

Procédure de gestion des rôles et permissions

Référence	Version	Date	Catégorie
PROC-VMS-002	v1.0	Mars 2025	Exploitation VMS & Vidéosurveillance

Cette procédure décrit la matrice des rôles applicables aux utilisateurs du VMS, le processus de demande et de validation d'un changement de rôle, ainsi que les exigences de traçabilité associées. Elle garantit que les droits d'accès au système de vidéoprotection restent proportionnés aux responsabilités réelles de chaque utilisateur.

01. Matrice des rôles

Le rôle Opérateur constitue le niveau d'accès de base. Un opérateur dispose exclusivement de la visualisation des flux vidéo en direct sur les caméras pour lesquelles il est habilité. Il n'a pas accès aux enregistrements, ne peut pas exporter d'images et ne reçoit pas de droits de configuration du système.

Le rôle Superviseur étend les droits de l'opérateur avec la capacité de relire les enregistrements sur une plage historique définie (par défaut 30 jours) et d'effectuer des exports d'extraits vidéo sous réserve d'une autorisation préalable. Le superviseur peut également accéder aux journaux de son propre compte, mais pas à ceux des autres utilisateurs.

Le rôle Administrateur confère un accès complet au système VMS : gestion des utilisateurs et des rôles, configuration des caméras et des règles d'enregistrement, accès aux journaux système et utilisateur, gestion des sauvegardes et des exports. Ce rôle est réservé au Responsable Sécurité et aux techniciens habilités de Mileo Technology.

02. Processus de demande de changement de rôle

Toute demande de modification de rôle doit être soumise par écrit (email ou formulaire interne) par le responsable hiérarchique de l'utilisateur concerné, à destination du Responsable Sécurité. La demande doit préciser le rôle actuel, le rôle demandé et la justification opérationnelle du changement.

Le Responsable Sécurité dispose de cinq jours ouvrés pour instruire la demande. Il vérifie la cohérence de la demande avec les missions de l'utilisateur et s'assure qu'elle ne contrevient pas au principe du moindre privilège. En cas de doute, il peut solliciter l'avis du DPO ou du responsable juridique.

03. Validation hiérarchique

Les changements de rôle vers le niveau Superviseur sont validés par le Responsable Sécurité seul. Les changements de rôle vers le niveau Administrateur requièrent une double validation : celle du Responsable Sécurité et celle du Directeur des Systèmes d'Information ou de son délégué.

Aucune élévation de privilèges temporaire n'est accordée sans traçabilité formelle. En cas d'urgence opérationnelle nécessitant un accès élevé, l'élévation est accordée pour une durée strictement limitée (maximum 8 heures), documentée en temps réel et révoquée dès la fin de l'intervention.

04. Traçabilité des changements de rôle

Chaque modification de rôle est enregistrée dans le journal d'administration du VMS avec l'identifiant de l'administrateur ayant effectué le changement, la date et l'heure, l'identifiant de l'utilisateur concerné, l'ancien rôle et le nouveau rôle. Ce journal est complété par l'archivage de la demande écrite et de la décision de validation.

Un rapport semestriel récapitulatif de l'ensemble des modifications de rôles est transmis à la Direction. Ce rapport permet de détecter les dérives progressives des droits (privilege creep) et de

**s'assurer que la matrice des rôles reste cohérente
avec l'organisation réelle.**

Document Mileo Technology — PROC-VMS-002 — v1.0 — Mars 2025 47
Boulevard de Courcelles, 75008 Paris — hello@mileotech.com

© 2026 Mileo Technology. Tous droits réservés.