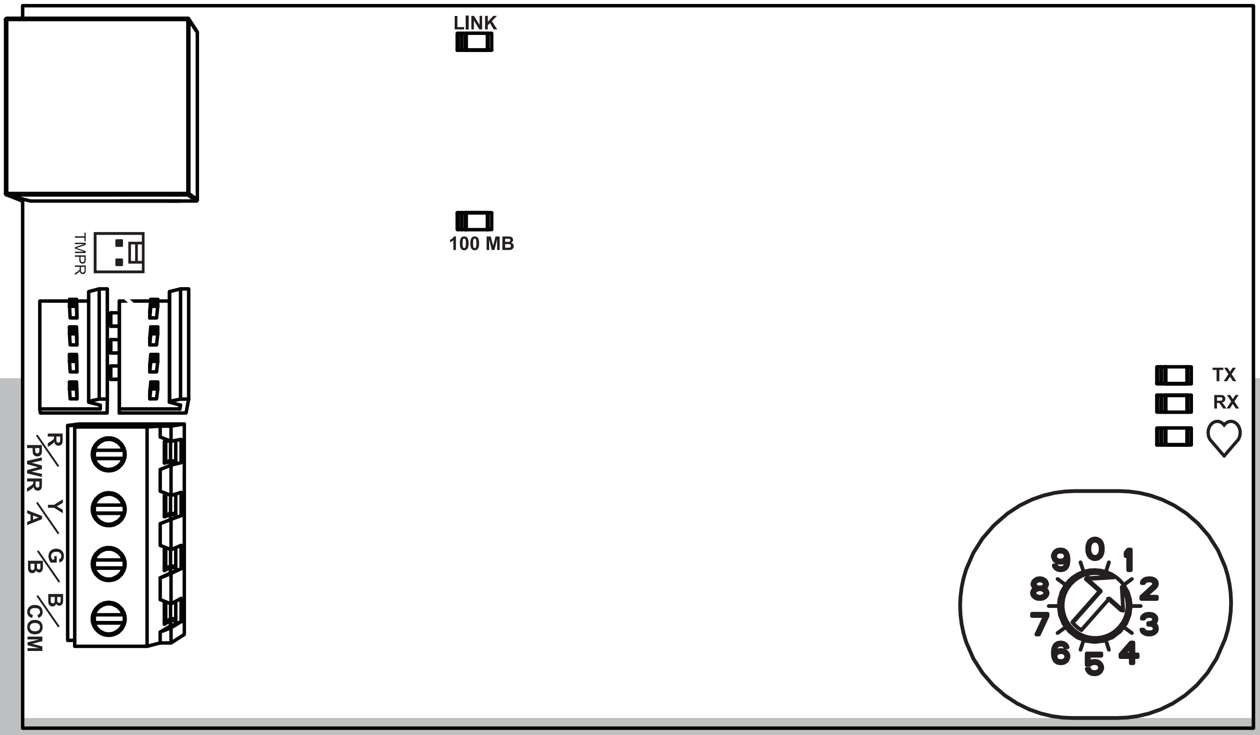
BOSCH

Conettix Ethernet Communication Module

B426



en Release Notes

Table of contents

1 **Introduction** 5
1.1 Requirements 5
1.2 About documentation 6
2 **Firmware version 3.15.014** 7
2.1 What's new 7
2.1.1 Security improvements 7
2.2 What's fixed 7
2.2.1 RPS fails to connect 7
2.2.2 HTTPS Port Number configuration 7
2.2.3 Expired TLS Certificate 7
3 **Firmware version 3.11** 8
3.1 What's new 8
3.1.1 Support for updated B426 certificates 8
4 **Firmware version 3.10** 9
5 **Firmware version 3.09** 10
5.1 What's new 10
5.1.1 California Security of Connected Devices Act 10
6 **Firmware version 3.08** 11
6.1 What's fixed 11
6.1.1 Updates to the bootloader 11
6.1.2 Updates to TCP keep alive 11
6.1.3 Updates to the web server 11
7 **Firmware version 3.06** 12
7.1 What's new 12
7.1.1 Incoming RPS connections 12
7.1.2 Secure connections using TLS v1.1 and v1.2 now supported 12
8 **Firmware version 3.05** 13
8.1 What's new 13
8.1.1 Remote Connect Service support 13
8.2 Known issues 13
8.2.1 Network Module Trouble with 2 modules 13
8.2.2 IP address error on keypads 13
9 **Firmware version 3.04.001** 14
9.1 What's new 14
9.1.1 Configuration using option bus control panels 14
9.1.2 SIA DC09 event reporting support for AMAX control panels 14
9.2 Corrections 14
9.2.1 Configuration pages 14
9.3 Known issues 14
9.3.1 Network Module Trouble with 2 modules 14
9.3.2 IP address error on keypads 14
10 **Revision history** 15
10.1 Version 3.03.009 firmware 15
10.1.1 Security protocol support 15
10.1.2 TCP connection timeouts 15
10.2 Version 3.03.007 firmware 15
10.2.1 High traffic network enhancements 15
10.3 Version 3.03 firmware 15

10.3.1 Solution 2000/3000 control panel support **15**

10.3.2 Email notifications **15**

10.3.3 Increased IPv6 compatibility **16**

10.3.4 Event reporting using CSV-IP protocol **16**

10.4 Version 3.02 firmware **16**

10.5 Version 3.01 firmware **16**

1 Introduction

These *Release Notes* are for the B426 with firmware version 3.15.014.

Notice!
Firmware version 3.15.014 is exclusively for the B426, B426-CN and B429-CN only. Do not install this firmware version on the B426-M.

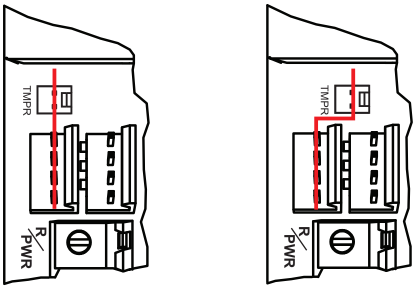
1.1 Requirements

Hardware identification for B426 modules

Notice!
B426-M firmware support
The B426-M supports firmware v3.03 and higher

Firmware v3.02 and higher require the new module hardware to operate. Modules with v3.01 firmware cannot update to this firmware version.
To determine a B426 hardware version, do one of the following:

- Compare the hardware to the diagram below. On the v3.01 hardware, the pins on the tamper switch connector align with the pins on one interconnect wiring connector. On the new hardware, the pins do not align.



v3.01 v3.02+

- Connect to the module using the web-based configuration and view the firmware version on the Device Information (home) page.

Compatibility

Control panels - B426	B9612G B8612G B6612 B5612 B4612 B9512G B8512G B6512 B5512 B4512 B3512 D9412GV4/D7412GV4/D7212GV4 D9412GV3/D7412GV3/D7212GV3 D9412GV2/D7412GV2/D7212GV2 Version 7.06 or higher

	DS7220 Version 2.10 or higher DS7240 Version 2.10 or higher DS7400XiV4 Version 4.10 or higher Easy Series V3+ FPD-7024 AMAX 2100/3000/4000 * Solution 2000/3000* *The B426-M is recommended for AMAX and Solution Series control panels.
Control panels - B426-M	AMAX 2100/3000/4000 v2.00+ Solution 2000/3000
Applications	A-Link Plus RPS/RPS Lite PC9000 (Supported on D9412GV2/D7412GV2/D7212GV2 v7.06 and higher, and D9412GV3/D7412GV3/D7212GV3 v8.05 and v8.13 and higher only) IS2000 (Supported on D9412GV2/D7412GV2/D7212GV2 v7.06 and higher, and D9412GV3/D7412GV3/D7212GV3 v8.05 and v8.13 and higher only) Remote Security Control (Supported on GV4, B9512G/B8512G, B9512G-E/B8512G-E, B6512/B5512/B4512/B3512, B5512E/B4512E/B3512E, and Solution 2000/3000) Remote Security Control+ (Supported on AMAX and Solution Series control panel)
Browsers	Microsoft Internet Explorer (Microsoft Windows 7 and higher) Mozilla Firefox

1.2 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

Manufacturing dates

For product manufacturing dates, go to http://www.boschsecurity.com/datecodes/ and refer to the serial number located on the product label.

2 Firmware version 3.15.014

What’s new

- *Security improvements, page 7*

What’s fixed

- *RPS fails to connect, page 7*
- *HTTPS Port Number configuration, page 7*
- *Expired TLS Certificate, page 7*

2.1 What's new

This section examines the new features of this firmware version.

2.1.1 Security improvements

- Configuration of minimum supported TLS version 1.2.
- Disable non-FIPS compliant TLS ciphers.
- Updated TLS and network stack libraries.
- Implemented lockout scheme for consecutive, invalid web page passcode entries. If 5 consecutive invalid passcode entries are made within a 10-minute period, subsequent passcode entries, whether valid or invalid, will be ignored until 10 minutes have elapsed since the first of the 5 invalid entries were made.

2.2 What's fixed

This section examines the corrections made in this firmware version.

2.2.1 RPS fails to connect

RPS fails to connect to B and G Series control panels using a B426 after control panel and B426 firmware updates have been installed.

2.2.2 HTTPS Port Number configuration

HTTP port number configuration change did not take affect.

2.2.3 Expired TLS Certificate

This device might allow an expired TLS certificate. This has been corrected.

3 Firmware version 3.11

What’s new?

– *Support for updated B426 certificates, page 8*

3.1 What's new

This firmware version addresses internal software performance improvements and enhancements.

3.1.1 Support for updated B426 certificates

B426 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. RPS v6.11 has been updated to accommodate this new B426 security certificate automatically.

IMPORTANT:

Customers upgrading or installing 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 B426 modules firmware v3.10 or older will not be affected by the certificate expiration and operations will continue without interruption.

4 Firmware version 3.10

What’s fixed

This firmware version addresses internal software performance improvements and enhancements.

5 Firmware version 3.09

What’s new

– California Security of Connected Devices Act

5.1 What's new

This section examines the new features of this firmware version.

5.1.1 California Security of Connected Devices Act

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

6 Firmware version 3.08

What's fixed

- *Updates to the bootloader, page 11*
- *Updates to TCP keep alive, page 11*
- *Updates to the web server, page 11*

6.1 What's fixed

6.1.1 Updates to the bootloader

This firmware release contains updates to improve the performance of the bootloader.

6.1.2 Updates to TCP keep alive

This firmware release contains performance improvements related to maintaining connections to the cloud.

6.1.3 Updates to the web server

This firmware release contains updates to improve the security/access of the webserver during login. Improvements allow for one user to have access during the login process of the webserver.

7 Firmware version 3.06

What's new

- Incoming RPS connections
- *Secure connections using TLS v1.1 and v1.2 now supported, page 12*

7.1 What's new

This section examines the new features of this firmware version.

7.1.1 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.

Notice!
Only applicable when connected to a Bosch B Series, or G Series control panel with firmware version 3.07 or higher.

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

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

8 Firmware version 3.05

What’s new

- *Remote Connect Service support, page 13*

Known issues

- *Network Module Trouble with 2 modules, page 13*
- *IP address error on keypads, page 13*

8.1 What's new

This section examines the new features of this firmware version.

8.1.1 Remote Connect Service support

Remote Connect Service enables a secure control panel connection to mobile apps and remote programming software using Bosch Cloud services. The service allows a secure TLS connection to a control panel without specific port and router settings and without a static IP or DNS.

Notice!
North America only
Remote Connect Services and Bosch Cloud services are currently available in North America only.

8.2 Known issues

This section examines the known issues of this firmware version.

8.2.1 Network Module Trouble with 2 modules

A Network Module Trouble might occur on a B9512G/B8512G system with two B426 modules when changing the Route Group information for the module through which RPS is connected. If the Trouble does not clear within a short period of time, reconnect with RPS. If reconnecting to the system with RPS does not clear the problem, restart the system. You can restart the system when connected to it using RPS by clicking the Reset checkbox.

8.2.2 IP address error on keypads

The B9512G/B8512G and B6512/B5512/B4512/B3512 control panels might show an incorrect error.
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.

9 Firmware version 3.04.001

What’s new

- *Configuration using option bus control panels , page 14*
- *SIA DC09 event reporting support for AMAX control panels, page 14*

Corrections

- *Configuration pages , page 14*

Known issues

- *Network Module Trouble with 2 modules, page 13*
- *IP address error on keypads, page 13*

9.1 What's new

This section examines the new features of this firmware version.

9.1.1 Configuration using option bus control panels

The module now supports configuration programming using an option bus connection with the control panel.

9.1.2 SIA DC09 event reporting support for AMAX control panels

AMAX control panels now support SIA DC09 event reporting.

9.2 Corrections

This section examines the corrections made in this firmware version.

9.2.1 Configuration pages

Minor bugs found in the configuration web pages have been fixed.

9.3 Known issues

This section examines the known issues of this firmware version.

9.3.1 Network Module Trouble with 2 modules

A Network Module Trouble might occur on a B9512G/B8512G system with two B426 modules when changing the Route Group information for the module through which RPS is connected. If the Trouble does not clear within a short period of time, reconnect with RPS. If reconnecting to the system with RPS does not clear the problem, restart the system. You can restart the system when connected to it using RPS by clicking the Reset checkbox.

9.3.2 IP address error on keypads

The B9512G/B8512G and B6512/B5512/B4512/B3512 control panels might show an incorrect error.
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.

10 Revision history

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

10.1 Version 3.03.009 firmware

Notable features

- *Security protocol support, page 15*
- *TCP connection timeouts, page 15*

10.1.1 Security protocol support

For increased security, the B426 no longer supports SSL3.0 and cipher suites with known vulnerabilities.

The B426 continues to support TLS1.0 with the following cipher suites:

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA

10.1.2 TCP connection timeouts

For increased security, the B426 now includes a 10 second timeout. The B426 closes a TCP connection if the module does not receive a message within 10 seconds of establishing a connection.

10.2 Version 3.03.007 firmware

Notable features

- *High traffic network enhancements, page 15*

10.2.1 High traffic network enhancements

This firmware version enhances the performance of the module on Ethernet networks with high volumes of broadcast and multicast traffic.

10.3 Version 3.03 firmware

Notable features

- *Solution 2000/3000 control panel support, page 15*
- *Email notifications, page 15*
- *Increased IPv6 compatibility, page 16*
- *Event reporting using CSV-IP protocol, page 16*

10.3.1 Solution 2000/3000 control panel support

The module now supports the Solution 2000/3000 control panels. The control panels replace the Solution Series control panels.

10.3.2 Email notifications

The module now supports personal notifications using email on control panels that support email; control panels B9512G/B8512G, B6512/B5512/B4512/B3512 v2.03 and higher, and Solution 2000/3000.

To enable the email notification option in the module, use remote programming software. Web-based configuration does not support programming of email server options with this version of firmware.

10.3.3 Increased IPv6 compatibility

This version includes modifications to the module that make it more compatible with IPv6.

10.3.4 Event reporting using CSV-IP protocol

The module now supports event reporting using CSV-IP protocol on the ICP-SOL2-P/ICP-SOL3-P (Solution 2000/3000) control panel.

10.4 Version 3.02 firmware

The module hardware includes additional memory to support the new v3.02 firmware features.

Notice!
Firmware v3.02 and higher require the new module hardware to operate. Modules with v3.01 firmware cannot update to newer (higher) firmware version. Refer to *Requirements, page 5*.

10.5 Version 3.01 firmware

This initial release of the B426 Conettix Ethernet Communication Module includes enhancements over its predecessor, the B420. Most notably, the B426 supports IPv6.

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

Building solutions for a better life

202409261436