

KONFIGURATION

Winkeo Token oder Badgeo Smartcard installieren und einsetzen

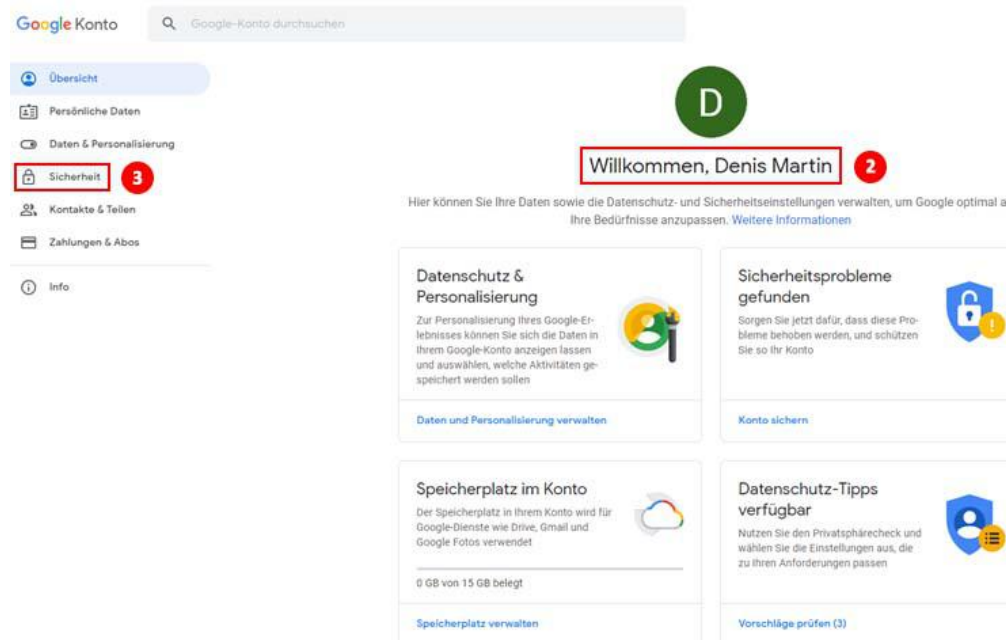
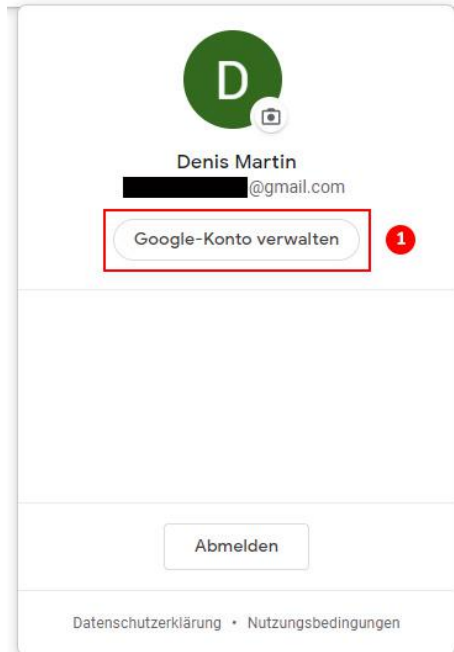
So verwenden Sie den Winkeo FIDO U2F Token

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".

The screenshot shows the Google Account Security page. On the left is a navigation menu with options: Übersicht, Persönliche Daten, Daten & Personalisierung, Sicherheit (highlighted), Kontakte & Teilen, Zahlungen & Abos, and Info. The main content area has a 'Sicherheit' header with a red '1' icon. Below it are three sections: 'Wir schützen Ihr Konto' with a 'Jetzt starten' link; 'Letzte sicherheitsrelevante Aktivität' with a list of recent security events; and 'Bei Google anmelden' with options for 'Passwort', 'Über das Smartphone anmelden', and 'Bestätigung in zwei Schritten' (highlighted with a red '2' icon).

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“.

← Bestätigung in zwei Schritten


This page explains the two-step verification process. It features an illustration of a person at a computer. The text states: 'Konto mit der Bestätigung in zwei Schritten schützen' and 'Jedes Mal, wenn Sie sich in Ihrem Google-Konto anmelden, benötigen Sie Ihr Passwort und einen Bestätigungscode.' Two benefits are listed: 'Bauen Sie zusätzliche Sicherheit ein' (requiring password and code) and 'Schutz vor Hackern' (preventing unauthorized access). A blue 'JETZT LOSLEGEN' button is highlighted with a red box at the bottom right.

The authentication page shows the Google logo, the name 'Denis Martin', and a redacted email address '@gmail.com'. The instruction is 'Bestätigen Sie Ihre Identität, um fortzufahren'. There is a password input field with a masked password '*****' and a 'Passwort anzeigen' checkbox. A blue 'Passwort vergessen?' link is on the left, and a blue 'Weiter' button is on the right, highlighted with a red box.

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.

← Bestätigung in zwei Schritten



Smartphone einrichten

Welche Telefonnummer möchten Sie verwenden?

FR [Redacted]

Google verwendet diese Nummer nur für die Sicherheit Ihres Kontos. Verwenden Sie keine Google Voice-Nummer. Möglicherweise fallen Gebühren für die SMS- und Datenübertragung an.

Wie möchten Sie Codes erhalten?

SMS Telefonanruf

[Weitere Optionen anzeigen](#)

Schritt 1 von 3 WEITER

← Bestätigung in zwei Schritten



Nummer bestätigen

Google hat gerade eine SMS mit einem Bestätigungscode an [Redacted] gesendet.

Code eingeben

Sie haben sie nicht erhalten? Erneut senden

ZURÜCK Schritt 2 von 3 WEITER

← Bestätigung in zwei Schritten



Es hat funktioniert! Möchten Sie die Bestätigung in zwei Schritten aktivieren?

Nachdem Sie nun den Ablauf des Prozesses gesehen haben, möchten Sie die Bestätigung in zwei Schritten für Ihr Google-Konto [Redacted]@gmail.com aktivieren?

Schritt 3 von 3 AKTIVIEREN

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“.

← Bestätigung in zwei Schritten

Die Bestätigung in zwei Schritten ist AKTIVIERT seit 08.06.2021

DEAKTIVIEREN

Mögliche zweite Schritte ¹

Nachdem Sie Ihr Passwort eingegeben haben, verwenden Sie einen zweiten Schritt, um Ihre Identität für die Anmeldung zu bestätigen. [Weitere Informationen](#)

Hinweis: Sie erhalten auf kompatiblen Smartphones, auf denen Sie sich anmelden, als weitere Option zur Bestätigung in zwei Schritten auch Aufforderungen von Google.

Sprachnachricht oder SMS (Standard) ²

Bestätigt

Bestätigungscodes werden per SMS gesendet.

Weitere zweite Schritte für die Identitätsbestätigung hinzufügen

Sie können zusätzliche zweite Schritte einrichten, damit Sie sich weiterhin anmelden können, falls die anderen Optionen nicht verfügbar sind.

Back-up-Codes

Mithilfe dieser einmaligen Sicherheitscodes zum Ausdrucken können Sie sich anmelden, wenn Sie sich nicht in der Nähe Ihres Smartphones befinden, beispielsweise auf Reisen.

EINRICHTEN

← Bestätigung in zwei Schritten

Back-up-Codes

Mithilfe dieser einmaligen Sicherheitscodes zum Ausdrucken können Sie sich anmelden, wenn Sie sich nicht in der Nähe Ihres Smartphones befinden, beispielsweise auf Reisen.

EINRICHTEN

Aufforderungen von Google

Nachdem Sie Ihr Passwort eingegeben haben, werden Aufforderungen von Google sicher an alle Smartphones gesendet, auf denen Sie angemeldet sind. Tippen Sie einfach auf die Benachrichtigung, lesen Sie sie und melden Sie sich an.

Wenn Sie auf einem bestimmten Smartphone keine Aufforderungen mehr erhalten möchten, melden Sie sich auf diesem Gerät ab. [Weitere Informationen](#)

Hinweis: Sie erhalten auf kompatiblen Smartphones, auf denen Sie sich anmelden, als weitere Option zur Bestätigung in zwei Schritten auch Aufforderungen von Google.

SMARTPHONE HINZUFÜGEN

Authenticator App

Nutzen Sie die Authenticator App, um kostenlos Bestätigungscodes zu erhalten, auch wenn ihr Smartphone offline ist. Verfügbar für Android-Smartphones und iPhones.

EINRICHTEN

Ersatztelefon

Fügen Sie eine Ersatztelefonnummer hinzu, sodass Sie sich weiterhin anmelden können, falls Sie Ihr Smartphone verlieren.

SMARTPHONE HINZUFÜGEN

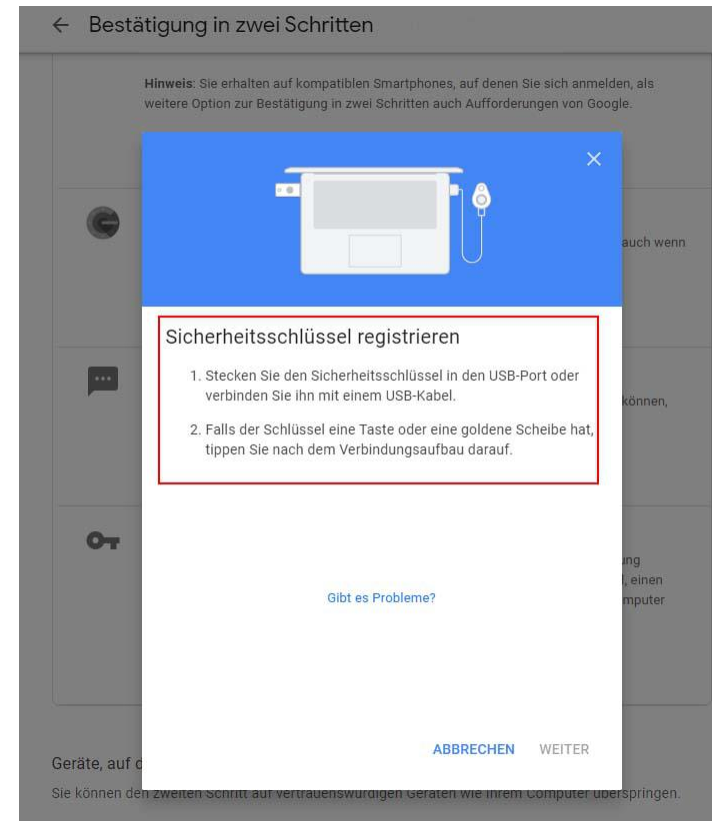
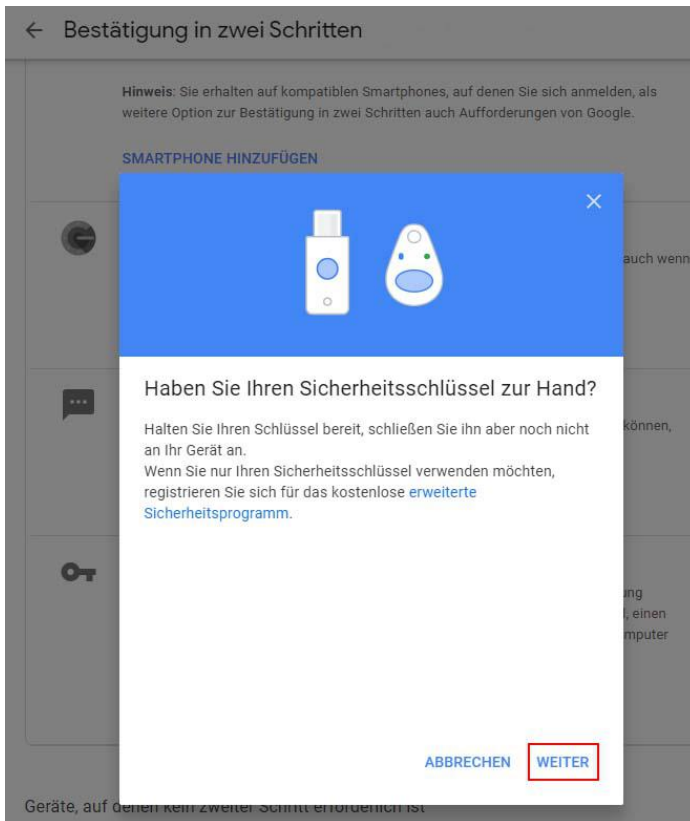
Sicherheitsschlüssel

Ein Sicherheitsschlüssel ist eine Bestätigungsmethode, die eine sichere Anmeldung ermöglicht. Sie können einen in Ihr Smartphone integrierten Sicherheitsschlüssel, einen Bluetooth-Sicherheitsschlüssel oder einen USB-Sicherheitsschlüssel für Ihren Computer verwenden.

SICHERHEITSSCHLÜSSEL HINZUFÜGEN ²

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.

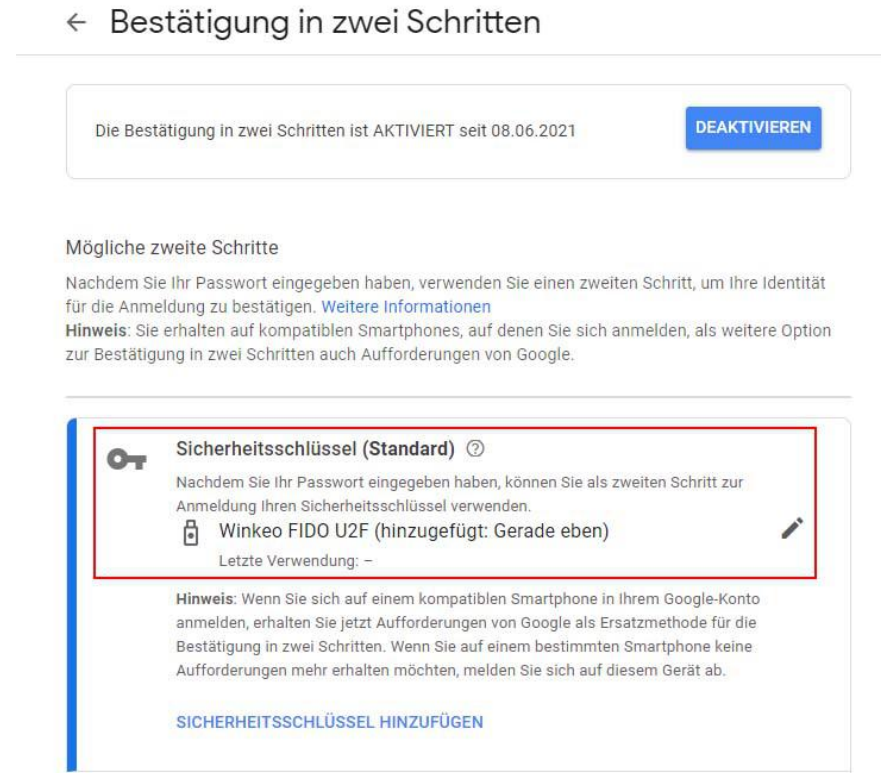
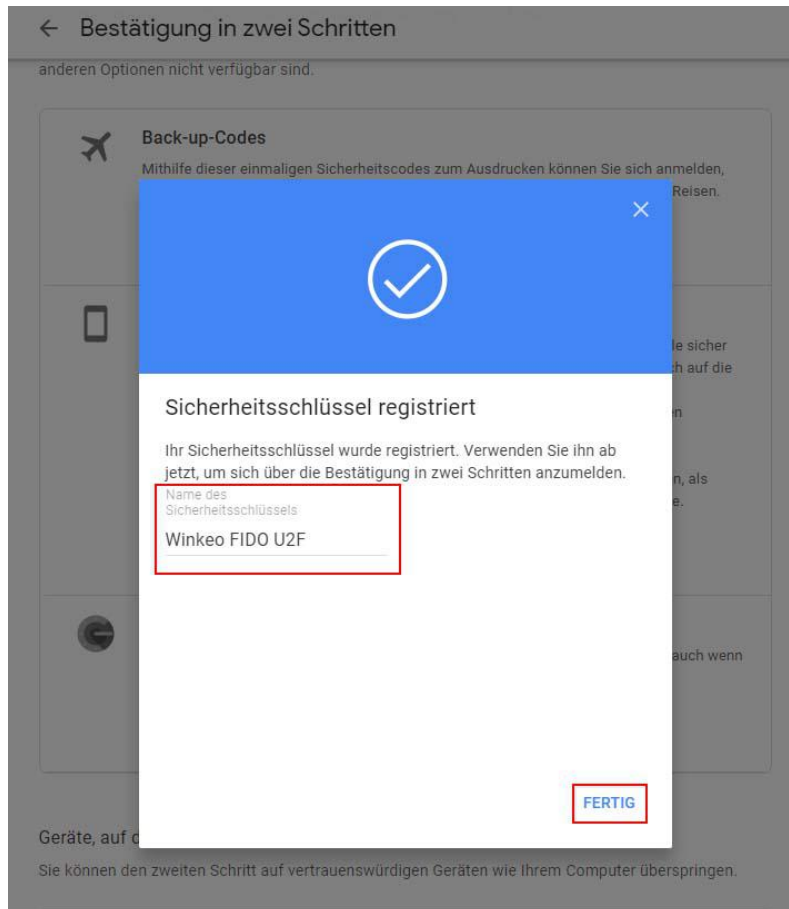


Schritt 7

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.

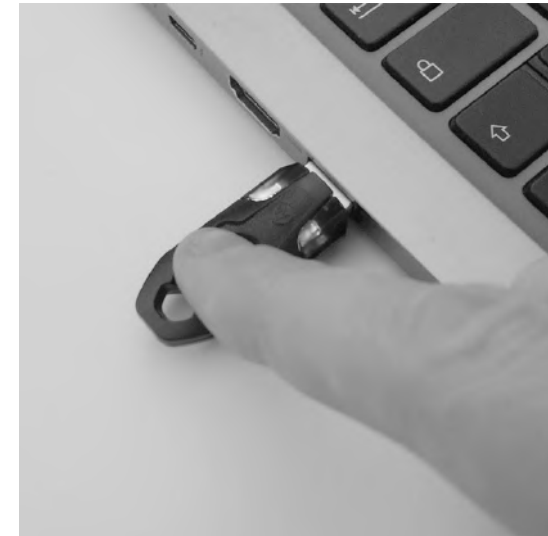
Schritt 8

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

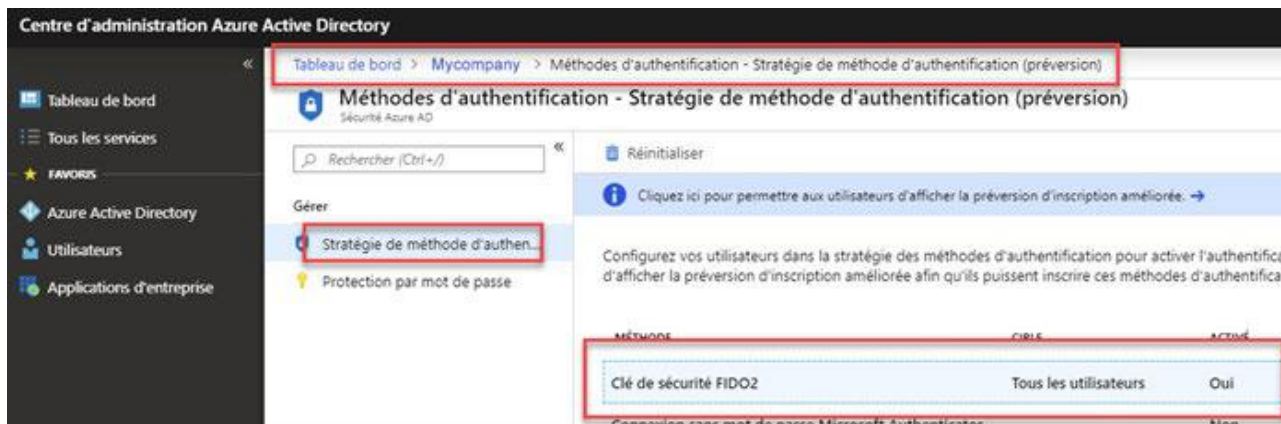
Um den Winkeo FIDO2-Token oder die Badgeo FIDO2-Smartcard mit Online-Diensten und -Anwendungen zu verknüpfen, bitten wir Sie, sich an unser Team oder Ihren System- / Netzwerkadministrator zu wenden. Detaillierte Anleitungen von Microsoft enthalten außerdem wichtige Schritte [zur Aktivierung der kennwortlosen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



The screenshot shows the Azure Active Directory Administration Center interface. The breadcrumb navigation at the top reads: "Tableau de bord > Mycompany > Méthodes d'authentification - Stratégie de méthode d'authentification (préversion)". The main heading is "Méthodes d'authentification - Stratégie de méthode d'authentification (préversion)". A search bar contains "Rechercher (Ctrl+/)". Under the "Gérer" section, "Stratégie de méthode d'authen..." is highlighted. Below it, "Protection par mot de passe" is visible. On the right, there is a "Réinitialiser" button and an information icon with the text "Cliquez ici pour permettre aux utilisateurs d'afficher la préversion d'inscription améliorée. →". A descriptive paragraph follows: "Configurez vos utilisateurs dans la stratégie des méthodes d'authentification pour activer l'authentification d'afficher la préversion d'inscription améliorée afin qu'ils puissent inscrire ces méthodes d'authentification". At the bottom, a table lists authentication methods:

MÉTHODE	CIBLE	ACTIVÉ
Clé de sécurité FIDO2	Tous les utilisateurs	Oui

Schritt 2

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

The screenshot shows two parts of the configuration interface. On the left, a red box highlights the 'CIBLE' (Target) section, which includes a dropdown menu set to 'Tous les utilisateurs' and a table with columns 'NOM', 'TYPE', and 'INSCRIPTION'. The table contains one row with 'Tous les utilisateurs', 'Groupe', and 'Facultatif'. On the right, the 'GÉNÉRAL' (General) section has two toggle switches: 'Autoriser la configuration libre-service' (set to 'Oui') and 'Appliquer l'attestation' (set to 'Oui'). Below this, a red box highlights the 'STRATÉGIE DE RESTRICTION DE CLÉ' (Key Restriction Strategy) section, which has a toggle switch for 'Appliquer les restrictions de clé' set to 'Non'.

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 auszuwählen.

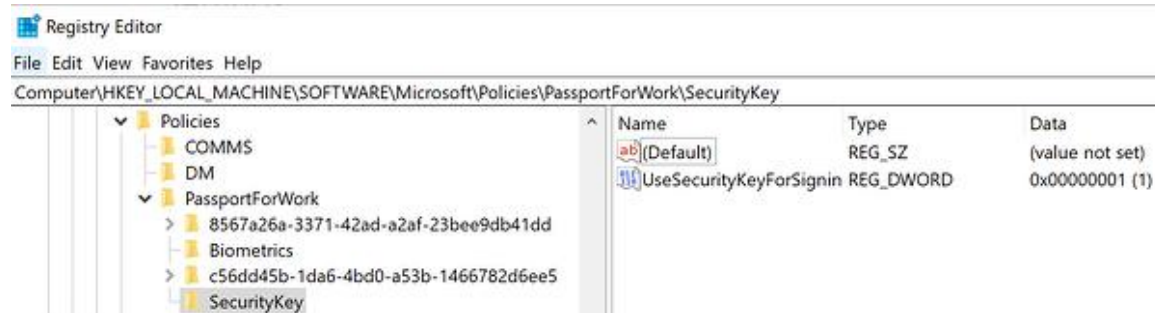
The screenshot shows the 'Mes connexions' (My connections) page in the Microsoft account portal. The 'Informations de sécurité' (Security information) section is active, showing the default connection method as 'Microsoft Authenticator - notification Changer'. A red box highlights the '+ Ajouter une méthode' (Add a method) button. Below it, a list of methods is shown, including 'Téléphone', 'Téléphone (bureau)', and several 'Mot de passe d'application' (App passwords) entries. A dialog box titled 'Ajouter une méthode' (Add a method) is open, asking 'Quelle méthode voulez-vous ajouter?' (Which method do you want to add?). The 'Clé de sécurité' (Security key) option is selected in the dropdown menu. The dialog has 'Annuler' (Cancel) and 'Ajouter' (Add) buttons.

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