Windows Hello

The goal of Windows Hello

With Windows Hello, Windows devices can be used as a second factor for logging in. Each device added then represents an additional second factor. Adding a Windows device does not affect other second factors such as SMS or OTP. Therefore, if you do not have access to the registered device, you can still use your other 2-factor settings.

Contents of the instructions

These instructions describe the optional use of Windows Hello on devices that are logged in to Windows with a TU work account. Participation is **voluntary**. Only devices connected to a TU account can use Windows Hello.

Please note that passkeys in Windows are sometimes also referred to as master keys. Both terms can be found in the various views and operating system versions.

Requirements

Before Windows Hello can be set up, the following conditions must be met:

- The device is running Windows 10 or Windows 11 (recommended: Windows 11, Windows 10 has very few displays for passkeys).
- MFA must be enabled for the account. Activation should be performed on a laptop or desktop, as problems may arise if the process is performed exclusively on a smartphone.
- The device has at least TPM 1.2
- The device has a supported authentication method (e.g., fingerprint sensor, facial recognition, etc.).

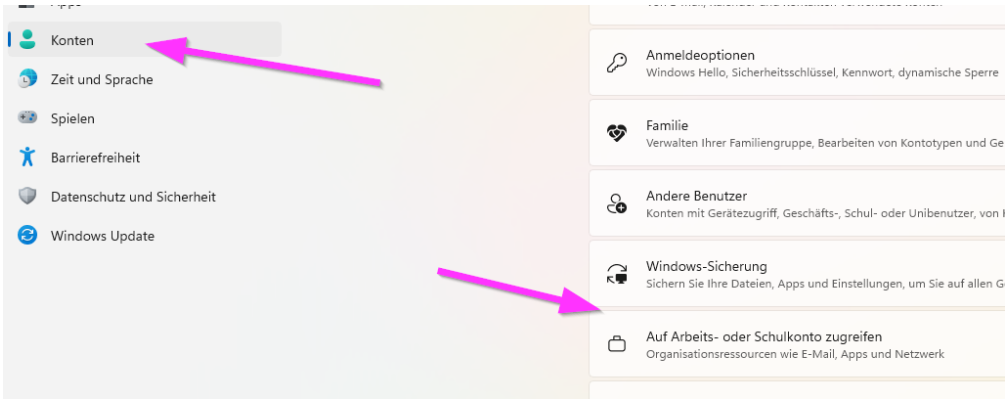
It is also recommended that

- If the device is already connected to the TU work account, it is recommended to disconnect it before setting up Windows Hello. To do this, select "Access work and school accounts" and then "Disconnect" for your account.

IMPORTANT: The following steps must **not** be performed via a **remote desktop connection**. Windows 11 blocks the setting of certain security settings during an RDP session or VPN connection to avoid potential risks. This can result in the linked account being removed and the entire setup process having to be repeated.

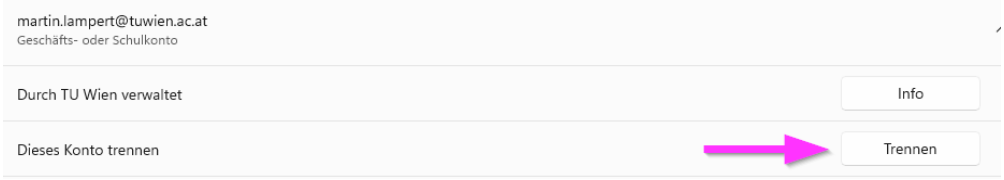
Setting up Windows Hello

1. Open "**Settings**."
2. Select "**Access work or school account.**"



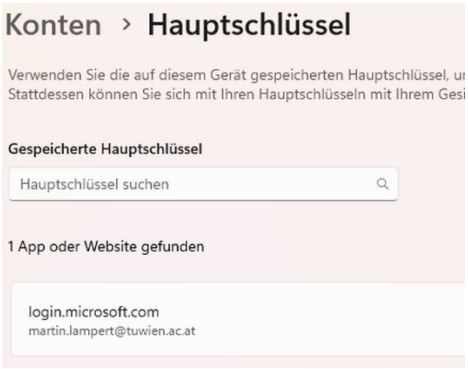
3. If your account is already connected:

- Click the drop-down button next to your account and select "**Disconnect this account**" → "**Disconnect**."



- Wait until the account has been completely disconnected. **This may take several minutes**.

4. Now connect your account to the device by clicking on "**Add work or school account**" → "**Connect**."
5. Enter your TU email address here (employeesvorname.nachname@tuwien.ac.at , studentsexxxxxxxx@student.tuwien.ac.at) and confirm your login via MFA. **This may take several minutes**.
6. Once the account has been reconnected to the device, a passkey master key will now be added to your device under "**Settings**" - "**Accounts**" - "**Master Key**" (Windows 11 only).



Important: Adding the master key will **disable** the device PIN by default, as it must be reauthorized.

7. Therefore, select "**Sign-in options**" under "**Accounts**."
8. Open the "**PIN**" option via the drop-down icon
9. You will see a display that looks like this and unfortunately has a very misleading title:

10. Click on "**This PIN does not work with your organization's resources**." You will now be prompted to reauthorize yourself on the device.
11. Once this has been successfully completed, the PIN will be reactivated.

    Important: This is the same PIN that you previously activated on the device.

12. By adding the master key, you will now be automatically verified via your device on all pages and accounts that are authenticated via Microsoft.

    Important: You may need to authenticate yourself again on your local O365, OneDrive, or Teams by clicking on your user. This only takes a few seconds and is also done using your stored master key.

Troubleshooting

If the setup or login does not work, the following steps may help:

- Settings → Accounts → Access work or school account → Check connection

- Ensure that all system updates are installed.
- Remove the current PIN or function in the login options and set it up again.
- If in doubt, completely disconnect the account and set it up again.
- Check that the camera or fingerprint sensor is working properly.
- If the error message "Something went wrong, please try again later" appears under "PIN," do **not** click "Remove," as this will remove the device PIN. Instead, disconnect the account and add it again as described above.
- If no master key is added and Windows Hello only displays "This option is currently unavailable" for all Windows Hello sign-in options, your device either does not support TPM 1.2 or the biometric sign-in devices are not sufficiently secure.
- If you do not have MFA, you can connect the device via "Connect account," but Windows Hello will not apply the policies at this point, as MFA is a prerequisite.

If an error occurs, you can check why activation failed at the following URL:

- https://shop.tusoftware.tuwien.ac.at:8888/get_mfa_report

Optional (additional) setup of a security key (passkey) on your smartphone

With this option, you have a passkey on your mobile phone that you can use on any laptop or desktop (on all operating systems) with Bluetooth. A passkey can therefore be used for all end devices and your mobile phone becomes a shared key (like an external hardware token); Windows Hello is not necessary in this case.

1. Install the **Microsoft Authenticator app** on your mobile device
2. Open the settings and go to passkey management
    a. On Android, for example, this is "Passwords, Passkeys & Accounts," "Passwords & Accounts," "Passwords & Autofill" – here now "Passwords & Passkeys" or "Passkey Providers" and select Microsoft Authenticator
    b. Detailed setup instructions for **iOS** can be found at: https://learn.microsoft.com/de-de/entra/identity/authentication/how-to-register-passkey-authenticator?tabs=iOS
    c. And for **Android** at: https://learn.microsoft.com/de-de/entra/identity/authentication/how-to-register-passkey-authenticator?tabs=Android
3. Now open Microsoft Authenticator on your device.
4. Select "Add Account" – "Work or School Account" and log in.
5. Select "Create Passkey."
6. You may now need to authenticate again using **MFA** or, if you haven't already done so, set up a screen lock on your device.

It is possible to activate the passwordless function when using the Microsoft Authenticator app. A detailed description of this can be found at:

https://support.microsoft.com/en-us/account-billing/how-to-go-passwordless-with-your-microsoft-account-674ce301-3574-4387-a93d-916751764c43

Important: The password itself cannot be deleted or disabled as an option.

Support and contact

Please note that Windows Hello is an optional feature. The service center is aware of this feature, but does **not** provide **individual support** for setting up or using Windows Hello.