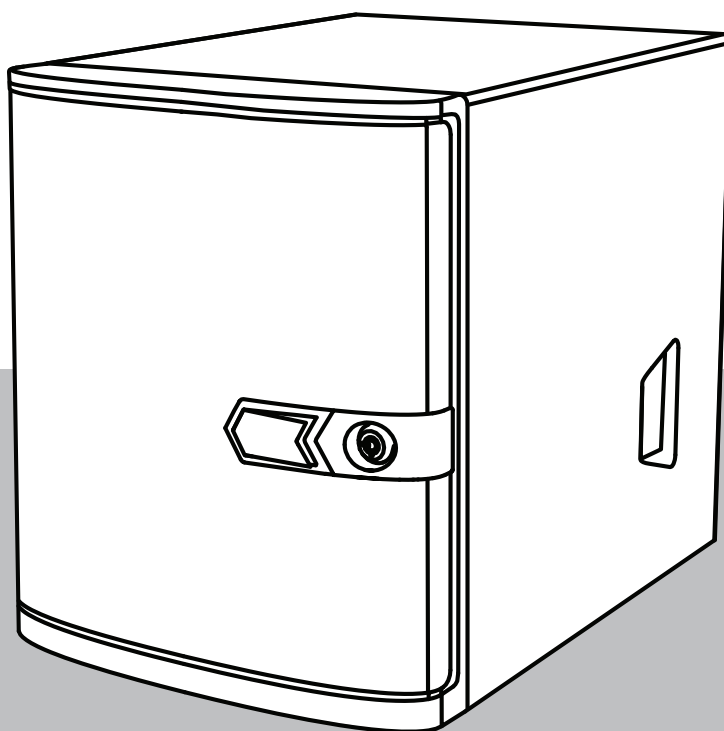




BOSCH

DIVAR IP all-in-one 4000

DIP-4420IG-00N | DIP-4424IG-2HD | DIP-4428IG-2HD |
DIP-442IIG-2HD



Inhoudsopgave

1	Veiligheid	4
1.1	Voorzorgmaatregelen	4
1.2	Voorzorgsmaatregelen voor cyberbeveiliging	5
1.3	Software voorzorgsmaatregelen	6
1.3.1	Gebruik de nieuwste software	6
1.3.2	OSS-informatie	6
2	Inleiding	7
3	Systeemoverzicht	8
4	Systeemconfiguratie	9
4.1	Standaardinstellingen	9
4.2	Vereisten	9
4.3	Eerste aanmelding en eerste systeeminstallatie	9
4.3.1	De bedrijfsmodus BVMS kiezen	11
4.3.2	De bedrijfsmodus VRM kiezen	11
4.3.3	De bedrijfsmodus iSCSI-opslag kiezen	12
5	Software upgraden	13
6	Externe verbinding met het systeem	15
6.1	Het systeem beschermen tegen onbevoegde toegang	15
6.2	Het doorsturen van poorten instellen	15
6.3	Een geschikte client kiezen	15
6.3.1	Externe verbinding met BVMS Operator Client.	15
6.3.2	Externe verbinding met de Video Security-app	16
6.4	Verbinden met een Enterprise Management Server	16
7	Onderhoud	17
7.1	Aanmelden bij het beheerdersaccount	17
7.2	Systeembewaking	17
7.3	Een defecte harde schijf vervangen en een nieuwe harde schijf configureren	18
7.3.1	Een defecte harde schijf vervangen	18
7.3.2	Configureer een nieuwe harde schijf	18
7.4	Logboekbestanden van de DIVAR IP-systeembeheerder verzamelen	20
7.5	Het apparaat herstellen	20
8	Meer informatie	22
8.1	Aanvullende documentatie en clientsoftware	22
8.2	Ondersteuningsservices en Bosch Academy	22

1 Veiligheid

Houd u aan de veiligheidsmaatregelen in dit hoofdstuk.

1.1 Voorzorgmaatregelen

**Opmerking!**

Gebruiksdoel

Dit product is alleen voor professioneel gebruik. Het is niet bedoeld voor installatie in een openbare ruimte die toegankelijk is voor het grote publiek.

**Opmerking!**

Gebruik dit product niet op vochtige of natte plaatsen.

**Opmerking!**

Neem voorzorgsmaatregelen om het apparaat te beschermen tegen schade door bliksem en stroomstoten.

**Opmerking!**

Houd de ruimte rondom het apparaat schoon en vrij van rommel.

**Opmerking!**

Openingen van de behuizing

De openingen mogen niet geblokkeerd of afgedekt worden. Alle openingen in de behuizing zijn bedoeld voor de ventilatie. Deze openingen voorkomen oververhitting en waarborgen een betrouwbare werking.

**Opmerking!**

Open of verwijder de afdekking van het apparaat niet. Het openen of verwijderen van de afdekking kan schade aan het systeem veroorzaken en zal de garantie ongeldig maken.

**Opmerking!**

Mors geen vloeistoffen op het apparaat.

**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.

**Opmerking!**

Ontkoppel de stroomtoevoer voordat het product wordt verplaatst. Verplaats het product voorzichtig. Overmatige kracht of schokken kunnen het product en de harde schijven beschadigen.

**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.

**Opmerking!**

Beeldverlies is inherent aan digitale video-opnamen. Derhalve kan Bosch Security Systems niet aansprakelijk worden gesteld voor schade tengevolge van het ontbreken van video-informatie.

Wij raden de toepassing aan van meerdere, redundante opnamesystemen en een procedure voor het maken van back-ups van alle analoge en digitale informatie om het risico van verlies van informatie tot een minimum te beperken.

1.2

Voorzorgsmaatregelen voor cyberbeveiliging

Neem voor de cyberbeveiliging het volgende in acht:

- Zorg ervoor dat de fysieke toegang tot het systeem alleen mogelijk is voor geautoriseerd personeel. Plaats het systeem in een met toegangscontrole beveiligde ruimte, om fysieke manipulatie te voorkomen.
- Vergrendel het voorpaneel als bescherming tegen ongeoorloofde verwijdering van de harde schijven. Verwijder de sleutel altijd uit het slot en sla deze op een veilige plaats op.
- Gebruik het achterste chassisdeel of de Kensington-sleuf als extra beveiliging van het apparaat.
- Het besturingssysteem bevat de nieuwste Windows-beveiligingspatches die beschikbaar waren op het moment dat de software-image werd gemaakt. Gebruik de online Windows updatefunctie of de overeenkomstige maandelijkse 'roll-up patches' voor offline installatie om regelmatig beveiligingsupdates voor het besturingssysteem te installeren.
- Schakel Windows Defender en de Windows firewall niet uit, en zorg ervoor dat deze altijd up-to-date zijn.
- Installeer geen extra antivirussoftware.
- Verstrek geen systeeminformatie en gevoelige gegevens aan personen die u niet kent, tenzij u zeker bent dat de persoon in kwestie bevoegd is.
- Verstuur geen gevoelige informatie via het internet voordat u de beveiliging van een website hebt gecontroleerd.
- Beperk de toegang tot het lokale netwerk tot apparaten die u vertrouwt. Details worden beschreven in de navolgende documenten die beschikbaar zijn in de online productcatalogus.
 - *Netwerkverificatie 802.1X*
 - *Handleiding cyberbeveiliging voor IP-videoproducten van Bosch*
- Gebruik alleen de veilige (gecodeerde) communicatiekanalen voor toegang via openbare netwerken.
- Het beheerdersaccount geeft volledige bevoegdheden aan de beheerder en onbeperkte toegang tot het systeem. Met beheerdersrechten kunnen gebruikers software installeren, bijwerken of verwijderen, en de configuratie-instellingen wijzigen. Daarnaast stellen beheerdersrechten gebruikers in staat registersleutels direct te openen en te wijzigen en daarmee centrale beheer- en beveiligingsinstellingen uit te schakelen. Op de beheerdersaccount aangemelde gebruikers kunnen firewalls omzeilen en antivirussoftware verwijderen, waardoor het systeem wordt blootgesteld aan virussen en cyberaanvallen. Dit kan een ernstig risico vormen voor het systeem en de veiligheid van

de gegevens.

Neem het volgende in acht om de risico's voor de cyberbeveiliging tot een minimum te beperken:

- Zorg ervoor dat het beheerdersaccount is beschermd met een complex wachtwoord volgens het wachtwoordbeleid.
- Zorg ervoor dat alleen een beperkt aantal vertrouwde gebruikers toegang hebben tot het beheerdersaccount.
- In verband met de werking mag het systeemstation niet worden gecodeerd. Zonder codering kunnen de op dit station opgeslagen gegevens gemakkelijk worden ingezien en verwijderd. Zorg ervoor dat alleen bevoegde personen toegang tot het systeem en het beheerdersaccount hebben om diefstal of onbedoeld verlies van gegevens te voorkomen.
- Voor installatie en updaten van de software en voor systeemherstel kan het nodig zijn USB-apparaten te gebruiken. Daarom mogen de USB-poorten van uw systeem niet zijn uitgeschakeld. Bij het aansluiten van USB-apparaten op het systeem bestaat echter een risico van malware-infectie. Zorg er om malware-aanvallen te voorkomen voor dat er geen geïnfecteerde USB-apparaten op het systeem zijn aangesloten.

1.3

Software voorzorgsmaatregelen

1.3.1

Gebruik de nieuwste software

Voordat u het apparaat voor de eerste keer gebruikt, moet u de meest recente toepasselijke release van uw softwareversie installeren. Voor een consistente functionaliteit, compatibiliteit, prestaties en beveiliging werkt u de software regelmatig bij gedurende de levensduur van het apparaat. Volg de instructies in de productdocumentatie met betrekking tot software-updates. De volgende koppelingen bieden meer informatie:

- Algemene informatie: <https://www.boschsecurity.com/xc/en/support/product-security/>
- Veiligheidsadviezen, dat wil zeggen een lijst met aangeduide zwakke plekken en voorgestelde oplossingen: <https://www.boschsecurity.com/xc/en/support/product-security/security-advisories.html>

Bosch aanvaardt geen enkele aansprakelijkheid voor schade die wordt veroorzaakt door gebruik van haar producten met verouderde softwarecomponenten.

U vindt de nieuwste software en beschikbare upgradepakketten in het downloadgedeelte van Bosch Security and Safety Systems onder:

<https://downloadstore.boschsecurity.com/>

1.3.2

OSS-informatie

In de DIVAR IP all-in-one producten gebruikt Bosch open source software.

De licenties voor de open source softwarecomponenten vindt u op het systeemstation onder:

```
C:\license txt\
```

De licenties van Open Source Softwarecomponenten die in andere op uw systeem geïnstalleerde software worden gebruikt, worden opgeslagen in de installatiemap van de betreffende software, bijvoorbeeld onder:

```
C:\Program Files\Bosch\SysMgmService\apps\sysmgm-commander\[version]\License
```

of onder:

```
C:\Program Files\Bosch\SysMgmService\apps\sysmgm-executor\[version]\License
```

2 Inleiding

DIVAR IP all-in-one 4000 is een betaalbare en gebruiksvriendelijke alles-in-één oplossing voor het opnemen, bekijken en beheren van netwerkbewakingssystemen tot 32 kanalen (met 8 vooraf gelicentieerde kanalen).

DIVAR IP all-in-one 4000 is een 2-bay mini tower unit die geavanceerde Bosch Video Management System mogelijkheden en state-of-the-art opnamebeheer in één kosteneffectief, gemakkelijk te installeren en te bedienen opnameapparaat voor IT-gerichte klanten combineert.

DIVAR IP all-in-one 4000 maakt gebruik van ingebouwde ontwerp- en kerncomponenten en is gebaseerd op het besturingssysteem Microsoft Windows Server IoT 2022 for Storage Workgroup.

De DIVAR IP all-in-one 4000 beschikt over 'enterprise-rated', aan de voorkant verwisselbare SATA-II harde schijven die maximaal 36 TB bruto-opslagcapaciteit bieden.

3 Systeemoverzicht

Besturingssysteem

Het Microsoft Windows Server IoT 2022 for Storage Workgroup-besturingssysteem biedt een gebruikersinterface voor initiële serverconfiguratie, universeel beheer van opslagapparaten, eenvoudige configuratie en beheer van opslag en gedeelde mappen, en ondersteuning voor Microsoft iSCSI Software Target.

Het systeem is speciaal afgestemd voor optimale prestaties voor op netwerk aangesloten opslag. Het besturingssysteem Microsoft Windows Server IoT 2022 for Storage Workgroup zorgt voor aanzienlijke verbeteringen met betrekking tot scenario's voor opslagbeheer en de integratie van onderdelen en functionaliteiten voor beheer van opslagapparaten.

DIVAR IP System Manager

De toepassing DIVAR IP System Manager is de centrale gebruikersinterface voor een eenvoudige systeeminstallatie, configuratie en software-upgrade.

Bedieningsmodi

DIVAR IP all-in-one 4000 systemen kunnen in drie verschillende modi werken:

- Volledig video-opname- en beheersysteem gebruikmakend van de belangrijkste BVMS- en Video Recording Manager-componenten en -diensten.
Deze modus biedt een geavanceerde IP-videobeveiligingsoplossing die naadloos beheer van digitale video, audio en gegevens via een IP-netwerk levert. Het combineert naadloos IP-camera's en encoders, biedt systeembreed gebeurtenis- en alarmbeheer, systeemgezondheidsbewaking, gebruikers- en prioriteitsbeheer. Deze modus biedt het beste videobeheersysteem dat past bij Bosch videobewakingsapparatuur, waarbij gebruik wordt gemaakt van de unieke mogelijkheden van Bosch camera's en opname-oplossingen. Het bevat Video Streaming Gateway-componenten om camera's van derden te integreren.
- Puur video-opnamesysteem, gebruikmakend van de Video Recording Manager belangrijkste componenten en -services, gebruikmakend van de unieke mogelijkheden van Bosch camera's en opnameoplossingen.
- iSCSI-opslaguitbreiding voor een BVMS of Video Recording Manager systeem, dat op andere hardware draait. Er kunnen maximaal twee van deze iSCSI-opslaguitbreidingen worden toegevoegd aan een BVMS- of Video Recording Manager-systeem dat op een DIVAR IP all-in-one 4000 draait.

Bij het instellen van het systeem moet u in de toepassing DIVAR IP System Manager de gewenste bedrijfsmodus kiezen om uw systeem te configureren.

Met de toepassing DIVAR IP System Manager kunt u tevens de geïnstalleerde software upgraden.

U vindt de nieuwste software en beschikbare upgradepakketten in het downloadgedeelte van Bosch Security and Safety Systems onder:

<https://downloadstore.boschsecurity.com/>



Opmerking!

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

4 Systeemconfiguratie

4.1 Standaardinstellingen

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

- Gebruikersnaam: **BVRAdmin**
- Wachtwoord: bij eerste aanmelding in te stellen.
Wachtwoordvereisten:
 - Minimaal 14 tekens.
 - Ten minste één hoofdletter.
 - Ten minste een kleine letter.
 - Ten minste een cijfer.

4.2 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.

4.3 Eerste aanmelding en eerste systeeminstallatie



Opmerking!

Wijzig geen instellingen van het besturingssysteem. Het wijzigen van de instellingen van het besturingssysteem kan leiden tot storingen in het systeem.



Opmerking!

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




Opmerking!

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.

Het systeem configureren:

1. Sluit de DIVAR IP all-in-one-unit en de camera's aan op het netwerk.
2. Schakel de unit in.
Instelroutines voor Microsoft Windows Server IoT 2022 for Storage Workgroup worden uitgevoerd. Dit proces kan enkele minuten duren. Schakel het systeem niet uit.
Nadat het proces is voltooid, wordt het taalselectiescherm van Windows weergegeven.
3. Selecteer uw land/regio, de gewenste taal van het besturingssysteem en de toetsenbordindeling in de lijst en klik vervolgens op **Volgende**.
De licentievoorwaarden van Microsoft software worden weergegeven.

4. Klik op **Accepteren** om de licentievoorwaarden te accepteren en wacht tot Windows opnieuw is opgestart. Dit kan enkele minuten duren. Schakel het systeem niet uit. Na het opnieuw opstarten wordt de Windows aanmeldpagina weergegeven.
5. Stel een nieuw wachtwoord in voor het beheerderaccount **BVRAdmin** en bevestig het. Wachtwoordvereisten:
 - Minimaal 14 tekens.
 - Ten minste één hoofdletter.
 - Ten minste een kleine letter.
 - Ten minste een cijfer.
 Druk daarna op Enter.
 De **Software Selection** pagina wordt weergegeven.
6. Het systeem scant automatisch het lokale station en alle aangesloten externe opslagmedia voor het DIVAR IP System Manager-installatiebestand, **SystemManager_x64_[software version].exe** dat zich in een map bevindt met de volgende structuur: *Drive root\BoschAppliance*. Het scannen kan even duren. Wacht totdat dit is voltooid.
7. Zodra het systeem het installatiebestand heeft gevonden, wordt dat weergegeven op de **Software Selection** pagina. Klik op de balk die het installatiebestand weergeeft om de installatie te starten.
8. Ga als volgt te werk als het installatiebestand tijdens het scanproces niet wordt gevonden:
 - Ga naar <https://downloadstore.boschsecurity.com/>.
 - Selecteer onder het **Software**-tabblad, **BVMS Appliances** uit de lijst en klik vervolgens op **Select**.
 Er een lijst met alle beschikbare softwarepakketten wordt weergegeven.
 - Zoek het ZIP-bestand **SystemManager_[software version].zip** en sla het op, op een opslagmedium zoals een USB-stick.
 - Pak het bestand uit op het opslagmedium door ervoor te zorgen dat de map **BoschAppliance** in de root van het opslagmedium is geplaatst.
 - Sluit het opslagmedium aan op uw DIVAR IP all-in-one-systeem.
 Het systeem scant automatisch het opslagmedium voor het installatiebestand. Het kan enige tijd duren voor de scan is uitgevoerd. Wacht totdat dit is voltooid.
 - Zodra het installatiebestand is gevonden, wordt dat weergegeven op de **Software Selection** pagina. Klik op de balk die het installatiebestand weergeeft om de installatie te starten.
Opmerking: om automatisch te worden gedetecteerd, moet het installatiebestand zich in een map met de volgende structuur bevinden: *Drive root\BoschAppliance* (bijvoorbeeld *F:\BoschAppliance*).
 Als het installatiebestand zich op een andere locatie bevindt, die niet overeenkomt met de vooraf gedefinieerde mapstructuur, klikt u op  om naar de betreffende locatie te navigeren. Klik dan op het installatiebestand om de installatie te starten.
9. Voordat de installatie begint, wordt het **End User License Agreement (EULA)** dialoogvenster weergegeven. Lees de licentievoorwaarden en klik dan op **Accept** om verder te gaan. De installatie begint.
10. Nadat de installatie is voltooid, wordt het systeem opnieuw opgestart en wordt u naar de Windows-aanmeldingspagina geleid. Meld u aan bij de beheerdersaccount.



11. De Microsoft Edge browser wordt geopend en de **DIVAR IP - Systeeminstellingen** pagina wordt weergegeven. De pagina toont het apparaattype en het serienummer van het apparaat, evenals de drie bedrijfsmodi en de beschikbare softwareversies voor elke bedrijfsmodus.

U moet de gewenste bedrijfsmodus en softwareversie kiezen om uw DIVAR IP all-in-one-systeem te configureren.

Opmerking: als de gewenste softwareversie voor de betreffende werkingsmodus niet beschikbaar is op een lokaal station, gaat u als volgt te werk:

- Ga naar <https://downloadstore.boschsecurity.com/>.
- Selecteer onder het **Software**-tabblad, **BVMS Appliances** uit de lijst en klik vervolgens op **Select**.
Er een lijst met alle beschikbare softwarepakketten wordt weergegeven.
- Zoek bijvoorbeeld de ZIP-bestanden van de gewenste softwarepakketten **BVMS_[BVMS version]_SystemManager_package_[package version].zip** op en sla ze op in een opslagmedium zoals een USB-stick.
- Pak de bestanden op het opslagmedium uit. Wijzig de mapstructuur van de uitgepakte bestanden niet.
- Sluit vervolgens het opslagmedium aan op uw DIVAR IP all-in-one-systeem.



Opmerking!

Als de bedrijfsmodus na de installatie wordt gewijzigd, moet het systeem volledig worden teruggezet naar de fabrieksinstellingen.

4.3.1

De bedrijfsmodus BVMS kiezen

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

1. Selecteer in het dialoogvenster **DIVAR IP - Systeeminstellingen** de bedrijfsmodus **BVMS VRM** en de gewenste BVMS-versie die u wilt installeren, klik vervolgens op **Volgende**. De BVMS-licentieovereenkomst wordt weergegeven.
2. Lees en accepteer de licentieovereenkomst, klik dan op **Installeren** om verder te gaan. De installatie start en het installatiedialoogvenster toont de voortgang ervan. Zet het systeem niet uit en verwijder de opslagmedia niet tijdens het installatieproces.
3. Het systeem start opnieuw op nadat alle softwarepakketten succesvol zijn geïnstalleerd. Nadat het systeem opnieuw is opgestart, wordt u doorgeleid naar het bureaublad van BVMS.
4. Klik op de gewenste toepassing op het bureaublad van BVMS om uw systeem te configureren.



Opmerking!

Raadpleeg voor verdere details de desbetreffende DIVAR IP all-in-one webgebaseerde training en de BVMS documentatie.

U vindt de training onder www.boschsecurity.com/xc/en/support/training/

4.3.2

De bedrijfsmodus VRM kiezen

Ga als volgt te werk om het DIVAR IP all-in-one-systeem te gebruiken als een puur voor video-opnamen bestemd systeem:

1. Selecteer in het dialoogvenster **DIVAR IP - Systeeminstellingen** de bedrijfsmodus **VRM** en de gewenste VRM-versie die u wilt installeren, klik vervolgens op **Volgende**. De VRM-licentieovereenkomst wordt weergegeven.

2. Lees en accepteer de licentieovereenkomst, klik dan op **Installeren** om verder te gaan. De installatie start en het installatiedialoogvenster toont de voortgang ervan. Zet het systeem niet uit en verwijder de opslagmedia niet tijdens het installatieproces.
3. Het systeem start opnieuw op nadat alle softwarepakketten succesvol zijn geïnstalleerd. Nadat het systeem opnieuw is opgestart, wordt u doorgeleid naar het aanmeldscherm van Windows.

**Opmerking!**

Raadpleeg de documentatie van VRM voor meer informatie.

4.3.3**De bedrijfsmodus iSCSI-opslag kiezen**

Ga als volgt te werk om het DIVAR IP all-in-one-systeem te gebruiken als iSCSI-opslaguitbreiding:

1. Selecteer op de **DIVAR IP - Systeeminstellingen**-pagina de bedrijfsmodus **iSCSI-opslag** en de gewenste iSCSI-opslagversie die u wilt installeren, klik vervolgens op **Volgende**. Het installatiedialoogvenster wordt weergegeven.
2. Klik in het installatiedialoogvenster op **Installeren** om verder te gaan. De installatie start en het installatiedialoogvenster toont de voortgang ervan. Zet het systeem niet uit en verwijder de opslagmedia niet tijdens het installatieproces.
3. Het systeem start opnieuw op nadat alle softwarepakketten succesvol zijn geïnstalleerd. Nadat het systeem opnieuw is opgestart, wordt u doorgeleid naar het aanmeldscherm van Windows.
4. Voeg het systeem toe als iSCSI-opslaguitbreiding aan een externe BVMS- of VRM-server met gebruikmaking van BVMS Configuration Client of Configuration Manager.

**Opmerking!**

Raadpleeg de documentatie van BVMS of Configuration Manager voor meer informatie.

5 Software upgraden

Met de toepassing DIVAR IP System Manager kunt u de geïnstalleerde software op uw systeem upgraden.

U vindt de nieuwste software en beschikbare upgradepakketten in het downloadgedeelte van Bosch Security and Safety Systems onder:


<https://downloadstore.boschsecurity.com/>



Opmerking!



Het downgraden van de geïnstalleerde software naar een eerdere versie wordt niet ondersteund.

U upgrade de geïnstalleerde software als volgt:

1. Ga naar <https://downloadstore.boschsecurity.com/>.
2. Selecteer onder het **Software**-tabblad, **BVMS Appliances** uit de lijst en klik vervolgens op **Select**.
Er een lijst met alle beschikbare softwarepakketten wordt weergegeven.
3. Zoek bijvoorbeeld de ZIP-bestanden van de gewenste softwarepakketten **BVMS_[BVMS version]_SystemManager_package_[package version].zip** op en sla ze op in een opslagmedium zoals een USB-stick.
4. Pak de bestanden op het opslagmedium uit. Wijzig de mapstructuur van de uitgepakte bestanden niet.
5. Start de toepassing DIVAR IP System Manager als volgt:
 - Als u zich met het beheerdersaccount **BVRAdmin** bij Windows hebt aangemeld, dubbelklikt u op het Windows-bureaublad op het pictogram DIVAR IP System Manager.
De toepassing DIVAR IP System Manager wordt gestart.
 - Als uw systeem in de bedrijfsmodus BVMS werkt, klikt u op het bureaublad BVMS op het pictogram DIVAR IP System Manager en meldt u zich aan bij het beheerdersaccount BVRAdmin. De toepassing DIVAR IP System Manager wordt geopend in een dialoogvenster met een volledig scherm (u kunt het dialoogvenster sluiten door op de knop Alt+ F4 te drukken).
6. De pagina **Softwarepakketten** wordt weergegeven waarop het apparaattype en het serienummer van het apparaat bovenaan de pagina staat.
 - In de kolom **Naam** ziet u alle softwaretoepassingen van de DIVAR IP System Manager die al op uw systeem zijn geïnstalleerd en ook alle andere softwaretoepassingen van de DIVAR IP System Manager die op het **Images**-station of op een opslagmedium door het systeem zijn gedetecteerd.
 - In de kolom **Geïnstalleerde versie** ziet u de versie van de softwaretoepassing die op dit moment op uw systeem is geïnstalleerd.
 - In de kolom **Status** ziet u de status van de desbetreffende softwaretoepassing:
 - Het pictogram  geeft aan dat er door het systeem geen latere versies van de geïnstalleerde softwaretoepassing op het **Images**-station of op een opslagmedium zijn gedetecteerd.

Opmerking: als u ervoor wilt zorgen dat u de nieuwste softwareversie gebruikt, controleert u de beschikbare softwareversies in de downloadstore van Bosch Security and Safety Systems onder:

<https://downloadstore.boschsecurity.com/>

- Het pictogram  geeft aan dat er door het systeem latere versies van de geïnstalleerde softwaretoepassing op het **Images**-station of op een opslagmedium zijn gedetecteerd.
Het pictogram wordt ook weergegeven als het systeem een softwaretoepassing heeft gedetecteerd die nog niet op uw systeem is geïnstalleerd.
- In de kolom **Beschikbare versie** ziet u de latere versies van de geïnstalleerde softwaretoepassingen. Deze versies zijn door het systeem op het **Images**-station of op een opslagmedium gedetecteerd.
In de kolom worden ook de beschikbare versies van de gedetecteerde softwaretoepassingen weergegeven die nog niet op uw systeem zijn geïnstalleerd.
Opmerking: alleen latere versies van de geïnstalleerde softwaretoepassingen worden weergegeven. Het downgraden van een softwaretoepassing naar een eerdere versie wordt niet ondersteund.
- 7. Klik in de kolom **Naam** op de respectievelijke optieknop om de softwaretoepassing te selecteren die u wilt upgraden of installeren.
- 8. Selecteer in de kolom **Beschikbare versie** de gewenste versie waar u uw softwaretoepassing naar wilt upgraden of die u wilt installeren en klik vervolgens op **Volgende**.
Er wordt indien van toepassing een dialoogvenster voor een licentieovereenkomst weergegeven.
- 9. Lees en accepteer de licentieovereenkomst, klik vervolgens op **Installeren** om door te gaan.
De installatie wordt gestart en het installatiedialoogvenster geeft de voortgang van de installatie weer. Zet het systeem niet uit en verwijder de opslagmedia niet tijdens het installatieproces.
- 10. Nadat alle softwarepakketten zijn geïnstalleerd, ontvangt u bovenaan de pagina het bericht **Installeren voltooid**.
- 11. Als de installatie niet is geslaagd, ontvangt u het bericht **Het installeren is mislukt**, en wordt het pictogram  weergegeven. Druk in dat geval op F5 om terug te gaan naar de pagina **Softwarepakketten**. Download de desbetreffende softwarepakketten nogmaals en probeer het opnieuw.
Als het probleem zich blijft voordoen, neemt u contact op met de technische ondersteuning.

6 Externe verbinding met het systeem

U kunt met uw DIVAR IP all-in-one-systeem een externe verbinding tot stand brengen en vanaf internet toegang krijgen.

Als u een externe verbinding tot stand wilt brengen, doet u het volgende:

1. *Het systeem beschermen tegen onbevoegde toegang, pagina 15.*
2. *Het doorsturen van poorten instellen, pagina 15.*
3. *Een geschikte client kiezen, pagina 15.*

6.1 Het systeem beschermen tegen onbevoegde toegang

Als u het systeem tegen onbevoegde toegang wilt beschermen, moet ervoor zorgen dat u regels voor een sterk wachtwoord volgt voordat u het systeem met internet verbindt. Hoe sterker het wachtwoord, hoe beter uw systeem beschermd zal zijn tegen onbevoegde personen en malware.

6.2 Het doorsturen van poorten instellen

Als u vanaf internet via een router met NAT/PAT-ondersteuning toegang tot een DIVAR IP all-in-one-systeem wilt, moet u het doorsturen van poorten op uw DIVAR IP all-in-one en op de router configureren.

U stelt het doorsturen van poorten als volgt in:

- ▶ Voer de volgende poortregels in de instellingen voor het doorsturen van poorten van uw internetrouter in:
 - Poort 5322 voor SSH-tunneltoegang met BVMS Operator Client.
Opmerking: deze verbinding is alleen van toepassing voor de bedrijfsmodus BVMS.
 - poort 443 voor HTTPS-toegang tot VRM met gebruikmaking van Video Security Client of de Video Security App.
Opmerking: deze verbinding is alleen van toepassing voor de bedrijfsmodus BVMS of VRM.

Uw DIVAR IP all-in-one is nu toegankelijk vanaf internet.

6.3 Een geschikte client kiezen

Er zijn twee opties om met uw DIVAR IP all-in-one-systeem een externe verbinding tot stand te brengen:

- *Externe verbinding met BVMS Operator Client., pagina 15.*
- *Externe verbinding met de Video Security-app, pagina 16.*



Opmerking!

De compatibiliteit van de versies van BVMS Operator Client of de Video Security App wordt bepaald door de versie van de software BVMS of VRM die in DIVAR IP is geïnstalleerd. Raadpleeg voor gedetailleerde informatie de desbetreffende softwaredocumentatie en het trainingsmateriaal.


6.3.1 Externe verbinding met BVMS Operator Client.



Opmerking!

Deze verbinding is alleen van toepassing voor de bedrijfsmodus BVMS.

U brengt als volgt een externe verbinding met BVMS Operator Client tot stand:

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 er een is geconfigureerd)
Wachtwoord: gebruikerswachtwoord
Verbinding: ssh://[public-IP-address-of-DIVAR-IP_all-in-one]:5322

6.3.2 Externe verbinding met de Video Security-app



Opmerking!

Deze verbinding is alleen van toepassing voor de bedrijfsmodus BVMS of VRM.

U brengt als volgt een externe verbinding met de Video Security App tot stand:

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. Verzekert u ervan dat Veilige verbinding (SSL) is ingeschakeld.
7. Selecteer **Toevoegen**.
8. Voer het volgende in:
Gebruikersnaam: admin (of andere gebruiker indien er een is geconfigureerd)
Wachtwoord: gebruikerswachtwoord

6.4 Verbinden met een Enterprise Management Server

Voor een centraal beheer van meerdere DIVAR IP all-in-one-systemen in de bedrijfsmodus BVMS kunt u een BVMS Enterprise Management Server gebruiken die op een aparte server wordt geïnstalleerd.

Raadpleeg voor gedetailleerde informatie over de configuratie en bediening van het BVMS Enterprise System de documentatie en het trainingsmateriaal van BVMS.

7

Onderhoud

7.1

Aanmelden bij het beheerdersaccount

In gebruiksmodus aanmelden bij de beheerdersaccount BVMS

Om u in gebruiksmodus aan te melden bij de BVMS-beheerdersaccount:

1. Druk op het BVMS-bureaublad op Ctrl+Alt+Del.
2. Druk onmiddellijk op de linker Shift-toets en houd deze ingedrukt nadat u hebt **geklikt** op **Andere gebruiker**.
3. Druk nogmaals op Ctrl+Alt+Del.
4. Selecteer de **BVRAdmin** gebruiker en voer het wachtwoord in dat tijdens de systeemconfiguratie is ingesteld. Druk vervolgens op Enter.

Opmerking: om terug te gaan naar het BVMS-bureaublad drukt u op Ctrl+Alt+Del en klikt u op **Van gebruiker wisselen** of **Uitloggen**. Het systeem gaat dan zonder systeemherstart automatisch terug BVMS naar het bureaublad.

Aanmelden bij de beheerdersaccount in VRM of iSCSI bewerkingsmodus

Om u bij de beheerdersaccount aan te melden in VRM of iSCSI bewerkingsmodus:

- Druk op het aanmeldingsscherm van Windows en voer Ctrl+Alt+Del het **BVRAdmin**-wachtwoord in.

7.2

Systeembewaking

De DIVAR IP all-in-one-systemen worden geleverd met de vooraf geïnstalleerde toepassing **SuperDoctor** die u kunt gebruiken om uw systeem te bewaken.

De bewakingsfunctie activeren

U activeert de bewakingsfunctie als volgt:

1. Meld u aan bij het beheerdersaccount (raadpleeg *Aanmelden bij het beheerdersaccount, pagina 17*).
2. Klik op het bureaublad in de map **Tools**, klik met de rechter muisknop op het script **startSD5Service** en klik vervolgens op **Run with PowerShell**.
3. Dubbelklik op het bureaublad op het pictogram **SuperDoctor 5 Web**.
4. Meld u aan bij de webinterface met de volgende standaardgegevens:
 - Gebruikersnaam: **admin**
 - Wachtwoord: **DivaripSD5**
5. Klik op het tabblad **Configuration**, klik vervolgens op **Account Setting** en wijzig het standaardwachtwoord.

Opmerking: Bosch raadt u dringend aan het standaardwachtwoord direct na de eerste aanmelding bij de toepassing **SuperDoctor** te wijzigen.
6. Klik onder het tabblad **Configuration** op **Alert Configuration**.
7. Activeer de **SNMP Trap** functies en geef het IP-adres van de ontvanger voor SNMP-traps op.

De bewakingsfunctie deactiveren

U deactiveert de bewakingsfunctie als volgt:

1. Meld u aan bij het beheerdersaccount (raadpleeg *Aanmelden bij het beheerdersaccount, pagina 17*).
2. Klik op het bureaublad in de map **Tools**, klik met de rechter muisknop op het script **stopSD5Service** en klik vervolgens op **Run with PowerShell**.

7.3 Een defecte harde schijf vervangen en een nieuwe harde schijf configureren

Als een harde schijf die op uw DIVAR IP all-in-one systeem is geïnstalleerd niet meer werkt en niet meer kan worden gebruikt, dient u de volgende stappen uit te voeren:

1. *Een defecte harde schijf vervangen, pagina 18.*
2. *Configureer een nieuwe harde schijf, pagina 18.*



Opmerking!

Bosch is niet aansprakelijk voor gegevensverlies, schade of systeemstoringen van apparaten die zijn uitgerust met harde schijven die niet door Bosch zijn geleverd. Bosch kan geen ondersteuning aanbieden als harde schijven die niet door Bosch zijn geleverd de oorzaak van het probleem blijken te zijn. Om mogelijke hardwareproblemen op te lossen, vereist Bosch de installatie van door Bosch geleverde harde schijven.

7.3.1 Een defecte harde schijf vervangen

U vervangt een defecte harde schijf als volgt:

1. Schakel het apparaat DIVAR IP all-in-one in.
2. Verwijder de defecte harde schijf uit de eenheid en installeer de nieuwe harde schijf. Raadpleeg het hoofdstuk *Een SATA-harde schijf installeren* in de installatiehandleiding.

7.3.2 Configureer een nieuwe harde schijf

Ga als volgt te werk bij het configureren van een nieuwe harde schijf:

1. *Nieuwe partitie en volume aanmaken, pagina 18*
2. *De serverservice inschakelen, pagina 19.*
3. *LUN's aanmaken (iSCSI virtuele schijven), pagina 19.*
4. *De serverservice uitschakelen, pagina 20.*
5. *LUN's formatteren, pagina 20*

Nieuwe partitie en volume aanmaken

Nieuwe partitie en volume aanmaken:

1. Selecteer in het startmenu **van** Windows **Server Manager** en selecteer vervolgens **File and Storage Services > Volumes > Disks**.
Alle schijven die in uw systeem zijn geïnstalleerd, worden weergegeven.
2. Klik met de rechtermuisknop op het nieuwe schijfstation dat u hebt geïnstalleerd en klik vervolgens op **New Volume...**
Het **New Volume Wizard** dialoogvenster wordt weergegeven.
3. Klik op **Next** om verder te gaan.
Het **Server and Disk** dialoogvenster wordt weergegeven.
4. Selecteer de betreffende server en de schijf en klik hierop om door **Next** te gaan.
Het **Size** dialoogvenster wordt weergegeven.
5. Voer in het **Volume size:** veld de gewenste volumegrootte in die u wilt gebruiken. Laat de voorgeselecteerde waarde ongewijzigd als u de maximum volumegrootte wilt gebruiken.
Klik vervolgens op **Next** om verder te gaan.
Het **Drive Letter or Folder** dialoogvenster wordt weergegeven.
6. Selecteer in de lijst **Drive letter:** de stationletter die aan het volume moet worden toegewezen en klik op **Next** om door te gaan.
Het **File System Settings** dialoogvenster wordt weergegeven.
7. Pas het volgende toe:
 - **File system: NTFS**
 - **Allocation unit size: Default**

- **Volume label:** voer hetzelfde volumelabel in als de schijf die defect is (of) die door een defecte schijf (**Data** of is vervangen **Data2**).
- 8. Klik op **Next** om verder te gaan.
Het **Confirmation** dialoogvenster wordt weergegeven.
- 9. Controleer of alle instellingen correct zijn en klik op **Create**.
Het systeem begint met het maken van de nieuwe partitie en volume.
Nadat de instelling is voltooid, wordt **Results** het dialoogvenster weergegeven.
- 10. Klik hierop **Next** om door te gaan.
De nieuwe partitie en volume zijn gemaakt en alle opslagruimte wordt toegewezen.

De serverservice inschakelen

1. Selecteer in het **startmenu** van Windows **Services**.
Het **Services** dialoogvenster wordt weergegeven.
2. Zoek de **Server**-service in de lijst en dubbelklik erop.
Het dialoogvenster **Server Properties** wordt weergegeven.
3. Selecteer onder het tabblad **General**, in de **Startup type**-lijst, **Manual** en klik vervolgens op **Apply**.
4. Klik onder **Service status**: Service status: om de service **Start** te starten en klik vervolgens op **OK** om de wijzigingen toe te passen. Sluit vervolgens het dialoogvenster **Services**.

LUN's aanmaken (iSCSI virtuele schijven)

1. Selecteer in het menu **Start** van Windows **Server Manager** en selecteer vervolgens **File and Storage Services > iSCSI**.
Alle virtuele iSCSI-schijven op uw systeem worden weergegeven.
2. Klik met de rechtermuisknop op de LUN (de virtuele iSCSI-schijf) van de vervangen vaste schijf met de status **Error**, en klik vervolgens op **Remove iSCSI Virtual Disk**.
Het dialoogvenster **Remove iSCSI Virtual Disk** wordt weergegeven.
3. Klik op **OK** om het verwijderen van de LUN te bevestigen.
4. Herhaal deze stappen voor alle LUN's met de status **Error**.
5. Rechtsklik in het dialoogvenster **iSCSI VIRTUAL DISKS** op een lege ruimte en klik vervolgens op **New iSCSI Virtual Disk...**
Het dialoogvenster **iSCSI Virtual Disk Location** wordt weergegeven.
6. Selecteer **Server** onder de betreffende server, selecteer onder **Storage location: Type a custom path** en voer de letter in die u aan de nieuwe harde schijf hebt toegewezen (*Nieuwe partitie en volume aanmaken, pagina 18*). Klik vervolgens op **Next** om verder te gaan.
Het **iSCSI Virtual Disk Name** dialoogvenster wordt weergegeven.
7. Geef de naam van de LUN in het veld **Name:** op. Klik vervolgens op **Next** om verder te gaan.
Het **iSCSI Virtual Disk Size** dialoogvenster wordt weergegeven.
8. Voer in het veld **Size** 2000 in en wijzig de grootte van de eenheid in **GB**.
Als er minder dan 2000 GB beschikbaar is, configureert u de grootte van de LUN op de beschikbare GB-ruimte min 50 MB.
9. Maak onder **Fixed size:** het selectievakje **Clear the virtual disk on allocation** leeg. Klik vervolgens op **Next** om verder te gaan.
Het **iSCSI Target** dialoogvenster wordt weergegeven.
10. Selecteer onder **Existing iSCSI target:** **TG0**. Klik vervolgens op **Next** om verder te gaan.
Het **Confirmation** dialoogvenster wordt weergegeven.

11. Controleer of alle instellingen correct zijn en klik op **Create**.
Het systeem begint met het maken van de nieuwe virtuele iSCSI-schijf.
Nadat de instelling is voltooid, wordt het dialoogvenster **Results** weergegeven.
12. Klik op **Close** om het dialoogvenster te sluiten.
13. Herhaal deze stappen om meer LUN's te maken met alle beschikbare ruimte.
14. Nadat alle LUN's zijn toegevoegd, worden deze in de lijst **iSCSI VIRTUAL DISKS** weergegeven.

De serverservice uitschakelen

1. Selecteer in het **startmenu** van Windows **Services**.
Het **Services** dialoogvenster wordt weergegeven.
2. Zoek de **Server**-service in de lijst en dubbelklik erop.
Het dialoogvenster **Server Properties** wordt weergegeven.
3. Klik op het tabblad **General** onder **Service status**: Service status: op om de **Stop**-service te stoppen.
4. Selecteer in de lijst **Startup type: Disabled** en klik vervolgens op **Apply**.
5. Klik op **OK** om de wijzigingen toe te passen en sluit vervolgens het dialoogvenster **Services**.

LUN's formatteren

1. Start de BVMS Configuration Client.
2. Navigeer in de **Apparaatstructuur** naar de pool met de defecte harde schijf, rechtsklik op het iSCSI-doel **TG0** en klik dan op **Doel scannen** om de lijst met beschikbare LUN's op dit iSCSI-doel bij te werken.
Hierdoor worden de LUN's die aan de defecte harde schijf zijn gekoppeld verwijderd en worden de LUN's toegevoegd die op de nieuwe harde schijf zijn gemaakt.
3. In **het dialoogvenster LUN's** worden alle beschikbare LUN's met hun status weergegeven (geformatteerd of ongeformatteerd).
4. Selecteer de ongeformatteerde LUN's en klik op **LUN formatteren** Format LUN. Klik vervolgens op **OK** om door te gaan.
5. Nadat het formatteren is voltooid, wordt een bevestigingsvenster weergegeven. Klik op **OK** om het proces te voltooien.

7.4

Logboekbestanden van de DIVAR IP-systeembeheerder verzamelen

De toepassing DIVAR IP System Manager bevat een speciaal script dat de verzameling logboekbestanden vereenvoudigt.

Logboekbestanden van de DIVAR IP System Manager verzamelt u als volgt:

1. Meld u aan bij het beheerdersaccount (raadpleeg *Aanmelden bij het beheerdersaccount, pagina 17*).
2. Klik in het menu **Start** van Windows op **Export System Manager Logs**.
Het script exporteert de logboekbestanden naar de map *Documents\Bosch* en maakt een ZIP-bestand met de volgende naamstructuur *SysMgrLogs-[date]_[time]*.
U kunt dit ZIP-bestand gebruiken om het aan de gedetailleerde foutbeschrijving te bevestigen.

7.5

Het apparaat herstellen

Herstellen van de unit:

1. Zet het apparaat aan en druk op F7 tijdens de BIOS power-on-zelftest om Windows PE te openen.
Het dialoogvenster **System Management Utility** wordt weergegeven.
2. Selecteer een van de volgende opties:
 - **System factory default:** deze optie formatteert videodata-partities en herstelt de partitie van het besturingssysteem met de fabrieksinstellingen.
Dit proces kan tot 5 minuten duren.
 - **Full data overwrite and system factory default:** deze optie formatteert videodata-partities, overschrijft bestaande gegevens helemaal en herstelt de besturingssysteem-partitie met de fabrieksinstellingen.
Dit proces kan tot 48 uren duren.
 - **OS system recovery only:** deze optie herstelt de partitie van het besturingssysteem met de fabrieksinstellingen en importeert bestaande virtuele stations van bestaande videodata.
Dit proces kan 5 minuten duren.

Opmerking:

De **OS system recovery only** optie verwijdert geen videobeelden die op de data HDD's zijn opgeslagen. Deze optie vervangt echter de volledige besturingssysteempartitie (inclusief de instellingen van het videomanagementsysteem) door een standaardconfiguratie. Om na het herstel toegang tot bestaand videomateriaal te krijgen, moet de configuratie van het videomanagementsysteem voor het systeemherstel worden geëxporteerd en daarna weer geïmporteerd.

**Opmerking!**

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

3. Bevestig de geselecteerde optie.
Het systeem start het formatterings- en herstelproces.
4. Bevestig het opnieuw starten van het systeem nadat het herstelproces is voltooid.
Het systeem start opnieuw op en de instelroutines worden uitgevoerd.
5. Nadat het proces is voltooid, wordt het taalselectiescherm van Windows weergegeven.
6. Ga verder met de eerste systeeminstelling.

Raadpleeg

- *Eerste aanmelding en eerste systeeminstallatie, pagina 9*

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.

U vindt de nieuwste software en beschikbare upgradepakketten in het downloadgedeelte van Bosch Security and Safety Systems onder:

<https://downloadstore.boschsecurity.com/>

8.2 Ondersteuningsservices en Bosch Academy



Ondersteuning

Ga naar onze **ondersteuningsservices** op www.boschsecurity.com/xc/en/support/.



Bosch Building Technologies Academy

Bezoek de website van Bosch Building Technologies Academy voor toegang tot

trainingscursussen, videozelfstudies en **documenten**: www.boschsecurity.com/xc/en/support/training/

Bosch Security Systems B.V.

Torenallee 49

5617 BA Eindhoven

Nederland

www.boschsecurity.nl

© Bosch Security Systems B.V., 2022

Building solutions for a better life.

202211241440