Gasthörer- und Seniorenstudium

KOOST-Post

40/2025 | 04.12.2025

Intro

Liebe Gasthörerinnen und Gasthörer, liebe Freundinnen und Freunde des Gasthörer- und Seniorenstudiums,

über mehrere E-Mails des KLIPS-Supports und auch Ankündigungen bei Veranstaltungen der KOOST sind Sie sicher bereits aufmerksam geworden: **Ab dem 04.12.2025 wird der Login in KLIPS 2.0 nur noch mit einer so genannten Multi-Faktor-Authentifizierung möglich sein**. Bisher war diese Art der Authentifizierung nur bei der Nutzung des VPN-Dienstes notwendig. Perspektivisch sollen noch weitere Dienste, wie z.B. ILIAS durch eine Multi-Faktor-Authentifizierung abgesichert werden.
Den Zugang zu KLIPS 2.0 benötigen Sie beispielsweise, wenn Sie Ihren **Gasthörer:innenausweis ausdrucken oder sich zu Veranstaltungen der Philosophischen und/oder Rechtswissenschaftlichen Fakultät anmelden** möchten. Daher ist es wichtig, dass Sie eine Authentifizierung durchführen können.
In dieser KOOST-Post möchten wir umfangreich zur Multi-Faktor-Authentifizierung informieren. Die Informationen und Anleitungen zur Multi-Faktor-Authentifizierung wurden vom **IT Center University of Cologne (ITCC)** zusammengestellt, die auch wunderbare Klickanleitungen auf ihren Webseiten zur Verfügung stellen und auf die wir in diesem Newsletter an verschiedenen Stellen verweisen.
Darüber hinaus hat unsere ehemalige Mitarbeiterin, Luisa Bauer, ein sehr gutes **Videotutorial** entwickelt, das Sie sich anschauen können. Den Link dazu finden Sie ebenfalls in diesem Newsletter.

Und nun los geht's!

Was ist eine Multi-Faktor-Authentifizierung und warum ist sie notwendig?

Um dem Risiko von Cyberangriffen entschieden entgegenzuwirken und den Schutz von Daten und Geräten zu intensivieren, führt die Universität zu Köln die Multi-Faktor-Authentifizierung für den Login von IT-Diensten (VPN und KLIPS 2.0) ein.
Neben Ihrem Login mit dem Studierendenaccount soll ein zusätzlicher, unabhängiger Faktor Ihren Login absichern. Hierdurch wird der Schutz vor unbefugtem Zugriff auf Dienste, Software und Daten erhöht.

Die Multi-Faktor-Authentifizierung (MFA) wird an der Universität zu Köln mit **Cisco Duo** umgesetzt. Cisco Duo ist ein System, das weitere Authentifizierungsmöglichkeiten (als sogenannten Zweiten Faktor) ermöglicht.

Die App Duo Mobile

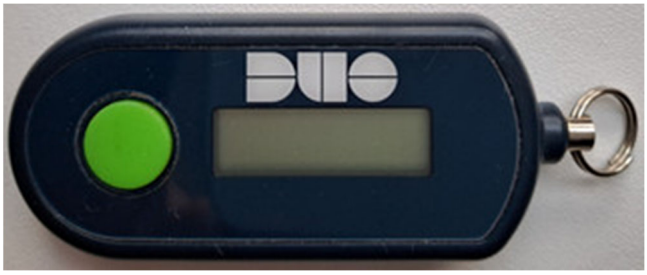
Die Cisco Duo-Authentifizierung erfolgt über die App „Duo Mobile“. Die App ist für die Betriebssysteme Android, iOS, iPadOS sowie watchOS verfügbar. Sie können die App auf Ihren Smartphones oder Tablets nutzen, um damit Ihre Identität gegenüber Systemen und Diensten beim Login zu bestätigen.
Aber Achtung: Für die Verwendung der App *Duo Mobile* als zweitem Faktor benötigen Sie ein Mobilgerät – typischerweise ein Smartphone oder Tablet – das eine der **folgenden Anforderungen** erfüllt:

- Android 11 oder höher
- iOS 16.0 oder höher
- iPadOS 16.0 oder höher
- watchOS 10.0 oder höher

Darüber hinaus muss auf dem verwendeten Mobilgerät zwingend eine **Displaysperre (z.B. PIN, Passwort, Fingerabdruck o.ä.)** eingerichtet sein. Ansonsten werden Authentifizierungsversuche zurückgewiesen.

Alternative über den Hardware-Token

Sollten Sie kein Smartphone benutzen können oder wollen, besteht für Studierende der Universität zu Köln die Möglichkeit, die Authentifizierung über ein Zusatzgerät, ein sogenanntes Token, durchzuführen. Diese Tokens können kostenfrei ausgeliehen werden.
Das ausleihbare Hardwaretoken ist ein Gerät in der Größe eines USB-Sticks mit einem Knopf und einem Display. Drücken Sie auf den Kopf, erscheint auf dem Display ein sechsstelliger Code, den Sie im Browser bei der Cisco-Duo-Abfrage eingeben können.



Umfangreiche Informationen zur Ausleihe und zur Anwendung des Tokens finden Sie hier:

https://itcc.uni-koeln.de/services/accounts-kommunikation/multi-faktor-authentifizierung-cisco-duo/hardware-token

oder auch in unserem Videotutorial:

https://gasthoerersenioren.uni-koeln.de/lehrvideos/lehrvideo-multifaktor-authentifizierung-mfa

Multi-Faktor-Authentifizierung über die App „Duo Mobile“

Wenn Sie sich für die Multi-Faktor-Authentifizierung über die APP „Duo Mobile“ entscheiden sind im Folgenden zwei Dinge zu tun:

1. Installation der App „Duo Mobile“ auf Ihrem Smartphone oder Tablet
2. Erstregistrierung in Cisco Duo

1. Installation der App „Duo Mobile“ auf Ihrem Smartphone oder Tablet

Installieren Sie zunächst die App "Duo Mobile" auf Ihrem Mobilgerät. Die App finden Sie in den jeweiligen Play- bzw. App-Stores.

Android:
https://play.google.com/store/apps/details?id=com.duosecurity.duomobile&hl=de

Apple: https://apps.apple.com/us/app/duo-mobile/id422663827?mt=8

In unserem Videotutorial wird die Installation der App am Beispiel eines Applegerätes gezeigt. Das Tutorial finden Sie hier:
https://gasthoerersenioren.uni-koeln.de/lehrvideos/lehrvideo-multifaktor-authentifizierung-mfa

2. Erstregistrierung in Cisco Duo

Die erstmalige Registrierung für *Cisco Duo* ist nur im universitätsinternen WLAN Eduroam möglich, d.h. Sie müssen sich mit Ihrem Gerät auf dem Campus der UzK befinden (nicht von zu Hause oder unterwegs per VPN).

Sie können die Erstregistrierung an einem Computer/Laptop oder an einem mobilen Endgerät vornehmen. Für beide Vorgehen hat das ITCC sehr gute Anleitungen zusammengestellt.
Anleitung für die Erstregistrierung mit einem Computer/Laptop:
https://itcc.uni-koeln.de/services/accounts-kommunikation/multi-faktor-authentifizierung-cisco-duo/erstregistrierung-in-cisco-duo#c25887

Anleitung für die Erstregistrierung mit einem mobilen Endgerät:
https://itcc.uni-koeln.de/services/accounts-kommunikation/multi-faktor-authentifizierung-cisco-duo/erstregistrierung-in-cisco-duo/erstregistrierung-ueber-ein-mobiles-endgeraet

In unserem Videotutorial wird die Erstregistrierung anhand eines Smartphones gezeigt.

Anwendung der App Duo Mobile beim Login von KLIPS 2.0

In unserem Videotutorial zeigt Ihnen Luisa Bauer außerdem die Anwendung der App beim zukünftigen Login in Klips 2.0:

https://gasthoerersenioren.uni-koeln.de/lehrvideos/lehrvideo-multifaktor-authentifizierung-mfa

Bei Fragen und Beratungsbedarf rund um die Multi-Faktor-Authentifizierung hilft Ihnen das ITCC

Das ITCC hat wunderbare Informationen für alle Fragen rund um die Multi-Faktor-Authentifizierung zusammengestellt. Diese finden Sie hier:

https://itcc.uni-koeln.de/services/accounts-kommunikation/multi-faktor-authentifizierung-cisco-duo/cisco-duo-faq

Bei Beratungsbedarf zum Beispiel zur Erstregistrierung können Sie sich an das ITCC-Helpdesk wenden:
https://itcc.uni-koeln.de/helpdesk/general-it-services

Adresse
Erdgeschoss
Weyertal 121 (Gebäude 133)
50931 Köln

Öffnungszeiten
Montag bis Freitag: 9.00–16.00 Uhr

Videotutorial der KOOST:

Unser Videotutorial beinhaltet Informationen zu:

- Allgemeine Informationen zur Multi-Faktor-Authentifizierung
- Der Hardwaretoken als Alternative: Ausleihe und Anwendung
- Installation der App „Duo Mobile“ auf dem Smartphone
- Erstregistrierung in Cisco Duo
- Anwendung der App beim Login in KLIPS 2.0

https://gasthoerersenioren.uni-koeln.de/lehrvideos/lehrvideo-multifaktor-authentifizierung-mfa

Das Video konnte mit der finanziellen Förderung des Vereins zur Förderung des Gasthörer- und Seniorenstudiums umgesetzt werden.

Herzliche Grüße

Anne Löhr