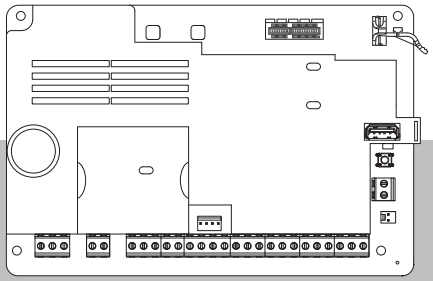
radionix

Paneles de control

B Series: B6512, B5512, B4512, B3512



es-AR Notas de la versión

Tabla de contenidos

1	**Introducción**	**5**
1.1	Acerca de la documentación	5
1.2	Requisitos	6
2	**Versión del firmware 3.15.116**	**10**
2.1	Novedades	10
2.2	Correcciones	11
3	**Versión del firmware 3.15.110**	**12**
3.1	Novedades	12
3.2	Correcciones	12
4	**Versión del firmware 3.15.024**	**14**
4.1	Novedades	14
4.2	Correcciones	16
5	**Historial de revisiones del firmware**	**20**
5.1	Versión del firmware 3.14.100	20
5.2	Versión del firmware 3.14.012	20
5.3	Versión del firmware 3.12.024	24
5.4	Versión del firmware 3.12.020	25
5.5	Versión del firmware 3.11.5	30

6 Programación del panel de control para que cumpla SIA 32

7 Requisitos mínimos del sistema para ANSI/SIA CP-01 39

8 Software de código abierto 3.15.116 40

1 Introducción

Estas *notas de la versión* son para el firmware del panel de control versión 3.15.116.

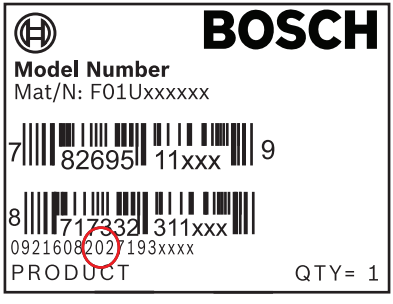
1.1 Acerca de la documentación

Derechos de autor
Este documento es propiedad intelectual de Radionix y está protegido por derechos de autor. Todos los derechos reservados.

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 Radionix
Para conocer las fechas de fabricación del producto, vaya a https://www.keenfinity-group.com/xc/en/datecodes/ y consulte el número de serie que se encuentra en la etiqueta del producto.

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 para que el software de programación remota (RPS) y los receptores/puerta de enlace Conettix sean compatibles con esta versión de firmware del panel de control.

1.2.1 Programación remota del software (RPS)

Para usar todas las funciones nuevas de esta versión de firmware, debe usar RPS versión 6.15 o superior.

1.2.2 Receptor/puerta de enlace Conettix

Formato Conettix Modem4

Al configurar el panel de control para enviar informes en formato Conettix Modem4, es posible que sea necesario actualizar el receptor/puerta de enlace de Conettix y el software de programación del receptor D6200CD.

Requisitos del formato de informe del módem Conettix Modem4

Receptor o puerta de enlace	Versión de CPU	Versión de D6200CD
Receptor de estación central D6600, 32 líneas (solo con tarjeta de línea telefónica D6641 instalada)	01.10.00	2.10
Receptor de estación central D6100IPV6-LT, 2 líneas, IP	01.10.00	2.10

Formato de identificación de contacto ANSI-SIA de Conettix

Cuando configura el panel de control para enviar informes en formato de ID de contacto en Conettix ANSI-SIA, el receptor o la puerta de enlace de la estación central Conettix y el software de programación del receptor D6200CD podrían requerir de una actualización.

Formato de informe compatible con ULC-S304 y ULC-S559

Notificación!

Formato de informe compatible con ULC-S304 y ULC-S559

Para los formatos de informe compatibles con ULC-S304 y ULC-S559, el receptor/puerta de enlace central Conettix y el software de programación del receptor D6200CD deben utilizar la versión que figura en la tabla.

Formato ANSI-SIA DC-09

El uso del formato ANSI-SIA DC-09 requiere un receptor de estación central que admita este formato de comunicador IP. Los receptores de estación central Bosch Conettix no son compatibles actualmente con este formato.

2 Versión del firmware 3.15.116

Correcciones

- *Se corrigió un error por el cual un mensaje "Route Group Comm Fail" (Fallo de comunicación del grupo de rutas) retenido no se borraba después de una recuperación de la comunicación., página 11*
- *Se solucionó una fuga de memoria en el panel., página 11*
- *Se solucionó el problema del envío de texto en el modo UTF-8, página 11*

2.1 Novedades

Esta sección examina las nuevas características de esta versión de firmware.
Esta versión del firmware solo contiene correcciones.

2.2 Correcciones

2.2.1 Se corrigió un error por el cual un mensaje "Route Group Comm Fail" (Fallo de comunicación del grupo de rutas) retenido no se borraba después de una recuperación de la comunicación.

2.2.2 Se solucionó una fuga de memoria en el panel.

2.2.3 Se solucionó el problema del envío de texto en el modo UTF-8

3 Versión del firmware 3.15.110

3.1 Novedades

Esta sección examina las nuevas características de esta versión de firmware.

3.1.1 La opción UPnP Enable ha cambiado de forma predeterminada a Deshabilitado.

La configuración predeterminada de fábrica se ha cambiado a UPnP desactivado para proporcionar un entorno más seguro y evitar ataques de denegación de servicio. Para mayor protección, Keenfinity recomienda desactivar UPnP en sus dispositivos actuales y eliminar todas las reglas de reenvío de puertos relacionadas con los productos de comunicación de Bosch en su enrutador.

3.2 Correcciones

Esta sección examina las correcciones realizadas en esta versión del firmware.

3.2.1 Se eliminó el cifrado 3DES de TLS 1.2.

Debido a los posibles riesgos de seguridad, el cifrado 3DES se eliminó de TLS 1.2.

3.2.2 El panel identificará y actualizará correctamente el B812.

El panel de control se actualizó para admitir el reconocimiento del B812, lo que permite su funcionamiento, las actualizaciones de firmware y el diagnóstico del RPS.

3.2.3 El panel identificará correctamente el B532 en el diagnóstico RPS.

El panel de control se actualizó para admitir el reconocimiento correcto del B532 para el diagnóstico del RPS.

4 Versión del firmware 3.15.024

Novedades

– *Certificación UL 2610 2.ª edición, página 14*
– *Seguridad mejorada, página 14*
– *Compatibilidad con fuente de alimentación auxiliar B532 y extensor SDI2 , página 16*
– *Soporte de modo 2, página 16*

4.1 Novedades

4.1.1 Certificación UL 2610 2.ª edición

Unidades y sistemas de alarma de seguridad para locales comerciales

4.1.2 Seguridad mejorada

– Configuración de la versión mínima compatible de TLS 1.2;

Advertencia!



Esta versión del firmware del panel impondrá el uso de TLS 1.2. La configuración de TLS solo se puede establecer en TLS 1.0 o 1.1 utilizando RPS versión 6.15 y superior. Si tiene herramientas que requieren las versiones 1.0 o 1.1 de TLS, NO actualice el firmware del panel hasta que tenga RPS 6.15 o superior.

Nota: Cuando también se utiliza un B426 o B450 en el sistema, estos módulos también deben actualizar su firmware a la versión 3.15 para aplicar la configuración de TLS.

- Deshabilitación de cifrados TLS no compatibles con FIPS;
- Bibliotecas de pila de red y TLS actualizadas;
- Verificado según NIST CAVP (certificado n.° A5272);
- Bloqueo temporal programable después de cinco fallas consecutivas de contraseña de acceso remoto.

4.1.3 Compatibilidad con fuente de alimentación auxiliar B532 y extensor SDI2

4.1.4 Soporte de modo 2

Soporte adicional para modo 2:

- Gestión de usuarios;
- Configuración del nivel de autoridad;
- Índices de vacaciones;
- Abrir/Cerrar ventanas.

4.2 Correcciones

4.2.1 Se corrigió la falta de POPIT que se produjo durante una actualización de programación

Boletín Técnico de Direcciones de fecha 30 de agosto de 2024.

4.2.2 Se solucionó el problema por el cual el teléfono no se podía restaurar después de un problema de comunicación telefónica.

4.2.3 Se solucionó el error "Datos fuera de rango" al agregar un nuevo usuario con BSM

4.2.4 Manejo mejorado del Modo 2 de "usuarios configurados"

4.2.5 Se eliminó el registro doble del evento "Acceso remoto no válido" cuando se desconecta Ethernet durante una conexión RPS o en la nube.

4.2.6 Ahora se envían informes SDI2 de fallas de cable abierto con el módem 4

4.2.7 Ahora se envían informes de "sobrecorriente" de la fuente de alimentación para cada salida

4.2.8 El evento de falla de CA de la fuente de alimentación ahora sigue la configuración de falla de CA de reenvío

4.2.9 Actualizaciones de estado de batería mejoradas para la fuente de alimentación B520/B532

4.2.10 El patrón de salida del teclado ahora se detiene si se elimina de la configuración del panel

4.2.11 El modo 2 Activar áreas del panel ya no fuerza el armado a menos que se le indique que lo haga

4.2.12 Se corrigió la falla "Parámetro de servicio" que puede ocurrir al omitir puntos desde un teclado

4.2.13 El problema B901 ya se puede solucionar

4.2.14 El evento de cambio de nombre de usuario ahora se registra en el registro de eventos del panel

4.2.15 Se solucionó el problema con el estado del punto PIE del modo 2 que no siempre se actualizaba correctamente

4.2.16 El bloqueo automático de la puerta ahora se envía al receptor

4.2.17 Manejo actualizado de certificados TLS vencidos

4.2.18 Se corrigió el problema al enviar correo electrónico a un servidor mediante IPv6

4.2.19 Actualizaciones de los niveles de transmisión del módem B430

4.2.20 Cuando un usuario cambia un código de acceso desde el menú de instalación del teclado, ya no genera una respuesta de cambio de punto

4.2.21 Actualizaciones del texto B915 y B920 cuando hay varias alarmas presentes

4.2.22 Se solucionó el problema por el cual la alarma silenciosa podía volverse audible antes de las dos fallas configuradas para enviar el evento.

5 Historial de revisiones del firmware

Esta sección examina las características más destacadas de las revisiones anteriores de este firmware.

5.1 Versión del firmware 3.14.100

5.1.1 Compatibilidad con credenciales de control de acceso HID de 32 bits: solo B6512

La compatibilidad con credenciales MIFARE classic de 32 bits permite que los clientes que utilizan tarjetas de acceso con este tipo de formato usen estas tarjetas con la interfaz de control de acceso B6512 y B901.
Esto se suma al formato de 26 bits, 35 bits y 37 bits que se admitía anteriormente.

5.2 Versión del firmware 3.14.012

5.2.1 Compatibilidad con el comunicador móvil enchufable B444-A2

Nueva compatibilidad con el módulo celular enchufable B444-A2, LTE de AT&T

5.2.2 Compatibilidad con el comunicador móvil enchufable B444-V2

Nueva compatibilidad con módulos celulares para el módulo celular enchufable B444-V2, Verizon LTE.

5.2.3 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.

5.2.4 Introducción de datos de acceso 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 introducidos desde un teclado no se cargaban correctamente en el panel de control.

5.2.5 Comando de desbloqueo de puerta desde una función SKED o personalizada.

En la versión de firmware 3.11, la función de desbloqueo de puerta permitía al usuario desbloquear una puerta mediante una función SKED o personalizada, incluso si la zona estaba armada. Esta corrección impide que se ejecute el comando de desbloqueo de puerta desde un SKED o una función personalizada cuando el sistema está armado.

5.2.6 El panel no recurrirá a la conexión "en la nube a través de datos móviles" si se produce un fallo en el DNS de Ethernet.

Si están habilitados los parámetros de conexión remota a la nube Ethernet y celular, el panel no cambiará a "nube a través de datos celulares" si la conexión "nube a través de Ethernet" presenta un fallo de DNS. Este problema ha sido corregido.

5.2.7 El funcionamiento celular puede fallar si el DNS de Ethernet no es público.

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.

5.2.8 El informe de apertura de área no se envía al cambiar del estado de activación total al estado de activación parcial.

Es posible que no se envíe un **Informe de apertura de área** si un usuario cambia el área de **Todo activado**, luego a **Parte activado**, y luego se desactiva. Al cambiar de **Activación parcial a Desactivación**, los **Informes de área abierta** solo se envían si los **Informes de activación parcial** están habilitados. Estos informes están desactivados por defecto. La activación de los **Informes parciales** aborda este problema.

5.2.9 Boletín técnico: Notificación personal por correo electrónico de las G Series y B Series

Es posible que el servicio de notificaciones personalizadas por correo electrónico deje de funcionar para algunos clientes debido a las funciones de seguridad del proveedor de correo electrónico que utilizan la verificación en dos pasos. Utilice la página de seguridad de su 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 permitir el funcionamiento de los correos electrónicos de notificación personal. Para obtener más información, consulte el correo electrónico de notificación personal del "Boletín Técnico de las Series G y B".

5.3 Versión del firmware 3.12.024

5.3.1 Novedades

Esta sección examina las nuevas características de esta versión de firmware.

5.3.1.1 El módulo comunicador celular enchufable B444-A no es reconocido.

Es posible que algunos módulos celulares B444-A aparezcan como "inválidos" durante la instalación y no sean reconocidos por el panel de control de las B o G Series. Esta versión de firmware permite que el dispositivo anfitrión celular reconozca correctamente estos módulos B444-A.

5.3.1.2 Falló cerrar informes:

En algunos casos, los escenarios de activación problemáticos pueden generar un informe de error al cerrar la alarma. Este informe solo debe enviarse si el Área no se ha cerrado al finalizar el período de cierre. Esta versión de firmware soluciona este posible problema.

5.4 Versión del firmware 3.12.020

5.4.1 Novedades

Esta sección examina las nuevas características de esta versión de firmware.

5.4.1.1 Compatibilidad con credenciales de control de acceso HID de 35 bits: solo B6512

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

5.4.1.2 Comunicaciones móviles mejoradas de AT&T

Se han incorporado mejoras para optimizar el funcionamiento del B444-A y adaptarse a los cambios en la red móvil de AT&T relacionados con la próxima retirada de la tecnología 3G.

5.4.2 Correcciones

Esta sección examina las correcciones realizadas en esta versión del firmware.

5.4.2.1 Problema de armado forzado con el firmware 3.11.530

La versión de firmware 3.12 corrige un problema relacionado con la función de armado forzado en nuestros paneles de control B9512G, B8512G, B6512, B5512, B4512 y B3512 que puede provocar que los puntos que se han armado forzadamente permanezcan desactivados sin ninguna indicación en el teclado. Tenga en cuenta que este problema solo existe en la versión de firmware 3.11.530.

5.4.3 Problemas conocidos

Esta sección examina los problemas conocidos de esta versión de firmware.

5.4.3.1 Sincronización de seguridad de código de acceso con RPS y nuevo panel

Al conectarse a un nuevo panel de control con firmware v3.11 mediante RPS v6.11 y, a continuación, recibir la configuración del nuevo panel, la siguiente opción de envío/recepción abrirá la ventana de sincronización del panel porque el parámetro de seguridad de código de acceso en el panel de control no coincide con la configuración del parámetro de seguridad de código de acceso en RPS.

Haciendo clic en la opción **Ver diferencias en los datos** en la ventana Sincronización del panel no muestra ninguna diferencia entre el parámetro Seguridad de código de acceso en RPS y el panel de control.

Recomendación

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

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

Al utilizar RPS 6.11 para programar un nuevo punto de pánico o un punto ambiental (agua, alta temperatura, baja temperatura) en un sistema de panel de control con versiones de firmware anteriores a la v3.11, el sistema no generará alertas ni condiciones como se espera.

En algunos casos, el tipo de punto Baja temperatura generará un evento de problema, mientras que en todos los casos los tipos de punto Pánico, Agua y Alta temperatura no generarán ninguna condición de evento.

Recomendación

Actualice el firmware del panel de control a la versión 3.11 o superior si necesita utilizar estos nuevos tipos de puntos.

5.4.3.3 Correo electrónico de notificación personal

Al utilizar las notificaciones personales por correo electrónico, algunas opciones de configuración del servidor (por ejemplo, la verificación en dos pasos de Gmail, permitir aplicaciones menos seguras: desactivado) pueden no funcionar correctamente. Para garantizar el funcionamiento, desactive las opciones adicionales del servidor de correo electrónico.

5.4.3.4 Período de bloqueo del teclado (bloqueo del teclado en caso de intentos fallidos de introducir el código de acceso)

Si el valor del tiempo de bloqueo supera los 6553 segundos, es posible que la función de bloqueo del teclado no funcione correctamente. Para garantizar el funcionamiento, configure el tiempo de bloqueo por debajo de 6553 segundos.

5.5 Versión del firmware 3.11.5

5.5.1 Conectividad mejorada a la red de Verizon.

La versión de firmware V3.11.5 mejora la gestión del APN de Verizon al utilizar los comunicadores celulares B444-V o B444, lo que resulta en una mayor fiabilidad de la conexión.

5.5.2 Índice de vacaciones 2

Notificación!
Esto se aplica únicamente al modelo B6512.

El índice de vacaciones 2 no se ejecutó según lo programado y se ha corregido en esta versión del firmware.

5.5.3 Corrupción del registro de historial durante la actualización del firmware

Las actualizaciones del firmware del panel desde la versión 3.06 o anterior a las versiones 3.07 a 3.09 pueden provocar la pérdida de eventos del registro histórico. El problema se produce durante un reinicio o restablecimiento del panel de control. El registro de historial del panel anterior debe cargarse antes de actualizar a la versión 3.07 - 3.09.

La versión 3.10 soluciona este problema y elimina cualquier corrupción en el registro de historial.

6 Programación del panel de control para que cumpla SIA

Nombre del parámetro	Configuraciones del panel de control necesarias para el cumplimiento de SIA	Configuración predeterminada
Nº de tel	(Agregue al número de teléfono de respaldo con el comando de desactivación de llamada en espera[1])	{Blank}
Tipo de coacción	Opción 3[2]	0 (Desactivado)
Cancelar informes	Sí	Sí
Tiempo de demora en la salida	45 segundos a 255 segundos	60 segundos

Habilitar coacción	Sí	No
Reinicio de retraso de salida	Sí o No	Sí
Todo encendido, sin salida	Sí o No	Sí
¿Regla de las dos personas:?	No	No
¿Emboscada inicial?	No	No
Advertencia de retraso de salida	Sí	Sí
Tono de entrada	Sí	Sí

Tono de salida	Sí o No	Sí
Cancelar visualización	Sí o No	Sí
Cancelar visualización	Sí o No	Sí
Verificar hora	De 10 a 60 segundos	60 segundos
Función de ingreso de código de acceso	Armado/desarmado	Armado/desarmado
Todo al instante	- (Desactivado)	- (Desactivado)
Arm Parcial Instant	- (Desactivado)	- (Desactivado)

Enviar coacción	- (Desactivado) o E (Activado)	E (Activado)
Desactivar	- (Desactivado) o E (Activado)	E (Activado)
Desactivación con contraseña	- (Desactivado) o E (Activado)	E (Activado)
Retardo de entrada	30 segundos a 240 segundos	30 segundos
Abortar alarma	Sí o No	Sí
Ventana de cancelación	15 segundos a 45 segundos	30 segundos
Longitud del código de acceso	De 3 a 6 dígitos	Desabilitado

Recuento de anulaciones de intercambio	1 a 2 disparos[3]	2 disparos
Advertencia remota	Sí	Sí
Temporizador de punto de cruce	De 5 a 255 segundos	20 segundos
Punto cruzado	Sí o No[4]	No
Prueba de caminata (todos los puntos que no sean de robo por incendio)	E (Activado)	E (Activado)

Prueba de caminata en todos los puntos de incendio	E (Activado)	E (Activado)
Retardo de respuesta desactivado	00:00	00:00
Retardo de respuesta activado	00:00	00:00

[1]La llamada en espera no se aplica a las redes celulares ni a la comunicación PSDN (red pública de datos conmutada). Un comando de desactivación de llamada en espera en una línea que no es de llamada en espera impedirá una conexión exitosa con la estación central.
[2]L14 es el nivel de autoridad de coacción predeterminado.
[3]El conteo de anulación de intercambio es programable hasta 4 disparos. Para cumplir con SIA, configúrelo en 1 o 2.

[4]Los puntos de cruce deben superponerse (proteger la misma área) para que un solo punto pueda proteger el área individualmente.

7 Requisitos mínimos del sistema para ANSI/SIA CP-01

Requisitos mínimos del sistema para la clasificación de acuerdo con ANSI/SIA CP-01:

- Unidad de control clasificada y listada por UL, modelo B6512, B5512, B4512 o B3512
- Teclado clasificado y listado por UL, modelo B942/B942W, B930, B921C/B921CW, B920 o B915/B915I
- Timbre local homologado por UL
- Medios de transmisión fuera de las instalaciones

8 Software de código abierto 3.15.116

Para este panel de control, Radionix incluye en el firmware los módulos de software de código abierto que se mencionan más abajo. La incorporación de estos módulos no limita la garantía de Radionix.

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 OpenSSL en www.boschsecurity.com, en el 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.

Radionix B.V.
Achtseweg Zuid 173
5651 GW Eindhoven
The Netherlands
www.radionix.com
© Radionix 2026

Radionix LLC
130 Perinton Pkwy.
Fairport, NY 14450
USA
www.radionix.com
© Radionix 2026

202611021238