



Livy Alive Webinterface

v0.2

- Confidential -

HU  **M**

Webinterface

Accessible from

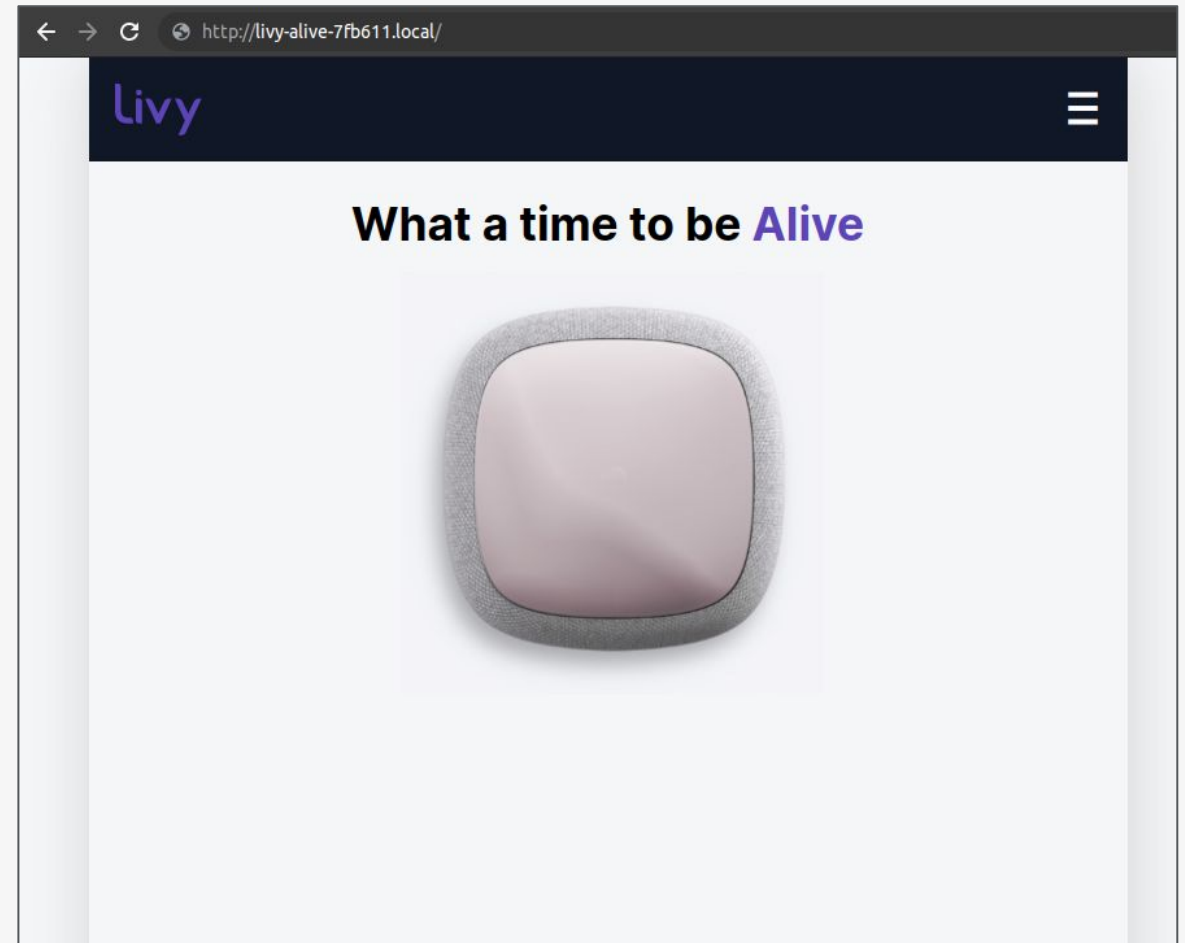
- any browser (Chrome, Firefox, etc.)
- on any device (Laptop, Smartphone, etc.)

From here on, this other device (Laptop, Smartphone) is referred to as:

Client

The Livy Alive Host is referred to as:

Alive



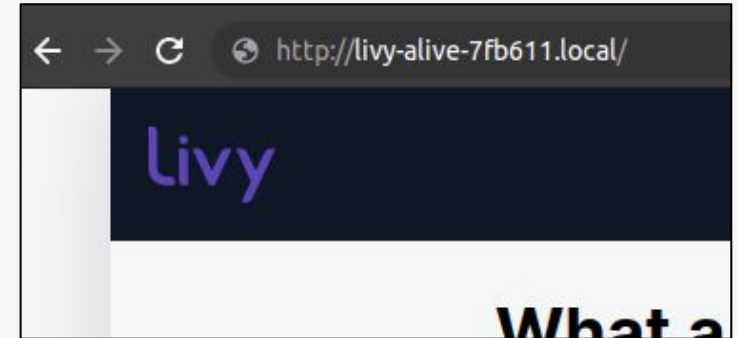
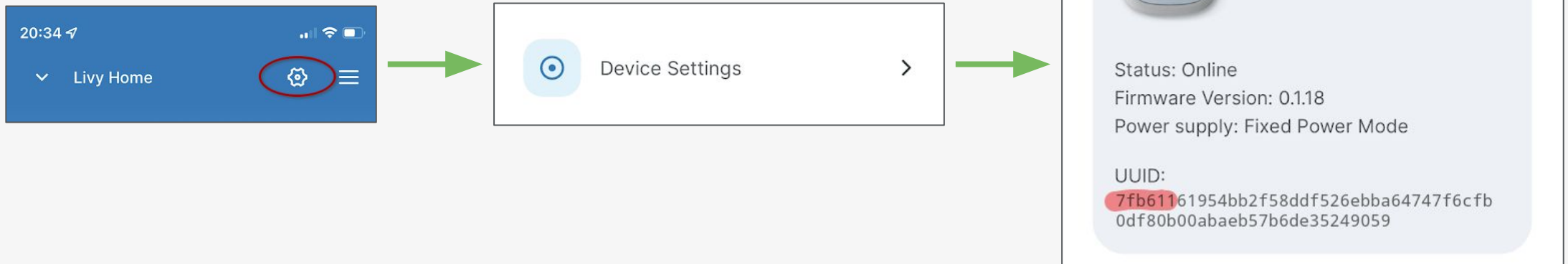
URL

Make sure **Alive** and the **Client** are in the **same** WiFi network.

The Webinterface can be accessed via the following URL:

```
http://livy-alive-<ID[6]>.local/
```

where **<ID[6]>** is the first 6 characters of the device UUID as found in the App under:





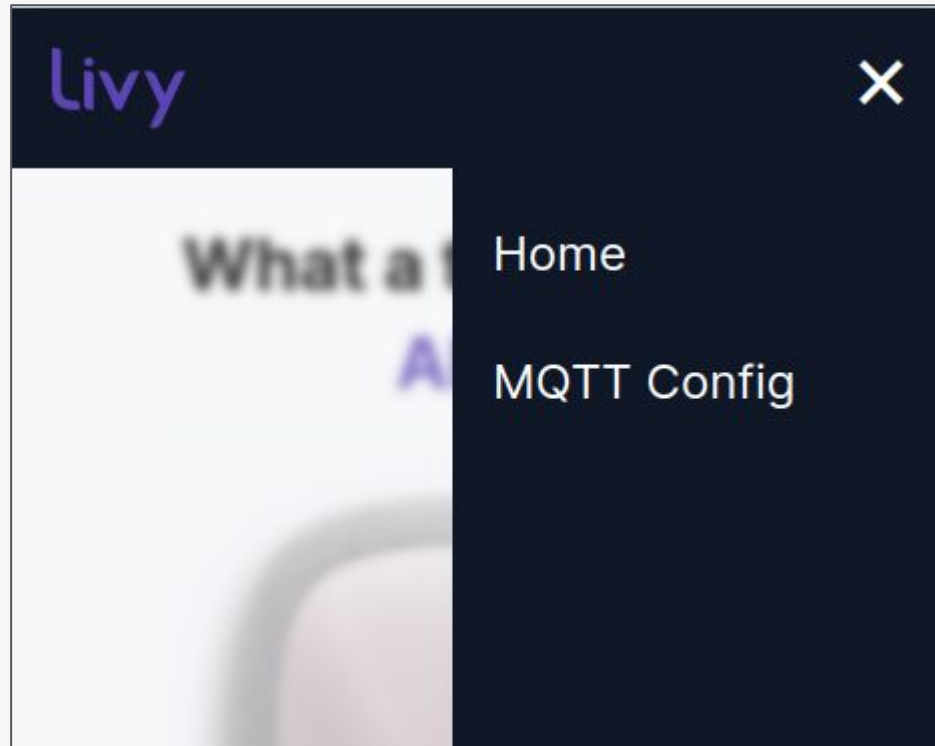
IP Address

Alternatively, the webinterface can also be accessed by entering the IP address of **Alive** in the local network, i.e.:

```
http://192.168.1.23/
```

MQTT Configuration

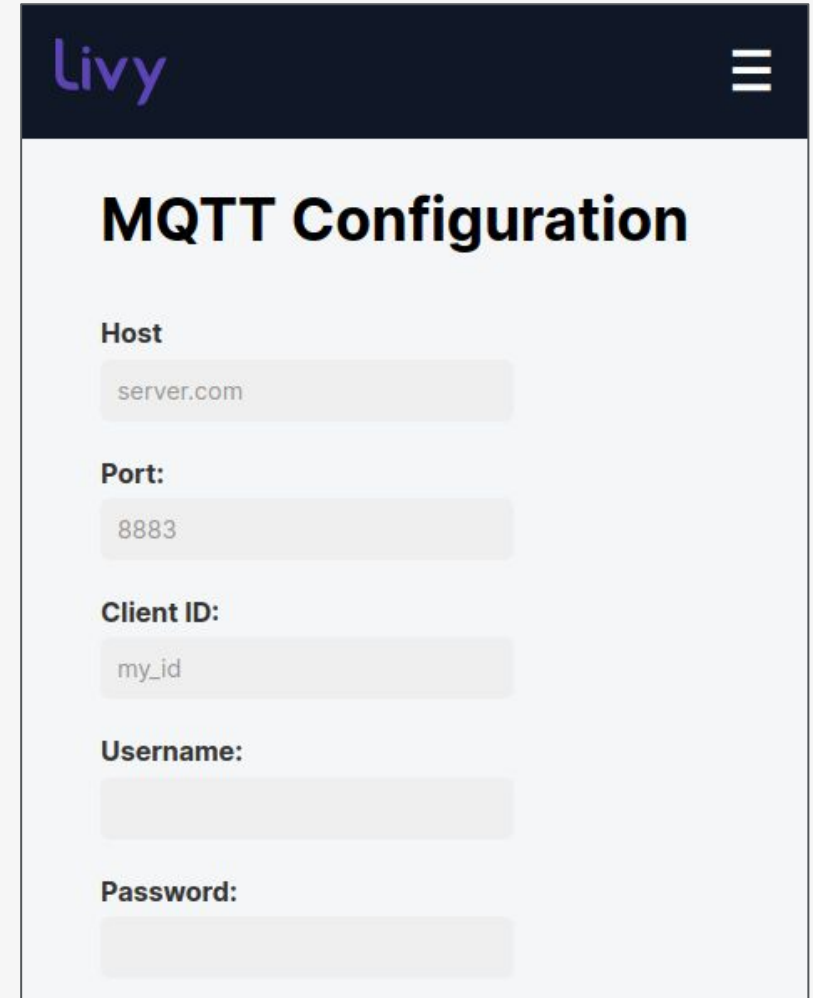
The MQTT broker can be configured via the Webinterface by navigating to MQTT Config.



MQTT Credentials

To set up the MQTT broker provide the following credentials:

- Host (as URL or IP)
- Port (typically 8883 for encrypted connections)
- Client ID (MQTT client identifier)
- Username
- Password



The screenshot shows the Livy web interface for MQTT Configuration. The header includes the 'Livy' logo and a hamburger menu icon. The main heading is 'MQTT Configuration'. Below this, there are five input fields with labels: 'Host' (containing 'server.com'), 'Port:' (containing '8883'), 'Client ID:' (containing 'my_id'), 'Username:', and 'Password:'. Each field is represented by a light gray rounded rectangle.

MQTT Certificate

Additionally a server certificate (for the MQTT broker) in PEM format must be provided, e.g.:

Server Certificate (in PEM format):

```
-----BEGIN CERTIFICATE-----  
QEFAAOCAQ8AMIIBCgKCAQEAESpAus9+l2eS1zdGF  
naW5nLibWJyb2tIMQswCQYDV  
QQGEwJCTTEPMA09/3eiJeJznNSOuNLnF+hmabAu  
7H0LT4K7EdqfF+XUZW/2jt537  
mZ28URKRYcvOUDGF9A7OjW7UfKk1ln3+6QDCi7X  
34RE161jqoaKfP67wJ93UW+gA  
wIBAgIJANHKOYazQG8drorw==  
-----END CERTIFICATE-----
```

TOTP Authentication

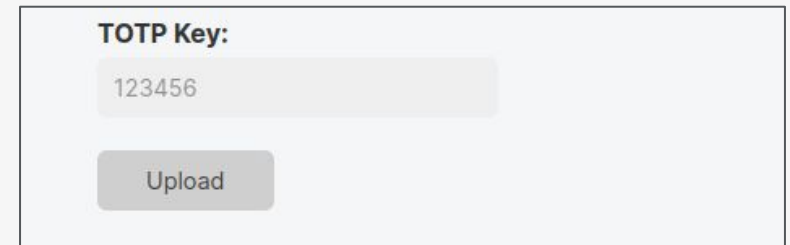
In order to submit the MQTT configuration form a **Time-based One-Time-Password (TOTP)** must be provided.

The secret (seed) for the TOTP is *unique* for every device and can be obtained from **HUM**-Systems.

The default configuration for the TOTP is

- 6 numeric characters in length
- 30 seconds timeout

This, however, may be subject to change in the future.



A screenshot of a web form for TOTP authentication. It features a label 'TOTP Key:' above a text input field containing the number '123456'. Below the input field is a button labeled 'Upload'.



Submit

After pressing “Upload” the **Alive** will respond with:

Success - Configuration has been accepted and the **Alive** will attempt to connect to the MQTT broker with the provided credentials.

Note: The connection might still fail if the provided credentials are incorrect.

Error - Some of the configuration data is faulty / could not be parsed.

Most often this will be due to incorrect certificates or incorrect TOTP.