

Einrichtung einer Multi-Faktor-Authentisierung (MFA) mittels der App 2FAS für Android / Setting up multi-factor authentication (MFA) using the 2FAS app for Android

03.12.2024

<https://kim.uni-hohenheim.de>



Die Multi-Faktor-Authentisierung (MFA) stellt ein wirksames Mittel zur Erhöhung der Sicherheit bei der Verwendung von klassischen Zugangsdaten wie Benutzername und Passwort dar. Zum Einsatz können dabei softwarebasierte oder hardwarebasierte Token kommen. Softwarebasierte Token werden beim Smartphone durch eine App realisiert. Seitens der Universität wird die freiverfügbare App 2FAS (verfügbar für iOS, iPadOS und Android) empfohlen und unterstützt.

Multi-factor authentication (MFA) is an effective means of increasing security when using traditional access data such as user name and password. Software-based or hardware-based tokens can be used. Software-based tokens are implemented on smartphones using an app. The university recommends and supports the freely available app 2FAS (available for iOS, iPadOS and Android).

Der Einsatz anderer Apps ist auf eigenes Risiko möglich (die App Microsoft-Authenticator liefert zum Zeitpunkt der Erstellung dieser Anleitung aber einen nicht verwendbaren Token).

The use of other apps is possible at your own risk (the app Microsoft-Authenticator do not provide an usable token at the time of writing these instructions).

Inhalt / Content

Installation von 2FAS und Grundeinstellungen (Vorbereitung) / Installation of 2FAS and basic settings (preparation)	2
Ein softwarebasiertes Token einrichten / Set up a software-based token.....	5
VPN-Verbindung mit MFA am Beispiel Windows / VPN connection with MFA using Windows as an example ...	10
Hinweise / Notes	12

Installation von 2FAS und Grundeinstellungen (Vorbereitung) / Installation of 2FAS and basic settings (preparation)

Laden Sie die App 2FAS aus dem Google Playstore herunter

Download the 2FAS app from the Google Playstore



Android:

<https://play.google.com/store/apps/details?id=com.twofasapp&hl=de&gl=de>

und installieren diese.

and install it.

Starten Sie nun bei Ihrem Smartphone die App 2FAS.

Now start the 2FAS app on your smartphone.

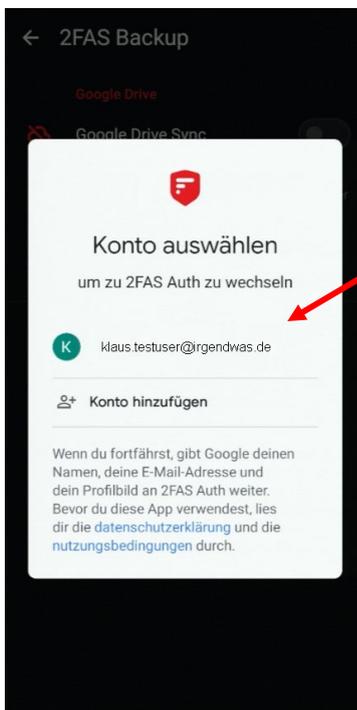
Beim ersten Starten sehen Sie eine kleine Einführung. Sie können mit „Fortsetzen“ (1) diese anschauen. Sie gelangen an die Stelle, wo Sie gefragt werden, ob Sie die Soft-Tokens mit Ihrem Google Konto verbinden wollen (2a). Sie können zunächst auch ohne Backup fortfahren (2b).

When you start the program for the first time, you will see a short introduction. You can view this with "Continue" (1). You will reach the point where you are asked whether you want to connect the soft tokens to your Google account (2a). You can also continue without a backup (2b).



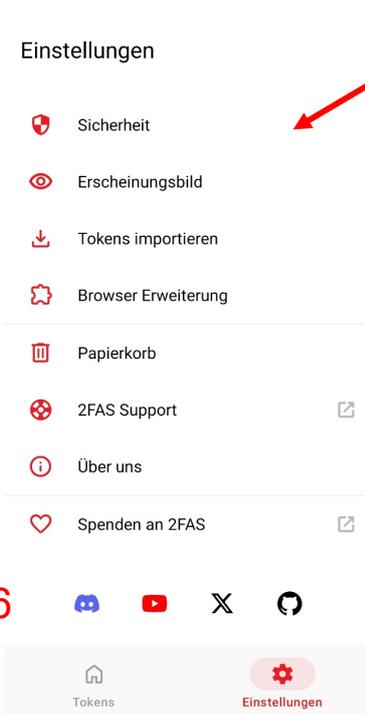
Sofern Sie sich mit Ihrem Google-Konto anmelden wollen, müssen Sie dieses auswählen (3) und der Nutzung zustimmen (4), (5).

If you want to log in with your Google account, you must select it (3) and agree to its use (4), (5).

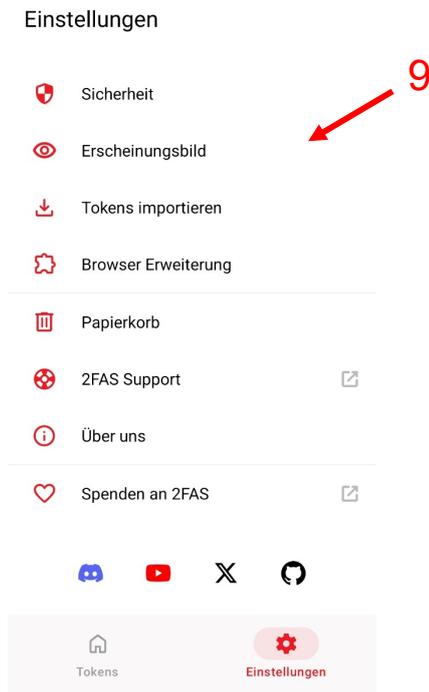


Über die Einstellungen (6), Sicherheit (7) können Sie auch nachträglich noch das 2FAS Backup aktivieren oder deaktivieren (8).

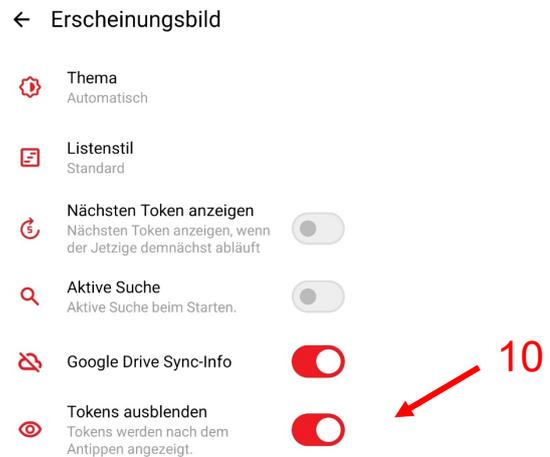
You can also activate or deactivate the 2FAS backup at a later date via Settings (6), App Security (7), and Backup (8).



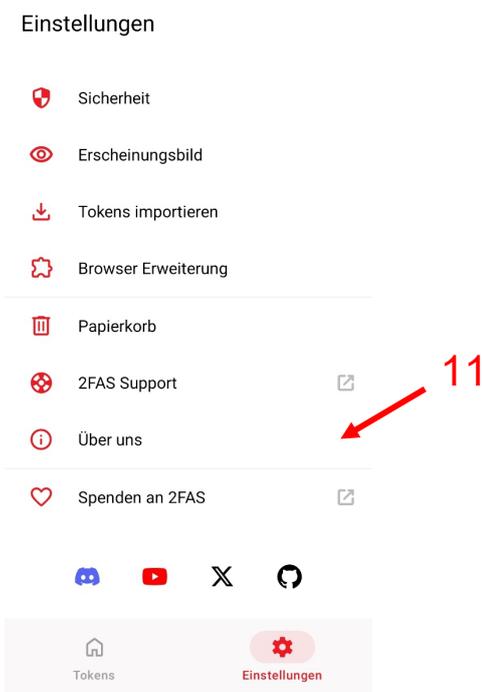
Unter „Erscheinungsbild“ (9) aktivieren Sie bitte „Tokens ausblenden“ (10) und dann zurück.



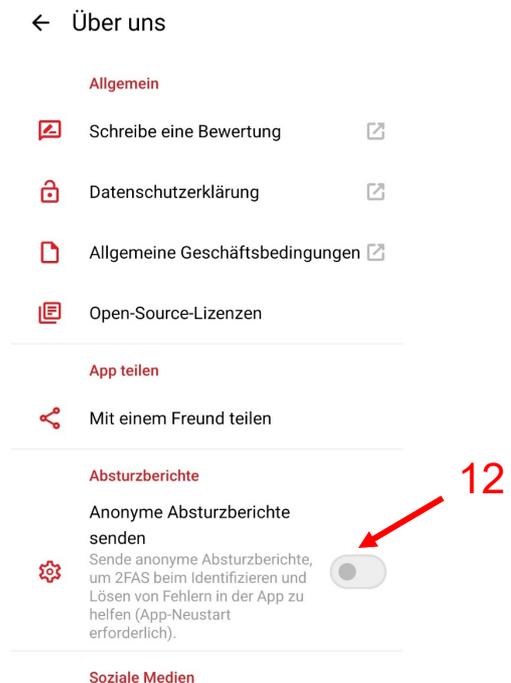
Under "Appearance" (9), please activate "Hide tokens" (10) and then go back.



In den Einstellungen nach unten bei unter „Über uns“ (11) deaktivieren Sie bitte bei Bedarf „Anonyme Absturzberichte senden“ (12). Anschließend zurück.



In the settings under "About" (11), please deactivate "Send anonymous crash reports" (12) if required. Then go back.



Die Vorbereitung sind nun abgeschlossen.

The preparations are now complete.

Ein softwarebasiertes Token einrichten / Set up a software-based token

Bitte rufen Sie die Webanwendung von Ihrem Personal Computer oder Smartphone auf

Please call up the web application from your personal computer or smartphone

<https://edumfa.uni-hohenheim.de>



Dazu müssen Sie am Campus mit dem Netzwerk verbunden sein (kabelgebunden oder eduroam).

To do this, you must be connected to the network on campus (wired or eduroam).

Es erscheint die Anmeldemaske. Dort geben Sie Ihre Hohenheimer Benutzerkennung (1) und das zugehörige Passwort (2) ein.

The login screen will appear. Enter your Hohenheim user ID (1) and the corresponding password (2).

Bitte geben Sie Ihren Benutzernamen und Ihr Passwort ein, um sich anzumelden.

eduMFA Universität Hohenheim
Multi-Faktor-Authentifizierungssystem

Hohenheimer Benutzerkennung

.....

Anmelden

1
2
3

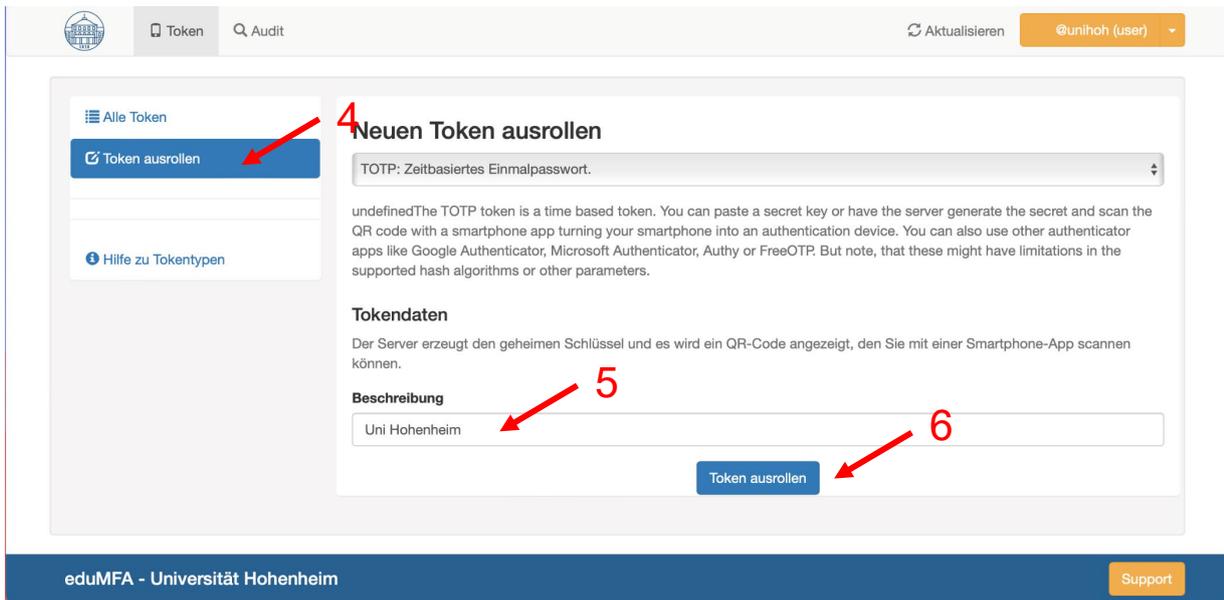
eduMFA - Universität Hohenheim Support

Anschließend drücken Sie mit der linken Maustaste bitte auf Anmelden (3).

Then click on Log In (3) with the left mouse button.

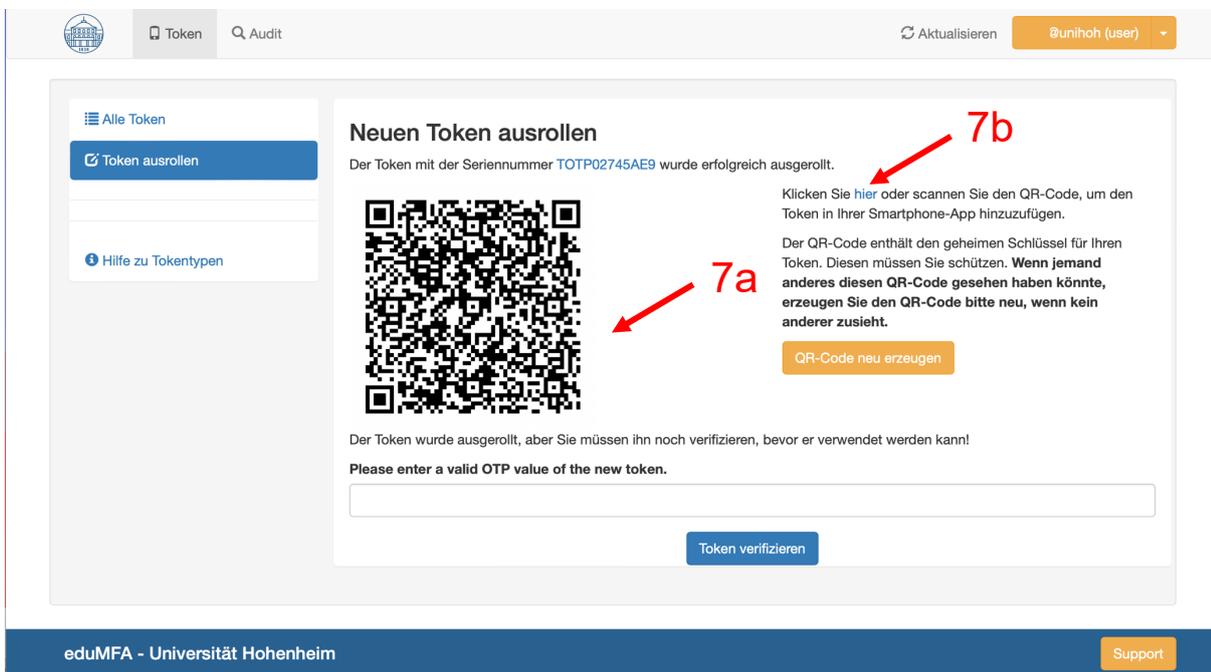
Im nächsten Schritt wählen Sie bitte im linken Bereich „Token ausrollen“ (4) aus und geben eine beliebige Beschreibung (5), z. B. Uni Hohenheim, ein.

In the next step, please select "Enroll token" (4) in the left-hand area and enter any description (5), e.g. University of Hohenheim.



Nun können Sie den „Token ausrollen“ (6) mit der linken Maustaste drücken. Im Anschluss wird der QR-Code (7a) angezeigt.

Now you can press the "Enroll Token" (6) with the left mouse button. The QR code (7a) is then displayed.



Wenn Sie die Webanwendung am Computer geöffnet haben, scannen Sie den QR-Code (7a) und machen Sie weiter mit Schritt 8. Bei Nutzung auf dem Smartphone, klicken Sie auf "hier" (7b).

If you have opened the web application on your computer, scan the QR code (7a) and continue with step 8. If you are using it on your smartphone, click on "here" (7b).

Wenn Sie auf den Link (7b) klicken, wählen Sie ggf. bitte die App 2FAS aus. Sie müssen die Übernahme des Eintrags bestätigen und gelangen direkt zu Ansicht der Tokens (10).

If you click on the link (7b), please select the 2FAS app if necessary. You must confirm the transfer of the entry and you will be taken directly to the view of the tokens (10).

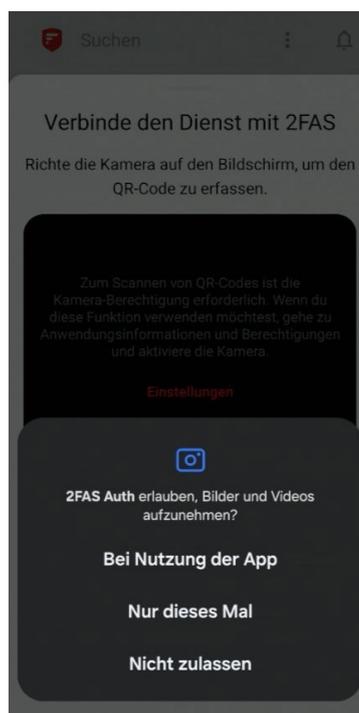
Zum Scannen des QR-Codes starten Sie bei Ihrem Smartphone die App 2FAS bzw. wechseln Sie zur App 2FAS.

To scan the QR code, start the 2FAS app on your smartphone or switch to the 2FAS app.



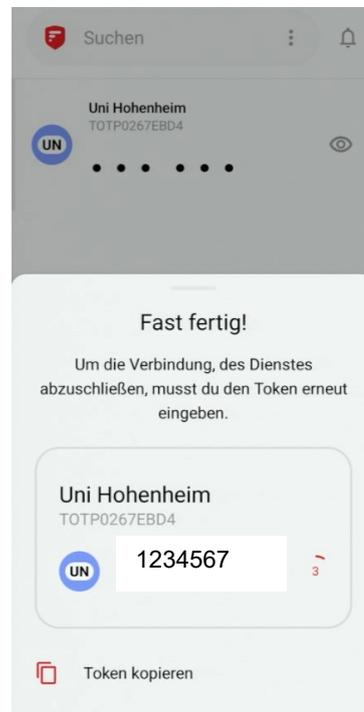
Hierfür wählen Sie zunächst in der Übersicht „Neuen Dienst koppeln“ (8) aus. Ggf. müssen Sie der App nun den Zugriff auf die Kamera „Erlauben“ (9).

To do this, first select "Pair new service" (8) in the overview. You may now need to "Allow" the app to access the camera (9).



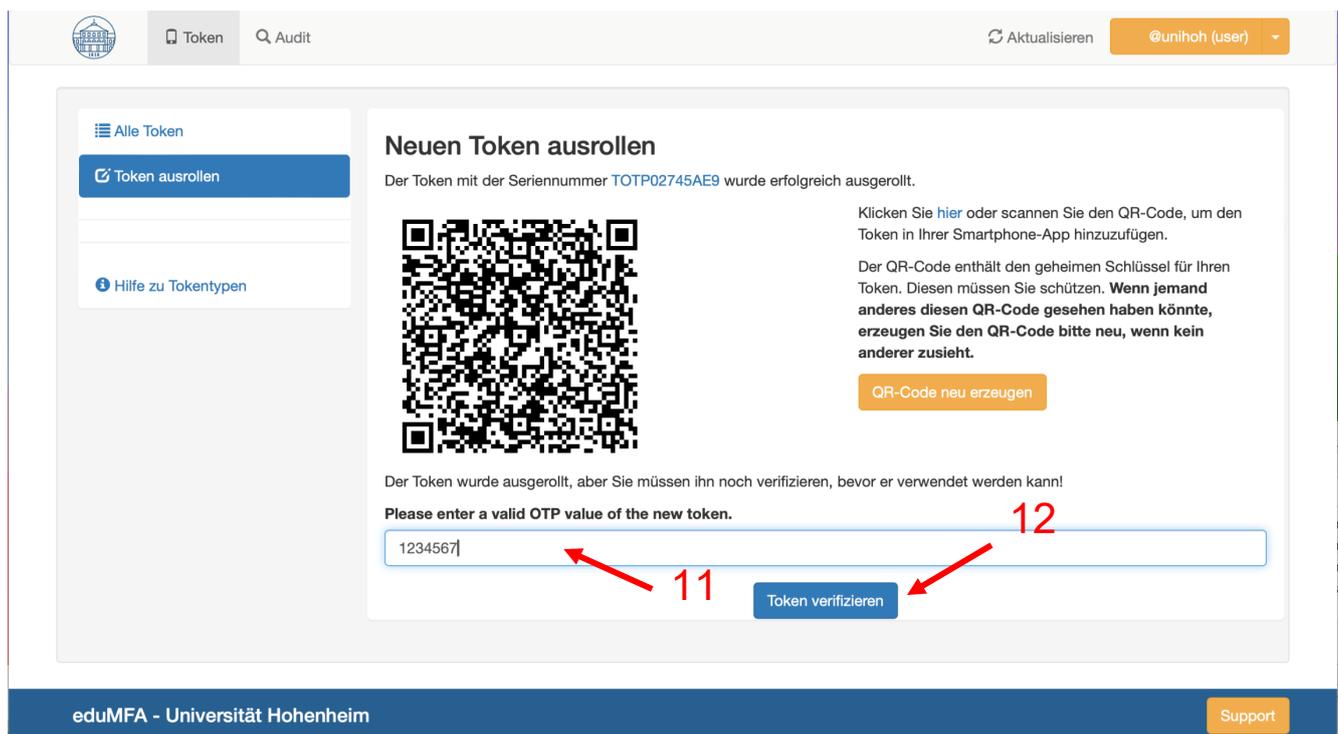
Scannen Sie nun den QR-Code von der Webseite (7a). Der Token (10) für Ihr Hohenheimer Benutzerkonto wird Ihnen daraufhin angezeigt.

Now scan the QR code from the website (7a). The token (10) for your Hohenheim user account will then be displayed.



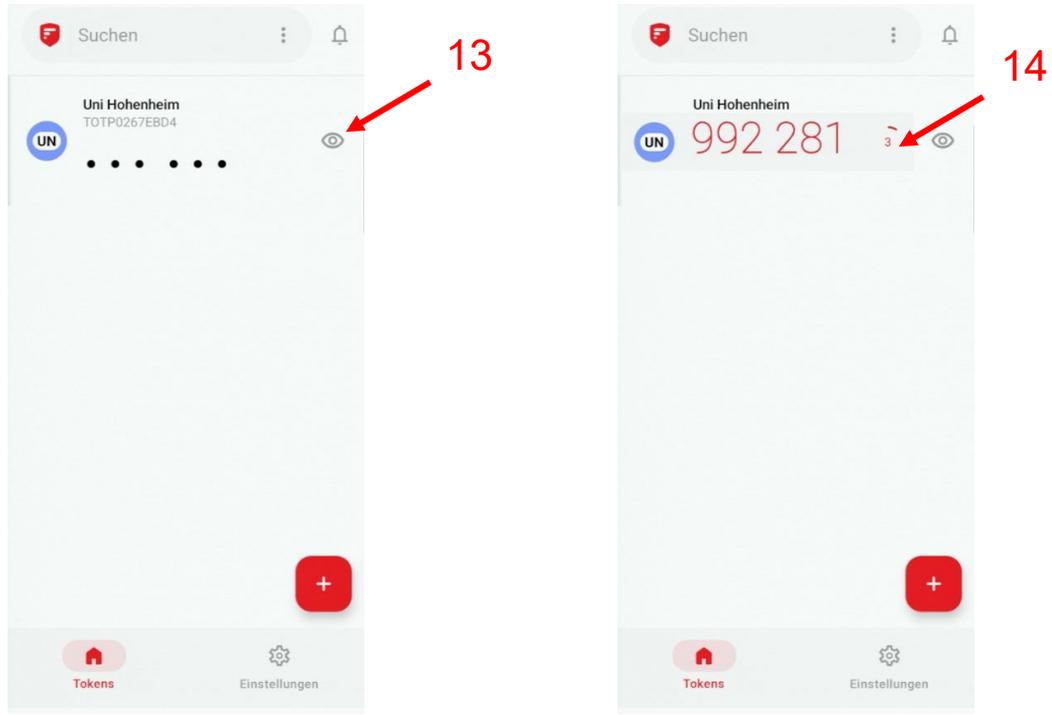
Den Token (10) geben Sie nun als Bestätigung auf der Webseite ein (11) und können damit den „Token verifizieren“ (12).

Now enter the token (10) as confirmation on the website (11) and you can use it to "Verify Token" (12).



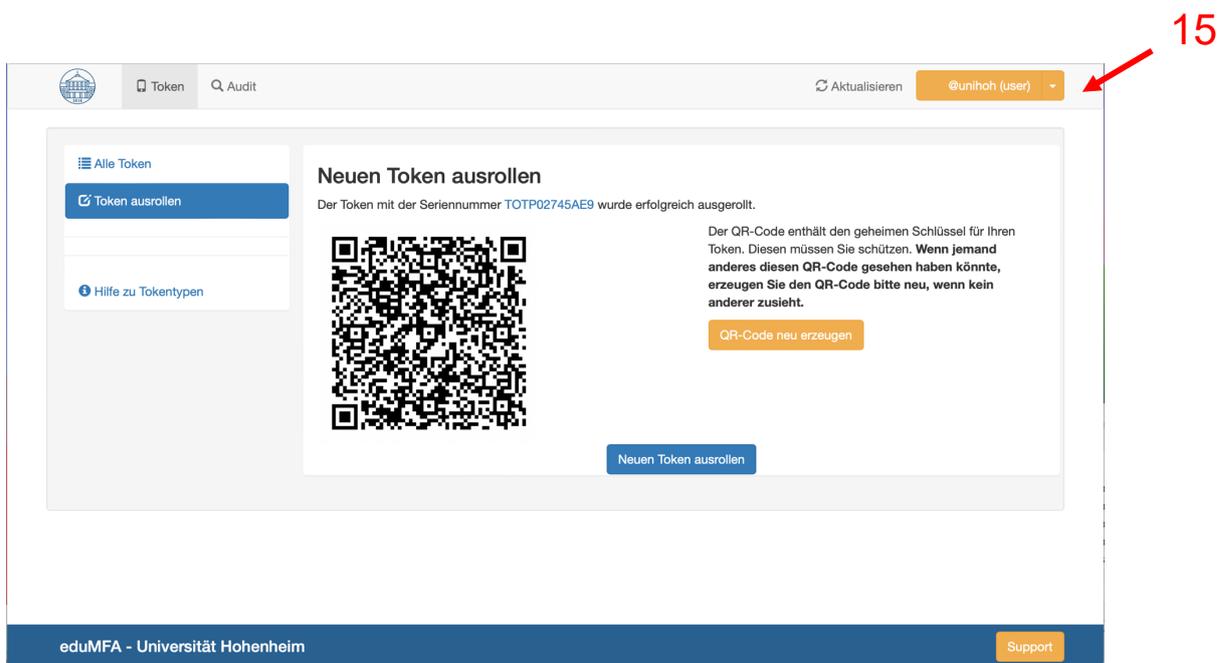
In der App wurde nun ein Eintrag angelegt. Wenn Sie das Auge (13) auswählen, dann erscheint der aktuelle Token und die Zeit wie langer dieser noch gültig ist (14).

An entry has now been created in the app. If you select the eye (13), the current token and the time for which it is still valid will appear (14).



In der Webanwendung wird der QR-Code nochmals angezeigt.

The QR code is displayed again in the web application.





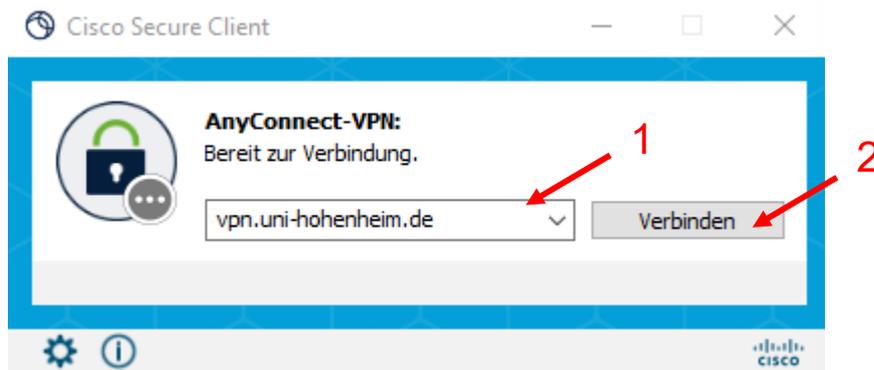
Falls Sie den Token noch auf ein anderes Gerät übertragen wollen, können Sie den QR-Code an dieser Stelle, z. B. mit einem anderen Gerät erneut einscannen. **Wenn alles funktioniert hat, sollten Sie nun den QR-Code sichern, z. B. durch Ausdrucken oder Abfotografieren. Er kann später an dieser Stelle nicht erneut angezeigt werden.** Anschließend können Sie sich abmelden (15).

If you still want to transfer the token to another device, you can scan the QR code again at this point, e.g. with another device. **If everything has worked, you should now save the QR code, e.g. by printing it out or photographing it. It cannot be displayed again at this point later.** You can then log out (15).

VPN-Verbindung mit MFA am Beispiel Windows / VPN connection with MFA using Windows as an example

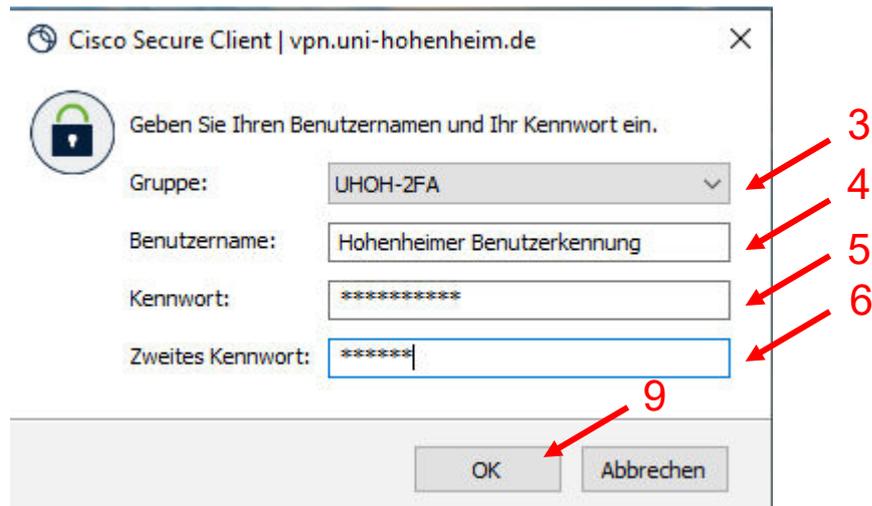
Eine praktische Anwendung findet die Multi-Faktor-Authentisierung bei der VPN-Verbindung. Die Verbindung wird wie gehabt zu vpn.uni-hohenheim.de (1) aufgebaut (2).

Multi-factor authentication is used in practice for the VPN connection. The connection is established as usual to vpn.uni-hohenheim.de (1) (2).



Sobald das softwarebasierte Token für Ihre Hohenheimer Benutzererkennung erfolgreich eingerichtet wurde, wählen Sie falls noch nicht voreingestellt die Gruppe UHOH-2FA (3) aus. Es wird ein zusätzliches Feld (Zweites Kennwort oder 2FA Token) angezeigt. Bitte geben Sie nun Ihren Hohenheimer Benutzernamen (4), das zugehörige Passwort (5) und das Token (6) ein.

As soon as the software-based token for your Hohenheim user ID has been successfully set up, select the UHOH-2FA group (3) if it has not already been set up. An additional field (Second password or 2FA token) will be displayed. Please now enter your Hohenheim user name (4), the corresponding password (5) and the token (6).



Den Token erhalten Sie aus der App 2FAS (7 und 8).

The token is obtained from the 2FAS app (7 and 8).



Die Verbindung wird mit OK (9) - wenn alle Daten korrekt sind - aufgebaut.

The connection is established with OK (9) - if all data is correct

Hinweise / Notes

- Der softwarebasierte Token kann nur aus dem Hohenheimer Netzwerk (vor Ort) initial beantragt und eingerichtet werden. Eine VPN-Verbindung ist aus Gründen der IT-Sicherheit nicht ausreichend.
- Der QR-Code kann nach der Einrichtung nicht erneut angezeigt werden. Es empfiehlt sich ein Backup anzulegen. Da der QR-Code nicht passwortgeschützt ist, sollte dieser QR-Code bzw. das Backup sorgfältig verwahrt werden.
- Die 2FAS-App bietet die Möglichkeit den Geheimschlüssel des Tokens anzuzeigen und in eine andere App zu kopieren. Dafür muss zuvor in der App ein „PIN Code“ gesetzt werden. Die Option befindet sich bei den Einstellungen im Bereich App-Sicherheit.
- Sobald der softwarebasierte Token erfolgreich eingerichtet wurde, kann dieser beim VPN-Dienst genutzt werden. Bitte ggf. die Gruppe UHOH-2FA auswählen.
- Der softwarebasierte Token ist zeitlich beschränkt gültig (max. 30 Sekunden, beginnend zur 0-ten und 30-ten Sekunde). Möglicherweise ist dieses bei Eingabe bereits ungültig. Dann bitte einen neuen Token aus der App 2FAS ablesen und übernehmen.
- Wenn der softwarebasierte Token verloren geht, dann kann dieser nutzerseitig nicht zurückgesetzt werden. In diesem Fall wenden Sie sich bitte an den IT-Service-Desk. Unter Vorlage eines amtlichen Ausweises (Personalausweis oder Reisepass) wird der softwarebasierte Token gelöscht und Sie können selbst gemäß dieser Anleitung einen neuen softwarebasierten Token erstellen.
- Über die Webanwendung (<https://edumfa.uni-hohenheim.de>) haben Sie die Möglichkeit den softwarebasierten Token zu testen und den Fehlerzähler selbständig zurückzusetzen. Die Deaktivierung kann Ihrerseits erfolgen, aber nicht rückgängig gemacht werden. Bitte wenden Sie sich in diesem Fall an den IT-Service-Desk.
- The software-based token can only be initially requested and set up from the Hohenheim network (on site). A VPN connection is not sufficient for IT security reasons.
- The QR code cannot be displayed again after it has been set up. It is recommended to create a backup. As the QR code is not password-protected, this QR code or the backup should be stored carefully.
- The 2FAS app offers the option of displaying the token's secret key and copying it to another app. To do this, a "PIN code" must first be set in the app. The option can be found in the settings in the app security section.
- As soon as the software-based token has been successfully set up, it can be used with the VPN service. Please select the UHOH-2FA group if necessary.
- The software-based token is valid for a limited time (max. 30 seconds, starting at the 0th and 30th second). It may already be invalid when you enter it. In this case, please read a new token from the 2FAS app and accept it.
- If the software-based token is lost, it cannot be reset by the user. In this case, please contact the IT Service Desk. On presentation of an official ID (ID card or passport), the software-based token will be deleted and you can create a new software-based token yourself in accordance with these instructions.
- You can test the software-based token and reset the error counter yourself via the web application (<https://edumfa.uni-hohenheim.de>). The deactivation can be carried out by you, but cannot be reversed. In this case, please contact the IT Service Desk.

Bei Fragen stehen wir Ihnen gerne am
IT-Service-Desk des KIM
Biogebäude 1, Garbenstraße 30, 1. UG
oder per E-Mail unter
kim-it-account@uni-hohenheim.de
zur Verfügung.

If you have any questions, please contact the
IT Service Desk of the KIM
Biogebäude 1, Garbenstraße 30, 1. Basement
or send us an email
kim-it-account@uni-hohenheim.de