UserGuide-W-GATE-ETH

User Guide

Ethernet Gateway

NOTICE

For best results, wait to power on your gateway until after you have registered an account on the sensor portal.

⚠ WARNING

THINK SAFETY FIRST

Read this Manual BEFORE using this equipment.

Failure to read and follow all safety and use information can result in death, serious personal injury, property damage, or damage to the equipment.

Keep this Manual for future reference.

WATTS®

Table of Contents

I. About the Gateway

The gateway allows wireless sensors to communicate with the Online Wireless Sensor Monitoring and Notification System or Sensor Portal without needing a PC. Simply provide power and plug the gateway into an open Ethernet port with an Internet connection. It will automatically connect with our online servers, providing the perfect solution for connected commercial locations.

The gateway is an advanced wireless Internet of Things (IoT) gateway that enables fast time-to-market solutions. It's specifically designed to respond to the increasing market need for global technology that accommodates various vertical IoT application segments and remote wireless sensor management solutions.

Gateway Features

- Wireless range of 1,200+ feet through 12+ walls*
- Frequency Hopping Spread Spectrum (FHSS)
- Improved interference immunity
- Encrypt-RF® Security (Diffie-Hellman Key Exchange + AES-128 CBC for sensor data messages)
- 30,000 sensor message memory**
- Over-the-air (OTA) updates (future proof)
- True plug and play, no hassles for Internet configuration setup
- No PC required for operation
- Low-cost cellular service packages***
- Local status LEDs with transmission and online status indicators
- AC power supply

* Actual range may vary depending on environment

** Total messages in memory varies with sensor type (30K total messages for Temperature)

*** When paired with a data plan

Example Applications

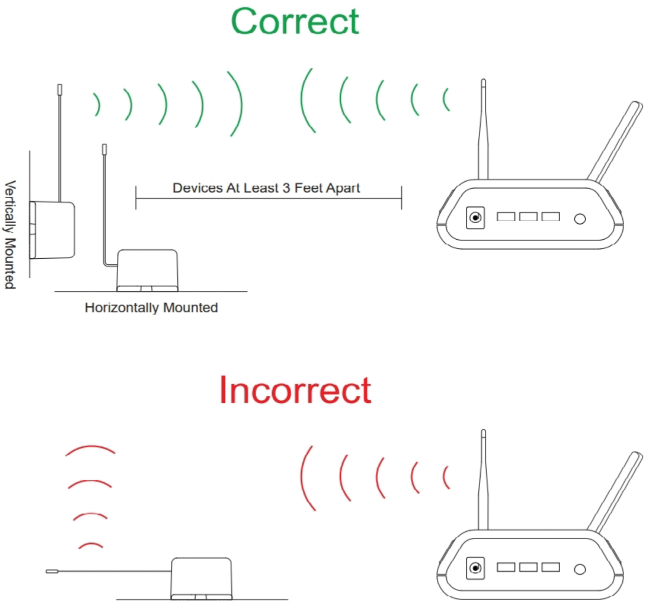
- Remote Location Monitoring
- Facility Management
- Shipping and Transportation
- Agricultural Monitoring
- Vacant Property Management
- Vacation Home Property Management
- Construction Site Monitoring
- Data Center Monitoring

II. How Your Gateway Works

Your Ethernet gateway manages communication between your sensors and the sensor portal. When running, the gateway will periodically transmit data on a heartbeat. The gateway will store information received from sensors until its next heartbeat.

Your gateway uses an Ethernet connection to relay data received from sensors to the sensor portal. Sensors communicate with the gateway. Then the gateway relays information to the cloud.

For your wireless sensors to work optimally, orient all antennas for your sensor(s) and gateway(s) the same direction (typically vertical). Sensors must also be at least three feet away from other sensors and the wireless gateway in order to function properly.



Correct

Incorrect

Figure 1

III. Gateway Security

The gateway has been designed and built to securely manage data from sensors monitoring your environment and equipment. The same methods utilized by financial institutions to transmit data are also used in the sensor portal security infrastructure. Gateway security features include tamper-proof network interfaces, data encryption, and bank-grade security.

Our proprietary sensor protocol uses low transmit power and specialized radio equipment to transmit application data. Packet-level encryption and verification are key to ensuring traffic isn't altered between sensors and gateways. Paired with best-in-class range and power consumption protocol, all data is transmitted securely from your devices.

Sensor Communication Security

The sensor-to-gateway secure wireless tunnel is generated using ECDH-256 (Elliptic Curve Diffie-Hellman) public key exchange to generate a unique symmetric key between each pair of devices. Sensors and gateways use this link-specific key to process packet-level data with hardware-accelerated 128-bit AES encryption. This minimizes power consumption to optimize battery life. Thanks to this combination, we offer robust, bank-grade security at every level.

Data Security on the Gateway

The gateway is designed to prevent prying eyes from accessing the data that is stored on the sensors. It doesn't run on an off-the-shelf, multi-function operating system. Instead it runs on a purpose-specific, real-time embedded state machine that can't be hacked to run malicious processes. There are also no active interface listeners that can be used to gain access to the device over the network. The fortified gateway secures data from attackers and protects the gateway from becoming a relay for malicious programs.

Server Communication Security

Communication between your gateway and sensor portal is secured by packet -level encryption. Similar to the security between the sensors and gateway, the gateway and server also establish a unique key using ECDH-256 for encrypting data. The packet level data is encrypted end to end, removing additional requirements to configure specialized cellular VPNs. The gateway can still operate within a VPN if it is present.

IV. Gateway Registration

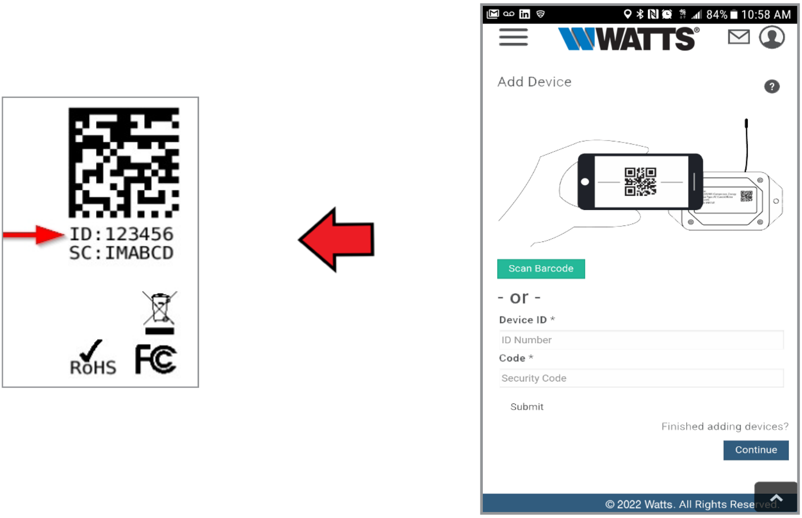
If this is your first time using the sensor portal, you will need to create a new account. If you have already created an account, start by logging in. To register for a new account, please go to https://monitor.watts.com.

Registering The Wireless Ethernet Gateway

You will need to enter the **Device ID** and the **Security Code (SC)** from your gateway in the corresponding text boxes. Use the camera on your smartphone to scan the QR code on your gateway. If you don't have a camera on your phone, or you are accessing the online portal through a desktop computer, you may enter the **Device ID** and **SC** manually. See Figure 2.

- The **Device ID** is a unique number located on each device label.
- Next you'll be asked to enter the **SC** on your device. The SC is all letters (no numbers). It can also be found on the barcode label of your gateway.

When completed, select the **Submit** button.



Add Device

Scan Barcode

- or -

Device ID *

ID Number

Code *

Security Code

Submit

Finished adding devices?

Continue

© 2022 Watts. All Rights Reserved.

Figure 2

IMPORTANT: Add the gateway and all sensors to the senor portal so that on boot, the gateway can download and whitelist the sensors from the account.

V. Using the Gateway

Using the Gateway

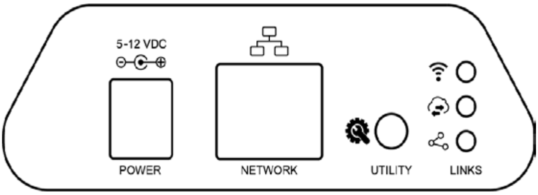


Figure 3

See Figure 3 above.

Power: Power cord connection location

Network: Ethernet connection location

Utility Button: During the boot sequence, a five-second press of this button will enable the local interface. When powered on, pressing the utility button for 10-15 seconds will reset the gateway. Pressing the button for 15+ seconds will clear all of the memory in addition to the factory reset.

1. Connect your antennas to the gateway.
2. Plug the power supply cord into an outlet.
3. After the three LED lights switch to green, your network is ready to use.

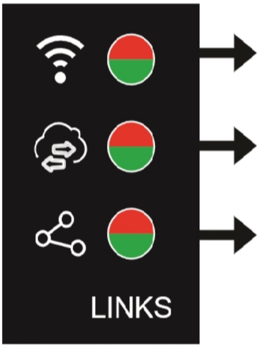
Understanding the Gateway Lights

The gateway will enter three stages as it powers on:

Power-on Stage: The gateway analyzes electronics and programming. The LED lights flash red and green before turning green for one second and entering a “waterfall” pattern. In case of failure, the light sequence repeats after 10 seconds. The gateway continues trying to boot until it succeeds. Please contact technical support if the lights aren’t green after two minutes.

Connection Stage: When the LEDs turn solid green for 1.5 seconds, the power-on step is complete. After the Network Uplink Connectivity LED displays a solid green LED, the gateway attempts to connect to its default server and other configured surfaces. The gateway attempts to settle all active connections. When the gateway first connects to the network, no other lights illuminate.

Operational Stage: All of the lights remain green while powered externally unless there is an issue. A blinking link light signals that the gateway encountered a network problem.



NETWORK UPLINK CONNECTIVITY LED
Steady Green: Communication with sensors is ok
Blinking Green: Active communication with sensors
Steady Red: Sensor communication problem

SERVER COMMUNICATION LED
Steady Green: Last communication with the server was ok
Blinking Green: Active communication with the server
Steady Red: Last communication with the server was unsuccessful

ETHERNET LINK LED
Steady Green: Internet connection successful
Steady Red: No Internet connection found

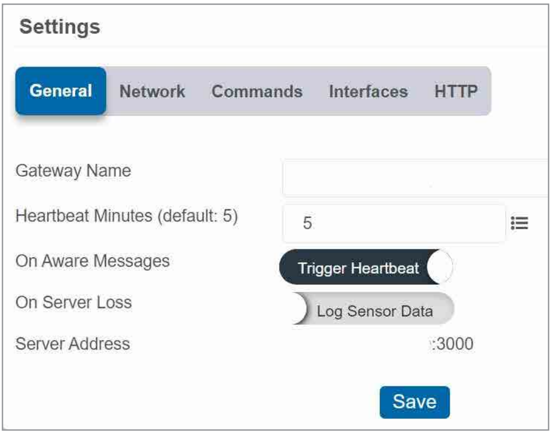
Figure 4

Gateway Settings

General

The gateway receives data from all sensors assigned to the network and within its range. It then returns this data to the server in a series of heartbeats.

You can access the gateway's settings by selecting **Gateways** in the main navigation panel. Choose the correct gateway from the list of gateways registered to your account. Select the **Settings** tab to edit the gateway:



Gateway Name

Heartbeat Minutes (default: 5) 5

On Aware Messages Trigger Heartbeat

On Server Loss Log Sensor Data

Server Address :3000

Figure 5

The **Gateway Name** field is where you assign your gateway a unique title. By default, the gateway name will be the type followed by the Device ID.

The **Heartbeat Minutes** configures the interval that the gateway checks in with the server. The default is five minutes. So every five minutes your gateway will report to the server.

When your sensors detect a threshold breach, they enter what is called an "aware state." The **On Aware Messages** toggle is set to "Trigger Heartbeat" by default. This means the gateway will check in with the server address immediately and relay the aware state information to the sensor portal.

Toggling this to "Wait for Heartbeat" will set the gateway to wait for its set heartbeat to elapse before communicating with the server.

The **On Server Loss** toggle switch sets what you wish to happen when the gateway loses communication with the server. The default setting "Log Sensor Data" commands the gateway to continue communicating with your sensors and store readings until it can re-establish a connection to the server.

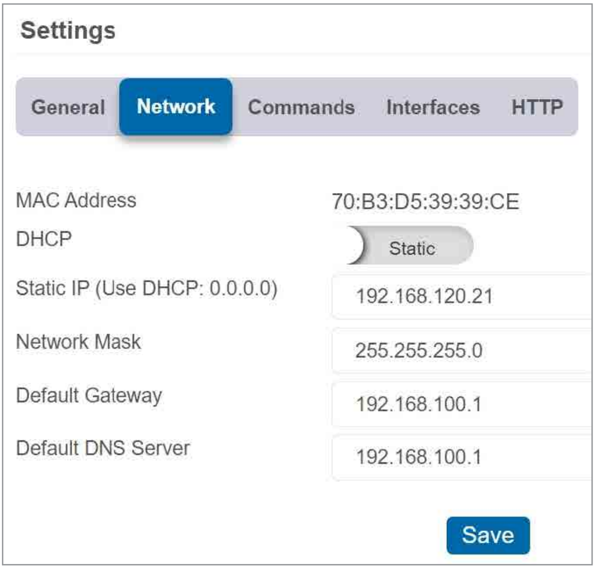
Toggling this to "Disable Wireless Network" will force the sensors communicating with this gateway to find a new gateway in order to deliver sensor messages to the server immediately.

Network

Choose the Local Area **Network** (LAN) tab under the Settings title to open up the LAN configuration page. The LAN includes the ability to switch your network Internet Protocol (IP) address from Dynamic Host Configuration Protocol (DHCP) to Static. DHCP will be the default network IP address.

Multiple interfaces can be active. If using any of the polling interfaces, we recommend using a Static IP address on the gateway. An IP address is a unique number typically formatted as XXX.XXX.XXX.XXX.

To change your IP address to a Static IP, navigate to the network IP option, and switch it from DHCP to Static. Then input your data for the **Static IP**, **Network Mask**, **Default Gateway**, and **Default DNS Server**. See Figure 6.



Settings

MAC Address 70:B3:D5:39:39:CE

DHCP Static

Static IP (Use DHCP: 0.0.0.0) 192.168.120.21

Network Mask 255.255.255.0

Default Gateway 192.168.100.1

Default DNS Server 192.168.100.1

Figure 6

Static IP - A Static IP address is a numerical sequence assigned to a computer by a network administrator. This is different from a Dynamic IP address in that a Static IP doesn't periodically change. It remains constant.

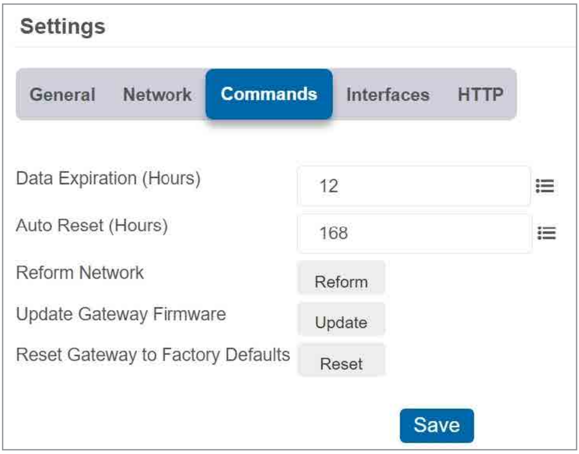
Network Mask - Also known as a "subnet mask," this number hides the network half of an IP address. The most common Network Mask number is 255.255.255.0.

Default Gateway - This is the forwarding host a computer utilizes to relay data to the Internet.

Default DNS Server - Domain Name System (DNS) Servers take alphanumerical data (like a URL address) and return the IP address for the server containing the information you're looking for.

Commands

Choose the **Commands** tab located just under the Settings title to access the commands page. See Figure 7.



Settings

Data Expiration (Hours): 12

Auto Reset (Hours): 168

Reform Network

Update Gateway Firmware

Reset Gateway to Factory Defaults

Figure 7

Data Expiration (Hours) - Manage data expiration time in the gateway. After this time has elapsed, the data pulled for the Modbus protocol and Simple Network Management Protocol (SNMP) will be zero-ed out.

The **Auto Reset** field is the amount of time in hours that the Local Interface will automatically reboot. Setting this to O will disable the feature. The maximum setting is 8760 hours.

Selecting the **Reform Network** command will trigger the gateway to remove all sensors from the internal whitelist, and then request a new sensor list from the server. This command will force all sensors to reinitialize their connection with the gateway.

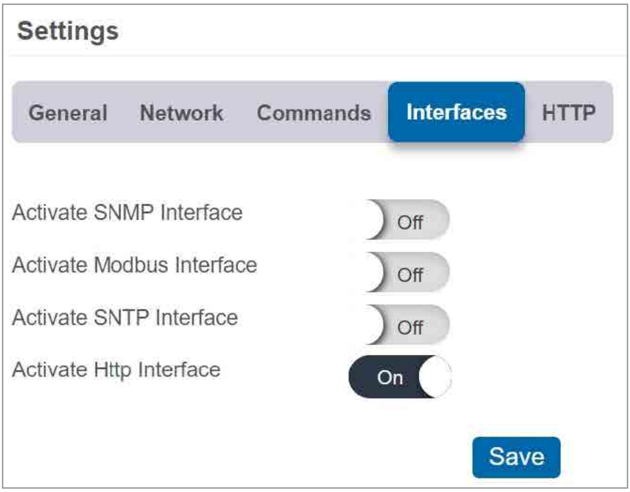
Reforming the network cleans up communication when multiple networks are in range of each other so they're all in sync. This is especially useful if you must move sensors to a new network, and would like to clear these sensors from the gateway's internal list. Reforming the network will place a new list of sensors that will continue to exchange data.

Picking the **Update Gateway Firmware** button signals the gateway to download and apply the latest firmware version available.

Choosing the **Reset Gateway to Factory Defaults** button will erase all of your unique settings and return the gateway to factory default settings.

Interface Activation

There are additional interfaces available for activation on your Gateway Settings page. To activate them, choose the **Interfaces** activation tab. Toggle on each of the interfaces to access their individual settings. See Figures 8 through 12.



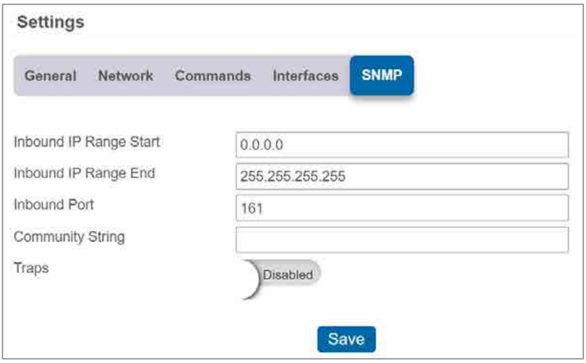
Activate SNMP Interface: Off

Activate Modbus Interface: Off

Activate SNTP Interface: Off

Activate Http Interface: On

Figure 8



Inbound IP Range Start: 0.0.0.0

Inbound IP Range End: 255.255.255.255

Inbound Port: 161

Community String:

Traps: Disabled

Figure 9

SNMP Interface - SNMP is an Internet application protocol that manages and monitors network device functionality. We use SNMP version 1. The settings can be configured both on the sensor portal and the local interface. See Figure 9.

Inbound IP Range Start and End - This is the accepted IP address range for the SNMP client. The gateway will only accept communication requests from IP addresses in this range.

Inbound Port - This is the number for where specifically in the server data from the gateway is received.

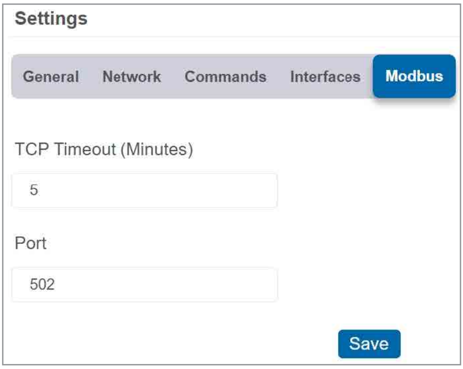
SNMP Community String - This is used as a configurable password for clients within the accepted IP Range. Communication will not be allowed if the Community String does not match. The default will be set to “public.”

Trap Settings - The switch for Trap Settings will be disabled by default. Enable to view the trap settings.

Trap IP Address - This is the IP Address for the SNMP Server where the trap will be sent.

Trap Port - The server port where the trap alert state is sent when active.

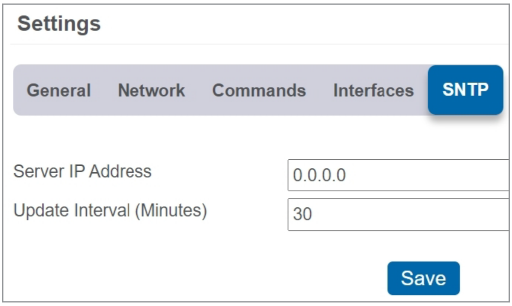
Modbus Interface - Modbus Transmission Control Protocol (TCP) is the Modbus remote terminal unit (RTU) protocol with a TCP interface that runs on Ethernet. We provide the Modbus TCP interface for you to pull gateway and sensor data. You can use Modbus without an active server interface. The data will not be sent to a server, but you can continue to poll for new data as it is received by the gateway. See Figure 10.


Settings

TCP Timeout (Minutes): 5

Port: 502

Figure 10


Settings

Server IP Address: 0.0.0.0

Update Interval (Minutes): 30

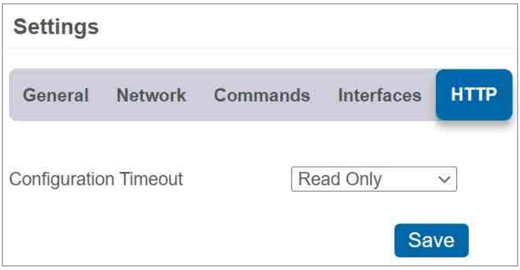
Figure 11

SNTP Interface - Simple Network Time Protocol (SNTP) is a synchronized computer clock on a network. An SNTP server can be set up on the same LAN as the gateway, such as on a router or a Linux computer. The gateway should be configured to retrieve time from only trusted servers, such as ones maintained by your ISP. Incorrect time can affect the delivery, of sensor traffic.

If the server is active, it will be utilized for time synchronization in ordinary operation. So SNTP will be used as a backup. If you disable the default server interface, you must configure the SNTP Interface. See Figure 11.

HTTP Interface - The Hypertext Transfer Protocol (HTTP) Interface allows you to set how long the local interface is active before being automatically disabled. You may configure the local HTTP interface to remain Read Only, or to be disabled after one minute, five minutes, 30 minutes, or always active.

See Figure 12.


Settings

Configuration Timeout: Read Only

Figure 12

VII. Using the Local Interface

If using the sensor portal is not an option, you can set up your gateway and sensors offline through the local interface.

- Connect the gateway's Ethernet cable to your computer directly.
- Plug in the gateway to a power outlet.
- Press and hold the utility button while the gateway is booting and the lights are scrolling. At the end of the boot process, all of the lights turn green for two seconds then shift to red. Release the button and the local web interface will be temporarily write-enabled (indicated by the lights flashing green quickly.
- After 30 seconds, the gateway's lights will all blink red rapidly. This means the gateway is in AUTO IP mode if DHCP is enabled. After an additional 30 seconds, the computer will also be in this networking mode (no Internet).
- Using a web browser type in the IP address currently assigned to the gateway. When the gateway is in AUTO IP mode, the IP address is always 169.254.100.1. The browser should then load the status page for this gateway.

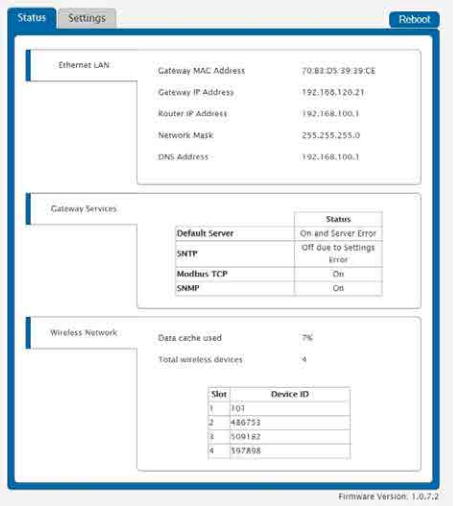
NOTICE

- When the gateway is connected to a router or other Internet access point, the local interface is reachable through the DHCP-assigned IP address, or the configured Static IP address.
- Each time a page is refreshed, the temporary timer to access these pages with configuration authorized will reset.
- If the interface is not used for five minutes or the gateway restarts, the HTTP interface will become read-only.

Status Tab

Ethernet LAN (Local Area Network Status)

This is a read-only section listing the current conditions for your LAN. See Figure 13.



Ethernet LAN

Gateway MAC Address 70:83:D5:39:39:CE

Geteway IP Address 192.168.120.21

Router IP Address 192.168.100.1

Network Mask 255.255.255.0

DNS Address 192.168.100.1

Gateway Services

	Status
Default Server	On and Server Error
SNTP	Off due to Settings Error
Modbus TCP	On
SNMP	On

Wireless Network

Data cache used 7%

Total wireless devices 4

Slot	Device ID
1	101
2	486753
3	509182
4	597898

Firmware Version: 1.0.7.2

Figure 13

Gateway MAC Address- This is the media access control (MAC) address of your gateway to exclusively identify the device to a Network Interface Controller.

Gateway IP Address - This is a network address for your gateway when it's connected to the Internet.

Router IP Address - This is a network address for your router when it's connected to the Internet.

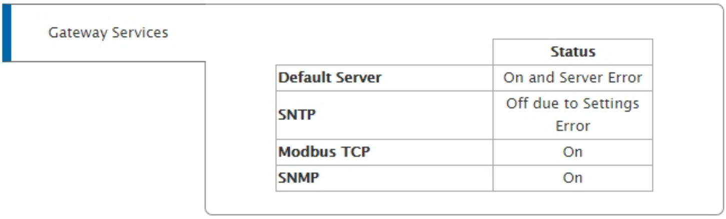
Network Mask - Also known as a "Subnet Mask," this masks the IP address by dividing it into the network address and the host address.

DNS Address - A DNS is the method employed by a URL of translating the alphabetic entry in an address bar into a numerical address associated with a server.

Gateway Services

See Figure 14.

Gateway Services Table - These status fields indicate the current operation status for each data interface. The status field will indicate when the appropriate service is “On,” “On and Server Error,” “On and Synced,” “On and Traps Ready,” “Off,” “Off due to Settings Error.”



Gateway Services

	Status
Default Server	On and Server Error
SNTP	Off due to Settings Error
Modbus TCP	On
SNMP	On

Figure 14

Wireless Network Status

Gateway data cache used - This percentage represents the amount of internal flash memory storage for holding sensor messages that has been used out of the maximum (896 kB). Messages sent from wireless sensors are stored temporarily in the gateway cache until a data interface, such as Default Server, SNMP, Modbus, confirms the data has been stored or transmitted elsewhere.

Total Wireless Devices - Below the gateway data cache is a section listing the number of sensors communicating with the gateway. A table below this number shows the exact slot number and device identification number associated with the gateway. There is a maximum of 256 available slots.

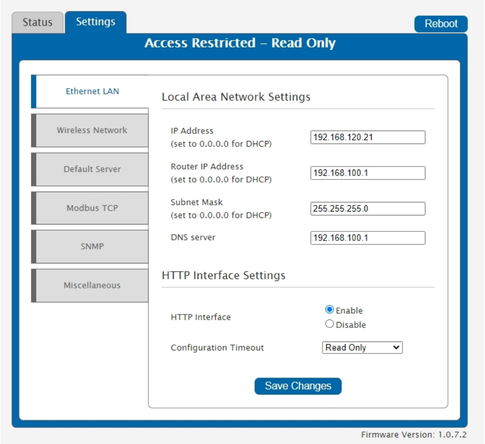
Settings Tab

See Figure 15.

From the Local Area Network Configuration tab, you can modify settings for your IP address, Network Mask, Default Gateway, and DNS Server.

Local Area Network Settings

In this section, you can edit LAN settings discussed on page 13.



Access Restricted – Read Only

Local Area Network Settings

IP Address (set to 0.0.0.0 for DHCP): 192.168.120.21

Router IP Address (set to 0.0.0.0 for DHCP): 192.168.100.1

Subnet Mask (set to 0.0.0.0 for DHCP): 255.255.255.0

DNS server: 192.168.100.1

HTTP Interface Settings

HTTP Interface: ● Enable ○ Disable

Configuration Timeout: Read Only

Firmware Version: 1.0.7.2

Figure 15

HTTP Interface Settings

HTTP Interface: The “Enable” radio button is active by default, allowing you to access the local interface. Choosing the “Disable” radio button and saving your changes will automatically log you out of the local interface. Follow the steps on page 14 to log back in.

Configuration Timeout: This allows you to set a time limit of one minute, five minutes, and 30 minutes for how long the local interface is active. “Read Only” keeps the interface active, but you can’t make any changes. You can only change the settings out of “Read Only” through the HTTP Interface on the sensor portal; see page 12. “Always Available” makes the interface always open and editable.

Wireless Network

See Figure 16.

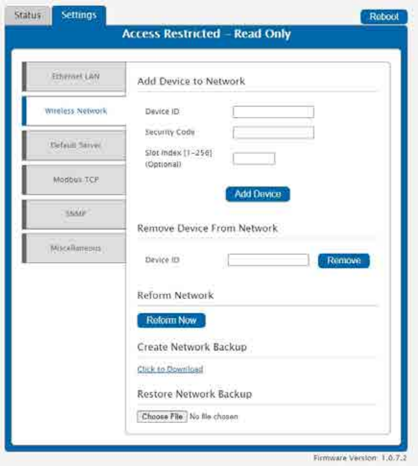


Figure 16

Add Device to Network

This section will allow you to add sensors and gateways to your account through the local interface.

Device ID - This is a unique numerical identifier included with your gateway and sensors listed on the back label.

Security Code - This is an alphabetical six letter code included with your gateway listed on the back label.

Slot Index - The slot index is an optional setting for assigning your gateway. If a Slot ID is entered, the device will be added to the appropriate slot in the Wireless Device List. If a Slot ID is not entered, the device will be 1 added to the first available slot.

Remove Device from Network

This section will allow you to remove a sensor or gateway from your account by typing in the numerical Device ID and selecting the Remove button.

Reform Network

Select the Reform Now button to remove all devices from the Wireless Device List.

Create Network Backup

Choose the “Click to Download” link to download a network backup for your gateway and sensors contained within an XML file.

Restore Network Backup

Choose a previously downloaded XML network backup file to load through the Local Interface.

Default Server

See Figure 17.

Default Server Settings

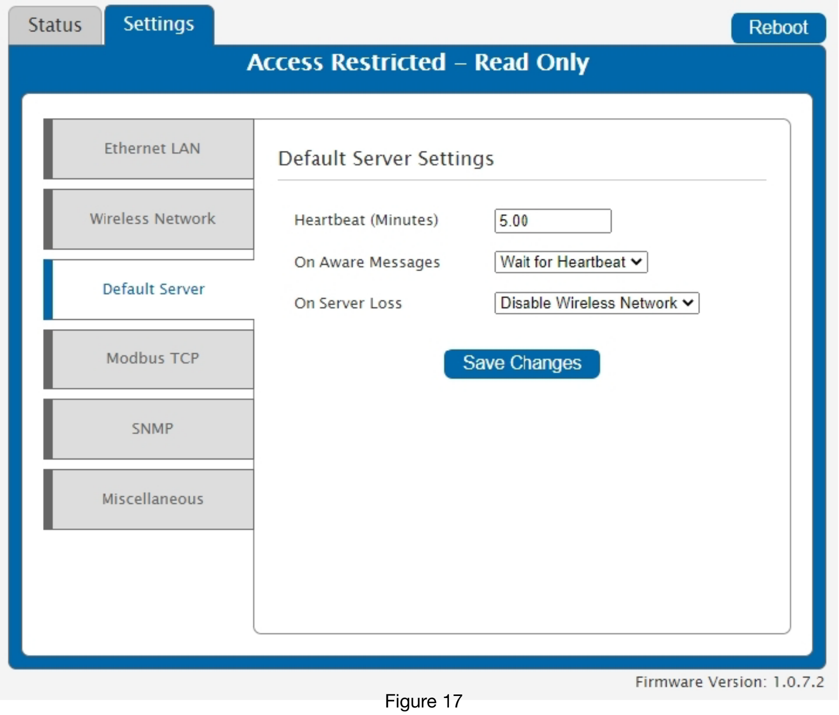
This is the default server. It is the only option enabled by default.

The **Heartbeat Minutes** configures the interval that the gateway checks in with the server. The default is five minutes. So every five minutes your gateway will report to the server.

When your sensors detect a threshold breach, they enter what is called an “aware state.” The **On Aware Messages** toggle is set to “Trigger Heartbeat” by default. This means the gateway will check in with the server address immediately and relay the aware state information to the sensor portal.

Leaving this set to the default “Wait for Heartbeat” setting will tell the gateway to wait for its set heartbeat to elapse before communicating with the server.

The **On Server Loss** field sets what happens when the gateway loses communication with the server. The default setting “Log Sensor Data” commands the gateway to continue communicating with your sensors and store readings until it can re-establish a connection to the server. Toggling this to “Disable Wireless Network” will force the sensors to find a new gateway to deliver sensor messages to the server immediately.



Default Server Settings

Heartbeat (Minutes) 5.00

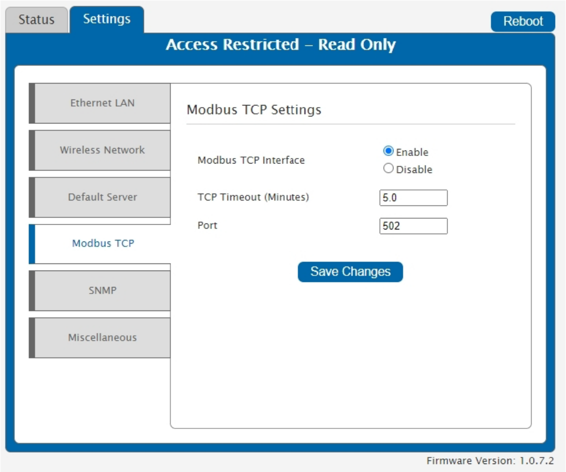
On Aware Messages Wait for Heartbeat

On Server Loss Disable Wireless Network

Figure 17

Modbus TCP (Transmission Control Protocol)

See Figure 18.



Access Restricted – Read Only

Modbus TCP Settings

Modbus TCP Interface ● Enable ○ Disable

TCP Timeout (Minutes) 5.0

Port 502

Firmware Version: 1.0.7.2

Figure 18

Modbus TCP Settings

Modbus TCP interface runs on an Ethernet connection. The TCP makes sure all data is received. Modbus TCP is a non-streaming data interface standard. This means data must be requested in order for it to be received. Additionally, only the current data points are available for reading. Historical sensor information is not available. See Figure 18.

The Modbus TCP Interface will store all data values in 16-bit registers. The registers and their associated data fields are mapped below. To access the sensor holding registers for a particular device, the assigned slot number for the device needs to be known. When reviewing added devices through the default server, the order in which devices are presented may not necessarily correspond to the order in which the devices are stored in the gateway network list as the default server will sort the devices based on their ID. To be certain which device is in a particular slot, go to the gateway local web interface status.htm page and note the device’s assigned slot.

After the slot number(s) for the desired devices to read from are known, the following formula may be applied to determine the correct starting register to read from to retrieve the recorded data from the device:

DATA ADDRESS:

Sensors information starts at 100 + 16 (Slot Number - 1)

REGISTER ADDRESS:

Sensors information starts at 40101 + 16 (Slot Number - 1)

Slot Number	Data Address	Register Address
1	100	40101
2	116	40117
256	4180	44181

Gateway Holding Registers

Field	Description	Register	Data Address
Gateway ID_High	The first 16 bits of a 32-bit serial ID number	40001	0
Gateway ID_Low	The last 16 bits of a 32-bit serial ID number	40002	1
Gateway Version Revision + Major	The gateway firmware Revision and Major version numbers (1 byte each)	40003	2
Gateway Version Minor + Release	The gateway firmware Minor and Release version numbers (1 byte each)	40004	3
Gateway Device Count	The number of devices in its wireless network	40005	4

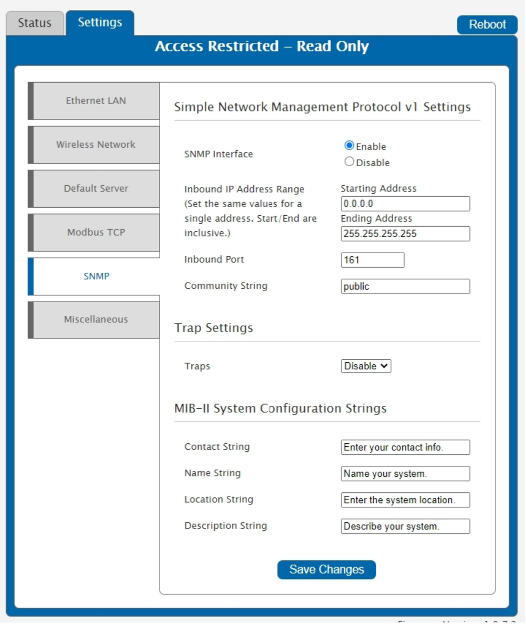
Sensor Holding Registers (Slot 1)

Field	Description	Register	Data Address
Sensor ID_High	The first 16 bits of a 32-bit serial ID number	40101	100
Sensor ID_Low	The last 16 bits of a 32-bit serial ID number	40102	101
Device Type	The unique type identifier for the sensor profile	40103	102
Data Age	The number of seconds that have elapsed since the last data was retrieved	40104	103
Is Device Active	0 indicates no data for this slot	40105	104
Is Aware	Becomes aware when a sensor threshold has been breached	40106	105
Voltage	Battery voltage	40107	106
RSSI	Signal Strength Indicator...0-100%	40108	107
Data 1	Sensor Data Field 1	40109	108
Data 2	Sensor Data Field 2	40110	109
Data 3	Sensor Data Field 3	40111	110
Data 4	Sensor Data Field 4	40112	111
Data 5	Sensor Data Field 5	40113	112
Data 6	Sensor Data Field 6	40114	113
Data 7	Sensor Data Field 7	40115	114
Data 8	Sensor Data Field 8	40116	115

The data listed in the registers above will be in raw format and will need to be converted into usable information.

SNMP

See Figure 19.



Simple Network Management Protocol v1 Settings

SNMP Interface: ● Enable ○ Disable

Inbound IP Address Range (Set the same values for a single address. Start/End are inclusive.)
Starting Address: 0.0.0.0
Ending Address: 255.255.255.255

Inbound Port: 161

Community String: public

Trap Settings

Traps: Disable

MIB-II System Configuration Strings

Contact String: Enter your contact info.

Name String: Name your system.

Location String: Enter the system location.

Description String: Describe your system.

Figure 19

The SNMP version 1 settings for a gateway can be adjusted on the offline local interface. You can continue to use SNMP without the server interface active. The data will not be sent to a server, but you can continue to poll for the data as it is received by the gateway. See Figures 19 and 20.

- **Inbound IP Range Start and End** - This is the IP address for the SNMP client. If you communicate with one device, the starting and ending IP addresses will be the same. Exchanging information with multiple machines will require a set of different starting and ending IP addresses.
- **Inbound Port** - This is the number for where specifically in the server data from the gateway is received.
- **SNMP Community String** - This is used as a configurable password for clients within the accepted IP Range. Communication will not be allowed if the Community String does not match. The default will be set to “public.”

Trap Settings

You have the option to “Enable” or “Disable” your trap settings. Choose “Enable” to bring up selections for **on Authentication Failure**, **on New Sensor Data**, and **on Sensor Alarms**. Your **Trap Address** is the IP Address for the SNMP Server where the trap will be sent. Your **Trap Port** is the server port where the trap alert state is sent when active.

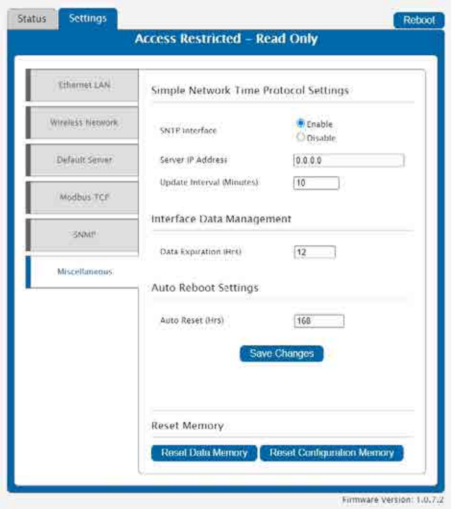
MIB-II System Configuration Strings

Although it’s not necessary, it’s a good idea to set the contact, name, location, and description strings available at the bottom of the SNMP configuration page on the local interface.

Miscellaneous System

See Figure 20.

SNTP Settings



Simple Network Time Protocol Settings

SNTP Interface ● Enable ○ Disable

Server IP Address 0.0.0.0

Update Interval (Minutes) 10

Interface Data Management

Data Expiration (Hrs) 12

Auto Reboot Settings

Auto Reset (Hrs) 168

Reset Memory

Firmware Version: 1.0.7.2

Figure 20

SNTP synchronizes computer clocks on a network when the sensor portal interface is unavailable.

Enable / Disable: You have the option to enable or disable the SNTP Interface. Disabling the SNTP will cause your time settings to be synchronized through the sensor portal.

SNTP IP Address: This is the IP Address for the server from which the time is pulled.

Interface Data Management

Data Expiration (Hours) - Manage data expiration in the gateway. After this time has elapsed, the data pulled for Modbus and SNMP will be zero-ed out.

Auto Reboot Settings

The **Auto Reset** field is the amount of time in hours that the Local Interface will automatically reboot. Setting this to 0 will disable the feature. The maximum setting is 8760 hours.

Reset Memory

Reset Data Memory button: Press this to wipe stored sensor readings from the gateway. All the changes you made to your settings remain intact.

Reset Configuration Memory button: Press this to reboot all your settings back to the factory defaults.

Troubleshooting

LED Indicators

Ethernet Cable Not Detected - The Bottom LED will blink Red twice rapidly to indicate the Ethernet Cable is not being detected. Double check the Ethernet connection or change the Ethernet Cable if the problem continues.

*Note - If the Ethernet Cable is not detected, the Middle LED on the gateway will turn Solid Red. This indicates the gateway is not able to communicate with the Default Server, or other configured services.

Gateway Services - Problems with any of the gateway services will be indicated by the Middle LED being Solid Red. This includes HTTP, NTP, Modbus TCP, SNMP, and the Default Server. To see which service is encountering the error use the Local Interface.

When ALL of these services have been configured OFF, the Middle LED will be OFF. If this occurs, a Factory Reset will recover the device.

Wireless Sensor Network - If there is a problem communicating with the Wireless Sensor Network (WSN) then the Top LED will be Solid Red. Power off the gateway for 10 seconds.

*Note - The gateway can be configured to disable the WSN when communication with the server fails. In this case, the Top LED will be Solid Red.

Will Not Connect to Sensor Portal

The gateway operates on a local Ethernet network which requires a connection to the Internet in order to deliver data to the online portal. There are a few conditions which must be met in order to allow for the traffic to be successfully delivered to the online portal:

- Confirm the device has been added to an account.
- Confirm the gateway is connected to power and completes the startup test.
- Confirm the gateway is operating on the local Ethernet network with a valid IP address.
- Confirm the network allows for traffic to the Internet over outbound TCP port 3000 (inbound port is not specified), and the DNS server on the network can resolve sensorsgateway.com.
- Restore Factory Defaults - Press and hold the Utility Button for 10 seconds.
- Update the gateway's firmware if an update is available once the gateway has successfully connected to the sensor portal.

Notes

Notes

Limited Warranty

Equipment Warranty

Watts (the "Company") warrants each product to be free from defects in material and workmanship under normal usage for a period of one year from the date of original shipment. In the event of such defects within the warranty period, the Company will, at its option, replace or recondition the product without charge.

THE WARRANTY SET FORTH HEREIN IS GIVEN EXPRESSLY AND IS THE ONLY WARRANTY GIVEN BY THE COMPANY WITH RESPECT TO THE PRODUCT. THE COMPANY MAKES NO OTHER WARRANTIES, EXPRESS OR IMPLIED. THE COMPANY HEREBY SPECIFICALLY DISCLAIMS ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

The remedy described in the first paragraph of this warranty shall constitute the sole and exclusive remedy for breach of warranty, and the Company shall not be responsible for any incidental, special or consequential damages, including without limitation, lost profits or the cost of repairing or replacing other property which is damaged if this product does not work properly, other costs resulting from labor charges, delays, vandalism, negligence, fouling caused by foreign material, damage from adverse water conditions, chemical, or any other circumstances over which the Company has no control. This warranty shall be invalidated by any abuse, misuse, misapplication, improper installation or improper maintenance or alteration of the product.

Some States do not allow limitations on how long an implied warranty lasts, and some States do not allow the exclusion or limitation of incidental or consequential damages. Therefore the above limitations may not apply to you. This Limited Warranty gives you specific legal rights, and you may have other rights that vary from State to State. You should consult applicable state laws to determine your rights. **SO FAR AS IS CONSISTENT WITH APPLICABLE STATE LAW, ANY IMPLIED WARRANTIES THAT MAY NOT BE DISCLAIMED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, ARE LIMITED IN DURATION TO ONE YEAR FROM THE DATE OF ORIGINAL SHIPMENT.**

Connected Features Warranty

Any connected features of the product and any collection of data by or from the product are governed by the Watts Terms of Use available at: https://www.watts.com/terms-of-use

WATTS®

USA: T: (978) 689-6066 • Watts.com
Canada: T: (888) 208-8927 • Watts.ca
Latin America: T: (52) 55-4122-0138 • Watts.com