Baseline Security Controls

Baseline uses symmetric cryptography to encrypt the data transmitted between controllers (similar to the TLS Handshake Protocol). This encryption ensures all communication between controllers, performance components, and the server is secure.

Security Controls for Communication with the Baseline Server

The Baseline server enables users to remotely connect to and operate Baseline irrigation controllers. Users operate their irrigation controllers through a web-based (browser-based) interface, and the controllers are connected through web-based ports. All traffic is TCP/IP with varying media types (Cellular Modem, Wi-Fi, Ethernet Radio, Ethernet Cable) deployed along the route. The server routes communication, performs maintenance tasks, stores data logs, and enables remote updating and configuration.

- All data is stored on a database server (mySQL) that is not externally accessible other than through activities and reports that are available through encrypted web access.
- The BaseStation 1000 and BaseStation 3200 controllers initiate communication with the server using AES256-bit encryption and will not accept any external connection requests from outside sources.
- The Baseline server requires controllers to be authorized in order to connect to the server.
- The Baseline server tracks and manages controller connections using the unique MAC address of each controller.
- The Baseline server generates authorization PINs for controllers that are attempting to connect for the first time.
    - The authorization PIN is displayed on the controller's main screen.
    - Company admins use the authorization PIN to connect controllers to their company in BaseManager.

Security Controls for Communication with the FlowStation and SubStation

The BaseStation 3200 controller sends and receives information over an encrypted communication path to other Baseline products.

- The BaseStation 3200 communicates with the FlowStation using AES256-bit encryption and symmetric cryptography.
- The BaseStation 3200 communicates with the SubStation using AES256-bit encryption and symmetric cryptography.

Security Controls for the Self-hosted Baseline Server

All communication to and from clients (browsers) and controllers is done over port 443. In order for controllers to work with the server, they must be able to talk to the server on that port and be enabled to use symmetric cryptography. Clients also need to be able to be routed to the server's Apache-httpd at that port.

- All data is stored on a local database server (mySQL).
- Traffic is internal only to the local drive. There is no database access from external connections.
- Industry standard Apache web security is employed. Further access control is supported to manage access via IP, network, or MAC address through the .htaccess facility of Apache.
- Controllers only listen to the assigned server, only over the WebSocket Protocol (not HTTP), and only through encrypted traffic.
- Controllers/clients need not respond over the same Ethernet device on the server. In some situations, it may be preferable to have controllers on their own Internet-isolated network.
- Webmin (a web-based system configuration and management tool) is enabled by default on a specified https port 10001. Webmin access can be disabled from external access (i.e., localhost only) or disabled entirely.

Security Controls for the Self-hosted Baseline Server Virtual Machine Image

The self-hosted server is also available as a virtual machine image suitable for installation in modern rack mount VMware server environments.

All communication to and from clients (browsers) and controllers is done over port 443. In order for controllers to work with the virtual machine, they must be able to talk to the server on that port and be enabled to use symmetric cryptography. Clients also need to be able to be routed to the virtual machine's Apache-httpd at that port.

- The self-hosted Baseline server virtual machine requires a minimum of 4GB of RAM, 120GB of disk space, and an Intel i3 class processor or equivalent.
- The self-hosted Baseline server in either the hardware-based version or the virtual machine image can be fully managed via the built-in secure web server.
- In order to allow mobile devices to access the self-hosted Baseline server, an externally accessible static IP address or hostname is required, and https web access to the self-hosted Baseline server will need to be enabled.