Guide de la cyberprotection

Comment durcir
Votre système vidéo MOBOTIX

Caméra - VMS - NAS

MOBOTIX

À propos de ce guide

Les cyber-attaques contre les logiciels et le matériel connectés à l'internet sont un problème croissant. Ces dernières années, les attaquants s'efforcent de plus en plus d'exploiter les liens les plus faibles au sein d'un périmètre de sécurité afin d'accéder aux applications critiques et aux données sensibles.

La technologie de la vidéosurveillance étant un élément essentiel de la sécurité des sites qui se trouvent souvent dans un réseau d'entreprise partagé, les dispositifs de vidéosurveillance sont de plus en plus souvent la cible de cyberattaques ciblées.

Conscient de cette nouvelle tendance, MOBOTIX a mis au point un ensemble d'**outils et de fonctions intégrés** permettant aux administrateurs de la sécurité informatique de configurer chaque appareil dans le cadre d'une approche multicouche de la cybersécurité.

Ces outils, lorsqu'ils sont utilisés avec d'autres éléments de sécurité tels que les pare-feu et la segmentation du réseau, peuvent réduire la surface d'attaque présentée par les appareils MOBOTIX dans le cadre d'une politique d'accès sécurisé pour les administrateurs et les utilisateurs.

Ce guide fournit des conseils pratiques sur la manière de configurer les appareils MOBOTIX afin d'offrir la meilleure protection possible contre les cyber-attaques, ainsi que des conseils sur les meilleures pratiques pour mettre en place une infrastructure de vidéosurveillance sécurisée.

Remarque : ce document est destiné à donner à l'administrateur responsable un aperçu complet de toutes les mesures possibles pour renforcer le système MOBOTIX. En fonction de l'application individuelle et pour éviter les reconfigurations, il peut ne pas être utile d'exécuter toutes les procédures expliquées dans ce guide.

Informations générales : MOBOTIX n'assume aucune responsabilité pour les erreurs techniques, les erreurs d'impression ou les omissions.

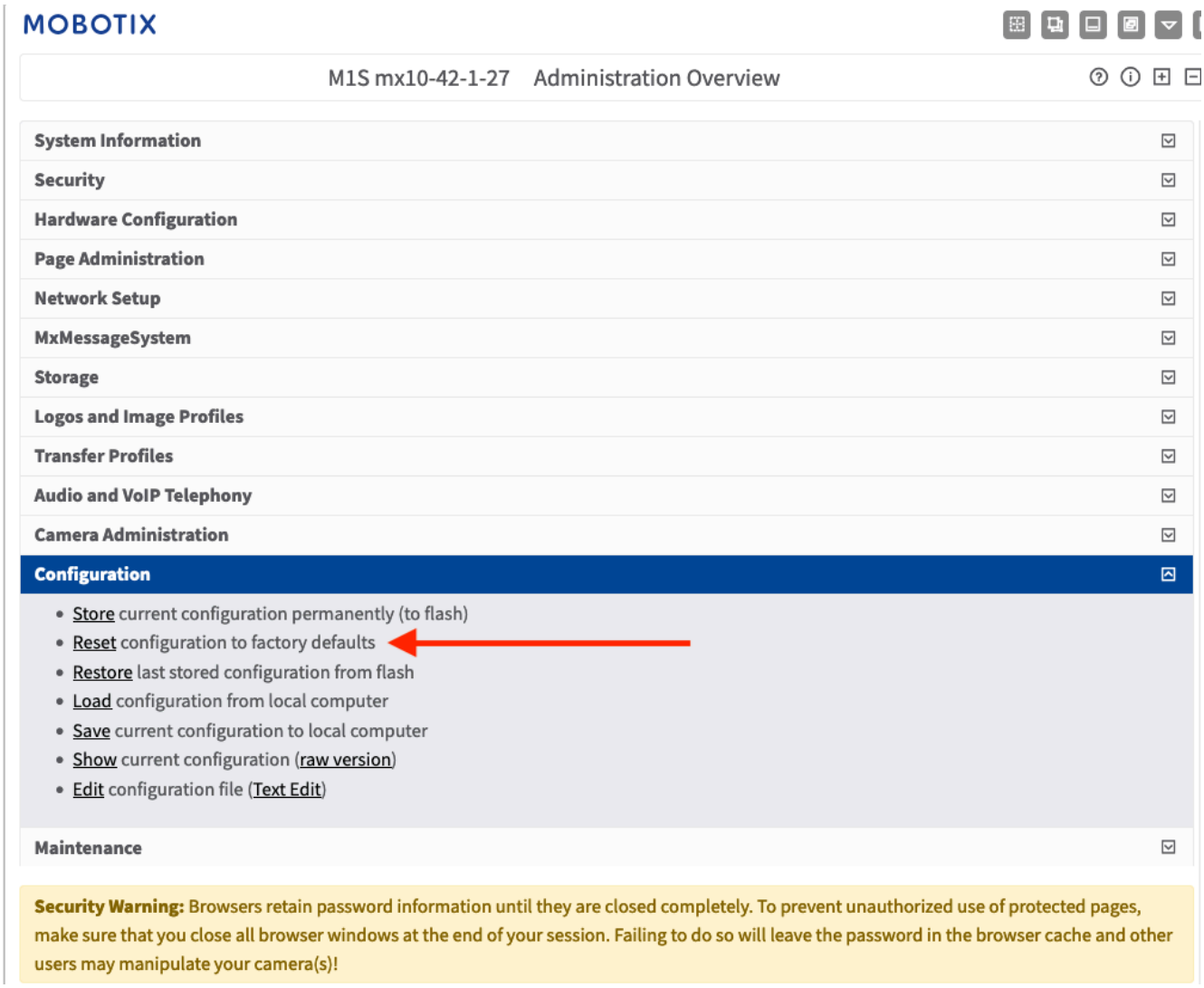
Configuration de la caméra

1. Maintenir le micrologiciel des caméras à jour

Le micrologiciel MOBOTIX peut être téléchargé gratuitement à partir de notre site Web : *www.mobotix.com > Support > Download Center* Vous ne savez pas comment procéder ? Veuillez consulter ce guide compact : *www.mobotix.com > Support > Download Center > Documentation > Brochures & Guides > Guides compacts > Mx_CG_FirmwareUpdate.pdf*

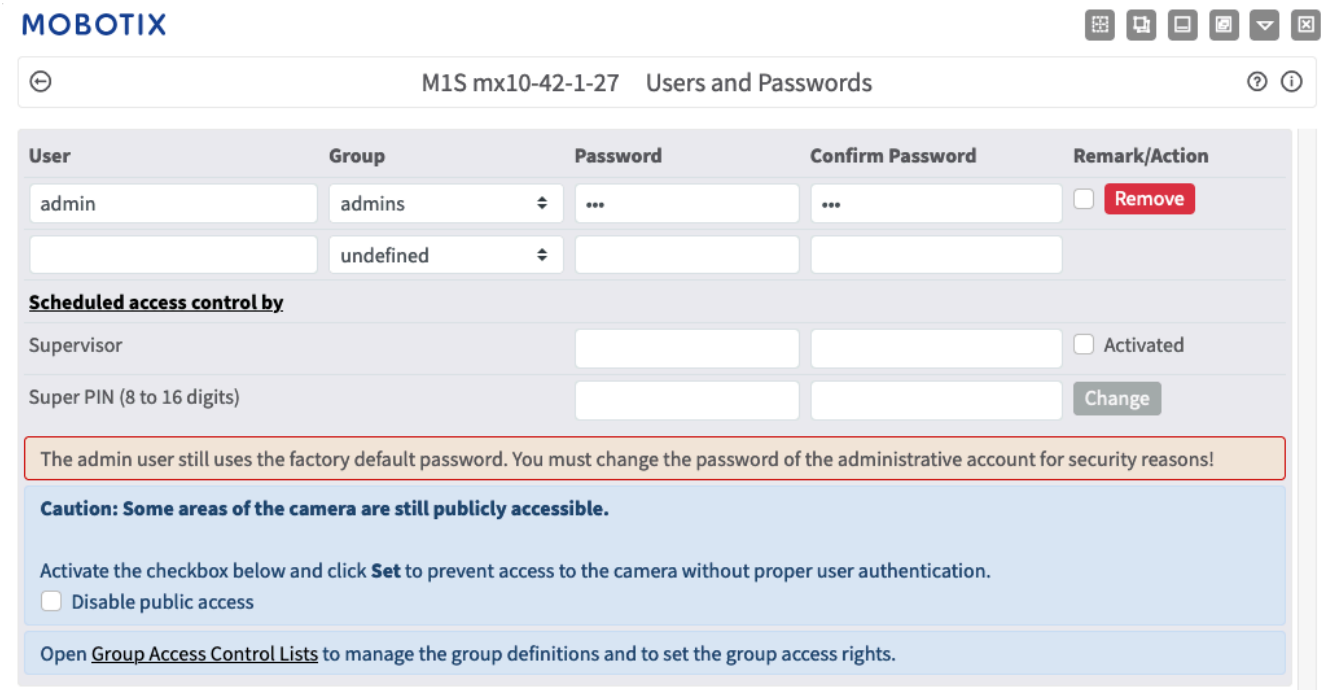
2. Réinitialiser la configuration aux valeurs d'usine

Menu Admin > Configuration > Réinitialiser la configuration aux valeurs d'usine



3. Modifier le mot de passe administrateur par défaut

Menu Admin > Sécurité > Utilisateurs et mots de passe



Il est toujours nécessaire de modifier le mot de passe par défaut "meinsm" la première fois que vous appelez l'appareil photo.

Une fois la configuration des utilisateurs, des mots de passe et des groupes terminée, vous devez toujours enregistrer les paramètres dans la mémoire permanente de l'appareil photo. Sinon, la configuration modifiée ne sera utilisée que jusqu'au prochain redémarrage de la caméra. Le bouton Fermer situé à la fin de la boîte de dialogue vous demande automatiquement d'enregistrer la configuration de la caméra dans sa mémoire permanente.

Veillez à conserver les informations relatives à votre mot de passe dans un endroit sûr. Veillez tout particulièrement à conserver le mot de passe d'au moins un utilisateur du groupe admins. Sans le mot de passe, l'accès administratif à la caméra n'est plus possible et il n'est pas possible de contourner le mot de passe. De même, il est impossible de retrouver l e mot de passe à partir d'une configuration sauvegardée en permanence.

Comment créer un mot de passe fort :

- Utiliser 8 caractères ou plus (jusqu'à 99)
- Au moins un caractère majuscule
- Au moins un caractère minuscule
- Au moins un chiffre
- Au moins un caractère spécial : ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~
- Éviter les mots et les dates les plus courants

Politique de réinitialisation des mots de passe :

Si le mot de passe administrateur n'est plus disponible, la caméra doit être réinitialisée par l'intermédiaire de

4. Créer des groupes d'utilisateurs différents avec des droits d'utilisation différents

Menu Admin > Sécurité > Utilisateurs et mots de passe

En général, tous les utilisateurs n'ont pas besoin des mêmes droits. Vous pouvez créer jusqu'à 25 groupes d'utilisateurs différents à partir de la page Menu Admin > Liste de contrôle d'accès des groupes.

5. Créer des utilisateurs différents et les affecter aux groupes appropriés

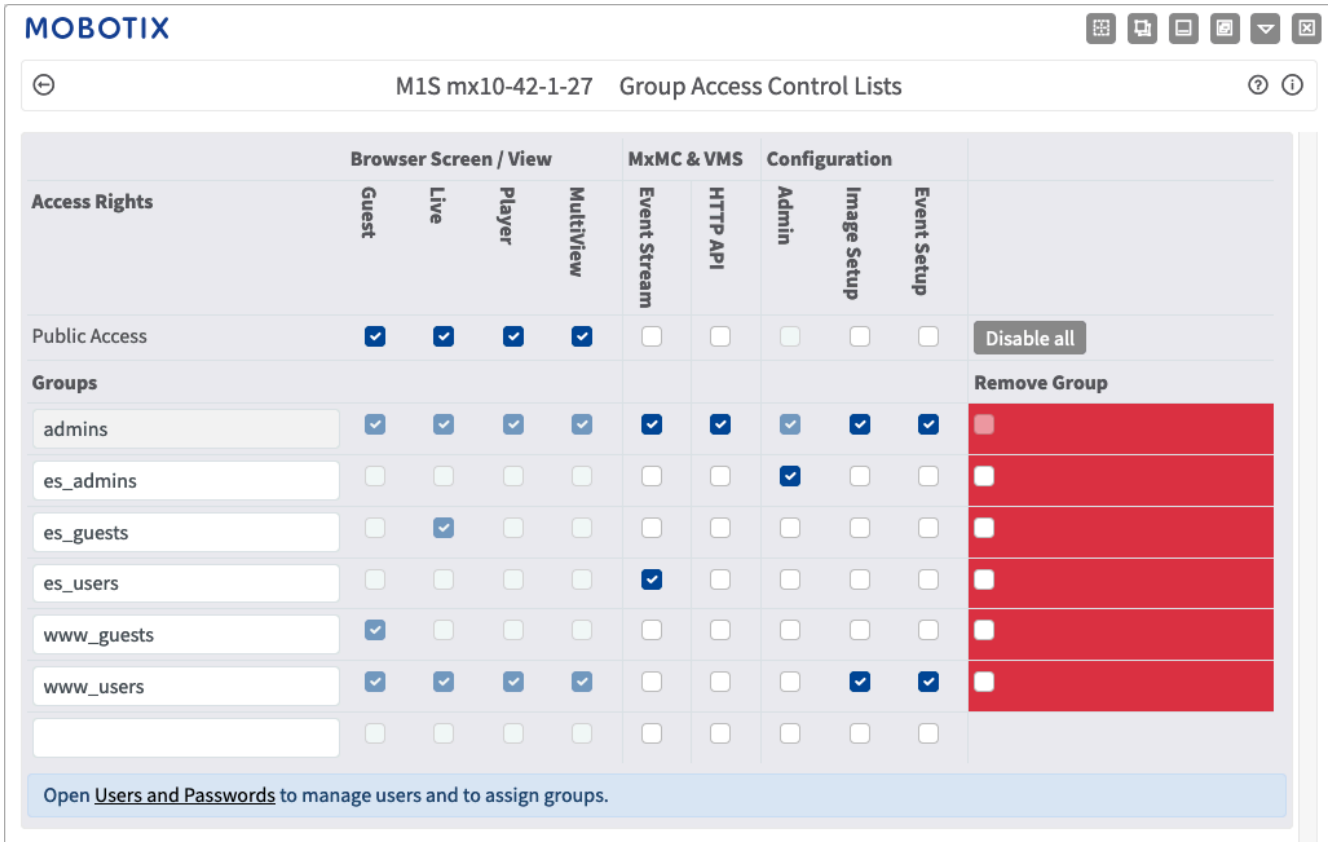
Menu Admin > Sécurité > Utilisateurs et mots de passe

Il est toujours conseillé de créer un utilisateur pour chaque personne autorisée à accéder à la caméra. Il est possible de créer jusqu'à 100 utilisateurs. Les actions effectuées par les utilisateurs autorisés sont enregistrées dans le fichier journal du serveur Web, ce qui permet de déterminer "qui a fait quoi" en cas de litige.

Reportez-vous à la description ci-dessus pour créer des mots de passe forts.

6. Désactiver l'accès public

Menu Admin > Sécurité > Listes de contrôle d'accès de groupe



L'accès public permet, s'il est activé, d'accéder à des ressources spécifiques de la caméra sans authentification. Il est fortement recommandé de désactiver l'accès public afin d'éviter que des utilisateurs non autorisés puissent afficher le flux en direct de la caméra, les enregistrements ou même contrôler la caméra (par exemple, modifier la configuration ou exécuter des actions). D'autres options de paramétrage sont disponibles sous "Plus".

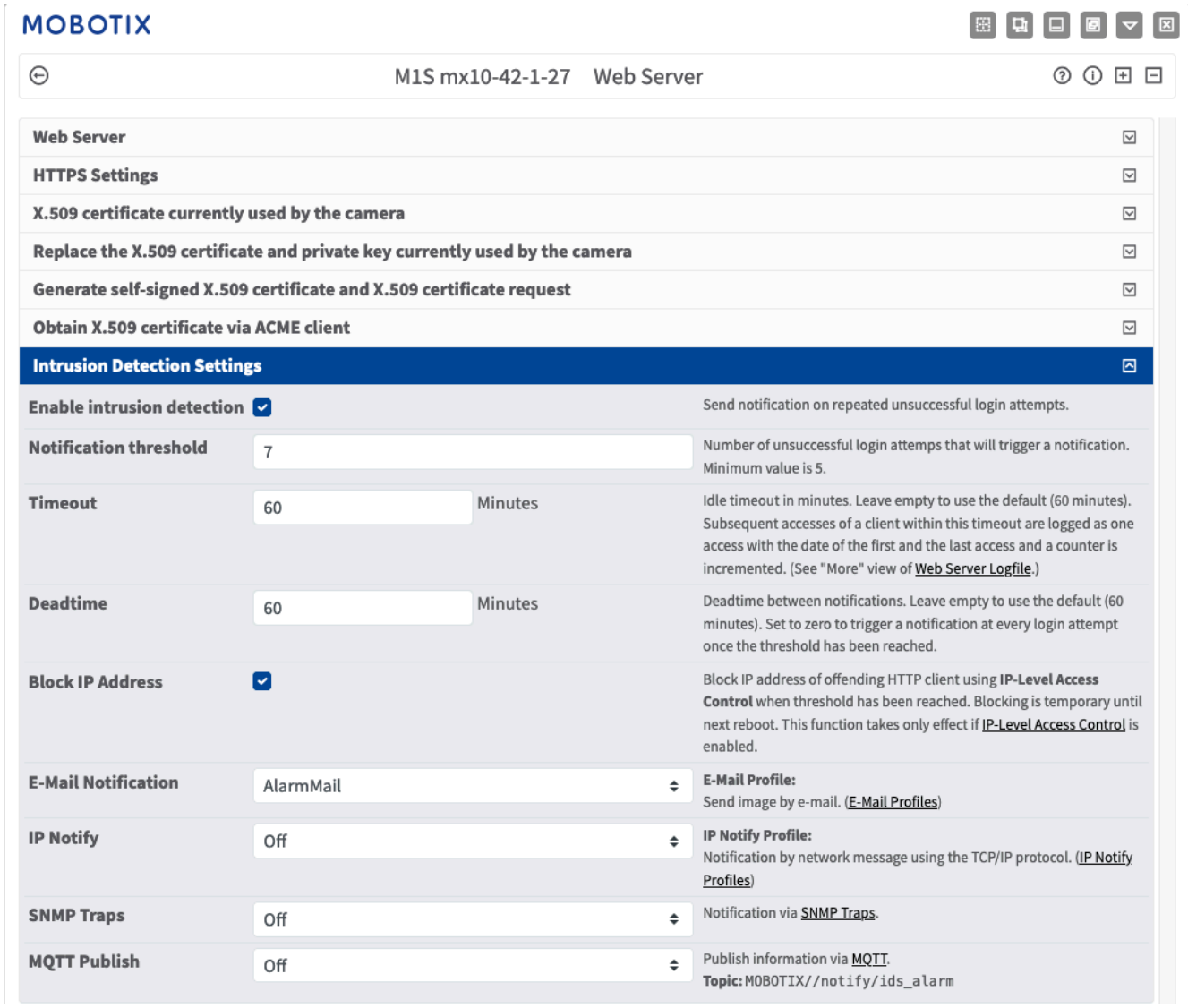
7. Activer la liste de contrôle d'accès IP

Menu Admin > Sécurité > Contrôle d'accès au niveau IP

La boîte de dialogue Contrôle d'accès permet de gérer les adresses IP, les sous-réseaux et les noms de domaine dont l'accès à la caméra est autorisé ou interdit. Cette possibilité de contrôler l'accès à la caméra utilise le niveau du protocole IP, est indépendante de l'authentification de l'utilisateur basée sur un mot de passe au niveau du protocole HTTP et remplace l'authentification basée sur un mot de passe. Si un ordinateur n'a pas d'accès à la caméra au niveau IP, il n'est pas possible d'accéder à la caméra à partir de cet ordinateur. Si un ordinateur dispose d'un accès IP à la caméra, l'étape suivante est l'authentification de l'utilisateur par mot de passe, comme indiqué dans la boîte de dialogue Utilisateurs et mots de passe.

8. Activer la détection d'intrusion avec notification et blocage de l'adresse IP d'origine

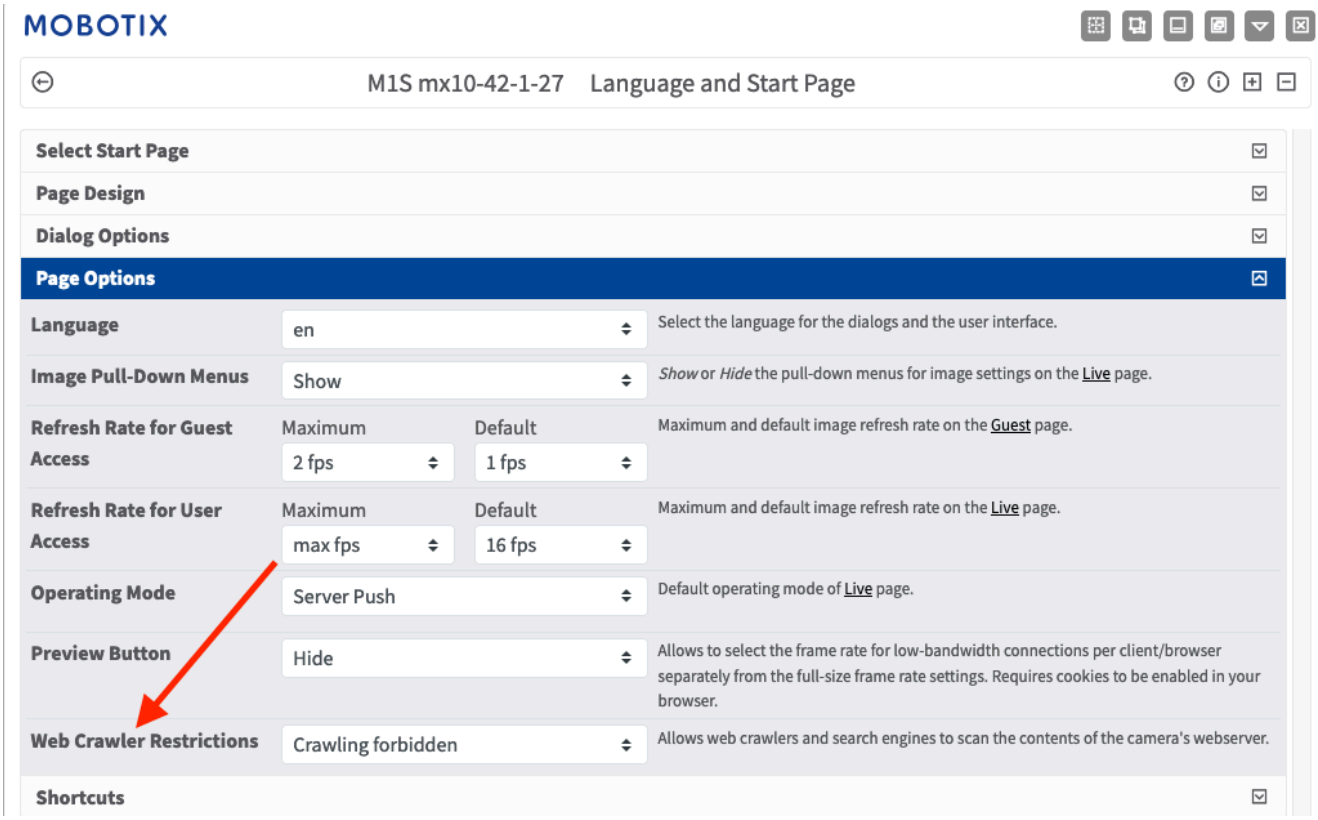
Menu Admin > Configuration du réseau > Serveur Web (pour les experts) > Paramètres de détection d'intrusion



Cette fonction constitue une défense automatique contre les attaques. Si un intrus tente d'accéder à la caméra en utilisant des méthodes de "force brute" pour deviner les noms d'utilisateur et les mots de passe, la caméra peut envoyer une alerte et verrouiller automatiquement l'adresse IP d'origine après un certain nombre de tentatives infructueuses.

9. Vérifier que l'exploration du Web est interdite

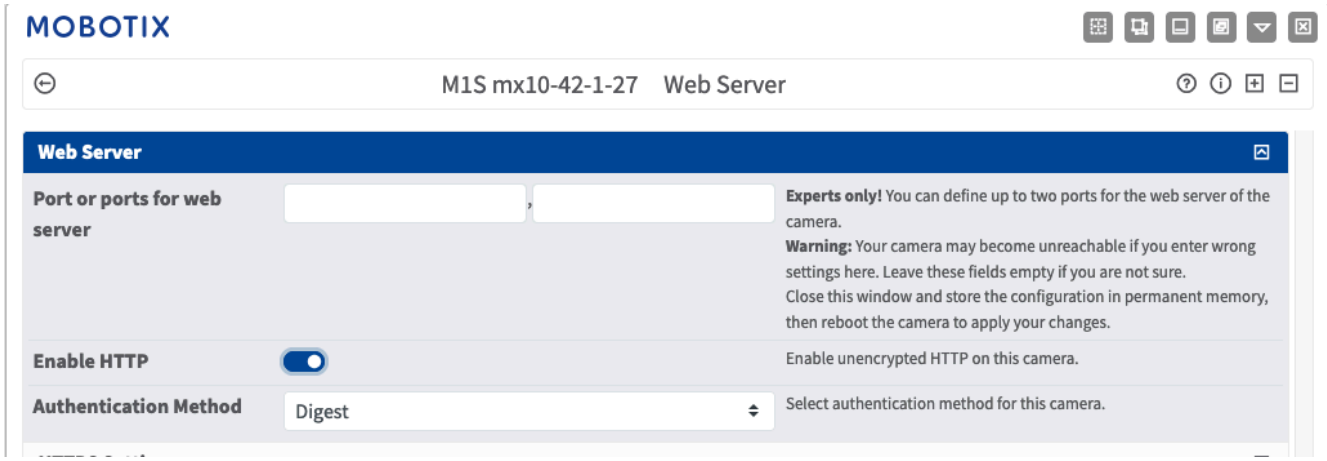
Menu Admin > Administration des pages > Langue et page de démarrage > Options de la page



Ce paramètre permet d'empêcher les moteurs de recherche, les autres robots automatiques et les robots d'indexation d'analyser le contenu du serveur Web de l'appareil photo. En règle générale, il n'est pas souhaitable qu'un moteur de recherche indexe toutes les images et les pages d'une caméra. N'autorisez l'exploration que si vous êtes conscient des risques de sécurité supplémentaires et du trafic réseau supplémentaire généré par les robots.

10. Activer l'authentification Digest

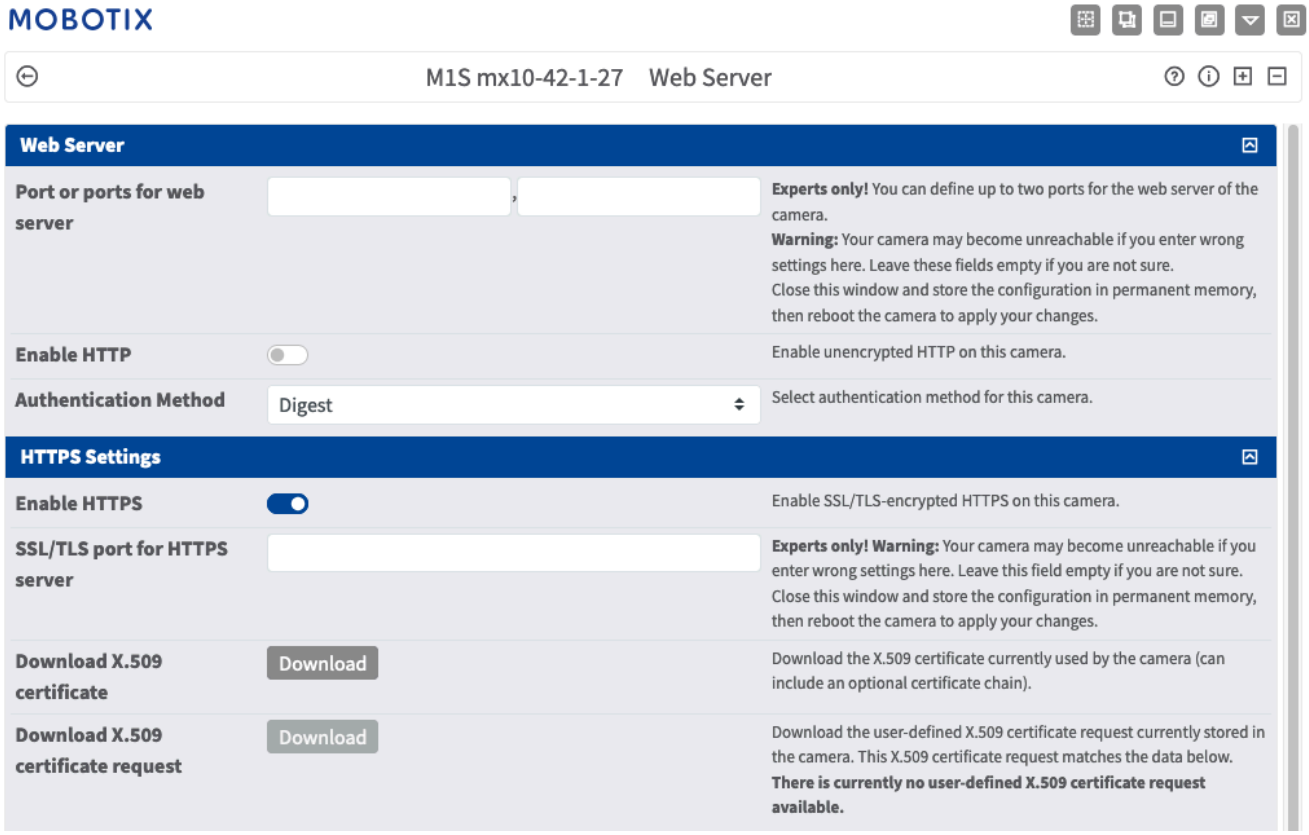
Menu Admin > Configuration du réseau > Serveur Web (pour les experts) > Serveur Web



L'authentification digest est l'une des méthodes convenues qu'un serveur Web (c'est-à-dire la caméra MOBOTIX) peut utiliser pour négocier des informations d'identification, telles que le nom d'utilisateur ou le mot de passe, avec un client (c'est-à-dire un navigateur Web). Avec l'authentification Digest, le mot de passe n'est jamais envoyé en clair et le nom d'utilisateur peut être haché.

11. Modifier les ports par défaut du serveur Web (pour l'accès à distance)

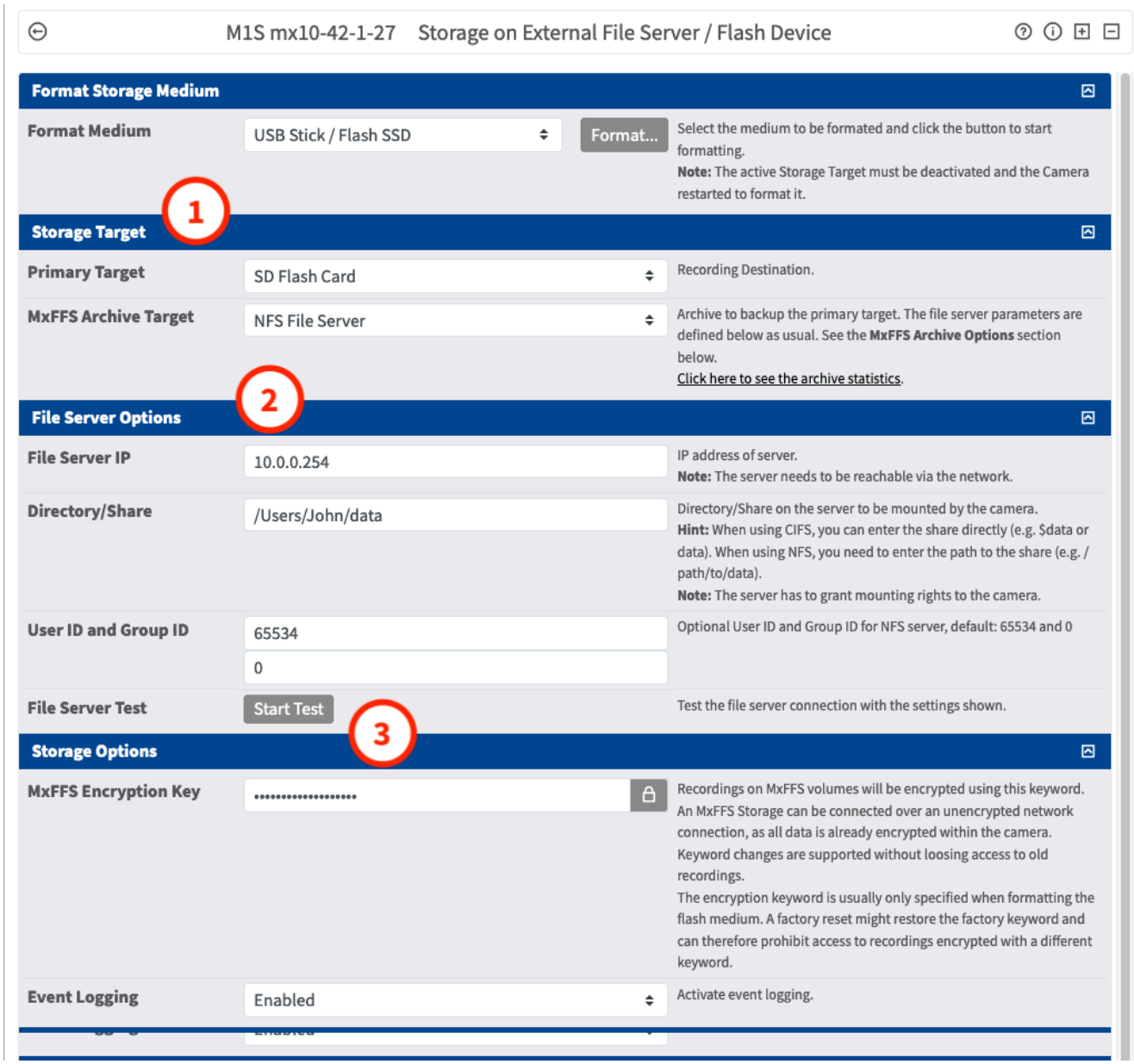
Menu Admin > Configuration du réseau > Serveur Web (pour les experts)



Les ports standard (80 TCP pour HTTP et 443 TCP pour HTTPS) sont plus exposés aux attaques. Le remplacement des ports par défaut par des ports personnalisés permet d'accroître la sécurité de la caméra. Dès que le protocole HTTP est désactivé, l'accès à la caméra dans le navigateur doit se faire via HTTPS.

12. Définir une clé de cryptage pour les enregistrements

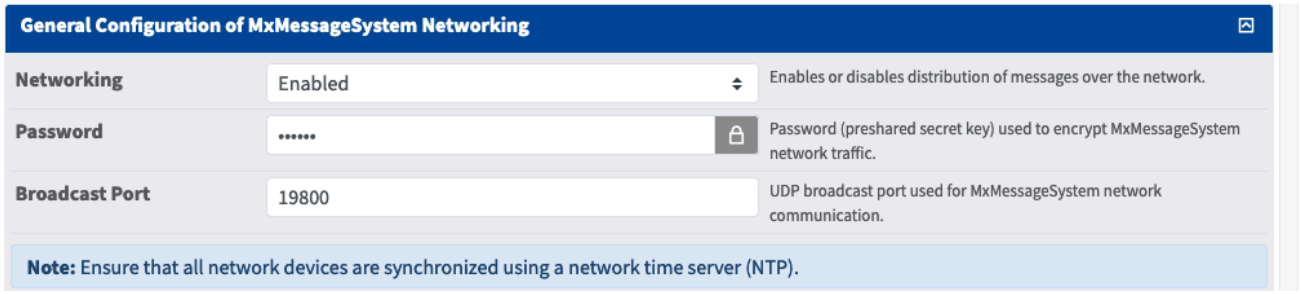
Menu Admin > Stockage > Stockage sur serveur de fichiers externe / périphérique Flash



Une clé de cryptage peut être définie pour crypter les enregistrements stockés sur le stockage interne (carte microSD / clé USB) ainsi que pour les enregistrements archivés sur le serveur de fichiers externe (SMB / NFS). Cliquez sur "Plus" ci-dessous pour voir toutes les options de réglage.

13. Modifier le mot de passe par défaut pour MxMessage (nécessaire uniquement en cas d'utilisation)

Menu Admin > MxMessageSystem > Distribution des messages en réseau



MxMessageSystem permet le transfert de messages entre les caméras sur le réseau. Un mot de passe (clé symétrique) d'au moins 6 caractères doit être défini pour crypter les messages transférés.

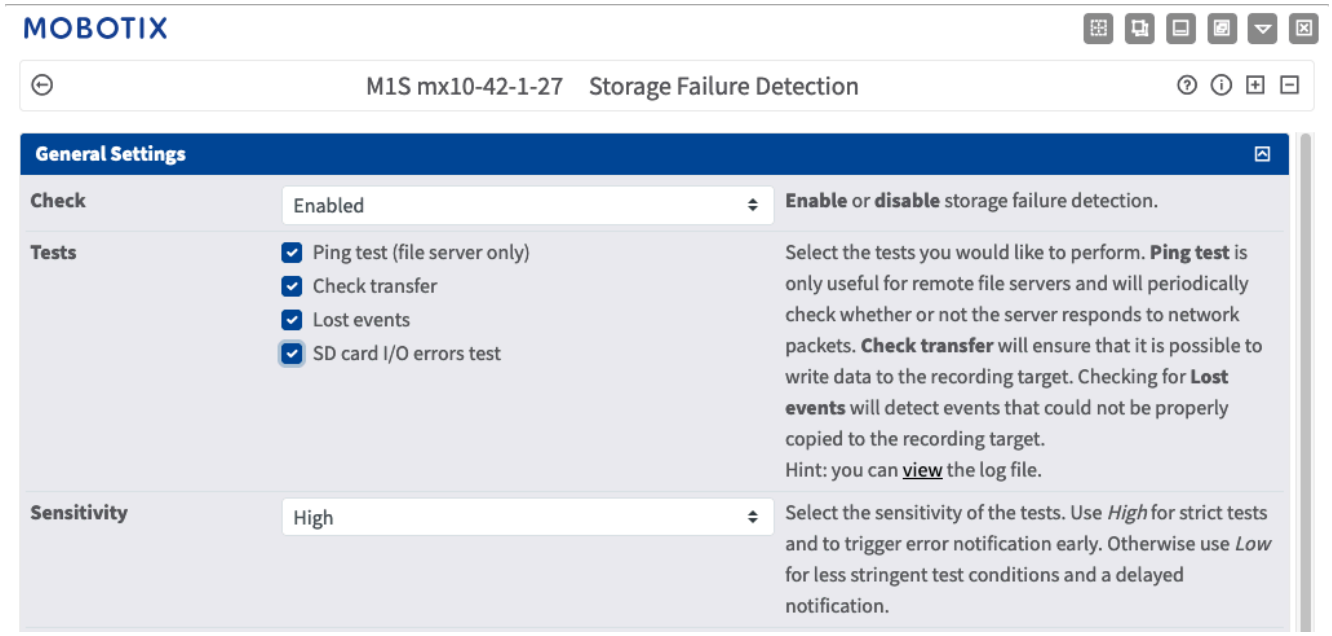
14. Activer la notification d'erreur

Menu Admin > Informations sur le système > Notification d'erreur

La boîte de dialogue Notification d'erreur propose plusieurs options pour recevoir des notifications (e-mail, notifications IP, appels VoIP, etc.) en cas de redémarrage ou d'erreurs détectées dans les différents systèmes de la caméra. Cet outil permet aux administrateurs système de s'assurer que toutes les caméras MOBOTIX fonctionnent correctement.

15. Activer la détection des défaillances du stockage

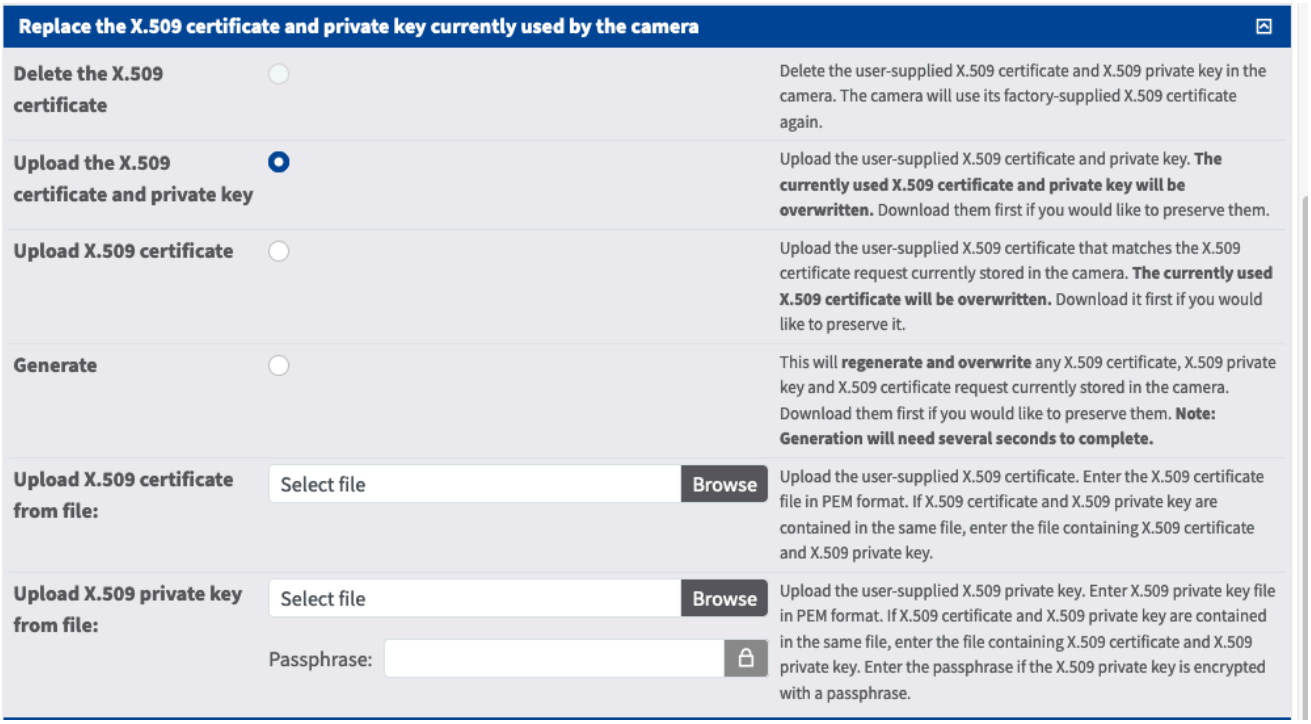
Menu Admin > Stockage > Détection des défaillances du stockage



La boîte de dialogue Détection des pannes de stockage permet de configurer des tests qui surveillent en permanence la cible de stockage externe (serveur de fichiers ou périphérique Flash) que la caméra utilise comme buffer d'anneau externe. La caméra surveille activement la cible de stockage et signale les problèmes d'enregistrement vidéo à l'aide des méthodes de notification spécifiées dans cette boîte de dialogue.

16. Générer et charger des certificats X.509 personnalisés

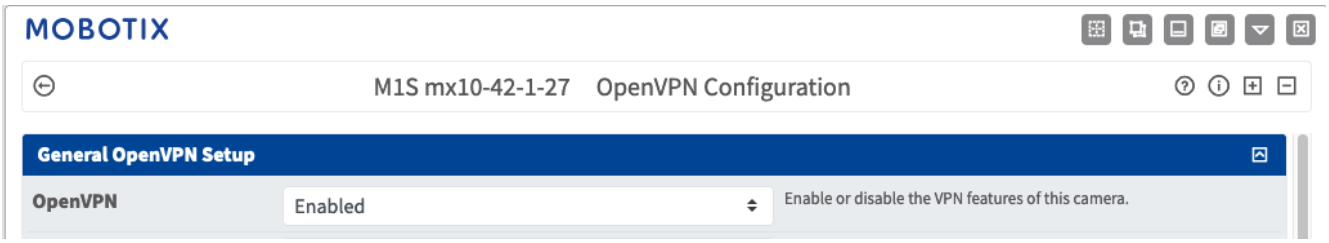
Menu Admin > Configuration du réseau > Serveur Web (pour les experts)



Le chargement d'un certificat personnalisé signé par une autorité de certification de confiance garantit la confidentialité et l'authenticité de toutes les connexions établies via HTTPS (SSL/TLS).

17. Configurer le client OpenVPN pour les connexions à distance

Menu Admin > Configuration du réseau > Paramètres du client OpenVPN



Pour optimiser la sécurité en cas de connexions à distance, il est possible d'utiliser le client OpenVPN intégré pour établir un tunnel VPN (Virtual Private Network) entre la caméra et l'hôte distant.

La création d'une connexion OpenVPN nécessite un serveur correspondant, qui fournit un accès sécurisé à la caméra. Pour ce faire, vous pouvez exploiter votre propre serveur OpenVPN ou utiliser le service d'un fournisseur OpenVPN.
Pour plus d'informations sur OpenVPN, visitez le site web de *la communauté OpenVPN.*

18. Évitez d'exposer l'appareil photo à l'internet, sauf en cas de nécessité absolue.

L'accès à distance à la caméra doit être accordé en toute connaissance de cause afin de réduire le risque d'attaques. Si un accès à distance est nécessaire, veillez à respecter les règles susmentionnées afin de limiter la possibilité de se connecter aux seuls utilisateurs prévus.

19. Utiliser des VLAN pour séparer le réseau de télévision en circuit fermé (niveau de sécurité de l'entreprise).

Dans les environnements d'entreprise, il est conseillé de séparer le réseau CCTV (caméras IP, NVR et stations de travail VMS) du reste des hôtes afin d'empêcher les accès non autorisés et d'éviter la congestion traffique.

20. Activer IEEE 802.1X (niveau de sécurité de l'entreprise)

Menu Admin > Configuration du réseau > Interface Ethernet (pour les experts) > IEEE 802.1X

Cette norme internationale est utilisée pour le contrôle d'accès au réseau (NAC) basé sur les ports. Cette procédure exige que tous les périphériques réseau (y compris la caméra MOBOTIX) s'authentifient auprès du commutateur pour obtenir une connexion réseau. Les périphériques réseau sans authentification appropriée seront rejetés.

Demandez à votre administrateur réseau si la norme IEEE 802.1X est prise en charge ou requise. Assurez-vous que le commutateur auquel la caméra est connectée (authentificateur) a été configuré en conséquence. En général, le commutateur (authentificateur) a également besoin d'un serveur d'authentification, tel qu'un serveur RADIUS. La procédure d'authentification est contrôlée par le serveur d'authentification. Veillez à ce que la caméra et le serveur d'authentification utilisent toujours la même procédure.

21. Vérifier régulièrement le fichier journal du serveur Web

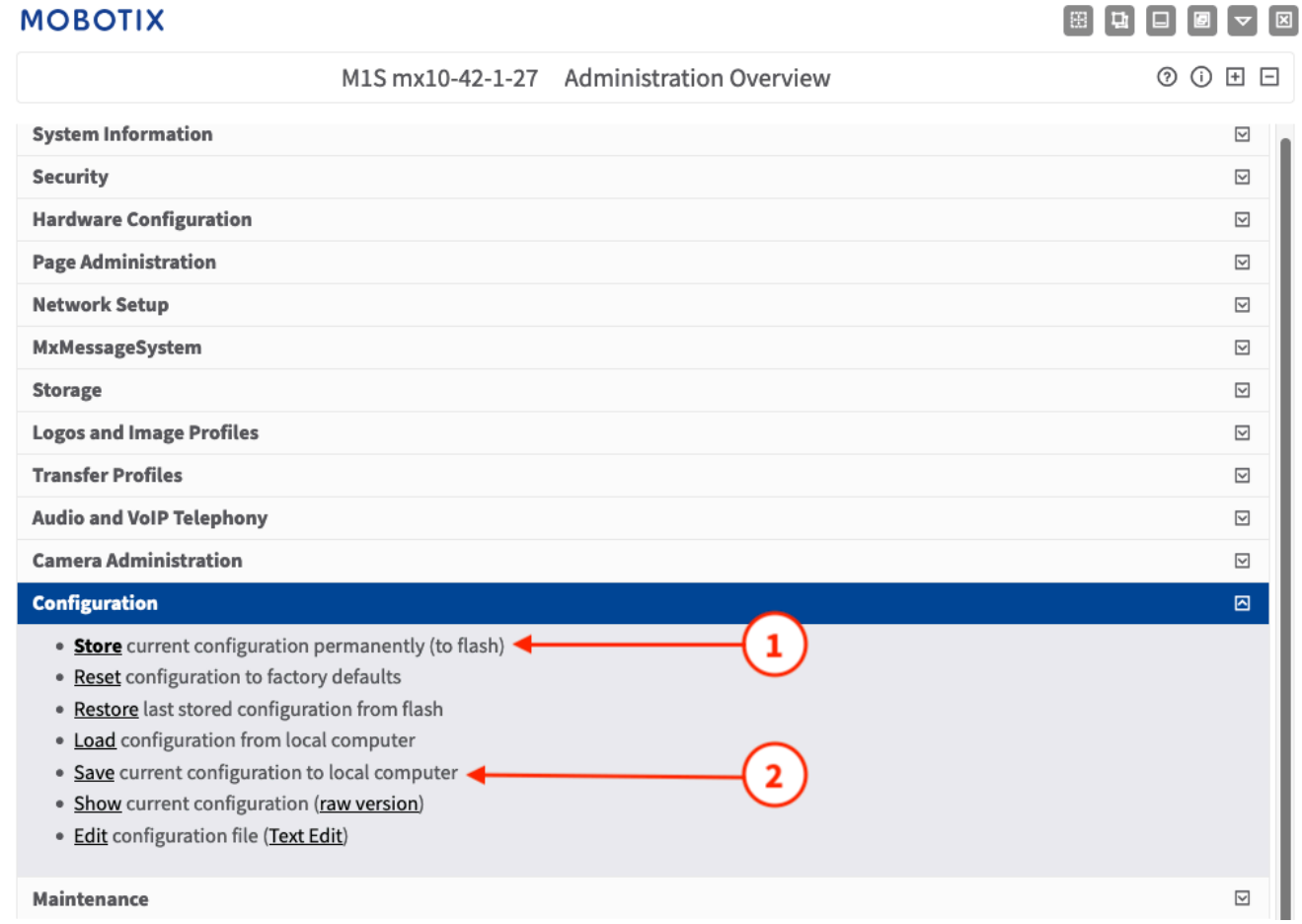
Menu Admin > Sécurité > Fichier journal du serveur Web

Host Name	IP	Status	User	Date & Time ↓↑	
10.5.8.6	10.5.8.6	Successful	-	today	15:40:59
			admin		15:40:58
			-		15:39:56
			admin		15:33:52
			-		15:30:25
			admin		15:29:10
10.2.3.4	10.2.3.4	Successful	-	2024-10-11	14:31:11
			admin		14:31:08
			-		14:30:24
			admin		14:20:56
10.0.0.2	10.0.0.2	Successful	-		12:32:14
			admin		12:31:11
			-		12:30:56
			admin		09:09:30
			-		09:09:21
10.2.3.4	10.2.3.4	Successful	admin		08:42:22
			-		08:42:14
10.32.150.131	10.32.150.131	Successful	admin		08:41:29
			-		08:39:27
			admin		08:39:22
			-	2024-10-10	17:39:49
			admin		17:39:38

Le fichier journal du serveur Web présente toutes les tentatives d'accès et les informations relatives à la date et à l'heure, ainsi que les messages d'état correspondants du serveur Web et le nom d'hôte de l'ordinateur accédant. Les tentatives d'accès non autorisé pourraient être la sonnette d'alarme pour les administrateurs de système qui souhaiteraient revoir la force de leur réseau.

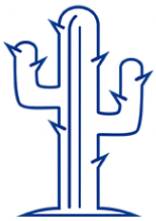
22. Stocker les fichiers de configuration de sauvegarde en lieu sûr

Menu Admin > Configuration > Mémoriser et enregistrer la configuration actuelle sur l'ordinateur local



Bien que les informations d'identification de la caméra (mots de passe utilisateur) soient hachées dans le fichier de configuration de la caméra, tout fichier de sauvegarde de la configuration doit être conservé en lieu sûr ; en outre, il est conseillé de crypter le fichier avec une phrase de passe pour plus de sécurité.

Félicitations - votre caméra MOBOTIX est maintenant cyber-sécurisée !



Configuration VMS (système de gestion vidéo)

1. Créer des comptes d'utilisateurs sur l'ordinateur utilisé

2. Créer des comptes d'utilisateurs sur la MxMC

3. Limiter les droits des utilisateurs du VMS

4. Évitez d'utiliser le compte administrateur pour accéder aux caméras via MxMC.

5. Activer la fonction "Auto log-off"

Félicitations - votre système de gestion vidéo est maintenant cyber-sécurisé !

Configuration NAS (stockage en réseau)

1. Placez l'appareil utilisé pour stocker les images en lieu sûr.

2. Définir un mot de passe fort pour le compte administratif

3. Définir un compte utilisateur standard (droits limités) pour les appareils MOBOTIX

4. Chiffrer les volumes

5. Utiliser un niveau RAID qui assure la redondance des données

Félicitations - votre système de stockage en réseau est maintenant cyber-sécurisé !