Operating Manual

Modbus IoT Gateway

Order No.: 10254255/01

Print Spec: N/A

CR: 800000075142

WARNING!

These instructions must be provided to users before use of the product and retained for ready reference by the user. Read this manual carefully before using or maintaining the device. The device will perform as designed only if it is used and maintained in accordance with the manufacturer's instructions. Otherwise, it could fail to perform as designed, and persons who rely on this device could sustain serious injury or death.

The warranties made by MSA with respect to the product are voided if the product is not installed and used in accordance with the instructions in this manual. Please protect yourself and your employees by following the instructions.

Please read and observe the WARNINGS and CAUTIONS inside. For additional information relative to use or repair, call 1-800-MSA-2222 during regular working hours.

The Safety Company

MSA Safety
1991 Tarob Court
Milpitas, CA 95035

U.S. Support Information:
+1 408 964-4443
+1 800 727-4377
Email: smc-support@msasafety.com

EMEA Support Information:
+31 33 808 0590
Email: smc-support.emea@msasafety.com

For your local MSA contacts, please go to our website www.MSAsafety.com

Contents

1 Modbus IoT Gateway Description

The Modbus IoT Gateway is a cloud-ready device that connects Modbus and OPCUA devices to the cloud, with user tools that enable easy gateway discovery and configuration. This edge device supports seamless interoperability with Modbus, OPCUA, and MQTT, while connecting to MSA Grid - FieldServer Manager and third-party clouds.

The Modbus IoT Gateway also includes Monitor View, Data Log Viewer, Virtual Points and Event Log data analysis features that allow tracking and logging of individual device data points across the connected network in real-time.

The Modbus IoT Gateway comes in the following four model types:

- FS-IOT-MOD – includes two RS-485 ports and one Ethernet 10/100 port
- FS-IOT-MOD2 – includes two RS-485 ports and two Ethernet 10/100 ports with WAN firewall options
- FS-IOT-MODW – includes two RS-485 ports, one Ethernet 10/100 port, and supports Wi-Fi network connection
- FS-IOT-MODA, FS-IOT-MODV, and FS-IOT-MODF – includes cellular connections for the chosen carrier (AT&T, Verizon, or Vodafone). The models also have one RS-485 port, one Ethernet 10/100 port, and supports Wi-Fi network connection.

Additionally, the Wi-Fi models act as a Wi-Fi access point for web-based configuration and remote access from any mobile device without user restrictions.

For more cloud information, refer to the MSA Grid - FieldServer Manager Start-up Guide available online. The latest versions of instruction manuals, driver manuals, configuration manuals, and support utilities are also available online through the MSA Safety FieldServer page.

⚠ WARNING!

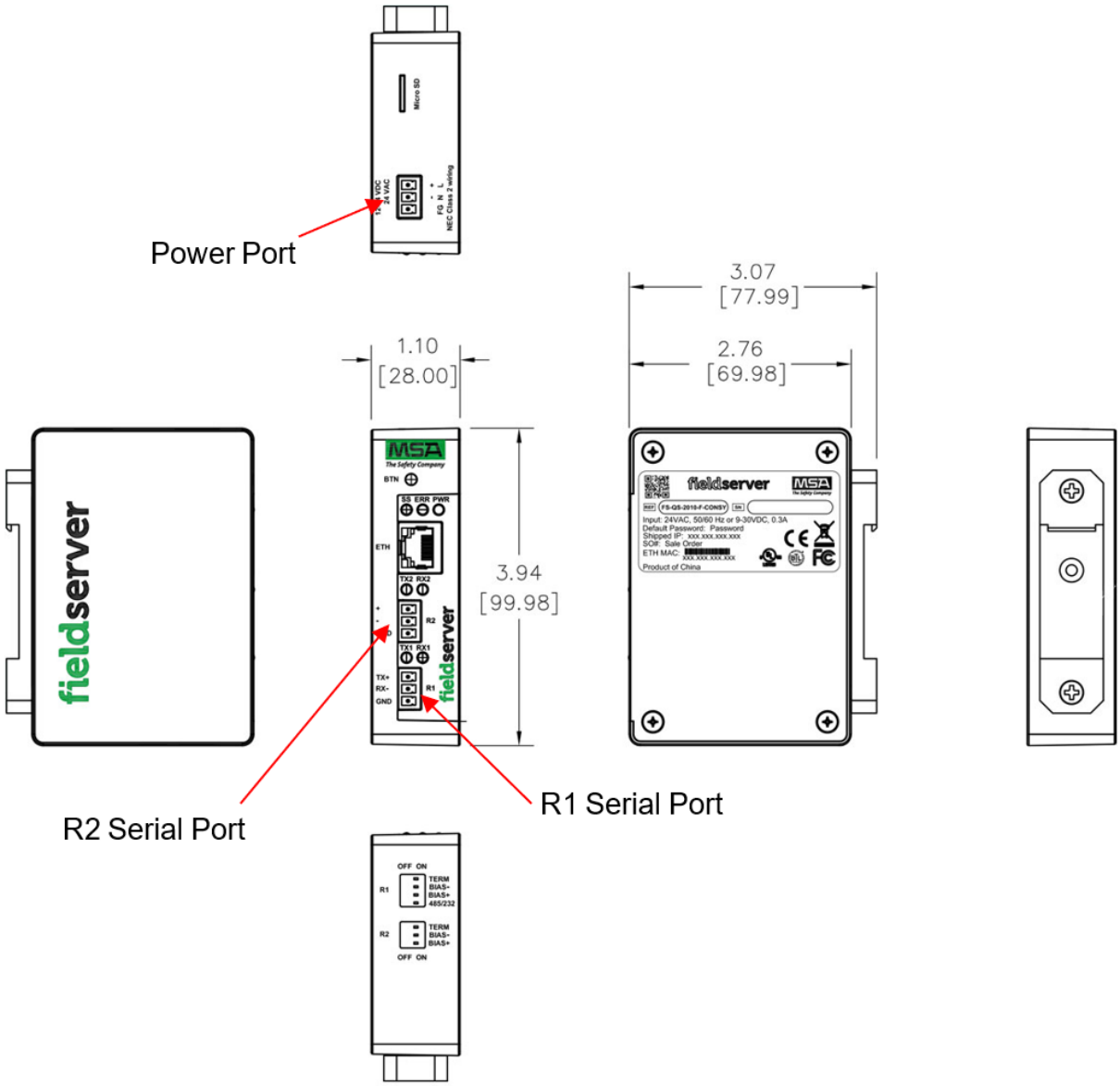
Read this manual and the manual of any device you are connecting to carefully before using or maintaining the device. The device will perform as designed only if it is used and maintained in accordance with the manufacturer's instructions.

Failure to follow this warning can result in serious personal injury or death.

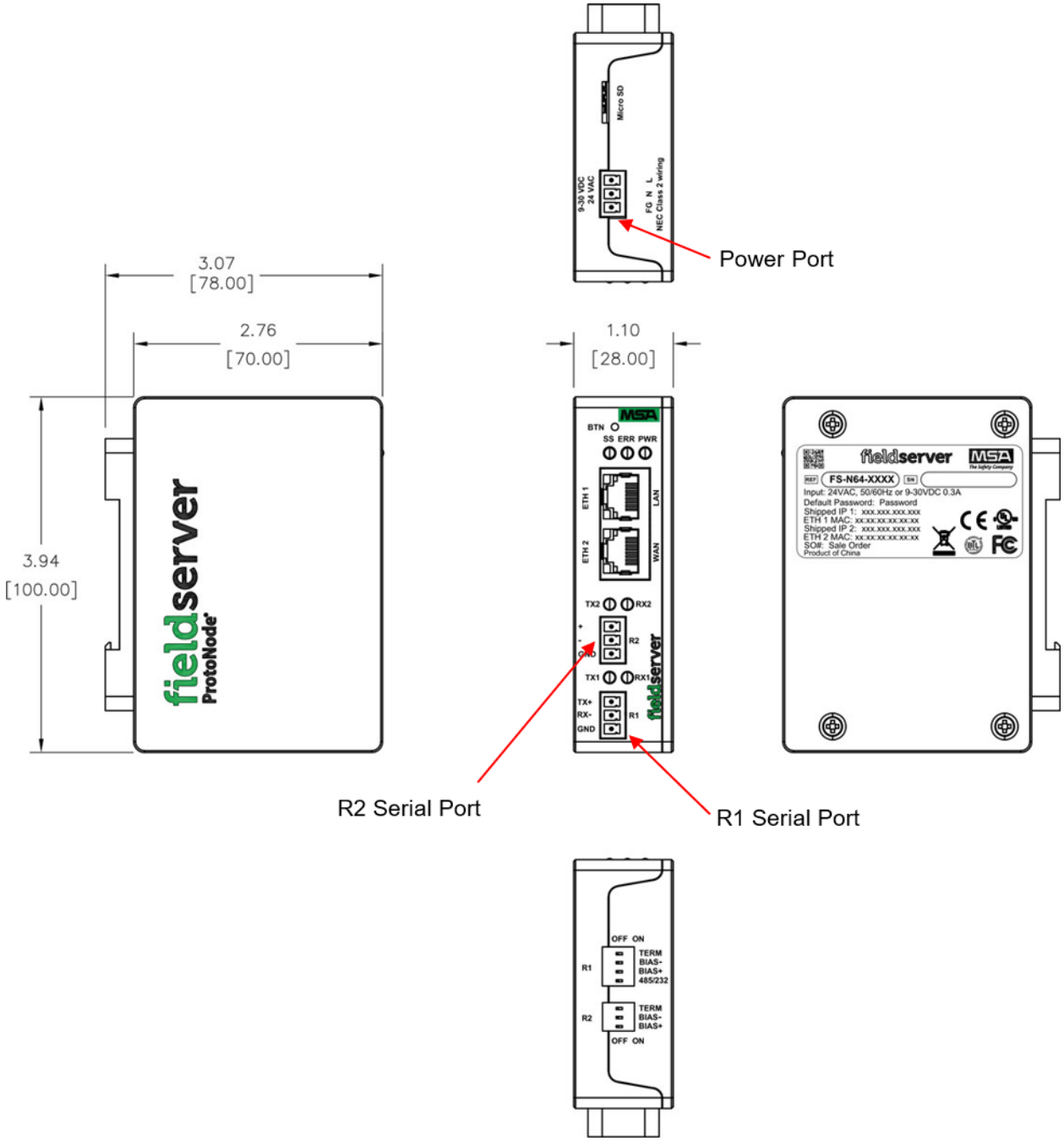
2 Equipment Setup

2.1 Physical Dimensions

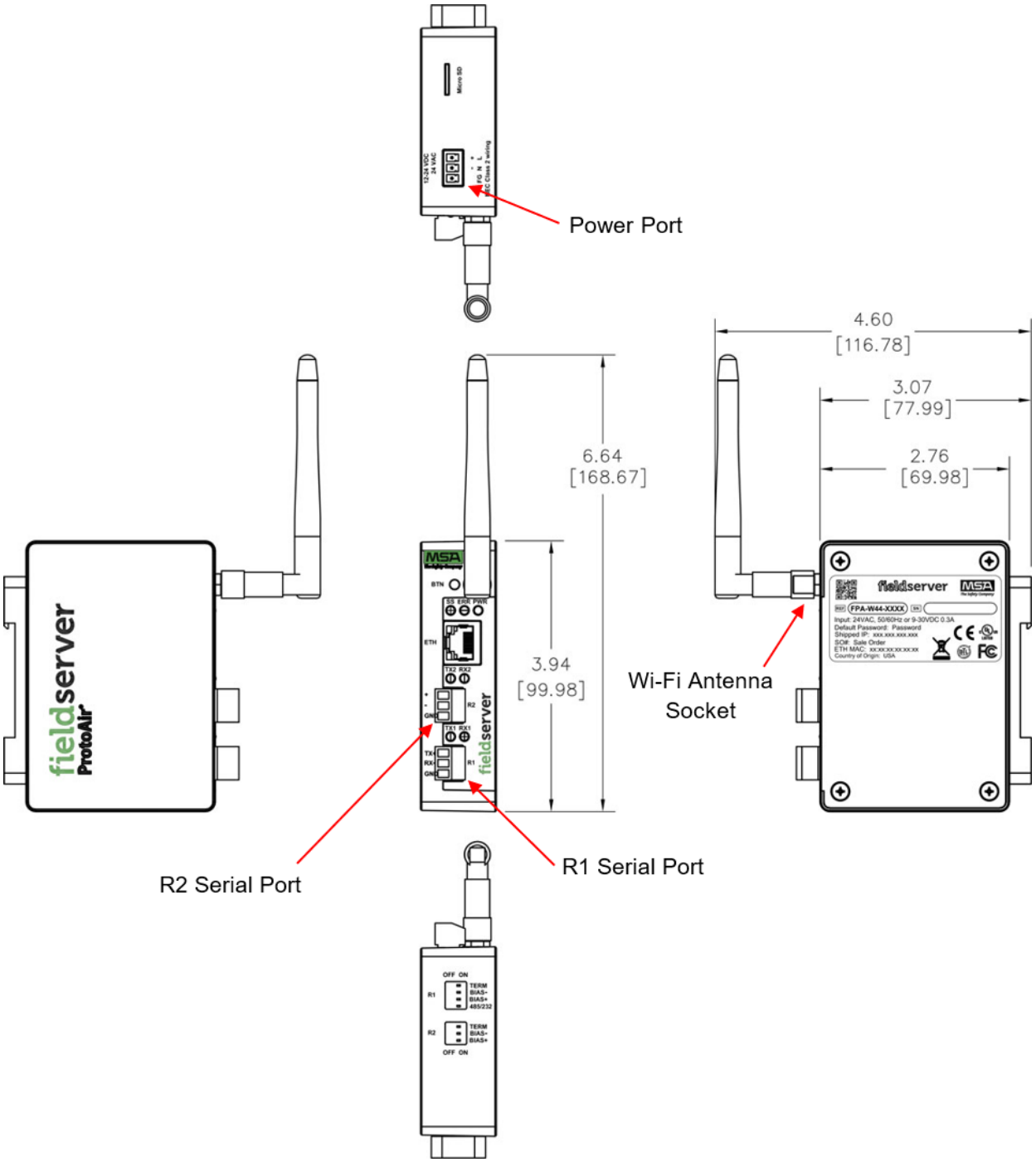
2.1.1 FS-IOT-MOD Drawing



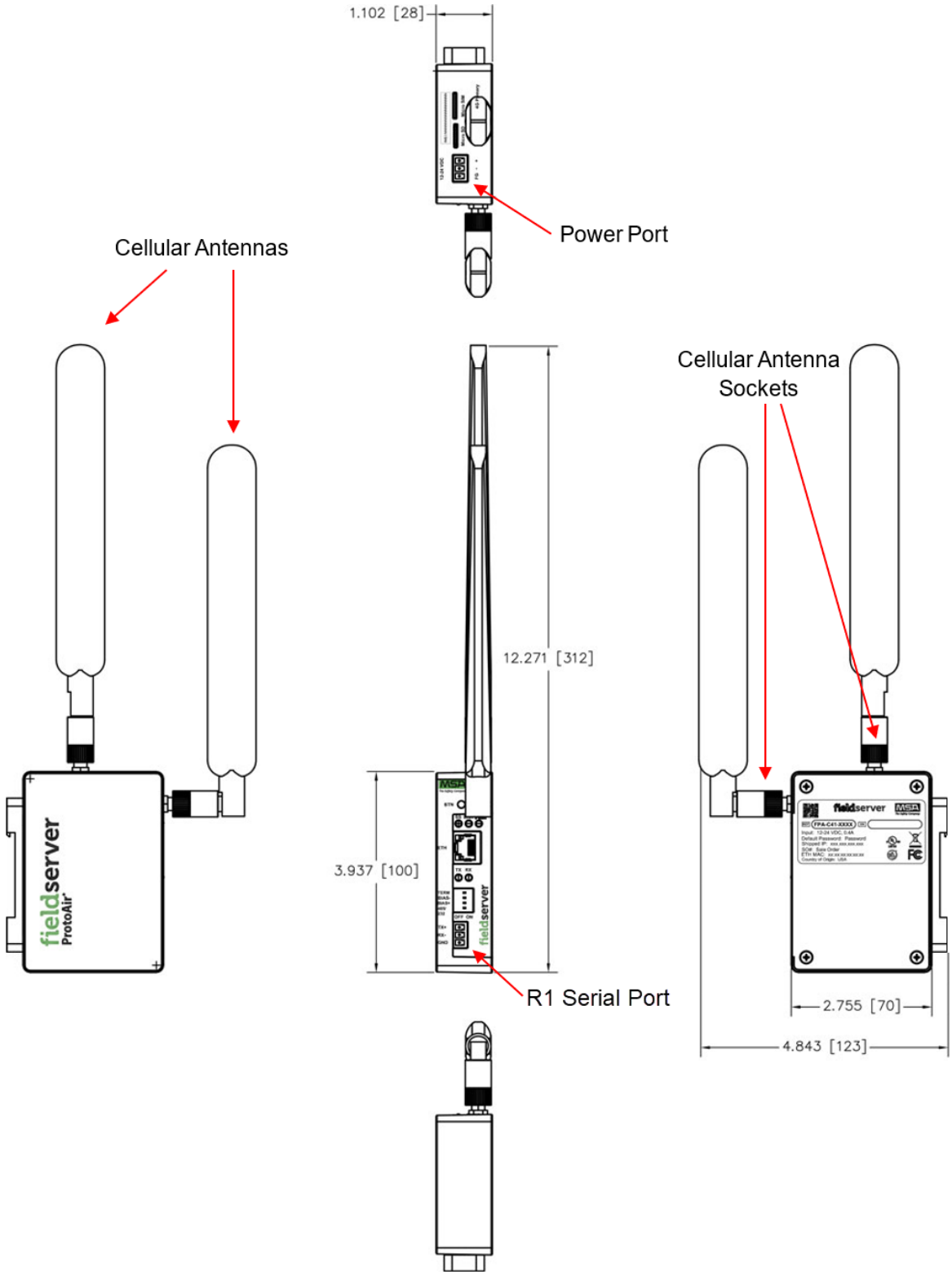
2.1.2 FS-IOT-MOD2 Drawing



2.1.3 FS-IOT-MODW Drawing

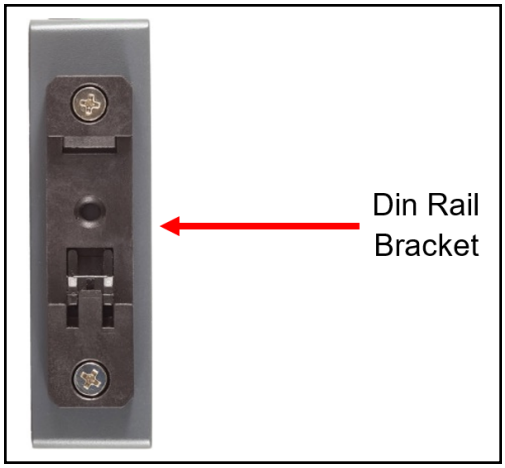


2.1.4 FS-IOT-MODA/V/F Drawing



2.2 Mounting

The gateway can be mounted using the DIN rail mounting bracket on the back of the unit.



2.3 Attaching the Antenna(s)

NOTE: This section does not apply to the FS-IOT-MOD model Modbus IoT Gateway.

If using the FS-IOT-MODW (Wi-Fi) model, screw in the Wi-Fi antenna to the front of the unit as shown in section 2.1.3 FS-IOT-MODW Drawing

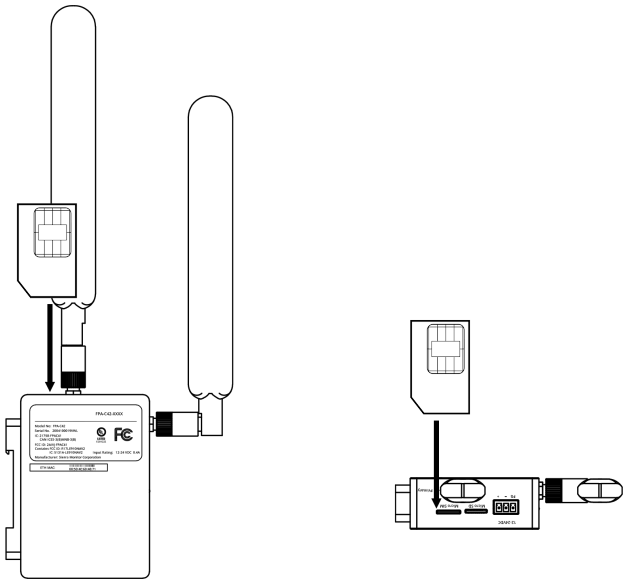
If using the FS-IOT-MODA/V/F models, screw in the two cellular antennas. One antenna is screwed into the socket on the top of the unit and one is screwed into the socket on the side as shown in section 2.1.4 FS-IOT-MODA/V/F Drawing.

2.4 Inserting the SIM Card

NOTE: To set up cellular functionality and create a data plan, a micro 4G SIM card must be purchased from AT&T, Verizon, or Vodafone.

AT&T, Verizon, and Vodafone contact information is available at the end of the section. Additionally, the IMEI can be found by accessing the FieldServer FS-GUI page and checking the Cellular network tab under “cellular model”.

With the chip on the SIM card facing away from the cellular antenna, insert the SIM card into the Micro SIM card slot as shown below.



See section **7.5 Cellular Settings (FS-IOT-MODA/V/F)** to complete cellular configuration.

SIM Card Vendor Contact Information:

- Verizon - A business contract is required to purchase a Verizon SIM card. The IMEI of the Modbus IoT Gateway is required to purchase the Verizon SIM card.
- AT&T - Call AT&T Customer Service at 800.331.0500 or find the nearest AT&T store.
- Vodafone - Contact the nearest Vodafone store.

3 Installation

⚠ WARNING!

- This gateway needs to be installed by a systems integrator who has basic electrical installation knowledge to prevent damage to the gateway.
- All installation and wiring must be performed in accordance with applicable local electrical codes and regulations. It is the responsibility of the installer to ensure that the installation complies with all relevant safety and legal requirements. Failure to adhere to these codes may result in unsafe operation, equipment damage, or violation of local laws.
- This product is not intended for use by the general public. It is generally intended for industry/commercial use.

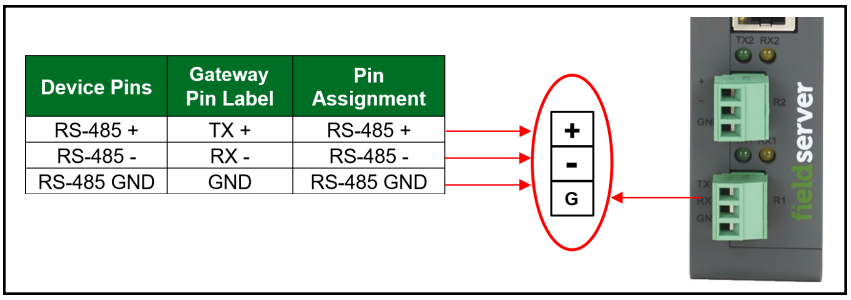
Failure to follow this warning can result in serious personal injury or death.

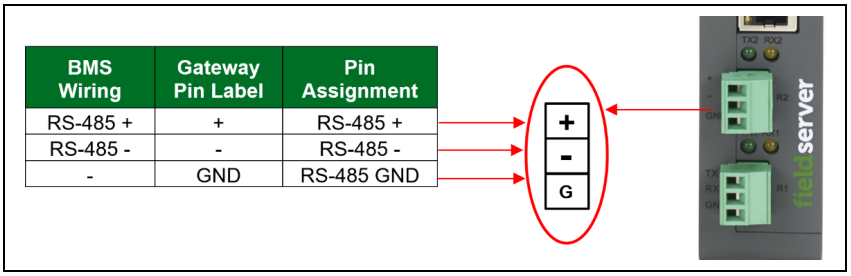
3.1 Connecting the R1 & R2 Ports (FS-IOT-MOD/MODW/MOD2)

For the R1 port only: The user can switch between RS-485 and RS-232 by moving the number 4 DIP switch left for RS-485 and right for RS-232 (see images below).

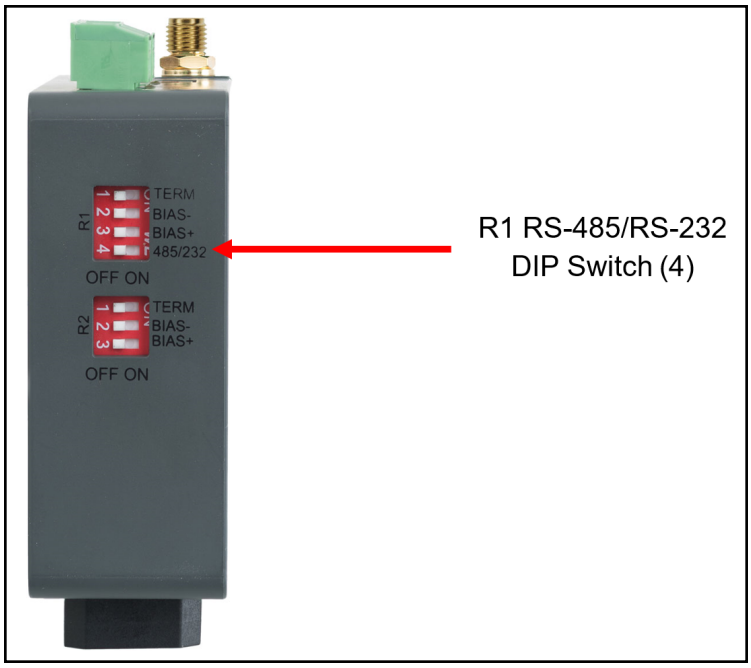
The R2 port is RS-485.

Connect to the 3-pin connector(s) as shown below.





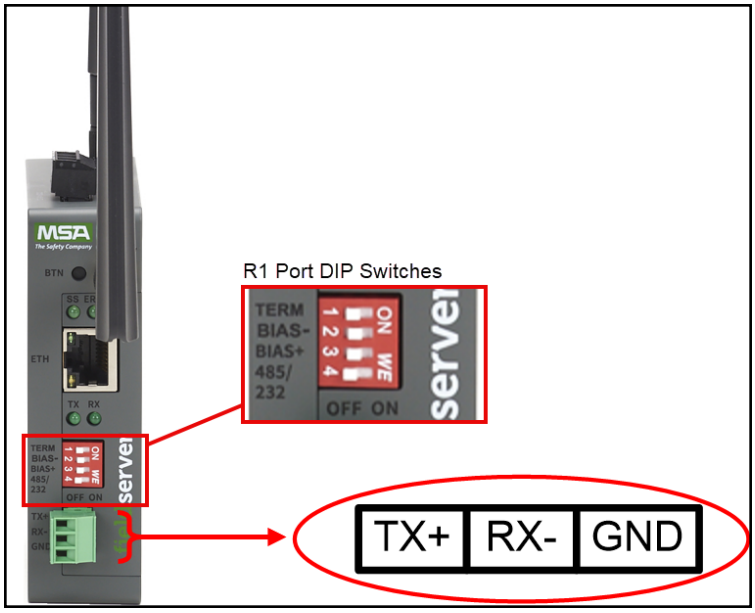
For the R1 port, ensure RS-485 is selected by checking the number 4 DIP switch is set to the left side, using the orientation in the image shown below.



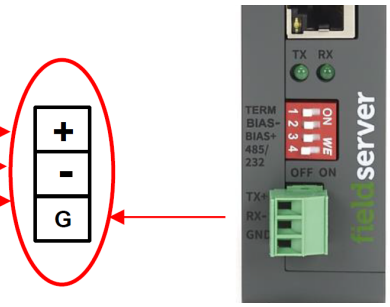
The RS-485/RS-232 interface and must be connected to the corresponding terminal on the BMS. If the cable is shielded, the shield must connected only at one end and to earth ground. This will help suppress the electromagnetic field interference. Connecting the shield at both ends will likely produce current loops, which could produce noise or interference that the shield was intended to block.

3.2 Connecting the R1 Port (FS-IOT-MODA/V/F)

For the R1 Port, ensure RS-485 is selected by checking the number 4 DIP Switch is set to the left side and connect the 3-pin connector. Use the images below for the correct settings.



Device Pins	ProtoAir Pin Label	Pin Assignment
RS-485 +	TX +	RS-485 +
RS-485 -	RX -	RS-485 -
RS-485 GND	GND	RS-485 GND

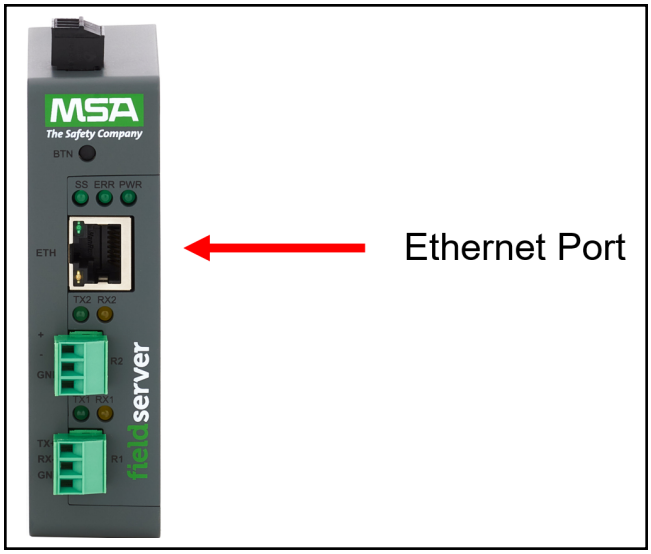


3.3 10/100 Ethernet Connection Port

NOTICE

Do not use shielded ethernet cables. The ethernet shield is connected to the internal 0V (digital ground) of the Modbus IoT Gateway. Using shielded ethernet cables could potentially create ground loops that damage the Modbus IoT Gateway or equipment connected to it, and void the warranty.

Failure to follow this notice will result in damage to the device.



The ethernet port is used both for ethernet protocol communications and for configuring the Modbus IoT Gateway via the web app. To connect the Modbus IoT Gateway, either connect the PC to the Modbus IoT's ethernet port or connect the Modbus IoT and PC to an ethernet switch. Use Cat-5 cables for the connection.

The default IP address of the Modbus IoT Gateway is 192.168.2.101, and the subnet mask is 255.255.255.0. For the FS-IOT-MOD2, the ETH 2's default IP address is 192.168.3.101.

The ETH2 port can be set to WAN mode to limit ethernet traffic. See section 7.7 Ethernet 2 Network Settings – WAN Mode (FS-IOT-MOD2) for details.

ETH1 and ETH2 must be configured with IP addresses on different IP subnets.

If the FS-IOT-MOD2 is a client on ETH1 and a server on ETH2 using the same protocol, the TCP or UDP ports need to be unique among the ETH1 and ETH2 ports.

3.4 Antenna Selection and Installation

The Modbus IoT Gateway uses SMA antennas. The antennas must be of the same type with lower or equal gain per the following table.

Frequency (MHz)	Antenna Type	Max Antenna Gain
2402-2480	Linear vertical Omnidirectional	2
2412-2462	Linear vertical Omnidirectional	2

4 Powering up the Modbus IoT Gateway

Check power requirements in the table below.

	Current Draw Type		
Modbus IoT Gateway Family	12VDC	24VDC	24VAC
FS-IOT-MOD/MODW/MOD2 (Typical)	250mA	125mA	125mA
FS-IOT-MOD/MODW/MOD2 (Maximum)	315mA	180mA	180mA
FS-IOT-MODA/V/F (Typical)	320mA	185mA	N/A
FS-IOT-MODA/V/F (Maximum)	670mA	390mA	N/A

Figure 1 Power Requirements for the Modbus IoT Gateway

WARNING!

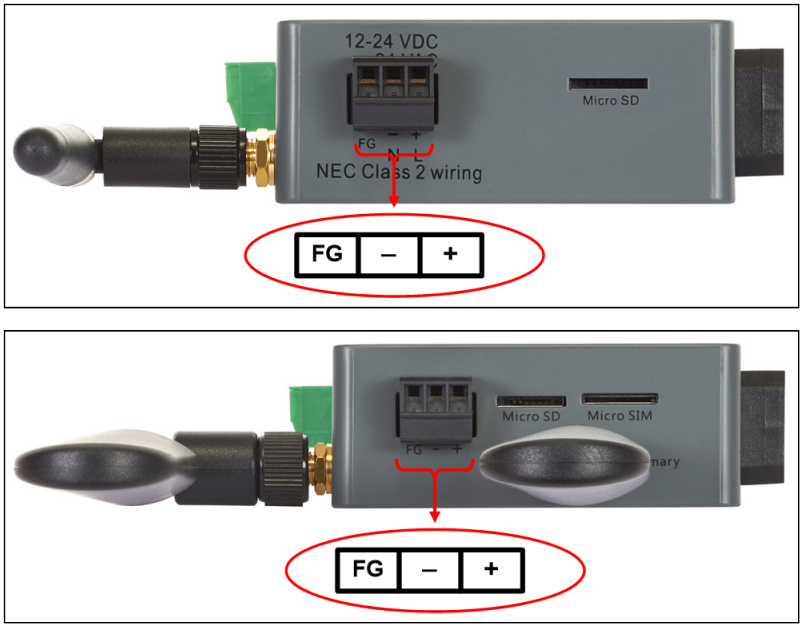
- Ensure that the power supply used complies with the specifications provided in section 15 Specifications.
- Ensure that the cable is grounded using the FG or “Frame GND” terminal.
- Frame GND should be connected to ensure personal safety and to limit material damages due to electrical faults. Ground planes are susceptible to transient events that cause sudden current surges. The frame ground connection provides a safe and effective path to divert the excess current from the equipment to earth ground.

Failure to follow these warnings can result in serious personal injury or death.

Apply power to the Modbus IoT Gateway as shown below.

- The FS-IOT-MOD/MODW/MOD2 Modbus IoT Gateway accepts 12-24VDC or 24VAC.
- The FS-IOT-MODA/V/F Modbus IoT Gateway accepts 12-24VDC.

NOTE: Only Class 2 Power Supply Units (PSUs) must be used to power the Modbus IoT Gateway.



5 Accessing Modbus IoT Gateway Using a Web Browser

1. Open a web browser and connect to the Modbus IoT Gateway's default IP address. The default IP address of the Modbus IoT Gateway is **192.168.2.101**, and the subnet mask is **255.255.255.0**. The default IP address of ETH 2 on FS-IOT-MOD2 is **192.168.3.101**.

If your PC's network settings prevent you from accessing the default IP address, you will need to temporarily modify your PC's network settings to access the Modbus IoT Gateway and change its network settings by following the steps below:

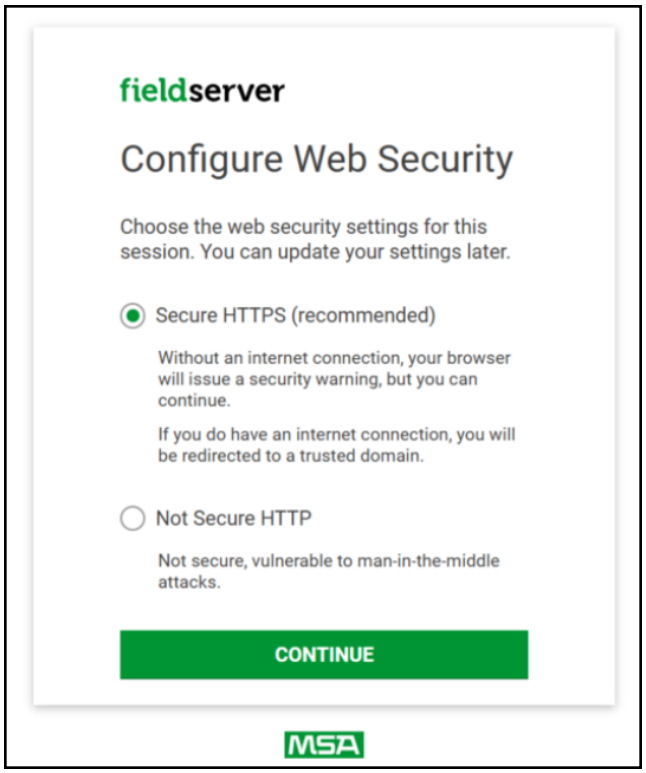
1. Make a note of your PC's network settings so that you can restore them later.
2. Assign a static IP address to the PC on the 192.168.2.X network and set the netmask to 255.255.255.0.
3. Open a browser to the Modbus IoT Gateway on 192.168.2.101.
4. Modify the Modbus IoT Gateway's network settings to work on your network (either by enabling DHCP, or by setting a new static IP Address).
5. Revert your PC's network settings to their original state to connect to the Modbus IoT Gateway at its new address.

If the IP address of the Modbus IoT Gateway has been changed or lost, the IP address can be discovered using the FS Toolbox utility. See section 16.2 Lost or Incorrect IP Address for instructions.

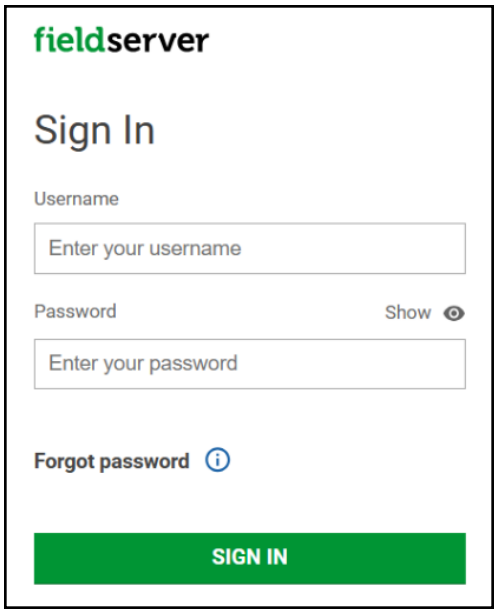
For supported browsers, check section 16.9 Internet Browser Software Support

6 Logging into the Modbus IoT Gateway

The first time the Modbus IoT Gateway GUI is opened in a browser, the IP address for the Modbus IoT Gateway will appear as untrusted. This will cause the following pop-up windows to appear.



1. Select the security level. MSA recommends using the Secure HTTPS option. After selecting the security level, the user will be forwarded to the login screen.



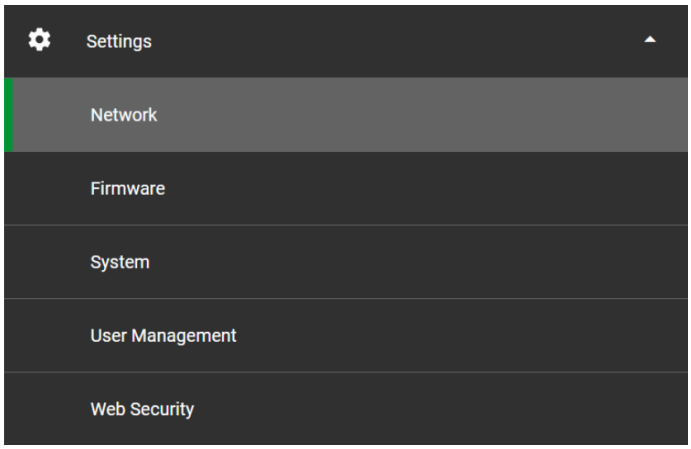
2. Enter “admin” in the username field.
3. Enter the default password found on the label of your unit into the password field.
    a. Alternatively, scan the QR code located on the product label. For convenience and accuracy, we recommend copying the password and pasting it in a text document to make future steps easier.
4. Click Sign In. After logging in, you will go through the product set up tour.
5. Click “Next” to continue on with the tour or click the X to skip.

After three incorrect login attempts, there will be a 10-minute lockout. Power cycling the Modbus IoT Gateway will reset the lockout timer.

Cookies are used for authentication. To change settings later or add user generated certificates, go to section 17.2 Changing Web Server Security Settings After Initial Setup.

7 Configuring the Network

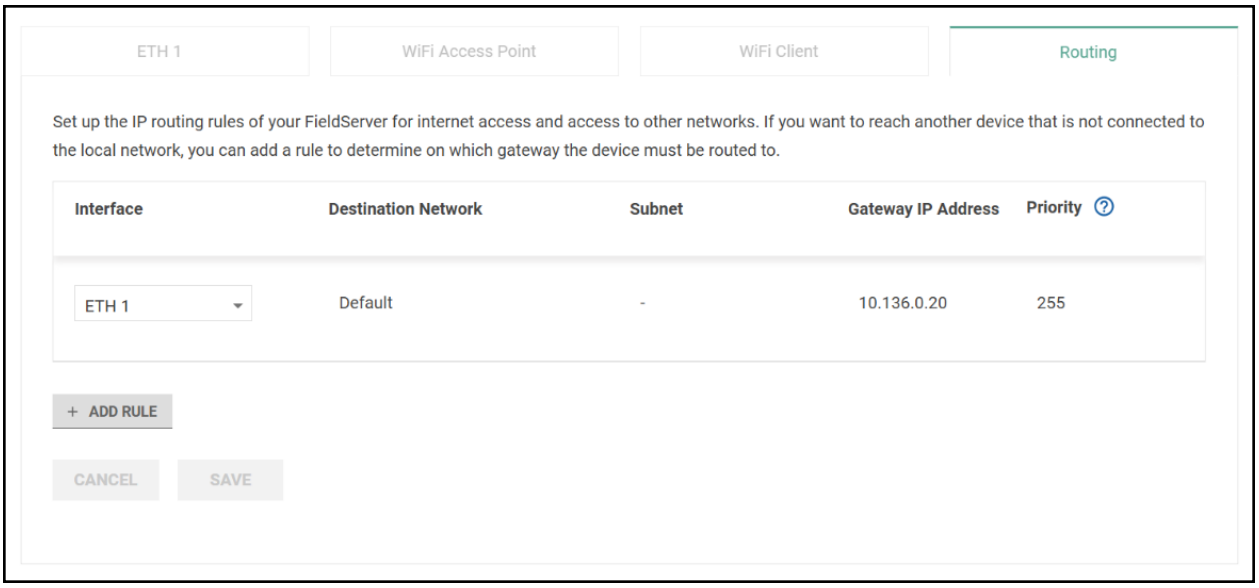
1. From the Web App landing page, click the Settings tab on the left side of the screen.
2. Click on the Network tab.



7.1 Routing Settings

The routing settings tab make it possible to set up the IP routing rules for the Modbus IoT Gateway's internet and network connections.

1. For FS-IOT-MOD2, select the interface in the first row as either ETH 1 or ETH 2. By default, it is set to ETH1.



2. Click the Add Rule button to add a new row and set a new destination network, netmask, and gateway IP address as needed.
3. Set the priority for each connection (1-255 with 1 as the highest priority and 255 as the lowest).
4. Click the Save button to activate the new settings.

7.2 Ethernet 1 Network Settings

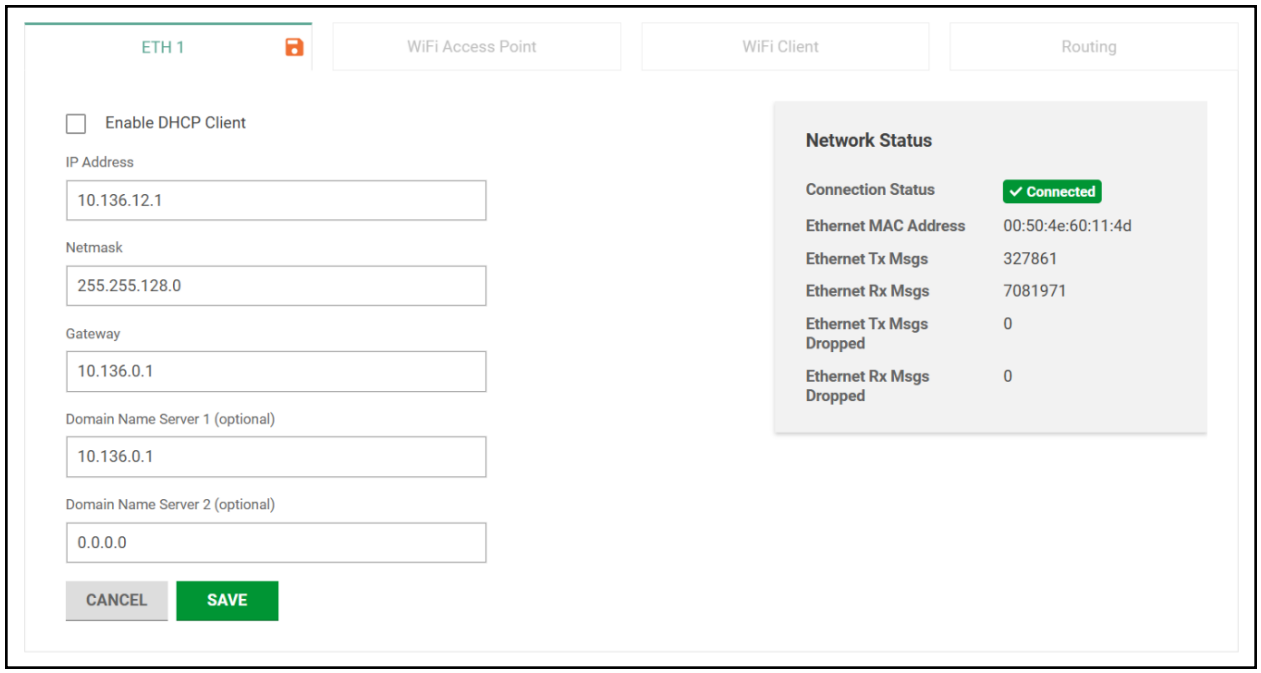
The ETH 1 tab is the landing page when selecting the Network settings tab. To change the Modbus IoT Gateway IP settings, follow these instructions:

1. Enable DHCP to automatically assign IP settings or modify the IP settings manually as needed, via these fields: IP Address, Netmask, Default Gateway, and Domain Name Server1/2.

NOTE: If the Modbus IoT Gateway is connected to a router, the IP gateway of the FieldServer must be set to the same IP address of the router.

2. Click Save to record and activate the new IP address.
3. Connect the FieldServer to the local network or router.

After changing the IP address, the browser needs to be updated to the Modbus IoT Gateway's new IP address before the settings will be accessible again.

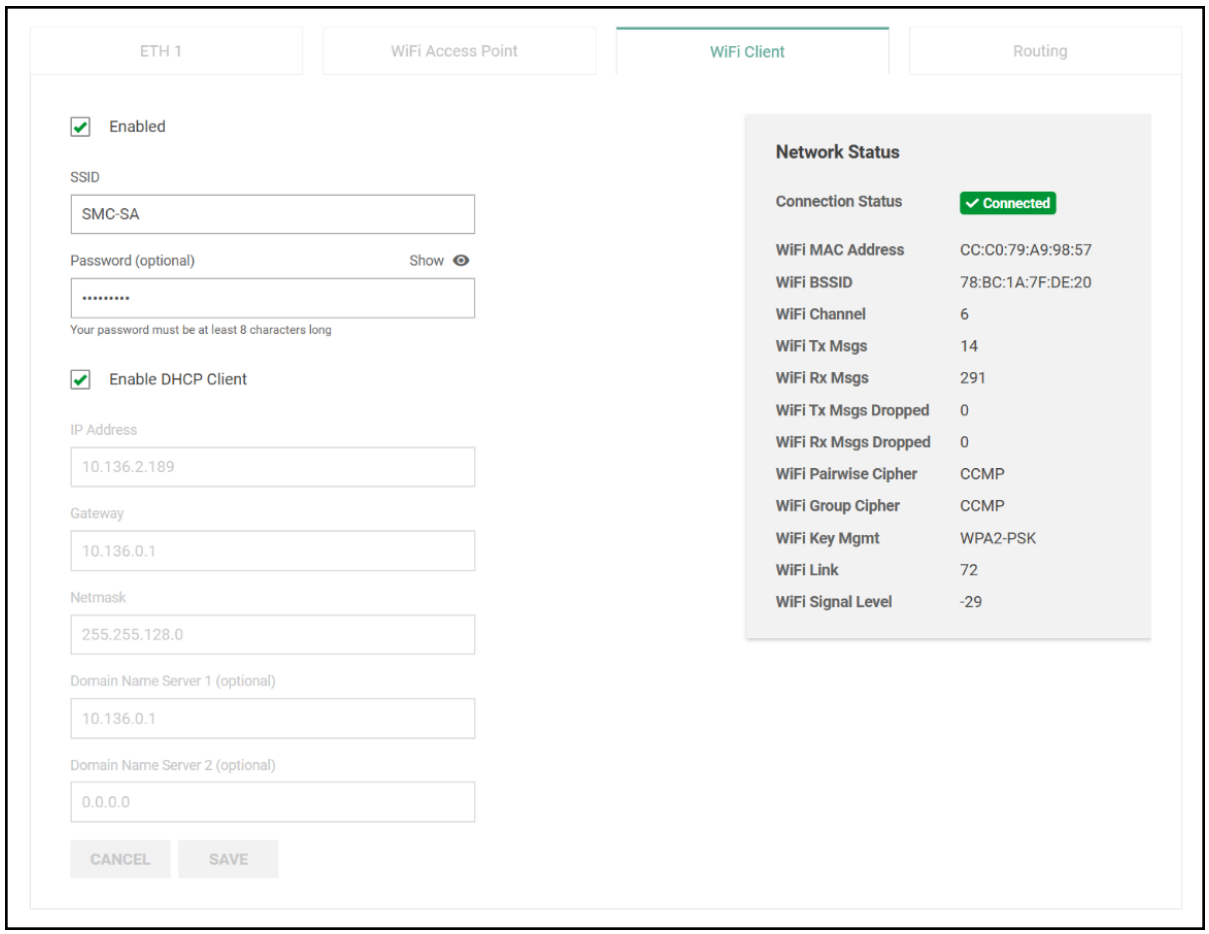


7.3 Wi-Fi Client Settings

1. Go to the WiFi Client tab.
2. Check the Enable/Enabled checkbox for the Modbus IoT Gateway to communicate with other devices via Wi-Fi.
3. Enter the Wi-Fi SSID and Wi-Fi Password for the local wireless access point.
4. Enable DHCP to automatically assign all Wi-Fi client settings or modify the settings manually, via the available fields on the screen.

NOTE: If connected to a router, set the IP gateway to the same IP address as the router.

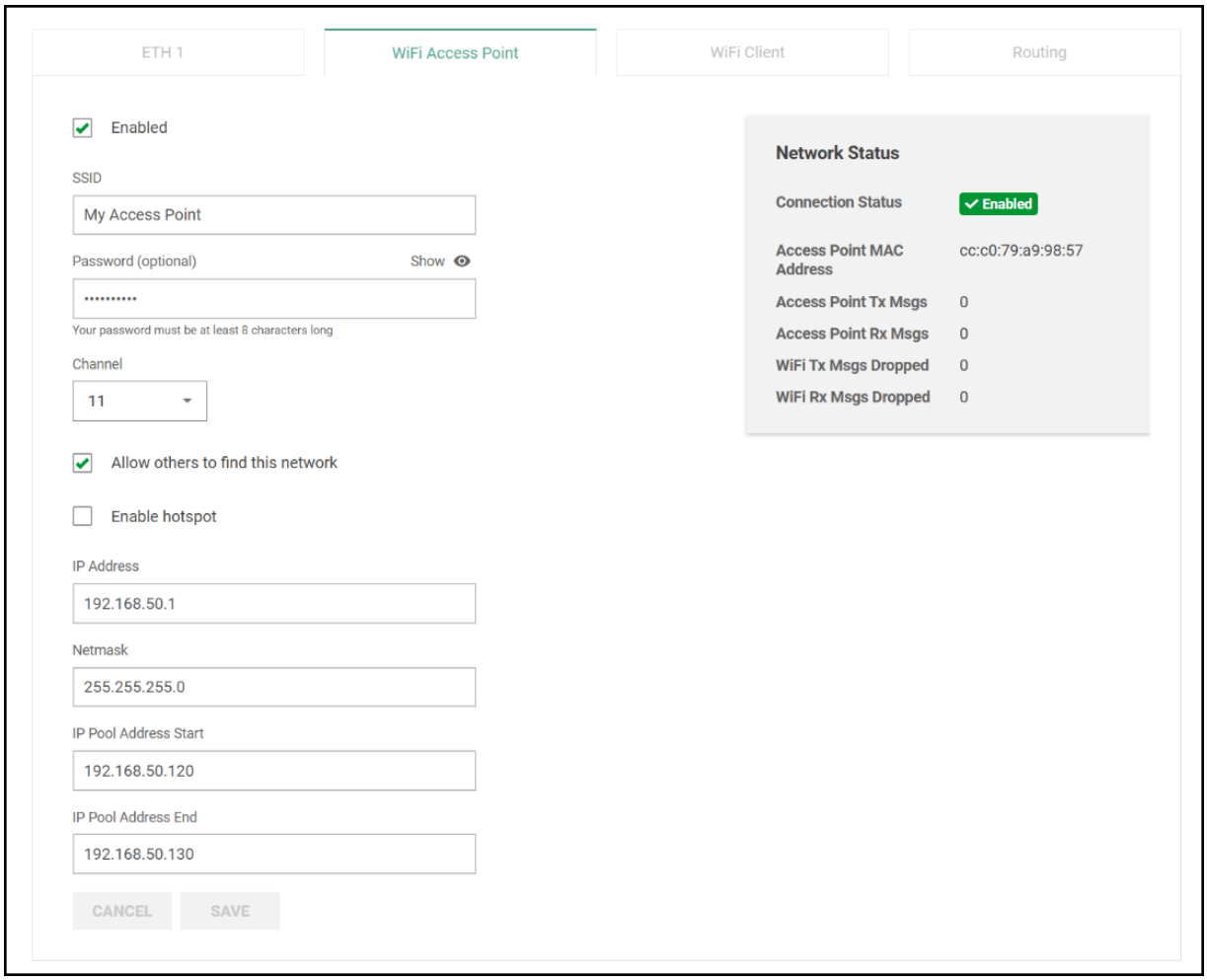
5. Click the Save button to activate the new settings.



6. Go to the Routing tab to set the default connection to Wi-Fi Client. See section 7.1 Routing Settings for more info.

7.4 Wi-Fi Access Point Settings

1. Go to the WiFi Access Point tab.
2. Check the Enable checkbox to allow connecting to the Modbus IoT Gateway via Wi-Fi Access Point.
3. Modify the settings manually as needed. The default channel is 11, and the default IP address is 192.168.50.1. The rest of the default settings are listed in the screenshot below.

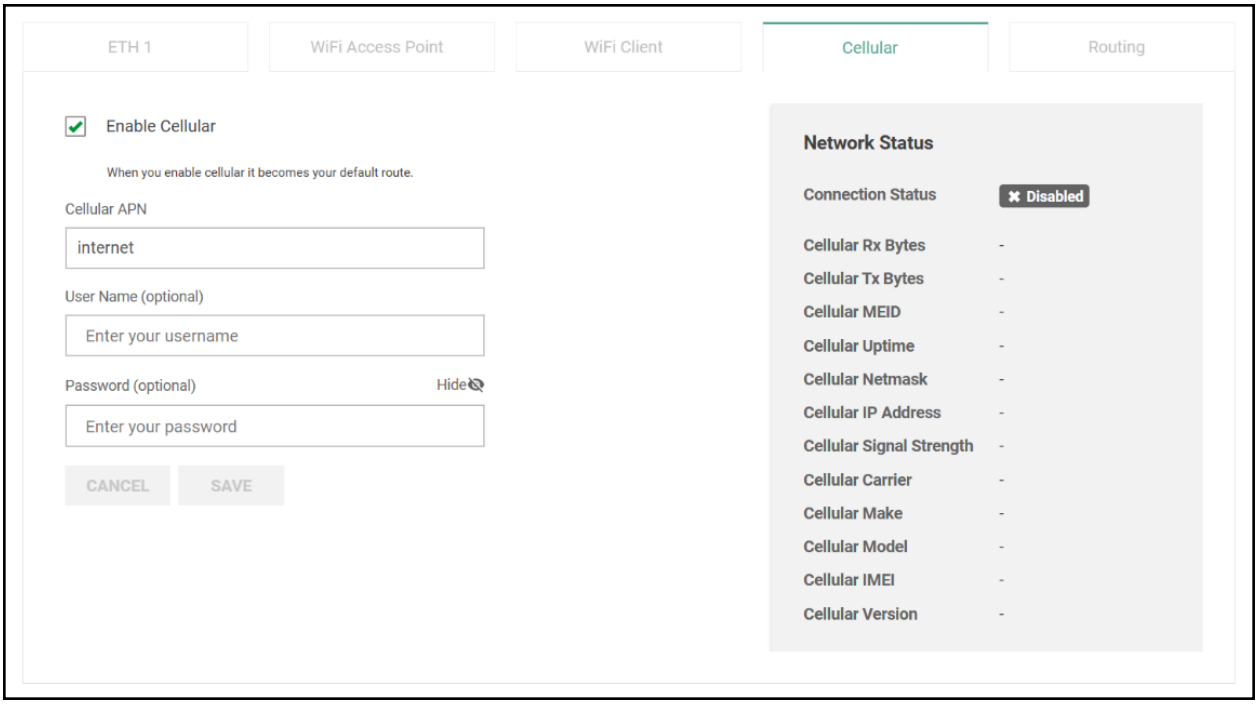


4. Click the Save button to activate the new settings.

If the webpage was opened in a browser via Wi-Fi, the browser will need to be updated with the new Wi-Fi details before the webpage will be accessible again.

7.5 Cellular Settings (FS-IOT-MODA/V/F)

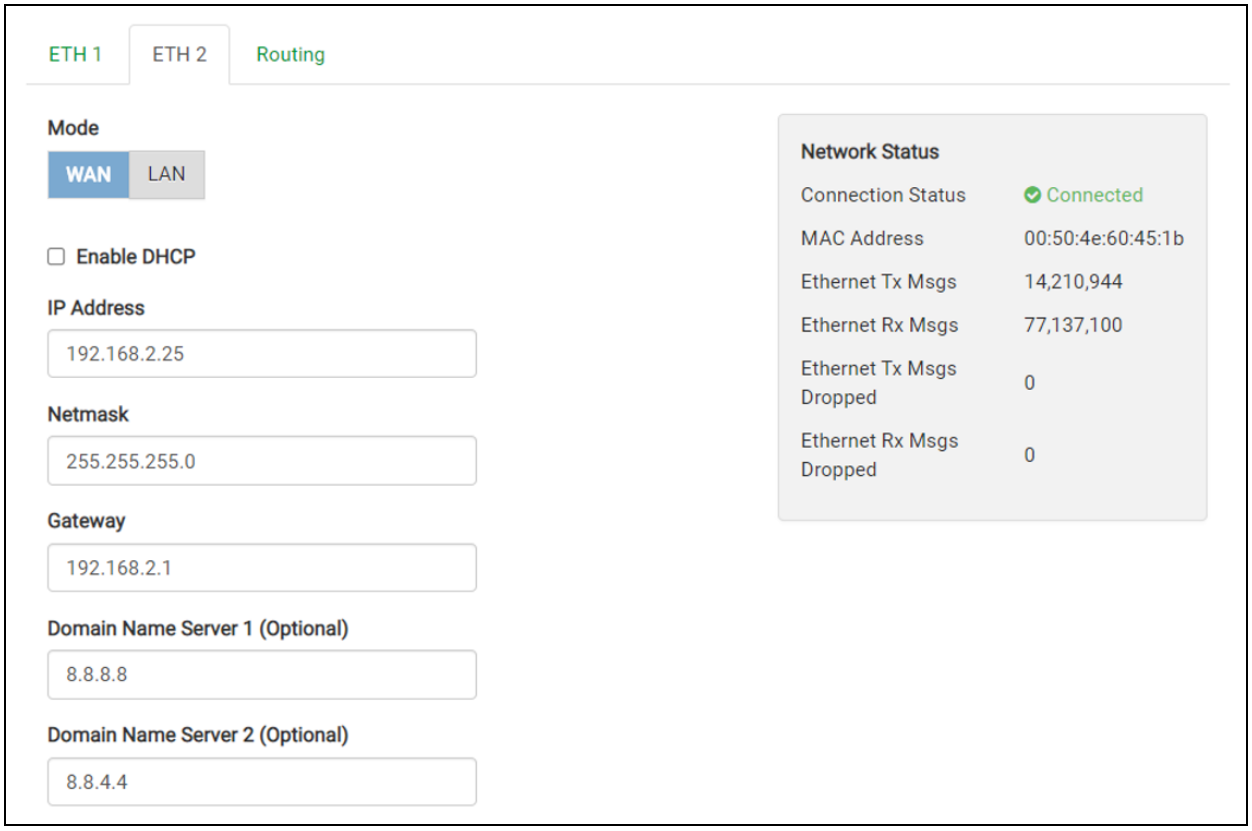
1. Go to the Cellular tab.
2. Check the Enable checkbox to allow connecting to the Modbus IoT Gateway through the Grid.
3. Modify the settings manually as needed, via these fields: Cellular APN (see section **17.1 APN Table**), User Name, and Password.



4. Click the Save button to activate the new settings.
5. Power cycle the Modbus IoT Gateway to update settings.

7.6 Ethernet 1 and Ethernet 2 Network Settings – LAN Mode (FS-IOT-MOD2)

1. Go to the ETH 2 tab.
2. Check that the Mode is set to LAN. If not, click LAN to change the ETH 2 port to LAN mode.
3. Enable DHCP to automatically assign IP settings or modify the IP settings manually as needed, via these fields: IP Address, Netmask, Gateway, and Domain Name Server1/2. If connected to a router, set the Modbus IoT Gateway to the same IP Address as the router.

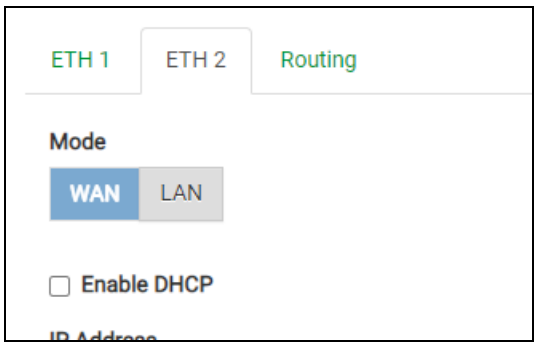


4. Click Save to record and activate the new IP address.
5. Connect the Modbus IoT Gateway to the local network or router.

If the webpage was open in a browser, the browser will need to be changed to the new IP address of the Modbus IoT Gateway before the webpage will be accessible again.

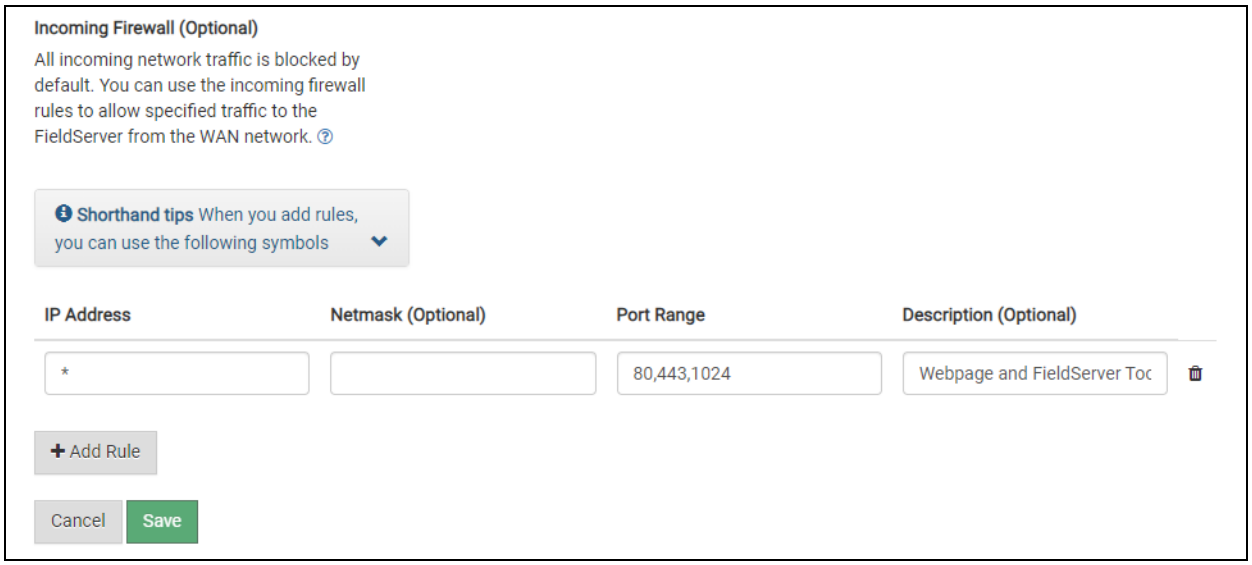
7.7 Ethernet 2 Network Settings – WAN Mode (FS-IOT-MOD2)

1. Go to the ETH 2 tab.
2. Click the blue WAN box to change the ETH 2 port to WAN mode. This prevents all unwanted incoming traffic on the ETH 2 port. It also allows an internet connection via port 80 & 443.



3. Scroll below the network settings for the firewall options with rules that allow specific incoming traffic and outgoing options. Firewall rule options are as follows:

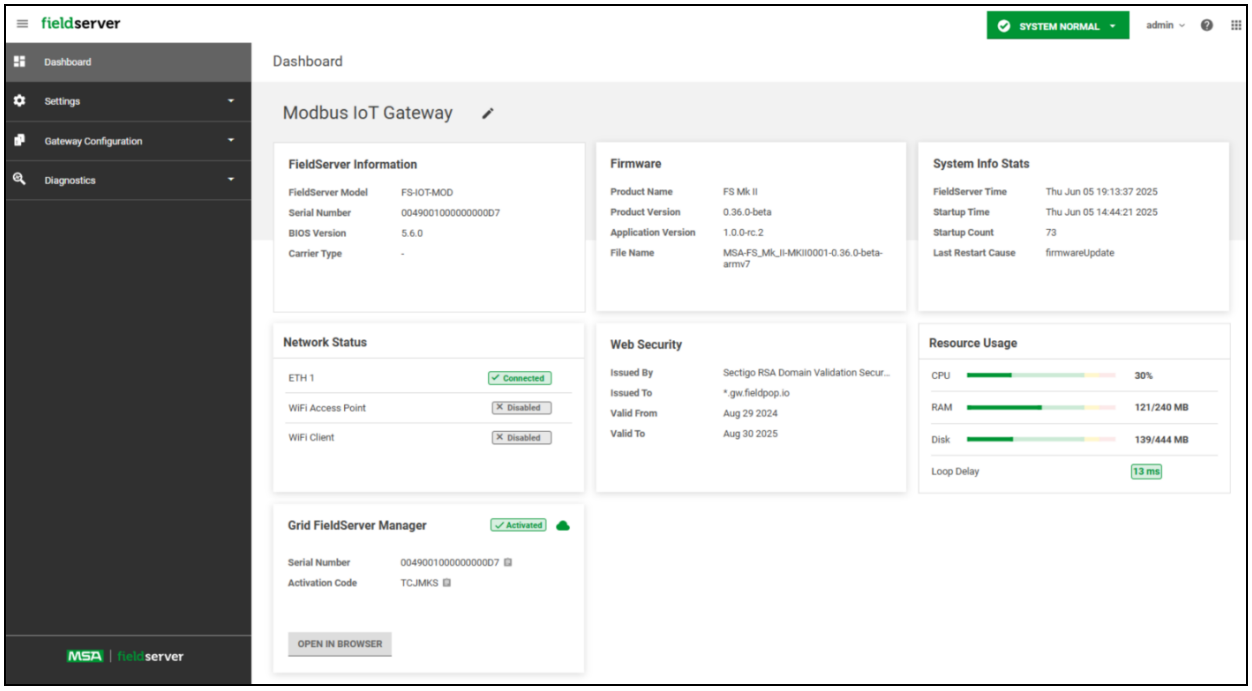
   - Add 1023 to the Port Range field to allow FieldServer Toolbox access
   - Add 80 & 443 to the Port Range field for web browser access
   - Use an asterisk (*) as a wild card for IP address



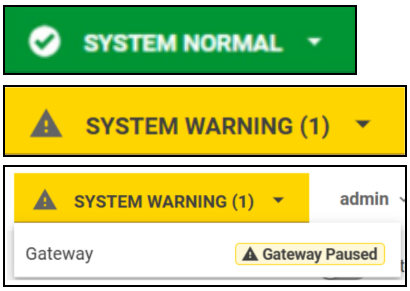
8 Using the Modbus IoT Gateway

8.1 Dashboard Features

Once the web server setup is complete, the Modbus IoT Gateway landing page Dashboard will appear.



At the top right of your dashboard, there is an admin toolbar. Toolbar features are detailed below.



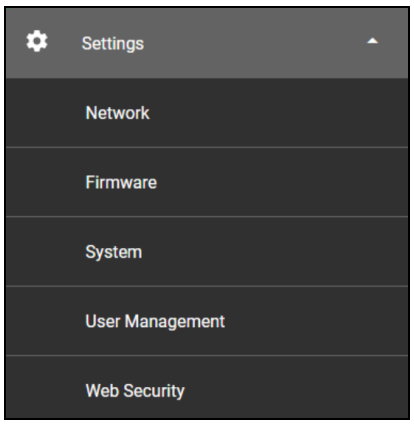
a. **System Status Indicator** – Color is green for normal status and changes color if there is a problem. Click the down arrow to see additional information.

b. **Logged-in User** – Click on it to change the password or log out of the system for the current user.

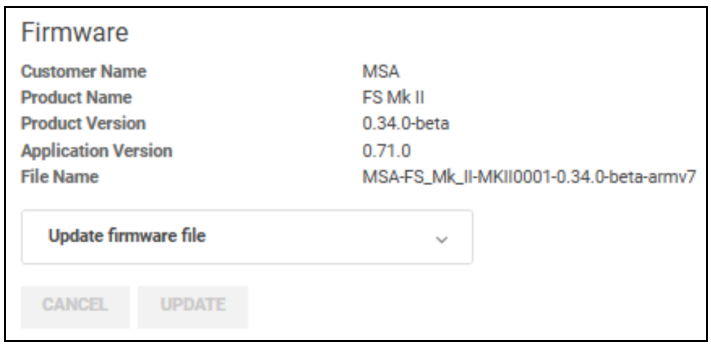
For Network Configuration, see Section 7 Configuring the Network. For Web Security Configuration, see Section 17.2 Changing Web Server Security Settings After Initial Setup.

8.2 Updating Firmware

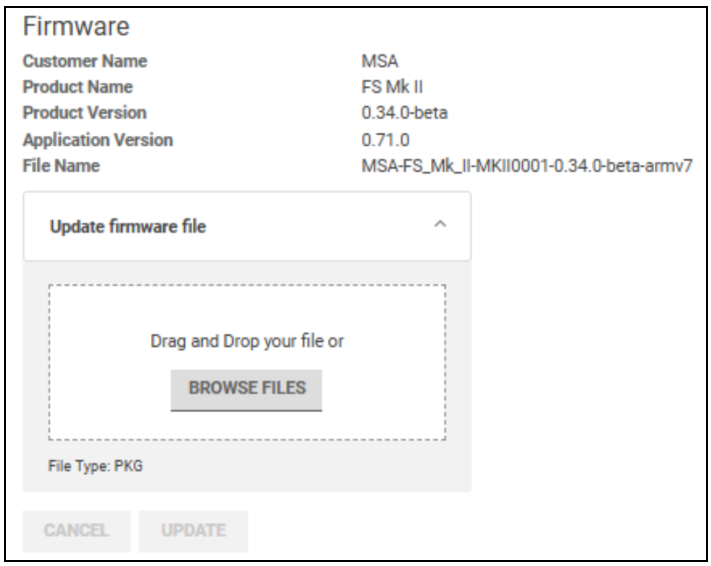
1. Click on Settings to expand the drop-down menu.



2. Click the Firmware tab.
3. Click "Update firmware file" to expand the section.



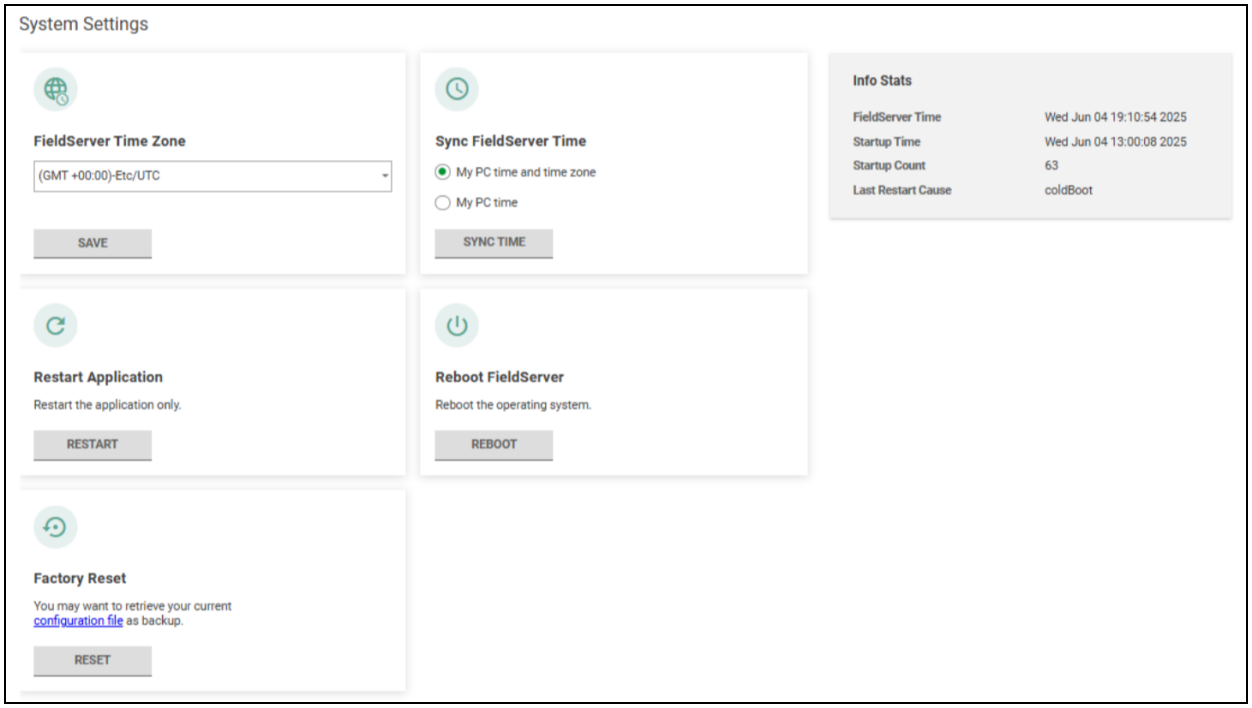
4. Click the "BROWSE FILES" button and choose the file from your local PC.



5. Click "UPDATE" to update your firmware.

8.3 Changing System Settings

In the System tab under Settings, you can view the following information:



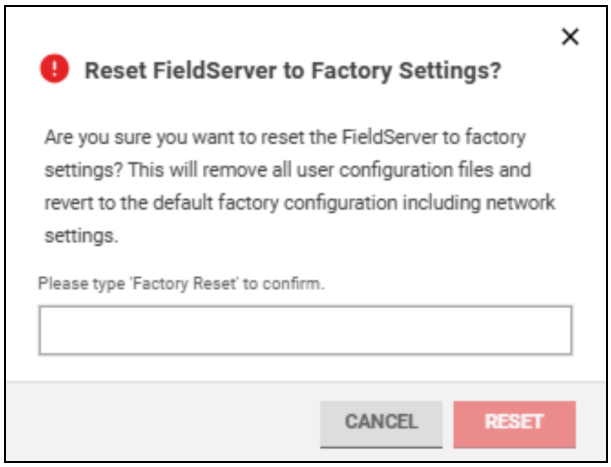
FieldServer Time Zone – Changes the Modbus IoT Gateway timezone.

Sync FieldServer Time – Syncs the Modbus IoT Gateway to this PC's time and/or timezone.

Restart Application – Restarts the Modbus IoT Gateway Software.

Reboot FieldServer – Performs a operating system reboot.

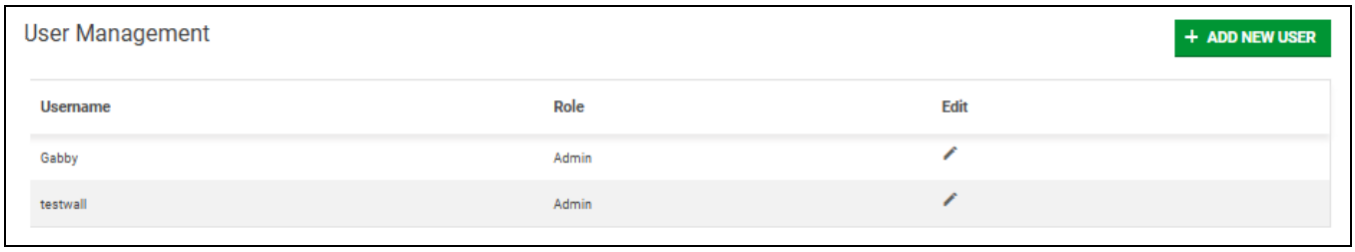
Factory Reset – Resets the Modbus IoT Gateway to the settings as shipped from MSA, including passwords, configurations etc. The following window will appear.



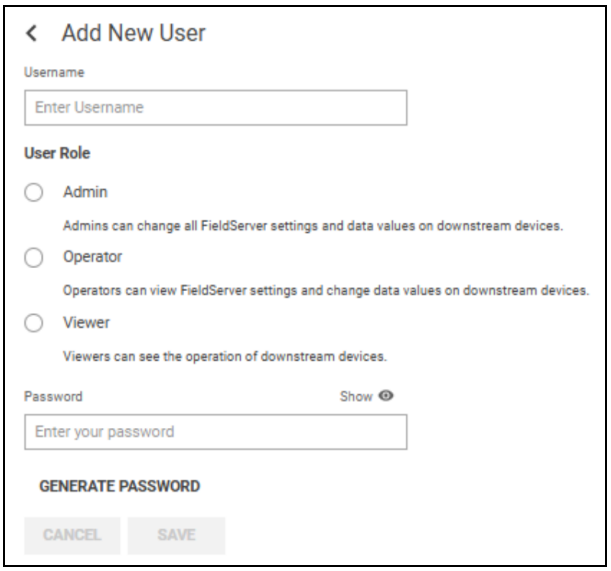
NOTE: Performing a Factory reset will completely clear all saved configuration files, security settings, users and network settings, reverting the unit to the default factory configuration.

8.4 Managing and Adding Users

1. Click the User Management tab under Settings in the navigation panel.



2. Click the green + ADD NEW USER button to add a new user, or the pencil icon to edit an existing user. You can select a role from the following user types.

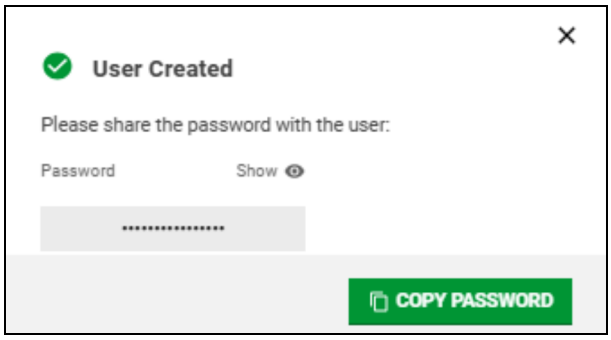


Admin – Can modify and view any settings on the Modbus IoT Gateway. They can also update firmware and obtain diagnostic information.

Operator – Can view all settings. Can view and modify field device data.

Viewer – Can only view settings / readings on the Modbus IoT Gateway.

3. Customize the user information, then click Save. When adding new users, a confirmation screen will appear stating that the user has been created.



8.5 Modbus IoT Gateway Configuration

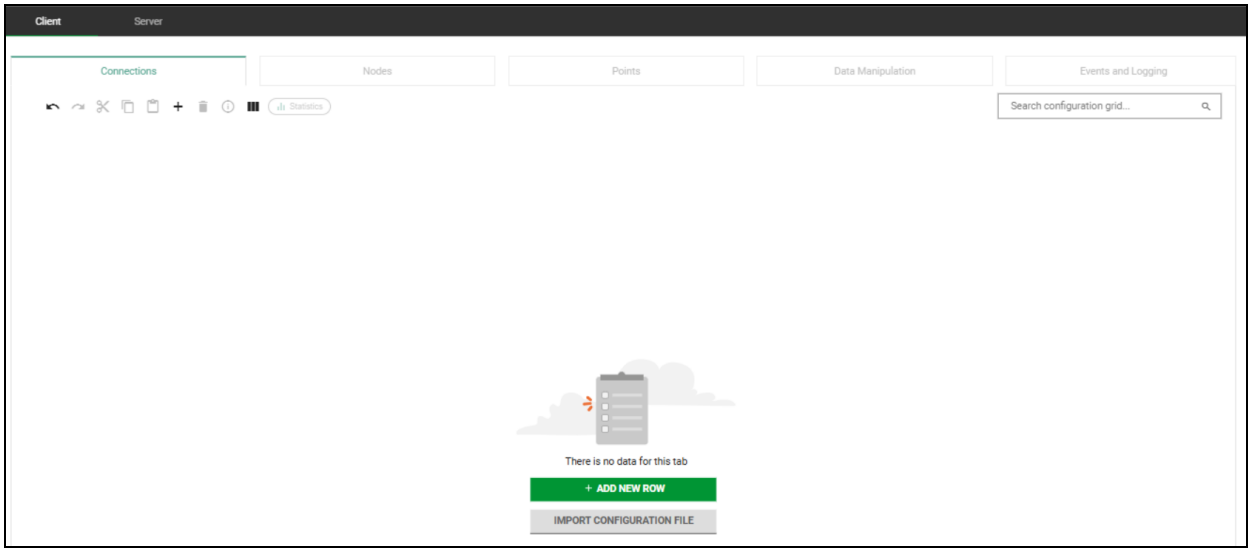
The Modbus IoT Gateway Configuration features a configuration journey where the user is guided through the process with only the required information.

Any changes are immediately saved to the FieldServer, and become active as soon as the save is complete. For larger configurations, saving the configuration can take up to a minute. After saving, the software provides immediate feedback as to whether any changes made were correct and are working as intended.

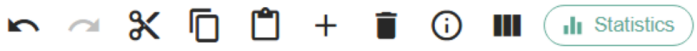
There are two approaches to configuration: free-form or profile-based configuration.

The free-form configuration (8.5.1 Free-form Configuration) is the most flexible approach to configuring the Modbus IoT Gateway, while profile-based configurations (8.5.2 Profile Editor and 8.5.3 Profile Instance Editor) are best suited for larger configurations where there are multiple repetitive sections with the same information.

Opening the Free-form Editor tab shows the following screen. A similar screen appears when clicking the Profile Editor's and Profile Instance Editor's Connections tab:



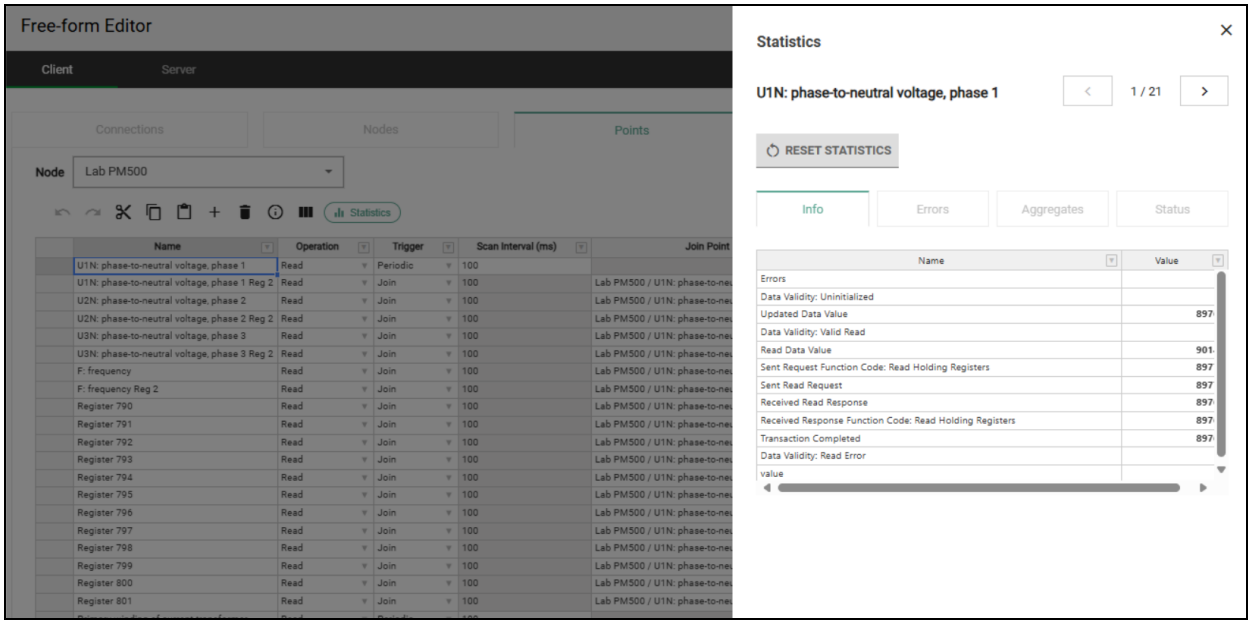
The top toolbar has the following features:



– Provides more information on the currently selected column.

– Hides / shows columns for easier viewing.

Statistics – Displays statistics, errors, and status of the selected row. An example screenshot of the statistics panel is shown below.



8.5.1 Free-form Configuration

The free-form configuration is used to completely set up a configuration from end-to-end. Free-form configuration includes editing the settings for every configurable item. This includes connections, nodes (devices), points, data manipulations, and all items that are required to read and server up data.

NOTE: The user must set up both the client and server for a complete translation in the following order:

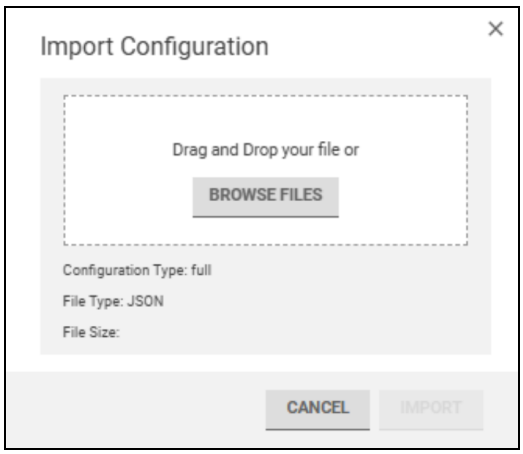
1. **Client** – The configuration that retrieves data by polling, subscribing to, or waiting for data from field devices. The user must also set up the connections, nodes, data points, and any data manipulation required to read data from the field devices. The following tabs are available for client protocols:
    a. **Connections** – Configure the physical connection parameters, which connector is used and settings like connection speed.
    b. **Nodes** – Configure the devices that the Modbus IoT Gateway is polling for data.
    c. **Points** – Set up the points that are to be read from the devices. This data is available from the manufacturer of the device that is being read.
    d. **Data Manipulation** – If required, set up any data changes that are required. This includes operations like add, combining 2 registers in a float etc. More information is available on the grid itself.
    e. **Events and Logging** – If required, set up event rules and logging rules for any points. Only logged points will be pushed to FieldServer Grid Manager. Events will be pushed to FieldServer Grid Manager and can be sent to the user as SMS's or emails.
2. **Server** – The configuration that provides data to systems like BMS, cloud providers, etc. The server listens for polls or publishes data. Data can be made available to other systems using one of the included protocols.
    a. **Connections** – Configure the physical connection parameters, which connector is used, and settings like connection speed.
    b. **Nodes** – Configure the logical devices that are available to other systems. For MQTT, nodes are used to configure the topics on which data is published.
    c. **Points** – Set up the points that are available to the 3rd party system.
    d. **Data Manipulation** – Set up any data changes that are required. This includes operations like add, combining 2 registers in a float etc. More information is available on the grid itself.

Adding a Configuration

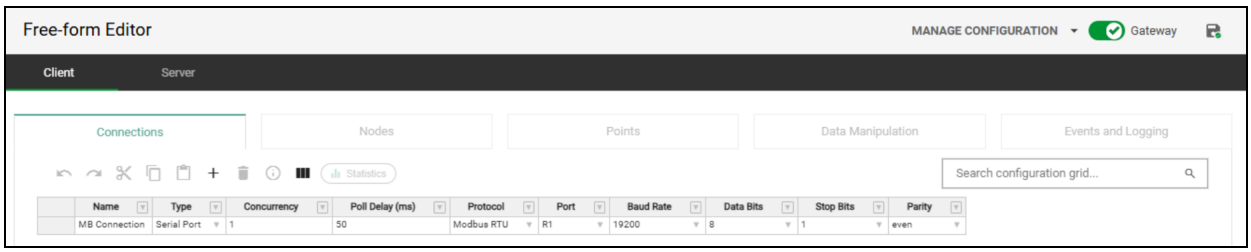
1. Click Free-form Editor in the navigation panel.
2. Click + ADD NEW ROW or IMPORT CONFIGURATION FILE.
    - For the + ADD NEW ROW option, fill in the columns.

	Name	Type	Concurrency	Poll Delay (ms)	Protocol	Port	Baud Rate	Data Bits	Stop Bits	Parity
	MB Connection	Serial Port	1	50	Modbus RTU	R1	19200	8	1	even

- For the Import from file option, click BROWSE FILES to select the appropriate JSON file, and click IMPORT.

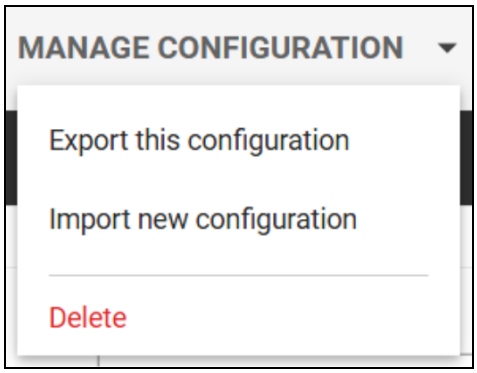


After adding a new row or importing a configuration, the configuration grid is displayed:



Managing a Configuration

1. Click MANAGE CONFIGURATIONS underneath the system status indicator.



2. Select from the following options:
   - **Export this configuration** – Saves a JSON file that contains the entire configuration of the Modbus IoT Gateway. This includes profiles, profile instances and all items configured under free-form.
   - **Import new configuration** – Imports a previously saved JSON file that replaces the entire configuration of the Modbus IoT Gateway.
   - **Delete** – Deletes the free-form configuration of the Modbus IoT Gateway and any configured profile instances.

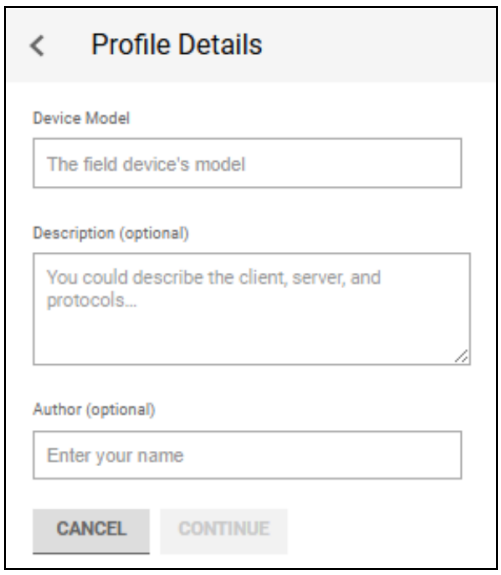
8.5.2 Profile Editor

The Profile Editor option is another way to configure the Modbus IoT Gateway. The Profile Editor includes:

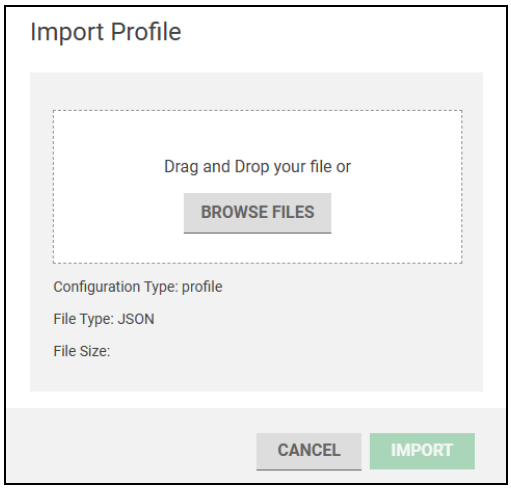
- Defining multiple templates with configured data and parametrized settings, known as profiles.
- Reusing profiles to build a larger configuration.
- Storing created profiles on the device in the Profile Library.

Adding Profiles

1. Click Profile Editor in the navigation panel.
2. Click Add Profile.
3. Select Create new or Import from file.
   - For the Create new option, fill in the respective fields and click CONTINUE.



   - For importing files, click BROWSE FILES to select the appropriate JSON file, and click IMPORT.



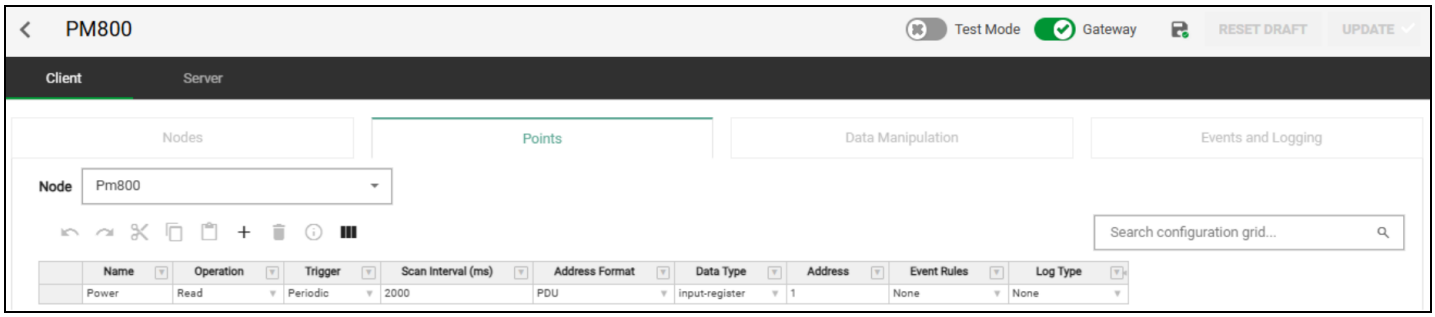
4. Click Add New Row or the + icon in the toolbar to add the new profile to the grid.

Adding Parameters

Parameters are used to make a profile instance unique when applying a profile. You must provide a value for each parameter to complete the Profile Instance.

To add or edit a parameter:

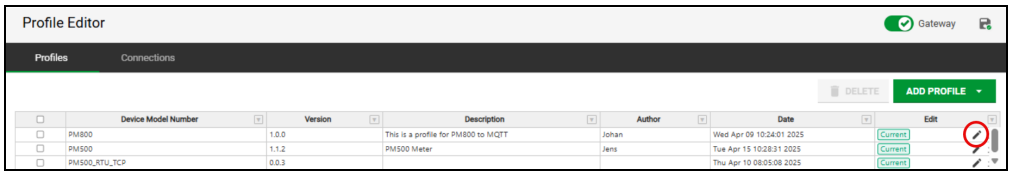
1. Right-click the field you want to designate as a parameter.
2. Select Profile Parameter from the context menu.
3. Enter a name for the parameter.
4. Save your changes.
5. Click on the Points Tab. Click on the + tab to add points and fill in respective fields
6. Click on the Data Manipulation tab and Events and logging if needed.
7. Click on the Server tab at the top and fill in the fields as needed for Nodes, Points, and Data manipulation.
8. Click Update in the top bar.



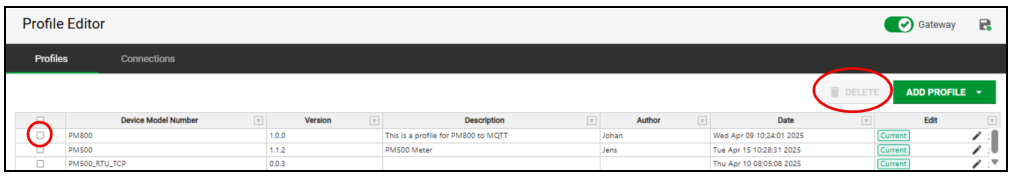
Editing and Deleting Profiles

Be aware of the green Current tag when editing or deleting a profile. If the profile is marked with a green Current tag, it means that the profile is currently deployed in a profile instance and used in a connection.

1. Find the row with the profile you want to edit or delete in the grid.
   - To edit a profile, click the pencil icon.



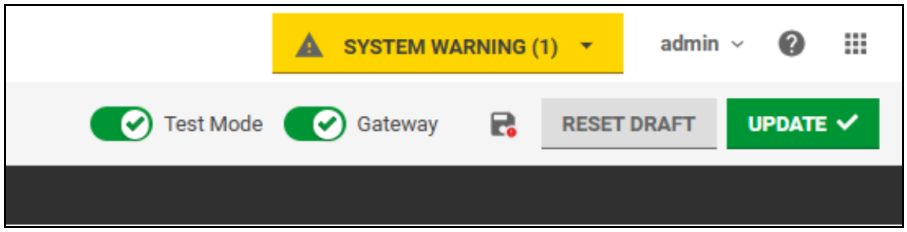
   - To delete a profile, check the box then click the Delete button.



Drafting a Profile in Test Mode

Testing a profile allows you to create a profile without deploying it to the live system. Follow the steps below to test a profile:

1. Toggle Test Mode in the upper right corner. This causes the system indicator to turn yellow and disables the rest of the system. However, real-time data will continue to display in the Values tab.



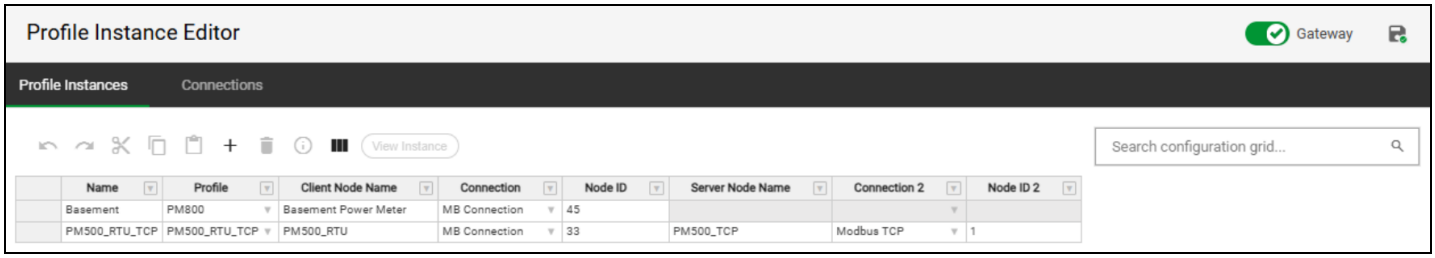
2. Create a profile. See the section Adding Profiles for more details.
3. Save the profile if desired.
   i. Click on the UPDATE button.
   ii. Edit the last two numbers of the profile version to ensure compatibility with other systems.
   iii. Edit the remaining fields as needed.
   iv. Click CONFIRM to save the changes.
4. Export the profile if desired by clicking the download icon . The JSON file will be downloaded to your local PC. Email this file to technical support to deploy the configuration to your units in production.

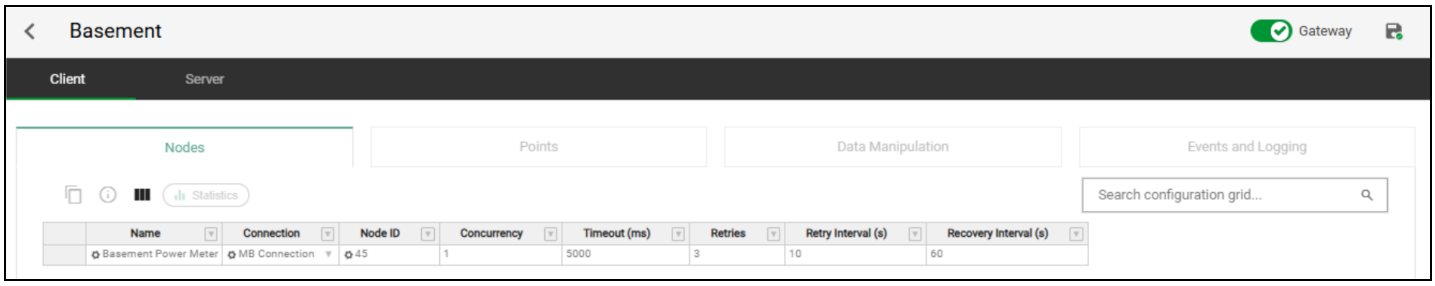
8.5.3 Profile Instance Editor

You can choose profiles from the profile library are used to create profile instances that contain all the settings defined by the selected profile. In addition, every Profile Instance will contain unique parameter values (e.g., device names or addresses). The profile instance uses a profile to establish a connection to the device.

Viewing Instances

1. Click Profile Instance Editor in the navigation panel. The editor opens to the Profile Instances section by default.
2. Click the desired instance.
3. Click the View Instance button in the toolbar to the nodes, points, data manipulation settings, events, and logging.





Reading Real-Time Values

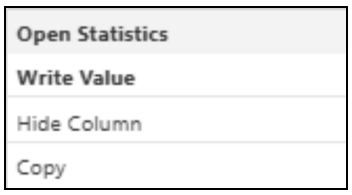
1. Click Profile Instance Editor in the navigation panel and click the desired instance.
2. Click the View Instance button in the toolbar.
3. Go to the Points tab or the Data Manipulation tab.
4. For the Points tab, scroll to the right to see real-time values in the Values column.

Checking if Data is Being Pushed to the Server

1. Click the Server section.
2. Click the Points tab and scroll to the right to the Values column.
3. Click the desired point and select the Statistics button in the toolbar.

Writing Values

1. Right click the text box that you want to edit, then click Write Value.



2. Enter the new value in the text field.

3. Click WRITE to save the new value. You can view the new value in real time in the Values column.

9 Modbus Configuration

The Modbus driver on the Modbus IoT Gateway allows for setup as a client or a server. A client will poll devices on the bus/network. A server waits for a poll from a client device and responds with the data requested. There can be multiple server devices on a RS-485 bus, but only one client device.

9.1 Modbus Client Configuration

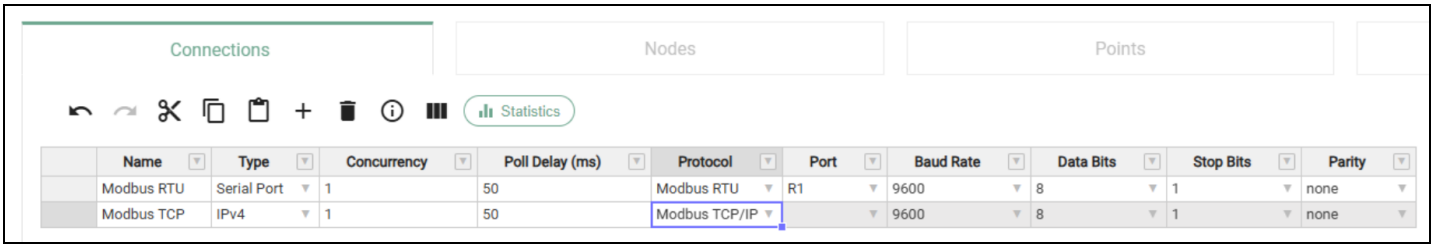
At each step, the difference between Modbus TCP / IP and Modbus RTU will be highlighted.

To configure the Modbus IoT Gateway as a client, you must set up all of the following:

- The connection
- The nodes that they want to poll
- The points on each node

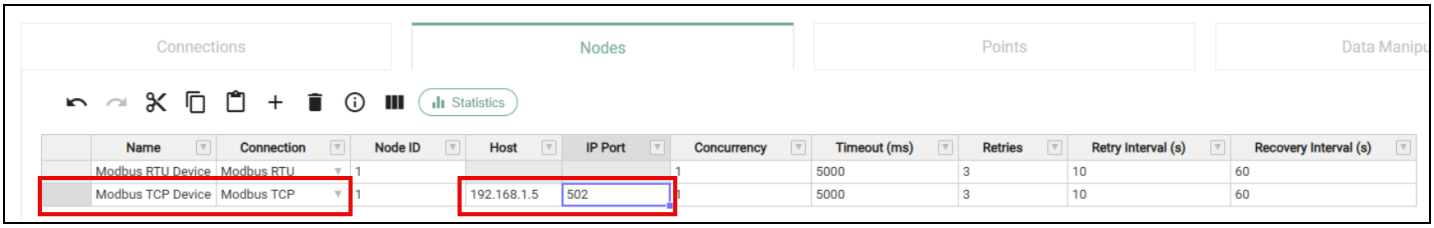
9.1.1 Connection Setup

For Modbus RTU, the user needs to specify the bus's physical settings. Grayed-out fields are ignored.



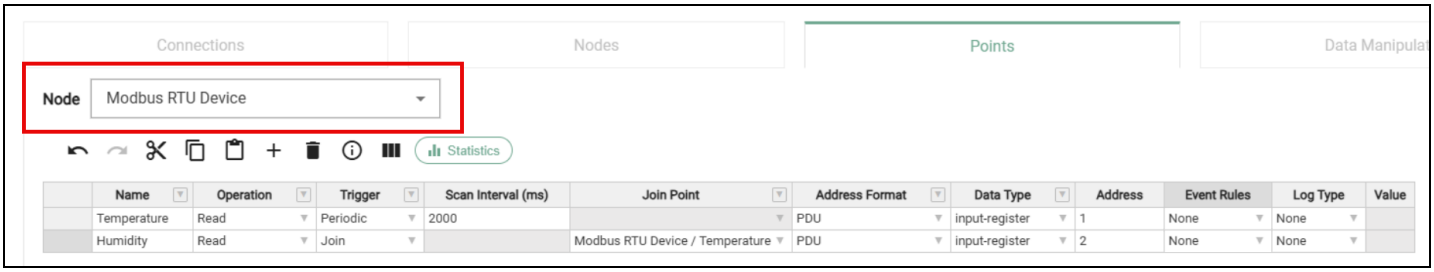
9.1.2 Node Setup

For the Modbus TCP / IP node, the host and IP port needs to be specified.



9.1.3 Point Setup

Before setting up points, select the correct node from the drop-down menu above the toolbar.



Only the points for the selected node will be shown.

9.1.4 Configuring Multiple-Point Modbus Transactions

The Points Grid lists individual data items. You are required to define each data item's name and other settings. This is useful when referring to the data items again in other places in the system, such as configuring a server interface or data

manipulation operations. The points definition also tells the Modbus IoT Gateway what to do with that point, e.g. to read or write. The Modbus is also able to transfer multiple items in a single transaction, which is generally more efficient.

To define a multiple-item transaction, follow the steps below:

1. Configure the first point in the transaction normally, using the operation and trigger options provided.
2. Add further points to this transaction by configuring them with the same operation.
3. Select the Join option as the trigger. A new prompt will appear.
4. Select where you want the current point to be included from previously configured points and operations. If your selection is not possible (for example, if a Modbus frame cannot accommodate all the specified addresses), then a feedback notification will appear.

To push data to the MSA Grid – FieldServer Manager, a Log Type must be configured. This can either be COV-based or log periodically.

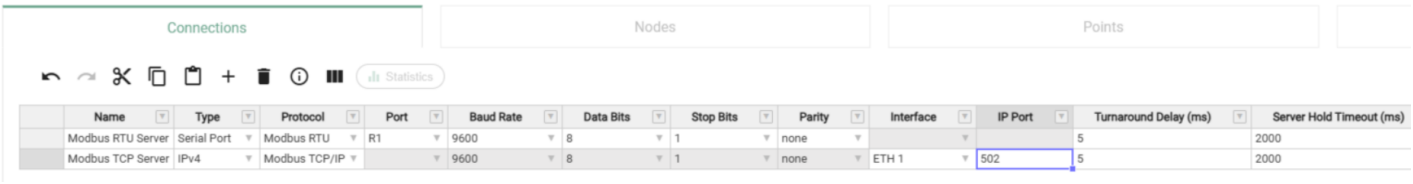
To set up notifications in FieldServer Manager, Event Rules must be configured.

9.2 Modbus Server Configuration

To configure the Modbus IoT Gateway as a server, you must set up the following:

- The connection
- The nodes that will be available to other devices
- The points that are available on each node

9.2.1 Connection Setup

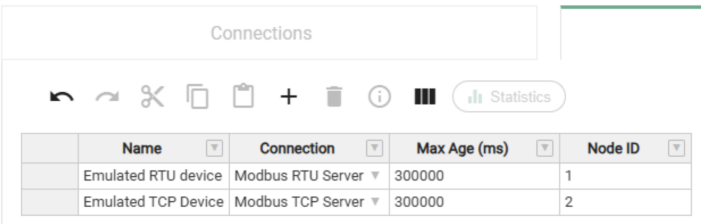


Name	Type	Protocol	Port	Baud Rate	Data Bits	Stop Bits	Parity	Interface	IP Port	Turnaround Delay (ms)	Server Hold Timeout (ms)
Modbus RTU Server	Serial Port	Modbus RTU	R1	9600	8	1	none			5	2000
Modbus TCP Server	IPv4	Modbus TCP/IP		9600	8	1	none	ETH 1	502	5	2000

For Modbus RTU the user needs to specify the physical settings of the bus. Grayed out fields are ignored. For the Modbus TCP/IP node, the IP Port that will be opened needs to be specified.

9.2.2 Node Setup

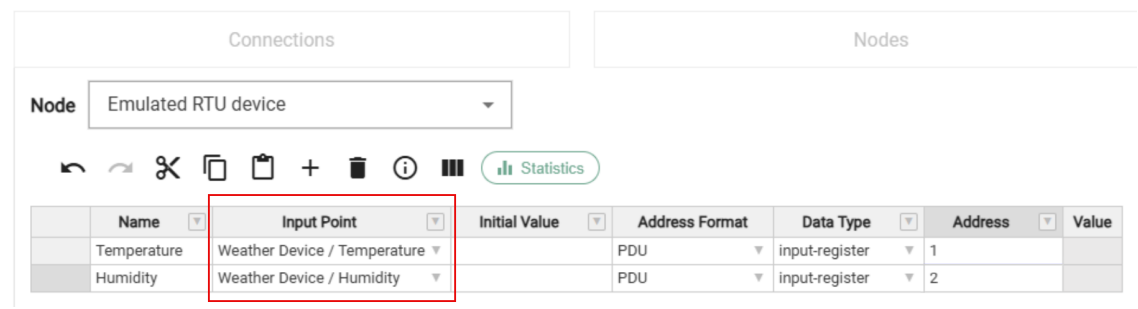
Before setting up points, select the correct node from the drop-down above the configuration grid. Only the points for the node selected will be shown.



Name	Connection	Max Age (ms)	Node ID
Emulated RTU device	Modbus RTU Server	300000	1
Emulated TCP Device	Modbus TCP Server	300000	2

9.2.3 Point Setup

The value for a server point needs to reference a client point. This is specified in the Input Point field and uses the format "Node Name / Point Name". In the Input Point cells, the user can type to filter the points or use the drop-down to select one of all available client points.



10 OPC UA Configuration

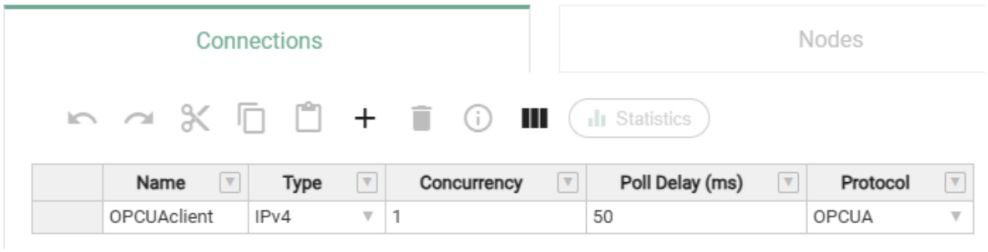
The OPC UA driver on the Modbus IoT Gateway allows for setup as a client or server.

10.1 OPC UA Client Configuration

To configure the Modbus IoT Gateway as a client, you must set up all of the following:

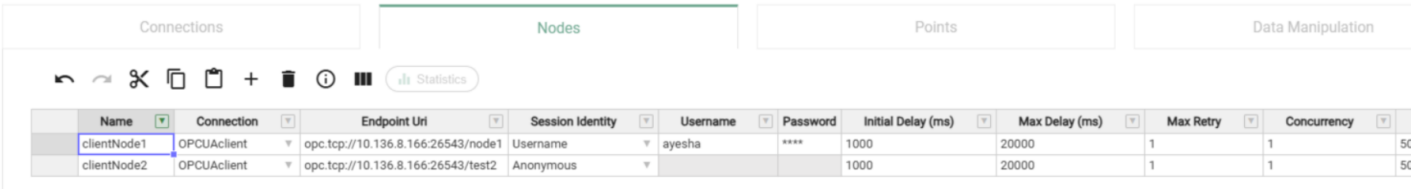
- The connection
- The nodes that they want to poll
- The points on each node

10.1.1 Connection Setup



10.1.2 Node Setup

The OPC UA driver supports authentication via username and password or an anonymous authentication.

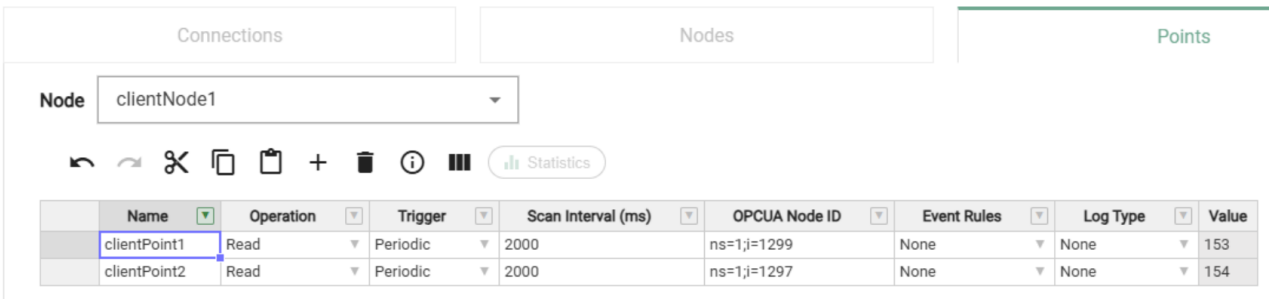


10.1.3 Point Setup

Before setting up points, select the correct node from the drop-down menu above the configuration grid. Only the points for the node selected will be shown.

To push data to MSA Grid – FieldServer Manager a Log Type must be configured. This can either be COV-based, or log periodically.

To set up notifications in FieldServer Manager, Event Rules must be configured.

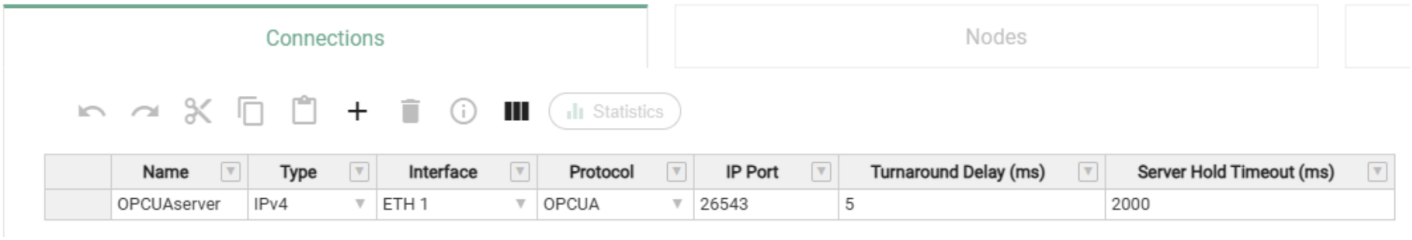


10.2 OPC UA Server Configuration

To configure the Modbus IoT Gateway as a server, the user needs to set up the connection, the nodes that will be available to other devices, and the points that are available on each node.

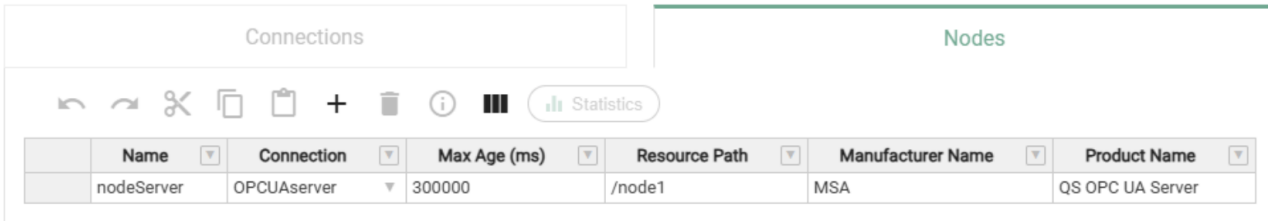
10.2.1 Connection Setup

The Modbus IoT Gateway only supports 1 OPC UA server connection.



10.2.2 Node Setup

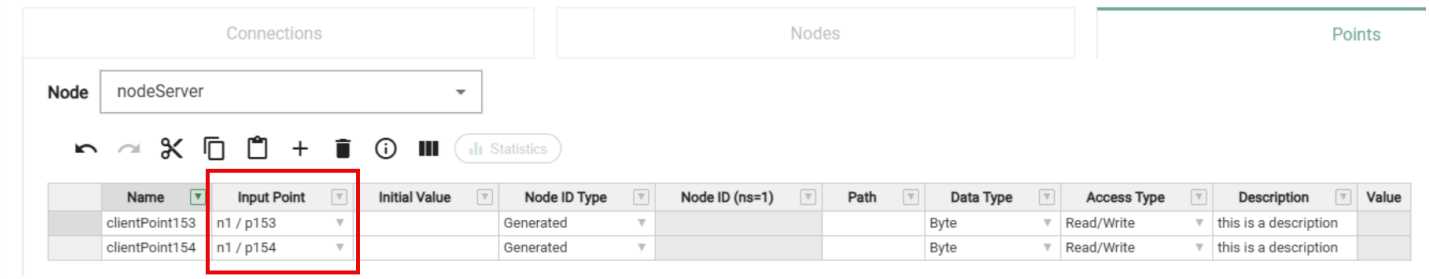
The Modbus IoT Gateway only supports 1 server node.



10.2.3 Point Setup

Before setting up points, select the correct node from the drop-down above the configuration grid. Only the points for the node selected will be shown.

The value for a server point needs to reference a client point. This is specified in the Input Point field and is in the format "Node Name / Point Name". In the Input Point cells, the user can type to filter the points or select from the drop-down of all available client points.



11 MQTT Integration

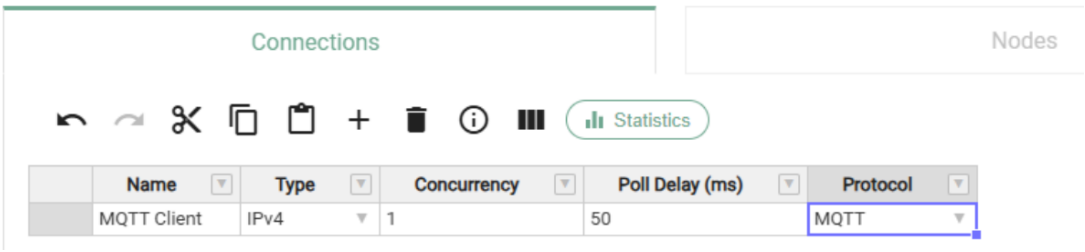
11.1 MQTT Published Messages

The MQTT driver on the Modbus IoT Gateway can connect to multiple brokers either as a client (subscriber) or a server (publisher) .

- As a client, it can subscribe to single topics and supports JSON paths, XML paths, or raw values. Those values can then be made available on a server driver or pushed to FieldServer Grid.
- As a server, it supports publishing multiple points in a single payload to a topic. It can also subscribe to single topics to support writing changes to a topic to a field device downstream.

11.2 MQTT Client Configuration

11.2.1 Connection Setup



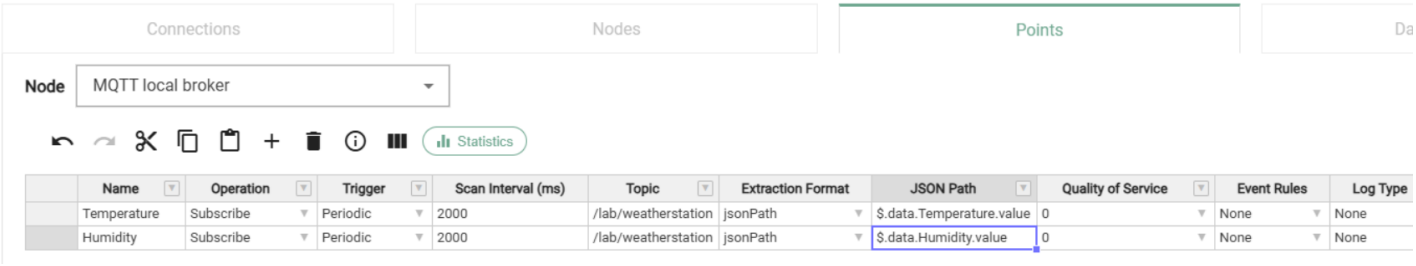
The client connection only needs to be configured as an MQTT connection.

11.2.2 Node Setup

The node needs to be set up with the broker URL, including the MQTT protocol and the port.

11.2.3 Point Setup

Specify the JSON path by starting with a $, followed by the rest of the path. The point will wait for the other device to publish, and can't actively read the point values as it waits.

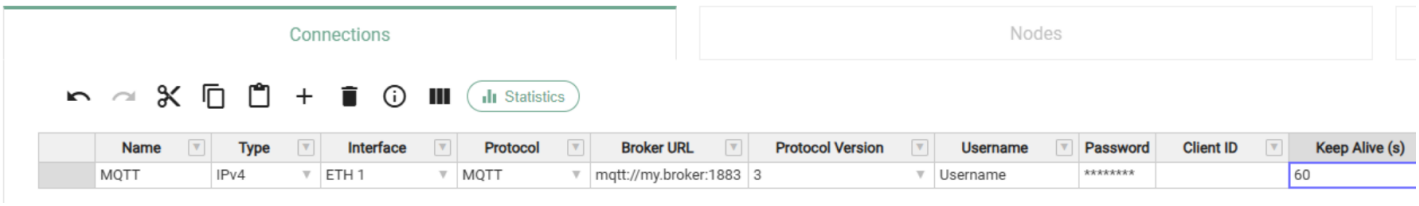


11.3 MQTT Server Configuration

This section requires a Modbus client to have been configured.

11.3.1 Connection Setup

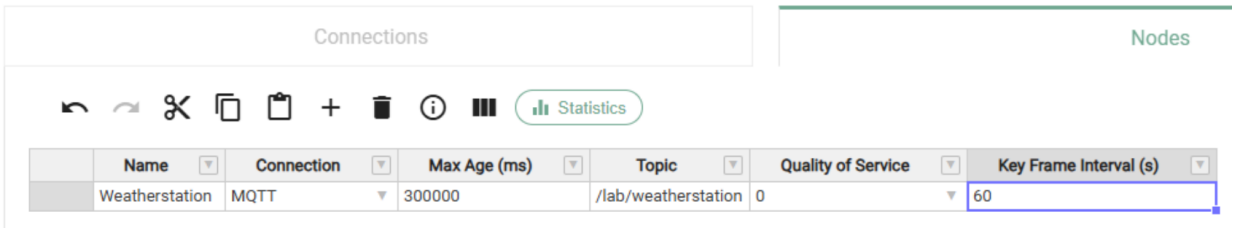
1. Add a new row to create a new connection.



2. Choose a name for the connection.
3. Complete all the fields per the heading requirement.

11.3.2 Node Setup

An MQTT server node represents the points that will be published as a single payload to the broker.



In this example, all points configured under the node will be published on the topic “/lab/weatherstation”. The format of the payload will be:

```
{
"timestamp": "2025-06-19T13:42:50.957Z",
"data": {
"Humidity": {
"value": 85,
"validity": "Initialized",
"timestamp": "2025-06-19T13:37:20.180Z"
},
"Temperature": {
"value": 76.5,
"validity": "Initialized",
"timestamp": "2025-06-19T13:37:20.180Z"
}
}
}
```

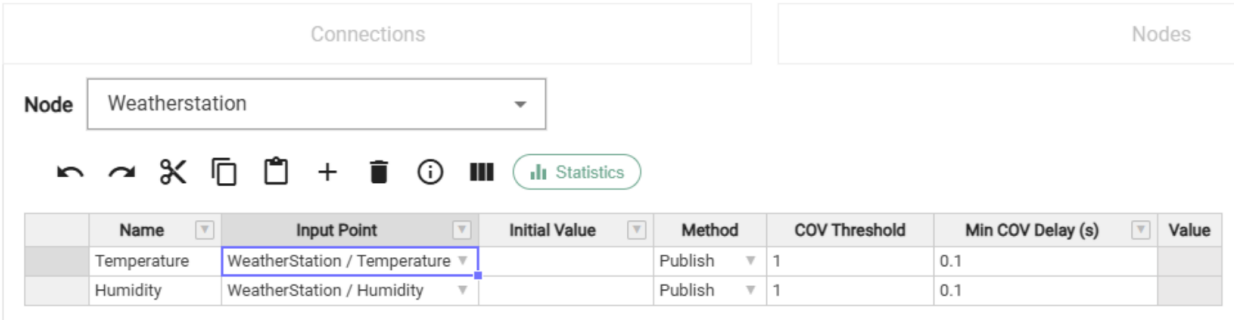
Each point will be represented by an entry in the data field. The point name will be the key in the object, and the data will be the value of that key. Each data point will send its value, validity, and the time stamp of when it was last updated.

The validity can have one of the following statuses:

- Initialized
- Valid
- Valid Read
- Valid Write
- Write Pending
- Uninitialized
- Expired
- Read Error
- Offline
- Write Error

11.3.3 Point Setup

Each point needs to be configured with a name and the source of the data from the Modbus client. The input point will be in the format of “Node Name / Point Name” from the client.



12 Integrating Azure IoT Hub with the MQTT Driver

12.1 Overview

This section describes how to configure the Modbus IoT Gateway to communicate with Azure IoT Hub using the MQTT protocol with X.509 certificate authentication. To do so, you must have an Azure subscription with access to create / manage IoT hubs and access to a Certificate Authority (CA) to sign certificate requests. It is also recommended that you have a basic understanding of X.509 certificates and MQTT protocols before continuing.

To set up communication with Azure IoT Hub, you must:

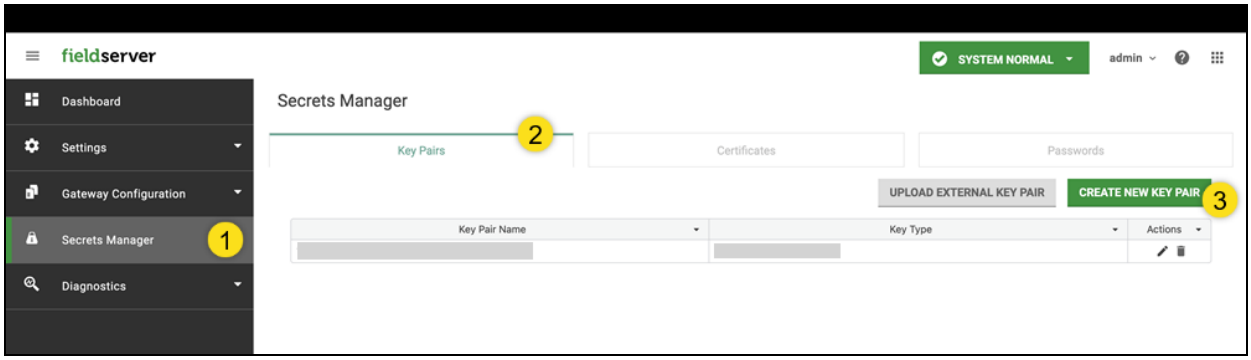
1. Generate cryptographic key pairs and certificate signing requests on the Modbus IoT Gateway.
2. Obtain a CA-signed certificate
3. Upload the CA-signed certificate to Modbus IoT Gateway.
4. Upload the CA certificate to the Azure IoT Hub.
5. Register the device in Azure IoT Hub.
6. Configure the MQTT driver with the appropriate connection settings.
7. Verify and test the connection.

The subsections in this chapter detail the steps listed above.

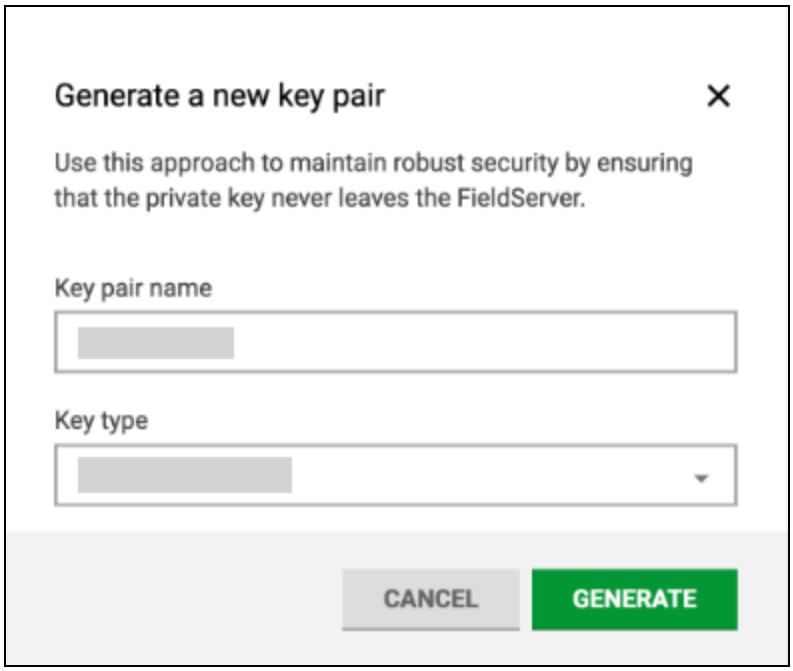
NOTE: The common name (CN) of the device certificate must match the device ID created in Azure IoT Hub. The CN must not contain spaces or unsupported characters.

12.2 Generating Cryptographic Key Pairs and Certificate Signing Requests

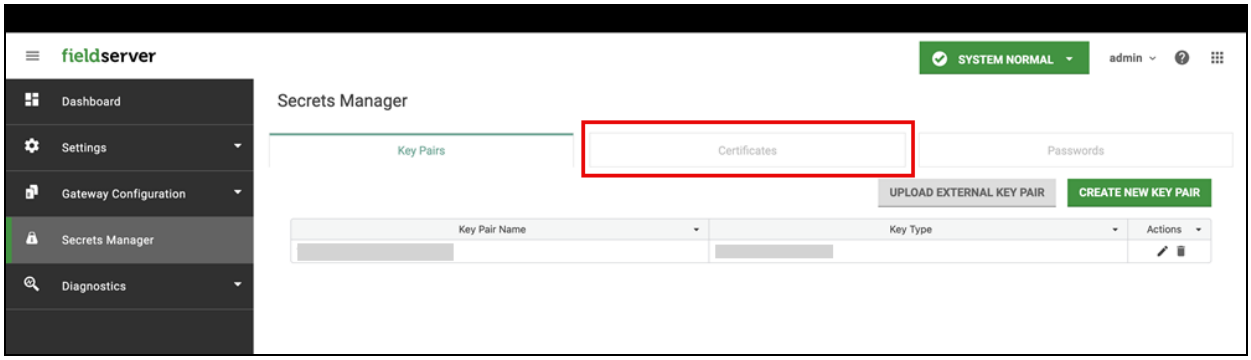
1. Log in to Modbus IoT Gateway, and go to Secrets Manager.
2. Go to the Key Pairs section.
3. Click CREATE NEW KEY PAIR. Key pairs are securely stored in Secrets Manager and never exposed in plain text.



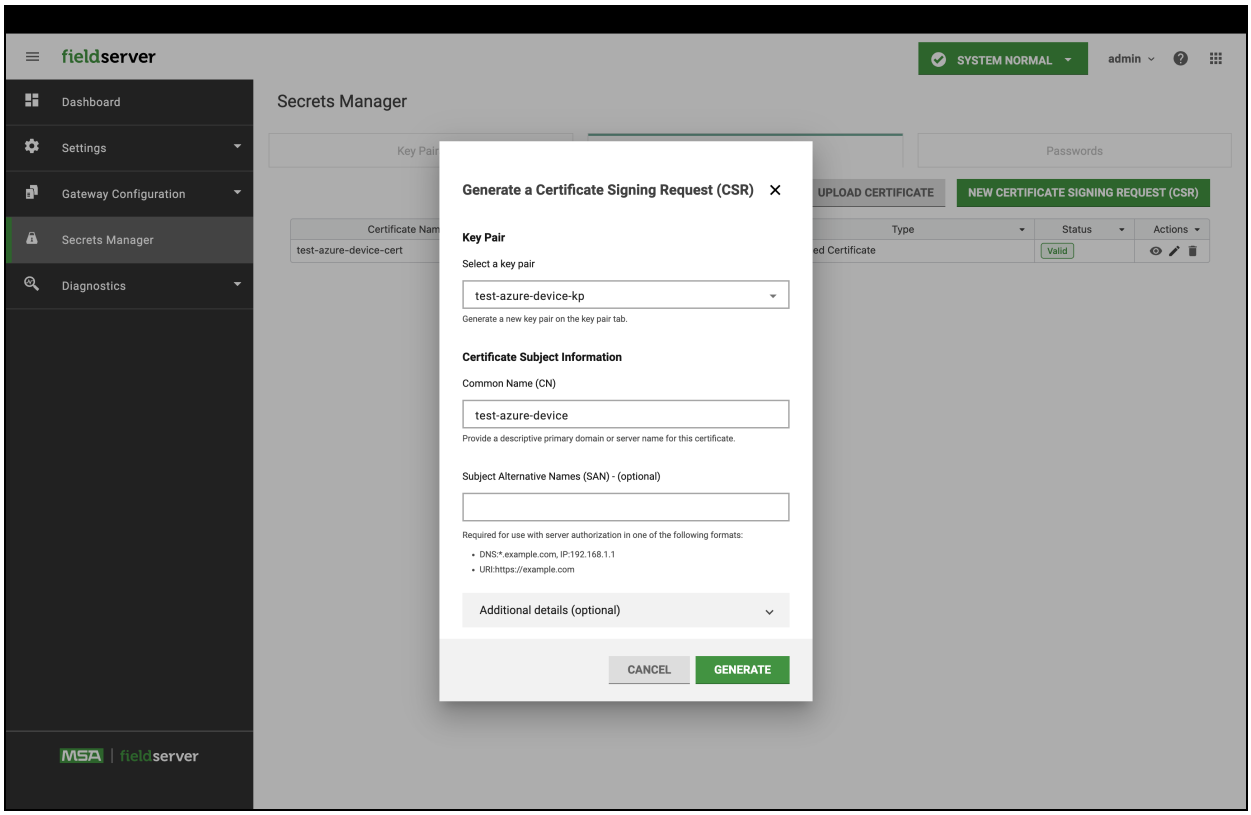
4. Complete the form. It is recommended to name the key pair with a descriptive name (e.g., "azure-device-keypair").



5. Click Generate for Modbus IoT Gateway to generate the key pair. This key pair is then used to generate a certificate signing request (CSR).
6. Next, generate a CSR by going to the Certificates tab.



7. Click the NEW CERTIFICATE SIGNING REQUEST (CSR) button.
8. Complete the form that appears.
   - For Key pair, select the key pair that you created in previous steps.
   - For Common Name (CN), enter the Device ID that will be used in Azure IoT Hub. **The device ID must be an exact match to the one you will use in Azure. The ID must use only alphanumeric characters and hyphens. Do not use spaces or other characters.**



9. Click GENERATE to generate the CSR.
10. Download the CSR file to your local PC, and proceed to sign the CSR. See 12.3 Obtaining a CA-signed Certificate for more info.

12.3 Obtaining a CA-signed Certificate

Generate a signed CSR using one of the three authentication methods in this section.

The methods include two options for X.509 CA signing. The X.509 CA signing methods are recommended for production. The other authentication method is for self-signing, has a simpler setup, and is recommended for testing / development.

The CA certificate used for signing must be available in .pem or .cer format.

12.3.1 X.509 CA Signing while Using an Internal / Self-Managed CA

1. Provide the CSR file to your certificate authority.
2. Request a signed certificate valid for device authentication.
3. Ensure that you receive both the signed device certificate (.pem or .cer format) and the CA certificate (.pem or .cer format) that signed it.

12.3.2 X.509 CA Signing while Using OpenSSL to Create a CA

```
# Generate CA private key
openssl genrsa -out azure-ca.key.pem 2048

# Generate CA certificate
openssl req -x509 -new -nodes -sha256 -days 3650 \
  -key azure-ca.key.pem \
  -subj "/CN=Azure Test CA/O=YourOrg/C=US" \
  -out azure-ca.cert.pem

# Sign the device CSR
openssl x509 -req -in device.csr \
  -CA azure-ca.cert.pem \
  -CAkey azure-ca.key.pem \
  -CAcreateserial \
  -days 825 -sha256 \
  -out device-signed.cert.pem
```

12.3.3 X.509 Self-signing a Certificate

For generating a self-signed certificate, you are not required to upload a CA to Azure.

However, you need the certificate thumbprint in order to register the device in Azure IoT hub. This is because the certificate is validated by thumbprint matching, not CA chain verification.

If you want to use X.509 Self-Signed authentication in Azure, you can create a self-signed certificate directly without a separate CA.

NOTE: Self-signed certificates are suitable for testing only. For production use, employ a trusted CA with X.509 CA Signed authentication.

```
# Generate a self-signed certificate directly from the CSR
# Note: You'll need the private key that was used to generate the CSR
openssl x509 -req -in device.csr \
  -signkey device.key.pem \
  -days 825 -sha256 \
```

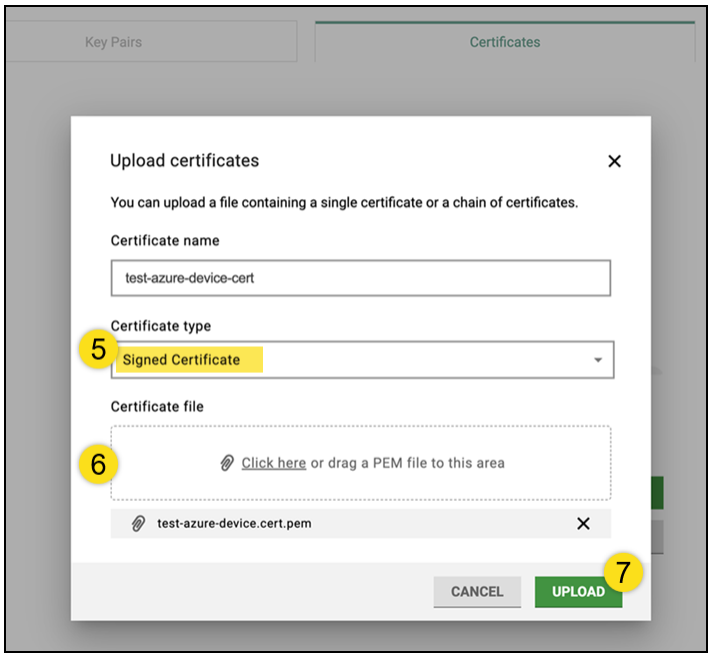
```
  -out device-self-signed.cert.pem


# Get the thumbprint for Azure IoT Hub registration (remove colons)

openssl x509 -in device-self-signed.cert.pem -noout -fingerprint -sha1 | sed 's/://g' | cut
-d'=' -f2
```

12.4 Uploading the Signed Certificate to Modbus IoT Gateway

1. Return to the Certificates section in Secrets Manager.
2. Find the certificate entry created in 12.2 Generating Cryptographic Key Pairs and Certificate Signing Requests.
3. Click Upload Certificate.
4. Provide a descriptive name.
5. Select Signed Certificate as the certificate type.
6. Upload the signed .pem or .cer certificate file.
7. Click the UPLOAD button. Uploading the file sends both the created private key and signed certificate to the FieldServer.

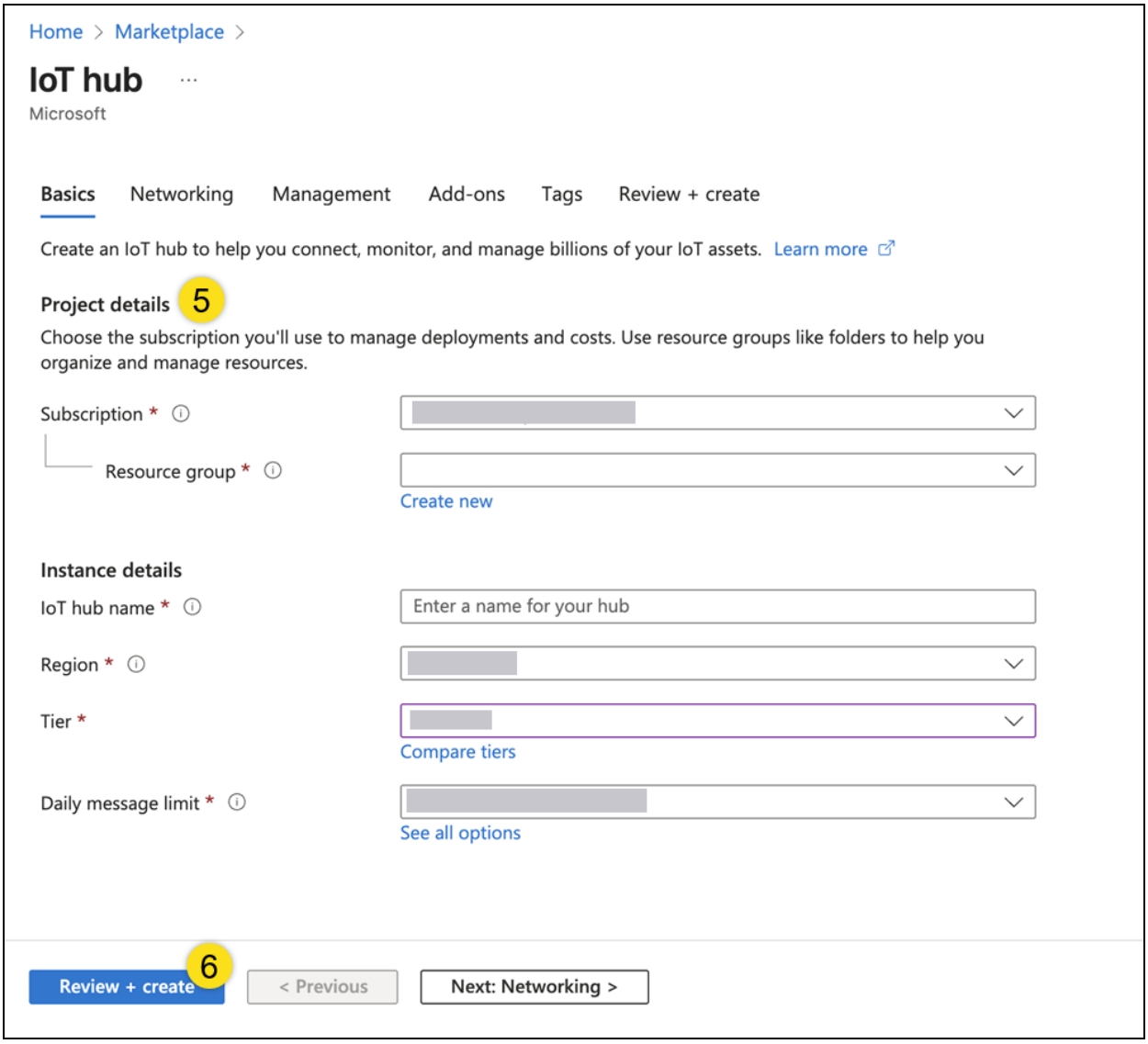


12.5 Uploading the CA Certificate to Azure IoT Hub (Only required for X.509 CA Signed Authentification)

This section is only required for X.509 CA signed authentication. If you are using X.509 Self-Signed authentication, go to 12.6 Registering the Device in Azure IoT Hub.

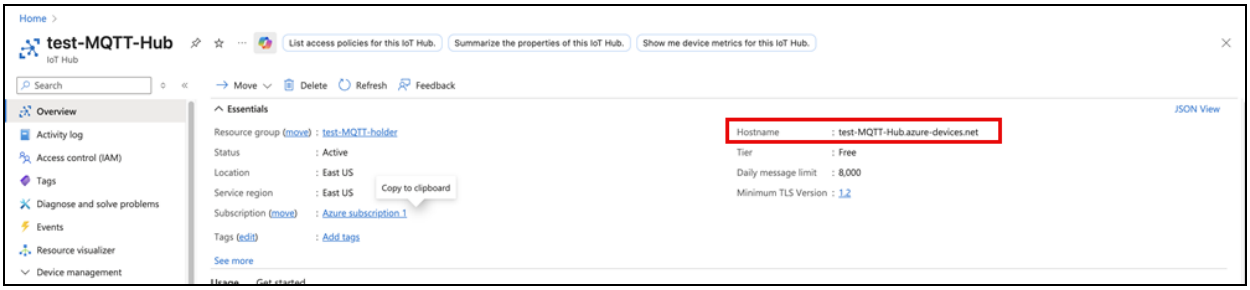
1. Create or select an Azure IoT hub.
   - If creating a new IoT hub:
     1. Sign in to the Azure Portal.
     2. Click Create a resource.
     3. Search for IoT hub, then select it.
     4. Click Create.

5. Configure the IoT hub according to your preferences for the subscription, resource group, IoT hub name, region, tier, and daily message limit.
6. Click Review + Create.



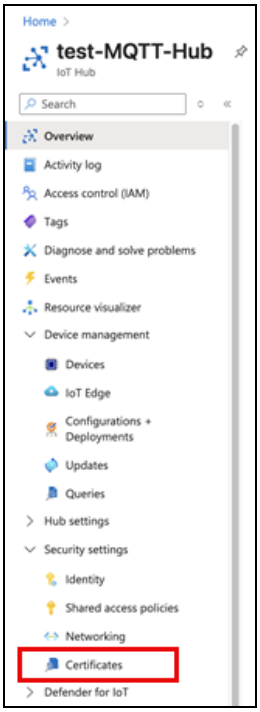
7. Click Create. After clicking, the newly created IoT hub will take time to deploy.

- If using an existing IoT Hub:
  1. Navigate to your existing IoT Hub in the Azure Portal.
  2. Take note of the IoT Hub hostname (e.g., "your-hub.azure-devices.net").



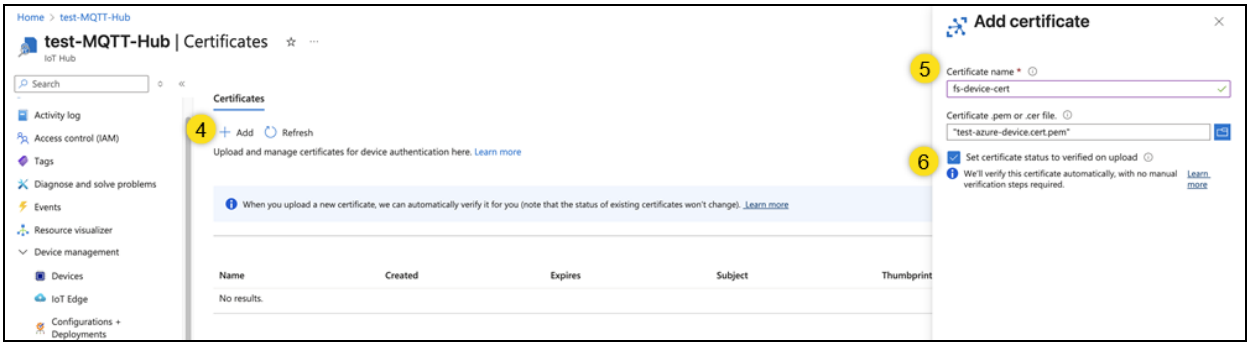
2. In the Azure Portal, navigate to your IoT Hub.

3. In the left panel, under Security Settings, click Certificates.



4. Click + Add to add a new certificate.
5. Name the certificate and upload the file.
6. **If using a publicly trusted CA**, set the certificate status to verified on upload.

   If using a self-managed CA, leave unchecked for self-managed CAs. Leaving it unchecked also means you must verify proof of possession by following steps 9 through 13 in this section.



7. Click Save.
8. Skip steps 9 through 13 if the certificate status is set to verified on upload, and follow if using a self-managed CA.

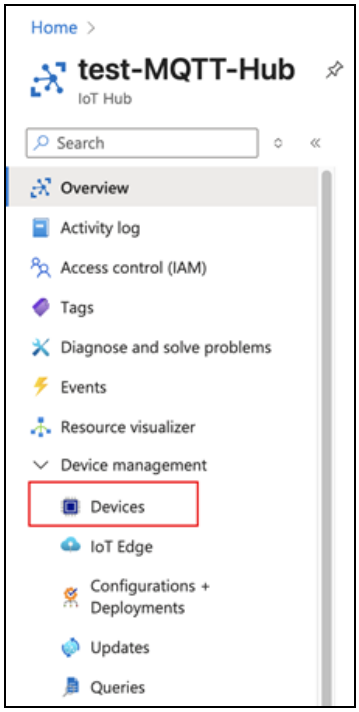
Proof of Possession

9. After uploading, click on the certificate name.
10. Click Generate Verification Code for Azure to display a verification code.
11. Create a new certificate with the verification code as the Common Name (CN).
12. Sign this certificate with your CA.
13. Upload the verification certificate. Azure will then verify that you possess the CA's private key. This ensures you control the CA's private key and can sign certificates.

12.6 Registering the Device in Azure IoT Hub

1. In the Azure Portal, navigate to your IoT Hub.

2. Go to Device management, and click Devices.



3. Click + Add Device.
4. Configure the device. For the Device ID, you must enter the exact common name from the device certificate. If using X.509 CA Signed, this device ID
5. Select the authentication type that you used, either X.509 CA Signed or X.509 Self-Signed.
   - For X.509 Self-Signed, you must provide the thumbprint to authenticate the certificate:
     1. Run the following command on your signed certificate to get the thumbprint:

```
# Get SHA-1 thumbprint of the certificate (remove colons for Azure)
        openssl x509 -in device-signed.cert.pem -noout -fingerprint -sha1 |
sed 's/://g' | cut -d'=' -f2
```

     2. Enter the thumbprint (40 hexadecimal characters, no colons) in the Primary Thumbprint field.
   - For X.509 CA Signed, device authentication uses any certificate signed by your uploaded CA that has the device ID from step 4 as its Common Name.
6. Click Save.

12.7 Configuring the MQTT FieldServer for Azure IoT Hub Integration

This section focuses on MQTT Server configuration for publishing / subscribing to Azure IoT Hub. Note that the location of broker, authentication, and topic settings differs between the MQTT Client and MQTT Server.

MQTT Client

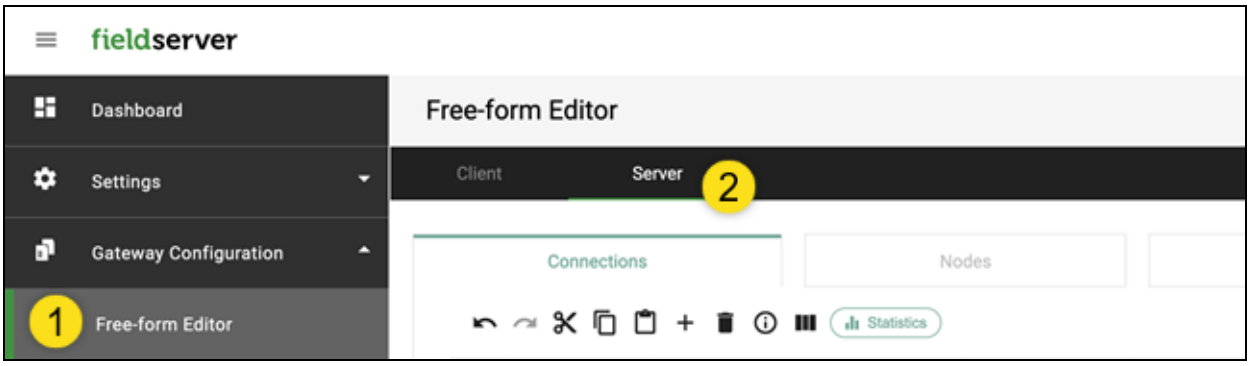
- Broker settings and authentication are configured on the Node.
- Topics are configured on the Point.

MQTT Server

- Topics are configured on the Point.
- Topics are configured on the Node.

To connect and configure the MQTT Server:

1. Go to Free-form Editor in Modbus IoT Gateway.
2. Click the Server section, then select the Connections tab.

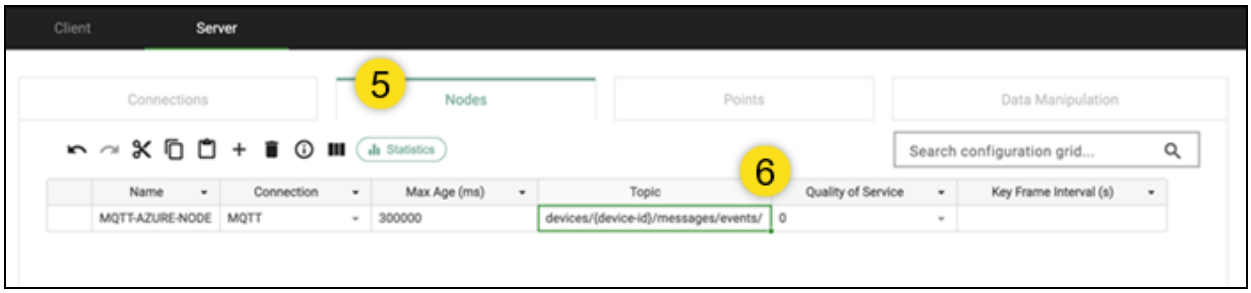


3. Create a new MQTT Server Connection or edit an existing one.
4. Configure the settings for the MQTT server row according to the following table:

Field	Value	Notes
Broker URL	mqtts://<your-hub>.azure-devices.net:8883	Replace <your-hub> with your IoT Hub name. Azure requires TLS (mqtts://) on port 8883.
Protocol Version	v3.1.1 or v5.0	Both are supported by Azure IoT Hub.
CA Certificate	Download and upload Azure root certificates	Use DigiCert Global Root G2 or Microsoft RSA Root CA 2017.
Client ID	Same as Device ID	This must match the Device ID in Azure.
Keep Alive	60 seconds	Default is acceptable.
Clean	true	Recommended for most use cases.
Authentication Method	Certificates	Select Certificates from drop-down.
Key Pair	Select your created key pair.	From Secrets Manager.
Signed Certificate	Select your created signed certificate.	From Secrets Manager.
Username	<iot-hub-name>.azure-devices.net/<device-id>/?api-version=2021-04-12	This is required for Azure even with certificates. Replace <iot-hub> and <device-id> with your values. Example: If your IoT Hub hostname is *fieldserver-hub.azure-devices.net* and Device ID is *device-001*, then your username would look like *fieldserver-hub.azure-devices.net/device-001/?api-version=2021-04-12*.
Password	Leave empty.	Not required for X.509 authentication.

The screenshot below was edited to display all the fields within the server row that you must configure. To see these fields, scroll right.

5. Configure your MQTT server node by creating a new MQTT server node or edit an existing one.
6. Configure the following node topic settings as needed:

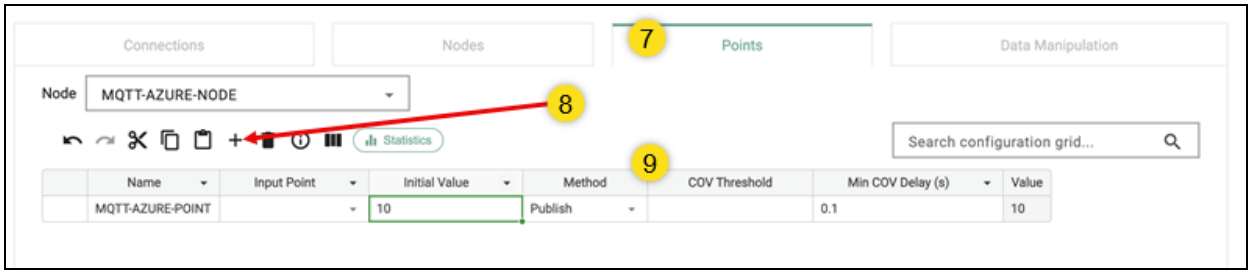


Field	Value	Notes
Topic	devices/<device-id>/messages/events/	For publishing: Replace <device-id> with your Device ID. This is the standard Azure IoT Hub telemetry topic.
Topic	devices/<device-id>/messages/devicebound/#	For subscribing: Replace <device-id> with your Device ID. Use # wildcard to receive all cloud-to-device messages.
Quality of Service (QoS)	0, 1	1 is recommended for reliable delivery - Azure does not support QoS 2.

Other common Azure IoT Hub MQTT Topics include:

- Telemetry (device-to-cloud): devices/{device-id}/messages/events/
- Cloud-to-device messages: devices/{device-id}/messages/devicebound/#
- Direct method requests: $iothub/methods/POST/#
- Device twin updates: $iothub/twin/PATCH/properties/desired/#

7. Go to the Points section to configure your data points under your MQTT server node.
8. Create the data points.
9. Configure the following fields based on your data requirements: Method, COV Threshold, and Min COV Delay (s).



The MQTT server connection, server node, and node data points are now configured.

12.8 Verifying and Testing Integration

After completing the previous sections, check the broker statistics and Azure to verify successful integration.

1. Select the MQTT server node, then click the Statistics icon.
2. Check for the following:
   - Connection status: Shows a message indicating it successfully "Connected" to the MQTT broker with the correct Azure IoT Hub URL.
   - Publish / Subscribe: Shows data for successful publish / subscribe operations with the MQTT broker.
   - Errors: 0 or empty
3. Go to Azure Portal and navigate to your IoT Hub.
4. Under Monitoring, click Metrics.
5. View the telemetry metrics:
   - Device-to-cloud messages
   - Cloud-to-device messages
   - Connection events
6. Check for successful message delivery and device connectivity.
7. Optional. For advanced monitoring, use Azure IoT Explorer.
   1. Download and install Azure IoT Explorer.
   2. Connect to your IoT Hub using the connection string.
   3. Select your device.
   4. Monitor telemetry in real-time.
   5. Send cloud-to-device messages to test subscriptions.

12.9 Troubleshooting Connection and Certificate Issues

12.9.1 Connection Issues

Error	Cause	Solution
"unable to get local issuer certificate"	The CA certificate for Azure IoT Hub's TLS certificate is not trusted.	1. Download the Azure root CA certificates: DigiCert Global Root G2 and Microsoft RSA Root CA 2017. 2. Upload to FieldServer Secrets Manager as a CA Certificate. 3. Select this CA Certificate in the broker settings.
"Connection refused" or "Not authorized"	• Device ID in Azure doesn't match certificate CN. • Certificate not properly signed by uploaded CA. • Username format incorrect. • Publishing / subscribing to an invalid or unauthorized topic.	1. Verify Device ID in Azure matches certificate CN exactly. 2. Verify CA certificate in Azure matches the CA that signed device cert. 3. Check username format: <hub>.azure-devices.net/<device-id>/?api-version=2021-04-12. 4. Verify Client ID matches Device ID. 5. Use Azure IoT Hub standard topics.

12.9.2 Certificate Issues

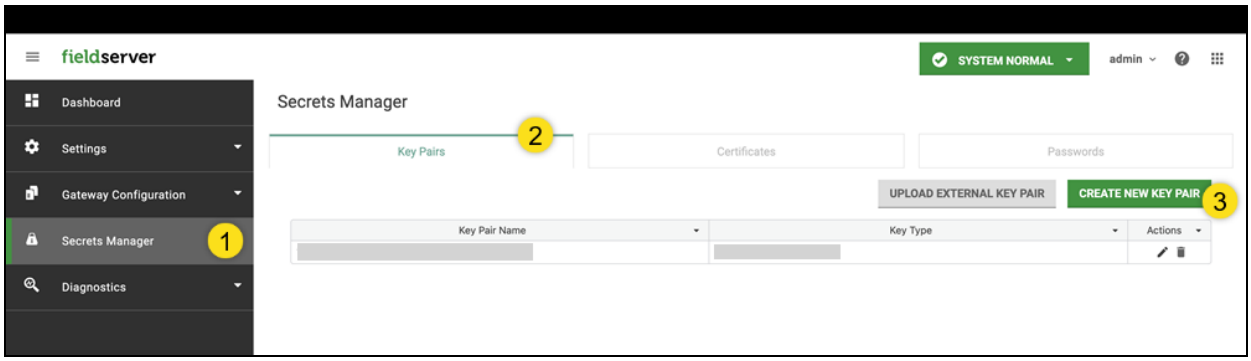
Issue	Cause	Solution
Device shows as registered but cannot connect.	Certificate's Common Name doesn't match the Device ID.	1. In Azure Portal, check the Device ID. 2. In FieldServer, check the certificate's Common Name. 3. Make sure the Device ID and certificate's CN match. 4. If they don't match, generate a new CSR with the correct CN. 5. Repeat the signing process with the new CSR.
Certificate uploaded but shows as "Unverified"	CA Certificate is not verified in Azure.	1. Click on the certificate in Azure Portal. 2. Follow the "Proof of Possession" process.

13 Integrating AWS IoT Core with Modbus IoT Gateway

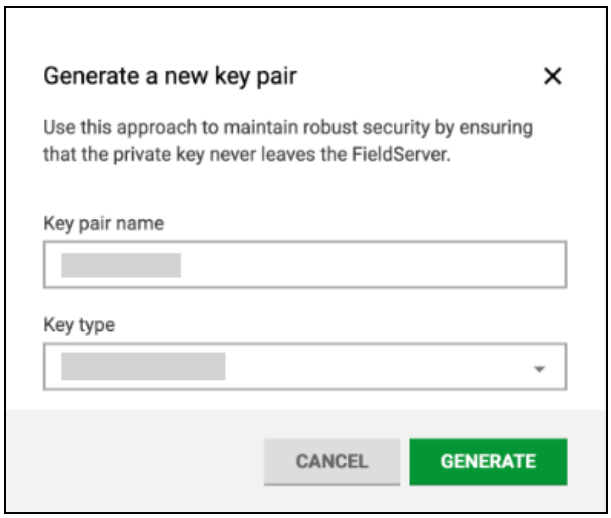
There are two options when integrating AWS IoT Core. One option uses private keys that are generated and securely stored in Modbus IoT Gateway, and the other option uses private keys generated outside of Modbus IoT Gateway. It is recommended that you use generate the keys with Modbus IoT Gateway so that the private keys remain unexposed.

13.1 Using Modbus IoT Gateway-Generated Private Keys for AWS IoT Core

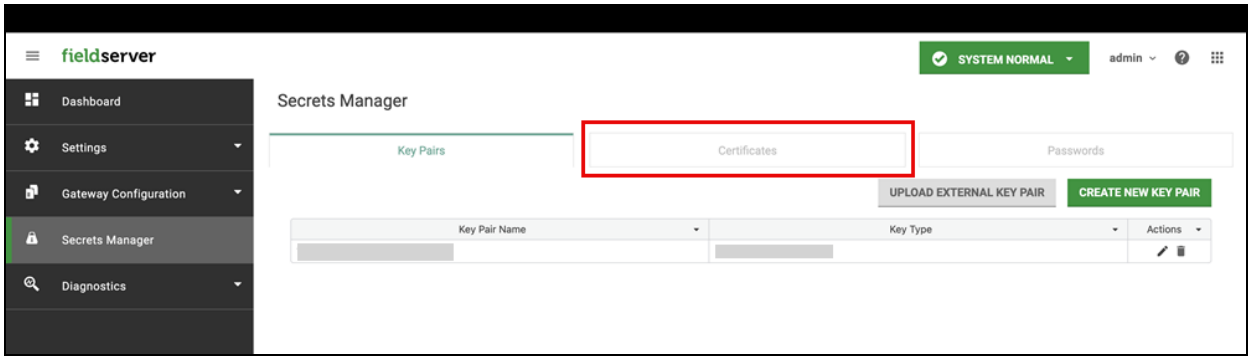
1. Log into Modbus IoT Gateway, and go to Secrets Manager.
2. Go to the Key Pairs section.
3. Click CREATE NEW KEY PAIR. Key pairs are securely stored in Secrets Manager and never exposed in plain text.



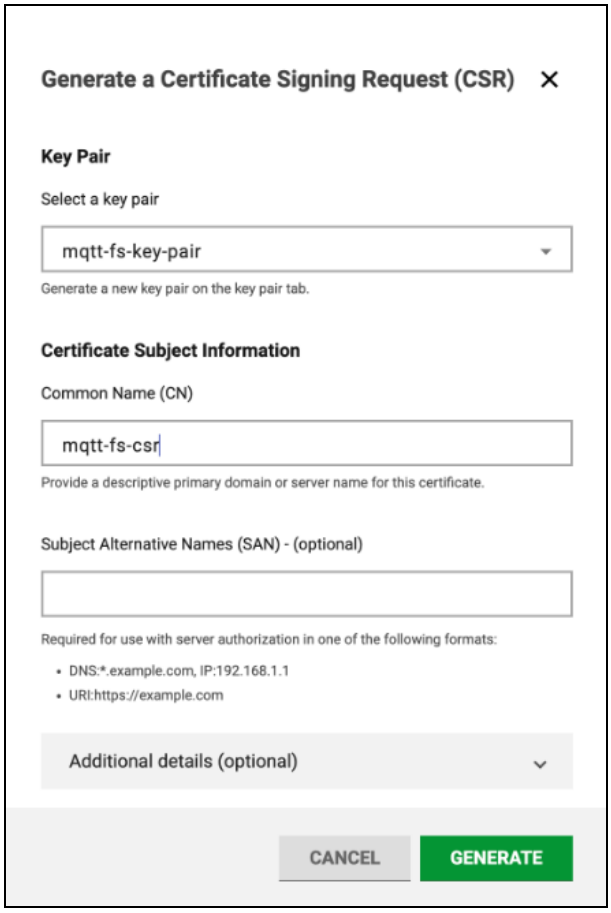
4. Complete the form. It is recommended to name the key pair with a descriptive name.



5. Click Generate for Modbus IoT Gateway to generate the key pair. This key pair is then used to generate a certificate signing request (CSR).
6. Next, generate a Certificate Signing Request by going to the Certificates tab.



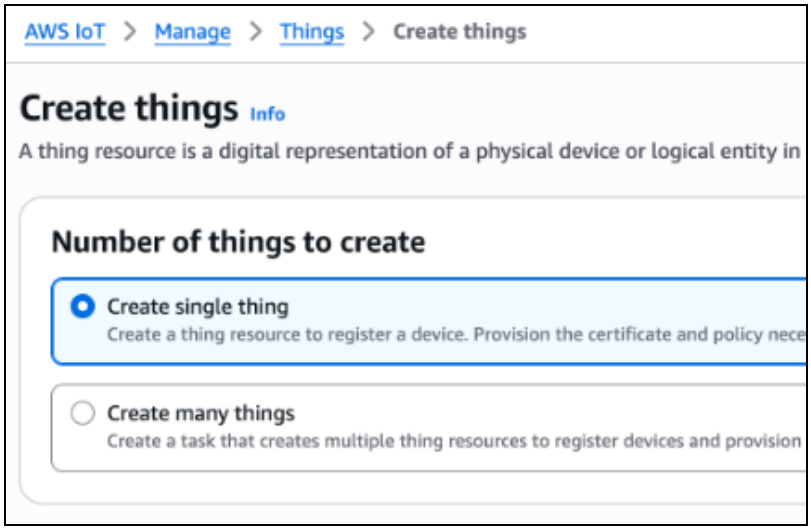
7. Click the NEW CERTIFICATE SIGNING REQUEST (CSR) button.
8. Complete the form that appears, and select the key pair that you created in previous steps.



9. Click GENERATE to generate the CSR. The CSR will then be signed by AWS IoT Core.
10. Log in to AWS, then search and click IoT Core in the AWS search bar.

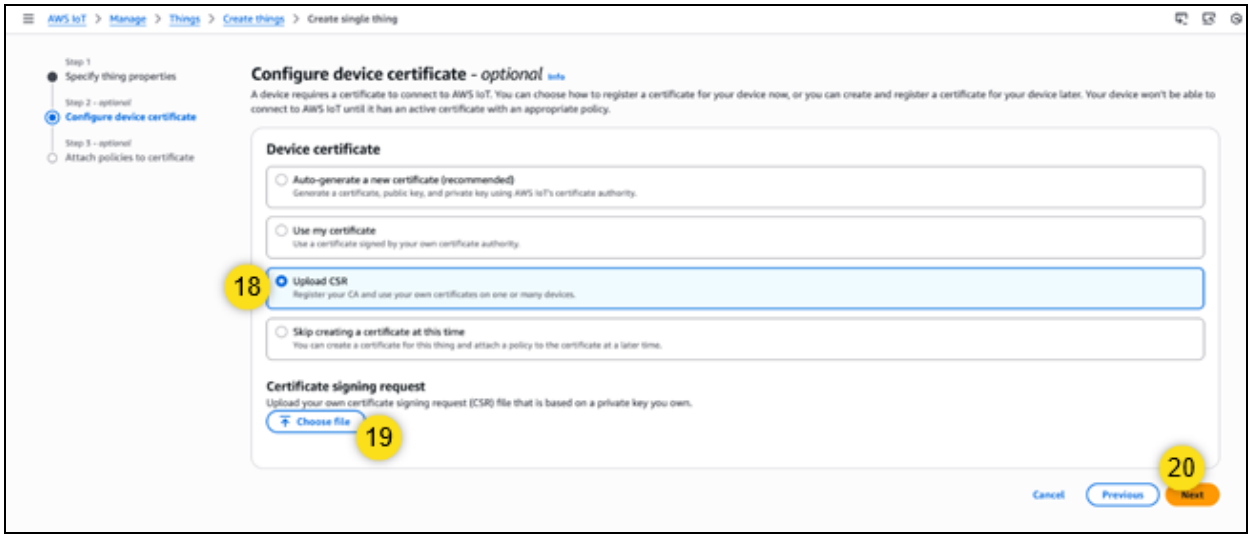
11. Go to Manage in the navigation panel.
12. Uncollapse All devices, then click Things.

13. Click the Create things button in the upper right corner.
14. Select the Create single thing option.

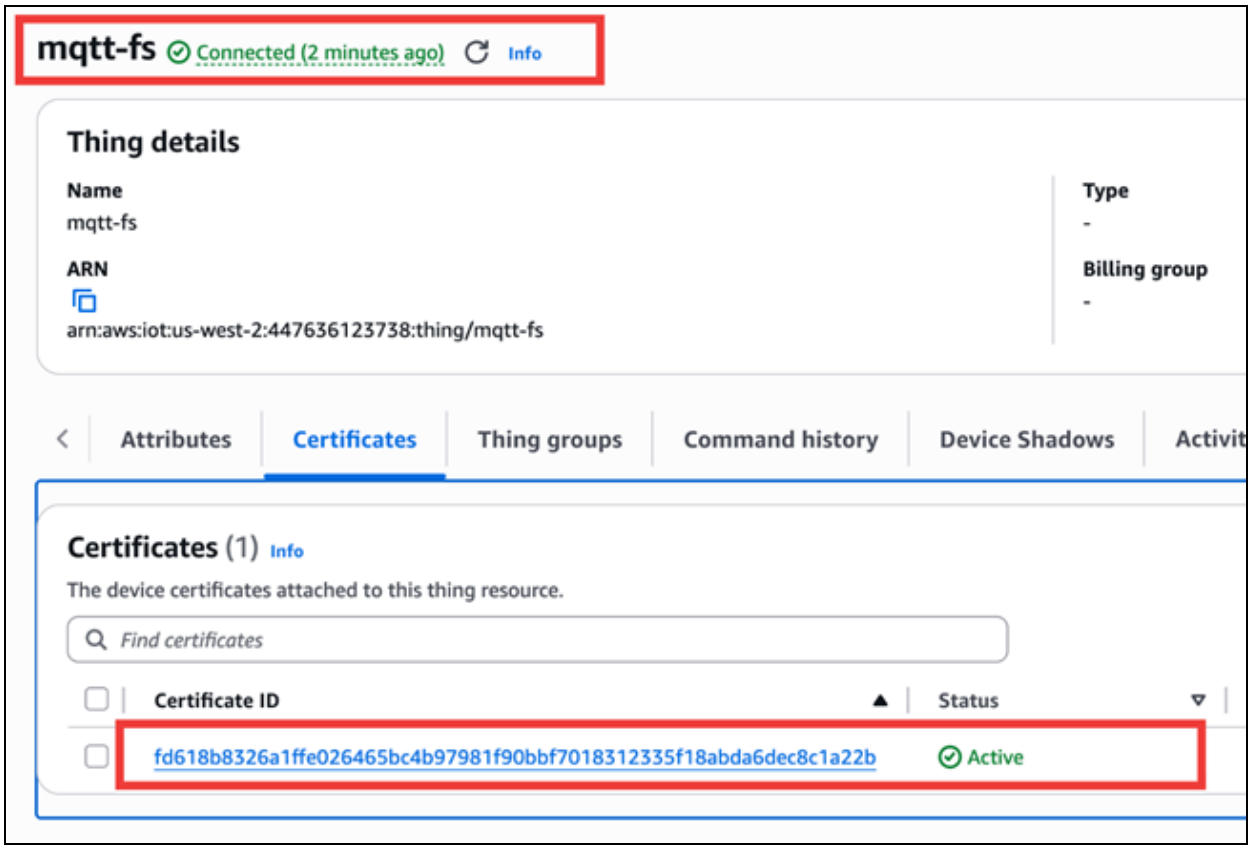


15. Click Next.
16. Enter a name for the Thing name field. **This must match the MQTT connection client ID for it to connect**.
17. Click Next.
18. Select the Upload CSR option.
19. Click the Choose file button, and upload the CSR that you generated in previous steps.

20. Click Next.

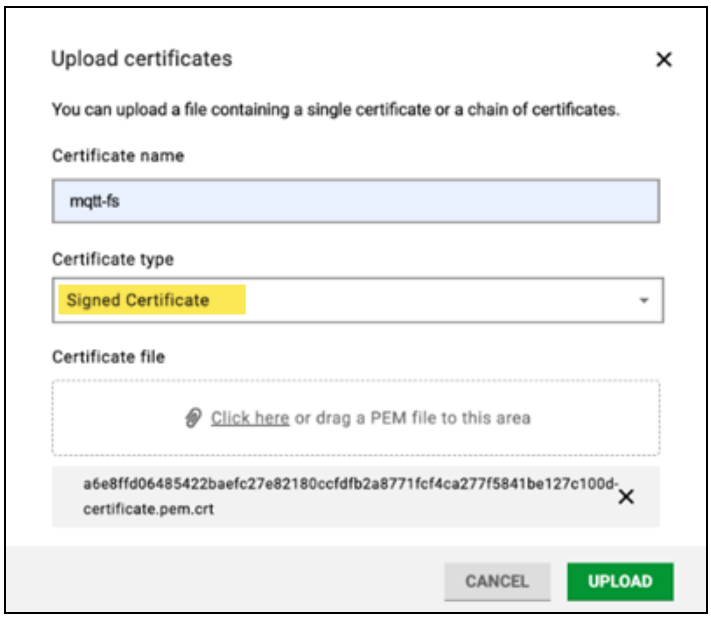


21. Attach a policy to the certificate by selecting or creating a policy with MQTT policy actions. See section 13.3.1 Creating MQTT Action Policies for instructions on creating a new policy.
22. Click the Create thing button. This creates a signed certificate, known in AWS IoT as a "thing".
23. Go to the Things page in All devices in the left panel.
24. Click the AWS IoT thing you created from the list. This opens up more configuration options and details.
25. Select the Certificates tab.
26. Check the statuses. If the statuses show connected and active, then connection was successful.

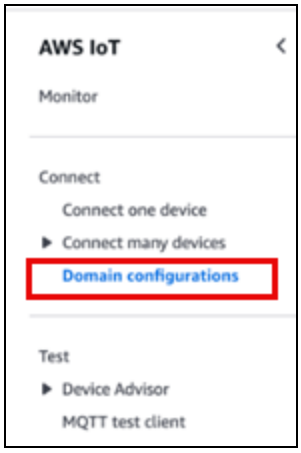


27. Click the certificate ID string, then click the Actions button in the upper right.
    - If the certificate's status shows Inactive, then click Activate to activate the certificate.
28. Click Download to download your X.509 AWS signed certificate.

29. Return to Modbus IoT Gateway and go to the Certificates tab in Secrets Manager.
30. Click Upload Certificate.
31. Enter a certificate name.
32. Select Signed certificate for Certificate type.
33. Upload the AWS signed certificate.
34. Click UPLOAD. The AWS signed certificate is now available in Gateway Configuration.

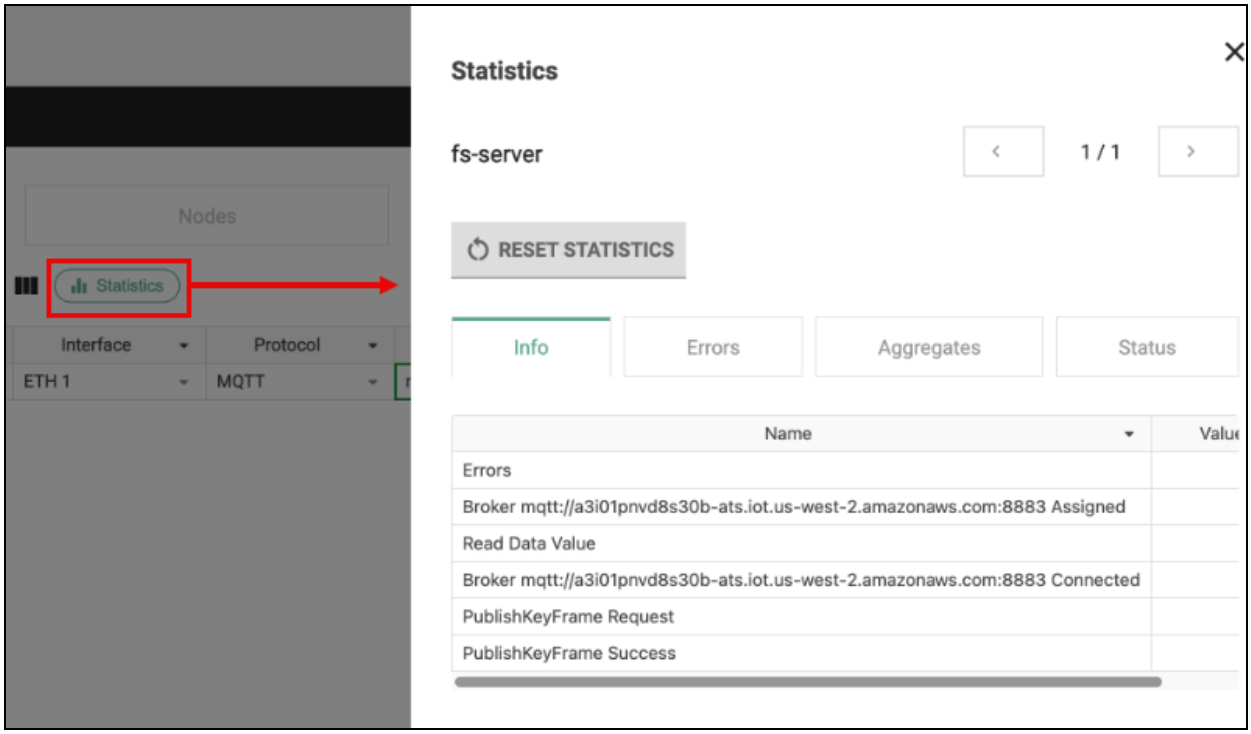


35. Go back to AWS IoT Core to continue integrating it with FieldServer using the AWS signed certificate.
36. In the left panel, go to Domain configurations.

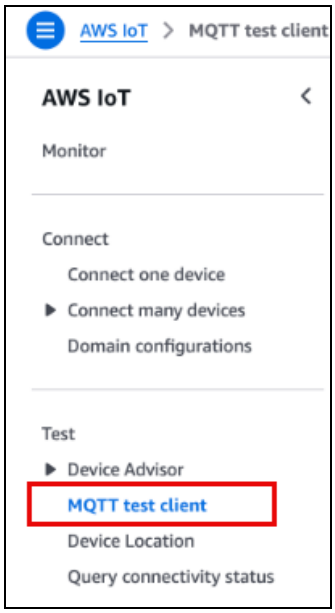


37. Check that the domain status is enabled. If the domain configuration doesn't exist, see 13.3.2 Creating Domain Configurations for additional instructions.

38. Copy the domain name by clicking the icon next to the name. The domain name forms part of your broker URL in the Modbus IoT Gateway configuration.
39. In Modbus IoT Gateway, go to Free-form Editor under Gateway Configuration.
40. Click the Server tab, then click the Connections tab.
41. Add a new row, and enter the following for the respective fields:
    - **Type:** IPv4.
    - **Protocol:** MQTT.
    - **Broker URL:** Paste the domain name copied from AWS IoT Core.
    - **Authentication:** Certificates.
    - **Key Pair:** Select the key pair associated with the AWS signed certificate.
    - **Signed Certificate:** Select the AWS signed certificate.
    - **Client ID:** Enter the AWS Thing name. This must be an exact match.
42. Click on the Nodes tab.
43. Add a new row, and enter the following for the respective fields:
    - **Name:** Enter a descriptive name.
    - **Connection:** Select the previously created connection.
    - **Key Frame Interval(s):** Input your desired publish time in seconds.
    - **Initial Value:** Add a value for testing.
    - **Method:** Publish.
44. Go back to the Connections tab.
45. Select any field for the row you created, then click the Statistics icon to display the connections.

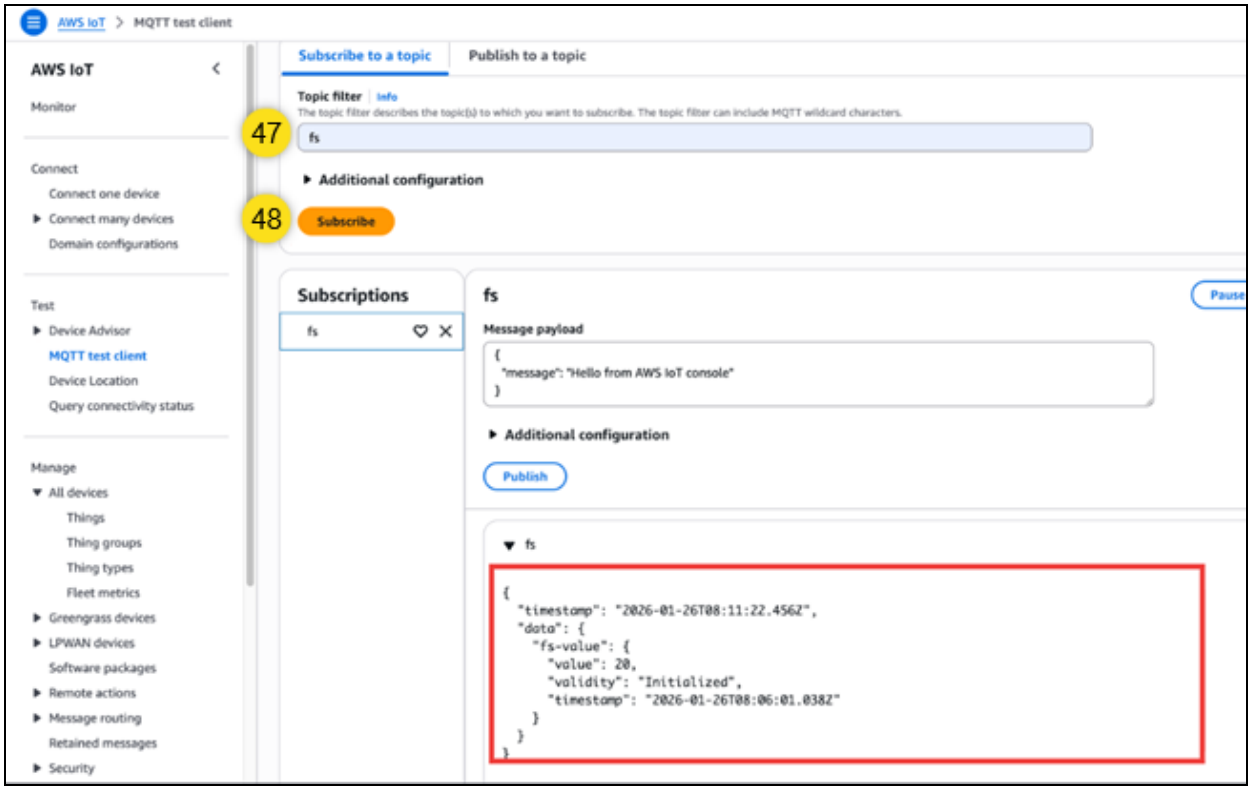


46. Go to AWS IoT Core, and click MQTT test client in the left panel.



47. In the Topic filter, add the topic you're publishing to the Modbus IoT Gateway.

48. Click Subscribe. The subscribed topic will then show the Modbus IoT Gateway data.

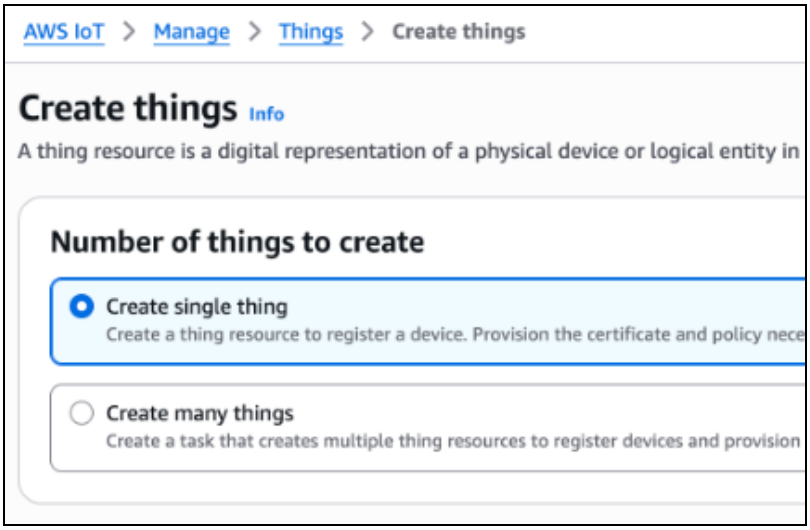


13.2 Using Externally-Generated Private Keys for AWS IoT Core

1. Log in to AWS, then search and click IoT Core in the AWS search bar.

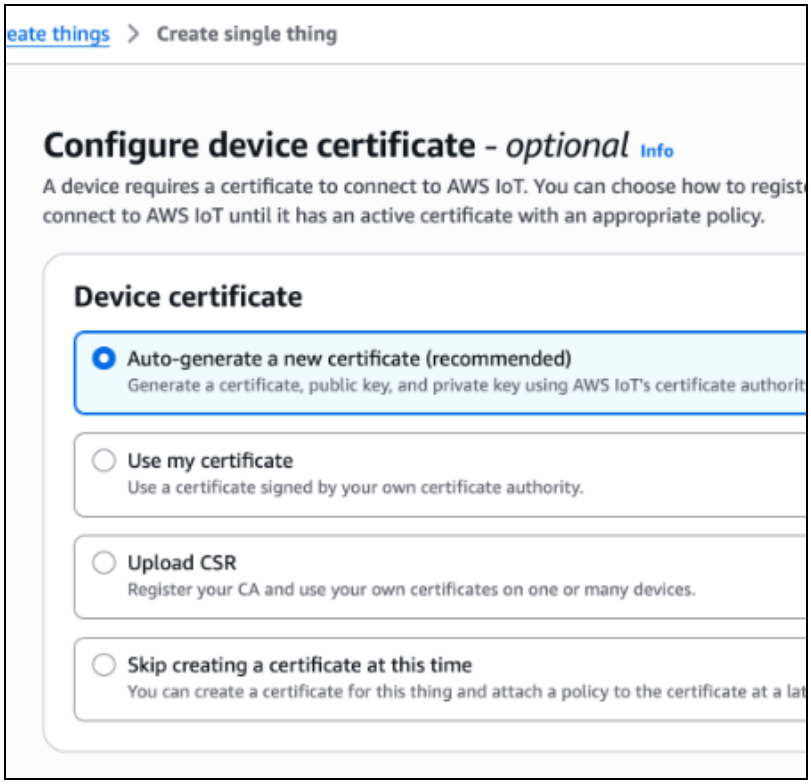
2. Go to Manage in the navigation panel.
3. Uncollapse All devices, then click Things.

4. Click the Create things button in the upper right corner.
5. Select the Create single thing option.



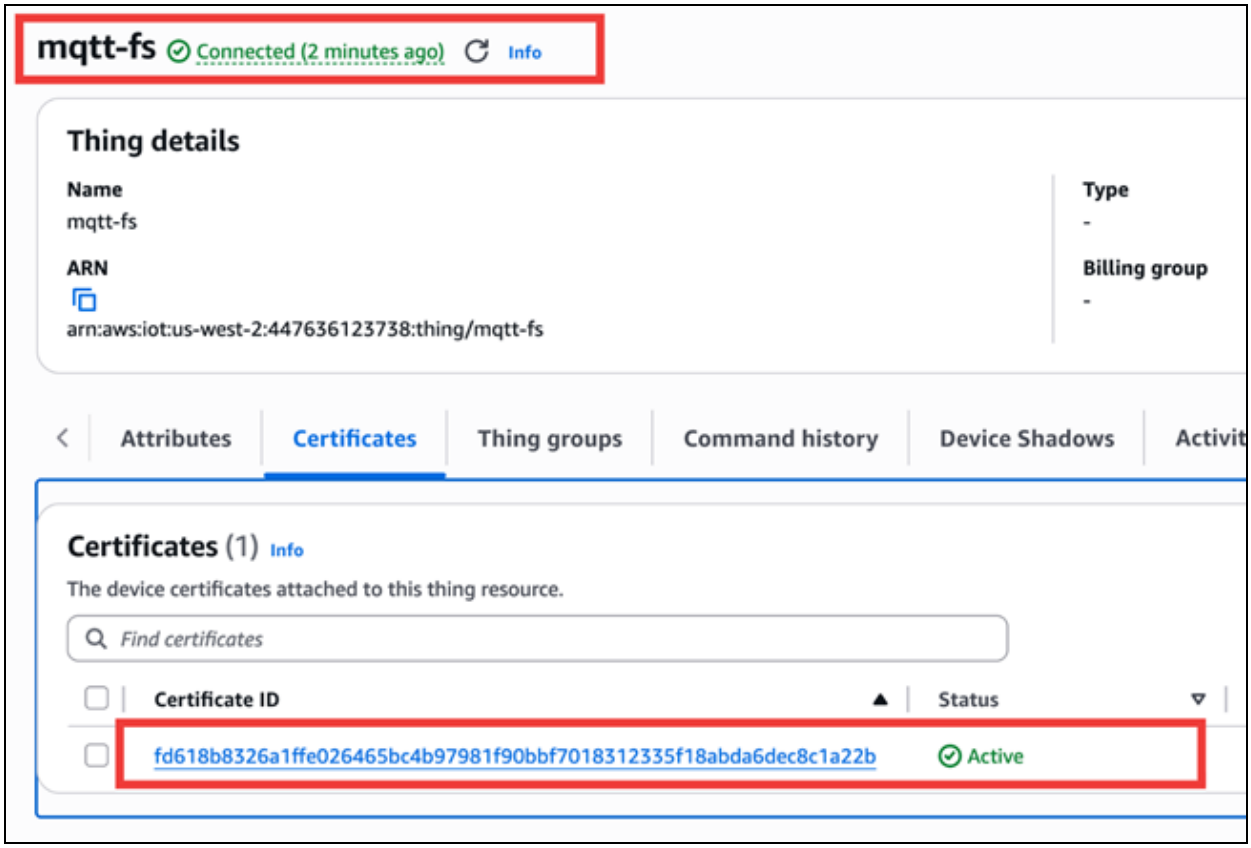
6. Click the Next button.
7. Fill in the Thing name field. **This must match the MQTT connection client ID for it to connect**.
8. Click Next.

9. Select the Auto-generate a new certificate option.

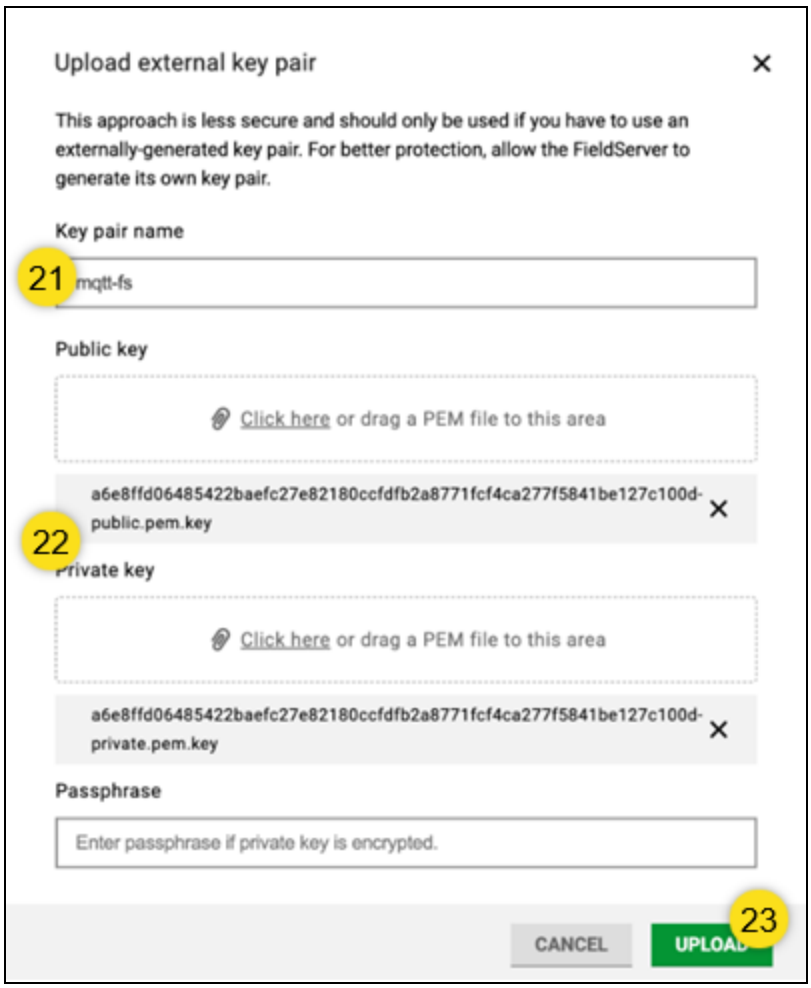


10. Click Next.
11. Select or Create a policy with MQTT policy actions. See section 13.3 Optional AWS IoT Core Steps for Integration for instructions on creating a new policy.
12. Click the Create thing button to create a Thing (signed certificate).
13. Click the Download all button to download all the certificates and keys. The files include a public key, private key, and self-signed device certificate that you must upload to FieldServer.
14. In the Things list, click the Thing that you created in the previous steps.
15. Select the Certificates tab.

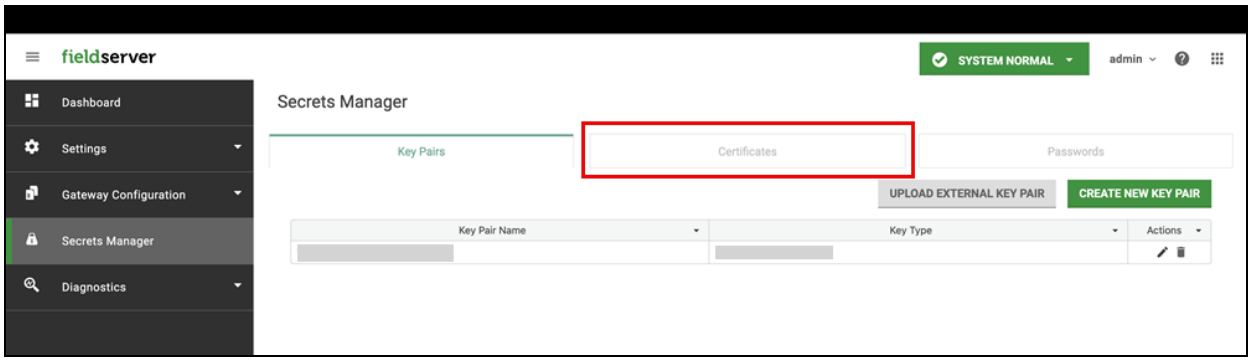
16. Check the statuses. If the statuses show connected and active, then connection was successful.



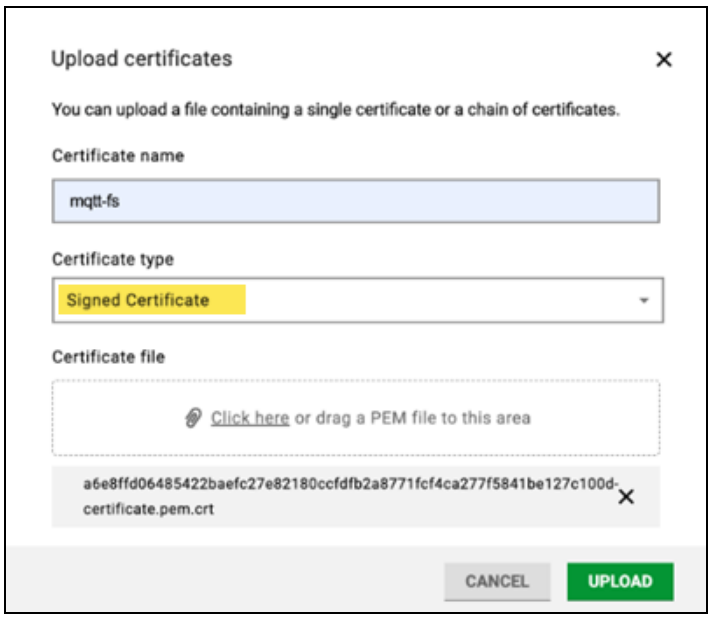
17. Click the certificate ID string, then click the Actions button in the upper right.
    - If the certificate's status shows Inactive, then click Activate to activate the certificate.
18. Click Download. The downloaded certificate is your AWS-signed certificate .
19. Log in to FieldServer, and go to Key Pair under Secrets Manager.
20. Click UPLOAD EXTERNAL KEY PAIR.
21. Name the key pair.
22. Browse and upload both the public and private key files that you downloaded from AWS IoT Core.
23. Click UPLOAD.



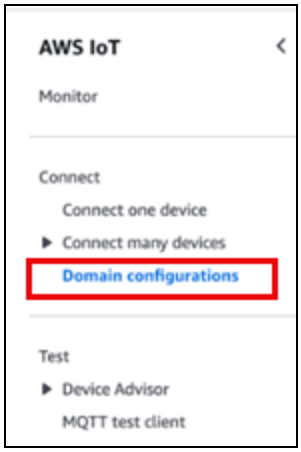
24. Go to the Certificates tab in Secrets Manager.



25. Click UPLOAD CERTIFICATE.
26. Fill in the certificate name.
27. Select Signed Certificate for the certificate type.
28. Click the UPLOAD button. The certificate is now available in Gateway Configuration in Modbus IoT Gateway.



29. Go back to AWS IoT Core to continue integrating it with Modbus IoT Gateway.
30. In the left panel, go to Domain configurations.

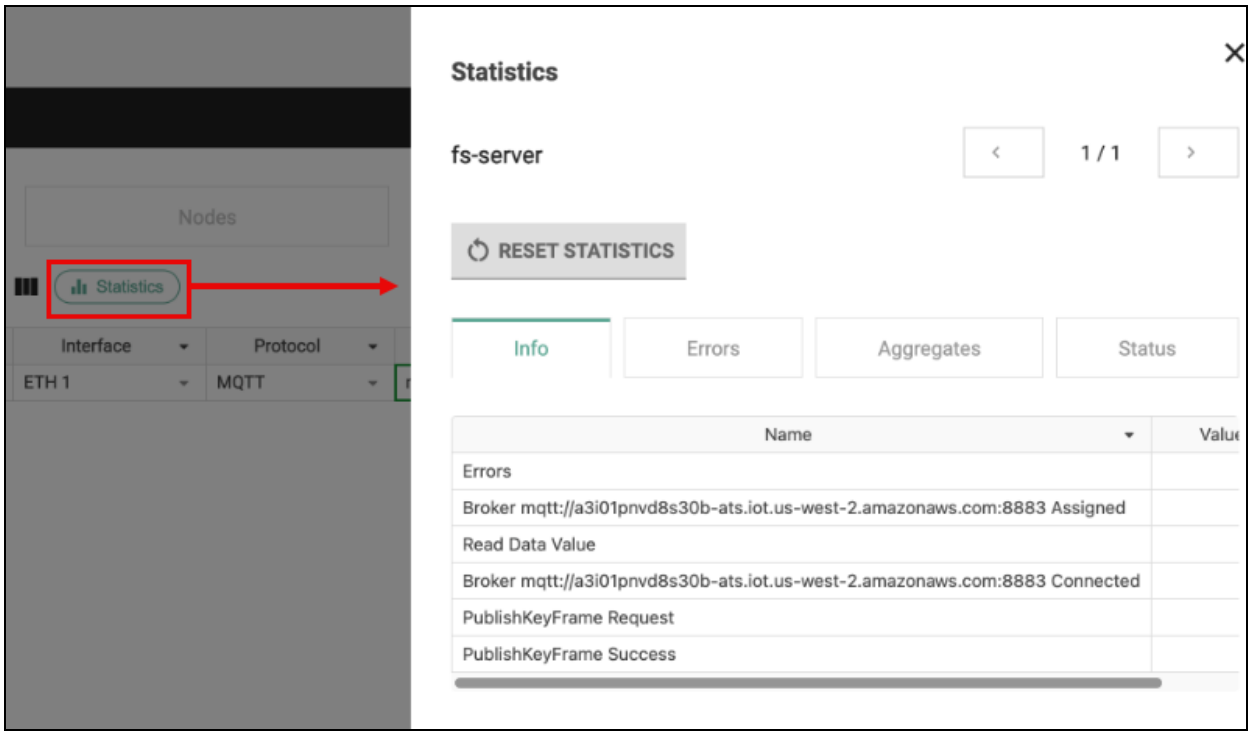


31. Check that the domain status is enabled. If the domain configuration doesn't exist, see 13.3.2 Creating Domain Configurations for additional instructions.

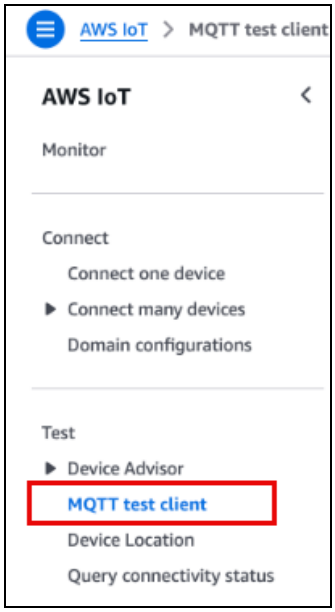
32. Copy the domain name by clicking the icon next to the name. The domain name forms part of your broker URL in the Modbus IoT Gateway configuration.
33. In Modbus IoT Gateway, go to Free-form Editor under Gateway Configuration.
34. Click the Server tab, then click the Connections tab.
35. Add a new row, and enter the following for the respective fields:
    - **Type:** IPv4.
    - **Protocol:** MQTT.
    - **Broker URL:** Paste the domain name copied from AWS IoT Core.

- **Authentication:** Certificates.
- **Key Pair:** Select the key pair associated with the AWS signed certificate.
- **Signed Certificate:** Select the AWS signed certificate.
- **Client ID:** Enter the AWS Thing name. This must be an exact match.

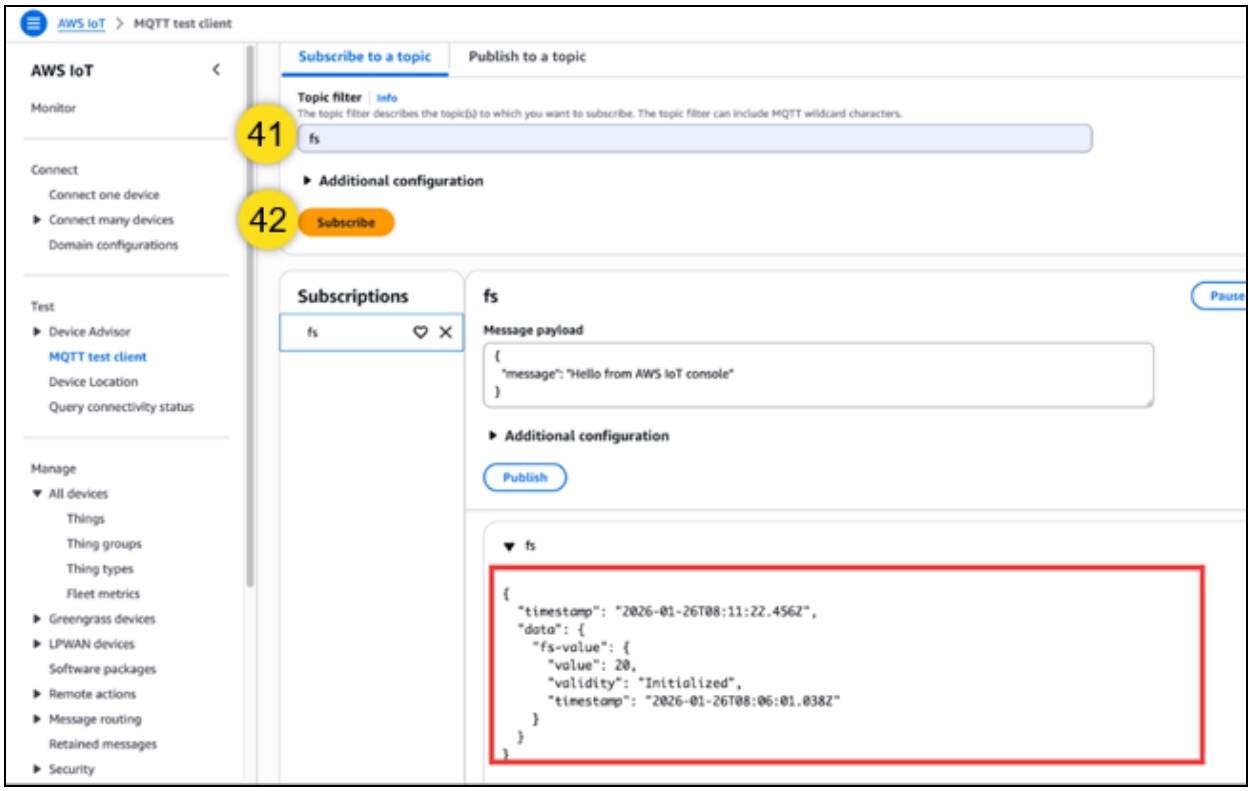
36. Click on the Nodes tab.
37. Add a new row, and enter the following for the respective fields:
    - **Name:** Enter a descriptive name.
    - **Connection:** Select the previously created connection.
    - **Key Frame Interval(s):** Input your desired publish time in seconds.
    - **Initial Value:** Add a value for testing.
    - **Method:** Publish.
38. Go back to the Connections tab.
39. Select any field for the row you created, then click the Statistics icon to display the connections.



40. Go to AWS IoT Core, and click MQTT test client in the left panel.



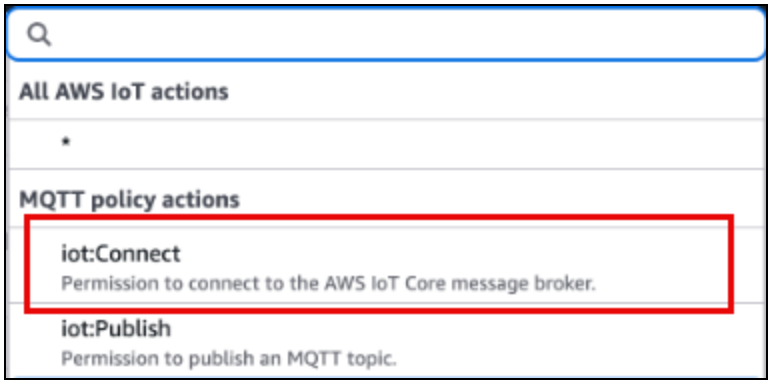
41. In the Topic filter, add the topic you're publishing to the Modbus IoT Gateway.
42. Click Subscribe. The subscribed topic will then show the FieldServer data.



13.3 Optional AWS IoT Core Steps for Integration

13.3.1 Creating MQTT Action Policies

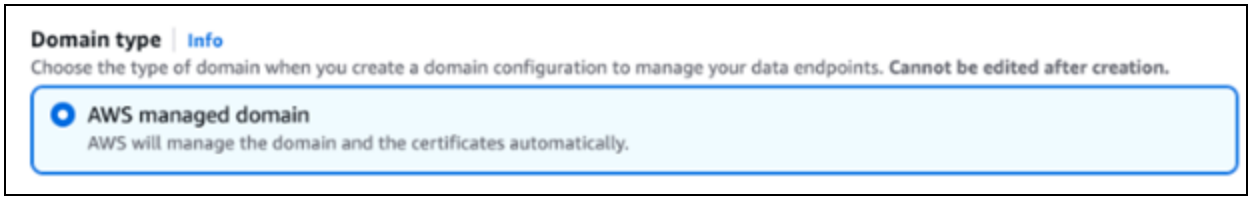
1. Click on the Policy Action drown-down.
2. Select IoT:Connect.



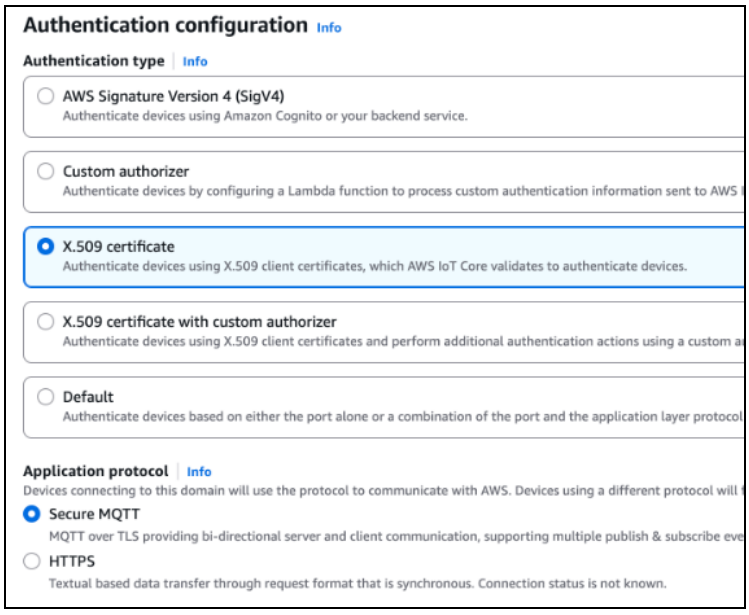
3. In the Policy Resource, add the following: ** or specific resource that is allowed*
4. Click Add new statement.
5. Add all available MQTT policy actions to Policy statements.
6. Click Create, then select this policy to attach to the certificate.

13.3.2 Creating Domain Configurations

1. Click the Create domain configuration button.
2. Add a domain configuration name.
3. For Domain type, select AWS managed domain.



4. For Authentication type, select X.509 certificate.
5. For Application protocol, select Secure MQTT.



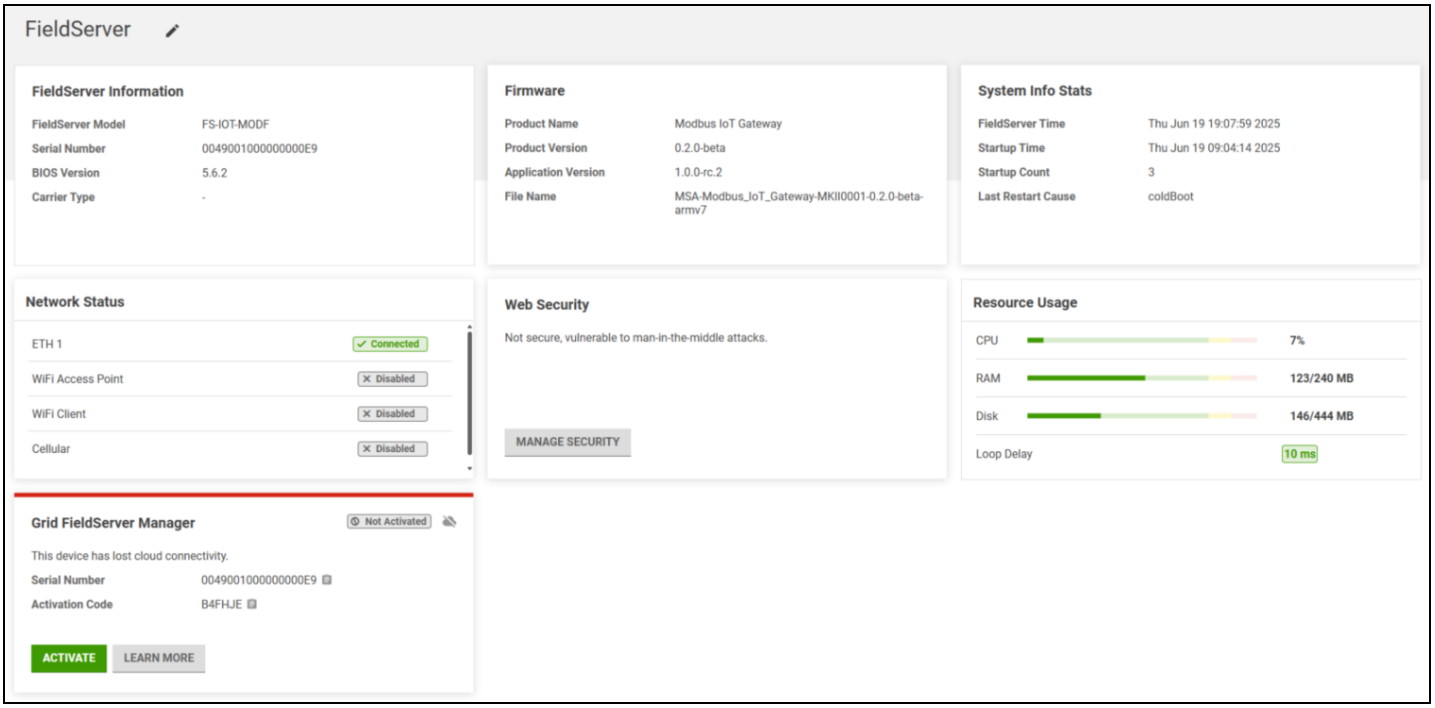
6. Click the Create domain configuration button.

14 MSA Grid - FieldSever Manager Setup

The MSA Grid is MSA Safety's device cloud solution for IIoT. Integration with the MSA Grid - FieldServer Manager enables a secure remote connection to field devices through a FieldServer and hosts local applications for device configuration, management, as well as maintenance. For more information about the FieldServer Manager, refer to the MSA Grid - FieldServer Manager Start-up Guide.

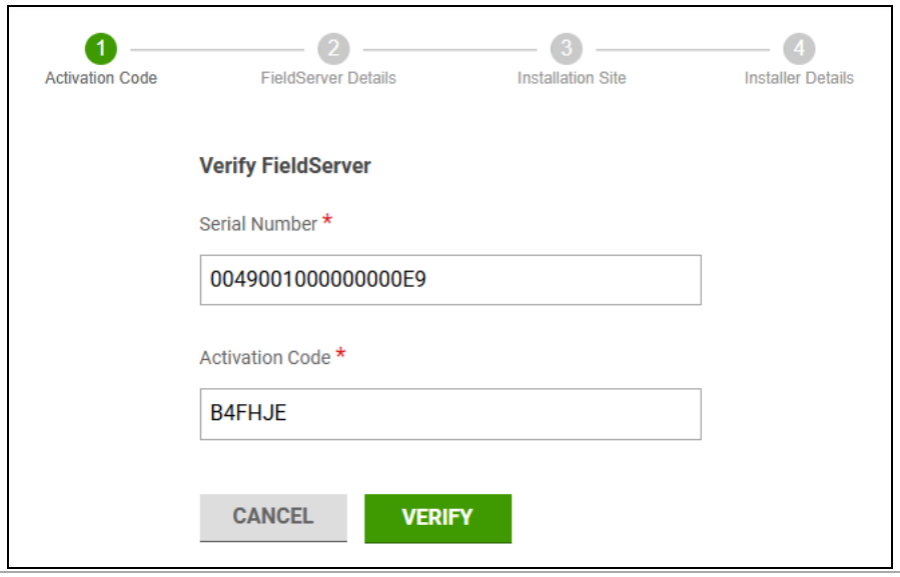
14.1 Activate the Modbus IoT Gateway on Grid – FieldServer Manager

The first step to connecting to the FieldServer Manager is to create an account. Please contact support (smc-support@msasafety.com) to create an account.

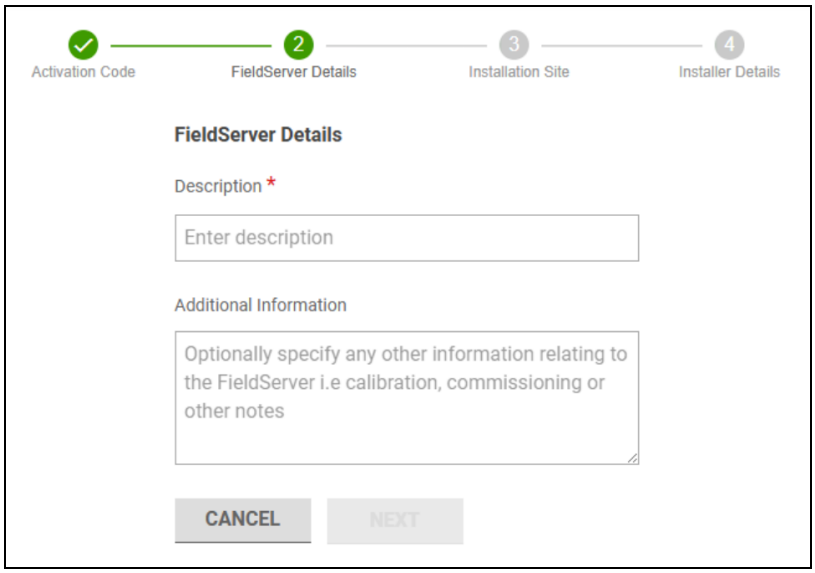


To activate the device on your account:

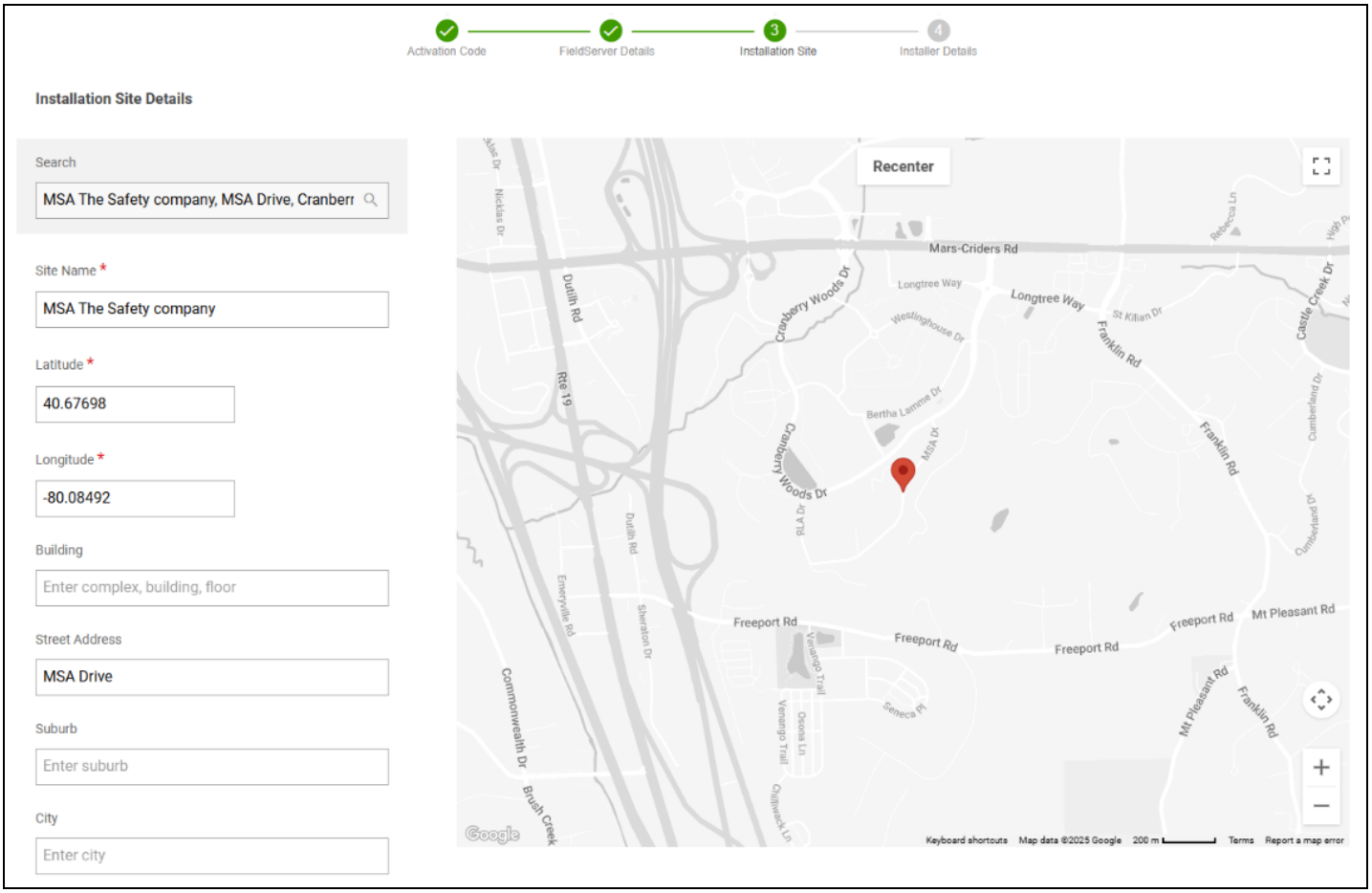
1. Go to the FieldServer Dashboard. The Grid FieldServer Manager tile at the bottom of the screen contains your FieldServer serial number and activation code.
2. Click the Activate button. The FieldServer Manager is opened in the browser.
3. Enter your credentials and login.
4. Confirm that the serial number and the activation code match your Modbus IoT Gateway, then click Verify.



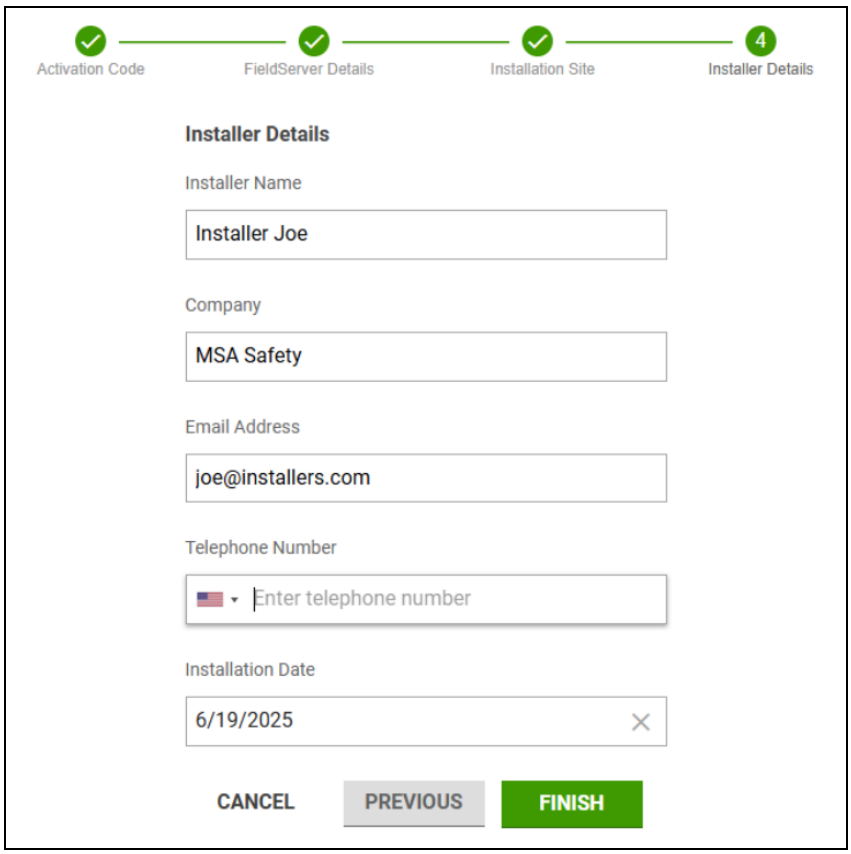
5. Fill in any extra details about the Modbus IoT Gateway on the next page.



6. Set the device location using the Search or the Map.



7. Fill in the site name where this device is located, then click Next.
8. Fill in the Installer Details form with all required fields and click Finish.



14.2 Using the FieldServer Manager

Connecting your FieldServer to the FieldServer Manager allows the user to:

- Securely tunnel to the device remotely
- Download device data logs
- Search for events and set up notifications on the device

15 Specifications

Electrical Connections	• One 3-pin Phoenix connector with RS-485/RS-232 (Tx+ / Rx- / gnd) • One 3-pin Phoenix connector with Power port (+ / - / Frame-gnd) • One Ethernet 10/100 BaseT port

MOD/MODW/MOD2 Power Requirements	• Input Voltage: 12-24VDC or 24VAC
	• Max Power: 3 Watts
	• Current Draw:
	  ○ 24VAC 0.125A
	  ○ 12-24VDC 0.25A @12VDC

MODA/V/FPower Requirements	• Input Voltage: 12-24VDC • Max Power: 8 Watts • Current Draw: @ 12V, 0.67A
Approvals	FCC Part 15, UL 60950-1 and CAN/CSA C22.2 No. 60950-1 (**MODW**), EN IEC 62368-1:2020+A11:2020, WEEE compliant, RoHS compliant, DNP 3.0 and Modbus conformance tested, PTCRB compliant (**MODA/V/F**), BTL marked, REACH compliant, UKCA and CE compliant, CAN ICES-003(B) / NMB-003(B) (**MODW/A/V/2**)
FCC ID	(MODW) P9R-FPAW44
IC ID	(MODW) 324C-FPAW44
Physical Dimensions	4 x 1.1 x 2.7 in (10.16 x 2.8 x 6.8 cm)
Weight	0.4 lbs (0.2 Kg)
Operating Temperature	-20°C to 70°C (-4°F to158°F)
Humidity	10-95% RH non-condensing
FS-IOT-MODA/V/F Cellular	• Features: LTE Cat 4 • Antenna: Omnidirectional 4G/LTE SMA • Uplink: Up to 50 Mbps • Downlink: Up to 150 Mbps

Table 1 FS-IOT-MOD, FS-IOT-MODW, and FS-IOT-MOD2/A/V/FSpecifications

NOTE: Specifications subject to change without notice.

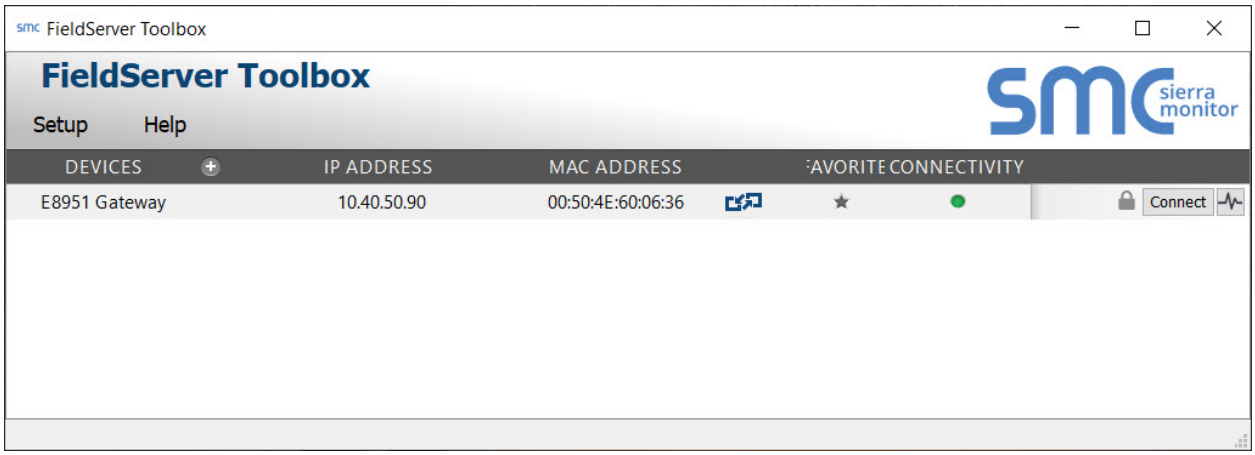
16 Troubleshooting

16.1 Communicating with the Modbus IoT Gateway Over the Network

1. Confirm that the network cabling is correct.
2. Confirm that the computer network card is operational and correctly configured.
3. Confirm that there is an Ethernet adapter installed in the PC's Device Manager list, and that it is configured to run the TCP/IP protocol.
4. Check that the IP netmask of the PC matches the Modbus IoT Gateway. The Default IP address of the Modbus IoT Gateway is 192.168.2.X, and the subnet mask is 255.255.255.0.
    a. Go to Start|Run
    b. Type in "ipconfig"
    c. The account settings should be displayed
    d. Ensure that the IP address is 102.168.2.X, and the netmask is 255.255.255.0
5. Ensure that the PC and Modbus IoT Gateway are on the same IP network, or assign a Static IP address to the PC on the 192.168.2.X network.

16.2 Lost or Incorrect IP Address

1. Ensure that FieldServer Toolbox is loaded onto the local PC. Otherwise, download the FieldServer-Toolbox.zip via the MSA Safety website.
2. Extract the executable file and complete the installation.
3. Connect a standard Cat-5 Ethernet cable between the user's PC and Modbus IoT Gateway.
4. Double click on the FS Toolbox Utility and click Discover Now on the splash page.
5. Check for the IP Address of the desired gateway.



16.3 Checking Wiring and Settings

No COMS on the side. If the Tx/Rx LEDs are not flashing rapidly, then there is a COM issue. To fix this problem, do the following:

- Visual observations of LEDs on the Modbus IoT Gateway. (Section **16.6 LED Functions**)
- Check baud rate, parity, data bits, and stop bits.
- Check device address.
- Verify wiring.
- Verify the device .

For Field COM problems:

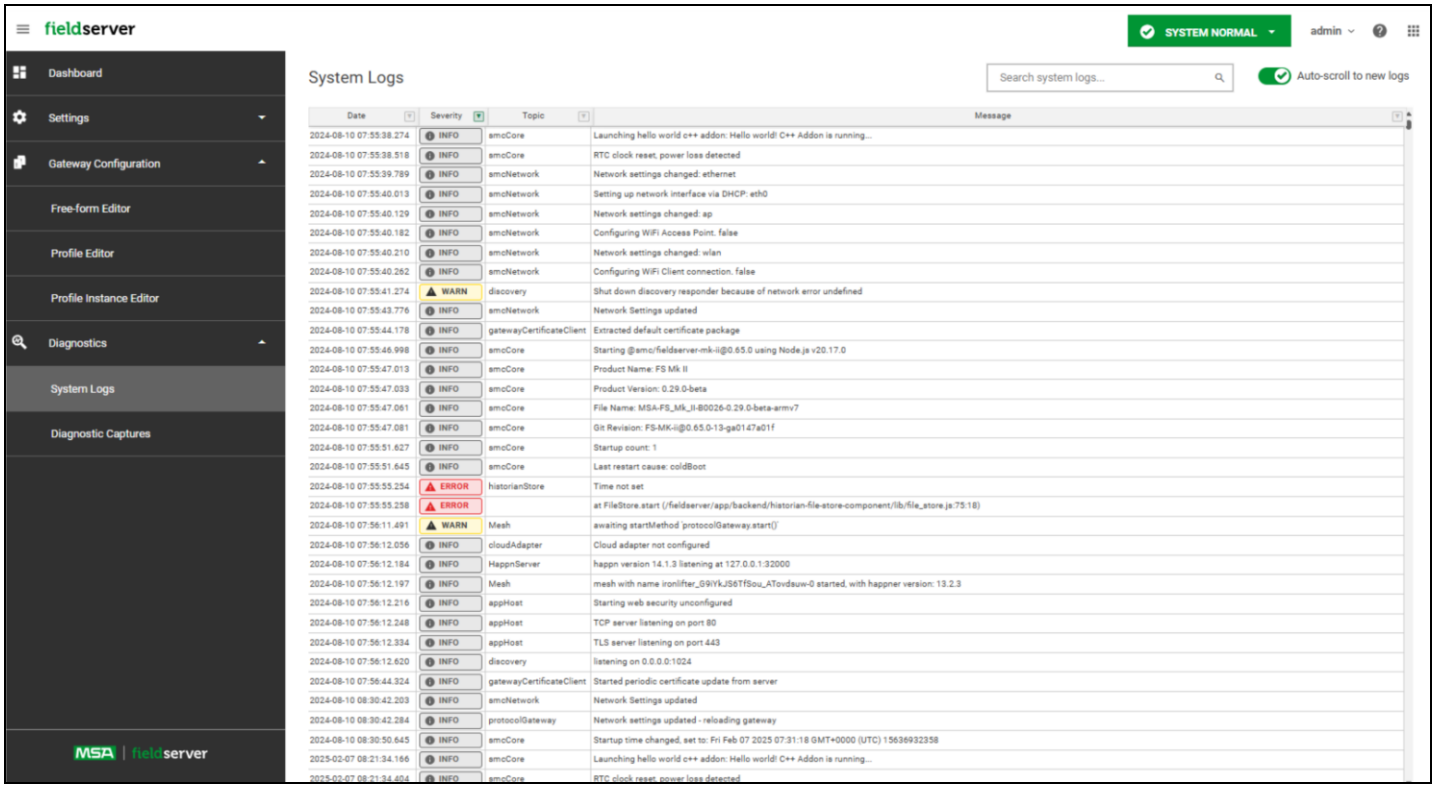
- Visual observations of LEDs on the Modbus IoT Gateway. (Section **16.6 LED Functions**)
- Verify wiring.
- Verify IP Address setting.

NOTE: If the problem still exists, a Diagnostic Capture needs to be taken and sent to support. (Section 16.4 Diagnostic Capture)

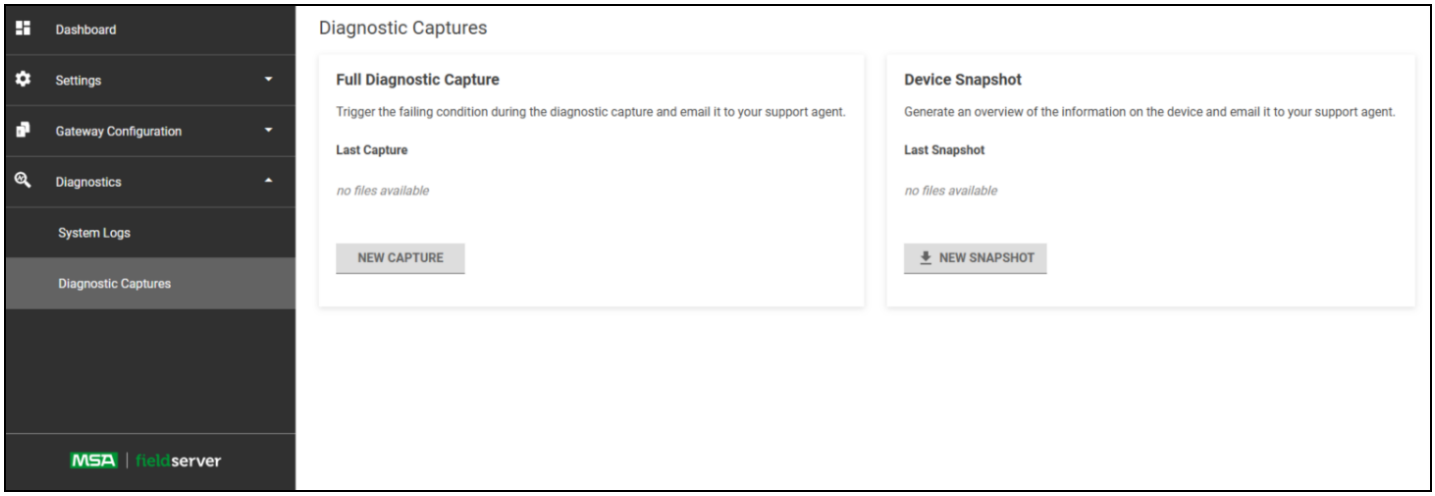
16.4 Diagnostic Capture

When there is a problem on-site that cannot easily be resolved, perform a diagnostic capture before contacting support. Once the diagnostic capture is complete, email it to technical support. The diagnostic capture will accelerate diagnosis of the problem.

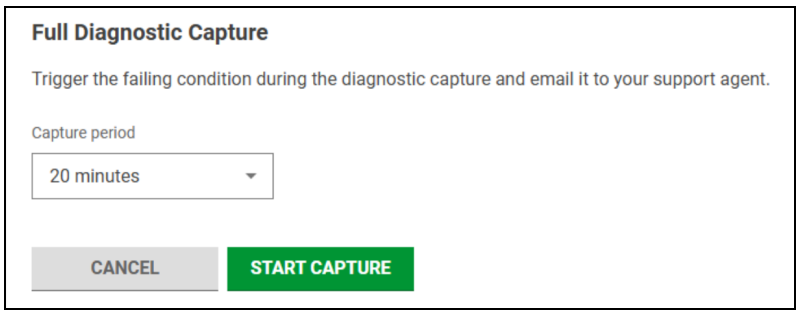
1. Access the FieldServer Diagnostics page by opening the FieldServer FS-GUI page and clicking on Diagnostics in the Navigation panel. Then click on System Logs.



2. Go to Diagnostic Captures and click NEW CAPTURE.



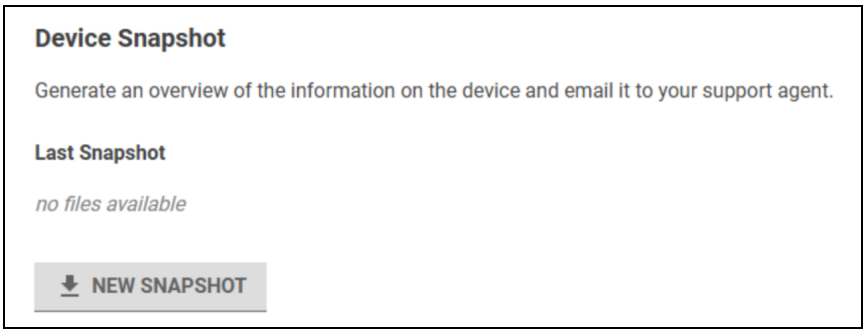
3. From the drop down, select your desired capture period, then click the START CAPTURE button. When the capture period is finished, a DOWNLOAD button will appear next to the START CAPTURE button.



4. Click DOWNLOAD for the capture to be downloaded to the local PC.
5. Email the diagnostic zip file to technical support (smc-support.@msasafety.com).

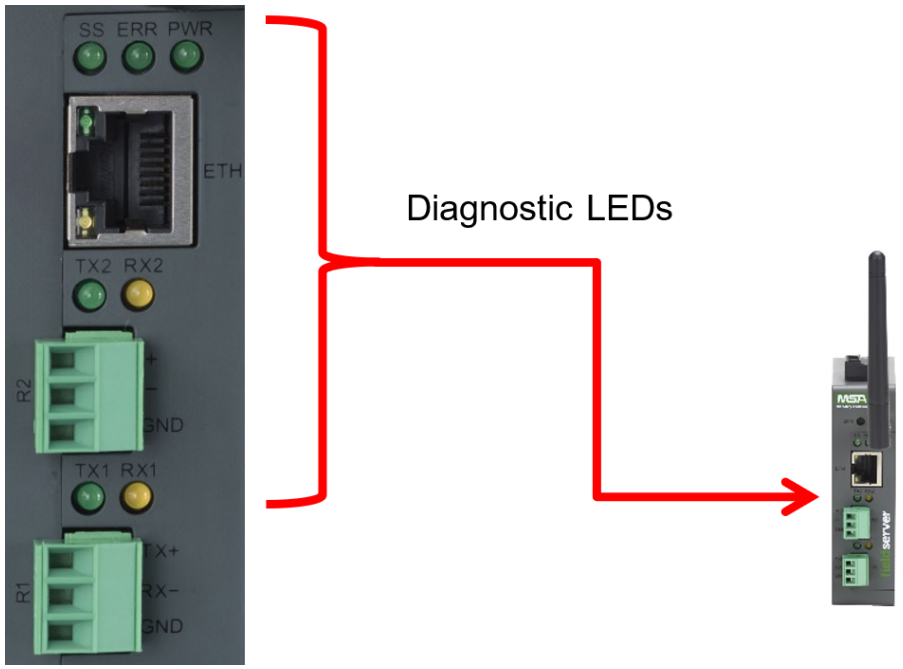
16.5 Device Snapshot

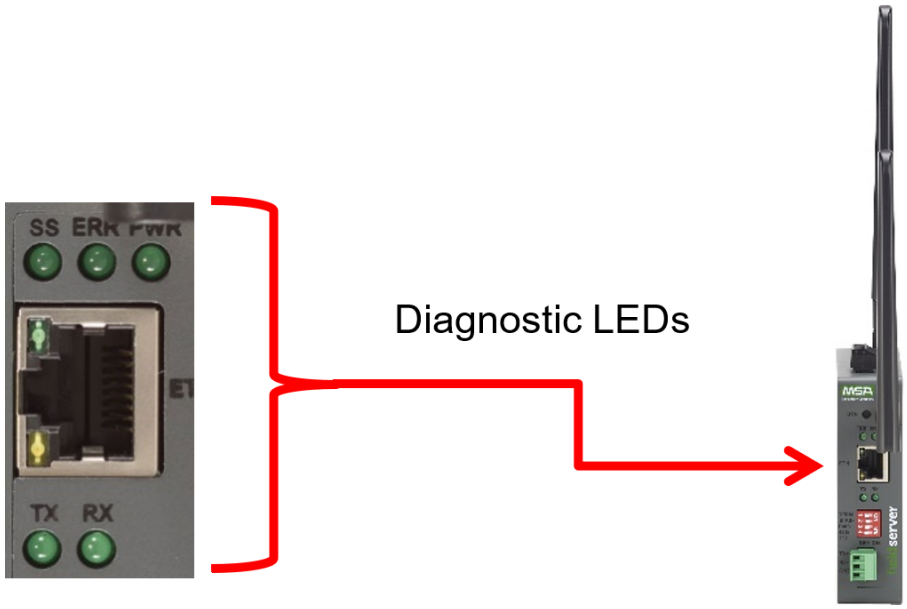
1. Open the FieldServer FS-GUI page and click Diagnostics in the Navigation panel.
2. In the Device Snapshot section, click NEW SNAPSHOT.



3. After the diagnostic zip file loads, click on the down arrow icon to download the capture to the local PC.
4. Email the diagnostic zip file to technical support (smc-support.@msasafety.com).

16.6 LED Functions





Tag	Description
SS	The SS LED will flash once a second to indicate that the bridge is in operation.
ERR	The SYS ERR LED will go on solid indicating there is a system error. If this occurs, immediately report the related “system error” shown in the error screen of the FS-GUI interface to support for evaluation.
PWR	This is the power light and should always be steady green when the unit is powered.
RX	The RX LED will flash when a message is received on the serial port on the 3-pin connector. If the serial port is not used, this LED is non-operational. **For the FS-IOT-MOD/MODW** RX1 applies to the R1 connection while RX2 applies to the R2 connection.
TX	The TX LED will flash when a message is sent on the serial port on the 3-pin connector. If the serial port is not used, this LED is non-operational. **For the FS-IOT-MOD/MODW** TX1 applies to the R1 connection while TX2 applies to the R2 connection.

16.7 Wi-Fi and Cellular Signal Strength

Wi-Fi	Cellular
<60dBm – Excellent	< 60dBm – Excellent
<70dBm – Very good	<70dBm – Very good
<80dBm – Good	<80dBm – Good
>80dBm – Weak	<90dBm – Weak
	>90dBm – Spotty; not good for data

NOTE: If the signal is weak or spotty, try to improve the signal strength by checking the antenna and the FieldServer position.

16.8 Factory Reset Instructions

For instructions on how to reset a FieldServer back to its factory released state, see ENOTE FieldServer Next Gen Recovery.

16.9 Internet Browser Software Support

The following web browsers are supported:

- Chrome Rev. 57 and higher
- Firefox Rev. 35 and higher
- Microsoft Edge Rev. 41 and higher
- Safari Rev. 3 and higher

Internet Explorer is no longer supported as recommended by Microsoft.

NOTE: Computer and network firewalls must be opened for Port 80 to allow Modbus IoT Gateway GUI to function.

16.10 Two Ethernet Port IP Subnets

If the user has one of the two Ethernet port units, the Eth1 and Eth2 ports need to be configured on different IP subnets, otherwise the Modbus IoT Gateway will not be able to discover any IP addresses or devices on the network.

For example, if the ETH1 port is configured at 192.168.2.101, then the Eth 2 port cannot be configured with the same 192.168.2.XXX settings.

16.11 Data Missing on RESTful API and/or the Grid

If a RESTful API call for data fails and the Modbus IoT Gateway is not listed as a Device Name in the Data Logs found on the Grid, check heck that the Modbus IoT Gateway has been registered to the Grid. (Section **14.1 Activate the Modbus IoT Gateway on Grid – FieldServer Manager**).

17 Additional Information

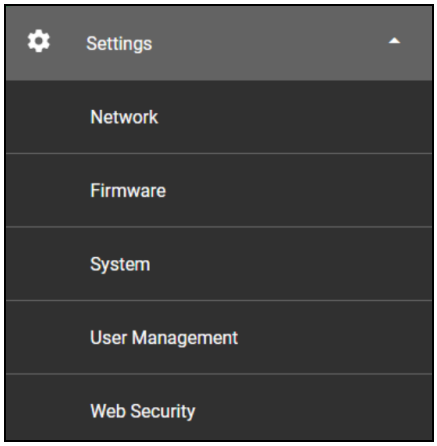
17.1 APN Table

Use the table below to enter one of the correct APNs for your sim card:

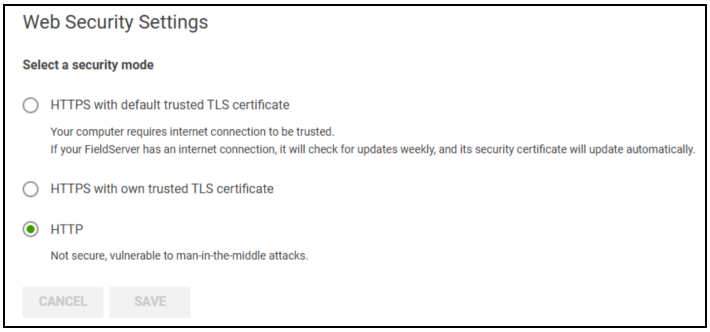
Cellular Provider	APN
AT&T	broadband NXTGENPHONE
Verizon	Vzwinternet internet
Kore	c2.korem2m.com

17.2 Changing Web Server Security Settings After Initial Setup

1. From the Modbus IoT Gateway landing page, click the Settings tab and click the Web Security tab.



The different security modes provides different levels of security:

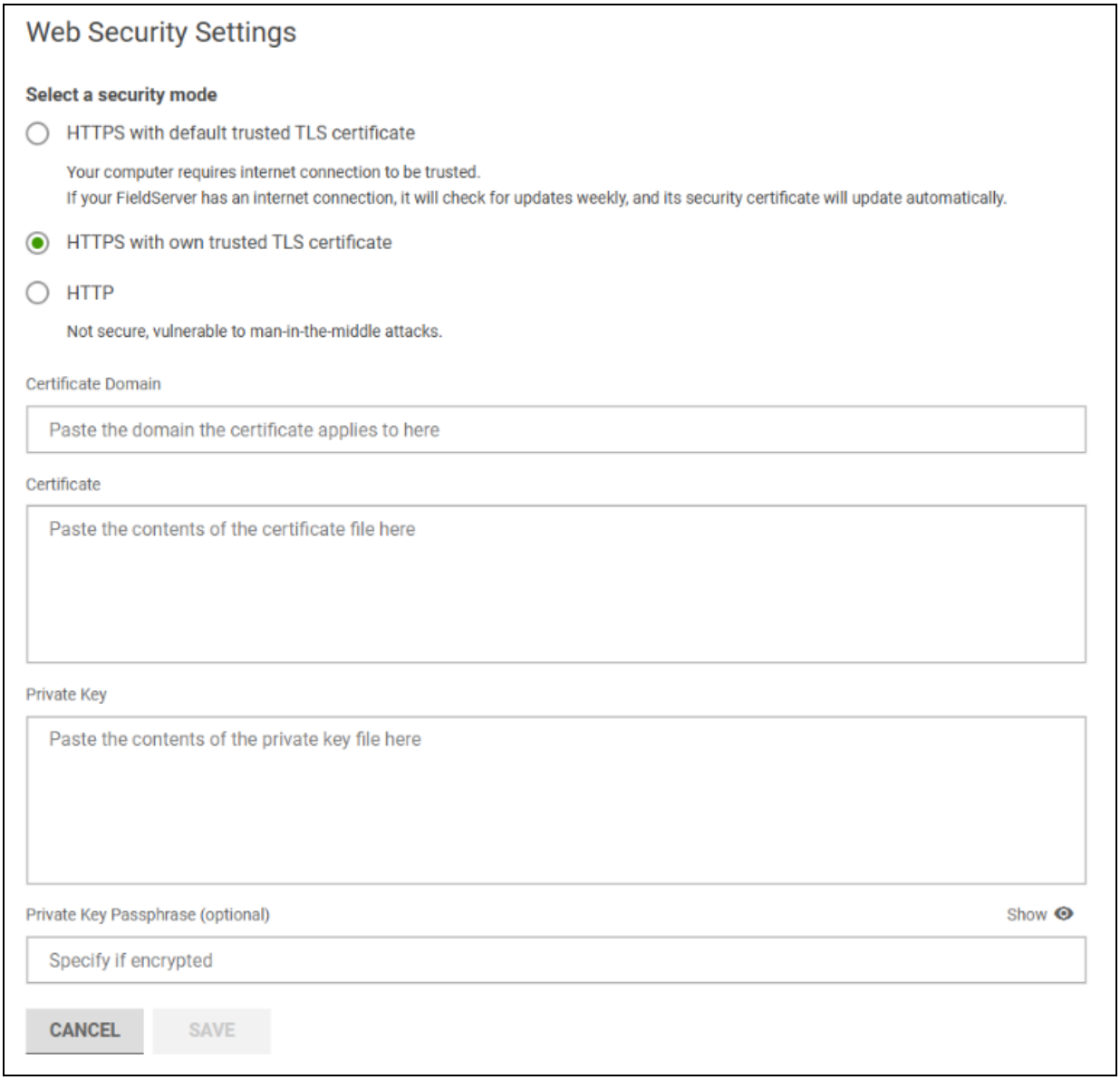


HTTP – Provides no encryption on the wire and is vulnerable to man-in-the-middle attacks.

HTTPS with own trusted TLS certificate – Requires the user to generate and sign their own certificate. This requires the user to also have a domain specifically for this device.

HTTP with default trusted TLS certificate – Provides a trusted connection with a certificate provided by MSA. This certificate renews every year and auto-updates on the device if it is connected to the internet. To use the secure connection, go to 192-168-2-101.gw.fieldpop.io. The first subdomain is the IP Address of the device delimited with dashes instead of dots.

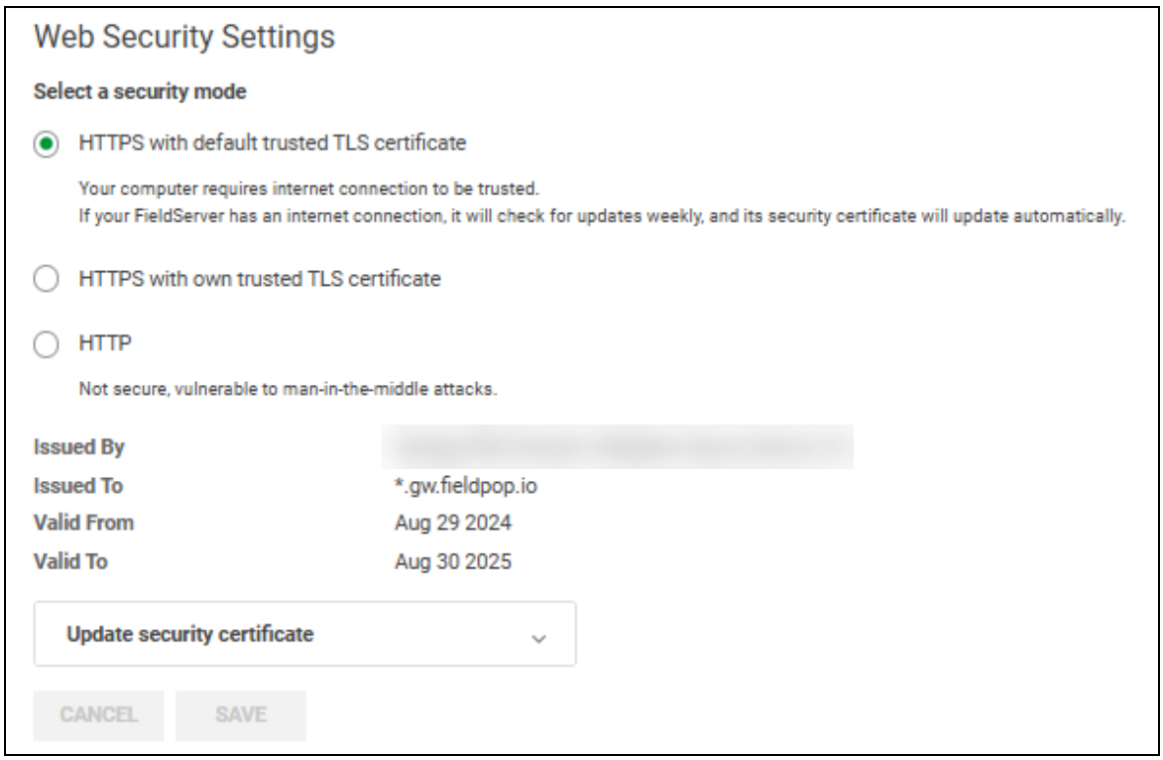
2. If selecting HTTPS with own trusted TLS certificate, paste the certificate contents, the private key, and the protective passphrase in the specified fields. It is also required to enter the chosen and configured domain for the FieldServer. Navigating to the domain will then ensure a trusted connection.



17.2.1 Updating a TLS Certificate

Security Certificates are valid for 1 year.

- If the Modbus IoT Gateway is connected to the internet the certificate will update automatically.
- If your PC has internet access, but the Modbus IoT Gateway does not, you can manually update the security certificate.
    1. Click on the arrow next to Update Security Certificate. There is a link to download the latest certificate.



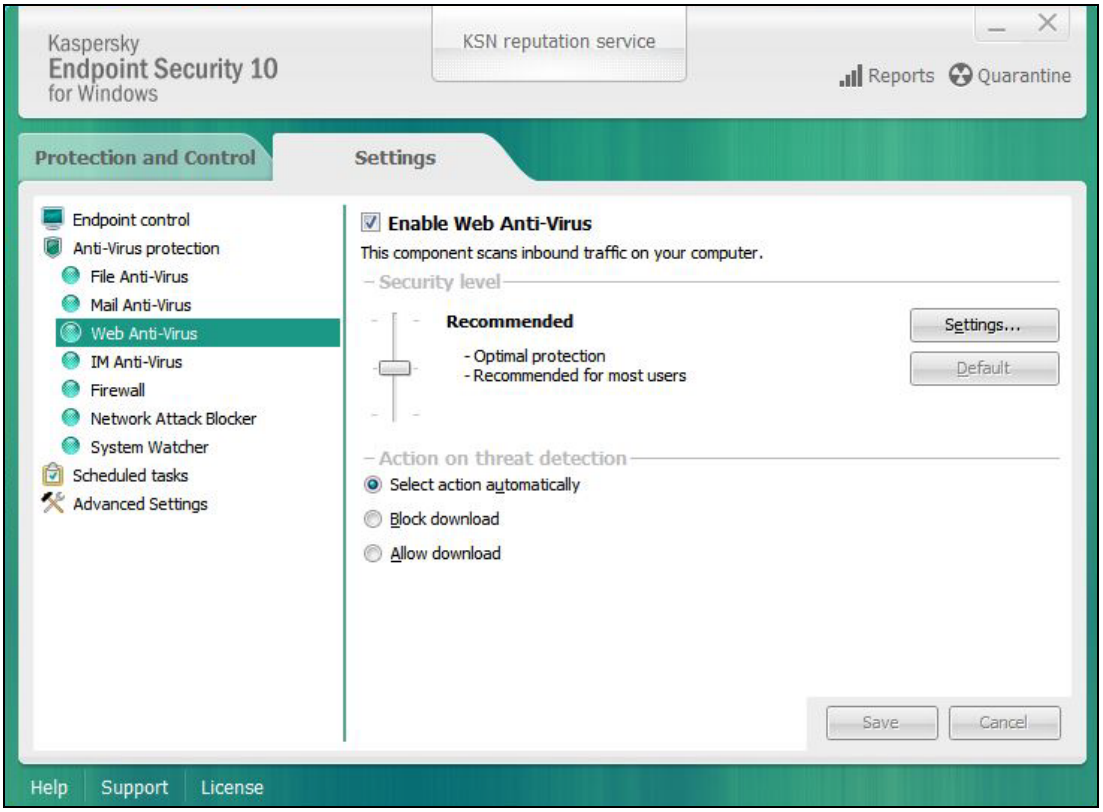
2. Click Browse Files to import the certificate.

17.3 Kaspersky Endpoint Security 10

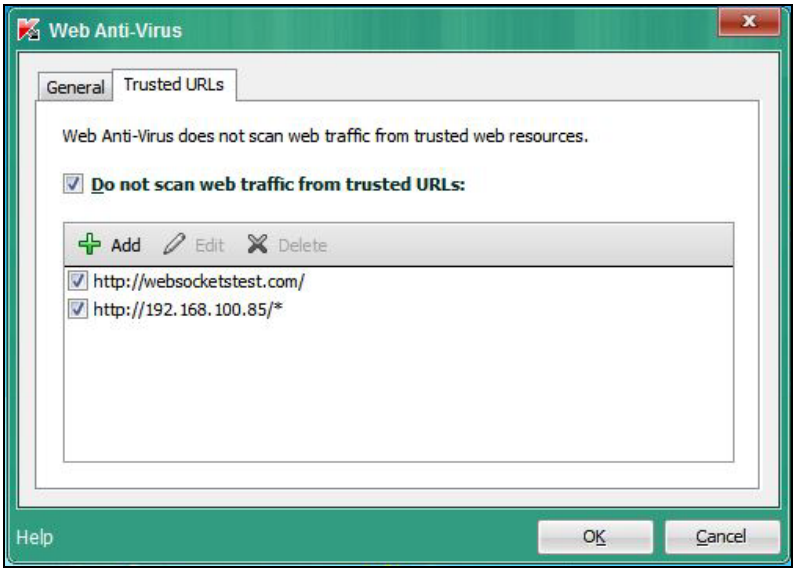
If Kaspersky Endpoint Security 10 is installed on the user's PC, the software needs to be modified to allow the PC to register bridges on the FieldServer Manager.

NOTE: This problem is specific to KES10. Kaspersky 2017 does not have this problem.

1. Open Kapersky Endpoint Security 10.
2. Go to Web Anti-Virus, then click the Settings button.



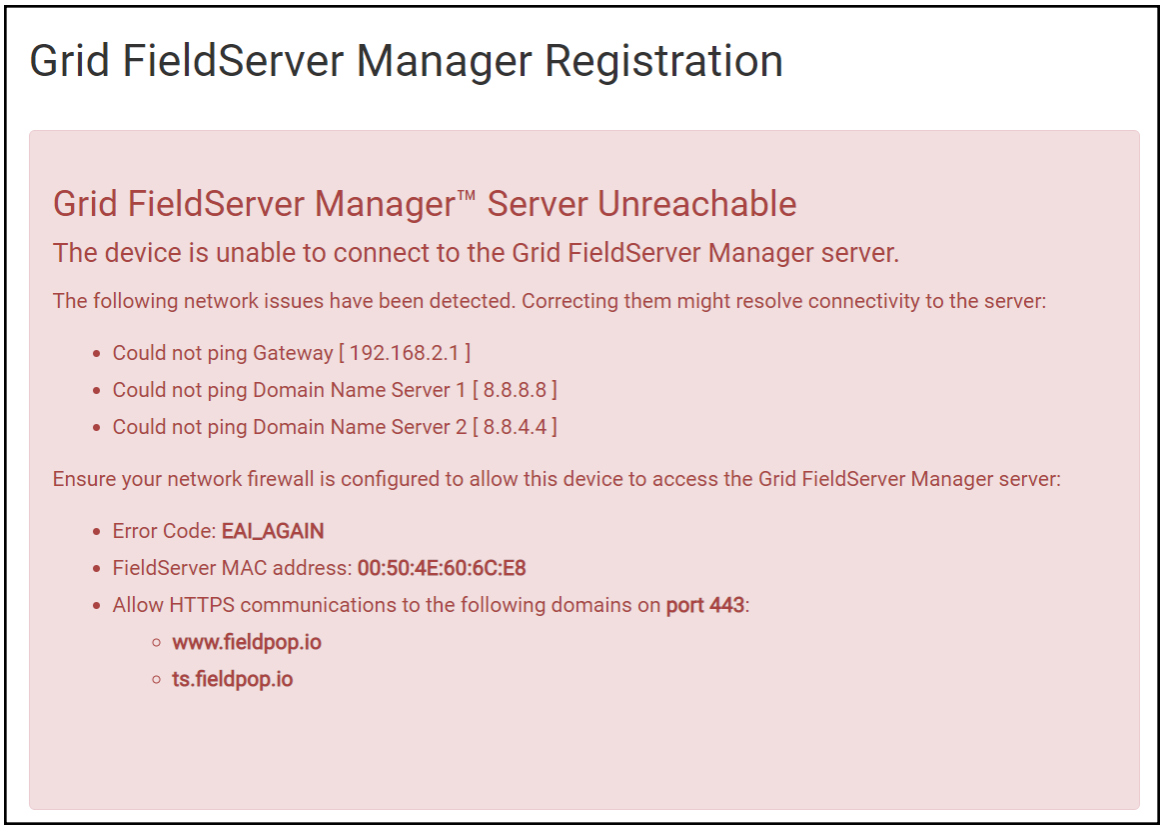
3. Set the Modbus IoT Gateway (see http://192.168.100.85/* in the image below) as a trusted URL.



17.4 FieldServer Manager Connection Warning Message

If a warning message appears instead of the page as shown below, follow the suggestion that appears on screen.

If the Modbus IoT Gateway cannot reach the server, the following message will appear



Follow the directions presented in the warning message.

1. Go to the network settings by clicking the Settings tab, then click the Network tab.
2. Check with the site's IT support that the DNS settings are setup correctly.
3. Ensure that the Modbus IoT Gateway is properly connected to the Internet.
4. Click the Save button.
5. Power cycle the Modbus IoT Gateway by clicking on the Confirm button, then click the bold Restart text in the yellow pop-up box that appears in the upper right corner of the screen.

17.5 Warnings for FCC and IC

Waste Disposal

⚠ WARNING!

- Products or product packages with the sign of “explosive” should not be disposed like household waste but delivered to specialized electrical & electronic waste recycling/disposal center. Proper disposal of this sort of waste helps avoiding harm and adverse effect upon surroundings and people’s health.

Failure to follow these warnings can result in serious personal injury or death.

Comply with the following safety tips:

⚠ WARNING!

- **Read and understand all Cautions and Warnings. Cautions and Warnings in this manual notify users of potential risks. These should be used in addition to complying with all safety requirements for your operation environment.**
- **Do not use near/keep away from a combustible and explosive environment.**
- Keep away from all energized circuits.
- Operators should not remove enclosure from the device. Only the group or person with factory certification is permitted to open the enclosure to adjust and replace the structure and components of the device.
- Do not change components unless the power cord is removed. In some cases, the device may still have residual voltage even if the power cord is removed. Therefore, it is a must to remove and fully discharge the device before contact so as to avoid injury.
- **Unauthorized changes to this product or its components are prohibited.**
- With the aim of avoiding accidents, it is not allowed to replace the system or change components unless with permission and certification. Please contact MSA Support for help.

Failure to follow these warnings can result in serious personal injury or death.

Notice

Considering that reasonable efforts have been made to assure accuracy of this manual, MSA Safety assumes no responsibility of possible missing contents and information, errors in contents, citations, examples, and source programs.

MSA Safety reserves the right to make necessary changes to this manual without prior notice. No part of this manual may be reprinted or publicly released.

FCC Warning (-MODW, -MODA, -MODV, -MOD2)

⚠ WARNING!

- Any modification to the product is not permitted unless authorized by MSA Safety. It's not allowed to disassemble the product; it is not allowed to replace the system or change components unless with permission and certification. Modification could void the user's authority to operate the equipment. Contact the FieldServer technical support department or local branches for help.

Failure to follow this warning can result in serious personal injury or death.

This device complies with FCC Rules. Operation is subject to the following conditions.

This device may not cause harmful interference.

This device must accept any interference received, including interference that may cause undesired operation.

This device complies with Part 15C of the FCC Rules.

For FS-IOT-MODA/V, this device complies with Part 22H, Part 24E and Part 27 of the FCC Rules.

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

ISED Statement

This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's licence-exempt RSS(s). Operation is subject to the following two conditions:

- This device may not cause interference.
- This device must accept any interference, including interference that may cause undesired operation of the device.

This class B digital apparatus complies with Canadian ICES-003.

Industry Canada ICES-003 Compliance Label:

CAN ICES-3 (B)/NMB-3(B)

L'émetteur/récepteur exempt de licence contenu dans le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence.

L'exploitation est autorisée aux deux conditions suivantes:

- l'appareil ne doit pas produire de brouillage.
- l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

FCC RF Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20cm between the radiator and any part of your body.

This equipment complies with IC RSS-102 radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20cm between the radiator and any part of your body.

Pour se conformer aux exigences de conformité CNR 102 RF exposition, une distance de séparation d'au moins 20 cm doit être maintenue entre l'antenne de cet appareil ettoutes les personnes.

FCC Supplier's Declaration of Conformity

M2M Gateway/ FPA-W44
This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

MSA Innovation, LLC
1100 Cranberry Woods Drive, Cranberry Township, PA 16066
Tel: 724-776-8600

Power Output

⚠ WARNING!

- The device should be professionally installed to ensure compliance with power requirements. A trained/certified electrician is not needed, but someone knowledgeable with electrical components is required to power up the unit, so that it isn't damaged.
- The antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and not be co-located with any other transmitters except in accordance with multi-transmitter product procedures.

Failure to follow these warnings can result in serious personal injury or death.

Frequency Range Output Power:

Wi-Fi *(-MODW, -MODA, -MODV, -MODF only)*

2402.0 – 2480 MHz 0.004 W

2412.0 – 2462.0 MHz 0.0258 W

LTE *(-MODA, -MODV, -MODF only)*

Supported Bands:

FS-IOT-MODA/V – B2, B4, B5, B12, B13 & B17 (0.25 W)

FS-IOT-MODF – B1, B3, B7, B8, B20 (0.25 W)

The Output Power listed is conducted. This device supports 20MHz and 40MHz bandwidth.

This radio transmitter [IC: 324C-FPAW44] has been approved by Innovation, Science and Economic Development Canada to operate with the antenna types listed below, with the maximum permissible gain indicated. Antenna types not included in this list that have a gain greater than the maximum gain indicated for any type listed are strictly prohibited for use with this device. The concrete contents to check are the following three points:

1. Antenna type is a Dipole with no more than 2dBi gain at 2.4G and -0.4 dBi gain at 5G.
2. Should be installed so that the end user cannot modify the antenna.
3. Feed line should be designed in 50ohm Fine-tuning of return loss etc.

A matching network can be used.

Le présent émetteur radio [IC: 324C-FPAW44] a été approuvé par Innovation, Sciences et Développement économique Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal. Les types d'antenne non inclus dans cette liste, et dont le gain est supérieur au gain maximal indiqué pour tout type figurant sur la liste, sont strictement interdits pour l'exploitation de l'émetteur. Le contenu concret à vérifier sont les trois points suivants.

1. Le type d'antenne est un Dipole avec pas plus de 2 dBi gain à 2.4G -0.4 dBi gain à 5G.
2. Doivent être installés de façon que l'utilisateur final ne peut pas modifier l'antenne.
3. La ligne d'alimentation doit être conçue en 50ohm Le réglage précis de la perte de rendement, etc.

peut être effectué en utilisant un réseau correspondant.

Frequency (MHz)	Antenna Type	Max Antenna Gain
2402-2480	Linear vertical Omnidirectional	2
2412-2462	Linear vertical Omnidirectional	2

18 Limited 2 Year Warranty

MSA warrants the product furnished, except software or software components, to be free from defects in workmanship or materials for a period of two (2) years after date of shipment, provided such product is installed, maintained, and used in accordance with MSA's instructions and/or recommendations. It is expressly agreed that the product user's sole and exclusive remedy for breach of the above warranty, for any tortious conduct of MSA or for any other cause of action, will be the repair or replacement, at MSA's option, of any equipment that after examination by MSA is shown to be defective in either workmanship or materials during the warranty period. Final determination of the nature and responsibility for defective or damaged equipment will be made by MSA personnel. Replacement equipment and/or components will be provided at no cost to Purchaser, F.O.B. MSA's plant. Failure of MSA to successfully replace any nonconforming equipment or components shall not cause the remedy established hereby to fail of its essential purpose. In all cases MSA's responsibility and liability under this warranty shall be limited to the cost of the equipment. The purchaser must obtain shipping instructions for the prepaid return of any item under this warranty provision and compliance with such instruction shall be a condition of this warranty.

This warranty is contingent upon proper use in the application for which the product was intended and does not cover products (including, without limitation, any software components) which have been modified or repaired by persons other than its own or authorized service personnel or without MSA's prior written approval, or on which original identification marks have been removed or altered. MSA shall be released from all obligations hereunder in the event a warranty claim results from normal wear and tear, product physical abuse, accident, alteration, misuse, or neglect. This Limited Warranty also will not apply to interconnecting cables or wires, consumables or to any damage resulting from battery leakage.

No agent, employee or representative of MSA may bind MSA to any affirmation, representation, or modification of the warranty concerning any product sold by MSA. This warranty constitutes the sole and entire warranty, and any change or modification hereto must be in writing and signed by the parties. MSA does not guarantee accuracy or completeness of its technical information, specifications, literature, and other printed materials, and reserves the right to change such information without notice to Purchaser.

EXCEPT FOR THE EXPRESS LIMITED WARRANTY STATED ABOVE, MSA EXPRESSLY DISCLAIMS ALL OTHER WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, WITH REGARD TO THE PRODUCT INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOFTWARE IS PROVIDED "AS IS" AND WITH ALL FAULTS, AND MSA MAKES NO WARRANTY WITH RESPECT TO SOFTWARE OR ANY SOFTWARE COMPONENT OF THE PRODUCT, WHETHER SOLD OR LICENSED (INCLUDING WITHOUT LIMITATION ANY CLICKWRAP LICENSE AGREEMENT), INCLUDING WHETHER SUCH SOFTWARE WILL OPERATE IN CONJUNCTION WITH ANY OTHER SOFTWARE OR WITH ANY EQUIPMENT OTHER THAN THE PRODUCT, AND MSA MAKES NO WARRANTY THAT SUCH SOFTWARE OR SOFTWARE COMPONENTS OF THE PRODUCT WILL OPERATE ERROR-FREE OR FREE OF HARMFUL CODE. MSA MAKES NO WARRANTY, EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE, REGARDING ANY THIRD-PARTY PRODUCT, COMPONENT, OR ACCESSORY BUT WILL PASS ALONG ANY WARRANTY IT RECEIVES FROM A THIRD PARTY WHERE AVAILABLE. THIS WARRANTY RUNS EXCLUSIVELY TO PURCHASER AND NO OTHER PERSON (INCLUDING ANY CUSTOMER OF PURCHASER OR ANY END USER).

THE EXPRESS WARRANTIES STATED HEREIN ARE IN LIEU OF ANY AND ALL OBLIGATIONS OR LIABILITIES ON THE PART OF MSA FOR DAMAGES INCLUDING, BUT NOT LIMITED TO, ECONOMIC, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OR LOSSES OF ANY KIND WHATSOEVER IN ANY WAY ARISING OUT OF OR IN CONNECTION WITH THE SALE, USE OR PERFORMANCE OF THE PRODUCT, INCLUDING, BUT NOT LIMITED TO, LOSS OF ANTICIPATED PROFITS. THIS EXCLUSION IS APPLICABLE TO CLAIMS FOR BREACH OF WARRANTY, TORTIOUS CONDUCT OR ANY OTHER CAUSE OF ACTION AGAINST MSA.