Politique de gestion des mots de passe

Référence	Version	Date	Catégorie
POL-CYB-002	v1.0	Mars 2025	Cybersécurité

La gestion des mots de passe est un pilier fondamental de la sécurité des systèmes installés. Des mots de passe faibles ou réutilisés constituent la principale porte d'entrée des attaquants sur les systèmes de vidéosurveillance exposés. Cette politique définit les exigences minimales applicables à l'ensemble des comptes créés ou gérés par Mileo Technology sur les installations de ses clients.

---

01. Exigences de complexité

Tout mot de passe créé ou modifié par Mileo Technology doit comporter un minimum de 16 caractères. Cette longueur minimale est portée à 20 caractères pour les comptes administrateurs et les comptes de service accédant à plusieurs systèmes.

Les mots de passe doivent combiner au minimum : une lettre majuscule, une lettre minuscule, un chiffre et un caractère spécial (parmi : ! @ # $ % ^ & * - _ = + [ ] { } | ; : , . ?). Les séquences prévisibles (123456, azerty, le nom du site ou de l'entreprise) sont explicitement interdites.

La complexité est vérifiée lors de la création du compte, idéalement par la fonction de contrôle intégrée au système. En l'absence de contrôle automatique, le technicien utilise un outil de vérification de force de mot de passe avant saisie.

---

02. Interdiction des mots de passe par défaut

Le remplacement des mots de passe par défaut du constructeur est une étape obligatoire et non négociable de toute mise en service. Aucun équipement ne peut être rendu opérationnel sans que ses mots

de passe d'usine aient été remplacés. Cette vérification figure dans la check-list de mise en service.

Les mots de passe par défaut connus (admin/admin, root/root, 12345, etc.) sont formellement interdits, même sur des systèmes supposément isolés du réseau. Un équipement découvert avec son mot de passe d'usine lors d'une intervention est immédiatement signalé et corrigé.

---

03. Rotation et renouvellement

Les mots de passe des comptes administrateurs sont renouvelés annuellement au minimum, ou immédiatement en cas de suspicion de compromission, de départ d'un collaborateur ayant eu accès au mot de passe, ou d'incident de sécurité.

Les mots de passe des comptes d'exploitation (opérateurs, visualisation) sont renouvelés tous les 18 mois. Le client est informé de cette exigence et ses équipes sont formées à la procédure de renouvellement lors de la formation initiale.

L'historique des mots de passe est conservé : un mot de passe ne peut être réutilisé avant un minimum de 12 cycles de renouvellement. Cette règle est configurée dans les systèmes qui la supportent ; pour les autres, elle est appliquée par procédure organisationnelle.

---

04. Gestionnaire de mots de passe

Mileo Technology impose l'utilisation d'un gestionnaire de mots de passe agréé pour la conservation de l'ensemble des credentials des systèmes clients. La mémorisation manuelle ou la conservation dans un fichier non chiffré (tableur, bloc-notes, email) est formellement interdite.

Le coffre-fort de mots de passe est organisé par client et par site, avec des droits d'accès nominatifs. Seuls les collaborateurs ayant besoin d'accéder à un compte y ont accès. Les accès au gestionnaire sont eux-mêmes protégés par un mot de passe maître fort et par MFA.

En cas de départ d'un collaborateur, les mots de passe auxquels il avait accès sont systématiquement renouvelés et ses droits d'accès au

gestionnaire sont révoqués immédiatement, dans les conditions définies par la procédure de révocation des accès.

---

05. Règles spécifiques aux équipements réseau

Les équipements réseau (routeurs, commutateurs, pare-feu) font l'objet de règles renforcées : mots de passe d'au moins 20 caractères, renouvellement semestriel, stockage séparé dans le gestionnaire de mots de passe avec accès restreint aux seuls ingénieurs réseau.

> **Les mécanismes d'authentification RADIUS ou TACACS+ sont privilégiés pour les équipements réseau qui les supportent, permettant une authentification centralisée et une traçabilité individuelle des accès. Les comptes locaux de secours sont désactivés ou leur mot de passe est placé sous enveloppe scellée.**