

Présentation

ADSelfService Plus

novembre 2023

Présentation ADSelfService Plus

Solution de gestion des mots de passe en libre-service et d'authentification unique pour les applications Active Directory et cloud

1. Réinitialisation de mot de passe en libre-service partout, à tout moment

Tickets de réinitialisation de mot de passe, fléau des DSI et des utilisateurs. Lorsque le nombre de ces tickets augmente, la DSI repousse souvent des problèmes cruciaux afin que les utilisateurs n'arrêtent pas leur tâche trop longtemps en attente de la réinitialisation du mot de passe. Si rien n'est fait, ces tickets peuvent devenir coûteux, près de 30 % de tous les tickets d'assistance résultant de mots de passe oubliés. Il n'est pas étonnant que de grandes entreprises aient dépensé plus d'un million de dollars à tenter de régler des appels d'assistance liés aux mots de passe.

ADSelfService Plus est un outil de gestion des mots de passe en libre-service et d'authentification unique qui permet de traiter tous les tickets de réinitialisation de mot de passe. En bref, qu'il s'agisse d'un mot de passe Office 365 ou Active Directory (AD) oublié, ADSelfService Plus permet aux utilisateurs de réinitialiser eux-mêmes leur mot de passe, sans assistance.

Avec l'adoption croissante d'applications cloud et de stratégies d'usage du matériel personnel (BYOD), les utilisateurs exploitent plusieurs points d'accès en plus de leur PC Windows pour remplir leur tâche. ADSelfService Plus leur permet d'effectuer une réinitialisation de mot de passe et un déverrouillage de compte en libre-service, qu'ils se trouvent au bureau, en déplacement ou chez eux.

1.1 Réinitialisation de mot de passe d'écrans de connexion

Permet aux utilisateurs de réinitialiser des mots de passe de leurs écrans de connexion Windows, macOS et Linux.

1.2 Réinitialisation de mot de passe d'appareils mobiles

Permet aux utilisateurs de réinitialiser leurs mots de passe de leurs appareils Android et iOS.

1.3 Réinitialisation de mot de passe d'un réseau privé

Permet aux utilisateurs de mettre à jour leurs identifiants en cache local après une réinitialisation de mot de passe à distance.

1.4 Réinitialisation de mot de passe de navigateurs Web

Permet aux utilisateurs de réinitialiser en toute sécurité leurs mots de passe via un navigateur Web dans le portail ADSelfService Plus.

Plates-formes prises en charge

ADSelfService Plus prend en charge plusieurs annuaires d'utilisateurs comme AD, OpenLDAP, AD LDS, G Suite, MS SQL, Salesforce, Microsoft 365, AS400, HP UX, Oracle DB et d'autres.

Méthodes d'authentification multifacteur (MFA) strictes pour protéger la réinitialisation de mot de passe

ADSelfService Plus permet aux administrateurs de déclencher un workflow d'authentification préconfiguré lorsqu'un utilisateur lance une réinitialisation de mot de passe. Le produit offre plus de 16 méthodes, dont la biométrie et YubiKey, pour authentifier des utilisateurs lors d'une réinitialisation de mot de passe ou d'un déverrouillage de compte en libre-service. Certains utilisateurs ont accès à des données d'entreprise sensibles et si un individu malveillant pirate leurs comptes, cela peut entraîner de graves conséquences. Pour l'éviter, ADSelfService Plus permet aux administrateurs d'appliquer différents types d'authentification à différents types d'utilisateurs.

The screenshot shows the 'Multi-factor Authentication' configuration page in the ADSelfService Plus interface. On the left is a navigation menu with options: Self-Service, Policy Configuration, Multi-factor Authentication (selected), Password Expiration Notification, Password Policy Enforcer, Directory Self Service, Administrative Tools, and Security Center. The main content area is titled 'Multi-factor Authentication' and includes a dropdown to 'Choose the Policy' (currently set to 'cloudssp.com'). Below this are two tabs: 'Authenticators Setup' and 'MFA / TFA Settings' (which is active). The 'MFA / TFA Settings' tab contains several sections: 'Enrollment Settings' with checkboxes for 'Enforce these authenticators during enrollment' and 'Hide Enrollment tab from end users portal for enrolled users'; 'MFA for Reset / Unlock' with a dropdown to 'Enable' (set to '3') and a dropdown for 'Configure authenticators for reset / unlock' (set to 'SMS Verification, Google Authenticator'); 'TFA for ADSelfService Plus Login' with a checked checkbox for 'Enable authenticators for ADSelfService Plus login' and a dropdown for 'Security Questions, Email Verification'; and 'Endpoint MFA' with checkboxes for 'Select the second authentication factor' and 'Bypass TFA if ADSelfService Plus is down'. At the bottom are 'Save Settings' and 'Cancel' buttons.

2. Notification d'expiration de mot de passe Active Directory pour un nombre illimité d'utilisateurs

Coût informatique indéniable des mots de passe Active Directory expirés.

Il est crucial de changer régulièrement les mots de passe Active Directory, car cela empêche des pirates d'accéder à des ressources réseau même s'ils volent des identifiants d'utilisateur. La définition de l'expiration des mots de passe sur un nombre de jours donné (par exemple, 90) est une pratique courante des administrateurs informatiques. Toutefois, les utilisateurs oublient de changer leurs mots de passe arrivant à expiration et créent un ticket de réinitialisation car ils :

- Possèdent des comptes Active Directory pour un VPN ou Outlook Web Access et ne se connectent donc jamais de façon interactive pour consulter les notifications Windows.
- Ils ne prêtent pas attention au rappel d'expiration du mot de passe dans leur barre des tâches Windows.
- Utilisent des postes de travail macOS ou Linux et ne reçoivent donc pas les notifications Active Directory.

3. Authentification multifacteur de terminal (MFA)

Protéger l'accès du point d'entrée des attaques

On estime à 70 % la proportion des violations ayant pour origine les terminaux, d'où l'urgence pour les administrateurs de prendre des mesures afin d'éviter ces intrusions grâce à l'authentification multifacteur (MFA). Cette fonctionnalité veille à ce que les utilisateurs prouvent leur identité via d'autres méthodes d'authentification comme la biométrie à la connexion à un poste de travail, un serveur ou un VPN. Son déploiement atténue les risques d'exposer des données sensibles, même en cas de mots de passe compromis à cause de pratiques inadéquates.

Repenser la sécurité des terminaux avec la MFA

ADSelfService Plus offre une solution d'authentification multifacteur de terminal pour aider les organisations à protéger divers points d'accès à leurs ressources sensibles. Cette solution protège l'accès à :

1. Machines Windows, macOS et Linux.
2. Principaux fournisseurs de VPN comme Fortinet, Cisco AnyConnect, Pulse, etc.
3. Terminaux compatibles avec l'authentification RADIUS comme Citrix Gateway, VMware Horizon et Microsoft Remote Desktop Gateway (RDP).

Protection intégrale des terminaux : fonctionnalité MFA d'ADSelfService Plus en action

Une fois l'authentification multifacteur de terminal établie, les utilisateurs s'authentifient d'abord via des identifiants de domaine Active Directory (AD), puis à l'aide de méthodes d'authentification comme des mots de passe à usage unique (OTP) envoyés par SMS ou courrier ou Yubico selon la configuration d'ADSelfService Plus. Ainsi, même si des pirates exploitent des identifiants d'utilisateur compromis, la MFA contrecarre leurs tentatives d'attaque.

ADSelfService Plus propose 17 méthodes d'authentification n'exigeant pas toujours un périphérique matériel externe (par exemple, questions de sécurité AD) ou sans impact sur la productivité des utilisateurs (par exemple, biométrie). Toutefois, il va de soi que différentes méthodes d'authentification conviennent mieux à divers groupes d'utilisateurs. Demander à des utilisateurs ne connaissant que les mots de passe à usage unique d'utiliser des jetons matériels engendre de nombreuses plaintes. De plus, certains utilisateurs disposent de privilèges supérieurs à d'autres. La protection des comptes privilégiés avec d'autres méthodes d'authentification est plus logique que d'appliquer le même nombre de facteurs à tous les utilisateurs de l'organisation.

ADSelfService Plus permet aux administrateurs d'utiliser différentes stratégies pour divers groupes d'utilisateurs afin de limiter les perturbations. Par exemple,

ils peuvent imposer des mots de passe à usage unique, des jetons ou des questions de sécurité pour un groupe d'utilisateurs (ceux au sein du réseau local) et configurer des méthodes d'authentification plus strictes comme l'empreinte digitale ou la reconnaissance faciale pour un autre (les hauts dirigeants ou les télétravailleurs).

Liste des méthodes d'authentification prises en charge :

1. Questions et réponses de sécurité
2. Vérification par courrier électronique
3. Vérification par SMS
4. Google Authenticator
5. Microsoft Authenticator
6. Duo Security
7. RSA SecurID
8. Authentification RADIUS
9. Authentification par notification directe
10. Empreinte digitale et reconnaissance faciale
11. Authentification par code QR
12. Mot de passe à usage unique et durée définie (TOTP)
13. SAML Authentication
14. Questions de sécurité AD
15. Authentification YubiKey
16. Mot de passe à usage unique et durée définie (TOTP)
17. Custom TOTP Authenticator

ADSelfService Plus offre des outils pour aider les administrateurs et simplifier l'administration:

1. **MFA selon l'OU ou le groupe** : appliquez une authentification multifacteur de terminal et adoptez différents jeux de méthodes d'authentification pour divers utilisateurs selon l'appartenance à un domaine, une OU ou un groupe.
2. **Inscription systématique** : automatisez l'inscription des utilisateurs en important des identifiants de domaine via des fichiers CSV ou imposez-la à l'aide de scripts de connexion.
3. **Rapports détaillés** : obtenez un aperçu complet sur l'activité des utilisateurs comme les échecs de vérification d'identité ou les tentatives de connexion et identifiez ceux ayant des mots de passe faibles.
4. **Authentification facile** : utilisez des méthodes d'authentification comme l'empreinte digitale, la notification directe, YubiKey et un code QR pour aider les utilisateurs à prouver leur identité le plus facilement possible.

4. Application d'une stratégie de mots de passe forts

Les cyberattaques deviennent de plus en plus répandues et difficiles à traiter. Les hackers tentent sans cesse d'exploiter des mots de passe faibles communs. Les entreprises doivent donc se protéger dans ce jeu sans fin du chat et de la souris. Et si vous pouviez éviter totalement les mots de passe faibles ? Toute brèche dans la cybersécurité risquant d'avoir de graves conséquences, il est crucial d'appliquer une stratégie de mots de passe forts. Toutefois, l'environnement natif Active Directory n'offre pas beaucoup d'options sur ce plan.

La fonction d'application de mots de passe ADSelfService Plus répond efficacement à ce besoin en vous permettant d'instaurer des règles sur mesure. Elle protège les mots de passe Windows Active Directory pour garantir la sécurité de votre organisation.

Exigences de complexité de la stratégie de mots de passe

Garantissez l'efficacité de votre stratégie personnalisée en exigeant que les mots de passe intègrent un ou plusieurs des éléments suivants :

- Une longueur minimale
- Des caractères majuscules et minuscules
- Une lettre en première position
- Des caractères spéciaux
- Des chiffres
- Aucun mot du dictionnaire, sur liste noire ni de modèle facile à casser

Appliquez des exigences plus ou moins strictes selon votre environnement. En outre, vous pouvez définir le nombre d'exigences de complexité que l'utilisateur doit respecter pour établir des mots de passe.

Conformité à une stratégie simple

Affichez les exigences de stratégie dans les pages de réinitialisation et de modification de mot de passe pour veiller à ce que les utilisateurs connaissent les règles. Les mots de passe ne respectant pas ces exigences sont rejetés.



Change Password

Change

- ✓ Minimum length should be at least 8
- ✓ Number of special characters to include 2
- ✓ Must start with a letter
- ✓ Must contain both upper and lowercase characters
- ✓ Number of numerals to include 1
- ✓ Must not be a palindrome
- ✓ Must not contain any character more than twice consecutively
- ✓ Must not have 5 consecutive characters from username
- ✓ Maximum length should not exceed 15



Change Password

Change your current domain password.

Old Password :

New Password :

Confirm New Password :

- ✓ Minimum length should be at least "8"
- ✓ Number of special characters to include "2"
- ✓ Must start with a letter
- ✓ Must contain both upper and lowercase characters
- ✓ Number of numerals to include "1"
- ✓ Must not be a palindrome
- ✓ Must not contain any character more than twice consecutively
- ✓ Must not have 5 consecutive characters from username
- ✓ Maximum length should not exceed "15"

Change Password

Cancel

Application universelle

Appliquez votre stratégie de réinitialisation des mots de passe dans l'écran GINA/CP (Ctrl+Alt+Suppr) et pendant les actions sur les utilisateurs et les ordinateurs Active Directory.

The screenshot shows the Windows Universal App login interface. On the left, there is a back arrow and a user profile icon. The main area is titled 'Other user' and contains a username field with 'user', two password fields with masked characters, and a blue arrow button. Below the password fields, it says 'Sign in to: SSPCHILD'. Underneath, there are links for 'How do I sign in to another domain?' and 'Reset Password / Unlock Account'. A list of password requirements follows, each preceded by a checkmark:

- ✓ Minimum length should be at least 8
- Number of special characters to include 2
- ✓ Must start with a letter
- ✓ Must contain both upper and lowercase characters
- ✓ Number of numerals to include 1
- ✓ Must not be a palindrome
- ✓ Must not contain any character more than twice consecutively
- ✓ Must not have 5 consecutive characters from username
- ✓ Maximum length should not exceed 15

Stratégies de mots de passe granulaires

Définissez des stratégies de mots de passe distinctes pour les objets OU et groupe, hormis celle établie pour le domaine. Cette flexibilité vous permet d'appliquer une stratégie stricte pour les utilisateurs privilégiés qui accèdent à des données sensibles et une allégée pour les autres utilisateurs.

Renforcement de la sécurité sans nuire à la productivité

Vous ne devez pas craindre qu'une stratégie de mots de passe stricte provoque une hausse des demandes de réinitialisation de mot de passe pour votre service d'assistance. ADSelfService Plus offre aussi des fonctionnalités de gestion des mots de passe en libre-service, qui permettent aux utilisateurs de réinitialiser leurs propres mots de passe sans intervention du service d'assistance. ADSelfService Plus garantit qu'une stratégie de mots de passe stricte ne nuit pas à l'efficacité de vos employés ou de votre service d'assistance.

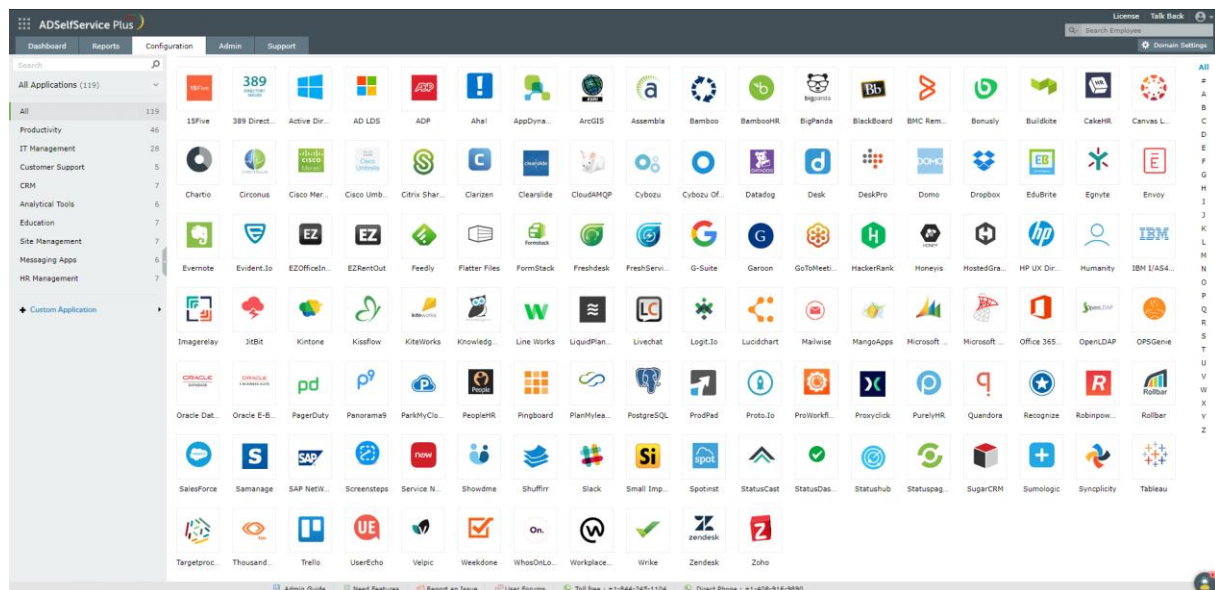
5. Synchronisation de mots de passe Active Directory entre plusieurs plateformes

Dans la plupart des environnements informatiques, le personnel doit mémoriser des identifiants pour les comptes autres que ceux Windows Active Directory par défaut. Pour compliquer les choses, chaque mot de passe fait l'objet de différentes stratégies et dates d'expiration. L'emploi de mots de passe distincts pour différents comptes accroît le risque que l'utilisateur les oublie et crée des tickets de réinitialisation de mot de passe. Le moyen le plus efficace de gérer plusieurs mots de passe consiste à les synchroniser entre toutes les applications connectées en temps réel.

Outil de synchronisation de mots de passe en temps réel d'ADSelfService

Plus : **outil unique pour synchroniser tous les mots de passe d'utilisateur**

ADSelfService Plus, solution de gestion des mots de passe en libre-service et d'authentification unique, permet de synchroniser des mots de passe en temps réel entre plusieurs plateformes. Elle réplique instantanément les changements de mot de passe Windows Active Directory et de compte entre une série d'applications cloud et sur site et offre une solution de gestion unifiée des identités en libre-service pour l'entreprise.



Synchronisez automatiquement les mots de passe Active Directory ou Azure des utilisateurs entre des systèmes SAP, Oracle, IBM, etc.

- Les utilisateurs modifient ou réinitialisent leurs mots de passe Windows Active Directory ou déverrouillent leur compte avec ADSelfService Plus, ou utilisent l'une des méthodes natives de Windows (via l'écran Ctrl+Alt+Suppr et la console ADUC).
- L'outil d'application d'une stratégie de mots de passe vérifie si le mot de passe tapé remplit tous les critères de complexité en vigueur. En savoir plus.

- L'agent de synchronisation de mots de passe enregistre le nouveau mot de passe, le chiffre et le transmet au serveur ADSelfService Plus via le protocole HTTPS. .
- L'agent commence à rechercher l'utilisateur dans d'autres systèmes configurés pour la synchronisation de mots de passe. Si l'identifiant d'utilisateur existe aussi dans les autres systèmes, l'agent de synchronisation effectue automatiquement une réinitialisation du mot de passe dans ces systèmes avec le nouveau mot de passe Windows Active Directory défini par l'utilisateur via ADSelfService Plus.
- ADSelfService Plus synchronise alors le nouveau mot de passe pour toutes les applications cloud configurées.
- Un message ou SMS de notification de changement de mot de passe Active Directory (alerte en temps réel) est envoyé à l'utilisateur pour l'aviser que son mot de passe a été modifié.
- De plus, si le mot de passe n'est pas mis à jour dans Active Directory, un message ou SMS avertit l'utilisateur.

6. Accès conditionnel

Le modèle du télétravail s'est avéré favorable pour les organisations et nombre d'entre elles offrent maintenant cette possibilité à leur personnel. Les utilisateurs distants étant plus exposés aux cyberattaques, il faut établir des mesures de sécurité strictes comme l'authentification multifacteur (MFA) pour éviter des incidents. Toutefois, l'application d'une stratégie d'accès stricte à toute l'organisation risque de nuire à l'expérience utilisateur. Alors que l'authentification à deux ou trois facteurs sécurise la connexion distante, elle peut créer une complication inutile pour les utilisateurs sur site déjà protégés au sein du périmètre du bureau. Une approche plus efficace consiste à appliquer des stratégies d'accès contextuelles. La fonctionnalité de stratégie d'accès conditionnel qu'offre ADSelfService Plus le permet. Cette fonctionnalité aide les organisations à :

- Déployer des contrôles d'accès sans intervention de l'administrateur.
- Améliorer le niveau de sécurité de l'organisation sans nuire à l'expérience utilisateur.

Automatisation de décisions d'accès conditionnel

L'accès conditionnel applique une série de règles qui analysent divers facteurs de risque, comme l'adresse IP, l'heure d'accès, l'appareil et la géolocalisation de l'utilisateur, pour imposer des décisions de contrôle d'accès automatisées. Les décisions s'appliquent en temps réel selon les facteurs de risque de l'utilisateur pour éviter des mesures de sécurité inutilement strictes imposées en l'absence de risque. On garantit ainsi une meilleure expérience utilisateur sans nuire à la sécurité.

L'accès conditionnel permet d'établir certains scénarios courants et les mesures de sécurité correspondantes :

- Authentification biométrique obligatoire à la connexion de l'administrateur.
- Accès à des applications importantes limité à des machines autorisées via l'authentification unique (SSO).
- Instauration de trois niveaux d'authentification pour les demandes de réinitialisation de mot de passe d'adresses à risque ou de clients pas membres du domaine.