



Protégez les identités Active Directory via un accès sur site, dans le cloud et à distance

Désormais, vous pouvez arrêter les connexions non autorisées à Active Directory (AD) grâce à une gestion MFA et des accès granulaires et efficaces, conçue pour les environnements Active Directory sur site et hybrides comme le vôtre.

Authentification à deux facteurs (2FA)

Activez une authentification à deux facteurs (2FA) personnalisable et simple pour la connexion Windows, le bureau à distance (RDP et passerelle RDS), IIS, VPN, hors ligne, hors domaine et SaaS.

Authentification unique (SSO)

Associez SSO à MFA pour offrir un accès sécurisé et fluide aux applications Microsoft 365 et SaaS en utilisant uniquement les informations d'identification Active Directory (AD).

Gestion des accès contextuels

Prenez le contrôle grâce à la possibilité de définir des restrictions d'accès granulaires basées sur des facteurs contextuels et basés sur les rôles :

- **Origine** : définissez l'accès en fonction de la machine, de l'emplacement, du rôle de l'utilisateur, etc. pour un utilisateur, un groupe ou une unité organisationnelle (UO).
- **Heure** : définissez les heures de connexion et les limites de durée de session en définissant un quota de temps de connexion.
- **Type de session** : gérez l'accès aux sessions de poste de travail, de terminal, Wi-Fi, VPN, IIS, SaaS, Bureau à distance (passerelle RDP et RD) et VDI.
- **Connexions simultanées** : limitez les connexions simultanées et définissez le nombre de points d'accès initiaux à autoriser par utilisateur, groupe ou unité d'organisation.

Number of initial access points allowed

Initial access points

Number of concurrent sessions allowed

Workstation sessions

Terminal sessions

Total interactive sessions

Wi-Fi / VPN sessions

IIS sessions

User status Session type User name

Protected	Workstation	Arianna BAKER
Protected	IIS	Aaliyah CAMPBE
High risk	Wi-Fi / VPN Workstation	Ava DAVIS
Protected	Terminal Workstation	Administrator
Protected	Wi-Fi / VPN	Audrey EVANS
New	Workstation	Alexis HILL
Protected	Workstation	Alyssa LOPEZ
Risk	Wi-Fi / VPN	Avery RODRIGUE

Gestion des sessions et surveillance des utilisateurs

Obtenez de la clarté grâce à une visibilité en temps réel sur l'accès des utilisateurs, configurez des alertes et répondez à distance pour bloquer ou restreindre n'importe quelle session directement depuis la console.

Session	Session status	Session type
WKS058	Open	Workstation
WKS068	Open	Workstation
WKS011	Open	Workstation
WKS018	Locked	Workstation
APPSERVER01	Locked	Terminal
APPSERVER03	Locked	Terminal
WKS071	Open	Workstation
WKS050	Open	Workstation
WKS049	Open	Workstation
WKS036	Open	Workstation

Block a user

Arianna BAKER

Message to display

Your account is blocked.

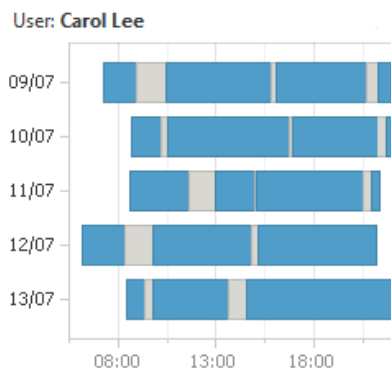
Close existing sessions and block user
 Leave existing sessions open but block us

Audit de connexion utilisateur

Suivez et enregistrez tous les événements de connexion des utilisateurs Windows avec un audit précis sur votre réseau Active Directory, le tout à partir d'un tableau de bord convivial et filtrable.

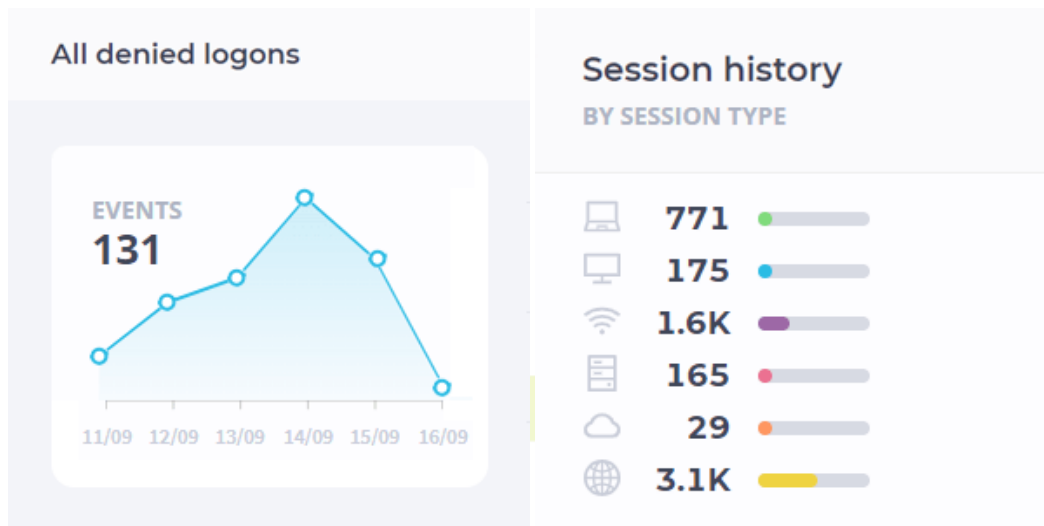
User	Deny reason
John LEACH	Machine restriction
Sue CARTER	Concurrent session restriction
Mike CROSS	Hour restriction
Todd DAVIS	Time quota restriction
Robyn WELDO	Initial access point restriction
Mike CROSS	Machine restriction
Sue CARTER	Hour restriction
John LEACH	Concurrent session restriction
Sue CARTER	Machine restriction

WORKING HOURS BY WEEK



Rapports d'activité des utilisateurs et des administrateurs

Créez des rapports sur toutes les activités de connexion/déconnexion des utilisateurs Active Directory, les événements d'authentification multifacteur (MFA), les actions de l'administrateur, les connexions refusées, etc. pour garantir la conformité, prendre en charge les analyses judiciaires et détecter les menaces.



Les avantages UserLock

Vous devez sécuriser les connexions des employés à Active Directory, sans frustrer les utilisateurs finaux ni créer davantage de travail pour le service informatique.

Grâce à une intégration transparente avec Active Directory, UserLock allège la complexité pour les équipes informatiques tout en offrant une expérience conviviale.

- **Protéger toutes les connexions :** Arrêtez tout accès non autorisé provenant d'informations d'identification compromises. Sécurisez les comptes AD avec une authentification forte et des politiques d'accès granulaires, avant que les dégâts ne soient causés.
- **Gérer toutes les connexions :** Bénéficiez d'une visibilité en temps réel et d'une piste d'audit centralisée sur tous les événements d'accès sur le réseau hybride. Surveillez et interagissez à distance avec n'importe quelle session directement depuis la console UserLock.
- **Être conforme sur la sécurisation de l'accès :** Répondez aux exigences réglementaires et d'assurance en prouvant que tous les accès et utilisations des données sont identifiables, audités et attribués à un utilisateur individuel.
- **Simple à utiliser :** UserLock est rapide à déployer, intuitif à gérer et s'adapte sans effort à un nombre illimité d'utilisateurs, afin d'alléger la charge du service informatique.
- **Non perturbateur :** UserLock fonctionne de manière transparente avec votre infrastructure Active Directory existante, réduisant ainsi la complexité et la frustration.
- **Facilement adopté :** Les contrôles granulaires de UserLock permettent des restrictions personnalisées qui protègent l'accès sans gêner inutilement les employés.
- **Rentable :** S'appuyant sur votre investissement dans Active Directory, UserLock offre une sécurité supplémentaire, efficace et abordable qui bloque les menaces avant que les dommages ne soient causés.



Les petits + avec Ozér

Avant de découvrir plus en détails les fonctionnalités de cette solution, découvrez ce qu'Ozér vous propose avec cette offre :

- **Solution self-hosted** = hébergée en France sur les serveurs français d'Ozér
- Appuyez-vous sur notre équipe technique pour sa **mise en place** et son **paramétrage** sur votre SI
- **Formation** et **accompagnement** dans son utilisation
- **Conseils personnalisés** dans une démarche de respect des bonnes pratiques et des référentiels

A propos d'IS Decisions

User Lock est un outil proposé par la société **IS DECISIONS**. Fondée en 2000 à Biarritz, il s'agit d'un éditeur de logiciels de sécurité permettant de renforcer votre défense contre les accès non autorisés et indésirables. Ces logiciels visent tous les secteurs d'activité, quelle que soit la taille de l'entreprise. Aujourd'hui, IS Decisions c'est plus de 3400 clients venant de 129 pays, dont certaines des organisations les plus règlementées et les plus soucieuses de la sécurité au monde (*U.S Army, Barclay, Département de la justice des Etats-Unis...*).

