

# Hunter®

 **Hydrawise™ Ready**  
IRRIGATION CONTROLLERS

## Hydrawise Software/App Owner's Manual



## Table of Contents

Table of Contents	2
Spectrum Router Bandwidth	3
AT&T Router Location	3
eero Mesh Network	4
Verizon Connection Issues	6
Comcast-Xfinity Router Connection Issues	6
Changing WiFi Channel in the Admin Tool	7
Changing WiFi Channel in xFi	7
Cisco Meraki MR52	7
Campus & Corporate Network Connection Issues	8

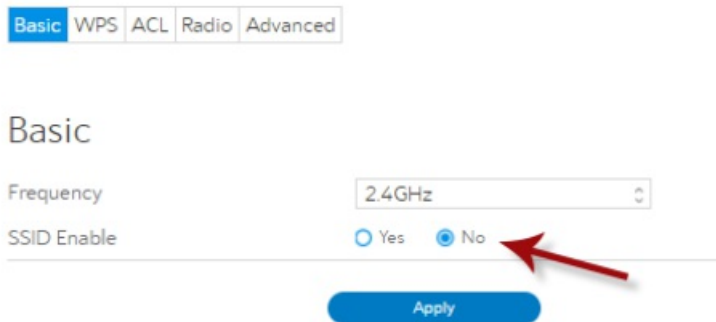
---

# Spectrum Router Bandwidth

The latest **SPECTRUM** routers are able to broadcast both 2.4GHz and 5GHz bandwidths. Hydrowise controller models operate on the bandwidth of 2.4GHz only. To use only the 2.4GHz channel, use the steps listed below.

1. Sign in to your Spectrum router account using your **ADMIN** credentials.
2. Under the **NETWORK** tab, select **WIRELESS**.
3. Under the **BASIC** tab, change the **FREQUENCY** to 2.4GHz.
4. Under the **SSID** selection, select **YES**.
5. Select **APPLY**.

For more support on your Spectrum router, visit their support section [here](#) <sup>[1]</sup>.



The screenshot shows the Spectrum router's configuration interface. At the top, there are tabs for 'Basic', 'WPS', 'ACL', 'Radio', and 'Advanced'. The 'Basic' tab is selected. Below the tabs, the 'Frequency' is set to '2.4GHz'. Under the 'SSID Enable' section, the 'No' radio button is selected, and a red arrow points to it. At the bottom, there is a blue 'Apply' button.

---

# AT&T Router Location

For optimum performance, AT&T highly recommends choosing a good location for the wireless router. When setting up the router, it should remain at least 3' (1 m) away from other wireless devices such as a Hydrowise enabled controller.

AT&T recommends the following as well:

- Install the router away from large metal objects such as metal racks and cabinets.
- Do not install it near other power sources. The power supply should be at least 6' (1.8 m) away.
- Install the router away from cordless phone bases or microwaves.
- Install the router vertically with nothing resting on or against it.
- Do not install the router in a closed area such as a cabinet or closet.

---

## eero Mesh Network

Eero mesh routers are compatible and successfully connect to all Hydrawise enabled controllers. The topics covered below can assist in controller connection challenges you might experience with an eero mesh network.

**Model:** All models

**Manufacturer:** eero

- Bridging Access Points
- Block From Network
- Naming Controller
- Reset modem and Router

### Bridged Access Points

Bridge your eero devices by using following the instructions below: **Bridged Access Points** - Mesh networks need to have their access points (AP) bridged so the IP allocation from the DHCP server match. This can be an issue with the IP the controller receives from the AP and DNS server which will cause the DNS to fail when doing a network test. [LEARN MORE](#) <sup>[2]</sup>

1. Open the eero app and tap **SETTINGS** (bottom right corner).
2. Select **ADVANCED**.
3. Select **DHCP & NAT**.
4. Switch your selection from **AUTOMATIC** (recommended) to **BRIDGE** or **MANUAL** (for those running static IP).
5. Click the **SAVE** button in the top right corner.



## Blocked From Network

If you notice a device that shouldn't be on your network, you can restrict it from accessing the internet by blocking it from the connected device list.

If you're using the iOS version of the app, tap on the **HOME TAB** to open the list of connected devices. You can tap on any device on this list, then scroll to the bottom of the menu that appears and select **BLOCK FROM NETWORK** to disable network access on that device.

Blocked devices will now appear in a new list that populates at the bottom of the home screen. You can tap on any device on this list to remove it from the block list, which will re-enable network access.

## Name Controller

The eero network may not allow unknown devices to connect. Please be sure to log in to the eero software and name the irrigation controller if this is the case.

## Reset Modem and Router

1. Unplug the modem and router for 2-3 minutes.
2. Plug in the modem and allow it to fully power up.
3. Plug in eero and let it power up.
4. Perform a soft reset on the eero device and allow to reboot.
5. Open the eero app (settings, troubleshooting, my device won't connect, my device is 2.4 ghz only, temporarily pause 5 ghz).
6. Reboot the controller and allow it to connect to the 2.4 ghz.

## Additional Troubleshooting Tips

- Perform eero router updates regularly using their app.
- If using a mesh network (multiple eero devices), use the eero app to check which eero device the Hydrowise controller is connected to. The controller may be communicating to an eero device that is NOT within range and you're unable to switch eero devices. Try a router reboot or temporarily change the SSID, then revert back to the previous name attempting to move the controller to the closest eero device.
- Power down all eero devices and leave one online to see if connection problems persist. This will confirm a mesh issue and the routers need to be moved closer to the controller.

## Additional eero Support <sup>[3]</sup>

---

# Verizon Connection Issues

## Verizon Connection Issues

If you receive a “password incorrect” message when using a Verizon router issue, we found that Verizon routers have a feature called **(SON)** Single Organized Network. Self-Organizing Networks (SON) can significantly improve Wi-Fi performance by automatically identifying and fixing Wi-Fi problems. This feature comes checked **OFF** when first installed. Once this service is checked back **ON**, your Hydrowise controller should connect without any issues at all.

Please follow the steps below:

1. Open MyFios App.
2. Select Wi-Fi settings.
3. Select Self-Organizing Network.
4. Turn SON **On**.

---

# Comcast-Xfinity Router Connection Issues

**Model:** Xfinity

**Manufacturer:** Comcast

The Comcast-Xfinity router by default has the Wi-Fi channels set to Auto. This may cause problems with connection to your Hydrowise controller. This can be easily fixed by changing the channel of your 2.4Ghz signal to channel 6. It is also recommended to change the bandwidth to 20/40. <

### Changing WiFi Channel in the Admin Tool

1. Connect to your WiFi network and access 10.0.0.1 from a web browser.
2. Navigate to **Gateway > Connection > Wi-Fi**, where you will see your private WiFi network name(s) displayed. If you would like to update your WiFi channel, click **EDIT**.
3. Mark the **Manual** radio button for the **Channel Selection** field, and choose your desired channel number in the **Channel** field.
4. To complete the change, click **Save Settings** at the bottom of the page.

### Changing WiFi Channel in xFi

1. Visit [www.xfinity.com/myxFi](http://www.xfinity.com/myxFi) <sup>[4]</sup> or open the Xfinity xFi app and sign in with your Xfinity username and password.
2. Navigate to the **More** section, where you will see your WiFi name(s) displayed (found under **Advanced Settings** in the xFi app).
3. Scroll down to **Additional Settings** and select **2.4 and 5 GHz WiFi**.
4. If you would like to select a specific WiFi channel, select **Edit** next to 2.4 or 5 GHz. A dialog window will appear.
5. Select the channel number from the **Channel** drop-down. To complete the change, select **Apply Changes** at the bottom of the dialog window.

# Cisco Meraki MR52

**Model:** Cisco Meraki MR52

**Manufacturer:** CISCO

**Device:** Wireless/Networking Business WAP “Wireless Access Point”

**Issue:** Due to the latest product and drivers not yet being supported, Hydrawise controllers are unable to connect to this wireless access point.

**Resolution:** You can log into the access point and will need to create a guest SSID. Choose to have a password or not password encrypted, make it a standalone 2.4 g connection, and set a WPA/WPA2 encryption. The controller will now connect to the cloud as it normally should. [Learn More](#) <sup>[5]</sup>.

---

# Campus & Corporate Network Connection Issues

## Campus & Corporate Network Connection Issues

In a typical corporate network, users will normally connect their laptops wirelessly to the internet using a username/password that comes from the organization’s Microsoft Active Directory servers. The protocol used for this is known as 802.1X authentication.

Utilizing username/password authentication for devices that don’t have a person logging into them each day is problematic for a number of reasons:

1. Devices such as printers, TVs and irrigation controllers won’t have a Microsoft Active Directory account so there is no username/password combination to enter on the device
2. Most user accounts have a password expiration policy meaning that you’d have to go to each of your wireless devices and change their password each time your password expires
3. Devices such as irrigation controllers are typically installed in secure locations and can be hard to reach. For example, your irrigation controller has a locked door and may be installed in a basement or plant equipment room.

Most devices such as printers, TVs, and irrigation controllers do not support 802.1X authentication for the reasons outlined above. With wireless-enabled devices becoming common, we are often asked for best practice for securely connecting these devices to the



internet. There are a number of ways of securely connecting your irrigation controller to the internet.

#### **Use a Wi-Fi 4G Hotspot**

Bypassing the campus network completely is one method of gaining access to the internet. Wi-Fi 4G hotspots allow the controller to connect to a dedicated Wi-Fi network with the internet connection via 3G, 4G, or LTE network. Wi-Fi hotspots (also known as Mi-Fi) are available from most wireless carriers such as AT&T and Verizon.

#### **Create a dedicated “device” wireless network**

Almost all corporate/campus wireless networks allow the creation of multiple wireless networks without the need to deploy additional hardware.

Follow these steps for setting up a security device network:

1. Using your wireless management software, create a new wireless SSID
2. Enable WPA2 encryption but make sure to disable 802.1X authentication
3. Choose a complex password for your new wireless network and enter this on devices that require access
4. Enable MAC address filtering on your new wireless network to allow only authorized devices (such as your controller) (optional)
5. Allow only access to the internet from your new wireless network (optional)