



# Guida alla sicurezza informatica

Come proteggere il sistema  
di videosorveglianza MOBOTIX

Telecamera • VMS • NAS



### Informazioni sulla guida

Gli attacchi informatici contro i dispositivi hardware e software connessi a Internet costituiscono una crescente minaccia. Negli ultimi anni gli aggressori puntano soprattutto a sfruttare gli anelli più deboli del perimetro di sicurezza per accedere ad applicazioni critiche e a dati sensibili.

La tecnologia di videosorveglianza è divenuta una componente fondamentale della sicurezza che spesso include una rete aziendale condivisa: ne consegue che gli attacchi informatici diretti si focalizzano sempre più frequentemente sui dispositivi di videosorveglianza. A fronte di questa tendenza, MOBOTIX ha progettato una serie di **strumenti e funzionalità integrate** che permettono agli esperti di sicurezza IT di configurare ciascun dispositivo come una parte di una strategia a più livelli per la sicurezza informatica.

Questi strumenti, qualora utilizzati in combinazione con altri componenti per la sicurezza, come firewall e segmentazione di rete, sono in grado di ridurre la superficie di attacco dei dispositivi MOBOTIX, offrendo a utenti e amministratori una politica sicura per gli accessi.

La guida fornisce consigli pratici sulle modalità di configurazione dei dispositivi MOBOTIX per ottenere la massima protezione dagli attacchi informatici, oltre a informazioni relative alla creazione di un'infrastruttura di videosorveglianza sicura.

**Nota:** il presente documento intende fornire all'amministratore una panoramica completa di tutte le misure destinate a proteggere il sistema MOBOTIX. Per quanto riguarda la singola applicazione, anche al fine di evitare inutili riconfigurazioni, potrebbe non essere necessario eseguire tutte le procedure illustrate in questa guida.

**Informazioni generali:** MOBOTIX non si assume alcuna responsabilità per errori tecnici, di stampa oppure omissioni.

**Copyright:** tutti i diritti riservati. MOBOTIX, il logo di MOBOTIX AG e MxAnalytics sono marchi commerciali di MOBOTIX AG registrati nell'Unione Europea, negli Stati Uniti e in altri paesi. © MOBOTIX AG 2024

## Configurazione della telecamera



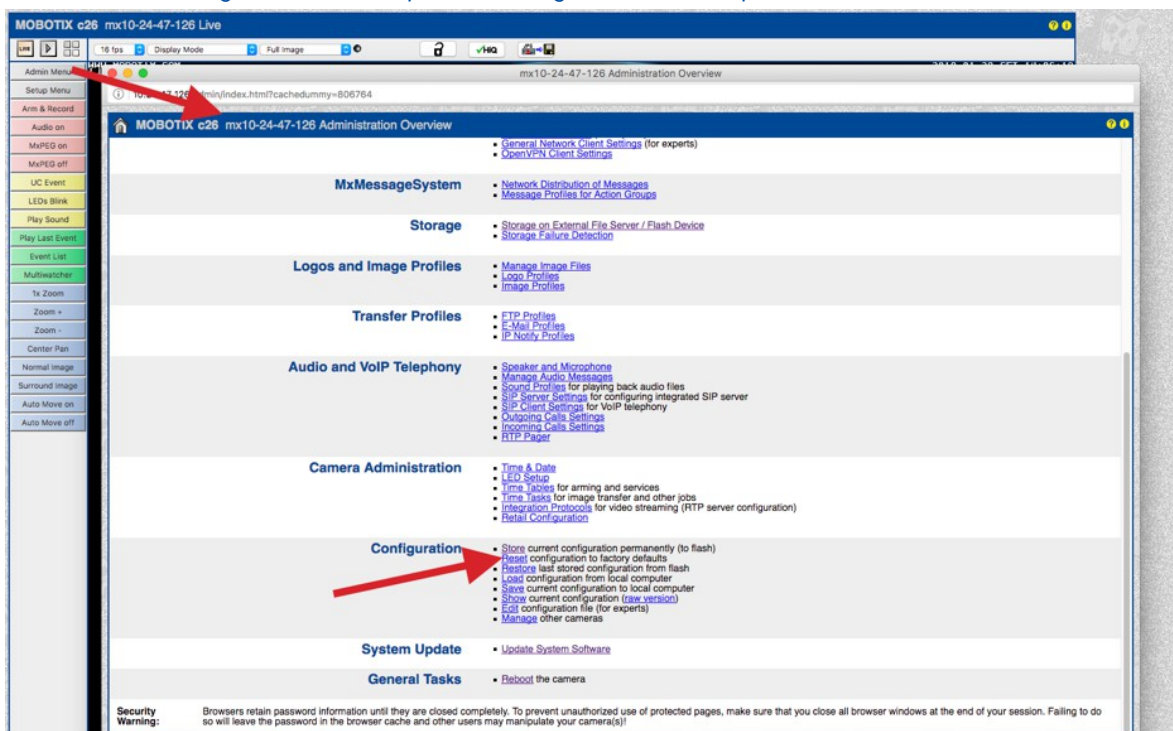
### 1. Mantenere aggiornato il firmware delle telecamere

Il firmware MOBOTIX può essere scaricato gratuitamente dal nostro sito web: [www.mobotix.com](http://www.mobotix.com) > [Supporto](#) > [Download Center](#)

Per avere istruzioni su come proseguire, consultare la guida compatta disponibile in: [www.mobotix.com](http://www.mobotix.com) > [Supporto](#) > [Download Center](#) > [Documentazione](#) > [Opuscoli e Istruzioni](#) > [Istruzioni compatte](#) > [Mx CG FirmwareUpdate.pdf](#)

### 2. Ripristinare la configurazione ai valori predefiniti impostati in fabbrica

[Admin Menu](#) > [Configurazione](#) > [Reimposta la configurazione alle impostazioni di default](#)



### 3. Modificare la password amministratore predefinita

Admin Menu > Sicurezza > Utenti e password

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

È sempre necessario cambiare la password predefinita "meinsm" la prima volta che si richiama la telecamera.

Una volta terminato di configurare utenti, password e gruppi, memorizzare le impostazioni nella memoria permanente della telecamera. In caso contrario, la configurazione modificata verrà utilizzata solamente fino al riavvio successivo della telecamera. Selezionare il pulsante Close posto nella parte inferiore della finestra di dialogo che richiede automaticamente se si desidera memorizzare la nuova configurazione nella memoria permanente della telecamera.

Conservare le informazioni sulle password in un luogo sicuro. Prestare particolare attenzione a conservare la password di almeno un utente del gruppo admin. Senza la password non è più possibile accedere alla telecamera come amministratore e non vi è alcuna possibilità di aggirare la procedura. È impossibile anche richiamare la password da una configurazione salvata in modo permanente.

#### Come creare una password sicura:

- Usare 8 o più caratteri (fino a 99)
- Usare almeno un carattere maiuscolo
- Usare almeno un carattere minuscolo
- Usare almeno un numero
- Usare almeno un carattere speciale: ! " # \$ % & ' ( ) \* + , - . / : ; < = > ? @ [ \ ] ^ \_ ` { | } ~
- Evitare parole e date comuni

**Politica di reset delle password:** Se la password amministratore non è più disponibile, la telecamera deve essere reimpostata tramite MOBOTIX a pagamento!

### 4. Creare diversi gruppi di utenti con diversi diritti utente

Admin Menu > Sicurezza > Utenti e password

In linea generale, non tutti gli utenti necessitano degli stessi diritti. È possibile creare fino a 25 diversi gruppi di utenti nella pagina Admin Menu > Group Access Control List.

### 5. Creare utenti differenti e assegnarli ai gruppi corretti

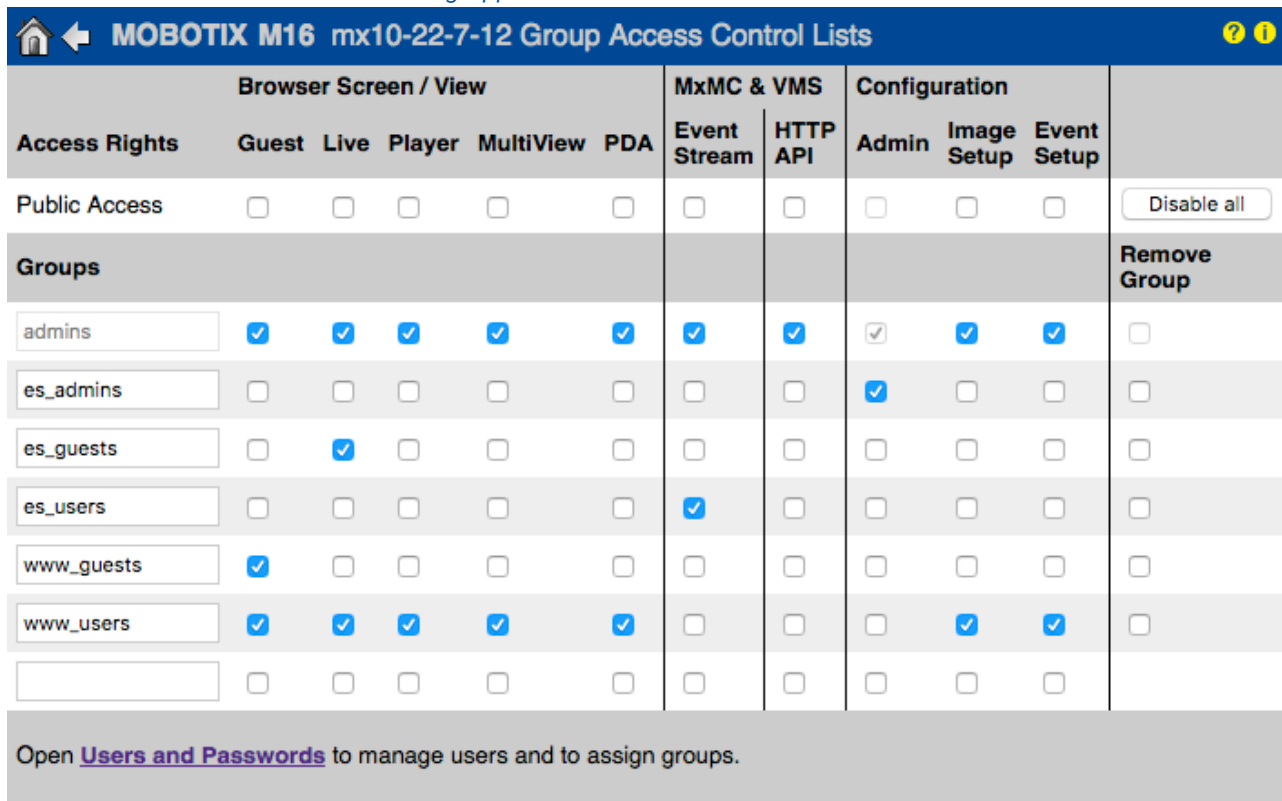
Admin Menu > Sicurezza > Utenti e password

Si consiglia di creare sempre un utente per ciascuna persona che disponga dell'autorizzazione per accedere alla telecamera. È possibile creare fino a 100 utenti. Le operazioni eseguite dagli utenti autorizzati sono tracciate nel file di registro del server Web: ciò contribuisce a definire "chi ha fatto cosa" in caso di controversie.

Fare riferimento alle indicazioni precedenti sulla creazione di password sicure.

## 6. Disabilitare l'accesso pubblico

Admin Menu > Sicurezza > Elenchi ACL di gruppo



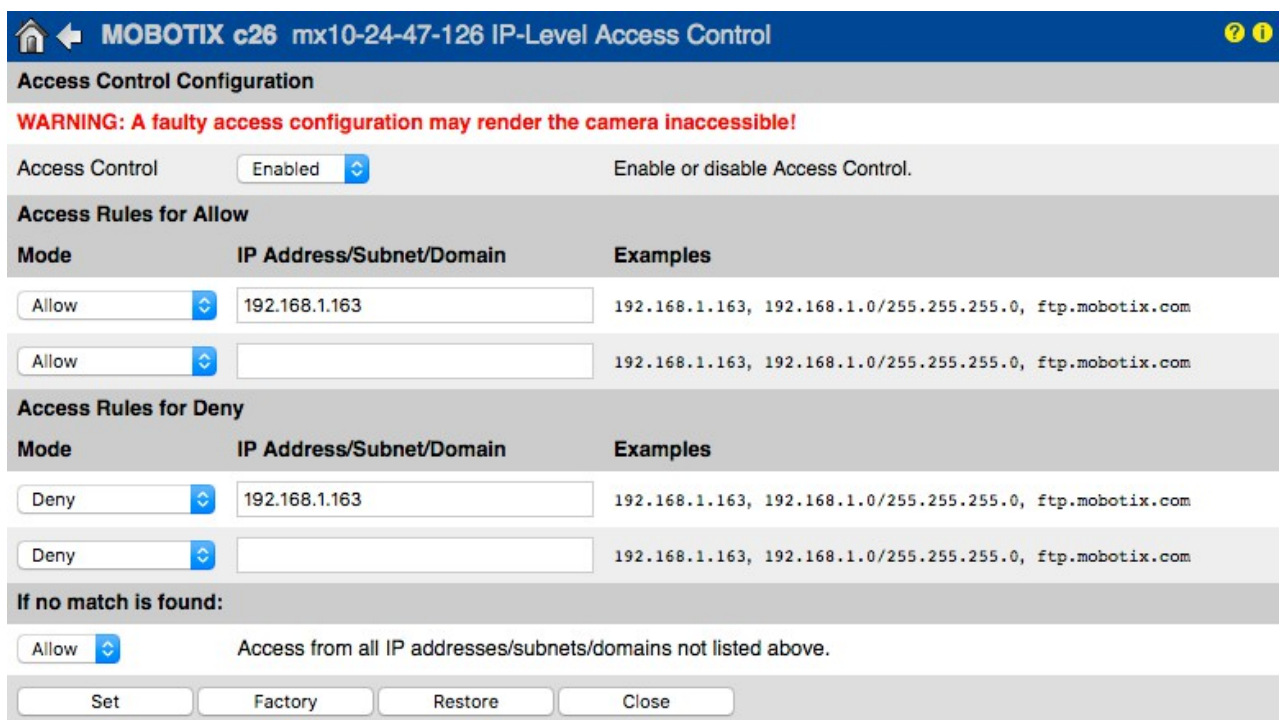
Access Rights	Browser Screen / View					MxMC & VMS		Configuration			Remove Group
	Guest	Live	Player	MultiView	PDA	Event Stream	HTTP API	Admin	Image Setup	Event Setup	
Public Access	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Disable all
<b>Groups</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"/>	<input type="checkbox"/>

Open [Users and Passwords](#) to manage users and to assign groups.

L'accesso pubblico, se attivato, consente di accedere a specifiche funzionalità della telecamera senza autenticazione. Si consiglia di disattivare l'accesso pubblico al fine di evitare che utenti non autorizzati possano visualizzare il video live e le registrazioni della telecamera o persino controllare la telecamera (ad esempio, modificare la configurazione o eseguire operazioni).

## 7. Attivare l'elenco per il controllo degli accessi IP

Admin Menu > Sicurezza > Controllo dell'accesso a livello IP



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

Access Control:  Enabled  Disabled  Disabled

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  Deny  Deny

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

Set Factory Restore Close

La finestra di dialogo Access Control permette di gestire indirizzi IP, le sottoreti e i nomi di dominio a cui è consentito ovvero non consentito l'accesso alla telecamera. La possibilità di controllare gli accessi alla telecamera sfrutta il livello del protocollo IP, non dipende dall'autenticazione utente basata su password a livello del protocollo HTTP e sostituisce l'autenticazione tramite password. Qualora un computer non disponga dell'accesso alla telecamera a livello IP, non sarà possibile accedervi da quel computer. Se invece un computer dispone dell'accesso alla telecamera a livello IP, la fase successiva prevede l'autenticazione utente basata su password, come descritto nella finestra di dialogo Users and Passwords.

### 8. Attivare la funzione Intrusion Detection con notifica e blocco dell'indirizzo IP dell'aggressore

*Admin Menu > Impostazione della rete > Server web (per utenti esperti) > Impostazioni della rilevazione intrusioni*

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> Send image by e-mail. ( <a href="#">E-Mail Profiles</a> )
IP Notify <input type="text" value="Off"/>	<b>IP Notify Profile:</b> Notification by network message using the TCP/IP protocol. ( <a href="#">IP Notify Profiles</a> )

Questa funzionalità fornisce un meccanismo di difesa automatico contro gli attacchi. Se un aggressore tenta di accedere alla telecamera sfruttando la "forza bruta" per indovinare i nomi utente e le password, la telecamera è in grado di inviare un allarme e bloccare automaticamente l'indirizzo IP dell'aggressore dopo un determinato numero di tentativi di accesso falliti.

### 9. Verificare che sia attivo il divieto di Web Crawling

*Admin Menu > Amministrazione delle pagine > Pagina iniziale e di selezione lingua > Opzioni pagina*

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 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 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 <a href="#">ActiveX</a> , 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.

Mediante questo parametro è possibile evitare che i motori di ricerca sul Web, altri robot automatici e i web crawler possano scansionare i contenuti del server Web della telecamera. Di norma nessuno vuole consentire a un motore di ricerca di indicizzare tutte le immagini e le pagine rilevate in una telecamera. Il crawling dovrebbe essere abilitato solamente se si è consapevoli dei rischi aggiuntivi che comporta per la sicurezza e del maggior traffico di rete generato dai crawler.

## 10. Attivare l'autenticazione digest

Admin Menu > Impostazione della rete > Server web (per utenti esperti) > Server Web

**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'autenticazione dell'accesso digest è uno dei metodi concordati che un server web (ad esempio una telecamera MOBOTIX) può utilizzare per negoziare le credenziali, quali username e password, con un client (ad esempio un browser web). Con l'autenticazione digest, la password non viene mai inviata in chiaro e il nome utente può essere gestito con hashing.

## 11. Impostare una chiave crittografica per le registrazioni

Admin Menu > Memorizzazione immagini > Memorizzazione su file server esterno / dispositivo Flash

**Format Storage Medium**

Format Medium **USB Stick / Flash SSD**  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** **1** 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** **2** IP address of server.  
**Note:** The server needs to be reachable via the network.

Directory/Share **/Users/gerwin.mueller/Desk** **2** Directory/Share on the server to be mounted by the camera.  
**Hint:** When using CIFS, you can enter the share directly (e.g. \$data 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  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 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.

È possibile impostare una chiave crittografica per criptare le registrazioni memorizzate nella memoria interna (scheda microSD / unità flash USB) e le registrazioni archiviate nel file server esterno (SMB / NFS).

## 12. Change default password for MxMessage (if enabled)

Admin Menu > MxMessageSystem > Distribuzione dei messaggi nella rete

**MOBOTIX M16 mx10-22-7-12 Network Distribution of Messages**

**General Configuration of MxMessageSystem Networking**

Networking  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 network time server (NTP).

MxMessageSystem permette di trasferire dei messaggi tra diverse telecamere tramite la rete. È necessario definire una password (chiave simmetrica) di almeno 6 caratteri per criptare i messaggi trasferiti.

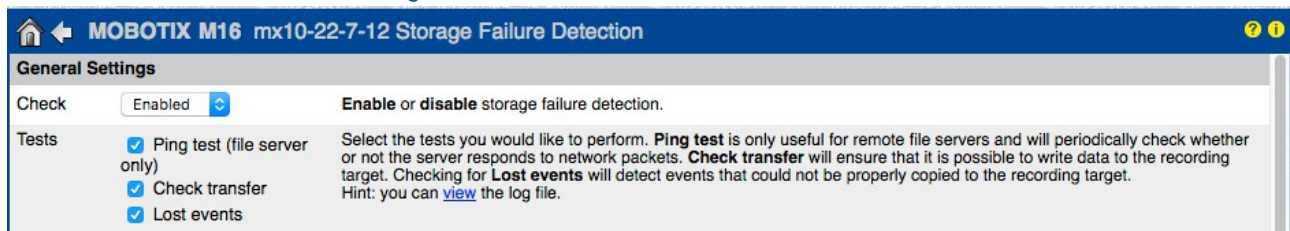
### 13. Abilitare la funzione Storage Failure Detection

*Admin Menu > Informazioni di sistema > Notifica degli errori*

La finestra di dialogo Error Notification offre svariate opzioni per la ricezione di notifiche (e-mail, notifiche IP, chiamate VoIP, ecc.) in caso di riavvio o qualora vengano rilevati errori all'interno dei diversi sistemi della telecamera. Questa funzionalità aiuta gli amministratori di sistema a garantire il funzionamento corretto di tutte le telecamere MOBOTIX.

### 14. Enable Storage Failure Detection

*Admin Menu > Memorizzazione immagini > Rilevamento errore di memorizzazione*

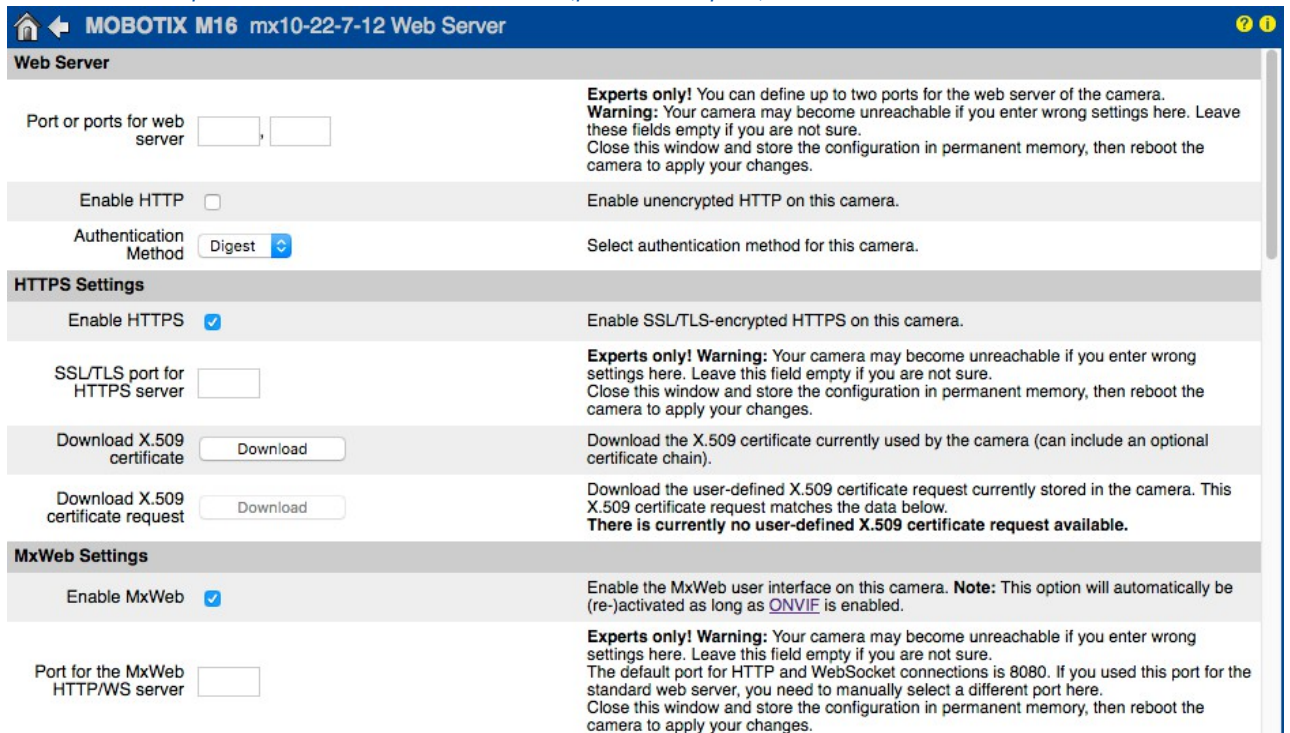


General Settings	
Check	Enabled <input type="button" value="v"/> Enable or disable storage failure detection.
Tests	<input checked="" type="checkbox"/> Ping test (file server only) Select the tests you would like to perform. <b>Ping test</b> is only useful for remote file servers and will periodically check whether 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 <a href="#">view</a> the log file. <input checked="" type="checkbox"/> Check transfer <input checked="" type="checkbox"/> Lost events

La finestra di dialogo Storage Failure Detection consente di configurare i test che controllano costantemente la destinazione dell'archiviazione esterna (il file server o il dispositivo Flash) utilizzata dalla telecamera come ring buffer esterno. La telecamera controllerà attivamente la destinazione di archiviazione segnalando eventuali problemi con la registrazione video mediante i sistemi di notifica definiti in questa finestra di dialogo.

### 15. Modificare le porte predefinite del server web (per l'accesso in remoto)

*Admin Menu > Impostazione della rete > Server web (per utenti esperti)*



Web Server	
Port or ports for web server	<input type="text"/> <input type="text"/> <b>Experts only!</b> You can define up to two ports for the web server of the camera. <b>Warning:</b> 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	<input type="checkbox"/> Enable unencrypted HTTP on this camera.
Authentication Method	Digest <input type="button" value="v"/> Select authentication method for this camera.
HTTPS Settings	
Enable HTTPS	<input checked="" type="checkbox"/> Enable SSL/TLS-encrypted HTTPS on this camera.
SSL/TLS port for HTTPS server	<input type="text"/> <b>Experts only! Warning:</b> 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	<input type="button" value="Download"/> Download the X.509 certificate currently used by the camera (can include an optional certificate chain).
Download X.509 certificate request	<input type="button" value="Download"/> Download the user-defined X.509 certificate request currently stored in the camera. This X.509 certificate request matches the data below. <b>There is currently no user-defined X.509 certificate request available.</b>
MxWeb Settings	
Enable MxWeb	<input checked="" type="checkbox"/> Enable the MxWeb user interface on this camera. <b>Note:</b> This option will automatically be (re-)activated as long as <b>ONVIF</b> is enabled.
Port for the MxWeb HTTP/WS server	<input type="text"/> <b>Experts only! Warning:</b> 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 the 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.

Le porte standard (80 TCP per HTTP e 443 TCP per HTTPS) sono più soggette agli attacchi. Sostituire le porte predefinite con porte personalizzate può incrementare ulteriormente il livello di sicurezza della telecamera.



### 16. Generare e caricare i certificati X.509 personalizzati

*Admin Menu > Impostazione della rete > Server web (per utenti esperti)*

**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="text" 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="text" value="Durchsuchen..."/> Keine Datei ausgewählt. Passphrase: <input type="password" value="*****"/>	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.

Caricare un certificato personalizzato e firmato da una CA (Certificate Authority) garantisce riservatezza e autenticità a tutte le connessioni stabilite tramite HTTPS (SSL/TLS).

### 17. Configurare il client OpenVPN per le connessioni remote

*Admin Menu > Impostazione della rete > Impostazioni client OpenVPN*

**MOBOTIX M16 mx10-22-7-12 OpenVPN Configuration**

**General OpenVPN Setup**

OpenVPN  Enable or disable the VPN features of this camera.

Per ottimizzare la sicurezza in caso di connessioni remote, è possibile sfruttare il client OpenVPN integrato per generare un tunnel VPN (Virtual Private Network) tra la telecamera e l'host remoto.

La creazione di una connessione OpenVPN richiede un server corrispondente che fornisce un accesso sicuro alla telecamera. A tal fine, è possibile utilizzare il proprio server OpenVPN oppure ricorrere al servizio esterno di un provider OpenVPN. Per ulteriori informazioni su OpenVPN, visitare il sito web di [OpenVPN Community](https://openvpn.com).

### 18. Evitare di connettere la telecamera a Internet se non è strettamente necessario

L'accesso remoto alla telecamera deve essere concesso con cautela al fine di ridurre il rischio di attacchi. Qualora si renda necessario usare l'accesso remoto, accertarsi di rispettare le regole illustrate precedentemente così da limitare la possibilità di connettersi ai soli utenti previsti.

### 19. Usare reti VLAN per separare la rete CCTV (livello di sicurezza aziendale)

Negli ambienti aziendali è buona norma tenere separata la rete CCTV (telecamere IP, NVR e workstation VMS) dal resto degli host così da prevenire gli accessi indesiderati ed evitare congestioni del traffico di rete.

### 20. Attivare IEEE 802.1X (livello di sicurezza aziendale)

*Admin Menu > Impostazione della rete > Interfaccia Ethernet (per utenti esperti) > IEEE 802.1X*

Questo standard internazionale è usato per il controllo degli accessi sulla rete (NAC) basato su porte. La procedura prevede che tutti i dispositivi di rete (quindi anche la telecamera MOBOTIX) debbano autenticarsi allo switch per ottenere una connessione di rete. I dispositivi di rete privi di un'adeguata autenticazione verranno rifiutati.

Chiedere all'amministratore di rete se il servizio IEEE 802.1X è supportato o necessario. Verificare che lo switch a cui è connessa la telecamera (autenticatore) sia stato configurato adeguatamente. In generale, lo switch (autenticatore) richiede anche un server di autenticazione, ad esempio un server RADIUS. La procedura di autenticazione è controllata dal server di autenticazione. Verificare che la telecamera e il server di autenticazione utilizzino sempre la medesima procedura.

## 21. Verificare regolarmente il file di registro del server Web

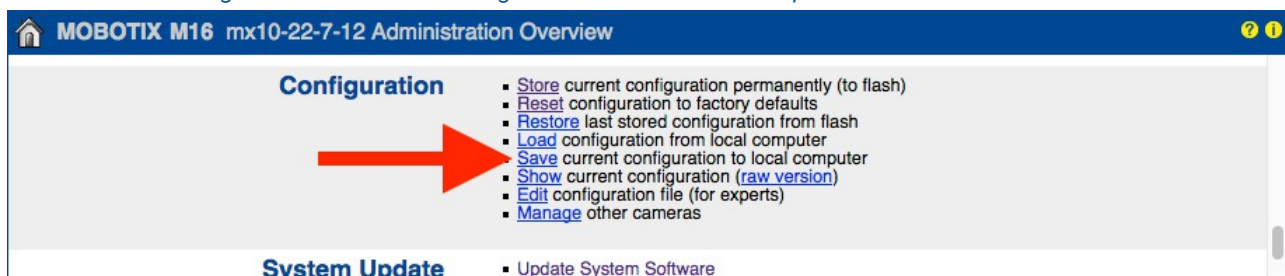
Admin Menu > Sicurezza > File log del server web

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	2018-02-05 09:52:32
			-	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

Il file di registro del server Web include tutti i tentativi di accesso, data e ora dell'accesso e i corrispondenti messaggi di stato del server Web, oltre al nome host dei PC che effettuano l'accesso. I tentativi di accesso non autorizzati potrebbero fungere da campanello d'allarme e segnalare agli amministratori di sistema che è necessario controllare solidità della rete.

## 22. Archiviare i file di configurazione di backup in un luogo sicuro

Admin Menu > Configurazione > Salva la configurazione corrente sul computer locale



Nonostante le credenziali della telecamera (password utente) siano dotate di hashing nel file di configurazione, qualsiasi file di configurazione di backup deve essere archiviato in un luogo sicuro. Inoltre, si consiglia di criptare il file con una passphrase per incrementare la sicurezza.

Complimenti, ora la telecamera MOBOTIX è protetta contro gli attacchi informatici!

## Configurazione VMS (sistema di gestione video)



1. Creare account utente nel computer in uso
2. Creare account utente su MxMC
3. Limitare i diritti agli utenti VMS
4. Evitare di usare account admin per accedere alle telecamere tramite MxMC
5. Abilitare la funzione “Auto log-off”

Complimenti, ora il sistema di gestione video è protetto contro gli attacchi informatici!

## Configurazione NAS (Network Attached Storage)



1. Tenere il dispositivo usato per memorizzare i filmati in un luogo sicuro
2. Impostare una password sicura per l'account amministratore
3. Impostare un account utente standard (diritti limitati) per i dispositivi MOBOTIX
4. Crittografare i volumi
5. Usare un livello RAID che garantisca la ridondanza dei dati

Complimenti, ora il sistema NAS è protetto contro gli attacchi informatici!