460TCPDFM-N700
Protocol Gateway

Product User Guide

Firmware Version 8.9.22

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.

© 2024 Real Time Automation, Inc. All rights reserved.

Revision History 6
Overview 8
Hardware Platforms 9
Hardware – N700 10
Powering the Gateway 10
Port Connections 11
Mounting with a DIN Rail 12
Installing 12
Removing 12
Accessing the Main Page 13
Committing Changes to the Settings 15
Main Page 16
Device Configuration 17
Network Configuration 18
TCP/IP Configuration 19
ASCII Configuration 20
Receive Data 21
Receive Data – Operation Mode 22
Transmit Data 23
Transmit Data – Triggering Methods 24
ASCII Configuration – Technology Triggering Method 26
ASCII Configuration – ASCII Parsing 28
ASCII Configuration – ASCII Parsing Examples 29
ASCII Configuration – ASCII Concatenating 31
ASCII Configuration – ASCII Concatenating Examples 33
ASCII Configuration – ASCII Message Counter 35
DF1 Master Configuration 36
DF1 Master Device Configuration 37
Configuring Read Scan Lines 38
Configuring Write Scan Lines 38
Configuring Read and Write Scan Lines (cont.) 39
Mapping - Transferring Data Between Devices 40

Display Mapping and Values 41
Display Data 41
Display String 44
Display String use case 46
Data and String Mapping – Auto-Configure 47
Data Mapping – Explanation 48
Data Mapping – Adding Diagnostic Information 49
String Mapping – Explanation 54
Mapping – Auto-Configure Mode to Manual Configure Mode 55
Mapping – Manual Configure Mode to Auto-Configure Mode 56
View as Text 57
Data Mapping 57
String Mapping 57
Base Triggering – Data Validiation Triggering 58
Security Configuration 60
Security Configuration-Security Levels 61
Security - Log In 62
Security - Log Out 62
Email Configuration 63
Alarm Configuration 64
Diagnostics – Alarm Status 66
Alarms – Active 66
Alarms – Clear 67
Change of State (COS) Configuration 68
Diagnostics Info 69
Diagnostics Mapping 69
Diagnostics – ASCII 70
Diagnostics – DF1 Master 75
Configuration Files 80
Export Configuration 80
Import Configuration 80
Save and Replace Configuration Using SD Card 82
Saving Configuration Using SD Card 82
Replacing Configuration Using SD Card 82

Utilities 83

Revision History

Version	Date	Notes
8.4.5	11/18/2019	Features Added 1. Released OPC UA Server (US) Protocol 2. Ability to now Import/Export Template Files with out an FTP session Bug Fixes 3. Updated Profinet Server (PS) on N34 hardware Platform 4. Updated Wi-Fi software
8.6.0	2/28/20	Bug Fixes 1. Omron Plc Communication fixes for EtherNet/IP 2. Profinet GSDML Substitute values fix
8.7.4	9/1/20	Features Added: 1. BMS, BM, DFM, DS, DM, TCP, USB, PBS have been ported to the latest base software 2. TCP,BMS,BM now Available on N2E and N2EW hardware Platform 3. New ASCII Mode Available on TCP/A/USB/WI protocols 4. User Guides updated with more examples Bug Fixes: 1. Improved Data Mapping and String Mapping performance 2. Improved functionality/performance on EC,ETC,ES,MC,MS,BS,BC, A,,WI,PS protocols
8.7.22	4/6/21	Features Added: 1. Support for RSLogix Versions 32 + with unsigned data type support 2. ETC now support Long integer files (L files) for MicroLogix PLCS that support them 3. SC now supports data block (DB) access
8.7.53	4/28/21	Features Added: 5. Added support for the NNBU hardware platform 6. Improved RFIDeas scanner support 7. Updated MM and MRS to use Modbus RTU Client and Modbus RTU Server terminology

Version	Date	Notes
8.9.22	2/5/24	Features Added: 1. Added priority-based reads for client protocols 2. Added improved diagnostic timers for client protocols 3. Reduced minimum delay between messages to zero ms on client protocols 4. Added support for USB serial connections 5. Added support for multiple connections on EtherNet/IP Adapter 6. Added 100ms and 1000ms heartbeat values for diagnostic use 7. Added configurable data size to EtherNet/IP adapter and DeviceNet Slave 8. Added support for TTL communications on N34, NNA1, NNA4, N2E, and N2EW hardware 9. Added support for JSON payloads to MQTT 10. Added Network Bitmap Status to ASCII, USB, and TCP protocols Bug Fixes: 11. Fixed COV Subscription Issues on BACnet MS/TP 12. Fixed timing issues affecting gateway performance 13. Fixed a bug where the Run Idle Header on the output instance for EtherNet/IP Scanner was not checked by default

Overview

The 460TCPDFM-N700 gateway Connects up to 10 Ethernet TCP/IP devices with as many as 32 DF1 slaves. By following this guide, you will be able to configure the 460TCPDFM-N700 gateway.

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

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

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

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

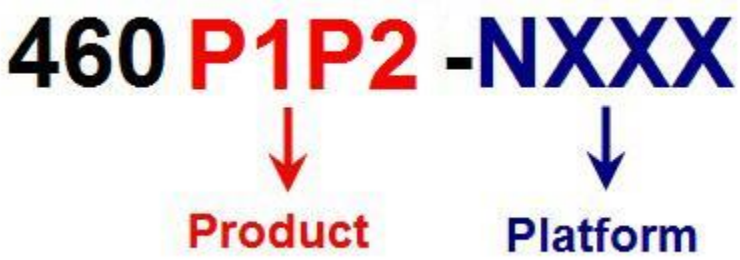
Hardware Platforms

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

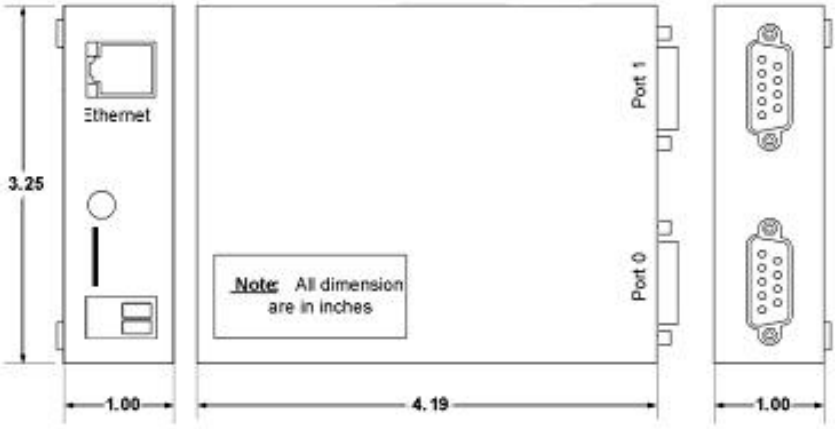
To find which hardware platform you are using:

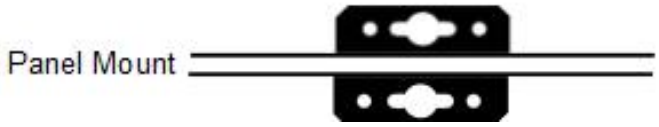
1) Look on the front or back label of the unit for the part number.
2) On the webpage inside the gateway, navigate to the dropdown menu under **Other** and select **Utilities**. Click the **Listing of Revisions** button. The full part number is displayed here.

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



Hardware – N700





Powering the Gateway

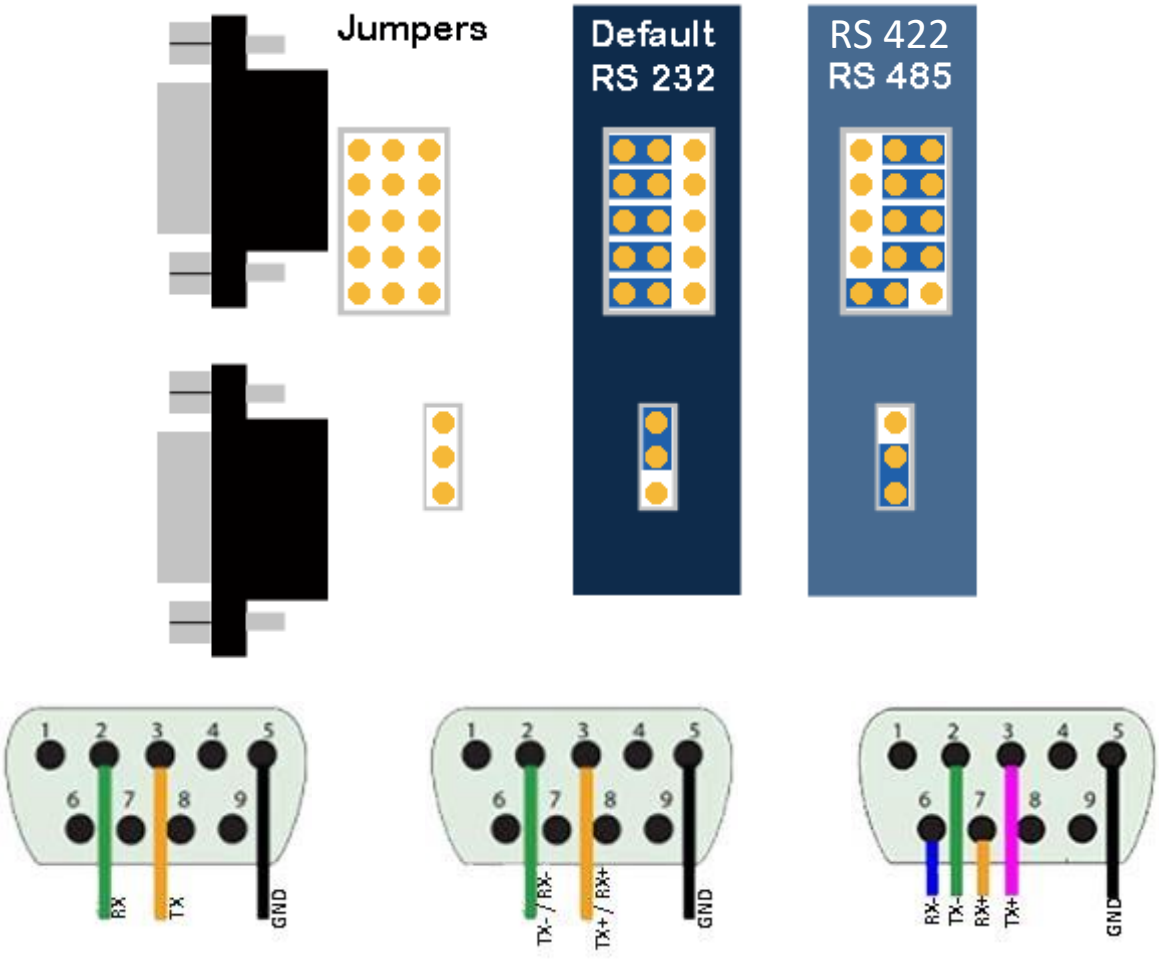
1) Connect a 12-24 VDC power source to the gateway:

   a) 2-Pin Terminal power connection with Red Wire = (+) Black Wire = (-)

Port Connections

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

Jumper Configuration



Port 0 & Port 1
RS232

Port 0
RS485

Port 0
RS422

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

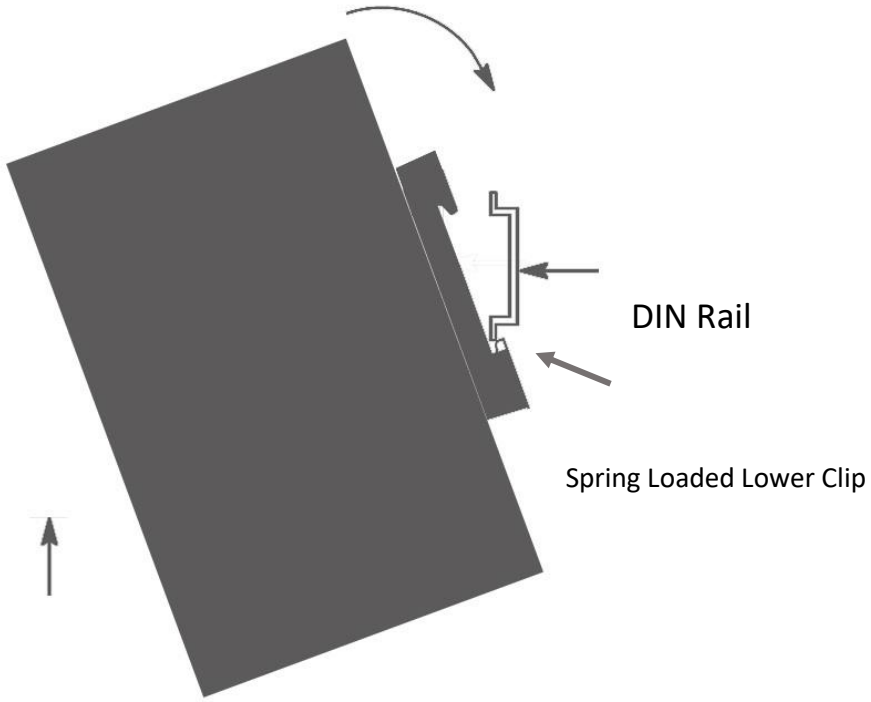
- **Port 0 – RS232**
- **Port 1 – RS232**

Mounting with a DIN Rail

Installing

Follow these steps to install your interface converter.

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



Removing

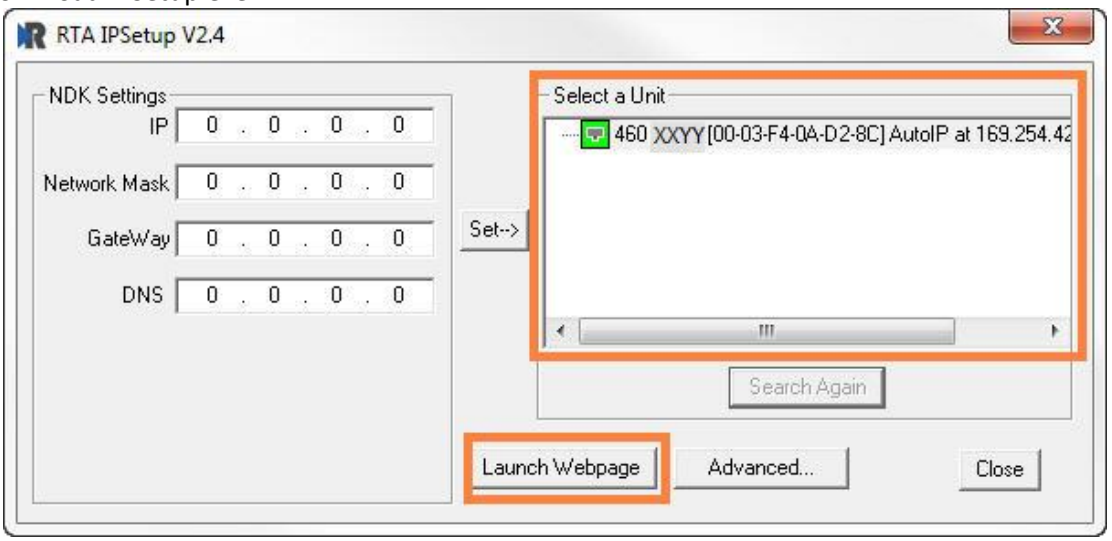
Follow these steps to remove your interface converter.

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

Accessing the Main Page

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

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



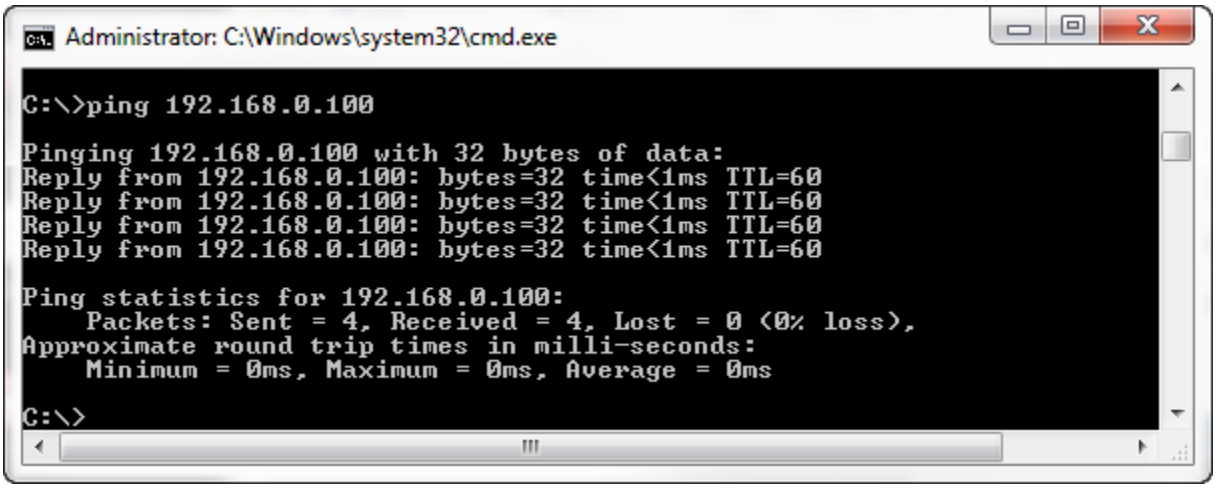
2) Run the IPSetup.exe program.
3) Find unit under "Select a Unit".
   a. Change Gateway's IP address to match that of your PC if DHCP has failed.
      i. You will know DHCP has failed if the gateway's IP address is AutoIP at 169.254.X.Y.
      ii. If successful, it will say DHCP'd at ex: 192.168.0.100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

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

Error: Main Page Does Not Launch

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

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



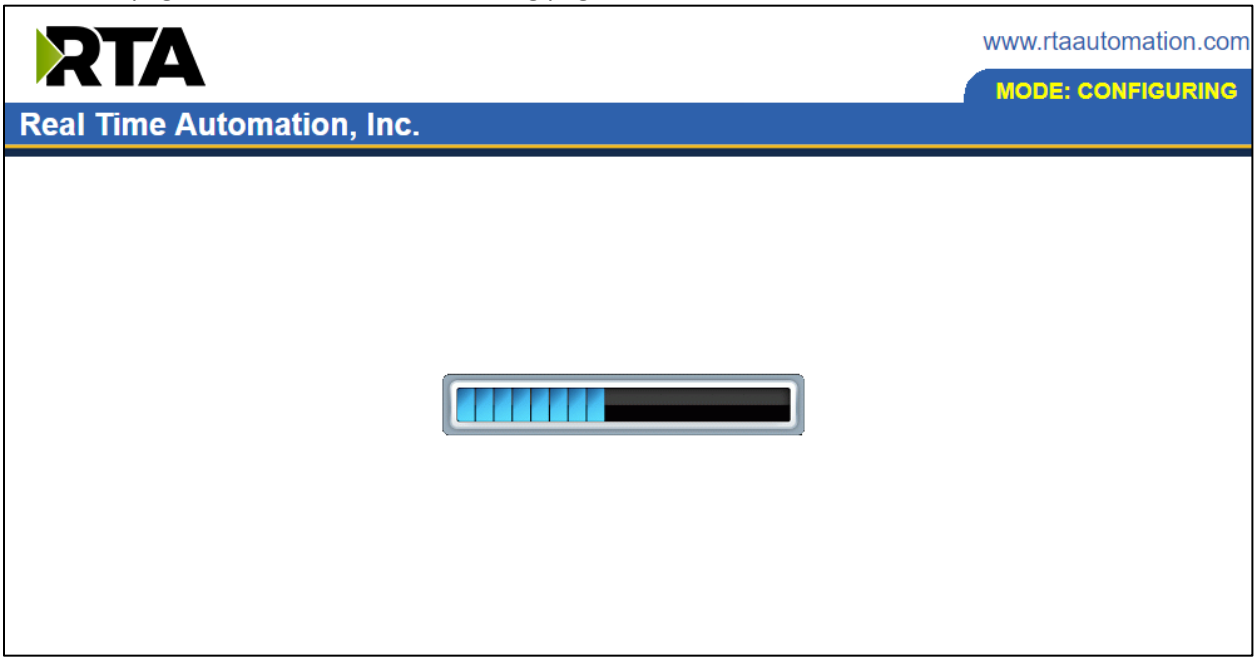
The Screenshot above shows a gateway that is currently set to a static IP Address of 192.168.0.100. If you are able to successfully ping your gateway, open a browser and try to view the main page of the gateway by entering the IP Address of the gateway as the URL.

Committing Changes to the Settings

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

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

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



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

Main Page

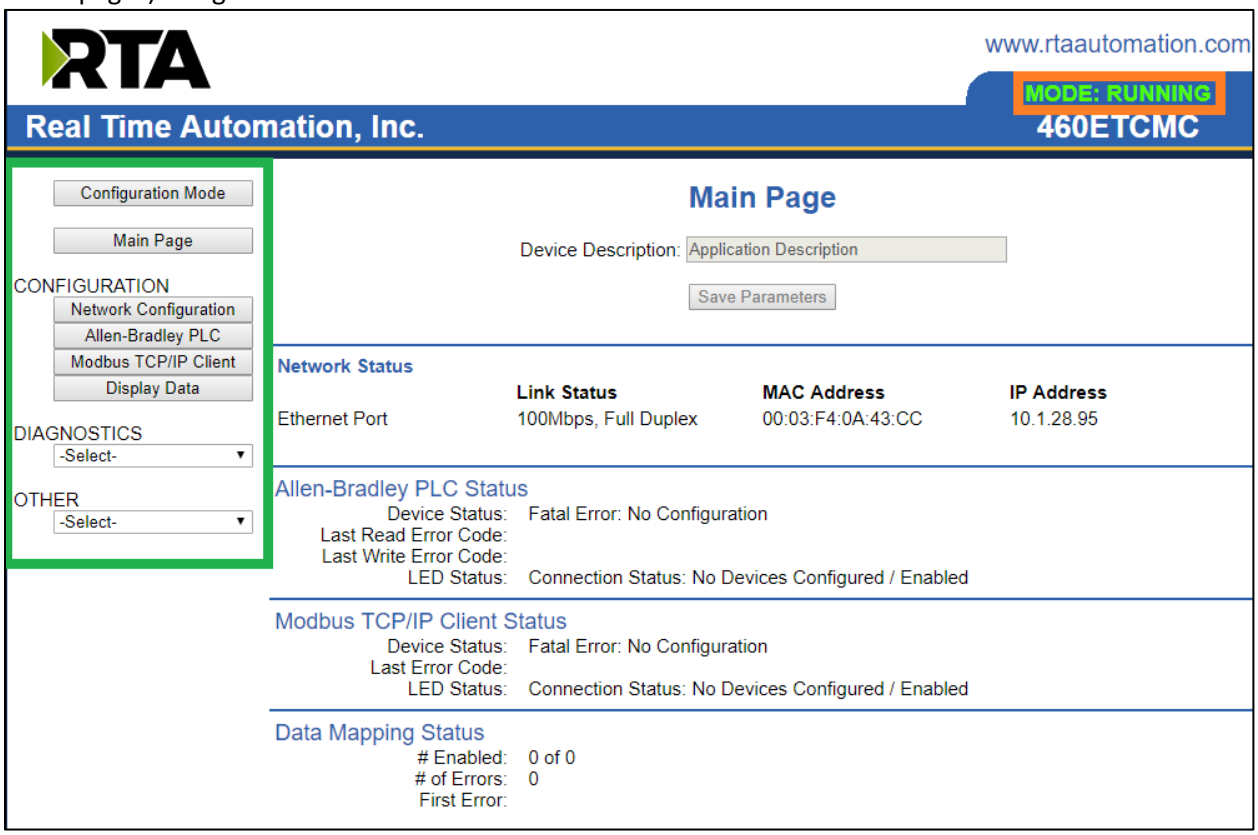
The main page is where important information about your gateway and its connections are displayed.
Mode (orange box below):
Running Mode:

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

Configuring Mode:

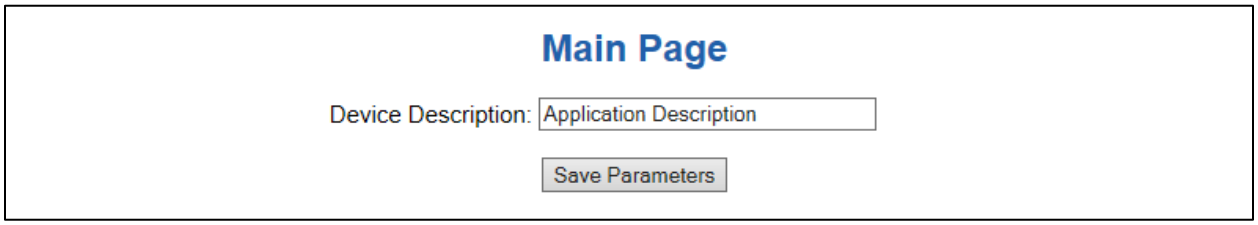
- Protocol communication is stopped and no data is transmitted
- Configuration is allowed

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



Device Configuration

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



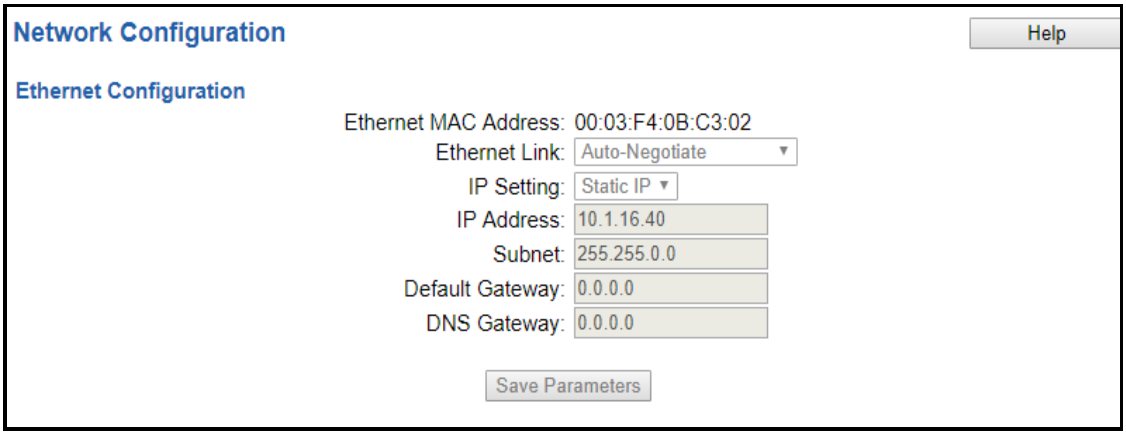
Once you are done configuring the Description, click the **Save Parameters** button.

Network Configuration

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

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

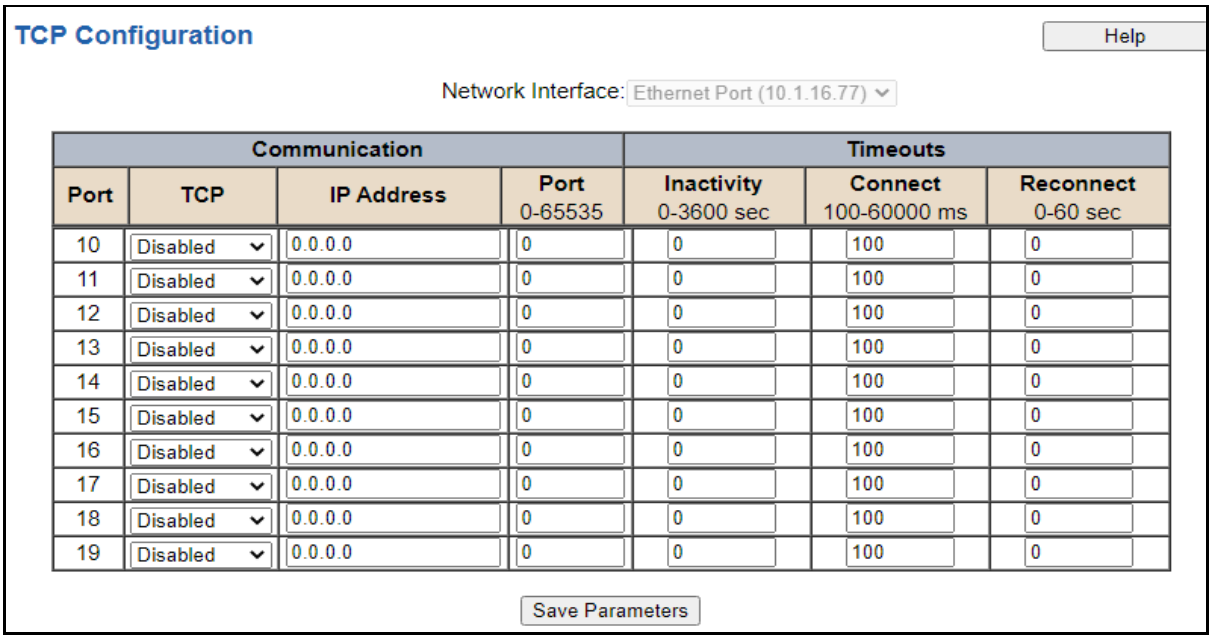
If you are changing the IP Address of the gateway, the change will not take effect until the unit has been rebooted. After reboot, you must enter the new IP Address into the URL.



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

TCP/IP Configuration

Click the **TCP/IP Configuration** button to access the primary configuration page for this device. If you have an N2E/N2EW hardware, then select which Network Interface ASCII comms will be on.



To connect to a TCP server device on the network, enable a TCP client connection in the gateway for one of the available ports:

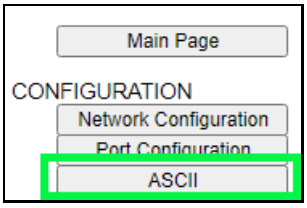
1) **TCP**: Under this dropdown select TCP Client.
2) **IP Address**: Enter the IP address of the TCP server to connect to.
3) **Port**: Enter the port to open a connection.
4) **Inactivity Timeout**: Enter the amount of time, in seconds, the gateway will wait for data to be transmitted to the gateway or sent from the gateway to the TCP device. If the timer expires, the gateway will close the connection.
5) **Connect Timeout**: Enter the amount of time, in milliseconds, the gateway will wait for the TCP server to accept the connection.
6) **Reconnect Timeout**: Enter the amount of time, in seconds, the gateway will wait after the Connect Timeout has expired before issuing another connect.

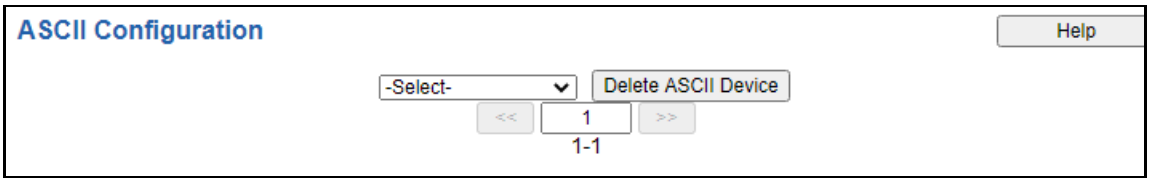
To connect to a TCP client device on the network, enable a TCP server connection in the gateway for one of the available ports:

1) **TCP**: Under this dropdown select TCP server.
2) **IP Address**: Enter the IP address of the TCP client that will connect to the gateway.
3) **Port**: Enter the port to listen for a connection.
4) **Inactivity Timeout**: Enter the amount of time, in seconds, the gateway will wait for data to be transmitted to the gateway or sent from the gateway to the TCP device. If the timer expires, the gateway will close the connection.
5) **Connect Timeout**: Not used in this case (Client only).
6) **Reconnect Timeout**: Not used in this case (Client only).

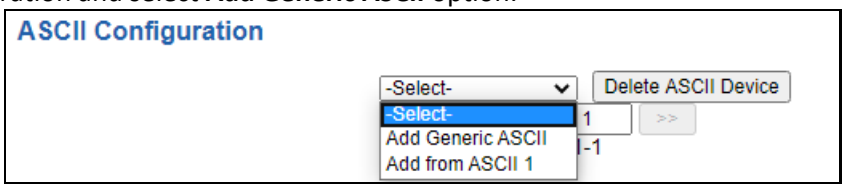
ASCII Configuration

After the port configuration has been completed, click the **ASCII** button to continue configuration.

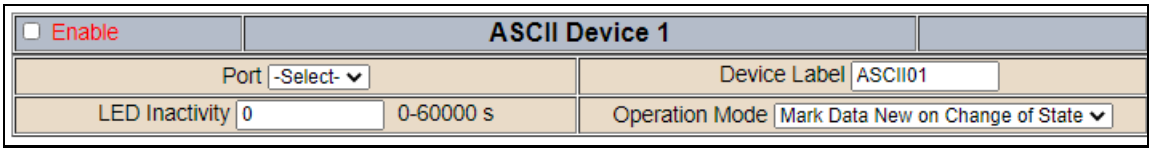




1) To add an ASCII device or additional ASCII device, click the -Select- dropdown menu under ASCII Configuration and select **Add Generic ASCII** option.

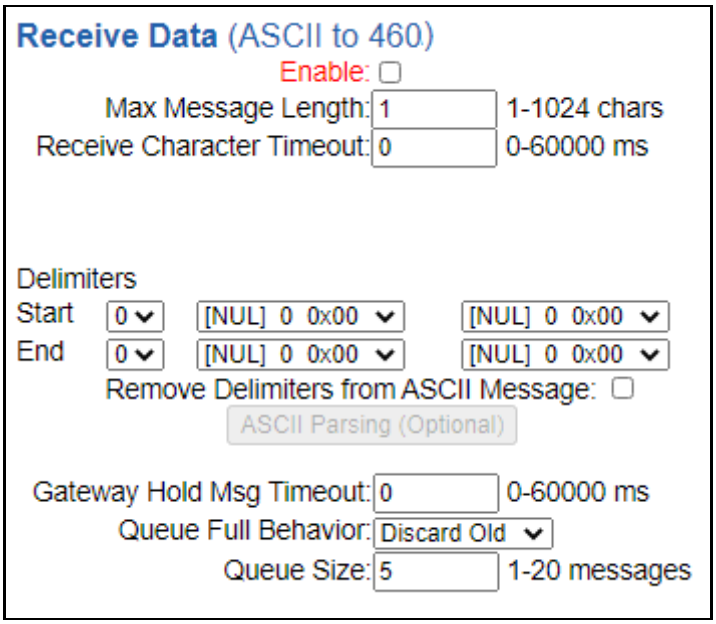


   a) To remove a device, navigate to the ASCII device to delete using the **<<** and **>>** buttons and click the **Delete ASCII Device** button.
   b) To create a new ASCII device with the same parameters already configured from another ASCII device, click the -Select- dropdown menu and select the **Add from ASCII X** option (where X represents the ASCII device you wish to copy parameters from).
   c) Once created, you can make any additional changes needed to that new ASCII device.
2) The **Enable** check box should be selected for the device.
3) **Port**: Select which port is being used for communication. This port must be configured on the Port/USB or TCP/IP (depending on your product) Configuration page. If it has not yet been configured, it will not display in this dropdown.
4) Enter a **Device Label** to identify the device within the gateway.
5) **LED Inactivity Timeout**: Enter the amount of time, in seconds, to wait before flashing the LED red indicating that no messages have been received or transmitted during this time.
6) **Operation Mode:**
   a. Mark Data New on Change of State: Send data to the mating technology, on a per point basis, upon a change of state. For more explanation see the Receive Data – Operation Mode section below.
   b. Mark Data New on New Message: Send data to the mating technology for all data points, no matter change of state or not. For more explanation see the Receive Data – Operation Mode section below.



Receive Data

This side is configured to receive data from the ASCII device into the gateway.



Use the following fields to determine when a message has been received.

1) **Enable**: Check this box to configure the Receive Data section.
2) **Max Message Length**: Enter the max number of characters that can be received by the gateway.

   Example: Max Message Length is set to 5 and the message of "helloworld" was sent by the ASCII device. This will be sent to the other protocol as "hello" followed by "world" as two messages.
3) **Receive Character Timeout:** Enter the max amount of time (in ms) between characters that the gateway will wait before issuing a timeout and calling the message complete.

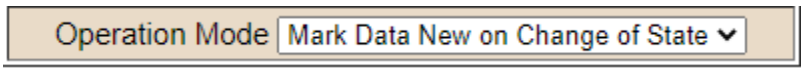
   Example: If Max Message Length varies in size, then use a timeout to call the message complete rather than message length. You can also use End Delimiters (below) to call a message complete.
4) **Number of Start Delimiters:** Select the number of delimiters that the gateway should look for before the gateway processes the data.
5) **Select Start Delimiters:** Select the start delimiters that the gateway should look for.
6) **Number of End Delimiters:** Select the number of delimiters that the gateway should look for to call a message complete.
7) **Select End Delimiters:** Select the end delimiters that the gateway should look for.
8) **Remove Delimiters from ASCII Message:** If checked, the gateway will remove all delimiters that have been configured before sending it to the other protocol.
9) **ASCII Parsing (Optional):** Additional parsing can be performed on the string before being passed to the other protocol. See the ASCII Configuration - ASCII Parsing section for more information.

10) **Gateway Hold Msg Timeout:** Enter the amount of time (in ms) to wait before sending a new message to the other protocol.
11) **Queue Full Behavior**: Select which message to discard when the queue is full. Once the queue is full, the gateway will discard either the oldest or newest message (Only used if Gateway Hold Msg Timeout is non-zero).
12) **Queue Size**: Select how many complete messages the gateway will hold before starting to discard (Only used if Gateway Hold Msg Timeout is non-zero).

Receive Data – Operation Mode

Mark Data New on Change of State (COS)

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

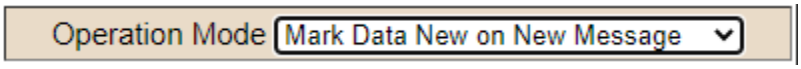


Example for 460ETCA

Operator scans "HelloWorld" with a barcode scanner. That data is gathered in the ASCII side of the RTA gateway, and is then processed and sent over to the ETC side and written over to the Allen-Bradley PLC. The next time the operator scans the same barcode "HelloWorld", the ASCII side gathers the data, but the data didn't change so it will not be sent over to the ETC portion of the RTA gateway. If the operator scans "1234567890" with the barcode scanner, the ASCII side of the RTA gateway will process the data. Since the data has changed it will be sent over to ETC and sent over to the PLC.

Mark Data New on New Message

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

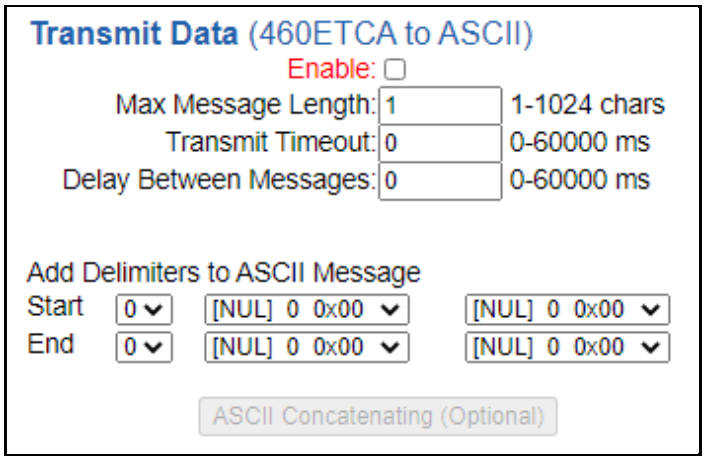


Example ETCA

Operator scans "HelloWorld" with a barcode scanner. That data is gathered in the ASCII side of the RTA gateway, and is then processed and sent over to the ETC side and written over to the Allen-Bradley PLC. The next time the operator scans the same barcode "HelloWorld", the ASCII side gathers the data, processes it, then sends it over to the ETC portion of the RTA gateway to be sent out. If the operator scans "1234567890", the ASCII side of the RTA gateway will process the data and send it over to ETC side and then to the PLC.

Transmit Data

This side is configured to transmit data from the gateway into the ASCII device.



Use the following setup fields to help the 460 transmit an ASCII message.

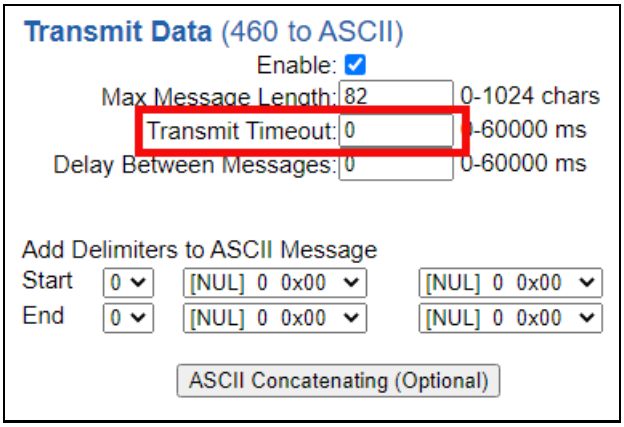
1) **Enable**: Check this box to configure the Transmit Data section.
2) **Max Message Length**: Enter the max number of characters that can be transmitted by the gateway.
3) **Transmit Timeout:** Enter the amount of time (in ms) that the gateway waits before sending an ASCII message (0 Sends Immediately). If the data has changed before the time expires, the gateway immediately sends the message to the ASCII device.
4) **Delay Between Messages:** Enter the amount of time (in ms) that the gateway waits before verifying a Change of State of the ASCII message OR will start the Transmit Timeout.
5) **Number of Start Delimiters:** Select the number of delimiters that will be added onto the beginning of the ASCII string.
6) **Select Start Delimiters:** Select the start delimiters that should be added to the ASCII string.
7) **Number of End Delimiters:** Select the number of delimiters that will be added onto the end of the ASCII string.
8) **Select End Delimiters:** Select the end delimiters that should be added to the ASCII string.
9) **ASCII Concatenating (Optional):** Additional concatenating can be performed on the string before being written to the ASCII device. See the ASCII Configuration – ASCII Concatenating section for more information.

Transmit Data – Triggering Methods

There are 3 methods that determine when the message is ready to be transmitted to your ASCII device:

1) **Cyclic** – This means that every *x* ms a new ASCII message will be transmitted, regardless of whether the data has changed or not.
2) **Triggering** – This means that a trigger event determines when a new ASCII message will be transmitted.
   Some methods can co-exist with others. Here are the optional rules:
   a) **Option 1:** Change-Of-State is defaulted, so this method is chosen if the Transmit Timeout field is left at 0 and **ALL** data is new.

      Example 1: From the PLC, send a message of "hello", through the RTA gateway, the ASCII device sees "hello". If you send "hello' again, nothing will happen because of the RTA Change-of-State Rule.



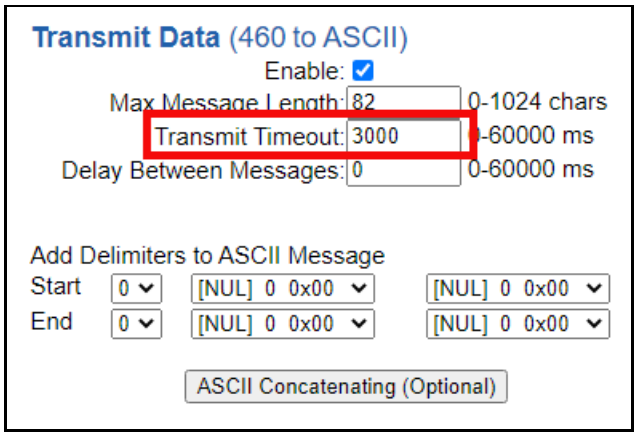
   b) **Option 2:** Technology Triggering (A/USB/TCP/WI). This method is chosen if the Transmit Timeout field is left at 0 and the trigger variables (as described in ASCII Configuration – Technology Triggering Method section of this manual) are mapped. This will disable Change-of-State. This method is recommended if your product in **NOT** an 460ETC product.

      NOTE: If you have an 460ETC it's high recommended you use the Optimization Triggering.

      Example 2: Using the Technology Triggering Mappings (shown below in the Technology Triggering Method section) you can make the data new only with a trigger. If you want to send the same/new message of based on a trigger and NOT cyclically, then keep the Transmit Timeout at 0 **AND** use the 2 Trigger Mappings. *See below for more examples in the* ASCII Configuration – Technology Triggering Method.

c. **Option 3:** Cyclic and Trigger can co-exist. For this to happen, the Transmit Timeout field needs be to nonzero and the trigger variables (as described in ASCII Configuration – ASCII Message Triggering Method section of this manual) are also mapped.

Example 3: From the PLC, send a message of "hello", based on whatever gets triggered first (the 3000ms Timeout or the trigger data point) the ASCII device will get updated. If the trigger data point is not updated, the then the RTA gateway will send the data every x ms to the ASCII device. See below for more examples in the ASCII Configuration – Technology Triggering Method.

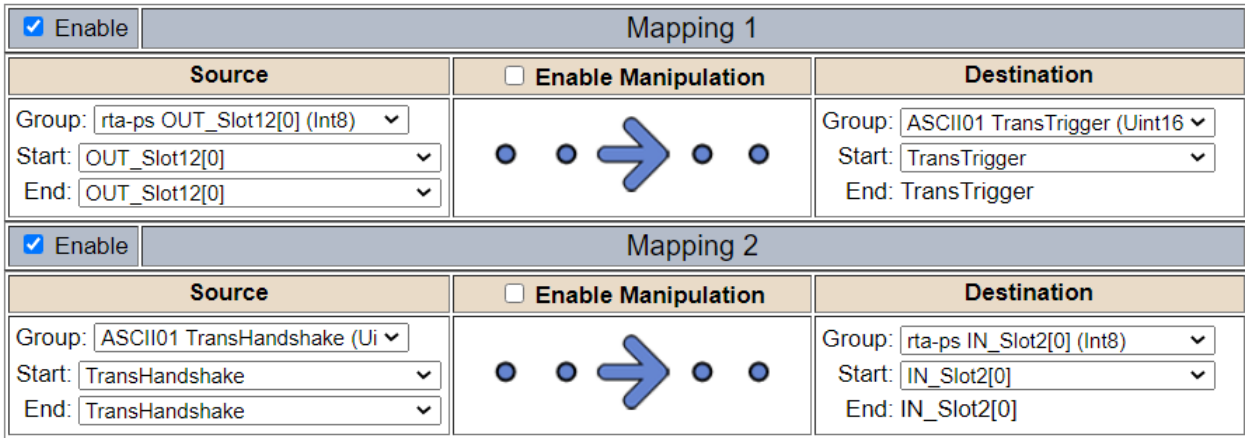


ASCII Configuration – Technology Triggering Method

This method allows the other protocol to signal when to send the next message using data handshakes. These "signals" are controlled using data variables (TransTrigger and TransHandshake) already in the mapping. The method will send the new/old data when triggered.

NOTE: These two data variables will need to be mapped manually on the Data Mapping webpage since it will not be mapped using Auto-Map.

While these two data variables are mapped, the Change-of-State method is disabled but messages can still be sent via the cyclic method, if configured. For more information on the ASCII triggering methods, please see the Transmit Data – Triggering Methods section of this user guide.



How the triggering method works: The example shown below is our 460PS* (*A/TCP/USB)

1) The mating protocol sends a numbered value to the ASCII TransTrigger diagnostic variable. This value must be different from the previous value for a new message to be triggered. The following example is Slot 12[0] as the trigger for the PLC to update everything in Slot 11[0] which is the data.

2) Depending on the TransTigger value in the Display Data page, one of 4 things will occur:
   a) If TransTrigger = 65535, then the triggering method is disabled. Usually on powerup.

RTA460 Display Data Example:

ASCII			460PSA	Profinet IO		
Name	**Value (Hex)**		**Manipulation**	**Name**	**Value (Hex)**	
TransTrigger	65535	0xFFFF	←	OUT_Slot12[0]	-1	0xFF

b) If TransTrigger = 0, then the triggering method is enabled, but no message will transmit.

RTA460 Display Data Example:

ASCII			460PSA	Profinet IO		
Name		**Value (Hex)**	**Manipulation**	**Name**		**Value (Hex)**
TransTrigger	0	0x0000	←	OUT_Slot12[0]	0	0x00
Trans_Field01	11	0x000B	←	OUT_Slot11[0]	11	0x0B

TIA Portal Example: The data will still go to the RTA gateway, however the RTA gateway will NOT transmit the data to the ASCII device until the Slot12[0] triggers the TransTrigger.

	Name	Address	Display for..	Monitor ...	Modify va...		Comment
1		%QB80	DEC+/-		11	☑ ⚠	Data to RTA ASCII
2		%QB88	DEC+/-		0	☑ ⚠	Trigger data to RTA

c) If TransTrigger is between 1-65534 **AND** the value **IS** equal to the TransHandshake diagnostic variable, then no new message will transmit, until Slot 12[0] triggers again.

RTA460 Display Data Example:

ASCII			460PSA	Profinet IO		
Name		**Value (Hex)**	**Manipulation**	**Name**		**Value (Hex)**
TransTrigger	1	0x0001	←	OUT_Slot12[0]	1	0x01

ASCII			460PSA	Profinet IO		
Name		**Value (Hex)**	**Manipulation**	**Name**		**Value (Hex)**
TransHandshake	1	0x0001	→	IN_Slot2[0]	1	0x01

d) If TransTrigger is between 1-65534 **AND** the value **IS NOT** equal to the TransHandshake diagnostic variable, then a new message will be transmitted. The value in TransTrigger will then be moved to TransHandshake.

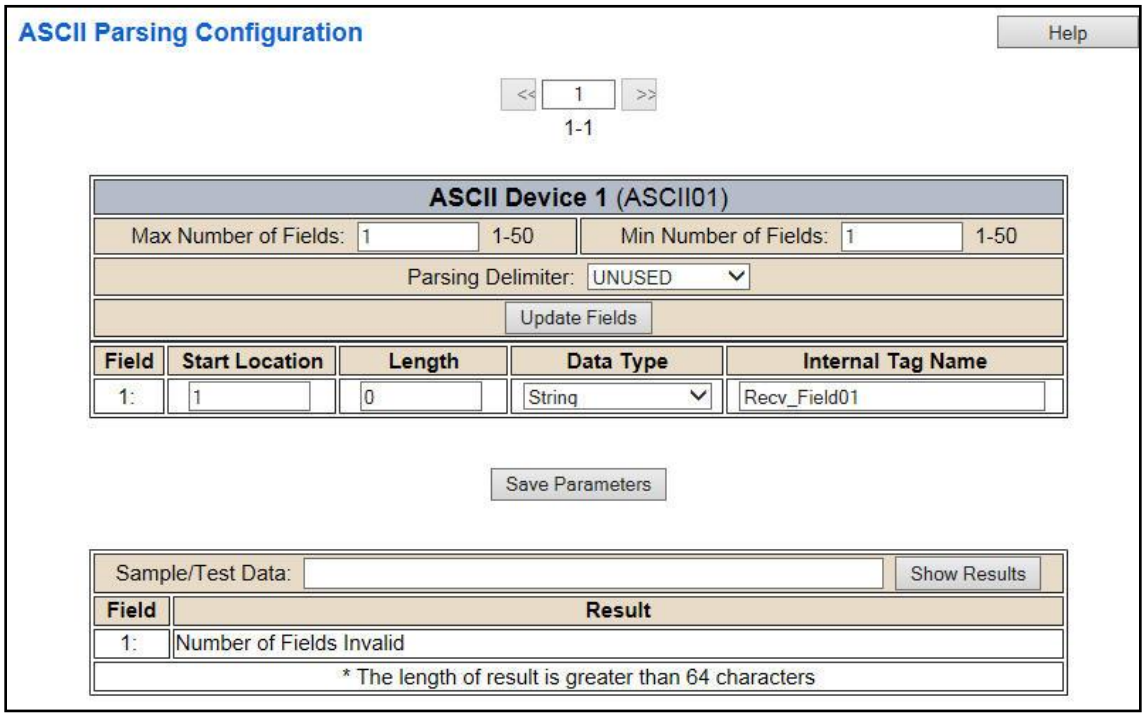
TIA Portal Example: Once the Slot12[0] increments (data is sent from the PLC to the ASCI device) then the Slot2[0] will get updated with the handshake

	Name	Address	Display format	Monitor value	Modify value		Comment
1		%QB80	DEC+/-		11	☑ ⚠	Data to RTA ASCII
2		%QB88	DEC+/-		1	☑ ⚠	Trigger data to RTA

	Address	Display format	Monitor value	Modify value		Comment
1	%IB92	DEC+/-	0		☐	Data From RTA
2	%IB100	DEC+/-	1		☐	RTA Handshake

ASCII Configuration – ASCII Parsing

The ASCII parsing feature allows you to break apart an incoming ASCII string by delimiter or character offset into multiple data fields. You can then apply a data type to the fields and deliver them to user defined locations in the mating protocol. Click the **ASCII Parsing (Optional)** button at the bottom of the ACII Configuration page to access the ASCII Parsing Configuration page for this device.

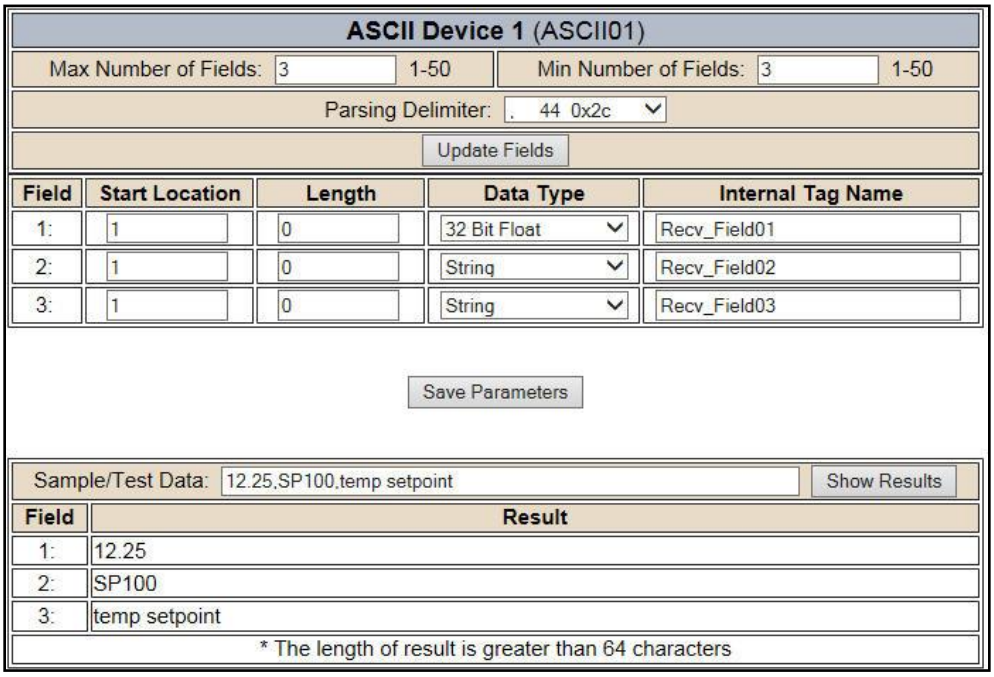


1) **Max Number of Fields:** This indicates the max number of fields the ASCII data will be parsed into (up to 50 values per message).
2) **Min Number of Fields:** This indicates the min number of fields that must be present in an ASCII string for the message to be considered valid. An error will be flagged if the actual number of fields is less than this value.
3) **Parsing Delimiter:** This defines the delimiter that will be used to parse an ASCII message. If delimiters are not present, select UNUSED and use the length fields to parse the message.
4) **Start Location & Length:**
    a. If a parsing delimiter is used, the **Start Location** will be the first character of the data field. The **Length** will be the number of characters from the Start Location. If the **Length** is 0, the gateway will read the entire field.
    b. If the parsing delimiter is unused, then the **Start Location** will be the first character of the string. The **Length** will be the number of characters from the Start Location. If the **Length** is 0, the gateway will read the entire message from the **Start Location** to the end of the ASCII string.
5) **Data Type:** Select the data type of the parsed value.
6) **Internal Tag Name:** Enter a name to reference this tag within the gateway's display and mapping pages.

ASCII Configuration – ASCII Parsing Examples

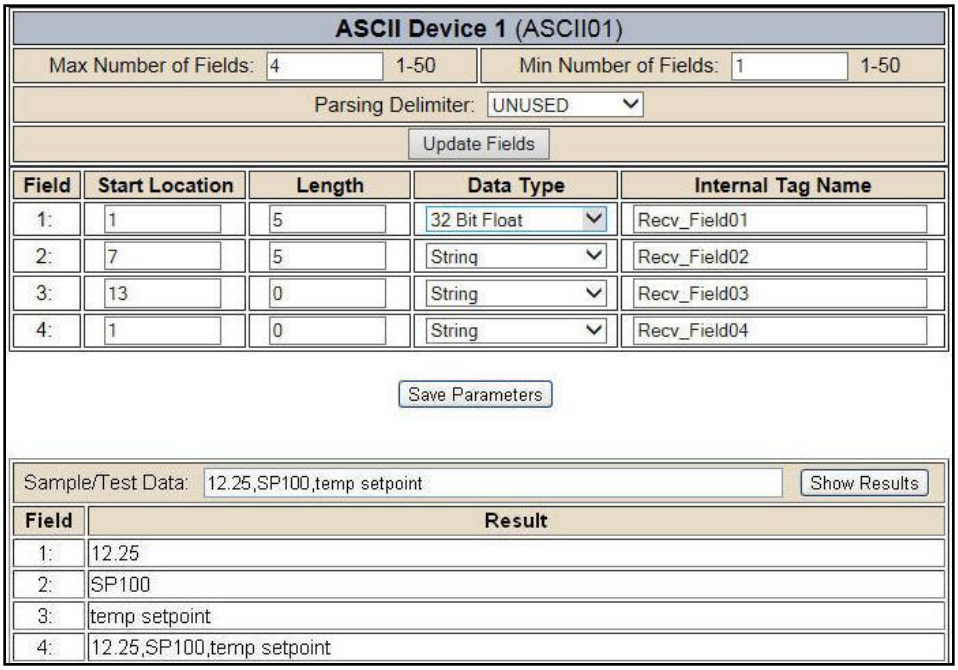
Example #1 - Parsing a message using the Parsing Delimiter option:

In this example, we are separating the string "12.25,SP100,temp setpoint" by a comma delimiter. The first value is being parsed into a float data type, the second and third values are being parsed into a string data type. Since the Min Number of Fields is 3, all 3 fields must be present for the message to be considered valid and processed. The output is seen below:

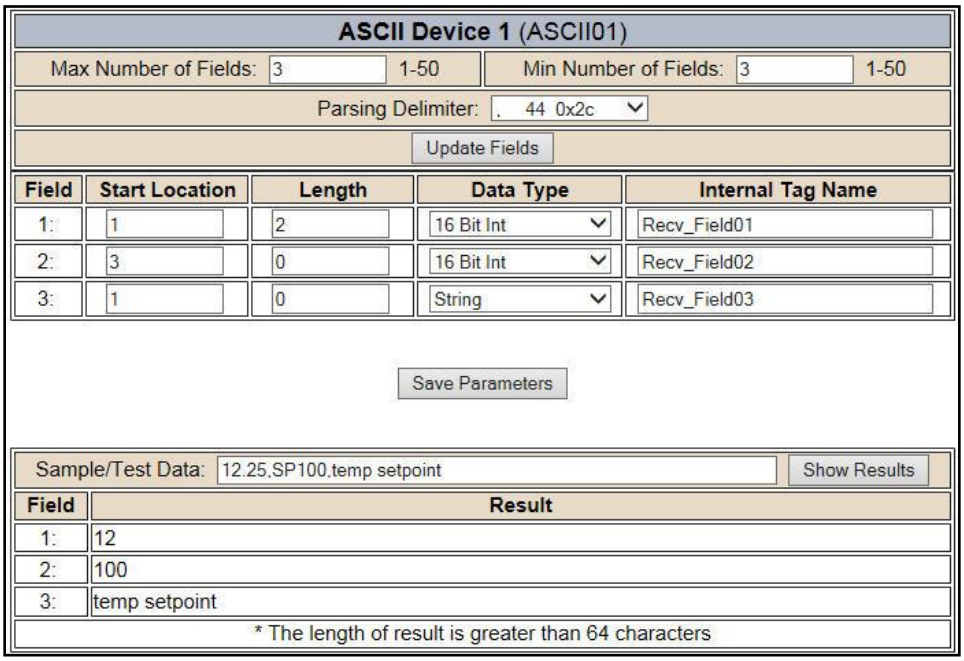


Example #2 - Parsing a message without the Parsing Delimiter option:

In this example, we are separating the fields in the string "12.25,SP100,temp setpoint" using the start and length parameters. The first value is being parsed from the 1st character for a length of 5 and stored into a float data type. The second value is being parsed from the 7th character for a length of 5 characters and stored into a string data type. The third value is being parsed starting from the 13th character for the rest of the remaining characters and stored into a string. The fourth value contains the entire ASCII message and is stored into a string. Only the first field needs to be present for the data to be considered valid and will be processed. If less than field 1 is present, the message will not be parsed and will be flagged an error. The output is seen below:

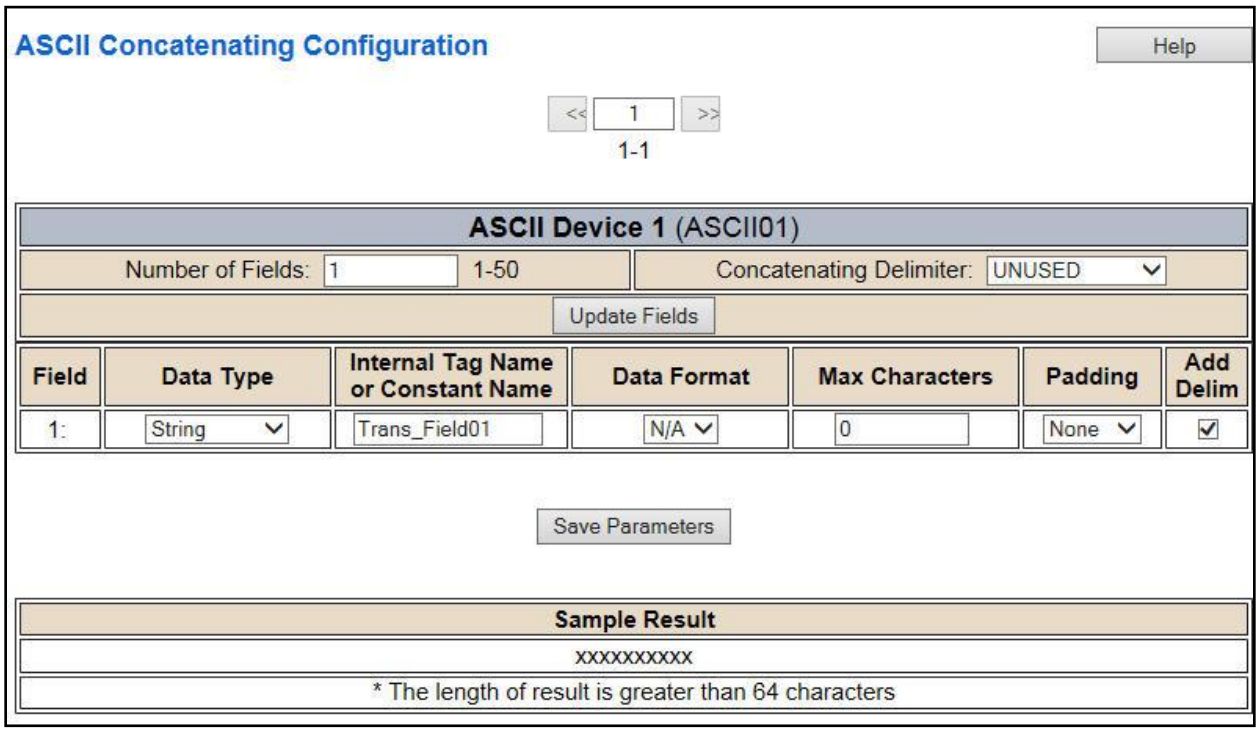


Example #3 - Parsing a message using the Parsing Delimiter option and Start Location and Length:
In this example, we are separating the fields in the string "12.25,SP100,temp setpoint" using the comma delimiter, the start, and length fields. The first value is being parsed from the 1st character for a length of 2 and stored into an integer data type. The second value is being parsed from the 3rd character of the second comma-parsed field for the remainder of that field and stored into an integer data type. The third value is being parsed starting from the 1st character of the third comma-parsed field for that entire field and stored into a string. All 3 fields need to be present for the message to be valid. The output is seen below:



ASCII Configuration – ASCII Concatenating

The ASCII concatenating feature allows you to combine multiple data points and locations, in the mating protocol, into a single ASCII string. Click the **ASCII Concatenating (Optional)** button at the bottom of the ACII Configuration page to access the ASCII Concatenating Configuration page for this device.



1) **Number of Fields:** This indicates how many values will be concatenated together to form a single ASCII message (up to 50 values per message).
2) **Concatenating Delimiter:** This adds a delimiter between data fields in the ASCII string. If a delimiter should not appear between each of the fields, select UNUSED.
3) **Data Type:** Select the data type of the parsed value.
    a. Signed and Unsigned 8/16/32/64 Bit Integers
    b. 32/64 Bit Floating Points
    c. String – in order to use, a String data type must be selected in the other protocol. Cannot concatenate an Integer to a String.
    d. Constant String
4) **Internal Tag Name/Constant Name:**
    a. If data type other than Constant String is selected, then this will be the name to reference this tag within the gateway. This value is used on the display page and the mapping page.
    b. If data type Constant String is selected, then this is the string value that will send.
5) **Data Format:**
    a. %d – used for Signed Integers
    b. %u – used for Unsigned Integers
    c. %lf – used for Floating Points with no set decimal precision
    d. %.1lf…%.6lf – used for Floating Points to show the offset of the decimal point value

i. EX: 123.456789 set as %.3lf will display as 123.456

e. %e – used for Exponential Notation
f. %x – used to represent Hexadecimal values for Signed/Unsigned Integers or Floating points
g. String and Constant String data types do not use this field

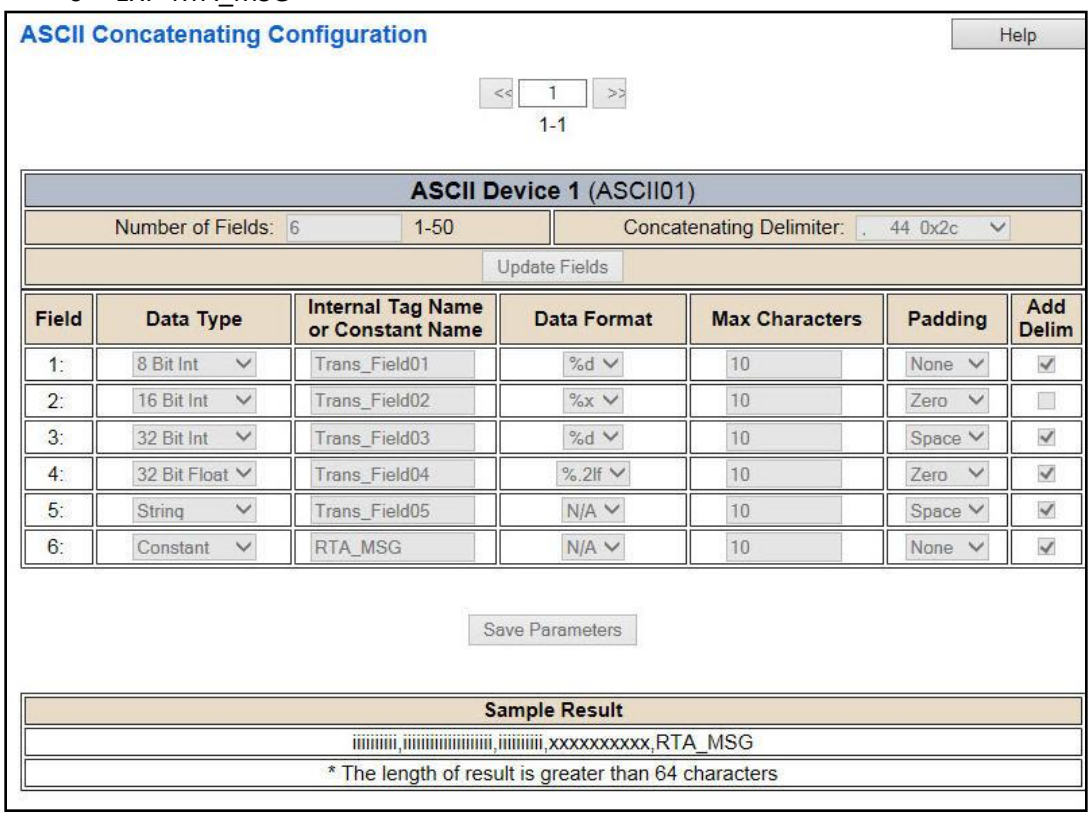
6) **Max Characters:** This is the max number of characters that can be transmitted for a single field.
Special Cases
   a. If set to 0, the entire field is transmitted.
   b. If the length of the value is less than the Max Characters, then the Padding Character will be used (if set).
   c. If the length of the value is greater than the Max Characters, then the value will be truncated.
7) **Padding:** If the length of the value is less than the Max Characters padding Zeroes, Spaces, or Nothing to the remaining character placeholders, the padding will occur to the left of the value.
8) **Add Delim:** Used when a concatenating delimiter is selected. Check to add the concatenating delimiter to the end of that field.
9) **Sample Result:** This will display an example of how the data will output. This will not display live data. It provides an example of the string structure.
NOTE: Sample Result field will only show the first 64 characters of the message.
   a. String data and constant data types will display as *x*'s.
   b. Any other data type will display as *i*'s.
   NOTE: For display purposes, if Max Characters is set to 0, only 10 characters will display for that field in the Sample Result section. The true value, if larger, will be processed correctly.
      EX: Field 1 is set for a String data type and Max Characters is set to 0, only 10 *x*'s will display in the sample result even though the max character length is set to 50.

ASCII Configuration – ASCII Concatenating Examples

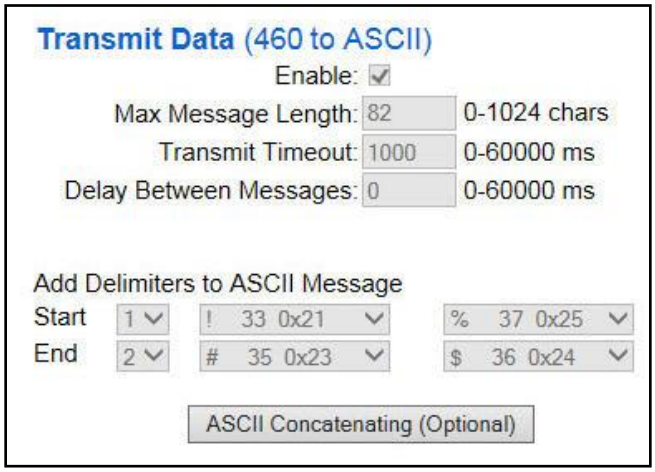
Example #1 - Concatenating a message using the concatenating delimiter option:

In this example, the comma is selected as the concatenating delimiter. Let's look at each field closer:

1) Field 1 –8 bit int represented as Trans_Field01 in the gateway. It will output as an integer with a max of 10 characters. No padding is used and a comma will be added to the end of the value.
   - EX: "34,"
2) Field 2 –16 bit int represented as Trans_Field02. It will output in Hexadecimal with a max of 10 characters, padded with zeros and no comma will be added to the end of the value.
   - EX: "00000000A0"
3) Field 3 –32 bit int represented as Trans_Field03. It will output as an integer with a max of 10 characters, padded with spaces and a comma will be added to the end of the value.
   - EX: "____123456," (shown with _'s to see spaces)
4) Field 4 –32 bit float represented as Trans_Field04. It will output as a float with 2 decimal places with a max of 10 characters, padded with zeros and a comma will be added to the end of the value.
   - EX: "00001234.56,"
5) Field 5 –String represented as Trans_Field05 in the gateway. It will output as string with a max of 10 characters, padded with spaces and a comma will be added to the end of the value.
   - EX: "___testing," (shown with _'s to see spaces)
6) Field 6 – Constant String will output as "RTA_MSG" with a max of 10 characters. No padding is used and no comma will be added to the end (though checked) since it is the last field.
   - EX: "RTA_MSG"



Below is a sample of the Transmit Data is set up with the following delimiters:



Example 1 Sample Result: This use case is sending data via 5 PLC tags. Using the concatenating setup example and the transmit example, the ASCII data will be displayed within your ASCII device shown in the example below.

```
!123,0000003039      1234,0000123.45,ASCII Test,RTA_MSG#$
```

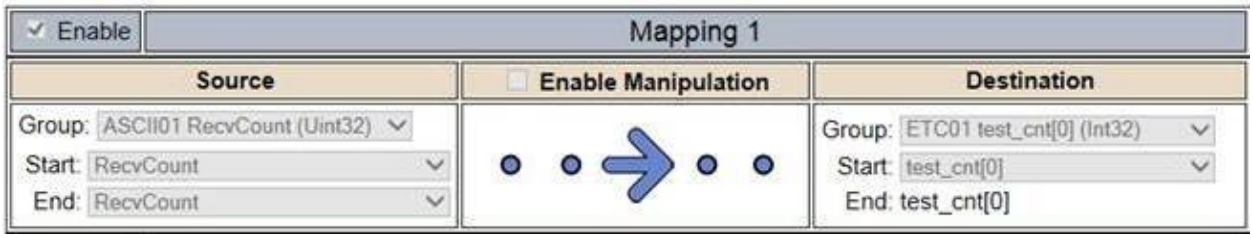
ASCII Configuration – ASCII Message Counter

There is an additional ASCII variable that is very useful to access within the gateway's mating protocol. This data variable will need to be added manually since it will not be mapped using Auto-Map.

RecvCount- indicates how many ASCII messages have been successfully read by the gateway for that device. A successful incoming message means that at least one of our three end cases (Max Length, Timeout or Delimiters) has been met. This will match the Diagnostic Variable Successful Receive Count for each ASCII device.

This variable can be mapped to the mating protocol using the Data Mapping webpage. It is mapped just like the Status_XY variable described in the Data Mapping- Adding Diagnostic Information section of this user guide.

Example: For this example, the other protocol in the gateway is the Allen-Bradley PLC. As you can see from the picture below, the RecvCount for ASCII Device 1 is mapped to the first index of a PLC tag array called test_cnt. The data type of this tag is an Int32 to match the data type of RecvCount. The tag test_cnt[0] will now hold the number of successfully read messages from ASCII Device 1.

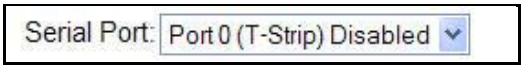


Application Use: This is particularly useful for applications connecting devices like barcode scanners and weigh scales. The gateway will cyclically update the mating protocol with the last ASCII message sent, a change in the RecvCount is the only way to identify a new message if the messages are identical.

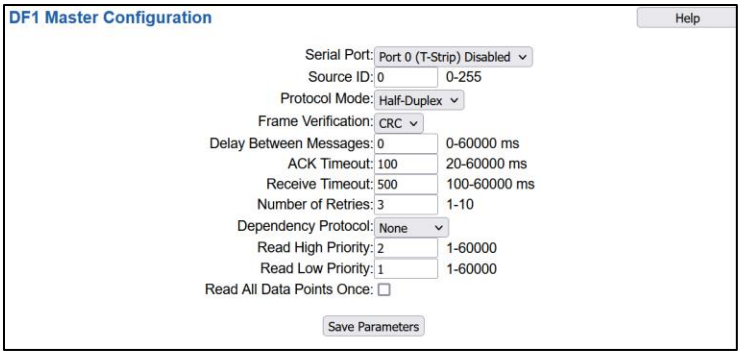
DF1 Master Configuration

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.



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.
10) **Read High Priority**: Configures the number of high priority requests to process before switching to low priority requests. This number should be higher than the Read Low Priority.
11) **Read Low Priority**: Enter the number of low priority requests to process before switching to high priority requests. This number should be lower than the Read High Priority.
12) **Read All Data Points Once**: If Enabled, the gateway will read all configured data points once on startup regardless of priority, then begin processing requests based on priority after all points have been read once.

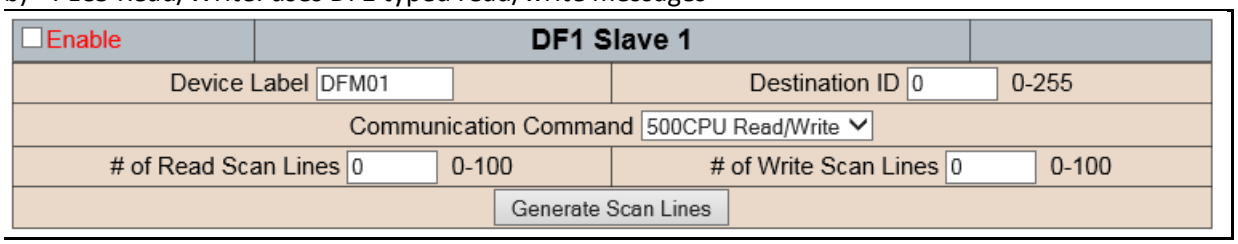


DF1 Master Device Configuration

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.

   a) If you are configuring multiple devices click **<<** or **>>** to navigate to another device.
   b) To create a new slave with the same parameters already configured from another slave, click the -Select- dropdown and select the **Add from 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.
   c) To remove a device, navigate to the slave to delete using the **<<** and **>>** buttons and click the **Delete DF1 Slave** button.
   d) Click the **Save Parameters** button to save your changes before restarting or going to another configuration page.
2) The **Enable** check box should be selected for the device.
3) Enter a **Device Label** to identify the device within the gateway.
4) Enter a unique **Destination ID** for the device on the network. This number should be different from the Source ID entered at the top of the page.
5) **Communication Command:** Select the DF1 read/write Communication Commands to use to communicate to the slave device.
   a) 500CPU read/write (default): uses DF1 Protected Typed Logical Read/Write messages with 3 address fields
   b) PLC5 Read/Write: uses DF1 typed read/write messages



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.
6) When configuring read scanlines there is an optional priority configuration. There are three priority selections available, how often each priority is read is configurable in the DF1 Master Configuration section using the Read High Priority and Read Low Priority Configurations.

    a. High: Read the scanline based on the Read High Priority configuration.

    b. Low: Read the scanline based on the Read Low Priority configuration.

    c. Once: Read the scanline once on gateway startup or upon a new connection and never again during normal operation.

Read Scan Lines (DF1 Slave to 460DFMSC)

	Line #	Priority	File Type	File Number	File Offset	# of Points *See Ranges Below
☐	1	High	B	0	0	1
		<< 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 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.

Write Scan Lines (460 to DF1 Slave)

	Line #	File Type	File Number	File Offset	# of Points *See Ranges Below
☐	1	B	0	0	0
		<< 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 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.

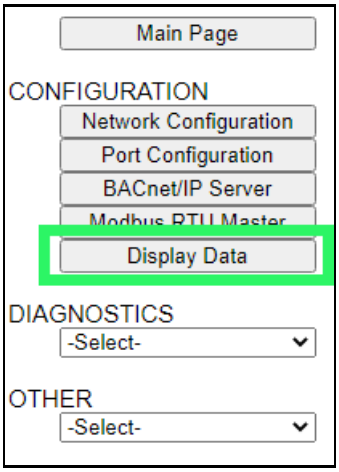
Going from Manual Mapping to Auto-Mapping will delete ALL mappings and manipulations configured.

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.

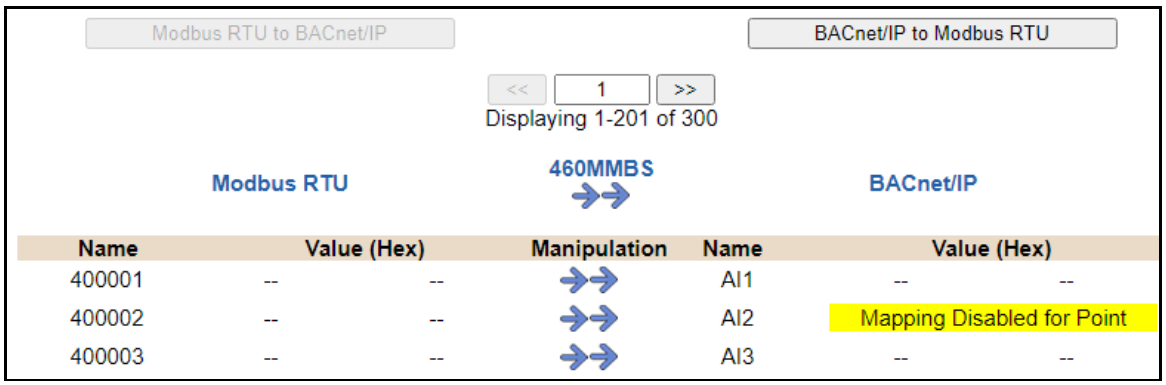
Display Data

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



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

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



In the above example, we see the following:

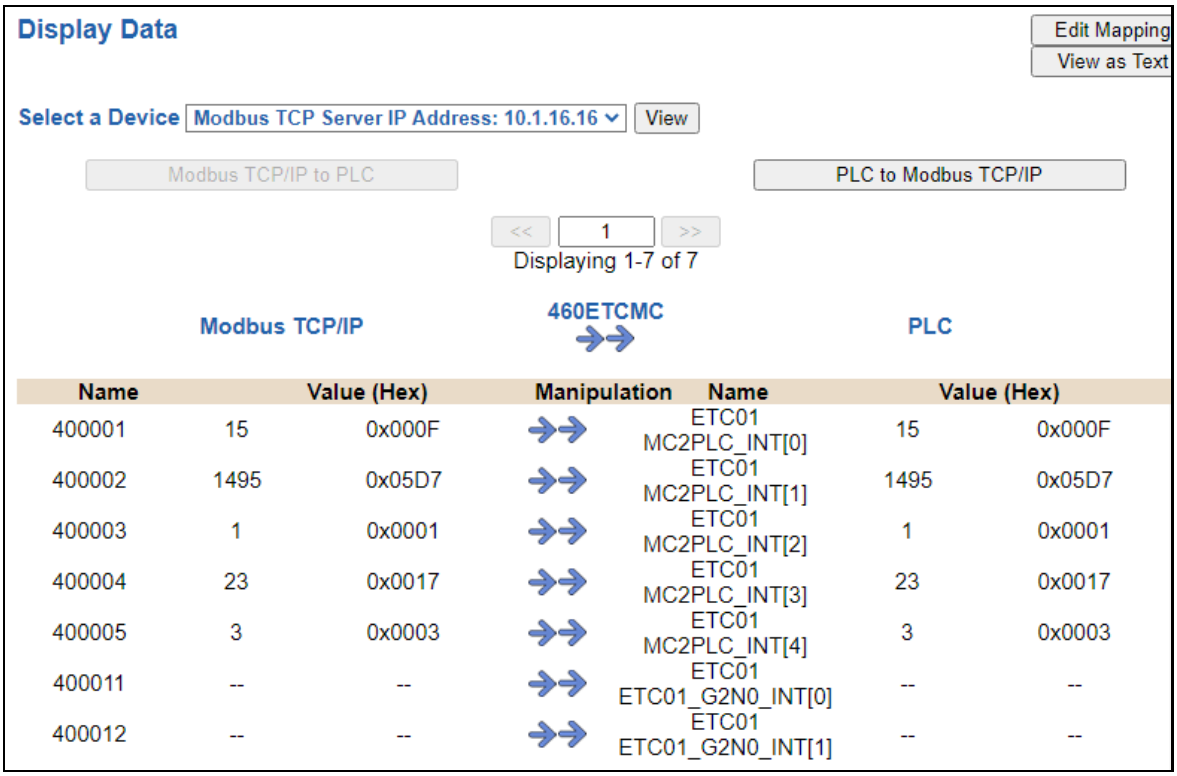
- Modbus register 400001 from Slave 1 is being mapped to AI1 on BACnet
- Nothing is being moved from Modbus register 400002 to AI2 on BACnet because the mapping is disabled
- Modbus register 400003 from Slave 1 is being mapped to AI3 on BACnet

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

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

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

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

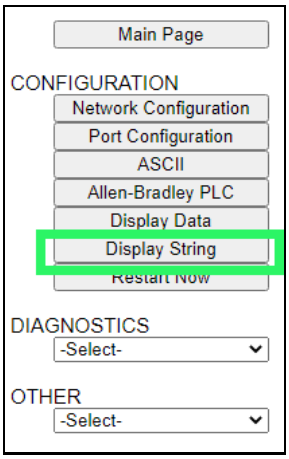


To view the actual data mappings, click the **Edit Mapping** button. For more details, see the Data Mapping-Explanation section.

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

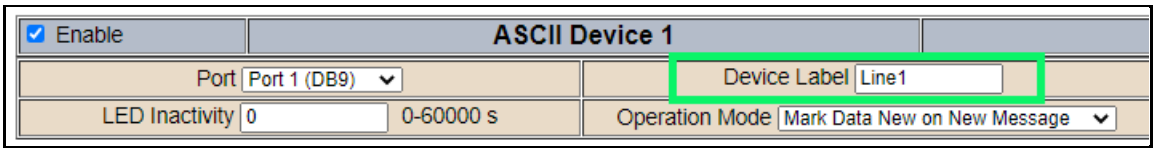
Display String

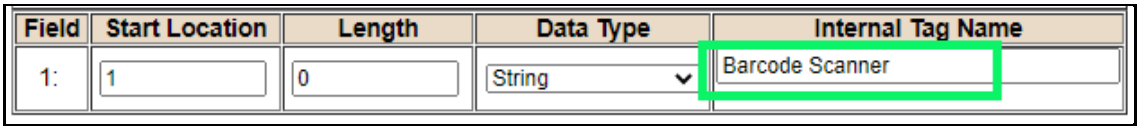
Click the **Display String** button to view what the values of each Parsing and/or Concatenating strings are, you can also click on the Edit Mapping to view the mapping of each string.



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

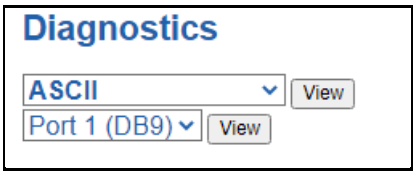
In the Group drop down, “Line1” is defined on the ASCII Device configuration page and “Barcode Scanner” is defined in the ASCII Parsing configuration.



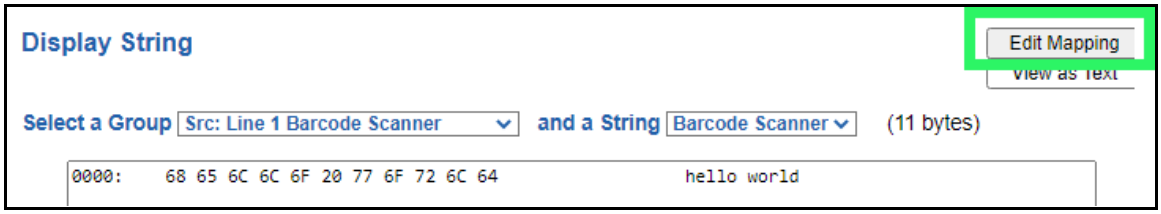


If there are values of “Data Not Valid “on this page, it indicates that the source has not been validated yet and no data is being sent to the destination.

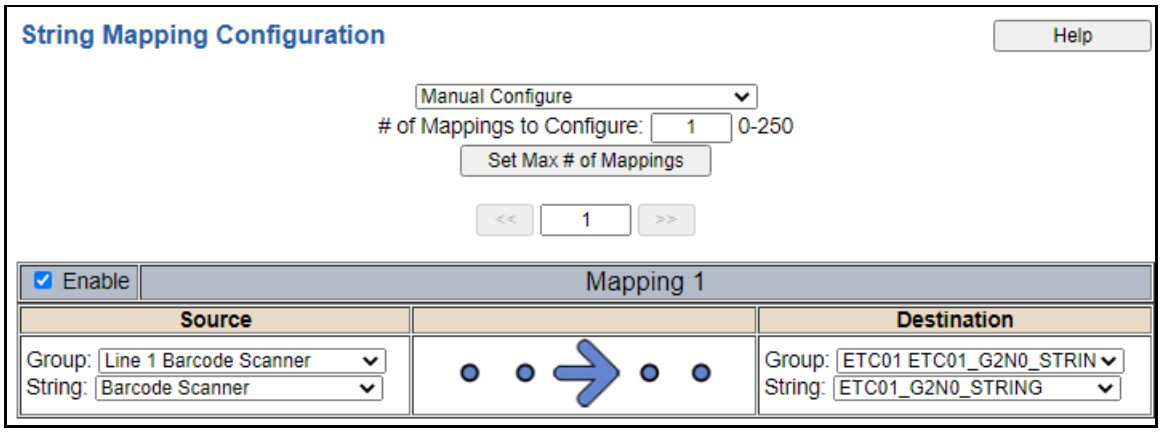
NOTE: You can view the whole string data by clicking on **Diagnostics Info** drop down and navigating to ASCII Diagnostics page. You will also have to select the port you want to view in the dropdown below ASCII.



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



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



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

Display String use case

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

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 6B 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 6B   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.

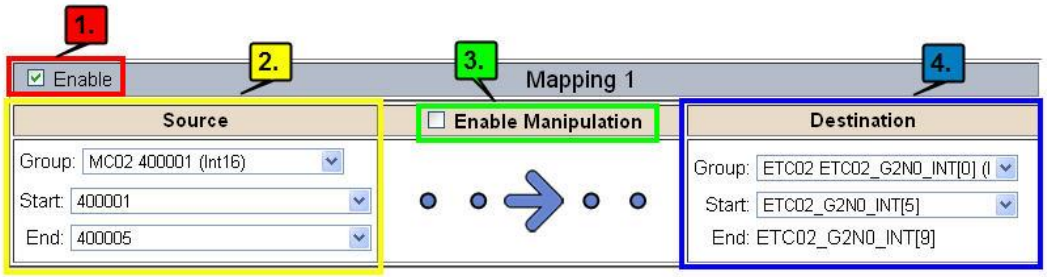
   a. Both Source values were able to be mapped to a corresponding Destination value.

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

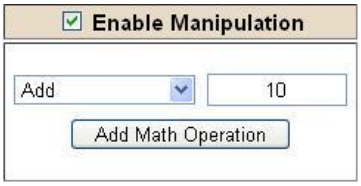
   a. The 32-bit Float from the Source location could not find a matching Destination data-type. After all other like data types were mapped, the only data type available was the 2nd 32-bit Uint data type. Auto-Configure was completed even though the data in the Float will be truncated.

Data Mapping – Explanation

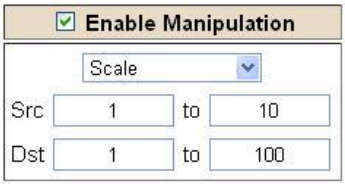
Below are the different parts that can be modified to make up a data mapping.



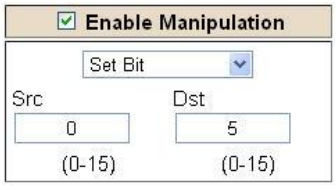
1) Enable (red box above): Check to enable mapping. If not checked, this mapping is skipped.
2) Source Field (yellow box above):
   a) Group - Select the data group you set up in the protocol config to use for this mapping.
   b) Start - This is the starting point for this mapping.
   c) End - This is 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.

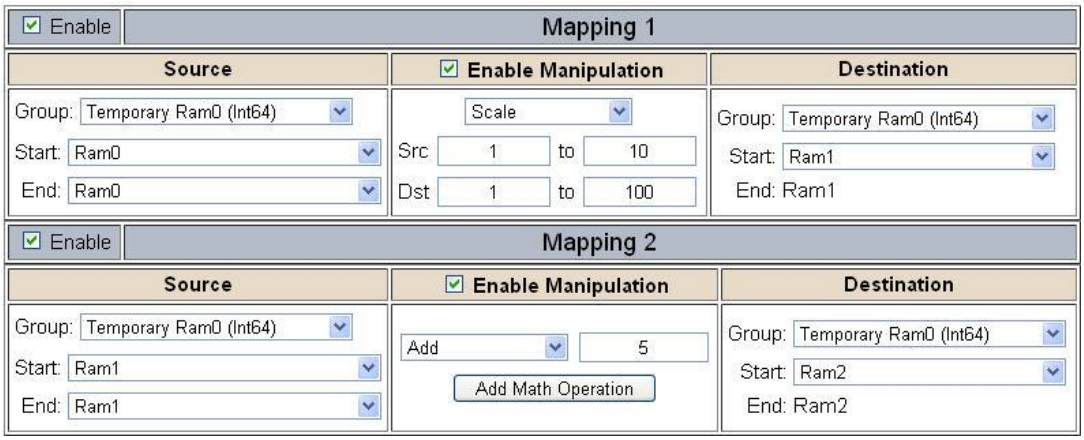
4) Destination Field (blue box above):
   a) Group - Select the data group you set up in the protocol config to use for this mapping.
   b) Start - This is the starting point for where the data is being stored.
   c) End - The End point is derived from the length of the source and cannot be modified.

Data Mapping – Adding Diagnostic Information

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

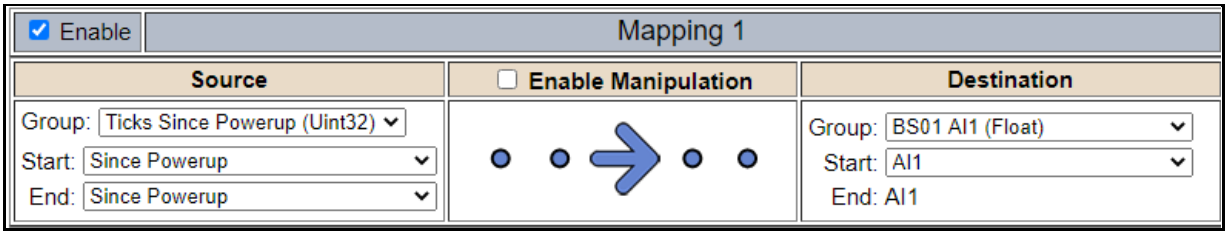
IMPORTANT NOTE: Only add Diagnostic Information **AFTER** both sides of the gateway have been configured. If changes to either protocol are made after diagnostic information has been added to the mapping table, it is necessary to verify all mappings. Remapping may be necessary.

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



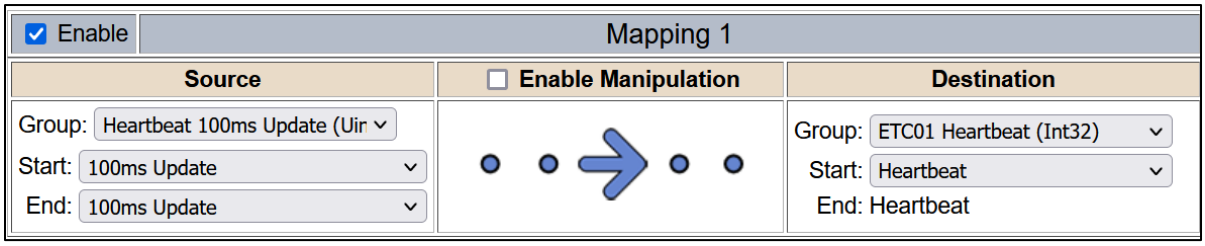
In this example, Ram0 is scaled into Ram1. Ram1 is then increased by 5 and stored into Ram2. Ram0 and Ram2 could be considered a source or destination group.

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



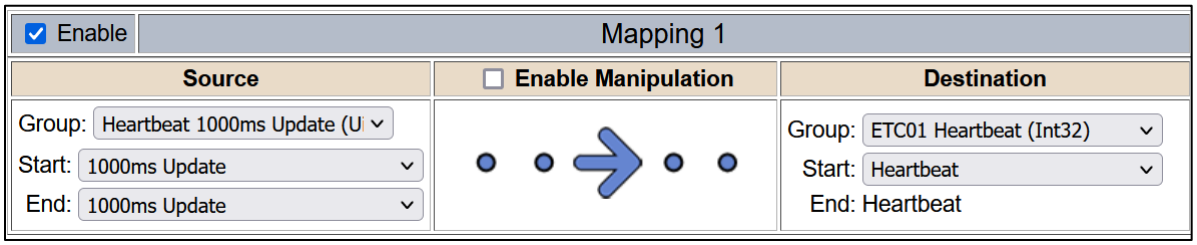
4) **Heartbeat 100ms Update**

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



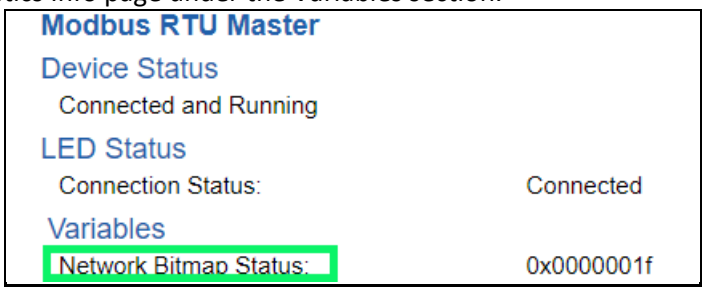
5) **Heartbeat 1000ms Update**

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



6) **XY_NetBmpStat**

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



b) Since a Client/Master may be trying to communicate with multiple devices on the network, it may be beneficial to know if a Server/Slave device is down. By using this Network Bitmap Status, you can expose the connection statuses of individual devices. **Values shown are in HEX.**

i) 0x00000002 shows that only device 2 is connected

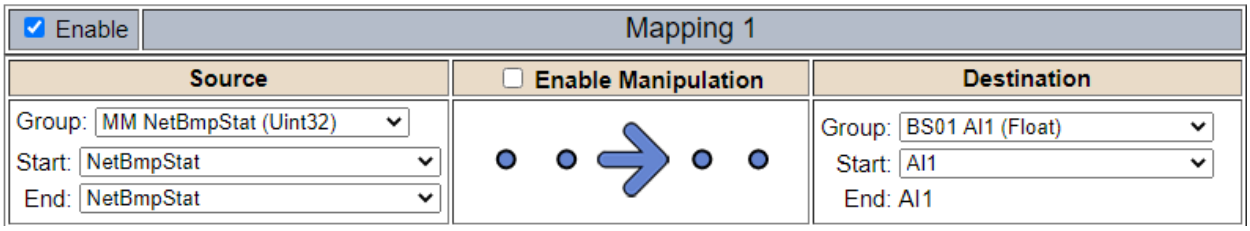
ii) 0x00000003 shows that only devices 1 and 2 are connected

iii) 0x0000001f shows that all 5 devices are connected (shown in image above)

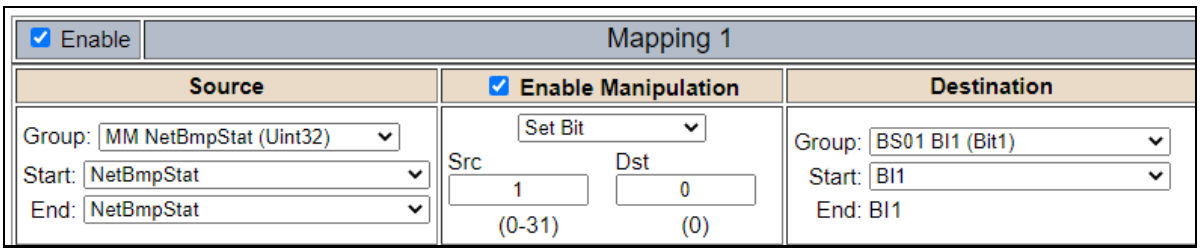
c) There are multiple ways to map the NetBmpStat.

Option 1: Map the whole 32bit value to a destination. Example below shows the NetBmpStat is going to an Analog BACnet object. Using a connection of 5 Modbus Slave devices AI1 will show a value of 31.0000. Open a calculator with programmer mode and type in 31, this will represent bits 0 – 4 are on. This mean all 5 devices are connected and running.

If using an AB PLC with a Tag defined as a Dint, then expand the tag within your RSlogix software to expose the bit level and define each bit as a description such as device1, device2, etc.



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



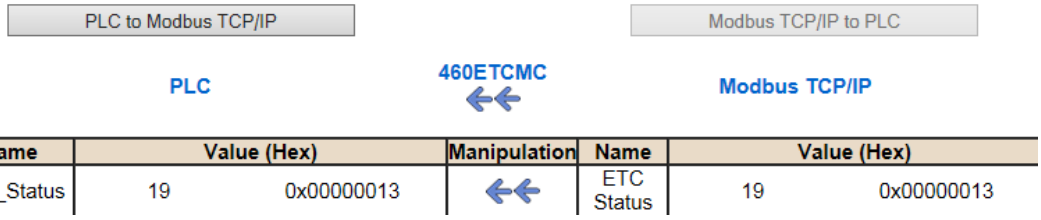
7) Status_XY

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

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

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

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



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

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

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

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

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

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

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

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

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

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

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

PLC — 460ETCMC — Modbus TCP/IP

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

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

Common Status:

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

Recoverable Faults:

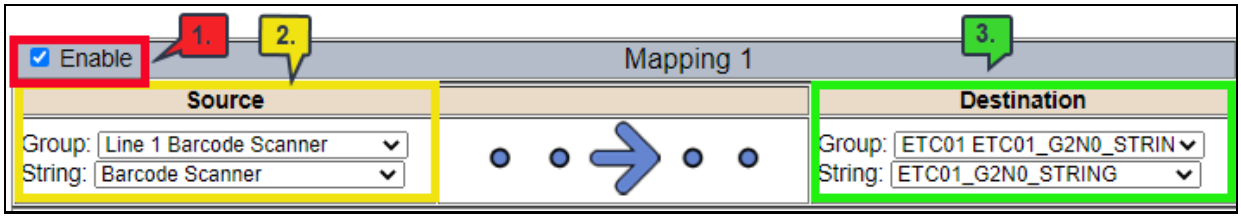
Hex:	Bit:	Decimal:	Explanation:
0x01	16	65,536	recoverable fault – timed

Total:	0x010041	65,601

String Mapping – Explanation

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

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

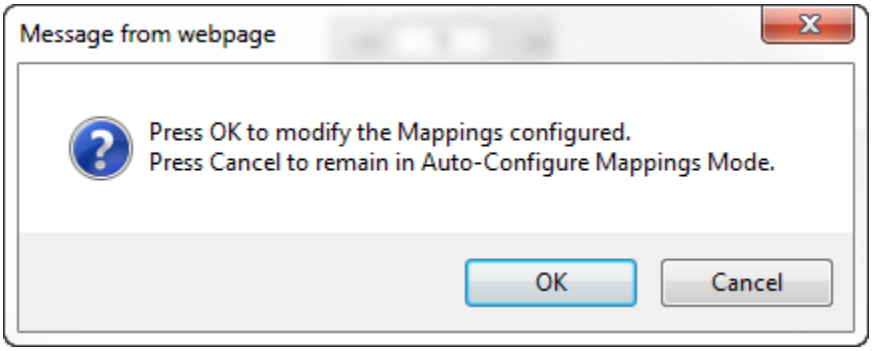


1) Enable (red box above): Check to enable mapping. If not checked, this mapping is skipped.
2) Source Field (yellow box above):
   a) Group - Select the string data group you set up in the protocol config to use for this mapping.
   b) String - This is the string used for this mapping.
3) Destination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

Mapping – Auto-Configure Mode to Manual Configure Mode

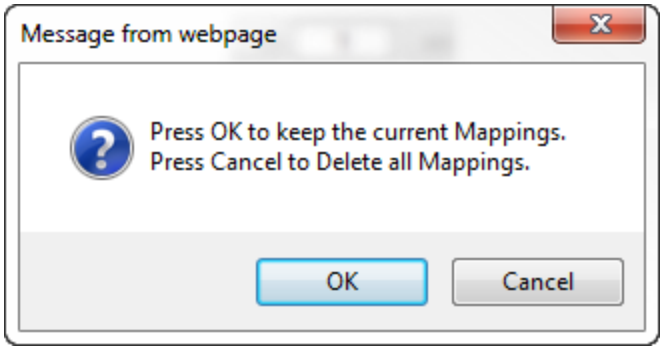
To transition from Auto-Configure Mapping Mode to Manual Configure Mode, click the dropdown at the top of the Mapping Configuration page and select Manual Configure.

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



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

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



1) To keep the mappings that are already configured press **OK**.

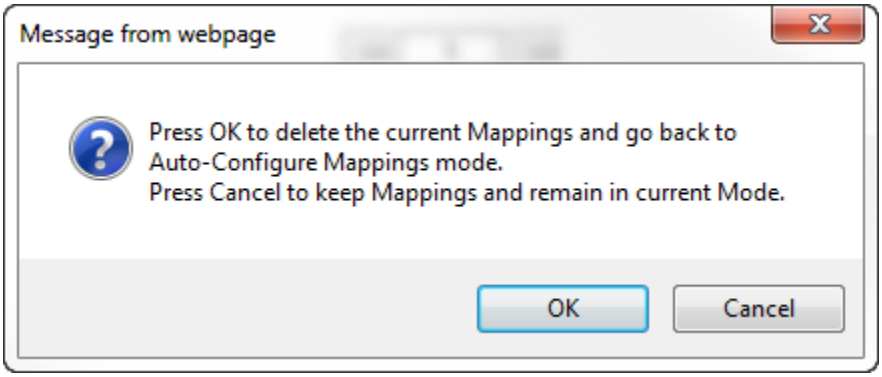
    a) You would want this option if you are adding additional mappings or you want to modify the mapping(s) that already exist.

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

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

Mapping – Manual Configure Mode to Auto-Configure Mode

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



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

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

View as Text

Data Mapping

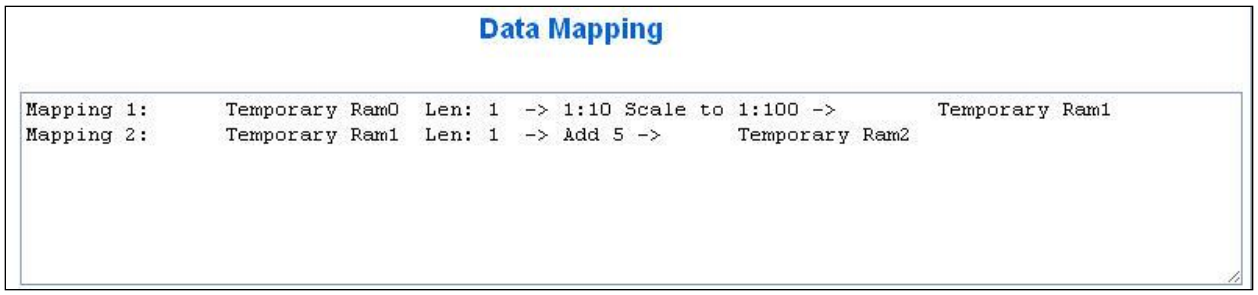
The View as Text page displays the point to point mapping(s) you set up in the Data Mapping section. This will also display any manipulation(s) that are configured.

Each line on this page will read as follows:

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

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

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



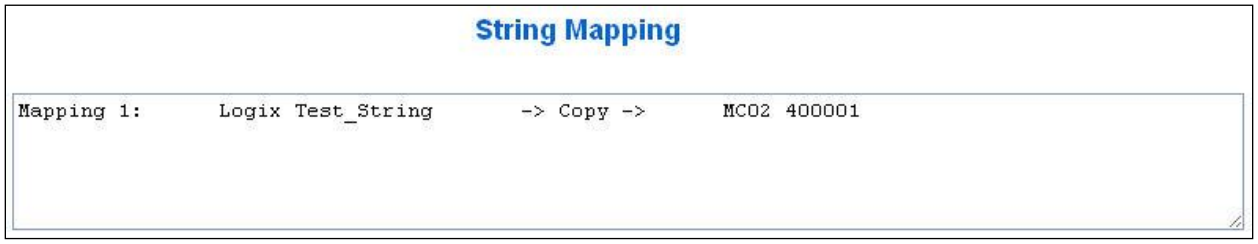
String Mapping

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

Each line on this page will read as follows:

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

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



Base Triggering – Data Validiation Triggering

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

How does this work?

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

How do you set this up?

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

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

Write Data Groups (BACnet/IP to 460MCBS)

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

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

Setup BACnet Names, Units, and COV

21	G01	Data Validation Trigger	Other	no-units	1.000000

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

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

40	G01	Data Validation Result	Other	no-units	1.000000

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

Enable	Mapping 2	
Source	**Enable Manipulation**	**Destination**
Group: BS01 AO1 (Float) Start: AO21 End: AO21		Group: MC Trigger 0 (Uint16) Start: Trigger 1 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.

Enable	Mapping 3	
Source	**Enable Manipulation**	**Destination**
Group: MC Handshake 0 (Uint16) Start: Handshake 1 End: Handshake 1		Group: BS01 AI1 (Float) Start: AI40 End: AI40

Security Configuration

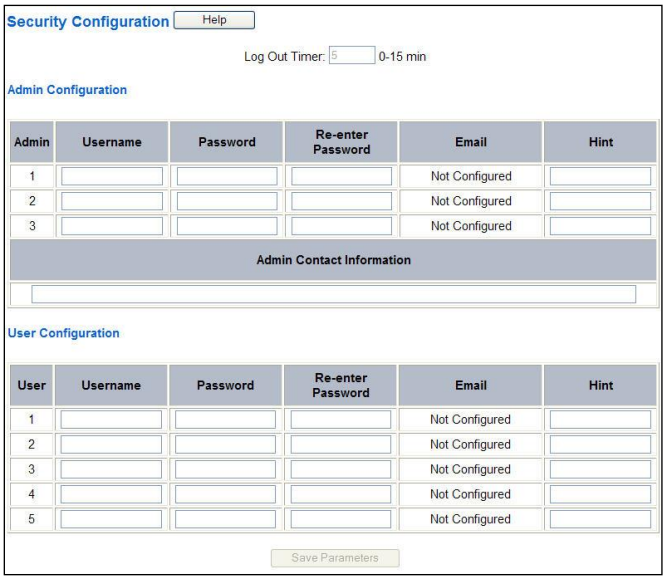
To setup security on the 460 gateway, navigate to **Other->Security Configuration**. You can configure Security for 3 administrators, 5 users, and 1 guest.

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-Security Levels

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

Security Levels:

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

Security - Log In

Username: Name of the user to login.

Password: Password of the user to login.

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

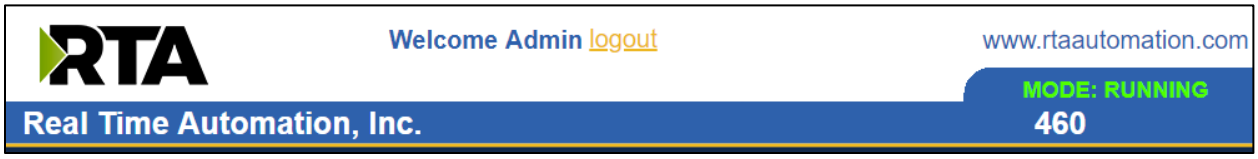
Send Password to Email: Sends the specified User's Password to the email configured for that user.

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

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

Security - Log Out

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



Closing the browser is not sufficient to log out.

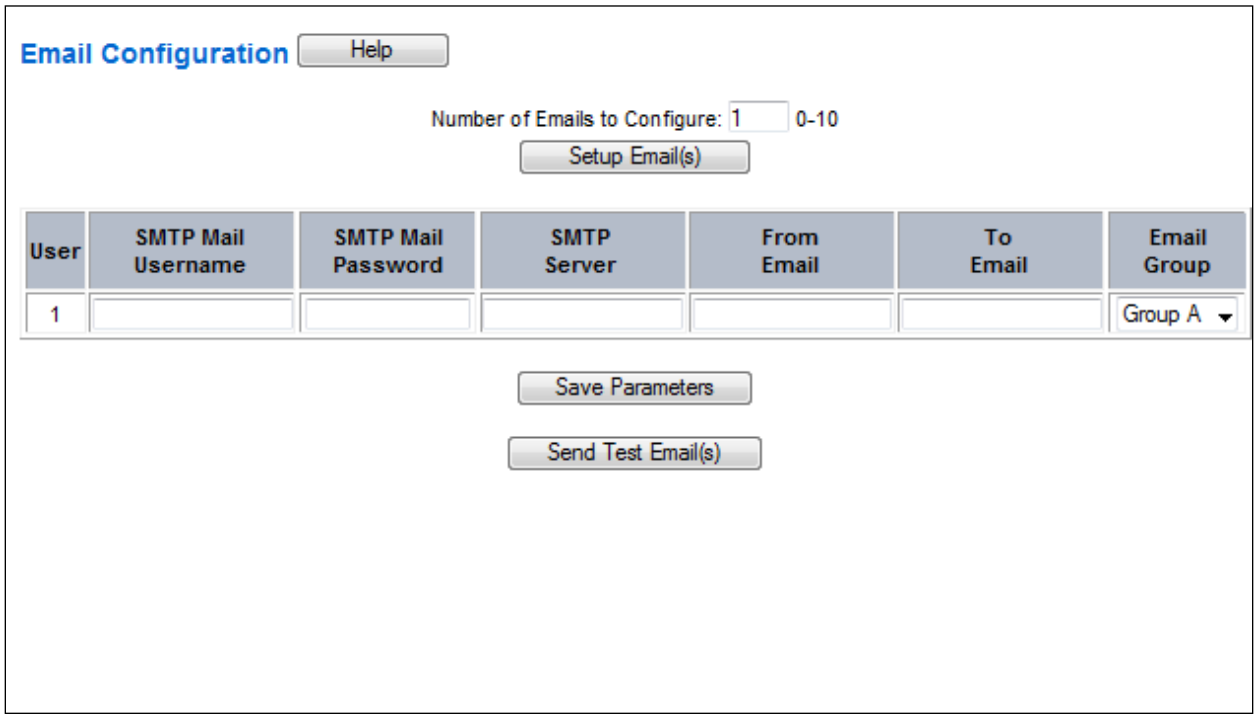
Email Configuration

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

You can configure up to 10 email addresses.

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

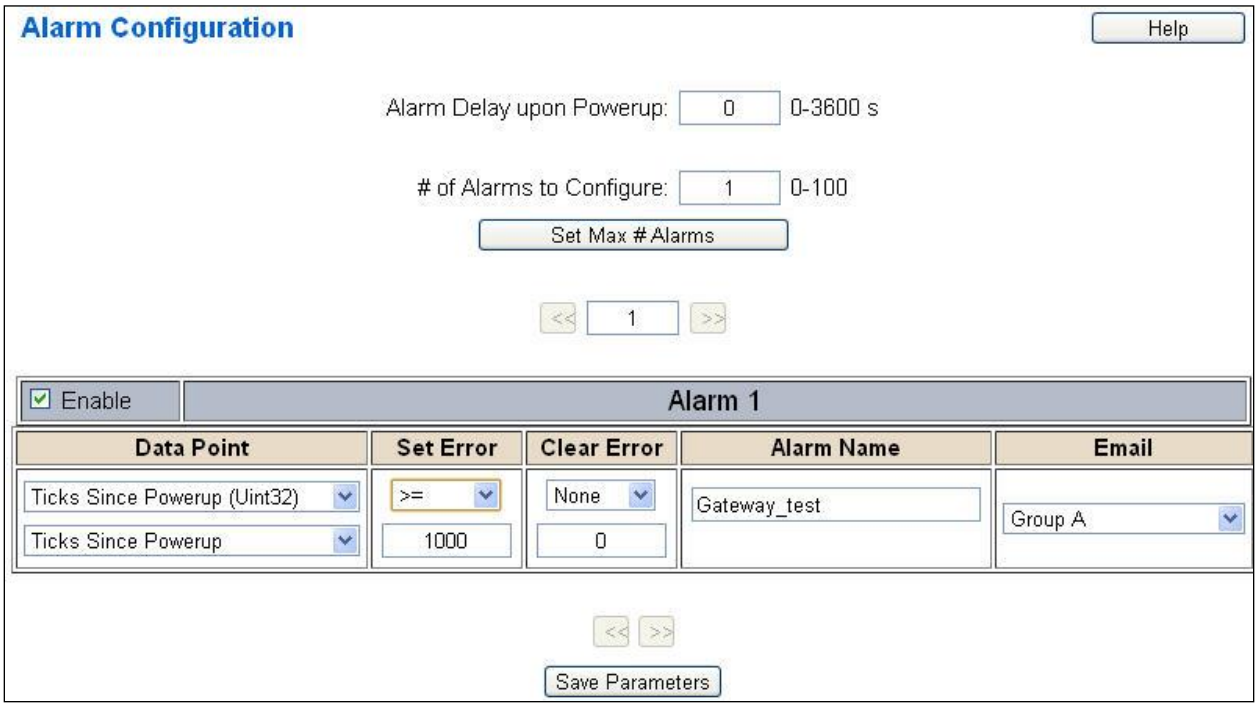
Click the **Save Parameters** button to commit the changes and reboot the gateway.



Alarm Configuration

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

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



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

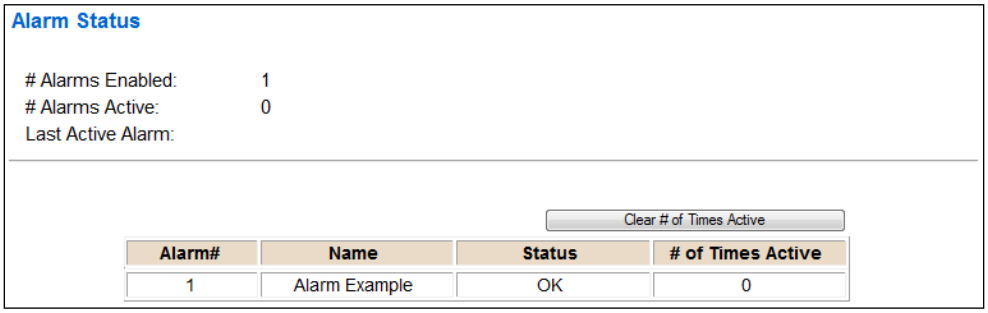
5) In the Clear Error Section:
    a. Select the Clear Error Operation. Available options are <, >, <=, >=, !=, ==, and Change of State (COS). This is the operation that will be used to compare the Data Point value against the Error Value to determine if the alarm needs to be cleared.
    b. Select the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

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

Diagnostics – Alarm Status

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

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

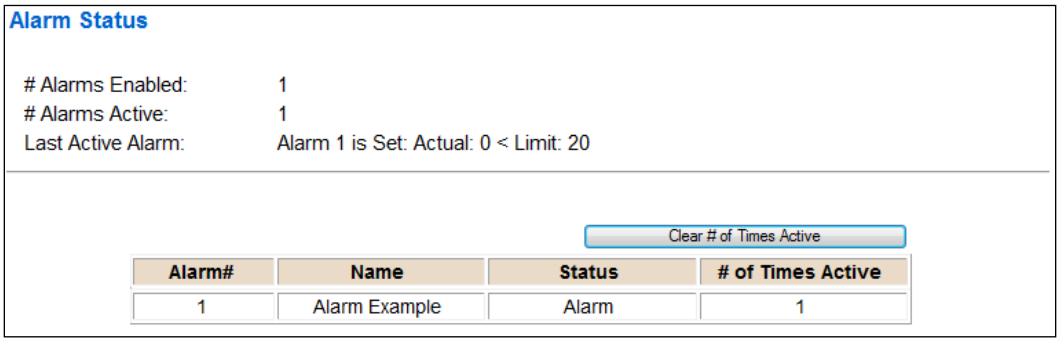


Alarms – Active

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

When an alarm is activated, the following will occur:

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



Alarms – Clear

When an alarm is cleared, the following will occur:

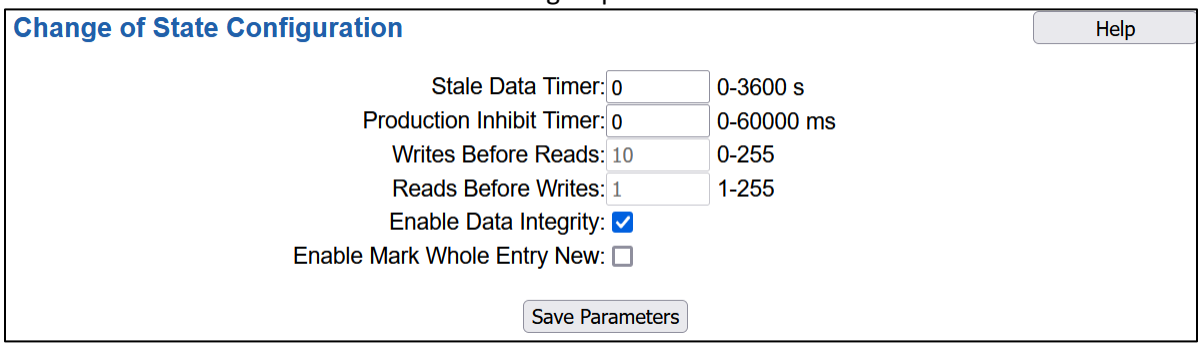
1) A one-time notification will be sent to the email associated with the alarm.
    a. For duplicate emails to occur, the alarm must become active and then be cleared again.
2) Total *# Alarms Active* will decrement. *Last Active Alarm* will not be changed.
3) Status of the Individual Alarm will be reset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

Change of State (COS) Configuration

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

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

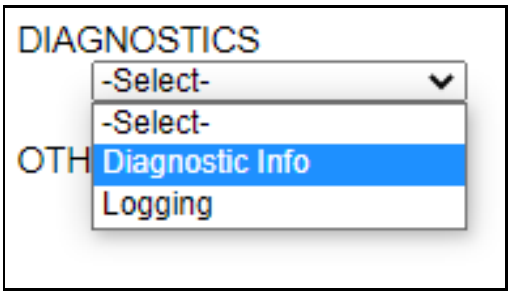
1) **Stale Data Timer**: If the data has not changed within the time allocated in this Stale Data Timer, the data will be marked as stale within the gateway and will force a write request to occur. This timer is to be used to force cyclic updates in the gateway, since data will only be written if it 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.
6) **Enable Mark Whole Entry New**: If Enabled, mark the entire scan line or data group new upon 1 data element within the scan line or data group to be new.



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

Diagnostics Info

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



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

Diagnostics Mapping

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

Common Errors:

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

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

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

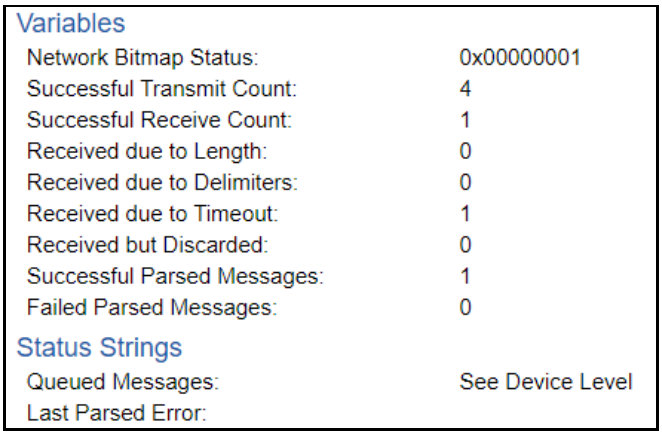
Diagnostics – ASCII

Select ASCII in the top dropdown menu on the Diagnostics Page to view a breakdown of the diagnostics that are displayed on the page. You may also view individual ASCII device counters and messages by selecting the device in the *All ASCII* dropdown and clicking **View**. Additional diagnostic information can be found by clicking the **Help** button.

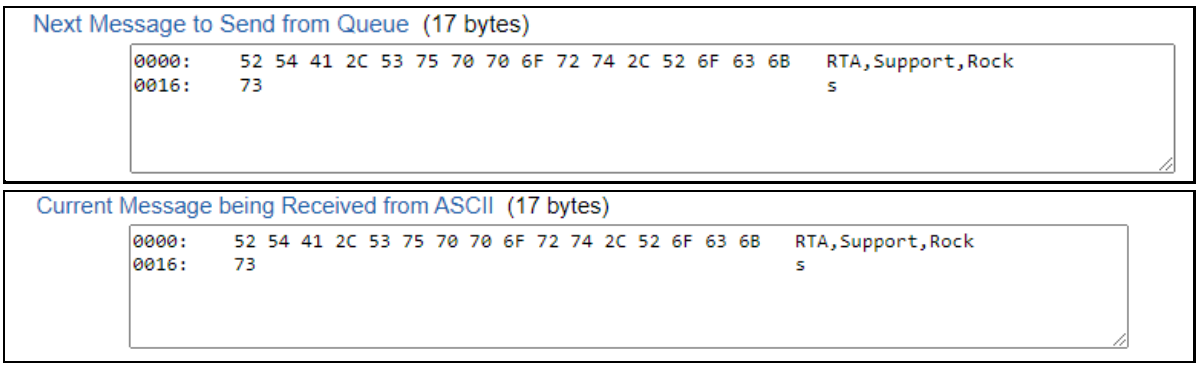
NOTE: This page will auto-refresh every five seconds with the latest data.

Clear All Values - This will only affect displayed values.

1) This will reset all displayed values back to zero and clear the Status Strings.
   Example: If viewing ASCII – Port #, this will only clear the values for Port #. This will reduce the *All ASCII* values indirectly.

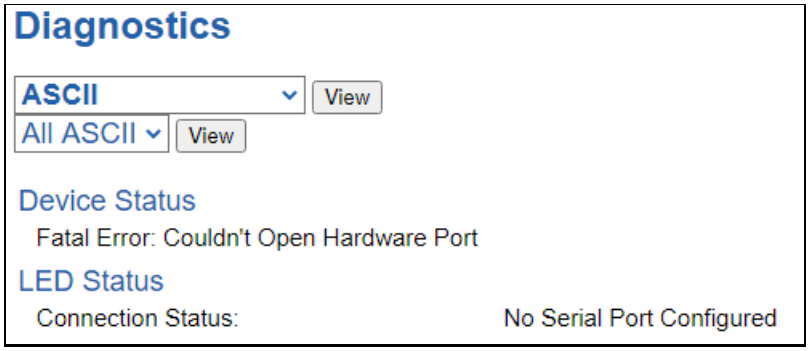


Clear Buffers - This will clear the Next Message to Send from Queue buffer and Current Message being received from ASCII buffer and any message stored in the Queue.

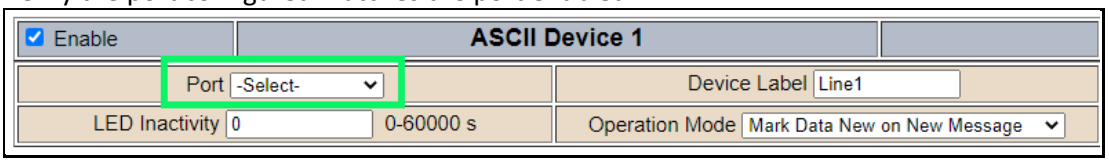


Device Status - This will only display when viewing *All ASCII*.

1) Connected and Running– The gateway is connected to all the ASCII devices and data is being received/transmitted.
2) Not Connected – There have been no messages received or transmitted.
   a. Verify that the serial /TCP/IP/USB settings match your device.
3) Fatal Error: Hardware Port Not Configured – The port selected on the ASCII Configuration page is not configured.

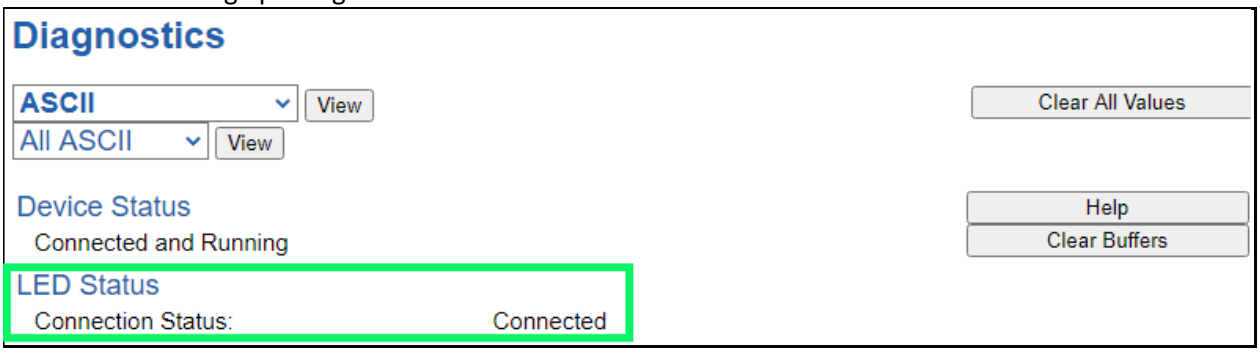


   a. Verify the ASCII device is enabled and configured.
   b. Verify the port configured matches the port enabled.



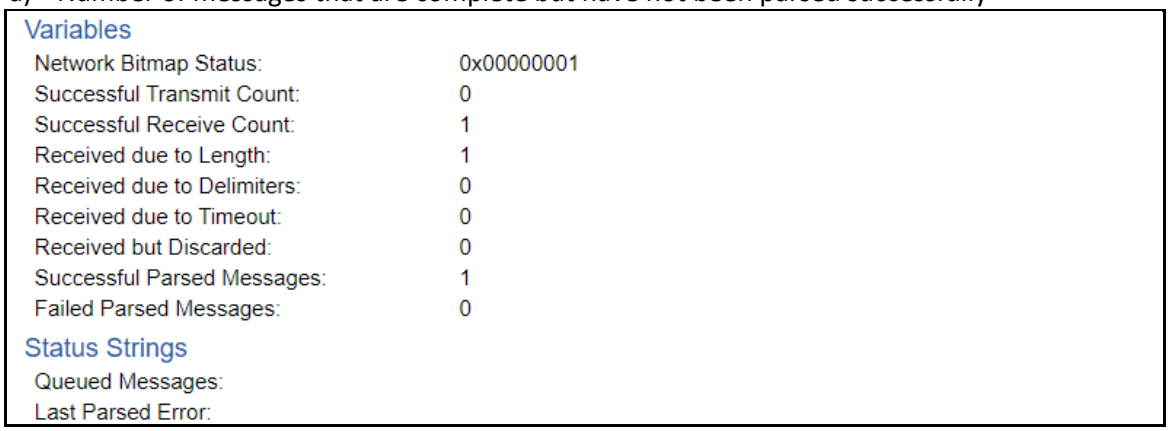
LED Status - This is the Status for *All ASCII* or the specific ASCII device selected.

1) Solid Green (Connected) – The gateway is receiving/transmitting data within the inactivity period for all the ASCII devices that are configured and enabled.
2) Flashing Green (Not Connected/First Time Scan) – Start up state. No messages have been received or transmitted, but port is connected.
3) Flashing Red (Connection Timeout) – The only way to exit this state is with a valid received message.
   a. Data has been discarded due to the queue being full.
   b. Data has not been received/transmitted within the inactivity period.
   c. Port not opened.
   d. Message parsing has failed.



Variables - These are the values for *All ASCII,* or the ASCII device selected.

1) Successful Transmit Count:
   a) Number of messages that the gateway has transmitted to the ASCII device
2) Successful Receive Count:
   a) Number of complete messages that the gateway has received from the ASCII device
3) Received due to Length:
   a) Number of messages completed due to the Max Message Length being reached
4) Received due to Delimiters:
   a) Number of messages completed due to the Start or End Delimiters being seen
5) Received due to Timeout:
   a) Number of messages completed due to the Receive Character Timeout being reached
6) Received but Discarded:
   a) Number of messages that are complete but discarded due to the queue being full
   b) Change the Gateway Hold Msg Timeout to be less than what you currently have set
7) Successful Parsed Messages:
   a) Number of messages that are complete and have been successfully parsed
8) Failed Parsed Messages:
   a) Number of messages that are complete but have not been parsed successfully



Status Strings - These are the values for *All ASCII,* or the ASCII device selected.

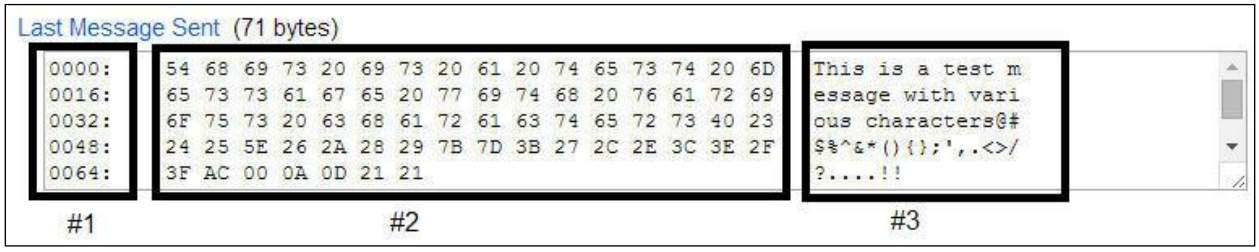
1) Queued Messages:
   a) The gateway will hold up to 20 (configurable) complete messages to send to the other protocol
   b) This will only increment if the Gateway Hold Msg Timeout is non-zero and messages are being received faster than we can send to the other protocol
2) Last Parsed Error:
   a) Last parsed error the gateway encountered

Common Error Messages:

1) **Number of Fields Invalid:** The total number of parsed fields is greater than the number of fields the gateway was expecting
2) **Discard:** The Field has been discarded
3) **Invalid Length for Field:** Number of characters parsed is greater than the number of characters that the gateway is expecting

4) **Calculated Length of Data exceeds 255 Characters:** Number of characters parsed within a field exceeds 255 characters

Buffers

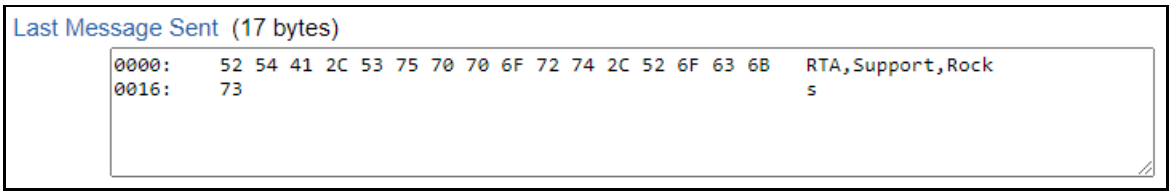


Each buffer text area is divided into three separate parts. Refer to screenshot above for labels.

1) Starting byte for that line
2) HEX character representation
3) ASCII character representation (Unprintable ASCII characters (like <CR>) will be displayed as '.' on the right-hand side of the buffer area.)

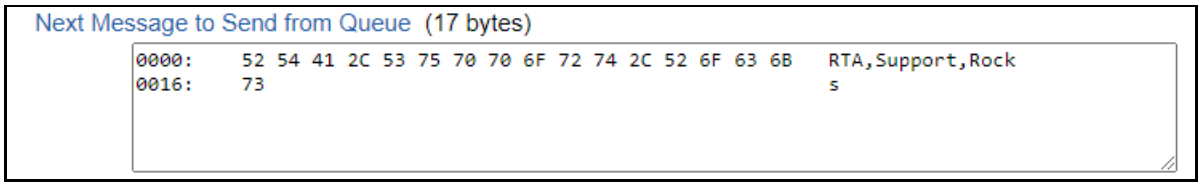
Last Message Sent:

1) Last complete message the gateway received from the ASCII device, processed, and sent to the other protocol



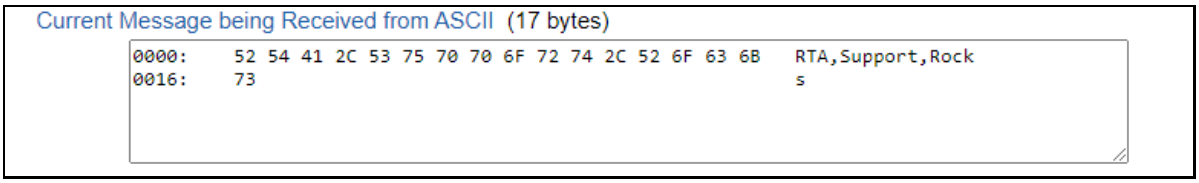
Next Message to Send from Queue:

2) This is the next complete message that the gateway has already received and processed from the ASCII device, and will be sent next to the other protocol



Current Message being Received from ASCII:

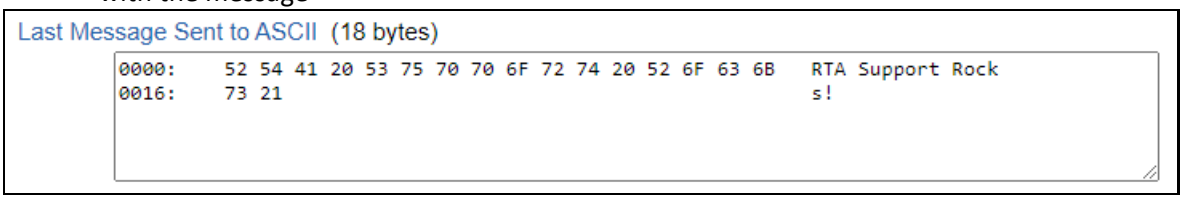
1) The current data that the gateway is receiving. The data needs to hit one of the three end cases to call a message complete:
   a) Max Message Length (max number of characters to receive)
   b) Receive Character Timeout (max time to wait after a character to call the current message complete)
   c) Delimiters (gateway has not received the delimiters that are specified)



Last Message Sent to ASCII:

1) Last message that the gateway sent to the ASCII device

   Note: The concatenated delimiters are not displayed in this message but will be transmitted with the message

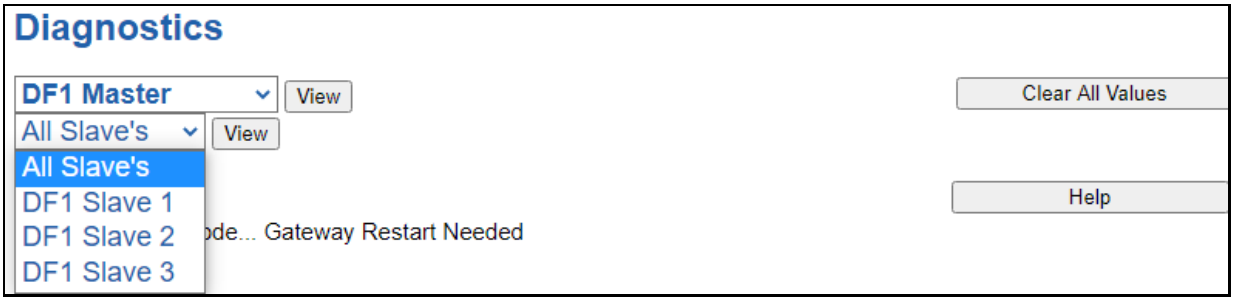


Send Data from Gateway to ASCII: (Used for testing only, Character limit of 1024):

1) Enter a message to send to your ASCII device
2) Can be used to test communication and test formatting of messages

Diagnostics – DF1 Master

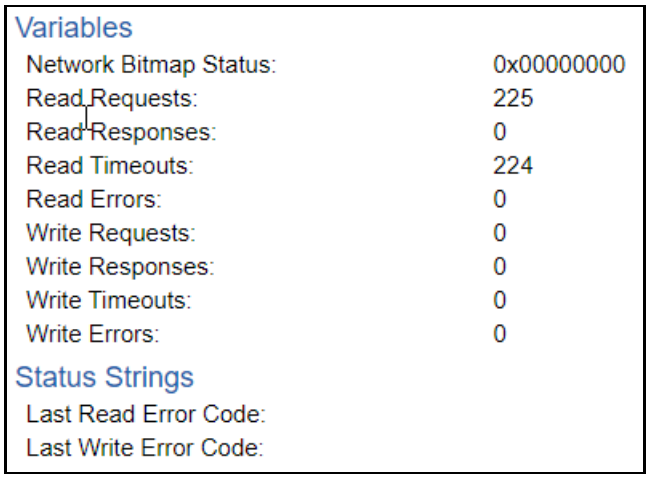
Select the DF1 Master in the top dropdown menu on the Diagnostics Page to view a breakdown of the diagnostics and common strings that are displayed on the page. You may also view individual slave counters by selecting the device in the *All Slaves* dropdown and clicking **View**. Additional diagnostic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



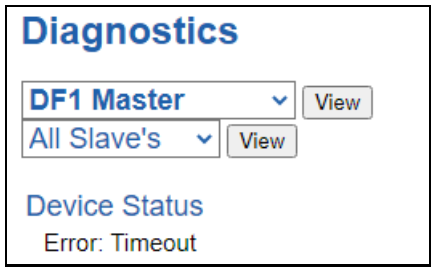
NOTE: This page will auto-refresh every five seconds with the latest data.

Clear All Values - This will only affect displayed values.

1) This will reset all displayed values back to zero and clear the Status Strings.
   Example: If viewing DF1 Master – Slave Address 1, this will only clear the values for Slave Address 1. This will reduce the *All Slaves* values indirectly, otherwise select All Servers to clear all devices.

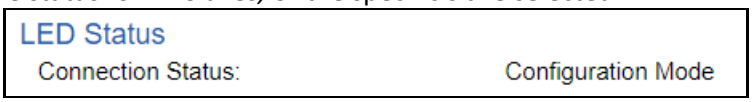


Device Status - This will only display when viewing *All Slaves*.



1) Connected and Running– The gateway is connected to all the DF1 slaves.
2) Error: Timeout – No DF1 scan lines are configured under an enabled slave.
   a) Or, one or more enabled DF1 slaves are missing.
   b) Verify DF1 device for correct Destination ID.
   c) Verify that Port Settings used match the DF1 slave(s) that the gateway is communicating with.
   d) 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 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 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 one 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.

Variables

Network Bitmap Status:	0x00000000
Read Requests:	0
Read Responses:	0
Read Timeouts:	0
Read Errors:	0
Write Requests:	0
Write Responses:	0
Write Timeouts:	0
Write Errors:	0
Read Request to Response Time (ms):	0
Read Response to Request Time (ms):	0
High Priority Read Loop Time (ms):	0
Low Priority Read Loop Time (ms):	0
Write Request to Response Time (ms):	0
Write Response to Request Time (ms):	0
Write Loop Time (ms):	0

Status Strings

Last Read Error Code:
Last Write Error Code:

1) Network Bitmap Status (Displayed in Hex):
   a) Each bit corresponds to a slave. If the bit is set, the slave is connected, otherwise the bit is 0.
   b) Bit 0 corresponds to slave 1 and Bit 4 is for slave 5 and so on.
2) Read Requests:
   a) Number of DF1 Read Requests that the gateway has sent to the slave device.
3) Read Responses:
   a) Number of valid DF1 Read Responses that the gateway has received from the slave device.
   b) **Note:** This should be equal to the number of Read Requests
4) Read Timeouts:
   a) Number of times the gateway has reached the timeout period waiting for a read response from the slave device.
5) Read Errors:
   a) Number of DF1 Read Errors
6) Write Requests:
   a) Number of DF1 Write Requests that the gateway has sent to the slave device.
7) Write Responses:
   a) Number of valid DF1 Write Responses that the gateway has received from the slave device.
   b) **Note:** This should be equal to the number of Write Requests
8) Write Timeouts:
   a) Number of times the gateway has reached the timeout period waiting for a Write Response from the slave device.
9) Write Errors:
   a) Number of DF1 write errors
10) Read Request to Response Time (ms):
   a) -Number of milliseconds it took the DF1 device to reply to a request

11) Read Response to Request Time (ms):
    a) -Number of milliseconds it took the gateway to execute the next request once the previous response has been received
12) High Priority Read Loop Time (ms):
    a) -Number of milliseconds it took to execute all high priority read requests
13) Low Priority Read Loop Time (ms):
    a) -Number of milliseconds it took to execute all low priority read requests
14) Write Request to Response Time (ms):
    a) -Number of milliseconds it took the DF1 device to reply to a request
15) Write Response to Request Time (ms):
    a) -Number of milliseconds it took the gateway to execute the next request once the previous response has been received
16) Write Loop Time (ms):
    a) -Number of milliseconds it took to execute all write requests

Status Strings - These are the values for *All Slaves,* or the specific slave selected.
1) Last Read Error Code:
    a) Last Read Request Error that the gateway received
2) Last Write Error Code:
    a) 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”
        i) Potential issues:
        ii) Selected Communication Command is not supported by the slave device
        iii) File Type and File Number does not exist in the slave device
        iv) File Offset does not exist in the Slave Device File Type and File Number
        v) Attempting to read more data elements than exist in the slave device
3) N (Slave Destination ID):
    a) Slave Destination ID of the slave that the error was received from
4) A (DF1 Request Address):
    a) Starting address of the DF1 Request in Offset Notation that the error was received from
5) L (Length):
    a) Number of points of the request that the error was received from

Example:

Read Errors:	2226
Write Requests:	0
Write Responses:	0
Write Timeouts:	0
Write Errors:	0
Status Strings	
Last Read Error Code:	STS=0x10,EXT_STS=0x00 (N:55 A:ST155:44444 L:1)
Last Write Error Code:	

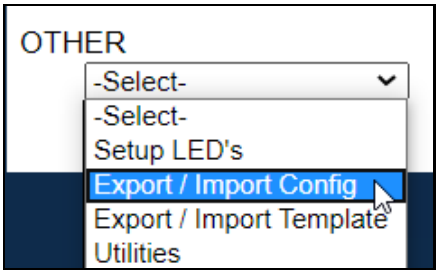
This Error Code indicates STS 0x10, EXT_STS=0x00, “Illegal command or format”. Other details are:

- 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.

Configuration Files

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



Export Configuration

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

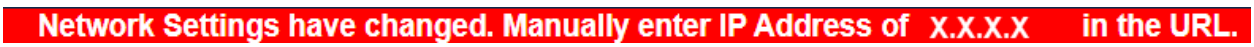
Upon clicking the **Save Configuration to File** button, you will be prompted to select a location to save the file. Different web browsers will yield different looks.

Import Configuration

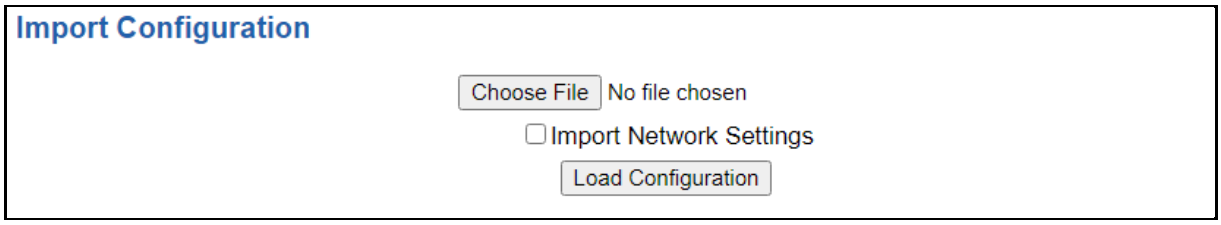
You can import a previously exported configuration file or a configuration file from another device into the 460 gateway, whenever it is in Configuration Mode.

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

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



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



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

Save and Replace Configuration Using SD Card

Saving Configuration Using SD Card

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

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

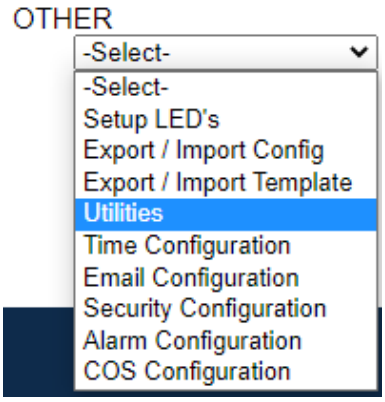
Replacing Configuration Using SD Card

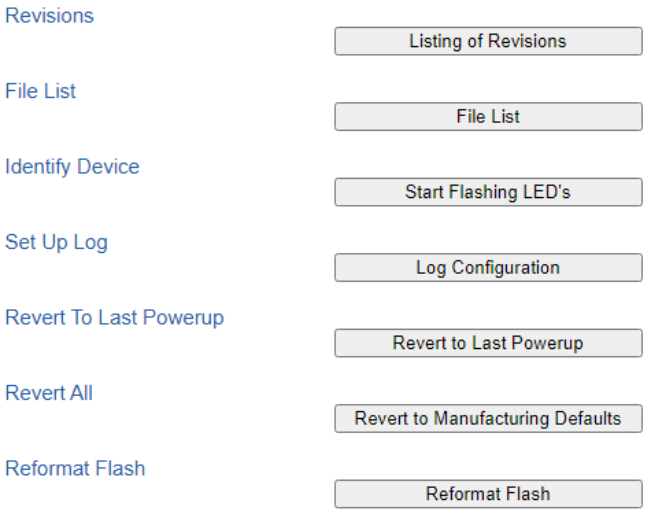
To replace a configuration in a gateway using the SD Card, a specific sequence of events must be followed for the replacement to happen correctly:

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

Utilities

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



Here you can also:

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