

Please note that the English version of this document has been machine-translated and has not been reviewed for errors. The English version is therefore intended to improve accessibility for individuals with limited knowledge of German; however, in case of doubt, the content of the German version is binding.

Adding a Passkey / Master Key

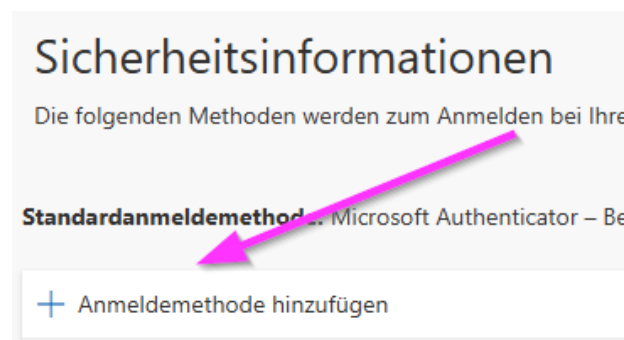
This quick guide provides step-by-step instructions on how to add a passkey or master key to your MFA profile. For a more comprehensive guide covering all methods, please visit: https://service.it.tuwien.ac.at/swsupport/docus/windowshello/mfa_handbuch.pdf

A **passkey**, also known as a master key, offers better protection than SMS, for example, and enables secure, password-free login. It can be used with various devices, such as smartphones, PCs, hardware security keys, or password managers like KeepassXC or 1Password. Depending on the provider, passkeys can also be securely synchronized across multiple devices.

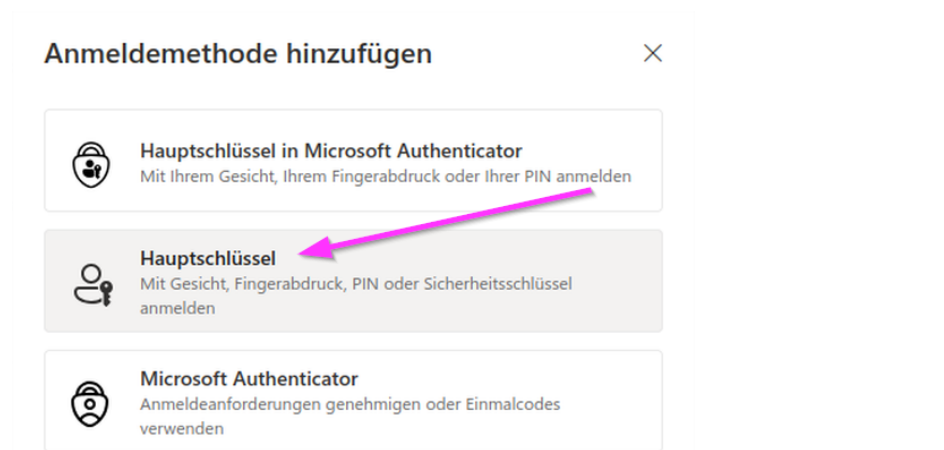
A passkey is available on Windows, Android, Apple, and Linux. It can also be used via browsers such as Chrome, Firefox, or Safari. However, since these are third-party products, no support can be provided for them.

1 Setting Up Passkey in Your Account

- Step 1: Go to <https://mysignins.microsoft.com/security-info>
- Step 2: Log in with your username and password.
- Step 3: Select **“Add Login Method”**



- Step 4: Select **“Master Key”** as the method.



- Step 5: Confirm the pop-up by clicking **“Next.”**

Sign in faster with your face, fingerprint, or PIN



Erstellen Sie einen Hauptschlüssel, um sich bei Ihrem Konto anzumelden. Es sind keine Apps, Kennwörter oder Codes erforderlich.

Zurück

Weiter

- Step 6: Setup will now continue in a separate window. Please complete the steps in this window; if the process does **not** continue automatically, confirm by clicking **“Next.”**

Ihr Hauptschlüssel wird eingerichtet...

Ihr Gerät öffnet ein Sicherheitsfenster. Befolgen Sie die Anweisungen, um die Einrichtung Ihres Hauptschlüssels abzuschließen.

• • • • •

Abbrechen

Weiter

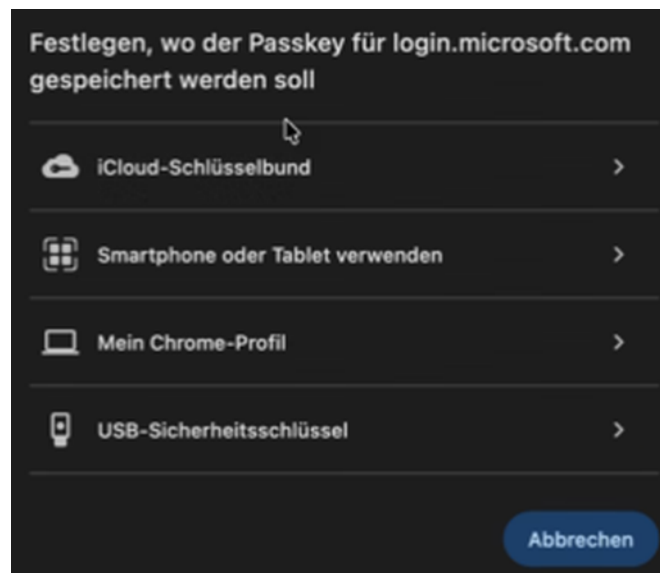
- Step 7: A pop-up will now open suggesting a method. Click “**Save differently**” here to view all options.

Einen Passkey zur Anmeldung in login.microsoft.com erstellen?

Du kannst diesen Passkey verwenden, um dich auf deinen Geräten schneller anzumelden. Er wird im Google Passwortmanager für gespeichert.



- Step 8: Now specify where the passkey should be stored. Depending on your device, there are numerous options available (e.g., Windows Hello, KeePass, USB security key, smartphone, tablet, Google Key Vault, iCloud, Chrome, KeePassXC, 1Password, etc.). The image shown here is for illustrative purposes only. Please keep privacy and security concerns in mind when using the various options.



- Step 9: Finally, give your master key a name so you can find it more easily in the list, and confirm by clicking **“Next.”**

Ihren Hauptschlüssel benennen

×



Geben Sie Ihrem Hauptschlüssel einen Namen, damit Sie ihn später leichter identifizieren können.

Weiter

- Step 10: The master key has now been created and can be used for all MFA logins in the future.

✓ Hauptschlüssel erstellt

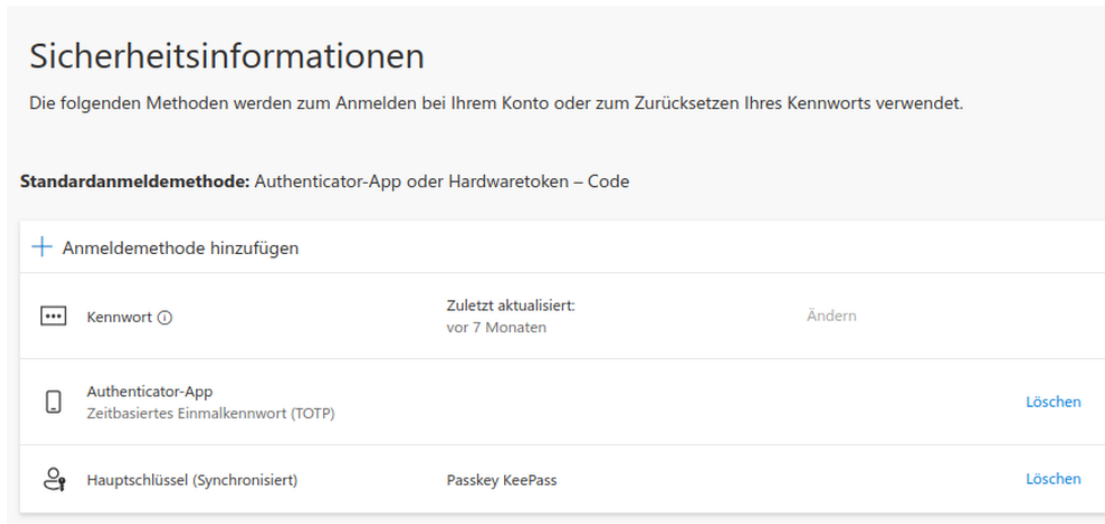


Sie können sich jetzt mit Ihrem Gesicht, Fingerabdruck oder Ihrer PIN bei Ihrem Konto anmelden.

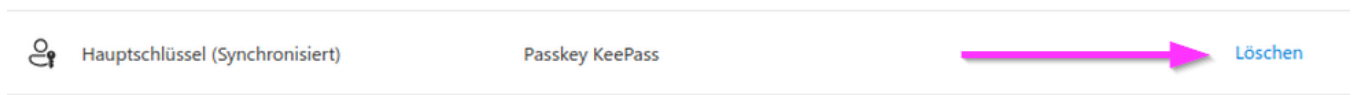
Fertig

2 Overview and Deletion:

- To view your existing MFA methods (and passkeys), go to <https://mysignins.microsoft.com/security-info>



- To delete an existing passkey, simply click the “Delete” button on the right.



3 Troubleshooting:

3.1 No access to the stored MFA method

If you no longer have access to your registered device or method:

- Use an **alternative stored MFA method** (e.g., backup code or a second app).
- If no alternative method is available, contact **IT support** to have your access reset.

3.2 MFA fails for unknown reasons

If you do not receive a clear error message but are still prompted to use MFA, please visit the following URL before creating a ticket:

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

There, you'll see a list of possible causes that could be limiting your ability to use the desired MFA method.

4 Support and Contact

If you encounter any issues while setting up or using Passkeys, please contact IT Support via the ticket system (for employees only) at <https://support.tuwien.ac.at/assystnet/> or by email athelp@it.tuwien.ac.at. If you are having trouble creating a Passkey, please include a screenshot of the MFA report mentioned above. Of course, you can also contact the Service Center by phone.