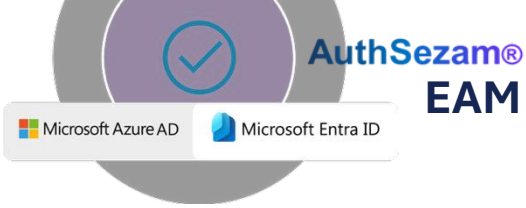
Fiche produit



AuthSezam EAM* est une **solution quick-win** qui s'intègre de façon **transparente à Microsoft Entra-ID** pour **simplifier la connexion et renforcer le niveau de sécurité des utilisateurs internes et externes.**

Son lien sécurisé contient des technologies avancées de **trace cryptographique** et d'**évaluation des risques** de chaque connexion en temps réel. Par essence, la solution fournit une solution antibot avancée « User-Centric » avec des **informations instantanées** et des **actions automatisables**.

Cas d'utilisation recommandés

AuthSezam 2nd facteur pour Entra ID : Idéal pour les entreprises qui utilisent Microsoft et qui cherchent à intégrer une solution d'authentification permettant de répondre à des cas d'usage de connexion par lien sécurisé (email, sms, messagerie instantanée, web push).

Présentation de la solution

Simple d'utilisation et de déploiement, grâce au **2nd facteur par lien sécurisé AuthSezam EAM**, vous pouvez rapidement mettre en place un contrôle d'accès MFA dans votre organisation pour les utilisateurs internes et externes.

Intuitif pour l'utilisateur, l'usage du lien ne nécessite aucune installation logicielle de la part de l'utilisateur.

Les comptes étant gérés depuis Entra ID, le parcours de création de compte MFA est donc transparent pour l'utilisateur et ne nécessite pas de formation ou de temps de support pour accompagner le déploiement de l'enrôlement.

L'usage du lien sécurisé peut également vous permettre de vérifier que le sous-traitant a toujours accès à sa boîte email professionnelle et qu'il est donc toujours salarié de l'entreprise externe. De plus, le contrôle au moment de la connexion est renforcé par une IA de 1èr niveau.

AuthSezam EAM est accessible dès la version Free, mais limité à une configuration **globale et basique**.

Pour plus d'option :

Pour des scénarios **granulaires (groupes, apps)** et la sécurité contextuelle
→ il faut **P1 ou Migrer vers AuthSezam IAM Start ou IAM IA ZT**

Pour du **MFA adaptatif au risque**
→ il faut **P2 ou Migrer vers AuthSezam IAM IA ZT**

Pour du **ZTNA continu (CAE)**
→ il faut **Suite ou Migrer vers AuthSezam IAM IA ZT**

Conformité au RGPD et sécurité dès la conception

- ✓ Renforcement de la surveillance à chaque connexion
- ✓ Détection de nouveaux profils de risque
- ✓ Traçabilité renforcée des logs de connexion
- ✓ Détection des menaces/fraudes personnalisables en option

Trace cryptographique, sans rejet possible des signatures.

Nativement interopérable avec tous les appareils, navigateurs et solutions de surveillance

Conforme aux exigences RGPD/CNIL et d'accessibilité

***EAM (Microsoft Authentication Methode) :** Microsoft Entra ID – External Authentication Methods (EAM) est la fonctionnalité qui permet d'intégrer la solution AuthSezam pour accéder aux ressources d'une organisation.*

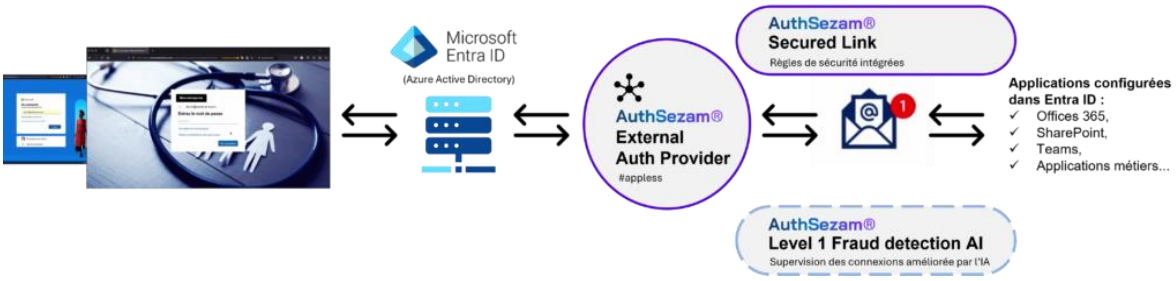
OpenSezam
Trust Authentication

Fiche produit

AuthSezam® EAM

Microsoft Azure AD | Microsoft Entra ID

Parcours de connexion



Cas d'usage

- Sous-traitants avec email professionnel actif
- Tout utilisateur ayant des difficultés d'usages avec les MFA traditionnel

Usage du 2nd facteur par lien

- Lien sécurisé : transmis en standard par email, et diffusable à la demande par SMS, chat interne ou webpush
- Chaque lien est protégé par une trace cryptographique et contrôlé par l'IA Zero Trust à chaque connexion.
- Les utilsateurs équipés de Windows Hello peuvent bénéficier d'une expérience 100% frictionless

Bénéfices pour la DSI :

- Conformité règlementaire en ajoutant un 2nd facteur
- Une fois intégrée, l'administration est transparente depuis Entra-ID
- Pas de flotte mobile à gérer : réduction des coûts et simplification IT.
- Adoption sans assistance

Bénéfices pour les utilisateurs :

- Pas d'enrôlement, ni formation nécessaire
- Pas d'application à installer

Sécurité IA en profondeur

- ✓ Renforcement de la surveillance à chaque connexion.
- ✓ Lien protégé : chaque lien MFA est renforcé par une trace cryptographique unique.
- ✓ IA Zero Trust : contrôle dynamique du contexte d'usage à chaque connexion.
- ✓ Analyse du navigateur, du contexte d'usage et du comportement de l'appareil.

*Génération automatiquement des **rapports détaillés** basés sur l'analyse comportementale et la détection des anomalies.*
Transmission des données possible par API/PushELK

Caractéristique	
Solution	AuthSezam EAM – méthode d'authentification externe pour Microsoft Entra ID
Sans mot de passe	✅
Sans application mobile	✅
Sans téléphone requis	✅ (dans certaines configurations)
Administration	✅ Directement dans Microsoft Entra ID
Cibles	✅ Internes, sous-traitants, profils terrain
Modes	Mot de passe Entra-ID ou Passkey Windows Hello + lien email sécurisé
Sécurité IA	✅ Détection de menace en temps réel à chaque connexion
Standards	OpenID Connect (OIDC) / WebAuthn
Compatibilité	✅ Cross-plateforme (PC, mobile, navigateur)
Interopérabilité	✅ Pas de flotte mobile à gérer : réduction des coûts et simplification IT.
Déploiement	✅ Adoption sans assistance avec un enrôlement à l'usage et sans application à installer (pré-enrollé par l'administrateur en amont depuis Entra ID)
Documentation	Tutoriel Entra ID
Page produit	AuthSezam EAM

OpenSezam Trust Authentication