Guía de ciberprotección

Cómo endurecer
Su sistema de vídeo MOBOTIX

Cámara - VMS - NAS

MOBOTIX

Acerca de esta guía

Los ciberataques contra software y hardware conectados a Internet son un problema creciente. En los últimos años, los atacantes se centran cada vez más en explotar los eslabones más débiles de un perímetro de seguridad para acceder a aplicaciones críticas y datos sensibles.

Con la tecnología de videovigilancia como parte vital de la seguridad del sitio que a menudo habita en una red corporativa compartida, los dispositivos de videovigilancia se están convirtiendo cada vez más en el objetivo de ciberataques dirigidos.

Reconociendo esta tendencia emergente, MOBOTIX ha desarrollado un conjunto de **herramientas y funciones integradas** que permiten a los administradores de seguridad informática configurar cada dispositivo como parte de un enfoque multicapa de la ciberseguridad.

Estas herramientas, cuando se utilizan junto con otros elementos de seguridad como cortafuegos y segmentación de red, pueden reducir la superficie de ataque que presentan los dispositivos MOBOTIX como parte de una política de acceso seguro para administradores y usuarios.

Esta guía proporciona consejos prácticos sobre cómo configurar los dispositivos MOBOTIX para ofrecer la máxima protección contra los ciberataques, así como orientación sobre las mejores prácticas para crear una infraestructura de videovigilancia segura.

Nota: Este documento pretende dar al administrador responsable una visión completa de todas las medidas posibles para reforzar el sistema MOBOTIX. En relación con la aplicación individual y para evitar reconfiguraciones, puede que no sea útil llevar a cabo cada uno de los procedimientos explicados en esta guía.

Información general: MOBOTIX no asume ninguna responsabilidad por errores técnicos, errores de impresión u omisiones.

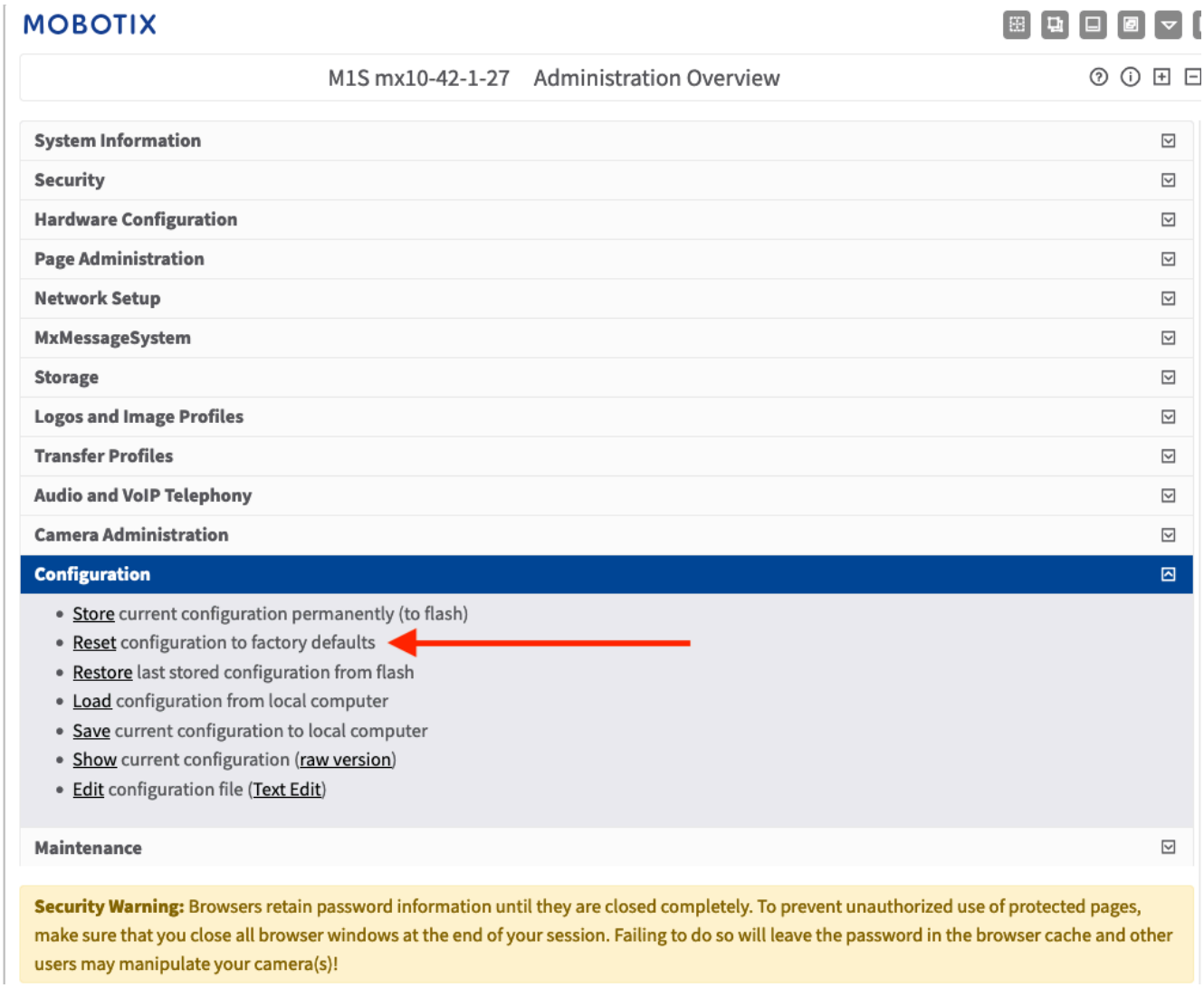
Configuración de la cámara

1. Mantener actualizado el firmware de las cámaras

El firmware de MOBOTIX puede descargarse gratuitamente desde nuestro sitio web: *www.mobotix.com > Soporte > Centro de* descargas ¿No está seguro de cómo proceder? Consulte esta guía *compacta*: *www.mobotix.com > Soporte > Centro de descargas > Documentación > Folletos y guías > Guías compactas > Mx_CG_FirmwareUpdate.pdf*

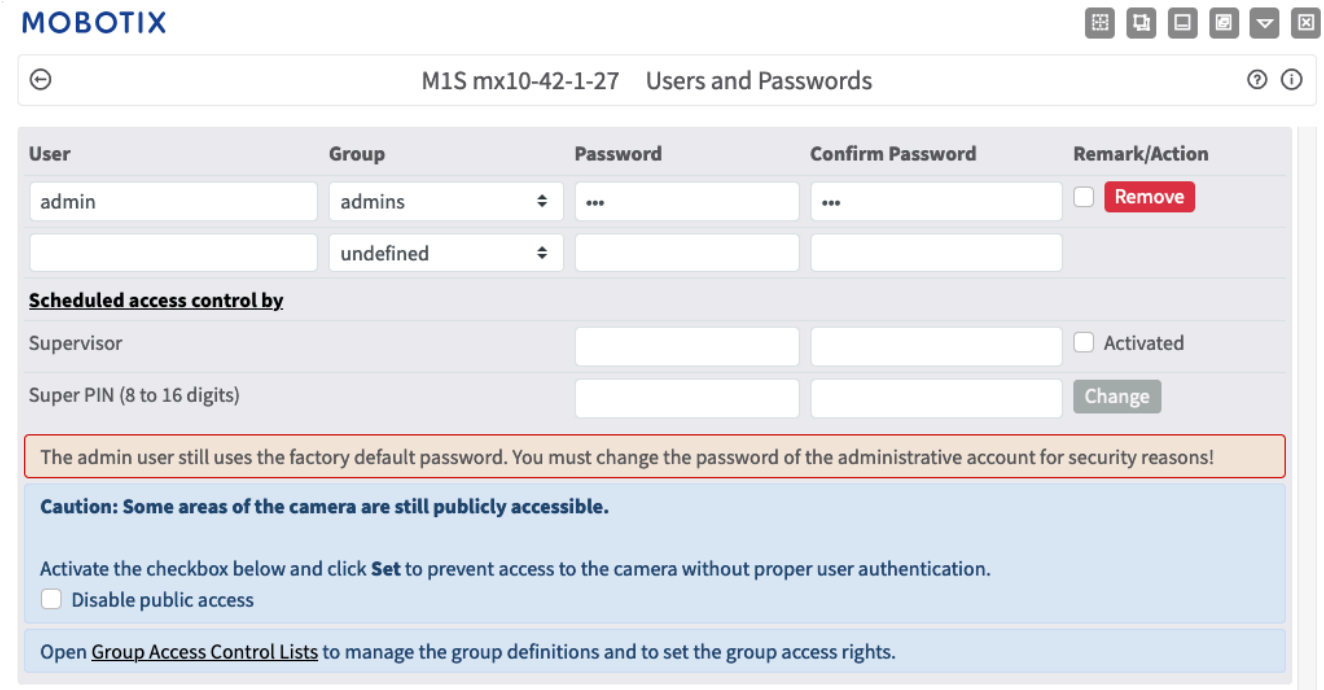
2. Restablecer la configuración a los valores de fábrica

Menú Admin > Configuración > Restablecer la configuración a los valores predeterminados de fábrica



3. Cambiar la contraseña de administrador por defecto

Menú Admin > Seguridad > Usuarios y contraseñas



Siempre es necesario cambiar la contraseña por defecto "meinsm" la primera vez que llame a la cámara.

Una vez que haya terminado de configurar usuarios, contraseñas y grupos, siempre debe almacenar la configuración en la memoria permanente de la cámara. De lo contrario, la configuración modificada sólo se utilizará hasta el próximo reinicio de la cámara. Utilice el botón Cerrar al final del cuadro de diálogo ya que le pedirá automáticamente que guarde la configuración de la cámara en la memoria permanente de la cámara.

Asegúrate de guardar la información de tu contraseña en un lugar seguro. Se debe tener especial cuidado en conservar la contraseña de al menos un usuario del grupo admins. Sin la contraseña, el acceso administrativo a la cámara ya no es posible y no hay posibilidad de eludir la contraseña. Asimismo, es imposible recuperar la contraseña de una configuración guardada permanentemente.

Cómo crear una contraseña segura:

- Utilice 8 o más caracteres (hasta 99)
- Al menos un carácter en mayúsculas
- Al menos un carácter en minúscula
- Al menos un dígito
- ¡Al menos un carácter especial: ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~
- Evitar palabras y fechas comunes

Política de restablecimiento de contraseñas:

¡Si la contraseña de administrador ya no está disponible, la cámara debe ser restablecida a través de MOBOTIX por

4. Crear diferentes grupos de usuarios con diferentes derechos de usuario

Menú Admin > Seguridad > Usuarios y contraseñas

En general, no todos los usuarios necesitan los mismos derechos. Puede crear hasta 25 grupos de usuarios diferentes desde la página Menú Admin > Lista de control de acceso de grupos.

5. Crear diferentes usuarios y asignarlos a los grupos adecuados

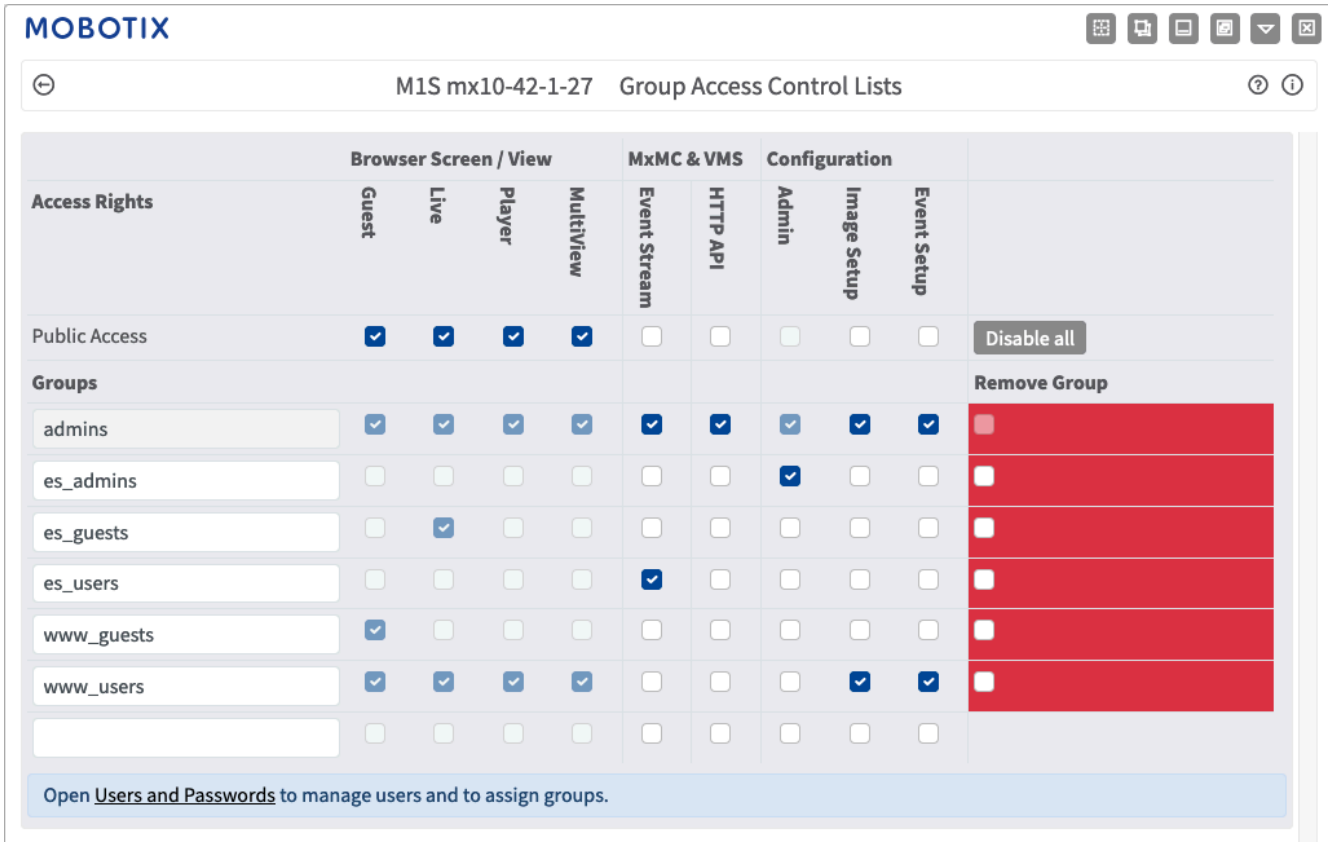
Menú Admin > Seguridad > Usuarios y contraseñas

Siempre es recomendable crear un usuario para cada persona autorizada a acceder a la cámara. Se pueden crear hasta 100 usuarios. Las acciones realizadas por los usuarios autorizados se rastrean en el archivo de registro del servidor Web; esto ayuda a determinar "quién hizo qué" en caso de disputas.

Consulte la descripción anterior para crear contraseñas seguras.

6. Desactivar el acceso público

Menú Admin > Seguridad > Listas de control de acceso de grupos



El Acceso Público permite, si está activado, acceder a recursos específicos de la cámara sin autenticación. Se recomienda encarecidamente desactivar el Acceso Público para evitar que usuarios no autorizados puedan visualizar la transmisión en directo de la cámara, las grabaciones o incluso controlar la cámara (por ejemplo, cambiar la configuración o ejecutar acciones). Más opciones de configuración en "Más".

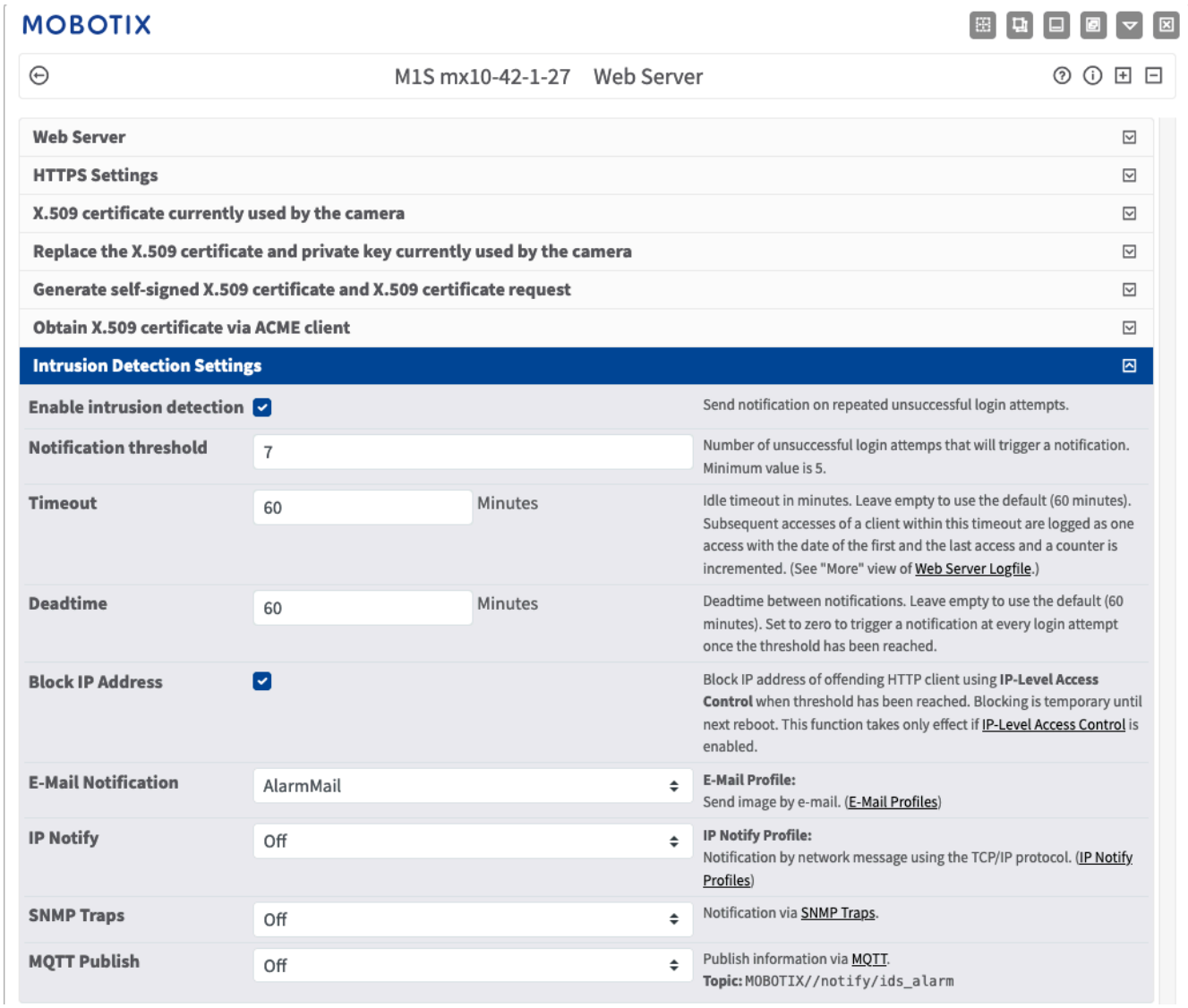
7. Activar la lista de control de acceso IP

Menú Admin > Seguridad > Control de acceso a nivel de IP

El cuadro de diálogo Control de Acceso permite gestionar las direcciones IP, subredes y nombres de dominio, a los que se les permite acceder a la cámara o a los que se les impide acceder a la cámara. Esta posibilidad de controlar el acceso a la cámara utiliza el nivel de protocolo IP, es independiente de la autenticación de usuario basada en contraseña en el nivel de protocolo HTTP y sustituye a la autenticación basada en contraseña. Si un ordenador no tiene acceso a nivel IP a la cámara, no hay posibilidad de acceder a la cámara desde ese ordenador. Si un ordenador tiene acceso a nivel IP a la cámara, la autenticación de usuario basada en contraseña sigue como siguiente paso, como se especifica en el cuadro de diálogo Usuarios y Contraseñas.

8. Activar la detección de intrusos con notificación y bloqueo de la dirección IP offending.

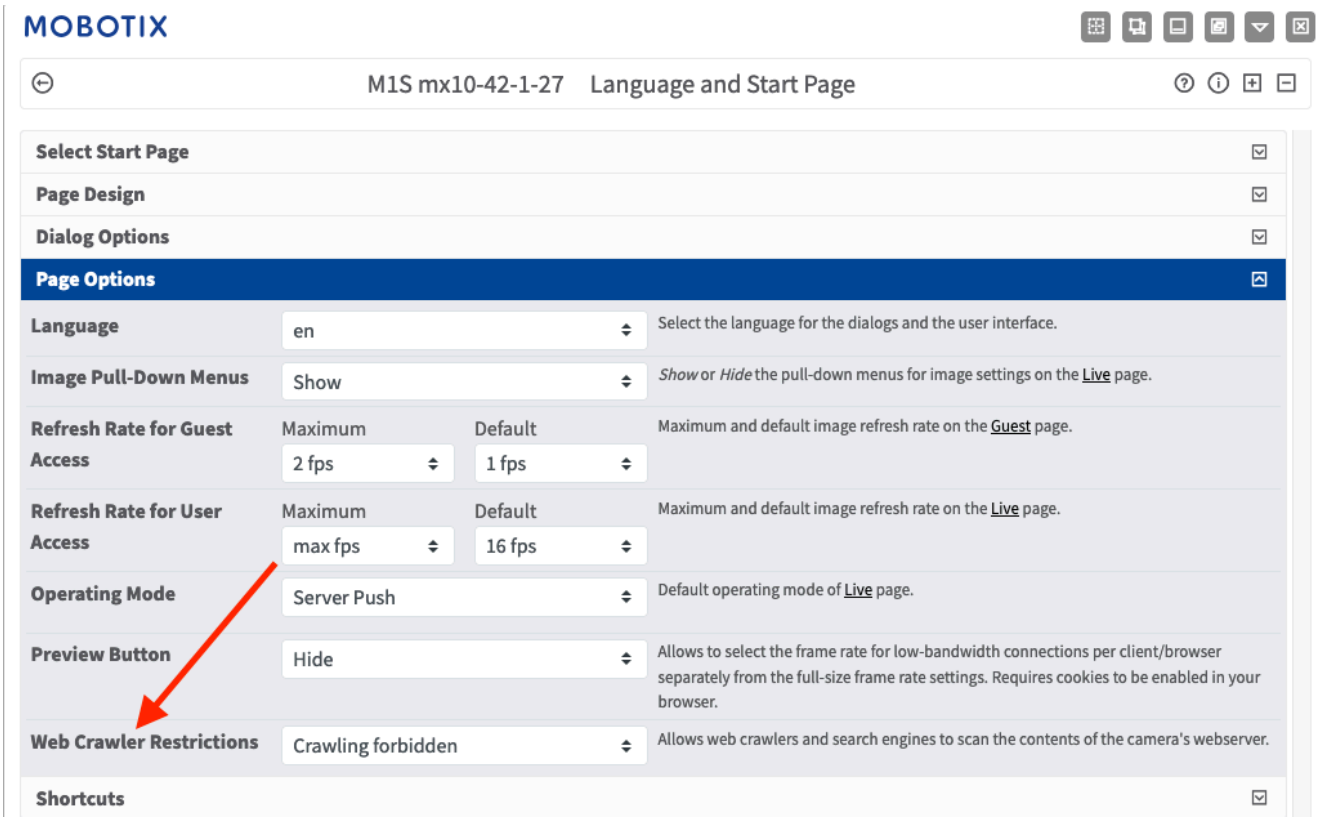
Menú Admin > Configuración de red > Servidor Web (para expertos) > Configuración de detección de intrusos



Esta función proporciona una defensa automática contra ataques. Si un intruso intenta acceder a la cámara utilizando métodos de "fuerza bruta" para adivinar nombres de usuario y contraseñas, la cámara puede enviar una alerta y bloquear automáticamente la dirección IP de origen tras un determinado número de intentos fallidos.

9. Compruebe que el rastreo web está prohibido

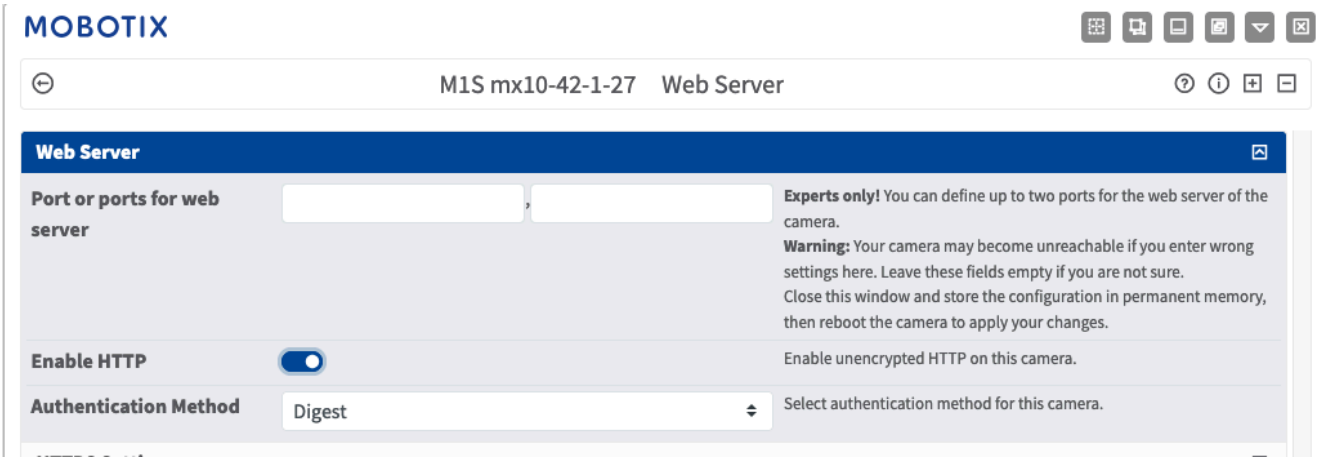
Admin Menu > Administración de Páginas > Idioma y Página de Inicio > Opciones de Página



Utilizando este parámetro, puede evitar que los motores de búsqueda web, otros robots automáticos y rastreadores web escaneen el contenido del servidor web de la cámara. Normalmente, no querrá que un motor de búsqueda indexe todas las imágenes y páginas encontradas en una cámara. Asegúrese de que sólo permite el rastreo si es consciente de los riesgos de seguridad adicionales y del traffic de red extra generado por los rastreadores.

10. Activar autenticación Digest

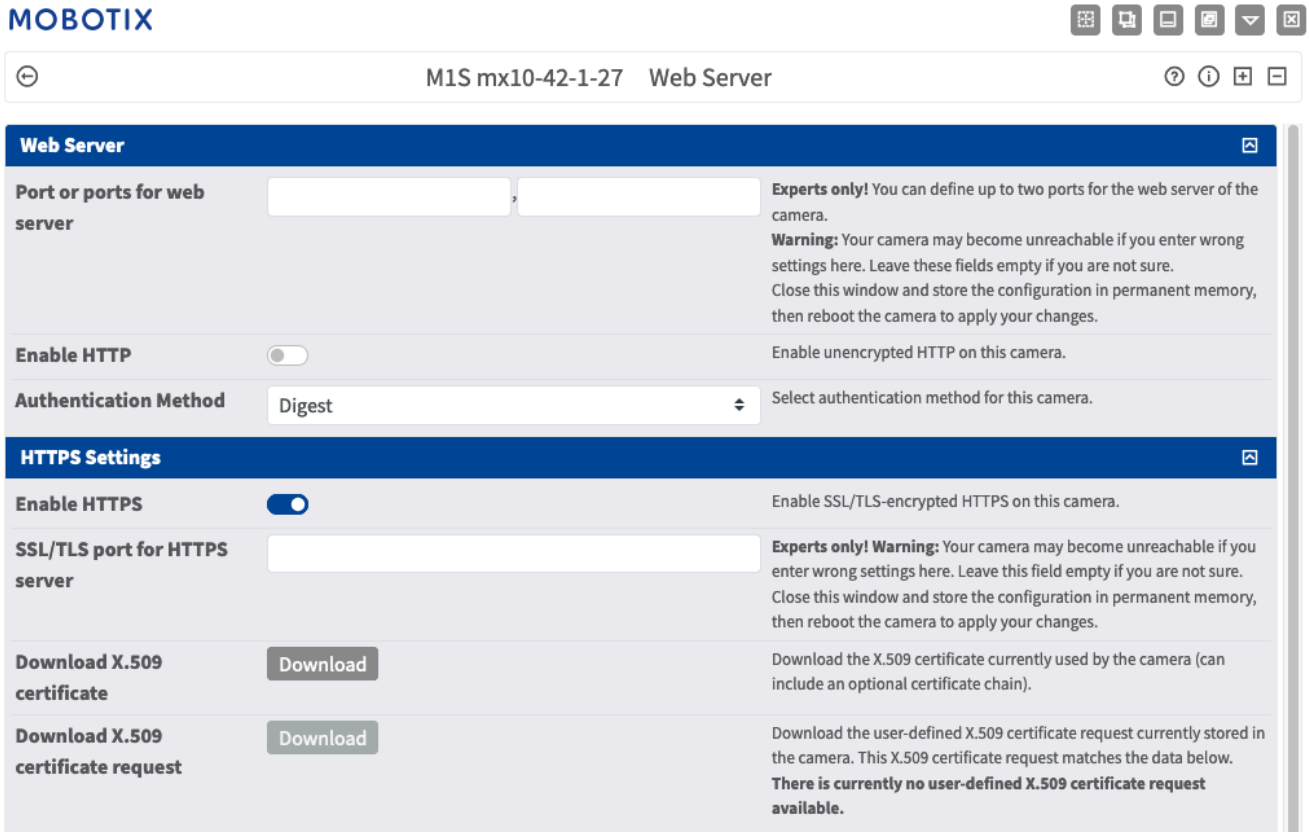
Menú Admin > Configuración de red > Servidor Web (para expertos) > Servidor Web



La autenticación de acceso Digest es uno de los métodos acordados que un servidor web (p.e. cámara MOBOTIX) puede utilizar para negociar credenciales, como nombre de usuario o contraseña, con un cliente (p.e. navegador web). Si se desea la Autenticación Digest la contraseña nunca se envía en claro, y el nombre de usuario puede ser hash.

11. Cambiar los puertos por defecto del Servidor Web (para acceso remoto)

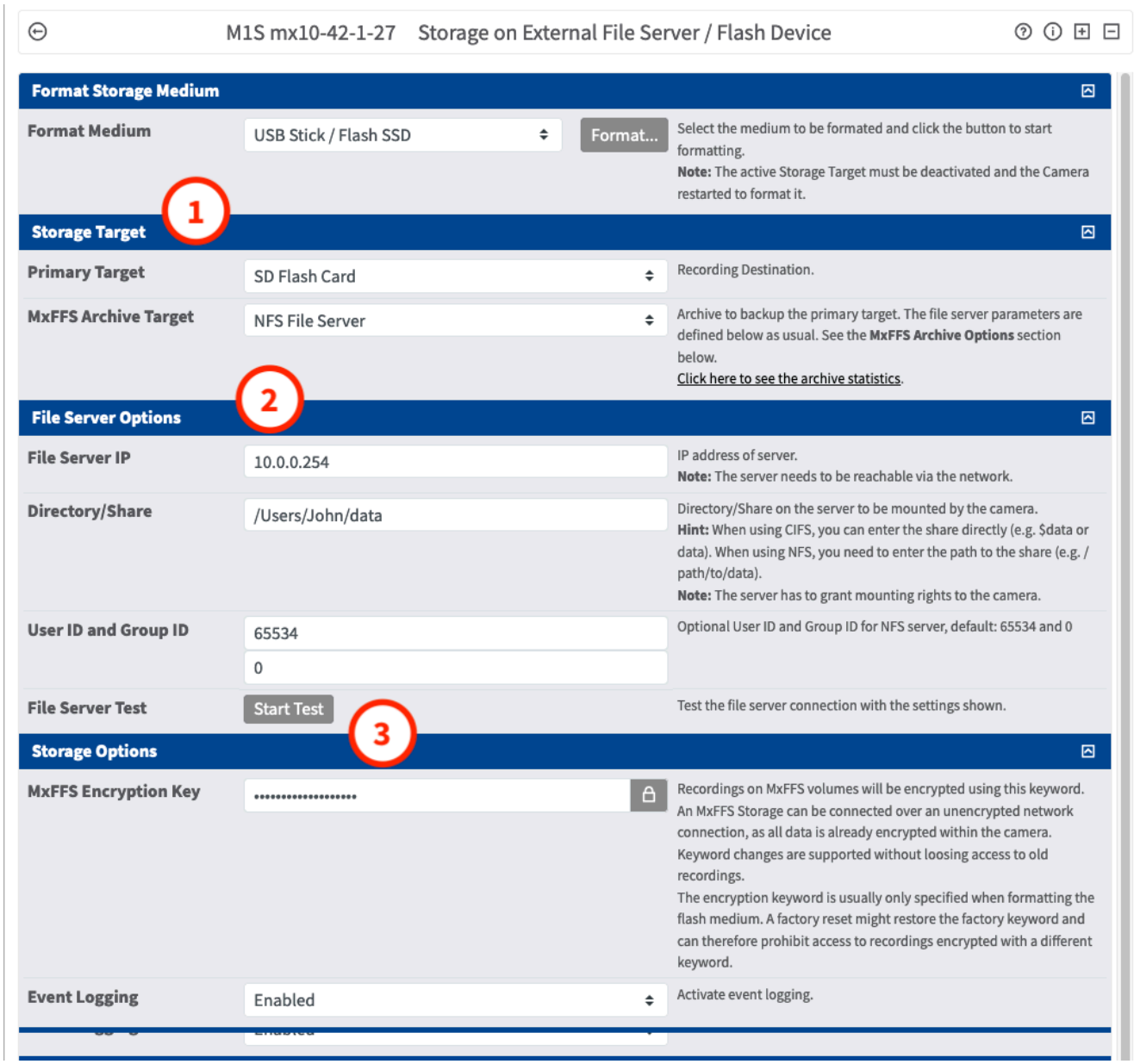
Menú Admin > Configuración de red > Servidor Web (para expertos)



Los puertos estándar (80 TCP para HTTP y 443 TCP para HTTPS) son más propensos a los ataques. Sustituir los puertos predeterminados por otros personalizados puede aumentar aún más la seguridad de la cámara. Inmediatamente después de deshabilitar HTTP, se debe acceder a la cámara en el navegador a través de HTTPS.

12. Establecer una clave de encriptación para las grabaciones

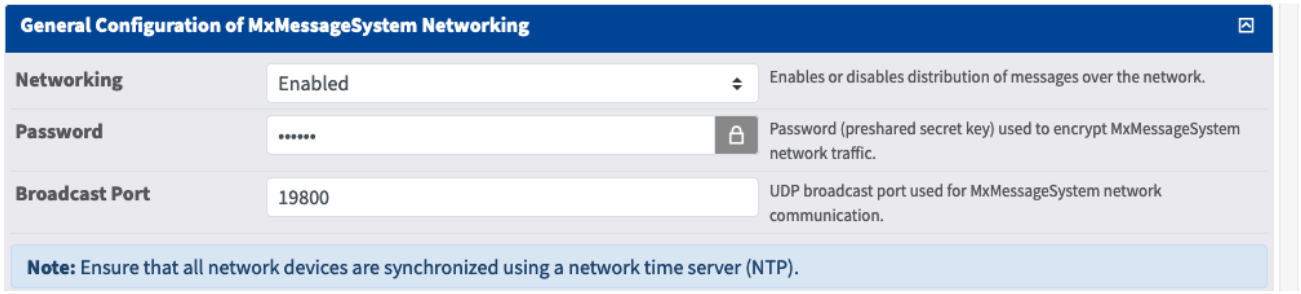
Menú Admin > Almacenamiento > Almacenamiento en Servidor de Archivos Externo / Dispositivo Flash



Se puede establecer una clave de cifrado para cifrar las grabaciones almacenadas en el almacenamiento interno (tarjeta microSD / unidad flash USB), así como para la grabación archivada en el servidor de archivos externo (SMB / NFS). Haz clic en "Más" para ver todas las opciones de configuración.

13. Cambiar la contraseña por defecto para MxMessage (sólo es necesario si se utiliza)

Menú Admin > MxMessageSystem > Distribución de mensajes en red



El MxMessageSystem permite la transferencia de mensajes entre cámaras a través de la red. Una contraseña (clave simétrica) de al menos 6 caracteres, debe ser definida para encriptar los mensajes transferidos.

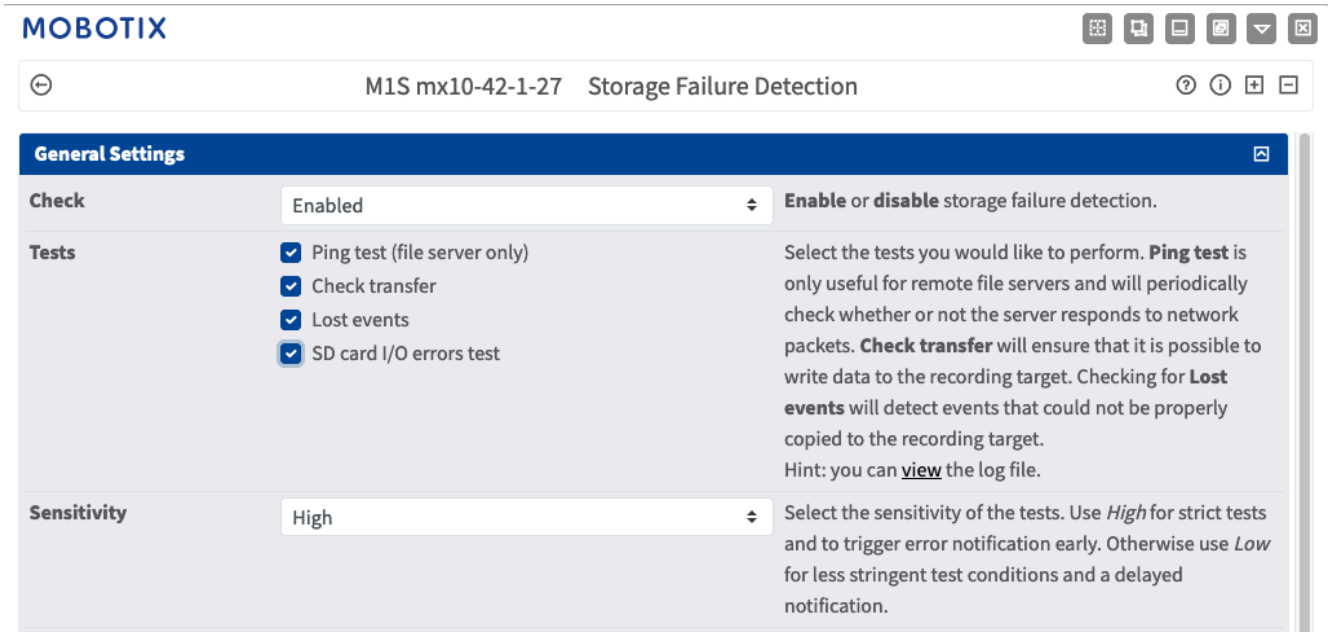
14. Activar la notificación de errores

Menú Admin > Información del sistema > Notificación de errores

El cuadro de diálogo Notificación de Errores proporciona varias opciones para obtener notificaciones (correo electrónico, notificaciones IP, llamadas VoIP, etc...) en caso de reinicio o errores que se detecten dentro de los differentes sistemas de la cámara. Esta herramienta puede ayudar a los administradores del sistema a asegurarse de que todas las cámaras MOBOTIX funcionan correctamente.

15. Activar la detección de fallos de almacenamiento

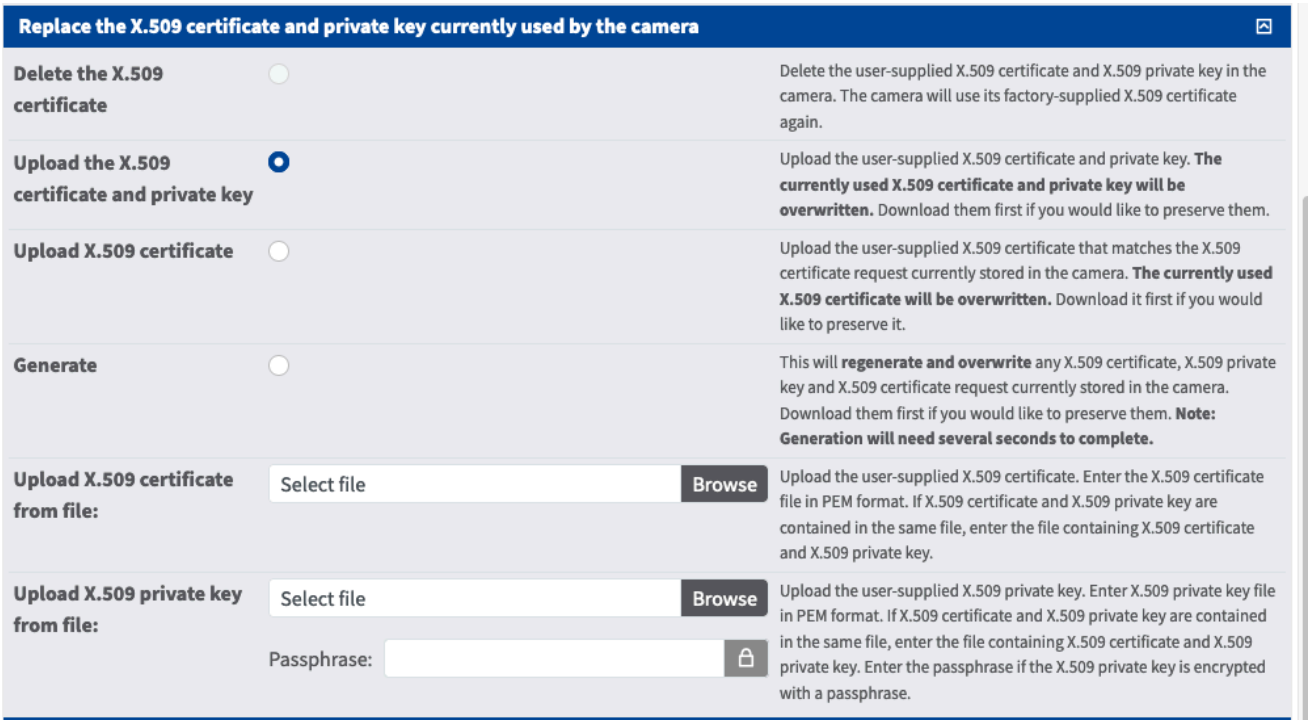
Menú Admin > Almacenamiento > Detección de fallos de almacenamiento



Utilice el cuadro de diálogo Detección de Fallo de Almacenamiento para configurar pruebas que supervisen constantemente el objetivo de almacenamiento externo (servidor de archivos o dispositivo Flash) que la cámara está utilizando como buffer de anillo externo. La cámara monitorizará activamente su objetivo de almacenamiento e informará de problemas con la grabación de vídeo utilizando los métodos de notificación especificados en este cuadro de diálogo.

16. Generar y cargar certificados X.509 personalizados

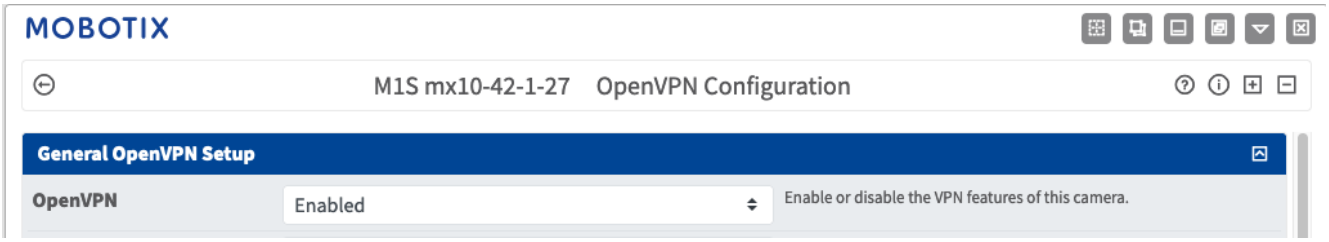
Menú Admin > Configuración de red > Servidor Web (para expertos)



La carga de un certificado personalizado firmado por una CA (Autoridad de Certificación) de confianza garantizará la confidencialidad y autenticidad de todas las conexiones establecidas a través de HTTPS (SSL/TLS).

17. Configurar el cliente OpenVPN para conexiones remotas

Menú Admin > Configuración de red > Configuración del cliente OpenVPN



Para optimizar la seguridad en caso de conexiones remotas, es posible aprovechar el cliente OpenVPN integrado para establecer un túnel VPN (red privada virtual) entre la cámara y el host remoto.

Crear una conexión OpenVPN requiere un servidor correspondiente, que proporcione acceso seguro a la cámara. Para ello, podrías ejecutar tu propio servidor OpenVPN o utilizar el servicio de un proveedor de OpenVPN.
Para más información sobre OpenVPN, visite el sitio web *de la comunidad OpenVPN*.

18. Evite exponer la cámara a Internet a menos que sea estrictamente necesario

El acceso remoto a la cámara debe concederse conscientemente para reducir el riesgo de ataques. Si es necesario un acceso remoto, asegúrese de respetar las normas mencionadas anteriormente para limitar la posibilidad de conectarse únicamente a los usuarios previstos.

19. Utilizar VLAN para separar la red de CCTV (nivel de seguridad empresarial)

En entornos empresariales es una buena práctica mantener la red de CCTV (cámaras IP, NVR y estaciones de trabajo VMS) separada del resto de hosts para evitar accesos no autorizados y evitar congestiones de tráfico.

20. Activar IEEE 802.1X (nivel de seguridad empresarial)

Menú Admin > Configuración de red > Interfaz Ethernet (para expertos) > IEEE 802.1X

Este estándar internacional se utiliza para el control de acceso a la red (NAC) basado en puertos. Este procedimiento requiere que todos los dispositivos de red (es decir, también la cámara MOBOTIX) necesiten autenticarse en el conmutador para obtener una conexión de red. Los dispositivos de red sin la autenticación adecuada serán rechazados.

Pregunte a su administrador de red si IEEE 802.1X es compatible o necesario. Asegúrese de que el switch al que está conectada la cámara (autenticador) se ha configurado en consecuencia. En general, el switch (autenticador) también necesita un servidor de autenticación, como un servidor RADIUS. El procedimiento de autenticación está controlado por el servidor de autenticación. Asegúrese de que la cámara y el servidor de autenticación utilizan siempre el mismo procedimiento.

21. Compruebe regularmente el archivo de registro del servidor web.

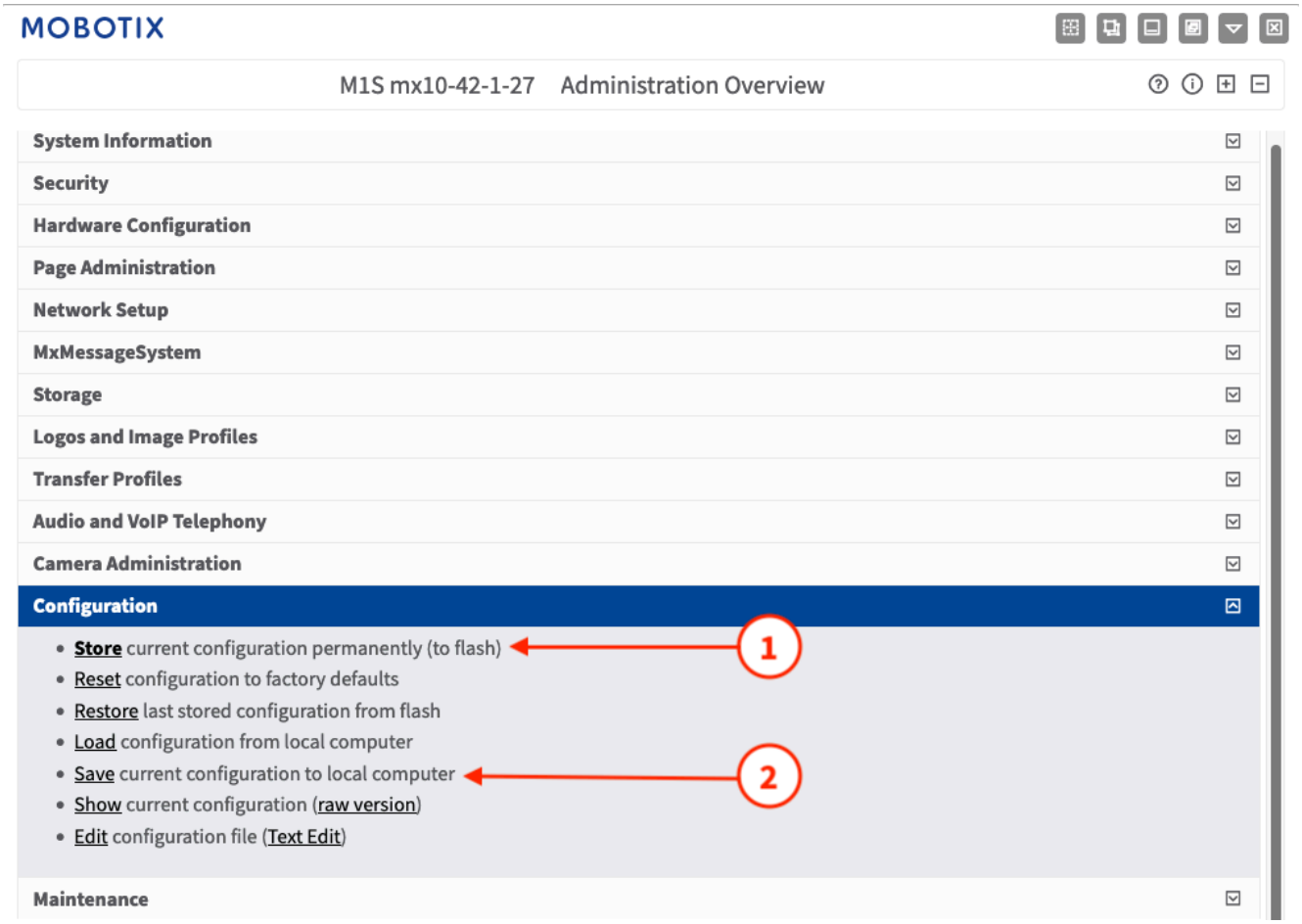
Menú Admin > Seguridad > Archivo de registro del servidor web

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

El Archivo de Registro del Servidor Web presenta todos los intentos de acceso y la información de fecha/hora con los correspondientes mensajes de estado del servidor web, así como el nombre de host del ordenador que accede. Los intentos de acceso no autorizados podrían ser la señal de alarma para los administradores de sistemas que deseen revisar la solidez de su red.

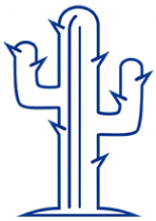
22. Guarde los archivos de configuración de copia de seguridad en un lugar seguro

Admin Menu > Configuración > Almacenar y guardar la configuración actual en el ordenador local



Aunque las credenciales de la cámara (contraseñas de usuario) están codificadas en el archivo de configuración de la cámara, cualquier archivo de copia de seguridad de la configuración debe guardarse en un lugar seguro; además, es aconsejable cifrar el archivo con una frase de contraseña para mayor seguridad.

Enhorabuena - ¡tu cámara MOBOTIX ya es cibersegura!



Configuración VMS (sistema de gestión de vídeo)

1. Crear cuentas de usuario en el ordenador en uso

2. Crear cuentas de usuario en MxMC

3. Limitar los derechos a los usuarios del VMS

4. Evitar el uso de la cuenta de administrador para acceder a las cámaras a través de MxMC

5. Activar el "Auto log-off"

Enhorabuena: ¡tu sistema de gestión de vídeo ya es ciberseguro!

Configuración NAS (Network Attached Storage)

1. Coloca el dispositivo utilizado para almacenar las grabaciones en un lugar seguro

2. Establezca una contraseña segura para la cuenta administrativa

3. Establecer una cuenta de usuario estándar (derechos limitados) para los dispositivos MOBOTIX

4. Cifrar los volúmenes

5. Utilice un nivel RAID que garantice la redundancia de los datos

Enhorabuena: su sistema de almacenamiento en red ya es ciberseguro.