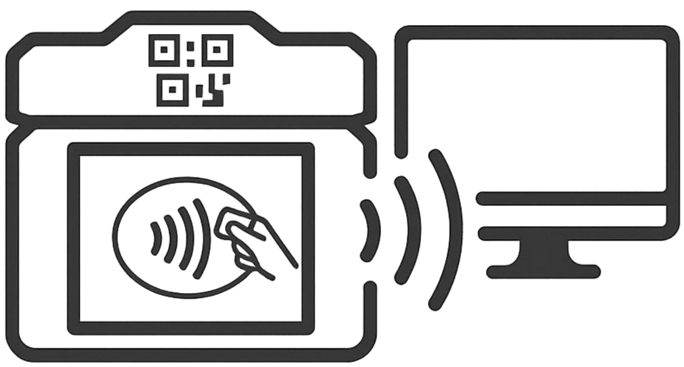
MagTek Demo Applications

Web HID-MQTT-WSS

MMS DEVICE USER GUIDE



October 2025

Document Number:
D998200713-100

REGISTERED TO ISO 9001:2015

MagTek I 1710 Apollo Court I Seal Beach, CA 90740 I Phone: (562) 546-6400 I Technical Support: (562) 546-6800
www.magtek.com

Table 0-1 - Revisions

Rev Number	Date	Notes
100	09/03/2025	Initial Release

Table of Contents

1.1 Introduction

This document provides instructions for using the browser-based **MagTek Demo Applications** to configure and test MagTek devices, including **MMS devices**, specifically the **DynaFlex family** (including DynaFlex, DynaFlex Pro, DynaFlex II, DynaFlex II PED, DynaFlex II Go and DynaProx, models).

The Demo Applications enable comprehensive testing of a wide array of capabilities, including core payment functions like EMV chip and NFC transactions, MSR reading, barcode scanning, and PIN entry. Note that **feature support is dependent on your specific device model**. For instance, the **DynaFlex II PED** model supports PIN entry, manual card entry, and signature capture functionalities.

⚠️ CRITICAL REQUIREMENT: For USB connected devices, these demos require a Desktop, Chromium Browser Only!

The MagTek Demo Applications rely on Web HID functionality for USB connected devices, which is not supported by mobile browsers (iOS/Android). You must use a desktop-based Chromium browser (like Google Chrome, Microsoft Edge, or Opera) for the demos to function correctly when using a USB connected device.

1.2 Demo Application Home Page

Upon opening the Web HID Demo home page, the Main Page is displayed. This page serves as the central menu and is organized into the following categories:

- **MMS Devices** – DynaFlex I/II device types and DynaProx (EMV, NFC, Barcode, PIN and MSR)
- **V5 Devices** – iDynamo, eDynamo, mDynamo, tDynamo (EMV, NFC and MSR)
- **V5 MSR/Manual Entry** – MSR swipe devices such as Dynamag and DynaPAD
- **V5 (SRED) Devices** – iDynamo 5 Gen III (MSR)
- **Magensa Services** – secure services for transaction testing
- **Miscellaneous** – configuration and GitHub source access

Each section provides a corresponding demo page with user interface elements for connecting a device, issuing commands, and reviewing results see **Figure 1.**

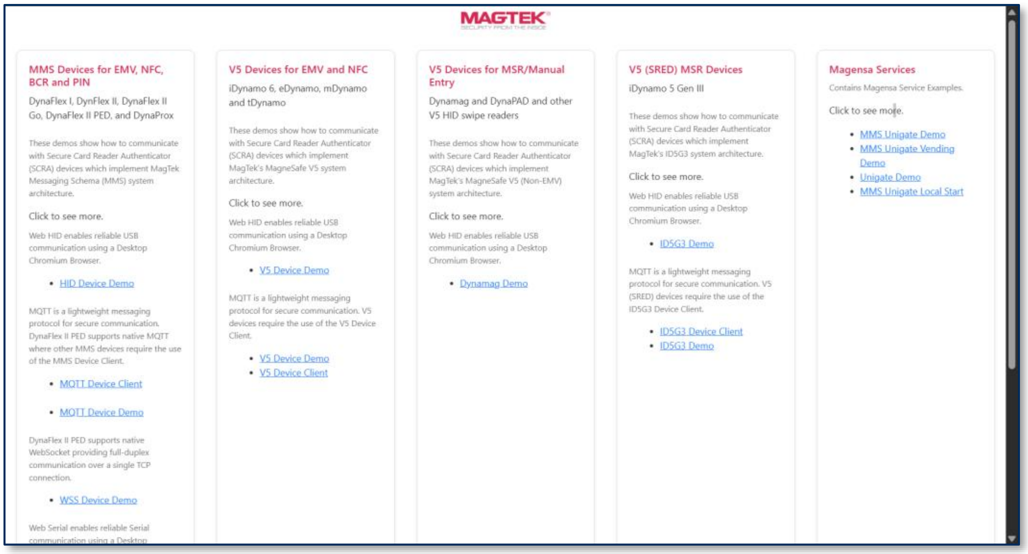


Figure 1 - Demo Application Home Page

1.3 MMS Devices

The MMS product family includes the following devices:

- DynaFlex/DynaFlex Pro
- DynaFlex II/DynaFlex II PED
- DynaFlex II GO
- DynaProx

Devices in this family generally support **EMV, NFC, barcode, MSR, and PIN functionality**, though specific features vary by model. The Demo Application connects through methods including **USB HID**, **WebSocket (WSS)**, **MQTT**, or **Bluetooth Low Energy (BLE)**, depending on the connection method enabled on your device.

1.4 Quick-Start Setup Guide

This checklist provides a summary of the steps required for configuring and running a demo with your device.

1. **Prepare Device:** Power on the device (if there is a power button) and connect it via USB, Wi-Fi, MQTT, or BLE.
2. **Open Demo Application:** Launch the Web HID Demo in a desktop Chromium browser.
3. **Configure Host App:** Be sure to enter **RMS, WebSocket, MQTT, and Contactless parameters** prior to using the various demos.
4. **Device Provisioning:** If using WSS or MQTT, provision the device's network and security settings (as outlined in Section 3).
5. **Open Session:** Select **Open** and confirm a successful connection.

6. **Send Command:** Choose a command (e.g., **Start EMV ALL**), paste command data if necessary, and select **Send Command**.
7. **View Results:** Swipe, insert, or tap a card, and observe the **transaction log** for the response and confirmation.

2 Essential Configuration: Connecting Your Device

For devices using **MQTT** or **WebSocket (WSS)**, configuring your host application and provisioning the device itself is mandatory to establish a successful secure connection. If connecting via USB HID, all steps listed in section 2 can be skipped.

Before using **MQTT** or **WebSocket (WSS)**, configuration is required. From the Demo Application Home Page, select **Miscellaneous → Configuration for the Demos**.

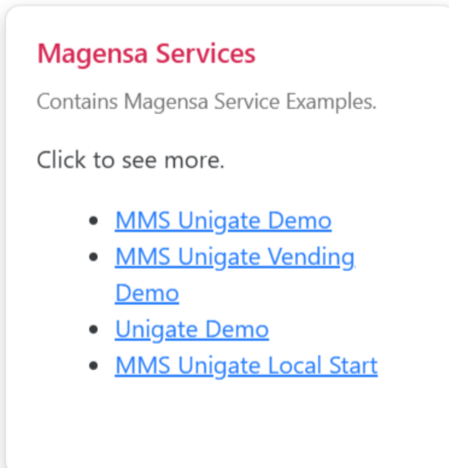


Figure 2 - Miscellaneous Configuration and Documentation Pages

2.1 Phase 1: Configure Host Application Settings

Configure the Demo Application by supplying the necessary API keys and server addresses.

1. From the Home Page, select **Miscellaneous → Configuration for the Demos**.
2. **Enter and save** the required settings.
    - **RMS Options:** Enter the Magensa API key and service URL.
    - **WebSocket Options:** Provide the WebSocket server address.
    - **MQTT Options:** Specify the Org Node, broker address, client ID, and user credentials.
    - **Contactless Options:** Adjust timing parameters for NFC operations.

Note: Configuration values must be entered and saved prior to establishing a secure session. Connection attempts without proper configuration will fail.

2.2 Phase 2: Provision Device for MQTT

The separate **MQTT Configuration** page is used to provision your physical device with its Wi-Fi credentials and MQTT broker details.

1. Connect your device via **USB HID**.

2. Open the **MQTT Configuration** demo page.
3. Select **Open** to connect to your device.
4. Use the **Wi-Fi Settings** section to enter the device's **SSID Name** and **SSID Password**.
5. Use the **MQTT Credentials** section to enter the **MQTT User**, **Password**, and **Org Node**.
6. Select **Save Config**.
7. The device will record these settings, allowing it to connect to your broker over the network.

Note: Configuration values must be entered and saved prior to establishing a secure session. Connection attempts without proper configuration will fail.

3 Using the Demo Pages

These instructions detail the operational steps once all necessary configurations (Section 2) are complete. If connecting via USB HID, the steps listed in section 2 can be skipped.

3.1 HID MMS Demo (Direct USB HID)

The **Human Interface Device (HID)** protocol enables **driverless plug-and-play** connectivity for your device via USB.

1. Ensure the device is powered on and connected via **USB**.
2. If this is the first time, you may have to **pair the device** in the Chromium browser, which involves granting the website permission via a pop-up prompt.
3. From the Demo Application, select **Open**, and choose the appropriate device. A **green check mark** confirms the device is successfully opened.
4. From the command dropdown menu, select a command such as **DynaFlex: START EMV ALL**.
5. Select **Send Command** to execute the action.
6. Insert or tap a test card and monitor the transaction log for the response.

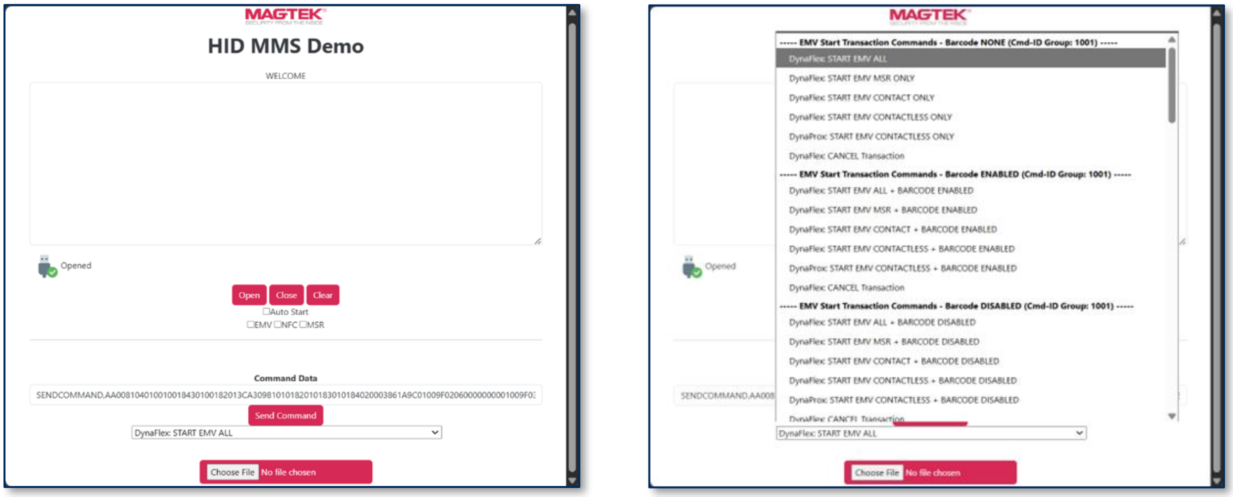


Figure 3 - HID MMS Demo

3.2 MQTT

Message Queuing Telemetry Transport (MQTT) is a lightweight messaging protocol commonly used for Internet of Things (IoT) applications. It provides efficient, reliable communication between devices and applications, even in environments with limited connectivity. **IMPORTANT: DynaFlex II PED is the only device that supports native MQTT**. All other Dyna Devices must use the HID MQTT Device Client.

Key characteristics include:

- **Publish/Subscribe model** – Devices publish data to a central broker; applications subscribe to receive data.
- **Low overhead** – Messages are compact and efficient, suitable for embedded systems.
- **Real-time updates** – Events such as card insertions are transmitted immediately to the Demo Application.
- **Cross operating system and cross browser connectivity:** MQTT ensures seamless interaction because it is platform-agnostic, meaning devices running Windows, Linux, macOS, or embedded OS, and applications running in different browsers, can all connect and exchange messages reliably.

Within the **HID MQTT Device Client** and **MQTT MMS Demo**, this protocol enables MagTek MMS devices (e.g., Dyna Family Devices) to securely communicate via MQTT across operating systems.

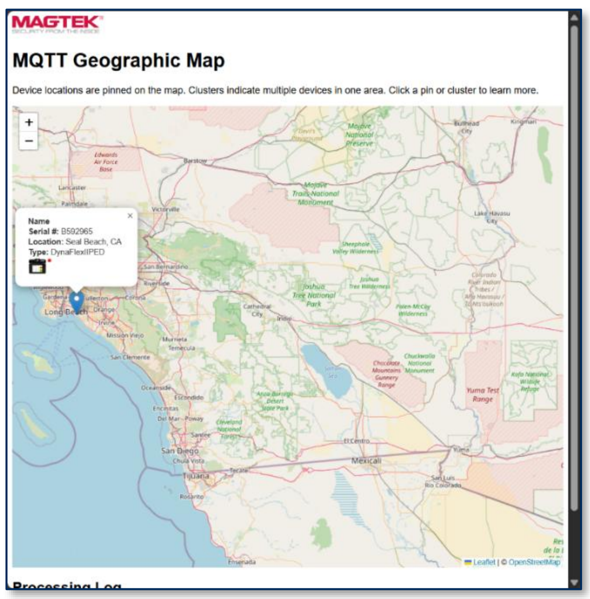


Figure 4 - MQTT Geographic Map

The MQTT MMS Demo serves as the control panel for MQTT-based device testing.

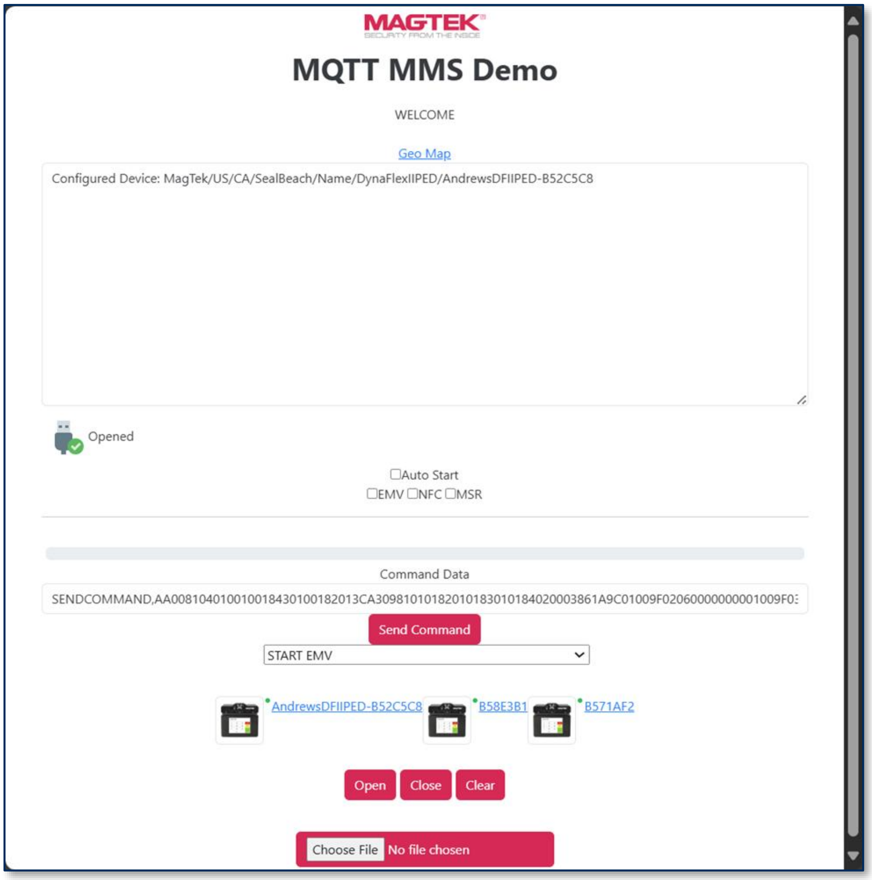


Figure 5 - MQTT MMS Demo

Components:

- **Configured Device** – Identifies the active device.
- **Status Indicator** – A green check mark indicates a successful connection.
- **Options** – Auto Start, EMV, NFC, and MSR session checkboxes.
- **Command Data** – Field for entering or pasting hexadecimal command data.
- **Controls** – Dropdown for pre-defined commands (e.g., **START EMV**) and **Send Command** button.
- **Device Instances** – Displays connected devices with selectable IDs.
- **File Upload** – Allows uploading of command scripts or batch test files.

Example Command Data (Hexadecimal): (Start Transaction command (arms Contact, Contactless and MSR interfaces))

```
AA0081040100100184301001820 13CA30981010182010183010184020003861A9C0100
9F020600000000001009F03060000000000005F2A020840
```

The command above, and others can be selected from the pulldown menu. The Choose File button allows the user to upload custom commands from a file. This screen also confirms device recognition, command formatting, and connectivity prior to further testing.

3.3 HID MQTT Device Client

The **HID MQTT Device Client** acts as a communication **gateway** that transforms your locally connected MagTek device (via USB HID) into a remote asset. This allows other applications to access the device securely via the **MQTT protocol**. **IMPORTANT: DynaFlex II PED is the only device that supports native MQTT which means it does NOT need to use the HID MQTT Device Client.**

1. Power on and connect the device via **USB**.
2. Open the **HID MQTT Device Client** page.
3. Select **Open** within the client.
4. Scan the QR code or select the provided link to open the separate **MQTT Device Demo Application**.
5. From the MQTT Device Demo Application's dropdown, select the required command, or use **Choose File** to upload a custom command script.
6. Select **Send Command** to execute the command remotely.

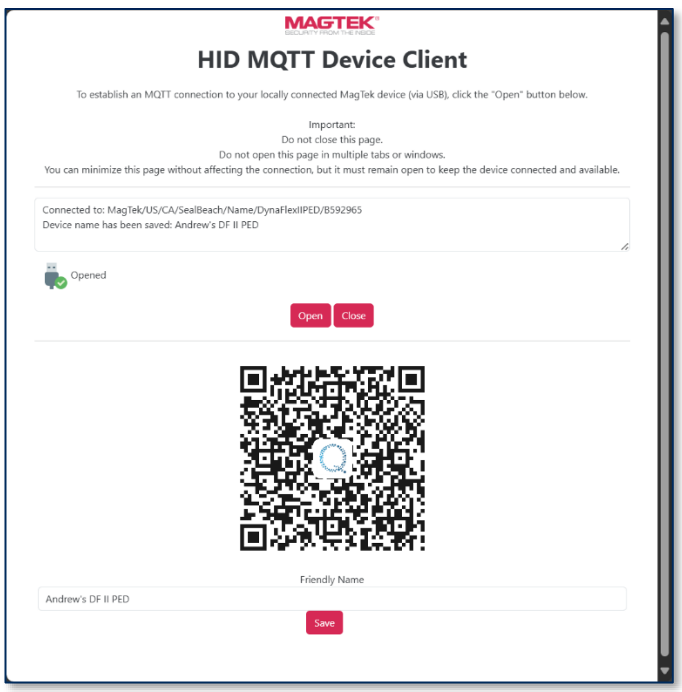


Figure 6 - HID MQTT Device Client

The **MQTT Geographic Map** displays device location and status for connected units, see **Figure** .

3.4 MQTT Configuration Page

The MQTT Configuration page provides controls and parameters necessary for device operation over MQTT.

- **Device Status Panel** – Displays device information (model, name, IP address, SSID) and records configuration progress.
- **Controls** – Includes **Open**, **Save Config**, **Reset Device**, **Close**, and **Clear**.
- **Wi-Fi Settings** – SSID and password configuration.
- **MQTT Credentials** – Org Node, username, and password for broker authentication.

Once configuration is complete and saved, the user may proceed to execute commands such as **Start EMV**. See **Figure 7 - MQTT Configuration.**

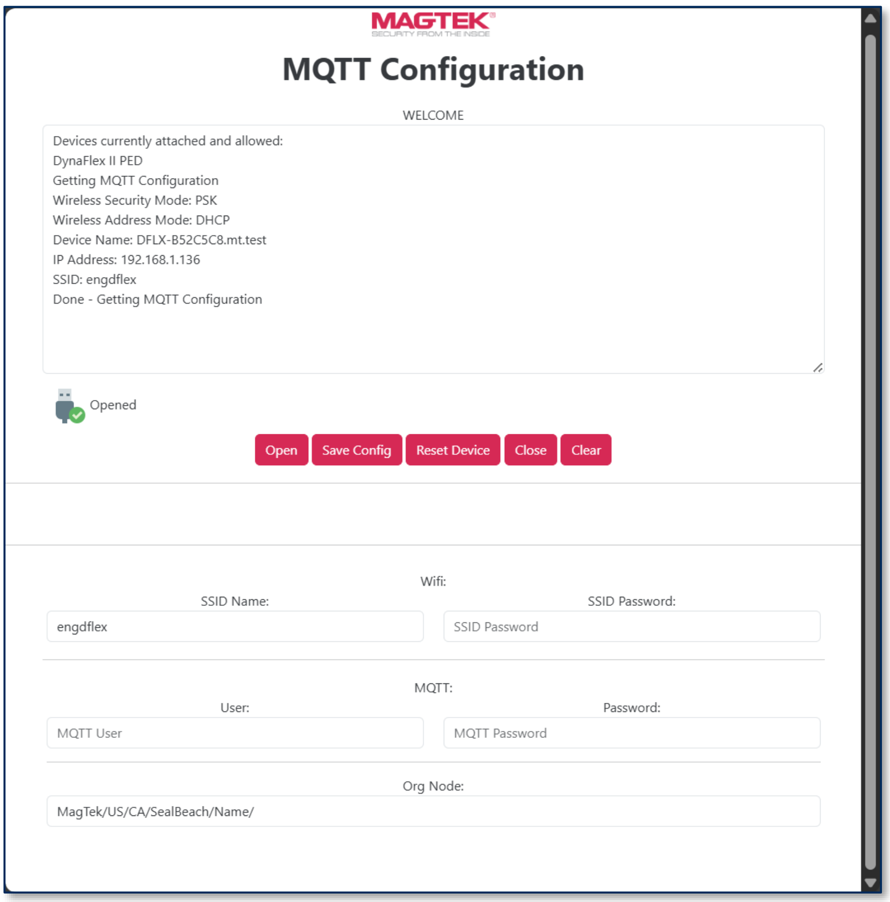


Figure 7 - MQTT Configuration

3.5 WSS Certificate and Trust

This interface is used to configure secure communication with WebSocket transport using TLS or mTLS. Functions include:

- **Network Settings** – Get DHCP and Set SSID.
- **Wi-Fi Setup** – Retrieve or assign SSID and password credentials.
- **Certificate and Trust Management** – Load TLS/mTLS certificates, verify certificates, and generate or sign Certificate Signing Requests (CSR).
    - For NonTLS connection,
        - Click **Load NoTLS Trust**
        - Next, reset the device.
    - For TLS/mTLS connections,
        - Click **Load TLS Trust** or **Load mTLS Trust**
        - Next, click **Get & Sign CSR**
        - Next, reset the device.
- **Controls** – **Open**, **Close**, **Clear**, and **Reset Device**.
- **Device Identity** – Display or update the registered device name and IP address.
- **Root CA Download** – Provides access to the root certificate authority file for verification.

Error Condition: If the status window displays *“OpenDevice No HID device selected or found”*, ensure the reader is connected via USB HID prior to attempting certificate operations.

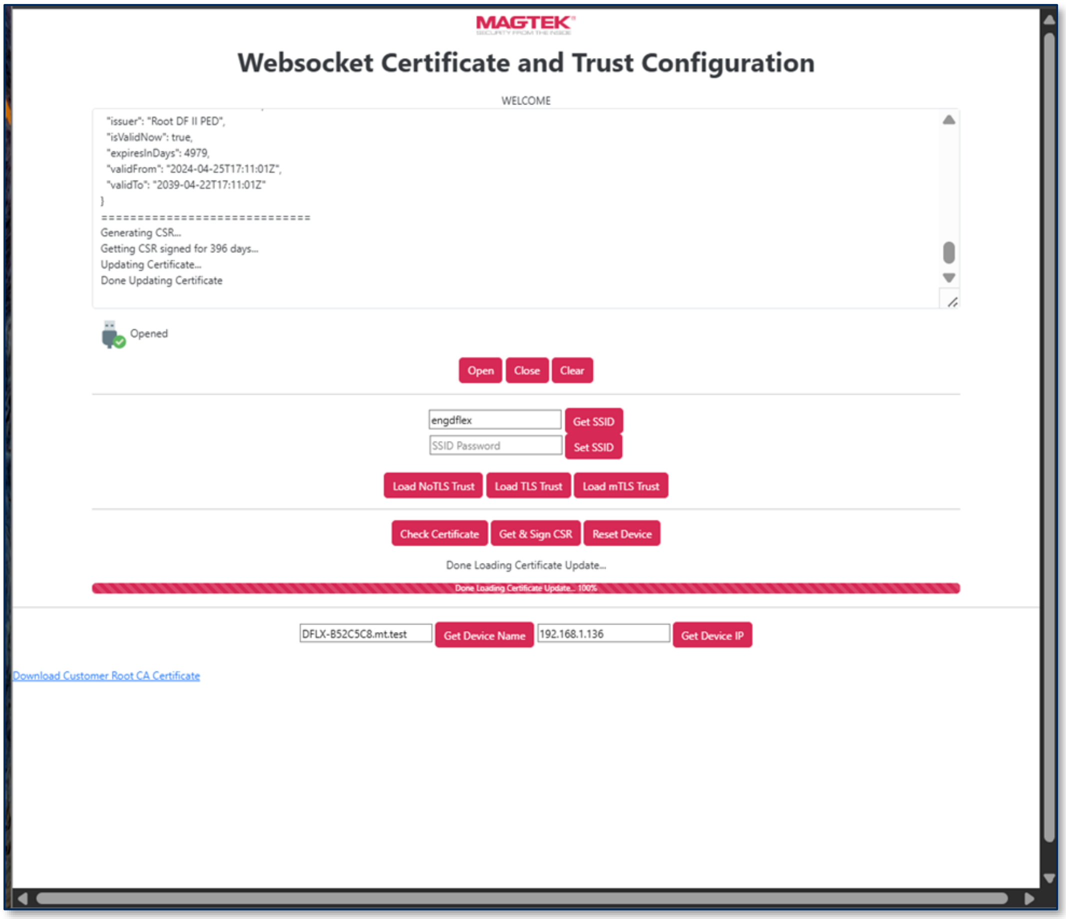


Figure 8 - WebSocket Certificate and Trust Configuration