Remote Monitoring for Business

SensorPrints™ Install Guide

General Description

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.

Principle of Operation

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.

SensorPrints requires sensor and gateway firmware ver. 16.34.x.x or greater to work.

Sensor/Gateway Communication Security

Monnit sensor to gateway and gateway to server secure 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 which minimizes power consumption to provide industry best battery life. Gateways use ECDH-256 to also generate their own keys to encrypt data to the server. Then the gateway sends sensor readings to iMonnit. Thanks to this combination, Monnit proudly offers robust bank-grade security at every level.

iMonnit Security

iMonnit 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, or an Application Programming Interface (API) safe-guarded 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 user or Premiere user of iMonnit. You can rest assured that your data is safe with iMonnit.

End-to-End Security

Sensor
Digitally signs data

Gateway

MONNIT
Verifies digital signature

To purchase SensorPrints for your wireless sensors, please follow these easy steps. Before beginning, please verify your sensors/gateways are firmware version 16.4.x.x. If they are not, you will need to purchase new hardware to use SensorPrints.

Temperature	Voltage Meter 0-5 VDC	Duct Temperature	Thermocouple
Water Rope	Dry Contact	Humidity	Open/Close
Current Meter	High Temperature	Low Temperature	

1
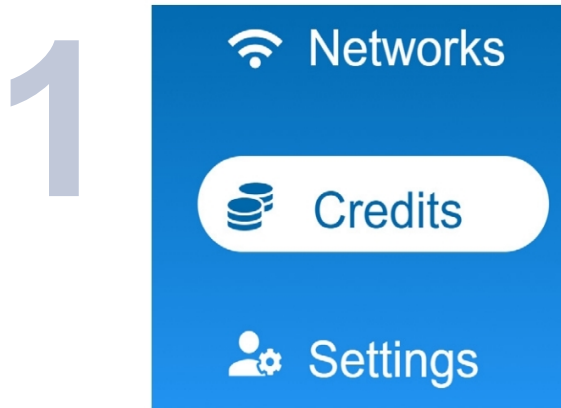
Log into iMonnit and select Credits in the main navigation menu.

2
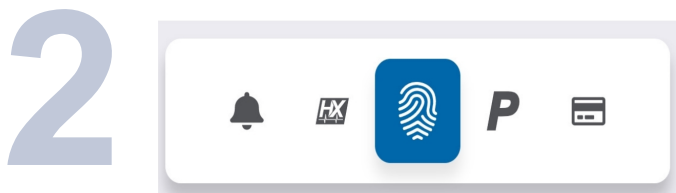
Choose the SensorPrints option from the tab bar.
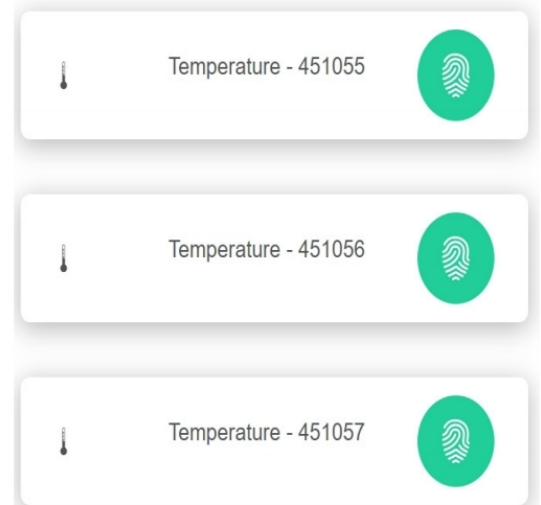
3

SensorPrint Store

Scroll down to the bottom of the page to buy SensorPrint credits from the store right in iMonnit.

4

Select any one of the sensors on your account to assign a SensorPrint to that device.

For more detailed instructions, documentation, how-to guides and video demonstrations on using Monnit wireless sensors, wireless gateways and iMonnit software, visit our support page at monnit.com/support/.

Monnit Corporation
3400 South West Temple • Salt Lake City, UT 84115 • 801-561-5555
www.monnit.com