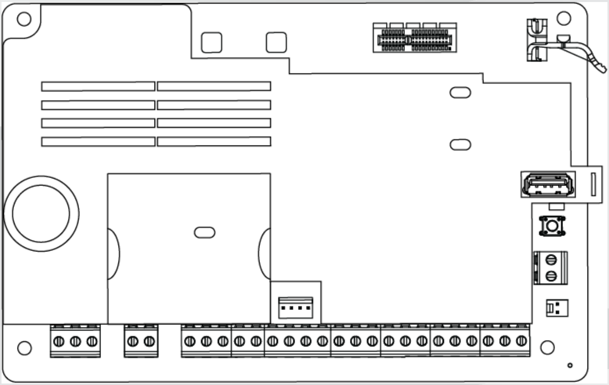
Control panels

B Series: B6512, B5512, B4512, B3512



en Release notes

Table of contents

1 Introduction

These Release Notes are for control panel firmware version 3.10.

1.1 About documentation

Copyright

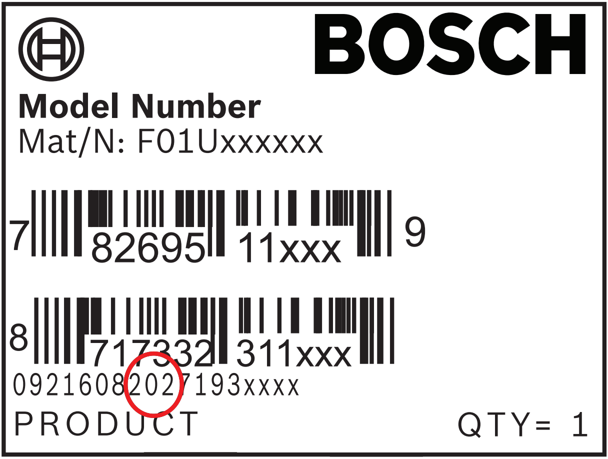
This document is the intellectual property of Bosch Security Systems B.V. and is protected by copyright. All rights reserved.

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 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 Requirements

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

1.2.1 Remote Programming Software (RPS)

To use all new features of this firmware version, you must use RPS version 6.10 or higher.

1.2.2 Conettix Receiver/Gateway

Conettix Modem4 format

When you configure the control panel to send reports in Conettix Modem4 format, the Conettix central station receiver/gateway and the D6200CD Receiver programming software might require an update.

Conettix Modem4 reporting format requirements

Receiver/Gateway	**CPU version**	**D6200CD version**
D6600 Central station receiver, 32-line (with D6641 Telephone line card installed only)	01.10.00	2.10
D6100IPV6-LT Central station receiver, 2-line, IP	01.10.00	2.10

Conettix ANSI-SIA Contact ID format

When you configure the control panel to send reports in Conettix ANSI-SIA Contact ID format, the Conettix central station receiver/gateway and the D6200CD Receiver programming software might require an update.

ULC-S304 and ULC-S559 compliant report format

Notice!

ULC-S304 and ULC-S559 compliant report format
For ULC-S304 and ULC-S559 compliant report formats, the Conettix central station receiver/gateway and the D6200CD Receiver programming software need to use the version in the table.

ANSI-SIA DC-09 format

Use of the ANSI-SIA DC-09 format requires a central station receiver that supports this IP communicator format. Bosch Conettix central station receivers do not currently support this format.

2 Firmware version 3.10

What's new

- *Configurable outputs, page 8*
- *UL 985 6th Edition, page 8*

Corrections

- *Holiday Index 2, page 9*
- *History log corruption during firmware upgrade, page 9*

Known issues

- *Personal notification email, page 10*

Refer to

- *Output Response Type operation, page 12*

2.1 What's new

This section examines the new features of this firmware version.

2.1.1 Configurable outputs

Output Profiles support custom programming and provide a way for outputs to operate based on unique application requirements.
Once an Output Profile is created, it can be reused and assigned to multiple outputs enabling quick output programming.
You can create Output Profiles that define how an output operates when specific events occur. Output Profiles provide a way to assign and use consistent output effects throughout the system.

2.1.2 UL 985 6th Edition

This firmware version now supports the latest edition of:

– UL 985 Household Fire Warning Systems Units

2.2 Corrections

This section examines the corrections made in this firmware version.

2.2.1 Holiday Index 2

Notice!

This applies only for B6512.

Holiday Index 2 did not execute as programmed and has been fixed in this firmware version.

2.2.2 History log corruption during firmware upgrade

Panel firmware upgrades from v3.06, or earlier, to v3.07 through v3.09 may lose events from the history log. The issue occurs during a reset or reboot of the control panel. The history log from the older panel should be uploaded prior to an upgrade to v3.07 - v3.09.
V3.10 resolves this issue and removes any corruption within the history log.

2.3 Known issues

This section examines the known issues of this firmware version.

2.3.1 Personal notification email

When using email personal notifications, some server configuration options (e.g. Gmail's 2-Step verification, Allow less secure apps: Off) may not work properly.

In order to ensure operation, disable additional email server options.

3 Firmware revision history

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

3.1 Firmware version 3.09.050

3.1.1 B444-A and B444-V support

The system now supports B444-A Plug-in cell module, AT&T LTE and B444-V Plug-in cell module, Verizon LTE.

B444-A/B444-V SIM card activation

Caution!

Activate the B444-A/B444-V SIM card before inserting. Failure to do so might result in failed communications to the control panel/module. Upon first power-up of the B444-A/B444-V, it might take up to 15 minutes for the activation process to be completed.

3.1.2 ANSI-SIA DC-09 format

The system now supports the following network communicator formats:

- Conettix Modem4
- Conettix ANSI-SIA Contact ID
- ANSI-SIA DC-09

Notice!

UL and ULC LISTED applications

ANSI-SIA DC-09 format is not available for UL and ULC LISTED applications.

3.1.3 Security of Connected Devices

In order to comply with the Security of Connected Devices Act (TITLE 1.81.26. Security of Connected Devices) and related legislation, this product uses a unique connection password.
The “RPS Passcode” for the initial connection to this product must match the unique Cloud ID of the product.
Ensure your RPS Operator uses the unique Cloud ID that is labeled on the product and included on the card in the box of the product.

3.1.4 Output Response Type operation

In control panel firmware v3.09.024, the configuration selections 1 and 2 of the Output Response Type operation were not working correctly.
This has been corrected in control panel firmware v3.09.050.
If you made changes in control panel firmware v3.09.024 to ensure proper operation, those changes are no longer required.

- In Output Response Type operation, return configuration selections 1 and 2 back to their expected, and documented, configuration.

3.2 Firmware version 3.08

3.2.1 Language support

Adds support for Dutch, German, and Swedish.

When both the control panel first language and the second language are set to Dutch, English, French, German, Hungarian, Italian, Portuguese, Spanish, or Swedish, the system uses the Standard, Latin-1 character set.
When either the control panel first language or the second language is set to Chinese, Greek, or Polish, the system uses the Extended, UTF-8 Unicode character set.

Notice!

Only B915/B915i and B942 keypads support Extended, UTF-8

Only B915/B915i keypads with firmware version 1.01.010 or higher, and B942 keypads with firmware version 1.02.022 or higher support the Extended, UTF-8 character set

3.2.2 Door shunt time

The longest possible selection for the door shunt time has been extended from 240 seconds to 8 hours.

This selection is available with the following firmware versions:

- Control panel firmware v3.08 or higher
- Remote Programming Software firmware v6.08 or higher
- B901 firmware version v1.05 or higher.

3.2.3 Backup destination devices

The control panel can send reports to four different route groups using one primary and up to three backup destination devices for each route group.

3.2.4 Custom test report

Either send a normal test report or a custom test report can be sent:

- Normal test report: Includes all route groups that have the test report function enabled, independent of which destination device is used to communicate. The test report is sent to the first successful destination device in a route group.

- Custom test report: You can select the route group and destination device you want to test. You can either test one destination device per route group or all configured destination devices for a route group.

3.3 Firmware version 3.07

Notable features

- *Incoming RPS connections, page 14*
- *B444 signal strength indication, page 14*
- *Stabilization of cell card performance, page 14*
- *APN usage for B442 and B443, page 15*

3.3.1 Incoming RPS connections

In addition to answering incoming calls from RPS using UDP (User Datagram Protocol), incoming calls from RPS using TCP (Transfer Control Protocol) are also supported. RPS version 6.07 is required for this modified connection method.

3.3.2 B444 signal strength indication

The B444 signal strength LED indication has been modified to more accurately represent performance. While LTE tower switching may still occur, their individual signal strength indications are more accurate.

3.3.3 Stabilization of cell card performance

Cell card stability enhancements are included within this firmware release.

3.3.4 APN usage for B442 and B443

The B442 and B443 plug-in cellular modules shall attempt connections using APNs in the following order:

1. Primary configured APN
2. gne
3. wyless.apn
4. wyless.com.attz

The plug-in cellular module will select and use the most appropriate APN.

If the APN is erroneous, the panel keypads may not display the details of this trouble condition.

3.4 Firmware version 3.06

Notable features

- *Language support, page 15*
- *Keypad programming, page 16*
- *PSTN, page 16*
- *Point Profile Circuit Style, page 16*
- *System Tamper Response, page 17*
- *Passcode [Esc], page 17*
- *Panel Event Log size, page 17*
- *New default for network Access Point Name (APN) parameter, page 17*

3.4.1 Language support

Adds support for Chinese, Greek, Hungarian, Italian, and Polish.

When both the control panel first language and the second language are set to English, French, Hungarian, Italian, Portuguese, or Spanish, the system uses the Standard, Latin-1 character set.
When either the control panel first language or the second language is set to Chinese, Greek, or Polish, the system uses the Extended, UTF-8 Unicode character set.

Notice!

Only B915/B915i and B942 keypads support Extended, UTF-8

Only B915/B915i keypads with firmware version 1.01.010 or higher, and B942 keypads with firmware version 1.02.022 or higher support the Extended, UTF-8 character set

3.4.2 Keypad programming

Added keypad programming options to the Installer Menu, such as a Device menu and a Miscellaneous menu. Detailed menu tree information can be found within the updated Installation Manual.

3.4.3 PSTN

Expanded PSTN compatibility parameter to support additional countries.

3.4.4 Point Profile Circuit Style

Expanded Point Profile Circuit Style options to include “Dual 1K EOL with Tamper”, “Single 1K EOL with Tamper”, and “Single 2K EOL with Tamper” selections. Selecting any of these styles enables sending the new Point Tamper Alarm and Point Tamper Alarm Restoral reports.

3.4.5 System Tamper Response

Added System Tamper Response parameter to configure system behavior and reporting during armed states.

3.4.6 Passcode [Esc]

Keypad Passcode [Esc] option now applies to both SDI and SDI2 keypads.

3.4.7 Panel Event Log size

Changed Panel Event Log size to: B3512=512, B4512=512, B5512=1024, B6512=1024.

3.4.8 New default for network Access Point Name (APN) parameter

Firmware version 3.06 and RPS version 6.05 changed the default network APN parameter to eaaa.bosch.vzwentp. The previous default - wyless.apn - is still valid. There is no need to change the APN for existing accounts.

3.5 Firmware version 3.05

Notable features

- *37 bit credentials with site code support, page 18*
- *B444 4G VZW LTE Cellular Support, page 18*
- *Brazil Daylight Saving Time scheme update, page 19*
- *Concurrent Mode 2 connections support, page 18*
- *Secure connections using TLS v1.1 and v1.2 now supported, page 19*

Corrections

- *“Ready to turn on” indication, page 19*
- *Custom function unbypass, page 20*
- *Force arming with faulted non-bypassable points , page 20*
- *Shared area reports, page 20*
- *Fire walk test for multiple latching smokes on one circuit, page 20*
- *Bypassed points incorrectly reviewed, page 21*
- *Open/Close personal notifications, page 21*
- *Automation Mode 2 and faulted points, page 21*
- *Aux power supply supervisory point silenced keypad display, page 21*

3.5.1 B444 4G VZW LTE Cellular Support

This firmware update supports the B444 Conettix Plug-in 4G VZW LTE Cellular Communicator. This module is for the US market only.
Note: Upon initial power-up of the B444 or B444-C, it can take up to 15 minutes for activation to complete. This will only occur during the first power application to the B444 and B444-C.

3.5.2 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.

3.5.3 37 bit credentials with site code support

For B6512 control panels only

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)

3.5.4 Secure connections using TLS v1.1 and v1.2 now supported

The firmware now supports secure connections, including personal notification email servers, using TLS v1.0 (strong ciphers only), v1.1, and v1.2. In previous versions of the firmware, control panel TLS connections required TLS v1.0 support.

3.5.5 Brazil Daylight Saving Time scheme update

Panels configured for “Brazil DST” will have the new Daylight Saving Time scheme now starting on the first Sunday of November, and in force since the beginning of 2018. The panels also support Carnival calendar variability.

3.5.6 “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.

3.5.7 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.

3.5.8 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.

3.5.9 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.

3.5.10 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.

3.5.11 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.

3.5.12 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.

3.5.13 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 v3.05.

3.5.14 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.

4 Open source software 3.10

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).
For more information, refer to the OpenSSL License on www.boschsecurity.com, under Product Catalog.

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