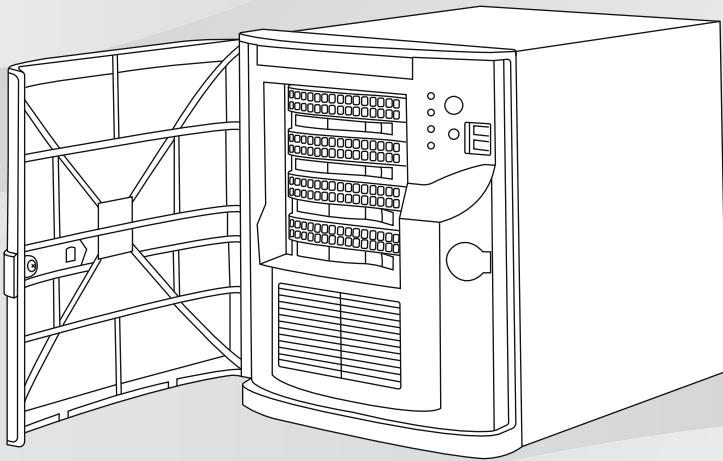




**BOSCH**

## **DIVAR IP all-in-one 5000**

DIP-5240IG-00N | DIP-5244IG-4HD | DIP-5248IG-4HD |  
DIP-524CIG-4HD | DIP-5240GP-00N | DIP-5244GP-4HD |  
DIP-5248GP-4HD | DIP-524CGP-4HD



nl

Installatiehandleiding



---

# Inhoudsopgave

1	<b>Veiligheidsmaatregelen</b>	<b>5</b>
1.1	Algemene veiligheidsmaatregelen	5
1.2	Veiligheidsmaatregelen voor elektriciteit	8
1.3	ESD-voorzorgsmaatregelen	9
1.4	Voorzorgmaatregelen voor bedrijf	10
1.5	Voorzorgsmaatregelen voor gegevensbeveiliging	11
2	<b>Inleiding</b>	<b>12</b>
2.1	Meegeleverde onderdelen	12
2.2	Productregistratie	12
3	<b>Systeemoverzicht</b>	<b>13</b>
3.1	Aanzichten van het apparaat	13
3.2	Elementen van bedieningspaneel	16
4	<b>Een harde schijf installeren</b>	<b>18</b>
4.1	Een harde-schijfdrager verwijderen uit een harde-schijfcompartiment	19
4.2	Een harde schijf installeren in een harde-schijfdrager	20
4.3	Een harde-schijfdrager installeren in een harde-schijfcompartiment	22
5	<b>Systeemconfiguratie</b>	<b>22</b>
5.1	Standaardinstellingen	22
5.2	Vereisten	23
5.3	Bedieningsmodi	23
5.4	Harde schijven voorbereiden voor video-opname	24
5.5	De toepassing starten	25
5.5.1	Gebruik als volledig video-opname- en beheersysteem	27
5.5.2	Gebruik als puur voor video-opnamen bestemd systeem	27
5.5.3	Gebruik als iSCSI-opslaguitbreiding	28
5.6	De configuratiewizard van BVMS gebruiken	28
5.7	Extra licenties toevoegen	29
5.8	BVMS Operator Client gebruiken	30
6	<b>Externe verbinding met het systeem</b>	<b>31</b>
6.1	Het systeem beschermen tegen onbevoegde toegang	31
6.2	Het doorsturen van poorten instellen	32
6.3	Een geschikte client kiezen	32

---

6.3.1	Externe verbinding met Operator Client	32
6.3.2	Externe verbinding met de Video Security-app	33
7	<b>Onderhoud</b>	<b>33</b>
7.1	Systeembewaking	33
7.2	Het apparaat herstellen	34
7.3	Onderhoud en reparatie	35
8	<b>Meer informatie</b>	<b>36</b>
8.1	Aanvullende documentatie en clientsoftware	36
8.2	Ondersteuningsservices en Bosch Academy	36

# 1 Veiligheidsmaatregelen

Houd u aan de veiligheidsmaatregelen in dit hoofdstuk.

## 1.1 Algemene veiligheidsmaatregelen

Volg onderstaande maatregelen om de algemene veiligheid te waarborgen:

- Houd de omgeving rond het systeem schoon en vrij van rommel.
- Plaats het bovenpaneel van het chassis en eventuele systeemcomponenten die zijn verwijderd uit de buurt van het systeem of op een tafel, zodat er niet per ongeluk op kan worden getrapt.
- Draag bij het werken met het systeem geen losse kleding zoals stropdassen en losgeknoopte mouwen. Losse kleding kan in aanraking komen met elektrische circuits of in een koelventilator worden getrokken.
- Draag geen sieraden of metalen voorwerpen op uw lichaam. Dit zijn uitstekende metaalgeleiders die kortsluiting kunnen veroorzaken en u kunnen verwonden wanneer ze in contact komen met printplaten of plaatsen waar spanning aanwezig is.

---

### Waarschuwing!

Onderbrekingen van netvoeding:

Er wordt onmiddellijk spanning geleverd wanneer de stekker in het stopcontact wordt gestoken.



Voor toestellen met een hoofdschakelaar is het apparaat echter alleen gereed voor gebruik wanneer de hoofdschakelaar (ON/OFF) in de stand ON staat. Wanneer de stekker uit het stopcontact wordt getrokken, wordt de voedingsspanning naar het apparaat volledig onderbroken.

---

---

**Waarschuwing!**

Behuizing verwijderen:

Om elektrische schokken te voorkomen mag de behuizing alleen worden verwijderd door gekwalificeerd onderhoudspersoneel.

Alvorens de behuizing te verwijderen moet de stekker altijd uit het stopcontact worden getrokken en losgekoppeld blijven zolang de behuizing is verwijderd. Onderhoudswerkzaamheden mogen alleen worden uitgevoerd door gekwalificeerd onderhoudspersoneel. De gebruiker mag geen reparaties uitvoeren.



---

**Waarschuwing!**

Voedingskabel en AC-adapter:

Gebruik bij het installeren van het product de meegeleverde of voorgeschreven aansluitkabels, voedingskabels en AC-adapters.

Het gebruik van andere kabels en adapters kan een storing of brand veroorzaken. De wet inzake de veiligheid van elektrische apparatuur en elektrisch materiaal verbiedt het gebruik van UL- of CSA-gecertificeerde kabels (met UL/CSA in de code) voor alle andere elektrische apparaten.



---

**Waarschuwing!**

Lithiumbatterij:

Incorrect geplaatste batterijen kunnen leiden tot een explosie. Vervang lege batterijen altijd door batterijen van hetzelfde type of een door de fabrikant aanbevolen gelijkwaardig type.

Gebruikte batterijen moeten zorgvuldig worden behandeld. De batterij mag op generlei wijze worden beschadigd. Bij een beschadigde batterij kunnen stoffen vrijkomen die schadelijk zijn voor het milieu.

Voer lege batterijen af volgens de voorschriften van de fabrikant of plaatselijke richtlijnen.



**Waarschuwing!**

Wanneer u het loodhoudende soldeermateriaal dat in dit product wordt gebruikt hanteert, kunt u worden blootgesteld aan lood. Dit is een chemisch element waarvan bij de Staat van Californië bekend is dat het geboorteafwijkingen en voortplantingsproblemen kan veroorzaken.

**Bericht!**

Apparaat dat gevoelig is voor statische elektriciteit: Om elektrostatische ontlading te voorkomen, moeten de CMOS/MOSFET veiligheidsmaatregelen correct worden uitgevoerd.

Draag gearde polsbanden en volg de juiste ESD-veiligheidsvoorschriften wanneer u in aanraking komt met de printplaten die gevoelig zijn voor statische elektriciteit.

**Bericht!**

De installatie mag alleen worden uitgevoerd door gekwalificeerd onderhoudspersoneel in overeenstemming met de geldende elektrische voorschriften.

**Bericht!**

Het besturingssysteem bevat de nieuwste Windows-beveiligingspatches die beschikbaar waren op het moment dat de software-image werd gemaakt. Wij raden u aan regelmatig de nieuwste beveiligingspatches te installeren met de Windows Update-functie.

**Afvalverwerking**

Uw Bosch-product is ontworpen en vervaardigd met materialen van hoge kwaliteit en componenten die opnieuw kunnen worden gebruikt.

Dit symbool geeft aan dat elektronische en elektrische apparatuur die het einde van de levensduur heeft bereikt, apart dient te worden ingezameld en gescheiden van het huishoudelijk afval moet worden afgevoerd.

Er bestaan in de EU reeds gescheiden inzamelsystemen voor gebruikte elektrotechnische en elektronische producten. Lever deze apparatuur in bij een plaatselijk afvalverzamelpunt of bij een verzamelpunt voor recycling.

## 1.2 Veiligheidsmaatregelen voor elektriciteit

De volgende basisveiligheidsmaatregelen voor elektriciteit moeten worden getroffen om persoonlijk letsel en schade aan het systeem te voorkomen:

- Houd rekening met de locatie van de aan/uit-schakelaar op het chassis en met de locaties van de noodstop-schakelaar, de afsluitschakelaar of het stopcontact in de ruimte. Bij een ongeval met de elektriciteit kunt u dan snel de voeding van het systeem loskoppelen.
- Werk nooit alleen met hoogspanningscomponenten.
- Koppel de netsnoeren los voordat u enige onderdelen installeert in of verwijdert uit de computer, inclusief de backplane.
- Schakel bij het loskoppelen van de voeding eerst het systeem uit en ontkoppel daarna de netsnoeren van alle voedingsmodules in het systeem.
- Bij het werken rond blootliggende elektrische circuits moet een andere persoon die bekend is met de uitschakelementen van de voeding in de buurt zijn om indien nodig de voeding uit te schakelen.
- Gebruik slechts één hand bij het werken aan elektrische apparatuur die is ingeschakeld. Zo voorkomt u dat er een volledig circuit wordt gevormd, wat een elektrische schok veroorzaakt. Wees uiterst voorzichtig met het gebruik van metalen gereedschappen, die elektrische componenten of printplaten waarmee ze in contact komen snel kunnen beschadigen.



- De netsnoeren moeten een aardingsstekker hebben en worden aangesloten op geaarde stopcontacten. Het apparaat beschikt over meerdere netsnoeren. Ontkoppel beide netsnoeren voordat er onderhoudswerkzaamheden worden uitgevoerd, om elektrische schokken te voorkomen.
- Vervangbare gesoldeerde zekeringen van moederbord: zelfherstellende PTC-zekeringen (Positive Temperature Coefficient) op het moederbord mogen alleen worden vervangen door geschoolde onderhoudsmonteurs. De nieuwe zekering moet gelijk of gelijkwaardig zijn aan de te vervangen zekering. Neem contact op met de technische ondersteuning voor meer informatie en ondersteuning.

---

### **Voorzichtig!**



Batterij van moederbord: Er bestaat gevaar voor explosie als de batterij op de kaart verkeerd om wordt geplaatst, waardoor ompoling ontstaat. Vervang deze batterij uitsluitend door een batterij van hetzelfde type of een vergelijkbaar type dat wordt aanbevolen door de fabrikant (CR2032). Voer lege batterijen af volgens de voorschriften van de fabrikant.

---

## **1.3 ESD-voorzorgsmaatregelen**

Elektrostatische ontlading (ESD) wordt gegenereerd door twee objecten met verschillende elektrische ladingen die met elkaar in contact komen. Een elektrische ontlading wordt gegenereerd om dit verschil te neutraliseren. Zo'n ontlading kan schade toebrengen aan elektronische componenten en printplaten. De volgende maatregelen zijn in het algemeen afdoende om dit verschil te neutraliseren voordat er contact wordt gemaakt om uw apparatuur te beveiligen tegen ESD:

- Gebruik geen matten die zijn bedoeld om elektrostatische ontlading te verminderen als beveiliging tegen elektrische schokken. Gebruik in plaats daarvan rubbermatten die specifiek zijn bedoeld als isolatie tegen elektriciteit.

- Gebruik een geaarde polsband die is bedoeld om statische ontlading te voorkomen.
- Laat alle componenten en printplaten (PCB's) in hun antistatische verpakking totdat ze worden gebruikt.
- Raak een geaard metalen voorwerp aan alvorens een printplaat uit zijn antistatische verpakking te halen.
- Laat geen componenten of printplaten in contact komen met uw kleding, die een lading kan bevatten, zelfs wanneer u een polsband draagt.
- Pak een printplaat uitsluitend aan de randen vast. Raak de componenten, chips, geheugenmodules of contacten niet aan.
- Raak bij het hanteren van chips of modules de pinnen ervan niet aan.
- Berg het moederbord en randapparatuur op in hun antistatische verpakking wanneer ze niet worden gebruikt.
- Zorg er met het oog op de aarding voor dat het computerchassis een optimale geleiding heeft tussen de voeding, de behuizing, de montagebevestigingen en het moederbord.

## 1.4 Voorzorgmaatregelen voor bedrijf

### Bericht!



Als het systeem in bedrijf is, moet het chassispaneel zijn geplaatst om te zorgen voor voldoende koeling.

Als deze instructie niet strikt wordt opgevolgd, kan schade aan het systeem ontstaan die niet door de garantie wordt gedekt.

### Bericht!



Gebruikte batterijen moeten zorgvuldig worden behandeld. De batterij mag op generlei wijze worden beschadigd. Bij een beschadigde batterij kunnen stoffen vrijkomen die schadelijk zijn voor het milieu. Gooi een gebruikte batterij niet bij het huisvuil of op een openbare vuilstort. Lever gebruikte batterijen in volgens de geldende milieuvoorschriften.

**Waarschuwing!**

Wees voorzichtig wanneer u rond de backplane werkzaamheden of onderhoud uitvoert. Wanneer het systeem in bedrijf is, is gevaarlijke spanning of energie aanwezig op de backplane. Raak de backplane niet met een metalen object aan en zorg dat de lintkabels de backplane niet raken.

## 1.5 Voorzorgsmaatregelen voor gegevensbeveiliging

Houd uit het oogpunt van gegevensbeveiliging rekening met het volgende:

- Beperk fysieke toegang tot het systeem tot uitsluitend geautoriseerd personeel. Het wordt ten zeerste aangeraden het systeem in een gebied met toegangscontrolebeveiliging te plaatsen om fysieke manipulatie van het systeem te vermijden.
- Voor de installatie van beveiligingsupdates van het besturingssysteem kan de online updatefunctionaliteit van Windows worden gebruikt of de overeenkomstige maandelijkse roll-up patches voor offline-installatie.
- Het wordt nadrukkelijk aanbevolen lokale netwerktoegang te beperken tot vertrouwde apparaten. Meer informatie hierover vindt u in de Technische opmerking Netwerkverificatie 802.1X en in het Bosch IP Video and Data Security Guidebook (Bosch IP Handboek voor video- en gegevensbeveiliging), dat beschikbaar is in de online productcatalogus.
- Gebruik voor toegang via openbare netwerken alleen de beveiligde (gecodeerde) communicatiekanalen.

**Raadpleeg**

- *Externe verbinding met het systeem, pagina 31*

## 2 Inleiding

Lees en volg de veiligheidsinstructies voordat u begint met de installatie.

### 2.1 Meegeleverde onderdelen

Controleer of alle onderdelen meegeleverd en onbeschadigd zijn. Als de verpakking of enige onderdelen beschadigd zijn, geeft u dit door aan de expediteur. Als er onderdelen ontbreken, neemt u contact op met de vertegenwoordiger of klantenservice van Bosch Security Systems.

Aantal	Component
1	DIVAR IP all-in-one 5000
1	Installatiehandleiding
1	Netsnoer EU
1	Netsnoer VS
2	Sleutels

### 2.2 Productregistratie

Registreer uw product:

<https://www.boschsecurity.com/product-registration/>



## 3 Systeemoverzicht

Het DIVAR IP all-in-one 5000 systeem is een gebruiksvriendelijke alles-in-één-oplossing voor het opnemen, weergeven en beheren van netwerkbewakingssystemen.

DIVAR IP all-in-one 5000 is een intelligent IP-opslagapparaat dat geen afzonderlijke NVR-server (Network Video Recorder) en opslaghardware nodig heeft en waarop de volledige BVMS (BVMS)-oplossing wordt uitgevoerd op basis van Bosch Video Recording Manager (VRM) inclusief de Bosch Video Streaming Gateway (VSG) voor de integratie van camera's van derden.

BVMS beheert al uw IP- en digitale video, audio en beveiligingsgegevens in het IP-netwerk. Bosch VMS combineert naadloos IP-camera's en encoders en zorgt voor gebeurtenis- en alarmbeheer in het hele systeem, systeemstatusbewaking en gebruikers- en prioriteitenbeheer.

DIVAR IP all-in-one 5000 is een minitower-unit met 4 opslagcompartimenten die beschikt over verwisselbare harde SATA-schijven aan de voorzijde.

Het systeem is eenvoudig te installeren en te bedienen. Alle systeemsoftware is vooraf geïnstalleerd, zodat het videobeheersysteem direct klaar is voor gebruik.

De DIVAR IP all-in-one 5000 maakt gebruik van het besturingssysteem Windows Storage Server 2016.

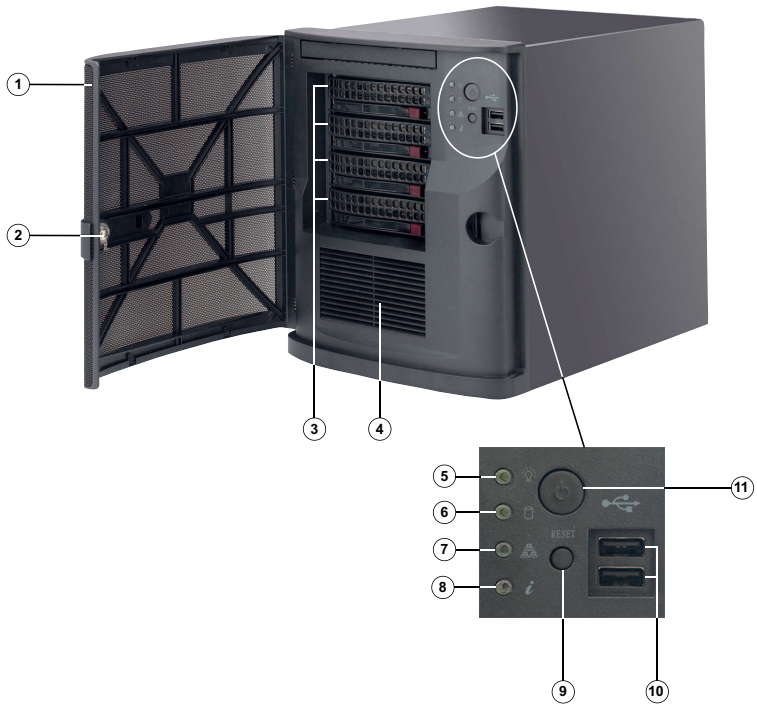
### 3.1 Aanzichten van het apparaat

Het DIVAR IP all-in-one 5000-systeem heeft een compact minitower-chassis. Het heeft een scharnierend frontpaneel waarachter de harde schijven en het bedieningspaneel verborgen zijn.

Het bedieningspaneel aan de voorzijde bevat aan/uit-knoppen en LED's voor statuscontrole.

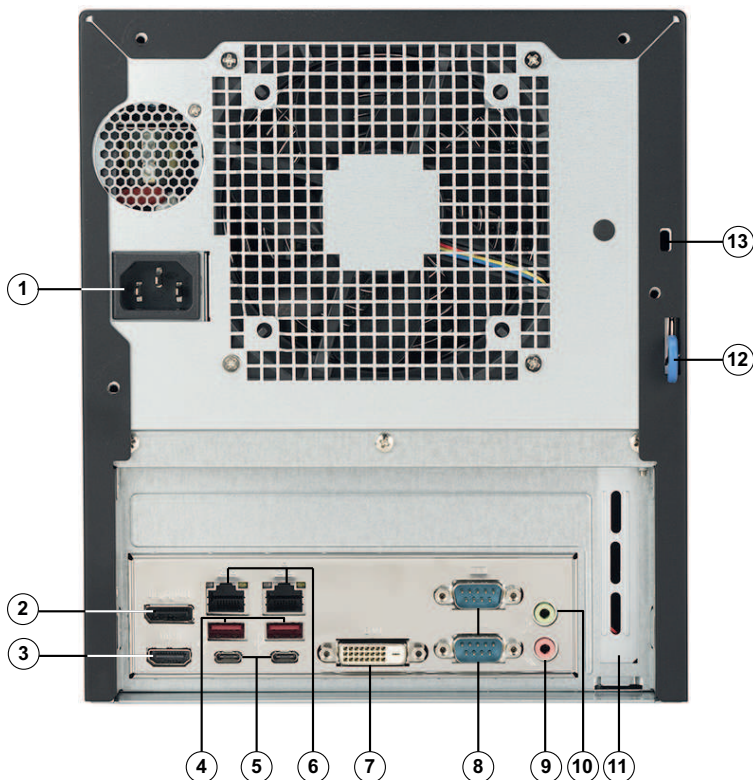
Aan de achterzijde zijn verschillende I/O-poorten ondergebracht.

## Vooraanzicht



1	Frontpaneel	2	Vergrendeling frontpaneel
3	4 poorten voor harde schijven (voor harde schijven van 3,5 inch)	4	Luchtinlaatfilter
5	Aan/uit-LED	6	HDD-LED (niet gebruikt)
7	Netwerk-LED	8	Informatie-LED
9	Resetknop	10	2 USB 2.0-poorten
11	Aan/uit-knop		

### Achteraanzicht




1	Netaansluiting	2	DisplayPort poort
3	HDMI 2.0-poort	4	2 USB 3.1-poorten (type A)
5	2 USB 3.1-poorten (type C)	6	2 LAN-poorten (RJ45), gekoppeld via teaming <b>Opmerking:</b> wijzig de teaming-modus niet!
7	DVI-D-poort	8	2 COM-poorten
9	Audio-microfooningang	10	Audio-lijnuitgang

11	<p>Extra GPU-kaart met 4 Mini DisplayPort-poorten (in dit geval moeten de Mini DisplayPort-poorten worden gebruikt voor het aansluiten van een of meer monitoren).</p> <p><b>Opmerking:</b> alleen beschikbaar voor DIP-5240GP-00N, DIP-5244GP-4HD, DIP-5248GP-4HD en DIP-524CGP-4HD.</p>	12	<p>Vergrendelingsbeugel (compatibel met uiteenlopende algemeen verkrijgbare sloten).</p> <p><b>Opmerking:</b> sloten zijn niet inbegrepen.</p>
13	<p>Kensington-beveiligingssleuf (voor een standaard Kensington-slot).</p> <p><b>Opmerking:</b> Kensington-slot is niet inbegrepen.</p>		


## 3.2 Elementen van bedieningspaneel

Het bedieningspaneel aan de voorzijde van het chassis bevat aan/uit-knoppen en LED's voor statuscontrole.





### Knoppen van het bedieningspaneel

Knop	Beschrijving
 <b>Voeding</b>	<p>Met de aan/uit-knop wordt de stroom van de voedingseenheid naar het systeem in- of uitgeschakeld.</p> <p><b>Opmerking:</b> als de systeemvoeding met deze knop wordt uitgeschakeld, wordt de hoofdvoeding uitgeschakeld maar wordt er nog wel standbyvoeding aan het systeem geleverd.</p>



Knop	Beschrijving
	<b>Om het systeem compleet spanningsloos te maken haalt u de stekker van het systeem uit het stopcontact voordat u onderhoudstaken verricht.</b>
 <b>Reset</b>	De resetknop dient om het systeem opnieuw op te starten.

### LED's op het bedieningspaneel

LED	Beschrijving				
 <b>Voeding</b>	Deze LED geeft aan dat er voeding wordt geleverd aan de voedingseenheden van het systeem. Normaal moet deze LED branden als het systeem in werking is.				
 <b>HDD</b>	Deze LED wordt niet gebruikt.				
 <b>Netwerk</b>	Wanneer deze LED knippert, geeft dit netwerkactiviteit aan.				
 <b>Informatie</b>	Deze LED geeft de systeemstatus aan.				
	<table border="1"> <thead> <tr> <th data-bbox="364 1169 628 1209">Systeemstatus</th> <th data-bbox="628 1169 974 1209">Beschrijving</th> </tr> </thead> <tbody> <tr> <td data-bbox="364 1209 628 1361">Continu aan en rood</td> <td data-bbox="628 1209 974 1361">Het systeem is oververhit. (Dit kan worden veroorzaakt door te hoge kabeldichtheid.)</td> </tr> </tbody> </table>	Systeemstatus	Beschrijving	Continu aan en rood	Het systeem is oververhit. (Dit kan worden veroorzaakt door te hoge kabeldichtheid.)
Systeemstatus	Beschrijving				
Continu aan en rood	Het systeem is oververhit. (Dit kan worden veroorzaakt door te hoge kabeldichtheid.)				

LED	Beschrijving	
	Knipperend rood (1 Hz)	Ventilatorstoring: controleer op een niet-werkende ventilator.
	Knipperend rood (0,25 Hz)	Stroomstoring: controleer op een niet-werkende voeding.
	Continu blauw	Lokale UID is geactiveerd. Gebruik deze functie om de eenheid te zoeken in een rekomgeving.
	Knipperend blauw (300 msec)	Externe UID is geactiveerd. Gebruik deze functie om de eenheid te zoeken vanaf een externe locatie.

## 4 Een harde schijf installeren

Het DIVAR IP all-in-one 5000-systeem beschikt over vier tijdens bedrijf aan de voorkant verwisselbare harde schijven. De harde schijven worden bevestigd in harde-schijfdragers om de installatie in en verwijdering uit het chassis te vergemakkelijken. Deze harde-schijfdragers zorgen tevens voor een goede luchtstroming voor de harde-schijfeenheden.

### Procedure

Voor het installeren van een harde schijf, moeten de volgende stappen worden uitgevoerd:

1. *Een harde-schijfdrager verwijderen uit een harde-schijfcompartiment, pagina 19*
2. *Een harde schijf installeren in een harde-schijfdrager, pagina 20*
3. *Een harde-schijfdrager installeren in een harde-schijfcompartiment, pagina 22*

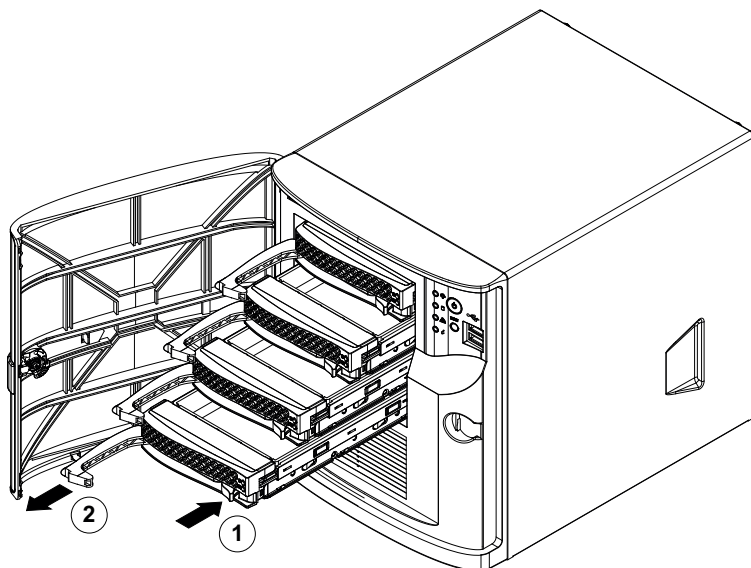
**Bericht!**

Lees de waarschuwingen en voorzorgsmaatregelen die staan beschreven in deze handleiding alvorens werkzaamheden te verrichten aan het chassis.

## 4.1 Een harde-schijfdrager verwijderen uit een harde-schijfcompartiment

### Een harde-schijfdrager verwijderen uit een harde-schijfcompartiment:

1. Ontgrendel het voorpaneel en open het.
2. Druk op de ontgrendelknop aan de rechterzijde van de harde-schijfdrager. Hierdoor komt de hendel van de harde-schijfdrager naar buiten.
3. Druk de harde-schijfdrager met behulp van de hendel uit het chassis.



1	Ontgrendelknop	2	Hendel van harde-schijfdrager
---	----------------	---	-------------------------------

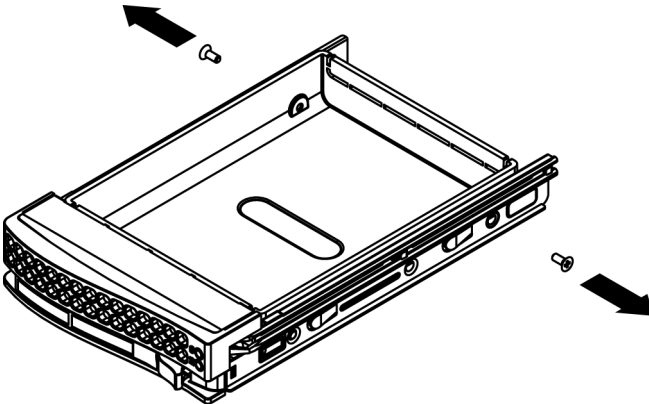
**Bericht!**

Schakel de eenheid niet in wanneer de harde-schijfdragers verwijderd zijn uit de compartimenten.

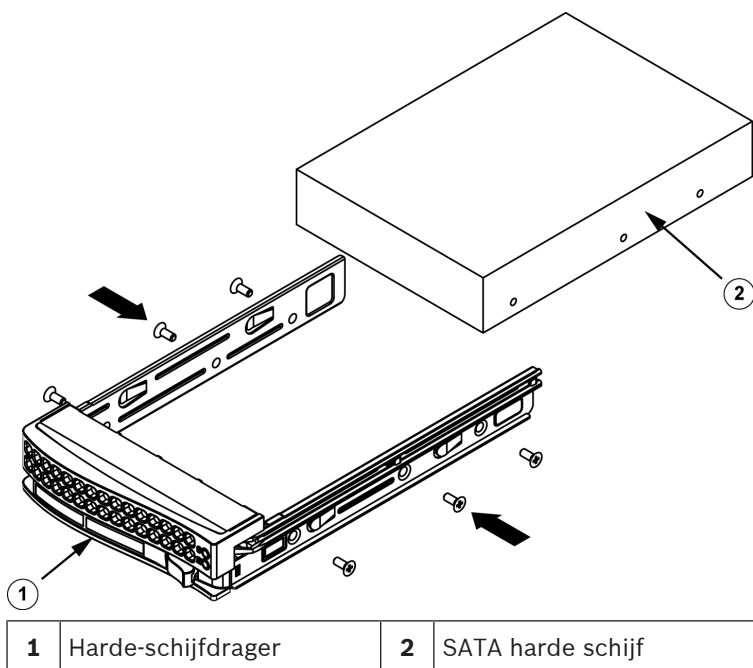
## 4.2 Een harde schijf installeren in een harde-schijfdrager

### Een harde schijf installeren in een harde-schijfdrager:

1. Verwijder de schroeven waarmee de dummy-schijf is bevestigd aan de harde-schijfdrager.



2. Verwijder de dummy-schijf uit de harde-schijfdrager en plaats de harde-schijfdrager op een vlakke ondergrond.
3. Schuif een nieuwe harde schijf in de harde-schijfdrager met de zijde van de printplaat naar beneden gericht.
4. Lijn de montagegaten in de harde-schijfdrager en de harde schijf uit.
5. Bevestig de harde schijf op de harde-schijfdrager met de zes schroeven.

**Bericht!**

Bosch raadt het gebruik van de bijbehorende harde schijven van Bosch aan. De harde schijven zijn zeer belangrijke componenten en worden zorgvuldig geselecteerd door Bosch op basis van beschikbare faalpercentages. Harde-schijfstations die niet door Bosch worden geleverd, worden niet ondersteund. Meer informatie over ondersteunde harde-schijfstations vindt u in het gegevensblad in de online productcatalogus van Bosch op:

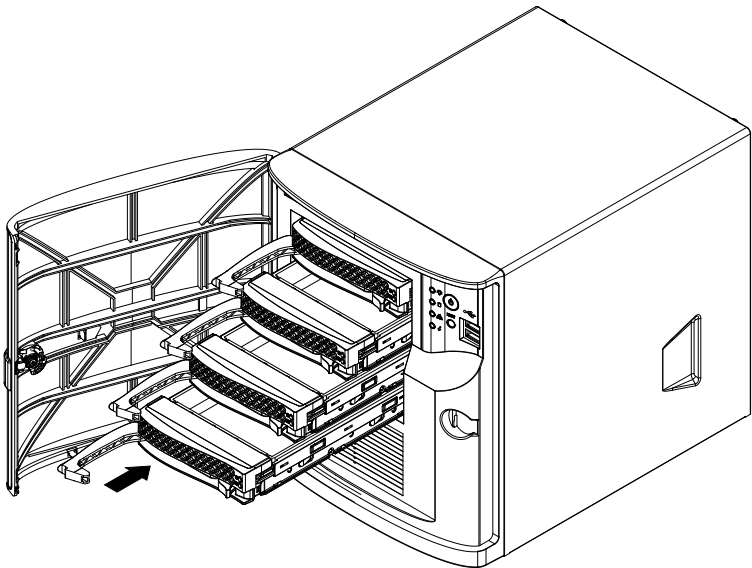
[www.boschsecurity.com](http://www.boschsecurity.com)



## 4.3 Een harde-schijfdrager installeren in een harde-schijfcompartiment

### Een harde-schijfdrager installeren in een harde-schijfcompartiment:

1. Plaats de harde-schijfdrager horizontaal in het harde-schijfcompartiment, waarbij u erop let dat de ontgrendelknop van de harde-schijfdrager zich aan de rechterzijde bevindt.
2. Druk de harde-schijfdrager in het compartiment tot de hendel wordt ingetrokken en de harde-schijfdrager op zijn plaats vastklikt.
3. Sluit het voorpaneel en vergrendel het.



## 5 Systeemconfiguratie

### 5.1 Standaardinstellingen

DIVAR IP systemen worden geleverd met een in de fabriek geïnstalleerde configuratie-wizard.

Alle DIVAR IP-systemen zijn vooraf geconfigureerd met een standaard IP-adres en standaard iSCSI-instellingen:

- IP-adres: automatisch toegewezen door DHCP (fallback-IP-adres: 192.168.0.200).
- Subnetmasker: automatisch toegewezen door DHCP (fallback-subnetmasker: 255.255.255.0).

#### **Standaard gebruikersinstellingen voor beheerdersaccount**

- Gebruiker: BVRAdmin
- Wachtwoord: WSS4Bosch

## 5.2 Vereisten

Houd rekening met het volgende:

- DIVAR IP moet een actieve netwerkverbinding hebben tijdens de installatie. Zorg ervoor dat de netwerkswitch waarmee u verbinding maakt, is ingeschakeld.
- Het standaard IP-adres mag niet worden gebruikt door andere apparaten in het netwerk. Verzeker u ervan dat de standaard IP-adressen van bestaande DIVAR IP-systemen in het netwerk worden gewijzigd voordat u nog een DIVAR IP toevoegt.
- Bepaal of de eerste installatie op een DHCP-netwerk wordt uitgevoerd. Indien dit niet het geval is, moet u geldige IP-adressen toewijzen aan de videoapparaten. Raadpleeg uw plaatselijke IT-beheerder voor een geldig IP-adresbereik voor gebruik met DIVAR IP en bijbehorende apparaten.
- De standaard iSCSI-instellingen zijn geoptimaliseerd voor gebruik met VRM.

## 5.3 Bedieningsmodi

### **Bedieningsmodi**

De DIVAR IP all-in-one-systemen kunnen in drie verschillende modi werken:

- Volledig video-opname- en beheersysteem, dat gebruikmaakt van de kerncomponenten en -services van BVMS en VRM: deze modus biedt geavanceerde videobeheerfuncties zoals gebeurtenis- en alarmfuncties.
- Puur voor video-opnamen bestemd systeem, dat gebruikmaakt van de kerncomponenten en -services van VRM.
- iSCSI-opslaguitbreiding voor een BVMS- of VRM-systeem, dat op verschillende hardware wordt uitgevoerd.

**Bericht!**

Opgenomen videostreams moeten zodanig worden geconfigureerd dat de maximale bandbreedte van het systeem (BVMS-/VRM-basisstelsysteem plus iSCSI-opslaguitbreidingen) niet wordt overschreden.

## 5.4 Harde schijven voorbereiden voor video-opname

Systemen die af fabriek worden geleverd met harde schijven, zijn meteen gereed voor opname.

Harde schijven die zijn toegevoegd aan een leeg systeem moeten worden voorbereid (geformatteerd) voordat ze kunnen worden gebruikt voor video-opnamen.

**Voor het formatteren van een harde schijf hebt u de volgende opties:**

- Uitvoeren van de aanvankelijke fabrieksconfiguratie: zie *Het apparaat herstellen, pagina 34*.
- Het formatteringsscript uitvoeren.

**Het formatteringsscript uitvoeren**

Om het formatteringsscript uit te kunnen voeren, moet u zich aanmelden met het beheerdersaccount (BVRAdmin).

1. Start het systeem op.
2. Druk in het standaardscherm van BVMS op CTRL+ALT+DEL.



3. Houd SHIFT ingedrukt, klik op **Andere gebruiker** en houd SHIFT ongeveer vijf seconden ingedrukt.
4. Voer de gebruikersnaam en het wachtwoord van de beheerder in.
5. Klik op het bureaublad in de map **Tools** met de rechtermuisknop op het script **Format\_data\_hard\_drives** en klik vervolgens op **Als administrator uitvoeren**.
6. Volg de instructies.
7. Na het formatteren kunt u het opslagmedium toevoegen aan de configuratie voor videobeheer.

**Bericht!**

Wanneer u een harde schijf formateert, worden alle bestaande gegevens op de harde schijf verwijderd.

## 5.5 De toepassing starten

De toepassing biedt een eenvoudig te installeren en intuïtief te gebruiken oplossing voor netwerkbewakingssystemen.

**Start de toepassing als volgt:**

1. Sluit de eenheid en de camera's op het netwerk aan.
2. Schakel het apparaat in.  
Het Windows Storage Server 2016-installatieproces wordt gestart.
3. Selecteer de gewenste taal voor de installatie en klik vervolgens op **Volgende**.
4. In de lijsten **Land of regio**, **Tijd en valuta** en **Toetsenbordindeling**, klikt u op het juiste item en vervolgens op **Volgende**.  
De Microsoft Software License Terms en EULA (eindgebruikersovereenkomst) worden weergegeven.
5. Accepteer de licentievoorwaarden en klik vervolgens op **Start**. Windows wordt opnieuw gestart.
6. Nadat het opnieuw opstarten is voltooid, drukt u op CTRL +ALT+DELETE. De aanmeldpagina van Windows wordt weergegeven.

7. Voer het standaardwachtwoord **WSS4Bosch** in.
8. Als u het wachtwoord hebt ingevoerd, verschijnt de melding dat u het wachtwoord moet wijzigen voordat u zich voor de eerste keer aanmeldt. Klik voor een bevestiging op **OK**.
9. Wijzig het wachtwoord.  
Een serie scripts voert belangrijke insteltaken uit. Dit kan enkele minuten duren. Schakel de computer niet uit. Het standaardscherm van BVMS wordt weergegeven. Nu kunt u beslissen in welke modus u het systeem wilt gebruiken:
  - *Gebruik als volledig video-opname- en beheersysteem, pagina 27*
  - *Gebruik als puur voor video-opnamen bestemd systeem, pagina 27*
  - *Gebruik als iSCSI-opslaguitbreiding, pagina 28*

---

**Bericht!**

Als u het wachtwoord bent vergeten, moet er een systeemherstel worden uitgevoerd zoals beschreven in de installatiehandleiding. De configuratie moet opnieuw worden uitgevoerd of moet worden geïmporteerd.

---

**Bericht!**

We raden u dringend aan om geen instellingen van het besturingssysteem te wijzigen. Het wijzigen van de instellingen van het besturingssysteem kan leiden tot storingen in het systeem.


---

**Bericht!**

Om beheerderstaken uit te kunnen voeren, moet u zich aanmelden bij het beheerdersaccount.

### 5.5.1 Gebruik als volledig video-opname- en beheersysteem

**Ga als volgt te werk om het DIVAR IP-systeem te gebruiken als volledig video-opname- en -beheersysteem:**

1. Dubbelklik in het standaardscherm van BVMS op het BVMS Config Wizard-pictogram  om de Config Wizard te starten.  
De pagina **Welcome** wordt weergegeven.
2. Configureer het systeem met gebruikmaking van de Config Wizard.

#### **Raadpleeg**

- *De configuratiewizard van BVMS gebruiken, pagina 28*

### 5.5.2 Gebruik als puur voor video-opnamen bestemd systeem

Om het DIVAR IP-systeem te gebruiken als puur voor video-opnamen bestemd systeem, moet u zich aanmelden bij het beheerdersaccount (BVRAdmin) om de vereiste configuratiestappen uit te voeren.

1. Druk in het standaardscherm van BVMS op CTRL+ALT+DEL.
2. Houd SHIFT ingedrukt, klik op **Andere gebruiker** en houd SHIFT ongeveer vijf seconden ingedrukt.
3. Voer de gebruikersnaam en het wachtwoord van de beheerder in.
4. Klik op het bureaublad in de map **Tools** met de rechtermuisknop op het script **Disable\_BVMS** en klik vervolgens op **Als administrator uitvoeren**.
5. Configureer de Video Recording Manager (VRM) vanaf een extern systeem met gebruikmaking van BVMS Configuration Client of Configuration Manager.

### 5.5.3 Gebruik als iSCSI-opslaguitbreiding

Om het DIVAR IP-systeem te gebruiken als iSCSI-opslaguitbreiding, moet u zich aanmelden bij het beheerdersaccount (BVRAdmin) om de vereiste configuratiestappen uit te voeren.

1. Druk in het standaardscherm van BVMS op CTRL+ALT+DEL.
2. Houd SHIFT ingedrukt, klik op **Andere gebruiker** en houd SHIFT ongeveer vijf seconden ingedrukt.
3. Voer de gebruikersnaam en het wachtwoord van de beheerder in.
4. Klik op het bureaublad in de map **Tools** met de rechtermuisknop op het script **Disable\_BVMS\_and\_VRM** en klik vervolgens op **Als administrator uitvoeren**.
5. Voeg het systeem toe als iSCSI-opslaguitbreiding aan een externe BVMS- of VRM-server met gebruikmaking van BVMS Configuration Client of Configuration Manager.

## 5.6 De configuratiewizard van BVMS gebruiken

De Config Wizard is bedoeld voor een snelle en eenvoudige configuratie van kleinere systemen. Met de Config Wizard kunt u het volledige systeem configureren, waaronder VRM, het iSCSI-systeem, camera's, opnameprofielen en gebruikersgroepen. Gebruikersgroepen en hun rechten worden automatisch geconfigureerd. U kunt gebruikers toevoegen of verwijderen en wachtwoorden instellen.

De Config Wizard heeft alleen op de lokale computer toegang tot Management Server.

U kunt een geactiveerde configuratie opslaan voor back-updoeleinden en deze configuratie later importeren. U kunt deze geïmporteerde configuratie wijzigen na het importeren.

Config Wizard voegt de lokale VRM automatisch toe.

#### **Beperkingen:**

De volgende taken kunnen niet worden uitgevoerd met de Config Wizard. Gebruik in plaats hiervan de Configuration Client van BVMS.

- schema's aanpassen
- systemen zonder of met meer Video Recording Managers configureren
- externe opslagapparaten configureren
- Video Streaming Gateway toevoegen
- alle geavanceerde configuraties die verdergaan dan basisinstellingen (bijvoorbeeld plattegronden of alarmen)

**Ga als volgt te werk om een snelle configuratie te bereiken met gebruikmaking van de Config Wizard:**

1. Dubbelklik op het pictogram Config Wizard op het standaardscherm van BVMS. De pagina **Welcome** wordt weergegeven.
2. Volg de wizard en de instructies op het scherm.

---

**Bericht!**



Raadpleeg de Handleiding van BVMS, die beschikbaar is in de online productcatalogus, voor meer informatie over de taken die niet kunnen worden uitgevoerd met de Config Wizard en voor gedetailleerde informatie over de Config Wizard zelf.

---

**Raadpleeg**

- *Aanvullende documentatie en clientsoftware, pagina 36*

## 5.7 Extra licenties toevoegen

U kunt extra licenties toevoegen met de Configuration Client.

**De software activeren:**


1. Start Configuration Client.
2. Klik in het menu **Tools** op **License Manager**.  
Het dialoogvenster **License Manager** wordt weergegeven.
3. Schakel de selectievakjes in voor het gewenste softwarepakket, de opties en de uitbreidingen die u wilt activeren. Voer het aantal licenties voor de uitbreidingen in. Als u een bundelinformatiebestand hebt ontvangen, klik dan op **Bundelinformatie importeren** om dit bestand te importeren.

4. Klik op **Activeren**.  
Het dialoogvenster **Licentie Activering** wordt weergegeven.
5. Noteer de computerhandtekening of kopieer deze naar een tekstbestand.
6. Voer op een computer met internettoegang de volgende URL in de browser in:  
`https://activation.boschsecurity.com`  
Als u geen account hebt die toegang biedt tot Bosch License Activation Center, kunt u een nieuwe account maken (aanbevolen) of op de koppeling klikken om een nieuwe licentie te activeren zonder dat u zich aanmeldt. Als u een account maakt en u zich vóór het activeren aanmeldt, houdt License Manager uw activeringen bij. U kunt deze dan te allen tijde raadplegen.  
Volg de instructies om de licentie-activerings sleutel te verkrijgen.
7. Ga terug naar de BVMS-software. Typ de licentie-activerings sleutel die u van License Manager hebt gekregen in het dialoogvenster **Licentie Activering** en klik vervolgens op **Activeren**.  
Het softwarepakket is geactiveerd.

## 5.8 BVMS Operator Client gebruiken

Gebruik de Operator Client van BVMS om de live-, opname- en afspeelfunctionaliteit van DIVAR IP te verifiëren.

### Functionaliteit voor live-beelden verifiëren in de Operator Client

1. Dubbelklik in het standaardscherm van BVMS op het pictogram Operator Client . De toepassing wordt gestart.

2. Voer de volgende gegevens in en klik op **OK**.  
**Gebruikersnaam:** admin  
**Wachtwoord:** geen wachtwoord vereist (indien niet ingesteld met de wizard)  
**Verbinding:** 127.0.0.1
3. Klik op het pictogram van het live-beeld. De logische structuur met de camera's wordt weergegeven.
4. Selecteer een camera en sleep deze naar een beeldvenster. Het beeld van de camera wordt weergegeven als de camera correct is toegewezen.  
**Opmerking:**  
camera's in het beeldvenster waarbij het pictogram van de camera een rode stip bevat, worden live weergegeven.

#### **De opnamefunctionaliteit in de Operator Client verifiëren**

- ▶ Camera's in de logische structuur waarbij het camerapictogram een rode stip bevat, nemen op.

#### **De afspeelfunctionaliteit in de Operator Client verifiëren**

- ▶ De indicator op de tijdlijn verschuift als de camera wordt weergegeven in de afspeelmodus.

Raadpleeg de handleiding van BVMS die beschikbaar is in de online productcatalogus voor meer informatie over andere functionaliteit.

## **6 Externe verbinding met het systeem**

In dit gedeelte worden de stappen beschreven die vereist zijn voor toegang tot het DIVAR IP-systeem vanaf internet.

### **6.1 Het systeem beschermen tegen onbevoegde toegang**

Om het systeem te beschermen tegen onbevoegde toegang, raden we u aan sterke wachtwoordregels te volgen voordat u het systeem verbindt met internet. Hoe sterker het wachtwoord, hoe beter uw systeem beschermd zal zijn tegen onbevoegde personen en malware.

## 6.2 Het doorsturen van poorten instellen

Voor toegang tot een DIVAR IP-systeem vanaf internet via een router met NAT/PAT-ondersteuning, moet het doorsturen van poorten zijn geconfigureerd op het DIVAR IP-systeem en op de router.

### Het doorsturen van poorten instellen:

- ▶ Voer de volgende poortregels in in de instellingen voor het doorsturen van poorten van uw internetrouter:
  - poort 5322 voor toegang via SSH-tunnel met gebruikmaking van BVMS Operator Client.
  - poort 443 voor HTTPS-toegang tot VRM met gebruikmaking van Video Security Client of de Video Security App.

Het DIVAR IP-systeem is nu toegankelijk vanaf internet.

## 6.3 Een geschikte client kiezen

In dit hoofdstuk worden de manieren beschreven waarop een externe verbinding tot stand kan worden gebracht met een DIVAR IP-systeem via internet.

Er zijn 2 manieren om een externe verbinding tot stand te brengen:

- *Externe verbinding met Operator Client, pagina 32.*
- *Externe verbinding met de Video Security-app, pagina 33.*

---

### Bericht!



Gebruik alleen de versie van BVMS Operator Client of de Video Security App die overeenkomt met de DIVAR IP. Andere clients of toepassingssoftware werken mogelijk, maar worden niet ondersteund.

---

### 6.3.1 Externe verbinding met Operator Client

**Ga als volgt te werk om een externe verbinding tot stand te brengen met BVMS Operator Client:**

1. Installeer BVMS Operator Client op het clientwerkstation.



2. Start, nadat de installatie is voltooid, Operator Client met gebruikmaking van de snelkoppeling op het bureaublad



3. Voer het volgende in en klik vervolgens op **OK**.  
**Gebruikersnaam:** admin (of andere gebruiker indien een andere gebruiker is geconfigureerd)  
**Wachtwoord:** voer het gebruikerswachtwoord in  
**Verbinding:** ssh://[public-IP-address-of-DIVAR-IP\_all-in-one]:5322

### 6.3.2 Externe verbinding met de Video Security-app

**Ga als volgt te werk om een externe verbinding tot stand te brengen met de Video Security App:**

1. Zoek in de App Store van Apple naar Bosch Video Security.
2. Installeer de Video Security-app op uw iOS-apparaat.
3. Start de Video Security-app.
4. Selecteer **Toevoegen**.
5. Voer het openbare IP-adres of de dynDNS-naam in.
6. Verzeker u ervan dat Veilige verbinding (SSL) is ingeschakeld.
7. Selecteer **Toevoegen**.
8. Voer het volgende in:  
**Gebruikersnaam:** admin (of andere gebruiker indien een andere gebruiker is geconfigureerd)  
**Wachtwoord:** voer het gebruikerswachtwoord in

## 7 Onderhoud

### 7.1 Systeembewaking

Het systeem biedt hulpmiddelen voor statusbewaking.

Om de bewakingsfunctionaliteit te activeren, moet u zich aanmelden met het beheerdersaccount (BVRAdmin).

1. Druk in het standaardscherm van BVMS op CTRL+ALT+DEL.
2. Houd SHIFT ingedrukt, klik op **Andere gebruiker** en houd SHIFT ongeveer vijf seconden ingedrukt.

3. Voer de gebruikersnaam en het wachtwoord in.
4. Dubbelklik in de map **Tools** op het bureaublad met de rechtermuisknop op het script **Enable\_SuperDoctor\_5\_Service** en klik vervolgens op **Als administrator uitvoeren**.
5. Dubbelklik op het pictogram **SuperDoctor 5 Web** in dezelfde map.
6. Meld u aan bij de webinterface met de volgende standaardreferenties:  
Gebruikersnaam: ADMIN  
Wachtwoord: ADMIN
7. Klik op de tab **Configuratie**, klik vervolgens op **Wachtwoordinstellingen** en wijzig het standaardwachtwoord.
8. Klik op de tab **Configuratie** en klik vervolgens op **Waarschuwingconfiguratie**.
9. Schakel de functie **SNMP-trap** in en geef het IP-adres van de ontvanger voor SNMP-traps op.

## 7.2 Het apparaat herstellen

In de volgende procedure wordt beschreven hoe u de standaard fabrieksinstelling van het product kunt herstellen.

### **Ga als volgt te werk om de standaard fabrieksinstelling van het product op het apparaat te herstellen:**

1. Start het apparaat en druk op **F7** tijdens de BIOS-zelftest tijdens inschakeling.  
Het herstelmenu wordt weergegeven.
2. Selecteer een van de volgende opties:
  - **Aanvankelijke fabrieksconfiguratie:** herstelt het systeem naar de standaard fabrieksimage en verwijdert alle gegevens op de harde-schijfstations.
  - of

- **Systeemherstel (terug naar fabrieksinstellingen):** herstelt het systeem naar de standaard fabrieksimage; de gegevens op de harde-schijfstations worden niet verwijderd.

**Opmerking:**

hoewel de optie **Systeemherstel** geen videobeelden verwijderd die zijn opgeslagen op de hard-schijfstations voor gegevens, wordt met deze optie wel de volledige partitie van het besturingssysteem (met inbegrip van de VMS-instellingen) vervangen door een standaardconfiguratie. Voor toegang tot de videobeelden na herstel moet de VMS-configuratie voorafgaand aan het systeemherstel worden geëxporteerd en na het systeemherstel weer worden geïmporteerd.

**Bericht!**

Schakel het apparaat niet uit tijdens het proces. Hierdoor raakt het herstelmedium beschadigd.

3. Het apparaat start vanaf het herstelmedium. Als de installatie is geslaagd, kiest u **Ja** om het systeem opnieuw op te starten.
4. Windows voert de eerste installatie van het besturingssysteem uit. Nadat Windows de installatie heeft voltooid, wordt het apparaat opnieuw opgestart.
5. Nadat de eenheid opnieuw is opgestart, zijn de fabrieksinstellingen ingesteld.

## 7.3 Onderhoud en reparatie

Op het opslagsysteem wordt 3 jaar garantie verleend. Storingen worden behandeld in overeenstemming met de richtlijnen voor service en ondersteuning van Bosch.

De opslagapparatuur wordt geleverd met een service- en ondersteuningsovereenkomst van de oorspronkelijke fabrikant.

In geval van storingen is de afdeling Technische ondersteuning van Bosch het enige aanspreekpunt, maar de service- en ondersteuningsverplichtingen worden nagekomen door de fabrikant of een partner.

Om de service- en ondersteuningsorganisatie van de fabrikant in staat te stellen om de serviceniveaus na te komen, moet het systeem opnieuw worden geregistreerd. Anders kan het gedefinieerde serviceniveau niet worden geboden, en kan enkel de best mogelijke service worden geboden.

Een beschrijving van welke informatie vereist is en waar deze informatie naar toe moet worden gestuurd, is als papieren versie opgenomen in elke levering. De beschrijving is tevens elektronisch beschikbaar in de online productcatalogus van Bosch.

## 8 Meer informatie

### 8.1 Aanvullende documentatie en clientsoftware

Bezoek <http://www.boschsecurity.com> en ga naar de desbetreffende productpagina in de productcatalogus voor meer informatie, softwaredownloads en documentatie.

### 8.2 Ondersteuningservices en Bosch Academy



#### Ondersteuning

Ga naar onze **ondersteuningservices** op <https://www.boschsecurity.com/xc/en/support/>.

Bosch Security and Safety Systems biedt ondersteuning op de volgende gebieden:

- [Apps en tools](#)
- [Building Information Modeling \(bouwinformatiemodellering\)](#)
- [Inbedrijfstelling](#)

- [Garantie](#)
- [Problemen oplossen](#)
- [Reparatie en ruilen](#)
- [Productbeveiliging](#)



### **Bosch Building Technologies Academy**

Bezoek de website van Bosch Building Technologies Academy voor toegang tot **trainingscursussen, videozelfstudies** en **documenten**: <https://www.boschsecurity.com/xc/en/support/training/>







**Bosch Security Systems B.V.**

Torenallee 49  
5617 BA Eindhoven  
Netherlands

**[www.boschsecurity.com](http://www.boschsecurity.com)**

© Bosch Security Systems B.V., 2020