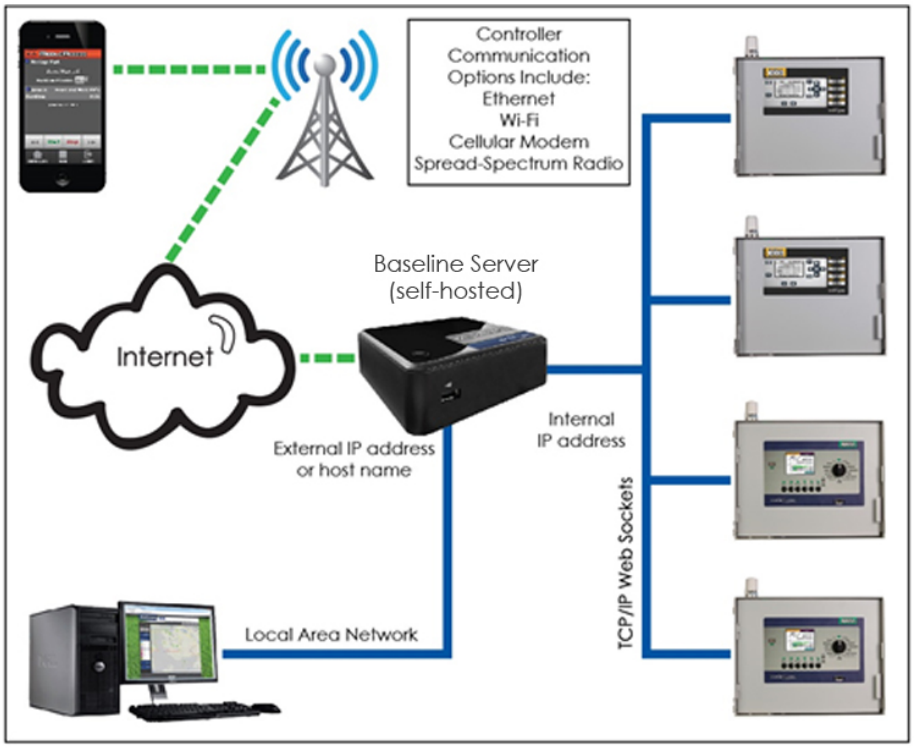
Self-Hosted Baseline Server Overview for Network Administrators

This document gives a brief overview of the self-hosted Baseline server. While the document is not intended to be a comprehensive description, it should help network administrators and other IT professionals understand the operation of AppManager™ and its associated apps including BaseManager™. This information should help address internal security concerns related to hosting an instance of the Baseline server.

Baseline Server Overview

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 (HTML-5 standard, WebSocket Protocol).

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 watering logs and information, and enables remote updating and configuration.



Network Topology Example for the Self-hosted Baseline Server

Networking

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 the latest level of security. Clients also need to be able to be routed to the server's Apache-httpd at that port. This approach prevents the need for opening firewall pinholes or configuring port mapping at an off-site facility. Typically, most IT installations route HTTPS out-bound traffic. If an Ethernet port can get out to the Internet, no other special configuration will be required at the controller side.

An important part of the browser-based AppManager client application is the map interface in BaseManager. The map data is loaded from a third-party. This data transfer requires general access from the client to the Internet and from the Internet back to the client. The client makes requests and downloads data over an Internet connection.

WebSocket Protocol

Communication in this system is based on the secure WebSocket Protocol. This approach allows for instantaneous, full-duplex communication.

Note: For more information on WebSocket Protocol, refer to the following URL:

https://en.wikipedia.org/wiki/Websocket

Running this communication protocol on the network means that traffic packets are not always in the format of a traditional HTTPS exchange (headers, body, etc.). Using this format and ensuring TLS-only traffic has proved to ease routing woes. We have found no difficulties yet in passing this traffic, even with sophisticated routers, packet-shapers (like F5), or web filters.

A secure version of the WebSocket protocol is implemented in the most current version of the Mozilla Firefox, Google Chrome, and Safari browsers. While most current browsers support this standard, noncompliant browsers are still in use.

Baseline Server Components

Baseline servers are built on the CentOS Linux distribution.

The lists below specify the required and optional packages that are included by default in the self-hosted Baseline server for both the hardware-based version and the virtual machine image.

Required Packages (Included in the Self-hosted Baseline Server Distribution)

Note: The following list includes only the packages that may be required in addition to those that are included in a minimum CentOS distribution.

- httpd-server
- mysql-server
- MySQL-python
- python-devel
- flex
- libtool
- make
- rsync
- mod_ssl
- python package
- pytz – time utilities
- webmin
- subversion (for checkout of mod_pywebsocket below)
- php
- php-mysql
- bind-utils (provides nslookup)
- gcc
- httpd-devel
- ntp
- ntpdate
- php-xml
- mod_python
- mod_pywebsocket (required for websocket operations)
- php_ioncube_loader

Optional/Helpful Software (Included in the Self-hosted Baseline Server Distribution)

- mlocate – Locate and update database

Security Overview

Note: Information about the specific security protocols that Baseline has implemented is available in the Baseline Security Controls Technical Specification found on the Baseline website.

- All IP traffic between the web-browser client and the Baseline server is encrypted.
- Firewall is established by Linux kernel IPTABLES (statewise). The only port essential to be opened is 443.
- Clients (browsers) are allowed to remain connected indefinitely or can be logged off and dropped.
- Controllers are able to connect to the IP address of a single assigned Baseline server (programmable).
- All data is stored on a local database server (mySQL). Traffic is internal only to 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.

Options for the Self-hosted Baseline Server

The self-hosted Baseline server is a full-function Linux based server. This server is available from Baseline pre-installed on a solid state server module based on the Intel™ Next Unit of Computing™ (NUC) hardware. The self-hosted Baseline server is fully web manageable and does not require a monitor or keyboard (a keyboard, monitor, and mouse are available as an optional purchase.) The system is designed to be a low power, high reliability server unit suitable for customers who do not have an existing rack-based virtual server environment, or for customers who do not wish to install AppManager or BaseManager on a managed IT server.

For those who prefer to use existing managed servers, the self-hosted server is also available as a virtual machine image suitable for installation in modern rack mount VMware® server environments. 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.

Software Updates and Technical Support

Software updates and technical support are available for a yearly fee per software package.

Remote installation support for the self-hosted Baseline server is available for a fee. Installation is limited to Baseline software only. Network configuration changes must be completed by site's network administrator.

On-site technical support is available for a daily fee plus travel expenses.

Please contact your Baseline sales representative for pricing.

For complete details, refer to the following Terms, Licenses, and Agreements on the Baseline web site:

- Support Services Agreement for AppManager, BaseManager, and BACnet Manager https://www.baselinesystems.com/support.php/bm2_ssa
- Self-Hosted AppManager, BaseManager, and BACnet Manager End User License Agreement https://www.baselinesystems.com/support.php/standalone_eula