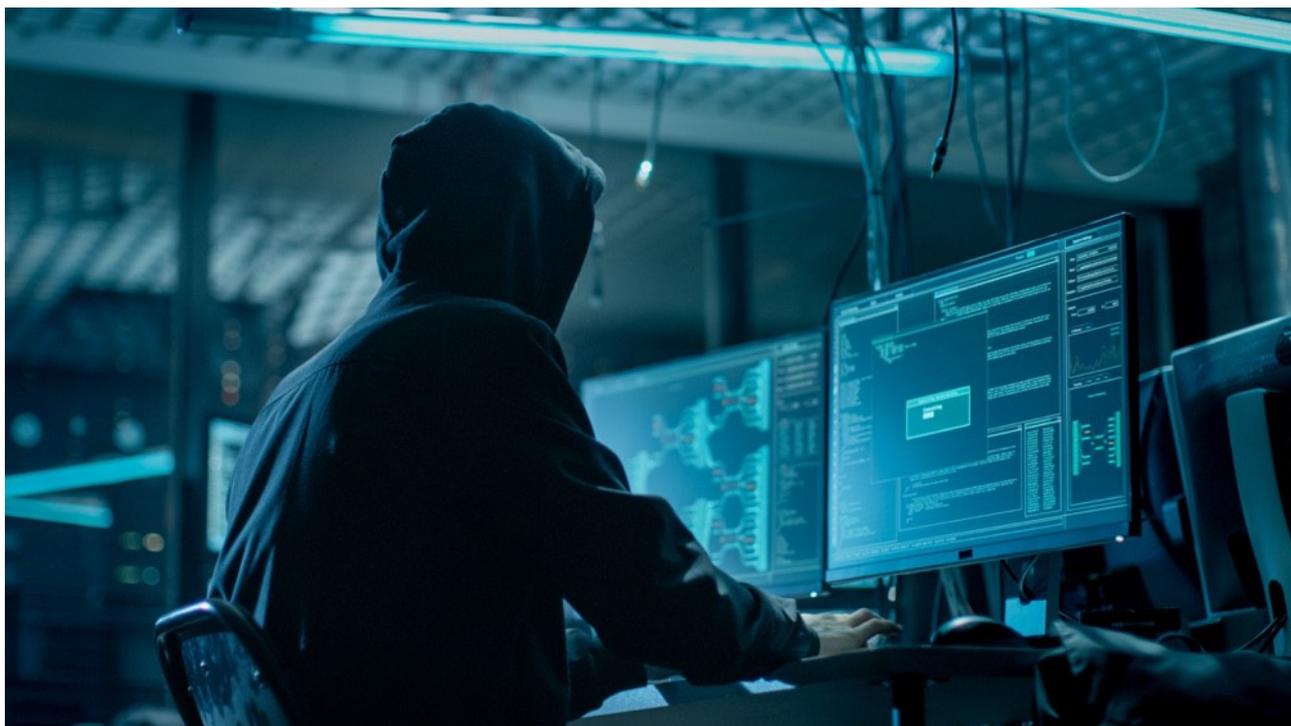




Guida alla protezione informatica

Come si indurisce
Il sistema video MOBOTIX
Telecamera - VMS - NAS



Informazioni su questa guida

Gli attacchi informatici contro software e hardware connessi a Internet sono un problema crescente. Negli ultimi anni, gli aggressori si sono sempre più concentrati sullo sfruttamento degli anelli più deboli all'interno di un perimetro di sicurezza per ottenere l'accesso ad applicazioni critiche e dati sensibili.

Con la tecnologia di videosorveglianza come parte vitale della sicurezza di un sito che spesso abita una rete aziendale condivisa, i dispositivi di videosorveglianza stanno diventando sempre più l'obiettivo di attacchi informatici diretti.

Riconoscendo questa tendenza emergente, MOBOTIX ha sviluppato una serie di **strumenti e funzioni integrate** che consentono agli amministratori della sicurezza IT di configurare ogni dispositivo come parte di un approccio multilivello alla sicurezza informatica.

Questi strumenti, se utilizzati insieme ad altri elementi di sicurezza come i firewall e la segmentazione della rete, possono ridurre la superficie di attacco presentata dai dispositivi MOBOTIX nell'ambito di una politica di accesso sicuro per amministratori e utenti.

Questa guida fornisce consigli pratici su come configurare i dispositivi MOBOTIX per garantire la massima protezione contro gli attacchi informatici, oltre a indicazioni sulle best practice per la realizzazione di un'infrastruttura di videosorveglianza sicura.

Nota bene: questo documento ha lo scopo di fornire all'amministratore responsabile una panoramica completa di tutte le misure possibili per la protezione del sistema MOBOTIX. In base alle singole applicazioni e per evitare riconfigurazioni, potrebbe non essere utile eseguire ogni singola procedura spiegata in questa guida.

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

Avvertenze sul copyright: Tutti i diritti riservati. MOBOTIX, il logo di MOBOTIX AG e MxAnalytics sono marchi registrati di MOBOTIX AG nell'Unione Europea, negli USA 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 > [Supporto](#) > [Download Center](#) Non sapete come procedere? Consultate questa guida compatta: www.mobotix.com > [Supporto](#) > [Download Center](#) > [Documentazione](#) > [Brochure e guide](#) > [Guide compatte](#) > [Mx CG FirmwareUpdate.pdf](#)

2. Ripristino della configurazione ai valori di fabbrica

[Menu Amministrazione](#) > [Configurazione](#) > [Ripristino della configurazione di fabbrica](#)

The screenshot shows the MOBOTIX web interface for a device labeled 'M1S mx10-42-1-27 Administration Overview'. The left sidebar contains a list of menu items, with 'Configuration' selected and highlighted in blue. The main content area displays the 'Configuration' menu with the following options:

- [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 ([Text Edit](#))

A red arrow points to the 'Reset configuration to factory defaults' option. Below the menu is a 'Maintenance' section with a checkmark icon. At the bottom, a yellow warning box contains the following text:

Security Warning: Browsers retain password information until they are closed completely. To prevent unauthorized use of protected pages, make sure that you close all browser windows at the end of your session. Failing to do so will leave the password in the browser cache and other users may manipulate your camera(s)!

3. Modificare la password di amministrazione predefinita

Menu Amministrazione > Sicurezza > Utenti e password

MOBOTIX



M1S mx10-42-1-27 Users and Passwords

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

Scheduled access control by

Supervisor Activated

Super PIN (8 to 16 digits)

The admin user still uses the factory default password. You must change the password of the administrative account for security reasons!

Caution: Some areas of the camera are still publicly accessible.

Activate the checkbox below and click **Set** to prevent access to the camera without proper user authentication.

Disable public access

Open [Group Access Control Lists](#) to manage the group definitions and to set the group access rights.

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

Una volta terminata la configurazione di utenti, password e gruppi, è necessario salvare sempre le impostazioni nella memoria permanente della telecamera. In caso contrario, la configurazione modificata sarà utilizzata solo fino al successivo riavvio della telecamera. Utilizzare il pulsante Chiudi alla fine della finestra di dialogo, che chiederà automaticamente di salvare la configurazione della telecamera nella memoria permanente della stessa.

Assicurarsi di conservare le informazioni sulla password in un luogo sicuro. È necessario prestare particolare attenzione a conservare la password di almeno un utente del gruppo admins. Senza la password, l'accesso amministrativo alla telecamera non è più possibile e non c'è possibilità di eludere la password. È altresì impossibile recuperare la password da una configurazione salvata in modo permanente.

Come creare una password forte:

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

Politica di reimpostazione della password:

Se la password dell'amministratore non è più disponibile, la telecamera deve essere resettata tramite MOBOTIX a

4. Creare gruppi di utenti diversi con diritti d'uso diversi.

Menu Amministrazione > Sicurezza > Utenti e password

In generale, non tutti gli utenti hanno bisogno degli stessi diritti. È possibile creare fino a 25 gruppi di utenti diversi dalla pagina Menu Amministrazione > Elenco di controllo dell'accesso ai gruppi.

Guida alla protezione

5. Creare utenti diversi e assegnarli ai gruppi giusti

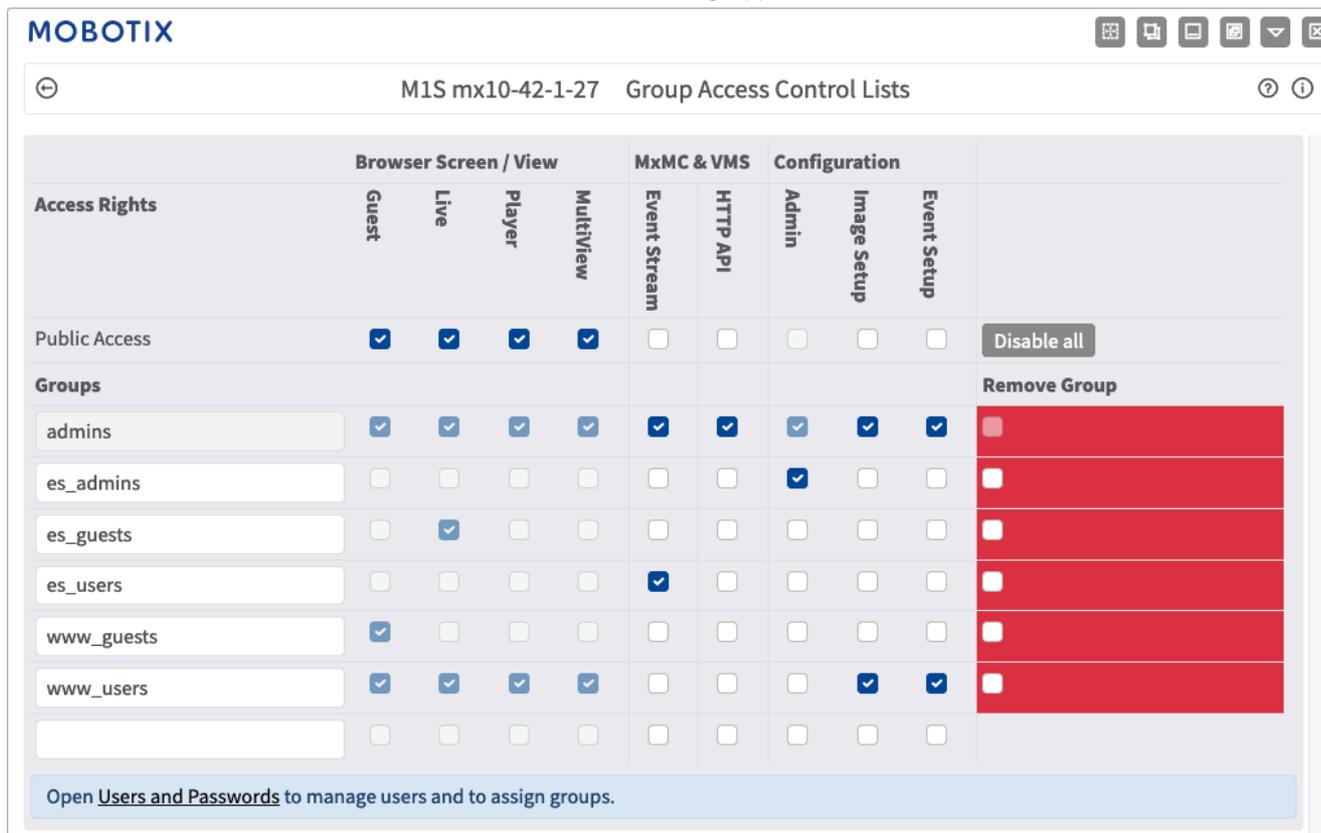
Menu Amministrazione > Sicurezza > Utenti e password

È sempre consigliabile creare un utente per ogni persona autorizzata ad accedere alla telecamera. È possibile creare fino a 100 utenti. Le azioni eseguite dagli utenti autorizzati sono tracciate nel file di registro del server Web; questo aiuta a determinare "chi ha fatto cosa" in caso di controversie.

Fare riferimento alla descrizione precedente per creare password forti.

6. Disattivare l'accesso pubblico

Menu Amministrazione > Sicurezza > Liste di controllo accesso di gruppo



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

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

L'Accesso pubblico consente, se abilitato, di accedere a risorse specifiche della telecamera senza autenticazione. Si consiglia vivamente di disabilitare l'Accesso pubblico per evitare che utenti non autorizzati possano visualizzare il flusso live della telecamera, le registrazioni o persino controllare la telecamera (ad esempio, modificare la configurazione o eseguire azioni). Ulteriori opzioni di impostazione in "Altro".

7. Abilitare la lista di controllo degli accessi IP

Menu Amministrazione > Sicurezza > Controllo accesso a livello IP

MOBOTIX 🏠 📄 📄 📄 📄 📄

M1S mx10-42-1-27 IP-Level Access Control ? ⓘ + ☰

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

Access Control Configuration 🗨

Access Control Enable or disable Access Control.

Strict Mode Enable or disable Strict Mode.

Access Rules for Allow 🗨

Mode	IP Address/Subnet/Domain	Examples
<input type="text" value="Allow"/>	<input type="text"/>	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
<input type="text" value="Deny"/>	<input type="text"/>	192.168.1.163, 192.168.1.0/255.255.255.0, ftp.mobotix.com

If no match is found: 🗨

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

La finestra di dialogo Controllo accesso consente di gestire gli indirizzi IP, le sottoreti e i nomi di dominio a cui è consentito o impedito l'accesso alla telecamera. Questa possibilità di controllare l'accesso alla telecamera utilizza il livello di protocollo IP, è indipendente dall'autenticazione utente basata su password a livello di protocollo HTTP e sostituisce l'autenticazione basata su password. Se un computer non ha accesso a livello IP alla telecamera, non è possibile raggiungere la telecamera da quel computer. Se un computer ha accesso a livello IP alla telecamera, l'autenticazione utente basata su password segue il passo successivo, come specificato nella finestra di dialogo Utenti e password.

8. Abilitare il rilevamento delle intrusioni con notifica e blocco dell'indirizzo IP offending.

Menu Amministrazione > Configurazione della rete > Server Web (per gli esperti) > Impostazioni di rilevamento delle intrusioni

MOBOTIX

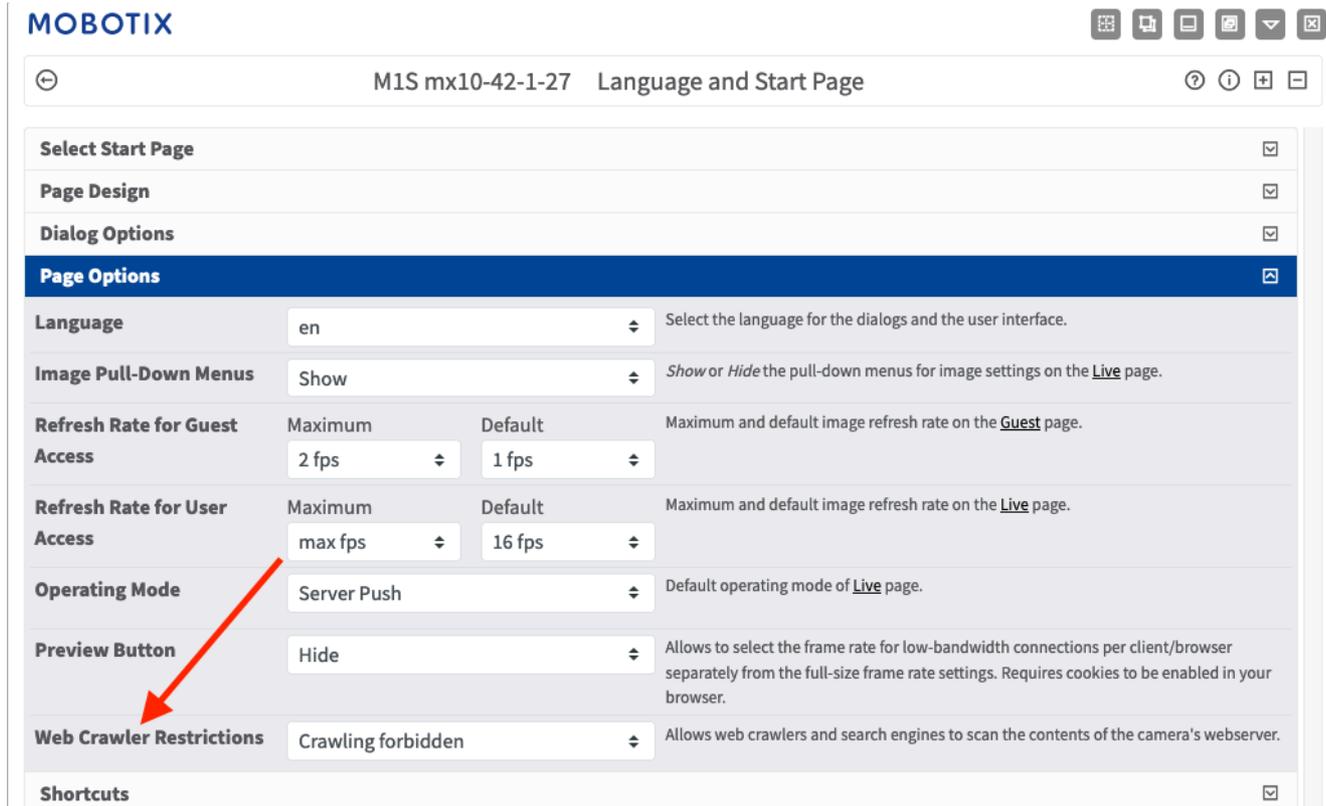
M1S mx10-42-1-27
Web Server

Web Server	<input checked="" type="checkbox"/>
HTTPS Settings	<input checked="" type="checkbox"/>
X.509 certificate currently used by the camera	<input checked="" type="checkbox"/>
Replace the X.509 certificate and private key currently used by the camera	<input checked="" type="checkbox"/>
Generate self-signed X.509 certificate and X.509 certificate request	<input checked="" type="checkbox"/>
Obtain X.509 certificate via ACME client	<input checked="" type="checkbox"/>
Intrusion Detection Settings	<input checked="" type="checkbox"/>
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 Web Server Logfile .)
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 IP-Level Access Control when threshold has been reached. Blocking is temporary until next reboot. This function takes only effect if IP-Level Access Control is enabled.
E-Mail Notification <input type="text" value="AlarmMail"/>	E-Mail Profile: Send image by e-mail. (E-Mail Profiles)
IP Notify <input type="text" value="Off"/>	IP Notify Profile: Notification by network message using the TCP/IP protocol. (IP Notify Profiles)
SNMP Traps <input type="text" value="Off"/>	Notification via SNMP Traps .
MQTT Publish <input type="text" value="Off"/>	Publish information via MQTT . Topic: MOBOTIX//notify/ids_alarm

Questa funzione offre una difesa automatica contro gli attacchi. Se un intruso dovesse tentare di accedere alla telecamera utilizzando metodi di "forza bruta" per indovinare nomi utente e password, la telecamera può inviare un avviso e bloccare automaticamente l'indirizzo IP offendentente dopo un certo numero di tentativi falliti.

9. Verificare che il Web Crawling sia vietato

Menu Amministrazione > Amministrazione della pagina > Lingua e pagina iniziale > Opzioni della pagina



MOBOTIX

M1S mx10-42-1-27 Language and Start Page

Select Start Page

Page Design

Dialog Options

Page Options

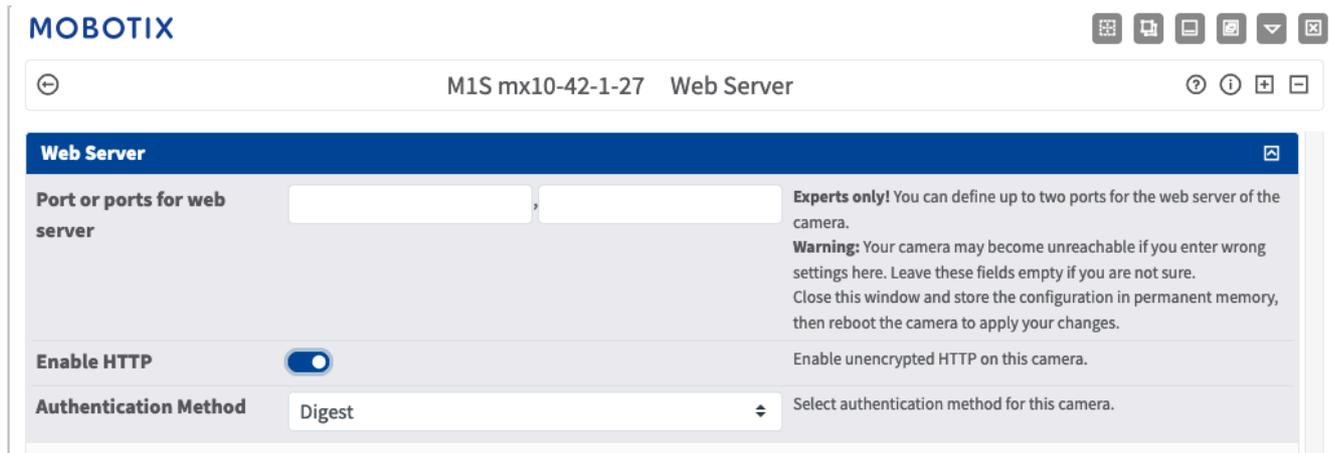
Language	en	Select the language for the dialogs and the user interface.
Image Pull-Down Menus	Show	Show or Hide the pull-down menus for image settings on the <u>Live</u> page.
Refresh Rate for Guest Access	Maximum: 2 fps Default: 1 fps	Maximum and default image refresh rate on the <u>Guest</u> page.
Refresh Rate for User Access	Maximum: max fps Default: 16 fps	Maximum and default image refresh rate on the <u>Live</u> page.
Operating Mode	Server Push	Default operating mode of <u>Live</u> page.
Preview Button	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	Crawling forbidden	Allows web crawlers and search engines to scan the contents of the camera's webserver.

Shortcuts

Con questo parametro è possibile impedire ai motori di ricerca Web, ad altri robot automatici e ai crawler Web di scansionare il contenuto del server Web della fotocamera. In genere, non si desidera che un motore di ricerca indicizzi tutte le immagini e le pagine presenti su una telecamera. Accertarsi di consentire il crawling solo se si è consapevoli dei rischi aggiuntivi per la sicurezza e del traffico di rete generato dai crawler.

10. Abilita l'autenticazione Digest

Menu Amministrazione > Configurazione della rete > Server Web (per gli esperti) > Server Web



The screenshot shows the MOBOTIX Web Server configuration interface. At the top, it says 'MOBOTIX' and 'M1S mx10-42-1-27 Web Server'. Below this is a 'Web Server' section with the following settings:

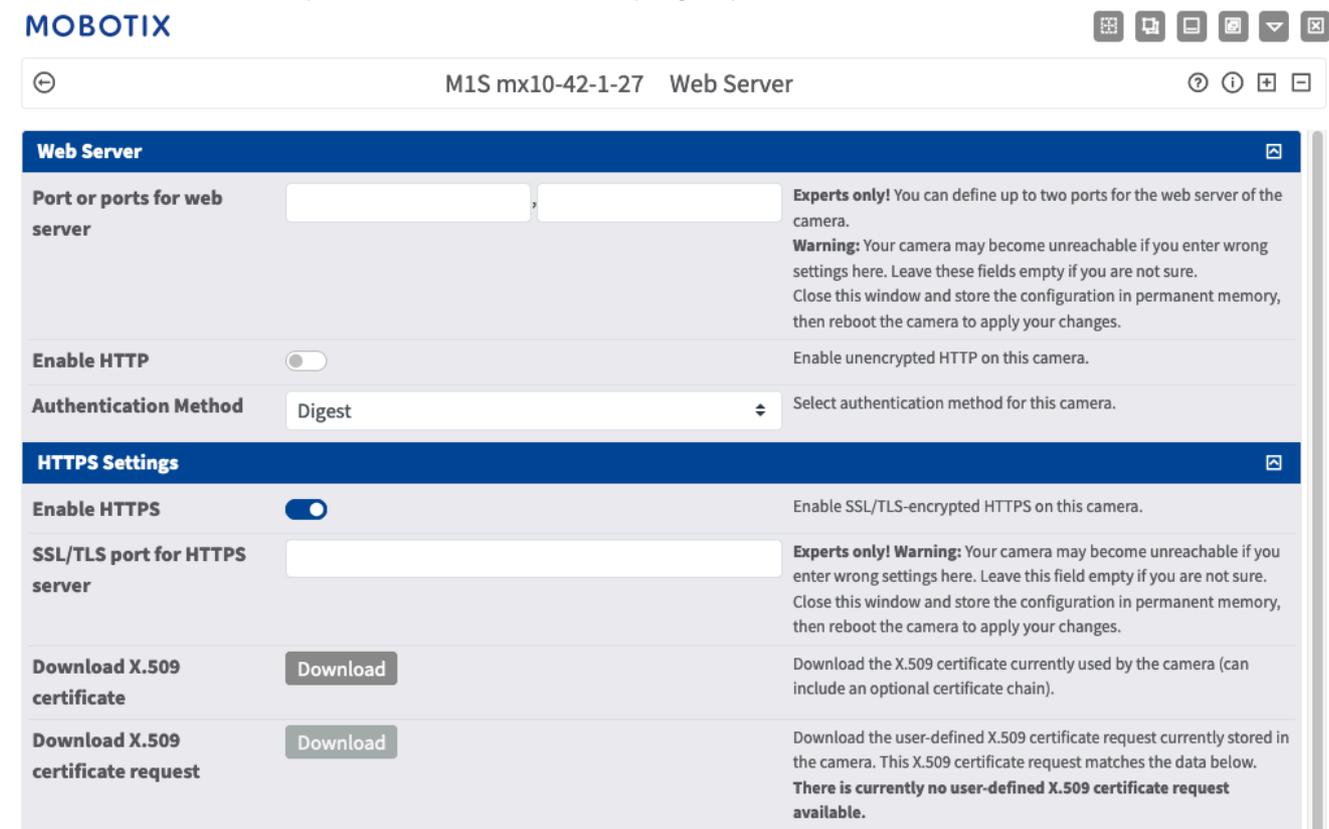
- Port or ports for web server:** Two empty input fields.
- Enable HTTP:** A toggle switch that is currently turned on.
- Authentication Method:** A dropdown menu set to 'Digest'.

On the right side of the 'Web Server' section, there is explanatory text: '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.' Below the 'Enable HTTP' toggle, it says 'Enable unencrypted HTTP on this camera.' Below the 'Authentication Method' dropdown, it says 'Select authentication method for this camera.'

L'autenticazione di accesso Digest è uno dei metodi concordati che un server Web (ad esempio la telecamera MOBOTIX) può utilizzare per negoziare le credenziali, come nome utente o password, con un client (ad esempio il browser Web). L'autenticazione Digest prevede che la password non venga mai inviata in chiaro e che il nome utente venga sottoposto a hashing.

11. Modificare le porte predefinite del server Web (per l'accesso remoto)

Menu Amministrazione > Impostazione rete > Server Web (per gli esperti)



The screenshot shows the MOBOTIX Web Server configuration interface. At the top, it says 'MOBOTIX' and 'M1S mx10-42-1-27 Web Server'. Below this is a 'Web Server' section with the following settings:

- Port or ports for web server:** Two empty input fields.
- Enable HTTP:** A toggle switch that is currently turned off.
- Authentication Method:** A dropdown menu set to 'Digest'.

Below the 'Web Server' section is an 'HTTPS Settings' section with the following settings:

- Enable HTTPS:** A toggle switch that is currently turned on.
- SSL/TLS port for HTTPS server:** An empty input field.
- Download X.509 certificate:** A 'Download' button.
- Download X.509 certificate request:** A 'Download' button.

On the right side of the 'Web Server' section, there is explanatory text: '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.' Below the 'Enable HTTP' toggle, it says 'Enable unencrypted HTTP on this camera.' Below the 'Authentication Method' dropdown, it says 'Select authentication method for this camera.'

On the right side of the 'HTTPS Settings' section, there is explanatory text: 'Enable SSL/TLS-encrypted HTTPS on this camera.' Below the 'SSL/TLS port for HTTPS server' input field, it says '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.' Below the 'Download X.509 certificate' button, it says 'Download the X.509 certificate currently used by the camera (can include an optional certificate chain).' Below the 'Download X.509 certificate request' button, it says '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.'

Le porte standard (80 TCP per HTTP e 443 TCP per HTTPS) sono più soggette ad attacchi. La sostituzione delle porte predefinite con porte personalizzate può aumentare ulteriormente la sicurezza della telecamera. Subito dopo aver disabilitato l'HTTP, è necessario accedere alla telecamera nel browser tramite HTTPS.

12. Impostare una chiave di crittografia per le registrazioni

Menu Amministrazione > Archiviazione > Archiviazione su file server esterno / dispositivo flash

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/John/data 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 Optional User ID and Group ID for NFS server, default: 65534 and 0
0

File Server Test Start Test Test the file server connection with the settings shown.

Storage Options

MxFFS Encryption Key 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.

Event Logging Enabled Activate event logging.

È possibile impostare una chiave di crittografia per criptare le registrazioni archiviate sulla memoria interna (scheda microSD / unità flash USB) e per le registrazioni archiviate sul File Server esterno (SMB / NFS). Fare clic su "Altro" per visualizzare tutte le opzioni di impostazione.

13. Modificare la password predefinita per MxMessage (necessaria solo se utilizzata)

Menu Amministrazione > MxMessageSystem > Distribuzione in rete dei messaggi

General Configuration of MxMessageSystem Networking

Networking Enabled 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 consente il trasferimento di messaggi tra telecamere in rete. Per criptare i messaggi trasferiti è necessario definire una password (chiave simmetrica) di almeno 6 caratteri.

Guida alla protezione

14. Abilita la notifica degli errori

Menu Amministrazione > Informazioni sul sistema > Notifica errori

La finestra di dialogo Notifica errori offre diverse opzioni per ricevere notifiche (e-mail, notifiche IP, chiamate VoIP, ecc.) in caso di riavvio o di errori rilevati all'interno dei differenti sistemi della telecamera. Questo strumento può aiutare gli amministratori di sistema a verificare che tutte le telecamere MOBOTIX funzionino correttamente.

15. Abilita il rilevamento dei guasti dello storage

Menu Amministrazione > Archiviazione > Rilevamento dei guasti di archiviazione

The screenshot shows the 'Storage Failure Detection' settings window in the MOBOTIX interface. The window title is 'M1S mx10-42-1-27 Storage Failure Detection'. The 'General Settings' section is expanded, showing the following configuration:

Setting	Value	Description
Check	Enabled	Enable or disable storage failure detection.
Tests	<input checked="" type="checkbox"/> Ping test (file server only) <input checked="" type="checkbox"/> Check transfer <input checked="" type="checkbox"/> Lost events <input checked="" type="checkbox"/> SD card I/O errors test	Select the tests you would like to perform. Ping test is only useful for remote file servers and will periodically check whether or not the server responds to network packets. Check transfer will ensure that it is possible to write data to the recording target. Checking for Lost events will detect events that could not be properly copied to the recording target. Hint: you can view the log file.
Sensitivity	High	Select the sensitivity of the tests. Use <i>High</i> for strict tests and to trigger error notification early. Otherwise use <i>Low</i> for less stringent test conditions and a delayed notification.

Utilizzare la finestra di dialogo Rilevamento errori di archiviazione per configurare test che monitorano costantemente la destinazione di archiviazione esterna (file server o dispositivo Flash) che la telecamera utilizza come buffer esterno. La telecamera monitora attivamente la destinazione di archiviazione e segnala i problemi di registrazione video utilizzando i metodi di notifica specificati in questa finestra di dialogo.

16. Generare e caricare certificati X.509 personalizzati

Menu Amministrazione > Impostazione rete > Server Web (per gli 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 checked="" type="radio"/>	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 <input type="radio"/>	Upload the user-supplied X.509 certificate that matches the X.509 certificate request currently stored in the camera. The currently used X.509 certificate will be overwritten. Download it first if you would like to preserve it.
Generate <input type="radio"/>	This will regenerate and overwrite 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. Note: Generation will need several seconds to complete.
Upload X.509 certificate from file: <input type="text" value="Select file"/> <input type="button" value="Browse"/>	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="Select file"/> <input type="button" value="Browse"/>	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.
Passphrase: <input type="text"/>	<input type="button" value="🔒"/>

Il caricamento di un certificato personalizzato firmato da una CA (Certificate Authority) affidabile garantirà la riservatezza e l'autenticità di tutte le connessioni stabilite tramite HTTPS (SSL/TLS).

17. Configurare il client OpenVPN per le connessioni remote

Menu Amministrazione > Impostazione rete > Impostazioni client OpenVPN

The screenshot shows the MOBOTIX web interface for 'M1S mx10-42-1-27 OpenVPN Configuration'. The 'General OpenVPN Setup' section is active, showing the 'OpenVPN' status as 'Enabled'. A description below the status says '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 stabilire un tunnel VPN (Virtual Private Network) tra la telecamera e l'host remoto.

La creazione di una connessione OpenVPN richiede un server corrispondente, che fornisca un accesso sicuro alla telecamera. A tal fine, è possibile gestire un proprio server OpenVPN o utilizzare il servizio di un provider OpenVPN. Per ulteriori informazioni su OpenVPN, visitate il sito web della [comunità OpenVPN](#).

18. Evitare di esporre la fotocamera a Internet se non strettamente necessario.

L'accesso remoto alla telecamera deve essere concesso consapevolmente per ridurre il rischio di attacchi. Se è necessario un accesso remoto, assicurarsi di osservare le regole sopra citate per limitare la possibilità di connessione ai soli utenti previsti.

19. Utilizzare le VLAN per separare la rete TVCC (livello di sicurezza aziendale).

Negli ambienti aziendali è buona norma mantenere la rete TVCC (telecamere IP, NVR e workstation VMS) separata dal resto degli host per prevenire accessi non autorizzati ed evitare la congestione del traffico.

Guida alla protezione

20. Abilitare IEEE 802.1X (livello di sicurezza aziendale)

Menu Amministrazione > Impostazione rete > Interfaccia Ethernet (per esperti) > IEEE 802.1X

Questo standard internazionale viene utilizzato per il controllo dell'accesso alla rete (NAC) basato sulle porte. Questa procedura prevede che tutti i dispositivi di rete (quindi anche la telecamera MOBOTIX) debbano autenticarsi presso lo switch per ottenere una connessione di rete. I dispositivi di rete senza un'autenticazione adeguata vengono rifiutati.

Chiedere all'amministratore di rete se IEEE 802.1X è supportato o richiesto. Assicurarsi che lo switch a cui è collegata la telecamera (autenticatore) sia stato configurato di conseguenza. In genere, lo switch (autenticatore) necessita anche di un server di autenticazione, ad esempio un server RADIUS. La procedura di autenticazione è controllata dal server di autenticazione. Assicurarsi che la telecamera e il server di autenticazione utilizzino sempre la stessa procedura.

21. Controllare regolarmente il file di log del server web.

Menu Amministrazione > Sicurezza > File di log del server web



Host Name	IP	Status	User	Date & Time
10.5.8.6	10.5.8.6	Successful	-	today 15:40:59
			admin	15:40:58
			-	15:39:56
			admin	15:33:52
			-	15:30:25
10.2.3.4	10.2.3.4	Successful	admin	2024-10-11 15:29:10
			-	14:31:11
			admin	14:31:08
10.0.0.2	10.0.0.2	Successful	-	14:30:24
			admin	14:20:56
			-	12:32:14
			admin	12:31:11
10.2.3.4	10.2.3.4	Successful	-	12:30:56
			admin	09:09:30
			-	09:09:21
10.32.150.131	10.32.150.131	Successful	admin	08:42:22
			-	08:42:14
			admin	08:41:29
			-	08:39:27
-	-	-	admin	08:39:22
			admin	2024-10-10 17:39:49
-	-	-	admin	17:39:38

Il file di registro del server Web presenta tutti i tentativi di accesso e le informazioni su data e ora con i relativi messaggi di stato del server Web e il nome host del computer che accede. I tentativi di accesso non autorizzati potrebbero essere il campanello d'allarme per gli amministratori di sistema che potrebbero voler rivedere la forza della loro rete.

22. Conservare i file di configurazione di backup in un luogo sicuro

Menu Amministrazione > Configurazione > Memorizza e salva la configurazione corrente sul computer locale

MOBOTIX



M1S mx10-42-1-27 Administration Overview



System Information	☑
Security	☑
Hardware Configuration	☑
Page Administration	☑
Network Setup	☑
MxMessageSystem	☑
Storage	☑
Logos and Image Profiles	☑
Transfer Profiles	☑
Audio and VoIP Telephony	☑
Camera Administration	☑
Configuration	☑
<ul style="list-style-type: none">• Store current configuration permanently (to flash) ← 1• Reset configuration to factory defaults• Restore last stored configuration from flash• Load configuration from local computer• Save current configuration to local computer ← 2• Show current configuration (raw version)• Edit configuration file (Text Edit)	
Maintenance	☑

Sebbene le credenziali della telecamera (password dell'utente) siano sottoposte a hashing all'interno del file di configurazione della telecamera, qualsiasi file di backup della configurazione deve essere conservato in un luogo sicuro; inoltre è consigliabile crittografare il file con una passphrase per una maggiore sicurezza.

Congratulazioni: la vostra telecamera MOBOTIX è ora cyber-sicura!



Configurazione VMS (Sistema di gestione video)



1. Creare account utente sul computer in uso
2. Creare account utente su MxMC
3. Limitare i diritti degli utenti VMS
4. Evitare di utilizzare l'account amministratore per accedere alle telecamere tramite MxMC.
5. Abilitare l'opzione "Auto log-off".

Congratulazioni: il vostro sistema di gestione video è ora cyber-sicuro!

Configurazione NAS (Network Attached Storage)



1. Riporre il dispositivo utilizzato per la memorizzazione dei filmati in un luogo sicuro.
2. Impostare una password forte per l'account amministrativo
3. Impostazione di un account utente standard (diritti limitati) per i dispositivi MOBOTIX
4. Crittografare i volumi
5. Utilizzare un livello RAID che garantisca la ridondanza dei dati.

Congratulazioni: il vostro sistema di Network Attached Storage è ora cyber-sicuro!