

FAQ zur Zwei-Faktor-Authentifizierung (2FA)

Frage: Ich habe ein Diensthandy. Was muss ich tun?

Antwort: Wenn Sie ein Diensthandy nutzen, ist die **Microsoft Authenticator App** bereits vorinstalliert. Sie können diese App für die Einrichtung der Zwei-Faktor-Authentifizierung (2FA) verwenden.

Frage: Kann ich auch eine andere Authenticator-App verwenden?

Antwort: Ja. Wir empfehlen die Microsoft Authenticator App, da wir diese App auch im Großteil für das mobile Arbeiten verwenden und diese auf Diensthandys bereits vorinstalliert ist. Grundsätzlich können Sie jedoch jede Authenticator-App verwenden, die den Standard für zeitbasierte Einmalcodes (TOTP) unterstützt.

Frage: Ich habe kein Handy. Was kann ich tun?

Antwort: Wenn Sie kein Smartphone besitzen oder dieses nicht für die Zwei-Faktor-Authentifizierung verwenden möchten, können Sie eine Authenticator-App auf Ihrem PC installieren. Nutzen Sie hierfür unsere Anleitung zur Installation einer Authenticator-App auf dem PC und richten Sie die Zwei-Faktor-Authentifizierung anschließend wie beschrieben ein:

https://awothueringen.de/fileadmin/media/Bilder_Landesverband/Dokumente/Anleitung_2FA_Browser.pdf

Frage: Die Anmeldung funktioniert nicht. Was kann ich tun?

Antwort: Ein häufiger Fehler bei der erstmaligen Anmeldung ist, dass das **Initialkennwort nicht vollständig oder nicht korrekt eingegeben** wurde.

Bitte achten Sie darauf, das **komplette Initialkennwort** zu übernehmen. Dazu gehören auch **alle Sonderzeichen, Groß- und Kleinbuchstaben sowie Zahlen**. Das Initialkennwort muss exakt so eingegeben werden, wie es Ihnen mitgeteilt wurde.

Sollte die Anmeldung trotz korrekter Eingabe weiterhin nicht funktionieren, wenden Sie sich bitte an den zuständigen Personalsachbearbeiter.

Frage: Kann ich mein Passwort selbst zurücksetzen?

Antwort: Nein, ein selbstständiges Zurücksetzen des Passworts ist nicht möglich.

Wenn Sie Ihr Passwort vergessen haben, wenden Sie sich bitte an den zuständigen Personalsachbearbeiter. Dieser wird Ihnen ein neues Passwort zur Verfügung stellen.

Frage: Die Zwei-Faktor-Authentifizierung wurde erfolgreich eingerichtet. Warum funktionieren die Zugangsdaten anschließend im Mitarbeiterportal nicht?

Antwort: Die Zwei-Faktor-Authentifizierung und das Mitarbeiterportal sind **zwei voneinander unabhängige Zugänge**. Lediglich der **Benutzername** ist für beide Portale **identisch**.

Für die Zwei-Faktor-Authentifizierung verwenden Sie die dafür eingerichteten Zugangsdaten. Das Mitarbeiterportal verfügt hingegen über einen **eigenständigen Zugang**. Für das Mitarbeiterportal bleiben die Zugangsdaten bestehen, die Sie bereits vor der Einführung der Zwei-Faktor-Authentifizierung verwendet haben.

Das bedeutet:

- **Zugang 1:** Zugangsdaten für die Zwei-Faktor-Authentifizierung
- **Zugang 2:** Zugangsdaten für das Mitarbeiterportal

Die Passwörter für beide Zugänge **können identisch sein, müssen es aber nicht**.

Wenn Sie nach der erfolgreichen Einrichtung der Zwei-Faktor-Authentifizierung zum Mitarbeiterportal weitergeleitet werden, verwenden Sie dort bitte weiterhin Ihre **bisherigen Zugangsdaten für das Mitarbeiterportal**.

Wichtig zu beachten!

Der persönliche Zugang zum Mitarbeiterportal sowie die hierfür verwendeten Zugangsdaten und die Daten der Zwei-Faktor-Authentifizierung (2FA) sind **vertraulich** und **ausschließlich zur persönlichen Nutzung** bestimmt.

Eine Weitergabe von Passwort, Zugangsdaten, Authenticator-Daten, Sicherheitsinformationen oder sonstigen Zugangsdaten an Dritte ist **nicht gestattet**.

Bei den Zugangsdaten zum Mitarbeiterportal und insbesondere bei den Daten zur Zwei-Faktor-Authentifizierung handelt es sich um **hochsensible Sicherheitsdaten**. Die Schutzbedürftigkeit ist mit derjenigen von Zugangsdaten zum Online-Banking vergleichbar. Eine unbefugte Weitergabe oder Nutzung kann dazu führen, dass Dritte auf vertrauliche Informationen und geschützte Bereiche zugreifen können.