

Conettix Ethernet Communicatiemodule

B426



BOSCH

nl Installatie- en bedieningshandleiding

Inhoudsopgave

1	Veiligheid	4
2	Inleiding	5
2.1	Over de documentatie	5
2.2	Bosch Security Systems, Inc. productiedata	5
2.3	Installatieschema	6
3	Systeemoverzicht	7
3.1	Overzicht	8
3.2	Busadres-instellingen	9
4	Installatie	11
4.1	Breng de module aan in de behuizing	11
4.2	De sabotageschakelaar monteren en bekabelen (optioneel)	11
4.3	De bedrading naar de inbraakcentrale	12
5	Configuratie	14
5.1	Plug-and-Play-configuratie voor SDI2 of inbraakcentrales met optiebus	14
5.2	Plug-and-Play-configuratie voor SDI of inbraakcentrales met optiebus	14
5.3	Webgebaseerde configuratie	14
5.3.1	Webgebaseerde configuratie: aanmelden en gebruiken	15
5.3.2	Pagina Device Information (home)	16
5.3.3	Instellingen wijzigen en opslaan met behulp van het web	16
5.3.4	De pagina Basic Network Settings	17
5.3.5	De pagina Advanced Network Settings	21
5.3.6	Pagina Panel Address Settings	22
5.3.7	Encryption and Security Settings page	24
5.3.8	Pagina Maintenance	25
5.3.9	Pagina Factory Default	27
5.3.10	Pagina Firmware Update	28
5.3.11	De webgebaseerde configuratiepagina's verlaten	29
6	LED's voor onderhoud en probleemoplossing	31
6.1	De firmwareversie weergeven	32
7	Specificaties	34
7.1	Technische specificaties	34
7.2	Compatibiliteit	34
8	Appendix	36
8.1	Module Hostname	36
8.2	IP-adres van module	36
8.2.1	DHCP gebruiken om het IP-adres van een met het netwerk verbonden module op te zoeken	36
8.2.2	Gebruik een SDI/SDI2-bedieningspaneel om het IP-adres van een module te achterhalen	36
8.2.3	Auto IP met een rechtstreeks aangesloten module gebruiken	37

1 Veiligheid

ESD-voorzorg



Merk op dat de B426-kaart zonder koffer/doors wordt geleverd, en dat alle onderdelen worden blootgesteld aan aanrakingen met de vingers - er dient daarom extra aandacht te worden besteed aan ESD-voorzorgsmaatregelen (elektrostatische ontlading). Zorg ervoor dat er geen statische storingen zijn wanneer u van de kaart gebruik maakt. Er dient voor geschikte ESD-bescherming te worden gezorgd en het is raadzaam om niet-elektrostatische materialen te dragen, zoals een anti-statische polsband.

ESD-schade kan variëren van prestatieverminderingen tot het compleet defect raken van het apparaat. Nauwkeurig geïntegreerde circuits kunnen schadegevoeliger zijn aangezien zeer kleine parametrische wijzigingen ervoor kunnen zorgen dat het apparaat niet meer aan zijn weergegeven specificaties voldoet.



Waarschuwing!

Het niet naleven van deze instructies kan leiden tot een storing die een alarmsituatie kan veroorzaken. Bosch Security Systems, Inc. is niet verantwoordelijk voor onjuist geïnstalleerde, geteste of onderhouden apparatuur. Volg deze instructies om letsel en schade aan de apparatuur te voorkomen.



Aanwijzing!

Informeer de beheerder en de bevoegde lokale overheid alvorens de module in een bestaand systeem te installeren.

Schakel alle voeding naar de inbraakcentrale uit alvorens de module te installeren.

Voordat u een B426 installeert, raadpleeg *Technische specificaties, Pagina 34*.

2 Inleiding

Dit gedeelte bevat basisinformatie en een controlelijst voor de installatie.

2.1 Over de documentatie

Auteursrecht

Deze handleiding is intellectueel eigendom van Bosch Security Systems, Inc. en is auteursrechtelijk beschermd. Alle rechten voorbehouden.

Handelsmerken

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

2.2 Bosch Security Systems, Inc. productiedata

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.



2.3 Installatieschema

Gebruik de onderstaande workflow om de module te installeren en configureren. Volg de stappen in de aangegeven volgorde van boven naar beneden. Vink steeds een vakje aan wanneer u de bijbehorende stap hebt uitgevoerd.



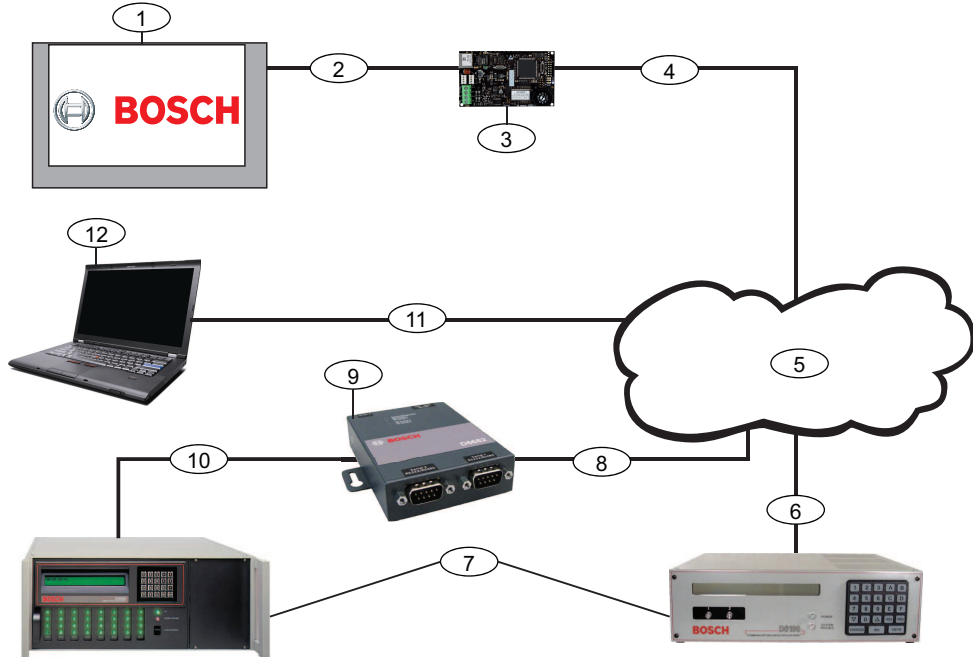
Voorzichtig!

Schakel de inbraakcentrale altijd uit tijdens het aansluiten van een module. Om de inbraakcentrale uit te schakelen, ontkoppelt u de transformator en de noodbatterij.

- Bereid de installatie voor. Zie *Systeemoverzicht, Pagina 7*.
- Stel de adresschakelaar in. Zie *Busadres-instellingen, Pagina 9*.
- Installeer de module. Zie *Breng de module aan in de behuizing, Pagina 11, De sabotageschakelaar monteren en bekabelen (optioneel), Pagina 11, en De bedrading naar de inbraakcentrale, Pagina 12*.
- Configureer de module. Zie *Plug-and-Play-configuratie voor SDI2 of inbraakcentrales met optiebus, Pagina 14, of Plug-and-Play-configuratie voor SDI of inbraakcentrales met optiebus, Pagina 14, of Webgebaseerde configuratie, Pagina 14*.
- Controleer de werking van de LED's. Zie *LED's voor onderhoud en probleemoplossing, Pagina 31*.

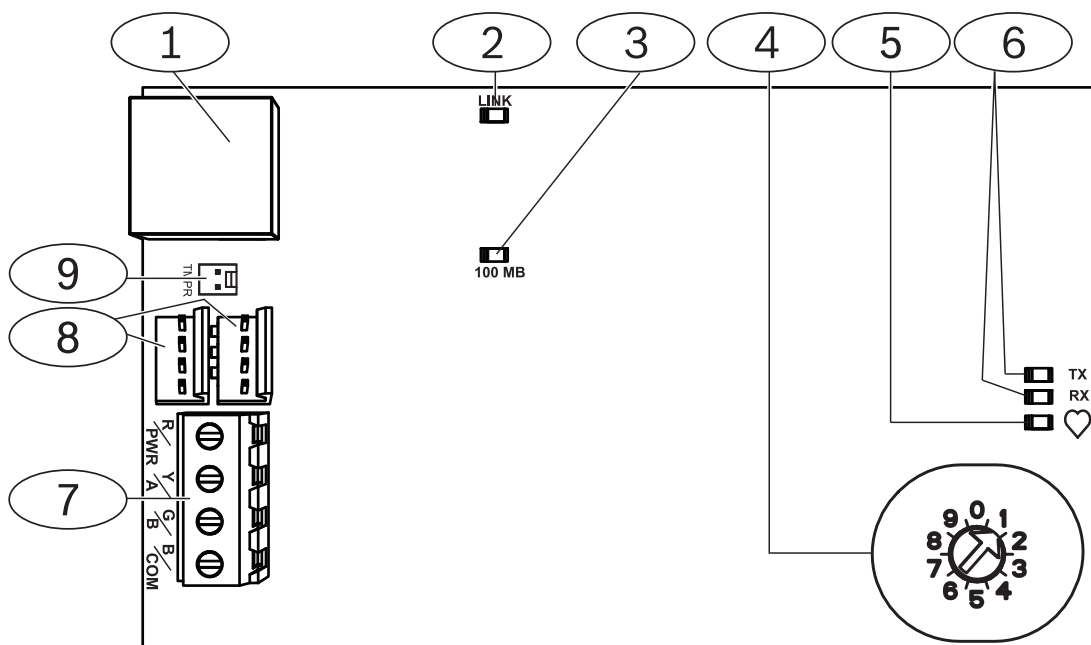
3 Systeemoverzicht

Gebruik de B426 voor bi-directionele communicatie via een Ethernet-netwerk.



Afbeelding 3.1: Overzicht B426-systeemaansluitingen

Ref. cijfer — Omschrijving	Ref. cijfer — Omschrijving
1 — Compatibele Bosch inbraakcentrale	7 — Conettix D6100i Ontvanger/Gateway en/of D6600 Conettix Ontvanger/Gateway (D6600 Conettix Ontvanger/Gateway vereist 8, 9, en 10)
2 — Databusverbinding tussen de inbraakcentrale en de module	8 — Ethernet netwerkverbinding met de Ethernet-adapter (D6680/ITS-D6682/ITS-D6686) (ITS-D6682 afgebeeld) Ethernet-netwerkadapter
3 — B426	9 — Conettix Ethernet-netwerkadapter (ITS-D6682 afgebeeld)
4 — Ethernet verbinding tussen module en Ethernet-netwerk	10 — Verbinding van ITS-D6682 met de COM4-poort op de D6600 Conettix Ontvanger/Gateway
5 — Ethernet-netwerk, Local Area Network (LAN), Metropolitan AreaNetwork (MAN), Wide Area Network (WAN), of internet	11 — Ethernet-netwerkverbinding tussen de Ethernet-netwerkinterfacekaart (NIC) van de hostcomputer en het Ethernet-netwerk
6 — Ethernet-netwerkverbinding met de D6100i-ontvanger (D6100i/D6100IPv6)	12 — Host-pc met Remote Programming Software, automatiserings- of de Conettix D6200 Programmeer-/systeembeheerssoftware

Moduleoverzicht B426**Afbeelding 3.2: B426 Conettix Ethernet Communicatiemodule**

Ref. cijfer	Omschrijving
1	Ethernet RJ-45-poort
2	Gele LINK LED
3	Groen 100MB LED
4	Adresschakelaar
5	Polling LED
6	TX- en RX-LED's
7	Aansluitklemmen (naar inbraakcentrale)
8	Connectoren verbindingsaansluitingen (naar de inbraakcentrale of andere compatibele modules)
9	Connector sabotageschakelaar

3.1**Overzicht**

De B426 Conettix Ethernet Communicatiemodule is een 4-draads gevoed SDI-, SDI2- of optiebusapparaat dat voorziet in bi-directionele communicatie met compatibele inbraakcentrales via IPv6 of IPv4 Ethernet-netwerken.

De ingebouwde schakelaar van de B426 bepaalt het busadres van het apparaat. Voer de configuratie uit van de B426 met behulp van de configuratie-webpagina's van de B426. Overige configuratie-opties omvatten:

- B9512G/B8512G, B6512/B5512/B4512/B3512, D9412GV4/D7412GV4 v2.xx. SDI2-bedieningspaneel en Remote Programming Software (RPS)-configuratie.
- AMAX 2000/2100/3000/4000 . A-Link-configuratie.

De B426 Conettix Ethernet Communicatiemodule is compatibel met IPv6.

Voor ULC-S559 kan de B426 worden gebruikt voor actieve of passieve communicatie. Voor passieve communicatie is de maximale communicatiecontrole 24 uur. Voor actieve communicatie is de maximale communicatiecontrole (heartbeat) 89 seconden. NIST-encryptie is vereist.

3.2 Busadres-instellingen

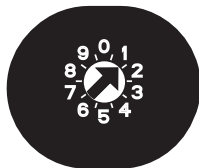
De adresschakelaar bepaalt het bustype en het adres van de module op de bus. De inbraakcentrale gebruikt het adres om te communiceren. Gebruik een schroevendraaier met platte kop om de adresschakelaar in te stellen.



Aanwijzing!

De module leest de instelling van de adresschakelaar alleen in tijdens het opstarten van de module. Als u de instelling wijzigt nadat u de module onder spanning heeft gezet, moet u de module spanningsloos brengen en de spanning terug aanbrengen om de nieuwe instelling te activeren.

Met de adresschakelaar van de B426 kan de waarde voor het adres van de module worden bepaald. In de afbeelding hieronder wordt de instelling van de adresschakelaar voor adres 1 afgebeeld. Zie de volgende tabel voor centralespecifieke instellingen.



Afbeelding 3.3: Adresschakelaar is ingesteld op adres 1

Inbraakcentrales	Schakelaarpositie	Adres inbraakcentrale	Bustype	Functie
B9512G/B8512G, B6512/B5512/B4512/B3512, GV4, Solution 2000/3000	1	1	SDI2	Automatisering, Programmeren op afstand of Rapportage
B9512G/B8512G, GV4, Solution 2000/3000	2	2		

Inbraakcentrales	Schakel arpositie	Adres inbraakcentr ale	Bustype	Functie
GV4, GV3, GV2, D9412G/ D7412G/D7212G v6.3 of hoger	3	80	SDI	Automatisering
GV4, GV3, GV2, D9412G/ D7412G/D7212G v6.3 of hoger	4	88		Rapportage of programmeren op afstand
GV4, GV3	5	92		
FPD-7024 v1.06+, DS7240V2, DS7220V2, Easy Series V3+, AMAX Series, CMS Series	6	134	Optie	
DS7400Xi	7	13		
DS7400Xi	8	14		Rapportage
FPD-7024, AMAX Series, CMS Series	9	250		Rapportage of programmeren op afstand

Tab. 3.1: Instellingen adressschakelaar B426

4 Installatie

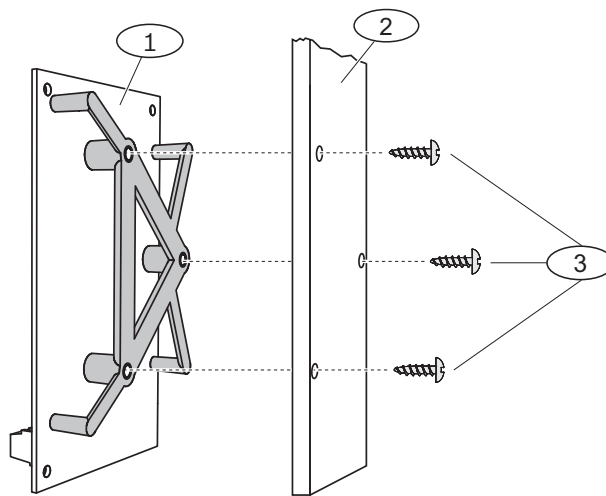
Nadat u de adresschakelaar voor het juiste adres hebt ingesteld, kunt u de module in de behuizing monteren en vervolgens de bekabeling leggen van de module naar de inbraakcentrale en naar de Ethernet-verbinding.

4.1 Breng de module aan in de behuizing

Monteer de B426 in het montagepatroon met 3 gaten van de behuizing met behulp van de meegeleverde bevestigingsschroeven en montagesteun.

Voor UL-gecertificeerde systemen dient u de module in de behuizing van de inbraakcentrale of in een UL-gecertificeerde behuizing te monteren (bijvoorbeeld, D8103 Universele behuizing).

Breng alle communicatieapparatuur onder in een behuizing die voorzien is van een sabotagecontact, conform de volgende bepalingen binnen standaard CAN/ULC-S304-06: 5.2.6; 5.2.9; 5.2.10 en 5.2.15.



Afbeelding 4.1: De module monteren

Ref. cijfer — Omschrijving
1 — B426 met montagebeugel geïnstalleerd
2 — Behuizing
3 — Bevestigingsschroeven (3)

4.2 De sabotageschakelaar monteren en bekabelen (optioneel)

Voor B9512G/B8512G, B6512/B5512/B4512/B3512 en GV4 v.2xx inbraakcentrales kunt u een sabotageschakelaar van de deurvergrendeling op één module in een behuizing aansluiten.

De optionele sabotageschakelaar installeren voor gebruik met een B426:

1. Breng de ICP-EZTS deksel en muur sabotageschakelaar (P/N: F01U009269) aan op de montageplaats voor de sabotageschakelaar in de behuizing. Raadpleeg *de Cover and Wall Tamper Switch (ICP- EZTS) Installation Guide* (P/N: F01U003734) voor alle instructies.
2. Sluit de bedrading van de sabotageschakelaar aan op de connector van de sabotageschakelaar van de module. Zie *Moduleoverzicht B426, Pagina 8* voor de locatie van de connector van de sabotageschakelaar.

4.3 De bedrading naar de inbraakcentrale

Bij het bekabelen van een B426 naar een SDI- of SDI2-inbraakcentrale, kunt u of ofwel de aansluitklemmen van de module, gelabeld R, Y, G, B (PWR, A, B, COM), of de connectoren verbindingaansluitingen van de module (inclusief kabel) gebruiken. In onderstaande afbeelding is de locatie van zowel de aansluitklemmen als de connectoren verbindingaansluitingen op de module afgebeeld.



Aanwijzing!

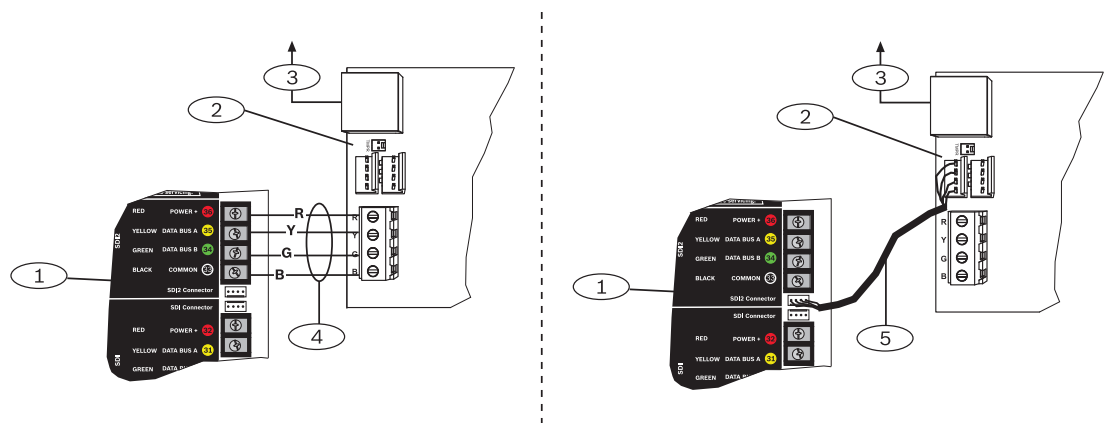
Schakel alle voeding uit (AC en batterij) voordat u verbinding maakt. Anders kan dit leiden tot persoonlijk letsel en/of beschadiging van de apparatuur.



Aanwijzing!

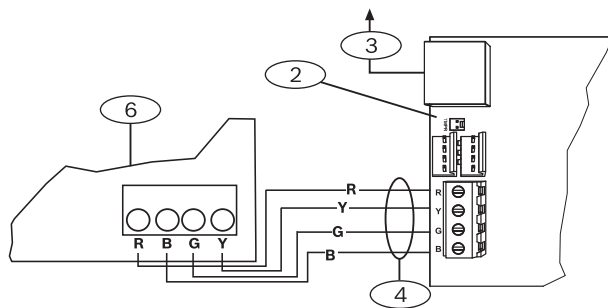
Gebruik ofwel de aansluitklemmen **of** verbindingskabel om een verbinding te maken naar de inbraakcentrale. Gebruik ze niet tegelijk. Bij het aansluiten van meerdere modules kunt u aansluitklemmen en connectoren verbindingaansluitingen gecombineerd gebruiken.

Leg de bekabeling van de module naar de databusterminals van de compatibele inbraakcentrale. Sluit de Ethernet-kabel aan op de Ethernet-poort op de module.



Afbeelding 4.2: Met behulp van aansluitklemmen of kabelaansluitingen (GV4-inbraakcentrale is afgebeeld)

Ref. cijfer	Omschrijving
1	SDI2 inbraakcentrale. Bij SDI-inbraakcentrales legt u de bekabeling van R, Y, G, B naar de SDI-bus.
2	Module
3	Naar het Ethernet-netwerk
4	Bedrading van aansluitklemmen
5	Verbindingskabel (P/N: F01U079745) (meegeleverd)



Afbeelding 4.3: Bekabeling naar aansluitklem van optiebus

Ref. cijfer	Omschrijving
1	Compatibele inbraakcentrale (inbraakcentrale FPD-7024 afgebeeld)
2	Module
3	Naar het Ethernet-netwerk
4	Bedrading van aansluitklemmen

Raadpleeg de documentatie bij de inbraakcentrale voor de volledige bekabelingsinstructies.

5 Configuratie

U kunt de B426 configureren met behulp van een van de methoden die in deze sectie voor uw inbraakcentrale-type zijn beschreven:

- *Plug-and-Play-configuratie voor SDI2 of inbraakcentrales met optiebus, Pagina 14*
- *Plug-and-Play-configuratie voor SDI of inbraakcentrales met optiebus, Pagina 14*
- *Webgebaseerde configuratie, Pagina 14* (alle compatibele inbraakcentrale-typen)

5.1 Plug-and-Play-configuratie voor SDI2 of inbraakcentrales met optiebus

Aanwijzing!

Inbraakcentrales met optiebus bevatten AMAX 2100/3000/4000 firmware-versie v1.5 of hoger.



Bij het verbinden van een B426 met een bestaande SDI2- of optiebus-inbraakcentrale, negeert de inbraakcentrale de instellingen van de module. Om de aangepaste module-instellingen te behouden wanneer u een module op een geconfigureerde inbraakcentrale aansluit, moet u Panel Programming Enable uitschakelen met behulp van webgebaseerde configuratie, voordat u de SDI2- of optiebus aansluit.

Wanneer de inbraakcentrale is aangesloten op een niet-standaard SDI2- of optiebus-inbraakcentrale, configureert de inbraakcentrale automatisch een aangesloten module.

1. Stel de adresschakelaar in op het juiste adres voor de inbraakcentrale als dit nog niet is ingesteld (SDI2-inbraakcentrales gebruiken adres 1 of 2, optiebus-inbraakcentrales gebruiken adres 134 of 250).
2. Sluit de module aan op de bus van de inbraakcentrale en breng de spanning aan.
3. Programmeer de communicatie-instellingen van de inbraakcentrale met behulp van RPS voor SDI2-inbraakcentrales, A-Link voor optiebus-inbraakcentrales of het bedieningspaneel.

De inbraakcentrale slaat de module-instellingen op en programmeert automatisch de aangesloten module. Om de automatische module-programmering te negeren, gebruikt u de webconfiguratiepagina's om de Panel Programming Enable-parameter in te stellen op **NEE** voordat u de installatie start.

5.2 Plug-and-Play-configuratie voor SDI of inbraakcentrales met optiebus

Wanneer de installatie plaatsvindt in een van de volgende situaties hoeft de B426 niet verder geconfigureerd te worden:

- DHCP is beschikbaar op uw netwerk.
- AES-encryptie is niet vereist.
- Standaardinstellingen voor de B426-poort (UDP op poort 7700) zijn goedgekeurd door de netwerkbeheerder.

5.3 Webgebaseerde configuratie

Voor installaties die een niet-standaard configuratie vereisen, kunt u gebruikmaken van de B426 Webgebaseerde configuratiepagina's.

**Aanwijzing!**

Bij aansluiting op een B9512G/B8512G-, B6512/B5512/B4512/B3512- of D9412GV4/D7412GV4/D7212GV4-inbraakcentrale, moet in de configuratie voor de module de optie Web Access Enable zijn ingesteld op Yes om toegang te krijgen tot de module of deze te configureren.

Om gebruik te maken van de B426 Configuratiepagina's, hebt u het IP-adres of de hostnaam van de module nodig. Zie:

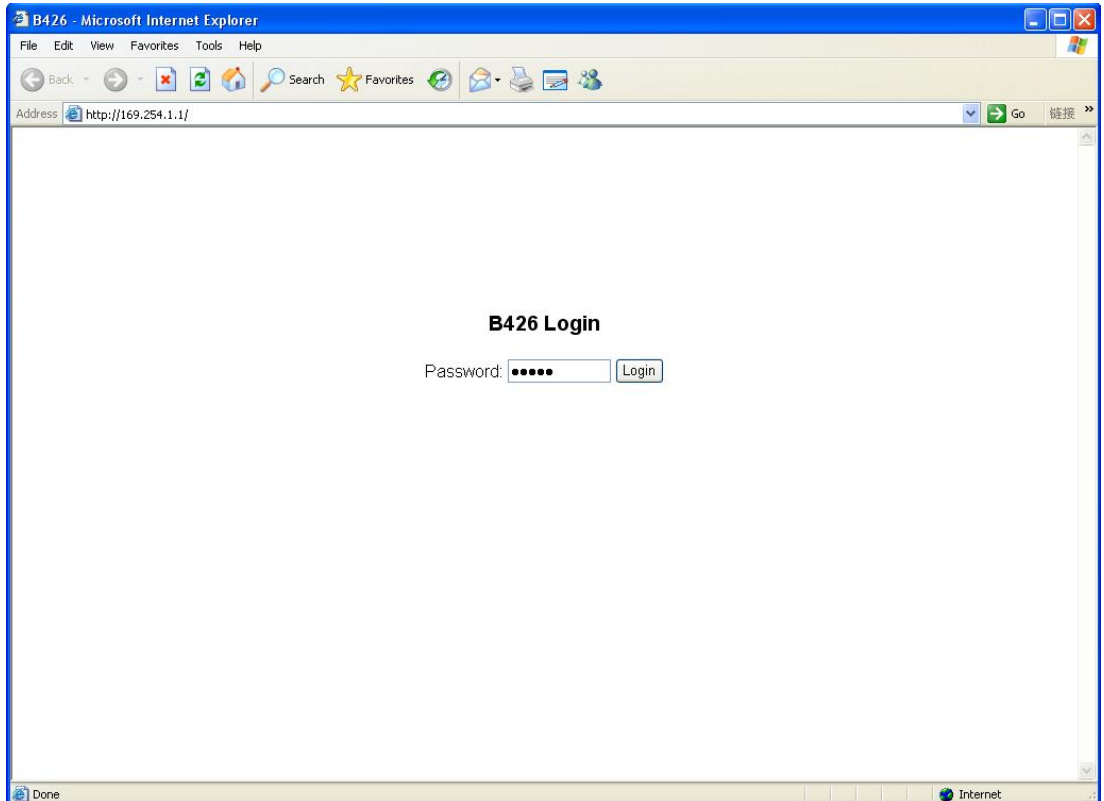
- *Module Hostname, Pagina 36*
- *IP-adres van module, Pagina 36*

5.3.1**Webgebaseerde configuratie: aanmelden en gebruiken****Aanwijzing!**

Als u geen verbinding kunt maken met de module, moet u mogelijk de configuratie van de webbrowser wijzigen, zodat er geen proxy-server wordt gebruikt. Raadpleeg de online helpfunctie van de browser voor instructies met betrekking tot het uitschakelen van de proxy-service.

Webgebaseerde configuratie gebruiken (B426 Configuratiepagina's):

1. Open een internetbrowser (Microsoft Internet Explorer 6 of hoger of Mozilla Firefox 3 of hoger), voer het IP-adres of de hostnaam van B426 in en druk op [Enter]. (Als Web and Automation Security is ingeschakeld op de B426, dient u **https://** in te voeren in plaats van **http://**). De **Login**-pagina van de B426 wordt geopend.



Afbeelding 5.1: Pagina B426 Login

2. Voer het wachtwoord in (het standaard wachtwoord is *B42V2*) en klik op **Login**. De hoofdpagina **Device Information** wordt geopend. (Zie *Pagina Device Information (home)*, *Pagina 16*.)
3. Blader naar de pagina met gewenste instellingen.
4. Wanneer u de wijzigingen op de pagina hebt doorgevoerd, klikt u op **OK**.



Aanwijzing!

Voordat u naar een nieuwe pagina met instellingen gaat, dient u op **OK** te klikken om de gewijzigde waarden op te slaan.

5. Klik op **Save & Execute** om alle wijzigingen op te slaan en deze toe te passen op het apparaat.

U dient het standaard wachtwoord te wijzigen om te garanderen dat de moduleconfiguratie wordt beveiligd. Wijzig het Web Access-wachtwoord met behulp van de pagina **Maintenance**.

5.3.2

Pagina Device Information (home)

In het hoofdvenster **Device Information** wordt basisinformatie weergegeven voor de module en aan de linkerzijde vindt u links naar de configuratie-webpagina's.

The screenshot shows a web browser window displaying the Bosch B426 Device Information page. The browser address bar shows the URL: `https://10.25.126.146/lgs.cgi?%26^%25%24%23%40=`. The page features the Bosch logo and the model number B426. A sidebar on the left contains navigation links: Home, Basic Network Settings, Advanced Network Settings, Panel Address Settings, Encryption and Security Settings, Maintenance, Factory Default, Save and Execute, Logout, and Firmware Update. The main content area is titled 'Device Information' and contains a table with the following data:

IP Address:	10.25.126.146 fe80::204:63ff:fe60:3525
MAC Address:	00-04-63-60-35-25
Firmware Version:	03.05.0001 (Apr 29 2016 11:18:27)
IP Stack Version:	08.07.8903
UPKI Version:	03.03.0202
AES Lib Version:	01.00.0000
Product ID:	96186.39340395219
Ethernet Speed:	100Mbps
Ethernet Duplex:	Half Duplex
UPnP Portmapping:	Disabled

At the bottom of the page, the copyright notice reads: 'Copyright: Bosch Security Systems, Inc. 2015. All rights reserved.'

Afbeelding 5.2: De pagina Device Information

5.3.3

Instellingen wijzigen en opslaan met behulp van het web

De instellingen voor de module zijn ingedeeld op onderwerp in de linkerkolom van de webinterface in de menustructuur van de module.

Sommige instellingen (menuopties) kunnen niet beschikbaar zijn als:

- de geconfigureerde instelling in strijd is met een andere geconfigureerde instelling (de **Static IP**-instelling is bijvoorbeeld niet beschikbaar als DHCP is ingeschakeld).
- de instelling in strijd is met de adresinstelling (de **Panel Address**-instelling is bijvoorbeeld ingesteld op read-only als de adresschakelaar op een andere stand dan de stand 0 staat).
- De instelling is niet beschikbaar in de huidige productversie.

Instellingen opslaan met behulp van het web

Om gewijzigde waarden te behouden, klikt u op de **OK**-toets op elke pagina voordat u naar een andere pagina met instellingen gaat (menu).

Om alle gewijzigde waarden op te slaan en toe te passen op de module, klikt u op de link **Save and Execute** .



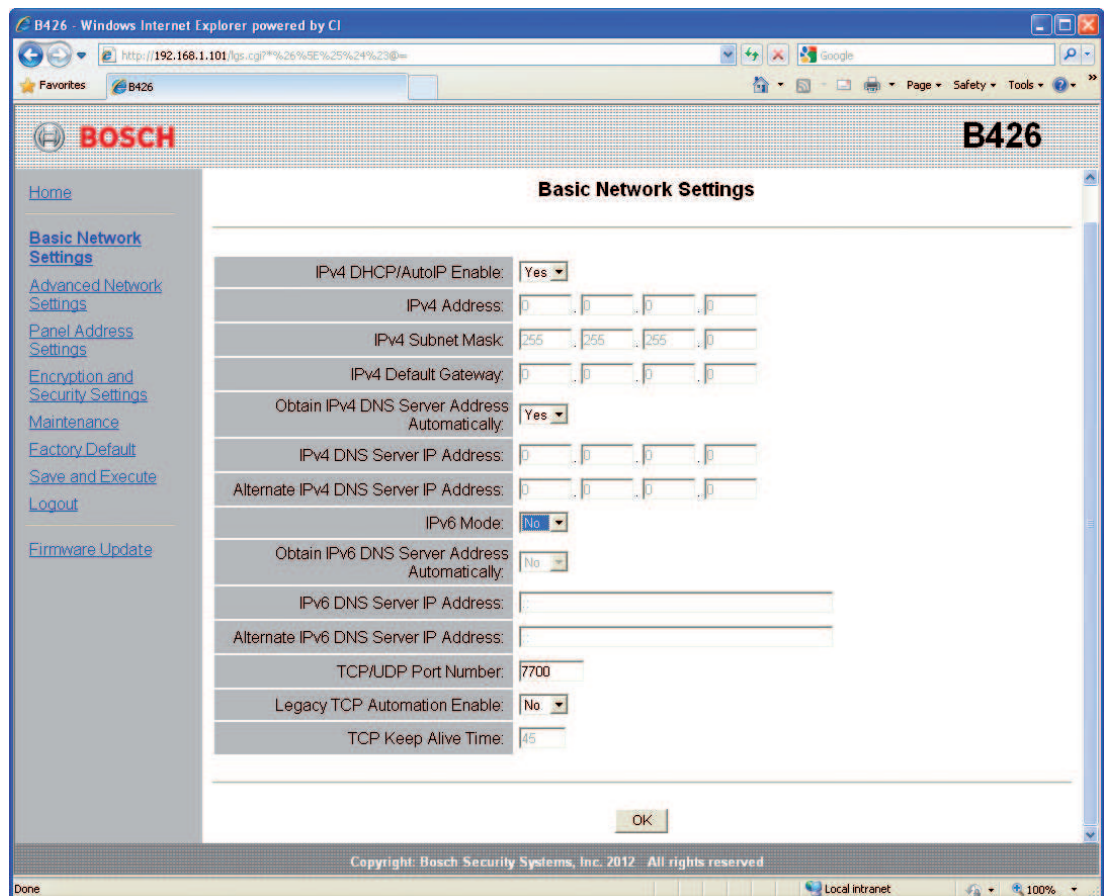
Aanwijzing!

Het opslaan van de instellingen kan ertoe leiden dat de huidige internetsessie wordt beëindigd.

5.3.4

De pagina Basic Network Settings

De pagina **Basic Network Settings** stelt de van toepassing zijnde opties beschikbaar, afhankelijk van het feit of de IPv6-modus is in- of uitgeschakeld.



Afbeelding 5.3: De standaard Basic Network Settings-webpagina

IPv4 DHCP/AutoIP Enable

Standaard: Yes

Selecties: Yes, No

Yes: DHCP /AutoIP is ingeschakeld.

No: DHCP/AutoIP is uitgeschakeld.

DHCP is een auto-configuratieprotocol dat ervoor zorgt dat een computer automatisch wordt geconfigureerd, zonder tussenkomst van een netwerkbeheerder. DHCP biedt ook een centrale database, waarmee computers worden gevolgd die verbinding maken met het netwerk. Hiermee wordt voorkomen dat twee computers geconfigureerd worden met hetzelfde IP-adres.

Auto-IP maakt het mogelijk om dynamische IP-adressen toe te wijzen aan een apparaat als dit wordt opgestart. Terwijl voor DHCP een DHCP-server nodig is, is voor AutoIP geen server nodig voor het selecteren van een IP-adres. Een host die is ingesteld met AutoIP krijgt een IP-adres van 169.254.xxx.xxx.



Aanwijzing!

Als u DHCP /AutoIP inschakelt, maakt de module geen gebruik van het IPv4-adres, subnetmasker of de gateway. De desbetreffende velden op de pagina zijn uitgeschakeld, maar eerder ingevoerde waarden worden weergegeven en kunnen niet worden gewijzigd. Als u DHCP /AutoIP uitschakelt, moet u het IPv4-adres, subnetmasker en de gateway instellen.

IPv4 Address

Standaard: 0.0.0.0

Selectie: 0.0.0.0 tot 255.255.255.255

Deze parameter stelt een statisch IPv4-adres in voor de module als DHCP is uitgeschakeld.

IPv4 Subnet Mask

Standaard: 255.255.255.0

Selectie: 0.0.0.0 tot 255.255.255.255

Het subnet wordt toegepast om het netwerk onder te verdelen in kleinere, efficiëntere subnetwerken, om overmatig botsen van Ethernet-pakketten in een groot netwerk te voorkomen. Een belangrijk kenmerk van subnetten is het subnetmasker. Door een subnetmasker toe te passen op een IP-adres, kunt u het netwerk en de knooppunten van het adres bepalen. Als DHCP/AutoIP ingesteld is op **Yes**, kan deze parameter niet worden gewijzigd.

IPv4 Default Gateway

Standaard: 0.0.0.0

Selectie: 0.0.0.0 tot 255.255.255.255

Een gateway is een knooppunt (normaal gezien een router) in een TCP/IP-netwerk dat dient als toegangspunt tot een ander netwerk. Een host maakt gebruik van een standaard gateway als het doeladres van een IP-pakket buiten het lokale subnet ligt. Het adres van de standaard gateway is meestal een interface die hoort bij de grensrouter van de LAN. In de DHCPmodus wordt de standaard gateway meestal automatisch bepaald. Als DHCP/AutoIP ingesteld is op **Yes** kan deze parameter niet worden gewijzigd.

Obtain IPv4 DNS Server Address Automatically

Standaard: Yes

Selectie: Yes, No

Als u deze parameter instelt op Nee, kunt u het serveradres invoeren. Als u deze parameter instelt op Ja, worden de adressen gewist en kunt u geen nieuw adres invoeren.

IPv4 DNS Server IP Address

Standaard: 0.0.0.0

Selectie: 0.0.0.0 tot 255.255.255.255

Een domeinnaamserver (DNS) converteert internet-domeinnamen of hostnamen naar hun overeenkomstige IP-adressen. Deze instelling wordt toegepast om het adres van een DNS-server te configureren in de statische IP-modus. In de DHCP-modus geeft de standaardwaarde 0.0.0.0 aan dat de standaardDNS van de DHCP-server wordt gebruikt. Om een aangepaste DNS-server in de DHCP-modus te gebruiken, dient u de parameter voor het specifieke IP-adres van de DNS-server te wijzigen.

Het adres heeft een punt-decimaal aanduiding die bestaat uit de vier octetten van het adres, die afzonderlijk in decimalen worden weergegeven, gescheiden door een punt. Elk octet heeft een waarde tussen 0-255.

Alternate IPv4 DNS Server IP Address

Standaard: 0.0.0.0

Selectie: 0.0.0.0 tot 255.255.255.255

Deze parameter biedt een alternatief IP-adres voor de IPv4 DNS-server.

Het adres heeft een punt-decimaal aanduiding die bestaat uit de vier octetten van het adres, die afzonderlijk in decimalen worden weergegeven, gescheiden door een punt. Elk octet heeft een waarde tussen 0-255.

Als de module geen adres kan verkrijgen van de primaire server, dan wordt, indien gespecificeerd, de alternatieve DNS-server gebruikt. Door het alternatieve adres te gebruiken, moet u een primair adres specificeren.

IPv6 Mode

Standaard: uitschakelen

Selectie: inschakelen, uitschakelen

Inschakelen: IPv6 ingeschakeld; module werkt met zowel IPv6 en IPv4-adressering.

Uitschakelen: IPv6 uitgeschakeld; module werkt alleen met IPv4-adressering.

IP Versie 6 (IPv6) is een nieuwe versie van Internet Protocol. Selecteer of de module werkt met IPv6 als aanvulling op IPv4-adressering.

Obtain IPv6 DNS Server Address Automatically

Standaard: Yes

Selectie: Yes, No

Als u deze parameter instelt op Nee, kunt u het serveradres invoeren. Als u deze parameter instelt op Ja, worden de adressen gewist en kunt u geen nieuw adres invoeren. In de DHCP-modus geeft de standaardwaarde 0.0.0.0 aan dat de standaardDNS van de DHCP-server wordt gebruikt. Om een aangepaste DNS-server in de DHCP-modus te gebruiken, dient u de parameter in Nee te wijzigen en het specifieke IP-adres van de DNS-server in te voeren.

IPv6 DNS Server IP Address

Standaard: ::**Selectie:** 0:0:0:0:0:0:0:0 tot FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF

Deze parameter configureert het IPv6 DNS-serveradres.

Een DNS-server converteert internet-domeinnamen of hostnamen naar hun overeenkomstige IP-adressen. In de DHCP-modus geeft de standaardwaarde aan dat de standaard-DNS van de DHCP-server wordt gebruikt. Om een aangepaste DNS-server in de DHCP-modus te gebruiken, dient u de parameter voor het specifieke IP-adres van de DNS-server te wijzigen.

Het DNS-adres van de IPv6 heeft een hexadecimale aanduiding die bestaat uit de acht groepen van het adres die afzonderlijk in hexadecimale worden weergegeven, gescheiden door een dubbele punt. Elke groep kan een waarde hebben tussen 0000-FFFF. Als deze via de DHCP-service is bepaald, dient de standaardwaarde te blijven staan.

Alternate IPv6 DNS Server IP Address**Standaard: ::****Selectie:** 0:0:0:0:0:0:0:0 tot FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF

Deze parameter biedt een alternatief IP-adres voor de IPv6 DNS-server.

Het alternatieve DNS-adres van de IPv6 heeft een hexadecimale aanduiding die bestaat uit de acht groepen van het adres die afzonderlijk in hexadecimale worden weergegeven, gescheiden door een dubbele punt. Elke groep heeft een waarde tussen 0000-FFFF.

Als deze via de DHCP-service is bepaald, dient de standaardwaarde te blijven staan. Als de module geen adres kan verkrijgen van de primaire server, dan wordt, indien gespecificeerd, de alternatieve IPv6 DNS-server gebruikt. De module kan alleen gebruikmaken van de alternatieve IPv6-serveradressen als het primaire adres niet het standaardadres is.

TCP/UDP Port Number**Standaard:** 7700**Selectie:** 0 tot 65535

Met deze parameter wordt het nummer van de lokale poort ingesteld waarop de module luistert naar inkomend netwerkverkeer. Deze poort is ook de bronpoort voor uitgaande communicatie.

De TCP/UDP-poort is doorgaans geconfigureerd als 7700 als de inbraakcentrale communiceert met de centrale ontvanger van de meldkamer, RPS, Automation of Remote Security Control.

De poortnummers worden op verschillende manieren toegewezen, op basis van drie categorieën:

- Systeempoorten: 0 t/m 1023
- Gebruikerspoorten: 1024 t/m 49151
- Dynamische of Privépoorten: 49152 t/m 65535

Opmerking: selecteer een cijfer hoger dan 1023 om ongewenst verkeer te beperken.

Legacy TCP Automation Enable**Standaard:** No**Selectie:** Yes, No

Indien ingeschakeld, is een enkele TCP-verbinding zonder beveiliging toegestaan.

TCP Keep Alive Time

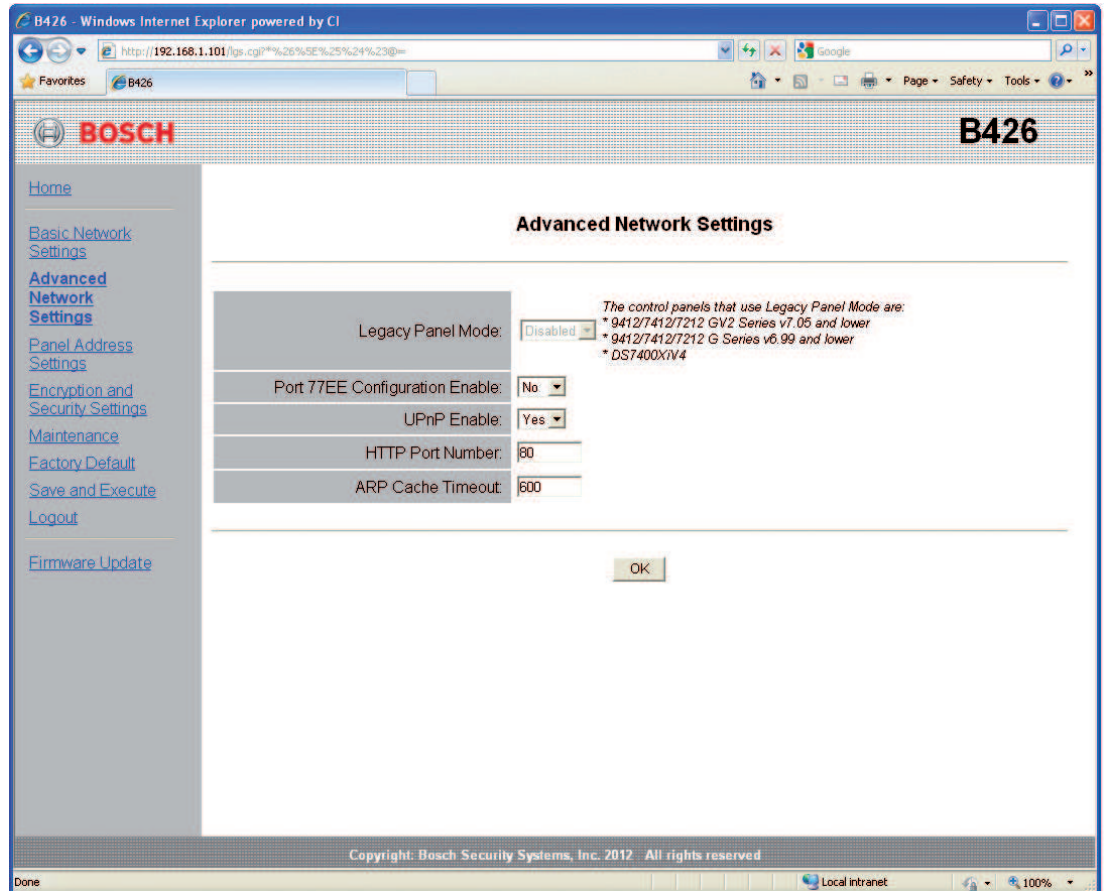
Standaard: 45

Selectie: 0 – 65 (0: uitschakelen, 1 - 65: keep-alive-tijd in seconden)

Selecteer het aantal seconden dat de eenheid moet wachten bij een stille verbinding voordat er wordt gecontroleerd of het huidige aangesloten netwerkapparaat zich nog steeds in het netwerk bevindt. Als er geen reactie komt, verbreekt het de verbinding.

5.3.5

De pagina Advanced Network Settings



Afbeelding 5.4: De pagina Advanced Network Settings

Legacy Panel Mode

Standaard: 0 (uitschakelen)

Selectie: 0, 1

0: Modus Oude centrale is uitgeschakeld.

1: Modus Oude centrale is ingeschakeld.

Deze optie zorgt ervoor dat de module de oude inbraakcentrales ondersteunt die met behulp van Datagram-modus 0 communiceren. Als Legacy Panel Mode is ingeschakeld, gebruikt de module de lokale-poortparameter zowel als bronpoort als bestemmingspoort.

De inbraakcentrales die gebruik maken van de Legacy Panel Mode zijn:

- GV2 v7,05 en lager
- D9412G/D7412G/D7212G v6.99 en lager
- DS7400XiV4

Port 77EE Configuration Enable

Standaard: No

Selecties: Yes, No

Ja: De netwerkconfiguratiepoort is ingeschakeld.

Neer: De netwerkconfiguratiepoort is uitgeschakeld.

De Conettix D6200 Programmeer-/systeembeheerssoftware gebruikt deze poort om te zoeken naar apparaten op het lokale netwerk.

UPnP Enable

Standaard: Yes

Selecties: Yes, No

Yes: UPnP is ingeschakeld.

No: UPnP is uitgeschakeld.

Universal Plug and Play (UPnP) maakt het mogelijk om apparatuur moeiteloos op elkaar aan te sluiten. Ook het uitrollen van particuliere en bedrijfsnetwerken wordt hiermee een stuk eenvoudiger. Indien ingeschakeld in de lokale router, wordt deze voorziening gebruikt om automatisch port forwarding rules op te zetten voor Remote Programming-verkeer naar de inbraakcentrale.

HTTP-poortnummer

Standaard: 80

Selecties: 1 tot 65535

Gebruik deze optie voor het configureren van het poortnummer voor de webserver van de module.

ARP Cache Timeout

Standaard: 600

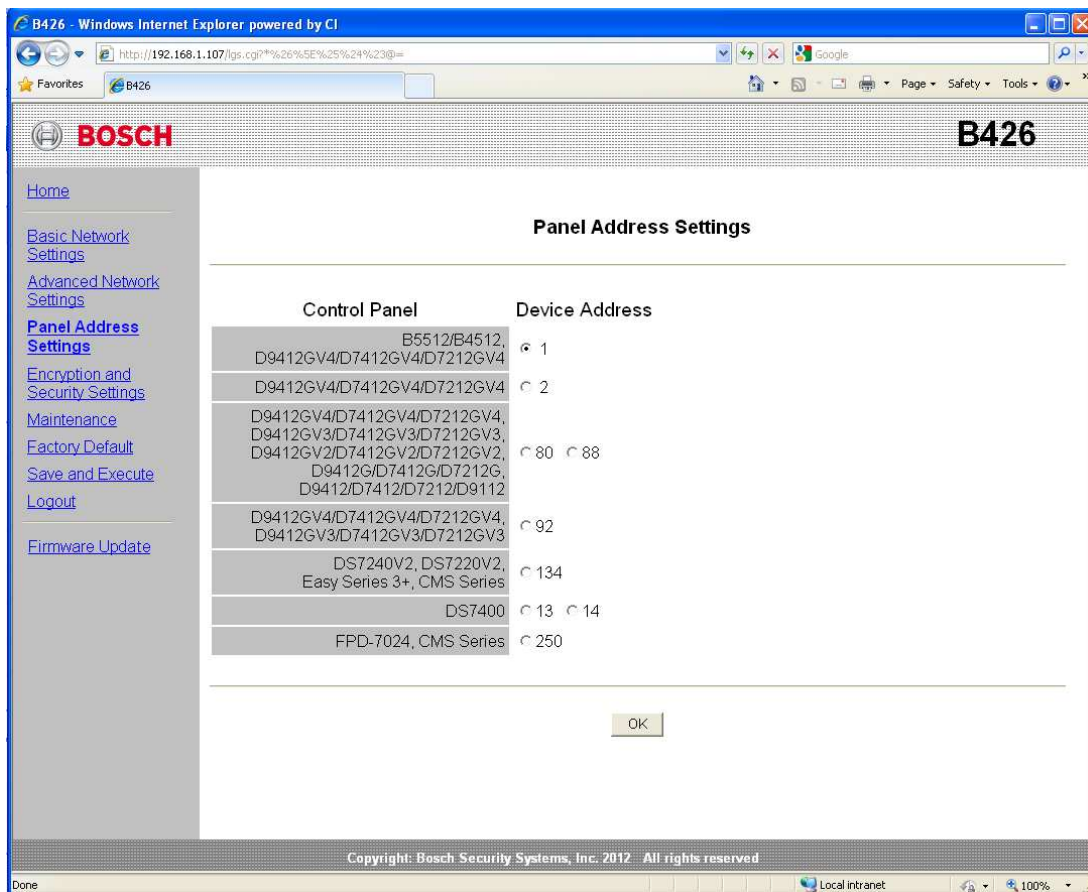
Selecties: 1 tot 600 (in stappen van 1 sec)

Wanneer de module met een ander apparaat in een netwerk communiceert, wordt dit voor elk van deze apparaten ingevoerd in de ARP-tabel. De ARP Cache Timeout definieert het aantal seconden (1 tot 600) voordat de ARP-tabel van de module wordt vernieuwd.

5.3.6

Pagina Panel Address Settings

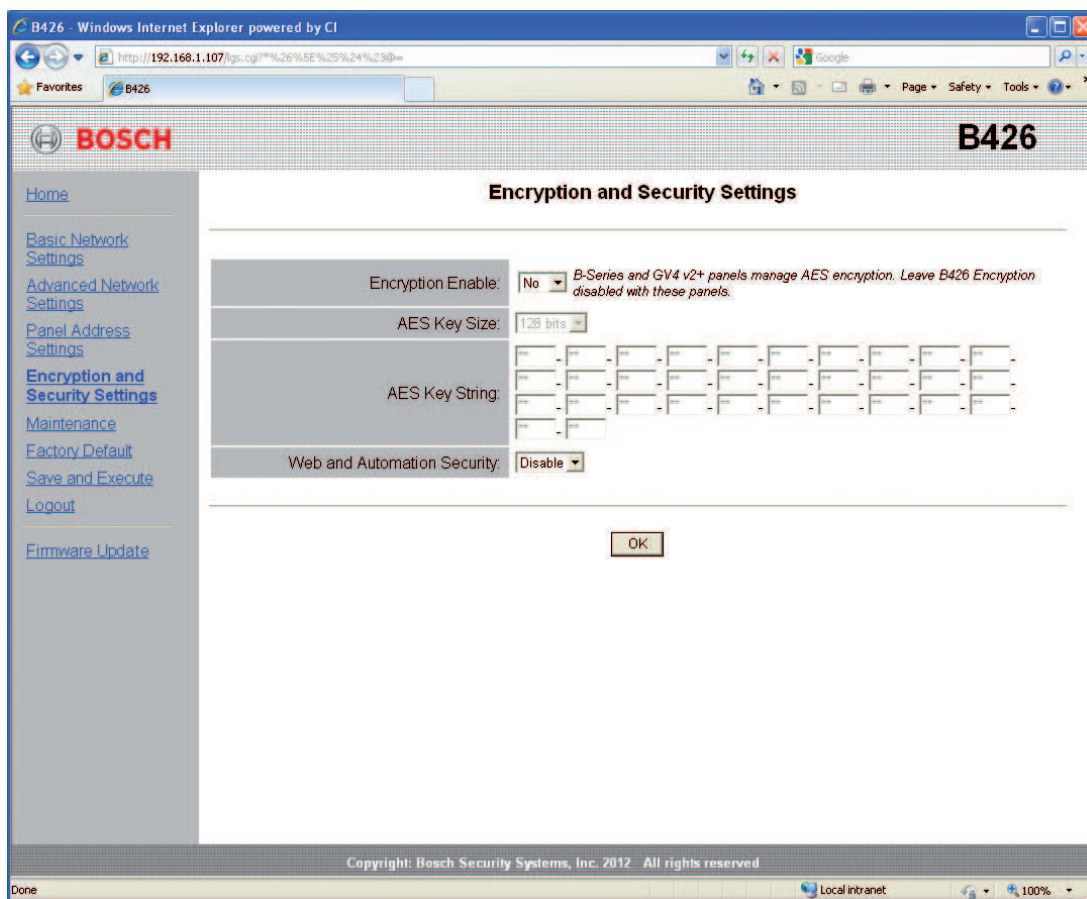
De pagina **Panel Address Setting** staat alleen configuratie toe als de adresschakelaar op de module is ingesteld op 0. Als de adresschakelaar op een andere positie dan 0 staat, wordt het ingestelde adres weergegeven.



Afbeelding 5.5: Pagina Panel Address Settings

Gebruik deze optie om het busadres te selecteren van het type inbraakcentrale waarop de module is aangesloten.

5.3.7 Encryption and Security Settings page



Afbeelding 5.6: Encryption and Security Settings Page

Encryption Enable

Standaard: No

Selecties: Yes, No

Ja: Alle UDP-communicatie (RPS en gebeurtenisrapporten) via de netwerkmodule is versleuteld. AES-encryptie moet ook zijn ingesteld op de ontvanger van de meldkamer en de pc waarop RPS wordt uitgevoerd.

No: Alle communicatie via de netwerkmodule wordt niet versleuteld.

Gebruik deze optie om AES-encryptie (Advanced Encryption Standard) op de module in of uit te schakelen.

Voor B9512G/B8512G, B6512/B5512/B4512/B3512 en GV4 v2.xx inbraakcentrales waarbij Panel Programming Enable op **Ja** is ingesteld, staat de module geen versleuteling toe, ongeacht de instelling.

AES Key Size

Standaard: 128

Selecties: 128, 192, 256

Gebruik deze optie om de AES sleutellengte te selecteren. De AES sleutellengte moet overeenkomen met de sleutellengte gebruikt in RPS en de ontvanger.

AES Key String

Standaard: de standaardwaarde varieert per sleutel.

Selecties: 64 hexadecimale tekens weergegeven in max. 32 velden (2 hexadecimale tekens per veld)

- 128 bit sleutelengte is 16 bytes (16 velden voor weergave van 2 ASCII-tekens [0-9, A-F]).
- 192 bit sleutelengte is 24 bytes (24 velden voor weergave van 2 ASCII-tekens [0-9, A-F]).
- 256 bit sleutelengte is 32 bytes. (32 velden voor weergave van 2 ASCII-tekens [0-9, A-F]).

Web and Automation Security

Standaard: Enable voor B9512G/B8512G, B6512/B5512/B4512/B3512 en GV4 v2.xx inbraakcentrales, Disable voor alle overige inbraakcentrales.

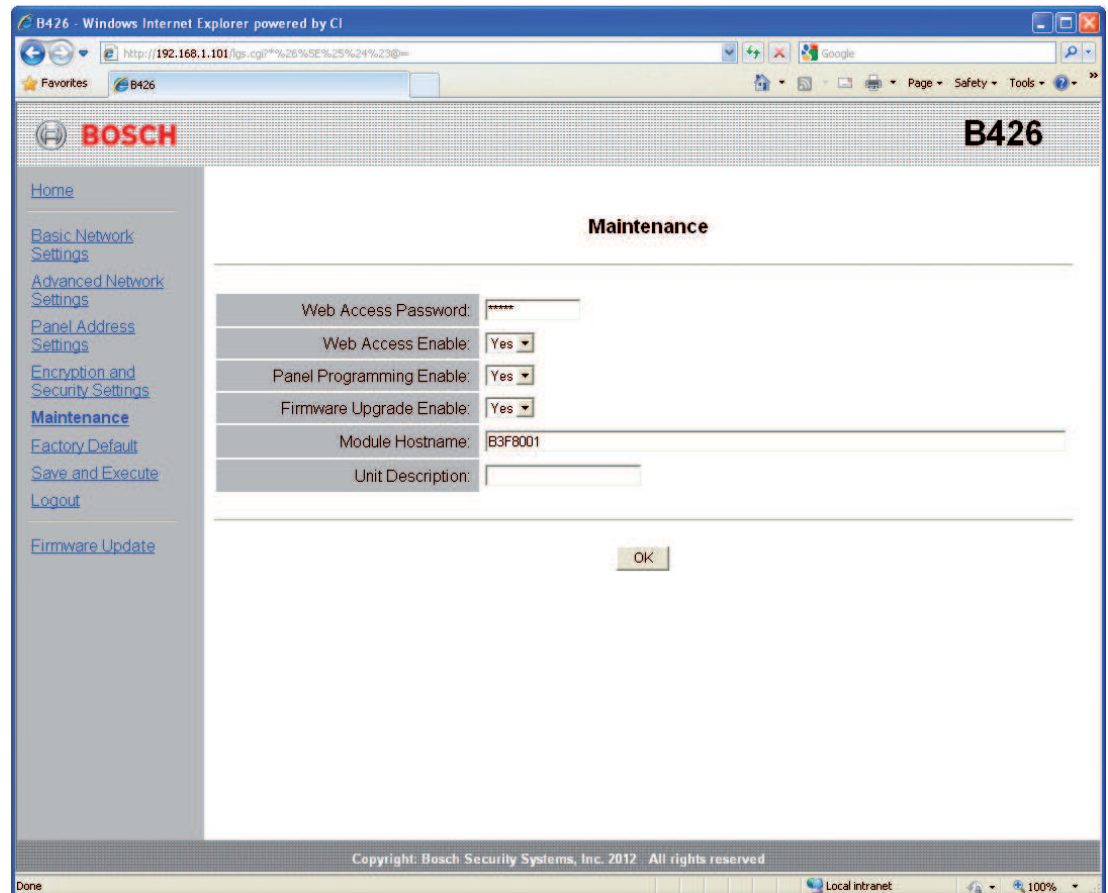
Selecties: Disable, Enable

Deze parameter schakelt de geavanceerde beveiliging voor Automation en B426 Web Access in.

Indien ingeschakeld, wordt HTTPS toegepast op B426 Web Access en verandert de standaardwaarde van de HTTP poortnummerparameter. Deze instelling schakelt ook TLS Security voor Automation in.

5.3.8

Pagina Maintenance



Afbeelding 5.7: Pagina Maintenance

Web Access Password

Standaard: B42V2

Selecties: Vier tot tien hoofdlettergevoelige alfanumerieke tekens

Voer het wachtwoord in om in te loggen op de configuratie-webpagina's. U wordt aanbevolen het standaard inlogwachtwoord te veranderen om de module van de configuratie te beveiligen.

Web Access Enable

Standaard: No voor B6512/B5512/B4512/B3512 en GV4 v2.xx of hoger inbraakcentrales, Yes voor alle overige inbraakcentrales

Selecties: Yes, No

Yes: Webconfiguratie is ingeschakeld

No: Webconfiguratie is uitgeschakeld

Schakel de toegang tot de configuratie-webpagina's in of uit.

Schakel web access NIET uit tenzij u werkt met een SDI2-centrale en AMAX 2100/ 3000/ 4000 met Panel Programming Enable ingeschakeld. Met SDI en optie-inbraakcentrales kan de module enkel via de webinterface worden geconfigureerd.

Panel Programming Enable

Standaard: Yes

Selecties: Yes, No

Yes: Inbraakcentrale programmeren is toegelaten.

No: Inbraakcentrale programmeren is uitgeschakeld.

Schakel het programmeren van de inbraakcentrale van de module met compatibele (alleen SDI2) inbraakcentrales en AMAX 2100/ 3000/ 4000 in of uit.

Schakel Web Access Enable en Panel Programming Enable niet uit. Als beide zijn uitgeschakeld, kunt u de module niet configureren.

Firmware Upgrade Enable

Standaard: No

Selecties: Yes, No

Yes: Maakt firmware-upgrades voor de B426 mogelijk.

No: Voorkomt firmware upgrades.

Schakel de mogelijkheid om de firmware module te upgraden via de configuratiepagina

Firmware Upgrade in of uit.

Module Hostname

Standaard: Leeg

Selecties: 64 alfanumerieke tekens

Leeg: Leeg herstelt de standaard hostnaam Bxxxxxx, waar xxxxxx de laatste zes cijfers van het MAC-adres van de module zijn.

Gebruik deze parameter om een hostnaam voor de module aan te maken of te wijzigen. Dit is de hostnaam van de module in het netwerk. U kunt ook de hostnaam gebruiken om contact op te nemen met de inbraakcentrale via RPS over het netwerk van Remote Security Control of voor webconfiguratie en diagnose van de module.



Aanwijzing!

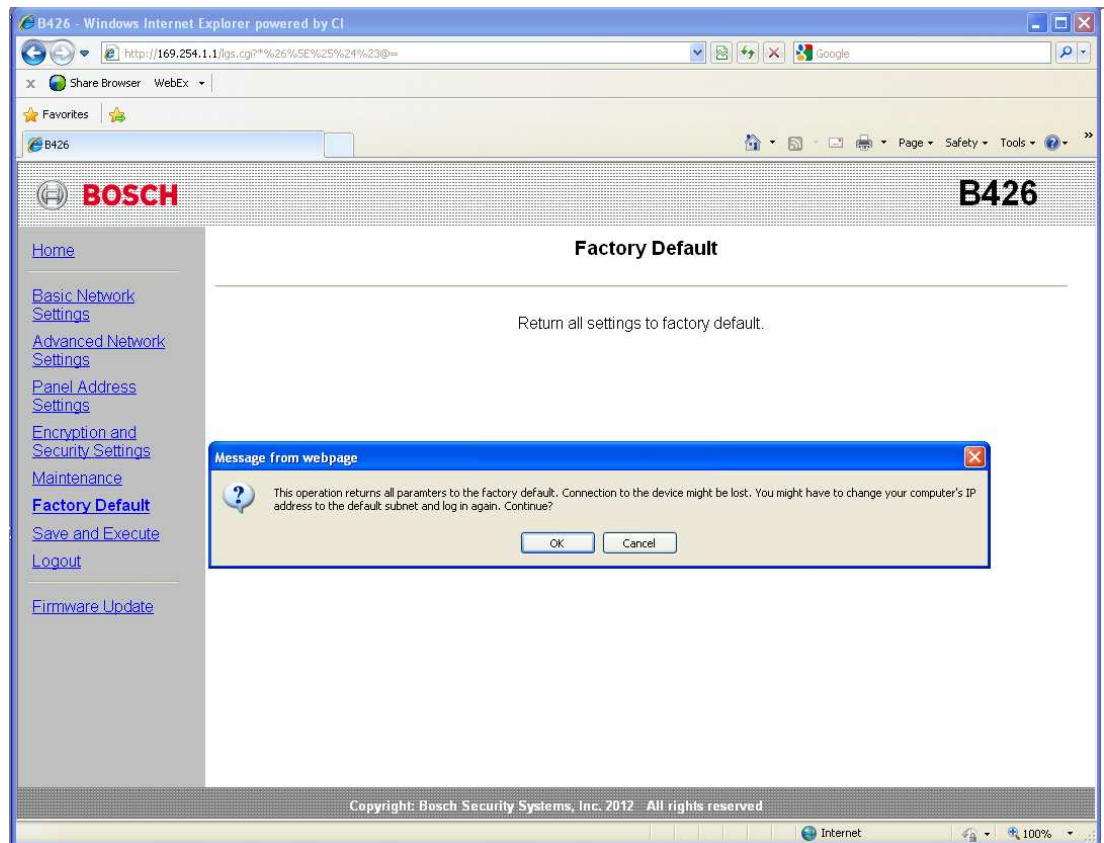
Gebruik de hostnaam op een lokaal netwerk met behulp van DHCP. Om de hostnaam extern te gebruiken, voert u de hostnaam in van de DNS-server.

Unit Description**Standaard:** Leeg**Selecties:** 20 alfanumerieke tekens

Gebruik deze parameter om een eenvoudige omschrijving van de unit aan te maken, zoals weergegeven in de webconfiguratiepagina's.

**Aanwijzing!**

Gebruik het dubbele aanhalingsteken (") niet, aangezien dit tot onverwachte resultaten leidt.

5.3.9**Pagina Factory Default****Afbeelding 5.8: Pagina Factory Default**

U kunt de module terugzetten naar de fabrieksinstellingen door op het **Factory Default**-menu te klikken.

Klik op **Cancel** om het terugzetten naar fabrieksinstellingen te annuleren. Als u **OK** selecteert, worden alle configuratieopties teruggezet naar de fabrieksinstellingen.



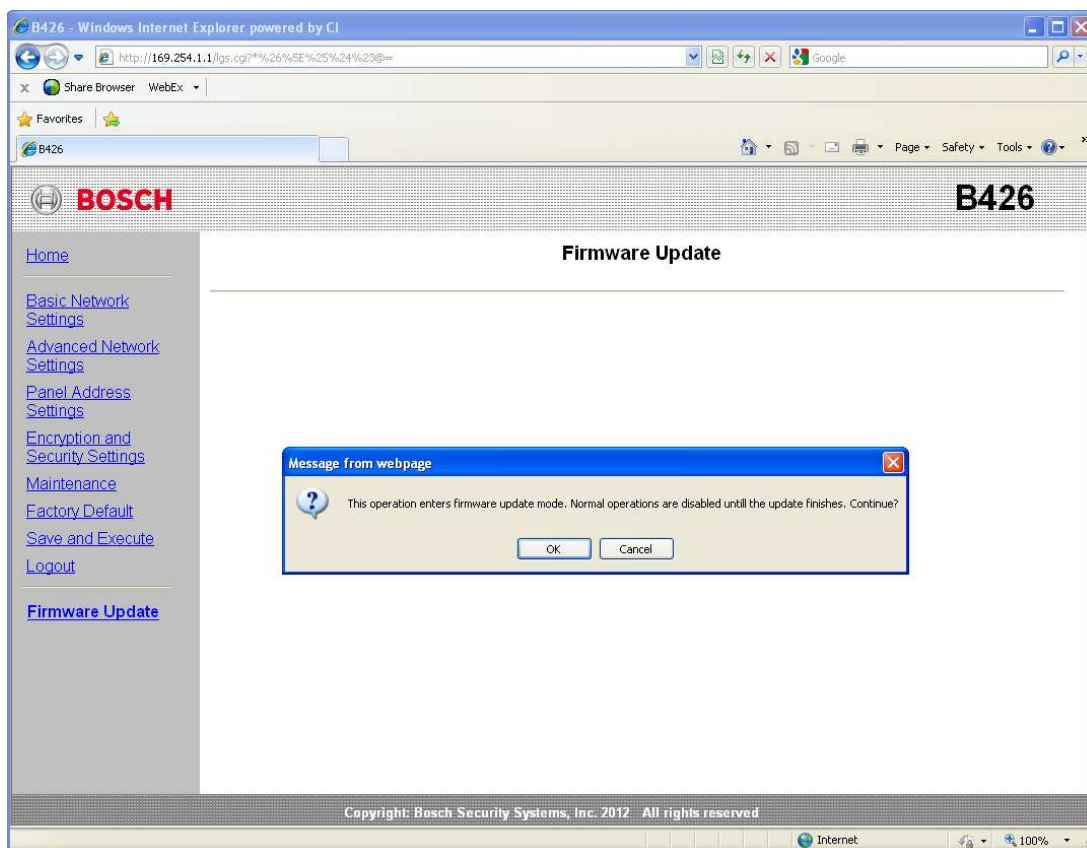
Aanwijzing!

Wanneer de module wordt teruggezet naar de fabrieksinstellingen kan de huidige internetsessie door de module worden beëindigd. Wanneer deze is verbonden met een compatibele SDI2inbraakcentrale, overschrijft inbraakcentrale de fabrieksinstellingen met de instellingen van de inbraakcentrale. U voorkomt het overschrijven van **Configuration Page**-instellingen door de inbraakcentrale-instellingen door Panel Programming Enable op No in te stellen nadat u de module hebt teruggezet naar de fabrieksinstellingen, maar voordat u op **Save and Execute** klikt.

5.3.10

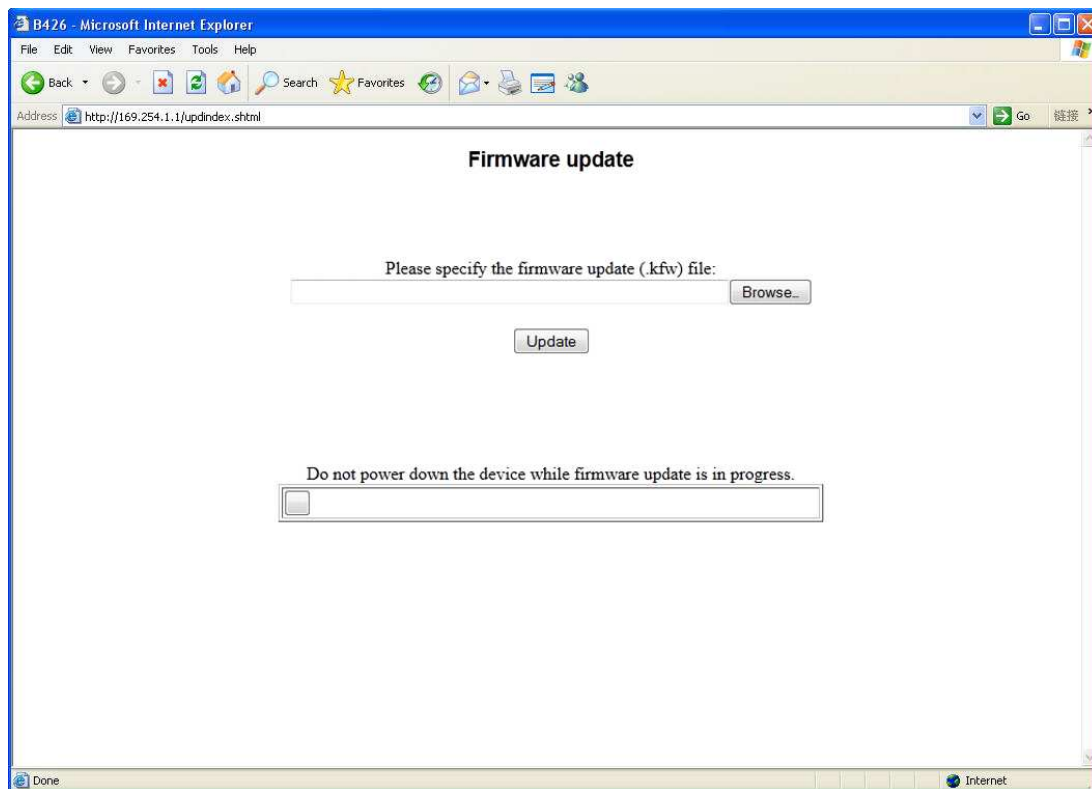
Pagina Firmware Update

Om de firmware in de module te upgraden, selecteert u de optie **Firmware Update** op de configuratie-hoofdpagina. De pagina **Firmware Update** wordt geopend.



Afbeelding 5.9: Pagina Firmware Update

Om door te gaan met de upgrade, klik op **OK**. Er wordt een nieuwe webpagina geopend, waarmee u het firmware-bestand kunt opzoeken en naar de module kunt uploaden.



Afbeelding 5.10: Upgradebestand specificeren bij firmware upgrade



Aanwijzing!

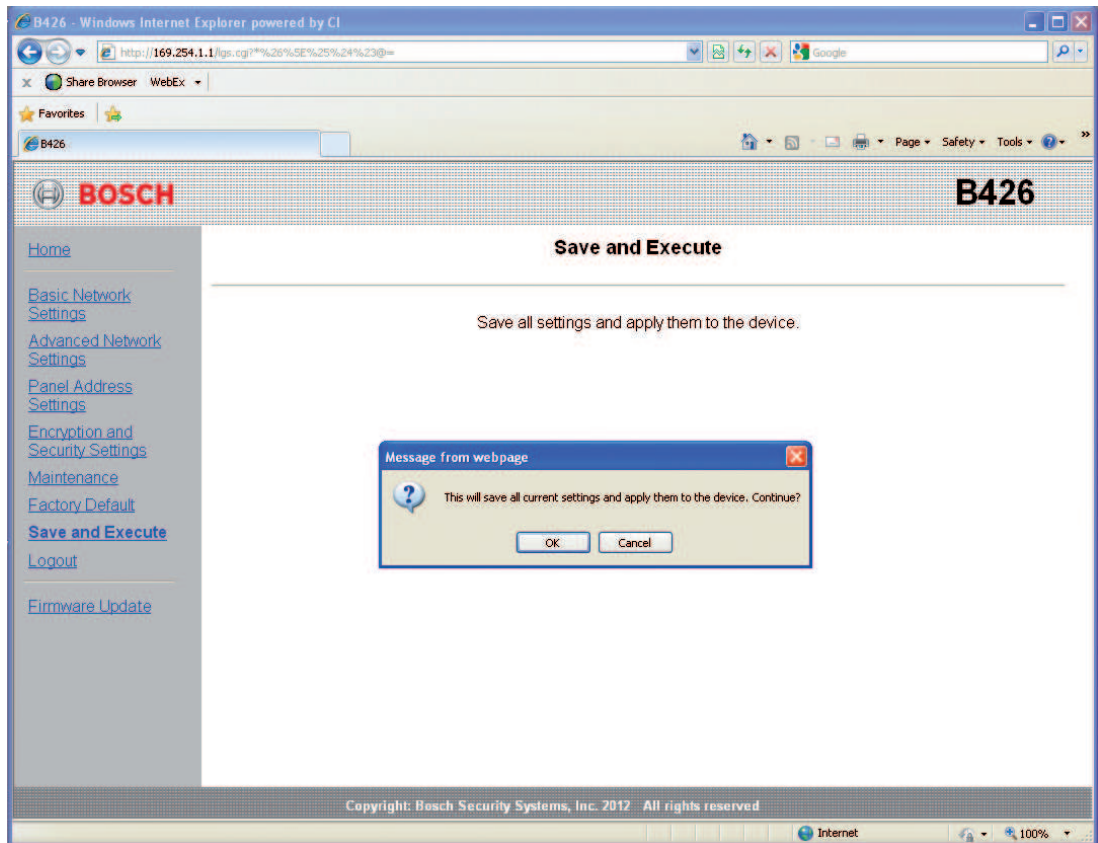
Door het upgraden van de firmware in de module wordt de huidige internetssessie beëindigd.

5.3.11

De webgebaseerde configuratiepagina's verlaten

Als u klaar bent met het configureren van de module, selecteert u de optie **Save and Execute**. De webpagina **Save and Execute** wordt geopend.

Om de wijzigingen in de configuratie op te slaan, klik op **OK**. Er verschijnt een bevestigingsmelding.



Afbeelding 5.11: Bevestiging Save and Execute





Om de configuratie-webpagina te verlaten, klikt u op **Logout**, hierna sluit u het venster van de internetbrowser.

6 LED's voor onderhoud en probleemoplossing

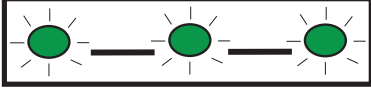

De B426 heeft de volgende ingebouwde LED's om te helpen bij probleemoplossing:

- Heartbeat (systeemstatus).
- RX (ontvangen).
- TX (verzenden).







Zie *Moduleoverzicht B426, Pagina 8* voor LED-locaties van Ethernet-koppelingen.



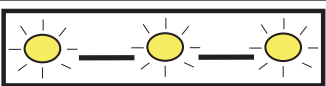

Knipperpatroon	Functie
Knippert 1 keer per sec 	Normale status. Geeft normale bedrijfstoestand aan.
Knippert 3 keer per sec 	Communicatiefoutstatus. Geeft een buscommunicatiefout aan. De module ontvangt geen opdrachten van de inbraakcentrale.
 Aan, aanhoudend	Probleemstatus. Geeft aan dat er een probleem is.
 Gedoofd	LED-probleemstatus. Module krijgt geen stroom of er is een ander probleem, waardoor de module de pollings-LED niet kan aansturen.

Tab. 6.2: Omschrijvingen heartbeat-LED

Knipperpatroon	Functie
 RX (ontvangen) Knipperend	Dit gebeurt wanneer de module een bericht ontvangt via de netwerkverbinding – UDP, TCP of DNS.
 TX (verzenden) Knipperend	Dit gebeurt wanneer de module een bericht verstuurt via de netwerkverbinding – UDP, TCP of DNS.



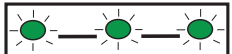


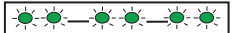






Tab. 6.3: Omschrijvingen RX- en TX-LED's

LINK (geel) LED-patroon	100Mb (groen) LED-patroon	Functie
 Gedoofd	 Gedoofd	Geen Ethernet-verbinding
 Aan, aanhoudend	 Gedoofd	10Base-T-verbinding
 Knipperend	 Gedoofd	10Base-T-activiteit

LINK (geel) LED-patroon	100Mb (groen) LED-patroon	Functie
 Aan, aanhoudend	 Aan, aanhoudend	100Base-TX-verbinding
 Knipperend	 Aan, aanhoudend	100Base-TX-activiteit

Tab. 6.4: Omschrijvingen LED's Ethernet-verbinding

Problemen weergegeven door LED's

Status	Heartbeat	Verzenden (TX)	Ontvangen (RX)
Netwerkkabel losgekoppeld	 Aan, aanhoudend	 Gedoofd	 Knippert 1 keer per sec.
Een IP-adres verkrijgen	 Aan, aanhoudend	 Gedoofd	 Knippert snel, 2 keer per sec
Lage busspanning	 Aan, aanhoudend	 Gedoofd	 Knippert 3 keer per sec
Interne fout	 Aan, aanhoudend	 Gedoofd	 Aan, aanhoudend

Tab. 6.5: Problemen



Aanwijzing!

Als de sabotageschakelaar wordt gesloten, zijn alle module LED's Gedoofd.

6.1

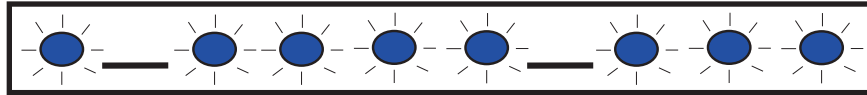
De firmwareversie weergeven

De firmwareversie weergeven met behulp van een LED-knipperpatroon:

- Als de optionele sabotageschakelaar is geïnstalleerd:
Activeer de sabotageschakelaar met de deur van de behuizing reeds geopend.
- Als de optionele sabotageschakelaar NIET is geïnstalleerd:
Sluit de sabotagepennen tijdelijk kort.

Als de sabotageschakelaar wordt geactiveerd (open naar gesloten) blijft de heartbeat-LED (pollings-LED) gedurende 3 sec Gedoofd, voordat de firmware-versie wordt aangegeven. De LED geeft de primaire, secundaire en tertiaire cijfers van de firmware knipperend weer, met een pauze van 1 sec. na ieder cijfer.

Hierna volgt een voorbeeld: versie 1.4.3 wordt weergegeven als het LED-knipperpatroon: [3 seconden pauze] * _**** _*** [3 seconden pauze, vervolgens normaal bedrijf].



Afbeelding 6.1: Voorbeeld van Firmware LED-knipperpatronen

7 Specificaties

Dit gedeelte bevat de specificaties van de module en informatie over compatibiliteit.

7.1 Technische specificaties

Omgevingseisen

Relatieve vochtigheidsgraad	Maximaal 93%, niet-condenserend
Bedrijfstemperatuur	0° - +49°C (+32° - +120°F)

Eigenschappen

Afmetingen print	59.5 mm x 108 mm x 16 mm (2.19 in x 4.25 in x 0.629 in)
------------------	---

Vereiste voeding

Stroomverbruik (maximum)	100 mA max.
Spanning	12 VDC nominal

Connectoren

LAN/WAN	Modulaire RJ-45-poort (Ethernet)
---------	----------------------------------

Bekabeling

Ethernet-kabel	UTP-kabel van categorie 5 (of beter)
Lengte Ethernet-kabel	Max. lengte 100 m (328 ft)

Bekabeling

Draaddikte databus	18 AWG of 22 AWG
Draadlengte databus	Maximale afstand – draaddikte : 150 m (500 ft) - 0.65 mm (22 AWG) 300 m (1000 ft) - 1.02 mm (18 AWG)

Browserondersteuning

Microsoft Internet Explorer (Microsoft Windows 7 en hoger)

Mozilla Firefox

7.2 Compatibiliteit

Compatibele inbraakcentrales

AMAX 2000/2100/3000/4000

B9512G/B9512G-E

B8512G/B8512G-E

B6512

B5512/B5512E

B4512/B4512E

B3512/B3512E

D9412GV4/D7412GV4/D7212GV4

D9412GV3/D7412GV3/D7212GV3

D9412GV2/D7412GV2/D7212GV2 versie 7.06 of hoger

DS7220 versie 2.10 of hoger
DS7240 versie 2.10 of hoger
DS7400XiV4 versie 4.10 of hoger
Easy Series V3+
FPD-7024
Solution 2000/3000

8 Appendix

Dit gedeelte bevat gedetailleerde instructies voor hostnamen en IP-adressen van de module.

8.1 Module Hostname

De hostnaam van een module bepalen:

In de standaard fabrieksinstelling van de module kan de DHCP-server een IP-adres toewijzen. Een standaard hostnaam op basis van het MAC-adres wordt door de DHCP-server geregistreerd als de module niet op een specifieke hostnaam is geregistreerd. U kunt de hostnaam alleen gebruiken voor modules die zijn geconfigureerd voor dynamische DHCP of statische IP-adressen. Hostnamen kunnen niet worden gebruikt wanneer er een directe verbinding tot stand wordt gebracht met behulp van AutoIP. De standaard hostnaam van de module bestaat uit de letter B, gevolgd door de laatste zes alfanumerieke tekens van het bijbehorende MAC-adres (bijvoorbeeld, B3F603F).

8.2 IP-adres van module

Om het IP-adres van de module (de positie van de adresschakelaar is niet relevant) te bepalen, is een van de volgende procedures nodig:

- *DHCP gebruiken om het IP-adres van een met het netwerk verbonden module op te zoeken, Pagina 36.*
- *Gebruik een SDI/SDI2-bedieningspaneel om het IP-adres van een module te achterhalen, Pagina 36. (alleen B9512G/B8512G, B6512/B5512/B4512/B3512 en GV4.)*
- *Auto IP met een rechtstreeks aangesloten module gebruiken, Pagina 37. Binnen 60 seconden wijst de B426 tijdelijk adres 169.254.1.1 toe voor configuratie.*



Aanwijzing!

Voor externe toegang is het publieke IP-adres nodig en poorttoewijzing van de gateway.

8.2.1 DHCP gebruiken om het IP-adres van een met het netwerk verbonden module op te zoeken

Als de module met een netwerk is verbonden, wijst een DHCP-server (Dynamic Host Configuration Protocol) het IP-adres toe aan de module.

Het IP-adres opzoeken op de DHCP server:

1. Log in op de DHCP-server.
2. Ga naar de IP-tabel op de DHCP-server.
3. Gebruik het MAC-adres dat is toegewezen aan de module (weergegeven op het label op de Ethernet RJ-45-poort), om het IP-adres te vinden dat aan de module is toegewezen.

8.2.2 Gebruik een SDI/SDI2-bedieningspaneel om het IP-adres van een module te achterhalen

Als de module is aangesloten op een B9512G/B8512G, B6512/B5512/B4512/B3512 of GV4 inbraakcentrale, kunt u een aangesloten bedieningspaneel gebruiken om het lokale (LAN) IP-adres op te zoeken.

Een IP-adres vinden met behulp van een SDI2 Bedieningspaneel (B920/B930-instructies):

1. Log met uw installateur-PIN in op een bedieningspaneel, ga daarna naar het [1] Installer menu.

2. Ga naar de menuoptie [3] Network > [1] B42x > [1] Settings. Het bedieningspaneel scrollt door de volgende sub-categorieën en geeft de programmering aan voor: hostnaam, IPv4-bron IP, IPv6-bron IP, MAC-adres.
3. Nadat u de informatie heeft bekeken, drukt u op [ESC] om het menu te verlaten.

Een IP-adres van de module vinden met behulp van een SDI2 Bedieningspaneel (D1255/D1260-instructies):

1. Druk op het bedieningspaneel op [9] [9] [ENTER] en druk vervolgens op [NEXT].
2. Druk in het Tools-menu op [ENTER]. Het bedieningspaneel vraagt nu om de installateurscode in te voeren.
3. Voer de installateurscode in en druk op [ENTER].
4. Ga naar IP-Diagnose > B420 Module (1-2) > menuoptie Instellingen en druk vervolgens tweemaal op [NEXT] om het IP-adres te openen.
5. Nadat u de informatie heeft bekeken, drukt u op [ESC] om het menu te verlaten.

8.2.3

Auto IP met een rechtstreeks aangesloten module gebruiken

Als de module rechtstreeks op een computer (laptop of PC) is aangesloten en niet op een netwerk (er is geen hub, router of switch aangesloten), kunt u de AutoIP van de module gebruiken. om de module aan te sluiten en te programmeren zonder dat het IP bekend is.



Aanwijzing!

Als u geen verbinding kunt maken met de AutoIP-optie, moet u mogelijk de configuratie van de webbrowser wijzigen, zodat er geen proxy-server wordt gebruikt. Zorg er ook voor dat de computer AutoIP heeft ingeschakeld. Raadpleeg de online helpfunctie van de browser voor instructies met betrekking tot het uitschakelen van de proxy-service.

Als het IP-adres van de module niet wordt opgenomen in de ARP-tabel van de hostcomputer en u het adres niet kent, volgt u onderstaande stappen.

De AutoIP gebruiken:

1. Verwijder de spanning van het module.
2. Koppel de module los van het netwerk.
3. Sluit de B426 rechtstreeks aan op de Ethernet-poort van de computer, schakel deze in en wacht 60 sec. Als de AutoIP-service op uw computer is ingeschakeld, wordt er nu een 169.254.XXX.XXX-adres aan uw computer toegewezen.
4. Open een internetbrowser (Microsoft Internet Explorer 6 of hoger, of Mozilla Firefox 3 of hoger) en voer het standaard AutoIP-adres in voor de B426: **169.254.1.1**, en druk op [Enter].
5. Voer het wachtwoord in (het standaard wachtwoord is B42V2) en klik op **Login**. De pagina **Device Information** wordt geopend.

Als AutoIP niet werkt op de hostcomputer, is er mogelijk een nieuwe registry key nodig om AutoIP in te schakelen. Zorg ervoor dat u toestemming hebt van de IT-afdeling van het bedrijf voordat u de registry wijzigt.

Om AutoIP op uw computer in te schakelen met behulp van een nieuwe registry key:

1. Open Notepad maak een nieuw bestand aan met de naam **AutoIP.reg**.
2. In Notepad voert u de volgende tekst in:


```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters]
"IPAutoconfigurationEnabled"=dword:00000001
```

3. Sla het bestand op een makkelijk terug te vinden locatie op de hostcomputer op.
4. Ga naar het opgeslagen bestand en klik er tweemaal op om deze aan de registry van de hostcomputer toe te voegen.
5. Start de hostcomputer opnieuw op.

Bosch Security Systems, Inc.

130 Perinton Parkway
Fairport, NY 14450
USA

www.boschsecurity.com

© Bosch Security Systems, Inc., 2016

Bosch Sicherheitssysteme GmbH

Robert-Bosch-Ring 5
85630 Grasbrunn
Germany