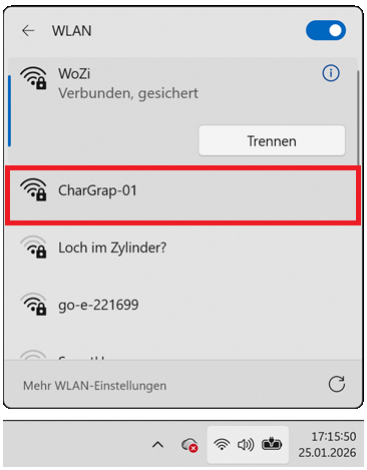
KARL KÜBEL SCHULE	**Chargraph** **- Firmware Update -** **(https://hedgedoc.karlkuebelschule.de/s/K4cE5zCoe)**	FIUO
26.01.2026 V01 rwd		Rainer Wieland

Update der Firmware

Der µController kann über FOTA mit neuer Software betankt werden.
Die akuelle Software haben Sie entweder selbst programmiert, oder von einer Quelle bezogen.
Es handelt sich dabei um eine .bin-Datei, welche auf den µController über WLAN oder USB hochgeladen wird. Der µController starten nach erfolgreichem Update neu und nutzt ab dann die aktualisierte Firmware für den weiteren Betrieb.

WLAN-Verbindung herstellen

- Versorgen Sie den µController über ein USB-Kabel mit Versorgungsspannung
- Verbinden Sie sich über WLAN von einem Endgeräte mit dem µController.



Sobald die Verbindung zwischen dem Endgerät und dem µController stabil aufgebaut ist, wechselt das Entgerät automatisch in das Captive-Portal.

Ein **Captive Portal** im FOTA-Kontext (Firmware Over The Air) ist ein Konfigurationsmechanismus für IoT-Geräte wie ESP8266/ESP32, der automatisch eine Weboberfläche öffnet, sobald Sie sich mit dem WLAN des Geräts verbinden.

Funktionsweise bei Embedded Devices

Das Gerät startet als Access Point mit eigener IP-Adresse (standardmäßig 192.168.4.1 beim ESP32). Ein DNS-Server leitet dabei **alle** Anfragen auf diese IP-Adresse um, sodass Ihr Smartphone oder Computer automatisch zur Konfigurationsseite weitergeleitet wird – ohne dass Sie die IP-Adresse manuell eingeben müssen.

Typische Anwendungsfälle

- **Erstkonfiguration**: WLAN-Zugangsdaten eingeben, ohne Display oder serielle Konsole zu benötigen
- **Firmware-Updates hochladen**: Neue Firmware direkt über die Weboberfläche flashen
- **Recovery-Modus**: Fallback-Netzwerk, wenn das konfigurierte WLAN nicht erreichbar ist
- **Geräteeinstellungen ändern**: Parameter anpassen ohne Code neu zu kompilieren

Technische Umsetzung (ESP32/ESP8266)

Sie benötigen drei Komponenten: einen Webserver (z.B. ESPAsyncWebServer), einen DNS-Server der alle Anfragen auf die Geräte-IP umleitet, und Handler die auf bekannte Captive-Portal-URLs reagieren (wie `/generate_204` für Android). Der `onNotFound` -Handler fängt alle anderen Anfragen ab und leitet auf Ihre Konfigurationsseite weiter. elliotmade (https://elliotmade.com/2021/09/01/esp-32-captive-portal/)

Sicherheitsaspekt

Im Gegensatz zu öffentlichen Hotspots dient das Captive Portal hier nicht der Authentifizierung von Nutzern, sondern als benutzerfreundliche Schnittstelle zur Geräteverwaltung – besonders praktisch für headless IoT-Projekte ohne physisches Interface. esphome (https://esphome.io/components/captive_portal/)

⚡ Die **Zugangsdaten** zum Captive-Portal von Ihrem µController erhalten Sie von Ihrem Betreuer.

Firmware-Update installieren (FOTA)

FOTA (Firmware Over The Air) bezeichnet die drahtlose Aktualisierung der Firmware von IoT-Geräten über Mobilfunknetze, WLAN, Satellit oder andere Funkfrequenzen – ohne physischen Zugriff auf das Gerät.

Grundlegende Funktionsweise

Das Update-Paket wird von einem zentralen Server (meist Cloud-basiert) an das Gerät übertragen. Das Gerät prüft die Authentizität des Updates durch digitale Signaturen und bestätigt nach erfolgreicher Installation, dass das Update funktioniert. Dies verhindert, dass manipulierte oder fehlerhafte Firmware installiert wird.

Drei typische Architekturen

Edge-to-Cloud

Das IoT-Gerät selbst hat direkten Internet-Zugang und empfängt Updates unmittelbar aus der Cloud. Diese Architektur ermöglicht gezielte Updates für einzelne Geräte oder Gerätegruppen, was besonders bei kritischen Anwendungen wichtig ist.

Gateway-to-Cloud

Ein zentrales Gateway mit Internet-Verbindung empfängt die Updates und verteilt sie an angeschlossene Geräte. Dies reduziert die Bandbreitennutzung und ermöglicht die Verwaltung von Geräten, die selbst keine Cloud-Verbindung haben.

Edge-to-Gateway-to-Cloud

Das Gateway lädt Updates herunter und leitet sie gezielt an verbundene IoT-Geräte weiter. Die Geräte benötigen weder eigene Internet-Verbindung noch leistungsstarke Mikrocontroller – sie kommunizieren nur mit dem Gateway.

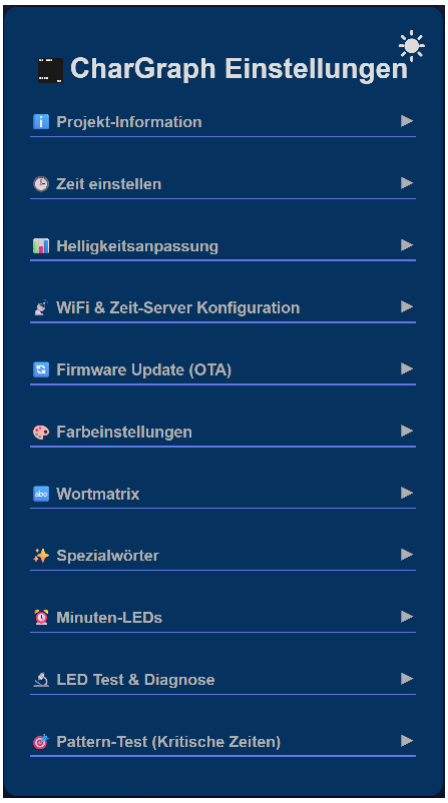
Vorteile für IoT-Systeme

FOTA ermöglicht es Ihnen, Sicherheitslücken zu schließen, neue Funktionen hinzuzufügen und Fehler zu beheben, ohne Techniker vor Ort schicken zu müssen. Besonders bei verteilten Gerätelandschaften (Smart Home, Industriesensoren) ist dies kosteneffizient und skalierbar. Sie können Updates zentral verwalten und gleichzeitig auf Hunderte Geräte ausrollen.

Automatischer oder händiger Browserstart

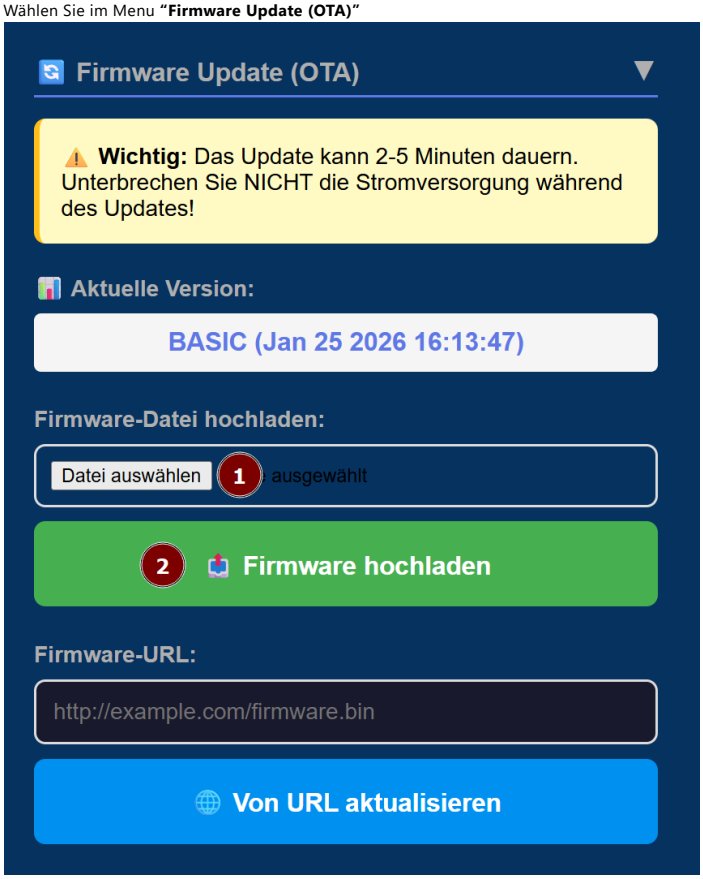
Sollte das Captive-Portal nach kurzer Zeit (weniger als 30 Sekunden) nicht automatisch am Endgerät sichtbar sein, müssen Sie möglicherweise die Freigabe für das Netzwerk erteilen (-1-), oder direkt auf die Webadresse gehen (-2-).

(*-1- Freigabe am Netwerk erteilen*)



(-2- Direkter Aufruf im Browser über die Webadresse http://192.168.4.1 (http://192.168.4.1))

- Wählen Sie im Menu **“Firmware Update (OTA)”**



- Wählen Sie die .bin-Datei an Ihrem Gerät aus (1)
- Starten Sie den Uploadvorgang mit “Firmware hochladen”