

{tip4u://188}

Version 6

Zentraleinrichtung für Datenverarbeitung (ZEDAT)

www.zedat.fu-berlin.de

Anmeldung mit Multifaktor-Authentifizierung

Diese Anleitung erklärt die Einrichtung der sicheren Anmeldeverfahren mit Multifaktor-Authentifizierung (MFA).

Einrichtung der sicheren Anmeldeverfahren (Multifaktor-Authentifizierung) für FU-Accounts

Einführung // Note: english version further down (page 13)

Der Schutz Ihrer persönlichen und akademischen Daten an der Freien Universität Berlin ist uns ebenso wichtig wie Ihnen. Deshalb haben wir die **Multifaktor-Authentifizierung (MFA)** für alle FU-Accounts eingeführt. Neben Ihrem Passwort wird ein zweiter Sicherheitsfaktor benötigt, um sich anzumelden. Dieser Schritt erhöht die Sicherheit Ihrer Daten erheblich, da ein potenzieller Angreifer nun sowohl Ihr Passwort als auch einen davon unabhängigen zweiten Faktor benötigt, um auf Ihr Konto zuzugreifen.

Sie können mehrere verschiedene Anmeldeverfahren gleichzeitig als Ihren zweiten Faktor aktivieren (daher: *Multifaktor*). Es reicht zur Anmeldung aus, wenn Sie immer eins Ihrer aktivierten Verfahren zusätzlich zu Ihrem Passwort nutzen können – es ist jedoch sinnvoll, mehrere der Verfahren einzurichten, falls Sie den Zugriff auf eines verlieren sollten.

In den folgenden Abschnitten erklären wir die Einrichtung der Anmeldeverfahren. Bitte denken Sie daran, dass Sie Ihren **zweiten Faktor** (Code-Matrix, Authentifizierungs-App, Sicherheitsschlüssel / Passkey oder Telefon-PIN) **niemals mit jemandem teilen** sollten – ebenso wenig wie Ihr Passwort. Auch unser IT-Personal wird Sie niemals nach Ihrem zweiten Faktor oder Ihrem Passwort fragen.

Um die sicheren Anmeldeverfahren vollständig einzurichten und zu verwalten, navigieren Sie bitte zunächst zum Abschnitt *Account* ▶ *Multifaktor-Authentifizierung* im ZEDAT-Portal: <https://portal.zedat.fu-berlin.de/>

[Startseite](#) > [Account](#) > [Multifaktor-Authentifizierung](#)

Multifaktor-Authentifizierung

Hier sehen Sie Ihre eingerichteten sicheren Anmeldeverfahren mit Multifaktor-Authentifizierung. Diese dienen dem Schutz Ihres Kontos vor unbefugtem Zugriff und werden jeweils zusätzlich zu Ihrem Passwort abgefragt. Eine Kurzbeschreibung der Verfahren erhalten Sie, wenn Sie mit dem Mauszeiger oder Finger auf das jeweilige Verfahren gehen. Sie können eines der Verfahren als Standard wählen, dieses wird dann bevorzugt verwendet.

Durch Klick auf den Namen des Verfahrens oder auf 'Verwalten', bekommen Sie weitere Informationen und haben die Möglichkeit, das Verfahren zu aktivieren, zu deaktivieren oder neue Schlüssel einzurichten.

Standardverfahren

Verfahren	Status	Aktionen
 Code-Matrix	aktiviert	<input type="button" value="Verwalten"/>

Weitere Verfahren

Verfahren	Status	Aktionen
 Authentifizierungs-App (Authenticator)	deaktiviert	<input type="button" value="Verwalten"/>
 Sicherheitsschlüssel / Passkey	deaktiviert	<input type="button" value="Verwalten"/>
 Telefon-TAN	deaktiviert	<input type="button" value="Verwalten"/>

Hilfe

Hier werden die einzelnen Verfahren erklärt.

[Hilfe zu den Verfahren](#)

Portal-Seite für die sicheren Anmeldeverfahren

Hier finden Sie die Übersicht zu Ihren Anmeldeverfahren. In der Tabelle werden die einzelnen Verfahren aufgelistet. Wenn Sie auf den Namen eines Verfahrens oder in der Spalte *Aktionen* auf *Verwalten* klicken, kommen Sie anschließend zur speziellen Konfigurationsseite des jeweiligen Verfahrens, um es einrichten zu können. In der Spalte *Status* erkennen Sie den aktuellen Status der einzelnen Verfahren – z.B. ob ein Verfahren aktiviert, deaktiviert oder gesperrt ist. Wie Sie ein Verfahren **sperrern, löschen oder deaktivieren** können und was dies bedeutet, erläutern wir weiter unten in dieser Anleitung in einem eigenen Abschnitt.

Initial ist lediglich das Verfahren „Code-Matrix“ aktiviert und als Standard festgelegt. Wenn Sie ein anderes Verfahren als Ihr Standardverfahren nutzen wollen, können Sie dies nach der Aktivierung des Verfahrens in der Spalte *Aktionen* über den Button *Als Standard* festlegen.

Unter *Hilfe zu den Verfahren* finden Sie außerdem eine Kurzübersicht zu den einzelnen Anmeldeverfahren.

Im Bereich *E-Mail-Benachrichtigung* können Sie einstellen, ob Sie bei Anmeldeversuchen eine Sicherheits-Benachrichtigung per Mail erhalten wollen.

Verfahren 1: Code-Matrix (Standard / Backup)

Das Verfahren „Code-Matrix“ ist immer aktiviert und für die initiale Einrichtung sowie als Backup vorgesehen. Bei Verwendung dieses Verfahrens werden Sie nach sechs zufälligen Positionen aus Ihrer individuellen Code-Matrix gefragt. Die Code-Matrix wird Ihnen üblicherweise zunächst per Post zugesandt. Es ist immer nur **eine** Code-Matrix aktiv. Bei Neuausstellung wird die vorherige ungültig.

	1	2	3	4	5	6	7	8	9
A	M	C	E	s	s	i	V	g	9
B	J	k	W	7	N	b	h	E	k
C	6	H	q	U	G	9	u	R	9
D	d	M	J	S	J	P	w	h	K
E	J	H	m	a	d	t	g	7	2
F	U	P	2	t	j	D	4	M	g
G	D	e	R	q	K	7	W	a	d
H	E	f	N	j	b	4	d	W	9
I	L	b	i	3	U	g	5	8	Q

Beispiel einer Code-Matrix

- Die individuelle 9x9 Code-Matrix enthält zufällige Klein- und Großbuchstaben sowie Ziffern.
- Im Anmeldevorgang mit diesem Verfahren werden Sie nach 6 zufällig gewählten Feldern aus dieser Matrix gefragt.

- Die Felder sind dabei nach ihrer Reihe und Spalte benannt. Die Bezeichnungen der Positionen setzen sich jeweils zusammen aus einem Buchstaben (A-I), der die Reihe angibt, sowie einer Ziffer (1-9), die die Spalte angibt.
- Wenn aufgefordert, geben Sie bitte die abgefragten Positionen aus Ihrer Matrix in der richtigen Reihenfolge ohne Leerzeichen sowie unter Beachtung von Groß- und Kleinschrift ins Eingabefeld ein und bestätigen Sie so Ihre Anmeldung.
- *Beispiel (nach obiger Beispiel-Matrix): Werden Sie etwa nach dem Inhalt des Feldes G8 gefragt, so müssen Sie den Buchstaben a eingeben.*

Vorgang mit dem Verfahren Code-Matrix bestätigen

Bitte den angeforderten Code aus der Code-Matrix eingeben

Seriennummer: PIIX0120653B

Positionen: G3 C4 H6 F4 G3 H9

Code:

Beispiel einer Code-Matrix-Abfrage

- Bewahren Sie die Code-Matrix sicher auf und teilen Sie diese mit niemandem.
- Falls Sie eines der anderen Anmeldeverfahren aktiviert haben, können Sie sich selbst bei Bedarf eine neue Code-Matrix im Portal ausstellen lassen (*Portal* ▶ *Account* ▶ *Multifaktor-Authentifizierung* ▶ *Code-Matrix* ▶ *Neue Matrix ausstellen*). Dabei verliert die alte Matrix ihre Gültigkeit und kann nicht mehr verwendet werden. Falls Sie keines der anderen Anmeldeverfahren aktiviert haben, wenden Sie sich bei Verlust der Matrix bitte an den Benutzerservice.

[Startseite](#) > [Account](#) > [Multifaktor-Authentifizierung](#) > [Code-Matrix](#)

Code-Matrix

Das Verfahren Code-Matrix ist immer aktiviert und für die initiale Einrichtung sowie als Backup vorgesehen.

Bei Verwendung dieses Verfahrens werden Sie nach sechs zufälligen Positionen aus Ihrer Code-Matrix gefragt. Die Positionen setzen sich jeweils zusammen aus einem Buchstaben (A-I), der die Reihe angibt, sowie einer Ziffer (1-9), die die Spalte angibt.

Zur Anmeldung geben Sie die Zeichen an den abgefragten Positionen in der richtigen Reihenfolge ein.

Es ist immer nur **eine** Code-Matrix aktiv. Bei Neuausstellung wird die vorherige gelöscht.

Code-Matrix verloren? Sie können hier eine neue ausstellen, Ihre alte Matrix wird damit gleichzeitig gelöscht.

Seriennummer	Anlegezeitpunkt	Sperrzeitpunkt	Sperrgrund	Status
PIIX0011146A	04.10.2023 11:15			aktiv

Portal-Seite zur Verwaltung der Code-Matrix

Hinzufügen von weiteren Anmeldeverfahren

Die Einrichtung mindestens eines der nachfolgenden zusätzlichen Verfahren erleichtert den Anmeldevorgang erheblich. Navigieren Sie dazu zunächst im ZEDAT-Portal zu *Account* ▶ *Multifaktor-Authentifizierung* und klicken Sie dort auf das entsprechende Verfahren.

[Startseite](#) > [Account](#) > [Multifaktor-Authentifizierung](#)

Multifaktor-Authentifizierung

Hier sehen Sie Ihre eingerichteten sicheren Anmeldeverfahren mit Multifaktor-Authentifizierung. Diese dienen dem Schutz Ihres Kontos vor unbefugtem Zugriff und werden jeweils zusätzlich zu Ihrem Passwort abgefragt. Eine Kurzbeschreibung der Verfahren erhalten Sie, wenn Sie mit dem Mauszeiger oder Finger auf das jeweilige Verfahren gehen. Sie können eines der Verfahren als Standard wählen, dieses wird dann bevorzugt verwendet.

Durch Klick auf den Namen des Verfahrens oder auf 'Verwalten', bekommen Sie weitere Informationen und haben die Möglichkeit, das Verfahren zu aktivieren, zu deaktivieren oder neue Schlüssel einzurichten.

Standardverfahren

Verfahren	Status	Aktionen
 Code-Matrix	aktiviert	<input type="button" value="Verwalten"/>

Weitere Verfahren

Verfahren	Status	Aktionen
 Authentifizierungs-App (Authenticator)	deaktiviert	<input type="button" value="Verwalten"/>
 Sicherheitsschlüssel	deaktiviert	<input type="button" value="Verwalten"/>
 Telefon-TAN	deaktiviert	<input type="button" value="Verwalten"/>

Hilfe

Hier werden die einzelnen Verfahren erklärt.

[Hilfe zu den Verfahren](#)

Portal-Seite für die sicheren Anmeldeverfahren

Verfahren 2: Authentifizierungs-App (Authenticator) (Empfohlen)

Beim Anmeldeverfahren „Authentifizierungs-App“ wird beim Anmeldevorgang ein zeitbasierter, einmaliger Bestätigungscode in Ihrer App generiert (TOTP / Time-based One-time Password). Diesen geben Sie beim Anmeldevorgang, wenn aufgefordert, zusätzlich zu Ihrem Passwort mit ein. Eine Authentifizierungs-App ist ein schneller und einfacher Weg der sicheren Anmeldung im Alltag. Sie können eine beliebige TOTP-Authentifizierungs-App nutzen (z.B. 2FAS Authenticator, Google Authenticator, Microsoft Authenticator). Sie können bis zu **drei** Apps auf verschiedenen Geräten einrichten und alternativ verwenden.

Schritt-für-Schritt-Anleitung für den 2FAS Authenticator:

- Navigieren Sie im ZEDAT-Portal zu *Account* ▶ *Multifaktor-Authentifizierung* ▶ *Authentifizierungs-App* und klicken Sie auf *Jetzt einrichten*. Klicken Sie dann auf *Weiter*.

Startseite > Account > Multifaktor-Authentifizierung > Authentifizierungs-App (Authenticator)

Authentifizierungs-App (Authenticator)

Hier finden Sie eine Übersicht über Ihre registrierten Authentifizierungs-Apps. Bereits angelegte Authentifizierungs-Apps können gesperrt oder gelöscht werden. Es können bis zu drei Authentifizierungs-Apps angelegt werden. Sie können auch das gesamte Verfahren deaktivieren, dadurch können Sie es nicht mehr verwenden, bis Sie es wieder aktivieren.

Verfahrensstatus: Das Verfahren ist nicht eingerichtet.

Jetzt einrichten

Zurück

Portal-Seite zur Verwaltung der Authenticator-Apps

- Zuerst vergeben Sie einen Namen für diesen Authenticator. Falls Sie mehrere Authentifizierungs-Apps einrichten, hilft Ihnen dieser Name bei der jeweiligen Identifizierung. Klicken Sie dann auf *Weiter*.

Namen vergeben

Damit Sie die App wiedererkennen, geben Sie ihr einen aussagekräftigen Namen. Es sind nur die folgenden Zeichen erlaubt: A-Z, a-z, 0-9, Bindestrich und Leerzeichen.

Geben Sie hier einen Namen ein:

App-Name

Zurück

Weiter

- Zum Einrichten der App wird Ihnen nun im Portal ein individueller QR-Code angezeigt.

QR-Code scannen

Scannen Sie mit Ihrer Authenticator App diesen QR-Code. Sie können auch [diesen Link](#) anklicken. Dadurch wird Ihre Authenticator App geöffnet.



Geben Sie nun den generierten Zifferncode ein, um sicherzustellen, dass Ihre Authenticator App korrekt eingerichtet wurde.

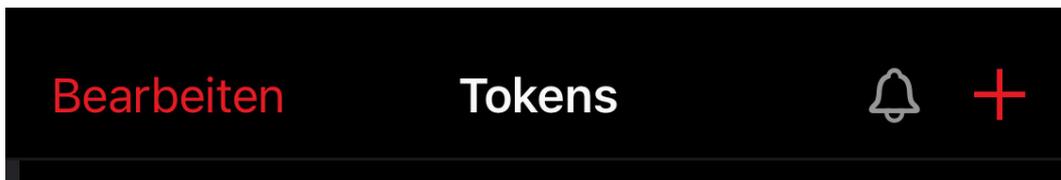
Zifferncode:

Zurück

Weiter

Portal-Seite für die Einrichtung der Authenticator-App

- Installieren Sie zunächst die 2FAS Authenticator App aus dem App Store (iOS) oder Google Play Store (Android).
 - iOS: <https://apps.apple.com/de/app/2fa-authenticator-2fas/id1217793794>
 - Android: <https://play.google.com/store/apps/details?id=com.twofasapp>
- Öffnen Sie die 2FAS Authenticator App und tippen Sie auf das Plus-Symbol (+), um Ihren FU-Account hinzuzufügen.
- Wählen Sie *QR-Code scannen* und scannen Sie den QR-Code, der auf dem Bildschirm im ZEDAT-Portal angezeigt wird. Gegebenenfalls müssen Sie der App vorher den Kamerazugriff erlauben.



- Die App generiert nun einen 6-stelligen Code, der alle 30 Sekunden erneuert wird. Geben Sie diesen Code im unten stehenden Eingabefeld im Portal ein.

Geben Sie nun einen generierten Zifferncode ein, um sicherzustellen, dass Ihre Authenticator App korrekt eingerichtet wurde.

Zifferncode:

Zurück

Weiter

Den generierten Code in dieses Feld eingeben



Beispiel eines Codes in der 2FAS Authenticator App

- Zuletzt bestätigen Sie die Einrichtung, indem Sie ein bereits aktives Verfahren wie etwa Ihre Code-Matrix benutzen.
- Bei zukünftigen Anmeldungen können Sie nun den zeitbasierten Zahlencode aus der App als Ihren zweiten Faktor nutzen, wenn Sie dazu aufgefordert werden.

Verfahren 3: Sicherheitsschlüssel / Passkey

Im Verfahren Sicherheitsschlüssel / Passkey können Sie einen physischen Schlüssel (z.B. Yubico Security Key) oder sogenannte Passkeys einrichten. Dies sind digitale Sicherheitsschlüssel, die aus einem öffentlich/privatem Schlüsselpaar bestehen. Passkeys können in Ihrem Gerät gespeichert sein (z.B. mit Windows Hello) oder über eine Cloud zwischen verschiedenen Geräten synchronisiert werden (via Google-Konto, Apple iCloud-Schlüsselbund). Für Passkeys auf Apple Geräten (iPhone, iPad, Mac) muss beispielsweise der iCloud-Schlüsselbund aktiviert sein - der Schlüssel wird hierbei dann auf alle Ihre Apple Geräte sicher per iCloud verteilt. Passkeys können ein sehr schneller und einfacher Weg der sicheren Anmeldung im Alltag sein.

Falls Sie einen Hardware-Sicherheitsschlüssel eingerichtet haben, müssen Sie diesen zur Anmeldung immer bei sich haben. In der Regel genügt es, bei Hardware-Schlüsseln nach Eingabe Ihres Passworts den eingesteckten Schlüssel anzutippen oder an die Rückseite des Smartphones zu halten (NFC) um ihn zu verwenden. Gegebenenfalls müssen Sie USB-Sicherheitsschlüssel mit einer PIN sichern, die vor der Benutzung abgefragt wird.

Sie können bis zu **drei** Schlüssel einrichten und alternativ verwenden.

Einrichtung eines Sicherheitsschlüssels / Passkeys:

- Navigieren Sie im ZEDAT-Portal zu *Account* ▶ *Multifaktor-Authentifizierung* ▶ *Sicherheitsschlüssel / Passkey* und klicken Sie auf *Jetzt einrichten*. Klicken Sie dann auf *Weiter*.

[Startseite](#) > [Account](#) > [Multifaktor-Authentifizierung](#) > [Sicherheitsschlüssel / Passkey](#)

Sicherheitsschlüssel / Passkey

Als Sicherheitsschlüssel können Sie physische Schlüssel (z.B. Yubico USB Security Key) oder sogenannte Passkeys einrichten. Passkeys können in Ihrem Gerät gespeichert sein (z.B. mit Windows Hello) oder über eine Cloud zwischen verschiedenen Geräten synchronisiert werden (via Google-Konto, Apple iCloud-Schlüsselbund). Einen USB-Schlüssel müssen Sie mit einer PIN sichern, die vor der Benutzung abgefragt wird. Zur Einrichtung und zur Benutzung folgen Sie den Hinweisen ihres Browsers, die als Pop-Up erscheinen. Sie können bis zu **drei** Schlüssel einrichten und alternativ verwenden.

Verfahrensstatus: Das Verfahren ist nicht eingerichtet.

[Jetzt einrichten](#)

[Zurück](#)

Portal-Seite zur Verwaltung der Sicherheitsschlüssel / Passkeys

- Zuerst vergeben Sie einen Namen für diesen Schlüssel. Falls Sie mehrere Schlüssel einrichten, hilft Ihnen dieser Name bei der jeweiligen Identifizierung.

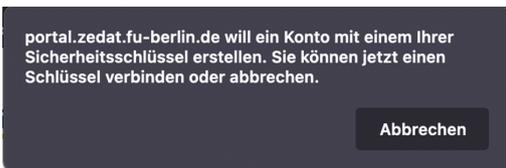
Namen vergeben

Damit Sie den Schlüssel wiedererkennen, geben Sie ihm einen aussagekräftigen Namen. Es sind nur die folgenden Zeichen erlaubt: A-Z, a-z, 0-9, Bindestrich und Leerzeichen.

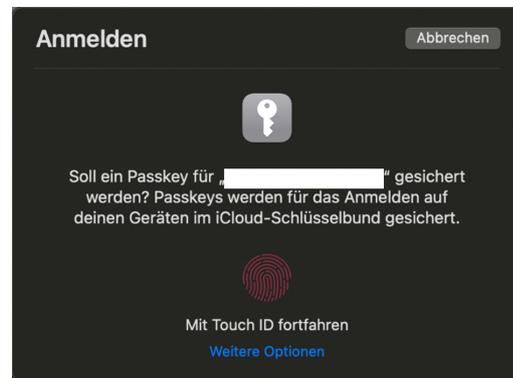
Geben Sie hier einen Namen ein:

Zurück
Weiter

- Anschließend werden Sie aufgefordert, Ihren Sicherheitsschlüssel einzurichten, indem Sie diesen z.B. in einen USB-Port stecken und aktivieren. Hierzu öffnet sich in der Regel ein Pop-Up-Fenster im Vordergrund. Wenn Ihr Gerät/Browser Passkeys unterstützt, wird eine Einrichtungsmöglichkeit für diese hier ebenfalls angezeigt. Je nach Typ des Schlüssels und Betriebssystem kann das Vorgehen von dem hier beschriebenen abweichen.
- Ihr Browser oder Betriebssystem führt Sie nun durch die Einrichtung Ihres Sicherheitsschlüssels / Passkeys.



Die Einrichtung ist browserabhängig. Ein solches Fenster kann sich etwa bei Mozilla Firefox öffnen.



Ein solches Fenster kann sich zur Einrichtung eines Passkeys in Safari auf einem Mac oder iOS Gerät öffnen.

- Bitte folgen Sie diesen Anweisungen. Nach erfolgreicher Einrichtung werden Sie automatisch zum nächsten Schritt weitergeleitet.
- Zuletzt bestätigen Sie die Einrichtung, indem Sie ein bereits aktives Verfahren benutzen.
- Bitte beachten Sie, dass ein physischer Sicherheitsschlüssel bei jedem Login in den Computer eingesteckt und bei der Aufforderung aktiviert werden muss.

Verfahren 4: Telefon-TAN (Nur für Beschäftigte)

Mit dem Telefon-TAN-Verfahren können Sie Bestätigungs-codes als Nachricht auf Ihr Cisco-Tischtelefon erhalten. Dazu ist es notwendig, dass Sie an Ihrem Tischtelefon angemeldet sind. Das ist der Fall, wenn Ihr Name oben links im Telefondisplay steht. Die Codes erhalten Sie **nicht** in der Webex App oder auf dem PC (Softphone).

Einrichtung der Telefon-TAN:

- Stellen Sie sicher, dass Sie bei Ihrem Tischtelefon mit Ihrem FU-Account angemeldet sind. (Benutzername + Telefon-PIN)
- Navigieren Sie im ZEDAT-Portal zu *Account* ▶ *Multifaktor-Authentifizierung* ▶ *Telefon-TAN* und klicken Sie auf *Jetzt einrichten*. Klicken Sie dann auf *Weiter*.

[Startseite](#) > [Account](#) > [Multifaktor-Authentifizierung](#) > [Telefon-TAN](#)

Telefon-TAN

Mit dem Telefon-TAN-Verfahren können Sie Bestätigungs-codes als Nachricht auf Ihr Cisco-Tischtelefon erhalten. Dazu ist es notwendig, dass Sie an Ihrem Tischtelefon angemeldet sind. Das ist der Fall, wenn Ihr Name oben links im Telefondisplay steht. Die Codes erhalten Sie nicht in der Webex App oder auf dem PC (Softphone).

Verfahrensstatus: Das Verfahren ist nicht eingerichtet.

[Jetzt einrichten](#)

[Zurück](#)

Portal-Seite zur Verwaltung des Telefon-TAN-Verfahrens

- Bestätigen Sie die Angaben zu Ihrem Tischtelefon am Bildschirm und klicken Sie dann auf *Weiter*.

Telefon-TAN-Verfahren Einrichten

Sie sind an folgendem Tischtelefon angemeldet:

Rufnummer: XXXXXXXXXX

Handelt es sich dabei nicht um das Telefon an Ihrem Arbeitsplatz, dann melden Sie sich zunächst am Telefon an. Hilfe zur Telefonanmeldung erhalten Sie hier: [Hilfe zum Telefon-Login](#)

Durch Klick auf 'Weiter' wird eine TAN auf dieses Telefon gesendet.

[Zurück](#)

[Weiter](#)

Portal-Seite mit Informationen zum angemeldeten Telefon

- Die Telefon-TAN erscheint nun als Nachricht auf dem Bildschirm Ihres Cisco-Tischtelefons.



Beispiel einer TAN am Cisco-Tischtelefon

- Die angezeigte TAN geben Sie nun in das Eingabefeld im Portal ein.
- Zuletzt bestätigen Sie die Einrichtung, indem Sie ein bereits aktives Verfahren benutzen.
- Bei zukünftigen Anmeldungen erhalten Sie eine Nachricht auf Ihrem angemeldeten Tischtelefon, um den Anmeldevorgang abzuschließen.

Sperren und Deaktivieren von Anmeldeverfahren

Verlust der Code-Matrix

Bei Verlust Ihrer Code-Matrix sollten Sie sich eine *Neue Matrix ausstellen*. Die bisherige Code-Matrix kann dann nicht mehr zur Authentifizierung genutzt werden. Wie bereits in der Erklärung zur Code-Matrix beschrieben, navigieren Sie hierzu im ZEDAT-Portal unter *Account* ▶ *Multifaktor-Authentifizierung* auf die Unterseite zur Code-Matrix und klicken dort auf den entsprechenden Button. Sie benötigen hierfür ein aktiviertes weiteres Anmeldeverfahren. Falls Sie kein weiteres Verfahren aktiviert haben, wenden Sie sich bitte an den Benutzerservice.

Deaktivieren anderer Verfahren

Die Anmeldeverfahren Authenticator-App, Sicherheitsschlüssel und Telefon-TAN können Sie deaktivieren, wenn Sie diese (vorübergehend) nicht zur Authentifizierung verwenden möchten. Navigieren Sie hierzu wieder im ZEDAT-Portal unter *Account* ▶ *Multifaktor-Authentifizierung* auf die entsprechende Unterseite des jeweiligen Verfahrens und klicken Sie dort auf *Deaktivieren*.

Sperren und Löschen einzelner Apps/Schlüssel

Bei den Verfahren Authentifizierungs-App und Sicherheitsschlüssel / Passkey können Sie einzelne Apps/Schlüssel entweder vorübergehend sperren oder endgültig löschen, etwa bei Verlust des Smartphones oder des Hardware-Sicherheitsschlüssels. Navigieren Sie hierzu wieder im ZEDAT-Portal unter *Account* ▶ *Multifaktor-Authentifizierung* auf die entsprechende Unterseite des jeweiligen Verfahrens und klicken Sie dort in der Spalte *Aktionen* auf *Sperren* oder *Löschen*. Falls Sie ein Verfahren sperren, können Sie es nur mit der Bestätigung durch ein anderes aktiviertes Verfahren wieder entsperren.

Authentifizierungs-App (Authenticator)

Hier finden Sie eine Übersicht über Ihre registrierten Authentifizierungs-Apps. Bereits angelegte Authentifizierungs-Apps können gesperrt oder gelöscht werden.

Es können bis zu drei Authentifizierungs-Apps angelegt werden. Sie können auch das gesamte Verfahren deaktivieren, dadurch können Sie es nicht mehr verwenden, bis Sie es wieder aktivieren.

Verfahrensstatus: **aktiviert**

Name	Anlegezeitpunkt	Sperrzeitpunkt	Sperrgrund	Status	Aktionen
Google Auth iPhone	29.06.2023 12:17			aktiv	<input type="button" value="Sperren"/> <input type="button" value="Löschen"/>

Sperren und Löschen einer Authentifizierungs-App

Kontakt bei weiteren Fragen

Die Einrichtung der Multifaktor-Authentifizierung ist ein wichtiger Schritt zur Verbesserung der Sicherheit Ihrer Daten und der universitären IT-Systeme. Wir empfehlen Ihnen dringend, diese zusätzlichen Sicherheitsmaßnahmen so schnell wie möglich vollständig einzurichten. Falls Sie noch offene Fragen haben oder weitergehende Hilfe benötigen, wenden Sie sich bitte an den Support:

- **+49 30 838-77777**
- service@fu-berlin.de

Hinweis:

Bitte denken Sie daran, dass Sie Ihren zweiten Faktor (Code-Matrix, Authentifizierungs-App, Sicherheitsschlüssel / Passkey oder Telefon-PIN) niemals mit jemandem teilen sollten. Auch unser IT-Personal wird Sie niemals nach Ihrem zweiten Faktor oder Ihrem Passwort fragen.

Security: Setting up secure login procedures (multi-factor authentication)

Introduction

The protection of your personal and academic data at Freie Universität Berlin is just as important to us as it is to you. That is why we have introduced **multi-factor authentication (MFA)** for all FU accounts. In addition to your password, a second security factor is required to log in. This step significantly increases the security of your data, as a potential attacker now needs both your password and an independent second factor to access your account.

You can activate several different login methods simultaneously as your second factor (hence: multifactor). It is sufficient for logging in if you can always use one of your activated procedures in addition to your password - however, it makes sense to set up several of the procedures in case you lose access to one.

The following sections explain how to set up the login procedures. Please remember that you should **never share your second factor** (code matrix, authentication app, security key / passkey or phone PIN) with anyone - nor should you share your password. Our IT staff will also never ask you for your second factor or password.

To fully set up and manage the secure login procedures, please first navigate to the Account → Multifactor Authentication section in the FUB-IT portal:

<https://portal.zedat.fu-berlin.de/>

Homepage > Account > Multi-factor Authentication

Multi-factor Authentication

This is an overview of your secure login procedures with multi-factor authentication. These serve to protect your account from unauthorized access and are requested in addition to your password. You will get a short description of the procedures if you move your mouse pointer or finger over the respective procedure. You can select one of the methods as the default, which will then be used as the preferred method. By clicking on the name of the procedure or on 'Manage', you get further information and have the possibility to activate or deactivate the procedure or to set up new keys.

You have only activated the code matrix procedure. It is strongly recommended that you set up at least one other procedure.

Default Procedure

Procedure	Status	Actions
 Code Matrix	active	<button>Manage</button>

Other Procedures

Procedure	Status	Actions
 Security Key / Passkey	inactive	<button>Manage</button>
 Authenticator App	inactive	<button>Manage</button>
 Telephone TAN	inactive	<button>Manage</button>

Help

The individual procedures are explained here.

[Help on the procedures](#)

Portal page for the secure login procedures

Here you will find an overview of your login procedures. The individual procedures are listed in the table. If you click on the name of a procedure or on Manage in the Actions column, you will then be taken to the special configuration page for the respective procedure so that you can set it up. In the Status column, you can see the current status of the individual procedures - e.g. whether a procedure is activated, deactivated or blocked. How you can block, delete or deactivate a procedure and what this means is explained in a separate section later in these instructions.

Initially, only the „Code matrix“ procedure is activated and set as the default. If you want to use a procedure other than your default procedure, you can specify this in the Actions column after activating the procedure by clicking the Set as default button.

You will also find a brief overview of the individual registration procedures under Help on the procedures.

In the Email notification area, you can set whether you want to receive a security notification by email when you attempt to log in.

Procedure 1: Code matrix (standard / backup)

The „Code matrix“ procedure is always activated and is intended for the initial setup and as a backup. When using this procedure, you will be asked for six random positions from your individual code matrix. The code matrix is usually first sent to you by post. Only one code matrix is active at a time. When a new code matrix is issued, the previous one becomes invalid.

	1	2	3	4	5	6	7	8	9
A	M	C	E	s	s	i	V	g	9
B	J	k	W	7	N	b	h	E	k
C	6	H	q	U	G	9	u	R	9
D	d	M	J	S	J	P	w	h	K
E	J	H	m	a	d	t	g	7	2
F	U	P	2	t	j	D	4	M	g
G	D	e	R	q	K	7	W	a	d
H	E	f	N	j	b	4	d	W	9
I	L	b	i	3	U	g	5	8	Q



Example of a code matrix

- The individual 9x9 code matrix contains random lower and upper case letters and numbers.
- During the registration process using this method, you will be asked to enter 6 randomly selected fields from this matrix.

- The fields are named according to their row and column. The names of the items each consist of a letter (A-I), which indicates the row, and a number (1-9), which indicates the column.
- If requested, please enter the requested items from your matrix in the correct order without spaces and in upper and lower case into the input field and confirm your registration.
- Example (according to the sample matrix above): If you are asked about the content of the field G8 field, you must enter the letter a must be entered.

Homepage > Account > Multi-factor Authentication > Confirmation

Confirm operation with the Code Matrix procedure

Please enter the requested positions from the code matrix PIIX002060C5

A1 A4 A2 A0 A0 A4

Example of a code matrix query

- Keep the code matrix in a safe place and do not share it with anyone.
- If you have activated one of the other login methods, you can have a new code matrix issued in the portal yourself if required (Portal → Account → Multifactor authentication → Code matrix → Issue new matrix). The old matrix loses its validity and can no longer be used. If you have not activated any of the other login methods, please contact User Service if you lose your matrix.

Homepage > Account > Multi-factor Authentication > Code Matrix

 Code Matrix

When using this method, you will be asked for six random positions from a code matrix. The positions are each composed of a letter (A-I) indicating the row and a digit (1-9) indicating the column. To log in, enter the characters at the prompted positions in the correct order. For employees the Code Matrix procedure is always enabled and is intended for initial setup and as a backup. Only **one** code matrix is active at a time. When a new one is issued, the previous one will be deleted. You can issue a new matrix here any time. Your old matrix will be deleted if present.

Serial number	Setup time	Locking time	Lock reason	Status
PIIX002060C5	29.10.2024 16:20			active

Portal page for managing the code matrix

Adding further login procedures

Setting up at least one of the following additional procedures makes the login process considerably easier. To do this, first navigate to Account → Multifactor authentication in the FUB-IT portal and click on the corresponding procedure.

Homepage > Account > Multi-factor Authentication

Multi-factor Authentication

This is an overview of your secure login procedures with multi-factor authentication. These serve to protect your account from unauthorized access and are requested in addition to your password. You will get a short description of the procedures if you move your mouse pointer or finger over the respective procedure. You can select one of the methods as the default, which will then be used as the preferred method. By clicking on the name of the procedure or on 'Manage', you get further information and have the possibility to activate or deactivate the procedure or to set up new keys.

You have only activated the code matrix procedure. It is strongly recommended that you set up at least one other procedure.

Default Procedure

Procedure	Status	Actions
 Code Matrix	active	<button>Manage</button>

Other Procedures

Procedure	Status	Actions
 Security Key / Passkey	inactive	<button>Manage</button>
 Authenticator App	inactive	<button>Manage</button>
 Telephone TAN	inactive	<button>Manage</button>

Help

The individual procedures are explained here.

[Help on the procedures](#)

Portal page for the secure login procedures

Procedure 2: Authentication app (Authenticator) (Recommended)

With the „Authentication app“ login procedure, a time-based, one-time confirmation code is generated in your app during the login process (TOTP / Time-based One-time Password). You enter this in addition to your password when prompted during the login process. An authentication app is a quick and easy way to log in securely in everyday life. You can use any TOTP authentication app (e.g. 2FAS Authenticator, Google Authenticator, Microsoft Authenticator). You can set up up to **three apps** on different devices and use them alternatively.

Step-by-step instructions for the 2FAS Authenticator:

- In the FUB-IT portal, navigate to Account → Multifactor authentication → Security Key/Passkey and click on Set up now. Then click on Next.

Homepage > Account > Multi-factor Authentication > Authenticator App

Authenticator App

Here you can find an overview of your authentication apps. Authentication apps that have already been created can be locked or deleted. Up to three authentication apps can be created. You can also disable the entire procedure, which will prevent you from using it until you enable it again.

Status of procedure: The procedure is not set up.

Portal page for managing the authenticator apps

- First assign a name for this authenticator. If you set up several authenticator apps, this name will help you with the respective identification. Then click on Next.

Namen vergeben

Damit Sie die App wiedererkennen, geben Sie ihr einen aussagekräftigen Namen. Es sind nur die folgenden Zeichen erlaubt: A-Z, a-z, 0-9, Bindestrich und Leerzeichen.

Geben Sie hier einen Namen ein:

- An individual QR code for setting up the app will now be displayed in the portal.

Homepage > Account > Multi-factor Authentication > Setup

Scan QR code

Scan this QR code with your Authenticator app. You can also click [this link](#). This will open your Authenticator app.

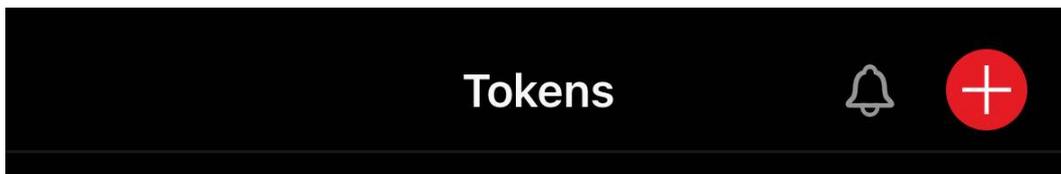


Now enter a generated numeric code to ensure that your Authenticator app has been set up correctly.

Numeric code:

Portal page for setting up the Authenticator app

- First install the 2FAS Authenticator app from the App Store (iOS) or Google Play Store (Android).
 - iOS: <https://apps.apple.com/de/app/2fa-authenticator-2fas/id1217793794>
 - Android: <https://play.google.com/store/apps/details?id=com.twofasapp>
- Open the 2FAS Authenticator app and tap on the plus symbol (+) to add your FU account.
- Select Scan QR code and scan the QR code that is displayed on the screen in the ZEDAT portal. You may need to allow the app to access the camera beforehand.



- The app will now generate a 6-digit code that is renewed every 30 seconds. Enter this code in the input field below in the portal.

Geben Sie nun einen generierten Zifferncode ein, um sicherzustellen, dass Ihre Authenticator App korrekt eingerichtet wurde.

Zifferncode:

Zurück

Weiter

Enter the generated code in this field



Example of a code in the 2FAS Authenticator app

- Finally, confirm the setup by using a procedure that is already active, such as your code matrix.
- For future logins, you can now use the time-based numeric code from the app as your second factor when prompted.

Procedure 3: Security key / passkey

In the security key / passkey procedure, you can set up a physical key (e.g. Yubico Security Key) or so-called passkeys. These are digital security keys that consist of a public/private key pair. Passkeys can be stored on your device (e.g. with Windows Hello) or synchronized between different devices via a cloud (via Google account, Apple iCloud keychain). For passkeys on Apple devices (iPhone, iPad, Mac), for example, the iCloud Keychain must be activated - the key is then securely distributed to all your Apple devices via iCloud. Passkeys can be a very quick and easy way to log in securely in everyday life.

If you have set up a hardware security key, you must always have it with you to log in. With hardware keys, it is usually sufficient to tap the inserted key after entering your password or hold it against the back of your smartphone (NFC) to use it. You may need to secure USB security keys with a PIN that is requested before use.

You can set up to **three keys** and use them alternatively.

Setting up a security key / passkey:

- In the FUB-IT portal, navigate to Account → Multifactor Authentication → Security Key / Passkey and click Set up now. Then click on Next.

Homepage > Account > Multi-factor Authentication > Security Key / Passkey

Security Key / Passkey

You can order Yubico USB Security Keys in Unikat. Item number 83.8880001089 and ITM128602, alternatively search for 'Yubico'.

You can set up physical keys (e.g. Yubico USB Security Key) or so-called passkeys as your security keys. Passkeys can be stored in your device (e.g. Windows Hello) or synchronized between different devices via a cloud (via Google account, Apple iCloud keychain). You must secure a USB key with a PIN that is requested before use. To set up and use the key, follow the instructions in your browser, which appear as pop-ups. You can set up to **three** keys and use them alternatively.

Status of procedure: The procedure is not set up.

Set up now

Back

Portal page for managing the security keys / passkeys

- First assign a name for this key. If you set up several keys, this name will help you to identify them.

Homepage > Account > Multi-factor Authentication > Setup

Choose a name

To make the key recognizable, give it a meaningful name. Only the following characters are allowed: A-Z, a-z, 0-9, hyphen and space.

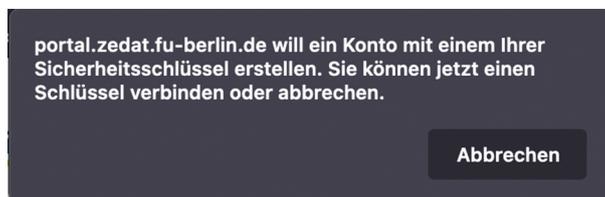
Enter a name here:

Key name

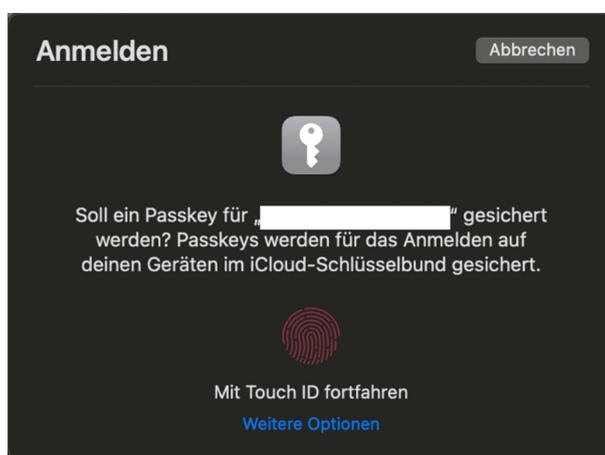
Back

Next

- You will then be asked to set up your security key, e.g. by inserting it into a USB port and activating it. This usually opens a pop-up window in the foreground. If your device/browser supports passkeys, a setup option for these will also be displayed here. Depending on the type of key and operating system, the procedure may differ from the one described here.
- Your browser or operating system will now guide you through setting up your security key / passkey.



The setup depends on the browser. Such a window may open in Mozilla Firefox, for example.



Such a window may open to set up a passkey in Safari on a Mac or iOS device.

- Please follow these instructions. After successful setup, you will be automatically re-directed to the next step.
- Finally, confirm the setup by using a procedure that is already active.
- Please note that a physical security key must be inserted into the computer each time you log in and activated when prompted.

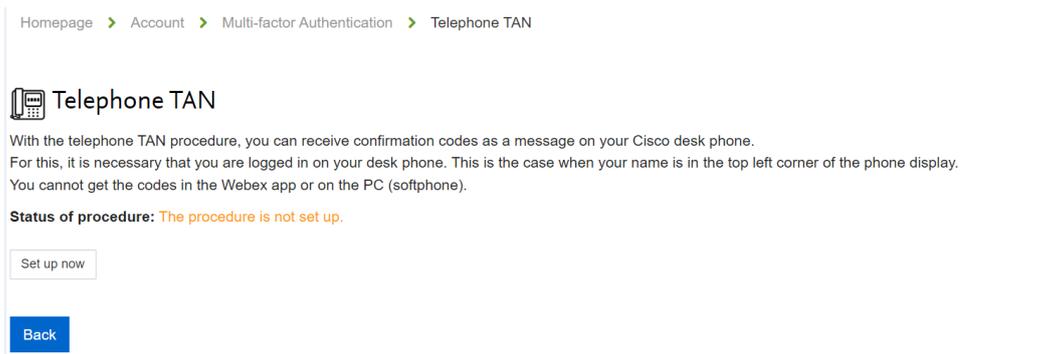
Procedure 4: Telephone TAN (*Only for employees*)

You can use the telephone TAN procedure to receive confirmation codes as a message on your Cisco desk phone. To do this, you must be logged on to your desk phone. This is the case if your name is shown in the top left-hand corner of the phone display. You will **not** receive the codes in the Webex app or on the PC (softphone).

Setting up the telephone TAN:

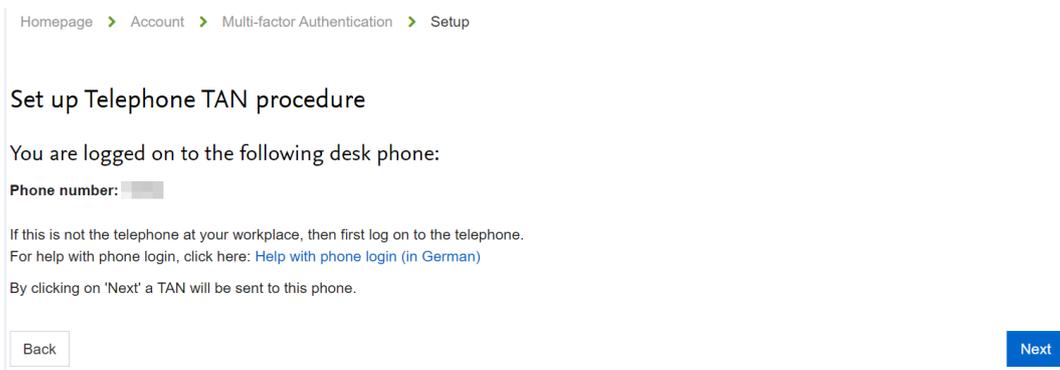
- Make sure you are logged in to your desk phone with your FU account. (user name + telephone PIN)

- In the FUB-IT portal, navigate to Account → Multifactor authentication → Telephone TAN and click on Set up now. Then click on Next.



Portal page for managing the telephone TAN procedure

- Confirm the details of your desk phone on the screen and then click Next



Portal page with information about the registered telephone

- The telephone TAN now appears as a message on the screen of your Cisco desk phone.



Example of a TAN on the Cisco desk phone

- Now enter the displayed TAN in the input field in the portal.
- Finally, confirm the setup by using a procedure that is already active.
- For future logins, you will receive a message on your registered desk phone to complete the login process.

Security: Blocking and deactivating login procedures (multi-factor authentication)

Loss of the code matrix

If you lose your code matrix, you should issue yourself with a new matrix. The previous code matrix can then no longer be used for authentication. As already described in the explanation of the code matrix, navigate to the subpage for the code matrix in the FUB-IT portal under Account → Multifactor authentication and click on the corresponding button. You need an activated additional login procedure for this. If you have not activated another procedure, please contact User Service.

Deactivating other procedures

You can deactivate the Authenticator app, security key and telephone TAN login procedures if you do not want to use them (temporarily) for authentication. To do this, navigate back to the FUB-IT portal under Account → Multifactor authentication to the corresponding subpage of the respective procedure and click on Deactivate.

Locking and deleting individual apps/keys

With the authentication app and security key / passkey procedures, you can either temporarily block or permanently delete individual apps/keys, for example if you lose your smartphone or hardware security key. To do this, navigate back to the FUB-IT portal under Account → Multifactor authentication to the corresponding subpage of the respective procedure and click on Lock or Delete in the Actions column. If you block a procedure, you can only unblock it again with the confirmation of another activated procedure.

Homepage > Account > Multi-factor Authentication > Authenticator App

Authenticator App

Here you can find an overview of your authentication apps. Authentication apps that have already been created can be locked or deleted. Up to three authentication apps can be created. You can also disable the entire procedure, which will prevent you from using it until you enable it again.

Status of procedure: active

Name	Setup time	Locking time	Lock reason	Status	Actions
Auth iPhone	29.10.2024 16:45			active	<input type="button" value="Lock"/> <input type="button" value="Delete"/>

Locking and deleting an authentication app

Contact for further questions

Setting up multi-factor authentication is an important step towards improving the security of your data and the university's IT systems. We strongly recommend that you set up these additional security measures in full as soon as possible. If you have any questions or require further assistance, please contact User Services.

- +49 (0)30 838 56069
- service@fu-berlin.de

Note:

Please remember that you should never share your second factor (code matrix, authentication app, security key or telephone PIN) with anyone. Our IT staff will also never ask you for your second factor or password.