

BaseManager Overview for Network Administrators

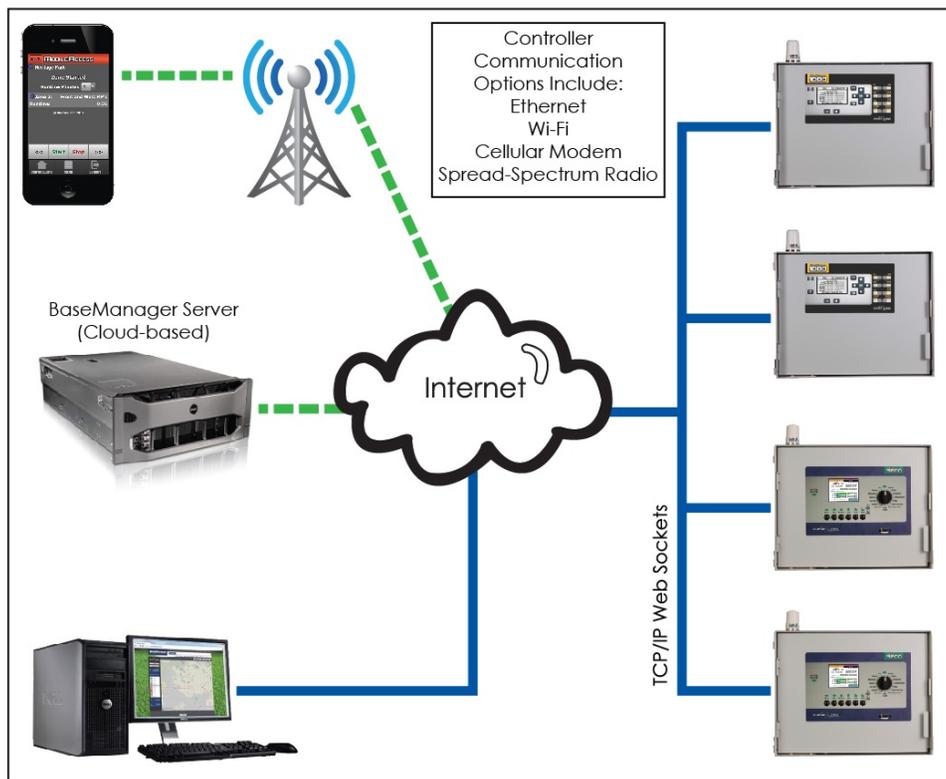
This document gives a brief overview of Baseline's BaseManager server. While the document is not intended to be a comprehensive description, it should help network administrators and other IT professionals understand the operation of BaseManager and address their own internal security concerns related to accessing the cloud-based server or hosting an instance of the server.

BaseManager Server Overview

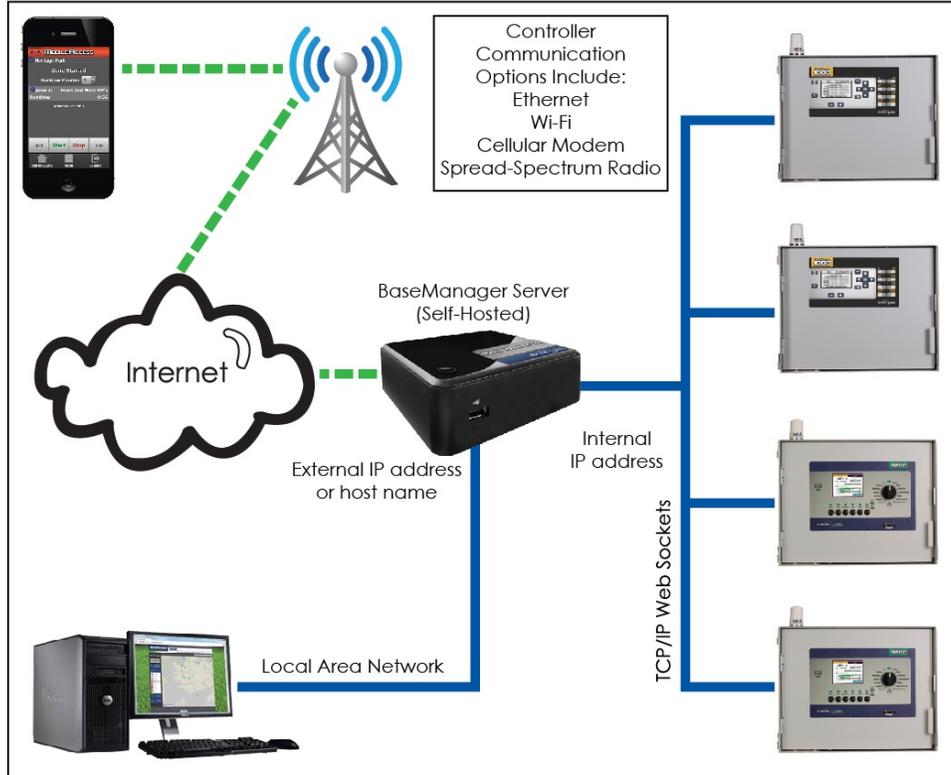
The BaseManager server enables users to remotely connect to and operate Baseline irrigation controllers. Users operate their irrigation controllers through a web-based (browser-based) interface, and the controllers are connected through web-based ports (HTML-5 standard, WebSocket Protocol).

All traffic is TCP/IP with varying media types (cell, wireless, packet-radio) as needed 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 Cloud-based BaseManager Server



Network Topology Example for the Self-hosted BaseManager Server



Networking

All communication to and from clients (browsers) and controllers is done over SSL 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 allowed to use SSLv3. 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 BaseManager client application is a map interface. 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:

<http://en.wikipedia.org/wiki/Websockets>

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 SSL-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.

BaseManager Server Components

BaseManager servers are built on the CentOS 6 distribution unless otherwise specified.

The lists below specify the required and optional packages that are included by default in the self-hosted BaseManager server and the virtual machine server image.

Required Packages (Included in BaseManager 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 BaseManager distribution)

- mlocate – Locate and update database

Security Overview

Security measures common to cloud-based and self-hosted BaseManager

- All IP traffic between the web-browser client and the BaseManager server is SSL-encrypted.
- Firewall is established by Linux kernel IPTABLES (statewise). The only port essential to be opened is 443. Although, if remote administration is desired, port 22 should be opened.
- 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 BaseManager server (programmable).

Security measures specific to cloud-based BaseManager

- All data is stored on a database server (mySQL) that is not externally accessible other than through activities and reports available through SSL-encrypted web access.
- External access to the server is available using pre-shared keys by Baseline administrative employees only from known IP addresses.
- Controllers initiate all connections to the server and will not accept any external connections.
- The BaseManager server requires controllers to be authorized in order to connect to the server.
- The BaseManager server tracks and manages controller connections using the unique MAC address of each controller.
- The BaseManager server generates authorization PINs for controllers that are attempting to connect for the first time.
 - The authorization PIN is displayed on the controller's front panel.
 - Company admins use the authorization PIN to connect controllers to their company.

Security measures specific to self-hosted BaseManager

- 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 controls 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 SSL (https) port 10001. Webmin access can be disabled from external access (i.e., localhost only) or disabled entirely.

Hardware Options for the Self-hosted Server

The self-hosted BaseManager 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 BaseManager server is fully web manageable and does not require a monitor or keyboard (a keyboard, monitor, and mouse are available as an option.) 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 BaseManager on a managed IT server.



For those who prefer to use existing managed servers, BaseManager is also available as a virtual machine image suitable for installation in modern rack mount server environments. The BaseManager virtual machine requires a minimum of 4GB of RAM, 120GB of disk space, and an Intel i3 class processor or equivalent.

The BaseManager self-hosted server or virtual machine server can be fully managed via the built-in secure web server.

In order to allow mobile devices to access the BaseManager server, an externally accessible static IP address or hostname is required, and https web access to the BaseManager server will need to be enabled.

Installation Support, Ongoing Support, and Software Updates

All BaseManager software purchases include 8 hours of remote training and configuration support and 6 months of free software updates.

After the first 6 months, software updates and technical support are available for a yearly fee of \$1000. This fee covers software updates and remote technical support, as long as virtual private network (VPN) access or a similar remote access method that provides SSH/SCP access to the BaseManager server has been granted to Baseline Support.

Remote installation support for the BaseManager server is available for a fee of \$2000. 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 \$1000 per day plus travel expenses.

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

- Support Services Agreement for BaseManager, Mobile Access Advanced, and BACnet Manager http://www.baselinesystems.com/support.php/bm2_ssa
- BaseManager & BACnet Manager Self-Hosted Software End User License Agreement http://www.baselinesystems.com/support.php/standalone_eula