

FICHE SOLUTION · GESTION DES ACCÈS ET DES IDENTITÉS (IAM)



## ManageEngine ADSelfService Plus

# Moins d'appels au support. Plus de contrôle sur chaque connexion.

Réinitialisation de mot de passe en libre-service, authentification multifacteur adaptative, authentification unique et politiques de mot de passe granulaires : ADSelfService Plus rend l'accès aux ressources simple pour vos collaborateurs, et contrôlé pour votre DSI.

Active Directory

Microsoft Entra ID

Microsoft 365

Google Workspace

Applications SAML

Windows, macOS, Linux

VPN et RADIUS

OWA et IIS

DEUX ÉDITIONS · LICENCE PAR NOMBRE D'UTILISATEURS

### Standard · Professionnelle

Tarif éditeur à partir de 245 €/an pour 100 utilisateurs de domaine — détail complet en page 4.

## 20

AUTHENTICATEURS  
PRIS EN CHARGE

## MFA

AUX ÉCRANS DE CONNEXION  
WINDOWS, MACOS ET LINUX

## Android · iOS

LIBRE-SERVICE EN MOBILITÉ,  
DANS TOUTES LES ÉDITIONS

## SAML · SCIM

AUTHENTIFICATION UNIQUE  
ET PROVISIONNEMENT JIT

# La sécurité des identités, ramenée à **un seul portail utilisateur.**

## Ce qu'est ADSelfService Plus

ADSelfService Plus réunit dans un portail unique la gestion des mots de passe en libre-service, l'authentification multifacteur et l'authentification unique d'entreprise. Chacun réinitialise son mot de passe, déverrouille son compte, tient à jour sa fiche d'annuaire et rejoint ses applications sans passer par le support. Côté DSI, chaque connexion reste soumise à des règles : politiques granulaires par unité d'organisation et par groupe, exigence d'authentification ajustée au contexte, vérification d'identité avant toute action sensible.

## Ce qu'elle permet de faire

- ◆ Laisser les utilisateurs réinitialiser leur mot de passe et déverrouiller leur compte sans solliciter le support.
- ◆ Protéger par authentification multifacteur les connexions aux machines Windows, macOS et Linux, aux VPN, à OWA et aux applications.
- ◆ Ajuster l'exigence d'authentification au contexte : adresse IP, heure, géolocalisation, appareil.
- ◆ Donner accès à toutes les applications avec un seul identifiant, voire sans mot de passe, et y créer les comptes dès la première connexion.
- ◆ Appliquer des politiques de mot de passe granulaires et synchroniser les mots de passe Active Directory en temps réel.

### PÉRIMÈTRE COUVERT

Active Directory et Entra ID

Microsoft 365, Google Workspace

Applications SAML

Windows, macOS, Linux, VPN, OWA

### MODÈLE DE LICENCE

Par  
utilisateur

DE DOMAINE

+ MFA de  
terminalMODULE  
FACTURÉ  
SÉPARÉMENT

### PRÉREQUIS SYSTÈME

**Processeur** 2,4 GHz · **RAM** 8 Go · **Disque** 100 Go, SSD recommandé

**Windows** Server 2019 et supérieur

**Navigateurs** Firefox, Chrome, Edge

**Bases de données** PostgreSQL par défaut, MS SQL

## Le périmètre couvert par la plateforme – 18 fonctionnalités, détaillées en page 3

### SÉCURISER LES CONNEXIONS

- ◆ MFA adaptative
- ◆ MFA hors ligne
- ◆ Accès conditionnel
- ◆ Sans mot de passe

### OUVRIR ET CONNECTER

- ◆ Authentification unique
- ◆ Provisionnement JIT
- ◆ Synchronisation AD
- ◆ Rapports et intégrations

### GÉRER LES MOTS DE PASSE

- ◆ Réinitialisation
- ◆ Politiques granulaires
- ◆ Alertes d'expiration
- ◆ Identifiants en cache
- ◆ Portail de changement

### AUTONOMISER LES COLLABORATEURS

- ◆ Mise à jour d'annuaire
- ◆ Organigramme
- ◆ Abonnement aux groupes
- ◆ Application mobile
- ◆ Workflow d'approbation

# Dix-huit fonctionnalités, un seul portail utilisateur

## Authentification multifacteur

Imposez une vérification d'identité pour les connexions aux machines Windows, macOS et Linux, aux VPN, à OWA et aux applications d'entreprise. Plus de vingt méthodes sont prises en charge : FIDO2, biométrie, TOTP, cartes à puce, YubiKey, Microsoft Authenticator, Duo Security, RSA SecurID. La protection s'étend aux comptes locaux des machines Windows, en groupe de travail comme en domaine.

## MFA hors ligne

Les collaborateurs qui ouvrent leur session sans lien réseau restent soumis à l'authentification multifacteur, sur Windows comme sur macOS. Le déplacement et la coupure de connexion cessent d'être des angles morts.

## Accès conditionnel

Automatisez le contrôle d'accès en modulant l'exigence d'authentification selon le contexte : adresse IP, heure de connexion, géolocalisation, appareil utilisé. Une connexion habituelle passe sans friction, une connexion inhabituelle déclenche un contrôle supplémentaire.

## Authentification unique d'entreprise

Reliez vos applications d'entreprise à l'Active Directory : une seule authentification avec les identifiants du domaine ouvre l'accès à l'ensemble du parc applicatif, sans multiplier les mots de passe ni les portails.

## Connexion sans mot de passe

Supprimez le mot de passe des connexions aux applications d'entreprise et fermez la porte aux attaques fondées sur le vol d'identifiants. L'authentification multifacteur prend le relais comme facteur de confiance.

## Provisionnement juste à temps

Le compte utilisateur se crée automatiquement dans l'application intégrée au moment de la première connexion, selon la norme SCIM. L'arrivée d'un collaborateur ne suppose plus une série de créations manuelles application par application.

## Réinitialisation en libre-service

L'utilisateur réinitialise son mot de passe et déverrouille son compte lui-même, après vérification d'identité, depuis le portail web, l'écran de connexion de sa machine ou l'application mobile. Le service d'assistance n'est plus dans la boucle.

## Synchronisation des mots de passe

Le mot de passe Active Directory est répercuté en temps réel sur les applications d'entreprise. Les utilisateurs circulent entre services cloud et systèmes sur site avec un seul mot de passe, sans écart entre les référentiels.

## Renforcement des politiques

Définissez des politiques de mot de passe granulaires par unité d'organisation et par groupe, dans Active Directory comme sur les autres plateformes : règles de complexité, restrictions de réutilisation, règle de dictionnaire, blocage des mots de passe compromis via Have I Been Pwned.

## Notifications d'expiration

Prévenez les utilisateurs, sur site comme à distance, de l'expiration prochaine de leur mot de passe ou de leur compte, par e-mail, SMS et notification push, à intervalles que vous fixez.

## Identifiants en cache

Après une réinitialisation à distance, les identifiants stockés sur le poste sont mis à jour automatiquement, avec ou sans connexion VPN. L'utilisateur nomade ne se retrouve pas bloqué avec deux mots de passe divergents.

## Portail web de changement

Les collaborateurs à distance disposent d'un portail sécurisé pour modifier leur mot de passe de domaine et celui de leurs applications d'entreprise, sans accès au réseau interne.

## Mise à jour de l'annuaire

Les utilisateurs actualisent eux-mêmes certains attributs de leur fiche Active Directory : adresse e-mail, numéro de téléphone, photo. Les données de l'annuaire restent justes sans intervention d'un administrateur.

## Annuaire et organigramme

Un annuaire d'entreprise complet permet de rechercher un collaborateur, un contact ou un groupe, et une vue en organigramme situe chacun dans la hiérarchie et son équipe.

## Abonnement aux groupes

Définissez des règles d'abonnement et laissez les utilisateurs rejoindre ou quitter certains groupes de distribution quand leur rôle évolue, sans ticket au support technique.

## Application mobile

L'application ADSelfService Plus, disponible sur Android et iOS, porte les actions en libre-service en déplacement. Elle est incluse dans toutes les éditions, sans coût supplémentaire.

## Rapports et intégrations

Des rapports d'audit prédéfinis retracent les tentatives de vérification d'identité, les actions en libre-service et l'état des mots de passe et des comptes. Le produit s'intègre par ailleurs aux solutions SIEM, ITSM et IAM en place.

## Workflow d'approbation

Pour les organisations qui veulent garder la main, les demandes en libre-service peuvent être routées vers l'équipe support pour validation avant exécution.

# Deux éditions. On vous aide à choisir la vôtre.

| LICENCE – ABONNEMENT ANNUEL   | STANDARD  | PROFESSIONNELLE |
|-------------------------------|-----------|-----------------|
| 100 utilisateurs de domaine   | 245 €     | 345 €           |
| 200 utilisateurs de domaine   | 345 €     | 595 €           |
| 500 utilisateurs de domaine   | 595 €     | 1 195 €         |
| 1 000 utilisateurs de domaine | 1 195 €   | 2 195 €         |
| 1 500 utilisateurs de domaine | 1 745 €   | 2 895 €         |
| 2 000 utilisateurs de domaine | 2 195 €   | 3 495 €         |
| 3 000 utilisateurs de domaine | 3 145 €   | 4 695 €         |
| 5 000 utilisateurs de domaine | 4 995 €   | 6 995 €         |
| Au-delà de 5 000 utilisateurs | sur devis | sur devis       |

## Module MFA de terminal

de 195 € à 6 795 €/an

De 100 à 5 000 utilisateurs, en édition Standard ou Professionnelle. C'est ce module qui porte la MFA sur les machines Windows, macOS et Linux, les VPN et serveurs RADIUS, OWA et IIS. Dix licences Standard sont incluses dans toute installation.

## Extensions Failover et SMS

395 €/an · SMS à partir de 595 €

Failover : haute disponibilité, répartition de charge et proxy inverse, même tarif dans les deux éditions. SMS : crédits Clickatell, modèle perpétuel, à partir de 2 000 crédits, traitement possible hors zone UE.

Tarifs publics éditeur, abonnement annuel, licence assise sur le nombre d'utilisateurs du ou des domaines — source : ManageEngine, page de tarification ADSelfService Plus, consultée le 13/08/2026. Prix indicatifs et non contractuels : le montant dépend du nombre d'utilisateurs, de l'édition retenue et des modules additionnels. Devis personnalisé LAZAR SOFT sur demande.

## COMMUN AUX DEUX ÉDITIONS

- ◆ Portail web de réinitialisation et de déverrouillage
- ◆ MFA pour la réinitialisation et le déverrouillage
- ◆ Notifications d'expiration de mot de passe et de compte
- ◆ Politiques de mot de passe sur le portail et l'application mobile
- ◆ Synchronisation des mots de passe
- ◆ Mise à jour de l'annuaire, organigramme et abonnement aux groupes

## RÉSERVÉ À L'ÉDITION PROFESSIONNELLE

- ◆ Réinitialisation depuis les écrans de connexion Windows, macOS et Linux
- ◆ Réinitialisation depuis l'application mobile et le navigateur mobile
- ◆ Accès conditionnel
- ◆ Politiques de mot de passe dans ADUC et à l'écran Ctrl+Alt+Suppr
- ◆ Mise à jour des identifiants en cache pour la réinitialisation à distance

## POUR ÉVALUER

- ◆ **Édition d'évaluation** — édition Professionnelle complète, module MFA de terminal inclus, utilisateurs illimités pendant 30 jours, puis bascule en édition gratuite
- ◆ **Édition gratuite** — fonctions de l'édition Standard, limitée à 50 utilisateurs sans limite de durée, avec le MFA de terminal Standard pour 10 utilisateurs

## Contactez-nous.

Une question ou un chiffrage précis : un #RocketExpert vous répond sous 24 h ouvrées.

TÉLÉPHONE

**+33 (0)1 76 21 60 43**

E-MAIL

**sales@lazarsoft.com**