Guida alla protezione informatica

Come si indurisce
Il sistema video MOBOTIX

Telecamera - VMS - NAS

MOBOTIX

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.

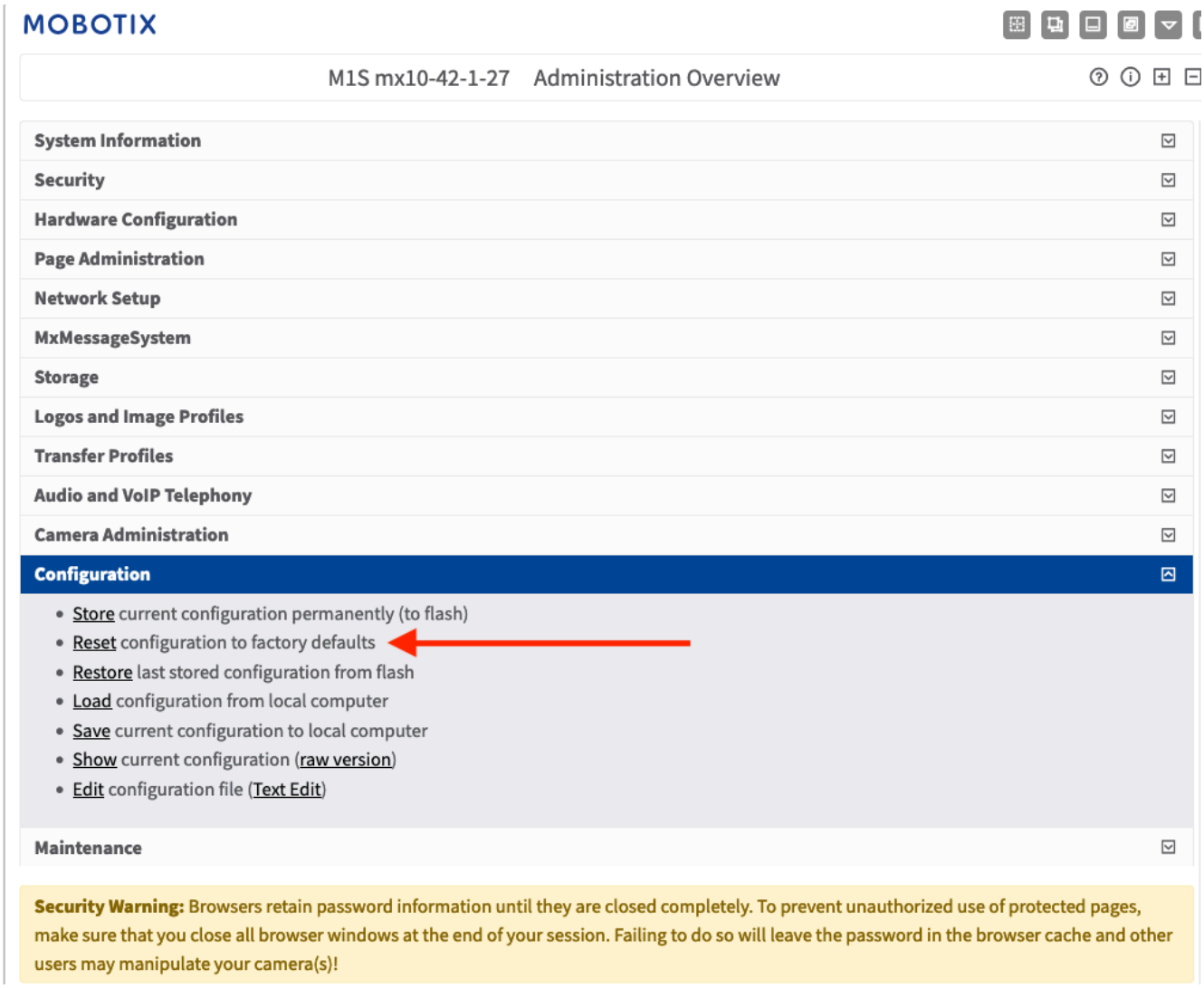
Configurazione della telecamera

1. Mantenere aggiornato il firmware delle telecamere

Il firmware MOBOTIX può essere scaricato gratuitamente dal nostro sito Web: *www.mobotix.com > Support > 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*

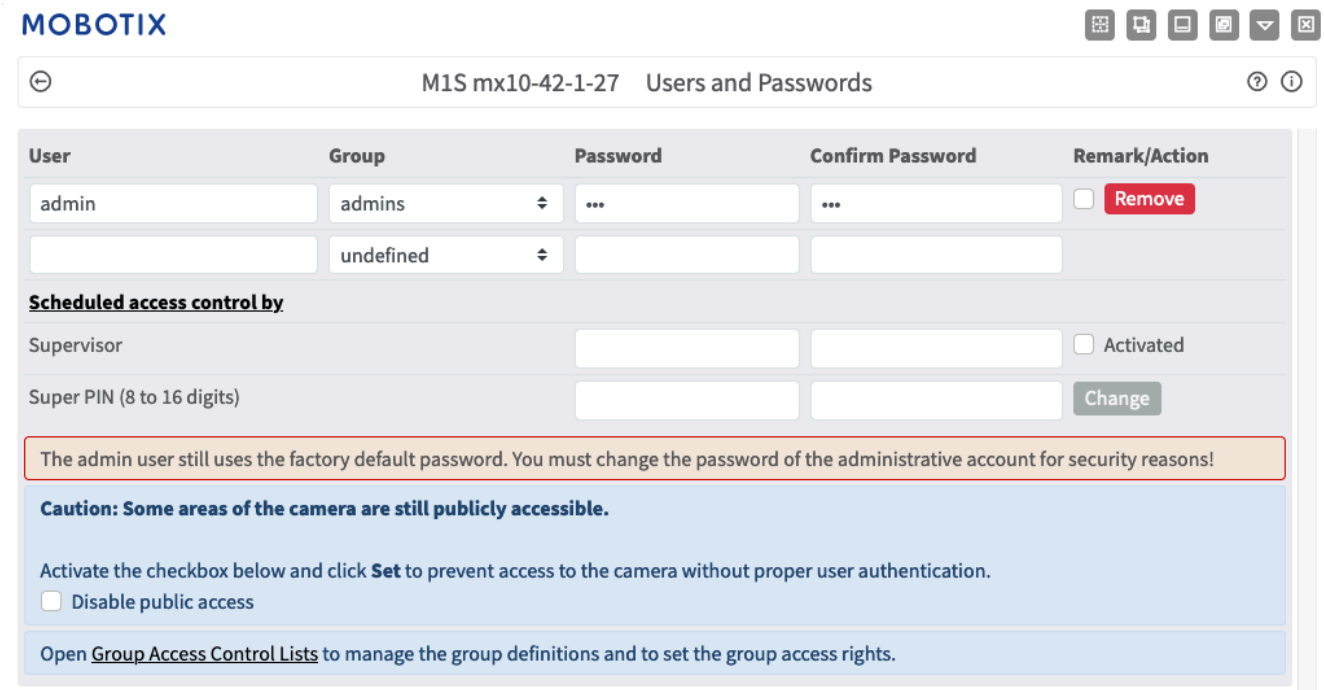
2. Ripristino della configurazione ai valori di fabbrica

Menu Amministrazione > Configurazione > Ripristino della configurazione di fabbrica



3. Modificare la password di amministrazione predefinita

Menu Amministrazione > Sicurezza > Utenti e password



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.

5. Creare utenti diversi e assegnarli ai gruppi giusti

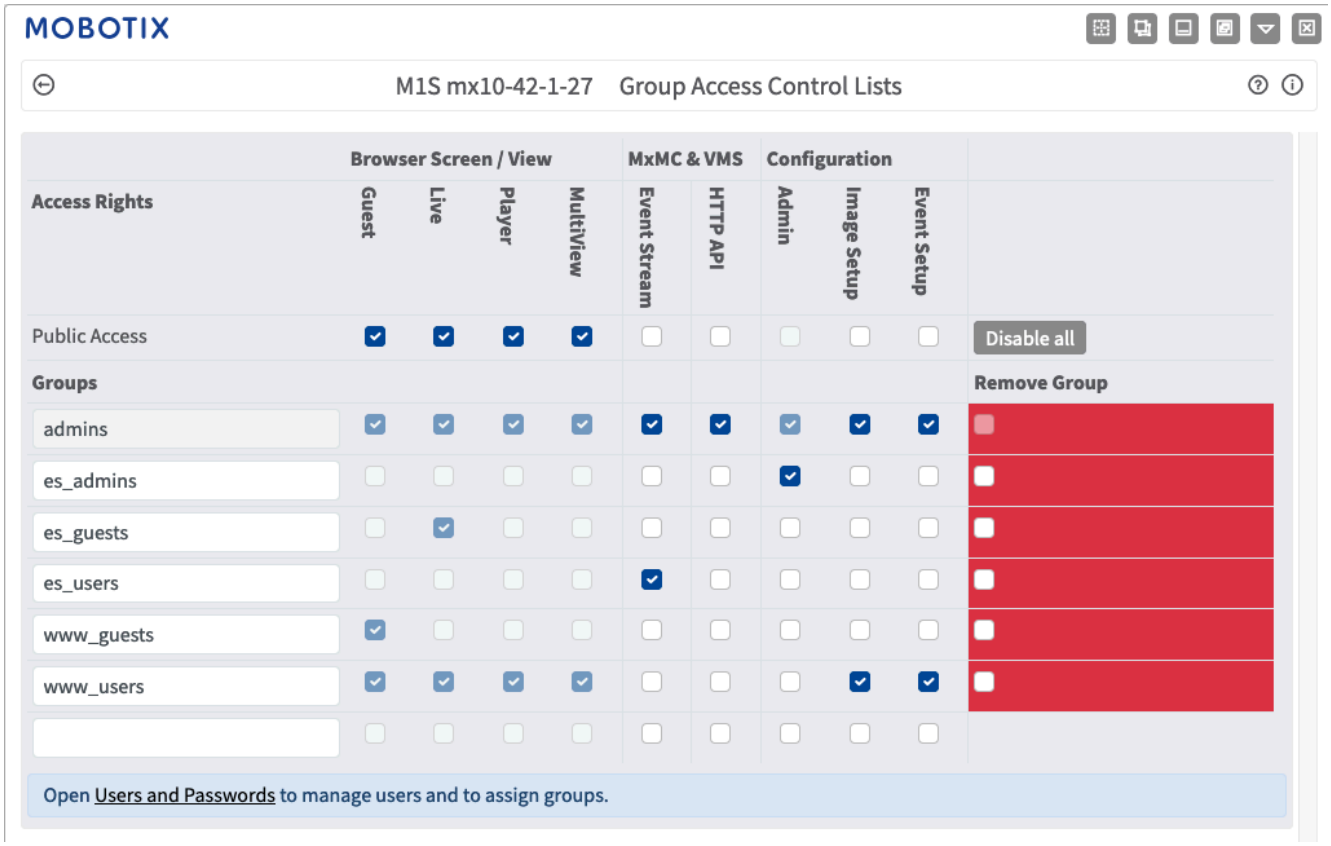
Menu Amministrazione > Sicurezza > Utenti e password

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



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".

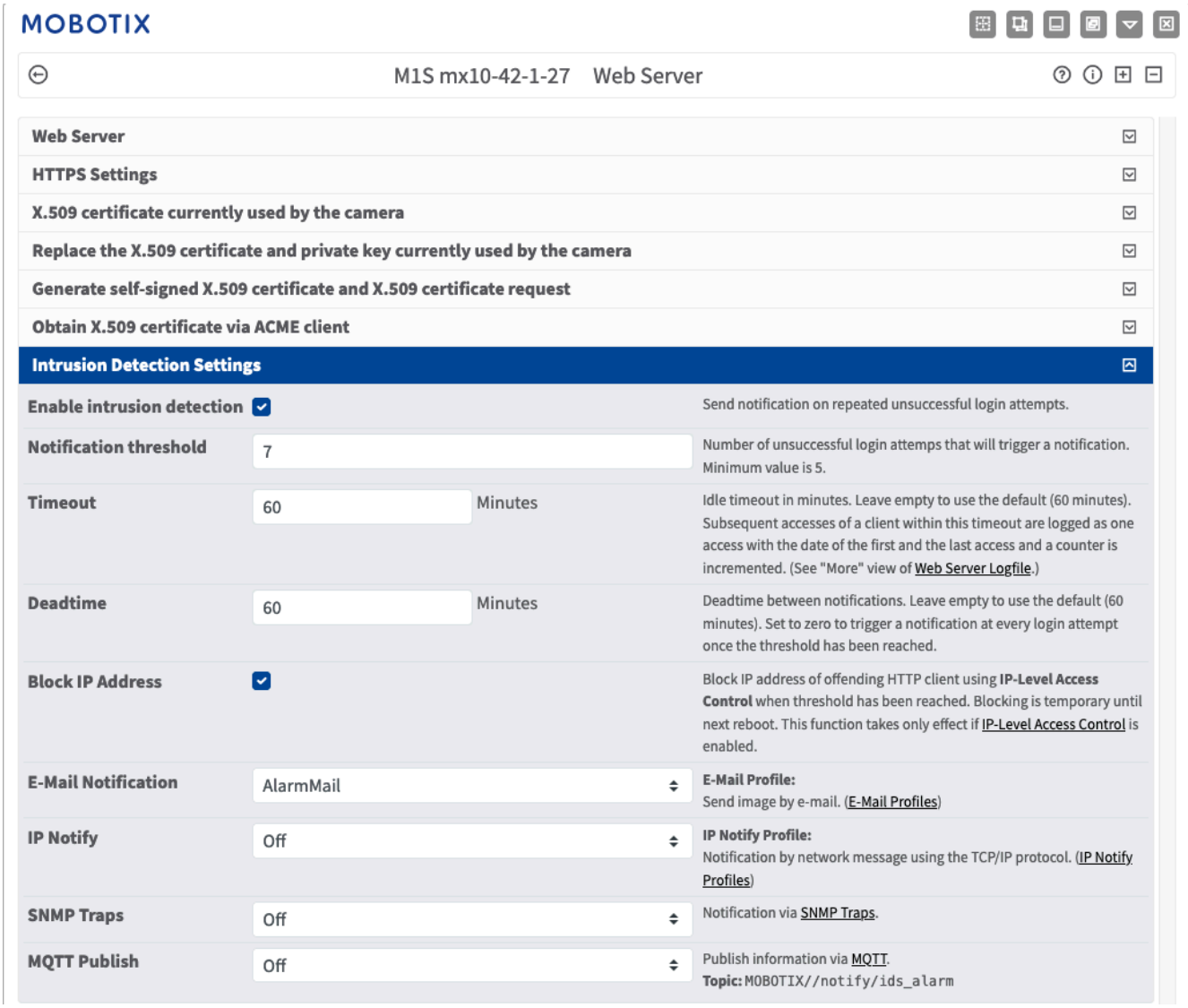
7. Abilitare la lista di controllo degli accessi IP

Menu Amministrazione > Sicurezza > Controllo accesso a livello IP

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.

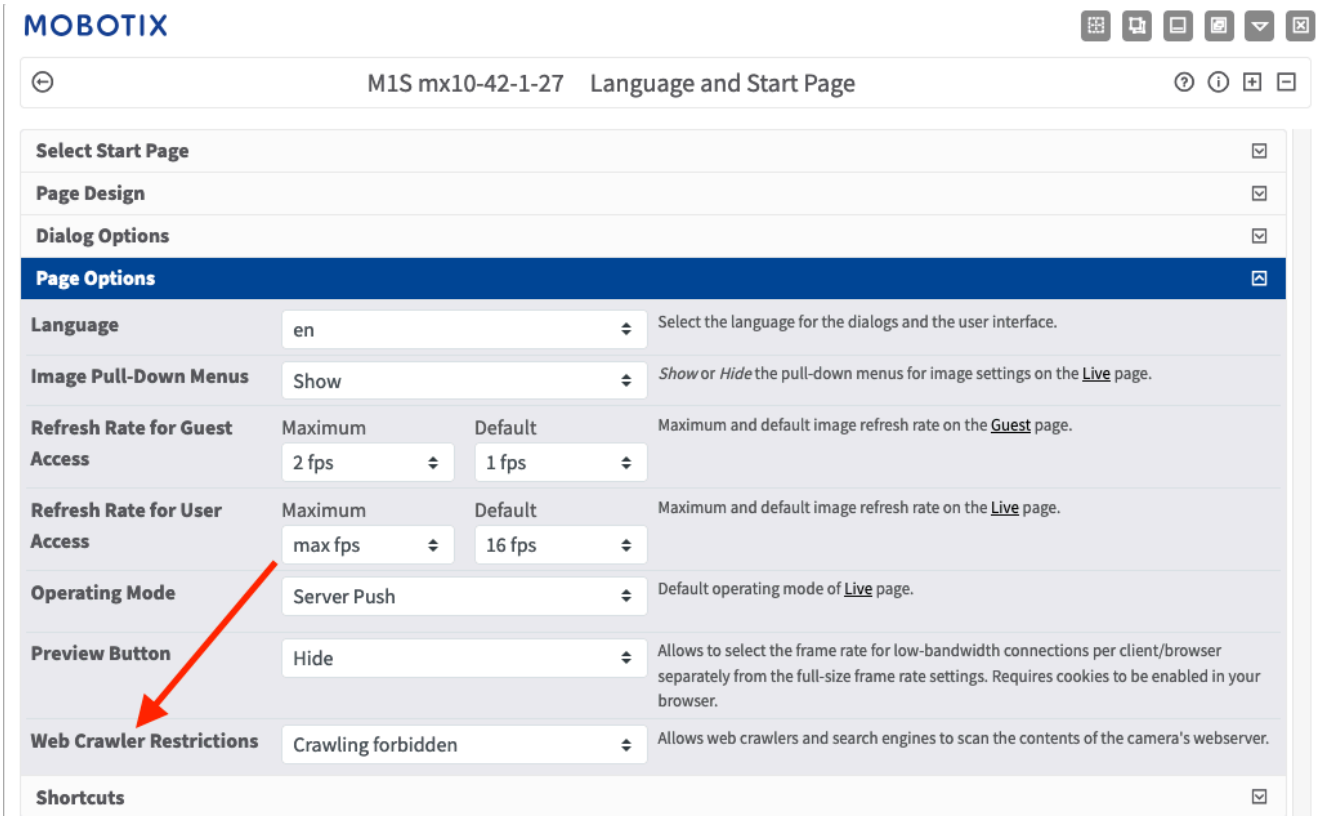
Menu Amministrazione > Configurazione della rete > Server Web (per gli esperti) > Impostazioni di rilevamento delle intrusioni



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 offendente dopo un certo numero di tentativi falliti.

9. Verificare che il Web Crawling sia vietato

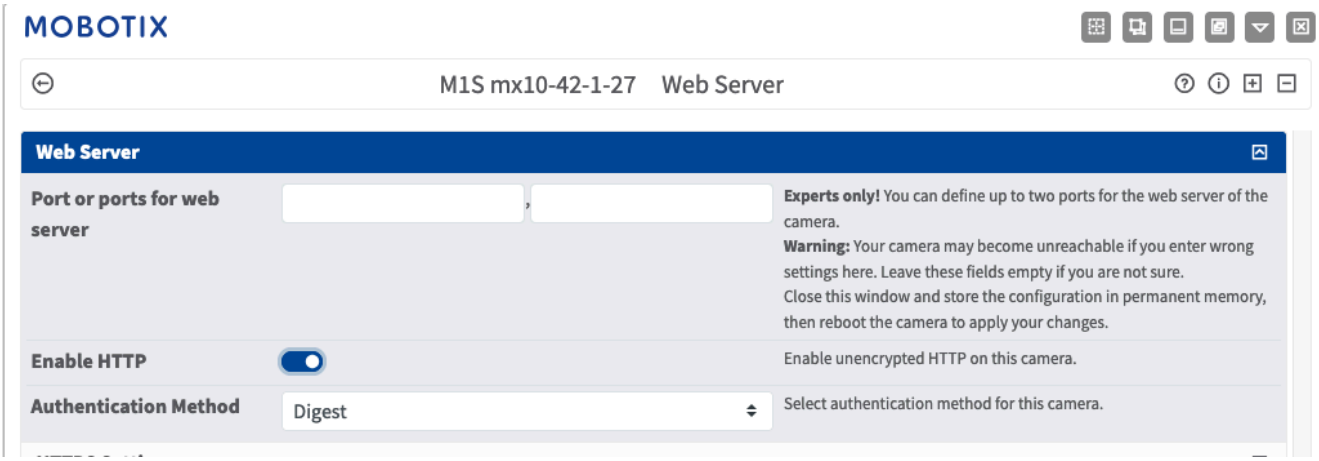
Menu Amministrazione > Amministrazione della pagina > Lingua e pagina iniziale > Opzioni della pagina



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 traffco di rete generato dai crawler.

10. Abilita l'autenticazione Digest

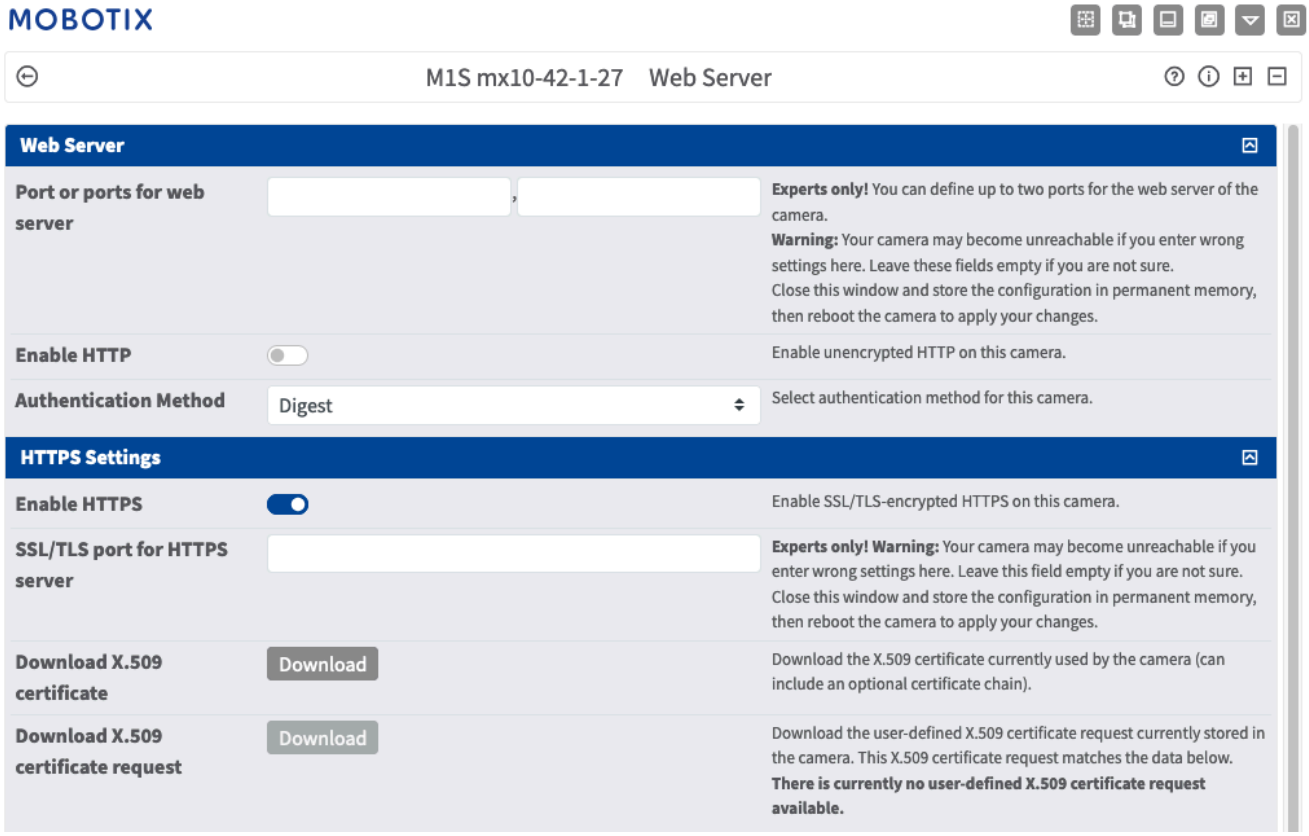
Menu Amministrazione > Configurazione della rete > Server Web (per gli esperti) > Server Web



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)

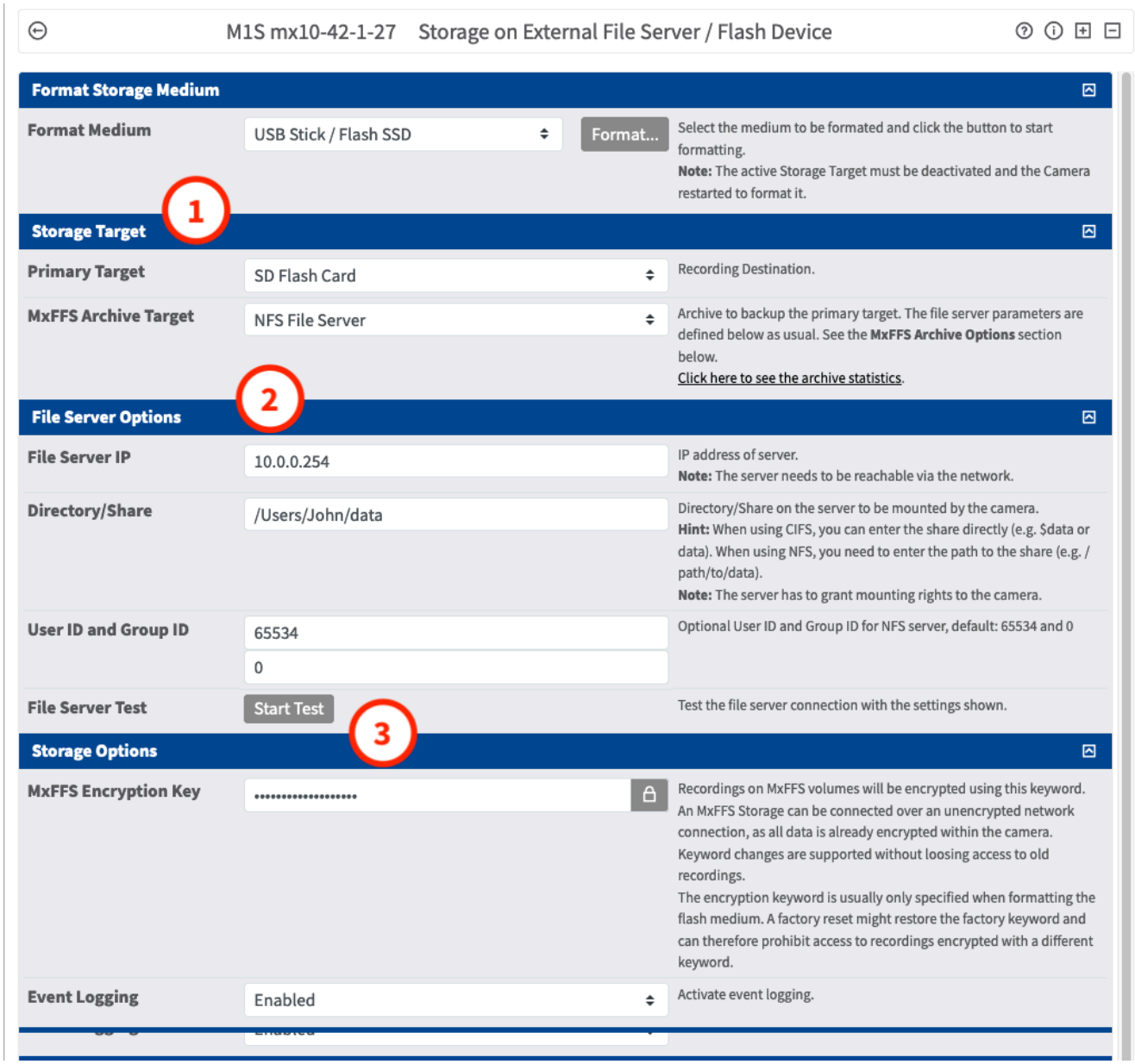
Menu Amministrazione > Impostazione rete > Server Web (per gli esperti)



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

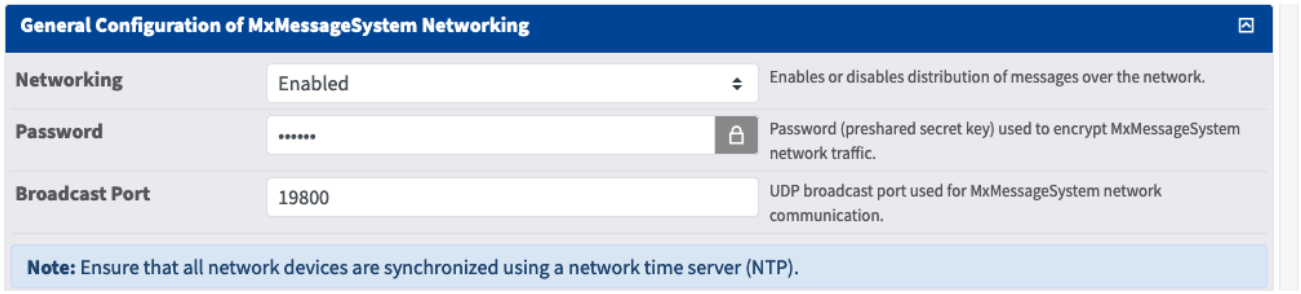
Menu Amministrazione > Archiviazione > Archiviazione su file server esterno / dispositivo flash



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



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.

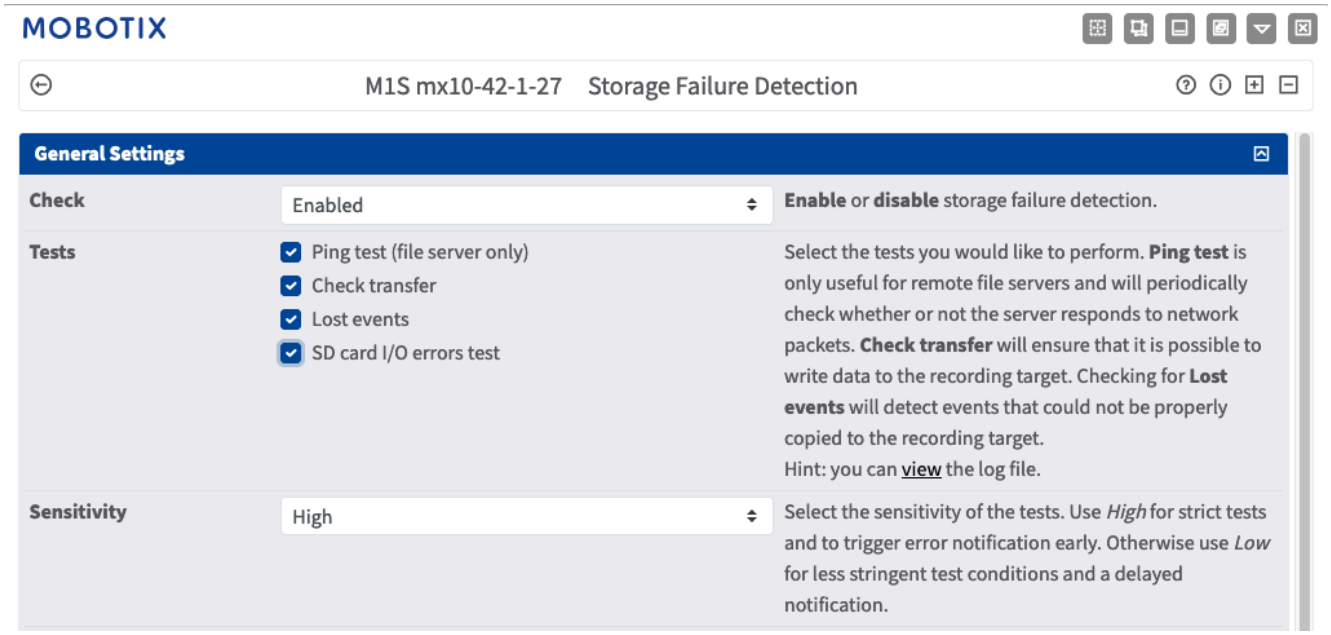
14. Abilita la notifica degli errori

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

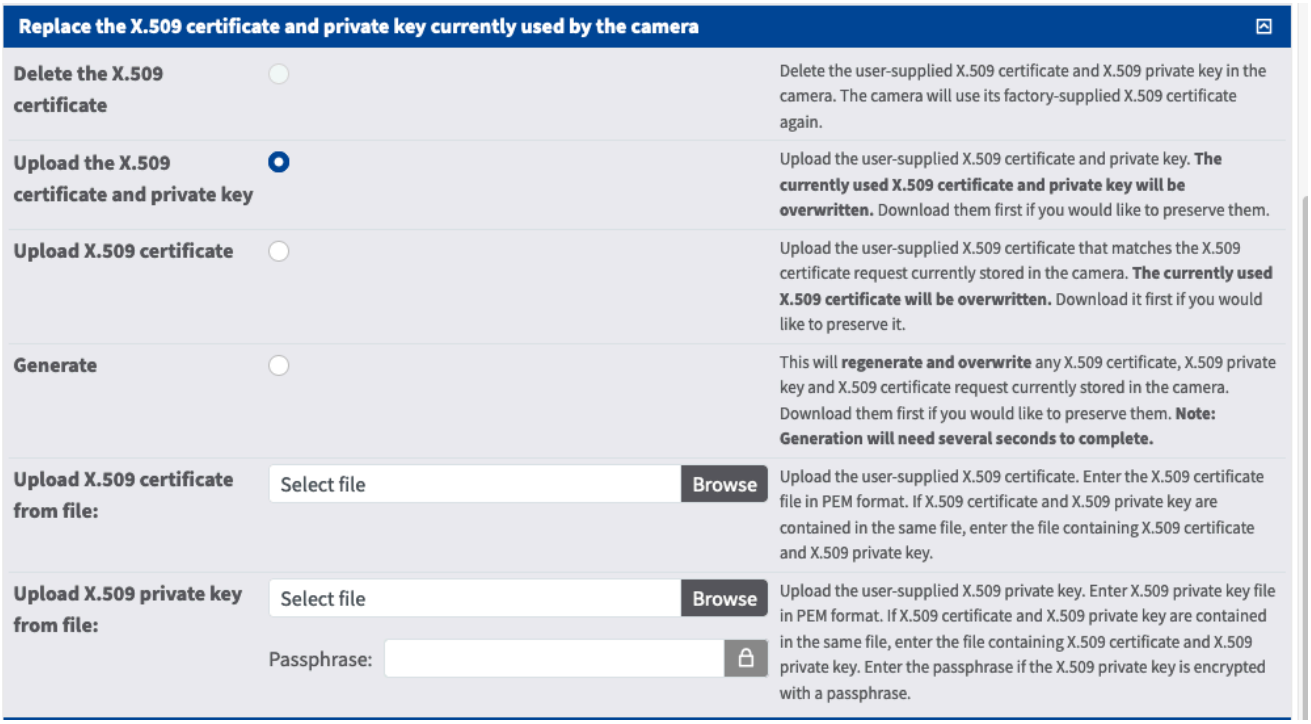
Menu Amministrazione > Archiviazione > Rilevamento dei guasti di archiviazione



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

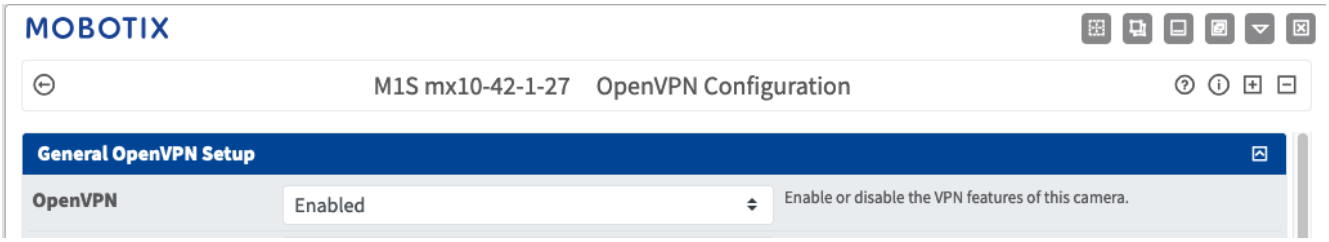
Menu Amministrazione > Impostazione rete > Server Web (per gli esperti)



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



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.

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.

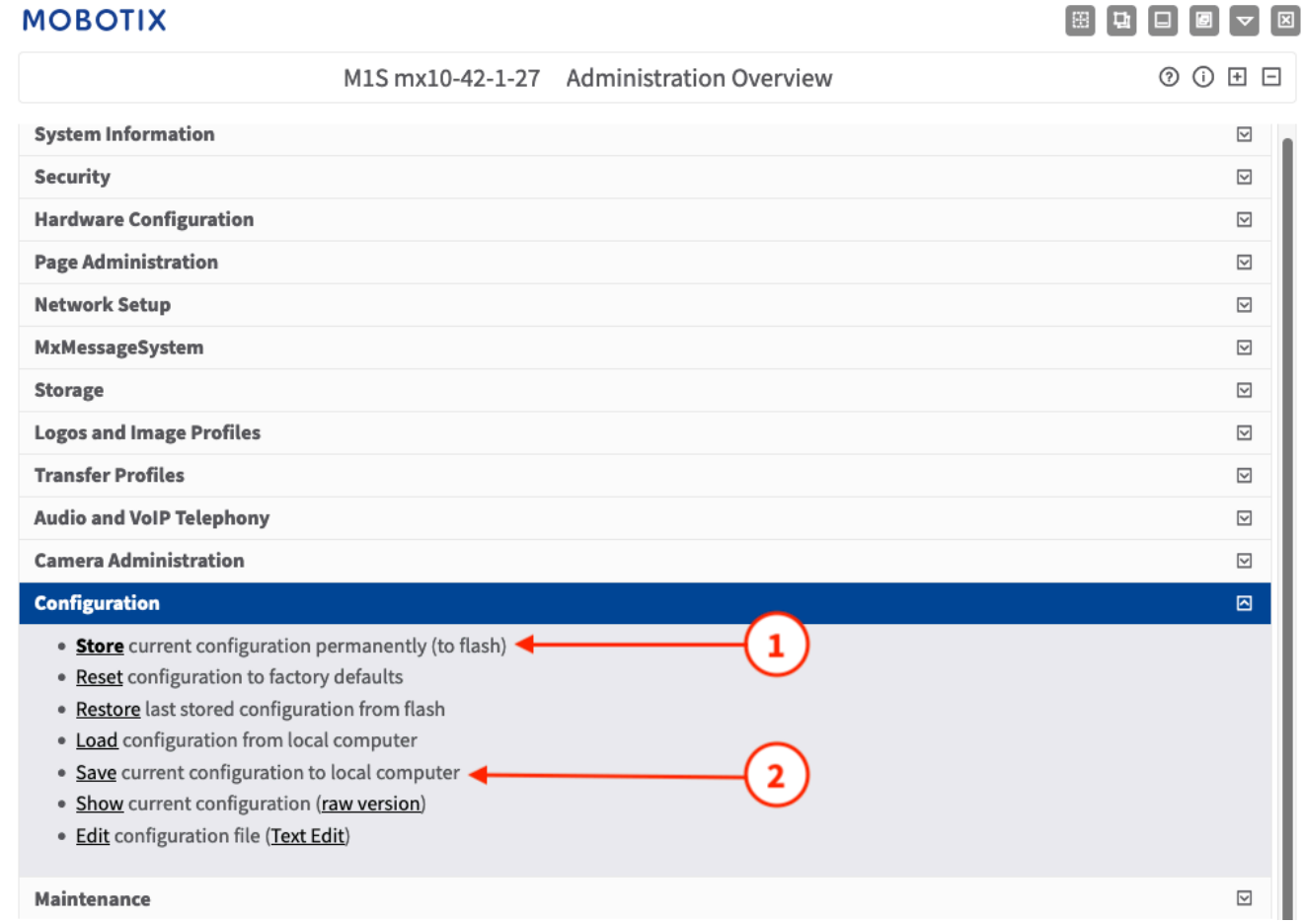
Menu Amministrazione > Sicurezza > File di log del server web

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
			admin	15:29:10
10.2.3.4	10.2.3.4	Successful	-	2024-10-11 14:31:11
			admin	14:31:08
			-	14:30:24
			admin	14:20:56
10.0.0.2	10.0.0.2	Successful	-	12:32:14
			admin	12:31:11
			-	12:30:56
			admin	09:09:30
			-	09:09:21
10.2.3.4	10.2.3.4	Successful	admin	08:42:22
			-	08:42:14
10.32.150.131	10.32.150.131	Successful	admin	08:41:29
			-	08:39:27
			admin	08:39:22
			-	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.

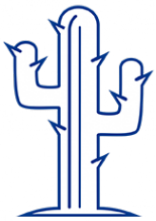
22. Conservare i file di configurazione di backup in un luogo sicuro

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



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!

MOBOTIX

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!