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)