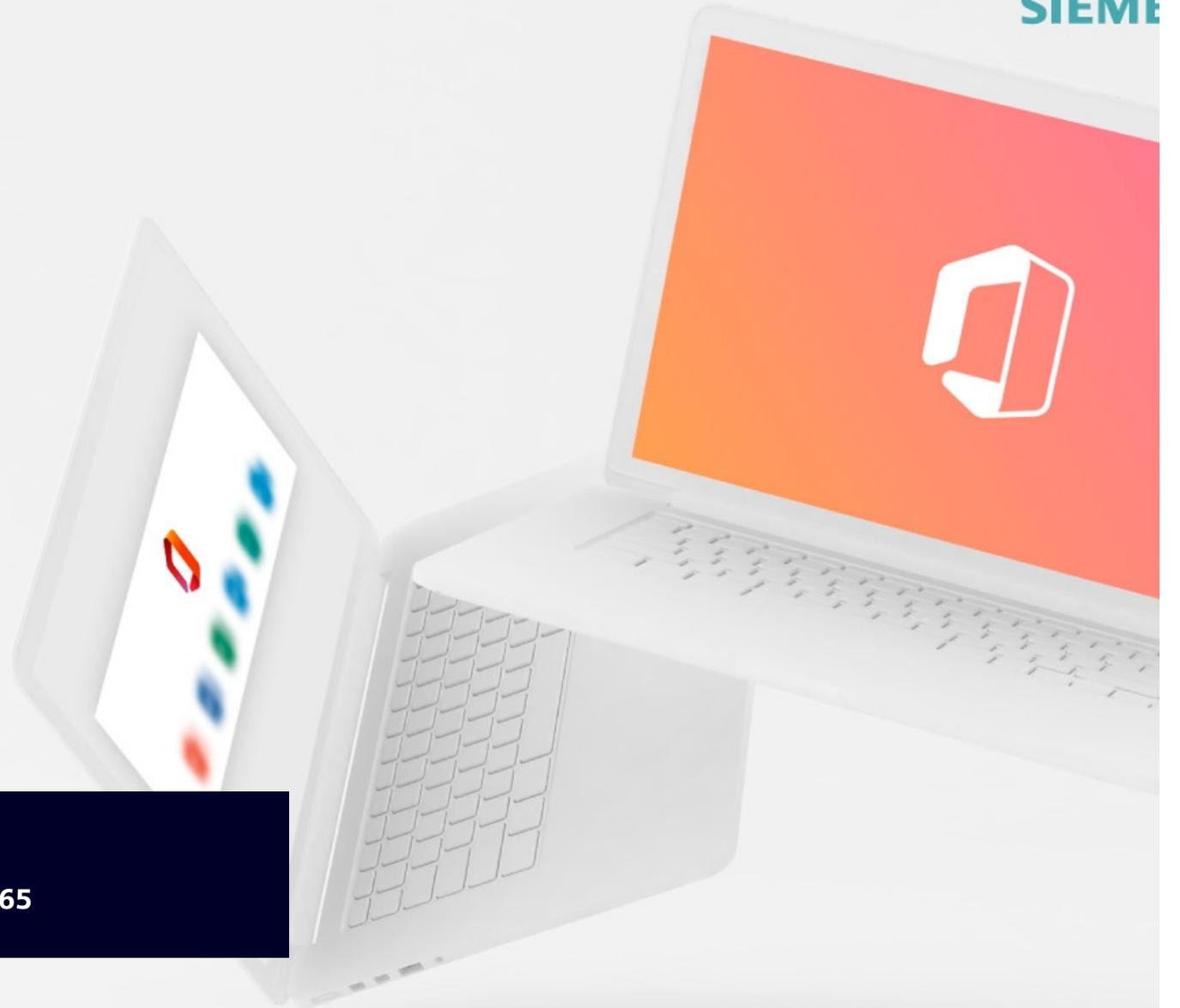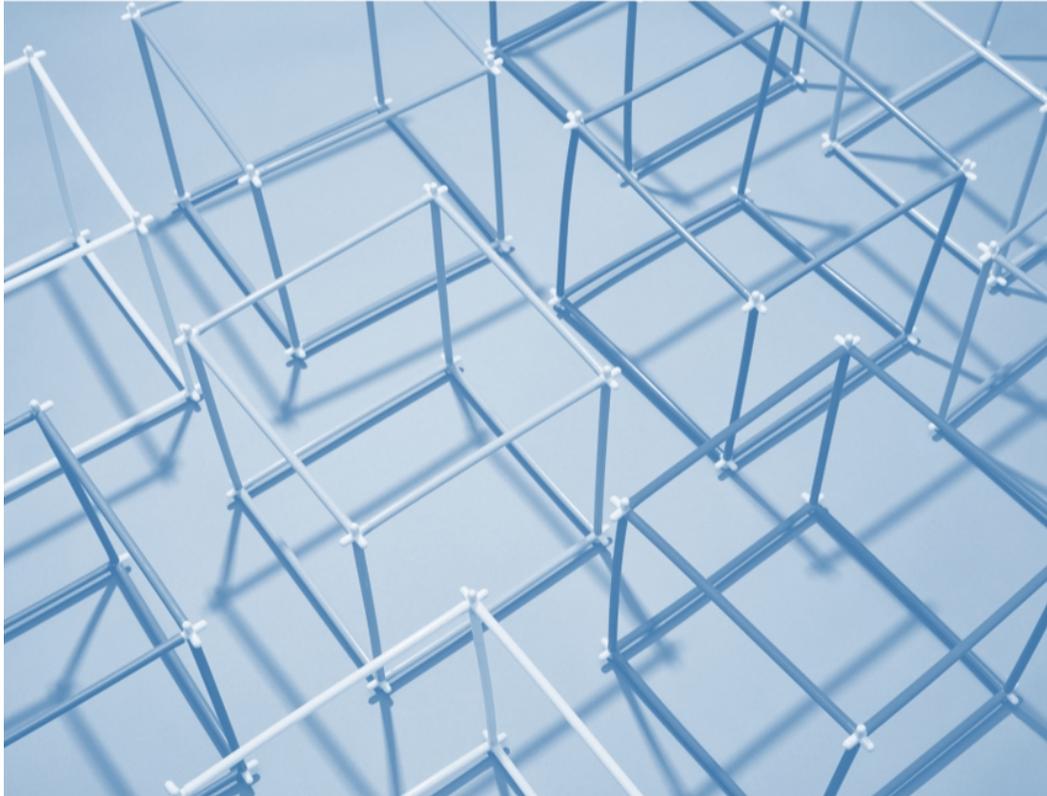# Microsoft MFA Setup Guide

Multi-Factor Authentication for Microsoft 365

Microsoft MFA Setup Guide

This guide provides you with information about the installation and configuration of Microsoft MFA.

What is Microsoft MFA? – page 3

Setup MFA
- Microsoft Authenticator App – page 4

How does Microsoft MFA work? – page 13

What is Microsoft MFA?

Microsoft Multi-Factor Authentication (MFA) helps to prevent unauthorized access to accounts by adding an additional level of security.

You will be prompted to use MFA when:
- Accessing M365 apps on a non-Siemens device.
- When suspicious user activity is detected.
- When an unsupported browser or incognito mode is used.

MFA can be completed by using one of the following:
•Microsoft Authenticator app (mobile app)
•Windows Hello for Business (Biometric or PIN)
•FIDO2 Security Key (USB Key)
•Smart OTP app (desktop app)
•PKI/Certificate Based Authentication

What is Microsoft MFA?

We highly recommend you use the Microsoft Authenticator App, since it's the most convenient & secure solution.

You'll be able to check instructions in the next pages of this UseIT Manual.

In case you want to use the SmartOTP app on your desktop, click right here >>>
In case you want to use Windows Hello for Business, click right here >>>
In case you want to use FIDO2, click right here >>>

MFA | Setup Requirements

MFA setup is only possible from a "Trusted Device" of Siemens AG Tenant, such as Accenture Client, Atos Client or Atos Virtual Client. For more information on a Trusted Device, see here.
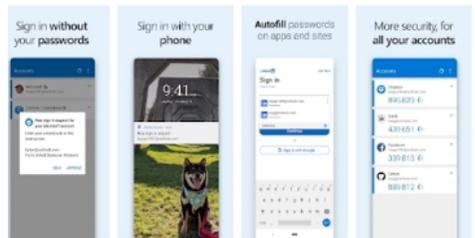
Microsoft Authenticator App

When using the Microsoft Authenticator mobile app for the additional two-step MFA security verification, it can work in one of the two ways:

• **Notification.** After you enter the username and password in the browser or Office application, a two-digit number (e.g. 51) will be shown on your computer screen and you will have to enter this number in the Microsoft Authenticator app.

• **Verification code.** After you enter the username and password in the browser or Microsoft application, you need to open the Authenticator app on your phone and enter the provided verification code from the app you are signing in.
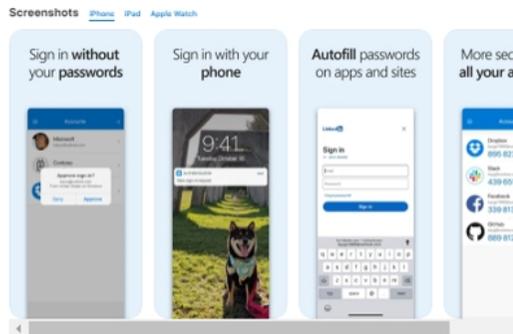
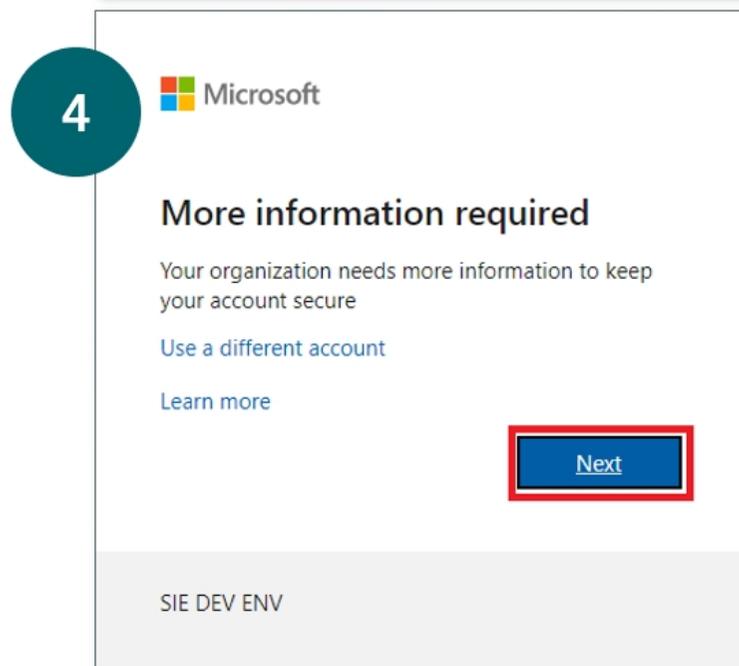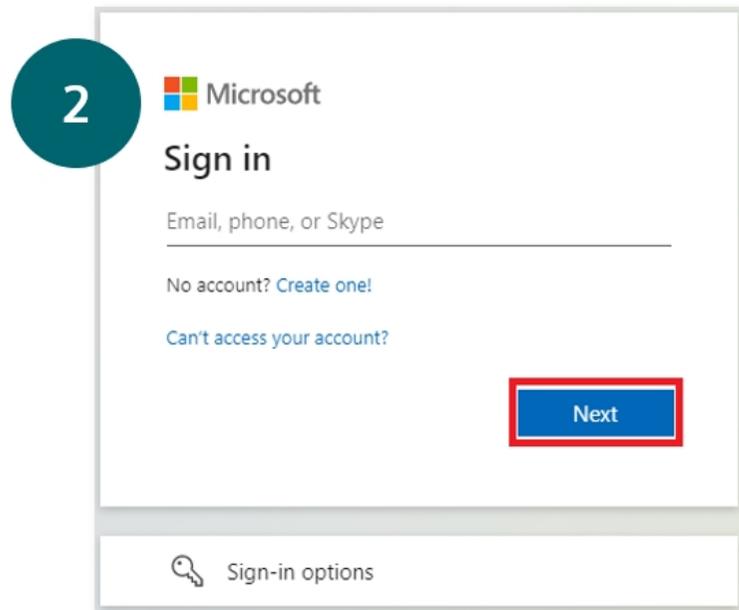*The verification code can also be used when the device has no internet connection (offline).*

Microsoft Authenticator app Installation

The Microsoft Authenticator app is available for Android and iOS. Search for it via the Google Play Store or Apple AppStore on your smartphone.

NOTE
- Android version 4.2 or newer is required.
- iOS version 9.0 or newer is required.
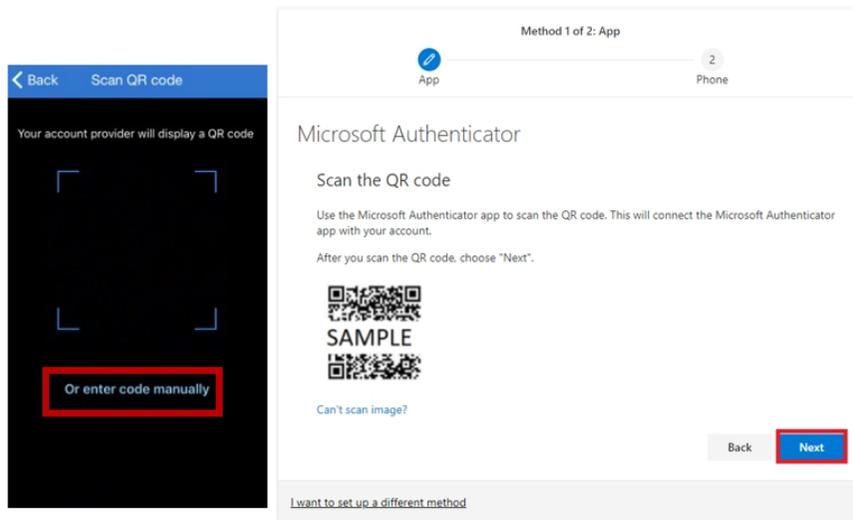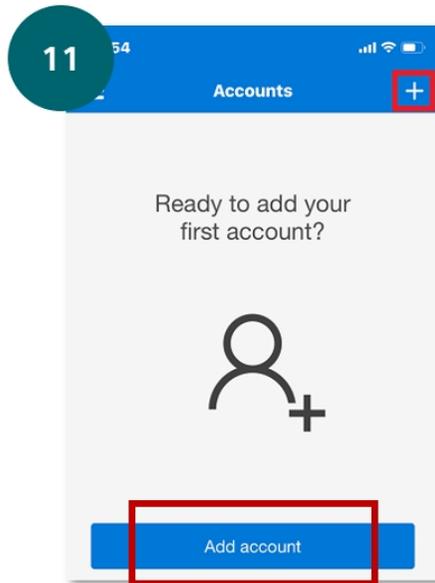
Microsoft Authenticator app Configuration 1/6

This chapter will guide you through how to add your work account to the app. The following screenshots show the initial setup process.

1. Please open the internet browser on your computer or another device (not on the smartphone where you will configure the Authenticator app). Then, navigate to the **Additional security verification page** (**https://mysignins.microsoft.com/security-info**).

2. Sign in with your **Siemens e-mail address**.

3. Click on **Next**.

4. A window like the one on the left will then be shown (it is possible that you will need to enter your Windows password as well).

5. Click on **Next**.
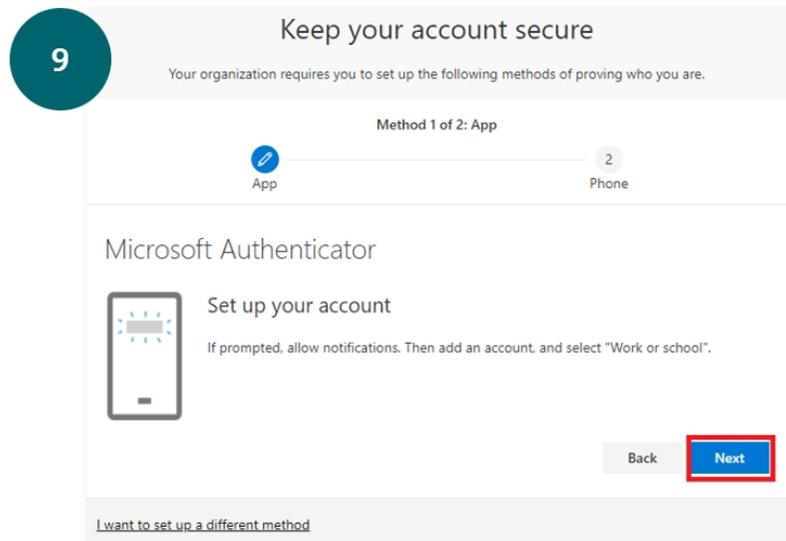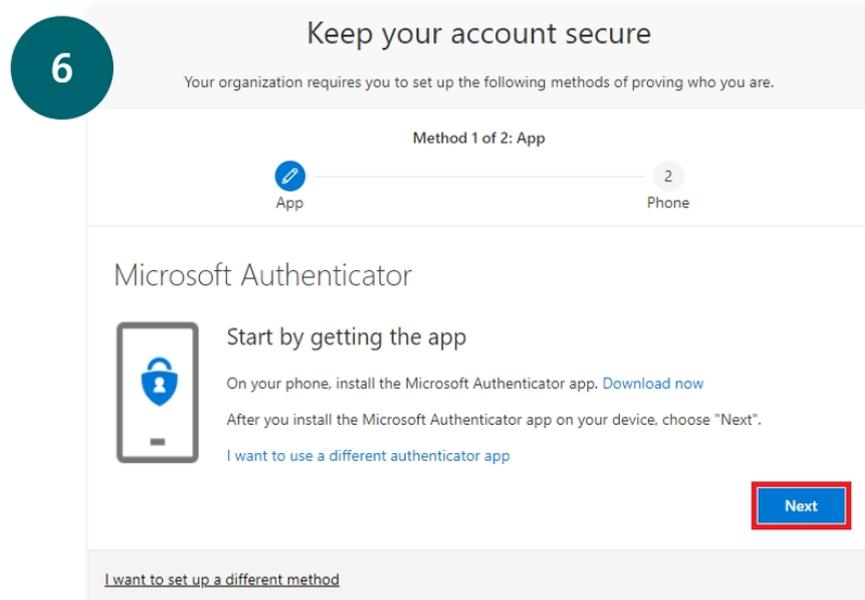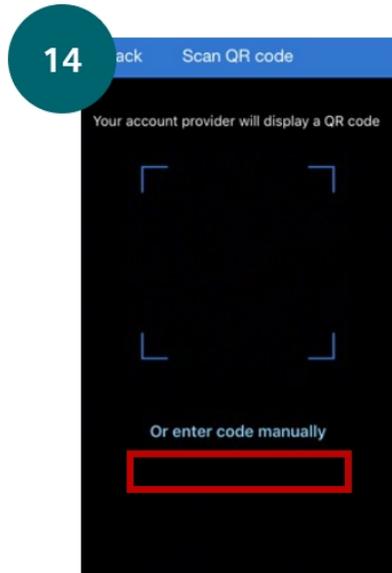
Microsoft Authenticator App Configuration 2/6

6. A window like the one on the left will appear.

7. Please select to setup the **Microsoft Authenticator app (strongly recommended)**.

8. Ensure you have installed the app and click on **Next**.

9. Click on **Next**.

Microsoft Authenticator App Configuration 3/6

10. Open the **Microsoft Authenticator app** on your smartphone.

11. On the Accounts screen, select **"+"** or **Add account**.

12. Then select **Work or school account**.

13. Choose the option to scan QR code and use your device's camera to scan the QR code shown in your browser. It may ask you to allow the app access to photos. Click **Accept**. With some phones, you may have to go into the settings to allow the app to use the camera. And click **Next**.

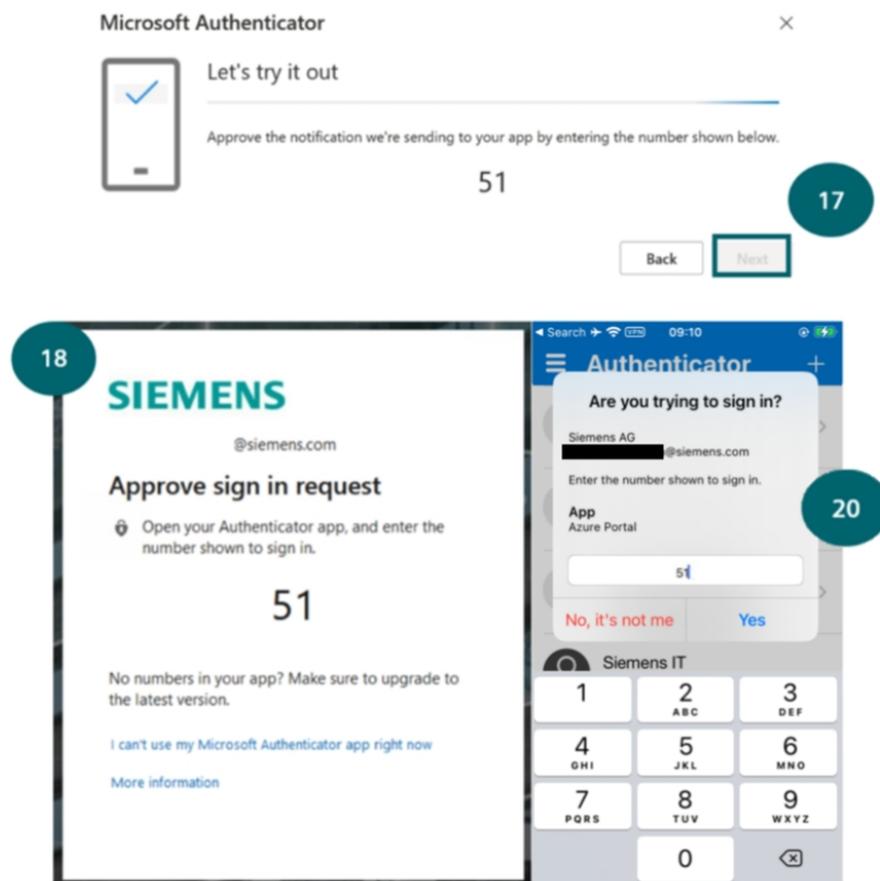**If you cannot use your phone's camera**, please see the next page.

Microsoft Authenticator App Configuration 4/6

If you cannot read QR codes you will need to add an account to the app manually.

14. In the QR scanner screen, select **"Or enter code manually"**.

15. Enter the code and URL from the screen with the QR code into the **Add an account** screen, and then click **Finish**.

Microsoft Authenticator App Configuration 5/6

16. Your account will be added automatically to the app and a six-digit code will be display. You can now return to the browser.

17. On your computer, click **Next** in the bottom right corner.

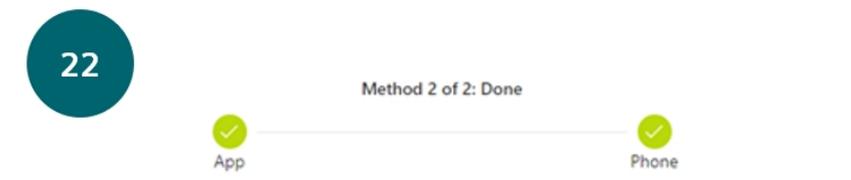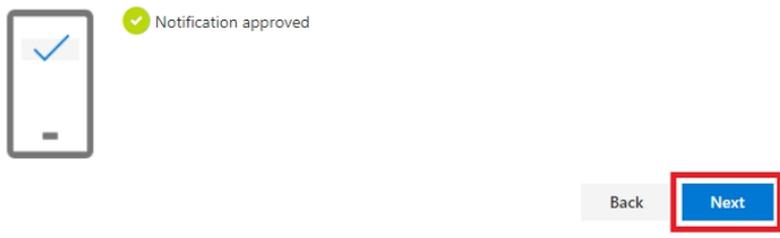18. A window like the one on the left will appear and you will receive a prompt on your mobile device.

19. In the Authenticator app on your mobile device, wait for the prompt. (if no prompt appears, refresh by using the "pull down" gesture in the app).

20. If the prompt appears, enter the two-digit number (e.g. 51) that appears on the computer screen and enter the two-digit number into the Microsoft Authenticator App

21

Method 1 of 2: App

App — 2 Phone

Microsoft Authenticator

✓ Notification approved

Back | **Next**

22

Method 2 of 2: Done

App — Phone

Success!

Great job! You have successfully set up your security info. Choose "Done" to continue signing in.

Default sign-in method:

📞 Phone
+4

🔒 Microsoft Authenticator

Done

# Microsoft Authenticator app Configuration 6/6

NOTE
The Accounts screen of the app **shows you your account name and a six-digit verification code.** For additional security, the verification code changes every 30 seconds, preventing you from using the same code twice. You can use this code when your mobile device does not have an internet connection.

21. After successfully approving the setup notification, you should see the window on the left, you can click on **Next**.

22. At this point, your verification should be successful.

Once you are shown a window like the one on the left, the configuration process is complete. Click on **Done** to finish the process.
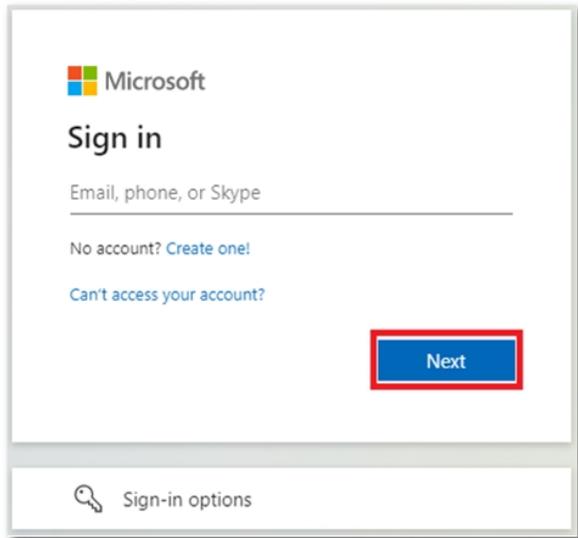
How does Microsoft MFA work? 1/3

Provide your username and password.

How does Microsoft MFA work? 2/3

You will be asked to approve a sign-in request on your phone. Once you have completed this step, you will be signed in.

SIEMENS

███████████ @siemens.com

Verify your identity

Use a certificate or smart card

Approve a request on my Microsoft Authenticator app

`123` Use a verification code

Text +XX XXXXXXXXX40

More information

Are your verification methods current? Check at
https://aka.ms/mfasetup

Cancel

How does Microsoft MFA work? 3/3

OPTIONAL:
Should you not be able to complete MFA, you can choose **Sign in another way** and use one of the following MFA options.

• If the **verification code** from the mobile app is chosen, you will need to enter the code from the app. This option works even if there is no network or internet connection (offline).

• If Use a certificate or smart card is selected, you must enter the PIN of the inserted smart card.

• If **text message** is chosen, a code will be sent to your phone by text message. This code then needs to be entered on your computer.

Note: Text message based authentication method will be discontinued soon.

More information

- [MFA page](#)
- [FAQ](#)

Support
In the case of technical problems, please contact your [IT Service Desk](#).