



# Guide de cyberprotection

## Comment protéger votre système vidéo MOBOTIX

Caméra • VMS • NAS





### 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 toute 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



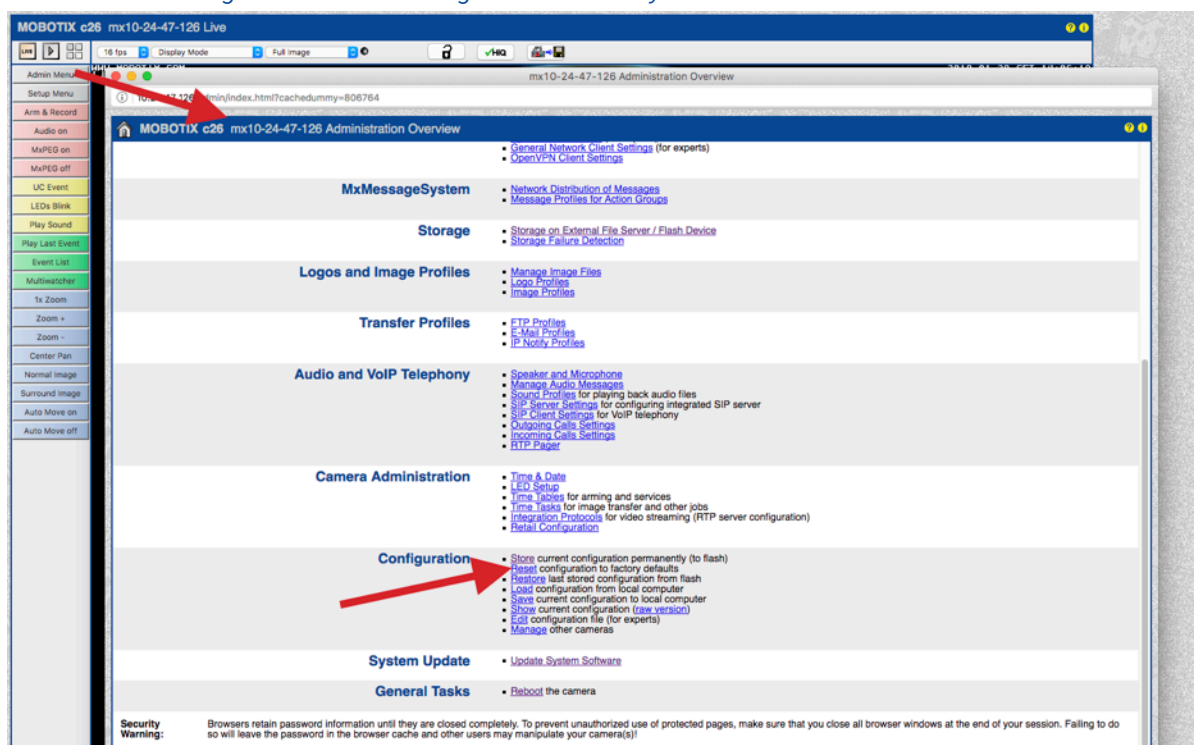
### 1. Mettez à jour le micrologiciel des caméras

Le micrologiciel MOBOTIX peut être téléchargé gratuitement sur notre site Internet : [www.mobotix.com](http://www.mobotix.com) > [Support](#) > [Download Center](#)

Vous ne savez pas comment procéder ? Veuillez vous référer à ce mini guide : [www.mobotix.com](http://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 > Reset configuration to factory defaults*



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

Admin Menu > Security > Users and Passwords

| User  | Group     | Password | Confirm Password | Remark/Action                   |
|-------|-----------|----------|------------------|---------------------------------|
| admin | admins    | ...      | ...              | <input type="checkbox"/> Remove |
|       | undefined |          |                  |                                 |

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 : ! " # \$ % & ' ( ) \* + , - . / : ; < = > ? @ [ \ ] ^ \_ ` { | } ~
- Éviter 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 > Security > Users and Passwords

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 > Security > Users and Passwords

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 > Security > Group Access Control Lists

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

| Access Rights | Browser Screen / View               |                                     |                                     |                                     |                                     | MxMC & VMS                          |                                     | Configuration                       |                                     |                                     |                              |
|---------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|------------------------------|
|               | Guest                               | Live                                | Player                              | MultiView                           | PDA                                 | Event Stream                        | HTTP API                            | Admin                               | Image Setup                         | Event Setup                         |                              |
| Public Access | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <button>Disable all</button> |
| <b>Groups</b> |                                     |                                     |                                     |                                     |                                     |                                     |                                     |                                     |                                     |                                     | <b>Remove Group</b>          |
| admins        | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/>     |
| es_admins     | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>     |
| es_guests     | <input type="checkbox"/>            | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>     |
| es_users      | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>     |
| www_guests    | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>     |
| www_users     | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/>     |
|               | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            |                              |

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 > Security > IP-Level Access Control

**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 supprime 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 > Network Setup > Web Server (for experts) > Intrusion Detection Settings*

| Intrusion Detection Settings                                   |                                                                                                                                                                                                                                                                                          |
|----------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Enable intrusion detection <input checked="" type="checkbox"/> | Send notification on repeated unsuccessful login attempts.                                                                                                                                                                                                                               |
| Notification threshold <input type="text" value="7"/>          | Number of unsuccessful login attempts that will trigger a notification. Minimum value is 5.                                                                                                                                                                                              |
| Timeout <input type="text" value="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 <a href="#">Web Server Logfile</a> ) |
| Deadtime <input type="text" value="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 <input checked="" type="checkbox"/>           | 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 <a href="#">IP-Level Access Control</a> is enabled.                                          |
| E-Mail Notification <input type="text" value="AlarmMail"/>     | <b>E-Mail Profile:</b><br>Send image by e-mail. ( <a href="#">E-Mail Profiles</a> )                                                                                                                                                                                                      |
| IP Notify <input type="text" value="Off"/>                     | <b>IP Notify Profile:</b><br>Notification by network message using the TCP/IP protocol. ( <a href="#">IP Notify Profiles</a> )                                                                                                                                                           |

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 > Page Administration > Language and Start Page > Page Options*

| Page Options                                                                                                            |                                                                                                                                                                                     |
|-------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Language <input type="text" value="en"/>                                                                                | Select the language for the dialogs and the user interface.                                                                                                                         |
| Image Pull-Down Menus <input type="text" value="Show"/>                                                                 | Show or Hide the pull-down menus for image settings on the <a href="#">Live</a> page.                                                                                               |
| Refresh Rate for Guest Access<br>Maximum <input type="text" value="2"/> fps Default <input type="text" value="1"/> fps  | Maximum and default image refresh rate on the <a href="#">Guest</a> page.                                                                                                           |
| Refresh Rate for User Access<br>Maximum <input type="text" value="30"/> fps Default <input type="text" value="16"/> fps | Maximum and default image refresh rate on the <a href="#">Live</a> page.                                                                                                            |
| Operating Mode <input type="text" value="Server Push"/>                                                                 | Default operating mode of <a href="#">Live</a> page. If you select <i>ActiveX</i> , the control will also be used to play event images on the <a href="#">Player</a> page.          |
| Preview Button <input type="text" value="Hide"/>                                                                        | 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 <input type="text" value="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 > Network Setup > Web Server (for experts) > 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 the camera to apply your changes.

Enable HTTP: ☒ Enable unencrypted HTTP on this camera.

Authentication Method: **Digest** Select authentication method for this camera.

**HTTPS Settings**

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 > Storage > Storage on External File Server / Flash Device

**Format Storage Medium**

Format Medium: USB Stick / Flash SSD [Format...]

Select the medium to be formatted and click the button to start formatting. **Note:** The active Storage Target must be deactivated and the Camera restarted to format it.

**Storage Target**

Primary Target: SD Flash Card Recording Destination.

MxFFS Archive Target: **NFS File Server** Archive to backup the primary target. The file server parameters are defined below as usual. See the [MxFFS Archive Options](#) section below. [Click here to see the archive statistics.](#)

**File Server Options**

File Server IP: 10.0.0.254 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, you need to enter the path to the share (e.g. /path/to/data). **Note:** The server has to grant mounting rights to the camera.

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: [Masked] 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 losing access to old recordings. The encryption keyword is usually only specified when formatting the flash medium. A factory reset might restore the factory keyword and can therefore prohibit access to recordings encrypted with a different keyword.

Buttons: Set, Factory, Restore, Close, Less

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 > Network Distribution of Messages

**General Configuration of MxMessageSystem Networking**

Networking: Enabled Enables or disables distribution of messages over the network.

Password: [Masked] Password (preserved 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 network time server (NTP).

Buttons: Set, Factory, Restore, Close, More

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.

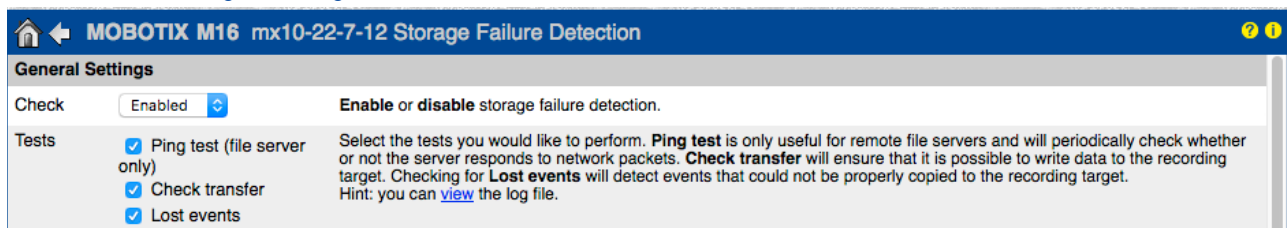
### 13. Activez la notification d'erreur

*Admin Menu > System Information > Error Notification*

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 > Storage > Storage Failure Detection*

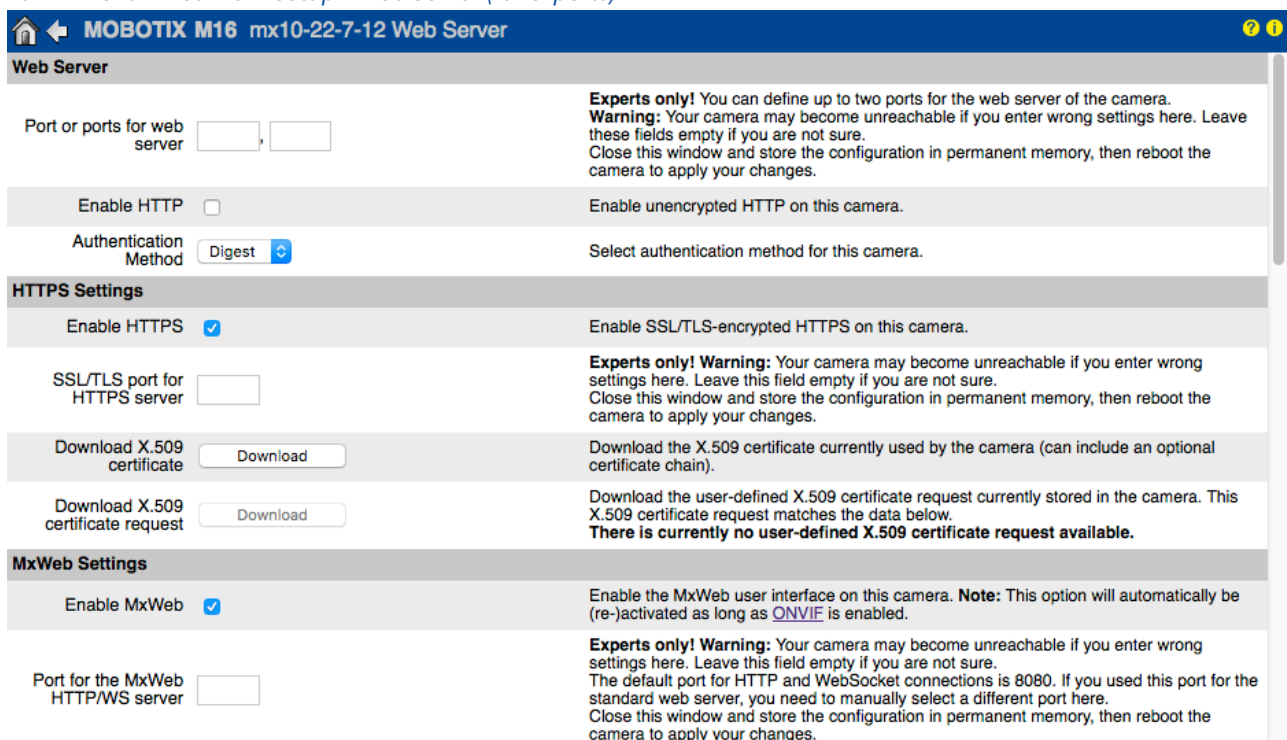


The screenshot shows the 'MOBOTIX M16 mx10-22-7-12 Storage Failure Detection' window. Under 'General Settings', the 'Check' is set to 'Enabled'. The 'Tests' section has three checked options: 'Ping test (file server only)', 'Check transfer', and 'Lost events'. A descriptive text on the right explains the tests and provides a hint to view the log file.

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. Désactivez HTTP, changez les ports par défaut du serveur Web (pour l'accès distant)

*Admin Menu > Network Setup > Web Server (for experts)*



The screenshot shows the 'MOBOTIX M16 mx10-22-7-12 Web Server' window. It includes sections for 'Web Server' (with fields for port and checkboxes for HTTP and HTTPS), 'HTTPS Settings' (with fields for SSL/TLS port and download buttons for certificates), and 'MxWeb Settings' (with a checkbox for MxWeb and a port field). Each section contains detailed warnings and instructions for configuration.

Les ports standards (TCP 80 pour l'HTTP et TCP 443 pour l'HTTPS) sont plus sujets aux attaques. Désactiver le protocole http et 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 > Network Setup > Web Server (for experts)

| Replace the X.509 certificate and private key currently used by the camera                                                                        |                                                                                                                                                                                                                                                                                                                     |
|---------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Delete the X.509 certificate <input type="radio"/>                                                                                                | 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 <input type="radio"/>                                                                                | Upload the user-supplied X.509 certificate and private key. <b>The currently used X.509 certificate and private key will be overwritten.</b> Download them first if you would like to preserve them.                                                                                                                |
| Upload X.509 certificate <input type="radio"/>                                                                                                    | 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 <input checked="" type="radio"/>                                                                                                         | 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: <input type="button" value="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: <input type="button" value="Durchsuchen..."/> Keine Datei ausgewählt.<br>Passphrase: <input type="password"/> | 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 > Network Setup > OpenVPN Client Settings

| MOBOTIX M16 mx10-22-7-12 OpenVPN Configuration      |                                                    |
|-----------------------------------------------------|----------------------------------------------------|
| General OpenVPN Setup                               |                                                    |
| OpenVPN <input checked="" type="checkbox"/> Enabled | 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](https://openvpn.com).

### 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 > Network Setup > Ethernet Interface (for 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 > Security > Web Server Logfile

| MOBOTIX M16 mx10-22-7-12 Web Server Logfile |            |            |       |                |          |
|---------------------------------------------|------------|------------|-------|----------------|----------|
| 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 > Save current configuration to local computer

MOBOTIX M16 mx10-22-7-12 Administration Overview

Configuration



- Store current configuration permanently (to flash)
- Reset configuration to factory defaults
- Restore last stored configuration from flash
- Load configuration from local computer
- Save current configuration to local computer
- Show current configuration (raw version)
- Edit configuration file (for experts)
- Manage other cameras

System Update

- Update System Software

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 !