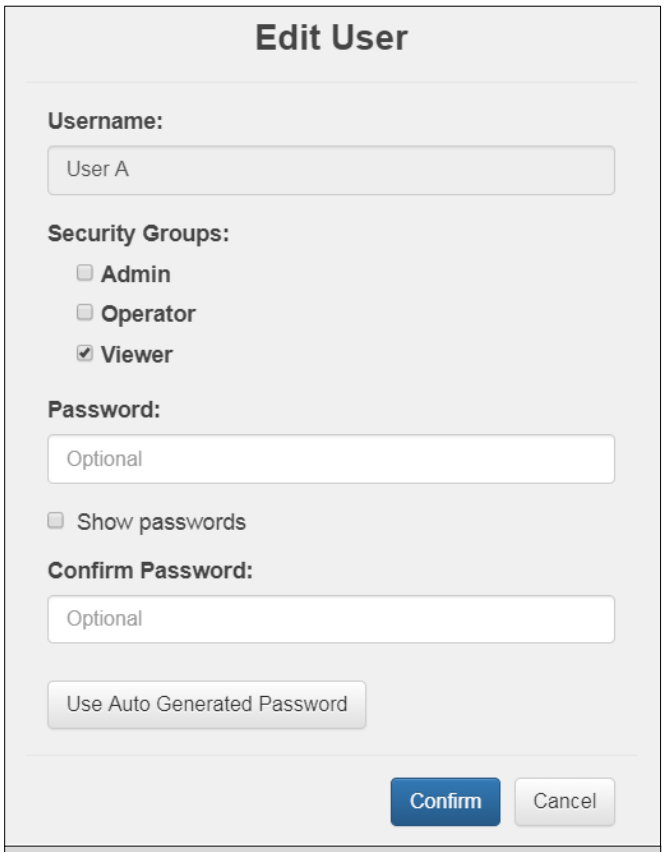


Figure 37: Edit User Window

- 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.

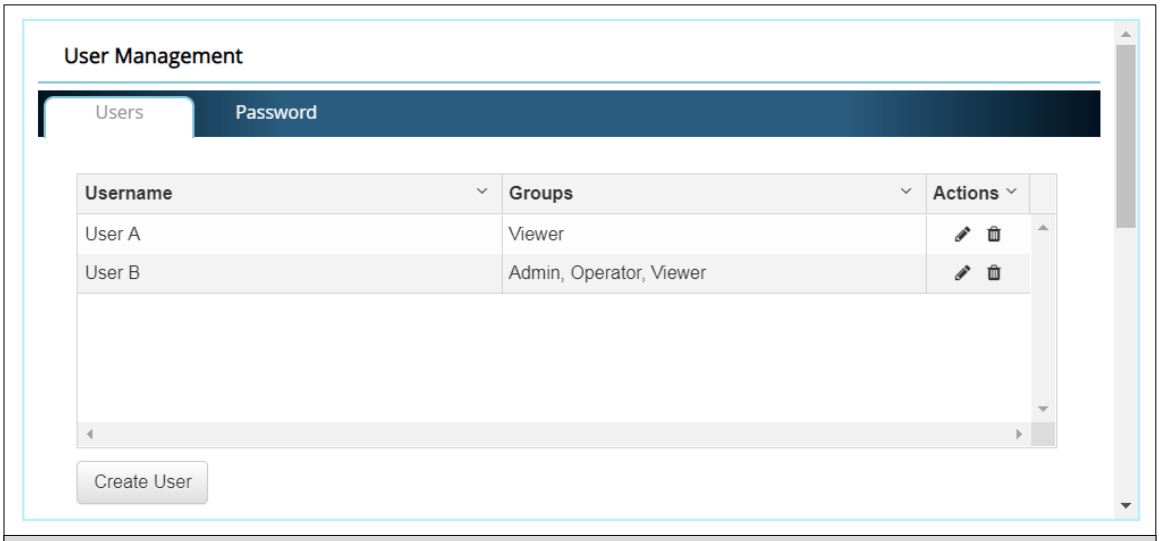


Figure 38: Setup Users

- When the warning message appears, click Confirm.

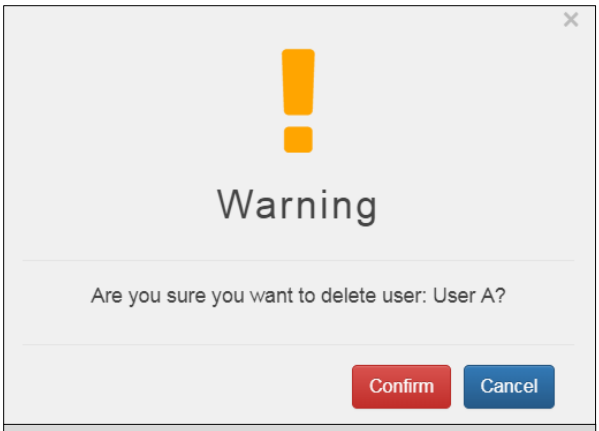


Figure 39: User Delete Warning

Appendix A.8.2. Change FieldServer Password

- Click the Password tab.

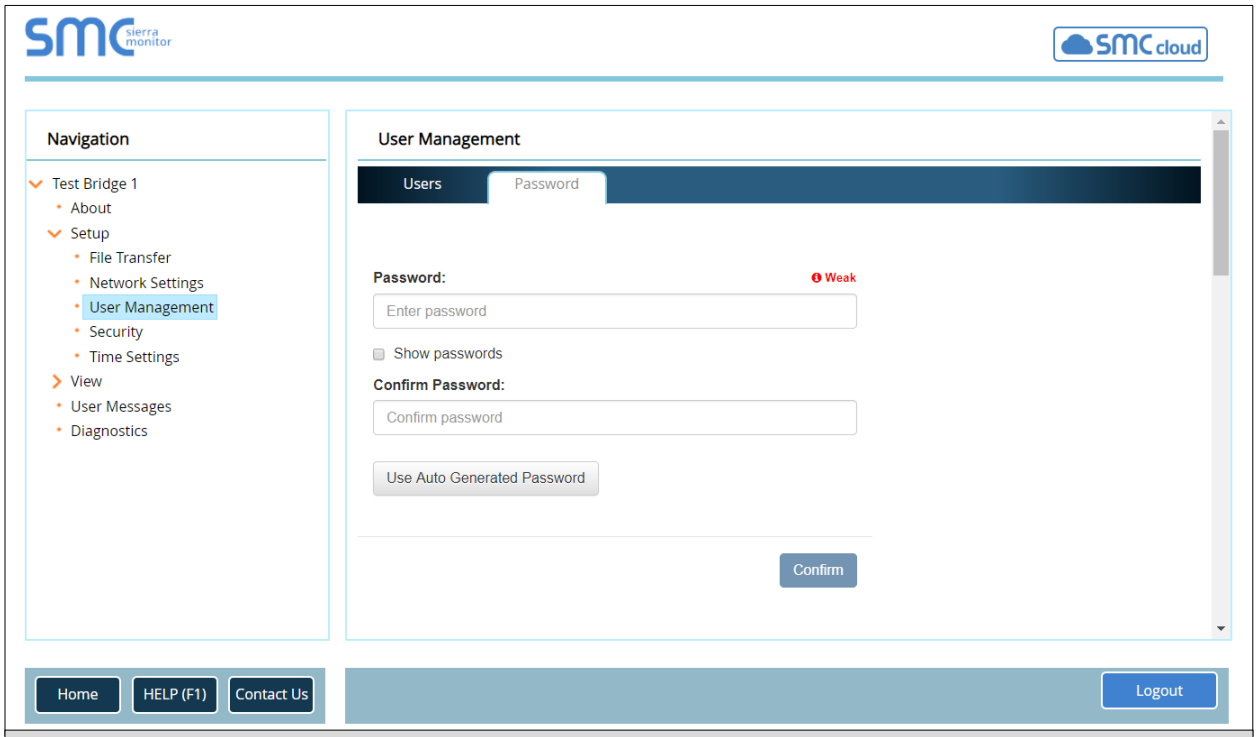


Figure 40: FieldServer Password Update via FS-GUI

- Change the login password for the FieldServer as needed.

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

NOTE: If a gateway in the field is updated to a secure gateway, the password will change to "admin1991!". This change will still occur if the gateway was already setup with a unique password that was loaded in the factory and printed on the label.

APPENDIX B. REFERENCE

Appendix B.1. Specifications

	FS-EZX-KNX-BAC [2]
Electrical Connections	One 6-pin Phoenix connector with: KNX port (+ / - / No Connection) Power port (+ / - / Frame-gnd) One 3-pin Phoenix connector with: RS-485 port (+ / - / gnd) One Ethernet 10/100 BaseT port
Power Requirements	*Input Voltage:* 9-30VDC or 12-24VAC *Current draw:* @ 12V, 240 mA *Max Power:* 2.5 Watts *Input Power Frequency:* 50/60 Hz.
Approvals	TUV approved to UL 916, RoHS3 compliant, FCC part 15 compliant, CE certified, BTL certified, WEEE compliant, REACH compliant
Physical Dimensions	5.05 x 2.91 x 1.6 in. (12.82 x 7.39 x 4.06 cm) excluding mounting tabs
Weight	0.4 lbs (0.2 Kg)
Operating Temperature	-40°C to 75°C (-40°F to167°F)
Surge Suppression	EN61000-4-2 ESD EN61000-4-3 EMC EN61000-4-4 EFT
Humidity	5 - 90% RH (non-condensing)

Figure 41: 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".

[2] Specifications subject to change without notice.

Appendix B.2. Compliance with UL Regulations

For UL compliance, the following instructions must be met when operating the EZ Gateway.

- The units shall be powered by listed LPS or Class 2 power supply suited to the expected operating temperature range.
- The interconnecting power connector and power cable shall:
  - Comply with local electrical code
  - Be suited to the expected operating temperature range
  - Meet the current and voltage rating for the EZ Gateway
- Furthermore, the interconnecting power cable shall:
  - Be of length not exceeding 3.05m (118.3”)
  - Be constructed of materials rated VW-1, FT-1 or better
- If the unit is to be installed in an operating environment with a temperature above 65 °C, it should be installed in a Restricted Access Area requiring a key or a special tool to gain access.
- This device must not be connected to a LAN segment with outdoor wiring.

Appendix B.3. Supported KNX Data Types

Below are listed all of the supported KNX data types and their descriptions:

KNX Data Types	Description
DPT1	1-bit Binary Switch
DPT2	2-bit Step Control
DPT3	4-bit Dimming
DPT4	8-bit Set
DPT5	8-bit Unsigned Value
DPT6	8-bit Signed Value
DPT7	16-bit Unsigned Value
DPT8	16-bit Signed Value
DPT9	16-bit Float
DPT12	32-bit Unsigned Value
DPT13	32-bit Signed Value
DPT14	32-bit Float
DPT15	32-bit Access
DPT17	8-bit Scene Number
DPT18	8-bit Scene Control
DPT20	8-bit Enum Value

NOTE: See KNX driver manual for additional information.

Appendix B.4. Dimension Drawing FS-EZX-KNX-BAC

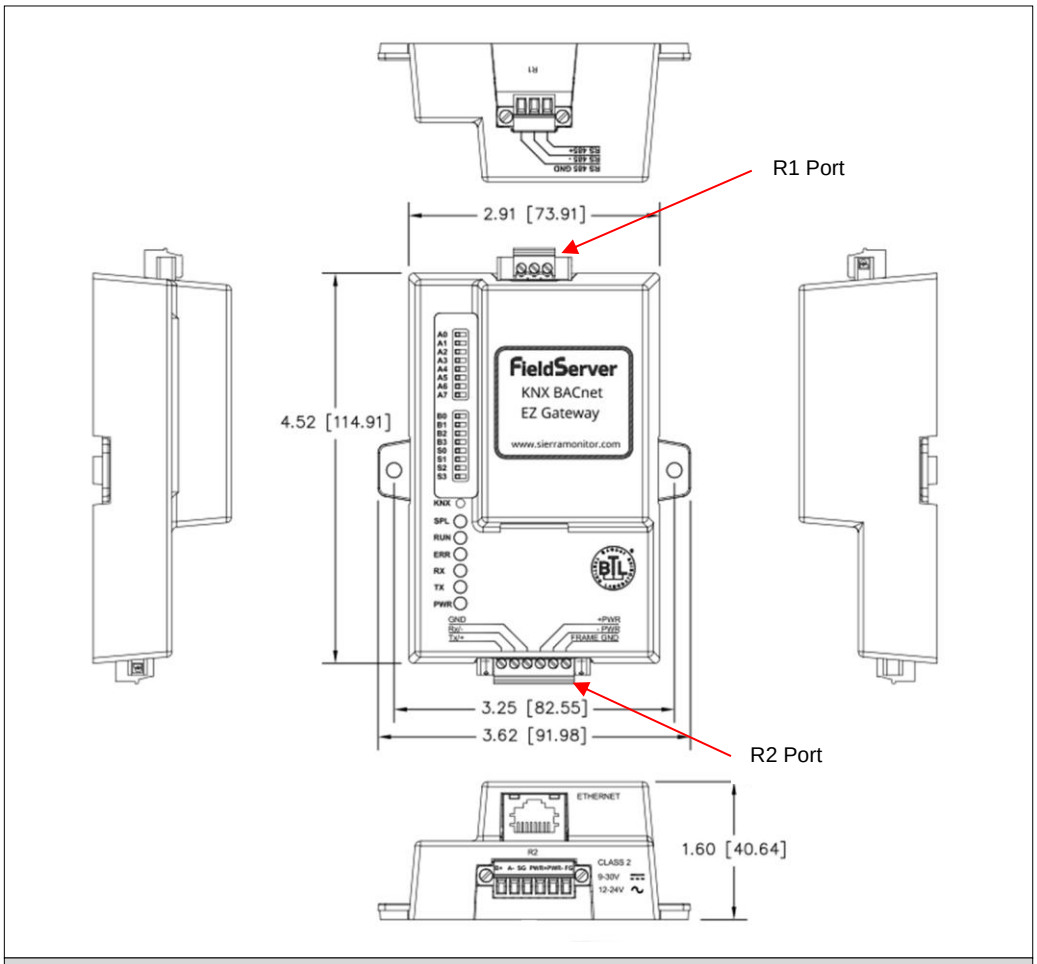


Figure 42: EZ Gateway Dimension Drawing

APPENDIX C. LIMITED 2 YEAR WARRANTY

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

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

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

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