KONFIGURATION

Winkeo Token oder Badgeo Smartcard installieren und einsetzen

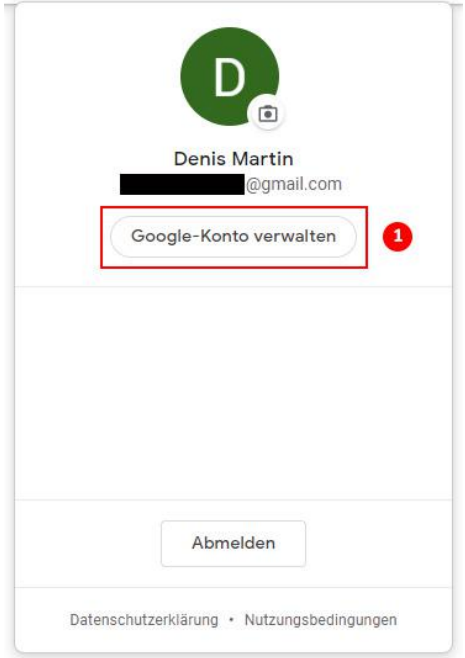
So verwenden Sie den Winkeo FIDO U2F Token

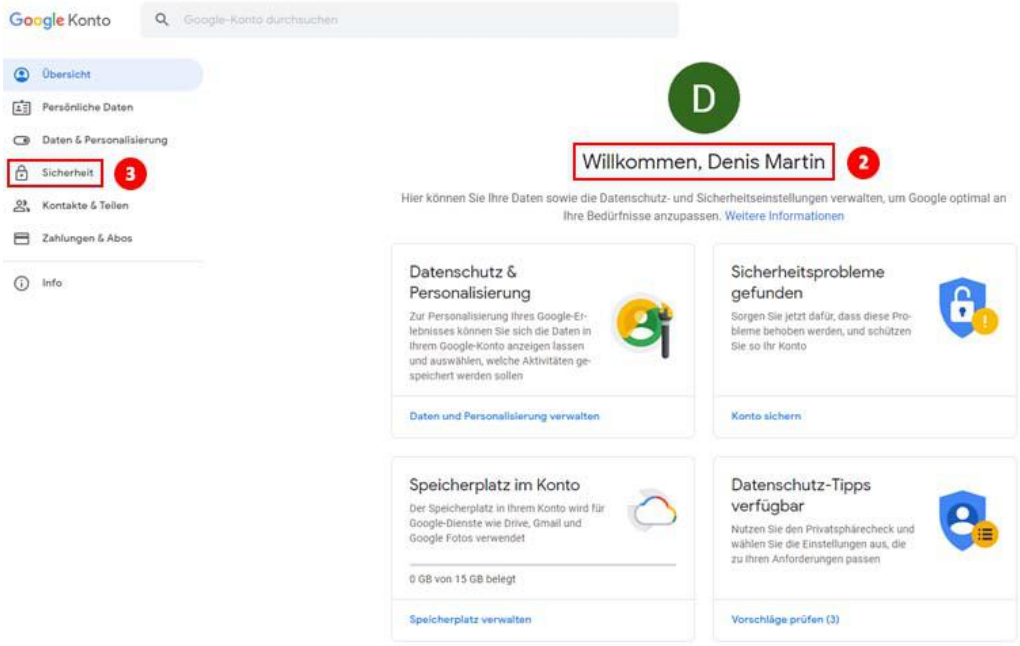
Bevor Sie Ihren Winkeo FIDO U2F-Token verwenden müssen Sie gegebenenfalls zuerst die Zwei-Faktor-Authentifizierung auf Ihrem Online-Konto einrichten. Nach der Aktivierung müssen Sie Ihren Winkeo FIDO U2F-Token mit Ihrem Konto verknüpfen. Die Vorgehensweisen finden Sie nachfolgend am Beispiel von «Google» erklärt. Die meisten Webdienste nutzen einen ähnlichen Workflow. Wählen Sie in den "Einstellungen" die Registerkarte "Sicherheit" aus und aktivieren Sie dann die "Zwei-Schritt-Validierung". Anschließend bestätigen Sie "Sicherheitsschlüssel hinzufügen".

FIDO U2F Google Tutorial

Schritt 1

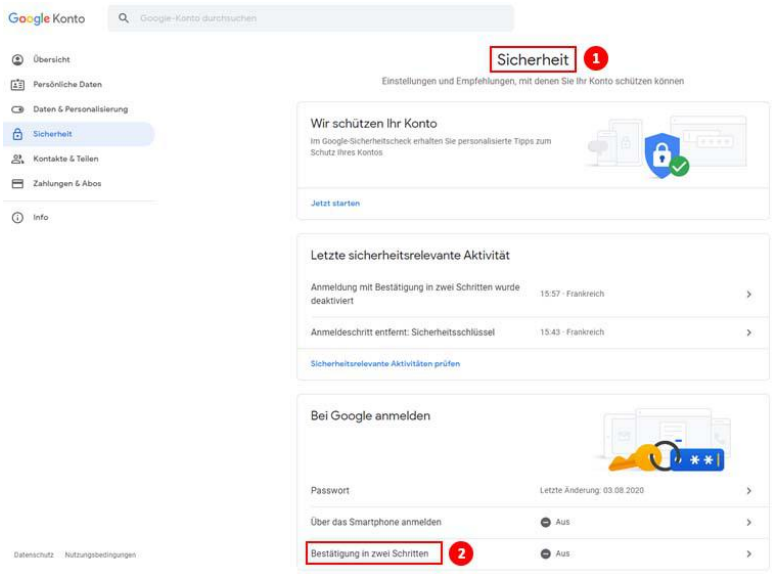
Melden Sie sich bei Ihrem Gmail-Konto an und klicken Sie dann oben rechts auf " Google-Konto verwalten".





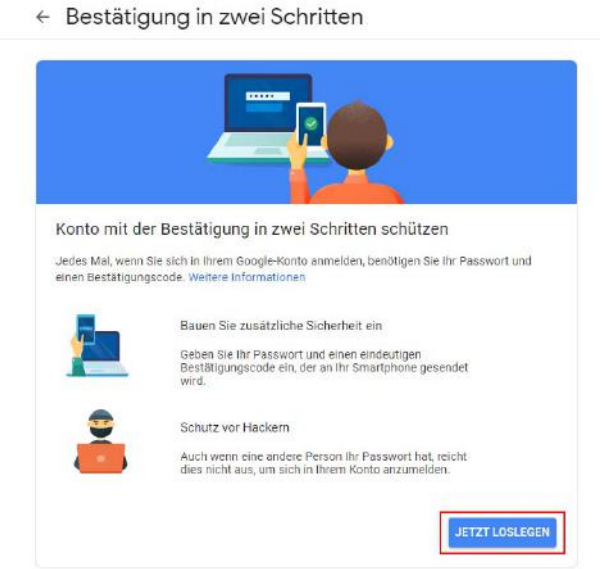
Schritt 2

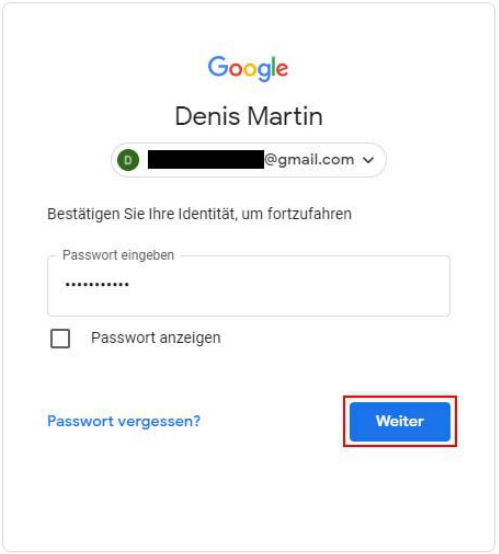
Klicken Sie auf der Seite "Willkommen" auf den Reiter "Sicherheit". Wählen Sie dann unter "Bei Google anmelden" die Option "Bestätigung in zwei Schritten".



Schritt 3

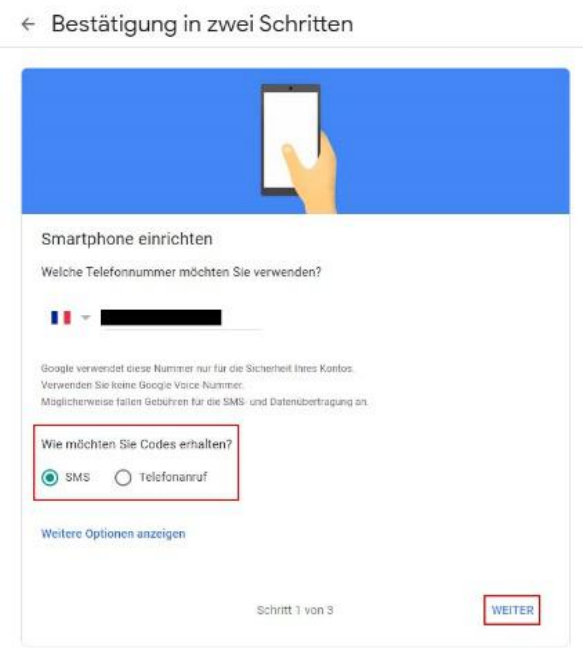
Fahren Sie fort, indem Sie auf „Jetzt loslegen“ klicken. Dann müssen Sie sich mit Ihrem Google-Passwort authentifizieren. Wenn Sie dies getan haben, klicken Sie auf „Weiter“.





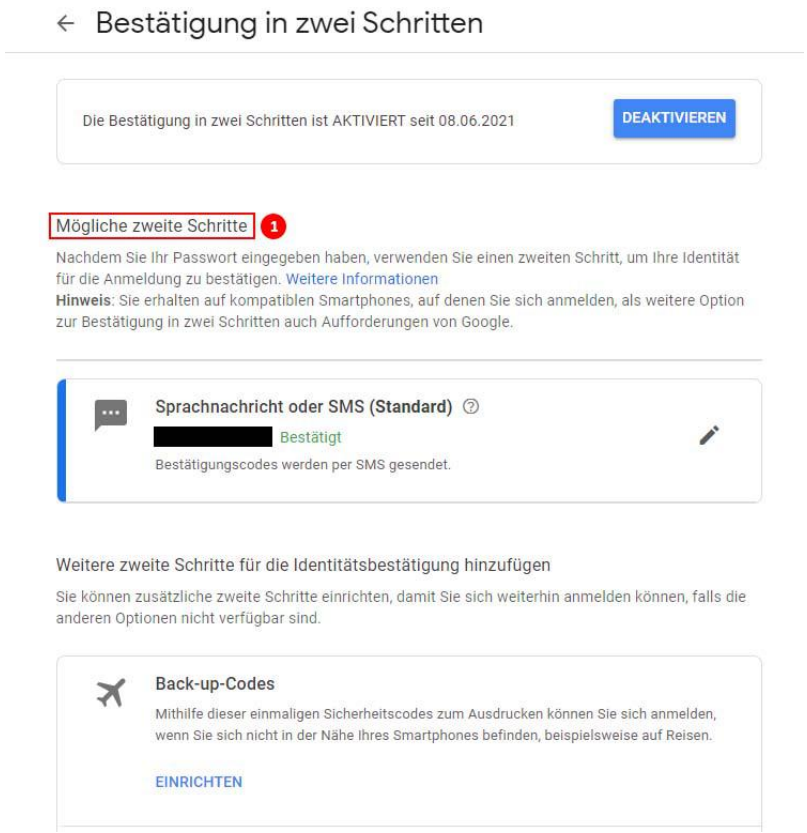
Schritt 4

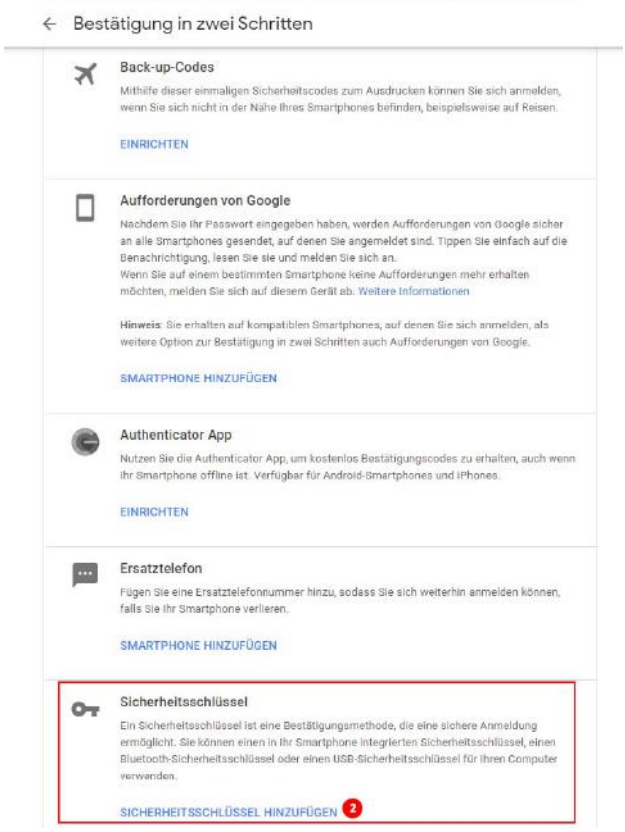
Sie werden nach einer Backup-Option gefragt und haben die Wahl zwischen SMS oder Sprachnachricht. In unserem Tutorial wählen wir die SMS-Methode. Nachdem Sie Ihre Telefonnummer eingegeben haben und die Option „SMS“ markiert haben, klicken Sie auf „Weiter“. Geben Sie den per SMS erhaltenen Code ein und klicken Sie auf "Weiter". Die Einrichtung der Zwei-Faktor-Authentifizierung für Ihr Google-Konto ist abgeschlossen. Klicken Sie auf „Aktivieren“, um die Aktivierung der Zwei-Faktor-Authentifizierung abzuschließen.



Schritt 5

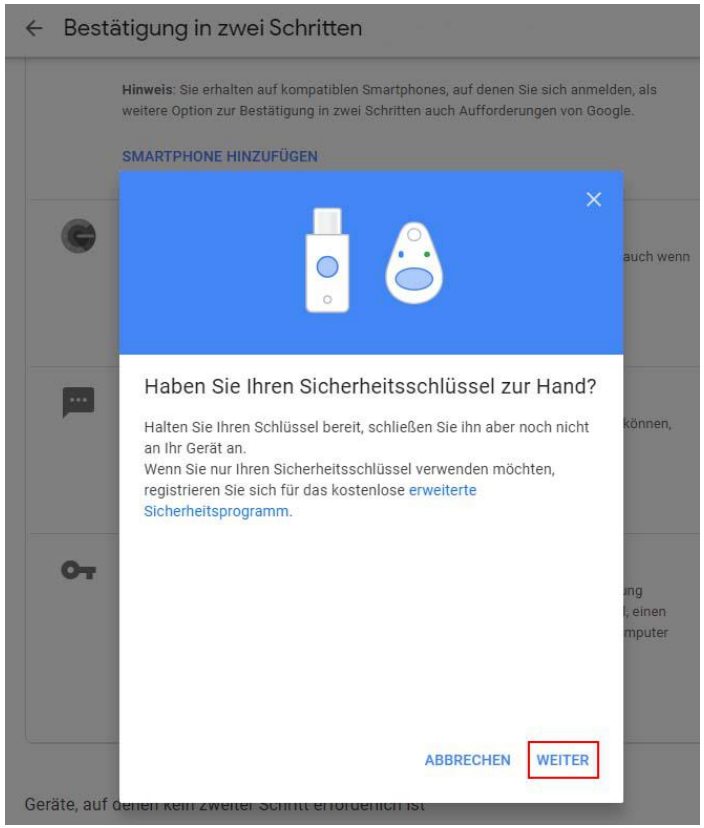
Als zweiten Authentifizierungsschritt müssen Sie nun den Winkeo FIDO U2F-Token hinzufügen. Scrollen Sie nach unten zum Abschnitt „Sicherheitsschlüssel“ und klicken Sie auf „Sicherheitsschlüssel hinzufügen“.

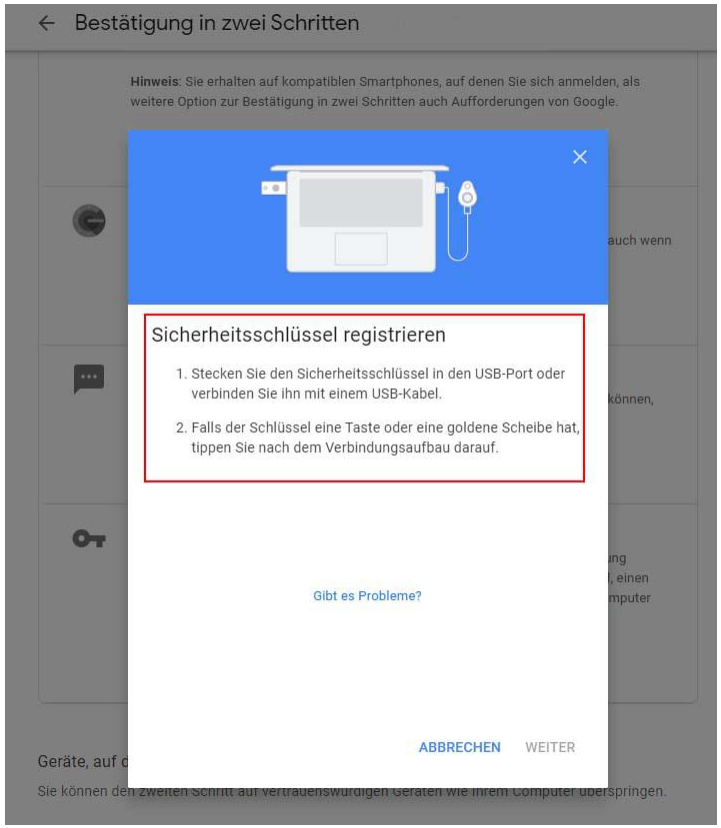




Schritt 6

Sie werden aufgefordert, Ihren Sicherheitsschlüssel auszuwählen. Klicken Sie in diesem Fall auf „USB oder Bluetooth“. In einigen Fällen werden Sie direkt gefragt „Haben Sie Ihren Sicherheitsschlüssel zur Hand?“ ohne den vorherigen Schritt zu durchlaufen. Drücken Sie dann auf „Weiter“. Ein Fenster " Sicherheitsschlüssel registrieren" wird geöffnet.



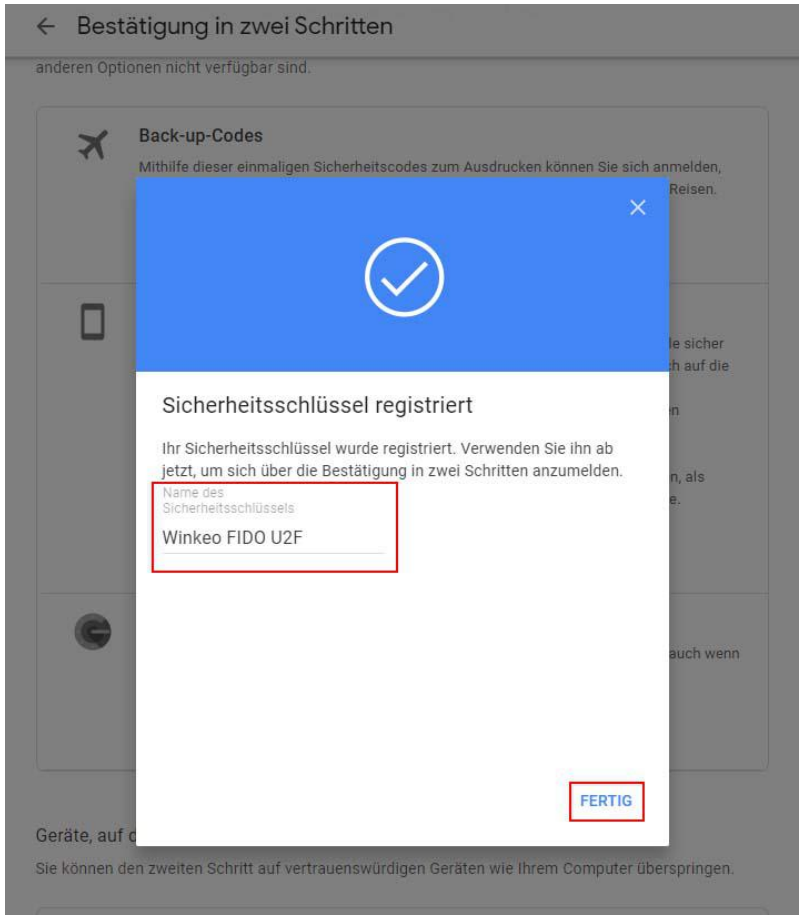


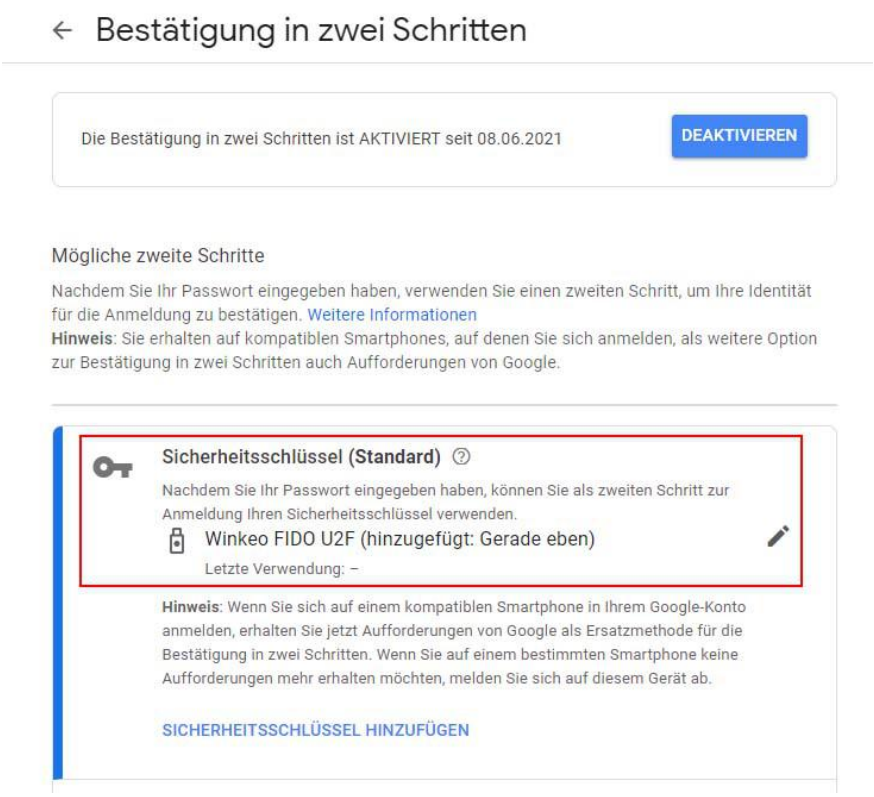
Schritt 7

Stecken Sie Ihren Token in den USB-Port Ihres Computers (die LED blinkt). Klicken Sie in den folgenden Pop-up-Fenstern auf "OK" («Sicherheitsschlüssel konfigurieren» und «Installation fortsetzen»). Wenn Sie fertig sind, werden Sie aufgefordert, den goldenen Knopf am Winkeo FIDO U2F-Token zu drücken.

Schritt 8

Ihr Sicherheitsschlüssel ist nun gespeichert und wird für die Anmeldung mit zweistufiger Verifizierung verwendet. Benennen Sie Ihren Sicherheitsschlüssel und drücken Sie „OK“. Die Bestätigung in zwei Schritten ist aktiviert und Ihr Sicherheitsschlüssel ist registriert.





Zukünftige Anmeldungen

Um sich zu zukünftig bei Ihrem Gmail-Konto zu authentifizieren müssen Sie zuerst Ihr Passwort eingeben, den Winkeo FIDO U2F-Token anstecken und dann die Taste drücken.

Wenn Sie Ihren Token nicht jedes Mal verwenden möchten, wenn Sie sich in Ihrem Google-Konto anmelden, aktivieren Sie das Kontrollkästchen "Auf diesem Gerät nicht mehr fragen". Das bedeutet, dass Ihr Computer vertrauenswürdig ist. Diese Möglichkeit ist jedoch nur auf den Geräten zu wählen, die Sie regelmäßig nutzen und die Sie nicht mit anderen teilen. Andernfalls deaktivieren Sie das Kontrollkästchen.

So verwenden Sie den Winkeo FIDO2 Token oder die Badgeo FIDO2 Smartcard

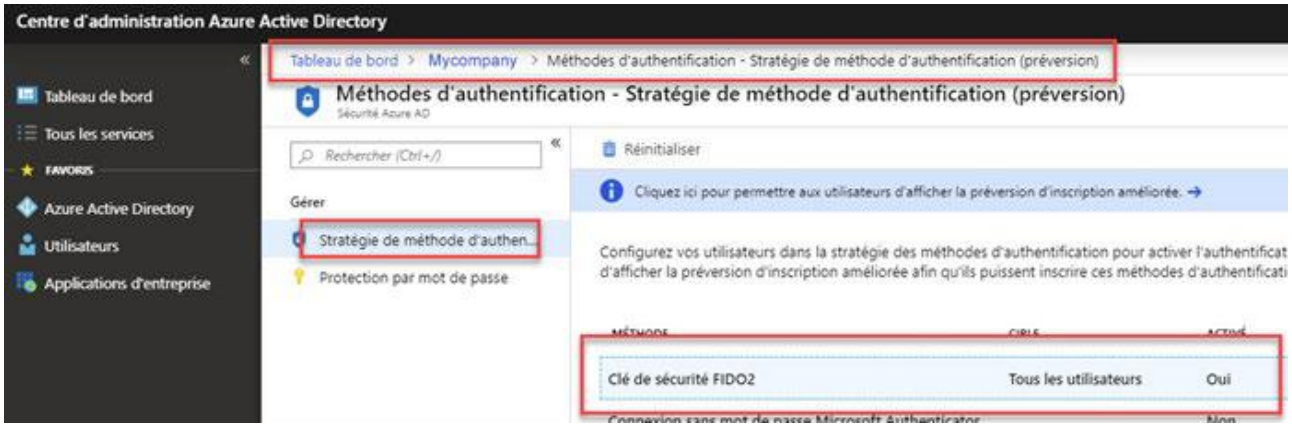
Um den Winkeo FIDO2-Token oder die Badgeo FIDO2-Smartcard mit Online-Diensten und -Anwendungen zu verknüpfen, bitten wir Sie, sich an unser Team oder Ihren System- / Netzwerkadministrator zu wenden. Detaillierte Anleitungen von Microsoft enthalten außerdem wichtige Schritte zur Aktivierung der kennwortlosen Token-Anmeldung, einschließlich Windows 10-Geräten mit Azure Active Directory.

Wir bieten auch eine kurze Anleitung zur Aktivierung eines Winkeo FIDO2-Schlüssels oder einer Badgeo FIDO2-Smartcard als Mittel zur Authentifizierung in Ihrem Azure AD-Unternehmensverzeichnis an.

FIDO2 Microsoft Tutorial

Schritt 1

Ihr Netzwerkadministrator muss die "FIDO2-Sicherheitsschlüssel" in der "Authentifizierungsrichtlinie" im Administrationscenter Ihres Azure Active Directory aktivieren https://aad.portal.azure.com

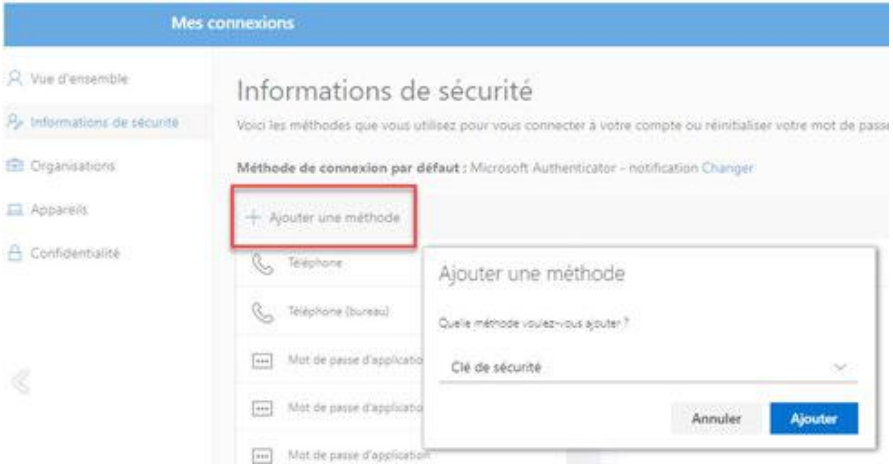


Schritt 2

Der Administrator muss dann die Benutzer auswählen, die diese Methode verwenden können, und muss auch die "Schlüsselbeschränkung" deaktivieren, die bestimmte Hardwarehersteller sperrt.

Schritt 3

Anschließend können Sie den Winkeo FIDO2-Token und/oder die Badgeo FIDO2-Karte in Ihrem eigenen Portal aktivieren. Dazu wechseln Sie zu https://mysignins.microsoft.com und klicken auf der Registerkarte "Sicherheitsinformationen" auf "Methode hinzufügen" um dann "Sicherheitsschlüssel" aus dem Dropdown-Menü auswählen.

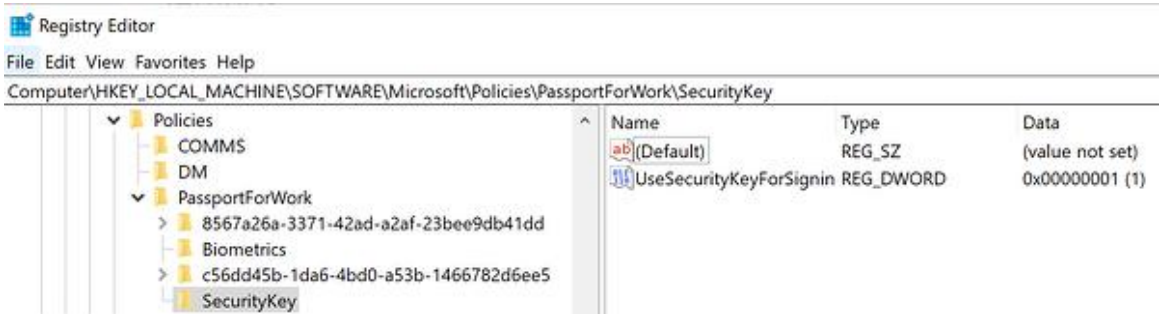


Schritt 4

Der Administrator muss dann in der lokalen "Registry" Ihres Arbeitsplatzes folgende Änderung vornehmen:

[HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Richtlinien \ PassportForWork \ SecurityKey]

"UseSecurityKeyForSignin" = dword: 00000001



Schritt 5

Nachdem diese Änderungen vorgenommen wurden, erscheint eine neue Authentifizierungsmöglichkeit per FIDO2-Token und / oder FIDO2-Smartcard zum Öffnen der Sitzung.

Um Ihren Web-Sicherheitsanforderungen so nahe wie möglich zu sein, werden NEOWAVE-Produkte in ganz Europa vertrieben

Der nächstgelegene (NEOWAVE Distributor für Deutschland, Österreich und Schweiz)

ProSoft

ProSoft GmbH

Buergermeister-Graf-Ring 10

D-82538 Geretsried

Tel. +49 (0) 8171/405-200

info@prosoft.de

www.prosoft.de