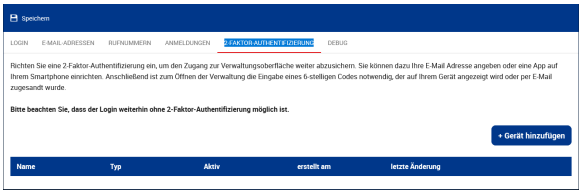
2-Faktor-Authentifizierung

In den Nutzereinstellungen ist es nun möglich, einen zweiten Faktor als zeitbasiertes Einmalpasswort (TOTP) zu hinterlegen, der anschließend erforderlich ist, um in die Verwaltung zu gelangen. Dementsprechend ist der Menüpunkt nur sichtbar für Nutzer mit lokalen oder zentralen Verwaltungsrechten.

> **Hinweis**
>
> Wird die optionale 2-Faktor-Authentifizierung nicht aktiviert, wird bei versuchtem Zugriff auf die Verwaltung das Nutzerpasswort des Administrators abgefragt. So wird der Verwaltungsbereich mit einem zusätzlichen Sicherheitsmechanismus geschützt, auch wenn ein Nutzer mit Administrationsrechten auf einem Computer in der Öffentlichkeit (z.B. in der Fahrzeughalle) aktiv eingeloggt ist.
>
> Die Eingabe des Passwortes ist alle 10 Minuten (ab letztem Seitenaufruf) erneut notwendig.

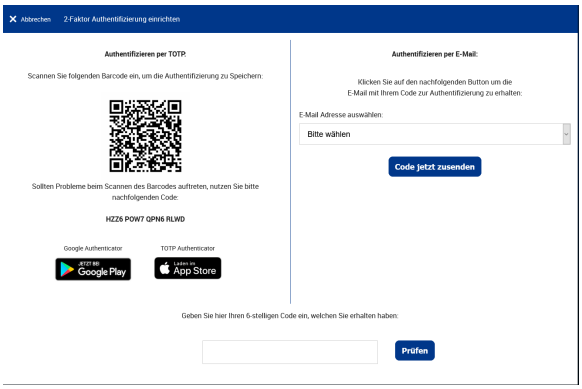
Einrichten der 2-Faktor-Authentifizierung

Gehen Sie zum Einrichten der 2-Faktor-Authentifizierung über den Browser in die Persönlichen Einstellungen (Namenskürzel oben Rechts). Dort finden Sie die Registerkarte *2-Faktor-Authentifizierung*



Klicken Sie auf **+ Gerät hinzufügen** um zugehörig zum Account ein weiteres Gerät als zusätzlichen Faktor zu registrieren.

Daraufhin öffnet sich die Seite zur Einrichtung der 2-Faktor-Authentifizierung.



Authentifizierung per E-Mail:

Wählen Sie eine Ihrer bestätigten E-Mail-Adressen aus, klicken Sie auf **Code jetzt zusenden**, geben Sie in das unten liegende Feld den erhaltenen Bestätigungscode ein und klicken Sie auf **Prüfen**.

Authentifizierung per Smartphone (Google Authenticator oder Apple TOTP Authenticator)

Laden Sie eine Authentifizierungs-App herunter und scannen Sie mit der Kamera den QR-Code ein. Die App wird Ihnen nach kurzer Zeit einen 6-stelligen Code nennen. Geben Sie diesen in das unten liegende Feld ein

und klicken Sie auf 

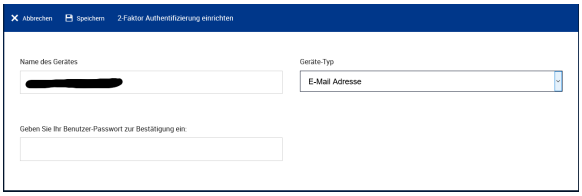
.

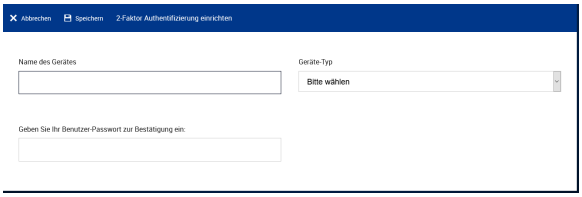
Zum Google Authenticator

Zum TOTP Authenticator

Im nächsten Schritt können Sie dem Gerät/der E-Mail Adresse einen Namen und einen Typen zur besseren Identifikation geben.

Bestätigen Sie die Eingaben mittels Benutzerpasswort.

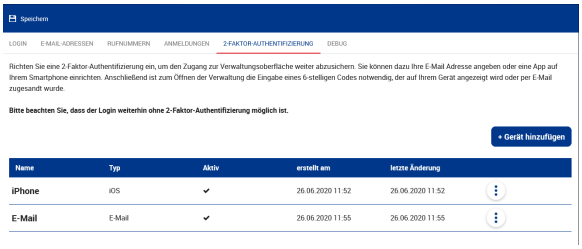




Verwalten der Authentifizierungsgeräte

Nach dem Speichern können dann alle verknüpften Geräte in der Liste eingesehen, bearbeitet, oder gelöscht werden. Hierzu müssen Sie nur

auf den Button auf der rechten Seite klicken.



Mit diesen Authentifizierungs-Apps klappt es:

	App/Anbieter	QR-Code	Link zu den App Stores (Apple /PlayStore)
	TOTP	✓	Apple App Store: Link Google Play Store: Link
	Google Authenticator	✓	Apple App Store: Link Google Play Store: Link
	Microsoft Authenticator	✓	Apple App Store: Link Google Play Store: Link
	Sophos Authenticator	✓	Apple App Store: Link Google Play Store: Link
	2FA Authenticator (2FAS)	✓	Apple App Store: Link Google Play Store: Link
	Last Pass	✓	Apple App Store: Link Google Play Store: Link

	Authenticator	✅	Apple App Store: Link Google Play Store: /
	Free OTP	✅	Apple App Store: Link Google Play Store: Link
blocked URL	Twilio Authy	✅	Apple App Store: Link Google Play Store: Link
blocked URL	Apple iCloud Schlüsselbund	✅	