

460PSQT-NNA1
Protocol Gateway
Product User Guide

Firmware Version 8.8.10

Trademarks

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

Limited Warranty

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

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

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

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

Government End-Users

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

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

Revision History	6
Overview	7
Hardware Platforms.....	8
Hardware – NNA1	9
Powering the Gateway.....	9
Mounting with a DIN Rail.....	10
Installing.....	10
Removing	10
Accessing the Main Page.....	11
Error: Main Page Does Not Launch	12
Committing Changes to the Settings	13
Main Page	14
Device Configuration.....	15
Network Configuration	16
PROFINET IO Server Configuration	17
PROFINET IO Server Slot Configuration	18
PROFINET IO Server Slot Configuration: Auto-Configure.....	19
Auto-Configure Group by Device vs. Auto-Configure Group by Data Type.....	20
Group by Device (Default Method).....	20
Group by Data Type	20
PROFINET IO Server Slot Configuration: Manual Mode.....	21
Setting up the PLC- Example Using Simatic Classic Step 7	22
Setting up the PLC- Example Using TIA Portal	28
MQTT Client Configuration	35
MQTT Devices Configuration	35
Configuring Subscribe and Publish Topics	36
Amazon Web Services (AWS) Configuration.....	37
Additional AWS Requirements.....	38
How to FTP files into the RTA gateway	38
AWS IoT Core Service Setup.....	40
AWS IoT Core Service Things Configuration	42
Certificate setup.....	43
Attach policies to certificate	44

Testing AWS Communication	48
Send data from AWS to RTA gateway (Subscribe Topic)	48
Send data from RTA gateway to AWS (Publish Topics)	50
Testing Your MQTT Connections with MQTT Explorer	51
Send data from RTA gateway to MQTT Explorer (Publish Topic)	52
Send data from MQTT Explorer to RTA gateway (Subscribe Topic)	52
Mapping - Transferring Data Between Devices	53
Display Mapping and Values	54
Display Data	54
Display String	57
Display String use case	59
Data and String Mapping – Auto-Configure	60
Data Mapping – Explanation	61
Data Mapping – Adding Diagnostic Information	62
String Mapping – Explanation	66
Mapping – Auto-Configure Mode to Manual Configure Mode	67
Mapping – Manual Configure Mode to Auto-Configure Mode	68
View as Text	69
Data Mapping	69
String Mapping	69
Base Triggering – Data Validation Triggering	70
Security Configuration	72
Security Configuration-Security Levels	73
Security - Log In	74
Security - Log Out	74
Email Configuration	75
Alarm Configuration	76
Diagnostics – Alarm Status	78
Alarms – Active	78
Alarms – Clear	79
Change of State (COS) Configuration	80
Diagnostics Info	81
Diagnostics Mapping	81

Diagnostics – PROFINET IO Server	82
Diagnostic – MQTT Client.....	84
LED Configuration	86
Configuration Files	87
Export Configuration	87
Import Configuration	87
Save and Replace Configuration Using SD Card.....	89
Saving Configuration Using SD Card.....	89
Replacing Configuration Using SD Card	89
Intelligent Reset Button	90
Utilities	91

Revision History

Version	Date	Notes
8.6.0	2/28/20	Bug Fixes <ol style="list-style-type: none"> 1. Omron Plc Communication fixes for EtherNet/IP 2. Profinet GSDML Substitute values fix
8.7.4	9/1/20	Features Added: <ol style="list-style-type: none"> 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: <ol style="list-style-type: none"> 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: <ol style="list-style-type: none"> 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
8.8.10	10/11/21	Features Added: <ol style="list-style-type: none"> 1. Added MQTT Protocol 2. Supports 2 MQTT Brokers with 1 AWS

Overview

The 460PSQT-NNA1 gateway connects a PROFINET IO controller with up to three MQTT brokers or an AWS IoT core service. By following this guide, you will be able to configure the 460PSQT-NNA1 gateway.

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

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

Toll free: 1-800-249-1612

Email: support@rtautomation.com

Hardware Platforms

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

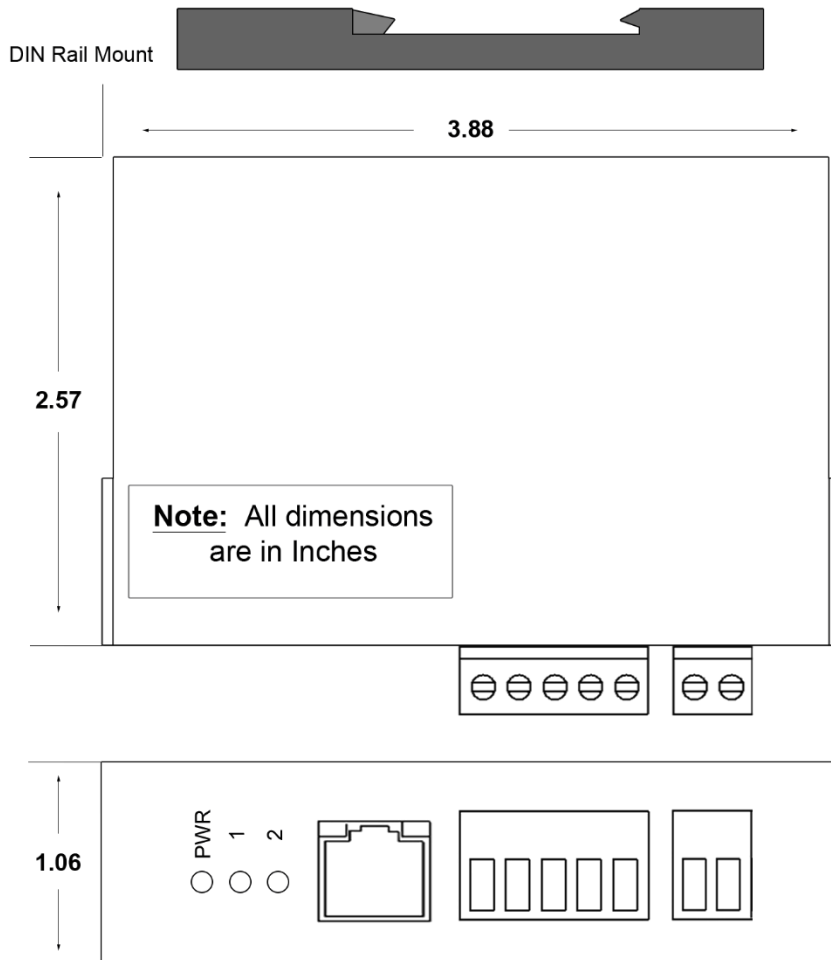
To find which hardware platform you are using:

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

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



Hardware – NNA1



Powering the Gateway

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



Mounting with a DIN Rail

Installing

Follow these steps to install your interface converter.

- 1) Mount your DIN Rail.
- 2) Hook the bottom mounting flange under the DIN Rail.
- 3) While pressing the 460PSQT-NNA1 against the rail, press up to engage the spring loaded lower clip and rotate the unit parallel to the DIN Rail.
- 4) Release upward pressure.



Removing

Follow these steps to remove your interface converter.

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

Accessing the Main Page

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

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



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

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

Error: Main Page Does Not Launch

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

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



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

C:\>ping 192.168.0.100

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

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

C:\>
```

The Screenshot above shows a gateway that is currently set to a static IP Address of 192.168.0.100.

If you are able to successfully ping your gateway, open a browser and try to view the main page of the gateway by entering the IP Address of the gateway as the URL.



Committing Changes to the Settings

- All changes made to the settings of the gateway in Configuration Mode will not take effect until the gateway is restarted via the webpage. Changes will not be stored if the gateway's power is removed prior to a reboot.
- **NOTE:** The gateway does not need to be restarted after every change. Multiple changes can be made before a restart, but they will not be committed until the gateway is restarted.
- When all desired changes have been made, press the **Restart Now** button.
- The webpage will redirect to our rebooting page shown below:



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

Main Page

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

Mode (orange box below):

Running Mode:

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

Configuring Mode:

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

Navigation (green box below):

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



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

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

Device Configuration

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

Main Page

Device Description:

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

Network Configuration

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

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

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



The screenshot shows a web interface for Network Configuration. At the top left is the title "Network Configuration" and at the top right is a "Help" button. Below the title is the sub-section "Ethernet Configuration". The configuration fields are as follows:

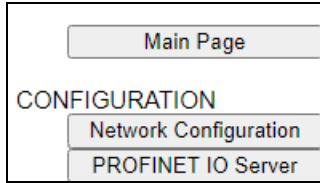
- Ethernet MAC Address: 00:03:F4:0B:C3:02
- Ethernet Link: Auto-Negotiate (dropdown menu)
- IP Setting: Static IP (dropdown menu)
- IP Address: 10.1.16.40
- Subnet: 255.255.0.0
- Default Gateway: 0.0.0.0
- DNS Gateway: 0.0.0.0

At the bottom center of the form is a "Save Parameters" button.

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

PROFINET IO Server Configuration

Click the **PROFINET IO Server** button to display the configuration page.



- 1) Select which **Network Interface** to use for this PROFINET IO connection. If using single port hardware, the Network Interface will default to Ethernet Port only.
- 2) **Device Label:** This is the PROFINET name that is assigned by TIA Portal or Classic STEP 7.

Profinet IO Server Configuration Help

Network Interface:

Device Name:

Profinet Slot List

Auto-Configure Group by Device

Input Slots (460ESPS to Profinet IO)			Output Slots (Profinet IO to 460ESPS)		
Slot	Data Size (Bytes)	Data Format	Slot	Data Size (Bytes)	Data Format
1	Disabled ▼	16 Bit Int ▼	11	Disabled ▼	16 Bit Int ▼
2	Disabled ▼	16 Bit Int ▼	12	Disabled ▼	16 Bit Int ▼
3	Disabled ▼	16 Bit Int ▼	13	Disabled ▼	16 Bit Int ▼
4	Disabled ▼	16 Bit Int ▼	14	Disabled ▼	16 Bit Int ▼
5	Disabled ▼	16 Bit Int ▼	15	Disabled ▼	16 Bit Int ▼
6	Disabled ▼	16 Bit Int ▼	16	Disabled ▼	16 Bit Int ▼
7	Disabled ▼	16 Bit Int ▼	17	Disabled ▼	16 Bit Int ▼
8	Disabled ▼	16 Bit Int ▼	18	Disabled ▼	16 Bit Int ▼
9	Disabled ▼	16 Bit Int ▼	19	Disabled ▼	16 Bit Int ▼
10	Disabled ▼	16 Bit Int ▼	20	Disabled ▼	16 Bit Int ▼

GSDML and Graphic Files
[GSDML-V2.34-RTA-460PSxx-20190219.zip](#)

Note: To properly set communication to the PROFINET controller, you will need to install the GSD file that is downloadable on the configuration web page or on the CD that was shipped with the unit. For instructions on how to do this, please see the [Setting up the PLC- Example Using Simatic Step 7 software](#) and [Setting up the PLC- Example Using TIA Portal](#) sections.

WARNING:

This gateway does not support the assignment of the IP address via the IO controller function. This function must be disabled for the system to function properly.

PROFINET IO Server Slot Configuration

The bottom area of the PROFINET IO Server Configuration page lets you configure multiple input and output slots.

- 1) Profinet server supports 1248 Input bytes and 1248 Output bytes.
- 2) Data Size is configurable. Options include: 8, 16, 32, 64, and 128 Bytes.
- 3) Data Format sets the formatting of the data. Automap will use this packing size to map data to/from the other protocol.

There are three ways to configure this protocol:

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

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

Auto-Configure Group by Device ▼

Input Slots (460 to Profinet IO)

Slot	Data Size (Bytes)	Data Format
1	Disabled ▼	16 Bit Int ▼
2	Disabled ▼	16 Bit Int ▼
3	Disabled ▼	16 Bit Int ▼
4	Disabled ▼	16 Bit Int ▼
5	Disabled ▼	16 Bit Int ▼
6	Disabled ▼	16 Bit Int ▼
7	Disabled ▼	16 Bit Int ▼
8	Disabled ▼	16 Bit Int ▼
9	Disabled ▼	16 Bit Int ▼
10	Disabled ▼	16 Bit Int ▼

Output Slots (Profinet IO to 460)

Slot	Data Size (Bytes)	Data Format
11	Disabled ▼	16 Bit Int ▼
12	Disabled ▼	16 Bit Int ▼
13	Disabled ▼	16 Bit Int ▼
14	Disabled ▼	16 Bit Int ▼
15	Disabled ▼	16 Bit Int ▼
16	Disabled ▼	16 Bit Int ▼
17	Disabled ▼	16 Bit Int ▼
18	Disabled ▼	16 Bit Int ▼
19	Disabled ▼	16 Bit Int ▼
20	Disabled ▼	16 Bit Int ▼

Save Parameters

PROFINET IO Server Slot Configuration: Auto-Configure

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

The data will be configured according to the following rules:

- 1) Any 8 Bit Signed/Unsigned data will be mapped as **8 Bit Int or 8 Bit Uint**, matching signs whenever possible.
- 2) Any 16 Bit Signed/Unsigned data will be mapped as **16 Bit Int or 16 Bit Uint**, matching signs whenever possible.
- 3) Any 32 Bit Signed/Unsigned data will be mapped as **32 Bit Int or 32 Bit Uint**, matching signs whenever possible.
- 4) Any 64 Bit Signed/Unsigned data will be mapped as **64 Bit Int or 64 Bit Uint**, matching signs whenever possible.
- 5) Any 32 Bit Float will be mapped as **32 Bit Float**.
- 6) Any 64 Bit Float will be mapped as **64 Bit Float**.
- 7) Any Strings will be mapped as **Short String**.

NOTE: When using a String Data Type, the 1st byte of each slot is reserved for the Length field. The remaining bytes will be used for the actual data.

- 8) Any Coils or 1/8/16/32 Bit Binary Packs will be mapped as **Binary 8 Bit Pack/Binary 16 Bit Pack/Binary 32 Bit Pack**, matching bit sizes whenever possible.
- 9) The input or output direction depends on whether it is configured as an input/read or output/write on the other protocol.
- 10) If the other protocol exceeds the number of data size supported, then nothing will be mapped. You will see all the data size values remain disabled and the main page will display the following error:

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

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

To edit slot data sizes or formats you will need to go into Manual Configure Mode.

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

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

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

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

Group by Device (Default Method)

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

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

Group by Data Type

Group by Data Type goes through the other protocol on the gateway and auto-configures the data groups on the PROFINET server for all the data points within the other protocol.

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

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

Device_1 has 1 integer scan line, 1 float scan line, 1 integer scan line- each for 1 point of data

Device_2 has 1 integer scan line, 1 float scan line, 1 integer scan line- each for 1 point of data

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

Group by Device - Protocol B will have 4 scan lines that will look like the following: Scan Line 1 and 2 will represent Device_1 and Scan Line 3 and 4 will represent Device_2.

Scan Line 1 => Type Integer, length of 2

Scan Line 2 => Type Float, length of 1

Scan Line 3 => Type Integer, length of 2

Scan Line 4 => Type Float, length of 1

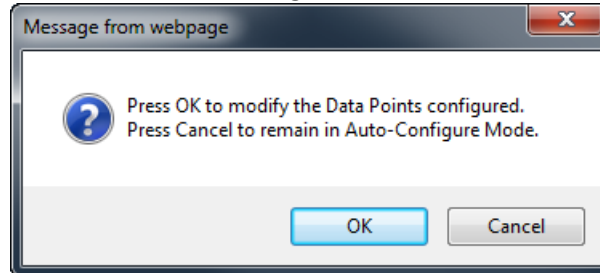
Group by Data Type - Protocol B will have 2 scan lines that will look like the following: All like data types from Device_1 and Device_2 will be combined.

Scan Line 1 => Type Integer, length of 4

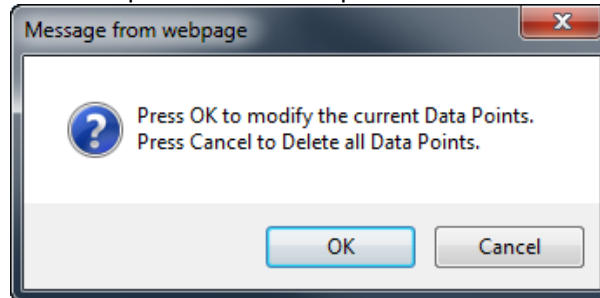
Scan Line 2 => Type Float, length of 2

PROFINET IO Server Slot Configuration: Manual Mode

- 1) To transition from either of the two Auto-Configure Modes to Manual Configure Mode, click the dropdown at the top of the PROFINET IO Server Configuration page and select Manual Configure.
- 2) When prompted, click **OK** to confirm mode change or **Cancel** to remain in Auto-Configure Mode.



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



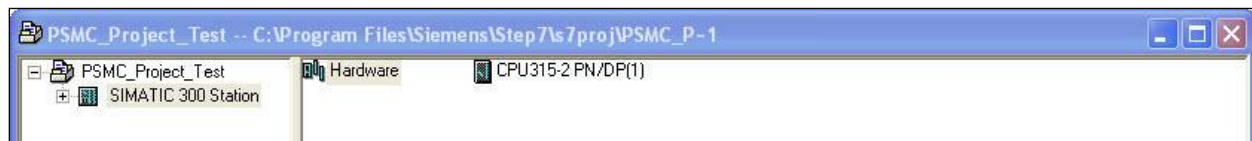
- 4) To keep the data slots that are already configured, press **OK**.
 - i) You would want this option if you are adding additional data slots or you want to modify the data slot(s) that already exist.
- 5) To delete the data slots that are already there and start over, press **Cancel**.
- 6) Input Slots: Select the data size, in bytes, to move data from the gateway to the controller. Then select the data format for that slot.
- 7) Output Slots: Select the data size, in bytes, to move data from the controller to the gateway. Then select the data format for that slot.

Setting up the PLC- Example Using Simatic Classic Step 7

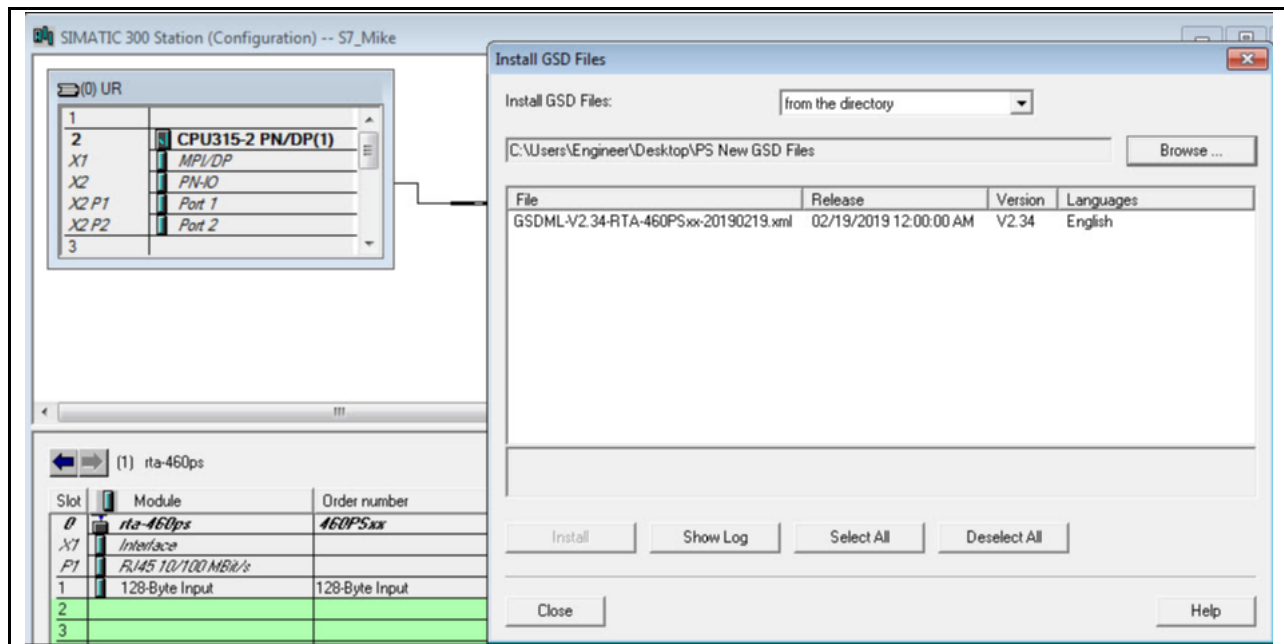
This is how you would set up the following example in your controller.

Input Slots (460PSMC to Profinet IO)			Output Slots (Profinet IO to 460PSMC)		
Slot	Data Size (Bytes)	Data Format	Slot	Data Size (Bytes)	Data Format
1	128	8 Bit Int	11	128	8 Bit Int

- 1) In your project, click the CPU and you should see the hardware option in the right pane. Double click on the Hardware icon.



- 2) IF YOU HAVE ALREADY INSTALLED THE GSD FILE, SKIP TO STEP 9.
OTHERWISE - Under Options, select **Install GSD Files**.



- 3) On the PROFINET IO Server configuration page, download the zip file

[GSDML and Graphic Files](#)
[GSDML-V2.35-RTA-460PS-20190930.zip](#)

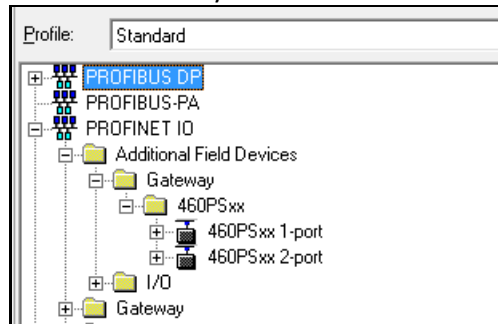
- 4) Browse to folder containing the GSD file.
- 5) Select the GSD file from the box and click **Install**.
- 6) When prompted to confirm installation because it cannot be undone, click **Yes**.



7) Click **OK** acknowledging that the install was successful.

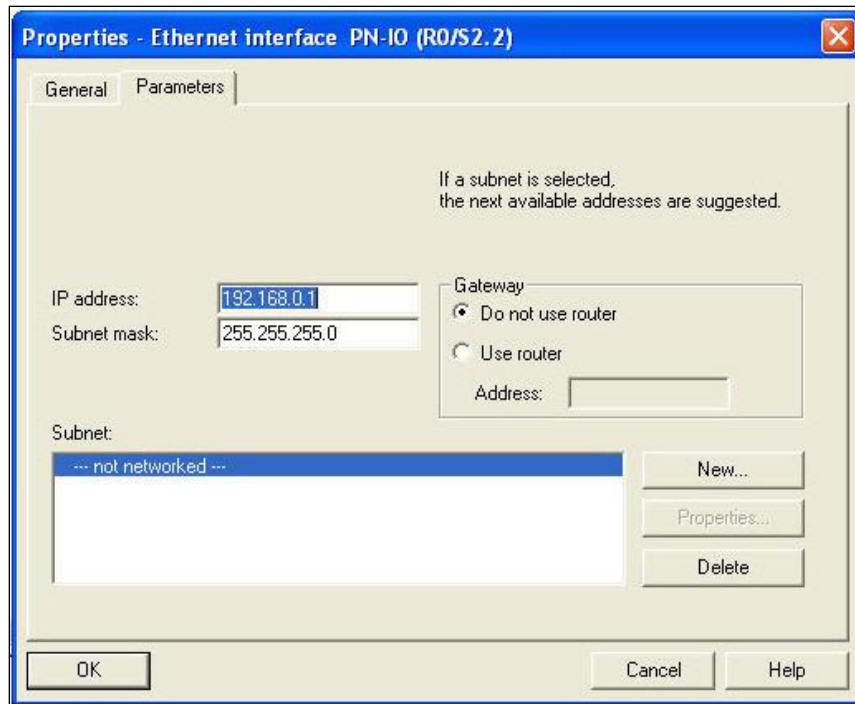


8) If you navigate to the right-hand side, you will see the RTA profile under: PROFINET IO->Additional Field Devices->Gateway->460PSxx

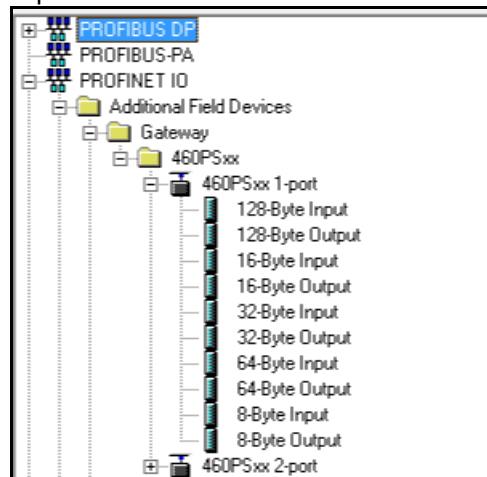


9) IF YOU HAVE ALREADY CONFIGURED THE PROFINET I/O CONTROLLER, SKIP TO STEP 11. OTHERWISE - Right-click on the PN-IO block and select **Insert PROFINET IO System**.

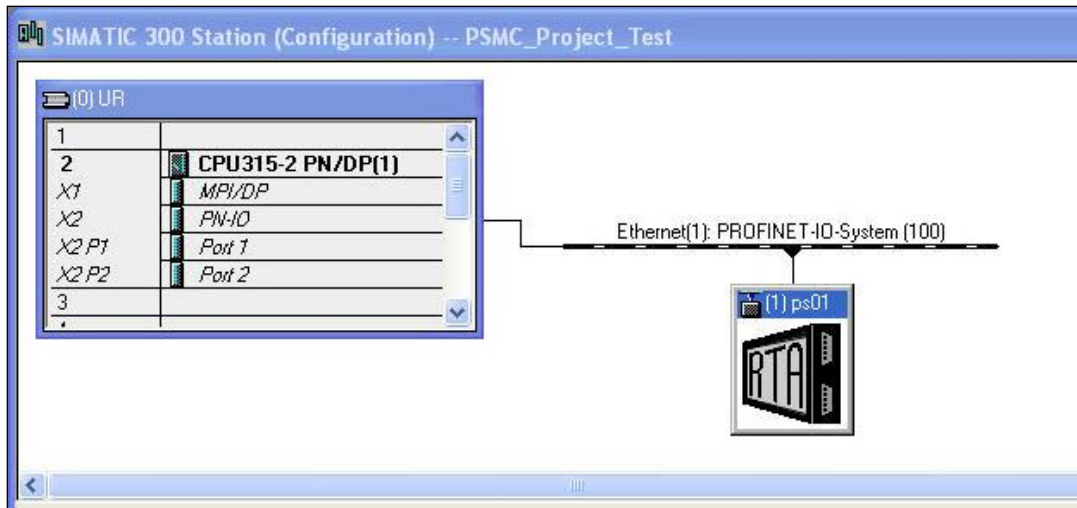
10) In the properties window, set the IP Address to match that of the PROFINET I/O controller and press **New** and **OK**.



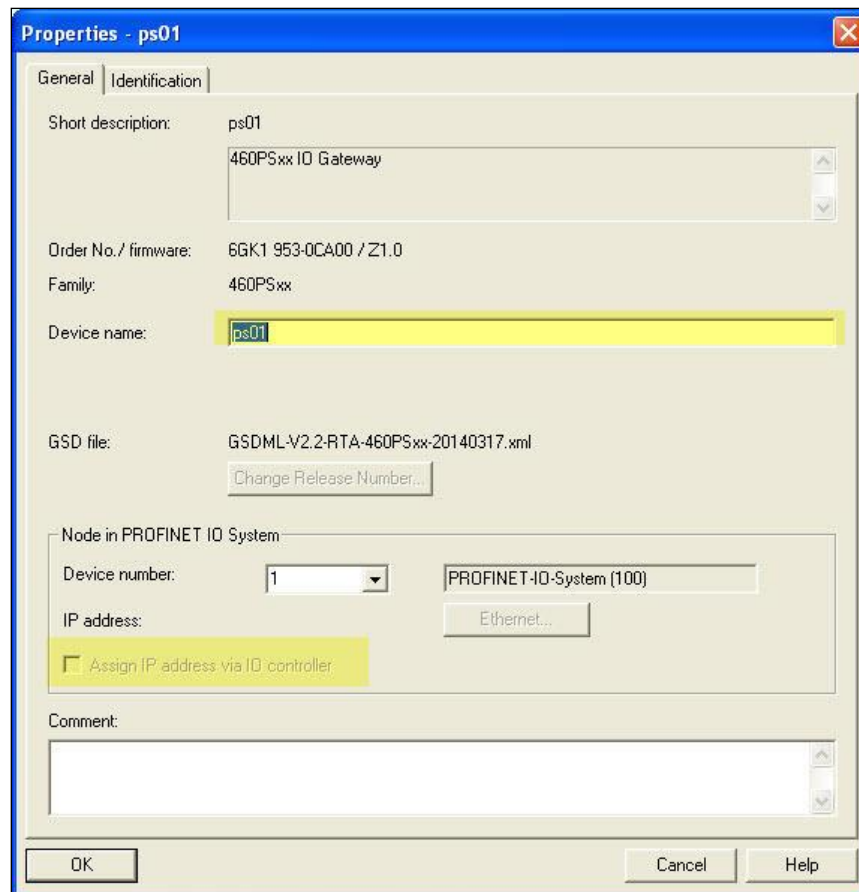
- 11) Find the RTA device in the I/O tree. It will be under PROFINET IO->Additional Field Devices->Gateway->460PSxx->460PSxx 1-port.



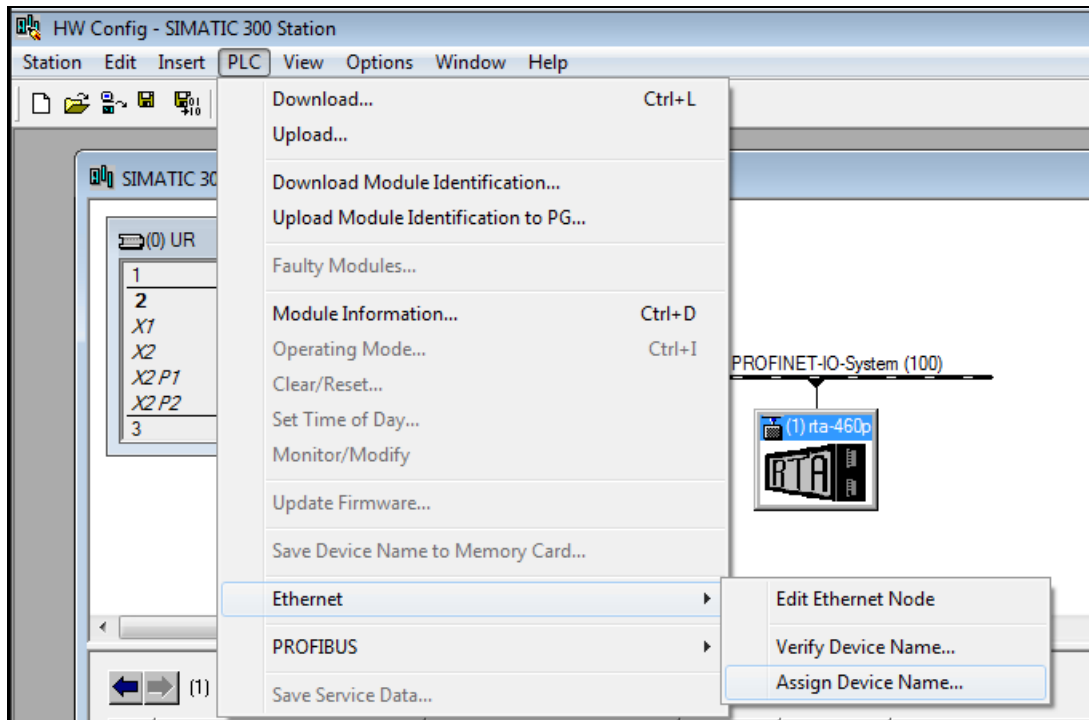
- 12) Once found, drag the Standard icon into the network line.



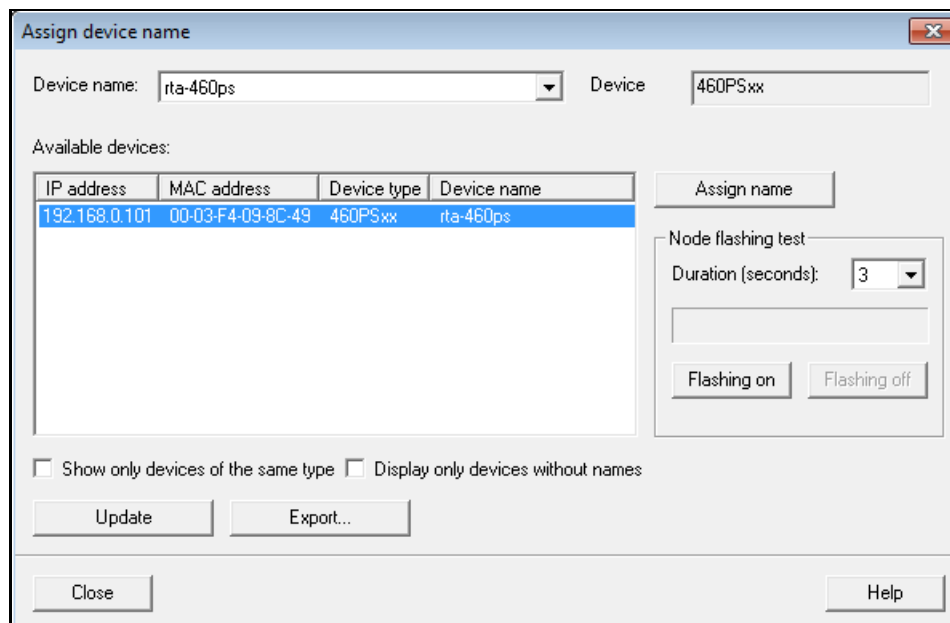
- 13) Double-click the gateway icon to open the properties window. If not already done, uncheck the **Assign IP Address via IO controller option** (some versions already do this) and press **OK**.



- 14) To Assign the RTA gateway a Device Name click on the RTA device, click on the *PLC* tab, select *Ethernet*, then *Assign Device Name*.



- 15) Click the **Assign name** button to give the RTA gateway a name. This name will appear on the RTA PROFINET configuration page. If you would like to assign your own name simple right click on the RTA device and select the objects properties.



16) Expand the Standard node on the right panel to show the available modules to insert (Refer to the picture in Step 11).

Input Slots (460PSMC to Profinet IO)			Output Slots (Profinet IO to 460PSMC)		
Slot	Data Size (Bytes)	Data Format	Slot	Data Size (Bytes)	Data Format
1	128	8 Bit Int	11	128	8 Bit Int

To match the above configuration in the 460 gateway, add one 128-byte input module to slot 1, and one 128-byte output module to slot 11.

Siemens PLC Configuration:

Slot	Module	Order number	I address	Q address	Diagnostic address:	Comment
0	ps01	6ES7 195-0CA0			2042*	
X7	Interface				2041*	
F1	PS 145 10/100				2040*	
1	128 bytes I		0...127			
2						
3						
4						
5						
6						
7						
8						
9						
10						
11	128 bytes Q			0...127		
12						
13						

17) When finished, click the **Save and Compile** button and then the **Download to PLC** button.



NOTE: When using a Short String Data Type, the 1st byte of each slot is reserved for the Length field. The remaining bytes will be used for the actual data.

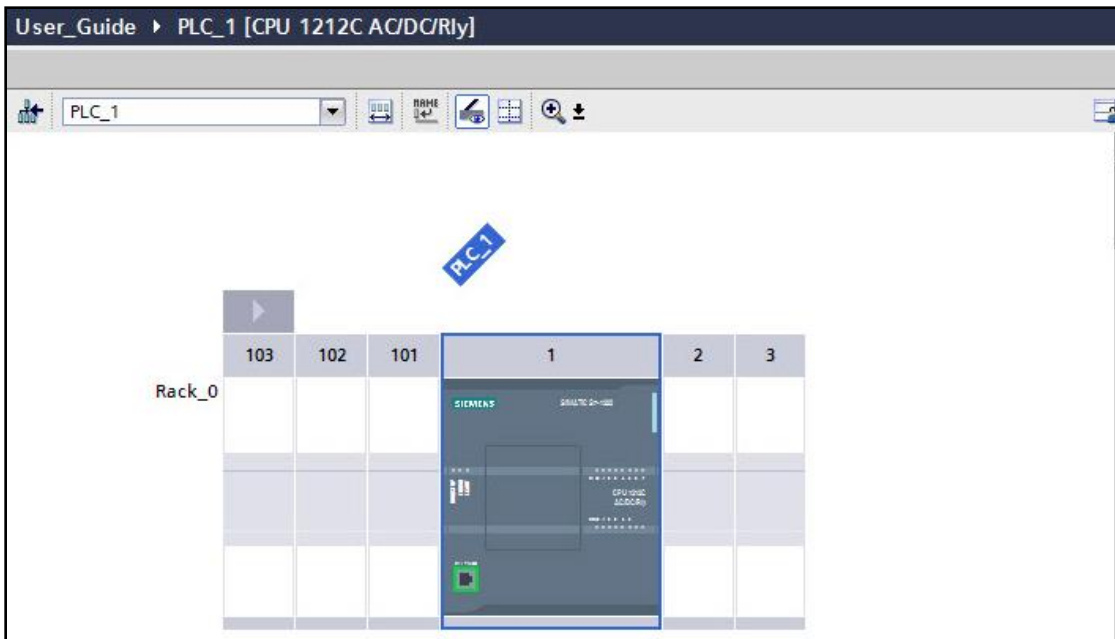
Terminology Note and Example: I addresses refer to input, Q addresses refer to output, %B refers to bytes and %W refers to words. So in this case, %IB0 would be used to represent how many bytes to read starting from %IB1 up to %IB127. Likewise, %QB0 would be used to represent how many bytes of information to write starting from %QB1 up to %QB127.

Setting up the PLC- Example Using TIA Portal

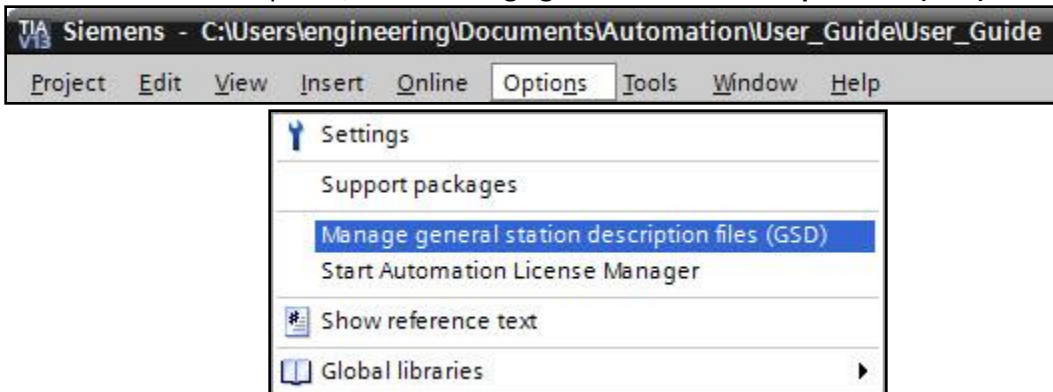
This is how you would set up the following example in your controller.

Input Slots (460PSMC to Profinet IO)			Output Slots (Profinet IO to 460PSMC)		
Slot	Data Size (Bytes)	Data Format	Slot	Data Size (Bytes)	Data Format
1	8	16 Bit Uint	11	32	32 Bit Int
2	128	32 Bit Uint	12	Disabled	16 Bit Int

- 1) In your project, click the Device View tab and select your PLC.



- 2) IF YOU HAVE ALREADY INSTALLED THE GSD FILE, SKIP TO STEP 9. OTHERWISE - Under Options, select **Manage general station description file (GSD)**.

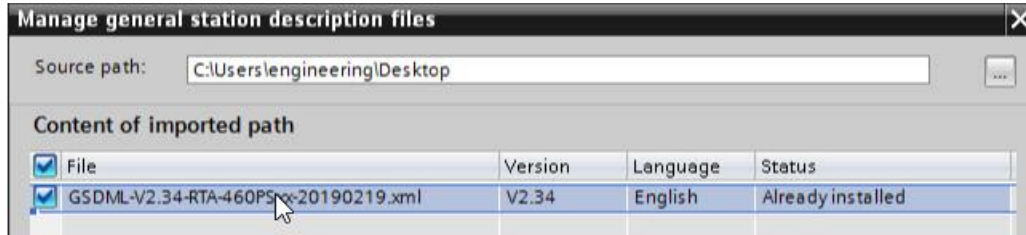


- 3) On the RTA PROFINET IO Server configuration page, download the zip file

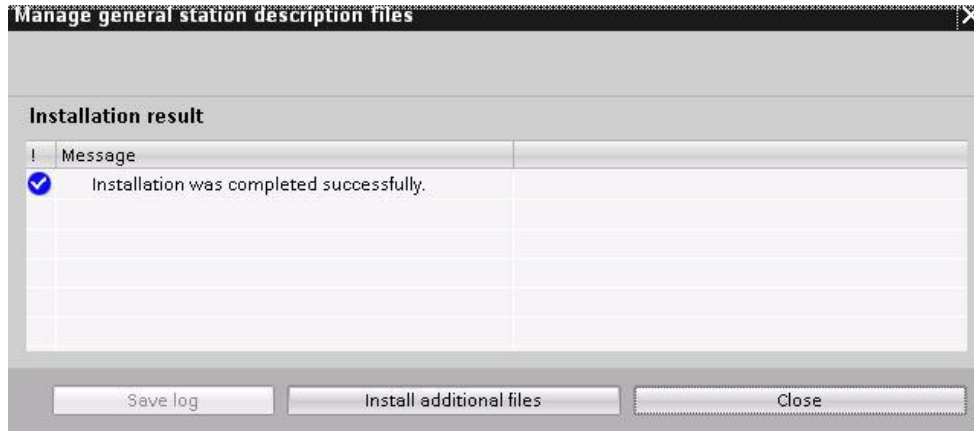
GSDML and Graphic Files

[GSDML-V2.35-RTA-460PS-20190930.zip](#)

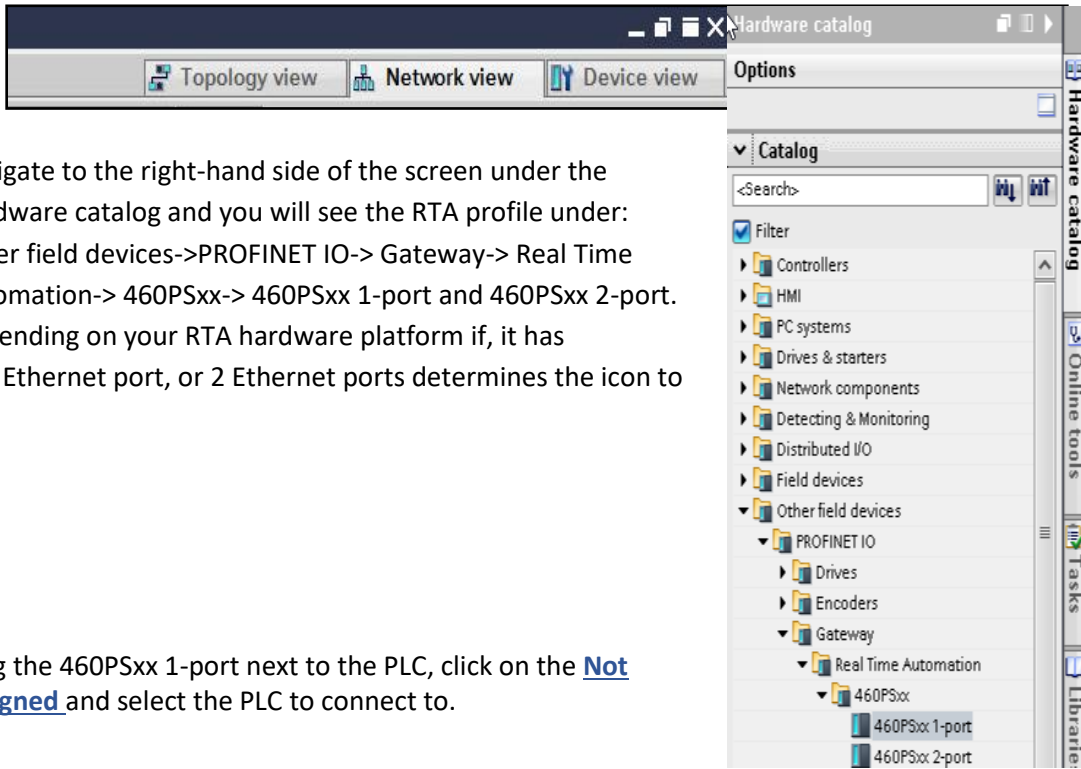
- 4) Browse to folder containing the GSD file.
- 5) Check the box to the left of the imported path and click **Install**.



- 6) Click **Close** when it was installed successfully.



7) Click the Network View tab in your project.



8) Navigate to the right-hand side of the screen under the Hardware catalog and you will see the RTA profile under: Other field devices->PROFINET IO-> Gateway-> Real Time Automation-> 460PSxx-> 460PSxx 1-port and 460PSxx 2-port. Depending on your RTA hardware platform if, it has one Ethernet port, or 2 Ethernet ports determines the icon to use.

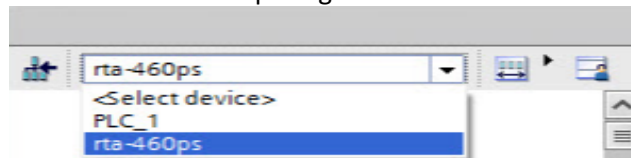
9) Drag the 460PSxx 1-port next to the PLC, click on the [Not Assigned](#) and select the PLC to connect to.



10) Once the RTA device is in the network click the Device view tab.



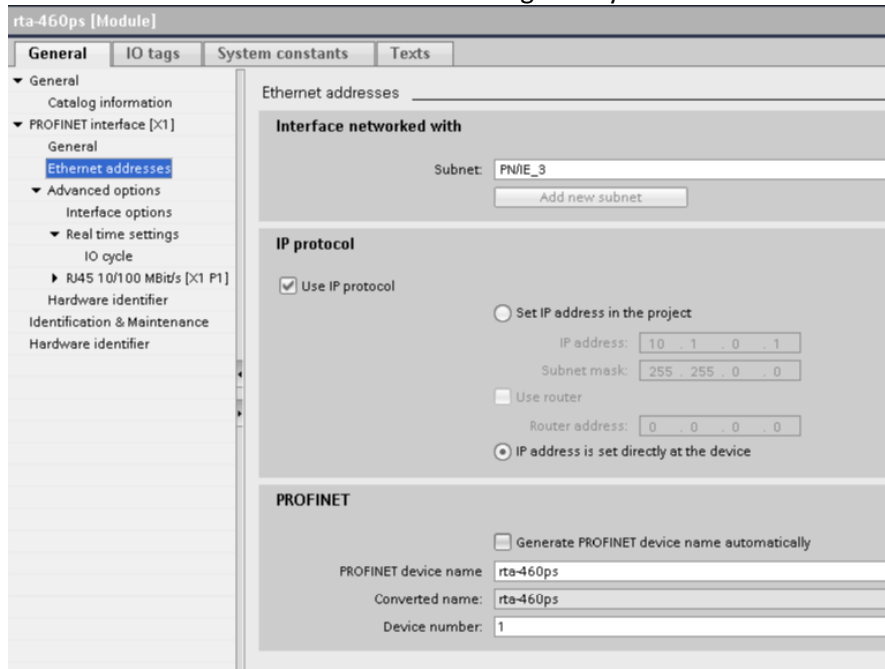
11) From the dropdown menu select rta-460ps. Right click on the RTA device to select Properties.



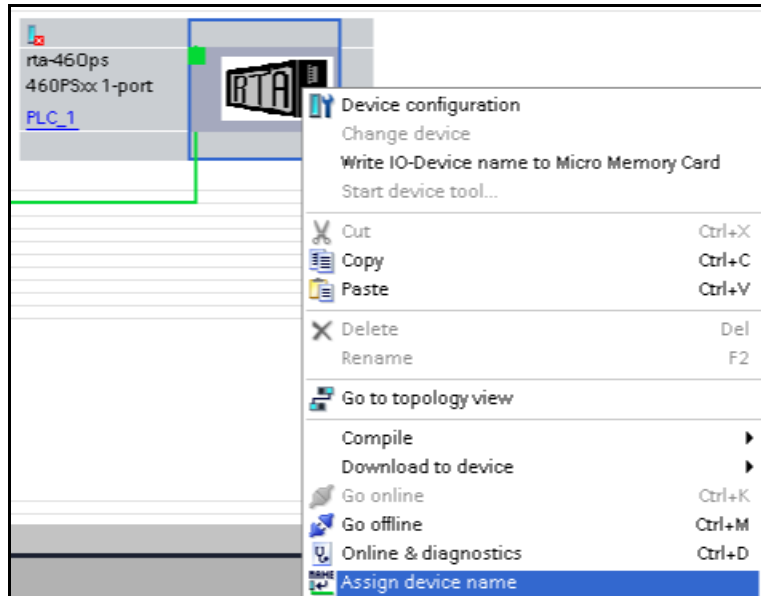
12) Go down to the Ethernet addresses.

13) Be sure that the "IP address is set directly at the device" option is selected and **uncheck** the "Generate PROFINET device name automatically."

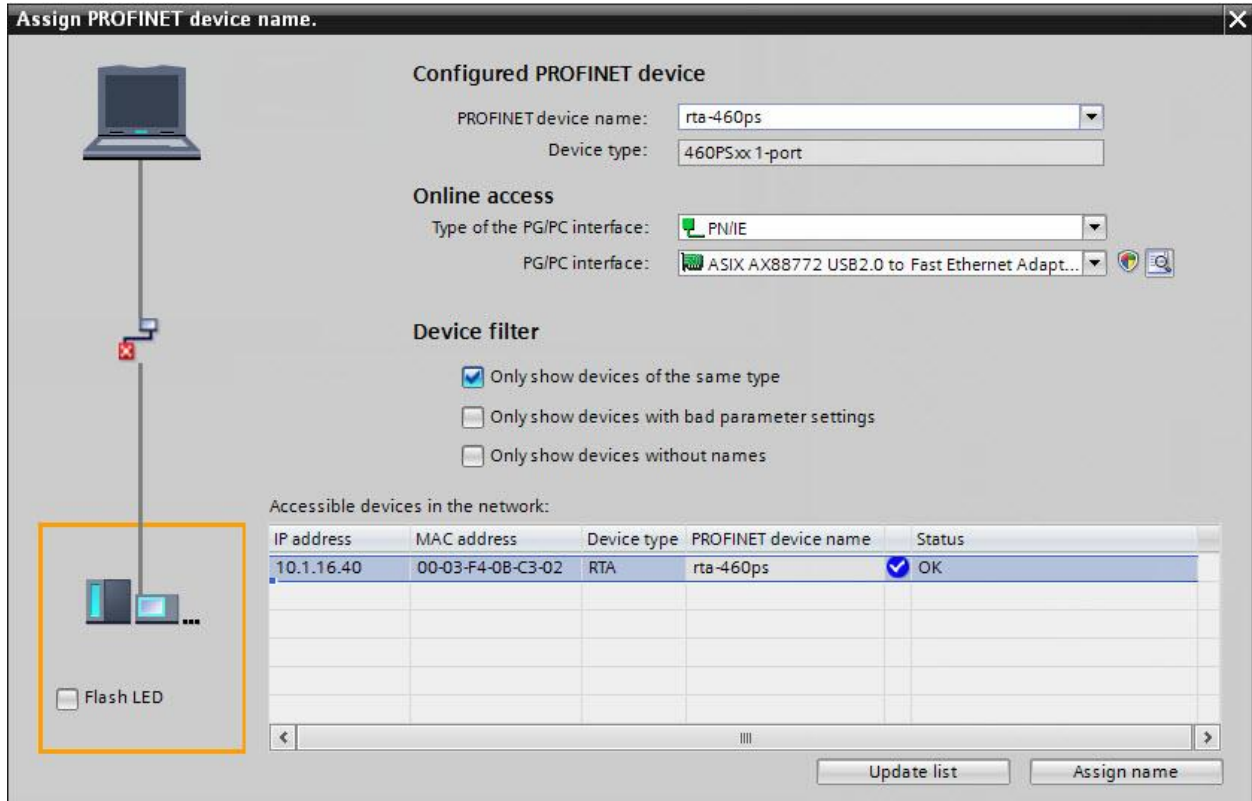
- a. *The **PROFINET Device Name** field is the name to assign to the RTA gateway
- b. *Make sure the PROFINET device and the gateway are on the same network.



14) Right click on the RTA device and select the Assign device name.



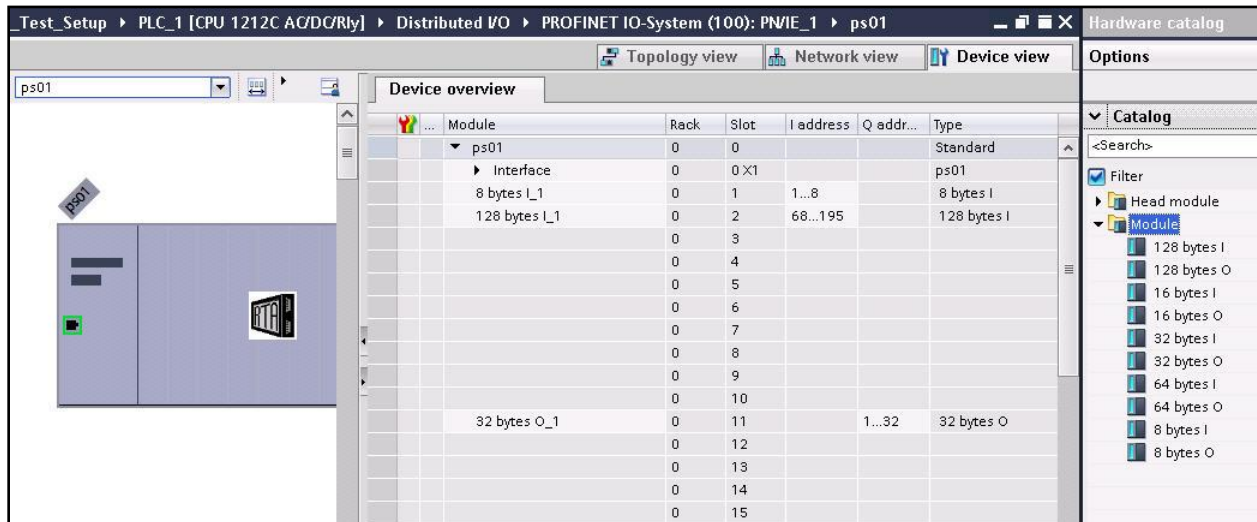
15) Select the RTA device and click the **Assign name** button to give the RTA a valid name on the network. Once the RTA gateway is in run mode this name will appear on the PROFINET web page.



16) To match the above configuration in the 460 gateway, add one 8-byte input module to slot 1, one 128-byte input module to slot 2, and one 32-byte output module to slot 11.

Input Slots (460PSMC to Profinet IO)			Output Slots (Profinet IO to 460PSMC)		
Slot	Data Size (Bytes)	Data Format	Slot	Data Size (Bytes)	Data Format
1	8	16 Bit Uint	11	32	32 Bit Int
2	128	32 Bit Uint	12	Disabled	16 Bit Int

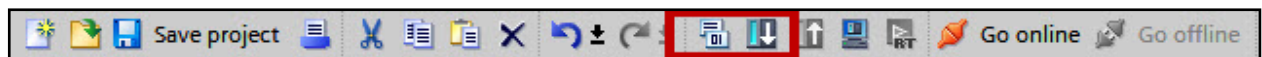
17) Expand the Module list under the catalog on the right panel to show the available modules to insert into the device overview slots.



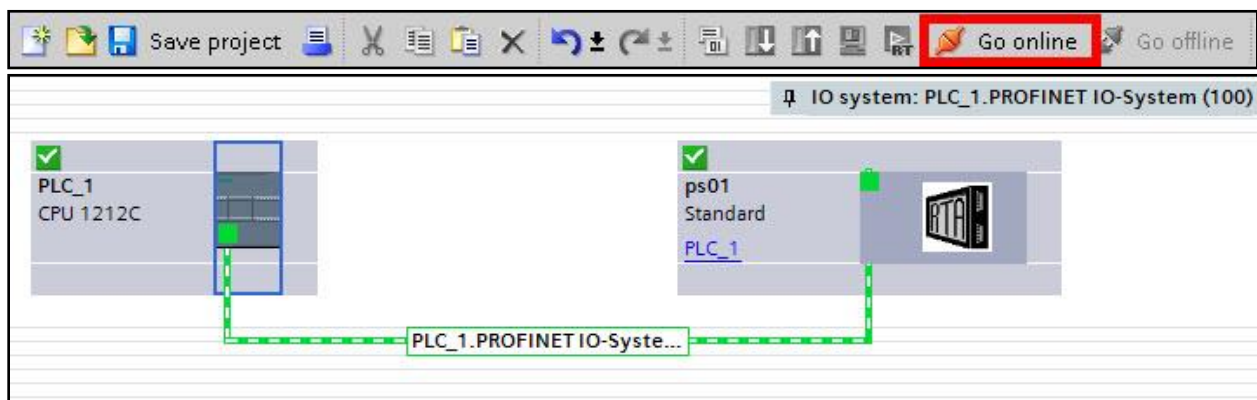
To insert a module, double click to add it to the next available slot.

Terminology Note and Example: I addresses refer to input, Q addresses refer to output, %B refers to bytes and %W refers to words. So in this case, you would use %IB1-8, %IB68-195 and %QB1-32 to access the data to/from the gateway in the PLC.

18) the Network view tab, click the port of PLC, click the Compile button and Download to Device button (in red).



19) Once everything is downloaded to the PLC there will be a green check box on both devices, then click **Go Online** (see red box).



NOTE: When using a Short String Data Type, the 1st byte of each slot is reserved for the Length field. The remaining bytes will be used for the actual data.

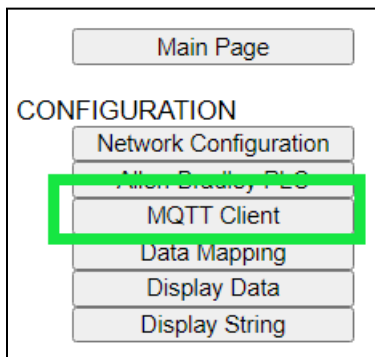
MQTT Client Configuration

You can configure up to three MQTT connections.

1. Configure up to three MQTT broker devices.
2. Configure up to one Amazon Web Services (AWS) IoT Core connection.
3. Configure up to one Microsoft Azure connection.

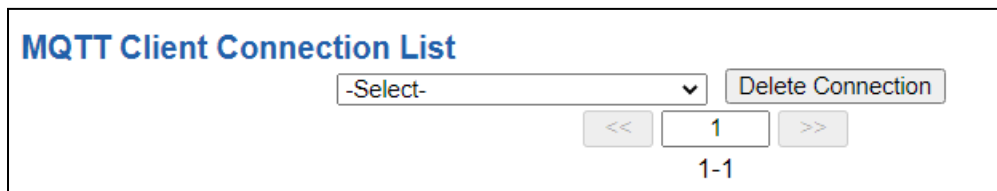
NOTE: A single AWS OR Azure connection is supported and can co-exist with up to two additional MQTT broker devices.

Click the **MQTT** button to continue configuration.

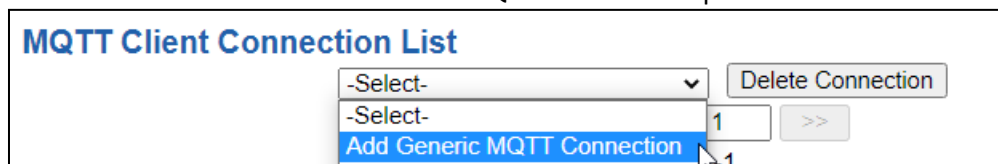


MQTT Devices Configuration

You can configure up to three MQTT devices.



- 1) To add an MQTT device, or additional MQTT devices, click the -Select- dropdown menu under MQTT Client Connection List and select **Add Generic MQTT Connection** option.



- a) To remove a device, navigate to the MQTT device and click the **Delete Connection** button.
 - b) To create a new MQTT device with the same parameters already configured from another MQTT device, click the -Select- dropdown menu and select the **Add from MQTT X** option (where X represents the MQTT device you wish to copy parameters from).
 - c) Once created, you can make any additional changes needed to that new MQTT device.
- 2) The **Enable** check box should be selected for the device to enable communications.
 - 3) Enter in a **Device Label** to identify the device in the gateways.

- 4) Select which **Network Interface** to use for MQTT device connection. Option only available on the N2E hardware platform.
- 5) Enter the unique MQTT **broker IP address**, if this value does not match, the gateway will timeout.
- 6) Enter **TCP Port** for the MQTT broker to open a connection on. If this value doesn't match, the gateway will not open a connection.
- 7) **Keep Alive**: Enter in the amount of time that the gateway should attempt to ping the broker to keep the MQTT connection alive, 0 disables this feature.
- 8) Enter a **Client ID** which is concatenated onto the Published messages (RTA Publish Topic) to the broker. **Ex:** If your Client ID is "RTA GW" and one of your topics is RM101/Lights, your RTA gateway will publish the message as RTA GW/RM101/Lights.
- 9) **Username and Password**: Enter if authentication to the MQTT broker is necessary.

<input type="checkbox"/> Enable	MQTT 1	
Device Label	QT03	Network Interface
Broker IP Address	0.0.0.0	TCP Port
Keep Alive	60	Client ID
Username		Password

Configuring Subscribe and Publish Topics

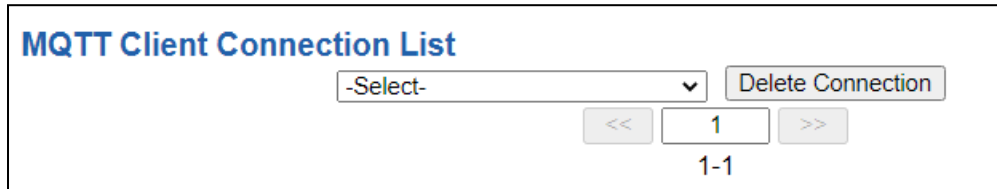
- 10) Enter in "**# of Subscribe Topics**" and/or "**# of Publish Topics**".
 - a) **NOTE: Only 1000 subscribe and a 1000 publish topics are shared between the 3 connections.**
- 11) Click **Generate Topics** button to have the lines generated for you. The Topic Name has a character limit of 64 characters and can support root level Topic Names. **Ex:** Line #1: RM101/Light, Line #2: RM102/Light, Line #3: RM103/Light....
- 12) **Subscribe Topics**: Enter in the number of topics to subscribe from the broker. Once the topics are subscribed to, the MQTT broker will publish the messages to the gateway.
- 13) **Publish Topics**: Enter the number of topics to publish to the broker from the mating protocol.
- 14) Select the **Point Type** of the topic
- 15) Click **Save Parameters** button when complete.

# of Subscribe Topics	3	0-1000	# of Publish Topics	3	0-1000
Generate Topics					
View Subscribe Topics			View Publish Topics		
Publish Topics (460ETCQT to MQTT)					
Line #	Enable	Topic Name	Point Type		
1	<input checked="" type="checkbox"/>		INT (8-bit)	▼	
2	<input checked="" type="checkbox"/>		INT (8-bit)	▼	
3	<input checked="" type="checkbox"/>		INT (8-bit)	▼	
<< 1-3 >>					

Amazon Web Services (AWS) Configuration

You can only configure one AWS IoT Core connection with your RTA product.

- 1) To add an AWS connection, click the **-Select-** dropdown menu under MQTT Client Connection List and select **Add Generic AWS Connection** option.
 - a. To remove a device, navigate to the AWS device to delete and click the **Delete Connection** button.

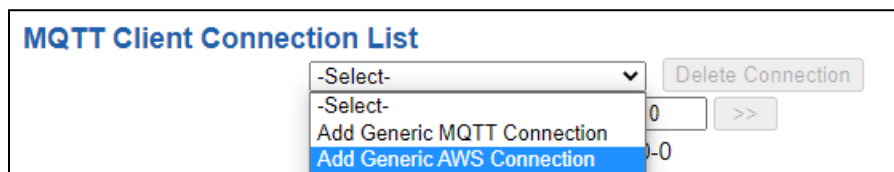


MQTT Client Connection List

-Select- [v] Delete Connection

<< 1 >>

1-1



MQTT Client Connection List

-Select- [v] Delete Connection

-Select- 0 >>

Add Generic MQTT Connection 0

Add Generic AWS Connection 0-0

- 2) The **Enable** check box should be selected for the device.
- 3) Enter in a **Device Label** to identify the device within the gateways mapping.
- 4) Select which **Network Interface** to use for AWS IoT Core connection. Option only available on the N2E hardware.
- 5) **Device Shadow URL:** Enter in the URL path for the AWS MQTT broker.
 - a. AWS IoT console will provide you a device shadow URL such as: https://aabb11224e9ex-ats.iot.us-east-2.amazonaws.com/things/RTA_Testing/shadow?name=RTA_Ninja
 - b. Within the RTA gateway configuration only enter in “aabb11224e9ex-ats.iot.us-east-2.amazonaws.com” portion of the URL, everything else is ignored.
- 6) Enter the **TCP Port** for the MQTT broker to open a connection on. If this value doesn’t match, the gateway will not open a connection.
- 7) **Keep Alive:** Enter in the amount of time that the gateway should attempt to ping the broker to keep the MQTT connection alive, 0 disables this feature.
- 8) Enter a **Client ID** which is concatenating onto the Published messages (RTA Write Topic) to the broker. **Ex:** If your Client ID is RTA GW and one of your topics is RM101/Lights, your RTA gateway will publish the message as RTA GW/RM101/Lights.

<input type="checkbox"/> Enable	AWS 1	
Device Label	QT01	Network Interface Ethernet Port 1 (10.1.16.22) [v]
Device Shadow URL		
TCP Port	8883	1-65535 (Default: 8883)
Keep Alive	60	0-200 sec (0 to Disable)
Client ID		

Additional AWS Requirements

There are three items that are required to establish an AWS IoT Core connection.

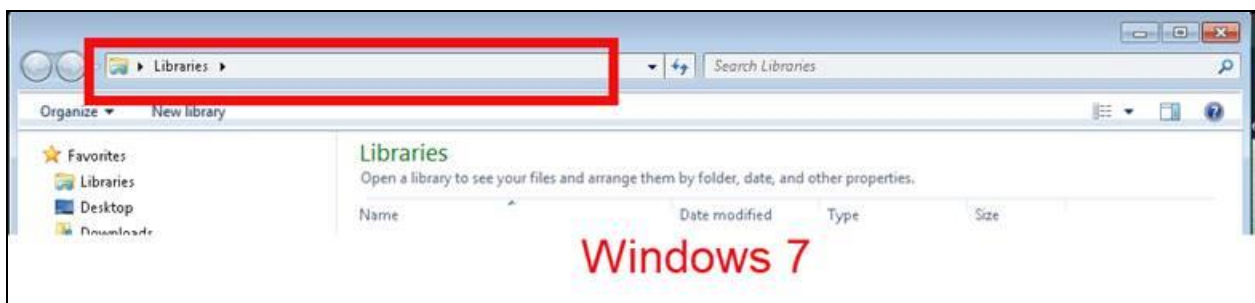
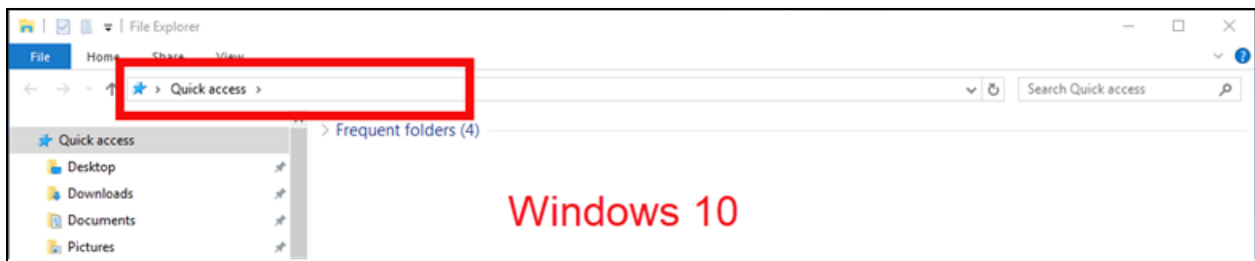
- 1) The Device Shadow URL
- 2) Within AWS create a certificate for your RTA gateway. Once AWS has generated a certificate, you'll be given a private key and certificate to download.
- 3) Both private key and certificate will need to be FTP'd into the RTA gateway's Flash File System.

How to FTP files into the RTA gateway

- 1) Save off the private key and certificate files to your desktop, keep these files in a secured location.
- 2) Within your Windows Task bar, right click and open a new Windows/File Explorer folder or go into your start menu and type File Explore.

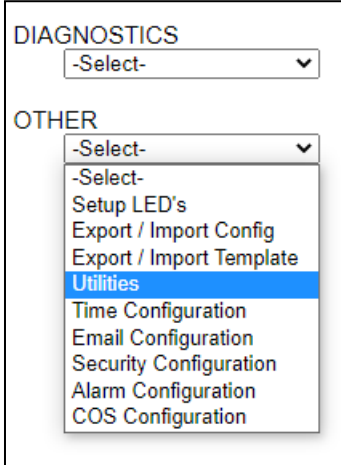


- 3) You should now have a window that looks like the image below.



- 4) In the address bar (within the red box shown above) type <ftp://xxx.xxx.xxx.xxx> (IP Address of RTA gateway).
 - a. You will then see a pop-up window, Username: **ffs** Password: **rtarocks**

- b. Paste the certificate and private key into this ftp session, close out the session by exiting out.
- 5) Navigate to the RTA gateway and on the left-hand side, click the OTHER -Select- dropdown and select Utilities.



- 6) Once on the Utilities page click the File List button.



- 7) Verify that your certification and private key files appear on this page.

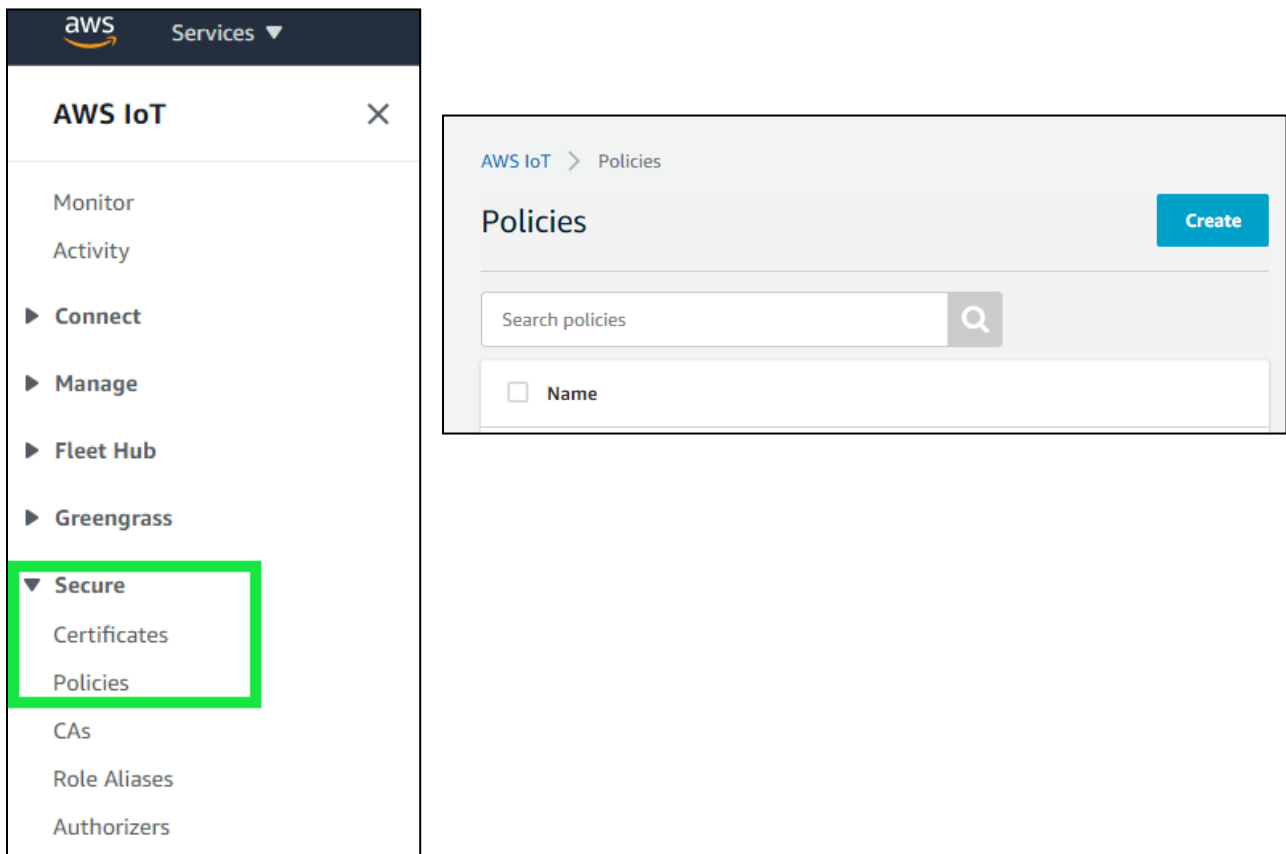
File Name	File Size (Bytes)
rtax_cfg.rta	291368
e8a739db31280821ca4a4912c-private.pem.key	1679
eips_460_nv_settings.eip_nv	10
e8a739db31280821ca4a4912c-certificate.pem.crt	1220
Total	294277 bytes

AWS IoT Core Service Setup

Within your AWS account you'll need to navigate to the IoT Core service page where you'll setup a "Thing" and "Policies".

Before you can register your RTA gateway as a "thing," we need to setup a "policy" for it. This policy will be assigned to our "thing" during the registration process and will grant it the permissions needed to access the MQTT topics that we will use to publish and subscribe messages. From the left-hand menu, select "Secure", and then the submenu of "Policies".

Click the button "Create".



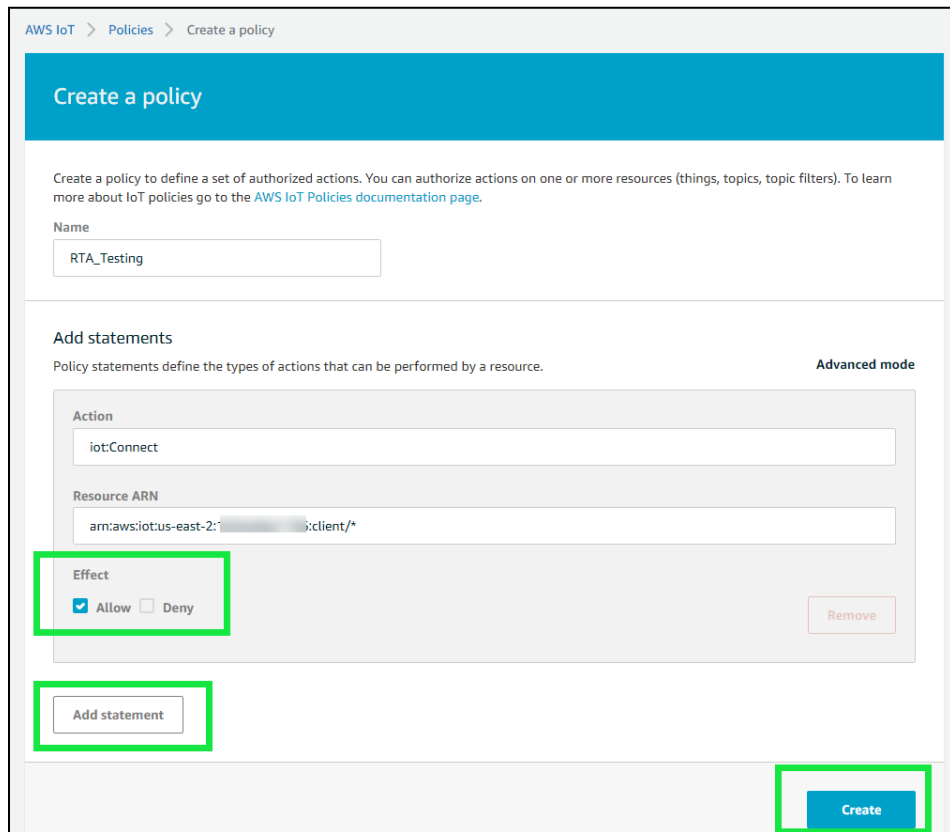
From the policy creation page, you add the statements that will dictate what connected devices are allowed to do. Assign a unique name to your policy and add four statements with the information listed below. Notice that when you type in the action, the field labeled “Resource ARN” will be automatically populated.

Check “Allow” under the “Effect” field and replace the last portion of each Resource ARN that reads, “replaceWithA”, with an asterisk (*). When finished, you should have the following statements:

Action	Resource ARN
iot : Connect	arn:aws:iot:(your region):(your account #):client/*
iot : Publish	arn:aws:iot:(your region):(your account #):topic/*
iot : Receive	arn:aws:iot:(your region):(your account #):topic/*
iot : Subscribe	arn:aws:iot:(your region):(your account #):topicfilter/*

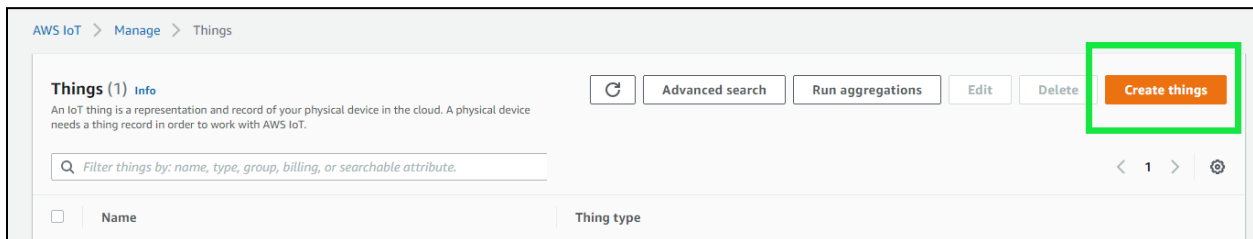
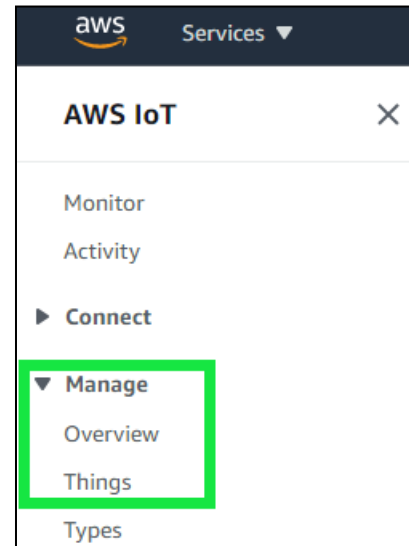
Click the **Add statement** button to create the Publish, Receive and Subscribe statements. Once completed click the **Create** button. Please note that in a production environment, you will want to be **more** selective with your policy creation (e.g., don’t use an asterisk at the end of a Resource ARN).

When they have been entered, click “Create”. Now it’s time to register our “thing”.



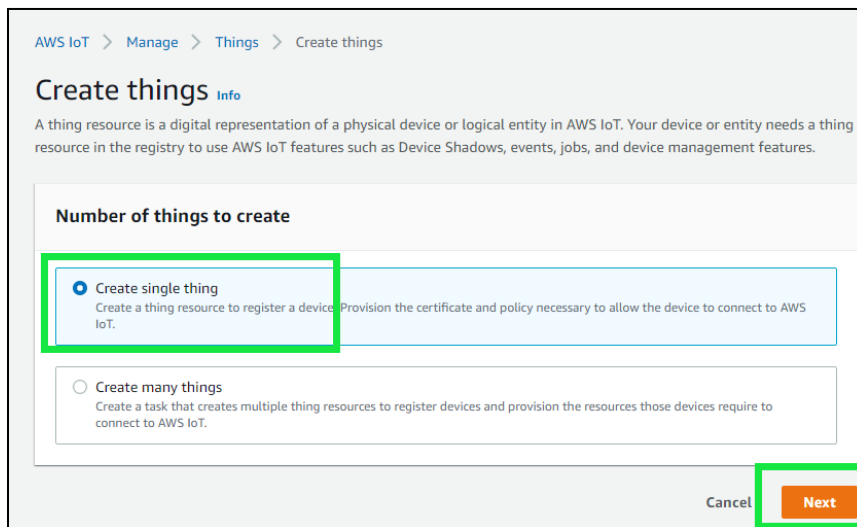
AWS IoT Core Service Things Configuration

Back at the main menu on the left pane, click on the “Manage” menu option, and then the “Things” submenu.

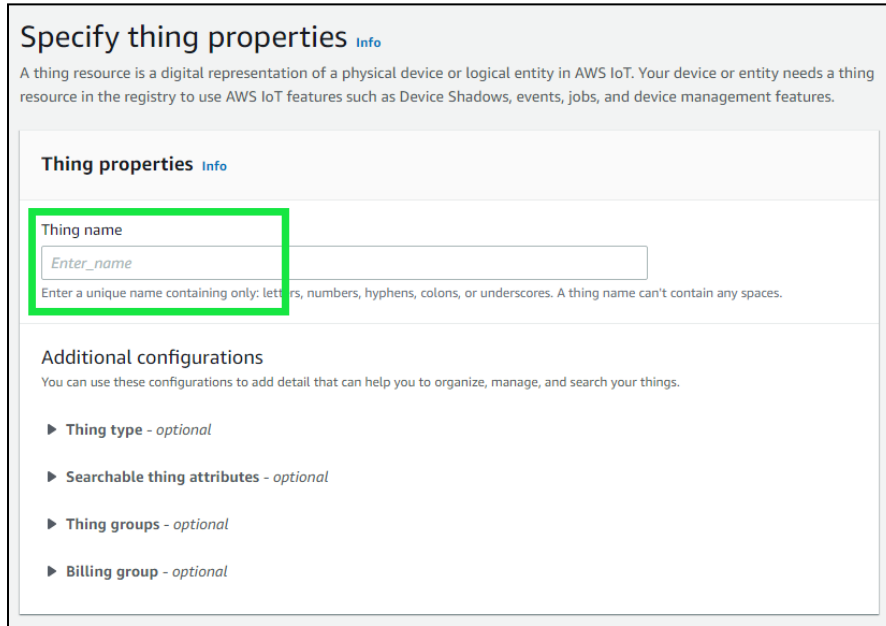


This will take us to a window that allows you to register a single “thing,” or multiple “things.” Click on the button labeled, “Create things.”

A new window will open with a number of things to create, chose “Create single thing” and click the Next button. If you have multiple RTA gateways, then you’ll need to select “Create many things”.



The next setting will be the “Specify thing properties”, here you will give your “Thing” a unique name and click the Next button at the bottom.



Specify thing properties [Info](#)

A thing resource is a digital representation of a physical device or logical entity in AWS IoT. Your device or entity needs a thing resource in the registry to use AWS IoT features such as Device Shadows, events, jobs, and device management features.

Thing properties [Info](#)

Thing name

Enter a unique name containing only: letters, numbers, hyphens, colons, or underscores. A thing name can't contain any spaces.

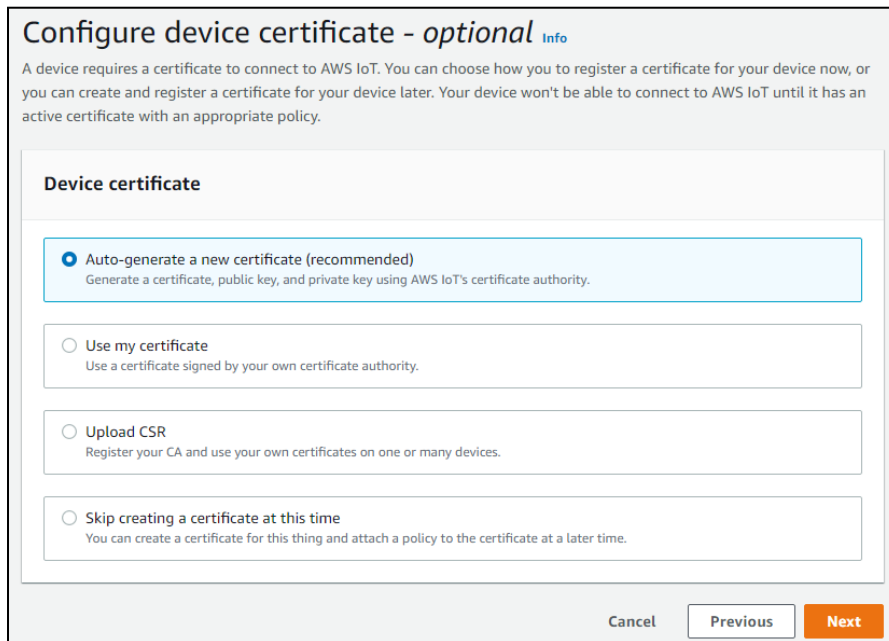
Additional configurations

You can use these configurations to add detail that can help you to organize, manage, and search your things.

- ▶ **Thing type** - optional
- ▶ **Searchable thing attributes** - optional
- ▶ **Thing groups** - optional
- ▶ **Billing group** - optional

Certificate setup

Here you associate your “Thing” with the certificate that will be used to authenticate it with the AWS IoT Core service. Auto-generate is fine, click the Next button.



Configure device certificate - optional [Info](#)

A device requires a certificate to connect to AWS IoT. You can choose how you to register a certificate for your device now, or you can create and register a certificate for your device later. Your device won't be able to connect to AWS IoT until it has an active certificate with an appropriate policy.

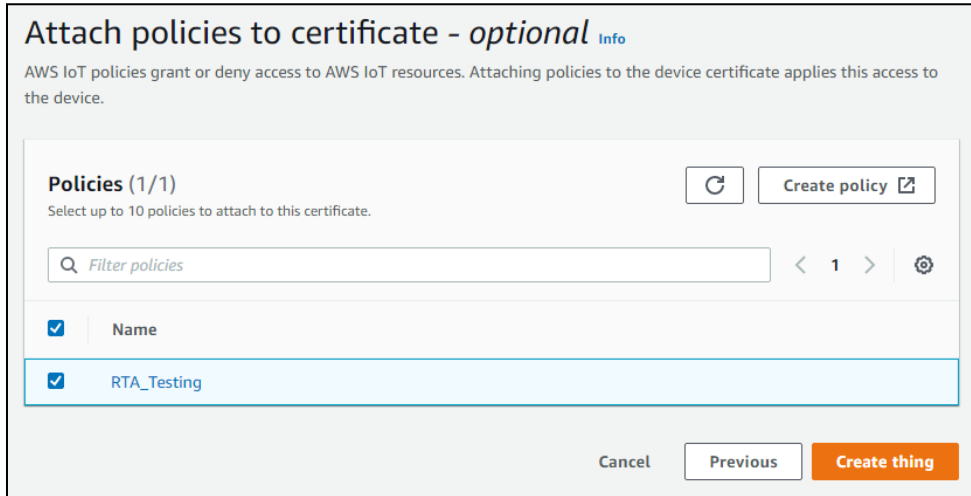
Device certificate

- Auto-generate a new certificate (recommended)**
Generate a certificate, public key, and private key using AWS IoT's certificate authority.
- Use my certificate**
Use a certificate signed by your own certificate authority.
- Upload CSR**
Register your CA and use your own certificates on one or many devices.
- Skip creating a certificate at this time**
You can create a certificate for this thing and attach a policy to the certificate at a later time.

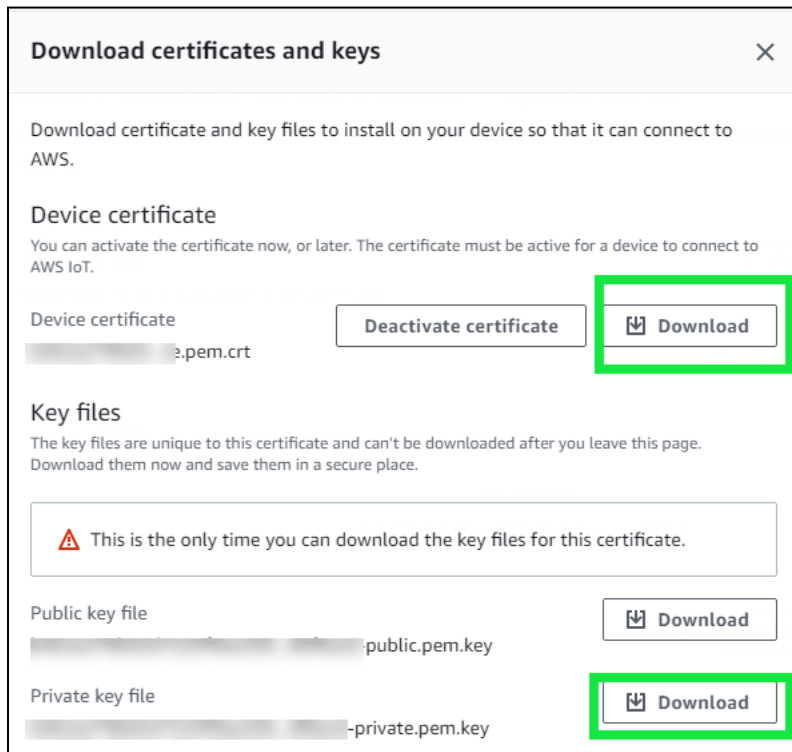
Cancel Previous **Next**

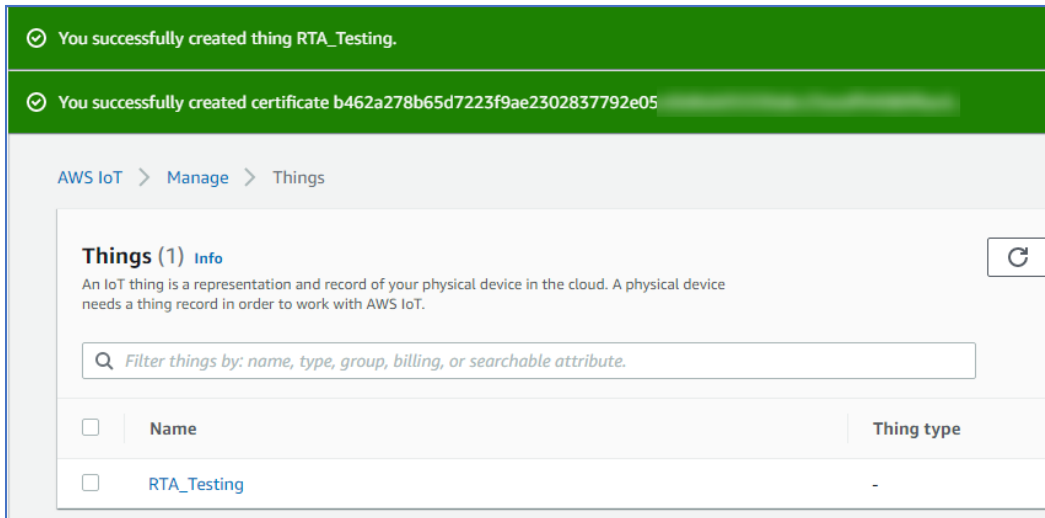
Attach policies to certificate

Next you'll see the policy you created previously, select the policy and click "Create thing" a pop up will appear to "Download certificates and keys".

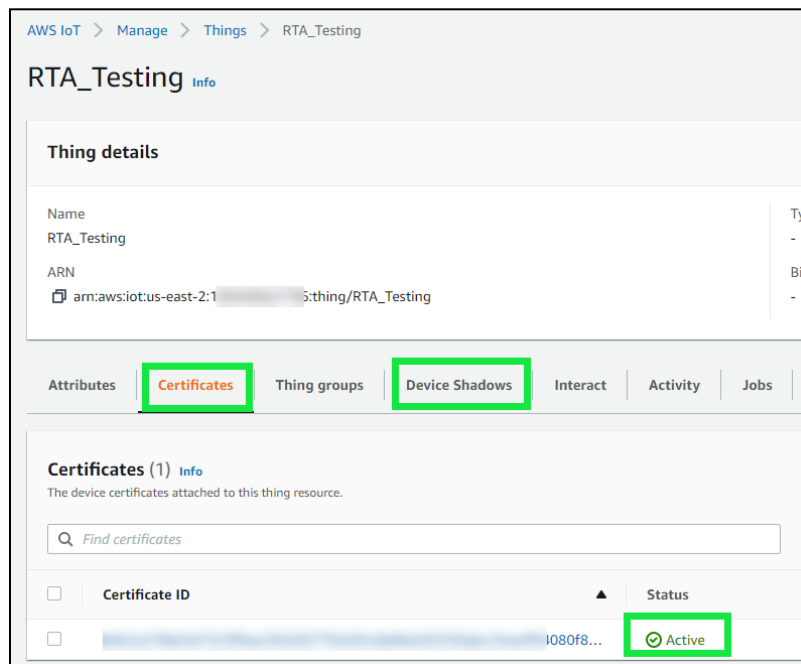


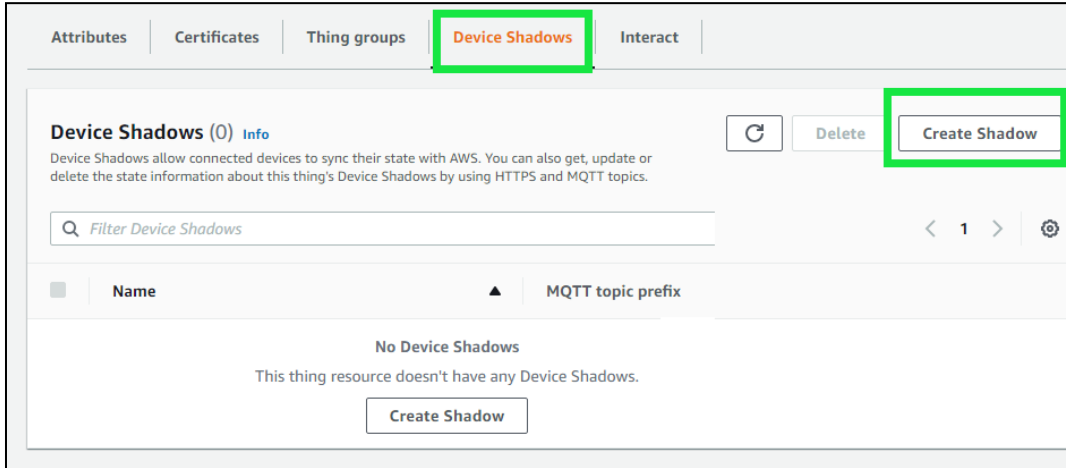
Download the certificate and the private key. Once downloaded, navigate back to this user guide section "how to FTP files into the RTA gateway" to load the certificate and private key into the gateway.





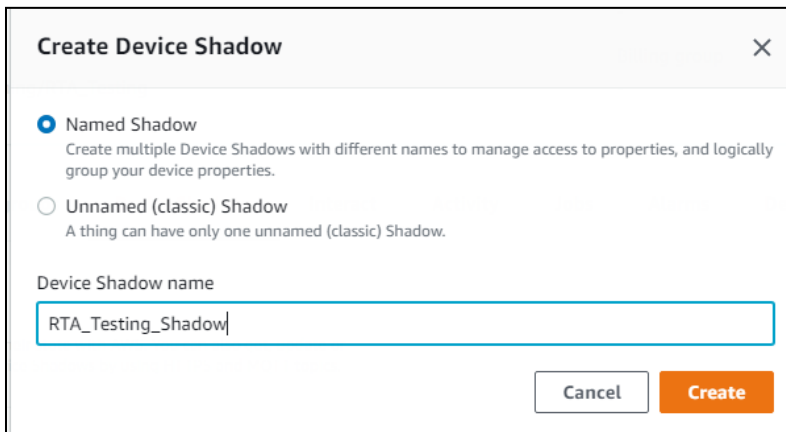
Once you have successfully downloaded the files you will be redirected to the Things page. Within the Things page, click on the thing name you setup, in this example it would be RTA_Testing. From this page, you can view if the certificate is active and create a Device Shadow URL.





Along with the certificate and private key, your RTA product will need the Device Shadow URL. Click the Device Shadows tab and click “Create Shadow”.

Enter in a Device Shadow name and click the Create button.



You will be redirected to the Things page where you’ll see your new Device Shadow created.

Click the Device Shadow name, in this case our example “RTA_Testing_Shadow” and it will display the details. You only want to copy the Device Shadow URL. Ignore the “https://” and everything after the “.com”

AWS IoT > Manage > Things > RTA_Testing > RTA_Testing_Shadow

RTA_Testing_Shadow

Device Shadow details

ARN
arn:aws:iot:us-east-2:1:thing/RTA_Testing/RTA_Testing_Shadow

MQTT topic prefix
\$aws/things/RTA_Testing/shadow/name/RTA_Testing_Shadow

Device Shadow URL
https://aabb11224e9ex-ats.iot.us-east-2.amazonaws.com/things/RTA_Testing/shadow?name=RTA_Testing_Shadow

Within the RTA gateway configuration Device Shadow URL, enter in “aabb11224e9ex-ats.iot.us-east-2.amazonaws.com,” everything else is ignored.

Attributes | Certificates | Thing groups | **Device Shadows** | Interact | Activity | Jobs | Alarms

Device Shadows (1) Info

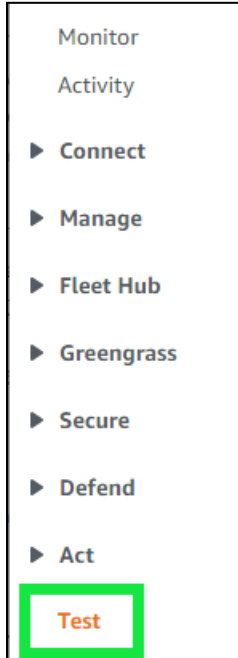
Device Shadows allow connected devices to sync their state with AWS. You can also get, update or delete the state information about this thing's Device Shadows by using HTTPS and MQTT topics.

Filter Device Shadows

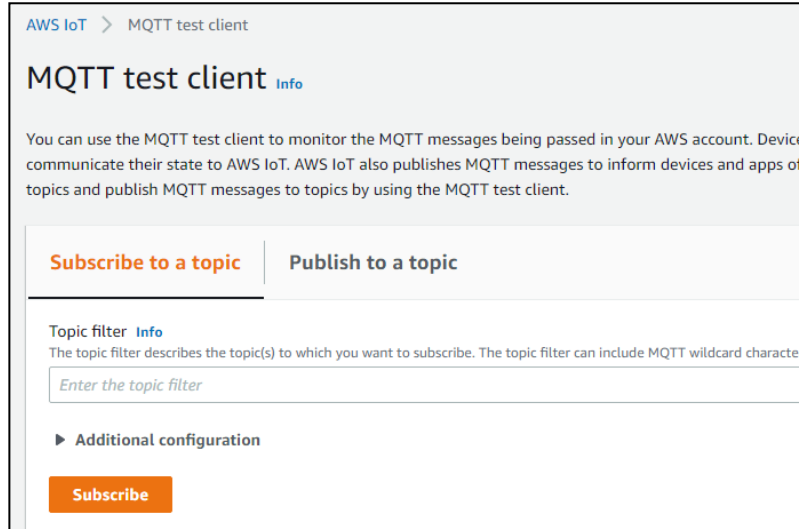
<input type="checkbox"/>	Name	MQTT topic prefix
<input type="checkbox"/>	RTA_Testing_Shadow	\$aws/things/RTA_Testing/shadow/name/RTA_Testing_Shadow

Testing AWS Communication

Once you have the AWS IoT Core service configured, you can use their “Test” feature to Publish a topic to the RTA gateway.



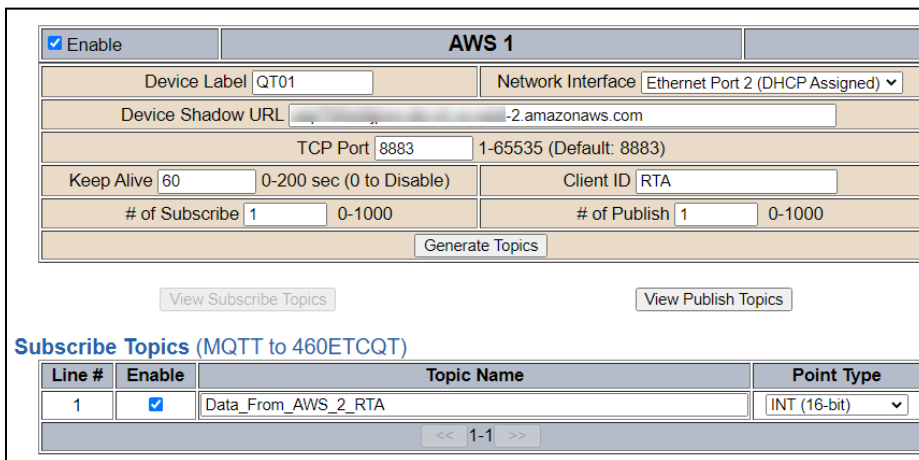
Note: This is assumed the certificate, private key and Device Shadow URL have already been configured in AWS, the two files have been FTP'd into the RTA gateway, and the Device Shadow URL is configured.



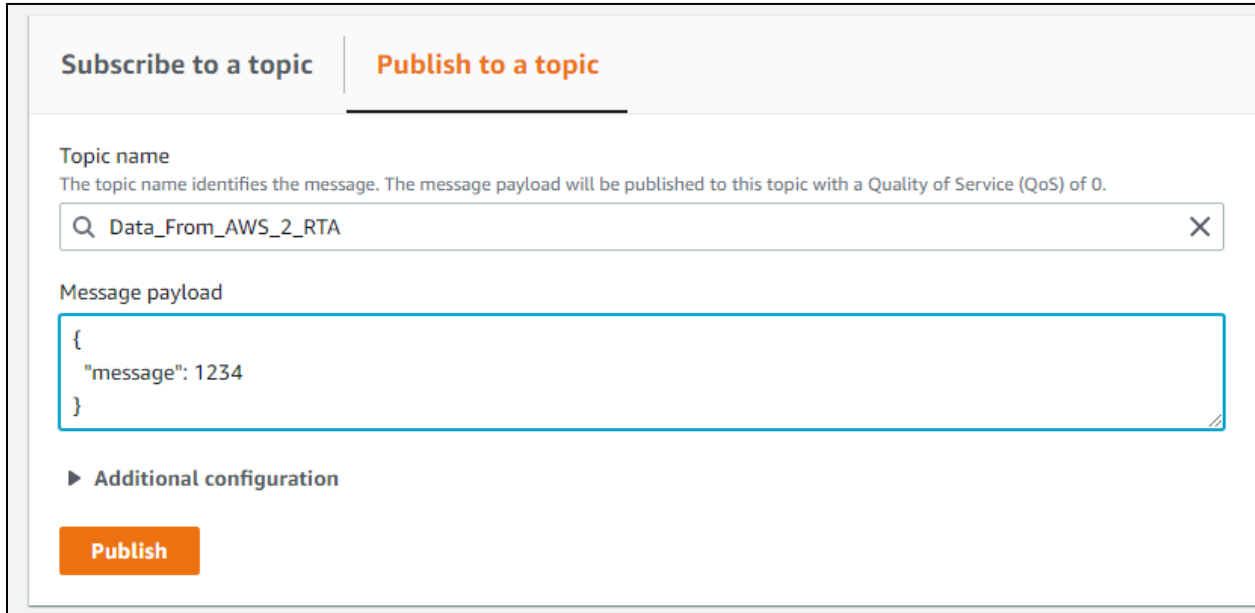
Using the AWS MQTT test client, you can Subscribe to a topic (data from the RTA), and you can Publish to a topic (data to the RTA).

Send data from AWS to RTA gateway (Subscribe Topic)

Below is how the RTA AWS IoT Core Service is setup to Subscribe data from AWS to the RTA.



Within AWS, click the “Publish to a topic” tab. Enter in the topic name that is defined in the RTA gateway “Subscribe Topics” configuration. In the Message payload, after the “:” enter in your value, if using a string be sure your data is in “ ”. For example, “message”: 1234 or “message”: “Hello World.” Once you have your data, click the Publish button.



Subscribe to a topic | **Publish to a topic**

Topic name
The topic name identifies the message. The message payload will be published to this topic with a Quality of Service (QoS) of 0.

Q Data_From_AWS_2_RTA X

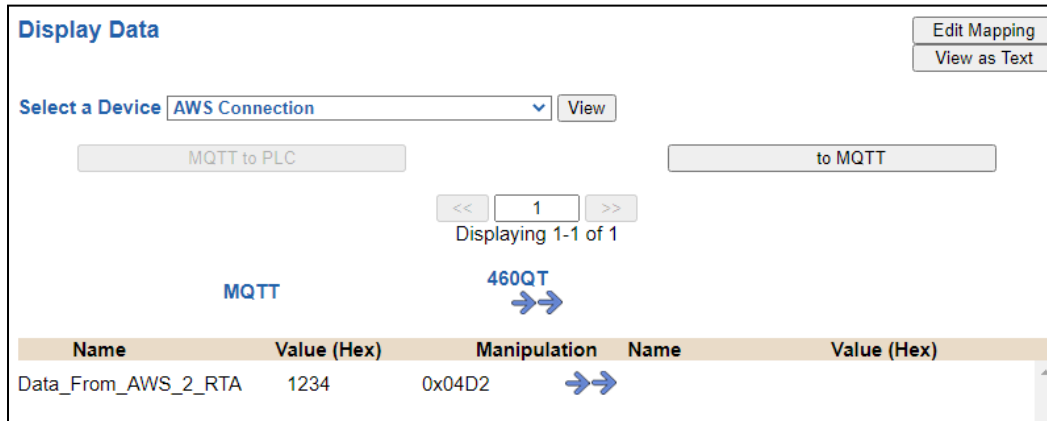
Message payload

```
{
  "message": 1234
}
```

▶ **Additional configuration**

Publish

Navigate to the RTA Display data and refresh the web page. You will see your data being updated.



Display Data Edit Mapping View as Text

Select a Device **AWS Connection** View

MQTT to PLC to MQTT

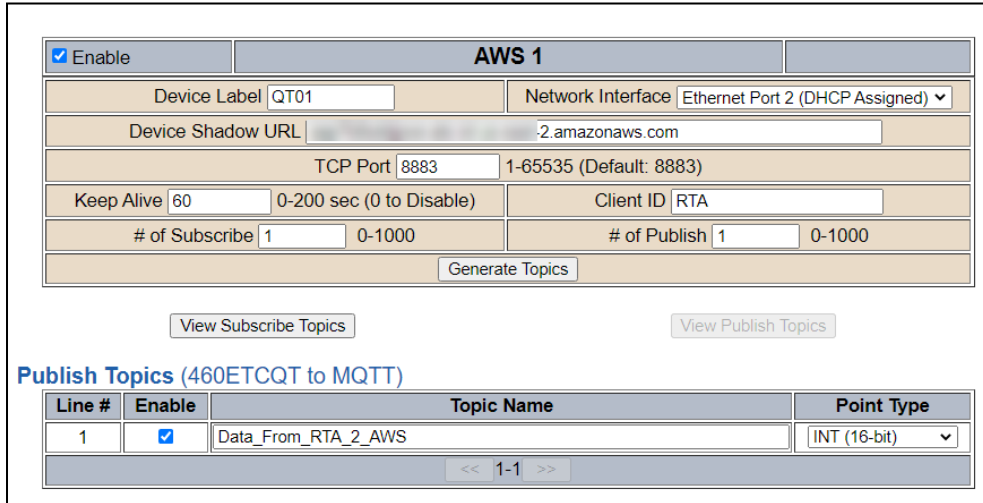
<< 1 >>
Displaying 1-1 of 1

MQTT 460QT →→

Name	Value (Hex)	Manipulation	Name	Value (Hex)
Data_From_AWS_2_RTA	1234	0x04D2		

Send data from RTA gateway to AWS (Publish Topics)

This example shows a PLC writing data to the RTA gateway and presenting that data to the Publish topic.



Line #	Enable	Topic Name	Point Type
1	<input checked="" type="checkbox"/>	Data_From_RT... (truncated)	INT (16-bit)

PLC		460ETCQT		MQTT	
Name	Value (Hex)	Manipulation	Name	Value (Hex)	
PLC_Data_2_AWS	111	0x006F	QT01 Data_From_RT... (truncated)	111	0x00

In the topic filter, use a wildcard character of “#” (subscribe to all topics), and click the Subscribe button. You’ll see the subscription once the new Publish data comes in. The “RTA” is the Client ID that is configured in the MQTT device configuration of the RTA. The “Data_From_RT... (truncated)” is the Publish Topic name configured in the AWS device configuration page of the RTA.



```

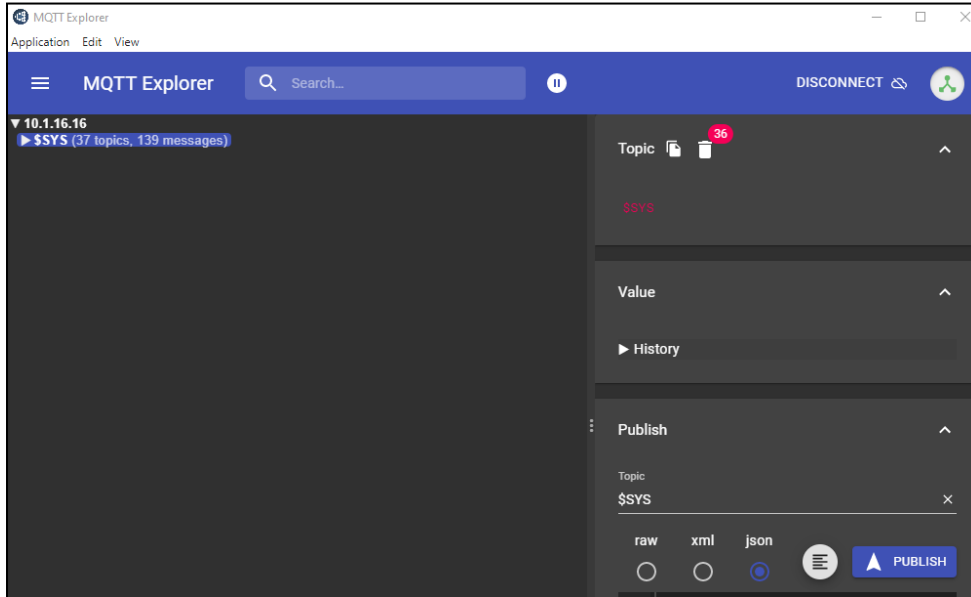
{
  "Data": 111
}

```

Testing Your MQTT Connections with MQTT Explorer

For this test example, we are going to be using MQTT Explorer (<https://mqtt-explorer.com/>) which can be downloaded for free. This tool can monitor MQTT client/broker relationships.

Once you launch the MQTT Explorer tool, setup a new connection. The host will be IP of your MQTT broker.



Next, you can configure the RTA gateway. The broker IP address listed below is set up to be “my PC,” this is where our MQTT broker is installed.

<input checked="" type="checkbox"/> Enable		MQTT 1	
Device Label	<input type="text" value="QT01"/>	Network Interface	<input type="text" value="Ethernet Port 1 (10.1.16.22)"/>
Broker IP Address	<input type="text" value="10.1.16.16"/>	TCP Port	<input type="text" value="1883"/> 1-65535 (Default: 1883)
Keep Alive	<input type="text" value="60"/> 0-200 sec (0 to Disable)	Client ID	<input type="text" value="RTA"/>
Username	<input type="text"/>	Password	<input type="text"/>
# of Subscribe Topics	<input type="text" value="01"/> 0-1000	# of Publish Topics	<input type="text" value="1"/> 0-1000
<input type="button" value="Generate Topics"/>			

Send data from RTA gateway to MQTT Explorer (Publish Topic)

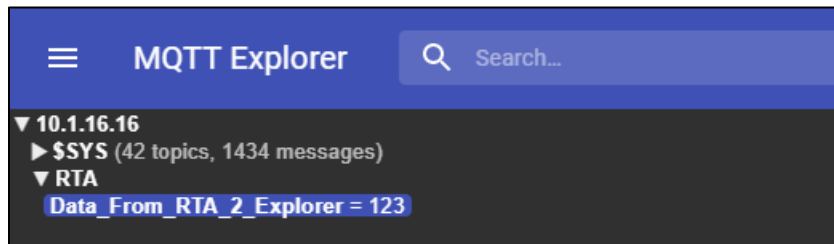
This example shows a PLC writing data to the RTA gateway and presenting that data to the MQTT publish topic.

Publish Topics (460ETCQT to MQTT)

Line #	Enable	Topic Name	Point Type
1	<input checked="" type="checkbox"/>	PLC_Data_2_Explorer	INT (16-bit)

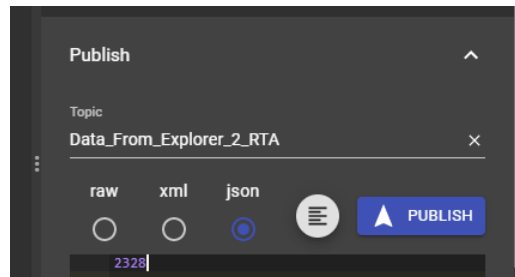
PLC			460ETCQT	MQTT	
Name	Value (Hex)	Manipulation		Name	Value (Hex)
PLC_Data_2_Explorer	123	0x007B	→→	Data_From_RT01_2_Explorer	123

Write a value in “my PLC” and MQTT Explorer will subscribe to that topic.



Send data from MQTT Explorer to RTA gateway (Subscribe Topic)

The RTA gateway has a topic name of Data_From_Explorer_2_RT01 that MQTT Explorer is going to be publishing to. Enter in the topic name to publish, enter in the value (our example is 2328), then click Publish.



PLC			460ETCQT	MQTT	
Name	Value (Hex)	Manipulation		Name	Value (Hex)
ETC01_G2N0_INT	2328	0x0918	←←	Data_From_Explorer_2_RT01	2328

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.

Modbus RTU			BACnet/IP		
Name	Value (Hex)	Manipulation	Name	Value (Hex)	
400001	-- --	→→	AI1	-- --	
400002	-- --	→→	AI2	Mapping Disabled for Point	
400003	-- --	→→	AI3	-- --	

In the above example, we see the following:

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

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

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

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

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

Display Data Edit Mapping View as Text

Select a Device Modbus TCP Server IP Address: 10.1.16.16 View

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

<<
1
>>

Displaying 1-7 of 7

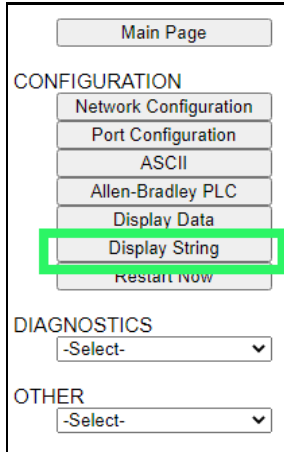
Modbus TCP/IP			460ETCMC ↔↔	PLC		
Name	Value (Hex)		Manipulation	Name	Value (Hex)	
400001	15	0x000F	↔↔	ETC01 MC2PLC_INT[0]	15	0x000F
400002	1495	0x05D7	↔↔	ETC01 MC2PLC_INT[1]	1495	0x05D7
400003	1	0x0001	↔↔	ETC01 MC2PLC_INT[2]	1	0x0001
400004	23	0x0017	↔↔	ETC01 MC2PLC_INT[3]	23	0x0017
400005	3	0x0003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

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

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

Display String

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



Main Page

CONFIGURATION

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

DIAGNOSTICS

-Select-

OTHER

-Select-

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

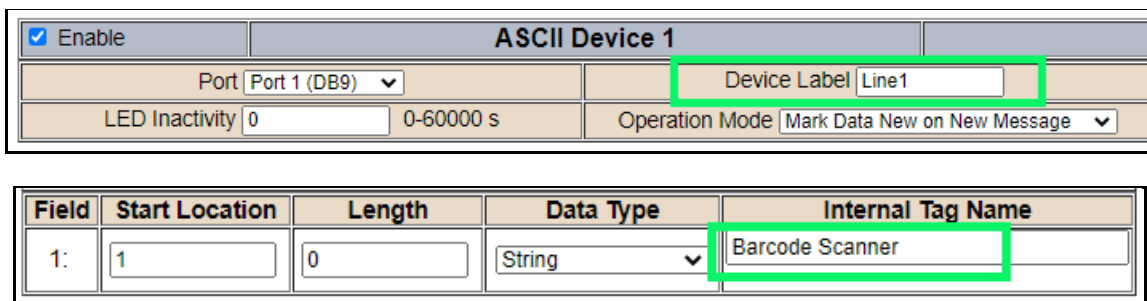


Display String Edit Mapping
View as Text

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

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

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



Enable **ASCII Device 1**

Port **Port 1 (DB9)** Device Label **Line1**

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

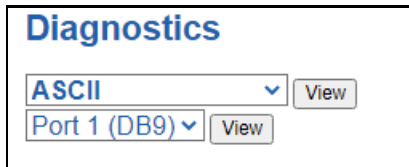
Field	Start Location	Length	Data Type	Internal Tag Name
1:	1	0	String	Barcode Scanner

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.



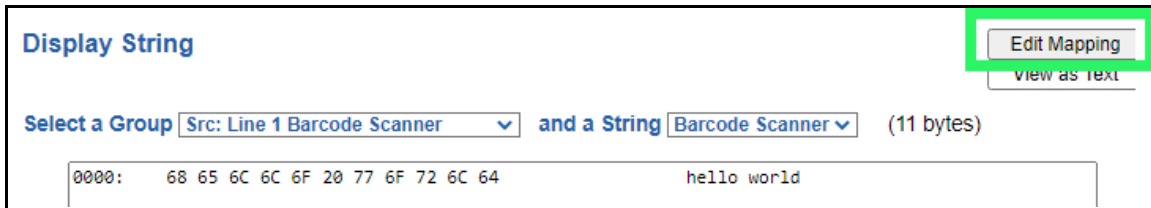
The screenshot shows a 'Display String' window with the title 'Display String'. In the top right corner, there are two buttons: 'Edit Mapping' and 'View as Text'. Below the title, there are two dropdown menus: 'Select a Group' with 'Src: Line 1 Barcode Scanner' selected, and 'and a String' with 'Barcode Scanner' selected. To the right of these dropdowns, it says '(0 bytes)'. Below this information, there is a text box containing the text 'Data Not Valid'.

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



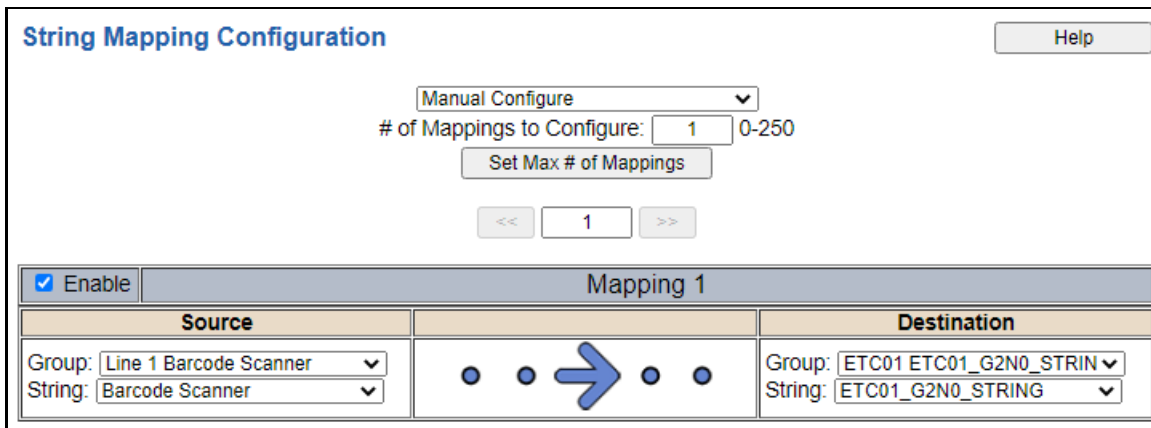
The screenshot shows a 'Diagnostics' window. It has two dropdown menus: 'ASCII' and 'Port 1 (DB9)'. To the right of each dropdown menu is a 'View' button.

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



The screenshot shows the 'Display String' window with the title 'Display String'. In the top right corner, the 'Edit Mapping' button is highlighted with a green box. Below the title, there are two dropdown menus: 'Select a Group' with 'Src: Line 1 Barcode Scanner' selected, and 'and a String' with 'Barcode Scanner' selected. To the right of these dropdowns, it says '(11 bytes)'. Below this information, there is a text box containing the text '0000: 68 65 6C 6C 6F 20 77 6F 72 6C 64 hello world'.

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



The screenshot shows the 'String Mapping Configuration' window. It has a 'Manual Configure' dropdown menu and a '# of Mappings to Configure' field with the value '1' and a range of '0-250'. Below this is a 'Set Max # of Mappings' button. There are also navigation buttons '<<', '1', and '>>'. Below this is a table with a header 'Mapping 1' and a 'Help' button. The table has three columns: 'Source', 'Destination', and a central area with a blue arrow pointing right. The 'Source' column has 'Group: Line 1 Barcode Scanner' and 'String: Barcode Scanner'. The 'Destination' column has 'Group: ETC01 ETC01_G2N0_STRIN' and 'String: ETC01_G2N0_STRING'.

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

Display String use case

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

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

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

Display String Edit Mapping
View as Text

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

0000: 52 54 41 RTA

Display String Edit Mapping
View as Text

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

0000: 53 75 70 70 6F 72 74 Support

Display String Edit Mapping
View as Text

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

0000: 52 6F 63 68 73 Rocks

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

Diagnostics Last Message Sent (17 bytes)

ASCII View

Port 1 (DB9) View

```

0000: 52 54 41 2C 53 75 70 70 6F 72 74 2C 52 6F 63 68 RTA,Support,Rock
0016: 73 s

```

Data and String Mapping – Auto-Configure

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

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

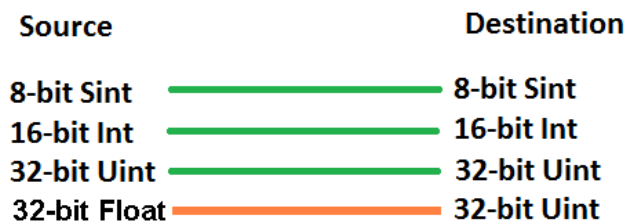
The following are examples of the Auto-Configure function.

- 1) This example shows a common valid setup.



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

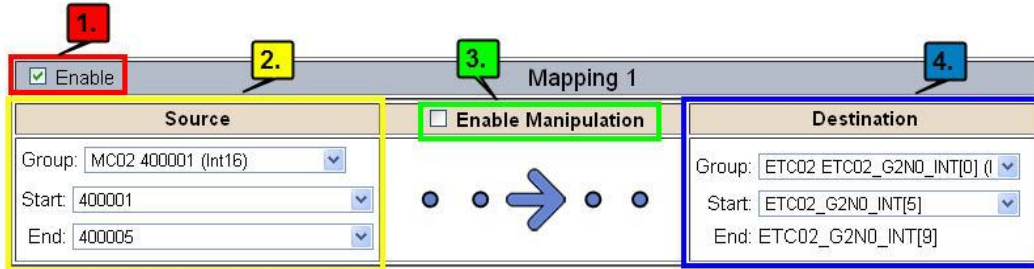
- 2) This example shows how Auto-Configure will make its best guess.



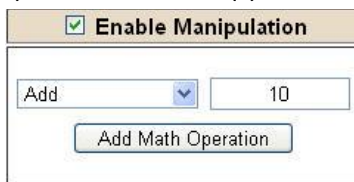
- a. The 32-bit Float from the Source location could not find a matching Destination data-type. After all other like data types were mapped, the only data type available was the 2nd 32-bit Uint data type. Auto-Configure was completed even though the data in the Float will be truncated.

Data Mapping – Explanation

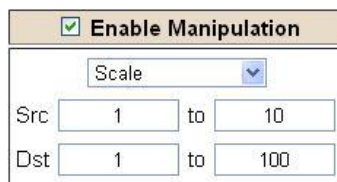
Below are the different parts that can be modified to make up a data mapping.



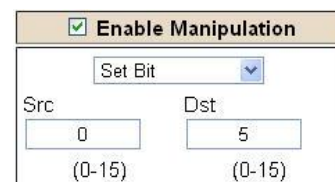
- 1) Enable (red box above): Check to enable mapping. If not checked, this mapping is skipped.
- 2) Source Field (yellow box above):
 - a) Group - Select the data group you set up in the protocol config to use for this mapping.
 - b) Start - This is the starting point for this mapping.
 - c) End - This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

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


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

2) Temporary Ram (Double)

- a) This is like the Temporary Ram (Int 64), except manipulations will be conducted against the 64bit floating point to allow for large data.

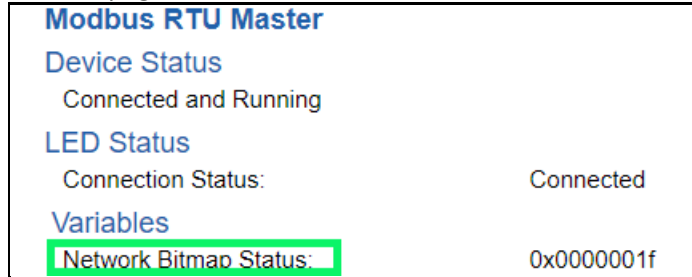
3) Ticks Per Second

- a) The gateway operates at 200 ticks per second. This equates to one tick every 5ms. Thus, mapping this to a destination will give easy confirmation of data flow without involving one of the two protocols. If data stops on the destination end, then the RTA is offline.

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

4) XY_NetBmpStat

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



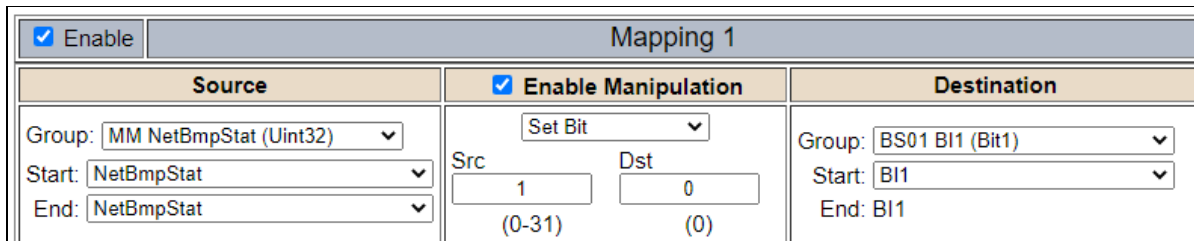
- b) Since a Client/Master may be trying to communicate with multiple devices on the network, it may be beneficial to know if a Server/Slave device is down. By using this Network Bitmap Status, you can expose the connection statuses of individual devices. **Values shown are in HEX.**
- i) 0x00000002 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.



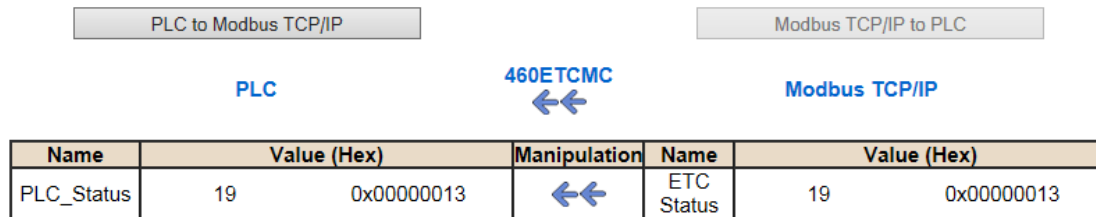
5) Status_XY

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

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

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

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



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)
<u>0x10</u>	<u>4(on)</u>	<u>16</u>	<u>running (usually added to connected)</u>
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

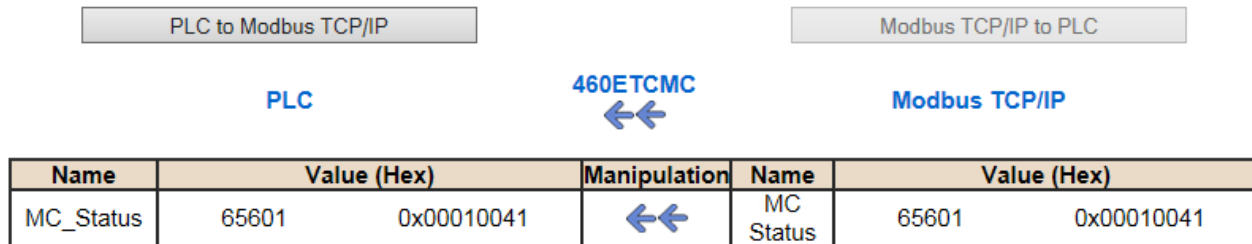
Recoverable Faults: **0x00FF0000 (bit 16-23) 3rd byte**

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



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.

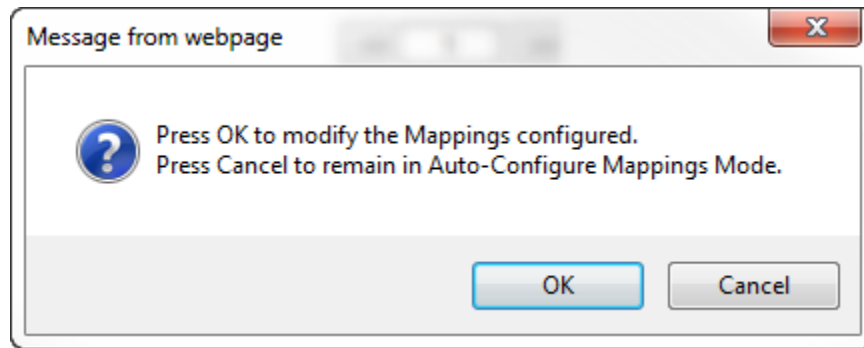
Mapping 1	
<input checked="" type="checkbox"/> Enable	
Source	Destination
Group: Line 1 Barcode Scanner	Group: ETC01 ETC01_G2N0_STRIN
String: Barcode Scanner	String: ETC01_G2N0_STRING

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

Mapping – Auto-Configure Mode to Manual Configure Mode

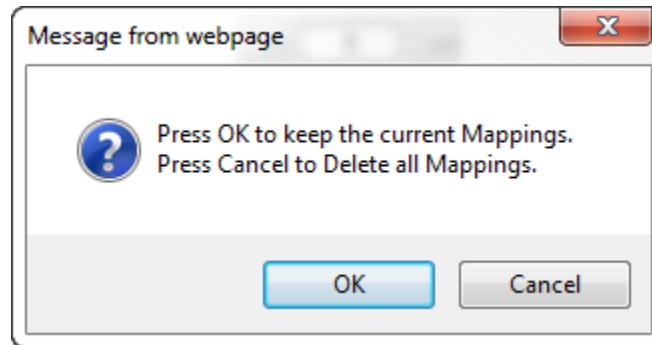
To transition from Auto-Configure Mapping Mode to Manual Configure Mode, click the dropdown at the top of the Mapping Configuration page and select Manual Configure.

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



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

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

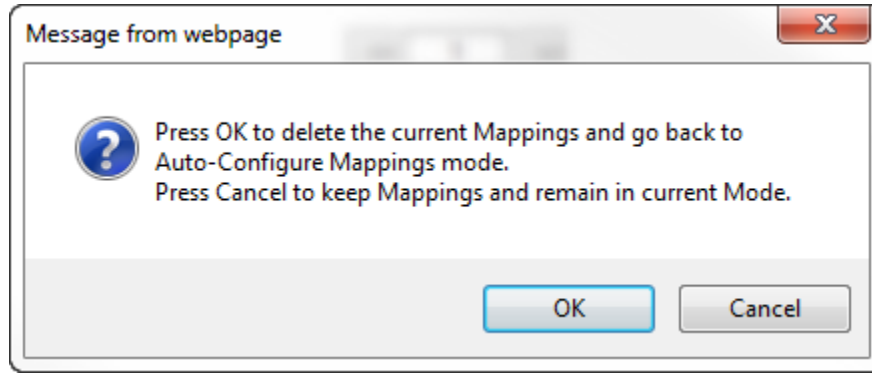


- 1) To keep the mappings that are already configured press **OK**.
 - a) You would want this option if you are adding additional mappings or you want to modify the mapping(s) that already exist.
- 2) To delete the mappings that are already there and start over press **Cancel**.

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

Mapping – Manual Configure Mode to Auto-Configure Mode

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



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

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

View as Text

Data Mapping

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

Each line on this page will read as follows:

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

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

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

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

String Mapping

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

Each line on this page will read as follows:

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

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

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

Base Triggering – Data Validation Triggering

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

How does this work?

- 1) Map the Triggering Variable (Source) over to Trigger # (Dest).
- 2) If Trigger # value changes states mark all Trigger # protocols read data as “Invalid”.
- 3) Read all source read data points until ALL source read data is valid.
- 4) Handshake # value is set equal to Trigger # value.
- 5) Map Handshake # to reference data point.

Note: # is an internal reference to the Server/Slave number you are settings up. **ex.** RTA Server/Slave products can only be Trigger 1 and Handshake 1 since we are only 1 device. If RTA is a Master/Client, then you can have a Trigger# for each server/slave connected too.

How do you set this up?

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

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

Write Data Groups (BACnet/IP to 460MCBS)

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

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

Setup BACnet Names, Units, and COV

21	G01	Data Validation Trigger	Other	no-units	1.000000
----	-----	-------------------------	-------	----------	----------

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

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

40	G01	Data Validation Result	Other	no-units	1.000000
----	-----	------------------------	-------	----------	----------

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

Mapping 2		
Source	<input type="checkbox"/> 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.

Mapping 3		
Source	<input type="checkbox"/> 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

Log Out Timer: 0-15 min

Admin Configuration

Admin	Username	Password	Re-enter Password	Email	Hint
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	Not Configured	<input type="text"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	Not Configured	<input type="text"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	Not Configured	<input type="text"/>

Admin Contact Information

User Configuration

User	Username	Password	Re-enter Password	Email	Hint
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	Not Configured	<input type="text"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	Not Configured	<input type="text"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	Not Configured	<input type="text"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	Not Configured	<input type="text"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>	Not Configured	<input type="text"/>

Security Configuration-Security Levels

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

Security Levels:

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

User 1: <input type="button" value="View"/>	
Web Page	Security
All Web Pages	No Access <input type="button" value="Set"/>
Web Page	Security
Main Page	Full Access <input type="button" value="v"/>
Device Configuration	Full Access <input type="button" value="v"/>
Port Configuration	Full Access <input type="button" value="v"/>
BACnet/IP Server	Full Access <input type="button" value="v"/>
Modbus RTU Master	Full Access <input type="button" value="v"/>
View Mapping	Full Access <input type="button" value="v"/>
Mapping	Full Access <input type="button" value="v"/>
Setup LED's	Full Access <input type="button" value="v"/>
Diagnostic Info	Full Access <input type="button" value="v"/>
Logging	Full Access <input type="button" value="v"/>
Display Data	Full Access <input type="button" value="v"/>
Export Configuration	Full Access <input type="button" value="v"/>
Import Configuration	Full Access <input type="button" value="v"/>
Save As Template	Full Access <input type="button" value="v"/>
Load From Template	Full Access <input type="button" value="v"/>
Utilities	Full Access <input type="button" value="v"/>
Email Configuration	Full Access <input type="button" value="v"/>
Alarm Configuration	Full Access <input type="button" value="v"/>
String Mapping	Full Access <input type="button" value="v"/>
View String Mapping	Full Access <input type="button" value="v"/>
Display String	Full Access <input type="button" value="v"/>

Security - Log In

Username: Name of the user to login.

Password: Password of the user to login.

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

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

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

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



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

Security - Log Out

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



The screenshot shows the header of the RTA web interface. On the left is the RTA logo. In the center, it says "Welcome Admin" followed by a "logout" link. On the right is the URL "www.rtaautomation.com". Below this is a blue bar with "Real Time Automation, Inc." on the left and "MODE: RUNNING 460" on the right.

Closing the browser is not sufficient to log out.

Email Configuration

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

You can configure up to 10 email addresses.

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

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

Email Configuration

Number of Emails to Configure: 0-10

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

Alarm Configuration

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

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

Alarm Configuration
Help

Alarm Delay upon Powerup: 0-3600 s

of Alarms to Configure: 0-100

<< >>

<input checked="" type="checkbox"/> Enable	Alarm 1			
Data Point	Set Error	Clear Error	Alarm Name	Email
Ticks Since Powerup (Uint32) ▼	>= ▼	None ▼	Gateway_test	Group A ▼
Ticks Since Powerup ▼	1000	0		

<< >>

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

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

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

Diagnostics – Alarm Status

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

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

Alarm Status

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

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

Alarms – Active

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


www.rtaautomation.com

Real Time Automation, Inc.
Alarms Active
MODE: RUNNING

460

When an alarm is activated, the following will occur:

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

5) *Last Active Alarm* field will be populated with details on what triggered the alarm.

Alarm Status

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

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

Alarms – Clear

When an alarm is cleared, the following will occur:

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

Change of State (COS) Configuration

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

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

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

Change of State Configuration Help

Stale Data Timer: 0-3600 s

Production Inhibit Timer: 0-60000 ms

Writes Before Reads: 0-255

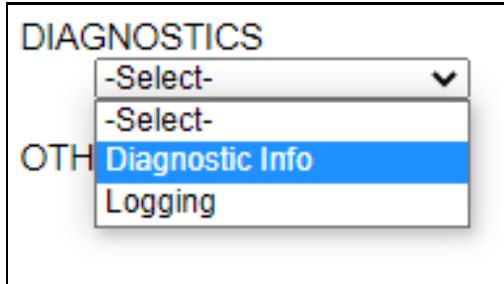
Reads Before Writes: 1-255

Enable Data Integrity:

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

Diagnostics Info

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



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

Diagnostics Mapping

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

Common Errors:

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

Data Mapping

# Enabled:	5 of 5
# of Errors:	0
First Error:	

String Mapping

# Enabled:	2 of 2
# of Errors:	0
First Error:	

Alarms

# Enabled:	3
# Active:	0
Last Active:	

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

Diagnostics – PROFINET IO Server

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

Diagnostics

Profinet IO Server View
Clear All Values

View
Help

Device Status

Configuration Mode... Gateway Restart Needed

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

Clear All Values - This will only affect displayed values.

- 1) This will reset all displayed values back to zero.
- 2) If viewing PROFINET IO Server, this will only clear the values for the PROFINET IO Server section of the gateway.

Device Status:

Device Status

Configuration Mode... Gateway Restart Needed

- 1) Connected - A PROFINET IO controller has a connection for the gateway.
- 2) Not Connected:
 - a) The PROFINET IO controller has not initiated communication to the gateway.
 - b) The PROFINET IO server has an invalid configuration or no parameters configured.

LED Status:

LED Status

Connection Status: Configuration Mode

- 1) Solid Green (Connected and Running) – Connected to a PROFINET IO controller and online.
- 2) Flashing Green (Connection not yet attempted) – Valid Configuration but no communication from the IO controller yet.
- 3) Solid Red (Fatal Error)
 - a) Invalid Configuration due to no input/output slots configured within the gateway
- 4) Flashing Red (Connection Timeout)
 - a) PROFINET IO controller’s slot configuration doesn’t match the gateway’s slot configuration
 - b) PROFINET IO controller was communicating to the gateway and is no longer communicating
- 5) Off (No Ethernet Cable Plugged In)

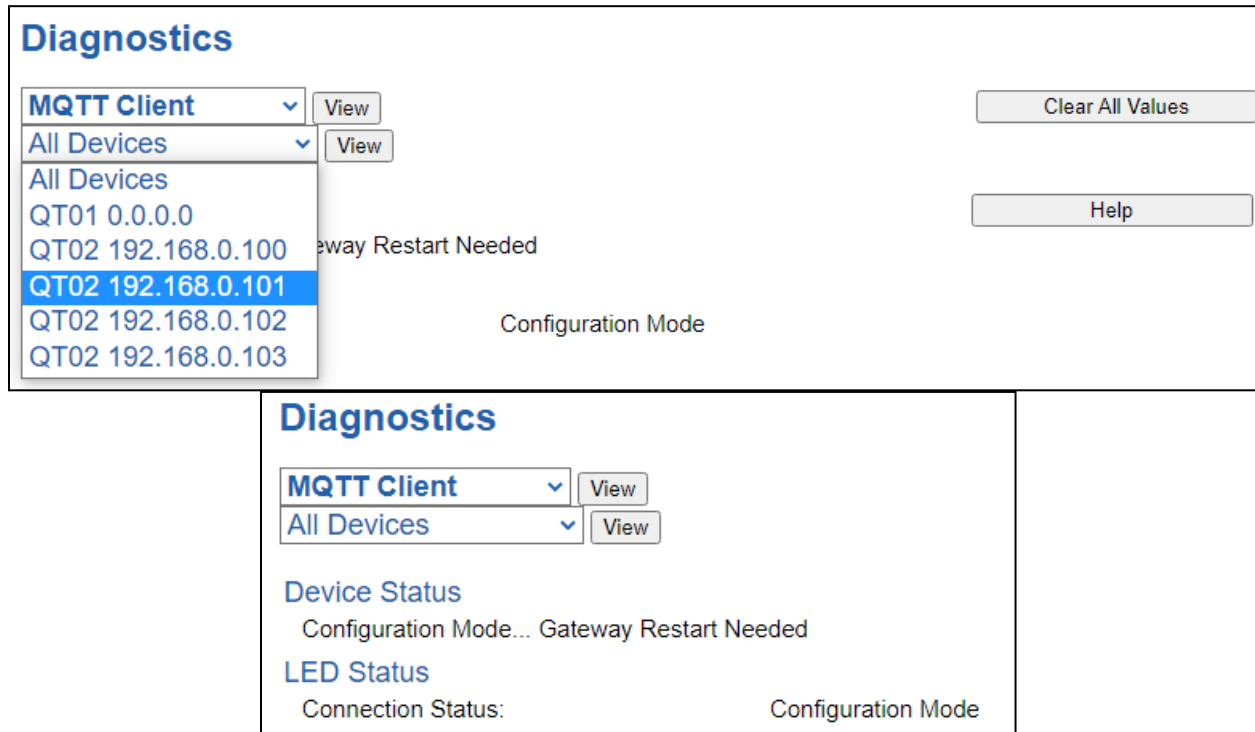
Variables:

Variables	
Application Ready Rcvd:	0
Release AR:	0
Parameters Written:	0
PN Ethernet Pkts Rcvd:	0
PN Ethernet Pkts Sent:	0
Connection Timeouts:	0
Speed Limit Increment:	0

- 1) Application Ready Rcvd:
 - a) The Application Ready Command has been received
 - b) The gateway has completed the PROFINET setup sequence and will start cyclic communication
- 2) Release AR:
 - a) A Release Application Relationship command has been received
 - b) PROFINET communication have been disconnected from the gateway
- 3) Parameters Written:
 - a) Rollover counter for the number of parameters written by the IO controller.
- 4) PN Ethernet Pkts Received:
 - a) Number of Layer 2 (Ethernet) Messages received
- 5) PN Ethernet Pkts Sent:
 - a) Number of Layer 2 (Ethernet) Messages transmitted
- 6) Connection Timeouts:
 - a) Number of Connection timeouts between the gateway and the IO controller
 - b) If this counter is incrementing, check your ethernet connection
 - c) If this counter is incrementing, verify the gateway is in the IO controller
- 7) Speed Limit Increments:
 - a) The gateway has received too much traffic to process all the data
 - b) The gateway will stop processing PROFINET data for a short time

Diagnostic – MQTT Client

Select the MQTT Client in the dropdown menu on the Diagnostic page to view the breakdown of the diagnostics and common strings that are display on the page. You may also view the individual MQTT device counters by selecting the device in the All Devices drop down and clicking **View**.



The screenshot shows the 'Diagnostics' page with two dropdown menus. The first dropdown is labeled 'MQTT Client' and has a 'View' button next to it. The second dropdown is labeled 'All Devices' and also has a 'View' button. The 'All Devices' dropdown is open, showing a list of devices: 'All Devices', 'QT01 0.0.0.0', 'QT02 192.168.0.100', 'QT02 192.168.0.101' (highlighted in blue), 'QT02 192.168.0.102', and 'QT02 192.168.0.103'. Below the dropdowns, there are buttons for 'Clear All Values' and 'Help'. The text 'Gateway Restart Needed' and 'Configuration Mode' is visible in the background.

NOTE: This page will auto-refresh every five seconds.

Clear All Values: This will only affect the Variables values.

- This will return all values displayed to zero. Example: If viewing QT02 192.168.0.101, this will only clear the values for that specific device.

Device Status: This will only display when viewing All Servers.

Connected: All Devices configured/enabled are communicating

Not Connected: Fatal Error No Configuration

- No Devices that have been configured are enabled
- No Devices that have been configured and enabled have topics configured

Not Connected: Dependency Protocol is Faulted

- The Dependency Protocol has Faulted

Error: Timeout

- One or more enabled devices are missing
- Verify MQTT broker for correct IP address.

LED Status

Solid Green (Connected):

- The gateway is connected to all the MQTT devices that are configured and enabled

Flashing Green (Not Connected):

- No MQTT devices are configured / enabled. Go to the MQTT Client Device Configuration to configure a device

Flashing Red (Not Connected):

- One or more of the MQTT brokers configured are missing (nodes missing)
- One or more of the MQTT brokers configured do not have topics configured
- The Dependency Protocol has faulted

Flashing Red (Communication not attempted yet):

- No topics are configured and data needed for writes isn't valid yet

Solid Red (Invalid Configuration):

- No devices are enabled
- One or more of the MQTT devices have a conflicted IP address

Off:

- No Power
- No Ethernet cable connected

Variables: These are the values for all servers, or the specific server selected.

Variables	
Network Bitmap Status:	0x00000000
Published Messages to MQTT:	0
Published Messages from MQTT:	0
Subscribed Messages Actual:	0
Subscribed Messages Expected:	0

Network Bitmap Status (Displayed in Hex):

- Each bit corresponds to a MQTT device. If the bit is set, the MQTT device is connected, otherwise the bit is 0.
- Bit 0 corresponds to MQTT device 1 and Bit 4 is for MQTT device 5 and so on.

Published Messages to MQTT:

- Number of Write Topics which have been sent to the MQTT broker

Published Messages from MQTT:

- Number of Read Topics which have been sent from the MQTT broker to the gateway

Subscribed Messages Actual:

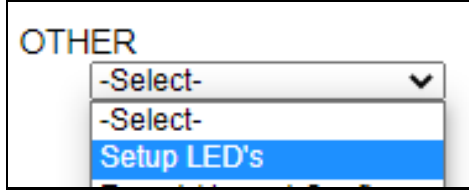
- Number of Successful Subscribed Topics
- This should equal the Subscribed Messages Expected

Subscribed Messages Expected:

- Number of Subscribed Topics that the gateway should have open

LED Configuration

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

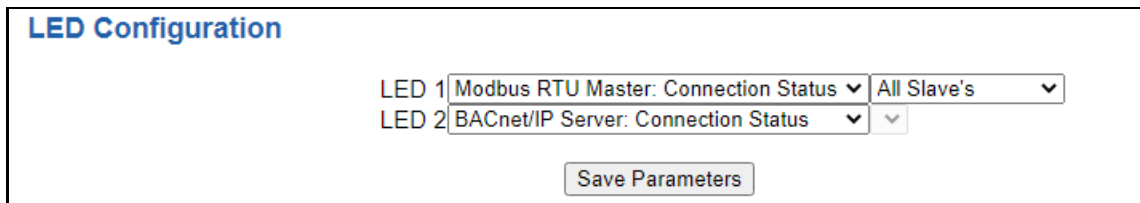


Each LED may be set to Disabled, Protocol 1, or Protocol 2. If either protocol is a master/client, you may set the LED to represent either all slaves/servers configured in the gateway or a slave/server device.

To select a slave/server device:

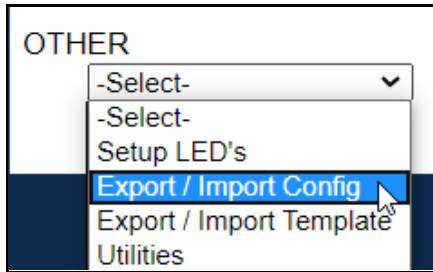
- 1) Select the protocol in the left dropdown menu.
- 2) Click **Save Parameters** to generate the second dropdown menu.
- 3) Select the individual slave/server in the right dropdown menu.

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



Configuration Files

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



Export Configuration

Export Configuration

Save Configuration to File

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

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



Import Configuration

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

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

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

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

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

Import Configuration

No file chosen

Import Network Settings

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

Save and Replace Configuration Using SD Card

Saving Configuration Using SD Card

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

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

Replacing Configuration Using SD Card

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

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

Intelligent Reset Button

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



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

Utilities

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



Here you can also:

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

Revisions	<input type="button" value="Listing of Revisions"/>
File List	<input type="button" value="File List"/>
Identify Device	<input type="button" value="Start Flashing LED's"/>
Set Up Log	<input type="button" value="Log Configuration"/>
Revert To Last Powerup	<input type="button" value="Revert to Last Powerup"/>
Revert All	<input type="button" value="Revert to Manufacturing Defaults"/>
Reformat Flash	<input type="button" value="Reformat Flash"/>