Control panels

G Series: B8512G, B9512G

en Release notes

Table of contents

1	**Introduction**	**4**
1.1	About documentation	4
1.2	Requirements	5
2	**Firmware version 3.11.5**	**8**
2.1	What's new	9
2.2	Corrections	9
2.3	Known issues	9
3	**Firmware revision history**	**12**
3.1	Firmware version 3.11	12
3.2	Firmware version 3.10	14
3.3	Firmware version 3.09.050	15
3.4	Firmware version 3.08	17
3.5	Firmware version 3.07	19
4	**Update a legacy account in RPS for 3.08**	**21**
4.1	Update an existing G Series control panel account to a B9512G/B8512G account	21
5	**Open source software 3.11.5**	**23**

1 Introduction

These Release Notes are for control panel firmware version 3.11.5.

1.1 About documentation

Copyright

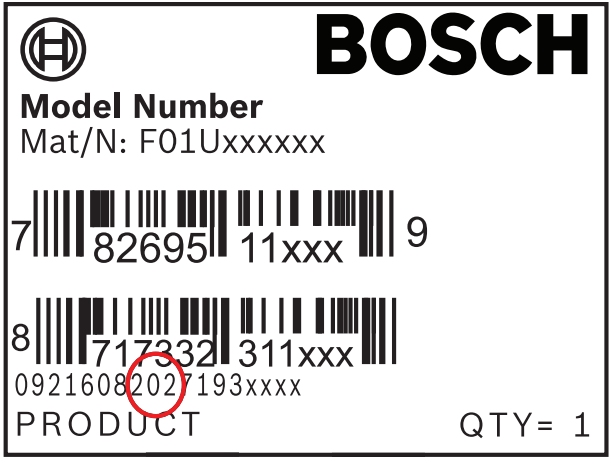
This document is the intellectual property of Bosch Security Systems B.V. and is protected by copyright. All rights reserved.

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 6.11 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 3.11.5

What's new

- *Improved connectivity to the Verizon network, page 9*
- *Update to the B444-A Cellular Communicator, page 9*

Corrections

- *History log corruption during firmware upgrade, page 9*

Known issues

- *Passcode security synchronization with RPS and new panel, page 10*
- *Programming new point types on firmware versions older than v3.11, page 10*
- *Personal notification email, page 11*
- *Keypad lockdown period (keypad lockouts on failed passcode attempts), page 11*

Refer to

- *Environmental point types, page 12*
- *Support for updated B and G Series control panel certificates, page 14*
- *Configurable passcode security, page 12*
- *FIPS compliant control panel firmware, page 13*
- *Temporary passcode, page 13*
- *Panic point type, page 12*
- *IP camera wired input support, page 13*
- *B9512G IP camera support, page 13*

2.1 What's new

This section examines the new features of this firmware version.

2.1.1 Improved connectivity to the Verizon network

FW V3.11.5 improves the management of the Verizon APN when using the B444-V or B444 Cellular Communicators, resulting in enhanced connection reliability.

2.1.2 Update to the B444-A Cellular Communicator

This firmware release configures the B444-A to insure that LTE connectivity is not disrupted when the AT&T 3G network is discontinued.

2.2 Corrections

This section examines the corrections made in this firmware version.

2.2.1 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 Passcode security synchronization with RPS and new panel

When connecting to a new control panel with v3.11 firmware using RPS v6.11, and then receiving the configuration from the new panel, the next send/receive option will open the Panel Synchronization window because the Passcode Security parameter in the control panel does not match the setting of the Passcode Security parameter in RPS.
Clicking the **See data differences** option in the Panel Synchronization window does not show a difference between the Passcode Security parameter in RPS and the control panel.

Recommendation

Send the RPS configuration to the panel to make RPS and the panel Passcode Security parameters match.

2.3.2 Programming new point types on firmware versions older than v3.11

When using RPS 6.11 to program a new Panic Point or Environmental Point (Water, High Temp, Low Temp) on a control panel system with earlier firmware versions than v3.11, the system will not generate alerts and conditions as expected.
For some scenarios, the Low Temp point type will generate a trouble event and in all scenarios the Panic, Water and High temp point types will not generate any event condition.

Recommendation

Upgrade the control panel firmware to v3.11 or higher if these new point types are needed.

2.3.3 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.

2.3.4 Keypad lockdown period (keypad lockouts on failed passcode attempts)

If the value of lockout time is beyond 6553 seconds, the keypad lockout operation may not work properly. In order to ensure operation, set the lockout time below 6553 seconds.

3 Firmware revision history

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

3.1 Firmware version 3.11

3.1.1 Panic point type

Added the Panic point type to the panel, which is a 24-hr burglary alarm intended for a panic input device.

3.1.2 Environmental point types

New point types are available:

- Water - alarm to a indicate water leak event.
- High Temp - alarm for a high temperature event.
- Low Temp - alarm for a low temperature event.

3.1.3 Configurable passcode security

User passcode tamper is now configurable for keypads and Automation clients to detect and act based on a defined number of invalid authentication attempts.

3.1.4 Temporary passcode

A one-time (single use) disarm authority passcode can be granted to a user for 1 or multiple control panel areas for temporary access. The associated authority level defines the user as a temporary user and only allows the user to disarm the system once, then the authority/passcode expires.

3.1.5 IP camera wired input support

The IP Camera Point Source now includes 2 wired inputs of an IP camera.
Configure the IP camera sources in RPS Point Assignments within Point groups. For example, Points 10 and 19 for IP camera 1, Points 20 and 29 for IP camera 2, Points 30 and 39 for IP camera 3, up to the number of cameras available on each control panel type.

3.1.6 B9512G IP camera support

The B9512G panel now supports up to 59 IP cameras.

3.1.7 FIPS compliant control panel firmware

RPS has been updated to operate in a secured Windows environment, such as FIPS (Federal Information Processing Standards).

– An additional AES/SHA encrypted firmware package is available for the B Series and G Series control panels in the Downloads > Software section of the Bosch Intrusion product catalog. This firmware can be used by any RPS 6.11 or newer installation.
– The appropriate firmware encrypted file is named by control panel type, firmware version number with the _SHA.fwr extension to indicate SHA encryption (B9512G_ B8512G_FW_3.11.xxx_SHA.fwr).

3.1.8 Support for updated B and G Series control panel certificates

Control panel firmware v3.11 introduces a new security certificate in advance of the current certificate expiration in April, 2022. This certificate is used for most automation (integration) and RPS TLS connections to the panel. The panel Cloud certificate is not affected. All Cloud connections will continue to function as they do today.
RPS v6.11 has been updated to accommodate this new panel security certificate automatically.

Notice!

Important

Customers upgrading or installing panels with firmware v3.11 must upgrade RPS to v6.11, and review other integrated applications (Bosch or 3rd Party) that need to use the new Bosch certificate, in order to maintain TCP connections to the panel after March, 2022.

Customers using RPS with panel firmware v3.10 or older will not be affected by the certificate expiration and operations will continue without interruption.

3.2 Firmware version 3.10

3.2.1 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.

3.2.2 UL 864 - 10th Edition

This firmware version now supports the latest edition of:
– UL 864 - Control Units and Accessories for Fire Alarm Systems (Commercial Fire)

3.2.3 UL 985 - 6th Edition

This firmware version now supports the latest edition of:
– UL 985 Household Fire Warning Systems Units

3.3 Firmware version 3.09.050

3.3.1 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.

3.3.2 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.

3.3.3 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.

3.3.4 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.

3.4 Firmware version 3.08

3.4.1 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

3.4.2 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.

3.4.3 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.

3.4.4 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.

3.4.5 Incorrect output behavior

In panel firmware v3.08.002, regardless of panel programming, output 3(C) activates any time an on-board point is faulted. This is resolved in panel firmware v3.08.004.

3.5 Firmware version 3.07

Notable features

– *Incoming RPS connections, page 19*
– *B444 signal strength indication, page 19*
– *Stabilization of cell card performance, page 19*
– *APN usage for B442 and B443, page 19*

3.5.1 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.

3.5.2 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.

3.5.3 Stabilization of cell card performance

Cell card stability enhancements are included within this firmware release.

3.5.4 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.

4 Update a legacy account in RPS for 3.08

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, then right-click the account and select Panel Data 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. When you upgrade a control panel to a B8512G or a B9512G, RPS makes an account copy automatically.

4. 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. Enter the current Panel Passcode into the RPS Passcode text box and click connect. The Panel Sync dialog box appears.
4. Select Send ALL Updated RPS Data to Panel and click OK. Note: Do not select Receive Panel Data.
5. When the Send ALL RPS data progress completes, you can exit from RPS.

5 Open source software 3.11.5

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
© Bosch Security Systems B.V., 2021

202107151456