

Moodle für externe User

[See english version below](#)

Login mit Zwei-Faktor-Authentifizierung einrichten

Die Anmeldung („Authentifizierung“) in Moodle erfolgt durch eine [Zwei-Faktor-Authentifizierung](#). Die zwei Faktoren sind:

1. Faktor: Username + Passwort
2. Faktor: Yubikey ODER Authenticator-App

Yubikey

Ein [Yubikey](#) ist ein kleiner USB-Stick, der zur Authentifizierung in den Computer eingesteckt werden muss.

Authenticator-App

Eine Authenticator-App ist eine App auf einem separaten Handy. Diese App generiert einen einmaligen Code der für die Anmeldung benötigt wird. Bitte nutzen Sie die Apps:

Google Authenticator:

- Link zum Google Store [Google Authenticator App - Playstore](#)
- Link zum Apple Store [Google Authenticator App - App Store für iPhone](#)

FreeOTP:

- Link zum Google Store [FreeOTP App - Playstore](#)
- Link zum Apple Store [FreeOTP App - App Store für iPhone](#)

Zwei-Faktor-Authentifizierung (2FA) aktivieren

Wenn die 2FA noch nicht aktiviert ist, erscheint auf der [Moodle-Anmeldeseite](#) folgende Meldung:

Hallo, 

Sie sind aktuell in der Kulanzzzeit. Möglicherweise haben Sie nicht genügend Faktoren eingerichtet, um sich nach Ablauf der Kulanzzzeit weiter anmelden zu können. Überprüfen Sie Ihren Authentifizierungsstatus auf der Seite [Nutzerpräferenzen](#) und richten Sie weitere Authentifizierungsfaktoren ein. Ihre Kulanzzzeit läuft in 6 Tage 23 Stunden ab.

- Klicken Sie im rosa Kasten auf den Link https://moodle.haw-landshut.de/admin/tool/mfa/user_preferences.php [Nutzerpräferenzen](#) bzw. kopieren Sie den Link und öffnen Sie ihn im Browser, wenn Klicken nicht möglich ist.

Es öffnet sich diese Seite zur Multi-Faktor-Authentifizierung:

Multi-Faktor-Authentifizierung

Machen Sie Ihr Nutzerkonto sicherer, indem Sie für das Anmelden eine zusätzliche Bestätigung einrichten.

Authentifizierungstoken
Physikalischen Security Key oder Fingerabdruckscanner verwenden

Authenticator-App
Generieren Sie einen Bestätigungscode mit einer Authenticator-App.

Anleitung zur Multi-Faktor-Authentifizierung

Es gibt zwei Möglichkeiten für den zweiten Faktor: „Authentifizierungstoken“ (=Yubikey) oder „Authenticator-App“. Entscheiden Sie sich für einen der beiden Faktoren.

- Klick auf den greuen Button Einrichten in einem der beiden Bereiche („Authentifizierungstoken“ oder „Authenticator-App“).

1. Möglichkeit: Yubikey

Yubikey registrieren

Nach Wahl der Option „Yubikey“, öffnet sich die Seite „Security Key einrichten“:

Security Key einrichten

Ein Security Key ist ein physisches Gerät, mit dem Sie sich authentifizieren können. Security Key können USB-Token, Bluetooth-Geräte oder in Ihrem Telefon bzw. Computer integrierte Fingerabdruckscanner sein.

1. Geben Sie Ihrem Security Key einen Namen.

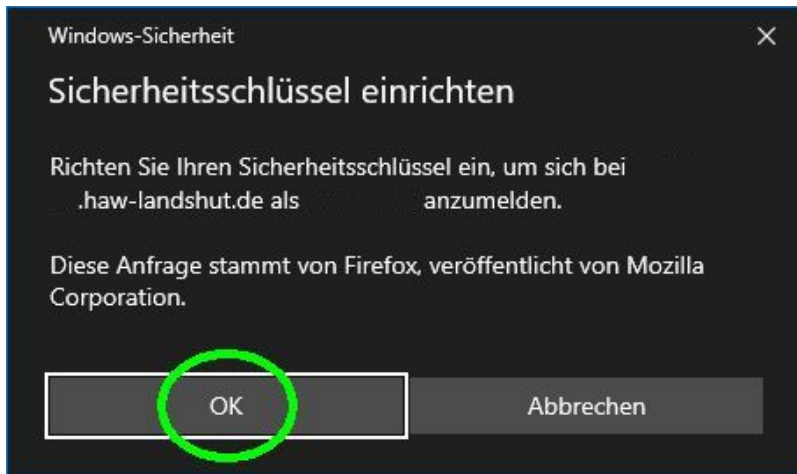
Name des Sicherheitsschlüssels

Dies hilft Ihnen herauszufinden, welchen Security Key Sie verwenden.

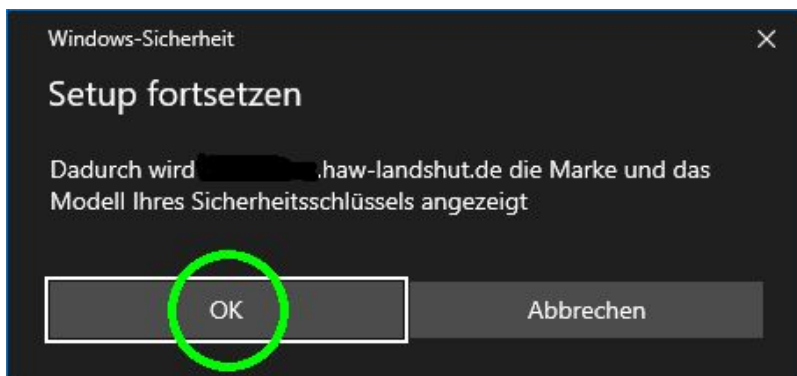
2. Einen Security Key registrieren

notwendig

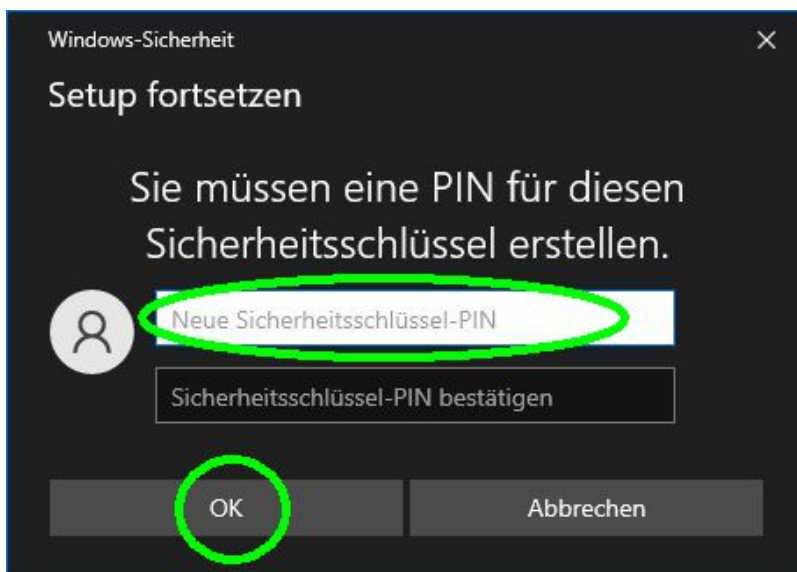
- Im Feld „Name des Sicherheitsschlüssels“ einen eindeutigen Name des Yubikeys eingeben. (Der Name ist frei wählbar.)
- Klick den grauen Button Security Key registrieren.



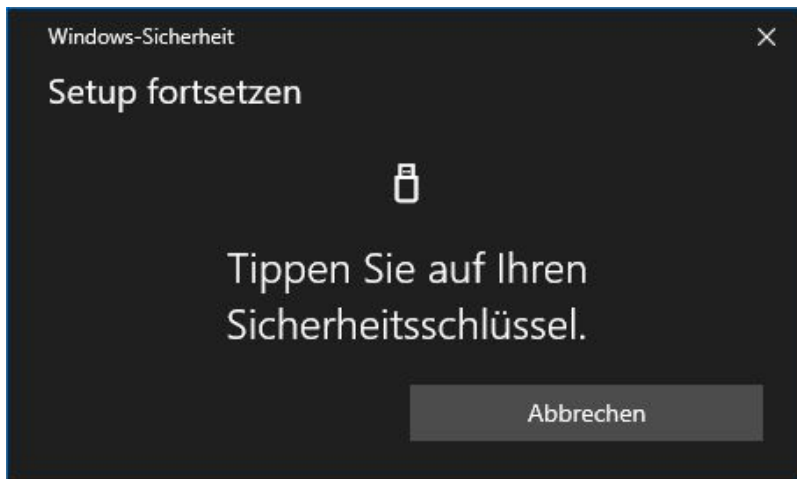
- Bestätige das Popup-Fenster „Sicherheitsschlüssel einrichten“ mit Klick auf OK.



- Bestätige das Popup-Fenster „Setup fortsetzen“ mit Klick auf OK.



- Im Popup-Fenster „Setup fortsetzen“ einen PIN eingeben. (Der PIN ist frei wählbar. Der PIN wird später für die Anmeldung benötigt.)
- Bestätige mit Klick auf OK.



- Beim Popup-Fenster „Tippen Sie auf Ihren Sicherheitsschlüssel“, tippe auf den Yubikey im USB-Anschluss.



- Evtl. öffnet sich ein Popup-Fenster neben der URL-Zeile im Browser. Klick auf den blauen Button Erlauben

Security Key einrichten

Ein Security Key ist ein physisches Gerät, mit dem Sie sich authentifizieren können. Security Key können USB-Token, Bluetooth-Geräte oder in Ihrem Telefon bzw. Computer integrierte Fingerabdruckscanner sein.

1. Geben Sie Ihrem Security Key einen Namen.

Name des Sicherheitsschlüssels

y-key

Dies hilft Ihnen herauszufinden, welchen Security Key Sie verwenden.

2. Einen Security Key registrieren

Security Key registrieren

Änderungen speichern Abbrechen

- Klick auf den grauen Button Änderungen speichern.

'Authentifizierungstoken - YK-dw' erfolgreich eingerichtet.

x

Multi-Faktor-Authentifizierung

Machen Sie Ihr Nutzerkonto sicherer, indem Sie für das Anmelden eine zusätzliche Bestätigung einrichten.

 Authentifizierungstoken Sie verwenden 'YK-dw' zur Authentifizierung. Aktiv Verwalten	 Authenticator-App Generieren Sie einen Bestätigungscode mit einer Authenticator-App. Einrichten
--	---

Anleitung zur Multi-Faktor-Authentifizierung

Die erfolgreiche Registrierung des Faktors „Authetifizierungstoken“ (=Yubikey) wird durch das „grüne Aktiv“ angezeigt.

2FA-Login mit Yubikey

- Loggen Sie sich aus Moodle wie gewohnt aus.

Verwenden Sie Ihr Nutzerkonto bei

 Hochschule Landshut

Anmelden mit Ihrem Moodle-Konto

Anmeldename

Kennwort

Login

Kennwort vergessen?

- Login im Bereich „Anmelden mit Ihrem Moodle-Konto“ (nicht „Verwenden Sie Ihr Nutzerkonto“)
- durch Eingabe von Anmeldename und Kennwort.
- Bestätigen Sie Ihre Anmeldung durch Klick auf Login.

Bestätigung in zwei Schritten

Um Ihr Nutzerkonto sicher zu halten, muss geprüft werden, ob Sie es wirklich sind.



Bestätigen Sie Ihre Identität per Security Key

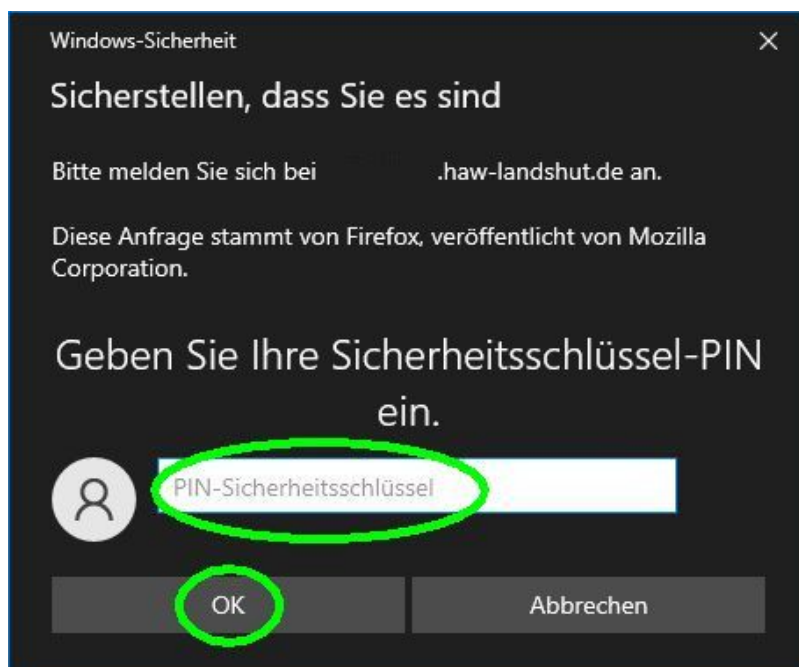
Klicken Sie auf "Weiter", um Ihren Security Key zu verwenden.

Weiter

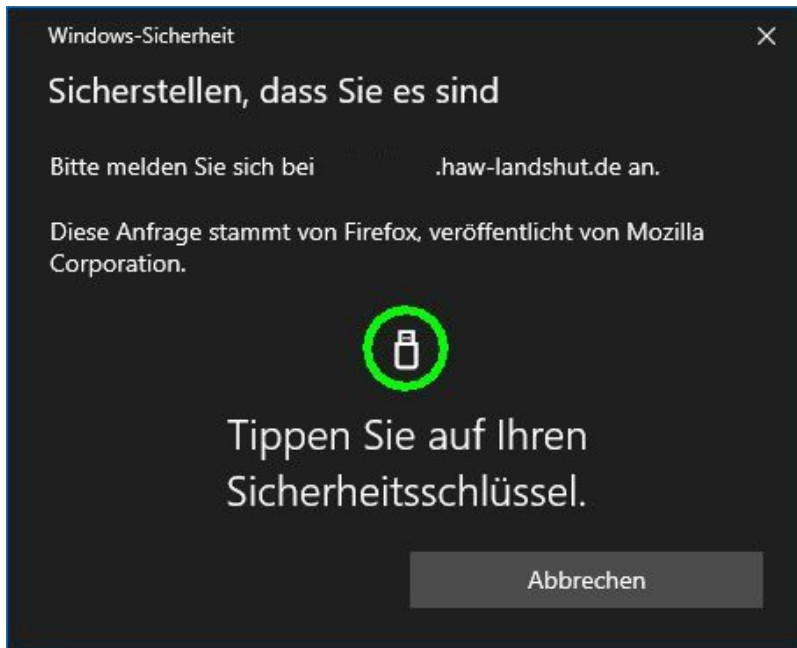
Anmeldung abbrechen

Brauchen Sie Hilfe? Anleitung zur Multi-Faktor-Authentifizierung

- Es öffnet sich die Seite „Bestätigung in zwei Schritten“-Seite. Klick auf Weiter.



- Im Popup-Fenster „Sicherstellen, dass Sie es sind“, den oben festgelegten PIN eingeben.
- Bestätige den PIN mit Klick auf OK.



- Wenn das Popup-Fenster „Sicherstellen, dass Sie es sind“, tippe auf den Yubikey am USB-Anschluss.

Sie sind wie gewohnt in Moodle angemeldet.

2. Möglichkeit: Authenticator-App

Multi-Faktor-Authentifizierung

Machen Sie Ihr Nutzerkonto sicherer, indem Sie für das Anmelden eine zusätzliche Bestätigung einrichten.

A screenshot of the 'Multi-Faktor-Authentifizierung' setup screen. It has two main options: 'Authentifizierungstoken' (Physical Security Key or Fingerprint scanner) and 'Authenticator-App' (Generate a confirmation code with an Authenticator App). Both options have a green 'Einrichten' button. The 'Einrichten' button for the 'Authenticator-App' is circled in green.

Anleitung zur Multi-Faktor-Authentifizierung

- Klick auf im Bereich „Authenticator-App“ auf Einrichten.

Authenticator-App einrichten

Um diese Methode einzurichten, benötigen Sie ein Gerät mit einer Authenticator-App. Wenn Sie keine App haben, können Sie eine herunterladen, z.B.: 2FAS Auth, FreeOTP, Google Authenticator, Microsoft Authenticator oder Twilio Authy.

1. Geben Sie Ihrem Gerät einen Namen.

Gerätename
 Dies hilft Ihnen herauszufinden, welches Gerät den Bestätigungscode erhält.

2. Scannen Sie den QR-Code mit Ihrer Authenticator-App.



Oder geben Sie die Details manuell ein.

3. Geben Sie den Bestätigungscode ein.

Bestätigungscode

 ● notwendig

- In das Feld „Gerätename“ einen (frei wählbar) Namen für das Handy oder Tablet mit der Authenticator-App eingeben.
- Öffne die Authenticator-App auf dem Handy oder Tablet und scanne den QR-Code vom Bildschirm.
- In der Authenticator-App wird ein Bestätigungscode generiert. Übertrage diesen Code in das Feld Bestätigungscode.
- Klick den grauen Button Änderungen speichern

'Authenticator-App - jhgf' erfolgreich eingerichtet.

x

Multi-Faktor-Authentifizierung

Machen Sie Ihr Nutzerkonto sicherer, indem Sie für das Anmelden eine zusätzliche Bestätigung einrichten.

 Authentifizierungstoken Physikalischen Security Key oder Fingerabdruckscanner verwenden Einrichten	 Authenticator-App Sie verwenden 'jhgf' zur Authentifizierung. Aktiv Verwalten
---	---

Anleitung zur Multi-Faktor-Authentifizierung

Der zweite

Faktor „Authenticator-App“ wird durch das „grüne Aktiv“ angezeigt.

2FA-Login mit Authenticator-App

- Loggen Sie sich aus Moodle wie gewohnt aus.

Verwenden Sie Ihr Nutzerkonto bei

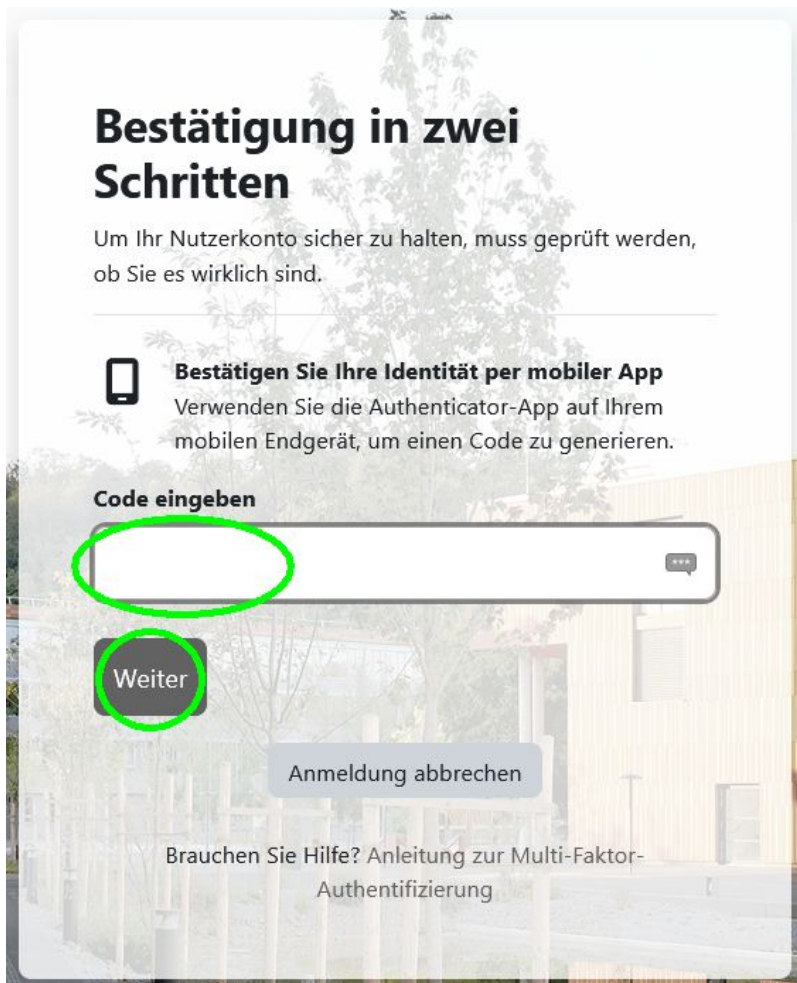
 Hochschule Landshut

Anmelden mit Ihrem Moodle-Konto



[Kennwort vergessen?](#)

- Login durch Klick auf Anmelden mit Ihrem Moodle-Konto (nicht „Verwenden Sie Ihr Nutzerkonto“.)



- Es öffnet sich die Seite „Bestätigen in zwei Schritten“-Seite.
- Öffne auf dem Handy oder Tablet die Authenticator-App.
- Gib den Code aus der App in das Feld „Code eingeben“ ein
- Klick auf den grauen Button Weiter.

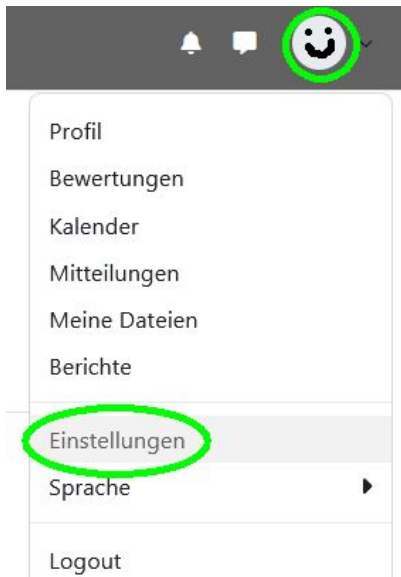
Sie sind wie gewohnt in Moodle angemeldet.

Verwaltung der Zwei Faktoren

Sie können den zweiten Faktor auch ändern (z.B. von Authenticator-App zu Yubikey wechseln) oder einen zweiten „zweiten Faktor“ hinzufügen, so dass Sie zur Anmeldung entweder einen Yubikey oder eine Authenticator-App verwenden können.

Wechsel von Authenticator-App zu Yubikey

Melden Sie sich zunächst mit zwei Faktoren in Moodle an.



- Klick rechts oben auf den Kreis mit dem User-Profil.
- Es öffnet sich ein Dropdown-Menü. Klick auf den Menüpunkt Einstellungen.

Einstellungen

Nutzerkonto

- [Profil bearbeiten](#)
- [Kennwort ändern](#)
- [Sprache wählen](#)
- [Foren einstellen](#)
- [Texteditor wählen](#)
- [Kalender einstellen](#)
- [Inhaltsspeicher einstellen](#)
- [Sicherheitsschlüssel](#)
- [Mitteilungen](#)
- [Systemnachrichten](#)
- [Multi-Faktor-Authentifizierung](#) (highlighted with a green circle)

Blogs

- [Blogeinstellungen](#)
- [Externe Blogs](#)
- [Externen Blog registrieren](#)

Badges

- [Badges verwalten](#)
- [Badges konfigurieren](#)

- Klick auf Multi-Faktor-Authentifizierung.

Multi-Faktor-Authentifizierung

Machen Sie Ihr Nutzerkonto sicherer, indem Sie für das Anmelden eine zusätzliche Bestätigung einrichten.

**Authentifizierungstoken**

Physikalischen Security Key oder Fingerabdruckscanner verwenden

[Einrichten](#) (highlighted with a green circle)

**Authenticator-App**

Sie verwenden 'android-handly' zur Authentifizierung.

Aktiv [Verwalten](#)

- Klick im Bereich „Authentifizierungstoken“ auf den grauen Button Einrichten.

Fahren Sie dann fort, wie im [Abschnitt Yubikey registrieren](#) beschrieben.

Wenn beide Faktoren „Authentifizierungstoken“ (=Yubikey) und „Authenticator-App“ registriert sind, erscheinen beide Bereiche mit „grünem Aktiv“. In diesem Zustand können beide Faktoren als zweiter Faktor verwendet werden.

'Authentifizierungstoken - y-key' erfolgreich eingerichtet.

x

Multi-Faktor-Authentifizierung

Machen Sie Ihr Nutzerkonto sicherer, indem Sie für das Anmelden eine zusätzliche Bestätigung einrichten.



Authentifizierungstoken
Sie verwenden 'y-key' zur Authentifizierung.

Aktiv

Verwalten



Authenticator-App
Sie verwenden 'android-handy' zur Authentifizierung.

Aktiv

Verwalten

Deaktivieren der Authenticator-App

Multi-Faktor-Authentifizierung

Machen Sie Ihr Nutzerkonto sicherer, indem Sie für das Anmelden eine zusätzliche Bestätigung einrichten.



Authentifizierungstoken
Sie verwenden 'y-key' zur Authentifizierung.

Aktiv

Verwalten



Authenticator-App
Sie verwenden 'android' zur Authentifizierung.

Aktiv

Verwalten

- Klick im Bereich „Authenticator-App“ auf den grauen Button Verwalten.

Authenticator-App verwalten

Gerät	Hinzugefügt	Zuletzt verwendet	Ersetzen	Entfernen
android-handy	22. September 2025, 14:52	-	Ersetzen	Entfernen

- Klick im Fenster „Authenticator-App verwalten“ auf den grauen Button Entfernen.

Authenticator-App ' entfernen? x

Sie können sich nicht mehr mit ' auf dieser Website anmelden.

Abbrechen Ja, entfernen

- Klick im Popup-Fenster „Authenticator-App“ entfernen auf den grauen Button Ja, entfernen.

Die Registrierung des Faktors „Authentifizierungstoken“ (=Yubikey) wird durch das „grüne Aktiv“ im entsprechenden Bereich angezeigt. Die Abmeldung des Faktors „Authenticator-App“ ist durch ein fehlendes „grünes Aktiv“ im entsprechenden Bereich zu erkennen.

Multi-Faktor-Authentifizierung

Machen Sie Ihr Nutzerkonto sicherer, indem Sie für das Anmelden eine zusätzliche Bestätigung einrichten.

 Authentifizierungstoken Sie verwenden 'y-key' zur Authentifizierung. Aktiv Verwalten	 Authenticator-App Generieren Sie einen Bestätigungscode mit einer Authenticator-App. Einrichten
--	--

Der Wechsel vom Faktor „Authentifizierungstoken“ (=Yubikey) zum Faktor „Authenticator-App“ erfolgt vice versa.

English Version

Moodle for external users

Set up login with two-factor authentication

The login („authentication“) in Moodle is done via a [two-factor authentication](#). The two factors are:

1. Factor 1: Username + Password
2. Factor 2: Yubikey OR Authenticator app

Yubikey

A [Yubikey](#) is a small USB stick that must be inserted into the computer for authentication.

Authenticator App

An authenticator app is an app on a separate mobile device. This app generates a one-time code that is required for login. Please use the apps: Google Authenticator or FreeOTP.

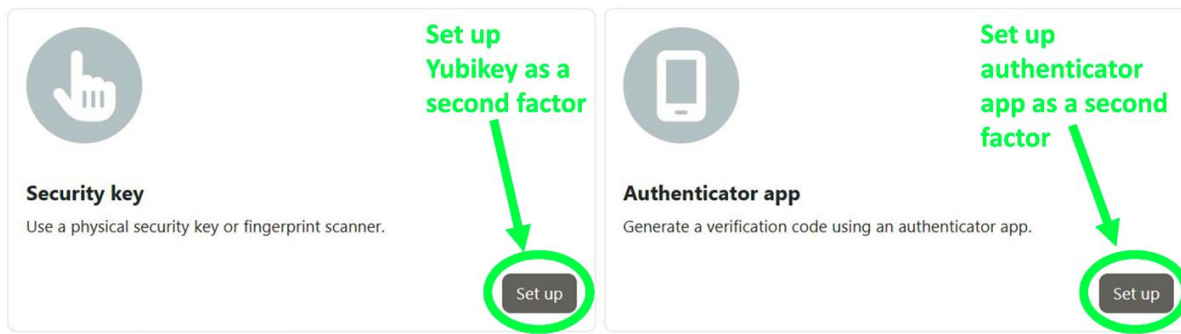
Enable Two-Factor Authentication (2FA)

If 2FA is not yet activated, you will be redirected to the [User preferences](#) page, and the following message will be shown to you. 

If you are not redirected automatically, please click this link to go to your [User preferences](#).

Multi-factor authentication

Make your account safer by requiring an additional verification method when you log in.



There are two options for the second factor: „Authentication token“ (= Yubikey) or „Authenticator app“. Choose one of the two factors.

- Click the gray Set up button in one of the two sections („Authentication token“ or „Authenticator app“).

1. Option: Yubikey

Register Yubikey

After selecting the „Yubikey“ option, the „Set up Security Key“ page opens:

Set up security key

A security key is a physical device that you can use to authenticate yourself. Security keys can be USB tokens, Bluetooth devices, or even built-in fingerprint scanners on your phone or computer.

1. Give your key a name.

Security key name

This helps you identify which security key you are using.

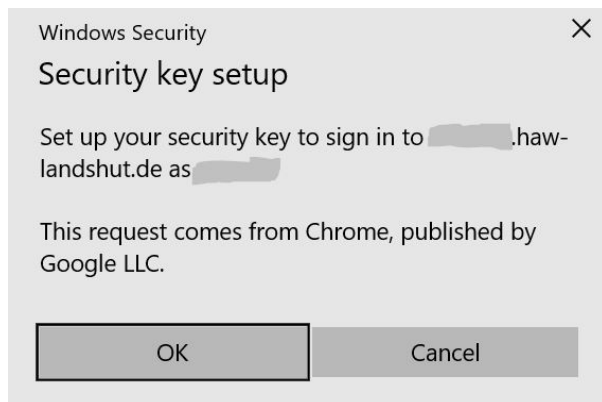
2. Register a security key.

Save changes

Cancel

i Required

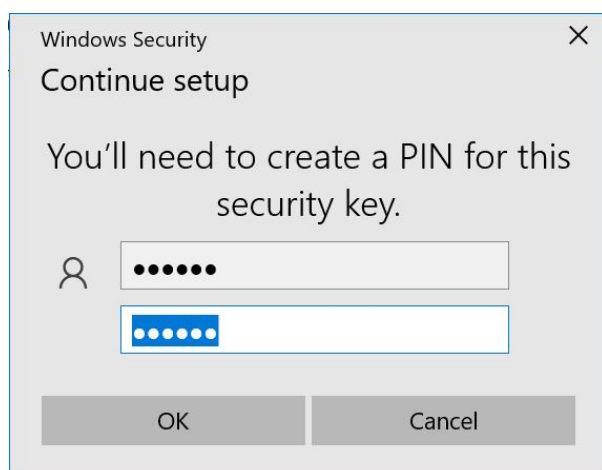
- In the „Name of the security key“ field, enter a unique Yubikey name. (The name can be chosen freely.)
- Click the gray Register Security Key button.



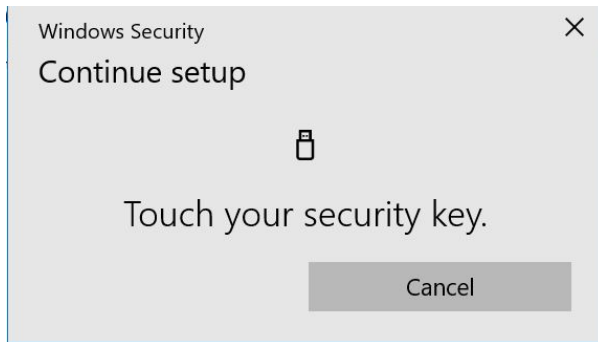
- Confirm the pop-up window „Set up security key“ by clicking OK.



- Confirm the pop-up window „Continue setup“ by clicking OK.



- In the pop-up window „Continue setup“, enter a PIN. (The PIN can be chosen freely. The PIN will be required later for login.)
- Confirm by clicking OK.



- When the pop-up window „Touch your security key“ appears, touch the Yubikey in the USB port.



- A pop-up window **may** appear next to the browser's address bar. Click the blue Allow button.

Set up security key

A security key is a physical device that you can use to authenticate yourself. Security keys can be USB tokens, Bluetooth devices, or even built-in fingerprint scanners on your phone or computer.

1. Give your key a name.

Security key name !

This helps you identify which security key you are using.

2. Register a security key.

! Required

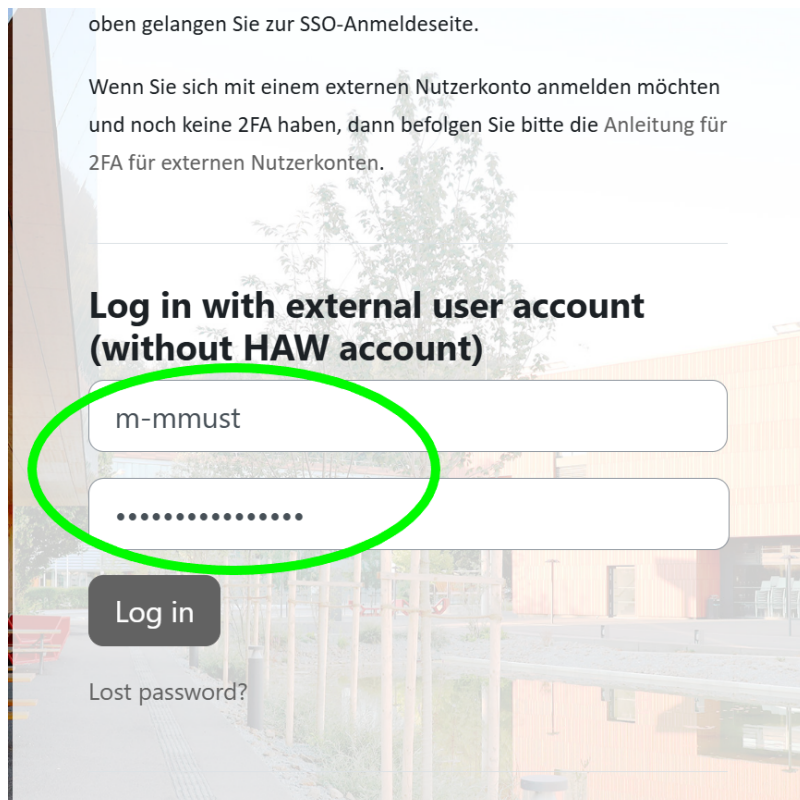
- Click the gray Save changes button.



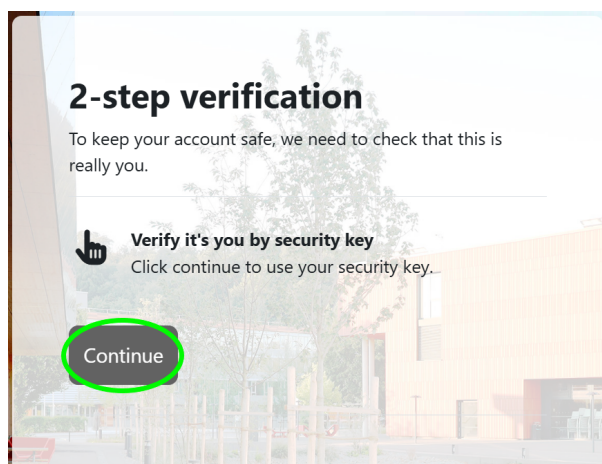
The successful registration of the „Authentication token“ factor (= Yubikey) is indicated by the green „Active“ status.

2FA login with Yubikey

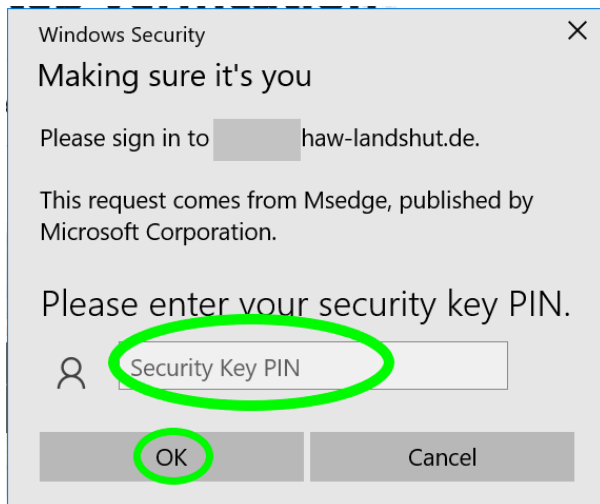
- Log out of Moodle as usual.



- Log in in the „Log in with your Moodle account“ section (not „Use your user account“) by entering your username and password.
- Confirm your login by clicking Log in.



- The „Two-step confirmation“ page opens. Click Continue.



- In the pop-up window „Make sure it's you“, enter the PIN you set earlier.
- Confirm the PIN by clicking OK.



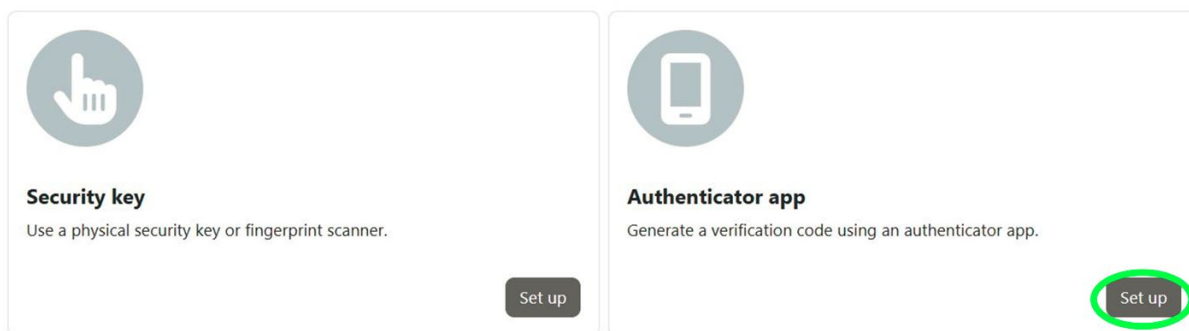
- When the pop-up window „Make sure it's you“ appears, touch the Yubikey in the USB port.

You are now logged into Moodle as usual.

2. Option: Authenticator app

Multi-factor authentication

Make your account safer by requiring an additional verification method when you log in.



Multi-factor authentication user guide

- In the „Authenticator app“ section, click Set up.

Set up authenticator app

To set up this method, you need to have a device with an authenticator app. If you don't have an app, you can download one. For example, 2FAS Auth, FreeOTP, Google Authenticator, Microsoft Authenticator or Twilio Authy.

1. Give your device a name.

Device name

eg "Work iPhone 11"

This helps you identify which device receives the verification code.

2. Scan the QR code with your authenticator app.



Scan the QR code with the authenticator app

Or enter details manually.

3. Enter the verification code.

Verification code

Save changes

Cancel

Required

- In the „Device name“ field, enter a name for the device (smartphone or tablet) with the authenticator app (can be chosen freely).
- Open the authenticator app on the device (smartphone or tablet) and scan the QR code from the screen.
- The authenticator app will generate a confirmation code. Enter this code in the Confirmation code field.
- Click the gray Save changes button.

'Authenticator app - Device1' successfully set up.

×

Multi-factor authentication

Make your account safer by requiring an additional verification method when you log in.



Security key

Use a physical security key or fingerprint scanner.

Set up



Authenticator app

You are using 'Device1' to authenticate.

Active

Manage

Multi-factor authentication user guide

The second factor „Authenticator app“ is indicated by the green „Active“ status.

The second

2FA-Login mit Authenticator-App

- Log out of Moodle as usual.

oben gelangen Sie zur SSO-Anmeldeseite.

Wenn Sie sich mit einem externen Nutzerkonto anmelden möchten und noch keine 2FA haben, dann befolgen Sie bitte die Anleitung für 2FA für externen Nutzerkonten.

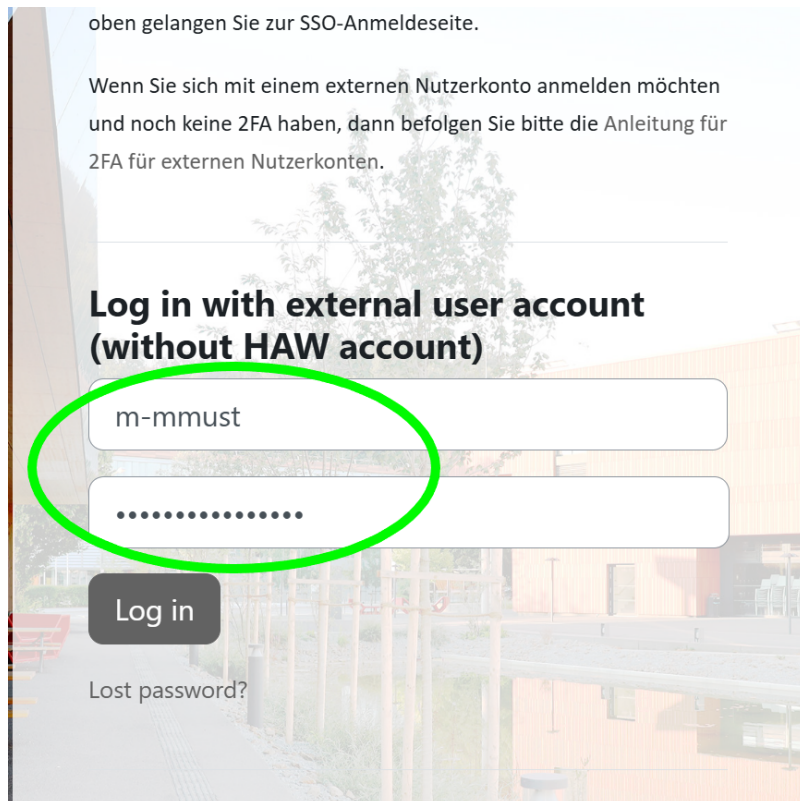
**Log in with external user account
(without HAW account)**

m-mmust

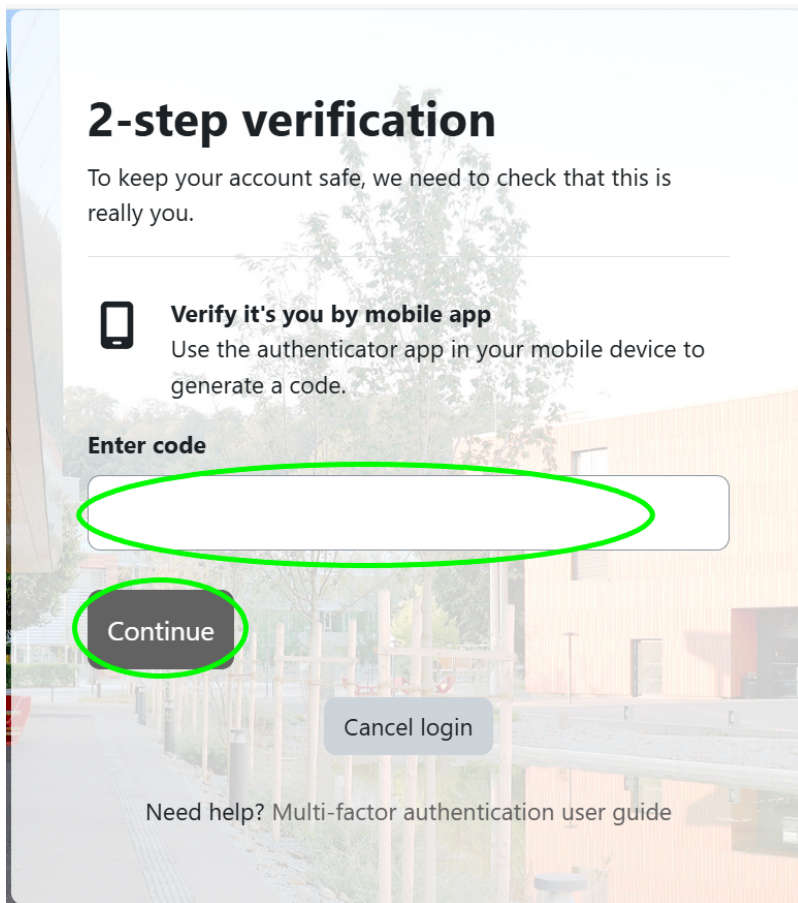
.....

Log in

Lost password?



- Log in by clicking Log in with your Moodle account (not „Use your user account“).



- The „Two-step confirmation“ page opens.
- Open the authenticator app on your device (smartphone or tablet).
- Enter the code from the app in the „Enter code“ field.
- Click the gray Continue button.

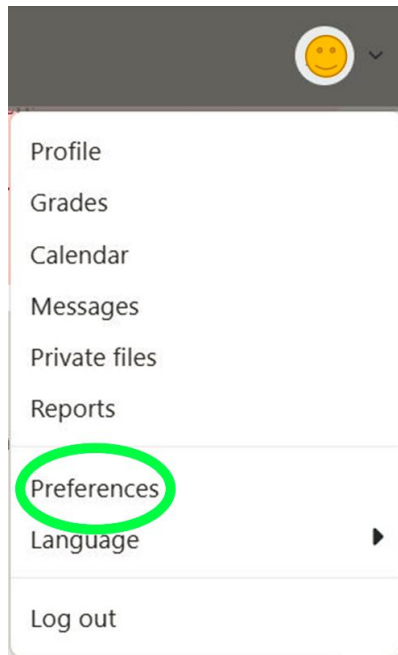
You are now logged into Moodle as usual.

Managing the two factors

You can also change the second factor (e.g., switch from authenticator app to Yubikey) or add a second „second factor“, so that you can log in using either a Yubikey or an authenticator app.

Switching from authenticator app to Yubikey

First, log in to Moodle with two-factor authentication.



- Click the circle with the user profile in the top right corner.
- A dropdown menu appears. Click the menu item Preferences.

Preferences

User account

[Edit profile](#)
[Change password](#)
[Preferred language](#)
[Forum preferences](#)
[Editor preferences](#)
[Calendar preferences](#)
[Content bank preferences](#)
[Security keys](#)
[Message preferences](#)
[Notification preferences](#)
[Multi-factor authentication preferences](#)

Badges

[Manage badges](#)
[Badge preferences](#)

- Click Multi-factor authentication preferences.

Multi-factor authentication

Make your account safer by requiring an additional verification method when you log in.



Security key
Use a physical security key or fingerprint scanner.

Set up



Authenticator app
You are using 'Device1' to authenticate.

Active

Manage

Multi-factor authentication user guide

- In the „Authentication token“ section, click the gray Set up button.

Then proceed as described in the [Yubikey registration section](#).

If both factors „Authentication token“ (= Yubikey) and „Authenticator app“ are registered, both sections appear with „green Active“. In this state, both factors can be used as the second factor.

'Security key - y-key' successfully set up.

Multi-factor authentication

Make your account safer by requiring an additional verification method when you log in.



Security key
You are using 'y-key' to authenticate.

Active

Manage



Authenticator app
You are using 'Device1' to authenticate.

Active

Manage

Deactivating the authenticator app

Multi-factor authentication

Make your account safer by requiring an additional verification method when you log in.



Security key
You are using 'y-key' to authenticate.

Active

Manage



Authenticator app
You are using 'Device1' to authenticate.

Active

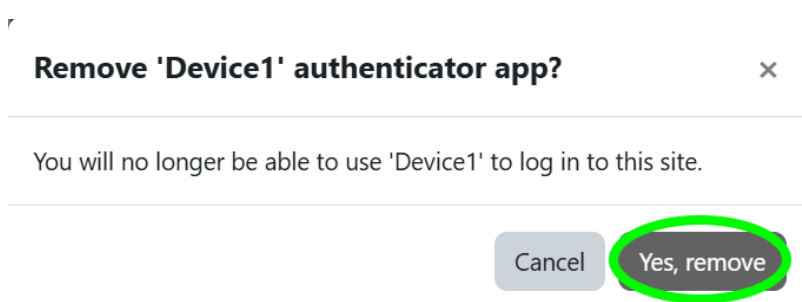
Manage

- In the „Authenticator app“ section, click the gray Manage button.

Manage authenticator app

Device	Added	Last used	Replace	Remove
Device1	26 January 2026, 7:48 PM	26 January 2026, 9:12 PM 14 mins ago	<button>Replace</button>	<button>Remove</button>

- In the „Manage authenticator app“ window, click the gray Remove button.



- In the pop-up window „Remove authenticator app“, click the gray Yes , remove button.

The registration of the factor „Authentication token“ (= Yubikey) is indicated by the „green Active“ in the corresponding section. The deregistration of the factor „Authenticator app“ is indicated by the absence of „green Active“ in the corresponding section.

Multi-factor authentication

Make your account safer by requiring an additional verification method when you log in.



Security key
You are using 'y-key' to authenticate.

Active

Manage



Authenticator app
Generate a verification code using an authenticator app.

Set up

Multi-factor authentication user guide

Switching from the factor „Authentication token“ (= Yubikey) to the factor „Authenticator app“ works vice versa.

From:

<https://wiki.zil.haw-landshut.de/> -

Permanent link:

https://wiki.zil.haw-landshut.de/doku.php?id=lern-management-system:moodle_externe&rev=1773127812

Last update: **10032026, 07:30**

