IT Requirements and Notes

Requirements

DicksonOne is a network connected or IoT system consisting of data loggers and cloud-based software. Depending on your organizations IT requirements you may need to collaborate with your IT team to either ensure the system will work with your IT network or to configure the units to get on your network.

The IT infrastructure and environment varies drastically from one organization to the next. As such, if you have any additional questions please feel free to reach out to us for more information. Below are some answers to the most common questions and concerns from an IT perspective.

- Active internet connection (devices connect via WiFi or Ethernet)
- The devices communicate on either Port 443 (HTTPS and default) or Port 80 (HTTP)
- All communication is generated by the device – no opening of ports is necessary as there are no incoming commands/control/access for these devices
- The devices have a proprietary OS/firmware (NOT Windows CE, Linux, Android, etc)
- Devices support both WiFi and ethernet
- 2.4Ghz B/G/N network types
- Support WEP, WPA Personal, WPA Enterprise, WPA2 Personal, and WPA2 Enterprise
- TWEs are proxy aware while DWEs are not (coming soon!)
- Devices are not compatible with a captive portal without additional network configuration (whitelisting MAC addresses)
- Devices can be configured in either DHCP or as a static IP address
- If using DHCP, ensure the devices are allowed to receive their own IP addresses via your DHCP server
- If your organization utilizes MAC address filtering, the MAC address for each logger (both ethernet and WiFi devices) can be found via the Network Connection Widget
- If your company utilizes firewalls, web filtering, or proxies ensure they are not blocking packets to or from DicksonOne.com
- If your facility uses multiple access points with the same SSID and security key to cover a large area, ensure the following: the device's encryption type set to Auto Select and the security keys are identical; we highly recommend that any two access points within range of one another are configured to use channels that do not overlap one another

Backup Data Independently from DicksonOne

While DicksonOne does have adequate backups and redundancy in place, some DicksonOne users desire the ability to backup their organization's data independently from DicksonOne. Organizations seeking this functionality can leverage the DicksonOne's REST API to integrate a backup solution of their choice. If you have developers and other IT staff who are familiar with and capable of working with REST APIs, you can utilize the documentation found here at https://www.dicksonone.com/api/rest/docs#api-reference

IT Requirements and Notes

WiFi Access Points

If your facility uses multiple access points with the same SSID and security key to cover a large area, ensure the following: the device's encryption type set to Auto Select and the security keys are identical. We highly recommend that any two access points within range of one another are configured to use channels that do not overlap one another.

Most access points have a limit to how many devices can concurrently be connected. This varies, but is often as few as 25. Consider laptops, cell phones, equipment, loggers, and any other devices that may be connected to an access point.

First generation (black cases) DicksonOne loggers are compatible with wireless B networks. Your access points must be configured to Wireless B or utilize a compatibility mode. DicksonOne enabled touchscreens and generation 2 DicksonOne loggers (late 2015) are compatible with B/G/N wireless networks.

First Generation Devices

The first generation can only communicate via HTTP port 80 and even though port 80 may be open and allow traffic out, DicksonOne.com responds with xml packets that are often blocked regardless of port 80 being open. The loggers must be able to send and receive information to/from the DicksonOne site in order to function properly.