BuildingCoach

BOCS (Building Operator Coaching Solution):

Installation Instructions and Cyber Security Plan

Table of Contents

BOCS Support Contact:

Intellimaton Support: 484-681-5490
William Macomber, Intellimation Technician: wmacomber@intellimation.net

BuildingCoach Program Contact:
Nora Sherman, CUNY Building Performance Lab: nsherman1@ccny.cuny.edu

BOCS Installation Instructions

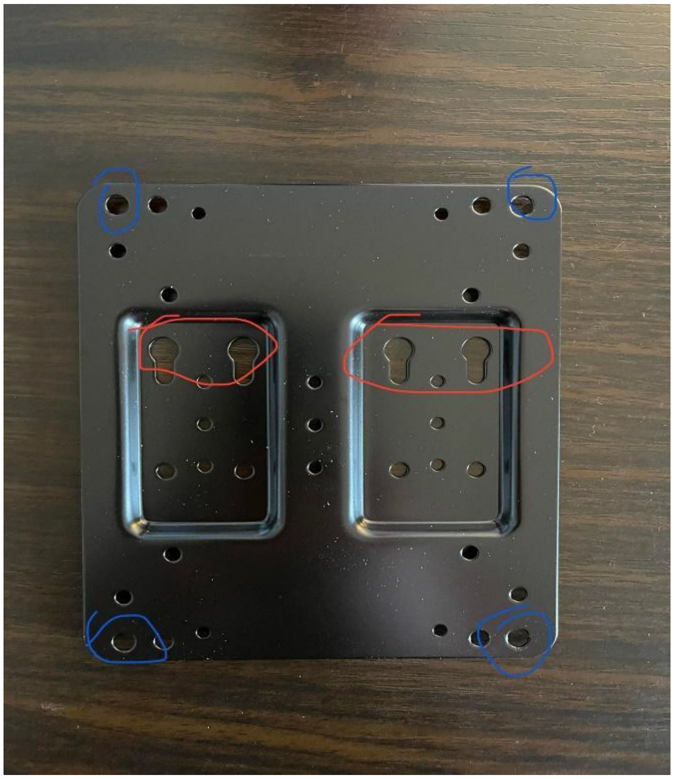
I. Introduction

The data collection box (BOCS) connects to your BAS/BMS via Ethernet and can discover all of the BACnet devices and their data points. It will then be set to trend the present value of a subset of these data points every 5 to 15 minutes. It will then push / send this data to a database in AWS (cloud). We will then normalize / standardize the data by adding tags to each point to better define the data. We will adhere to two industry standards, https://project-haystack.org/ & https://brickschema.org/ .

It is important to note that the BOCS talks BACnet only. If your BAS/BMS is or includes any legacy / proprietary protocols, BOCS will not be able to communicate with them. Typically, a gateway can be added to convert almost any legacy / proprietary devices to BACnet. This has many advantages, but comes with an additional cost.

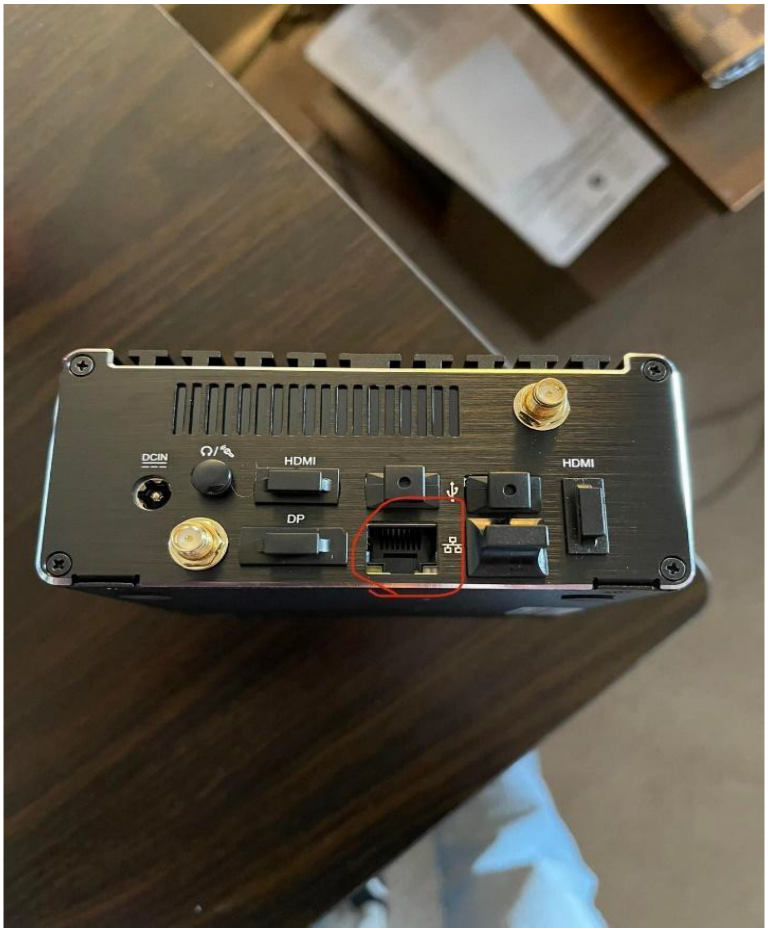
The BOCS will require 120 VAC power, an Ethernet connection to the BAS/BMS, and a path to the Internet. If your BAS/BMS is already on the IT infrastructure, it probably has a path to the Internet. If the BAS/BMS is not on the It infrastructure, then we will need to add a wired or cellular Internet connection. Cyber security is covered in a separate document.

The BOCS can be installed / mounted inside an existing BAS/BMS panel or near the BAS/BMS workstation PC. It comes with a mounting bracket that can be used if desired.



II. Connecting the Data Collection Box to the Network

Find the ethernet cable that your local IT department has provided for you and plug it into the Data collection box box. Make sure that you plug it into the ethernet port marked in red in reference image D. We have preconfigured the boxes to have the appropriate IP address and subnet mask prior to shipping them, so the box should be working once you power it on. The power button is located at the top left corner on the front of the Data collection box, just above the COM port.

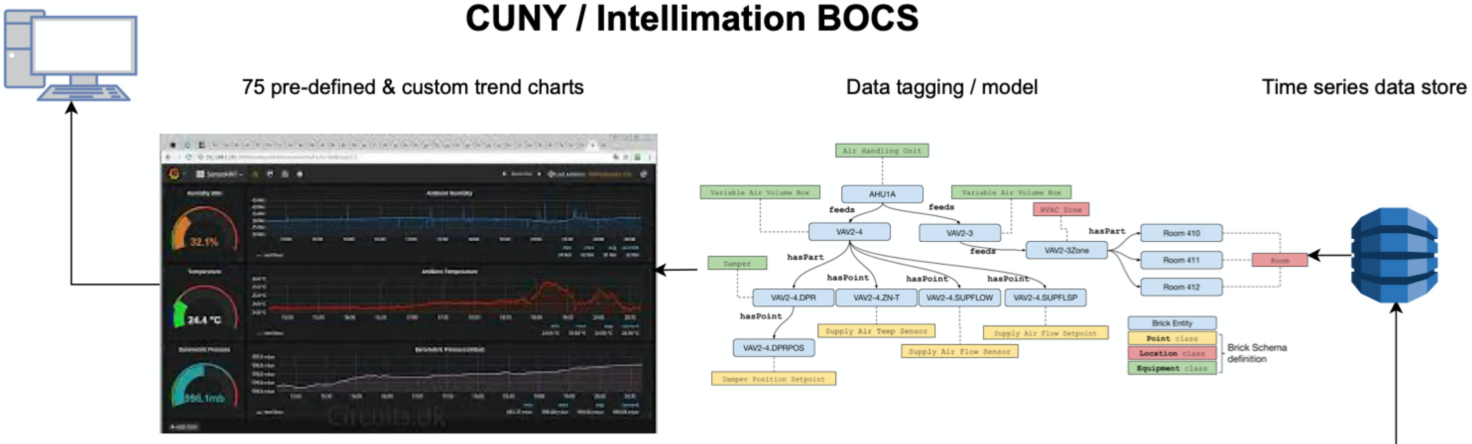


III. Testing Your Data Collection Box for Proper Operation

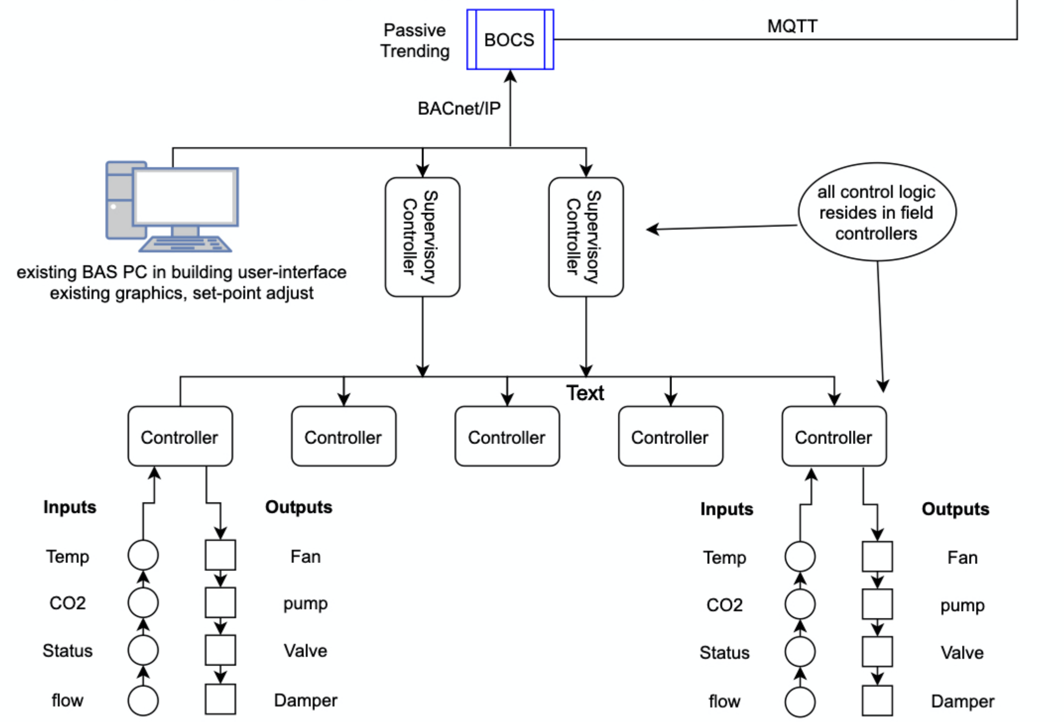
Once connected, call the Intellimaton support at 484-681-5490 to verify that we can see the BOCS is online. You are done. We will take it from here.

CUNY / Intellimation BOCS

Cloud Platform



Existing Building Automation System



Supervisory Level

Supervisory logic, alarm logic, scheduling resides here. There are 1 to 5 of these / building

Equipment Controller Level

Programmable controller for a piece of HVAC equipment or system. Most control logic resides here. There are a hundred of these / building

Sensor & Actuator Level

Inputs (sensors) and outputs (actuators) wired to equipment level controllers. There are a thousand of these / building

CUNY / BOCS Cyber Security Plan with Firewall

I. Introduction

This plan implements the use of Defense in Depth (referenced as DiD going forward). Our main focus was how to connect the data collection box for trending (the clients) to our MQTT broker without leaving vulnerabilities that could be exploited for malicious purposes. There will be a section of this document dedicated to the definition of terms that are used throughout this document. We are taking a layered security approach that utilizes a multi-pronged approach to security through the use of certificates, credential management, modern encryption standards, and strategic placement of equipment on the network.

II. Credential Management

Each box will be fitted with a username and password that will be used to allow the client to connect to the MQTT broker. These credentials are sent plaintext, so we will be using a TLS 1.2 certificate to encrypt them in transit. There are no practically-applicable attacks that have been created to work against TLS 1.2, so this is the standard we have chosen to go with. TLS 1.0 and 1.1 can be mitigated, so we will **not** be using these as a standard.

III. Password Requirements

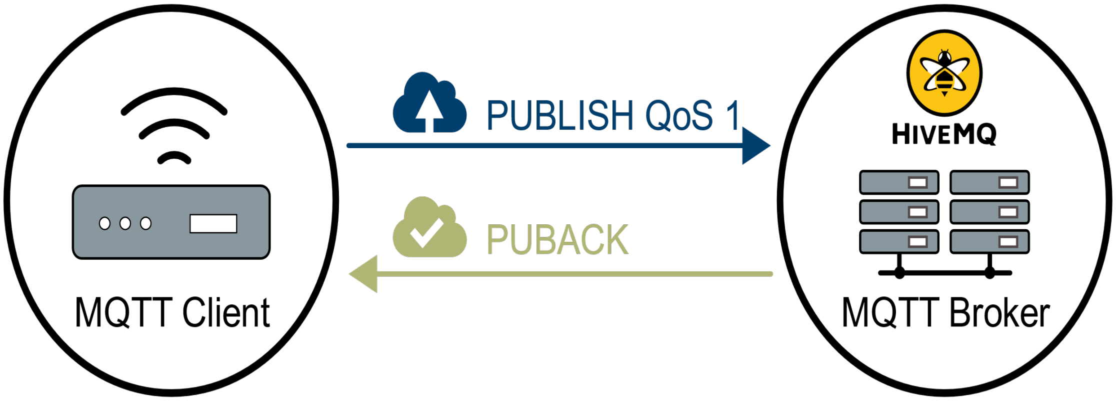
The passwords used by the clients will be changed every three months, or as often as the customer would like, in accordance with this cyber security plan. No special characters will be used in the password standard as MQTT struggles with non-ASCII character codes. This implementation will lower the probability that the client and broker have communication issues down the line.

IV. Security Certificate Creation and Management

Intellimation will create and utilize a server certificate on each data collection box. The certificate will be the same across all the data collection devices. This certificate will be similar, but not an SSH specific certificate**.** This will be a server certificate that allows the server to recognize clients. No Certificate Authority (CA) will be used for this process, and because the MQTT broker is public-facing, this is a requirement to secure the broker and the communications to and from it. The purpose of the certificate is to prevent Man-In-The-Middle attacks.

V. Quality of Service

We are planning to implement a Quality-of-Service level of 1 to our communications between the MQTT broker and the client. This guarantees that the message will be delivered at least one time to the receiver. The client stores the message until it gets a PUBACK packet from the receiver that acknowledges the receipt of the message (data). It is possible for the message to be sent and delivered multiple times. See below on the next page for a diagram on how QoS 1 works.



VI. **Box Access (Option 1)**

The trender will have a VPN certificate and the customer will provision a connection from that device to our VPN server in the cloud via ports 443/1194.

Box Access (Option 2)

The primary model for accessing the boxes will be to VPN into a bastion computer on the customer network, and from there we will be able to connect to the boxes. Access management for our employees will be determined by governing IT documentation and practices at the customer level. Each customer will have different access management policies that we will adhere to as necessary.

The VPN software used will be an enterprise level version of OpenVPN.

Box Access (Option 3 - No Remote Access)

Physical access is the third option for sites that do not allow remote connections. In this instance, we will have to fly somebody on site to physically troubleshoot the box.

VII. **Ports Used**

a. Port 8883 – This is the port used by MQTT for secure communication.
    i. Port 8883 (TCP/IP) is reserved with IANA for use with MQTT.
b. Port 8080 – This is the default HTTP port for the HTTP protocol normally used over a TCP connection. This port is reserved for the Normal Framework web interface running on the data collection boxes.
c. Port 9100 – This will be used for Prometheus.
d. Port 22 – This will be reserved for SSH.
e. TCP Port 443 – Outbound port for OpenVPN
f. UDP Port 1194 – Outbound port for OpenVPN

VIII. **OpenVPN Connection**

We are going to utilize OpenVPN access server (enterprise version) to give us the capability to SSH into the boxes and communicate with them directly and securely. Each box will have a VPN client and profile installed prior to its arrival to your site.

The OpenVPN Access Server covers four primary cases we are concerned with.

1. Provides users with secure access to enterprise servers in any environment, on-prem, or in the cloud.
2. Offers site-to-site connectivity using OpenVPN protocol-compatible routers to bridge different enterprise networks or public cloud environments.
3. Protects the remote desktop and screen sharing protocols with strong authentication and network access controls.
4. Enforces zero trust access through identity-driven policies, strong authentication, strict destination controls, and access control lists.

IX. **BACnet Security**

We do not plan to route BACnet traffic outside of the customer firewall. All of the data flowing outside the network will be encrypted via MQTT standards previously laid out in this document. Local IT departments are free to take steps to isolate BACnet traffic behind their firewall.

X. **VLAN Security**

Assuming that our infrastructure can be constructed in a VLAN environment, one option is building it on a private VLAN on a switch, with isolated ports. The isolated port option gives the customer the option to have complete layer 2 separation from all other ports within the same Private VLAN, except for the promiscuous ports. Promiscuous ports have the ability to communicate with all other ports within the private VLAN.

Most universities and hotels, places with a large number of users and network nodes, utilize private VLANs with isolated port configurations. Anything that we need our isolated ports to talk to can be put onto promiscuous ports, ensuring that the private ports will be able to communicate with them.

Cyber Security Definitions

1. Defense In Depth – A process in which multiple layers of security controls are utilized throughout an IT system.
2. MQTT Client – Any device (from micro-controllers to servers) that runs an MQTT library and connects to an MQTT broker over a network.
3. MQTT Broker – A server that receives all messages from the clients and then routes them to the appropriate destination clients.
4. TLS (Transport Layer Security) – This is the successor to the deprecated SSL standard. It is designed to provide communications security over a computer network.
5. Man-In-The-Middle attack – This is a cyber-attack where the perpetrator secretly relays and potentially alters the communications moving between two parties. In the case of our scenario, this would be the communications between the broker and the client.
6. Quality of Service (QoS) – An agreement between the sender of a message and the receiver of a message that defines the guarantee of delivery for a specific message. There are three levels to this, 0 (at most once), 1 (at least once), and 2 (exactly once).
7. PUBACK – This is a response to a PUBLISH packet with QoS Level 1. This packet has no payload.
8. Demilitarized Zone (DMZ) – A subnetwork containing an organization’s exposed, outward-facing services. IT acts as the exposed point to an untrusted network, commonly the Internet at large. The goal of a DMZ is to add an extra layer of security to an organization’s local area network.
9. Prometheus Software – A software application used for event monitoring and alerting. It records real-time metrics in a time series database built using an HTTP pull model,