Guía de protección cibernética

Cómo fortalecer el sistema de vídeo MOBOTIX

Cámara • VMS • NAS

MOBOTIX

Acerca de esta guía

Los ataques cibernéticos contra el software y el hardware conectados a Internet son un problema que no deja de crecer. En los últimos años, los atacantes se centran cada vez más en explotar los eslabones más débiles de un perímetro de seguridad a fin de lograr el acceso a aplicaciones esenciales y datos confidenciales. Con la tecnología de videovigilancia como parte vital de la seguridad de una ubicación, que a menudo reside en una red corporativa compartida, los dispositivos de videovigilancia se están convirtiendo cada vez más en el blanco de los ataques cibernéticos dirigidos. En respuesta a esta tendencia emergente, MOBOTIX ha desarrollado un conjunto de **funciones y herramientas integradas** que permite a los administradores de seguridad de TI configurar cada dispositivo como parte de un enfoque multicapa de la seguridad cibernética.

Estas herramientas, cuando se usan junto con otros elementos de seguridad, como cortafuegos y segmentación de red, pueden reducir la superficie de ataque expuesta de 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 mejor protección contra los ataques cibernéticos, junto con la guía de mejores prácticas para crear una infraestructura de videovigilancia segura.

Tenga en cuenta: Este documento tiene como objeto proporcionar al administrador responsable una visión general completa de todas las medidas posibles para fortalecer el sistema MOBOTIX. Con respecto a la aplicación individual, y para evitar reconfiguraciones, puede que no sea útil llevar a cabo todos y cada uno de los procedimientos que se explican en esta guía.

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

Configuración de las cámaras

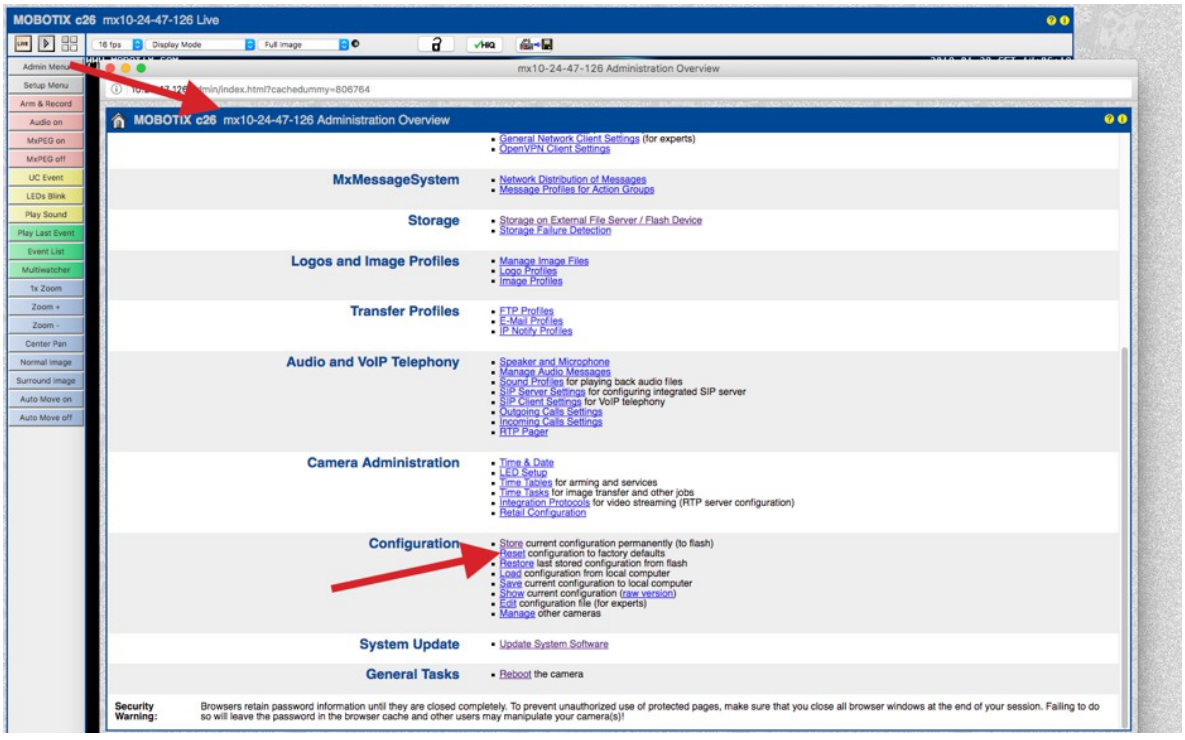
1. Mantenga actualizado el firmware de las cámaras

El firmware de MOBOTIX se puede descargar de forma gratuita desde nuestro sitio web: *www.mobotix.com > Soporte > Download Center*

¿No está seguro de cómo proceder? Consulte esta guía compacta: *www.mobotix.com > Soporte > Download Center > Documentación > Folletos y Guías > Guía compacta > Mx_CG_FirmwareUpdate.pdf*

2. Restablezca la configuración a los ajustes de fábrica

Admin Menu > Configuración > Reset configuración por defecto



3. Cambie la contraseña de administrador por defecto

Admin Menu > Seguridad > Usuarios y Contraseñas

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

Una vez que haya acabado de configurar usuarios, contraseñas y grupos, debería almacenar siempre los ajustes en la memoria permanente de la cámara. De lo contrario, la configuración modificada sólo se conservará hasta el siguiente reinicio de la cámara. Utilice el botón Close al final del cuadro de diálogo, ya que este le pedirá automáticamente guardar la configuración de la cámara en su memoria permanente.

Asegúrese de guardar la información de contraseñas en un lugar protegido. Se debería tener especial cuidado de mantener la contraseña de al menos un usuario del grupo admin. Sin la contraseña, el acceso administrativo a la cámara ya no será posible y no hay posibilidad de recuperar la contraseña. Asimismo, tampoco es posible recuperar la contraseña de una configuración guardada permanentemente.

Cómo crear una contraseña segura:

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

Política de restablecimiento de contraseñas: Si la contraseña de administrador ya no está disponible, la cámara debe ser reseteada a través de MOBOTIX por un precio.

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

Admin Menu > 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 Admin Menu > Group Access Control List

5. Cree diferentes usuarios y asígnelos a los grupos correctos

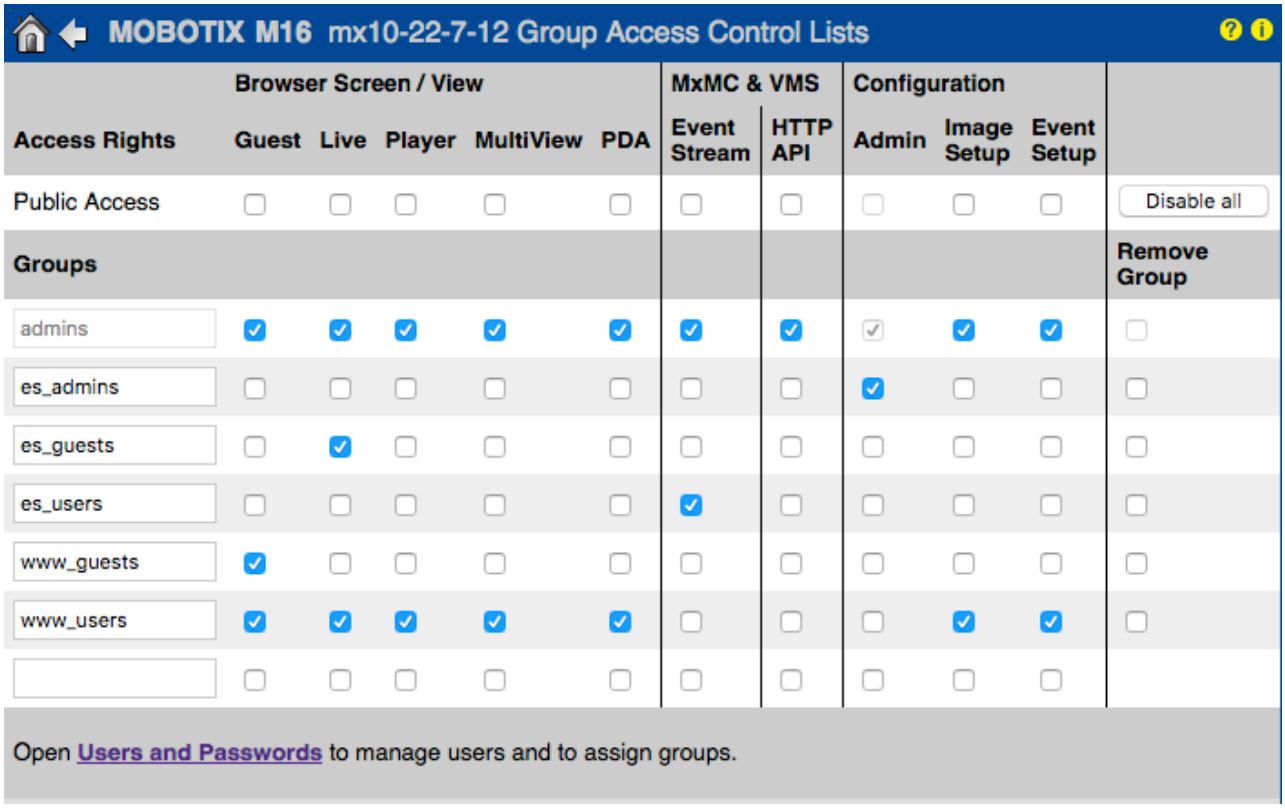
Admin Menu > Seguridad > Usuarios y Contraseñas

Es aconsejable crear un usuario para cada persona con autorización para acceder a la cámara. Se pueden crear hasta 100 usuarios. Las acciones realizadas por los usuarios autorizados se registran en el archivo de registro del servidor web; esto ayuda a determinar “quién hizo qué” en caso de disputa.

Consulte la descripción anterior para crear contraseñas seguras.

6. Deshabilite el acceso público

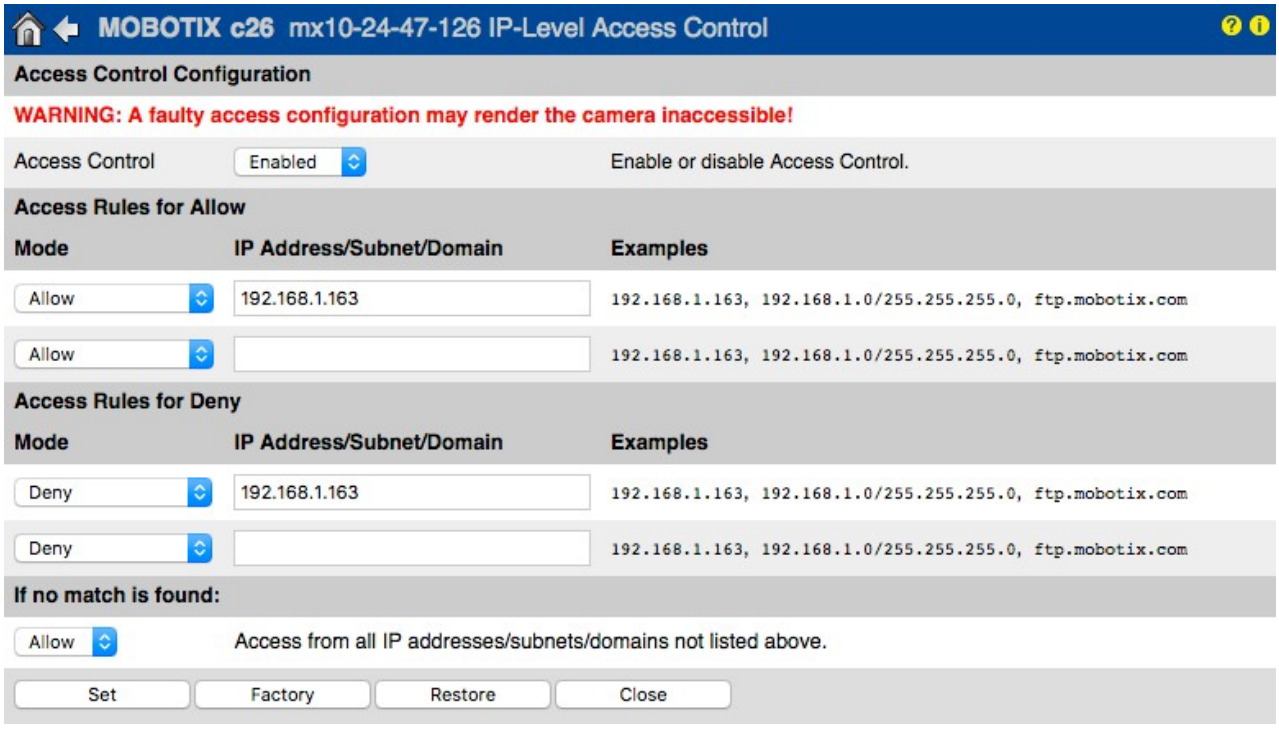
Admin Menu > Seguridad > Listas de Control de Grupos de Acceso



El acceso público, si se habilita, permite acceder a recursos específicos de la cámara sin autenticación. Se recomienda encarecidamente deshabilitar el acceso público para evitar que usuarios no autorizados puedan mostrar la transmisión en vivo o las grabaciones de la cámara, o incluso controlar la cámara (por ejemplo, cambiar su configuración o ejecutar acciones).

7. Habilite la lista de control de acceso a nivel IP

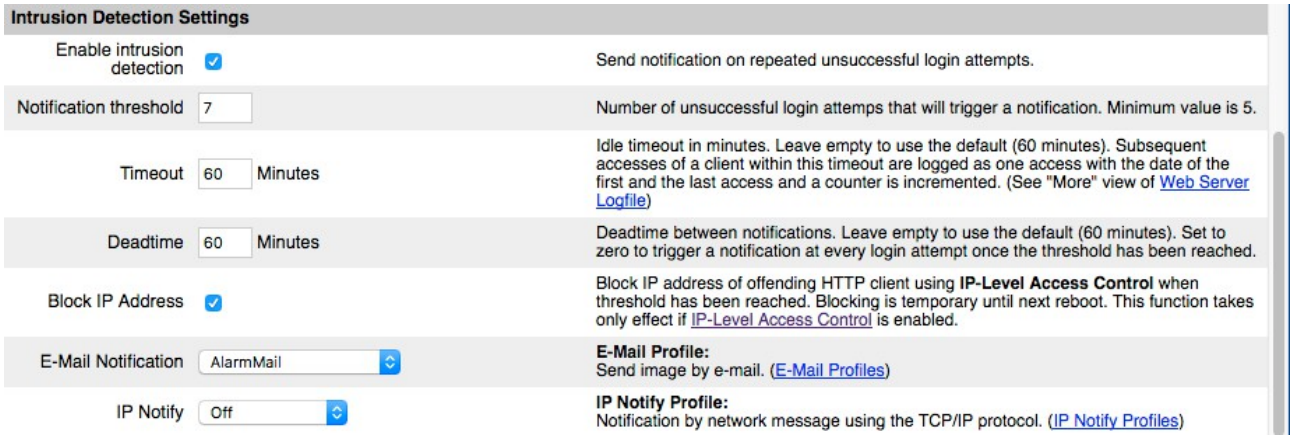
Admin Menu > Seguridad > Control de Acceso a Nivel IP



El cuadro de diálogo Access Control permite gestionar las direcciones IP, las subredes y los nombres de dominio que pueden y no pueden acceder a la cámara. Esta opción de control del 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 por contraseña. Si un ordenador no tiene acceso a nivel IP a la cámara, no hay posibilidad de llegar a la cámara desde ese ordenador. Si un ordenador tiene acceso a nivel IP a la cámara, la autenticación de usuario por contraseña será el siguiente paso, según se especifique en el cuadro de diálogo Users and Passwords.

8. Habilite la detección de intrusos con notificación y bloqueo de la dirección IP ilegal

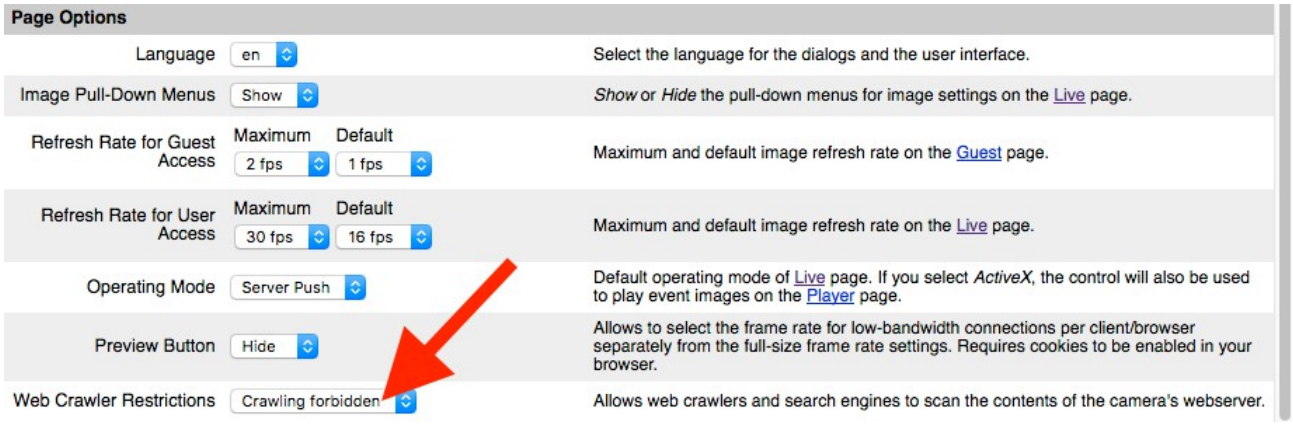
Admin Menu > Configuración de Red > Servidor Web (para expertos) > Configuración de Detección de Intrusos



Esta función proporciona una defensa automática frente a los ataques. Si un intruso intenta acceder a la cámara utilizando métodos de “fuerza bruta” para averiguar nombres de usuario y contraseñas, la cámara puede enviar una alerta y bloquear automáticamente la dirección IP ilegal después de un cierto número de intentos fallidos.

9. Compruebe que el rastreo web está prohibido

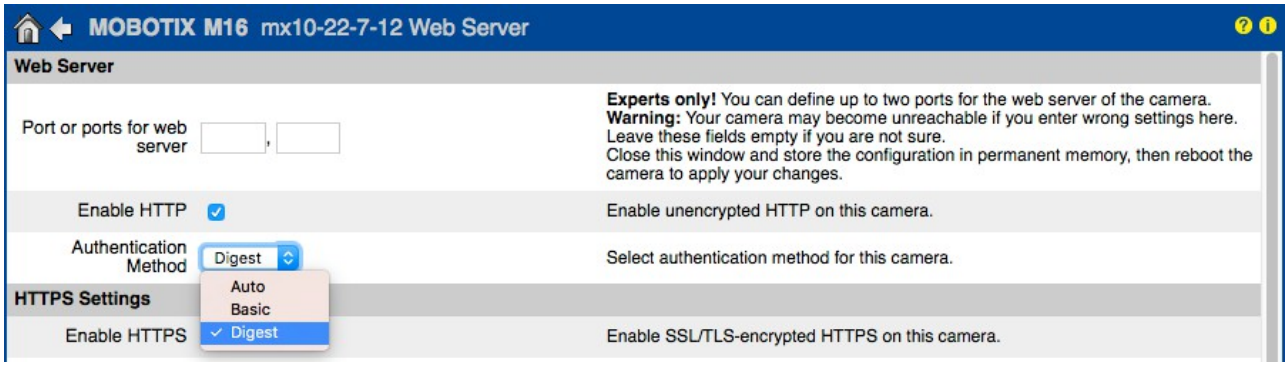
Admin Menu > Administración de Página > Página de Idioma y Inicio > Opciones de Página



Con este parámetro, puede evitar que motores de búsqueda web, otros robots automáticos y rastreadores web escaneen el contenido del servidor web de la cámara. Por lo general, no le interesa que un motor de búsqueda indexe todas las imágenes y las páginas que se encuentran en una cámara. Asegúrese de permitir el rastreo sólo si es consciente de los riesgos de seguridad adicionales y el mayor tráfico de red que generan los rastreadores.

10. Habilite la autenticación digest

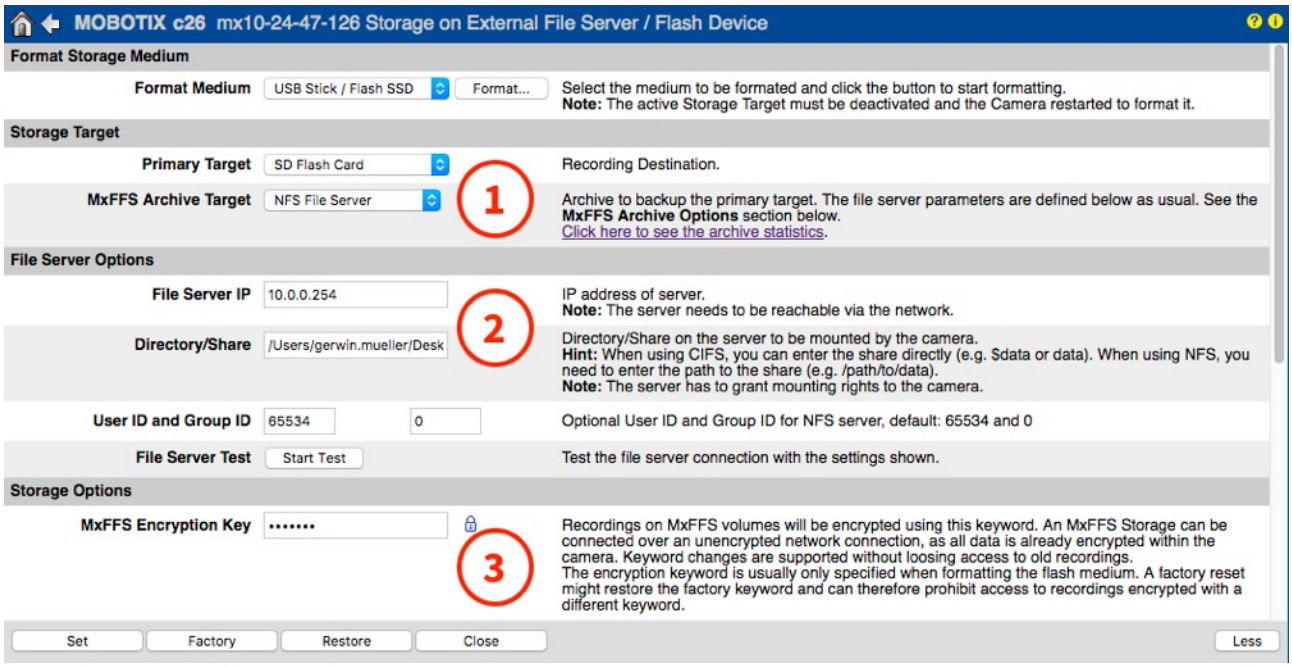
Admin Menu > Configuración de Red > Servidor Web (para expertos) > Servidor Web



La autenticación de acceso digest es uno de los métodos acordados que un servidor web (es decir, la cámara MOBOTIX) puede usar para negociar credenciales, como nombres de usuario o contraseñas, con un cliente (es decir, un navegador web). Con la autenticación digest, la contraseña nunca se envía de forma explícita, y el nombre de usuario se puede codificar.

11. Establezca una clave de cifrado para las grabaciones

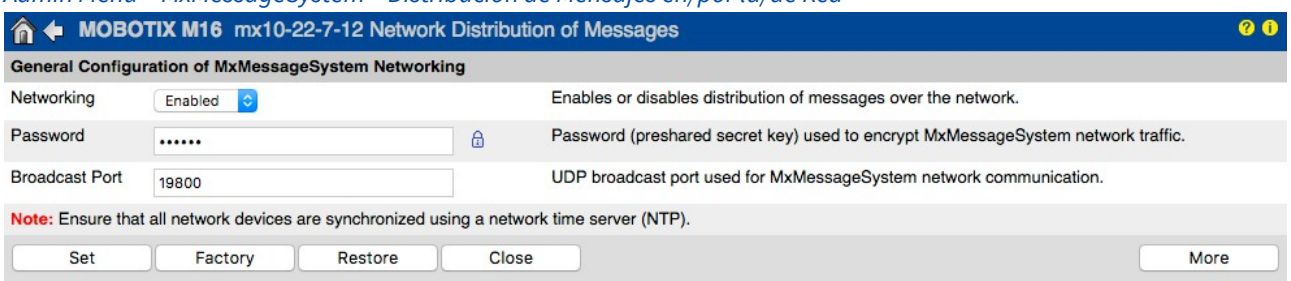
Admin Menu > Almacenamiento > Almacenamiento en Servidor de Ficheros Externo/Dispositivo Flash



Se puede configurar una clave para cifrar las grabaciones almacenadas en el almacenamiento interno (tarjeta microSD/unidad flash USB) y la grabación archivada en el servidor de archivos externo (SMB/NFS).

12. Cambie la contraseña por defecto de MxMessage (si está habilitada)

Admin Menu > MxMessageSystem > Distribución de Mensajes en/por la/de Red



MxMessageSystem permite la transferencia de mensajes entre cámaras a través de la red. Se debe definir una contraseña (clave simétrica) de al menos 6 caracteres para cifrar los mensajes transferidos.

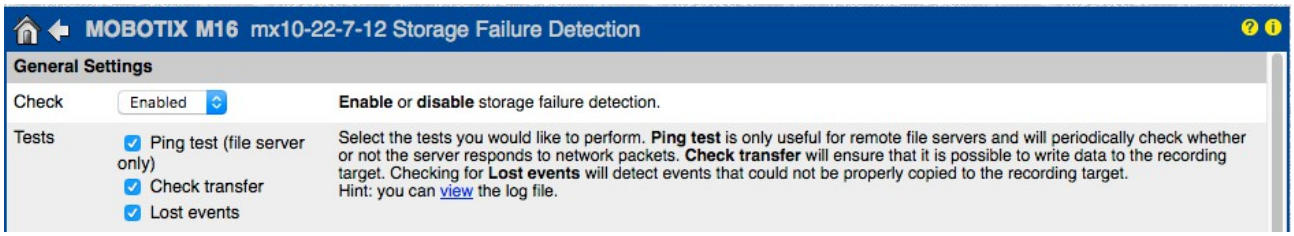
13. Habilite la notificación de errores

Admin Menu > Información del Sistema > Notificación de Error

El cuadro de diálogo Error Notification ofrece varias opciones para recibir notificaciones (correo electrónico, notificaciones IP, llamadas mediante VoIP, etc.) en caso de reinicio o por errores detectados en los diferentes sistemas de la cámara. Esta herramienta ayuda a los administradores del sistema a asegurarse de que todas las cámaras MOBOTIX funcionan correctamente.

14. Habilite la detección de fallos de almacenamiento

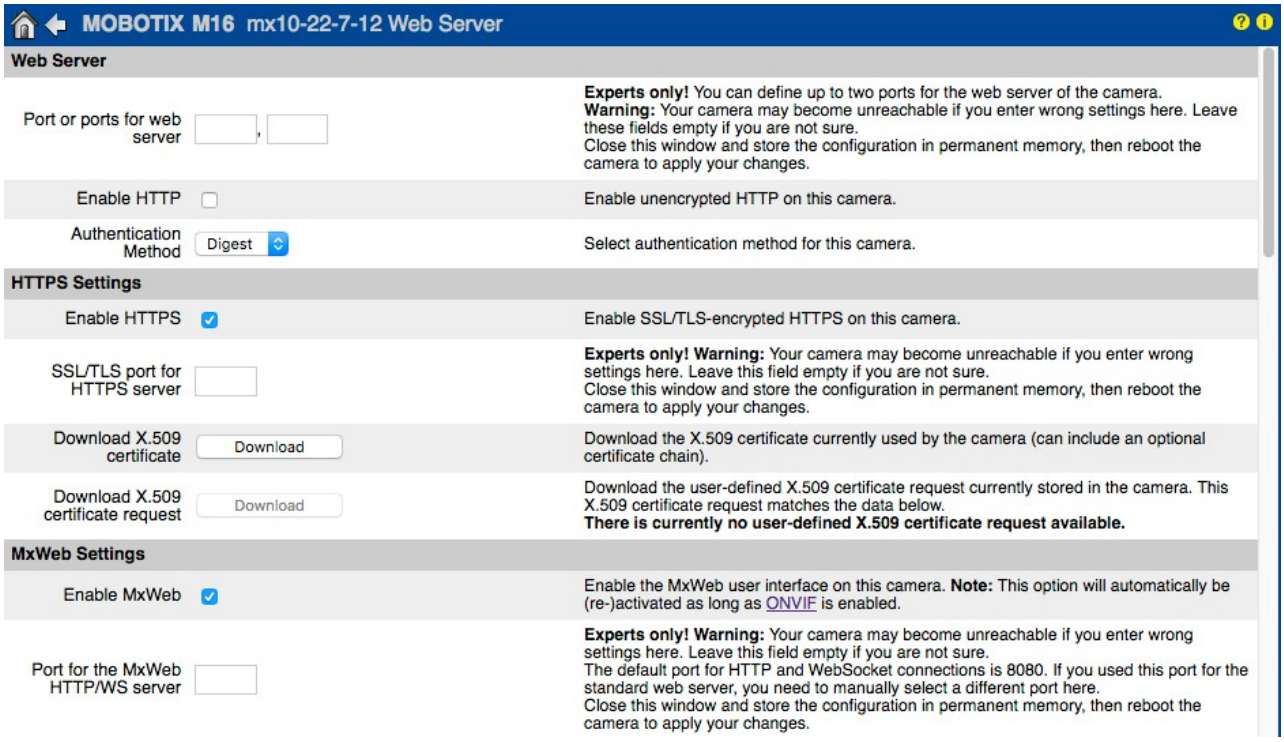
Admin Menu > Almacenamiento > Detección de Fallo de Almacenamiento



Use el cuadro de diálogo Storage Failure Detection para configurar pruebas que monitoricen constantemente el destino de almacenamiento externo (servidor de archivos o dispositivo flash) que la cámara utiliza como búfer circular externo. La cámara monitorizará activamente el destino de almacenamiento y le informará de problemas en la grabación de vídeo de acuerdo con los métodos de notificación especificados en este cuadro de diálogo.

15. Cambie los puertos por defecto del servidor web (para el acceso remoto)

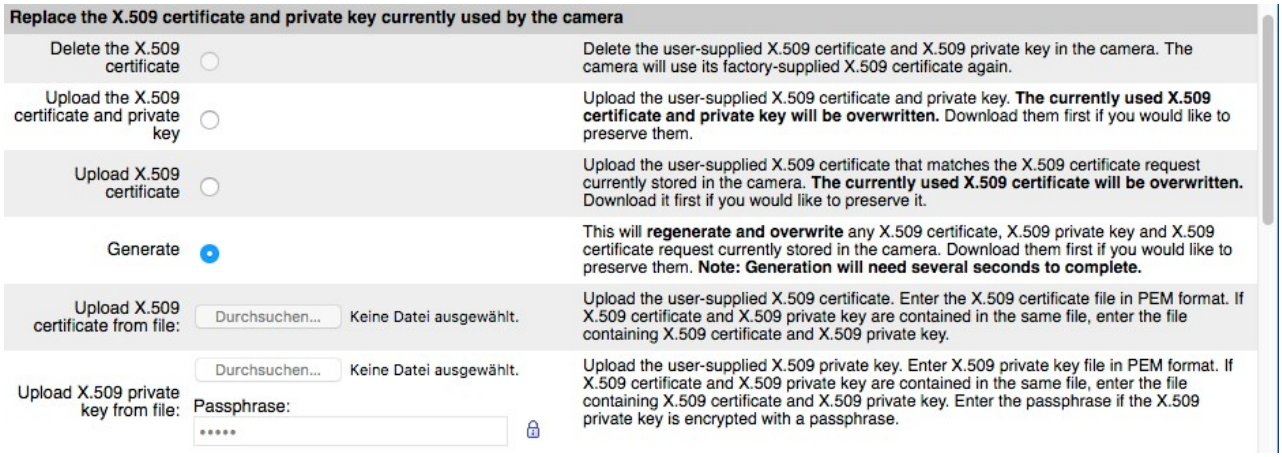
Admin Menu > Configuración de Red > Servidor Web (para expertos)



Los puertos estándar (80 TCP para HTTP y 443 TCP para HTTPS) son más propensos a los ataques. Sustituir estos puertos predeterminados por otros personalizados puede aumentar aún más la seguridad de la cámara.

16. Genere y cargue certificados personalizados X.509

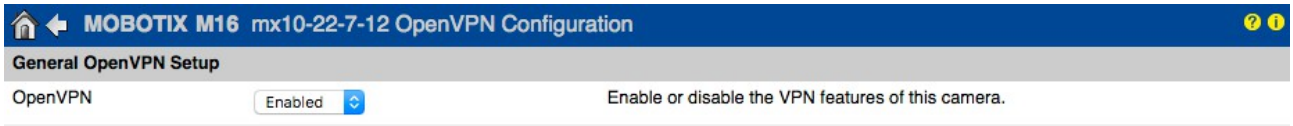
Admin Menu > Configuración de Red > Servidor Web (para expertos)



Cargar un certificado personalizado firmado por una CA (autoridad de certificación) de confianza garantizará la confidencialidad y la autenticidad de todas las conexiones establecidas a través de HTTPS (SSL/TLS).

17. Configure el cliente de OpenVPN para conexiones remotas

Admin Menu > Configuración de Red > Configuración de client OpenVPN



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

Crear una conexión de OpenVPN requiere un servidor correspondiente, el cual proporciona un acceso seguro a la cámara. Para hacerlo, puede ejecutar su propio servidor de OpenVPN o usar el servicio de un proveedor de OpenVPN.
Para obtener más información sobre OpenVPN, visite el sitio web *OpenVPN Community*.

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

El acceso remoto a la cámara debe concederse de manera consciente para reducir el riesgo de ataques. Si fuera necesario el acceso remoto, asegúrese de observar las reglas previamente indicadas para limitar la conexión únicamente a los usuarios previstos.

19. Haga uso de redes VLAN para separar la red de CCTV (nivel de seguridad de empresa)

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

20. Habilite IEEE 802.1X (nivel de seguridad de empresa)

Admin Menu > Configuración de Red > Interfaz Ethernet (para expertos) > IEEE 802.1X

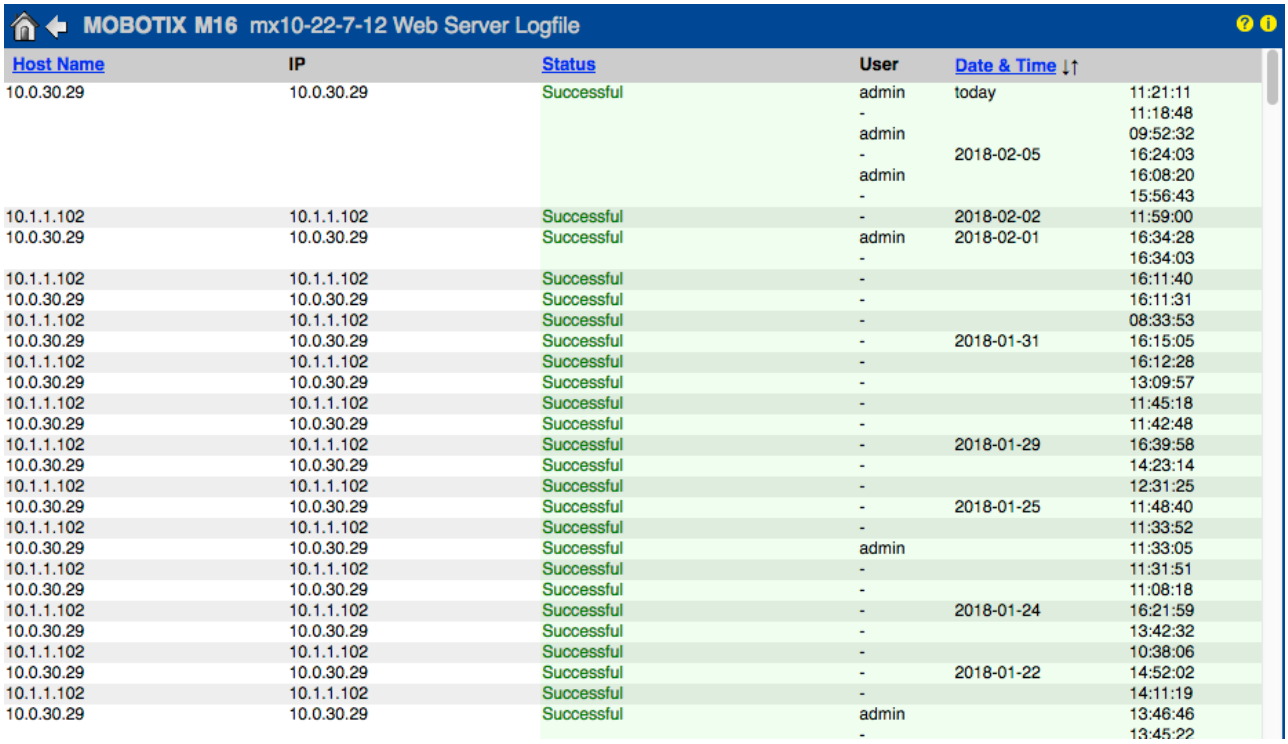
Esta norma internacional se utiliza para el control de acceso a la red (NAC) basado en puertos. Este procedimiento requiere que todos los dispositivos de la red (también la cámara MOBOTIX) se autentiquen en el conmutador para obtener una conexión de red. Los dispositivos de red sin una autenticación adecuada son rechazados.

Pregunte a su administrador de red si la norma IEEE 802.1X es compatible o necesaria. Asegúrese de que el conmutador al que está conectada la cámara (autenticador) se haya configurado en consecuencia. En general, el conmutador (autenticador) también necesita un servidor de autenticación, como un servidor RADIUS. El

procedimiento de autenticación lo controla el servidor de autenticación. Asegúrese de que la cámara y el servidor de autenticación utilizan siempre el mismo procedimiento.

21. Compruebe con regularidad el archivo de registro del servidor web

Admin Menu > Seguridad > Registro de Servidor Web

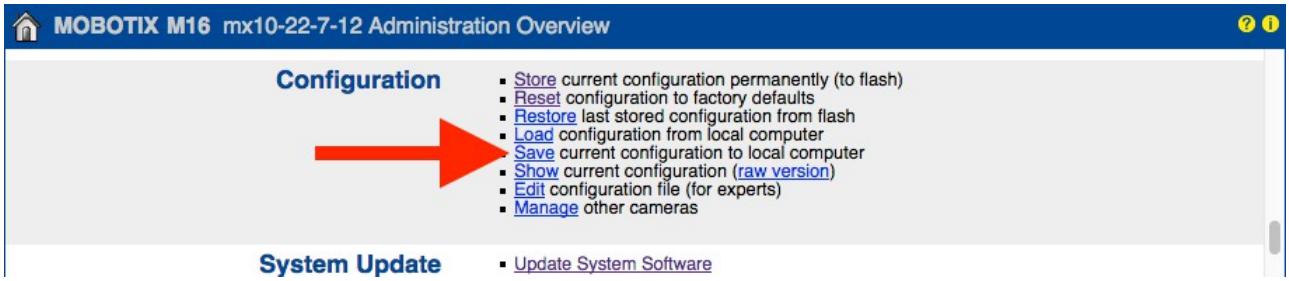


Host Name	IP	Status	User	Date & Time ↓↑	
10.0.30.29	10.0.30.29	Successful	admin	today	11:21:11
			-		11:18:48
			admin		09:52:32
			-	2018-02-05	16:24:03
			admin		16:08:20
			-		15:56:43
10.1.1.102	10.1.1.102	Successful	-	2018-02-02	11:59:00
10.0.30.29	10.0.30.29	Successful	admin	2018-02-01	16:34:28
			-		16:34:03
10.1.1.102	10.1.1.102	Successful	-		16:11:40
10.0.30.29	10.0.30.29	Successful	-		16:11:31
10.1.1.102	10.1.1.102	Successful	-		08:33:53
10.0.30.29	10.0.30.29	Successful	-	2018-01-31	16:15:05
10.1.1.102	10.1.1.102	Successful	-		16:12:28
10.0.30.29	10.0.30.29	Successful	-		13:09:57
10.1.1.102	10.1.1.102	Successful	-		11:45:18
10.0.30.29	10.0.30.29	Successful	-		11:42:48
10.1.1.102	10.1.1.102	Successful	-	2018-01-29	16:39:58
10.0.30.29	10.0.30.29	Successful	-		14:23:14
10.1.1.102	10.1.1.102	Successful	-		12:31:25
10.0.30.29	10.0.30.29	Successful	-	2018-01-25	11:48:40
10.1.1.102	10.1.1.102	Successful	-		11:33:52
10.0.30.29	10.0.30.29	Successful	admin		11:33:05
10.1.1.102	10.1.1.102	Successful	-		11:31:51
10.0.30.29	10.0.30.29	Successful	-		11:08:18
10.1.1.102	10.1.1.102	Successful	-	2018-01-24	16:21:59
10.0.30.29	10.0.30.29	Successful	-		13:42:32
10.1.1.102	10.1.1.102	Successful	-		10:38:06
10.0.30.29	10.0.30.29	Successful	-	2018-01-22	14:52:02
10.1.1.102	10.1.1.102	Successful	-		14:11:19
10.0.30.29	10.0.30.29	Successful	admin		13:46:46
			-		13:45:22

El archivo de registro del servidor web contiene todos los intentos de acceso y la información de fecha/hora, junto con los mensajes de estado correspondientes del servidor web, así como el nombre de host del ordenador que accede al sistema. Los intentos de acceso no autorizados pueden actuar como alarma para los administradores del sistema y una invitación a revisar la fortaleza de su red.

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

Admin Menu > Configuración > Guardar configuración actual al ordenador local



Aunque las credenciales de la cámara (contraseñas de usuario) están codificadas dentro del archivo de configuración de la cámara, los archivos de copia de seguridad de la configuración deben mantenerse en un lugar seguro; además, es recomendable cifrar el archivo con una frase de contraseña para mayor seguridad.

Enhorabuena. Su cámara MOBOTIX ahora es cibernéticamente segura.

Configuración de VMS (sistema de gestión de vídeo)

1. Cree cuentas de usuario en el ordenador en uso

2. Cree cuentas de usuario en MxMC

3. Limite los derechos a los usuarios de VMS

4. Evite usar la cuenta de administrador para acceder a las cámaras a través de MxMC

5. Habilite la opción de desconexión automática

Enhorabuena. Su sistema de gestión de vídeo ahora es cibernéticamente seguro.

Configuración del NAS (almacenamiento conectado a la red)

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

2. Establezca una contraseña segura para la cuenta de administrador

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

4. Cifre los volúmenes

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

Enhorabuena. Su almacenamiento conectado a la red ahora es cibernéticamente seguro.