

Bosch IP video products



Contenido

1	Propósito del documento y público objetivo	5
2	Concepto y consideraciones sobre seguridad	6
3	Instalación segura	7
3.1	Servidores y dispositivos de almacenamiento	7
3.2	Cámaras y dispositivos perimetrales	7
4	Configuración segura	8
4.1	Asignar direcciones IP	8
4.1.1	Gestionar DHCP	10
4.2	Cuentas de usuario y contraseñas	11
4.2.1	Asignación de contraseñas	11
4.2.2	Cómo asignar contraseñas mediante la página web del dispositivo	12
4.2.3	Asignación de contraseñas mediante Configuration Manager	13
4.2.4	Asignación de contraseñas para la instalación independiente de VRM	14
4.2.5	Asignación de contraseñas mediante BVMS (en DIVAR IP o independiente)	16
4.3	Reforzar la seguridad del acceso a los dispositivos	17
4.3.1	Uso general de puertos de red y transmisión de vídeo	17
4.3.2	Versión mínima de TLS	18
4.3.3	Uso de puertos de HTTP, HTTPS y vídeo	18
4.3.4	Software de vídeo y selección de puertos	19
4.3.5	SSH Tunneling	20
4.3.6	Acceso Telnet	20
4.3.7	RTSP: Real Time Streaming Protocol	20
4.3.8	UPnP: Universal Plug and Play	21
4.3.9	Multidifusión	22
4.3.10	Filtrado IPv4	23
4.3.11	SNMP	24
4.3.12	Base de tiempo segura	25
4.3.13	Servicios basados en la nube	25
4.4	Refuerzo de cámaras IP	26
4.4.1	Niveles de refuerzo	26
4.4.2	Descripción del refuerzo	26
4.4.3	Descripción de las funciones y recomendaciones de refuerzo	28
4.4.4	Defensa en profundidad	31
4.5	Refuerzo del almacenamiento	32
4.5.1	Establecimiento de una contraseña CHAP en dispositivos iSCSI	32
4.6	Refuerzo de servidores	33
4.6.1	Configuración recomendada del hardware de servidor	33
4.6.2	Configuración de seguridad recomendada en sistema operativo Windows	33
4.6.3	Actualizaciones de Windows	34
4.6.4	Instalación de software antivirus	34
4.6.5	Configuración recomendada en sistema operativo Windows	34
4.6.6	Activar el control de cuentas de usuario en el servidor	34
4.6.7	Desactivar la reproducción automática	35
4.6.8	Dispositivos externos	35
4.6.9	Configuración de la asignación de derechos de usuario	36
4.6.10	Protector de pantalla	37
4.6.11	Activar la configuración de directiva de contraseña	37
4.6.12	Desactivar los servicios de Windows no esenciales	37

4.6.13	Cuentas de usuario del sistema operativo Windows	38
4.6.14	Activar el firewall en el servidor	39
4.7	Refuerzo de clientes Windows	39
4.7.1	Estaciones de trabajo Windows	39
4.7.2	Configuración recomendada del hardware de las estaciones de trabajo Windows	39
4.7.3	Configuración de seguridad recomendada en sistema operativo Windows	39
4.7.4	Configuración recomendada en sistema operativo Windows	39
4.7.5	Activar el control de cuentas de usuario en el servidor	40
4.7.6	Desactivar la reproducción automática	40
4.7.7	Dispositivos externos	41
4.7.8	Configuración de la asignación de derechos de usuario	41
4.7.9	Protector de pantalla	42
4.7.10	Activar la configuración de directiva de contraseña	42
4.7.11	Desactivar los servicios de Windows no esenciales	43
4.7.12	Cuentas de usuario del sistema operativo Windows	43
4.7.13	Activar el firewall en la estación de trabajo	44
4.8	Proteger el acceso a la red	44
4.8.1	VLAN: LAN virtual	45
4.8.2	VPN: Red privada virtual	45
4.8.3	Desactivar los puertos de switch no utilizados	46
4.8.4	Redes protegidas con 802.1x	46
5	Funcionamiento seguro	47
5.1	Separación de red	47
5.2	Almacenamiento seguro de claves en el almacén de hardware	47
5.3	Certificados de dispositivos únicos	47
5.4	Comprobación de los archivos de registro	48
5.5	Sistema SIEM	49
5.6	PKI	49
5.7	AD FS	49
5.8	Funcionamiento seguro de las cámaras IP	49
5.8.1	Generar confianza con certificados	49
5.8.2	Autenticación de vídeo	50
6	Administración de actualizaciones de seguridad	52
7	Control de la seguridad	53
8	Eliminación y desmantelamiento seguros	54
9	Información adicional	55
	Glosario	56

1 Propósito del documento y público objetivo

La tecnología evoluciona a una velocidad que, a veces, es de lo más increíble. Los rápidos avances en inteligencia artificial (AI) e Internet de las cosas (IoT) y su uso masivo (AIoT) modifican el perfil de riesgo de los productos y servicios. Los ataques maliciosos intencionados son más factibles y probables debido a la mayor conectividad. El objetivo de Bosch es ofrecer productos y servicios seguros y fiables a los clientes.

Esta guía debería ayudar a los integradores a reforzar los productos de vídeo IP de Bosch para que cumplan mejor las políticas y los procedimientos de seguridad de red actuales 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 el uso de Configuration Manager para realizar las configuraciones mencionadas. En la mayoría de los casos, todas las configuraciones pueden realizarse utilizando BVMS Configuration Client, Configuration Manager y la interfaz web integrada de un dispositivo de vídeo.

2 Concepto y consideraciones sobre seguridad

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 Instalación segura

3.1 Servidores y dispositivos de almacenamiento

Todos los componentes del servidor (por ejemplo BVMS Management Server y el servidor de Video Recording Manager) y los dispositivos de almacenamiento deben instalarse en una zona segura. El acceso a la zona segura se debe proteger con un sistema de control de acceso y se debe supervisar. El grupo de usuarios que tiene acceso a la sala de servidores central se debe limitar a un pequeño grupo de personas.

A pesar de que los servidores y los dispositivos de almacenamiento se instalan en una zona segura, deben estar protegidos del acceso no autorizado.

Consulte

- *Refuerzo de servidores, Página 33*
- *Refuerzo del almacenamiento, Página 32*

3.2 Cámaras y dispositivos perimetrales

Se debe elegir una ubicación de instalación y una orientación de montaje seguras para la instalación de cámaras y dispositivos perimetrales. La ubicación ideal para este dispositivo es donde no se pueda interferir con él de forma intencionada o accidental.

4 Configuración segura

4.1 Asignar direcciones IP

Todos los dispositivos de vídeo IP de Bosch vienen actualmente en un estado predeterminado de fábrica y aceptan 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 ejecuta el firmware 6.32 o superior) aplicará automáticamente una dirección local de enlace fuera del rango de 169.254.1.0 a 169.254.254.255, o 169.254.0.0/16.

Con el firmware anterior, se asignará la dirección IP predeterminada 192.168.0.1.

Existen varias herramientas que se pueden utilizar para realizar la asignación de direcciones IP a dispositivos de vídeo IP de Bosch, por ejemplo:

- Bosch Configuration Manager
- BVMS Configuration Client
- BVMS Configuration Wizard

Todas las herramientas de software ofrecen la opción de asignar una sola dirección IPv4 estática, así como un rango de direcciones IPv4 a varios dispositivos simultáneamente. Esto incluye la máscara de subred y el direccionamiento de puerta de acceso predeterminado.

Es necesario introducir todas las direcciones IPv4 y valores de máscara de subred en la denominada "notación de punto decimal".

Aviso!



Uno de los primeros pasos para limitar las posibilidades de ataques informáticos internos en una red, ejecutados por dispositivos de red no autorizados que se conectan localmente, es limitar las direcciones IP disponibles que no se utilizan. Esto se hace utilizando IPAM (Administración de direcciones IP, **IP Address Management**), junto con la creación de una subred con el rango de direcciones IP que se va a utilizar.

La creación de subredes es el acto de tomar prestados bits a la parte del host de una dirección IP para dividir una gran red en varias redes más pequeñas. Cuanto más bits se tomen prestados, más redes se pueden crear, pero cada red admitirá menos direcciones de host.

Sufijo	Hosts	CIDR	Prestado	Binary
.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	. 10000000

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:

	Valor predeterminado	Subred
Intervalo 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 sobrantes	65.192	168

4.1.1

Gestionar DHCP

IPAM puede utilizar DHCP como una eficaz herramienta para controlar y utilizar las direcciones IP de su entorno. DHCP puede configurarse para utilizar un ámbito específico de direcciones IP. También se puede configurar para excluir un rango de direcciones.

Si utiliza DHCP, lo más recomendable sería, al implementar dispositivos de vídeo, configurar las reservas de direcciones que no caducan en función de la dirección MAC de cada dispositivo.

Aviso!



Incluso antes de utilizar la administración de direcciones IP para realizar un seguimiento del uso de las direcciones IP, una práctica recomendada en la administración de redes es limitar el acceso a la red a través de seguridad de puerto en los conmutadores perimetrales (por ejemplo, solo una dirección MAC específica puede acceder a través de un puerto específico).

4.2 Cuentas de usuario y contraseñas

Todos los codificadores y cámaras de vídeo IP Bosch incluyen tres cuentas de usuario integradas:

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

Se debe asignar una contraseña para cada una de las cuentas de usuario. La asignación de contraseñas es un paso fundamental en la protección de cualquier dispositivo de red. Se recomienda encarecidamente asignar contraseñas a todos los dispositivos de vídeo de red instalados.



Aviso!

Con la versión de firmware 6.30, se ha mejorado la administración de usuarios para aumentar la flexibilidad a la hora de permitir otros usuarios y nombres de usuario con contraseñas propias. Los antiguos niveles de cuenta ahora representan los niveles de grupos de usuarios. Con la versión de firmware 6.32, se ha introducido una directiva de contraseñas más estricta (para obtener más detalles, consulte *Cómo asignar contraseñas mediante la página web del dispositivo, Página 12*).

4.2.1 Asignación de 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.



Aviso!

Como se ha mencionado antes, la protección mediante contraseña es crítica cuando se trata de proteger los datos contra posibles ciberataques. Esto es aplicable a todos los dispositivos de red de todo el conjunto de su infraestructura de seguridad. La mayoría de las organizaciones ya tienen en vigor políticas de contraseñas seguras, pero, si trabaja con una nueva instalación que no tiene políticas en vigor, a continuación se indican las mejores prácticas al implementar la protección mediante contraseñas:

- Las contraseñas deben tener una longitud de entre 8 y 12 caracteres.
- Las contraseñas deben contener letras mayúsculas y minúsculas.
- Las contraseñas deben contener al menos un carácter especial.
- Las contraseñas deben contener al menos un dígito.

Ejemplo:

Utilizando la frase "to be or not to be" y nuestras reglas básicas de generación de buenas contraseñas.

- 2be0rnOt!t0Be



Aviso!

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.

4.2.2

Cómo asignar contraseñas mediante la 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 se 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.

Password

Password 'service'	<input type="password" value="●●●●●●●●●●"/>	Strong
Confirm password	<input type="password"/>	
Password 'user'	<input type="password" value="●●●●●●●●"/>	Medium
Confirm password	<input type="password"/>	
Password 'live'	<input type="password" value="●●●●●"/>	Weak
Confirm password	<input type="password"/>	

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.



User Management

 Please make sure that all users are password protected.

User name	Group	Type	
service	service	Password	 
user	user	Password	 
live	live	Password	 



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.



Aviso!

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.

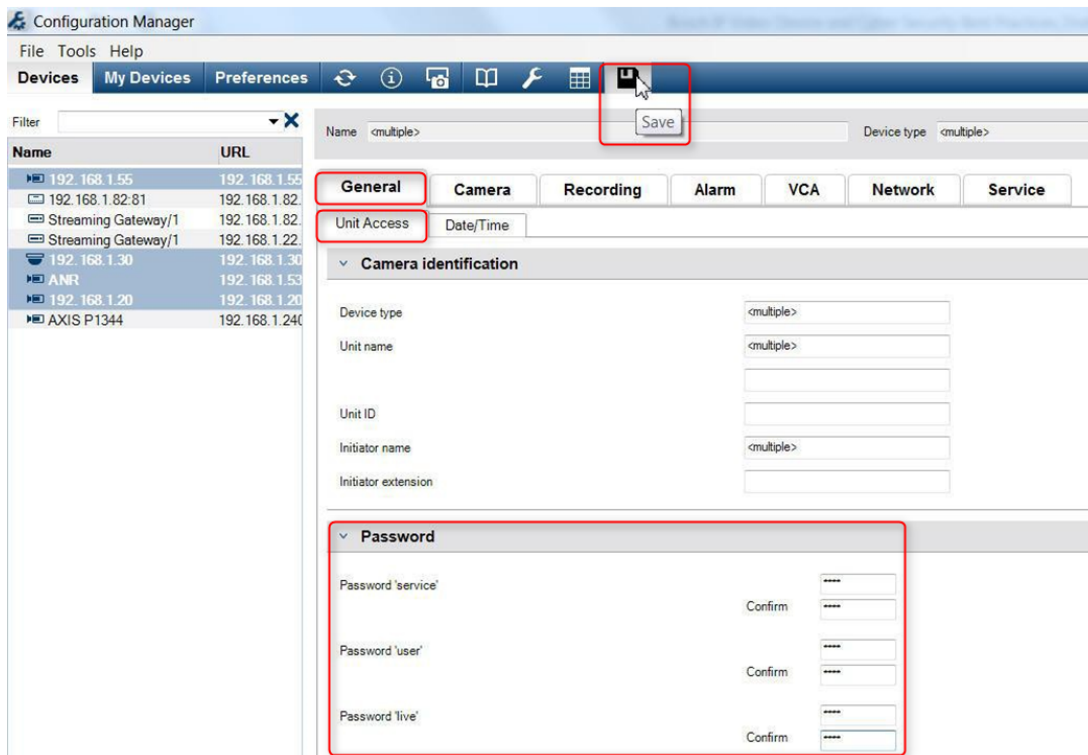
4.2.3

Asignación de contraseñas mediante Configuration Manager

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 de mayor tamaño gestionadas por BVMS o Video Recording Manager instalado en un dispositivo de grabación, se pueden aplicar contraseñas globales a todos los dispositivos de vídeo IP que se agreguen al sistema. Esto facilita la administración y garantiza un nivel estándar de seguridad en todo el sistema de vídeo en red.

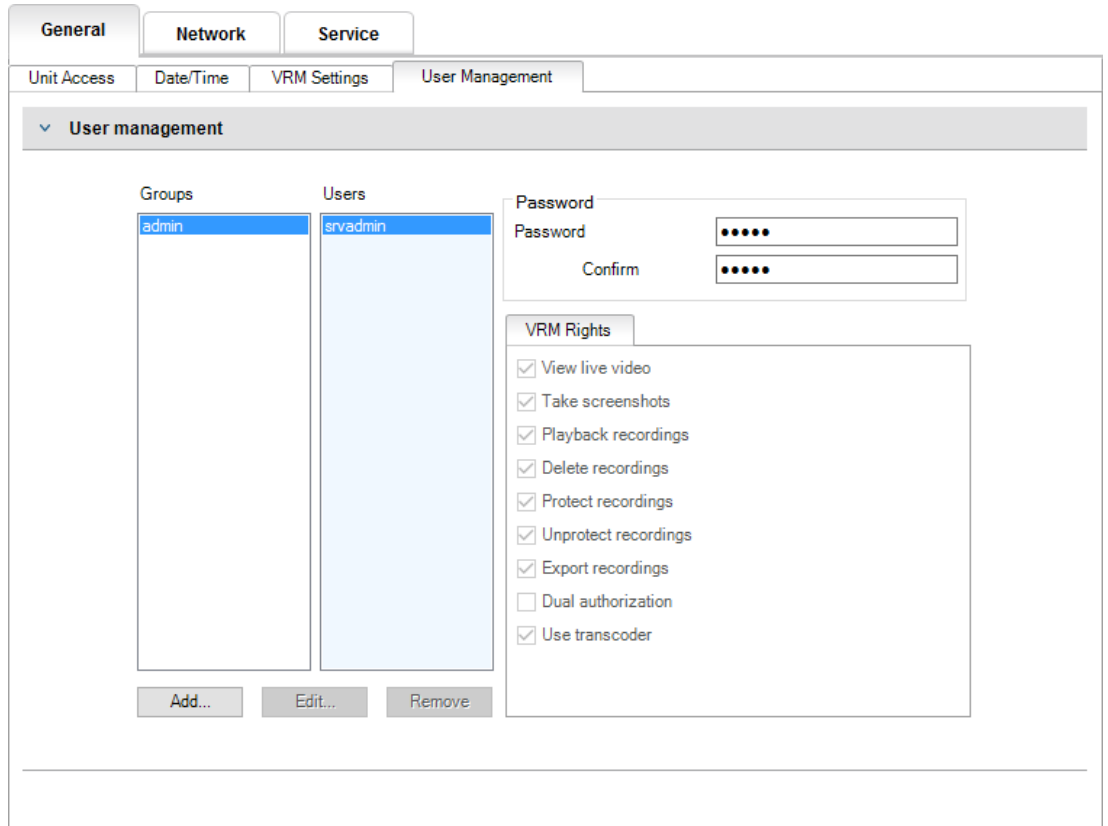
4.2.4

Asignación de contraseñas para la instalación independiente de VRM

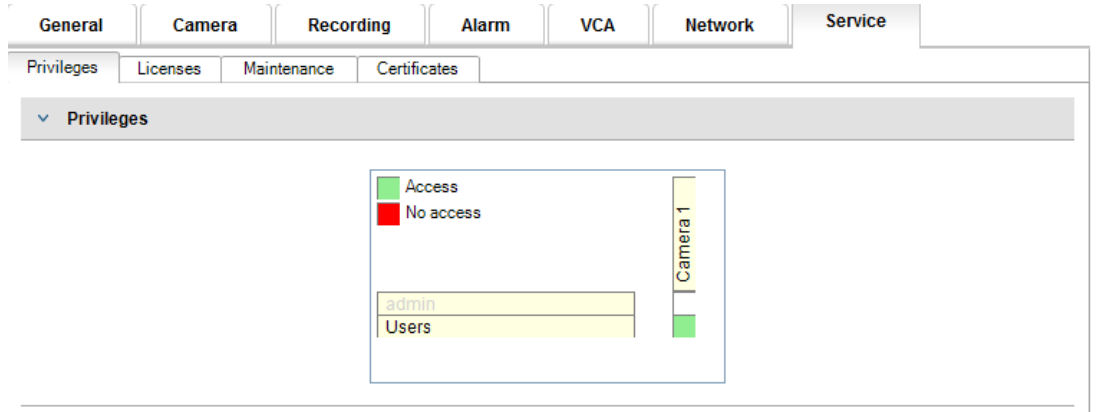
Video Recording Manager proporciona la administración de usuarios para aumentar la flexibilidad y la seguridad.

De forma predeterminada, no hay contraseñas asignadas a ninguna de las cuentas de usuario. La asignación de contraseñas es un paso fundamental en la protección de cualquier dispositivo de red. Se recomienda encarecidamente asignar contraseñas a todos los dispositivos de vídeo de red instalados.

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.



4.2.5 Asignación de contraseñas mediante BVMS (en DIVAR IP o independiente)

Protección del dispositivo mediante contraseña

Las cámaras y codificadores, gestionados por BVMS, pueden protegerse del acceso no autorizado mediante contraseña.

Las contraseñas para las cuentas de usuario integradas de codificadores/cámaras se pueden configurar con BVMS Configuration Client.

Para establecer una contraseña para las cuentas de usuario integradas en BVMS Configuration Client:

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

Protección mediante contraseña predeterminada

La versión 5.0 y posteriores de BVMS ofrecen la posibilidad de implementar contraseñas globales en todos los dispositivos de un sistema de vídeo de hasta 2000 cámaras IP. Se puede acceder a esta función mediante BVMS Configuration Wizard al trabajar con los dispositivos de grabación DIVAR IP 3000 o DIVAR IP 7000, o a través de BVMS Configuration Client en cualquier sistema.

Para acceder al menú de contraseñas globales en BVMS 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 **Forzar la protección con contraseña al activar.**

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 administrador de Video Recording Manager.



Aviso!

Si los dispositivos ya tienen contraseñas establecidas en alguna de las cuentas, no se sobrescribirán.

Por ejemplo, si la contraseña se establece para service pero no para live y user, la contraseña global solo se configurará para las cuentas live y user.

Configuración de BVMS y ajustes de VRM

De forma predeterminada, BVMS utiliza la cuenta de administración integrada **srvadmin** para conectarse a Video Recording Manager con protección mediante contraseña. Para evitar el acceso no autorizado a Video Recording Manager, la cuenta de administrador **srvadmin** debe protegerse con una contraseña compleja.

Para cambiar la contraseña de la cuenta **srvadmin** en BVMS 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 muestra el cuadro de diálogo **Cambiar contraseña....**

3. Introduzca una contraseña nueva para la cuenta **srvadmin** y haga clic en **Aceptar.**

Comunicación encriptada con las cámaras

Desde BVMS versión 7.0, los datos de vídeo en directo y la comunicación de control entre la cámara y BVMS Operator Client, Configuration Client, Management Server y Video Recording Manager se pueden codificar.

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

La cadena de conexión de BVMS utilizada internamente cambiará de rcpp://a.b.c.d (conexión RCP+ sin formato en el puerto 1756) a https://a.b.c.d (conexión HTTPS en el puerto 443) en su lugar.

Para los dispositivos antiguos que no admiten HTTPS, la cadena de conexión permanece sin cambios (RCP+).

Si selecciona la comunicación HTTPS, la comunicación usará HTTPS (TLS) para codificar toda la comunicación de control y la carga útil del vídeo a través del motor de codificación del dispositivo. Al utilizar TLS, todas las comunicaciones de control HTTPS y la carga útil del vídeo se codifican con una clave de codificación AES de hasta 256 bits de longitud.

Para activar la comunicación codificada en BVMS Configuration Client:

1. En el árbol de dispositivos, seleccione el codificador o la cámara que desee.
2. Haga clic con el botón derecho del ratón en el codificador o la cámara y luego haga clic en **Editar codificador**.
3. En el cuadro de diálogo **Editar codificador**, habilite **Conexión segura**.
4. Guarde la configuración y actívela.

Después de activar la conexión segura con el codificador, se pueden desactivar otros protocolos (consulte *Uso general de puertos de red y transmisión de vídeo, Página 17*).



Aviso!

BVMS solo admite el puerto HTTPS 443 predeterminado. No se admite el uso de puertos diferentes.

4.3

Reforzar la seguridad del acceso a los dispositivos

Todos los dispositivos de vídeo IP Bosch incluyen páginas web integradas para múltiples fines. Las páginas web específicas del dispositivo admiten funciones de vídeo en directo y de reproducción de vídeo, así como algunos ajustes de configuración específicos a los que es posible que no se pueda acceder mediante un sistema de gestión de vídeo. Las cuentas de usuario integradas actúan como acceso a las distintas secciones de las páginas web específicas. Si bien el acceso a la página web no se puede desactivar completamente mediante la propia página web (se podría usar Configuration Manager), existen varios métodos para restringir la presencia del dispositivo, restringir el acceso y gestionar el uso del puerto de vídeo.

4.3.1

Uso general de puertos de red y transmisión de vídeo

Todos los dispositivos de vídeo IP de Bosch utilizan Remote Control Protocol 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 dispositivos de vídeo IP Bosch: 1756, 1757 y 1758. Cuando se trabaja con BVMS u otro sistema de gestión de vídeo de proveedores de otros fabricantes que tenga dispositivos de vídeo IP Bosch integrados a través de Bosch VideoSDK, se debe acceder a los puertos mostrados en la red para que los dispositivos de vídeo IP funcionen correctamente.

El vídeo se puede transmitir desde los dispositivos de varias formas: UDP (Dinámico), HTTP (80) o HTTPS (443).

Se puede modificar el uso del puerto HTTP y HTTPS (consulte *Uso de puertos de HTTP, HTTPS y vídeo, Página 18*). Antes de realizar cualquier modificación en el puerto, se debe configurar la forma de comunicación deseada con un dispositivo. Puede acceder al menú de comunicaciones mediante 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.



Aviso!

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.

4.3.2

Versión mínima de TLS

Puede que algunos clientes más antiguos deban utilizar versiones de TLS más antiguas y menos seguras. Sin embargo, si es posible, defina una versión mínima para TLS a fin de evitar que los clientes hagan que el dispositivo utilice un modo de acceso menos seguro. Seleccione la versión de TLS más alta posible como versión mínima.



Aviso!

Al definir el nivel mínimo de seguridad para acceder a dispositivos de un software cliente, asegúrese de que todos los puertos y protocolos que permiten un nivel de acceso inferior se desconectan o desactivan en los dispositivos.

4.3.3

Uso de puertos de HTTP, HTTPS y vídeo

El uso de puertos HTTP y HTTPS en todos los dispositivos se puede modificar o desactivar. Se puede aplicar obligatoriamente la comunicación codificada deshabilitando el puerto RCP+ y el puerto HTTP, haciendo que todas las comunicaciones utilicen codificación. Si el uso del puerto HTTP está desactivado, HTTPS permanecerá activado y cualquier intento para desactivarlo fallará.

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**



Aviso!

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 conectarse a la dirección predeterminada generará un error.

4.3.4

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 se establecen en el puerto HTTP 10000, por ejemplo, BVMS Operator Client se configura para "TCP tunneling", todas las transmisiones de vídeo de la red se realizarán a través del puerto HTTP 10000.



Aviso!

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.



Aviso!

Dependiendo del escenario de implementación y la seguridad de la instalación, las prácticas recomendadas pueden variar. La deshabilitación y el redireccionamiento del uso del puerto HTTP o HTTPS tiene sus ventajas. El cambio del puerto en cualquiera de los protocolos puede ayudar a evitar el suministro de información a herramientas de red como NMAP (Network Mapper, escáner de seguridad gratuito). Aplicaciones como NMAP se utilizan normalmente como herramientas de conexión para identificar todos los puntos débiles de cualquier dispositivo de la red. Esta técnica, combinada con una implementación de contraseñas seguras, aumenta la seguridad general del sistema.

4.3.5 SSH Tunneling

Para un acceso remoto a los dispositivos con BVMS Operator Client mediante redes públicas, BVMS proporciona un túnel Secure Shell (SSH) para garantizar una comunicación segura (codificada).

SSH Tunneling crea un túnel codificado que se establece mediante un protocolo SSH/una conexión de socket. Este túnel codificado ofrece opciones de transporte tanto para el tráfico codificado como para el no codificado. La implementación de SSH de Bosch utiliza también el protocolo Omni-Path, un protocolo de comunicaciones de baja latencia desarrollado por Intel.

Para obtener más información sobre cómo configurar el servicio SSH en BVMS, consulte la documentación de BVMS.

Para obtener más información sobre cómo configurar sistemas DIVAR IP para un acceso remoto seguro con BVMS Operator Client, consulte la documentación de DIVAR IP.

4.3.6 Acceso Telnet

Telnet es un protocolo de capa de aplicación que proporciona comunicación a los dispositivos a través de una sesión de terminal virtual para tareas de mantenimiento y solución de problemas. Todos los dispositivos de vídeo IP Bosch son compatibles con Telnet y, de manera predeterminada, la compatibilidad con Telnet está activada en las versiones de firmware hasta la 6.1x. Desde la versión 6.20 del firmware en adelante, el puerto Telnet está desactivado de forma predeterminada.



Aviso!

Desde 2011 ha aumentado el número de ataques informáticos con el protocolo Telnet. En el entorno actual, las prácticas recomendadas indican que se debe deshabilitar la compatibilidad con Telnet en todos los dispositivos hasta que sea necesario para el mantenimiento o la 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**.



Aviso!

Desde la versión 6.20 del firmware, Telnet también es compatible con los denominados "web sockets", que utilizan conexiones HTTPS seguras. Los web sockets no utilizan el puerto Telnet estándar y proporcionan una forma segura de acceder a la interfaz de línea de comandos del dispositivo IP, si es necesario.

4.3.7 RTSP: Real Time Streaming Protocol

El protocolo de transmisión por secuencias en tiempo real (RTSP) es el componente de vídeo principal que utiliza el protocolo ONVIF para proporcionar control del flujo de vídeo y del dispositivo a los sistemas de administración de vídeo compatibles con ONVIF. El protocolo RTSP también lo utilizan varias aplicaciones de vídeo de terceros para funciones de

transmisión básicas y, en algunos casos, se puede utilizar para solucionar problemas de la red y los dispositivos. Todos los dispositivos de vídeo IP Bosch pueden generar flujos mediante 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



Aviso!

Se han recibido informes recientes de ataques informáticos que utilizan un ataque por desbordamiento de búfer de pila RTSP. Estos ataques se escriben en dispositivos de proveedores específicos. Las prácticas recomendadas serían deshabilitar el servicio si no se utiliza en un sistema de gestión de vídeo compatible con ONVIF o en una transmisión básica en tiempo real.

Como alternativa, y cuando el cliente de destino lo permita, la comunicación RTSP se puede tunelizar mediante una conexión HTTPS, que es, hasta ahora, la única forma de transmitir datos RTSP codificados.



Aviso!

Para obtener más información sobre el protocolo RTSP, consulte la nota de la aplicación sobre el *uso de RTSP con dispositivos VIP de Bosch* en el catálogo de productos en línea de Bosch Security Systems disponible en el siguiente enlace:

https://resources-boschsecurity-cdn.azureedge.net/public/documents/RTSP_VIP_Application_note_enUS_9007200806939915.pdf

4.3.8

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**.



Aviso!

UPnP no se debe utilizar en instalaciones de gran tamaño debido al gran número de notificaciones de registro y el riesgo potencial de accesos no deseados o ataques.

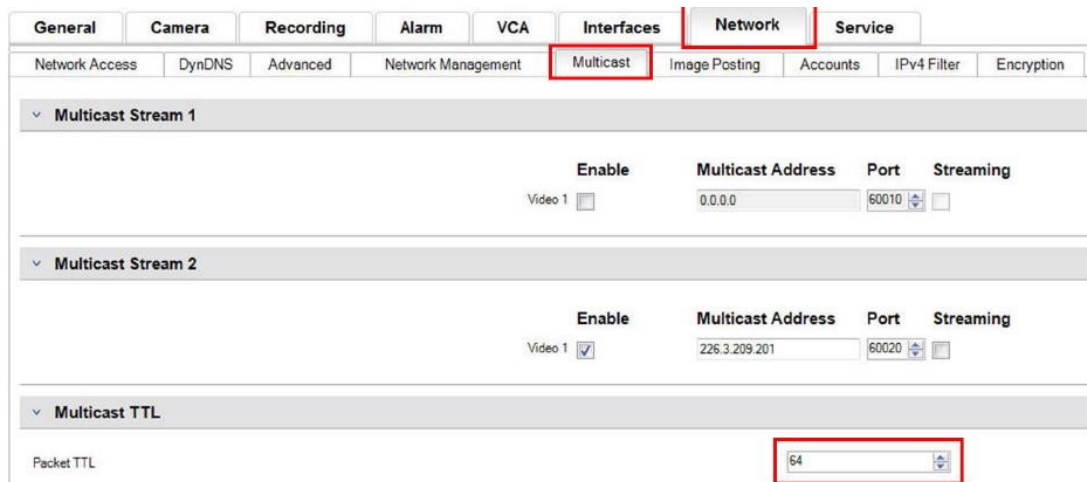
4.3.9

Multidifusión

Todos los dispositivos de vídeo IP de Bosch pueden ofrecer tanto "Multidifusión a demanda" como vídeo de "Multidifusión Streaming". Mientras que las transmisiones de vídeo monodifusión están basadas en destinos, la multidifusión se basa en el origen, lo cual puede introducir problemas de seguridad en el nivel de red, lo que incluye: control de acceso a grupos, confianza en el centro de grupos y confianza en el router. Aunque la configuración del router está fuera del alcance de esta guía, hay una solución de seguridad que se puede implementar desde el propio dispositivo de vídeo IP.

El alcance TTL (periodo de vida) define dónde hasta dónde se permite que fluya el tráfico multidifusión dentro de una red, cada tramo disminuye en uno el TTL. Cuando se configuran los dispositivos de vídeo IP para el uso multidifusión, el paquete TTL del dispositivo se puede modificar.

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



Aviso!

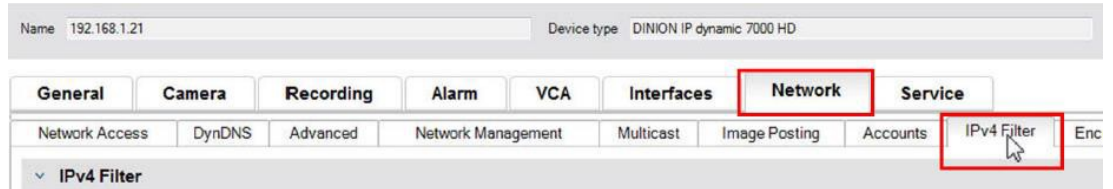
Al ocuparse de los datos de videovigilancia, la mejor práctica sería que estableciera los ajustes del TTL en 15, limitándolos al mismo sitio. O mejor aún, si sabe cuál es el número máximo exacto de tramos, úselo como valor del TTL.

4.3.10

Filtrado IPv4

Puede eliminar 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**.



Aviso!

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.



Aviso!

Basándose en la configuración de su sistema, el uso de la opción **Filtro IPv4** puede reducir la visibilidad no deseada de los dispositivos de una red. Si habilita esta función, asegúrese de documentar los ajustes para futuras consultas.

Tenga en cuenta que el dispositivo seguirá siendo accesible a través de IPv6, de modo que el filtrado IPv4 solo tiene sentido en las redes IPv4 puras.

4.3.11

SNMP

El protocolo simple de gestión de red (SNMP) es un protocolo común para controlar el estado de un sistema. Un sistema de control como este suele tener un servidor de administración central que recopila todos los datos de los componentes y dispositivos compatibles del sistema.

SNMP proporciona dos métodos para obtener el estado del sistema:

- El servidor de administración de red puede realizar sondeos sobre el estado de un dispositivo mediante solicitudes SNMP.
- Los dispositivos pueden notificar de forma activa al servidor de gestión de red su estado de sistema en caso de error o condición de alarma mediante el envío de capturas SNMP al servidor SNMP. Estas capturas 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 *cadena 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.

Aviso!

Tanto SNMPv1 como SNMPv2c se han visto amenazados debido a su falta de características de seguridad. Solo utilizan "cadena de seguridad" como un tipo de contraseña, que se transmite en texto sin cifrar.

Por tanto, SNMPv1 o SNMPv2c solo se utilizarán cuando se pueda garantizar que la red está protegida físicamente contra el acceso no autorizado.

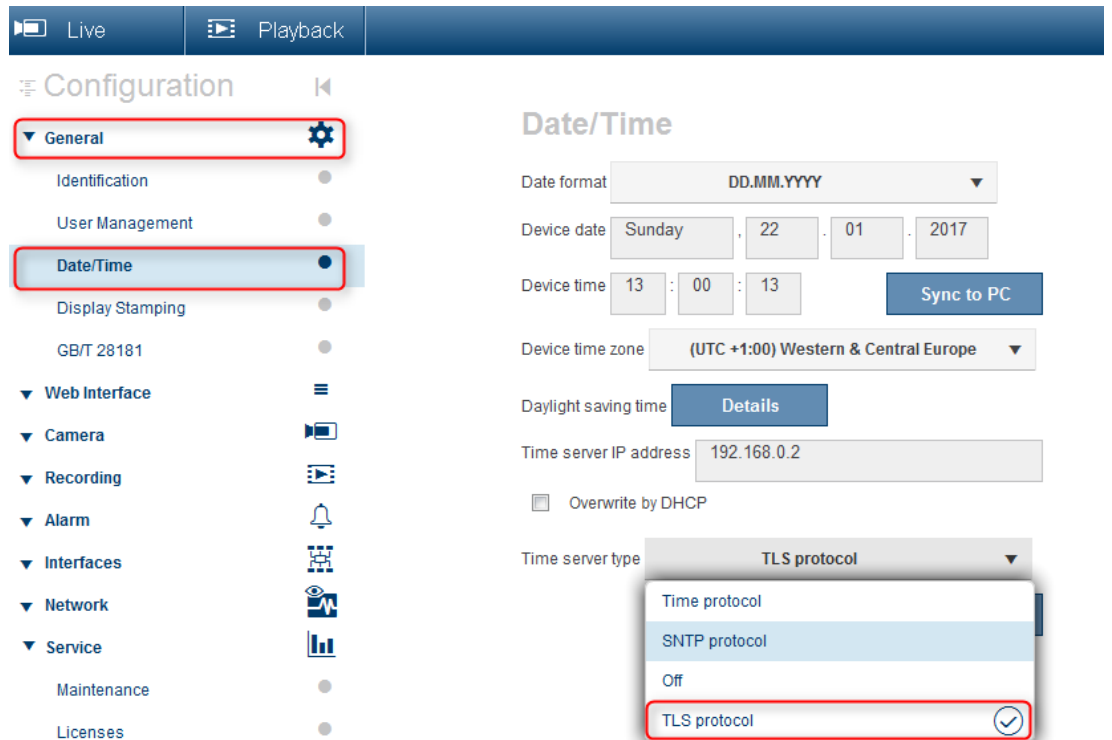
Actualmente, las cámaras Bosch solo son compatibles con SNMPv1. Asegúrese de que SNMP está desactivado si no lo utiliza.



4.3.12 Base de tiempo segura

Además del protocolo Time y SNTP, que son protocolos no protegidos, se ha introducido un tercer modo para el cliente de servidor horario con FW 6.20, que utiliza el protocolo TLS. Este método también se conoce normalmente 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.



Aviso!

Asegúrese de que la dirección IP del servidor horario introducida tiene una base temporal estable y seguro.

4.3.13 Servicios basados en la nube

Todos los dispositivos de vídeo IP de Bosch pueden comunicarse con servicios basados en la nube de Bosch, como Remote Portal. Según la región de implementación, esto permite a los dispositivos IP de vídeo utilizar servicios como Remote Device Management o Cloud VMS para enviar alarmas y otros datos a una estación central.

Para obtener más información, consulte la base de información de Bosch Building Technologies:

<https://community.boschsecurity.com>.

Los servicios pasados en la nube tienen tres modos de funcionamiento:

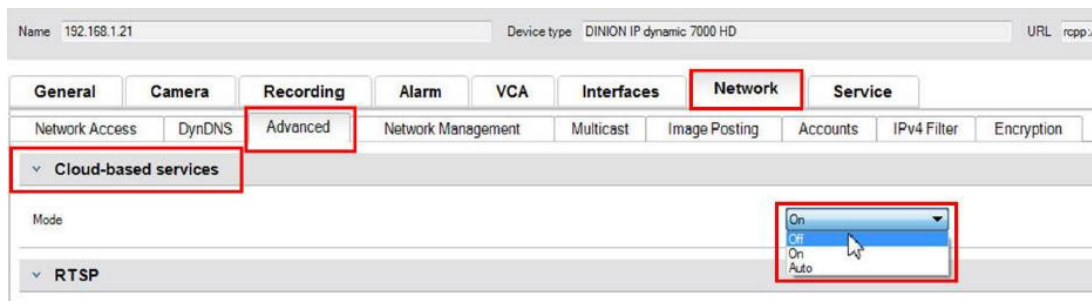
- **Activado:**
El dispositivo de vídeo sondeará constantemente el servidor en la nube.
- **Auto** (predeterminado):
Los dispositivos de vídeo tratarán de sondear el servidor en la nube unas cuantas veces y si no lo consiguen, dejarán de intentar llegar al servidor en la nube.

– **Desactivado:**

No se realizarán sondeos.

Los servicios basados en la nube se pueden desactivar fácilmente mediante Configuration Manager.

1. En Configuration Manager, seleccione el dispositivo deseado.
2. Seleccione la pestaña **Red** y, a continuación, la pestaña **Avanzado**.
3. Busque la sección **Servicios basados en la nube** de la página y seleccione **Off** (Desactivado) en la lista.



Aviso!

Si está utilizando los servicios basados en la nube de Bosch, mantenga la configuración predeterminada.

En todos los demás casos cambie el modo de los servicios basados en la nube a **Off** (Desactivado).

4.4

Refuerzo de cámaras IP

Las cámaras IP de Bosch se suministran con una configuración predeterminada que permite una fácil integración en diferentes entornos.

En función del entorno de destino y el nivel de seguridad previsto, puede que sea necesario cambiar algunos ajustes de la cámara para aumentar la seguridad informática y de los datos. Sin embargo, pueden existir limitaciones del entorno operativo que impongan la utilización de un determinado protocolo o función que sean menos seguros (por ejemplo SNMPv1).

4.4.1

Niveles de refuerzo

Hay dos niveles de refuerzo definidos: *elevado* y *estricto*.

El nivel de refuerzo *estricto* representa el medio más seguro para configurar un dispositivo, pero podría limitar el uso de este, ya que se desactivan funciones como la detección automática del mismo. Para cada función, debe evaluarse si se puede aplicar el ajuste *elevado* o *estricto*.

4.4.2

Descripción del refuerzo

Red - Servicios de red	Valor predeterminado	Elevado	Estricto
HTTP	Activado	Desactivado	Desactivado
HTTPS	Activado	Activado	Activado
RTSP	Activado	Opcional	Desactivado
RCP	Activado	Desactivado	Desactivado
SNMPv1	Desactivado	Desactivado	Desactivado
SNMPv3	Desactivado	Activado	Activado

Red - Servicios de red	Valor predeterminado	Elevado	Estricto
iSCSI	Activado	Opcional	Desactivado
UPnP	Desactivado	Desactivado	Desactivado
NTP Server	Desactivado	Desactivado	Desactivado
Discovery	Activado	Activado	Desactivado
ONVIF Discovery	Activado	Activado	Desactivado
GBT/28181	Desactivado	Desactivado	Desactivado
Mecanismo de restablecimiento de la contraseña	Activado	Desactivado	Desactivado
Respuesta a ping	Activado	Activado	Desactivado
RTSPS	Activado	Activado	Activado
HTTP	Activado	Desactivado	Desactivado

Red - Acceso a la red	Valor predeterminado	Elevado	Estricto
Versión mínima de TLS	1.0	1.2	1.2
HSTS	Desactivado	Activado	Activado

Red - Avanzado	Valor predeterminado	Elevado	Estricto
802.1x	Desactivado	Opcional	Activado
Syslog	Desactivado	TCP	TLS

Red - Gestión de red	Valor predeterminado	Elevado	Estricto
Modo SNMPv3	Desactivado	SHA1 / AES	SHA1 / AES

Red - Filtro IPv4	Valor predeterminado	Elevado	Estricto
Filtro IPv4	Desactivado	Activado	Activado

General - Fecha/Hora	Valor predeterminado	Elevado	Estricto
Fecha/Hora (cliente NTP)	Desactivado	Fecha de SNTP/TLS	Fecha de TLS

Conectividad - Servicios en la nube	Valor predeterminado	Elevado	Estricto
Remote Portal	Desactivado	Activado	Activado

Servicio - Registro	Valor predeterminado	Elevado	Estricto
Sellado por software	Desactivado	Activado	Activado

4.4.3

Descripción de las funciones y recomendaciones de refuerzo

HTTP

HTTP está habilitado de forma predeterminada, pero no está codificado, por lo que las credenciales o los ajustes se transfieren sin codificar si se utilizan.

Recomendación: El protocolo HTTP simple debe deshabilitarse a favor del protocolo HTTPS codificado, especialmente si la red no es de confianza.

HTTPS

HTTPS está codificado y debe ser la opción predeterminada para acceder a la interfaz web o a la API RCP basada en Web. Se recomienda que utilice sus propios PKI y certificados.

Recomendación: HTTPS es el protocolo seguro predeterminado que se utiliza para la configuración y debe permanecer habilitado.

RTSP

RTSP se utiliza para el flujo de vídeo, pero normalmente no está codificado. Si el software que recibe el flujo de vídeo puede utilizar RTSPS, se recomienda deshabilitar el protocolo RTSP simple. Al utilizar otros componentes de Bosch (por ejemplo, decodificadores/BVMS/VRM/DIVAR IP), se puede habilitar una codificación propia de Bosch para RTSP, lo que protege la transmisión.

Recomendación: Enfoque basado en el riesgo si el vídeo se puede transmitir sin codificar o mediante codificación de Bosch. Si es posible, utilice RTSPS codificado.

RCP

El protocolo de control remoto propio de Bosch es también el protocolo de configuración de las cámaras IP de Bosch. El protocolo RCP simple no está codificado, por lo que los ajustes se transfieren sin codificar. Todas las herramientas de Bosch llevan algún tiempo usando la comunicación RCP sobre HTTPS, pero puede que sea necesario seguir confiando en este protocolo para herramientas de integración o herramientas de programación de terceros.

Recomendación: Deshabilite RCP si no lo utilizan herramientas de terceros ni sistemas antiguos.

SNMPv1

SNMP es el protocolo común de control de red utilizado para consultar información de estado de un dispositivo o enviar traps a un receptor remoto, pero sin encriptar.

Recomendación: Manténlo deshabilitado si no es necesario para el control del estado u otros motivos de compatibilidad. Utilice SNMPv3 si es posible.

SNMPv3

SNMPv3 es el sucesor de SNMPv1 y también se puede utilizar encriptado.

Recomendación: Se recomienda si se debe implementar el control de SNMP.

iSCSI

Deshabilita el servidor iSCSI interno que se utiliza para realizar grabaciones internas en la cámara accesible mediante iSCSI. iSCSI es un protocolo no codificado.

Recomendación: Deshabilite el servidor iSCSI si no se utiliza en la cámara.

UPnP

Hacer que la cámara se detecte mediante el protocolo UPnP.

Recomendación: Deshabilite UPnP si no es necesario.

NTP Server

Habilite un servidor NTP en la cámara para que otros dispositivos o cámaras sincronicen la hora. Si es posible, un dispositivo específico debe proporcionar la hora a la red de la cámara, permitiendo la separación de servicios. Si no hay ningún otro dispositivo disponible, una cámara puede proporcionar la hora.

Recomendación: El servidor NTP debe deshabilitarse si no es necesario.

Discovery

Mediante un mecanismo propiedad de Bosch para hacer que las cámaras se detecten mediante software de Bosch, como Configuration Manager.

Recomendación: Cuando se trabaja con direcciones IP dinámicas, esta función debe permanecer habilitada. Esta función se puede desactivar cuando se trabaje en un entorno con direcciones IP fijas.

ONVIF Discovery

Admite la detección de dispositivos de cámara mediante el protocolo ONVIF Discovery.

Recomendación: Esta función debe permanecer habilitada al trabajar con direcciones IP dinámicas y herramientas conformes con ONVIF. Esta función se puede desactivar cuando se trabaje en un entorno fijo con direcciones IP fijas.

GBT/28181

GBT/28181 es un estándar chino para la interoperabilidad entre diferentes dispositivos.

Recomendación: Manténgalo deshabilitado si no es necesario.

Mecanismo de restablecimiento de la contraseña

Las cámaras IP se pueden montar en ubicaciones muy remotas, lo que dificulta la realización de tareas de mantenimiento o un restablecimiento de fábrica en caso de que el acceso a la cámara haya quedado bloqueado. Bosch ofrece la posibilidad de restablecer la contraseña de una cámara mediante un mecanismo de desafío-respuesta que se basa en un mecanismo de pares de claves públicas/privadas seguras.

Recomendación: Si no necesita esta función, se recomienda deshabilitarla.

Respuesta a ping

Configura si la cámara responde a las solicitudes de ping en la red. Puede ayudarle con la depuración. En una red de alta seguridad, se puede deshabilitar para evitar que el dispositivo se desvíe a través del barrido ping, aunque hay otros medios de detección de dispositivos que se pueden utilizar mediante un barrido ping.

Recomendación: Enfoque basado en el riesgo, se puede deshabilitar para redes de alta seguridad.

RTSPS

RTSPS es la versión codificada de RTSP y se usa para el flujo de vídeo. Si el software de recepción lo admite, se debe tener preferencia por RTSPS antes que por RTSP simple. Como muchos clientes RTSP no admiten la variante segura, RTSP sigue habilitado para la seguridad del nivel 1.

Recomendación: Use RTSPS si es posible.

Versión mínima de TLS

Las cámaras IP no permiten conexiones SSLv3 no seguras o más antiguas. IETF ha rechazado las versiones 1.0 y 1.1 de TLS. Además, existen problemas de seguridad potenciales conocidos (BEAST, FREAK).

Las cámaras CPP4, CPP6, CPP7 y CPP7.3 admiten el protocolo TLS 1.2 seguro, que se debe establecer como la versión mínima necesaria.

Las cámaras CPP13 y CPP14 no permiten las versiones de TLS anteriores a 1.2. También admiten la nueva especificación TLS 1.3.

Recomendación: Establezca la versión de TLS mínima en la 1.2.

HSTS

HTTP Strict Transport Security (HSTS) es una política establecida por un sitio web para proteger contra los ataques de intermediarios ("man-in-the-middle") y ataques de degradación de protocolo. Permite al sitio web informar al navegador de que solo se permiten conexiones HTTPS en esta conexión y no permita las conexiones HTTP no codificadas.

Recomendación: Habilite HSTS en la cámara.

802.1x

802.1x es un estándar para el Control de Acceso a la Red (NAC). Permite a los dispositivos autenticarse en la red, otorgando acceso a la misma únicamente a los dispositivos autenticados. Las cámaras IP de Bosch admiten 802.1x con autenticación mediante contraseña o basada en certificado; el método preferido es la autenticación basada en certificado. Para utilizar 802.1x, el conmutador de red debe admitir este estándar, por lo que se necesita un servidor de autenticación.

Recomendación: Si la infraestructura de red lo permite, utilice la autenticación de red con 802.1x.

Syslog

Como la cámara solo proporciona un espacio limitado para mensajes de registro, los mensajes de registro se deben enviar a una ubicación central y analizar para detectar cualquier ataque o error de configuración.

Recomendación: Utilice TCP Syslog para evitar la pérdida de mensajes debido a una pérdida de paquetes. Use Syslog con TLS para codificar y autenticar los mensajes.

Modo SNMPv3

SNMPv3 es el sucesor de SNMPv1 y permite la autenticación y transferencia de información seguras.

Recomendación: Cuando utilice SNMPv3, use SHA1 como protocolo de autenticación y AES como protocolo de privacidad (si es compatible).

Filtro IP

En Filtro IP, se pueden definir varias direcciones IP (hosts únicos o subredes de red) que pueden acceder a la cámara. Se recomienda definir los ordenadores o redes que acceden a la cámara aquí.

Recomendación: Se recomienda utilizar el filtro IP para definir las redes o hosts permitidos.

Fecha/hora

Para tener la marca de hora correcta en los registros y los datos de vídeo, se recomienda sincronizar la hora con un servidor horario central. Para tal fin se puede usar tanto la fecha de SNTP como de TLS. La ventaja de SNTP es una sincronización horaria más precisa. La ventaja de la fecha de TLS es la posibilidad de comprobar si hay un certificado correcto, lo que la convierte en la solución más segura.

Recomendación: Utilice un medio seguro de sincronización de la hora, ya sea con la fecha de SNTP o TLS.

Servicios basados en la nube

Bosch ofrece sus propios servicios basados en la nube para gestionar las cámaras en la nube de Bosch (Remote Portal). Los servicios basados en la nube no se conectan automáticamente a Remote Portal y están deshabilitados de forma predeterminada. En primer lugar, es necesario conectar cada cámara a Remote Portal si se debe utilizar. Se han tomado todas las precauciones necesarias para proteger la conexión entre Remote Portal y la cámara, de forma que, si es necesario, Remote Portal puede utilizarse en cualquier entorno.

Recomendación: Remote Portal se puede usar en función de si se está utilizando una solución en la nube.

Sellado por software

Una vez completada la configuración de una cámara IP, los ajustes del dispositivo no deben cambiarse. Se puede habilitar un sellado de software para notificar los cambios de configuración del dispositivo.

Recomendación: Habilite el sellado de software si no hay cambios en la configuración pendientes.

4.4.4**Defensa en profundidad**

La defensa en profundidad hace referencia a un enfoque de seguridad por capas en el que ninguna medida sola es responsable de la seguridad de un producto, sino que hay varias capas que un atacante debe traspasar para explotar un producto. En cada versión de un producto, se evalúa si se necesitan nuevas características para mitigar nuevos ataques o aumentar la seguridad global del producto.

A continuación se ofrece una descripción de las principales funciones de seguridad de la cámara IP.

– Firma del firmware

Cada archivo de actualización de firmware se codifica y firma con un certificado de Bosch. Solo se pueden instalar las actualizaciones que publicó Bosch en las cámaras para evitar la instalación de firmware malintencionado.

– Arranque seguro

Las cámaras de las plataformas CPP13, CPP14 o posteriores incluyen un mecanismo de arranque seguro. El arranque seguro comprueba la integridad de todo el sistema, empezando por el cargador de arranque y continuando por el propio firmware en las

cámaras. Cada paso del proceso de arranque verifica el siguiente, comenzando por una raíz de hardware de confianza sin cambios. Esto evitará que el cargador de arranque o el firmware se modifiquen en el dispositivo.

- **Cortafuegos para inicio de sesión**
Para proteger contra ataques de fuerza bruta contra la contraseña pero al mismo tiempo permitir a los administradores iniciar sesión y protegerse contra ataques de denegación de servicio (DoS), el cortafuegos para inicio de sesión comprueba los intentos de inicio de sesión a partir de análisis de comportamiento y, de forma dinámica, bloquea o permite el acceso basado en direcciones IP.
- **Autenticación de la cámara**
Para identificar y autenticar de forma exclusiva una cámara, se crea un certificado de dispositivo Bosch en cada cámara durante la producción. Este certificado se puede utilizar para comprobar si se comunica con un dispositivo Bosch auténtico. Además, se pueden cargar o crear certificados personalizados en la cámara para integrarlos en un entorno PKI con el fin de proteger contra los ataques de intermediarios (man-in-the-middle).

4.5 Refuerzo del almacenamiento

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 el acceso no autorizado a los datos de vídeo grabados, las unidades iSCSI deben protegerse contra accesos no autorizados:

- Utilice la autenticación mediante contraseña a través de CHAP para asegurarse de que solo los dispositivos conocidos pueden acceder al destino iSCSI. Establezca 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 automáticamente a todos los dispositivos. Si se utiliza una contraseña CHAP en un entorno BVMS VRM, todos los sistemas de almacenamiento se deben configurar para utilizar la misma contraseña.
- Elimine todos los nombres de usuario predeterminados y las contraseñas del destino iSCSI.
- Utilice contraseñas seguras en las cuentas de usuario administrativo del destino iSCSI.
- Deshabilite el acceso administrativo mediante Telnet en los destinos iSCSI. En su lugar, utilice el acceso SSH.
- Proteja el acceso de consola al destino iSCSI mediante una contraseña segura.
- Deshabilite las tarjetas de interfaz de red no utilizadas.
- Supervise el estado de los almacenamientos iSCSI mediante herramientas de terceros para identificar irregularidades.

4.5.1 Establecimiento de una contraseña CHAP en dispositivos iSCSI

Al establecer una contraseña CHAP global en BVMS Configuration Client, esta contraseña se transfiere automáticamente a todos los codificadores, decodificadores y dispositivos VSG.

En algunos dispositivos iSCSI no se admite esta función. Debe establecer la contraseña CHAP en estos dispositivos manualmente.

**Aviso!**

Debe establecer la contraseña CHAP global en los dispositivos iSCSI antes de agregarlos a BVMS.

Los dispositivos iSCSI no se pueden agregar a una configuración BVMS si la contraseña CHAP global ya está activada.

Para establecer manualmente una contraseña CHAP en un dispositivo iSCSI (por ejemplo, DIVAR IP), que se basa en una versión reciente del sistema operativo Microsoft Windows Server:

1. Abra el **Administrador de servidores** y desplácese a **File and Storage Services (Servicios de archivo y almacenamiento) > iSCSI**.
2. En la lista de **DESTINOS iSCSI**, haga clic con el botón derecho del ratón en el destino iSCSI deseado y haga clic en **Propiedades**.
Aparecerá el cuadro de diálogo **Propiedades**.
3. En el cuadro de diálogo **Propiedades**, haga clic en **Seguridad** y, a continuación, active la casilla de verificación **Enable CHAP** (Habilitar CHAP).
4. Introduzca lo siguiente:
 - **Nombre de usuario:** usuario
 - **Contraseña:** introduzca la contraseña CHAP global tal y como se proporciona en BVMS Configuration Client (en el menú **Hardware > Protect iSCSI storages with CHAP password... (Proteger almacenamientos iSCSI con contraseña CHAP)**).
5. Haga clic en **Aceptar**.
La contraseña CHAP se asigna al destino de iSCSI.

4.6 Refuerzo de servidores

4.6.1 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.

4.6.2 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.

4.6.3 Actualizaciones de Windows

Los parches y las actualizaciones de software de Windows deberán instalarse y mantenerse actualizados. Las actualizaciones de Windows incluyen a menudo parches para vulnerabilidades de seguridad recién detectadas, como la vulnerabilidad SSL Heartbleed, que afecta a millones de ordenadores de todo el mundo. Se deben instalar parches de mantenimiento para estos problemas significativos.

4.6.4 Instalación de software antivirus

Instale software antivirus y antispyware y manténgalo al día.

4.6.5 Configuración recomendada en sistema operativo Windows

Se recomiendan los siguientes ajustes en la directiva de grupo local en los sistemas operativos Windows Server. Para cambiar las directivas de equipos locales (LCP) predeterminadas, utilice el Editor de directiva de grupo local.

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**.

4.6.6 Activar el control de cuentas de usuario en el servidor

Local Computer Policies -> Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Security Options (Directivas de equipos locales -> Configuración de equipo -> Configuración de Windows -> Configuración de seguridad -> Directivas locales -> Opciones de seguridad)

Control de cuentas de usuario: modo de aprobación de administrador para la cuenta de administrador integrada	Activado
Control de cuentas de usuario: permita que las aplicaciones UIAccess soliciten la elevación sin utilizar el escritorio seguro.	Desactivado
Control de cuentas de usuario: comportamiento del indicador de elevación para los administradores en modo de aprobación de administrador	Aviso de autorización
Control de cuentas de usuario: comportamiento del indicador de elevación para usuarios estándar	Solicitar credenciales en el escritorio seguro
Control de cuentas de usuario: detección de instalaciones de aplicaciones y aviso de elevación	Activado

Control de cuentas de usuario: elevar solo los ejecutables firmados y validados	Desactivado
Control de cuentas de usuario: ejecutar todos los administradores en modo de aprobación de administrador	Activado
Control de cuentas de usuario: cambiar al escritorio seguro cuando se solicite elevación	Activado
Control de cuentas de usuario: virtualizar los fallos de escritura de archivo y registro en las ubicaciones de cada usuario	Activado

Local Computer Policies -> Computer Configuration -> Administrative Templates -> Windows Components -> Credential User Interface (Directivas de equipos locales -> Configuración del equipo -> Plantillas administrativas -> Componentes de Windows -> Interfaz de usuario de credenciales)

Enumerar las cuentas de administrador al realizar la elevación	Desactivado
--	-------------

4.6.7

Desactivar la reproducción automática

Local Computer Policies -> Computer Configuration -> Administrative Templates -> Windows Components -> AutoPlay Policies (Directivas de equipos locales -> Configuración del equipo -> Plantillas administrativas -> Componentes de Windows -> Directivas de reproducción automática)

Desactivar la reproducción automática	Todas las unidades habilitadas
Comportamiento predeterminado para la ejecución automática	Habilitado, no ejecutar ningún comando de ejecución automática
Desactivar la reproducción automática para dispositivos sin volumen	Activado

4.6.8

Dispositivos externos

Local Computer Policies -> Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Security Options (Directivas de equipos locales -> Configuración de equipo -> Configuración de Windows -> Configuración de seguridad -> Directivas locales -> Opciones de seguridad)

Dispositivos: permitir desacoplar sin tener que iniciar sesión	Desactivado
Dispositivos: se permite formatear y expulsar medios extraíbles	Administradores
Dispositivos: evitar que los usuarios instalen controladores de impresora	Activado
Dispositivos: limitar el acceso al CD-ROM solo al usuario conectado localmente	Activado
Dispositivos: limitar el acceso a disquetes solo al usuario conectado localmente	Activado

4.6.9

Configuración de la asignación de derechos de usuario**Local Computer Policies -> Computer Configuration -> Windows Settings -> Security****Settings -> Local Policies -> User Rights Assignment** (Directivas de equipos locales -> Configuración del equipo -> Configuración de Windows -> Configuración de seguridad -> Directivas locales -> Asignación de derechos de usuario)

Acceder al administrador de credenciales como emisor de confianza	Nadie
Acceder a este ordenador desde la red	Usuarios autenticados
Actuar como parte del sistema operativo	Nadie
Agregar estaciones de trabajo al dominio	Nadie
Permitir el inicio de sesión a través de Servicios de escritorio remoto	Administradores, usuarios de escritorio remoto
Cambiar la hora del sistema	Administradores
Cambiar la zona horaria	Administradores, servicio local
Crear un archivo de paginación	Administradores
Crear un objeto de token	Nadie
Crear objetos compartidos permanentes	Nadie
Denegar el acceso a este ordenador desde la red	Inicio de sesión anónimo, grupo de invitados
Denegar el inicio de sesión como tarea por lotes	Inicio de sesión anónimo, grupo de invitados
Denegar el inicio de sesión como servicio	Nadie
Denegar el inicio de sesión localmente	Inicio de sesión anónimo, grupo de invitados
Denegar el inicio de sesión a través de Servicios de escritorio remoto	Inicio de sesión anónimo, invitado
Permitir que las cuentas de usuario y equipo sean de confianza para la 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 descargar controladores de dispositivo	Administradores
Modificar una etiqueta de objeto	Nadie
Modificar valores de entorno de firmware	Administradores
Realizar tareas de mantenimiento de volumen	Administradores
Proceso único de perfil	Administradores

Eliminar el ordenador de la estación base	Administradores
Restaurar archivos y directorios	Administradores
Apagar el sistema	Administradores
Sincronizar datos del servicio de directorio	Nadie
Asumir la propiedad de los archivos u otros objetos	Administradores

4.6.10 Protector de pantalla

- Activar el salvapantallas protegido por contraseña y definir el tiempo de espera:
Local Computer Policies -> User Configuration -> Administrative Templates -> Control Panel -> Personalization (Directivas de equipos locales -> Configuración de usuario -> Plantillas administrativas -> Panel de control -> Personalización)

Habilitar el salvapantallas	Activado
Proteger el salvapantallas mediante contraseña	Activado
Tiempo de espera del salvapantallas	1800 segundos

4.6.11 Activar la configuración de directiva de contraseña

- Al habilitar la configuración de directivas de contraseñas, se garantiza que los usuarios cumplan los requisitos mínimos de contraseña
Local Computer Policies -> Windows Settings -> Security Settings -> Account Policies -> Password Policy (Directivas de equipo local -> Configuración de Windows -> Configuración de seguridad -> Directivas de cuenta -> Directiva de contraseña)

Aplicar historial de contraseñas	Se recuerdan 10 contraseñas
Duración máxima de la contraseña	90 días
Duración mínima de la contraseña	1 día
Longitud mínima de la contraseña	10 caracteres
La contraseña debe cumplir los requisitos de complejidad	Activado
Almacenar la contraseña mediante codificación reversible para todos los usuarios del dominio	Desactivado

4.6.12 Desactivar los servicios de Windows no esenciales

- Al desactivar los servicios de Windows que no son esenciales, se puede mejorar el nivel de seguridad y minimizar los puntos de ataque.

Servicio de puerta de acceso de capa de aplicación	Desactivado
Administración de aplicaciones	Desactivado
Navegador del ordenador	Desactivado
Distributed Link Tracking Client	Desactivado
Host del proveedor de detección de funciones	Desactivado
Publicación de recursos de detección de funciones	Desactivado

Acceso a dispositivos de interfaz humana	Desactivado
Uso compartido de la conexión a Internet (ICS)	Desactivado
Asignador de detección de topología de capa de enlace	Desactivado
Planificador de clase multimedia	Desactivado
Archivos fuera de línea	Desactivado
Administrador de conexiones automáticas de acceso remoto	Desactivado
Administrador de conexiones de acceso remoto	Desactivado
Enrutamiento y acceso remoto	Desactivado
Detección de hardware de shell	Desactivado
Asistente de consola de administración especial	Desactivado
Detección de SSDP	Desactivado

4.6.13

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

Local Computer Policies -> Computer Configuration -> Windows Settings -> Security Settings -> Account Policies -> Account Lockout Policy (Directivas de equipos locales -> Configuración del equipo -> Configuración de Windows -> Configuración de seguridad -> Directivas de cuenta -> Directiva de bloqueo de cuenta)

Duración del bloqueo de cuenta	Duración del bloqueo de cuenta
15 minutos Umbral de bloqueo de cuenta 10 intentos de conexión fallidos	15 minutos Umbral de bloqueo de cuenta 10 intentos de conexión fallidos

Restablecer el contador de bloqueo de cuenta después de	Restablecer el contador de bloqueo de cuenta después de
---	---

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

4.6.14 Activar el firewall en el servidor

- ▶ Active la comunicación del puerto estándar de BVMS conforme a los puertos de BVMS.



Aviso!

Consulte la documentación de BVMS para obtener información sobre los ajustes de puerto correspondientes y su uso. Compruebe de nuevo los ajustes cuando se realicen actualizaciones de firmware o software.

4.7 Refuerzo de clientes Windows

4.7.1 Estaciones de trabajo Windows

Los sistemas operativos de escritorio de Windows, que se usan para las aplicaciones cliente de BVMS como BVMS Operator Client o Configuration Client, se instalan fuera del área de seguridad. Las estaciones de trabajo se deben reforzar para proteger los datos de vídeo, los documentos y otras aplicaciones contra el acceso no autorizado.

Se deben aplicar o comprobar los siguientes ajustes.

4.7.2 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.

4.7.3 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.

4.7.4 Configuración recomendada en sistema operativo Windows

Se recomiendan los siguientes ajustes en la directiva de grupo local en los sistemas operativos Windows Server. Para cambiar las directivas de equipos locales (LCP) predeterminadas, utilice el Editor de directiva de grupo local.

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**.

4.7.5

Activar el control de cuentas de usuario en el servidor

Local Computer Policies -> Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Security Options (Directivas de equipos locales -> Configuración de equipo -> Configuración de Windows -> Configuración de seguridad -> Directivas locales -> Opciones de seguridad)

Control de cuentas de usuario: modo de aprobación de administrador para la cuenta de administrador integrada	Activado
Control de cuentas de usuario: permita que las aplicaciones UIAccess soliciten la elevación sin utilizar el escritorio seguro.	Desactivado
Control de cuentas de usuario: comportamiento del indicador de elevación para los administradores en modo de aprobación de administrador	Aviso de autorización
Control de cuentas de usuario: comportamiento del indicador de elevación para usuarios estándar	Solicitar credenciales en el escritorio seguro
Control de cuentas de usuario: detección de instalaciones de aplicaciones y aviso de elevación	Activado
Control de cuentas de usuario: elevar solo los ejecutables firmados y validados	Desactivado
Control de cuentas de usuario: ejecutar todos los administradores en modo de aprobación de administrador	Activado
Control de cuentas de usuario: cambiar al escritorio seguro cuando se solicite elevación	Activado
Control de cuentas de usuario: virtualizar los fallos de escritura de archivo y registro en las ubicaciones de cada usuario	Activado

Local Computer Policies -> Computer Configuration -> Administrative Templates -> Windows Components -> Credential User Interface (Directivas de equipos locales -> Configuración del equipo -> Plantillas administrativas -> Componentes de Windows -> Interfaz de usuario de credenciales)

Enumerar las cuentas de administrador al realizar la elevación	Desactivado
--	-------------

4.7.6

Desactivar la reproducción automática

Local Computer Policies -> Computer Configuration -> Administrative Templates -> Windows Components -> AutoPlay Policies (Directivas de equipos locales -> Configuración del equipo -> Plantillas administrativas -> Componentes de Windows -> Directivas de reproducción automática)

Desactivar la reproducción automática	Todas las unidades habilitadas
Comportamiento predeterminado para la ejecución automática	Habilitado, no ejecutar ningún comando de ejecución automática
Desactivar la reproducción automática para dispositivos sin volumen	Activado

4.7.7

Dispositivos externos

Local Computer Policies -> Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Security Options (Directivas de equipos locales -> Configuración de equipo -> Configuración de Windows -> Configuración de seguridad -> Directivas locales -> Opciones de seguridad)

Dispositivos: permitir desacoplar sin tener que iniciar sesión	Desactivado
Dispositivos: se permite formatear y expulsar medios extraíbles	Administradores
Dispositivos: evitar que los usuarios instalen controladores de impresora	Activado
Dispositivos: limitar el acceso al CD-ROM solo al usuario conectado localmente	Activado
Dispositivos: limitar el acceso a disquetes solo al usuario conectado localmente	Activado

4.7.8

Configuración de la asignación de derechos de usuario

Local Computer Policies -> Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> User Rights Assignment (Directivas de equipos locales -> Configuración del equipo -> Configuración de Windows -> Configuración de seguridad -> Directivas locales -> Asignación de derechos de usuario)

Acceder al administrador de credenciales como emisor de confianza	Nadie
Acceder a este ordenador desde la red	Usuarios autenticados
Actuar como parte del sistema operativo	Nadie
Agregar estaciones de trabajo al dominio	Nadie
Permitir el inicio de sesión a través de Servicios de escritorio remoto	Administradores, usuarios de escritorio remoto
Cambiar la hora del sistema	Administradores
Cambiar la zona horaria	Administradores, servicio local
Crear un archivo de paginación	Administradores
Crear un objeto de token	Nadie
Crear objetos compartidos permanentes	Nadie

Denegar el acceso a este ordenador desde la red	Inicio de sesión anónimo, grupo de invitados
Denegar el inicio de sesión como tarea por lotes	Inicio de sesión anónimo, grupo de invitados
Denegar el inicio de sesión como servicio	Nadie
Denegar el inicio de sesión localmente	Inicio de sesión anónimo, grupo de invitados
Denegar el inicio de sesión a través de Servicios de escritorio remoto	Inicio de sesión anónimo, invitado
Permitir que las cuentas de usuario y equipo sean de confianza para la 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 descargar controladores de dispositivo	Administradores
Modificar una etiqueta de objeto	Nadie
Modificar valores de entorno de firmware	Administradores
Realizar tareas de mantenimiento de volumen	Administradores
Proceso único de perfil	Administradores
Eliminar el ordenador de la estación base	Administradores
Restaurar archivos y directorios	Administradores
Apagar el sistema	Administradores
Sincronizar datos del servicio de directorio	Nadie
Asumir la propiedad de los archivos u otros objetos	Administradores

4.7.9

Protector de pantalla

- Activar el salvapantallas protegido por contraseña y definir el tiempo de espera:
Local Computer Policies -> User Configuration -> Administrative Templates -> Control Panel -> Personalization (Directivas de equipos locales -> Configuración de usuario -> Plantillas administrativas -> Panel de control -> Personalización)

Habilitar el salvapantallas	Activado
Proteger el salvapantallas mediante contraseña	Activado
Tiempo de espera del salvapantallas	1800 segundos

4.7.10

Activar la configuración de directiva de contraseña

- Al habilitar la configuración de directivas de contraseñas, se garantiza que los usuarios cumplan los requisitos mínimos de contraseña

Local Computer Policies -> Windows Settings -> Security Settings -> Account Policies -> Password Policy (Directivas de equipo local -> Configuración de Windows -> Configuración de seguridad -> Directivas de cuenta -> Directiva de contraseña)

Aplicar historial de contraseñas	Se recuerdan 10 contraseñas
Duración máxima de la contraseña	90 días
Duración mínima de la contraseña	1 día
Longitud mínima de la contraseña	10 caracteres
La contraseña debe cumplir los requisitos de complejidad	Activado
Almacenar la contraseña mediante codificación reversible para todos los usuarios del dominio	Desactivado

4.7.11

Desactivar los servicios de Windows no esenciales

- Al desactivar los servicios de Windows que no son esenciales, se puede mejorar el nivel de seguridad y minimizar los puntos de ataque.

Servicio de puerta de acceso de capa de aplicación	Desactivado
Administración de aplicaciones	Desactivado
Navegador del ordenador	Desactivado
Distributed Link Tracking Client	Desactivado
Host del proveedor de detección de funciones	Desactivado
Publicación de recursos de detección de funciones	Desactivado
Acceso a dispositivos de interfaz humana	Desactivado
Uso compartido de la conexión a Internet (ICS)	Desactivado
Asignador de detección de topología de capa de enlace	Desactivado
Planificador de clase multimedia	Desactivado
Archivos fuera de línea	Desactivado
Administrador de conexiones automáticas de acceso remoto	Desactivado
Administrador de conexiones de acceso remoto	Desactivado
Enrutamiento y acceso remoto	Desactivado
Detección de hardware de shell	Desactivado
Asistente de consola de administración especial	Desactivado
Detección de SSDP	Desactivado

4.7.12

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

Local Computer Policies -> Computer Configuration -> Windows Settings -> Security Settings -> Account Policies -> Account Lockout Policy (Directivas de equipos locales -> Configuración del equipo -> Configuración de Windows -> Configuración de seguridad -> Directivas de cuenta -> Directiva de bloqueo de cuenta)

Duración del bloqueo de cuenta	Duración del bloqueo de cuenta
15 minutos Umbral de bloqueo de cuenta 10 intentos de conexión fallidos	15 minutos Umbral de bloqueo de cuenta 10 intentos de conexión fallidos
Restablecer el contador de bloqueo de cuenta después de	Restablecer el contador de bloqueo de 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.

4.7.13

Activar el firewall en la estación de trabajo

- ▶ Active la comunicación del puerto estándar de BVMS conforme a los puertos de BVMS.



Aviso!

Consulte la documentación de BVMS para obtener información sobre los ajustes de puerto correspondientes y su uso. Compruebe de nuevo los ajustes cuando se realicen actualizaciones de firmware o software.

4.8

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.

4.8.1

VLAN: LAN virtual

Una red LAN virtual crea subdividiendo una LAN en varios segmentos. La segmentación de la red se realiza a través del conmutador de red o la configuración del router. Una VLAN tiene la ventaja de que las necesidades de recursos se pueden solucionar sin necesidad de cambiar las conexiones de red del dispositivo.

Los esquemas de Quality of Service, aplicados a segmentos específicos como la videovigilancia, puede ayudar no solo a mejorar la seguridad, sino también el rendimiento.

Los dispositivos VLAN se implementan en la capa de enlace de datos (capa OSI 2) y ofrecen una analogía a la creación de subredes IP (consulte *Asignar direcciones IP, Página 8*), que es similar en la capa de red (capa OSI 3).

4.8.2

VPN: Red privada virtual

Una red privada virtual es una red separada (privada), que a menudo se extiende a través de las redes públicas o Internet. Existen varios protocolos disponibles para crear una VPN, normalmente un túnel que transporta el tráfico protegido. Las redes privadas virtuales se pueden diseñar como túneles punto a punto, conexiones "alguno a alguno" o conexiones multipunto. Las VPN se pueden implementar con comunicaciones codificadas o simplemente se puede confiar en la comunicación segura dentro de la propia VPN.

Las VPN se pueden usar para conectar sitios remotos mediante conexiones de red de área extensa (WAN), a la vez que protegen la privacidad y aumentan la seguridad dentro de una red de área local (LAN). Como una VPN actúa como una red independiente, todos los dispositivos agregados a la VPN funcionarán perfectamente como si estuvieran en una red normal. VPN no solo añade una capa adicional de protección para un sistema de vigilancia, sino que también ofrece la ventaja adicional de segmentar el tráfico comercial y de vídeo de las redes de producción.



Aviso!

Si procede, las redes VLAN o VPN aumentan el nivel de seguridad del sistema de vigilancia si se combinan con la 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.

4.8.3 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.

4.8.4 Redes protegidas con 802.1x

Todos los dispositivos de vídeo IP de Bosch se pueden configurar como clientes 802.1x. Esto permite autenticarse en un servidor RADIUS y participar en una red segura. Antes de conectar los dispositivos de vídeo a la red segura, necesitará conectarse directamente al dispositivo de vídeo desde el ordenador portátil de un técnico para introducir credenciales válidas, tal y como se indica 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**.

The screenshot shows the Configuration Manager interface for a device named '192.168.1.50' with device type 'DINION IP dynamic 7000 HD'. The 'Network' tab is selected and highlighted with a red box. Within the 'Network' tab, the 'Advanced' sub-tab is also highlighted with a red box. Other tabs include General, Camera, Recording, Alarm, VCA, Interfaces, and Service. Below the tabs, there are sub-tabs for Network Access, DynDNS, Advanced, Network Management, Multicast, Image Posting, Accounts, and IPv4.

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.

Aviso!



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.

Protocolo de autenticación extensible-Seguridad de la capa de transporte

Extensible Authentication Protocol (EAP) permite usar varios métodos de autenticación. La Seguridad de la capa de transporte (TLS) proporciona autenticación mediante contraseña, negociación del conjunto de cifrado con protección de integridad e intercambio de claves entre dos extremos. EAP-TLS es compatible con la autenticación de contraseñas basada en certificados y la derivación de claves. En otras palabras, EAP-TLS encapsula el proceso en el que tanto el servidor como el cliente se envían un certificado.

Aviso!



Consulte el documento técnico específico *Network Authentication - 802.1x - Secure the Edge of the Network* (Autenticación de red - 802.1x - Proteger el perímetro de la red), disponible en el catálogo de productos en línea de Bosch Security Systems, en:

http://resource.boschsecurity.com/documents/WP_802.1x_Special_enUS_22335867275.pdf.

5 Funcionamiento seguro

5.1 Separación de red

Si es posible, el dispositivo debe operar en una red independiente (por ejemplo, utilizando la tecnología VLAN), con restricciones de acceso para limitar el tráfico de difusión y protegerlo de los ataques en la red.

5.2 Almacenamiento seguro de claves en el almacén de hardware

Las claves privadas de los certificados se protegen mejor si se almacenan de forma segura en un componente de hardware o un almacén de hardware. Estos chips ofrecen protección frente a accesos no autorizados a las claves privadas, incluso cuando el dispositivo está físicamente abierto para acceder a él.

En las cámaras Bosch, dichas claves se almacenan en un dispositivo multiprocesador o elemento seguro (SE) independiente. Ambos ofrecen almacenamiento seguro, así como funciones criptográficas que nunca exponen las claves privadas a ubicaciones o memoria en las que se puedan recuperar.

En estaciones de trabajo y servidores, normalmente hay un chip del módulo de plataforma segura (TPM) disponible. Siempre que sea posible, se deben configurar bibliotecas y funciones criptográficas para poder utilizar el almacenamiento TPM.

5.3 Certificados de dispositivos únicos

Aunque suele haber un certificado predeterminado autofirmado con todos los dispositivos que son compatibles con TLS o HTTPS, este certificado no debe considerarse suficiente solo para la autenticación, ya que no protege de los ataques de intermediarios (MITM).

Si los dispositivos se encuentran en un entorno en el que se requieren pasos adicionales para validar la identidad de cada dispositivo de vídeo IP, pueden crearse y cargarse nuevos certificados y claves privadas en los propios dispositivos de vídeo. Los nuevos certificados pueden obtenerse de una autoridad emisora de certificados (CA) o pueden crearse con un kit de herramientas OpenSSL.

Si los dispositivos se utilizan en redes públicas, se recomienda obtener certificados de una autoridad emisora de certificados pública, o tener certificados propios firmados por dicha autoridad, que también puede verificar el origen y la validez, es decir, la confianza del certificado del dispositivo.

Desde hace años, todas las cámaras Bosch vienen con un certificado de dispositivo único preinstalado y una clave privada, que se deriva del certificado raíz de Bosch y se instala en un entorno de producción seguro, lo que demuestra que la cámara es un dispositivo Bosch original. Este certificado se utiliza automáticamente para las conexiones HTTPS y se puede utilizar para identificar y autenticar un dispositivo mediante la verificación de la cadena de certificados hasta el certificado raíz de Bosch.



Aviso!

Los certificados se deben utilizar para autenticar un único dispositivo. Se recomienda crear un certificado específico por dispositivo, derivado de un certificado raíz.

La variante más segura de una implementación de certificado es generar una solicitud de firma de certificado (CSR) en el dispositivo y solicitar un certificado de una autoridad emisora de certificados interna o externa.

Con una solicitud de firma de certificado, el dispositivo mantiene la clave privada interna y solo muestra el resto del certificado para que la autoridad emisora de certificados lo firme. La clave privada se almacena de forma segura en el elemento seguro (SE) de la cámara o, por ejemplo, en el módulo de plataforma segura (TPM) del dispositivo.

Por lo tanto, siempre que un dispositivo le ofrezca la posibilidad de CSR, esta debe ser la forma preferida de crear un certificado.

Los certificados se pueden cargar en un dispositivo mediante la página web de un dispositivo de vídeo o mediante Configuration Manager.

Carga de certificados mediante la página web del dispositivo

Los certificados se pueden cargar mediante la página web del dispositivo de un dispositivo de vídeo.

En la página web del dispositivo, en la página **Certificados**, puede agregar y eliminar nuevos certificados, así como definir su uso.

Carga de certificados mediante el uso de Configuration Manager

En Configuration Manager, los certificados se pueden cargar fácilmente en uno o varios dispositivos de forma simultánea.

Para cargar certificados:

1. En Configuration Manager, seleccione uno o varios dispositivos.
2. Haga clic con el botón derecho del ratón en **Carga de archivo**, haga clic en **Certificado SSL...**

Se abre una ventana del Explorador de Windows para localizar el certificado para la carga.

En sistemas más pequeños, Configuration Manager ofrece una función muy beneficiosa, llamada **MicroCA**, que permite crear o utilizar un CA raíz y derivar certificados de este para los dispositivos, o bien utilizarlo para firmar las solicitudes de firma de certificado de los dispositivos, también para varios dispositivos de forma simultánea. Para obtener más detalles, consulte el Manual de usuario de Configuration Manager.

Consulte

- *Generar confianza con certificados, Página 49*

5.4

Comprobación de los archivos de registro

El control de los archivos de registro es una parte importante del análisis de seguridad o de la actividad de mantenimiento. Una revisión frecuente de los archivos de registro puede mostrar problemas de configuración o infracciones de seguridad, como inicios de sesión falsos.

Para analizar los archivos de registro y almacenarlos a largo plazo, es aconsejable enviarlos a un servidor Syslog o a un sistema SIEM, ya que, por ejemplo, una cámara reserva un espacio fijo para el registro internamente, pero sobrescribirá los registros más antiguos si dicho espacio está lleno.

5.5 Sistema SIEM

El sistema de información de seguridad y gestión de eventos (SIEM) se utiliza para recoger y analizar información de distintos dispositivos y sistemas. Los dispositivos pueden integrarse con un sistema SIEM enviando los registros mediante el protocolo Syslog. El análisis de estos registros puede ayudar a realizar el mantenimiento y a detectar errores de configuración o ataques en el dispositivo (por ejemplo, inicios de sesión falsos).

5.6 PKI

La Infraestructura de clave pública (PKI) hace referencia a los sistemas necesarios para generar y gestionar certificados digitales. Para HTTPS, la autenticación de red con 802.1x, la autenticación de usuario con certificados y otras funciones de codificación, se pueden instalar certificados personalizados en el dispositivo.

5.7 AD FS

Active Directory Federation Services (AD FS) es un servicio de Microsoft que permite la autenticación en un directorio Active Directory local (mediante un servidor AD FS) o en la nube de Azure. Además de la autenticación de usuario local con contraseñas o la autenticación basada en certificados, la integración de dispositivos en un dominio de Active Directory es posible con AD FS para autenticar y administrar el acceso de los usuarios de forma centralizada.

5.8 Funcionamiento seguro de las cámaras IP

5.8.1 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**.

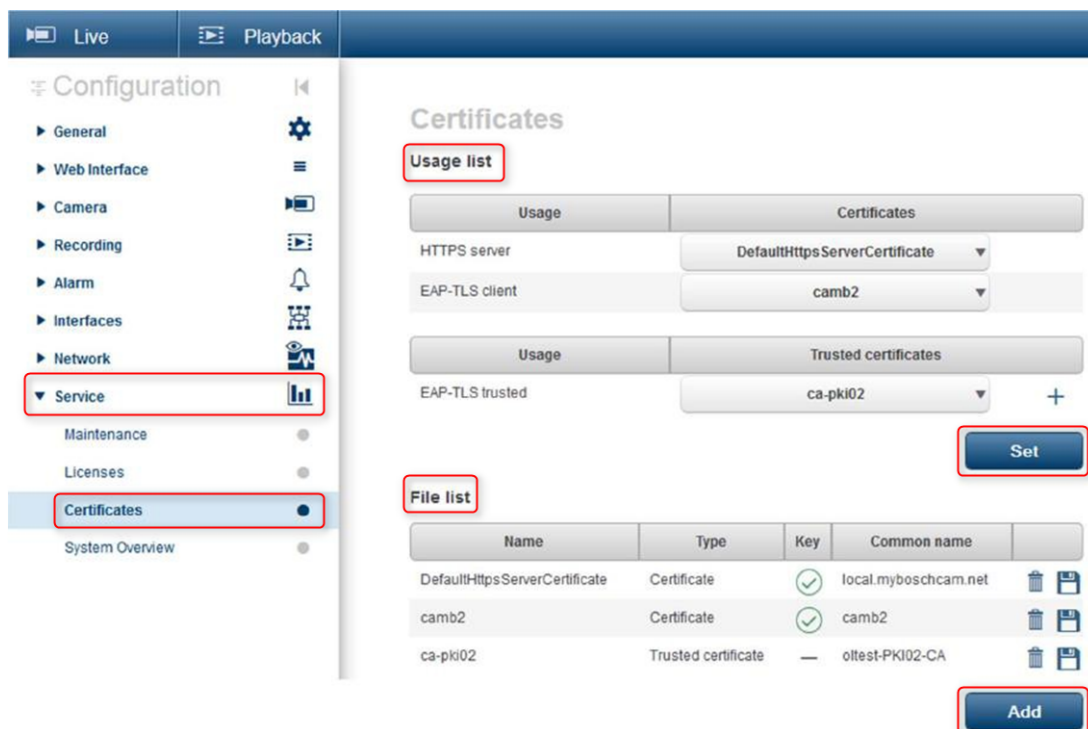


Figura 5.1: Ejemplo: los certificados EAP/TLS almacenados en una cámara Bosch (FW6.11)

Los certificados se aceptan en formato *.pem, *.cer o *.crt, y se deben estar codificados en base64. Pueden cargarse como un archivo combinado o dividirse en certificados y partes clave y cargarse en este orden como archivos independientes para volver a combinarlos automáticamente.

Desde la versión 6.20 del firmware, se admiten claves privadas PKCS#8 protegidas con contraseña (codificadas AES) que se deben cargar en formato *.pem codificadas en base64.

5.8.2 Autenticación de vídeo

Una vez que los dispositivos de un sistema están protegidos y autenticados correctamente, es importante mantener la atención también en los datos de vídeo que se les proporcionaron. El método se denomina autenticación de vídeo.

El único objetivo de la autenticación del vídeo consiste en ofrecer métodos para validar la autenticidad del mismo, y no centrarse en cuestiones relacionadas con la transmisión de vídeo o datos en modo alguno.

Antes de la versión 5.9 del firmware, las marcas de agua se realizaban mediante un sencillo algoritmo de suma de control a través del flujo de vídeo. Cuando trabajamos con marcas de agua, no se utilizan certificados ni codificación. Una suma de control es una medida de referencia de la "firmeza de los datos" de un archivo y valida la integridad del mismo.

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.

Display Stamping

Camera name stamping: Off

Logo: [?] [Browse...] [Upload]

Logo position: Off

Time stamping: Off

Display milliseconds: Off

Alarm mode stamping: Off

Alarm message: [] (max. 31 characters)

Transparent background:

Video authentication: SHA-256 (selected)

Signature interval [s]: [] [Set]



Aviso!

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.



Aviso!

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.

6 Administración de actualizaciones de seguridad

Antes de utilizar el dispositivo por primera vez, asegúrese de instalar la última versión aplicable de la versión del programa. Para una funcionalidad, compatibilidad, rendimiento y seguridad coherentes, actualice el software periódicamente durante la vida útil del dispositivo. Siga las instrucciones de la documentación del producto relativas a las actualizaciones de software.

Los siguientes enlaces ofrecen más información:

- Información general: <https://www.boschsecurity.com/xc/en/support/product-security/>
- Avisos de seguridad, una lista de vulnerabilidades identificadas y soluciones propuestas: <https://www.boschsecurity.com/xc/en/support/product-security/security-advisories.html>

Bosch no asume responsabilidad alguna por los daños ocasionados por el funcionamiento de sus productos con componentes de software obsoletos.

Puede encontrar las últimas versiones de firmware y software en la tienda de descargas de Bosch Security and Safety Systems:

<https://downloadstore.boschsecurity.com/>

En el caso de los dispositivos conectados a Remote Portal, los usuarios pueden recibir una notificación por correo electrónico sobre las actualizaciones de firmware disponibles a través del servicio de alerta remota.

Los paquetes de descarga más completos se distribuyen a través del catálogo de productos de Bosch Security and Safety Systems:

<https://www.boschsecurity.com>

7 Control de la seguridad

Debido a que los requisitos cambian constantemente, nunca se puede garantizar la seguridad al 100 %. Por lo tanto, se establece en Bosch un proceso de gestión de incidentes y vulnerabilidad estructurado para gestionar profesionalmente las posibles vulnerabilidades e incidencias de seguridad del producto.

Para nosotros, es muy importante la gestión profesional y sistemática de las vulnerabilidades notificadas, así como la transparencia hacia nuestros clientes. Por ello, se tienen que investigar todos los informes técnicos. Llevamos a cabo una evaluación de las vulnerabilidades del producto de acuerdo con el Sistema de puntuación de vulnerabilidades comunes (CVSS). CVSS es un estándar del sector abierto y gratuito para analizar la gravedad de las vulnerabilidades de seguridad de los sistemas informáticos. Las puntuaciones se calculan según una fórmula que depende de varias métricas que aproximan la facilidad de explotación y el impacto de la misma. Los marcadores oscilan entre 0 y 10, siendo 10 el más grave.

En caso de confirmación, informamos a los clientes acerca de la vulnerabilidad de seguridad identificada en el producto o solución y su recuperación mediante la publicación de un aviso de seguridad. Todos los avisos de seguridad incluyen:

- Descripción de la vulnerabilidad con referencia al estándar de Vulnerabilidades y exposiciones comunes (CVE) y la puntuación CVSS.
- Identidad de los productos y versiones de software/hardware afectados conocidos.
- Información sobre los factores de atenuación y resoluciones.
- Línea de tiempo y ubicación de las soluciones disponibles u otras medidas correctivas.

Puede encontrar la lista de avisos de seguridad publicados en nuestro sitio web: <https://www.boschsecurity.com/xc/en/support/product-security/security-advisories.html>.

Siempre que piense que ha identificado una vulnerabilidad de seguridad o cualquier otro problema de seguridad relacionado con un producto o servicio de Bosch, póngase en contacto con el Equipo de respuesta a incidentes de seguridad del producto (PSIRT) de Bosch: <https://psirt.bosch.com>.

8 Eliminación y desmantelamiento seguros

En un momento determinado del ciclo de vida de un producto o sistema, es posible que tenga que sustituir o retirar el dispositivo o un componente. Como el dispositivo o el componente pueden contener datos confidenciales, como credenciales o certificados, asegúrese de borrar estos datos de forma completa y segura.

Puede establecer los ajustes predeterminados de fábrica en la mayoría de los dispositivos. Para la mayoría de codificadores y cámaras IP, puede utilizar este botón de restablecimiento. Para los que no tengan un botón de restablecimiento, utilice la función predeterminada de fábrica a través de la interfaz web antes de desmontarlos de la red.

Todos los usuarios y sus contraseñas respectivas se suprimirán y se restablecerán los ajustes predeterminados de fábrica. También se borrarán todos los certificados y sus respectivas claves almacenadas en el TPM o elemento seguro.

Puede que en otros dispositivos haya diferentes opciones para establecerlos en el ajuste predeterminado de fábrica. Consulte en la documentación de usuario correspondiente los procedimientos de eliminación correctos.

Los servidores y las estaciones de trabajo también pueden tener certificados y credenciales almacenados. Utilice las herramientas y métodos adecuados para asegurarse de que se eliminan de forma segura los datos correctos durante el desmantelamiento o antes de la eliminación.

Se recomienda establecer los dispositivos en los ajustes predeterminados de fábrica también en caso de que se deban trasladar a otra instalación que pueda utilizar otras credenciales o certificados.

**Aviso!**

Consulte en la documentación de usuario correspondiente los procedimientos de eliminación correctos.

9 Información adicional

Para obtener más información, descargas de software y documentación, vaya a la página de producto correspondiente en el catálogo de productos:

<http://www.boschsecurity.com>

Glosario

802.1x

La norma IEEE 802.1x proporciona un método general de autenticación y autorización en redes IEEE-802. La autenticación se lleva a cabo mediante el autenticador, que comprueba la información de autenticación transmitida mediante un servidor de autenticación (consulte Servidor RADIUS) y aprueba o deniega el acceso a los servicios ofrecidos (LAN, VLAN o WLAN) según corresponda.

autenticación

Proceso de verificación de la autenticidad de una secuencia de vídeo. El usuario puede iniciar un proceso de autenticación. Si se encuentran datos no auténticos, aparece un mensaje.

DHCP

Dynamic Host Configuration Protocol, protocolo de configuración dinámica de host: utiliza un servidor adecuado para permitir la asignación dinámica de una dirección IP y otros parámetros de configuración a los ordenadores de una red (Internet o LAN)

Dirección IPv4

Un número de 4 bytes que define de forma exclusiva a cada unidad en Internet. Suele escribirse con puntos separadores; por ejemplo, "209.130.2.193".

dispositivo

Componente de hardware como una cámara, codificador/decodificador, NVR, DiBos, matriz analógica, ATM/puente POS.

Grupo de usuarios

Los grupos de usuarios se utilizan para definir atributos de usuarios comunes, como permisos, privilegios y prioridad de PTZ. Al convertirse en miembro de un grupo, un usuario hereda automáticamente todos los atributos del grupo.

HTTP

Hypertext Transfer Protocol, protocolo de transferencia de hipertexto: protocolo para la transmisión de datos por la red.

HTTPS

Hypertext Transfer Protocol Secure, protocolo seguro de transferencia de hipertexto: codifica y autentica la comunicación entre el servidor Web y un navegador.

LAN

Siglas de Local Area Network, red de área local. Se trata de una red que conecta dispositivos dentro de una zona geográfica limitada.

Máscara de red

Máscara que explica qué parte de una dirección IP es una dirección de red y qué parte es la dirección del host. Se suele escribir con puntos separadores, por ejemplo, "255.255.255.192"

Multidifusión

Comunicación que se establece entre un único transmisor y varios receptores de una red mediante la distribución de una sola secuencia de datos en la red a determinados receptores de un grupo definido. Para una operación de multidifusión, es necesaria una red compatible con la multidifusión con implementación de los protocolos UDP e IGMP.

ONVIF

ONVIF (Open Network Video Interface Forum, Foro abierto de interfaces de vídeo en red). Estándar global para los productos de vídeo en red. Los dispositivos que cumplen con ONVIF permiten intercambiar vídeo en directo, audio, metadatos, controlar información y garantizar su detección y conexión automática a las aplicaciones en red tales como los sistemas de gestión de vídeo.

RCP+

Protocolo de control remoto: un protocolo propio de Bosch que utiliza puertos estáticos específicos para detectar y comunicarse con dispositivos de vídeo IP de Bosch.

Red de área extensa

Enlace de gran alcance que se emplea para ampliar o conectar redes de área local ubicadas remotamente.

refuerzo

Proceso de aumento de la seguridad de un sistema utilizando solo software dedicado que es necesario para el funcionamiento del sistema, aplicando ajustes de protección específicos y eliminando el software que no es obligatorio.

RTSP

Siglas de Real Time Streaming Protocol, protocolo de transmisión por secuencias en tiempo real. Un protocolo de red que permite controlar la transmisión continua de software o datos de audio e imágenes en redes IP.

Servidor RADIUS

Remote Authentication Dial-in User Service, Servicio de usuario de autenticación de marcación remota: es un protocolo cliente-servidor para la autenticación, autorización y cuentas de usuarios en conexiones por marcación para redes de ordenadores. RADIUS es el estándar establecido para la autenticación centralizada de las conexiones por marcación a través del módem, ISDN, VPN, LAN inalámbricas (consulte 802.1x) y DSL.

SNMP

Simple Network Management Protocol, protocolo simple de gestión de redes: para la gestión de redes y administración y control de los componentes de redes.

SSL

Secure Sockets Layer (Capa de sockets seguros): un protocolo de codificación obsoleto para la transmisión de datos en redes basadas en IP (véase TLS).

TCP

Protocolo de control de transmisión Protocolo de comunicación, orientado a las conexiones, que se utiliza para transmitir datos a través de una red IP. Ofrece una transmisión de datos fiable y ordenada.

Telnet

Protocolo de inicio de sesión con el que los usuarios pueden acceder a un equipo remoto (host) en Internet.

TLS

Seguridad de capa de transporte. TLS 1.0 y 1.1 son las versiones avanzadas estándar de SSL 3.0 (consulte SSL). Los dispositivos modernos utilizan TLS 1.2 o 1.3

TTL

Time-To-Live, período de vida: ciclo vital de un paquete de datos en transferencias de estación.

UDP

Siglas de User Datagram Protocol, protocolo de datagrama de usuario. Protocolo sin conexión utilizado para intercambiar datos por una red IP. El UDP es más eficaz que el TCP para la transmisión de vídeo debido a su menor sobrecarga.

VPN

Una red privada virtual (VPN) implementa una red privada en una red pública, como Internet. El tráfico de red dentro de la VPN se codifica y de esta forma se encuentra protegido contra el espionaje.

Bosch Sicherheitssysteme GmbH

Robert-Bosch-Ring 5

85630 Grasbrunn

Germany

www.boschsecurity.com

© Bosch Sicherheitssysteme GmbH, 2023

Building solutions for a better life.

202302091959