



# **Die Einrichtung der Hardware-Token der Firma MTRIX**

**zur Nutzung der 2-Faktor-Authentifizierung  
in WebUntis**

**(Stand: 01/2020)**

## Allgemeines

Durch die 2-Faktor-Authentifizierung werden die Sicherheitsanforderungen des Landes Baden-Württemberg, bei Nutzung eines digitalen Klassenbuches, erfüllt (vgl. [Netzbrief](#) vom Mai 2018).

Neben der bisherigen Kombination aus Benutzernamen und Passwort, ist bei der 2-Faktor-Authentifizierung noch ein zusätzlicher Code einzugeben, der nur eine kurze Zeit gültig ist. Diese Anleitung bezieht sich auf Hardware-Token der Firma [MTRIX](#). Alternativ können Sie noch Smartphone-Apps wie den Google Authenticator verwenden.

Zu den verschiedenen Methoden haben wir ebenfalls Dokumentationen bereitgestellt:

- [Einrichtung der 2-Faktor-Authentifizierung in WebUntis – für Administratoren](#)
- [Einrichtung des Google Authenticator – für Benutzer](#)

Bei der Bestellung der Hardware-Token der Firma MTRIX achten Sie bitte darauf, dass die Geräte den TOTP-Algorithmus unterstützen und einen Zeitintervall von 60 Sekunden programmiert haben. Die Verschlüsselung muss dem SHA256-Standard entsprechen.

## Einrichtung

Wenn ein Benutzer einer Benutzergruppe zugeordnet wurde, die die 2-Faktor-Authentifizierung durchführen muss, erhält dieser nach dem ersten Einloggen die Aufforderung, die 2-Faktor-Authentifizierung zu aktivieren.

1



Abbildung 1

Klicken Sie auf die Schaltfläche WEITER (siehe Abbildung 1), um die Einrichtung zu starten.

Im nachfolgenden Schritt wählen Sie die Methode SECURITY-TOKEN (HARDWARE MIT EINEM 021180 ONE-TIME-PASSWORD-(OTP-)GENERATOR) aus (siehe Abbildung 2).

**Zwei-Faktor-Authentifizierung - Aktivierung (1/3)**

Mit der Zwei-Faktor-Authentifizierung können Sie Ihren Benutzerzugang zusätzlich schützen.  
Eine Authenticator App am Smartphone oder ein Security-Token erzeugt einen Code, der beim Anmelden zusätzlich zum Passwort abgefragt wird.

Bitte wählen Sie

App Authenticator (z.B. FreeOTP oder Google Authenticator)

Security-Token (Hardware mit einem One-Time Password-(OTP-)Generator)

Zurück Weiter

Abbildung 2

Nachdem Sie die Methode ausgewählt haben, fragt der Assistent den sog. SCHLÜSSEL ab. Diesen erhalten Sie mit Ihrer Bestellung des Hardware-Tokens. und könnte folgendermaßen aussehen:

260871920009xx, D2C1FC8EB17AA1221CAA08246A8DB2F38ED0A1562FA6DA5243B8CD273C2698F, totp, 6, 60

Während der **erste Block** die Seriennummer des Geräts abbildet, gibt der **zweite Block** den SCHLÜSSEL an, den Sie in das gleichnamige Feld des Einrichtungsassistenten eintragen müssen (siehe Abbildung 3).

**Zwei-Faktor-Authentifizierung - Aktivierung (2/3)**

Sie benötigen ein Security-Token.

Bitte geben Sie den Schlüssel ein, den Sie zu Ihrem Security-Token bekommen haben. Wählen Sie bitte wenn notwendig die richtige Codierung (Base32 oder Hex) des Schlüssels.

D2C1FC8EB17AA1221CAA ✓

Kodierung

BASE32

HEX

Berechnungsverfahren

Standard (SHA1, 30s)

OTP c200 (SHA256, 60s)

Zurück Weiter

Abbildung 3

Nach der Eingabe des Schlüssels erkennt der Einrichtungsassistent die KODIERUNG und wählt selbstständig die Option HEX aus. Sie müssen lediglich noch das BERECHNUNGSVERFAHREN auf OTP c200 (SHA256,60s) einstellen (siehe Abbildung 3). Bestätigen Sie die Angaben anschließend mit der Schaltfläche WEITER.

Im nächsten Schritt müssen Sie das erste Mal einen BESTÄTIGUNGSCODE eintragen, den Sie auf Ihrem Hardware-Token angezeigt bekommen. Bestätigen Sie diesen dann mit der Schaltfläche Aktivieren (siehe Abbildung 4).



Zwei-Faktor-Authentifizierung - Aktivierung (3/3)

Bitte geben Sie den aktuellen Bestätigungscode ein, den Ihr Security-Token anzeigt.

123456 ✓

Zurück Aktivieren

Abbildung 4

Der Einrichtungsassistent schließt sich nach der erfolgreichen Eingabe des Bestätigungscode und Sie befinden sich in Ihrer WebUntis-Umgebung. Von nun an ist bei jeder Anmeldung, neben der Eingabe des WebUntis-Passwortes, auch die Eingabe des Codes Ihres Hardware-Tokens notwendig.