O3 Sensor Hub 2.0

Hardening Guide

Edition 1.0

Delta™

CONTROLS

A Delta Group Company

Contents

Introduction

This document describes how to harden Delta Controls O3 Sensor Hub 2.0 (O3-HUB2) devices against unauthorized access and use.

It is expected that device configuration will be carried out by personnel trained in Delta software and systems, based on the requirements set out by the IT security policy. Accordingly, this document does not provide step-by-step configuration instructions for enteliWEB users. For more details, refer to enteliWEB's built-in help or go to help.deltacontrols.com.

The security practices described in this guide are recommended practices to securely configure O3-HUB2 devices. However, Delta Controls cannot guarantee that the implementation of the security practices or recommendations described in this guide will ensure the security of O3-HUB2 systems, or prevent or alter the potential impact of any unauthorized access or damage caused by a cybersecurity incident.

Related documents

- enteliWEB Network Hardening Guide
- KBA2252: Delta Product Security
- KBA2037: Securing enteliWEB using HTTPS

These documents are available on support.deltacontrols.com.

Overview of the O3 Sensor Hub 2.0

The O3 Sensor Hub 2.0 is an IoT device that communicates over Bluetooth® Low Energy, MQTT, and BACnet. Both BACnet/Ethernet and BACnet/IP protocol options are supported, but BACnet/IP and any associated IP services must be explicitly enabled by the user. We recommended using BACnet/Ethernet whenever possible and enabling BACnet/IP only when there is a need to connect multiple subnets over BACnet.

Enabling BACnet/IP enables the IPv4 stack, which includes ICMP, ARP, TCP, UDP default port 47808 (configurable), and DNS. DHCP is also available.

The sensor hub does not route and does not support BACnet BBMD function, so users cannot connect to it directly from a remote network.

Ports on the sensor hub

Port	Type	Description
68	UDP	systemd-network (network configuration service)
80	TCP	mosquitto (Paho internal webserver)
1883	TCP	mosquitto (internal MQTT broker)
42725	TCP	bnserver6 (BACnet server)

If enteliWEB is used as the BACnet front end, refer to the *enteliWEB Network Hardening Guide* for a list of ports on the enteliWEB server.

Hardening Steps

Upgrade device firmware

Upgrade sensor hubs to the latest firmware. You can upgrade the firmware in the O3 Setup app, over BACnet, or over MQTT.

- To upgrade the firmware over BACnet, create object **CSV43** with the name "Firmware Upgrade", command it to manual mode, then enter the following object value: **{**"version": *"FIRMWARE_VERSION"*, "url": *"FIRMWARE_URL"***}**.

    For example: **{**"version": "1.6.0-alpha.8", "url": "firmware.o3hub.com/download"**}**

- To upgrade the firmware over MQTT, publish **{**"data": **{**"version": *"FIRMWARE_VERSION"*, "url": *"FIRMWARE_URL"***}}** to **commands/fw/updateFw**.

Disable BLE

Using the O3 Setup mobile app, users can connect to the sensor hub over Bluetooth to write network settings, check diagnostic data, and upgrade firmware.

To secure the sensor hub against unauthorized writes over Bluetooth, disable Bluetooth Low Energy (BLE) communication on the hub.

- To disable BLE over BACnet, set object **BV31** ("Enable BLE") to **Off**.

- To disable BLE over MQTT, publish **{**"data": "0"**}** to **commands/object/bleEnable**.

If you want to keep BLE enabled (for example, to upgrade firmware using the app), change the BLE PIN to a unique 6-digit value for each job. You can change the BLE PIN in the O3 Setup app, over BACnet, or over MQTT.

Note: The new PIN cannot be 000000.

- To change the BLE PIN over BACnet, create object **CSV45** with the name "BLE PIN", command it to manual mode, then enter the new PIN as the object value.

- To change the BLE PIN over MQTT, publish **{**"data": *"VALUE"***}** to **setting/ble/pin**, where *VALUE* is the new PIN. After changing the BLE PIN, reset the sensor hub.

Change internal MQTT broker password

The sensor hub comes with an internal MQTT broker that allows users to write directly to the hub's configuration file. The default username/password is **user**/**admin**. To secure writes to the internal MQTT broker, you must replace the default password with a unique password. *It is important to do this even if you don't plan to access the hub over MQTT.*

The password is case-sensitive and must be between 5 and 31 characters in length. Special characters are allowed.

- To change the password over BACnet, create object **CSV46** with the name "MQTT Password", command it to manual mode, then enter the new password as the object value.

- To change the password over MQTT, publish **{"data":** *"NEW_PASSWORD"***}** to **setting/mqttPassword**, where *NEW_PASSWORD* is the new password.

After changing the MQTT password, reset the sensor hub. The new password does not take effect until the next reboot.

Use BACnet/Ethernet instead of BACnet/IP

Use BACnet/Ethernet whenever possible and BACnet/IP only when there is a need to connect multiple subnets over BACnet.

To disable BACnet/IP in enteliWEB, open the **NP6** object, select the **Out Of Service** checkbox, then click **Save**. The network change is applied immediately.

Disabling BACnet/IP closes all open ports.

Hardening Checklist

Use this checklist to harden O3 Sensor Hub 2.0 devices against unauthorized access and use. This checklist includes only the most critical tasks and does not aim to be comprehensive. You should constantly monitor and test your security plan for areas that need improvement.

☐   Upgrade the firmware to the latest build.

☐   Disable Bluetooth Low Energy communication (or, alternatively, change the BLE PIN).

☐   Change the password of the internal MQTT broker.

☐   Use BACnet/Ethernet instead of BACnet/IP whenever possible.

Document Revision History

Edition	Date	Author	Change Description
1.0	November 12, 2020	S. Clarke	New document.

O3 Sensor Hub 2.0 Hardening Guide
Document Edition 1.0