

## Anmeldung mit MFA an Microsoft - M365-Diensten

Zur Erhöhung der Sicherheit bei der Anmeldung an M365-Diensten für: Lehrende und Mitarbeiter führt die Evangelische Hochschule Darmstadt zum Start des Sommersemesters die Multi-Faktor-Authentifizierung (MFA) ein.

### Hinweis:

Die MFA ist **nur** für die Anmeldung an M365-Diensten und Programme die auf diese angewiesen sind **notwendig**, Moodle, CAS, das WLAN, die Technikausleihe, ... usw. funktionieren weiterhin mit den gewohnten Zugangsdaten **ohne MFA**.

### M365-Dienste:

MS Teams: <https://teams.microsoft.com/>  
Exchange Online (E-Mail): <https://outlook.office.com/mail/>  
Intranet: <https://ehdarmstadtde.sharepoint.com/sites/IntranetderEHD>  
Office 365: <https://office.com>

### Lokal Installierte Programme

Outlook

MS Office 365

### Zugangsdaten eingeben:

E-Mail-Adresse: [Benutzername + @ maildomain]

[rainer.test@eh-darmstadt.de](mailto:rainer.test@eh-darmstadt.de)



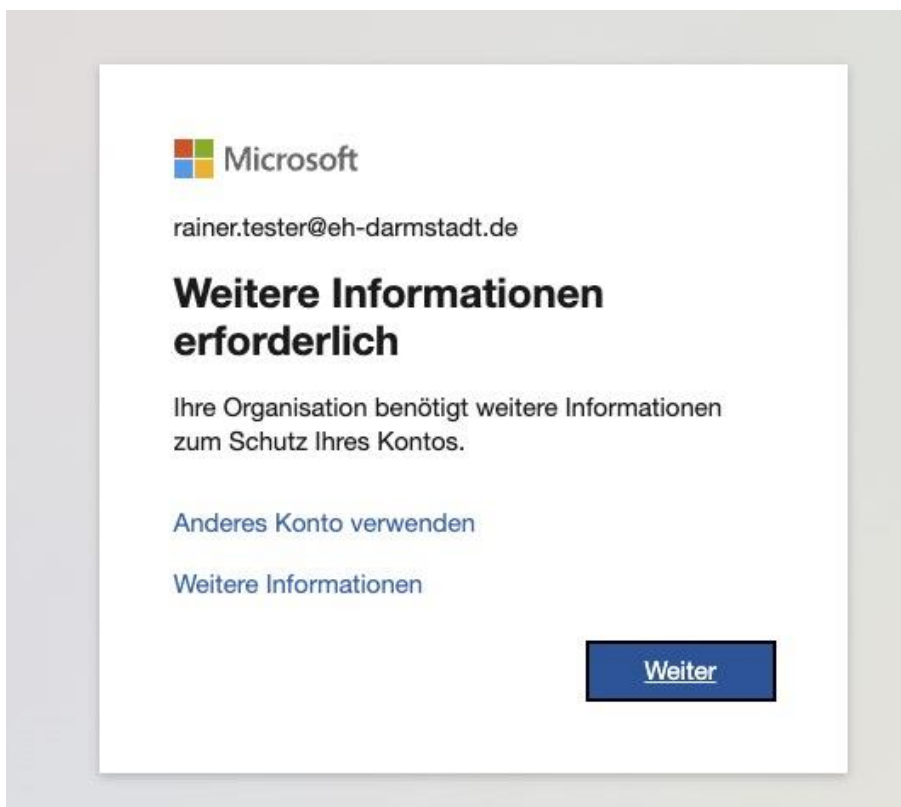
The screenshot shows the Microsoft login interface. At the top left is the Microsoft logo. Below it, the word 'Anmelden' is displayed in a large, bold font. Underneath, the email address 'rainer.test@eh-darmstadt.de' is entered into a text field. Below the text field, there is a link that says 'Sie können nicht auf Ihr Konto zugreifen?'. At the bottom of the login area, there are two buttons: 'Zurück' (grey) and 'Weiter' (blue). Below the main login area, there is a separate box containing a key icon and the text 'Anmeldeoptionen'.

Ihr EHD-Passwort eingeben:



The screenshot shows a Microsoft login interface. At the top left is the Microsoft logo. Below it, the email address 'rainer.test@eh-darmstadt.de' is displayed with a back arrow. The main heading is 'Kennwort eingeben'. There is a password input field with a masked password '.....' and a cursor. Below the field is a link 'Kennwort vergessen'. At the bottom right is a blue button labeled 'Anmelden'.

Hinweis zur MFA-Authentifizierung, auf „Weiter“ klicken



The screenshot shows a Microsoft login interface for MFA authentication. At the top left is the Microsoft logo. Below it, the email address 'rainer.test@eh-darmstadt.de' is displayed. The main heading is 'Weitere Informationen erforderlich'. Below this is the text 'Ihre Organisation benötigt weitere Informationen zum Schutz Ihres Kontos.' There are two links: 'Anderes Konto verwenden' and 'Weitere Informationen'. At the bottom right is a blue button labeled 'Weiter'.

## 2. Methode der Multi-Faktor-Authentifizierung

Sie haben nun verschiedene Auswahlmöglichkeiten für die zusätzliche Authentifizierungsmethode zur Verfügung:


- a. Microsoft Authenticator (bevorzugte Variante)
- b. Weitere Authenticator Apps (z. B. Google Authenticator)
- c. **Hardware Token (z. B. ReinerSCT Authenticator)**
- d. andere Methode z. B. über SMS

### Schützen Sie Ihr Konto

Methode 1 von 2: App


App 2  
App-Kennwort

#### Microsoft Authenticator

 Rufen Sie zuerst die App ab.

Installieren Sie die Microsoft Authenticator-App auf Ihrem Smartphone. [Jetzt herunterladen](#)

Nachdem Sie die Microsoft Authenticator-App auf Ihrem Gerät installiert haben, wählen Sie "Weiter".

 [Ich möchte eine andere Authenticator-App verwenden](#)

[Weiter](#)


[Ich möchte eine andere Methode einrichten.](#)

### Schützen Sie Ihr Konto

Methode 1 von 2: App

App 2  
App-Kennwort

#### Authenticator-App

 **Konto einrichten**

Fügen Sie Ihrer App ein neues Konto hinzu.

[Zurück](#) [Weiter](#)

[Ich möchte eine andere Methode einrichten.](#)

### 3. Reiner SCT Authenticator



1. „OK“ drücken zum Einschalten.



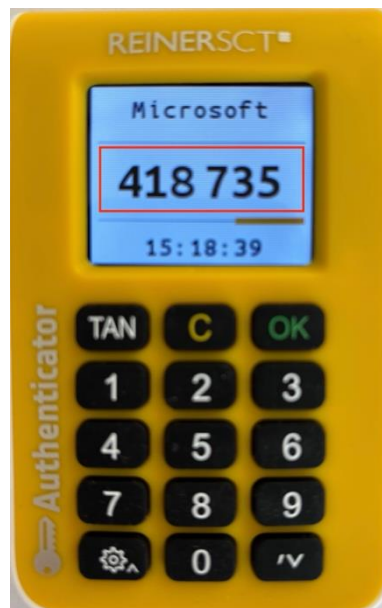
2. Das „Zahnrad“ drücken um in die Einstellungen zu gelangen.



3. Die Taste „3“ drücken, um Konten hinzuzufügen.



4. Die Taste „1“ drücken, um den QR-Code mit der integrierten Kamera zu scannen.



5. Die Einrichtung des Microsoft-Kontos ist abgeschlossen, der angezeigte Code kann jetzt zur Verifizierung des Kontos genutzt werden.

#### 4. QR-Code mit dem Reiner SCT Authenticator scannen.

### Schützen Sie Ihr Konto

Methode 1 von 2: App


App 2  
App-Kennwort

#### Authenticator-App

QR-Code scannen

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

Nachdem Sie den QR-Code gescannt haben, wählen Sie "Weiter".



Das Bild wird nicht gescannt?

QR-Code mit dem Reiner SCT Authenticator scannen.

[Ich möchte eine andere Methode einrichten.](#)

### Schützen Sie Ihr Konto

Methode 1 von 2: App

App 2  
App-Kennwort

#### Authenticator-App

Code eingeben

Geben Sie den sechsstelligen Code ein, der in der Authenticator-App angezeigt wird.

angezeigter Code vom Reiner SCT Authenticator

[Ich möchte eine andere Methode einrichten.](#)

## Schützen Sie Ihr Konto

Methode 2 von 2: App-Kennwort



App



App-Kennwort

### App-Kennwort

Erstellen Sie zuerst einen Namen für Ihr App-Kennwort. So können Sie es von anderen unterscheiden.

Welchen Namen möchten Sie verwenden? Die Mindestlänge beträgt 8 Zeichen.

Namen für Authentifizierungsmethode eingeben

Weiter

## Schützen Sie Ihr Konto

Methode 2 von 2: App-Kennwort



App



App-Kennwort

### App-Kennwort

Das App-Kennwort wurde erfolgreich erstellt. Kopieren Sie das Kennwort in die Zwischenablage, und fügen Sie es in Ihre App ein. Kehren Sie anschließend hierher zurück, und klicken Sie auf "Fertig".

**Name:**

Reiner SCT

**Kennwort:**

lbvjbtmzsjvyrqvm



Hinweis: Bewahren Sie dieses Kennwort an einem sicheren Ort auf. Es wird nicht noch einmal angezeigt.

Zurück

Fertig



Die Einrichtung ist erfolgreich abgeschlossen.

Der Reiner SCT Authenticator ist erfolgreich eingerichtet und kann ab sofort für die Authentifizierung verwendet werden.

Sobald Sie versuchen, sich an einem Microsoft M365-Dienst anzumelden, und eine zusätzliche Authentifizierung per MFA nötig ist, benötigen Sie den Reiner SCT Authenticator, um sich anzumelden.

Bei Verlust wenden Sie sich umgehend an die IT, damit der verloren gegangene Reiner SCT Authenticator aus Ihrem Account gelöscht wird.

#### **Wichtiger Hinweis:**

Ein deaktivieren der MFA bei Verlust ist nicht möglich!

Um bei Verlust weiter Arbeiten zu können, müssen Sie entweder direkt ein Ersatzgerät beschaffen oder abholen oder den MS Authentifikator (App) als zweiten Faktor einrichten.

Schützen Sie den Reiner SCT Authenticator mit einem persönlichen PIN.  
Eine Anleitung und weitere Informationen finden Sie unter:

<https://www.reiner-sct.com/material/downloads/bedienungsanleitung/REINER-SCT-Bedienungsanleitung-REINER-SCT-Authenticator.pdf>