Enabling
Smart Buildings™

Igor PoE Lighting Solution Security Measures

Cloud Encryption & Authentication

Igor's HTTPS Gateway to Cloud Portal communications use the latest in cloud technology provided by Microsoft Azure. All communication (including licensing, data uploads, and system health information) is performed securely using 256-bit AES encryption. An OAuth2 authorization framework further protects user accounts access.

Gateway Authentication

The Igor Gateway is the "brains" between the lighting network and other networks and the outside world. Users of Igor's Software Admin application are registered and verified before access is granted. All critical settings are uploaded to the Cloud Portal for future reference or recovery. All third-party system and user requests to the Igor Gateway Software API must use a shared key with a valid JSON Web Token (JWT). In addition, Gateway software is compatible with most antivirus applications provided the recommended software path and process exclusions are implemented. The Gateway software is regularly updated with additional protections.

Network Protocols

Igor recommends using Dynamic Host Configuration Protocol (DHCP) to point Igor Nodes directly to the Gateway Internet Protocol (IP) address in lieu of User Datagram Protocol (UDP) multicast messaging. (UDP is a connectionless protocol that is easy to spoof and manipulate.) The Igor CoAP (Constrained Application Protocol) Service is responsible for communicating to all Igor enabled, third-party devices (switches, light fixtures, sensors). However, the Igor system can easily implement and support additional protocols, such as Universal Plug and Play (UPnP).

Users are encouraged to employ an isolated Virtual Local Area Network (VLAN). A VLAN provides several advantages, including security policy enforcement. An isolated/private VLAN prevents access from other TCP/IP/Ethernet networks.