MONNIT®

Remote Monitoring for Business

MONNIT DATA SECURITY

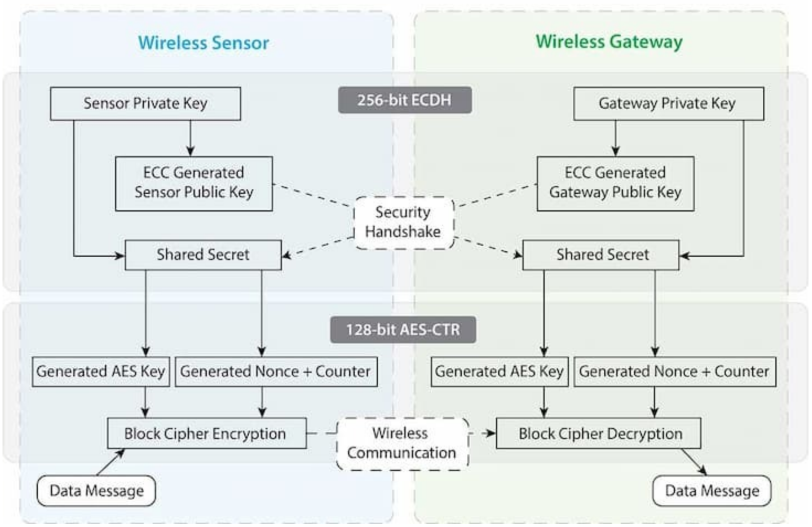
Monnit ALTA Wireless, PoE•X (Power over Ethernet), and MoWi (Wi-Fi) sensors have been designed and built to securely manage data. Monnit works to ensure your data security is handled with the utmost care. The same methods utilized by financial institutions to transmit data are also used in Monnit's security infrastructure. Security features from sensors to gateways include tamper-proof network interfaces, data encryption, and bank-grade security.

Monnit's proprietary sensor protocol uses low power and specialized radio equipment to transmit application data. Wireless devices listening on open communication protocols cannot eavesdrop on sensors. Packet-level encryption and verification is key to ensuring data traffic isn't altered between sensors and gateways. Paired with a best-in-class range and power consumption protocol, all data is transmitted securely from your devices, ensuring a smooth, worry-free experience.

SENSOR COMMUNICATION SECURITY

Monnit's sensor-to-gateway, secure wireless tunnel, **Encrypt-RF**™, 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, which minimizes power consumption to provide better battery life. Thanks to this combination, Monnit proudly offers robust bank-grade security at every level.

How Monnit Encrypt-RF™ Works



DATA SECURITY ON THE GATEWAY

ALTA Gateways are designed to prevent prying eyes from accessing the data that is stored on the sensors. Gateways do not run on an off-the-shelf, multi-function operating system. Instead, they run on a purpose-specific, real-time, and 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 gateway secures your data from attackers and secures the gateway from becoming a relay for malicious programs.

More information on Ethernet Gateway Security https://monnit.blob.core.windows.net/site/documents/other/ethernet-gateway-security-brief.pdf

iMONNIT SECURITY

The iMonnit system is the online software and central hub for configuring your device settings. All data is secured on dedicated servers operating Microsoft SQL Server. Access is granted through the iMonnit user interface that requires Two-Factor Authentication, or an Application Programming Interface (API) safeguarded by 256-bit Transport Layer Security (TLS 1.2) encryption. TLS is a blanket of protection to encrypt all data exchanged between iMonnit and you. The same encryption is available to you whether you are a Basic or Premiere user of iMonnit. You can rest assured that your data is safe with iMonnit.

iMONNIT ENTERPRISE

If your organization does not allow for external data communication due to sensitive information or regulations, such as national laboratories, where information systems need to remain behind advanced security protocols and firewalls, Monnit offers an on-premise version of iMonnit. iMonnit Enterprise provides the same feature set as the iMonnit Premiere online software but allows your organization to host and maintain its own sensor data.

OPTIONAL DATA AUTHENTICATION

SensorPrints is the industry's only end-to-end Internet of Things data authentication platform for low-power wireless sensors. SensorPrints authenticates data by issuing a unique fingerprint for each device within the IoT. Data is secured from the point of generation to the point of consumption. Easy to install and use, SensorPrints is is the definitive IoT security solution for any enterprise.

SensorPrints authenticates data at both the point of generation and consumption, creating trust between the sensor and server levels. Implementing 256-bit SHA 3 authentication, SensorPrints creates a "fingerprint" for a Monnit Wireless Sensor that contains an authenticated sensor message. When data is transmitted from the sensor, it is accompanied by a generated authentication token. Upon receipt by the application, the token is evaluated via crytographic hash function against a unique per sensor secret key. This step provides an unprecedented level of full-coverage security for any Monnit user wishing to secure their IoT devices and data. More information can be found at https://www.monnit.com/products/software/sensorprints-data-authentication/.