

Haftungsausschluss: Dieses Dokument wurde mit Lilly Translate übersetzt. Obwohl wir uns um Genauigkeit bemühen, beachten Sie bitte, dass die Übersetzung Fehler oder Ungenauigkeiten enthalten kann. Bitte kontaktieren Sie IdentityManagementServices@lilly.com, wenn Sie Korrekturvorschläge haben.

Einleitung

Um einen FIDO2-Sicherheitsschlüssel zu erhalten, geben Sie eine Bestellung über das [Antragsformular für den globalen Sicherheitsschlüssel](#) des ServiceNow-Katalogs auf.

Befolgen Sie diese Anweisungen oder [sehen Sie sich dieses Video an](#), um Ihren FIPS-fähigen Sicherheitsschlüssel als kennwortlose Anmeldemethode einzurichten. Da für Sicherheitsschlüssel ein physisches Gerät und etwas erforderlich ist, das nur Sie kennen (*die eindeutige PIN, die Sie einrichten werden*), gilt dies als stärkere Verifizierungsmethode als ein Benutzername und ein Kennwort.

Führen Sie diese Schritte aus, um Ihren Sicherheitsschlüssel zu registrieren und ihm eine eindeutige PIN zu geben, bevor Sie sich mit dem Schlüssel bei Ihrem Lilly-Konto anmelden können.

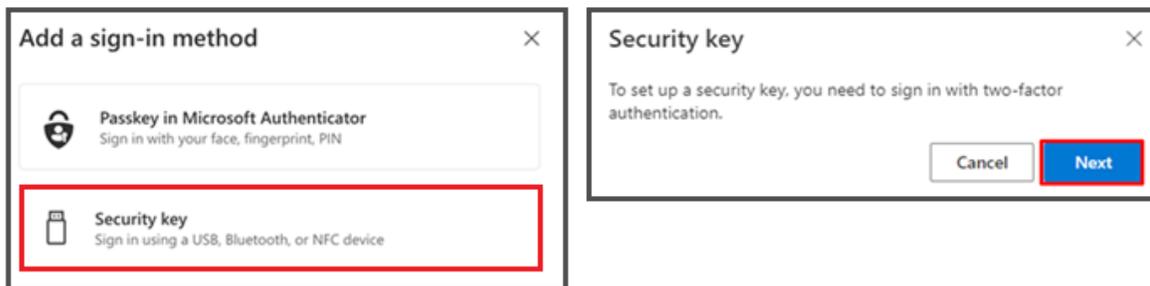
Zum Abschnitt springen (Strg + Klick verwenden):

1. [Registrieren Sie Ihren Sicherheitsschlüssel – Windows-Gerät](#)
2. [Registrieren Sie Ihren Sicherheitsschlüssel – Mac-Gerät](#)
3. [Zusätzliche Hilfe](#)

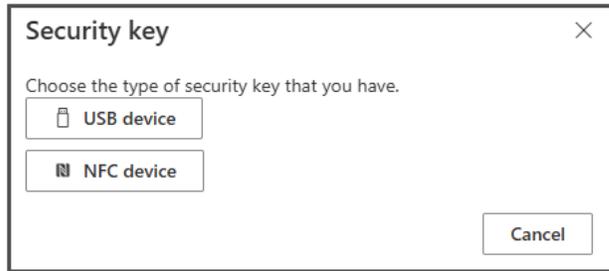
Registrieren Sie Ihren Sicherheitsschlüssel – Windows-Gerät

Verwenden Sie diese Anweisungen, wenn Sie einen Sicherheitsschlüssel auf einem Windows-Gerät registrieren.

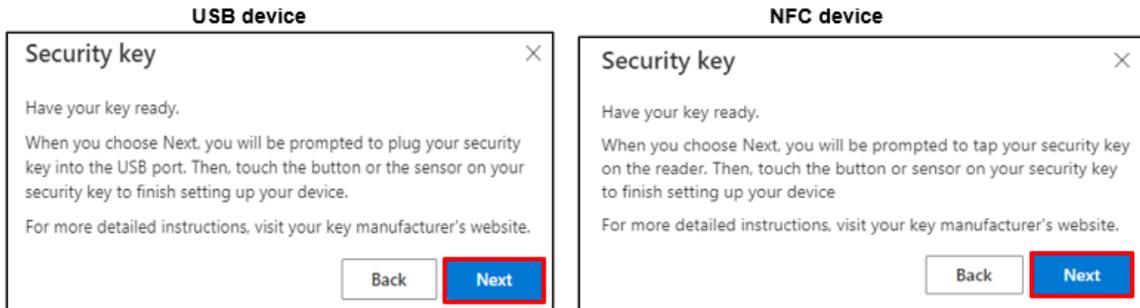
1. Öffnen Sie **Microsoft Edge**, und greifen Sie auf [Meine Anmeldungen zu](#). Klicken Sie in der oberen rechten Ecke auf Ihr Bild und vergewissern Sie sich, dass Sie mit dem Konto angemeldet sind, das Sie mit Ihrem Sicherheitsschlüssel verwenden möchten (z. B. -CA).
2. Wählen Sie **+ Anmeldemethode hinzufügen** aus.
3. Wählen Sie **auf dem Bildschirm** Anmeldemethode hinzufügen **die Option Sicherheitsschlüssel** aus . Wählen Sie **Weiter** aus, um sich mit mehrstufiger Authentifizierung anzumelden.



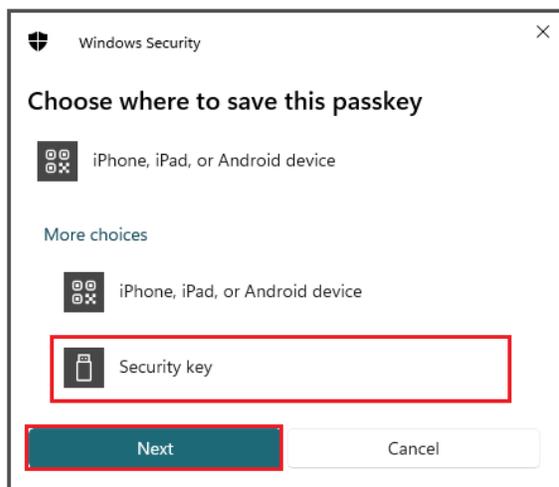
4. Überprüfen Sie Ihre Identität, indem Sie sich mit Ihrer bevorzugten Methode authentifizieren, und wählen Sie dann den **USB-Gerätetyp** aus.



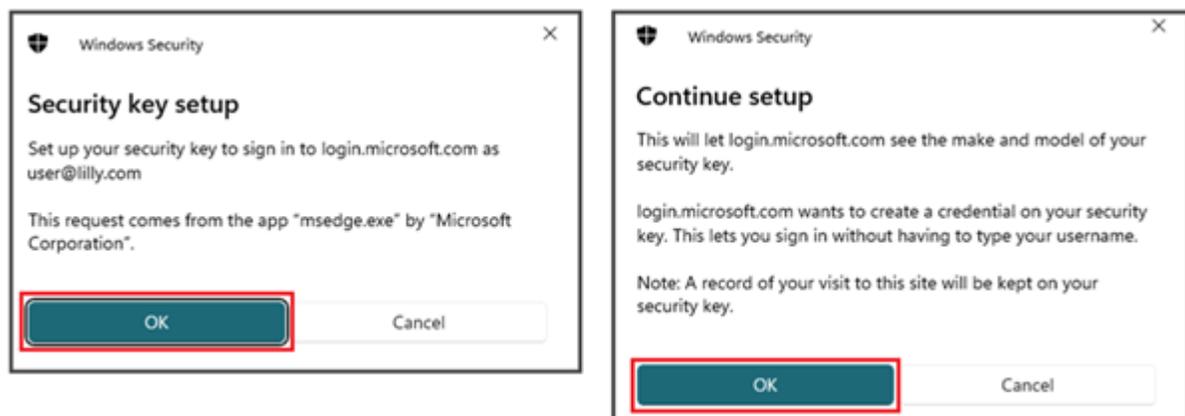
5. Halten Sie Ihren Schlüssel bereit, und wählen Sie **Weiter** aus.



6. Wählen Sie unter **Auswählen, wo dieser Hauptschlüssel gespeichert werden soll** die Option **Sicherheitsschlüssel** aus, und klicken Sie auf **Weiter**.



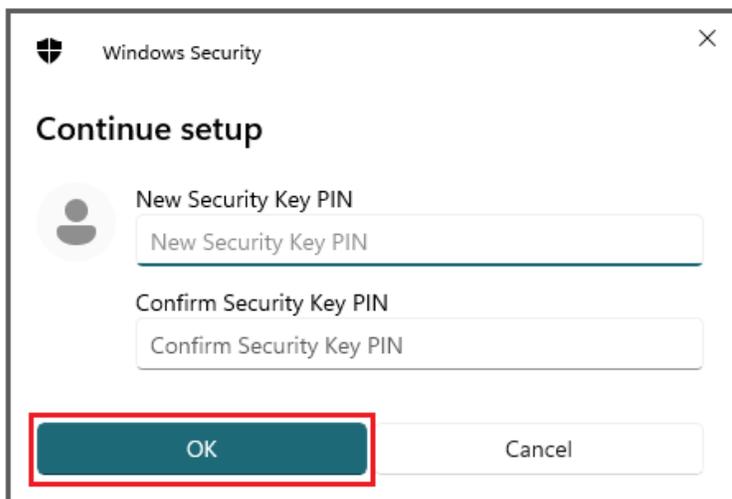
7. Wählen Sie **OK** aus, um Ihren Sicherheitsschlüssel einzurichten, und dann **erneut OK**, um mit dem Setup fortzufahren.



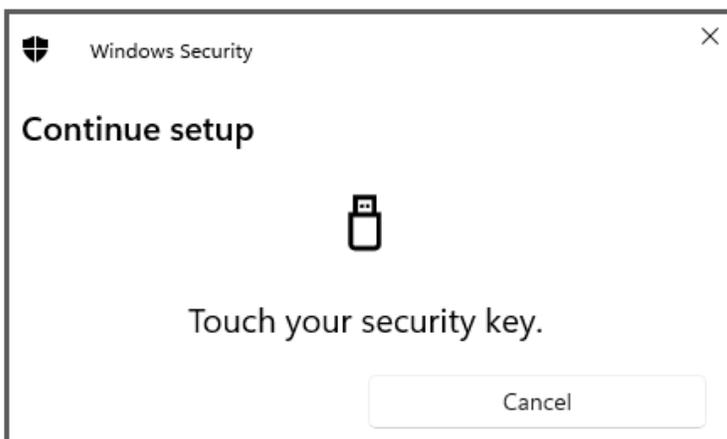
8. Geben Sie auf dem **Bildschirm Setup fortsetzen** Ihren Sicherheitsschlüssel ein.



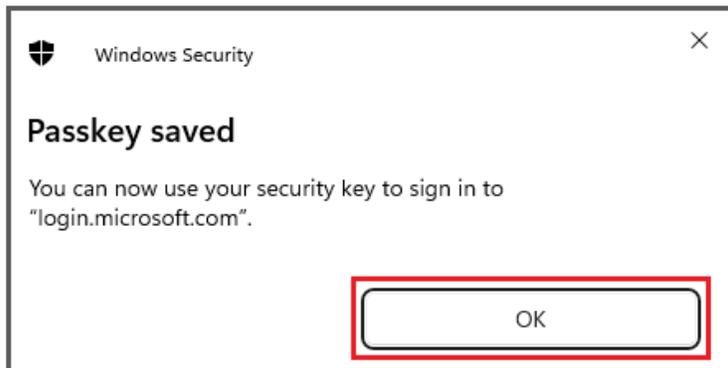
9. Geben Sie auf dem **Bildschirm Setup fortsetzen** eine 6-stellige numerische PIN für beide Felder ein und klicken Sie auf **OK**.



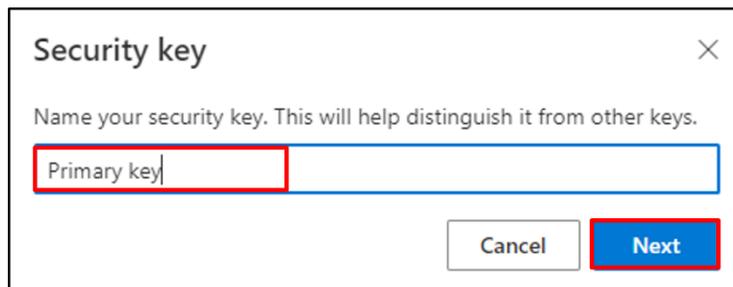
10. Tippen Sie auf dem **Bildschirm Setup fortsetzen** auf Ihren Sicherheitsschlüssel.



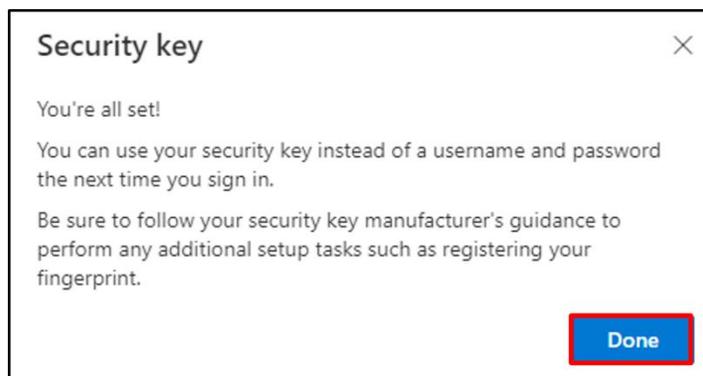
11. Klicken Sie auf dem Bildschirm **Passkey saved (Hauptschlüssel gespeichert)** auf **OK**.



12. **Geben Sie einen Namen für den Sicherheitsschlüssel ein**, um ihn von anderen Schlüsseln zu unterscheiden, und wählen Sie **Weiter** aus.



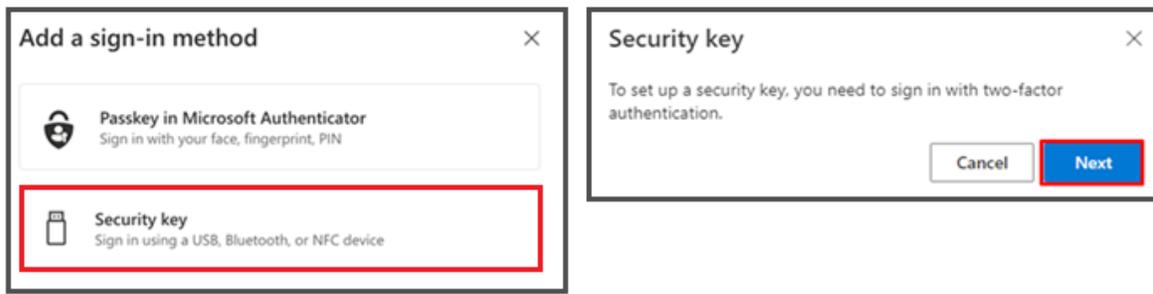
13. Ihr Sicherheitsschlüssel ist offiziell eingerichtet. Wählen Sie **Fertig** aus, um die Seite **Sicherheitsschlüssel** zu schließen.



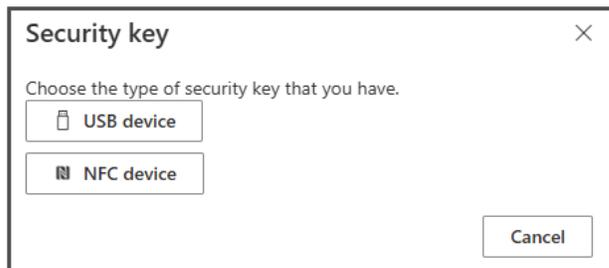
Registrieren Sie Ihren Sicherheitsschlüssel – Mac-Gerät

Befolgen Sie diese Anweisungen, wenn Sie einen Sicherheitsschlüssel auf einem Mac-Gerät registrieren.

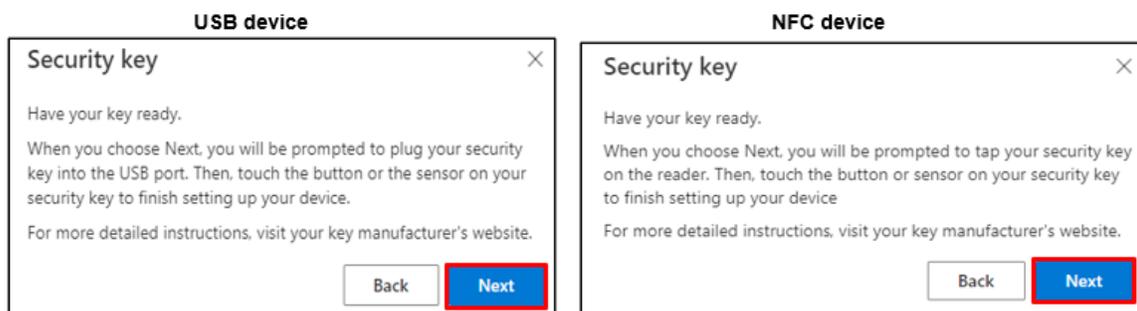
1. Öffnen Sie **Microsoft Edge** (es funktioniert **nicht** in Safari) und greifen Sie auf [Meine Anmeldungen zu](#). Klicken Sie in der oberen rechten Ecke auf Ihr Bild und vergewissern Sie sich, dass Sie mit dem Konto angemeldet sind, das Sie mit Ihrem Sicherheitsschlüssel verwenden möchten (z. B. -CA).
2. Wählen Sie **+ Anmeldemethode hinzufügen** aus.
3. Wählen Sie **auf dem Bildschirm** Anmeldemethode hinzufügen **die Option Sicherheitsschlüssel** aus . Wählen Sie **Weiter** aus, um sich mit mehrstufiger Authentifizierung anzumelden.



4. Überprüfen Sie Ihre Identität, indem Sie sich mit Ihrer bevorzugten Methode authentifizieren, und wählen Sie dann den **USB-Gerätetyp** aus .



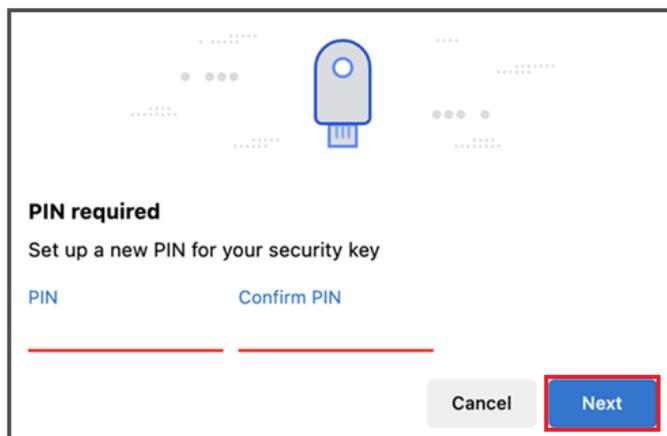
5. Halten Sie Ihren Schlüssel bereit, und wählen Sie **Weiter** aus.



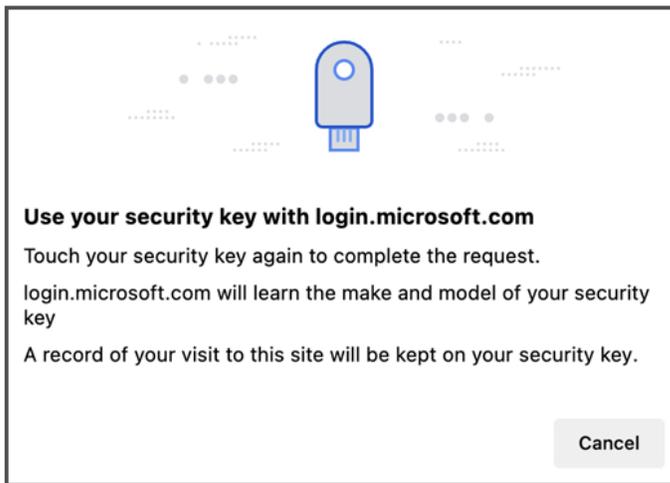
6. Geben Sie auf dem **Bildschirm** Passkeys & Security Key **Ihren Sicherheitsschlüssel ein und berühren Sie ihn**. Scannen Sie den QR-Code nicht.



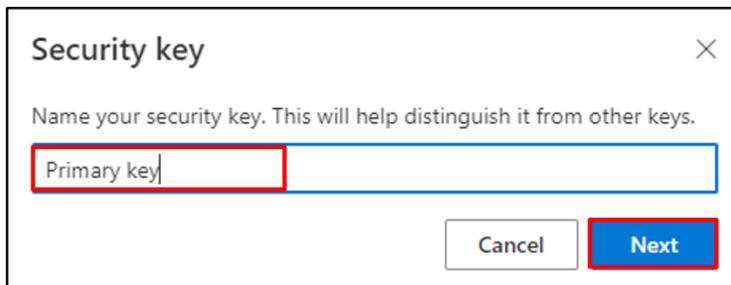
7. Geben Sie auf dem **Bildschirm** PIN erforderlich eine 6-stellige numerische PIN für beide Felder ein und klicken Sie auf **Weiter**.



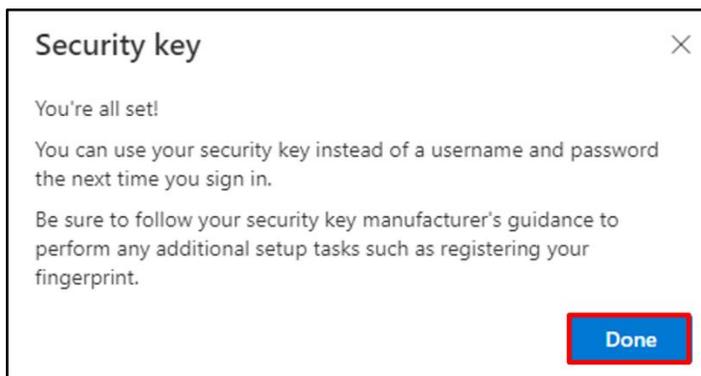
8. Tippen Sie auf dem **Bildschirm Sicherheitsschlüssel verwenden** auf Ihren Sicherheitsschlüssel.



9. **Geben Sie einen Namen für den Sicherheitsschlüssel ein**, um ihn von anderen Schlüsseln zu unterscheiden, und wählen Sie **Weiter** aus.



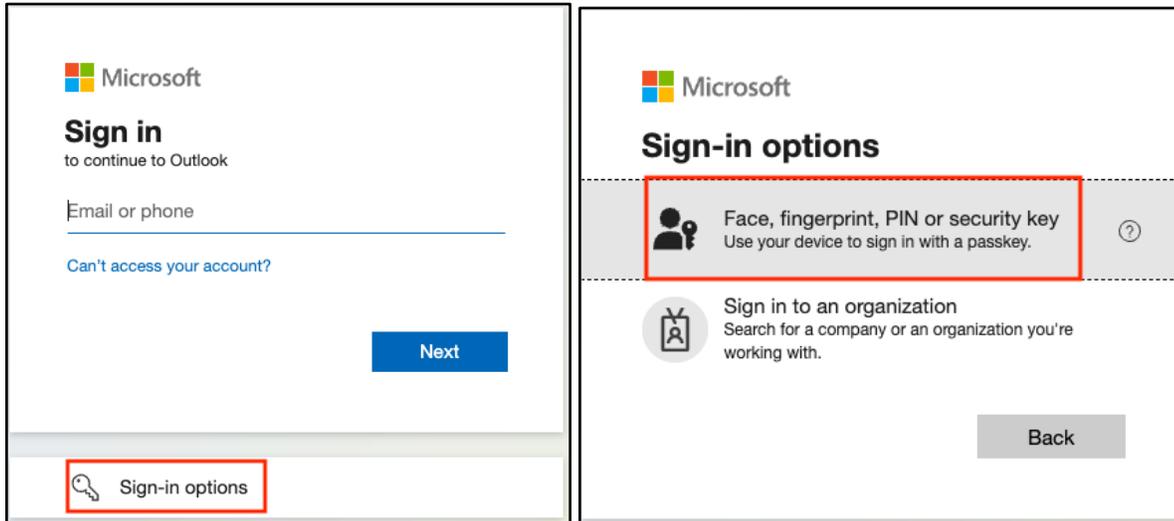
10. Ihr Sicherheitsschlüssel ist offiziell eingerichtet. Wählen Sie **Fertig** aus, um die Seite **Sicherheitsschlüssel** zu schließen.



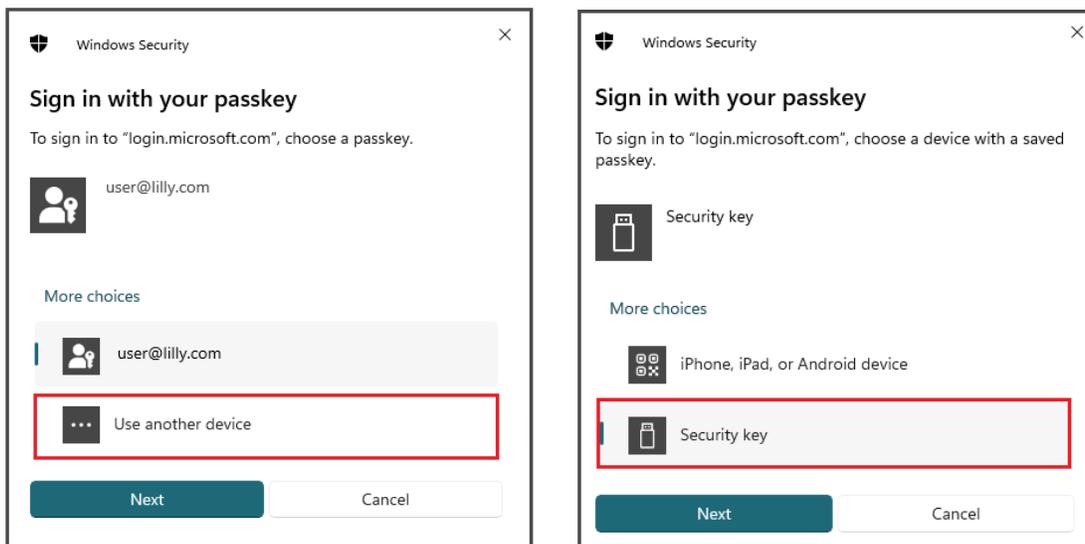
Festlegen Ihres Sicherheitsschlüssels als Standardanmeldemethode

Befolgen Sie die Schritte [in der Arbeitshilfe zum Aktualisieren Ihrer Sicherheitsinformationen](#), um Ihre Standardanmeldemethode in Microsoft Authenticator – Benachrichtigung zu ändern.

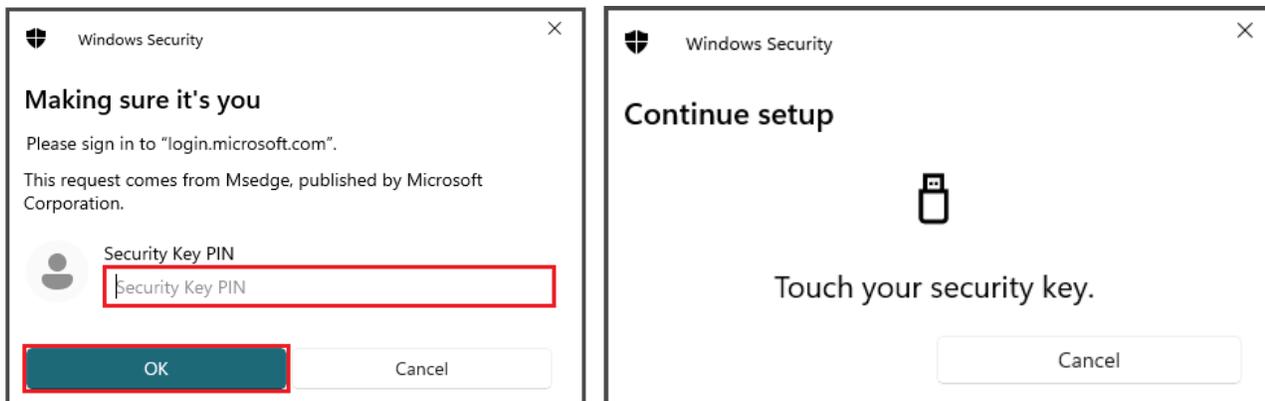
Wenn Sie das nächste Mal aufgefordert werden, sich anzumelden, wählen Sie **Optionen für die Anmeldung** und dann **Melden Sie sich mit einem Sicherheitsschlüssel an**.



Auswählen **Verwenden Sie ein anderes Gerät** oder **Sicherheitsschlüssel** und wählen Sie dann **Nächster**.



Geben Sie die **PIN Ihres Sicherheitsschlüssels** ein, wählen Sie **OK aus**, und berühren Sie dann Ihren Sicherheitsschlüssel.



Zusätzliche Hilfe

Bitte überprüfen Sie diese [Häufig gestellte Fragen](#) um Unterstützung zu bitten. Wenn Sie Ihre Frage nicht beantwortet sehen, empfehlen wir Ihnen, sie an die [Einführung der Identity Services-Community](#).

Für technische Unterstützung, die nicht in den FAQs oder Arbeitshilfen behandelt wird, wenden Sie sich bitte an Ihre lokale IT-Abteilung [Jetzt chatten](#), um einen Incident zu öffnen und ihn dem **MFA-SUPP-GLB** Schlange