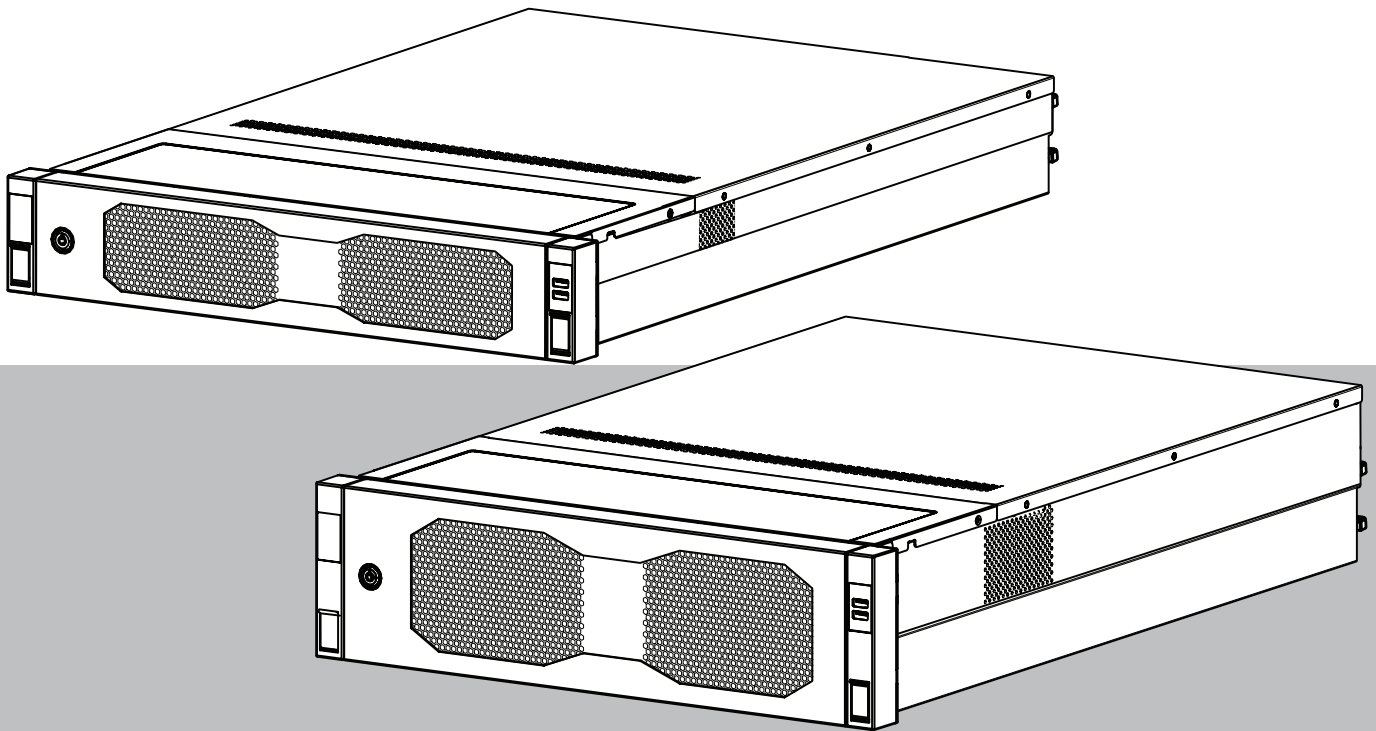


DIVAR IP all-in-one 7000 2U | DIVAR IP all-in-one 7000 3U

DIP-74C0-00N | DIP-74C4-8HD | DIP-74C8-8HD | DIP-74CI-8HD |
DIP-74CI-12HD | DIP-74G0-00N | DIP-74GI-16HD



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	8
3	Descripción del sistema	9
4	Configuración del sistema	10
4.1	Ajustes predeterminados	10
4.2	Requisitos previos	10
4.3	Primer inicio de sesión y configuración inicial del sistema	10
4.3.1	Elegir el modo de operación BVMS	12
4.3.2	Elegir el modo de funcionamiento VRM	13
4.3.3	Elección del modo de funcionamiento de almacenamiento iSCSI	13
5	Mejora de software	15
5.1	Actualización de DIVAR IP System Manager	15
5.2	Actualización del software mediante DIVAR IP System Manager	15
6	Conexión remota al sistema	18
6.1	Proteger el sistema frente al acceso no autorizado	18
6.2	Configuración del reenvío de puertos	18
6.3	Selección de un cliente adecuado	18
6.3.1	Conexión remota con BVMS Operator Client.	18
6.3.2	Conexión remota con la aplicación Video Security	19
6.4	Conexión a un Enterprise Management Server	19
6.5	Conexión con Remote Portal	19
6.5.1	Creación de una cuenta de Remote Portal	20
6.5.2	Registro de dispositivos DIVAR IP all-in-one en Remote Portal	20
6.5.3	Anulación del registro de dispositivos DIVAR IP all-in-one desde Remote Portal	20
7	Mantenimiento	22
7.1	Inicio de sesión en la cuenta de administrador	22
7.2	Monitorización del sistema	22
7.2.1	Monitorización del sistema con la aplicación ASUS Inband Tool	22
7.2.2	Monitorización del sistema mediante la interfaz web BMC	23
7.3	Sustitución de un disco duro defectuoso y configuración de un disco duro nuevo	24
7.3.1	Sustitución de un disco duro defectuoso	24
7.3.2	Reconstrucción de RAID5 con el disco duro nuevo	24
7.4	Recopilación de los archivos de registro de DIVAR IP System Manager	25
7.5	Recuperación de la unidad	25
8	Información adicional	27
8.1	Software cliente y documentación adicional	27
8.2	Servicios de asistencia y Bosch Academy	27

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 evitar la extracción no autorizada de los discos duros. Quite siempre la llave de la cerradura y guárdela en un lugar seguro.
- Utilice la función Chassis Intrusion Sensor para detectar cualquier acceso físico no autorizado al interior del 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.
- Para asegurarse de que el navegador Web está protegido y funcione correctamente, manténgalo siempre actualizado.
- No desactive Windows Defender ni el cortafuegos de Windows y manténgalo siempre actualizado. No instale software antivirus adicional, ya que puede alterar las configuraciones de seguridad.
- 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.
- No cambie los ajustes de UEFI de la BIOS. Si cambia los ajustes de UEFI de la BIOS puede poner en peligro o incluso provocar el mal funcionamiento del sistema.
- El sistema BMC no debe conectarse a la red pública.

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>
- Información sobre seguridad, que incluye los posibles efectos causados por vulnerabilidades de terceros: <https://www.boschsecurity.com/us/en/support/product-security/security-information.html>

Para recibir actualizaciones sobre nuevos avisos de seguridad, puede suscribirse a los canales RSS de la página de avisos de seguridad de Bosch Security and Safety Systems en: <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 7000 es una solución todo en uno asequible y fácil de utilizar para grabar, visualizar y gestionar sistemas de vigilancia en red de hasta 256 canales (con 8 canales prelicenciados incluidos).

El DIVAR IP all-in-one 7000 2U/3U es una unidad con montaje en rack 2U/3U que combina capacidades de Bosch Video Management System avanzadas y gestión de grabaciones de vanguardia en un único dispositivo de grabación rentable, práctico de instalar y de usar diseñado para clientes que buscan soluciones de TI.

DIVAR IP all-in-one 7000 utiliza un diseño integrado y componentes principales y se basa en el sistema operativo Microsoft Windows Server IoT 2022 for Storage Standard. Dispone de discos duros SATA intercambiables en caliente de calidad empresarial, que ofrecen hasta 216/288 TB de capacidad de almacenamiento bruta.

3 Descripción del sistema

Sistema operativo

El sistema operativo Microsoft Windows Server IoT 2022 for Storage Standard 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 Standard 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 7000 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.
- Solución de grabación de vídeo avanzada para un sistema BVMS 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. Se pueden añadir hasta dos servidores Video Recording Manager a un sistema BVMS que se ejecute en un dispositivo DIVAR IP all-in-one.
- Ampliación de almacenamiento iSCSI para un sistema BVMS que se ejecuta en un hardware diferente. Se pueden añadir hasta cuatro de estas ampliaciones de almacenamiento iSCSI a un sistema BVMS que se ejecuta en un dispositivo DIVAR IP all-in-one 7000.

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!

Los flujos de vídeo grabados se deben configurar 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
- La contraseña debe contener caracteres de tres de las cuatro categorías siguientes:
 - Al menos una letra en mayúsculas.
 - Al menos una letra en minúsculas.
 - Al menos un dígito.
 - Al menos un carácter especial.

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.




Aviso!

Por motivos de seguridad, se muestran cuadros de diálogo Control de Cuentas de Usuario (UAC) solicitando la confirmación para realizar los cambios previstos en el sistema. Solo puede continuar la instalación después de confirmar que desea realizar los cambios adecuados.

Para configurar el sistema:

1. Conecte la unidad DIVAR IP all-in-one y las cámaras a la red.
2. Encienda la unidad.
Espere a que se muestre la pantalla de la BIOS y se lleven a cabo las rutinas de configuración para Microsoft Windows Server IoT 2022 for Storage Standard. 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. Defina una nueva contraseña para la cuenta del administrador **BVRAdmin** y confírmela.
Requisitos de contraseña:
 - 14 caracteres como mínimo
 - La contraseña debe contener caracteres de tres de las cuatro categorías siguientes:
 - Al menos una letra en mayúsculas.
 - Al menos una letra en minúsculas.
 - Al menos un dígito.
 - Al menos un carácter especial.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.
Aviso: asegúrese de que se ha instalado la última versión de DIVAR IP System Manager. Puede encontrar el software más reciente y los paquetes de actualización disponibles en la página de descargas de Bosch Security and Safety Systems en: <https://downloadstore.boschsecurity.com/>.
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.
 10. En los siguientes cuadros de diálogo Control de cuentas de usuario, haga clic en **Yes** para continuar. La instalación se inicia.
 11. 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.
 12. El navegador Microsoft Edge se abre 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 de BVMS que desea instalar, a continuación, haga clic en **Instalar modo operativo**.
Se muestra el contrato de licencia de BVMS.
2. Lea y acepte el contrato de licencia y, a continuación, haga clic en **Sí, 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 de VRM que desea instalar, a continuación, haga clic en **Instalar modo operativo**.
Se muestra el contrato de licencia de VRM.
2. Lea y acepte el contrato de licencia y, a continuación, haga clic en **Sí, 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 **Instalar modo operativo**.
Se muestra el cuadro de diálogo de instalación.
2. En el cuadro de diálogo de instalación, haga clic en **Sí, instalar** para continuar.
La instalación se inicia y el cuadro de diálogo de instalación muestra el progreso de la instalación. No apague el sistema ni retire el soporte 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

Asegúrese de actualizar DIVAR IP System Manager a la versión más reciente.

5.1 Actualización de DIVAR IP System Manager

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. Busque el archivo ZIP **SystemManager_[versión del software 2.3.0 o superior].zip** y guárdelo en un soporte de almacenamiento, como una unidad USB.
4. Descomprima el archivo en el soporte de almacenamiento.
5. Conecte el soporte de almacenamiento a su dispositivo DIVAR IP all-in-one.
6. Iniciar DIVAR IP System Manager:
 - Si ha iniciado sesión en Windows con la cuenta de administrador de **BVRAdmin**, haga doble clic en el icono de DIVAR IP System Manager en el escritorio de Windows.
DIVAR IP System Manager se inicia.
 - Si el sistema se está ejecutando en modo de funcionamiento de BVMS, haga clic en el icono de DIVAR IP System Manager en el escritorio de BVMS e inicie sesión en la cuenta de administrador de BVRAdmin. DIVAR IP System Manager abre un cuadro de diálogo de pantalla completa (puede salir del cuadro de diálogo pulsando Alt+F4).
7. Se mostrará la página **Paquetes de software**. Seleccione el paquete de software DIVAR IP System Manager y, a continuación, haga clic en **Instalar paquete** para continuar.
Se mostrará un cuadro de diálogo de instalación.
8. En el cuadro de diálogo de instalación, haga clic en **Sí, instalar** para continuar.
Así se inicia la instalación, que puede tardar unos minutos.
No apague el sistema y no retire el medio de almacenamiento durante el proceso de instalación.
Tenga en cuenta las notificaciones que aparecen en la parte superior de la página.

5.2 Actualización del software mediante DIVAR IP System Manager

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. Iniciar DIVAR IP System Manager:
 - Si ha iniciado sesión en Windows con la cuenta de administrador de **BVRAdmin**, haga doble clic en el icono de DIVAR IP System Manager en el escritorio de Windows.
DIVAR IP System Manager se inicia.
 - Si el sistema se está ejecutando en modo de funcionamiento de BVMS, haga clic en el icono de DIVAR IP System Manager en el escritorio de BVMS e inicie sesión en la cuenta de administrador de BVRAdmin. DIVAR IP System Manager abre un cuadro de diálogo de pantalla completa (puede salir del cuadro de diálogo pulsando 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 del paquete de software**, 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 del paquete de software**, 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 **Instalar paquete**. 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 **Sí, 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 satisfactoriamente todos los paquetes de software, verá una confirmación de que se ha realizado la instalación correctamente.
11. Si no se ha realizado la instalación correctamente, verá el mensaje correspondiente con información de cómo continuar en ese caso.

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 18.*
2. *Configuración del reenvío de puertos, Página 18.*
3. *Selección de un cliente adecuado, Página 18.*

También puede conectarse a su DIVAR IP all-in-one a través de Bosch Remote Portal y utilizar las funciones actuales y futuras disponibles a través de Remote Portal. Para obtener más información, consulte la *Conexión con Remote Portal, Página 19.*

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 18.*
- *Conexión remota con la aplicación Video Security, Página 19.*



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.
2. Una vez finalizada la instalación correctamente, inicie Operator Client utilizando el

acceso directo del Escritorio .

3. 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:

1. Busque en la App Store de Apple Bosch Video Security.
2. Instale la aplicación Video Security en su dispositivo iOS.
3. Inicie la aplicación Video Security.
4. Seleccione **Añadir**.
5. Introduzca la dirección IP pública o el nombre dynDNS.
6. Asegúrese de que está activada la conexión segura (SSL).
7. Seleccione **Añadir**.
8. 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.

6.5 Conexión con Remote Portal

Es posible conectar con su dispositivo DIVAR IP all-in-one mediante Bosch Remote Portal para utilizar funcionalidades actuales y futuras, como el servicio Bosch Remote System Management, que está disponible a través de Remote Portal.

Para obtener información detallada acerca del servicio Remote System Management, consulte la documentación y el material de formación de Remote System Management.

Requisitos previos

Conexión Remote Portal

Para conectar dispositivos DIVAR IP all-in-one a Remote Portal asegúrese de que se cumplen los siguientes requisitos previos:

- En el dispositivo debe estar instalado DIVAR IP System Manager 2.3.0 (o una versión superior).
- Se debe crear una cuenta de Remote Portal.

Comunicación de Remote Portal

Requisitos de conectividad para la comunicación de Remote Portal.

Aviso: todas las conexiones son salientes.

HTTPS (puerto 443)

- <https://api.remote.boschsecurity.com/rest/iot/devices>
- <https://sw-repo-remote.s3.eu-central-1.amazonaws.com>

MQTTS (puerto 8883)

- <tls://a1j83emmuys8gs-ats.iot.eu-central-1.amazonaws.com:8883>

6.5.1

Creación de una cuenta de Remote Portal

Para crear una cuenta de Remote Portal:

1. Vaya a <https://remote.boschsecurity.com/login>.
2. Haga clic en **Sign up**.
3. Introduzca el nombre de la empresa y su correo electrónico.
4. Seleccione la región de su empresa.
5. Lea los términos y condiciones y el aviso de protección de datos y, a continuación, seleccione las casillas de verificación para aceptarlos.
6. Haga clic en **Sign up** para crear una cuenta.

6.5.2

Registro de dispositivos DIVAR IP all-in-one en Remote Portal

Para registrar un dispositivo DIVAR IP all-in-one en Remote Portal:

1. Inicie DIVAR IP System Manager.
2. Haga clic en la pestaña **Conexión Remote Portal**.
3. Si ya tiene una cuenta de Remote Portal vigente, introduzca su correo electrónico y contraseña y, a continuación, haga clic en **Register** para registrar el dispositivo DIVAR IP all-in-one en Remote Portal.
4. Si su correo electrónico está asignado más de una cuenta de empresa con privilegios de administrador, se le muestra un cuadro de diálogo con las cuentas de empresa correspondientes.

En el cuadro de diálogo de selección, elija la cuenta de empresa donde desee registrar el dispositivo DIVAR IP all-in-one.

Aviso!

SingleKey ID

Bosch ha introducido SingleKey ID como proveedor de identidad (IdP) para permitir el inicio de sesión centralizado en todas las aplicaciones, servicios y plataformas de Bosch. Para conectar el dispositivo a Remote Portal mediante SingleKey ID, siga las instrucciones que se muestran en pantalla.



5. Si todavía no dispone de una cuenta de Remote Portal, haga clic en **Create account** para crear una cuenta de Remote Portal primero. Consulte .

6.5.3

Anulación del registro de dispositivos DIVAR IP all-in-one desde Remote Portal

Para anular el registro de un dispositivo DIVAR IP all-in-one desde Remote Portal:

1. Inicie DIVAR IP System Manager.
2. Haga clic en la pestaña **Remote Portal connection**.
3. Haga clic en **Anular el registro** para anular el registro de su dispositivo DIVAR IP all-in-one desde Remote Portal.

Nota: la anulación del registro del dispositivo desde Remote Portal no elimina la

configuración del dispositivo en Remote Portal. Para eliminar la configuración del dispositivo, inicie sesión en la cuenta de la empresa del Remote Portal correspondiente.

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 Monitorización del sistema

7.2.1 Monitorización del sistema con la aplicación ASUS Inband Tool

Los sistemas DIVAR IP all-in-one llevan la aplicación ASUS **Inband Tool** preinstalada. Esta aplicación se puede usar para monitorizar el sistema.

De forma predeterminada, el servicio de la aplicación está activado.

Para iniciar la aplicación:

1. Inicie sesión con la cuenta de administrador (consulte *Inicio de sesión en la cuenta de administrador*, *Página 22*).
2. En el escritorio, abra la carpeta **Tools** y haga doble clic en el acceso directo a ASUS Inband Tool para iniciar la aplicación.
3. Inicie sesión utilizando las credenciales de acceso predeterminadas siguientes:
 - Cuenta: **admin**
 - Contraseña **admin**
4. Después de iniciar sesión por primera vez, se le solicitará que cambie esta contraseña inicial.

Introduzca una contraseña nueva y confírmela.

Asegúrese de guardar la contraseña nueva en un lugar seguro.

La contraseña debe cumplir los requisitos siguientes:

 - Las contraseñas deben tener una longitud mínima de 14 caracteres.
 - Las contraseñas deben contener al menos una letra en mayúscula.
 - Las contraseñas deben contener al menos una letra en minúscula.
 - Las contraseñas deben contener al menos un carácter especial.
 - Las contraseñas deben contener al menos un número.
5. Después de confirmar la contraseña nueva, se muestra la página **Dashboard**, donde se muestra el estado general del sistema.
6. En el panel **MENU** del lado izquierdo, puede seleccionar las páginas correspondientes para ver información detallada del estado del sistema.
7. En la opción de menú **SNMP**, puede configurar usuarios de SNMP y destinos de SMMP.
8. En la página **Report**, puede generar informes con la información que haya seleccionado.

7.2.2

Monitorización del sistema mediante la interfaz web BMC

DIVAR IP all-in-one 7000 dispone de un puerto BMC dedicado en la parte trasera.

Cada unidad de DIVAR IP all-in-one 7000 se suministra con el nombre de usuario de BMC predeterminado **admin** y con una contraseña de BMC inicial. La contraseña inicial de la BMC es única para cada unidad. Puede encontrarla en la etiqueta de la parte trasera de la unidad, debajo del puerto BMC.

Tras la primera conexión a la interfaz web de BMC, se le solicitará que cambie esta contraseña inicial. Asegúrese de guardar la nueva contraseña en una ubicación segura.

Tenga en cuenta los siguientes requisitos de contraseña:

- Las contraseñas deben tener una longitud mínima de 14 caracteres.
- Las contraseñas deben contener al menos una letra en mayúscula.
- Las contraseñas deben contener al menos una letra en minúscula.
- Las contraseñas deben contener al menos un carácter especial.
- Las contraseñas deben contener al menos un número.



Aviso!

Por motivos de seguridad, no conecte el dispositivo a una red pública a través del puerto BMC.

Cómo configurar los ajustes de BMC

Para configurar los ajustes de BMC:

1. Encienda la unidad y pulse Supr para introducir la configuración de la BIOS.



Aviso!

Contraseña BIOS

La contraseña inicial de la BIOS es única para cada unidad. Puede encontrarla en la etiqueta de la parte trasera de la unidad. Bosch recomienda encarecidamente cambiar esta contraseña inicial. Asegúrese de guardar la nueva contraseña en una ubicación segura.

Tenga en cuenta los siguientes requisitos de contraseña:

- Las contraseñas deben tener una longitud mínima de 14 caracteres.
- Las contraseñas deben contener al menos una letra en mayúscula.
- Las contraseñas deben contener al menos una letra en minúscula.
- Las contraseñas deben contener al menos un carácter especial.
- Las contraseñas deben contener al menos un número.

2. En la configuración de la BIOS, desplácese hasta la pestaña **Server Mgmt.**
3. Seleccione la opción **BMC Network Configuration** y, a continuación, pulse Entrar.
4. En el siguiente cuadro de diálogo, seleccione la opción **Configuration Address source** y, a continuación, pulse Entrar .
Se muestra el cuadro de diálogo **Configuration Address source**.
5. En el cuadro de diálogo **Configuration Address source**, seleccione la opción en la que se debe configurar la dirección BMC. A continuación, pulse Entrar.
6. Defina los parámetros de configuración de red deseados.
7. Pulse F4 y Entrar para guardar y salir.
La unidad DIVAR IP all-in-one 7000 se reinicia.

Funcionamiento remoto mediante la interfaz BMC iKVM

De forma predeterminada, los dispositivos DIVAR IP all-in-one 7000 están destinados a funcionar con uno o dos monitores locales conectados a las interfaces HDMI disponibles en la parte posterior de la unidad.

Si no hay monitores locales conectados a las interfaces HDMI, es posible controlar remotamente la unidad utilizando la interfaz BMC iKVM.

Para poder controlar el sistema remotamente:

1. Asegúrese de que no haya ningún monitor HDMI local conectado al sistema.
2. Inicie sesión en la interfaz web de BMC.
3. En el panel de menús de la izquierda, seleccione la página **Remote Control**.
4. Haga clic en el botón **Launch H5Viewer**.

Se accede a una ventana que muestra la salida de monitor de DIVAR IP all-in-one 7000 y proporciona control sobre el ratón y al teclado del equipo remoto.

7.3

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



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:

- ▶ 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

Reconstrucción de RAID5 con el disco duro nuevo

Reconstrucción automática de RAID5

1. En el escritorio de DIVAR IP all-in-one, haga doble clic en el acceso directo **Launch LSA**. Se inicia la aplicación **LSI Storage Authority** y se muestra la página **Remote Server Discovery**.
2. Inicie sesión con las credenciales de cuenta de administrador de **BVRAdmin**. Se mostrará un cuadro de diálogo que muestra que hay un controlador que tiene un problema crítico.
3. En la parte superior de la página, haga clic en **Select Controller** y, a continuación, en la barra **Controller ID:** para acceder a los ajustes del controlador.
 - Si aún no ha retirado el disco duro defectuoso, se mostrará dentro de **Drives > Foreign Drives > Unconfigured Drives**.
 - Después de extraer el disco duro defectuoso e instalar el nuevo, el sistema iniciará automáticamente la reconstrucción de RAID5 con el disco duro nuevo y se mostrará una barra de progreso de la reconstrucción.



4. Después de completar la reconstrucción correctamente, se muestra el icono

Reconstrucción manual de RAID5

Si la reconstrucción de RAID5 del disco duro nuevo no se inicia automáticamente, haga lo siguiente:

1. En el cuadro de diálogo de ajustes del controlador, **Drives > Foreign Drives > Unconfigured Drives**, seleccione el disco duro que está en estado **Unconfigured Bad** y, a continuación, en el panel de la derecha, seleccione **Make Unconfigured Good**. Se mostrará un cuadro de diálogo.

2. Active la casilla de verificación **Confirm** y, a continuación, haga clic en **Yes, Make Unconfigured Good** para continuar.
El sistema inicia la reconstrucción de RAID5 con el disco duro nuevo.



3. Después de completar la reconstrucción correctamente, se muestra el icono

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).
2. En el menú **Inicio** de Windows, haga clic con el botón derecho del ratón en **Export System Manager Logs** y ejecute el script como administrador.
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 tardará varios 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.
Nota: este proceso puede tardar varios días.
 - **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 tardará varios 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.

8 Información adicional

8.1 Software cliente y documentación 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>

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

Netherlands

www.boschsecurity.com

© Bosch Security Systems B.V., 2024

Soluciones para edificios para una vida mejor

202404171736