



Guía de ciberprotección

Cómo endurecer Su sistema de vídeo MOBOTIX

Cámara - VMS - NAS



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.

Avisos sobre derechos de autor: Todos los derechos reservados. MOBOTIX, el logotipo de MOBOTIX AG y MxAnalytics son marcas registradas de MOBOTIX AG en la Unión Europea, EE.UU. y otros países. © MOBOTIX AG 2024

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](#)

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)• 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)	
Maintenance	☑

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. Cambiar la contraseña de administrador por defecto

Menú Admin > Seguridad > Usuarios y contraseñas

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.

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

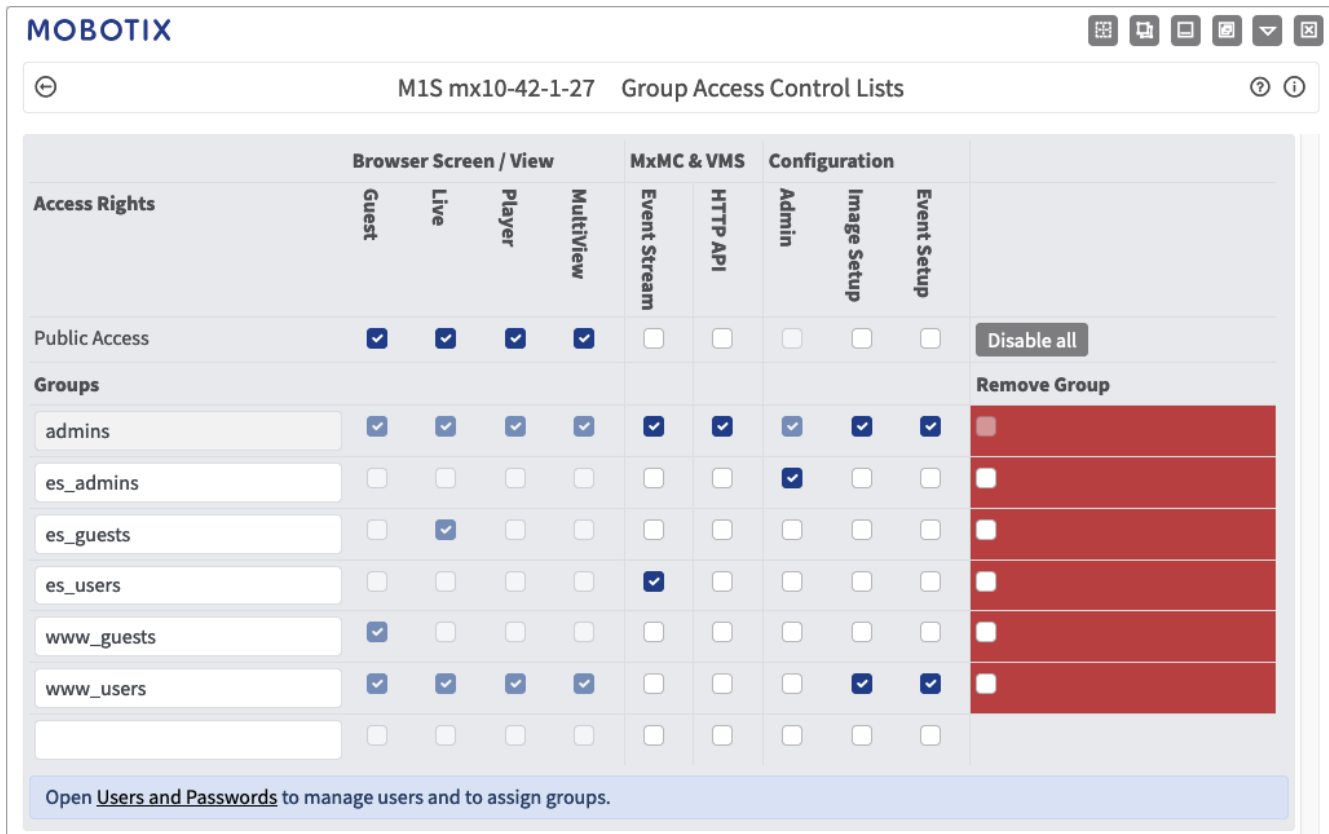
Menú Admin > Seguridad > Usuarios y contraseñas

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



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 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 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"/>	<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.

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

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	Disabled	Enable or disable Access Control.
Strict Mode	Disabled	Enable or disable Strict Mode.

Access Rules for Allow

Mode	IP Address/Subnet/Domain	Examples
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, 192.168.1.0/255.255.255.0, ftp.mobotix.com

If no match is found:

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

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

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

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

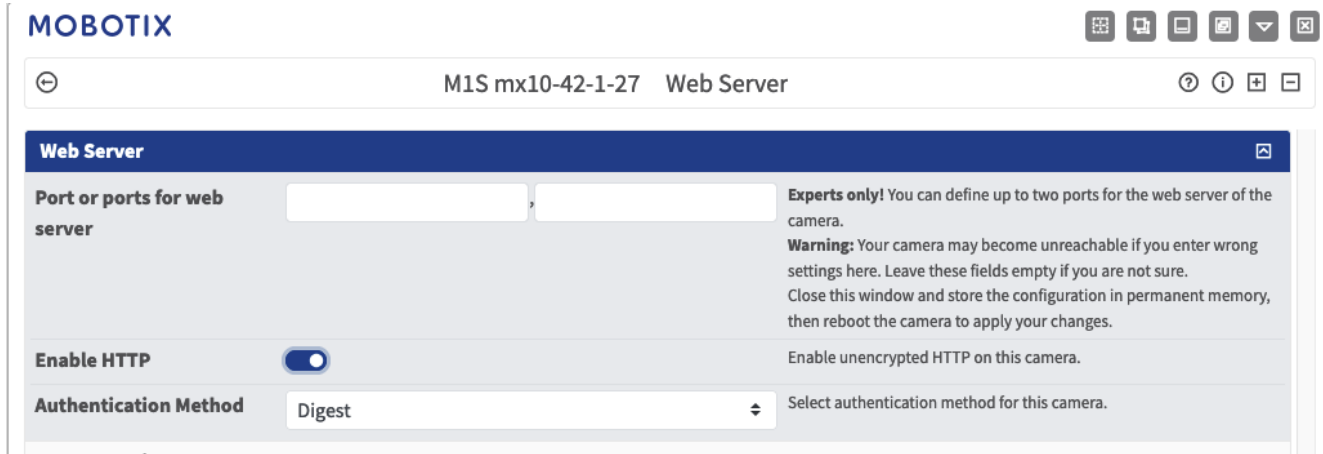
The screenshot shows the MOBOTIX web interface for configuration. The page title is 'Language and Start Page'. The 'Page Options' section is expanded, showing several settings:

- Select Start Page**: [checked]
- Page Design**: [checked]
- Dialog Options**: [checked]
- Page Options**: [checked]
- 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 Live page.)
- Refresh Rate for Guest Access**: Maximum: 2 fps, Default: 1 fps (Maximum and default image refresh rate on the Guest page.)
- Refresh Rate for User Access**: Maximum: max fps, Default: 16 fps (Maximum and default image refresh rate on the Live page.)
- Operating Mode**: Server Push (Default operating mode of Live 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**: [checked]

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 tráfico de red extra generado por los rastreadores.

10. Activar autenticación Digest

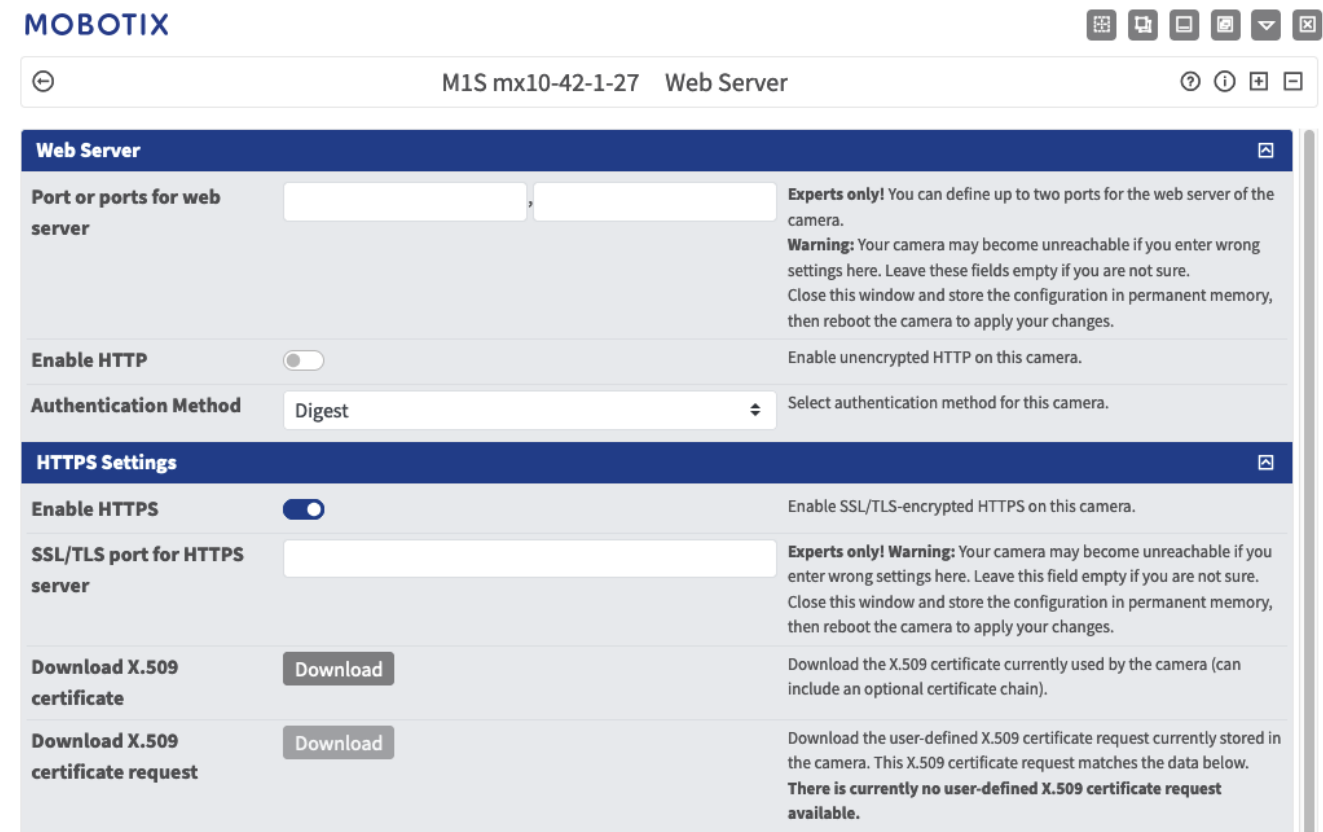
Menú Admin > Configuración de red > Servidor Web (para expertos) > Servidor Web



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

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.

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

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).

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 diferentes 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

The screenshot shows the MOBOTIX web interface for the 'Storage Failure Detection' settings of camera 'M1S mx10-42-1-27'. The page has a dark blue header with the MOBOTIX logo and navigation icons. Below the header is a breadcrumb trail and a title bar. The main content area is titled 'General Settings' and contains three sections: 'Check', 'Tests', and 'Sensitivity'. The 'Check' section has a dropdown menu set to 'Enabled' and a description: 'Enable or disable storage failure detection.' The 'Tests' section has four checked checkboxes: 'Ping test (file server only)', 'Check transfer', 'Lost events', and 'SD card I/O errors test'. A description explains that 'Ping test' is for remote file servers, 'Check transfer' ensures data can be written, and 'Lost events' detects copying issues. A hint suggests viewing the log file. The 'Sensitivity' section has a dropdown menu set to 'High' and a description: 'Select the sensitivity of the tests. Use High for strict tests and to trigger error notification early. Otherwise use Low for less stringent test conditions and a delayed notification.'

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)

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="🔒"/>

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

The screenshot shows the MOBOTIX web interface for 'M1S mx10-42-1-27'. The page title is 'OpenVPN Configuration'. Under the 'General OpenVPN Setup' section, the 'OpenVPN' status is set to 'Enabled'. A description below the dropdown reads: 'Enable or disable the VPN features of this camera.'

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

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	☑

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.