

# ***460MSBS-NNA1*** ***Protocol Gateway***

## **Product User Guide**

---

*Firmware Version 8.7.22*

## 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.

© 2021 Real Time Automation, Inc. All rights reserved.

Revision History .....	6
Overview .....	7
Hardware Platforms.....	8
Hardware – NNA1 .....	9
Powering the Gateway.....	9
Mounting with a DIN Rail.....	10
Installing.....	10
Removing .....	10
Accessing the Main Page.....	11
Error: Main Page Does Not Launch .....	12
Committing Changes to the Settings .....	13
Main Page .....	14
Device Configuration.....	15
Network Configuration .....	16
Modbus TCP/IP Server Configuration .....	17
Modbus TCP/IP Server Configuration-Data Groups.....	18
Auto-Configure Group by Device vs. Auto-Configure Group by Data Type.....	19
Group by Device (Default Method).....	19
Group by Data Type .....	19
Modbus TCP/IP Server Data Group Configuration: Auto-Configure.....	20
Modbus TCP/IP Server Data Group Configuration: Manual Mode.....	21
Configure Read and Write Data Groups .....	22
BACnet/IP Server Configuration .....	23
BACnet/IP Server Configuration-Data Groups .....	24
BACnet/IP Server Configuration: Auto-Configure Mode (Default).....	26
BACnet/IP Server Configuration: Manual Configure Mode .....	27
BACnet/IP Server Object Configuration – Analog Objects.....	28
BACnet/IP Server Object Configuration – Binary Objects.....	29
BACnet/IP Server Object Configuration – CharacterString Value Objects.....	30
BACnet/IP Server Object Configuration – Group Names.....	31
BACnet/IP Server Routing Configuration .....	32
Mapping - Transferring Data Between Devices .....	33
Display Mapping and Values .....	34
Display Data .....	34

Display String.....	37
Display String use case .....	39
Data and String Mapping – Auto-Configure.....	40
Data Mapping – Explanation.....	41
Data Mapping – Adding Diagnostic Information .....	42
String Mapping – Explanation .....	46
Mapping – Auto-Configure Mode to Manual Configure Mode .....	47
Mapping – Manual Configure Mode to Auto-Configure Mode .....	48
View as Text .....	49
Data Mapping.....	49
String Mapping.....	49
Base Triggering – Data Validation Triggering .....	50
Security Configuration .....	52
Security Configuration-Security Levels .....	53
Security - Log In.....	54
Security - Log Out.....	54
Email Configuration .....	55
Alarm Configuration.....	56
Diagnostics – Alarm Status.....	58
Alarms – Active .....	58
Alarms – Clear .....	59
Change of State (COS) Configuration .....	60
Diagnostics Info.....	61
Diagnostics Mapping.....	61
Diagnostics – Modbus TCP/IP Server .....	62
Diagnostics – BACnet/IP Server .....	64
LED Configuration .....	67
Configuration Files .....	68
Export Configuration.....	68
Import Configuration .....	68
Save and Replace Configuration Using SD Card.....	70
Saving Configuration Using SD Card.....	70
Replacing Configuration Using SD Card .....	70
Intelligent Reset Button .....	71

Utilities .....	72
-----------------	----

## Revision History

Version	Date	Notes
<b>8.4.5</b>	11/18/2019	<p>Features Added</p> <ol style="list-style-type: none"> <li>Released OPC UA Server (US) Protocol</li> <li>Ability to now Import/Export Template Files with out an FTP session.</li> </ol> <p>Bug Fixes</p> <ol style="list-style-type: none"> <li>Updated Profinet Server (PS) on N34 hardware Platform</li> <li>Updated Wi-Fi software</li> </ol>
<b>8.6.0</b>	2/28/20	<p>Bug Fixes</p> <ol style="list-style-type: none"> <li>Omron Plc Communication fixes for EtherNet/IP</li> <li>Profinet GSDML Substitute values fix</li> </ol>
<b>8.7.4</b>	9/1/20	<p>Features Added:</p> <ol style="list-style-type: none"> <li>BMS, BM, DFM, DS, DM, TCP, USB, PBS have been ported to the latest base software.</li> <li>TCP,BMS,BM now Available on N2E and N2EW hardware Platform</li> <li>New ASCII Mode Available on TCP/A/USB/WI protocols</li> <li>User Guides updated with more examples</li> </ol> <p>Bug Fixes:</p> <ol style="list-style-type: none"> <li>Improved Data Mapping and String Mapping performance</li> <li>Improved functionality/performance on EC,ETC,ES,MC,MS,BS,BC, A,,WI,PS protocols.</li> </ol>
<b>8.7.22</b>	4/6/21	<p>Features Added:</p> <ol style="list-style-type: none"> <li>Support for RSLogix Versions 32 + with unsigned data type support</li> <li>ETC now support Long integer files (L files) for MicroLogix PLCs that support them</li> <li>SC now supports data block (DB) access</li> </ol>

## Overview

The 460MSBS-NNA1 gateway connects a Modbus TCP Client with a BACnet/IP Client. By following this guide, you will be able to configure the 460MSBS-NNA1 gateway.

For further customization and advanced use, please reference the appendices located on the CD or 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](mailto:support@rtautomation.com)

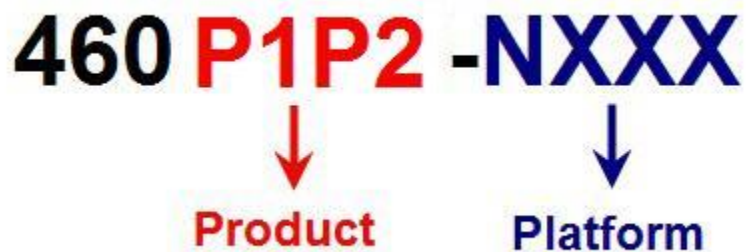
## Hardware Platforms

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 – NNA1



## Powering the Gateway

- 1) Connect a 12-24 VDC power source to the gateway, Red Wire = (+) Black Wire = (-).
  - a) The unit draws 175mA @ 12 V.



## 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 460MSBS-NNA1 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

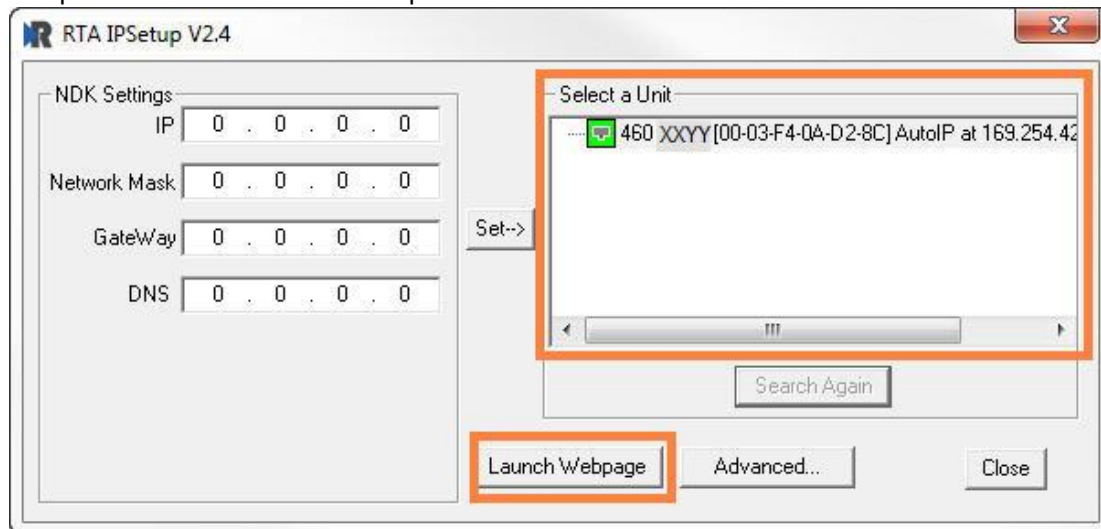
Follow these steps to remove your interface converter.

- 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 Access Browser Configuration Doc on the CD or download from our support web site.

- 1) Insert the provided CD-ROM into a computer also on the network.



- 2) Run the IPSetup.exe program from the CD-ROM.
- 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.



```
Administrator: C:\Windows\system32\cmd.exe

C:\>ping 192.168.0.100

Pinging 192.168.0.100 with 32 bytes of data:
Reply from 192.168.0.100: bytes=32 time<1ms TTL=60
Reply from 192.168.0.100: bytes=32 time<1ms TTL=60
Reply from 192.168.0.100: bytes=32 time<1ms TTL=60
Reply from 192.168.0.100: bytes=32 time<1ms TTL=60

Ping statistics for 192.168.0.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

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.



The screenshot shows the RTA Main Page interface. At the top left is the RTA logo and the text 'Real Time Automation, Inc.'. At the top right is the website 'www.rtaautomation.com' and a status box indicating 'MODE: RUNNING' and '460ETCMC'. On the left side, there is a navigation menu with buttons for 'Configuration Mode' and 'Main Page'. Below these are sections for 'CONFIGURATION' (Network Configuration, Allen-Bradley PLC, Modbus TCP/IP Client, Display Data), 'DIAGNOSTICS' (a dropdown menu), and 'OTHER' (a dropdown menu). The main content area is titled 'Main Page' and contains a 'Device Description' field with the value 'Application Description' and a 'Save Parameters' button. Below this is a 'Network Status' table with columns for Ethernet Port, Link Status, MAC Address, and IP Address. The table shows one entry for Ethernet Port with a Link Status of 100Mbps, Full Duplex, MAC Address of 00:03:F4:0A:43:CC, and IP Address of 10.1.28.95. Below the table are sections for 'Allen-Bradley PLC Status', 'Modbus TCP/IP Client Status', and 'Data Mapping Status', each showing device status and error codes.

Ethernet Port	Link Status	MAC Address	IP Address
Ethernet Port	100Mbps, Full Duplex	00:03:F4:0A:43:CC	10.1.28.95

**Allen-Bradley PLC Status**  
 Device Status: Fatal Error: No Configuration  
 Last Read Error Code:  
 Last Write Error Code:  
 LED Status: Connection Status: No Devices Configured / Enabled

**Modbus TCP/IP Client Status**  
 Device Status: Fatal Error: No Configuration  
 Last Error Code:  
 LED Status: Connection Status: No Devices Configured / Enabled

**Data Mapping Status**  
 # Enabled: 0 of 0  
 # of Errors: 0  
 First Error:

## 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.

### Main Page

Device Description:

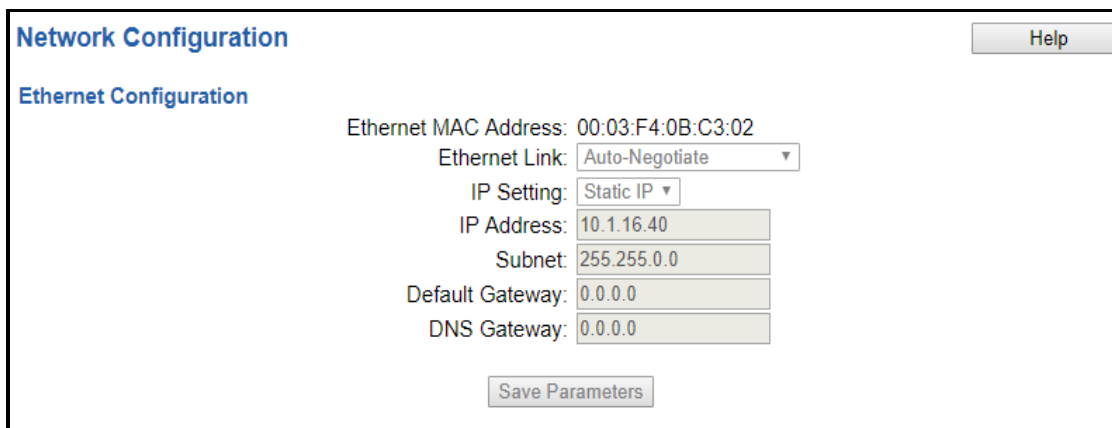
Once you are done configuring the Description, click the **Save Parameters** button.

## 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.



The screenshot shows the 'Network Configuration' window. It has a title bar with 'Network Configuration' and a 'Help' button. Below the title bar is the 'Ethernet Configuration' section. It displays the 'Ethernet MAC Address' as '00:03:F4:0B:C3:02'. The 'Ethernet Link' is set to 'Auto-Negotiate' in a dropdown menu. The 'IP Setting' is set to 'Static IP' in a dropdown menu. Below these are input fields for 'IP Address' (10.1.16.40), 'Subnet' (255.255.0.0), 'Default Gateway' (0.0.0.0), and 'DNS Gateway' (0.0.0.0). At the bottom of the configuration area is a 'Save Parameters' button.

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.



## Modbus TCP/IP Server Configuration

Click the **Modbus TCP/IP Server** button to access the configuration page.

- 1) Select which **Network Interface** to use for this Allen-Bradley PLC connection. If using single port hardware, the Network Interface will default to Ethernet port only.
- 2) Enter a **Device Label** to identify the device within the gateway.
- 3) **TCP Port**: Enter a TCP Port for the Modbus TCP server to listen on. Default for Modbus TCP/IP is 502.
- 4) **Inactivity Timeout**: Amount of time the gateway will wait for a read/write request before issuing a timeout.
- 5) To enable data swapping, select the required **Swap Indicator**. If the bytes appear in the wrong order, enable swapping to change the data. This swapping does *NOT* change coils and their ordering inside the Bit Pack.
- 6) **Bit Pack**: Select the formatting of the Coil Status/Input Status. Automap will use this packing size to map coils 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.

### Modbus TCP/IP Server Configuration

[Help](#)

Network Interface: Ethernet Port (10.1.16.77) ▼  
Device Label: MS01  
TCP Port: 502 1-65535 (Default: 502)  
Inactivity Timeout: 5000 0-60000 ms  
Swap Indicator: Swap None ▼  
Bit Pack: 1 Bit ▼ Coil / Input Status Only

Save Parameters

## Modbus TCP/IP Server Configuration-Data Groups

The bottom area of the Modbus TCP/IP Server Configuration page lets you configure up to 100 data groups for both the read and write.

There are three ways to configure this protocol:

- 1) Auto-Configure Group by Device (Default)
- 2) Auto-Configure Group by Data Type
- 3) Manual Mode

**NOTE:** You may go back and forth between modes, but when reverting from Manual Mode to either of the two Auto-Configure modes, all changes made in Manual Mode will be discarded.

**Modbus TCP/IP Server Point List**

# of Read Data Groups:	<input type="text" value="1"/>	<div><div>Manual Configure</div><div>Auto-Configure Group by Device</div><div>Auto-Configure Group by Data Type</div><div>Manual Configure</div></div>	# of Write Data Groups:	<input type="text" value="1"/>	<input type="text" value="0-100"/>
<input type="button" value="Generate Data Groups"/>					

## Auto-Configure Group by Device vs. Auto-Configure Group by Data Type

There are two different methods for Auto-Configure: Group by Device or Group by Data Type.

There are a couple of rules to keep in mind when using Auto-Configure Mode:

- 1) If the other protocol inside the gateway is a server, slave, or adapter protocol, then there are no differences between the Auto-Configure modes.

### Group by Device (Default Method)

Group by Device goes through the other protocol on the gateway and auto-configures the data groups in the Modbus TCP/IP server for all the data points on the other protocol's first device. After it finishes with the first device, it will auto-configure all the points for the second device (if one is configured), and so on.

The data in this method is not optimized- there could potentially be a lot of wasted/unused data space, but it will be organized more logically from the master/client's point of view.

### Group by Data Type

Group by Data Type goes through the other protocol on the gateway and auto-configures the data groups in the Modbus TCP/IP server for all the data points within the other protocol.

Another way to view this option is to say that the data points allocated are packed together so there is very little wasted data space. The data is packed or optimized.

**Example:**      *Protocol A is a master/client protocol that has 2 devices with the same setup:*

*Device\_1 has 1 integer scan line, 1 float scan line, 1 integer scan line- each for 1 point of data*

*Device\_2 has 1 integer scan line, 1 float scan line, 1 integer scan line- each for 1 point of data*

*Protocol B is a server/slave/adapter protocol that can be mapped as follows:*

**Group by Device** - Protocol B will have 4 scan lines that will look like the following: Scan Line 1 and 2 will represent Device\_1 and Scan Line 3 and 4 will represent Device\_2.

Scan Line 1 => Type Integer, length of 2

Scan Line 2 => Type Float, length of 1

Scan Line 3 => Type Integer, length of 2

Scan Line 4 => Type Float, length of 1

**Group by Data Type** - Protocol B will have 2 scan lines that will look like the following: All like data types from Device\_1 and Device\_2 will be combined.

Scan Line 1 => Type Integer, length of 4

Scan Line 2 => Type Float, length of 2

## Modbus TCP/IP Server Data Group Configuration: Auto-Configure

While in either of the two Auto-Configure modes, the # of Data Groups and the actual data groups themselves cannot be edited. Auto-Configure Mode looks at the other protocol and then configures the data groups to match. The data formats will be defined after the other protocol is configured.

The data will be configured according to the following rules:

- 1) Any Coils, 8 Bit Signed/Unsigned, or 1/8/16/32 Bit Binary Packs data will be mapped as **0x Coil Status**.
- 2) Any 16 Bit Signed/Unsigned data will be mapped as **4x Hold Reg 16 Bit Int or 16 Bit Uint**, matching signs whenever possible.
- 3) Any 32 Bit Signed/Unsigned data will be mapped as **4x Hold Reg 32 Bit Int or 32 Bit Uint**, matching signs whenever possible.
- 4) Any 64 Bit Signed/Unsigned data will be mapped as **4x Hold Reg 64 Bit Int or 64 Bit Uint**, matching signs whenever possible.
- 5) Any 32 Bit Float will be mapped as **4x Hold Reg 32 Bit Float**.
- 6) Any 64 Bit Float will be mapped as **4x Hold Reg 64 Bit Float**.
- 7) Any String data types will be mapped as **4x Hold Reg String**.
- 8) The read or write direction depends on whether it is configured as a read or write on the other protocol.
- 9) If the other protocol exceeds the number of data groups supported, then nothing will be mapped. You will see the # of Data Groups remain at 0 and the main page will display the following error:



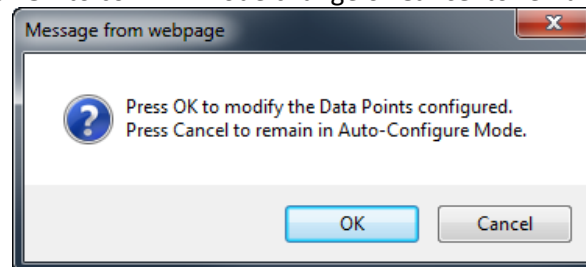
ERROR xx 460 Re-Initialization (Auto-Config Failed -9)

- a) To fix this error, simply decrease the amount of data you configured on the other protocol so that the max number of Data Groups is not exceeded or call customer support to increase the limits.

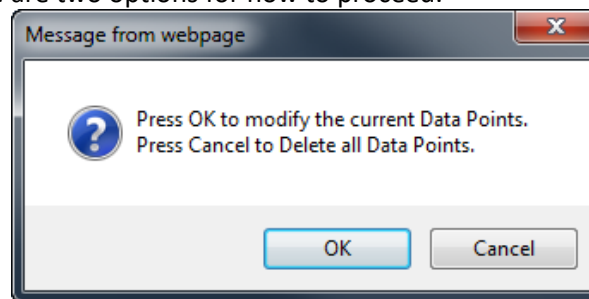
To add additional or edit existing data groups, you will need to go into Manual Configure Mode. **If you go back to Auto-Configure Mode, you will lose ALL manual edits.**

## Modbus TCP/IP Server Data Group Configuration: Manual Mode

- 1) To transition from either of the two Auto-Configure modes to Manual Configure Mode, click the dropdown at the top of the Modbus TCP/IP server Configuration page and select Manual Configure.
  - a) When prompted, click **OK** to confirm mode change or **Cancel** to remain in Auto-Configure Mode.



- 2) Once OK is clicked, there are two options for how to proceed.



- 3) To keep the data groups that are already configured, press **OK**.
  - a) You would want this option if you are adding additional data groups or you want to modify the data group(s) that already exist.
- 4) To delete the data groups that are already there and start over, press **Cancel**.
- 5) Enter the number of Read Data Groups and/or Write Data groups.

# of Read Data Groups: <input style="width: 50px; text-align: center;" type="text" value="1"/> 0-100	# of Write Data Groups: <input style="width: 50px; text-align: center;" type="text" value="1"/> 0-100
<input type="button" value="Generate Data Groups"/>	
<input type="button" value="View Read Data Groups"/>	<input type="button" value="View Write Data Groups"/>

- 6) Click the **Generate Data Groups** button to have the read and write data groups auto-generate for you. You may manually configure the read and write data groups after they have been generated.

## Configure Read and Write Data Groups

Follow these steps to manually configure read or write data groups.

- 1) Select **View Read Data Groups** or **View Write Data Groups** if not already selected.

View Read Data Groups
View Write Data Groups

### Read Data Groups (460 to Modbus TCP/IP)

Read Data Groups	Point Type	Starting Address	# of Points (1-512)
1	4x Hold Reg (16 Bit Int) ▼	1	5
<span>&lt;&lt;</span> 1-1 <span>&gt;&gt;</span>			

View Read Data Groups
View Write Data Groups

### Write Data Groups (Modbus TCP/IP to 460)

Write Data Groups	Point Type	Starting Address	# of Points (1-512)
1	0x Coil Status ▼	1	1
<span>&lt;&lt;</span> 1-1 <span>&gt;&gt;</span>			

- 2) Select a **Point Type** for each scan line. Options include: Coil Status, Input Status, Input Registers, and Holding Registers. **Note:** Input/Holding Registers have a data type associated with them.
  - a) String Point Type- If the mating protocol supports strings, you may select string as a point type in Modbus. With this point type, 2 characters will be packed into a single register and the first register will be set aside for the length.
  - b) EX: 4x Hold Reg (String) with a Starting Address of 1 for a length of 5 Registers.  
This means that Register 1 will hold the length of the string and Registers 2-5 will hold the string contents. This string can contain a max of 8 characters.
- 3) Enter a **Starting Address** (1-based).
- 4) Enter the **# of Points** to read or write. This will allocate the number of the data type selected.

View Read Data Groups
View Write Data Groups

### Read Data Groups (460 to Modbus TCP/IP)

Read Data Groups	Point Type	Starting Address	# of Points (1-512)
1	0x Coil Status ▼	1000	500
2	4x Hold Reg (16 Bit Int) ▼	1001	500
3	4x Hold Reg (32 Bit Int) ▼	2001	500
4	4x Hold Reg (32 Bit Float) ▼	3001	500
<span>&lt;&lt;</span> 1-4 <span>&gt;&gt;</span>			

## BACnet/IP Server Configuration

Click the **BACnet/IP Server** button to access the primary configuration page for this device.

- 1) Select which **Network Interface** to use for this BACnet/IP connection. If using single port hardware, the Network Interface will default to Ethernet Port only.
- 2) Enter a **Device Label**. This is an internal device alias used during data mapping.
- 3) Enter the decimal value of the **UDP Port** that the gateway will communicate on. Default is 47808 (0xBAC0).
- 4) Enter a unique **Instance** identifier for the gateway. This value must be unique on the BACnet/IP network.
- 5) **Inactivity Timeout**: Enter the amount of time, in milliseconds, the gateway should wait before a timeout state is declared. If the BACnet/IP client does not initiate communication within this time frame the BACnet/IP LED will flash red and the timeout counter will increment. Enter zero to disable this feature.
- 6) Enter a **Name**, **Description** and **Location** for the gateway. These are used to identify the gateway on the BACnet/IP network.
- 7) **Bit Pack**: Select the formatting of the binary input/output. Automap will use this packing size to map binary objects to/from the other protocol.

**BACnet/IP Server Configuration**
Help

Network Interface: Ethernet 1 (192.168.47.206) ▼

Device Label: BS01

UDP Port: 47808 1-65535 (Recommend 47808-47823)

Instance: 50 0-4194302

Inactivity Timeout: 3000 0-Disable; 1000-65000 ms

Name: Gateway Name

Description: Gateway Description

Location: Gateway Location

Bit Pack: 1 Bit ▼ Binary Input/Output Only

Save Parameters

## BACnet/IP Server Configuration-Data Groups

The bottom area of the BACnet/IP Server Configuration page lets you configure multiple objects for read and write groups.

There are two ways to configure this protocol:

- 1) Auto-Configure Group by Data Type (Default)
- 2) Manual Configure Mode

**NOTE:** You may go back and forth between modes, but when reverting from Manual Configure Mode to Auto-Configure Mode, all changes made in Manual Mode will be discarded.

Auto-Configure Group by Data Type ▼

### Read Data Groups (460 to BACnet/IP)

Data Group	Object Type	Starting Object	# of Objects
1	Analog Input (32 Bit Float)	1	1
2	Binary Input	1	8
3	CharacterString Value	1	0

### Write Data Groups (BACnet/IP to 460)

Data Group	Object Type	Starting Object	# of Objects
1	Analog Output (32 Bit Float)	1	500
2	Binary Output	1	0
3	CharacterString Value	51	1

The setup in the example above will give you the following results:

- 1 AI is created with the address of AI1
- 8 BIs are created with the addresses BI1 through BI8
- 500 AOs are created with the addresses AO1 through AO500
- 1 CSV is created with the address of CSV51

### Data Group Data Limit

Object Type	# of Objects
Analog Input / Analog Output	1200
Binary Input / Binary Output	1600
CharacterString Value	50





## BACnet/IP Server Configuration: Auto-Configure Mode (Default)

While in Auto-Configure Mode, no fields under the data groups can be edited. Auto-Configure Mode looks at the other protocol and then configures the data groups below to match. BACnet/IP points will be defined after the other protocol is configured.

Within the BACnet/IP server, the data will automatically be configured according to the following rules:

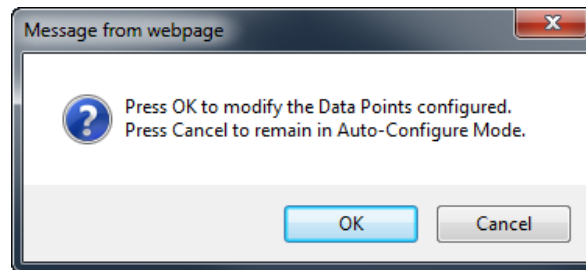
- 3) Any 8 Bit Signed/Unsigned, 16 Bit Signed/Unsigned, 32 Bit Signed/Unsigned, 64 Bit Signed/Unsigned, 32 Bit Float, and 64 Bit Float data will be mapped as **Analog Objects**.
- 4) Any Coils or 1/8/16/32 Bit Binary Packs will be mapped as **Binary Objects**.
- 5) Any String Data Types will be mapped as **CharacterString Value Objects**.
- 6) The input or output object direction depends on whether it is configured as a read or write on the other protocol.
- 7) If the other protocol exceeds the number of analog, binary or CharacterString value objects the BACnet/IP server supports (see limits on webpage), then nothing will be mapped. You will see the # of Objects column remain at 0 and the main page will display the following error:

**ERROR bs\_460 Re-initialization (Auto-Config Failed -9)**

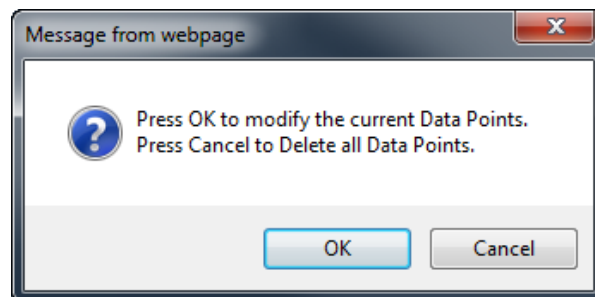
- To fix this error, simply decrease the amount of data you configured on the other protocol so that the max number of BACnet/IP objects is not exceeded or call customer support to increase the limits.

## BACnet/IP Server Configuration: Manual Configure Mode

- 1) To transition from Auto-Configure Mode to Manual Configure Mode, click the dropdown in the middle of the BACnet/IP Server Configuration page and select Manual Configure.
  - a. When prompted, click **OK** to confirm mode change or **Cancel** to remain in Auto-Configure Mode.



- b. Once OK is clicked, there are two options for how to proceed.



- i. To keep the current data groups and object properties (includes any default object names, units and COV) that are already configured, press **OK**.
      - You would want this option if you are adding additional data groups or you want to modify the data group(s) that already exist.
    - ii. To delete the current data groups and object properties (includes any default object names, units and COV) that are already there and start over, press **Cancel**.
- 2) For each object type in the read and write data groups sections, select the number of objects that the server will support.
- 3) Each object has its starting object number sequentially identified at one. This field may be modified.
- 4) When done, click the **Save Parameters** button.

## BACnet/IP Server Object Configuration – Analog Objects

Click the **Set Up BACnet Names, Units, and COV** button at the bottom of the BACnet/IP Server Configuration page to access the Object Configuration page.

When in Auto-Configure Mode, these fields are not configurable.

BACnet/IP Server Object Configuration					
Analog Input ▼		<< 1 >>			
Object	Group	Name	Unit Category	Unit	COV
1	G01 ▼	Load IA	Electrical ▼	A: (amperes) ▼	1.000000
2	G01 ▼	Load IB	Electrical ▼	A: (amperes) ▼	1.000000
3	G01 ▼	Load IC	Electrical ▼	A: (amperes) ▼	1.000000
4	G01 ▼	Total Active Power	Power ▼	W: (watts) ▼	1.000000
5	G01 ▼	Fuel Level	Other ▼	per: (percent) ▼	1.000000

Follow these steps to customize analog inputs or outputs in Manual Configure Mode:

- 1) Select **Analog Input** or **Analog Output** from the upper left dropdown menu.
- 2) Select a **Group** to use.
  - a) These group names are defined on this page under the “Group Name” dropdown menu.
  - b) **Use case example:** If there are multiple server/slave devices the RTA gateway is monitoring and sending over to the Build Automation System (BAS) to monitor, you can configure the group to represent each device. The image above displays 1 device, if there are 5 total devices then you can call Group 1 “Basement”, Group 2 “1<sup>st</sup> Floor”, Group 3 “Roof Top” etc..
- 3) Enter a **Name** to identify this object on the network.
- 4) The combination of **Group** and **Name** should be unique for each point in the gateway.
- 5) Select the **Unit Category** corresponding to the units you want this object to be identified with (optional). Then select the **Unit** from the dropdown menu.
- 6) Set the **COV** (Change of Value) for this object.
- 7) If the BACnet IP client issues a COV-Subscription, the gateway will issue a COV Notification when the Present-Value changes by more than the given COV-Value. This value shift can be in a positive or negative direction.

## BACnet/IP Server Object Configuration – Binary Objects

Click the **Set Up BACnet Names, Units, and COV** button at the bottom of the BACnet/IP Server Configuration page to access the Object Configuration page for this device.

When in Auto-Configure Mode, these fields are not configurable.

### BACnet/IP Server Object Configuration

Binary Input
▼

1

<<
>>

Object	Group	Name
1	G01 ▼	BI1
2	G01 ▼	BI2
3	G01 ▼	BI3
4	G01 ▼	BI4
5	G01 ▼	BI5
6	G01 ▼	BI6
7	G01 ▼	BI7
8	G01 ▼	BI8

Save Parameters

Follow these steps to configure binary inputs or outputs in Manual Configure Mode:

- 1) Select **Binary Input** or **Binary Output** from the upper left dropdown menu.
- 2) Select a **Group** to use.
  - These group names are defined on this page under the “Group Name” dropdown menu.
- 3) Enter a **Name** to identify this object on the network.
  - The combination of **Group** and **Name** should be unique for each point in the gateway.

## BACnet/IP Server Object Configuration – CharacterString Value Objects

Click the **Set Up BACnet Names, Units, and COV** button at the bottom of the BACnet/IP Server Configuration page to access the Object Configuration page for this device.

When in Auto-Configure Mode, these fields are not configurable.

### BACnet/IP Server Object Configuration

CharacterString Value Write ▾

<<

51

>>

Object	Group	Name
51	G01 ▾	CSV_W51

Save Parameters

Follow these steps to configure CharacterString value reads and writes in Manual Configure Mode:

- 1) Select **CharacterString Value Read** or **CharacterString Value Write** from the upper left dropdown menu.
- 2) Select a **Group** to use.
  - These group names are defined on this page under the “Group Name” dropdown menu.
- 3) Enter a **Name** to identify this object on the network.
  - The combination of **Group** and **Name** should be unique for each point in the gateway.

## BACnet/IP Server Object Configuration – Group Names

Click the **Set Up BACnet Names, Units, and COV** button at the bottom of the BACnet/IP Server Configuration page.

When in Auto-Configure Mode, these fields are not configurable.

The **Group Name** is designed to be used when there are multiple BACnet/IP objects that have the same name. This is useful when you have multiple, identical devices connected on the other protocol.

### BACnet/IP Server Object Configuration

Group Name ▼

Group #	Group Name
1	G01
2	G02
3	G03
4	G04
5	G05
6	G06
7	G07
8	G08
9	G09
10	G10

Follow these steps to configure the Group Names in Manual Configure Mode:

- 1) Select **Group Name** from the upper left dropdown menu.
- 2) For each **Group Name** used in the previous setup, change the name to your desired text. Any names not used do not need to be changed or configured.

## BACnet/IP Server Routing Configuration

Click the **Foreign Device Registration** button at the bottom of the BACnet/IP Server Configuration page to access the BACnet Routing Configuration page for this device.

These settings are used when connecting to a BACnet/IP client on a different subnet.

- 1) Foreign Device Registration (recommended): This option can be used ONLY when the BACnet/IP Broadcast Management Device (BBMD) device on the other subnet (often integrated into client devices) supports Foreign Device Registration. To use, enter the IP Address of the BBMD device into the gateway and select a Time-To-Live (TTL), the TTL defines how often the gateway should send a message to the BBMD device alerting them of the gateway presence.

**BACnet Routing Configuration**  
**Foreign Device Registration**  
  
IP Address:  0.0.0.0 to Disable  
Time-To-Live:  1-3600 s



## 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.

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

## 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.



Main Page

CONFIGURATION

- Network Configuration
- Port Configuration
- BACnet/IP Server
- Modbus RTU Master
- Display Data**

DIAGNOSTICS

-Select-

OTHER

-Select-

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.



**Display Data**

Edit Mapping

View as Text

Select a Device: Modbus TCP Server IP Address: 0.0.0.0 View

Protocol 1 to Protocol 2 Protocol 2 to Protocol 1

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.

Modbus RTU to BACnet/IP			BACnet/IP to Modbus RTU		
<< 1 >>			Displaying 1-201 of 300		
Modbus RTU		460MMBS ↔	BACnet/IP		
Name	Value (Hex)		Manipulation	Name	Value (Hex)
400001	--	--	↔	AI1	--
400002	--	--	↔	AI2	Mapping Disabled for Point
400003	--	--	↔	AI3	--

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.

Display Data

Edit Mapping  
View as Text

Select a Device
Modbus TCP Server IP Address: 10.1.16.16
View

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

<< 1 >>  
Displaying 1-7 of 7

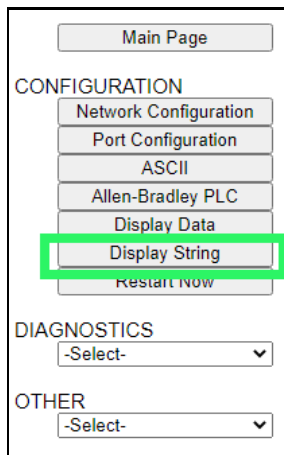
Modbus TCP/IP			460ETCMC ↔	PLC		
Name	Value (Hex)		Manipulation	Name	Value (Hex)	
400001	15	0x000F	↔	ETC01	15	0x000F
400002	1495	0x05D7	↔	MC2PLC_INT[0]	1495	0x05D7
400003	1	0x0001	↔	ETC01	1	0x0001
400004	23	0x0017	↔	MC2PLC_INT[1]	23	0x0017
400005	3	0x0003	↔	ETC01	3	0x0003
400011	--	--	↔	MC2PLC_INT[2]	--	--
400012	--	--	↔	ETC01	--	--
				MC2PLC_INT[3]		
				ETC01		
				MC2PLC_INT[4]		
				ETC01		
				ETC01_G2N0_INT[0]		
				ETC01		
				ETC01_G2N0_INT[1]		

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.



Main Page

CONFIGURATION

- Network Configuration
- Port Configuration
- ASCII
- Allen-Bradley PLC
- Display Data
- Display String**
- Restart Now

DIAGNOSTICS

-Select-

OTHER

-Select-

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.

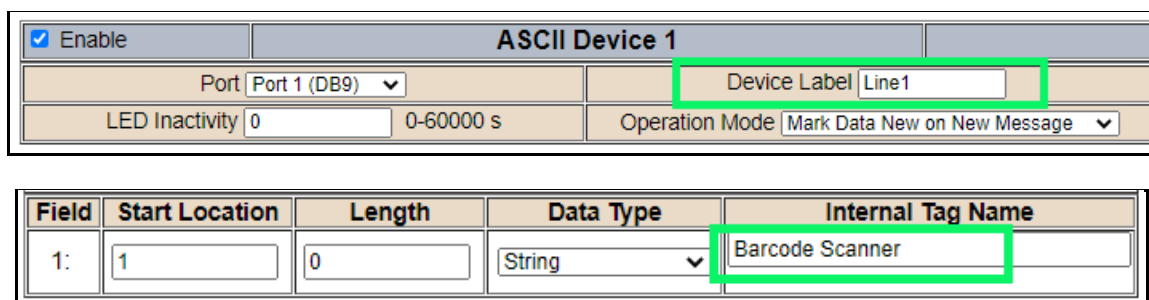


**Display String** Edit Mapping View as Text

Select a Group Src: Line 1 Barcode Scanner and a String Barcode Scanner (11 bytes)

0000: 68 65 6C 6C 6F 20 77 6F 72 6C 64 hello world

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



☒ Enable **ASCII Device 1**

Port Port 1 (DB9) Device Label Line1

LED Inactivity 0 0-60000 s Operation Mode Mark Data New on New Message

Field	Start Location	Length	Data Type	Internal Tag Name
1:	<span>1</span>	<span>0</span>	<span>String</span>	<span>Barcode Scanner</span>

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.

Display String

Edit Mapping  
View as Text

Select a Group
Src: Line 1 Barcode Scanner
and a String
Barcode Scanner
(0 bytes)

Data Not Valid

**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.

Diagnostics

ASCII
View

Port 1 (DB9)
View

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

Display String

Edit Mapping  
View as Text

Select a Group
Src: Line 1 Barcode Scanner
and a String
Barcode Scanner
(11 bytes)

0000: 68 65 6C 6C 6F 20 77 6F 72 6C 64
hello world

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


String Mapping Configuration

Help

Manual Configure
# of Mappings to Configure: 1 0-250
Set Max # of Mappings
<< 1 >>

☒ Enable

Mapping 1

Source		Destination
Group: Line 1 Barcode Scanner String: Barcode Scanner		Group: ETC01 ETC01_G2N0_STRIN String: ETC01_G2N0_STRING

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.

ASCII Device 1 (Line1)				
Max Number of Fields: 3		1-50		Min Number of Fields: 1
				1-50
Parsing Delimiter: , 44 0x2c				
Update Fields				
Field	Start Location	Length	Data Type	Internal Tag Name
1:	1	0	String	Header 1
2:	1	0	String	Header 2
3:	1	0	String	Header 3

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

**Display String**
Edit Mapping  
View as Text

Select a Group Src: Line1 Header 1 and a String Header 1 (3 bytes)

0000: 52 54 41 RTA

**Display String**
Edit Mapping  
View as Text

Select a Group Src: Line1 Header 2 and a String Header 2 (7 bytes)

0000: 53 75 70 70 6F 72 74 Support

**Display String**
Edit Mapping  
View as Text

Select a Group Src: Line1 Header 3 and a String Header 3 (5 bytes)

0000: 52 6F 63 68 73 Rocks

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.

**Diagnostics**

ASCII View  
Port 1 (DB9) View

Last Message Sent (17 bytes)  
0000: 52 54 41 2C 53 75 70 70 6F 72 74 2C 52 6F 63 68 RTA,Support,Rock  
0016: 73 s

## 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.

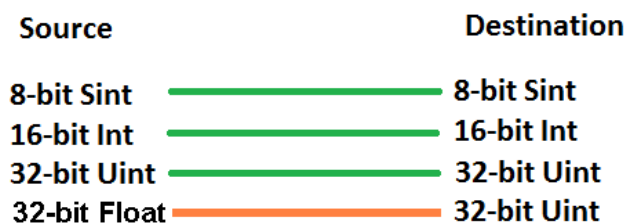
The following are examples of the Auto-Configure function.

- 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.

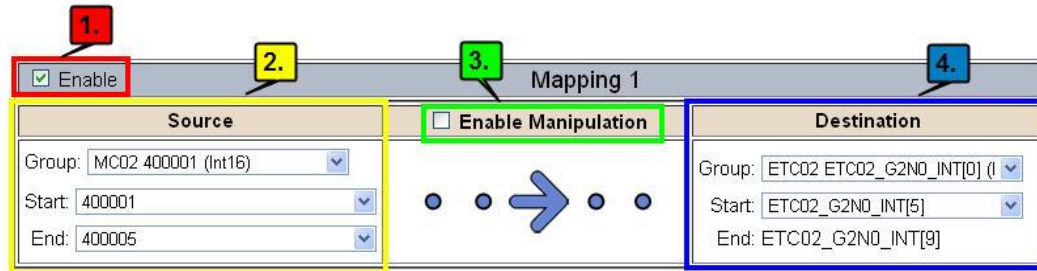


- a. The 32-bit Float from the Source location could not find a matching Destination data-type. After all other like data types were mapped, the only data type available was the 2<sup>nd</sup> 32-bit Uint data type. Auto-Configure was completed even though the data in the Float will be truncated.

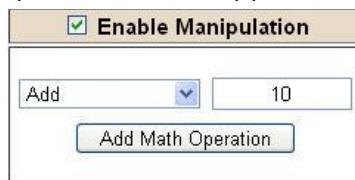


## Data Mapping – Explanation

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 0<sup>th</sup> source bit and copy it into the value of the 5<sup>th</sup> 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 necessary.

### 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.

Mapping 1		
Source	Enable Manipulation	Destination
<input checked="" type="checkbox"/> Enable Group: Temporary Ram0 (Int64) Start: Ram0 End: Ram0	<input checked="" type="checkbox"/> Enable Manipulation Scale Src: 1 to 10 Dst: 1 to 100	Group: Temporary Ram0 (Int64) Start: Ram1 End: Ram1
Mapping 2		
Source	Enable Manipulation	Destination
<input checked="" type="checkbox"/> Enable Group: Temporary Ram0 (Int64) Start: Ram1 End: Ram1	<input checked="" type="checkbox"/> Enable Manipulation Add 5 Add Math Operation	Group: Temporary Ram0 (Int64) Start: Ram2 End: Ram2


*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.

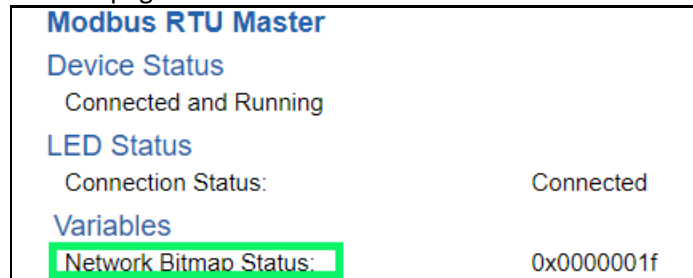
### 3) Ticks Per Second

- 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.

Mapping 1		
Source	Enable Manipulation	Destination
<input checked="" type="checkbox"/> Enable Group: Ticks Since Powerup (UInt32) Start: Since Powerup End: Since Powerup	<input type="checkbox"/> Enable Manipulation 	Group: BS01 AI1 (Float) Start: AI1 End: AI1

#### 4) 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.



**Modbus RTU Master**

**Device Status**  
Connected and Running

**LED Status**  
Connection Status: Connected

**Variables**  
**Network Bitmap Status:** 0x0000001f

- 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.



☒ Enable Mapping 1

Source	<input type="checkbox"/> Enable Manipulation	Destination
Group: MM NetBmpStat (Uint32)		Group: BS01 AI1 (Float)
Start: NetBmpStat		Start: AI1
End: NetBmpStat		End: AI1

**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.



☒ Enable Mapping 1

Source	<input checked="" type="checkbox"/> Enable Manipulation	Destination
Group: MM NetBmpStat (Uint32)	Set Bit	Group: BS01 BI1 (Bit1)
Start: NetBmpStat	Src: 1 (0-31)	Start: BI1
End: NetBmpStat	Dst: 0 (0)	End: BI1

## 5) 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) 1<sup>st</sup> 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



**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) 2<sup>nd</sup> 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) 3<sup>rd</sup> 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) 4<sup>th</sup> 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



**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:

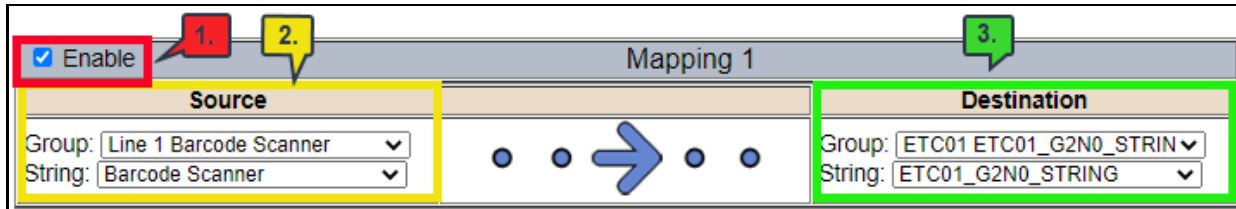
Hex:	Bit:	Decimal:	Explanation:
0x01	16	65,536	recoverable fault - timed

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.

Data Mapping

Mapping 1:	Temporary Ram0	Len: 1	-> 1:10	Scale to 1:100	->	Temporary Ram1
Mapping 2:	Temporary Ram1	Len: 1	-> Add 5	->		Temporary Ram2

### 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 Validation 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.

<input checked="" type="checkbox"/> Enable	Mapping 2	
<b>Source</b>	<input type="checkbox"/> Enable Manipulation	<b>Destination</b>
Group: BS01 AO1 (Float)		Group: MC Trigger 0 (Uint16)
Start: AO21		Start: Trigger 1
End: AO21		End: Trigger 1

- 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.

<input checked="" type="checkbox"/> Enable	Mapping 3	
<b>Source</b>	<input type="checkbox"/> Enable Manipulation	<b>Destination</b>
Group: MC Handshake 0 (Uint16)		Group: BS01 AI1 (Float)
Start: Handshake 1		Start: AI40
End: Handshake 1		End: AI40

## 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 event a password is forgotten.

**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
Help

Log Out Timer: 5 0-15 min

Admin Configuration

Admin	Username	Password	Re-enter Password	Email	Hint
1				Not Configured	
2				Not Configured	
3				Not Configured	

Admin Contact Information

User Configuration

User	Username	Password	Re-enter Password	Email	Hint
1				Not Configured	
2				Not Configured	
3				Not Configured	
4				Not Configured	
5				Not Configured	

Save Parameters

## 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.

User 1: ▼

View

User 1:  
 User 2:  
 User 3:  
 User 4:  
 User 5:  
 Guest

Web Page	Security
All Web Pages	No Access <span style="font-size: 0.8em;">▼</span> <span style="border: 1px solid #ccc; padding: 0 5px;">Set</span>

Web Page	Security
Main Page	Full Access <span style="font-size: 0.8em;">▼</span>
Device Configuration	Full Access <span style="font-size: 0.8em;">▼</span>
Port Configuration	Full Access <span style="font-size: 0.8em;">▼</span>
BACnet/IP Server	Full Access <span style="font-size: 0.8em;">▼</span>
Modbus RTU Master	Full Access <span style="font-size: 0.8em;">▼</span>
View Mapping	Full Access <span style="font-size: 0.8em;">▼</span>
Mapping	Full Access <span style="font-size: 0.8em;">▼</span>
Setup LED's	Full Access <span style="font-size: 0.8em;">▼</span>
Diagnostic Info	Full Access <span style="font-size: 0.8em;">▼</span>
Logging	Full Access <span style="font-size: 0.8em;">▼</span>
Display Data	Full Access <span style="font-size: 0.8em;">▼</span>
Export Configuration	Full Access <span style="font-size: 0.8em;">▼</span>
Import Configuration	Full Access <span style="font-size: 0.8em;">▼</span>
Save As Template	Full Access <span style="font-size: 0.8em;">▼</span>
Load From Template	Full Access <span style="font-size: 0.8em;">▼</span>
Utilities	Full Access <span style="font-size: 0.8em;">▼</span>
Email Configuration	Full Access <span style="font-size: 0.8em;">▼</span>
Alarm Configuration	Full Access <span style="font-size: 0.8em;">▼</span>
String Mapping	Full Access <span style="font-size: 0.8em;">▼</span>
View String Mapping	Full Access <span style="font-size: 0.8em;">▼</span>
Display String	Full Access <span style="font-size: 0.8em;">▼</span>

Save Parameters

## 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.



The form is titled "Security Log In" with a subtitle "Application Description". It contains two input fields: "Username:" with the value "Admin" and "Password:". Below these fields are three buttons: "Log In", "Display Hint", and "Reset Password". At the bottom, there is a label "Admin Contact:" followed by the text "Admin Contact Information Goes Here".

## 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.



The footer contains the RTA logo on the left, the text "Welcome Admin [logout](#)" in the center, and the website "www.rtaautomation.com" on the right. Below this is a blue bar with "Real Time Automation, Inc." on the left and "MODE: RUNNING 460" on the right.

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.

**Email Configuration**

Number of Emails to Configure:  0-10

User	SMTP Mail Username	SMTP Mail Password	SMTP Server	From Email	To Email	Email Group
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Group A ▼

## 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.

Alarm Configuration

Help

Alarm Delay upon Powerup:  0-3600 s

# of Alarms to Configure:  0-100

Set Max # Alarms

<<  >>

☒ Enable

Alarm 1				
Data Point	Set Error	Clear Error	Alarm Name	Email
<div>Ticks Since Powerup (Uint32)</div> <div>Ticks Since Powerup</div>	<div>&gt;=</div> <div>1000</div>	<div>None</div> <div>0</div>	Gateway_test	Group A

<< >>

Save Parameters

- 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.

**Alarm Status**

# Alarms Enabled: 1  
# Alarms Active: 0  
Last Active Alarm:

Clear # of Times Active

Alarm#	Name	Status	# of Times Active
1	Alarm Example	OK	0

## 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.


[www.rtaautomation.com](http://www.rtaautomation.com)

**Real Time Automation, Inc.**
Alarms Active

**MODE: RUNNING**  
**460**

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.

**Alarm Status**

# Alarms Enabled: 1  
# Alarms Active: 1  
Last Active Alarm: Alarm 1 is Set: Actual: 0 < Limit: 20

Clear # of Times Active

Alarm#	Name	Status	# of Times Active
1	Alarm Example	Alarm	1

## 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 performance.**

- 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.

**Change of State Configuration**
Help

Stale Data Timer:

0-3600 s

Production Inhibit Timer:

0-60000 ms

Writes Before Reads:

0-255

Reads Before Writes:

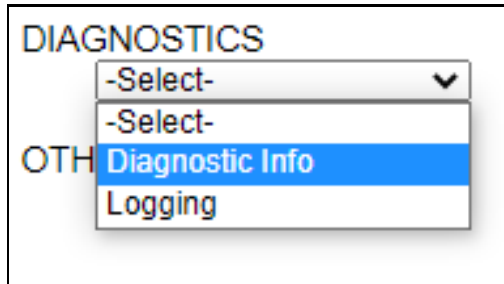
1-255

Enable Data Integrity:
☒

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:	

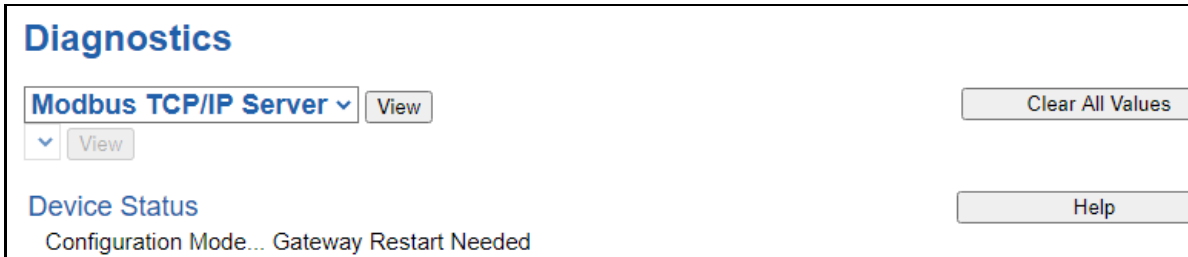
### Alarms

# Enabled:	3
# Active:	0
Last Active:	

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

## Diagnostics – Modbus TCP/IP Server

Select the **Modbus TCP/IP Server** in the dropdown menu on the Diagnostics Page to view a breakdown of the diagnostics and common strings that are displayed on the page. Additional diagnostic information can be found by clicking the **Help** button.



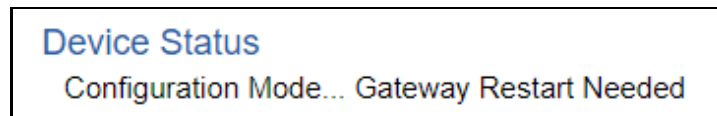
The screenshot shows the 'Diagnostics' section of the interface. It features a dropdown menu set to 'Modbus TCP/IP Server' with a 'View' button next to it. To the right is a 'Clear All Values' button. Below the dropdown is another 'View' button. Underneath, the 'Device Status' section is visible, showing 'Configuration Mode...' and 'Gateway Restart Needed'. A 'Help' button is located to the right of the Device Status section.

**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.
- 2) If viewing Modbus TCP/IP Server, this will only clear the values for the Modbus TCP/IP Server section of the gateway.

### Device Status



The screenshot shows the 'Device Status' section with the text 'Configuration Mode...' and 'Gateway Restart Needed'.

- 1) Connected - A Modbus TCP/IP client has a connection for the gateway.
- 2) Not Connected:
  - a) Ethernet Cable not plugged in.
  - b) The Modbus TCP/IP client has not initiated communication to the gateway.
  - c) The Modbus TCP/IP client has not communicated to the gateway in “x” milliseconds, where “x” is the inactivity timeout specified in the Modbus TCP/IP Server Configuration.

### LED Status:



The screenshot shows the 'LED Status' section with the text 'Connection Status:' and 'Configuration Mode'.

- 1) Solid Green (Connected and Running) – The gateway is connected to a Modbus TCP/IP client and communicating as expected.
- 2) Flashing Green (Connection not yet attempted) – The Modbus TCP/IP client has never attempted to connect to the gateway.
- 3) Flashing Red (Nodes Missing Timeout) - The gateway has lost a connection to the Modbus TCP/IP client.
- 4) Off:
  - a) No power.

b) No Ethernet cable plugged in.

#### Variables:

Variables	
FC01 Read Coil Status:	0
FC02 Read Input Status:	0
FC03 Read Holding Registers:	0
FC04 Read Input Registers:	0
FC05 Force Single Coil:	0
FC06 Preset Single Register:	0
FC15 Force Multiple Coils:	0
FC16 Preset Multiple Registers:	0
FC23 Read/Write 4X Registers:	0
Successful Responses Sent:	0
Error Responses Sent:	0
Timeout, TCP Closed:	0
TCP Connections Open:	0

- 1) FC01 Read Coil Status – Modbus Function Code 1: Number of Read Coil Status requests received.
- 2) FC02 Read Input Status – Modbus Function Code 2: Number of Read Input Status requests received.
- 3) FC03 Read Holding Registers – Modbus Function Code 3: Number of Read Holding Registers requests received.
- 4) FC04 Read Input Registers – Modbus Function Code 4: Number of Read Input Registers requests received.
- 5) FC05 Force Single Coil – Modbus Function Code 5: Number of Write Coil Status requests received.
- 6) FC06 Preset Single Register – Modbus Function Code 6: Number of Write Holding Register requests received.
- 7) FC15 Force Multiple Coils – Modbus Function Code 15: Number of Write Multiple Coil Status requests received.
- 8) FC16 Preset Multiple Registers – Modbus Function Code 16: Number of Write Multiple Holding Register requests received.
- 9) FC23 Read/Write 4X Register – Modbus Function Code 23: Number of Read/Write Holding Registers requests received.
- 10) Successful Responses Sent – Total number of Read/Write messages sent by the gateway.
- 11) Error Responses Sent - Total number of Read/Write errors sent by the gateway.
- 12) Timeouts TCP Closed – Total number of Read/Write timeouts that cause the Modbus TCP/IP connection to close.
- 13) TCP Connections Open – Number of Modbus TCP/IP connections that have been opened to the gateway.

## Diagnostics – BACnet/IP Server

Select the **BACnet/IP Server** in the drop-down menu on the Diagnostics Page. Additional diagnostic information can be found by clicking the **Help** button.

**Diagnostics**

BACnet/IP Server ▾

View

▾

View

Clear All Values

Device Status

Configuration Mode...

Gateway Restart Needed

Help

**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.
- 2) If viewing BACnet/IP Server, this will only clear the values for the BACnet/IP Server section of the gateway.

### Device Status:

Device Status

Configuration Mode... Gateway Restart Needed

- 1) Connected – The gateway is connected to a BACnet/IP client.
- 2) Not Connected – The gateway is not connected to a BACnet/IP client.
- 3) Error: Timeout –The gateway has not received a read/write request in the amount of time specified by the Inactivity Timeout.

### LED Status:

LED Status

Connection Status:

Configuration Mode

- 1) Good Communication (Solid Green) – Connected to a BACnet/IP client.
- 2) Never Connected (Blink Green) – Gateway has never been connected to a BACnet/IP client.
- 3) Connection Timeout (Blink Red) –The gateway has not received a read/write request in the amount of time specified by the inactivity timeout.



## Variables:

<b>Variables</b>	
Total Msg Request Count:	0
Read Prop Request Rcvd:	0
Read Mult Prop Request Rcvd:	0
Write Prop Request Rcvd:	0
Write Mult Prop Request Rcvd:	0
Total Msg Response Count:	0
Read Prop Response Sent:	0
Read Mult Prop Response Sent:	0
Write Prop Response Sent:	0
Write Mult Prop Response Sent:	0
Error Response Count:	0
TMO Response Count:	0
COV Success Count:	0
COV Error Count:	0
<b>Status Strings</b>	
Last Error Code:	

- 1) Total Msg Request Count – Total number of messages received from the BACnet/IP client.
- 2) Read Property Request Received – Number of Read Property requests received from the BACnet/IP client.
- 3) Read Multiple Property Request Received – Number of Read Property Multiple requests received from the BACnet/IP client.
- 4) Write Property Request Received – Number of Write Property requests received from the BACnet/IP client.
- 5) Write Property Multiple Request Received – Number of Write Property Multiple requests received from the BACnet/IP client.
- 6) Total Msg Response Count – Total number of messages sent to the BACnet/IP client.
- 7) Read Property Response Sent – Number of Read Property Responses sent to the BACnet/IP client.
- 8) Read Multiple Property Response Sent – Number of Read Property Multiple responses sent to the BACnet/IP client.
- 9) Write Property Response Sent – Number of Write Property responses sent to the BACnet/IP client.
- 10) Write Multiple Property Response Sent – Number of Write Property Multiple responses sent to the BACnet/IP client.
- 11) Error Response Count – Total number of read/write errors received.
- 12) Timeout Response Count – Total number of read/write timeouts.
- 13) COV Success Count – Total number of successful COV messages.
- 14) COV Error Count – Total number of COV error messages.

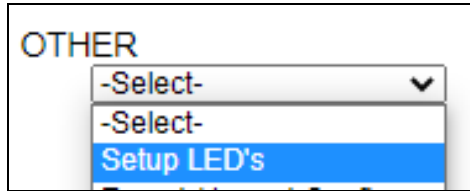
## Common Error Strings:

- 1) BS: UNHANDLED\_MSG\_TYPE – The gateway received a BACnet/IP message that it doesn't know how to process.
- 2) BS: Message Abort - The gateway aborted a message due to one of the common reasons below:

- a) "Buffer Overflow" – The BACnet/IP client is asking for too much information in a single message.
  - b) "Invalid ADPU" – The gateway is not able to process the message, try again later.
  - c) "Preempted by Higher Priority" – The BACnet/IP client message has aborted due to a higher priority task, try again later.
  - d) "Segmentation Not Supported" – The gateway does not support segmentation. Break up the client request into multiple requests.
- 3) BS: Message Reject - The gateway rejected a message due to one of the common reasons below:
- a) "Buffer Overflow" – The BACnet/IP client is asking for too much information in a single message.
  - b) "Invalid Parameter Data Type" – This BACnet/IP data type is not supported.
  - c) "Invalid Tag" – BACnet/IP message is not how the gateway expects the message.
  - d) "Parameter Out of Range" – The BACnet/IP client is asking for information outside of the gateway's defined range.
- 4) BS: Message Error "XXXXX" – The gateway is sending an error a message due to the listed explanation:
- a) "Inconsistent parameters" –
    - i) BACnet/IP client tried to write a priority that was out of range or reserved (Priority 6) and was rejected.
    - ii) BACnet/IP client tried to write to ALL, REQUIRED, or OPTIONAL object property.
  - b) "Invalid Data Type" – BACnet/IP client tried to use a data type with an object that is not supported.
  - c) "Service request denied" – BACnet/IP request cannot be processed because the BACnet/IP connection is not established.
  - d) "Read access denied" – BACnet/IP read request cannot be processed.
  - e) "Unknown object" – BACnet/IP client tried to access an object our gateway does not support.
  - f) "Unknown property" – BACnet/IP client tried to access a property our gateway does not support for that object type.
  - g) "Unsupported object type" – BACnet/IP client tried to access an object type our gateway does not support.
  - h) "Value out of range" – BACnet/IP message could not be completed because the passed value was not in the valid range.
  - i) "Write access denied" – BACnet/IP client tried to write a non-writeable property in our gateway.
  - j) "Invalid array index" –
    - i) BACnet/IP client tried to write a priority that was out of range or reserved (Priority 6) and was rejected.
    - ii) BACnet/IP client tried to write an array for an object or property that doesn't have an array index.
  - k) "Unknown device" – Gateway is trying to send a message to a device we have not had previous communication with on the network.
  - l) "Timeout" – BACnet/IP message timed out.
  - m) "Resources busy" – BACnet/IP message cannot be processed right now.
  - n) "Segmentation not supported" – BACnet/IP message is too large to send in one message.
  - o) "Service not supported" – BACnet/IP client tried to perform a service that the gateway does not support.
  - p) "Abort Other" – BACnet/IP message is aborted for an unknown reason.
  - q) "Invalid Tag" – BACnet/IP message is not how we expect.
  - r) "Unknown" – BACnet/IP message error for an unknown reason.

## LED Configuration

To modify the behavior of the LEDs on the 460 gateway, navigate to **Other->Setup LEDs**.

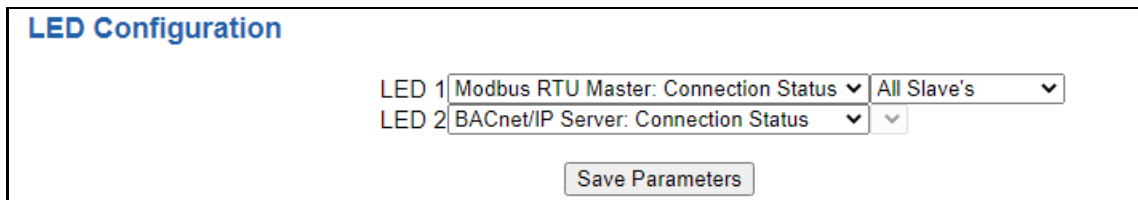


Each LED may be set to Disabled, Protocol 1, or Protocol 2. If either protocol is a master/client, you may set the LED to represent either all slaves/servers configured in the gateway or a slave/server device.

To select a slave/server device:

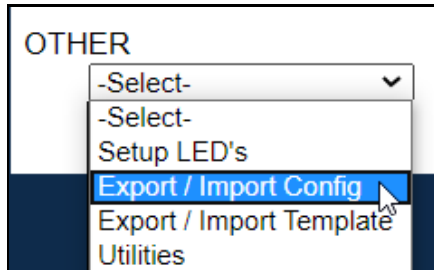
- 1) Select the protocol in the left dropdown menu.
- 2) Click **Save Parameters** to generate the second dropdown menu.
- 3) Select the individual slave/server in the right dropdown menu.

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

A screenshot of the 'LED Configuration' form. The title 'LED Configuration' is in blue. Below it, there are two rows of dropdown menus. The first row is labeled 'LED 1' and contains two dropdowns: 'Modbus RTU Master: Connection Status' and 'All Slave's'. The second row is labeled 'LED 2' and contains two dropdowns: 'BACnet/IP Server: Connection Status' and an empty dropdown. Below the dropdowns is a button labeled 'Save Parameters'.

## Configuration Files

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



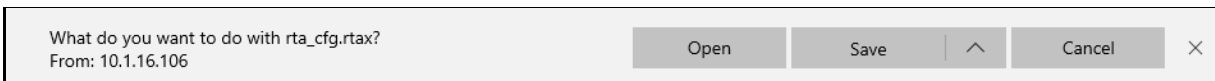
## Export Configuration

### Export Configuration

Save Configuration to File

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.

**Network Settings have changed. Manually enter IP Address of X.X.X.X in the URL.**

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.

### Import Configuration

No file chosen

☐ Import Network Settings

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.

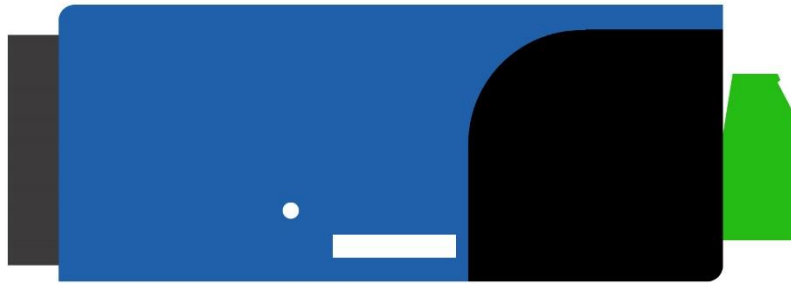
### Replacing Configuration Using SD Card

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.

## Intelligent Reset Button

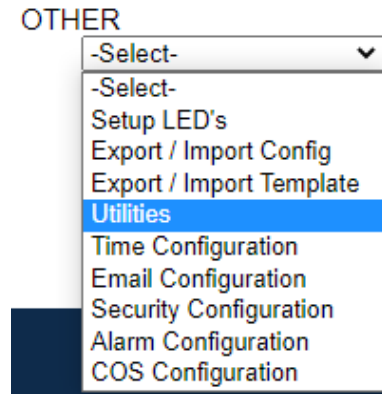
If the IP Address of the gateway is forgotten or is unknown, there is an easy way to recover the IP Address using a reset button on the hardware.



- 1) On the side of the gateway with the SD card slot, there is a small pinhole. Using a paperclip, press the button through this pinhole and hold the button for at least 5 seconds.
- 2) After 5 seconds, the unit will acknowledge the command and LED 1 and LED 2 will start an alternate Blink Green quickly pattern.
- 3) Release the button and the gateway will reset to default IP settings (DHCP).

## 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.

Revisions

Listing of Revisions

File List

File List

Identify Device

Start Flashing LED's

Set Up Log

Log Configuration

Revert To Last Powerup

Revert to Last Powerup

Revert All

Revert to Manufacturing Defaults

Reformat Flash

Reformat Flash