MOBOTIX HUB – Guía de endurecimiento

Inhaltsverzeichnis

1 Derechos de autor, marcas comerciales y exención de responsabilidad

Marcas

MOBOTIX HUB es una marca registrada de MOBOTIX AG.
Microsoft y Windows son marcas comerciales registradas de Microsoft Corporation. App Store es una marca de servicio de Apple Inc. Android es una marca comercial de Google Inc.
Todas las demás marcas comerciales mencionadas en este documento son marcas comerciales de sus respectivos propietarios.

Renuncia

Este texto está destinado únicamente a fines de información general y se ha tenido el debido cuidado en su preparación.
Cualquier riesgo que surja del uso de esta información recae en el destinatario, y nada de lo aquí contenido debe interpretarse como constitutivo de ningún tipo de garantía.
MOBOTIX AG se reserva el derecho de realizar ajustes sin previo aviso.
Todos los nombres de personas y organizaciones utilizados en los ejemplos de este texto son ficticios. Cualquier parecido con cualquier organización o persona real, viva o muerta, es pura coincidencia y no intencionada.
Este producto puede hacer uso de software de terceros para el que se pueden aplicar términos y condiciones específicos. Cuando ese sea el caso, puede encontrar más información en el archivo *3rd_party_software_terms_and_conditions.txt* se encuentra en la carpeta de instalación del sistema MOBOTIX HUB.

2 Introducción

En esta guía se describen las medidas de seguridad y física, así como las mejores prácticas que pueden ayudar a proteger su software de gestión de vídeo (VMS) MOBOTIX HUB frente a ciberataques. Esto incluye consideraciones de seguridad para el hardware y el software de los servidores, clientes y componentes de dispositivos de red de un sistema de videovigilancia.

Esta guía adopta controles estándar de seguridad y privacidad y los asigna a cada una de las recomendaciones. Eso hace que esta guía sea un recurso para el cumplimiento de los requisitos de seguridad de la industria y el gobierno, y de seguridad de la red.

2.1 ¿Qué es el "endurecimiento"?

El desarrollo y la implementación de medidas de seguridad y mejores prácticas se conoce como "endurecimiento". El endurecimiento es un proceso continuo de identificación y comprensión de los riesgos de seguridad y de adopción de las medidas adecuadas para contrarrestarlos. El proceso es dinámico porque las amenazas, y los sistemas a los que se dirigen, evolucionan continuamente.

La mayor parte de la información de esta guía se centra en la configuración y las técnicas de TI, pero es importante recordar que la seguridad física también es una parte vital del endurecimiento. Por ejemplo, use barreras físicas para los servidores y los equipos cliente, y asegúrese de que elementos como los recintos de las cámaras, las cerraduras, las alarmas antisabotaje y los controles de acceso sean seguros.

A continuación se indican los pasos prácticos para proteger un VMS:

1. Comprender los componentes que se deben proteger
2. Refuerce los componentes del sistema de vigilancia:
    1. Refuerce los servidores (físicos y virtuales) y los equipos y dispositivos cliente
    2. Endurecer la red
    3. Endurece las cámaras
3. Documentar y mantener la configuración de seguridad en cada sistema
4. Capacite e invierta en personas y habilidades, incluida su cadena de suministro

2.1.1 Público objetivo

Todos los miembros de una organización deben comprender al menos los conceptos básicos sobre la seguridad de redes y software. Los intentos de comprometer la infraestructura crítica de TI son cada vez más frecuentes, por lo que todos deben tomarse en serio el endurecimiento y la seguridad.

Esta guía proporciona información básica y avanzada para usuarios finales, integradores de sistemas, consultores y fabricantes de componentes.

- Las descripciones básicas ofrecen una visión general de la seguridad
- Las descripciones avanzadas proporcionan orientación específica de TI para reforzar los productos MOBOTIX HUB VMS. Además del software, también describe las consideraciones de seguridad para los componentes de hardware y dispositivo del sistema.

2.1.2 Recursos y referencias

Las siguientes organizaciones proporcionan recursos e información sobre las mejores prácticas de seguridad:

- Organización Internacional de Normalización (ISO),
- Instituto Nacional de Estándares y Tecnología (NIST) de los Estados Unidos (EE. UU.)
- Directrices de implementación técnica de seguridad (STIG) de la Administración de Sistemas de Información de Defensa (DISA) de EE. UU.

- Centro para la Seguridad en Internet
- Instituto SANS
- Alianza de seguridad en la nube (CSA)
- Grupo de Trabajo de Ingeniería de Internet (IETF)
- Normas británicas

Además, los fabricantes de cámaras proporcionan orientación para sus dispositivos de hardware.

Ver Apéndice 1 - Recursos en la página 103 para obtener una lista de referencias y Apéndice 2 - Acrónimos en la página 103 para obtener una lista de acrónimos.

Esta guía aprovecha los estándares y especificaciones nacionales, internacionales y de la industria. En particular, se refiere a la Publicación Especial 800-53 del Instituto Nacional de Normas y Tecnología del Departamento de Comercio de los Estados Unidos Controles de seguridad y privacidad para sistemas y organizaciones federales de información (http://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf).

El documento del NIST está escrito para el gobierno federal de los EE. UU.; sin embargo, es generalmente aceptado en la industria de la seguridad como el conjunto actual de mejores prácticas.

Esta guía hace referencia a información adicional sobre los controles de seguridad y los enlaces a ella. La guía puede hacer referencias cruzadas a los requisitos específicos de la industria y a otros estándares y marcos internacionales de seguridad y gestión de riesgos. Por ejemplo, el marco de ciberseguridad actual del NIST utiliza SP 800-53 Rev4 como base para los controles y la orientación. Otro ejemplo es el Apéndice H en SP 800-53 Rev 4, que contiene una referencia a los requisitos de ISO/IEC 15408, como los Criterios Comunes.

2.1.3 Componentes de hardware y dispositivos

Además del software, los componentes de una instalación de MOBOTIX HUB VMS suelen incluir dispositivos de hardware, como:

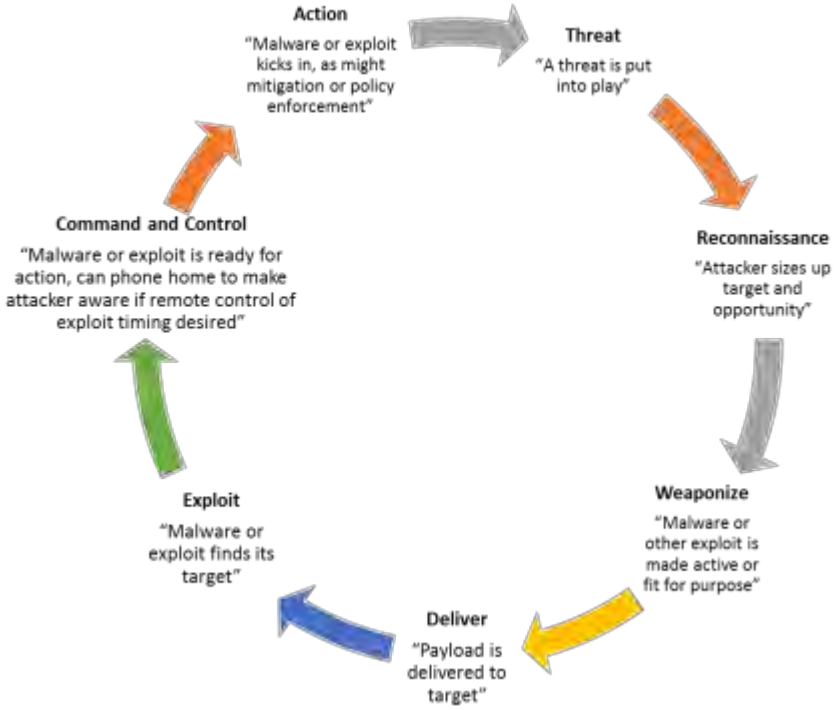
- Cámaras
- Codificadores
- Productos de red
- Sistemas de almacenamiento
- Servidores y equipos cliente (máquinas físicas o virtuales)
- Dispositivos móviles, como teléfonos inteligentes

Es importante incluir dispositivos de hardware en sus esfuerzos por reforzar la instalación de MOBOTIX HUB VMS. Por ejemplo, las cámaras suelen tener contraseñas predeterminadas. Algunos fabricantes publican estas contraseñas en línea para que los clientes puedan encontrarlas fácilmente. Desafortunadamente, eso significa que las contraseñas también están disponibles para los atacantes.
Este documento proporciona recomendaciones para dispositivos de hardware.

2.2 Amenazas cibernéticas y riesgos cibernéticos

Hay muchas fuentes de amenazas para un VMS, incluidos los ataques o fallos empresariales, tecnológicos, de procesos y humanos. Las amenazas tienen lugar a lo largo de un ciclo de vida. El ciclo de vida de las amenazas, a veces llamado "muerte cibernética" o "cadena de amenazas cibernéticas", se desarrolló para describir las etapas de las amenazas cibernéticas avanzadas.

Cada etapa del ciclo de vida de la amenaza lleva tiempo. La cantidad de tiempo para cada etapa es particular de la amenaza, o combinación de amenazas, y sus actores y objetivos.



El ciclo de vida de las amenazas es importante para la evaluación de riesgos, ya que muestra dónde se pueden mitigar las amenazas. El objetivo es reducir el número de vulnerabilidades y abordarlas lo antes posible. Por ejemplo, disuadir a un atacante que está sondeando un sistema en busca de vulnerabilidades puede eliminar una amenaza.

El endurecimiento pone en marcha acciones que mitigan las amenazas en cada fase del ciclo de vida de las amenazas. Por ejemplo, durante la fase de reconocimiento, un atacante escanea para encontrar puertos abiertos y determinar el estado de los servicios relacionados con la red y el VMS. Para mitigar esto, la guía de protección es cerrar los puertos del sistema innecesarios en las configuraciones de MOBOTIX HUB VMS y Windows.

El proceso de evaluación de riesgos y amenazas incluye los siguientes pasos:

- Identifique los riesgos de información y seguridad
- Evalúe y priorice los riesgos
- Implementar políticas, procedimientos y soluciones técnicas para mitigar estos riesgos

El proceso general de evaluación de riesgos y amenazas, y la implementación de controles de seguridad, se conoce como marco de gestión de riesgos. Este documento se refiere a los controles de seguridad y privacidad del NIST y otras publicaciones sobre marcos de gestión de riesgos.

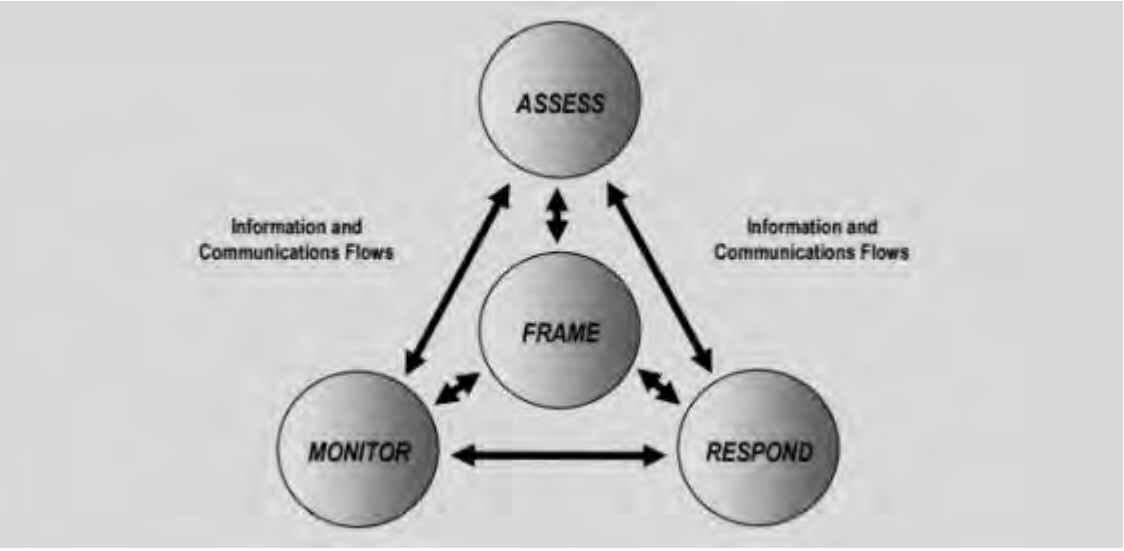
2.2.1 Marco de gestión de riesgos cibernéticos

Los controles de seguridad y privacidad de SP 800-53 Revisión 4 (http://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf) forman parte de un marco general de gestión de riesgos del NIST. El documento SP800-39 (http://csrc.nist.gov/publications/nistpubs/800-39/sp800-39-final.pdf) del NIST es una guía para aplicar un marco de gestión de riesgos. SP800-36 es un documento fundamental para el Marco de Ciberseguridad del NIST, que se describe en Marco de Ciberseguridad (http://www.nist.gov/cyberframework/).

Las cifras aquí muestran:

- Una visión general del proceso de gestión de riesgos. Muestra un enfoque general de alto nivel.
- Gestión de riesgos a nivel de negocio, teniendo en cuenta consideraciones estratégicas y tácticas.
- El ciclo de vida de un marco de gestión de riesgos y los documentos del NIST que proporcionan detalles de cada uno de los pasos del ciclo de vida.

Los controles de seguridad y privacidad representan acciones y recomendaciones específicas que se deben implementar como parte de un proceso de gestión de riesgos. Es importante que el proceso incluya la evaluación de la organización, los requisitos particulares de una implementación determinada y la agregación de estas actividades en un plan de seguridad. SP 800-18 Revisión 1 (http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf) proporciona referencias para planes de seguridad detallados.



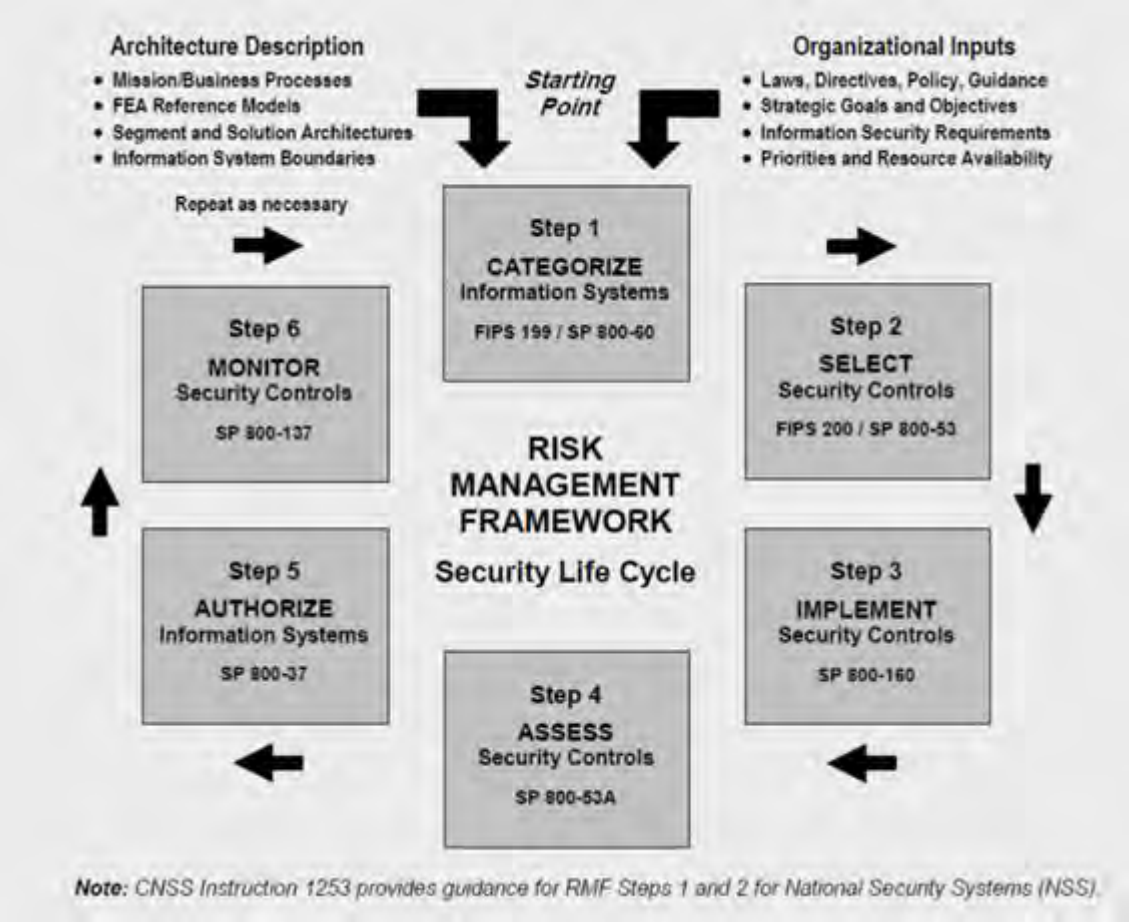
Visión de alto nivel de la gestión de riesgos (SP 800-39, página 8 (http://csrc.nist.gov/publications/nistpubs/800-39/sp800-39-final.pdf))

El proceso es interactivo y las respuestas y sus resultados son iterativos. Las amenazas, los riesgos, las respuestas y los resultados de seguridad son dinámicos y se adaptan, por lo que también debe hacerlo un plan de seguridad. Este diagrama muestra cómo un marco de gestión de riesgos considera los sistemas de TI, los procesos de negocio y la organización en su conjunto para encontrar un equilibrio para el plan de seguridad.

Equilibrio entre la seguridad y los objetivos empresariales (SP 800-39, página 9 (http://csrc.nist.gov/publications/nistpubs/800-39/sp800-39-final.pdf))

Al fortalecer un sistema, se equilibra el impacto en la productividad empresarial y la facilidad de uso en aras de la seguridad, y viceversa, en el contexto de los servicios que presta. La orientación de seguridad no está aislada de otras actividades empresariales y de TI.

Por ejemplo, cuando un usuario introduce su contraseña incorrectamente en tres intentos consecutivos, la contraseña se bloquea y no puede acceder al sistema. El sistema está a salvo de ataques de fuerza bruta, pero el usuario desafortunado no puede utilizar el dispositivo para hacer su trabajo. Una política de contraseñas seguras que requiera contraseñas de 30 caracteres y cambiar las contraseñas cada 30 días es una buena práctica, pero también es difícil de usar.



Ejemplo de marco de gestión de riesgos (SP 800-53 Rev 5 página 8 (https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final))

Para documentar su marco de gestión de riesgos, el NIST produjo varias publicaciones especiales. Incluye los siguientes componentes:

1. Categorización (identificación del nivel de riesgo)
2. Selección de controles de seguridad y privacidad
3. Implementación
4. Evaluación de la eficacia de los controles de seguridad
5. Creación de un perfil de seguridad del sistema mejorado y lo que se denomina una Autoridad para Operar (ATO)
6. Supervisión y evaluación a través de iteraciones

El marco de gestión de riesgos ayuda a poner un plan de seguridad y una guía en un contexto de seguridad.

2.3 Endurecimiento de los componentes del sistema

Para proteger los componentes del sistema, cambie las configuraciones para reducir el riesgo de un ataque exitoso. Los atacantes buscan una forma de entrar y buscan vulnerabilidades en las partes expuestas del sistema. Los sistemas de vigilancia pueden involucrar 100 o incluso 1000 componentes. La falta de seguridad de cualquier componente puede comprometer el sistema.

A veces se pasa por alto la necesidad de mantener la información de configuración. MOBOTIX HUB VMS proporciona funciones para gestionar configuraciones, pero las organizaciones deben contar con una política y un proceso, y comprometerse a hacer el trabajo.

El endurecimiento requiere que mantenga actualizados sus conocimientos sobre seguridad:

- Tenga en cuenta los problemas que afectan al software y al hardware, incluidos los sistemas operativos, los dispositivos móviles, las cámaras, los dispositivos de almacenamiento y los dispositivos de red. Establezca un punto de contacto para todos los componentes del sistema. Lo ideal es utilizar procedimientos de informes para realizar un seguimiento de los errores y vulnerabilidades de todos los componentes.
- Manténgase al día sobre las vulnerabilidades y exposiciones comunes (CVE) (descritas en Vulnerabilidades y exposiciones comunes (https://cve.mitre.org/)) para todos los componentes del sistema. Estos pueden estar relacionados con los sistemas operativos, los dispositivos que tienen contraseñas de mantenimiento codificadas, etc. Aborde las vulnerabilidades de cada componente y alerte a los fabricantes sobre las vulnerabilidades.
- Mantener actualizada la configuración y la documentación del sistema para el sistema. Utilice procedimientos de control de cambios para el trabajo que realice y siga las prácticas recomendadas para la administración de la configuración, tal como se describe en SP 800-128 (https://csrc.nist.gov/publications/detail/sp/800-128/final).

En las secciones siguientes se proporcionan recomendaciones básicas y avanzadas de protección y seguridad para cada componente del sistema. Las secciones también contienen ejemplos de cómo se relacionan con controles de seguridad específicos descritos en la Publicación especial 800-53 del NIST, revisión 4, titulada Controles de *seguridad y privacidad para organizaciones y sistemas de información federales*.

Además del documento del NIST, se hace referencia a las siguientes fuentes:

- Centro para la Seguridad en Internet
- SP 800-53
- ISO 27001
- ISO/IEC 15408 (también conocida como Common Criteria, ISO/IEC 15408-1:2022 (https://www.iso.org/standard/72891.html)).

Apéndice 1 - Recursos en la página 103 En este documento se proporcionan recomendaciones de los fabricantes de cámaras. Este es un esfuerzo relativamente nuevo de los fabricantes, por lo que los recursos disponibles son limitados. En su mayor parte, las recomendaciones se pueden generalizar a todos los fabricantes de cámaras.

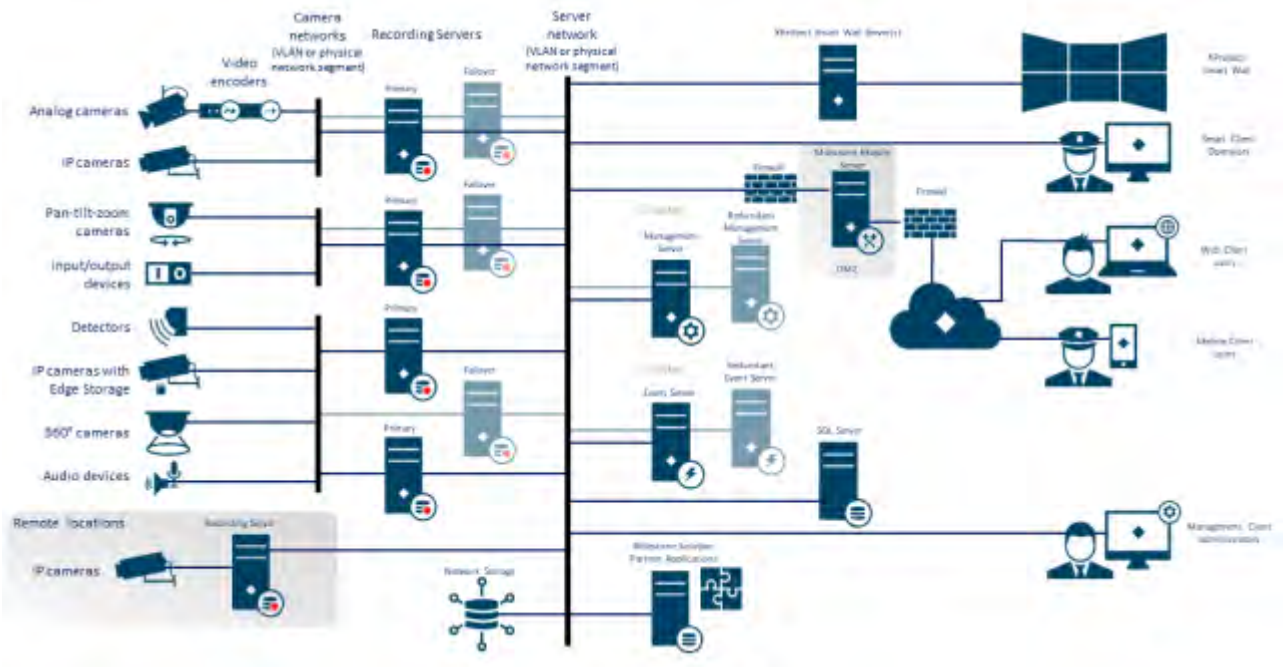
3 Configuración general

3.1 Visión general

Para ayudar a proteger su sistema de vigilancia, MOBOTIX recomienda lo siguiente:

- Restrinja el acceso a los servidores. Mantenga los servidores en habitaciones cerradas con llave y dificulte el acceso de los intrusos a los cables de red y alimentación.
  (PE2 y PE3 en los Apéndices D y F del NIST SP 800-53 Rev5 (https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final) (PE Protección Física y del Medio Ambiente).)
- Diseñe una infraestructura de red que utilice la segmentación de red física o VLAN tanto como sea posible.
  (SC3 en los Apéndices D y F del NIST SP 800-53 Rev5 (https://csrc.nist.gov/publications/detail/sp/800-53 /rev-5/final) (Protección del sistema y las comunicaciones SC).)
  - Separe la red de cámaras de la red de servidores teniendo dos interfaces de red en cada servidor de grabación: una para la red de cámaras y otra para la red de servidores.
  - Coloque el servidor móvil en una "zona desmilitarizada" (DMZ) con una interfaz de red para el acceso público y otra para la comunicación privada con otros servidores.
    (SC7 en los Apéndices D y F NIST SP 800-53 Rev5 (https://csrc.nist.gov/publications/detail/sp/800-53 /rev-5/final).)
  - Se pueden tomar muchas precauciones cuando se trata de la configuración general. Además de los firewalls, estos incluyen técnicas para segmentar la red y controlar el acceso a los servidores, clientes y aplicaciones.
    (AC3, AC4, AC6, CA3, CM3, CM6, CM7, IR4, SA9, SC7, SC28, SI3, SI 8 en los Apéndices D y F en NIST SP 800-53 Rev5 (https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final) (Controles de acceso de CA), (Gestión de configuración CM) (Respuesta a incidentes IR) (Sistema SA y adquisición de servicios) (Sistemas SI e integridad de la información).)
- Configure el VMS con roles que controlen el acceso al sistema y designen tareas y responsabilidades.
  (AC2, AC3, AC6, AC16, AC25, AU6, AU9, CM5, CM11, IA5, PL8, PS5, PS7, SC2, SI7, en los Apéndices D y F en NIST SP 800-53 Rev5 (https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final) (AU Auditoría y Responsabilidad) (Identificación y Autenticación de IA) (PL Planning).)

La figura muestra un ejemplo de una configuración general.



3.1.1 Privacidad desde el diseño

Los productos MOBOTIX están diseñados para ofrecer una comunicación segura de extremo a extremo. Los productos MOBOTIX están diseñados para proteger la privacidad y los datos. La protección de datos siempre es importante, pero especialmente si tiene la intención de cumplir con el Reglamento General de Protección de Datos (GDPR) en la UE.

De acuerdo con el RGPD, el responsable del tratamiento de datos personales, al procesar dichos datos, tiene la obligación de implementar medidas técnicas u organizativas diseñadas para implementar los principios de protección de datos establecidos en el RGPD. El RGPD se refiere a esto como privacidad desde el diseño.

En el contexto de una cámara de vigilancia, un ejemplo relevante de privacidad por diseño sería una característica que permite digitalmente al usuario restringir la captura de imágenes a un determinado perímetro, evitando que la cámara capture imágenes fuera de este perímetro que de otro modo se capturarían.

En MOBOTIX HUB, hay soporte para el enmascaramiento de privacidad en dos formas: máscaras permanentes que no se pueden quitar y máscaras elevables que (con los permisos adecuados) se pueden levantar para revelar la imagen detrás de la máscara.

El responsable del tratamiento también tiene la obligación de aplicar medidas técnicas u organizativas que, por defecto, garanticen el tratamiento menos intrusivo para la privacidad de los datos personales en cuestión. El GDPR se refiere a esto como privacidad por defecto. En el contexto de una cámara, un ejemplo relevante de privacidad de forma predeterminada podría ser el uso del enmascaramiento de privacidad para mantener privada un área sensible dentro de la vista de la cámara.

¿Qué debe hacer para garantizar la privacidad desde el diseño?

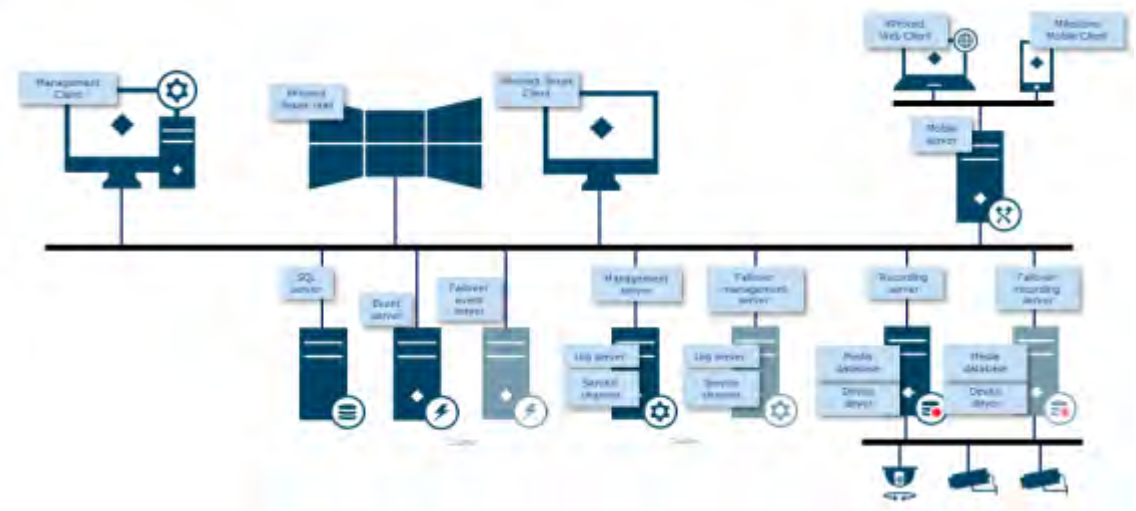
- Tenga en cuenta la resolución de los diferentes puntos de la escena de la cámara y documente estos ajustes
  Diferentes propósitos requieren diferentes calidades de imagen. Cuando la identificación no es necesaria, se debe elegir la resolución de la cámara y otros factores modificables para garantizar que no se capturen imágenes faciales reconocibles.

- Encripta tus grabaciones
  MOBOTIX recomienda proteger sus grabaciones activando al menos el cifrado Light en el almacenamiento y los archivos de sus servidores de grabación. MOBOTIX utiliza el algoritmo AES-256 para el cifrado. Al seleccionar Cifrado ligero, solo se cifra una parte de la grabación. Al seleccionar Cifrado seguro, se cifra toda la grabación.
- Proteger la red
  MOBOTIX recomienda seleccionar cámaras que sean compatibles con HTTPS. Se recomienda configurar las cámaras en VLAN separadas y utilizar HTTPS para la comunicación entre la cámara y el servidor de grabación.
  Se recomienda que los clientes inteligentes MOBOTIX HUB y los Smart Walls MOBOTIX HUB estén en la misma VLAN que los servidores.
  Utilice una red VPN encriptada o similar si utiliza Smart Client o Smart Wall desde una ubicación remota.
- Habilite y documente el tiempo de retención previsto
  De conformidad con el artículo 4, apartado 1, letra e) del RGPD, las grabaciones no deben conservarse más tiempo del necesario para los fines específicos para los que se realizaron. MOBOTIX recomienda establecer el tiempo de retención de acuerdo con las leyes y requisitos regionales y, en cualquier caso, establecer el tiempo de retención en un máximo de 30 días.
- Exportaciones seguras
  MOBOTIX recomienda permitir el acceso a la funcionalidad de exportación solo a un conjunto selecto de usuarios que necesiten este permiso.
  MOBOTIX también recomienda cambiar el perfil de Smart Client para permitir solo la exportación en formato MOBOTIX HUB con el cifrado habilitado. No se deben permitir las exportaciones AVI y JPEG, ya que no se pueden hacer seguras. Esto hace que la exportación de cualquier material de evidencia esté protegida por contraseña, encriptada y firmada digitalmente, asegurándose de que el material forense sea genuino, no manipulado y visto solo por el receptor autorizado.
- Habilite el enmascaramiento de privacidad: permanente o elevable
  Utilice el enmascaramiento de privacidad para ayudar a eliminar la vigilancia de áreas irrelevantes para su objetivo de vigilancia.
  MOBOTIX recomienda instalar una máscara difuminadora elevable para las zonas sensibles y en los lugares donde no se permita la identificación de personas. A continuación, cree un segundo rol que pueda autorizar que se levante la máscara.
- Restringir los derechos de acceso con roles
  Aplicar el principio de privilegio mínimo (PoLP).
  MOBOTIX recomienda que solo permita el acceso a la funcionalidad a un conjunto selecto de usuarios que necesiten este permiso. De forma predeterminada, solo el administrador del sistema puede acceder al sistema y realizar tareas. Todos los nuevos roles y usuarios que se crean no tienen acceso a ninguna función hasta que un administrador los configura deliberadamente.
  Configure permisos para todas las funciones, entre las que se incluyen: ver vídeos y grabaciones en directo, escuchar audio, acceder a metadatos, controlar cámaras PTZ, acceder y configurar Smart Wall, levantar máscaras de privacidad, trabajar con exportaciones, guardar instantáneas, etc.
  Otorgue acceso solo a las cámaras a las que el operador específico necesita acceder, y restrinja el acceso al video, audio y metadatos grabados para los operadores, ya sea por completo, o otorgue acceso solo al video, audio o metadatos grabados en las últimas horas o menos.

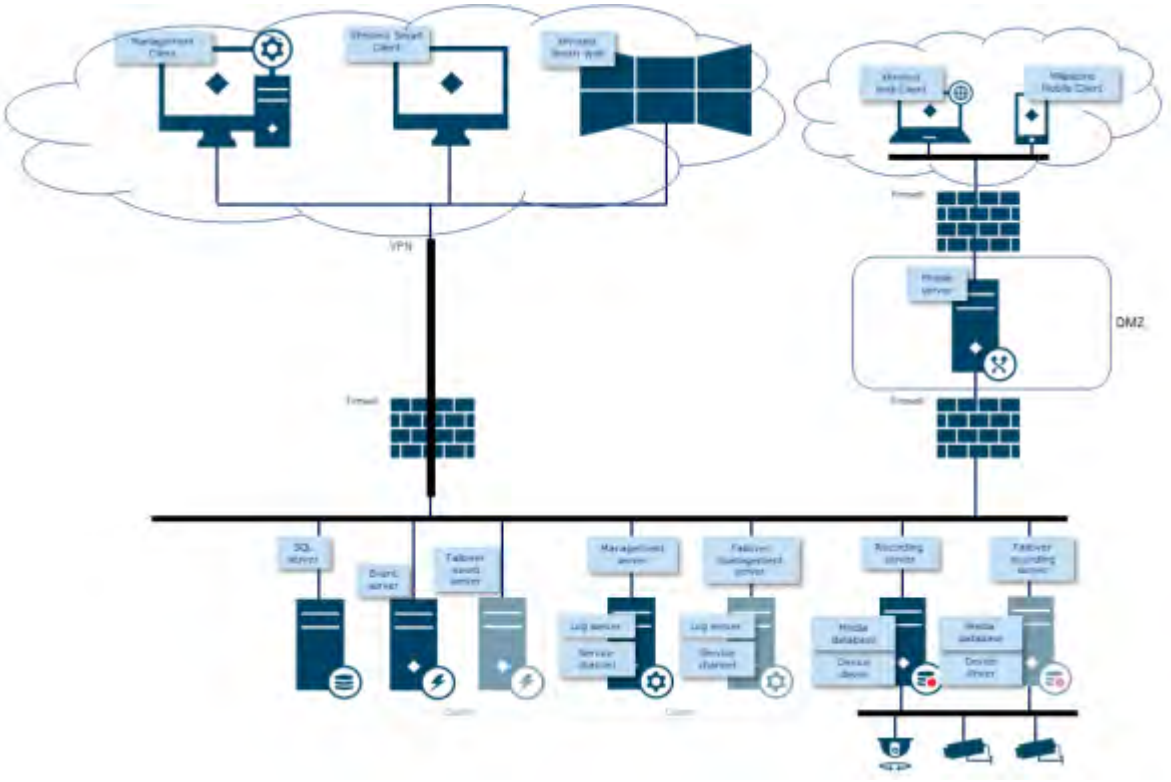
Evaluar y revisar periódicamente las funciones y responsabilidades de los operadores, investigadores, administradores de sistemas y otras personas con acceso al sistema. ¿Sigue siendo aplicable el principio del mínimo privilegio?

- Habilitar y usar la verificación en dos pasos
  MOBOTIX recomienda especificar un paso de inicio de sesión adicional para los usuarios de MOBOTIX HUB Mobile o MOBOTIX HUB Web Client habilitando la verificación en dos pasos.
- Restringir los permisos de administrador
  MOBOTIX recomienda limitar el número de usuarios que tienen una función de administrador. Si necesita crear varios roles de administrador, puede restringir su acceso mediante la creación de roles de administrador que solo puedan administrar partes seleccionadas del sistema, como ciertos dispositivos o funciones.
  MOBOTIX también recomienda que el administrador del VMS no tenga todos los derechos de administrador sobre el almacenamiento que contiene el vídeo grabado, y que el administrador del almacenamiento no tenga acceso al VMS ni a la administración de la copia de seguridad.

Por motivos de seguridad, segmente la red para que haya una red de cliente/administración y redes de cámaras detrás de los servidores de grabación:



Para mayor seguridad, coloque el servidor móvil en una "zona desmilitarizada" (DMZ) con una interfaz de red para el acceso público y otra para la comunicación privada con otros servidores, y use redes cifradas VPN para conexiones externas o para aumentar la seguridad para redes internas menos seguras:


VPN
DMZ

4 Servidores, estaciones de trabajo, clientes y aplicaciones

En esta sección se proporcionan instrucciones de protección basadas en Microsoft Windows y los servicios que utiliza MOBOTIX HUB VMS. Esto incluye:

- El producto MOBOTIX HUB VMS, por ejemplo, MOBOTIX HUB® Corporate o MOBOTIX HUB® Enterprise que se ejecuta en servidores Windows
- El paquete de dispositivos instalado en los servidores de grabación
- El hardware del servidor o las plataformas virtuales, así como los sistemas operativos y servicios
- Los ordenadores cliente para MOBOTIX HUB® Smart Client y MOBOTIX HUB® Web Client
- Dispositivos móviles y sus sistemas operativos y aplicaciones

4.1 Pasos básicos

4.1.1 Establecer objetivos de vigilancia y seguridad

Antes de implementar el VMS, MOBOTIX recomienda establecer objetivos de vigilancia. Defina los objetivos y expectativas relacionados con la captura y el uso de datos de vídeo y metadatos relacionados. Todas las partes interesadas deben comprender los objetivos de la vigilancia.

Los detalles de los objetivos de vigilancia se pueden encontrar en otros documentos, por ejemplo, BS EN 62676-1-1: Sistemas de *videovigilancia para su uso en aplicaciones de seguridad. Requisitos del sistema. General.*

Cuando se establecen objetivos de vigilancia, puede establecer los objetivos de seguridad. Los objetivos de seguridad respaldan los objetivos de vigilancia al abordar lo que se debe proteger en el VMS. Una comprensión compartida de los objetivos de seguridad facilita la protección del VMS y el mantenimiento de la integridad de los datos.
Con los objetivos de vigilancia y seguridad establecidos, puede abordar más fácilmente los aspectos operativos de la protección del VMS, como por ejemplo:

- Evite que los datos se vean comprometidos
- Responda a las amenazas y los incidentes cuando ocurran, incluidas las funciones y responsabilidades.

Aprende más

Los siguientes controles proporcionan instrucciones adicionales:

- Plan de seguridad del sistema NIST SP 800-53 PL-2
- Proceso de adquisición de NIST SP 800-53 SA-4

4.1.2 Establecer una política de seguridad formal y un plan de respuesta

De conformidad con NIST SP 800-100 Information Security Handbook: A Guide for Managers (https://csrc.nist.gov/publications/detail/sp/800-100/final), MOBOTIX recomienda que establezca una política de seguridad formal y un plan de respuesta que describa cómo su organización aborda los problemas de seguridad, en términos de procedimientos prácticos y directrices. Por ejemplo, una política de seguridad puede incluir:

- Una política de contraseñas definida por el departamento de TI interno
- Control de acceso con tarjetas identificativas
- Restricciones para que los teléfonos inteligentes se conecten a la red

Adopte las políticas y planes de TI existentes si se adhieren a las mejores prácticas de seguridad.

Aprende más

Los siguientes controles proporcionan instrucciones adicionales:

- Política y procedimientos de respuesta a incidentes NIST SP 800-53 IR-1
- Plan del programa de seguridad de la información NIST SP 800-53 PM-1

4.1.3 Usar usuarios de Windows con Active Directory

Hay dos tipos de usuarios en MOBOTIX HUB VMS:

- Usuario básico: una cuenta de usuario de VMS dedicada autenticada mediante una combinación de nombre de usuario y contraseña mediante una política de contraseñas. Los usuarios básicos se conectan al VMS mediante una capa de sockets seguros (SSL) con la sesión de protocolo de seguridad (https://datatracker.ietf.org/wg/tls/charter/) actual de la capa de transporte (TLS) para iniciar sesión, cifrando el contenido del tráfico y el nombre de usuario y contraseña.
- Usuario de Windows: la cuenta de usuario es específica de una máquina o un dominio, y se autentica en función del inicio de sesión de Windows. Los usuarios de Windows que se conectan al VMS pueden usar Microsoft Windows Challenge/Response (NTML) para el inicio de sesión, Kerberos (consulte

Autenticación Kerberos (explicación) en la página 39) u otras opciones de SSP de Microsoft (https://msdn.microsoft.com/en-us /library/windows/desktop/aa380502(v=vs.85).aspx).

MOBOTIX recomienda que, siempre que sea posible, utilice usuarios de Windows en combinación con Active Directory (AD) para autorizar el acceso al VMS. Esto le permite hacer cumplir:

- Una política de contraseñas que requiere que los usuarios cambien su contraseña con regularidad
- Protección de fuerza bruta, de modo que la cuenta de Windows AD se bloquea después de una serie de intentos de autenticación fallidos, de nuevo en línea con la política de contraseñas de la organización
- Autenticación multifactor en el VMS, especialmente para los administradores
- Permisos basados en roles, para que puedas aplicar controles de acceso en todo tu dominio

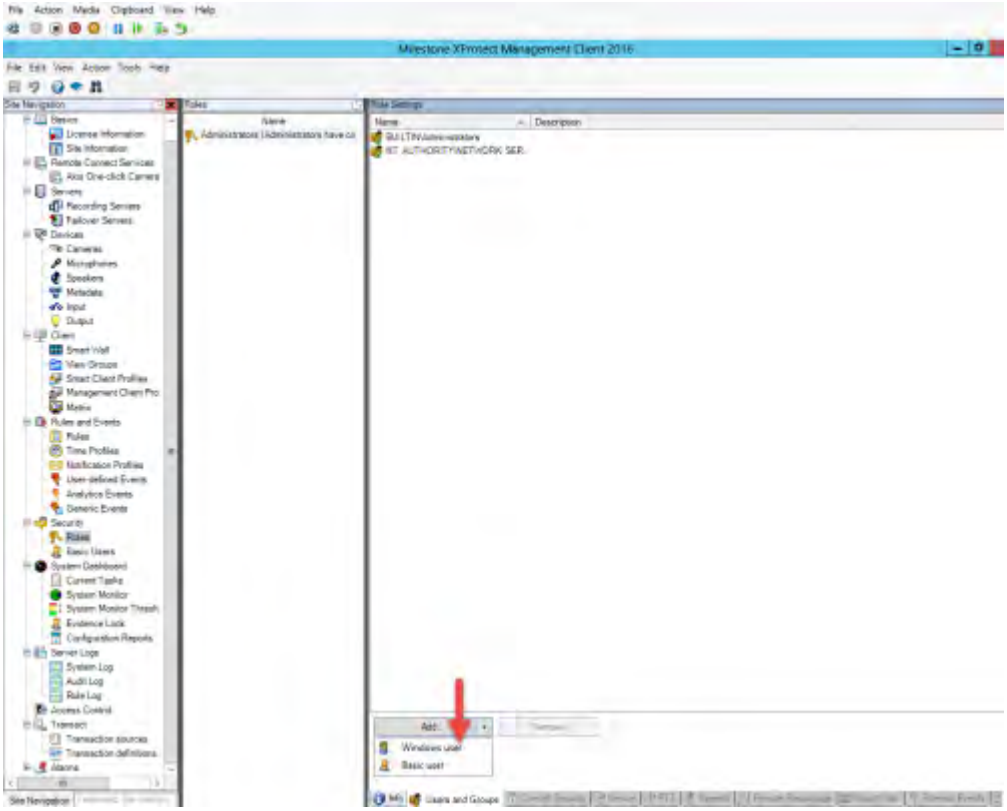
Si su organización no usa AD, puede agregar usuarios de Windows a grupos de trabajo en el servidor de administración. Los grupos de trabajo le brindan algunas de las mismas ventajas que los usuarios de Windows con AD. Puede aplicar una política de contraseñas, que ayuda a protegerse contra ataques de fuerza bruta, pero MOBOTIX recomienda utilizar un dominio de Windows, ya que esto le proporciona un control central sobre las cuentas de usuario.

Los usuarios de Windows tienen la ventaja de ser autenticados a través del directorio como un único origen autorizado y servicio empresarial para la red y no ad hoc para su máquina local. Esto le permite usar controles de acceso basados en roles para asignar permisos a usuarios y grupos de forma coherente en el dominio y los equipos de la red.

Si utiliza usuarios locales de Windows, el usuario debe crear un nombre de usuario y una contraseña locales en cada equipo, lo que es problemático desde el punto de vista de la seguridad y la facilidad de uso.

Para agregar usuarios o grupos de Windows a roles en el cliente de administración, siga estos pasos:

1. Abra el cliente de administración.
2. Expanda el nodo Seguridad.



3. Seleccione el rol al que desea agregar los usuarios de Windows.

la pestaña Usuarios y grupos, haga clic en Agregar y seleccione Usuario de Windows. Aparecerá una ventana emergente.

5. Si el nombre de dominio no aparece en el campo Desde esta ubicación, haga clic en Ubicaciones.
6. Especifique el usuario de Windows y, a continuación, haga clic en Aceptar.

Para comprobar que el usuario de Windows es un usuario de AD, el nombre de dominio debe aparecer como un prefijo, por ejemplo, "Dominio\Juan".

Aprende más

Los siguientes controles proporcionan instrucciones adicionales:

- Ajustes de configuración de NIST SP 800-53 CM-6
- Documentación del sistema de información NIST SP 800-53 SA-5
- NIST SP 800-53 SA-13 Confiabilidad

4.1.4 Comunicación segura (explicación)

El Protocolo de Transferencia de Hipertexto Seguro (HTTPS) es una extensión del Protocolo de Transferencia de Hipertexto (HTTP) para la comunicación segura a través de una red informática. En HTTPS, el protocolo de comunicación se cifra mediante Transport Layer Security (TLS) o su predecesor, Secure Sockets Layer (SSL).
En MOBOTIX HUB VMS, la comunicación segura se obtiene mediante el uso de SSL/TLS con cifrado asimétrico (RSA).
SSL/TLS utiliza un par de claves, una privada y otra pública, para autenticar, proteger y administrar conexiones seguras.
Una entidad de certificación (CA) puede emitir certificados a los servicios web de los servidores que utilizan un certificado de CA. Este certificado contiene dos claves, una clave privada y una clave pública. La clave pública se instala en los clientes de un servicio web (clientes de servicio) mediante la instalación de un certificado público. La clave privada se utiliza para firmar certificados de servidor que deben instalarse en el servidor. Cada vez que un cliente de servicio llama al servicio web, el servicio web envía el certificado del servidor, incluida la clave pública, al cliente. El cliente de servicio puede validar el certificado de servidor mediante el certificado de CA pública ya instalado. El cliente y el servidor ahora pueden usar el certificado de servidor público y privado para intercambiar una clave secreta y así establecer una conexión SSL/TLS segura.
Para obtener más información sobre TLS: https://en.wikipedia.org/wiki/Transport_Layer_Security

Los certificados tienen una fecha de caducidad. MOBOTIX HUB VMS no le avisará cuando un certificado esté a punto de caducar. Si un certificado caduca:- Los clientes ya no confiarán en el servidor de grabación con el certificado caducado y, por lo tanto, no podrán comunicarse con él
- Los servidores de grabación ya no confiarán en el servidor de gestión con el certificado caducado y, por lo tanto, no podrán comunicarse con él
- Los dispositivos móviles ya no confiarán en el servidor móvil con el certificado caducado y, por lo tanto, no podrán comunicarse con él
Para renovar los certificados, siga los pasos de esta guía como lo hizo al crear certificados.

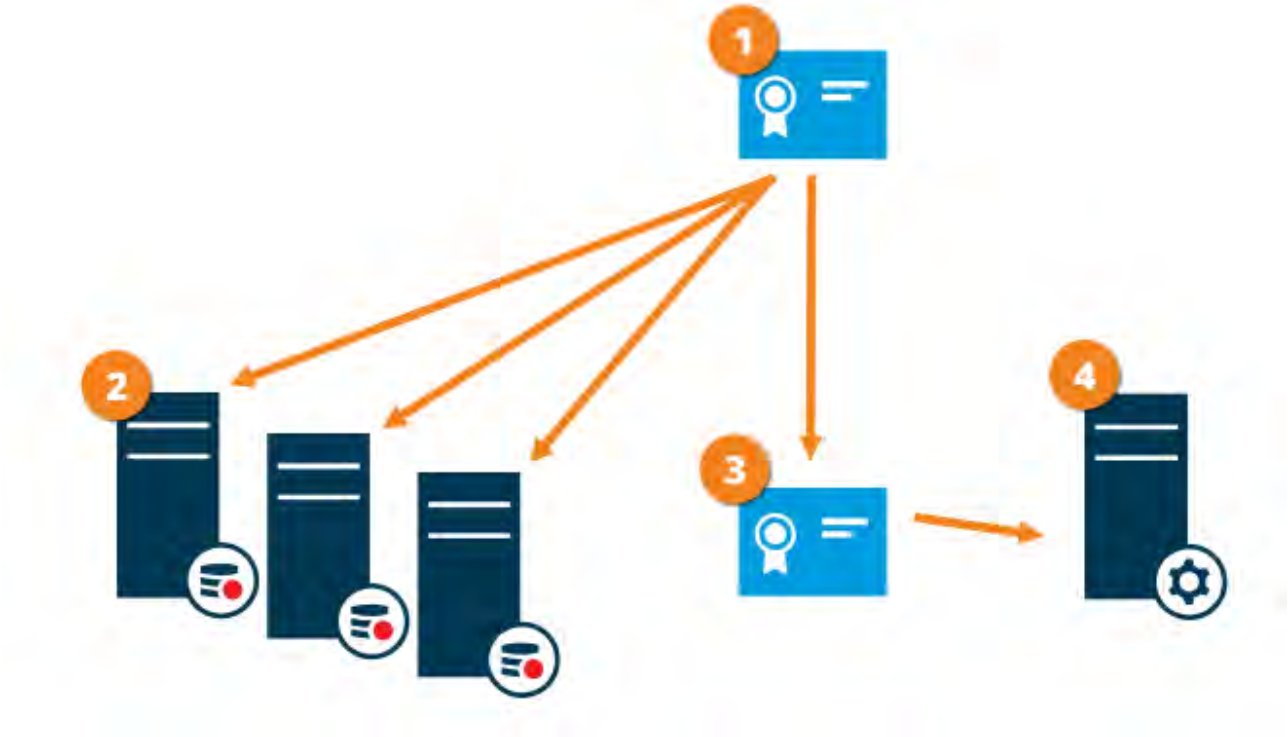
Para obtener más información, consulte la guía de certificados sobre cómo proteger las instalaciones de MOBOTIX Hub VMS .

4.1.5 Cifrado del servidor de administración (explicación)

Puede cifrar la conexión bidireccional entre el servidor de gestión y el servidor de grabación. Cuando se habilita el cifrado en el servidor de administración, se aplica a las conexiones de todos los servidores de grabación que se conectan al servidor de administración. Si habilita el cifrado en el servidor de administración, también debe habilitar el cifrado en todos los servidores de grabación. Antes de habilitar el cifrado, debe instalar certificados de seguridad en el servidor de administración y en todos los servidores de grabación.

Distribución de certificados para servidores de administración

El gráfico ilustra el concepto básico de cómo se firman, confían y distribuyen los certificados en MOBOTIX HUB VMS para proteger la comunicación con el servidor de gestión.



❶ Un certificado de CA actúa como un tercero de confianza, en el que confían tanto el sujeto/propietario (servidor de administración) como la parte que verifica el certificado (servidores de grabación)
❷ El certificado de CA debe ser de confianza en todos los servidores de grabación. De esta manera, los servidores de grabación pueden verificar la validez de los certificados emitidos por la CA
❸ El certificado de CA se utiliza para establecer una conexión segura entre el servidor de administración y los servidores de grabación
❹ El certificado de CA debe estar instalado en el equipo en el que se ejecuta el servidor de administración
Requisitos para el certificado de servidor de administración privado:

- Se emite al servidor de administración para que el nombre de host del servidor de administración se incluya en el certificado, ya sea como sujeto (propietario) o en la lista de nombres DNS a los que se emite el certificado
- De confianza en el propio servidor de administración, mediante la confianza en el certificado de CA que se usó para emitir el certificado del servidor de administración
- De confianza en todos los servidores de grabación conectados al servidor de gestión, mediante la confianza en el certificado de CA que se utilizó para emitir el certificado del servidor de gestión

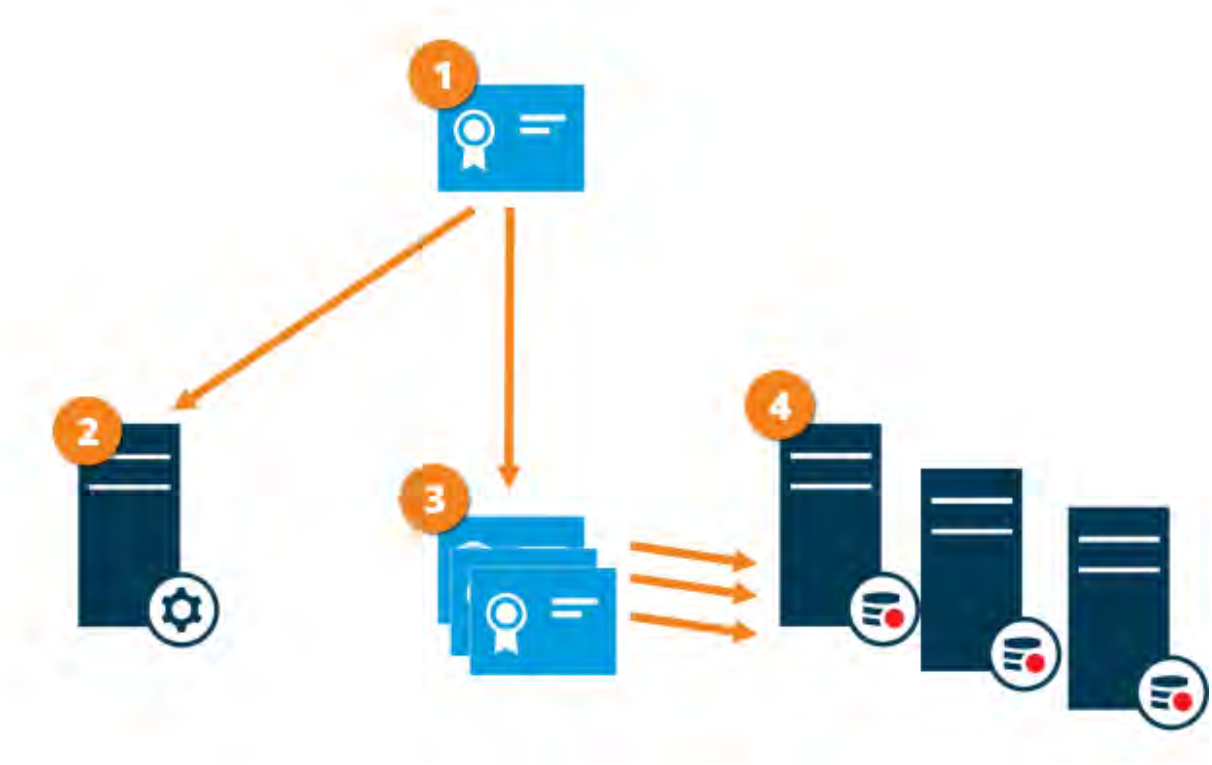
4.1.6 Cifrado desde el servidor de administración hasta el servidor de grabación (explicación)

Puede cifrar la conexión bidireccional entre el servidor de gestión y el servidor de grabación. Cuando se habilita el cifrado en el servidor de administración, se aplica a las conexiones de todos los servidores de grabación que se

conectan al servidor de administración. El cifrado de esta comunicación debe seguir la configuración de cifrado del servidor de administración. Por lo tanto, si el cifrado del servidor de administración está habilitado, también debe estar habilitado en los servidores de grabación y viceversa. Antes de habilitar el cifrado, debe instalar certificados de seguridad en el servidor de administración y en todos los servidores de grabación, incluidos los servidores de grabación de conmutación por error.

Distribución de certificados

El gráfico ilustra el concepto básico de cómo se firman, confían y distribuyen los certificados en MOBOTIX HUB VMS para proteger la comunicación desde el servidor de gestión.



❶ Un certificado de CA actúa como un tercero de confianza, en el que confían tanto el sujeto/propietario (servidor de grabación) como la parte que verifica el certificado (servidor de administración)

❷ El certificado de CA debe ser de confianza en el servidor de administración. De esta manera, el servidor de administración puede verificar la validez de los certificados emitidos por la CA

❸ El certificado de CA se utiliza para establecer una conexión segura entre los servidores de grabación y el servidor de administración

❹ El certificado de CA debe estar instalado en los equipos en los que se ejecutan los servidores de grabación

Requisitos para el certificado de servidor de grabación privada:

- Se emite al servidor de grabación para que el nombre de host del servidor de grabación se incluya en el certificado, ya sea como sujeto (propietario) o en la lista de nombres DNS a los que se emite el certificado
- De confianza en el servidor de administración, mediante la confianza en el certificado de CA que se usó para emitir el certificado del servidor de grabación

4.1.7 Cifrado entre el servidor de administración y el servidor del recopilador de datos (explicación)

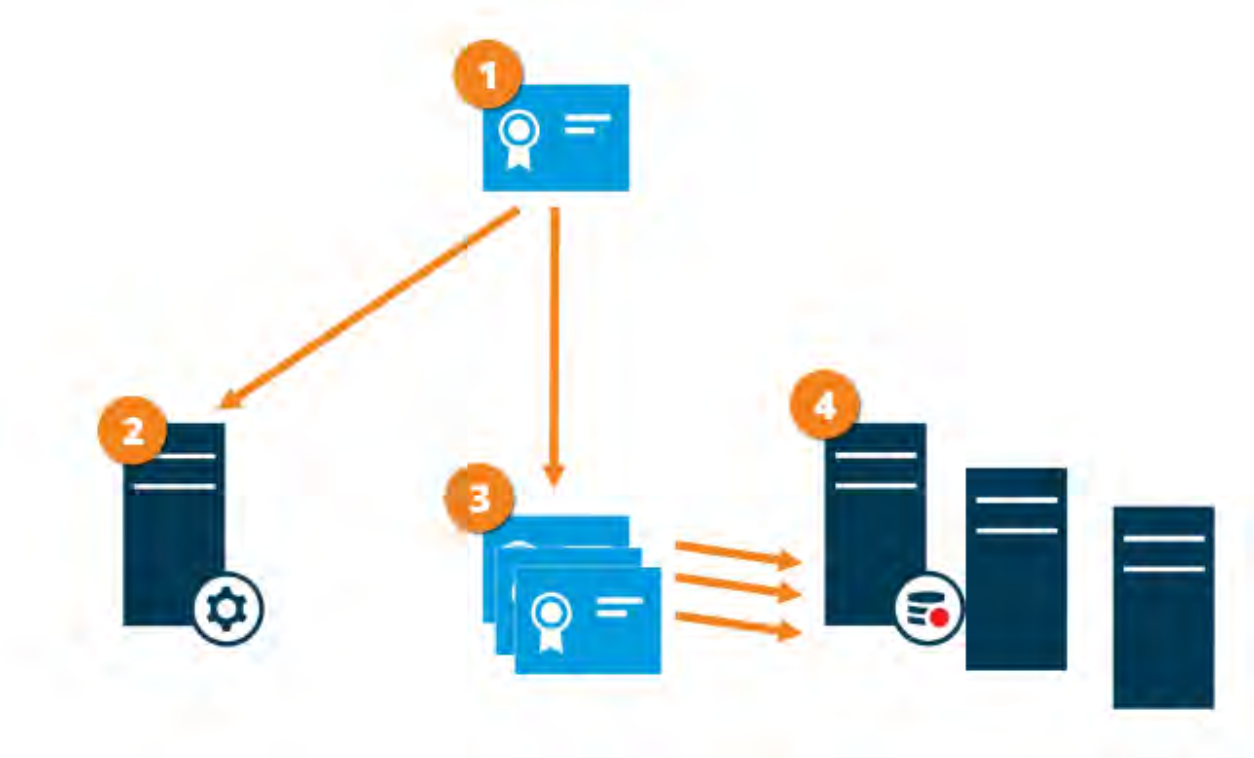
Puede cifrar la conexión bidireccional entre el servidor de administración y el recopilador de datos afiliado cuando tenga un servidor remoto del siguiente tipo:

- Servidor de grabación
- Servidor de eventos
- Servidor de registro
- Servidor LPR
- Servidor móvil

Cuando se habilita el cifrado en el servidor de administración, se aplica a las conexiones de todos los servidores del recopilador de datos que se conectan al servidor de administración. El cifrado de esta comunicación debe seguir la configuración de cifrado del servidor de administración. Por lo tanto, si el cifrado del servidor de administración está habilitado, también debe estar habilitado en los servidores del recopilador de datos afiliados a cada servidor remoto y viceversa. Antes de habilitar el cifrado, debe instalar certificados de seguridad en el servidor de administración y en todos los servidores del recopilador de datos afiliados a los servidores remotos.

Distribución de certificados

El gráfico ilustra el concepto básico de cómo se firman, confían y distribuyen los certificados en MOBOTIX HUB VMS para proteger la comunicación desde el servidor de gestión.



❶ Un certificado de CA actúa como un tercero de confianza, en el que confían tanto el sujeto/propietario (servidor del recopilador de datos) como la parte que verifica el certificado (servidor de administración)

❷ El certificado de CA debe ser de confianza en el servidor de administración. De esta manera, el servidor de administración puede verificar la validez de los certificados emitidos por la CA

3 El certificado de CA se utiliza para establecer una conexión segura entre los servidores del recopilador de datos y el servidor de administración

4 El certificado de CA debe estar instalado en los equipos en los que se ejecutan los servidores del recopilador de datos

Requisitos para el certificado de servidor de recopilador de datos privados:

- Se emite al servidor del recopilador de datos para que el nombre de host del servidor del recopilador de datos se incluya en el certificado, ya sea como sujeto (propietario) o en la lista de nombres DNS a los que se emite el certificado
- De confianza en el servidor de administración, mediante la confianza en el certificado de CA que se usó para emitir el certificado del servidor del recopilador de datos

4.1.8 Cifrado a clientes y servidores que recuperan datos del servidor de grabación (explicación)

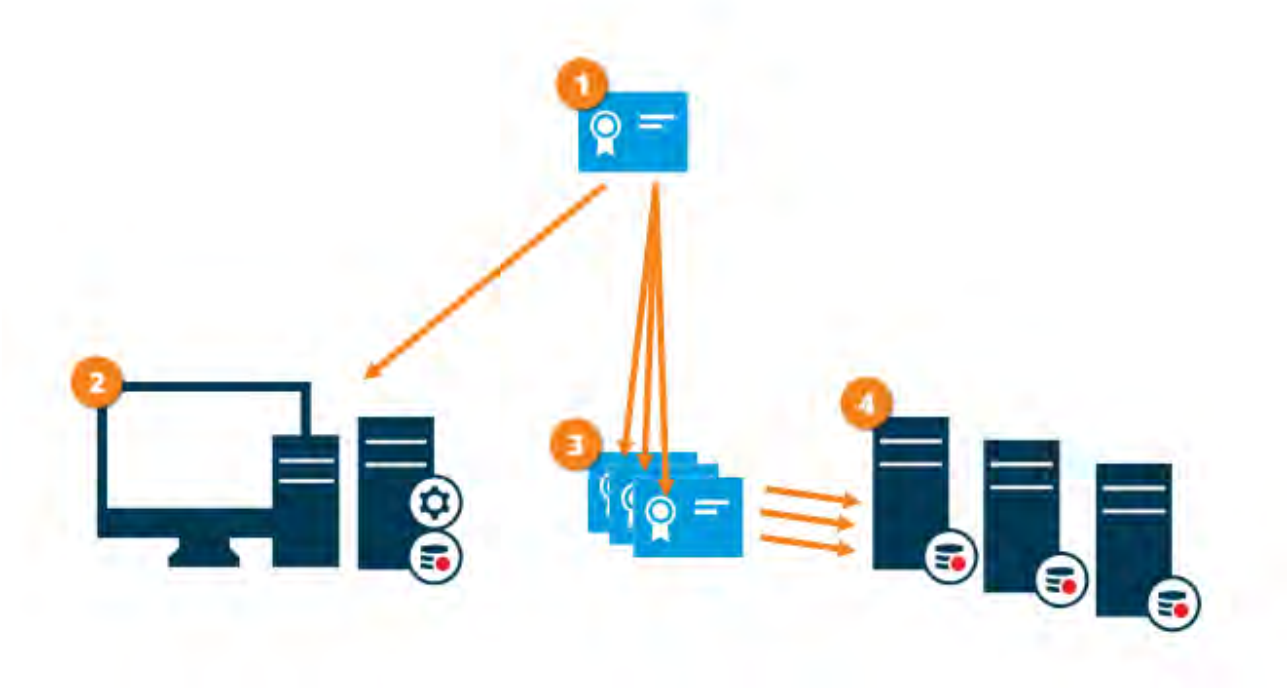
Cuando se habilita el cifrado en un servidor de grabación, se cifra la comunicación con todos los clientes, servidores e integraciones que recuperan flujos de datos del servidor de grabación. En el presente documento se hace referencia a ellos como «clientes»:

- Cliente inteligente MOBOTIX HUB
- Cliente de gestión
- Servidor de administración (para el Monitor del sistema y para imágenes y clips de vídeo AVI en notificaciones por correo electrónico)
- Servidor móvil MOBOTIX HUB
- Servidor de eventos MOBOTIX HUB
- BUJE MOBOTIX LPR
- Puente de red abierto de MOBOTIX
- Servidor DLNA HUB de MOBOTIX
- Sitios que recuperan flujos de datos del servidor de grabación a través de MOBOTIX Interconnect
- Algunas integraciones de SDK de MIP de terceros

En el caso de las soluciones creadas con el SDK de MIP 2018 R3 o versiones anteriores que acceden a servidores de grabación: si las integraciones se realizan con bibliotecas del SDK de MIP, deben reconstruirse con el SDK de MIP 2019 R1; si las integraciones se comunican directamente con las API del servidor de grabación sin usar las bibliotecas del SDK de MIP, los integradores deben agregar compatibilidad con HTTPS ellos mismos.

Distribución de certificados

El gráfico ilustra el concepto básico de cómo se firman, confían y distribuyen los certificados en MOBOTIX HUB VMS para proteger la comunicación con el servidor de grabación.



❶ Un certificado de CA actúa como un tercero de confianza, en el que confían tanto el sujeto/propietario (servidor de grabación) como la parte que verifica el certificado (todos los clientes)

❷ El certificado de CA debe ser de confianza en todos los clientes. De esta manera, los clientes pueden verificar la validez de los certificados emitidos por la CA

❸ El certificado de CA se utiliza para establecer una conexión segura entre los servidores de grabación y todos los clientes y servicios

❹ El certificado de CA debe estar instalado en los equipos en los que se ejecutan los servidores de grabación

Requisitos para el certificado de servidor de grabación privada:

- Se emite al servidor de grabación para que el nombre de host del servidor de grabación se incluya en el certificado, ya sea como sujeto (propietario) o en la lista de nombres DNS a los que se emite el certificado
- De confianza en todos los equipos que ejecutan servicios que recuperan flujos de datos de los servidores de grabación, mediante la confianza en el certificado de CA que se usó para emitir el certificado del servidor de grabación
- La cuenta de servicio que ejecuta el servidor de grabación debe tener acceso a la clave privada del certificado en el servidor de grabación.

Si habilita el cifrado en los servidores de grabación y su sistema aplica servidores de grabación de conmutación por error, MOBOTIX recomienda que también prepare los servidores de grabación de conmutación por error para el cifrado.

4.1.9 Cifrado de la comunicación con el servidor de eventos

Puede cifrar la conexión bidireccional entre el servidor de eventos y los componentes que se comunican con el servidor de eventos, incluido el servidor LPR. Cuando se habilita el cifrado en el servidor de eventos, se aplica a las conexiones de todos los componentes que se conectan al servidor de eventos. Antes de habilitar el cifrado, debe instalar certificados de seguridad en el servidor de eventos y en todos los componentes de conexión.

Cuando la comunicación del servidor de eventos está cifrada, esto se aplica a todas las comunicaciones con ese servidor de eventos. Es decir, solo se admite un modo a la vez, ya sea http o https, pero no al mismo tiempo.

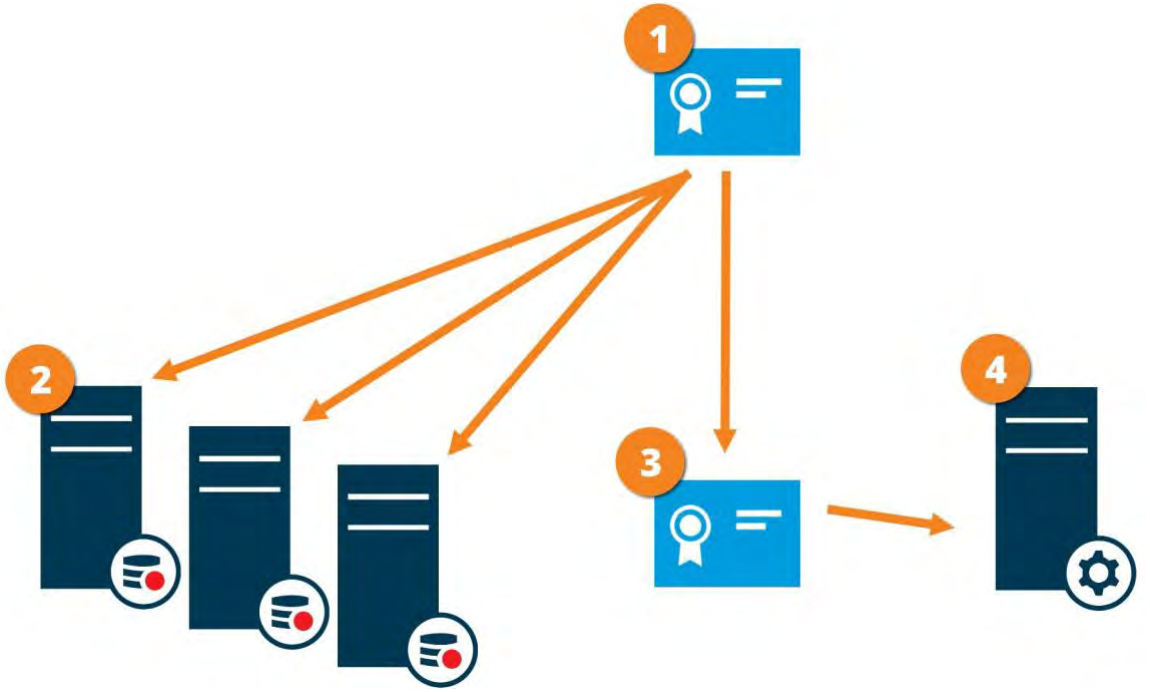
El cifrado se aplica a todos los servicios hospedados en el servidor de eventos, incluidos Transact, Maps, GisMap e Intercommunication.

Antes de habilitar el cifrado en el servidor de eventos, todos los clientes (Smart Client y Management Client) y el plug-in MOBOTIX HUB PR deben estar actualizados al menos a la versión 2022 R1.

HTTPS solo se admite si todos los componentes se actualizan al menos a la versión 2022 R1.

Distribución de certificados

El gráfico ilustra el concepto básico de cómo se firman, confían y distribuyen los certificados en MOBOTIX HUB VMS para proteger la comunicación con el servidor de eventos



❶ Un certificado de CA actúa como un tercero de confianza, en el que confían tanto el sujeto/propietario (servidor de eventos) como la parte que verifica el certificado

❷ El certificado de CA debe ser de confianza en todos los clientes. De esta manera, los clientes pueden verificar la validez de los certificados emitidos por la CA

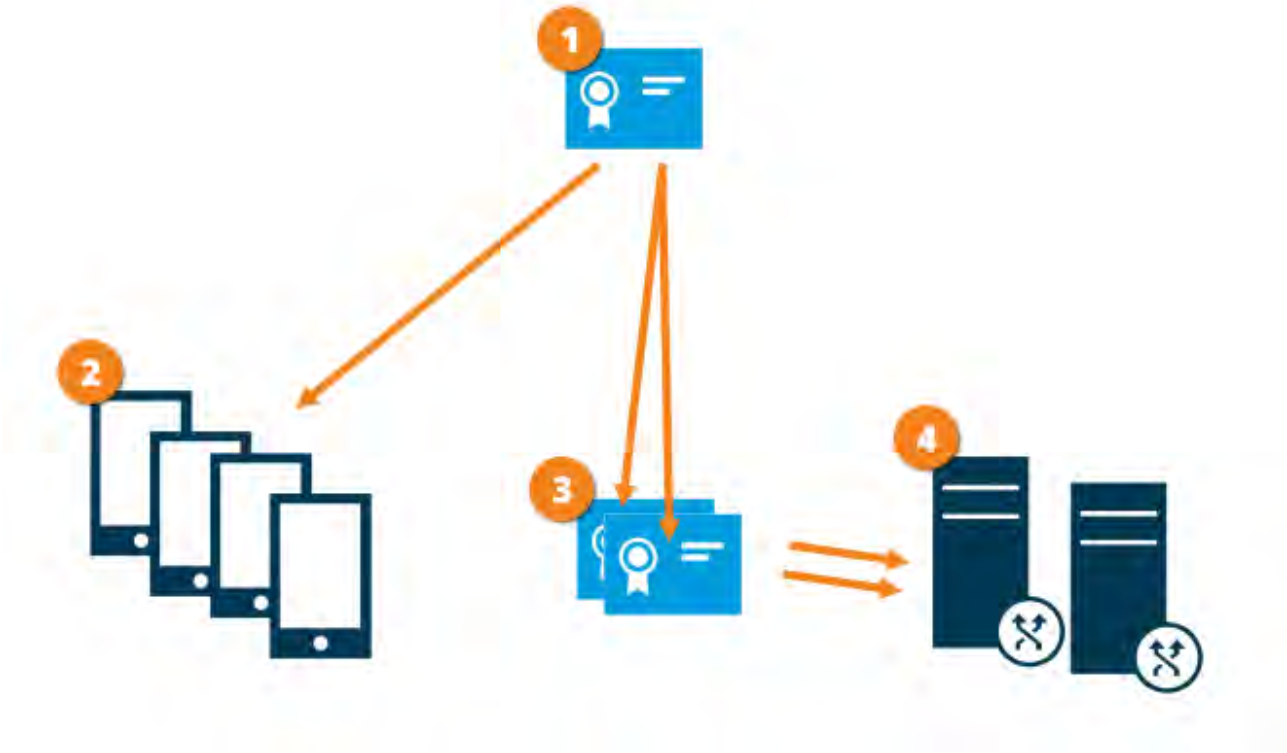
❸ El certificado de CA se utiliza para establecer una conexión segura entre el servidor de eventos y los clientes ❹ El certificado de CA debe estar instalado en el equipo en el que se está ejecutando el servidor de eventos

4.1.10 Cifrado de datos del servidor móvil (explicación)

En MOBOTIX HUB VMS, el cifrado se habilita o deshabilita por servidor móvil. Cuando habilite el cifrado en un servidor móvil, tendrá la opción de usar la comunicación cifrada con todos los clientes, servicios e integraciones que recuperan flujos de datos.

Distribución de certificados para servidores móviles

El gráfico ilustra el concepto básico de cómo se firman, confían y distribuyen los certificados en MOBOTIX HUB VMS para proteger la comunicación con el servidor móvil.



❶ Un certificado de CA actúa como un tercero de confianza, en el que confían tanto el sujeto/propietario (servidor móvil) como la parte que verifica el certificado (todos los clientes)
❷ El certificado de CA debe ser de confianza en todos los clientes. De esta manera, los clientes pueden verificar la validez de los certificados emitidos por la CA
❸ El certificado de CA se utiliza para establecer una conexión segura entre el servidor móvil y los clientes y servicios
❹ El certificado de CA debe estar instalado en el equipo en el que se está ejecutando el servidor móvil

Requisitos para el certificado de CA:

- El nombre de host del servidor móvil debe incluirse en el certificado, ya sea como sujeto/propietario o en la lista de nombres DNS a los que se emite el certificado
- El certificado debe ser de confianza en todos los dispositivos que ejecutan servicios que recuperan flujos de datos del servidor móvil
- La cuenta de servicio que ejecuta el servidor móvil debe tener acceso a la clave privada del certificado de CA

Requisitos de cifrado de servidor móvil para clientes

Si no habilita el cifrado y utiliza una conexión HTTP, la función push-to-talk de MOBOTIX HUB Web Client no estará disponible.

4.1.11 Autenticación Kerberos (explicación)

Kerberos es un protocolo de autenticación de red basado en tickets. Está diseñado para proporcionar una autenticación sólida para aplicaciones cliente/servidor o servidor/servidor.

Use la autenticación Kerberos como alternativa al antiguo protocolo de autenticación LAN NT (NTLM) de Microsoft.

La autenticación Kerberos requiere autenticación mutua, donde el cliente se autentica en el servicio y el servicio se autentica en el cliente. De este modo, puede autenticarse de forma más segura desde los clientes de MOBOTIX HUB a los servidores de MOBOTIX HUB sin exponer su contraseña.

Para que la autenticación mutua sea posible en su MOBOTIX HUB VMS, debe registrar los nombres principales de servicio (SPN) en el directorio activo. Un SPN es un alias que identifica de forma única una entidad, como un servicio de servidor MOBOTIX HUB. Cada servicio que use la autenticación mutua debe tener un SPN registrado para que los clientes puedan identificar el servicio en la red. Sin SPN registrados correctamente, no es posible la autenticación mutua.

En la siguiente tabla se enumeran los diferentes servicios de MOBOTIX con los números de puerto correspondientes que debe registrar:

Servicio	Número de puerto
Servidor de administración: IIS	80 - Configurable
Servidor de administración - Interno	8080
Servidor de grabación - Recopilador de datos	7609
Servidor de conmutación por error	8990
Servidor de eventos	22331
Servidor LPR	22334

El número de servicios que necesita registrar en el directorio activo depende de su instalación actual. El recopilador de datos se instala automáticamente al instalar el servidor de administración, el servidor de grabación, el servidor de eventos, el servidor LPR o el servidor de conmutación por error.

Debe registrar dos SPN para el usuario que ejecuta el servicio: uno con el nombre de host y otro con el nombre de dominio completo.

Si ejecuta el servicio con una cuenta de servicio de usuario de red, debe registrar los dos SPN para cada equipo que ejecute este servicio.

Este es el esquema de nomenclatura SPN de MOBOTIX:

```
VideoOS/[DNS Host Name]:[Puerto]
VideoOS/[Nombre de dominio completo]:[Puerto]
```

A continuación se muestra un ejemplo de SPN para el servicio de servidor de grabación que se ejecuta en un equipo con los siguientes detalles:

```
Nombre de host: Record-Server1
Dominio: Surveillance.com
```

para registrar:
`VideoOS/Record-Server1:7609`
`VideoOS/Record-Server1.Surveillance.com:7609`

4.1.12 Usar la actualización de Windows

MOBOTIX recomienda utilizar Windows Update para proteger su VMS contra vulnerabilidades en el sistema operativo, asegurándose de que estén instaladas las actualizaciones más recientes. MOBOTIX HUB VMS está basado en Windows, por lo que las actualizaciones de seguridad de Windows Update son importantes.
Las actualizaciones pueden requerir una conexión a Internet, por lo que MOBOTIX recomienda que esta conexión esté abierta solo cuando sea necesario y que se supervise para detectar patrones de tráfico inusuales.
Las actualizaciones de Windows a menudo requieren un reinicio. Esto puede ser un problema si se requiere alta disponibilidad, ya que el servidor no puede recibir datos de los dispositivos mientras se reinicia.
Hay varias formas de evitar esto o minimizar el impacto. Por ejemplo, puede descargar actualizaciones en el servidor y, a continuación, aplicarlas en un momento en el que un reinicio interrumpa la vigilancia lo menos posible.
Si la alta disponibilidad es un problema, MOBOTIX recomienda ejecutar el servidor de gestión y los servidores de eventos en clústeres que incluyan uno o más servidores de conmutación por error. El servidor de conmutación por error tomará el control mientras se reinicia el servidor de grabación y la vigilancia no se interrumpe. No incluya servidores de grabación en el clúster. Para los servidores de grabación, utilice un servidor de grabación de conmutación por error.

Antes de implementar actualizaciones de Windows en toda la organización, MOBOTIX recomienda verificar las actualizaciones en un entorno de prueba. Consulte NIST 800-53 CM-8 Inventario de componentes del sistema de *información y sandboxing y Cámaras de detonación SC-44*.

Aprende más

Los siguientes controles proporcionan instrucciones adicionales:

- NIST SP 800-53 SI-2 Corrección de defectos

4.1.13 Mantenga actualizados el software y el firmware del dispositivo

MOBOTIX recomienda utilizar la última versión de MOBOTIX HUB VMS y firmware para los dispositivos de hardware, por ejemplo, las cámaras. Esto asegurará que su sistema incluya las últimas correcciones de seguridad.
Para el hardware, los componentes de red y los sistemas operativos, consulte la base de datos de CVE, así como las actualizaciones enviadas por los fabricantes.
Antes de actualizar el firmware del dispositivo, compruebe que MOBOTIX HUB VMS lo admita. Además, asegúrese de que el paquete de dispositivos instalado en los servidores de grabación sea compatible con el firmware del dispositivo.
Haga esto en un entorno de prueba para la configuración, integración y prueba antes de ponerlo en el entorno de producción.
Para comprobar que el VMS es compatible con un dispositivo, siga estos pasos:

1. Abra este enlace (https://www.mobotix.com/mobotix_custom_table/hub_compatibility).
2. Seleccione el fabricante del dispositivo y, a continuación, haga clic en Filtrar. La versión del firmware que admite el paquete de dispositivos se muestra en la columna Firmware probado.

Aprende más

Los siguientes controles proporcionan instrucciones adicionales:

- NIST SP 800-53 SI-2 Corrección de defectos

4.1.14 Use antivirus en todos los servidores y computadoras

MOBOTIX recomienda instalar software antivirus en todos los servidores y ordenadores que se conecten al VMS. El malware que ingresa a su sistema puede bloquear, cifrar o comprometer los datos en los servidores y otros dispositivos de la red.

Si los dispositivos móviles se conectan al VMS, esto incluye asegurarse de que los dispositivos tengan instalados los últimos sistemas operativos y parches (aunque no directamente antivirus).

Al realizar un análisis de virus, no analice los directorios y subdirectorios del servidor de grabación que contengan bases de datos de grabación. Además, no busque virus en los directorios de almacenamiento de archivos. El análisis en busca de virus en estos directorios puede afectar al rendimiento del sistema.

Para obtener información sobre los puertos, directorios y subdirectorios que se deben excluir del análisis de virus, consulte la sección Acerca del *análisis de virus* en el manual del administrador de *MOBOTIX HUB VMS*.

Aprende más

Los siguientes controles proporcionan instrucciones adicionales:

- Arquitectura de seguridad de la información NIST SP 800-53 PL-8
- NIST SP 800-53 SI-2 Corrección de defectos
- NIST SP 800-53 SI-3 Protección contra código malicioso
- NIST SP 800-53 SI Monitoreo de sistemas de información

4.1.15 Supervise los registros en el VMS en busca de signos de actividad sospechosa

MOBOTIX HUB VMS proporciona funciones para generar y ver registros que proporcionan información sobre patrones de uso, rendimiento del sistema y otros problemas. MOBOTIX recomienda supervisar los registros en busca de signos de actividades sospechosas.

Existen herramientas que aprovechan los registros con fines operativos y de seguridad. Muchas empresas utilizan servidores syslog para consolidar los registros. Puede utilizar syslog para anotar actividades a nivel de Windows, sin embargo, MOBOTIX HUB VMS no es compatible con syslog.

MOBOTIX recomienda utilizar el registro de auditoría en MOBOTIX HUB VMS y habilitar el registro de acceso de usuarios en Management Client. De forma predeterminada, el registro de auditoría solo anota los inicios de sesión de los usuarios. Sin embargo, puede activar el registro de acceso de usuarios para que el registro de auditoría anote todas las actividades de los usuarios en todos los componentes de cliente de los productos MOBOTIX HUB VMS. Esto incluye las horas de las actividades y las direcciones IP de origen.

Los componentes del cliente son MOBOTIX HUB Smart Client, Web Client, el componente MOBOTIX HUB Management Client y las integraciones realizadas mediante el SDK de MIP. Ejemplos de actividades son las exportaciones, la activación de salidas, la visualización de cámaras en directo o en reproducción, etc.

El registro de auditoría no anota los intentos de inicio de sesión incorrectos ni cuando el usuario cierra la sesión.

El registro de todas las actividades de usuario en todos los clientes aumenta la carga en el sistema y puede afectar al rendimiento.

Puede ajustar la carga especificando los siguientes criterios que controlan cuándo el sistema generará una entrada de registro:

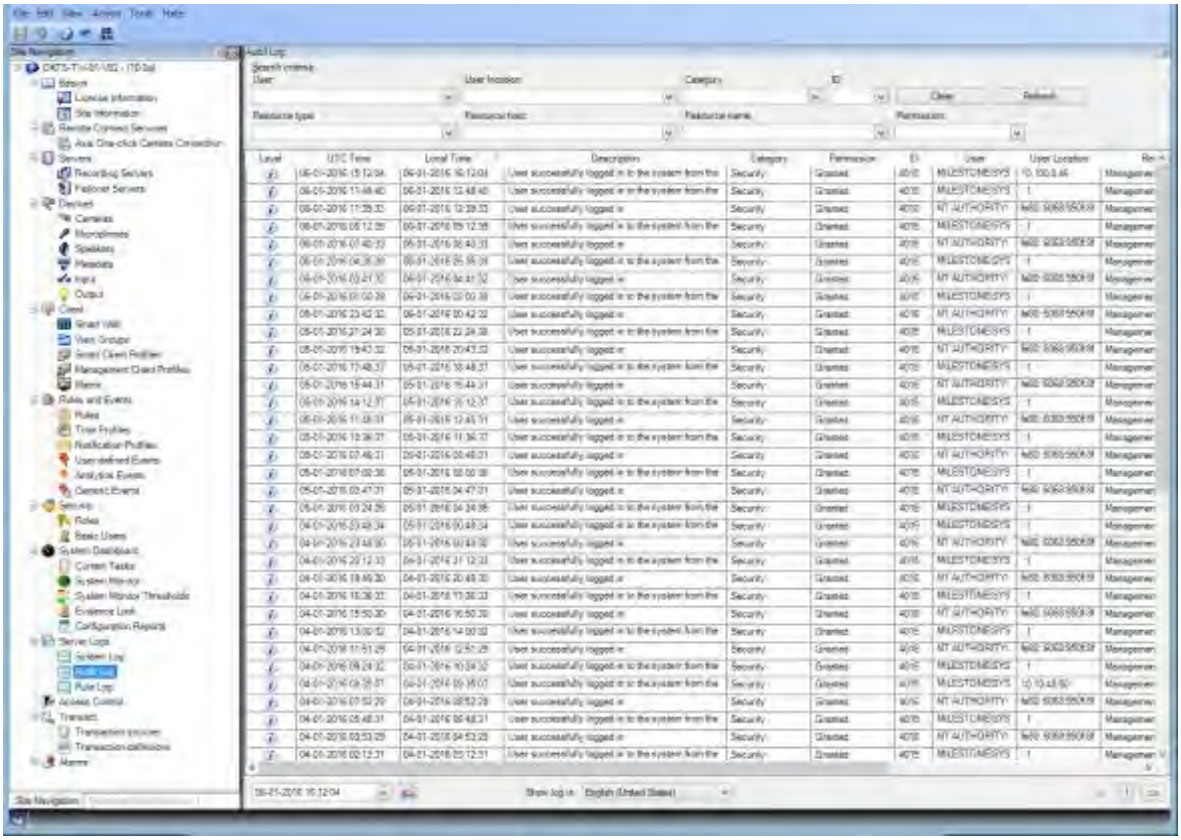
- El número de segundos que componen una secuencia. El VMS genera una entrada de registro cuando un usuario reproduce vídeo dentro de la secuencia.
- El número de fotogramas que un usuario debe ver al reproducir vídeo antes de que el VMS genere una entrada de registro.

Para activar y configurar el registro de acceso de usuario extendido, siga estos pasos:

1. En Cliente de administración, haga clic en Herramientas y seleccione Opciones.
2. En la pestaña Registros del servidor, en Configuración de registro, seleccione Registro de auditoría.
3. En Configuración, active la casilla Habilitar el registro de acceso de usuario.
4. Opcional: Para especificar las limitaciones de la información que se anota y reducir el impacto en el rendimiento, realice selecciones en los campos Longitud de registro de secuencia de reproducción y Registros vistos antes del registro.

Para ver el registro de auditoría en MOBOTIX HUB VMS, siga estos pasos:

1. Abra el cliente de administración.
2. Expanda el nodo Registros del servidor.
3. Haga clic en Registro de auditoría.



Aprende más

Los siguientes controles proporcionan instrucciones adicionales:

- NIST SP 800-53 AU-3 Contenido de los registros de auditoría
- Escaneo de vulnerabilidades NIST SP 800-53 RA-5
- NIST SP 800-53 AU-6 Revisión de auditoría, análisis e informes

4.2 Pasos avanzados

4.2.1 Adopte estándares para implementaciones seguras de redes y VMS

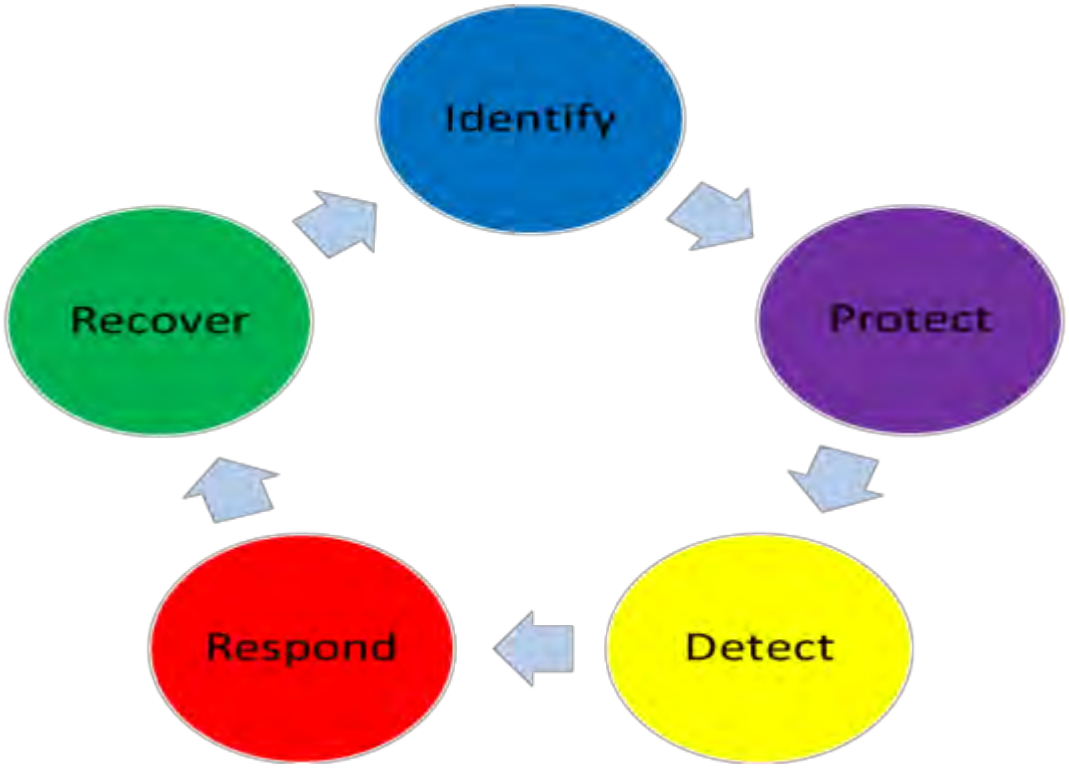
MOBOTIX recomienda que adopte estándares para redes seguras e implementaciones de MOBOTIX HUB VMS. El uso de estándares es un componente básico de Internet y de la ingeniería de redes, y la base de la

interoperabilidad y la conformidad del sistema. Esto también se aplica al uso de soluciones criptográficas, donde la criptografía basada en estándares es el enfoque más comúnmente aceptado.

4.2.2 Establecer un plan de respuesta a incidentes

MOBOTIX recomienda comenzar con un conjunto de políticas y procedimientos y establecer un plan de respuesta a incidentes. Designe personal para monitorear el estado del sistema y responder a eventos sospechosos. Por ejemplo, actividades que ocurren en momentos inusuales. Establezca un punto de contacto (POC) de seguridad con cada uno de sus proveedores, incluido MOBOTIX.

La siguiente imagen es una adaptación del Marco de Ciberseguridad del NIST (http://www.nist.gov/cyberframework/). Muestra el ciclo de vida que se debe tener en cuenta al crear un plan. El material de apoyo del marco proporciona detalles sobre el ciclo de vida y los controles de seguridad de los planes de respuesta a incidentes.



Aprende más

Los siguientes controles proporcionan instrucciones adicionales:

- NIST SP 800-53 IR 1-13 Respuesta a incidentes

4.2.3 Proteja los componentes confidenciales de VMS

MOBOTIX recomienda utilizar el control de acceso físico y utilizar el VMS para supervisar y proteger sus componentes sensibles del VMS. La restricción física y el control de acceso físico basado en roles son contramedidas que mantienen la seguridad de los servidores y las estaciones de trabajo.

Los administradores y usuarios solo deben tener acceso a la información que necesitan para cumplir con sus responsabilidades. Si todos los usuarios internos tienen el mismo nivel de acceso a los datos críticos, es más fácil para los atacantes acceder a la red.

Aprende más

Los siguientes controles proporcionan instrucciones adicionales:

- NIST SP 800-53 PE-1 Política y Procedimientos de Protección Física y Ambiental
- Autorizaciones de acceso físico NIST SP 800-53 PE-2
- NIST SP 800-53 PE-3 Control de acceso físico
- NIST SP 800-53 AC-4 Privilegio mínimo

4.2.4 Siga las prácticas recomendadas de seguridad del sistema operativo de Microsoft

MOBOTIX recomienda seguir las mejores prácticas de seguridad para los sistemas operativos (SO) de Microsoft para mitigar los riesgos del SO y mantener la seguridad. Esto le ayudará a mantener seguros los servidores de Microsoft y los equipos cliente.

Para obtener más información, consulte *Guía de actualización de seguridad de Microsoft* (https://msrc.microsoft.com/update-guide).

4.2.5 Usar herramientas para automatizar o implementar la política de seguridad

MOBOTIX recomienda que busque una o varias herramientas que le ayuden a automatizar e implementar la política de seguridad. La automatización reduce el riesgo de error humano y facilita la gestión de la política. Por ejemplo, puede automatizar la instalación de parches de seguridad y actualizaciones en servidores y equipos cliente.

Una manera de implementar esta recomendación es combinar Microsoft Security Configuration Manager (SCCM) con el Protocolo de automatización de contenido de seguridad (SCAP). (Véase, por ejemplo, *Geek de todos los oficios: Automatice la configuración de seguridad de referencia* (https://technet.microsoft.com/en-us/magazine/ff721825.aspx) y *el programa de validación (https://csrc.nist.gov/projects/scap-validation-program) del protocolo de automatización de contenido de seguridad (SCAP*).) Esto le proporciona un marco para crear, distribuir y validar la configuración de seguridad en los equipos de toda la red.

Aprende más

Los siguientes controles proporcionan instrucciones adicionales:

- Política y procedimientos de administración de configuración de NIST SP 800-53 CM-1
- Configuración de línea base NIST SP 800-53 CM-2
- NIST SP 800-53 CM-3 Control de cambio de configuración

4.2.6 Siga las mejores prácticas de seguridad de red establecidas

MOBOTIX recomienda seguir las mejores prácticas de TI y del proveedor para asegurarse de que los dispositivos de su red estén configurados de forma segura. Pida a sus proveedores que proporcionen esta información. Es importante iniciar y mantener un diálogo sobre seguridad, y un buen punto de partida es un debate sobre las mejores prácticas.

Es importante denegar el acceso al VMS no utilizando la configuración de red vulnerable. Para obtener más información, consulte *SP 800-128* (https://csrc.nist.gov/publications/detail/sp/800-128/final), *SP 800-41-rev1* (https://csrc.nist.gov/publications/detail/sp/800-41/rev-1/final) (específico para firewalls) y *Estándares y referencias de ICS-CERT* (https://www.cisa.gov/ics) (lista general).

Aprende más

Los siguientes controles proporcionan instrucciones adicionales:

- Ajustes de configuración de NIST 800-53 CM-6
- NIST 800-53 MA-3 Herramientas de mantenimiento

5 Dispositivos y red

En esta sección se proporcionan instrucciones para proteger los dispositivos y los componentes de red relacionados con MOBOTIX HUB VMS. Esto incluye partes clave del sistema, como las cámaras, el almacenamiento y la red.

Los sistemas de vigilancia a menudo incluyen cámaras en el borde de la red. Las cámaras y sus conexiones de red, si se dejan desprotegidas, representan un riesgo significativo de compromiso, lo que podría dar a los intrusos un mayor acceso al sistema.

5.1 Pasos básicos – Dispositivos

5.1.1 Utilice contraseñas seguras en lugar de contraseñas predeterminadas

MOBOTIX recomienda cambiar las contraseñas predeterminadas de los dispositivos, por ejemplo, de una cámara. No utilice contraseñas predeterminadas porque a menudo se publican en Internet y están fácilmente disponibles. En su lugar, utilice contraseñas seguras para los dispositivos. Las contraseñas seguras incluyen ocho o más caracteres alfanuméricos, usan mayúsculas y minúsculas y caracteres especiales.

Aprende más

Los siguientes controles proporcionan instrucciones adicionales:

- Administración de autenticadores NIST 800-53 IA-4
- Comentarios del autenticador NIST 800-53 IA-8
- NIST 800-53 SI-11 Manejo de errores

5.1.2 Detener los servicios y protocolos no utilizados

Para ayudar a evitar el acceso no autorizado o la divulgación de información, MOBOTIX recomienda que detenga los servicios y protocolos no utilizados en los dispositivos. Por ejemplo, Telnet, SSH, FTP, UPnP, Ipv6 y Bonjour. También es importante utilizar una autenticación segura en cualquier servicio que acceda al VMS, la red o los dispositivos. Por ejemplo, use claves SSH en lugar de nombres de usuario y contraseñas, y use certificados de una autoridad de certificación para HTTPS. Para obtener más información, consulte las guías de protección y otras instrucciones del fabricante del dispositivo.

Aprende más

Los siguientes controles proporcionan instrucciones adicionales:

- Acceso remoto NIST SP 800-53 AC-17 (deshabilitar protocolos no utilizados)
- Ajustes de configuración de NIST SP 800-53 CM-6
- NIST SP 800-53 CM-7 Funcionalidad mínima

- NIST SP 800-53 IA-2 Identificación y autenticación
- NIST SP 800-53 SA-9 Servicios de información externa

5.1.3 Crear cuentas de usuario dedicadas en cada dispositivo

Todas las cámaras tienen una cuenta de usuario predeterminada con un nombre de usuario y una contraseña que el VMS utiliza para acceder al dispositivo. Con fines de auditoría, MOBOTIX recomienda cambiar el nombre de usuario y la contraseña predeterminados.

Cree una cuenta de usuario específica para su uso por el VMS y utilice esta cuenta de usuario y contraseña cuando agregue la cámara al VMS. Cuando un servidor de grabación se conecta a la cámara, utiliza el nombre de usuario y la contraseña que ha creado. Si la cámara tiene un registro, este registro muestra que el servidor de grabación se ha conectado a la cámara.

Con un nombre de usuario y una contraseña dedicados, los registros del dispositivo pueden ayudarlo a determinar si un servidor de grabación o una persona accedió a la cámara. Esto es relevante cuando se investigan posibles problemas de seguridad que afectan a los dispositivos.

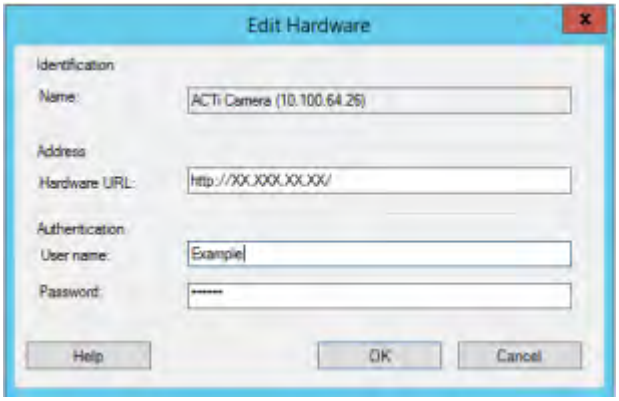
Puede cambiar el nombre de usuario y la contraseña de un dispositivo antes o después de agregarlo en Management Client.

Para cambiar el nombre de usuario y la contraseña antes de agregar el dispositivo, siga estos pasos:

1. Vaya a la interfaz web del dispositivo y cambie el nombre de usuario y la contraseña predeterminados.
2. En Cliente de administración, agregue el dispositivo y especifique el nombre de usuario y la contraseña.

Para cambiar el nombre de usuario y las contraseñas de los dispositivos que ya están agregados, siga estos pasos:

1. En Cliente de administración, en el panel Navegación del sitio, expanda el nodo Servidores y seleccione Servidores de grabación.
2. En el panel Servidor de grabación, expanda el servidor de grabación que contiene el dispositivo y, a continuación, haga clic con el botón secundario en el dispositivo y seleccione Editar hardware.



3. En Autenticación, introduzca el nuevo nombre de usuario y contraseña.

Aprende más

Los siguientes controles proporcionan instrucciones adicionales:

- NIST SP 800-53 AC-2 Administración de cuentas
- NIST SP 800-53 AC-4 Privilegio mínimo

5.1.4 Escaneo de dispositivos

El análisis de dispositivos (por ejemplo, **el análisis** rápido o el **análisis de intervalo de direcciones** al agregar hardware) se realiza mediante difusiones que pueden contener nombres de usuario y contraseñas en texto sin formato.

A menos que se trate de una configuración inicial, esta funcionalidad no debe utilizarse para agregar dispositivos al sistema. En su lugar, utilice la **opción Manual** y seleccione manualmente el controlador.

En sistemas sensibles, la función **de detección automática de dispositivos** debe estar desactivada en MOBOTIX HUB Professional VMS (ubicada en **Configuración** > **Conexión de dispositivos de hardware**), ya que enviará periódicamente difusiones que pueden contener nombres de usuario y contraseñas.

5.2 Pasos básicos – Red

5.2.1 Utilice una conexión de red segura y de confianza

Las comunicaciones de red deben ser seguras, ya sea que esté en una red cerrada o no. De forma predeterminada, se deben utilizar comunicaciones seguras al acceder al VMS. Por ejemplo:

- Túneles VPN o HTTPS de forma predeterminada
- Última versión de Transport Layer Security (https://datatracker.ietf.org/wg/tls/charter/) (TLS, actualmente 1.2) con certificados válidos que cumplen con las mejores prácticas de la industria, como los de Public-Key Infrastructure (X.509) (https://datatracker.ietf.org/wg/ipsec/documents/) y CA/Browser Forum (https://cabforum.org/).

De lo contrario, las credenciales pueden verse comprometidas y los intrusos pueden usarlas para acceder al VMS. Configure la red para permitir que los equipos cliente establezcan sesiones HTTPS seguras o túneles VPN entre los dispositivos cliente y los servidores VMS.

Aprende más

Los siguientes controles proporcionan instrucciones adicionales:

- NIST SP 800-53 SI-2 Corrección de defectos
- Ajustes de configuración de NIST SP 800-53 CM-6
- NIST SP 800-53 SC-23 Autenticidad de la sesión

5.2.2 Utilice firewalls para limitar el acceso IP a servidores y equipos

MOBOTIX recomienda utilizar conexiones seguras y los siguientes pasos adicionales:

- Usar la autenticación segura de dispositivos
- Usar TLS
- Usar la lista blanca de dispositivos para autenticar dispositivos
- Utilice firewalls para limitar la comunicación de red entre los servidores y los equipos y programas cliente.

los componentes de MOBOTIX HUB y los puertos que necesitan se enumeran en las secciones individuales a continuación. Para asegurarse, por ejemplo, de que el cortafuegos bloquea solo el tráfico no deseado, debe especificar los puertos que utiliza el MOBOTIX HUB VMS. Solo debe habilitar estos puertos. Las listas también incluyen los puertos utilizados para los procesos locales.

Se organizan en dos grupos:

- Componentes del servidor (servicios): ofrecen su servicio en los puertos, por lo que deben escuchar las solicitudes de los clientes en estos puertos. Por lo tanto, estos puertos deben abrirse en el Firewall de Windows para las conexiones entrantes.
- Componentes de cliente (clientes): inicie conexiones a los puertos de los componentes del servidor. Por lo tanto, estos puertos deben abrirse para las conexiones salientes. Las conexiones salientes suelen estar abiertas de forma predeterminada en el Firewall de Windows.

Si no se menciona nada más, los puertos para los componentes del servidor deben abrirse para las conexiones entrantes y los puertos para los componentes del cliente deben abrirse para las conexiones salientes.

Tenga en cuenta que los componentes del servidor también pueden actuar como clientes de otros componentes del servidor.

Los números de puerto son los números predeterminados, pero esto se puede cambiar. Póngase en contacto con el servicio de asistencia de MOBOTIX si necesita cambiar los puertos que no se pueden configurar a través del cliente de gestión.

Componentes del servidor (conexiones entrantes)

En cada una de las secciones siguientes se enumeran los puertos que deben abrirse para un servicio en particular. Para averiguar qué puertos deben abrirse en una computadora en particular, debe considerar todos los servicios que se ejecutan en esta computadora.

Restrinja el acceso remoto al servidor de administración agregando reglas de firewall para permitir que solo los servidores de grabación se conecten al puerto TCP 9993.

Servicio de servidor de administración y procesos relacionados

Número de puerto	Protocolo	Proceso	Conexiones desde...	Propósito
80	HTTP	IIS	Todos los servidores, el cliente inteligente MOBOTIX HUB y el cliente de gestión	El propósito del puerto 80 y el puerto 443 es el mismo. Sin embargo, el puerto que usa el VMS depende de si ha usado certificados para proteger la comunicación. • Cuando no se ha asegurado la comunicación con los certificados, el VMS utiliza el puerto 80. • Cuando haya protegido la comunicación con certificados, el VMS utiliza el puerto 443, excepto para la comunicación entre el servidor de eventos y el servidor de administración. La comunicación entre el servidor de eventos y el servidor de administración utiliza Windows Secured Framework (WCF) y la autenticación de Windows en el puerto 80.
443	HTTPS	IIS		
6473	TCP	Servicio de servidor de administración	Icono de la bandeja del Administrador del servidor de administración, solo conexión local.	Mostrar el estado y administrar el servicio.
8080	TCP	Servidor de administración	Solo conexión local.	Comunicación entre procesos internos en el servidor.
9000	HTTP	Servidor de administración	Servicios de servidor de grabación	Servicio web para la comunicación interna entre servidores.

Número de puerto	Protocolo	Proceso	Conexiones desde...	Propósito
12345	TCP	Servicio de servidor de administración	Cliente inteligente MOBOTIX HUB	Comunicación entre el sistema y los destinatarios de la Matriz. Puede cambiar el número de puerto en el cliente de administración.
12974	TCP	Servicio de servidor de administración	Servicio SNMP de Windows	Comunicación con el agente de extensión SNMP. No utilice el puerto para otros fines, incluso si su sistema no aplica SNMP. En los sistemas MOBOTIX HUB 2014 o anteriores, el número de puerto era 6475. En los sistemas MOBOTIX HUB 2019 R2 y anteriores, el número de puerto era 7475.

Servicio SQL Server

Número de puerto	Protocolo	Proceso	Conexiones desde...	Propósito
1433	TCP	Servidor SQL	Servicio de servidor de administración	Almacenamiento y recuperación de configuraciones.
1433	TCP	Servidor SQL	Servicio de servidor de eventos	Almacenamiento y recuperación de eventos.
1433	TCP	Servidor SQL	Servicio de servidor de registros	Almacenamiento y recuperación de entradas de registro.

Servicio de recopilador de datos

Número de puerto	Protocolo	Proceso	Conexiones desde...	Propósito
7609	HTTP	IIS	En el equipo del servidor de administración: servicios de recopilador de datos en todos los demás servidores. En otros equipos: Servicio de recopilador de datos en el servidor de administración.	Monitor del sistema.

Servicio de servidor de eventos

Número de puerto	Protocolo	Proceso	Conexiones desde...	Propósito
1234	TCP/UDP	Servicio de servidor de eventos	Cualquier servidor que envíe eventos genéricos a su sistema MOBOTIX HUB.	Escucha de eventos genéricos de sistemas o dispositivos externos. Solo si la fuente de datos relevante está habilitada.
1235	TCP	Servicio de servidor de eventos	Cualquier servidor que envíe eventos genéricos a su sistema MOBOTIX HUB.	Escucha de eventos genéricos de sistemas o dispositivos externos. Solo si la fuente de datos relevante está habilitada.
9090	TCP	Servicio de servidor de eventos	Cualquier sistema o dispositivo que envíe eventos analíticos a su sistema MOBOTIX HUB.	Escuchar eventos de análisis de sistemas o dispositivos externos. Solo es relevante si la función Eventos de Analytics está habilitada.
22331	TCP	Servicio de servidor de eventos	MOBOTIX HUB Smart Client y el cliente de gestión	Configuración, eventos, alarmas y datos de mapas.
22333	TCP	Servicio de servidor de eventos	Plug-ins y aplicaciones de MIP.	Mensajería MIP.

Servicio de servidor de grabación

Número de puerto	Protocolo	Proceso	Conexiones desde...	Propósito
25	SMTP	Servicio de servidor de grabación	Cámaras, codificadores y dispositivos de E/S.	Escuchar mensajes de eventos de dispositivos. El puerto está deshabilitado de forma predeterminada. (En desuso) Al habilitar esta opción, se abrirá un puerto para conexiones no cifradas y no se recomienda.
5210	TCP	Servicio de servidor de grabación	Servidores de grabación de conmutación por error.	Fusión de bases de datos después de que se haya ejecutado un servidor de grabación de conmutación por error.
5432	TCP	Servicio de servidor de grabación	Cámaras, codificadores y dispositivos de E/S.	Escuchar mensajes de eventos de dispositivos.

Número de puerto	Protocolo	Proceso	Conexiones desde...	Propósito
				El puerto está deshabilitado de forma predeterminada.
7563	TCP	Servicio de servidor de grabación	MOBOTIX HUB Smart Client, cliente de gestión	Recuperación de flujos de vídeo y audio, comandos PTZ.
8966	TCP	Servicio de servidor de grabación	Icono de la bandeja del Administrador del servidor de grabación, solo conexión local.	Mostrar el estado y administrar el servicio.
9001	HTTP	Servicio de servidor de grabación	Servidor de administración	Servicio web para la comunicación interna entre servidores. Si hay varias instancias de Recording Server en uso, cada instancia necesita su propio puerto. Los puertos adicionales serán 9002, 9003, etc.
11000	TCP	Servicio de servidor de grabación	Servidores de grabación de conmutación por error	Sondeo del estado de los servidores de grabación.
12975	TCP	Servicio de servidor de grabación	Servicio SNMP de Windows	Comunicación con el agente de extensión SNMP. No utilice el puerto para otros fines, incluso si su sistema no aplica SNMP. En los sistemas MOBOTIX HUB 2014 o anteriores, el número de puerto era 6474. En los sistemas MOBOTIX HUB 2019 R2 y anteriores, el número de puerto era 7474.
65101	UDP	Servicio de servidor de grabación	Solo conexión local	Escuchar las notificaciones de eventos de los conductores.

Además de las conexiones entrantes al servicio de servidor de grabación mencionado anteriormente, el servicio de servidor de grabación establece conexiones de salida a cámaras, NVR y sitios remotos interconectados (MOBOTIX Interconnect ICP).

Servicio de servidor de conmutación por error y servicio de servidor de grabación de conmutación por error

Número de puerto	Protocolo	Proceso	Conexiones desde...	Propósito
25	SMTP	Servicio de servidor de grabación de conmutación por error	Cámaras, codificadores y dispositivos de E/S.	Escuchar mensajes de eventos de dispositivos. El puerto está deshabilitado de forma predeterminada. (En desuso) Al habilitar esta opción, se abrirá un puerto para conexiones no cifradas y no se recomienda.
5210	TCP	Servicio de servidor de grabación de conmutación por error	Servidores de grabación de conmutación por error	Fusión de bases de datos después de que se haya ejecutado un servidor de grabación de conmutación por error.
5432	TCP	Servicio de servidor de grabación de conmutación por error	Cámaras, codificadores y dispositivos de E/S.	Escuchar mensajes de eventos de dispositivos. El puerto está deshabilitado de forma predeterminada.
7474	TCP	Servicio de servidor de grabación de conmutación por error	Servicio SNMP de Windows	Comunicación con el agente de extensión SNMP. No utilice el puerto para otros fines, incluso si su sistema no aplica SNMP.
7563	TCP	Servicio de servidor de grabación de conmutación por error	Cliente inteligente MOBOTIX HUB	Recuperación de flujos de vídeo y audio, comandos PTZ.
8844	UDP	Servicio de servidor de grabación de conmutación por error	Solo conexión local.	Comunicación entre los servidores.
8966	TCP	Servicio de servidor de grabación de conmutación por error	Icono de la bandeja del Administrador del servidor de grabación por error, solo conexión local.	Mostrar el estado y administrar el servicio.
8967	TCP	Servicio de servidor de conmutación por error	Icono de bandeja del Administrador del servidor de conmutación por error, solo conexión local.	Mostrar el estado y administrar el servicio.
8990	TCP	Servicio de servidor de conmutación por error	Servicio de servidor de administración	Supervisión del estado del servicio del servidor de conmutación por error.

Número de puerto	Protocolo	Proceso	Conexiones desde...	Propósito
9001	HTTP	Servicio de servidor de conmutación por error	Servidor de administración	Servicio web para la comunicación interna entre servidores.

Además de las conexiones entrantes al servicio Servidor de conmutación por error/Servidor de grabación por conmutación enumerado anteriormente, el servicio Servidor de conmutación por error/Servidor de grabación por conmutación por error establece conexiones salientes con las grabadoras, cámaras y para inserción de vídeo habituales.

Servicio de servidor de registros

Número de puerto	Protocolo	Proceso	Conexiones desde...	Propósito
22337	HTTP	Servicio de servidor de registros	Todos los componentes de MOBOTIX HUB, excepto el cliente de gestión y el servidor de grabación.	Escriba, lea y configure el servidor de registros.

Servicio de servidor móvil

Número de puerto	Protocolo	Proceso	Conexiones desde...	Propósito
8000	TCP	Servicio de servidor móvil	Icono de la bandeja del Administrador del servidor móvil, solo conexión local.	Aplicación SysTray.
8081	HTTP	Servicio de servidor móvil	Clientes móviles, clientes web y clientes de administración.	Envío de flujos de datos; video y audio.
8082	HTTPS	Servicio de servidor móvil	Clientes móviles y clientes web.	Envío de flujos de datos; video y audio.
40001 - 40099	HTTP	Servicio de servidor móvil	Servicio de servidor de grabación	Empuje de video para servidor móvil. Este intervalo de puertos está deshabilitado de forma predeterminada.

Servicio de servidor LPR

Número de puerto	Protocolo	Proceso	Conexiones desde...	Propósito
22334	TCP	Servicio de servidor LPR	Servidor de eventos	Recuperación de matrículas reconocidas y estado del servidor. Para conectarse, el servidor de eventos debe tener instalado el complemento LPR.
22334	TCP	Servicio de servidor LPR	Icono de la bandeja del Administrador del servidor LPR, solo conexión local.	Aplicación SysTray

Servicio MOBOTIX Open Network Bridge

Número de puerto	Protocolo	Proceso	Conexiones desde...	Propósito
580	TCP	Servicio de puente de red abierta de MOBOTIX	Clientes ONVIF	Autenticación y solicitudes de configuración de transmisión de vídeo.
554	RTSP	Servicio RTSP	Clientes ONVIF	Transmisión de video solicitado a clientes ONVIF.

Servicio de servidor MOBOTIX HUB DLNA

Número de puerto	Protocolo	Proceso	Conexiones desde...	Propósito
9100	HTTP	Servicio de servidor DLNA	Dispositivo DLNA	Detección de dispositivos y configuración de canales DLNA. Solicitudes de transmisiones de vídeo.
9200	HTTP	Servicio de servidor DLNA	Dispositivo DLNA	Transmisión de vídeo solicitado a dispositivos DLNA.

Servicio de grabación de pantalla MOBOTIX HUB

Número de puerto	Protocolo	Proceso	Conexiones desde...	Propósito
52111	TCP	Grabador de pantalla MOBOTIX HUB	Servicio de servidor de grabación	Proporciona vídeo desde un monitor. Aparece y actúa de la misma manera que una cámara en el servidor de grabación.

Número de puerto	Protocolo	Proceso	Conexiones desde...	Propósito
				Puede cambiar el número de puerto en el cliente de administración.

Servicio de gestión de incidencias MOBOTIX HUB

Número de puerto	Protocolo	Proceso	Conexiones desde...	Propósito
80	HTTP	IIS	MOBOTIX HUB Smart Client y el cliente de gestión	El propósito del puerto 80 y el puerto 443 es el mismo. Sin embargo, el puerto que usa el VMS depende de si ha usado certificados para proteger la comunicación. • Cuando no se ha asegurado la comunicación con los certificados, el VMS utiliza el puerto 80. • Cuando haya asegurado la comunicación con certificados, el VMS utiliza el puerto 443
443	HTTPS			

Componentes del servidor (conexiones salientes)

Servicio de servidor de administración

Número de puerto	Protocolo	Conexiones a...	Propósito
443	HTTPS	El servidor de licencias que aloja el servicio de administración de licencias.	Activación de licencias.

Servicio de servidor de grabación

Número de puerto	Protocolo	Conexiones a...	Propósito
80	HTTP	Cámaras, NVR, codificadores Sitios interconectados	Autenticación, configuración, flujos de datos, vídeo y audio. Iniciar sesión
443	HTTPS	Cámaras, NVR, codificadores	Autenticación, configuración, flujos de datos, vídeo y audio.
554	RTSP	Cámaras, NVR, codificadores	Flujos de datos, vídeo y audio.
7563	TCP	Sitios interconectados	Flujos de datos y eventos.
11000	TCP	Servidores de grabación de conmutación por error	Sondeo del estado de los servidores de grabación.
40001 – 40099	HTTP	Servicio de servidor móvil	Empuje de video para servidor móvil. Este intervalo de puertos está deshabilitado de forma predeterminada.

Servicio de servidor de conmutación por error y servicio de servidor de grabación de conmutación por error

Número de puerto	Protocolo	Conexiones a...	Propósito
11000	TCP	Servidores de grabación de conmutación por error	Sondeo del estado de los servidores de grabación.

Servicio de servidor de registros

Número de puerto	Protocolo	Conexiones a...	Propósito
443	HTTPS	Servidor de registros	Reenvío de mensajes al servidor de registros.

Puerta de enlace de API

Número de puerto	Protocolo	Conexiones a...	Propósito
80	HTTP	Servidor de administración	RESTful API
443	HTTPS	Servidor de administración	RESTful API

Cámaras, codificadores y dispositivos de E/S (conexiones entrantes)

Número de puerto	Protocolo	Conexiones desde...	Propósito
80	TCP	Servidores de grabación y servidores de grabación de conmutación por error	Autenticación, configuración y flujos de datos; video y audio.
443	HTTPS	Servidores de grabación y servidores de grabación de conmutación por error	Autenticación, configuración y flujos de datos; video y audio.
554	RTSP	Servidores de grabación y servidores de grabación de conmutación por error	Flujos de datos; video y audio.

Cámaras, codificadores y dispositivos de E/S (conexiones salientes)

Número de puerto	Protocolo	Conexiones a...	Propósito
25	SMTP	Servidores de grabación y servidores de grabación de conmutación por error	Envío de notificaciones de eventos (en desuso).
5432	TCP	Servidores de grabación y servidores de grabación de conmutación por error	Envío de notificaciones de eventos. El puerto está deshabilitado de forma predeterminada.
22337	HTTP	Servidor de registros	Reenvío de mensajes al servidor de registros.

Solo unos pocos modelos de cámara son capaces de establecer conexiones de salida.

Componentes de cliente (conexiones salientes)

Cliente inteligente MOBOTIX HUB, Cliente de gestión MOBOTIX HUB, Servidor móvil MOBOTIX HUB

Número de puerto	Protocolo	Conexiones a...	Propósito
80	HTTP	Servicio de servidor de administración	Autenticación
443	HTTPS	Servicio de servidor de administración	Autenticación de usuarios básicos.
7563	TCP	Servicio de servidor de grabación	Recuperación de flujos de vídeo y audio, comandos PTZ.
22331	TCP	Servicio de servidor de eventos	Alarmas.

Cliente web MOBOTIX HUB, cliente móvil MOBOTIX HUB

Número de puerto	Protocolo	Conexiones a...	Propósito
8081	HTTP	Servidor móvil MOBOTIX HUB	Recuperación de secuencias de vídeo y audio.
8082	HTTPS	Servidor móvil MOBOTIX HUB	Recuperación de secuencias de vídeo y audio.

Aprende más

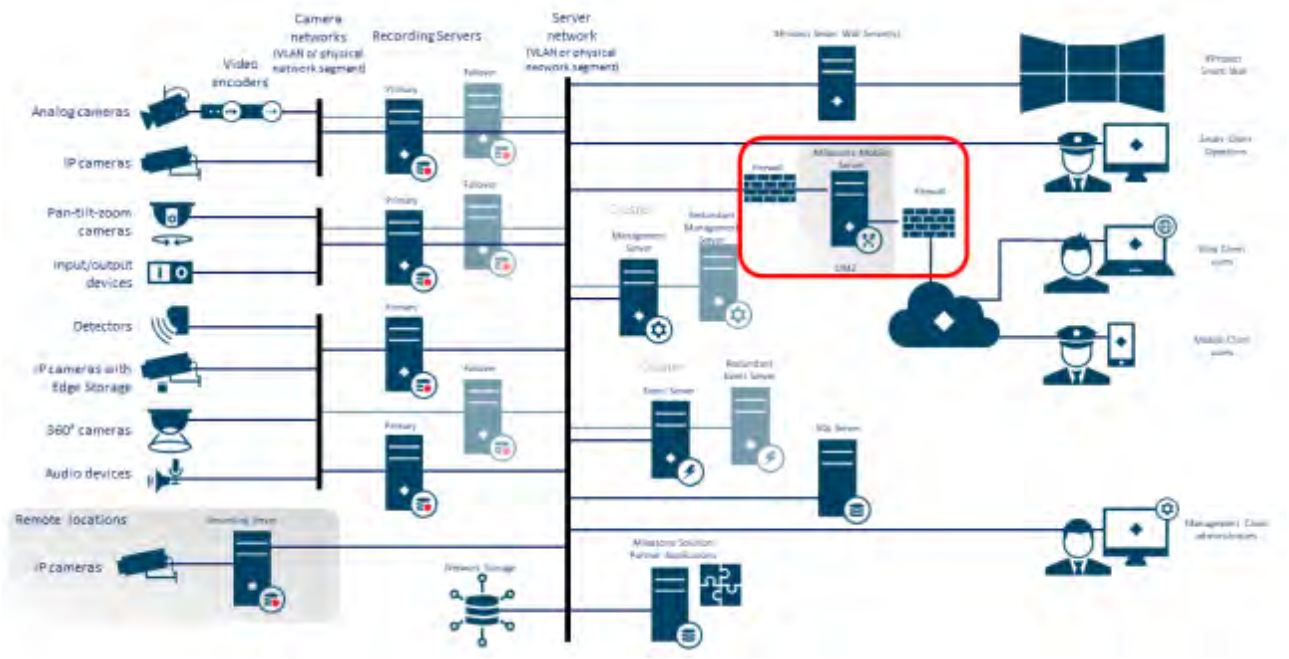
Los siguientes controles proporcionan instrucciones adicionales:

- Interconexiones de sistemas NIST SP 800-53 CA-3
- Ajustes de configuración de NIST SP 800-53 CM-6
- NIST SP 800-53 SC-7 Protección de límites

5.2.3 Utilice un firewall entre el VMS e Internet

El VMS no debe conectarse directamente a Internet. Si expone partes del VMS a Internet, MOBOTIX recomienda utilizar un cortafuegos configurado adecuadamente entre el VMS e Internet.

Si es posible, exponga solo el componente de servidor móvil de MOBOTIX a Internet y ubíquelo en una zona desmilitarizada (DMZ) con cortafuegos a ambos lados. Esto se ilustra en la siguiente figura.



Aprende más

Los siguientes controles proporcionan instrucciones adicionales:

- Interconexiones de sistemas NIST SP 800-53 CA-3

5.2.4 Conecte la subred de la cámara solo a la subred del servidor de grabación

MOBOTIX recomienda conectar la subred de la cámara únicamente a la subred del servidor de grabación. Las cámaras y otros dispositivos solo necesitan comunicarse con los servidores de grabación. Para obtener más información, consulte Servidor de grabación en la página 63.

Aprende más

Los siguientes controles proporcionan instrucciones adicionales:

- NIST 800-53 SC-7 Protección de límites

5.3 Pasos avanzados – Dispositivos

5.3.1 Utilice el protocolo simple de administración de red para monitorear eventos

MOBOTIX recomienda utilizar el Protocolo simple de gestión de red (SNMP) para supervisar los eventos en los dispositivos de la red. Puede utilizar SNMP como complemento para syslog. SNMP funciona en tiempo real con muchos tipos de eventos que pueden activar alertas, por ejemplo, si se reinicia un dispositivo.

Para que esto funcione, los dispositivos deben admitir el registro a través de SNMP.

Hay varias versiones de protocolos SNMP disponibles. Las versiones 2c y 3 son las más actuales. La implementación implica un conjunto de estándares. Se puede encontrar una buena descripción general en el sitio de referencia de SNMP (http://www.snmp.com/protocol/snmp_rfcs.shtml).

Aprende más

Los siguientes controles proporcionan instrucciones adicionales:

- Monitoreo de eventos NIST SP 800-53 SI-4

5.4 Pasos avanzados – Red

5.4.1 Usar protocolos inalámbricos seguros

Si utiliza redes inalámbricas, MOBOTIX recomienda utilizar un protocolo inalámbrico seguro para evitar el acceso no autorizado a dispositivos y ordenadores. Por ejemplo, utilice configuraciones estandarizadas. La guía del NIST sobre redes de área local inalámbricas proporciona detalles específicos sobre la administración y configuración de la red. Para obtener más información, consulte *SP 800-48 revisión 1, Guía para proteger redes inalámbricas IEEE 802.11 heredadas* (https://csrc.nist.gov/publications/detail/sp/800-48/rev-1/archive/2008-07-25).
Además, MOBOTIX recomienda no utilizar cámaras inalámbricas en ubicaciones de misión crítica. Las cámaras inalámbricas son fáciles de interferir, lo que puede provocar la pérdida de vídeo.

Aprende más

Los siguientes controles proporcionan instrucciones adicionales:

- Acceso inalámbrico NIST SP 800-53 AC-18
- NIST SP 800-53 SC-40 Protección de enlace inalámbrico

5.4.2 Usar el control de acceso basado en puertos

Utilice el control de acceso basado en puertos para evitar el acceso no autorizado a la red de cámaras. Si un dispositivo no autorizado se conecta a un puerto de switch o router, el puerto debe bloquearse. La información sobre cómo configurar switches y routers está disponible en los fabricantes. Consulte *SP 800-128, Guía para la gestión de la configuración centrada en la seguridad de los sistemas de información* (https://csrc.nist.gov/publications/detail/sp/800-128/final), para obtener información sobre la gestión de la configuración de los sistemas de información.

Aprende más

Los siguientes controles proporcionan instrucciones adicionales:

- Política y procedimientos de administración de configuración NIST 800-53 CM-1
- Configuración de línea base NIST 800-53 CM-2
- NIST 800-53 AC-4 Privilegio mínimo
- Ajustes de configuración de NIST 800-53 CM-6
- NIST 800-53 CM-7 Funcionalidad mínima

5.4.3 Ejecute el VMS en una red dedicada

MOBOTIX recomienda que, siempre que sea posible, separe la red en la que se ejecuta el VMS de las redes con otros fines. Por ejemplo, una red compartida, como la red de impresoras, debe estar aislada de la red VMS. Además, las implementaciones de MOBOTIX HUB VMS deben seguir un conjunto general de prácticas recomendadas para las interconexiones de sistemas.

Aprende más

Los siguientes controles proporcionan instrucciones adicionales:

- Interconexiones de sistemas NIST SP 800-53 CA-3

6 Servidores MOBOTIX

6.1 Pasos básicos – Servidores MOBOTIX

6.1.1 Utilice controles de acceso físico y supervise la sala de servidores

MOBOTIX recomienda que coloque el hardware con los servidores instalados en una sala de servidores designada y que utilice controles de acceso físicos. Además, debe mantener registros de acceso para documentar quién ha tenido acceso físico a los servidores. La vigilancia de la sala de servidores también es una precaución preventiva. MOBOTIX admite la integración de los sistemas de control de acceso y su información. Por ejemplo, puede ver los registros de acceso en MOBOTIX HUB Smart Client.

Aprende más

Los siguientes controles proporcionan instrucciones adicionales:

- NIST 800-53 PE-3 Control de acceso físico

6.1.2 Utilizar canales de comunicación encriptados

MOBOTIX recomienda utilizar una VPN para los canales de comunicación de las instalaciones en las que los servidores se distribuyen a través de redes que no son de confianza. Esto es para evitar que los atacantes intercepten las comunicaciones entre los servidores. Incluso en el caso de redes de confianza, MOBOTIX recomienda utilizar HTTPS para la configuración de cámaras y otros componentes del sistema.

Aprende más

Los siguientes controles proporcionan instrucciones adicionales:

- NIST 800-53 AC-4 Aplicación del flujo de información
- Acceso remoto NIST 800-53 AC-17

6.2 Pasos avanzados: servidores MOBOTIX

6.2.1 Ejecución de servicios con cuentas de servicio

MOBOTIX recomienda crear cuentas de servicio para los servicios relacionados con MOBOTIX HUB VMS, en lugar de utilizar una cuenta de usuario normal. Configure las cuentas de servicio como usuarios del dominio y asígneles solo

los permisos necesarios para ejecutar los servicios relevantes. Ver 4.1.11 Autenticación Kerberos (explicación). Por ejemplo, la cuenta de servicio no debería poder iniciar sesión en el escritorio de Windows.

Aprende más

Los siguientes controles proporcionan instrucciones adicionales:

- NIST 800-53 AC-5 Separación de funciones
- NIST 800-53 AC-6 Privilegio mínimo

6.2.2 Ejecución de componentes en servidores físicos o virtuales dedicados

MOBOTIX recomienda ejecutar los componentes de MOBOTIX HUB VMS solo en servidores virtuales o físicos dedicados sin ningún otro software o servicio instalado.

Aprende más

Los siguientes controles proporcionan instrucciones adicionales:

- Plan de gestión de configuración NIST 800-53 CM-9

6.2.3 Restrinja el uso de medios extraíbles en computadoras y servidores

MOBOTIX recomienda restringir el uso de medios extraíbles, por ejemplo, llaves USB, tarjetas SD y teléfonos inteligentes en ordenadores y servidores en los que estén instalados componentes de MOBOTIX HUB VMS. Esto ayuda a evitar que el malware ingrese a la red. Por ejemplo, permita que solo los usuarios autorizados conecten medios extraíbles cuando necesite transferir pruebas de vídeo.

Aprende más

Los siguientes controles proporcionan instrucciones adicionales:

- Uso de medios NIST 800-53 MP-7

6.2.4 Utilice cuentas de administrador individuales para una mejor auditoría

A diferencia de las cuentas de administrador compartidas, MOBOTIX recomienda utilizar cuentas individuales para los administradores. Esto le permite realizar un seguimiento de quién hace qué en MOBOTIX HUB VMS. Esto ayuda a evitar que el malware ingrese a la red. A continuación, puede utilizar un directorio autoritativo, como Active Directory, para administrar las cuentas de administrador.
Asigne cuentas de administrador a roles en Cliente de administración en **Roles**.

Aprende más

Los siguientes controles proporcionan instrucciones adicionales:

- NIST 800-53 AC-5 Separación de funciones
- Plan de gestión de configuración NIST 800-53 CM-9

6.2.5 Utilice subredes o VLAN para limitar el acceso al servidor

MOBOTIX recomienda agrupar lógicamente los diferentes tipos de hosts y usuarios en subredes separadas. Esto puede tener ventajas en la administración de privilegios para estos hosts y usuarios como miembros de un grupo con una función o rol determinado. Diseñe la red de modo que haya una subred o VLAN para cada función. Por ejemplo, una subred o VLAN para operadores de vigilancia y otra para administradores. Esto le permite definir reglas de firewall por grupo en lugar de por hosts individuales.

Aprende más

Los siguientes controles proporcionan instrucciones adicionales:

- NIST SP 800-53 AC-2 Administración de cuentas
- NIST SP 800-53 CSC 11: Configuraciones seguras para dispositivos de red como firewalls, enrutadores y conmutadores
- NIST SP 800-53 SC-7 Protección de límites

6.2.6 Habilitar solo los puertos usados por el servidor de eventos

MOBOTIX recomienda habilitar solo los puertos utilizados por el servidor de eventos y bloquear todos los demás puertos, incluidos los puertos predeterminados de Windows.
Los puertos de servidor de eventos utilizados en MOBOTIX HUB VMS son: 22331, 22333, 9090, 1234 y 1235.

Los puertos utilizados dependen de la implementación. En caso de duda, póngase en contacto con el servicio de asistencia de MOBOTIX.

Aprende más

Los siguientes controles proporcionan instrucciones adicionales:

- NIST SP 800-53 CSC 11: Configuraciones seguras para dispositivos de red como firewalls, enrutadores y conmutadores

6.3 Servidor SQL

6.3.1 Conexión al servidor SQL y a la base de datos

Se puede especificar cualquier cadena de conexión SQL, incluida una en la que se utilice la autenticación SQL (nombre de usuario/contraseña). Esto puede ser útil durante las pruebas porque no requiere acceso a un AD. Sin embargo, no se recomienda usar la autenticación de nombre de usuario y contraseña para las configuraciones de producción, ya que tanto el nombre de usuario como la contraseña se conservan sin cifrar en el equipo. Para las configuraciones de producción, recomendamos utilizar la seguridad integrada.

La comunicación entre el MOBOTIX MOBOTIX HUB VMS y el servidor SQL y la base de datos puede ser potencialmente manipulada por un atacante porque el certificado no está validado.
Para mitigar esto, primero debe configurar certificados de servidor verificables. Una vez configurados los certificados, debe modificar ConnestionString en el Registro de Windows quitando trustServerCertificate=true, como se indica a continuación:
Clave del Registro: Computer\HKEY_LOCAL_MACHINE\SOFTWARE\VideoOS\Server\Common\ConnectionString

- Actual
  cadena de conexión: Fuente de datos = localhost; catálogo inicial='Vigilancia'; Seguridad Integrada = SSPI; encrypt=true; trustServerCertificate=true
- Endurecido
  cadena de conexión: Fuente de datos = localhost; catálogo inicial='Vigilancia'; Seguridad Integrada = SSPI; encrypt=true

Esto da como resultado que el cifrado solo se produzca si hay un certificado de servidor verificable, de lo contrario, se produce un error en el intento de conexión.
Este problema se describe en detalle en el artículo Uso del cifrado sin validación.

6.3.2 Ejecute SQL Server y la base de datos en un servidor independiente

MOBOTIX recomienda hacer que el servidor SQL Server y la base de datos sean redundantes. Esto reduce el riesgo de tiempo de inactividad real o percibido.

Para admitir Windows Server Failover Clustering (WSFC), MOBOTIX recomienda ejecutar el servidor SQL Server y la base de datos en un servidor independiente, y no en el servidor de gestión.

SQL Server debe ejecutarse en la configuración de WSFC y los servidores de administración y eventos deben ejecutarse en una configuración de Microsoft Cluster (o tecnología similar). Para obtener más información acerca de WSFC, vea *Clústeres de conmutación por error de Windows Server (WSFC) con SQL Server* (https://msdn.microsoft.com/en-us/library/hh270278.aspx).

Aprende más

Los siguientes controles proporcionan instrucciones adicionales:

- NIST 800-53 SC-7 Protección de límites
- Plan de gestión de configuración NIST 800-53 CM-9

6.4 Servidor de administración

6.4.1 Ajustar el tiempo de espera del token

MOBOTIX HUB VMS utiliza tokens de sesión cuando inicia sesión en el servidor de gestión mediante los protocolos SSL (usuarios básicos) o NTLM (usuarios de Windows). Un token se recupera del servidor de gestión y se utiliza en los servidores secundarios, por ejemplo, el servidor de grabación y, a veces, también el servidor de eventos. Esto es para evitar que la búsqueda de NTLM y AD se realice en todos los componentes del servidor.

De forma predeterminada, un token es válido durante 240 minutos. Puede ajustar esto a intervalos de 1 minuto. Este valor también se puede ajustar con el tiempo. Los intervalos cortos aumentan la seguridad, sin embargo, el sistema genera comunicación adicional cuando renueva el token.

El mejor intervalo a utilizar depende de la implementación. Esta comunicación aumenta la carga del sistema y puede afectar al rendimiento.

Aprende más

Los siguientes controles proporcionan instrucciones adicionales:

- Administración de autenticadores NIST SP 800-53 IA-5

6.4.2 Habilitar solo los puertos utilizados por el servidor de administración

MOBOTIX recomienda habilitar solo los puertos utilizados por el servidor de gestión y bloquear todos los demás puertos, incluidos los puertos predeterminados de Windows. Esta guía es coherente para los componentes de servidor de MOBOTIX HUB VMS.

Los puertos del servidor de gestión utilizados en MOBOTIX HUB VMS son: 80, 443, 1433, 7475, 8080, 8990, 9993, 12345.

Los puertos utilizados dependen de la implementación. En caso de duda, póngase en contacto con el servicio de asistencia de MOBOTIX.

Aprende más

Los siguientes controles proporcionan instrucciones adicionales:

- NIST SP 800-53 AC-2 Administración de cuentas
- NIST SP 800-53 SC-7 Protección de límites

6.4.3 Deshabilitar protocolos no seguros

Cuando un usuario básico inicia sesión en el servidor de administración a través de IIS, el cliente de administración usará cualquier protocolo disponible. MOBOTIX recomienda implementar siempre la última versión de Transport Layer Security (TLS, actualmente 1.2) (https://datatracker.ietf.org/wg/tls/charter/) y desactivar todos los conjuntos de cifrado incorrectos y las versiones obsoletas de los protocolos SSL/TLS. Realice acciones para bloquear protocolos no seguros en el nivel del sistema operativo. Esto evita que el cliente de administración utilice protocolos que no sean seguros. El sistema operativo determina el protocolo que se va a utilizar.

Los protocolos utilizados dependen de la implementación. En caso de duda, póngase en contacto con el servicio de asistencia de MOBOTIX.

Aprende más

Los siguientes controles proporcionan instrucciones adicionales:

- Acceso remoto NIST 800-53 AC-17 (deshabilitar protocolos no utilizados)
- Ajustes de configuración de NIST 800-53 CM-6
- NIST 800-53 CM-7 Funcionalidad mínima

6.4.4 Deshabilitar el canal remoto heredado

La comunicación entre los servidores de grabación y el servidor de gestión se ha vuelto más segura con la solución implementada en 2019 R2. Si actualiza desde una versión anterior de MOBOTIX HUB VMS, el servidor de gestión seguirá iniciando la tecnología de terceros heredada para poder comunicarse con los servidores de grabación de versiones anteriores.

Cuando todos los servidores de grabación de su sistema se actualicen a la versión 2019 R2 o posterior, puede configurar el servidor de gestión para que no inicie el canal de comunicación remota heredado, para que su sistema sea menos vulnerable, MOBOTIX recomienda establecer **UseRemoting** en **Falso** en el archivo de configuración del servidor de gestión.

Aprende más

Los siguientes controles proporcionan instrucciones adicionales:

- Acceso remoto NIST 800-53 AC-17 (deshabilitar protocolos no utilizados)
- Ajustes de configuración de NIST 800-53 CM-6

6.4.5 Administrar la información de encabezado de IIS

Deshabilitar la información del encabezado de IIS

Por motivos de seguridad, MOBOTIX recomienda desactivar los encabezados X-Powered-By HTTP y X-AspNet-Version.

El encabezado HTTP X-Powered-By revela la versión de IIS que se usa en el servidor. Deshabilite este encabezado haciendo lo siguiente:

1. Abra el Administrador de IIS.
2. Seleccione el sitio web predeterminado.
3. Seleccione Encabezados de respuesta HTTP.
4. Seleccione el encabezado HTTP X-Powered-By y seleccione Eliminar.

El encabezado HTTP X-AspNet-Version revela la versión de ASP.NET que utiliza el grupo de aplicaciones del Servidor de administración. Deshabilite este encabezado haciendo lo siguiente:

1. Abra el archivo web.config ubicado en %windir%\Microsoft.NET\Framework\v4.0.30319\CONFIG.
2. Después de la etiqueta <system.web>, agregue lo siguiente: <httpRuntime enableVersionHeader="false" />
3. Guarde el archivo.

La variable de encabezado SERVER no debe eliminarse, ya que provocará que se interrumpa la funcionalidad del Servidor de administración.

Establecer opciones de X-Frame

Por motivos de seguridad, MOBOTIX recomienda configurar X-Frame-Options en **denegar**.

Cuando se establece el encabezado HTTP X-Frame-Options en deny, se deshabilita la carga de la página en un marco, independientemente del sitio que esté intentando obtener acceso.

Cambie este encabezado haciendo lo siguiente:

1. Abra el Administrador de IIS.
2. Seleccione el sitio web predeterminado > Instalación.
3. Seleccione Encabezados de respuesta HTTP.
4. Haga clic con el botón derecho y seleccione Agregar... desde el menú
5. En el campo Nombre, escriba X-Frame-Options y en el campo Valor, escriba deny.

6.4.6 Deshabilitar los verbos HTTP TRACE / TRACK de IIS

Por motivos de seguridad, MOBOTIX recomienda desactivar el verbo HTTP TRACE en la instalación de IIS.

Deshabilite el verbo HTTP TRACE haciendo lo siguiente:

1. Abra el administrador de IIS.
2. Seleccione el sitio web predeterminado.
3. Haga doble clic en Filtrado de solicitudes.

Si **el filtrado de solicitudes** no está disponible, instálelo siguiendo las instrucciones que se indican aquí: https://docs.microsoft.com/en-us/iis/configuration/system.webserver/security/requestfiltering/

4. Seleccione la pestaña Verbos HTTP.
5. Seleccione Denegar verbo en el menú Acciones.
6. Escriba TRACE y haga clic en Aceptar.
7. Seleccione Denegar verbo en el menú Acciones.

8. Escriba TRACK y haga clic en Aceptar.
9. Seleccione Denegar verbo en el menú Opciones.
10. Escriba OPCIONES y haga clic en Aceptar.

6.4.7 Deshabilitar la página predeterminada de IIS

Por motivos de seguridad, MOBOTIX recomienda desactivar la página predeterminada de IIS. Al hacerlo, se quita la información que se podría usar para detectar qué tecnologías se usan en la instalación y se alinea con los procedimientos recomendados de IIS definidos por Microsoft. Deshabilite la página predeterminada haciendo lo siguiente:

1. Abra el administrador de IIS.
2. Seleccione el sitio web predeterminado.
3. Haga doble clic en Documento predeterminado.
4. Seleccione Deshabilitar en el menú Acciones.

6.5 Proveedor de identidad

6.5.1 Deshabilitar la información de encabezado de IIS en el proveedor de identidades

Por motivos de seguridad, MOBOTIX AG recomienda desactivar la cabecera del servidor en la aplicación Identity Provider .

El encabezado del servidor describe el software utilizado por el servidor original que maneja una solicitud. Deshabilite este encabezado haciendo lo siguiente.

Esto solo es aplicable para IIS 10 y versiones posteriores.

1. Abra el Administrador de IIS.
2. En el sitio web predeterminado, seleccione **IDP**.
3. Abra el editor de **configuración**.
4. Seleccione la sección **system.webServer/security/requestFiltering**.
5. Establezca **removeServerHeader** en **True**.

6.6 Servidor de grabación

6.6.1 Propiedades de Configuración de almacenamiento y grabación

La funcionalidad disponible depende del sistema que esté utilizando. Consulte https://www.mobotix.com/en/vms/mobotix-hub/levels para obtener más información.

En el cuadro de diálogo **Configuración de almacenamiento y grabación**, especifique lo siguiente:

Nombre	Descripción
Nombre	Cambie el nombre del almacenamiento si es necesario. Los nombres deben ser únicos.
Camino	Especifique la ruta de acceso al directorio en el que guarda las grabaciones en este almacenamiento. El almacenamiento no tiene que estar necesariamente ubicado en el ordenador servidor de grabación.

Nombre	Descripción
	Si el directorio no existe, puede crearlo. Las unidades de red deben especificarse mediante el formato UNC (Convención de nomenclatura universal), por ejemplo: \\server\volume\directory\.
Tiempo de retención	Especifique durante cuánto tiempo deben permanecer las grabaciones en el archivo antes de que se eliminen o se muevan al siguiente archivo (en función de la configuración del archivo). El tiempo de retención siempre debe ser mayor que el tiempo de retención del archivo anterior o de la base de datos de grabación predeterminada. Esto se debe a que el número de días de retención especificados para un archivo incluye todos los períodos de retención indicados anteriormente en el proceso.
Tamaño máximo	Seleccione el número máximo de gigabytes de datos de grabación que se guardarán en la base de datos de grabación. Los datos de grabación que superan el número especificado de gigabytes se mueven automáticamente al primer archivo de la lista, si se especifica alguno, o se eliminan. Cuando hay menos de 5 GB de espacio libre, el sistema siempre archiva automáticamente (o elimina si no se ha definido un próximo archivo) los datos más antiguos de una base de datos. Si hay menos de 1 GB de espacio libre, se eliminan los datos. Una base de datos siempre requiere 250 MB de espacio libre. Si alcanza este límite (si los datos no se eliminan lo suficientemente rápido), no se escribirán más datos en la base de datos hasta que haya liberado suficiente espacio. El tamaño máximo real de la base de datos es la cantidad de gigabytes que especifique, menos 5 GB.
Fichaje	Habilita una firma digital a las grabaciones. Esto significa, por ejemplo, que el sistema confirma que el vídeo exportado no ha sido modificado ni manipulado cuando se reproduce. El sistema utiliza el algoritmo SHA-2 para la firma digital.
Encriptación	Seleccione el nivel de cifrado de las grabaciones: • Ninguno • Ligero (menos uso de CPU) • Fuerte (más uso de CPU) El sistema utiliza el algoritmo AES-256 para el cifrado. Si selecciona **Luz**, una parte de la grabación se cifra. Si selecciona Fuerte, toda la grabación está encriptada. Si elige habilitar el cifrado, también debe especificar una contraseña a continuación.
Contraseña	Introduzca una contraseña para los usuarios autorizados a ver los datos cifrados. MOBOTIX recomienda utilizar contraseñas seguras. Las contraseñas seguras no contienen palabras que se puedan encontrar en un diccionario o que formen parte del nombre del usuario. Incluyen ocho o más caracteres alfanuméricos, mayúsculas y minúsculas y caracteres especiales.

6.6.2 Utilice tarjetas de interfaz de red independientes

MOBOTIX recomienda utilizar varias tarjetas de interfaz de red (NIC) para separar la comunicación entre los servidores y dispositivos de grabación de la comunicación entre los servidores de grabación y los programas cliente. Los programas cliente no necesitan comunicarse directamente con los dispositivos.

Aprende más

Los siguientes controles proporcionan instrucciones adicionales:

- NIST SP 800-53 SC-7 Protección de límites

6.6.3 Fortalezca el almacenamiento conectado a la red (NAS) para almacenar datos multimedia grabados

El servidor de grabación puede utilizar el almacenamiento conectado a la red (NAS) para almacenar datos de medios grabados.

Si decide utilizar NAS, se puede reforzar mediante el uso de mejoras de seguridad de SMB 3.0, como se describe en este documento sobre mejoras de seguridad de SMB.

6.7 Componente de servidor móvil de MOBOTIX

6.7.1 Habilite solo los puertos que utiliza el servidor móvil de MOBOTIX

MOBOTIX recomienda habilitar solo los puertos que utiliza el servidor MOBOTIX HUB Mobile y bloquear todos los demás puertos, incluidos los puertos predeterminados de Windows.

De forma predeterminada, el servidor móvil utiliza los puertos 8081 y 8082.

Los puertos utilizados dependen de la implementación. En caso de duda, póngase en contacto con el servicio de asistencia de MOBOTIX.

Aprende más

Los siguientes controles proporcionan instrucciones adicionales:

- NIST SP 800-53 AC-2 Administración de cuentas
- NIST SP 800-53 SC-7 Protección de límites

6.7.2 Usar una "zona desmilitarizada" (DMZ) para proporcionar acceso externo

MOBOTIX recomienda instalar el servidor MOBOTIX HUB Mobile en una DMZ y en un ordenador con dos interfaces de red:

- Uno para la comunicación interna
- Uno para el acceso público a Internet

Esto permite a los usuarios de clientes móviles conectarse al servidor móvil de MOBOTIX con una dirección IP pública, sin comprometer la seguridad o la disponibilidad de la red VMS.

Aprende más

Los siguientes controles proporcionan instrucciones adicionales:

- NIST SP 800-53 SC-7 Protección de límites

6.7.3 Deshabilitar protocolos no seguros

MOBOTIX recomienda utilizar solo los protocolos necesarios y solo las versiones más recientes. Por ejemplo, implemente la versión más reciente de la seguridad de la capa de transporte (TLS, actualmente 1.2) y deshabilite todos los demás conjuntos de cifrado y las versiones obsoletas de los protocolos SSL/TLS. Esto requiere la configuración de Windows y otros componentes del sistema, y el uso adecuado de certificados y claves digitales.

La misma recomendación se da para el servidor de administración. Para obtener más información, consulte Deshabilitar protocolos no seguros en la página 61.

Aprende más

Los siguientes controles proporcionan instrucciones adicionales:

- Acceso remoto NIST 800-53 AC-17 (deshabilitar protocolos no utilizados)
- Ajustes de configuración de NIST 800-53 CM-6
- NIST 800-53 CM-7 Funcionalidad mínima

6.7.4 Configurar usuarios para la verificación en dos pasos por correo electrónico

La funcionalidad disponible depende del sistema que esté utilizando. Consulte https://www.mobotix.com/en/vms/mobotix-hub/levels para obtener más información.

Para imponer un paso de inicio de sesión adicional a los usuarios del cliente móvil MOBOTIX HUB o del cliente web MOBOTIX HUB, configure la verificación en dos pasos en el servidor móvil de MOBOTIX HUB. Además del nombre de usuario y la contraseña estándar, el usuario debe introducir un código de verificación recibido por correo electrónico.

La verificación en dos pasos aumenta el nivel de protección de su sistema de vigilancia.

Requisitos

- Ha instalado un servidor SMTP.
- Ha añadido usuarios y grupos a su sistema MOBOTIX HUB en el cliente de gestión, en el nodo Roles del panel de navegación del sitio. En el rol correspondiente, seleccione la pestaña Usuarios y grupos.
- Si ha actualizado su sistema desde una versión anterior de MOBOTIX HUB, debe reiniciar el servidor móvil para habilitar la función de verificación en dos pasos.

En el cliente de administración o la aplicación de administración, realice estos pasos:

1. Introduzca información sobre su servidor SMTP.
2. Especifique la configuración del código de verificación que se enviará a los usuarios del cliente.
3. Asigne el método de inicio de sesión a usuarios y grupos de dominio.

En este tema se describe cada uno de estos pasos.

Introduzca información sobre su servidor SMTP

El proveedor utiliza la información sobre el servidor SMTP:

1. En el panel de navegación, seleccione Servidores móviles y, a continuación, seleccione el servidor móvil correspondiente.
2. En la pestaña Verificación en dos pasos, active la casilla Habilitar verificación en dos pasos.
3. Debajo de Configuración del proveedor, en la pestaña Correo electrónico, introduzca información sobre el servidor SMTP y especifique el correo electrónico que el sistema enviará a los usuarios cliente cuando inicien sesión y estén configurados para un inicio de sesión secundario. Para obtener más información sobre cada parámetro, consulte la pestaña Verificación en dos pasos en la página 67.

Especifique el código de verificación que se enviará a los usuarios

Para especificar la complejidad del código de verificación:

1. En la pestaña Verificación en dos pasos, en la sección Configuración del código de verificación, especifique el período durante el cual los usuarios del cliente móvil MOBOTIX o del cliente web MOBOTIX HUB no tienen que volver a verificar su inicio de sesión en caso de, por ejemplo, una red desconectada. El período predeterminado es de 3 minutos.
2. Especifique el período dentro del cual el usuario puede usar el código de verificación recibido. Después de este período, el código no es válido y el usuario debe solicitar un nuevo código. El período predeterminado es de 5 minutos.
3. Especifique el número máximo de intentos de entrada de código, antes de que se bloquee al usuario. El número predeterminado es 3.
4. Especifique el número de caracteres del código. La longitud predeterminada es 6.
5. Especifique la complejidad del código que desea que componga el sistema.

Asignar método de inicio de sesión a usuarios y grupos de Active Directory

En la pestaña **Verificación en dos pasos**, en la sección **Configuración de usuario**, aparece la lista de usuarios y grupos añadidos a su sistema MOBOTIX HUB.

1. En la columna Método de inicio de sesión, seleccione entre sin inicio de sesión, sin verificación en dos pasos o método de entrega de códigos.
2. En el campo Detalles, agregue los detalles de entrega, como las direcciones de correo electrónico de usuarios individuales. La próxima vez que el usuario inicie sesión en el cliente web de MOBOTIX HUB o en el cliente móvil de MOBOTIX HUB, se le pedirá un inicio de sesión secundario.
3. Si un grupo está configurado en Active Directory, el servidor móvil utiliza detalles, como direcciones de correo electrónico, de Active Directory.
4. Los grupos de Windows no admiten la verificación en dos pasos.
5. Guarde la configuración.

Ha completado los pasos para configurar a sus usuarios para la verificación en dos pasos por correo electrónico.

Pestaña de verificación en dos pasos

La funcionalidad disponible depende del sistema que esté utilizando. Consulte https://www.mobotix.com/en/vms/mobotix-hub/levels para obtener más información.

Utilice la pestaña **Verificación en dos pasos** para habilitar y especificar un paso de inicio de sesión adicional en los usuarios de:

- Aplicación móvil MOBOTIX HUB en sus dispositivos móviles iOS o Android
- Cliente web MOBOTIX HUB

El primer tipo de verificación es una contraseña. El segundo tipo es un código de verificación, que puede configurar para que se envíe al usuario por correo electrónico.

Para obtener más información, consulte Configurar usuarios para la verificación en dos pasos por correo electrónico En la página 66.

En las tablas siguientes se describe la configuración de esta pestaña.

Configuración del proveedor > correo electrónico

Nombre	Descripción
Servidor SMTP	Introduzca la dirección IP o el nombre de host del servidor del protocolo simple de transferencia de correo (SMTP) para los correos electrónicos de verificación en dos pasos.
Puerto de servidor SMTP	Especifique el puerto del servidor SMTP para enviar correos electrónicos. El número de puerto predeterminado es 25 sin SSL y 465 con SSL.
Usar SSL	Active esta casilla de verificación si su servidor SMTP admite el cifrado SSL.
Nombre de usuario	Especifique el nombre de usuario para iniciar sesión en el servidor SMTP.
Contraseña	Especifique la contraseña para iniciar sesión en el servidor SMTP.
Usar autenticación de contraseña segura (SPA)	Active esta casilla de verificación si el servidor SMTP es compatible con SPA.
Dirección de correo electrónico del remitente	Especifique la dirección de correo electrónico para enviar códigos de verificación.
Asunto del correo electrónico	Especifique el título del asunto del correo electrónico. Ejemplo: Tu código de verificación en dos pasos.
Texto del correo electrónico	Introduzca el mensaje que desea enviar. Ejemplo: Su código es {0}. Si olvida incluir la variable {0}, el código se agrega al final del texto de forma predeterminada.

Configuración del código de verificación

Nombre	Descripción
Tiempo de espera de reconexión (0-30 minutos)	Especifique el período durante el cual los usuarios del cliente móvil de MOBOTIX HUB no tienen que volver a verificar su inicio de sesión en caso de, por ejemplo, una red desconectada. El período predeterminado es de tres minutos. Esta configuración no se aplica a MOBOTIX HUB Web Client.
El código caduca después de (1-10 minutos)	Especifique el período dentro del cual el usuario puede usar el código de verificación recibido. Después de este período, el código no es válido y el usuario debe solicitar un nuevo código. El período predeterminado es de cinco minutos.
Intentos de introducción de código (1-10 intentos)	Especifique el número máximo de intentos de entrada de código antes de que el código proporcionado deje de ser válido. El número predeterminado es tres.
Longitud del código (4-6 caracteres)	Especifique el número de caracteres del código. La longitud predeterminada es seis.
Composición del código	Especifique la complejidad del código que desea que genere el sistema. Puede seleccionar entre: Mayúsculas latinas (A-Z) Minúsculas latinas (a-z) Dígitos (0-9) Caracteres especiales (!@#...)

Configuración de usuario

Nombre	Descripción
Usuarios y grupos	Enumera los usuarios y grupos añadidos al sistema MOBOTIX HUB. Si un grupo está configurado en Active Directory, el servidor móvil utiliza detalles, como direcciones de correo electrónico, de Active Directory. Los grupos de Windows no admiten la verificación en dos pasos.
Método de verificación	Seleccione una configuración de verificación para cada usuario o grupo. Puede seleccionar entre: Sin inicio de sesión: el usuario no puede iniciar sesión No hay verificación en dos pasos: el usuario debe ingresar el nombre de usuario y la contraseña Correo electrónico: el usuario debe ingresar un código de verificación además del nombre de usuario y la contraseña
Datos del usuario	Introduzca la dirección de correo electrónico a la que cada usuario recibirá los códigos.

6.7.5 Configurar la política de seguridad de contenido (CSP)

Los WebSockets con caracteres comodín deben quitarse de los encabezados CSP en el servidor móvil. Actualmente, el ws://*:* y el wss://*:* no se pueden eliminar del CSP descrito en Configuración del servidor móvil debido a las limitaciones del navegador Safari.

Para aumentar la seguridad en su servidor móvil, haga lo siguiente:

1. Abra el archivo VideoOS.MobileServer.Service.exe.config, que se encuentra en la carpeta de instalación del servidor móvil.
2. Modifique la sección <HttpHeaders>, donde el valor de key="Content-Security-Policy" de la siguiente manera:
   - Si no es necesario ser compatible con el navegador Safari, elimine ws://*:* y wss://*:* del encabezado.
   - Si se requiere compatibilidad con el navegador Safari, reemplace ws://*:* y wss://*:* con los valores 'ws:// [hostname]:[port] y wss://[hostname]:[port]', donde hostname y port son los relevantes utilizados para acceder al servidor móvil.
3. Reinicie el servidor móvil.

6.8 Servidor de registro

6.8.1 Instalación del servidor de registros en un servidor independiente con SQL Server

En el caso de sistemas muy grandes con muchas transacciones hacia y desde la base de datos SQL del servidor de registros, MOBOTIX recomienda instalar el componente Log Server en un servidor independiente con su propio SQL Server y almacenar los registros en una base de datos SQL en ese SQL Server local. Si el servidor de registro se ve afectado por problemas de rendimiento, por ejemplo, debido a inundaciones u otros motivos, y utiliza el mismo SQL Server que el servidor de administración, ambos servicios pueden verse afectados.

Aprende más

Los siguientes controles proporcionan instrucciones adicionales:

- NIST SP 800-53 SC-7 Protección de límites

- Plan de gestión de configuración NIST SP 800-53 CM-9

6.8.2 Limitar el acceso IP al servidor de registro

MOBOTIX recomienda que solo los componentes del VMS puedan ponerse en contacto con el servidor de registros. El servidor de registros utiliza el puerto 22337.

Aprende más

Los siguientes controles proporcionan instrucciones adicionales:

- Ajustes de configuración de NIST 800-53 CM-6
- NIST 800-53 CM-7 Funcionalidad mínima

7 Programas de cliente

En esta sección se proporcionan instrucciones sobre cómo proteger los programas cliente de MOBOTIX.

Los programas cliente son:

- Cliente inteligente MOBOTIX HUB
- Cliente web MOBOTIX HUB
- Cliente de gestión de MOBOTIX HUB
- Cliente móvil de MOBOTIX

7.1 Pasos básicos (todos los programas cliente)

7.1.1 Usar usuarios de Windows con AD

MOBOTIX recomienda que, siempre que sea posible, utilice usuarios de Windows en combinación con Active Directory (AD) para iniciar sesión en el VMS con los programas cliente. Esto le permite aplicar una política de contraseñas y aplicar la configuración de usuario de forma coherente en todo el dominio y la red. También proporciona protección contra ataques de fuerza bruta. Para obtener más información, consulte Usar usuarios de Windows con Active Directory.

Aprende más

Los siguientes controles proporcionan instrucciones adicionales:

- Ajustes de configuración de NIST 800-53 CM-6
- Documentación del sistema de información NIST 800-53 SA-5
- NIST 800-53 SA-13 Confiabilidad

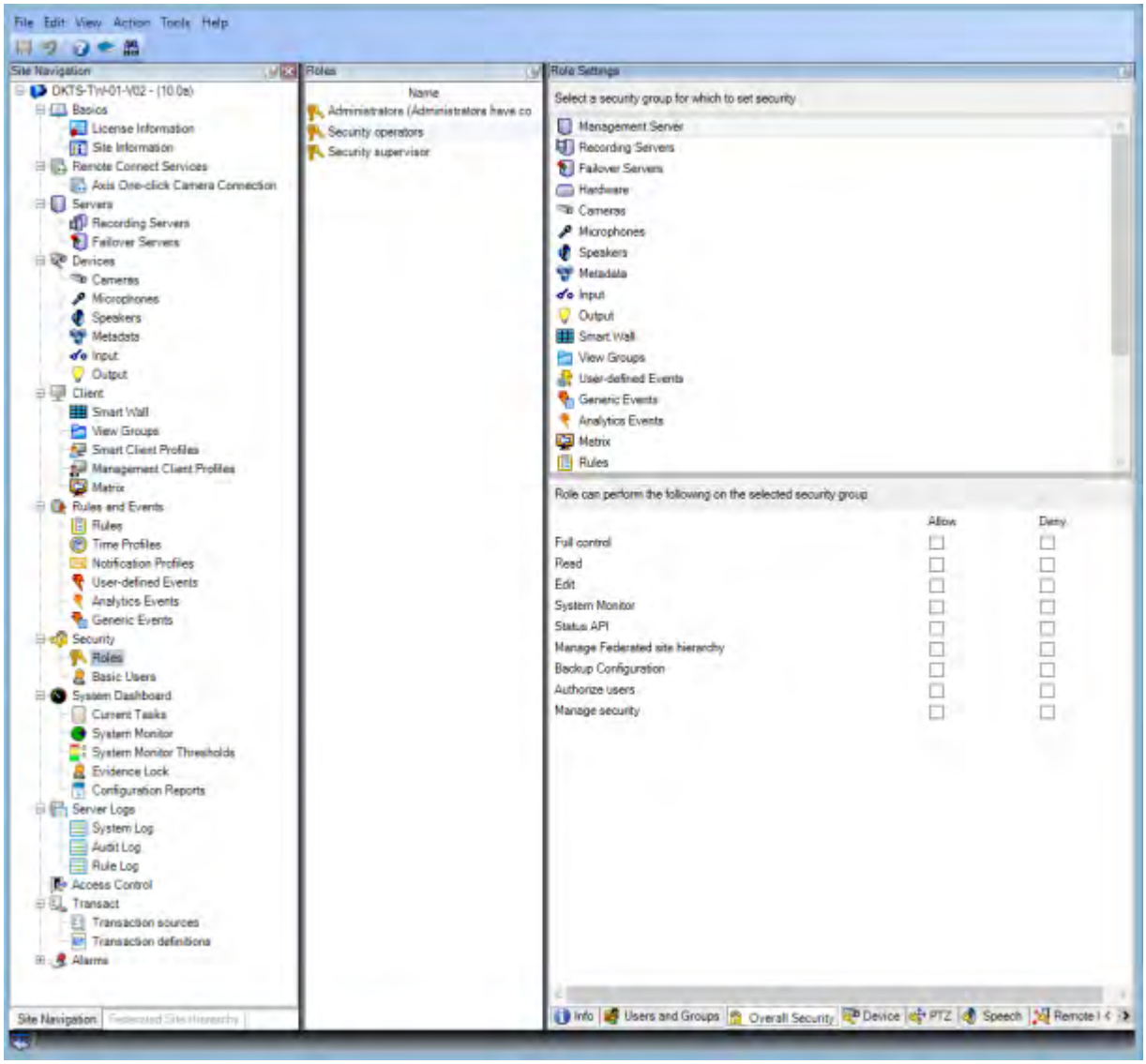
7.1.2 Restringir los permisos de los usuarios cliente

MOBOTIX recomienda a los administradores que especifiquen lo que los usuarios pueden hacer en Management Client o MOBOTIX HUB Smart Client.

Las siguientes instrucciones describen cómo hacerlo.

Para restringir los permisos de usuario del cliente, siga estos pasos:

1. Abra el cliente de administración.
2. Expanda el nodo Seguridad, seleccione Roles y, a continuación, seleccione el rol al que está asociado el usuario.
3. En las pestañas de la parte inferior, puede establecer permisos y restricciones para el rol.



De forma predeterminada, todos los usuarios asociados con el rol de administrador tienen acceso sin restricciones al sistema. Esto incluye a los usuarios que están asociados con el rol de administrador en AD, así como a aquellos con el rol de administrador en el servidor de administración.

Aprende más

Los siguientes documentos proporcionan información adicional:

- NIST 800-53 AC-4 Privilegio mínimo
- Ajustes de configuración de NIST 800-53 CM-6
- NIST 800-53 CM-7 Funcionalidad mínima

7.1.3 Ejecute siempre clientes en hardware de confianza en redes de confianza

MOBOTIX recomienda ejecutar siempre clientes MOBOTIX HUB en dispositivos de hardware con la configuración de seguridad adecuada. La guía específica para dispositivos móviles está disponible en SP 800-124 (https://csrc.nist.gov/publications/detail/sp/800-124/rev-1/final). Estos ajustes son específicos del dispositivo.

Aprende más

Los siguientes controles proporcionan instrucciones adicionales:

- NIST SP 800-53 SC-7 Protección de límites
- Ajustes de configuración de NIST SP800-53 CM-6

7.2 Pasos avanzados: MOBOTIX HUB Smart Client

7.2.1 Restrinja el acceso físico a cualquier ordenador que ejecute MOBOTIX HUB Smart Client

MOBOTIX recomienda restringir el acceso físico a los ordenadores que ejecuten MOBOTIX HUB Smart Client. Permitir que solo el personal autorizado acceda a las computadoras. Por ejemplo, mantenga la puerta cerrada con llave y utilice los controles de acceso y la vigilancia.

Aprende más

Los siguientes controles proporcionan instrucciones adicionales:

- NIST SP 800-53 PE-1 Política y Procedimientos de Protección Física y Ambiental
- Autorizaciones de acceso físico NIST SP 800-53 PE-2
- NIST SP 800-53 PE-3 Control de acceso físico
- NIST SP 800-53 PE-6 Monitoreo de acceso físico

7.2.2 Utilice siempre una conexión segura de forma predeterminada, especialmente a través de redes públicas

Si necesita acceder al VMS con MOBOTIX HUB Smart Client a través de una red pública o que no sea de confianza, MOBOTIX recomienda utilizar una conexión segura a través de VPN. Esto ayuda a garantizar la protección de la comunicación entre MOBOTIX HUB Smart Client y el servidor VMS.

Aprende más

Los siguientes controles proporcionan instrucciones adicionales:

- NIST SP 800-53 AC-2 Administración de cuentas
- Acceso remoto NIST SP 800-53 AC-17
- Ajustes de configuración de NIST SP 800-53 CM-6

7.2.3 Activar la autorización de inicio de sesión

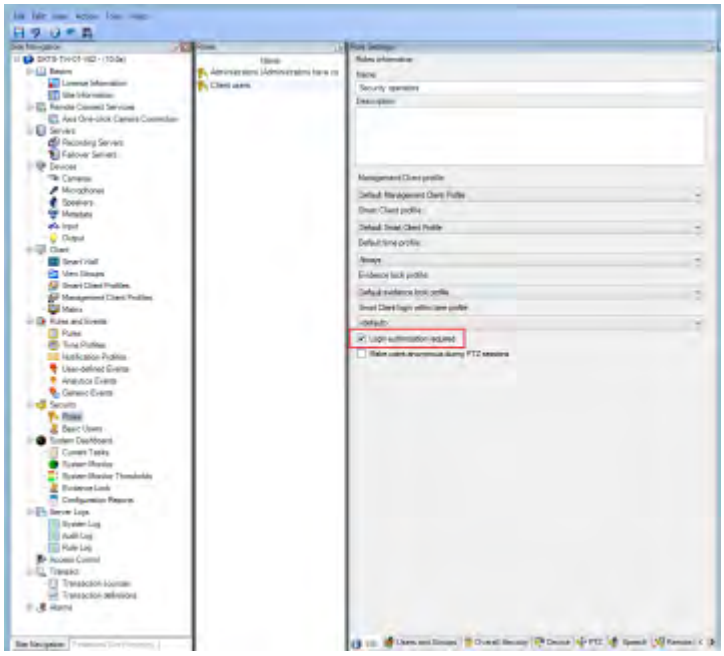
La autorización de inicio de sesión requiere que un usuario inicie sesión en MOBOTIX HUB Smart Client o Management Client, y que otro usuario que tenga un estado elevado, como un supervisor, proporcione su aprobación.

Configure la autorización de inicio de sesión en los roles. A los usuarios asociados con el rol se les solicita que un segundo usuario (un supervisor) autorice su acceso al sistema.

Actualmente, la autorización de inicio de sesión no es compatible con el cliente móvil, el cliente web MOBOTIX HUB ni con ninguna integración del SDK de MOBOTIX Integration Platform (MIP).

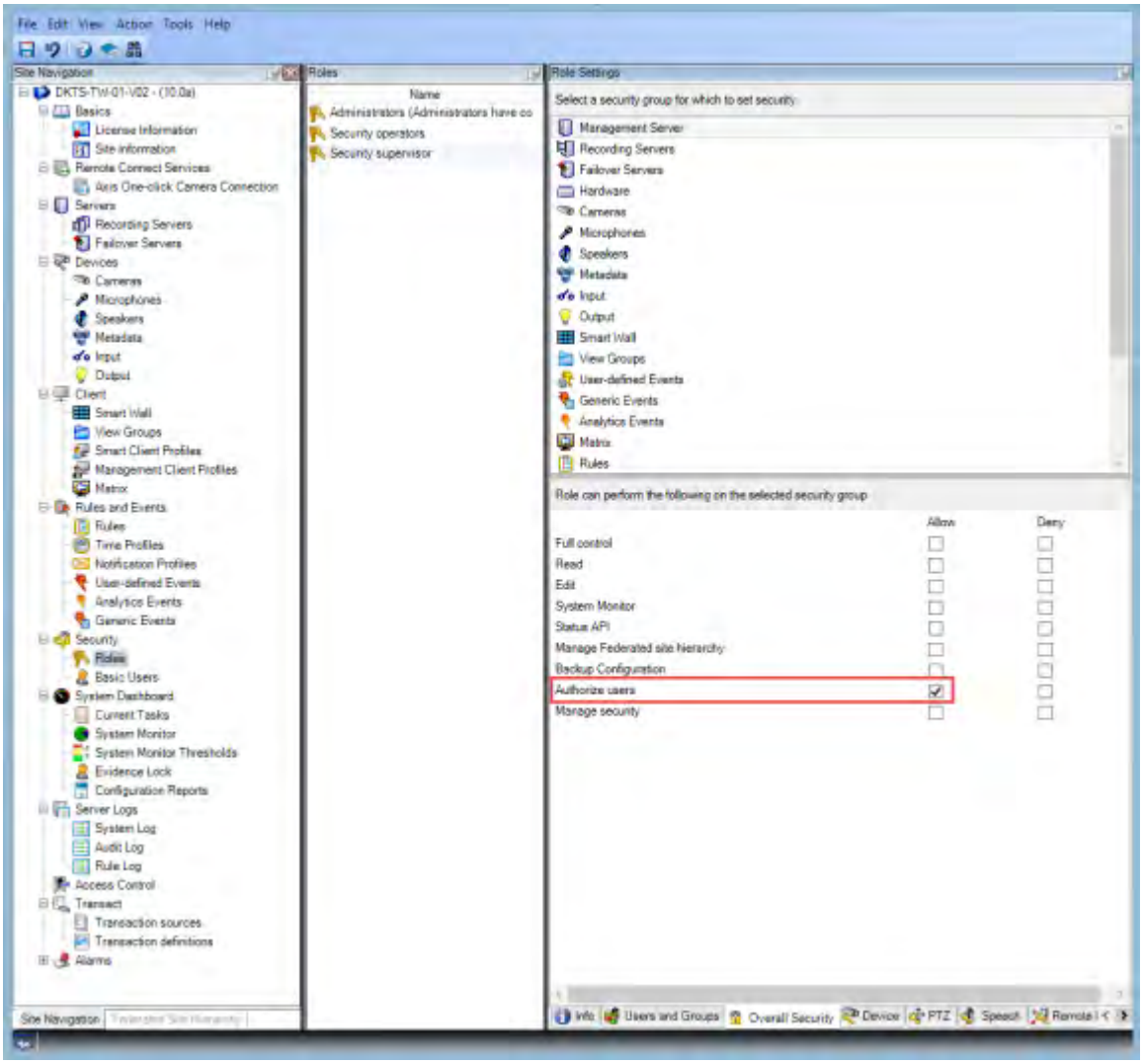
Para activar la autorización de inicio de sesión para un rol, siga estos pasos:

1. Abra el cliente de administración.
2. Expanda el nodo Seguridad, seleccione Roles y, a continuación, seleccione el rol correspondiente.
   Active la casilla **de verificación Autorización de inicio de sesión requerida**.



Para configurar los roles que autorizan y conceden acceso, siga estos pasos:

1. Para crear un nuevo rol, por ejemplo, "Supervisor de seguridad", expanda el nodo Seguridad, haga clic con el botón derecho en Roles y cree un nuevo rol.
2. Haga clic en la pestaña Seguridad general y seleccione el nodo Servidor de administración.
   Active la casilla **de verificación Permitir** junto a la casilla de verificación **Autorizar usuarios**.



Aprende más

Los siguientes controles proporcionan instrucciones adicionales:

- NIST SP 800-53 AC-2 Administración de cuentas
- NIST SP 800-53 AC-6 Privilegio mínimo
- Acceso remoto NIST SP 800-53 AC-17
- Ajustes de configuración de NIST SP 800-53 CM-6

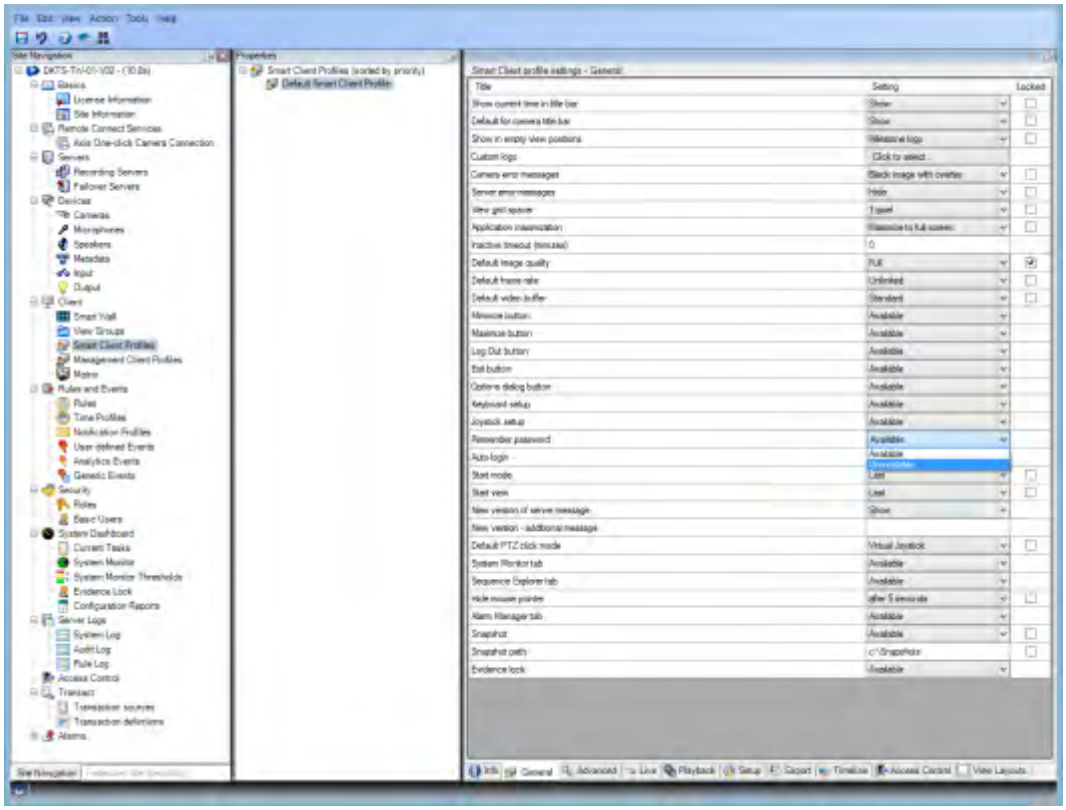
7.2.4 No guardes contraseñas

MOBOTIX HUB Smart Client ofrece la opción de recordar las contraseñas de los usuarios. Para reducir el riesgo de acceso no autorizado, MOBOTIX recomienda no utilizar esta función.

Para desactivar la función Recordar contraseña, siga estos pasos:

1. Abra el cliente de administración.
2. Expanda el nodo Cliente, seleccione Perfiles de cliente inteligente y, a continuación, seleccione el perfil de cliente inteligente correspondiente.
3. En la lista Recordar contraseña, seleccione No disponible.

La opción **Recordar contraseña** no estará disponible la próxima vez que un usuario con este perfil inicie sesión en MOBOTIX HUB Smart Client.



Aprende más

Los siguientes controles proporcionan instrucciones adicionales:

- NIST SP 800-53 AC-2 Administración de cuentas
- Ajustes de configuración de NIST SP 800-53 CM-6
- Política y procedimientos de identificación y autenticación NIST SP 800-53 IA-1

7.2.5 Activar solo las características de cliente necesarias

Active solo las funciones necesarias y desactive las funciones que un operador de vigilancia no necesite. El punto es limitar las oportunidades de mal uso o errores.

Puede activar y desactivar funciones en MOBOTIX HUB Smart Client y en MOBOTIX HUB Management Client.

En Management Client, configure los perfiles de Smart Client para especificar conjuntos de permisos para los usuarios asignados al perfil. Los perfiles de Smart Client son como los perfiles de Management Client, y se puede asignar el mismo usuario a cada tipo de perfil.

Para configurar un perfil de Smart Client, siga estos pasos:

1. Abra el cliente de administración.
2. Expanda el nodo Cliente, seleccione Perfiles de cliente inteligente y, a continuación, seleccione el perfil de cliente inteligente correspondiente.
3. Utilice las pestañas para especificar la configuración de las funciones en Smart Client. Por ejemplo, utilice la configuración de la pestaña Reproducción para controlar las funciones utilizadas para investigar el vídeo grabado.

Antes de asignar un usuario a un perfil de Smart Client, asegúrese de que los permisos para el rol del usuario sean adecuados para el perfil. Por ejemplo, si desea que un usuario pueda investigar vídeo, asegúrese de que el rol permita al usuario reproducir vídeo de las cámaras y de que la pestaña Explorador de secuencias esté disponible en el perfil de Smart Client.

Aprende más

Los siguientes controles proporcionan instrucciones adicionales:

- NIST SP 800-53 AC-2 Administración de cuentas
- NIST SP 800-53 AC-6 Privilegio mínimo
- Ajustes de configuración de NIST SP 800-53 CM-6

7.2.6 Usar nombres separados para las cuentas de usuario

MOBOTIX recomienda crear una cuenta de usuario para cada usuario y utilizar una convención de nomenclatura que facilite la identificación personal del usuario, como su nombre o sus iniciales. Esta es una práctica recomendada para limitar el acceso solo a lo que es necesario y también reduce la confusión al auditar.

Aprende más

Los siguientes controles proporcionan instrucciones adicionales:

- NIST 800-53 AC-4 Privilegio mínimo
- Política y procedimientos de administración de configuración NIST 800-53 CM-1
- Configuración de línea base NIST 800-53 CM-2
- Ajustes de configuración de NIST 800-53 CM-6
- NIST 800-53 CM-7 Funcionalidad mínima

7.2.7 Prohibir el uso de medios extraíbles

En el caso de las exportaciones de vídeo, establezca una cadena de procedimientos que sean específicos de las pruebas. MOBOTIX recomienda que la política de seguridad permita que solo los operadores autorizados de MOBOTIX HUB Smart Client conecten dispositivos de almacenamiento extraíbles, como unidades flash USB, tarjetas SD y smartphones, al ordenador en el que está instalado MOBOTIX HUB Smart Client.
Los medios extraíbles pueden transferir malware a la red y someter el vídeo a una distribución no autorizada. Como alternativa, la política de seguridad puede especificar que los usuarios solo puedan exportar pruebas a una ubicación específica de la red o solo a una grabadora de medios. Puede controlar esto a través del perfil de Smart Client.

Aprende más

Los siguientes controles proporcionan instrucciones adicionales:

- Uso de medios NIST SO 800-53 MP-7
- NIST SP 800-53 SI-3 Protección contra código malicioso

7.3 Pasos avanzados – Cliente móvil de MOBOTIX

SP 800-124 revisión 1 (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf) proporciona instrucciones específicas para dispositivos móviles. La información que contiene se aplica a todos los temas de esta sección.

7.3.1 Utilice siempre el cliente móvil de MOBOTIX en dispositivos seguros

MOBOTIX recomienda utilizar siempre el cliente MOBOTIX HUB Mobile en dispositivos seguros que estén configurados y mantenidos de acuerdo con una política de seguridad. Por ejemplo, asegúrese de que los dispositivos móviles no permitan a los usuarios instalar software de fuentes no autorizadas. Una tienda de aplicaciones empresariales es un ejemplo de una forma de restringir las aplicaciones de dispositivos como parte de la administración general de dispositivos móviles.

Aprende más

Los siguientes controles proporcionan instrucciones adicionales:

- NIST SP 800-53 SC-7 Protección de límites
- Ajustes de configuración de NIST SP800-53 CM-6

7.3.2 Descargue el cliente móvil de MOBOTIX de fuentes autorizadas

MOBOTIX recomienda descargar el cliente MOBOTIX HUB Mobile desde una de estas fuentes:

- Tienda de Google Play
- Tienda de aplicaciones de Apple
- Tienda Microsoft Windows.

Aprende más

Los siguientes controles proporcionan instrucciones adicionales:

- NIST SP 800-53 SC-7 Protección de límites
- Ajustes de configuración de NIST SP 800-53 CM-6

7.3.3 Los dispositivos móviles deben estar protegidos

Si desea acceder al VMS con un dispositivo móvil a través de una red pública o que no sea de confianza, MOBOTIX recomienda que lo haga con una conexión segura, utilice la autenticación adecuada y la seguridad de la capa de transporte (TLS) (https://datatracker.ietf.org/wg/tls/charter/) (o se conecte a través de VPN (https://datatracker.ietf.org/wg/ipsec/documents/)) y HTTPS. Esto ayuda a proteger las comunicaciones entre el dispositivo móvil y el VMS.

MOBOTIX recomienda que los dispositivos móviles utilicen el bloqueo de pantalla. Esto ayuda a evitar el acceso no autorizado al VMS, por ejemplo, si se pierde el teléfono inteligente. Para obtener la máxima seguridad, implemente una política de seguridad que prohíba que el cliente móvil de MOBOTIX HUB recuerde el nombre de usuario y la contraseña.

Aprende más

Los siguientes controles proporcionan instrucciones adicionales:

- NIST SP 800-53 AC-2 Administración de cuentas
- Acceso remoto NIST SP 800-53 AC-17
- Ajustes de configuración de NIST SP 800-53 CM-6

7.4 Pasos avanzados: cliente web MOBOTIX HUB

7.4.1 Ejecute siempre MOBOTIX HUB Web Client en equipos cliente de confianza

Conecte siempre de forma segura todos los componentes del VMS. Las conexiones de servidor a servidor y de cliente a servidor deben utilizar la autenticación adecuada y la seguridad de la capa de transporte (TLS) (https://datatracker.ietf.org/wg/tls/charter/) (o conectarse a través de VPN (https://datatracker.ietf.org/wg/ipsec/documents/)) y HTTPS. Ejecute siempre MOBOTIX HUB Web Client en ordenadores de confianza, por ejemplo, no utilice un ordenador cliente en un espacio público. MOBOTIX recomienda que eduque a los usuarios sobre las medidas de seguridad que deben recordar al utilizar aplicaciones basadas en navegador, como MOBOTIX HUB Web Client. Por ejemplo, asegúrese de que sepan que no deben permitir que el navegador recuerde su contraseña.

Aprende más

Los siguientes controles proporcionan instrucciones adicionales:

- NIST SP 800-53 AC-2 Administración de cuentas
- Ajustes de configuración de NIST SP 800-53 CM-6
- NIST SP 800-53 IA-2 Identificación y autenticación

7.4.2 Utilice certificados para confirmar la identidad de un servidor móvil de MOBOTIX

Este documento hace hincapié en el uso de la versión más reciente de TLS. Con eso viene la necesidad del uso adecuado de los certificados y la implementación del conjunto de cifrado TLS. MOBOTIX recomienda instalar un certificado en el servidor móvil de MOBOTIX HUB para confirmar la identidad del servidor cuando un usuario intente conectarse a través de MOBOTIX HUB Web Client.

Para obtener más información, consulte la *sección Editar certificado* en el manual del administrador de *MOBOTIX HUB VMS*.

Aprende más

Los siguientes controles proporcionan instrucciones adicionales:

- NIST SP 800-53 AC-2 Administración de cuentas
- Ajustes de configuración de NIST SP 800-53 CM-6
- NIST SP 800-53 IA-2 Identificación y autenticación

7.4.3 Utilice solo navegadores compatibles con las últimas actualizaciones de seguridad

MOBOTIX recomienda instalar solo uno de los siguientes navegadores en los equipos cliente. Asegúrese de incluir las últimas actualizaciones de seguridad.

- Apple Safari
- Google Chrome
- Microsoft Edge
- Mozilla Firefox

Aprende más

Los siguientes controles proporcionan instrucciones adicionales:

- Política y procedimientos de administración de configuración de NIST SP 800-53 CM-1
- Configuración de línea base NIST SP 800-53 CM-2
- Ajustes de configuración de NIST SP 800-53 CM-6

- Arquitectura de seguridad de la información NIST SP 800-53 PL-8
- NIST SP 800-53 SI-3 Protección contra código malicioso

7.5 Pasos avanzados: cliente de administración

7.5.1 Utilice los perfiles de cliente de administración para limitar lo que los administradores pueden ver

MOBOTIX recomienda utilizar los perfiles de Management Client para limitar lo que los administradores pueden ver en Management Client.

Los perfiles de cliente de administración permiten a los administradores del sistema modificar la interfaz de usuario del cliente de administración. Asocie los perfiles de cliente de administración con roles para limitar la interfaz de usuario y representar la funcionalidad disponible para cada rol de administrador.

Muestre solo las partes del VMS que los administradores necesitan para realizar sus funciones.

Aprende más

Los siguientes controles proporcionan instrucciones adicionales:

- NIST 800-53 AC-4 Privilegio mínimo
- Política y procedimientos de administración de configuración NIST 800-53 CM-1
- Configuración de línea base NIST 800-53 CM-2
- Ajustes de configuración de NIST 800-53 CM-6
- NIST 800-53 CM-7 Funcionalidad mínima

7.5.2 Permitir que los administradores accedan a partes relevantes del VMS

Si tiene una configuración que requiere varios administradores, MOBOTIX recomienda configurar diferentes derechos de administrador para los administradores que utilizan el cliente de gestión.

Para definir los permisos de administrador, siga estos pasos:

1. En Cliente de administración, expanda el nodo Seguridad, seleccione Roles y, a continuación, seleccione el rol de administrador correspondiente.
   No puede modificar el rol de administrador incorporado, por lo que debe crear roles de administrador adicionales.
2. En la pestaña Seguridad general, especifique las acciones que el administrador puede realizar para cada grupo de seguridad.
3. En las otras pestañas, especifique la configuración de seguridad para el rol en el VMS.
   Para obtener más información, consulte el manual del administrador de MOBOTIX HUB VMS.
4. En la pestaña Información, asocie el rol con un perfil de cliente de administración.

Puede activar o desactivar características mediante el perfil de cliente de administración. Antes de asignar un usuario a un perfil de cliente de administración, asegúrese de que los permisos para el rol del usuario sean adecuados para el perfil. Por ejemplo, si desea que un usuario pueda administrar cámaras, asegúrese de que el rol permita al usuario hacerlo y de que las cámaras estén habilitadas en el perfil del cliente de administración.

Aprende más

- Los siguientes controles proporcionan instrucciones adicionales:
- NIST 800-53 AC-4 Privilegio mínimo
- Política y procedimientos de administración de configuración NIST 800-53 CM-1
- Configuración de línea base NIST 800-53 CM-2
- Ajustes de configuración de NIST 800-53 CM-6
- NIST 800-53 CM-7 Funcionalidad mínima

7.5.3 Ejecute el cliente de administración en redes seguras y de confianza

Si accede al Servidor de administración con el Cliente de administración a través de HTTP, la comunicación de texto sin formato puede contener detalles del sistema sin cifrar. MOBOTIX recomienda ejecutar el cliente de gestión solo en redes conocidas y de confianza. Utilice una VPN para proporcionar acceso remoto.

Aprende más

Los siguientes controles proporcionan instrucciones adicionales:

- NIST SP 800-53 AC-2 Administración de cuentas
- Ajustes de configuración de NIST SP 800-53 CM-6
- NIST SP 800-53 IA-2 Identificación y autenticación

8 Conformidad

8.1 Cumplimiento de FIPS 140-2

En esta sección se explica FIPS 140-2 y cómo configurar y utilizar MOBOTIX HUB VMS para que funcione en modo compatible con FIPS 140-2.

Los términos "Compatible con FIPS 140-2" y "Modo compatible con FIPS 140-2" no son legalmente vinculantes. Los términos se utilizan aquí para mayor claridad.

Cumplir con FIPS 140-2 significa que el software utiliza instancias validadas por FIPS 140-2 de algoritmos y funciones hash en todas las instancias en las que se importan o exportan datos cifrados o hash desde el software. Además, esto significa que el software administrará las claves de manera segura, como se requiere de los módulos criptográficos validados por FIPS 140-2. El proceso de administración de claves también incluye la generación y el almacenamiento de claves.

El modo compatible con FIPS 140-2 se refiere al software que contiene métodos de seguridad aprobados por FIPS y no aprobados por FIPS, donde el software tiene al menos un "modo de operación FIPS". Este modo de operación solo permite el funcionamiento de métodos de seguridad aprobados por FIPS. Esto significa que cuando el software está en el "modo FIPS", no se utiliza un método no aprobado por FIPS en lugar del método aprobado por FIPS.

Se discuten los siguientes temas.

8.1.1 ¿Qué es FIPS?

Los Estándares Federales de Procesamiento de Información (FIPS) son una familia de estándares desarrollados por los siguientes dos organismos gubernamentales:

- El Instituto Nacional de Estándares y Tecnología (NIST) de los Estados Unidos
- El Establecimiento de Seguridad de las Comunicaciones (CSE) en Canadá

Estas normas tienen como objetivo garantizar la seguridad informática y la interoperabilidad.

Todas las soluciones de software implementadas en el gobierno y las industrias altamente reguladas en los Estados Unidos y Canadá deben cumplir con FIPS 140-2.

8.1.2 ¿Qué es FIPS 140-2?

FIPS 140-2, titulado "Requisitos de seguridad para módulos criptográficos", especifica qué algoritmos de cifrado y qué algoritmos de hash se pueden usar y cómo se deben generar y administrar las claves de cifrado.
Los requisitos de seguridad especificados en esta norma están destinados a mantener la seguridad proporcionada por un módulo criptográfico, pero la conformidad con esta norma no es suficiente para garantizar que un módulo en particular sea seguro. El operador de un módulo criptográfico es responsable de garantizar que la seguridad proporcionada por el módulo sea suficiente y aceptable para el propietario de la información que se está protegiendo, y que se reconozca y acepte cualquier riesgo residual.

8.1.3 ¿Qué aplicaciones MOBOTIX HUB VMS pueden funcionar en un modo compatible con FIPS 140-2?

A partir de MOBOTIX HUB VMS 2020 R3, todos los algoritmos de cifrado se han sustituido por la criptografía de nueva generación (CNG) de Microsoft, que se adhiere a las últimas tecnologías de seguridad disponibles y cumple con FIPS. Es decir, todas las aplicaciones MOBOTIX HUB VMS 2020 R3 pueden funcionar en modo compatible con FIPS.
En aras de la compatibilidad con versiones anteriores, algunos algoritmos y procesos no conformes persisten en MOBOTIX HUB VMS, incluso después de la versión 2020 R3, pero esto no afecta a la capacidad de operar el sistema en modo compatible con FIPS.

¿MOBOTIX HUB VMS siempre cumple con FIPS?

No. Algunos algoritmos y procesos no conformes persisten en MOBOTIX HUB VMS. Sin embargo, MOBOTIX HUB VMS puede configurarse y funcionar de forma que solo utilice las instancias de algoritmo certificadas por FIPS 140-2 y, por lo tanto, funcione en un modo compatible con FIPS.

¿Debería habilitar el modo FIPS 140-2?

Antes de habilitar el modo FIPS 140-2, es necesario comprender si lo necesita o no. Por ejemplo, si está trabajando y conectado a una red e infraestructura del gobierno de EE. UU. o Canadá, entonces es obligatorio cumplir con FIPS 140-2 y habilitarlo en su computadora para la comunicación según el estándar. Además, habilitar el modo FIPS 140-2 en su sistema operativo Windows restringe la ejecución de muchos programas y servicios, ya que solo se admitirán algoritmos y servicios aprobados por FIPS después de eso. Por lo tanto, se recomienda verificar si es necesario o no.

8.1.4 ¿Cómo garantizar que MOBOTIX HUB VMS pueda funcionar en modo compatible con FIPS 140-2?

Para utilizar MOBOTIX HUB VMS en un modo de funcionamiento FIPS 140-2, debe:

- Asegúrese de que las integraciones de terceros puedan funcionar en un sistema operativo Windows habilitado para FIPS (consulte Verificación de integraciones de terceros en la página 85)
- Conéctese a los dispositivos de una manera que garantice un modo de funcionamiento compatible con FIPS 140-2 (consulte Conectar dispositivos: antecedentes en la página 85)
- Asegúrese de que los datos de la base de datos multimedia estén cifrados con algoritmos compatibles con FIPS 140-2 (consulte Base de datos multimedia: Consideraciones sobre la compatibilidad con versiones anteriores en la página 86)

- Ejecute el sistema operativo Windows en modo de funcionamiento aprobado por FIPS 140-2. Consulte el sitio de Microsoft para obtener información sobre cómo habilitar FIPS.

8.1.5 Consideraciones sobre la actualización

La actualización a MOBOTIX HUB VMS 2020 R3 para que funcione en modo compatible con FIPS requiere un proceso de actualización único. Este proceso de actualización solo es necesario para los usuarios existentes de MOBOTIX HUB VMS que deben operar en un modo compatible con FIPS.

El proceso de actualización depende de la versión de MOBOTIX HUB VMS desde la que se actualice.

Proceso de actualización recomendado para los clientes que ejecutan MOBOTIX HUB VMS

1. Inicie la investigación para ver si las integraciones de terceros son compatibles con FIPS 140-2 (consulte Verificación de integraciones de terceros en la página 85).
2. Prepare las conexiones de dispositivos para que sean compatibles con FIPS 140-2 (consulte Conectar dispositivos: antecedentes en la página 85).
3. Exporte grabaciones realizadas con versiones de MOBOTIX HUB VMS anteriores a 2017 R2 (consulte Base de datos de medios: Consideraciones sobre la compatibilidad con versiones anteriores en la página 86). Esto se aplica a los clientes que han cifrado o firmado grabaciones en cualquier momento.
4. Deshabilite FIPS en el sistema operativo Windows (consulte Directiva de grupo FIPS en el sistema operativo Windows en la página 91).
5. Instale MOBOTIX HUB VMS2020 R3 (consulte Instalación de MOBOTIX HUB VMS2020 R3 en la página 91).
6. Actualice las grabaciones de la base de datos de medios que se realizan con MOBOTIX HUB VMS 2019 R3 o una versión anterior (consulte Base de datos de medios: Consideraciones sobre la compatibilidad con versiones anteriores en la página 86).
7. Actualice el cifrado de las contraseñas de detección de hardware (consulte Cifrar contraseñas de detección de hardware en la página 91).
8. Habilite FIPS en el sistema operativo Windows y reinicie todos los ordenadores que tengan instalado MOBOTIX HUB VMS.

No habilite FIPS hasta que todos los ordenadores de la red MOBOTIX HUB VMS, incluidas las estaciones de trabajo MOBOTIX HUB Smart Client, estén preparados para FIPS.

8.1.6 Verifica las integraciones de terceros

Si una integración no es compatible con FIPS 140-2, no se puede ejecutar en un sistema operativo Windows con la marca de directiva de grupo FIPS habilitada.
Además, debido a los cambios realizados en el SDK de MIP en relación con FIPS, las integraciones que acceden a la lista de funciones de la licencia deben volver a compilarse.
Para asegurarse de que las integraciones seguirán funcionando después de actualizar a MOBOTIX HUB VMS 2020 R3, debe:

- Realice un inventario de todas sus integraciones con MOBOTIX HUB VMS
- Póngase en contacto con los proveedores de estas integraciones y pregunte si las integraciones cumplen con FIPS 140-2 y si prevén que las integraciones deban cambiarse debido a las actualizaciones del SDK de MIP
- Implemente las integraciones compatibles con FIPS 140-2 en MOBOTIX HUB VMS después de que se haya actualizado el VMS

8.1.7 Conectar dispositivos: en segundo plano

Si desea utilizar MOBOTIX HUB VMS en un modo compatible con FIPS, debe asegurarse de que los controladores y, por lo tanto, la comunicación con los dispositivos, también cumplan con FIPS.
Los controladores de dispositivos MOBOTIX HUB VMS pueden ser compatibles con FIPS 140-2 porque se pueden configurar y operar de modo que solo utilicen instancias de algoritmo compatibles con FIPS 140-2. Solo los controladores específicos de una configuración específica son compatibles con FIPS 140-2. En esta configuración específica de FIPS 140-2, el controlador podrá comunicarse con los dispositivos de forma compatible. Los dispositivos deben cumplir varios requisitos para poder aceptar esta comunicación. Además, la marca de directiva de grupo FIPS debe estar habilitada en Windows en el servidor donde está instalado el servidor de grabación.
Cuando se habilita la marca de directiva de grupo FIPS, los controladores compatibles con FIPS 140-2 funcionarán en modo compatible y no usarán primitivas criptográficas no aprobadas. Los controladores usarán los algoritmos utilizados solo para los canales de comunicación seguros.

Requisitos de conectividad del dispositivo

MOBOTIX HUB VMS está garantizado y puede aplicar el modo de funcionamiento conforme a FIPS 140-2 si se cumplen los siguientes criterios:

- Los dispositivos usan solo controladores de la lista (controladores compatibles en la página 92) para conectarse a MOBOTIX HUB VMS
  Esta lista muestra los controladores que pueden garantizar y hacer cumplir el cumplimiento.
- Los dispositivos usan la versión 11.1 o superior del paquete de dispositivos
  Los controladores de los paquetes de dispositivos de controladores heredados no pueden garantizar una conexión compatible con FIPS 140-2.
- Los dispositivos se conectan a través de HTTPS y en el Protocolo de transporte seguro en tiempo real (SRTP) o el Protocolo de transmisión en tiempo real (RTSP) a través de HTTPS para la transmisión de vídeo

  Los módulos de controlador no pueden garantizar el cumplimiento de FIPS 140-2 de una conexión a través de HTTP. La conexión puede ser compatible, pero no hay garantía de que sea realmente compatible.

- El equipo que ejecuta el servidor de grabación debe tener habilitada la marca de directiva de grupo FIPS en Windows

Efectos de operar en modo compatible con FIPS 140-2

Cuando se opera en modo compatible con FIPS 140-2, algunos controladores no estarán disponibles para su uso. Es posible que los controladores que figuran como FIPS 140-2 no puedan conectarse a dispositivos que no cumplan los requisitos del dispositivo.

Un controlador es compatible con FIPS 140-2 y la comunicación con el dispositivo es compatible con FIPS 140-2 si el controlador compatible con FIPS 140-2:

- Funciona en un entorno con la directiva de grupo FIPS habilitada
- Está conectado a un dispositivo que cumple con los requisitos del dispositivo (consulte Requisitos del dispositivo en la página 92)
- Está configurado correctamente (consulte Cómo configurar el dispositivo y el controlador para FIPS 140-2 en la página 93)

Si no se cumple alguno de los requisitos para el modo compatible con FIPS 140-2, no hay garantía sobre el cumplimiento de FIPS 140-2 del controlador o la comunicación con el dispositivo. Ver Controladores y FIPS 140-2 en la página 92 para obtener más información.

Dispositivos que se ejecutan a través de MOBOTIX Open Network Bridge

Cuando se ejecuta en un ordenador que tiene activada la marca de directiva de grupo FIPS en Windows, el Open Network Bridge de MOBOTIX utiliza SHA265 para cifrar la comunicación. En un equipo que no tenga FIPS habilitado, puede seleccionar MD5 o SHA165 para el cifrado.

8.1.8 Base de datos de medios: consideraciones sobre la compatibilidad con versiones anteriores

Es posible tener grabaciones en el mismo almacenamiento de varias versiones diferentes de MOBOTIX HUB VMS al mismo tiempo.

Los datos firmados o cifrados deben ser:

- Exportado desde el almacenamiento si se grabó con MOBOTIX HUB VMS versión 2017 R1 o anterior
  La exportación de datos se realiza mediante MOBOTIX HUB Smart Client.
- Actualizado, si se grabó con MOBOTIX HUB VMS versión 2017 R2 o posterior
  La actualización de datos se realiza en colaboración con el servicio de asistencia de MOBOTIX, mediante una herramienta de conversión de medios proporcionada por el servicio de asistencia de MOBOTIX.

La marca de directiva de grupo FIPS debe estar deshabilitada en el sistema operativo Windows para que se ejecute la herramienta de conversión de medios.

El servidor de grabación también debe detenerse mientras se ejecuta la herramienta de conversión de medios y no se deben realizar grabaciones mientras la herramienta se está ejecutando.

Actualización de medios en función de la versión de MOBOTIX HUB VMS

- Datos registrados con MOBOTIX HUB VMS versión 2017 R1 y anteriores
  Los datos de medios cifrados que se registraron con MOBOTIX HUB VMS 2017 R1 y versiones anteriores no están disponibles si se habilita FIPS, incluso si se ha ejecutado la herramienta de conversión de medios.
  Exporte los datos multimedia que se registraron con MOBOTIX HUB VMS 2017 R1 y versiones anteriores para acceder a ellos sin conexión.
  Ver Actualización de datos de la base de datos de medios: MOBOTIX HUB VMS 2017 R1 y versiones anteriores en la página 89.
- Datos registrados con MOBOTIX HUB VMS versión 2017 R2 a 2019 R3

Los datos multimedia que se registraron con las versiones 2017 R2 a 2019 R3 de MOBOTIX HUB VMS no se volverán a cifrar automáticamente. La conversión puede llevar mucho tiempo y debe planificarse.
Para actualizar los datos antiguos y utilizar algoritmos compatibles con FIPS, póngase en contacto con el servicio de asistencia de MOBOTIX para obtener la herramienta de conversión de medios.
Consulte Actualización de la base de datos de medios: MOBOTIX HUB VMS 2017 R2 a MOBOTIX HUB VMS 2019 R3 en la página 89.

- Datos registrados con MOBOTIX HUB VMS versión 2020 R1 o 2020 R2
  Los datos multimedia que se registraron con MOBOTIX HUB VMS 2020 R1 o 2020 R2 se volverán a cifrar automáticamente con algoritmos compatibles con FIPS 140-2 cuando se inicie el servidor de grabación después de una actualización. Ver Actualización de la base de datos de medios: MOBOTIX HUB VMS 2020 R1 o MOBOTIX HUB VMS 2020 R2 en la página 91.

Detalles de la actualización de medios

Volver a cifrar los datos con un servidor de grabación con algoritmos compatibles con FIPS es una parte central del proceso de actualización. Por lo tanto, el proceso de actualización varía en función de la versión de MOBOTIX HUB VMS utilizada para registrar esos datos.

<table>
<tr><th colspan="5">Los datos registrados con</th></tr>
<tr><th></th><th>R1 2017 y anteriores</th><th>2017 R2 - 2019 R3</th><th>R1 2020 - R2 2020</th><th>R3 2020 y posteriores</th></tr>
<tr><td>Cambios</td><td>Datos cifrados con DES
Firma con MD5
Contraseñas: Cookie en el almacenamiento CONFIG.XML
Contraseña _a y _b en la tabla CONFIG. XML's
Encriptado DES</td><td>Datos cifrados con AES
Firma con SHA</td><td>Lista de contraseñas en el almacenamiento CONFIG.XML
Las contraseñas de la lista de contraseñas están encriptadas con DES</td><td>Las contraseñas de la lista de contraseñas se cifran mediante AES
Hay disponible una herramienta de conversión de medios para actualizar la tabla CONFIG. XML de tener _a de contraseña y _b, para usar la lista de contraseñas actualizada</td></tr>
<tr><td>FIPS deshabilitado</td><td colspan="4">Toda la funcionalidad funciona según lo esperado</td></tr>
<tr><td>FIPS habilitado sDatos firmados</td><td>Los datos firmados se pueden reproducir
Se produce un error en la verificación de la firma durante la exportación</td><td colspan="3">Los datos firmados se pueden reproducir
Verificación de la firma durante los trabajos de exportación</td></tr>
<tr><td>FIPS habilitado</td><td colspan="3">El almacenamiento permanece sin conexión</td><td>Toda la funcionalidad funciona según lo esperado</td></tr>
</table>

<table>
<tr><th colspan="5">Los datos registrados con</th></tr>
<tr><th></th><th>R1 2017 y anteriores</th><th>2017 R2 - 2019 R3</th><th>R1 2020 - R2 2020</th><th>R3 2020 y posteriores</th></tr>
<tr><td>Datos cifrados
La herramienta de conversión de medios no se ejecuta</td><td colspan="3">(Es posible que el almacenamiento permanezca sin conexión si alguna vez se habilitó el cifrado para el almacenamiento)</td><td></td></tr>
<tr><td>FIPS habilitado
Sin cifrado
La herramienta de conversión de medios no se ejecuta</td><td colspan="4">Toda la funcionalidad funciona según lo esperado</td></tr>
<tr><td>La herramienta de conversión de medios se ha ejecutado</td><td colspan="2">La herramienta de conversión de medios puede requerir mucho tiempo para ejecutarse porque actualiza la tabla CONFIG. XML para todas las tablas cifradas</td><td>La herramienta de conversión de medios se ejecuta rápidamente porque solo necesita actualizar el almacenamiento CONFIG.XML</td><td>La herramienta de conversión de medios se ejecuta rápidamente porque no se necesita ninguna actualización</td></tr>
<tr><td>FIPS habilitado
Datos cifrados
La herramienta de conversión de medios se ha ejecutado</td><td>Los datos cifrados no están disponibles
Conexión perdida durante la reproducción
Al archivar con Reducir a fotogramas clave, se archiva todo el GoP</td><td colspan="3">Los datos cifrados se pueden reproducir
El archivado con Reducir a fotogramas clave funciona según lo esperado</td></tr>
<tr><td>FIPS habilitado
Sin cifrado</td><td colspan="4">Toda la funcionalidad funciona según lo esperado</td></tr>
</table>

Los datos registrados con				
	R1 2017 y anteriores	**2017 R2 - 2019 R3**	**R1 2020 - R2 2020**	**R3 2020 y posteriores**
Sin firmar La herramienta de conversión de medios se ha ejecutado				

Actualización de datos de la base de datos de medios: MOBOTIX HUB VMS 2017 R1 y versiones anteriores

Si está ejecutando MOBOTIX HUB VMS versión 2017 R1 o anterior, o si tiene datos firmados o cifrados grabados con estas versiones, las grabaciones se cifran con algoritmos que no se consideran seguros según el estándar FIPS 140-2.

No es posible acceder a estas grabaciones desde un equipo en el que esté habilitada la marca de directiva de grupo FIPS.

Como consecuencia, es necesario exportar la base de datos de medios a una ubicación donde aún se pueda acceder a ella.

Actualización de la base de datos de medios: MOBOTIX HUB VMS 2017 R2 a MOBOTIX HUB VMS 2019 R3

Si está ejecutando una versión de MOBOTIX HUB VMS entre MOBOTIX HUB VMS 2017 R2 y MOBOTIX HUB VMS 2019 R3 y si en algún momento se ha habilitado el cifrado en la base de datos de medios, para acceder a estas grabaciones debe realizar una de las siguientes opciones.

Ambas opciones requieren el uso de la herramienta de conversión de medios. El servidor de grabación debe detenerse mientras se ejecuta la herramienta de conversión de medios y no se deben realizar grabaciones mientras la herramienta se está ejecutando. Ver ¿Qué es la herramienta de conversión de medios? En la página 90 para obtener más información.

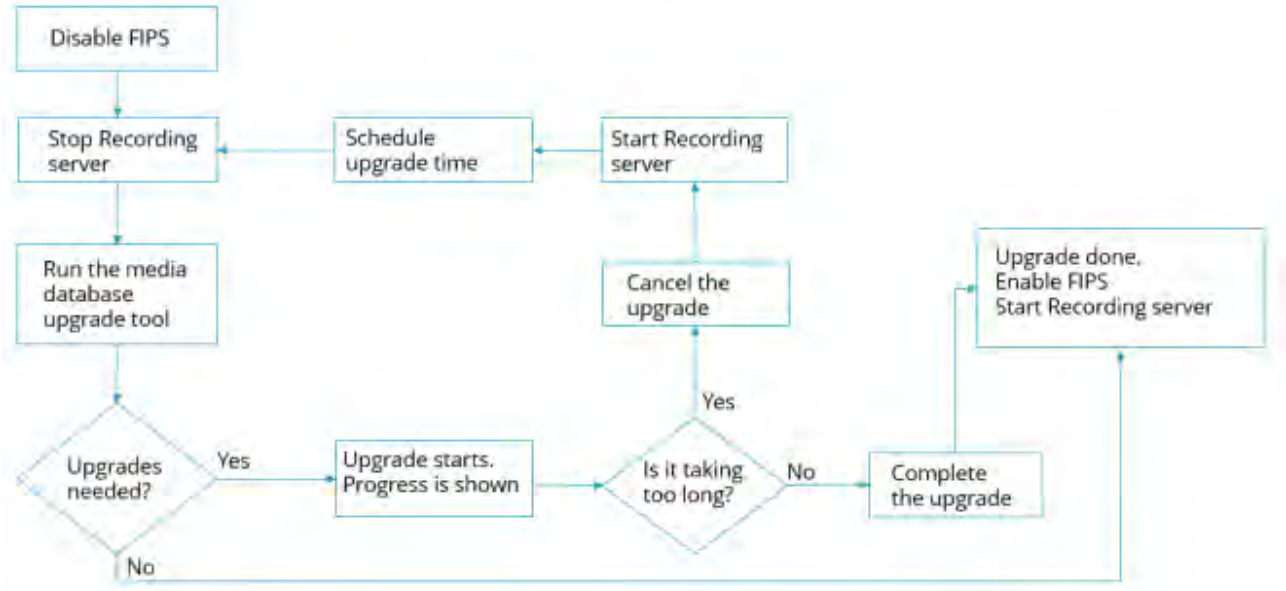
- Opción 1
  Utilice esta opción para poder operar en un entorno FIPS de inmediato y si tiene un tiempo de retención prolongado. El tiempo necesario para ejecutar la herramienta de conversión de medios podría ser significativo.
  1. Actualice MOBOTIX HUB VMS a 2020 R3.
  2. Con FIPS desactivado en el sistema operativo Windows, ejecute la herramienta de conversión de medios proporcionada por el soporte de MOBOTIX.
  3. Habilite la marca de directiva de grupo FIPS en el sistema operativo Windows.
- Opción 2
  Utilice esta opción si el funcionamiento en un entorno FIPS puede esperar, si tiene un tiempo de retención corto y si está ejecutando la herramienta de conversión de medios con menos datos.
  1. Actualice MOBOTIX HUB VMS a 2020 R3.

2. Ejecute el MOBOTIX HUB VMS durante el tiempo de retención sin habilitar FIPS en el sistema operativo Windows.
3. Ejecute la herramienta de conversión de medios para asegurarse de que todos los datos se conviertan para que sean compatibles con FIPS.
4. Habilite la marca de directiva de grupo FIPS en el sistema operativo Windows.

¿Qué es la herramienta de conversión de medios?

La herramienta de conversión de medios es un script de PowerShell independiente, que se entrega en el código fuente. No forma parte de ninguna instalación.
Se distribuirá a los clientes únicamente a través del servicio de asistencia de MOBOTIX.
Puede convertir todo el almacenamiento de forma masiva o se puede ejecutar en un almacenamiento específico.
Los indicadores de progreso muestran hasta dónde ha llegado la herramienta.
Si la conversión tarda demasiado, puede cancelar el trabajo y continuar sin FIPS habilitado.
La herramienta de conversión de medios convierte las credenciales cifradas dentro de los archivos de tabla de medios existentes al formato más reciente que es compatible con FIPS.
La herramienta de conversión de medios no cambia el cifrado de los datos de video en sí. Si los datos de vídeo se cifran con un algoritmo no compatible (DES), se cargarán las tablas actualizadas, pero no se podrá acceder al vídeo en el modo compatible con FIPS.
La herramienta de conversión de medios convierte y comprueba si todas las tablas utilizan algoritmos compatibles con FIPS.
Las tablas aprobadas se marcarán para evitar que vuelvan a ser verificadas por la herramienta de conversión de medios.
Después de ejecutar la herramienta de conversión de medios, el MOBOTIX HUB VMS 2020 R3 podrá cargar tablas en modo compatible con FIPS.

Flujo de trabajo de la herramienta de conversión de medios



Actualización de la base de datos de medios: MOBOTIX HUB VMS 2020 R1 o MOBOTIX HUB VMS 2020 R2

Si está ejecutando MOBOTIX HUB VMS versión 2020 R1 o MOBOTIX HUB VMS 2020 R2, los datos multimedia que se registren con una de estas versiones se volverán a cifrar automáticamente con algoritmos compatibles con FIPS 140-2 durante la actualización del servidor de grabación.

8.1.9 Directiva de grupo FIPS en el sistema operativo Windows

El modo de funcionamiento FIPS está habilitado y deshabilitado con la marca de directiva de grupo FIPS en el sistema operativo Windows. Consulte el sitio de Microsoft para obtener información sobre cómo habilitar y deshabilitar FIPS.

Antes de realizar la actualización, debe desactivar la marca de directiva de grupo FIPS en todos los equipos que formen parte de las máquinas virtuales de MOBOTIX HUB, incluido el equipo que aloja SQL Server y todas las estaciones de trabajo MOBOTIX HUB Smart Client.

Hay dos razones por las que el indicador de directiva de grupo FIPS debe estar desactivado en todos los ordenadores del MOBOTIX HUB VMS antes de realizar la actualización:

- Durante la actualización, los datos que se cifran con algoritmos FIPS no aprobados se vuelven a cifrar con algoritmos aprobados. Para ejecutar el descifrado en el sistema operativo Windows, la marca de directiva de grupo FIPS debe estar deshabilitada.
- Si la marca de directiva de grupo FIPS está habilitada en Windows, no podrá utilizar el MOBOTIX HUB VMS hasta que se actualicen todos los componentes. Por ejemplo, un cliente inteligente MOBOTIX HUB 2020 R2 no podrá comunicarse con un servidor de gestión 2020 R3 si el servidor de gestión está en un ordenador que tenga habilitada la marca de directiva de grupo FIPS.

Política de grupo FIPS y arquitectura federada de MOBOTIX

Si algún sitio de una arquitectura federada de MOBOTIX debe funcionar con el indicador de política de grupo FIPS habilitado en Windows, todos los sitios también deben funcionar con el indicador de política de grupo FIPS habilitado en Windows.

En consecuencia, toda la instalación de MOBOTIX Federated Architecture debe actualizarse a la versión 2020 R3.

8.1.10 Instalar MOBOTIX HUB VMS2020 R3

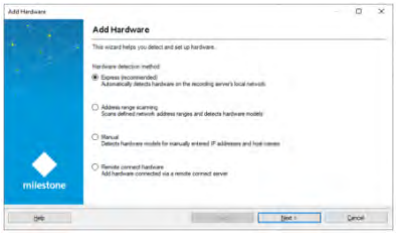
Al realizar la actualización, el instalador de MOBOTIX HUB VMS comprobará la política de seguridad de FIPS e impedirá que se inicie la actualización si FIPS está activado.

8.1.11 Cifrar contraseñas de detección de hardware

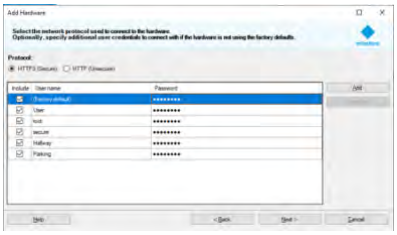
Las contraseñas de detección de hardware deben actualizarse después de actualizar a MOBOTIX HUB VMS 2020 R3. El cifrado de las contraseñas de detección de hardware no se actualiza durante la actualización desde una versión anterior de MOBOTIX HUB VMS. Pero estas contraseñas no se pueden leer si la marca de directiva de grupo FIPS está habilitada en Windows.

Debe desencadenar una conversión de estas contraseñas antes de habilitar FIPS. Haga lo siguiente:

1. Asegúrese de que la marca de directiva de grupo FIPS esté deshabilitada en Windows.
2. En MOBOTIX HUB Management Client, abra el asistente Añadir hardware.



3. Seleccione el método de detección para abrir la página de detección de hardware.



Esto desencadena el recifrado de las contraseñas de detección de hardware con algoritmos compatibles con FIPS.

Las credenciales ahora están cifradas con algoritmos compatibles con FIPS.

8.2 Controladores y FIPS 140-2

En esta sección se explica FIPS 140-2 y cómo configurar y utilizar los controladores MOBOTIX para que funcionen en modo compatible con FIPS 140-2.

8.2.1 Requisitos para el modo compatible con FIPS 140-2

Los controladores de dispositivos MOBOTIX HUB VMS pueden ser compatibles con FIPS 140-2 porque se pueden configurar y operar de modo que solo utilicen instancias de algoritmo compatibles con FIPS 140-2. Solo los controladores específicos de una configuración específica son compatibles con FIPS 140-2. En esta configuración específica de FIPS 140-2, el controlador podrá comunicarse con los dispositivos de forma compatible. Los dispositivos deben cumplir varios requisitos para poder aceptar esta comunicación. Además, la marca de directiva de grupo FIPS debe estar habilitada en Windows en el servidor donde está instalado el servidor de grabación. Cuando se habilita la marca de directiva de grupo FIPS, los controladores compatibles con FIPS 140-2 funcionarán en modo compatible y no usarán primitivas criptográficas no aprobadas. Los controladores usarán los algoritmos utilizados solo para los canales de comunicación seguros.

Requisitos del dispositivo

Para que un dispositivo pueda comunicarse con un controlador que se ejecuta en modo compatible con FIPS 140-2, debe cumplir todo lo siguiente:

- El dispositivo debe admitir la comunicación HTTPS con al menos un conjunto de cifrado compatible con FIPS 140-2 (para ver ejemplos, consulte Ejemplo de conjuntos de cifrado compatibles con FIPS 140-2 en la página 97)
- El dispositivo debe ser compatible con RTSP a través de HTTPS (tunelización RTSP y RTP a través de HTTP) mediante la autenticación básica HTTP (RFC2068 Sección 11.1) o la autenticación implícita HTTP (RFC2069, RFC7616)

  o

  El dispositivo debe ser compatible con la transmisión de medios mediante SRTP y RTSPS (RFC3711)

Controladores compatibles

Actualmente, solo un subconjunto de controladores es compatible con FIPS 140-2. Estos controladores admiten la comunicación a través de un canal seguro para todas las funciones disponibles.

Eje 1 canal	Eje PTZ de 1 canal	Eje 2 canales	Eje 3 canales
Eje 4 canales	Eje 8 canales	Eje 11 canales	Eje 12 canales
Axis Audio	Bosch PTZ	Bosch 1 canal	Bosch 2 canales
Bosch 3 canales	Bosch 16 canales	Bosch X20XF	Bosch X40XF
Canon 1 canal	Canon PTZ de 1 canal	Canon VBM	Canon VBM 40

Canon VBS	Canon VBS No Ptz	Decodificador TVI de barreras digitales	Hanwha Genérico
ONVIF	ONVIF16	Universal	Universal de 16 canales
Universal de 64 canales	Empuje de video		

Los controladores de la tabla pueden ejecutarse en modo compatible con FIPS 140-2 cuando se configuran correctamente. Esta lista no es definitiva y puede ampliarse en el futuro. Algunos controladores son compatibles con FIPS 140-2 con capacidades limitadas. Consulte las secciones específicas de controladores a continuación para obtener información sobre cómo configurarlos y cualquier limitación.
El modo compatible con FIPS 140-2 para controladores está disponible desde Device Pack 11.1.

8.2.2 Efectos de la ejecución en modo compatible con FIPS 140-2

Cuando se opera en modo compatible con FIPS 140-2, algunos controladores no estarán disponibles para su uso. Es posible que los controladores que figuran como FIPS 140-2 no puedan conectarse a dispositivos que no cumplan los requisitos del dispositivo.
Un controlador es compatible con FIPS 140-2 y la comunicación con el dispositivo es compatible con FIPS 140-2 si el controlador compatible con FIPS 140-2:

- Funciona en un entorno con la directiva de grupo FIPS habilitada
- Está conectado a un dispositivo que cumple con los requisitos del dispositivo (consulte Requisitos del dispositivo en la página 92)
- Está configurado correctamente (consulte Cómo configurar el dispositivo y el controlador para FIPS 140-2 en la página 93)

Si no se cumple alguno de los requisitos para el modo compatible con FIPS 140-2, no hay garantía sobre el cumplimiento de FIPS 140-2 del controlador o la comunicación con el dispositivo.

8.2.3 Cómo configurar el dispositivo y el controlador para FIPS 140-2

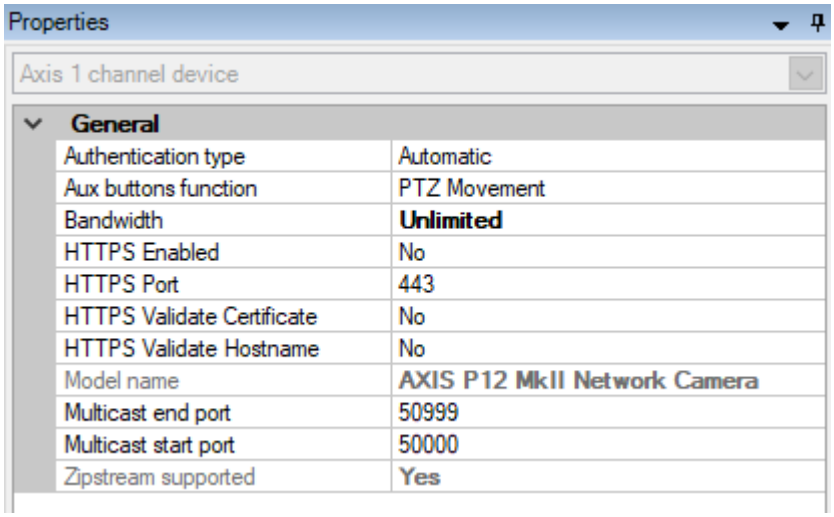
La configuración del dispositivo y el controlador para el modo compatible con FIPS 140-2 es específica del dispositivo y del controlador. Se aplican algunas pautas generales:

- Los canales de comunicación entre el controlador y el dispositivo deben ser seguros y cifrados (HTTPS, RTSP sobre HTTPS, SRTP).
- El dispositivo debe estar configurado para funcionar mediante canales seguros.
- El controlador y el dispositivo deben estar configurados para utilizar canales seguros para la comunicación en MOBOTIX HUB VMS.

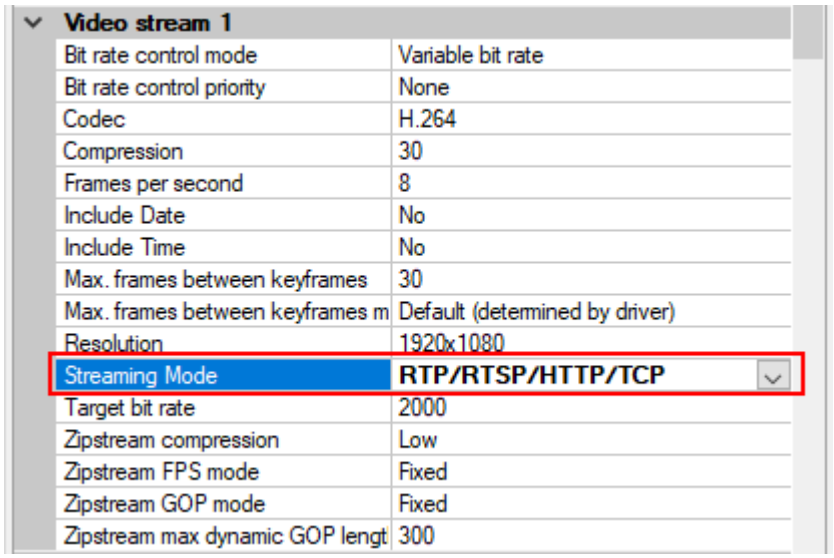
Controladores de ejes

Haga lo siguiente:

- Establezca HTTPS habilitado en Sí.
- Establezca Certificado de validación HTTPS en Sí.
- Establezca HTTPS Validate Hostname en Yes.

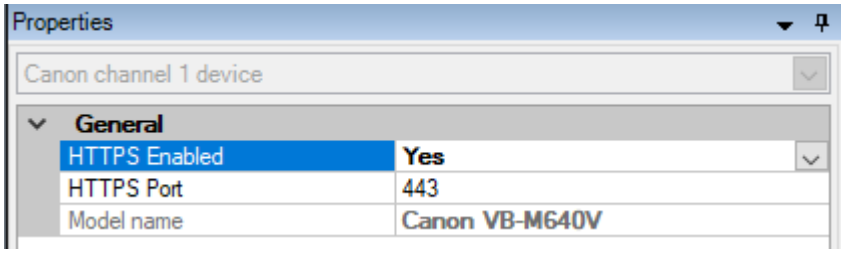


- Para cada canal de medios y flujo de medios habilitados, establezca el modo de transmisión en RTP/RTSP/HTTP/TCP.

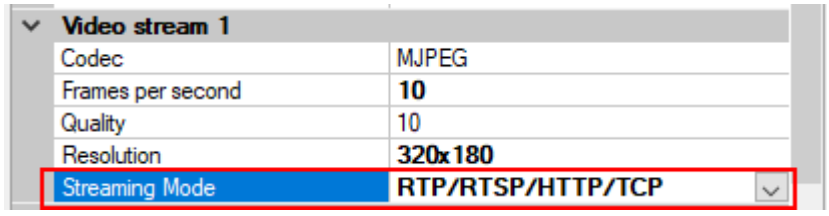


Controladores de Canon

- Establezca HTTPS habilitado en Sí.



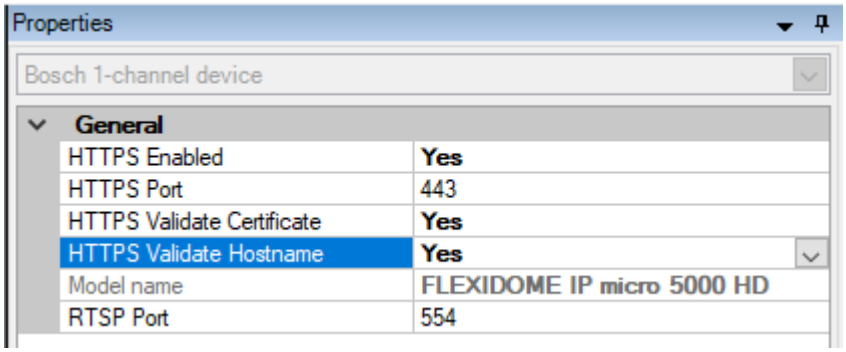
- Para cada canal de medios y flujo de medios habilitados, establezca el modo de transmisión en RTP/RTSP/HTTP/TCP.



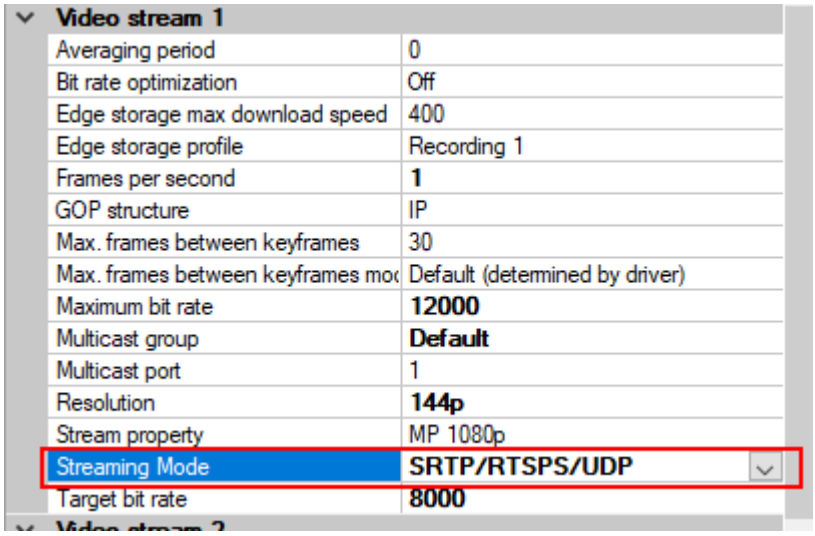
Controladores Bosch

Haga lo siguiente:

- Establezca HTTPS habilitado en Sí.
- Establezca Certificado de validación HTTPS en Sí.
- Establezca HTTPS Validate Hostname en Yes.

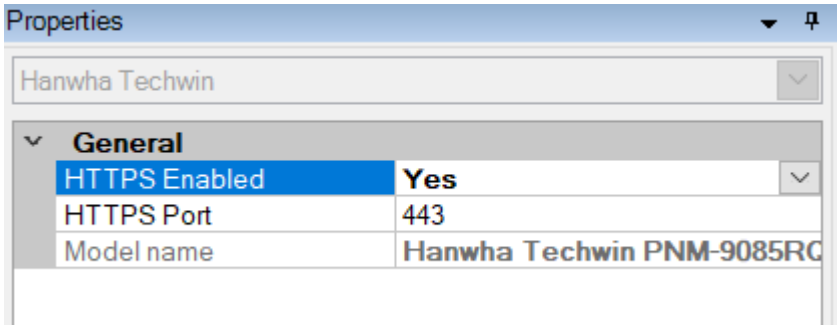


- Para cada canal multimedia y flujo multimedia habilitados, establezca el modo de transmisión en una de las siguientes opciones:
  - RTP/RTSP/HTTP/TCP
  - SRTP/RTSPS/UDP
  - Multidifusión SRT/RTSPS/UDP

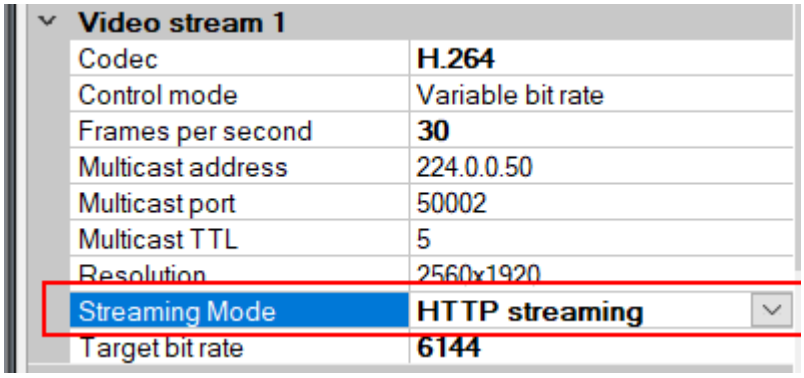


Conductores de Hanwha

- Establezca HTTPS habilitado en Sí.



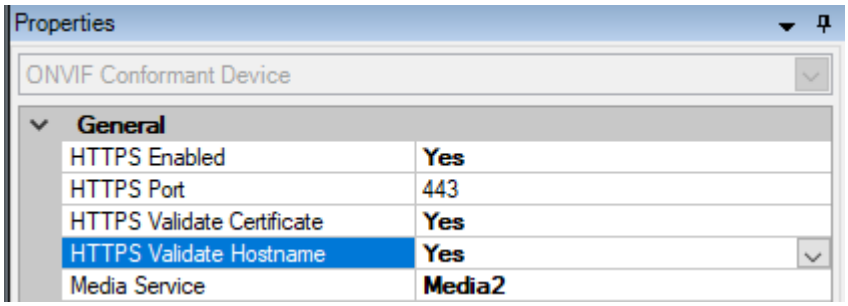
- Para cada canal de medios y transmisión de medios habilitados, establezca el modo de transmisión en transmisión HTTP.



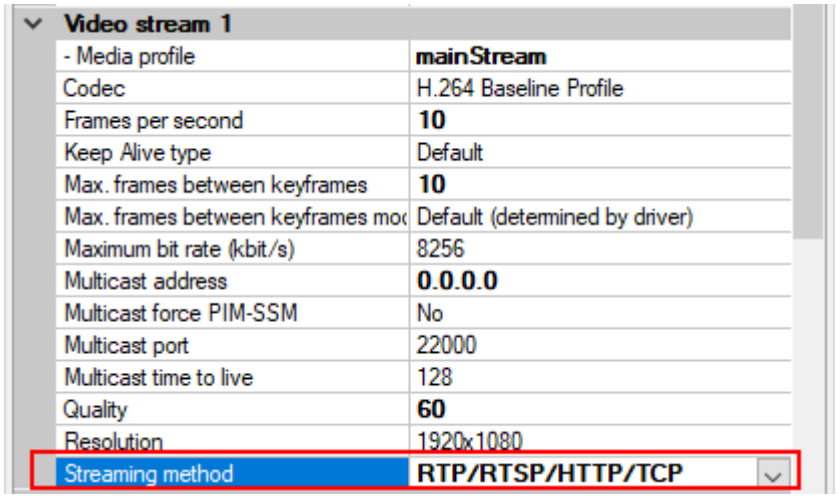
Controladores ONVIF

Haga lo siguiente:

- Establezca HTTPS habilitado en Sí.
- Establezca Certificado de validación HTTPS en Sí.
- Establezca HTTPS Validate Hostname en Yes.



- Para cada canal de medios y flujo de medios habilitados, establezca Método de transmisión en RTP/RTSP/HTTP/TCP.

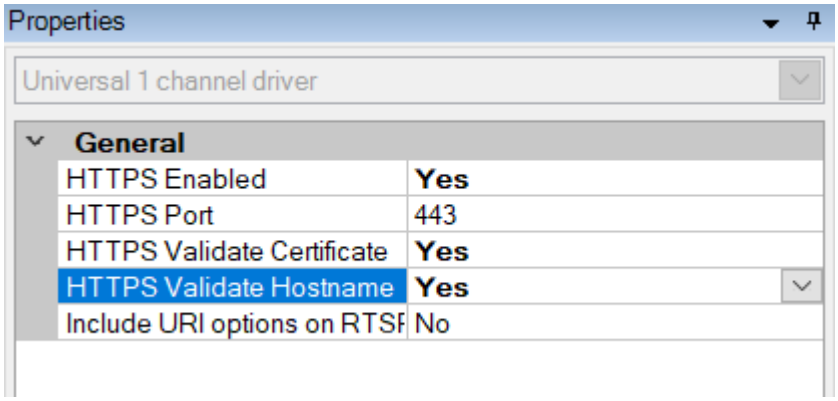


- El canal posterior de audio (salida de audio, altavoz del dispositivo) no se debe usar cuando el controlador se ejecuta en modo compatible con FIPS 140-2.

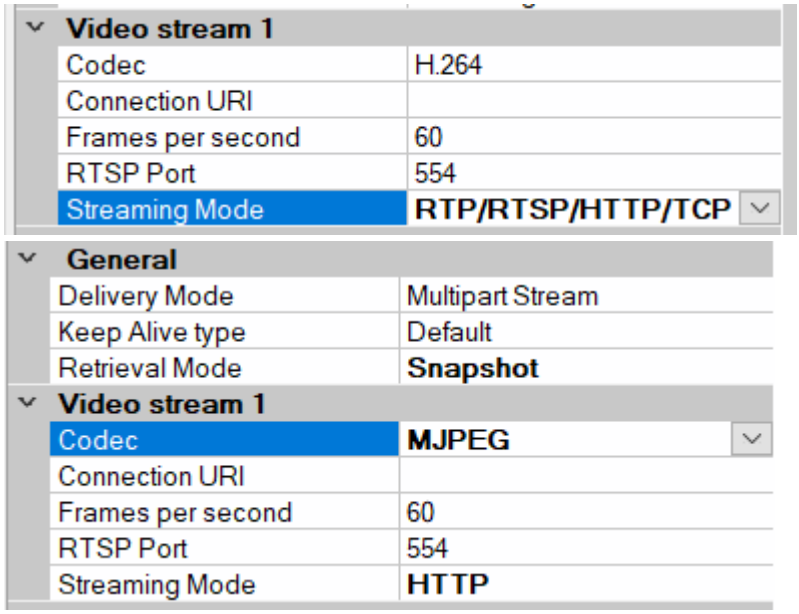
Controladores universales

Haga lo siguiente:

- Establezca HTTPS habilitado en Sí.
- Establezca Certificado de validación HTTPS en Sí.
- Establezca HTTPS Validate Hostname en Yes.



- Para cada canal de medios y transmisión de medios habilitados, establezca el modo de transmisión en RTP/RTSP/HTTP/TCP o HTTP, dependiendo de si se utiliza el modo de transmisión o recuperación de instantáneas.



Controlador VideoPush

No se necesita ninguna configuración específica. La activación de la directiva de grupo FIPS obligará al controlador a comunicarse con el servidor móvil MOBOTIX HUB de forma compatible con FIPS 140-2.

8.2.4 Ejemplo de conjuntos de cifrado compatibles con FIPS 140-2

0x1302	TLS_AES_256_GCM_SHA384
0x1303	TLS_CHACHA20_POLY1305_SHA256
0x1301	TLS_AES_128_GCM_SHA256
0xC02C	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
0xC030	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
0x00A3	TLS_DHE_DSS_WITH_AES_256_GCM_SHA384
0x009F	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
0xC02B	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
0xC02F	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
0x00A2	TLS_DHE_DSS_WITH_AES_128_GCM_SHA256

0x009E	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
0xC024	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
0xC028	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
0x006B	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
0x006A	TLS_DHE_DSS_WITH_AES_256_CBC_SHA256
0xC023	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
0xC027	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
0x0067	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
0x0040	TLS_DHE_DSS_WITH_AES_128_CBC_SHA256
0x00AD	TLS_RSA_PSK_WITH_AES_256_GCM_SHA384
0x00AB	TLS_DHE_PSK_WITH_AES_256_GCM_SHA384
0x009D	TLS_RSA_WITH_AES_256_GCM_SHA384
0x00A9	TLS_PSK_WITH_AES_256_GCM_SHA384
0x00AC	TLS_RSA_PSK_WITH_AES_128_GCM_SHA256
0x00AA	TLS_DHE_PSK_WITH_AES_128_GCM_SHA256
0x009C	TLS_RSA_WITH_AES_128_GCM_SHA256
0x00A8	TLS_PSK_WITH_AES_128_GCM_SHA256
0x003D	TLS_RSA_WITH_AES_256_CBC_SHA256
0x003C	TLS_RSA_WITH_AES_128_CBC_SHA256
0x0035	TLS_RSA_WITH_AES_256_CBC_SHA
0x002F	TLS_RSA_WITH_AES_128_CBC_SHA

Esta lista no es exhaustiva. Hay otros conjuntos de cifrado que son compatibles con FIPS 140-2. Esta lista se proporciona solo como una muestra de conjuntos de cifrado que son compatibles con FIPS 140-2.

8.3 Recursos de FIPS

1. Requisitos de seguridad de FIPS 140-2 para módulos criptográficos
   https://csrc.nist.gov/publications/detail/fips/140/2/final
2. Anexo A: Funciones de seguridad aprobadas para FIPS PUB 140-2
   https://csrc.nist.gov/CSRC/media/Publications/fips/140/2/final/documents/fips1402annexa.pdf
3. Directrices para la selección, configuración y uso de implementaciones de seguridad de la capa de transporte (TLS)
   https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r2.pdf
4. Guía de implementación para FIPS 140-2 y el programa de validación de módulos criptográficos
   https://csrc.nist.gov/csrc/media/projects/cryptographic-module-validation-program/documents/fips140-2/fips1402ig.pdf
5. Enfoque de Microsoft para la validación FIPS 140-2
   https://docs.microsoft.com/en-us/windows/security/threat-protection/fips-140-validation
6. Información general sobre TLS/SSL (Schannel SSP)
   https://docs.microsoft.com/en-us/windows-server/security/tls/tls-ssl-schannel-ssp-overview
7. Conjuntos de cifrado en TLS/SSL (Schannel SSP)
   https://docs.microsoft.com/en-us/windows/win32/secauthn/cipher-suites-in-schannel

8. Conjuntos de cifrado TLS en Windows 10 v1903, v1909 y v2004
   https://docs.microsoft.com/en-us/windows/win32/secauthn/tls-cipher-suites-in-windows-10-v1903
9. Curvas elípticas TLS en Windows 10 versión 1607 y posteriores
   https://docs.microsoft.com/en-us/windows/win32/secauthn/tls-elliptic-curves-in-windows-10-1607-and-later

9 Tabla comparativa de productos

9.1 Cuadro comparativo de productos

MOBOTIX HUB VMS incluye los siguientes productos:

- MOBOTIX HUB L1
- MOBOTIX HUB L2
- MOBOTIX HUB L3
- MOBOTIX HUB L4
- MOBOTIX HUB L5

La lista completa de funciones está disponible en la página de resumen del producto en el sitio web de MOBOTIX https://www.mobotix.com/en/vms/mobotix-hub

A continuación se muestra una lista de las principales diferencias entre los productos:

Nombre	MOBOTIX HUB L1	MOBOTIX HUB L2	MOBOTIX HUB L3	MOBOTIX HUB L4	MOBOTIX HUB L5
Sitios por SLC	1	1	Multisitio	Multisitio	Multisitio
Servidores de grabación por SLC	1	1	Irrestricto	Irrestricto	Irrestricto
Dispositivos de hardware por servidor de grabación	8	48	Irrestricto	Irrestricto	Irrestricto
Interconexión™ de MOBOTIX	-	Sitio remoto	Sitio remoto	Sitio remoto	Sitio central/remoto
Arquitectura™ federada de MOBOTIX	-	-	-	Sitio remoto	Sitio central/remoto
Conmutación por error del servidor de grabación	-	-	-	Modo de espera frío y caliente	Modo de espera frío y caliente
Servicios de conexión remota	-	-	-	-	✓
Compatibilidad con almacenamiento perimetral	-	-	✓	✓	✓
Almacenamiento de vídeo en varias etapas	Bases de datos en vivo + 1 archivo	Bases de datos en vivo + 1 archivo	Bases de datos en vivo + 1 archivo	Bases de datos en vivo + archivos sin restricciones	Bases de datos en vivo + archivos sin restricciones
Notificación SNMP	-	-	-	✓	✓
Derechos de acceso de usuario controlados por tiempo	-	-	-	-	✓
Reducir la velocidad de fotogramas (limpieza)	-	-	-	✓	✓

Nombre	MOBOTIX HUB L1	MOBOTIX HUB L2	MOBOTIX HUB L3	MOBOTIX HUB L4	MOBOTIX HUB L5
Cifrado de datos de vídeo (servidor de grabación)	-	-	-	✓	✓
Firma de base de datos (servidor de grabación)	-	-	-	✓	✓
Niveles de prioridad PTZ	1	1	3	32000	32000
PTZ ampliada (reserva de sesión PTZ y patrullaje desde MOBOTIX HUB Smart Client)	-	-	-	✓	✓
Bloqueo de pruebas	-	-	-	-	✓
Función de marcador	-	-	Solo manual	Manual y basado en reglas	Manual y basado en reglas
Multitransmisión en vivo o multidifusión / Transmisión adaptativa	-	-	-	✓	✓
Transmisión directa	-	-	-	✓	✓
Seguridad general	Derechos de usuario del cliente	Derechos de usuario del cliente	Derechos de usuario del cliente	Derechos de usuario del cliente	Derechos de usuario del cliente/ Derechos de usuario administrador
Gestión de MOBOTIX HUB Perfiles de cliente	-	-	-	-	✓
Perfiles de cliente inteligente de MOBOTIX HUB	-	-	3	3	Irrestricto
Pared inteligente MOBOTIX HUB	-	-	-	opcional	✓
Monitor del sistema	-	-	-	✓	✓
Mapa inteligente	-	-	-	✓	✓
Verificación en dos pasos	-	-	-	-	✓
Compatibilidad con DLNA	-	✓	✓	✓	✓

Nombre	MOBOTIX HUB L1	MOBOTIX HUB L2	MOBOTIX HUB L3	MOBOTIX HUB L4	MOBOTIX HUB L5
Enmascaramiento de privacidad	-	✓	✓	✓	✓
Administración de contraseñas de dispositivos			✓	✓	✓

10 Apéndice

10.1 Apéndice 1 – Recursos

Describe los requisitos mínimos para un sistema de videovigilancia. Véanse también las normas relacionadas.

1. Axis Communications: Guía de endurecimiento
2. Sistemas de seguridad de Bosch: Guía de seguridad de datos y vídeo IP de Bosch
3. Norma británica BS EN 62676-1-1: Sistemas de videovigilancia para uso en aplicaciones de seguridad, Parte 1-1: Requisitos del sistema – Generalidades
4. Describe los requisitos mínimos para un sistema de videovigilancia. Véanse también las normas relacionadas.
5. Centro para la Seguridad de Internet: Los Controles de Seguridad Críticos del CIS para una Defensa Cibernética Efectiva
6. Alianza de seguridad en la nube (CSA) y matriz de controles en la nube
7. Agencia de Sistemas de Información de Defensa (DISA): Guías de Implementación Técnica de Seguridad (STIG)
8. Grupo de Trabajo de Ingeniería de Internet (IETF), múltiples referencias
9. ISO/IEC 15048 Tecnología de la información - Técnicas de seguridad - Criterios de evaluación para la seguridad informática
10. ISO/IEC 31000, Gestión de riesgos – Principios y directrices
11. ISO/IEC 31010, Gestión de riesgos – Técnicas de evaluación de riesgos
12. ISO 27001: Seguridad de la información, ciberseguridad y protección de la privacidad — Sistemas de gestión de la seguridad de la información — Requisitos
13. ISO 27002: Seguridad de la información, ciberseguridad y protección de la privacidad — Controles de seguridad de la información
14. Guía de actualización de seguridad de Microsoft
15. Consulte también Administrar la configuración de la política de seguridad, entre otros
16. Instituto Nacional de Estándares y Tecnología: División de Seguridad Informática Centro de Recursos de Seguridad Informática
17. Instituto Nacional de Estándares y Tecnología: Marco de Ciberseguridad
18. Marco de gestión de riesgos para sistemas de información y organizaciones: un enfoque del ciclo de vida del sistema para la seguridad y la privacidad
19. Instituto Nacional de Estándares y Tecnología: Gestión del riesgo de seguridad de la información
20. Instituto Nacional de Estándares y Tecnología: Controles de Seguridad y Privacidad para Sistemas y Organizaciones de Información Federales SP 800-53- Revisión 5
21. Manual de seguridad de la información NIST SP 800-100: una guía para gerentes
22. NIST SP 800-124 Directrices para administrar la seguridad de los dispositivos móviles en la empresa
23. Sitio web del Instituto SANS y los Controles de Seguridad Críticos de SANS
24. XProtect® Corporate – Gestión avanzada de la seguridad

10.2 Apéndice 2 - Acrónimos

AD – Directorio Activo

CSA – Alianza de seguridad en la nube

CVE: vulnerabilidades y exposiciones comunes

HTTP – Protocolo de transferencia de hipertexto

HTTPS – Protocolo de Transferencia de Hipertexto Seguro

IEC – Comisión Electrotécnica Internacional

IETF – Grupo de Trabajo de Ingeniería de Internet

IP – Protocolo de Internet
ISO – Organización Internacional de Normalización
TI – Tecnología de la Información
KB – Base de conocimientos
NIST – Instituto Nacional de Estándares y Tecnología
RSTP – Protocolo de árbol de expansión rápida
SMTP – Protocolo Simple de Transferencia de Correo
SSL – Capa de conexión segura
STIG – Guía de información técnica de seguridad
TCP – Protocolo de Control de Transmisión
TLS- Seguridad de la capa de transporte
UDP – Protocolo de datagramas de usuario
VMS – Software de gestión de vídeo
VPN – Red Privada Virtual

MOBOTIX

BeyondHumanVision

EN_08/23

MOBOTIX AG • Kaiserstrasse • D-67722 Langmeil • Tel.: +49 6302 9816-103 • sales@mobotix.com • www.mobotix.com