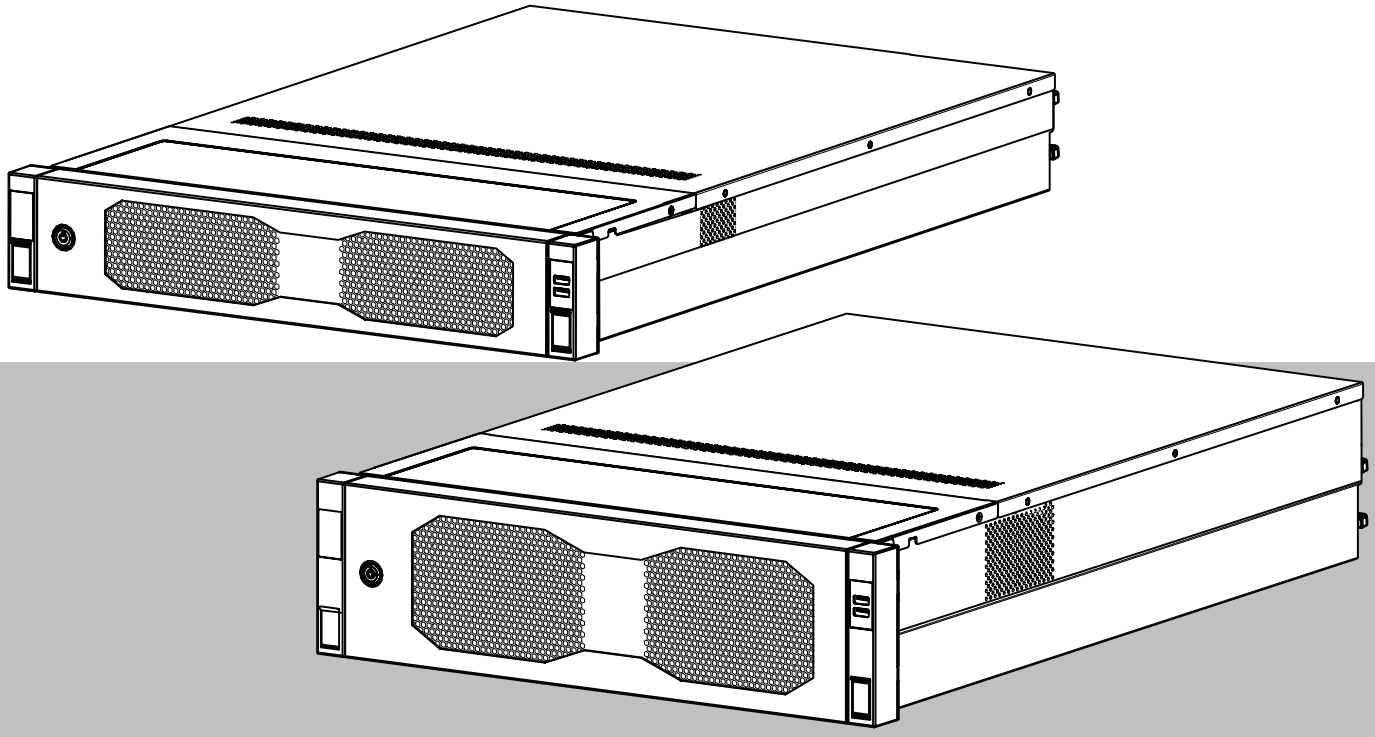
DIVAR IP all-in-one 7000 2U | DIVAR IP all-in-one 7000 3U

DIP-74C0-00N | DIP-74C4-8HD | DIP-74C8-8HD | DIP-74CI-8HD | DIP-74CI-12HD | DIP-74G0-00N | DIP-74GI-16HD



nl Bedieningshandleiding

Inhoudsopgave

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 cyber security

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 de voorkant om te voorkomen dat onbevoegden de harde schijven verwijderen. Verwijder de sleutel altijd uit het slot en sla deze op een veilige plaats op.
- Gebruik de functie Chassis Intrusion Sensor om ongeautoriseerde fysieke toegang tot de binnenkant van het apparaat te detecteren.
- 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.
- Houd de webbrowser altijd up-to-date om ervoor te zorgen dat deze veilig is en goed werkt.
- Schakel Windows Defender en de Windows firewall niet uit, en zorg ervoor dat deze altijd up-to-date zijn. Installeer geen extra antivirussoftware die de beveiligingsconfiguraties kan verstoren.
- 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.

Gebruikers die zijn aangemeld bij het beheerdersaccount kunnen firewalls doorkruisen 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. Om malware-aanvallen te voorkomen moet u ervoor zorgen dat geen geïnfecteerde USB-apparaten op het systeem worden aangesloten.
- Wijzig de BIOS UEFI-instellingen niet. Als u de BIOS UEFI-instellingen wijzigt, kan dit het systeem nadelig beïnvloeden of storingen veroorzaken.
- Het BMC-systeem mag niet worden verbonden met het openbare netwerk.

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
- Beveiligingsinformatie, die potentiële effecten veroorzaakt door kwetsbaarheden van derden behandelt: https://www.boschsecurity.com/us/en/support/product-security/security-information.html

Als u updates over nieuwe beveiligingsberichten wilt ontvangen, kunt u zich abonneren op de RSS-feeds op de pagina Beveiligingsberichten van Bosch Security and Safety Systems: 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 Introductie

DIVAR IP all-in-one 7000 is een betaalbare en gebruiksvriendelijke alles-in-één oplossing voor het opnemen, bekijken en beheren van netwerkbewakingssystemen tot 256 kanalen (met 8 vooraf gelicentieerde kanalen).
DIVAR IP all-in-one 7000 2U/3U is een 2U/3U rackmount 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 7000 maakt gebruik van embedded ontwerp en kerncomponenten, en is gebaseerd op het besturingssysteem Microsoft Windows Server IoT 2022 for Storage Standard en beschikt over 'enterprise-rated' hot-swappable SATA-harde schijven, die tot 216/288 TB aan opslagcapaciteit bieden.

3 Systeemoverzicht

Besturingssysteem

Het Microsoft Windows Server IoT 2022 for Storage Standard-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 Standard 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.

Bedrijfsmodi

DIVAR IP all-in-one 7000-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.
– Geavanceerde oplossing voor video-opname voor een BVMS-systeem, met gebruikmaking van de Video Recording Manager kerncomponenten en diensten, waarbij gebruik wordt gemaakt van de unieke mogelijkheden van Bosch camera's en opnameoplossingen. Er kunnen maximaal twee Video Recording Manager-servers worden toegevoegd aan een BVMS- systeem dat draait op een DIVAR IP all-in-one-apparaat.
– iSCSI-opslaguitbreiding voor een BVMS-systeem, dat op andere hardware draait. Er kunnen maximaal vier van deze iSCSI-opslaguitbreidingen worden toegevoegd aan een BVMS-systeem dat op een DIVAR IP all-in-one 7000-apparaat 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
  - Het wachtwoord moet tekens uit drie van de volgende vier categorieën bevatten:
    Ten minste één hoofdletter.
    Ten minste één kleine letter.
    Ten minste een cijfer.
    Ten minste één speciaal teken.

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.

Opmerking!
Om veiligheidsredenen worden dialoogvensters Voor gebruikersaccountbeheer (UAC) weergegeven waarin u wordt gevraagd of u de beoogde wijzigingen in uw systeem wilt aanbrengen. U kunt pas verder gaan met de installatie nadat u hebt bevestigd dat u de betreffende wijzigingen wilt aanbrengen.

Het systeem configureren:

1. Sluit de DIVAR IP all-in-one-eenheid en de camera's aan op het netwerk.
2. Schakel de eenheid in.
   Wacht tot het BIOS-scherm wordt weergegeven en de installatieroutines Microsoft Windows Server IoT 2022 for Storage Standard 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
– Het wachtwoord moet tekens uit drie van de volgende vier categorieën bevatten:
  – Ten minste één hoofdletter.
  – Ten minste één kleine letter.
  – Ten minste een cijfer.
  – Ten minste één speciaal teken.

   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.
   Opmerking: zorg ervoor dat de laatste versie van DIVAR IP System Manager is geïnstalleerd. U vindt de nieuwste software en beschikbare upgradepakketten in het downloadgedeelte van Bosch Security and Safety Systems onder: https://downloadstore.boschsecurity.com/.
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 vervolgens op **Accept** om door te gaan.
10. Klik in de volgende dialoogvensters voor Gebruikersaccountbeheer op **Yes** om door te gaan. De installatie begint.
11. Nadat de installatie is voltooid, wordt het systeem opnieuw opgestart en wordt u naar de Windows-aanmeldingspagina geleid. Meld u aan bij de beheerdersaccount.
12. De Microsoft Edge browser opent 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 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. Op de pagina **DIVAR IP - Systeeminstellingen** selecteert u de werkingsmodus **BVMS** en de gewenste BVMS-versie die u wilt installeren, klikt u vervolgens op **Bedieningsmodus installeren**.
   De BVMS-licentieovereenkomst wordt weergegeven.

2. Lees en accepteer de licentieovereenkomst, klik dan op **Ja, 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 **Bedieningsmodus installeren**.
   De VRM-licentieovereenkomst wordt weergegeven.
2. Lees en accepteer de licentieovereenkomst, klik dan op **Ja, 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 **Bedieningsmodus installeren**.
   Het installatiedialoogvenster wordt weergegeven.
2. Klik in het installatiedialoogvenster op **Ja, installeren** om verder te gaan.
   De installatie start en het installatiedialoogvenster toont de voortgang ervan. Zet het systeem niet uit en verwijder het opslagmedium 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

Zorg ervoor dat u upgradet DIVAR IP System Manager naar de nieuwste versie.

5.1 Upgraden DIVAR IP System Manager

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 het ZIP-bestand **SystemManager_[software version 2.3.0 of hoger].zip** en sla het op een opslagmedium op, zoals een USB-stick.
4. Pak het bestand op het opslagmedium uit.
5. Sluit vervolgens het opslagmedium aan op uw DIVAR IP all-in-one-apparaat.
6. Start DIVAR IP System Manager:
   - Als u zich met het **BVRAdmin**-beheerdersaccount bij Windows hebt aangemeld, dubbelklikt u op het Windows-bureaublad op het pictogramDIVAR IP System Manager.
     DIVAR IP System Manager wordt gestart.
   - Als uw systeem in de bedrijfsmodus BVMS draait, klikt u op het pictogram DIVAR IP System Manager op het bureaublad BVMS en meldt u zich aan bij de beheerdersaccount BVRAdmin. DIVAR IP System Manager wordt geopend in een dialoogvenster op een volledig scherm (U kunt het dialoogvenster afsluiten door op Alt+ F4 te drukken).
7. De pagina**Softwarepakketten** wordt weergegeven. Selecteer het softwarepakket DIVAR IP System Manager en klik vervolgens op **Pakket installeren** om door te gaan.
   Het dialoogvenster voor de installatie wordt weergegeven.
8. Klik in het installatiedialoogvenster op **Ja, installeren** om door te gaan.
   De installatie begint.
   Het installatieproces kan enkele minuten duren. Schakel het systeem niet uit en verwijder het opslagmedium niet tijdens het installatieproces.
   Let op de meldingen die bovenaan de pagina worden weergegeven.

5.2 De software upgraden met behulp van DIVAR IP System Manager

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 DIVAR IP System Manager:
   - Als u zich met het **BVRAdmin**-beheerdersaccount bij Windows hebt aangemeld, dubbelklikt u op het Windows-bureaublad op het pictogramDIVAR IP System Manager.
     DIVAR IP System Manager wordt gestart.
   - Als uw systeem in de bedrijfsmodus BVMS draait, klikt u op het pictogram DIVAR IP System Manager op het bureaublad BVMS en meldt u zich aan bij de beheerdersaccount BVRAdmin. DIVAR IP System Manager wordt geopend in een dialoogvenster op een volledig scherm (U kunt het dialoogvenster afsluiten door op 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 van softwarepakket** 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 van softwarepakket** 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 **Pakket installeren**.
   Er wordt indien van toepassing een dialoogvenster voor een licentieovereenkomst weergegeven.
9. Lees en accepteer de licentieovereenkomst, klik vervolgens op **Ja, 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 met succes zijn geïnstalleerd, krijgt u een bevestiging dat de installatie is gelukt.
11. Als de installatie niet gelukt is, ontvangt u een bericht met informatie over hoe u in dat geval verder moet gaan.

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 18*.
2. *Het doorsturen van poorten instellen, pagina 18*.
3. *Een geschikte client kiezen, pagina 18*.

U kunt ook verbinding maken met uw DIVAR IP all-in-one via Bosch Remote Portal en gebruik maken van de huidige en toekomstige functionaliteit die beschikbaar is via Remote Portal. Raadpleeg *Verbinding met Remote Portal, pagina 19* voor meer informatie.

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 19*.
- *Externe verbinding met de Video Security-app, pagina 19*.

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. Verzeker 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.

6.5 Verbinding met Remote Portal

U kunt verbinding maken met uw DIVAR IP all-in-one apparaat via Bosch Remote Portal en gebruik maken van huidige en toekomstige functionaliteit zoals de Bosch Remote System Management-service die beschikbaar is via Remote Portal.
Raadpleeg de Remote System Management-documentatie en het trainingsmateriaal voor gedetailleerde informatie over de Remote System Management-service.

Vereisten

Remote Portal-verbinding

Om DIVAR IP all-in-one-apparaten met de Remote Portal te verbinden, moet u ervoor zorgen dat aam de volgende vereisten wordt voldaan:

– DIVAR IP System Manager 2.3.0 (of hoger) moet op het apparaat zijn geïnstalleerd.
– Er moet een Remote Portal-account worden gemaakt.

Remote Portal-communicatie

Verbindingsvereisten voor de Remote Portal-communicatie.

Let op: Alle verbindingen zijn uitgaand.

HTTPS (Port 443)

– https://api.remote.boschsecurity.com/rest/iot/devices
– https://sw-repo-remote.s3.eu-central-1.amazonaws.com

MQTTS (Port 8883)

– tls://a1j83emmuys8gs-ats.iot.eu-central-1.amazonaws.com:8883

6.5.1 Een Remote Portal-account maken

Een Remote Portal-account maken:

1. Ga naar https://remote.boschsecurity.com/login.
2. Klik op **Sign up**.
3. Voer uw bedrijfsnaam en uw e-mail in.
4. Selecteer uw bedrijfsgebied.
5. Lees de algemene voorwaarden en de mededeling over gegevensbescherming en schakel de selectievakjes in om deze te accepteren.
6. Klik op **Sign up** om een account te maken.

6.5.2 DIVAR IP all-in-one-apparaten registreren op Remote Portal

Om een DIVAR IP all-in-one-apparaat te registreren op Remote Portal:

1. Start DIVAR IP System Manager.
2. Klik op het tabblad **Remote Portal-verbinding**.
3. Als u een bestaand Remote Portal-account hebt, voer dan uw e-mailadres en wachtwoord in en klik vervolgens op **Registreren** om uw DIVAR IP all-in-one-apparaat te registreren op Remote Portal.
4. Als uw e-mail is toegewezen aan meerdere bedrijfsaccounts met beheerdersrechten, wordt er een selectiedialoogvenster weergegeven met de respectieve bedrijfsaccounts. Selecteer in het selectiedialoogvenster de gewenste bedrijfsaccount waarop u uw DIVAR IP all-in-one apparaat wilt registreren.

Opmerking!

SingleKey ID

Bosch heeft SingleKey ID geïntroduceerd als een Identity Provider (IdP) om een centrale aanmelding bij alle Bosch-applicaties, services en platforms mogelijk te maken.

Om het apparaat met Remote Portal te verbinden door SingleKey ID te gebruiken, volgt u de instructies op het scherm.

5. Als u nog geen Remote Portal-account hebt, klik dan op **Account maken** om eerst een Remote Portal-account te maken. Raadpleeg .

6.5.3 DIVAR IP all-in-one-apparaten afmelden bij Remote Portal

Een DIVAR IP all-in-one-apparaat afmelden bij Remote Portal:

1. Start DIVAR IP System Manager.
2. Klik op het tabblad tabblad **Remote Portal connection**.

3. Klik op **Uitschrijven** om uw DIVAR IP all-in-one-apparaat uit de Remote Portal te verwijderen.
   Let op: Door het apparaat uit het Remote Portal te verwijderen, wordt de apparaatconfiguratie in het Remote Portal niet verwijderd. Om de apparaatconfiguratie te verwijderen, moet u zich aanmelden bij de betreffende Remote Portal-bedrijfsaccount.

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

7.2.1 Het systeem bewaken met de toepassing ASUS Inband Tool

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

De toepassingsservice is standaard geactiveerd.

Start de toepassing als volgt:

1. Meld u aan bij het beheerdersaccount (raadpleeg *Aanmelden bij het beheerdersaccount, pagina 22*).
2. Op het bureaublad opent u de map **Tools** en dubbelklikt u op de snelkoppeling ASUS Inband Tool.
   De toepassing wordt gestart.
3. Meld u aan met de volgende standaardgegevens:

– Account: **admin**
– Wachtwoord **admin**

4. Na de eerste keer aanmelden wordt u gevraagd dit initiële wachtwoord te wijzigen.
   Voer een nieuw wachtwoord in en bevestig het.
   Zorg ervoor dat u het nieuwe wachtwoord op een veilige plaats opslaat.
   Houd u aan de volgende wachtwoordvereisten:

– Wachtwoorden moeten uit minimaal 14 tekens bestaan.
– Wachtwoorden moeten ten minste één hoofdletter bevatten.
– Wachtwoorden moeten ten minste één kleine letter bevatten.
– Wachtwoorden moeten minstens één speciaal teken bevatten.
– Wachtwoorden moeten minimaal één nummer bevatten.

5. Nadat u het nieuwe wachtwoord bevestigd hebt, wordt de pagina **Dashboard** weergegeven waarop u de algemene status van het systeem kunt zien.
6. In het deelvenster **MENU** aan de linkerkant kunt u de respectieve pagina's selecteren om gedetailleerde informatie over de gezondheidsstatus van het systeem te ontvangen.
7. In het menu **SNMP** unt u SNMP-gebruikers en SMMP-bestemmingen instellen.

8. Op de pagina **Rapport** kunt u een rapport genereren dat de juiste informatie bevat die u hebt geselecteerd.

7.2.2 Het systeem bewaken met de BMC-webinterface

DIVAR IP all-in-one 7000 heeft aan de achterzijde een speciaal BMC-poort.
Elke DIVAR IP all-in-one 7000-eenheid wordt geleverd met de standaard BMC-gebruikersnaam **admin** en een initieel BMC-wachtwoord. Het initiële BMC-wachtwoord is voor elke eenheid uniek. U vindt dit op het label aan de achterzijde van de eenheid, onder de BMC-poort.
Na de eerste keer aanmelden bij de BMC-webinterface wordt u gevraagd om dit initiële wachtwoord te wijzigen. Sla het nieuwe wachtwoord op een veilige locatie op.
Neem de volgende wachtwoordvereisten in acht:
– Wachtwoorden moeten uit minimaal 14 tekens bestaan.
– Wachtwoorden moeten ten minste één hoofdletter bevatten.
– Wachtwoorden moeten ten minste één kleine letter bevatten.
– Wachtwoorden moeten minstens één speciaal teken bevatten.
– Wachtwoorden moeten minimaal één nummer bevatten.

Opmerking!
Sluit het apparaat om veiligheidsredenen niet aan op een openbaar netwerk via de BMC-poort.

De BMC-instellingen configureren
De BMC-instellingen configureren:
1. Schakel de eenheid in en druk op Del om naar de BIOS-instellingen te gaan.

Opmerking!
BIOS-wachtwoord
Het initiële BIOS-wachtwoord is voor elke eenheid uniek. U vindt dit op het label aan de achterzijde van de eenheid. Bosch raadt u daarom dringend aan dit eerste wachtwoord te wijzigen. Sla het nieuwe wachtwoord op een veilige locatie op.
Neem de volgende wachtwoordvereisten in acht:
- Wachtwoorden moeten uit minimaal 14 tekens bestaan.
- Wachtwoorden moeten ten minste één hoofdletter bevatten.
- Wachtwoorden moeten ten minste één kleine letter bevatten.
- Wachtwoorden moeten minstens één speciaal teken bevatten.
- Wachtwoorden moeten minimaal één nummer bevatten.

2. Navigeer in de BIOS-instellingen naar het tabblad **Server Mgmt**.
3. Selecteer de optie **BMC Network Configuration** en druk vervolgens op Enter.
4. Selecteer in het volgende dialoogvenster de optie **Configuration Address source**, en druk vervolgens op Enter.
   Het dialoogvenster **Configuration Address source** wordt weergegeven.
5. Op het tabblad **Configuration Address source**-dialoogvenster, selecteer de gewenste optie hoe het BMC-adres moet worden geconfigureerd en druk vervolgens op Enter.
6. Stel de gewenste netwerkconfiguratieparameters in.
7. Druk op F4 en op Enter om op te slaan en af te sluiten.
   De DIVAR IP all-in-one 7000 eenheid start opnieuw.

Bediening op afstand via de BMC iKVM-interface

Standaard zijn de DIVAR IP all-in-one 7000-apparaten bedoeld om te werken met één of twee lokale monitors, aangesloten op de HDMI-interfaces aan de achterkant van de eenheid. Als er geen lokale monitors zijn aangesloten op de HDMI-interfaces, kan de eenheid op afstand worden bediend via de BMC iKVM-interface.

Om externe bediening van het systeem mogelijk te maken:

1. Zorg ervoor dat er geen lokale HDMI-monitor is aangesloten op het systeem.
2. Meld u aan bij de BMC-webinterface.
3. Selecteer in het linkermenupaneel de pagina **Externe bediening.**
4. Klik op de knop **H5Viewer starten**.
   Er wordt een venster geopend dat de DIVAR IP all-in-one 7000-monitoruitvoer toont en de muis en het toetsenbord van de externe machine bedient.

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

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:

- 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 RAID5 met de nieuwe harde schijf opnieuw opbouwen

RAID5 automatische opnieuw opbouwen

1. Dubbelklik op de DIVAR IP all-in-one-desktop op de snelkoppeling **Launch LSA**.
   De toepassing **LSI Storage Authority** wordt gestart en de pagina **Remote Server Discovery** wordt weergegeven.
2. Meld u aan met de gegevens voor het beheerdersaccount **BVRAdmin**.
   Er wordt een dialoogvenster weergegeven dat laat zien dat er een controller met een kritiek probleem is.
3. Klik boven aan de pagina op **Controller selecteren** en klik vervolgens op de balk **Controller ID:** om de instellingen van de controller te openen.
   - Als u de defecte harde schijf nog niet hebt verwijderd, wordt deze weergegeven onder **Drives** > **Foreign Drives** > **Unconfigured Drives.**
   - Zodra u de defecte harde schijf hebt verwijderd en de nieuwe harde schijf hebt geïnstalleerd, start het systeem automatisch de nieuwe opbouw van RAID5 met de nieuwe harde schijf en geeft een voortgangsbalk de voortgang van het opnieuw opbouwen weer.
4. Nadat het opnieuw opbouwen is voltooid, wordt het pictogram  weergegeven.

RAID5 handmatig opnieuw opbouwen

Als de nieuwe opbouw van RAID5 van de nieuwe harde schijf niet automatisch start, doet u het volgende:

1. Selecteer in het dialoogvenster van de controllerinstellingen onder **Drives** > **Foreign Drives** > **Unconfigured Drives** de harde schijf met de status **Unconfigured Bad** en selecteer vervolgens **Make Unconfigured Good** in het rechterdeelvenster.
   Er wordt een dialoogvenster weergegeven.
2. Schakel het selectievakje **Confirm** in en klik vervolgens op **Yes, Make Unconfigured Good** om door te gaan.
   Het systeem start de nieuwe opbouw van RAID5 met de nieuwe harde schijf.
3. Nadat het opnieuw opbouwen is voltooid, wordt het pictogram  weergegeven.

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).
2. Klik met de rechtermuisknop in het menu **Start** van Windows op **Export System Manager Logs** en voer het script uit als beheerder.
   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 De eenheid 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**: Met deze optie worden videogegevenspartities geformatteerd en wordt de OS-partitie hersteld met de fabrieksinstellingen.
     Dit proces zal enkele minuten duren.
   - **Full data overwrite and system factory default**: Met deze optie worden videogegevenspartities geformatteerd, worden bestaande gegevens volledig overschreven en wordt de os-partitie hersteld met de fabrieksinstellingen.
     Opmerking: Dit proces kan enkele dagen duren.
   - **OS system recovery only**: Met deze optie wordt de OS-partitie hersteld met de fabrieksinstellingen en worden bestaande virtuele harde schijven geïmporteerd uit bestaande videogegevenspartities.
     Dit proces zal enkele 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 voltooid is, wordt het Windows taalkeuzescherm weergegeven.
6. Ga verder met de eerste installatie van het systeem.

8 Meer informatie

8.1 Aanvullende documentatie en clientsoftware

Ga voor meer informatie, softwaredownloads en documentatie naar de betreffende productpagina in de productcatalogus:
http://www.boschsecurity.com
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
Netherlands
www.boschsecurity.com

Oplossingen voor gebouwen voor een beter leven

202404171736