460BMWI-N700 Protocol Gateway

Product User Guide

Firmware Version 8.7.4

Trademarks
CompactLogix, ControlLogix, & PLC-5 are registered trademarks of Rockwell Automation, Inc. EtherNet/IP is a trademark of the ODVA. MicroLogix, RSLogix 500, and SLC are trademarks of Rockwell Automation, Inc. Microsoft, Windows, and Internet Explorer are registered trademarks of Microsoft Corporation. BACnet® is a registered trademark of American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE). All other trademarks and registered trademarks are the property of their holders.

Limited Warranty
Real Time Automation, Inc. warrants that this product is free from defects and functions properly.

EXCEPT AS SPECIFICALLY SET FORTH ABOVE, REAL TIME AUTOMATION, INC. DISCLAIMS ALL OTHER WARRANTIES, BOTH EXPRESSED AND IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR APPLICATION. THIS LIMITED WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY ALSO HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE.

The examples and diagrams in this manual are included solely for illustrative purposes. Because of the many variables and requirements associated with any particular application, Real Time Automation, Inc. cannot assume responsibility or liability for actual use based on the examples and diagrams. Except as specifically set forth above, Real Time Automation and its distributors and dealers will in no event be liable for any damages whatsoever, either direct or indirect, including but not limited to loss of business profits, income, or use of data. Some states do not allow exclusion or limitation of incidental or consequential damages; therefore, the limitations set forth in this agreement may not apply to you.

No patent liability is assumed by Real Time Automation with respect to use of information, circuits, equipment, or software described in this manual.

Government End-Users
If this software is acquired by or on behalf of a unit or agency of the United States Government, this provision applies: The software (a) was developed at private expense, is existing computer software, and was not developed with government funds; (b) is a trade secret of Real Time Automation, Inc. for all purposes of the Freedom of Information Act; (c) is “restricted computer software” submitted with restricted rights in accordance with subparagraphs (a) through (d) of the Commercial “Computer Software-Restricted Rights” clause at 52.227-19 and its successors; (d) in all respects is proprietary data belonging solely to Real Time Automation, Inc.; (e) is unpublished and all rights are reserved under copyright laws of the United States. For units of the Department of Defense (DoD), this software is licensed only with “Restricted Rights”: as that term is defined in the DoD Supplement of the Federal Acquisition Regulation 52.227-7013 (c) (1) (ii), rights in Technical Data and Computer Software and its successors, and: Use, duplication, or disclosures is subject to restrictions as set forth in subdivision (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at 52.227-7013. If this software was acquired under GSA schedule, the U.S. Government has agreed to refrain from changing or removing any insignia or lettering from the Software or documentation that is provided or from producing copies of the manual or media. Real Time Automation, Inc.

© 2026 Real Time Automation, Inc. All rights reserved.

Overview 5
Hardware Platforms 6
Hardware – N700 7
Powering the Gateway 7
Port Connections 8
Mounting with a DIN Rail 9
Installing 9
Removing 9
Accessing the Main Page 10
Committing Changes to the Settings 11
Main Page 12
Device Configuration 13
Network Configuration 14
BACNet MS/TP Manager Configuration 15
BACnet MS/TP Manager Device Configuration 16
Configuring Read Scan Lines 17
Configuring Writes Scan Lines 17
Web Interface Configuration 18
Web Interface Client/Server Configuration 18
Web Interface Name/Value Pair Configuration 21
Web Interface Client/Server Configuration: Advanced Configuration 22
Operation Mode 24
Mapping - Transferring Data Between Devices 25
Display Mapping and Values 25
Display Data 25
Display String 28
Display String use case 30
Data and String Mapping – Auto-Configure 31
Data Mapping – Explanation 32

Data Mapping – Adding Diagnostic Information 33
String Mapping – Explanation 38
Mapping – Auto-Configure Mode to Manual Configure Mode 39
Mapping – Manual Configure Mode to Auto-Configure Mode 40
View as Text 41
Data Mapping 41
String Mapping 41
Base Triggering – Data Validiation Triggering 42
Security Configuration 44
Security Configuration-Security Levels 45
Security - Log In 46
Security - Log Out 46
Email Configuration 47
Alarm Configuration 48
Diagnostics – Alarm Status 50
Alarms – Active 51
Alarms – Clear 51
Change of State (COS) Configuration 52
Diagnostics Info 53
Diagnostics Mapping 53
Diagnostics – BACnet MS/TP Manager 54
Diagnostics – Web Interface 58
Configuration Files 60
Export Configuration 60
Import Configuration 60
Save and Replace Configuration Using SD Card 62
Saving Configuration Using SD Card 62
Replacing Configuration Using SD Card 62
Utilities 63

Overview

The 460BMWI-N700 gateway Connects up to 32 BACnet MS/TP Subordinates devices to a web interface. By following this guide, you will be able to configure the 460BMWI-N700 gateway.

Number of ASCII devices is dependent on the Hardware and Product number of the 460 gateway.

For further customization and advanced use, please reference the appendices located online at: http://www.rtautomation.com/product/460-gateway-support/.

If at any time you need further assistance, do not hesitate to call Real Time Automation support. Support Hours are Monday-Friday 8am-5pm CST

Toll free: 1-800-249-1612
Email: support@rtautomation.com

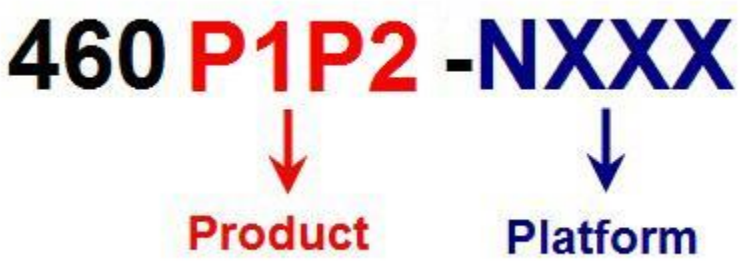
Hardware Platforms

The 460 Product Line supports a number of different hardware platforms. There are differences in how they are powered, what serial settings are supported, and some diagnostic features supported (such as LEDs). For these sections, be sure to identify the hardware platform you are using.

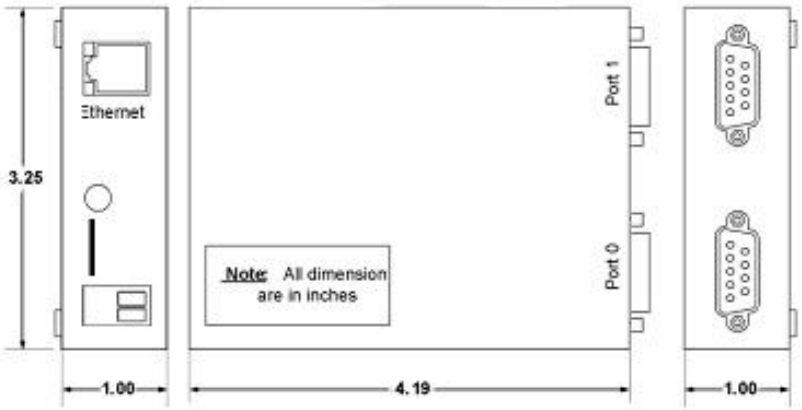
To find which hardware platform you are using:

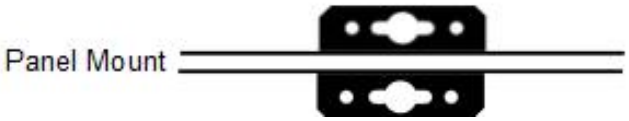
1) Look on the front or back label of the unit for the part number.
2) On the webpage inside the gateway, navigate to the dropdown menu under **Other** and select **Utilities**. Click the **Listing of Revisions** button. The full part number is displayed here.

Once you have the full part number, the platform will be the number following the "-N":



Hardware – N700





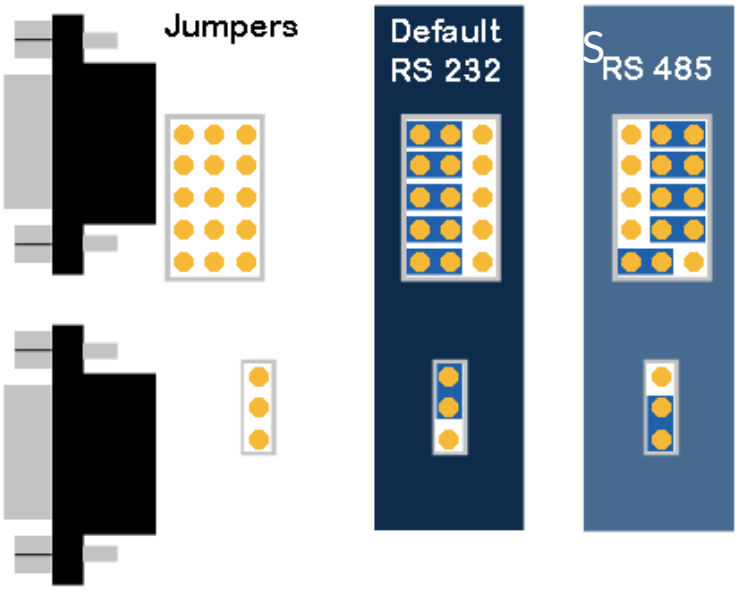
Powering the Gateway

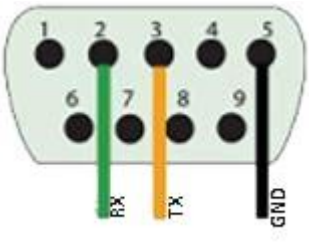
1) Connect a 12-24 VDC power source to the gateway:
   a) 2-Pin Terminal power connection with Red Wire = (+) Black Wire = (-)

Port Connections

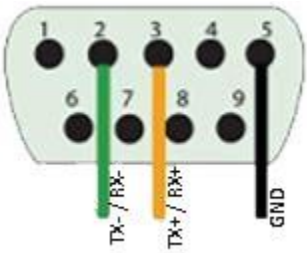
The factory default port settings for Port 0 and Port 1 are RS232. If the default port settings are not compatible with your ASCII device, Port 0 can be configured for RS232, RS485, or RS422. Port 1 can only be configured for RS232.

Jumper Configuration

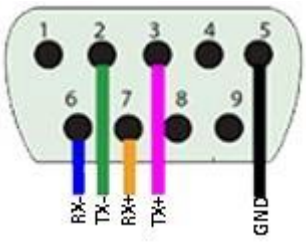




Port 0 & Port 1
RS232



Port 0
RS485



Port 0
RS422

The default jumper configurations are setup for the following serial modes:

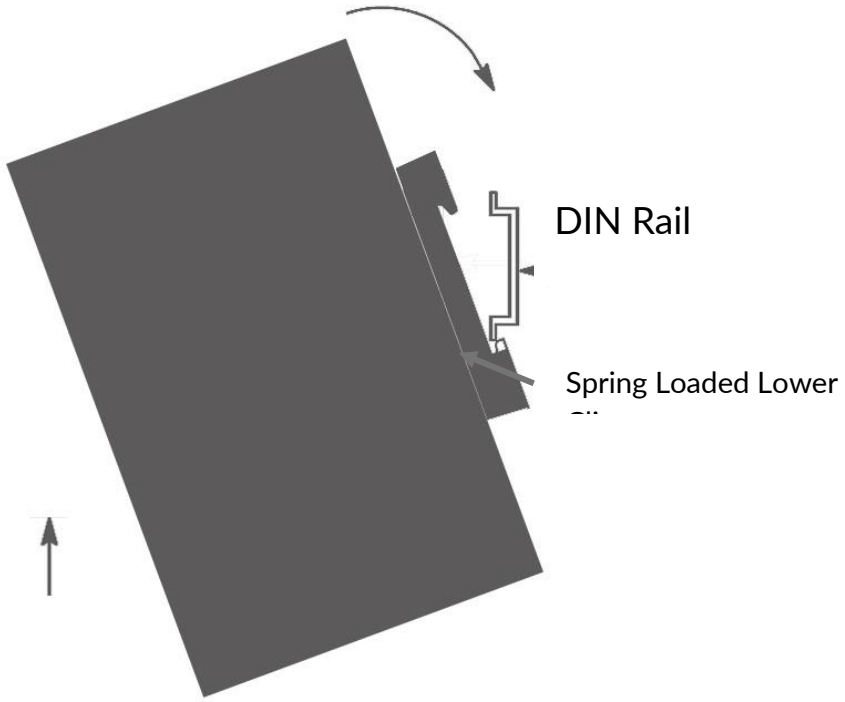
- **Port 0 – RS232**
- **Port 1 – RS232**

Mounting with a DIN Rail

Installing

Follow these steps to install your interface converter.

1) Mount your DIN Rail.
2) Hook the bottom mounting flange under the DIN Rail.
3) While pressing the 460BMWI-N700 against the rail, press up to engage the spring loaded lower clip and rotate the unit parallel to the DIN Rail.
4) Release upward pressure.



Removing

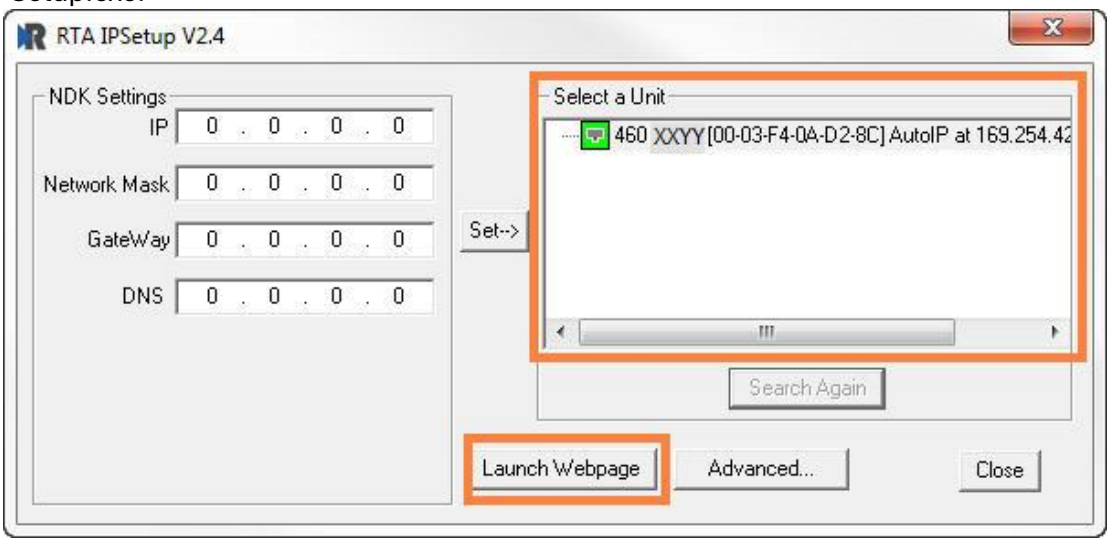
Follow these steps to remove your interface converter.

1) Press up on unit to engage the spring loaded lower clip.
2) Swing top of the unit away from DIN Rail.

Accessing the Main Page

The following steps will help you access the browser based configuration of the gateway. By default, DHCP is enabled. If the gateway fails to obtain an IP address over DHCP it will Auto IP with 169.254.X.Y. For more information on your Operating system network setting refer to the Accessing Browser Configuration document from our support web site.

1) Scan the QR code on the back of the unit or navigate to www.rtautomation.com/460-gateway-support and download IPSetup.exe.



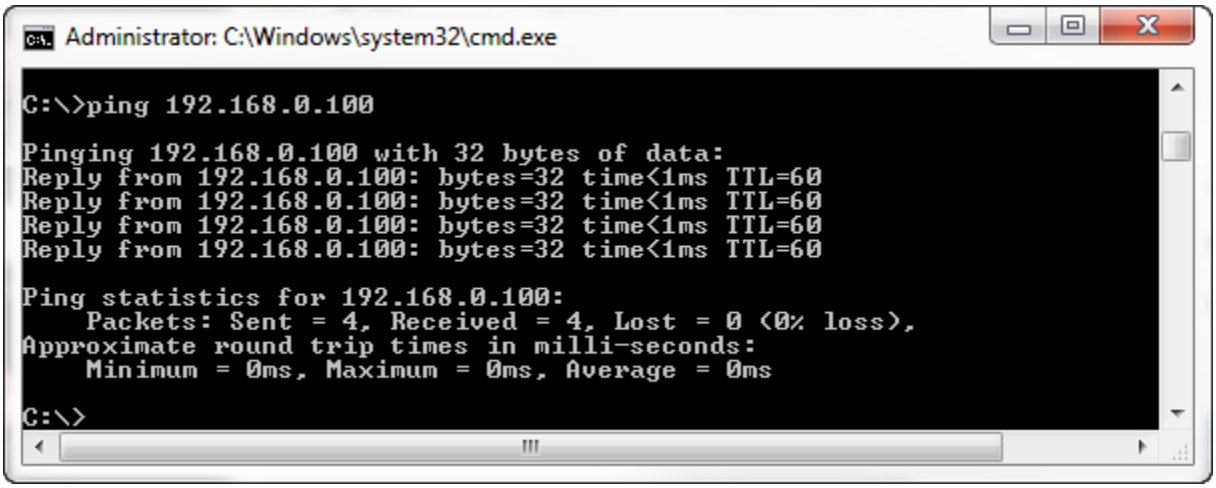
2) Run the IPSetup.exe program.
3) Find unit under “Select a Unit”.
   a. Change Gateway’s IP address to match that of your PC if DHCP has failed.
      i. You will know DHCP has failed if the gateway’s IP address is AutoIP at 169.254.X.Y.
      ii. If successful, it will say DHCP’d at ex: 192.168.0.100 or however your DCHP Client is set up.
   b. If you do not see the gateway in this tool, then your PC is most likely set up as a static IP.
      i. Change your PC’s network settings to be DHCP. If DHCP fails, then it will change to be on the 169.254.x.y network.
      ii. Relaunch the IP Setup tool to see if gateway can be discovered now.
4) Click **Launch Webpage**. The Main page should appear.

Default setting is set to DHCP. If DHCP fails, default IP Address is 169.254.x.y

Error: Main Page Does Not Launch

If the Main Page does not launch, please verify the following:

1) Check that the PC is set for a valid IP Address
   a. Open a MS-DOS Command Prompt
   b. Type "ipconfig" and press enter
   c. Note the PC's IP Address, Subnet, and Default Gateway
2) The gateway must be on the same Network/Subnet as the PC whether it's setup for DHCP or Static. Once you have both devices on the same network, you should be able to ping the gateway using a MS-DOS Command Prompt.



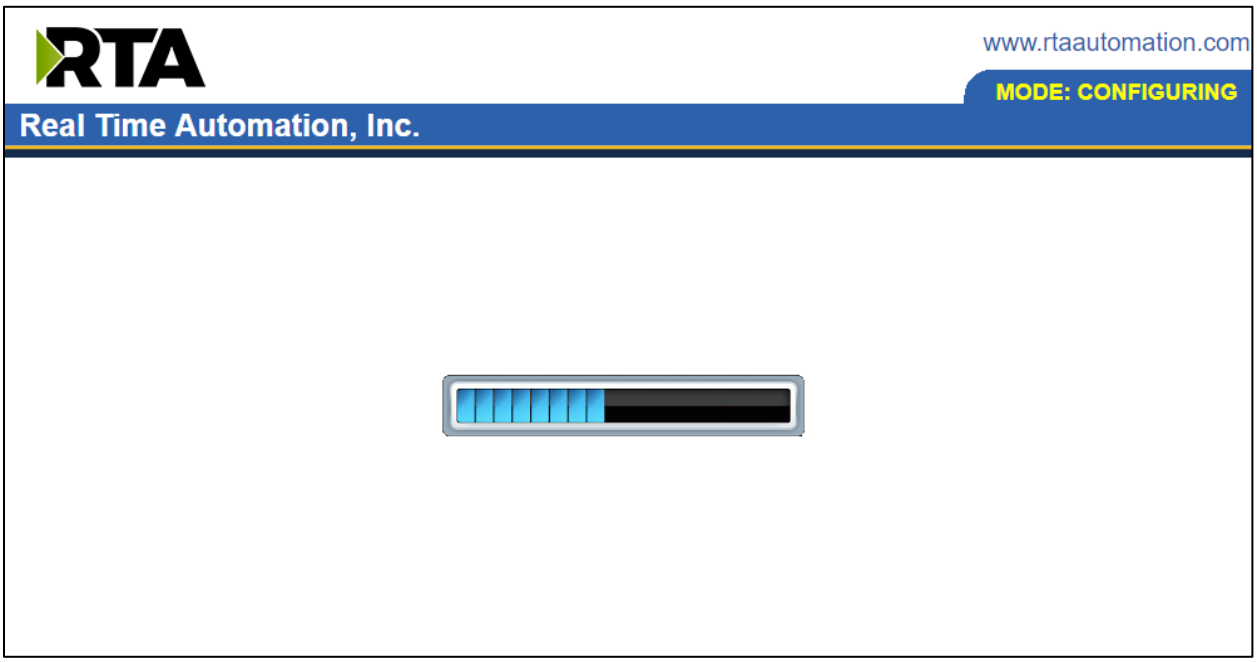
The Screenshot above shows a gateway that is currently set to a static IP Address of 192.168.0.100. If you are able to successfully ping your gateway, open a browser and try to view the main page of the gateway by entering the IP Address of the gateway as the URL.

Committing Changes to the Settings

All changes made to the settings of the gateway in Configuration Mode will not take effect until the gateway is restarted via the webpage. Changes will not be stored if the gateway's power is removed prior to a reboot.

NOTE: The gateway does not need to be restarted after every change. Multiple changes can be made before a restart, but they will not be committed until the gateway is restarted.

When all desired changes have been made, press the **Restart Now** button.
The webpage will redirect to our rebooting page shown below:



The reboot can take up to 20 seconds.
If the IP address has not been modified, the gateway will automatically redirect to the main page.
If the IP address was modified, a message will appear at the top of the page to instruct the user to manually open a new webpage at that new IP.

Main Page

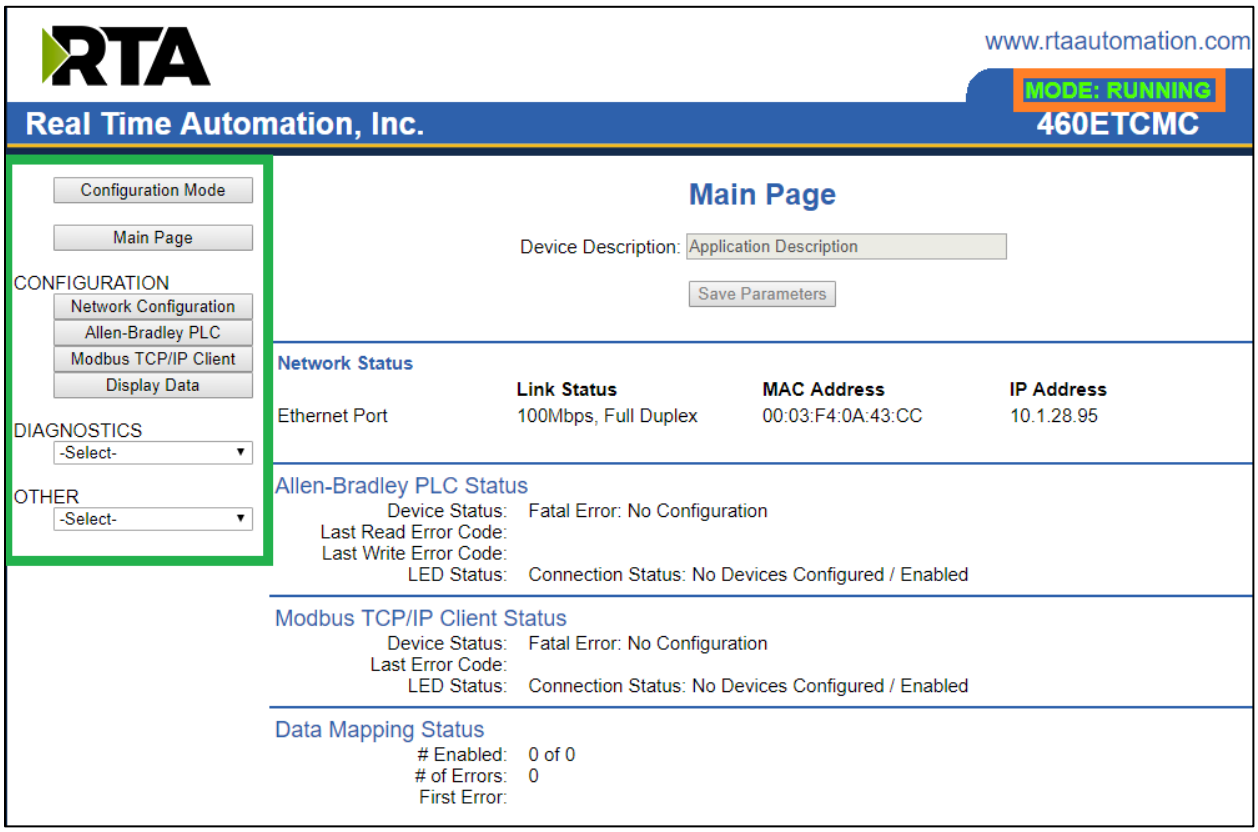
The main page is where important information about your gateway and its connections are displayed.
Mode (orange box below):
Running Mode:

- Protocol communications are enabled
- Configuration cannot be changed during Running Mode. If changes are needed, click the **Configuration Mode** button shown in the green box below

Configuring Mode:

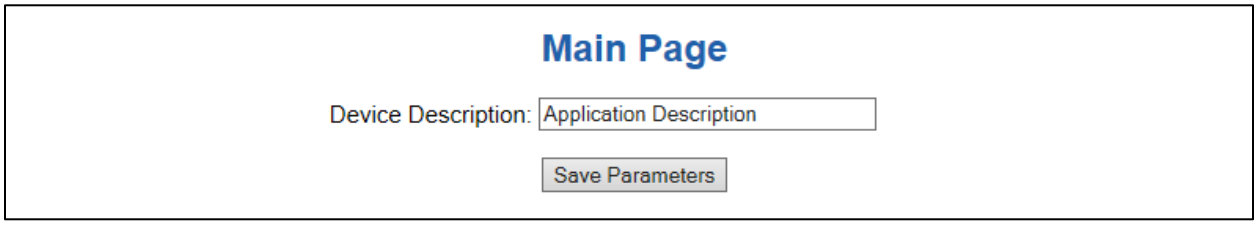
- Protocol communication is stopped and no data is transmitted
- Configuration is allowed

Navigation (green box below):
You can easily switch between modes and navigate between pages (Configuration, Diagnostics, and Other pages) using the buttons on the left hand side.



Device Configuration

The device configuration area is where you assign the device description parameter. Changes can only be made when the gateway is in Configuration Mode.



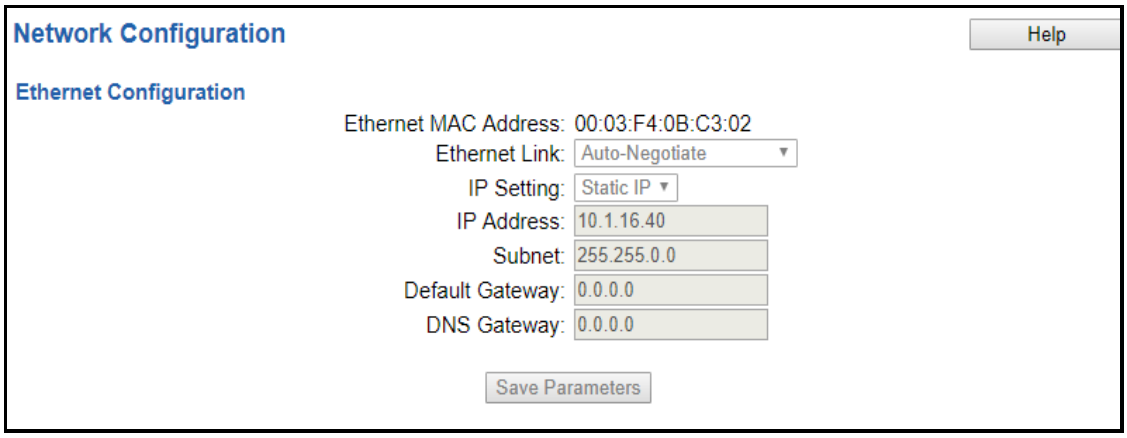
Once you are done configuring the Description, click the **Save Parameters** button.

Network Configuration

The network configuration area is where you assign the IP address and other network parameters. Changes can only be made when the gateway is in Configuration Mode.

Once you are done configuring the Network Settings, click the **Save Parameters** button.

If you are changing the IP Address of the gateway, the change will not take effect until the unit has been rebooted. After reboot, you must enter the new IP Address into the URL.

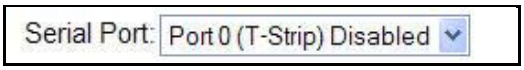


It is recommended to leave the DNS Gateway set to 0.0.0.0 and the Ethernet Link as Auto-Negotiate. If configuring the gateway to use E-mail, the DNS Gateway must be set.

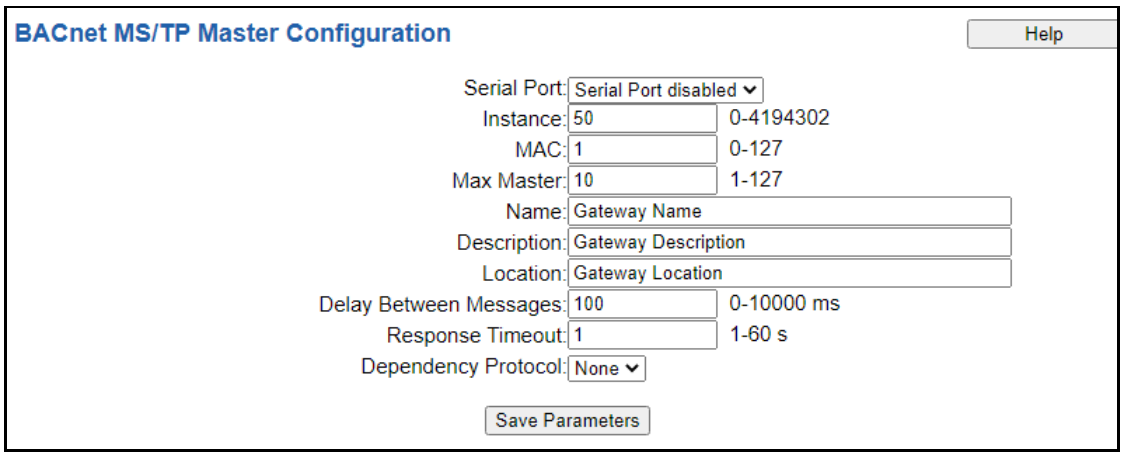
BACNet MS/TP Manager Configuration

Click the **BACnet MSTP Manager** button to access the configuration page.

1) **Serial Port**: Select which serial port is being used for communication. This port must be configured on the Port Configuration page. If it has not yet been configured, it will display *Disabled* after the Port description in this dropdown.



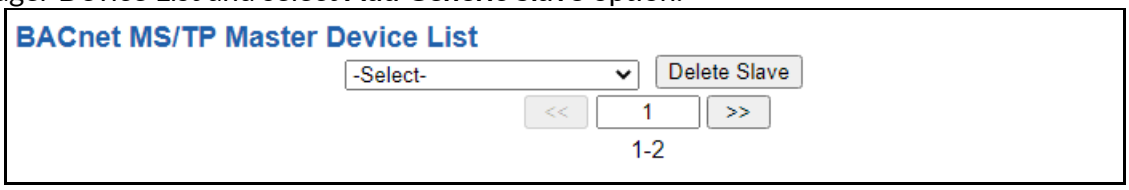
2) Enter a unique **Instance** identifier for the gateway. This Instance must be unique on the BACnet MS/TP network.
3) Enter a unique **MAC** identifier for the gateway. This MAC must be unique on the BACnet MS/TP network.
4) **Max Master**: Enter the maximum MAC ID that the gateway will communicate with on the BACnet MS/TP network. This value should be equal to or greater than the largest MAC ID on the MS/TP Network. The gateway cannot communicate with any MAC ID that is greater than the value entered in this field. In an ideal network, this should match the other devices on the BACnet MS/TP network.
5) Enter a **Name**, **Description** and **Location** for the gateway. These are used to identify the gateway on the BACnet MS/TP network.
6) **Delay Between Messages**: Enter the length of time to delay between read and write scan line requests (ms).
7) **Response Timeout**: Enter the amount of time the gateway should wait before a timeout is issued for a read/write request(s).
8) **Dependency Protocol**: If enabled, BACnet MS/TP communication will stop if communication to the selected protocol is lost.



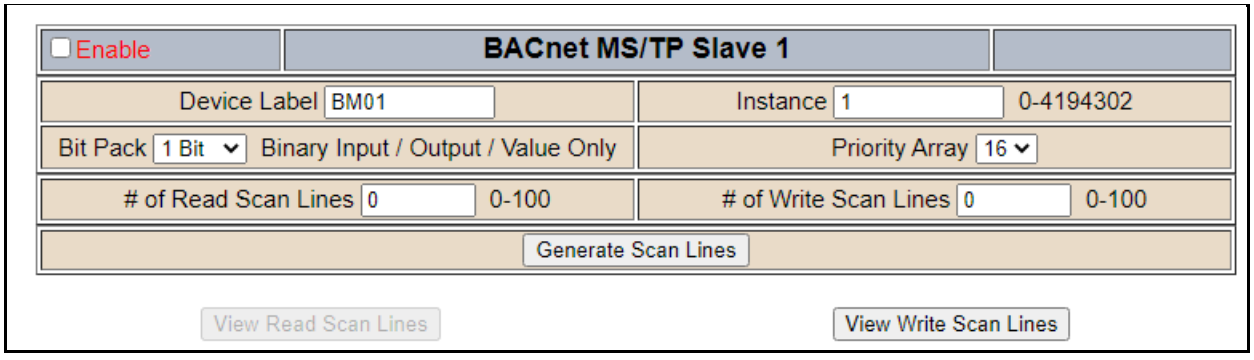
BACnet MS/TP Manager Device Configuration

The bottom area of the BACnet MS/TP Manager Configuration page lets you configure up to 32 external BACnet MS/TP devices.

1) To add additional Slave connections, click the -Select- dropdown menu under BACnet MS/TP Manager Device List and select **Add Generic Slave** option.



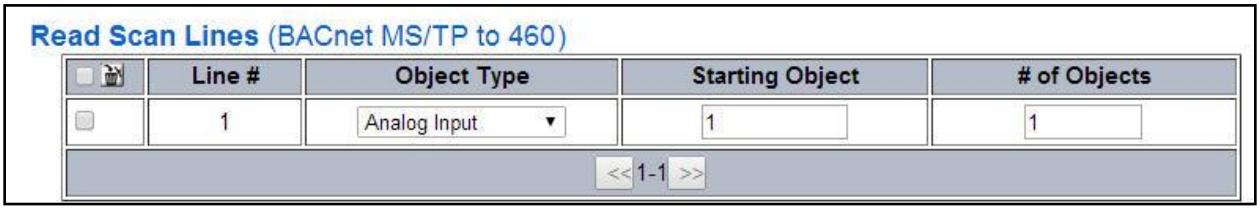
   a. If you are configuring multiple devices click **<<** or **>>** to navigate to another device.
   b. To create a new slave with the same parameters already configured from another slave, click the -Select- dropdown and select the **Add from BACnet MS/TP X** option (where X represents the slave you wish to copy parameters from). Once created, you can make any additional changes needed to that new slave.
   c. To remove a device, navigate to the slave to delete using the **<<** and **>>** buttons and click the **Delete Slave** button.
   d. Click **Save Parameters** to save your changes before a restart or going to another configuration page.
2) The **Enable** check box should be selected for the device.
3) Enter a **Device Label** to identify the device within the gateway.
4) Enter the unique **Instance** that matches the slave. If this value doesn't match, the gateway will timeout.
5) **Bit Pack:** Select the formatting of the Binary Input/Output/Value Objects. Automap will use this packing size to map binary objects to/from the other protocol. The bit pack selection here should match that of the other protocol. The starting address is considered Bit 0 and is the low-order bit.
6) **Priority Array:** Select the Priority Array index to use for the Writeable Commandable BACnet Objects.
7) Enter the number of Read Scan Lines and Write Scan Lines.
8) Click the **Generate Scan Lines** button to have the read and write scan lines auto-generate for you. You may manually configure the read and write scan lines after they have been generated.



Configuring Read Scan Lines

Follow these steps to manually configure Read Scan Lines.

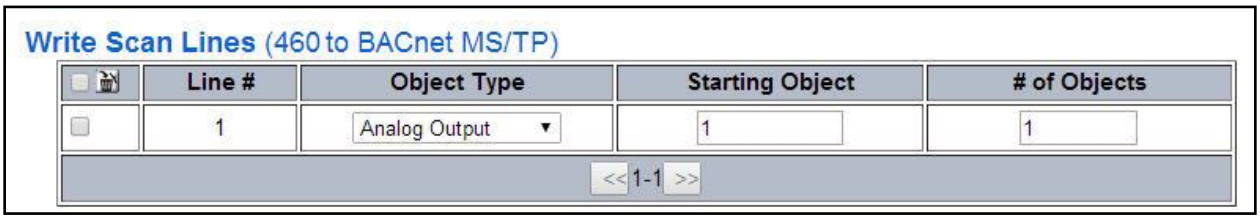
1) Select **View Read Scan Lines** if not already selected.
2) Select an Object Type for each Scan Line. Options include: Analog Input, Analog Output, Analog Value, Binary Input, Binary Output, Binary Value, and Multi-State Input, Multi-State Output, Multi-State Value, CSV (CharacterString Value).
3) Enter a Starting Object.
4) Enter the # of consecutive objects to read for that object type. You can enter a value of 1 to 128.



Configuring Writes Scan Lines

Follow these steps to manually configure Write Scan Lines.

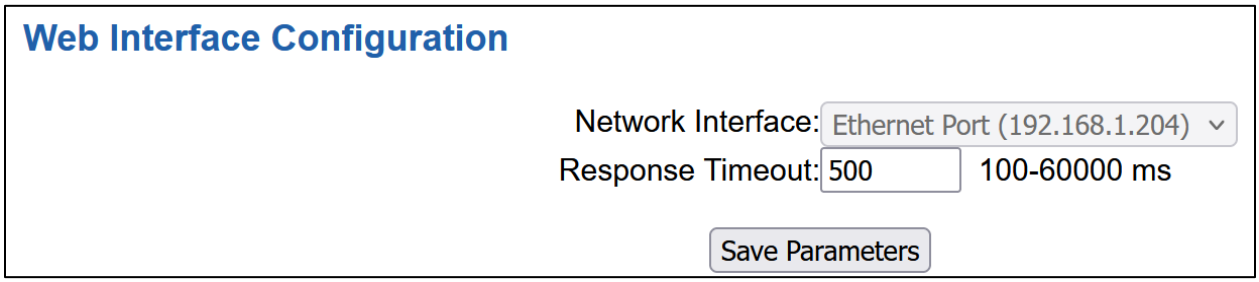
1) Select **View Write Scan Lines** if not already selected.
2) Select an Object Type for each Scan Line. Options include: Analog Output, Analog Value, Binary Output, Binary Value, Multi-State Output, Multi-State Value, and CSV (CharacterString Value).
3) Enter a Starting Object.
4) Enter the # of consecutive objects to write for that object type. You can enter a value of 1 to 128.



Web Interface Configuration

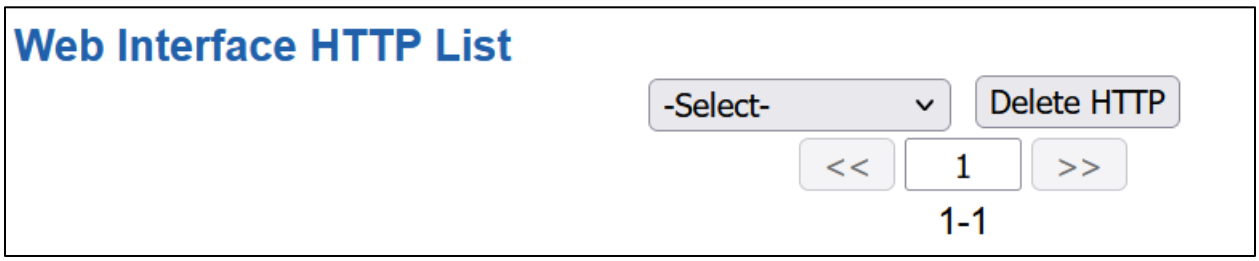
Click the **Web Interface** button to access the configuration page.

1) Select which **Network Interface** to use for the Web Interface.
2) Enter a **Response Timeout** in milliseconds.

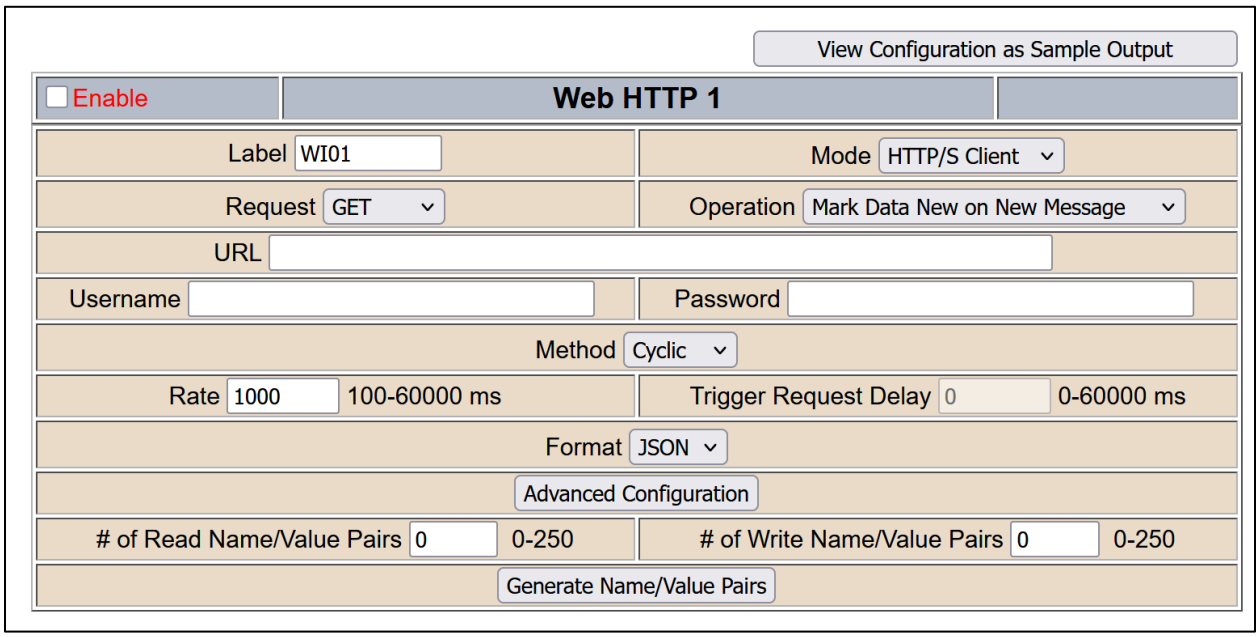


Web Interface Client/Server Configuration

The bottom area of the Web Interface Configuration page allows for the configuration of up to 20 HTTP/S Clients/Servers.



1. The -Select- dropdown under the Web Interface HTTP list can be used to add additional HTTP connections.
    a. **Add HTTP** – Adds a new unconfigured HTTP connection
    b. **Add From Web** – Adds a copy of an existing HTTP connection
2. When configuring multiple HTTP connections, the **<<** & **>>** buttons can be used to navigate between connections.
3. A HTTP connection can be removed by navigating to the connection using the **<<** & **>>** buttons and hitting the **Delete HTTP** button.
4. Click the **Save Parameters** button to save changes before restarting or going to another configuration page.



1. **Enable** – Enables/Disables communication for the selected connection.
2. **Label** – An internal label used when referencing the connection within the gateways configuration.
3. **Mode**
    a. **HTTP/S Client –** The connection will act as an HTTP/S client and make requests to the defined URL.
    b. **HTTP/S Server** – The connection will act as an HTTP/S server and receive requests at the defined URL.
4. **Request**
    a. **GET** – The connection will send/respond to HTTP GET requests.
    b. **POST** – The connection will send/respond to HTTP POST requests.
    c. **PUT** – The connection will send/respond to HTTP PUT requests.
    d. **DELETE** – The connection will send/respond to HTTP DELTE requests.
5. **Operation**
    a. **Mark Data New on Change of State** – Send data to the mating technology, on a per point basis, upon a change of state. For more explanation see the Operation Mode section below.
    b. **Mark Data New on New** Message – Send data to the mating technology for all data points, no matter change of state or not. For more explanation see the Operation Mode section below.
6. **URL**
    a. **Client** – When the connection mode is configured as HTTP/S client the URL is used to define the remote device and route to connect to.

    For example, http://192.168.1.100/Example will connect to that web route and communicate on port 80.

If a port other than 80 is desired this can be achieved by adding a colon followed by the desired port number to the defined URL: http://192.168.1.100:7777/Example

If HTTPS is desired this can be achieved by defining HTTPS in the request instead of HTTP. HTTPS will use port 443 by default unless another port is specified: https://192.168.1.100/Example
NOTE: HTTPS will not function unless HTTP Access is set to enable HTTPS in the gateways Security Configuration.

b. **Server** – When the connection mode is configured as HTTP/S server the URL is used to define the web route to be used for the connection on the gateway.

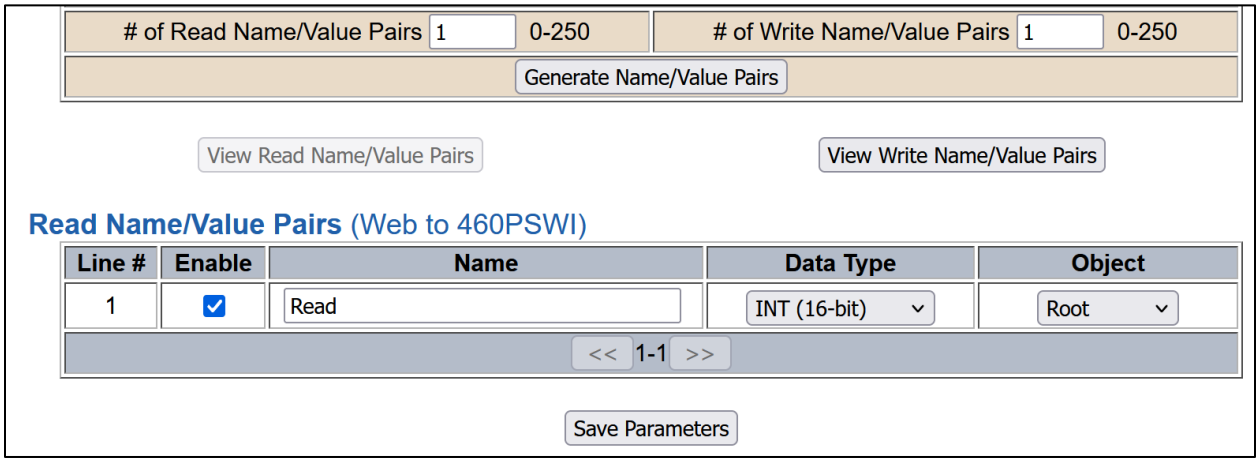
For example, configuring the URL as **/Example** will allow the gateway to receive requests at http://<Gateway_IP>/Example & https://<Gateway_IP>/Example.

User defined ports are not supported when operating as a server. Port 80 will be used for HTTP and port 443 will be used for HTTPS.

NOTE: HTTPS will not function unless HTTP Access is set to enable HTTPS in the gateways Security Configuration.

7. **Username** – Username to be used for basic auth when acting as a client and connecting to a remote server. Not used when acting as a server.
8. **Password** – Password to be used for basic auth when acting as a client and connecting to a remote server. Not used when acting as a server.
9. **Method** – The method to use when forwarding data as an HTTP Client. Not used when acting as a server.
    a. **Cyclic** – Send requests cyclically at the rate defined in the Rate configuration.
    b. **Triggered –** Send requests by incrementing a value from the mating technology.
10. **Rate** – The rate in milliseconds (ms) to cyclically make requests when using the cyclic method.
11. **Trigger Request Delay** – The maximum rate at which publishes can be triggered when using the triggered method. Set to 0 to disable.
12. **Format** – The data Format to be used for the payload.
13. **# of Read Name/Value Pairs** – The number of read Name/Value pairs to be configured.
14. **# of Write Name/Value Pairs** – The number of write Name/Value pairs to be configured.

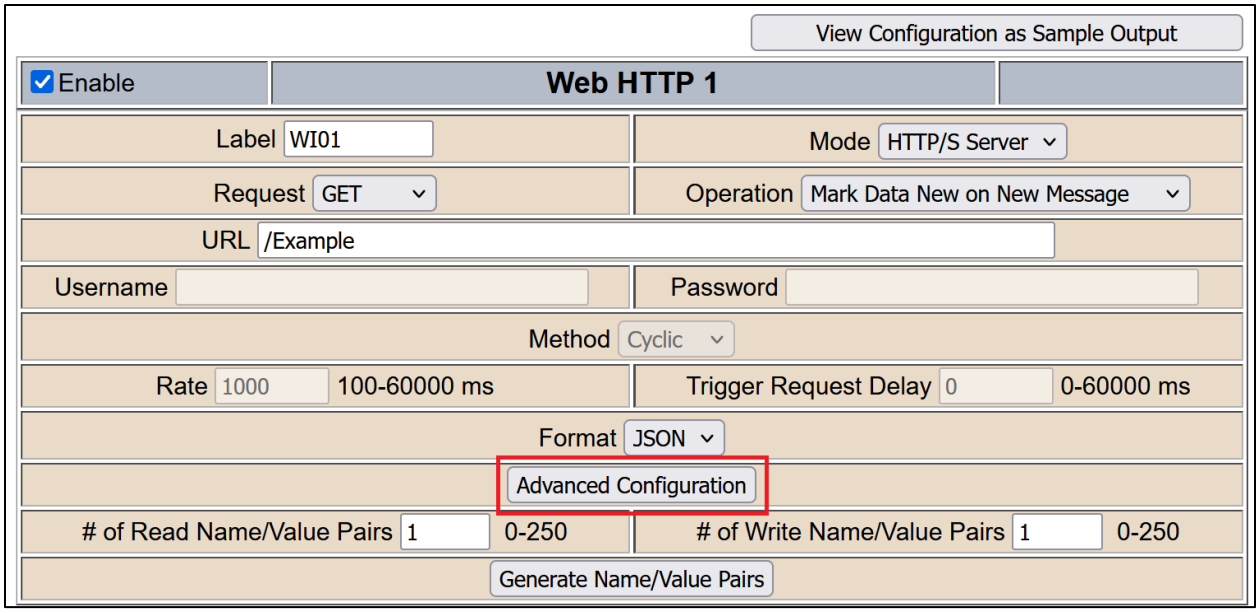
Web Interface Name/Value Pair Configuration



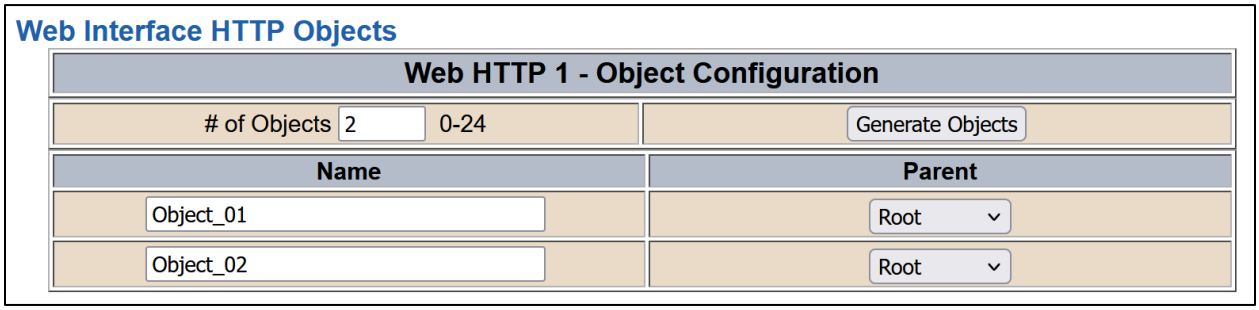
1. Configure **the # of Read Name/Value Pairs** & **# of Write Name/Value Paris** and hit the **Generate Name/Value Pairs** button to add them to the configuration.
2. Use the **View Read Name/Value Pairs** & **View Write Name/Value Pairs** buttons to switch between configuring Read/Write Name/Value Pairs.
3. Use the **Enable** checkbox to add/remove a Name/Value pair from the payload without removing the scanline.
4. Use the **Name** column to configure the Name for the Name/Value Pair.
5. Use the **Data Type** column to configure the data type for the Name/Value Pair.
6. Use the **Object** column to configure the object the Name/Value Pair should be contained within. For more information on this view the Web Interface Client/Server Configuration: Advanced Configuration section below.

Web Interface Client/Server Configuration: Advanced Configuration

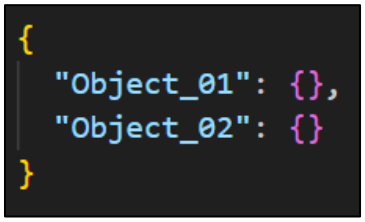
The HTTP/S connections advanced configuration can be accessed by clicking the Advanced Configuration button on the HTTP/S connections configuration window, outlined in red in the image below.



The advanced configuration is used to add additional structure to the payload by configuring objects that can be contained within the main payload object.



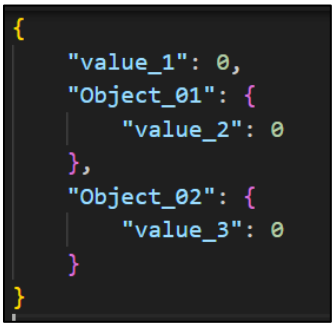
For example, in the image above there are two objects configured with a parent object of Root, which is the main payload object. This configuration would leave us with a base payload that looks like this:



Then Name/Value pairs can be associated with a specific object by using the Object column in the Name/Value Pairs configuration section as shown below.

Line #	Enable	Name	Data Type	Object
1	☑	value_1	INT (16-bit)	Root
2	☑	value_2	INT (16-bit)	Object_01
3	☑	value_3	INT (16-bit)	Object_02
<< 1-3 >>				

The configuration above would yield this JSON output:



When configuring the Objects in the advanced configuration the parent dropdown can be used to change which object is the parent to that object allowing for the creation of nested objects. In the example below the parent of Object_02 has been changed from root to Object_01.

Web Interface HTTP Objects

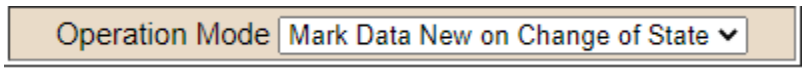
Web HTTP 1 - Object Configuration	
# of Objects 2 0-24	Generate Objects
Name	**Parent**
Object_01	Root
Object_02	Object_01

This will result in the following JSON payload:

Operation Mode

Mark Data New on Change of State (COS)

When data comes into the RTA gateway, it will be sent over to the matting protocol only if the data has a different value.

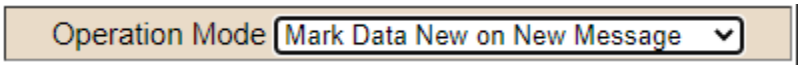


Example for 460ETCWI

Operator sends "HelloWorld" from the PLC. That data is gathered in the WI side of the RTA gateway and is processed and sent over to the web sever. Next time the operator sends the same data "HelloWorld". The WI side gathers the data, but the data didn't change so it will not be sent over to the WI portion of the RTA gateway. The operator sends "1234567890" from the PLC. The WI side of the RTA gateway will process the data and since the data has changed, it will be sent over to the web server.

Mark Data New on New Message

When data comes into the RTA gateway, it will be sent over to the mating protocol regardless if it's the same data. This allow you to send the same data over again to the mating protocol.



Example for ETCWI

Operator sends "HelloWorld" from the PLC. That data is gathered in the WI side of the RTA gateway and is processed and sent over to the web server. Next time the operator sends the same data "HelloWorld", the WI side gathers the data, processes it, then sends over to the web server. The operator sends "1234567890", the WI side of the RTA gateway will process the data and send it over to the web server.

Mapping - Transferring Data Between Devices

There are 5 ways to move data from one protocol to the other. You can combine any of the following options to customize your gateway as needed.

Option 1 – Data Auto-Configure Mappings: The gateway will automatically take the data type (excluding strings) from one protocol and look for the same data type defined in the other protocol. If there isn't a matching data type, the gateway will map the data to the largest available data type. See Data Auto-Configure section for more details.

Option 2 – String Auto-Configure: The gateway will automatically take the string data type from one protocol and map it into the other. See String Auto-Configure section for more details.

Option 3 – Manual Configure Mappings: If you don't want to use the Auto-Configure Mappings function, you must use the manual mapping feature to configure translations.

Option 4 – Manipulation/Scaling: You can customize your data by using math operations, scaling, or bit manipulation. See Data Mapping-Explanation section for more details.

Option 5 – Move Diagnostic Information: You can manually move diagnostic information from the gateway to either protocol. Diagnostic information is not mapped in Auto-Configure Mappings Mode. See Diagnostic Info section for more details.

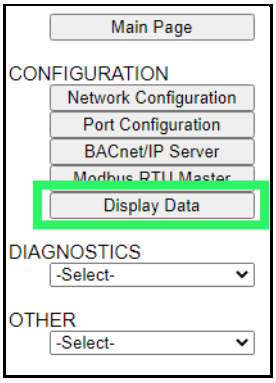
Display Mapping and Values

The Display Data and Display String pages are where you can view the actual data for each mapping that is set up.

Display Data

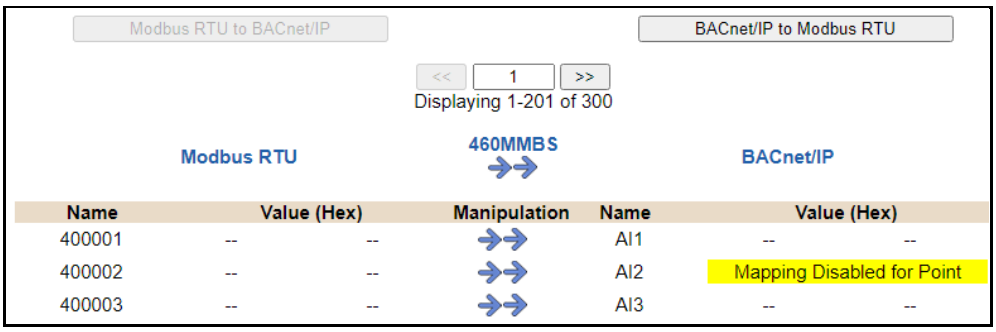
Click the **Display Data** button to view how the data is mapped and what the values of each mapping are.

Going from Manual Mapping to Auto-Mapping will delete ALL mappings and manipulations configured.



Here you will see how each data point (excluding strings) is mapped. To view, select the device from the dropdown menu and click **View** to generate the information regarding that device. Then select either the ***Protocol 1 to Protocol 2*** or ***Protocol 2 to Protocol 1*** button, correlating to the direction you wish to see the data.

This page is very useful when verifying that all data is mapped somehow from one protocol to another. If a data point is not mapped, it will display on this page in a yellow highlighted box. The Display Data page will display up to 200 mappings per page, simply navigate to the next page for the additional mapping to display.



In the above example, we see the following:

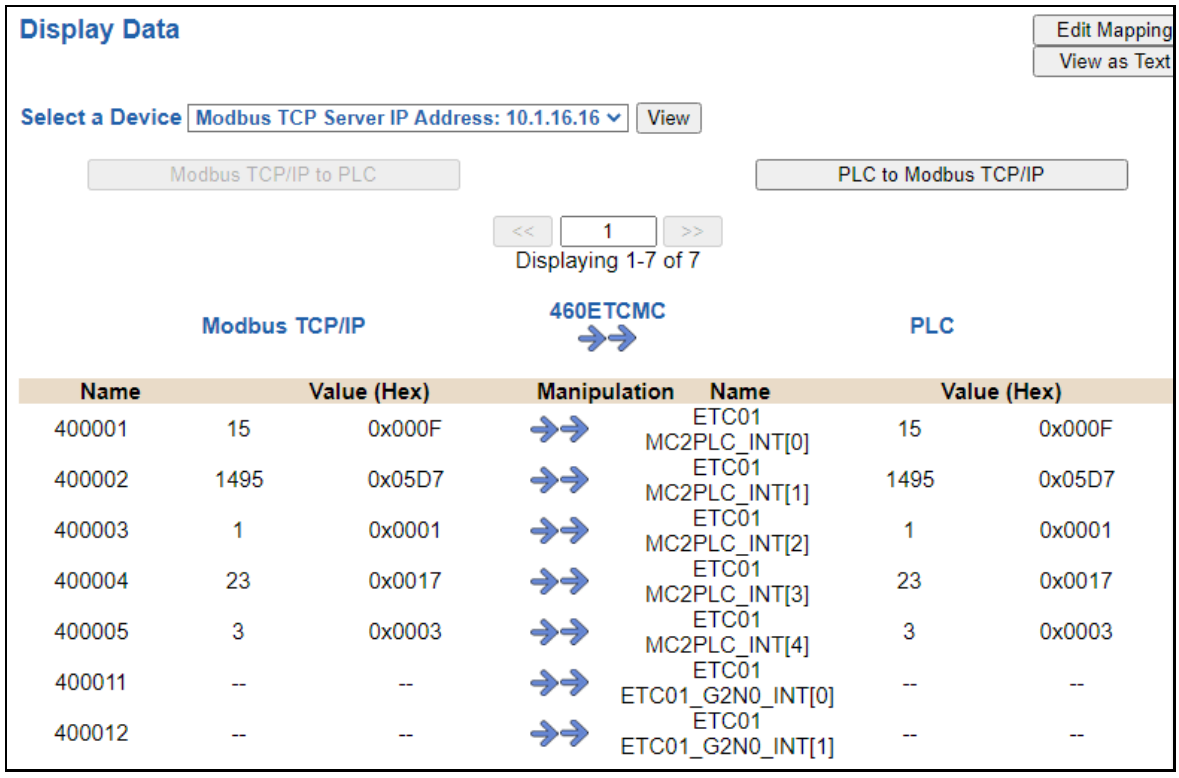
- Modbus register 400001 from Slave 1 is being mapped to AI1 on BACnet
- Nothing is being moved from Modbus register 400002 to AI2 on BACnet because the mapping is disabled
- Modbus register 400003 from Slave 1 is being mapped to AI3 on BACnet

NOTE: If a data point is mapped twice, only the first instance of it will show here. EX: If Modbus 400001 & 400040 from Slave 1 are both mapped to AI1, only 400001 will show as being mapped to AI1.

If there are values of "- - "on this page, it indicates that the source has not yet been validated and no data is being sent to the destination.

The example below reflects the Modbus to PLC flow of data. The Modbus (left side) is the source and the PLC (right side) is the destination.

- The 460 gateway has received valid responses from Modbus registers 400001- 400005 and therefore can pass the data on to the PLC tag called MC2PLC_INT.
- The 460 gateway has NOT received valid responses from Modbus register 400011 & 400012. As a result, the data cannot be passed to the PLC tag ETC01_GN0_INT2 and indicates so by using "- - "in the value column of the table.

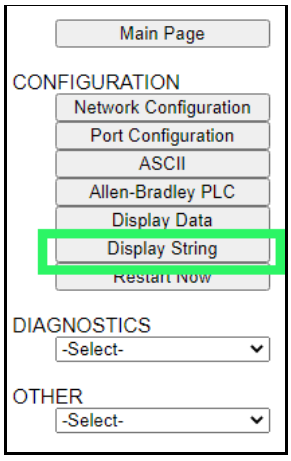


To view the actual data mappings, click the **Edit Mapping** button. For more details, see the Data Mapping-Explanation section.

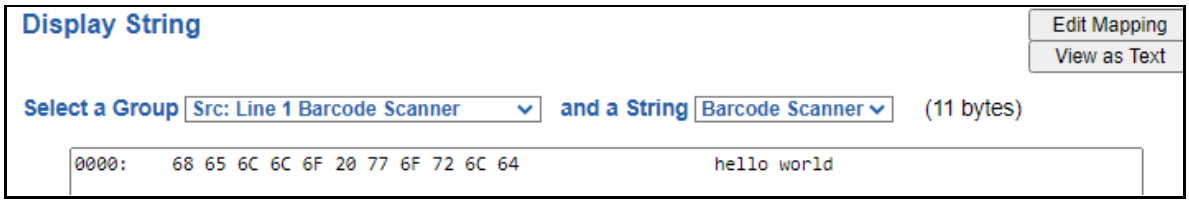
To view the data mappings purely as text, click the **View as Text** button. For more details, see the View Data Mapping as Text section.

Display String

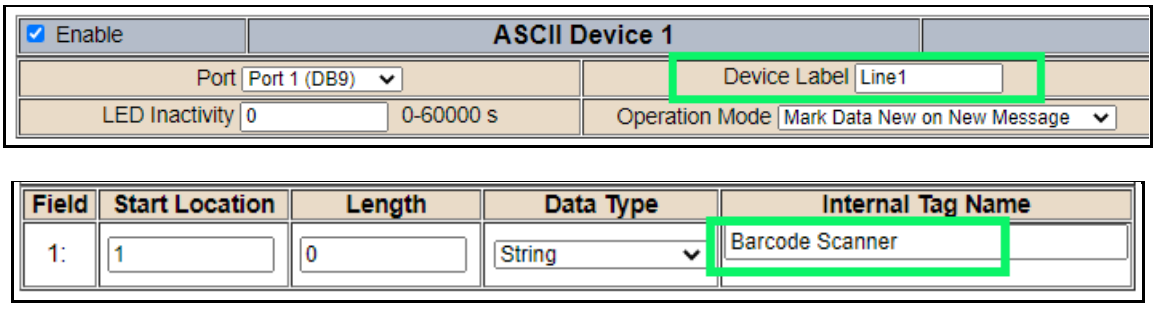
Click the **Display String** button to view what the values of each Parsing and/or Concatenating strings are, you can also click on the Edit Mapping to view the mapping of each string.



To view the source or destination groups from a string, click the dropdown menu to generate the information regarding that device. The string data will be displayed in both Hex and ASCII (only the ASCII data is sent). The example below shows data that is coming from the source device. A group will be displayed for each Parsing/Concatenating String field that is configured.

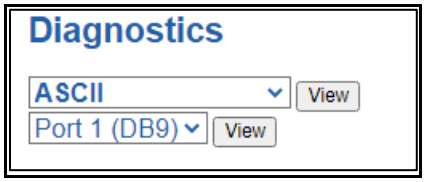


In the Group drop down, “Line1” is defined on the ASCII Device configuration page and “Barcode Scanner” is defined in the ASCII Parsing configuration.

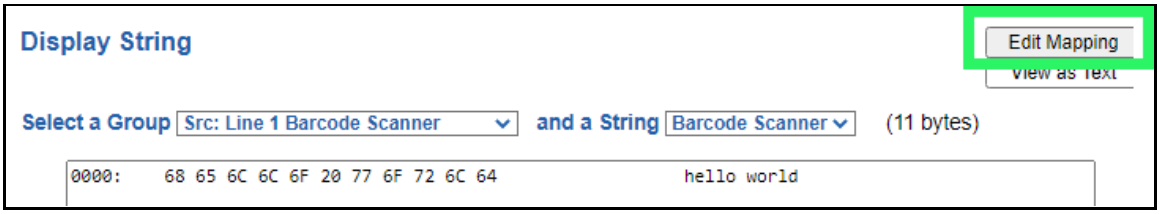


If there are values of “Data Not Valid “on this page, it indicates that the source has not been validated yet and no data is being sent to the destination.

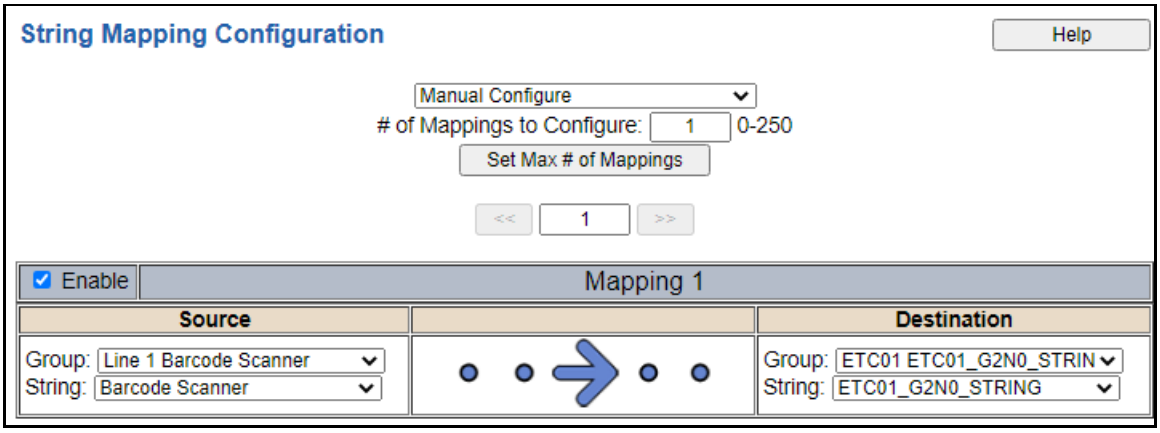
NOTE: You can view the whole string data by clicking on **Diagnostics Info** drop down and navigating to ASCII Diagnostics page. You will also have to select the port you want to view in the dropdown below ASCII.



To view the string mappings, click the **Edit Mapping** button. For more details see the **String Mapping-Explanation** section.



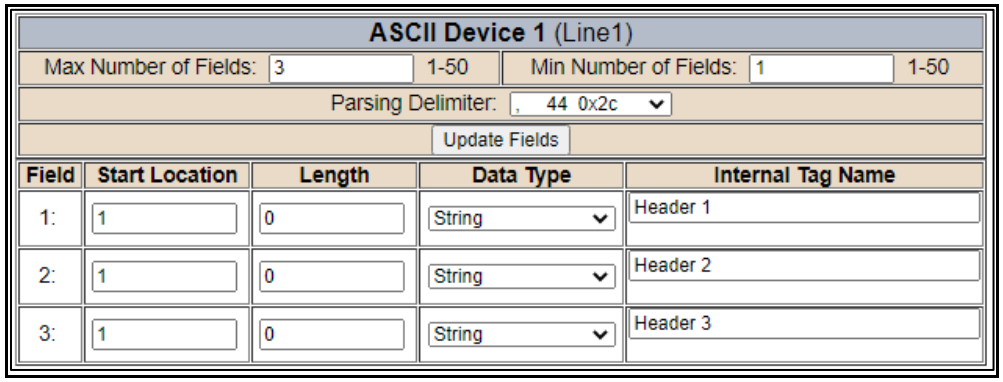
NOTE: Only String data types can be mapped to another String data type.



To view the string mappings purely as text, click the **View as Text** button. For more details see the **View String Mapping** as Text section.

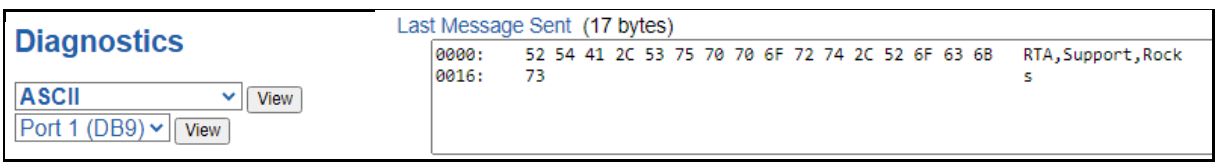
Display String use case

Sending a message of “RTA,Support,Rocks” from an ASCII device to the RTA unit. The ASCII Parsing Configuration would look like my example below. There are more detailed examples of what all the fields represent in the ASCII Parsing section.



The message is broken up into 3 “Groups” or Parsing fields.

To view the Entire message, click on the Diagnostic drop down, select Diagnostics Info. Select ASCII, click view, select your Port. Whole data will be in the Last Message Sent Diagnostic box.



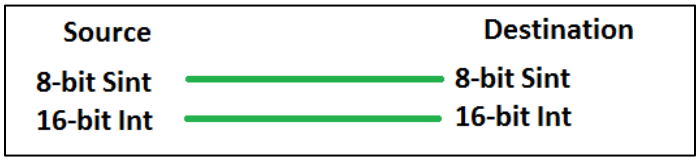
Data and String Mapping – Auto-Configure

The Auto-Configure function looks at both protocols and will map the data between the two protocols as best as it can so that all data is mapped. Inputs of like data types will map to outputs of the other protocols like data types first. If a matching data type cannot be found, then the largest available data type will be used. Only when there is no other option is data truncated and mapped into a smaller data type.

If the Auto-Configure function does not map the data as you want or you want to add/modify the mappings, you may do so by going into Manual Configure mode.

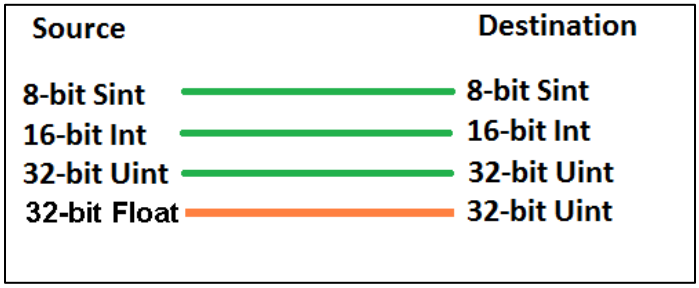
The following are examples of the Auto-Configure function.

1) This example shows a common valid setup.



   a. Both Source values were able to be mapped to a corresponding Destination value.

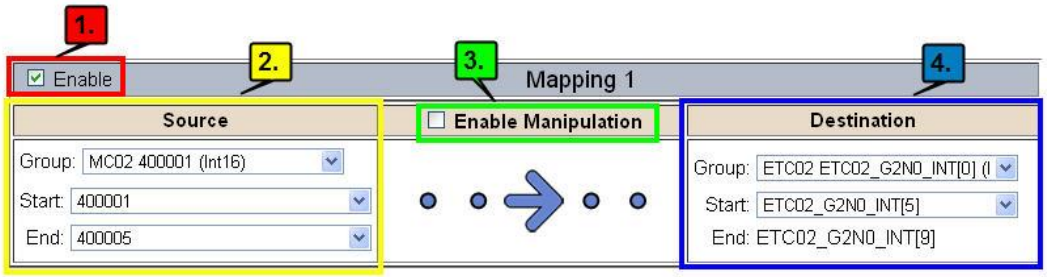
2) This example shows how Auto-Configure will make its best guess.



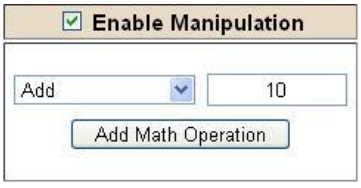
   a. The 32-bit Float from the Source location could not find a matching Destination data-type. After all other like data types were mapped, the only data type available was the 2nd 32-bit Uint data type. Auto-Configure was completed even though the data in the Float will be truncated.

Data Mapping – Explanation

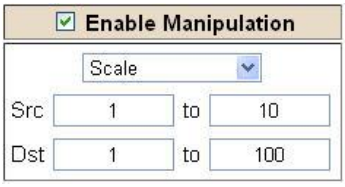
Below are the different parts that can be modified to make up a data mapping.



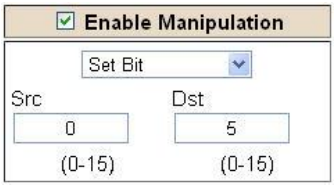
1) Enable (red box above): Check to enable mapping. If not checked, this mapping is skipped.
2) Source Field (yellow box above):
   a) Group - Select the data group you set up in the protocol config to use for this mapping.
   b) Start - This is the starting point for this mapping.
   c) End - This is the final point to be included for this mapping.
3) Manipulation Area (green box above):
   a) Enable the Data Manipulation. This can be enabled for any mapping.
   b) Click **Add Math Operation** for each operation needed. Up to 3 are allowed unless you are using the Scale, Set Bit, or Invert Bit functions. If using Scale, Set Bit, or Invert Bit, then only 1 operation is allowed.
   c) Select the Operation(s) to perform.
      i) Math Operations are performed in the order they are selected.
      ii) If more than one point is selected on the source, the Math Operations will be performed on every point.
   d) Enter the value(s) for the operation.



Example of Add (similar for Subtract, Multiple, Divide, and MOD). This will add a value of 10 to the source field before it is written to the destination field.



Example of Scale. This will scale the source values from 1-10 into 1-100 for the destination.



Example of Set Bit (similar to Invert Bit). This will take the value of the 0th source bit and copy it into the value of the 5th destination bit.

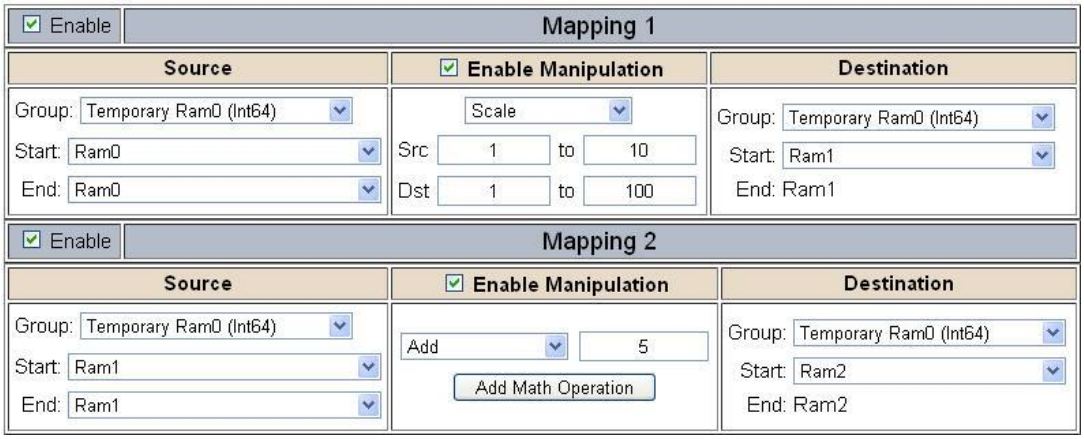
4) Destination Field (blue box above):
   a) Group - Select the data group you set up in the protocol config to use for this mapping.
   b) Start - This is the starting point for where the data is being stored.
   c) End - The End point is derived from the length of the source and cannot be modified.

Data Mapping – Adding Diagnostic Information

Data Mapping offers 5 different types of information in addition to any scan lines specified for each protocol.

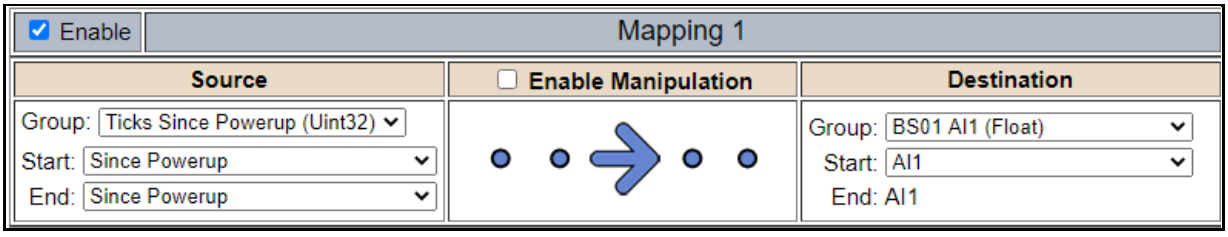
IMPORTANT NOTE: Only add Diagnostic Information **AFTER** both sides of the gateway have been configured. If changes to either protocol are made after diagnostic information has been added to the mapping table, it is necessary to verify all mappings. Remapping may be

1) **Temporary Ram (Int64)**
   a) This offers five levels of 64bit Integer space to assist in multiple stages of math operations. For example, you may wish to scale and then add 5. You can set up a single translation to scale with the destination as the temporary ram. Then another translation to add 5 with the source as the temporary ram.
   b) The gateway will automatically convert the Source to fit the Destination, so there is no need for Int 8, 16, 32 since the 64 may be used for any case.

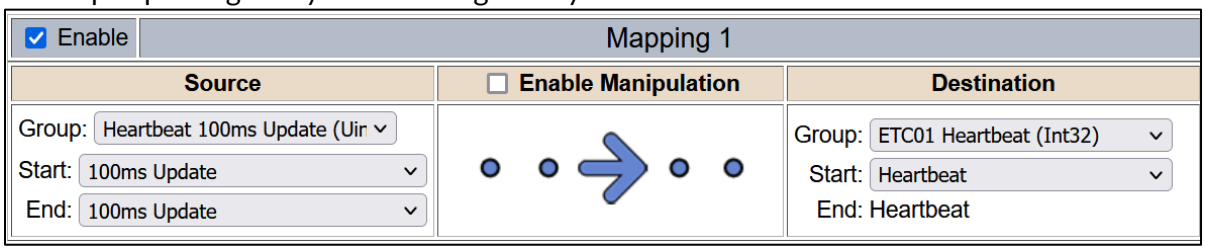


In this example, Ram0 is scaled into Ram1. Ram1 is then increased by 5 and stored into Ram2. Ram0 and Ram2 could be considered a source or destination group.

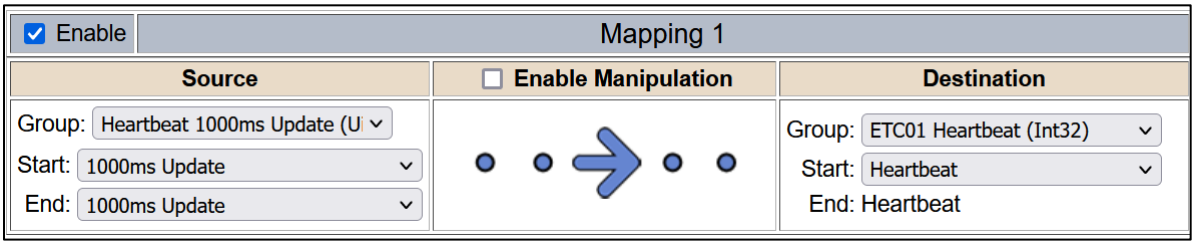
2) **Temporary Ram (Double)**
   a) This is like the Temporary Ram (Int 64), except manipulations will be conducted against the 64bit floating point to allow for large data.
3) **Ticks Per Second**
   a) The gateway operates at 200 ticks per second. This equates to one tick every 5ms. Thus, mapping this to a destination will give easy confirmation of data flow without involving one of the two protocols. If data stops on the destination end, then the RTA is offline.



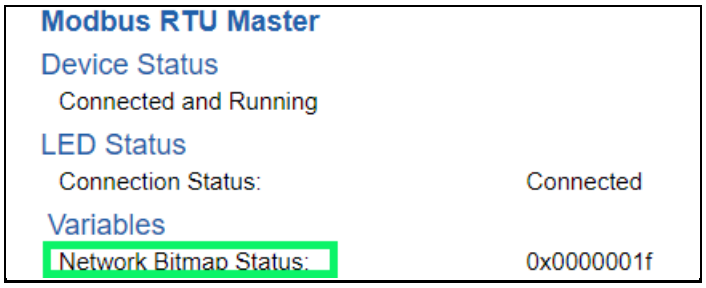
4) **Heartbeat 100ms Update**
   a) The Heartbeat 100ms Update variable can be used as a heartbeat that updates once every 100ms. The variable starts at 0 on gateway startup and increments by 1 every 100ms. This can be mapped into a destination on one of the available protocols to monitor the gateways connection status. If the value stops updating every 100ms the gateway is offline.



5) **Heartbeat 1000ms Update**
   a) The Heartbeat 1000ms Update variable can be used as a heartbeat that updates once every 1000ms. The variable starts at 0 on gateway startup and increments by 1 every 1000ms. This can be mapped into a destination on one of the available protocols to monitor the gateways connection status. If the value stops updating every 1000ms the gateway is offline.



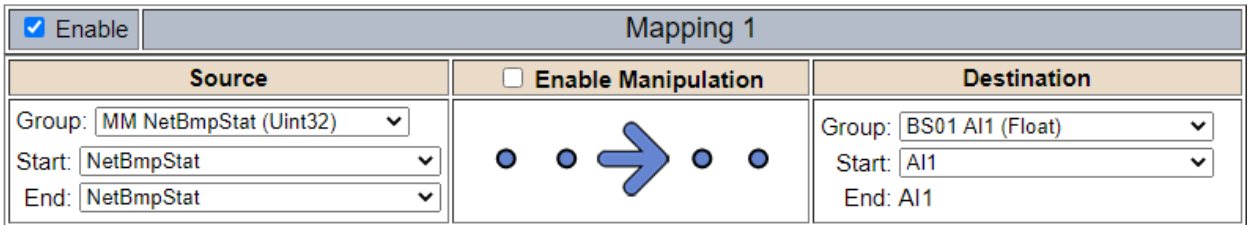
6) **XY_NetBmpStat**
   a) If a protocol is a Client/Master, there is a Network Bitmap Status that is provided on the Diagnostics Info page under the Variables section.



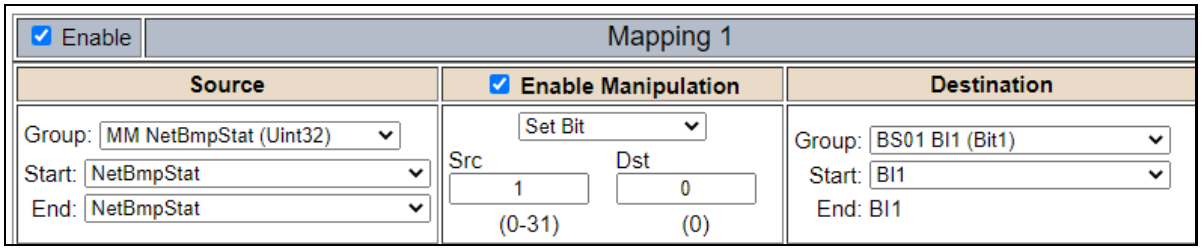
   b) Since a Client/Master may be trying to communicate with multiple devices on the network, it may be beneficial to know if a Server/Slave device is down. By using this Network Bitmap Status, you can expose the connection statuses of individual devices. **Values shown are in HEX.**
      i) 0x00000002 shows that only device 2 is connected
      ii) 0x00000003 shows that only devices 1 and 2 are connected
      iii) 0x0000001f shows that all 5 devices are connected (shown in image above)

c) There are multiple ways to map the NetBmpStat.

Option 1: Map the whole 32bit value to a destination. Example below shows the NetBmpStat is going to an Analog BACnet object. Using a connection of 5 Modbus Slave devices AI1 will show a value of 31.0000. Open a calculator with programmer mode and type in 31, this will represent bits 0 – 4 are on. This mean all 5 devices are connected and running.
If using an AB PLC with a Tag defined as a Dint, then expand the tag within your RSlogix software to expose the bit level and define each bit as a description such as device1, device2, etc.



Option 2: You can extract individual bits from the NetBmpStat by using the Set Bit Manipulation and map those to a destination. You'll need a mapping for each device you want to monitor. Example below shows Modbus device 2 (out of 5) is being monitor to a BACnet Binary Object. You can define the object in the BACnet Name configuration.



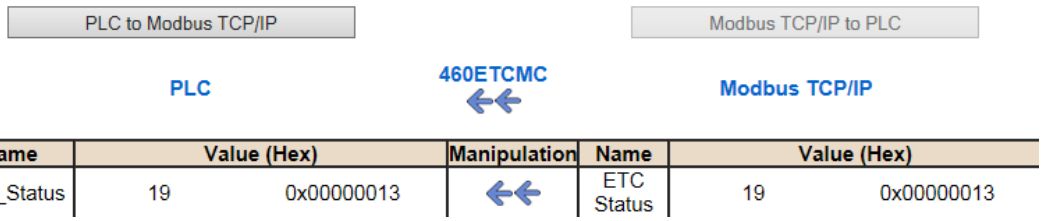
7) **Status_XY**

a) There are two Statuses provided, one for each protocol. This gives access to the overall status of that Protocol. Each Bit has its own meaning as follows:

Common Status: 0x000000FF (bit 0-7)1st byte

Hex:	Bit Position:	Decimal:	Explanation:
0x00	0	0	if we are a Slave/Server
0x01	0	1	if we are a Master/Client
0x02	1	2	connected (0 not connected)
0x04	2	4	first time scan
0x08	3	8	idle (usually added to connected)
0x10	4	16	running (usually added to connected)
0x20	5	32	bit not used
0x40	6	64	recoverable fault
0x80	7	128	nonrecoverable fault

For this example, the ETC Status is mapped to a PLC tag called PLC_Status



Name	Value (Hex)		Manipulation	Name	Value (Hex)	
PLC_Status	19	0x00000013		ETC Status	19	0x00000013

Example: ETC Status is 0x00000013 (19 decimal), here is the break down

Hex	Bit	Decimal	Explanation
0x01	0(on)	1	if we are a Master/Client
0x02	1(on)	2	connected (0 not connected)
0x10	4(on)	16	running (usually added to connected)
Total:	0x13	19	

External Faults: 0x0000FF00 (bit 8-15)2nd byte

Hex:	Bit Position:	Decimal:	Explanation:
0x00	8	0	local control
0x01	8	256	remotely idle
0x02	9	512	remotely faulted
0x04	10	1,024	idle due to dependency
0x08	11	2,048	faulted due to dependency

Recoverable Faults: 0x00FF0000 (bit 16-23)3rd byte

Hex:	Bit Position:	Decimal:	Explanation:
0x01	16	65,536	recoverable fault - timed out
0x02	17	131,072	recoverable fault - Slave err

Non-Recoverable Faults 0xFF000000 (bit 24-31) 4th byte

Hex:	Bit Position:	Decimal:	Explanation:
0x01	24	16,777,216	nonrecoverable fault – task fatal err
0x02	25	33,554,432	nonrecoverable fault – config missing
0x04	26	67,108,864	nonrecoverable fault – bad hardware port
0x08	27	134,217,728	nonrecoverable fault – config err
0x10	28	268,435,456	Configuration Mode
0x20	29	536,870,912	No Ethernet Cable Plugged In

For this example, the MC Status is mapped to a PLC tag called MC_Status

PLC to Modbus TCP/IP Modbus TCP/IP to PLC

PLC 460ETCMC Modbus TCP/IP

Name	Value (Hex)		Manipulation	Name	Value (Hex)	
MC_Status	65601	0x00010041	⇐⇐	MC Status	65601	0x00010041

Example: MC Status is 0x00010041 (65601 decimal), here is the break down, we know that bytes 1 and 3 are being used, so here is the break down,

Common Status:

Hex:	Bit:	Decimal:	Explanation:
0x01	0(on)	1	if we are a Master/Client
0x40	6(on)	64	recoverable fault

Recoverable Faults:

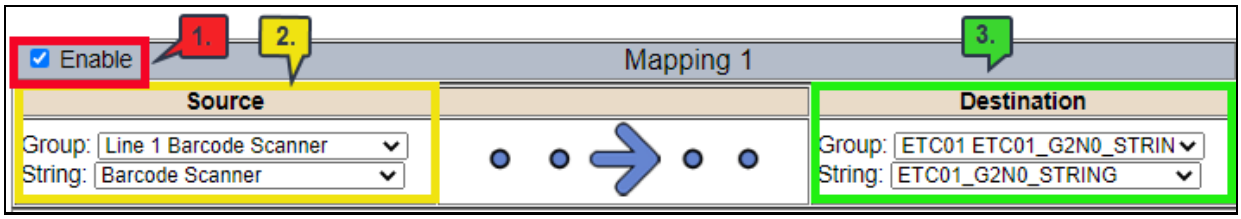
Hex:	Bit:	Decimal:	Explanation:
0x01	16	65,536	recoverable fault – timed

Total:	0x010041	65,601

String Mapping – Explanation

Below are the different parts that can be modified to make up a string mapping.

String data types can only be mapped to other string data types. There is no manipulation that can be done on the string.

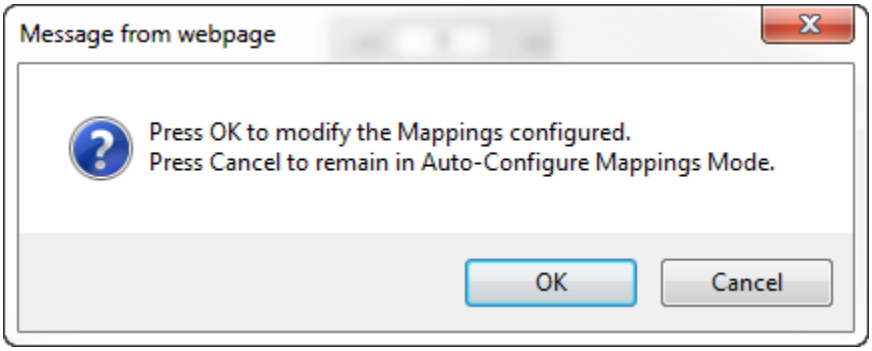


1) Enable (red box above): Check to enable mapping. If not checked, this mapping is skipped.
2) Source Field (yellow box above):
   a) Group - Select the string data group you set up in the protocol config to use for this mapping.
   b) String - This is the string used for this mapping.
3) Destination Field (green box above):
   a) Group - Select the string data group you set up in the protocol config to use for this mapping.
   b) String - This is the string where the data is being stored.

Mapping – Auto-Configure Mode to Manual Configure Mode

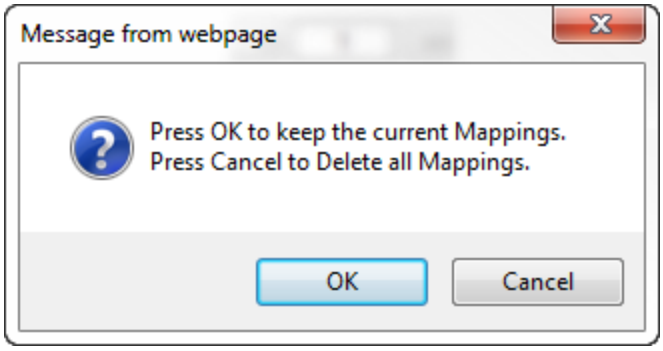
To transition from Auto-Configure Mapping Mode to Manual Configure Mode, click the dropdown at the top of the Mapping Configuration page and select Manual Configure.

After you click this button, you will be prompted to confirm if this is really what you want to do.



Click **OK** to proceed to Manual Configure Mode or click **Cancel** to remain in Auto-Configure Mappings Mode.

Once OK is clicked, there are 2 options on how to proceed from here.

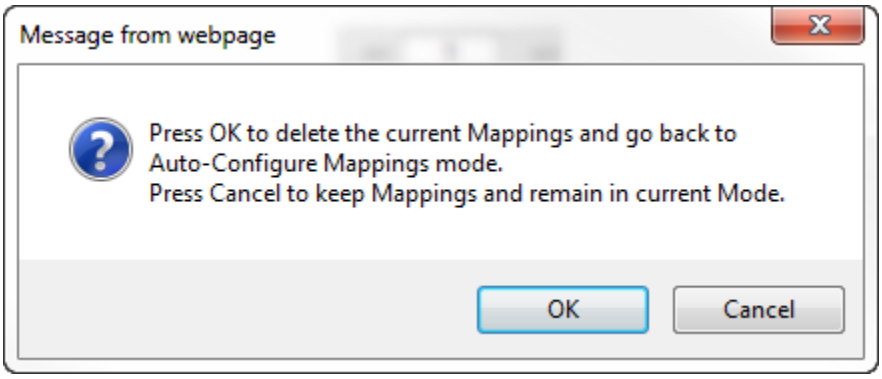


1) To keep the mappings that are already configured press **OK**.
    a) You would want this option if you are adding additional mappings or you want to modify the mapping(s) that already exist.
2) To delete the mappings that are already there and start over press **Cancel**.

To modify the number of mappings, enter a number in the text field next to **# of Mappings to Configure** and click the **Set Max # of Mappings** button. You can always add more mappings if needed.

Mapping – Manual Configure Mode to Auto-Configure Mode

To transition from Manual Configure Mode to Auto-Configure Mapping Mode, click the dropdown menu at the top of the Mapping Configuration page and select Auto-Configure Mappings.



Click **OK** to proceed to delete all current mappings and go back to Auto-Configure Mappings Mode. Click **Cancel** to keep all mappings and remain in Manual Configure Mode.

NOTE: Once you revert to Auto-Configure Mapping Mode there is no way to recover the mappings you lost. Any mappings you previously have added will be deleted as well.

View as Text

Data Mapping

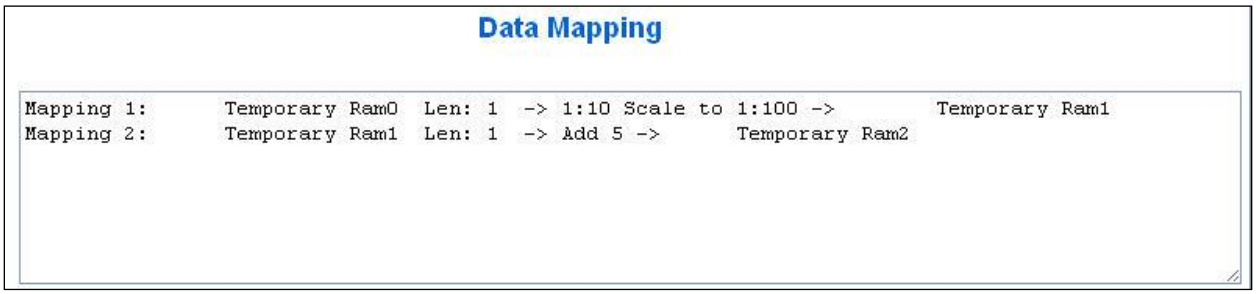
The View as Text page displays the point to point mapping(s) you set up in the Data Mapping section. This will also display any manipulation(s) that are configured.

Each line on this page will read as follows:

> **Mapping** *number*: *source point* **Len:** *Number of points mapped* **->** *manipulation (if blank then no manipulation)* **->** *destination point*

If you are looking for a specific point to see if it is mapped, you can do a find in this text box for your point in question. Example: you defined 20 Registers starting at register 1 and want to see if 400011 is mapped. If it is not in this text box, then it is not mapped, and no data will be transferred.

This is the text display for the example shown under the *Data Mapping- Adding Diagnostic Information* section.



String Mapping

The View as Text page displays the string mapping(s) you set up in the String Mapping section.

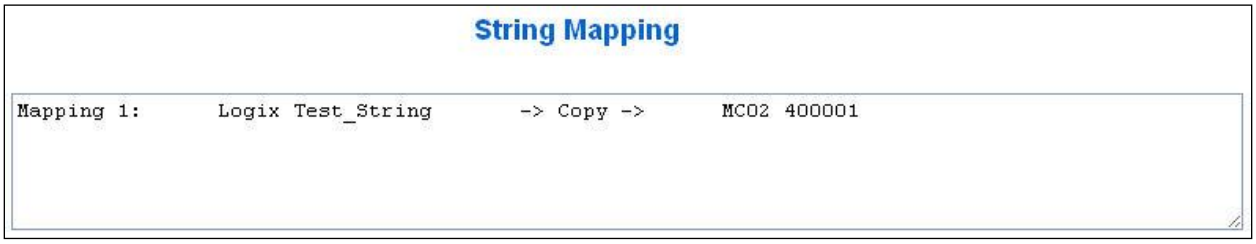
Each line on this page will read as follows:

> **Mapping** *number*: *source point* **-> Copy ->** *destination point*

If you are looking for a specific point to see if it is mapped, you can do a find in this text box for your point in question. Example: you defined 20 String Tags in the PLC and want to see if "Test_String" in the Logix PLC is mapped. If it is not in this text box, then it is not mapped, and no data will be transferred.

String Mapping

```
Mapping 1:      Logix Test_String       -> Copy ->      MC02 400001
```



Base Triggering – Data Validiation Triggering

With Base Triggering, you will be marking data as "Invalid" and force RTA Master/Controller/Client protocols to read all the read data points sources until ALL source protocols data is valid. You will be able to utilize the Handshake to map over to Technology Trigger and/or back over to your source protocol for reference.

How does this work?

1) Map the Triggering Variable (Source) over to Trigger **#** (Dest).
2) If Trigger **#** value changes states mark all Trigger **#** protocols read data as "Invalid".
3) Read all source read data points until ALL source read data is valid.
4) Handshake **#** value is set equal to Trigger **#** value.
5) Map Handshake **#** to reference data point.
   Note: **#** is an internal reference to the Server/Slave number you are settings up. **ex**. RTA Server/Slave products can only be Trigger 1 and Handshake 1 since we are only 1 device. If RTA is a Master/Client, then you can have a Trigger# for each server/slave connected too.

How do you set this up?

In this example I'm using a 460MCBS. My Building Automation System wants to verify that all data read from Modbus TCP/IP Server is valid.

1) Add an extra Analog Output for your Trigger. This tells the RTA to mark all data invalid.

Write Data Groups (BACnet/IP to 460MCBS)

Data Group	Object Type	Starting Object	# of Objects
1	Analog Output (32 Bit Float)	1	21
2	Binary Output	1	0
3	CharacterString Value	51	0

   a) You can define AI21 as your validation name in the Setup BACnet Names Configuration.

Setup BACnet Names, Units, and COV

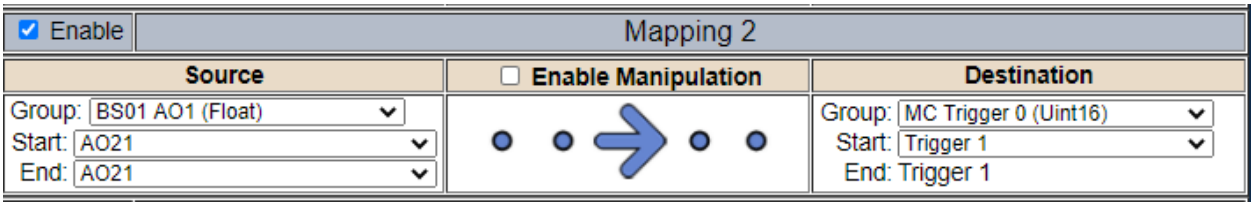
21	G01	Data Validation Trigger	Other	no-units	1.000000

2) Add another Analog Input as reference for when data has been validated. When you write from AO21 to validate data, the RTA will reply to AI40 saying "validation complete".

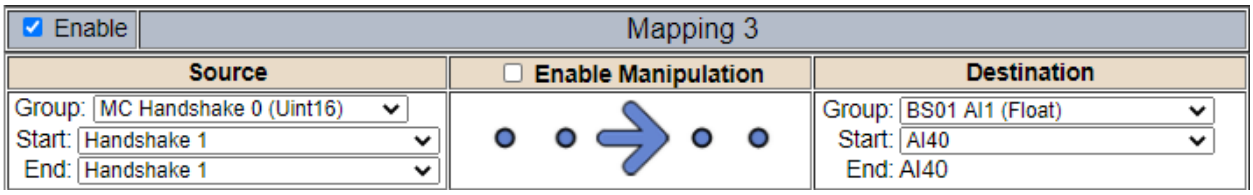
Data Group	Object Type	Starting Object	# of Objects
1	Analog Input (32 Bit Float)	1	40
2	Binary Input	1	0
3	CharacterString Value	1	0

40	G01	Data Validation Result	Other	no-units	1.000000

3) Within the Data Mapping page manually add 2 additional mappings.
4) The first mapping is going to be the Data Validation Triggering. AO21 will write to the RTA, MC Trigger 1 will mark data invalid.



5) The second mapping, the MC Handshake will increment that all data is validated and write to AI21 “all data is validated”. The value of AI40 and AO21 should be the same.



Security Configuration

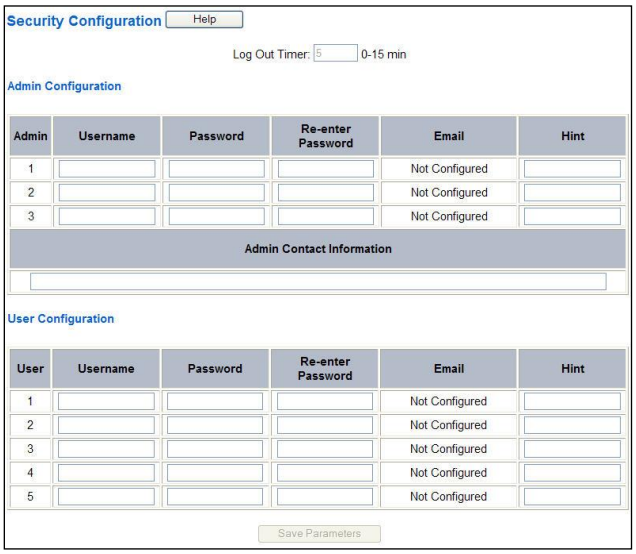
To setup security on the 460 gateway, navigate to **Other->Security Configuration**. You can configure Security for 3 administrators, 5 users, and 1 guest.

THIS IS NOT A TOTAL SECURITY FEATURE

The security feature offers a way to password protect access to diagnostics and configuration on the network. The security feature does not protect against "Air Gap" threats. If the gateway can be physically accessed, security can be reset. All security can be disabled if physical contact can be made. From the login page, click the Reset Password button twice. You will be forced to do a hard reboot (power down) on the gateway within 15 minutes of clicking the button. This process should be used in the

Note: Only Admins have configuration access to all web pages.

1) Log Out Timer: The system will automatically log inactive users off after this period of time. **NOTE**: A time of 0 means that the user will not be automatically logged off. Instead, they must manually click the **Logout** button.
2) Username: Enter a username, max of 32 characters.
3) Password: Enter a password for the username, max of 32 characters, case sensitive.
    a. Re-enter the Password
4) E-mail: In case the password was forgotten, a user can have their password e-mailed to them if e-mail was configured.
5) Hint: A helpful reminder of what the password is.



Security Configuration-Security Levels

Each webpage in the gateway can have a separate security level associated with it for each user.

Security Levels:

1) **Full Access**: Capability to view and configure a web page.
2) **View Access**: Capability to view a web page, but cannot configure parameters.
3) **No Access**: No capability of viewing the web page and page will be removed from Navigation.

Security - Log In

Username: Name of the user to login.

Password: Password of the user to login.

Log In: If login is successful, the user will be redirected to the Main Page.

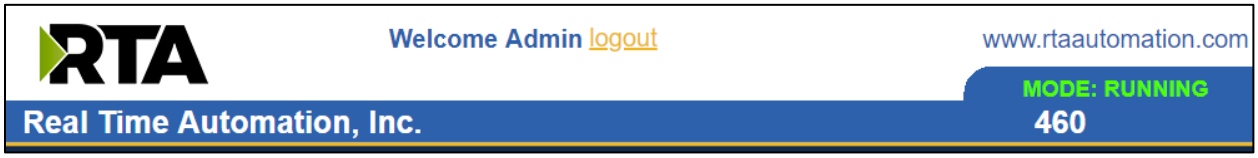
Send Password to Email: Sends the specified User's Password to the email configured for that user.

Display Hint: Displays the hint specified for the User if one was set up.

Reset Password: This is used to reset security settings. Confirm reset password must be selected to confirm this action. Once confirmed, there is a 15 minute window to do a hard reset of the gateway by physically removing and restoring power from the gateway. Once power is restored, you may navigate to the IP address of the gateway as normal.

Security - Log Out

Once a user is done with a session they may click **logout** at the top of any page. The user may also be logged out for inactivity based off of the Log Out Timer specified during the configuration.



Closing the browser is not sufficient to log out.

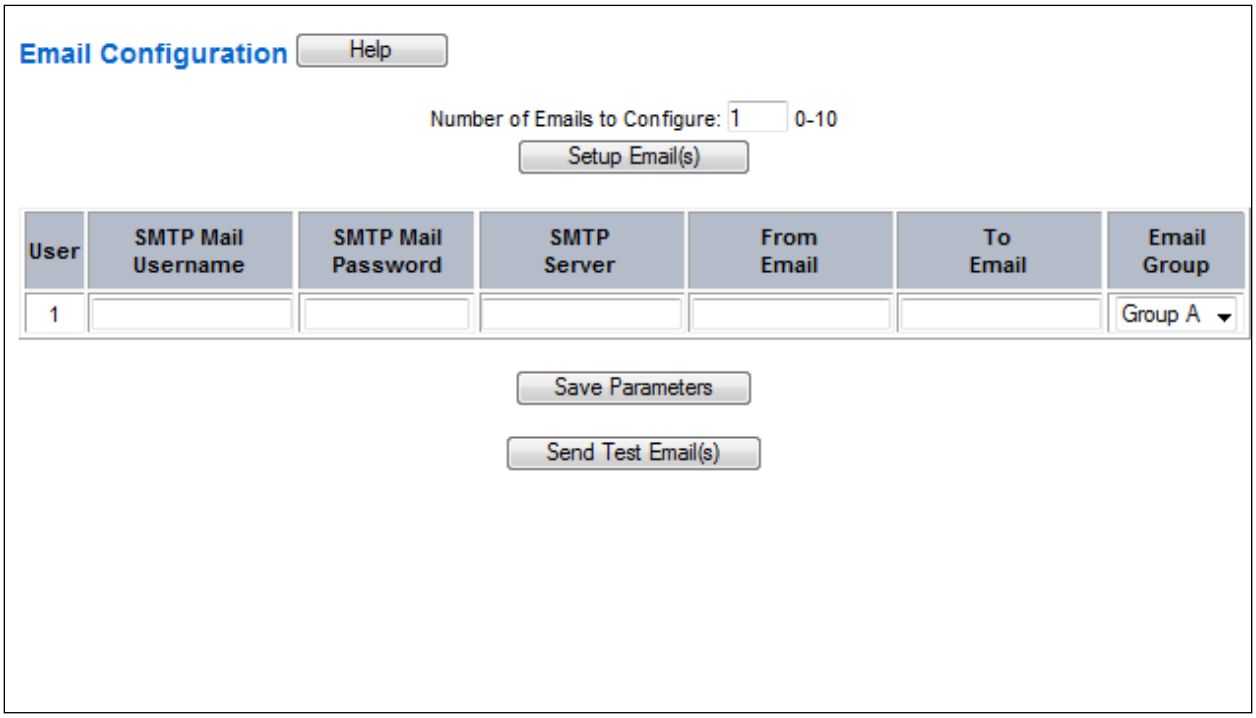
Email Configuration

To setup e-mails on the 460 gateway, navigate to **Other->Email Configuration**.

You can configure up to 10 email addresses.

1) SMTP Mail Username: The email address that the SMTP server has set up to use.
2) SMTP Mail Password: If authentication is required, enter the SMTP Server's password (Optional).
3) SMTP Server: Enter the Name of the SMTP Server or the IP Address of the Server.
4) From E-mail: Enter the e-mail that will show up as the sender.
5) To E-mail: Enter the e-mail that is to receive the e-mail.
6) E-mail Group: Choose a group for the user. This is used in other web pages.

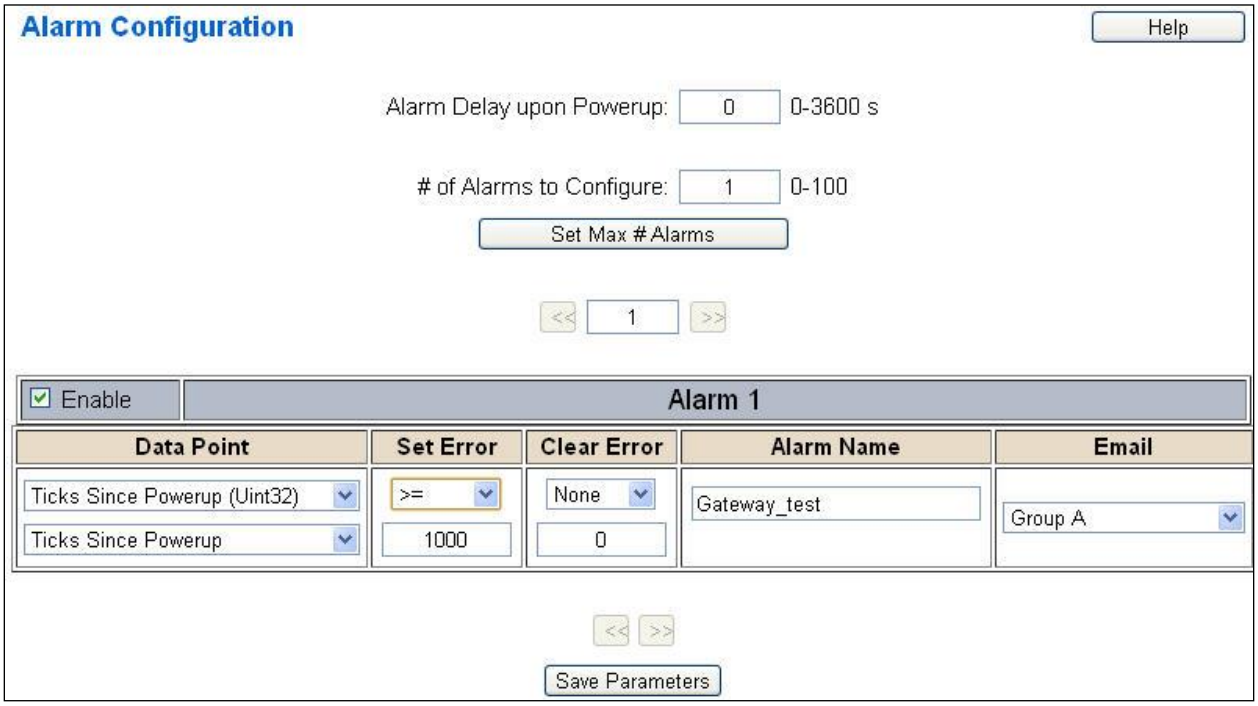
Click the **Save Parameters** button to commit the changes and reboot the gateway.



Alarm Configuration

To setup alarms on the 460 gateway, navigate to **Other->Alarm Configuration**.

1) Alarm Delay upon Powerup: At Powerup, the gateway will have values of '0' stored for all data. This may cause alarms to trigger before these values are updated by the mating protocols. Set this field to provide needed time to update fields before considering values for alarms.



2) Enter the number of alarms to configure and click **Set Max # Alarms** to generate those lines.
3) In the Data Point Section:
    a. Top dropdown: select the Data Group. This dropdown menu will contain all groups that go from the gateway to the network.
    b. Lower dropdown: select the Data Point's Specific Point. This is used to select which point in the group will be monitored for alarms.
4) In the Set Error Section:
    a. Select the Set Error Operation in the top dropdown menu. Available options are <, >, <=, >=, !=, ==, and Change of State (COS). This is the operation that will be used to compare the Data Point value against the Error Value to determine if the alarm needs to be set.
    b. Select the Set Error Value. This value is used as: 'Data Point's Value' 'Operation' 'Value.' Ex: Ticks Since Powerup >= 1000. This will set the alarm after 1000 ticks have elapsed since the unit powered up.

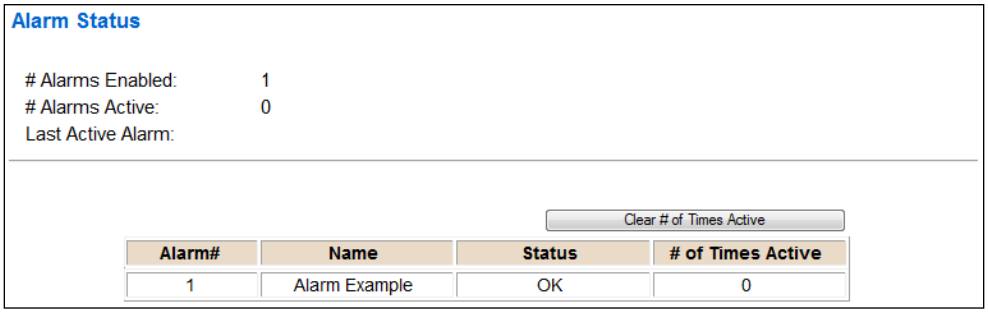
5) In the Clear Error Section:
    a. Select the Clear Error Operation. Available options are <, >, <=, >=, !=, ==, and Change of State (COS). This is the operation that will be used to compare the Data Point value against the Error Value to determine if the alarm needs to be cleared.
    b. Select the Clear Error Value.
    -Ex: Ticks Since Powerup >= 5000. This will clear the alarm after 5000 ticks have elapsed since the unit powered up.
6) Enter an Alarm Name. This will make the alarm unique and will be available in the Alarm Status page as well as in the email generated by the alarm.
7) Select an email to associate this alarm with. When an alarm is set, it sends an email. When an alarm is cleared, it will also send an email.

Click the **Save Parameters** button to commit the changes to memory and reboot the gateway.

Diagnostics – Alarm Status

Alarm Status will only display under the Diagnostic menu tab if at least 1 Alarm is enabled.

1) # Alarms Enabled: This is a count of enabled alarms.
2) # Alarms Active: This is how many alarms are presently active (set).
3) Last Active Alarm: This is the last alarm that the gateway detected.
4) **Clear # of Times Active**: This will reset all alarms '# of Times Active' to 0.
5) Alarm #: The reference number to the given alarm on the alarm setup page.
6) Name: The name of the alarm.
7) Status: The current status of the alarm, either OK or ALARM.
8) # of Times Active: This count represents the number of times this alarm has become active. If an alarm is triggered, this count will increment.

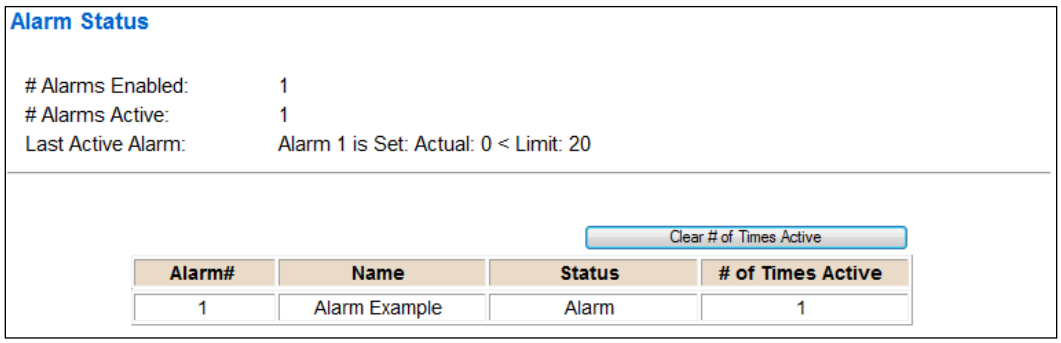


Alarms – Active

While one or more alarms are active, every page will display 'Alarms Active' at the top of the page. This will no longer be displayed if all active alarms have been cleared.

When an alarm is activated, the following will occur:

1) A one-time notification will be sent out to the email associated with the alarm.
2) For duplicate emails to occur, the alarm must be cleared and then become active again.
3) *# Alarms Active* and *# of Times Active* will be incremented.
4) Status of the Individual Alarm will be set to *Alarm*.
5) *Last Active Alarm* field will be populated with details on what triggered the alarm.



Alarms – Clear

When an alarm is cleared, the following will occur:

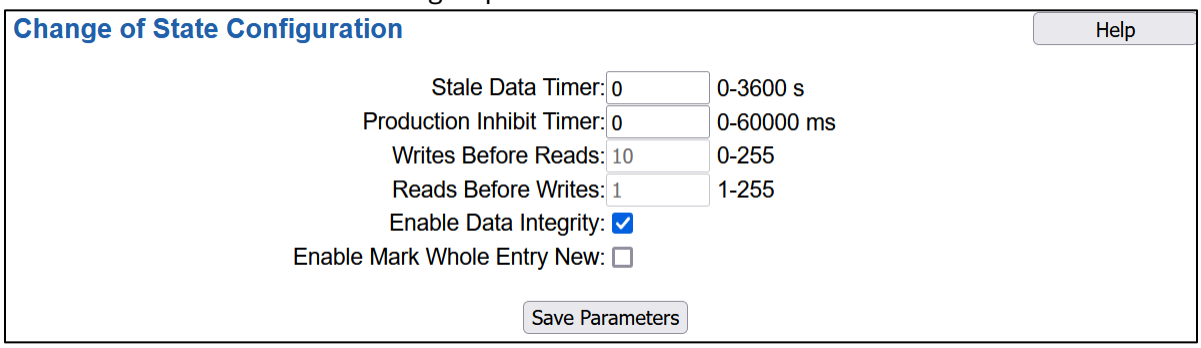
1) A one-time notification will be sent to the email associated with the alarm.
    a. For duplicate emails to occur, the alarm must become active and then be cleared again.
2) Total *# Alarms Active* will decrement. *Last Active Alarm* will not be changed.
3) Status of the Individual Alarm will be reset to *OK*.

Change of State (COS) Configuration

To access the configuration files in the 460 gateway, navigate to dropdown **Other->COS Configuration**. The gateway, by default only writes when data has changed. The gateway also waits to write any data to the destination until the source protocol is successfully connected.

Default values should fit most applications. Change these values with caution as they affect

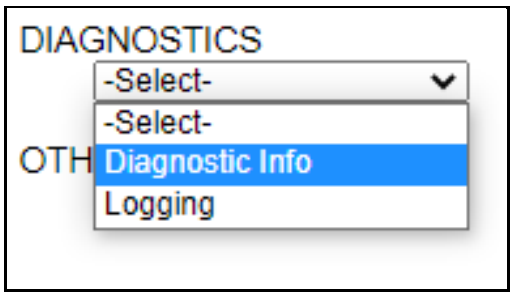
1) **Stale Data Timer**: If the data has not changed within the time allocated in this Stale Data Timer, the data will be marked as stale within the gateway and will force a write request to occur. This timer is to be used to force cyclic updates in the gateway, since data will only be written if it has changed by default. There is a separate timer per data mapping.
   Gateway behavior:
   - If time = 0s => (DEFAULT) The gateway will write out new values on a Change of State basis.
   - If time > 0s => The gateway will write out new values whenever the timer expires to force cyclic updates (write every *x* seconds).
2) **Production Inhibit Timer:** Amount of time after a Change of State write request has occurred before allowing a new Change of State to be written. This is to be used to prevent jitter. Default value is 0ms. This timer takes priority over the Stale Data Timer. There is a separate timer per data mapping. This timer is active only after the first write goes out and the first COS event occurs.
3) **Writes Before Reads**: If multiple writes are queued, execute # of Writes Before Reads before the next read occurs. Default is 10 and should fit most applications.
   Warning: A value of 0 here may starve reads if a lot of writes are queued. This may be useful in applications where a burst of writes may occur and you want to guarantee they all go out before the next set of reads begin.
4) **Reads Before Writes:** If multiple writes are queued, the # of Writes Before Reads will occur before starting the # of Reads Before Writes. Once the # of Reads Before Writes has occurred, the counter for both reads and write will be reset. Default is 1 and should fit most applications.
5) **Enable Data Integrity**: If enabled, do not execute any write requests to the destination until the source data point is connected and communicating. This prevents writes of 0 upon power up.
6) **Enable Mark Whole Entry New**: If Enabled, mark the entire scan line or data group new upon 1 data element within the scan line or data group to be new.



Click the **Save Parameters** button to commit the changes to memory and reboot the gateway.

Diagnostics Info

The Diagnostics page is where you can view both protocols' diagnostics information, # of Data Mappings, # of String Mapping and # Alarm Mappings.



For protocol specific diagnostic information, refer to the next few pages.

Diagnostics Mapping

This section displays the number of mappings that are enabled, Data Mapping and String Mapping will show the # of Errors and First Errors. Alarms will show # active and Last Alarm that was active.

Common Errors:

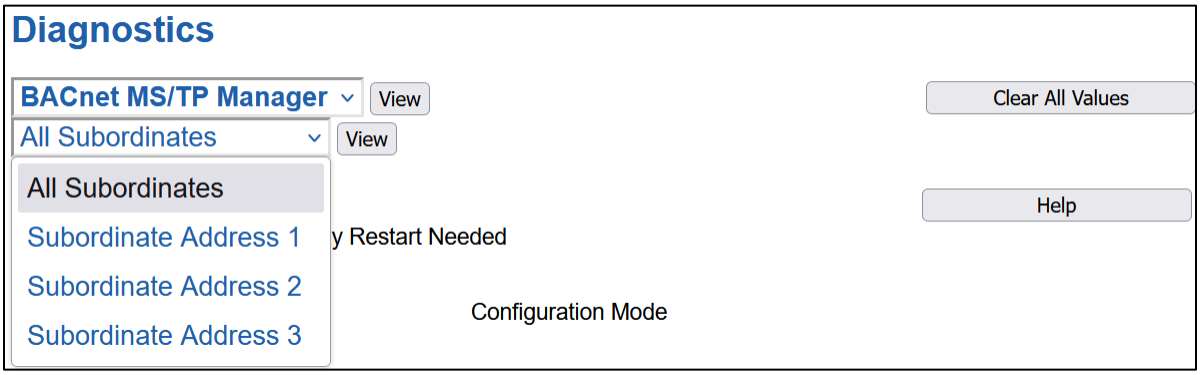
1) Destination or Source Point does not exist
   a) Solution: Re-map the mapping
2) Source or Destination Pointer too small
   a) There is not enough space on either the Source, or the Destination for the data you want to copy. This is typically seen when the Destination is smaller than the amount of data being transferred to it.
3) Range Discard, Min or Max Value
   a) The actual data value is outside of the defined range
4) Math Error
   a) Operation value cannot be 0
5) Scaling Error
   a) Source Min must be smaller than Source Max
   b) Destination Min must be smaller than Destination Max

Data Mapping	
# Enabled:	5 of 5
# of Errors:	0
First Error:	
String Mapping	
# Enabled:	2 of 2
# of Errors:	0
First Error:	
Alarms	
# Enabled:	3
# Active:	0
Last Active:	

Note: you can also view this information on the Main Page.

Diagnostics – BACnet MS/TP Manager

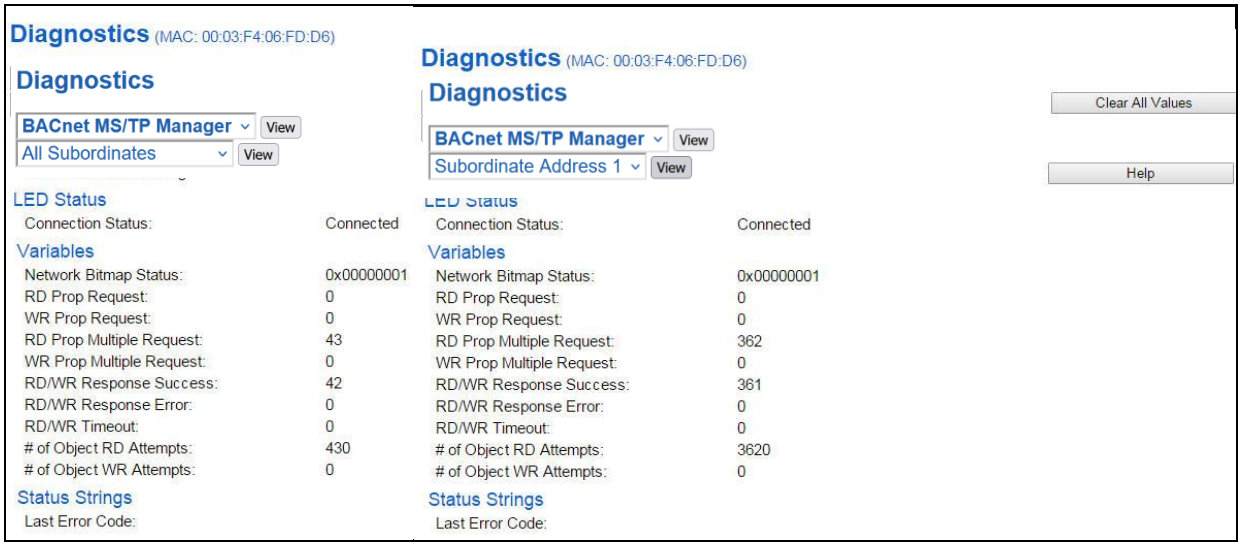
Select the BACnet MS/TP Manager in the dropdown menu on the Diagnostics Page to view a breakdown of the diagnostics and common strings that are displayed on the page. You may also view individual Subordinate counters by selecting the device in the *All Subordinates* dropdown and clicking **View**. Additional diagnostic information can be found by clicking the **Help** button.



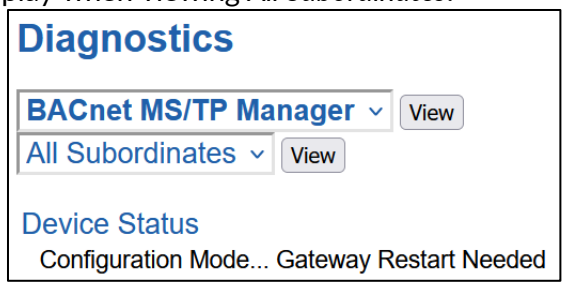
NOTE: This page will auto-refresh every five seconds with the latest data.

Clear All Values - This will only affect displayed values.

1) This will reset all displayed values back to zero and clear the Status Strings.
   Example: If viewing BACnet MS/TP Manager – Subordinate Address, this will only clear the values for that specific device. This will reduce the overall values indirectly, otherwise select All Servers to clear all devices.

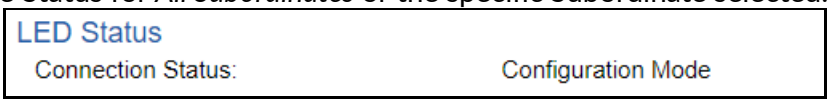


Device Status - This will only display when viewing *All Subordinates*.



1) Connected – The gateway is connected to all the BACnet MS/TP Subordinates that are enabled and configured.
2) Error: Timeout – One or more enabled BACnet MS/TP Subordinates have timeouts.
3) Fatal Error: No Configuration – No BACnet MS/TP Subordinates are configured or none of the BACnet MS/TP Subordinates configured are enabled.
4) Fatal Error: Configuration Invalid – One or more of the Subordinates configured are enabled, but do not have any scan lines configured.
5) Fatal Error: Couldn't Open Hardware Port – Port configured in the BACnet MS/TP Manager configuration page is not enabled in the Port Configuration page.
6) Dependency Protocol Faulted – The dependent protocol is missing causing the communication to go inactive.
7) Unknown: First Scan Not Complete – Multiple scan lines are set up for the device and the gateway has not completed all the scan lines for the first time.

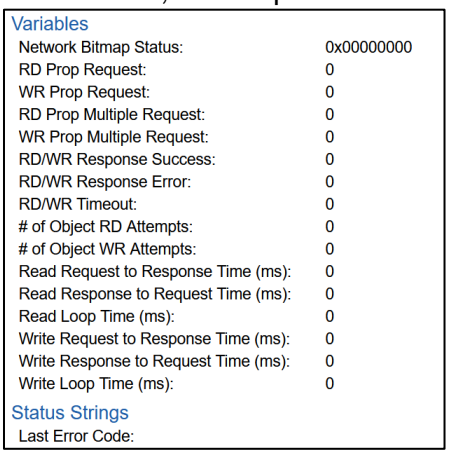
LED Status - This is the Status for *All Subordinates* or the specific Subordinate selected.



1) Solid Green (Connected) – The gateway is connected to all the BACnet MS/TP Subordinates that are configured and enabled.
2) Flashing Green (Not Connected) – The gateway has never been connected to a BACnet MS/TP Subordinate that is configured and enabled.
   a) Verify BACnet MS/TP settings and ensure that the *Enable* checkbox is checked for the appropriate device(s).
   b) Verify the *Enable* checkbox is checked for the appropriate device(s).
3) Flashing Red (Communication not attempted yet) – (Specific Subordinate only) No reads are configured and data needed for writes isn't valid yet.
4) Flashing Red (Connection Timeout) – One or more enabled BACnet MS/TP Subordinates are timed out.
   a) Verify that the Device Instance and MAC of each BACnet MS/TP Subordinate is valid and is not a duplicate on the network.
   b) Verify that there are valid scan lines configured for each Subordinate that is enabled.
5) Flashing Red (Dependency Error) – The dependent protocol is missing or timed out causing the communication to go inactive.
   a) The other protocol must be *Connected*.
6) Solid Red (No Devices Configured/Enabled) – There are no BACnet MS/TP Subordinates that are configured/enabled.

7) Solid Red (Empty Scan List) - One or more enabled BACnet MS/TP Subordinates have no scan lines configured.
   a) Verify there are scan lines configured for devices that are enabled.
8) Solid Red (No Serial Port Configured) – Port configured in the BACnet MS/TP Manager configuration page is not enabled in the Port Configuration page.

Variables - These are the values for *All Subordinates*, or the specific Subordinate selected.



1) Network Bitmap Status (Displayed in Hex):
   a) Each bit corresponds to a Subordinate. If the bit is set, the Subordinate is connected, otherwise the bit is 0.
   b) Bit 0 corresponds to Subordinate 1 and Bit 4 is for Subordinate 5 and so on.
2) RD Prop Request– Number of Read Property Single requests sent to the BACnet MS/TP devices.
   a) **NOTE**: Read Property Single Requests are only used if the BACnet MS/TP device does not support Read Property Multiple (RPM).
3) WR Prop Request– Number of Write Property Single requests sent to the BACnet MS/TP devices.
   a) **NOTE**: Write Property Single Requests are only used if the BACnet MS/TP device does not support Write Property Multiple (WPM).
4) RD Prop Multiple Request– Number of Read Property Multiple requests sent to the BACnet MS/TP devices.
5) WR Prop Multiple Request– Number of Write Property Multiple requests sent to the BACnet MS/TP devices.
6) RD/WR Response Success – Number of successful read or write responses received. This value should be equal to RD Single + WR Single + RD Multiple + WR Multiple Variable Counts.
7) RD/WR Response Error – Number of read or write error responses received.
   a) **NOTE**: If the gateway receives an error of Unsupported Service for a RPM or WPM request, then RP/WR Single requests will be used for that device for the duration of that power up.
8) RD/WR Timeout – Total number of read/write requests sent to the BACnet MS/TP device with no reply received within the response timeout configured.
9) # of Object Read Attempts – Total number of objects that the gateway attempted to read.
10) # of Object Write Attempts – Total number of objects that the gateway attempted to write.
11) Read Request to Response Time (ms) – Number of milliseconds it took the Subordinate device to reply to a request.
12) Read Response to Request Time (ms) – Number of milliseconds it took the gateway to execute the next request once the previous response has been received.

13) Read Loop Time (ms) – Number of milliseconds it took to execute all read requests.
14) Write Request to Response Time (ms) – Number of milliseconds it took the Subordinate device to reply to a request.
15) Write Response to Request Time (ms) – Number of milliseconds it took the gateway to execute the next request once the previous response has been received.
16) Write Loop Time (ms) – Number of milliseconds it took to execute all write requests.

Status Strings - These are the values for *All Subordinates*, or the specific Subordinate selected.

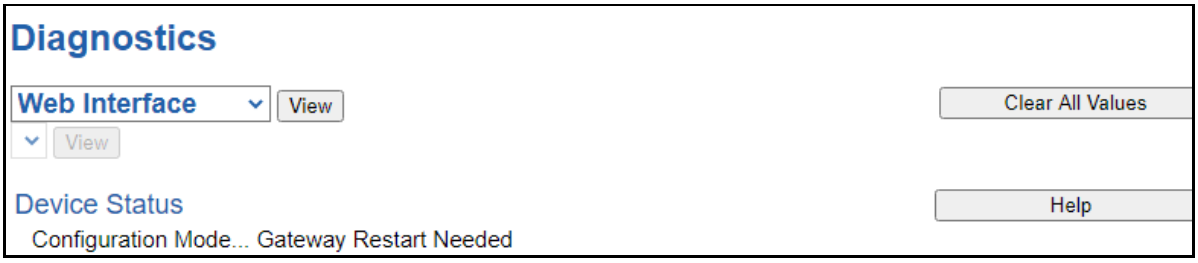
1) Last Error Code:
   a) Last read/write reply error that the gateway received

Error Code Breakdown:

1) Rx Err Reply ["ErrorCode"] frm DevInst "Inst" "function" req Obj "ObjectID"
   a) "ErrorCode" – see descriptions of error codes below.
   b) "Inst" – This will give you the Device Instance of the Subordinate that had the error.
   c) "Function" – This will either be *rd* for read request or *wr* for write request.
   d) "ObjectID" – This will give you the object type and object number for the request that had the error.
2) Error Codes - The gateway is sending an error a message due to the listed explanation:
   a) "Inconsistent Parm" -
      i) The gateway tried to write a priority that was out of range or reserved (Priority 6) and was rejected by the Subordinate.
      ii) The gateway tried to write to ALL, REQUIRED or OPTIONAL object property and was rejected by the Subordinate.
   b) "Invalid Data Type" – The gateway tried to use a data type with an object that is not supported by the Subordinate.
   c) "Service Request Denied" – BACnet MS/TP request cannot be processed because the BACnet MS/TP connection is not established.
   d) "Read Access Denied" – BACnet MS/TP read request cannot be processed.
   e) "Unknown Obj" – The gateway tried to access an object the Subordinate does not support.
   f) "Unknown Property" – The gateway tried to access a property the Subordinate does not support for that object type.
   g) "Unsupported Object Type" – The gateway tried to access an object type the Subordinate does not support.
   h) "Value out of range" – BACnet MS/TP message could not be completed because the passed value was not in the valid range.
   i) "Write Access Denied" – The gateway tried to write a non-writeable property in the Subordinate.
   j) "Invalid array index" –
      i) The gateway tried to write a priority that was out of range or reserved (Priority 6) and was rejected.
      ii) The gateway tried to write an array for an object or property that doesn't have an array index.
   k) "Unknown device" – The gateway is trying to send a message to a Subordinate we have not had previous communication with on the network.
   l) "Timeout" – BACnet MS/TP message timed out.
   m) "Segm Not Supported" – BACnet MS/TP message is too large to send in one message.
   n) "Invalid Tag" – BACnet MS/TP message is not how the Subordinate expects.
   o) "Unknown" – BACnet MS/TP message error for an unknown reason.

Diagnostics – Web Interface

Select **Web Interface** in the top dropdown menu on the Diagnostics Page to view a breakdown of the diagnostics that are displayed on the page.

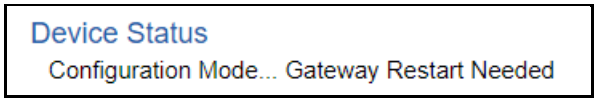


NOTE: This page will automatically refresh every five seconds with the latest data.

Clear All Values - This will only affect displayed values.

1) This will reset all displayed values back to zero and clear the Status Strings.
2) If the view is set to *Web Interface*, this will only clear the values for the Web Interface section of the gateway.

Device Status:

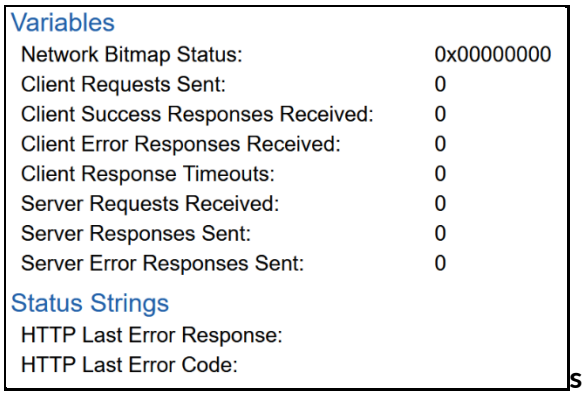


1) Connected and Running - The gateway is servicing HTTP GET or HTTP POST operations and the inactivity timeout (if configured) has not expired.
2) Connected (Idle) – The gateway is servicing HTTP GET or HTTP POST operations and the inactivity timeout has expired.
3) Not Connected – The gateway has never serviced any HTTP GET or HTTP POST operations.
4) Fatal Error: No Configuration – No data points have been configured for the Web Interface.

LED Status

1. Connected - Most recent HTTP request or response was successfully serviced
2. Connected(Idle) - No HTTP requests or responses have been serviced yet
3. Not Connected - The gateway has not sent or received any HTTP messages
4. Fatal Error No Configuration - No Data Points have been configured for the gateway

Variables



s

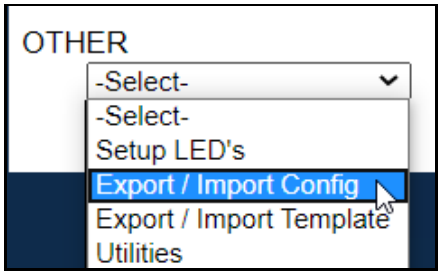
1. Network Bitmap Status:
    a. Bitmap U32 of all configured WI devices and their connection status (1 for connected and 0 for disconnected)
2. Client Requests Sent:
    a. Number of Client Requests that have been sent to a server
3. Client Success Responses Received:
    a. Number of 200-299 HTTP Responses received after sending a request as client
4. Client Error Responses Received:
    a. Number of bad responses (i.e. 400 Bad Request) received after sending a request as a client
5. Client Response Timeouts:
    a. Number of times the client request has timed out (configurable in the WI onfiguration page as Response Timeout)
6. Server Requests Received:
    a. Number of client requests the WI has received when acting as a server
7. Server Responses Sent:
    a. Number of responses sent to clients
8. Server Error Responses Sent:
    a. Number of times an Error Response (i.e. 404 Not Found) was sent to a client

Status Strings

1) Last Error Message:
    a) Message details about the last error. See Common Error Messages below for more information.
2) Last Error Code:
    a) Last HTTP Error Code resulting from client request issued by the gateway

Configuration Files

To access the configuration file in the 460 gateway, select the dropdown **Other->Export/Import Config**.



Export Configuration

The Export Configuration allows you to save your configuration file for backup or to be imported into another gateway. This file is named *rta_cfg.rtax* by default.

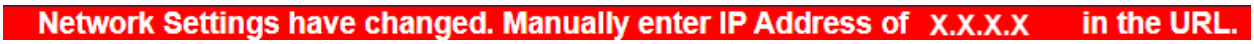
Upon clicking the **Save Configuration to File** button, you will be prompted to select a location to save the file. Different web browsers will yield different looks.

Import Configuration

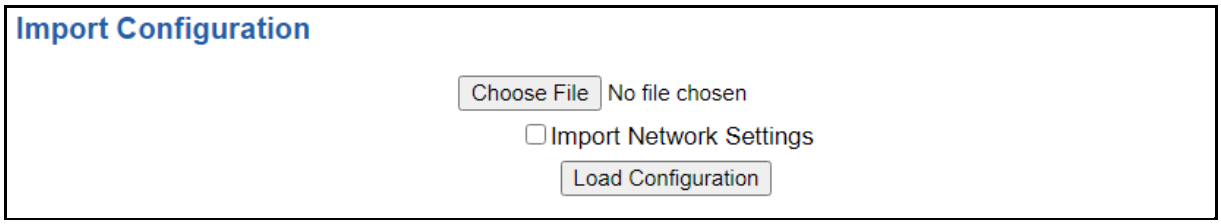
You can import a previously exported configuration file or a configuration file from another device into the 460 gateway, whenever it is in Configuration Mode.

Upon clicking the **Choose File** button, you will be prompted to select a location from which to load the saved file. Once the location is selected, you can choose the **Import Network Settings** checkbox if you want to load the network settings of the configuration file or just load the configuration without the network setting.

If you choose to Import Network Settings, this will override your current gateway's network setting with the settings in the configuration file. After you click on the Load Configuration button, a banner will display your gateway's new IP address.



If the configuration has successfully loaded, the gateway will indicate that it was successful, and a message will appear under the Load Configuration button indicating Restart Needed.



If it encountered an error while trying to load the saved configuration, the gateway will indicate the first error it found and a brief description about it under the Load Configuration button. Contact RTA Support with a screenshot of this error to further troubleshoot.

Save and Replace Configuration Using SD Card

Saving Configuration Using SD Card

This function saves the gateway's configuration automatically to an SD Card each time the gateway is rebooted via the **Restart Now** button on the web page. If this unit should fail in the future, the last configuration stored on the SD card and can be used for a new gateway to get the application back up and running quickly.

This SD Card replaces every configurable field in the gateway, **EXCEPT** for IP Address, Subnet Mask, and Default Gateway.

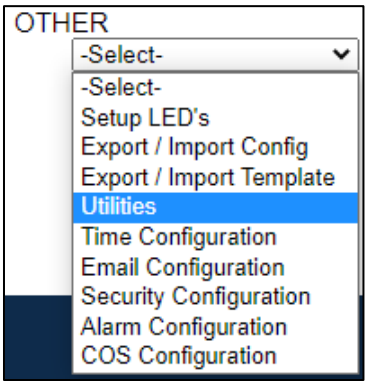
Replacing Configuration Using SD Card

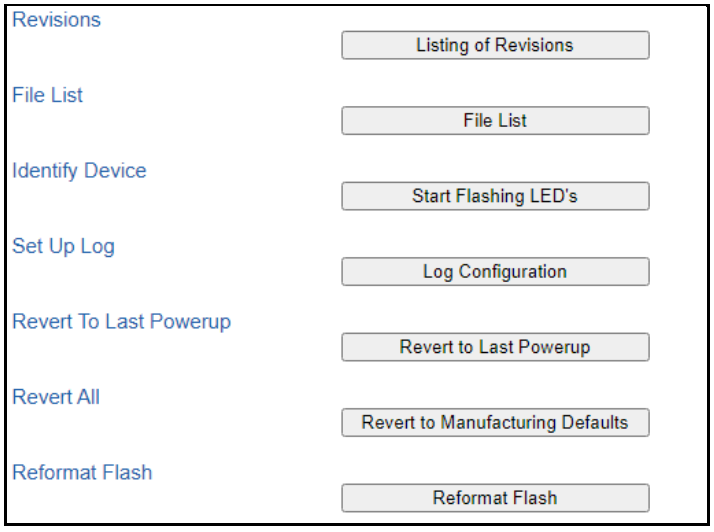
To replace a configuration in a gateway using the SD Card, a specific sequence of events must be followed for the replacement to happen correctly:

1) Extract SD Card from gateway you wish to copy the configuration from.
2) Power up the gateway you wish to copy the configuration to. DO NOT INSERT SD CARD YET.
3) Navigate to the webpage inside the unit.
4) Navigate to the dropdown **Other->Utilities**.
5) If you are not currently in *Mode: Configuration*, go into Configuration Mode by clicking the **Configuration Mode** button at the top left-hand side of the screen.
6) Press the **Revert to Manufacturing Defaults** button on the Utilities Page. The Configuration will ONLY be replaced by the SD Card if the gateway does not have a configuration already in it.
7) When the unit comes back in *Mode: Running*, insert the SD Card.
8) Do a hard power cycle to the unit by unplugging power. DO NOT RESET POWER VIA WEB PAGES.
    a. It will take an additional 30 seconds for the unit to power up while it is transferring the configuration. During this time, the gateway cannot be accessed via the web page.
9) When the unit comes back up, the configuration should be exactly what was on the SD Card.

Utilities

To access the Utilities page in the 460 gateway, navigate to **Other->Utilities**. The Utilities screen displays information about the gateway including Operation Time, File System Usage, Memory Usage, and Memory Block Usage.



Here you can also:

- View the full revision of the software.
- View all the files stored in the Flash File System within the gateway.
- Identify your device by clicking the **Start Flashing LEDs** button. By clicking this button, the two diagnostic LEDs will flash red and green. Once you have identified which device you are working with, click the button again to put the LEDs back into running mode.
- Configure the size of the log through the Log Configuration.
- Bring the device back to its last power up settings.
- Bring the device back to its original manufacturing defaults.
    - Remove the Configuration File and Flash Files within the gateway.