460MMDFM-NNA4 Protocol Gateway

Product User Guide

Firmware Version 5.2.14

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.

Revision History

Version	Date	Notes
5.1.1	6/7/16	Features Added 1. Reworked AutoMap functions to automap per device and made default for most productssupport@rtaautomation.com 2. Implemented Automatic reboot and redirect upon startup 3. Modified Template usage so it can be applied easily on a protocol or product level 4. All imported configurations will force Manual mode for Mapping and AutoServer functionalities 5. Allow saving/replacing of configuration via SD Card 6. Added DHCP for Network Settings (default)
5.2.1	10/12/16	Features Added 1. Replaced Build Date with Revision Number 2. DF1 Master (DFM) Released 3. NNA4 Dual RS485 Hardware Bug Fixes 1. BACnet/IP Server (BS) Relinquish Default 2. BACnet MS/TP (BMS) Reninquish Default 3. BACnet MS/TP Slave (BMS) CSV Object Parameter 4. Modbus TCP/IP Client (MC) XML Import Bug when Write Only 5. Modbus TCP/IP Client (MC) Write Directional changed Web Parameters
5.2.2	1/12/17	Features Added 1. Added ability to add in prefixes to the filename (for BETA and DEMO) 2. Updated Copyright Year to 2017
5.2.3	1/19/17	Bug Fixes 1. BACnet/IP Server (BS) COV (Change of Value) Notifications with Binary Objects (both Input and Output)
5.2.4	1/25/17	Bug Fixes 1. BACnet/IP Server (BS) COV (Change of Value) Notifications with Binary Output Objects
5.2.5	2/16/17	Bug Fixes 1. BACnet/IP Server (BS) increased the number of COV's supported from 100 to 2800 across all objects 2. BACnet MS/TP Slave (BMS) increased the number of COV's supported from 100 to 2800 across all objects
5.2.6	2/21/17	Bug Fixes 1. BACnet/IP Server (BS) fixed the auto-server for Binary Objects for non-1 Bit Pack Option 2. BACnet MS/TP Slave (BMS) fixed the auto-server for Binary Objects for non-1 Bit Pack Option 3. BACnet MS/TP Slave (BMS) fixed the load template for Binary Output Objects for 1 Bit Pack Option
5.2.9	3/15/17	Bug Fixes 1. Update for Translator Web Display for Mapping Configuration (buffer too small) 2. Update for String Translator Web Display for Mapping Configuration (buffer too small)
5.2.14	5/4/17	Bug Fixes 1. Completely removed unit id from MS protocol. MS will respond to all Unit IDs 2. Removed "Unit ID" description from MS help page

Overview

The 460MMDFM-NNA4 gateway connects up to 32 Modbus RTU Slaves with as many as 32 DF1 Slaves. By following this guide, you will be able to configure the 460MMDFM-NNA4 gateway.

For further customization and advanced use, please reference the appendices located on the CD or online at: http://www.rtaautomation.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@rtaautomation.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 – NNA4

DIN Rail Mount

3.88

2.57

Note: All dimensions are in Inches

1.06

PWR 1 2
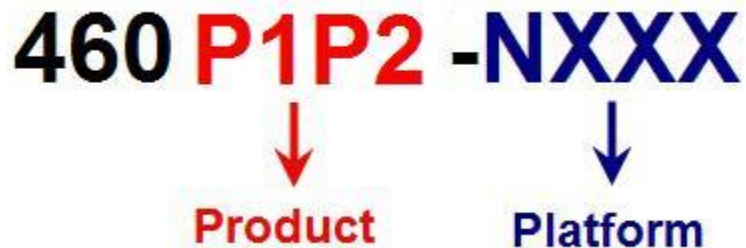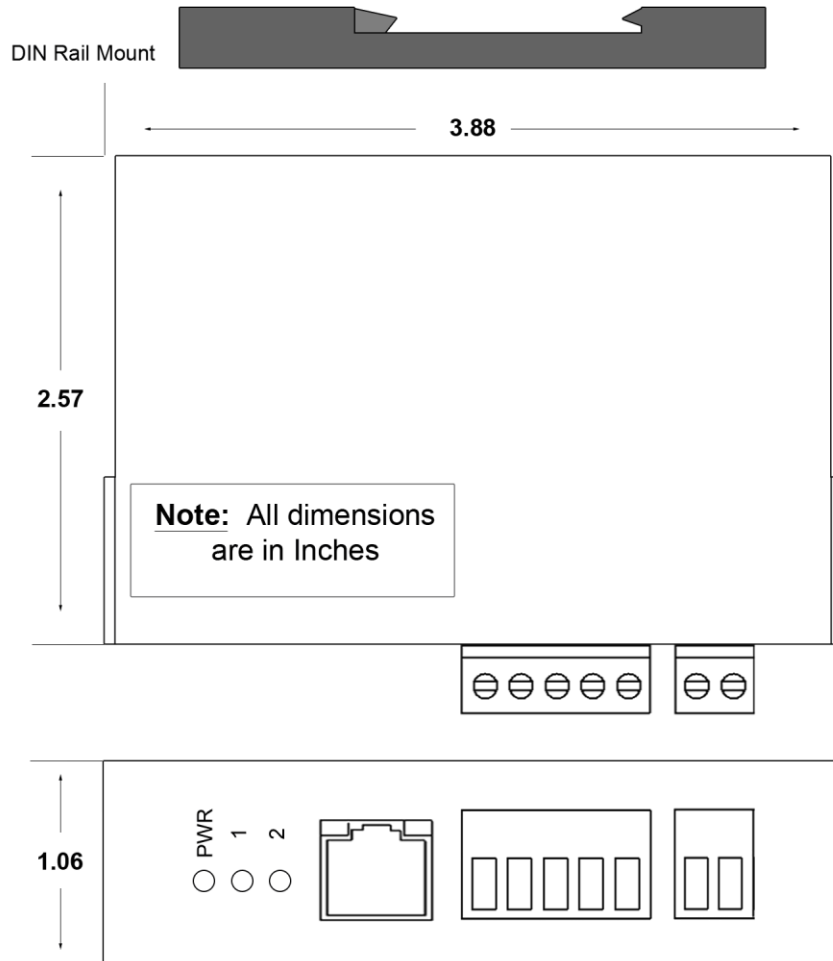
Powering the Gateway

- An 8-24 VDC power source to the gateway, Red Wire = (+) Black Wire = (-).
    a. The unit draws 175mA @ 12V.
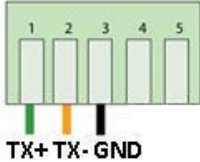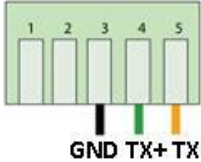
Port Configuration

The Port Configuration page is where you set port specific parameters. These settings must match the settings of the device(s) that you are connecting to.

When you have completed your port configuration, click the **Save Parameters** button.

Mounting with a DIN Rail

Installing

Follow these steps to install your interface converter.

1) Mount your DIN Rail.

2) Hook the top mounting flange over the DIN Rail.

3) While pressing the 515RTAAIC against the rail, press down to engage the spring loaded upper clip and rotate the unit parallel to the DIN Rail.

4) Release downward pressure.

Spring Loaded Upper Clip
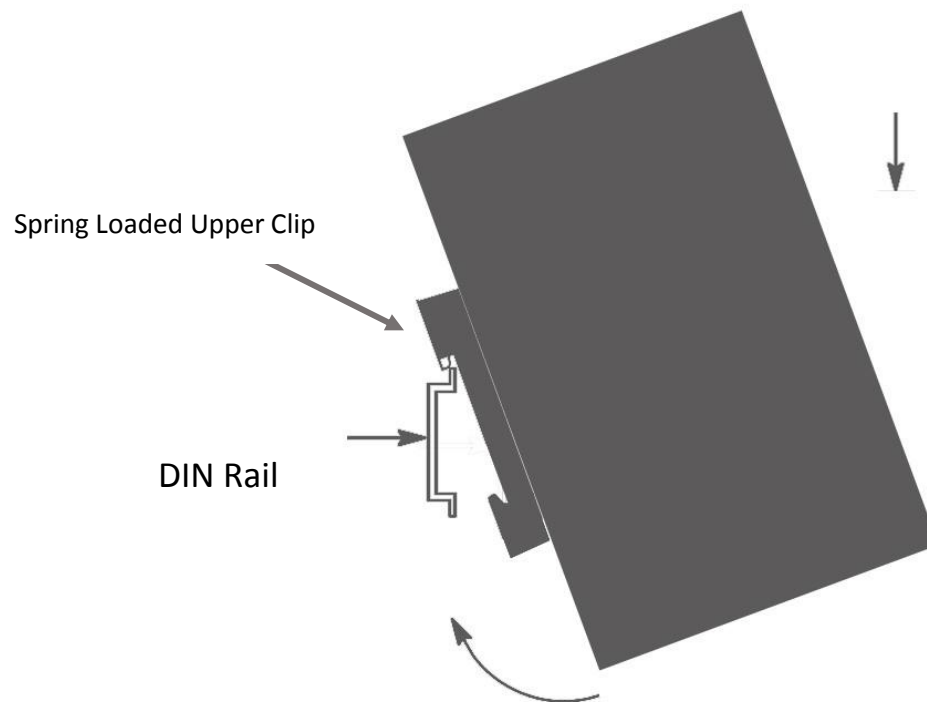
DIN Rail

Removing

Follow these steps to remove your interface converter.

1) Press down on unit to engage the spring loaded upper clip.

2) Swing bottom of 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.

1) Insert the provided CD-ROM into a computer also on the network.
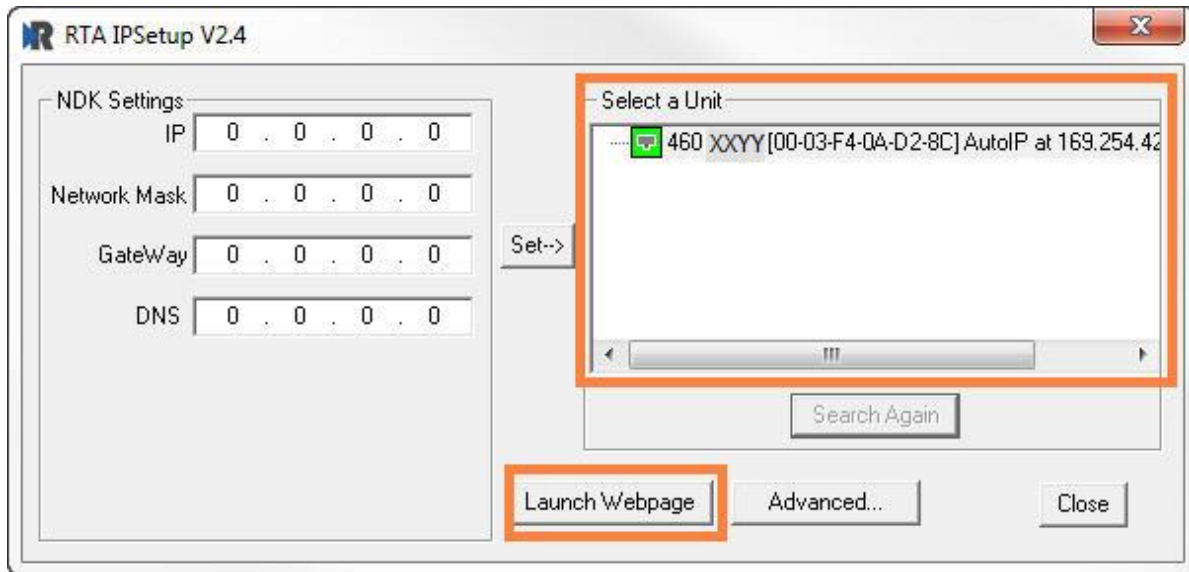
2) Run the IPSetup.exe program from the CD-ROM.

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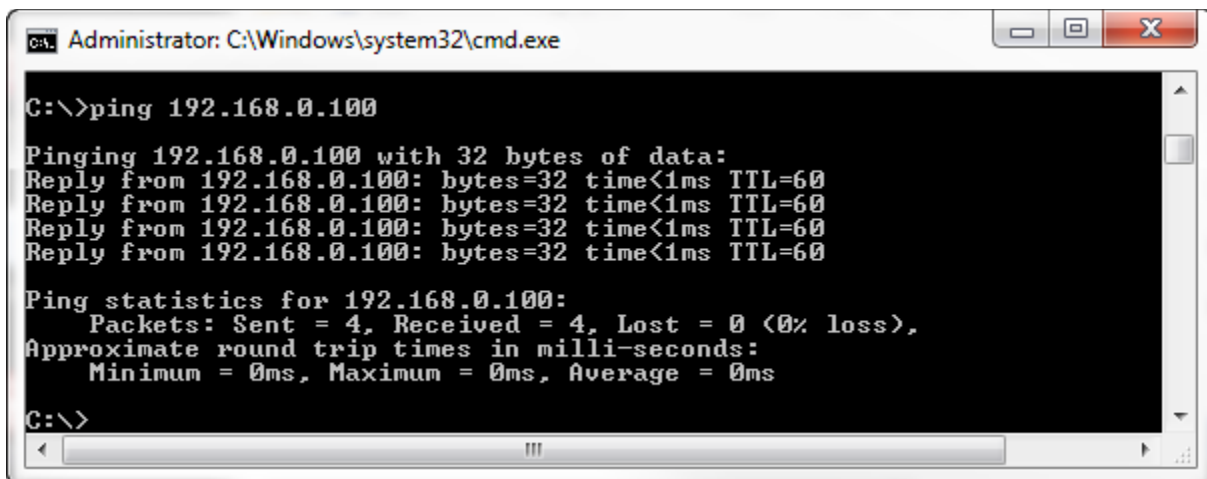
> **Default setting is set to DHCP. If DHCP fails, default IP Address is 169.254.x.y**

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.

192.168.0.100
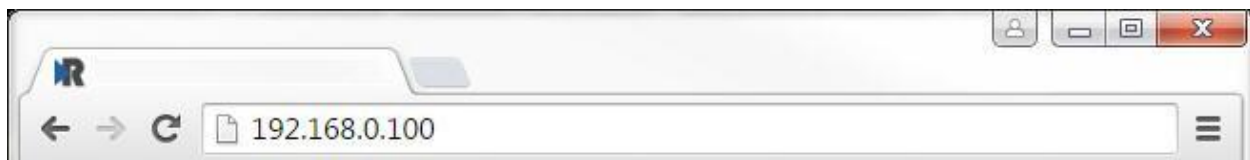
Committing Changes to the Settings

- 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:
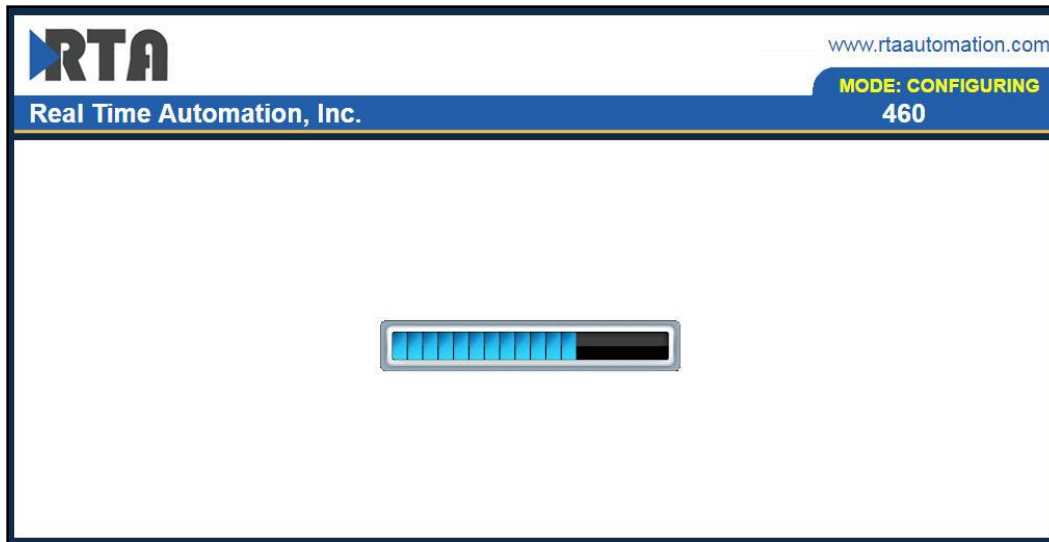
- The reboot can take up to 20 seconds. You will know the save was successful if the red box is no longer present.
    - If the IP address has not been modified, the gateway will automatically redirect to the main page.
    - If the IP address was modified, a message will appear at the top of the page to instruct the user to manually open a new webpage at that new IP.

Main Page

The main page is where important information about your gateway and its connections are displayed.

 Mode (orange box below):

Running Mode:
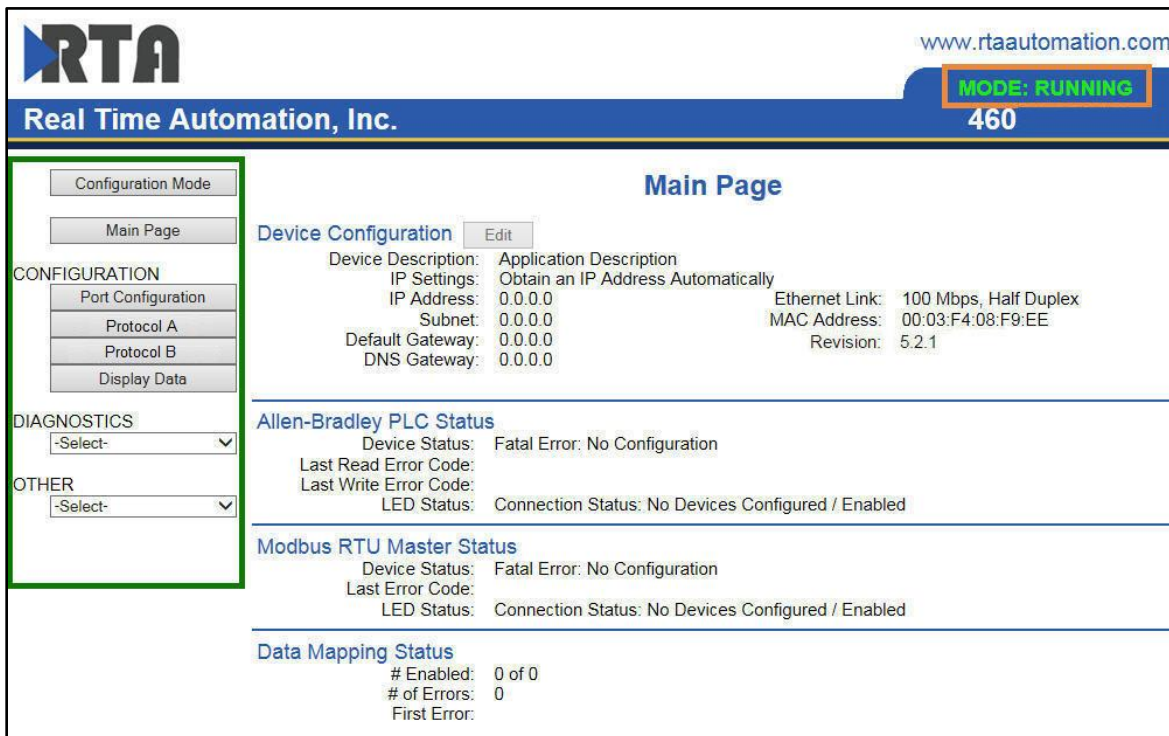
- Protocol communications are enabled

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

Configuring Mode:

- Protocol communication is stopped and no data is transmitted

- Configuration is allowed

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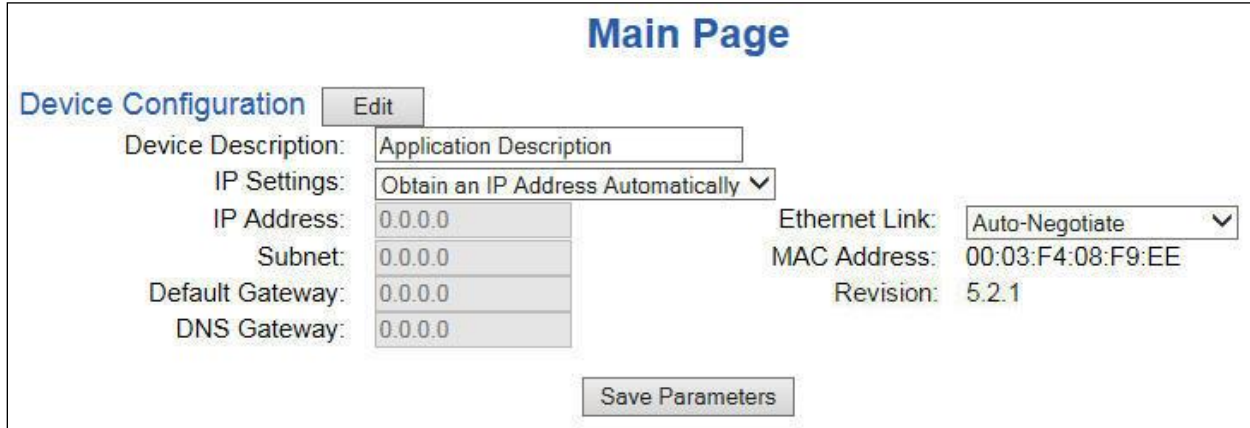
You can easily switch between modes and navigate between pages (Configuration, Diagnostics, and Other pages) using the buttons on the left hand side.

Device Configuration

The device configuration area is where you assign the device description, IP address, and other network parameters. Changes can only be made when the gateway is in Configuration Mode. Click the **Edit** button to make these changes.

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

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

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

Modbus RTU Master Configuration

Click the **Modbus RTU Master** button to access the configuration page.

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

Serial Port: Port 0 (T-Strip) Disabled ▼

2) **Delay Between Messages**: Enter the length of time to delay between read and write scan line requests (ms).

3) **Response Timeout**: Enter the amount of time the gateway should wait before a timeout is issued for a read/write request (ms).

4) **Dependency Protocol**: If enabled, Modbus RTU Master communication will stop if communication to the selected protocol is lost.

Modbus RTU Master Configuration Help

Serial Port: Port 0 (T-Strip) Disabled ▼
Delay Between Messages: 10   10-60000 ms
Response Timeout: 500   50-60000 ms
Dependency Protocol: None ▼

Save Parameters

Modbus RTU Master Device Configuration

The bottom area of the Modbus RTU Master Configuration page lets you configure up to 32 external Modbus RTU Slave devices.

1) To add additional Slave connections, click the -Select- dropdown under Modbus RTU Master Device List and select **Add Generic Slave** option.

-To remove a device, navigate to the slave to delete using the **<<** and **>>** buttons and click the **Delete Slave** button.

-To create a new slave with the same parameters already configured from another slave, click the -Select- dropdown and select the **Add from Modbus RTU X** option (where X represents the slave you wish to copy parameters from). Once created, you can make any additional changes needed to that new slave.

2) The **Enable** check box should be selected for the device.

3) Enter a **Device Label** to identify the device within the gateway.

4) Enter a unique Modbus RTU **Slave Address** for the device on the network.

5) **Force Function Code 15/16 for Single Writes:** Only select this if the Modbus RTU device does not support Modbus Function Code 5/6.

6) **Enable 0-Based Addressing**: Check ONLY if the Slave you are connecting to begins their register numbering at 0 OR they specify that their device addresses are 0-based.

7) **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.

8) **Enable Modbus ASCII**: Only select this if your Modbus device is also using ASCII messaging. By default, the device will use Modbus RTU.

9) 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.

10) Enter the number of Read Scan Lines and Write Scan Lines.

11) Click the **Generate Scan Lines** button to have the read and write scan lines auto-generate for you. You may manually configure the read and write scan lines after they have been generated.

Configuring Read Scan Lines

Follow these steps to manually configure Read Scan Lines.

1) Select **View Read Scan Lines** if not already selected.

2) Select a Point Type for each Scan Line. Options include: Coil Status, Input Status, Input Registers, and Holding Registers. **Note**: Input/Holding Registers also 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.

   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 (This will be 1 based if *Enable 0-Base Addressing* is unchecked, or 0 based if checked).

4) Enter the # of consecutive points to read for that point/data type. See the *Scan Line Data Limit* section at the bottom of the webpage for max values in a scan line.

		Line #	Point Type	Starting Address	# of Points *See Limits Below
☐	🗑	1	0x Coil Status ▼	1	1

Read Scan Lines (Modbus RTU to 460)

<< 1-1 >>

Configuring Write Scan Lines

Follow these steps to manually configure Write Scan Lines.

1) Select **View Write Scan Lines** if not already selected.

2) Select a Point Type to configure. Options include: Coil Status and Holding Registers. **Note**: Holding Registers also 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.

      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 (This will be 1 based if *Enable 0-Base Addressing* is unchecked, or 0 based if checked).

4) Enter the # of consecutive points to write for that point/data type. See the *Scan Line Data Limit* section at the bottom of the webpage for max values in a scan line.

View Read Scan Lines				View Write Scan Lines

Write Scan Lines (460 to Modbus RTU)

☐ 🗑	Line #	Point Type	Starting Address	# of Points *See Limits Below
☐	1	0x Coil Status ▼	1	1
			<< 1-1 >>	

Configuring Read and Write Scan Lines (cont.)

If you are configuring more than 25 scan lines click **<<** or **>>** to navigate to the next group of 25. When finished, click the **Save Parameters** button.

Below is the Scan Line Data Limit for each Point Type and the max Length Range associated with them.

Note: If the first address of the Modbus RTU Slave device starts at 0 (Register/Coil starting addresses can be found in the Modbus RTU Slave's documentation), be sure to check the *Enable 0-Base Addressing* box in the gateway to ensure proper communication. If improperly configured, expected addressing may be off by +/- 1.

Scan Line Data Limit

Point Type	Length Range
Coil Status	512
Input Status	512
Input Register (16 Bit Int/Uint)	125
Input Register (32 Bit Int/Uint/Float)	62
Input Register (64 Bit Int/Uint/Float)	31
Input Register (String - 2 char/reg)	125
Holding Register (16 Bit Int/Uint)	125
Holding Register (32 Bit Int/Uint/Float)	62
Holding Register (64 Bit Int/Uint/Float)	31
Holding Register (String - 2 char/reg)	125

DF1 Master Configuration

Click the **DF1 Master** button to access the configuration page.

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

Serial Port: Port 0 (T-Strip) Disabled

2) **Source ID**: Enter the Source Station ID for the gateway acting as the DF1 Master device.

3) **Protocol Mode**: Select the DF1 Protocol Mode: Half-duplex or Full-duplex.

4) **Frame Verification**: Select the DF1 Frame Verification: CRC (16-bit) or BCC (8-bit). All DF1 Slaves need to match this selection

5) **Delay Between Messages**: Enter the length of time to delay between read and write scan line requests (ms).

6) **ACK Timeout**: Enter the amount of time to wait for the DF1 Acknowledgement message before flagging a timeout (ms).

7) **Receive Timeout**: Enter the amount of time the gateway should wait before a timeout is issued for a read/write request (ms).

8) **Number of Retries**: Enter the number of times the gateway will re-send messages before logging a timeout error and moving onto the next message.

9) **Dependency Protocol**: If enabled, DF1 Master communication will stop if communication to the selected protocol is lost.

DF1 Master Device Configuration

The bottom area of the DF1 Master Configuration page lets you configure up to 32 external DF1 Slave devices.

1) To add additional Slave connections, click the -Select- dropdown under DF1 Master Device List and select **Add Generic Slave** option.

DF1 Master Device List

-Select- ▼ | Delete DF1 Slave

-To remove a device, navigate to the slave to delete using the **<<** and **>>** buttons and click the **Delete DF1 Slave** button.

-To create a new slave with the same parameters already configured from another slave, click the -Select- dropdown and select the **Add from DF1 X** option (where X represents the slave you wish to copy parameters from). Once created, you can make any additional changes needed to that new slave.

2) The **Enable** check box should be selected for the device.

3) Enter a **Device Label** to identify the device within the gateway.

4) Enter a unique **Destination ID** for the device on the network. This number should be different from the Source ID entered above.

5) **Communication Command:** Select the DF1 Read/Write Communication Commands to use to communicate to the Slave device.
   - 500CPU Read/Write (default): uses DF1 Protected Typed Logical Read/Write messages with 3 address fields
   - PLC5 Read/Write: uses DF1 Typed Read/Write messages

DF1 Master Device List

-Select- ▼	Delete DF1 Slave	
<<	1	>>
	1-1	

☐ Enable	**DF1 Slave 1**	
Device Label DFM01	Destination ID 0	0-255
Communication Command 500CPU Read/Write ▼		
# of Read Scan Lines 0	0-100	# of Write Scan Lines 0	0-100
Generate Scan Lines		

6) Enter the number of Read Scan Lines and Write Scan Lines.

7) Click the **Generate Scan Lines** button to have the read and write scan lines auto-generate for you. You may manually configure the read and write scan lines after they have been generated.

Configuring Read Scan Lines

Follow these steps to manually configure Read Scan Lines.

1) Select **View Read Scan Lines** if not already selected.

2) Select a File Type for each Scan Line. Options include: B (Binary), N (Int), F (Real), and ST (String).

3) Enter the File Number for the File Type selected.

4) Enter the File Offset for the File Number selected.

5) Enter the # of consecutive points to read for that File Type. See the *Scan Line Data Limit* section at the bottom of the webpage for max values in a scan line.

Configuring Write Scan Lines

Follow these steps to manually configure Write Scan Lines.

1) Select **View Write Scan Lines** if not already selected.

2) Select a File Type for each Scan Line. Options include: B (Binary), N (Int), F (Real), and ST (String).

3) Enter the File Number for the File Type selected.

4) Enter the File Offset for the File Number selected.

6) Enter the # of consecutive points to read for that File Type. See the *Scan Line Data Limit* section at the bottom of the webpage for max values in a scan line.

Configuring Read and Write Scan Lines (cont.)

If you are configuring more than 25 scan lines click **<<** or **>>** to navigate to the next group of 25. When finished, click the **Save Parameters** button.

Below is the Scan Line Data Limit for each Data Type and the max Length Range associated with them.

Scan Line Data Limit

Data Type	Length Range
Binary (B)	100
Int (N)	100
Real (F)	50
String (ST)	1

Mapping - Transferring Data Between Devices

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

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

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

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

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

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

Display Mapping and Values

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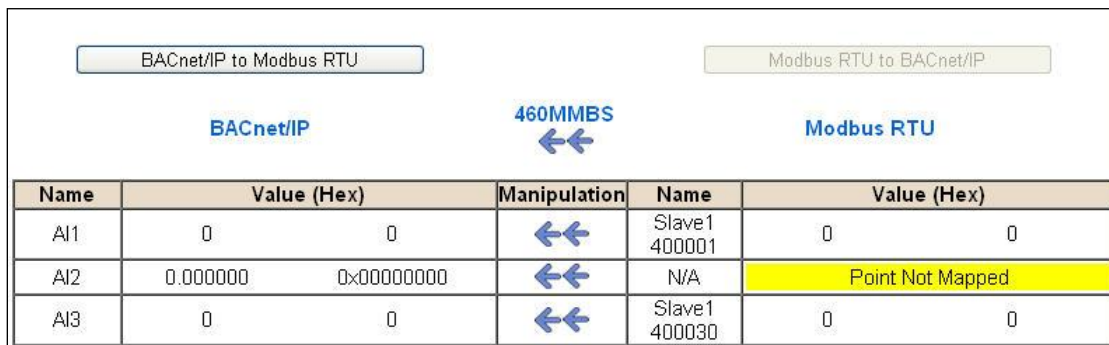
Display Data

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

This page is very useful when verifying that all data is mapped somehow from one protocol to another. If a data point is not mapped, it will display on this page in a yellow highlighted box.

In the above example, we see the following:

- Modbus 400001 from Slave 1 is being mapped to AI1 on BACnet

- Nothing is being moved from Modbus to AI2 on BACnet

- Modbus 400030 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 (right side) is the source and the PLC (left side) is the destination.

- The 460 gateway has received valid responses from Modbus registers 400001-400005 and therefore can pass the data on to the PLC tag called MC2PLC_INT.

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

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

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

Display String

Click the **Display String** button to view how the string data types are mapped and what the values of each string are. Here you will see how each string from each protocol is mapped to the other. To view, select the source or destination group and the String from the dropdown menu to generate the information regarding that device. The string data will be displayed in both hex and ASCII.

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.

In the example below, this page reflects the Modbus to PLC flow of data. Since the Destination "Dst: ETC01 ETC01_G2N0_STRING" displays "Data Not Valid", it can be assumed that the source field has not yet been validated.

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

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.

Data and String Mapping – Auto-Configure

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

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

The following are examples of the Auto-Configure function.

1) This example shows a common valid setup.

    a. Both Source values were able to be mapped to a corresponding Destination value.
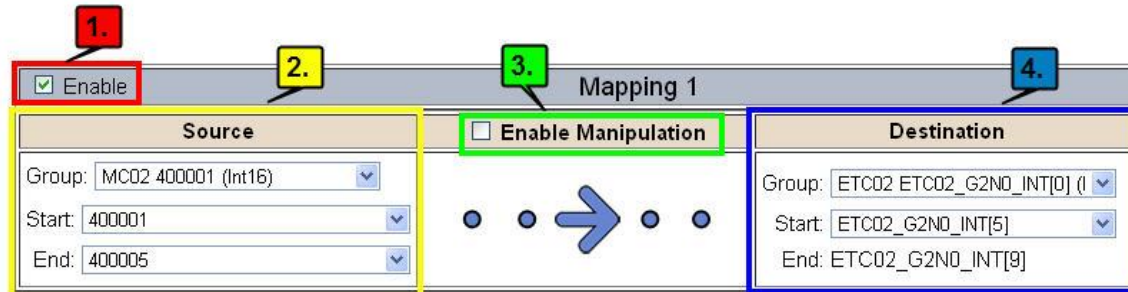
2) This example shows how Auto-Configure will make its best guess.
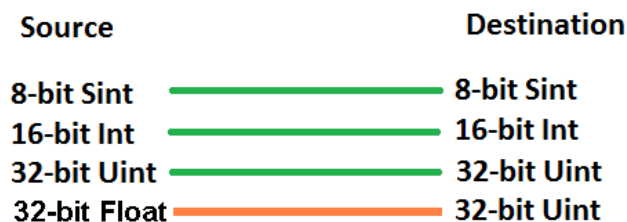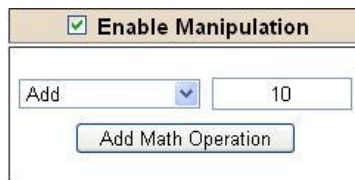
    a. The 32-bit Float from the Source location could not find a matching Destination data-type. After all other like data types were mapped, the only data type available was the 2nd 32-bit Uint data type. Auto-Configure was completed even though the data in the Float will be truncated.

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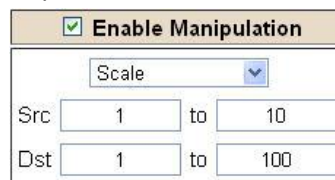
Below are the different parts that can be modified to make up a data mapping.
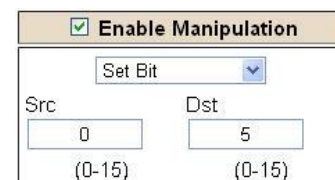
1) Enable (red box above): Check to enable mapping. If not checked, this mapping is skipped.
2) Source Field (yellow box above) :
   a. Group - Select the data group you set up in the protocol config to use for this mapping.
   b. Start - This is the starting point for this mapping.
   c. End - This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

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

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

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

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

Data Mapping – Adding Diagnostic Information

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

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

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

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

2) Temporary Ram (Double)
   a. This is similar to 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.
4) XY_NetBmpStat
   a. If a protocol is a Client/Master, there is a Network Bitmap Status that is provided. 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.
   b. 0x00000002 shows that only device 2 is connected
   c. 0x00000003 shows that only devices 1 and 2 are connected
   d. 0x00000004 shows that only device 3 is connected

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)1st byte***

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

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

	PLC to Modbus TCP/IP				Modbus TCP/IP to PLC	
	PLC		**460ETCMC** ←←		**Modbus TCP/IP**	
Name	**Value (Hex)**		**Manipulation**	**Name**	**Value (Hex)**	
PLC_Status	19	0x00000013	←←	ETC Status	19	0x00000013
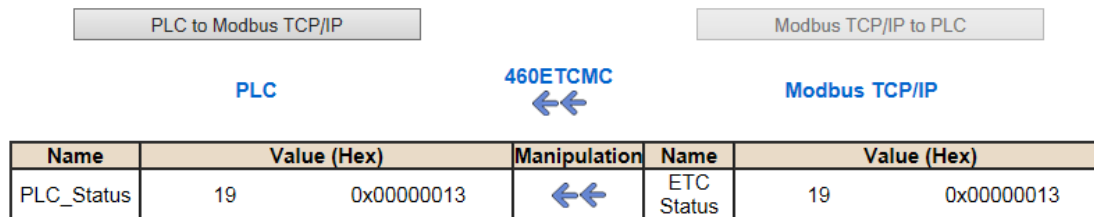
Example: ETC Status is 0x00000013 (19 decimal), here is the break down

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

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

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

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

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

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

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

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

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

PLC   **460ETCMC**   **Modbus TCP/IP**
                              ←←

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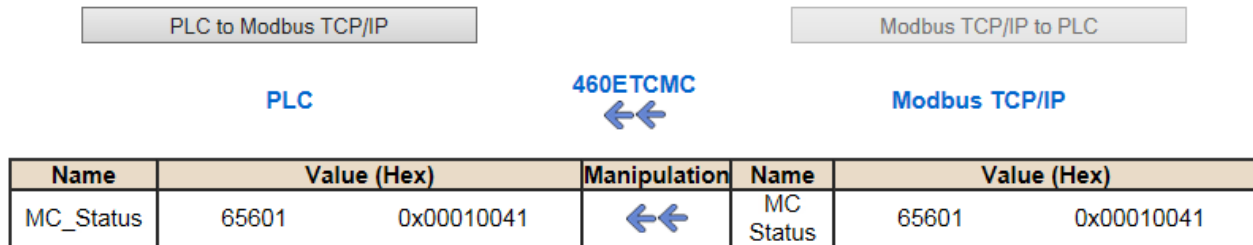
Example: MC Status is 0x00010041 (65601 decimal), here is the break down, we know that bytes 1 and 3 are being used, so here is the break down,

Common Status:

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

Recoverable Faults:

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

Total: 0x010041   65,601

String Mapping – Explanation

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

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

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

Mapping – Auto-Configure Mode to Manual Configure Mode

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

After you click this button, you will be prompted to confirm if this is really what you want to do.
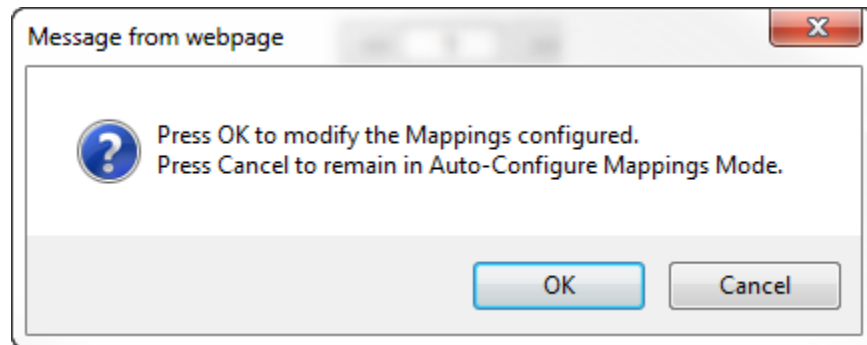
Click **OK** to proceed to Manual Configure Mode or click **Cancel** to remain in Auto-Configure Mappings Mode.

Once OK is clicked, there are 2 options on how to proceed from here.
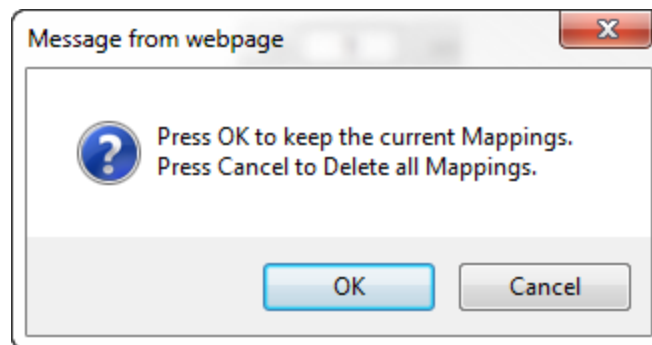
1) To keep the mappings that are already configured press **OK**.

   a. You would want this option if you are adding additional mappings or you want to modify the mapping(s) that already exist.

2) To delete the mappings that are already there and start over press **Cancel**.

To modify the number of mappings, enter a number 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.
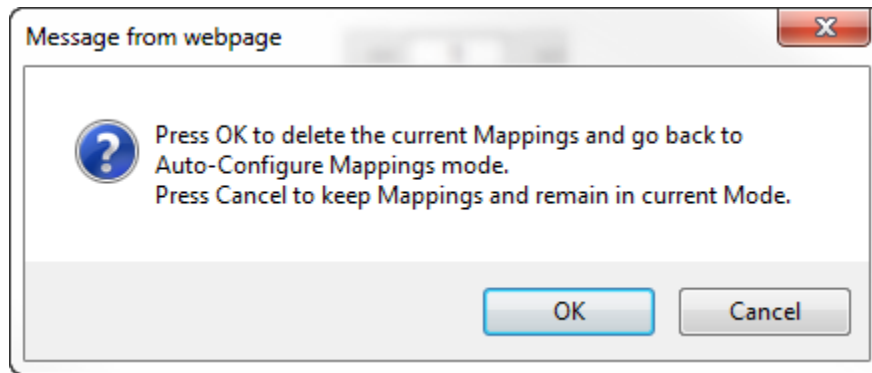
Click **OK** to proceed to delete all current mappings and go back to Auto-Configure Mappings Mode. Click **Cancel** to keep all mappings and remain in Manual Configure Mode.

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

View as Text

Data Mapping

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

Each line on this page will read as follows:

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

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

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

String Mapping

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

Each line on this page will read as follows:

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

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

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-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.

Web Page	Security
All Web Pages	No Access ∨ Set

Web Page	Security
Main Page	Full Access ∨
Device Configuration	Full Access ∨
Port Configuration	Full Access ∨
BACnet/IP Server	Full Access ∨
Modbus RTU Master	Full Access ∨
View Mapping	Full Access ∨
Mapping	Full Access ∨
Setup LED's	Full Access ∨
Diagnostic Info	Full Access ∨
Logging	Full Access ∨
Display Data	Full Access ∨
Export Configuration	Full Access ∨
Import Configuration	Full Access ∨
Save As Template	Full Access ∨
Load From Template	Full Access ∨
Utilities	Full Access ∨
Email Configuration	Full Access ∨
Alarm Configuration	Full Access ∨
String Mapping	Full Access ∨
View String Mapping	Full Access ∨
Display String	Full Access ∨

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

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.

Security - Log Out

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

Closing the browser is not sufficient to log out.

Email Configuration

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

You can configure up to 10 email addresses.

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

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

Email Configuration [Help]

Number of Emails to Configure: 1   0-10
[Setup Email(s)]

User	SMTP Mail Username	SMTP Mail Password	SMTP Server	From Email	To Email	Email Group
1						Group A ▼

[Save Parameters]

[Send Test Email(s)]

Alarm Configuration

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

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

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

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

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

Diagnostics – Alarm Status

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

1) # Alarms Enabled: This is a count of enabled alarms.

2) # Alarms Active: This is how many alarms are presently active (set).

3) Last Active Alarm: This is the last alarm that the gateway detected.

4) **Clear # of Times Active**: This will reset all alarms '# of Times Active' to 0.

5) Alarm #: The reference number to the given alarm on the alarm setup page.

6) Name: The name of the alarm.

7) Status: The current status of the alarm, either OK or ALARM.

8) # of Times Active: This count represents the number of times this alarm has become active. If an alarm is triggered, this count will increment.

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.

![RTA Real Time Automation, Inc. logo with www.rtaautomation.com, 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	0-3600 s
Production Inhibit Timer: 0	0-60000 ms
Writes Before Reads: 10	0-255
Reads Before Writes: 1	1-255
Enable Data Integrity: ☑	

Save Parameters

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

Diagnostics Info

The Diagnostic page is where you can view the gateway's translations and protocol specific status information.

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

Diagnostics – Data and String Mapping

The Diagnostics->Diagnostic Info->System section displays the number of translations that are enabled, for both Data and String data types, the number of mappings that have an error, and the first mapping that has an error.

 # Enabled: Number of mappings that are enabled.

 # Error: The number of mappings that are enabled that have an error.

First Error: This is a detailed description of the first mapping that has an error.

Common Errors:

1) Destination or Source Point does not exist
   -Solution: Re-map the mapping
2) Source or Destination Pointer too small
   - 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
   - The actual data value is outside of the defined range
4) Math Error
   - Operation value cannot be 0
5) Scaling Error
   - Source Min must be smaller than Source Max
   - Destination Min must be smaller than Destination Max

Diagnostics – Modbus RTU Master

Select the Modbus RTU Master in the top dropdown menu on the Diagnostic page to view a breakdown of the diagnostics and common strings that are displayed on the page. You may also view individual Slave counters by selecting the device in the *All Slaves* dropdown and clicking **View**. Additional diagnostic information can be found by clicking the **Help** button.

NOTE: This page will auto-refresh every 5 seconds with the latest data.

Clear All Values - This will only affect current displayed values.
1) This will return all values displayed to 0 and clear the Status Strings.
   Example: If Viewing Modbus RTU Master – Slave Address 1, this will only clear the values for Slave Address 1. This will reduce the *All Slaves* values indirectly.

Device Status - This will only display when viewing *All Slaves*.
1) Connected and Running– the gateway is connected to all of the Modbus RTU Slaves.
2) Error: Timeout – No Modbus RTU Scan Lines are configured under an enabled Slave.
   Or, one or more enabled Modbus RTU Slaves are missing.
   a. Verify Modbus RTU device for Slave Address, 0 or 1 Base Addressing, ASCII Messaging, and Starting Addresses
   b. Verify that Port Settings used match the Modbus Slave that the gateway is communicating with.
   c. Verify wires for specific port settings.
3) Dependency Protocol Faulted – The dependent protocol is missing causing the communication to go inactive.
4) Unknown: First Scan Not Complete – Multiple Scan Lines are set up for the device and the gateway has not completed all of the scan lines for the first time.
5) Fatal Error: Couldn't Open Hardware Port – The serial port selected on the Modbus RTU Master Configuration page is not configured.
6) Fatal Error: No Configuration – No Modbus RTU Slaves are enabled though a Serial Port is enabled.

Diagnostics (MAC: 00:03:F4:06:15:E6)		**Diagnostics** (MAC: 00:03:F4:06:15:E6)	
Modbus RTU Master ▼ [View]	[Clear All Values]	Modbus RTU Master ▼ [View]	[Clear All Values]
All Slave's ▼ [View]		Slave Address 1 ▼ [View]	
Device Status	[Help]		[Help]
Connected and Running			
LED Status		**LED Status**	
Connection Status:	Connected	Connection Status:	Connected
Variables		**Variables**	
Network Bitmap Status:	0x00000003	Network Bitmap Status:	0x00000003
FC01 Read Coil Status:	2317	FC01 Read Coil Status:	912
FC02 Read Input Status:	0	FC02 Read Input Status:	0
FC03 Read Holding Registers:	0	FC03 Read Holding Registers:	0
FC04 Read Input Registers:	0	FC04 Read Input Registers:	0
FC05 Force Single Coil:	0	FC05 Force Single Coil:	0
FC06 Preset Single Register:	0	FC06 Preset Single Register:	0
FC15 Force Multiple Coils:	0	FC15 Force Multiple Coils:	0
FC16 Preset Multiple Registers:	0	FC16 Preset Multiple Registers:	0
Successful Responses Received:	2317	Successful Responses Received:	913
Error Responses Received:	0	Error Responses Received:	0
Timeouts:	0	Timeouts:	0
Status Strings		**Status Strings**	
Last Error Code:		Last Error Code:	

LED Status - This is the Status for *All Slaves* or the specific Slave selected.

1) Solid Green (Connected) – The gateway is connected to all of the Modbus RTU Slaves that are configured and enabled.
2) Flashing Green (Not Connected) – No Modbus RTU Slaves are enabled/configured.
   a. Verify Modbus RTU settings and ensure that the *Enable* checkbox is checked for the appropriate Slave(s).
3) Flashing Red (Connection Timeout) - The gateway cannot open a connection to 1 or more of the enabled Modbus RTU devices.
   a. Verify Modbus RTU device for Slave Address, 0 or 1 Base Addressing, ASCII Messaging, and Starting Addresses
   b. Verify Port Settings used match the Modbus Slave that the gateway is communicating with.
   c. Verify wires for specific port settings.
4) Flashing Red (Empty Scan List) - One or more enabled Modbus Slaves have no scan lines configured.
5) Flashing Red (Communication not attempted yet) – (Specific Slave Only) No reads are configured and data needed for writes isn't valid yet.
6) Flashing Red (Dependency Error) - The dependent protocol is missing causing the communication to go to inactive.
   a. The other Protocol must be *Connected*.
7) Solid Red (Fatal Error) – The serial port selected on the Modbus RTU Master Configuration page is not configured.
   a. Verify that Modbus RTU has an enabled Port selected. If needed, configure Port Settings.

Variables - These are the values for *All Slaves* or the Specific Slave Selected.
Network Bitmap Status (Displayed in Hex):
    -Each bit corresponds to a Slave. If the bit is set, the Slave is connected, otherwise the bit is 0.
    -Bit 0 corresponds to Slave 1 and Bit 4 is for Slave 5 and so on.
FC01 Read Coil Status:
    -Function Code 1: Number of read Coil Status requests sent
    -Point Type Used: 0x Coil Status
    -# of Points: Any
FC02 Read Input Status:
    -Function Code 2: Number of read Input Status requests sent
    -Point Type Used: 1x Input Status
    -# of Points: Any
FC03 Read Holding Registers:
    -Function Code 3: Number of read Holding Register requests sent
    -Point Type Used: 4x Hold Reg
    -# of Points: Any
FC04 Read Input Registers:
    -Function Code 4: Number of read Input Register requests sent
    -Point Type Used: 3x Input Reg
    -# of Points: Any
FC05 Force Single Coil:
    -Function Code 5: Number of write Coil Status requests sent
    -Point Type Used: 0x Coil Status
    -# of Points: 1

FC06 Preset Holding Register:
    -Function Code 6: Number of write Holding Register requests sent
    -Point Type Used: 4x Holding Reg
    -# of Points: 1

FC15 Force Multiple Coils:
    -Function Code 15: Number of write Multiple Coil Status requests sent
    -Point Type Used: 0x Coil Status
    -# of Points: 2 or More OR Force Function Code 15/16 Enabled for # of Points of 1

FC16 Preset Multiple Registers:
    -Function Code 16: Number of write Multiple Holding Register requests sent
    -Point Type Used: 4x Holding Reg
    -# of Points: 2 or More OR Force Function Code 15/16 Enabled for # of Points of 1

Successful Responses Received:
    -Total number of Read and Write response messages received
    -Note: Add up all of the Function Code Variables and it should equal the number of Successful Responses Received

Error Responses Received:
    -Total number of Read and Write error messages received

Timeouts:
    -Total number of Read and Write response messages not received

Status Strings - These are the values for *All Slaves* or the Specific Slave Selected.

Last Error Code:
    -Last Read Request Error that the gateway received

Error Code Breakdown:

1) Error Code "code" - "Function" (N:"SlaveAddr" A:"StartAddr" L:"Length"))
    a. Note: The Slave Address will inform you of the device that had the error. The Starting Address and Length will inform you the specific scan line that had the error
2) Error Codes:
    a. Error Code 1: Function Code received by the Slave is not valid
    b. Error Code 2: The Register/Status received by the Slave is not valid
    c. Error Code 3: The value received by the Slave is not allowable
    d. Error Code 4: An unrecoverable error occurred while the Slave was attempting to reply
    e. Error Code 5: The Slave has accepted the request and is processing it, but a long duration of time will be required to reply
    f. Error Code 6: The Slave is processing another message. The gateway will skip this message.
    g. Error Code 7: The Slave has replied with a NAK. The server cannot perform the program function received in the query
3) Functions:
    - Specific to the Function Code being used for the Scan Line
4) N (Slave Address):
    - Slave Address of the Slave that the error was received from
5) A (Starting Address):
    - Starting Address of the Register/Status that the error was received from
6) L (Length):
    - Number of Points of the Register/Status that the error was received from

Example:

Successful Responses Received:	0
Error Responses Received:	29
Timeouts:	0
Status Strings	
Last Error Code:	Error Code 2 - FC15_WrMCls (N:1 A:101 L:32)

This Error Code indicates Code 2, the Register was not valid. Other details are:

- Received the error with FC 15, trying to Force Multiple Coils (WrMCls – Write Multiple Coils)

- N:1, from device 1, the first configured device

- A:101, Starting address of 101; aka: 000101 or 00101

- L:32, Multiple Registers were trying to write 32 Coils.

The Error Code indicates *not valid*, so the starting address was not found, or there were not 32 sequential coils to be written (101 through 132). To solve this, change the starting address, or reduce the *# of Points* configured.

Diagnostics – DF1 Master

Select the DF1 Master in the top dropdown menu on the Diagnostic page to view a breakdown of the diagnostics and common strings that are displayed on the page. You may also view individual Slave counters by selecting the device in the *All Slaves* dropdown and clicking **View**. Additional diagnostic information can be found by clicking the **Help** button.

NOTE: This page will auto-refresh every 5 seconds with the latest data.
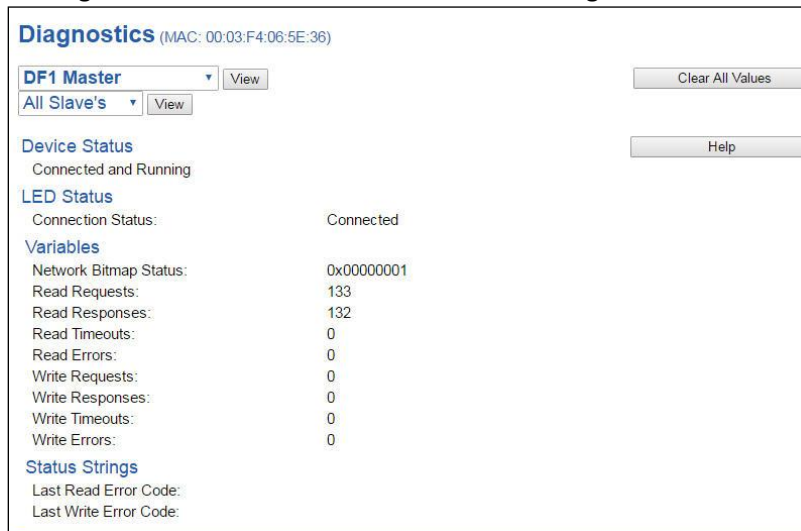
Clear All Values - This will only affect current displayed values.
1) This will return all values displayed to 0 and clear the Status Strings.
    Example: If Viewing DF1 Master – Slave Address 1, this will only clear the values for Slave Address 1. This will reduce the *All Slaves* values indirectly.

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

1) Connected and Running– the gateway is connected to all of the DF1 Slaves.
2) Error: Timeout – No DF1 Scan Lines are configured under an enabled Slave.
    Or, one or more enabled D1 Slaves are missing.
    a. Verify DF1 device for correct Destination ID.
    b. Verify that Port Settings used match the DF1 Slave(s) that the gateway is communicating with.
    c. Verify wires for specific port settings.
3) Dependency Protocol Faulted – The dependent protocol is missing causing the communication to stop.
4) Unknown: First Scan Not Complete – Multiple Scan Lines are set up for the device and the gateway has not completed all of the scan lines for the first time.
5) Fatal Error: Couldn't Open Hardware Port – The serial port selected on the DF1 Master Configuration page is not configured.
6) Fatal Error: No Configuration – No DF1 Slaves are enabled though a Serial Port is enabled.

LED Status - This is the Status for *All Slaves* or the specific Slave selected.
1) Solid Green (Connected) – The gateway is connected to all of the DF1 Slaves that are configured and enabled.
2) Flashing Green (Not Connected) – No DF1 Slaves are enabled/configured.
   a. Verify DF1 settings and ensure that the *Enable* checkbox is checked for the appropriate Slave(s).
3) Flashing Red (Connection Timeout) - The gateway cannot open a connection to 1 or more of the enabled DF1 devices.
   a. Verify DF1 Communication Command.
   b. Verify DF1 Destination IDs.
   c. Verify Port Settings used match the DF1 Slave that the gateway is communicating with, including Protocol Mode and Frame Verification.
   d. Verify wires for specific port settings.
4) Flashing Red (Empty Scan List) - One or more enabled DF1 Slaves have no scan lines configured.
5) Flashing Red (Communication not attempted yet) – (Specific Slave Only) No reads are configured and data needed for writes isn't valid yet.
6) Flashing Red (Dependency Error) - The dependent protocol is missing causing the communication to go to inactive.
   a. The other Protocol must be *Connected*.
7) Solid Red (Fatal Error) – The serial port selected on the DF1 Master Configuration page is not configured.
   a. Verify that DF1 has an enabled Port selected. If needed, configure Port Settings.

Variables - These are the values for *All Slaves* or the Specific Slave Selected.
Network Bitmap Status (Displayed in Hex):
    -Each bit corresponds to a Slave. If the bit is set, the Slave is connected, otherwise the bit is 0.
    -Bit 0 corresponds to Slave 1 and Bit 4 is for Slave 5 and so on.
Read Requests:
    - Number of DF1 Read Requests that the gateway has sent to the Slave device.
Read Responses:
    - Number of valid DF1 Read Responses that the gateway has received from the Slave device.
    - NOTE: This should be equal to the number of Read Requests
Read Timeouts:
    - Number of times the gateway has reached the timeout period waiting for a Read Response from the Slave device.
Read Errors:
    - Number of DF1 Read Errors
Write Requests:
    - Number of DF1 Write Requests that the gateway has sent to the Slave device.
Write Responses:
    - Number of valid DF1 Write Responses that the gateway has received from the Slave device.
    - NOTE: This should be equal to the number of Write Requests
Write Timeouts:
    - Number of times the gateway has reached the timeout period waiting for a Write Response from the Slave device.
Write Errors:
    - Number of DF1 Write Errors

Status Strings - These are the values for *All Slaves* or the Specific Slave Selected.
Last Read Error Code:

- Last Read Request Error that the gateway received

Last Write Error Code:

- Last Write Request Error that the gateway received

Error Code Breakdown:
Format of Error: STS='Err Code',EXT_STS='Err Code' (N:'Slave Destination ID' A:'DF1 Request Address in Offset Notation' L:'Number of points to Read')

1) STS='Err Code',EXT_STS='Err Code' (N:'Slave Destination ID' A:'DF1 Request Address in Offset Notation' L:'Number of points to Read/Write')
   a. NOTE: The Slave Destination ID will inform you of the device that had the error. The DF1 Request Address and Length will inform you the specific scan line that had the error
2) Error Codes:
   a. Most common STS error ix 0x010: "Illegal command or format"
      Potential issues:
      i) Selected Communication Command is not supported by the Slave device
      ii) File Type and File Number does not exist in the Slave device
      iii) File Offset does not exist in the Slave device File Type and File Number
      iv) Attempting to read more data elements than exist in the Slave device
3) N (Slave Destination ID):
   - Slave Destination ID of the Slave that the error was received from
4) A (DF1 Request Address):
   - Starting Address of the DF1 Request in Offset Notation that the error was received from
5) L (Length):
   - Number of Points of the request that the error was received from

Example:

This Error Code indicates STS 0x10, EXT_STS=0x00, "Illegal command or format". Other details are:

- N:55, from Slave device with Destination ID of 55

- A:ST155:44444; File Type of ST, File Number of 155, File Offset of 44444

- L:1, the scan line with a single point was rejected

The Error Code indicates *not valid*, so check to see if there is a File Type of ST with File Number 155 set up. Also make sure that the File Offset of 44444 is valid in ST155 for a length of 1.

LED Configuration

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

The LED Configuration page lets you configure the LEDs on the gateway.

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 particular Slave/Server device.

To select a particular 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.

Configuration Files

To access the configuration files in the 460 gateway, navigate to dropdown **Other->Export/Import Config**.

Export Configuration

The export tool allows you to save your gateway configuration for backup or to be exported into another gateway. This file is named *rta_cfg.rtax* by default. Network settings will not be saved in this configuration since they must be unique for each gateway.

Upon clicking the **Save Configuration to File** button, you will be prompted to select a location to save the file.
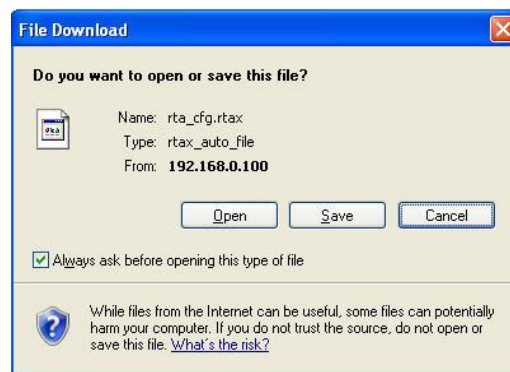
Import Configuration

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, click the **Load Configuration** button.

If it has successfully loaded, the gateway will indicate that it was successful and a message will appear under the Load Configuration button indicating you should reboot the gateway.

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. The configuration file is xml and can be modified with any text editor. Once that error is fixed, try loading again until it is successful.

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 webpage. If this unit should fail in the future, the last configuration the gateway used is 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: Configuring*, go into Configuration Mode by clicking on 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*, now insert the SD Card.
8) Do a hard Power Cycle to the unit by unplugging power. DO NOT RESET POWER VIA WEBPAGES.
   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 webpage.
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 LED's** button. By clicking this button, the two diagnostic LED's will flash red and green. Once you have identified which device you are working with, click the button again to put the LED's 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.