

Kurzanleitung zur Einrichtung der Multi-Faktor-Authentifizierung (MFA)

IT-Servicedesk (E-Mail: it-servicedesk@lmu.de)

Stand: 17.05.2024



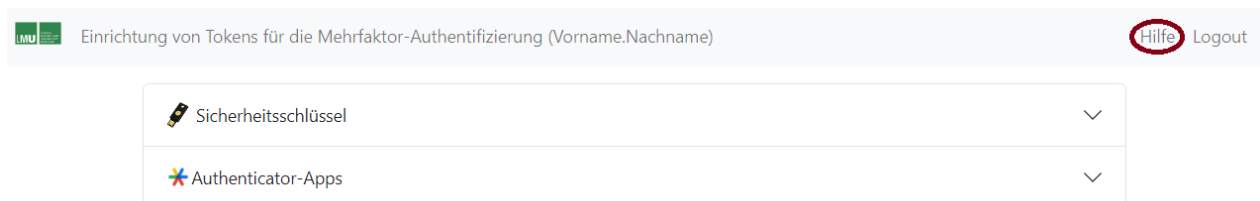
Kurzanleitung zur Einrichtung der Multi-Faktor-Authentifizierung (MFA)

Einrichtung von Tokens

Bevor Sie Ihre Anwendung mit Multi-Faktor-Authentifizierung (MFA) nutzen können, müssen Sie einmalig Tokens einrichten.

Hierzu rufen Sie die [LMU MFA-Enrollment-App](#) auf und melden sich dort mit Ihrer LMU-/LRZ-Kennung an.

Unter [Hilfe](#) können Sie Hintergrundinformationen zur Multi-Faktor-Authentifizierung nachlesen:

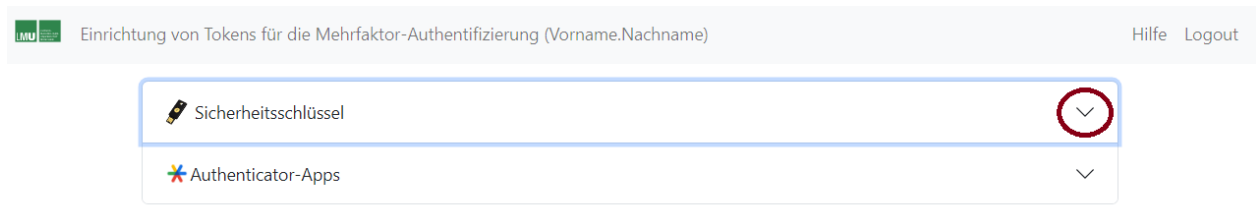


Wir empfehlen Ihnen dringend, mindestens zwei Tokens einzurichten. Bei Verlust eines dieser Tokens haben Sie somit die Möglichkeit, auf Ihr alternatives Token zurückzugreifen. Damit können Sie sich in der [LMU MFA-Enrollment-App](#) anmelden, das verlorene Token löschen und ein weiteres Token registrieren.

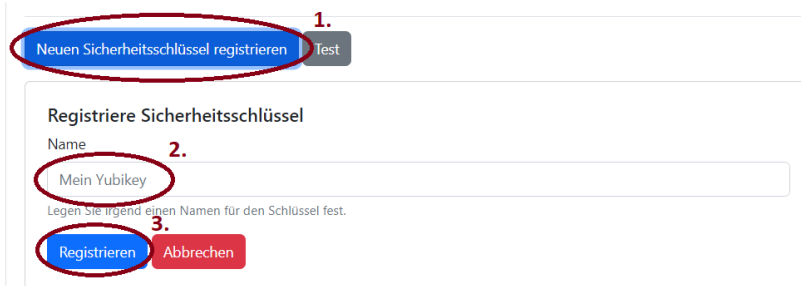
Bei Verlust eines einzigen registrierten Tokens ist ein persönlicher Termin beim IT-Servicedesk erforderlich, um Ihr Token entfernen zu lassen.

Einrichtung eines Sicherheitsschlüssels

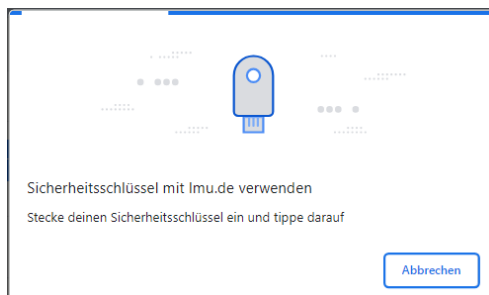
Um einen neuen Sicherheitsschlüssel (z. B. Yubikey) zu registrieren, klicken Sie auf den Pfeil neben "Sicherheitsschlüssel":



Im Anschluss klicken Sie auf die Option "Neuen Sicherheitsschlüssel registrieren" (siehe 1. in der nachfolgenden Abbildung) und tragen einen Namen, mit welchem Sie zu einem späteren Zeitpunkt Ihren Sicherheitsschlüssel eindeutig erkennen können (z. B. "Mein Yubikey USB-A") ein (siehe 2. in der nachfolgenden Abbildung). Mit dem Klick auf "Registrieren" schließen Sie den Registrierungsvorgang ab (siehe 3. in der nachfolgenden Abbildung):



Sie werden nun aufgefordert, Ihren Sicherheitsschlüssel zu verwenden:



Stecken Sie dazu Ihren Sicherheitsschlüssel in einen USB-Anschluss Ihres Rechners. Sobald die goldene Stelle Ihres Sicherheitsschlüssels blinkt, tippen Sie diese mit dem Finger an. Damit ist der Sicherheitsschlüssel hinzugefügt.

Wenn Sie Ihren Sicherheitsschlüssel erstmalig an Ihrem Rechner anstecken, kann es sein, dass folgende Meldung, dass das Gerät eingerichtet wird, erscheint:



In diesem Fall müssen Sie bis zu 30 Sekunden warten, bis folgende Meldung erscheint:



Erst dann ist Ihr Sicherheitsschlüssel einsatzbereit und kann registriert werden.

Hinweis: Je nach Gerätemodell kann es sein, dass Ihr Betriebssystem gegebenenfalls zusätzliche Sicherheitsfeatures unterstützt und eine solche oder ähnliche Meldung bei der Einrichtung und Verwendung des Yubikeys erscheint:



In diesem Fall wählen Sie die Option "Windows Hello oder externer Sicherheitsschlüssel".

Einrichtung einer Authenticator-App

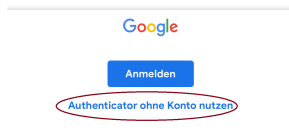
Es gibt verschiedene Authenticator-Apps. Wir empfehlen den Google Authenticator, der im Google-Playstore und im App Store von Apple kostenlos verfügbar ist, falls Sie keinen Sicherheitsschlüssel (z. B. Yubikey) verwenden können oder möchten. Die vorliegende Anleitung beschreibt die Einrichtung eines Sicherheitsschlüssels mit der Google Authenticator-App. Sie dürfen auch Authenticator-Apps von anderen Herstellern, z. B. von Microsoft verwenden. In diesem Fall müssen Sie aber selbst beurteilen, ob diese geeignet sind. Ebenso können wir keine Unterstützung leisten, falls etwas nicht funktioniert.

Sofern Sie die Google Authenticator-App noch nicht auf Ihrem Smartphone installiert haben, holen Sie dies bitte im ersten Schritt nach. Sie dürfen hierfür auch Ihr privates Smartphone verwenden. Beim ersten Öffnen der Google Authenticator-App können Sie entscheiden, ob Sie Ihre Sicherheitsschlüssel in Ihrem Google-Konto sichern möchten oder nicht. Sie können den Authenticator auch ohne Konto nutzen:

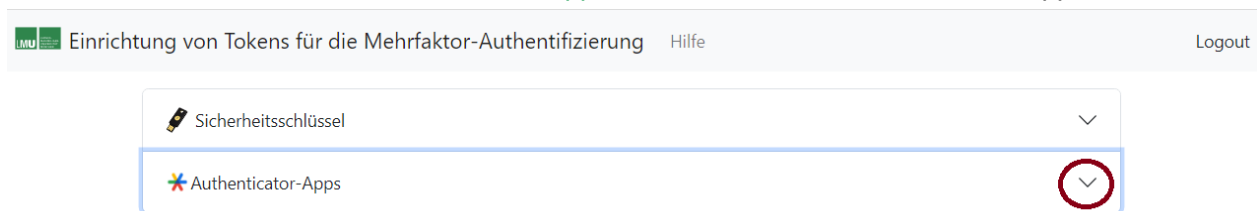


Willkommen bei Google Authenticator

Melden Sie sich an, um Ihre Codes in Ihrem
Google-Konto zu sichern



Nun klicken Sie in der **LMU MFA-Enrollment-App** auf den Pfeil neben "Authenticator-Apps":



1. Mit der Option "Neue Authenticator-App registrieren" (siehe 1. in der nachfolgenden Abbildung) starten Sie die Registrierung. Unter dem Schriftzug "Registrierte Authenticator-App" sehen Sie einen QR-Code.
2. Öffnen Sie nun auf Ihrem Smartphone die App "Authenticator". Nach Tippen auf das Symbol "+" auf der rechten unteren Seite Ihres Smartphone-Bildschirms erhalten Sie die Option "QR-Code scannen". Tippen Sie diese Option an und scannen Sie damit den auf Ihrem Arbeitsplatzrechner angezeigten QR-Code (siehe 2. in der nachfolgend gezeigten Abbildung).
Auf Ihrem Smartphone wurde in der Google Authenticator-App nun eine Zeile hinzugefügt. Durch einen langen Klick auf diese Zeile können Sie in den Bearbeitungs-Modus wechseln und durch Antippen des Stiftsymbols auf der rechten oberen Seite den Defaultwert für den Namen Ihres Kontos überschreiben und ihm einen sprechenden Namen geben, z. B. "Meine Anwendung 2FA", damit Sie bei späterer Verwendung den richtigen Eintrag identifizieren können.
3. Nun wechseln Sie wieder an Ihren Arbeitsplatzrechner. Um die Registrierung zu vervollständigen müssen Sie nur noch unter "Name" einen Namen für das Gerät, auf welchem die Google Authenticator-App läuft, festlegen (z. B. "Mein Privathandy", siehe 3. in der nachfolgenden Abbildung), die auf der Google Authenticator-App angezeigte 6-stellige Zahl eingeben (siehe 4. in der nachfolgenden Abbildung) und die Registrierung durch Klick auf "Registrieren" abschließen (siehe 5. in der nachfolgenden Abbildung):

1. **Neue Authenticator-App registrieren** Test

2. **Registriere Authenticator-App**
 Scannen Sie mit Ihrer Authenticator-App den QR-Code
 oder
 Geben Sie folgenden Einrichtungsschlüssel manuell ein (ohne die Bindestriche):

Legen Sie anschließend einen Namen für das Gerät fest und geben Sie die Zahl ein, die Ihre Authenticator-App anzeigt.
 Wenn Sie wollen, können Sie den QR-Code auch gerne [ausdrucken](#). Bewahren Sie den Ausdruck aber *unbedingt* an einem sicheren Ort auf!

3. Name:

Legen Sie irgend einen Namen für das Gerät fest.

4. Code:

5. Geben Sie die Zahl ein, die Ihre Authenticator-App anzeigt

Registrieren Abbrechen

Wichtig ist, dass Sie zeitnah nach Eingabe der 6-stelligen Nummer auf "Registrieren" klicken, da die Nummer nur eine kurze Gültigkeitsdauer hat.

Mit der Yubico Authenticator App können Sie sich die Vorteile Ihres Yubikeys zunutze machen ohne Ihren Yubikey zwingend an den gleichen Rechner, auf welchem Sie Ihren zweiten Faktor nutzen möchten, einzustecken.

Die Yubico Authenticator App ist für verschiedene Betriebssysteme verfügbar und kann unter <https://www.yubico.com/products/yubico-authenticator/#h-download-yubico-authenticator> heruntergeladen werden. Nach Installation der Yubico Authenticator App erfolgt die Registrierung analog zum oben beschriebenen Vorgehen.

Entfernung von Tokens

Bei Verlust oder Defekt eines Tokens oder bei einem Wechsel Ihres Smartphones sollten Sie nicht mehr benötigte oder verfügbare Tokens unbedingt aus der **LMU MFA-Enrollment-App** entfernen. Dazu klicken Sie auf das Papierkorb-Symbol rechts neben dem Token, welches Sie entfernen möchten:

Sicherheitsschlüssel

Authenticator-Apps

Name	Registrierungsdatum	
Mein Privathandy	16.1.2024, 14:31:17	
Mein Privathandy KeePass2Android	17.1.2024, 11:05:24	

Neue Authenticator-App registrieren Test

Diesen Vorgang müssen Sie anschließend noch mit "OK" bestätigen:

JavaScript von „login.lmu.de“

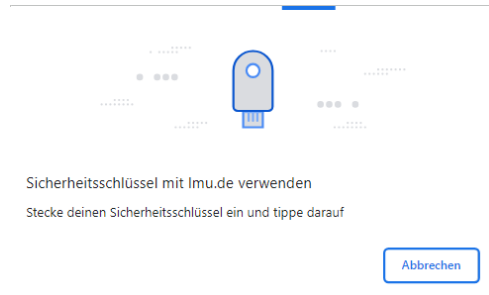
Soll die Authenticator-App Mein Privathandy KeePass2Android, registriert 17.1.2024, 11:05:24, wirklich gelöscht werden?

OK Abbrechen

Verwendung der Multi-Faktor-Authentifizierung

Verwendung eines Yubikeys

Um einen bereits registrierten Sicherheitsschlüssel (z. B. Yubikey) an Ihrem Arbeitsplatzrechner zu verwenden, stecken Sie diesen in einen freien USB-Slot am Rechner. Nun melden Sie sich mit Ihrer LMU-/LRZ-Kennung in der Anwendung, welche die Multi-Faktor-Authentifizierung erfordert, an. Im nächsten Schritt werden Sie aufgefordert, Ihren Sicherheitsschlüssel zu verwenden:



Sie müssen die goldene Stelle Ihres eingesteckten Sicherheitsschlüssels nur berühren, sobald diese blinkt, und die Anmeldung in Ihrer Anwendung erfolgt.

Um den Yubikey nutzen zu können, ohne ihn an dem Rechner, an welchem Sie die Multi-Faktor-Authentifizierung benötigen, angeschlossen zu haben, verwenden Sie bevorzugt die Yubico Authenticator App. Nach Start der Yubico Authenticator App werden Sie aufgefordert, Ihren Yubikey einzustecken. Nach erfolgreicher Anmeldung in der App erhalten Sie im Yubico Authenticator die eingerichteten Accounts angezeigt und können wie im Abschnitt [Verwendung einer Authenticator-App](#) beschrieben fortfahren.

Verwendung einer Authenticator-App

Nach Aufruf Ihrer Anwendung, welche die Multi-Faktor-Authentifizierung erfordert, loggen Sie sich im ersten Schritt mit Ihrer LMU-/LRZ-Kennung und Ihrem Passwort ein. Haben Sie einen Sicherheitsschlüssel hinterlegt, werden Sie nun aufgefordert, diesen einzustecken. Möchten Sie stattdessen eine Authenticator-App verwenden, klicken Sie auf "Abbrechen". Stattdessen öffnen Sie auf Ihrem Smartphone Ihre Authenticator-App und geben den für Ihre Anwendung angezeigten 6-stelligen Code an der unter 1. im Screenshot gezeigten Stelle ein. Durch Klick auf "Anmelden" schließen Sie die Anmeldung ab (siehe 2. im nachfolgenden Screenshot):

LMU-Login

The screenshot shows the LMU login interface. At the top, under the heading "Sicherheitsschlüssel", there is a link "Abgebrochen" and a green button labeled "Nochmal versuchen". Below this, the word "Oder" is displayed. Under the heading "Authenticator-App", there is a text prompt: "Bitte geben Sie den Code ein, den Ihre Authenticator-App anzeigt". Below the prompt is a text input field labeled "6-stellige Zahl". A red circle with the number "1." points to this input field. Below the input field is a green button labeled "→ Anmelden", which is also circled in red with the number "2." next to it.

Support

Um Ihnen und dem Support-Team überflüssigen Aufwand zu ersparen, empfehlen wir dringend, mindestens zwei Tokens zu hinterlegen. Bei Verlust oder Defekt eines einzigen hinterlegten Tokens müssen Sie sich zur Zurücksetzung persönlich an den [IT-Servicedesk](#) wenden.

Bei weiteren Problemen und Fragen zur Multi-Faktor-Authentifizierung wenden Sie sich bitte an Ihre jeweiligen Anwendungsbetreuer.

Glossar

LMU MFA-Enrollment-App

Als LMU MFA-Enrollment-App bezeichnen wir die unter <https://login.lmu.de/mfa-enrollment/index.html> erreichbare Webseite, welche der Verwaltung der **Tokens** für die **Multi-Faktor-Authentifizierung** dient.

Token

Komponente zur Identifizierung und Authentifizierung von Benutzern. Es gibt Hardware-Tokens (z. B. Yubikeys) und Software-Tokens (z. B. der durch eine Authenticator-App generierte 6-stellige Code).

USB-A und USB-C

Die von der LMU ausgegebenen **Yubikeys** sind in zwei unterschiedlichen Varianten erhältlich.

Die Yubikeys mit dem USB-A-Anschluss sind durch einen flachen, rechteckigen, circa 1,2 Zentimeter breiten Anschluss, bei welchem nur auf einer Seite Kontakte zu sehen sind, gekennzeichnet.

Charakteristisch für USB-A-Stecker ist, dass diese nur in einer Richtung eingesteckt werden können.

Die Yubikeys mit USB-C-Anschluss besitzen einen circa 8mm breiten Stecker, welcher durch abgerundete Seiten und eine offene Mitte erkennbar ist. Diese Stecker sind symmetrisch, so dass es irrelevant ist, in welcher Weise der Stecker angeschlossen wird.

Yubikey

Sicherheits-Token der Firma Yubico

Multi-Faktor-Authentifizierung

Zusätzlich zu den bekannten Log-In-Daten (LMU-/LRZ-Kennung und Passwort) benötigen Sie bei der Multi-Faktor-Authentifizierung noch einen zweiten Faktor (z. B. einen Yubikey oder einen von einer Authenticator-App generierten Code), um sich einzuloggen. Sie müssen Ihre Identität mittels einer Kombination zweier unterschiedlicher und voneinander unabhängiger Faktoren nachweisen.