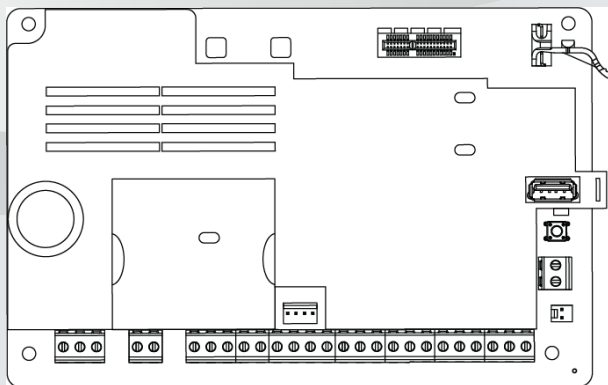




BOSCH

Paneles de control

B Series: B6512, B5512, B4512, B3512



es

Notas de la versión

Contenido

1	Introducción	4
1.1	Acerca de la documentación	4
1.2	Requisitos	5
2	Versión de firmware 3.10	8
2.1	Novedades	8
2.2	Correcciones	9
2.3	Problemas conocidos	9
3	Historial de revisiones del firmware	11
3.1	Firmware versión 3.09.050	11
3.2	Firmware versión 3.08	12
3.3	Firmware versión 3.07	14
3.4	Firmware versión 3.06	15
3.5	Firmware versión 3.05	18
4	Software de código abierto en 3.10	24

1 Introducción

Estas notas de la versión corresponden al firmware del panel de control versión 3.10.

1.1 Acerca de la documentación

Copyright

Este documento es propiedad intelectual de Bosch Building Technologies y está protegido mediante copyright. Todos los derechos reservados.


Marcas comerciales

Todos los nombres de productos de software y hardware utilizados en este documento pueden ser marcas comerciales registradas y deben tratarse en consecuencia.

Fechas de fabricación de los productos de Bosch Security Systems, Inc.

Utilice el número de serie que se encuentra en la etiqueta del producto y consulte el sitio web de Bosch Security Systems en <http://www.boschsecurity.com/datecodes/>.

La imagen siguiente muestra un ejemplo de la etiqueta del producto y resalta dónde encontrar la fecha de fabricación en el número de serie.



BOSCH

Model Number

Mat/N: F01Uxxxxxx

7 | 82695 | 11xxx | 9

8 | 717332 | 311xxx

09216082027193xxxx

PRODUCT

QTY= 1

1.2 Requisitos

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

1.2.1 Remote Programming Software (RPS)

Para poder utilizar las nuevas funciones de esta versión de firmware, deberá utilizar la RPS versión 6.10 o superior.

1.2.2 Estación de recepción central/puerta de enlace Conettix

Formato Conettix Modem4

Al configurar el panel de control para enviar informes en formato Modem4 de Conettix, podría ser necesario actualizar el software de programación de la estación de recepción central/puerta de enlace Conettix y la estación de recepción central D6200CD.

Requisitos del formato de notificación Conettix Modem4

Estación de recepción central/puerta de enlace	Versión CPU	Versión D6200CD
Estación de recepción central D6600, 32 líneas (con la tarjeta de líneas telefónicas D6641 instalada únicamente)	01.10.00	2.10
Estación de recepción central D6100IPV6-LT, 2 líneas, IP	01.10.00	2.10

Formato ANSI-SIA Contact ID de Conettix

Al configurar el panel de control para enviar informes en formato Contact ID ANSI-SIA de Conettix, podría ser necesario actualizar el software de programación de la estación de recepción central/puerta de enlace Conettix y la estación de recepción central D6200CD.

Formato de informe compatible con ULC-S304 y ULC S559

Aviso!



Formato de informe compatible con ULC-S304 y ULC S559
Para los formatos de informe compatibles ULC-S304 y ULC S559, es necesario que el software de programación de la estación de recepción central/puerta de enlace Conettix y la estación de recepción central D6200CD utilice la versión de la tabla.

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 de firmware 3.10

Novedades

- *Salidas configurables, Página 8*
- *UL 985, 6ª edición, Página 9*

Correcciones

- *Índice de festivos 2, Página 9*

Problemas conocidos

- *Correo electrónico de notificación personal, Página 9*

Consulte

- *Operación Tipo de respuesta de salida, Página 12*

2.1 Novedades

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

2.1.1 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.

2.1.2 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

2.2 Correcciones

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

2.2.1 Índice de festivos 2



Aviso!

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.

2.3 Problemas conocidos

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

2.3.1 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.

3 Historial de revisiones del firmware

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

3.1 Firmware versión 3.09.050

3.1.1 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



Precaución!

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.

3.1.2 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



Aviso!

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

3.1.3 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.

3.1.4 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.

3.2 Firmware versión 3.08

3.2.1 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.

Aviso!



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.

3.2.2 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
- Firmware de B901 versión v1.05 o superior.

3.2.3 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.

3.2.4 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.

3.3 Firmware versión 3.07

Funciones importantes

- *Conexiones de RPS entrantes, Página 14*
- *Indicación de intensidad de la señal B444, Página 15*
- *Estabilización del rendimiento de la tarjeta de móvil, Página 15*
- *Uso de APN para B442 y B443, Página 15*

3.3.1 Conexiones de RPS entrantes

Además de contestar a las llamadas entrantes de RPS mediante UDP (Protocolo de datagrama de usuario), las llamadas entrantes de RPS también son compatibles mediante TCP (Protocolo de transferencia de Control). Se requiere RPS versión 6.07 para este método de conexión modificado.

3.3.2 Indicación de intensidad de la señal B444

La indicación LED de intensidad de la señal B444 se ha modificado para representar el rendimiento con más precisión. Aunque todavía puede producirse la conmutación de torre LTE, sus indicaciones de intensidad de la señal individuales son más precisas.

3.3.3 Estabilización del rendimiento de la tarjeta de móvil

En esta versión del firmware se incluyen mejoras de estabilidad de la tarjeta de móvil.

3.3.4 Uso de APN para B442 y B443

Los módulos móviles conectables B442 y B443 tratarán de hacer conexiones mediante APN en el orden siguiente:

1. APN configurado principal
2. gne
3. wyles.apn
4. wyles.com.attz

El módulo móvil conectable seleccionará y utilizará el APN más adecuado.

Si el APN es erróneo, los teclados del panel no pueden mostrar los detalles de este problema.

3.4 Firmware versión 3.06

Funciones importantes

- *Compatibilidad con idiomas, Página 16*
- *Programación con teclado, Página 17*
- *RTC, Página 17*
- *Point Profile Circuit Style (Estilo de circuito de perfil de punto), Página 17*

- *System Tamper Response (Respuesta de manipulación del sistema), Página 17*
- *Passcode (Contraseña) [Esc], Página 18*
- *Tamaño del registro de eventos del panel, Página 18*
- *Nuevo valor predeterminado para el parámetro de red Access Point Name (Nombre de punto de acceso) (APN), Página 18*

3.4.1 Compatibilidad con idiomas

Incorpora la compatibilidad con chino, griego, húngaro, italiano y polaco.

Cuando tanto el primer idioma del panel de control como el segundo están configurados como inglés, francés, húngaro, italiano, portugués o español, 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.

Aviso!



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.

3.4.2 Programación con teclado

Se han añadido opciones de programación para teclados en el menú Installer (Instalador), como un menú Device (Dispositivo) y un menú Miscellaneous (Varios). El Manual de instalación contiene información detallada sobre el árbol de menús.

3.4.3 RTC

Parámetro de compatibilidad ampliada con RTC para admitir países adicionales.

3.4.4 Point Profile Circuit Style (Estilo de circuito de perfil de punto)

Las opciones ampliadas de estilo de circuito de perfil de punto incluyen las opciones “Dual 1K EOL with Tamper” (RFL doble de 1K con antisabotaje), “Single 1K EOL with Tamper” (Una sola RFL de 1K con antisabotaje) y “Single 2K EOL with Tamper” (Una sola RFL de 2K con antisabotaje). La selección de cualquiera de estos estilos permite enviar los nuevos informes Point Tamper Alarm (Alarma de sabotaje de punto) y Point Tamper Alarm Restoral (Restauración de alarma de sabotaje de punto).

3.4.5 System Tamper Response (Respuesta de manipulación del sistema)

Se ha añadido el parámetro System Tamper Response (Respuesta de manipulación del sistema) para configurar el comportamiento del sistema y sus notificaciones durante los estados de armado.

3.4.6 Passcode (Contraseña) [Esc]

Ahora, la opción Passcode (Contraseña) [Esc] del teclado se aplica tanto a teclados SDI como SDI2.

3.4.7 Tamaño del registro de eventos del panel

El tamaño del registro de eventos del panel ha cambiado a:
B3512 = 512, B4512 = 512, B5512 = 1024, B6512 = 1024.

3.4.8 Nuevo valor predeterminado para el parámetro de red Access Point Name (Nombre de punto de acceso) (APN)

En la versión de firmware 3.06 y la versión 6.05 de RPS, se ha modificado el parámetro de APN de red predeterminado por eaaa.bosch.vzwentp. El valor predeterminado anterior, wyles.apn, sigue siendo válido. No es necesario cambiar el APN en las cuentas existentes.

3.5 Firmware versión 3.05

Funciones importantes

- *Compatibilidad con credenciales de 37 bits con código de sitio, Página 20*
- *Compatibilidad para comunicaciones móviles 4G VZW LTE de B444, Página 19*
- *Actualización del esquema de horario de verano brasileño, Página 20*
- *Compatibilidad de conexiones simultáneas en modo 2, Página 19*
- *Ahora se admiten conexiones seguras mediante TLS 1.1 y 1.2, Página 20*

Correcciones

- *Indicación "Listo para activar" (armar), Página 21*
- *Desanulación mediante función personalizada, Página 21*
- *Armado forzado con puntos no anulables en estado de fallo , Página 21*
- *Informes de áreas compartidas, Página 22*
- *Prueba de paseo de incendio para varios detectores de humo con enclavamiento en un solo circuito, Página 22*
- *Puntos anulados revisados incorrectamente, Página 22*
- *Notificaciones personales de apertura y cierre, Página 23*
- *Modo 2 de automatización y puntos en estado de fallo, Página 23*
- Pantalla del teclado de silencio del punto de supervisión de la fuente de alimentación auxiliar

3.5.1 Compatibilidad para comunicaciones móviles 4G VZW LTE de B444

Esta actualización de firmware es compatible con comunicador móvil 4G VZW LTE conectable Conettix B444. Este módulo solo está destinado al mercado de Estados Unidos.

Nota: después del encendido inicial de B444 o B444-C, la activación puede tardar hasta 15 minutos en completarse. Esto solo sucederá la primera vez que se encienda la alimentación de la unidad B444 o B444-C.

3.5.2 Compatibilidad de conexiones simultáneas en modo 2

Ahora el panel de control admite hasta tres conexiones simultáneas de automatización en modo 2. Con las versiones anteriores del firmware, el panel de control solo admitía una conexión de automatización en modo 2 a la vez.

3.5.3 Compatibilidad con credenciales de 37 bits con código de sitio

Además de las credenciales HID de 26 bits y 37 bits (sin código de sitio), el panel de control ahora admite credenciales HID de 37 bits con códigos de sitio. Ahora el panel de control es compatible con los siguientes:

- HID de 37 bits H10304 (con código de sitio)
- HID de 37 bits H10302 (sin código de sitio)
- HID de 26 bits H10301
- EM EM4200 (3 bits o 5 bits)

3.5.4 Ahora se admiten conexiones seguras mediante TLS 1.1 y 1.2

El firmware ahora es compatible con las conexiones seguras, lo que incluye los servidores de correo electrónico para las notificaciones personales, mediante TLS v1.0 (solo cifrado fuerte), v1.1 y v1.2. En versiones anteriores del firmware, las conexiones mediante TLS con el panel de control requerían la compatibilidad con TLS v1.0.

3.5.5 Actualización del esquema de horario de verano brasileño

Ahora, los paneles configurados para el esquema "Brazil DST" (Horario de verano de Brasil) utilizarán el nuevo esquema, que comienza el primer domingo de noviembre, en vigor a partir de principios de 2018. Los paneles también admiten la variabilidad en el calendario de Carnaval.

3.5.6 Indicación "Listo para activar" (armar)

En versiones anteriores del firmware, en sistemas con una estación de recepción central inalámbrica B810 RADION o B820 Inovonics, los teclados podían no mostrar la indicación correcta de Listo para activar. Por ejemplo, se podía mostrar "Listo para activar" mientras había puntos en estado de fallo.

Esto se ha solucionado en esta versión del firmware.

3.5.7 Desanulación mediante función personalizada

En versiones anteriores del firmware, al desanular puntos mediante una función personalizada, no se desanulaban correctamente los puntos controlados, en estado de fallo. Este problema se ha resuelto con esta versión del firmware. Ahora los puntos en estado de fallo en áreas desarmadas se desanulan correctamente al utilizar la función personalizada. Los puntos de 24 horas en estado de fallo no se desanulan.

3.5.8 Armado forzado con puntos no anulables en estado de fallo

En una versión anterior del firmware, los paneles de control podían haber permitido armar (activar) de forma forzada el sistema si había algún punto no anulable en estado de fallo durante la revisión para el armado forzado.

Este problema se ha resuelto con esta versión del firmware. El panel de control no permite forzar el armado mediante la anulación de puntos no anulables.

3.5.9 Informes de áreas compartidas

En versiones anteriores del firmware, cuando un usuario activaba (armaba) o desactivaba (desarmaba) un área asociada, de modo que se activara o desactivara el área compartida, solo se enviaba el estado del área asociada a la estación de recepción central y solo este se almacenaba en el registro de eventos.

A partir de esta versión del firmware, el panel de control envía y registra el estado del área compartida además del área asociada.

3.5.10 Prueba de paseo de incendio para varios detectores de humo con enclavamiento en un solo circuito

En las versiones anteriores de este firmware, al realizar una prueba de paseo de incendio, el detector de humo no se restablecía a menos que finalizara la prueba de paseo de incendio. Por consiguiente, si había más de un detector de humo conectado a un circuito, no se podían probar todos los detectores de humo del lazo sin finalizar la prueba de paseo de incendio y volver a iniciarla.

Este problema se ha resuelto con esta versión del firmware.

3.5.11 Puntos anulados revisados incorrectamente

En versiones anteriores del firmware, al forzar el armado del panel de control, el teclado mostraba puntos adicionales para forzar el armado. Por ejemplo, al forzar el armado del vestíbulo, el teclado también pedía que se forzase el armado de puntos anulados en una planta superior. Este problema se ha resuelto con esta versión del firmware.

3.5.12 Notificaciones personales de apertura y cierre

En versiones anteriores del firmware, los paneles de control configurados con niveles de autoridad que limitaran el envío de eventos de apertura y cierre y configurados para enviar notificaciones personales de eventos de apertura y cierre enviaban incorrectamente los eventos de apertura/cierre al usuario restringido mediante las notificaciones personales. El problema no afectaba a los eventos que se enviaban a la estación de recepción central.

Este problema se ha resuelto con esta versión del firmware.

3.5.13 Modo 2 de automatización y puntos en estado de fallo

En el firmware v3.03, el panel de control permitía a los clientes con automatización en modo 2 el armado con puntos en estado de fallo.

Esto se ha corregido en v3.05.

4 Software de código abierto en 3.10

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

Copyright © 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved.

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

Copyright © 2002 Michael Ringgaard. All rights reserved.

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

Netherlands

www.boschsecurity.com

© Bosch Security Systems B.V., 2020