



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



Content

| | |
|-------------------------------------------------------------------|---|
| 1. Introduction | 3 |
| 1.1 Second factors for two-factor authentication methods | 3 |
| 2. How to configure your first, second factor with Azure MFA..... | 3 |
| 2.1 Mobile App | 4 |
| 2.2 Phone Factors..... | 6 |
| 2.3 Manage or Modify URL: | 8 |
| 3. FAQs..... | 8 |

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

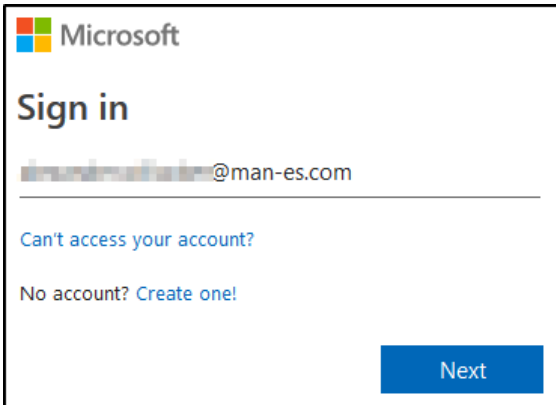
We recommend configuring your second factor before using applications that requires a two-factor authentication.

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:

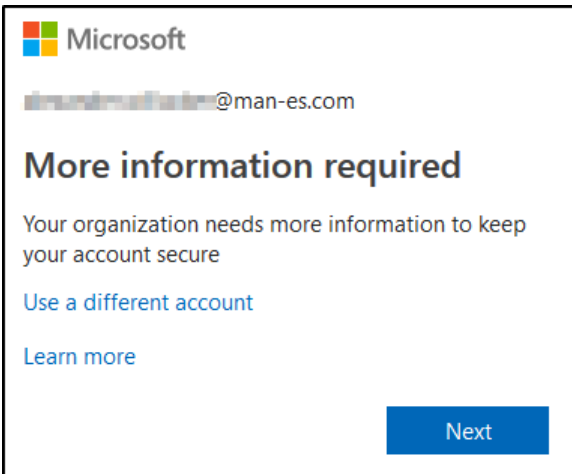
<https://account.activedirectory.windowsazure.com/proofup.aspx?proofup=1&whr=mdt-ext.biz>

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

The screenshot shows the 'Additional security verification' setup page. At the top, it says 'Secure your account by a' followed by a callout bubble: 'When selecting mobile app ...'. Below this is a link: 'new video to know how to secure your account'. The main heading is 'Step 1: How should we contact you?'. There is a dropdown menu with 'Mobile app' selected. Below that, a question asks 'How do you want to use the mobile app?' with two radio button options: 'Receive notifications for verification' and 'Use verification code'. A callout bubble points to the first option: '.. you can choose if you want to type the verification code shown on your phone (Use verification code) or if you just want to click "confirm" on your phone during logon (Receive notifications)'. At the bottom, there is a 'Set up' button and a note: 'Please configure the mobile app.' A green callout bubble points to the 'Set up' button: 'Note: The easiest way to use Azure MFA is probably the Mobile App with "Receive Notifications".'

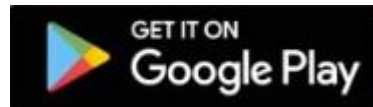
When you click on the "Set up" button you will be guided through the Mobile App setup process.

Please download the app in the Appstore and Google Play.

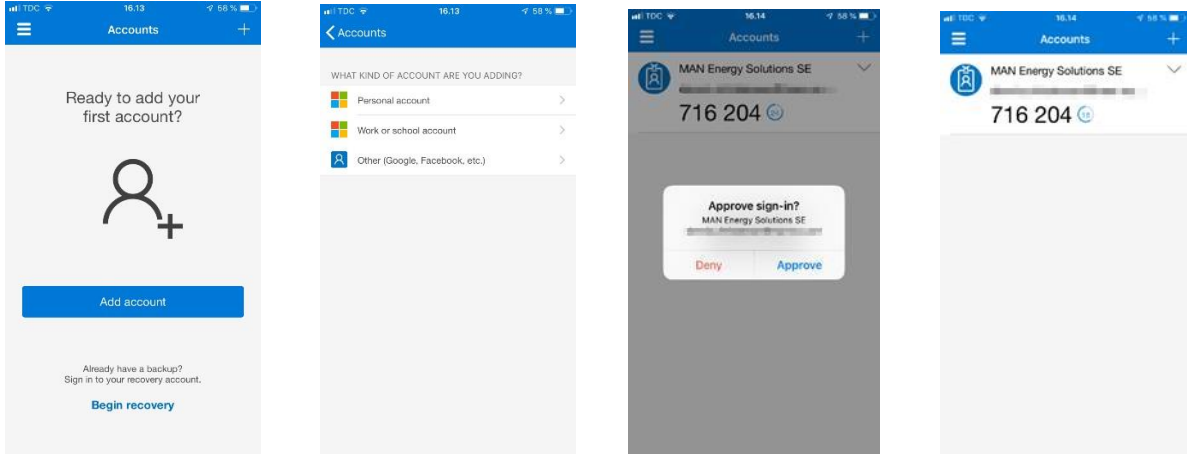
Just scan the QR-Code – after that continue with Step 2

[App at Apple AppStore](#)

[App at Android Google Playstore](#)



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

Personal security verification

Secure your account by adding phone verification to your password. [View video to know how to secure](#)

Step 1: How should we contact you?

Authentication phone

Germany (+49)

Method

Call me

Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply.

Choose between different factor types, like phone call or Mobile App.

When selecting office phone, the phone number is not changeable.
When selecting Authentication Phone you can change the phone number (your mobile work number is preselected).



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

Step 2: Let's make sure that we can reach you on your Office Phone

• We are now trying to reach your office phone at +49 (821) [REDACTED]. Please follow the instructions on your phone.

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

Step 2: Let's make sure that we can reach you on your Office Phone

Verification successful!

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

2.3 Manage or Modify URL:

Additional security verification

When you sign in with your password, you are also required to respond from a registered device. This makes it harder for a hacker to sign in with just a stolen password. [View video to know how to secure your account](#)

what's your preferred option?
We'll use this verification option by default.

how would you like to respond?
Set up one or more of these options. [Learn more](#)

- Authentication phone
- Office phone
- Alternate authentication phone
- Authenticator app or Token

Authenticator app -

Your phone numbers will be used for account security. Standard telephone and SMS charges will apply.

Callouts:

- Change default method.
- By selecting/deselecting a checkbox you can configure or remove a factor.
- Set up Authenticator app
- You can add additional mobile apps here.
- These are your already configured mobile apps.
- Click Save when you are finished.

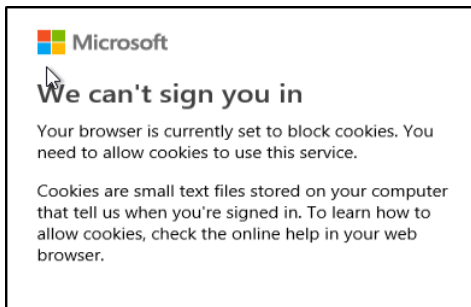
Contact your admin if you need to update your office number. Do not use a Lync phone.

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

