MAN Energy Solutions

Azure Multi Factor Authentication (MFA) – MAN ES User Guide

Content

1. Introduction

This gives you a short overview how to configure and use Azure MFA.

1.1 Second factors for two-factor authentication methods

- Allowed factors
  - Phone Factor (Phone Call)
  - Token via Mobile App
  - **Push Notification via Mobile App (Phone needs to be connected to the internet)**
  - SMS - Note: SMS does not have a guaranteed delivery - therefore it should be avoided and replaced with the Phone Factor.
- Disallowed factors
  - Hardware Token
  - Mail (not supported)

We always recommend configuring two methods for two-factor authentications.

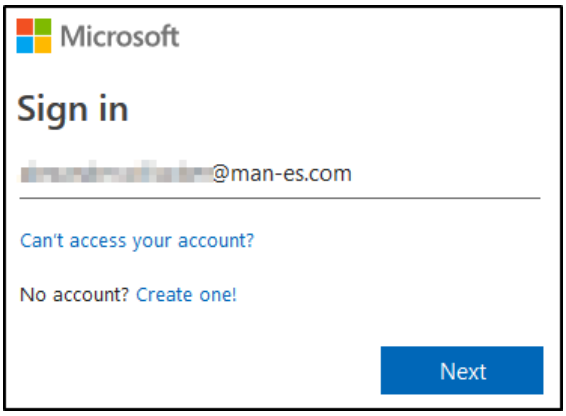
The easiest method to use is Push Notification via the mobile app, therefore we propose to use this as default.

2. How to configure your first, second factor with Azure MFA

We recommend configuring your second factor before using applications that requires a two-factor authentication.
If you have not configured a second factor and authenticate to an application, which requires a two-factor, you are redirected to the Azure MFA self-onboarding page.

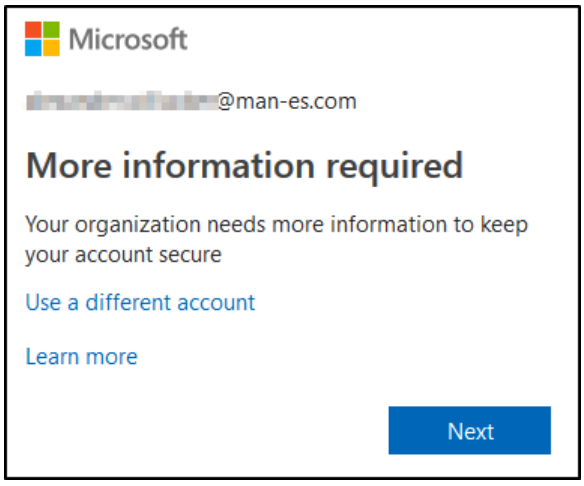
To configure Azure MFA as MAN ES partner (Extranet, Nexus user) please go to:
https://account.activedirectory.windowsazure.com/proofup.aspx?proofup=1&whr=mdt-ext.biz

Note: If you are on premise, you will be logged in automatically.



Now you will be asked for “more information”, please click “NEXT”

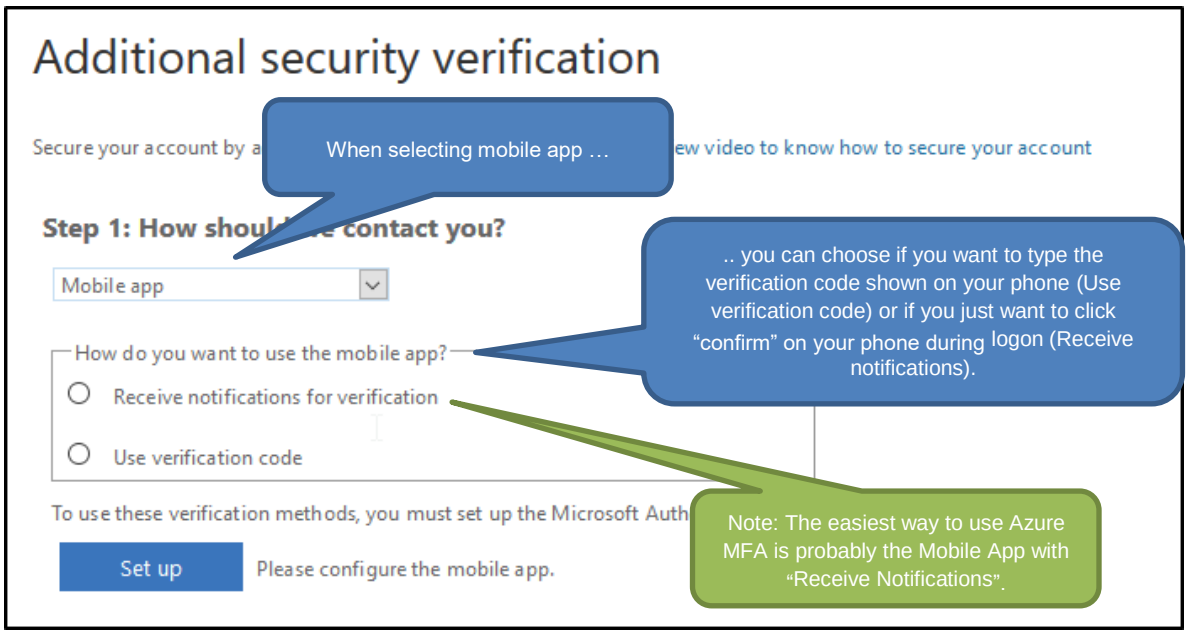
Now you can start configuring your first, second factor.



- If you have a smartphone, we recommend that you configure the Microsoft Authenticator App as second factor authentication. In this case, go to section **2.1 Mobile App**.

- If you do not have a smartphone, you should configure the second factor authentication as described in section **2.2 Phone Factors**.

2.1 Mobile App



When you click on the "Set up" button you will be guided through the Mobile App setup process.

Please download the app in the Appstore and Google Play.

Just scan the QR-Code – after that continue with Step 2

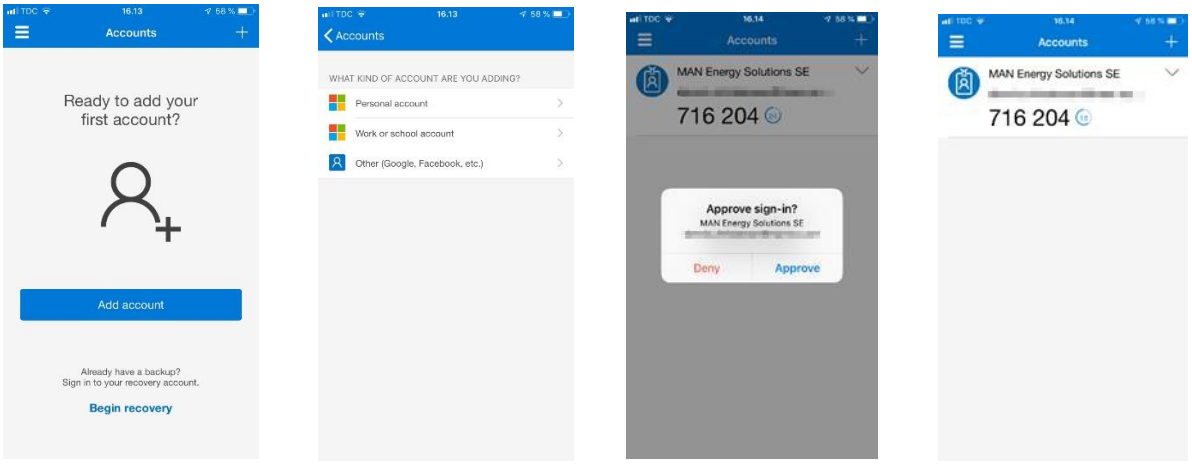
App at Apple AppStore

Download on the App Store

App at Android Google Playstore

GET IT ON Google Play

Follow instructions to install the **Microsoft Authenticator** app and launch it for registration.

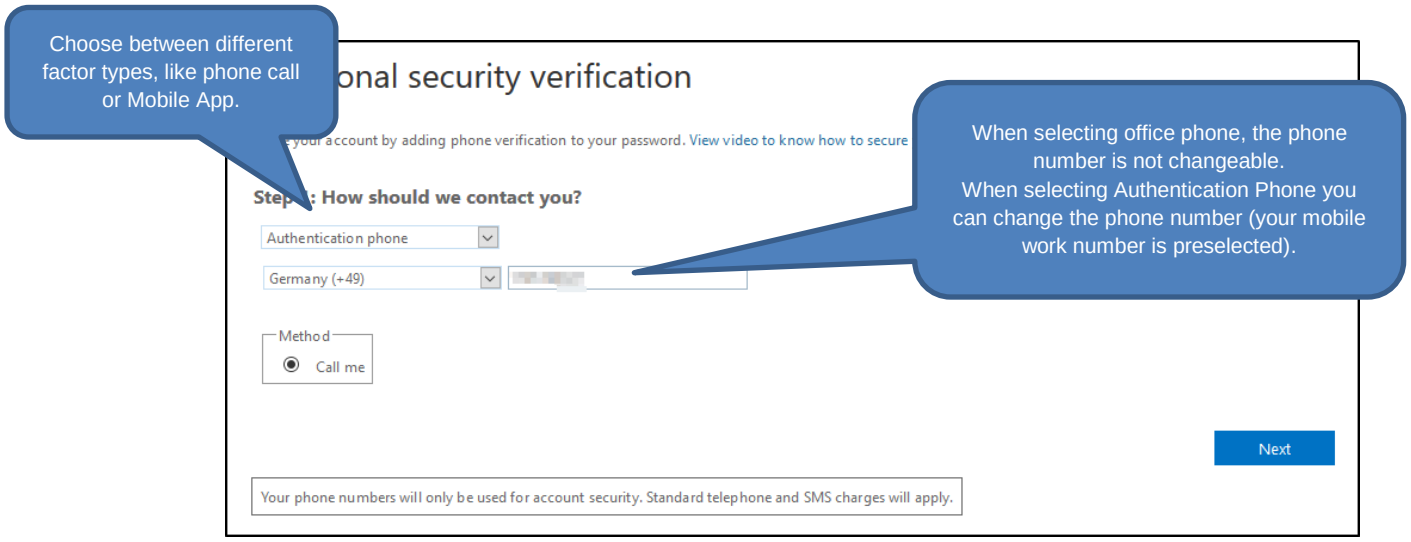


- Launch app
- Add Work or School account (this choice is important for the notification to work)
- Scan QR code from Web registration page
- Approve sign-in challenge
- The App is registered and ready for use

Note: If the QR scan in step 3 fails, you can change to manual entering the verification code. (a possible failure cause is, that you disallowed the app to use the camera)

Congratulations, you have successfully configured second factor for two-factor authentication.

2.2 Phone Factors

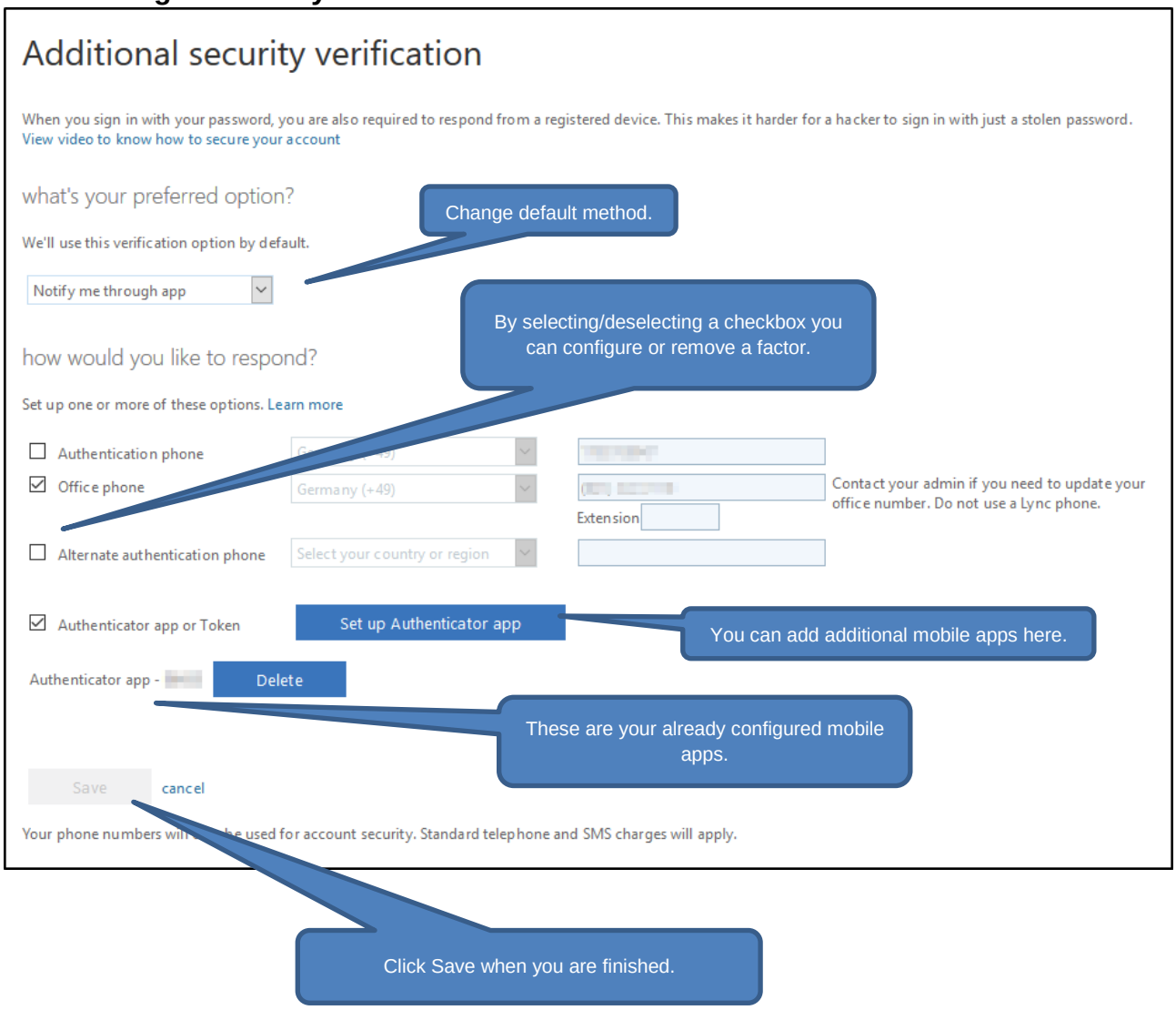


When you click on next, you will receive the verification call.

Note: The pound key is the # on the keypad.

Congratulations, you have successfully configured second factor for two-factor authentication.

2.3 Manage or Modify URL:



Note: If you have lost access to all your second factors, you can reset your account via the Nexus Support at nexusinfo@man-es.com.

3. FAQs

- What can I do, when I have lost or broke my mobile phone or deleted Microsoft Authenticator App by mistake?

- In case of problems with the registration or if the user is somehow locked, our nexusinfo@man-es.com must be contacted to reset the user. After a reset, you can start onboarding from scratch as described in this guide.

- You receive this error when trying to create/modify your second factor.

  - Root Cause: You have set your browser to block Cookies from Microsoft:
  - Resolve it:

    Go to Internet options/Privacy/Sites

    Remove microsoftonline.com here