

MyEye

Video Recorder 4

Smart Video Recording up to 4 cameras

NL - Instructies en waarschuwingen voor installatie en gebruik

Nice

1 - INLEIDING	3
1.1 - Algemeen	3
1.2 - Veiligheidsinstructies	3
1.3 - Privacyverklaring	3
1.4 - Over deze gids	3
2 - BELANGRIJKE GEVAREN EN WAARSCHUWINGEN	4
2.1 – Elektrische veiligheid	4
2.2 - Milieu	4
2.3 - Bediening en dagelijks onderhoud	4
3 - INSTALLATIE	5
3.1 - Afmetingen	5
3.2 - Harde schijf installeren	5
3.3 – Aansluiting	6
4 - CONFIGURATIE	7
4.1 - Inbedrijfstelling	7
4.2 - De unit initialiseren	7
4.3 - Netwerkconfiguratie	8
4.4 - IP-camera's toevoegen	9
4.4.1 - IP-camera's initialiseren	9
4.4.2 - IP-camera's toevoegen via zoekresultaten	10
4.4.3 - IP-camera's handmatig toevoegen	11
4.5 - Het opslagschema voor video-opnames configureren	11
4.6 - Aanmelden bij de webinterface	13
5 - AANBEVELINGEN VOOR CYBERBEVEILIGING	13
6 - AANVULLENDE	14

1.1 - Algemeen

Deze snelstartgids (hierna de "gids" genoemd) beschrijft de functies, installatie en bediening van het apparaat.

1.2 - Veiligheidsinstructies

In de gids kunt u gecategoriseerde signaalwoorden van specifieke typen bekijken.

Waarschuwingssignalen	Betekenis
Waarschuwing	Geeft een middelmatig of laag risico aan dat kan leiden tot lichte of matige verwondingen als het gevaar niet wordt afgewend.
Attentie	Geeft een potentieel risico aan dat kan leiden tot materiële schade, gegevensverlies, lagere prestaties of onvoorspelbare resultaten als het risico niet wordt vermeden.
Annotatie	Geeft extra informatie als markering en aanvulling op de tekst.

1.3 - Privacyverklaring

Als apparaatgebruiker of gegevensbeheerder kunt u persoonlijke informatie van andere mensen verzamelen, zoals gezichten, vingerafdrukken, autoregistratienummers, e-mailadressen, telefoonnummers, gps-gegevens, enz. U moet voldoen aan de lokale privacywetten en -regelgeving om de legitieme rechten te beschermen en belangen van anderen door maatregelen te nemen, waaronder maar niet beperkt tot: duidelijke en zichtbare identificatie om de betrokkene te informeren over het bestaan van het monitoringgebied en zorgen voor passend contact.

1.4 - Over deze gids

- De gids is alleen ter referentie. In het geval van een discrepantie tussen de Gids en het daadwerkelijke product, prevaleert het daadwerkelijke product.
- Wij zijn niet verantwoordelijk voor eventuele verliezen veroorzaakt door operaties die niet in overeenstemming zijn met de Gids.
- De gids wordt bijgewerkt volgens de laatste wet- en regelgeving van gerelateerde regio's. Scan voor meer informatie de QR-code of bezoek onze officiële website. In het geval van een discrepantie tussen de papieren gebruikershandleiding en de elektronische versie, prevaleert de elektronische versie.
- Alle ontwerpen en software kunnen zonder voorafgaande schriftelijke kennisgeving worden gewijzigd. Productupdates kunnen enkele verschillen veroorzaken tussen het eigenlijke product en de Gids. Neem contact op met de klantenservice voor het nieuwste programma en aanvullende documentatie.
- Afwijkingen in specificaties, beschrijvingen van functies en bewerkingen of drukfouten kunnen voorkomen. Raadpleeg in geval van twijfel of geschillen onze huidige definitieve verduidelijking.
- Alle handelsmerken, geregistreerde handelsmerken en bedrijfsnamen in de Gids zijn het eigendom van hun respectieve eigenaars.
- Bezoek onze website en neem contact op met uw leverancier of klantenservice als u problemen ondervindt bij het gebruik van het apparaat.
- Raadpleeg bij twijfel of controversiële situaties onze actuele, definitieve uitleg.

2.1 - Elektrische veiligheid

- Alle hierin beschreven installaties en bewerkingen moeten voldoen aan de lokale elektrische veiligheidsvoorschriften.
- Gebruik een SELV-voeding (Safety Extra Low Voltage) en een voeding met een nominale spanning die voldoet aan de IEC60950-1 beperkte voedingsvereisten. Raadpleeg de apparaatlabels voor specifieke stroomvereisten.
- Voordat u het apparaat start, moet u ervoor zorgen dat het voedingsapparaat operationeel is.
- Er moet een gemakkelijk toegankelijke ontkoppelinrichting in de bedrading van het gebouw worden opgenomen.
- Zorg ervoor dat er niet op het netsnoer wordt gelopen en dat het niet bekneld raakt, met name de stekker, het stopcontact en de connector die uit het apparaat steken.

2.2 - Milieu

- Stel het apparaat niet bloot aan sterk geconcentreerd licht, zoals lamplicht of zonlicht; anders kan dit overmatige helderheid of heldere vlekken in het beeld veroorzaken, die geen defect van het apparaat zijn en de CMOS-levensduur (Complementaire metaaloxide halfgeleider) kunnen beïnvloeden.
- Plaats het apparaat niet in een vochtige of stoffige omgeving, bij zeer hoge of lage temperaturen, op plaatsen met sterke elektromagnetische straling of onstabiele verlichting.
- Houd het apparaat uit de buurt van vloeistoffen om schade aan interne onderdelen te voorkomen.
- Bescherm de binnenkant van het apparaat tegen regen of vocht om brand of bliksem te voorkomen.
- Zorg voor goede ventilatie om warmteopbouw te voorkomen.
- Transporteer, gebruik en bewaar het apparaat binnen het toegestane vochtigheids- en temperatuurbereik.
- Zware belastingen, hevige trillingen of waterspatten zijn niet toegestaan tijdens transport, opslag en installatie.
- Verpak het apparaat voor transport in een standaard fabrieksverpakking of vergelijkbaar materiaal.
- Installeer het apparaat op een plaats die alleen toegankelijk is voor professioneel personeel met voldoende kennis van veiligheidsmaatregelen en waarschuwingen. Onbedoeld letsel kan optreden bij niet-professionals die de montageruimte betreden terwijl de apparatuur normaal werkt.

2.3 - Bediening en dagelijks onderhoud

- Raak het warmteafvoerelement van het apparaat niet aan om brandwonden te voorkomen.
- Volg bij het demonteren van het apparaat nauwkeurig de instructies in de handleiding; onprofessionele demontage kan leiden tot waterlekage of slechte beeldkwaliteit. Neem contact op met de klantenservice om het droogmiddel te vervangen als er na het uitpakken condens op de lens verschijnt of als het droogmiddel groen wordt (niet alle modellen zijn uitgerust met een droogmiddel).
- Het wordt aanbevolen om het apparaat samen met een bliksemafleider te gebruiken om het bliksembeveiligingseffect te verbeteren.
- Het wordt aanbevolen om het aardingsgat met aarde te verbinden om de betrouwbaarheid van het apparaat te vergroten.
- Raak de beeldsensor (CMOS) niet rechtstreeks aan. Stof en vuil kunnen worden verwijderd met een blaasbalgje of de lens kan voorzichtig worden afgeveegd met een zachte doek die is bevochtigd met alcohol.
- De buitenkant van het apparaat kan worden gereinigd met een zachte, droge doek, die ook kan worden gebruikt om hardnekkige vlekken te verwijderen wanneer deze is bevochtigd met een mild reinigingsmiddel. Gebruik geen vluchtige oplosmiddelen zoals alcohol, benzeen, verdunner of sterke en schurende reinigingsmiddelen om mogelijke schade aan het oppervlak van de behuizing van de machine te voorkomen, wat zou kunnen leiden tot verminderde prestaties.
- De koepelafdekking is een optisch onderdeel, raak de afdekking niet rechtstreeks met uw handen aan of veeg deze af tijdens montage of gebruik. Om stof, vet of vingerafdrukken te verwijderen, veegt u af met een licht bevochtigde, olievrije diethylkatoen of een vochtige, zachte doek. Een blazer kan ook worden gebruikt om stof te verwijderen.

Waarschuwing

- Versterk de bescherming van uw netwerk, apparaatgegevens en persoonlijke informatie door maatregelen zoals, maar niet beperkt tot, het gebruik van een sterk wachtwoord, het regelmatig wijzigen van uw wachtwoord, het bijwerken van uw apparaatsoftware naar de nieuwste versie en het instellen van een privécomputer netwerk. Voor sommige apparaten met oude softwareversies wordt het ONVIF-wachtwoord niet automatisch gewijzigd wanneer het systeemwachtwoord wordt gewijzigd en moet u de software bijwerken of het ONVIF-wachtwoord handmatig bijwerken.
- Gebruik standaardcomponenten of accessoires van de fabrikant en zorg ervoor dat het apparaat wordt geïnstalleerd en onderhouden door professionele monteurs.
- Het oppervlak van de beeldsensor mag niet worden blootgesteld aan laserstraling in de omgeving waar het laserstraalapparaat wordt gebruikt.
- Voed het apparaat niet met twee of meer voedingsbronnen. Tenzij anders vermeld. Het niet opvolgen van deze instructies kan het apparaat beschadigen.

3 INSTALLATIE

Let op

Alle installatie- en bedieningshandelingen die hier worden beschreven, moeten voldoen aan de plaatselijke elektrische veiligheidsvoorschriften. Het apparaat is niet geschikt voor wandmontage met het voorpaneel naar beneden gericht.

- De volgende afbeeldingen dienen alleen ter referentie. Het daadwerkelijke product is doorslaggevend.

3.1 - Afmetingen

De volgende afbeeldingen dienen alleen ter referentie, het daadwerkelijke product is doorslaggevend.

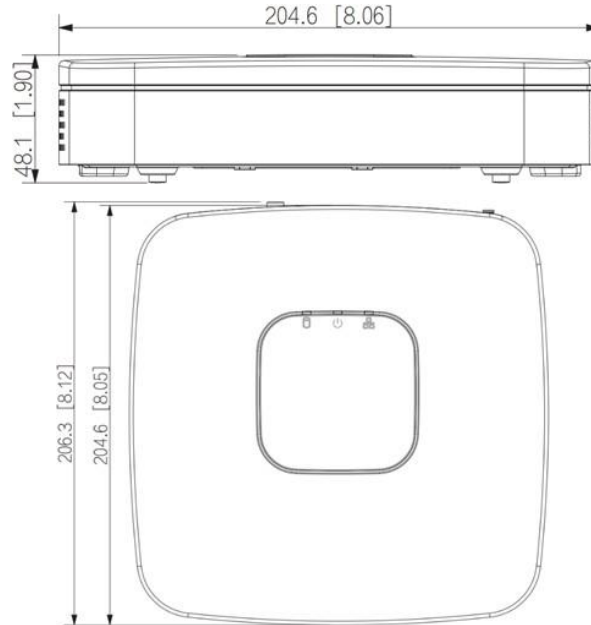
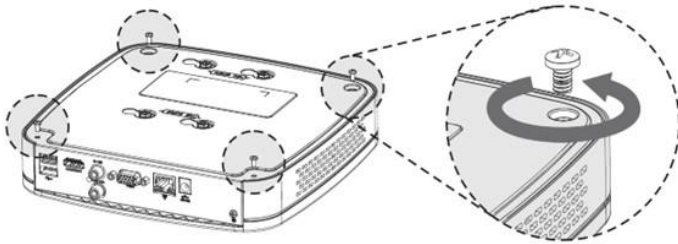


Figure 3-1 Dimensions (Unit: mm[inch])

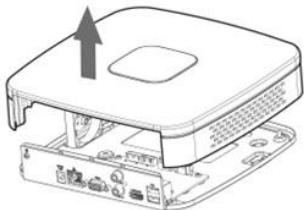
3.2 - Harde schijf installeren

Schakel de NVR uit en haal de stekker uit het stopcontact voordat u het deksel opent om de HDD te vervangen. Controleer tijdens de eerste installatie of de HDD al is geïnstalleerd. Het wordt aanbevolen HDD's van ondernemingsniveau of bewakingsniveau te gebruiken. Het gebruik van een harde schijf voor pc's wordt afgeraden.

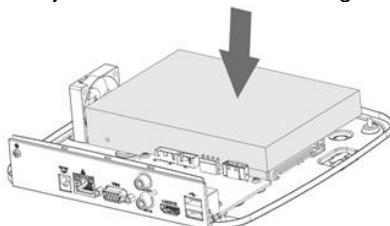
1. Draai het apparaat om en verwijder de vier bevestigingsschroeven op de basiskaart.



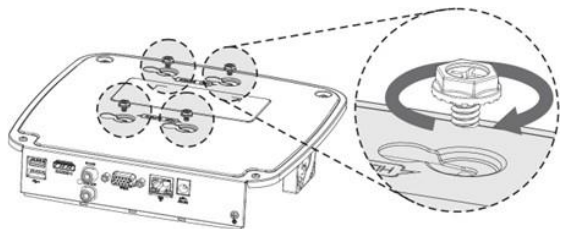
2. Draai het apparaat om en verwijder de vier bevestigingsschroeven op de basiskaart.



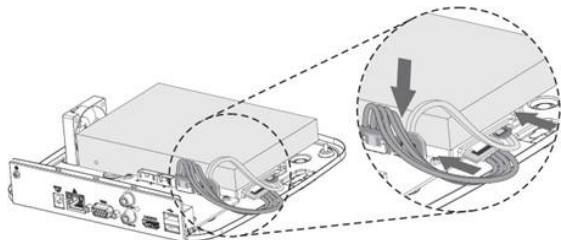
3. Verwijder het deksel in de richting van de volgende pijl.



4. Draai het apparaat ondersteboven, zorg dat de schroeven overeenkomen met de gaten op de HDD en maak ze vast. De HDD zit vast op de basiskaart.



5. Sluit de datakabel van de HDD en de voedingskabel aan op het apparaat.

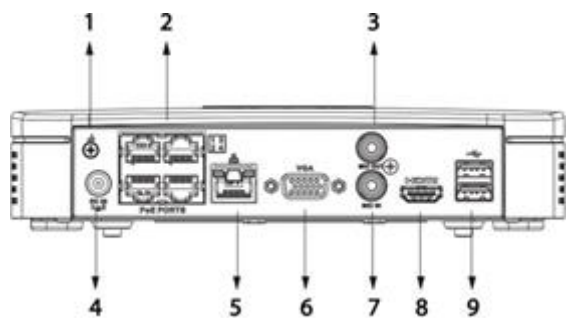


6. Plaats het deksel terug en draai de vier schroeven op de basiskaart vast om de installatie te voltooien.



3.3 - Aansluiting

- De volgende afbeeldingen dienen alleen ter referentie. Het daadwerkelijke product is doorslaggevend.
- Controleer de pictogrammen op het achterpaneel zorgvuldig en raadpleeg het daadwerkelijke product voor gedetailleerde informatie.
- Als het pictogram (DC12V) is, voert u 12V gelijkstroom in. Als het pictogram (DC48V) is, voert u een gelijkstroomvoeding van 48 V in.



- | | | | |
|---|-------------------------------|---|----------------|
| 1 | Aarding | 2 | PoE-poorten |
| 3 | AUDIO OUT, RCA-connector | 4 | Voedingsingang |
| 5 | Netwerkpoort | 6 | VGA-poort |
| 7 | AUDIO-ingang, RCA-aansluiting | 8 | HDMI-poort |
| 9 | USB-poorten | | |

4 CONFIGURATIE

4.1 - Inbedrijfstelling

Controleer voor ingebruikname of

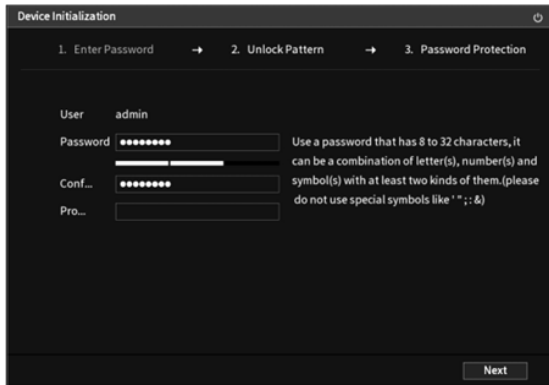
- De nominale ingangsspanning overeenkomt met de voedingsvereisten van de NVR (Netwerk Videorecorder).
- De voedingskabel is aangesloten.
- Om de veiligheid van de eenheid te garanderen, sluit u de NVR eerst aan op de voeding en vervolgens op het stopcontact.
- Gebruik altijd een stabiele stroomsterkte. Het wordt aanbevolen om een UPS te gebruiken als voedingsbron.
- Apparaten van sommige series hebben geen aan/uit-knop. Het apparaat kan worden ingeschakeld wanneer de voeding is aangesloten.

Sluit het apparaat met een HDMI-kabel aan op een monitor of tv, steek de stekker in het stopcontact en druk vervolgens op de aan/uit-knop om het apparaat op te starten.

4.2 - De unit initialiseren

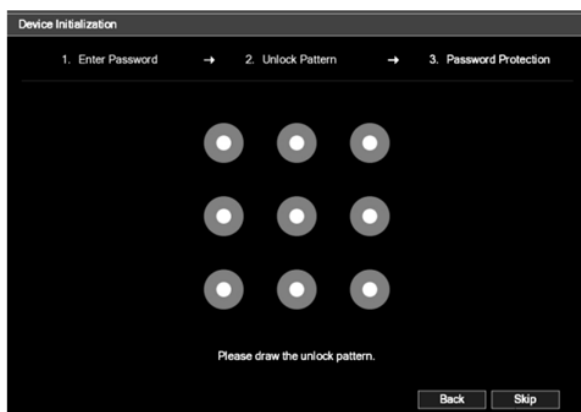
Tijdens de eerste opstart moet de wachtwoordinformatie voor de beheerder worden geconfigureerd (standaard). Om de veiligheid van het apparaat te garanderen, moet het inlogwachtwoord voor de beheerder goed worden verborgen en regelmatig worden gewijzigd.

1. Schakel het apparaat in. De initialisatie-interface van het apparaat wordt weergegeven
2. Stel de locatie, taal en videostandaard in. Selecteer naar wens de regio, taal en videostandaard in de vervolgkeuzelijst.
3. Lees de Softwarelicentieovereenkomst en selecteer "Ik heb alle voorwaarden gelezen en accepteer deze".
4. Selecteer een tijdzone en configureer de systeemtijd.
5. Configureer de wachtwoordinformatie voor de beheerder. Raadpleeg de volgende tabel voor meer informatie.



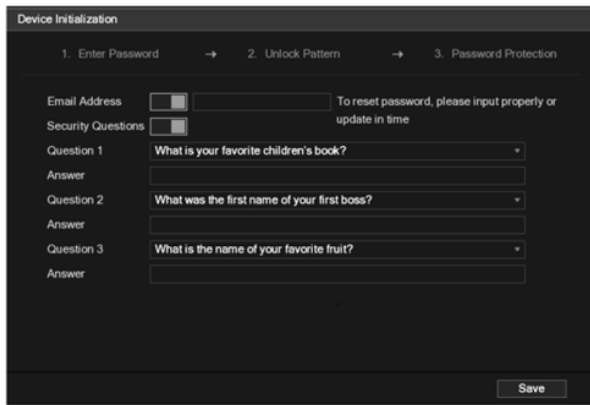
P	D
Gebruiker	De standaardgebruiker is admin.
Wachtwoord	Voer in het veld Wachtwoord het beheerderswachtwoord in. Het nieuwe wachtwoord kan tussen 8 en 32 tekens bevatten.
Bevestig wachtwoord	De tekens moeten ten minste twee soorten cijfers, letters en speciale tekens bevatten (uitgezonderd "!", ":", "&").
Ondersteunende vraag	Voer in het veld Prompt Question (Vraag) informatie in die u aan uw wachtwoord kan herinneren.

6. Gebruik de muis om een ontgrendelingspatroon te tekenen en teken het dan nogmaals ter bevestiging.




- Het patroon dat u wilt instellen moet minstens vier punten doorkruisen.
- Als u het ontgrendelingspatroon niet wilt configureren, klikt u op Overslaan.
- Zodra u het ontgrendelingspatroon hebt geconfigureerd, wordt het gebruikt als de standaard verificatiemethode. Als u deze instellingsoptie overslaat, voert u het wachtwoord voor aanmelding in

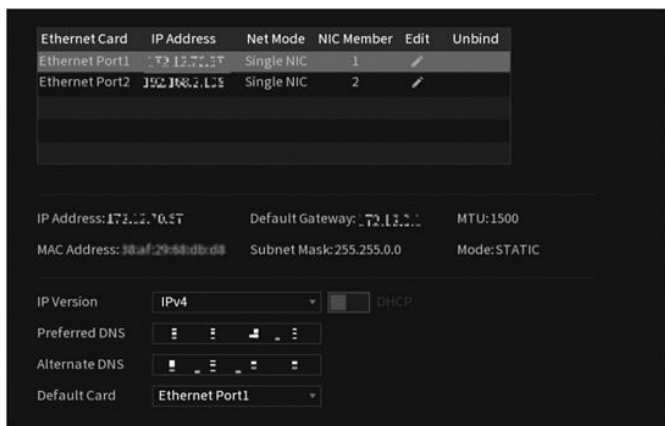
7. Pas het gereserveerde e-mailadres en de beveiligingsvragen toe op de NVR.



- Schakel het selectievakje E-mailadres in en voer het e-mailadres in.
 - Schakel het selectievakje Beveiligingsvragen inschakelen in en voer de antwoorden op deze vragen in.
 - Als het wachtwoord voor de beheerder eenmaal is geconfigureerd, kunt u het opnieuw instellen met het gereserveerde e-mailadres of de beveiligingsvragen.
 - Als je geen instellingen wilt configureren, schakel dan de functies e-mailadres en beveiligingsvragen uit in de interface.
8. Klik op OK om de initialisatie te voltooien.

4.3 - Netwerkconfiguratie

Selecteer Hoofdmenu > Netwerk > TCP/IP. De TCP/IP-interface wordt weergegeven. Klik op  om het IP-adres te wijzigen volgens uw huidige thuisadres uw thuisnetwerkinstellingen (het standaard IP-adres is 192.168.1.108)



Parameter	Beschrijving
IP-versie	Je kunt IPv4 of IPv6 selecteren in de lijst IP-versie. Beide versies worden ondersteund voor toegangsdoeleinden.
MAC-adres	Geeft het MAC-adres van de NVR weer.
DHCP	De DHCP-functie inschakelen. Het IP-adres, subnetmasker en standaardgateway zijn niet beschikbaar voor configuratie wanneer DHCP is ingeschakeld. <ul style="list-style-type: none"> • Als de DHCP-functie actief is, wordt de verkregen informatie weergegeven in de velden IP-adres, Subnetmasker en Standaardgateway. Anders geven alle waarden 0.0.0.0 aan. • Als de PPPoE-verbinding succesvol is, zijn het IP-adres, subnetmasker, standaardgateway en DHCP niet beschikbaar voor configuratie.
IP-adres	Voer het IP-adres in en configureer het juiste subnetmasker en de standaardgateway.
Subnetmasker	OPMERKING
Standaard gateway	Het IP-adres en de standaardgateway moeten zich op hetzelfde netwerksegment bevinden.
Voorkeur DNS	Voer het IP-adres van DNS in.
Alternatieve DNS	Voer het IP-adres van de alternatieve DNS in.
MTU	Voer de waarde voor de netwerkkaart in. De waarde varieert van 1280 tot 1500 bytes. De standaardwaarde is 1500. Aanbevolen MTU-waarden zijn als volgt. 1500: De grootste waarde van het Ethernet-informatiepakket. Deze waarde wordt meestal gekozen als er geen PPPoE- of VPN-verbinding is, en is ook de standaardwaarde voor sommige routers, netwerkkaarten en switches. 1492: Geoptimaliseerde waarde voor PPPoE. 1468: Geoptimaliseerde waarde voor DHCP. 1450: Geoptimaliseerde waarde voor VPN.
Test	Klik op Test om te controleren of het ingevoerde IP-adres en de gateway samenwerken.

4.4 - IP-camera's toevoegen

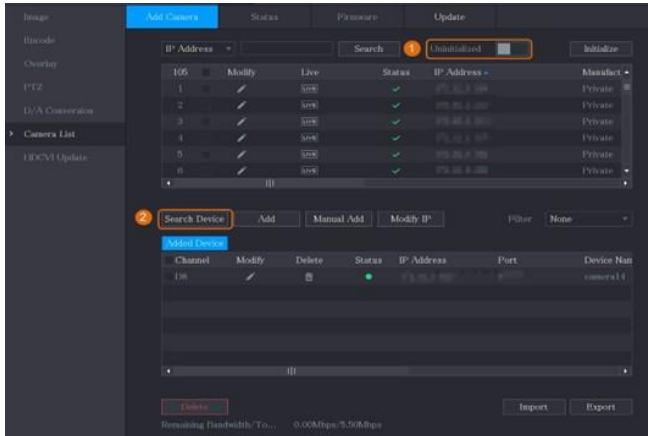
Een IP-camera kan worden toegevoegd op basis van zoekresultaten of door handmatig de IP-adresgegevens in te voeren.

4.4.1 - IP-camera's initialiseren

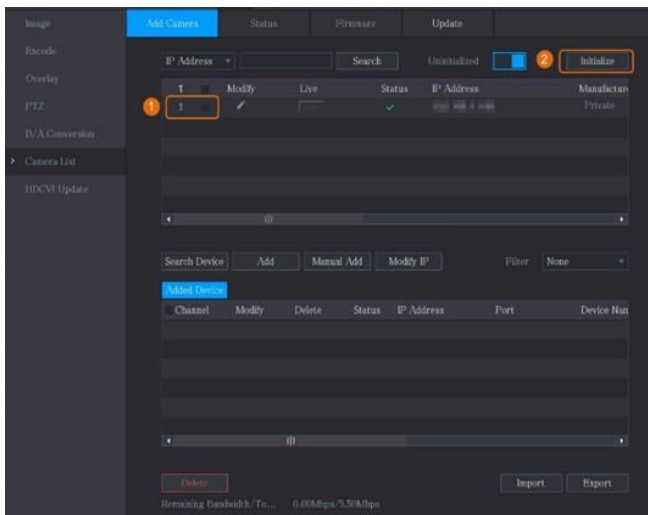
Dit onderwerp laat zien hoe u nieuwe camera's of camera's na een fabrieksreset initialiseert.

- Wanneer een camera op de NVR wordt aangesloten via de ingebouwde PoE-poort, initialiseert de NVR de camera automatisch. De camera accepteert standaard het NVR-wachtwoord en e-mailadres.

1. Selecteer Hoofdmenu > Camera > Cameralist > Camera toevoegen.
2. Schakel het selectievakje Niet geïnitieerd in en klik vervolgens op Apparaat zoeken.



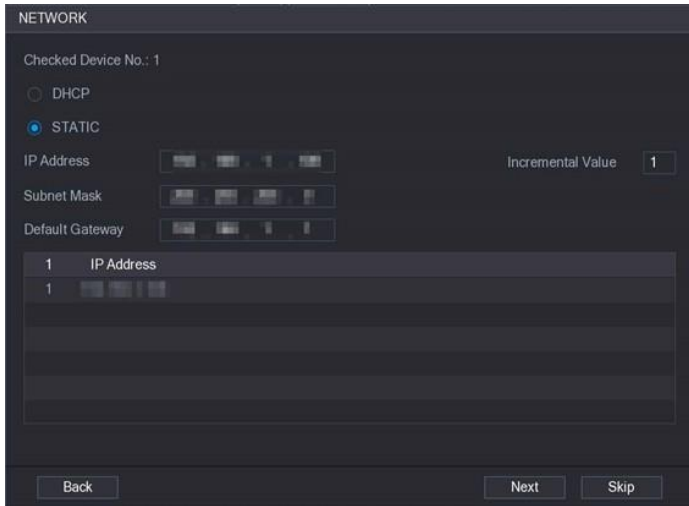
3. Selecteer de camera die u wilt initialiseren en klik vervolgens op de knop Initialiseren.



4. Pas het wachtwoord en de e-mailgegevens toe op de IP-camera.
 - Selecteer "Using current device password and email info" (Huidig wachtwoord en e-mailgegevens gebruiken) om dezelfde gegevens voor de camera te gebruiken als in de NVR.
 - Vink "Using current device password and email info" (Huidig apparaatwachtwoord en e-mailinfo gebruiken) uit om andere referenties voor de camera te definiëren.
5. Het IP-adres van de camera configureren
 - Selecteer DHCP als een DHCP-server is geïmplementeerd.
 - Selecteer Static (voorkeur) en voer vervolgens het IP-adres, subnetmasker, standaardgateway en incrementele waarde in.

Opmerking

- Stel de incrementele waarde in als u de IP-adressen van meerdere camera's tegelijk wilt wijzigen. De NVR zal incrementeel een waarde toevoegen aan de vierde sectie van het IP-adres na het toewijzen van een IP-adres voor deze camera's

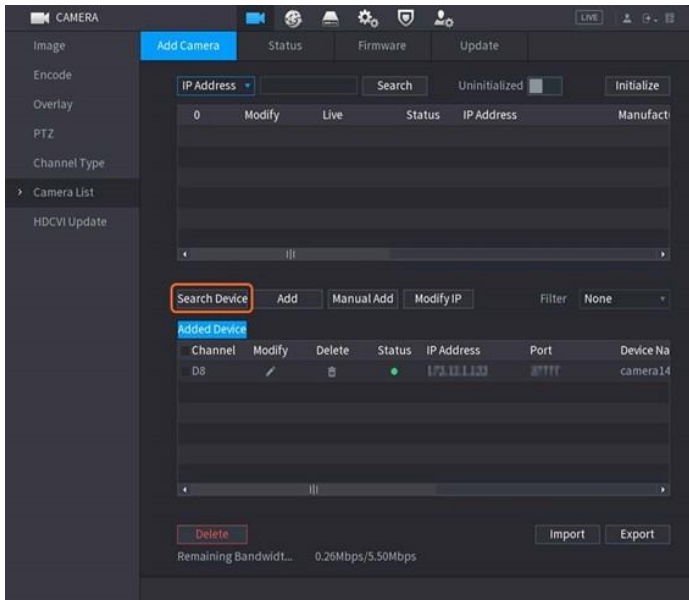


6. Klik op Volgende. Wacht 1-2 minuten tot de initialisatieprocedure is voltooid. Klik op Voltooid.

4.4.2 - IP-camera's toevoegen via zoekresultaten

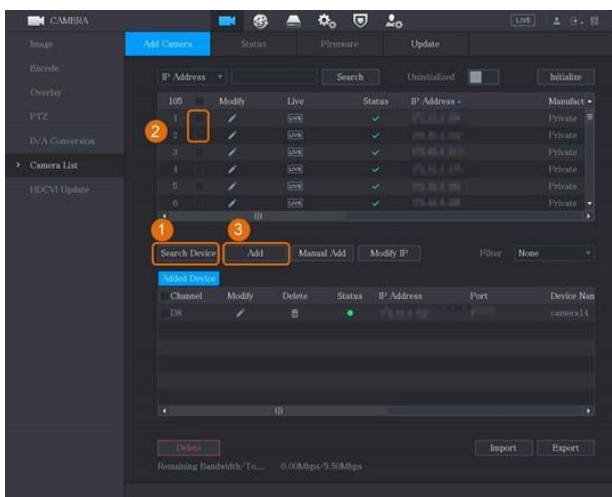
Zorg ervoor dat de camera's die u wilt toevoegen al zijn geïntialiseerd en op het juiste netwerk zijn aangesloten.

1. Selecteer Hoofdmenu > Camera > Cameralist > Camera toevoegen.
2. Klik op Een apparaat zoeken.



3. IP-camera's toevoegen:

- Toevoegen door te dubbelklikken: Dubbelklik op de doelcamera om deze toe te voegen aan de lijst met toegevoegde apparaten.
- Met deze methode kan slechts één camera tegelijk worden toegevoegd.
- Toevoegen via selectievakje: Selecteer het selectievakje van de doelcamera en klik vervolgens op Toevoegen om deze toe te voegen aan de lijst met toegevoegde apparaten.
- U kunt meer dan één selectievakje inschakelen en camera's in batches toevoegen.



- Als de status van de toegevoegde camera groen is, betekent dit dat de camera correct is toegevoegd aan de NVR.
- Als de status van de toegevoegde camera rood is, duidt dit op een verbindingfout tussen de camera en de NVR. Controleer de cameraparameters, zoals wachtwoord, protocol en kanaalnummer, en probeer de camera opnieuw toe te voegen.

4.4.3 - IP-camera's handmatig toevoegen

Per IP-informatie kan één IP-camera per keer worden toegevoegd.

Zorg ervoor dat de camera's die u wilt toevoegen al zijn geïnitieerd en aangesloten op het juiste netwerk.

1. Selecteer Hoofdmenu > Camera > Cameralijst > Camera toevoegen.
2. Klik op Handmatig toevoegen.
3. Configureer de parameters in het dialoogvenster Handmatig toevoegen.

Parameter	Beschrijving
Kanaal	Selecteer in de vervolgkeuzelijst Kanaal het kanaal dat u wilt dat de NVR gebruikt om verbinding te maken met het externe apparaat.
Producent	Selecteer de fabrikant van het externe apparaat in de vervolgkeuzelijst Fabrikant.
IP-adres	Voer het IP-adres van de IP-camera in het veld IP-adres in. <ul style="list-style-type: none"> • Wijzig de standaardwaarde (192.168.0.0) waarmee het systeem geen verbinding kan maken.
RTSP-poort	De standaardwaarde is 554. Deze waarde kan indien nodig worden gewijzigd.
HTTP-poort	De standaardwaarde is 80. Deze waarde kan indien nodig worden gewijzigd. <ul style="list-style-type: none"> • Als u een andere waarde invoert, bijvoorbeeld 70, voer dan 70 in na het IP-adres wanneer u zich aanmeldt bij de NVR via de browser.
TCP poort	De standaardwaarde is 37777, deze waarde kan indien nodig worden gewijzigd.
Naam gebruiker	Voer de gebruikersnaam van het externe apparaat in.
Wachtwoord	Voer het gebruikerswachtwoord van het externe apparaat in.
Remote CH.	Voer het kanaalnummer in van het externe apparaat dat u wilt toevoegen.
Decoderstrategie	Selecteer in de lijst Decoderstrategie de optie Standaard, Realtime of Fluent naar wens.
Type protocol	<ul style="list-style-type: none"> • Als de IP-camera wordt toegevoegd via een privéprotocol, selecteer dan TCP. • Als de IP-camera is toegevoegd via ONVIF, selecteer Auto, TCP, UDP of MULTICAST. • Als de IP-camera is toegevoegd via derden, selecteer dan TCP of UDP.
Codering	Als de IP-camera is toegevoegd via het ONVIF-protocol, zorgt het inschakelen van het selectievakje Encryptie voor encryptie van de verzonden gegevens. HTTPS moet ingeschakeld zijn voor de externe IP-camera om deze functie te kunnen gebruiken.

4.5 - Het opslagschema voor video-opnames configureren

Standaard nemen alle camera's 24 uur per dag continu video op. U kunt de instellingen indien nodig wijzigen.

1. Selecteer Hoofdmenu > Geheugen > Schema > Opname



2. Configureer de parameters.

Parameter	Beschrijving
Kanaal	Klik op de vervolgkeuzelijst Z-kanaal en selecteer een kanaal om de instellingen voor video-opname te wijzigen.
Vooropname	Stel in het veld Pre-opname de opnametijd in voor de extra video die vóór de gebeurtenis verschijnt om context te bieden voor de opname. Waardenbereik: 0 tot 30 s.
Overtolligheid	<p>Hiermee kunnen gebruikers een van de harde schijven instellen als redundante harde schijf om opgenomen bestanden op verschillende harde schijven op te slaan. In het geval van een storing aan de harde schijf, kan een back-up van de opname worden gevonden op de redundante harde schijf.</p> <ul style="list-style-type: none"> • Selecteer Hoofdmenu > OPSLAAN > Schijfbeheer en stel de HDD in als een redundante HDD. • Selecteer Hoofdmenu > OPSLAG > Schema > Opname en vink het vakje Redundantie aan. • Als het geselecteerde kanaal niet opneemt, wordt de redundatiefunctie van kracht bij de volgende opname, ongeacht of het vakje wel of niet is aangevinkt. • Als het geselecteerde kanaal wel opneemt, worden de momenteel opgenomen bestanden ingepakt en wordt de opname gestart volgens het nieuwe schema. • Deze functie is beschikbaar op geselecteerde modellen. • De redundante harde schijf maakt alleen back-ups van opgenomen video's, maar niet van snapshots.
Type gebeurtenis	<p>Schakel het selectievakje in voor het type gebeurtenis.</p> <p>Algemeen: Algemeen opnemen betekent dat de NVR alle video's binnen een bepaald tijdsinterval opneemt. Algemene opname wordt groen gemarkeerd.</p> <p>Beweging: Bewegingsopname betekent dat de NVR alleen video's opneemt wanneer bewegingsdetectie wordt geactiveerd. Bewegingsopname wordt weergegeven door de gele kleur.</p> <p>Alarm: Alarmopname betekent dat de NVR video opneemt wanneer een alarm wordt geactiveerd. Alarmopname wordt weergegeven door de kleur rood.</p> <p>M&A: M&A-opname combineert bewegingsopname en alarmopname. Het apparaat neemt video op wanneer beweging wordt gedetecteerd of een alarm wordt geactiveerd. M&A-opname wordt weergegeven door de kleur oranje.</p> <p>Smart: Smart-opname betekent dat de NVR video opneemt wanneer smart-detectie wordt geactiveerd. Smart recording wordt weergegeven door de kleur blauw.</p> <p>POS: POS-opname betekent dat de NVR video opneemt wanneer een POS-apparaat wordt gebruikt om betalingen te verrichten. POS-opname wordt weergegeven door de kleur paars.</p> <p>Smart: Smart-opname betekent dat de NVR video opneemt wanneer smart-detectie wordt geactiveerd. Smart recording wordt weergegeven door de kleur blauw.</p> <p>POS: POS-opname betekent dat de NVR video's opneemt wanneer een POS-apparaat wordt gebruikt om betalingen te verrichten. POS-opname wordt weergegeven door de kleur paars.</p>
Periode	Specificeert de periode waarin de geconfigureerde opname-instelling actief is. Het systeem activeert het alarm alleen tijdens de gedefinieerde periode.
Kopiëren naar	Klik op Kopiëren om de instellingen naar andere kanalen te kopiëren.

3. Stel de planning in door te tekenen of te bewerken

- Teken: houd de linkermuisknop ingedrukt en sleep de muis om een periode te tekenen
- Bewerken: klik om de periode  configureren en klik vervolgens op OK

4. Klik op Toepassen

- Het geconfigureerde opnameschema kan alleen van kracht worden als de automatische opnamefunctie is ingeschakeld.

4.6 - Aanmelden bij de webinterface

1. Open Internet Explorer, voer het IP-adres van het apparaat in de adresbalk in en druk op Enter. Als de installatiewizard verschijnt, volg dan de instructies om de instellingen te voltooien.
2. Voer uw gebruikersnaam en wachtwoord in het aanmeldvak in en klik op Aanmelden.
3. Als je voor de eerste keer inlogt, klik dan op [Klik hier](#) om de plugin te downloaden en installeer de plugin volgens de instructies.
4. De hoofdinterface wordt weergegeven.

5 AANBEVELINGEN VOOR CYBERBEVEILIGING

Verplichte maatregelen voor cyberbeveiliging

A. Wachtwoorden wijzigen en sterke wachtwoorden gebruiken:

De belangrijkste reden voor "gehackte" systemen is het hebben van zwakke of standaardwachtwoorden. Het wordt aanbevolen om standaardwachtwoorden onmiddellijk te wijzigen en waar mogelijk sterke wachtwoorden te kiezen. Een sterk wachtwoord moet bestaan uit ten minste 8 tekens en een combinatie van speciale tekens, cijfers en hoofdletters en kleine letters.

B. Firmware bijwerken

Zoals het een standaardprocedure is in de technische industrie, raden we aan om de firmware van NVR's en IP-camera's up-to-date te houden om ervoor te zorgen dat het systeem de nieuwste beveiligingspatches en -oplossingen gebruikt.

"Nice to have" Aanbevelingen voor een betere netwerkbeveiliging

A. Wijzig wachtwoorden regelmatig

Wijzig regelmatig de wachtwoorden voor uw apparaten om ervoor te zorgen dat alleen bevoegde gebruikers toegang hebben tot het systeem.

B. Wijzig de standaard HTTP- en TCP-poorten:

- Wijzig de standaard HTTP- en TCP-poorten voor je systemen. Dit zijn de twee poorten die worden gebruikt voor communicatie en het op afstand bekijken van videofeeds.
- Deze poorten kunnen worden gewijzigd in een willekeurige reeks nummers in het bereik 1025-65535. Door de standaardpoorten te vermijden, vermindert u het risico dat buitenstaanders kunnen raden welke poorten u gebruikt.

C. Versleutelde audio- en videotransmissie

Als de inhoud van je audio- en videogegevens erg belangrijk of gevoelig is, raden we je aan om de functie voor versleutelde verzending te gebruiken om het risico te verkleinen dat audio- en videogegevens worden gestolen tijdens de verzending.

Herinnering: gecodeerde transmissie zal resulteren in enig verlies van transmissieprestaties.

D. IP-filter inschakelen:

Als je de IP-filter inschakelt, krijgt niemand toegang tot het systeem, behalve degenen met specifieke IP-adressen.

E. ONVIF-wachtwoord wijzigen:

Bij oudere IP-camerafirmware verandert het ONVIF-wachtwoord niet wanneer de systeemgegevens worden gewijzigd. U moet de camerafirmware bijwerken naar de nieuwste versie of het ONVIF-wachtwoord handmatig wijzigen.

F. Accountvergrendeling inschakelen

De accountvergrendeling is standaard ingeschakeld en we raden aan om deze functie ingeschakeld te laten om accountbeveiliging te garanderen. Als een aanvaller meerdere keren probeert in te loggen met het verkeerde wachtwoord, worden het bijbehorende account en bron-IP-adres geblokkeerd.

G. Stuur alleen de noodzakelijke poorten door:

- Stuur alleen de HTTP- en TCP-poorten door die je nodig hebt. Stuur geen grote reeks nummers door naar het apparaat. DMZ het IP-adres van het apparaat niet.
- U hoeft geen poorten door te sturen voor individuele camera's als ze allemaal zijn aangesloten op de DVR op locatie; u hebt alleen de NVR nodig.

H. Beperk de functionaliteit van gastaccounts:

Als het systeem is geconfigureerd voor meerdere gebruikers, zorg er dan voor dat elke gebruiker alleen toegang heeft tot de functies die ze nodig hebben om hun werk te doen.

I. Schakel onnodige services uit en selecteer veilige modi

Als het niet nodig is, is het aan te raden om bepaalde services zoals SNMP, SMTP, UPnP, enz. uit te schakelen om risico's te beperken.

Indien nodig wordt aanbevolen om veilige modi te gebruiken, inclusief maar niet beperkt tot de volgende services:

- SNMP: Selecteer SNMP v3 en configureer sterke codering en verificatiewachtwoorden.
- SMTP: Selecteer TLS voor toegang tot de postbusserver.
- FTP: Selecteer SFTP en configureer sterke wachtwoorden.

- Hotspot AP: Selecteer WPA2-PSK-coderingsmodus en stel sterke wachtwoorden in.

J. Beveiligde audit

Online gebruikerscontrole: we raden u aan regelmatig online gebruikers te controleren om te zien of de NVR is aangemeld zonder autorisatie.

Apparaatlogboeken controleren: Door de logboeken te bekijken, kunt u de IP-adressen achterhalen die zijn gebruikt om in te loggen op de apparaten en hun sleutelbewerkingen.

K. Netwerklogboek

Door de beperkte geheugencapaciteit van het apparaat is het opgeslagen log beperkt. Als het nodig is om het logboek voor een lange periode op te slaan, is het aanbevolen om de netwerklogfunctie in te schakelen om ervoor te zorgen dat kritieke logboeken worden gesynchroniseerd met de netwerklogserver voor traceringsdoeleinden.

L. Het apparaat fysiek vergrendelen:

Idealiter moet ongeautoriseerde fysieke toegang tot het systeem worden voorkomen. De beste manier om dit te bereiken is door de logger in een afgesloten kast, afsluitbare serverkast of in een kamer achter een afgesloten deur te installeren.

M. IP-camera's aansluiten op de PoE-poorten aan de achterkant van de NVR-eenheid:

Camera's die zijn aangesloten op de PoE-poorten aan de achterkant van de NVR zijn geïsoleerd van de buitenwereld en kunnen niet rechtstreeks worden benaderd.

N. Een veilige netwerkomgeving creëren

Om de veiligheid van uw apparatuur beter te garanderen en potentiële cyberbedreigingen te verminderen, raden we u aan:

- Schakel de poortmappingfunctie van de router uit om directe toegang tot intranetapparaten vanuit het externe netwerk te voorkomen.
- Het netwerk moet worden gepartitioneerd en geïsoleerd volgens de werkelijke behoeften van het netwerk. Als er geen communicatievereisten zijn tussen twee subnetten, wordt voorgesteld om VLAN's, GAP-netwerken en andere technologieën te gebruiken om het netwerk te partitioneren om netwerkisolatie te bereiken.
- EZorg voor een 802.1x-toegangsverificatiesysteem om het risico op ongevoegde toegang tot privénetwerken te verkleinen.

O. Het wordt aanbevolen om een firewall of een blokkeer- en toestemmingslijstfunctie in te schakelen om het risico op aanvallen op het apparaat te verkleinen.

6 AANVULLENDE

Ga voor meer informatie en het downloaden van de benodigde software naar de volgende website:





Nice SpA
Oderzo TV Italia
info@niceforyou.com

www.niceforyou.com