

Multi-Faktor-Authentifizierung

Inhaltsverzeichnis

- Vorbereitung
- Einrichtung im syBOS
- Multi-Faktor-Authentifizierung entfernen



Multi-Faktor-Authentifizierung ist ein Sicherheitsverfahren, das zwei oder mehr verschiedene Authentifizierungsfaktoren zur Verifikation der Identität eines Benutzers verwendet. Ziel ist es, die Sicherheit zu erhöhen und unbefugten Zugriff auf vertrauliche Informationen zu verhindern.

Vorbereitung

Um einen Software-Token verwenden zu können, muss eine passende App auf einem Smartphone zur Verfügung stehen.

Folgende Authentifizierungs-Apps können verwendet werden (Beispiele):

- Google Authenticator
- Microsoft Authenticator



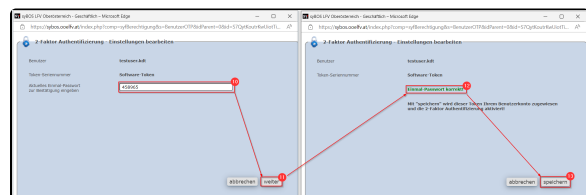
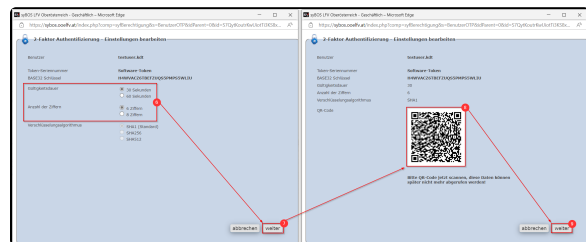
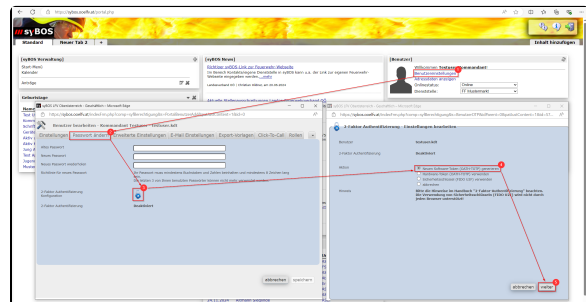
Einrichtung im syBOS

1. Auf der Portalseite beim Benutzer die **"Benutzereinstellungen"** öffnen
2. Auf den Tab **"Passwort ändern"** wechseln
3. Auf das **"Schlosssymbol"** **blocked URL** klicken
4. Aktion **"Neuen Software-Token (OATH-TOTP) generieren"** auswählen
5. **Weiter** klicken
6. Die Gültigkeitsdauer und die Anzahl der Ziffern wählen (**30 Sekunden und 6 Ziffern**)
7. **Weiter** klicken
8. Den **QR-Code** mit der **Authentifizierungs-App am Smartphone** öffnen
9. Sobald das Konto am Smartphone hinzugefügt wurde kann auf **Weiter** geklickt werden
10. Das **Einmal-Passwort**, welches in der Authentifizierungs-App angezeigt wird eingeben
11. **Weiter** klicken
12. Nun sollte **"Einmal-Passwort korrekt!"** angezeigt werden
13. Mit **Speichern** ist die Einrichtung abgeschlossen



Betrifft Schritt 6: Zum aktuellen Zeitpunkt sollen nur die **Standardwerte** verwendet werden (**30 Sekunden und 6 Ziffern**). Mit anderen Kombinationen kann es zu Fehlern kommen!

Sobald die Multi-Faktor-Authentifizierung im syBOS konfiguriert und aktiv ist, wird bei jeder Anmeldung auch das Einmal-Passwort benötigt.



Multi-Faktor-Authentifizierung entfernen

Sollte der Zugriff über MFA nicht mehr funktionieren (Smartphone Verlust, etc.) kann der **zuständige IT-Administrator der Feuerwehr** diese deaktivieren.

- Über **Portal Administration Berechtigung Benutzer-Verwaltung** einsteigen und den betroffenen Benutzer öffnen.
- Auf das **Sicherheitsschloss blocked URL** klicken
- **2-Faktor Authentifizierung deaktivieren** auswählen
- **Weiter** klicken

Im Anschluss daran muss die MFA neu eingerichtet werden.

