

# **Guide de cyberprotection**

# Comment protéger votre système vidéo MOBOTIX

### Caméra • VMS • NAS

© MOBOTIX AG • www.mobotix.com • 09/2019 Guide de cyberprotection





#### 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.

**Avis de copyright :** tous droits réservés. MOBOTIX, le logo de MOBOTIX AG et MxAnalytics sont des marques déposées de MOBOTIX AG en Union européenne, aux Etats-Unis et dans d'autres pays. © MOBOTIX AG 2018

### Configuration de la caméra



#### 1. Mettez à jour le micrologiciel des caméras

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

Vous ne savez pas comment procéder ? Veuillez vous référer à ce mini guide : <u>www.mobotix.com > Support ></u> <u>Download Center > Documentation > Brochures & Guides > Guides compacts > Mx\_CG\_FirmwareUpdate.pdf</u>

#### 2. Revenez à la configuration par défaut.

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

	Live	2		
16 fps C Display Mo	de 🖸 Fullimage 🖸 🔍	DÍ VHQ		
o Menu	Ania faday kunitarahadunanya 000704		mx10-24-47-126 Administration Overview	1
Record	ninjindex.ntmi/cachedummy=606764			-
	c26 mx10-24-47-126 Administration Ov	erview		00
G on		-	General Network Client Settings (for experts)	
G off				
vent	MxMessageS	System	Network Distribution of Messages Message Profiles for Action Groups	
31ink				
E Event	S	torage	Storage on External File Server / Flash Device Storage Failure Detection	
List				
tcher	Logos and Image P	rofiles	Manage Image Files	
om		- 1	Image Profiles	
1+	Transfer P	rofiles •	ETP Profiles	
n -		:	E-Mail Profiles	
Pan	Availation of MalD Tale		0	
Image	Audio and voiP Tele	epnony	Speaker and Microphone Manage Audio Messages	
ave on		-	Surver Settings for brighting back addit mes SIP Server Settings for configuring integrated SIP server	- 1
ive off		-	Outgoing Calls Settings	
			ATP Pager	
	Camera Adminis	tration •1	Time & Date	- 1
		:	LED Setup Time Tables for arming and services	- 1
		:	Time Tasks for image Transfer and other jobs Integration Protocols for video streaming (RTP server configuration)	- 1
		- 1	Retail Configuration	- 1
	Config	uration .	Store current configuration permanently (to flash)	
			Reset configuration to factory defaults Restore last stored configuration from flash	
		:	Load computation from local computer Save current configuration to local computer	
	_	:	Edit configuration file (for experts)	
		- 1	maraye over carreras	
	System I	Update •	Update System Software	
	General	Tasks •	Reboot the camera	
Security	Browsers retain password information until they a	re closed completely	y. To prevent unauthorized use of protected pages, make sure that you close all browser windows at the end of your session. Failing to d	to I
Warning:	so will leave the password in the browser cache a	and other users may	manipulate your camera(s)!	

#### 3. Changez le mot de passe admin par défaut

🏠 🔶 мовс	<b>TIX M16</b> mx10-22-7	-12 Users and Pa	asswords	0 0
User	Group	Password	Confirm Password	Remark/Action
admin	admins ᅌ	•••	•••	Remove
	undefined ᅌ			

*Admin Menu > Sécurité > Utilisateurs et mots de passe* 

Il est toujours nécessaire de changer le mot de passe par défaut <<meinsm>> la première fois que vous appelez la caméra.

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 le mot de passe administrateur n'est plus disponible, la caméra doit être réinitialisée via MOBOTIX moyennant des frais !

#### 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

Transformation of the second s					<b>?</b> ()						
	Brows	er Scr	een / Vie	w		MxMC 8	VMS	Configu	uration		
Access Rights	Guest	Live	Player	MultiView	PDA	Event Stream	HTTP API	Admin	Image Setup	Event Setup	
Public Access											Disable all
Groups											Remove Group
admins								1	<ul> <li>Image: A start of the start of</li></ul>		
es_admins											
es_guests											
es_users											
www_guests	<b>~</b>										
www_users											
Open Users and Pa	assword	s to m	anage u	sers and to a	assign	groups.					

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

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

🏠 🔶 МОВОТІХ	c26 mx10-24-47-126 IP-Level	Access Control	? i
Access Control Conf	iguration		
WARNING: A faulty access configuration may render the camera inaccessible!			
Access Control	Enabled ᅌ	Enable or disable Access Control.	
Access Rules for Allo	w		
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 Der	ıy		
Mode	IP Address/Subnet/Domain	Examples	
Deny ᅌ	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 ᅌ	Access from all IP addresses/subnets/o	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

Intrusion Detection S	ettings	
Enable intrusion detection	0	Send notification on repeated unsuccessful login attempts.
Notification threshold	7	Number of unsuccessful login attemps that will trigger a notification. Minimum value is 5.
Timeout	60 Minutes	Idle timeout in minutes. Leave empty to use the default (60 minutes). Subsequent accesses of a client within this timeout are logged as one access with the date of the first and the last access and a counter is incremented. (See "More" view of <u>Web Server Logfile</u> )
Deadtime	60 Minutes	Deadtime between notifications. Leave empty to use the default (60 minutes). Set to zero to trigger a notification at every login attempt once the threshold has been reached.
Block IP Address	٥	Block IP address of offending HTTP client using <b>IP-Level Access Control</b> when threshold has been reached. Blocking is temporary until next reboot. This function takes only effect if <u>IP-Level Access Control</u> is enabled.
E-Mail Notification	AlarmMail	E-Mail Profile: Send image by e-mail. ( <u>E-Mail Profiles</u> )
IP Notify	Off 🗘	IP Notify Profile: Notification by network message using the TCP/IP protocol. (IP Notify Profiles)

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

Page Options		
Language	en 🗘	Select the language for the dialogs and the user interface.
Image Pull-Down Menus	Show ᅌ	Show or Hide the pull-down menus for image settings on the Live page.
Refresh Rate for Guest Access	Maximum Default 2 fps C 1 fps C	Maximum and default image refresh rate on the Guest page.
Refresh Rate for User Access	Maximum Default 30 fps C 16 fps C	Maximum and default image refresh rate on the Live page.
Operating Mode	Server Push	Default operating mode of <u>Live</u> page. If you select <i>ActiveX</i> , the control will also be used to play event images on the <u>Player</u> page.
Preview Button	Hide O	Allows to select the frame rate for low-bandwidth connections per client/browser separately from the full-size frame rate settings. Requires cookies to be enabled in your browser.
Web Crawler Restrictions	Crawling forbidden	Allows web crawlers and search engines to scan the contents of the camera's webserver.

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

🏫 🔶 МОВОТІХ	M16 mx10-2	22-7-12 Web Server		? 🛈
Web Server				
Port or ports for web server	,		Experts only! You can define up to two ports for the web server of the camera. Warning: Your camera may become unreachable if you enter wrong settings here. Leave these fields empty if you are not sure. Close this window and store the configuration in permanent memory, then reboot th camera to apply your changes.	ne
Enable HTTP			Enable unencrypted HTTP on this camera.	
Authentication Method	Digest 🗘		Select authentication method for this camera.	
HTTPS Settings	Auto Basic			
Enable HTTPS	✓ Digest		Enable SSL/TLS-encrypted HTTPS on this camera.	

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

MOBOTIX c26 mx10	0-24-47-126 Storage on	External F	File Server / Flash Device	<b>?</b> i
Format Storage Medium				
Format Medium	USB Stick / Flash SSD ᅌ	Format	Select the medium to be formated and click the button to start formatting. Note: The active Storage Target must be deactivated and the Camera restarted to format it.	- 1
Storage Target				
Primary Target	SD Flash Card	$\frown$	Recording Destination.	- 1
MxFFS Archive Target	NFS File Server		Archive to backup the primary target. The file server parameters are defined below as usual. See MxFFS Archive Options section below. Click here to see the archive statistics.	the
File Server Options				
File Server IP	10.0.0.254	$\bigcirc$	IP address of server. Note: The server needs to be reachable via the network.	
Directory/Share	/Users/gerwin.mueller/Desk		Directory/Share on the server to be mounted by the camera. Hint: When using CIFS, you can enter the share directly (e.g. Sdata or data). When using NFS, yo need to enter the path to the share (e.g. /path/d/data). Note: The server has to grant mounting rights to the camera.	bu
User ID and Group ID	65534 0		Optional User ID and Group ID for NFS server, default: 65534 and 0	
File Server Test	Start Test		Test the file server connection with the settings shown.	
Storage Options				
MxFFS Encryption Key		3	Recordings on MxFFS volumes will be encrypted using this keyword. An MxFFS Storage can be connected over an unencrypted network connection, as all data is already encrypted within the camera. Keyword changes are supported without loosing access to old recordings. The encryption keyword is usually only specified when formatting the flash medium. A factory rese might restore the factory keyword and can therefore prohibit access to recordings encrypted with a different keyword.	et a
Set Factory	Restore	Close		.ess

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	Admin Menu > MxMessageSystem > Distribution des messages réseau			
🏠 🔶 МОВО	MOBOTIX M16 mx10-22-7-12 Network Distribution of Messages			
General Configur	General Configuration of MxMessageSystem Networking			
Networking	Enabled ᅌ	Enables or disables distribution of messages over the network.		
Password	•••••	Password (preshared secret key) used to encrypt MxMessageSystem network traffic.		
Broadcast Port	19800	UDP broadcast port used for MxMessageSystem network communication.		
Note: Ensure that	all network devices are synchronized using a r	network time server (NTP).		
Set	Factory Restore (	Close Mo	re	

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

<b>渝</b> 🔶 M	OBOTIX M16 mx10-2	2-7-12 Storage Failure Detection	<b>?</b> i
General Se	ettings		
Check	Enabled ᅌ	Enable or disable storage failure detection.	
Tests	<ul> <li>Ping test (file server only)</li> <li>Check transfer</li> <li>Lost events</li> </ul>	Select the tests you would like to perform. <b>Ping test</b> is only useful for remote file servers and will periodically check wheth or not the server responds to network packets. <b>Check transfer</b> will ensure that it is possible to write data to the recording target. Checking for <b>Lost events</b> will detect events that could not be properly copied to the recording target. Hint: you can <u>view</u> the log file.	er

#### Guide de cyberprotection

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)

🏠 🔶 МОВОТІХ	M16 mx10-22-7-12 Web Server		? i
Web Server			
Port or ports for web server	· · · · · · · · · · · · · · · · · · ·	Experts only! You can define up to two ports for the web server of the camera. Warning: Your camera may become unreachable if you enter wrong settings here. Leav these fields empty if you are not sure. Close this window and store the configuration in permanent memory, then reboot the camera to apply your changes.	e
Enable HTTP		Enable unencrypted HTTP on this camera.	
Authentication Method	Digest 🗘	Select authentication method for this camera.	
HTTPS Settings			
Enable HTTPS		Enable SSL/TLS-encrypted HTTPS on this camera.	
SSL/TLS port for HTTPS server		Experts only! Warning: Your camera may become unreachable if you enter wrong settings here. Leave this field empty if you are not sure. Close this window and store the configuration in permanent memory, then reboot the camera to apply your changes.	
Download X.509 certificate	Download	Download the X.509 certificate currently used by the camera (can include an optional certificate chain).	
Download X.509 certificate request	Download	Download the user-defined X.509 certificate request currently stored in the camera. This X.509 certificate request matches the data below. There is currently no user-defined X.509 certificate request available.	
MxWeb Settings			
Enable MxWeb	0	Enable the MxWeb user interface on this camera. Note: This option will automatically be (re-)activated as long as <u>ONVIF</u> is enabled.	1
Port for the MxWeb HTTP/WS server		Experts only! Warning: Your camera may become unreachable if you enter wrong settings here. Leave this field empty if you are not sure. The default port for HTTP and WebSocket connections is 8080. If you used this port for 1 standard web server, you need to manually select a different port here. Close this window and store the configuration in permanent memory, then reboot the camera to apply your changes.	he

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))

Replace the X.509 certificate and private key currently used by the camera

riepidee the X.505 cer	incate and private key currently used b	y the camera
Delete the X.509 certificate		Delete the user-supplied X.509 certificate and X.509 private key in the camera. The camera will use its factory-supplied X.509 certificate again.
Upload the X.509 certificate and private key	0	Upload the user-supplied X.509 certificate and private key. The currently used X.509 certificate and private key will be overwritten. Download them first if you would like to preserve them.
Upload X.509 certificate	0	Upload the user-supplied X.509 certificate that matches the X.509 certificate request currently stored in the camera. <b>The currently used X.509 certificate will be overwritten.</b> Download it first if you would like to preserve it.
Generate	0	This will <b>regenerate and overwrite</b> any X.509 certificate, X.509 private key and X.509 certificate request currently stored in the camera. Download them first if you would like to preserve them. <b>Note: Generation will need several seconds to complete.</b>
Upload X.509 certificate from file:	Durchsuchen Keine Datei ausgewählt.	Upload the user-supplied X.509 certificate. Enter the X.509 certificate file in PEM format. If X.509 certificate and X.509 private key are contained in the same file, enter the file containing X.509 certificate and X.509 private key.
Upload X.509 private key from file:	Durchsuchen Keine Datei ausgewählt. Passphrase:	Upload the user-supplied X.509 private key. Enter X.509 private key file in PEM format. If X.509 certificate and X.509 private key are contained in the same file, enter the file containing X.509 certificate and X.509 private key. Enter the passphrase if the X.509 private key is encrypted with a passphrase.

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

🏫 🔶 МОВОТІХ М16	mx10-22-7-12 OpenVPN Configura	ation	? ()
General OpenVPN Setup			
OpenVPN	Enabled ᅌ	Enable or disable the VPN features of this camera.	

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 euxmêmes 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

n 🔶 MOBOTIX M16 mx	10-22-7-12 Web Server Lo	ogfile			? (
Host Name	IP	<u>Status</u>	User	Date & Time ↓↑	
10.0.30.29	10.0.30.29	Successful	admin - admin - admin -	today 2018-02-05	11:21:11 11:18:48 09:52:32 16:24:03 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

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 !