Guía de seguridad de datos y vídeo IP de Bosch

BOSCH

es

Tabla de contenidos

1 Introducción

Aunque todas las organizaciones de hoy en día suelen contar con políticas y procedimientos de ciberseguridad, los estándares varían de una organización a otra en función de muchos factores, como el tamaño, la región o el sector de actividad.
En febrero de 2014, el National Institute of Standards and Technology (NIST) presentó su Cyber Security Framework (Marco de ciberseguridad). Este marco de trabajo se basa en la Orden Ejecutiva 13636 y se creó utilizando estándares, directivas y mejores prácticas ya existentes. Está diseñado específicamente para reducir los riesgos cibernéticos para infraestructuras críticas y los dispositivos y datos conectados a sus redes. Este marco de trabajo está diseñado para ayudar a las organizaciones a comprender los riesgos de ciberseguridad internos y externos y es aplicable a organizaciones de cualquier tamaño con categoría de capa 1 (parcial) a capa 4 (adaptativa).

Este artículo educativo está destinado a ayudar a los integradores a reforzar los productos de vídeo IP de Bosch a fin de adherirse mejor a los procedimientos y las políticas de red de las redes existentes de sus clientes.
En esta guía se trata lo siguiente:

- Información crítica sobre las características y los fundamentos de los dispositivos de vídeo IP Bosch
- Características específicas que se pueden modificar o desactivar
- Características específicas que se pueden activar y utilizar
- Mejores prácticas relativas a los sistemas de vídeo y la seguridad

Esta guía se centra principalmente en utilizar Bosch Configuration Manager para llevar a cabo las configuraciones que se analizan. En la mayoría de los casos, toda la configuración se puede llevar a cabo utilizando Bosch Video Management System Configuration Client, Bosch Configuration Manager y la interfaz web integrada en un dispositivo de vídeo.

2 Dispositivos de vídeo IP de Bosch

Los productos de vídeo IP se están convirtiendo en productos de uso común en los entornos de red actuales y, al igual que sucede con cualquier dispositivo IP colocado en una red, los administradores de TI y de seguridad tienen derecho a conocer en detalles todo el conjunto de funciones y capacidades de los dispositivos.

Al tratar con dispositivos de vídeo IP de Bosch, la primera línea de protección son los propios dispositivos. Los codificadores y las cámaras de Bosch están fabricados en un entorno controlado y seguro que se audita continuamente. Solo es posible escribir en los dispositivos mediante una carga válida de firmware, que es específica de la serie de hardware y el chipset.

La mayoría de dispositivos de vídeo IP de Bosch cuentan con un chip de seguridad en placa que proporciona una funcionalidad parecida a las de las tarjetas inteligentes criptográficas y el llamado Trusted Platform Module, abreviado como TPM. Este chip actúa como una caja fuerte para los datos críticos y protege los certificados, las claves, las licencias, etc. frente a accesos no autorizados incluso cuando se abre la cámara físicamente para acceder a ella.

Los dispositivos de vídeo IP de Bosch se han sometido a más de treinta mil (30 000) pruebas de vulnerabilidad y penetración realizadas por proveedores independientes de seguridad. Por el momento, no se ha producido ningún ciberataque con éxito en un dispositivo protegido correctamente.

3 Asignar direcciones IP

Actualmente, todos los dispositivos de vídeo IP de Bosch salen de fábrica en un estado predeterminado, listos para aceptar una dirección IP DHCP.
Si no hay ningún servidor DHCP disponible en la red activa en la que se implementa un dispositivo, el dispositivo (si utiliza el firmware 6.32 o posterior) aplicará automáticamente una dirección de enlace local en el rango 169.254.1.0 a 169.254.254.255 o 169.254.0.0/16.
Con un firmware anterior, se asignará por sí solo la dirección IP predeterminada 192.168.0.1.
Existen varias herramientas adecuadas para realizar la asignación de direcciones IP a dispositivos de vídeo IP de Bosch, entre ellas:

- IP Helper
- Bosch Configuration Manager
- Bosch Video Management System Configuration Client
- Bosch Video Management System Configuration Wizard

Todas las herramientas de software disponen de la opción de asignar una sola dirección IPv4 estática, así como un rango de direcciones IPv4 a varios dispositivos a la vez. Esto incluye el uso de máscaras de red y el direccionamiento de puerta de acceso predeterminado.
Todas las direcciones IPv4 y los valores de máscara de subred se deben introducir en la llamada "notación decimal con puntos".

Nota!
Consejo de seguridad de datos n.º 1
Uno de los primeros pasos para limitar las posibilidades de ciberataques internos en una red, ejecutados por dispositivos de red no autorizados conectados localmente a la red, es limitar las direcciones IP disponibles no utilizadas. Esto se consigue utilizando IPAM, del inglés **IP A**ddress **M**anagement (Gestión de direcciones IP), además de utilizar el rango de direcciones IP que se va a utilizar en una subred.

Utilizar una subred consiste en tomar prestados bits de la parte del host de una dirección IP para dividir una red grande en varias redes más pequeñas. Cuantos más bits se toman prestados, más redes se pueden crear, pero cada una de las admite menos direcciones de hosts.

Sufijo	Hosts	CIDR	Prestado	Binario
.255	1	/32	0	.11111111
.254	2	/31	1	.1111111**0**
.252	4	/30	2	.111111**00**
.248	8	/29	3	.11111**000**
.240	16	/28	4	.1111**0000**
.224	32	/27	5	.111**00000**
.192	64	/26	6	.11**000000**
.128	128	/25	7	.1**0000000**

Desde 1993, la Internet Engineering Task Force (IETF) introdujo un nuevo concepto de asignación de bloques de direcciones IPv4 de forma más flexible que la que se utilizaba anteriormente, mediante la arquitectura de asignación de direcciones mediante clases. El nuevo método se denomina enrutamiento entre dominios sin clases (CIDR o Classless Inter-Domain Routing en inglés) y también se utiliza con direcciones IPv6.

Las redes con clases IPv4 están designadas como clases A, B y C, con números de red de 8, 16 y 24 bits respectivamente, así como la clase D, que se utiliza para el direccionamiento multidifusión.

Ejemplo:
Para ofrecer un ejemplo fácil de entender, utilizaremos el caso con direcciones de clase C. La máscara de subred predeterminada de una dirección de clase C es 255.255.255.0. Técnicamente, esta máscara no define una subred, así que todo el último octeto está disponible para direccionar hosts de forma válida. Si tomamos prestados bits de la dirección de host, tenemos las opciones de máscaras posibles siguientes en el último octeto: .128, .192, .224, .240, .248 y .252.

Si utilizamos la máscara de subred 255.255.255.240 (4 bits) obtenemos 16 redes más pequeñas que admiten 14 direcciones de host por subred.

- ID de subred 0:
  rango de direcciones de host de 192.168.1.1 a 192.168.1.14. Dirección de difusión 192.168.1.15
- ID de subred 16:
  rango de direcciones de host de 192.168.1.17 a 192.168.1.30. Dirección de difusión 192.168.1.31
- ID de subred 32, 64, 96, etc.

Para redes mayores, podría ser necesario utilizar la clase B de red mayor, o definir un bloque de CIDR adecuado.

Ejemplo:
Antes de implementar una red de seguridad de vídeo, se debe realizar un cálculo sencillo para determinar cuántos dispositivos IP serán necesarios en la red, a fin de dejar espacio para futuras ampliaciones:

- 20 estaciones de trabajo de vídeo
- 1 servidor central
- 1 servidor VRM
- 15 cabinas de almacenamiento iSCSI
- 305 cámaras IP

Total = se necesitan 342 direcciones IP

Teniendo en cuenta el número calculado de 342 direcciones IP, como mínimo necesitamos una estructura de direcciones IP de clase B para acomodar esas direcciones IP: Utilizar la máscara de subred predeterminada de clase B, 255.255.0.0, permite disponer de 65534 direcciones IP en la red.

Alternativamente, se puede planificar la red utilizando un bloque de CIDR con 23 bits utilizados como prefijo, lo cual deja un espacio de 512 direcciones para 510 hosts.

Al dividir una red grande en partes más pequeñas, simplemente definiendo subredes, o especificando un bloque CIDR, se puede reducir este riesgo.

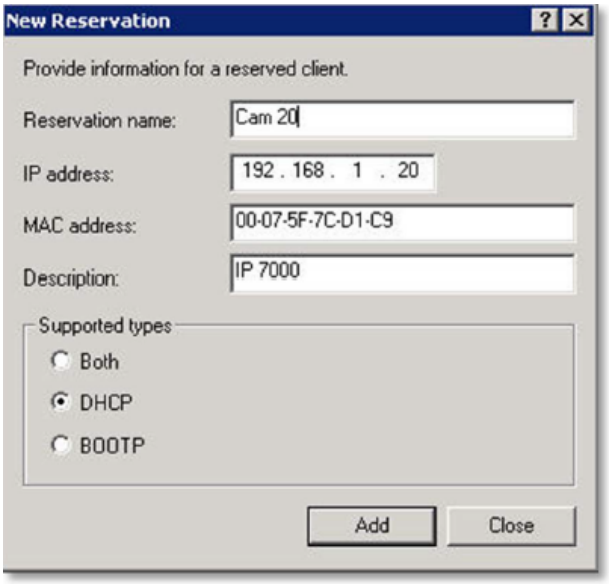
Ejemplo:

	Predeterminado	**Con subred**
Rango de direcciones IP	172.16.0.0 – 172.16.255.255	172.16.8.0 – 172.16.9.255
Máscara de subred	255.255.0.0	255.255.254.0
Notación CIDR	172.16.0.0/16	172.16.8.0/23
Número de subredes	1	128
Número de hosts	65.534	510
Direcciones en exceso	65.192	168

3.1 Gestionar DHCP

IPAM puede utilizar DHCP como una potente herramienta para controlar y utilizar direcciones IP en un entorno. DHCP se puede configurar para utilizar un intervalo específico de direcciones IP. También se puede configurar para que excluya un intervalo de direcciones.

Al utilizar DHCP, la mejor forma de implementar dispositivos de vídeo es configurar reservas de direcciones sin caducidad basadas en las direcciones MAC de cada dispositivo.



Nota!

Consejo de seguridad de datos n.º 2

Incluso antes de utilizar la gestión de direcciones IP para realizar el seguimiento de las direcciones IP, una buena práctica de gestión de redes es limitar el acceso a la red a través de la seguridad de puertos de los switches de frontera. Por ejemplo, solo una dirección MAC específica debe poder acceder a través de un puerto determinado.

4 Cuentas de usuario y contraseñas

Todos los dispositivos de vídeo IP de Bosch se suministran con tres cuentas de usuario integradas:

– **live**
  Esta cuenta de usuario estándar permite acceder solo al flujo de vídeo en directo.
– **user**
  Esta cuenta de usuario más avanzada permite acceder al vídeo en directo y al vídeo grabado, así como a los controles de la cámara, como el control PTZ.
  Esta cuenta no permite acceder a los ajustes de configuración.
– **service**
  Esta cuenta de administración permite acceder a todos los menús y ajustes de configuración del dispositivo.

De forma predeterminada, las cuentas no tienen ninguna contraseña asignada. La asignación de contraseñas es un paso crucial para proteger cualquier dispositivo en una red. Se recomienda encarecidamente asignar contraseñas a todos los dispositivos de vídeo instalados en una red.

Nota!
Con la versión 6.30 del firmware, se ha flexibilizado la gestión de usuarios a fin de permitir otros usuarios y nombres de usuario con sus propias contraseñas. Los niveles de cuenta anteriores ahora corresponden a los niveles de grupos de usuario.
Con la versión 6.32 del firmware, se ha introducido una política de contraseñas más estricta (consulte los detalles en *Página web del dispositivo, Página 11*).

4.1 Aplicar contraseñas

Las contraseñas se pueden asignar de varias formas, según el tamaño del sistema de seguridad de vídeo y el software que se utilice. En instalaciones más pequeñas, de unas pocas cámaras, se pueden establecer las contraseñas utilizando la página web del dispositivo o puesto que permite configurar más de un dispositivo a la vez y dispone de un práctico asistente de configuración, Bosch Configuration Manager.

Nota!
Consejo de seguridad de datos n.º 3
Tal como hemos dicho anteriormente, la protección con contraseña es crucial para proteger los datos de posibles ciberataques. Esto se aplica a todos los dispositivos de red de una infraestructura de seguridad completa. La mayoría de las organizaciones ya cuentan con políticas de contraseñas seguras pero, si trabaja en una instalación nueva sin políticas definidas, las siguientes son algunas de las mejores prácticas aplicables para implementar la protección mediante contraseñas:
- Las contraseñas deben tener entre 8 y 12 caracteres de longitud.
- Las contraseñas deben contener letras mayúsculas y minúsculas.
- Las contraseñas deben contener por lo menos un carácter especial.
- Las contraseñas deben contener por lo menos un dígito.

Ejemplo:
Utilizando la frase "to be or not to be" y nuestras reglas básicas de generación de buenas contraseñas.
– 2be0rnOt!t0Be

Nota!
Hay algunas restricciones para el uso de caracteres especiales como: ‘@’, '&', '<', '>', ‘:’ en las contraseña debido a su significado específico en XML y otros lenguajes de marcas. Aunque la interfaz web pueda aceptarlas, otros programas de software de administración y configuración pueden rechazarlas.

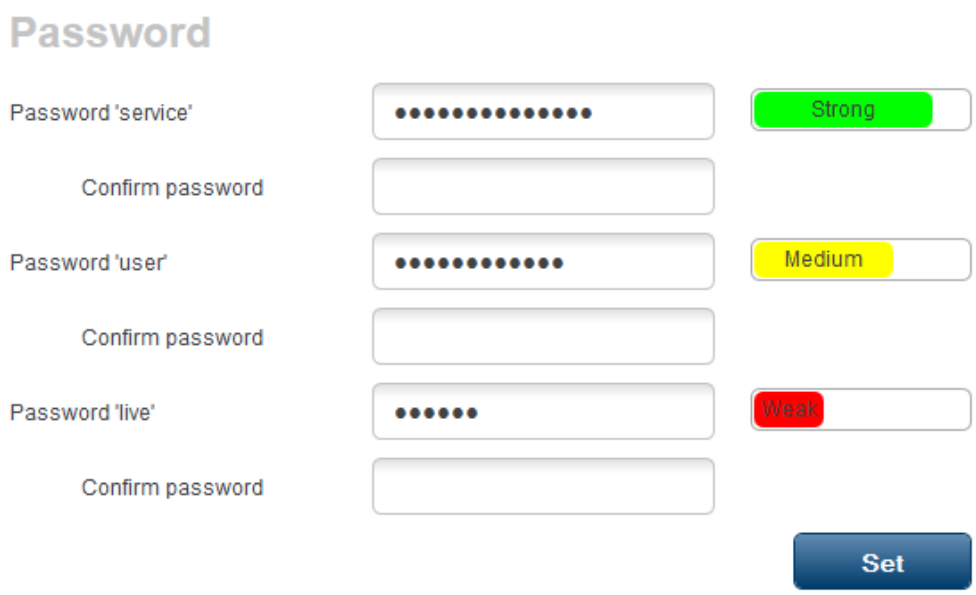
4.2 Página web del dispositivo

1. En la página web del dispositivo vaya a la página **Configuración**.
2. Seleccione el menú **General** y el submenú **Gestión de usuarios** (nota: antes de la versión 6.30 del firmware, el submenú **Gestión de usuarios** se llamaba **Contraseña**).

Al acceder a la página web de una cámara por primera vez, se pide al usuario que asigne contraseñas para garantizar una mínima protección.
Esto ser repite cada vez que se cargan las páginas web de la cámara hasta que se configure la contraseña. Al hacer clic en **Aceptar**, se accede al menú **Gestión de usuarios** automáticamente.

En el firmware 6.30 existía la opción para activar una casilla de verificación **Do not show...** (No mostrar). Esta opción se ha eliminado con el firmware 6.32 para evitar que se omitan elementos de seguridad.

1. Seleccione el menú **Gestión de usuarios** e introduzca y confirme la contraseña deseada para cada una de las tres cuentas.
   Tenga en cuenta lo siguiente:
   - Las contraseñas se deben asignar al nivel de acceso máximo (**Contraseña 'service'**) primero.
   - A partir de la versión 6.20 de la versión del firmware y en adelante, existe un indicador nuevo "medidor de la seguridad de la contraseña" que indica la posible resistencia de las contraseñas. Esta herramienta solo sirve como apoyo y no garantiza que una contraseña cumpla las exigencias de seguridad de una instalación.
2. Haga clic en **Establecer** para aplicar y guardar los cambios.



La opción **Gestión de usuarios** introducida con la versión 6.30 del firmware proporciona más flexibilidad para crear usuarios con nombres asignados libremente y con sus propias contraseñas. Los niveles de cuenta anteriores ahora corresponden a los niveles de grupos de usuario.

Los usuarios antiguos siguen existiendo, y siguen utilizando las contraseñas asignadas con el firmware anterior; no se pueden eliminar ni se puede cambiar su nivel de grupo de usuarios.

Las contraseñas se pueden asignar o cambiar haciendo clic en o  .
Si no todos los usuarios están protegidos con contraseñas, se muestra un mensaje de advertencia.

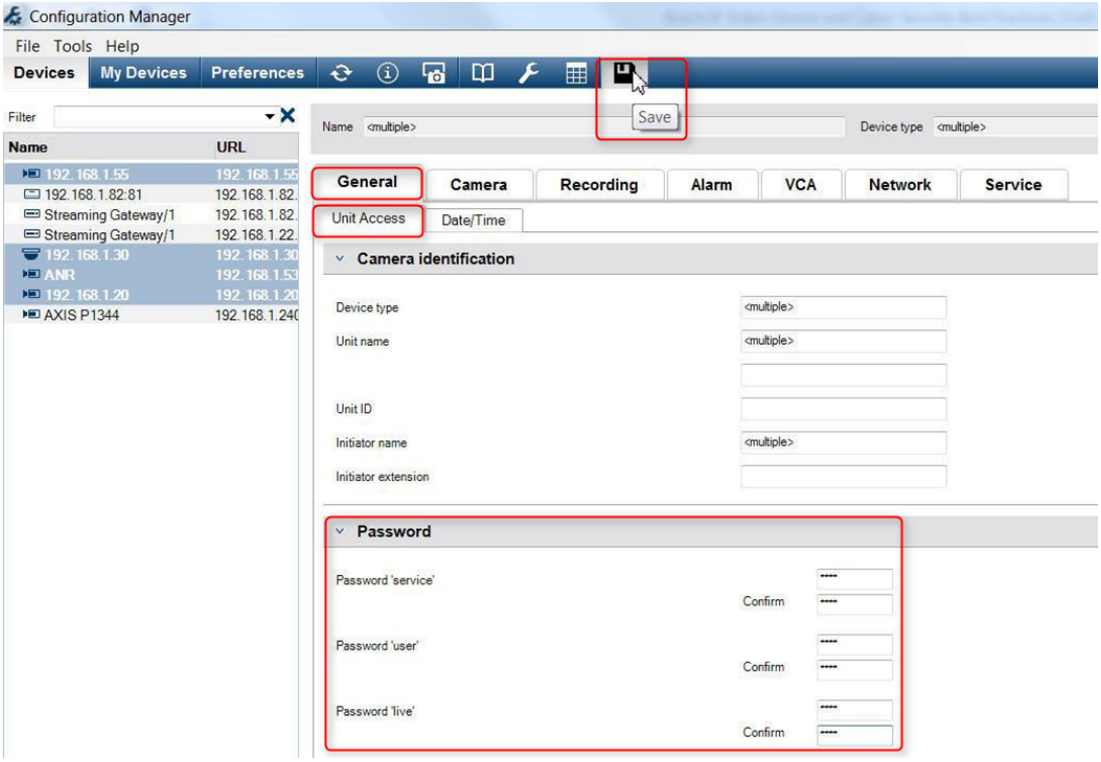
1. Para añadir un usuario nuevo, haga clic en **Añadir**.
   Se mostrará una ventana emergente.
2. Introduzca las credenciales nuevas y asigne el grupo de usuarios.
3. Haga clic en **Establecer** para guardar los cambios.

Nota!
Con la versión 6.32 del firmware también se ha introducido una política más estricta sobre las contraseñas.
Ahora, las contraseñas deben tener por lo menos 8 caracteres de longitud.

4.3 Administrador de configuración

Utilizando Bosch Configuration Manager, es posible aplicar contraseñas fácilmente a uno o más dispositivos a la vez.

1. En Configuration Manager, seleccione uno o más dispositivos.
2. Seleccione la ficha **General** y, a continuación, seleccione **Acceso a unidad**.
3. En el menú **Contraseña**, introduzca y confirme la contraseña deseada para cada una de las tres cuentas (**Contraseña 'service'**, **Contraseña 'user'** y **Contraseña 'live'**).
4. Haga clic en  para aplicar y guardar los cambios.



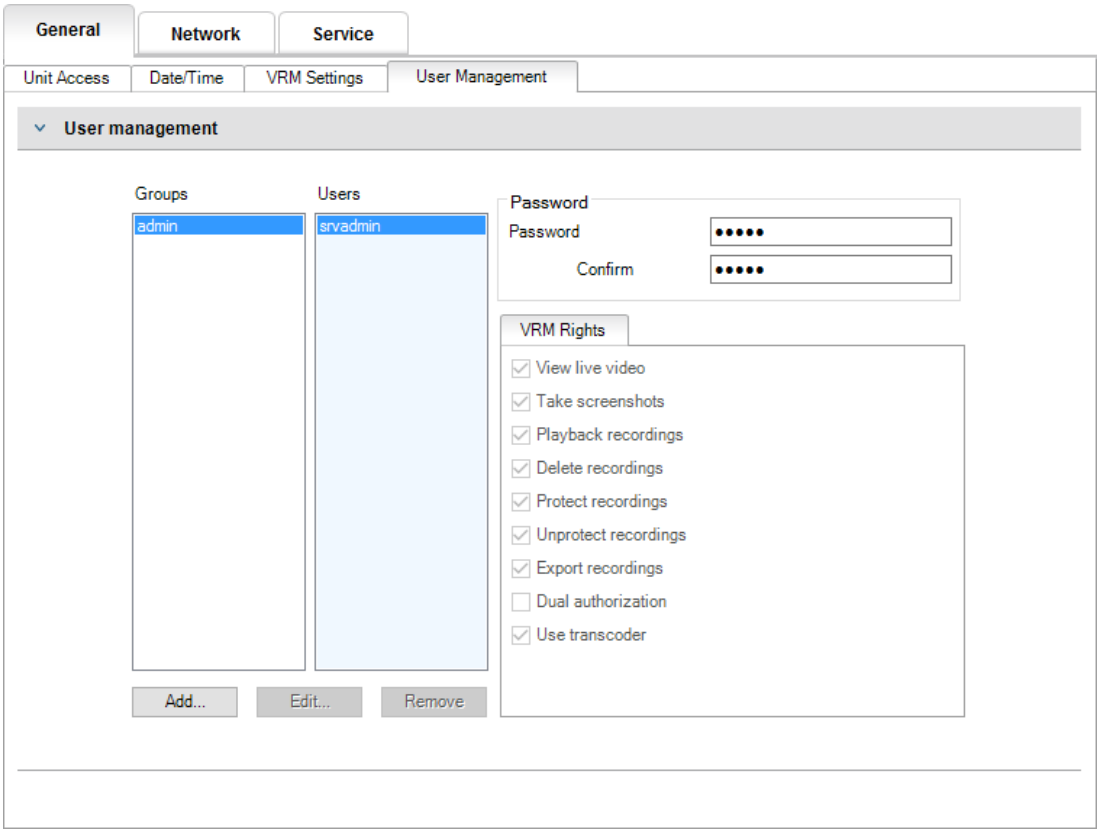
En instalaciones mayores gestionadas mediante Bosch Video Management System o Video Recording Manager instalado en una unidad de grabación, se pueden aplicar contraseñas globales a todos los dispositivos de vídeo IP añadidos al sistema. Esto permite facilitar la gestión y garantiza un nivel de seguridad estándar en todos los sistemas de vídeo de la red.

4.4 DIVAR IP 2000 / DIVAR IP 5000

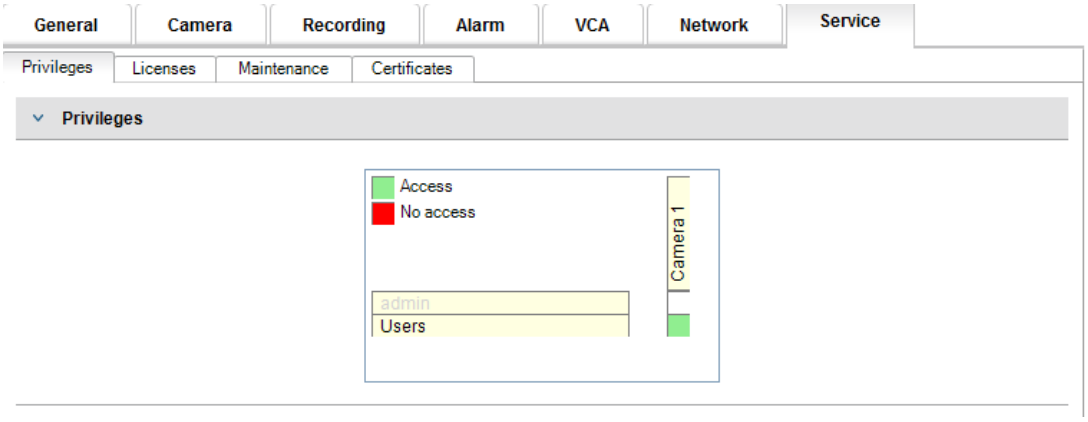
Los dispositivos de grabación DIVAR IP están equipados con un Configuration Wizard fácil de usar. Al configurar el sistema, es obligatorio asignar una contraseña de administración para todo el sistema. Esta contraseña se asigna a la cuenta service de todas las cámaras de vídeo IP añadidas al sistema. El Configuration Wizard también permite añadir una contraseña para la cuenta user, pero su implementación no es obligatoria. El indicador de seguridad de la contraseña utiliza un algoritmo parecido al que utilizan las páginas web de la cámara.

4.5 Instalación autónoma de VRM

Bosch Video Recording Manager proporciona gestión de usuarios para mejorar la flexibilidad y seguridad.
De forma predeterminada, las cuentas no tienen ninguna contraseña asignada. La asignación de contraseñas es un paso crucial para proteger cualquier dispositivo en una red. Se recomienda encarecidamente asignar contraseñas a todos los dispositivos de vídeo instalados en una red.
Lo mismo es válido para los usuarios de Video Recording Manager.



Además, es posible permitir el acceso de grupos de usuarios a ciertas cámaras y privilegios. De este modo se puede lograr una gestión de derechos de usuario detallada.

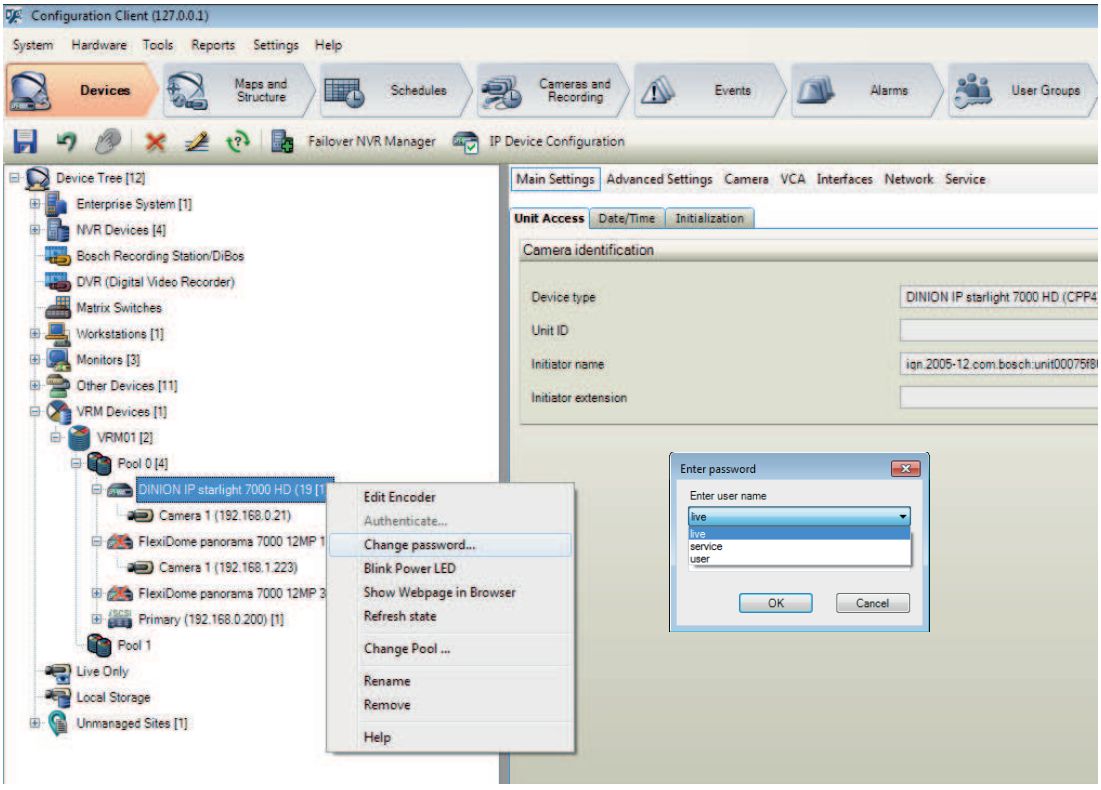


4.6 Bosch Video Management System

4.6.1 Bosch VMS / DIVAR IP 3000 / DIVAR IP 7000: protección de dispositivos con contraseñas

Las cámaras y los codificadores gestionados por Bosch Video Management System se pueden proteger frente a accesos no autorizados mediante contraseñas.
Las contraseñas de las cuentas de usuario integradas en los codificadores y las cámaras se pueden configurar mediante Bosch Video Management System Configuration Client.
Para configurar una contraseña para las cuentas de usuarios integradas en Bosch Video Management System Configuration Client:

1. En el árbol de dispositivos, seleccione el codificador que desee.
2. Haga clic con el botón derecho del ratón en el codificador y haga clic en **Cambiar contraseña....**
3. Introduzca una contraseña para las tres cuentas de usuario integradas live, user y service.

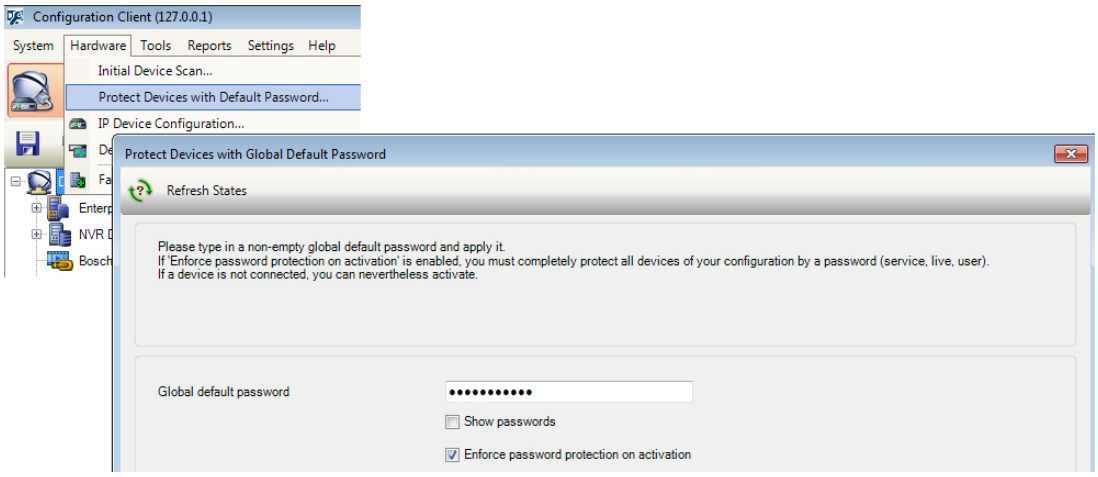


4.6.2 Bosch VMS / DIVAR IP 3000 / DIVAR IP 7000: protección con contraseña predeterminada

Las versiones de Bosch Video Management System 5.0 y posteriores proporcionan la capacidad de implementar contraseñas globales en todos los dispositivos de un sistema de vídeo de hasta 2000 cámaras IP. Esta característica está accesible mediante Bosch Video Management System Configuration Wizard al trabajar con los dispositivos de grabación DIVAR IP 3000 o DIVAR IP 7000, o mediante Bosch Video Management System Configuration Client en cualquier sistema.
Para acceder al menú de contraseñas globales de Bosch Video Management System Configuration Client:

1. En el menú **Hardware**, haga clic en **Proteger dispositivos con la contraseña predeterminada...**.

2. En el campo **Contraseña predeterminada global**, introduzca una contraseña y seleccione **Aplicar protección mediante contraseña durante la activación**.



Después de guardar y activar los cambios del sistema, la contraseña introducida se aplicará a las cuentas live, user y service de todos los dispositivos, incluida la cuenta de administración de Video Recording Manager.

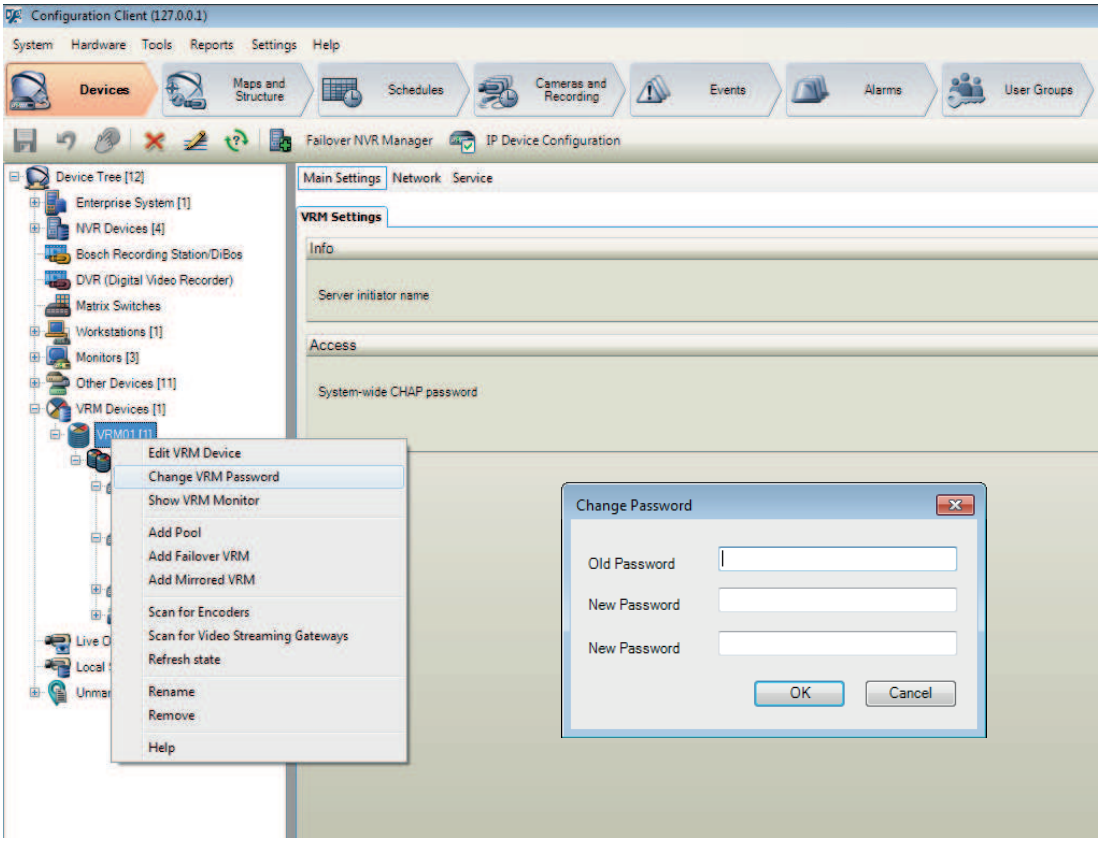
Nota!
Si los dispositivos ya disponen de contraseñas configuradas en cualquiera de las cuentas, estas no se modificarán.
Por ejemplo, si hay una contraseña configurada para service pero no para live y user, la contraseña global solo se aplicará a las cuentas live y user.

4.6.3 Configuración de Bosch VMS y VRM

De forma predeterminada, Bosch Video Management System dispone de la cuenta de administración integrada **srvadmin** para conectarse a Video Recording Manager con protección mediante contraseña. Para evitar accesos no autorizados a Video Recording Manager, la cuenta de administración **srvadmin** se debe proteger con una contraseña compleja.

Para cambiar la contraseña de la cuenta **srvadmin** en Bosch Video Management System Configuration Client:

1. En el árbol de dispositivos, seleccione el dispositivo VRM.
2. Haga clic con el botón derecho del ratón en el dispositivo VRM y haga clic en **Cambiar contraseña VRM.**
   Se mostrará el cuadro de diálogo **Cambiar contraseña...**.
3. Introduzca una contraseña nueva para la cuenta **srvadmin** y haga clic en **Aceptar**.



4.6.4 Bosch VMS / DIVAR IP 3000 / DIVAR IP 7000: comunicación cifrada con las cámaras

Desde la versión 7.0 de Bosch Video Management System, es posible encriptar los datos de vídeo en directo y las comunicaciones de control entre las cámaras y Bosch Video Management System Operator Client, Configuration Client, Management Server y Video Recording Manager,

Después de activar la conexión segura en el cuadro de diálogo **Editar codificador**, Bosch Video Management System Server, Operator Client y Video Recording Manager utilizarán una conexión segura HTTPS para conectarse a una cámara o un codificador.

La cadena de conexión interna que utiliza internamente Bosch Video Management System cambiará de rcpp://a.b.c.d (conexión RCP+ normal en el puerto 1756) a https://a.b.c.d (conexión HTTPS en el puerto 443).

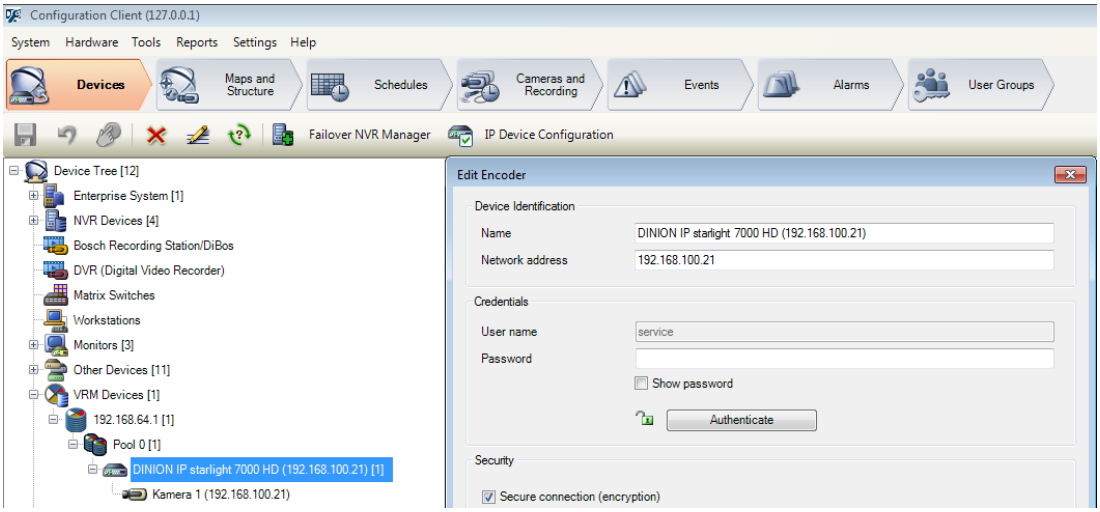
En dispositivos antiguos que no admitan HTTPS, la cadena de conexión permanece inalterada (RCP+).

Al seleccionar la comunicación mediante HTTPS, la comunicación utilizará HTTPS (TLS) para cifrar todas las comunicaciones de control y la carga de datos de vídeo mediante el motor de cifrado que contiene el dispositivo. Al utilizar TLS, todas las comunicaciones de control y la carga de datos de vídeo HTTPS se cifran con una clave de cifrado AES de 256 bits de longitud.

Para permitir la comunicación cifrada en Bosch Video Management System Configuration Client:

1. En el árbol de dispositivos, seleccione el codificador o la cámara que desee.
2. Haga clic con el botón derecho en el codificador o la cámara y haga clic en **Editar codificador**.
3. En el cuadro de diálogo **Editar codificador**, active **Conexión segura (encriptación).**

4. Guarde y active la configuración.



Después de activar la conexión segura con el codificador, es posible desactivar otros protocolos (consulte *Uso general de puertos de red y transmisión de vídeo, Página 19*).

Nota!
Bosch VMS solo admite el puerto HTTPS predeterminado 443. No se admite el uso de otros puertos.

5 Reforzar la seguridad del acceso a los dispositivos

Todos los dispositivos de vídeo IP de Bosch disponen de páginas web integradas con varios fines. Las páginas web específicas de los dispositivos admiten las funciones de vídeo en directo y reproducción de vídeo, así como algunos ajustes de configuración específicos que pueden no ser accesibles mediante un sistema de gestión de vídeo. Las cuentas de usuario integradas actúan como acceso a las distintas secciones de las páginas web específicas. Aunque el acceso a las páginas web no se puede desactivar totalmente mediante la propia página web (Configuration Manager se podría utilizar para ello), existen varios métodos para encubrir la presencia del dispositivo, limitar el acceso y gestionar el uso de los puertos de vídeo.

5.1 Uso general de puertos de red y transmisión de vídeo

Todos los dispositivos de vídeo IP de Bosch utilizan el protocolo de control remoto Plus (RCP +) para la detección, el control y las comunicaciones. RCP+ es un protocolo propio de Bosch que utiliza puertos estáticos específicos para detectar y comunicarse con dispositivo de vídeo IP de Bosch (1756, 1757 y 1758). Al trabajar con Bosch Video Management System u otros sistemas de gestión de vídeo de terceros con dispositivos de vídeo IP de Bosch integrados mediante Bosch VideoSDK, es necesario que los puertos enumerados sean accesibles en la red para que los dispositivos de vídeo IP funcionen correctamente.

El vídeo se puede transferir en forma de flujo desde los dispositivos de varias formas: UDP (dinámico), HTTP (80) o HTTPS (443).
Es posible modificar el uso de los puertos HTTP y HTTPS (consulte *Uso de puertos de HTTP, HTTPS y vídeo, Página 20*). Antes de realizar cualquier modificación en los puertos, es necesario configurar la forma deseada de comunicación con un dispositivo. Se accede al menú Communication (Comunicación) utilizando Configuration Manager.

1. En Configuration Manager, seleccione el dispositivo deseado.
2. Seleccione la ficha **General** y, a continuación, seleccione **Acceso a unidad**.
3. Busque la parte **Acceso a dispositivo** de la página.

4. En la lista **Protocolo**, seleccione el protocolo deseado:

– RCP+
– HTTP (predeterminado)
– HTTPS

Al seleccionar comunicaciones HTTPS, para la comunicación entre Configuration Manager y los dispositivos de vídeo se utilizará HTTPS (TLS) a fin de cifrar la carga de datos con una clave de cifrado AES de hasta 256 bits de longitud. Esta es una característica básica gratuita. Al utilizar TLS, todas las comunicaciones de control y los datos de la carga de vídeo HTTPS se cifran con el motor de cifrado del dispositivo.

Nota!
El cifrado se realiza específicamente para la ruta de transmisión: Una vez que un descodificador software o hardware reciben el vídeo, el flujo se descifra de forma permanente.

Nota!

Consejo de seguridad de datos n.º 4

Al definir el nivel mínimo de seguridad para acceder a dispositivos desde software de cliente, asegúrese de que todos los puertos y protocolos que permiten un nivel de acceso interior estén apagados o desactivados en los dispositivos.

5.1.1 Uso de puertos de HTTP, HTTPS y vídeo

Es posible modificar o desactivar el uso de puertos HTTP y HTTPS en todos los dispositivos. Es posible forzar la comunicación cifrada desactivando el puerto RCP+ y el puerto HTTP, lo cual obliga a utilizar el cifrado en todas las comunicaciones. Si se desactiva el uso del puerto HTTP, HTTPS seguirá activado y los intentos de desactivarlo generarán errores.

1. En Configuration Manager, seleccione el dispositivo deseado.
2. Seleccione la ficha **Red** y, a continuación, seleccione **Acceso a la red**.
3. Busque la parte **Detalles** de la página.

4. En la parte **Detalles**, modifique los puertos HTTP y HTTPS del navegador y el puerto RCP+ utilizando el menú desplegable:
   - Modificación de puertos de navegador HTTP: 80 o puertos 10000 a 10100
   - Modificación de puertos de navegador HTTPS: 443 o puertos 10443 a 10543
   - Puerto RCP+ 1756: **Activado** o **Desactivado**

Nota!

En las versiones 6.1x del firmware, si se desactiva el puerto HTTP y se intenta acceder a la página web del dispositivo, la solicitud se redirige al puerto HTTPS definido en ese momento. La característica de redirección se omitió en las versiones 6.20 y posteriores del firmware. Si el puerto HTTP está desactivado y se ha modificado el puerto HTTPS para utilizar otro puerto que no sea el 443, solo es posible acceder a las páginas web navegando a la dirección IP de los dispositivos más el puerto asignado.

Ejemplo:

https://192.168.1.21:10443. Cualquier intento de conectase a la dirección predeterminada generará un error.

5.1.2 Software de vídeo y selección de puertos

Ajustar estos parámetros de configuración también afecta al puerto que se utiliza para la transmisión de vídeo al utilizar software de gestión de vídeo en la LAN.

Si todos los dispositivos de vídeo IP están configurados con el puerto HTTP 10000, por ejemplo, y Bosch Video Management System Operator Client está configurado con la opción de túnel TCP, todas las transmisiones de vídeo de la red se llevarán a cabo mediante el puerto HTTP 10000.

Nota!
Los cambios en la configuración de los puertos de los dispositivos deben ir acorde con la configuración del sistema de gestión y sus componentes, así como con la de los clientes.

Nota!
Consejo de seguridad de datos n.º 5
En función del entorno de implementación y los objetivos de seguridad de la instalación, las mejores prácticas pueden variar. Desactivar y redirigir el uso de puertos HTTP y HTTPS tiene sus ventajas. Cambiar el puerto en cualquier protocolo puede ayudar a evitar proporcionar información a herramientas de red como NMAP (Network Napper, que es un analizador gratuito de la seguridad). Por lo general, las aplicaciones como NMAP se utilizan para realizar reconocimientos a fin de identificar puntos débiles en cualquier dispositivo de una red. Esta técnica, combinada con la implementación de contraseñas fuertes, añade seguridad al sistema en general.

5.1.3 Acceso Telnet

Telnet es un protocolo de capa de comunicaciones que proporciona comunicación con dispositivos mediante una sesión de terminal virtual con fines de mantenimiento y de localización y solución de problemas. Todos los dispositivos de vídeo IP de Bosch son aptos para Telnet y, de forma predeterminada, la compatibilidad con Telnet está activada en las versiones de firmware hasta 6.1x. A partir de la versión 6.20 del firmware en adelante, el puerto de Telnet está desactivado de forma predeterminada.

Nota!
Consejo de seguridad de datos n.º 6
Desde 2011 se ha producido un aumento de los ciberataques utilizando el protocolo Telnet. En los entornos actuales, las mejores prácticas recomiendan desactivar la compatibilidad con Telnet en todos los dispositivos hasta que sea necesario por motivos de mantenimiento o de localización y solución de problemas.

1. En Configuration Manager, seleccione el dispositivo deseado.
2. Seleccione la ficha **Red** y, a continuación, seleccione **Acceso a la red**.
3. Busque la parte **Detalles** de la página.

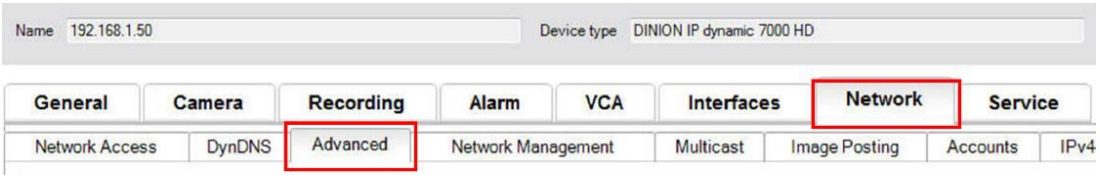
4. En la sección **Detalles**, **Active** o **Desactive Soporte de Telnet**.

Nota!
Consejo de seguridad de datos n.º 7
Desde la versión 6.20 del firmware, también se admite Telnet mediante sockets web, los cuales utilizan conexiones seguras HTTPS. Los sockets web o utilizan el puerto Telnet estándar y son una forma segura de acceder a la interfaz de línea de comandos del dispositivo IP si es necesario.

5.1.4 RTSP: Real Time Streaming Protocol

Real Time Streaming Protocol (RTSP) es el principal componente de vídeo que utiliza el protocolo ONVIF para proporcionar flujos de vídeo y control de dispositivos a los sistemas de gestión de vídeo compatibles con ONVIF. Diversas aplicaciones de vídeo de terceros también utilizan RTSP para funciones básicas de transmisión de flujos y, en algunos casos, se puede utilizar para localizar y solucionar problemas en los dispositivos y en la red. Todos los dispositivos de vídeo IP de Bosch pueden proporcionar flujos con el protocolo RTSP.
Los servicios RTSP se pueden modificar fácilmente utilizando Configuration Manager.

1. En Configuration Manager, seleccione el dispositivo deseado.
2. Seleccione la ficha **Red** y, a continuación, seleccione **Avanzado**.



3. Busque la parte **RTSP** de la página.
4. En el menú desplegable **Puerto RTSP**, desactive o modifique el servicio RSTP.
   - Puerto predeterminado de RTSP: 554
   - Modificación del puerto RTSP: 10554 a 10664

Nota!
Consejo de seguridad de datos n.º 8
Existen informes recientes de ciberataques utilizando asaltos a través del búfer de rebose de pila de RTSP. Estos ataques estaban dirigidos a dispositivos de proveedores específicos. Las mejores prácticas indican que es recomendable desactivar el servicio si no se utiliza en un sistema de gestión de vídeo compatible con ONVIF ni para la transmisión básica de flujos en tiempo real.
Alternativamente, si el cliente receptor lo permite, es posible utilizar la comunicación RTSP mediante túnel utilizando una conexión HTTPS, lo cual es, por el momento, la única forma de transmitir datos RTSP cifrados.

Nota!
Para obtener más información sobre RTSP, consulte la nota de servicio técnico "Uso de RTSP con dispositivos Bosch VIP" en el catálogo de productos en línea de Bosch Security Systems, en el enlace siguiente:

http://resource.boschsecurity.com/documents/RTSP_VIP_Configuration_Note_enUS_9007200806939915.pdf

5.1.5 UPnP: Universal Plug and Play

Los dispositivos de vídeo IP de Bosch son capaces de comunicarse con dispositivos de red mediante **UPnP**. Esta característica se utiliza principalmente en sistemas pequeños, con solo unas cuantas cámaras que aparecen automáticamente en el directorio de red de un PC y, por consiguiente, son fáciles de encontrar. Sin embargo, lo mismo se puede decir de cualquier dispositivo de la red.
UPnP se puede desactivar utilizando Configuration Manager.

1. En Configuration Manager, seleccione el dispositivo deseado.

2. Seleccione la ficha **Red** y, a continuación, seleccione **Gestión de red**.

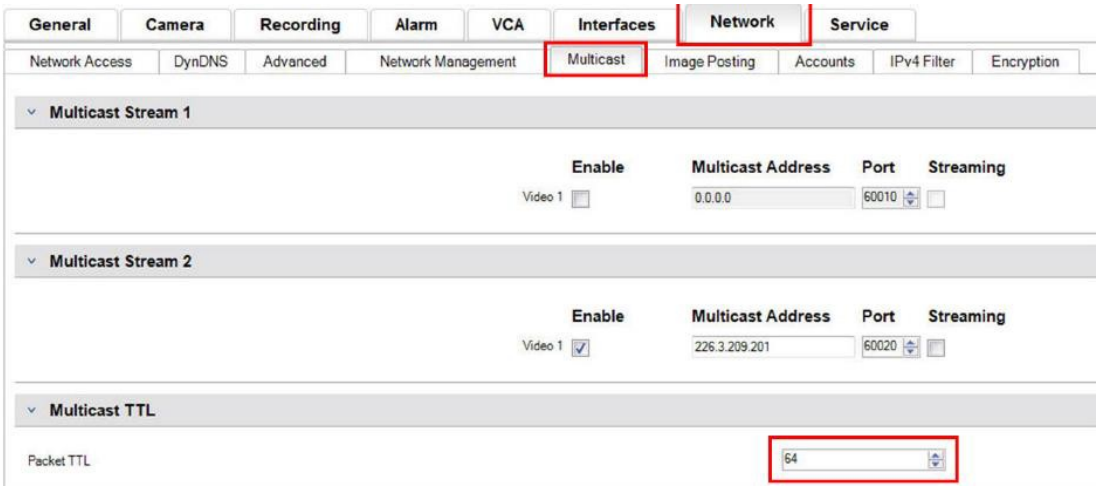
3. Busque la parte **UPnP** de la página.
4. En el menú desplegable **UPnP**, seleccione **Off** (Desactivado) para desactivar **UPnP**.

Nota!
Consejo de seguridad de datos n.º 9
No se debe utilizar **UPnP** en grandes instalaciones debido al gran número de notificaciones de registro y el riesgo de accesos o ataques no deseados.

5.1.6 Multidifusión

Todos los dispositivos de vídeo IP de Bosch pueden proporcionar vídeo en "multidifusión bajo demanda" o "flujos multidifusión". Mientras que las transmisiones de vídeo de difusión única se basan en el destino, la multidifusión se basa en el origen y esto puede provocar problemas de seguridad en la red, incluido el control del acceso a grupos, la confianza en los centros de usuarios y la confianza en los routers. Aunque la configuración de los routers queda fuera del ámbito de esta guía, existe una solución que se puede implementar desde el propio dispositivo de vídeo IP.
El alcance TTL ("time-to-live" en inglés, o tiempo de validez) define dónde y hasta dónde se permite el flujo de tráfico multidifusión dentro de una red, donde cada salto reduce el TTL en una unidad. Al configurar los dispositivos de vídeo IP para el uso en multidifusión, se puede modificar el paquete TTL de cada dispositivo.

1. En Configuration Manager, seleccione el dispositivo deseado.
2. Seleccione la ficha **Red** y, a continuación, seleccione **Multidifusión**.
3. Busque la parte **TTL de multidifusión** de la página.
4. Ajuste la configuración de **TTL de paquete** utilizando los valores y límites de alcance de TTL siguientes:
   - Valor TTL 0 = Limitado al host local
   - Valor TTL 1 = Limitado a la misma subred
   - Valor TTL 15 = Limitado al mismo sitio
   - Valor TTL 64 (predeterminado) = Limitado a la misma región
   - Valor TTL 127 = Todo el mundo
   - Valor TTL 191 = Todo el mundo con ancho de banda limitado
   - Valor TTL 255 = Datos ilimitados



Nota!

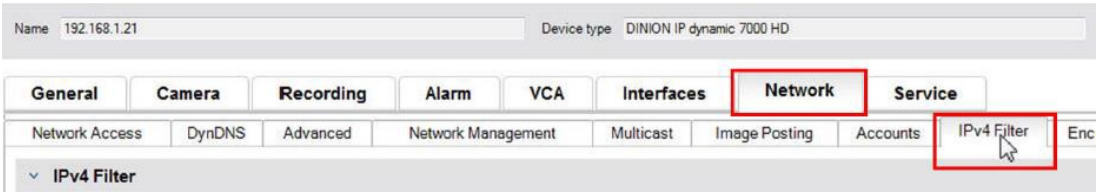
Consejo de seguridad de datos n.º 10

Al tratar con datos de videovigilancia, una práctica recomendada es configurar el ajuste de TTL a 15, lo cual limita al mismo sitio. Es incluso mejor, si conoce el número máximo exacto de saltos, utilizarlo como valor de TTL.

5.1.7 Filtrado IPv4

Puede liminar el acceso a cualquier dispositivo de vídeo IP de Bosch mediante una característica que se llama filtrado IPv4. El filtrado IPv4 utiliza los fundamentos básicos de la creación de subredes para definir hasta dos rangos de direcciones IP permisibles. Una vez definido, deniega el acceso desde cualquier dirección IP de fuera de estos rangos.

1. En Configuration Manager, seleccione el dispositivo deseado.
2. Seleccione la ficha **Red** y, a continuación, seleccione **Filtro IPv4**.

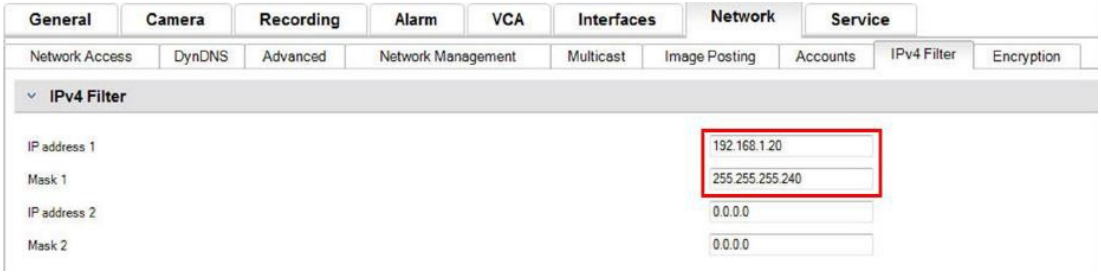


Nota!

Para configurar esta característica correctamente, es necesario tener conocimientos básicos de subredes o poder acceder a una calculadora de subredes. Introducir valores incorrectos en este ajuste puede limitar el acceso al propio dispositivo y puede ser necesario restablecerlo a sus valores predeterminados de fábrica para poder volver a acceder a él.

3. Para añadir una regla de filtro, realice dos entradas:
   - Introduzca una dirección IP base dentro de la regla de subred que haya creado. La dirección IP base especifica qué subred se va a permitir y debe quedar dentro del rango deseado.
   - Introduzca una máscara de subred que defina las direcciones IP con las que el dispositivo de vídeo IP aceptará la comunicación.

En el ejemplo siguiente se han introducido la **Dirección IP 1** igual a 192.168.1.20 y la **Máscara 1** 255.255.255.240. Este ajuste limitará el acceso desde dispositivos que queden dentro del rango de IP definido de 192.168.1.16 a 192.168.1.31.



Mientras se utiliza la característica de **Filtro IPv4**, es posible detectar los dispositivos RCP+, pero no es posible acceder a la configuración ni al vídeo con clientes que se encuentren fuera del rango de direcciones IP permitidas. Esto incluye el acceso con navegador web.
No es necesario localizar el dispositivo de vídeo IP en sí en el rango de direcciones permitidas.

Nota!
Consejo de seguridad de datos n.º 11
Según la base de la estructura del sistema, utilizar la opción **Filtro IPv4** puede reducir la visibilidad indeseada de los dispositivos en la red. Si decide activar esta opción, asegúrese de documentar la configuración para futuras consultas.
Tenga en cuenta que el dispositivo será accesible IPv6, así que el filtrado IPv4 solo tiene sentido en redes puramente IPv4.

5.1.8 SNMP

Simple Network Management Protocol (SNMP) es un protocolo de uso corriente para monitorizar el estado de funcionamiento de un sistema. Por lo general, este sistema de monitorización utiliza un servidor de gestión central que recopila todos los datos de los componentes y dispositivos compatibles con el sistema.
SNMP proporciona dos métodos para acceder al estado de funcionamiento del sistema:
– El servidor de gestión de la red puede sondear el estado de funcionamiento de un dispositivo mediante solicitudes SNMP.
– Los dispositivos pueden notificar su estado de funcionamiento activamente al servidor de gestión de red en caso de error o de que se produzca una situación de alarma enviando trampas SNMP al servidor SNMP. Estas trampas se deben configurar dentro del dispositivo.

SNMP también permite configurar algunas variables en los dispositivos y componentes.
La información, qué mensajes admite un dispositivo y qué trampas puede enviar, derivan de la base de información de gestión, o el llamado archivo MIB, que es un archivo que se suministra con un producto para facilitar su integración en un sistema de monitorización de red.

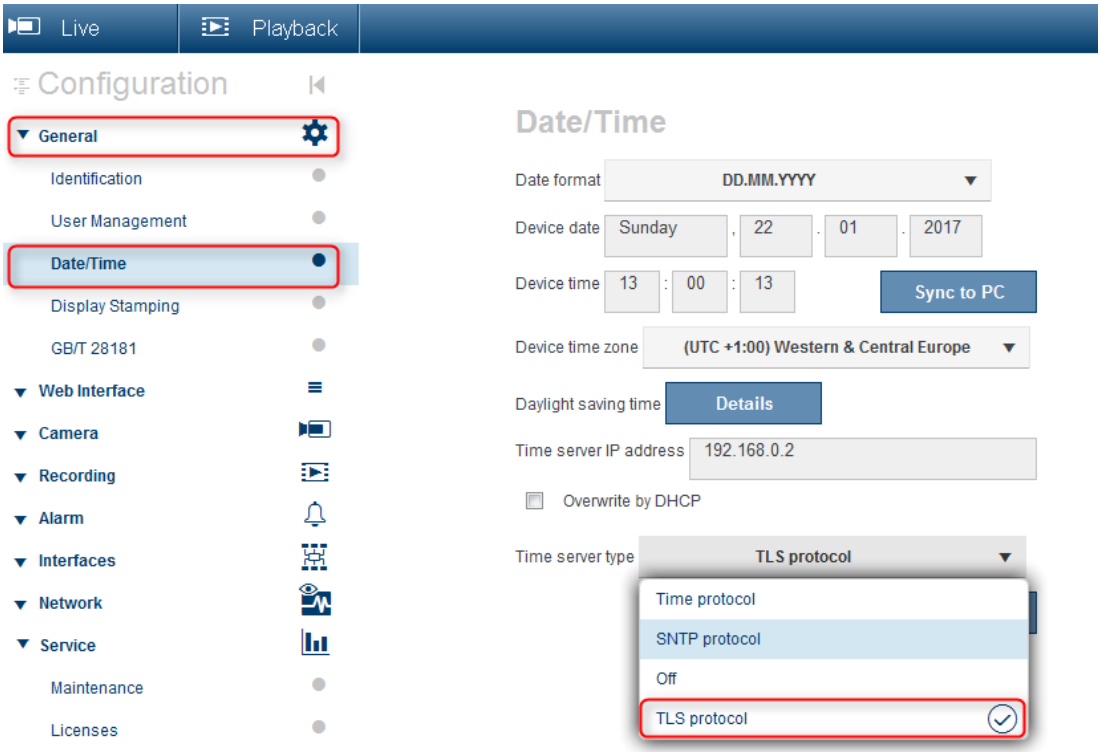
Existen tres versiones distintas del protocolo SNMP:
– SNMP versión 1
  SNMP version 1 (SNMPv1) es la implementación inicial del protocolo SNMP. Se utiliza de forma generalizada y se ha convertido en el protocolo estándar de hecho para la gestión y monitorización de redes.
  Pero SNMPv1 se ha convertido en una amenaza debido a su carencia de características de seguridad. Solo utiliza *cadenas de la comunidad* a modo de contraseñas, que se transmiten sin cifrar.
  Por consiguiente, SNMPv1 solo se puede utilizar cuando se puede garantizar que la red está protegida físicamente frente a accesos no autorizados.

– SNMP versión 2
  SNMP versión 2 (SNMPv2) incluyó mejoras en la seguridad y la confidencialidad, entre otras, e introdujo una solicitud masiva para recuperar grandes cantidades de datos con una sola solicitud. Sin embargo, su enfoque de seguridad se consideró demasiado complejo, lo cual obstaculizó su aceptación.
  Por este motivo, pronto se vio desplazada por la versión SNMPv2c, que es como SNMPv2 pero sin su controvertido modelo de seguridad y, por consiguiente, con el mismo método basado en la comunidad de SNMPv1 y con su misma falta de seguridad.
– SNMP versión 3
  SNMP versión 3 (SNMPv3) añade, principalmente, mejoras en la seguridad y en la configuración remota. Entre ellas figuran mejoras en la confidencialidad mediante el cifrado de paquetes, la integridad de mensajes y la autenticación de mensajes.
  También aborda la implementación de SNMP a gran escala.

Nota!
Consejo de seguridad de datos n.º 12
Tanto SNMPv1 como SNMPv2c se han visto amenazados debido a su falta de características de seguridad. Solo utilizan "cadenas de la comunidad" a modo de contraseñas, y estas se transmiten sin cifrar.
Por este motivo, SNMPv1 y SNMPv2c solo se deben utilizar cuando se puede garantizar que la red está protegida físicamente frente a accesos no autorizados.
Hasta la fecha, las cámaras de Bosch solo admiten SNMPv1. Si no va a utilizar SNMP, asegúrese de desactivarlo.

5.2 Base de tiempo segura

Además del protocolo de tiempo y SNTP, que son dos protocolos sin protección, a partir del firmware versión 6.20 se ha introducido un tercer modo para el cliente del servidor de tiempo utilizando el protocolo TLS. Este método también se conoce habitualmente como *TLS-Date*.
En este modo, cualquier servidor HTTPS arbitrario se puede utilizar como servidor de tiempo. El valor de tiempo se deriva del proceso de establecimiento de conexión de HTTPS. La transmisión está protegida mediante TLS. Se puede cargar un certificado raíz para el servidor HTTPS en el almacén de certificados de la cámara con el fin de autenticar el servidor.



Nota!
Consejo de seguridad de datos n.º 13
Asegúrese de que la propia dirección IP del servidor de tiempo configurada tenga una base de tiempo protegida.

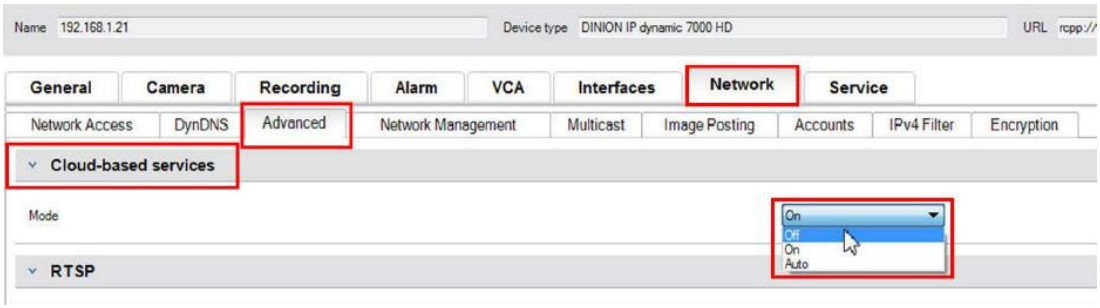
5.3 Servicios basados en la nube

Todos los dispositivos de vídeo IP de Bosch se pueden comunicar con **Servicios basados en la nube** de Bosch. Según la región de implementación, esto permite a los dispositivos de vídeo IP reenviar las alarmas y otros datos a una estación central.
Existen tres modos de funcionamiento de **Servicios basados en la nube**:

- **On** (activado):
  El dispositivo de vídeo sondeará continuamente el servidor en la nube.
- **Auto** (predeterminado):
  Los dispositivos de vídeo tratarán de sondear el servidor en la nube unas cuantas veces y, si no lo consiguen, dejarán de tratar de alcanzar el servidor en la nube.
- **Off** (desactivado):
  No se realiza ningún sondeo.

Servicios basados en la nube se pueden desactivar fácilmente utilizando Configuration Manager.

1. En Configuration Manager, seleccione el dispositivo deseado.
2. Seleccione la ficha **Red** y, a continuación, seleccione **Avanzado**.
3. Busque la parte **Servicios basados en la nube** de la página.
4. En el menú desplegable, seleccione **Off** (Desactivado).



Nota!

Consejo de seguridad de datos n.º 14

Si va a utilizar **Servicios basados en la nube** de Bosch, mantenga la configuración predeterminada.

En todos los demás casos, configure el modo **Servicios basados en la nube** en **Off** (Desactivado).

6 Reforzar la seguridad del almacenamiento

Las unidades de almacenamiento iSCSI se deben instalar en el área segura. El acceso al área segura se debe proteger mediante un sistema de control de acceso y se debe monitorizar. El grupo de usuarios que tenga acceso a la sala central de servidores debe estar limitado a un pequeño grupo de personas.

Puesto que las cámaras IP o los codificadores de Bosch son capaces de establecer una sesión iSCSI directamente con una unidad iSCSI y escribir datos de vídeo en una unidad iSCSI, las unidades iSCSI deben estar conectadas a la misma LAN o WAN que los dispositivos periféricos de Bosch.

Para evitar accesos no autorizados a los datos de vídeo grabados, las unidades iSCSI deben estar protegidas frente a accesos no autorizados:

- De forma predeterminada, las unidades iSCSI conceden a todos los iniciadores de iSCSI el acceso a los LUN iSCSI. Para garantizar que solo los componentes de la solución de gestión de vídeo de Bosch (cámaras, codificadores, estaciones de trabajo y servidores) tengan permiso de acceso a los LUN iSCSI, se puede desactivar la asignación predeterminada de LUN.

  Para permitir a los dispositivos el acceso a destinos iSCSI de un Bosch Video Management System, los nombres cualificados de iSCSI (IQN) de todos los componentes del Bosch Video Management System deben estar configurados en todos los destinos iSCSI. Esto supone un esfuerzo durante la instalación, pero minimiza el riesgo de que se pierdan, fuguen o manipulen los datos de vídeo.
- Utilice la autenticación con contraseña mediante CHAP para garantizar que solo los dispositivos conocidos tengan permiso para acceder al destino iSCSI. Configure una contraseña CHAP en el destino iSCSI e introduzca la contraseña configurada en la configuración de VRM. La contraseña CHAP es válida para VRM y se envía a todos los dispositivos automáticamente. Si se utiliza una contraseña CHAP en un entorno de Bosch Video Management System VRM, es necesario configurar la misma contraseña en todos los sistemas de almacenamiento.
- Quite todos los nombres de usuario y contraseñas predeterminados en el destino iSCSI.
- Utilice contraseñas seguras para las cuentas de usuario administrativas del destino iSCSI.
- Desactive el acceso de administración mediante Telnet al destino iSCSI. Utilice el acceso mediante SSH en su lugar.
- Proteja el acceso mediante consola al destino iSCSI utilizando una contraseña segura.
- Desactive las tarjetas de interfaz de red que no se utilicen.
- Monitorice el estado del sistema de los almacenamientos iSCSI mediante herramientas de terceros para identificar anomalías.

7 Reforzar la seguridad de los servidores

7.1 Servidores Windows

Todos los componentes de servidor como Bosch VMS Management Server y el servidor de Video Recording Manager se deben colocar en una zona segura. El acceso al área segura se debe proteger mediante un sistema de control de acceso y se debe monitorizar. El grupo de usuarios que tenga acceso a la sala central de servidores debe estar limitado a un pequeño grupo de personas.
Aunque el hardware del servidor esté instalado en una zona segura, es necesario proteger el hardware frente a accesos no autorizados.

7.1.1 Configuración recomendada del hardware de servidor

– La BIOS del servidor permite configurar contraseñas de bajo nivel.
  Estas contraseñas permiten limitar la capacidad de la gente para reiniciar el ordenador, reiniciar desde dispositivos extraíbles y cambiar la configuración de la BIOS o la UEFI (Unified Extensible Firmware Interface) sin permiso.
– Para evitar la transferencia de datos al servidor, se deben desactivar los puertos USB y la unidad de CD/DVD.
  Además, los puertos NIC no utilizados se deben desactivar y los puertos de gestión, como los puertos de la interfaz HP ILO (HP Integrated Lights Out) o de consola se deben desactivar o proteger con contraseña.

7.1.2 Configuración de seguridad recomendada en sistema operativo Windows

Los servidores deben formar parte de un dominio de Windows.
Con la integración de los servidores en un dominio de Windows, los permisos de usuario se asignan a usuarios de red gestionados por un servidor central. Puesto que, a menudo, estas cuentas de usuario implementan reglas sobre la seguridad y la caducidad de las contraseñas, esta integración puede ser más segura que con cuentas locales que no tengan estas restricciones.

7.1.3 Actualizaciones de Windows

Los parches de software y las actualizaciones de Windows se deben instalar y mantener al día. A menudo, las actualizaciones de Windows contienen parches frente a vulnerabilidades de seguridad recién descubiertas, como la vulnerabilidad de latido SSL, que afectó a millones de ordenadores en todo el mundo. Es necesario instalar los parches para estos problemas importantes.

7.1.4 Instalación de software antivirus

Instale software antivirus y antispyware y manténgalo al día.

7.1.5 Configuración recomendada en sistema operativo Windows

La configuración de directivas de grupos locales siguiente es recomendada para entornos con grupos en un sistema operativo Windows Server. Para cambiar las directivas de grupos locales (LCP), utilice el editor de directivas de grupos locales.
Es posible acceder al editor de directivas de grupos locales utilizando la línea de comando o la consola de administración de Microsoft (MMC).

Para abrir el editor de directivas de grupos locales desde la línea de comandos:

- Haga clic en **Inicio**. En el cuadro de búsqueda de **Inicio**, escriba **gpedit.msc** y pulse Intro.

Para abrir el editor de directivas de grupos locales como complemento de MMC:

1. Haga clic en **Inicio**. En el cuadro de búsqueda **Inicio**, escriba **mmc** y pulse Intro.
2. En el cuadro de diálogo **Añadir o quitar complementos**, haga clic en **Editor de objetos de directiva de grupo** y, a continuación, en **Agregar**.
3. En el cuadro de diálogo **Seleccionar objeto de directiva de grupo**, haga clic en **Examinar**.
4. Haga clic en **Equipo** para editar el objeto de directiva de grupo local o haga clic en **Usuarios** para editar los objetos de directiva de grupo de administrador, no administrador o por usuario.
5. Haga clic en **Finalizar**.

7.1.6 Activar el control de cuentas de usuario en el servidor

LCP -> Configuración del equipo -> Configuración de Windows -> Configuración de seguridad -> Directivas locales -> Opciones de seguridad

Control de cuentas de usuario: Modo de aprobación del administrador para la cuenta de Administrador integrada	Activada
Control de cuentas de usuario: Permitir a las aplicaciones UIAccess solicitar la elevación sin utilizar el escritorio seguro	Desactivada
Control de cuentas de usuario: Comportamiento de la solicitud de elevación para administradores de Modo de aprobación de administrador	Solicitar confirmación
Control de cuentas de usuario: Comportamiento de la solicitud de elevación para usuarios estándar	Solicitar credenciales en el escritorio seguro
Control de cuentas de usuario: Detectar instalaciones de aplicaciones y solicitar elevación	Activada
Control de cuentas de usuario: Elevar solo ejecutables firmados y validados	Desactivada
Control de cuentas de usuario: Ejecutar todos los administradores en Modo de aprobación de administrador	Activada
Control de cuentas de usuario: Cambiar al escritorio seguro al solicitar la elevación	Activada
Control de cuentas de usuario: Virtualizar los fallos de escritura de archivos y registros a las ubicaciones de los usuarios	Activada

LCP -> Configuración del equipo -> Plantillas de administración -> Componentes de Windows -> Interfaz de usuario de credenciales

Enumerar las cuentas de administración al elevar	Desactivada

7.1.7 Desactivar la reproducción automática

LCP -> Configuración del equipo -> Plantillas de administración -> Componentes de Windows -> Directivas de reproducción automática

Desactivar la reproducción automática	Todas las unidades activadas

Comportamiento predeterminado de la reproducción automática	Activado, no ejecutar ningún comando de ejecución automática
Desactivar la reproducción automática para los dispositivos que no sean volúmenes	Activada

7.1.8 Dispositivos externos

LCP -> Configuración del equipo -> Configuración de Windows -> Configuración de seguridad -> Directivas locales -> Opciones de seguridad

Dispositivos: Permitir la desconexión sin tener que iniciar sesión	Desactivada
Dispositivos: Permiso para formatear y eyectar soportes extraíbles	Administradores
Dispositivos: Evitar que los usuarios pueden instalar controladores de impresoras	Activada
Dispositivos: Limitar el acceso al CD-ROM solo a usuarios con sesión iniciada localmente	Activada
Dispositivos: Limitar el acceso a la disquetera solo a usuarios con sesión iniciada localmente	Activada

7.1.9 Configuración de la asignación de derechos de usuario

LCP -> Configuración del equipo -> Configuración de Windows -> Configuración de seguridad -> Directivas locales -> Asignación de derechos de usuario

Acceder a Credential Manager como llamante de confianza	Nadie
Acceder a este equipo desde la red	Usuarios autenticados
Actuar como parte del sistema operativo	Nadie
Añadir estaciones de trabajo al dominio	Nadie
Permitir el inicio de sesión mediante Remote Desktop Services	Administradores, usuarios de Remote Desktop
Hacer copias de seguridad de archivos y directorios	Administradores
Cambiar la hora del sistema	Administradores
Cambiar la zona horaria del sistema	Administradores, servicio local
Crear un archivo de página	Administradores
Crear un objeto de token	Nadie
Crear objetos compartidos permanentes	Nadie
Depurar programas	Nadie
Denegar el acceso a este equipo desde la red	Inicio de sesión anónimo, invitado
Denegar el inicio de sesión como tarea por lotes	Inicio de sesión anónimo, invitado

Denegar el inicio de sesión como servicio	Nadie
Denegar el inicio de sesión local	Inicio de sesión anónimo, invitado
Denegar el inicio de sesión mediante Remote Desktop Services	Inicio de sesión anónimo, invitado
Permitir que se confíe en cuentas del equipo y de usuario con fines de delegación	Nadie
Forzar el apagado desde un sistema remoto	Administradores
Generar auditorías de seguridad	Servicio local, servicio de red
Aumentar la prioridad de programación	Administradores
Cargar y desactivar controladores de dispositivos	Administradores
Gestionar el registro de auditoría y de seguridad	Administradores
Modificar la etiqueta de un objeto	Nadie
Modificar los valores de entorno del firmware	Administradores
Realizar tareas de mantenimiento en volúmenes	Administradores
Realizar perfil de un proceso único	Administradores
Realizar perfil del funcionamiento del sistema	Administradores
Quitar el ordenador de la base	Administradores
Restablecer archivos y directorios	Administradores
Apagar el sistema	Administradores
Sincronizar datos de servicio de directorios	Nadie
Asumir la propiedad de archivos u otros objetos	Administradores

7.1.10 Protector de pantalla

– Activar el protector de pantalla protegido por contraseña y definir el tiempo de espera: **LCP -> Configuración del usuario -> Plantillas de administración -> Panel de control -> Personalización**

Activar el protector de pantalla	Activada
Proteger el protector de pantalla con contraseña	Activada
Tiempo de espera del protector de pantalla	1800 segundos

7.1.11 Activar la configuración de directiva de contraseña

– Activar la configuración de directivas de contraseñas garantiza que las contraseñas de los usuarios cumplan unos requisitos mínimos

LCP -> Configuración de Windows -> Configuración de seguridad -> Directivas de cuentas -> Directiva de contraseñas

Aplicar el historial de contraseñas	Se recuerdan 10 contraseñas

Antigüedad máxima de la contraseña	90 días
Antigüedad mínima de la contraseña	1 día
Longitud mínima de la contraseña	10 caracteres
La contraseña debe cumplir requisitos de complejidad	Activada
Almacenar la contraseña utilizando cifrado reversible para todos los usuarios del dominio	Desactivada

7.1.12 Desactivar los servicios de Windows no esenciales

– Desactivar los servicios de Windows no esenciales permite un nivel de seguridad mayor y minimiza los puntos de ataque.

Servicio de puerta de acceso a la capa de aplicaciones	Desactivada
Gestión de aplicaciones	Desactivada
Explorador del equipo	Desactivada
Cliente de seguimiento de vínculos distribuidos	Desactivada
Host de proveedor de detección de función	Desactivada
Publicación de recurso de detección de función	Desactivada
Acceso a dispositivos de interfaz humana	Desactivada
Uso compartido de la conexión a Internet (ICS)	Desactivada
Asignación de detección de topologías de nivel de vínculo	Desactivada
Programador de aplicaciones multimedia	Desactivada
Archivos sin conexión	Desactivada
Administrador de conexión automática de acceso remoto	Desactivada
Administrador de conexión de acceso remoto	Desactivada
Enrutamiento y acceso remoto	Desactivada
Detección de hardware shell	Desactivada
Ayudante especial de la consola de administración	Desactivada
Detección SSDP	Desactivada
Audio de Windows	Desactivada
Compilador de extremo de audio de Windows	Desactivada

7.1.13 Cuentas de usuario del sistema operativo Windows

Es necesario proteger las cuentas del sistema operativo Windows con contraseñas complejas. Por lo general, los servidores de gestionan y mantienen mediante cuentas de administración de Windows. Por consiguiente, es necesario asegurarse de que estas cuentas utilicen contraseñas seguras.

Las contraseñas deben contener caracteres de tres de las categorías siguientes:

- Letras mayúsculas de los idiomas europeos (de la A a la Z, con acentos diacríticos, caracteres griegos y cirílicos)
- Letras minúsculas de los idiomas europeos (de la a a la z, Eszett, con acentos diacríticos, caracteres griegos y cirílicos)
- Dígitos en base 10 (del 0 al 9)
- Caracteres o alfanuméricos: ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/
- Cualquier carácter Unicode categorizado como alfabético que no sea mayúsculo ni minúsculo. Esto incluye los caracteres Unicode de los idiomas asiáticos.

Utilice el bloqueo de cuentas de Windows para que resulte más difícil que los ataques por adivinación de la contraseña tengan éxito.
La recomendación de la seguridad básica de Windows 8.1 era, a fecha de 15/10/15:

- 10 intentos fallidos
- 15 minutos de bloqueo
- Restablecimiento de la cuenta al cabo de 15 minutos

LCP -> Configuración del equipo -> Configuración de Windows -> Configuración de seguridad -> Directivas de cuentas -> Directiva de bloqueo de cuentas

Duración del bloqueo de la cuenta	Duración del bloqueo de la cuenta
Bloqueo de cuenta durante 15 minutos con un umbral de 10 intentos fallidos de inicio de sesión	Bloqueo de cuenta durante 15 minutos con un umbral de 10 intentos fallidos de inicio de sesión
Restablecer el contador de bloqueo de la cuenta después de	Restablecer el contador de bloqueo de la cuenta después de

- Asegúrese de que todas las contraseñas del servidor y el sistema operativo Windows se sustituyan por contraseñas seguras.

7.1.14 Activar el firewall en el servidor

- Active la comunicación del puerto estándar de Bosch VMS conforme a los puertos de Bosch VMS.

Nota!
Consejo de seguridad de datos n.º 15
Consulte la información relevante sobre la configuración y el uso de puertos en la documentación de instalación y del usuario de Bosch VMS. Asegúrese de volver a comprobar la configuración cuando se actualice el software o el firmware.

8 Reforzar la seguridad de los clientes

8.1 Estaciones de trabajo Windows

Los sistemas operativos de escritorio Windows que se utilizan para las aplicaciones clientes de Bosch VMS como Bosch VMS Operator Client o Configuration Client están instalados fuera del área segura. Es necesario reforzar las estaciones de trabajo para proteger los datos de vídeo, los documentos y otras aplicaciones frente al acceso no autorizado.
Es necesario aplicar o comprobar los ajustes siguientes.

8.1.1 Configuración recomendada del hardware de las estaciones de trabajo Windows

- Configure una contraseña de BIOS/UEFI para evitar que alguien pueda arrancar con sistemas operativos alternativos.
- Para evitar la transferencia de datos al cliente, se deben desactivar los puertos USB y la unidad de CD/DVD. También se deben desactivar los puertos NIC que no se utilicen.

8.1.2 Configuración de seguridad recomendada en sistema operativo Windows

- La estación de trabajo debe formar parte de un dominio de Windows.
  La integración de la estación de trabajo en un dominio de Windows permite gestionar ajustes de configuración importantes de forma centralizada.
- Actualizaciones de Windows
  Manténgase al día de los parches y las actualizaciones del sistema operativo Windows.
- Instalación de software antivirus
  Instale software antivirus y antispyware y manténgalo al día.

8.1.3 Configuración recomendada en sistema operativo Windows

La configuración de directivas de grupos locales siguiente es recomendada para entornos con grupos en un sistema operativo Windows Server. Para cambiar las directivas de grupos locales (LCP), utilice el editor de directivas de grupos locales.
Es posible acceder al editor de directivas de grupos locales utilizando la línea de comando o la consola de administración de Microsoft (MMC).

Para abrir el editor de directivas de grupos locales desde la línea de comandos:

- Haga clic en **Inicio**. En el cuadro de búsqueda de **Inicio**, escriba **gpedit.msc** y pulse Intro.

Para abrir el editor de directivas de grupos locales como complemento de MMC:

1. Haga clic en **Inicio**. En el cuadro de búsqueda **Inicio**, escriba **mmc** y pulse Intro.
2. En el cuadro de diálogo **Añadir o quitar complementos**, haga clic en **Editor de objetos de directiva de grupo** y, a continuación, en **Agregar**.
3. En el cuadro de diálogo **Seleccionar objeto de directiva de grupo**, haga clic en **Examinar**.
4. Haga clic en **Equipo** para editar el objeto de directiva de grupo local o haga clic en **Usuarios** para editar los objetos de directiva de grupo de administrador, no administrador o por usuario.
5. Haga clic en **Finalizar**.

8.1.4 Activar el control de cuentas de usuario en el servidor

LCP -> Configuración del equipo -> Configuración de Windows -> Configuración de seguridad -> Directivas locales -> Opciones de seguridad

Control de cuentas de usuario: Modo de aprobación del administrador para la cuenta de Administrador integrada	Activada

Control de cuentas de usuario: Permitir a las aplicaciones UIAccess solicitar la elevación sin utilizar el escritorio seguro	Desactivada
Control de cuentas de usuario: Comportamiento de la solicitud de elevación para administradores de Modo de aprobación de administrador	Solicitar confirmación
Control de cuentas de usuario: Comportamiento de la solicitud de elevación para usuarios estándar	Solicitar credenciales en el escritorio seguro
Control de cuentas de usuario: Detectar instalaciones de aplicaciones y solicitar elevación	Activada
Control de cuentas de usuario: Elevar solo ejecutables firmados y validados	Desactivada
Control de cuentas de usuario: Ejecutar todos los administradores en Modo de aprobación de administrador	Activada
Control de cuentas de usuario: Cambiar al escritorio seguro al solicitar la elevación	Activada
Control de cuentas de usuario: Virtualizar los fallos de escritura de archivos y registros a las ubicaciones de los usuarios	Activada

LCP -> Configuración del equipo -> Plantillas de administración -> Componentes de Windows -> Interfaz de usuario de credenciales

Enumerar las cuentas de administración al elevar	Desactivada

8.1.5 Desactivar la reproducción automática

LCP -> Configuración del equipo -> Plantillas de administración -> Componentes de Windows -> Directivas de reproducción automática

Desactivar la reproducción automática	Todas las unidades activadas
Comportamiento predeterminado de la reproducción automática	Activado, no ejecutar ningún comando de ejecución automática
Desactivar la reproducción automática para los dispositivos que no sean volúmenes	Activada

8.1.6 Dispositivos externos

LCP -> Configuración del equipo -> Configuración de Windows -> Configuración de seguridad -> Directivas locales -> Opciones de seguridad

Dispositivos: Permitir la desconexión sin tener que iniciar sesión	Desactivada
Dispositivos: Permiso para formatear y eyectar soportes extraíbles	Administradores
Dispositivos: Evitar que los usuarios pueden instalar controladores de impresoras	Activada

Dispositivos: Limitar el acceso al CD-ROM solo a usuarios con sesión iniciada localmente	Activada
Dispositivos: Limitar el acceso a la disquetera solo a usuarios con sesión iniciada localmente	Activada

8.1.7 Configuración de la asignación de derechos de usuario

LCP -> Configuración del equipo -> Configuración de Windows -> Configuración de seguridad -> Directivas locales -> Asignación de derechos de usuario

Acceder a Credential Manager como llamante de confianza	Nadie
Acceder a este equipo desde la red	Usuarios autenticados
Actuar como parte del sistema operativo	Nadie
Añadir estaciones de trabajo al dominio	Nadie
Permitir el inicio de sesión mediante Remote Desktop Services	Administradores, usuarios de Remote Desktop
Hacer copias de seguridad de archivos y directorios	Administradores
Cambiar la hora del sistema	Administradores
Cambiar la zona horaria del sistema	Administradores, servicio local
Crear un archivo de página	Administradores
Crear un objeto de token	Nadie
Crear objetos compartidos permanentes	Nadie
Depurar programas	Nadie
Denegar el acceso a este equipo desde la red	Inicio de sesión anónimo, invitado
Denegar el inicio de sesión como tarea por lotes	Inicio de sesión anónimo, invitado
Denegar el inicio de sesión como servicio	Nadie
Denegar el inicio de sesión local	Inicio de sesión anónimo, invitado
Denegar el inicio de sesión mediante Remote Desktop Services	Inicio de sesión anónimo, invitado
Permitir que se confíe en cuentas del equipo y de usuario con fines de delegación	Nadie
Forzar el apagado desde un sistema remoto	Administradores
Generar auditorías de seguridad	Servicio local, servicio de red
Aumentar la prioridad de programación	Administradores
Cargar y desactivar controladores de dispositivos	Administradores

Gestionar el registro de auditoría y de seguridad	Administradores
Modificar la etiqueta de un objeto	Nadie
Modificar los valores de entorno del firmware	Administradores
Realizar tareas de mantenimiento en volúmenes	Administradores
Realizar perfil de un proceso único	Administradores
Realizar perfil del funcionamiento del sistema	Administradores
Quitar el ordenador de la base	Administradores
Restablecer archivos y directorios	Administradores
Apagar el sistema	Administradores
Sincronizar datos de servicio de directorios	Nadie
Asumir la propiedad de archivos u otros objetos	Administradores

8.1.8 Protector de pantalla

– Activar el protector de pantalla protegido por contraseña y definir el tiempo de espera:
LCP -> Configuración del usuario -> Plantillas de administración -> Panel de control -> Personalización

Activar el protector de pantalla	Activada
Proteger el protector de pantalla con contraseña	Activada
Tiempo de espera del protector de pantalla	1800 segundos

8.1.9 Activar la configuración de directiva de contraseña

– Activar la configuración de directivas de contraseñas garantiza que las contraseñas de los usuarios cumplan unos requisitos mínimos

LCP -> Configuración de Windows -> Configuración de seguridad -> Directivas de cuentas -> Directiva de contraseñas

Aplicar el historial de contraseñas	Se recuerdan 10 contraseñas
Antigüedad máxima de la contraseña	90 días
Antigüedad mínima de la contraseña	1 día
Longitud mínima de la contraseña	10 caracteres
La contraseña debe cumplir requisitos de complejidad	Activada
Almacenar la contraseña utilizando cifrado reversible para todos los usuarios del dominio	Desactivada

8.1.10 Desactivar los servicios de Windows no esenciales

– Desactivar los servicios de Windows no esenciales permite un nivel de seguridad mayor y minimiza los puntos de ataque.

Servicio de puerta de acceso a la capa de aplicaciones	Desactivada
Gestión de aplicaciones	Desactivada
Explorador del equipo	Desactivada

Cliente de seguimiento de vínculos distribuidos	Desactivada
Host de proveedor de detección de función	Desactivada
Publicación de recurso de detección de función	Desactivada
Acceso a dispositivos de interfaz humana	Desactivada
Uso compartido de la conexión a Internet (ICS)	Desactivada
Asignación de detección de topologías de nivel de vínculo	Desactivada
Programador de aplicaciones multimedia	Desactivada
Archivos sin conexión	Desactivada
Administrador de conexión automática de acceso remoto	Desactivada
Administrador de conexión de acceso remoto	Desactivada
Enrutamiento y acceso remoto	Desactivada
Detección de hardware shell	Desactivada
Ayudante especial de la consola de administración	Desactivada
Detección SSDP	Desactivada
Audio de Windows	Desactivada
Compilador de extremo de audio de Windows	Desactivada

8.1.11 Cuentas de usuario del sistema operativo Windows

Es necesario proteger las cuentas del sistema operativo Windows con contraseñas complejas. Por lo general, los servidores de gestionan y mantienen mediante cuentas de administración de Windows. Por consiguiente, es necesario asegurarse de que estas cuentas utilicen contraseñas seguras.

Las contraseñas deben contener caracteres de tres de las categorías siguientes:
- Letras mayúsculas de los idiomas europeos (de la A a la Z, con acentos diacríticos, caracteres griegos y cirílicos)
- Letras minúsculas de los idiomas europeos (de la a a la z, Eszett, con acentos diacríticos, caracteres griegos y cirílicos)
- Dígitos en base 10 (del 0 al 9)
- Caracteres o alfanuméricos: ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/
- Cualquier carácter Unicode categorizado como alfabético que no sea mayúsculo ni minúsculo. Esto incluye los caracteres Unicode de los idiomas asiáticos.

Utilice el bloqueo de cuentas de Windows para que resulte más difícil que los ataques por adivinación de la contraseña tengan éxito.
La recomendación de la seguridad básica de Windows 8.1 era, a fecha de 15/10/15:
- 10 intentos fallidos
- 15 minutos de bloqueo
- Restablecimiento de la cuenta al cabo de 15 minutos

LCP -> Configuración del equipo -> Configuración de Windows -> Configuración de seguridad -> Directivas de cuentas -> Directiva de bloqueo de cuentas

Duración del bloqueo de la cuenta	Duración del bloqueo de la cuenta
Bloqueo de cuenta durante 15 minutos con un umbral de 10 intentos fallidos de inicio de sesión	Bloqueo de cuenta durante 15 minutos con un umbral de 10 intentos fallidos de inicio de sesión
Restablecer el contador de bloqueo de la cuenta después de	Restablecer el contador de bloqueo de la cuenta después de

- Asegúrese de que todas las contraseñas del servidor y el sistema operativo Windows se sustituyan por contraseñas seguras.
- Desactive las cuentas del sistema operativo Windows que no se utilicen.
- Desactive el acceso mediante Remote Desktop a la estación de trabajo cliente.
- Haga funcionar la estación de trabajo sin derechos de administración para evitar que un usuario estándar cambie la configuración del sistema.

8.1.12 Activar el firewall en la estación de trabajo

▸ Active la comunicación del puerto estándar de Bosch VMS conforme a los puertos de Bosch VMS.

Nota!

Consejo de seguridad de datos n.º 16

Consulte la información relevante sobre la configuración y el uso de puertos en la documentación de instalación y del usuario de Bosch VMS. Asegúrese de volver a comprobar la configuración cuando se actualice el software o el firmware.

9 Proteger el acceso a la red

Actualmente, muchos sistemas de videovigilancia IP de tamaño pequeño o mediano se implementan en la infraestructura de red del cliente "como cualquier otra aplicación de TI". Aunque esto tiene ventajas en términos de coste y mantenimiento, este tipo de implementación también expone el sistema de seguridad a amenazas indeseadas, incluidas las internas. Es necesario aplicar medidas adecuadas y evitar situaciones como que el vídeo se fugue hacia Internet o redes sociales. Un evento de este tipo no solo podría infringir la privacidad, sino también perjudicar la empresa.

Existen dos técnicas principales para crear una red dentro de una red. La que elijan los arquitectos de las infraestructuras de TI depende en gran manera de la infraestructura de red existente, los equipos de red implementados y las capacidades necesarias y la topología de la red.

9.1 VLAN: LAN virtual

Una LAN virtual se crea subdividiendo una LAN en varios segmentos. La segmentación de la red se consigue mediante la configuración de un switch o router de red. La ventaja de la VLAN es que es posible abordar las necesidades de recursos sin tener que cambiar el cableado de las conexiones de red.
Las fórmulas de calidad del servicio aplicadas a ciertos segmentos, como para videovigilancia, pueden ayudar a mejorar tanto la seguridad como el rendimiento.

Las VLAN se implementan sobre la capa de vínculos de datos (capa OSI 2) y son análogas a las subredes IP (consulte *Asignar direcciones IP, Página 7*), que son similares pero sobre capas de red (capa OSI 3).

9.2 VPN: Red privada virtual

Una red privada virtual es una red aparte (privada) que, a menudo, se extiende sobre redes públicas o Internet. Para crear una VPN existen varios protocolos. Por lo general, se utiliza un túnel que transporta el tráfico protegido. Las redes privadas virtuales se pueden diseñar como túneles punto a punto, conexiones de todos con todos o conexiones multipunto. Las VPN se pueden implementar con comunicaciones cifradas o confiar en la comunicación segura dentro de la propia VPN.

Las VPN se pueden utilizar para conectar sitios remotos mediante conexiones de red de gran área (WAN) a la vez que se protege y aumenta la seguridad dentro de una red de área local (LAN). Puesto que una VPN actúa como una red aparte, todos los dispositivos que se añaden a la VPN funcionan, de forma transparente, como si estuviesen en una red típica. Una VPN no solo añade una capa de protección adicional a un sistema de vigilancia. Además, proporciona la ventaja adicional de segmentar el tráfico de negocio y de vídeo en las redes de producción.

Nota!
Consejo de seguridad de datos n.º 17
Si es posible utilizarla, la VLAN o VPN aumenta el nivel de seguridad del sistema de vigilancia combinado con una infraestructura de TI existente.

Además de proteger el sistema de vigilancia de accesos no autorizados en infraestructuras de TI compartidas, es necesario tener en cuenta a quién se permite la conexión a la red en absoluto.

9.3 Desactivar los puertos de switch no utilizados

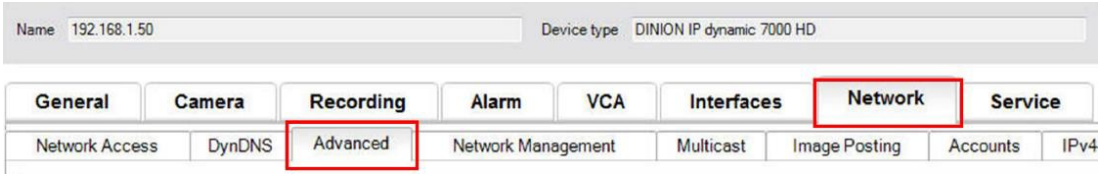
Desactivar los puertos de red no utilizados garantiza que dispositivos no autorizados no puedan acceder a la red. Esto mitiga el riesgo de que alguien trate de acceder a una subred de seguridad conectando su dispositivo en un switch o un socket de red que o se utiliza. La opción de desactivar ciertos puertos es habitual en los switches gestionados, tanto de bajo coste como empresariales.

9.4 Redes protegidas con 802.1x

Todos los dispositivos de vídeo IP de Bosch se pueden configurar como clientes 802.1x. Esto les permite autenticarse con un servidor RADIUS y participar en una red protegida. Antes de colocar los dispositivos en la red protegida, es necesario conectarse directamente a cada dispositivo de vídeo desde un portátil de un técnico para introducir las credenciales válidas tal como se describe en detalle en los pasos siguientes.

Los servicios 802.1x se pueden configurar fácilmente mediante Configuration Manager.

1. En Configuration Manager, seleccione el dispositivo deseado.
2. Seleccione la ficha **Red** y, a continuación, seleccione **Avanzado**.



3. Busque la parte **802.1x** de la página.
4. En el menú desplegable **802.1x**, seleccione **On** (Activado).
5. Introduzca valores de **Identidad** y **Contraseña válidos.**
6. Guarde los cambios.
7. Desconecte y coloque los dispositivos en la red protegida.

Nota!
Por sí solo, 802.1x no proporciona una comunicación segura entre el solicitante y el servidor de autenticación.
Como resultado, el nombre de usuario y la contraseña se podrían "extraer" de la red. 802.1x puede utilizar EAP-TLS para garantizar una comunicación segura.

9.4.1 Protocolo de autenticación extensible (EAP): seguridad de la capa de transporte

El protocolo de autenticación extensible (EAP) proporciona soporte para diversos métodos de autenticación. La seguridad de la capa de transporte (TLS) proporciona autenticación mutua, integridad, negociación protegida de conjuntos de cifras e intercambio de claves entre dos puntos extremos. EAP-TLS incluye el soporte para la autenticación mutua basada en certificados y la derivación de claves. En otras palabras, EAP-TLS encapsula el proceso mediante el cual el servidor y el cliente se envían un certificado del uno al otro.

Nota!
Consejo de seguridad de datos n.º 18
Consulte el artículo técnico específico "Autenticación de red - 802.1x - Proteger el límite de la red", disponible en el catálogo de productos en línea de Bosch Security Systems, dentro de: http://resource.boschsecurity.com/documents/WP_802.1x_Special_enUS_22335867275.pdf.

10 Generar confianza con certificados

Todas las cámaras IP de Bosch que ejecutan el firmware 6.10 o posterior utilizan un almacén de certificados que se puede encontrar en el menú **Servicio** de la configuración de la cámara. Es posible añadir certificados de servidor, certificados de cliente y certificados de confianza específicos al almacén.

Para añadir un certificado al almacén:

1. En la página web del dispositivo vaya a la página **Configuración**.
2. Seleccione el menú **Servicio** y el submenú**Certificados**.
3. En la sección **Lista de archivos**, haga clic en **Añadir**.
4. Cargue los certificados que desee.
   Al finalizar la carga, los certificados aparecen en la sección **Lista de uso**.
5. En la sección **Lista de uso**, seleccione el certificado que desee.
6. Para activar el uso del certificado, es necesario reiniciar la cámara. Para reiniciar la cámara, haga clic en **Establecer**.

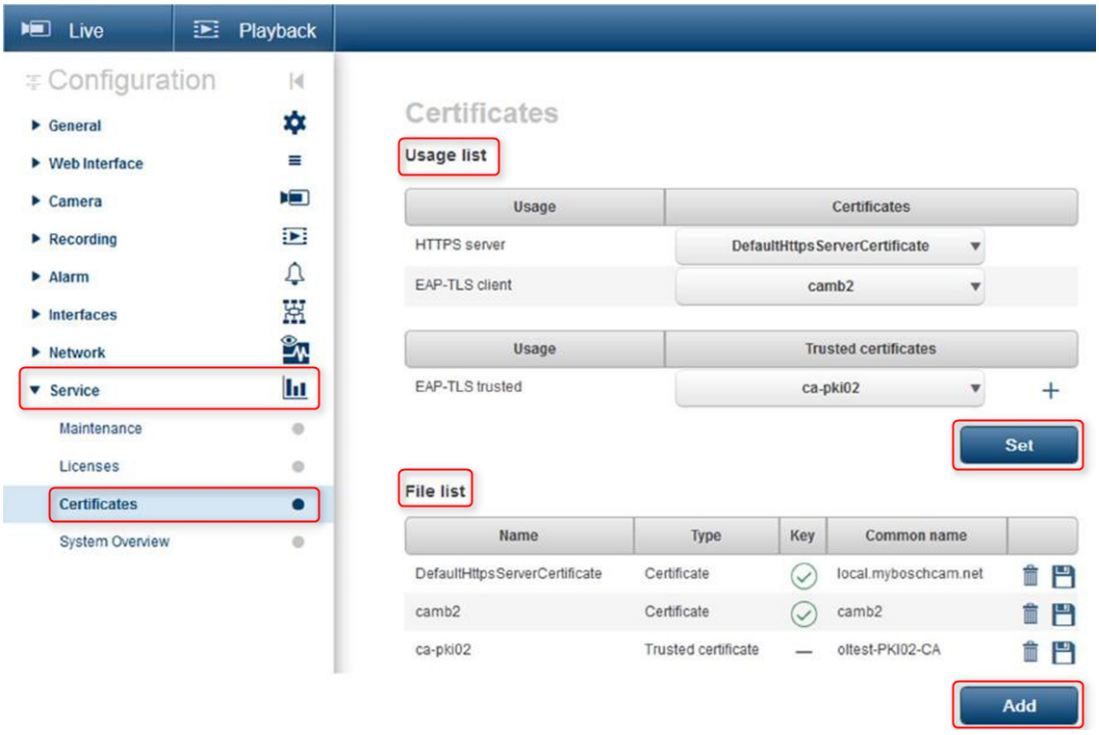


Figura 10.1: Ejemplo: los certificados EAP/TLS almacenados en una cámara Bosch (FW6.11)

10.1 Protección en una caja fuerte (módulo de plataforma de confianza)

Las claves se almacenan en un chip como los que se utilizan en las SmartCards cifradas. También se le llama módulo de plataforma de confianza o TPM. Este chip actúa como una caja fuerte para los datos críticos y protege los certificados, las claves, las licencias, etc. frente a accesos no autorizados incluso cuando se abre la cámara físicamente para acceder a ella.

Se aceptan certificados en formatos *.prm, *.cer o *.crt y codificados en base 64. Se deben cargar como un solo archivo combinado o bien se deben dividir en archivos separados con las partes de certificados y claves y cargar en este orden para recombinarlos automáticamente.

Desde la versión 6.20 del firmware, se admiten claves privadas protegidas mediante contraseña PKCS#8 (cifradas con AES). Estas se deben cargar en formato *.pem codificadas en base 64.

10.2 Certificados TLS

Todos los dispositivos de vídeo de Bosch que utilizan el firmware hasta la versión 6.1x llevan un certificado y una clave privada de TLS preinstalados que se utilizan automáticamente para las conexiones HTTPS. El certificado y la clave predeterminados sirven solo para realizar pruebas, ya que todos los dispositivos se suministran con el mismo certificado predeterminado.

Desde el firmware 6.20, se crea automáticamente un certificado TLS autofirmado específico del dispositivo cuando es necesario para establecer conexiones HTTPS, lo cual permite realizar una autenticación exclusiva. Este certificado autofirmado se puede renovar manualmente; basta con eliminarlo. El dispositivo creará uno nuevo por sí solo en cuanto sea necesario.

Si se implementan los dispositivos en un entorno donde se necesitan pasos adicionales para validar la identidad de cada dispositivo de vídeo IP específico, es posible crear nuevos certificados y claves privadas y cargarlos en cada dispositivo. Los nuevos certificados se pueden obtener de una Autoridad certificadora (CA) o se pueden crear, por ejemplo, con OpenSSL Toolkit.

10.2.1 Página web del dispositivo

Es posible cargar los certificados utilizando la página web del dispositivo de vídeo.
Es posible añadir y eliminar certificados y definir su utilización en la página **Certificados**.

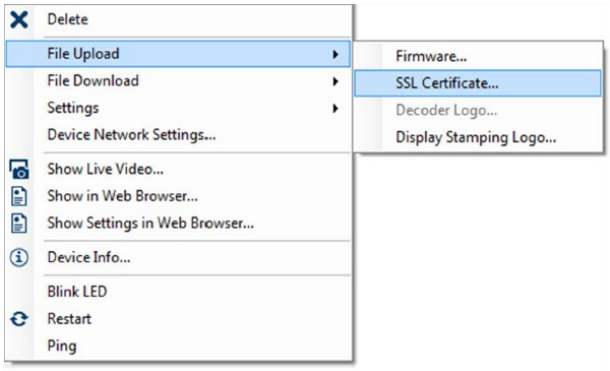
Consulte también

– *Generar confianza con certificados, Página 44*

10.2.2 Administrador de configuración

Con Configuration Manager, se pueden cargar fácilmente certificados a uno o más dispositivos a la vez.
Para cargar certificados:

1. En Configuration Manager, seleccione uno o más dispositivos.
2. Haga clic con el botón derecho del ratón y en **Carga de archivo** y, a continuación en **Certificado SSL...**.
   Se abrirá una ventana del explorador de Windows para buscar el certificado para cargar.



Nota!
Es posible cargar certificados utilizando Configuration Manager, pero solo se puede definir su utilización mediante la página web **Certificados**.

Nota!
Consejo de seguridad de datos n.º 19
Los certificados se utilizan para autenticar un solo dispositivo. Se recomienda crear un certificado específico para cada dispositivo, derivado de un certificado raíz.
Si los dispositivos se van a utilizar en redes públicas, se recomienda obtener los certificados en una Autoridad certificadora pública o firmar los propios certificados en ella, ya que también es capaz de verificar el origen y la validez (es decir, la confianza) del certificado del dispositivo.

11 Autenticación de vídeo

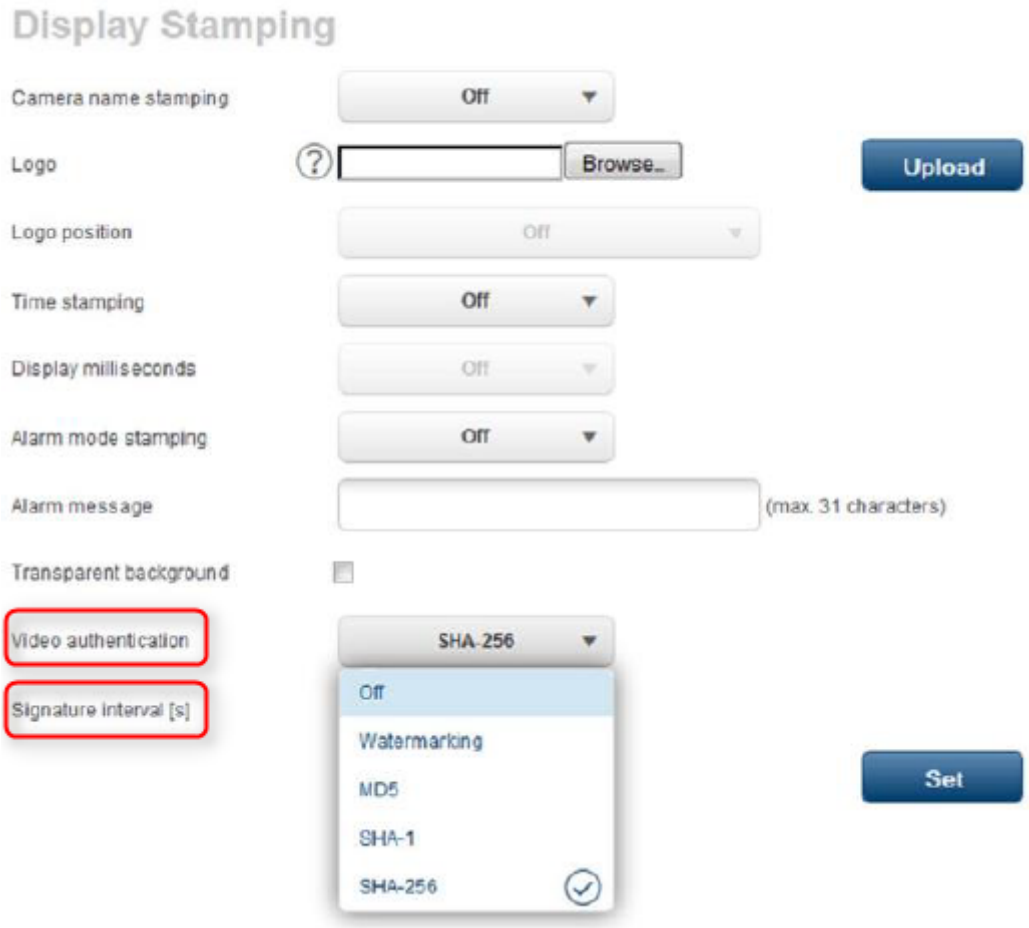
Después de proteger y autenticar correctamente los dispositivos de un sistema, también vale la pena mantener controlados los datos que proceden de ellos. Este procedimiento se denomina autenticación de vídeo.

La autenticación de vídeo solo se refiere a métodos de validación de la autenticidad de un vídeo. La autenticación de vídeo no se refiere, en ningún modo, la transmisión del vídeo ni de los datos.

Antes de la publicación de la versión 5.9 del firmware, se aplicaban marcas de agua mediante un simple algoritmo de suma de verificación sobre el flujo de vídeo. Al tratar con un marcado básico, no se utilizan certificados ni cifrado. Una suma de verificación es una medida básica de la corrección de los datos de un archivo y de la integridad del archivo.

Para configurar la autenticación de vídeo, por ejemplo en un navegador web:

1. Vaya al menú **General** y seleccione **Mostrar texto**.
2. En el menú desplegable **Autenticación de vídeo**, seleccione la opción que desee:
   Las versiones 5.9 y posteriores del firmware ofrecen tres opciones de autenticación de vídeo además de la marca de agua convencional:
   - MD5: Resumen de mensaje que genera un valor hash de 128 bits.
   - SHA-1: Diseñado por la Agencia de Seguridad Nacional de Estados Unidos, es un estándar de procesamiento de información federal de Estados Unidos publicado por el NIST de Estados Unidos. SHA-1 genera un valor hash de 160 bits.
   - SHA-256: El algoritmo SHA-256 genera un hash de 256 bits (32 bytes) casi único y de tamaño fijo.



Nota!
La función de generación de valores hash es una función de un solo sentido; no se puede descifrar.

Al utilizar la autenticación de vídeo, se genera un valor hash cada paquete de un flujo de vídeo. Estos valores hash se integran en el flujo de vídeo y se combinan junto con los datos del vídeo. Esto garantiza la integridad del contenido del flujo.

Los valores hash están firmados periódicamente, según el intervalo de firma definido, utilizando la clave privada del certificado almacenado en el TPM del dispositivo. Todas las grabaciones de alarmas y todos los cambios de bloques en grabaciones en iSCSI están cerrados con una forma que garantiza la autenticidad continua del vídeo.

Nota!
Calcular la firma digital requiere potencia de cálculo y puede influir de forma importante en el rendimiento global de una cámara si se realiza con demasiada frecuencia. Por consiguiente, se debe elegir un intervalo razonable.

Puesto que los valores hash y las firmas digitales están integrados en el flujo de vídeo, también se almacenan en la grabación. Esto permite autenticar el vídeo también durante la reproducción y las exportaciones.

Bosch Sicherheitssysteme GmbH
Robert-Bosch-Ring 5
85630 Grasbrunn
Germany
www.boschsecurity.com