Multi-Factor-Authentication for Microsoft 365
Introduction

Multi-Factor-Authentication (MFA) increases the security of a user's own account by implementing an additional security factor besides the password. This increased user account security serves, among other things, to effectively combat phishing mails.

All information provided in connection with MFA (e.g., telephone number) is used exclusively for MFA.

We recommend that you use the "Microsoft Authenticator" app to set MFA up:
• for iOS go to slide 3
• for Android go to slide 18

If you have any questions or problems, please contact the PC tutors by email (tutor@unisg.ch).
MFA setup with iOS and Microsoft Authenticator
Setting up MFA on your computer (1/3)

Open Office
Use the following link to open the Office portal in an InPrivate or incognito window of a browser.
https://www.office.com/
Click on "Log in".

Enter email address
Enter your UNISG email address and click "Next".
Enter password
Enter the password of your UNISG account and click "Log in". After logging in, you may see a gray "Log in to access this site" window. Enter your UNISG email address and password again here and click "OK".

Further information required
You will now receive a message that further information is required to protect your account. You have the option to skip the MFA setup for now and perform it within the next 14 days. **We recommend that you perform the setup directly.** To do so, click on "Next".
Setting up MFA on your computer (3/3)

Configure mobile app
Install the Microsoft Authenticator App on your smartphone according to the following steps (see next pages) and add your HSG user account in the app.

Then click on "Next".

Please pick up your smartphone
and follow the steps below
Installation and configuration of the «Microsoft Authenticator» (1/2)

Open the App Store. Tap on the „Search“ Icon. Search for „Microsoft Authenticator“. Install the App. Tap on the Download button. «Open» the Microsoft Authenticator after it has been downloaded.
Installation and configuration of the «Microsoft Authenticator» (2/2)

Tap on the "agree" button. Tap on the «Scan QR-Code» button. To scan the QR-Code the app requires access to your camera. Tap on «OK».

For authentication requests, push notifications are sent to you, which you must confirm. Click "Allow".

Tap on «OK».
Completing the MFA configuration with your smartphone and computer (1/5)

**Complete account setup**
In the previous steps you have already set up your account. Click on "Next".

**Scan QR code**
Now you need your smartphone and your computer.

Scan the QR code displayed on the computer screen with your smartphone.
Then click on "Next".
Completing the MFA configuration with your smartphone and computer (2/5)

Check functionality
After scanning the QR code on your computer screen with your smartphone camera, the connection between your user account and the app will be checked. Wait until a message appears on your smartphone, as it will appear every time you log in with MFA in the future.

*Approve* the login on your smartphone. Then click "Next" on your computer screen.

Notification approved
You will now receive a message on your computer screen that the notification has been approved. Click on "Next".
Completing the MFA configuration with your smartphone and computer (2/5)

**Timeout**
It may occur that during these final steps setting up the app you run into a timeout and cannot complete the setup. Especially if some time passed between the steps (e.g. due to critical tasks you needed to take care of when you were in the middle of the setup). In this case please check if your account appears in the app.

- If no, just restart the setup.
- If yes, please go to this page which always triggers a MFA request: [My Sign-Ins (microsoft.com)](https://microsoft.com)
  - If the MFA request appears on your mobile phone the setup is completed (even though during the setup process the test request was not sent and instead it ran into a timeout).
  - In case you don’t get any MFA notification by requesting this page, please delete your account in the MFA app and start again with the setup.
Completing the MFA configuration with your smartphone and computer (3/5)

Configure Phone
To set up another method for the security check, the “Phone” method is configured. To do this, select the country and enter your phone number. You can either store your cell phone number or also a landline number.

Please read the advantages and disadvantages resulting from the deposited phone number in the table. So you can weigh up for yourself which is the best option for you. Please note that the phone is only used if you cannot authenticate yourself with the app. The app is stored as the default method and will be used first. The phone will only be used if you indicate in the MFA message that you cannot authenticate using your default method and want to fall back on the second method.

Finally, you select whether you want to be called or receive an SMS message.

<table>
<thead>
<tr>
<th>Phone number</th>
<th>Advantage</th>
<th>Disadvantage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cell Phone</td>
<td>Cell phone usually within reach (which is why the app is also stored as the default method). If you don't have internet and can't use the app, you can fall back on calling/SMS to your cell phone.</td>
<td>Two methods on one device: If the phone is not there or the battery is empty, you cannot authenticate yourself</td>
</tr>
<tr>
<td>Landline (Home)</td>
<td>Two methods on two devices: if one device cannot be accessed, authentication takes place via a second device</td>
<td>Less flexible, not possible to authenticate on the go</td>
</tr>
<tr>
<td>Landline (Office)</td>
<td>Two methods on two devices: if one device cannot be accessed, authentication takes place via a second device</td>
<td>Less flexible, not possible to authenticate on the move Due to planned changes in telephony in 2022, this method cannot be used permanently</td>
</tr>
</tbody>
</table>
Check functionality
After the phone is set up, an SMS with a code is sent or a call is triggered, depending on the selected method.

Code entry (SMS) or answering the call.
You will now receive a message on your computer screen that the test authentication via a SMS/call was successful. Click on "Next".
Set up additional factors and change default login method
You have the option to set up additional factors at https://mysignins.microsoft.com/security-info.
Here you also have the possibility to change your preferred verification option at any time.

Congratulations, you have made your account much more secure by setting up MFA!
Completing the MFA configuration with your smartphone and computer (5/5)

Since Apple's own mail program uses a different system, we do not recommend using this program. It is possible that the mail service does not work properly. Unfortunately, we cannot offer support in this area.

If you are already using Apple's native Mail app, the MFA setup process will require you to delete your account and then set it up again.

To delete your account, you would need to follow the steps below:

Settings > Mail > Accounts > Select Account and then click on "Delete Account".

To add an account, please proceed as follows:

Settings > Mail > Accounts > Add account > Microsoft Exchange
MFA Fraud - Report fraud with the Authenticator App

Tap "Decline" if you have not performed a registration yourself.

Tap "Report" if you are sure that another person has made an application.

IT has been informed about the fraud report. The person who performed the login does not get access to your account and receives a message that the request was denied.
MFA Fraud - Report Fraud by Call

| Answer the call. | Enter the "0" and the ",#". Then enter the "1" if you are sure that another person has performed a login. | IT has been informed about the fraud report. The person who performed the login does not get access to your account and receives a message that the request was denied. |

Answer the call.

Enter the "0" and the ",#". Then enter the "1" if you are sure that another person has performed a login.

IT has been informed about the fraud report. The person who performed the login does not get access to your account and receives a message that the request was denied.
MFA setup with Android and Microsoft Authenticator
Setting up MFA on your computer (1/3)

Open Office
Use the following link to open the Office portal:
https://www.office.com/
Click on “Log in.”

Enter email address
Enter your UNISG email address and click “Next.”
Enter password
Enter the password of your UNISG account and click "Log in". After logging in, you may see a grey "Log in to access this site" window. Enter your UNISG email address and password again here and click "OK".

Further information required
You will now receive a message that further information is required to protect your account. You have the option to skip the MFA setup for now and perform it within the next 14 days. We recommend that you perform the setup directly. To do so, click on "Next".
Setting up MFA on your computer (3/3)

Configure mobile app
Install the Microsoft Authenticator App on your smartphone according to the following steps (see next pages) and add your HSG user account in the app.

Then click on "Next".

Please pick up your smartphone

And follow the steps below
Installation and configuration of the «Microsoft Authenticator» (1/2)

Open the Play Store. Tap on the search box Search for «Microsoft Authenticator».

Install the app. Tap on «Install». «Open» the Microsoft Authenticator after it has been downloaded.
**Installation and configuration of the «Microsoft Authenticator» (2/2)**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Tap on the “agree” button.</td>
</tr>
<tr>
<td>2</td>
<td>Tap on the «Scan QR-Code» button.</td>
</tr>
<tr>
<td>3</td>
<td>To scan the QR-Code the app requires access to your camera. Tap on «OK».</td>
</tr>
<tr>
<td>4</td>
<td>Tap on «Allow», in order to allow the app to take pictures and to record videos.</td>
</tr>
</tbody>
</table>
Completing the MFA configuration with your smartphone and computer (1/6)

**Complete account setup**
In the previous steps you have already set up your account. Click on "Next".

**Scan QR code**
Now you need your smartphone and your computer.
Scan the QR code displayed on the computer screen with your smartphone.
Then click on "Next".
Completing the MFA configuration with your smartphone and computer (2/6)

Activating the app lock
A notice appears in the Microsoft Authenticator app on your smartphone that App Lock is being activated. Click OK.

Disable battery optimization
You need to disable battery optimization to receive push notifications / notifications without time delay.

Ignore battery optimization
You are informed that deactivation may lead to higher battery consumption. Click on "Allow".
Completing the MFA configuration with your smartphone and computer (3/6)

**Check functionality**
After scanning the QR code on your computer screen with your smartphone camera, the connection between your user account and the app will be checked. Wait until a message appears on your smartphone, as it will appear every time you log in with MFA in the future. “Approve” the login on your smartphone. Then click “Next” on your computer screen.

**Notification approved**
You will now receive a message on your computer screen that the notification has been approved. Click on “Next”.

It may occur that during this or the previous step (scanning the QR Code) you run into a timeout and cannot complete the setup. Especially if some time passed between the steps (e.g. due to critical tasks you needed to take care of when you were in the middle of the setup. In this case please check if your account appears in the app. If no, just restart the setup. If yes, please go to this page.
Completing the MFA configuration with your smartphone and computer (3/6)

Timeout
It may occur that during these final steps setting up the app you run into a timeout and cannot complete the setup. Especially if some time passed between the steps (e.g. due to critical tasks you needed to take care of when you were in the middle of the setup).
In this case please check if your account appears in the app.
• If no, just restart the setup.
• If yes, please go to this page which always triggers a MFA request: My Sign-Ins (microsoft.com)
  • If the MFA request appears on your mobile phone the setup is completed (even though during the setup process the test request was not sent and instead it ran into a timeout).
  • In case you don't get any MFA notification by requesting this page, please delete your account in the MFA app and start again with the setup.
Completing the MFA configuration with your smartphone and computer (4/6)

Configure Phone
To set up another method for the security check, the “Phone” method is configured. To do this, select the country and enter your phone number. You can either store your cell phone number or also a landline number.

Please read the advantages and disadvantages resulting from the deposited phone number in the table. So you can weigh up for yourself which is the best option for you. Please note that the phone is only used if you cannot authenticate yourself with the app. The app is stored as the default method and will be used first. The phone will only be used if you indicate in the MFA message that you cannot authenticate using your default method and want to fall back on the second method.

Finally, you select whether you want to be called or receive an SMS message
Completing the MFA configuration with your smartphone and computer (5/6)

Check functionality
After the phone is set up, an SMS with a code is sent or a call is triggered, depending on the selected method.

Code entry (SMS) or answering the call.
You will now receive a message on your computer screen that the test authentication via SMS/call was successful. Click on “Next”.
Completing the MFA configuration with your smartphone and computer (6/6)

Set up additional factors and change default login method
You have the option to set up additional factors at https://mysignins.microsoft.com/security-info. Here you also have the possibility to change your preferred verification option at any time.

Congratulations, you have made your account much more secure by setting up MFA!
MFA Fraud - Report fraud with the Authenticator App

Tap "Decline" if you have not performed a registration yourself.

Tap "Report" if you are sure that another person has made an application.

IT has been informed about the fraud report. The person who performed the login does not get access to your account and receives a message that the request was denied.
MFA Fraud - Report Fraud by Call

Answer the call. Enter the "0" and the "#". Then enter the "1" if you are sure that another person has performed a login.

IT has been informed about the fraud report. The person who performed the login does not get access to your account and receives a message that the request was denied.