Einrichtung Multi-Faktor-Authentifizierung für interne und externe Benutzer mit einer U-Kennung

(for English version, please see page 11)

Benutzer mit einer U-Kennung (Benutzerkonto), welche die Microsoft 365-Dienste und -Ressourcen der MVV Energie AG oder verbundener Gesellschaften nutzen möchten, müssen zur Anmeldung eine Multi-Faktor-Authentifizierung (im Folgenden “MFA”) mittels Microsoft Authenticator App verwenden. Die Anmeldung mittels MFA ist erforderlich, sobald Sie ein Gerät verwenden, das nicht von der Soluvia IT-Services zur Verfügung gestellt und verwaltet wird. Diese Anleitung soll Ihnen dabei helfen, die MS Authenticator App einzurichten und Ihr Konto für die MFA einzustellen.
Bei Fragen oder technischen Problemen wenden Sie sich bitte wie immer telefonisch an den Anwenderservice der Soluvia IT-Services unter der Nummer +49-621-2903636.

1. Voraussetzungen

Nutzer mit U-Kennung

Um MFA nutzen zu können, benötigen Sie zunächst ein Benutzerkonto (U-Kennung), das über Ihren Ansprechpartner bei der MVV oder einer der verbundenen Gesellschaften beantragt und eingerichtet wurde. Sie haben somit bereits eine

- Benutzerkennung,
- eine E-Mail-Adresse und
- ein initiales Passwort erhalten.

2. Multifaktor-Authentifizierung einrichten

Eine Anmeldung per MFA läuft in zwei Schritten ab:

- Die von Ihnen angeforderte Microsoft 365-Ressource (Aufruf einer Connect-Webseite, SharePoint-Verzeichnis, Zugriff auf Ihr Exchange Online Postfach oder Teams usw.) fordert Sie zur Eingabe von Benutzername und Passwort auf.

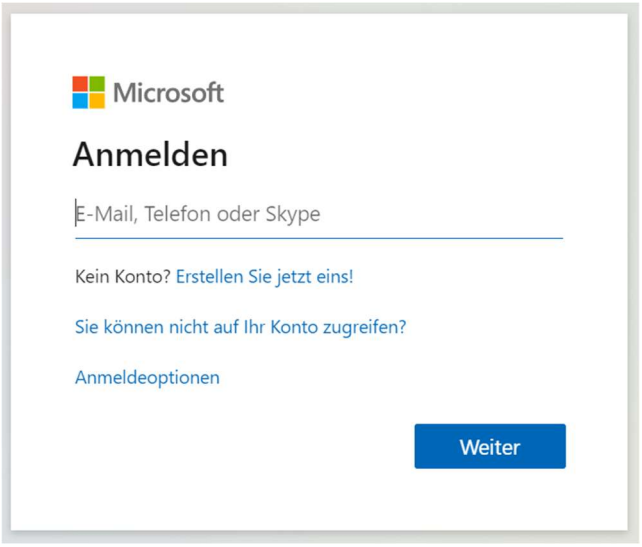
- Nach erfolgreicher Eingabe sendet das System eine Authentifizierungsanfrage an Ihre MS Authenticator App (zweiter Faktor) auf Ihrem Smartphone. Diese wird als Pop-Up angezeigt. Nach Bestätigung durch Sie wird der Zugang gewährt.

2.1. Aktivierung Multifaktor-Authentifizierung

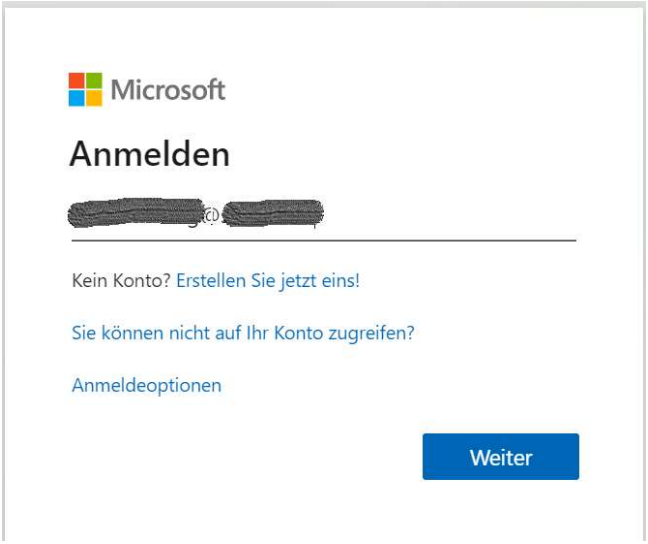
Nach Einrichtung eines Benutzerkontos ist zunächst kein weiterer Zugriff auf Ressourcen im Konzern möglich, solange das Benutzerkonto nicht auf MFA umgestellt ist. Öffnen Sie hierzu in einem Webbrowser die Adresse:

https://aka.ms/MFASetup

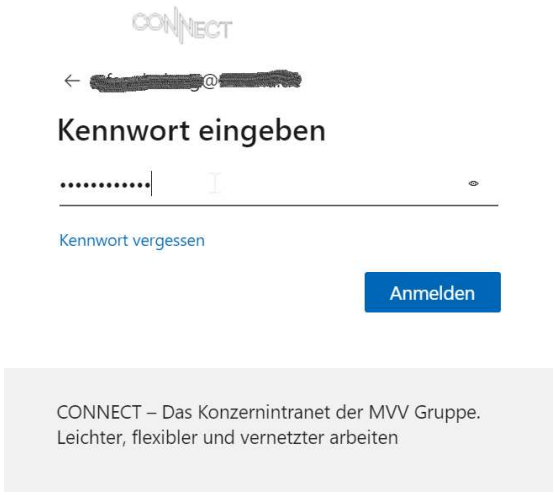
Dieser Aufruf führt Sie zur Kontenverwaltung Ihres Microsoft Cloud-Benutzerkontos. Melden Sie sich mit der Ihnen bekannten Benutzerkennung (siehe 1.) an:



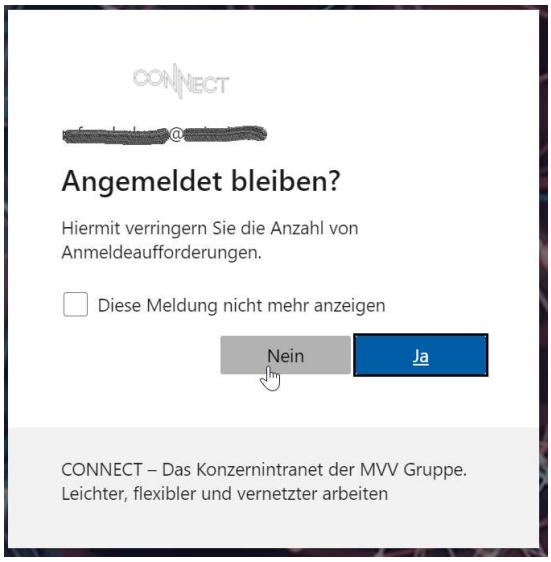
Geben Sie dazu zunächst Ihre E-Mail-Adresse ein und drücken Sie „Weiter“



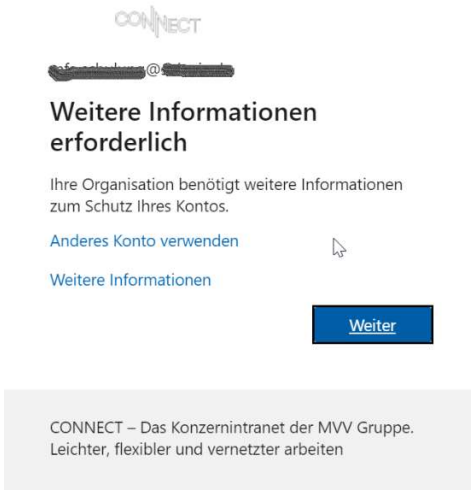
Geben Sie dann Ihr Kennwort ein und klicken sie auf „Anmelden“



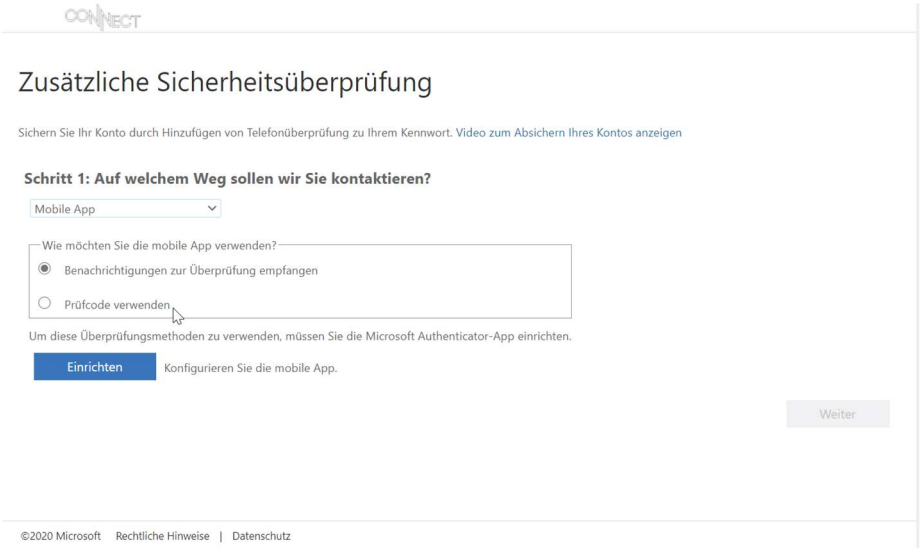
Im folgenden Bildschirm empfehlen wir aus Sicherheitsgründen „Nein“ auszuwählen:



Nach erfolgreicher Anmeldung wird automatisch erkannt, dass für Ihre Benutzerkennung weitere Einstellungen nötig sind:



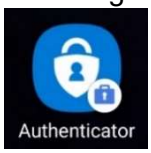
Nach einem Klick auf „Weiter“ werden die nötigen Informationen zur Konfiguration von MFA abgefragt:
In **Schritt 1** wählen Sie in dem Pull-Down-Menü „Mobile App“ als Methode aus. Bei der Frage „Wie möchten Sie die mobile App verwenden?“ wählen Sie die Option „Benachrichtigung zur Überprüfung empfangen“ aus:



Bevor Sie nun auf „Weiter“ klicken können, erfolgt die Einbindung der MS Authenticator App. Führen Sie nun folgende Schritte aus:

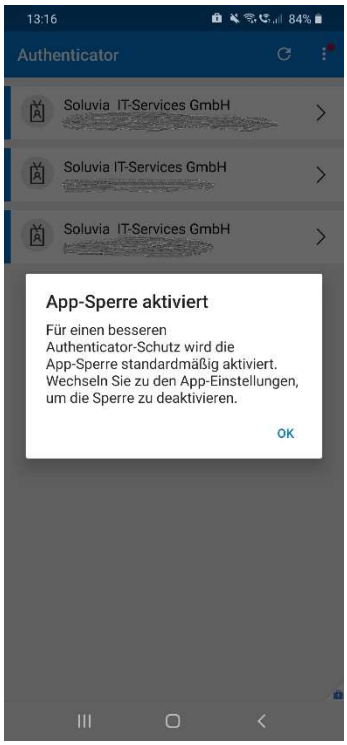
2.2. Installation und Konfiguration der Authenticator App

- Installieren Sie sich auf Ihrem Smartphone die App „Microsoft Authenticator“. Achten Sie darauf, dass es sich um die App von Microsoft handelt, da es viele Apps mit ähnlichem Namen gibt:

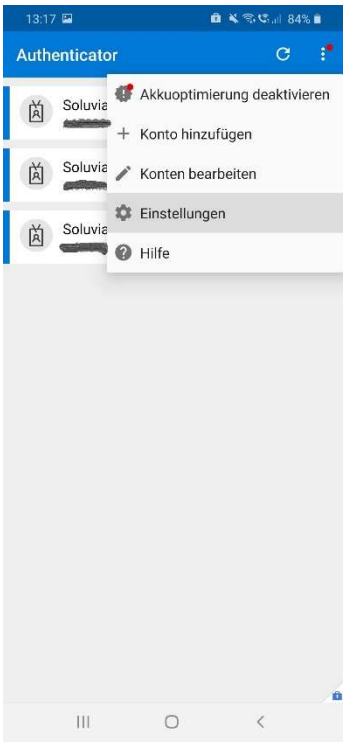
  Google Play (Android): https://play.google.com/store/apps/details?id=com.azure.authenticator
  Apple App Store (iOS): https://apps.apple.com/de/app/microsoft-authenticator/id983156458

Nach der Installation der Anwendung starten Sie die App. Die Authenticator App fordert nun die Eingabe des Gerätepassworts:

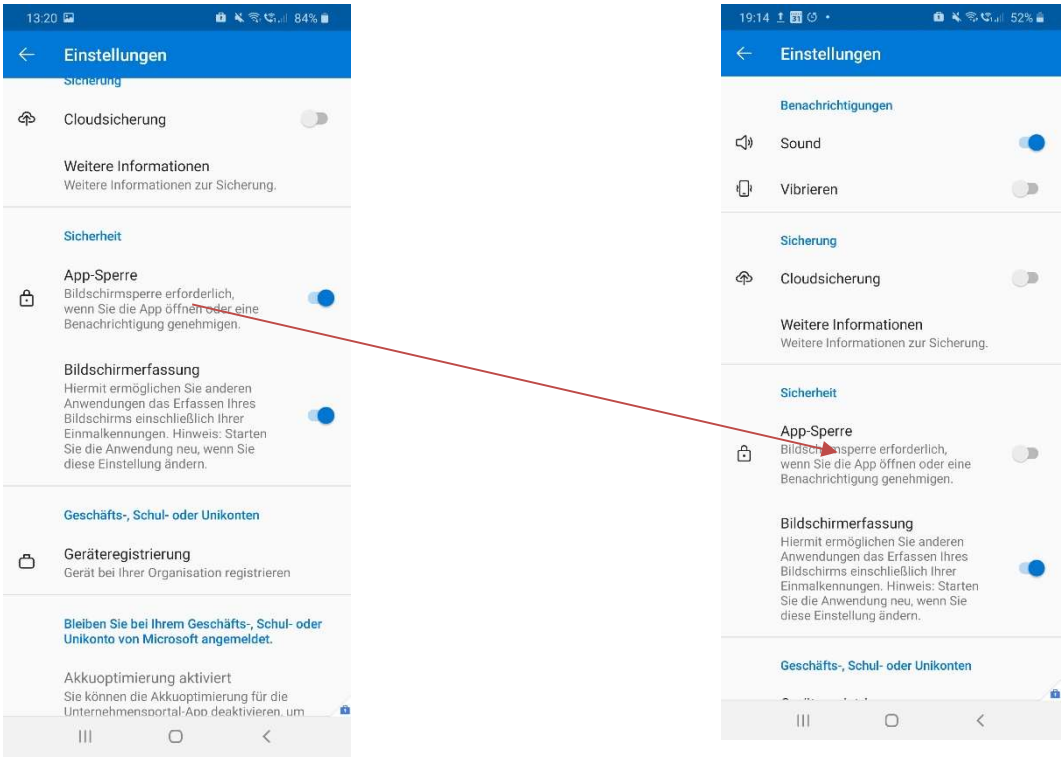


Die separate Absicherung der App durch das Gerätepasswort ist eine sinnvolle Sicherheitsergänzung. Diese mehrfache Eingabe des Gerätepassworts kann jedoch bei Bedarf wie folgt deaktiviert werden.

Öffnen Sie zunächst die App-Einstellungen:



In den Einstellungen kann dort die App-Sperre deaktiviert werden, indem der Schalter unter „App-Sperre“ deaktiviert wird:

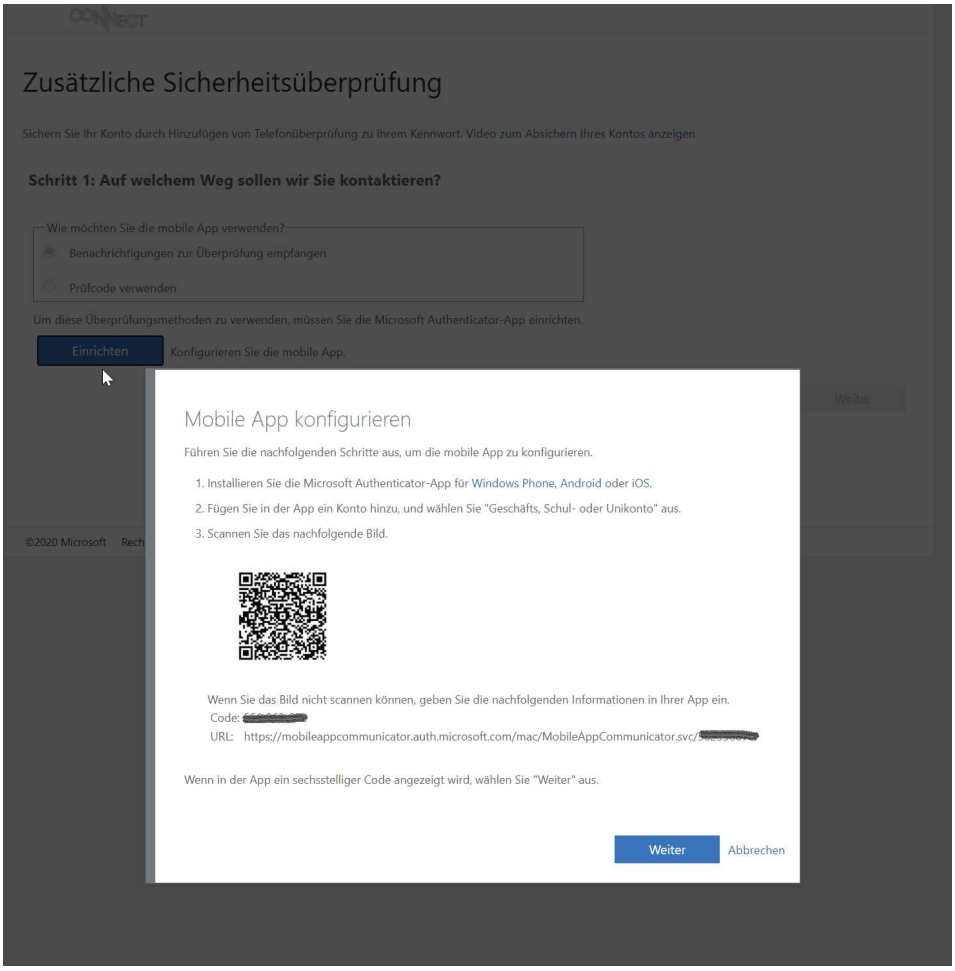


Die Authenticator App muss nun noch mit ihrem Microsoft Konto verknüpft werden, wie im Folgenden beschrieben.

2.3. Abschließende Konfiguration des Microsoft-Kontos

- Klicken Sie nun im Menü „Zusätzliche Sicherheitsüberprüfung“ aus Kap. 2.2 auf „Einrichten“.

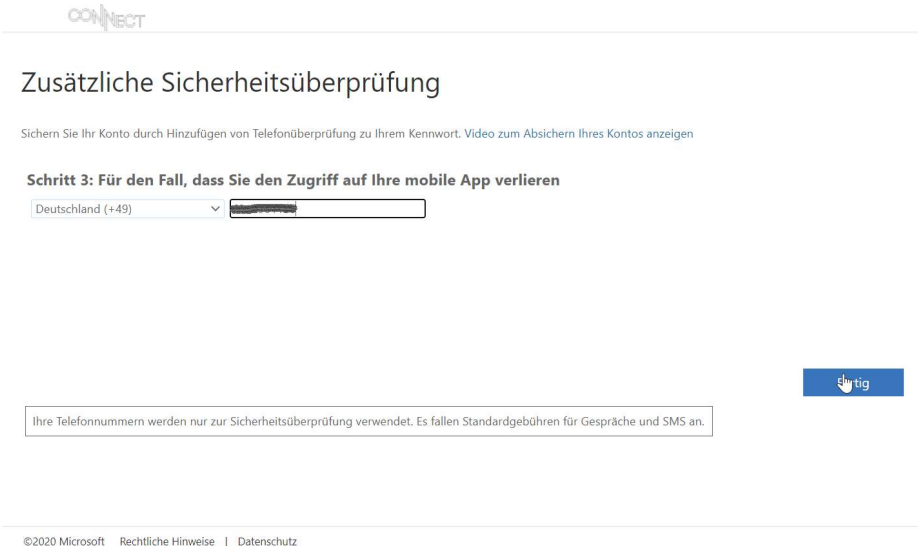
- Folgen Sie den Anweisungen und fügen Sie Ihr Konto in der Authenticator App hinzu:



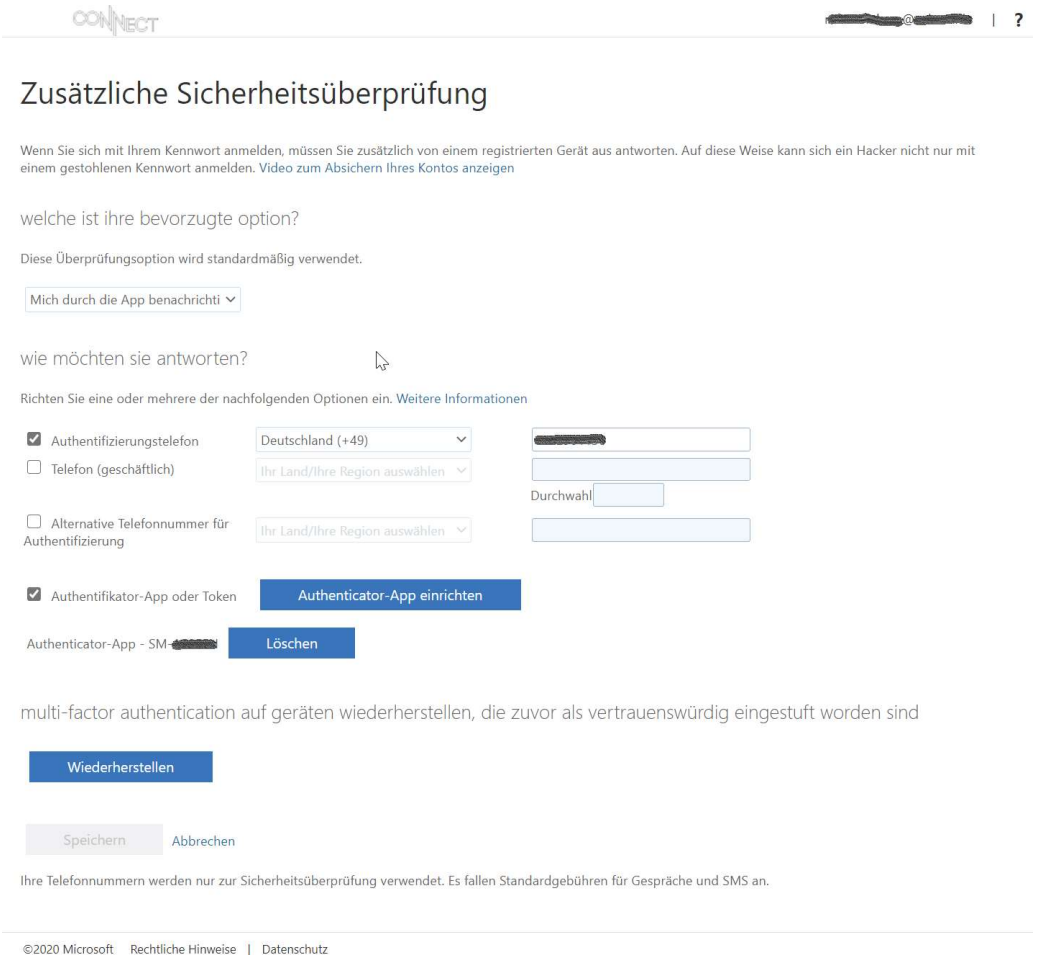
Nach erfolgreicher Registrierung der App klicken Sie auf „Weiter“. Den wichtigsten Teil haben Sie damit bereits erledigt:

Für die vollständige Einrichtung ist es nun noch notwendig ihre Mobilfunknummer zu hinterlegen, damit Sie sich auch per SMS oder Sprachanruf authentifizieren können. Fügen Sie zudem im nächsten Schritt auch eine alternative Telefonnummer hinzu, die Sie zur Authentifizierung oder im Falle eines Verlusts des Smartphones zur Authentifizierung nutzen können.

Dies sollte dann nicht die Mobilfunknummer Ihres Smartphones sein:

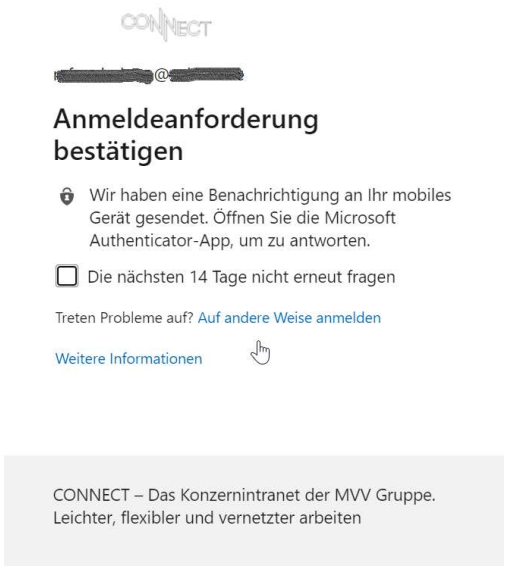


Klicken Sie dann auf „Weiter“. Nach diesem Schritt sehen Sie eine Zusammenfassung Ihrer Einstellungen. Sie können hier Ihre Einstellungen auch anpassen, weitere Geräte registrieren oder eine bestehende Registrierung auch wieder löschen.



Mit Abschluss dieser Einrichtung steht Ihnen nun MFA für Ihre Anmeldung an den Cloud-Diensten zur Verfügung.

Wenn Sie sich nun anmelden, so werden Sie zunächst nach Ihrem Benutzernamen und Ihrem Passwort gefragt. Nach Eingabe des Passworts sollten Sie, je nach Service, das folgende Fenster sehen:



Da die Authenticator App in Ihrem Profil als bevorzugte Authentifizierungsmethode konfiguriert ist, sollten Sie nun auf Ihrem Smartphone eine Mitteilung (Pop-Up) erhalten und können den Anmeldeversuch genehmigen oder ablehnen:

Im Normalfall möchten Sie die Anmeldung natürlich genehmigen und Sie haben sich damit erfolgreich authentifiziert.

Es kann jedoch Situationen geben, in denen Sie eine alternative Authentifizierungsmethode nutzen möchten. In diesem Fall steht Ihnen eine Authentifizierung per SMS oder Sprachanruf

zur Verfügung. Sie können eine alternative Methode auswählen, indem Sie in dem vorherigen Fenster auf „Auf andere Weise anmelden“ klicken. Es werden Ihnen dann alternative Möglichkeiten angeboten:

Sollten Sie allerdings eine Anfrage zur Genehmigung einer Anmeldung erhalten, obwohl Sie selbst aktuell NICHT versucht haben, sich an Connect anzumelden, so lehnen Sie diese aus Sicherheitsgründen ab. Wiederholt sich dieses Phänomen mehrfach, handelt es sich vermutlich um einen Versuch, Ihr Konto zu übernehmen. Informieren Sie in diesem Fall bitte unbedingt den Anwenderservice der Soluvia IT-Services unter der Nummer +49-621-2903636.

Configuration of Multi Factor Authentication for internal and external Users with U-Identifier

Users with a U-identifier (user account) who wish to use the Microsoft 365 services and resources of MVV Energie AG or affiliated companies must use multi-factor authentication (hereinafter "MFA") via Microsoft Authenticator App to log in. Logging in using MFA is required as soon as you use a device that is not provided and managed by Soluvia IT Services.
This guide is intended to help you set up the MS Authenticator App and set your account for MFA.
As always, if you have any questions or technical problems, please call Soluvia IT-Services' User Service at +49 621 2903636.

1. Prerequisites

In order to use MFA you first need a user account. This should have been requested and set up via your contact person at the MVV or one of its affiliates. You therefore already should have

- a User ID and/or
- an email address and
- received an initial password

2. Enable multi factor authentication

A multi factor authentication takes place in a two-step process:

- First, you will be prompted for your username and password by the resource you requested (a Web page login, directory, or similar)
- Second, after successful input, the system sends an authentication request to the MS Authenticator app (second factor) associated with your smartphone. The request is displayed as a pop-up message. Upon confirmation by you access will be granted.

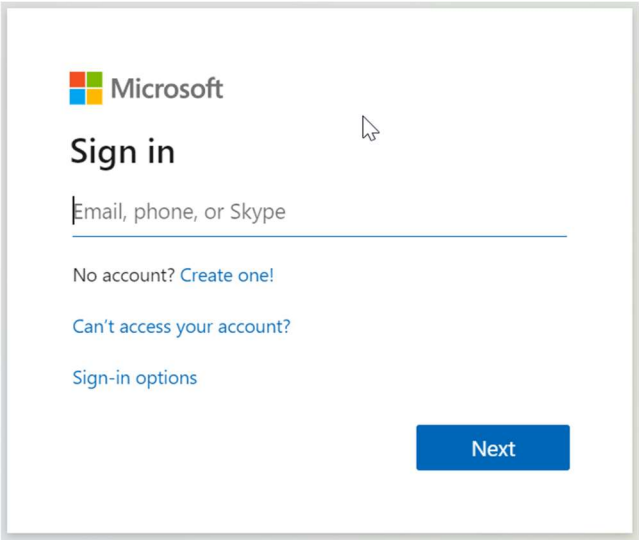
2.1. Activating multi factor authentication

After initial setup of your user account, you cannot access corporate resources until the user account is configured to use MFA. To do this, open the following address in a web browser:

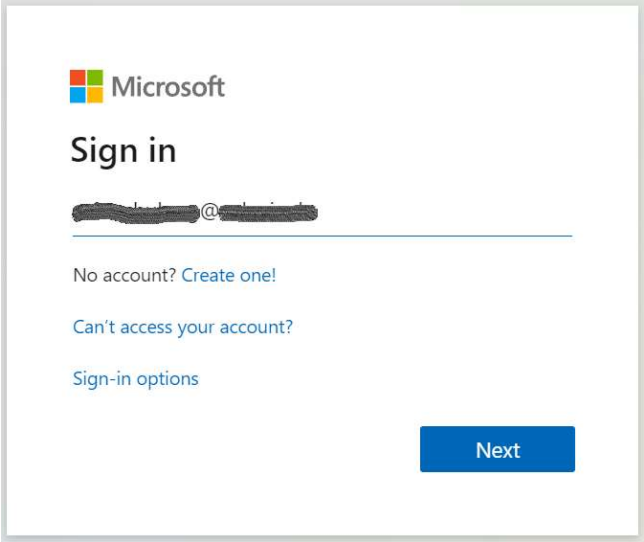
https://aka.ms/MFASetup

This will open your Microsoft Cloud user account management.

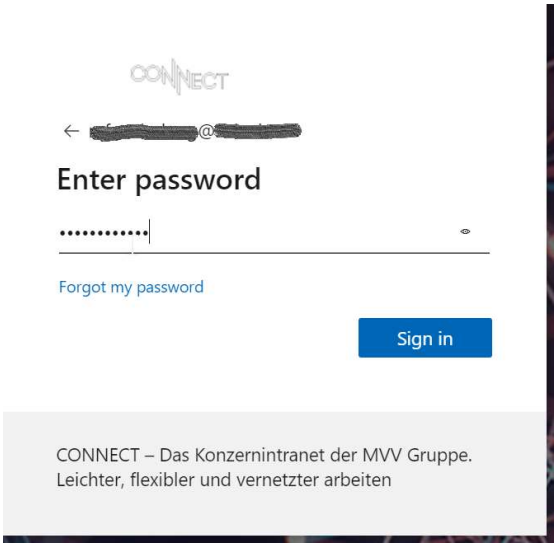
Log in with your user credentials:



Enter your email address first and then press "Next"

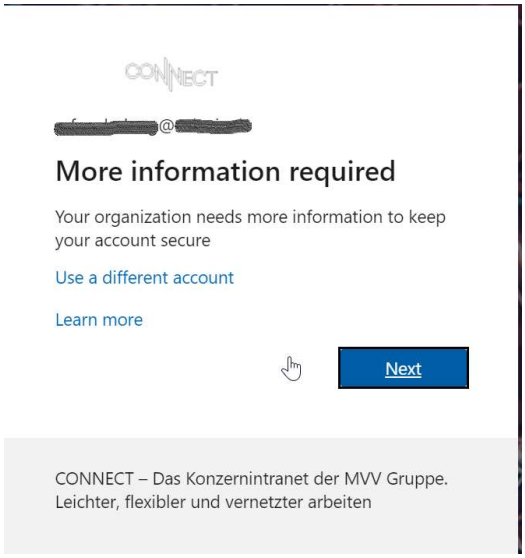


Enter your password and click on “Sign in”



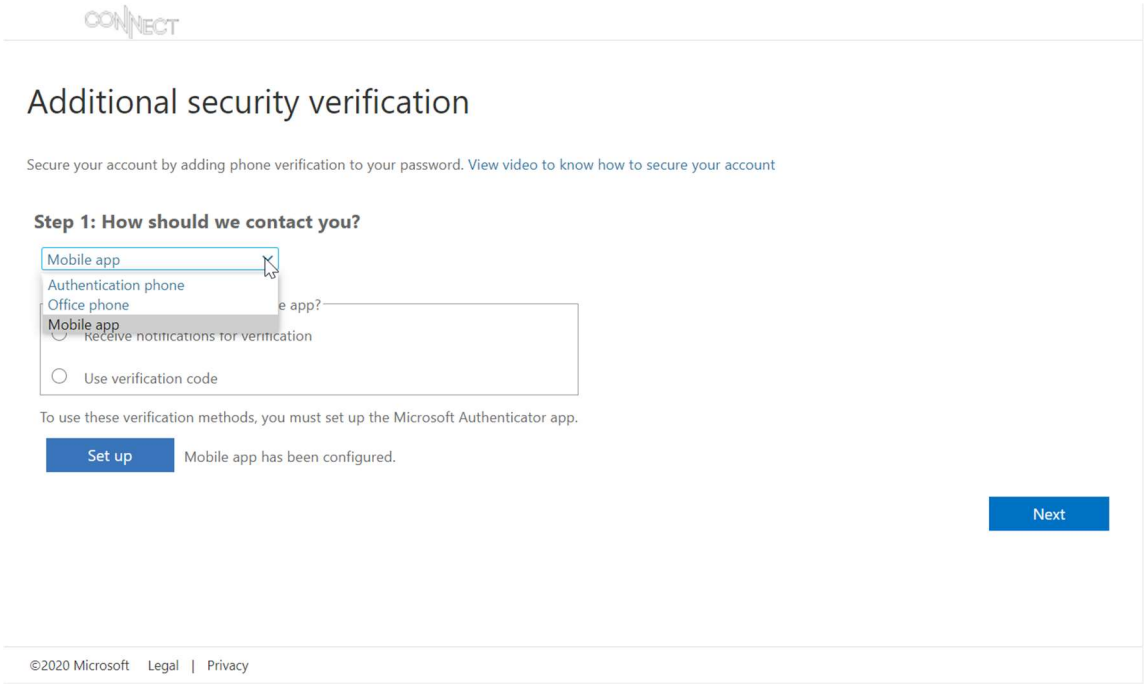
In the next panel we suggest choosing “No” for security reasons

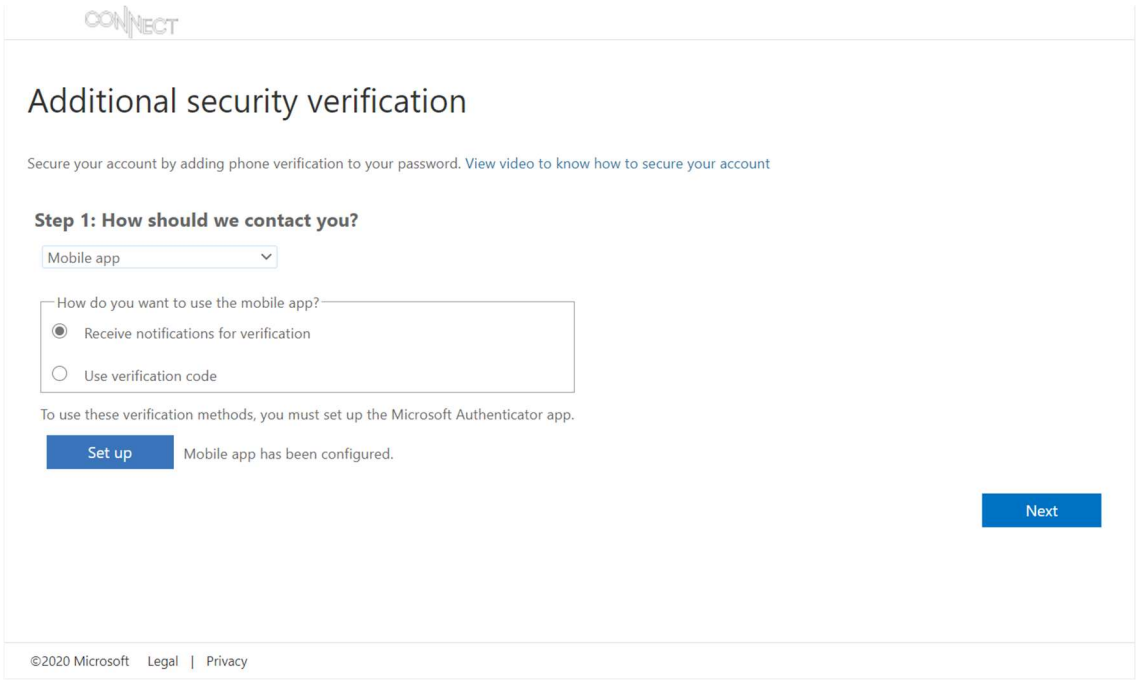
After successful login the system will recognize that your user ID requires additional settings:



After clicking „Next“ an assistant will guide you through the configuration process.

In Step 1 select “Mobile App” from the pull-down menu. In the section “How do you want to use the mobile app?” select “Receive notification for verification”:





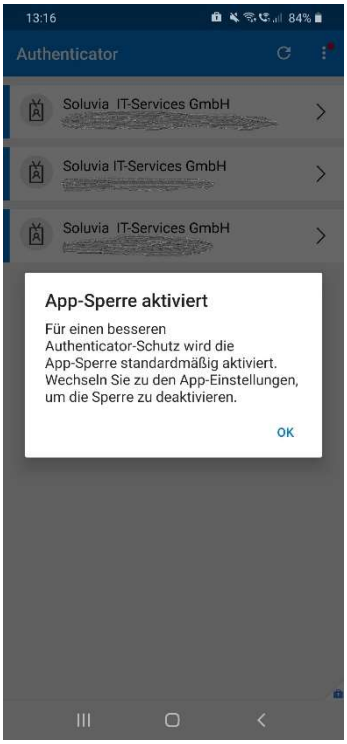
Before you can click "Next", the authenticator app must be installed and connected to your Microsoft online account. Please carry out the following steps:

2.2. Installation and configuration of the authenticator app

- Install the Microsoft Authenticator app on your smartphone.
- Make sure to choose the original app Authenticator from Microsoft, as there are many apps with similar names:

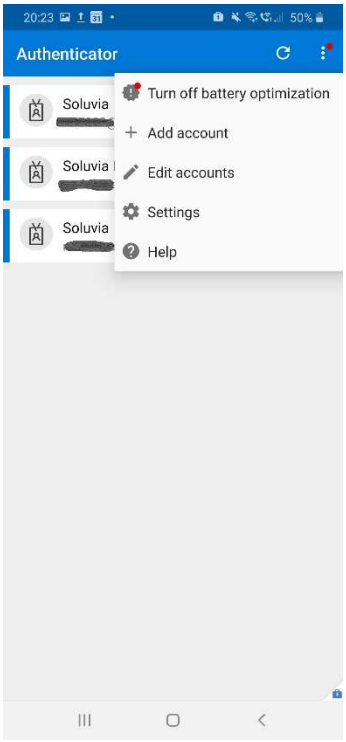
Google Play (Android):
https://play.google.com/store/apps/details?id=com.azure.authenticator
Apple App Store (iOS): https://apps.apple.com/de/app/microsoft-authenticator/id983156458

- Please launch the application after installation. The Authenticator app will now ask you to enter the device password:

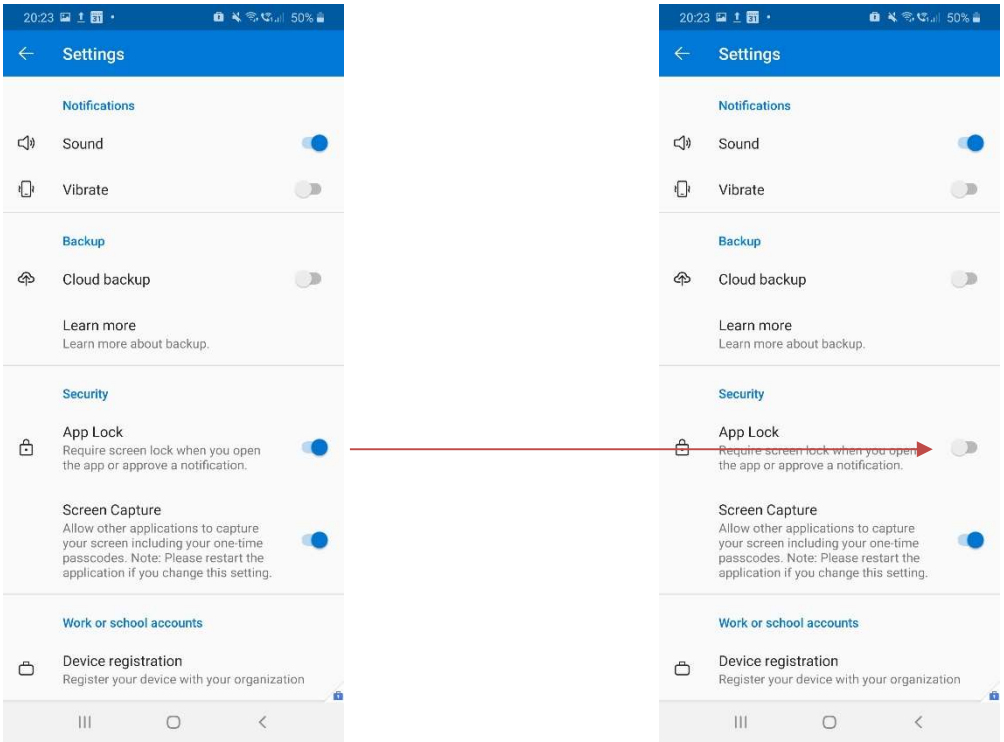


The separate protection of the app by the device password is a useful security addition. However, this multiple entry of the device password can be deactivated as follows if required.

First open the app settings:

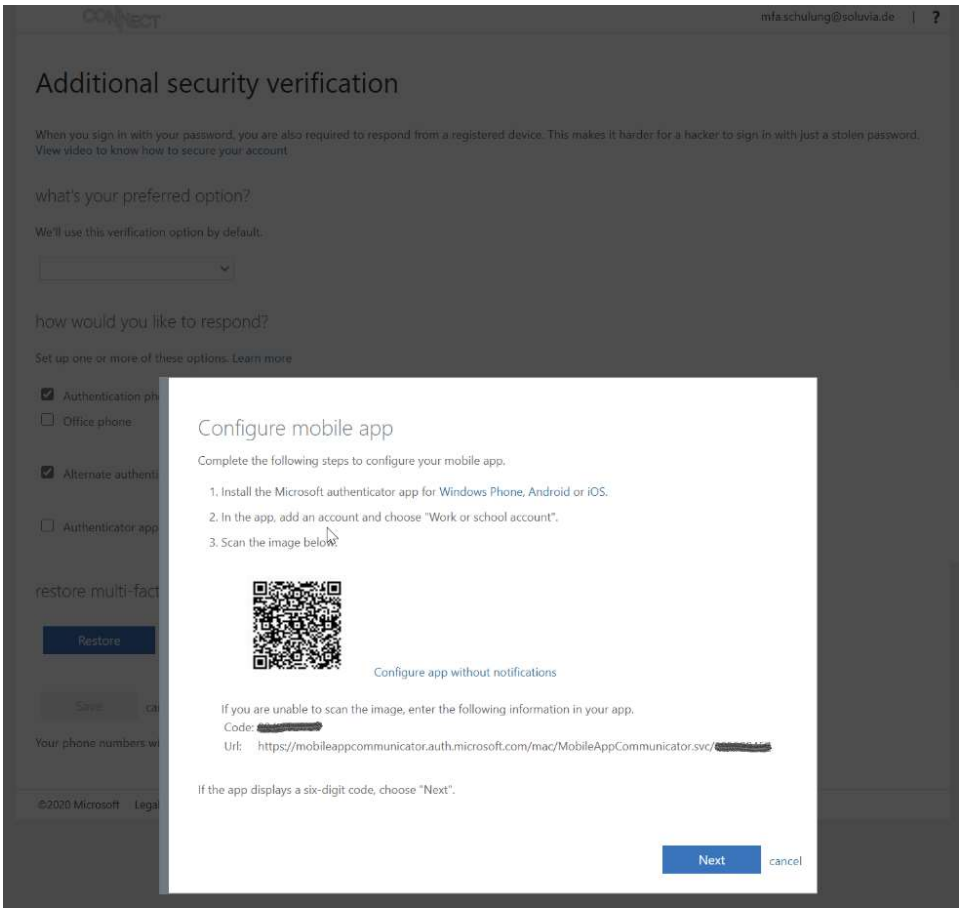


You can deactivate App-Lock in the app settings:



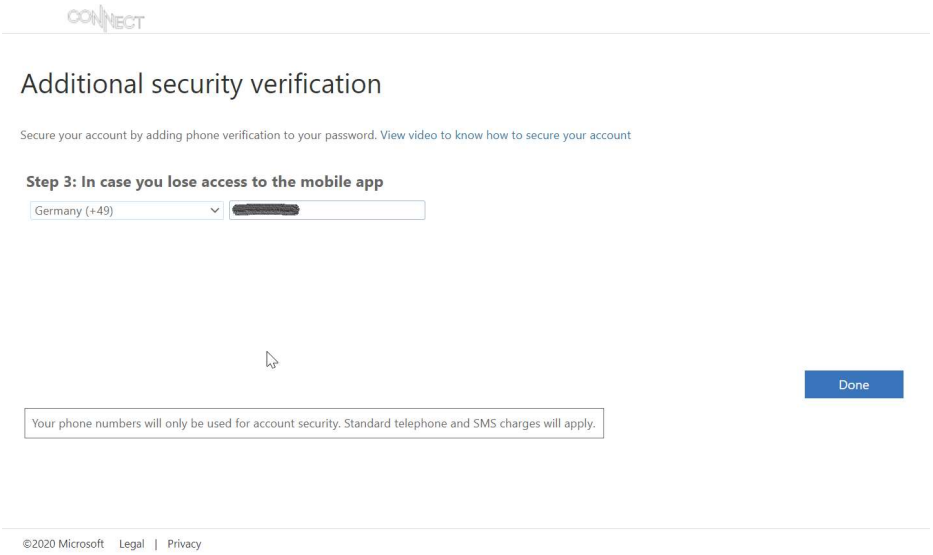
2.3. Finalizing the configuration of your Microsoft online account

- Now click on "Set up" in the "Additional security check" menu from Chap. 2.2. Follow the instructions and add your account in the Authenticator app:

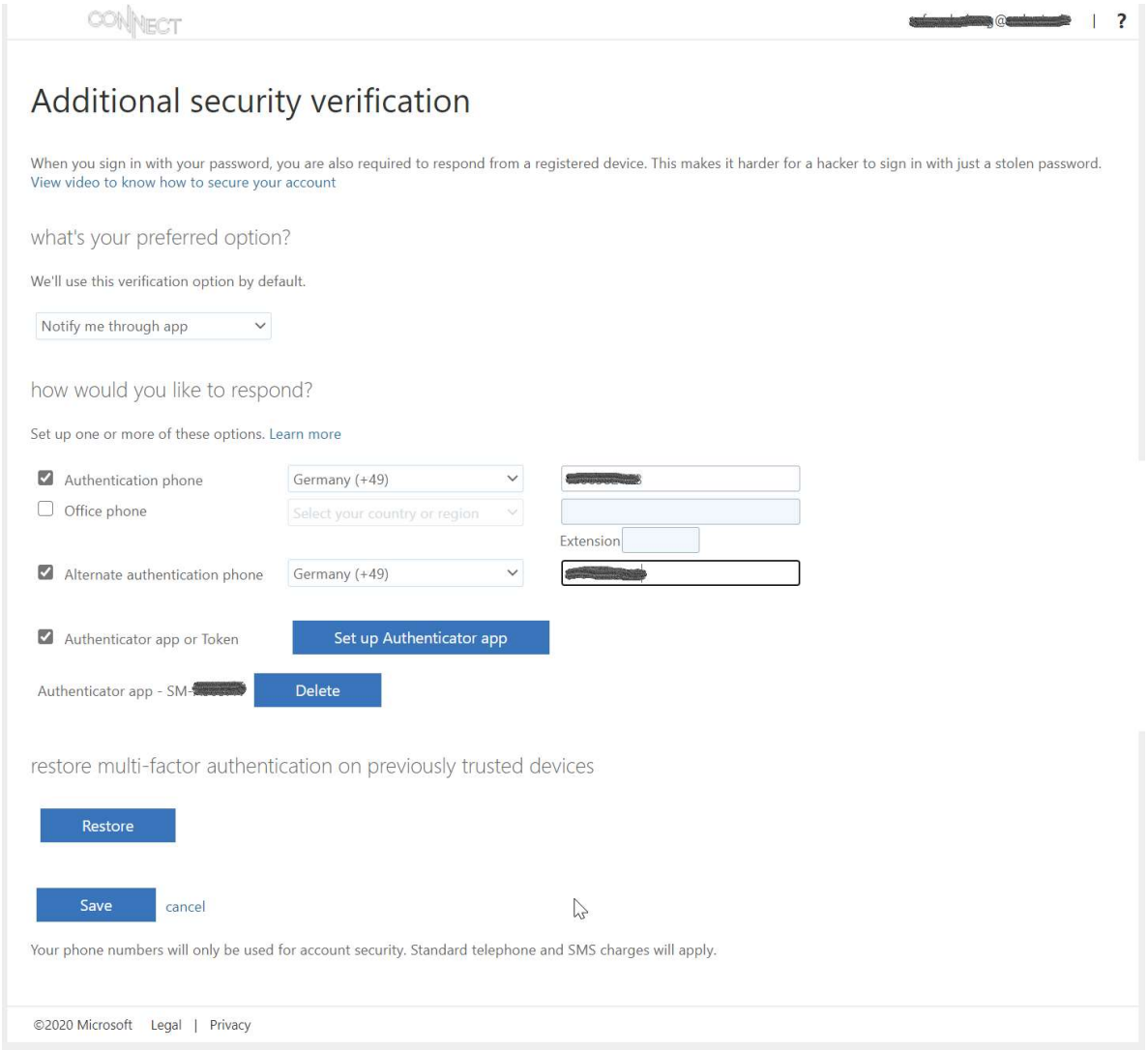


After successful registration of the app, click "Next". You will receive a notification on your smartphone in order to verify successful communication.
You now have already completed the most important part of the configuration process. For full setup, it is now necessary to enter your mobile phone number so that you can use alternative authentication methods like SMS or phone call. You should also configure an alternative phone number for authentication, in case you lose your smartphone.

Obviously, this should not be the mobile phone number of your smartphone:

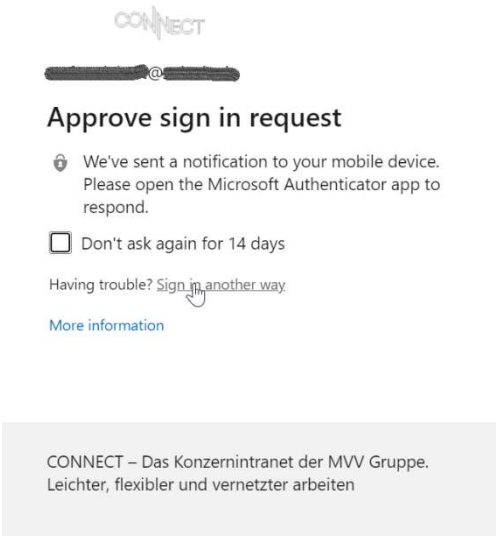


Then click "Next". After this step, you will see a summary of your settings. You can still adjust your settings here, register additional devices or delete an existing registration.



With the completion of this setup, MFA is now available to sign in to the cloud services.

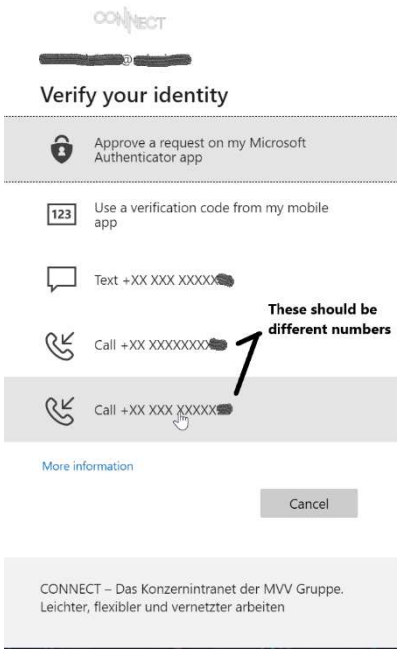
When you log in, you will first be asked for your username and password. After entering the password, you will see, depending on the service requested, the following panel:



Since the authenticator app is configured as your preferred authentication method you should receive a pop-up message on your smartphone signaling that a login attempt has taken place and asking for approval:

Under normal circumstances you want to approve this attempt, of course, since you by yourself are trying to log-in at this very moment. After approval you have been authenticated successfully.

However, it might be necessary to use an alternative authentication method. In this case use “Sign in another way” from the previous panel. You can then choose from various methods like text message or phone call. The phone numbers you configured in the previous steps will be presented here as alternatives:



However, if you receive a request to approve a registration, even though you have not attempted to log in to Connect or any other service at this time, you should reject this request for security reasons. If this phenomenon repeats several times, it is probably an attempt to take over your account. In this case, please inform the Soluvia IT-Services' User Service immediately at +49 621 2903636.