

Inhaltsverzeichnis / Table of Contents

Multifaktor-Authentifizierung (MFA) für die Uni-ID.....	2
Authentifizierungsapps.....	2
Empfohlene Authentifizierungsapps.....	2
Anleitung zur Einrichtung einer Authentifizierungsapp (TOTP).....	3
Kontakt und Support.....	3
Multifactor Authentication (MFA) for the Uni-ID.....	4
Authentication apps.....	4
Recommended authentication apps.....	4
Setting up the authentication app (TOTP).....	5
Contact and support.....	5

Multifaktor-Authentifizierung (MFA) für die Uni-ID

Für: neue Studierende ab dem Wintersemester 2026/ 2027

Die Uni-ID gewährt Zugriff zu unterschiedlichen Diensten, die in vielen Fällen auch mit Zugriff auf personenbezogene Daten oder sensible Prozesse der IT-Infrastruktur einhergehen. Eine Absicherung nur mit einem Passwort ist für einige Dienste daher nicht ausreichend, da Passwörter wiederverwendbar sind, leicht gestohlen oder einfach erraten werden können.

Eine mit Multifaktor-Authentifizierung (MFA) abgesicherte Uni-ID benötigt zur Anmeldung nicht nur das Passwort, sondern auch einen zusätzlichen Faktor, in Ihrem Fall eine Authentifizierungs-App.

Authentifizierungsapps

Authentifizierungsapps auf Ihrem Smartphone generieren zeitbasierte Codes (TOTP), die bei jeder Anmeldung abgelesen und eingegeben werden müssen.

Für die Einrichtung installieren Sie eine Authentifizierungsapp auf Ihrem Smartphone. Die Einrichtung wird abgeschlossen, indem ein QR-Code gescannt und anschließend ein von der App erzeugter Code eingegeben wird.

Empfohlene Authentifizierungsapps

App	Android	iOS	Desktop
<u>Aegis Authenticator</u>	<u>Google Play Store</u> <u>F-Droid</u>	n/a	n/a
<u>FreeOTP</u>	<u>Google Play Store</u> <u>F-Droid</u>	App Store	n/a
<u>2FAS Auth</u>	<u>Google Play Store</u> <u>APK (Github)</u>	<u>App Store</u>	n/a
<u>Proton Authenticator</u>	<u>Google Play Store</u> <u>F-Droid</u>	<u>App Store</u>	Windows MacOS Linux <u>https://proton.me/authenticator/download</u>
<u>2fast</u>	n/a	n/a	Windows <u>https://apps.microsoft.com/detail/9p9d81glh89q</u>
<u>Ente Auth</u> (Offline-Modus)	<u>Google Play Store</u> <u>F-Droid</u>	App Store	Windows MacOS Linux <u>https://ente.com/auth/</u>
<u>KeepassXC</u> (Passwortmanager)	n/a	n/a	Windows MacOS Linux <u>https://keepassxc.org/download/</u>

Anleitung zur Einrichtung einer Authentifizierungsapp (TOTP)

Die Authentifizierungsapp wird auf Ihrem Smartphone oder Tablet installiert. Wir empfehlen die Verknüpfung Ihrer Uni-ID mit einer App in GOsa ggf. auf einem zweiten Endgerät durchzuführen.

1.	Öffnen Sie zur Aktivierung Ihrer Uni-ID GOsa auf einem Endgerät: https://gosa.gosa.uni-bonn.de/ Halten Sie zusätzlich Ihr Smartphone oder Tablet mit installierter Authentifizierungsapp bereit.
2.	Nach der Aktivierung gelangen Sie direkt zum Verknüpfungsprozess. Die Option „Authentifizierungsapp“ sollte vorausgewählt sein, ansonsten wählen Sie diese Option und klicken Sie auf „Auswählen“.
3.	Legen Sie eine Beschreibung fest, mit der Sie die Authentifizierungsapp bei späteren Anmeldungen wiedererkennen können. Sie können die Beschreibung auch später noch in GOsa ändern. Klicken Sie auf „Weiter“.
4.	Es wird ein QR-Code angezeigt, den Sie mit Ihrer Authentifizierungsapp scannen müssen. Alternativ tippen Sie den darunterstehenden Code manuell in Ihrer Authentifizierungsapp ein. Dazu nutzen Sie die Option zum Hinzufügen eines neuen Kontos (oft ein Button mit einem '+' oder einem QR-Code Symbol) und folgen den Anweisungen in der App. Stellen Sie sicher, dass niemand diesen QR-Code sehen konnte. Wenn Sie sich unsicher sind, erzeugen Sie einen neuen QR-Code über die gleichnamige Schaltfläche. Wenn das Konto in der Authentifizierungsapp eingerichtet ist, klicken Sie auf „Weiter“.
5.	Bestätigen Sie die korrekte Einrichtung der Authentifizierungsapp, indem Sie den dort nun sichtbaren sechsstelligen Code in GOsa eingeben. Beachten Sie, dass der Code sich regelmäßig ändert. Wenn der Code korrekt ist, wird die Multifaktor-Authentifizierung für Ihre Uni-ID aktiv. Das betrifft auch Ihre nächste Anmeldung an GOsa.

Kontakt und Support

Bitte wenden Sie sich bei Fragen oder Problemen bei der Einrichtung und Verwendung mit der Multifaktor-Authentifizierung an den MFA-Support: mfa-support@uni-bonn.de

Multifactor Authentication (MFA) for the Uni-ID

For: new students starting winter semester 2026/ 2027

The Uni-ID allows access to many different services that often include access to personalised data or sensitive processes of the IT infrastructure. For some of these services, a password-only protection is therefore not enough, as passwords are reusable, can be easily stolen or simply guessed.

A Uni-ID protected by Multifactor Authentication (MFA) requires an additional factor, in your case an authentication app, next to the password for successful logins.

Authentication apps

Authentication apps on your smartphone generate time-based codes (TOTP), which have to be read off and entered for each login.

For the setup, install an authentication app on your smartphone. The setup is completed by scanning a QR code and subsequently entering a code generated by the app.

Recommended authentication apps

App	Android	iOS	Desktop
Aegis Authenticator	Google Play Store F-Droid	n/a	n/a
FreeOTP	Google Play Store F-Droid	App Store	n/a
2FAS Auth	Google Play Store APK (Github)	App Store	n/a
Proton Authenticator	Google Play Store F-Droid	App Store	Windows MacOS Linux https://proton.me/authenticator/download
2fast	n/a	n/a	Windows https://apps.microsoft.com/detail/9p9d81glh89g
Ente Auth (Offline-Modus)	Google Play Store F-Droid	App Store	Windows MacOS Linux https://ente.com/auth/
KeepassXC (Passwortmanager)	n/a	n/a	Windows MacOS Linux https://keepassxc.org/download/

Setting up the authentication app (TOTP)

The authentication app will be installed on your smartphone or tablet. We recommend to use a second device for connecting your Uni-ID with an app in GOsa, if applicable.

1.	To activate your Uni-ID, open GOsa on your device: https://gosa.gosa.uni-bonn.de/ Additionally , have your smartphone or tablet with an installed authentication app on hand.
2.	After the activation you are directly forwarded to the connection process. The option "Authentication App" should be preselected, otherwise select this option manually.
3.	Choose a description for this entry in the authentication app, so you can recognise it later during login processes. You can change the description later in GOsa. Select "Continue".
4.	A QR code will be displayed, which you will have to scan with your authentication app. As an alternative you can manually enter the code displayed underneath into your authentication app. To do this, use the option to add a new account (usually a button with a '+' or a QR code symbol) and follow the instructions in the app. Make sure nobody was able to see the QR code. If you are unsure, generate a new QR code via the same interface. Once you have set up the account in the authentication app, select continue.
5.	Confirm the correct setup of the authentication app by entering the now visible six digit code into GOsa. Please keep in mind that the code changes regularly. If the code is correct, the multifactor authentication is active for your Uni-ID. This includes your next login into GOsa.

Contact and support

If you have questions or regarding the setup and use of the multifactor authentication, please contact the MFA support: mfa-support@uni-bonn.de