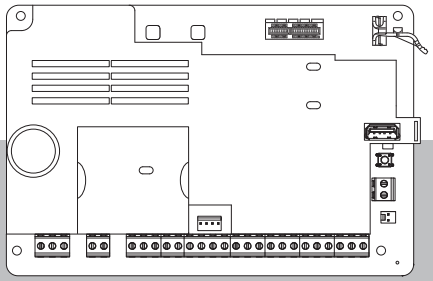
Control panels

B Series: B6512, B5512, B4512, B3512



en Release notes

Table of contents

1 Introduction

These *Release Notes* are for control panel firmware version 3.14.100.

1.1 About documentation

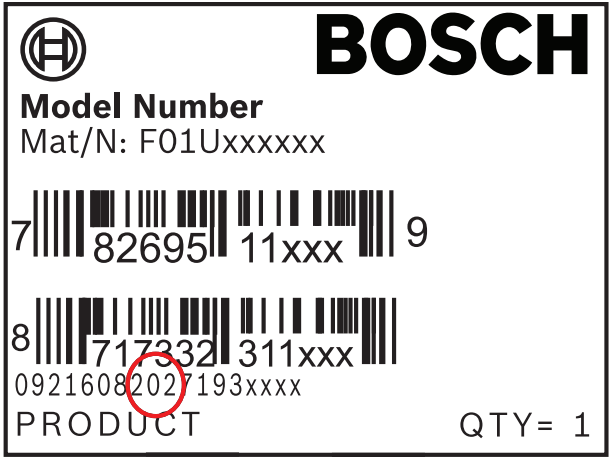
Copyright

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 B.V. 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 6.14.001_SP1 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 3.14.100

What's new

– *Support for 32-Bit HID access control credentials - B6512 only, page 8*

2.1 What's new

This section examines the new features of this firmware version.

2.1.1 Support for 32-Bit HID access control credentials - B6512 only

Support of 32-Bit MIFARE Classic credential allows customers who use the MIFARE Classic format access cards to use these cards with the B6512 and the B901 Access Control interface.
This is in addition to the previously supported 26-bit, 35-bit, and 37-bit format.

3 Firmware version 3.14.012

What's new

Corrections

Known issues

Refer to

- *B444-A Plug-in Cellular Communicator Module Is Not Recognized, page 14*
- *Fail to Close Report, page 15*

3.1 What's new

This section examines the new features of this firmware version.

3.1.1 B444-A2 Plug-in Cellular Communicator support

New cellular module support for the B444-A2 Plug-in cell module, AT&T LTE.

3.1.2 B444-V2 Plug-in Cellular Communicator support

New cellular module support for the B444-V2 Plug-in cell module, Verizon LTE.

3.2 Corrections

This section examines the corrections made in this firmware version.

3.2.1 Force Arm Returnable Updated

In previous firmware versions, when the Force Arm Returnable parameter of a point profile was set to YES, after disarming the system, the user had to manually unbypass any forced points with that profile. With firmware version 3.14.010, when the Force Arm Returnable parameter is set to YES, any forced point(s) will automatically unbypass and return to normal, once the system is disarmed.

3.2.2 Entering 26-bit Card Type access data from keypad

In firmware version 3.11 and 3.12, access card data being entered from a keypad did not upload to the control panel accurately.

3.2.3 Door Unlock command from a SKED or Custom Function

In firmware version 3.11, the Door Unlock feature allowed a user to unlock a door via a SKED or Custom Function, even if the area was armed. This correction prevents the Door Unlock command from a SKED or Custom Function during an armed state.

3.2.4 Panel will not fall back to "cloud over cellular" connection if Ethernet DNS failure occurs

If both Ethernet and cellular Cloud Remote Connect parameters are enabled, the panel will not switch to “cloud over cellular” if “cloud over Ethernet” connection has a DNS failure. This issue has been corrected.

3.2.5 Cellular operation may fail if Ethernet DNS is not public

When programming a specific DNS server IP address for IPv4 Ethernet, it will be shared by cellular. If the IPv4 DNS address for Ethernet is not accessible on the public network, then the cellular interface will be unable to resolve URLs.
When using both on-board Ethernet and cellular, a private IPv4 DNS is required for Ethernet. A separate DNS setting for plugin cellular is now available.

3.3 Known issues

This section examines the known issues of this firmware version.

3.3.1 Area Opening Report not sent when switching from All-On to Part-On arm state

An **Area Open Report** might not send if a user changes the area from **All-On**, then to **Part-On**, and then disarms. When switching from **Part-On to Disarm**, **Area Open Reports** are only sent if **Part-On Reports** are enabled. These reports are off by default. Enabling the **Part-On Reports** addresses this issue.

3.3.2 Technical Bulletin - G Series, B Series personal notification email

The personal notification email messaging may stop working for some customers, due to email provider security features using Two-Step Verification. Use the email provider's security page (Google, for Example) to create an App Password. That password will be used in the control panel, as the email server Authentication Password, to allow the personal notification emails to function. Please see the "Technical Bulletin G Series, B Series personal notification email" for more information.

4 Firmware version 3.12.024

What's new

- *B444-A Plug-in Cellular Communicator Module Is Not Recognized, page 14*
- *Fail to Close Report, page 15*

Refer to

- *Support for 35-Bit HID access control credentials (B6512 only), page 18*
- *Enhanced AT&T cellular communications, page 18*

4.1 What's new

This section examines the new features of this firmware version.

4.1.1 B444-A Plug-in Cellular Communicator Module Is Not Recognized

Some B444-A cellular modules may report as "invalid" during installation and will not be recognized by the B or G Series control panel. This firmware version allows the cellular host device to properly recognize these B444-A modules.

4.1.2 Fail to Close Report

Some problematic Arming scenarios may send a Fail to Close report. This report should only be sent if the Area has not been Closed at the end of the Closing Window. This firmware version resolves this potential issue.

5 Firmware revision history

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

5.1 Firmware version 3.12.020

What's new

- *Support for 35-Bit HID access control credentials (B6512 only), page 18*
- *Enhanced AT&T cellular communications, page 18*

Corrections

- *Forced Arming Issue with Firmware 3.11.530, page 18*

Known issues

- *Passcode security synchronization with RPS and new panel, page 19*
- *Programming new point types on firmware versions older than v3.11, page 20*
- *Personal notification email, page 20*
- *Keypad lockdown period (keypad lockouts on failed passcode attempts), page 21*

Refer to

- *B444-A Plug-in Cellular Communicator Module Is Not Recognized, page 14*
- *Fail to Close Report, page 15*
- *Improved connectivity to the Verizon network, page 21*
- *Environmental point types, page 22*
- *Support for updated B and G Series control panel certificates, page 24*
- *Configurable passcode security, page 23*
- *FIPS compliant control panel firmware, page 24*
- *Temporary passcode, page 23*
- *Panic point type, page 22*
- *IP camera wired input support, page 23*
- *History log corruption during firmware upgrade, page 22*
- *Holiday Index 2, page 21*

5.1.1 What's new

This section examines the new features of this firmware version.

5.1.1.1 Support for 35-Bit HID access control credentials (B6512 only)

Support of 35-bit HID credentials allows customers who use the Corporate 1000 format to use these cards with Bosch panels and the B901 Access Control interface. This is in addition to the 26-bit and 37-bit format cards that were previously supported. Note that this feature is available only for the B6512 control panel.

5.1.1.2 Enhanced AT&T cellular communications

Enhancements have been added to improve B444-A operation and accommodate changes in the AT&T cellular network associated with the upcoming 3G sunset.

5.1.2 Corrections

This section examines the corrections made in this firmware version.

5.1.2.1 Forced Arming Issue with Firmware 3.11.530

The 3.12 firmware version corrects an issue regarding the force-arm feature in our B9512G, B8512G, B6512, B5512, B4512 and B3512 control panels that may cause

points that have been force-armed to remain bypassed with no indication at the keypad. Note that this issue exists only in firmware version 3.11.530.

5.1.3 Known issues

This section examines the known issues of this firmware version.

5.1.3.1 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.

5.1.3.2 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.

5.1.3.3 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.

5.1.3.4 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.

5.2 Firmware version 3.11.5

5.2.1 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.

5.2.2 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.

5.2.3 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.

5.3 Firmware version 3.11

5.3.1 Panic point type

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

5.3.2 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.

5.3.3 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.

5.3.4 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.

5.3.5 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.

5.3.6 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 (*B3512_B4512_ B5512_ B6512_FW_3.11.xxx_SHA.fwr*).

5.3.7 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.

5.4 Firmware version 3.10

5.4.1 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.

5.4.2 UL 985 6th Edition

This firmware version now supports the latest edition of:

– UL 985 Household Fire Warning Systems Units

5.5 Firmware version 3.09.050

5.5.1 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.

5.5.2 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.

5.5.3 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.

5.5.4 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.

6 Open source software 3.14.100

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

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 B.V.
Torenallee 49
5617 BA Eindhoven
Netherlands
www.boschsecurity.com

Building solutions for a better life.

202304281627