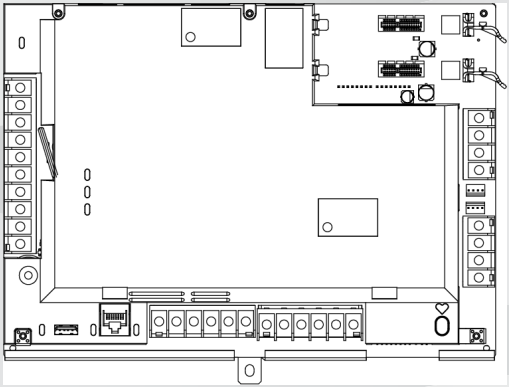
# Control panels

G Series: B9512G, B8512G



**nl** Opmerkingen bij de huidige versie

# Inhoudsopgave

# 1 Inleiding

Deze *Versie-opmerkingen* hebben betrekking op de firmwareversie 3.09.050 van inbraakcentrales.

## 1.1 Over de documentatie

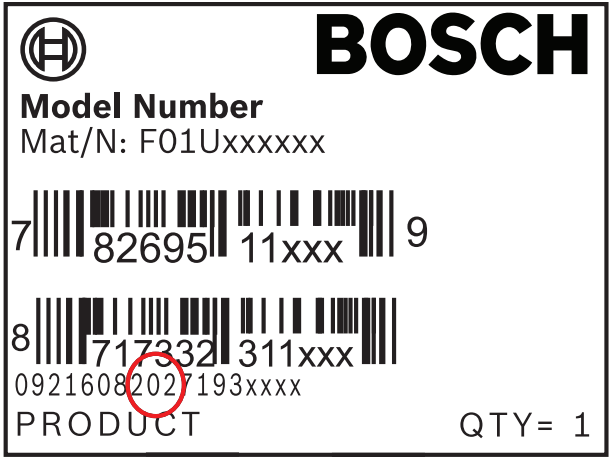


**Handelsmerken**

Alle productnamen van hardware en software in dit document zijn waarschijnlijk gedeponeerde handelsmerken en dienen als zodanig te worden behandeld.

**Bosch Building Technologies, Inc. productiedatums**

Gebruik het serienummer dat zich bevindt op het productlabel en zie de website van Bosch Security Systems, Inc. op http://www.boschsecurity.com/datumcodes/.
Op de volgende afbeelding ziet u een voorbeeld van een productlabel, met een markering op de plaats waar u de productiedatum in het serienummer kunt vinden.




## 1.2 Vereisten

In deze sectie vindt u de vereisten waaraan RPS (Remote Programming Software, software voor programmeren op afstand) en Conettix Ontvanger/Gateway moeten voldoen om deze firmwareversie voor inbraakcentrales te ondersteunen.

### 1.2.1 Software voor programmeren op afstand (RPS)

Om alle nieuwe functies van deze firmwareversie te kunnen gebruiken, moet RPS versie 6.09 of hoger worden gebruikt.

### 1.2.2 Conettix Ontvanger/Gateway

#### Conettix Modem4-indeling

Als de inbraakcentrale zodanig wordt geconfigureerd dat deze rapporten verzendt in de Conettix Modem4-indeling, kan een update nodig zijn voor de programmeersoftware van de Conettix ontvanger/gateway van de meldkamer en de D6200CD ontvanger.

#### Vereisten voor indeling van Conettix Modem4-rapportage

| Ontvanger/gateway | CPU-versie | D6200CD-versie |
|---|---|---|
| D6600 Ontvanger meldkamer, 32 lijnen (alleen met D6641 Telefoonlijnkaart geïnstalleerd) | 01.10.00 | 2.10 |
| D6100IPV6-LT Ontvanger meldkamer, 2 lijnen, IP | 01.10.00 | 2.10 |

#### Conettix ANSI-SIA Contact-ID-indeling

Als u de inbraakcentrale zodanig configureert dat deze rapporten verzendt in de Conettix ANSI-SIA Contact-ID-indeling, kan een update nodig zijn voor de programmeersoftware van de Conettix ontvanger/gateway van de meldkamer en de D6200CD ontvanger.

**Met ULC-S304 en ULC-S559 compatibele rapportindeling**

**Bericht!**

Met ULC-S304 en ULC-S559 compatibele rapportindeling

Voor rapportindelingen die compatibel zijn met ULC-S304 en ULC-S559 moeten de programmeersoftware van de Conettix ontvanger/gateway van de meldkamer en de D6200CD ontvanger de versie in de tabel gebruiken.

**ANSI-SIA DC-09-indeling**

Voor het gebruik van de ANSI-SIA DC-09-indeling is een ontvanger van de meldkamer vereist die deze IP-communicatiemodule-indeling ondersteunt. Bosch Conettix ontvangers van de meldkamer ondersteunen deze indeling momenteel niet.

# 2 Firmwareversie 3.09.050

**Nieuw in deze versie**



**Correcties**



**Bekende problemen**



## 2.1 Nieuw in deze versie

In deze sectie worden de nieuwe functies van deze firmwareversie nader beschreven.

### 2.1.1 Ondersteuning van B444-A en B444-V

Het systeem ondersteunt nu de B444-A Mobiele insteekmodule, AT&T LTE en de B444-V Mobiele insteekmodule, Verizon LTE.

**B444-A/B444-V SIM-kaartactivering**

**Voorzichtig!**

Activeer de B444-A/B444-V SIM-kaart voordat u deze plaatst. Als u dit niet doet, kunnen communicatiestoringen optreden met de inbraakcentrale/module. Nadat de B444-A/B444-V voor het eerst is opgestart, kan het tot 15 minuten duren voordat het activeringsproces is voltooid.

### 2.1.2 ANSI-SIA DC-09-indeling

Het systeem ondersteunt nu de volgende netwerkcommunicatie-indelingen:

- Conettix Modem4
- Conettix ANSI-SIA Contact-ID
- ANSI-SIA DC-09

**Bericht!**

UL- en ULC-gecertificeerde toepassingen

De indeling ANSI-SIA DC-09 is niet beschikbaar voor UL- en ULC-gecertificeerde toepassingen.

### 2.1.3 Security of Connected Devices Act (Wet inzake beveiliging van verbonden apparaten) van Californië

Om te voldoen aan de Wet inzake beveiliging van verbonden apparaten (TITEL 1.81.26. Security of Connected Devices) maakt dit product gebruik van een uniek verbindingswachtwoord.
De 'RPS-toegangscode' voor de aanvankelijke verbinding met dit product moet overeenkomen met de unieke cloud-ID van het product.

Zorg dat uw RPS-operator de unieke cloud-ID gebruikt die op het product is gelabeld en is vermeld op de kaart in de doos van het product.

## 2.2 Correcties

In deze sectie worden de correcties in deze firmwareversie nader beschreven.

### 2.2.1 Bewerking Uitgangresponstype

In de firmwareversie 3.09.024 van de inbraakcentrale werkten de configuratieselecties 1 en 2 van de bewerking Uitgangresponstype niet naar behoren.
Dit is gecorrigeerd in de firmwareversie 3.09.050 van de inbraakcentrale.
Als u wijzigingen hebt aangebracht in de firmwareversie 3.09.024 van de inbraakcentrale om een juiste werking te verzekeren, zijn die wijzigingen niet meer nodig.

- Zet de configuratieselecties 1 en 2 in de bewerking Uitgangresponstype terug op de verwachte, en gedocumenteerde, configuratie.

## 2.3 Bekende problemen

In deze sectie worden de bekende problemen van deze firmwareversie nader beschreven.

### 2.3.1 E-mail met persoonlijke alarmmelding

Bij het gebruik van e-mails met persoonlijke alarmmeldingen is het mogelijk dat sommige opties voor de serverconfiguratie (bijv. verificatie in twee stappen van Gmail, Minder veilige apps toestaan: Uit) kan mogelijks niet juist werken.
Schakel extra opties voor de e-mailserver uit om een juiste werking te verzekeren.

# 3 Geschiedenis van firmware-revisies

In dit gedeelte worden de noemenswaardige functies van vorige revisies van deze firmware nader beschreven.

## 3.1 Firmwareversie 3.08

### 3.1.1 Taalondersteuning

In deze versie wordt ondersteuning toegevoegd voor Nederlands, Duits en Zweeds.

Wanneer zowel de eerste taal als de tweede taal van de inbraakcentrale zijn ingesteld op Duits, Engels, Frans, Hongaars, Italiaans, Nederlands, Portugees, Spaans of Zweeds, gebruikt het systeem de tekenset Standaard, Latin-1.
Wanneer ofwel de eerste taal ofwel de tweede taal van de inbraakcentrale is ingesteld op Chinees, Grieks of Pools, gebruikt het systeem de Uitgebreide Unicode-tekenset UTF-8.

**Bericht!**

**Alleen bedieningspanelen B915/B915i en B942 ondersteunen Uitgebreid, UTF-8**

Alleen B915/B915i-bedieningspanelen met firmwareversie 1.01.010 of hoger, en B942-bedieningspanelen met firmwareversie 1.02.022 of hoger ondersteunen de tekenset Uitgebreid, UTF-8

### 3.1.2 Shunttijd van deur

De langst mogelijke selectie voor de shunttijd van de deur is verlengd van 240 seconden naar 8 uur.
Deze selectie is beschikbaar in de volgende firmwareversies:
– Inbraakcentralefirmware v3.08 of hoger
– Remote Programming Software firmware v6.08 of hoger
– B901 firmwareversie v1.05 of hoger.

### 3.1.3 Apparaten voor back-upbestemming

De inbraakcentrale kan rapporten verzenden naar vier verschillende routegroepen, met één primaire en maximaal drie back-upbestemmingsapparaten voor elke routegroep.

### 3.1.4 Aangepast testrapport

Een normaal testrapport of een aangepast testrapport kan worden verzonden:
– Normaal testrapport: omvat alle routegroepen waarbij de functie voor testrapporten is ingeschakeld, onafhankelijk van het gebruikte bestemmingsapparaat voor de communicatie. Het testrapport wordt verzonden naar het eerste geslaagde bestemmingsapparaat in een routegroep.
– Aangepast testrapport: u kunt de te routegroep en het te testen doelapparaat selecteren. U kunt één bestemmingsapparaat per routegroep of alle geconfigureerde bestemmingsapparaten voor een routegroep testen.

### 3.1.5 Onjuist uitganggedrag

In de inbraakcentralefirmware v3.08.002 wordt output 3(C) elke keer geactiveerd dat een ingebouwde zone wordt verstoord, ongeacht de programmering van de centrale. Dit is opgelost in de inbraakcentralefirmware v3.08.004.

## 3.2 Firmwareversie 3.07

**Noemenswaardige functies**

- *Binnenkomende RPS-verbindingen, pagina 14*
- *Indicatie van signaalsterkte van B444, pagina 14*
- *Stabilisatie van prestaties van mobiele kaart, pagina 14*
- *APN-gebruik voor B442 en B443, pagina 15*

### 3.2.1 Binnenkomende RPS-verbindingen

Naast de beantwoording van binnenkomende oproepen van RPS met gebruikmaking van UDP (User Datagram Protocol), worden ook binnenkomende oproepen van RPS met gebruikmaking van TCP (Transfer Control Protocol) ondersteund. RPS versie 6.07 is vereist voor deze gewijzigde verbindingsmethode.

### 3.2.2 Indicatie van signaalsterkte van B444

De LED-indicatie van de signaalsterkte van de B444 is gewijzigd om een nauwkeuriger beeld te geven van de prestaties. Hoewel LTE-mastoverschakeling nog steeds mogelijk is, zijn de afzonderlijke indicaties voor signaalsterkte nauwkeuriger.

### 3.2.3 Stabilisatie van prestaties van mobiele kaart

Verbeteringen op het gebied van de stabiliteit van de mobiele kaart zijn opgenomen in deze firmware-release.

### 3.2.4 APN-gebruik voor B442 en B443

De mobiele B442- en B443-insteekmodules proberen in de volgende volgorde verbindingen tot stand te brengen met gebruikmaking van APN's:

1. Primair geconfigureerde APN
2. gne
3. wyless.apn
4. wyless.com.attz

De mobiele insteekmodule selecteert en gebruikt de meest geschikte APN.

Als de APN onjuist is, worden de details van deze probleemtoestand mogelijk niet weergegeven op de bedieningspanelen.

## 3.3 Firmwareversie 3.06

**Noemenswaardige functies**


– *Taalondersteuning, pagina 15*
– *Programmering van bedieningspaneel, pagina 16*
– *PSTN, pagina 16*
– *Circuitstijl van zoneprofiel, pagina 17*
– *Respons op systeemsabotage, pagina 17*
– *PIN-code [Esc], pagina 17*
– *Nieuwe standaardwaarde voor parameter Naam van netwerktoegangspunt (APN), pagina 17*


### 3.3.1 Taalondersteuning

In deze versie wordt ondersteuning toegevoegd voor Chinees, Grieks, Hongaars, Italiaans en Pools.

Wanneer zowel de eerste taal als de tweede taal van de inbraakcentrale zijn ingesteld op Engels, Frans, Hongaars, Italiaans, Portugees of Spaans, gebruikt het systeem de tekenset Standaard, Latin-1. Wanneer ofwel de eerste taal ofwel de tweede taal van de inbraakcentrale is ingesteld op Chinees, Grieks of Pools, gebruikt het systeem de Uitgebreide Unicode-tekenset UTF-8.

**Bericht!**

**Alleen bedieningspanelen B915/B915i en B942 ondersteunen Uitgebreid, UTF-8**

Alleen B915/B915i-bedieningspanelen met firmwareversie 1.01.010 of hoger, en B942-bedieningspanelen met firmwareversie 1.02.022 of hoger ondersteunen de tekenset Uitgebreid, UTF-8

### 3.3.2 Programmering van bedieningspaneel

Aan het installateursmenu zijn opties voor programmering via het bedieningspaneel toegevoegd, zoals het menu *Apparaat* en het menu *Diverse*. Gedetailleerde informatie over de menustructuur vindt u in de bijgewerkte Installatiehandleiding.

### 3.3.3 PSTN

Parameter voor PSTN-compatibiliteit is uitgebreid voor de ondersteuning van extra landen.

### 3.3.4 Circuitstijl van zoneprofiel

De opties van Circuitstijl van zoneprofiel zijn uitgebreid met de selecties 'Tweevoudige 1K EOL met sabotage', 'Enkelvoudige 1K EOL met sabotage' en 'Enkelvoudige 2K EOL met sabotage'. Door een van deze stijlen te kiezen, kunt u de nieuwe rapporten *Zonesabotage-alarm* en *Herstel zonesabotage-alarm* verzenden.

### 3.3.5 Respons op systeemsabotage

De parameter *Respons op systeemsabotage* voor het configureren van systeemgedrag en -rapportage tijdens Inschakeling is toegevoegd.

### 3.3.6 PIN-code [Esc]

De bedieningspaneeloptie *PIN-code [Esc]* is nu van toepassing op zowel SDI- als SDI2-bedieningspanelen.

### 3.3.7 Nieuwe standaardwaarde voor parameter Naam van netwerktoegangspunt (APN)

In firmwareversie 3.06 en RPS-versie 6.05 is de standaard netwerk-APN-parameter gewijzigd in *eaaa.bosch.vzwentp*. De vorige standaardwaarde - *wyless.apn* - is nog steeds geldig. De APN hoeft niet te worden gewijzigd voor bestaande accounts.

## 3.4 Firmwareversie 3.05

**Noemenswaardige functies**

- *Ondersteuning van mobiele B444 4G VZW LTE, pagina 18*
- *Ondersteuning van gelijktijdige Modus 2-verbindingen, pagina 18*
- *37-bits referenties met ondersteuning van locatiecode, pagina 19*

- *Veilige verbindingen met gebruikmaking van TLS versie 1.1 en versie 1.2 worden nu ondersteund, pagina 19*
- *Update van schema voor zomertijd Brazilië, pagina 19*

**Correcties**

- *Indicatie 'Ready to turn on' (Klaar voor Inschakeling), pagina 20*
- *Overbruggen ongedaan maken met aangepaste functie, pagina 20*
- *Geforceerde Inschakeling met verstoorde, niet-overbrugbare zones , pagina 20*
- *Gedeelde gebiedsrapporten, pagina 21*
- *Looptest Brand voor meerdere vergrendelende rookcondities op één circuit, pagina 21*
- *Overbrugde zones onjuist geëvalueerd, pagina 21*
- *Persoonlijke meldingen voor openen/sluiten, pagina 22*
- *Modus 2-automatisering en verstoorde zones, pagina 22*
- *Weergave op bedieningspaneel van uitgeschakelde bewakingszone van Aux-voeding, pagina 22*

### 3.4.1 Ondersteuning van mobiele B444 4G VZW LTE

Deze firmware-update ondersteunt de B444 Conettix 4G VZW LTE mobiele insteekcommunicatiemodule. Deze module is alleen bestemd voor de Amerikaanse markt.
Opmerking: wanneer de B444 of B444-C voor het eerst wordt opgestart, kan het tot 15 minuten duren voordat de activering voltooid is. Dit gebeurt alleen bij de eerste inschakeling van de B444 en B444-C.

### 3.4.2 Ondersteuning van gelijktijdige Modus 2-verbindingen

De inbraakcentrale ondersteunt nu maximaal drie gelijktijdige Modus 2-automatiseringsverbindingen. In eerdere firmwareversies ondersteunde de inbraakcentrale één Modus 2-automatiseringsverbinding tegelijk.

### 3.4.3 37-bits referenties met ondersteuning van locatiecode

**Alleen voor B6512-inbraakcentrales**

Naast 26-bits en 37-bits (geen locatiecode) HID-referenties, ondersteunt de inbraakcentrale nu 37-bits HID-referenties met locatiecodes. De inbraakcentrale ondersteunt nu de volgende referenties:

– 37-bits HID H10304 (met locatiecode)
– 37-bits HID H10302 (geen locatiecode)
– 26-bits HID H10301
– EM EM4200 (3-bytes of 5-bytes)

### 3.4.4 Veilige verbindingen met gebruikmaking van TLS versie 1.1 en versie 1.2 worden nu ondersteund

De firmware ondersteunt nu veilige verbindingen, met inbegrip van e-mailservers voor persoonlijke alarmmeldingen, met gebruikmaking van TLS versie 1.0 (alleen sterke vercijfering), versie 1.1 en versie 1.2. In eerdere versies van de firmware was ondersteuning van TLS versie 1.0 vereist voor TLS-verbindingen.

### 3.4.5 Update van schema voor zomertijd Brazilië

Bij centrales die zijn geconfigureerd voor 'Brazil DST' (Zomertijd Brazilië) begint het nieuwe zomertijdschema nu op de eerste zondag van november en wordt het schema van kracht vanaf het begin van 2018. De centrales ondersteunen tevens agendaverschillen voor carnaval.

### 3.4.6 Indicatie 'Ready to turn on' (Klaar voor Inschakeling)

Bij eerdere versies van de firmware werd voor systemen met een B810 RADION of B820 draadloze ontvanger op bedieningspanelen mogelijk de indicatie Klaar voor Inschakeling niet juist weergegeven. Zo kon bijvoorbeeld 'Klaar voor Inschakeling' worden weergegeven, terwijl er verstoorde zones waren.
Dit is opgelost in deze firmwareversie.

### 3.4.7 Overbruggen ongedaan maken met aangepaste functie

In eerdere firmwareversies werd bij het ongedaan maken van overbruggingen met een aangepaste functie, het overbruggen van verstoorde, gecontroleerde zones niet op de juiste wijze ongedaan gemaakt. Dit is opgelost in deze firmwareversie. Het overbruggen van verstoorde zones in Uitgeschakelde gebieden wordt nu op de juiste wijze ongedaan gemaakt bij gebruik van de aangepaste functie. De overbrugging van verstoorde 24-uurs zones kan niet ongedaan worden gemaakt.

### 3.4.8 Geforceerde Inschakeling met verstoorde, niet-overbrugbare zones

In eerdere versies van de firmware stond de inbraakcentrale u wellicht toe het systeem geforceerd In te schakelen wanneer tijdens de controle van geforceerd Inschakelen niet-overbrugbare zones verstoord waren. Dit is opgelost in deze firmwareversie. De inbraakcentrale staat geforceerd Inschakelen door niet-overbrugbare zones te overbruggen niet toe.

### 3.4.9 Gedeelde gebiedsrapporten

In eerdere versies van de firmware werd, wanneer een gebruiker een gekoppeld gebied in- of uitschakelde, waardoor het gedeelde gebied werd In- of Uitgeschakeld, alleen de status van het gekoppelde gebied naar de ontvanger van de meldkamer gestuurd en opgeslagen in het gebeurtenissenlogboek.
Met ingang van deze firmwareversie wordt naast de status van het gekoppelde gebied ook de status van het gedeelde gebied verzonden en geregistreerd door de inbraakcentrale.

### 3.4.10 Looptest Brand voor meerdere vergrendelende rookcondities op één circuit

In eerdere versies van deze firmware werd bij het uitvoeren van een brandlooptest de rookmelder pas gereset nadat de brandlooptest was beëindigd. Als er dus meerdere rookmelders waren aangesloten op een circuit, was het niet mogelijk alle rookmelders in de lus te testen zonder eerst de brandlooptest te beëindigen en opnieuw te starten.
Dit is opgelost in deze firmwareversie.

### 3.4.11 Overbrugde zones onjuist geëvalueerd

Bij eerdere versies van de firmware gaf het bedieningspaneel extra zones voor geforceerd Inschakelen weer wanneer de inbraakcentrale geforceerd werd Ingeschakeld. Als bijvoorbeeld de lobby geforceerd werd Ingeschakeld, zou het bedieningspaneel vragen of overbrugde zones op een bovenverdieping ook geforceerd moesten worden Ingeschakeld.
Dit is opgelost in deze firmwareversie.

### 3.4.12 Persoonlijke meldingen voor openen/sluiten

Bij eerdere firmwareversies stuurden inbraakcentrales waarop autorisatieniveaus die het verzenden van openings-/sluitingsgebeurtenissen beperken, waren geconfigureerd in combinatie met het verzenden van persoonlijke meldingen voor openings-/sluitingsgebeurtenissen, de openings-/sluitingsgebeurtenissen voor de beperkte gebruiker ten onrechte via persoonlijke meldingen. Het probleem deed zich niet voor bij gebeurtenissen die naar de ontvanger van de meldkamer werden gestuurd.
Dit is opgelost in deze firmwareversie.

### 3.4.13 Modus 2-automatisering en verstoorde zones

Bij versie 3.03 van de firmware stond de inbraakcentrale Modus 2-automatiseringsclients toe In te schakelen terwijl er verstoorde zones waren. Dit is gecorrigeerd in versie 3.05.

### 3.4.14 Weergave op bedieningspaneel van uitgeschakelde bewakingszone van Aux-voeding

Bij eerdere firmwareversies werd, wanneer een gebruiker een verstoorde zone die een bewakingszone-index van de Aux-voeding gebruikte, Uitschakelde en vervolgens het systeem werd gereset zonder terug te keren naar normaal, de verstoorde zone niet weergegeven op het scherm van het bedieningspaneel.
Dit probleem is opgelost in deze firmwareversie.

## 3.5 Firmwareversie 3.03.014

### Noemenswaardige functies

– *ULC-S559-goedkeuring, pagina 23*

### 3.5.1 ULC-S559-goedkeuring

De inbraakcentrale heeft nu de goedkeuring ULC-S559 Centrales en systemen voor ontvangst van brandalarm voor Canada verworven. Raadpleeg de *ULC-installatiehandleiding* voor goedgekeurde modules, behuizingen en installatie-instructies.
De inbraakcentrale kan worden geconfigureerd om te voldoen aan de vereisten van een ULC-S559- of een ULC-S304-systeem.
De inbraakcentrale kan worden geconfigureerd om te voldoen aan de vereisten van een gecombineerd ULC-S559- en ULC-S304-systeem.

### 3.5.2 Conformiteit met ULC Canada beïnvloedt bericht op bedieningspaneel tijdens firmware-updates

Wanneer de parameter Conformiteit met ULC Canada in RPS wordt ingesteld op Ja, wordt de werking van de inbraakcentrale aangepast aan de conformiteit met UL Canada. Als gevolg hiervan wordt, met ingang van deze versie, het service-oproepbericht in de instellingen van het bedieningspaneel weergegeven na 90 seconden na het verbreken van de verbinding in plaats van na 180 seconden. Dit zou ertoe kunnen leiden dat op een bedieningspaneel tijdens een firmware-update het

service-oproepbericht wordt weergegeven, zelfs als een oproep niet nodig is. Op het bedieningspaneel wordt tekst voor inactieve werking weergegeven wanneer de firmware-update is voltooid

### 3.5.3 Ondersteuning van Remote Connect-service

De Remote Connect-service maakt een veilige verbinding van de inbraakcentrale met mobiele apps en software voor programmering op afstand met gebruikmaking van Bosch Cloud-services mogelijk. Met de service kan een veilige TLS-verbinding met een inbraakcentrale worden gebruikt zonder specifieke poort- en routerinstellingen en zonder een statisch IP of DNS.

**Bericht!**

**Alleen Noord-Amerika**

Remote Connect-services en Bosch Cloud-services zijn momenteel alleen beschikbaar in Noord-Amerika.

### 3.5.4 Datum/tijd-notatie

De instellingen van het bedieningspaneel bieden gebruikers nu de optie om een notatie te kiezen voor zowel de datum als de tijd. Voor de datum kunnen gebruikers kiezen uit de notaties MM/DD/JJ, DD/MM/JJ en JJ/MM/DD. Voor de tijd kunnen gebruikers kiezen uit de 12-uurs AM/PM-notatie en de 24-uurs notatie.

### 3.5.5 End-of-line-opties voor ingangszone

De inbraakcentrale ondersteunt nu 1 kΩ, tweevoudige EOL (1 kΩ + 1 kΩ) en 2 kΩ end-of-line (EOL)-weerstanden naast de optie Geen EOL voor on-board- en B208-ingangszones. Voorafgaand aan deze versie ondersteunde de inbraakcentrale 1 kΩ EOL en tweevoudige EOL (1 kΩ + 1 kΩ).

### 3.5.6 Verbinding inbraakcentrale verbreken niet meer vereist

De inbraakcentrale reageert nu op RPS-programmeringswijzigingen zonder dat de verbinding hoeft te worden verbroken. U hoeft enkel de wijzigingen te verzenden in RPS. De inbraakcentrale past de nieuwe configuratie onmiddellijk toe.

### 3.5.7 Controlemodus na opstarten

Als de inbraakcentrale is ingesteld op Controlemodus, blijft de Controlemodus-conditie (Aan of Uit) nu bestaan na een aan/uit-cyclus (accu- en netstroomvoeding uitgeschakeld en vervolgens weer ingeschakeld).

### 3.5.8 Geluidsopties voor communicatieproblemen

RPS kent nu een parameter voor het instellen van communicatieproblemen op zichtbaar (weergegeven op het bedieningspaneel en overeenkomstig de probleemtooninstellingen van het bedieningspaneel) of onzichtbaar (geen indicatie weergegeven op het bedieningspaneel). Dit is alleen van invloed op communicatieproblemen en niet op fouten met routegroepen.

### 3.5.9 Bijgewerkte ondersteuning voor B440/B441

Firmwareversies 3.02 en 3.03 van inbraakcentrales ondersteunen de nieuwste versies van de B440 en B441 mobiele insteekmodules (B440 versie 15.00.026 en B441 versie 18.02.022). De nieuwste firmware van de B440/B441 omvat bijgewerkte bibliotheken voor het behoud van de Verizon-certificering.

Met de firmwareversie 3.03 van de inbraakcentrale, in combinatie met de nieuwste firmware van de B440/B441, wordt de MEID juist weergegeven op het bedieningspaneel via het installateursmenu. Bij de firmwareversie 3.02 van de inbraakcentrale werd de MEID afgekapt. Dit betekende dat de MEID van het etiket moest worden overgenomen in plaats van deze te lezen via het bedieningspaneel. De normale werking werd hierdoor echter verder niet beïnvloed.

# 4 Een ouder account in RPS voor 3.08 bijwerken

De B9512G is een directe vervanging voor de vorige inbraakcentralemodellen D9412GV4, D9412GV3, D9412GV2 en D9412G.
De B8512G is een directe vervanging voor de vorige inbraakcentralemodellen D7412GV4, D7412GV3, D7412GV2 en D7412G.
Als u een bestaande inbraakcentrale uit de G-serie vervangt door een B9512G/B8512G, kunt u het bestaande RPS-account bijwerken naar een B9512G/B8512G-account, zodat u het account niet opnieuw hoeft te maken.

**Bericht!**
Lees, voordat u een bestaand account bijwerkt naar een B9512G/B8512G-account in RPS, de update-informatie voor de inbraakcentrale in de *Versie-opmerkingen bij RPS*.

## 4.1 Een bestaand account van een inbraakcentrale uit de G-serie bijwerken naar een B9512G/B8512G-account

Bijwerken naar een B9512G/B8512G-account:
1. Markeer het account van de inbraakcentrale in het venster met de centralelijst, klik vervolgens met de rechtermuisknop op het account en selecteer Weergeven. Het venster Centralegegevens - Weergave wordt geopend.

2. Klik op Bewerken. Ga naar de selectie Centraletype aan de rechterzijde van het venster Gegevensweergave.
3. Selecteer in de vervolgkeuzelijst Centraletype het gewenste type centrale en klik op OK. Wanneer u een inbraakcentrale bijwerkt naar een B8512G of een B9512G, maakt RPS automatisch een accountkopie.
4. Bevestig dat de nieuwe, automatisch gewijzigde configuratiewaarden overeenkomen met de vereiste waarden voor de inbraakcentrale. Breng eventueel vereiste wijzigingen aan.

Zodra de conversie is voltooid en u de wijzigingen hebt bevestigd, stuurt u het bijgewerkte programma naar de inbraakcentrale:

1. Open het nieuwe account van de inbraakcentrale dat u zojuist hebt gemaakt in de voorgaande stappen.
2. Klik op Verbinden. Het dialoogvenster Centralecommunicatie verschijnt.
3. Voer in het tekstvak RPS-toegangscode de huidige PIN-code van de centrale in en klik op Verbinden. Het dialoogvenster Centralesync wordt weergegeven.
4. Selecteer ALLE RPS-gegevens naar centrale verzenden en klik op OK. Opmerking: selecteer Centralegegevens ontvangen niet.
5. Sluit desgewenst RPS af wanneer de firmware-update is voltooid.

# 5 Open source-software 3.09.050

Bosch heeft de hieronder vermelde open source-softwaremodules opgenomen in de firmware voor deze inbraakcentrale. Het feit dat deze modules zijn opgenomen, houdt geen beperking in van de garantie van Bosch.

### 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).
Raadpleeg de OpenSSL-licentie op www.boschsecurity.com onder Productcatalogus voor meer informatie.

## Regents of the University of California


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**