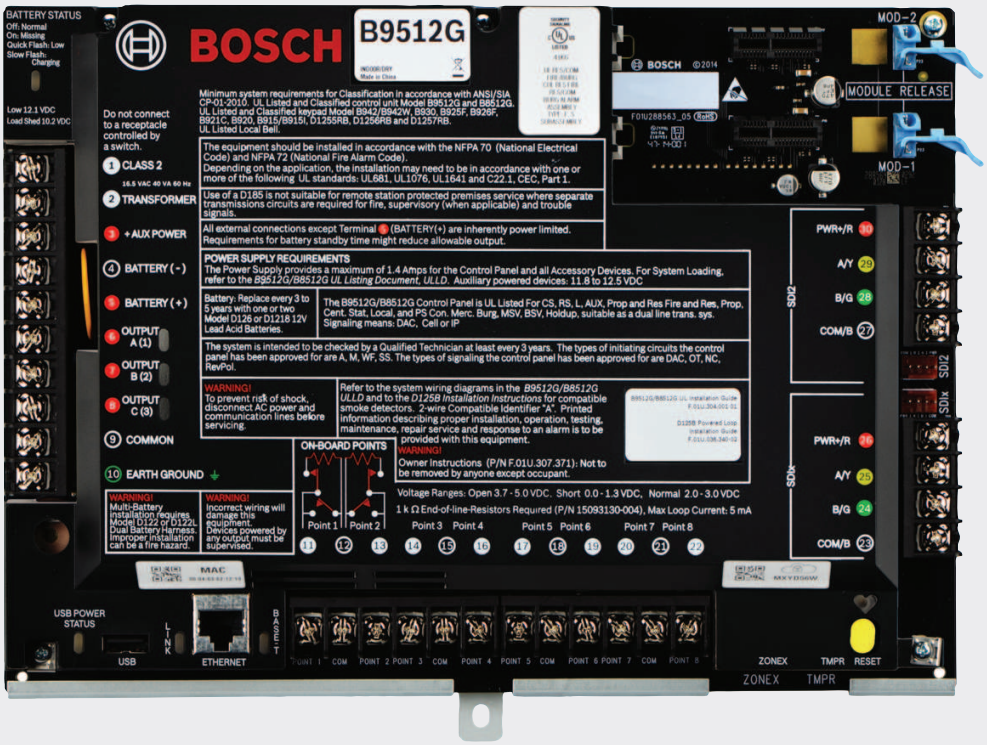


Control Panels

B9512G/B8512G (B9512G-E/B8512G-E)

BOSCH

en Release Notes

Table of contents

1 Introduction

These *Release Notes* are for control panel firmware version 3.04.

1.1 Requirements

This section shows requirements for RPS (Remote Programming Software) and Conettix Receiver/Gateways to support this control panel firmware version.

1.1.1 Remote Programming Software (RPS)

To program all new features of this firmware version, you must use RPS version 6.04 or higher.

1.1.2 Conettix Receiver/Gateway

When the control panel is configured to report in Modem4 format, the Conettix central station receiver/gateway and the D6200 Programming/Administration Software may require an update. Requirements are shown in the Modem4 requirements table below.

Modem4 reporting format requirements

Receiver/Gateway	CPU version	D6200 version
Conettix D6600 Communications Receiver/Gateway (with D6641 line cards installed only)	01.10.00	2.10
Conettix D6100IPv6 Communications Receiver/Gateway	01.10.00	2.10
Conettix D6100i Communications Receiver/Gateway	01.10.00	2.10

When the control panel is configured to report in the Contact ID reporting format, the Conettix central station receiver/gateway and the D6200 Programming/Administration Software may require an update as shown in the Contact ID requirements table below.

ContactID reporting format requirements

Receiver/Gateway	CPU version	D6200 version
Conettix D6600 Communications Receiver/Gateway (with D6641 line cards installed only)	01.03.02	1.35
Conettix D6100IPv6 Communications Receiver/Gateway	61.10.00	2.10
Conettix D6100i Communications Receiver/Gateway	61.04.00	1.35

Notice!

Compliance with ULC-S304 and ULC-S559

For compliance, the Conettix central station receiver/gateway and D6200 Programming/Administration Software must be updated as shown in the following table for both the Modem4 reporting format and the Contact ID reporting format.

ULC-S304/ULC-S559 Modem4 and ContactID reporting format requirements

Receiver/Gateway	CPU version	D6200 version
Conettix D6600 Communications Receiver/Gateway (with D6641 line cards installed only)	01.11.00	2.20
Conettix D6100IPv6 Communications Receiver/Gateway	61.11.00	2.20
Conettix D6100i Communications Receiver/Gateway	61.11.00	2.20

1.2 About documentation

Copyright

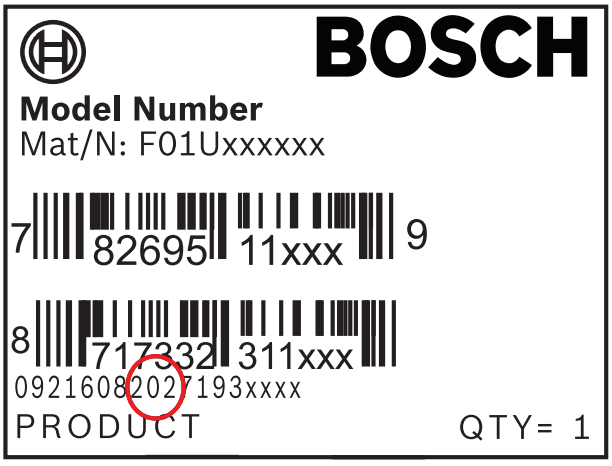
Trademarks

All hardware and software product names used in this document are likely to be registered trademarks and must be treated accordingly.

Bosch Security Systems, Inc. product manufacturing dates

Use the serial number located on the product label and refer to the Bosch Security Systems, Inc. website at http://www.boschsecurity.com/datecodes/.

The following image shows an example of a product label and highlights where to find the manufacturing date within the serial number.



1.2.1 Related documentation

Control Panels (B9512G/B8512G) Release Notes (this document)*
Control Panels (B9512G/B8512G) Installation and System Reference Guide (P/N: F01U303996)[+]
Control Panels (B9512G/B8512G/B6512/B5512/B4512/B3512) Owner's Manual (English) (P/N: F01U307371)* [+]
Control Panels (B9512G/B8512G) Program Entry Guide (P/N: F01U303998)[+]
Control Panels (B9512G/B8512G) UL Installation Guide[+] (P/N: F01U304001)* [+]
Control Panels (B9512G/B8512G) SIA Quick Reference Guide (P/N: F01U304000)* [+]
Control Panels (B9512G/B8512G/B6512/B5512/B4512/B3512) ULC Installation Guide (P/N: F01U321698)
*Shipped with the control panel. [+]Located on the documentation CD shipped with the control panel.

2 Firmware version 3.04

What's new

Corrections

Known issues

2.1 What's new

This section examines the new features of this firmware version.

2.1.1 Concurrent Mode 2 connections support

The control panel now supports up to three automation Mode 2 connections concurrently. In previous versions of firmware, the control panel supported one automation Mode 2 connection at a time.

2.1.2 37 bit credentials with site code support

In addition to 26 bit and 37 bit (no site code) HID credentials, the control panel now supports 37 bit HID credentials with site codes. The control panel now supports the following:

– 37 bit HID H10304 (With Site Code)
– 37 bit HID H10302 (No Site Code)
– 26 bit HID H10301
– EM EM4200 (3-byte or 5-byte)

2.1.3 Email servers using TLS v1.1 and v1.2 supported

The firmware now supports personal notification with providers using TLS v1.0, v1.1, and v1.2. In previous versions of the firmware, personal notifications using email required that the email provider supports TLS v1.0.

2.2 Corrections

This section examines the corrections made in this firmware version.

2.2.1 "Ready to turn on" indication

In previous versions of the firmware, for systems with a B810 RADION or B820 Inovonics wireless receiver, keypads might not display the proper Ready to turn on indication. For example, showing "Ready to turn on" while points are faulted.

This is resolved in this version of the firmware.

2.2.2 Custom function unbypass

In previous versions of firmware, unbypassing points using a Custom Function did not correctly unbypass faulted, controlled points. This is resolved in this firmware version. Faulted points in disamerd areas are now unbypassed correctly when using the custom function. Faulted 24-hour points are not unbypassed.

2.2.3 Force arming with faulted non-bypassable points

In a previous version of the firmware, the control panels might have allowed you to force arm (turn on) the system if non-bypassable points were faulted during the force arming review. This is resolved in this firmware version. The control panel does not allow you to force arm by bypassing unbypassable points.

2.2.4 Shared area reports

In previous versions of firmware, when a user turned on (armed) or turned off (disarmed) an associate area, causing the shared area to turn on or off, only the associate area status was sent to the central station receiver and stored in the event log.
Starting in this firmware version, the control panel sends and records the shared area status in addition to the associate area.

2.2.5 Fire walk test for multiple latching smokes on one circuit

In previous versions of this firmware, when performing a fire walk test, the smoke detector did not reset without ending the fire walk test. Therefore, if more than one smoke detector was connected to a circuit, you could not test all smoke detectors on the loop without ending the fire walk test and starting it again.
This is resolved in this firmware version.

2.2.6 Bypassed points incorrectly reviewed

In previous versions of the firmware, when force arming the control panel, the keypad would show additional points for force arming. For example, if you force armed the lobby, the keypad asked if you also wanted to force arm bypassed points on an upper floor.
This is resolved in this firmware version.

2.2.7 Open/Close personal notifications

In previous firmware versions, control panels control panels configured with authority levels that restrict sending open/close events and also configured to send Open/Close event personal notifications incorrectly sent the Open/Close events for the restricted user over personal notifications. The issue did not impact events sent to the central station receiver.
This is resolved in this firmware version.

2.2.8 Automation Mode 2 and faulted points

In firmware v3.03, the control panel let automation Mode 2 clients arm with faulted points.
This is corrected in v3.04.

2.2.9 Aux power supply supervisory point silenced keypad display

In previous firmware versions, when the user silenced a faulted point that used an Aux AC Supervision point index and then reset without returning to normal, the keypad display did not show the faulted point.
This issue is resolved in this firmware version.

2.3 Known issues

This section examines the known issues of this firmware version.

2.3.1 Manual alarm history events

History events viewed in RPS for manual alarms at a keypad do not list the keypad number at which the alarm occurred. View the correct information in the Event Log from a keypad.

2.3.2 UL 864 Fire application, compliance setting, PSTN RPS connection

When the RPS compliance setting for UL 864 Fire Application is set to Yes, the control panel must be in service mode prior to connecting using the B430 Plug-in Telephone Communicator. This is normal operation for the setting.

If you establish the RPS-control panel connection using the B430 without the control panel in service mode, and attempt to send configuration data, the control panel terminates the connection (hangs up). RPS shows “retry count exceeded” instead of indicating that the control panel must be in service mode to connect.

2.3.3 IP address error with B426

If the keypad shows "IP Address Error" in the display, RPS might still be capable of connecting to the control panel using direct connect with a B426.

2.3.4 Dual Authentication and Auto Re-Arm

It is recommended that Dual Authentication and Auto Re-Arm are not used in combination. Enabling both does not deliver the expected Dual Authentication operation.

2.3.5 Custom function for bypassing points and delay

If a custom function is configured to both bypass a point and turn on (arm) the system, and the custom function is programmed so that it does not require a passcode, the system bypasses the point, then asks for the passcode to arm the system.

Until this is resolved, insert into the custom function a Delay set to 1 second between the bypass and the On function.

3 Firmware revision history

This section examines the notable features of previous revisions of this firmware.

3.1 Firmware version 3.03.014

Notable features

3.1.1 ULC-S559 listing

The control panel now carries the ULC-S559 Fire Signal Receiving Centres and Systems listing for Canada. Refer to the *ULC Installation Guide* for listed modules, enclosures, and installation instructions.
The control panel can be configured to meet the requirements of a combined ULC-S559 and ULC-S304 system.

3.1.2 ULC Canada Compliance affects keypad message during firmware updates

Setting the ULC Canada Compliance parameter in RPS to Yes adjusts the control panel operation for UL Canada compliance. Beginning in this version, this includes reducing the keypad settings to show a Call for Service message after 90 seconds of disconnect instead of 180 seconds. This might cause a keypad to show the Call for Service message during a firmware update, even when a call is not required. The keypad shows idle text when the firmware update completes.

3.1.3 Remote Connect Service support

Remote Connect Service enables a secure control panel connection to mobile apps and remote programming software using Bosch Cloud services. Using this service allows a secure TLS connection to control panel without specific port and router settings or the need for static IP or DNS.

Notice!
Remote Connect Services and Bosch Cloud Services
Remote Connect Services and Bosch Cloud services are currently available in North America only.

3.1.4 Date/time formats

The keypad settings now provide users the option to select a format for both the date and time. For date, users can choose between MM/DD/YY, DD/MM/YY, and YY/MM/DD formats. For the time, users choose between 12-hour AM/PM format and 24 hour formats.

3.1.5 Input point End-of-line options

The control panel now supports 1 kΩ, dual EOL (1 kΩ + 1 kΩ), and 2 kΩ end-of-line (EOL) resistors as well as a No EOL option for on-board and B208 input points. Prior to this version, control panel supported 1 kΩ EOL and dual EOL (1 kΩ + 1 kΩ).

3.1.6 Control panel disconnect no longer required

The control panel now responds to RPS programming changes without needing to disconnect. In RPS, simply send the changes. The control panel immediately applies the new configuration.

3.1.7 Watch mode after power up

If the control panel is set for Watch Mode, the Watch Mode condition (On or Off) now persists through a power cycle (battery and AC power removed and reapplied).

3.1.8 Comm Trouble sound options

RPS now includes a parameter to set the Comm Troubles to visible (shown at the keypad and follows the trouble tone settings of the keypad) or invisible (no indication shows at the keypad). This only affects communication troubles not route group failures.

3.1.9 Updated B440/B441 support

Control panel firmware v3.02 and v3.03 support the latest versions of the B440 and B441 plug-in cellular modules (B440 v15.00.026 and B441 v18.02.022). The latest B440/B441 firmware includes updated libraries to maintain Verizon certification.
Control panel firmware v3.03, combined with the latest B440/B441 firmware, correctly shows the MEID on the keypad through the Installer menu. With control panel firmware v3.02, the MEID was truncated. This required you to read the MEID off the label instead of through the keypad, but otherwise did not affect normal operation.

3.2 Firmware version 3.02

Notable features

- *Bosch VMS integration support, page 11*
- *Shortcut Menu access from D1256RB keypads, page 11*

3.2.1 Bosch VMS integration support

With Bosch Video Management System (Bosch VMS) and an intrusion system, the VMS operator has a single user interface to monitor and control the intrusion system combined with video surveillance. With Bosch VMS and a control panel, the operator can, for example:

- View videos triggered by intrusion events, including all relevant information such as areas, point, and user show in the display with the event.
- View areas, points, outputs, and doors – with their statuses – on the Bosch VMS map, providing the exact location in the system.
- Turn on (arm) and turn off (disarm) areas.
- Bypass and unbypass points.
- Lock and unlock doors (Bosch VMS 6.0 and higher).

3.2.2 Shortcut Menu access from D1256RB keypads

Access to Shortcut Menu has been enabled through the use of the [ESC] key. This change allows use of a Shortcut from a keypad without a [CMD] key. Now, pressing the [ESC] key shows 4 fixed keypad functions, followed by the RPS-configured shortcuts programmed for that particular keypad address.

3.3 Firmware version 3.01

Notable features

- *Dual EOL resistor circuit style, page 12*
- *Improved Automation security, page 12*

Corrections

- *Fire Drill user number logged, page 12*
- *Fire Drills and area wide keypads, page 12*
- *Active alarms during fire drill, page 12*
- *Passcode to silence display on non-fire keypads, page 12*
- *Point Text display, page 12*

3.3.1 Dual EOL resistor circuit style

This version supports dual EOL resistors for the control panel on-board sensor loops, and for B208 Octo-input sensor loops. To configure points for dual EOL resistors, assign them to a Point Index with its Point Type / Response / Circuit Style parameter set to Dual EOL.

Notice!

RPS and B208 Octo-input firmware requirements for Dual EOL Circuit Style

RPS version 6.01 or higher is required to configure points for dual EOL resistors. Firmware v1.05.001 or higher is required for B208 Octo-inputs.

3.3.2 Improved Automation security

When the RPS parameter Automation Device is set for "Mode 1 using onboard connection with TLS" or "Mode 2", control panels with v3.01 firmware use either the AES 128 cipher or the AES 256 cipher. Both are readily available in all modern encryption libraries. This firmware does not support the less secure RC4, DES, or Triple DES ciphers.

3.3.3 Fire Drill user number logged

When a user initiated a Fire Drill and that Fire Drill ends because of a Fire Alarm, the control panel previously logged and reported the user number of the user who started the Fire Drill as the user who ended the drill. Now, the control panel logs and reports that a Fire Alarm ended the drill.

3.3.4 Fire Drills and area wide keypads

Fire drills started at area-wide keypads are not ended by a fire alarm in a different area. In previous firmware versions, the fire alarm display at panel-wide keypads incorrectly changed to a fire drill display after a user silence the alarm. This issue is resolved with this firmware version so that the fire alarm display remains when a fire drill continues in another area.

3.3.5 Active alarms during fire drill

In v3.00, during panel wide fire drills on control panels with shared outputs, pressing [Silence] or entering a passcode might not turn off the shared outputs. This is resolved in this firmware version so that now pressing [Silence] or entering a passcode will turn off shared outputs.

3.3.6 Passcode to silence display on non-fire keypads

In firmware v3.00, if a user pressed [Silence] on a B925F/B926F keypad to silence an active alarm, non-fire keypads showed "Please enter passcode to silence", even though a passcode is not required. This is resolved in this firmware version so that the non-fire keypads now correctly show idle text.

3.3.7 Point Text display

With previous control panel firmware versions, D1255 and D1260 keypads showed the first 16 characters (20 for D1260) of point descriptions, including the point number (PT ###), making it more difficult to identify the point based on its description.

This issue is corrected with control panel firmware v3.01. D1255 and D1260 keypads now show the first 16 characters (20 for D1260) of the point text, not including the point number.

3.4 Firmware version 3.00

The B9512G and the B8512G control panels were introduced with firmware version 3.00.
The B9512G is a direct replacement for previous control panel models D9412GV4, D9412GV3, D9412GV2, and D9412G.
The B8512G is a direct replacement for previous control panel models D7412GV4, D7412GV3, D7412GV2, and D7412G.

Notable features

The control panel includes the following technologies:

- *Control panel capacities, page 13*
- *On-board Ethernet, page 14*
- *On-board USB, page 14*
- *IP camera support, page 14*
- *Plug-in module support, page 14*
- *Personal notification, page 15*
- *SDI2 bus POPEX module (B299) support, page 15*
- *ZONEX retrofit module (B600) support, page 15*
- *SDI2 bus access control interface module (B901) support, page 15*
- *B925F/B926F Fire Keypad support, page 15*

3.4.1 Control panel capacities

Features	B9512G/ B9512G-E	B8512G/ B8512G-E
Number of users	2000	500
Total number of doors	32[1]	8[1]
Number of cards/tokens	2000	500
Number of custom functions	32	8
Number of areas	32	8
Number of points	599	99
Number of outputs	599	99
Total number of keypads	32[2]	16[2]
Number of octo-intput modules (B208)	59	9
Number of POPEX modules (B299)	6	1
Number of octo-output modules (B308)	59	9
Number of on-board Ethernet ports (“E” control panel variants do **not** include an Ethernet port)	1	1
Number of B426 or B450 modules	2	2
Number of B430 communicators plug-in PSTN)	2	2
Number of plug-in cellular communicators (B440/B440-C/B441/B441-C/B442/B443/ B444)	1	1
Number of auxiliary power supply modules (B520)	8	4
Number of wireless receivers (B810/B820)	1	1

Features	B9512G/ B9512G-E	B8512G/ B8512G-E
Number of cameras[3]	16	8
[1]The control panel supports 32 doors using the optional B901 Access Control Module. The control panel supports up to 8 doors using the optional D9210C Access Control Interface Module. [2]The control panel supports up to 16 of the keypads as SDI keypads. [3]Bosch IP cameras use is supplementary in UL Listed systems.		

The control panel also includes:

Features	B9512G/ B9512G-E	B8512G/ B8512G-E
Number of SKEDs	80	40
Number of open/close windows	32	8
Number of user group windows	32	8
Number of holiday schedules	8	4
Number of events	10,192	2,048
Number of personal notification destinations	32	32

3.4.2 On-board Ethernet

The control panel includes an on-board Ethernet port for Conettix IP alarm communication and remote programming. The port is compatible with modern IP networks including IPv6/ IPv4, AutoIP, and Universal Plug and Play.

3.4.3 On-board USB

The control panel includes an on-board USB port for easy on-site RPS programming.
In addition to connecting RPS to the control panel for programming, you can use the USB port on the control panel to power USB-powered devices.
When enabled, the USB port provides 500 mA of 5 V power, which it draws from the control panel. Ensure that there is enough power for all the powered devices you want to connect to the system.

3.4.4 IP camera support

The control panel can integrate directly with Bosch IP cameras, using them as fully supervised points and outputs.
Integration of cameras allows the camera's video motion detection to activate points on the control panel. The control panel's virtual outputs can be configured to trigger camera actions, including sending video snapshots via email.

3.4.5 Plug-in module support

The control panel has two plug-in module connections for PTSN and cellular communication. With plug-in connectors, the plug-in modules connect directly to the control panel without tools or wiring. The plug-in module installation process allows for easy adoption of new technologies. The control panel supports the following plug-in modules: B430 Plug-in Telephone Communicator for PTSN, and the B440 Conettix Plug-in Cellular Communicator, B441 Conettix Plug-in Cellular Communicator, B442 Conettix Plug-in Cellular Communicator, and B443 Conettix Plug-in Cellular Communicator for cellular communication.

3.4.6 Personal notification

The control panel can send text messages and emails for personal notification over Ethernet or using a cellular communicator. You can configure up to 32 destinations using a combination of cellular phone numbers and email addresses. The control panel sends notifications in the user's programmed primary language.

3.4.7 SDI2 bus POPEX module (B299) support

The control panel supports the new B299 POPEX Module.
The B299 POPEX Module is an SDI2 compatible device. The module communicates to the control panel over the SDI2 bus, and provides support for up to 100 POPIT (Point Of Protection Input Transponder) devices. This occurs over a single expansion loop using two pairs of terminals.

3.4.8 ZONEX retrofit module (B600) support

The control panel supports the new B600 Retrofit (ZONEX) Module.
The B600 Retrofit (ZONEX) Module communicates to the control panel through a proprietary connection, and provides support for two ZONEX busses. Connect the B600 module to the control panel through a proprietary connection.

3.4.9 SDI2 bus access control interface module (B901) support

The control panel supports the new B901 Access Control Interface Module.
The B901 Access Control Interface Module is a fully supervised, addressable SDI/SDI2 bus device that allows access control integration for Bosch compatible control panels. This module offers 14 programmable levels of access authority. Authority for access is controlled by the user level, the group of the user, the time of day, the door state, and the area armed state. Control each authority restriction through automatic and manual functions.

3.4.10 B925F/B926F Fire Keypad support

The control panel supports the new B925F and B926F Fire Keypads.
The B925F Fire Keypad is a fully supervised SDI2 device for combined fire/burglary applications.
The B926F Fire Keypad is a fully supervised SDI2 device for fire applications.
Each keypad has user-adjustable backlit keys, a display that shows system messages, and a sounder. The sounder emits distinct condition tones to alert you to a fire alarm, a fire trouble, or fire supervisory events as they occur. The keypad includes fire status indicators and fire function keys.

4 Update a legacy account in RPS

The B9512G is a direct replacement for previous control panel models D9412GV4, D9412GV3, D9412GV2, and D9412G.
The B8512G is a direct replacement for previous control panel models D7412GV4, D7412GV3, D7412GV2, and D7412G.
If you replace an existing G Series control panel with a B9512G/B8512G, you can update the existing RPS account to a B9512G/B8512G account so that you do not need to recreate the account.

Notice!
Before you upgrade an existing account to a B9512G/B8512G account in RPS, read the control panel update information in the *RPS Release Notes*.

4.1 Update an existing G Series control panel account to a B9512G/B8512G account

Updating to a B9512G/B8512G account:

1. In the Panel list window, highlight the control panel account, and then right-click the account and select View. The Panel Data – View window opens.
2. Click Edit. Locate the Panel Type selection on the right side of the Data View window.
3. From the Panel Type dropdown list, select the desired control panel type, and then click OK.
4. When you upgrade a control panel to a B8512G or a B9512G, RPS makes an account copy automatically.
5. Confirm the new, automatically changed configuration values match those needed for the control panel. Make any necessary changes.

Once the conversion completes and you confirmed the changes, send the updated program to the control panel.

1. Open the new control panel account you just created in the previous steps.
2. Click Connect. The Panel Communication dialog box appears.
3. Temporarily change the passcode in the RPS Passcode text box to 999999, and click Connect. (On the next connection, you do not need to change the passcode to connect to the control panel because the account's passcode is used.)
4. The Panel Sync dialog box appears.
5. Select Send ALL Updated RPS Data to Panel and click OK. Note: Do not select Receive Panel Data.
6. When the firmware update completes, exit RPS, if desired.

5 Open source notifications

Bosch includes the open source software modules listed below in the firmware for this control panel. The inclusion of these modules does not limit the Bosch warranty.

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).

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

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, Inc.
130 Perinton Parkway
Fairport, NY 14450
USA
www.boschsecurity.com

Bosch Sicherheitssysteme GmbH
Robert-Bosch-Ring 5
85630 Grasbrunn
Germany