Guide de cyberprotection

Comment protéger
votre système vidéo MOBOTIX

Caméra • VMS • NAS

CYBER SECURITY
INITIATIVE 2018

MOBOTIX

A propos de ce guide

Les cyberattaques contre le matériel et les logiciels connectés à Internet représentent un problème croissant. Depuis quelques années, les pirates informatiques cherchent de plus en plus à exploiter les maillons les plus faibles d'un périmètre de sécurité afin d'accéder aux applications critiques et aux données sensibles.

Comme la technologie de vidéosurveillance joue un rôle central dans les dispositifs de sécurité des sites souvent intégrés à un réseau d'entreprise partagé, les appareils de vidéosurveillance sont devenus la cible privilégiée de cyberattaques qui ne doivent rien au hasard.

Prenant conscience de ce nouveau phénomène, MOBOTIX a développé une série **d'outils et de fonctionnalités intégrés** qui permettent aux administrateurs de sécurité informatique de configurer chaque outil selon une approche multi-niveaux de la cybersécurité.

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

Ce guide prodigue des conseils pratiques sur la manière de configurer les appareils MOBOTIX pour obtenir une protection optimale contre les cyberattaques, et dévoile des bonnes pratiques permettant de concevoir une infrastructure de vidéosurveillance sûre.

Remarque : ce document vise à donner à l'administrateur responsable un aperçu complet de toutes les mesures existantes permettant de protéger un système MOBOTIX. Selon l'application choisie et afin d'éviter les reconfigurations, il n'est pas forcément utile d'effectuer toutes les procédures mentionnées dans ce guide.

Informations générales : MOBOTIX décline tout responsabilité quant aux omissions et aux erreurs techniques et d'impression.

Configuration de la caméra

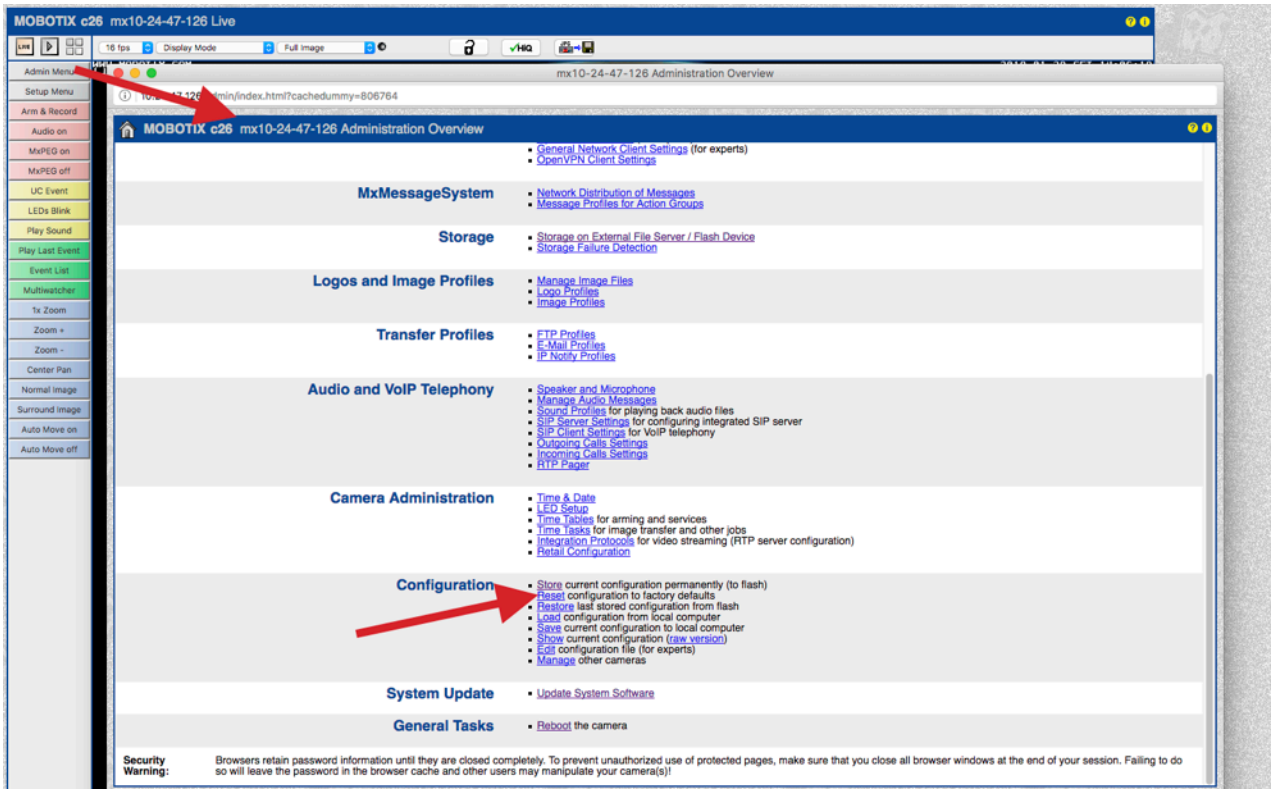
1. Mettez à jour le micrologiciel des caméras

Le micrologiciel MOBOTIX peut être téléchargé gratuitement sur notre site Internet : *www.mobotix.com > Support > Download Center*

Vous ne savez pas comment procéder ? Veuillez vous référer à ce mini guide : *www.mobotix.com > Support > Download Center > Documentation > Brochures & Guides > Guides compacts > Mx_CG_FirmwareUpdate.pdf*

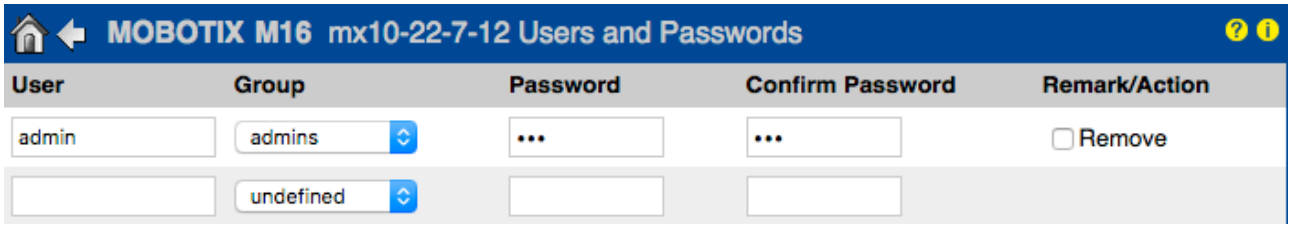
2. Revenez à la configuration par défaut.

Admin Menu > Configuration > Sauvegarder la configuration actuelle dans la mémoire permanente



3. Changez le mot de passe admin par défaut

Admin Menu > Sécurité > Utilisateurs et mots de passe



Il est fortement recommandé de changer le nom d'utilisateur « admin » et le mot de passe par défaut « meinsm ». Une fois la configuration des utilisateurs, des mots de passe et des groupes effectuée, vous devez toujours enregistrer les paramètres dans la mémoire permanente de la caméra. Faute de quoi, la configuration modifiée ne sera prise en compte que jusqu'au prochain redémarrage de la caméra. Utilisez le bouton Close situé en bas de la boîte de dialogue lorsque celle-ci vous demandera automatiquement d'enregistrer la configuration de la caméra dans sa mémoire permanente.

Veillez à enregistrer votre mot de passe dans un endroit sûr. Assurez-vous de connaître le mot de passe d'au moins un utilisateur du groupe des administrateurs. Sans mot de passe, l'administrateur ne peut plus accéder à la caméra. Il n'est pas possible de se soustraire à la saisie du mot de passe. De la même façon, il est impossible de récupérer le mot de passe depuis une configuration permanente.

Pour créer un mot de passe sécurisé, il faut utiliser :

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

Politique de réinitialisation des mots de passe : si vous avez oublié le mot de passe de l'administrateur, vous devez renvoyer la caméra à MOBOTIX pour qu'elle procède à une réinitialisation des paramètres d'usine !

4. Créez plusieurs groupes d'utilisateurs avec différents droits d'utilisateur

Admin Menu > Sécurité > Utilisateurs et mots de passe

En général, les utilisateurs n'ont pas tous besoin des mêmes droits. Vous pouvez créer jusqu'à 25 groupes d'utilisateurs différents depuis la page Admin Menu > Group Access Control List

5. Créez différents utilisateurs et affectez-les aux bons groupes

Admin Menu > Sécurité > Utilisateurs et mots de passe

Il est toujours conseillé de créer un profil utilisateur pour chaque personne autorisée à accéder à la caméra. Vous pouvez créer jusqu'à 100 utilisateurs. Les opérations réalisées par les utilisateurs autorisés sont consignées dans le fichier journal du serveur Web, ce qui permet de savoir « qui a fait quoi » en cas de litige.

Référez-vous à la description ci-dessus pour créer des mots de passe sécurisés.

6. Désactivez l’accès public

Admin Menu > Sécurité > Contrôle d'accès aux groupes (ACL)

MOBOTIX M16 mx10-22-7-12 Group Access Control Lists

Access Rights	Browser Screen / View: Guest	Live	Player	MultiView	PDA	MxMC & VMS: Event Stream	HTTP API	Configuration: Admin	Image Setup	Event Setup	
Public Access	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	Disable all
Groups											**Remove Group**
admins	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☐
es_admins	☐	☐	☐	☐	☐	☐	☐	☑	☐	☐	☐
es_guests	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐
es_users	☐	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐
www_guests	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
www_users	☑	☑	☑	☑	☑	☐	☐	☐	☑	☑	☐
	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	

Open Users and Passwords to manage users and to assign groups.

S’il est activé, l’accès public permet d’accéder à des ressources spécifiques de la caméra sans avoir besoin de s’authentifier. Nous vous conseillons fortement de désactiver l’accès public afin d’éviter que des utilisateurs non autorisés puissent consulter le flux en direct de la caméra et les enregistrements ou même réussissent à prendre le contrôle de la caméra (et modifient la configuration de la caméra ou effectuent des actions, p. ex.).

7. Activez la liste de contrôle d’accès IP

Admin Menu > Sécurité > Restriction d'accès par IP

MOBOTIX c26 mx10-24-47-126 IP-Level Access Control

Access Control Configuration

WARNING: A faulty access configuration may render the camera inaccessible!

Access Control: Enabled — Enable or disable Access Control.

Access Rules for Allow

Mode	IP Address/Subnet/Domain	Examples
Allow	192.168.1.163	192.168.1.163, 192.168.1.0/255.255.255.0, ftp.mobotix.com
Allow		192.168.1.163, 192.168.1.0/255.255.255.0, ftp.mobotix.com

Access Rules for Deny

Mode	IP Address/Subnet/Domain	Examples
Deny	192.168.1.163	192.168.1.163, 192.168.1.0/255.255.255.0, ftp.mobotix.com
Deny		192.168.1.163, 192.168.1.0/255.255.255.0, ftp.mobotix.com

If no match is found:

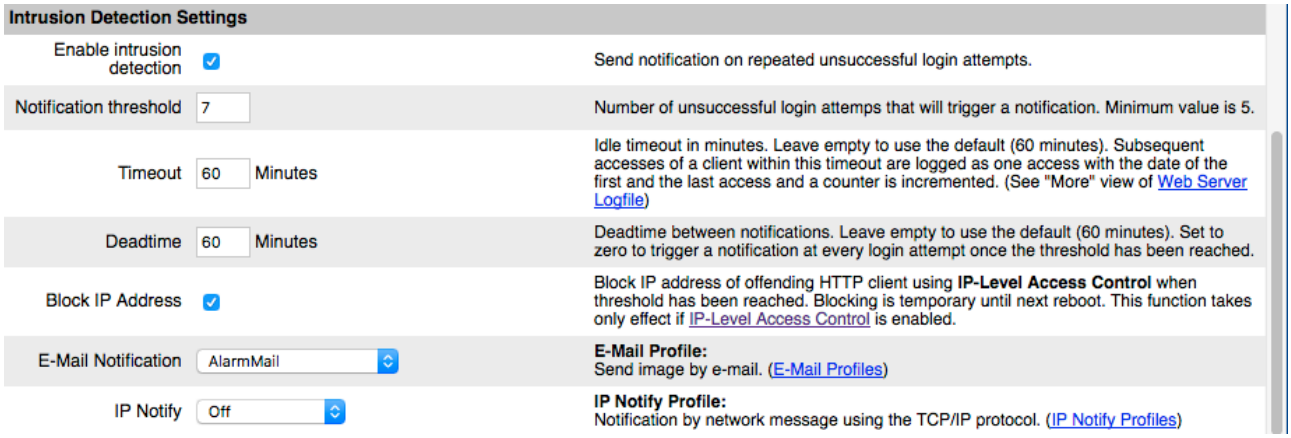
Allow — Access from all IP addresses/subnets/domains not listed above.

Set | Factory | Restore | Close

La boîte de dialogue Access Control vous permet de gérer les adresses IP, les sous-réseaux et les noms de domaine qui sont autorisés ou non à accéder à la caméra. Cette fonctionnalité de contrôle de l'accès à la caméra fonctionne au niveau du protocole IP, elle ne dépend pas de l'authentification utilisateur basée sur un mot de passe au niveau du protocole HTTP et supplante l'authentification basée sur un mot de passe. Si un ordinateur n'a pas accès à la caméra au niveau IP, il est impossible d'accéder à la caméra avec cet ordinateur. Si un ordinateur possède un accès à la caméra au niveau IP, l'authentification utilisateur basée sur le mot de passe est l'étape suivante, comme indiqué dans la boîte de dialogue Users and Passwords.

8. Activez la détection d'intrusion avec notification et blocage des adresses IP en cause

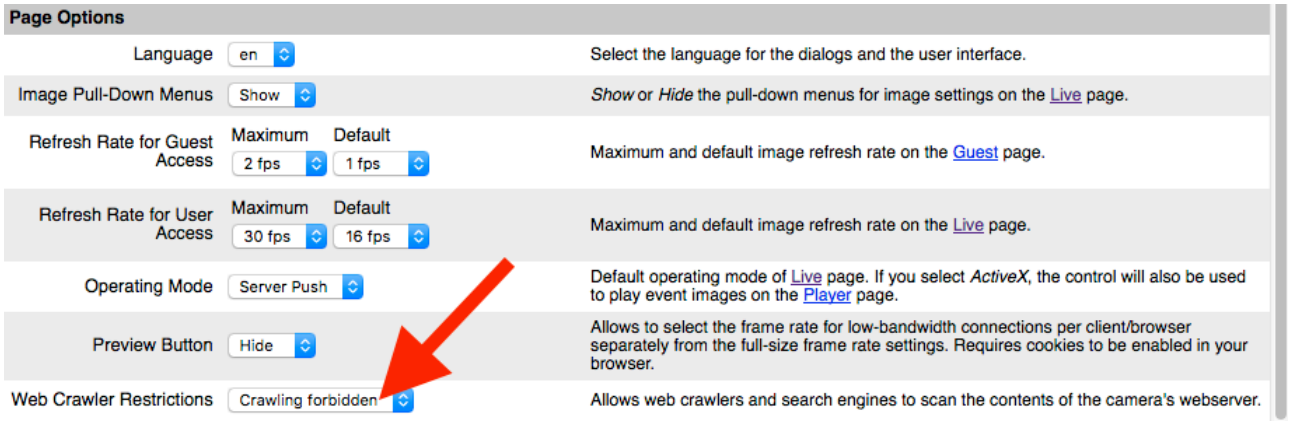
Admin Menu > Configuration du réseau > Serveur Web (pour les experts) > Paramètres de la détection d'intrus



Cette fonction vous permet de vous défendre automatiquement contre les attaques. Si un intrus essaie d'accéder à la caméra en employant la « méthode forte » pour deviner les noms et les mots de passes des utilisateurs, la caméra est capable d'envoyer une alerte et de verrouiller automatiquement l'adresse IP en cause après un certain nombre de tentatives ratées.

9. Assurez-vous que le Web crawling est interdit

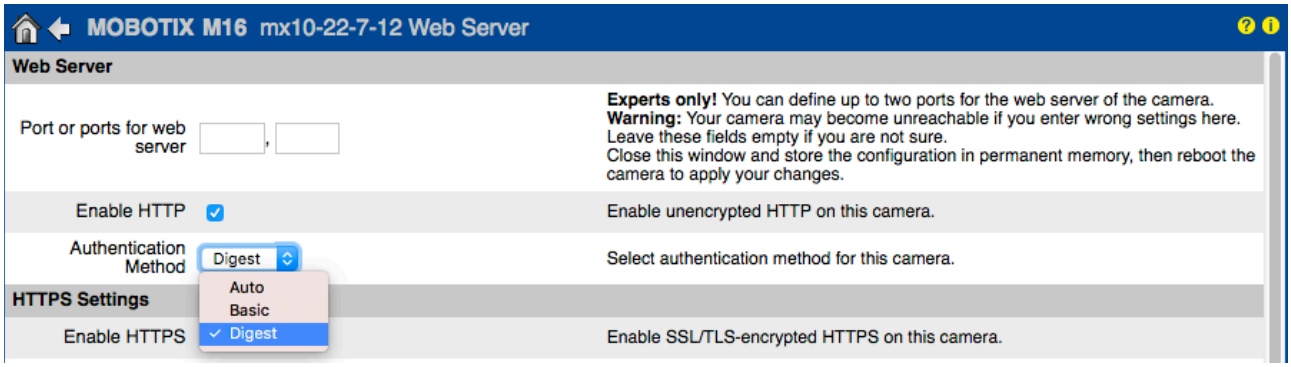
Admin Menu > Configuration des pages > Langue et page d'accueil > Options de page



Ce paramètre vous permet d'empêcher les moteurs de recherche Web, les Web crawlers et autres robots automatiques de scanner les contenus du serveur Web de la caméra. En règle générale, vous ne voudriez pas qu'un moteur de recherche répertorie toutes les images et pages trouvées sur une caméra. Nous vous conseillons donc de n'autoriser le crawling que si vous connaissez les risques de sécurité et le trafic réseau supplémentaires engendrés par les crawlers.

10. Activez l'authentification Digest

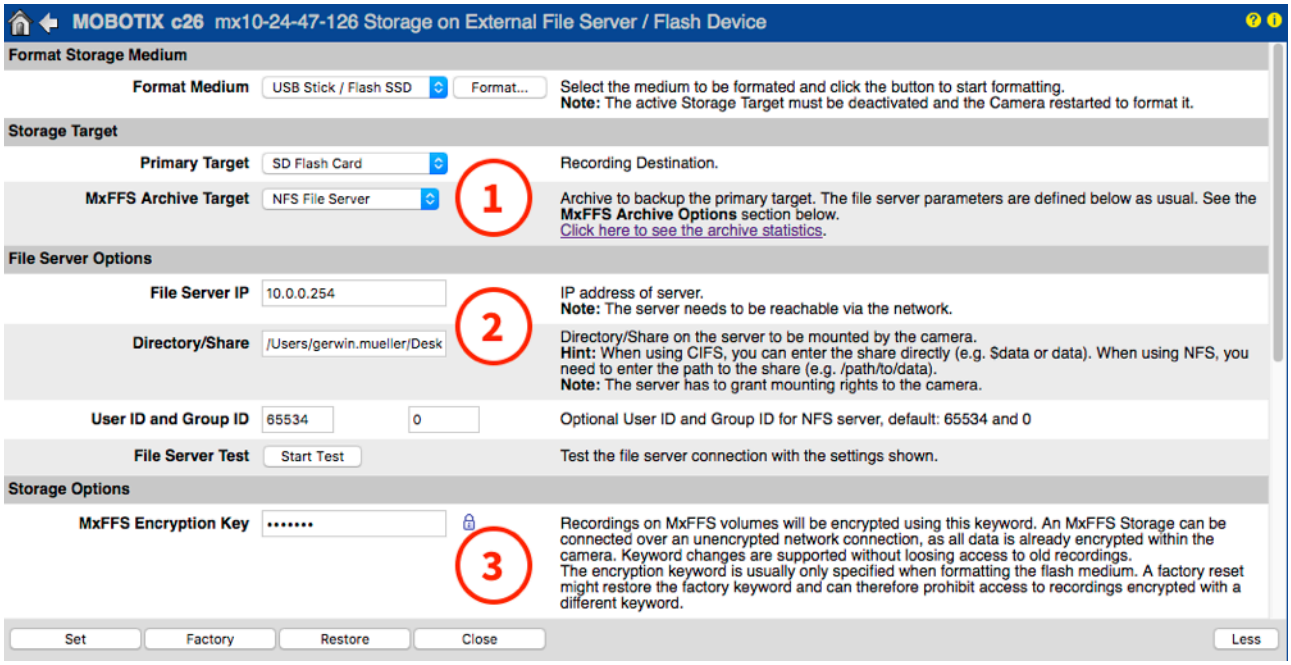
Admin Menu > Configuration du réseau > Serveur Web (pour les experts) > Serveur Web



L'authentification d'accès Digest est l'une des méthodes contractuelles qu'un serveur Web (c.-à-d. une caméra MOBOTIX) peut utiliser pour négocier des identifiants, tels qu'un nom d'utilisateur ou un mot de passe, avec un client (c.-à-d. 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. Configurez une clé de cryptage pour les enregistrements

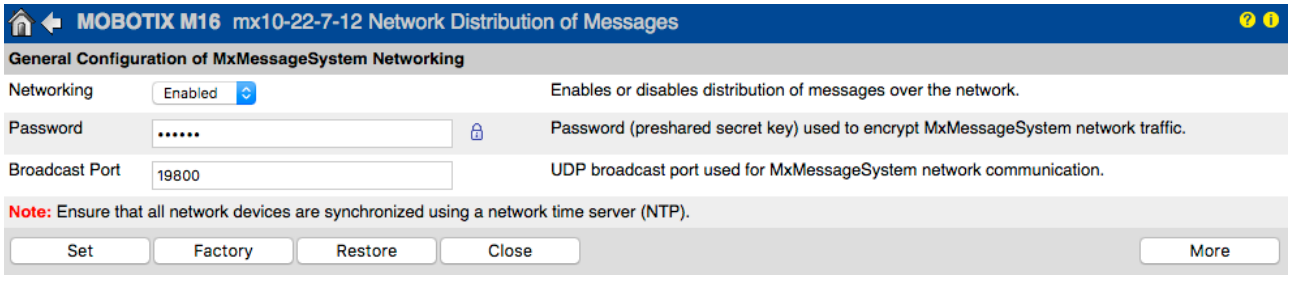
Admin Menu > Stockage > Enregistrement sur un serveur de fichiers externe / support Flash



Vous pouvez configurer une clé de cryptage pour chiffrer les enregistrements sauvegardés sur le dispositif de stockage interne (carte microSD/clé USB) ainsi que les enregistrements archivés sur le serveur de fichiers externe (SMB/NFS).

12. Changez le mot de passe par défaut de MxMessage (si activé)

Admin Menu > MxMessageSystem > Distribution des messages réseau



MxMessageSystem permet de transférer des messages entre les différentes caméras du réseau. Il faut configurer un mot de passe (clé symétrique) comportant au moins 6 caractères pour crypter les messages transférés.

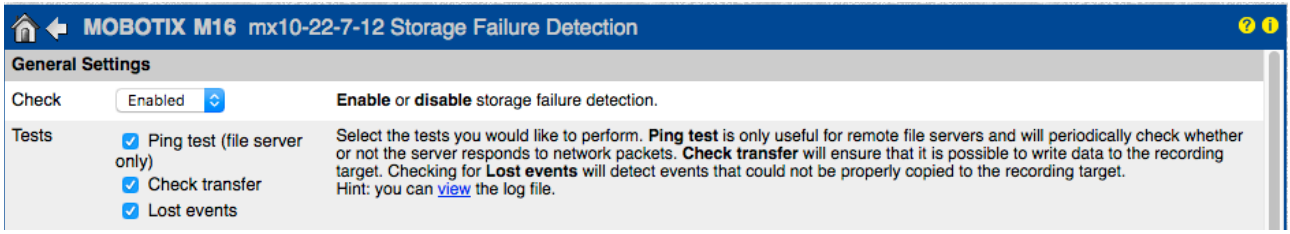
13. Activez la notification d'erreur

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

La boîte de dialogue Error Notification propose plusieurs options de réception de notifications (e-mail, notifications IP, appels VoIP, etc.) en cas de redémarrage ou de détection d'erreurs dans les différents systèmes de la caméra. Cet outil aide les administrateurs système à s'assurer que toutes les caméras MOBOTIX fonctionnent correctement.

14. Activez la détection d'erreurs de stockage

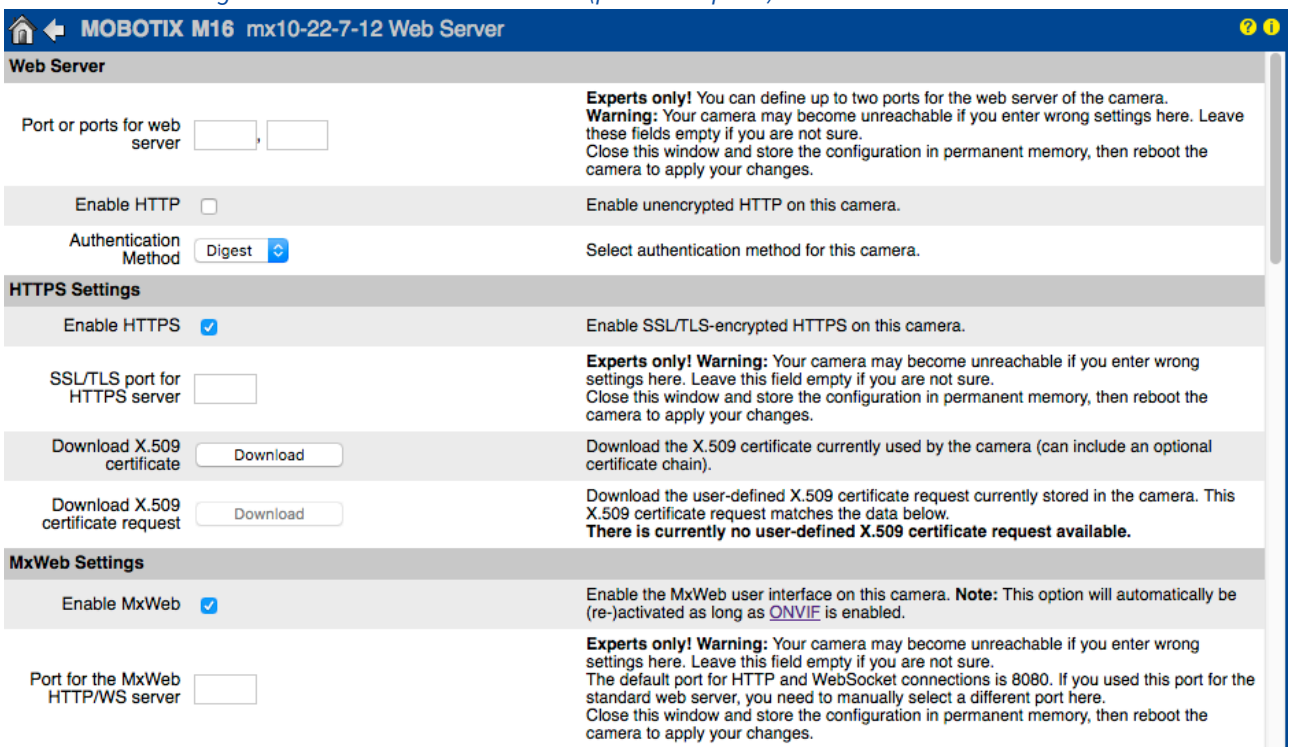
Admin Menu > Stockage > Contrôle de panne de la mémoire



Utilisez la boîte de dialogue Storage Failure Detection pour configurer des tests qui surveillent en continu la cible mémoire externe (serveur de fichiers ou périphérique flash) que la caméra utilise comme mémoire tampon circulaire externe. La caméra surveillera activement sa cible mémoire et signalera les problèmes d'enregistrement vidéo en utilisant les méthodes de notification mentionnées dans la boîte de dialogue.

15. Changez les ports par défaut du serveur Web (pour l'accès distant)

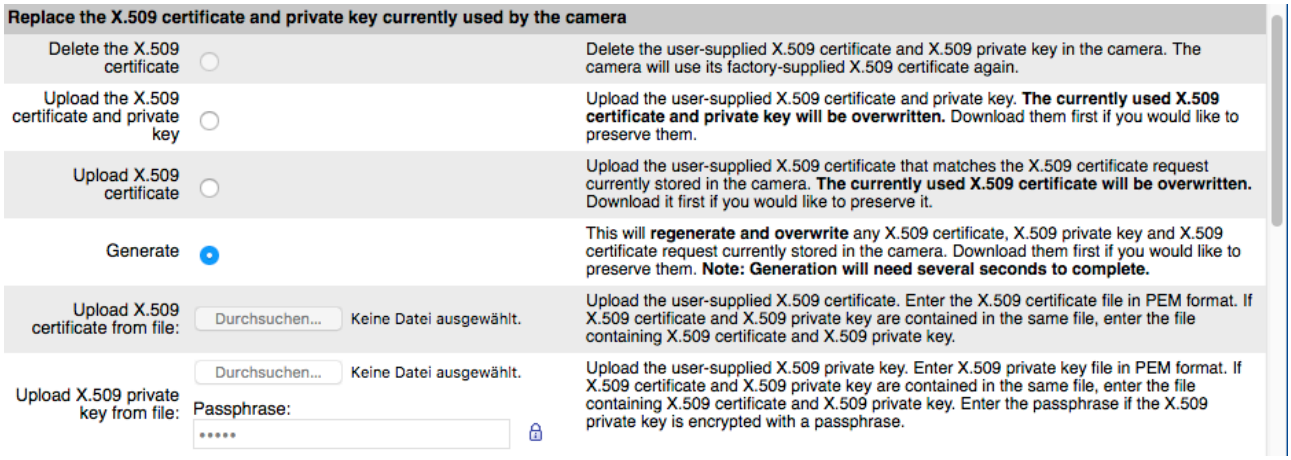
Admin Menu > Configuration du réseau > Serveur Web (pour les experts)



Les ports standards (TCP 80 pour l'HTTP et TCP 443 pour l'HTTPS) sont plus sujets aux attaques. Remplacer les ports par défaut par des ports personnalisés peut aider à renforcer la sécurité de la caméra.

16. Générez et téléchargez des certificats X.509 personnalisés

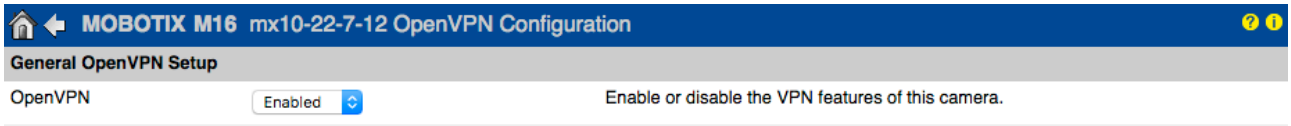
Admin Menu > Configuration du réseau > Serveur Web (pour les experts))



Télécharger un certificat personnalisé signé par une AC (Autorité de Certification) fiable permettra de garantir la confidentialité et l'authenticité de toutes les connexions établies via un serveur HTTPS (SSL/TLS).

17. Configurez un client OpenVPN pour les connexions distantes

Admin Menu > Configuration du réseau > Configuration du client OpenVPN



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

Pour créer une connexion OpenVPN, vous devez disposer d'un serveur correspondant qui permet d'accéder de manière sécurisée à la caméra. Pour ce faire, vous pouvez utiliser votre propre serveur OpenVPN ou faire appel à un fournisseur OpenVPN.
Pour obtenir plus d'informations sur OpenVPN, rendez-vous sur le site Internet *OpenVPN Community* .

18. Sauf nécessité absolue, évitez d'exposer la caméra sur Internet

Permettre à un utilisateur d'accéder à la caméra à distance doit être un choix délibéré pour réduire les risques d'attaque. Si vous avez besoin d'un accès distant, veuillez respecter scrupuleusement les règles susmentionnées pour ne permettre qu'aux utilisateurs prévus de se connecter.

19. Utilisez des VLAN pour séparer le réseau CCTV (niveau de sécurité de l'entreprise)

Dans les environnements d'entreprise, il est recommandé de tenir le réseau CCTV (caméras IP, postes de travail NVR et VMS) à l'écart des autres hôtes pour éviter les accès non autorisés et la saturation du trafic.

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

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

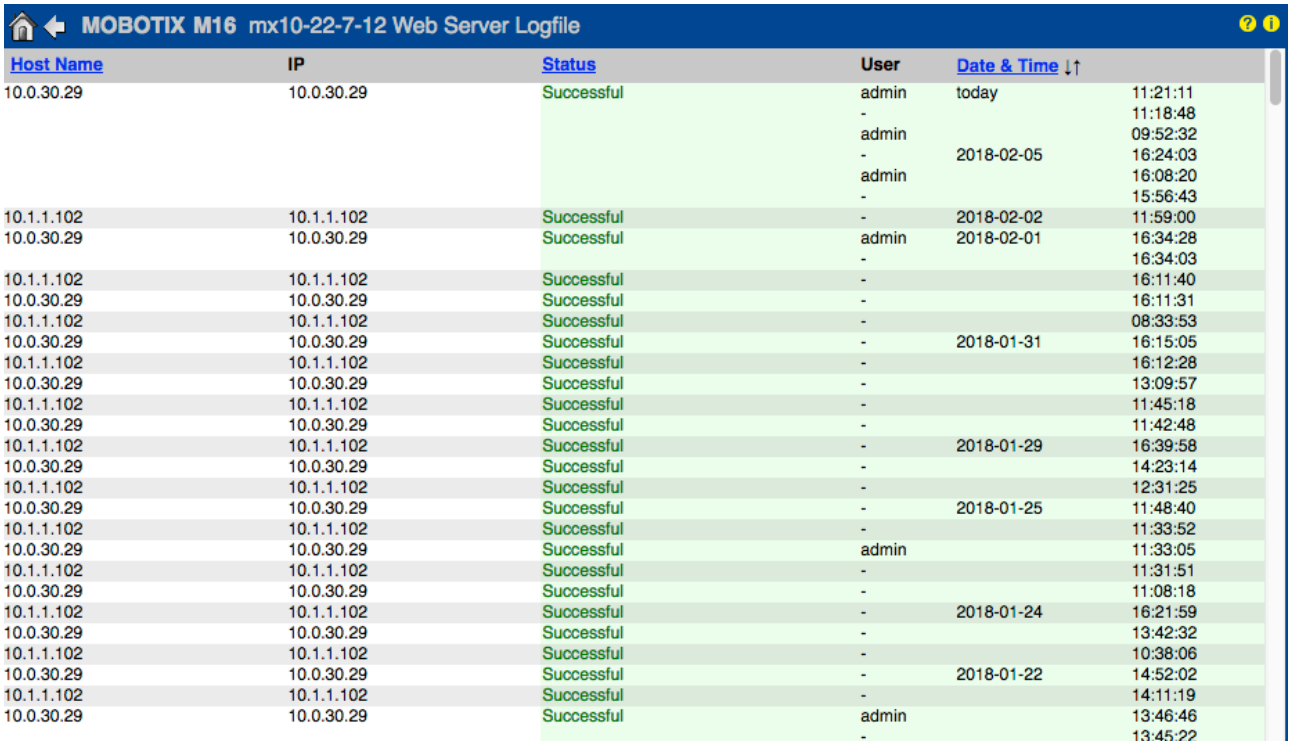
Cette norme internationale est utilisée pour le contrôle d'accès du réseau basé sur les ports (NAC). Pour pouvoir utiliser cette procédure, il faut que tous les appareils réseau (y compris la caméra MOBOTIX) s'authentifient eux-mêmes au commutateur pour obtenir une connexion réseau. Les appareils réseau sans authentification valide seront rejetés.

Adressez-vous à votre administrateur réseau pour savoir 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 convenablement. En général, le commutateur (authentificateur) a également besoin d'un serveur

d'authentification tel qu'un serveur RADIUS. Le serveur d'authentification contrôle la procédure d'authentification. Assurez-vous que la caméra et le serveur d'authentification suivent toujours la même procédure.

21. Consultez régulièrement le fichier journal du serveur Web

Admin Menu > Sécurité > Fichier journal du serveur Web

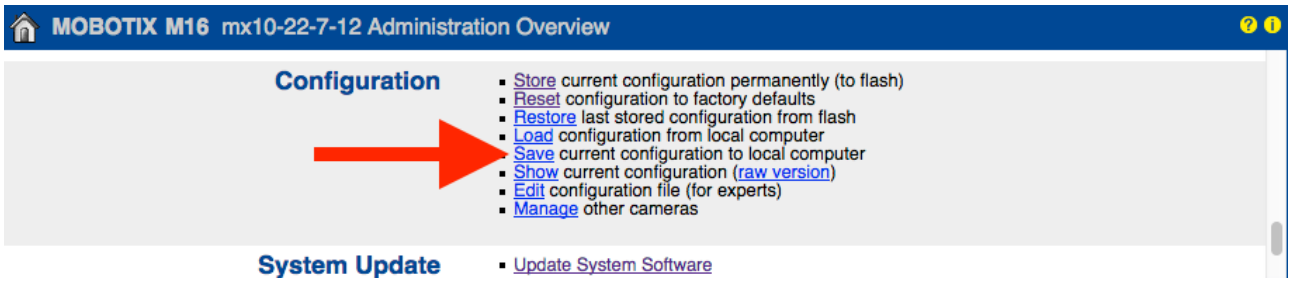


Host Name	IP	Status	User	Date & Time ↓↑	
10.0.30.29	10.0.30.29	Successful	admin	today	11:21:11
			-		11:18:48
			admin		09:52:32
			-	2018-02-05	16:24:03
			admin		16:08:20
			-		15:56:43
10.1.1.102	10.1.1.102	Successful	-	2018-02-02	11:59:00
10.0.30.29	10.0.30.29	Successful	admin	2018-02-01	16:34:28
			-		16:34:03
10.1.1.102	10.1.1.102	Successful	-		16:11:40
10.0.30.29	10.0.30.29	Successful	-		16:11:31
10.1.1.102	10.1.1.102	Successful	-		08:33:53
10.0.30.29	10.0.30.29	Successful	-	2018-01-31	16:15:05
10.1.1.102	10.1.1.102	Successful	-		16:12:28
10.0.30.29	10.0.30.29	Successful	-		13:09:57
10.1.1.102	10.1.1.102	Successful	-		11:45:18
10.0.30.29	10.0.30.29	Successful	-		11:42:48
10.1.1.102	10.1.1.102	Successful	-	2018-01-29	16:39:58
10.0.30.29	10.0.30.29	Successful	-		14:23:14
10.1.1.102	10.1.1.102	Successful	-		12:31:25
10.0.30.29	10.0.30.29	Successful	-	2018-01-25	11:48:40
10.1.1.102	10.1.1.102	Successful	-		11:33:52
10.0.30.29	10.0.30.29	Successful	admin		11:33:05
10.1.1.102	10.1.1.102	Successful	-		11:31:51
10.0.30.29	10.0.30.29	Successful	-		11:08:18
10.1.1.102	10.1.1.102	Successful	-	2018-01-24	16:21:59
10.0.30.29	10.0.30.29	Successful	-		13:42:32
10.1.1.102	10.1.1.102	Successful	-		10:38:06
10.0.30.29	10.0.30.29	Successful	-	2018-01-22	14:52:02
10.1.1.102	10.1.1.102	Successful	-		14:11:19
10.0.30.29	10.0.30.29	Successful	admin		13:46:46
			-		13:45:22

Le fichier journal du serveur Web répertorie toutes les tentatives d'accès horodatées avec les messages d'état correspondants du serveur Web ainsi que le nom d'hôte de l'ordinateur qui accède à la caméra. Les tentatives d'accès non autorisées peuvent mettre en alerte les administrateurs système et les inciter à revoir la solidité de leur réseau.

22. Enregistrez les fichiers de configuration de secours dans un endroit sûr

Admin Menu > Configuration > Enregistrer la configuration actuelle sur un ordinateur local



Même si les identifiants de la caméra (mots de passe utilisateur) sont hachés dans le fichier de configuration de la caméra, tous les fichiers de configuration de secours doivent être sauvegardés dans un endroit sûr. Nous vous conseillons en outre de crypter les fichiers avec une phrase de passe pour renforcer la sécurité.

Félicitations – votre caméra MOBOTIX est désormais cybersécurisée !

Configuration VMS (système de gestion vidéo)

1. Créez des comptes utilisateur sur l'ordinateur utilisé

2. Créez des comptes utilisateur sur MxMC

3. Limitez les droits aux utilisateurs VMS

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

5. Activez la « déconnexion auto »

Félicitations – votre système de gestion vidéo est désormais cybersécurisé !

Configuration NAS (Network Attached Storage)

1. Conservez l’appareil utilisé pour sauvegarder les images dans un endroit sûr

2. Saisissez un mot de passe sécurisé pour le compte administrateur

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

4. Cryptez les volumes

5. Choisissez un niveau RAID garantissant la redondance des données

Félicitations – votre système de stockage en réseau NAS est désormais cybersécurisé !