Routers and Internet Service Provider (ISP) Challenges

As Hydrawise continues to make the connection process as seamless as possible, we have seen some challenges with connecting our Hydrawise controllers to certain networks and devices. Please check from the list below to see if your device is in this category.

- Comcast-Xfinity Router Connection Issues
- Verizon Connection Issues
- Cisco Meraki MR52
- Campus Network Connection Issues

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 Hydrawise 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 [1] 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.

Verizon Connection Issues

If you are receiving 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 Hydrawise 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 "Off"

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 [2].

Campus 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)

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)