AYI NEDJIMI Consultants

Passwordless : stratégie complète pour zéro mot de passe

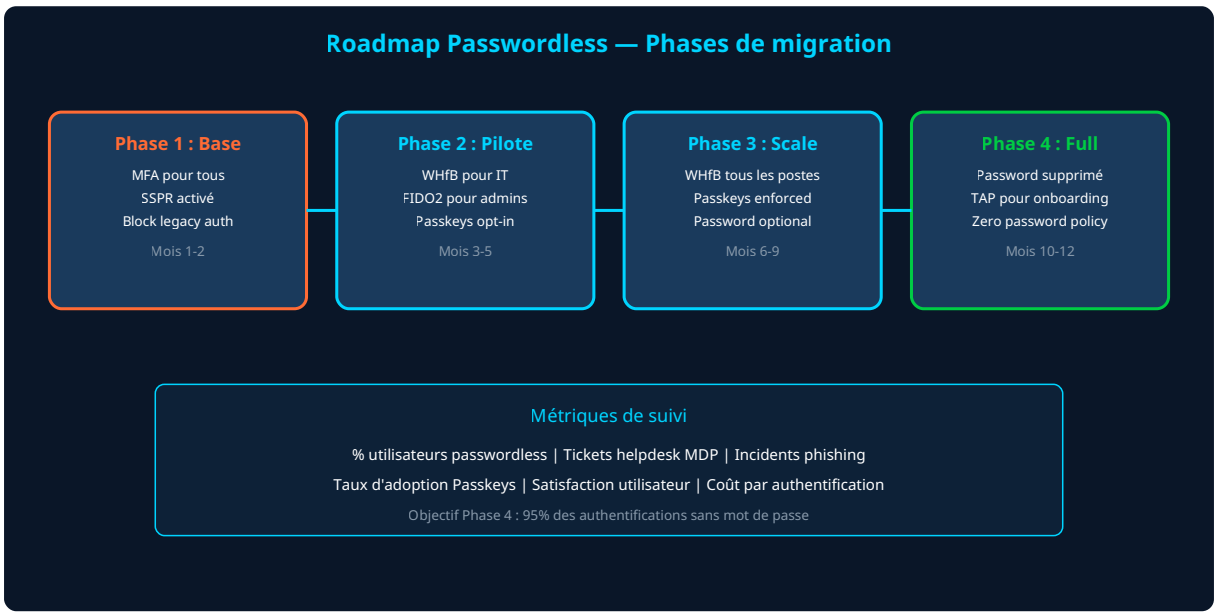
Catégorie : IAM et Gestion des Identités Lecture : 7 min Publié le : 12/03/2026 Auteur : Ayi NEDJIMI

Stratégie passwordless complète : éliminez les mots de passe avec FIDO2, Passkeys, Windows Hello et SSPR pour réduire le phishing et simplifier l'UX.

Les mots de passe sont le maillon faible de la sécurité depuis trente ans. Réutilisés, faibles, phishés, volés, oubliés — ils génèrent 40% des tickets helpdesk et restent le vecteur d'entrée de 80% des cyberattaques. Et pourtant, la plupart des organisations continuent de baser leur sécurité sur ce mécanisme fondamentalement défaillant. La stratégie passwordless ambitionne de supprimer complètement les mots de passe au profit de méthodes d'authentification plus sûres et plus ergonomiques : FIDO2, Passkeys, Windows Hello for Business, authentification biométrique. Ce guide vous accompagne dans la conception et le déploiement d'une stratégie passwordless réaliste, de l'audit de l'existant au rollout global. Nous aborderons les technologies disponibles, les prérequis techniques, la gestion de la transition et les cas d'usage qui résistent encore au passwordless. Le self-service password reset (SSPR), souvent vu comme un palliatif, trouve sa place dans cette stratégie comme filet de sécurité pendant la transition. L'objectif est de vous fournir une feuille de route complète, adaptable à votre contexte, avec des jalons mesurables et des quick wins identifiés.

Points clés à retenir

- Le **passwordless** réduit les attaques de phishing de 99% et les tickets helpdesk de 40%
- **Windows Hello for Business** est le pilier passwordless pour les postes Windows gérés
- Les **Passkeys** synchronisées remplacent le mot de passe pour les applications web et mobiles
- Le **SSPR** reste nécessaire pendant la transition comme mécanisme de fallback sécurisé
- La migration se fait par vagues : admins IT → early adopters → utilisateurs standards → legacy



Pourquoi les mots de passe doivent disparaître

Les chiffres sont accablants. **81%** des brèches impliquent des credentials compromis (Verizon DBIR 2025). Le coût moyen d'un ticket helpdesk pour réinitialisation de mot de passe est de **25 à 70€** (Forrester). Un employé passe en moyenne **11 heures par an** à gérer ses mots de passe. Et malgré les politiques de complexité, les utilisateurs continuent de réutiliser les mêmes mots de passe avec des variations prévisibles (Password2024! → Password2025!).

Les attaques par mot de passe exploitent cette réalité avec une efficacité redoutable. Le password spraying teste quelques mots de passe courants contre des milliers de comptes. Le credential stuffing utilise les milliards de credentials leakés pour tenter des accès. Le phishing AiTM intercepte même le MFA classique. La seule solution durable : éliminer le mot de passe comme facteur d'authentification. Plus de mot de passe à voler, plus de mot de passe à phisher, plus de mot de passe à cracker.

Technologies passwordless disponibles en 2026

Quatre technologies composent l'arsenal passwordless. **Windows Hello for Business** (WHfB) remplace le mot de passe Windows par une authentification biométrique (empreinte, reconnaissance faciale) ou PIN protégé par TPM. Le credential est lié au device et ne quitte jamais la puce TPM — impossible à exfiltrer ou à rejouer. WHfB est le pilier passwordless pour les postes Windows gérés par Intune ou SCCM.

Les **clés FIDO2** (YubiKey, Feitian) offrent une authentification résistante au phishing pour les navigateurs et les applications OIDC/SAML. Les **Passkeys** synchronisées (Apple Keychain, Google Password Manager, Windows Hello) démocratisent FIDO2 sans matériel dédié. L'**authentification par certificat** (CBA — Certificate-Based Authentication) utilise des certificats X.509 stockés sur smart card ou dans le TPM. Le choix entre ces technologies dépend de la population, des terminaux et du niveau de sécurité requis — le guide FIDO2 et Passkeys détaille chaque option.

Technologie	Résistant phishing	Matériel requis	UX	Population cible
Windows Hello for Business	Oui	TPM 2.0	Excellente	Postes Windows gérés
FIDO2 (clé physique)	Oui	Clé USB/NFC	Bonne	Admins, VIP
Passkeys (synced)	Oui	Aucun	Excellente	Tous utilisateurs
Certificate-Based Auth	Oui	Smart card/TPM	Moyenne	Env. réglementés
Microsoft Authenticator	Partiel	Smartphone	Bonne	Transition / fallback

SSPR : le filet de sécurité pendant la transition

Le *Self-Service Password Reset* (SSPR) permet aux utilisateurs de réinitialiser leur mot de passe sans appeler le helpdesk. Dans une stratégie passwordless, le SSPR joue un rôle transitoire mais critique. Pendant la migration, certains utilisateurs et certaines applications nécessitent encore un mot de passe comme fallback. Le SSPR sécurisé (avec MFA obligatoire pour la réinitialisation) évite que ce fallback ne devienne un vecteur d'attaque.

La configuration SSPR dans Entra ID : exigez au minimum deux méthodes de vérification pour la réinitialisation (Microsoft Authenticator + email alternatif ou téléphone). Activez le password writeback vers l'AD on-premise pour les environnements hybrides. Configurez les notifications de changement de mot de passe. Et progressivement, quand l'adoption passwordless atteint 90%+, vous pouvez restreindre le SSPR aux cas d'urgence et désactiver l'option de mot de passe pour les comptes pleinement migrés.

Temporary Access Pass : l'onboarding sans mot de passe

Le **Temporary Access Pass** (TAP) résout le problème de l'œuf et de la poule du passwordless. Comment un nouvel employé enregistre-t-il sa méthode d'authentification passwordless s'il n'a pas encore de méthode d'authentification ? Le TAP est un code temporaire à usage unique, généré par l'IT, que l'employé utilise lors de sa première connexion pour enregistrer son Windows Hello, sa Passkey ou sa clé FIDO2.

Le workflow d'onboarding passwordless : le RH crée le dossier dans le SIRH, l'IGA provisionne le compte Entra ID, l'IT génère un TAP valide 24 heures et le communique au nouvel arrivant de manière sécurisée (en personne ou via un canal vérifié). Le jour J, l'employé utilise le TAP pour se connecter, enregistre WHfB et une Passkey de backup, et le TAP expire automatiquement. Le mot de passe n'a jamais existé sur ce compte. C'est l'approche Zero Trust appliquée dès le premier jour.

Gérer la transition et les résistances

La conduite du changement est le facteur n°1 de succès d'un projet passwordless. Les utilisateurs sont attachés à leurs habitudes, même quand ces habitudes les frustrent (oublier son mot de passe tous les 90 jours est frustrant, mais familier). Trois leviers fonctionnent. La

démonstration par l'exemple : commencez par les équipes IT qui deviendront des ambassadeurs. La **communication sur les bénéfices utilisateur** : « plus jamais de mot de passe à retenir, connexion en 2 secondes avec votre empreinte ». Le **support renforcé** pendant les 4 premières semaines : permanence helpdesk dédiée, tutoriels vidéo, FAQ en ligne.

Les cas d'usage qui résistent au passwordless : les postes partagés (kiosques, ateliers), les applications legacy qui exigent un mot de passe dans leur mécanisme d'authentification interne, les accès d'urgence break-glass et les comptes de service. Pour chaque cas, documentez la solution de contournement : badge NFC + PIN pour les kiosques, fédération SAML/OIDC devant les applications legacy, TAP pour les break-glass, vault de secrets pour les comptes de service.

Métriques et suivi de la migration passwordless

Cinq *KPIs* mesurent la progression du passwordless. Le **taux d'adoption passwordless** : pourcentage d'authentifications sans mot de passe sur le total (cible : 95% à 12 mois). Le **nombre de tickets helpdesk MDP** : doit diminuer de 40% minimum. Le **nombre d'incidents phishing réussis** : doit tendre vers zéro pour les utilisateurs migrés. Le **temps moyen d'authentification** : doit être inférieur avec le passwordless (WHfB : 2 secondes vs mot de passe + MFA : 15 secondes). Le **score de satisfaction utilisateur** : sondage trimestriel sur l'expérience d'authentification.

Intégrez ces métriques dans un tableau de bord présenté mensuellement au COMEX. Le ROI passwordless est tangible et mesurable : réduction des coûts helpdesk (25-70€ x nombre de tickets éliminés), réduction des incidents (coût moyen d'un phishing réussi : 50-200 k€) et gain de productivité (11 heures/an/employé x coût horaire). Selon Microsoft, les organisations passwordless réduisent leurs coûts d'authentification de 75% en moyenne.

Questions fréquentes sur la stratégie passwordless

Que se passe-t-il si la biométrie WHfB échoue ?

Windows Hello for Business offre toujours un fallback vers le PIN protégé par TPM. Ce PIN n'est PAS un mot de passe : il est lié au device et protégé par la puce TPM, ce qui le rend impossible à exfiltrer ou à rejouer sur un autre poste. En cas d'échec du PIN, une Passkey de backup ou une clé FIDO2 secondaire prend le relais. Le mot de passe ne revient dans l'équation que comme dernier recours d'urgence, protégé par MFA et session restreinte.

Comment déployer le passwordless avec un AD on-premise ?

Windows Hello for Business supporte le déploiement hybride avec AD on-premise via cloud trust ou key trust. Le cloud trust (recommandé) utilise Entra ID comme autorité de confiance et ne nécessite pas de PKI dédiée. Le key trust nécessite une PKI enterprise pour les certificats de contrôleurs de domaine. Dans les deux cas, Entra Connect synchronise les clés entre Entra ID et l'AD on-premise. Le résultat : authentification passwordless sur les postes Windows avec SSO vers les ressources AD et les applications cloud.

Quel budget prévoir pour un projet passwordless de 1000 utilisateurs ?

Le budget varie selon l'approche choisie. WHfB est gratuit si vos postes ont un TPM 2.0 (standard depuis 2016). Les Passkeys sont gratuites. Les clés FIDO2 pour les 100-200 admins et VIP coûtent entre 10 000 et 20 000€ (2 clés par personne). Le coût principal est la conduite du changement et le support : 30 à 50 k€ pour la communication, la formation et le support renforcé. Le ROI est atteint en 6 à 12 mois grâce à la réduction des tickets helpdesk et des incidents.

Sources et références : ANSSI · MITRE ATT&CK

Synthèse et premières actions

Le passwordless n'est plus une utopie technologique — c'est une réalité déployable avec les outils disponibles en 2026. Votre feuille de route commence cette semaine : activez le SSPR, bloquez les legacy protocols, déployez WHfB sur les postes des équipes IT. En trois mois, vos premiers utilisateurs seront passwordless. En douze mois, 95% de votre organisation peut fonctionner sans aucun mot de passe. Chaque mot de passe éliminé est un vecteur d'attaque en moins et une frustration utilisateur en moins. Le futur de l'authentification est déjà là — il ne vous reste qu'à le déployer. Pour aller plus loin, consultez les recommandations ANSSI sur l'authentification et les mots de passe.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr