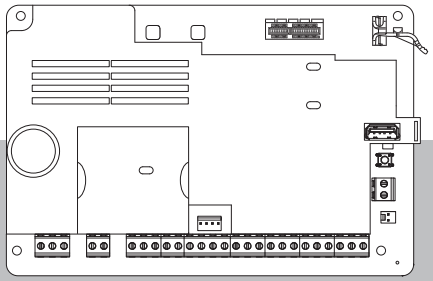
Paneles de control

B Series: B6512, B5512, B4512, B3512



es-AR Notas de la versión

Tabla de contenidos

1	**Introducción**	**4**
1.1	Acerca de la documentación	4
1.2	Requisitos	5
2	**Versión del firmware 3.14.012**	**10**
2.1	Novedades	11
2.2	Reformatorios	12
2.3	Problemas conocidos	14
3	**Firmware versión 3.12.024**	**16**
3.1	Novedades	16
4	**Firmware versión 3.12.020**	**18**
4.1	Novedades	19
4.2	Correcciones	20
4.3	Problemas conocidos	21
5	**Historial de revisiones del firmware**	**24**
5.1	Firmware versión 3.11.5	24
5.2	Firmware versión 3.11	25
5.3	Versión de firmware 3.10	29
5.4	Firmware versión 3.09.050	30
5.5	Firmware versión 3.08	32
6	**Software de código abierto 3.14.012**	**35**

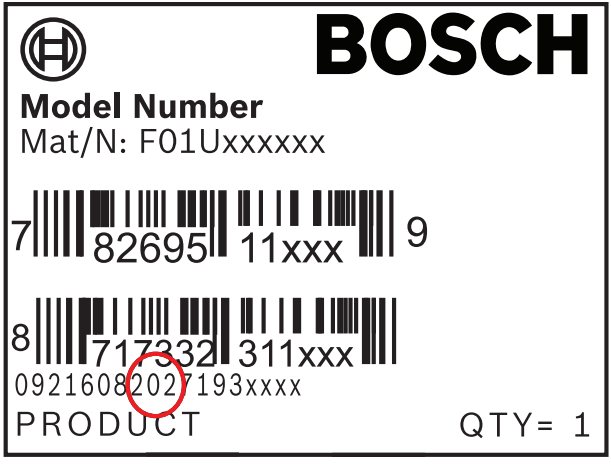
1 Introducción

Estas *notas de la versión* son para el firmware del panel de control versión 3.14.012.

1.1 Acerca de la documentación

Marcas registradas
Los nombres de todos los productos de hardware y software que se utilicen en este documento pueden ser marcas registradas y deben ser tratadas como tales.

Fechas de fabricación de los productos de Bosch Security Systems, B.V.
Utilice el número de serie ubicado en la etiqueta del producto y consulte el sitio web Bosch Security Systems, Inc. en http://www.boschsecurity.com/datecodes/.
En la siguiente imagen se muestra un ejemplo de una etiqueta de producto y se resalta el lugar donde se encuentra la fecha de fabricación dentro del número de serie.



1.2 Requisitos

Esta sección muestra los requisitos de RPS (Remote Programming Software) y de las estaciones de recepción central/puertas de enlace Conettix para admitir esta versión del firmware del panel de control.

1.2.1 Remote Programming Software (RPS)

Para usar todas las nuevas funciones de esta versión del firmware, es necesario utilizar RPS versión 6.12 o superior.

1.2.2 Estación de recepción central/puerta de enlace Conettix

Cuando configura el panel de control para realizar informes en formato Modem4, el receptor o la puerta de enlace de la estación central Conettix y el software de programación del receptor D6200 podrían requerir de una actualización. Lea la siguiente tabla para ver si Conettix necesita una actualización.

Requisitos del formato de notificación Conettix Modem4

Receptor o puerta de enlace	Versión de CPU	Versión de D6200
Receptor/puerto de comunicaciones Conettix D6600 (con tarjetas de línea D6641 instaladas únicamente)	01.10.00	2.10
Receptor/puerto de comunicaciones Conettix D6100IPv6	01.10.00	2.10
Receptor/puerto de comunicaciones Conettix D6100i	01.10.00	2.10

Cuando configura el panel de control para realizar informes en formato de ID de contacto, el receptor o la puerta de enlace de la estación central Conettix y el software de programación del receptor D6200 podrían requerir de una actualización. Lea la siguiente tabla para ver si Conettix necesita una actualización.

Requisitos de formato de informes de ID de contacto

Receptor o puerta de enlace	Versión de CPU	Versión de D6200
Receptor/puerto de comunicaciones Conettix D6600 (con tarjetas de línea D6641 instaladas únicamente)	01.03.02	1.35
Receptor/puerto de comunicaciones Conettix D6100IPv6	61.10.00	2.10
Receptor/puerto de comunicaciones Conettix D6100i	61.04.00	1.35

Notificación!
Cumple con ULC-S304 y ULC-S559.
Por cuestiones de cumplimiento, actualice el receptor o la puerta de enlace de la estación central Conettix y el software de programación o administración de D6200. Consulte la siguiente tabla.

Requisitos de formato de informes de ULC-S304 o ULC-S559 Modem4 e ID de contacto

Receptor o puerta de enlace	Versión de CPU	Versión de D6200
Receptor/puerto de comunicaciones Conettix D6600 (con tarjetas de línea D6641 instaladas únicamente)	01.11.00	2.20
Receptor/puerto de comunicaciones Conettix D6100IPv6	61.11.00	2.20
Receptor/puerto de comunicaciones Conettix D6100i	61.11.00	2.20

Formato ANSI-SIA DC-09

Para usar el formato ANSI-SIA DC-09, es necesario disponer de una estación de recepción central que admita este formato de comunicador IP. Las estaciones receptoras de la Central Conettix de Bosch no admiten este formato actualmente.

2 Versión del firmware 3.14.012

Nota: No se ha publicado la versión 3.13 del firmware del panel de control. La versión de firmware del panel de control saltó a la versión 3.14 para mantener la sincronización numérica con la versión de software RPS correspondiente.

Novedades

- *Compatibilidad con comunicador móvil enchufable B444-A2, página 11*
- *Compatibilidad con comunicador móvil enchufable B444-V2, página 11*

Reformatorios

- *Actualización de la restitución de armado forzado, página 12*
- *Introducción de los datos de acceso al tipo de tarjeta de 26 bits desde el teclado, página 12*
- *Comando Desbloquear puerta de una función personalizada o SKED, página 13*
- *La central no volverá a la conexión "nube a través de red móvil" si se produce un fallo de DNS de Ethernet, página 13*
- *El funcionamiento móvil podría fallar si la DNS de Ethernet no es pública, página 14*

Problemas conocidos

– *El informe de apertura de área no se envía al cambiar de estado de armado Todas-activadas a Parte-activadas, página 14*
– *Boletín técnico - Correo electrónico de notificación personal de G Series, B Series, página 15*

2.1 Novedades

Esta sección examina las nuevas funciones de esta versión del firmware.

2.1.1 Compatibilidad con comunicador móvil enchufable B444-A2

Compatibilidad de nuevo módulo móvil para el módulo móvil enchufable B444-A2, AT&T LTE.

2.1.2 Compatibilidad con comunicador móvil enchufable B444-V2

Compatibilidad de nuevo módulo móvil para el módulo móvil enchufable B444-V2, Verizon LTE.

2.2 Reformatorios

En esta sección se describen las correcciones realizadas en esta versión del firmware.

2.2.1 Actualización de la restitución de armado forzado

En versiones anteriores del firmware, cuando el parámetro de Restitución de armado forzado de un perfil de punto se establecía en SÍ, después de desarmar el sistema, el usuario tenía que anular manualmente cualquier punto forzado con ese perfil. Con la versión 3.14.010 del firmware, cuando el parámetro de Restitución de armado forzado se establece en SÍ, cualquier punto forzado se desactivará automáticamente y volverá a la normalidad, una vez que el sistema esté desarmado.

2.2.2 Introducción de los datos de acceso al tipo de tarjeta de 26 bits desde el teclado

En las versiones de firmware 3.11 y 3.12, los datos de la tarjeta de acceso que se introducen desde un teclado no se cargaron en el panel de control correctamente.

2.2.3 Comando Desbloquear puerta de una función personalizada o SKED

En la versión de firmware 3.11, la función Desbloquear puerta permite al usuario desbloquear una puerta mediante una función personalizada o SKED, incluso si la zona estaba armada. Esta corrección evita el comando Desbloquear puerta desde una función personalizada o SKED con un estado armado.

2.2.4 La central no volverá a la conexión "nube a través de red móvil" si se produce un fallo de DNS de Ethernet

Si están activados los parámetros Ethernet y Conexiones remotas a la nube móvil, la central no cambia a "nube a través de red móvil" si la conexión "nube a través de Ethernet" tiene un fallo de DNS. Este problema se ha corregido.

2.2.5 El funcionamiento móvil podría fallar si la DNS de Ethernet no es pública

Al programar una dirección IP de servidor DNS específica para IPv4 Ethernet, esta se compartirá por celular. Si no se puede acceder a la dirección DNS IPv4 para Ethernet en la red pública, la interfaz celular no podrá resolver las URL.
Cuando se utiliza Ethernet integrado y celular, se requiere un DNS IPv4 privado para Ethernet. Ahora está disponible una configuración de DNS distinta para el módulo celular.

2.3 Problemas conocidos

En esta sección se describen los problemas conocidos de esta versión del firmware.

2.3.1 El informe de apertura de área no se envía al cambiar de estado de armado Todas-activadas a Parte-activadas

Podría no enviarse el **Informe de área abierta** si un usuario cambia el área de **Todas-activadas**, después a **Parte-activadas** y, a continuación, la desarma. Al cambiar de **Parte-activadas a Desarmar**, los **Informes de área abierta** solo se envían si están habilitados los

Informes de parte-activadas. Estos informes están deshabilitados por defecto. Al habilitar los **Informes de parte-activadas** se corrige el problema.

2.3.2 Boletín técnico - Correo electrónico de notificación personal de G Series, B Series

Los mensajes de correo electrónico de notificación personal podrían dejar de funcionar para algunos clientes debido a las funciones de seguridad de los proveedores de correo electrónico que emplean la verificación en dos pasos. Utilice la página de seguridad del proveedor de correo electrónico (Google, por ejemplo) para crear una contraseña de aplicación. Esa contraseña se utilizará en el panel de control, como contraseña de autenticación del servidor de correo electrónico, para que funcionen los correos electrónicos de notificación personal. Consulte el "Boletín técnico Correo electrónico de notificación personal de G Series, B Series" para obtener más información.

3 Firmware versión 3.12.024

Novedades

- *El módulo de comunicador para teléfono móvil conectable B444-A no se reconoce, página 16*
- *Informe de Fallo al cerrar, página 17*

Consulte

- *Compatibilidad con credenciales de control de acceso HID de 35 bits (solo B6512), página 20*
- *Comunicaciones móviles AT&T mejoradas, página 20*

3.1 Novedades

Esta sección examina las nuevas funciones de esta versión del firmware.

3.1.1 El módulo de comunicador para teléfono móvil conectable B444-A no se reconoce

Algunos módulos móviles B444-A podrían notificar que "no son válidos" durante la instalación y el panel de control B Series o G Series no los reconoce. Esta versión del firmware permite al dispositivo host móvil reconocer correctamente estos módulos B444-A.

3.1.2 Informe de Fallo al cerrar

Algunas situaciones de armado problemáticas pueden enviar un informe de fallo al cerrar. Este informe solo se debe enviar si el área no se ha cerrado al final de la ventana de cierre. Esta versión de firmware resuelve este posible problema.

4 Firmware versión 3.12.020

Novedades

– *Compatibilidad con credenciales de control de acceso HID de 35 bits (solo B6512), página 20*
– *Comunicaciones móviles AT&T mejoradas, página 20*

Correcciones

– *Problema de armado forzado con el firmware 3.11.530, página 21*

Problemas conocidos

– *Sincronización de seguridad de contraseña con RPS y nuevo panel, página 21*
– *Programación de nuevos tipos de puntos en versiones de firmware anteriores a v3.11, página 22*
– *Correo electrónico de notificación personal, página 23*
– *Período de bloqueo del teclado (el teclado se bloquea con intentos de contraseña fallidos), página 23*

Consulte

– *El módulo de comunicador para teléfono móvil conectable B444-A no se reconoce, página 16*

– *Informe de Fallo al cerrar, página 17*
– *Conectividad mejorada a la red de Verizon, página 24*
– *Tipos de puntos ambientales, página 25*
– *Compatibilidad con los certificados del panel de control B Series y G Series actualizados, página 28*
– *Seguridad de contraseña configurable, página 26*
– *Firmware del panel de control conforme a FIPS, página 27*
– *Contraseña temporal, página 26*
– *Tipo de punto de pánico, página 25*
– *Soporte de entrada cableada de cámara IP, página 26*
– *Registro histórico dañado durante la actualización del firmware, página 25*
– *Índice de festivos 2, página 24*

4.1 Novedades

Esta sección examina las nuevas funciones de esta versión del firmware.

4.1.1 Compatibilidad con credenciales de control de acceso HID de 35 bits (solo B6512)

La compatibilidad con las credenciales HID de 35 bits permite a los clientes que utilizan el formato Corporate 1000 utilizar estas tarjetas con los paneles de control Bosch y la interfaz de control de acceso B901. Esto se añade a las tarjetas de formato de 26 y 37 bits que se admitían anteriormente. Tenga en cuenta que esta función solo está disponible para el panel de control B6512.

4.1.2 Comunicaciones móviles AT&T mejoradas

Se han añadido mejoras para mejorar el funcionamiento del B444-A y adaptarse a los cambios en la red móvil de AT&T asociados a la próxima desaparición del 3G.

4.2 Correcciones

En esta sección se describen las correcciones realizadas en esta versión del firmware.

4.2.1 Problema de armado forzado con el firmware 3.11.530

La versión 3.12 del firmware corrige un problema relacionado con la función de armado forzado en nuestros paneles de control B9512G, B8512G, B6512, B5512, B4512 y B3512 que puede hacer que los puntos que se han armado de manera formada permanezcan anulados sin indicación en el teclado. Tenga en cuenta que este problema solo se da en la versión de firmware 3.11.530.

4.3 Problemas conocidos

En esta sección se describen los problemas conocidos de esta versión del firmware.

4.3.1 Sincronización de seguridad de contraseña con RPS y nuevo panel

Cuando se conecta a un nuevo panel de control con firmware v3.11 utilizando el RPS v6.11 y, a continuación, se recibe la configuración desde el panel nuevo, la opción de envío/recepción siguiente abrirá la ventana de sincronización del panel, ya que el

parámetro de seguridad de contraseña del panel de control no coincide con la configuración del parámetro de seguridad de contraseña en RPS.
Al hacer clic en la opción **Ver las diferencias en los datos** de la ventana de sincronización del panel no se ve ninguna diferencia entre el parámetro de seguridad de contraseña de RPS y del panel de control.

Recomendación

Envíe la configuración de RPS al panel para hacer que coincidan los parámetros de seguridad del RPS y de contraseña del panel.

4.3.2 Programación de nuevos tipos de puntos en versiones de firmware anteriores a v3.11

Al utilizar RPS 6.11 para programar un nuevo punto de pánico o punto ambiental (agua, alta temperatura, baja temperatura) en un sistema de panel de control con versiones de firmware anteriores a v 3.11, el sistema no generará alertas y condiciones como se espera.
En algunas situaciones, el tipo de punto de temperatura baja generará un evento de problema y, en todos los escenarios, el pánico, el agua y los tipos de puntos temporales altos no generarán ninguna condición de evento.

Recomendación
Actualice el firmware del panel de control a v3.11 o superior, si se necesitan estos nuevos tipos de puntos.

4.3.3 Correo electrónico de notificación personal

Cuando se utilizan notificaciones personales por correo electrónico, algunas opciones de configuración del servidor (por ejemplo, la verificación en 2 pasos de Gmail, Permitir aplicaciones menos seguras: Desactivado) no funcionan correctamente. Para garantizar el funcionamiento, deshabilite las opciones de servidor de correo electrónico adicionales.

4.3.4 Período de bloqueo del teclado (el teclado se bloquea con intentos de contraseña fallidos)

Si el valor del tiempo de bloqueo es superior a 6553 segundos, es posible que la operación de bloqueo del teclado no funcione correctamente. Para garantizar el funcionamiento, ajuste el tiempo de bloqueo por debajo de los 6553 segundos.

5 Historial de revisiones del firmware

En esta sección se analizan las funciones más importantes de las versiones anteriores de este firmware.

5.1 Firmware versión 3.11.5

5.1.1 Conectividad mejorada a la red de Verizon

FW V3.11.5 mejora la gestión de la APN de Verizon cuando se utilizan los comunicadores móviles B444-V o B444, lo que se traduce en una mayor fiabilidad de la conexión.

5.1.2 Índice de festivos 2

Notificación!
Esto solo es válido para B6512.

El Índice de Vacaciones 2 no se ejecutó tal y como se programó y se ha corregido en esta versión de firmware.

5.1.3 Registro histórico dañado durante la actualización del firmware

Las actualizaciones del firmware del panel desde v3.06 o anterior a v3.07 hasta v3.09 pueden perder eventos del registro histórico. El problema se produce durante el restablecimiento o reinicio del panel de control. El registro histórico del panel anterior se debe cargar antes de actualizar a la v3.07 - v3.09.
V3.10 resuelve este problema y quita los daños que se produzcan en el registro histórico.

5.2 Firmware versión 3.11

5.2.1 Tipo de punto de pánico

Se ha añadido el tipo de punto de Pánico al panel, que es una alarma antirrobo de 24 horas pensada para un dispositivo de entrada de pánico.

5.2.2 Tipos de puntos ambientales

Hay disponibles nuevos tipos de puntos:
- Agua: alarma referida a un evento de fuga de agua.
- Temperatura alta: alarma para un evento de temperaturas elevadas.
- Temperatura baja: alarma para un evento de temperatura baja.

5.2.3 Seguridad de contraseña configurable

El sabotaje de contraseña de usuario puede configurarse ahora en teclados y clientes de automatización para detectar y actuar según un número definido de intentos de autenticación no válidos.

5.2.4 Contraseña temporal

Se puede conceder una contraseña de autoridad de desarme (uso único) a un usuario para una o varias áreas del panel de control para un acceso temporal. El nivel de autoridad asociado define al usuario como usuario temporal y sólo permite al usuario desarmar el sistema una vez y, a continuación, caduca la autoridad/contraseña.

5.2.5 Soporte de entrada cableada de cámara IP

La fuente de punto de cámara IP ahora incluye dos entradas cableadas de una cámara IP.
Configure las fuentes de cámara IP en asignaciones de puntos RPS en grupos de puntos. Por ejemplo, los puntos 10 y 19 para la cámara IP 1, los puntos 20 y 29

para la cámara IP 2, los puntos 30 y 39 para la cámara IP 3, hasta el número de cámaras disponibles en cada tipo de panel de control.

5.2.6 Firmware del panel de control conforme a FIPS

El RPS se ha actualizado para funcionar en un entorno de Windows seguro, como FIPS (Federal Information Processing Standards).

- Hay un paquete de firmware codificado AES/SHA adicional disponible para los paneles de control de las B series y G series en la sección Descargas > Sección de software del catálogo de productos de intrusión de Bosch. Cualquier instalación de RPS 6.11 o posterior puede utilizar este firmware.
- El archivo codificado de firmware correspondiente se nombra mediante el tipo de panel de control, el número de versión de firmware con la extensión _SHA.fwr para indicar el cifrado SHA (*B3512_B4512_ B5512_ B6512_FW_3.11.xxx_SHA.fwr*).

5.2.7 Compatibilidad con los certificados del panel de control B Series y G Series actualizados

El firmware del panel de control v3.11 introduce un nuevo certificado de seguridad con antelación a la caducidad del certificado actual en abril de 2022. Este certificado se utiliza para la mayoría de las conexiones de automatización (integración) y mediante TLS de RPS al panel. El certificado de la nube del panel no se ve afectado. Todas las conexiones en la nube seguirán funcionando igual que en la actualidad.
RPS v6.11 se ha actualizado para admitir este nuevo certificado de seguridad de panel automáticamente.

Notificación!
Importante
Los clientes que actualicen o instalen paneles con el firmware v3.11 deben actualizar RPS a v6.11 y revisar las demás aplicaciones integradas (de Bosch o de terceros) que necesiten utilizar el nuevo certificado de Bosch para mantener las conexiones TCP al panel después de marzo de 2022.

Los clientes que usen RPS con un firmware de panel v3.10 o una versión anterior no se verán afectados por la expiración del certificado y las operaciones continuarán sin interrupciones.

5.3 Versión de firmware 3.10

5.3.1 Salidas configurables

Los perfiles de las salidas son compatibles con la programación de los clientes y proporcionan una ruta para que las salidas operen basándose en requisitos de aplicación únicos.
Una vez que se ha creado un Perfil de Salida, puede reutilizarse y asignarse a salidas múltiples, lo que permite una programación rápida de la salida.
Se pueden crear Perfiles de Salida que definan la forma de operar de una salida cuando sucede un evento específico. Los perfiles de salida proporcionan una forma de asignar y de utilizar efectos de salida coherentes en todo el sistema.

5.3.2 UL 985, 6ª edición

Esta versión de firmware es ahora también compatible con la última edición de:

– UL 985, Unidades de Sistemas de Aviso de Incendios residenciales

5.4 Firmware versión 3.09.050

5.4.1 Compatibilidad con e B444-A y B444-V

El sistema ahora admite el módulo conectable móvil B444-A para LTE AT&T y el módulo conectable móvil B444-V para LTE Verizon.

Activación de la tarjeta SIM de B444-A/B444-V

Cuidado!
Active la tarjeta SIM de B444-A/B444-V antes de insertarla. En caso contrario, pueden producirse fallos en las comunicaciones con el panel de control/módulo. La primera vez que se enciende el B444-A/B444-V, el proceso de activación puede tardar hasta 15 minutos en completarse.

5.4.2 Formato ANSI-SIA DC-09

Ahora el sistema admite los formatos de comunicador de red siguientes:

– Conettix Modem4

– Conettix ANSI-SIA Contact ID
– ANSI-SIA DC-09

Notificación!

Aplicaciones HOMOLOGADAS según UL y ULC
El formato ANSI-SIA DC-09 no está disponible para las aplicaciones homologadas según UL y ULC.

5.4.3 Seguridad de los dispositivos conectados

Con el fin de cumplir con las disposiciones de seguridad de dispositivos conectados (TÍTULO 1.81.26. Seguridad de dispositivos conectados) y con la legislación pertinente, este producto utiliza una contraseña de conexión única.
La “contraseña RPS” para la conexión inicial con este producto debe coincidir con el ID de la nube único. Asegúrese de que el operador de RPS utilice el ID de nube único que figura en la etiqueta del producto y se incluye en la tarjeta que se entrega en la caja del producto.

5.4.4 Operación Tipo de respuesta de salida

En el firmware v3.09.024 del panel de control, las opciones de configuración 1 y 2 de la operación Tipo de respuesta de salida no funcionaban correctamente.
Esto se ha corregido en el firmware v3.09.050 del panel de control.
Si ha realizado cambios en el firmware v3.09.024 del panel de control para garantizar el funcionamiento correcto, esos cambios ya no son necesarios.

- En la operación Tipo de respuesta de salida, devuelva las opciones de configuración 1 y 2 a la configuración esperada y documentada.

5.5 Firmware versión 3.08

5.5.1 Compatibilidad con idiomas

Agrega compatibilidad para holandés, alemán y sueco.

Cuando el primer idioma del panel de control como el segundo idioma están configurados como holandés, inglés, francés, alemán, húngaro, italiano, portugués, español o sueco, el sistema utiliza el conjunto de caracteres estándar, Latin-1.

Si el primer o el segundo idioma del panel de control está configurado con chino, griego o polaco, el sistema utiliza el juego de caracteres extendido, UTF-8 Unicode.

Notificación!
Solo los teclados B915/B915i y B942 son compatibles con el juego de caracteres extendido UTF-8
Solo los teclados B915/B915i con la versión de firmware 1.01.010 o superior y los teclados B942 con la versión de firmware 1.02.022 o superior son compatibles con el juego de caracteres extendido UTF-8.

5.5.2 Tiempo de derivación de puerta

La selección más larga posible para el tiempo de derivación de la puerta se ha ampliado de 240 segundos a 8 horas.
Esta selección está disponible con las siguientes versiones de firmware:

- Firmware del panel de control v3.08 o superior
- Firmware de Remote Programming Software v6.08 o superior

– Firmare de B901 versión v1.05 o superior.

5.5.3 Dispositivos de destino de backup

El panel de control puede enviar informes a cuatro grupos de rutas diferentes usando un dispositivo de destino principal y hasta tres dispositivos de destino de backup para cada grupo de rutas.

5.5.4 Informe de prueba personalizado

Se puede enviar un informe de prueba normal o un informe de prueba personalizado:

– Informe de prueba normal: incluye todos los grupos de rutas que tienen la función de informe de prueba activada, con independencia del dispositivo de destino que se use para la comunicación. El informe de prueba se envía al primer dispositivo de destino correcto de un grupo de rutas.
– Informe de prueba personalizado: puede seleccionar el grupo de rutas y el dispositivo de destino que desee probar. Puede probar un dispositivo de destino por cada grupo de rutas o todos los dispositivos de destino configurados para un grupo de rutas.

6 Software de código abierto 3.14.012

Bosch incluye los módulos de software de código abierto que se enumeran a continuación en el firmware de este panel de control. La incorporación de estos módulos no limita la garantía de Bosch.

Digital Equipment Corporation

Portions Copyright (c) 1993 by Digital Equipment Corporation.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies, and that the name of Digital Equipment Corporation not be used in advertising or publicity pertaining to distribution of the document or software without specific, written prior permission.

THE SOFTWARE IS PROVIDED "AS IS" AND DIGITAL EQUIPMENT CORP. DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL DIGITAL EQUIPMENT CORPORATION BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES

WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Digital historical

Copyright 1987 by Digital Equipment Corporation, Maynard, Massachusetts, and the Massachusetts Institute of Technology, Cambridge, Massachusetts.

All Rights Reserved

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the names of Digital or MIT not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

DIGITAL DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL DIGITAL BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES

OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

OpenSSL License

Copyright (c) 1998-2008 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:
"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"
THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY

DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Para obtener más información, consulte la licencia de OpenSSL en www.boschsecurity.com, en Catálogo de productos.

Regents of the University of California

Copyright (c) 1985, 1993

The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by the University of California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.
THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR

CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

RSA data security

The "RSA Data Security, Inc. MD5 Message-Digest Algorithm" is included in the control panel firmware. RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

Time routines

This software [Time routines] is provided by the copyright holders and contributors "as is" and any express or implied warranties, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose are disclaimed. In no event shall the copyright owner or contributors be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services; loss of use, data, or profits; or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this software, even if advised of the possibility of such damage.

Bosch Security Systems B.V.
Torenallee 49
5617 BA Eindhoven
Países Bajos
www.boschsecurity.com

Building solutions for a better life.

202304141013