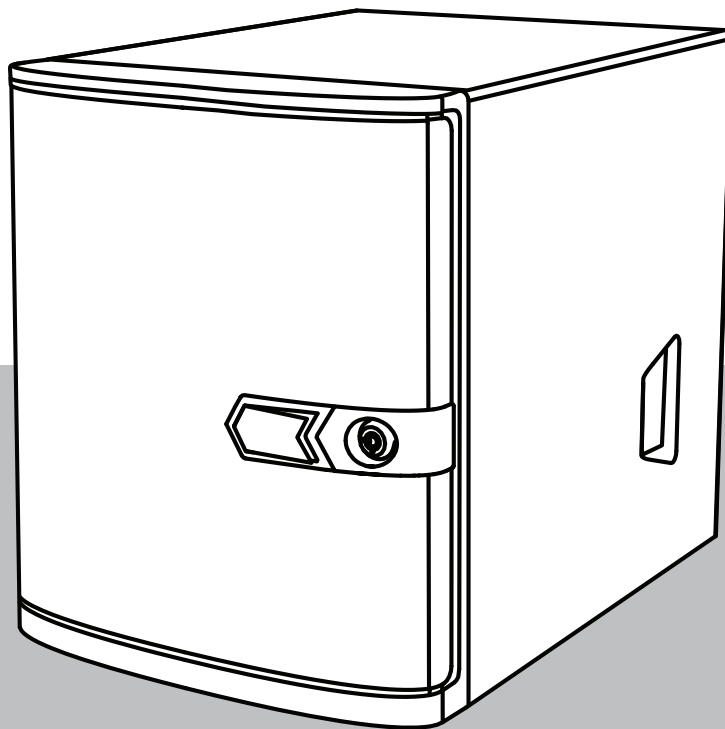


DIVAR IP all-in-one 4000

DIP-4420IG-00N | DIP-4424IG-2HD | DIP-4428IG-2HD |
DIP-442IIG-2HD



Contenido

1	Seguridad	4
1.1	Precauciones de uso	4
1.2	Precauciones de seguridad informática	5
1.3	Precauciones de software	6
1.3.1	Usar el software más reciente	6
1.3.2	Información de la OSS	6
2	Introducción	7
3	Descripción del sistema	8
4	Configuración del sistema	9
4.1	Ajustes predeterminados	9
4.2	Requisitos previos	9
4.3	Primer inicio de sesión y configuración inicial del sistema	9
4.3.1	Elegir el modo de operación BVMS	11
4.3.2	Elegir el modo de funcionamiento VRM	12
4.3.3	Elección del modo de funcionamiento de almacenamiento iSCSI	12
5	Mejora de software	13
6	Conexión remota al sistema	15
6.1	Proteger el sistema frente al acceso no autorizado	15
6.2	Configuración del reenvío de puertos	15
6.3	Selección de un cliente adecuado	15
6.3.1	Conexión remota con BVMS Operator Client.	15
6.3.2	Conexión remota con la aplicación Video Security	16
6.4	Conexión a un Enterprise Management Server	16
7	Mantenimiento	17
7.1	Inicio de sesión en la cuenta de administrador	17
7.2	Supervisión del sistema	17
7.3	Sustitución de un disco duro defectuoso y configuración de un disco duro nuevo	17
7.3.1	Sustitución de un disco duro defectuoso	18
7.3.2	Configuración de un disco duro nuevo	18
7.4	Recopilación de los archivos de registro de DIVAR IP System Manager	20
7.5	Recuperación de la unidad	20
8	Información adicional	22
8.1	Software cliente y documentación adicional	22
8.2	Servicios de asistencia y Bosch Academy	22

1 Seguridad

Tenga en cuenta las precauciones de seguridad de este capítulo.

1.1 Precauciones de uso

**Aviso!**

Uso recomendado

Este producto es exclusivamente para uso profesional. No está diseñado para instalarse en un lugar público al que pueda acceder la población general.

**Aviso!**

No utilice este producto en lugares húmedos o mojados.

**Aviso!**

Tome precauciones para proteger el dispositivo de picos de tensión y caídas de rayos.

**Aviso!**

Mantenga el área alrededor del dispositivo limpia y despejada.

**Aviso!**

Aberturas de la carcasa

No bloquee ni cubra las aberturas. Las aberturas de la carcasa tienen como objeto ventilar la carcasa. Estas aberturas evitarán el sobrecalentamiento y garantizarán un funcionamiento de confianza.

**Aviso!**

No abra ni retire la cubierta del dispositivo. Si se abre o se retira la cubierta, podría dañar el sistema y anular la garantía.

**Aviso!**

No derrame líquidos sobre el dispositivo.

**Advertencia!**

Tenga cuidado cuando realice trabajos de mantenimiento y reparación en el panel posterior. Hay tensión peligrosa en el panel posterior cuando el sistema está en funcionamiento. No toque el panel posterior con ningún objeto metálico y asegúrese de que ninguno de los cables planos lo toque.

**Aviso!**

Antes de mover el producto, desconecte el cable de alimentación. Desplace el producto con cuidado. Una fuerza excesiva o los golpes podrían dañar el producto y las unidades de disco duro.

**Advertencia!**

La manipulación de materiales con soldaduras de plomo que se utilizan en este producto puede exponerle al plomo, un elemento químico del que el Estado de California tiene constancia de que ocasiona defectos en los nacimientos y otras lesiones reproductivas.

**Aviso!**

Dado que la pérdida de vídeo es un elemento inherente a la grabación de vídeo digital, Bosch Security Systems no se hace responsable de ningún daño derivado de la pérdida de información de vídeo.

Para minimizar el riesgo de pérdida de información, se recomienda la implementación de varios sistemas de grabación redundantes, así como el uso de un procedimiento para realizar copias de seguridad de toda la información analógica y digital.

1.2**Precauciones de seguridad informática**

Por motivos de seguridad informática, tenga en cuenta lo siguiente:

- Asegúrese de que el acceso físico al sistema esté limitado exclusivamente al personal autorizado. Coloque el sistema en una zona protegida con control de acceso para evitar manipulaciones físicas.
- Bloquee el panel frontal para protegerlo frente a la extracción no autorizada de los discos duros. Quite siempre la llave de la cerradura y guárdela en un lugar seguro.
- Use el cerrojo del chasis trasero o la ranura Kensington para garantizar una mayor seguridad para el dispositivo.
- El sistema operativo incluye los últimos parches de seguridad de Windows disponibles en el momento en que se creó la imagen de software. Utilice la función de actualización de Windows en línea o los correspondientes parches mensuales de instalación sin conexión para instalar periódicamente las actualizaciones de seguridad del sistema operativo.
- No desactive Windows Defender ni el cortafuegos de Windows y manténgalo siempre actualizado.
- No instale software antivirus adicional.
- No facilite información del sistema ni datos confidenciales a personas que no conozca a menos que esté seguro de que cuentan con autorización.
- No envíe información confidencial a través de Internet antes de comprobar la seguridad de un sitio Web.
- Limite el acceso a la red local solo a dispositivos de confianza. Los detalles se describen en los siguientes documentos, que están disponibles en el catálogo de productos en línea:
 - *Autenticación de red 802.1X*
 - *Guía de seguridad informática de los productos de vídeo IP de Bosch*
- Para tener acceso mediante redes públicas, utilice únicamente los canales de comunicación (cifrados) seguros.
- La cuenta de administrador proporciona privilegios administrativos completos y acceso no restringido al sistema. Los derechos de administrador permiten a los usuarios instalar, actualizar o eliminar software y cambiar los ajustes de configuración. Además, los derechos de administrador permiten a los usuarios acceder y cambiar directamente las claves del registro, anulando así la administración central y los ajustes de seguridad. Los usuarios que han iniciado sesión en la cuenta de administrador pueden traspasar cortafuegos y eliminar software de antivirus, lo que expondrá el sistema a virus y ataques

informáticos. Esto puede suponer un riesgo grave para la seguridad del sistema y de los datos.

Para minimizar los riesgos de seguridad informática, tenga en cuenta lo siguiente:

- Asegúrese de que la cuenta de administrador esté protegida con una contraseña compleja acorde con la política de contraseñas.
- Asegúrese de que solo un número limitado de usuarios de confianza tenga acceso a la cuenta de administrador.
- Debido a los requisitos de funcionamiento, la unidad del sistema no se debe codificar. Sin codificación, se puede acceder a los datos almacenados en esta unidad y eliminarlos con facilidad. Para evitar robos o pérdidas accidentales de datos, asegúrese de que solo tengan acceso al sistema y a la cuenta de administrador personas autorizadas.
- A fin de instalar y actualizar el software, así como para la recuperación del sistema, es posible que tenga que utilizar dispositivos USB. Por lo tanto, los puertos USB del sistema no se deben deshabilitar. No obstante, la conexión de dispositivos USB al sistema supone un riesgo de infección por malware. Para evitar ataques de malware, asegúrese de que no hay dispositivos USB infectados conectados al sistema.

1.3 Precauciones de software

1.3.1 Usar el software más reciente

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 el software más reciente y los paquetes de actualización disponibles en la tienda de descargas de Bosch Security and Safety Systems en:

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

1.3.2 Información de la OSS

Bosch utiliza software de código abierto (Open Source Software) en los productos DIVAR IP all-in-one.

Encontrará las licencias de los componentes de software de código abierto utilizados en la unidad del sistema en:

```
C:\license txt\
```

Las licencias de los componentes de software de código abierto que se utilizan en cualquier otro software instalado en su sistema están guardadas en la carpeta de instalación del software correspondiente; por ejemplo, en:

```
C:\Program Files\Bosch\SysMgmService\apps\sysmgm-commander\[version]\License
```

o en:

```
C:\Program Files\Bosch\SysMgmService\apps\sysmgm-executor\[version]\License
```

2 Introducción

DIVAR IP all-in-one 4000 es una solución todo en uno asequible y fácil de utilizar para grabar, visualizar y gestionar sistemas de vigilancia en red de hasta 32 canales (con 8 canales prelicenciados incluidos).

El DIVAR IP all-in-one 4000 es una unidad minitorre de 2 módulos que combina capacidades de Bosch Video Management System avanzadas y gestión de grabaciones de vanguardia en un único dispositivo de grabación IP rentable, práctico de instalar y de usar diseñado para clientes que buscan soluciones de TI.

DIVAR IP all-in-one 4000 utiliza un diseño integrado y componentes básicos y se basa en el sistema operativo Microsoft Windows Server IoT 2022 for Storage Workgroup.

DIVAR IP all-in-one 4000 dispone de discos duros SATA reemplazables desde la parte frontal de altas prestaciones que proporcionan 36 TB de capacidad de almacenamiento bruto.

3 Descripción del sistema

Sistema operativo

El sistema operativo Microsoft Windows Server IoT 2022 for Storage Workgroup proporciona una interfaz de usuario para la configuración inicial del servidor, así como una gestión unificada de los dispositivos de almacenamiento, una configuración y gestión simplificadas del espacio de almacenamiento y compatibilidad con Microsoft iSCSI Software Target. Estos sistemas están especialmente diseñados para ofrecer un rendimiento óptimo del almacenamiento en red. El sistema operativo Microsoft Windows Server IoT 2022 for Storage Workgroup proporciona unas mejoras significativas en cuanto a la gestión del almacenamiento, así como integración de los componentes y funciones de gestión de los dispositivos de almacenamiento.

DIVAR IP System Manager

La aplicación DIVAR IP System Manager es la interfaz de usuario central que facilita la instalación, configuración y actualización del sistema.

Modos de funcionamiento

Los sistemas DIVAR IP all-in-one 4000 pueden funcionar en tres modos diferentes:

- Sistema de gestión y grabación de vídeo completo que utiliza los componentes y servicios clave de BVMS y Video Recording Manager.
Este modo ofrece una solución de seguridad de vídeo IP avanzada única que proporciona una gestión totalmente integrada de vídeo digital, audio y datos en una red IP. Combina perfectamente cámaras IP y codificadores, proporciona gestión de alarmas y eventos del sistema, control del estado del sistema y gestión de prioridades y usuarios. Este modo proporciona el mejor sistema de gestión de vídeo para los dispositivos de videovigilancia de Bosch, ya que aprovecha las capacidades exclusivas de las cámaras y las soluciones de grabación de Bosch. Incluye componentes de Video Streaming Gateway para integrar cámaras de terceros.
- Sistema de grabación de vídeo simple que utiliza los componentes y servicios clave de Video Recording Manager, aprovechando las capacidades exclusivas de las cámaras y las soluciones de grabación de Bosch.
- Ampliación de almacenamiento iSCSI para un sistema BVMS o Video Recording Manager que se ejecuta en un hardware diferente. Se pueden añadir hasta dos de estas ampliaciones de almacenamiento iSCSI a un sistema BVMS o Video Recording Manager que se ejecuta en un DIVAR IP all-in-one 4000.

Al configurar el sistema, en la aplicación DIVAR IP System Manager, debe elegir el modo de operación que desea para configurar el sistema.

Con la aplicación DIVAR IP System Manager, también puede actualizar y mejorar el software instalado.

Puede encontrar el software más reciente y los paquetes de actualización disponibles en la tienda de descargas de Bosch Security and Safety Systems en:

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



Aviso!

Las secuencias de vídeo grabadas deben configurarse de forma que no se supere el ancho de banda máximo del sistema (sistema base BVMS/VRM más las expansiones de almacenamiento iSCSI).

4 Configuración del sistema

4.1 Ajustes predeterminados

Todos los sistemas DIVAR IP están preconfigurados con una dirección IP y unos ajustes iSCSI predeterminados:

- Dirección IP: automáticamente asignada por DHCP (dirección IP de respaldo: 192.168.0.200).
- Máscara de subred: asignada por DHCP de forma automática (máscara de subred de respaldo: 255.255.255.0).

Ajustes predeterminados del usuario para la cuenta de administrador

- Nombre de usuario: **BVRAdmin**
- Contraseña: se debe establecer la primera vez que se inicia sesión.
Requisitos de contraseña:
 - 14 caracteres como mínimo.
 - Al menos una letra en mayúsculas.
 - Al menos una letra en minúsculas.
 - Al menos un dígito.

4.2 Requisitos previos

Tenga en cuenta lo siguiente:

- DIVAR IP debe tener un enlace de red activa durante la instalación. Asegúrese de que el conmutador de red que está intentando conectar está encendido.
- La dirección IP predeterminada no debe estar ocupada por ningún otro dispositivo de la red. Asegúrese de que las direcciones IP predeterminadas de sistemas DIVAR IP existentes en la red se cambian antes de añadir otra DIVAR IP.

4.3 Primer inicio de sesión y configuración inicial del sistema



Aviso!

No cambie los ajustes del sistema operativo. Si cambia los ajustes del sistema operativo, podría producirse un fallo de funcionamiento del sistema.



Aviso!

Para llevar a cabo tareas administrativas, debe iniciar sesión en la cuenta de administrador.



Aviso!

En caso de pérdida de la contraseña, se deberá realizar una recuperación del sistema como se describe en el manual de instalación. La configuración se debe realizar desde cero o importarse.

Para configurar el sistema:


1. Conecte la unidad DIVAR IP all-in-one y las cámaras a la red.
2. Encienda la unidad.

Se realizan rutinas de configuración para Microsoft Windows Server IoT 2022 for Storage Workgroup. Este proceso puede tardar varios minutos. No apague el sistema.

Una vez completado el proceso, se muestra la pantalla de selección de idioma de Windows.

3. Seleccione su país o región, el idioma del sistema operativo deseado y la distribución del teclado en la lista y, a continuación, haga clic en **Siguiente**.
Se muestran los términos de licencia del software de Microsoft.
4. Haga clic en **Aceptar** para aceptar los términos de licencia y espere hasta que se reinicie Windows. Esto puede tardar varios minutos. No apague el sistema.
Después de reiniciar, se muestra la página de inicio de sesión de Windows.
5. Establezca una nueva contraseña para la cuenta del administrador **BVRAdmin** y confírmela.
Requisitos de contraseña:
 - 14 caracteres como mínimo.
 - Al menos una letra en mayúsculas.
 - Al menos una letra en minúsculas.
 - Al menos un dígito.A continuación, pulse Entrar.
Se muestra la página **Software Selection**.
6. El sistema explora de forma automática la unidad local y los medios de almacenamiento externos conectados para localizar el archivo de instalación de DIVAR IP System Manager **SystemManager_x64_[software version].exe**, que se encuentra en una carpeta con la estructura siguiente: *Drive root\BoschAppliance*.
La exploración puede llevar algún tiempo. Espere a que finalice.
7. Una vez que el sistema ha detectado el archivo de instalación, se muestra en la página **Software Selection**. Haga clic en la barra que muestra el archivo de instalación para iniciar la instalación.
8. Si durante el proceso de análisis no se encuentra el archivo de instalación, haga lo siguiente:
 - Vaya a <https://downloadstore.boschsecurity.com/>.
 - En la pestaña **Software**, seleccione **BVMS Appliances** de la lista y, a continuación, haga clic en **Select**.
Aparece una lista de todos los paquetes de software disponibles.
 - Localice el archivo ZIP **SystemManager_[software version].zip** y guárdelo en un soporte de almacenamiento como una memoria USB.
 - Descomprima el archivo en el soporte de almacenamiento asegurándose de que la carpeta **BoschAppliance** se encuentra en la raíz del soporte de almacenamiento.
 - Conecte el soporte de almacenamiento a su sistema DIVAR IP all-in-one.
El sistema explorará automáticamente el soporte de almacenamiento en busca del archivo de instalación.
La exploración puede llevar algún tiempo. Espere a que finalice.
 - Una vez detectado el archivo de instalación, se mostrará en la página **Software Selection**. Haga clic en la barra que muestra el archivo de instalación para iniciar la instalación.

Nota: para que se detecte automáticamente, el archivo de instalación debe encontrarse en una carpeta con la siguiente estructura: *Drive root\BoschAppliance* (por ejemplo *F:\BoschAppliance*).

Si el archivo de instalación se encuentra en otra ubicación que no coincide con la estructura de carpetas predefinida, haga clic en  para desplazarse hasta la ubicación correspondiente. Después, haga clic en el archivo de instalación para iniciar la instalación.

9. Antes de que se inicie la instalación, se muestra el cuadro de diálogo **End User License Agreement (EULA)**. Lea los términos de licencia y, a continuación, haga clic en **Accept** para continuar. La instalación se inicia.
10. Una vez completada la instalación, el sistema se reinicia y se abre la página de inicio de sesión de Windows. Inicio de sesión en la cuenta de administrador.
11. Se abre el navegador Microsoft Edge y se muestra la página **DIVAR IP - Configuración del sistema**. La página muestra el tipo de dispositivo y el número de serie del dispositivo, así como los tres modos de funcionamiento y las versiones de software disponibles para cada modo de funcionamiento.

Debe elegir el modo de funcionamiento deseado y la versión de software deseada para configurar su sistema DIVAR IP all-in-one.

Nota: si la versión de software deseada para el modo de funcionamiento correspondiente no está disponible en una unidad local, haga lo siguiente:

- Vaya a <https://downloadstore.boschsecurity.com/>.
- En la pestaña **Software**, seleccione **BVMS Appliances** de la lista y, a continuación, haga clic en **Select**.
Aparece una lista de todos los paquetes de software disponibles.
- Localice los archivos ZIP de los paquetes de software deseados, por ejemplo **BVMS_[BVMS version]_SystemManager_package_[package version].zip** y guárdelos en un soporte de almacenamiento, como una memoria USB.
- Descomprima los archivos en el soporte de almacenamiento. No cambie la estructura de carpetas de los archivos descomprimidos.
- Conecte el soporte de almacenamiento a su sistema DIVAR IP all-in-one.



Aviso!

Cambiar el modo de funcionamiento después de la instalación requiere un restablecimiento completo de fábrica.

4.3.1

Elegir el modo de operación BVMS

Para que funcione el sistema DIVAR IP all-in-one como un sistema de grabación y gestión de vídeo completo:

1. En la página **DIVAR IP - Configuración del sistema**, seleccione el modo de funcionamiento **BVMS** y la versión deseada BVMS que desea instalar, a continuación, haga clic en **Siguiente**.
Se muestra el contrato de licencia de BVMS.
2. Lea y acepte el contrato de licencia y, a continuación, haga clic en **Instalar** para continuar.
La instalación se inicia y el cuadro de diálogo de instalación muestra el progreso de la instalación. No apague el sistema y no retire los medios de almacenamiento durante el proceso de instalación.
3. Una vez que se han instalado correctamente todos los paquetes de software, el sistema se reinicia. Después del reinicio, se le dirigirá al escritorio de BVMS.
4. En el escritorio de BVMS, haga clic en la aplicación deseada para configurar el sistema.



Aviso!

Para obtener más información, consulte la formación basada en web DIVAR IP all-in-one correspondiente y la documentación de BVMS.

Puede encontrar la formación en: www.boschsecurity.com/xc/en/support/training/

4.3.2 Elegir el modo de funcionamiento VRM

Para utilizar el sistema DIVAR IP all-in-one solo como sistema de grabación de vídeo:

1. En la página **DIVAR IP - Configuración del sistema**, seleccione el modo de funcionamiento **VRM** y la versión deseada VRM que desea instalar, a continuación, haga clic en **Siguiente**.
Se muestra el contrato de licencia de VRM.
2. Lea y acepte el contrato de licencia y, a continuación, haga clic en **Instalar** para continuar.
La instalación se inicia y el cuadro de diálogo de instalación muestra el progreso de la instalación. No apague el sistema y no retire los medios de almacenamiento durante el proceso de instalación.
3. Una vez que se han instalado correctamente todos los paquetes de software, el sistema se reinicia. Después del reinicio, se le dirigirá a la pantalla de inicio de sesión de Windows.



Aviso!

Si desea más información, consulte la documentación de VRM.

4.3.3 Elección del modo de funcionamiento de almacenamiento iSCSI

Para operar el sistema DIVAR IP all-in-one como una ampliación de almacenamiento iSCSI:

1. En la página **DIVAR IP - Configuración del sistema**, seleccione el modo de funcionamiento de **almacenamiento iSCSI** y la versión de almacenamiento iSCSI que desee instalar, a continuación, haga clic en **Siguiente**.
Se muestra el cuadro de diálogo de instalación.
2. En el cuadro de diálogo de instalación, haga clic en **Instalar** para continuar.
La instalación se inicia y el cuadro de diálogo de instalación muestra el progreso de la instalación. No apague el sistema y no retire los medios de almacenamiento durante el proceso de instalación.
3. Una vez que se han instalado correctamente todos los paquetes de software, el sistema se reinicia. Después del reinicio, se le dirigirá a la pantalla de inicio de sesión de Windows.
4. Agregar el sistema como ampliación de almacenamiento iSCSI a un servidor externo BVMS o VRM con BVMS Configuration Client o Configuration Manager.



Aviso!

Si desea más información, consulte la documentación de BVMS or Configuration Manager.

5 Mejora de software

Con la aplicación DIVAR IP System Manager, puede actualizar el software instalado en el sistema.

Puede encontrar el software más reciente y los paquetes de actualización disponibles en la tienda de descargas de Bosch Security and Safety Systems en:


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



Aviso!



No se admite la actualización del software instalado a una versión anterior.

Para mejorar el software instalado:

1. Vaya a <https://downloadstore.boschsecurity.com/>.
2. En la pestaña **Software**, seleccione **BVMS Appliances** de la lista y, a continuación, haga clic en **Select**.
Aparece una lista de todos los paquetes de software disponibles.
3. Localice los archivos ZIP de los paquetes de software deseados, por ejemplo **BVMS_[BVMS version]_SystemManager_package_[package version].zip** y guárdelos en un soporte de almacenamiento, como una memoria USB.
4. Descomprima los archivos en el soporte de almacenamiento. No cambie la estructura de carpetas de los archivos descomprimidos.
5. Inicie la aplicación DIVAR IP System Manager:
 - Si ha iniciado sesión en Windows con la cuenta de administrador **BVRAdmin**, haga doble clic en el icono de DIVAR IP System Manager.
Se inicia la aplicación DIVAR IP System Manager.
 - Si el sistema se está ejecutando en modo de funcionamiento BVMS, haga clic en el icono DIVAR IP System Manager en el escritorio de BVMS e inicie sesión en la cuenta BVRAdmin de administrador. La aplicación DIVAR IP System Manager se abre en un cuadro de diálogo de pantalla completa (para salir del cuadro de diálogo, pulse la tecla Alt+ F4).
6. Se abre la página **Paquetes de software**, que muestra el tipo de dispositivo y el número de serie en la parte superior de la página.
 - En la columna **Nombre**, verá todas las aplicaciones de software de DIVAR IP System Manager ya instaladas en el sistema y todas las demás aplicaciones de software de DIVAR IP System Manager detectadas en el sistema, en la unidad **Images** o en medios de almacenamiento.
 - En la columna **Versión instalada**, verá la versión de la aplicación de software que está instalada en el sistema.
 - En la columna **Estado**, verá el estado de la aplicación de software correspondiente:
 - El icono  indica que el sistema no ha detectado ninguna versión más reciente de la aplicación de software en la unidad de **Images** ni en medios de almacenamiento.

Nota: Para asegurarse de que utiliza la versión de software más reciente, revise las versiones de software disponibles en el almacén de descargas de Bosch Security and Safety Systems en:

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

- El icono  indica que el sistema ha detectado versiones más recientes de la aplicación de software en la unidad de **Images** o en algún medio de almacenamiento. También se muestra el icono si el sistema ha encontrado una aplicación de software que todavía no está instalada en su sistema.
- En la columna **Versión disponible**, verá las versiones posteriores de las aplicaciones de software instaladas. El sistema ha detectado estas versiones en la unidad **Images** o en un medio de almacenamiento.
La columna también muestra las versiones disponibles de las aplicaciones de software detectadas que todavía no se han instalado en el sistema.
Nota: solo se muestran versiones posteriores de las aplicaciones de software instaladas. No se admite la actualización de una aplicación de software instalada a una versión anterior.
- 7. En la columna **Nombre**, haga clic en el botón de la opción correspondiente para seleccionar la aplicación de software que desea actualizar o instalar.
- 8. En la columna **Versión disponible**, seleccione la versión a la que desea actualizar la aplicación de software, o la que desea instalar, y haga clic en **Siguiente**.
Si corresponde, verá un cuadro de diálogo de acuerdo de licencia.
- 9. Lea y acepte el contrato de licencia y, a continuación, haga clic en **Instalar** para continuar.
Se inicia la instalación y el cuadro de diálogo de instalación muestra el progreso. No apague el sistema y no retire los medios de almacenamiento durante el proceso de instalación.
- 10. Después de instalar correctamente todos los paquetes de software, verá el mensaje **Instalación finalizada correctamente** en la parte superior de la página.
- 11. Si no se ha realizado la instalación correctamente, verá el mensaje **No se ha podido instalar** y el icono . En este caso, pulse F5 para volver a la página **Paquetes de software**. Vuelva a descargar los paquetes de software correspondientes e inténtelo de nuevo.
Si el problema persiste, póngase en contacto con el servicio de asistencia técnica.

6 Conexión remota al sistema

Puede realizar una conexión remota a su sistema DIVAR IP all-in-one y acceder a él por Internet.

Para crear una conexión remota, haga lo siguiente:

1. *Proteger el sistema frente al acceso no autorizado, Página 15.*
2. *Configuración del reenvío de puertos, Página 15.*
3. *Selección de un cliente adecuado, Página 15.*

6.1 Proteger el sistema frente al acceso no autorizado

Para proteger el sistema frente a accesos no autorizados, asegúrese de seguir reglas para contraseñas seguras antes de conectar el sistema a Internet. Cuanto más segura sea la contraseña, más protegido estará su sistema del acceso de personas no autorizadas y de malware.

6.2 Configuración del reenvío de puertos

Para acceder a un sistema DIVAR IP all-in-one desde Internet a través de un router compatible con NAT/PAT, es necesario configurar el reenvío de puertos en el sistema DIVAR IP all-in-one y en el router.

Para configurar el reenvío de puertos:

- ▶ Introduzca las siguientes reglas de puerto en la configuración de reenvío de puertos de su router de Internet:
 - Puerto 5322 para túnel SSH mediante BVMS Operator Client.
Nota: esta conexión solo se aplica al modo de funcionamiento BVMS.
 - puerto 443 para el acceso de HTTPS a VRM con Video Security Client o Video Security App.
Nota: esta conexión solo se aplica al modo de funcionamiento BVMS o VRM.

Ahora se puede acceder a DIVAR IP all-in-one a través de Internet.

6.3 Selección de un cliente adecuado

Hay dos opciones para realizar una conexión remota con un sistema DIVAR IP all-in-one:

- *Conexión remota con BVMS Operator Client., Página 15.*
- *Conexión remota con la aplicación Video Security, Página 16.*



Aviso!

La compatibilidad de las versiones de BVMS Operator Client o Video Security App viene determinada por las versiones del software BVMS o VRM instaladas en DIVAR IP.

Para obtener información detallada, consulte la documentación y el material de formación del software correspondiente.

6.3.1 Conexión remota con BVMS Operator Client.




Aviso!

Esta conexión solo se aplica al modo de funcionamiento BVMS.

Para establecer una conexión remota con BVMS Operator Client:

1. Instale BVMS Operator Client en la estación de trabajo del cliente.

- Una vez finalizada la instalación correctamente, inicie Operator Client utilizando el acceso directo del Escritorio .
- Introduzca la información siguiente y haga clic en **Aceptar**.
Nombre de usuario: admin (u otro usuario, si se ha configurado)
Contraseña: contraseña del usuario
Conexión:ssh://[dirección-IP-pública-de-DIVAR-IP_all-in-one]:5322

6.3.2 Conexión remota con la aplicación Video Security



Aviso!

Esta conexión solo se aplica al modo de funcionamiento BVMS o VRM.

Para establecer una conexión remota con Video Security App:

- Busque en la App Store de Apple Bosch Video Security.
- Instale la aplicación Video Security en su dispositivo iOS.
- Inicie la aplicación Video Security.
- Seleccione **Añadir**.
- Introduzca la dirección IP pública o el nombre dynDNS.
- Asegúrese de que está activada la conexión segura (SSL).
- Seleccione **Añadir**.
- Introduzca lo siguiente:
Nombre de usuario: admin (u otro usuario, si se ha configurado)
Contraseña: contraseña del usuario

6.4 Conexión a un Enterprise Management Server

Para gestionar más de un sistema DIVAR IP all-in-one de forma centralizada en modo de BVMS puede utilizar un BVMS Enterprise Management Server instalado en un servidor aparte. Para obtener información detallada sobre la configuración y el funcionamiento de BVMS Enterprise System, consulte la documentación y el material de formación de BVMS.

7 Mantenimiento

7.1 Inicio de sesión en la cuenta de administrador

Inicio de sesión en la cuenta de administrador en modo de funcionamiento BVMS

Para iniciar sesión en la cuenta de administrador en modo de funcionamiento BVMS:

1. En el escritorio de BVMS, pulse Ctrl+Alt+Supr.
2. Mantenga pulsada la tecla izquierda Mayús. inmediatamente después de hacer clic en **Cambiar usuario**.
3. Vuelva a pulsar Ctrl+Alt+Supr.
4. Seleccione el usuario **BVRAdmin** e introduzca la contraseña establecida durante la configuración del sistema. A continuación, pulse Entrar.

Nota: para volver al escritorio de BVMS, pulse Ctrl+Alt+Supr y haga clic en **Cambiar usuario** o **Salir**. El sistema volverá automáticamente al escritorio de BVMS sin reiniciar el sistema.

Inicio de sesión en la cuenta de administrador en modo de funcionamiento VRM o iSCSI

Para iniciar sesión en la cuenta de administrador en modo de funcionamiento VRM o iSCSI:

- ▶ En la pantalla de inicio de sesión de Windows, pulse Ctrl+Alt+Supr e introduzca la contraseña de **BVRAdmin**.

7.2 Supervisión del sistema

Los sistemas DIVAR IP all-in-one llevan la aplicación **SuperDoctor** preinstalada; esta aplicación se puede usar para monitorizar el sistema.

Activar la función de monitorización

Para activar la función de monitorización:

1. Inicie sesión con la cuenta de administrador (consulte *Inicio de sesión en la cuenta de administrador, Página 17*).
2. En el escritorio, en la carpeta **Tools**, haga clic con el botón derecho del ratón en el script **startSD5Service** y, a continuación, haga clic en **Run with PowerShell**.
3. Haga doble clic en el icono **SuperDoctor 5 Web** en el escritorio.
4. Inicie sesión en la interfaz web utilizando las credenciales predeterminadas siguientes:
 - Nombre de usuario: **admin**
 - Contraseña: **DivaripSD5**
5. Haga clic en la pestaña **Configuration** y, a continuación, haga clic en **Account Setting** y cambie la contraseña predeterminada.

Nota: Bosch recomienda encarecidamente cambiar la contraseña predeterminada inmediatamente después del primer inicio de sesión en la aplicación **SuperDoctor**.
6. En la pestaña **Configuration**, haga clic en **Alert Configuration**.
7. Active la función **SNMP Trap** y especifique la dirección IP del receptor de capturas SNMP.

Desactivar la función de monitorización

Para desactivar la función de monitorización:

1. Inicie sesión con la cuenta de administrador (consulte *Inicio de sesión en la cuenta de administrador, Página 17*).
2. En el escritorio, en la carpeta **Tools**, haga clic con el botón derecho del ratón en el script **stopSD5Service** y, a continuación, haga clic en **Run with PowerShell**.

7.3 Sustitución de un disco duro defectuoso y configuración de un disco duro nuevo

Si un disco duro que está instalado en el sistema DIVAR IP all-in-one está defectuoso y no se puede utilizar más tiempo, debe hacer lo siguiente:

1. *Sustitución de un disco duro defectuoso, Página 18.*
2. *Configuración de un disco duro nuevo, Página 18.*

**Aviso!**

Bosch no se responsabiliza de pérdidas de datos, daños ni fallos del sistema de unidades que dispongan de discos duros que no haya suministrado Bosch. Bosch no puede proporcionar asistencia si se considera que los discos duros no suministrados por Bosch son la causa del problema. Para solucionar posibles problemas de hardware, Bosch requerirá la instalación de discos duros suministrados por Bosch.

7.3.1**Sustitución de un disco duro defectuoso**

Para sustituir un disco duro defectuoso:

1. Apague la unidad DIVAR IP all-in-one.
2. Retire el disco duro defectuoso de la unidad e instale el nuevo.
Consulte el capítulo *Instalación de un disco duro SATA* en el manual de instalación.

7.3.2**Configuración de un disco duro nuevo**

Para configurar un nuevo disco duro, debe hacer lo siguiente:

1. *Creación de nueva partición y volumen, Página 18*
2. *Habilitación del servicio de servidor, Página 19.*
3. *Creación de LUN (discos virtuales iSCSI), Página 19.*
4. *Deshabilitación del servicio de servidor, Página 20.*
5. *Formateo de LUN, Página 20.*

Creación de nueva partición y volumen

Para crear la nueva partición y volumen:

1. En el menú **Inicio** de Windows, seleccione **Server Manager** y, a continuación **File and Storage Services > Volumes > Disks**.
Se muestran todas las unidades de disco instaladas en su sistema.
2. Haga clic con el botón derecho del ratón en la nueva unidad de disco instalada y, a continuación, haga clic en **New Volume...**
Aparece el cuadro de diálogo **New Volume Wizard** .
3. Haga clic en **Next** para continuar.
Se muestra el cuadro de diálogo **Server and Disk**.
4. Seleccione el servidor y el disco correspondientes y haga clic en **Next** para continuar.
Aparece el cuadro de diálogo **Size**.
5. En el campo **Volume size:**, introduzca el tamaño de volumen que desea utilizar. Si desea utilizar el tamaño de volumen máximo, no realice ningún cambio en el valor preseleccionado. Haga clic entonces en **Next** para continuar.
Aparece el cuadro de diálogo **Drive Letter or Folder**.
6. En la lista **Drive letter:**, seleccione la letra de la unidad que se debe asignar al volumen y, a continuación, haga clic en **Next** para continuar.
Aparece el cuadro de diálogo **File System Settings**.
7. Se aplica lo siguiente:
 - **File system: NTFS**
 - **Allocation unit size: Default**
 - **Volume label:** introduzca la misma etiqueta de volumen que el del disco defectuoso sustituido (**Data** o **Data2**).
8. Haga clic en **Next** para continuar.
Se muestra el cuadro de diálogo **Confirmation**.

9. Compruebe si todos los ajustes son correctos y, a continuación, haga clic en **Create**. El sistema inicia la creación de una nueva partición y un volumen. Una finalizada la creación, aparece el cuadro de diálogo **Results**.
10. Haga clic en **Next** para continuar. La nueva partición y el volumen se han creado correctamente y se ha asignado todo el espacio de almacenamiento.

Habilitación del servicio de servidor

1. En el menú **Inicio** de Windows, seleccione **Services**. Aparece el cuadro de diálogo **Services**.
2. Busque el servicio **Server** en la lista y haga doble clic en él. Aparece el cuadro de diálogo **Server Properties**.
3. En la pestaña **General**, en la lista **Startup type:**, seleccione **Manual** y, a continuación, haga clic en **Apply**.
4. En **Service status:**, haga clic en **Start** para iniciar el servicio y, a continuación, haga clic en **OK** para aplicar los cambios. Cierre entonces el cuadro de diálogo **Services**.

Creación de LUN (discos virtuales iSCSI)

1. En el menú **Inicio** de Windows, seleccione **Server Manager** y, a continuación, seleccione **File and Storage Services > iSCSI**. Se muestran todos los discos virtuales iSCSI de su sistema.
2. Haga clic con el botón derecho del ratón en el LUN (el disco virtual iSCSI) del disco duro sustituido, que tiene el estado **Error** y, a continuación, haga clic en **Remove iSCSI Virtual Disk**. Aparece el cuadro de diálogo **Remove iSCSI Virtual Disk**.
3. Haga clic en **OK** para confirmar la extracción del LUN.
4. Repita estos pasos con todos los LUN que tengan el estado **Error**.
5. En el cuadro de diálogo **iSCSI VIRTUAL DISKS**, haga clic con el botón derecho del ratón en un espacio en blanco y, a continuación, haga clic en **New iSCSI Virtual Disk...** Aparece el cuadro de diálogo **iSCSI Virtual Disk Location**.
6. En **Server**, seleccione el servidor correspondiente en **Storage location:**, seleccione **Type a custom path** e introduzca la letra que ha asignado al disco duro nuevo (consulte *Creación de nueva partición y volumen, Página 18*). Haga clic entonces en **Next** para continuar. Aparece el cuadro de diálogo **iSCSI Virtual Disk Name**.
7. En el campo **Name:**, introduzca el nombre del LUN. Haga clic entonces en **Next** para continuar. Aparece el cuadro de diálogo **iSCSI Virtual Disk Size**.
8. En el campo **Size**, introduzca 2000 y cambie la unidad de tamaño a **GB**. Si hay menos de 2000 GB disponibles, configure el tamaño del LUN en el espacio de GB disponible menos 50 MB.
9. En **Fixed size:**, desactive la casilla de verificación **Clear the virtual disk on allocation**. Haga clic entonces en **Next** para continuar. Aparece el cuadro de diálogo **iSCSI Target**.
10. En **Existing iSCSI target:**, seleccione **TG0**. Haga clic entonces en **Next** para continuar. Aparece el cuadro de diálogo **Confirmation**.
11. Compruebe si todos los ajustes son correctos y, a continuación, haga clic en **Create**. El sistema inicia la creación del disco virtual iSCI nuevo. Una finalizada la creación, aparece el cuadro de diálogo **Results**.

12. Haga clic en **Close** para cerrar el cuadro de diálogo.
13. Repita estos pasos para crear más LUN utilizando todo el espacio disponible.
14. Una vez creados todos los LUN, aparecen en la lista **iSCSI VIRTUAL DISKS**.

Deshabilitación del servicio de servidor

1. En el menú **Inicio** de Windows, seleccione **Services**.
Aparece el cuadro de diálogo **Services**.
2. Busque el servicio **Server** en la lista y haga doble clic en él.
Aparece el cuadro de diálogo **Server Properties**.
3. En la pestaña **General**, en **Service status:**, haga clic en **Stop** para detener el servicio.
4. En la lista **Startup type:**, seleccione **Disabled** y, a continuación, haga clic en **Apply**.
5. Haga clic en **OK** para aplicar los cambios y, a continuación, cierre el cuadro de diálogo **Services**.

Formateo de LUN

1. Inicie BVMS Configuration Client.
2. En **Árbol de Dispositivos**, desplácese al grupo en el que se incluye el disco duro defectuoso, haga clic con el botón derecho del ratón en el destino de iSCSI **TGO** y, a continuación, haga clic en **Explorar destino** para actualizar la lista de LUN disponibles en este destino iSCSI.
De esta forma se eliminarán los LUN asociados al disco duro defectuoso y se añadirán los LUN creados en el disco duro nuevo.
3. El cuadro de diálogo de los **LUN** muestra una lista de todos los LUN disponibles y su estado (formateado o sin formatear).
4. Seleccione los LUN sin formatear y haga clic en **Dar formato a LUN**. Haga clic entonces en **Aceptar** para continuar.
5. Una vez finalizado el formateo, aparece un cuadro de diálogo de confirmación. Haga clic en **Aceptar** para finalizar el proceso.

7.4 Recopilación de los archivos de registro de DIVAR IP System Manager

La aplicación DIVAR IP System Manager incluye un script específico que simplifica la recopilación de los archivos de registro.

Para recopilar los archivos de registro de DIVAR IP System Manager:

1. Inicie sesión con la cuenta de administrador (consulte *Inicio de sesión en la cuenta de administrador*, Página 17).
2. En el menú **Inicio** de Windows, haga clic en **Export System Manager Logs**.
El script exporta los archivos en la carpeta `Documents\Bosch` y crea un archivo ZIP denominado según la estructura `SysMgrLogs-[date]_[time]`.
Puede utilizar este archivo ZIP para adjuntarlo a la descripción detallada de los errores.

7.5 Recuperación de la unidad

Para recuperar la unidad:

1. Encienda la unidad y pulse F7 durante la comprobación automática de la BIOS en el arranque para acceder a Windows PE.
Se muestra el cuadro de diálogo **System Management Utility**.
2. Seleccione una de las opciones siguientes:

- **System factory default:** esta opción formatea las particiones de datos de vídeo y restaura la partición del sistema operativo con la imagen predeterminada de fábrica. Este proceso puede tardar hasta 5 minutos.
- **Full data overwrite and system factory default:** esta opción formateará las particiones de datos de vídeo, sobrescribiendo por completo los datos existentes y restaura la partición del sistema operativo con la imagen predeterminada de fábrica. Este proceso podría tardar hasta 48 horas.
- **OS system recovery only:** esta opción restaurará la partición del sistema operativo con la imagen predeterminada de fábrica e importará los discos duros virtuales existentes desde las particiones de datos de vídeo existentes. Este proceso podría tardar hasta 5 minutos.

Nota:

la opción **OS system recovery only** no borra las secuencias de vídeo almacenadas en los discos duros de datos. Sin embargo, sustituye la partición completa del sistema operativo (incluidos los ajustes del sistema de gestión de vídeo) por una configuración predeterminada. Para acceder a las imágenes de vídeo existentes tras la recuperación, la configuración del sistema de gestión de vídeo debe exportarse antes de la recuperación del sistema y volver a importarse después.

**Aviso!**

No apague la unidad durante el proceso. Esto dañaría los medios de recuperación.

3. Confirme la opción seleccionada.
El sistema inicia el proceso de formateo y recuperación de imagen.
4. Una vez completado el proceso de recuperación, confirme el reinicio del sistema.
El sistema se reinicia y se realizan las rutinas de configuración.
5. Una vez finalizado el proceso, aparece la pantalla de selección de idioma de Windows.
6. Continúe con la configuración inicial del sistema.

Consulte

- *Primer inicio de sesión y configuración inicial del sistema, Página 9*

8 Información adicional

8.1 Software cliente y documentación adicional

Para obtener más información, descargas de software y documentación, visite <http://www.boschsecurity.com> y vaya a la página de producto correspondiente en el catálogo de productos.

Puede encontrar el software más reciente y los paquetes de actualización disponibles en la tienda de descargas de Bosch Security and Safety Systems en:

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

8.2 Servicios de asistencia y Bosch Academy



Soporte

Acceda a nuestros **servicios de asistencia** en www.boschsecurity.com/xc/en/support/.



Bosch Building Technologies Academy

Visite el sitio web de Bosch Building Technologies y acceda a los **cursos de formación, los tutoriales en vídeo** y la **documentación**: www.boschsecurity.com/xc/en/support/training/

Bosch Security Systems B.V.

Torenallee 49

5617 BA Eindhoven

Países Bajos

www.boschsecurity.com

© Bosch Security Systems B.V., 2022

Building solutions for a better life.

202211241440