

User Guide



## Contents

Dual Gateway	3
Gateway Features	3
Applications	3
How the Gateway Works	4
Using the Gateway	5
Understanding the Gateway Lights	6
Standard or Forced-High Power Mode Operation	7
On Battery or Forced-Low Power Mode Operation	8
Ethernet Gateway	9
Gateway Features	9
Applications	9
How the Gateway Works 1	0
Using the Gateway1	1
Understanding the Gateway Lights	1
Auto Reboot Settings 1	2
Reset Memory	2
Troubleshooting 1	2
Gateway Placement 1	3
Connecting to Nexa 1	4
Security Protocols	5
Gateway Security	5
Sensor Communication Security	5
Data Security	5
Server Communication Security1	5
Certifications	6
Safety Recommendations	8

### A WARNING



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.

Nexa<sup>™</sup> Dual Gateway features a powerful wireless transceiver with up to 1 Watt transmission strength, an amplified receiver, and 4G LTE CAT-M1/NB2 cellular technology to backhaul Nexa sensor data. Dual



Gateway can send and receive data communications with Nexa sensors at 2,000+ feet through 18+ walls in commercial building environments.

You only need a power source and the Nexa cloud platform to monitor virtually any environment and equipment using Nexa industry-leading wireless IoT devices. The gateway communicates with Nexa sensors and Nexa to deliver data and send alerts about various machine, equipment, or area conditions.

The gateway is equipped with a 60-hour backup battery and continues to communicate with Nexa through its advanced cellular engine transmission in the event of a power outage.

Additionally, the gateway comes with an RJ-45 Ethernet jack for local device configuration. However, it is ideal for applications without a wired internet connection or with infrastructure dedicated to other resources.

The gateway also includes a GNSS location chipset supporting GPS, GLONASS, BeiDou, Galileo, and QZSS satellites.

### **Gateway Features**

- 4G LTE CAT-M1/NB2 cellular technology
- Wireless range of 2,000+ feet through 18+ walls\*
- Frequency-hopping Spread Spectrum (FHSS)
- Best-in-class interference immunity
- Encrypt-RF® Security (256-bit Diffie-Hellman Key Exchange + AES-128 CBC for sensor data messages)
- 32,000 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
- Local status LEDs with transmission and online status indicators
- AC power supply
- Up to 60-hour battery backup in the event of a power outage
- External on/off and magnetic utility switches (industrial version only)
- RJ-45 10/100BASE-TX Ethernet jack for configuration and server connectivity
- Location data subscription supported (GPS/GLONASS/BeuDou/Galileo/QZSS)

## Applications

- Domestic hot water pipes, risers, and branches
- Cold water lines
- Boiler and chiller supply and return
- Ambient temperature
- Additional applications

#### **IMPORTANT!**

The antenna must be connected at all times if the gateway is powered. Failure to do this causes the device to consume more than the rated power. Extended operation may potentially cause premature product failure.

<sup>\*</sup> Actual range may vary depending on the environment and the gateway.

<sup>\*\*</sup> Total messages in memory varies with sensor type (32,000 is for temperature sensors).

### How the Gateway Works

The gateway manages communication between Nexa sensors and Nexa. When running, the gateway periodically transmits data on a user-configured preset heartbeat interval (in minutes). The gateway receives data from all sensors assigned to the network (within range) and stores the data it receives from the sensors until its next heartbeat.

The gateway is a cellular (LTE-M or CAT-M1) device. It uses its connection to relay data received from Nexa sensors to Nexa software. Sensors communicate with the gateway, then the gateway relays information to Nexa.

For your wireless sensors to work optimally, orient all antennas for your sensors and gateways in the same direction (typically vertical). Sensors must also be at least 3 feet away from other sensors and the gateway to function properly.





## Using the Gateway



#### **On/Off Switch**

Power: Power cord connection port

Network: Ethernet connection port

**Utility Button:** During the boot sequence, a 5 second press of this button enables the local interface. When powered on, pressing the utility button for 10 to 15 seconds resets the gateway. Pressing the button for 15+ seconds clears all of the memory in addition to the factory reset. **Note:** Applies only when connected by Ethernet.

- 1. Attach the Nexa and cellular antennas to the back of the gateway.
- 2. Plug the power adapter cord into an electrical outlet and power on the gateway.
- 3. After the three LEDs switch to green, the gateway is ready for use.

## Understanding the Gateway Lights



The gateway enters three stages as it powers on.

**Power-on Stage:** The gateway analyzes electronics and programming. The LEDs flash red and green before turning green for 1 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. Contact Nexa Support if the lights are not green after 2 minutes.

**Connection Stage:** The gateway attempts to settle all operational connections. As the gateway first connects to the network, all other lights are dark. A blinking green light indicates the gateway is attempting to make a tower connection. A flashing red light is a signal the cellular connection has encountered a problem.

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



#### Sensor Data

Steady Green: Communication with sensors is OK Blinking Green: Active communication with sensors Steady Red: Sensor communication problem



#### Internet Server

Steady Green: Last communication with the Nexa server was OK Blinking Green: Active communication with the Nexa server Steady Red: Last communication with the Nexa server was unsuccessful





#### Cellular Service

Steady Green: Internet connection ready Single Blink Green: Cellular connection idle Double Blink Green: Scanning for tower Triple Blink Green: Requesting data session and IP Address Solid Green with Single Red Blink: Low signal report Solid Red with 1 Second Flashing Red/Green: SIM Fault Solid Red with Single Green Blink: Limited or no internet Flashing Red for 1 Second: Cellular module startup fault Flashing Green for 3 Seconds: Cellular FOTA download in progress Flashing Green for 3 Seconds: Cellular FOTA upgrading

**Note:** When setting up the gateway, initial tower connections may take 2 to 20 minutes depending on the carrier/SIM specific setup and the number of cellular bands enabled. Subsequent connections are typically faster.

## Standard or Forced-High Power Mode Operation



While the gateway is powered normally or configured to Forced-High power mode, the gateway remains fully active and ready to communicate with the server. All LED indicators are active (as described in the preceding section). The Ethernet and cellular interfaces stay connected, and GPS location services remain active.

GPS location services are permitted to acquire satellite data for up to 9 minutes. If a suitable location calculation is not achieved during that time, the gateway reports the lack of a location-fix and the gateway waits for the next location heartbeat to reacquire a location fix.

The gateway attempts to communicate with the server for up to 1 minute for every interface enabled (default is 2 minutes). If the gateway is unable to connect with the server using either the Ethernet or cellular interface, the gateway begins to retry connectivity based on the following sequence:

Attempt	Back-off Time Between Attempts	Cumulative Time Attempting Communication		
0	N/A	0 minutes		
1	0 minutes	2 minutes		
2	0 minutes	4 minutes		
3	1 minute	7 minutes		
4	2 minutes	11 minutes		
5	5 minutes	18 minutes		
6	10 minutes	30 minutes		
7	15 minutes	47 minutes		
8+	random 20–40 minutes	22–42 minutes added on every failure		

## On Battery or Forced-Low Power Mode Operation



If the gateway is running off of battery power or the device has been switched to a Forced-Low power mode, all lights are typically off. The sensor data light blinks green when data is received by the gateway. The internet server light blinks every 5 seconds, indicating the status of the last connection. If the light is green, the communication was good. If the light is red, the communication failed. In this mode, the Ethernet connectivity is powered down and the HTTP interface is not available.

**Gateway Heartbeats, Polls, and GPS Location:** These services are limited to a minimum of 15 minutes during low power events. However, if a wireless device signals that an urgent communication is required to be delivered to the server, the gateway powers up Ethernet, cellular, and GPS services temporarily during a server connection. If the gateway is unable to connect with the server using either the Ethernet or cellular interface, the gateway begins to retry connectivity based on the following sequence:

Attempt	Back-off Time Between Attempts	Cumulative Time Attempting Communication		
0	N/A	0 minutes		
1	5 minutes	7 minutes		
2	5 minutes	14 minutes		
3	5 minutes	21 minutes		
4	5 minutes	28 minutes		
5+	random 20–40 minutes	22–42 minutes added on every failure		

**Utility Button Actions:** The utility button can be used during the operational stage to perform a configuration reset or a full-factory reset. The configuration reset erases all of your unique settings and returns the gateway to factory default settings, while saving any data collected by the sensors prior to the reset. The full-factory reset not only restores default settings but also erases any data on the gateway.

To perform a configuration reset, the utility button is pressed for 5 to 10 seconds and released during that time. After pressing the utility button for more than 5 seconds, all of the LEDs turn solid red. Releasing the button during this LED display results in the configuration reset.

If the utility button is held for more than 10 seconds, all of the LEDs begin to blink red. Releasing the utility button when all of the LEDs are blinking red results in a full factory reset of the gateway, restoration of default settings, and the loss of all data in memory.

Nexa<sup>™</sup> Ethernet Gateway features a powerful wireless transceiver with up to 1 Watt of transmission power and an amplified receiver. Ethernet Gateway can send and receive data communications with Nexa sensors 2,000+ feet through 18+ walls in commercial building environments.



Additionally, the gateway allows Nexa sensors to communicate with Nexa IoT Monitoring and Notification System without needing a computer. Simply provide power and plug the gateway into an open Ethernet port with an internet connection. It automatically connects with the Nexa servers, providing the perfect solution for internet-enabled commercial locations.

The gateway is an advanced device that enables fast, reliable IoT data solutions. It is 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 2,000+ feet through 18+ walls\*
- Frequency-hopping Spread Spectrum (FHSS)
- · Best-in-class interference immunity
- Encrypt-RF® Security (Diffie-Hellman Key Exchange + AES-128 CBC for sensor data messages)
- 32,000 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
- · Local-status LEDs with transmission and online status indicators
- AC power supply

### Applications

- Domestic hot water pipes, risers, and branches
- Cold water lines
- Boiler and chiller supply and return
- Ambient temperature
- Additional applications

#### IMPORTANT!

The antenna must be connected at all times if the gateway is powered. Failure to do this causes the device to consume more than the rated power. Extended operation may potentially cause premature product failure.

<sup>\*</sup> Actual range may vary depending on the environment and the gateway.

<sup>\*\*</sup> Total messages in memory varies with sensor type (32,000 total messages for temperature).

## How the Gateway Works

The gateway manages communication between Nexa sensors and Nexa. When running, the gateway periodically transmits data on a user-configured preset heartbeat interval (in minutes). The gateway receives data from all sensors assigned to the network (within range) and stores the data it receives from the sensors until its next heartbeat.

The gateway uses an Ethernet connection to relay data received from Nexa sensors to Nexa software. Sensors communicate with the gateway, then the gateway relays information to Nexa.

For your wireless sensors to work optimally, orient all antennas for your sensors and gateways in the same direction (typically vertical). Sensors must also be at least 3 feet away from other sensors and the wireless gateway to function properly.







### Using the Gateway



Power: Power cord connection port

**Network:** Ethernet connection port

**Utility Button:** During the boot sequence, a 5 second press of this button enables the local interface. When powered on, pressing the utility button for 10 to 15 seconds resets the gateway. Pressing the button for 15+ seconds clears all of the memory in addition to the factory reset.

1. Attach the antenna to the gateway.

2. Plug the power adapter cord into an electrical outlet.

3. After the three LEDs switch to green, the gateway is ready for use.

### Understanding the Gateway Lights

The gateway enters three stages as it powers on:

**Power-on Stage:** The gateway analyzes electronics and programming. The LEDs flash red and green before turning green for 1 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. Contact Nexa Support if the lights are not green after 2 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**

Steady Green: Communication with sensors is ok Blinking Green: Active communication with sensors Steady Red: Sensor communication problem

#### **Server Communication**

Steady Green: Last communication with the Nexa server was ok Blinking Green: Active communication with the Nexa server Steady Red: Last communication with the Nexa server was unsuccessful

#### Ethernet Link

Steady Green: Internet connection successful Steady Red: No internet connection found

## Auto Reboot Settings



The Auto Reset field is the amount of time in hours that the local interface automatically reboots. Setting this to 0 disables the feature. The maximum setting is 8760 hours.

### **Reset Memory**

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

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

### Troubleshooting

**Ethernet Cable Not Detected –** The bottom LED blinks 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 turns 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 is 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 is OFF. If this occurs, a Factory Reset recovers the device.

**Nexa System –** If there is a problem communicating with the Nexa then the top LED is solid red. Power off the gateway for 10 seconds. If the problem persists, contact Nexa Support.

**Note:** The gateway can be configured to disable when communication with the server fails. In this case, the top LED is solid red.

## **Gateway Placement**

### Sensor and Gateway Distance



Place each Nexa sensor within 2,000+ feet of a Nexa gateway. The sensor should be located to

avoid transmissions through a lot of metal, or concrete, and repositioned to avoid such obstacles if cellular communication is spotty.

The strength of the signal between a sensor and a gateway can vary. Sensors which can transmit long distances can sometimes have more difficulty up close. The nearer the sensor to the gateway depending on the strength of the signal, the more garbled the signal can be.

Sensors need at least 3 feet between them and the gateways for effective close transmission. This distance is particularly important during setup when the sensors are trying to connect initially with gateway. The sensors actively scan to contact the gateway the moment the battery is inserted, or the sensor powered on.

An analogy: A person standing next to a loud speaker will be able to hear an announcement but may not be able to understand it. After moving away from the loud speaker, the person will be able to both hear and understand the announcement.

## Connecting to Nexa

Now that your gateway(s) and sensors have been successfully installed, you need to contact your dedicated Customer Success Manager (CSM) to register you and your team on the Nexa platform. Your CSM connects your system data to the cloud, creates a system map, sets alerts, and assumes responsibility for fully onboarding your team, providing visibility and generating valuable insights.

To complete the registration, your Customer Success Manager will need some important information. Every gateway and sensor has a unique identification number (ID) and security code (SC) located on the back of the gateway. (See example on the right.) Record and relay that information along with the precise location within the facility for each sensor and gateway. Those location names are how you will be able to identify critical data for each sensor within Nexa.



As shown here, for each sensor registered on Nexa, the record includes sensor name, sensor location, sensor type, last sensor reading, last reading time, and manufacturer ID. Tap the 3-dot menu on the right end of a row to edit or delete the sensor record or to copy the ID.

× X No	ω × +						- a ×
← → (	ී බ 🙁 nexaplatform.com	√sensors				\$	5   O 😩 :
≙ ≎ ★ ♠	Sensors Manage your sensors and gat SENSORS GATEWAYS	eways.					CREATE NEW
₽+ <b>₽</b>	Search by sensor or equip	oment Q Location	✓ Sensor Type	*			LEAR ALL
ih.	Sensor	Location	Туре	Last Reading	Last Reading Time	Manufacturer ID	
	CWS Temp In West Wing MR	Nexa Headquarters	Temperature Sensor	51.3°F	04/10/24 11:22 EDT	52737	^
	Flow Meter 1	West Wing Mechanical Room	G Flow Meter	118.0 gpm	04/10/24 11:22 EDT	336601	
•	Flow Meter 2	West Wing Mechanical Room	G Flow Meter	15.9 gpm	04/10/24 11:22 EDT	336606	
2	Flow Meter 3	West Wing Mechanical Room	G Flow Meter	25.0 gpm	04/10/24 11:22 EDT	336607	/ Edit
((*))	Heater Combo Temp Out West	West Wing Mechanical Room	Temperature Sensor	127.7°F	04/10/24 11:22 EDT	52749	Delete Copy ID
Φ <sub>0</sub>	Leak Tank (West)	West Wing Mechanical Room	Leak Detector	Leak	04/10/24 11:20 EDT	52741	
\$	Leak WH (West)	WH Plant	Leak Detector	Leak	04/10/24 11:20 EDT	52740	
0	Mixing Valve Out	Nexa Headquarters	Temperature Sensor	148.0°F	04/10/24 11:01 EDT	52755	
[→	Pressure 300 PSI	West Wing Mechanical Room	Pressure Sensor	76.1 psi	04/10/24 11:01 EDT	52735	
	Pressure In WH 1 West	WH Plant	Pressure Sensor	106.0 psi	04/10/24 11:00 EDT	52736	
					Rows per page	: 10 - 1-10 of 21	< >

## Security Protocols

## Gateway Security

Designed and built to manage data from sensors, the gateways monitor your environment and equipment securely. The same methods used by financial institutions to transmit data are also used in the Nexa security infrastructure. The gateway security features tamper-proof network interfaces, data encryption, and high-grade security.

Nexa proprietary sensor protocol uses low transmit power and specialized radio equipment to share application data. Packet-level encryption and verification are vital to ensuring traffic is not altered between sensors and gateways. Paired with a bestin-class range and power consumption protocol, all data transmit securely from your devices.

### Sensor Communication Security

Wireless devices listening on open communication protocols cannot eavesdrop on Nexa sensors. Nexa sensor-to-gateway data communication implements Encrypt-RF® encryption technology. This creates a secure wireless tunnel, generated using ECDH-256 (Elliptic Curve Diffie-Hellman) public key exchange to develop 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. Due to this combination, Nexa offers robust high-grade security at every level.

### Data Security

The gateways prevent prying eyes from accessing the data stored on the sensors. The gateways do not run on an off-the-shelf, multifunction operating system. Instead, it runs on a purpose-specific, real-time embedded state machine that cannot 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 gateways secure data from attackers and protects the gateway from becoming a relay for malicious programs.

### Server Communication Security

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

# Certifications

### United States FCC

This equipment has been tested and found to comply with the limits for a Class B digital devices, 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 instruction manual, 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 of 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.

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.

### A WARNING

Changes or modifications not expressly approved by Nexa could void the users authority to operate the equipment.

## A WARNING

**RF Exposure.** To satisfy FCC RF exposure requirements for mobile transmitting devices, the antenna used for this transmitter must not be co-located in conjunction with any antenna or transmitter. Additionally, a separation distance of 8.7 in. (22 cm) or more should be maintained between this device and persons during device operation.

#### Approved Antennas

Nexa devices have been designed to operate with any one of the approved antennas (listed below) having a maximum gain of 14 dBi. Antennas having a gain greater than 14 dBi are strictly prohibited for use with this device. The required antenna impedance is 50 ohms.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (EIRP) is not more than that required for successful communication. The system antenna(s) used with the device must not exceed the following levels:

Part Number	Manufacturer	Description	<b>Required Cable Loss</b>
XQZ-900E-2	Xianzi	3 dBi Dipole Omni	0 dB
HG905RD-RSP	Hyperlink	5 dBi Dipole Omni	0.44 dB
HG908U-PRO	Hyperlink	8 dBi Fiberglass Omni	3.48 dB
HG8909P	Hyperlink	9 dBi Flat Panel	3.54 dB
HG914YE-NF	Hyperlink	14 dBi Yagi	1074 dB

## Canada (IC)

### English

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum(or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (EIRP) is not more than that necessary for successful communication.

The radio transmitters (IC: 9794A-RFSC1, IC: 9794A-G2SC1, IC: 4160a-CNN0301, IC: 5131A-CE910DUAL, IC: 5131A-HE910NA, IC: 5131A-GE910 and IC: 8595A2AGQN4NNN) have been approved by Industry Canada to operate with the antenna types listed on previous page with the maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

#### Français

Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peut fonctionner avec une antenne d'un type et d'un gain maximal (ou inférieur) approuvé pour l'émetteur par Industrie Canada. Dans le but de réduire les risques de brouillage radioélectrique à l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que la Puissance Isotrope Rayonnée Èquivalente (P.I.R.È) ne dépasse pas l'intensité nécessaire à l'établissement d'une communication satisfaisante.

Le présent émetteurs radio (IC: 9794A-RFSC1, IC: 9794A-G2SC1, IC: 4160a-CNN0301, IC: 5131A-CE910DUAL, IC: 5131A-HE910NA, IC: 5131A-GE910 et IC: 8595A2AGQN4NNN) a été approuvé par Industrie Canada pour fonctionner avec les types d'antenne figurant sur la page précédente et ayant un gain admissible maximal et l'impédance requise pour chaque type d'antenne. Les types d'antenne non inclus dans cette liste, ou dont le gain est supérieur au gain maximal indiqué, sont strictement interdits pour l'exploitation de l'émetteur.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, méme si le brouillage est susceptible d'en compromettre le fonctionnement.

#### A WARNING

**RF Exposure.** To satisfy IC RF exposure requirements for mobile transmitting devices, the antenna used for this transmitter must not be co-located in conjunction with any antenna or transmitter. Additionally, a separation distance of 12.6 in. (32.1 cm) or more should be maintained between this device and persons during device operation.

## Safety Recommendations

Be sure the use of this product is allowed in the country and in the environment required. The use of this product may be dangerous and has to be avoided in the following areas:

- Where it can interfere with other electronic devices in environments such as hospitals, airports, and aircraft.
- Where there is risk of explosion such as gasoline stations, oil refineries, etc.

It is the responsibility of the user to enforce the country regulation and the specific environment regulation. Do not disassemble the product; any mark of tampering will compromise the warranty. We recommend following the instructions of this user guide for correct setup and use of the product.

Handle the product with care, avoiding any dropping and contact with the internal circuit board as electrostatic discharges may damage the product itself. The same precautions should be taken if manually inserting a SIM card, checking carefully the instruction for its use. Do not insert or remove the SIM if the product is capable of going into power saving mode.

Every device has to be equipped with a proper antenna with specific characteristics. The antenna has to be installed with care in order to avoid any interference with other electronic devices and has to guarantee a minimum distance from the body (US: 22cm or IC: 32.1cm). In case this requirement cannot be satisfied, the system integrator has to assess the final product against the SAR regulation.

#### Equipment Errata: Power Supply Advisory

When using the gateway in remote area or powering the gateway with an inverter, there is a potential for unbalanced or noisy power (not true sinusoidal AC power). The gateway may experience random reboots and Ethernet link instability in these situations. Nexa recommends using the AC/DC power supply issued with the device in those situation. Additionally, Power line filters or higher-end power inverters may all be required for stable operation.

#### Coverage Maps

AT&T https://www.att.com/maps/wireless-coverage.html

Verizon

https://www.verizonwireless.com/wcms/overlays/international-travel-coverage-map.html

## Notes


Limited Warranty: Watts Regulator Co. (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. SSO 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.



by WATTS

UserGuide-N-Gateways 2410