

Multi-Faktor-Authentifizierung (MFA) für Gastkonten

Seit August 2026 ist Multi-Faktor-Authentifizierung (MFA) für Gastkonten an der Hochschule Düsseldorf verbindlich. Im Folgenden wird die Einrichtung von MFA für Gastkonten beschrieben. Beschäftigte und Studierende können die Anleitungen im [CITipedia](#) zurate ziehen.

Einrichtungsaufforderung

Sobald die Nutzung verbindlich ist, werden Sie nach der Anmeldung zur Einrichtung aufgefordert.

HSD

Lassen Sie uns Ihr Konto schützen

Wir helfen Ihnen, eine andere Methode einzurichten, um zu überprüfen, ob Sie es sind.

[Anderes Konto verwenden](#)

[Weitere Informationen zur Verifizierung Ihrer Identität](#)

Weiter

Bitte geben Sie die **E-Mail Adresse** Ihres **HSD Accounts** ein.

Gäste geben Ihre externe E-Mail Adresse ein.
[Anleitung](#) zur Einrichtung der MFA für Gäste.

Einrichtung

Im Standard wird Microsoft Authenticator angeboten. Alternativ können auch alternative Authenticator Apps, welche das TOTP-Verfahren unterstützen, oder physische TOTP-Generatoren verwendet werden. Im Folgenden wird zunächst die Einrichtung von Microsoft Authenticator und anschließend die Einrichtung des TOTP-Verfahrens beschrieben.

Microsoft Authenticator

Um die Microsoft Authenticator App einzurichten, installieren Sie die App auf Ihrem Smartphone und navigieren *Weiter*.

HSD

#EXT#@fhd.onmicrosoft.com

Microsoft Authenticator installieren



Installieren Sie die App auf Ihrem mobilen Gerät und kehren Sie dann hierher zurück, um fortzufahren.

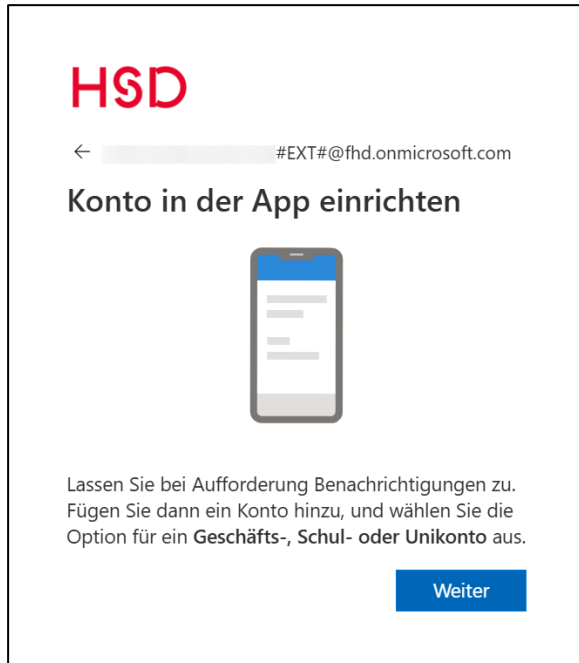
GET IT ON
Google Play

Download on the
App Store

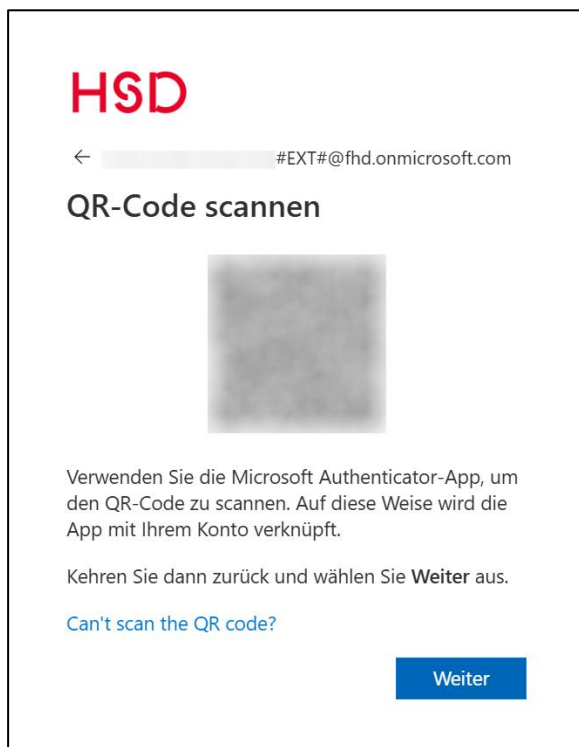
[Andere App für die Authentifizierung einrichten](#)

Weiter

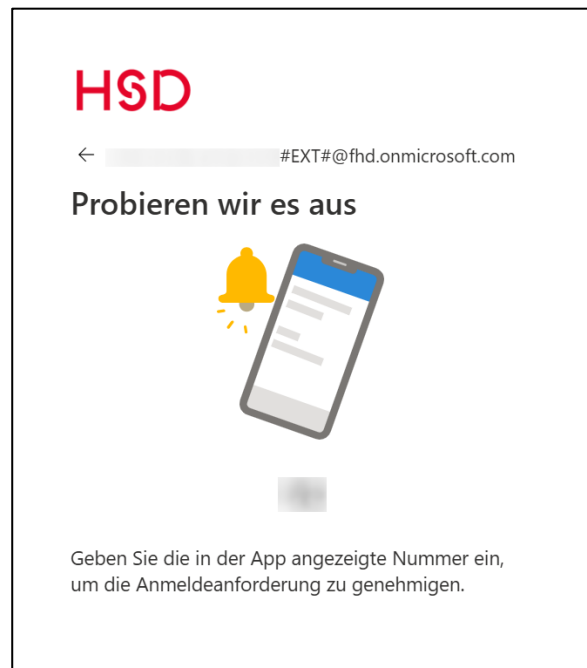
Nach der Installation der Authenticator App öffnen Sie diese und erlauben die Zustellung von Benachrichtigungen. Anschließend wählen Sie in der App die Option **+ Konto hinzufügen > Geschäfts- oder Schulkonto > QR-Code scannen**. Im Einrichtungsdialog navigieren Sie *Weiter*.



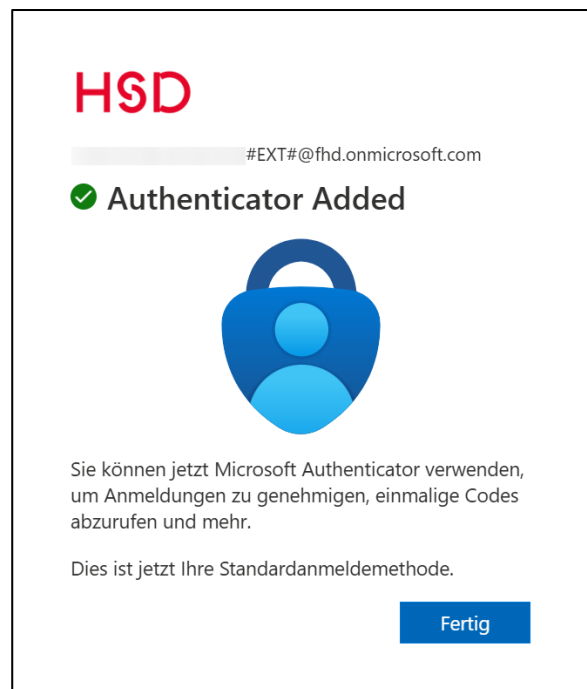
Scannen Sie nun mit Ihrem Smartphone den angezeigten QR-Code aus dem Einrichtungsdialog. Nach erfolgreichem Scannen navigieren Sie *Weiter*.



Im nächsten Schritt wird die Einrichtung mittels Codes validiert. Auf Ihrem Smartphone erscheint eine Benachrichtigung zur Eingabe des angezeigten Codes.



Nach erfolgreicher Eingabe des Codes ist die Verbindung hergestellt und die Authentifizierungsmethode erfolgreich eingerichtet.



Alternatives TOTP Verfahren

Um eine andere TOTP basierte Authenticator App oder einen physischen TOTP-Generator einzurichten, folgen Sie nachfolgenden Schritten. Wählen Sie im Einrichtungsdialog *Andere App für die Authentifizierung einrichten*.

HSD

← #EXT#@fhd.onmicrosoft.com

Microsoft Authenticator installieren



Installieren Sie die App auf Ihrem mobilen Gerät und kehren Sie dann hierher zurück, um fortzufahren.



[Andere App für die Authentifizierung einrichten](#)

Weiter

Bereiten Sie Ihre Authenticator App oder TOTP-Generator für die Einrichtung vor und navigieren *Weiter*.

HSD

← #EXT#@fhd.onmicrosoft.com

Konto in der App einrichten



Fügen Sie zunächst Ihr Konto hinzu.

Weiter

Scannen Sie nun mit Ihrer Authenticator App oder Ihrem TOTP-Generator den gezeigten QR-Code und navigieren anschließend *Weiter*.

HSD

← #EXT#@fhd.onmicrosoft.com

QR-Code scannen



Verwenden Sie Ihre Authenticator-App, um den QR-Code zu scannen. Auf diese Weise wird die App mit Ihrem Konto verknüpft.

Kehren Sie dann zurück und wählen Sie **Weiter** aus.

[Can't scan the QR code?](#)

Weiter

Alternativ können Sie sich den Wert auch anzeigen lassen zur manuellen Kopie durch Wählen von *Can't scan the QR code?* Navigieren Sie anschließend *Weiter*.

HSD

← #EXT#@fhd.onmicrosoft.com

Enter the following into Authenticator

Öffnen Sie den QR-Code-Scanner in Authenticator und wählen Sie **Code manuell eingeben** aus.

Kontoname: [Namen kopieren](#)

Hochschule Düsseldorf: [#EXT#@fhd.onmicrosoft.com](#)

Geheimer Schlüssel: [Schlüssel kopieren](#)

Weiter

Im nächsten Schritt wird die Einrichtung mittels Codes validiert. Geben Sie den Code, der nun in Ihrer Authenticator App oder Ihrem TOTP-Generator angezeigt wird, ein und *Überprüfen* diesen.

HSD

Code eingeben

123 Geben Sie den Code ein, der in der Authenticator-App auf Ihrem mobilen Gerät angezeigt wird

Code

[Weitere Informationen](#)

AbbrechenÜberprüfen

Bitte geben Sie die **E-Mail Adresse** Ihres [HSD Accounts](#) ein.

Gäste geben Ihre externe E-Mail Adresse ein.
[Anleitung](#) zur Einrichtung der MFA für Gäste.

War die Eingabe erfolgreich, ist die Einrichtung der Authentifizierungsmethode abgeschlossen.

HSD

#EXT#@fhd.onmicrosoft.com

 **Authenticator-App
hinzugefügt**



Verwenden Sie Codes aus dieser App, wenn Sie sich das nächste Mal anmelden.

Fertig