Application Note

Using SignalFire Encryption

OVERVIEW

As of August 1, 2016, SignalFire has released new firmware for all products. This release implements security and encryption. All devices shipped after this date will be loaded with the new firmware. Additionally, the ToolKit has been updated to support this new feature.

USING ENCRYPTION

Legacy Corporate IDs

Previously SignalFire issued a corporate ID to each end user, and this ID was pre-configured before the devices were shipped. The function of the corporate ID was to prevent devices from customer "A" from communicating with devices from customer "B", even if the same network and network group were configured. While this does provide network isolation its functionally is limited and a more flexible and secure method was needed.

Backwards Compatibility

If a new device is to be installed into an existing network, it must be configured to use the same corporate ID as the gateway. This is set using the SignalFire ToolKit. Note that the legacy corporate ID should only be used for existing networks where updating to the latest firmware that supports encryption is not feasible.

New Installations

For any new installations it is highly recommended that encryption is used. The Gateway (and every node to communicate with it) must be configured with the same "key" (6 to 16 characters) in addition to the network and network group settings. The "key" is the only new setting needed. Note that the "key" can be configured to be unrecoverable. If this is set, the "key" can **never** be read back out of the device, so if it is forgotten or unknown every device must be re-configured with a new "key". Use the unrecoverable option with caution!

CONCLUSION

SignalFire's encryption has been designed to allow backward compatibility with existing networks and to be simple to enable on all new network installations.