

Anleitung Zwei-Faktor-Authentifizierung(2FA)

Inhaltsverzeichnis

1. Anmeldung	1
2. Installation der Authenticator-App.....	1
3. 2FA-App Konfiguration	2
4. Zwei-Fraktor Bestätigung	3
5. Hinzufügen von weiteren Zwei-Faktor-Authentifizierungen	3

1. Anmeldung

Melden Sie sich an Ihrer IServ Umgebung an.

2. Installation der Authenticator-App

Laden Sie sich zuerst eine kompatible Authenticator-App auf Ihrem privaten Endgerät herunter. Wir empfehlen hier den Google Authenticator. Alternativ kann das dienstliche iPad benutzt werden, hier ist die GoogleAuthenticator-App bereits installiert.

Klicken Sie dann auf „weiter: 2FA Konfigurieren“.

 Zwei-Faktor-Authentifizierung ist für Ihren Account seit dem 29.01.2025 erforderlich.
Sie haben noch 14 Tage zur Einrichtung.

Das folgende Video zeigt Ihnen, wie Sie die Zwei-Faktor-Authentifizierung einrichten: [Zwei-Faktor-Authentifizierung einrichten](#).

Schritt 1: Kompatible App herunterladen

Erhöhen Sie die Sicherheit Ihres Kontos, indem Sie die Zwei-Faktor-Authentifizierung (2FA) aktivieren. Laden Sie dazu zunächst eine kompatible 2FA-App herunter.

Wir empfehlen die Verwendung von TOTP-Apps wie Duo, LastPass, Authenticator, Authy und FreeOTP.

Cloud-basierte Anwendungen ermöglichen es Ihnen, den Zugriff wiederherzustellen, wenn Sie Ihr Telefon verlieren. Ein Administrator kann Ihre Zwei-Faktor-Authentifizierung deaktivieren, wenn Sie sich einmal komplett ausgesperrt haben.


Cisco
DUO


GoTo Inc.
LastPass


Google
Authenticator


Twilio
Authy


Red Hat
FreeOTP

[→ Weiter: 2FA konfigurieren](#)

Weiter ohne Zwei-Faktor

Angemeldet als adm-wehren.

Abmelden

3. 2FA-App Konfiguration

1. Bezeichnung: Definieren Sie auf welchem Gerät die 2FA-APP installiert ist. Diese Angabe können nur Sie in Ihrem IServ Profil sehen.
2. Passwort: Geben Sie zur Bestätigung nochmal Ihr IServ Passwort ein.
3. Scannen Sie in der Authenticator-App nun den QR-Code aus Ihrer IServ-Oberfläche oder geben den Code manuell ein.
4. Der Eintrag in der Authenticator-App sollte dann so aussehen:



5. Den angezeigten Code tragen Sie dann unten bei Schritt 5 ein und gehen Sie auf „Aktivieren“

Zwei-Faktor-Authentifizierung ist für Ihren Account seit dem 13.11.2024 erforderlich.
Richten Sie Zwei-Faktor-Authentifizierung ein, um Ihren Account weiter zu benutzen.

Schritt 2: Bezeichnung wählen (Optional)

Bezeichnung iPhone Privat ⋮

Zur besseren Identifizierung Ihrer 2FA

Schritt 3: Intention mit aktuellen Passwort bestätigen

Passwort * ***** ⋮

Bitte geben Sie Ihr aktuelles Passwort ein, um die Aktivierung zu bestätigen.

Schritt 4: Code scannen



Auf Mobilgeräten klicken Sie die Schaltfläche um die 2FA App zu öffnen:

[In App öffnen](#)

Falls Sie den Code nicht scannen können, ist auch eine manuelle Eingabe möglich:

Manuelle Eingabe

⌵

Um den Eintrag manuell hinzuzufügen, geben Sie die folgenden Daten in der Anwendung auf Ihrem Telefon ein:

Account [REDACTED]

Klartext-Schlüssel [REDACTED]

ⓘ Die Leerzeichen dienen nur der Lesbarkeit und sind nicht Teil des Schlüssels.

Zeitbasiert Ja

Schritt 5: Code aus der App eingeben

2FA-Code * 180814

Nachdem Sie den Code gescannt haben, zeigt die App einen Code an, den Sie hier eingeben müssen.

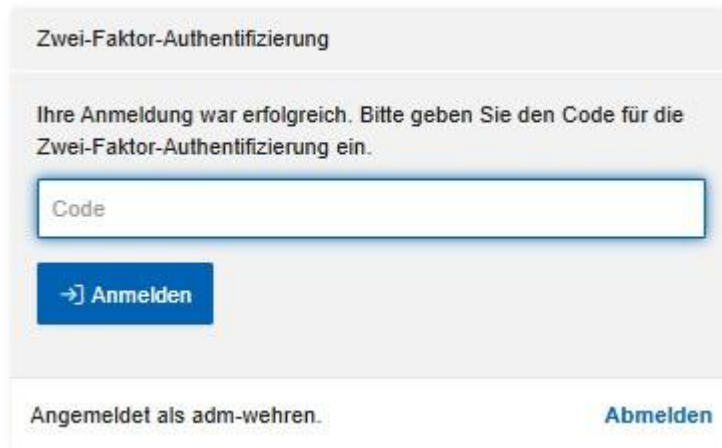
[← Zurück](#)
[✓ Aktivieren](#)

Angemeldet als adm-wehren.

[Abmelden](#)

4. Zwei-Faktor Bestätigung

Geben Sie im folgenden Fenster nochmals den 2FA-Code ein und gehen Sie dann auf „Anmelden“.



Die Zwei-Faktor-Authentifizierung ist nun bei Ihnen aktiviert

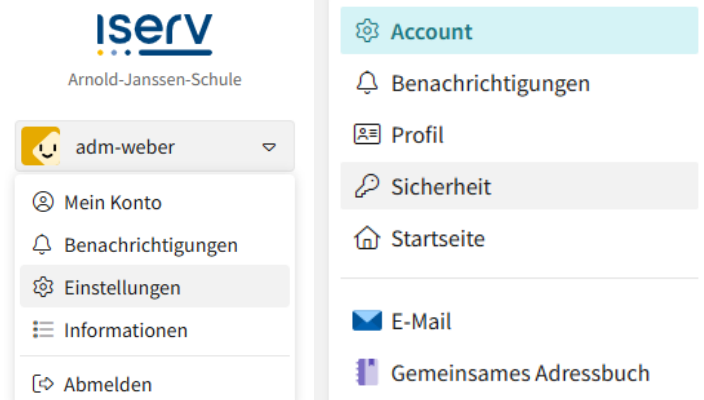
Der Code wird nun bei jeder Anmeldung über den neuen Webbrowser abgefragt.

In der IServ-App, auf dem Smartphone oder Tablet, wird dieser nur bei der ersten Einrichtung abgefragt.

5. Hinzufügen von weiteren Zwei-Faktor-Authentifizierungen

Es können auch weitere Authentifizierungsmöglichkeiten in iServ hinterlegt werden.

1. Gehen Sie dazu in die Sicherheitseinstellungen in Ihrem iServ Konto, dieses erreichen Sie über Ihr Konto-Symbol oben rechts auf der iServ Startseite (Einstellungen>Sicherheit).



2. Klicken Sie auf „2FA hinzufügen

Zwei-Faktor-Authentifizierung (2FA)

Die Zwei-Faktor-Authentifizierung sichert nur den Zugriff auf die Weboberfläche und nicht auf andere Dienste wie E-Mail.

Bezeichnung	Aktionen
Hinzugefügt am 27.03.2026	✎ 🗑

[+ 2FA hinzufügen](#)

3. Laden Sie bei Bedarf eine kompatible App herunter und klicken Sie auf „Weiter: 2FA konfigurieren“

Zwei-Faktor-Authentifizierung (2FA)

Das folgende Video zeigt Ihnen, wie Sie die Zwei-Faktor-Authentifizierung einrichten: [Zwei-Faktor-Authentifizierung einrichten](#).

Schritt 1: Kompatible App herunterladen

Erhöhen Sie die Sicherheit Ihres Kontos, indem Sie die Zwei-Faktor-Authentifizierung (2FA) aktivieren. Laden Sie dazu zunächst eine kompatible 2FA-App herunter. Wir empfehlen die Verwendung von TOTP-Apps wie Duo, LastPass, Authenticator, Authy und FreeOTP.

Cloud-basierte Anwendungen ermöglichen es Ihnen, den Zugriff wiederherzustellen, wenn Sie Ihr Telefon verlieren. Ein Administrator kann Ihre Zwei-Faktor-Authentifizierung deaktivieren, wenn Sie sich einmal komplett ausgesperrt haben.



Cisco
DUO



LastPass



Google
Authenticator



Twilio
Authy



Red Hat
FreeOTP

[← Zurück](#)
[→ Weiter: 2FA konfigurieren](#)

4. Geben Sie dem neuen 2FA eine Bezeichnung und bestätigen Sie die Aktion mit ihrem bereits existierenden 2FA Code.

5. Richten Sie den neuen 2FA ein, indem Sie ihn scannen oder manuell in der entsprechenden App hinzufügen. Geben Sie den 6-stelligen Code in Schritt 5 in iServ ein. Klicken Sie anschließend auf „Aktivieren“

Zwei-Faktor-Authentifizierung (2FA)

Schritt 2: Bezeichnung wählen (Optional)

Bezeichnung

Zur besseren Identifizierung Ihrer 2FA

Schritt 3: Intention mit existierendem 2FA-Code bestätigen

Code *

Bitte geben Sie einen Code einer bestehenden Zwei-Faktor-App zur Bestätigung der Aktivierung ein.

Schritt 4: Code scannen



Auf Mobilgeräten klicken Sie die Schaltfläche um die 2FA App zu öffnen:

[In App öffnen](#)

Falls Sie den Code nicht scannen können, ist auch eine manuelle Eingabe möglich:

[Manuelle Eingabe](#)

Schritt 5: Code aus der App eingeben

2FA-Code *

Nachdem Sie den Code gescannt haben, zeigt die App einen Code an, den Sie hier eingeben müssen.

[← Zurück](#)
[✓ Aktivieren](#)