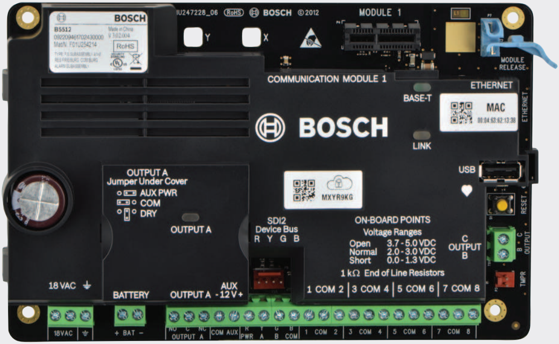


Control Panels

B6512/B5512/B4512/B3512 (B5512E/B4512E/B3512E)

en Release Notes

Table of contents

1 Introduction

These *Release Notes* are for control panel firmware version 3.03.014.

1.1 About documentation

Copyright

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

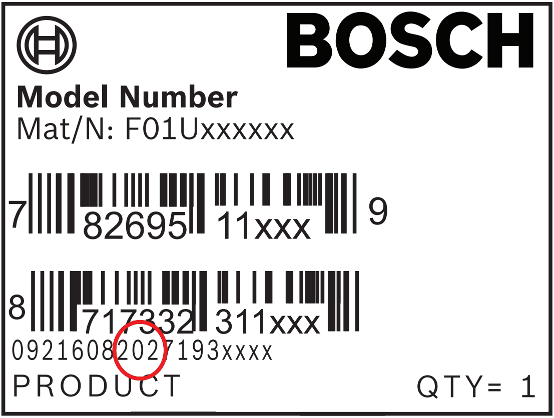
Trademarks

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, 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.



1.1.1 Related documentation

*Control Panels (B5512/B4512/B3512) Release Notes** (this document)
Control Panels (B5512/B4512/B3512) Installation and System Reference Guide (P/N: F01U287180)⁺
Control Panels (B9512G/B8512G/B5512/B4512/B3512) Owner's Manual (P/N: F01U287181)* ⁺
Control Panels (B5512/B4512/B3512) Program Entry Guide (P/N: F01U287183)⁺
Control Panels (B5512/B4512/B3512) UL Installation Guide (P/N: F01U287185)* ⁺

Control Panels (B5512/B4512/B3512) SIA Quick Reference Guide (P/N: F01U287184)* +
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.

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 program all new features of this firmware version, you must use RPS version 6.03 or higher.

1.2.2 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

Receiver/Gateway	**CPU version**	**D6200 version**
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

2 Version 3.03.014 firmware

What’s new

- *B6512 control panels, page 10*
- *ULC-S559 listing, page 10*
- *ULC Canada Compliance affects keypad message during firmware updates, page 10*
- *Remote Connect Service support, page 11*
- *Date/time formats, page 11*
- *Input point End-of-line options, page 11*
- *Control panel disconnect no longer required, page 12*
- *Watch mode after power up, page 12*
- *Comm Trouble sound options, page 12*
- *Updated B440/B441 support, page 12*

Corrections

- *Event log and automation, page 13*
- *Force arm permission and manually bypassed, page 13*
- *Off-normal test reports no longer generated for non-faulted intrusion points, page 13*
- *Ready to arm on systems with wireless points, page 14*
- *Control panel and RPS synchronized, page 14*

Known issues

- *Email servers require TLS v1.0, page 15*
- *Manual alarm history events, page 15*
- *Open/Close personal notifications, page 15*
- *Custom function for bypassing points and delay, page 15*
- *IP address error with B426, page 16*
- *Dual Authentication and Auto Re-Arm, page 16*
- *Erroneous “Ready to turn on” indication, page 16*

2.1 What's new

This section examines the new features of this firmware version.

2.1.1 B6512 control panels

The new B6512 control panel supports up to 100 users, 6 custom functions, up to 6 areas, up to 96 points, up to 91 outputs, up to 12 supervised keypads, and up to 4 door controllers.

2.1.2 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 ULC-S559 system or a ULC-S304 system.

2.1.3 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.

2.1.4 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.

2.1.5 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.

2.1.6 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).

2.1.7 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.

2.1.8 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).

2.1.9 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.

2.1.10 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.

2.2 Corrections

This section examines the corrections made in this firmware version.

2.2.1 Event log and automation

In a previous firmware version, when using automation and the control panel history log reached the maximum stored events, the event data returned to automation became inconsistent.

This is resolved in this firmware version.

2.2.2 Force arm permission and manually bypassed

Force arm permission is no longer required to arm a system that has points that were previously bypassed. If there are points in a system that were previously bypassed by user with bypass permission, a user can now arm the system without force arm permission.

In previous versions, only users with force arm authority could arm the system with bypassed points.

2.2.3 Off-normal test reports no longer generated for non-faulted intrusion points

When the Expand Test Report parameter is set to Yes, the control panel expands test reports to include off-normal system status information. The control panel expands manually initiated test reports and SKED initiated (scheduled) test reports. Previously, the control panel included some intrusion points in the expanded test report whose status was not off-normal. This issue is corrected.

Also, when Expand Test Reports is set to No, the system reports normal or off-normal control panel status. Previously, the control panel generated off-normal for points whose status was not off-normal.

2.2.4 Ready to arm on systems with wireless points

For systems with wireless points configured, after a system restart it was possible the ready to arm function would not operate as expected. In those cases, the LED would not update and the keypad would not show the list of faulted points when arming for both wireless and wired points. Once the system was reset and operating properly, the system would continue to operate properly. Alarm processing and the watch tone feature were not impacted.
This issue is resolved in this firmware version.

2.2.5 Control panel and RPS synchronized

In a previous firmware version, RPS might require you to perform a receive (Receive Panel Data) from the control panel in order to show the account record as synchronized, without having made changes at the control panel.
This is resolved in this firmware version.

2.3 Known issues

This section examines the known issues of this firmware version.

2.3.1 Email servers require TLS v1.0

Personal notifications using email require that the email provider’s server supports TLS v1.0. Higher versions of TLS are not currently supported.

2.3.2 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.

2.3.3 Open/Close personal notifications

Control panels configured to send Open/Close event personal notifications restricted by authority level, will incorrectly send the Open/Close events for the restricted user over personal notifications. For example, if the control panel is configured so that Open/Close events are not sent for users with authority level 1, the control panel will still send the notification.
This issue does not impact events sent to the central station receiver.

2.3.4 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 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.

2.3.5 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.

2.3.6 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.

2.3.7 Erroneous “Ready to turn on” indication

For systems with a B810 RADION or B820 Inovonics wireless receiver, after a control panel reboot keypads might not display the proper Ready to turn on indication. For example, showing “Ready to turn on” while points are faulted. If this occurs, power cycle the control panel and the B810/B820, wait two minutes, and then retest. The keypads should now provide the proper Ready to turn on indications.

3 Firmware revision history

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

3.1 Version 3.02 firmware revision history

Notable features

- *Bosch VMS integration support, page 17*

3.1.1 Bosch VMS integration support

Bosch Video Management System integration

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.

Requirements to integrate Bosch VMS with a control panel:

- A licensed Bosch VMS system using Professional Editions v5.5 or higher or Bosch VMS Enterprise
- Edition v5.5 or higher.

- Expansion license to integrate the intrusion control panel. One license needed per control panel. Order number MBX-XINT-xx for the expansion license added to a Bosch VMS base license. Refer to the Bosch Video Management Software product page on the Bosch website, www.boschsecurity.com.
- Access to Remote Programming Software (RPS).

3.2 Version 3.01 firmware revision history

Notable features

- *Dual EOL resistor circuit style, page 18*
- *Better alignment with B9512G/B8512G , page 19*
- *Improved Automation security, page 19*

Corrections

- *B3512 on-board outputs, page 19*

3.2.1 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.

3.2.2 Better alignment with B9512G/B8512G

With control panel firmware v3.01 the B5512, B4512, and B3512 control panels share the RPS user interface and parameter organization with the new B9512G and B8512G control panels.

3.2.3 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.

3.2.4 B3512 on-board outputs

In firmware v2.03 and v2.04, commands to turn on on-board output, when sent from a keypad to the B3512, did not turn the outputs on. This issue is resolved in this firmware version.

3.3 Version 2.04 firmware revision history

Notable features

- *Cellular library enhancements, page 19*

3.3.1 Cellular library enhancements

This firmware version includes enhancements to the control panel cellular library to improve cellular connection robustness.

3.4 Version 2.03.018 firmware revision history

Notable features

- *Full support for integrated (connected) Bosch IP cameras, page 20*

3.4.1 Full support for integrated (connected) Bosch IP cameras

This firmware version offers full support for connected Bosch IP cameras, including the ability to view IP camera video from within the Remote Security Control (RSC) app v2.3.x or higher.

4 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.

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

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