TCS Basys Controls®

QD/QWL Series Security and Functionality

This document provides information on the communications and security functionality of the QD/QWL Internet Communications Gateways (client devices) and the Ubiquity Web-based Application (Ubiquity).

Introduction

Ubiquity™ from TCS Basys Controls is the web-based application that accepts communications and data from the QD/QWL Internet Communications Gateways (client devices) over the Internet.

Ubiquity aggregates near real-time site monitoring/controls data and trended point data collected from the thermostat and controls network (e.g., HVAC, lighting, refrigeration, etc.) at individual sites. The web-based application creates a secure, centralized location for monitoring, programming, scheduling, and report generation for an entire multiple-site enterprise.

Each client device and Ubiquity communicate using a passive polling model based entirely on the HTTP/HTTPS protocol. The client devices initiate all communication out through the Internet to the Ubiquity server cluster. No active listening ports are forwarded or opened on the client device that might create a security vulnerability. Additionally, each client device may be completely firewall-secured from the outside Internet and the internal network. Supported HTTPS encryption allows for operation through corporate web proxies.

The TCS controls network communicates directly to the QD/QWL device over either an RS-485 serial wired network or a ZigBee™ wireless network. The only IP communication is between each client device and Ubiquity. All other communication may be blocked.

Design & Security Measures

The Ubiquity Web-based Application and operating code inside the QD/QWL Series devices are built upon the TCS Framework. This framework utilizes industry-standard open source applications and protocols wherever/whenever possible. This includes use of the Linux operating system for both hosting of and processing on the Ubiquity Web-based Application and the QD/QWL devices.

The development and release cycle is handled in-house including rigorous testing and validation of internal code and third party applications. The software and hardware engineering teams work in concert across a uniform development platform to streamline interoperability and maintain up-to-date security, software, and firmware updates.

Security & Redundancy

The Ubiquity server cluster is securely housed in a Tier 1 data center with failover capability to a secondary location in the event of a catastrophic failure. Individual servers in the cluster are redundant and all database and program data are regularly backed up. TCS maintains

99.9% Ubiquity uptime. Enterprise trended data is maintained for a minimum 90 days on Ubiquity.

In the event a QD/QWL device loses Internet connectivity to Ubiquity, service at the location is not affected. The device will store all polling data and programming settings locally until the device can reconnect to Ubiquity at which time locally saved data is transmitted over time.

Passive Polling Model

The passive polling communication model allows for a high level of security and straight-forward installation at each site.

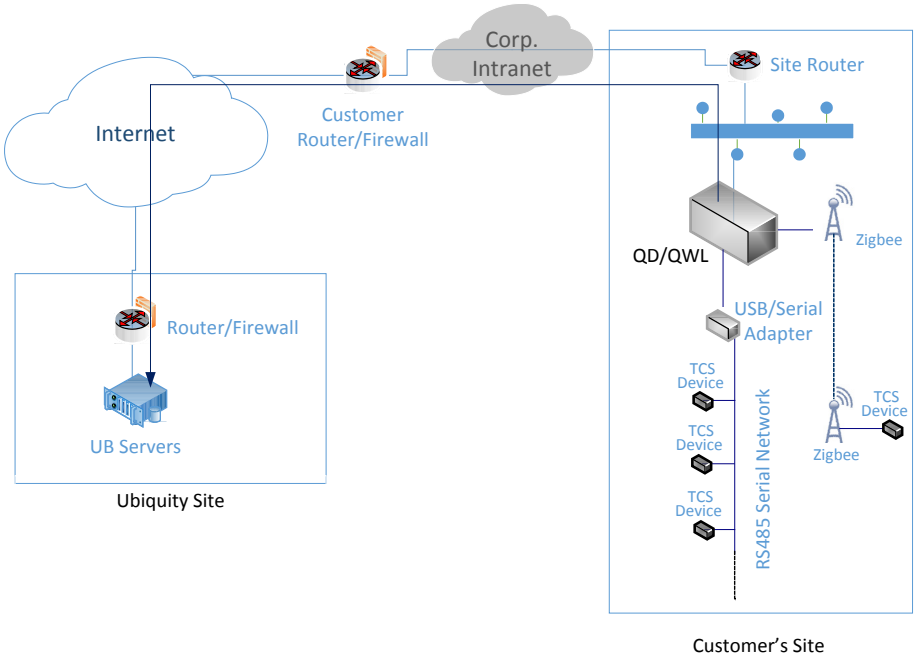
On an adjustable 60-second cycle, the client device originates a one-way web request to www.ubiquitysystems.net. All information to and from the QD/QWL client device is sent and retrieved via standard HTTP GET and POST commands. The device transmits any data or changes that are stored from the controller network to Ubiquity and asks www.ubiquitysystems.net for any changes made on the web-based application intended for the local controller network. www.ubiquitysystems.net expects regular device-initiated requests and displays the last time it communicated with each site. If a device fails to communication with Ubiquity for 24 hours, Ubiquity will change the status of the site to “Extended Offline” in the web-based application and email an alert to the appropriate parties.

Passive Polling Model

Gateway - UB TCS standard communication

1. QD/QWL initiates communications with UB Server
2. Establish SSL Certificate based connection with UB Server (If customer IT allowed port 443 across customer’s firewall)
3. Push data over SSL or Hex encoded over HTTP (port 80)
4. UB Server replies over the established connection with updates as necessary.
5. Connection terminated by QD/QWL

- Ubiquity must wait until the site contacts it.
- No communication channels opened between customer’s QD/QWL and TCS support.
- Gateway communication is not tunneled.



FAQ

Bandwidth Requirements

Ubiquity requires a very small amount of network bandwidth during normal day-to-day operation. While the amount of data passed over the network varies slightly depending on the number of devices on the controls network itself, the average amount of data per polling cycle is 1.1kb.

Latency

TCS Basys Controls equipment can handle up to 5000ms (5 secs) of network latency.

Internet Connectivity

All QD/QWL Series devices can tolerate short interruptions in Internet connectivity. The devices can function autonomously, storing and maintaining polling data and programming settings when unable to communicate with the Ubiquity server.

NOTE: An extended outage of 6 days or more may result in scheduling errors and possible data loss.