Windows Hello

Ziel von Windows Hello

Mit Windows Hello können Windows-Endgeräte als zweiter Faktor bei der Anmeldung genutzt werden. Jedes hinzugefügte Gerät stellt dann einen weiteren zweiten Faktor dar. Das Hinzufügen eines Windows-Geräts beeinflusst andere zweite Faktoren wie SMS oder OTP nicht. Sollten Sie daher einmal keinen Zugriff auf das angemeldete Gerät haben, können Sie weiterhin Ihre anderen 2-Faktor-Einstellungen nutzen.

Inhalt der Anleitung

Diese Anleitung beschreibt die optionale Nutzung von Windows Hello auf Geräten, die mit einem TU-Arbeitskonto unter Windows angemeldet sind. Die Teilnahme ist **freiwillig**. Nur Geräte, die mit einem TU-Konto verbunden sind, können Windows Hello verwenden.

Bitte beachten Sie, dass Passkeys in Windows teilweise auch als Hauptschlüssel bezeichnet werden. Beide Begriffe sind in den verschiedenen Ansichten und Betriebssystemversionen zu finden.

Voraussetzungen

Bevor Windows Hello eingerichtet werden kann, müssen folgende Bedingungen erfüllt sein:

- Das Gerät läuft unter Windows 10 oder Windows 11 (empfohlen: Windows 11, Windows 10 hat nur sehr wenige Anzeigen für Passkeys).
- Für das Konto muss MFA zwingend aktiviert werden. Die Aktivierung sollte auf einem Laptop oder Desktop erfolgen, da es zu Problemen kommen kann, wenn der Vorgang ausschließlich auf einem Smartphone durchgeführt wird.
- Das Gerät verfügt mindestens über TPM 1.2
- Das Gerät verfügt über eine unterstützte Authentifizierungsmethode (z.B. Fingerabdrucksensor, Gesichtserkennung, ...)

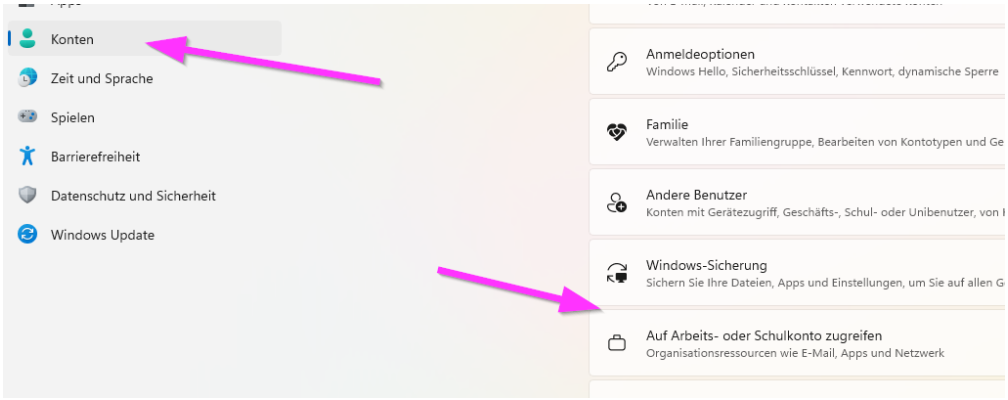
Zudem wird empfohlen

- Sollte das Gerät bereits mit dem TU-Arbeitskonto verbunden sein, so wird empfohlen, dieses vor Einrichtung von Windows Hello zu trennen. Wählen Sie dazu den Punkt „Auf Arbeits- und Schulkonto zugreifen“ und dann bei Ihrem Konto den Punkt „Trennen“.

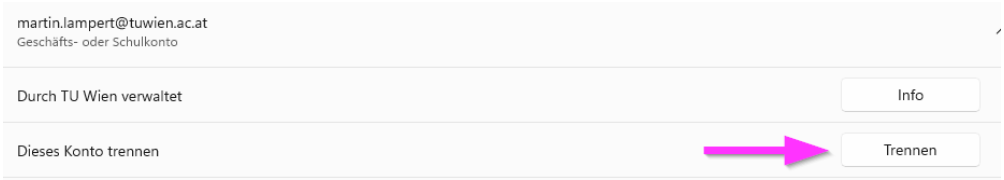
WICHTIG: Die folgenden Schritte dürfen **nicht** über eine **Remote-Desktop-Verbindung** ausgeführt werden. Windows 11 blockiert das Setzen bestimmter Sicherheitseinstellungen während einer RDP-Sitzung oder VPN-Verbindung, um mögliche Risiken zu vermeiden. Dies kann dazu führen, dass das verknüpfte Konto entfernt und der gesamte Einrichtungsprozess erneut durchgeführt werden muss.

Einrichtung von Windows Hello

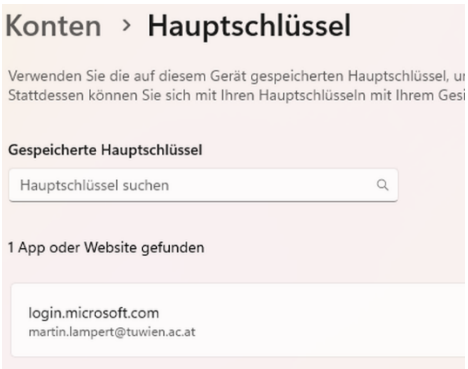
1. Öffnen Sie den Punkt "**Einstellungen**".
2. Wählen Sie den Punkt "**Auf Arbeits- oder Schulkonto zugreifen**"



3. Sollte Ihr Konto bereits verbunden sein:
    - Klicken Sie auf den Dropdown-Button neben Ihrem Account und wählen Sie den Punkt "**Dieses Konto trennen**" → "**Trennen**"



    - Warten Sie, bis das Konto komplett getrennt wurde. **Dies kann mehrere Minuten dauern**.
4. Verbinden Sie Ihr Konto nun mit dem Gerät, in dem Sie auf "**Geschäfts-, Uni- oder Schulkonto hinzufügen**" - "**Verbinden**" klicken.
5. Geben Sie hier ihre TU E-Mail-Adresse ein (Mitarbeitende vorname.nachname@tuwien.ac.at, Studierende exxxxxxxx@student.tuwien.ac.at) und bestätigen Sie die Anmeldung via MFA **Dies kann mehrere Minuten dauern**.
6. Sowie der Account neu mit dem Gerät verbunden wurde, wird Ihrem Gerät unter "**Einstellungen**" - "**Konten**" - "**Hauptschlüssel**" (nur Windows 11) nun ein Passkey-Hauptschlüssel hinzugefügt.



Wichtig: Durch das Hinzufügen des Hauptschlüssels wird standardmäßig der Geräte-Pin **deaktiviert**, da dieser neu autorisiert werden muss.

7. Wählen Sie daher hier nun unter dem Punkt "**Konten**" den Punkt "**Anmeldeoptionen**" aus
8. Öffnen Sie hier den Punkt "**PIN**" via Dropdown-Symbol
9. Sie erhalten hier eine Anzeige die folgendermaßen aussieht und leider sehr irreführend betitelt ist:

10. Klicken Sie auf "**Diese Pin funktioniert nicht mit Ressourcen Ihrer Organisation**". Sie werden nun dazu aufgefordert, sich am Gerät neu zu autorisieren.
11. Sowie dies erfolgreich abgeschlossen ist, wird der PIN wieder aktiviert.

    Wichtig: Es handelt sich dabei um denselben Pin, den Sie bereits zuvor am Gerät aktiviert hatten.

12. Durch das hinzufügen des Hauptschlüssels werden Sie nun bei allen Seiten und Accounts, die via Microsoft authentifiziert werden, automatisch über Ihr Gerät verifiziert.

    Wichtig: Es ist möglich, dass Sie sich bei ihrem lokalen O365, OneDrive oder Teams nochmals via Klick auf Ihren Benutzer authentifizieren müssen. Dies dauert nur wenige Sekunden und erfolgt ebenfalls über Ihren hinterlegten Hauptschlüssel.

Fehlerbehebung

Wenn die Einrichtung oder Anmeldung nicht funktioniert, können folgende Schritte helfen:

- Einstellungen → Konten → Auf Arbeits- oder Schulkonto zugreifen → Verbindung prüfen
- Sicherstellen, dass alle Systemupdates installiert sind.
- In den Anmeldeoptionen die aktuelle PIN oder Funktion entfernen und neu einrichten.
- Im Zweifelsfall das Konto nochmals komplett trennen und neu einrichten.
- Überprüfen, ob Kamera oder Fingerabdrucksensor ordnungsgemäß funktionieren.
- Sollte unter dem Punkt "PIN" die Fehlermeldung "Da hat etwas nicht geklappt, versuchen Sie es später erneut" aufscheinen, klicken Sie bitte **nicht** auf "Entfernen", da dieses sonst den Geräte-Pin entfernt. Trennen Sie stattdessen das Konto und fügen Sie dieses wie oben beschrieben neu hinzu.
- Wird kein Hauptschlüssel hinzugefügt und Windows Hello zeigt nur "Diese Option ist derzeit nicht verfügbar" bei allen Windows-Hello-Anmeldeoptionen an, so unterstützt Ihr Gerät entweder kein TPM 1.2 oder die Biometrischen Anmeldegeräte sind nicht ausreichend sicher.
- Sollten Sie nicht über MFA verfügen, so können Sie das Gerät zwar via "Konto verbinden" verbinden, Windows Hello wird jedoch an dieser Stelle die Richtlinien nicht anwenden, da MFA eine Grundvoraussetzung darstellt.

Unter folgender URL kann im Fehlerfall überprüft werden, warum die Aktivierung gescheitert ist:

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

Optionale (zusätzliche) Einrichtung eines Sicherheitsschlüssels (Passkey) auf dem Smartphone

Mit dieser Option haben Sie einen Passkey auf Ihrem Mobiltelefon, den Sie auf beliebigen Laptops oder Desktops (auf allen Betriebssystemen) mit Bluetooth nutzen können. Ein Passkey ist also für alle Endgeräte einsetzbar und Ihr Mobiltelephon wird zum gemeinsamen Schlüssel (wie ein externer Hardware-Token), Windows Hello ist in dem Fall nicht notwendig.

1. Installieren Sie die **Microsoft Authenticator App** auf Ihrem Mobilgerät
2. Öffnen Sie die Einstellungen gehen Sie zur Passkey-Verwaltung
    a. Unter Android ist dies Beispielsweise „Passwörter, Passkeys & Konten“, „Passwörter & Konten“, „Passwörter & Autofill“ - hier nun „Passwörter & Passkeys“ oder „Passkey-Anbieter“ und wählen Sie den Microsoft Authenticator
    b. Eine detaillierte Anleitung für die Einrichtung finden Sie für **IOS** unter: https://learn.microsoft.com/de-de/entra/identity/authentication/how-to-register-passkey-authenticator?tabs=iOS
    c. Und für **Android** unter: https://learn.microsoft.com/de-de/entra/identity/authentication/how-to-register-passkey-authenticator?tabs=Android
3. Öffnen Sie nun den Microsoft Authenticator auf Ihrem Gerät

4. Wählen Sie „Konto Hinzufügen“ – „Arbeits- oder Schulkonto“ und melden Sie sich an.
5. Wählen Sie „Passkey erstellen“.
6. Es kann nun notwendig sein, dass Sie sich nochmals mittels **MFA** authentifizieren müssen oder – falls noch nicht geschehen – auf Ihrem Gerät eine Bildschirmsperre eingerichtet werden muss.

Es ist möglich, bei Verwendung der Microsoft Authenticator App die **Passwordless**-Funktion zu aktivieren. Eine genaue Beschreibung hierzu finden Sie unter:

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

Wichtig: Das Passwort selbst kann nicht gelöscht oder als Option deaktiviert werden.

Support und Kontakt

Bitte beachten Sie, dass Windows Hello ein optionales Angebot darstellt. Das Servicecenter ist über die Funktion informiert, es erfolgt jedoch **kein individueller Support** zur Einrichtung oder Nutzung von Windows Hello.