Azure Multi-Factor Authentication (MFA)

Publiziert spoc.cit.services@fhnw.ch allgemeine Anleitung Corporate IT Doku

Zeigt auf wie Azure MFA eingerichtet und verwaltet werden kann,

---

LINK: https://help.fhnw.ch/4584

<-- zu allen Artikeln rund um O365 / Azure AD

Wann braucht es MFA und wie funktioniert das?

Um die Sicherheit zu erhöhen, setzen wir die Verwendung eines zweiten Authentifizierungsfaktors voraus. Alle Dienste in Office 365 werden mit einem zweiten Faktor zusätzlich gesichert. Das heisst zum Beispiel für eine «Outlook im Web» oder Teams Anmeldung.

Folgende Optionen stehen zu dem zweiten Faktor zur Verfügung:

- Microsoft Authenticator-App (empfohlene Methode 1) 
- E-Mail (empfohlene Methode 2)
- OATH-Hardwaretoken (Token2 oder Yubikey)
- Google Authenticator, LastPass Authenticator

Folgende Methoden werden nicht mehr unterstützt:

- **SMS**
- **Anruf**

Wir empfehlen Microsoft Authenticator-App auf ihrem Smartphone.

Das Einrichten erfolgt automatisch durch einen Assistenten von Microsoft und wird im folgenden Abschnitt kurz beschrieben.

Genauere Infos dazu, können dem folgenden Link entnommen werden:

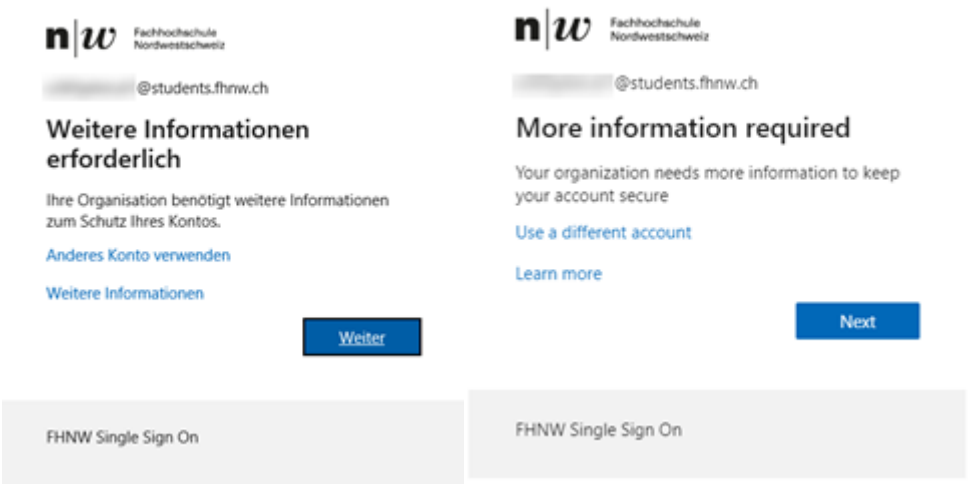
https://docs.microsoft.com/de-ch/azure/active-directory/authentication/concept-mfa-howitworks

Wie kann ich MFA Einrichten?

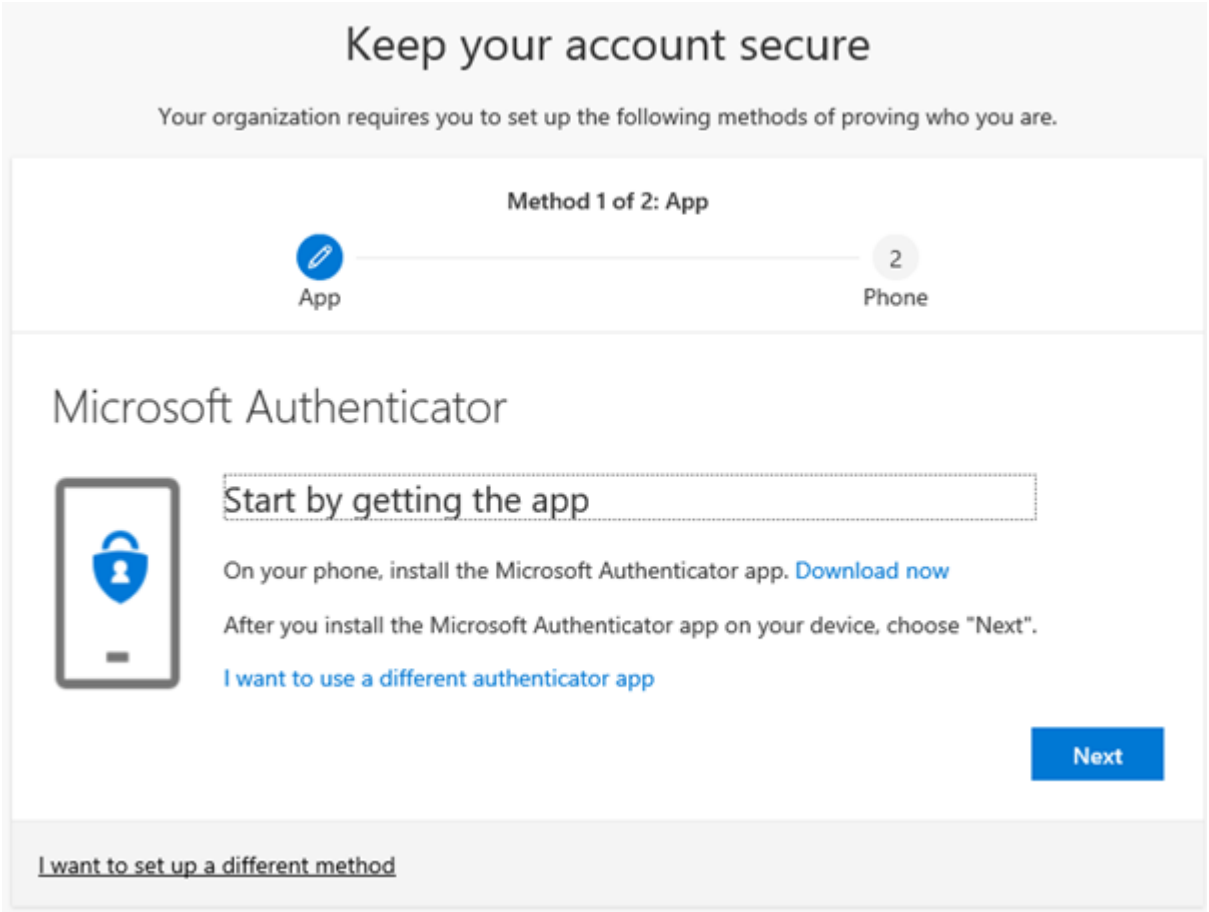
Schritt für Schritt Anleitung mit Bildern https://help.fhnw.ch/3331/mfa-azure-multi-factor-authentification/

Es wird empfohlen die einmalige Registration von MFA in einem separaten Browserfenster (Inkognito / privates Browser Fenster) zu machen und nicht in einer Office 365 App wie Teams.

Öffnen Sie den Browser und melden Sie sich auf https://office.com mit Ihrer FHNW E-Mail-Adresse an und befolgen die Anweisungen des Assistenten, um das Konto zu schützen.



Mit dem Klick auf «Weiter» wird man aufgefordert den zweiten Faktor festzulegen.



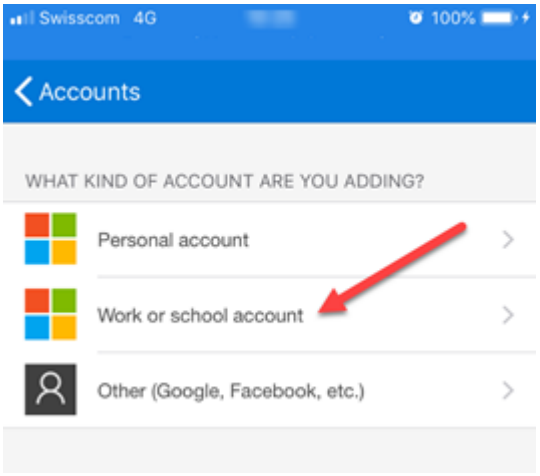
Der Faktor Microsoft Authenticator-App ist standardmässig bereits festgelegt. Wenn man eine andere Authenticator App verwenden will kann man das über folgende Optionen machen:

- Anderes Authenticator App (Bsp. von Google oder Authy) kann man das via «Ich möchte eine andere Methode einrichten / I want to set up a different methode»

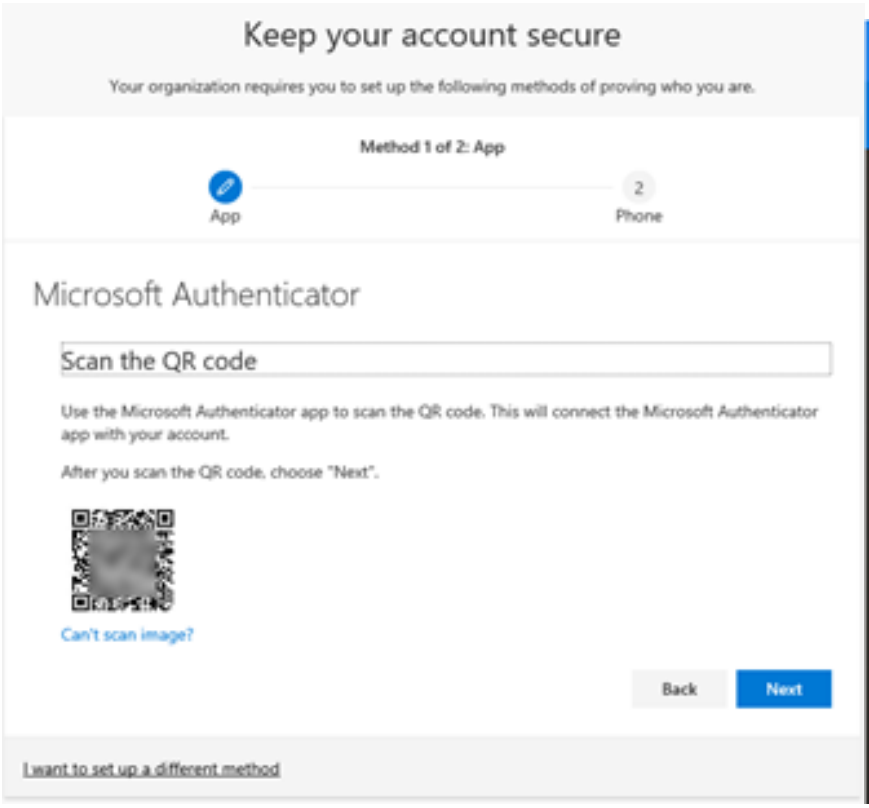
Wir fokussieren in der Anleitung auf das Microsoft Authenticator App. Das Einrichten eines anderen Faktors folgt nach dem gleichen Schema. Siehe https://help.fhnw.ch/1645/azure-active-directory-self-service-password-reset-sspr/

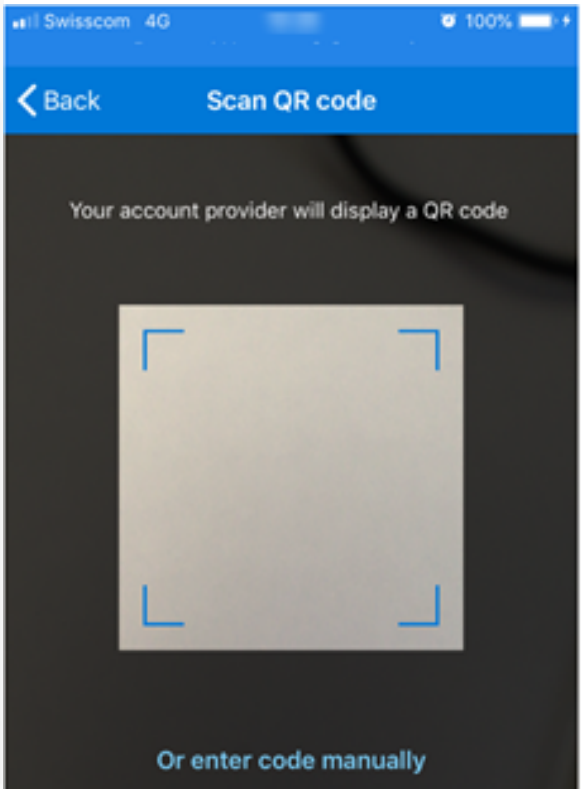
Als ersten Schritt müssen Sie das Microsoft Authenticator App auf ihrem Smartphone installieren. Sie finden dies im App Store des Smartphone Herstellers. Nach der Installation auf dem Smartphone können sie mit «Next» den Dialog im Browser bestätigen.

Sie werden nun aufgefordert auf im kürzlich installieren Microsoft Authenticator App einen neuen Account hinzuzufügen. Wählen Sie dafür «Work or school account» aus.



Nun können Sie den QR code scannen, welchem im Browser angezeigt wird.

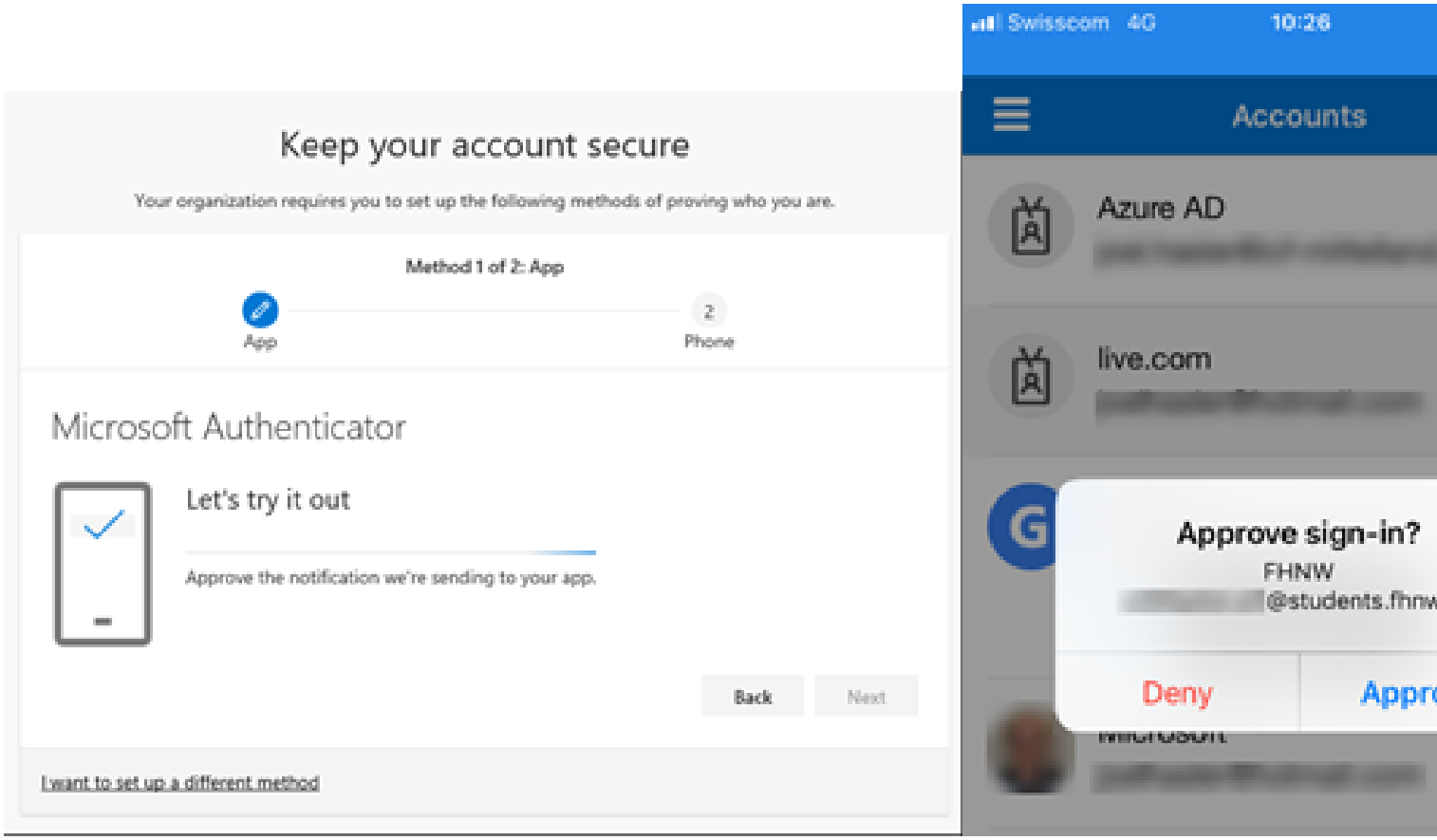




Browser Sicht

Smartphone Sicht

Mit dem Klick auf «Next» im Browser können Sie zum Ersten Mal den zweiten Faktor über das Microsoft Authenticator App bestätigen. Der Dialog sieht wie folgt aus:

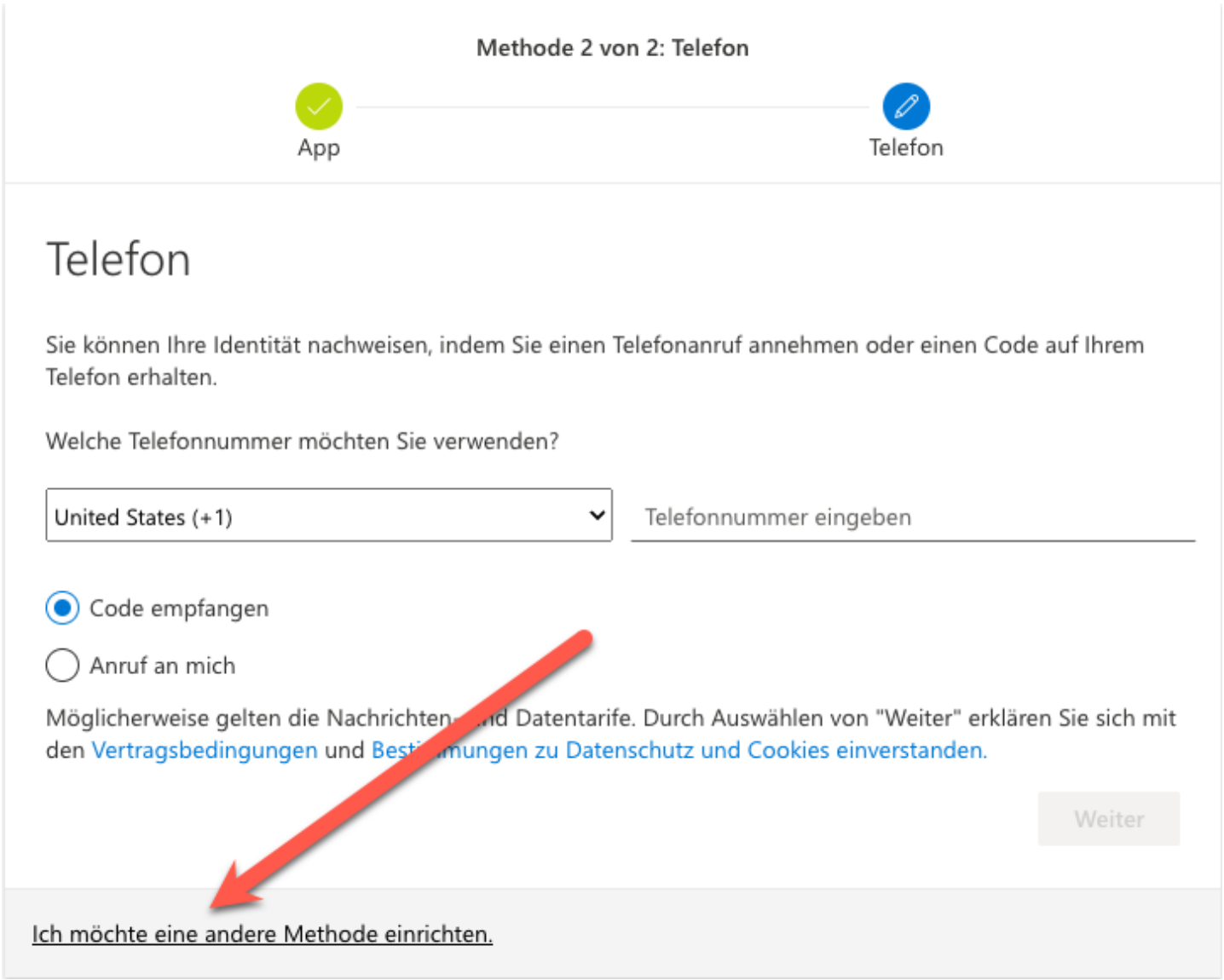


Browser Sicht Smartphone Sicht

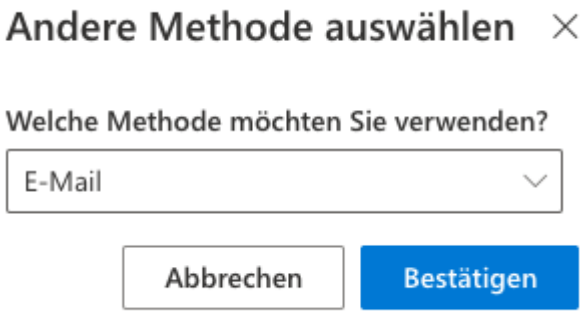
Mit dem Klick auf «Approve» auf Ihrem Smartphone haben Sie den ersten Teil der Einrichtung von zweiten Faktor abgeschlossen.

Im nächsten Schritt werden Sie aufgeforderd die zweite Methode (private Emailadresse) zu registrieren. Damit können Sie in Zukunft Ihr passwort bequem selbst neu setzen (Azure Active Directory self-service password reset).

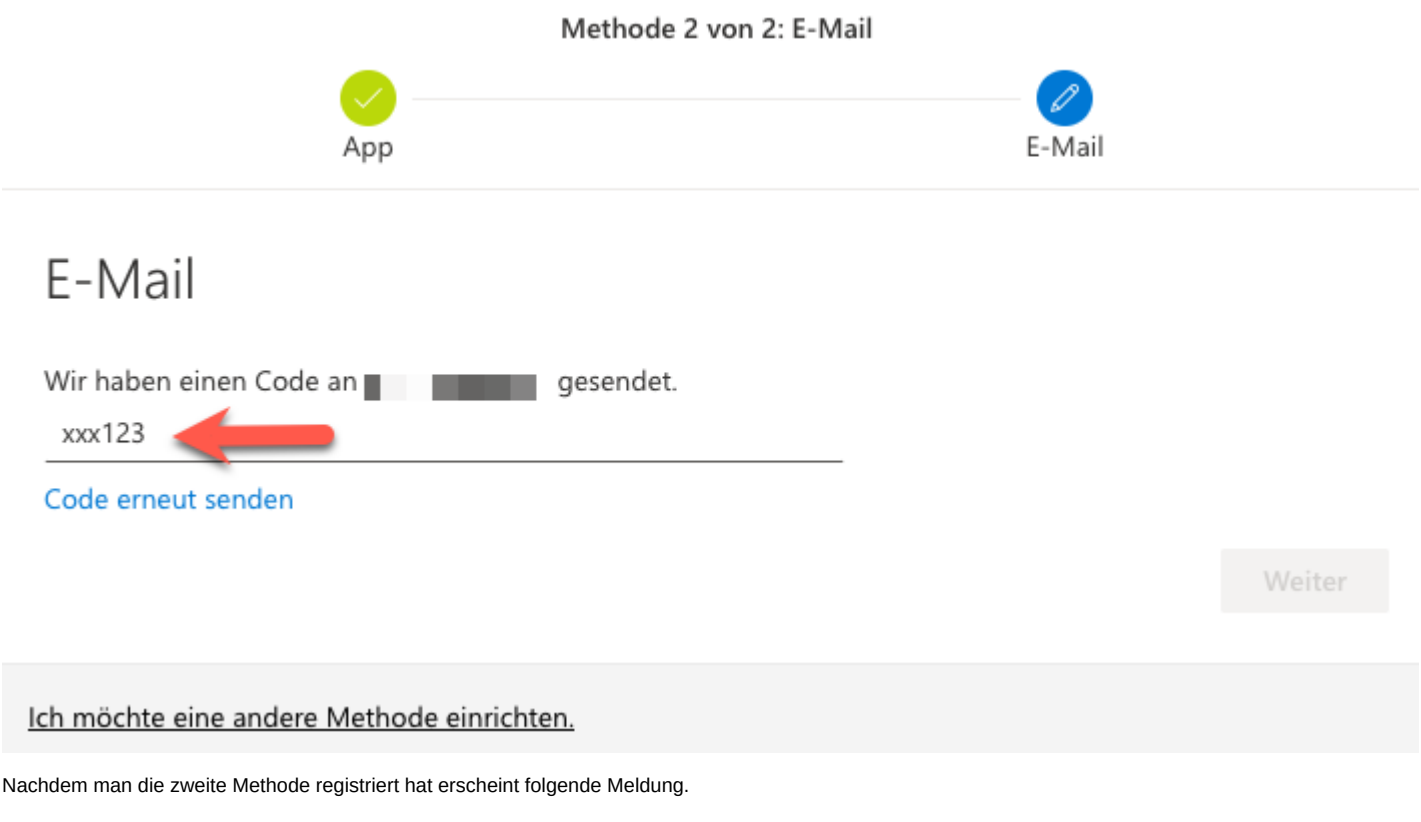
Standardmässig ist die Option Telefonnummer (Phone) ausgewählt, welche nicht mehr unterstützt wird. Über den Dialog «Ich möchte eine andere Methode einrichten / I want to set up a different methode» können Sie die Email Variante auswählen und die notwendigen Schritte durchführen. Bitte nicht die FHNW Emailadresse als Authentifizierung verwenden, **richtig wäre die private E-Mail**.



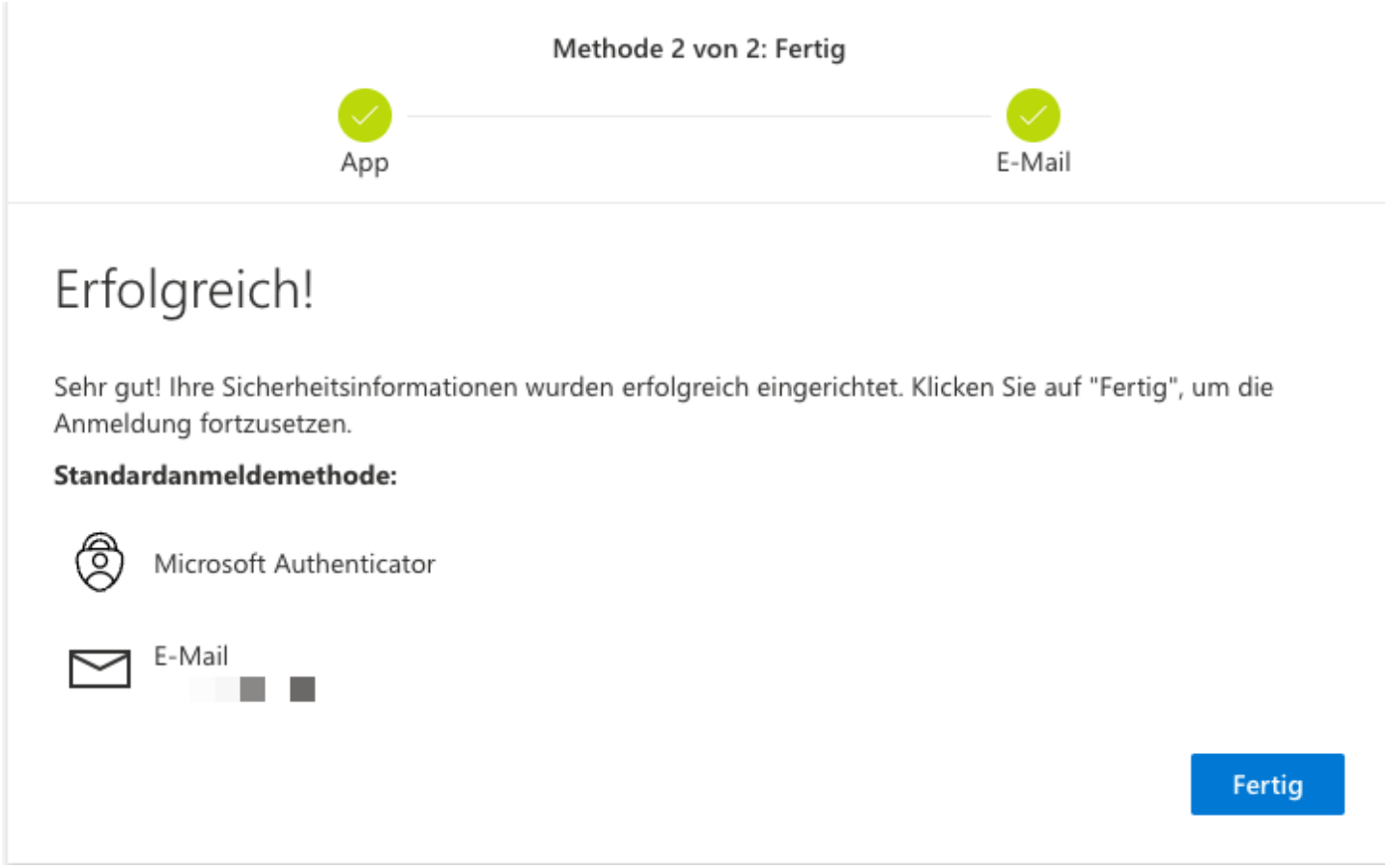
Nun erscheint die folgende Auswahl und hier bitte die E-Mail methode auswählen.



Innerhalb kurzer Zeit erhalten Sie im privaten Postfach einen 6-stelligen Pin, welcher hier eingetragen werden muss:



Nachdem man die zweite Methode registriert hat erscheint folgende Meldung.



Nun ist die MFA Registration mit Azure Active Directory self-service password reset abgeschlossen.

Wie kann ich die MFA Faktoren verwalten?

Die Verwaltung erfolgt über folgende URL: https://mysignins.microsoft.com

Darin können Sie unter «Security info» die erfassten Faktoren von Ihrem Account verwalten. So können Sie aus beispielsweise bei einem neuen Smartphone das Microsoft Authenticator App neu registrieren lassen. Wichtig ist, dass dies nur geht wenn man VPN aktiv hat.

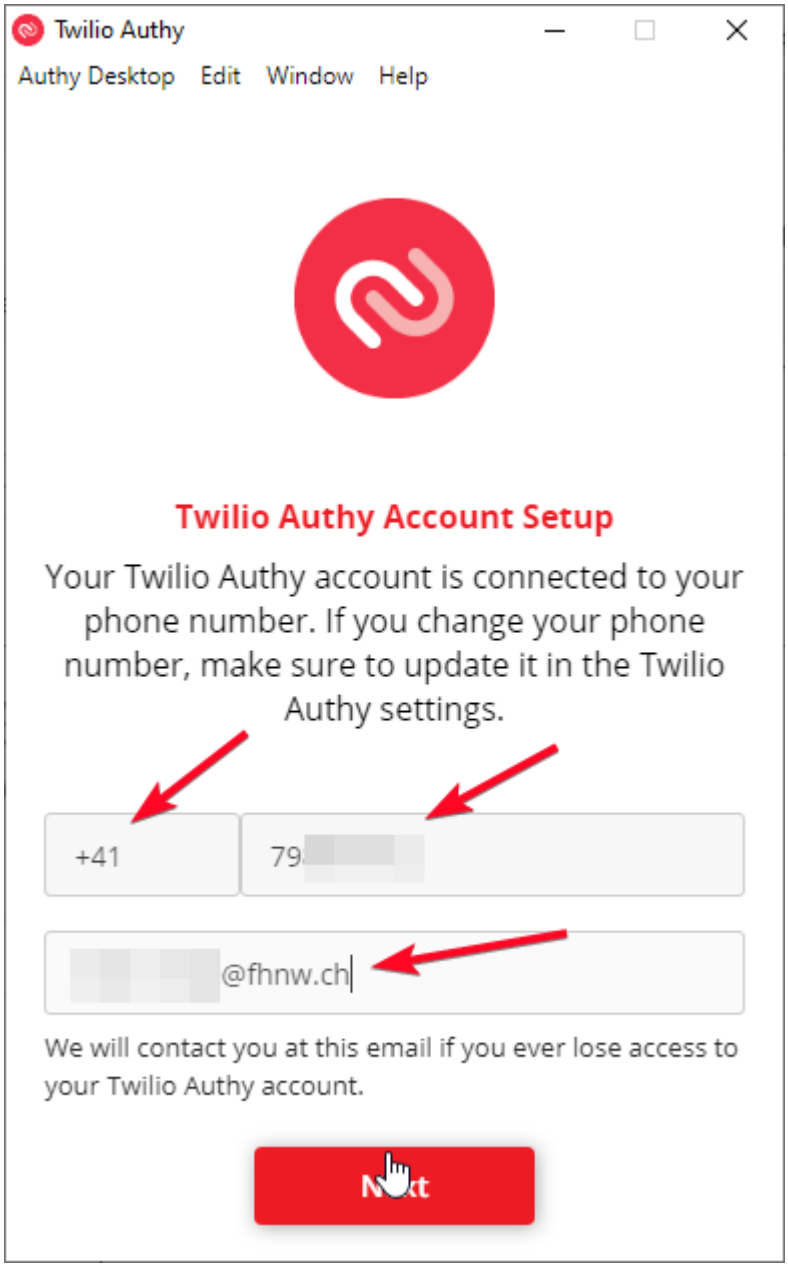
Weitere Fragen rund um MFA

1. Kann ich alternative MFA Apps nutzen?

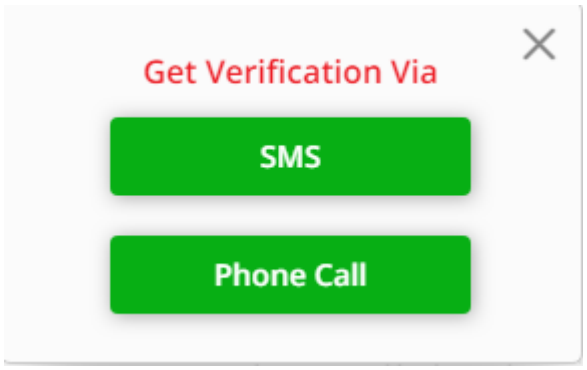
Ja, es können auch alternative MFA Apps verwendet werden (z. B. Authy).

Die App "Authy" steht im ServicePortal sowohl für Windows als auch für MacOS zur Verfügung (https://help.fhnw.ch/1265/software-kiosk-im-sccm/) oder sie downloaden es sich direkt unter https://authy.com/download/, wählen das passende Betriebsystem und klicken anschliessend auf Download.

Starten Sie nun die gedownloadete Datei und Tragen eine Telefonnummer und ihre FHNW Mailadresse ein.



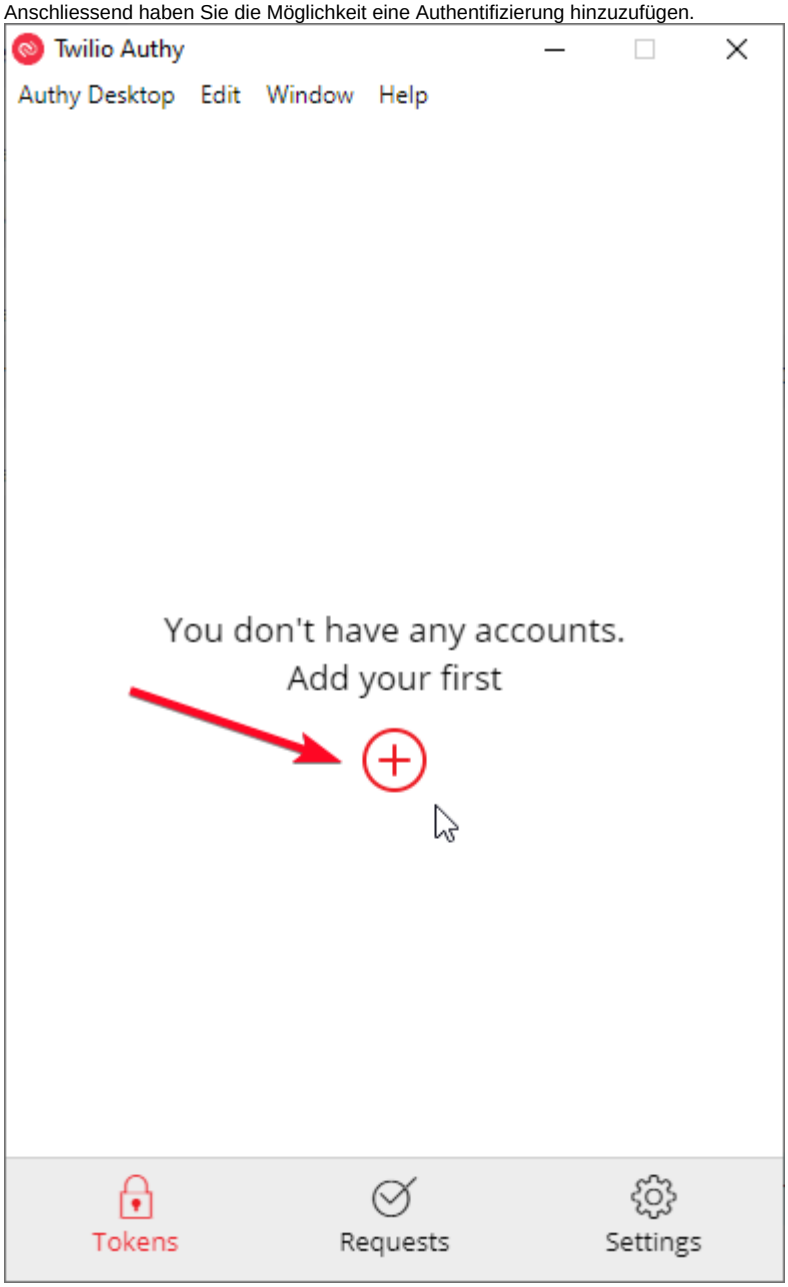
Nun muss eine Verifikation durchgeführt werden, entweder via SMS Code oder per anruf.

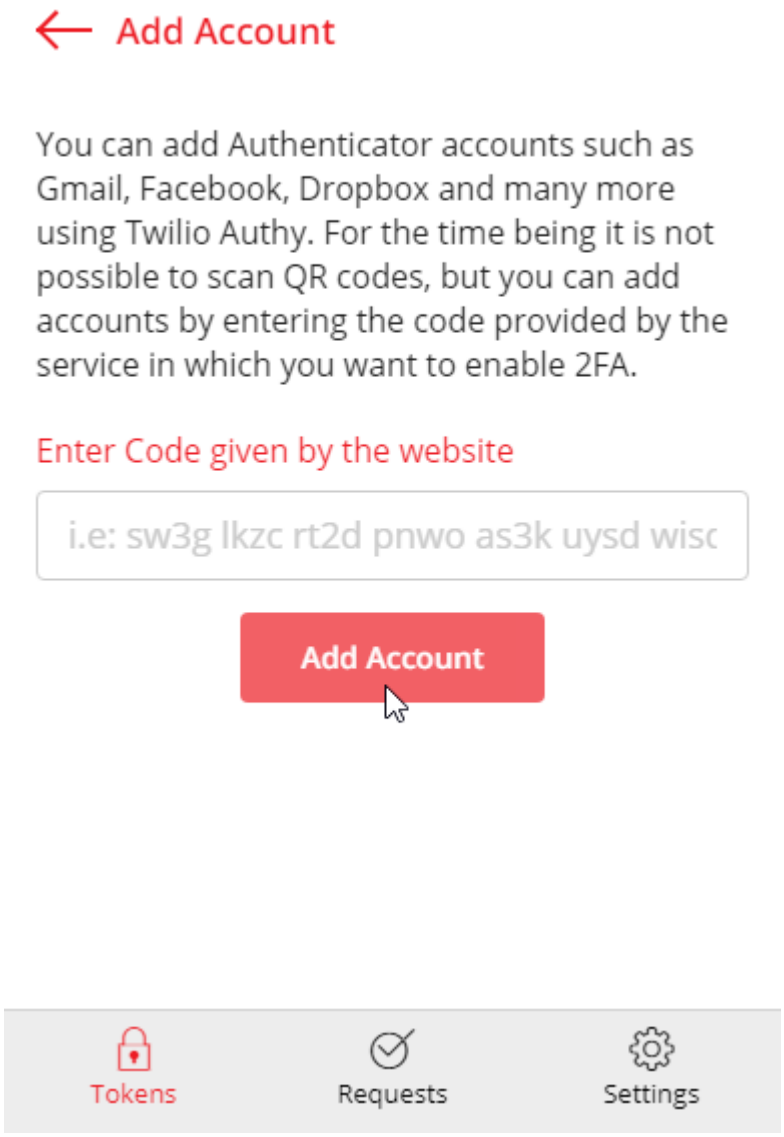


Im oberen Fall erhalten Sie einen 6-stelligen Code via SMS, welchen Sie eintippen müssen.

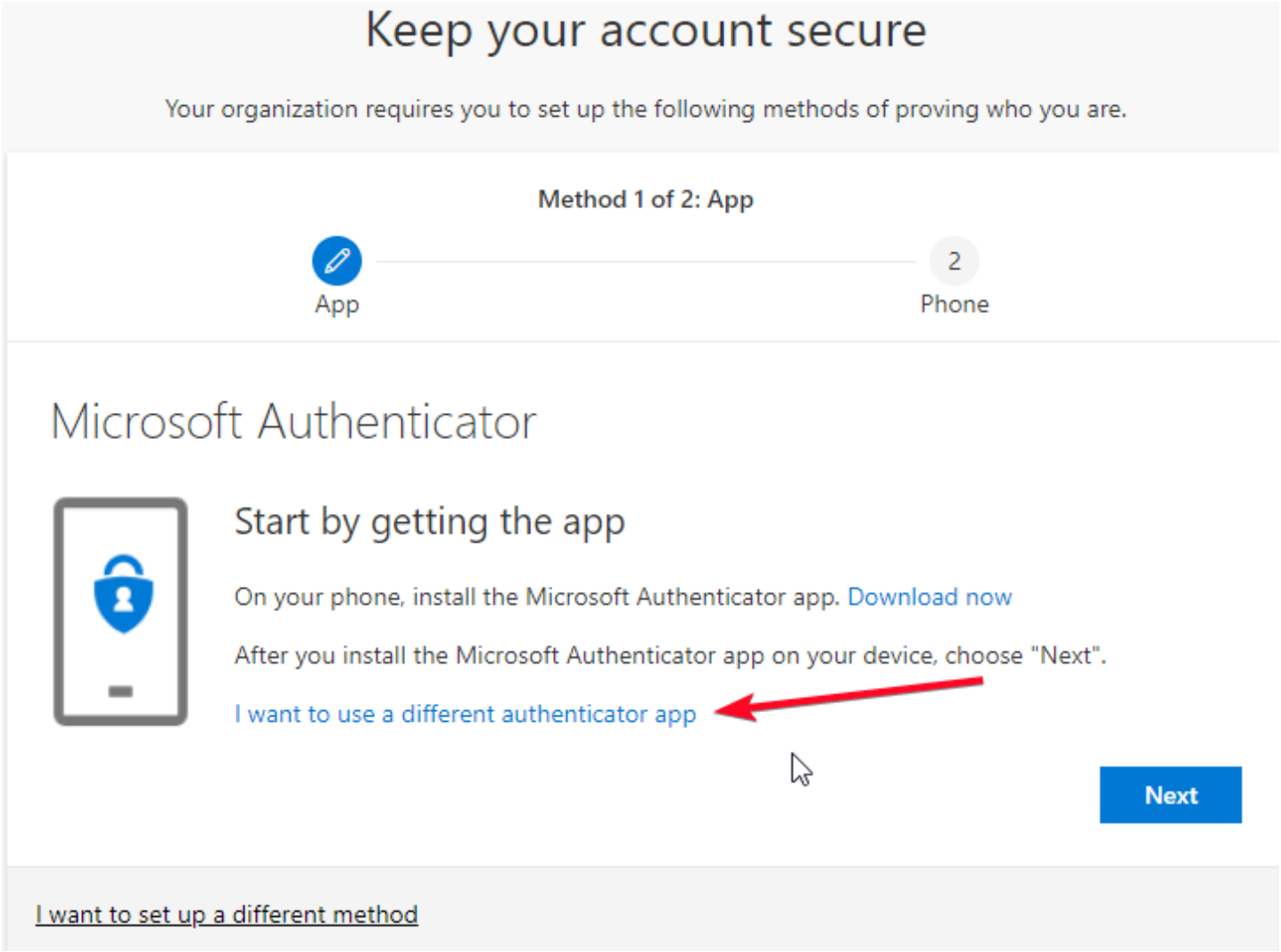
Im unteren Fall erhalten Sie einen Anrufen, bei dem Ihnen eine automatische Ansage sagt, was Sie tun müssen.

Anschliessend haben Sie die Möglichkeit eine Authentifizierung hinzuzufügen.

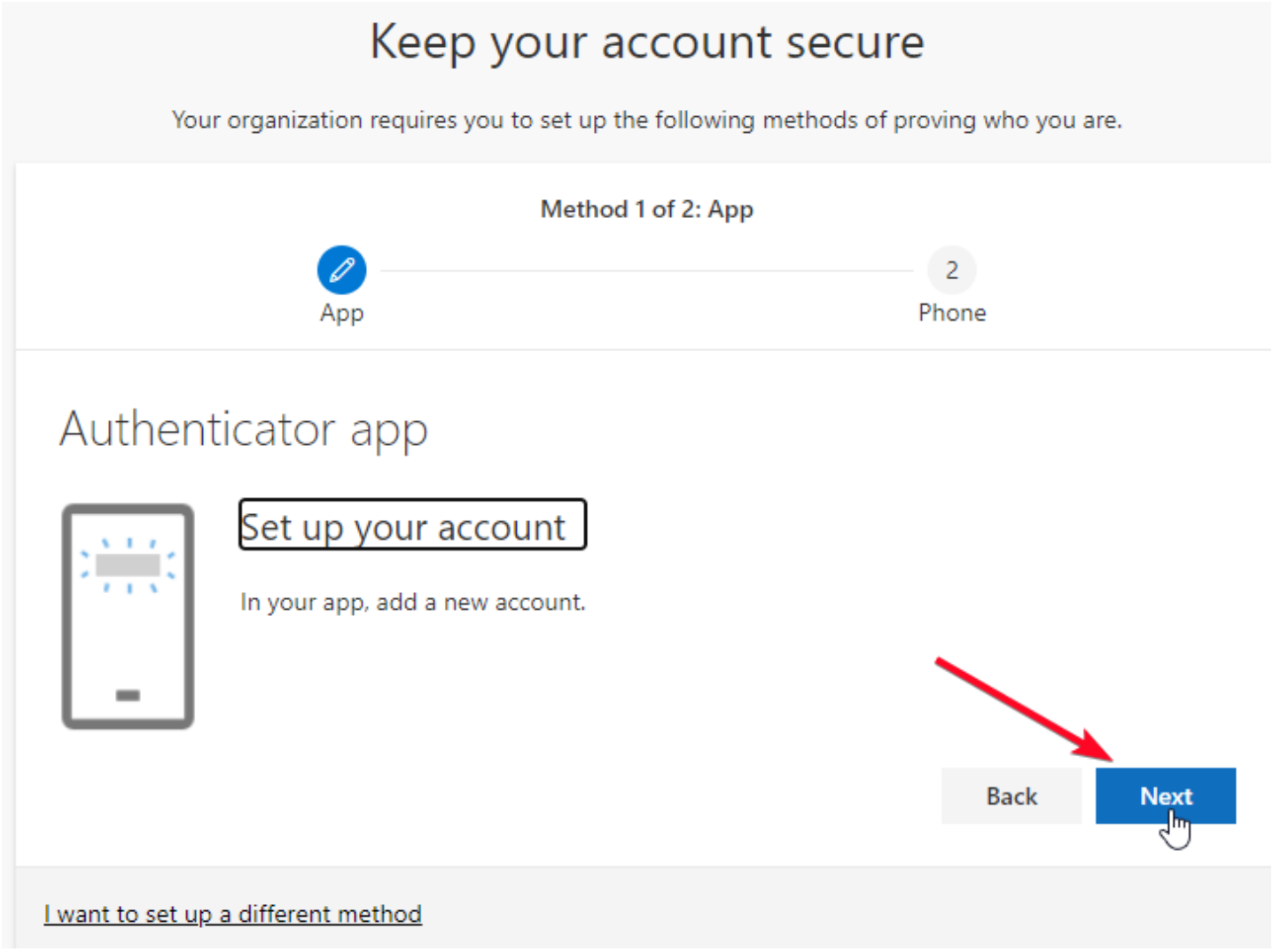




wechseln Sie nun zu ihrer MFA Registrierung und klicken Sie auf: "I want to use a different authenticator app".



Ein Klick auf "Next".



Nun klicken Sie auf: "Can't scan image?" und kopieren den Scret Key in die Authy App.

Method 1 of 2: App

App — 2 Phone

Authenticator app

Scan the QR code

Use the authenticator app to scan the QR code. This will connect your authenticator app with your account.

After you scan the QR code, choose "Next".

1

Can't scan image?

Enter the following into your app:

Account name: FHNW:ralph.lange@fhnw.ch

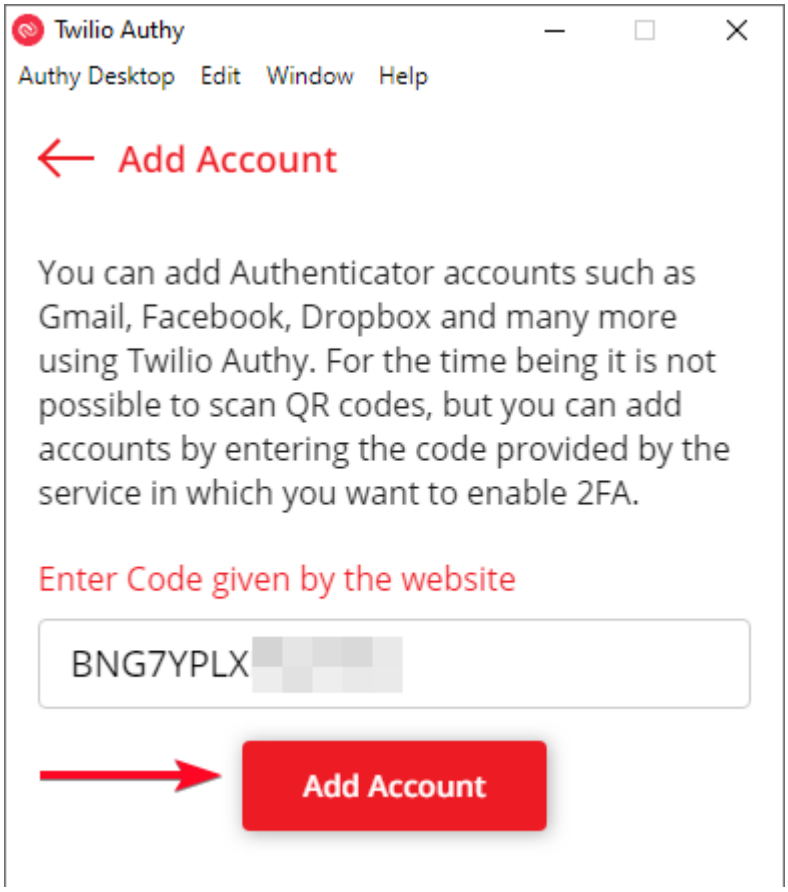
Secret key: bng7yplxpcjxtjfz

2

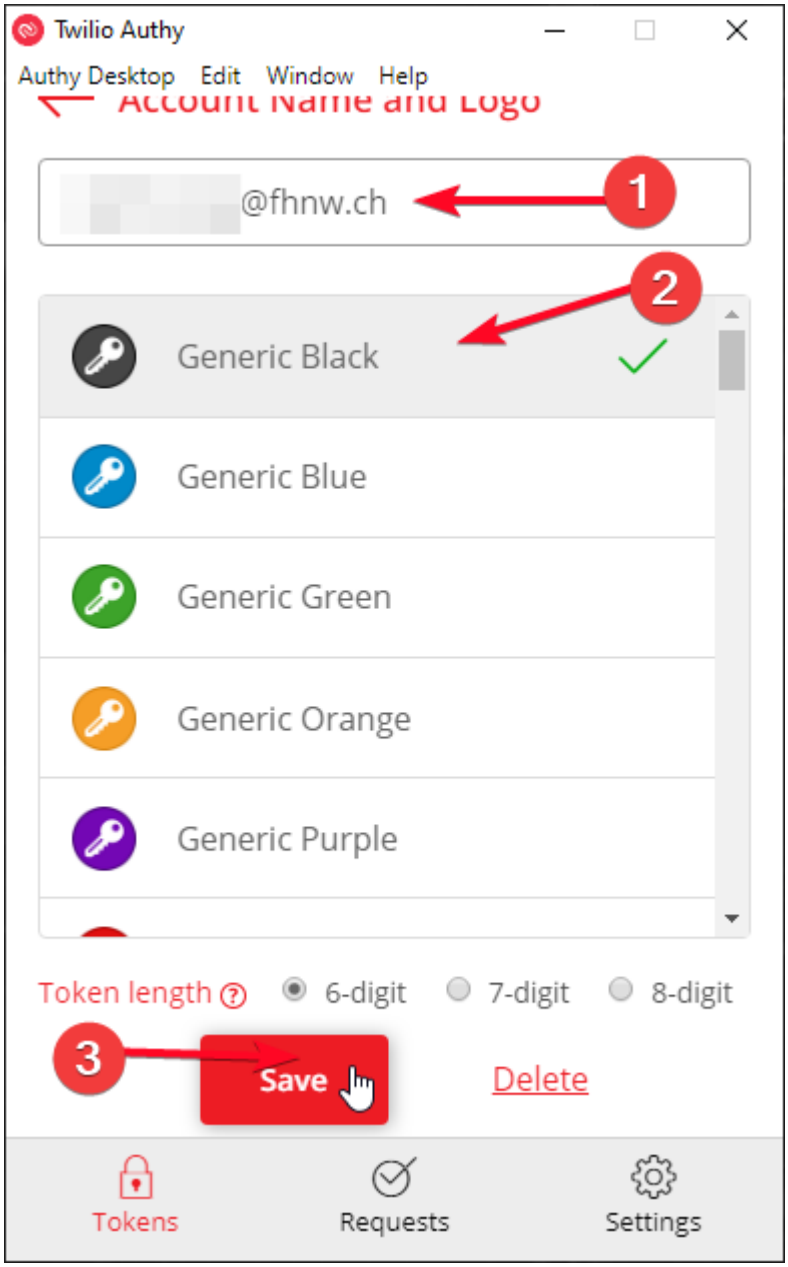
3

Back Next

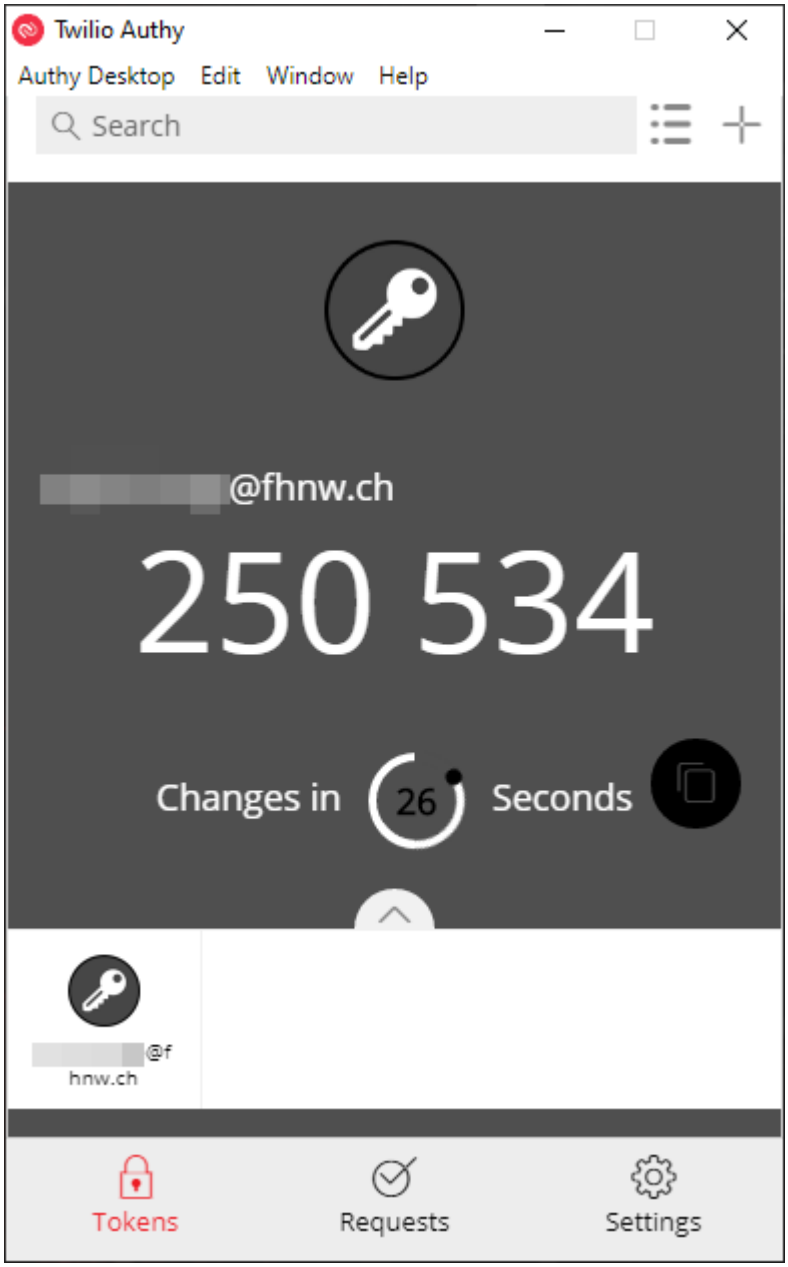
I want to set up a different method



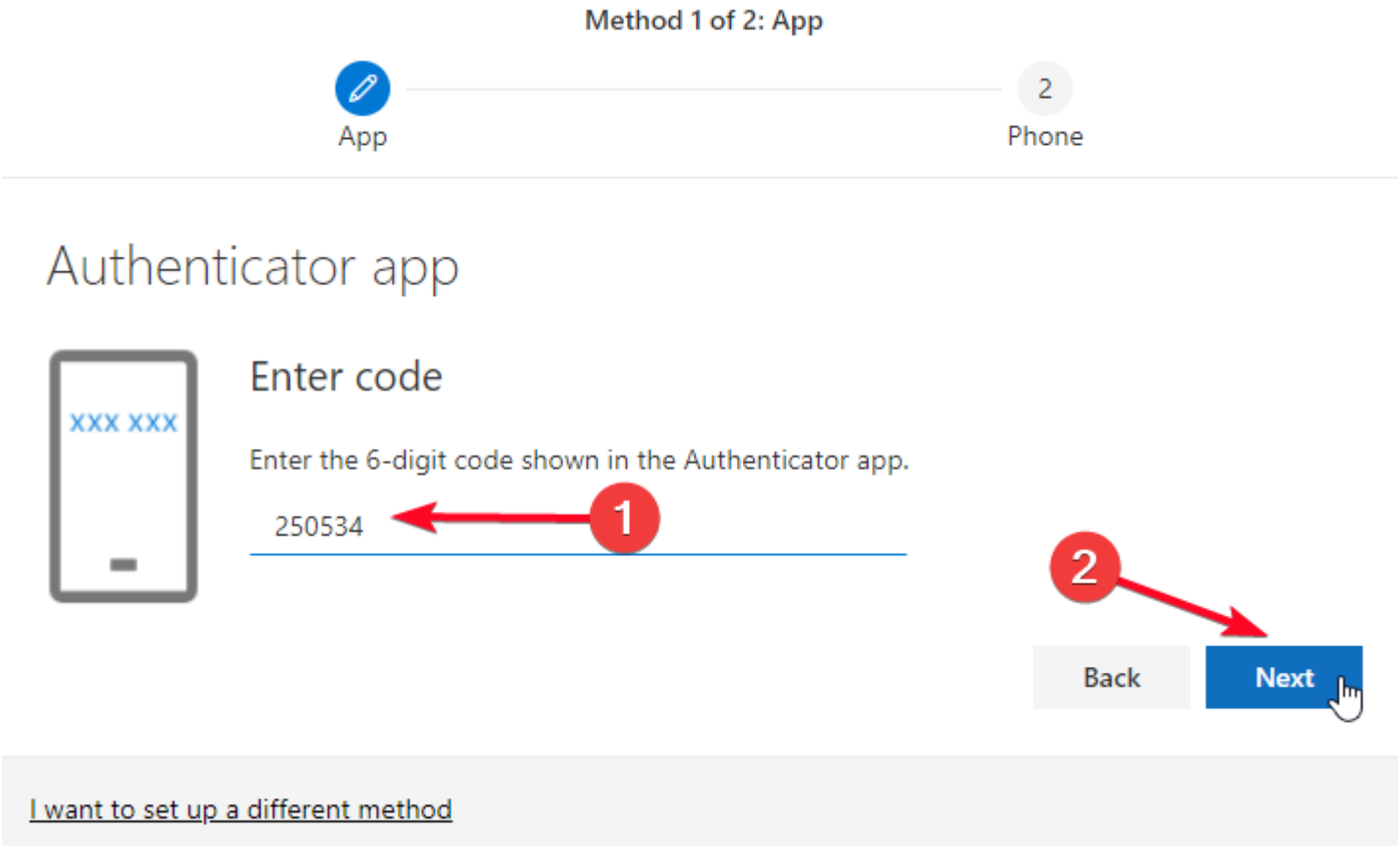
Vergeben Sie einen Name und ein Symbol für den Account - im Besipiel die Mailadresse als Name.
6-digit länge sollte die standard Einstellung sein, anschliessend noch ein klick auf Save.



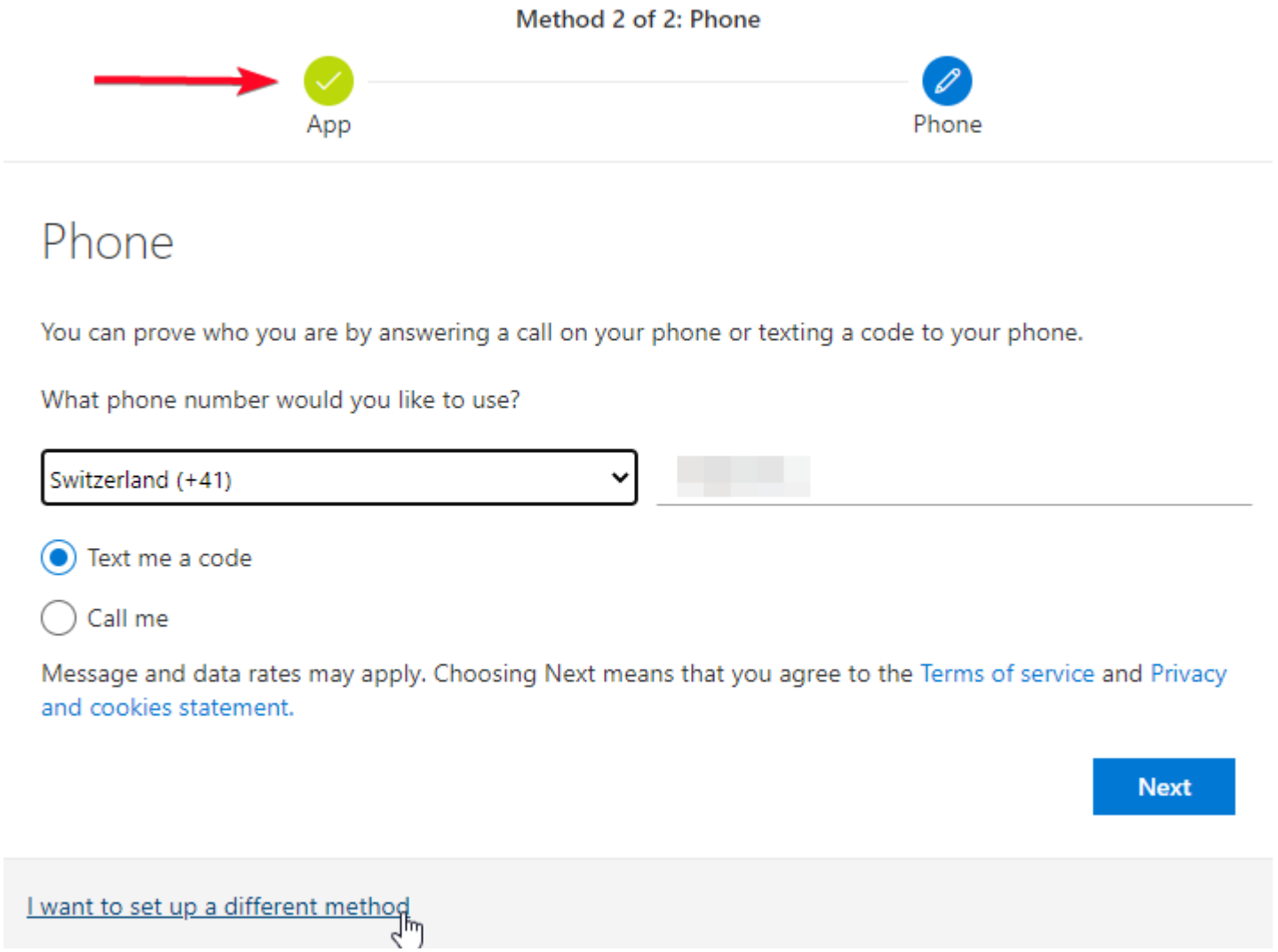
Nun generiert ihnen die App alle 30 Sekunden einen neuen 6-stelligen Code.
Diesen müssen Sie vor Ablauf in der MFA Registration hinterlegen.


Twilio Authy
Authy Desktop Edit Window Help
Search
@fhnw.ch
250 534
Changes in 26 Seconds
@f
hnw.ch
Tokens
Requests
Settings

Öffnen Sie nun wieder ihre Browsersitzung und die MFA Registration und tragen Sie den 6-stelligen Code ein.



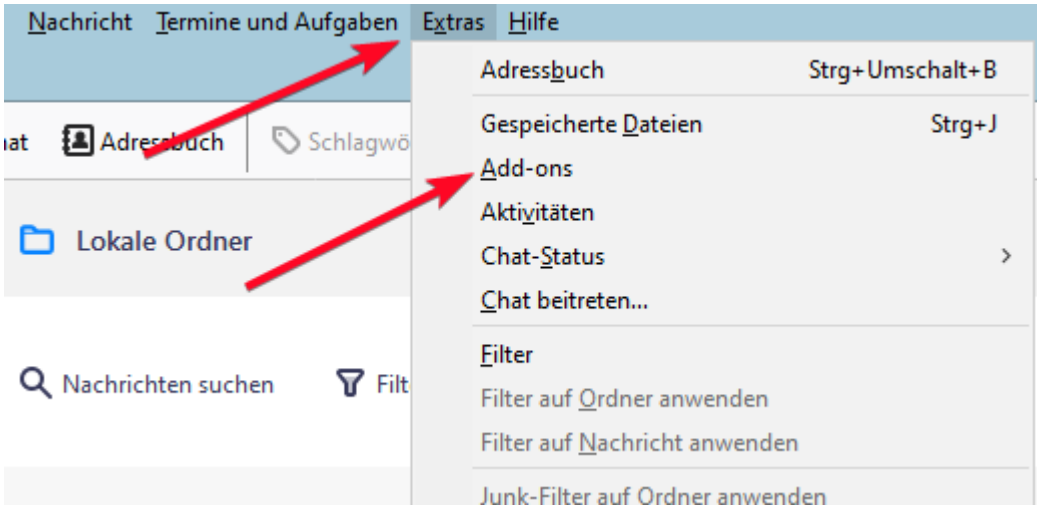
Nun ist die Registrierung einer alternativen App abgeschlossen.



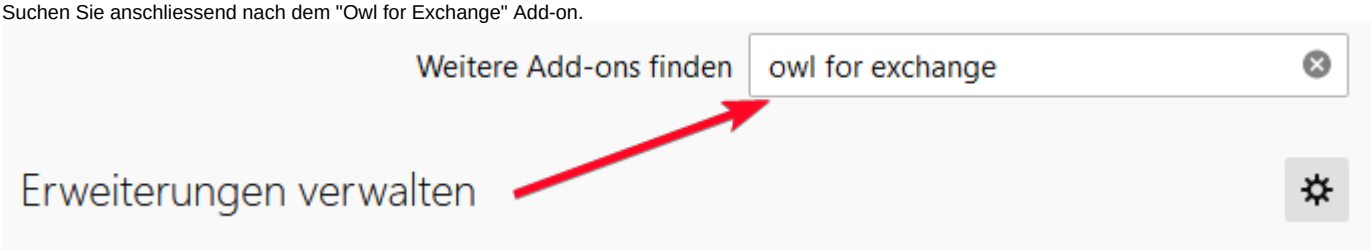
2. IMAP und SMTP wird nicht mehr unterstützt. Wie konfiguriere ich zukünftig mein Linux-System damit es Mails versenden und empfangen kann.

Es gibt für Linux die Möglichkeit den Thunderbird Mail Client zu nutzen, um ein Exchange Online Postfach zu nutzen. Dazu muss für Thunderbird das Addon "Owl for Exchange (Konstenpflichtig!)" installiert und eingerichtet werden.

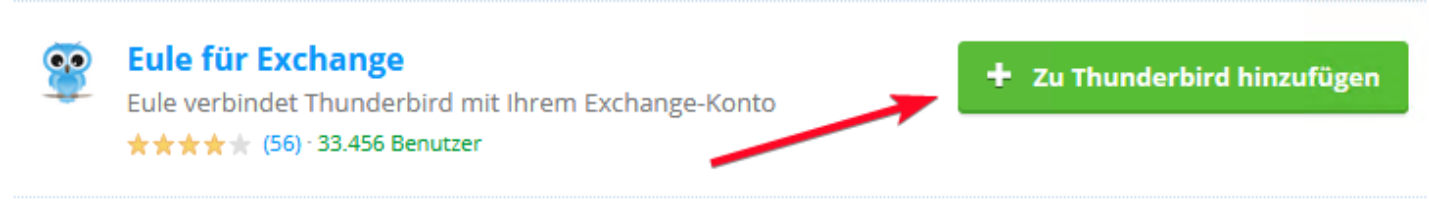
Öffnen Sie dazu Thunderbird und wählen Sie im Menü Extras den Punkt Add-ons.



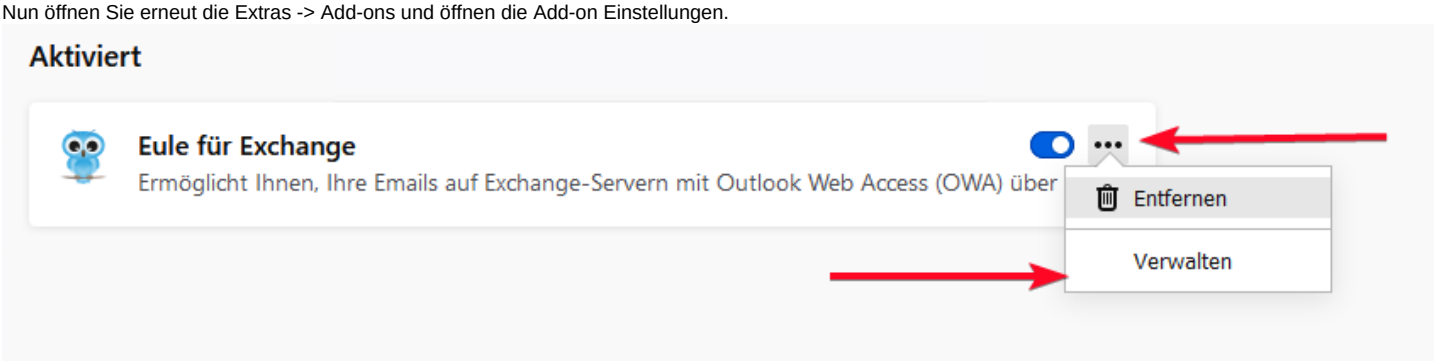
Suchen Sie anschliessend nach dem "Owl for Exchange" Add-on.



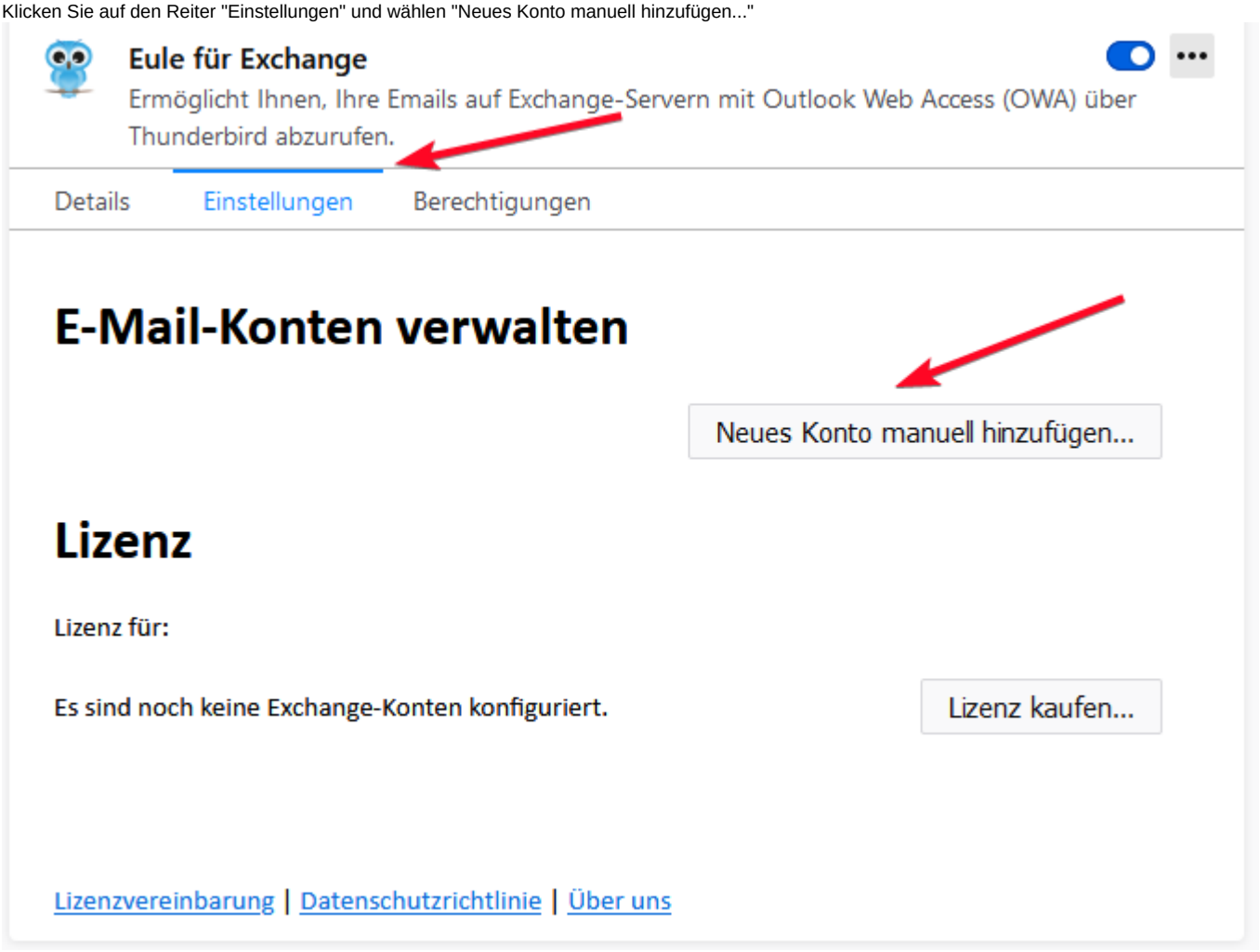
Klicken Sie auf hinzufügen um das Add-on zu installieren.



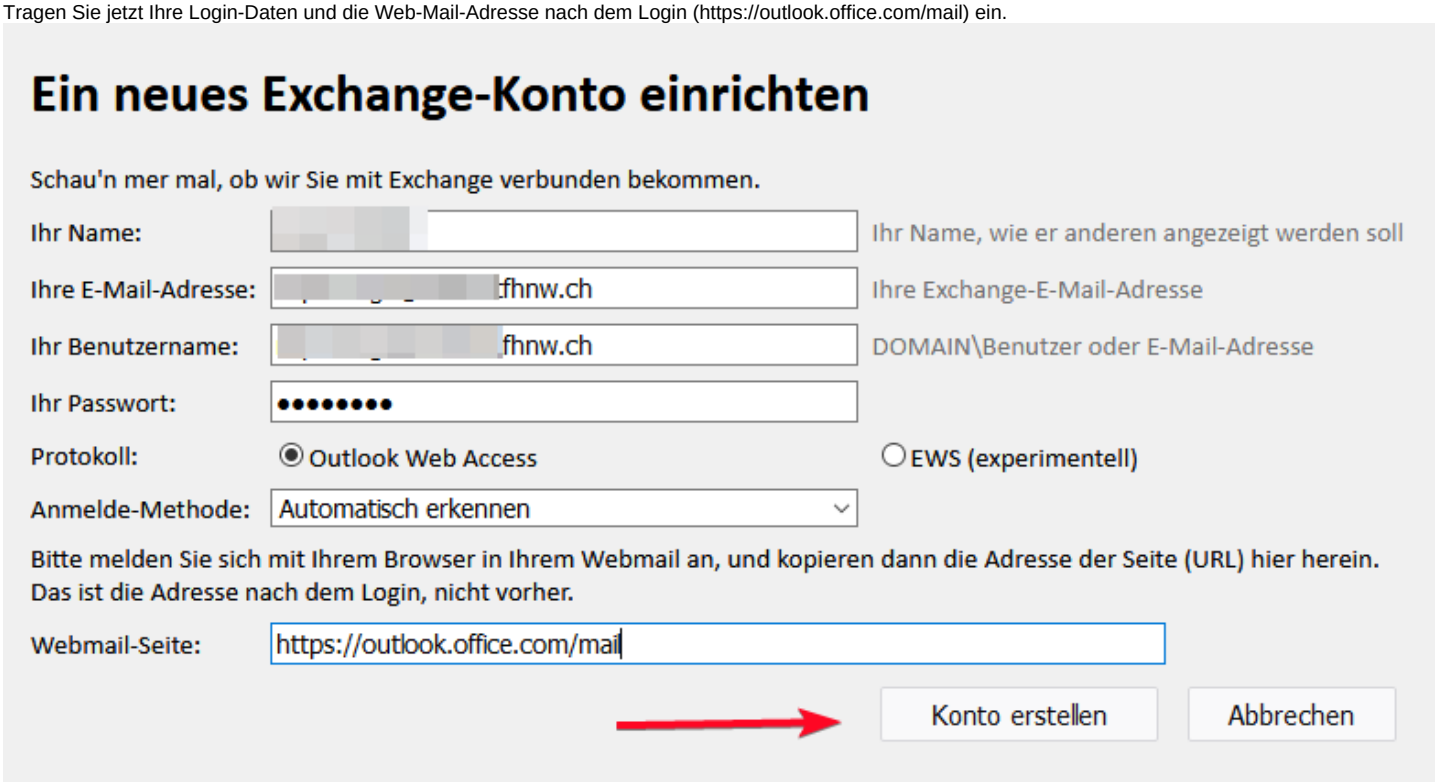
Nun öffnen Sie erneut die Extras -> Add-ons und öffnen die Add-on Einstellungen.



Klicken Sie auf den Reiter "Einstellungen" und wählen "Neues Konto manuell hinzufügen..."



Tragen Sie jetzt Ihre Login-Daten und die Web-Mail-Adresse nach dem Login (https://outlook.office.com/mail) ein.



Nachdem Sie das Konto erstellt haben, müssen Sie einige Zeit warten, bis da Konto vollständig synchronisiert wurde. Ausserdem wird nach der Synchronisation dringend ein Neustart der Thunderbird Applikation empfohlen.

3. Brauche ich für MFA zwingend ein Handy?

Nein. Es ist möglich als zweiten/dritten Faktor eine Mobilfunknummer hinzuzufügen um entweder einen Authentifizierungsanruf oder einen SMS-Code zu erhalten. Eine alternativ E-Mailadresse kann nur für den "Self Service Passwort Reset" verwendet werden. Es ist nicht möglich die alternativ E-Mailadresse für die MFA Anmeldung zu verwenden.

4. Ist auch im internen Netz der FHNW eine MFA notwendig

Aktuell ist das noch der Fall, allerdings werden die Policy's derzeit überarbeitet um die Anzahl der MFA-Aufforderungen so gering wie möglich zu halten.

5. Für welche Systeme benötige ich den zweiten Faktor

Für alle die eine Anmeldung an einer Microsoft O365 Applikation oder einem Online Dienst (z. B.: https://www.office.com/) benötigen.
Beispiele für Anwendungen sind: Outlook, Word, Excel, Powerpoint, OneNote, Visio, Microsoft Teams, ToDo, etc...

6. Wie oft muss ich mich mit MFA authentifizieren

Es gibt während der Anmeldung mit MFA die Möglichkeit ein Gerät als für einen Zeitraum von 90 Tagen zu speichern. Danach muss die MFA für das jeweilige Gerät erneut durchgeführt werden und kann anschliessend wieder gespeichert werden.

7. Warum wird die Umstellung auf MFA vollzogen. Das alte System hat gut funktioniert und war einfacher.

Aufgrund einer immer weiter steigenden Cyber-Kriminalität werden auch immer mehr Accounts gehackt und Daten missbraucht/gestohlen. Das liegt zu einem Grossteil an zu einfachen Passwörtern und nur einer Authentifizierung. Ein zweiter oder dritter Faktor ist natürlich ein kleiner Mehraufwand, dennoch unerlässlich um mehr Sicherheit gewährleisten zu können.

8. Kann ich weiterhin über https://webmail.fhnw.ch/ auf mein E-Mail Posftach zugreifen

Grundsätzlich Ja, da eine Weiterleitung auf die neue Web-Adresse eingerichtet ist. Wenn hierbei doch der Fehler Auftritt "Something went wrong" muss der Browser Cache gelöscht werden oder man benutzt direkt die neue Adresse: https://outlook.office.com/

9. Brauche ich MFA auch für die Anmeldung an meinem Windows / Apple Rechner der FHNW.

Nein, es betrifft nur die Anmeldung an O365 Anwendungen (wie unter Punkt 5. beschrieben).

Sonstiges:

Mit welcher Konfiguration arbeitet unser MFA System / Token?

- Algorithmus: SHA1 / SHA 256

- Digits: 6

- Intervall: 30

Diese Angaben können benötigt werden, wenn alternative MFA Apps (statt dem Microsoft Authenticator) verwendet werden wollen. (z.B. Open Source Clients)

Troubleshooting:

Authenticator App zeigt keine Push Notification:

> Schliessen Sie die App auf Ihrem Smartphone und testen Sie erneut. Sollte das schliessen der App nicht ausreichen, starten Sie ihr Smartphone neu und probieren nochmal.

<-- zu allen Artikeln rund um O365 / Azure AD

Verwandte Artikel

- SWITCH edu-ID, MFA Multi-Faktor-Authentifizierung - einrichten
- Helpsammlung MFA
- Welche elektronische Signatur für welches Dokument?
- Schritt für Schritt Anleitung mit Bildern für MFA (Azure Multi-Factor Authentification)
- 1) Elektronische Signatur an der FHNW

publiziert: 20. Mai 2020 11:02 Service: S1309 - IT Infrastruktur Basisdienste (AD | Entra ID | SCEP | Entra Application Proxy) Stichwörter: Anmeldung Office Security