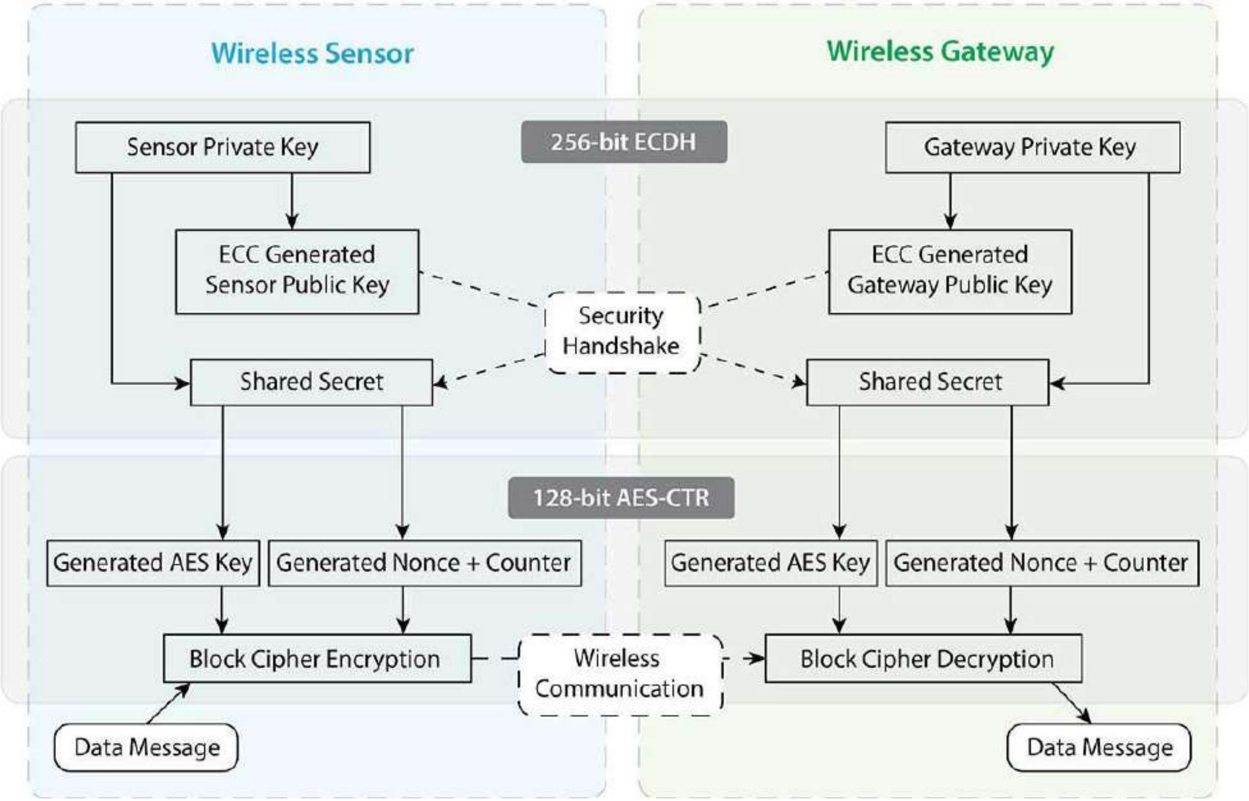
TopJet Alert System Security Overview

At TopJet Alert we take security seriously. We have addressed security concerns at all levels of our distributed intelligence sensing platform. Keeping data safe is top priority at each level of communication, starting with intelligent sensor line, all the way up to the online sensor monitoring software, where the data safely resides and people are notified of events occurring in their world that have been captured by TopJet sensors.



One of the great advantages of using a TopJet sensor system is that ours are intelligent sensors. Their bi-directional communication allows them to verify delivery of messages and to receive and store values that can affect their behavior. Receiving acknowledgements for the messages they send allows the sensors to continually confirm they are connected to a gateway so they can know their data is safe. The wireless protocol gives you best in class range and battery life, it also protects against radio interference and spoofing of sensor data by third parties. Even in the unfortunate event of a power outage or similar that takes a gateway offline, the intelligent sensors recognize that their secure connection has been disrupted and enter a “Link” state waiting for the power to be restored to the gateway and then only after reestablishing their connection with the gateway do they start transmitting data again.

Distributed intelligence means intelligence at all levels of the system, our gateways are no exception. We have experience building gateways that communicate over many communication mediums Serial, Ethernet, Wi-Fi, and Cellular. We proprietary gateway communication protocol allows maximum performance with minimal bandwidth consumption. While this compressed data has always been obfuscated and the small packet size difficult to decipher, the newest addition to this protocol boasts a powerful 128 bit encryption engine. Until January 2000 US law prohibited exporting software that utilized greater than 40 bit encryption with national security concerns. The repeal of this law enabled strong 128 bit encryption to be deployed worldwide. Our sensors and gateways are available in frequencies which can be distributed anywhere in the world and the communication to the online software is now backed by the same level of encryption that secures our online transactions.

Ultimately the real usefulness of the data is culminated in the online software where raw data from multiple sensor networks are brought together and parsed into meaningful data. The data now in its easy to consume state is stored securely on dedicated servers running Microsoft SQL Server. Access to the data is made available through either the user interface or an application programming interface (API). Both of which utilize 256 bit Secure Socket Layer (SSL) certificates issued by a certified third party. Our certificates are automatically recognized by 99.9% of web browsers. This cryptographic protocol encrypts packets at the application layer before it is even handed off to be packaged for transmission. SSL uses asymmetric cryptography for exchanging encryption keys, and message authentication codes to ensure data integrity after it arrives at its destination. This is the same security used by banks and other financial institutions to protect online banking transactions. All of this is available with either a free Basic account, or a Advance subscription for a full featured sensor monitoring solution.

Users of these sensor systems rest easy knowing that starting at the sensor, data collected is protected all the way through the process. We maintain the highest standards of data protection to ensure data entrusted to the system arrives at its intended destination securely.

Data Security

The wireless communication technology provides several features to help protect your data in transit. Our proprietary sensor protocol uses very low transmit power and requires specialized radio equipment to operate. Typical wireless devices that operate on non-proprietary communication protocols (Wi-Fi, Bluetooth, Zigbee) operate using different frequency bands so they can’t be used to eavesdrop on the radio communications from the family of sensors. We also uses a robust packet tampering evaluation routine to ensure traffic wasn’t altered between sensors and gateways. This enables us to check for well-formed data packets that only originated from enabled devices. To further protect data, we use algorithms to protect against spoofing and re-transmission of wireless data packets. This is included with best-in-class range and a power consumption protocol developed for wireless sensor systems.

Data security is important for multiple reasons. First, it is always important to keep the data sent from inside your network protected during transmission. Second, it is important to protect responses from the monitoring software from being compromised. Protocols Gateways utilize a proprietary protocol that enables sensor data to be sent with minimal overhead. This also prevents casual lookers from observing the traffic and being able to interpret it. As opposed to many text based protocols (e.g. HTML/XML/JSON) the data is encoded in binary form that is not directly convertible to human readable values. This TopJet Gateway Protocol is the basis for all communication between the gateway and the monitoring software.

When enabled there are other protocols that allow the gateway to be used by other systems that implement those protocols. The two currently supported are Modbus over TCP and SNMP. These are for convenience and utility by certain users and are not enabled by default.

Encryption

In addition to binary protocols and rejecting unrequested network traffic, the EGW 3.0 also implements 128-bit AES encryption while sending and receiving data from the servers. This encryption allows all transmitted data that would otherwise be difficult for someone to read, to also be encrypted. The encryption is bi-directional so both the data that is being sent as well as the responses being returned are encrypted.

How is sensor data protected during wireless transmission?
Application data is 18 bytes in length, and the total TX packet size is 40 bytes. The wireless communication technology provides several features to help protect your data in transit. Our proprietary sensor protocol uses very low transmit power and requires specialized radio equipment to operate. Typical wireless devices that operate on non-proprietary communication protocols (Wi-Fi, Bluetooth, Zigbee) operate using different frequency bands so they can’t be used to eavesdrop on the radio communications from the family of sensors. We also uses a robust packet tampering evaluation routine to ensure traffic wasn’t altered between sensors and gateways.
This enables us to check for well-formed data packets that only originated from enabled devices. To further protect data, we use algorithms to protect against spoofing and re-transmission of wireless data packets. This is included with best-in-class range and a power consumption protocol developed for wireless sensor systems.

How secure is the communications on the wireless network?
We uses the same encryption methods used by websites to transmit financial data. Secure socket layer (SSL) protocol is employed with 256-bit data encryption making data hosted on your network secure.

Network Security

Network security addresses factors that affect the local network into which the gateway is installed.

Addressing

The EGW 3.0 will utilize standard DHCP to obtain a dynamic IP Address from the local network. Doing so enables most users of the EGW 3.0 to enjoy zero configuration setup. During the DHCP setup the gateway announces itself so the network administrator can easily locate which IP address is given to the gateway. If desired, the gateway can be assigned a static IP Address by the network administrator. There are several methods which can be used to configure the gateway to receive this address. It can be done by the monitoring software if a temporary DHCP address can be used. If there is not a DHCP server available to issue a temporary address, there is a local web based interface that can be accessed for configuration. Physical access to the gateway is required to temporarily enable this interface.

Operating System

Because of the single use nature of the EGW 3.0, there is no embedded operating system utilized on the hardware. This means there is no system that can be used to run any third-party code. Anyone trying to hack into a system to run their own code will find it unsuccessful.

Network Ports

The EGW 3.0 sends its data to the monitoring software over port 3000. The gateway creates a standard TCP connection to the software and then communicates the data.
The monitoring software responds as needed to the gateway. This enables network administrators to easily monitor traffic to and from the device without having to separate it from other protocols using common ports. If needed, the gateway can be configured to communicate over any port on which the monitoring software has also been configured to listen for gateway communication.
The online portal has several alternative ports already configured for use. Any of the monitoring solutions can be configured to listen on specific or multiple ports.

Listeners

There are no listeners on the gateway responding to any TCP or UDP network traffic. The gateway will respond to an ICMP ping to assist network administrators with network troubleshooting. All other traffic is ignored on the network unless it is part of a TCP connection that was initialized from the Ethernet Gateway.

Because all traffic is initiated from the gateway, in most networks there is no configuration needed to the firewall as all traffic originates from within. No monitoring solutions will initiate communication from the server and try to communicate with the gateway. The monitoring solutions only respond to communications they receive from a gateway.

Advanced users can configure one or more of the local interfaces to respond to communication from within the network. The interfaces available are:

1. Proprietary TCP based binary protocol that enables a status application to communicate with the gateway.
2.Modbus over TCP protocol that enables a PLC or other Modbus enabled device to poll for data from the sensors that has been delivered to the gateway.
3.SNMP, a UDP based protocol that enables any SNMP enabled device or software to poll

for data from the sensors that has been delivered to the gateway.

How is sensor data protected during wireless transmission?
Application data is 18 bytes in length, and the total TX packet size is 40 bytes. The wireless communication technology provides several features to help protect your data in transit. Our proprietary sensor protocol uses very low transmit power and requires specialized radio equipment to operate. Typical wireless devices that operate on non-proprietary communication protocols (Wi-Fi, Bluetooth, Zigbee) operate using different frequency bands so they can&#39;t be used to eavesdrop on the radio communications from the family of sensors. We also use a robust packet tampering evaluation routine to ensure traffic wasn't altered between sensors and gateways. This enables us to check for well-formed data packets that only originated from enabled devices. To further protect data, we use algorithms to protect against spoofing and re-transmission of wireless data packets. This is included with best-in-class range and a power consumption protocol developed for wireless sensor systems.

How secure is the communications on the wireless network?

We uses the same encryption methods used by websites to transmit financial data. Secure socket layer (SSL) protocol is employed with 256-bit data encryption making data hosted on your network secure.

Ultra products use new Encrypt-RF® bank level security, featuring a 256-bit exchange to establish a global unique key, and an AES-128 CTR for all data messages.
So security is maintained at all communication points from sensor to gateway, gateway to software, and back again.