Cisco Secure Client VPN mit Multifaktor-Authentifizierung

Publiziert net.services@fhnw.ch allgemeine Anleitung Corporate IT Doku

VPN MFA

Per 14.2.2022 wird für VPN Verbindungen eine sichere Multifaktor-Authentifizierung eingeführt. Dies führt zu höherer Sicherheit für die FHNW Infrastruktur. Es wird die bereits bekannte Authentifizierung von Microsoft verwendet, damit die UserInnen nicht einen weiteren MFA Registrierungsprozess durchlaufen müssen.

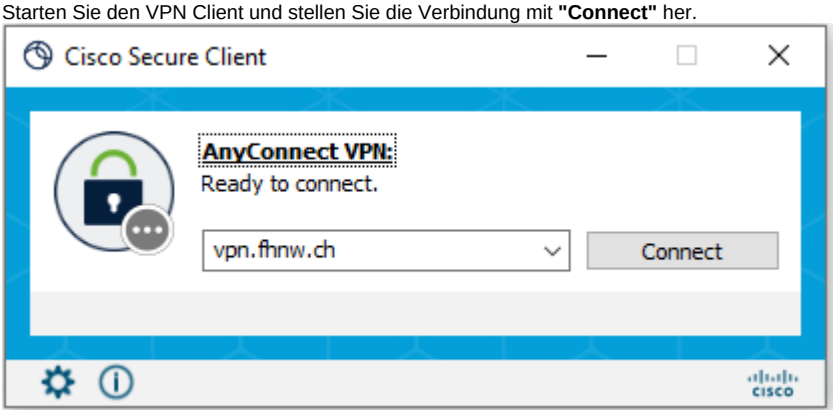
Download Cisco Secure Client (Win / MAC) vpn.fhnw.ch

Download Cisco Secure Client (ARM-Prozessoren)
Sollten Sie ein Gerät mit einem ARM-Prozessor verwenden (z. B. ein Microsoft Surface), müssen Sie den Cisco Secure Client für ARM herunterladen. Diesen finden Sie hier: https://web.fhnw.ch/ict/softwaredownload/liste.php?&pf=Windows

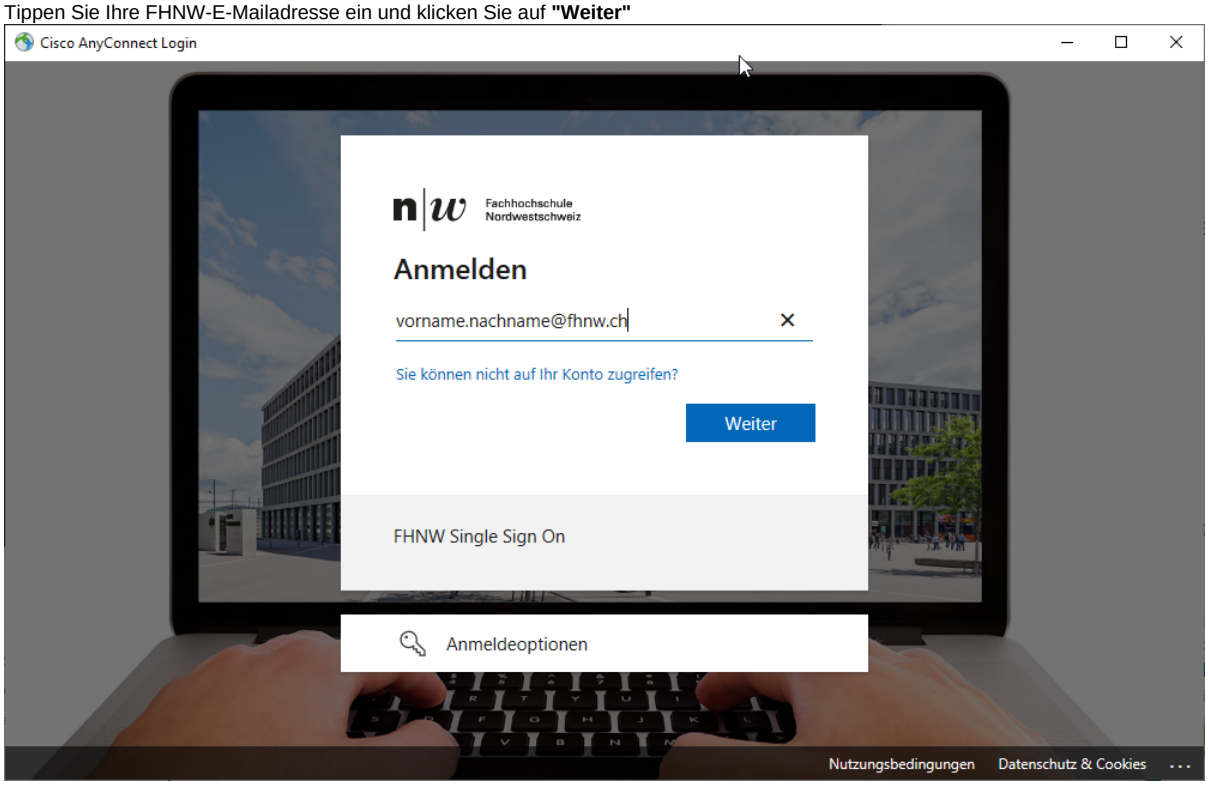
Windows

VPN Anmeldung mit MFA unter Windows

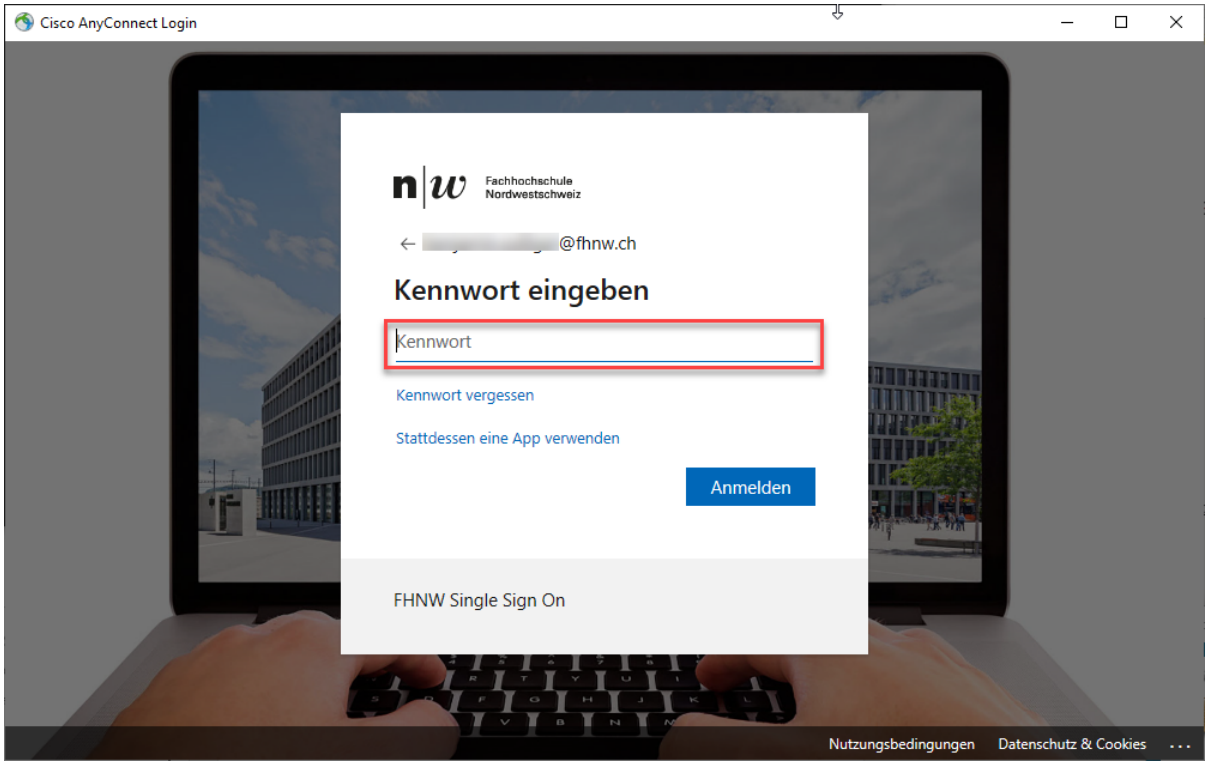
1. Starten Sie den VPN Client und stellen Sie die Verbindung mit **"Connect"** her.



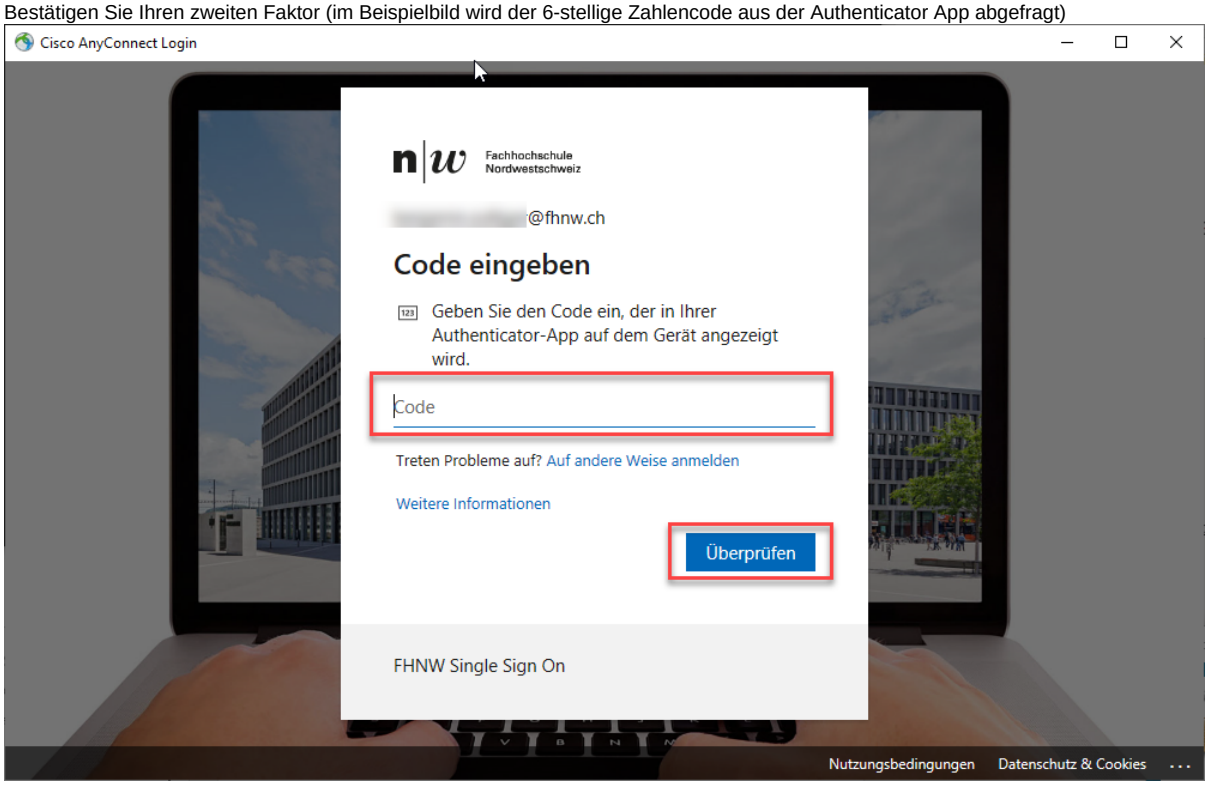
2. Tippen Sie Ihre FHNW-E-Mailadresse ein und klicken Sie auf **"Weiter"**



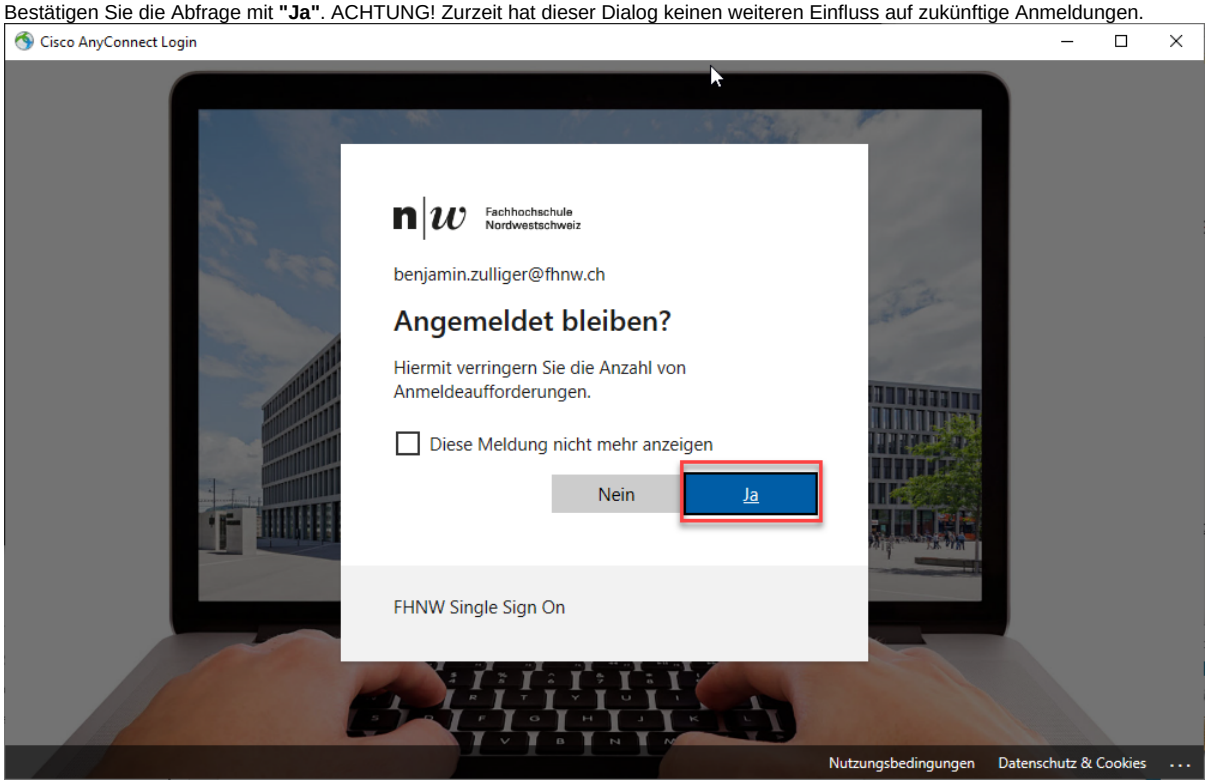
3. Geben Sie als ersten Faktor Ihr FHNW-Passwort ein und klicken Sie anschliessend auf **"Anmelden"**



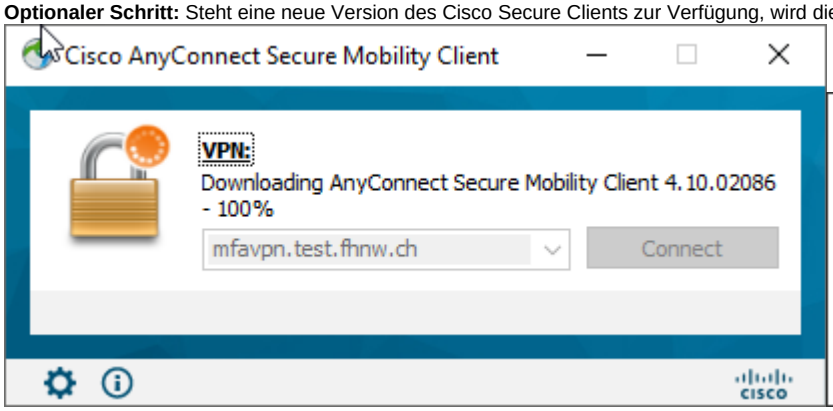
4. Bestätigen Sie Ihren zweiten Faktor (im Beispielbild wird der 6-stellige Zahlencode aus der Authenticator App abgefragt)

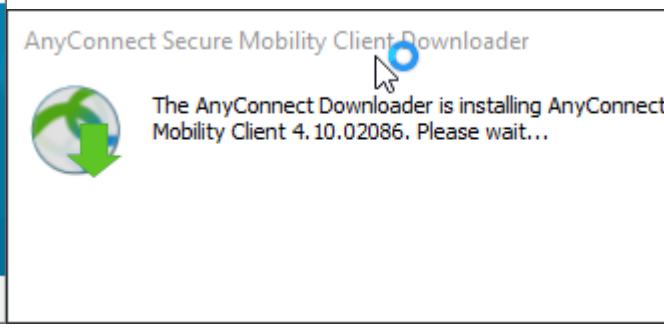


5. Bestätigen Sie die Abfrage mit **"Ja"**. ACHTUNG! Zurzeit hat dieser Dialog keinen weiteren Einfluss auf zukünftige Anmeldungen.

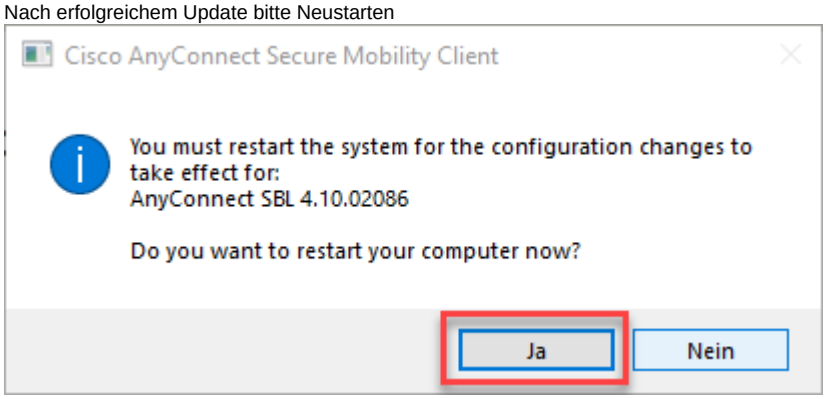


6. **Optionaler Schritt:** Steht eine neue Version des Cisco Secure Clients zur Verfügung, wird dieser während der Anmeldung aktualisiert.

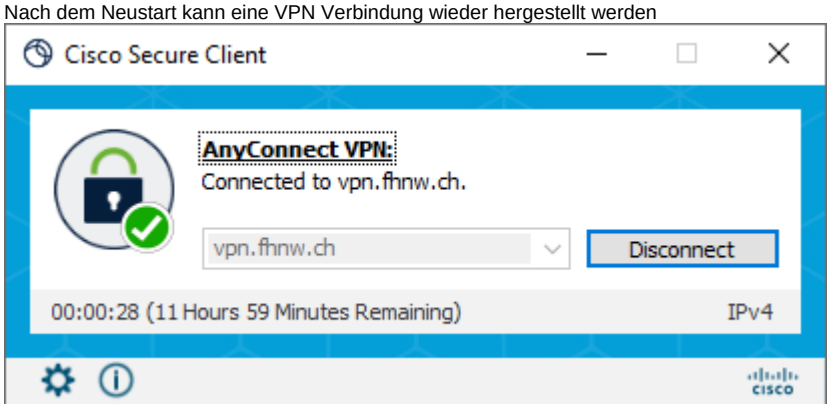




7. Nach erfolgreichem Update bitte Neustarten



8. Nach dem Neustart kann eine VPN Verbindung wieder hergestellt werden



Windows bekannte Probleme

Fehler bei der Suche nach Ihrem Konto

Grund: Der Fehler tritt nur bei nicht FHNW Geräten auf und auch nur dann, wenn das Gerät mit einem anderen Azure Active Directory als der FHNW verbunden ist.

Fehlermeldung: Fehler bei der Suche nach Ihrem Konto. Tippen Sie auf "Weiter", um es noch mal zu versuchen.

Vorgehen: Registrieren Sie das FHNW Konto als Arbeits- und Schulkonto in den Einstellungen --> Konten --> "Auf Arbeits- oder Schulkonto zugreifen" --> Verbinden wählen.

Anmeldung nimmt immer ein falsches Konto

Grund: Cisco Secure Client ist so konfiguriert dass er die bestehende Azure Anmeldung verwendet. Bei nicht FHNW Geräten kann es sein dass er den falschen Account nimmt und man gar keine Möglichkeit hat dies zu ändern.

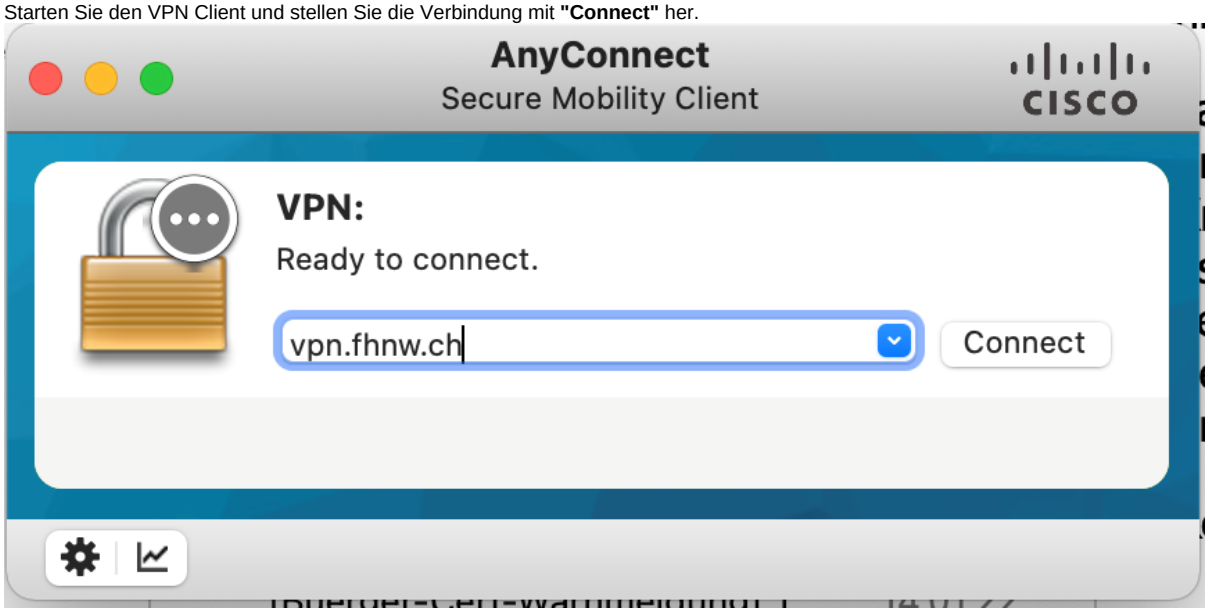
Fehlermeldung:

Vorgehen: Registrieren Sie das FHNW Konto als Arbeits- und Schulkonto in den Einstellungen --> Konten --> "Auf Arbeits- oder Schulkonto zugreifen" --> Verbinden wählen. Gleiches Vorgehen wie oben.

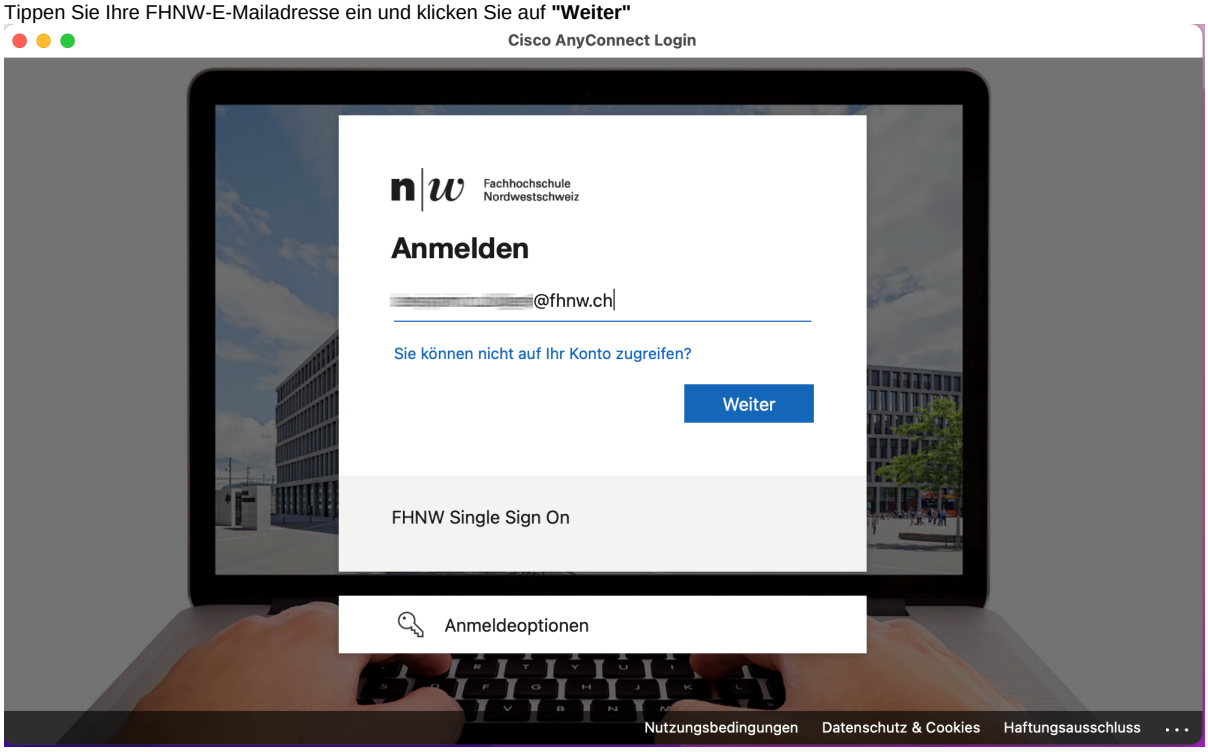
macOS

VPN Anmeldung mit MFA unter macOS

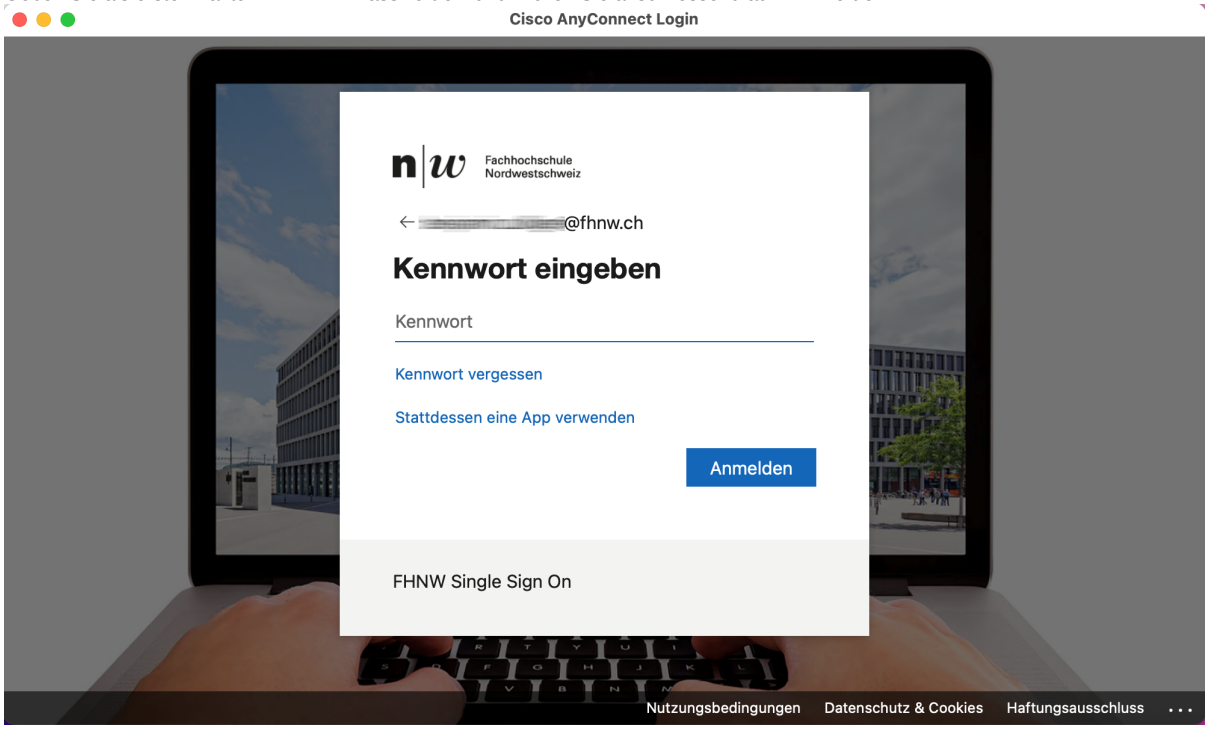
1. Starten Sie den VPN Client und stellen Sie die Verbindung mit **"Connect"** her.



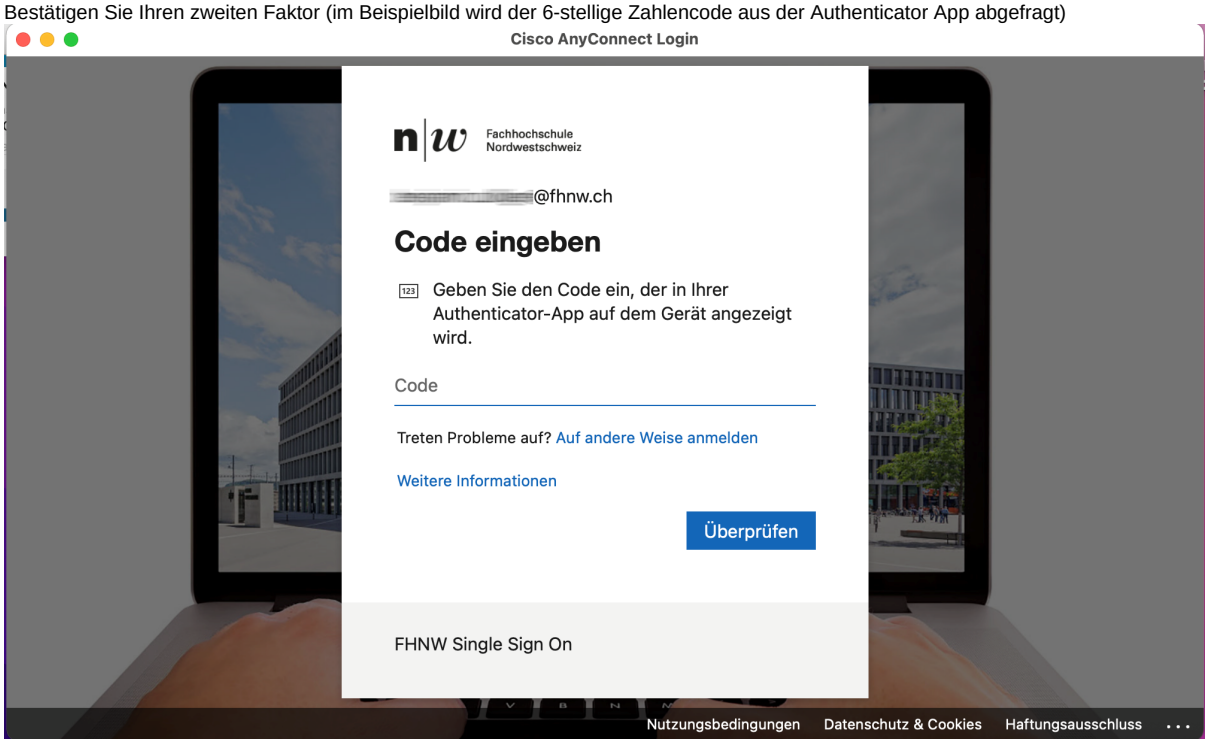
2. Tippen Sie Ihre FHNW-E-Mailadresse ein und klicken Sie auf **"Weiter"**



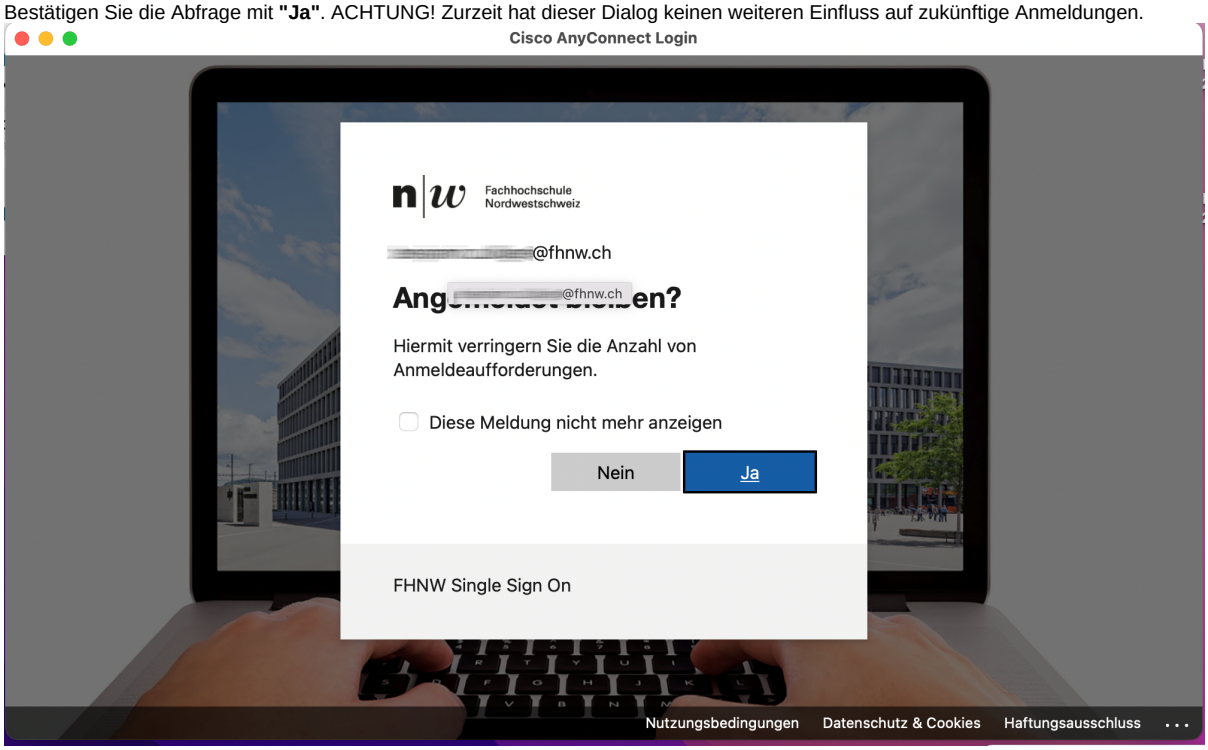
3. Geben Sie als ersten Faktor Ihr FHNW-Passwort ein und klicken Sie anschliessend auf **"Anmelden"**



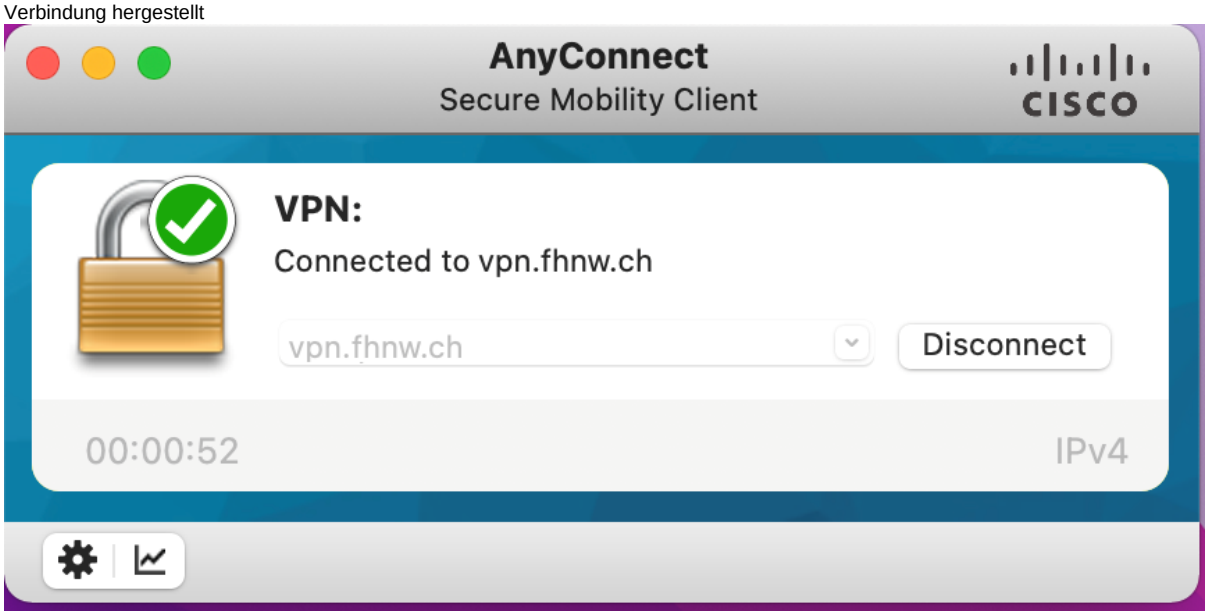
4. Bestätigen Sie Ihren zweiten Faktor (im Beispielbild wird der 6-stellige Zahlencode aus der Authenticator App abgefragt)



5. Bestätigen Sie die Abfrage mit **"Ja"**. ACHTUNG! Zurzeit hat dieser Dialog keinen weiteren Einfluss auf zukünftige Anmeldungen.



6. Verbindung hergestellt

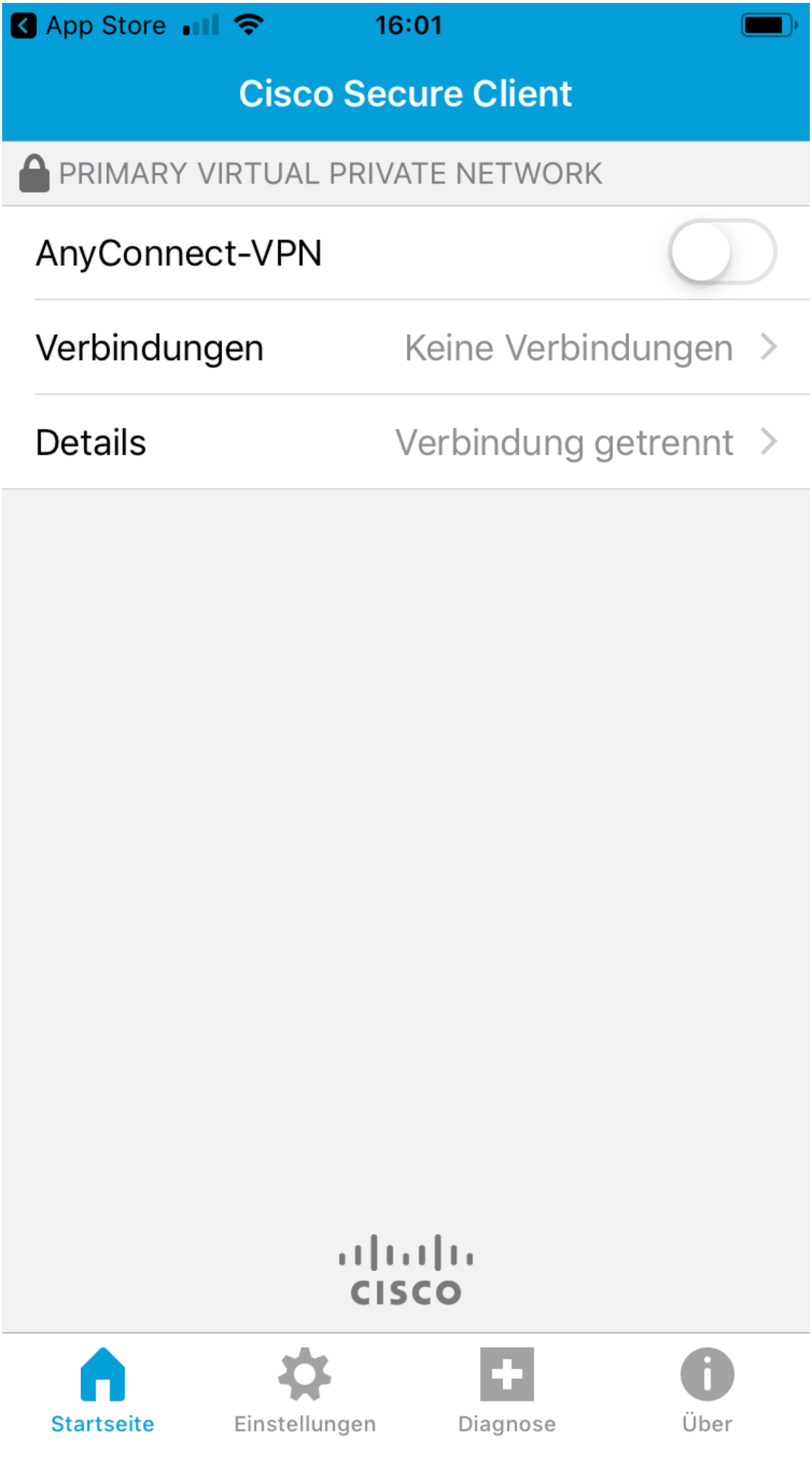


iOS

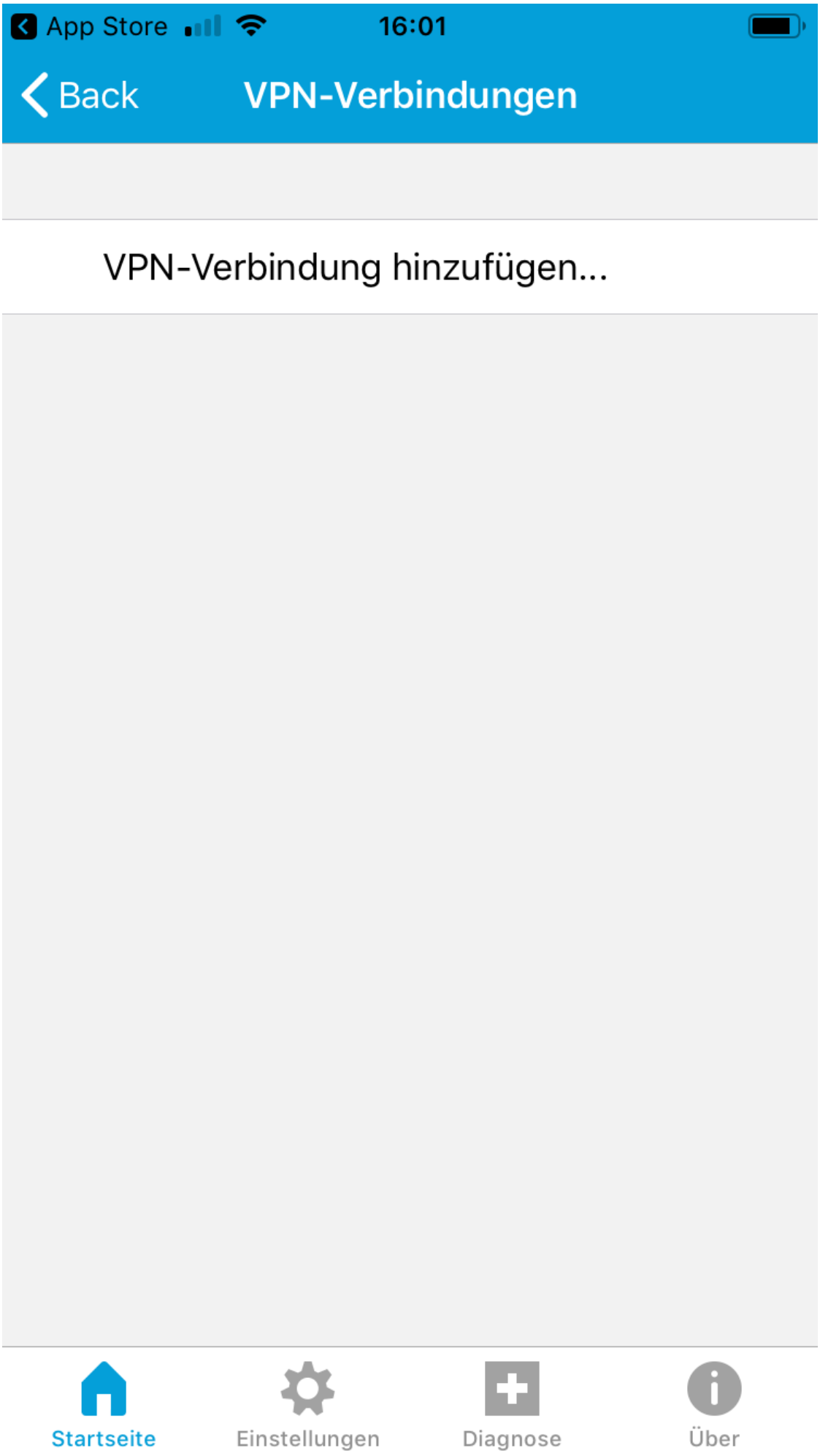
VPN Anmeldung mit MFA unter iOS

Um den Cisco AnyConnect Client auf einem iPhone oder iPad zu nutzen, muss zuerst die App aus dem Apple App Store heruntergeladen werden.
https://apps.apple.com/de/app/cisco-anyconnect/id1135064690

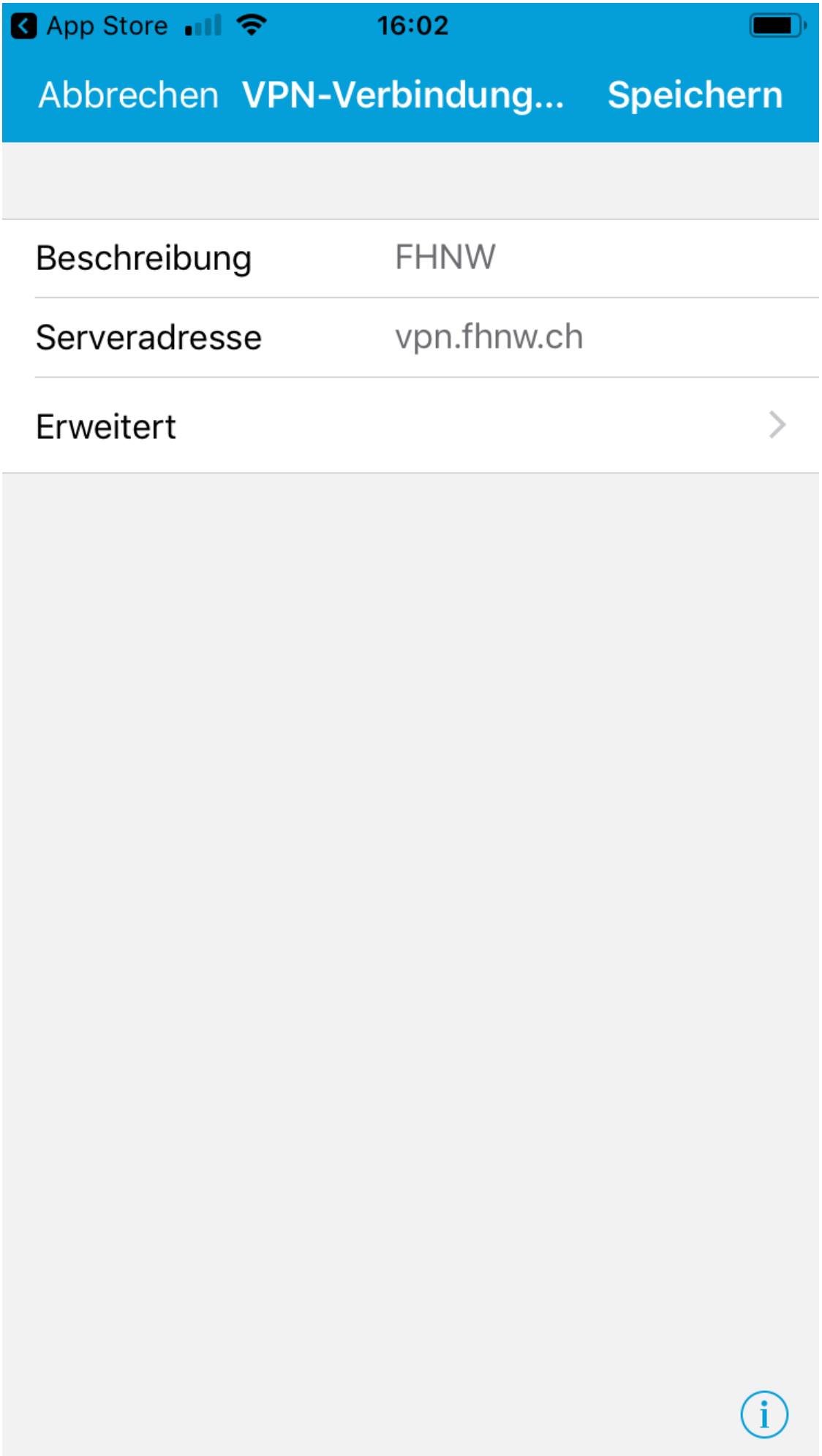
1. Starten Sie die App.


App Store
16:01
Cisco Secure Client
PRIMARY VIRTUAL PRIVATE NETWORK
AnyConnect-VPN
Verbindungen
Keine Verbindungen
Details
Verbindung getrennt
cisco
Startseite
Einstellungen
Diagnose
Über

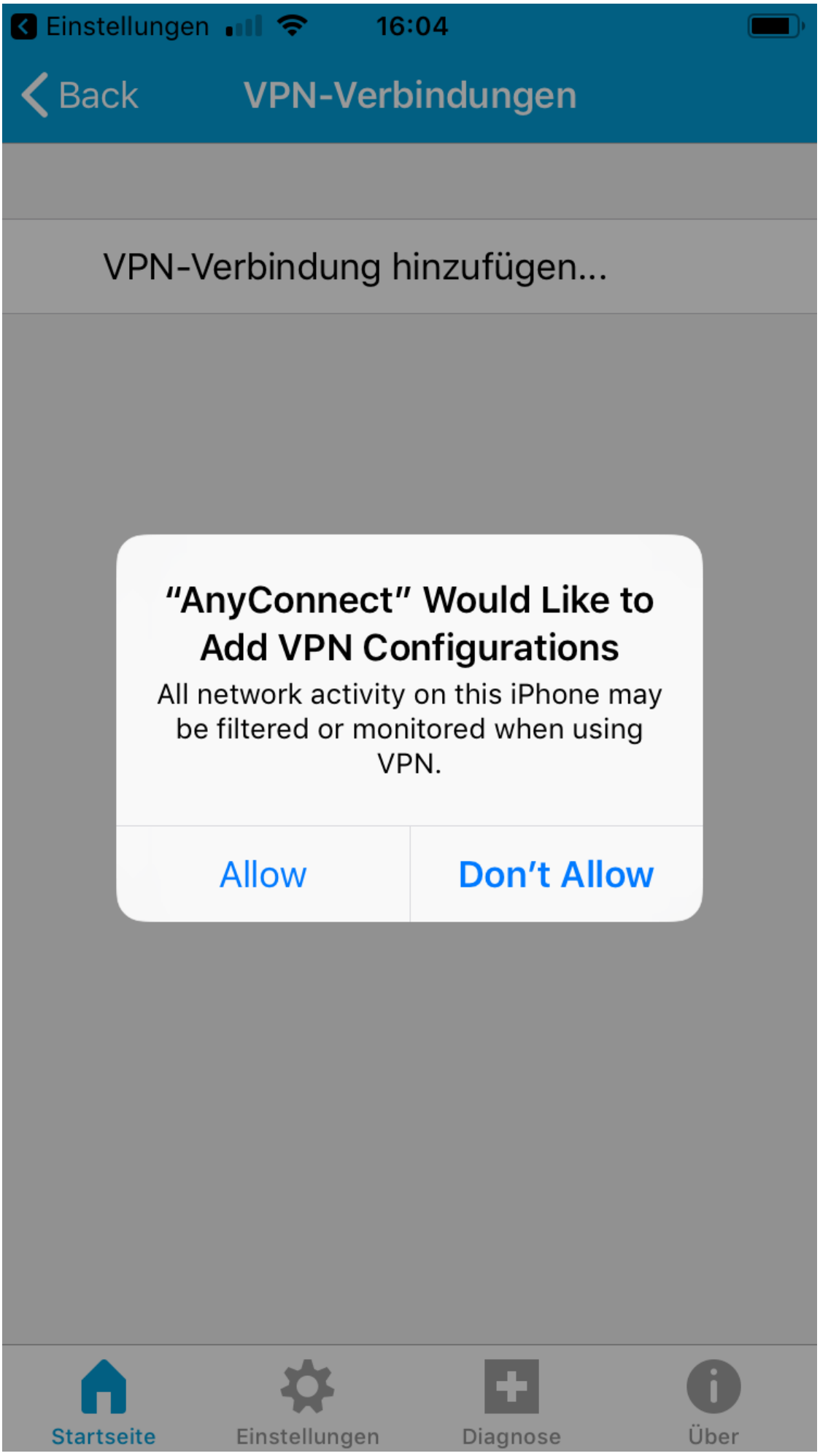
2. Klicken Sie auf Keine Verbindungen, um eine neue Verbindung hinzufügen.



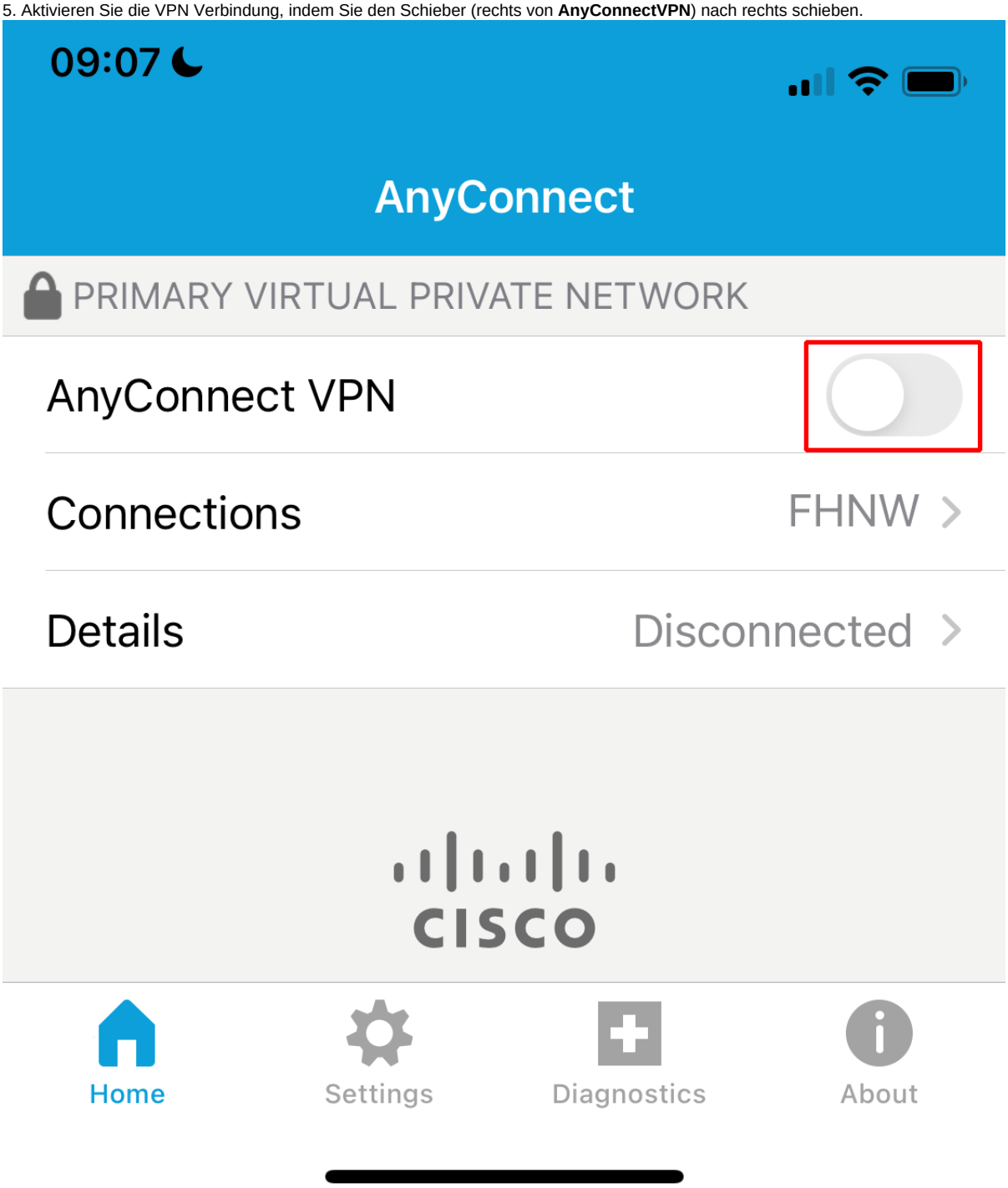
3. Tippen Sie Beschreibung und Serveradresse und klicken Sie auf Speichern.


App Store
16:02
Abbrechen
VPN-Verbindung...
Speichern
Beschreibung
FHNW
Serveradresse
vpn.fhnw.ch
Erweitert

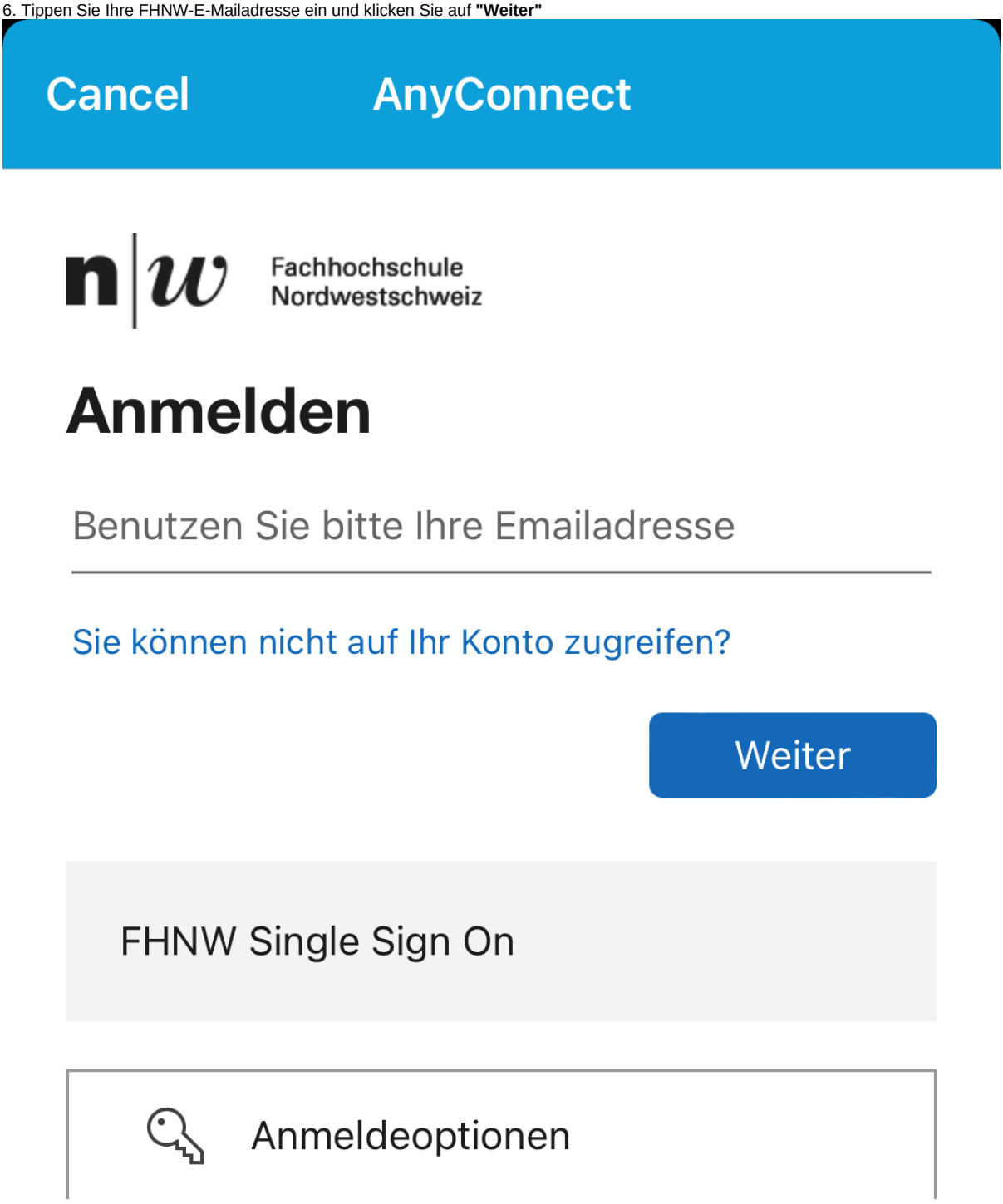
4. Klicken Sie auf Allow



5. Aktivieren Sie die VPN Verbindung, indem Sie den Schieber (rechts von **AnyConnectVPN**) nach rechts schieben.

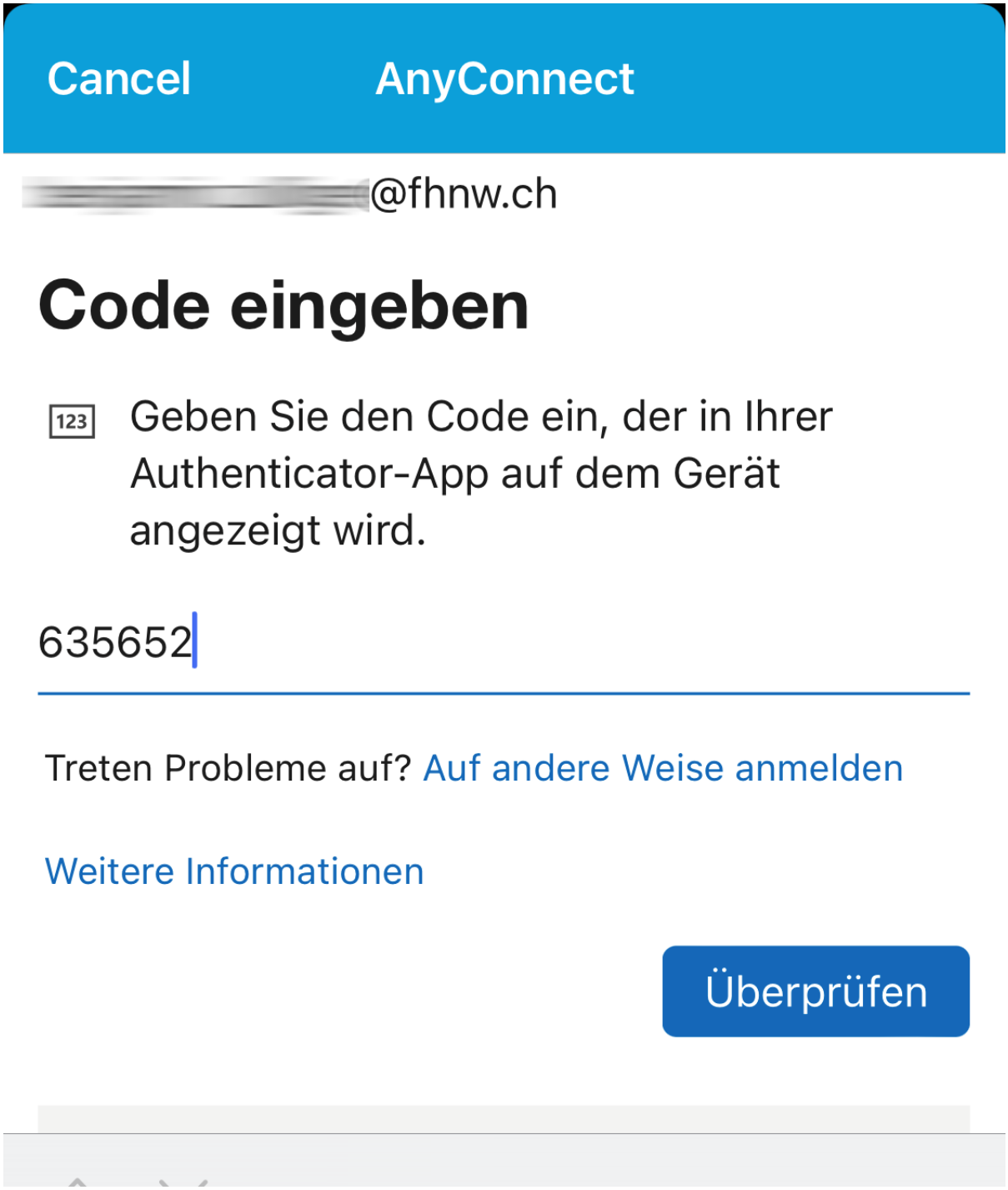


6. Tippen Sie Ihre FHNW-E-Mailadresse ein und klicken Sie auf **"Weiter"**

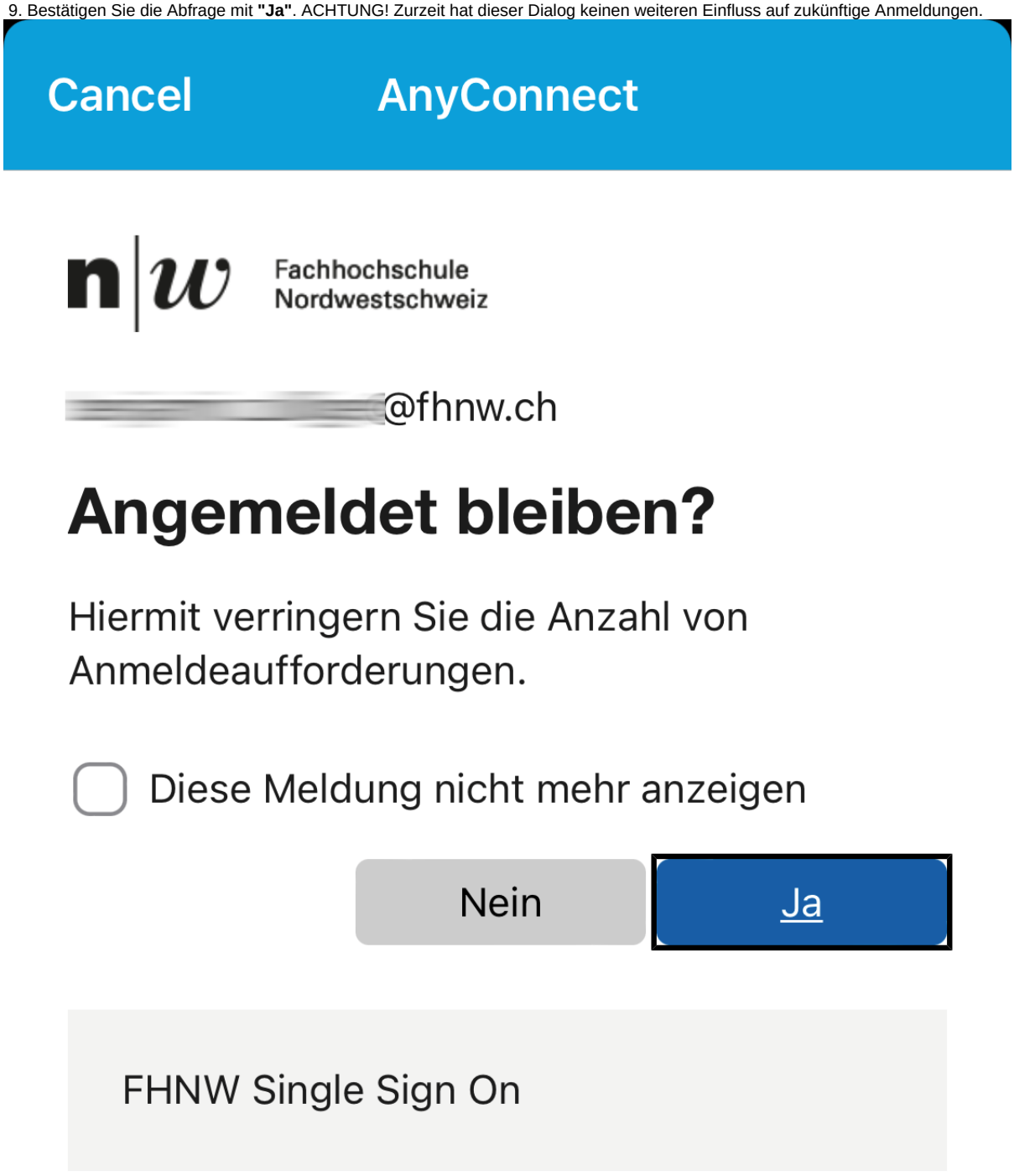


7. Geben Sie als ersten Faktor Ihr FHNW-Passwort ein und klicken Sie anschliessend auf **"Anmelden"**

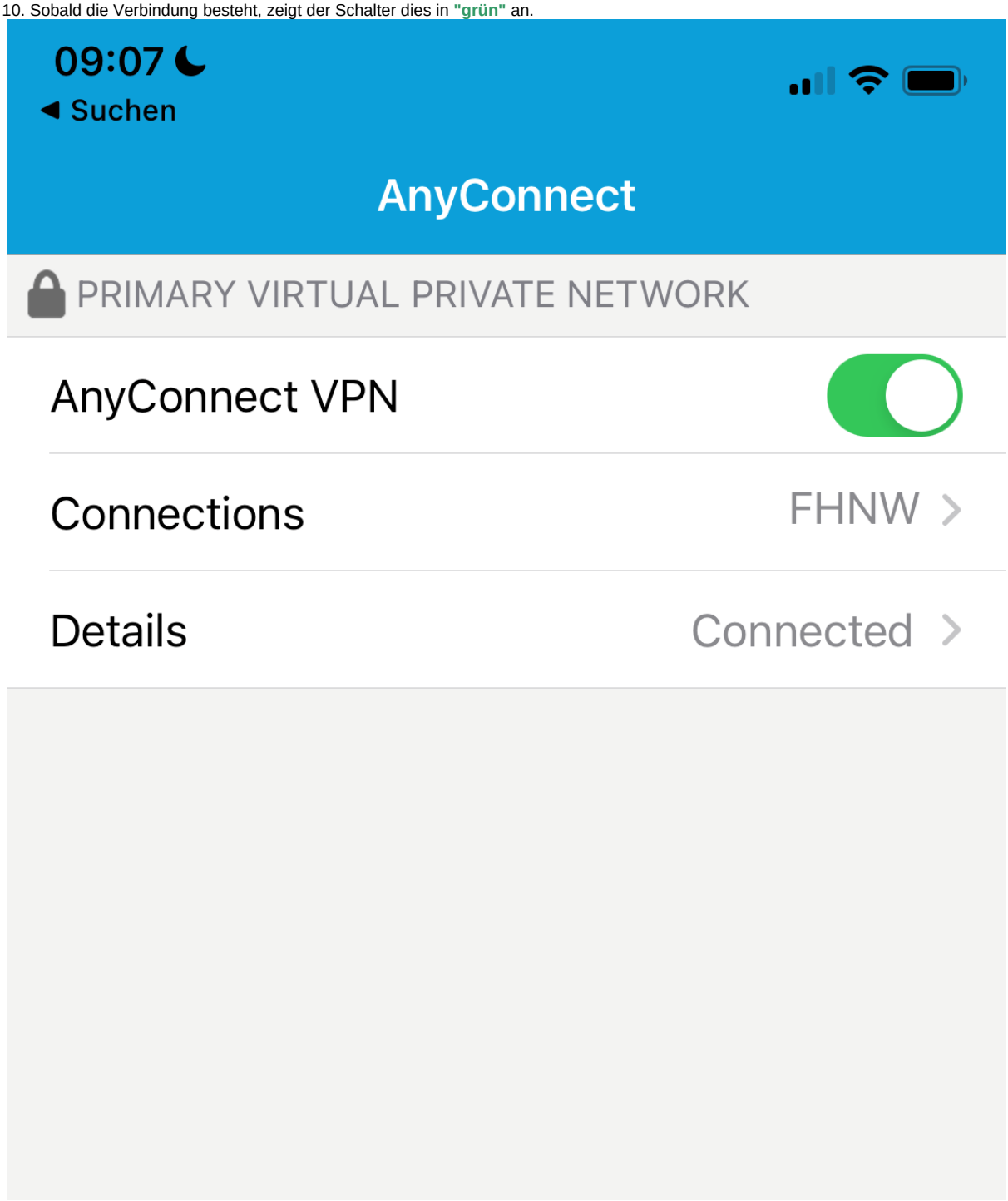
8. Wechseln Sie zur Authenticator App und kopieren Sie den Authenticator Code. Fügen Sie diesen in diesem Fenster ein oder kopieren Sie den Zahlencode aus der SMS oder bestätigen Sie die Anmeldung in Ihrer Authenticator App.


Cancel
AnyConnect
[redacted]@fhnw.ch
Code eingeben
123
Geben Sie den Code ein, der in Ihrer Authenticator-App auf dem Gerät angezeigt wird.
635652
Treten Probleme auf? Auf andere Weise anmelden
Weitere Informationen
Überprüfen

9. Bestätigen Sie die Abfrage mit **"Ja"**. ACHTUNG! Zurzeit hat dieser Dialog keinen weiteren Einfluss auf zukünftige Anmeldungen.



10. Sobald die Verbindung besteht, zeigt der Schalter dies in **"grün"** an.

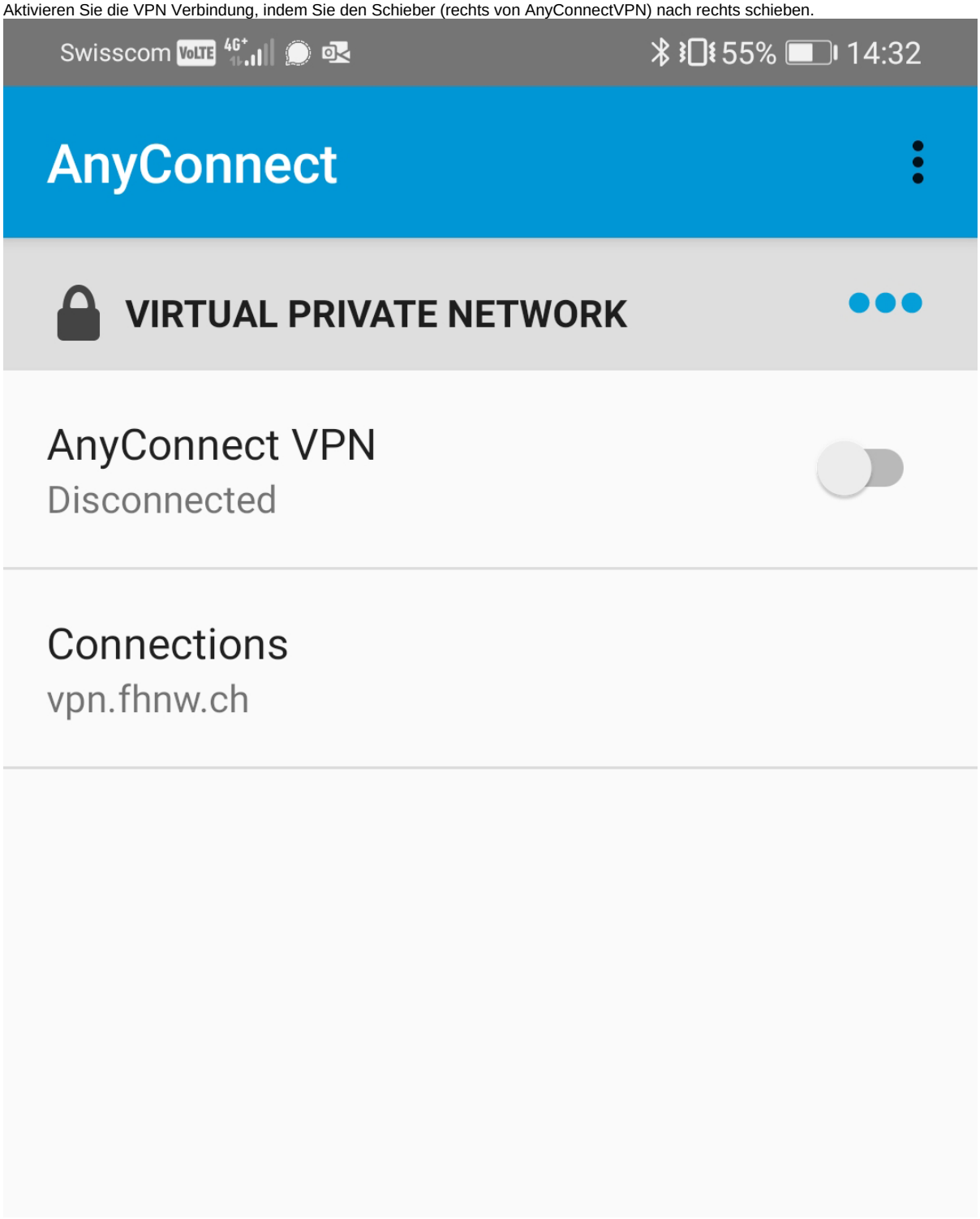


Android

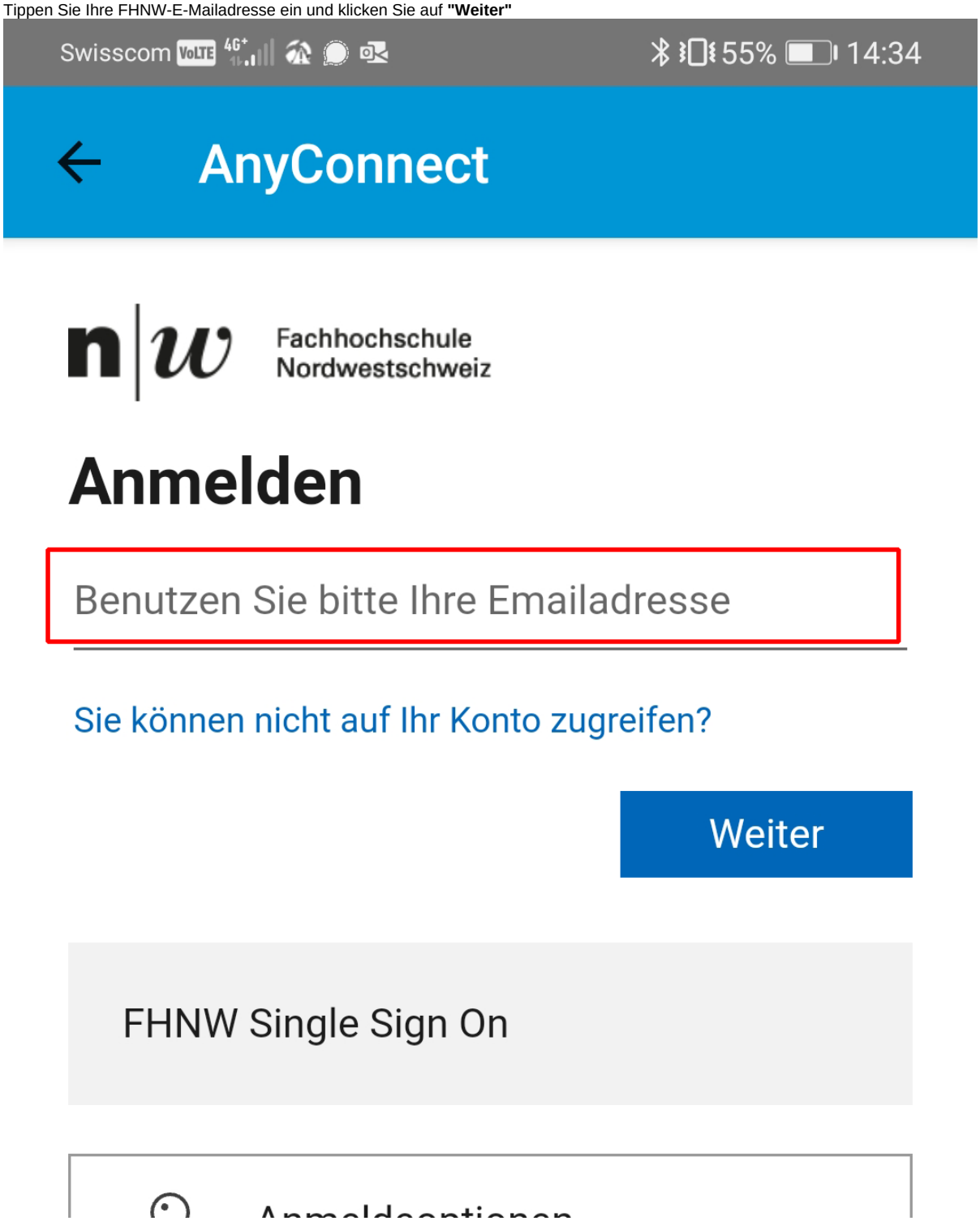
VPN Anmeldung mit MFA unter Android

Um den Cisco AnyConnect Client auf einem Android Smartphone oder Tablet zu nutzen, muss zuerst die App aus dem App Store heruntergeladen werden. https://play.google.com/store/apps/details?id=com.cisco.anyconnect.vpn.android.avf Bitte verwenden Sie keine alternativen App Stores, da in diesen oftmals Malware verteilt wird.

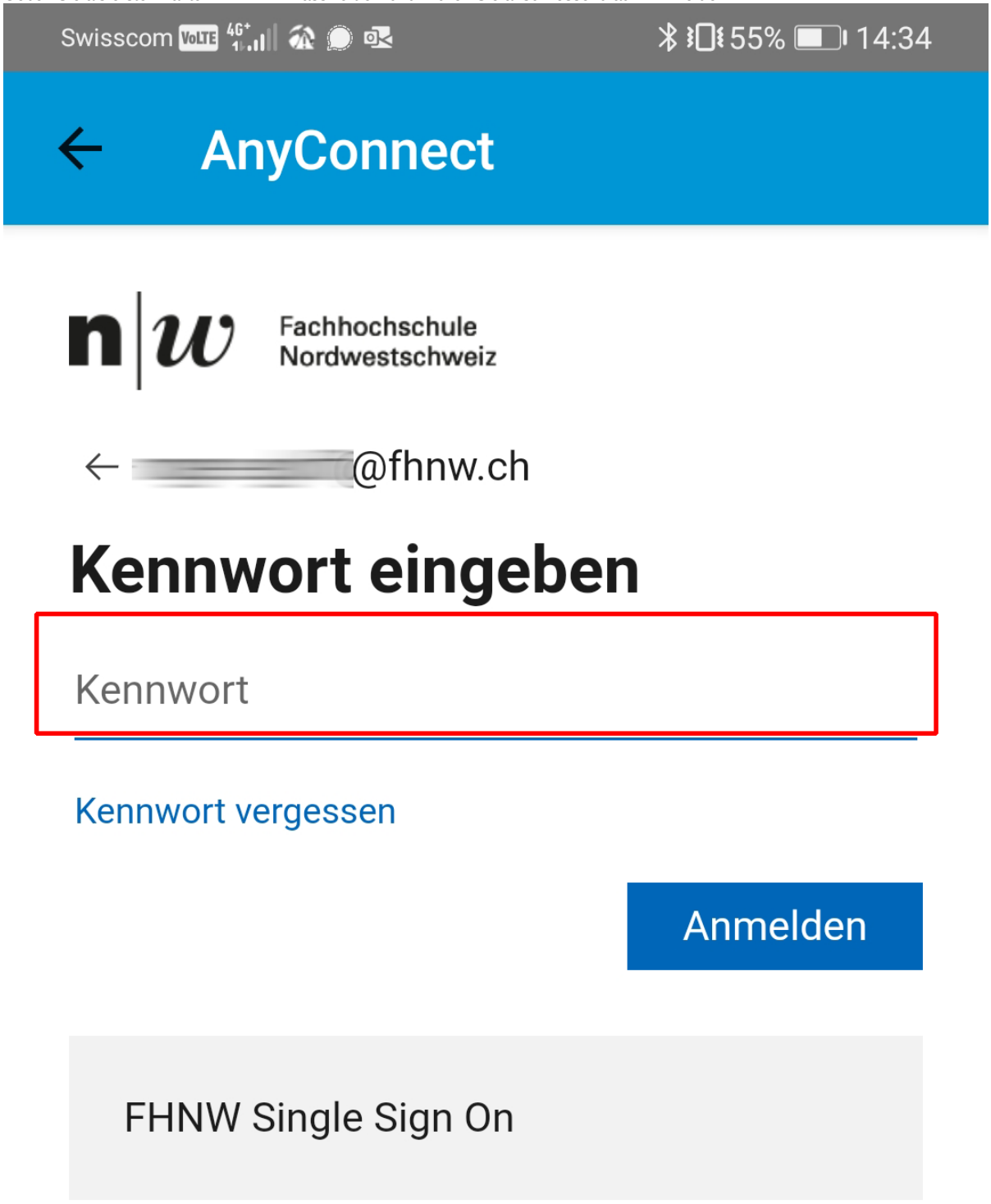
1. Aktivieren Sie die VPN Verbindung, indem Sie den Schieber (rechts von AnyConnectVPN) nach rechts schieben.



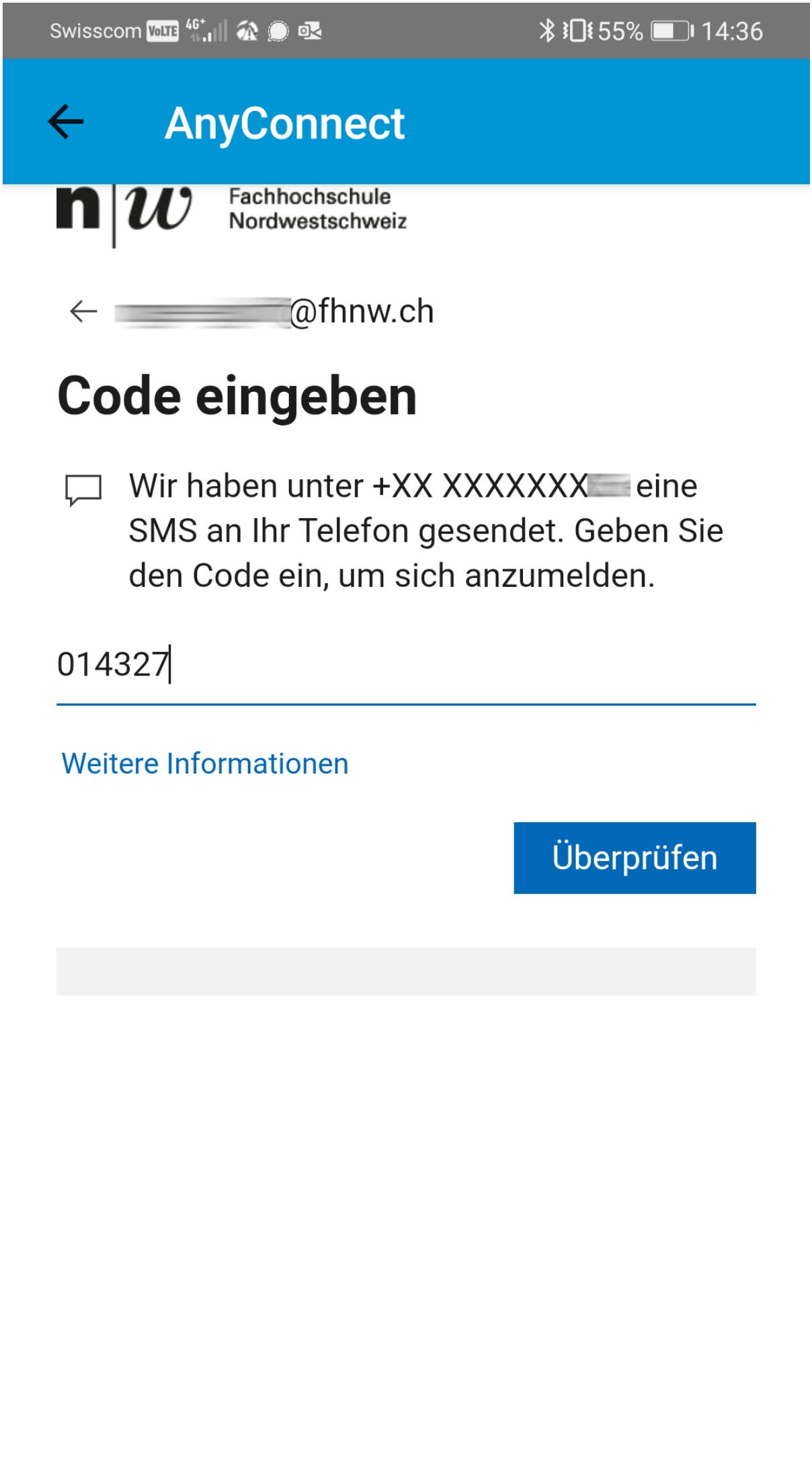
2. Tippen Sie Ihre FHNW-E-Mailadresse ein und klicken Sie auf **"Weiter"**



3. Geben Sie als ersten Faktor Ihr FHNW-Passwort ein und klicken Sie anschliessend auf **"Anmelden"**



4. Wechseln Sie zur Authenticator App und kopieren Sie den Authenticator Code. Fügen Sie diesen in diesem Fenster ein oder kopieren Sie den Zahlencode aus der SMS oder bestätigen Sie die Anmeldung in Ihrer Authenticator App.


Swisscom
55%
14:36
AnyConnect
Fachhochschule
Nordwestschweiz
[redacted]@fhnw.ch
Code eingeben
Wir haben unter +XX XXXXXXX[redacted] eine SMS an Ihr Telefon gesendet. Geben Sie den Code ein, um sich anzumelden.
014327
Weitere Informationen
Überprüfen

[redacted]@fhnw.ch

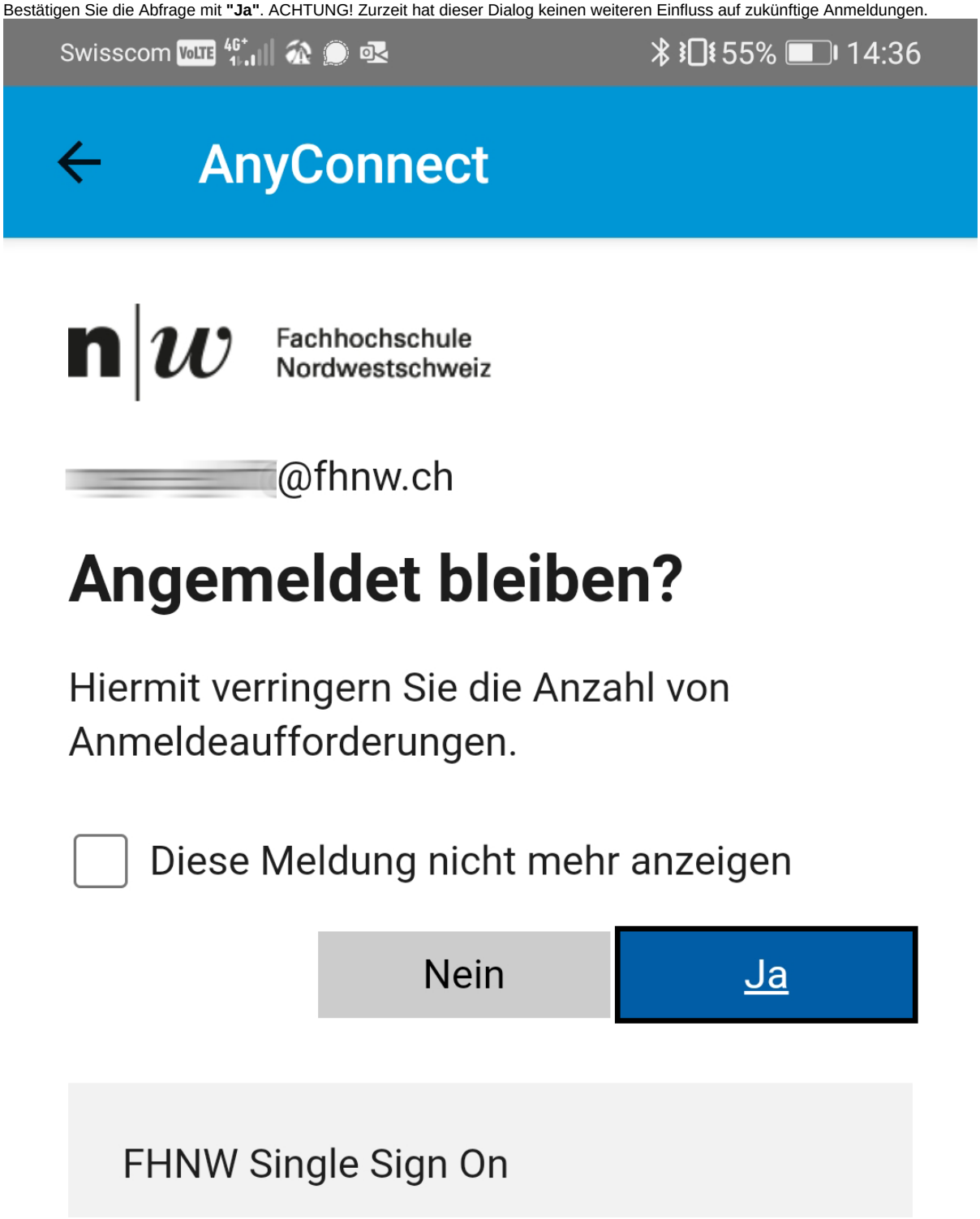
Anmeldeanforderung bestätigen

Öffnen Sie Ihre Microsoft Authenticator-App, und genehmigen Sie die Anmeldeanforderung.

Ich kann meine Microsoft Authenticator-App im Moment nicht verwenden.

Weitere Informationen

5. Bestätigen Sie die Abfrage mit **"Ja"**. ACHTUNG! Zurzeit hat dieser Dialog keinen weiteren Einfluss auf zukünftige Anmeldungen.

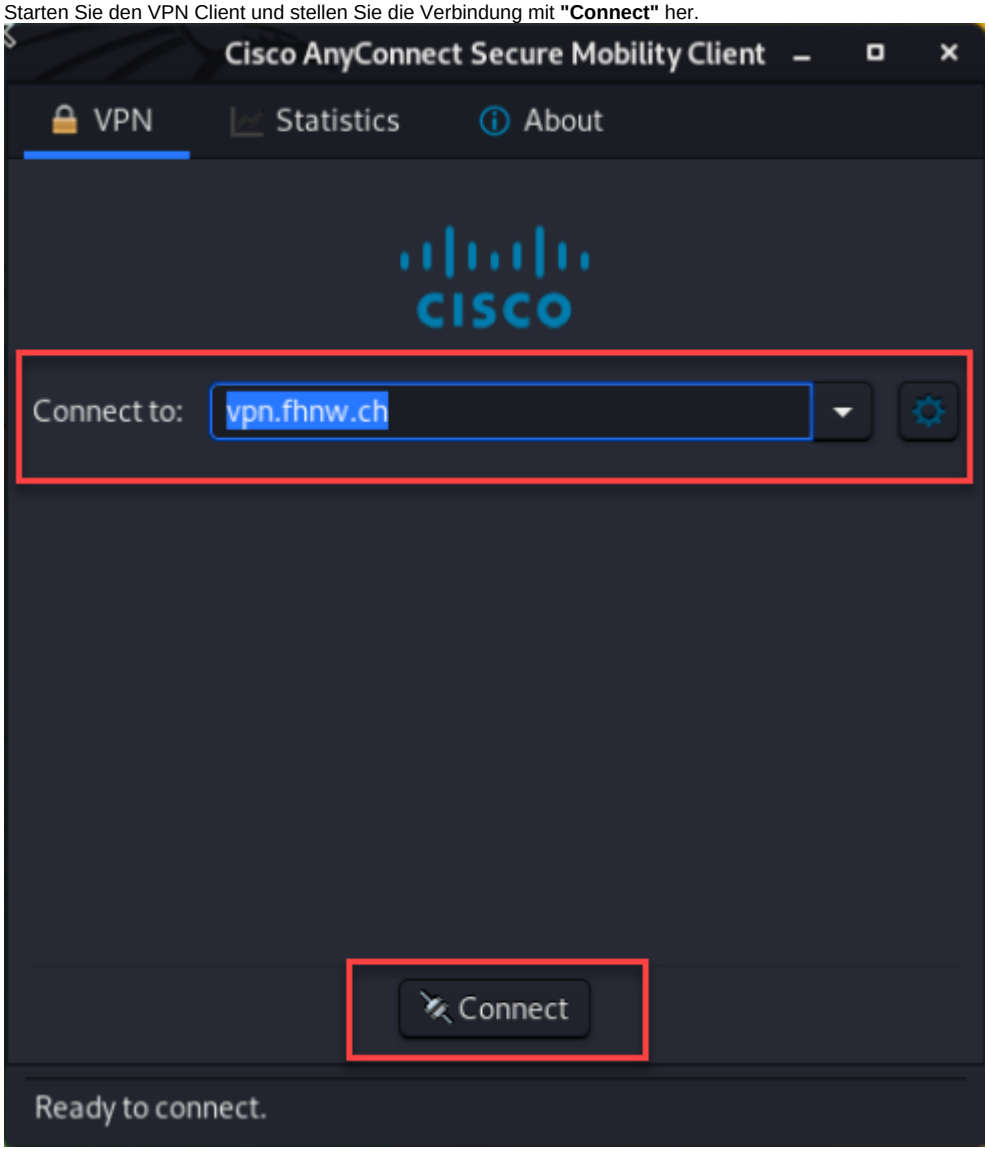


6. Sobald die Verbindung besteht, zeigt der Schalter dies in **"grün"** an.

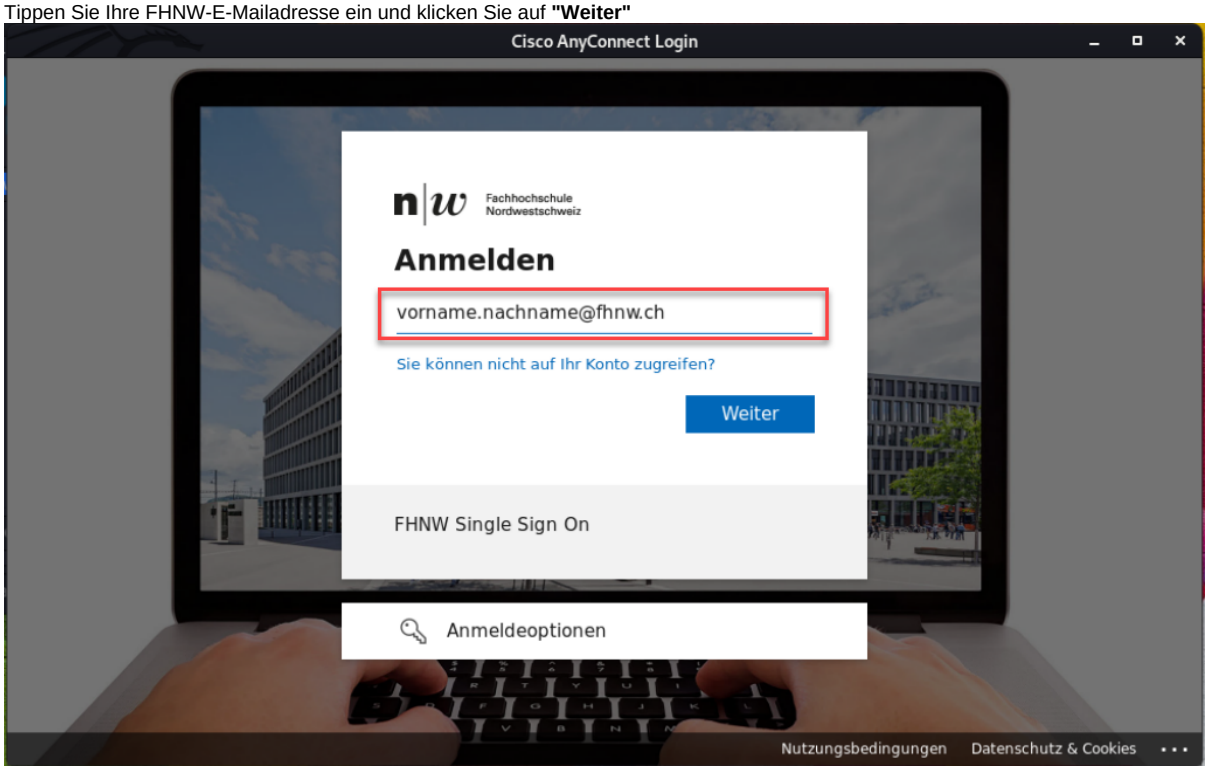
Linux

VPN Anmeldung mit MFA unter Linux

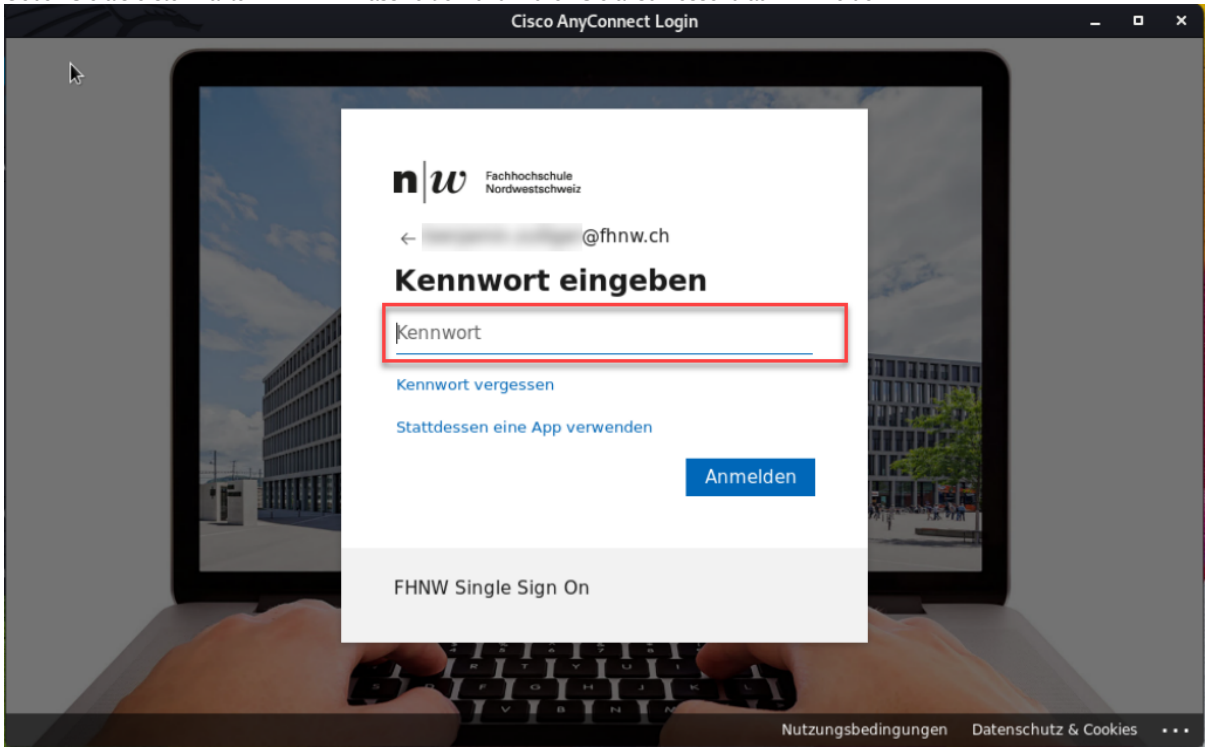
1. Starten Sie den VPN Client und stellen Sie die Verbindung mit **"Connect"** her.



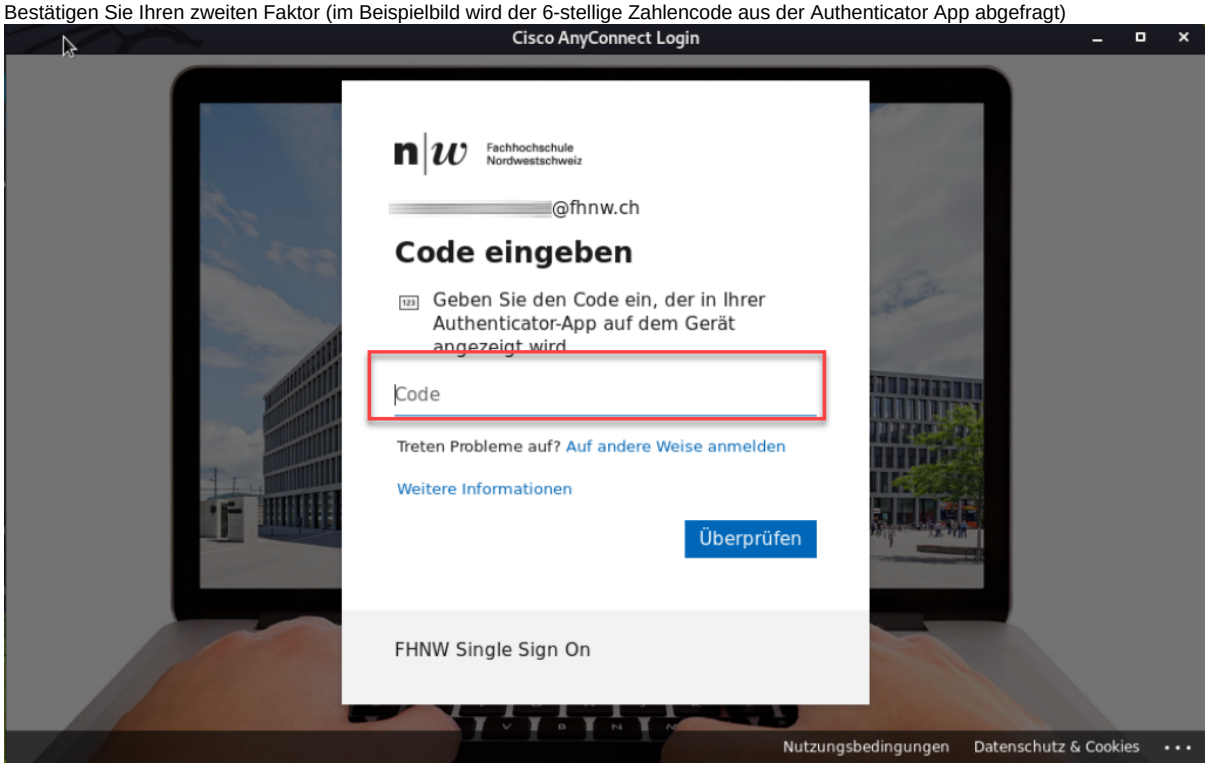
2. Tippen Sie Ihre FHNW-E-Mailadresse ein und klicken Sie auf **"Weiter"**



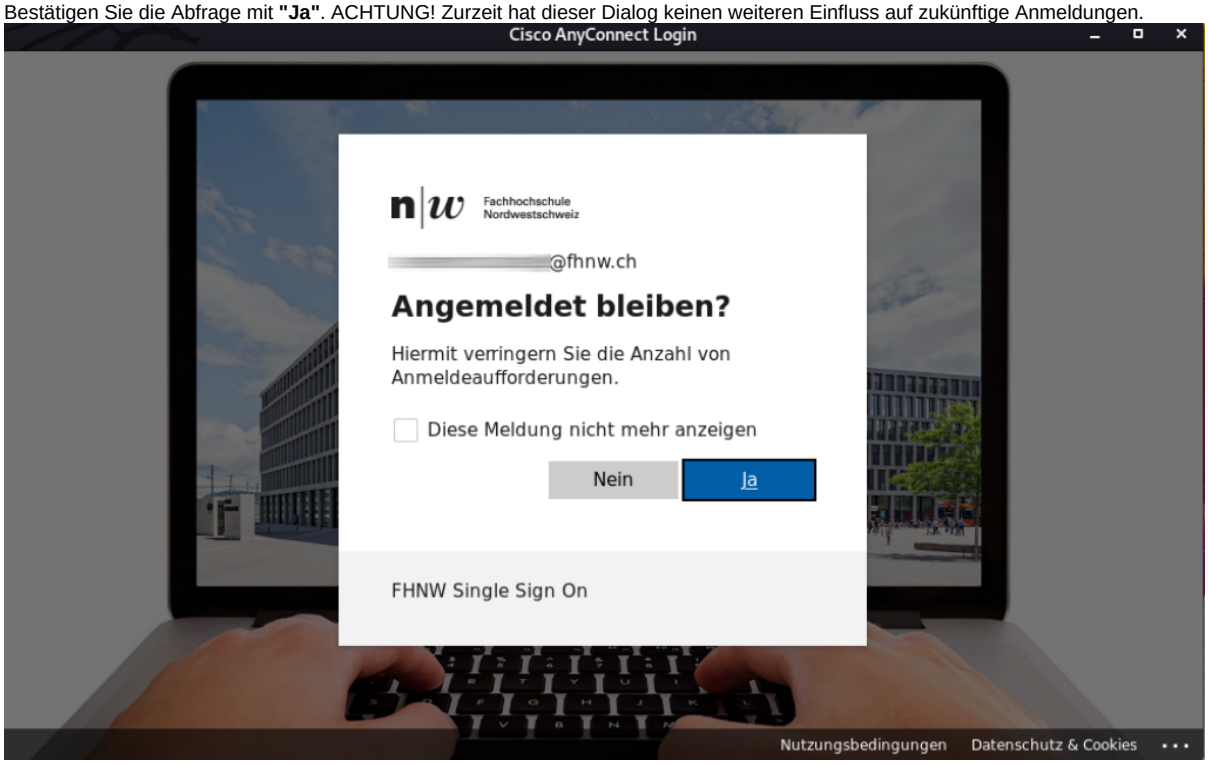
3. Geben Sie als ersten Faktor Ihr FHNW-Passwort ein und klicken Sie anschliessend auf **"Anmelden"**



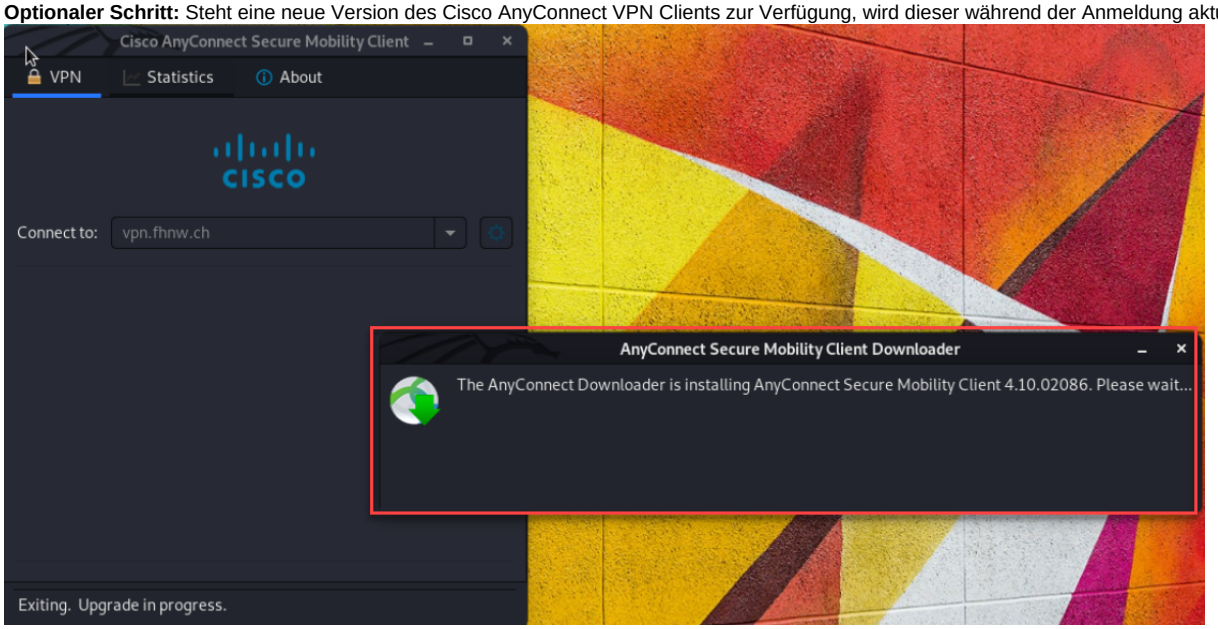
4. Bestätigen Sie Ihren zweiten Faktor (im Beispielbild wird der 6-stellige Zahlencode aus der Authenticator App abgefragt)



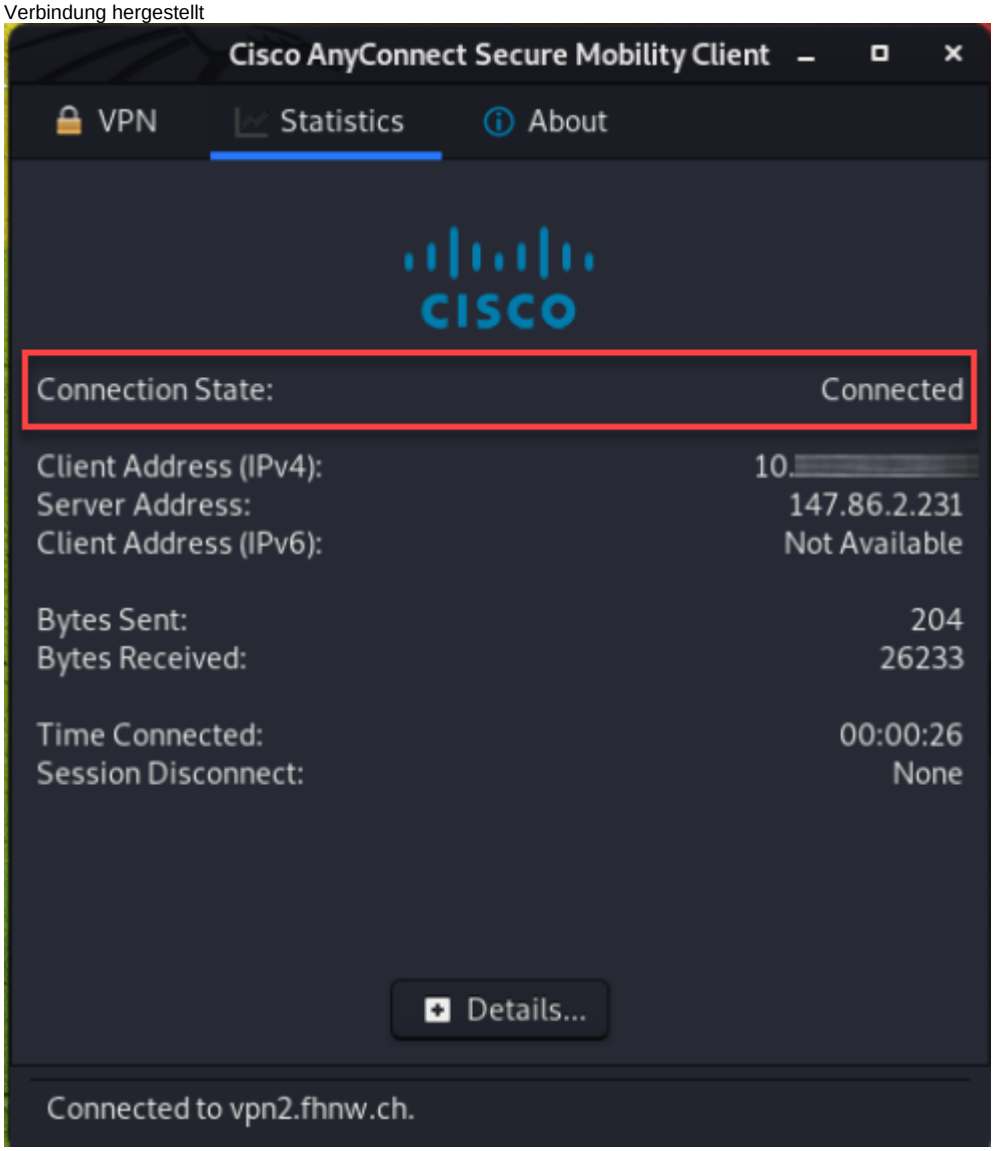
5. Bestätigen Sie die Abfrage mit **"Ja"**. ACHTUNG! Zurzeit hat dieser Dialog keinen weiteren Einfluss auf zukünftige Anmeldungen.



6. **Optionaler Schritt:** Steht eine neue Version des Cisco AnyConnect VPN Clients zur Verfügung, wird dieser während der Anmeldung aktualisiert.



7. Verbindung hergestellt



---

publiziert: 19. Januar 2022 10:38 Service: S0004 - VPN S0154 - IT Security FHNW