Politique MFA et comptes administrateurs

Référence	Version	Date	Catégorie
POL-CYB-003	v1.1	Mai 2025	Cybersécurité

> ***Prioritaire***

L'authentification multifacteur (MFA) est une protection indispensable contre le vol de credentials et les attaques par force brute. Mileo Technology impose le MFA sur l'ensemble des accès d'administration aux systèmes de ses clients. Cette exigence est non négociable et s'applique dès la mise en service, indépendamment des contraintes opérationnelles invoquées.

---

01. Périmètre d'obligation

Le MFA est obligatoire pour tous les accès administrateurs aux systèmes suivants : logiciels VMS (Video Management System), enregistreurs NVR et DVR disposant d'une interface d'administration réseau, routeurs et pare-feu, concentrateurs VPN, contrôleurs d'accès et leurs logiciels de gestion.

Les accès aux interfaces d'administration cloud des constructeurs (portails de gestion à distance) sont également concernés. La vérification de la disponibilité du MFA sur chaque équipement ou logiciel est réalisée en phase de conception de projet ; les équipements ne supportant pas le MFA font l'objet d'une dérogation documentée.

Les accès VPN réalisés par les techniciens de Mileo Technology pour la maintenance à distance sont systématiquement protégés par MFA, indépendamment du niveau d'accès utilisé lors de la session.

---

02. Méthodes acceptées

Les méthodes MFA acceptées sont : les applications TOTP (Time-based One-Time Password) telles que Google Authenticator, Microsoft Authenticator ou Aegis ; les clés de sécurité physiques FIDO2/WebAuthn (YubiKey, Nitrokey). Ces méthodes offrent une résistance éprouvée aux attaques de phishing et d'interception.

L'authentification par SMS (OTP envoyé par message texte) est explicitement interdite en raison de sa vulnérabilité aux attaques de type SIM swapping et SS7. Les notifications push applicatives sans confirmation du contexte de la demande sont déconseillées et soumises à validation préalable.

Les clés FIDO2 sont la méthode recommandée pour les comptes d'administration à privilèges élevés (super-administrateurs, accès à l'infrastructure réseau). Leur coût est intégré dans les devis de projet pour les sites critiques.

---

03. Comptes de service

Les comptes de service (utilisés par des applications ou scripts pour accéder aux systèmes, sans intervention humaine) ne peuvent pas utiliser le MFA interactif par nature. Ces comptes sont donc soumis à des compensations de sécurité renforcées : mots de passe de 32 caractères minimum générés aléatoirement, restriction d'accès à l'adresse IP ou au réseau source, principe de moindre privilège strict.

La création d'un compte de service doit être formellement documentée et validée par le référent cybersécurité. Le registre des comptes de service est maintenu à jour et révisé semestriellement. Tout compte de service inactif depuis plus de 90 jours est désactivé.

---

04. Exceptions et dérogations

Toute exception à l'obligation MFA doit être formellement documentée : identifiant du compte concerné, justification technique (équipement ne supportant pas le MFA), mesures compensatoires mises en place, durée de la dérogation, et validation par le référent cybersécurité.

Les dérogations sont enregistrées dans un registre dédié, révisé trimestriellement. Chaque dérogation est accompagnée d'un plan

d'action visant à sa résolution (remplacement de l'équipement, mise à jour du firmware ajoutant le support MFA, etc.).

Aucune dérogation permanente n'est acceptée pour les accès distants sur Internet. Si un équipement ne supporte pas le MFA et doit rester accessible à distance, il doit impérativement être placé derrière un VPN lui-même protégé par MFA.

---

05. Gestion des comptes administrateurs

Les comptes administrateurs sont strictement nominatifs : aucun compte générique partagé entre plusieurs personnes n'est autorisé. Chaque intervenant dispose de son propre compte avec ses propres credentials et son propre second facteur. Cette règle garantit la traçabilité individuelle de toutes les actions d'administration.

> **Les droits administrateurs sont attribués selon le principe du moindre privilège : un technicien en charge de la maintenance vidéo ne dispose pas d'accès administrateur au réseau, et inversement. Les droits sont documentés dans la fiche de configuration du site et révisés lors de chaque intervention.**

Boulevard de Courcelles, 75008 Paris — hello@mileotech.com