Security Features

PoolWarden / MiniWarden / SmarterPool

ControlOMatic
Automated Pool & Spa Solutions

The ControlOMatic controller models all include the same security features.

Controller

The basics of security is that sensitive equipment is installed in a protected area where only authorized personal have access. Controllers all have a lockable enclosure.

Passwords

Security Menu: There are 10 passwords and 4 password levels. The master password is the only one that can modify the passwords. The controllers do not have an operating system so there is no back door or sequence of button presses that can get around the password.

Forgotten Password: If you forgot your password ControlOMatic can provide a code to reset the passwords. The serial number is required and a check with the dealer to get the OK to provide the code. Each controller has a unique reset code so knowing the code for one controller will not clear the passwords on another.

Entered Password Resetting: When you enter the password you will have access to all appropriate menus for a period of time (typically 2 minutes, adjustable in the PoolWarden up to 17 minutes). When the display back light turns off, the password is reset and the password will have to be entered again. If you walk away from the controller after entering the password, the controller may be at risk for a couple minutes for someone else to access the controller. If that is a concern enter an invalid password to reset it.

Internet

A big feature of the controllers is the support for data collection (data server) and remote setup changes (direct connect).

Data Server: Data is sent to the server using FTP and this is in the direction from the controller to the data server. The data server sends nothing back to the controller and can't make any changes. The FTP method is standard and the data is around 100 binary bytes. This feature is optional, setting the Interval in the LAN/Data Server Setup menu to 00:00:00 will disable this feature. The controllers have no file structure and will not receive data over FTP. The data server has an SSL certificate and any stored information is protected. Visit https://www.poolwarden.com and click on the GoDaddy certificate at the bottom of the page for details.

Direct Connect: This allows any Internet connected device with a web browser to make a direct connection to the controller. This is for retrieving the controllers data, configuration, and making configuration changes including calibration. This is a big security concern and the following security features are included, this feature is also optional.

- **Passwords**: If the password security feature has not been entered (no passwords) then you can still make a direct connection but the main menu will not be accessible (where the configuration changes can be made). ControlOMatic has no back door and will need to be provided the password when asked for help.
- **Firewall**: The controller doesn't have to be available to the world wide web and can be setup for local access only. When making a path through the firewall, put it on an external port which will make it more difficult for hackers to locate.
- **Client IP Security:** If all of the above security items are not enough, the controllers also have an additional feature which does take some additional setup. Allows a connection from up to 10 specific IP addresses and disallows any connection if not on the list. There will be no response from the controllers for an invalid incoming IP address, not even an invalid page request. You must enter into the controller the IP address for the devices that you will make a connection from, and the controllers will only allow those connections. To disable the direct connect feature, enter 001.001.001.001 for the first IP address.
- **End Direct Connect:** When finished, press the Terminate link on the browser to reset the password. When an active session is in process the letter "R" will display in the lower right hand corner for remote access. The controller buttons are all inactive during the session and and passwords that are entered are hidden. If the terminate link isn't pressed when finished, then the remote session will remain active until the back light time finishes and the entered password resets.