

Gestion puissante des autorisations avec AEOS

Un contrôle d'accès basé sur les personnes et non les badges



Autorisez les individus, pas les identifiants

Traditionnellement, les systèmes de sécurité attribuent des droits d'accès à des identifiants comme des badges, des empreintes digitales ou des codes PIN. Cependant, le contrôle d'accès n'est pas vécu ainsi par la plupart des gens. Une personne ou un véhicule a besoin d'un accès, ce qui n'est pas le cas d'un badge. AEOS offre un modèle d'autorisation unique qui attribue des droits d'accès à des personnes et des véhicules plutôt qu'à leurs identifiants.

Plus rapide et plus sûr

La flexibilité de ce modèle d'autorisation le rend plus facile à gérer et permet d'éviter les erreurs. L'attribution d'autorisations à des personnes permet de gérer plusieurs identifiants par personne, et de remplacer plus facilement les identifiants. Le nombre ou le type d'identifiants qu'une personne utilise n'a plus d'importance, qu'il s'agisse d'un badge, d'un code-barres imprimé, de son passeport, de son empreinte digitale ou de sa voix, voire même de tous ces éléments conjointement. Tous les identifiants d'une personne sont liés aux mêmes droits d'accès, ce qui facilite grandement l'attribution d'identifiants supplémentaires.

Fonctionnement du modèle d'autorisation

Dans AEOS, les porteurs désignent les personnes et les véhicules. Un porteur peut avoir un ou plusieurs identifiants, tels qu'un badge ou une empreinte digitale. Les porteurs peuvent avoir le droit d'utiliser un ou plusieurs accès ou groupes d'accès durant une tranche horaire spécifique : leur programme horaire et journalier.

Les identifiants, les accès autorisés et les plages de dates/heures pour chaque type de porteurs (p. ex. employé, visiteur ou prestataire) sont associés au sein de modèles de porteurs faciles à gérer. Ces modèles de porteurs peuvent ensuite être attribués à un seul porteur ou à un groupe de porteurs. Un porteur peut se voir attribuer plusieurs modèles de porteurs, tels que employé R&D et personnel d'intervention d'urgence.

Pour les autorisations qui ne s'appliquent qu'à un seul porteur, vous pouvez utiliser un profil de porteur afin de désactiver des autorisations spécifiques figurant dans le modèle de ce porteur.

Automatisez la saisie des données d'autorisation avec le moteur de règles

Le quotidien des administrateurs peut devenir beaucoup plus simple grâce au moteur de règles d'AEOS. Celui-ci peut lier automatiquement et en temps réel les autorisations d'accès aux attributs de la base de données des employés du service RH, tels que le service, le bâtiment ou la date d'embauche. Un simple clic suffit pour appliquer les autorisations à des personnes ou à des groupes complets, localement ou dans le monde entier. Les droits d'accès des employés qui quittent l'entreprise peuvent être bloqués automatiquement. Quant aux autorisations

'Pourquoi saisir manuellement dans le système de contrôle d'accès des données qui se trouvent déjà dans la base de données de l'entreprise ?'

'Si quelqu'un perd son badge, notre réceptionniste peut bloquer l'ancien badge et en attribuer un nouveau en quelques secondes à peine. Je vous assure que je ne plaisante pas.'

des employés qui changent de bureau, elles peuvent être appliquées immédiatement aux nouveaux locaux. Avec le moteur de règles, les changements qui devaient se faire manuellement sont désormais automatisés et appliqués sans erreur. Ainsi, les autorisations sont constamment à jour et les risques de sécurité sont réduits.

Optez instantanément pour des scénarios de sécurité différents grâce aux niveaux de sécurité

En cas d'incident de sécurité grave, il peut être nécessaire de prendre immédiatement des mesures draconiennes. Grâce aux niveaux de sécurité d'AEOS, vous pouvez prédéfinir à votre convenance plusieurs scénarios de sécurité qui peuvent être activés en quelques secondes.

Par exemple, vous pouvez prédéfinir les autorisations et les groupes de porteurs applicables en cas de grève, d'alarme incendie, de journée portes ouvertes ou de visite guidée du bâtiment. Vous pouvez basculer sur le scénario approprié puis revenir au scénario d'autorisation normal dès que le feu vert vous est donné.

La fonctionnalité Niveaux de sécurité convient parfaitement aux contextes suivants :

- Grandes entreprises exerçant leur activité sur divers sites, dans plusieurs régions ou pays.
- Organisations où les allées et venues d'employés et de visiteurs sont nombreuses et complexes.
- Entreprises ayant besoin d'une sécurité renforcée en raison des matières dangereuses ou des marchandises précieuses qu'elles traitent.