Cyber Protection Guide

How To Harden
Your MOBOTIX Video System

Camera • VMS • NAS

CYBER SECURITY
INITIATIVE 2018

MOBOTIX

About This Guide

Cyber-attacks against internet connected software and hardware is a growing problem. In recent years, attackers are increasingly focused on exploiting the weakest links within a security perimeter to gain access to critical applications and sensitive data.

With video surveillance technology as a vital part of site security that often inhabits a shared corporate network; video surveillance devices are increasingly becoming the target of directed cyber-attacks.

Recognising this emerging trend, MOBOTIX has developed a set of **built-in tools and features** allowing IT security administrators to configure each device as part of a multi-layered approach to cyber security.

These tools when used alongside other security elements such as firewalls and network segmentation can reduce the attack surface presented by MOBOTIX devices as part of a secure access policy for administrators and users.

This guide provides practical advice on how to configure MOBOTIX devices to offer the most protection against cyber-attack along with best practice guidance on building a secure video surveillance infrastructure.

Please note: This document is intended to give the responsible admin a complete overview of all possible measurements to harden the MOBOTIX system. Regarding the individual application and to avoid reconfigurations, it may not be useful to carry out every single procedure explained in this guide.

General information: MOBOTIX assumes no liability for technical errors, printing errors or omissions.

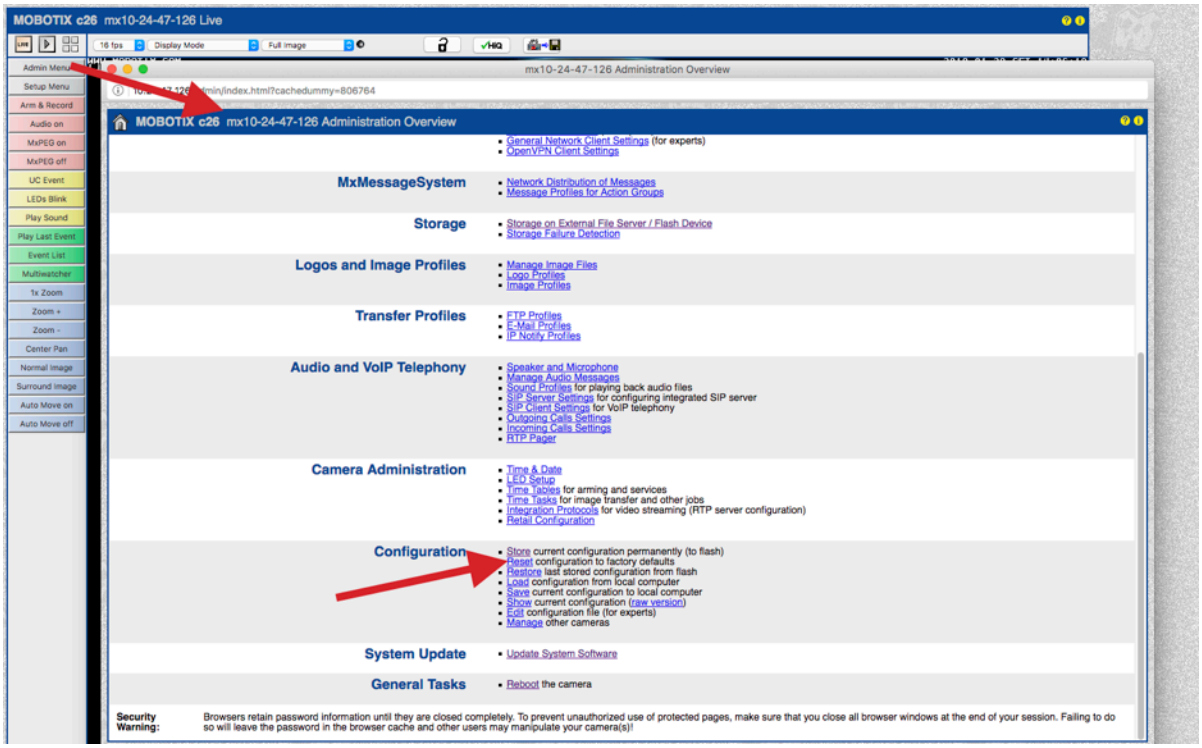
Camera Configuration

1. Keep the firmware of the cameras up-to-date

MOBOTIX firmware can be downloaded for free from our web site: *www.mobotix.com > Support > Download Center*
Not sure how to to proceed? Please refer to this compact guide: *www.mobotix.com > Support > Download Center > Documentation > Brochures & Guides > Compact Guides > Mx_CG_FirmwareUpdate.pdf*

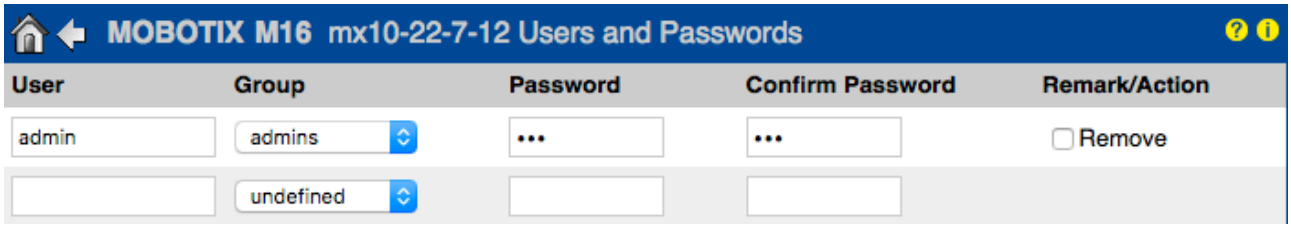
2. Reset the configuration to factory defaults

Admin Menu > Configuration > Reset configuration to factory defaults



3. Change the default admin password

Admin Menu > Security > Users and Passwords



It is strongly recommended to change the “admin” user name and the default password “meinsm”.
Once you have finished configuring users, passwords and groups, you should always store the settings in the camera's permanent memory. Otherwise, the modified configuration will only be used until the next camera reboot. Use the Close button at the end of the dialog as it will automatically ask you to store the camera configuration to the camera's permanent memory.

Make sure that you store your password information in a secure place. Special care should be taken to retain the password of at least one user of the admins group. Without the password, administrative access to the camera is not possible any more and there is no possibility to circumvent the password. It is likewise impossible to retrieve the password from a permanently saved configuration.

How to create a strong password:
- Use 8 or more characters (up to 99)
- At least one upper-case character
- At least one lower-case character
- At least one digit
- At least one special character: ! “ # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ `{|} ~
- Avoid common words and dates

Password reset policy: If the administrator password is no longer available, you will have to send the camera back to MOBOTIX for a factory reset!

4. Create different user groups with different user rights

Admin Menu > Security > Users and Passwords

Generally speaking, not all the users need the same rights. You can create up to 25 different users group from the page Admin Menu > Group Access Control List

5. Create different users and assign them to the right groups

Admin Menu > Security > Users and Passwords

It’s always advisable to create a user for each person who is authorized to access the camera. Up to 100 users can be created. Actions performed by authorized users are tracked in the Web Server Log file; this helps to determine “who did what” in case of disputes.

Refer to the description above to create strong passwords.

6. Disable Public Access

Admin Menu > Security > Group Access Control Lists

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.

Public Access allows, if enabled, to access specific resources of the camera without authentication. It's strongly recommended to disable Public Access to avoid that unauthorized users can display the camera's live stream, recordings or even control the camera (e.g. change the configuration or execute actions).

7. Enable IP Access Control List

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:

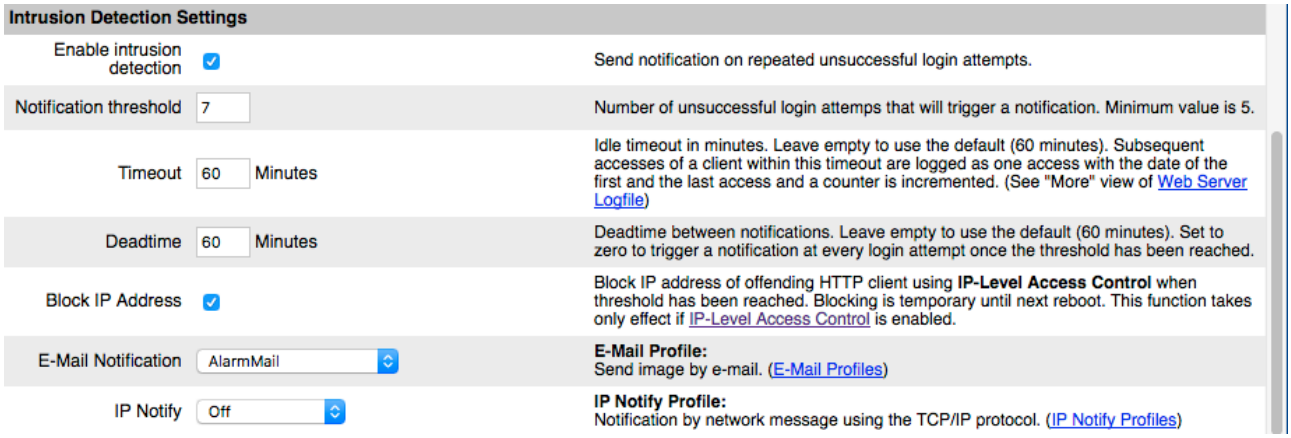
Allow — Access from all IP addresses/subnets/domains not listed above.

Set | Factory | Restore | Close

The Access Control dialog allows managing the IP addresses, subnets and domain names, which are allowed to access the camera or which are prevented from accessing the camera. This possibility to control access to the camera uses the IP protocol level, is independent of password-based user authentication on HTTP protocol level and supersedes password-based authentication. If a computer does not have IP-level access to the camera, there is no possibility to reach the camera from that computer. If a computer has IP-level access to the camera, password-based user authentication follows as next step, as specified in the Users and Passwords dialog.

8. Enable the Intrusion Detection with notification and block of offending IP address

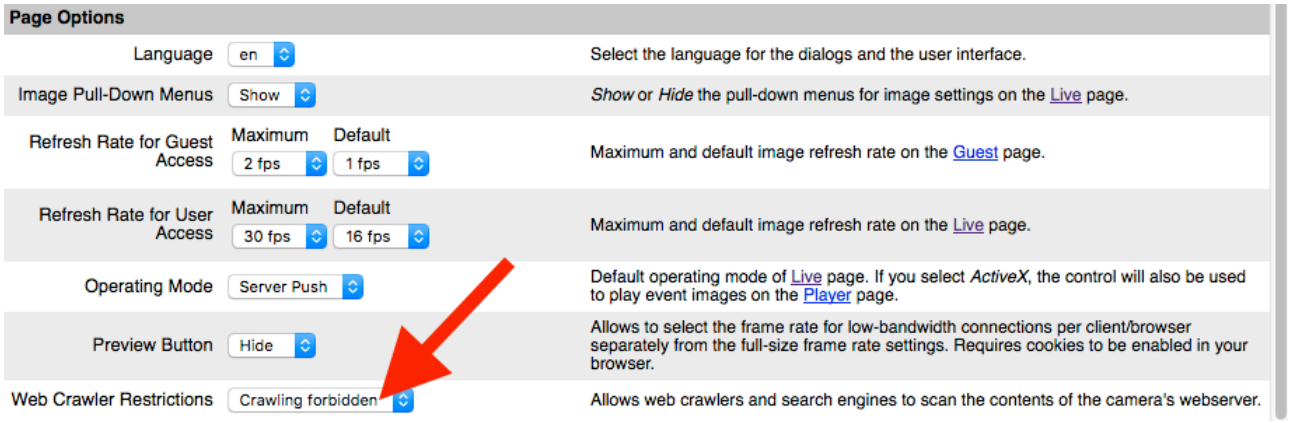
Admin Menu > Network Setup > Web Server (for experts) > Intrusion Detection Settings



This feature provides an automatic defense against attacks. If an intruder should try to access the camera using "brute force" methods to guess user names and passwords, the camera can send an alert and automatically lock out the offending IP address after a certain number of failed attempts.

9. Check that Web Crawling is forbidden

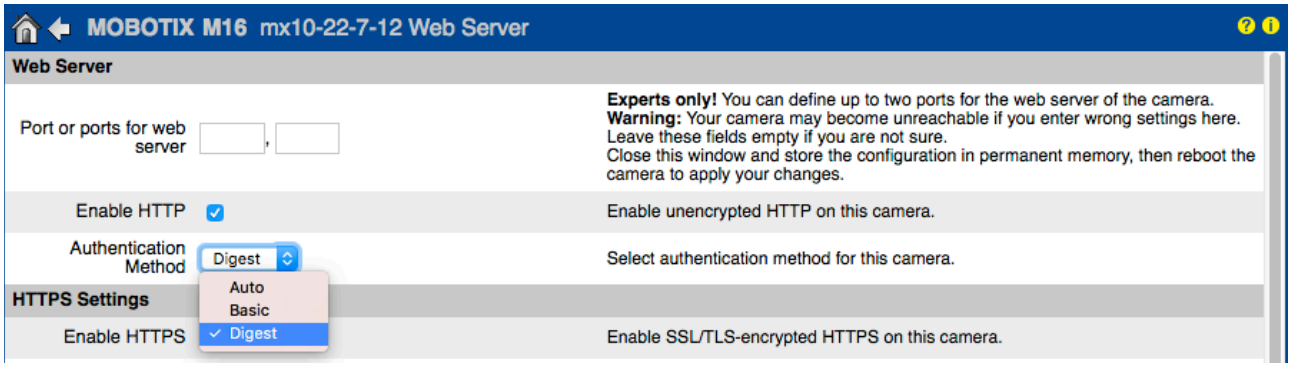
Admin Menu > Page Administration > Language and Start Page > Page Options



Using this parameter, you can prevent Web search engines, other automatic robots and web crawlers from scanning the contents of the camera's Web server. Usually, you would not want a search engine to index all the images and pages found on a camera. Make sure that you only allow crawling if you are aware of the additional security risks and the extra network traffic generated by the crawlers.

10. Enable Digest Authentication

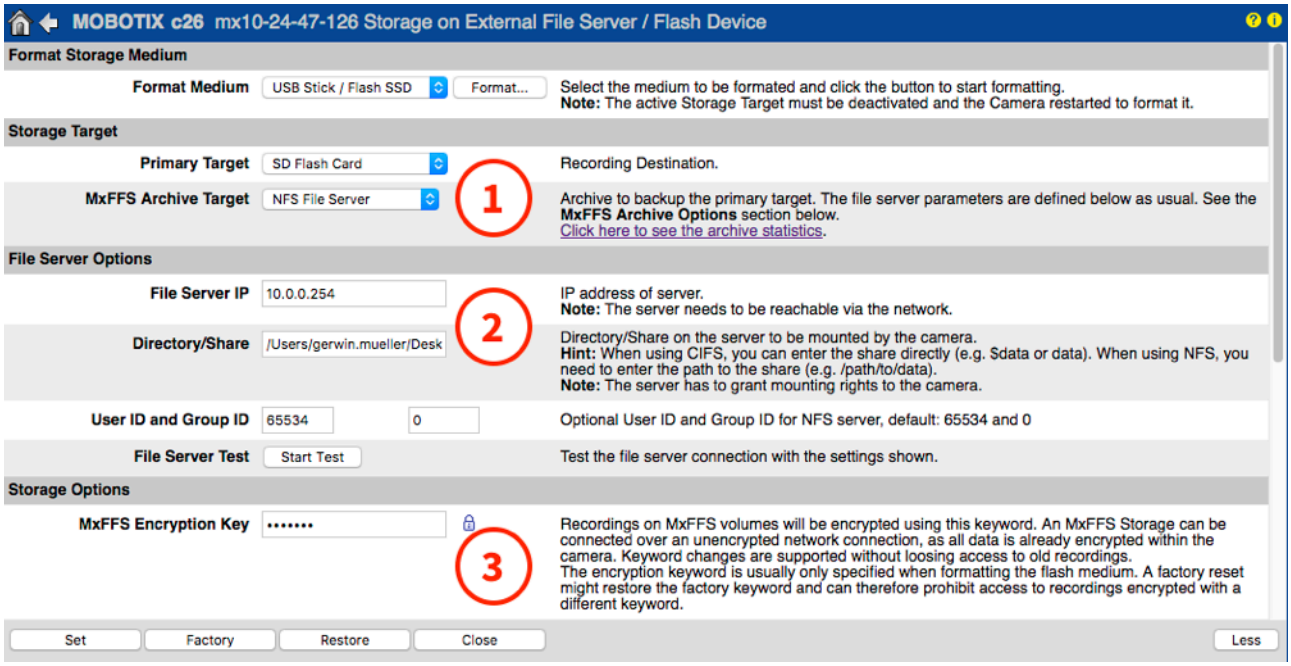
Admin Menu > Network Setup > Web Server (for experts) > Web Server



Digest access authentication is one of the agreed-upon methods a web server (i.e. MOBOTIX camera) can use to negotiate credentials, such as username or password, with a client (i.e. web browser). Wish Digest Authentication the password is never sent in the clear, and the username can be hashed.

11. Set an encryption key for recordings

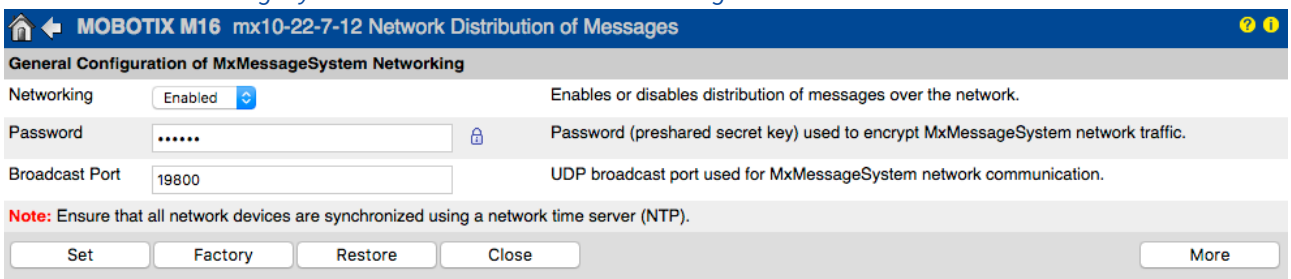
Admin Menu > Storage > Storage on External File Server / Flash Device



An encryption key can be set to encrypt the recordings stored onto the internal storage (microSD card / USB flash drive) as well as for the recording archived to the external File Server (SMB / NFS).

12. Change default password for MxMessage (if enabled)

Admin Menu > MxMessageSystem > Network Distribution of Messages



MxMessageSystem allows the transfer of messages between cameras over the network. A password (symmetrical key) of at least 6 characters, should be defined to encrypt the transferred messages.

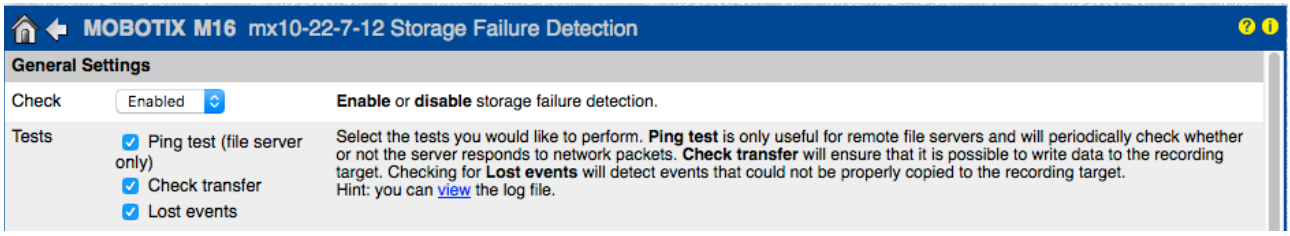
13. Enable Error Notification

Admin Menu > System Information > Error Notification

The Error Notification dialog provides several options for getting notifications (e-mail, IP notifications, VoIP calls, etc...) in case of reboot or errors that are detected within the different systems of the camera. This tool can help system administrators make sure that all the MOBOTIX cameras are functioning properly.

14. Enable Storage Failure Detection

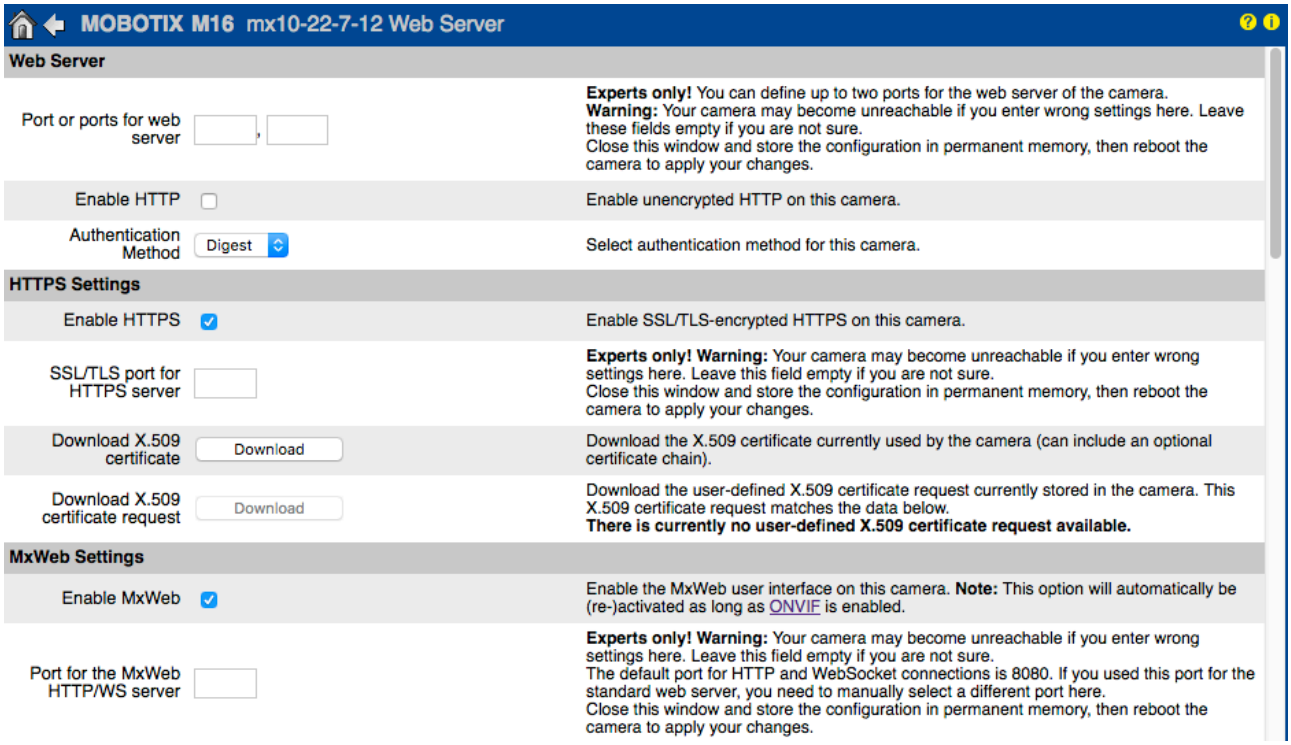
Admin Menu > Storage > Storage Failure Detection



Use the Storage Failure Detection dialog to configure tests that constantly monitor the external storage target (file server or Flash device) that the camera is using as an external ring buffer. The camera will actively monitor its storage target and reports problems with video recording using the notification methods specified in this dialog.

15. Change the default ports of the Web Server (for remote access)

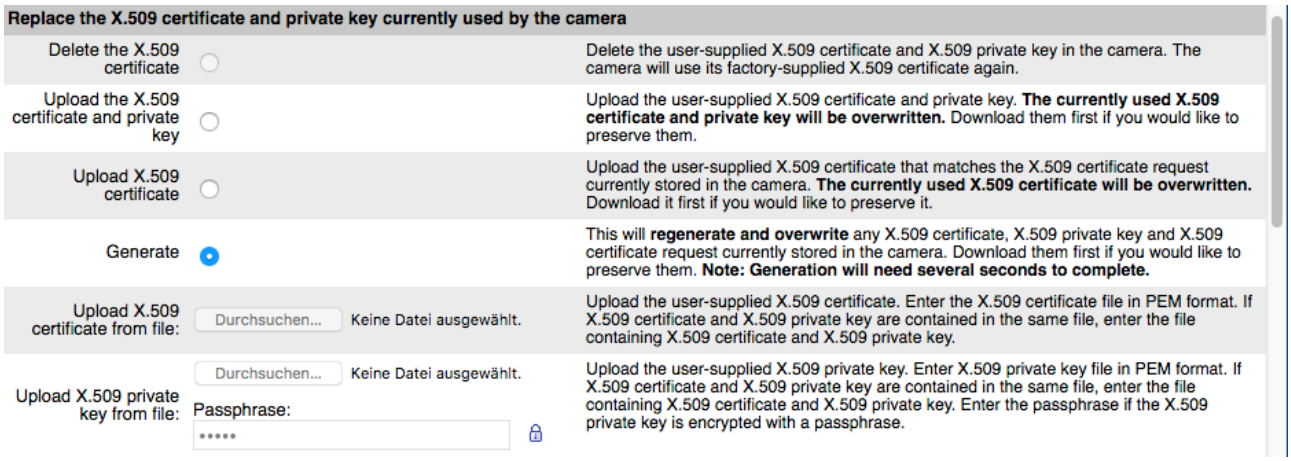
Admin Menu > Network Setup > Web Server (for experts)



Standard ports (80 TCP for HTTP and 443 TCP for HTTPS) are more prone to attacks. Replacing the default ports with custom ones can further increase the security of the camera.

16. Generate and load custom X.509 certificates

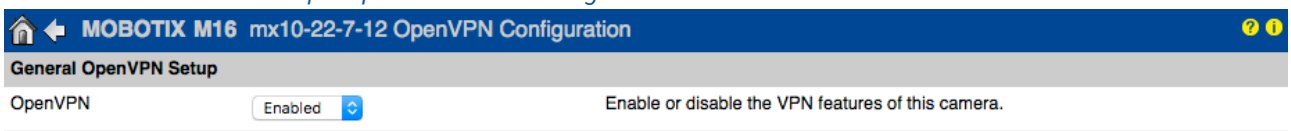
Admin Menu > Network Setup > Web Server (for experts)



Loading a custom certificate signed by a trusted CA (Certificate Authority) will ensure confidentiality and authenticity to all the connections established via HTTPS (SSL/TLS).

17. Configure OpenVPN client for remote connections

Admin Menu > Network Setup > OpenVPN Client Settings



To optimize the security in case of remote connections it's possible to leverage the embedded OpenVPN client to establish a VPN (Virtual Private Network) tunnel between the camera and the remote host.

Creating an OpenVPN connection requires a corresponding server, which provides secure access to the camera. To do so, you could run your own OpenVPN server or use the service from an OpenVPN provider.
For more information about OpenVPN, visit the *OpenVPN Community* website.

18. Avoid to expose the camera to the Internet unless strictly necessary

Remote access to the camera should granted consciously to reduce the risk of attacks. If a remote access is necessary, please make sure to observe the aforementioned rules to limit the possibility to connect to the intended users only.

19. Make use of VLANs to separate the CCTV network (enterprise security level)

In enterprise environments it's good practice to keep the CCTV network (IP cameras, NVR and VMS workstations) separated from the rest of the hosts to prevent unauthorized accesses and avoid traffic congestion.

20. Enable IEEE 802.1X (enterprise security level)

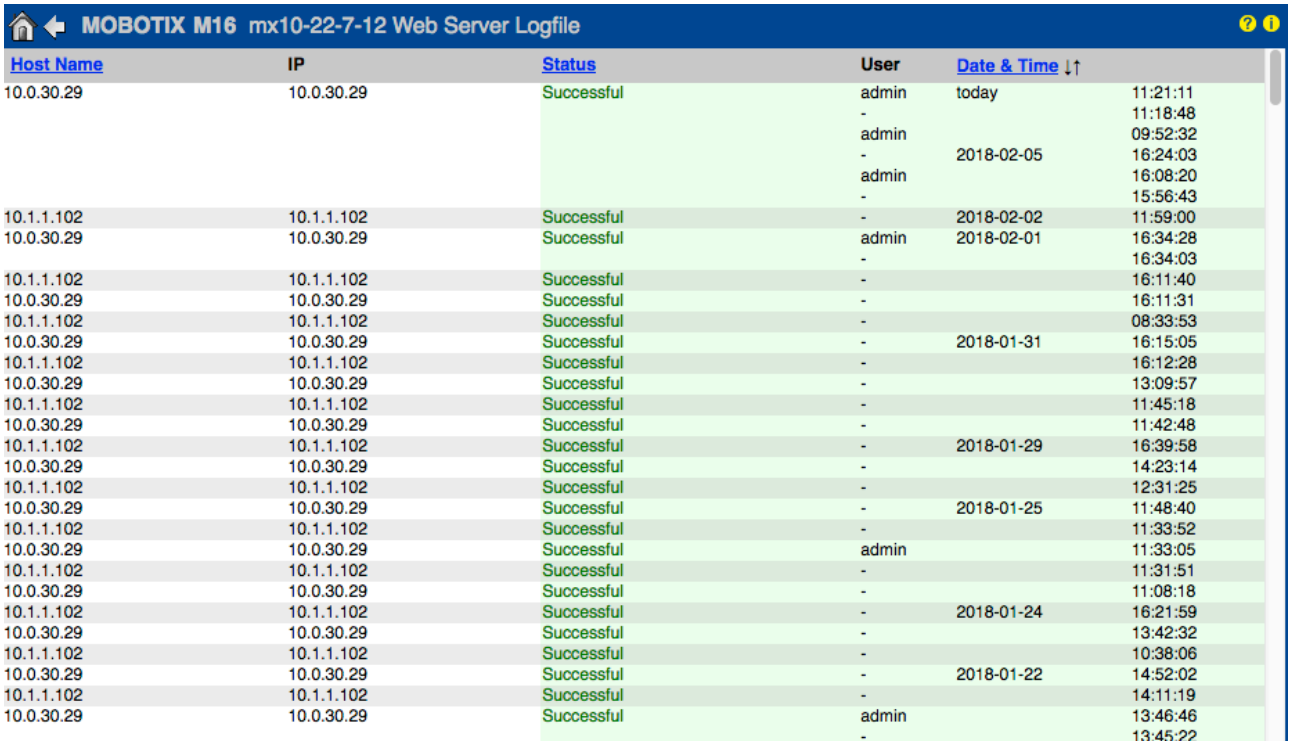
Admin Menu > Network Setup > Ethernet Interface (for experts) > IEEE 802.1X

This international standard is used for port-based network access control (NAC). This procedure requires that all network devices (i.e., also the MOBOTIX camera) need to authenticate themselves at the switch to obtain a network connection. Network devices without proper authentication will be rejected.

Ask your network administrator whether IEEE 802.1X is supported or required. Make sure that the switch to which the camera is connected (authenticator) has been configured accordingly. In general, the switch (authenticator) also needs an authentication server, such as a RADIUS server. The authentication procedure is controlled by the authentication server. Make sure that the camera and the authentication server always use the same procedure.

21. Check the Web Server log file on a regular basis

Admin Menu > Security > Web Server Logfile



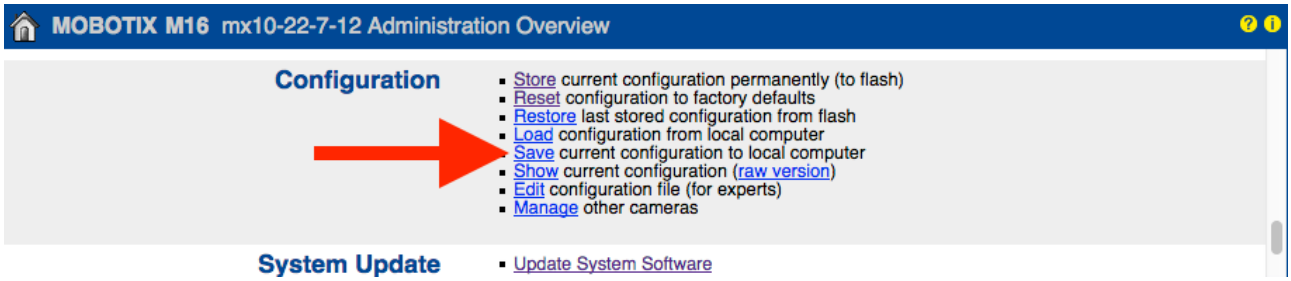
MOBOTIX M16 mx10-22-7-12 Web Server Logfile

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

The Web Server Logfile presents all access attempts and the date/time information with the corresponding status messages of the web server as well as the host name of the accessing computer. Unauthorized access attempts could be the the alarm bell for System Administrators that may want to revise the strength of their network.

22. Store backup configuration files in a safe place

Admin Menu > Configuration > Save current configuration to local computer



Although camera credentials (user passwords) are hashed within the camera configuration file, any configuration backup file should be kept in a safe place; moreover it's advisable to encrypt the file with a passphrase for further security.

Congratulations – your MOBOTIX camera is cyber secure now!

VMS Configuration (Video Management System)

1. Create User Accounts on the computer in use

2. Create User Accounts on MxMC

3. Limit rights to VMS users

4. Avoid using admin account to access cameras via MxMC

5. Enable the "Auto log-off"

Congratulations – your Video Management System is cyber secure now!

MOBOTIX

NAS Configuration (Network Attached Storage)

1. Place the device used to store the footage in a safe place

2. Set a strong password for the administrative account

3. Set a standard user account (limited rights) for MOBOTIX devices

4. Encrypt the volumes

5. Use a RAID level that ensures data redundancy

Congratulations – your Network Attached Storage System is cyber secure now!