

Die Zwei-Faktor-Authentisierung (2FA)

1. Information

Die Universität Oldenburg ist einer anhaltenden Bedrohung durch Cyberattacken ausgesetzt. Häufig versuchen Angreifende, über Phishing-Mails an Passwörter zu gelangen. Als zusätzlichen Schutz vor Angreifenden, die sich auf diese Weise Zugriff auf Konten und IT-Systeme verschaffen wollen, führt die Universität die sogenannte Zwei-Faktor-Authentisierung (2FA) ein. Bei der Anmeldung wird künftig nach der Passworteingabe eine zusätzliche Bestätigung mittels eines „zweiten Faktors“ benötigt.

2FA - was ist das?

Zwei-Faktor-Authentisierung (2FA) beschreibt die Authentisierung mit mehr als einem Faktor, also die Anmeldung an IT-Systemen mit einem Passwort und einem zusätzlichen Schutzmechanismus. So wird verhindert, dass unbefugte Dritte Zugang zu Daten oder Funktionen erhalten, nur weil sie in den Besitz des Passworts gelangt sind. Wichtig ist, dass die Faktoren dabei aus verschiedenen Kategorien stammen, d.h. eine Kombination aus Wissen (in diesem Fall das Passwort) und Besitz (in diesem Fall der TOTP-Generator auf einem Smartphone oder Tablet) verwendet wird.

Was passiert, wenn ich den zweiten Faktor nicht einrichte?

Wenn Sie den zweiten Faktor nicht einrichten, haben Sie ab dem 03. November 2025 keinen Zugriff mehr auf die IT-Systeme der Universität, dies betrifft bspw. Stud.IP und Ihr E-Mail-Postfach. Eine Kontolöschung oder Abmeldung tritt hingegen nicht ein, Sie bleiben also weiterhin im Gasthörstudium eingeschrieben.

2. Aktivierung des zweiten Faktors

Ab dem 03. November 2025 wird nach der Umstellung der Anmeldewebseite auch der zweite Faktor verpflichtend für Gasthörende sein. Das bedeutet, dass Sie dann zwingend die 2-Faktor-Sicherheit aktiviert haben müssen, um diese Dienste nutzen zu können! Nutzen Sie mindestens eine der nachfolgend genannten Möglichkeiten zur Aktivierung des 2-Faktor-Schutzes:

Möglichkeit 1: TOTP-Generator-App auf Smartphone oder Tablet

Möglichkeit 2: KeePassXC auf dem Computer (für **Gasthörende**, die kein Smartphone/Tablet besitzen)

3. TOTP-Generator-App auf Smartphone oder Tablet

Als zweiter Faktor bei der Anmeldung an Online-Diensten der Universität kann eine App auf Smartphone oder Tablet verwendet werden, welche bei Bedarf ein Einmalpasswort (auch TOTP = time-based one-time password) erzeugen kann, also einen 6-stelligen Zifferncode, der dann zusätzlich zum normalen Passwort eingegeben wird. Für das Einrichten des TOTP-Verfahrens im 2FA-Portal der Universität wird ein **mobiles Endgerät** (z. B. Smartphone oder Tablet) benötigt, welches einen QR-Code scannen kann.

TOTP-App installieren

Installieren Sie den TOTP-Dienst als App auf dem Smartphone oder einem anderen Endgerät. Wählen Sie dafür die App aus, die zum Betriebssystem des Geräts passt. Grundsätzlich können Sie jede Authentisierungs-App nutzen. Wir empfehlen die Nutzung folgender App:



2FA Authenticator

Die App können Sie im Google Playstore oder Apple Store kostenfrei herunterladen.

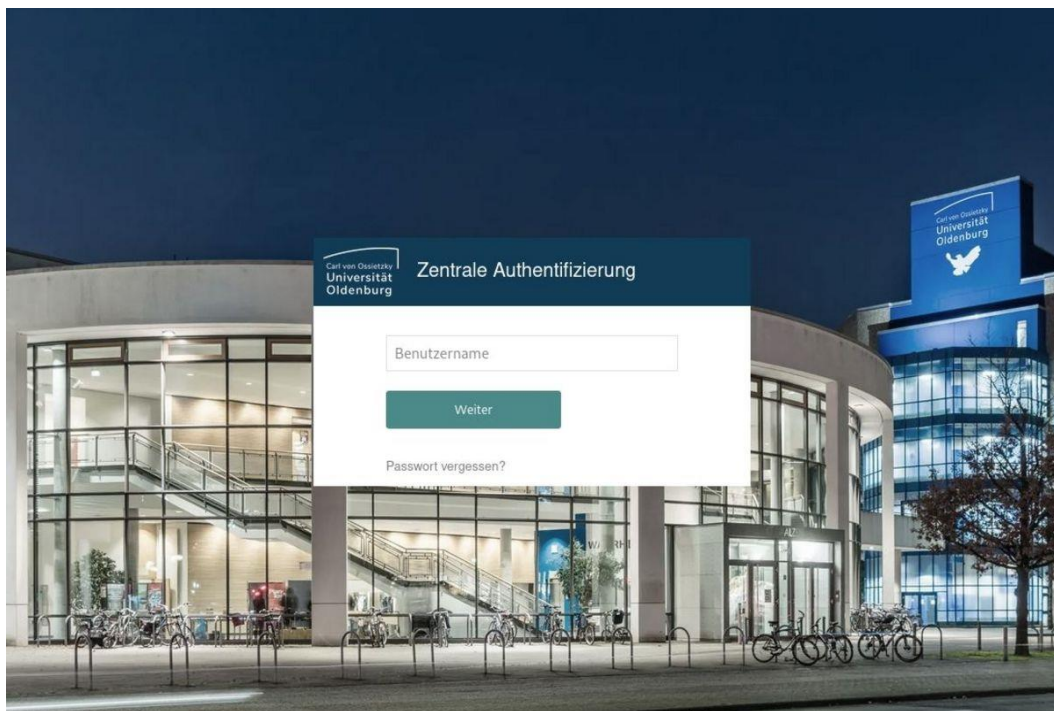
Sollten Sie bereits einen anderen TOTP-Dienst nutzen, können Sie auch diesen für die Zwei-Faktor-Authentisierung an der Universität Oldenburg nutzen

Wichtig: Damit Sie im späteren Verlauf (3. Schritt) den QR-Code scannen können, muss die App auf einem zweiten Gerät installiert sein, anders ist ein Fotografieren des Codes nicht möglich. Nutzen Sie also bspw. ein Laptop/PC für die Einrichtung und laden sich die App auf Ihr Handy oder Tablet.

Schritt-für-Schritt-Anleitung: TOTP-App im 2FA-Portal registrieren

Rufen Sie das 2FA-Portal der Universität Oldenburg auf und führen die Registrierung mit den nachfolgenden Schritten durch. Rufen Sie folgende Seite auf: <https://auth.uni-oldenburg.de>

Schritt 1: Loggen Sie sich im 2FA-Portal der Universität Oldenburg mit Ihrem Benutzernamen (Format abcd1234) und Ihrem Passwort ein.



Nach dem Einloggen im 2FA-Portal öffnet sich die Übersicht Ihrer Authentisierungsmethoden

Carl von Ossietzky
Universität
Oldenburg

2-Faktor Authentisierung (2FA) Portal

Willkommen beim Selbstbedienungsportal für Advanced Authentication

In diesem Portal können Sie Ihre Authentifizierungsmethoden verwalten.

Registrierte Methoden sind Authenticators, die Sie bereits registriert haben und zur Anmeldung verwenden können. Einmalpasswort-Methoden sind Authenticators mit Einmalpasswort.

Ihre registrierten Einfachmethoden für die Anmeldung

In diesem Abschnitt werden alle Methoden angezeigt, für die Sie sich registriert haben. Mit der Schaltfläche "+" können Sie weitere Methoden hinzufügen.

Automatisch erstellt
Flex OTP

Auto-created
Universitäts Passwort

Hinzufügen

Schritt 2: Wählen Sie die Option + zum Hinzufügen eines neuen Authentifikators.

Carl von Ossietzky
Universität
Oldenburg

2-Faktor Authentisierung (2FA) Portal

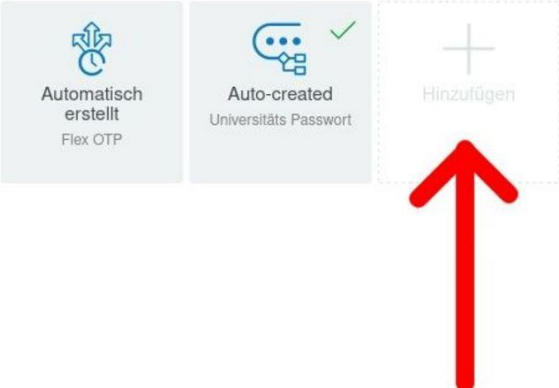
Willkommen beim Selbstbedienungsportal für Advanced Authentication

In diesem Portal können Sie Ihre Authentifizierungsmethoden verwalten.

Registrierte Methoden sind Authenticators, die Sie bereits registriert haben und zur Anmeldung verwenden können. Einmalpasswort-Methoden sind Authenticators mit Einmalpasswort.

Ihre registrierten Einfachmethoden für die Anmeldung

In diesem Abschnitt werden alle Methoden angezeigt, für die Sie sich registriert haben. Mit der Schaltfläche "+" können Sie weitere Methoden hinzufügen.



The screenshot shows three cards in a row. The first card is titled 'Automatisch erstellt Flex OTP' and has a blue icon of three arrows pointing outwards. The second card is titled 'Auto-created Universitäts Passwort' and has a blue icon of a speech bubble with a checkmark. The third card is titled 'Hinzufügen' and has a grey plus sign icon. A large red arrow points upwards from below the 'Hinzufügen' card.

Carl von Ossietzky
Universität
Oldenburg

2-Faktor Authentisierung (2FA) Portal

Verfügbare Methoden für die Registrierung

Wählen Sie eine Authentifizierungsmethode für die Registrierung aus. Nach der Registrierung kann die Methode zur Anmeldung verwendet werden. Einmalpasswort-Methoden sind Authenticators mit Einmalpasswort.



The screenshot shows four cards in a row. The first card is titled 'Einmalpasswort (HOTP)' and has a grey icon of a USB key. The second card is titled 'Einmalpasswort (TOTP)' and has a grey icon of a clock. The third card is titled 'Universitäts Passwort' and has a blue icon of a speech bubble with a checkmark. The fourth card is titled 'YubiKey (FIDO2)' and has a grey icon of a globe with a padlock. A large red arrow points upwards from below the 'Einmalpasswort (TOTP)' card.

Klicken Sie „Einmalpasswort (TOTP) an

Schritt 3: Es öffnet sich eine Eingabemaske für die Erstellung eines QR Codes. Hier angegebene Felder sind hauptsächlich zur eigenen Identifizierung des Einmalpassworts in der App des mobilen Endgerätes.

2-Faktor Authentisierung (2FA) Portal

Einmalpasswort bezeichnet wird. Dieses Einmalpasswort muss innerhalb eines bestimmten Zeitraums verwendet werden.

Anzeigename
 Geben Sie hier einen freigeählten Namen ein

Kategorie Belassen Sie die Kategorie auf „Standard“

Dienstname Der Dienstname ist ebenfalls frei wählbar, schreiben Sie bspw. „Uni Oldenburg“ o.ä.


Kontoname Geben Sie hier Ihre Kennung ein

Diese Methode mit einer der folgenden Optionen verwenden:

- Geben Sie im Abschnitt zum OATH-Token die Seriennummer des OATH-Tokens ein, die sich üblicherweise auf der Rückseite des Tokens befindet. Generieren Sie ein Einmalpasswort vom Token und geben Sie es an.
- Klicken Sie auf QR-Code abrufen und scannen Sie dann den QR-Code mit einer Smartphone-App.

OATH-Token

Rufen Sie den QR-Code ab

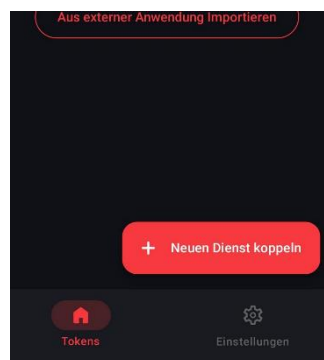


Schritt 4: Öffnen Sie die 2FA-App. Hier werden Sie im Verlauf der Einrichtung aufgefordert den gerade generierten QR-Code zu scannen.

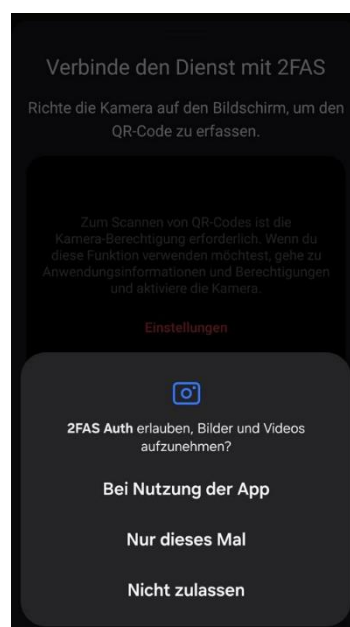
Schritt 5: Öffnen Sie ihre installierte TOTP App (hier im Beispiel 2FAS)



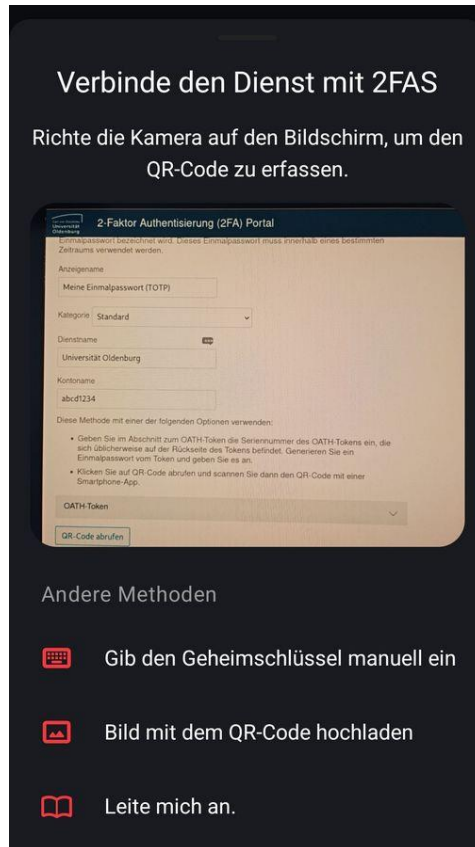
Schritt 6: Wählen Sie in der App „+ Neuen Dienst koppeln“ aus. (Ggf. werden Sie dazu aufgefordert, mit Google Drive o.ä. zu synchronisieren. Bitte tun Sie dies NICHT!)



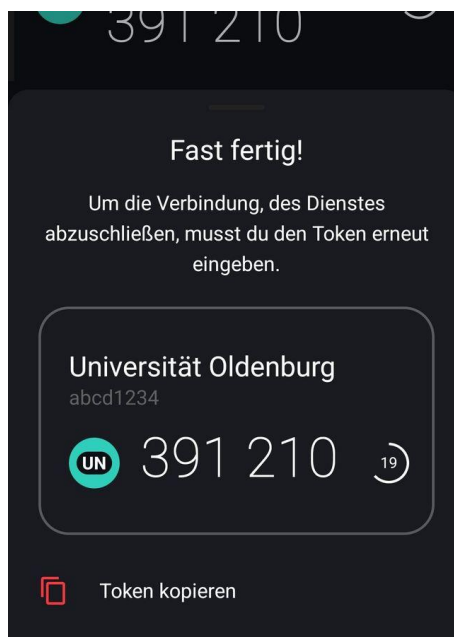
Schritt 7: Bei Abfrage von Berechtigungen die Nutzung der Smartphone-Kamera erlauben



Schritt 8: Scannen Sie den QR-Code vom PC-Bildschirm mit der Smartphone-Kamera



Schritt 9: Nach dem Einscannen des QR-Codes wird ein erstes zeitliches TOTP (Einmalpasswort, 6-stelliger Zifferncode) angezeigt. Die Einrichtung ist damit abgeschlossen.



Schritt 10: Speichern Sie nun die eingerichtete Methode über den Button **"Speichern"**.

Einmalpasswort bezeichnet wird. Dieses Einmalpasswort muss innerhalb eines bestimmten Zeitraums verwendet werden.

Anzeigename
Meine Einmalpasswort (TOTP)

Kategorie Standard

Dienstname
Universität Oldenburg

Kontoname
abcd1234

Diese Methode mit einer der folgenden Optionen verwenden:

- Geben Sie im Abschnitt zum OATH-Token die Seriennummer des OATH-Tokens ein, die sich üblicherweise auf der Rückseite des Tokens befindet. Generieren Sie ein Einmalpasswort vom Token und geben Sie es an.
- Klicken Sie auf QR-Code abrufen und scannen Sie dann den QR-Code mit einer Smartphone-App.

OATH-Token

QR-Code abrufen

Speichern Abbrechen

Im 2FA-Portal sehen Sie in der Übersicht Ihrer Authentisierungsmethoden nun, dass die Methode "Einmalpasswort (TOTP)" registriert ist. Bitte testen Sie die 2FA-Anmeldung jetzt unbedingt einmal!

2-Faktor Authentisierung (2FA) Portal

Willkommen beim Selbstbedienungsportal für Advanced Authentication

In diesem Portal können Sie Ihre Authentifizierungsmethoden verwalten.

Registrierte Methoden sind Authenticators, die Sie bereits registriert haben und zur Anmeldung verwenden können. Einmalpasswort-Methoden sind Authenticators mit Einmalpasswort.

Ihre registrierten Einfachmethoden für die Anmeldung

In diesem Abschnitt werden alle Methoden angezeigt, für die Sie sich registriert haben. Mit der Schaltfläche "+" können Sie weitere Methoden hinzufügen.

Meine Einmalpasswo... Einmalpasswort (TOTP)	Auto-created Flex OTP	Automatisch erstellt Universitäts Passwort	USB-A one YubiKey (FIDO2)	Hinzufügen
--	--------------------------	--	------------------------------	------------

Beratungsmöglichkeiten

Sollten Sie Unterstützung bei der Installation benötigen oder Fragen haben, wenden Sie sich bitte an den IT-Dienst der Universität. Die dortigen Kolleg*innen helfen gerne weiter.

Kontakt

IT-Servicedesk

Mo. – Do. 09:00 – 15:30 Uhr und Fr. 09:00 – 12:00 Uhr

E-Mail: Servicedesk@uol.de oder Tel.: 0441/798-5555

IT-Beratung

Mo. – Fr. 09:00 – 18:00 Uhr und Sa. 10:00 – 18:00 Uhr

Sie finden die IT-Beratung am Campus Haarentor in den Räumen der Zentralbibliothek auf der Ebene 1 und dort im Saal 1.