

# 460ETCQT-NNA1 Protocol Gateway

## Product User Guide

Firmware Version 8.8.37



#### 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<sup>®</sup> is a registered trademark of American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE). All other trademarks and registered trademarks are the property of their holders.

#### **Limited Warranty**

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

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

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

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

#### Government End-Users

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and its successors; (d) in all respects is proprietary data belonging solely to Real Time Automation, Inc.; (e) is unpublished and all rights are reserved under copyright laws of the United States.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

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



Revision History	6
Overview	8
Hardware Platforms	9
Hardware – NNA1	
Powering the Gateway	
Mounting with a DIN Rail	11
Installing	11
Removing	11
Accessing the Main Page	
Committing Changes to the Settings	14
Main Page	15
Device Configuration	16
Network Configuration	
Allen-Bradley PLC Configuration	
External PLC Configuration	
External PLC Configuration: Auto-Configure	20
Auto-Configure Group by Device vs. Auto-Configure Group by Data Type	21
Group by Device (Default Method)	21
Group by Data Type	21
External PLC Configuration: Manual Configure Mode	22
Configuring Read and Write Scan Lines	24
Access Program Scope Tags	27
Optimized Trigger Guide	28
MQTT Client Configuration	
MQTT Devices Configuration	
Configuring Subscribe and Publish Topics	
Amazon Web Services (AWS) Configuration	35
Additional AWS Requirements	
How to FTP files into the RTA gateway	
AWS IoT Core Service Setup	
AWS IoT Core Service Things Configuration	41
Certificate setup	42
Real Time Automation, Inc. 3	1-800-249-1612



Attach policies to certificate	44
Testing AWS Communication	48
Send data from AWS to RTA gateway (Subscribe Topic)	49
Send data from RTA gateway to AWS (Publish Topics)	50
Testing Your MQTT Connections with MQTT Explorer	53
Send data from RTA gateway to MQTT Explorer (Publish Topic)	54
Send data from MQTT Explorer to RTA gateway (Subscribe Topic)	55
Microsoft Azure Service Setup	56
Testing Microsoft Azure Communication	66
Send data from Microsoft Azure to RTA gateway	68
Send data from RTA gateway to Microsoft Azure (Publish Topics)	70
QT Publish Trigger	72
Mapping - Transferring Data Between Devices	73
Display Mapping and Values	74
Display Data	74
Display String	77
Display String use case	79
Data and String Mapping – Auto-Configure	80
Data Mapping – Explanation	81
Data Mapping – Adding Diagnostic Information	82
String Mapping – Explanation	87
Mapping – Auto-Configure Mode to Manual Configure Mode	88
Mapping – Manual Configure Mode to Auto-Configure Mode	89
View as Text	90
Data Mapping	90
String Mapping	
Base Triggering – Data Validiation Triggering	91
Security Configuration	93
Security Configuration-Security Levels	94
Security - Log In	95
Security - Log Out	95
Email Configuration	96
Alarm Configuration	97
Real Time Automation, Inc. 4	1-800-249-1612



Diagnostics – Alarm Status	99
Alarms – Active	
Alarms – Clear	
Change of State (COS) Configuration	
Diagnostics Info	
Diagnostics Mapping	
Diagnostics – Allen-Bradley PLC	
Diagnostic – MQTT Client	
LED Configuration	
Configuration Files	
Export Configuration	
Import Configuration	
Save and Replace Configuration Using SD Card	
Saving Configuration Using SD Card	
Replacing Configuration Using SD Card	
Intelligent Reset Button	
Utilities	



## **Revision History**

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



Version	Date	Notes
8.9.22	2/5/24	<ul> <li>Features Added:</li> <li>1. Added priority-based reads for client protocols</li> <li>2. Added improved diagnostic timers for client protocols</li> <li>3. Reduced minimum delay between messages to zero ms on client protocols</li> <li>4. Added support for USB serial connections</li> <li>5. Added support for multiple connections on EtherNet/IP Adapter</li> <li>6. Added 100ms and 1000ms heartbeat values for diagnostic use</li> <li>7. Added configurable data size to EtherNet/IP adapter and DeviceNet Slave</li> <li>8. Added support for TL communications on N34, NNA1, NNA4, N2E, and N2EW hardware</li> <li>9. Added support for JSON payloads to MQTT</li> <li>10. Added Network Bitmap Status to ASCII, USB, and TCP protocols</li> <li>Bug Fixes:</li> <li>11. Fixed COV Subscription Issues on BACnet MS/TP</li> <li>12. Fixed timing issues affecting gateway performance</li> <li>13. Fixed a bug where the Run Idle Header on the output instance for EtherNet/IP Scanner was not checked by default</li> </ul>
8.9.29	4/1/24	<ul> <li>Features Added:</li> <li>14. Added ability to do raw HEX byte copy when receiving data over ASCII, TCP, or USB.</li> <li>Bug Fixes:</li> <li>15. Fixed bug where function code 15 did not work on MM/MC.</li> <li>16. Fixed bug relating to writing zeros on start up on BS.</li> <li>17. Fixed bug where MQTT client did not appear in display data page when MQTT was paired with BACnet</li> </ul>
8.9.37	7/30/24	Bug Fixes: 18. EIP IO Communication fixes 19. Timing fixes 20. USB Fixes a. Inactivity Timeout b. Inactivity Timeout Logging c. Port Restart Logging d. Webpage fixes 21. ProfiNet Timing Fix 22. EIP PanelView Fixes a. Support for Explicit Messaging



### Overview

The 460ETCQT-NNA1 gateway Easily and securely connect Allen-Bradley PLCs to an MQTT broker . By following this guide, you will be able to configure the 460ETCQT-NNA1 gateway.

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

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

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 460ETCQT-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 <u>Accessing Browser</u> <u>Configuration</u> document from our support web site.

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

NDK Settings IP	0.	0.	0.	0		- Select a	Unit 60 XXYY	(00-03-F4-0A	-D2-8C] Auto	P at 169.254.4
Network Mask	0.	0.	0.	0						
GateWay	0.	0.	0.	0	Set>					
DNS 🛛	0.	0.	0.	0				m		
								Search	Again	
					-	L	1			

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

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



#### Error: Main Page Does Not Launch

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

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



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

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





## Committing Changes to the Settings

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

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

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



The reboot can take up to 20 seconds.

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



#### Main Page

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

Running Mode:

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

Configuring Mode:

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

#### Navigation (green box below):

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

RTA				www.rtaautomation.com
Real Time Auton	nation, Inc.			460ETCMC
Configuration Mode		Mair	n Page	
Main Page		Device Description: Applicat	tion Description	
CONFIGURATION Network Configuration Allen-Bradley PLC		Save F	Parameters	
Modbus TCP/IP Client	Network Status	Link Otatur		
DIAGNOSTICS -Select-	Ethernet Port	100Mbps, Full Duplex	00:03:F4:0A:43:CC	10.1.28.95
OTHER -Select- ▼	Allen-Bradley PLC Statu Device Status: Last Read Error Code:	JS Fatal Error: No Configurati	ion	
	LED Status:	Connection Status: No Dev	vices Configured / Enabled	
	Modbus TCP/IP Client S Device Status: Last Error Code:	Status Fatal Error: No Configurati	ion	
	LED Status:	Connection Status: No De	vices Configured / Enabled	
	Data Mapping Status # Enabled: # of Errors: First Error:	0 of 0 0		



## **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: Application Description	]
Save Parameters	

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.

Network Configuration	Help				
Ethernet Configuration					
Ethernet MAC Address:	00:03:F4:0B:C3:02				
Ethernet Link:	Auto-Negotiate 🔻				
IP Setting:	Static IP 🔻				
IP Address:	10.1.16.40				
Subnet:	255.255.0.0				
Default Gateway:	0.0.0.0				
DNS Gateway:	0.0.0.0				
Save Parameters					

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.



## Allen-Bradley PLC Configuration

Click the Allen-Bradley PLC button to access the configuration page.

- 1) Select which **Network Interface** to use for this Allen-Bradley PLC connection. If using single port hardware, the Network Interface will default to Ethernet port only.
- 1) **Delay Between Messages**: Enter the length of time to delay between read and write scan line requests (ms).
- 2) **Response Timeout**: Enter the amount of time the gateway should wait before a timeout is issued for a read/write request (ms).
- 3) **Delay Between Connect Attempts**: Enter the amount of time the gateway should wait between attempts to connect to the PLC.
- 4) **Dependency Protocol**: If enabled, the Allen-Bradley PLC communication will stop if communication to the selected protocol is lost.
- 5) **Read High Priority**: Configures the number of high priority requests to process before switching to low priority requests. This number should be higher than the Read Low Priority.
- 6) **Read Low Priority**: Enter the number of low priority requests to process before switching to high priority requests. This number should be lower than the Read High Priority.
- 7) **Read All Data Points Once**: If Enabled, the gateway will read all configured data points once on startup regardless of priority, then begin processing requests based on priority after all points have been read once.

Allen-Bradley PLC Configuration	Help
Network Interface:	e: Ethernet Port 1 (192.168.1.133) V
Delay Between Messages:	s: 0 0-60000 ms
Response Timeout:	ut: 500 100-60000 ms
Delay Between Connect Attempts:	s: 1000 1000-60000 ms
Dependency Protocol:	Dl: None 🗸
Read High Priority:	y: 2 1-60000
Read Low Priority:	y: 1 1-60000
Read All Data Points Once:	e: 🗖
Save Par	Parameters



#### **External PLC Configuration**

The bottom area of the Allen-Bradley PLC Configuration page lets you configure up to five PLCs.

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.

Allen-Bradley PLC Device List	
	-Select- V Delete PLC
	<< 1 >>>
	1-2

- 1) To add additional PLCs, click the -Select- dropdown under Allen-Bradley PLC Device List and select Add Generic PLC option.
  - a) To remove a device, navigate to the server to delete using the << and >> buttons and click the **Delete PLC** button.
  - b) To create a new PLC with the same parameters already configured from another PLC, click the -Select- dropdown and select the Add from PLC X option (where X represents the PLC you wish to copy parameters from). Once created, you can make any additional changes needed to that new PLC.

**NOTE**: Auto-Configure Modes can ONLY be used in PLC 1.

2) To edit scan lines, you will need to go into Manual Configure Mode.

Allen-Bradley PLC Device List						
-Select-						
1-1						
Manual Config	ure 🗸					
Auto-Configure	Auto-Configure Group by Device					
Auto-Configure Group by Data Type						
	Allen Bredley BLC 1					
Device Label ETC01	IP Address 10.1.16.200					
Controller Slot 0 0-49	PLC Type CompactLogix V Update Type					
Comms Mode Connected (Class 3 Explicit) V						
Optimized Trigger Tag/File Name (16-Bit Int)						
# of Read Scan Lines 1 0-150	# of Write Scan Lines 1 0-150					
Gene	ate Scan Lines					

Real Time Automation, Inc.



#### External PLC Configuration: Auto-Configure

While in either of the two Auto-Configure modes, the number of scan lines and the actual scan lines themselves cannot be edited. Auto-Configure Mode looks at the other protocol and then configures the scan lines within the PLC to match. The PLC Tag/File Names and Data Types will be defined after the other protocol is configured.

If the PLC is a CompactLogix, ControlLogix or FlexLogix, the data will be configured according to the following rules:

- 1) Any 8 Bit Signed/Unsigned data will be mapped as **Sint**.
- 2) Any 16 Bit Signed/Unsigned data will be mapped as Int.
- 3) Any 32 Bit Signed/Unsigned data will be mapped as Dint.
- 4) Any 32 Bit Float and 64 Bit Float data will be mapped as **Real**.
- 5) Any Coils or 1 Bit Binary Packs will be mapped as **Bool (1 Bit)**.
- 6) Any Coils or 8/16/32 Bit Binary Packs will be mapped as Bit Array (32 bit).
- 7) Any String Data Types will be mapped as **String**.

If the PLC is a MicroLogix, SLC or PLC5E, the data will be configured according to the following rules:

- 1) Any 8 Bit Signed/Unsigned and 16 Bit Signed/Unsigned data will be mapped as Int.
- 2) Any 32 Bit Signed/Unsigned, 32 Bit Float, and 64 Bit Float data will be mapped as **Real**.
- 3) Any Coils or 1/8/16/32 Bit Binary Packs will be mapped as **Bit Array (16 bit)**.
- 4) Any String Data Types will be mapped as **String**.

Regardless of PLC type, the following is also true:

- 1) The read or write direction depends on whether it is configured as a read or write on the other protocol.
- 2) If the other protocol exceeds the number of Sint, Int, Dint, Real, Bool, Bit Array, or String data types the Allen-Bradley PLC supports (see limits on webpage), then nothing will be mapped. You will see the number of scan lines remain at 0 and the main page will display the following error:

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

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



## 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 Allen-Bradley PLC 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 Allen-Bradley PLC 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: 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



#### External PLC Configuration: Manual Configure Mode

- 1) To transition from either of the two Auto-Configure modes to Manual Configure Mode, click the dropdown in the middle of the Allen-Bradley Configuration page and select Manual Configure.
  - a) When prompted, click **OK** to confirm mode change or **Cancel** to remain in Auto-Configure Mode.



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

Message fr	om webpage
?	Press OK to modify the current Data Points. Press Cancel to Delete all Data Points.
	OK Cancel

- 3) To keep the scan lines that are already configured, press **OK**.
  - a) You would want this option if you are adding additional scan lines or you want to modify the scan line(s) that already exist.
- 4) To delete the scan lines that are already there and start over, press **Cancel**.
- 5) To add additional PLCs, click the -Select- dropdown under Allen-Bradley PLC Device List and select **Add Generic PLC** option.

Allen-Bradley PLC Device List	
	-Select- V Delete PLC
	<< 1 >>>
	1-2

- a) To remove a device, navigate to the server to delete using the << and >> buttons and click the **Delete PLC** button.
- b) To create a new PLC with the same parameters already configured from another PLC, click the -Select- dropdown and select the Add from PLC X option (where X represents the PLC you wish to copy parameters from). Once created, you can make any additional changes needed to that new PLC.
- 6) The **Enable** check box should be selected for the device.
- 7) Enter a **Device Label** to identify the device within the gateway.

Real Time Automation, Inc.



8) Enter the IP Address of the PLC, the Controller Slot (Integrated Ethernet, use Slot 0), and select the PLC Type. The Controller Slot is the slot where the controller is located, not the Ethernet card being used. These three parameters must match the PLC you are communicating to.

NOTE: ControlLogix Rev 32 is ONLY supported with CompactLogix 5380 and above and ControlLogix 5580 and above.

NOTE: When using GuardLogix PLCs select ControlLogix as the PLC Type. When connecting to GuardLogix PLCs the RTA Gateway will be unable to read or write safety tags.

- 9) Select the Comms Mode. Unconnected (UCMM) messaging relies on shared resources to transfer data to the PLC. This could result in message timeouts if there are a lot of devices fighting for these shared buffers. If you don't want the RTA gateway to constantly keep the connection open to the PLC but only maintain a connection when there is data needed to be transferred, then Unconnected (UCMM) will work best if you are only writing to the PLC. Connected (Class 3 Explicit) messaging relies on reserved resources to transfer data to/from the PLC. Connected (Class 3 Explicit) messaging is recommended if you are reading and writing and always want to keep that connection open to the PLC.
- 10) Enter an **Optimized Trigger Tag/File Name** to enable the triggering optimization that is available. The Optimized Trigger forces the 460ETC gateway to read ONLY the Optimized Trigger Tag until a value has a change of state. Please reference the <u>Optimized Trigger Guide</u> in the section below.
- 11) Enter the "# of Read Scan Lines" and "# of Write Scan Lines".
- 12) Click **Generate Scan Lines** to have the read and write scan lines auto generated for you. If you need to manually configure the read and write scan lines you can do so after they have been generated.

C Enable	Allen-Bradley PLC 1			
Device Label ETC01			IP Address	
Controller Slot 0 0-49			PLC Type CompactLogix ~ Update Type	
	Comms Mode Connected (Class 3 Explicit) 🗸			
Optimize	Optimized Trigger Tag/File Name (16-Bit Int)			
# of Read Scan Lines 0 0-150 # of Write Scan Lines 0			# of Write Scan Lines 0 0-150	
Generate Scan Lines				



#### Configuring Read and Write Scan Lines

Follow these steps to manually configure Read and Write Scan Lines.

#### 1) Click the View Read Scan Lines or View Write Scan Lines button.

	View Read Scan Lines View Write Scan Lines					
Write Sca	Write Scan Lines (460 to Allen-Bradley PLC)					
	Line #	Tag/File Name	Data Type	<b># of Points</b> *See Ranges Below		
	1		Int (16 Bit Int) 🗸	1		
		<< 1-1 >>				
	View Re	ad Scan Lines	View Write Scan L	ines		
Read Sca	an Lines (Alle	en-Bradley PLC to 460)				
	Line # Tag/File Name Data Type # of Points *See Ranges Below					
	1		Int (16 Bit Int) V	1		
<< 1-1 >>						

2) Enter the **Tag/File Name** that is set up within the PLC. If you are trying to access a tag that is defined in the Program Scope, please see the <u>Access Program Scope Tag</u> section below.

**NOTE:** If you are **ONLY** using Write Scan Lines, then the RTA gateway will not connect to the PLC until we receive valid data from the source. It's recommended you use **Unconnected** messaging so when the RTA gateway sends data to the PLC, we only send it once and close the connection until a Change of State. Leaving it at Connected messaging, once we receive data, the RTA gateway will constantly be writing to the PLC to maintain that connection.

- a) If you wish to start from a point other than the base, add [#] to the end of the Tag/File Name to specify which point is the starting point.
  - i) Example: A tag called "ReadTag" has dimension of 100 in the PLC. By default, we will start at point 0 of that array. Therefore, "ReadTag" and "ReadTag[0]" refer to the same point. To start from a different point, such as array index 27, enter in "ReadTag[27]" as the Tag/File Name in the gateway's scan line. This means the gateway will go to "ReadTag" and start at array index 27.
  - *ii)* If you wish to access a specific bit from any data type, you <u>must</u> use the Mapping Page's Set Bit math function. *You may not use ReadTag/0.0 to access bits.*

Real Time Automation, Inc.



1

- 3) Select the **Data Type** of the Tag/File.
- 4) Enter the **# of Points** you want to move from the PLC Tag/File to the gateway. See the *Scan Line Data Limit* section at the bottom of the page for the given max values.
  - a) If using a CompactLogix or ControlLogix, below are the scan line data limits.

Scan Line Data Limit		
	Data Type	Length Range
	Bool	1
	Bit Array	100
	Sint	400
	Int	200
	Dint	100
	Real	100
	String	1

b) If using a ControlLogix Rev 32 (CompactLogix 5380 or ControlLogix 5580), below are the scan line limits.

Data Type	Length Range
Bool	1
Bit Array	100
Sint	400
USint	400
Int	200
UInt	200
Dint	100
UDint	100
Real	100
String	1

c) If using Micrologix PLC, below are the scan line limits.

Scan Line Data Limit		
	Data Type	Length Range
	Bit Array	100
	Int	100
	Real	50
	String	1
	Long	50



d) If using a SLC 5/05 or PLC5E, below are the scan line limits.

Scan Line Data Limit		
	Data Type	Length Range
	Bit Array	100
	Int	100
	Real	50
	String	1

- 5) When configuring read scanlines there is an optional priority configuration. There are three priority selections available, how often each priority is read is configurable in the Allen-Bradley PLC Configuration section using the Read High Priority and Read Low Priority Configurations.
  - a) High: Read the scanline based on the Read High Priority configuration.
  - b) Low: Read the scanline based on the Read Low Priority configuration.
  - c) Once: Read the scanline once on gateway startup or upon a new connection and never again during normal operation.

Re	Read Scan Lines (Allen-Bradley PLC to 460ETCMC)						
		Line #	Priority	Tag/File Name	Data Type	# of Points *See Ranges Below	
		1	High 🗸	ETC01_N2G0_BIT1	Bool (1 Bit) V	1	
			High	<< 1-1 >>			
			Low				
			Once	Save Parameters			

- 6) Click the **Save Parameters** button.
- 7) Repeat for the other direction if needed.



#### Access Program Scope Tags

There are two different types of tags in the PLC: Controller Scope tags and Program Scope tags. With Controller Scope tags, these tag names can be entered into the gateway without any additional syntax. If you are using a tag that is defined within Program Scope, then the tag name inside of the RTA gateway needs additional syntax for it to successfully communicate.

Example: "AnotherTag" is created in the Program Scope called "AnotherProgram".



To access this Program Scope tag within the RTA 460, you must use the following syntax:

Tag Name = "PROGRAM:ProgramName.TagName" where Program Name = Scope name & TagName = Actual Tag Name, Data type will vary.

Line #	Tag/File Name	Data Type	<b># of Points</b> *See Ranges Below		
1	PROGRAM:Anotherprogram.Anothertag	Dint (32 Bit Int)	1		
<< 1-1 >>					



## **Optimized Trigger Guide**

The Optimized Trigger forces the 460ETC gateway to read ONLY the Optimized Trigger Tag until the trigger value has a change of state. Once there is a change of state then it will mark **ALL** ETC Read Scan Lines "Invalid", then will execute a read for all ETC Read Scan Lines until **ALL** read data is valid. Once all Read Scan Lines have been read and marked valid, it will set the ETC Handshake **#** to the value of ETC Optimized Trigger. You will be able to utilize the ETC Handshake **#** to map over to any of the Technology Triggers and/or as a Handshake Reference.

**Note**: **#** represents the Allen-Bradley PLC **#** on the Allen-Bradley configuration page of the gateway, if you only have 1 PLC configured your **#** is 1

If you have a timeout and we are not able to read a particular Read Scan Line, then you will stay in a loop of trying to make sure all data is valid before setting the Handshake value equal to Trigger value.

## How does this work?

- 1) Read ETC Optimized Trigger tag until Change of State.
  - a. Value 0 = Enabled but Not valid value
  - b. Value 65535 = Disabled
- 2) Map the ETC Optimized Trigger (Source) over to ETC Trigger # (Dest).
- 3) If ETC Trigger # value changes states, mark all ETC Read Scan Lines "Invalid".
- 4) Read all ETC Read Scan Lines until ALL source read data is valid.
- 5) ETC Handshake # value is set equal to ETC Trigger 0 value.
- 6) Map ETC Handshake # to protocol 2 Technology Trigger (A/USB/TCP/WI) and/or reference data point.

#### How do you set this up?

There are 2 options below to synchronize all data when sending data over to protocol 2.

## Option 1: Sends data every trigger no matter if it's new or not

We'll be using an 460ETCA for this example, this will utilize the ETC Optimization Trigger and the Technology Trigger (A/USB/TCP/WI) for ASCII (A).

- 1) Configure all your Read Scan Lines your looking to send over to your ASCII device.
- Within the ETC configuration, setup a PLC tag that you can identify as your Optimization Trigger.
   \*Optimized Trigger tag can be unique to your PLC program\*

Optimized Trigger Tag/File Name (16-Bit Int) RTA\_Opt\_Trigger



3) In the Data Mapping page, manually add 2 additional mappings identical to the example below.

C Enable	Mapping 1				
Source	Enable Manipulation	Destination			
Group: ETC01 RTA_Opt_Trigger (Int1 V) Start: RTA_Opt_Trigger V End: RTA_Opt_Trigger V	• • • • •	Group: ETC Trigger 0 (Uint16)  Start: Trigger 1  End: Trigger 1			
C Enable	Mapping 2				
Enable     Source	Mapping 2	Destination			

- 4) Update all your Read Scan Line PLC tags with data.
- 5) Nothing should have updated in your ASCII device.
- 6) Update the RTA\_Opt\_Trigger PLC tag to 1.

Þ	RTA_Opt_Trigger	1
---	-----------------	---

- 7) Now your ASCII device will be updated with the data.
- 8) Increment the RTA\_Opt\_Trigger PLC tag
- 9) Your ASCII device will get update again, regardless if data is new or not.

#### If your product is a Web Interface e.g. 460ETCWI acting only as a Client:

1) On the WI configuration page change the Update Method to be Triggered.

Update Method Triggered >

2) In the Data Mapping page, manually add 2 additional mappings identical to the example below.

C Enable	Mapping 1			
Source	Enable Manipulation	Destination		
Group: ETC01 RTA_Opt_Trigger (Int1		Group: ETC Trigger 0 (Uint16)		
Start: RTA_Opt_Trigger		Start: Trigger 1 🗸		
End: RTA_Opt_Trigger		End: Trigger 1		
Enable Mapping 2				
Source	Enable Manipulation	Destination		
Group: ETC Handshake 0 (Uint16) 🗸		Group: WI Upload Trigger (Uint16) 🗸		
Start: Handshake 1		Start:		
		Vian.		



## Option 2: Sends data ONLY on Change of State

We'll be using an 460ETCA for this example, this will utilize the ETC Optimization Trigger and a Write Scan Line for a handshake so that the PLC knows the triggering functionality is working.

\*If using the WI (Web Interface 460ETCWI) then use the WI Upload Trigger in your destination mapping\*

- 1) Configure all your Read Scan Lines your looking to send over to your ASCII device.
- 2) Configure a Write Scan line that updates the PLC with the Handshake from the RTAgateway.

#### \*Handshake tag can be unique to your PLC program\*

Write S	Vrite Scan Lines (460ETCA to Allen-Bradley PLC)				
	Line #	Tag/File Name	Data Type	<b># of Points</b> *See Ranges Below	
	1	RTA460_OPT_Handshake	Int (16 Bit Int) 🗸	1	
	<< 1-1 >>				

Within the ETC configuration, setup a PLC tag that you can identify as your Optimization Trigger.
 \*Optimized Trigger tag can be unique to your PLC program\*

Optimized Trigger Tag/File Name (16-Bit Int) RTA\_Opt\_Trigger

4) In the Data Mapping page, manually add 2 additional mappings identical to the example below.

Enable	Mapping 1		
Source	Enable Manipulation	Destination	
Group: ETC01 RTA_Opt_Trigger (Int1 Start: RTA_Opt_Trigger End: RTA_Opt_Trigger		Group: ETC Trigger 0 (Uint16)  Start: Trigger 1  End: Trigger 1	
Enable Mapping 2			
	11 5		
Source	Enable Manipulation	Destination	

- 5) Update all your Read Scan Line PLC tags with data.
- 6) Nothing should have updated in your ASCII device.
- 7) Update the RTA\_Opt\_Trigger PLC tag to 1.

▶ RTA\_Opt\_Trigger

- 8) Now your ASCII device will be updated with the data.
- 9) Increment the RTA\_Opt\_Trigger PLC tag
- 10) The ASCII device should NOT be updated because the data is not new.
- 11) Update your Read Scan Line tag with new data. Real Time Automation, Inc. 30

1



- 12) Increment the RTA\_Opt\_Trigger PLC tag again
- 13) Now your ASCII device will be updated with the new data.
- 14) In a working application the Handshake tag in your PLC should match the Optimization Trigger tag.

RTA_Opt_Trigger	5	
<ul> <li>RTA460_OPT_Handshake</li> </ul>	5	



## **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.

MQTT Client Connection List		
-Select-	Delete Connection	
	< 1 >>	
	1-1	

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.

MQTT Client Connec	tion List		
	-Select-		Delete Connection
	-Select-	1	>>
	Add Generic MQTT Connection	5	1

- 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** or **URL**, 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** to be used when connecting to the Broker.
- 9) Check the **Add Timestamp to Publishes** checkbox to add a timestamp to the published JSON payloads.
- 10) Username and Password: Enter if authentication to the MQTT broker is necessary.

Enable	MQ	FT 1
Device L	abel QT01	Network Interface Ethernet Port 1 (192.168.1.104)
Broker IP / URL		
Client ID		Add Timestamp to Publishes
TCP Port 1883	1-65535 (Default: 1883)	Keep Alive 60 0-200 sec (0 to Disable)
Username		Password

#### **Configuring Subscribe and Publish Topics**



#### **JSON Name/Value Pairs**

Line #	Path	JSON Name	JSON Point Type
1	-No Path Defined-		INT (8-bit) V
2	-No Path Defined-		INT (8-bit) V
3	-No Path Defined-		INT (8-bit) ~
		<< 1-3 >>	

Save Parameters

View Publish Paths

```
View Subscribe Paths
```

#### Publish Paths (460ETCQT to MQTT)

Line #	Enable	Path Name
1		
		<< 1-1 >>

- 11) Enter in "# of Subscribe Paths" and/or "# of Publish Paths".
- 12) Enter in "# of JSON Name/Value Pairs"
- 13) Click the **Generate Paths** button to have the lines generated for you.
- 14) **# of Subscribe Paths:** 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.

Real Time Automation, Inc.



- 15) **# of Publish Paths:** Enter the number of topics to publish to the broker from the mating protocol.
- 16) # of JSON Name/Value Pairs: Enter the number of JSON name/value pairs to configure, each
- name/value pair can be associated with a single publish or subscribe path.
- 17) Select the publish or subscribe path each name/value pair should be associated with.
- 18) Select the **Point Type** of the name/value pairs
- 19) Click Save Parameters button when complete.



#### 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.

	-Select-	Delete Connection     << 1 >>     1-1
MQTT Client C	Connection List	Delete Connection

Add Generic MQTT Connection

Add Generic AWS Connection

-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: <u>https://aabb11224e9ex-</u> 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** to be used when connecting to the Broker.
- 9) Check the Add Timestamp to Publishes checkbox to add a timestamp to the payload.

Enable	AWS 1		
Device L	_abel QT01	Network Interface Ethernet Port 1 (192.168.1.104)	
Device Shadow URL			
Client ID		Add Timestamp to Publishes	
TCP Port 8883	1-65535 (Default: 8883)	Keep Alive 60 0-200 sec (0 to Disable)	



#### Additional AWS Requirements

There are five 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) A root certificate to authenticate the connection. Specifically, the **Starfield Class 2 Certification Authority Root Certificate** is required. This can be obtained from:
  - Starfield techs certificate repository: <u>https://certs.starfieldtech.com/repository</u>
  - or a direct download link here: <u>https://certs.starfieldtech.com/repository/sf-class2-</u> root.crt
- 4) The private key, certificate, and root certificate will need to be FTP'd into the RTA gateway's Flash File System.
- 5) The time configuration will need to be set to the current date and time to establish a connection. This can be done in one of two ways:
  - The date and time can be set manually; however, this will need to be set again any time the gateway experiences a power loss or reboot.
  - $\circ$   $\;$  The date and time can be set automatically by utilizing an NTP server.
  - Both options can be configured by navigating to Other > Time Configuration on the gateway's webpage.

#### 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.


🐂   🕑 🏢 🖛   File Ex	plorer			- ×
File Home Sh	are View			~ 😗
	Quick access >		V 🖉 Search Quick access	٩,
🖈 Quick access		> Frequent folders (4)		
늘 Desktop	*			
🔈 Downloads	*		Mindawa 10	
Documents	*		vvindows 10	
The Pictures	*			

🛛 🔀 🖡 Libraries 🕨		<ul> <li>✓ 4→ Search Libraries</li> </ul>					3
Organize 👻 New library		-			≡ •	61	6
🔆 Favorites 🧊 Libraries	Libraries Open a library to see your files	and arrange them by folder, date, and	l other properties.				
E Desktop	Name	Date modified	Type	Size			
in Downloads		Windows 7	7				

- 4) In the address bar (within the red box shown above) type <u>ftp://xxx.xxx.xxx</u> (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.

	-Select-
OTH	ER
	-Select-
	-Select-
	Setup LED's
	Export / Import Config
	Export / Import Template
	Utilities
	Time Configuration
	Email Configuration
	Security Configuration
	Alarm Configuration
	COS Configuration

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

Revisions	Listing of Revisions
File List	File List
Identify Device	Start Flashing LED's

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





## 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".

aws Services ▼				
AWS IoT	×			
Monitor Activity		AWS IOT > Policies Policies		Create
► Connect		Search policies	Q	
Manage		Name		
► Fleet Hub				
Greengrass				
<ul> <li>Secure</li> <li>Certificates</li> <li>Policies</li> </ul>				
CAs				
Role Aliases Authorizers				



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 *a lot* 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".

Create a policy	
Create a policy to define a set of authorized actions. You can authorize actions on one or more about IoT policies go to the AWS IoT Policies documentation page.	more resources (things, topics, topic filters). To learn
Name	
RTA_Testing	
Add statements	
Policy statements define the types of actions that can be performed by a resource.	Advanced mod
Action	
iot:Connect	
Resource ARN	
arn:aws:lot:us-east-2: 5:client/*	
Effect	
Allow Deny	Remove
Add statement	
	Create

Real Time Automation, Inc.



AWS IoT Core Service Things Configuration	aws Services 🔻	
	AWS IoT ×	<
Back at the main menu on the left pane, click on the "Manage" menu option, and then the "Things" submenu.	Monitor Activity	
	<ul> <li>Manage</li> <li>Overview</li> <li>Things</li> </ul>	
AWS IoT > Manage > Things	1360	
Things (1) Info       An IoT thing is a representation and record of your physical device in the cloud. A physical device needs a thing record in order to work with AWS IoT.       C       Advanced search         Q       Filter things by: name, type, group, billing, or searchable attribute.       C       C	Run aggregations Edit Delete Create thin	gs ©
Name     Thing type		

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".

AWS IoT > Manage > Things > Create things				
Create things 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.				
Number of things to create         Create single thing         Create a thing resource to register a device         Provision the certificate and policy necessary to allow the device to connect to AWS loT.				
Create many things Create a task that creates multiple thing resources to register devices and provision the resources those devices require to connect to AWS IoT.				
Cancel				

Real Time Automation, Inc.



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 thing resource is a digitates esource in the registry to	I properties Info al representation of a physical device or logical entity in AWS IoT. Your device or entity needs a thing use AWS IoT features such as Device Shadows, events, jobs, and device management features.				
Thing properties	Info				
Thing name					
Enter_name					
Enter a unique name conta	Enter a unique name containing only: lett rs, numbers, hyphens, colons, or underscores. A thing name can't contain any spaces.				
Additional configue You can use these configue	urations rations to add detail that can help you to organize, manage, and search your things.				
Thing type - option	nal				
Searchable thing attributes - optional					
Thing groups - opt	ional				
Billing group - opt	ional				

#### 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.
O 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".

Attach policies to certificate – <i>optional</i> Info AWS IoT policies grant or deny access to AWS IoT resources. Attaching policies to the device certificate applies this access to the device.			
<b>Policies</b> (1/1) Select up to 10 policies to attach to this certificate.	C Create policy		
<b>Q</b> Filter policies	< 1 > ©		
✓ Name			
RTA_Testing			
Can	cel Previous Create thing		

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.

Download certificates a	and keys	×
Download certificate and key f AWS.	iles to install on your device so t	that it can connect to
Device certificate You can activate the certificate now AWS IoT.	, or later. The certificate must be acti	ve for a device to connect to
Device certificate 2.pem.crt	Deactivate certificate	e ➡ Download
Key files The key files are unique to this certi Download them now and save them	ficate and can't be downloaded after i in a secure place.	you leave this page.
A This is the only time you	u can download the key files for	this certificate.
Public key file	public.pem.key	☑ Download
Private key file	-private.pem.key	🕑 Download

Real Time Automation, Inc.



⊘ You successfully created certificate b462a278b65d7223f9ae2302837792e05	
AWS IoT > Manage > Things	
Things (1) Info An IoT thing is a representation and record of your physical device in the cloud. A physical device needs a thing record in order to work with AWS IoT.	C
<b>Q</b> Filter things by: name, type, group, billing, or searchable attribute.	
Name	Thing type
RTA_Testing	-

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.

Thing details				
Name				1
RTA_Testing				-
ARN				E
Attributes	Thing groups	Device Shadows	Interact Activit	ty Jobs
Certificates (1) Info				
Certificates (1) Info The device certificates attached to	this thing resource.			

Real Time Automation, Inc.



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".

Attributes Certifi	cates Thing groups Device Shadows Interact	:	
Device Shadows (( Device Shadows allow conn delete the state information	D) Info ected devices to sync their state with AWS. You can also get, update or n about this thing's Device Shadows by using HTTPS and MQTT topics.	C Delete	Create Shadow
Q Filter Device Shade	JWS		< 1 > @
Name	▲ MQTT topic prefi	K	
	No Device Shadows This thing resource doesn't have any Device Shadows. Create Shadow		

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

Create Device Shadow		×
<ul> <li>Named Shadow</li> <li>Create multiple Device Shadows with different names to manage access to group your device properties.</li> </ul>	properties, and log	ically
<ul> <li>Unnamed (classic) Shadow</li> <li>A thing can have only one unnamed (classic) Shadow.</li> </ul>		
Device Shadow name		
RTA_Testing_Shadow		
Can	cel Creat	e

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  ARN  MQTT topic prefix  Saws/things/RTA_Testing/shadow/name/RTA_Testing_Shadow	
Device Shadow URL	dow?

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 grou	ps Device Shadows Interact Activity Jobs Alarms
Device Shadows (1) Info Device Shadows allow connected devices to sync their s	state with AWS. You can also get, update or
delete the state information about this thing's Device S           Q         Filter Device Shadows	hadows by using HTTPS and MQTT topics.
Name	▲ MQTT topic prefix
RTA_Testing_Shadow	日 \$aws/things/RTA Testing/shadow/name/RTA Testing Sha

Real Time Automation, Inc.



## **Testing AWS Communication**

Once you have the AWS IoT Core service configured, you can use their "MQTT test client" feature to Publish a topic to the RTA gateway and view published data.

AWS IoT ×	AWS IoT > MQTT test client
Monitor	MQTT test client Info You can use the MQTT test client to monitor the MQTT messages being passed in your AWS account. Device
Connect Connect one device	communicate their state to AWS IoT. AWS IoT also publishes MQTT messages to inform devices and apps of topics and publish MQTT messages to topics by using the MQTT test client.  Subscribe to a topic Publish to a topic
Connect many devices	Topic filter Info The topic filter describes the topic(s) to which you want to subscribe. The topic filter can include MQTT wildcard characters
Test <ul> <li>Device Advisor</li> </ul> MQTT test client	Enter the topic filter  Additional configuration  Subscribe
Device Location New	

**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.

	Enable				AW	'S 1					
		Device Label QT01 Network Interface Ethernet Por					Port 2	2 (DHCP Assign	ed)		
	Device Shadow URL										
	Client ID RTA_Thing										
	TCP	CP Port         8883         1-65535 (Default: 8883)         Keep Alive         60         0-200				200 s	sec (0 to Disa	ble)			
			# of	JSON Nam	e/Value	e Pairs 1	0-5	00			
		# of Publish	Paths 1	0-250		# of S	ubsc	ribe Paths	s 1	0-250	
					Generat	e Paths					
JS	ON Nam	e/Value P	airs								
	Line #		Path			JSON N	ame			JSON Poin	t Type
	1										
	•	Data_From_	_RTA_2_AWS	~	messa	ge				INT (16-bit)	~
		Data_From_	_RTA_2_AWS	~	messa	ge -1 >>				INT (16-bit)	~
		Data_From_	RTA_2_AWS	✓ S	messa << 1- Save Par	ge -1 >> rameters	[	View Subso	cribe	INT (16-bit) Paths	~
Su	bscribe	Data_From_ View	RTA_2_AWS Publish Paths QTT to 460E	S TCQT)	messa << 1- Save Par	ge 1 >> ] ameters		View Subso	cribe	INT (16-bit) Paths	
Su	bscribe Line #	View Paths (MC Enable	RTA_2_AWS Publish Paths QTT to 460E	s TCQT)	messa << 1-	ge 1 >> rameters Path Nam	18	View Subso	cribe	INT (16-bit) Paths	~
Su	bscribe Line #	View Paths (MC Enable	RTA_2_AWS Publish Paths QTT to 460E	v s_2_rta	messa << 1-	ge 1 >> ameters Path Nam	16	View Subso	cribe	INT (16-bit) Paths	▼

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.



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

Topic name The topic name identifies the message. The message payload will be published to this topic with a Quality of Servi Q Data_From_AWS_2_RTA Message payload { "message": 1234 } Additional configuration	ce (QoS) of 0.
Q Data_From_AWS_2_RTA  Message payload  {     "message": 1234 } Additional configuration	×
Message payload { "message": 1234 } Additional configuration	
{     "message": 1234 } Additional configuration	
Additional configuration	
Publish	
Data	Edit Map

Display Data				Edit Map	ping Text
Select a Device AW	/S Connection	✓ View			
Ν	IQTT 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			<b>^</b>

#### 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.



Enable	AM					
Device L	abel QT01	Network Interface	Ethernet Port 2 (DHCP Assigned) 🗸			
Device Shado	Device Shadow URL					
Client ID RTA_Thing						
TCP Port 8883	1-65535 (Default: 8883)	Keep Alive 60	0-200 sec (0 to Disable)			
# of JSON Name/Value Pairs 1 0-500						
# of Publish	Paths 1 0-250	# of Subso	ribe Paths 1 0-250			
	Genera	te Paths				

#### **JSON Name/Value Pairs**

	Line #		Path		JSON Name	Ð	JSON Point T	Гуре	
	1	Data_From	_RTA_2_AWS ~	·	Data		INT (16-bit)	~	
	<< 1-1 >>								
Pu	Save Parameters View Publish Paths View Subscribe Paths Publish Paths (460FTCQT to MQTT)								
	Line #	Enable			Path Name				
	1		Data_From_RTA_2_AWS	S					
	<< 1-1 >>								
2									

	PLC		460ETCQT →→		MQTT	
Name	Valı	ue (Hex)	Manipulation	n Name	Value (He	x)
PLC_Data_2_AWS	111	0x006F	<b>→</b> →	QT01 Data_From_RTA	_2_AWS 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\_RTA\_2\_AWS" is the Publish Topic name configured in the AWS device configuration page of the RTA.



Subscribe to a to	pic Publish to a topic	
Topic filter Info The topic filter describes t # ► Additional configu Subscribe	he topic(s) to which you want to subscribe. The topic filter can include MQTT wildcard characters.	
Subscriptions	#	Pause Clear Export Edit
# ♡×	▼ RTA/Data From RTA 2 AWS	October 05, 2021, 11:33:42 (UTC-0500)
4	{ "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.

MQTT Explorer     Application Edit View					- 🗆 ×
	Q Search	1		DISCONNE	ст 💩 🙏
▼ 10.1.16.16 ▶ \$SYS (37 topics, 139 messages)			Topic 🖺 🧂		^
			Value		^
			► History		
			Publish		^
			Topic \$SYS		×
			raw xml	json	
			0 0		PUBLISH

Next, you can configure the RTA gateway. The broker IP address listed below is set up to be the IP of the machine where the broker is installed.

C Enable	MQ	TT 1			
Device L	abel QT01	Network Interface Ethernet Port 1 (192.168.1.26)			
Broker IP / U	URL 10.1.16.16				
	Client ID RTA_Thing				
TCP Port 1883	1-65535 (Default: 1883)	Keep Alive 60 0-200 sec (0 to Disable)			
Username		Password			
# of JSC 0-256 characters e Pairs 2 0-500					
# of Publish	Paths 1 0-250	# of Subscribe Paths 1 0-250			
	Generat	re Paths			

53

Real Time Automation, Inc.



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

JS	ON Name	e/Value P	airs							
	Line #		Path			JSON I	Name	JS	ON Point Ty	ре
	1	PLC_Data_2	2_Explorer	~	Data			INT	(8-bit)	•
					<< ]1-1	>>				
	Save Parameters									
	View Publish Paths View Subscribe Paths									
Su	Subseribe Beths (MOTT to 460ETCOT)									
Uu	l ine #	Enable		(1)		Path Na	me			
	1		PLC Data 2 Explor	or		Taurna				
					<<_1-1	>>				
			PL C		460	ETCQT		MC	דדר	
			FLC		-	<b>&gt;→</b>		IVIC		
	Name		Value (Hex)		Mani	pulation	Name		Value (He	ex)
PL	.C_Data_2	_Explorer	123	0x007	7B	<b>→</b> →	PLC_Data_2_Exp Data	olorer	123	
This pub	This example shows a PLC writing data to the RTA gateway and presenting that data to the MQTT publish topic.									

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\_RTA 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	Valu	e (Hex)	Manipulation	Name	Value (Hex)
ETC01_G2N0_INT	2328	0x0918	<b>←←</b> Da	QT01 ta_From_Explo	rer_2_RTA 2328



### Microsoft Azure Service Setup

Please note this section outlines the bare minimum configuration to get the RTA gateway connected to Azure and is not necessarily a recommended configuration in a production environment.

- 1. Create a Microsoft Azure subscription if you do not have one already
- 2. Create a resource group
  - a. In the search bar at the top type in "Resource Groups" and select the resource groups under services to navigate to the resource groups page.
  - b. Hit Add in the top left corner, there may also be a create resource group button in the middle if no resource groups exist.

🔨 Subscriptions - Microsoft Azi	re 🗙 🔼 Resource groups - Microsoft Azure 🗙 🕂				- 0 ×
d D C D	portal.azure.com/?fromAccountsPortal=true#blade/HubsExtension/B	IrowseResourceGroups		1 🔍 🔺	•
Microsoft Azure	● Upgrade P Search resources, services, and docs (G+/)		⊡ <b>₽</b> ₽ ⊗		
Home >					
Resource group	S ☆				×
🕂 Add 🕲 Manage view	V 💟 Refresh 🚽 Export to CSV 😵 Open query   🕲 Assign tag	s 🛛 🛇 Feedback			
Filter by name	Subscription == all Location == all X <sup>+</sup> Y Add filter				
Showing 0 to 0 of 0 records.			No grouping	~ [ L	ist view 🗸
Name 1.		Subscription 14	Locatio	n ↑↓	
	No resource Try changing your fitters if you Lea Create re	groups to display u dont see what youre looking for. m more of source group			

c. In the create a resource group window give the resource group a name, the available Azure subscription should be selected by default.



Home > Resource groups >						
Create a resource group						
Basics Tags Review + create						
Resource group - A container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization. Learn more B						
Project details						
Subscription * 🕡	Azure subscription 1					
Resource group * ①	rta-resource-group-1					
Resource details						
Region * 🕕	(US) East US 🗸					
Review + create < Previous	Next : Tags >					

- d. Hit Review + Create in the bottom left corner.
- e. In the review window, hit create in the bottom left corner to create the resource group.
- f. You should be re-directed back to the resource groups window where you can see the newly created resource group is listed.
- 3. Create an IoT Hub
  - a. In the search bar at the top type in "IoT Hub" and select the IoT under services to navigate to the IoT Hub page.

Microsoft Azure 💿 🔎	int hub			
	02 road	× 🔉	; 🖉 🐵 ? 😊 📒	DEFAULT DIRE
Azure services + Create a resource Navigate Subscriptions Tools	ervices	See all Marketplace I to T Hub Crosser Iot Connectivity & St Documentation Azure IoT Hub Documentation   Introduction to Azure IoT Hub J Azure IoT Hub support for virtua Azure IoT Hub high availability a Resource Groups No result	ienvice eaming Analytics See all Microsoft Docs Alcrosoft Docs Inetworks   Microsoft Docs nd disaster recovery	→ pre services
Microsoft Learn s Learn Azure with the training from Micro	No results were found. earching all subscriptions. Change e online Monitor your apps and soft infrastructure	Secure your apps and infrastructure	Analyze and optimize you cloud spend for free	r
Useful links			Azure mobile app	
Technical Documentation of Azure Migration Tools	Azure Services g <sup>*</sup> Find an Azure expert	Recent Azure Updates (3" Quickstart Center	Commented on the App Store Googe	e Play

a. Hit Add in the top left corner, there may also be a create IoT Hub button in the middle if no IoT Hubs exist.



b. Select the resource group created previously, enter a name for the hub, and select a region.

oT hub … <sup>Iicrosoft</sup>		
Basics Networking Manag	ement Add-ons Tags Review+create	
Create an IoT hub to help you conr	nect monitor, and manage billions of your IoT assets	. Learn more ⊡"
Project details		
Choose the subscription you'll use organize and manage resources.	to manage deployments and costs. Use resource gr	oups like folders to help you
Subscription * 🕕	Azure subscription 1	~
Resource group * (i)	rta-resource-group	
2 .	Create new	
Instance details		
IoT hub name * i	rta-test-hub-1	N
Region * 🛈	East US	~
	Standard (most popular)	~
Tier *	Compare tiers	
Tier *	compare tiers	
Tier * Daily message limit * 🛈	400,000 (\$25/month)	~

- c. Hit Next at the bottom of the page to proceed to the networking tab.
- d. In the networking tab under connectivity configuration, ensure public access is selected.



- e. Hit review and create in the bottom left corner of the page.
- f. On the review and create page, hit create in the bottom left corner of the page.



g. One the deployment is completed click on "Go to Resource" to be re-directed to the newly created IoT Hubs overview page. If go to resource is not an option, navigate to the IoT hub and select your newly created IoT hub to access the overview page.

rta-test-hub			×
₽ Search ○ «	$ ightarrow$ Move $\sim$ 🔋 Delete 🖒 Refresh 🖗 Feedback		
💦 Overview	↑ Essentials		JSON View
Activity log	Resource group (move) : rta-resource-group	Hostname : rta-t	est-hub.azure-devices.net
Access control (IAM)	Status : Active	Tier : Free	
🗳 Tags	Location : East US	Daily message limit : 8,000	0
X Diagnose and solve problems	Service region : East US	Minimum TLS Version : 1.0	
Events	Subscription (move) : Azure subscription 1		
Prevents	Tags (edit) : Add tags		
Device management	See more		
Devices	Usage Get started		
IoT Edge		Show data for last (1 Hours 6 Hours 12 Hours 10 Door) 7 Door	20 Days
Configurations + Deployments		THOUR O HOURS 12 HOURS 12 HOURS 12 HOURS 12 HOURS	so bays
🧼 Updates			
🔎 Queries	IoT Hub Usage	Number of messages used	Device to cloud messages
> Hub settings			100
> Security settings	<ul> <li>Massages used todays 2</li> </ul>	2	90
> Defender for IoT	messages used today. 2		80
Monitoring	Daily messages quota: 8000 ①	15	60
> tutomoting		1	40
Automation	IoT Devices: 2		30
> Help		03	10
		0	0
		6 PM Oct 18 6 AM UTC-05:00	6 PM Citt 18 6 AM UTC-05.00
		Total number of messages used (Max), rta-t   2	Telemetry messages sent (Sum), rta-test-hub   0

- h. In the left panel of the IoT Hub overview select Devices under the Device Management section.
- i. Click Add Device button in the top left corner of the page to create a new IoT device in this hub.
- j. In the create a device window enter a name for the device in the Device ID section and ensure the "Connect his device to an IoT hub" option is enabled.

Home > Io1 Hub >	ta-test-hub   De	vices >		
🕂 Create a	device			
-				
i Find Certified for	Azure IoT devices in	1 the Device Catalo	g	
Device ID * 🕕				
rta-test-device-1				
loT Edge Device				
Authentication type ③				
Symmetric key X.5	09 Self-Signed	X.509 CA Signed	)	
Auto-generate keys 🛈	)			
$\checkmark$				
Connect this device to	an IoT hub 🕕			
Enable Disable				
Parent device 🕕				
No parent device				
Set a parent device				

- k. Hit Save in the bottom left corner of the window to create the device and be re-directed to the device list in the IoT Hubs overview window.
- I. Click on the newly created device in the device list to view the devices configuration.



# m. Copy the Primary connection string for the device, this will be used when connecting the RTA gateway to Azure.

Home > IoT Hub > rta-test-hub   D	ome > IoT Hub > rta-test-hub   Devices >										
rta-test-device ☆ … <sup>rta-test-hub</sup>	ta-test-device 🖈 … a-test-hub										
🗟 Save 🔍 Manage keys 🗸 🖂	🖩 Save 🔍 Manage keys 🗡 🖂 Message to Device 💉 Direct method 🕂 Add Module Identity 🗮 Device twin 🖒 Refresh										
Device ID ①	rta-test-device				D						
Primary key 🛈	•••••	•••••		0	D						
Secondary key 🕕	•••••	•••••		•	D						
Primary connection string 🛈	•••••	•••••		•	D						
Secondary connection string 🛈	•••••	•••••		•	D						
Tags ( <u>edit</u> )	No tags										
Enable connection to IoT Hub 🛈	Enable O Disable										
Parent device 🛈	No parent device										
Module Identities Configurations											
Module ID	Connection State	Connection State Last Updated	Last Activity Time (UTC)								
There are no module identities for this o	device.										



- 4. Create an Event Hub
  - a. In the search bar at the top type in "Event Hubs" and select the Event Hubs under services to navigate to the Event Hubs page.
  - b. Hit Add in the top left corner, there may also be a create Event Hub button in the middle if no Event Hubs Namespaces exist.
  - c. In the Create Namespace window, select your previously created resource group, enter a name for the namespace, and select a pricing tier based on your needs.

Home > Event Hubs >		
Event Hubs		
Basics Advanced Networking	Tags Review + create	
Project Details		
Select the subscription to manage depl manage all your resources.	loyed resources and costs. Use resource groups like folders to a	organize and
Subscription *	Azure subscription 1	$\sim$
Resource group *	rta-resource-group	$\sim$
	Create new	
Instance Details Enter required settings for this namesp	pace, including a price tier and configuring the number of units (	capacity).
Namespace name *	rta-test-namespace-1	~
	.serviceb	ous.windows.net
Location *	East US	$\sim$
	The region selected supports Availability zones. Your namespa Availability Zones enabled. <u>Learn more.</u>	ce will have
Pricing tier *	Basic (~\$11 USD per TU per Month)	$\sim$
	Browse the available plans and their features	
Throughput Units *	0	1
Review + create < Previous	Next: Advanced >	

- d. Hit Review + Create in the bottom left corner of the page.
- e. Hit Create in the bottom left corner of the page to create the namespace.



f. Once the namespace has finished initializing click on go to resource to navigate to the namespaces main panel. If go to resource in not an option navigate to Event Hubs and select the newly created namespace to open the main panel.

Event Hubs Namespace	☆ ☆ …				×
P Search	🕂 Event Hub 📋 Delete 💍 Refresh 🛛 🖗 Give feedback				
🗵 Overview	↑ Essentials				JSON View
Activity log	Resource group (move) : rta-resource-group		Created	: Monday, February 5, 2024 at 13:10:12 CST	
Access control (IAM)	Status : Active		Updated	: Monday, February 5, 2024 at 13:11:02 CST	
🗳 Tags	Location : East US		Zone Redundancy	: Enabled	
X Diagnose and solve problems	Subscription (move) : Azure subscription 1		Pricing tier	: Basic	
	Subscription ID : 4f0bf630-94d0-4b0b-b594-fccd8aa31dff		Throughput Units	: <u>1 unit</u>	
Data Explorer (preview)	Host name : rta-test-namespace.servicebus.windows.n	et 🗅	Auto-inflate throughput	: Not Supported	
Events			Local Authentication	: Enabled	
> Settings	Tags (edit) : Add tags				
> Entities	NAMESPACE CONTENTS KAFKA SURFACE ZONE REDUNDANCY				
> Monitoring	1 EVENT HUB NOT SUPPORTED ENABLED				
> Automation	Show data for the last:	7 days 30 days			
> Help		, adjs 50 adjs			
	Requests	Messages		Throughput	
		90		908	
		80		808	
	0.8	70		708	
	0.6	50		508	
	04	40		408	
				308	
	0.2	10		108	
		0		80	
	11:45 AM 12 PM UTC-05:00	11:45 AM 12 PM	ut-namernace 0	Incoming Bider (Sum) datert-namernace OP	016-0200
	1/2 Successful Requests (Sum), rta-test-namespace 1	1/2 Outgoing Messages (Sum), rta-te	st-namespace 0	Outgoing Bytes. (Sum), ita test namespace OB	
	Server Errors. (Sum), rta-test-namespace 0	Captured Messages. (Sum), rta-ti	st-namespace 0	Captured Bytes. (Sum), rta-test-namespace 0B	

- g. Click Add Event Hub in the top left corner.
- h. Enter in a name for the event hub
- i. Click review + create in the bottom left corner.
- j. On the review page hit create in the bottom left corner.

Home > Event Hubs > rta-test-namespace >	
Create Event Hub	
Basics Capture Review + create	
Event Hub Details	
Enter required settings for this event hub, in	ncluding partition count and message retention.
Name * 🕕	rta-test-hub-1
Partition count 🕕	01
Retention	
Configure retention settings for this Event H	lub. Learn more
Cleanup policy 🛈	Delete ~
Retention time (hrs) * 🛈	1 🗸
	min. 1 hour, max. 24 hours (1day)
Review + create < Previous	Next: Capture >

Real Time Automation, Inc.

1-800-249-1612



k. You should be returned to the namespace overview, scroll down and you should see the newly created event hub at the bottom of the overview section.

Frant Hube Namespace	\$ \$ ··· \$		×
Search • «	🕂 Event Hub 📋 Delete 🖒 Refresh 🔗 Give f	eedback	
🔄 Overview	Host name : rta-test-namespace.servicebu	is.windows.net Auto-infl	ate throughput : <u>Not Supported</u>
Activity log	Tage (adit) : Add tage	Local Au	thentication : <u>Enabled</u>
Access control (IAM)	Tags (edit) · Auto tags		
🗳 Tags	NAMESPACE CONTENTS KAFKA SURFACE ZONE RE 1 EVENT HUB NOT SUPPORTED ENABLED	DUNDANCY	
× Diagnose and solve problems	_		
🛃 Data Explorer (preview)	Show data for the last: 1 hour 6 hours 12 hour	s 1 day 7 days 30 days	
🗲 Events	Requests	Messages	Throughput
> Settings		100	1008
> Entities	1		508
> Monitoring	0.8	70	708
Automation	0.6		608 508
Automation		40	408
> Help	0.4	30	308
	0.2	20	
	0	0	08
	11:45 AM 12 PM 12:15 PM	UTC-05:00 11:45 AM 12 PM 12:15 PM	UTC-05:00 11:45 AM 12 PM 12:15 PM UTC-05:00
	1/2 Incoming Requests (Sum), rta-test-namespace   1	1/2 Incoming Messages (Sum), rta-test-namespa-	ce   0 Incoming Bytes. (Sum), rta-test-namespace   0B
	Server Errors (Sum), ita-test-namespace	Cantured Messages (Sum), rta-test-namespa	ce 0 Cartured Bites (Sum), naneschamespace (UB
	Event Hubs (1)		
	Search to filter items by name		
	Name	Status Message re	etention Partition count
	rta-test-hub	Active 1 hour	2

- 5. Create an Event Grid System Topic
  - a. In the search bar at the top type in "Event Grid System Topics" and select the event grid system topics option under services to navigate to the even grid system topics page..
  - b. Click create in the top left corner to create a new event grid system topic.
  - c. In the Create Even Grid System Topic window enter set the Topic Types to "Azure IoT Hub Accounts, Select your azure subscription, select your resource group, and enter a name for the topic



Home > Event Grid   System topics >	om Tonic
Event Grid	
Basics Tags Review + create	
Topic Details	
System topic resource is associated with a emitted by that resource. System topic res source.	in existing azure resource which allows customer to subscribe events source is created in the same subscription and resource group as the
Topic Types	Azure IoT Hub Accounts
Subscription *	Azure subscription 1
Resource Group *	rta-resource-group $\checkmark$
Resource *	rta-test-hub V
System Topic Details	
Enter required settings for this system top	ic.
Name *	rta-test-topic 🗸
Location	eastus D
Identity	
Managed identities are used to authentica Learn more about Managed Identities	te an Event Grid topic to Azure service instances when delivering events.
System assigned identity $\bigcirc$	
Review + create < Previous	Next: Tags >

- d. Click Review + create in the bottom left corner.
- e. On the review + create page click create the create the Event Grid System Topic.
- f. Once the event grid system topic is initialized click go to resource to navigate to the Event Grid System Topic Panel. If go to resource is not an option navigate back to the even grid system topic section and select the newly created event grid system topic from there to access the main panel.

Home > Event Grid   System topics >		-								
Event Grid System Topic										$\times$
₽ Search 0 «	+ Event Subscription	🔋 Delete 🖒 Refresh 🔗 Give feedt	back							
E Overview	^ Essentials									JSON View
Activity log	Resource group (move)	) : rta-resource-group			Source : rta-test-hub					
Access control (IAM)	Status	: Active			Source Type : Microsoft.Devices.IoTHub	5				
Ther	Location	: East US								
<ul> <li>Tays</li> </ul>	Subscription (move)	: Azure subscription 1								
> Settings	Subscription ID	: 4f0bf630-94d0-4b0b-b594-fccd8aa31dff								
> Entities	Taos (edit)	: Add taos								
> Monitoring	ingr caab									
> Automation	Show metrics: Gene	ral Errors Latency Dead-Letter				For the last: 1 hour	6 hours 12 hours	1 day	7 days	30 days
> Help	100									
	90									
	40									
	70									
	60									
	- 50									
	20									
	10									
	0									
	12 PM		12.15 PM	1	130 PM	12:45 PM			U	TC-05:00
	Published Events (Si	um) sta-test-tonic	ents (Sum) ita-test-tonic	Matched Events (Sum) sta-test-toni	- Delivered Events (Sum) sta-test-tonic	Devid Lettered Events (Su	m) ita-test-topic			
	Delivery Eailed Event	ts (Sum) stastert-tonic Drooned Fur	nots (Sum), sta-test-tonic	Advanced Filter Evaluations (Sum) at	atest topic					

- g. In the your new event grid system topics main panel hit add event subscription in the top left corner.
- h. In the create Event Subscription window:
  - i. Enter a name for the subscription



- ii. Under event types, ensure that Device Created, Device Deleted, Device Connect, Device Disconnect, and Device Telemetry are all selected.
- iii. Under Endpoint Select Event Hub as the endpoint type.
- iv. Under endpoint details click "Configure an Endpoint"
- v. In the newly opened Select Event Hub window, select your azure subscription, resource group, namespace, and event hub and click confirm selection.

Home > Event Grid   System topics > rta-test-topic >         Create Event Subscription         Basics       Filters         Additional Features       Delivery Properties         Event Grid       Event Grid         Basics       Filters         Additional Features       Delivery Properties         Event Subscriptions listen for events emitted by the topic resource and send them to the endpoint resource.         Event Subscription DETAILS         Name *       rta-test-sub         Event Schema       Image: State St	0 1,	, ,	
Create Event Subscription Create Event Subscription Create Subscription Create Subscription Create Subscriptions Create Subscriptions Create Subscriptions Create Subscriptions Create Subscriptions Create Subscription Create	Home > Event Grid   System topics >	rta-test-topic >	
Basis       Filters       Additional Features       Delivery Properties         Event Subscriptions listen for events emitted by the topic resource and send them to the endpoint resource. Learn more       EVENT SUBSCRIPTION DETAILS         Name *       rta-test-subl       Image: Instance         COPIC DETAILS       Image: Instance       Image: Instance         TOPIC DETAILS       Image: Instance       Image: Instance         TOPIC DETAILS       Image: Instance       Image: Imag	Create Event Subsci	ription	
Event Subscriptions listen for events emitted by the topic resource and send them to the endpoint resource. Learn more  EVENT SUBSCRIPTION DETAILS Name *	Basics Filters Additional Features	Delivery Properties	
EVENT SUBSCRIPTION DETAILS         Name *       rta-test-subi	Event Subscriptions listen for events emitte Learn more	d by the topic resource and send them to the endpoint resource.	
Name *     Int-test-sub       Event Schema     Event Grid Schema       TOPIC DETAILS       Pick a topic resource for which events should be pushed to your destination. Learn more       Topic Type       Opic Type       Pick which event types get pushed to your destination. Learn more       Filter to Event Types *       Selected       ENDPOINT DETAILS       Pick an event handler to receive your events. Learn more       Endpoint Type *       Managed identifies are used to authentilate an Event Grid typic to Azure service instances when delivering events. Select different a system assigned or a user assigned managed identity. You should have already configured or authentilate an Event Grid typic to Azure service instances when delivering events. Select differe a system assigned or a user assigned managed identity. You should have already configured or authentilate an Event Subscription is associated. Learn more about Managed identity type	EVENT SUBSCRIPTION DETAILS		
Event Schema         TOPIC DETAILS         Pick a topic resource for which events should be pushed to your destination. Learn more         Topic Type         Source Resource         On It A topic Name         Extended in the test-thub         Topic Name         Pick which event types get pushed to your destination. Learn more         Fitter to Event Types *         Selected         ENDPOINT DETAILS         Pick an event handler to receive your events. Learn more         Endpoint Type *         Endpoint *         rea-test-hub (shange)         MANAGED IDENTIFY FOR DELIVERY         Managed identifies are used to authentilicate an Event Grid topic to Azure service instances when delivering events. Siect Either a system assigned or a user assigned or as user assigned identify. You should have already configured one or more identifies on the topic to which the event subscription is associated. Learn more about Managed identify type         Managed identify type       None	Name *	rta-test-sub	~
TOPIC DETAILS         Pick a topic resource for which events should be pushed to your destination. Learn more         Topic Type       A IoT Hub         Source Resource       O rta-test-hub         Topic Name       E rta-test-hup         Topic Name       E rta-test-hup         Pick which event types get pushed to your destination. Learn more         Fitter to Event Types*       Selected         Pick avent handler to receive your events. Learn more         Endpoint Type *       E Event Hub (sharge)         Endpoint *       rta-test-hub (sharge)         MANAGED IDENTITY FOR DELIVERY         Namaged identifies are used to avail to which this event Subscription is associated. Learn more about Managed identifies.         Managed identifies on the topic to which this event subscription is associated. Learn more about Managed identifies.         Managed identifies are used to avail the subscription is associated. Learn more about Managed identifies.         Managed identifies are used to avail the subscription is associated. Learn more about Managed identifies.         Managed identifies are used to avail the subscription is associated. Learn more about Managed identifies.	Event Schema	Event Grid Schema	$\sim$
Pick a topic resource for which events should be pushed to your destination. Learn more         Topic Type       Source Resource         Or rta-test-hub         Topic Name       Tra-test-hub         Topic Name       If rta-test-hub         EVENT TYPES         Pick which event types get pushed to your destination. Learn more         Fifter to Event Types*       Selected         ENDPOINT DETAILS         Pick an event handler to receive your events. Learn more         Endpoint *       rta-test-hub (charge)         Endpoint *       E E vent Hub (charge)         MANAGED DIDENTITY FOR DELIVERY         Managed identities are used to which this event Subarciption is associated. Learn more about Managed identities         means of identities on the topic to which this event subarciption is associated. Learn more about Managed identities         Managed identities to the topic to which this event subarciption is associated. Learn more about Managed identities	TOPIC DETAILS		
Topic Type       All IoT Hub         Source Resource       Or rta-test-hub         Topic Name       Er rta-test-hupic         EVENT TYPES       Pick which event types get pushed to your destination. Learn more         Filter to Event Types*       Selected         ENDPOINT DETAILS       Pick an event handler to receive your events. Learn more         Endpoint *       Tea-test-hub (stange)         Endpoint *       Tea-test-hub (stange)         MANAGED IDENTITY FOR DELIVERY       Namaged identities are used to which this event subscription is associated. Learn more about Managed identities         Managed identities on the topic to which this event subscription is associated. Learn more about Managed identities         Managed identity type       None	Pick a topic resource for which events show	Id be pushed to your destination. Learn more	
Source Resource  In ta-test-hub Topic Name  Fit ra-test-topic  EVENT TYPES Pick which event types get pushed to your destination. Learn more  Fitter to Event Types *  Selected  ENDPOINT DETAILS  Pick an event handler to receive your events. Learn more Endpoint *  MANAGED DIDENTITY FOR DELIVERY  Managed identifies are used to authenticate an Event Grid topic to Azure service instances when delivering events Select either a system assigned or a user assigned managed identifies, to whould have already configured one or more identifies on the topic to which this event subscription is assigned assigned to authenticate Managed identifies on the topic to which this event subscription is assigned assigned when the topic to which this event subscription is assigned assigned when the topic to which this event subscription is assigned assigned when the topic to which this event subscription is assigned assigned assigned between the topic to which this event subscription is assigned assigned assigned between the topic to which this event subscription is assigned assigned between the topic to which this event subscription is assigned assigned by the subscription is assigned assigned assigned assigned by the subscription is assigned by the subscription is assigned assigned by the subscription is assigned by the s	Торіс Туре	🕅 loT Hub	
Topic Name     E rta-test-topic       EVENT TYPES     Pick which event types get pushed to your destination. Learn more       Filter to Event Types*     Selected       FODPOINT DETAILS     Pick an event handler to receive your events. Learn more       Endpoint Type *     E Event Hub (sharge)       Endpoint *     rta-test-hub (sharge)       MANAGED IDENTITY FOR DELIVERY     Namaged identifies are used to authentilate an Event Gid topic to Azurs service instances when delivering events Select ather a system assigned on a user assigned managed identifies.       Managed identifies on the topic to which this event subscription is associated. Learn more about Managed identifies on the topic to which this event subscription is associated. Learn more about Managed identifies on the topic to which this event subscription is associated. Learn more about Managed identifies on the topic to which this event subscription is associated. Learn more about Managed identifies on the topic to which this event subscription is associated. Learn more about Managed identifies on the topic to which this event subscription is associated. Learn more about Managed identifies on the topic to which this event subscription is associated. Learn more about Managed identifies on the topic to which this event subscription is associated. Learn more about Managed identifies are used identifies on the topic to which this event subscription is associated. Learn more about Managed identifies are used identifies and the about the about the about the about Managed identifies are used identifies are used identifies and the about the abou	Source Resource	🗘 rta-test-hub	
EVENT TYPES Pick which event types get pushed to your destination. Learn more Fitter to Event Types * Selected  ENDPOINT DETAILS Pick an event handler to receive your events. Learn more Endpoint Type * Endpoint * Tra-test-hub (charge) MMANAGED IDENTITY FOR DELIVERY Managed identifies are used to authenticate an Event Grid topic to Azurs service instances when delivering events Select ather a system assigned or a user assigned managed identify. You should have already configured identifies Managed identifies on the topic to which this event subscription is associated. Learn more about Managed identifies Managed identify type None	Topic Name	🗵 rta-test-topic	
Pick which event types get pushed to your destination. Learn more  Fitter to Event Types * Selected   ENDPOINT DETAILS  Pick an event handler to receive your events. Learn more Endpoint Type * E Event Hub (dange) Endpoint * rta-test-hub (dange)  MANAGED DIENTITY FOR DELIVERY  Managed identifies are used to authenticate an Event Grid topic to Azure service instances when delivering events Select either a system assigned or a user assigned managed identify. You should have already configured identifies Managed identifies on the topic to which this event subscription is associated. Learn more about Managed identifies Managed identify type None	EVENT TYPES		
Filter to Event Types*     S selected       ENDPOINT DETAILS       Prick an event handler to receive your events. Learn more       Endpoint Type *       Endpoint Type *       MANAGED DIDENTITY FOR DELIVERY       Managed identifies are used to authentiate an Event Grid topic to Azurs service instances when delivering events solered there a system assigned or a user assigned managed identifies on the topic to which this event subscription is associated. Learn more about Managed identifies (Learn more about Managed identifies on the topic to which this event subscription is associated. Learn more about Managed identifies (Learn more about Managed identifies on the topic to which this event subscription is associated. Learn more about Managed identifies (Learn more about	Pick which event types get pushed to your	destination. Learn more	
ENDPOINT DETAILS Pick an event handler to receive your events. Learn more Endpoint Type * E Event Hub (dange) Endpoint * rta-test-hub (dange) MANAGED DIENTITY FOR DELIVERY Managed identifies are used to authenticate an Event Grid topic to Azure service instances when delivering events Select either a system assigned or a user assigned managed identify. You should have already configured identifies Managed identifies on the topic to which this event subscription is associated. Learn more about Managed identifies Managed identify type None	Filter to Event Types *	5 selected	$\sim$
Pick an event handler to receive your events. Learn more       Endpoint Type *     E Event Hub (charge)       Endpoint *     tra-test-hub (charge)       MANAGED IDENTITY FOR DELIVERY       Managed identities are used to authenticate an Event Grid topic to Azure service instances when delivering events. Select either a system assigned or a user assigned managed identity. You should have already configured identities       Managed identity type     None	ENDPOINT DETAILS		
Endpoint Type * E Event Hub (sharpe) Endpoint * rta-test-hub (sharpe) MANAGED IDENTITY FOR DELIVERY Managed identifies are used to authenticate an Event Grid topic to Azure service instances when delivering events. Select either a system assigned or a user assigned managed identify. You should have aiready configured one or more identifies on the topic to which this event subscription is associated. Learn more about Managed identifies Managed identify type None	Pick an event handler to receive your event	s. Learn more	
Endpoint * rta-test-hub (dauge) MANAGED IDENTITY FOR DELIVERY Managed identifies are used to authenticate an Event Grid topic to Azure service instances when delivering events. Select either a system assigned or a user assigned managed identity. You should have already configured identities Managed identity type None	Endpoint Type *	Event Hub (change)	
MANAGED IDENTITY FOR DELIVERY Managed identifies are used to authenticate an Event Grid topic to Azure service instances when delivering events. Select either a system assigned or a user assigned managed identify. You should have already configured one or more identifies on the topic to which this event subscription is associated. Learn more about Managed identifies Managed identify type None	Endpoint *	rta-test-hub (change)	
Managed identities are used to authenticate an Event Grid topic to Azure service instances when delivering events. Select either a system assigned or a user assigned managed identity. You should have already configured one or more identities on the topic to which this event subscription is associated. Learn more about Managed Identities Managed identity type None	MANAGED IDENTITY FOR DELIVERY		
Managed identity type None	Managed identities are used to authentica events. Select either a system assigned or a one or more identities on the topic to whi Identities	te an Event Grid topic to Azure service instances when delivering user assigned managed identity. You should have already configu th this event subscription is associated. Learn more about Manage	red d
	Managed identity type	None	$\checkmark$
Create	Create		

i. Click create in the lower left corner of the webpage.



## **Testing Microsoft Azure Communication**

Once you have the Azure configured, you can use their <u>Azure IoT Explorer</u> utility to test the connection is working.

To set up Azure IoT Explorer:

- 1. open the utility and select the IoT Hubs tab on the left
- 2. Click the Add connection button
- 3. In the Add connection String window that appears enter the connection string for your IoT Hub.
  - a. This can be obtained by navigating to the IoT Hubs overview window in azure, selecting Shared access policies from the left pane, and opening the iothubowner policy.
- 4. Click save.
- 5. Your hub should now be listed in the IoT hubs section as shown below.

Home > IoT hubs		
=	+ Add connection   Switch authentication method	
움 loT hubs		
o <sup>g⊄</sup> IoT Plug and Play Settings	rta-test-hub	1
Notification Center	Host name	
	rta-test-hub.azure-devices.net	D
	Shared access policy name	
	iothubowner	D
	Shared access policy key	
	•••••	D
	Connection String	
	······································	ß
	ightarrow View devices in this hub	
		)

6. You can then click on the hub name to view devices available in the hub and see their current status.



Home > rta-test-hub > Devices				
🛨 New 💍 Refresh 🛍 Delete				
Query by device ID	$\rightarrow$ $\bigcirc$ Add quer	y parameter		
Device ID $\smallsetminus$	Status $\vee$	Connectio $\vee$	Authentica $\vee$	Last status $\vee$
mqtt-explorer-device	Enabled	Disconnected	Sas	
rta-test-device	Enabled	Disconnected	Sas	

7. Selecting a device within the hub will provide device specific information such as its Primary Connection string. It also provides useful tools for seeing data being from the device to Azure as well as send test messages from Azure to the device.



#### Send data from Microsoft Azure to RTA gateway

Below is how the RTA Microsoft Azure Service is set up to receive data from Microsoft Azure.

	<mark> E</mark> nable				Azu	re 1							
		Device La	abel QT01			Net	work Inte	rface	Switch Mo	de	(DHCP	Assigne	ed) ~
	Prima	ary Connection	on String Hos	tName=rta-te	est-hub.a	zure-dev	/ices.net;D	Devicel	id=rta-test	de	vice;Sha	redAcc	es
	Client	ID rta-test-de	vice					Add T	imestamp	to	Publis	nes	
	TCP	Port 8883	1-65535 (	Default: 888	3)	Ke	ep Alive	60	0-20	00	sec (0	to Disa	ible)
	# of JSON Name/Value Pairs 1 0-500												
		# of Publish	Paths 0	0-250			# of \$	Subsc	ribe Path	5 1		0-1	
					Generat	e Paths	)						
sc	ON Nam	e/Value Pa	irs										
	Line #		Path				ISON Na	me			JSO	N Poin	t Type
	1	devices/rta-te	est-device/devi	cebound, ~	message				]	INT (8-bit) ~			
					<1·	1 >>							
				(	Save Par	ameters							
		View F	Publish Paths					V	iew Subscr	be	Paths		
uk	ubscribe Paths (MQTT to 460ETCQT)												
	Line #	Enable				Path I	Name						QoS
	1		devices/rta	a-test-device/	devicebo	und/#/							0 ~
					<1·	1 >>	)						

In Azure IoT Explorer, navigate to the device you wish to receive data from Azure on. In the device configuration select the Cloud-to-device message tab on the left.

In the Cloud-to-device message tab, enter the message to be sent to the RTA in the message body section and click Send message to device at the top of the page. An example payload for the configuration above can be seen in the image below.



Home > rta-test-hub > Devices >	rta-test-device > Cloud-to-device message
=	Send message to device
Device identity	Cloud to dovice message You can send mess
🔁 Device twin	cloud-to-device message voi cur send mess
Telemetry	Message body ①
✓ Direct method	{ "message" : 24 }
Cloud-to-device message	
🛠 Module identities	Add timestamp to message body
🖉 IoT Plug and Play components	∧ Properties ①
	Add custom property
	Key $\vee$

Navigate to the RTA display data page, view data from MQTT, refresh the page, and the value should be visible as shown below.

DTA						www.rtautomation.com
Real Time Auto	mation, Inc.					MODE: RUNNING 460ETCQT
Configuration Mode	Display Data					Edit Mapping View as Text
CONFIGURATION	Select a Device A	llen-Bradley PLC (	Not Configu	red) view		
Allen-Bradley PLC		MQTT to PLC				PLC to MQTT
MQTT Client Data Mapping				IDisplaying 1-1 of 1		
Display Data DIAGNOSTICS		MQTT		460ETCQT →→		PLC
-Select- v	Name	Value (	Hex)	Manipulation	Name	Value (Hex)
OTHER -Select-	message	24	0x18	<b>→→</b>	N/A	Point Not Mapped



#### Send data from RTA gateway to Microsoft Azure (Publish Topics)

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

	Enable				Azu	re 1				
	Device Label QT01				Network Interface Switch Mode (DHCP Assigned) V					
	Primary Connection String HostName=rta-test-hub.azure-devices.net;DeviceId=rta-test-device;SharedAcces									
	Client ID rta-test-device Add Timestamp to Publishes									
	TCP Port 8883 1-65535 (Default: 8883)			Keep Alive 60 0-200 sec (0 to Disable)				e)		
			# o	f JSON Nan	ne/Value	Pairs 1	0-500			
		# of Publish	Paths 1	0-250		# of S	ubscribe Paths	0	0-1	
					Generat	e Paths				
JSO	SON Name/Value Pairs									
L	Line #		Path			JSON Nar	ne	JSO	N Point Ty	уре
	Line #	devices/rta-	Path test-device/mess	sages/ev v	Data	JSON Nar	ne	JSOI INT (	<b>N Point T</b> y 8-bit)	ype ~
	Line # 1	devices/rta-	Path test-device/mest	sages/ev ~	Data	JSON Nar	ne	JSOI INT (	N Point Ty 8-bit)	ype ~
	Line #	devices/rta-1	Path test-device/mest	sages/ev v)	Data	JSON Nar	ne	JSOI INT (	N Point Ty 8-bit)	ype ~
	Line #	devices/rta-	Path test-device/mess Publish Paths	sages/ev > )	Data	JSON Nar	ne View Subscrib	JSOI INT ( Pe Paths	N Point Ty 8-bit)	ype v
Publ	Line #	devices/rta- View ths (460E	Path test-device/mess Publish Paths TCQT to MC	sages/ev v)	Data	JSON Nar	ne	JSOI INT ( Pe Paths	N Point Ty 8-bit)	ype ~
Publ	Line # 1 lish Pat	devices/rta- View ths (460E Enable	Path test-device/mess Publish Paths TCQT to MC	sages/ev v)	Data	JSON Nar	ne	JSOI INT ( e Paths	N Point Ty 8-bit)	ype v
Publ	Line # 1 lish Pat Line # 1	devices/rta- View ths (460E Enable ☑	Path test-device/mess Publish Paths TCQT to MC devices/rta	sages/ev v)	Data	JSON Nar	ne View Subscrib	JSOI INT ( ne Paths	N Point Ty 8-bit)	ype v l v l v l v l v l v l v l v v v v v v v v v v v v v

Р	LC	460E			MQTT	
Name	Value (Hex)	Manip	ulation	Name	Value	(Hex)
Data_From_PLC_2_AZR	68	0x44	<b>→</b> →	devices/rta-te messages/ Data_From_R Data	st-device/ events/ TA_2_AZR a	68



In Azure IoT Explorer, navigate to the device you would like to publish data to and select the telemetry tab on the left. In the telemetry window click Start in the top left corner. Any messages published to the selected device will now be shown in the telemetry window.

Home > rta-test-hub > Devices > rta-test-device > Telemetry					
=	Stop 🗌 Show system properties 💼 Clear events {} Simulate a device 🗍 Customize Content Type				
Device identity	Tolens where the second state of the state o				
🔁 Device twin	leiemetry rou can monitor telemetry that the device senas to the lot hub				
🖵 Telemetry	Consumer group ① \$Default				
✓ Direct method	Specify enqueue time ①				
☑ Cloud-to-device message	Use built-in event hub				
🛠 Module identities	Yes				
🔗 IoT Plug and Play components	(i) Receiving events				
	Tue Oct 22 2024 09:50:31 GMT-0500 (Central Daylight Time):				
	{     "body": {         "Data": 68     },     "enqueuedTime": "Tue Oct 22 2024 09:50:31 GMT-0500 (Central Daylight Time)" }				



# QT Publish Trigger

By default, the RTA gateway will publish to the broker based on change of state. This means a new publish to the broker will occur any time a value changes. In an application where the client is being charged per publish, such as with AWS, this is not ideal. In this situation the QT Publish trigger can be configured. When the QT Publish Trigger is configured a publish will only occur when the trigger value is incremented, allowing the user to control when data is published.

In the example below, it is shown how the trigger would be configured for MQTT device 1. A trigger value is being mapped from the mating protocol into the QT TriggerPublish1 destination. With this configuration all topics configured on MQTT device 1 will be published when the trigger value is incremented.

Enable	Mapping 2				
Source	Enable Manipulation	Destination			
Group: ETC01 Trigger_Value (Int16) V Start: Trigger_Value V End: Trigger_Value V	• • -> • •	Group: QT TriggerPublish1 (Uint16) V Start: TriggerPublish1 V End: TriggerPublish1			

To trigger for MQTT device 2 or 3, TriggerPublish2 or TriggerPublish3 should be selected under the "Start" dropdown in the destination configuration as shown below.

C Enable	Mapping 2				
Source	Enable Manipulation	Destination			
Group: ETC01 Trigger_Value (Int16) V Start: Trigger_Value V End: Trigger_Value V	• • • • •	Group: QT TriggerPublish1 (Uint16) V Start: TriggerPublish1 V End: TriggerPublish1			
	<< >>	TriggerPublish2 TriggerPublish3			


# 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.

Display Data	Edit Mapping View as Text
Select a Device Modbus TCP Server IP Address: 0.0.0.0 View	
Protocol 1 to Protocol 2	Protocol 2 to Protocol 1



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

Mo	dbus RTU to BACr	et/IP			BACnet/IP to Modb	us RTU
		l	< 1 > Displaying 1-201 of 3	> 300		
	Modbus RTU	I	460MMBS		BACnet/IP	
Name	Valu	ie (Hex)	Manipulation	Name	Value	e (Hex)
400001			<b>&gt;</b> >	Al1		
400002			<b>&gt;&gt;</b>	AI2	Mapping Dis	abled for Point
400003			<b>&gt;&gt;</b>	AI3		

In the above example, we see the following:

- Modbus register 400001 from Slave 1 is being mapped to Al1 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 Al1, only 400001 will show as being mapped to Al1.

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	a					Edit Mapping View as Text		
Select a Devic	Select a Device Modbus TCP Server IP Address: 10.1.16.16 V View							
	Modbus TCP/	IP to PLC			PLC to Modbus	TCP/IP		
			< Displayin	1 >> ng 1-7 of 7				
	Modbus	TCP/IP	460E	тсмс	PLC			
Name		Value (Hex)	Manip	ulation Name	Valu	ie (Hex)		
400001	15	0x000F	<b>→→</b>	ETC01 MC2PLC_INT[0]	15	0x000F		
400002	1495	0x05D7	<b>→→</b>	ETC01 MC2PLC_INT[1]	1495	0x05D7		
400003	1	0x0001	<b>→</b> →	ETC01 MC2PLC_INT[2]	1	0x0001		
400004	23	0x0017	<b>→</b> →	ETC01 MC2PLC_INT[3]	23	0x0017		
400005	3	0x0003	<b>→</b>	ETC01 MC2PLC_INT[4]	3	0x0003		
400011			<b>→</b> →	ETC01 ETC01_G2N0_INT[0]				
400012			<b>→</b> →	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						
	Restant Now						
DIAGNOSTICS							
	-Select-						
OTH	ER -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 byte	s)
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	Opera	tion Mode Mark Data New	on New Messa	age 🗸

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.

Display String	(	Edit Mapping
	(	View as Text
Select a Group Src: Line 1 Barcode Scanner V and a String Barcode Scanner (0 b	bytes)	
Data Not Valid		

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

Diagnostics				
ASCII	✓ View			
Port 1 (DB9) ✔	View			

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

Display String	Edit Mapping
	View as Text
Select a Group Src: Line 1 Barcode Scanner v and a String Barcode Scanner v (11 bytes)	
0000: 68 65 6C 6C 6F 20 77 6F 72 6C 64 hello world	

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

String Mapping Configuration		Help			
Manual Configure # of Mappings to Configure: 1 0-250 Set Max # of Mappings					
Enable	Mapping 1				
Source Destination					
Group: Line 1 Barcode Scanner	• • • • • •	Group: ETC01 ETC01_G2N0_STRIN  String: ETC01_G2N0_STRING			

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

Real Time Automation, Inc.



# 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	Max Number of Fields: 3 1-50 Min Number of Fields: 1 1-50				
		Parsing D	Delimiter: 📜 44 (	0x2c	▼
	Update Fields				
Field	Start Location	Length	Data Type Internal		Internal Tag Name
1:	1	0	String	~	Header 1
2:	1	0	String	~	Header 2
3:	1	0	String	~	Header 3

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

Display String			Edit Mapping View as Text
Select a Group Src: Line1 Header 1	✓ and a String Header 1 ✓	(3 bytes)	
0000: 52 54 41	RTA		
Display String			Edit Mapping View as Text
Select a Group Src: Line1 Header 2	✓ and a String Header 2 ✓	(7 bytes)	
0000: 53 75 70 70 6F 72 74	Support		
Display String			Edit Mapping View as Text
Select a Group Src: Line1 Header 3	✓ and a String Header 3 ✓	(5 bytes)	
0000: 52 6F 63 6B 73	Rocks		

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

Diagnostica	Last Messa	ge Sent (17	/ bytes)		
Diagnostics	0000:	52 54 41	2C 53 75 70	70 6F 72 74 2C 52 6F 63 6	B RTA,Support,Rock
ASCII View Port 1 (DB9) View	0010:	75			5



# 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.

Source	Destination
8-bit Sint	8-bit Sint
16-bit Int	16-bit Int
32-bit Uint	32-bit Uint
32-bit Float	32-bit Uint

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



# Data Mapping – Explanation

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



1) Enable (red box above): Check to enable mapping. If not checked, this mapping is skipped.

#### 2) Source Field (yellow box above):

- a) Group Select the data group you set up in the protocol config to use for this mapping.
- b) Start This is the starting point for this mapping.
- c) End This is the final point to be included for this mapping.
- 3) Manipulation Area (green box above):
  - a) Enable the Data Manipulation. This can be enabled for any mapping.
  - b) Click Add Math Operation for each operation needed. Up to 3 are allowed unless you are using the Scale, Set Bit, or Invert Bit functions. If using Scale, Set Bit, or Invert Bit, then only 1 operation is allowed.
  - c) Select the Operation(s) to perform.
    - i) Math Operations are performed in the order they are selected.
    - ii) If more than one point is selected on the source, the Math Operations will be performed on every point.
  - d) Enter the value(s) for the operation.



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

	Enable	Manip	ulation
	Scale		*
Src	1	to [	10
Dst	1	to	100

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

🗹 Enable	Manipulation
Set Bit	*
Src	Dst
0	5
(0-15)	(0-15)

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

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

1-800-249-1612



# 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.

☑ Enable	Mapping 1				
Source	Enable Manipulation	Destination			
Group: Temporary Ram0 (Int64) 🛛 💌	Scale	Group: Temporary Ram0 (Int64) 🛛 💌			
Start: Ram0 💽	Src 1 to 10	Start: Ram1 🛛 😪			
End: RamO 💌	Dst 1 to 100	End: Ram1			
Enable     Mapping 2					
Enable	Mapping 2				
Source	Mapping 2	Destination			
Source Group: Temporary Ram0 (Int64)	Mapping 2	Destination Group: Temporary Ram0 (Int64)			
Source       Group: Temporary Ram0 (Int64)       Start: Ram1	Mapping 2       Enable Manipulation       Add       Add       Add	Destination       Group: Temporary RamD (Int64)       Start: 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.

Enable Mapping 1			
Source	Enable Manipulation	Destination	
Group: Ticks Since Powerup (Uint32)  Start: Since Powerup End: Since Powerup	• • -> • •	Group: BS01 Al1 (Float)  Start: Al1  Contemporation of the second	

Real Time Automation, Inc.



#### 4) Heartbeat 100ms Update

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

Enable Mapping 1				
Source	Enable Manipulation	Destination		
Group:       Heartbeat 100ms Update (Uir ~)         Start:       100ms Update       ~)         End:       100ms Update       ~)	• • • • •	Group: ETC01 Heartbeat (Int32) v Start: Heartbeat v End: Heartbeat		

#### 5) Heartbeat 1000ms Update

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

Enable     Mapping 1				
Source		Enable Manipulation	Destination	
Group: Heartbeat 1000ms Update (U 🗸			Group: ETC01 Heartbeat (Int32) V	
Start: 1000ms Update v	•	$\circ \longrightarrow \circ \circ$	Start: Heartbeat 🗸	
End: 1000ms Update V			End: Heartbeat	

#### 6) XY\_NetBmpStat

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

Modbus RTU Master	
Device Status	
LED Status	
Connection Status:	Connected
Variables	
Network Bitmap Status:	0x0000001f

- b) Since a Client/Master may be trying to communicate with multiple devices on the network, it may be beneficial to know if a Server/Slave device is down. By using this Network Bitmap Status, you can expose the connection statuses of individual devices. **Values shown are in HEX.** 
  - i) 0x0000002 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 Al1 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.

C Enable Mapping 1			
Source		Enable Manipulation	Destination
Group: MM NetBmpStat (Uint32)  Start: NetBmpStat  Contemp Stat  Contemp	•	• -> • •	Group: BS01 Al1 (Float)  Start: Al1  Control Al1

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

Enable Mapping 1						
Source	Enable Manipulation	Destination				
Group: MM NetBmpStat (Uint32)  Start: NetBmpStat End: NetBmpStat	Set Bit            Src         Dst           1         0           (0-31)         (0)	Group: BS01 BI1 (Bit1)  Start: BI1 Find: BI1				



#### 7) Status\_XY

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

Commo	on Status:	0x000000FF	(bit 0-7)1 <sup>st</sup> byte
Hex:	Bit Position:	Decimal:	Explanation:
0x00	0	0	if we are a Slave/Server
0x01 0x02	1	1 2	connected (0 not connected)
0x04 0x08	2 3	4 8	first time scan idle (usually added to connected)
0x10 0x20	4	16 32	running (usually added to connected)
0x40	6	64 128	recoverable fault
0700	1	120	HOHLECOVELADIE LAULU

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

	F	PLC to Modbus TCP/I	P			Modbus TCP/I	P to PLC		
		PLC		460ETCMC €€		Modbus TC	:P/IP		
Nan	ne	Value	(Hex)	Manipulation	Name	Va	ue (Hex)		
PLC_S	tatus	19	0x00000013	<b>*</b>	ETC Status	19	0x00000013		
Examp	ole: ET	C Status is 0x00	000013 (19 (	decimal), here	e is the	break down			
	Hex	Bit D	Decimal	Expla	nation				
	0x01	. 0(on)	1	if we are	a Mas	ter/Client			
	0x02	1(on)	2	connected (0 not connected)					
	<u>0x10</u>	9 4(on)	16	running (u	suall	y added to	connected)		
	Tota	l: 0x13	19						
Exte:	rnal	Faults:		0x0000FF0	00 (bi	t 8-15)2 <sup>nd</sup>	' byte		
Hex:	<u>Bit</u>	Position:	Decimal:	Expla	natio	n:			
0x00		8	0	loca	l con	trol			
0x01		8	256	remo	tely	idle			
0x02		9	512	remo	tely	faulted			
0x04		10	1,024	idle	e due i	to depende	ncy		
0x08		11	2,048	faul	ted d	ue to depe	ndency		
Reco	veral	ble Faults	: 0x00F	F0000 (bi	t 16	23)3 <sup>rd</sup> byt	e		
Hex:	Bit	Position:	Decimal:	Expla	inatio	n:			
0x01		16	65,536	reco	verab	le fault -	timed out		
0x02		17	131,07	2 reco	verab	le fault -	Slave err		

#### 1-800-249-1612



#### Non-Recoverable Faults 0xFF000000 (bit 24-31)4<sup>th</sup> byte

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

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

	PLC to Modbus TC	P/IP			Modbus TCP/IP to PLC			
	PLC		460ETCMC Modbus TCP/IP			P/IP		
Name	Val	ue (Hex)	Manipulation	Name	Val	ue (Hex)		
MC_Status	65601	0x00010041	<b>44</b>	MC Status	65601	0x00010041		

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

Common	Status:			
Hex:	<u>Bit:</u>	Decimal:	Explanation:	
0x01	0(on)	1	if we are a Master/Client	
0x40	6(on)	64	recoverable fault	
<b>Recover</b> <u>Hex:</u>	able Fan <u>Bit:</u>	ults: Decimal:	Explanation:	
0x01	16	65,536	recoverable fault - timed	
0x010041		65,601		

Total:



# 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.

	Enable	Mapping 1	3.		
I	Source	Destination			
	Group: Line 1 Barcode Scanner	O     O	RIN V		

- 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.

Message from webpage	×
Press OK to keep the co Press Cancel to Delete	urrent Mappings. all Mappings.
ОК	Cancel

- 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.

Message fr	rom webpage
?	Press OK to delete the current Mappings and go back to Auto-Configure Mappings mode. Press Cancel to keep Mappings and remain in current Mode.
	OK Cancel

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

# 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 ->	MCO2 400001				

Real Time Automation, Inc.



# Base Triggering – Data Validiation Triggering

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

#### How does this work?

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

#### How do you set this up?

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

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

rite 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 BACn				
					-	
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.

C Enable	Mapping 2					
Source			Enable Manipulat	tion	Destination	
Group: BS01 AO1 (Float)	~				Group: MC Trigger 0 (Uint16)	~
Start: A021	~	0	$\circ \bigcirc \circ$	•	Start: Trigger 1	~
End: AO21	~				End: Trigger 1	

5) The second mapping, the MC Handshake will increment that all data is validated and write to Al21 "all data is validated". The value of Al40 and AO21 should be the same.

C Enable	Mapping 3							
Source		Enat	ole Manip	oulat	ion		Destination	
Group: MC Handshake 0 (Uint16)						Group:	BS01 Al1 (Float)	~
Start: Handshake 1 🗸	•	0	$\Rightarrow$	0	•	Start:	AI40	~
End: Handshake 1 🗸						End:	AI40	



# **Security Configuration**

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

# THIS IS NOT A TOTAL SECURITY FEATURE

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

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

- 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.

Admin	Username	Password	Re-enter Password	Email	Hint
1				Not Configured	
2				Not Configured	
3				Not Configured	
ser Con	figuration	Admi	n Contact Informatio	on	
ser Con	figuration Username	Adm	n Contact Information Re-enter Password	Email	Hint
ser Con User	figuration Username	Adm	n Contact Information Re-enter Password	Email Not Configured	Hint
Ser Con User 1 [ 2 [	figuration Username	Adm Password	Re-enter Password	Email Not Configured Not Configured	Hint
User [ 1 [ 2 [ 3 [	figuration Username	Adm Password	Re-enter Password	Email Not Configured Not Configured Not Configured	Hint
<b>User</b> 1 2 3 4	figuration	Adm Password	Re-enter Password	Email Email Not Configured Not Configured Not Configured Not Configured	Hint

Real Time Automation, Inc.



# Security Configuration-Security Levels

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

Security Levels:

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

Web Page	Security
All Web Pages	No Access 👻 Set
Web Page	Security
Main Page	Full Access 🛩
Device Configuration	Full Access 👻
Port Configuration	Full Access 💌
BACnet/IP Server	Full Access 💌
Modbus RTU Master	Full Access 💙
View Mapping	Full Access 💙
Mapping	Full Access 💌
Setup LED's	Full Access 🛩
Diagnostic Info	Full Access 💌
Logging	Full Access 😪
Display Data	Full Access 😒
Export Configuration	Full Access 😪
Import Configuration	Full Access 😪
Save As Template	Full Access 🔽
Load From Template	Full Access 💌
Utilities	Full Access 🛩
Email Configuration	Full Access 💌
Alarm Configuration	Full Access 🗸
String Mapping	Full Access 🗸
View String Mapping	Full Access 🗸
Display String	Full Access 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.

Applic	ation Description
Username:	Admin
Password:	
Display Hint	Log In Reset Password

#### Security - Log Out

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



Closing the browser is not sufficient to log out.



# **Email Configuration**

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

You can configure up to 10 email addresses.

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

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





# Alarm Configuration

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

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

Alarm Configuration				Help
	Alarm Delay	upon Powerup:	0 0-3600 s	
	# of Alarm	is to Configure: Set Max #Ala	1 0-100 arms	
		<< <u>1</u>		
Enable		1	Alarm 1	
Data Point	Set Error	Clear Error	Alarm Name	Email
Ticks Since Powerup (Uint32)	>= •	None 💌	Gateway_test	Group A
Ticks Since Powerup				

- 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 Statu	IS			
# Alarms En	abled:	1		
# Alarms Ac	tive:	0		
Last Active	Alarm:			
			Clea	r # of Times Active
	Alarm#	Name	Status	# of Times Active
	1	Alarm Example	OK	0

#### Alarms - Active

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



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. Real Time Automation, Inc. 99 1-800-249-1612



Alarm Statu	S			
# Alarms En	abled:	1		
# Alarms Ac	tive:	1		
Last Active A	Alarm:	Alarm 1 is Set: Actual: (	0 < Limit: 20	
				Clear # of Times Active
	Alarm#	Name	Status	# of Times Active
	1	Alarm Example	Alarm	1

#### Alarms – Clear

When an alarm is cleared, the following will occur:

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



# Change of State (COS) Configuration

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

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

<ul> <li>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.</li> <li>Gateway behavior: <ul> <li>If time = 0s =&gt; (DEFAULT) The gateway will write out new values on a Change of State basis.</li> <li>If time &gt; 0s =&gt; The gateway will write out new values whenever the timer expires to force cyclic updates (write every <i>x</i> seconds).</li> </ul> </li> <li>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</li> </ul>
<ul> <li>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.</li> <li>Gateway behavior: <ul> <li>If time = 0s =&gt; (DEFAULT) The gateway will write out new values on a Change of State basis.</li> <li>If time &gt; 0s =&gt; The gateway will write out new values whenever the timer expires to force cyclic updates (write every x seconds).</li> </ul> </li> <li>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</li> </ul>
<ul> <li>Changed by default. There is a separate timer per data mapping.</li> <li>Gateway behavior: <ul> <li>If time = 0s =&gt; (DEFAULT) The gateway will write out new values on a Change of State basis.</li> <li>If time &gt; 0s =&gt; The gateway will write out new values whenever the timer expires to force cyclic updates (write every x seconds).</li> </ul> </li> <li>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</li> </ul>
<ul> <li>If time = 0s =&gt; (DEFAULT) The gateway will write out new values on a Change of State basis.</li> <li>If time &gt; 0s =&gt; The gateway will write out new values whenever the timer expires to force cyclic updates (write every <i>x</i> seconds).</li> <li>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</li> </ul>
<ul> <li>If time = 0s =&gt; (DEFAULT) The gateway will write out new values on a Change of State basis.</li> <li>If time &gt; 0s =&gt; The gateway will write out new values whenever the timer expires to force cyclic updates (write every <i>x</i> seconds).</li> <li>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</li> </ul>
<ul> <li>If time &gt; 0s =&gt; The gateway will write out new values whenever the timer expires to force cyclic updates (write every <i>x</i> seconds).</li> <li>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</li> </ul>
2) <b>Production Inhibit Timer:</b> 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
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 th
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
the next set of reads begin
4) <b>Reads Before Writes:</b> If multiple writes are queued the # of Writes Before Beads 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) <b>Enable Data Integrity</b> : If enabled, do not execute any write requests to the destination until the
source data point is connected and communicating. This prevents writes of 0 upon power up.
6) Enable Mark Whole Entry New: If Enabled, mark the entire scan line or data group new upon 1
data element within the scan line or data group to be new.
Change of State Configuration Help
Stale Data Timer: 0 0-3600 s
Production Inhibit Timer: 0 0-60000 ms
Writes Before Reads: 10 0-255
Reads Before Writes: 1 1-255
Enable Data Integrity: 🗹
Enable Mark Whole Entry New:
Save Parameters

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

Real Time Automation, Inc.



# **Diagnostics Info**

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

DIAG	GNOSTICS	
	-Select-	~
	-Select-	
OTH	Diagnostic Info	
	Logging	

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:**

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

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



# **Diagnostics – Allen-Bradley PLC**

Select the **Allen-Bradley PLC** in the dropdown menu on the Diagnostics Page to view a breakdown of the diagnostics and common strings that are displayed on the page. You may also view individual counters by selecting the device in the **All PLC's** dropdown menu and clicking **View**. Additional diagnostic information can be found by clicking the **Help** button.

## **Diagnostics**

Allen-Bradley PLC	View	Clear All Values
All PLC's 🗸	View	
All PLC's		
ETC01 10.1.16.200		Help
ETC01 10.1.16.201	teway Restart Needed	
ETC01 10.1.16.202		

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

Clear All Values - This will only affect displayed values.

1) This will reset all displayed values back to zero and clear the Status Strings.

Example: If viewing Allen-Bradley PLC – ETC01 10.1.100.18, this will only clear the values for that specific PLC. This will reduce the *All PLC's* values indirectly, otherwise select All PLCs to clear all devices.

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



- 1) Connected The gateway is connected to all the PLCs that are configured and enabled.
- 2) Nodes Missing (timed out) One or more enabled PLCs are missing.
- 3) Empty Scan List No PLCs are configured.
- 4) Dependency Protocol Faulted The dependent protocol is missing causing the communication to go to inactive.



**LED Status** - This is the Status for *All PLCs* or the specific PLC selected.

# LED Status Connection Status:

Configuration Mode

- 1) Connected (Solid Green) All the enabled PLC devices are connected and running.
- 2) Not Connected (Flashing Green) No PLCs are enabled.
  - a) Verify Allen-Bradley PLC settings and ensure that the *Enable* checkbox is checked for the appropriate device(s).
- 3) Connection Timeout (Flashing Red) The gateway cannot open a connection to one or more of the enabled PLCs.
  - a) Verify the IP, slot and controller type are accurate for the missing connection. Missing connection can be determined from the Network Bitmap Status value.
- 4) Communication not attempted yet (Flashing Red) (Specific Server Only) No reads are configured and data needed for writes isn't valid yet.
- 5) Dependency Error (Flashing Red) The dependent protocol is missing causing the communication to go to inactive.
  - a) The other protocol must be connected.

Variables - These are the values for All PLCs, or the specific PLC selected.

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

- 1) Network Bitmap Status (hex) Each bit corresponds to a PLC. If the bit is set, then the PLC is connected, otherwise the bit is 0. Bit 0 (right most) is PLC 1 and Bit 4 is PLC 5.
- 2) Read Requests Number of read requests sent from the gateway to the PLC (N2G).
- 3) Read Responses Number of valid responses sent from PLC to the gateway (G2N).



- 4) Read/Write Timeouts Since we are TCP based, the gateway will timeout on the read or write and close the TCP connection. This counter will not continually increment. The Network Bitmap Status will reflect the missing PLC.
- 5) Read Errors Number of read error responses sent from the PLC to the gateway.
- 6) Write Requests Number of write requests sent from the gateway to the PLC (G2N).
- 7) Write Responses Number of valid write responses sent from the PLC to the gateway.
- 8) Write Errors Number of write error responses sent from the PLC to the gateway.
- 9) Read Request to Response Time Number of milliseconds it took the PLC to reply to a request
- 10) Read Response to Request Time Number of milliseconds it took the gateway to execute the next request once the previous response has been received.
- 11) High Priority Read Loop Time Number of milliseconds it took to execute all high priority read requests.
- 12) Low Priority Read Loop Time Number of milliseconds it took to execute all low priority read requests.
- 13) Write Request to Response Time Number of milliseconds it took the PLC to reply to a request.
- 14) Write Response to Request Time Number of milliseconds it took the gateway to execute the next request once the previous response has been received.
- 15) Write Loop Time Number of milliseconds it took to execute all write requests.

**Common Error Strings** - These are the values for *All PLCs,* or the specific PLC selected.

- 1) IP: xxx.xxx.xxx "tagname" (04) Path Segment Error The tag name is wrong, or the tag is not defined as a controller scope tag.
- 2) IP: xxx.xxx.xxx "tagname" (08) Service Not Supported The IP address or the slot number does not match with the PLC the gateway is setup to communicate with.
- 3) IP: xxx.xxx.xxx "tagname" (1E) Embedded Server Error The tag name that is setup within the gateway doesn't match a tag setup in the PLC.
- 4) IP: xxx.xxx.xxx "tagname" (ff,2105) Access beyond end of array Tried to read/write too much data.
- 5) IP: xxx.xxx.xxx "tagname" (ff, 2107) Abbreviated type mismatch The data type of the tag, on a write, in the gateway doesn't match the tag in the PLC.



# 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**.

Diagnostics			
MQTT Client ~	View	[	Clear All Values
All Devices	View		
All Devices		_	
QT01 0.0.0.0			Help
QT02 192.168.0.100	eway Restart Needed		
QT02 192.168.0.101			
QT02 192.168.0.102	Configuration Mode		
QT02 192.168.0.103			
D	iagnostics		
N A	IQTT Client     View       II Devices     View		
D	evice Status Configuration Mode Gateway Restart Ne	eded	
L	ED Status Connection Status:	Configuration Mode	

**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**

Real Time Automation, Inc.



#### 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:	0x0000000
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 2 is for MQTT device 3 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**.

OTH	IER	
	-Select-	~
	-Select-	
	Setup LED's	
		-

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.

LED Configuration		
	LED 1 Modbus RTU Master: Connection Status V LED 2 BACnet/IP Server: Connection Status V	All Slave's  V
	Save Parameters	


# **Configuration Files**

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

OTHER				
	-Select-			
	-Select-			
	Setup LED's			
	Export / Import Config 📐			
	Export / Import Template			
	Utilities			

## **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.

What do you want to do with rta cfo.rtax?			1		
From: 10.1.16.106	Open	Save	^	Cancel	$\times$

# **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.

Real Time Automation, Inc.



Import Configuration	
	Choose File No file chosen
	Import Network Settings
	Load Configuration

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.

#### OTHER

	-Select-
	-Select-
	Setup LED's
	Export / Import Config
	Export / Import Template
	Utilities
	Time Configuration
	Email Configuration
1	Security Configuration
	Alarm Configuration
	COS Configuration

Here you can also:

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

Revisions	
	Listing of Revisions
Eile Liet	
Flie List	File List
Identify Device	
	Start Flashing LED's
0-(1)-1	
Set Up Log	Log Configuration
	Log Comguration
Revert To Last Powerup	
	Revert to Last Powerup
B (1)	
Revert All	Boyort to Manufacturing Defaulte
	Revent to Manufacturing Deladits
Reformat Flash	
	Reformat Flash

Real Time Automation, Inc.