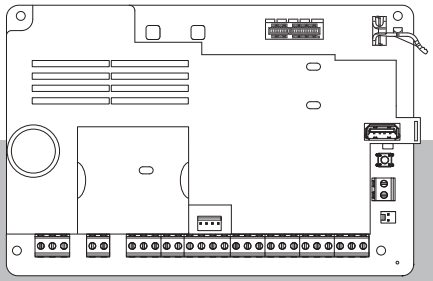
radionix

Control panels

B Series: B6512, B5512, B4512, B3512



en Release notes

Table of contents

1	**Introduction**	**5**
1.1	About documentation	5
1.2	Requirements	6
2	**Firmware version 3.15.116**	**9**
2.1	What's new	9
2.2	Corrections	9
3	**Firmware version 3.15.110**	**10**
3.1	What's new	10
3.2	Corrections	10
4	**Firmware version 3.15.024**	**12**
4.1	What's new	12
4.2	Corrections	14
5	**Firmware revision history**	**18**
5.1	Firmware version 3.14.100	18
5.2	Firmware version 3.14.012	18
5.3	Firmware version 3.12.024	21
5.4	Firmware version 3.12.020	22
5.5	Firmware version 3.11.5	26

6 Programming the control panel for SIA Compliance 28

7 Minimum system requirements for ANSI/SIA CP-01 33

8 Open source software 3.15.116 34

1 Introduction

These *Release Notes* are for control panel firmware version 3.15.116.

1.1 About documentation

Copyright

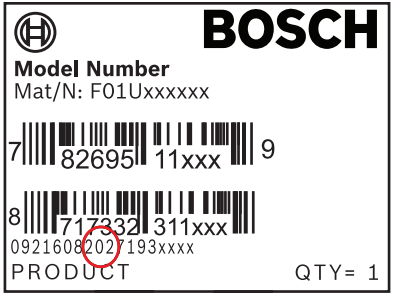
This document is the intellectual property of Radionix and is protected by copyright. All rights reserved.

Trademarks

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

Radionix product manufacturing dates

For product manufacturing dates, go to https://www.keenfinity-group.com/xc/en/datecodes/ and refer to the serial number located on the product label.
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 6.15 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 3.15.116

Corrections

– *Fixed an error with a latched "Route Group Comm Fail" message not clearing after a comm recovery, page 9*
– *Fixed a memory leak on the panel, page 9*
– *Fixed sending text in UTF-8 mode, page 9*

2.1 What's new

This section examines the new features of this firmware version.

This version of firmware only contains fixes.

2.2 Corrections

2.2.1 Fixed an error with a latched "Route Group Comm Fail" message not clearing after a comm recovery

2.2.2 Fixed a memory leak on the panel

2.2.3 Fixed sending text in UTF-8 mode

3 Firmware version 3.15.110

3.1 What's new

This section examines the new features of this firmware version.

3.1.1 UPnP Enable default changed to Disable

The factory default has been changed to Disable UPnP to provide a more secure environment and avoid Denial of Service attacks. For added protection, Keenfinity recommends disabling UPnP in your existing devices and removing all port forwarding rules pertaining to Bosch communication products from your router.

3.2 Corrections

This section examines the corrections made in this firmware version.

3.2.1 Removed 3DES cipher from TLS 1.2

Due to potential security risks, the 3DES cipher was removed from TLS 1.2.

3.2.2 Panel will correctly identify and update the B812

The control panel was updated to support recognition of the B812, enabling operation, firmware updates, and RPS diagnostics.

3.2.3 Panel will correctly identify the B532 in RPS diagnostics

The control panel was updated to support the correct recognition of the B532 for RPS diagnostics.

4 Firmware version 3.15.024

What's new

– *UL 2610 2nd Edition Certification, page 12*
– *Enhanced Security, page 12*
– *Compatibility with B532 Aux. power supply and SDI2 extender , page 13*
– *Mode 2 support, page 13*

4.1 What's new

4.1.1 UL 2610 2nd Edition Certification

Commercial Premises Security Alarm Units and Systems

4.1.2 Enhanced Security

– Configuration of minimum supported TLS version 1.2;

Warning!



This version of panel firmware will enforce the use of TLS 1.2. The TLS setting can only be set to TLS 1.0 or 1.1 using RPS version 6.15 and higher. If you have tools that require TLS versions 1.0 or 1.1, DO NOT update the panel firmware until you have RPS 6.15 or higher.

Note: When a B426 or B450 is also in use in the system, these modules must also update their firmware to version 3.15 to enforce the TLS settings.

- Disabling of non FIPS compliant TLS ciphers;
- Updated TLS and network stack libraries;
- Verified to NIST CAVP (cert # A5272);
- Temporary programmable lockout after five consecutive remote access password failures.

4.1.3 Compatibility with B532 Aux. power supply and SDI2 extender

4.1.4 Mode 2 support

Additional mode 2 support for:

- User management;
- Authority level configuration;
- Holiday indexes;
- Open/close windows.

4.2 Corrections

4.2.1 Corrected POPIT Missing which occurred during a programming update

Addresses Technical Bulletin dated August 30, 2024.

4.2.2 Fixed issue where phone could not be restored after a phone comm trouble

4.2.3 Fixed "Data Out of Range" error when adding a new user with BSM

4.2.4 Improved Mode 2 handling of "configured users"

4.2.5 Removed double logging of "Invalid Remote Access" event when Ethernet is disconnected during an RPS or Cloud Connection

4.2.6 SDI2 reports for open wire faults with Modem 4 are now being sent

4.2.7 Power supply "over current" reports for each output are now being sent

4.2.8 Power Supply AC Fail event now follows resend AC Fail setting

4.2.9 Improved Battery status updates for B520/B532 Power Supply

4.2.10 Keypad Output Pattern now stops if removed from panel configuration

4.2.11 Mode 2 Arm Panel Areas is no longer force arming unless directed to do so

4.2.12 Corrected "Service Parameter" fault that may occur while bypassing points from a keypad

4.2.13 B901 trouble can now be cleared

4.2.14 User's Name change event is now logged to panel event log

4.2.15 Fixed issue with Mode 2 PIE Point State not always updating correctly

4.2.16 Automatic Door Locked even is now sent to the receiver

4.2.17 Updated handling of expired TLS certificates

4.2.18 Corrected issue sending e-mail to a server using IPv6

4.2.19 Updates to B430 Modem Transmit levels

4.2.20 When a user changes a passcode from the keypad installer menu, it no longer generates a Point Change response

4.2.21 Updates to B915 and B920 text when multiple alarms are present

4.2.22 Fixed issue where silent alarm can become audible before the configured two failures to send the event

5 Firmware revision history

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

5.1 Firmware version 3.14.100

5.1.1 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.

5.2 Firmware version 3.14.012

5.2.1 B444-A2 Plug-in Cellular Communicator support

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

5.2.2 B444-V2 Plug-in Cellular Communicator support

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

5.2.3 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.

5.2.4 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.

5.2.5 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.

5.2.6 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.

5.2.7 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.

5.2.8 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.

5.2.9 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.

5.3 Firmware version 3.12.024

5.3.1 What's new

This section examines the new features of this firmware version.

5.3.1.1 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.

5.3.1.2 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.

5.4 Firmware version 3.12.020

5.4.1 What's new

This section examines the new features of this firmware version.

5.4.1.1 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.

5.4.1.2 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.

5.4.2 Corrections

This section examines the corrections made in this firmware version.

5.4.2.1 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.

5.4.3 Known issues

This section examines the known issues of this firmware version.

5.4.3.1 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.

5.4.3.2 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.

5.4.3.3 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.

5.4.3.4 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.

5.5 Firmware version 3.11.5

5.5.1 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.

5.5.2 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.

5.5.3 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.

6 Programming the control panel for SIA Compliance

Parameter name	Required control panel settings for SIA Compliance	Default
Phone #	(Prefix backup phone number with Call Waiting[1] disable command)	{Blank}
Duress Type	Option 3[2]	0 (Disabled)
Cancel Reports	Yes	Yes
Exit Delay Time	45 seconds to 255 seconds	60 seconds
Duress Enable	Yes	No
Exit Delay Restart	Yes or No	Yes
All On - No Exit	Yes or No	Yes

Two Man Rule?	No	No
Early Ambush?	No	No
Exit Delay Warning	Yes	Yes
Entry Tone	Yes	Yes
Exit Tone	Yes or No	Yes
Abort Display	Yes or No	Yes
Cancel Display	Yes or No	Yes
Verify time	10 to 60 seconds	60 seconds
Passcode Enter Function	Arm/Disarm	Arm/Disarm

All On Instant	- (Disabled)	- (Disabled)
Part On Instant	- (Disabled)	- (Disabled)
Send Duress	- (Disabled) or E (Enabled)	E (Enabled)
Disarm	- (Disabled) or E (Enabled)	E (Enabled)
Passcode Disarm	- (Disabled) or E (Enabled)	E (Enabled)
Entry Delay	30 seconds to 240 seconds	30 seconds
Alarm Abort	Yes or No	Yes
Abort Window	15 seconds to 45 seconds	30 seconds
Passcode Length	3 to 6 digits	Disabled
Swinger Bypass Count	1 to 2 trips[3]	2 trips

Remote Warning	Yes	Yes
Cross Point Timer	5 to 255 seconds	20 seconds
Cross Point	Yes or No[4]	No
Walk Test (All Non Fire Burg Points	E (Enabled)	E (Enabled)
Walk Test All Fire Points	E (Enabled)	E (Enabled)
Delay Response, Disarmed	00:00	00:00
Delay Response, Armed	00:00	00:00

[1]Call waiting does not apply to cellular networks or PSDN (Public Switched Data Network) communication. A call waiting disable command on a non-call waiting line will prevent successful connection to the central station.
[2]L14 is the default duress authority level.
[3]Swinger bypass count is programmable up to 4 trips. For SIA compliance, set to 1 or 2.
[4]Cross points must overlap (protect the same area) so that a single point can protect the area individually.

7 Minimum system requirements for ANSI/SIA CP-01

Minimum system requirements for classification in accordance with ANSI/SIA CP-01:

- UL Listed and Classified control unit Model B6512, B5512, B4512, or B3512
- UL Listed and Classified keypad Model B942/B942W, B930, B921C/B921CW, B920, or B915/B915I
- UL Listed Local Bell
- Off -premises transmission means

8 Open source software 3.15.116

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

Radionix B.V.
Achtseweg Zuid 173
5651 GW Eindhoven
The Netherlands
www.radionix.com
© Radionix 2026

Radionix LLC
130 Perinton Pkwy.
Fairport, NY 14450
USA
www.radionix.com
© Radionix 2026

202610271538