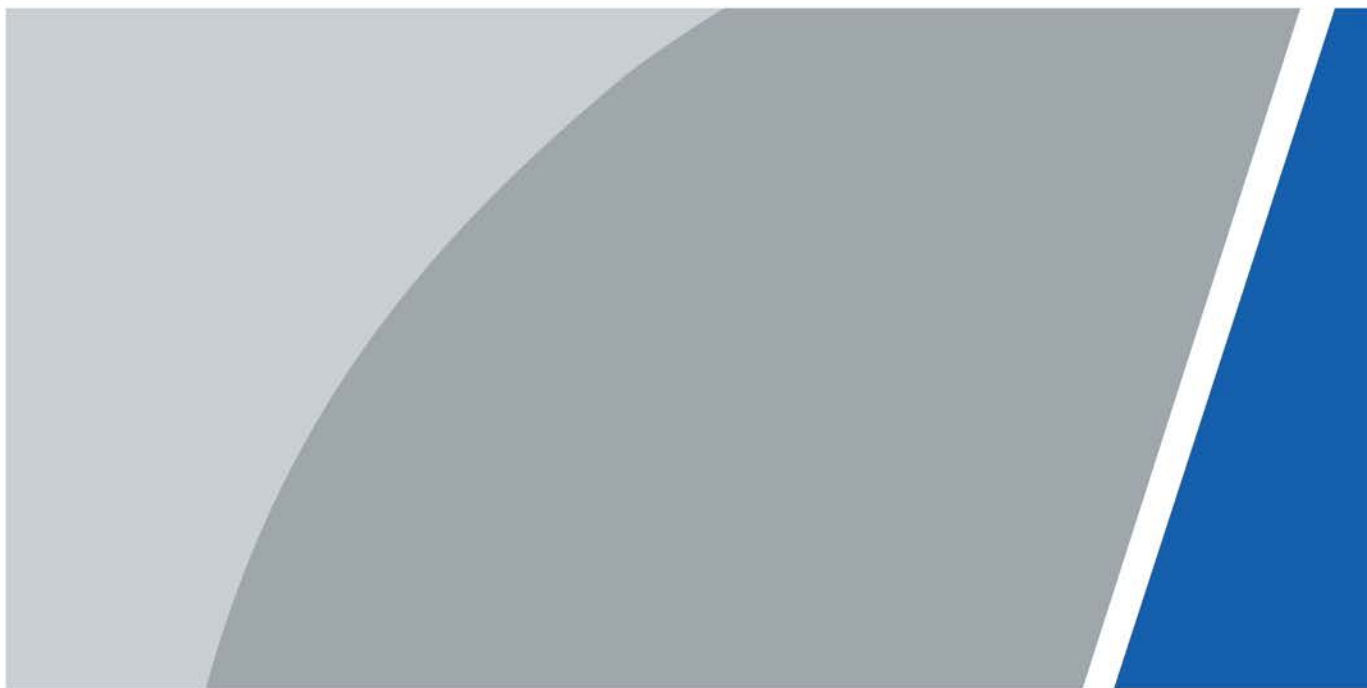


2-draads controller

Gebruikershandleiding



Voorwoord

Algemeen

Deze handleiding introduceert de structuur, functies en werking van de 2-draads controller (hierna te noemen "de Controller"). Lees aandachtig door voordat u het apparaat gebruikt en bewaar de handleiding op een veilige plaats voor toekomstig gebruik.

Veiligheidsinstructies

De volgende signaalwoorden kunnen in de handleiding voorkomen.

Signaalwoorden	Betekenis
 DANGER	Geeft een groot potentieel gevaar aan dat, indien niet vermeden, zal resulteren in de dood of ernstig letsel.
 WARNING	Geeft een middelmatig of laag potentieel gevaar aan dat, indien het niet wordt vermeden, kan leiden tot licht of matig letsel.
 CAUTION	Geeft een potentieel risico aan dat, indien niet vermeden, kan leiden tot schade aan eigendommen, gegevensverlies, prestatievermindering of onvoorspelbare resultaten.
 NOTE	Biedt aanvullende informatie als aanvulling op de tekst.

Revisiegeschiedenis

Versie	Herziening Inhoud	Vrijgavetijd
Versie 1.0.1	Herzien netwerkdiagram.	September 2024
Versie 1.0.0	Eerste release.	Juli 2024

Privacybeschermingsverklaring

Als gebruiker van het apparaat of als gegevensbeheerder kunt u persoonlijke gegevens van anderen verzamelen, zoals hun gezicht, audio, vingerafdrukken en kentekennummer. U moet voldoen aan uw lokale privacybeschermingswetten en -regelgeving om de legitieme rechten en belangen van andere mensen te beschermen door maatregelen te implementeren die onder meer het volgende omvatten: Het verstrekken van een duidelijke en zichtbare identificatie om mensen te informeren over het bestaan van het bewakingsgebied en het verstrekken van vereiste contactgegevens.

Over de handleiding

- De handleiding is alleen ter referentie. Er kunnen kleine verschillen zijn tussen de handleiding en het product.
- Wij zijn niet aansprakelijk voor verliezen die ontstaan doordat het product op een manier wordt gebruikt die niet in overeenstemming is met de handleiding.
- De handleiding wordt bijgewerkt volgens de laatste wetten en regels van de betreffende rechtsgebieden. Voor gedetailleerde informatie, zie de papieren gebruikershandleiding, gebruik onze CD-ROM, scan de QR-code of bezoek onze officiële website. De handleiding is alleen ter referentie. Er kunnen kleine verschillen zijn tussen de elektronische versie en de papieren versie.

- Alle ontwerpen en software kunnen zonder voorafgaande schriftelijke kennisgeving worden gewijzigd. Productupdates kunnen ertoe leiden dat er verschillen ontstaan tussen het daadwerkelijke product en de handleiding. Neem contact op met de klantenservice voor het nieuwste programma en aanvullende documentatie.
- Er kunnen fouten in de afdruk of afwijkingen in de beschrijving van de functies, handelingen en technische gegevens voorkomen. Als er twijfel of geschil is, behouden wij ons het recht voor om een definitieve uitleg te geven.
- Werk de lezerssoftware bij of probeer andere gangbare lezerssoftware als de handleiding (in PDF-formaat) niet kan worden geopend.
- Alle handelsmerken, geregistreerde handelsmerken en bedrijfsnamen in de handleiding zijn eigendom van hun respectievelijke eigenaren.
- Bezoek onze website en neem contact op met de leverancier of de klantenservice als er problemen optreden tijdens het gebruik van het apparaat.
- Indien er onduidelijkheid of controverse ontstaat, behouden wij ons het recht voor om een definitieve uitleg te geven.

Belangrijke voorzorgsmaatregelen en waarschuwingen

Deze sectie introduceert inhoud die betrekking heeft op de juiste behandeling van het apparaat, het voorkomen van gevaren en het voorkomen van schade aan eigendommen. Lees aandachtig door voordat u het apparaat gebruikt en volg de richtlijnen bij het gebruik ervan.

Installatievereisten



WARNING

- Sluit de stroomadapter niet aan op het apparaat terwijl de adapter is ingeschakeld.
- Sluit het apparaat niet aan op twee of meer soorten voedingen, om schade aan het apparaat te voorkomen.
- Volg de elektrische vereisten om het apparaat van stroom te voorzien.
 - ◇ Hieronder staan de vereisten voor het selecteren van een stroomadapter.
 - De voeding moet voldoen aan de eisen van de normen IEC 60950-1 en IEC 62368-1.
 - De spanning moet voldoen aan de SELV-vereisten (Safety Extra Low Voltage) en mag de ES-1-normen niet overschrijden.
 - Wanneer het vermogen van het apparaat niet hoger is dan 100 W, moet de voeding voldoen aan de LPS-vereisten en niet hoger zijn dan PS2.
 - ◇ Wij raden u aan de bij het apparaat geleverde stroomadapter te gebruiken.
 - ◇ Bij het selecteren van de stroomadapter zijn de vereisten voor de stroomvoorziening (zoals de nominale spanning) afhankelijk van het label op het apparaat.



- Personeel dat op hoogte werkt, moet alle nodige maatregelen nemen om de persoonlijke veiligheid te waarborgen, waaronder het dragen van een helm en veiligheidsgordels.
- Plaats het apparaat niet op een plaats waar het wordt blootgesteld aan zonlicht of in de buurt van warmtebronnen.
- Houd het apparaat uit de buurt van vocht, stof en roet.
- Plaats het apparaat op een stabiel oppervlak om te voorkomen dat het valt.
- Installeer het apparaat op een goed geventileerde plaats en blokkeer de ventilatie niet.
- Gebruik een adapter of kastvoeding die door de fabrikant wordt geleverd.
- Gebruik de netsnoeren die worden aanbevolen voor de regio en die voldoen aan de specificaties voor het nominale vermogen.
- Het apparaat is een elektrisch apparaat van klasse I. Zorg ervoor dat de voeding van het apparaat is aangesloten op een stopcontact met beschermende aarding.

Operationele vereisten



DANGER

Voorzorgsmaatregelen voor de accu

Preventieve maatregelen (inclusief maar niet beperkt tot):

- Vervoer, bewaar of gebruik de batterijen niet op grote hoogte met lage druk en in omgevingen met extreem hoge en lage temperaturen.
- Gooi de batterijen niet in vuur of een hete oven en plet of snijd de batterijen niet mechanisch om een explosie te voorkomen.
- Laat de batterijen niet achter in omgevingen met extreem hoge temperaturen om explosies en lekkage van ontvlambare vloeistoffen of gassen te voorkomen.
- Stel de batterijen niet bloot aan extreem lage luchtdruk om explosies en lekkage van ontvlambare vloeistoffen of gassen te voorkomen.



- Controleer voor gebruik of de voeding correct is.
- Haal de stekker van het apparaat niet uit het stopcontact terwijl de adapter is ingeschakeld.
- Gebruik het apparaat binnen het nominale bereik van het ingangs- en uitgangsvermogen.
- Vervoer, gebruik en bewaar het apparaat onder de toegestane vochtigheids- en temperatuurcondities.
- Als het apparaat langer dan een maand uitgeschakeld is, moet het in de originele verpakking worden geplaatst en verzegeld. Zorg ervoor dat het uit de buurt van vocht blijft en bewaar het onder toegestane vochtigheids- en temperatuurcondities.
- Laat geen vloeistof op het apparaat vallen of spat er geen vloeistof op en zorg ervoor dat er geen met vloeistof gevulde voorwerpen op het apparaat staan om te voorkomen dat er vloeistof in stroomt.
- Haal het apparaat niet uit elkaar zonder professionele instructies.

Inhoudsopgave

Voorwoord	I
Belangrijke voorzorgsmaatregelen en waarschuwingen	III
1 Overzicht	1
1.1 Inleiding	1
1.2 Structuur	1
2 Netwerkdigram	3
3 Webpaginabewerkingen	7
3.1 Startpagina	7
3.2 Beheercentrum	8
3.2.1 Het wachtwoord opnieuw instellen	8
3.2.2 Het gebruikersbericht wijzigen	9
3.2.3 De fabrieksinstellingen herstellen	10
3.2.4 Het apparaat opnieuw opstarten	10
3.2.5 Uitloggen	10
3.3 Beveiligingscentrum	11
3.3.1 Beveiligingsstatus	11
3.3.2 HTTPS configureren	11
3.3.3 Aanval Verdediging	12
3.3.3.1 Firewall configureren	12
3.3.3.2 Accountvergrendeling configureren	14
3.3.3.3 Anti-DoS-aanval configureren	14
3.3.4 Apparaatcertificaat installeren	15
3.3.4.1 Certificaat aanmaken	15
3.3.4.2 Aanvragen en importeren van CA-certificaat	16
3.3.4.3 Bestaand certificaat installeren	18
3.3.5 Het vertrouwde CA-certificaat installeren	18
3.3.6 Beveiligingswaarschuwing	19
3.3.7 Beveiligingsauthenticatie	19
3.4 VTO-configuratie	20
3.4.1 Personeelsmanagement	20
3.4.2 VTH-kamernummertoewijzing	23
3.4.3 Toegangscontrole	23
3.4.3.1 Configuratie	23
3.4.3.2 RS-485	24
3.4.4 Module	25

3.4.5 Onderhoud	25
3.5 Persoon	26
3.6 Personen in batches importeren	28
3.7 Netwerkinstellingen	28
3.7.1 TCP/IP configureren	28
3.7.2 Basisservices configureren	29
3.8 Onderhoudscentrum	31
3.8.1 Diagnose met één klik	31
3.8.2 Systeeminformatie	31
3.8.3 Configuratiebestanden exporteren en importeren	32
3.8.4 Het systeem updaten	32
3.8.5 Geavanceerd onderhoud	33
3.8.5.1 Exporteren	33
3.8.5.2 Pakket vastleggen	33
Bijlage 1 Beveiligingsaanbeveling	34

1 Overzicht

1.1 Inleiding

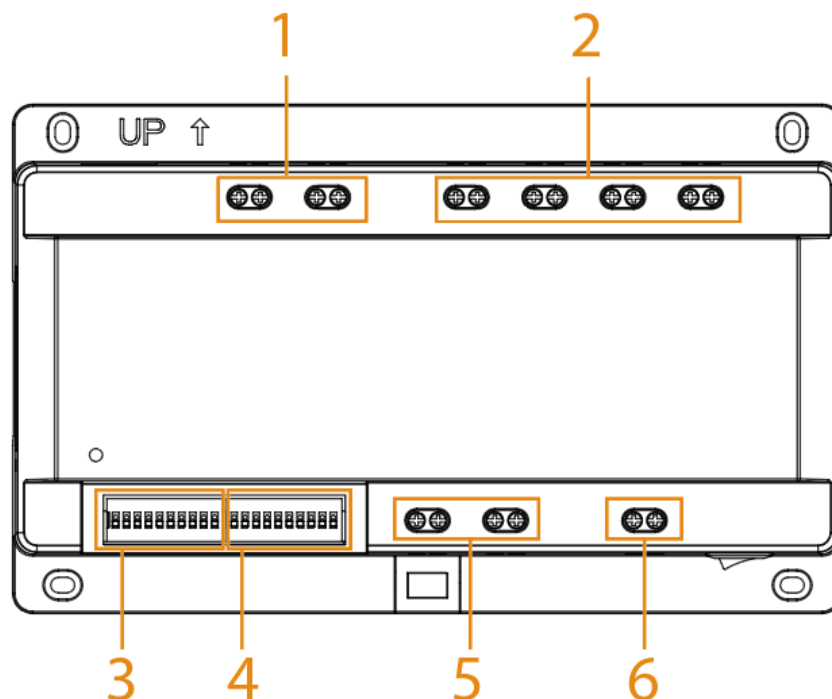
De 2-draads controller gebruikt het plastic materiaal en ondersteunt slide rail installatie. Tot 100 analoge VTH's of 22 VTH's met Wi-Fi functie kunnen worden aangesloten op één 2-draads controller. De 2-draads controller kan verbinding maken met andere 2-draads controllers in de cascademodus (tot 10 niveaus van cascadering worden ondersteund). U kunt inloggen op de webpagina van de controller om de apparaten te beheren.



- In de cascademodus configureert u de apparaten tegelijkertijd via één webpagina van de 2-draadscontroller.
- Gebruik de aanbevolen voeding.

1.2 Structuur

Figuur 1-1 Voorpaneel

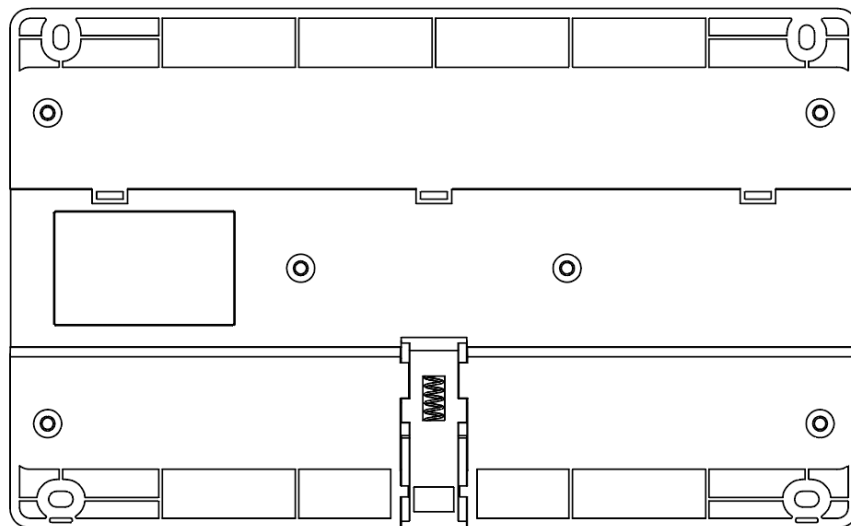


Tabel 1-1 Beschrijving van het voorpaneel

Nee.	Beschrijving
1	Maak verbinding met VTO.
2	Maak verbinding met VTH.

Nee.	Beschrijving
3	Nadat u verbinding hebt gemaakt met VTH's, stelt u de DIP in op de minimale ID van alle VTH-ID's.  Beweeg de actuator volledig naar de bovenste of onderste positie. Als de actuator in de middelste positie staat, wordt deze beschouwd als in de bovenste positie.
4	Nadat u verbinding hebt gemaakt met VTH's, stelt u de DIP in op de maximale ID van alle VTH-ID's.  Beweeg de actuator volledig naar de bovenste of onderste positie. Als de actuator in de middelste positie staat, wordt deze beschouwd als in de bovenste positie.
5	Verbinden met andere 2-draads controllers. De UP -poort kan alleen worden verbonden met de Down -poort op een andere controller. De Down -poort kan alleen worden verbonden met de Up -poort op een andere controller. Zie het bedradingsschema voor meer informatie.
6	Sluit aan op de voeding.

Afbeelding 1-2 Achterpaneel



2 Netwerkdigram



Wanneer er meerdere binnenmonitoren in cascademodus op de poort op de aftakklem zijn aangesloten, moet de 14e DIP-schakelaar van de binnenmonitor die het verst van de poort is verwijderd, worden ingeschakeld om signaalreflectie te verminderen.

Raadpleeg de volgende afbeelding om de DIP-switch van het apparaat in de cascade te configureren. De DIP-switch van ID moet worden geconfigureerd volgens de werkelijke situatie.

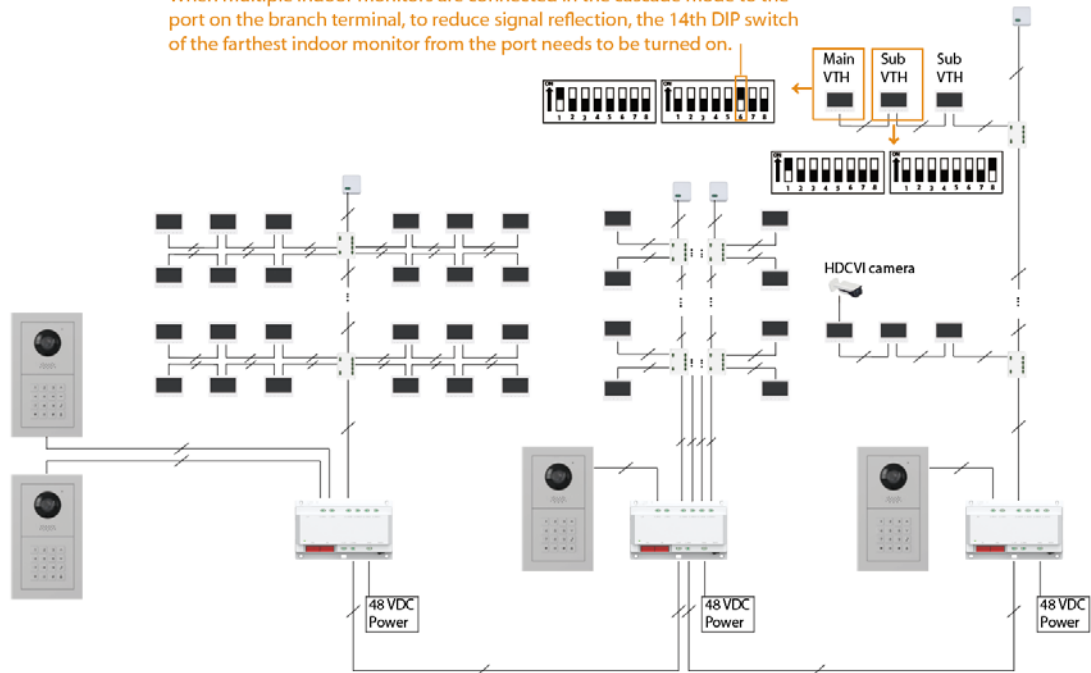


- De voeding van de HDCVI-camera kan niet worden geaard.
- Het uiterlijk van het product is alleen ter referentie.

Netwerkdigram

Figuur 2-1 Netwerkdigram

When multiple indoor monitors are connected in the cascade mode to the port on the branch terminal, to reduce signal reflection, the 14th DIP switch of the farthest indoor monitor from the port needs to be turned on.

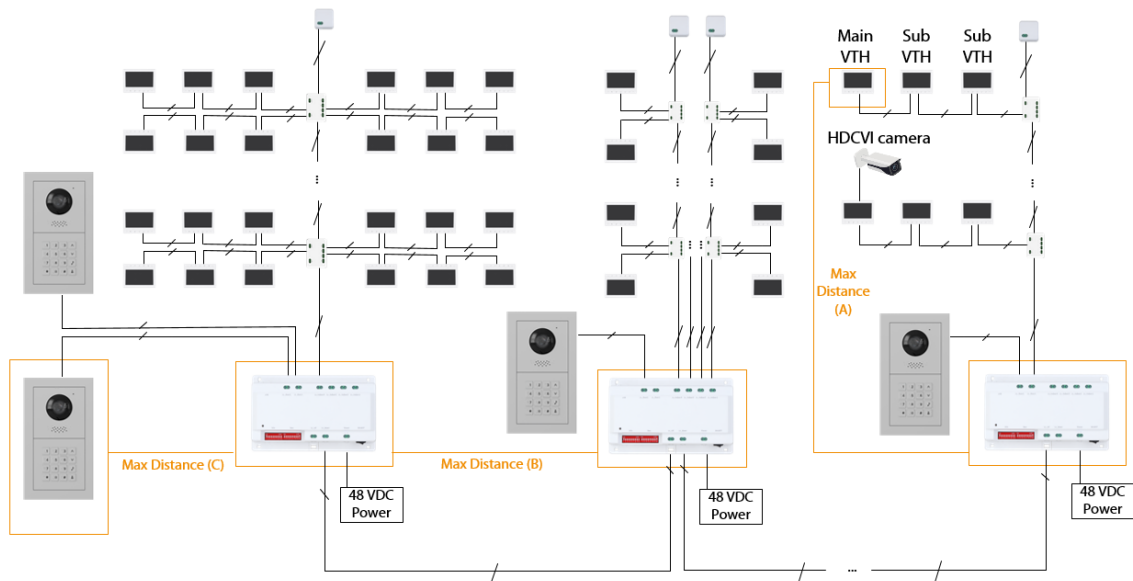


Bedradingsafstand tussen de controller, VTH en de VTO



- Maximale afstand (A) verwijst naar de afstand tussen de 2-draads controller en de VTH. $A \leq 100$ m.
- Maximale afstand (B) verwijst naar de afstand tussen de in cascade geschakelde 2-draads controllers. $B \leq 100$ m.
- Maximale afstand (C) verwijst naar de afstand tussen de 2-draads controller en de VTO. $C \leq 100$ m.
- Het aantal cascaderende controllers moet kleiner of gelijk zijn aan 10.

Figuur 2-2 Maximale afstand



Netwerkcapaciteit voor VTH

De capaciteit van de VTH geeft het maximale aantal VTH's aan dat op één binnenmonitorpoort op de 2-draadscontroller kan worden aangesloten.

Met elke controller kunt u maximaal 22 VTH's met wifi-functie of maximaal 100 VTH's zonder wifi-functie verbinden.



- De 2-draads VTH's met de Wi-Fi-functie kunnen tegelijkertijd werken. Het aantal 2-draads VTH's zonder de Wi-Fi-functie die tegelijkertijd werken, is 5% van de maximale capaciteit volgens verschillende kabelspecificaties en afstanden.
- De capaciteitswaarden zijn gebaseerd op de standaardinstellingen voor spraak- en schermhelderheid en standaardkabels die in de volgende tabel worden genoemd.
- Als u in het netwerk de VTH met Wi-Fi-functie wilt vervangen door de VTH zonder Wi-Fi-functie, is de conversieverhouding 1:8.
Als u bijvoorbeeld 1 VTH met Wi-Fi-functie in het netwerk wilt verminderen, kunt u verbinding maken met 8 VTH's zonder Wi-Fi-functie.



Het maximale aantal VTH's met Wi-Fi-functie mag niet meer dan 22 bedragen.

Het maximale aantal VTH's zonder Wi-Fi-functie mag niet meer dan 100 bedragen.

Tabel 2-1 Netwerkkapaciteit voor VTH

Kabeltype	Kabelspecificatie	AWG	Apparaattype	Een = 0-25 meter	A=26-50 meter	Een = 51-75 meter	A=76-100 meter
Normale kabel	RVV 2 × 1,5 mm ² (aanbevolen)	AWG-15	Met wifi	22	22	22	17
			Zonder wifi	100	100	100	100
	RVV 2 × 1 mm ²	AWG-17	Met wifi	22	22	18	13
			Zonder wifi	100	100	100	100
	RVV 2 × 0,5 mm ²	AWG-20	Met wifi	22	17	11	8
			Zonder wifi	100	100	91	68
Netwerk kabel	Dubbelpaar netwerkkabel	AWG-21	Met wifi	22	14	9	7
			Zonder wifi	100	100	75	56
	Enkelbaar netwerkkabel	AWG-24	Met wifi	14	7	4	3
			Zonder wifi	100	56	37	28

Netwerkkapaciteit voor 2-draads controller

De capaciteit van de 2-draadscontroller geeft het maximale aantal controllers aan dat op één overeenkomstige poort op de controller kan worden aangesloten.



De capaciteitswaarden zijn gebaseerd op standaardkabels die in de volgende tabel staan vermeld.

Tabel 2-2 Netwerkkapaciteit voor de controller

Kabeltype	Kabelspecificatie	AWG	B=0-100m
Normale kabel	RVV 2 × 1,5 mm ²	AWG-15	8
	RVV 2 × 1 mm ²	AWG-17	10
	RVV 2 × 0,5 mm ² (aanbevolen)	AWG-20	10

Kabeltype	Kabelspecificatie	AWG	B=0–100m
Netwerkkabel	Dubbelpaar netwerkkabel	AWG-21	10
	Enkelpaar netwerkkabel	AWG-24	10

Netwerkc capaciteit voor VTO

De capaciteit van de VTO geeft het maximale aantal VTO's aan dat op één 2-draads controller kan worden aangesloten.

Er kunnen maximaal 2 VTO's op één 2-draads controller worden aangesloten.



De capaciteitswaarden zijn gebaseerd op standaardkabels die in de volgende tabel staan vermeld.

Tabel 2-3 Netwerkc capaciteit voor de VTO

Kabeltype	Kabelspecificatie	AWG	C=0–25 m	C=26–50 meter	C=51–75 meter	C=76–100 meter
Normale kabel	RVV 2 × 1,5 mm ² (aanbevolen)	AWG-15	2	2	2	2
	RVV 2 × 1 mm ²	AWG-17	2	2	2	2
	RVV 2 × 0,5 mm ²	AWG-20	2	2	2	2
Netwerkkabel	Dubbelpaar netwerkkabel	AWG-21	2	2	2	2
	Enkelpaar netwerkkabel	AWG-24	2	2	1	1

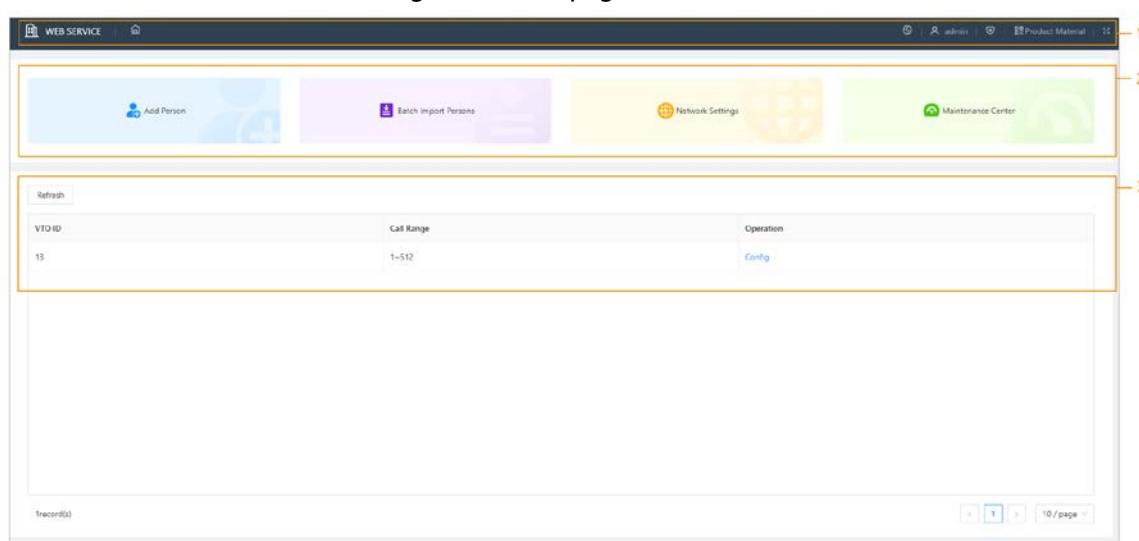
3 Webpaginabewerkingen

Wanneer u zich voor de eerste keer aanmeldt, moet u het apparaat initialiseren op de webpagina. Meld u aan op de webpagina om de parameters van de controller te configureren en de VTO te beheren die is aangesloten op de huidige controller en de VTO die is aangesloten op cascaderende controllers.

3.1 Startpagina

Nadat u bent ingelogd, gaat het systeem automatisch naar de startpagina.

Figuur 3-1 Startpagina



Tabel 3-1 Inleiding startpagina

Nee.	Icon	Functie	Beschrijving	Referentie
1		Home-knop	Ga terug naar de startpagina.	—
		Taal	Wijzig de taal van de webpagina op het apparaat.	—
		Beheercentrum	Wijzig het wachtwoord, meld u af bij het huidige apparaat, start het systeem opnieuw op en herstel de fabrieksinstellingen van het apparaat.	"3.2 Beheercentrum"
		Beveiligingscentrum	Bekijk en configureer de beveiligingsinstellingen.	"3.3 Beveiligingscentrum"
		Productmateriaal	Scan de QR-code om het productmateriaal te bekijken, zoals de gebruikershandleiding.	—

Nee.	Icon	Functie	Beschrijving	Referentie
		Volledig scherm	Bekijk de webpagina in volledig scherm. Klik nogmaals of druk op de Exit-toets om de modus Volledig scherm te verlaten.	—
2	—	Persoon toevoegen	Voeg de persoon toe en stuur de informatie naar VTO's.	"3.5 Persoon toevoegen"
	—	Batch-import personen	Nadat u de persoonsgegevens uit de VTO hebt geëxporteerd, kunt u de personen in batches importeren naar andere VTO's.	"3.6 Personen in batches importeren"
	—	Netwerkinstellingen	Configureer de netwerkparameters zoals TCP/IP en basisservices.	"3.7 Netwerkinstellingen"
	—	Onderhoudscentrum	Bekijk de systeeminformatie. Exporteer en importeer configuratiebestanden. Werk het apparaat bij en meer.	"3.8 Onderhoudscentrum"
3	—	VTO-configuratie	Beheer persoonsinformatie op de VTO. Configureer de VTO-parameters, inclusief toegangscontroleparameters, moduleparameters en meer.	"3.4 VTO-configuratie"

3.2 Beheercentrum

U kunt op de startpagina het wachtwoord wijzigen, uitloggen, het apparaat opnieuw opstarten, de fabrieksinstellingen van het apparaat herstellen en andere handelingen uitvoeren.

3.2.1 Het wachtwoord opnieuw instellen

Als u het wachtwoord van het beheerdersaccount bent vergeten, scant u de QR-code om het wachtwoord opnieuw in te stellen.

Vereisten

Zorg ervoor dat u **Wachtwoord opnieuw instellen hebt ingeschakeld** via **Netwerkinstellingen > Basisservices**.



Als u het e-mailadres niet hebt geconfigureerd tijdens de initialisatie, meldt het systeem een fout.
Neem contact op met de lokale dealer of de technische ondersteuning voor hulp.

Procedure

Stap 1 Klik op **Wachtwoord vergeten?** op de inlogpagina en klik vervolgens op **Volgende** .

Stap 2 Ontvang de **beveiligingscode** volgens de instructies.



- U kunt maximaal 2 beveiligingscodes met dezelfde QR-code krijgen. Als u meer beveiligingscodes nodig hebt, moet u de QR-code vernieuwen en opnieuw scannen.
- De beveiligingscode wordt naar uw e-mailadres verzonden. U moet deze binnen 24 uur gebruiken. Anders is de beveiligingscode ongeldig.
- Als u 5 keer achter elkaar de verkeerde beveiligingscode invoert, wordt uw account gedurende 5 minuten geblokkeerd.

Stap 3 Voer de beveiligingscode in die u hebt ontvangen en klik op **Volgende** .

Stap 4 Voer het nieuwe wachtwoord in, bevestig het nieuwe wachtwoord en klik vervolgens op **OK** .

3.2.2 Het gebruikersbericht wijzigen

Wijzig het inlogwachtwoord en het e-mailadres van de gebruiker.

Procedure

Stap 1 Klik  **admin** op de startpagina.

Stap 2 Klik op **Wachtwoord wijzigen** .

Stap 3 Schakel de functie in, configureer de parameters en klik vervolgens op **OK** .

Figuur 3-2 Het gebruikersbericht wijzigen

3.2.3 De fabrieksinstellingen herstellen

Procedure

Stap 1 Selecteer  **Fabrieksinstellingen** .



Het terugzetten van de controller naar de standaardconfiguraties zal resulteren in dataverlies. Wees gewaarschuwd.

Stap 2 Voer het inlogwachtwoord in en klik vervolgens op **OK** .

Stap 3 Herstel indien nodig de fabrieksinstellingen.

3.2.4 Het apparaat opnieuw opstarten

Selecteer  **Opnieuw opstarten** en klik vervolgens op **OK** in het pop-upvenster. Het apparaat start automatisch opnieuw op en de webpagina gaat naar de inlogpagina.

3.2.5 Uitloggen

Selecteer  **Afmelden** . De webpagina gaat naar de inlogpagina.

3.3 Beveiligingscentrum

3.3.1 Beveiligingsstatus

Scan de gebruikers-, service- en beveiligingsmodules om de beveiligingsstatus van de controller te controleren.

Achtergrondinformatie

- Gebruikers- en servicedetectie: controleer of de huidige configuraties voldoen aan de aanbevelingen.
- Scannen van beveiligingsmodules: scan de actieve status van beveiligingsmodules, zoals vertrouwde bescherming, firmware-encryptie en aanvalsverdediging.

Procedure

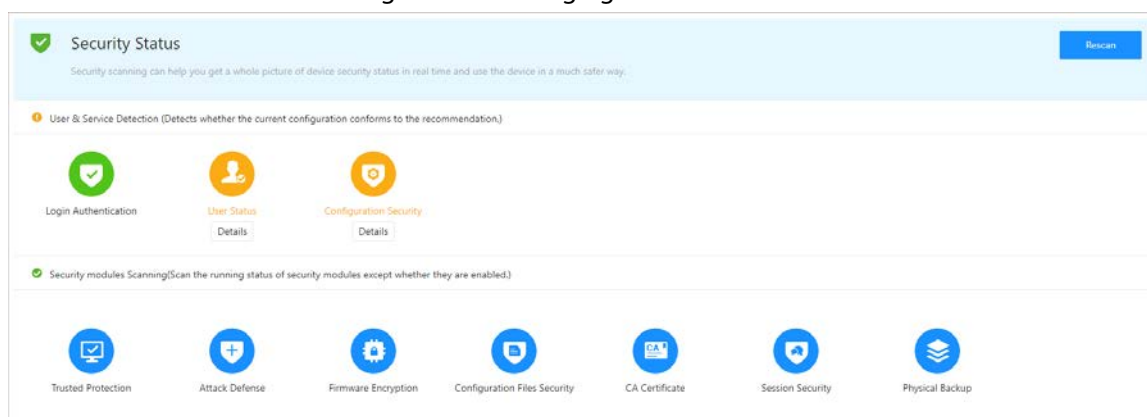
Stap 1 Selecteer >  Beveiligingsstatus .

Stap 2 Klik op **Scannen** om een beveiligingsscan van het apparaat uit te voeren.



- Beweeg de muis over de pictogrammen van de beveiligingsmodules om hun actieve status te bekijken.
- Als u de status na de eerste scan wilt controleren, klikt u op **Opnieuw scannen** .

Figuur 3-3 Beveiligingsstatus



Verwante bewerkingen

Nadat u de scan hebt uitgevoerd, worden de resultaten in verschillende kleuren weergegeven. Geel geeft aan dat de beveiligingsmodules abnormaal zijn en groen geeft aan dat de beveiligingsmodules normaal zijn.

- Klik op **Details** om de details van de scanresultaten te bekijken.
- Klik op **Negeren** om de afwijking te negeren, en deze zal niet worden gescand. De afwijking die werd genegeerd zal grijs worden gemarkeerd.
- Klik op **Optimaliseren** om het probleem op te lossen.

3.3.2 HTTPS configureren

Maak een certificaat of upload een geauthenticeerd certificaat, en dan kunt u inloggen op de

webpagina via HTTPS op uw computer. HTTPS beveiligt communicatie via een computernetwerk.

Procedure

Stap 1 Selecteer  > **Systeemservice** > **HTTPS**.

Stap 2: Schakel de HTTPS-service in.



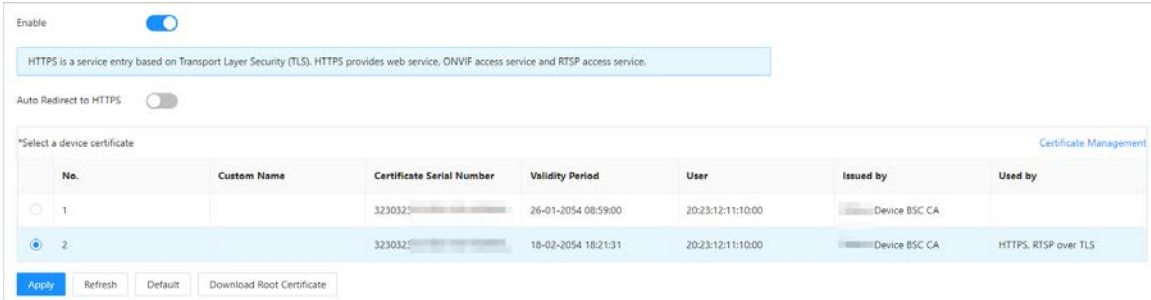
Als u de compatibele versie van TLS v1.1 en eerdere versies inschakelt, kunnen er beveiligingsrisico's optreden. Wees gewaarschuwd.

Stap 3 Selecteer het certificaat.



Als er geen certificaten in de lijst staan, klikt u op **Certificaatbeheer** om een certificaat te uploaden.

Figuur 3-4 HTTPS



No.	Custom Name	Certificate Serial Number	Validity Period	User	Issued by	Used by
1		323032	26-01-2054 08:59:00	2023:12:11:10:00	Device BSC CA	
2		323032	18-02-2054 18:21:31	2023:12:11:10:00	Device BSC CA	HTTPS, RTSP over TLS

Stap 4 Klik op **Toepassen**.

Voer "https:// IP-adres : httpssport " in een webbrowser in. Als het certificaat is geïnstalleerd, kunt u succesvol inloggen op de webpagina. Als dat niet het geval is, zal de webpagina het certificaat weergeven als onjuist of niet-vertrouwd.

3.3.3 Aanval Verdediging

3.3.3.1 Firewall configureren

Configureer de firewall om de toegang tot het apparaat te beperken.

Procedure

Stap 1 Selecteer  > **Aanvalsverdediging** > **Firewall**.

Stap 2 Klik  om de firewallfunctie in te schakelen.

Figuur 3-5 Firewall

Stap 3 Selecteer de modus: **Toestaanlijst** of **Blokkeringslijst**.

- **Toestemmingslijst** : alleen IP-/MAC-adressen op de toestemmingslijst hebben toegang tot het apparaat.
- **Blokkeringslijst** : De IP/MAC-adressen op de blokkeringslijst hebben geen toegang tot het apparaat.

Stap 4 Klik op **Toevoegen** om de IP-gegevens in te voeren.

Figuur 3-6 IP-informatie toevoegen

Stap 5 Klik op **OK**.

Verwante bewerkingen

- Klik  om de IP-gegevens te bewerken.
- Klik  om het IP-adres te verwijderen.

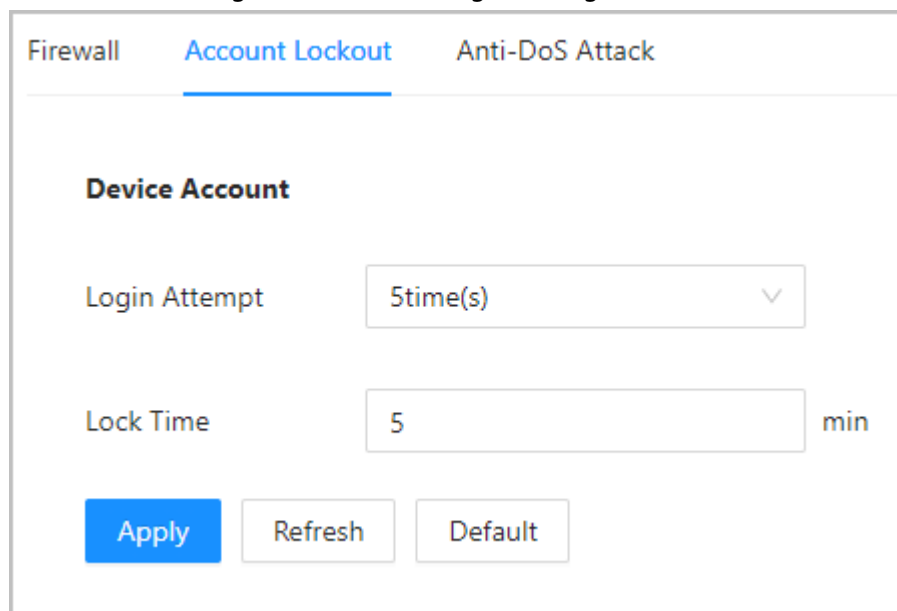
3.3.3.2 Accountvergrendeling configureren

Als u een bepaald aantal keren een onjuist wachtwoord invoert, wordt uw account geblokkeerd.

Procedure

- Stap 1 Selecteer  > **Aanvalsverdediging** > **Accountvergrendeling** .
- Stap 2 Voer het aantal aanmeldpogingen en de duur in dat het beheerdersaccount en de ONVIF-gebruiker geblokkeerd moeten worden.

Figuur 3-7 Accountvergrendeling



- Login Attempt: De limiet van loginpogingen. Als het onjuiste wachtwoord een bepaald aantal keren wordt ingevoerd, wordt het account geblokkeerd.
- Vergrendelingstijd: De duur waarin u niet kunt inloggen nadat het account is vergrendeld.

- Stap 3 Klik op **Toepassen** .

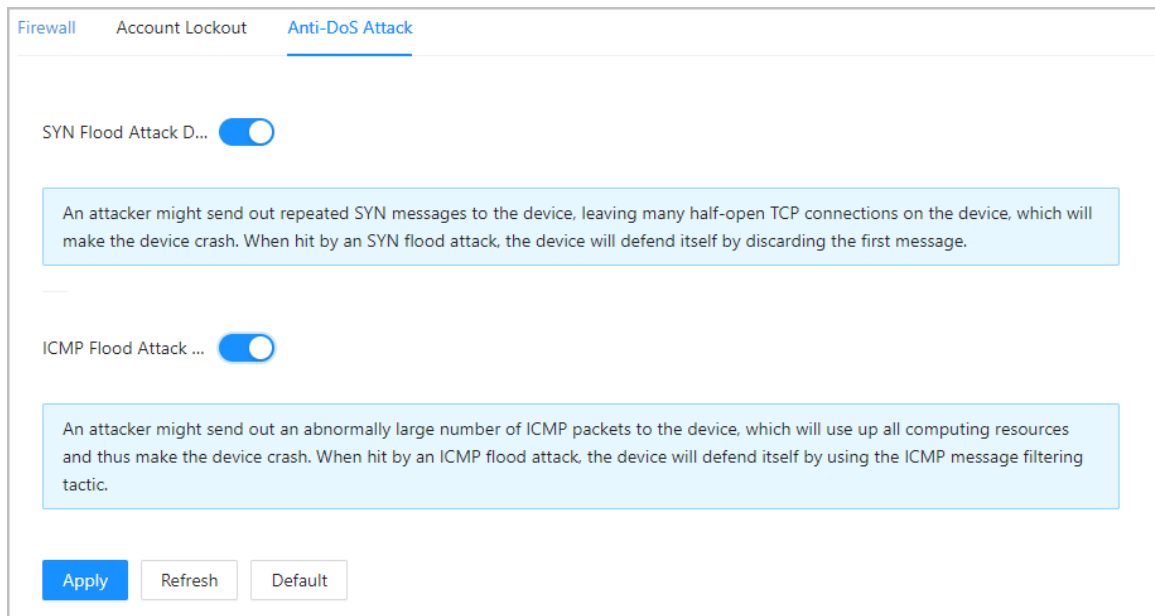
3.3.3.3 Anti-DoS-aanval configureren

SYN Flood Attack Defense en **ICMP Flood Attack Defense** inschakelen om het apparaat te verdedigen tegen Dos-aanvallen.

Procedure

- Stap 1 Selecteer  > **Aanvalsverdediging** > **Anti-DoS-aanval** .
- Stap 2: Schakel **SYN Flood Attack Defense** of **ICMP Flood Attack Defense in** om het apparaat te beschermen tegen DOS-aanvallen.

Figuur 3-8 Anti-DoS-aanval



Stap 3 Klik op **Toepassen** .

3.3.4 Apparaatcertificaat installeren

Maak een certificaat aan of upload een geauthenticeerd certificaat. Vervolgens kunt u via HTTPS inloggen op uw computer.

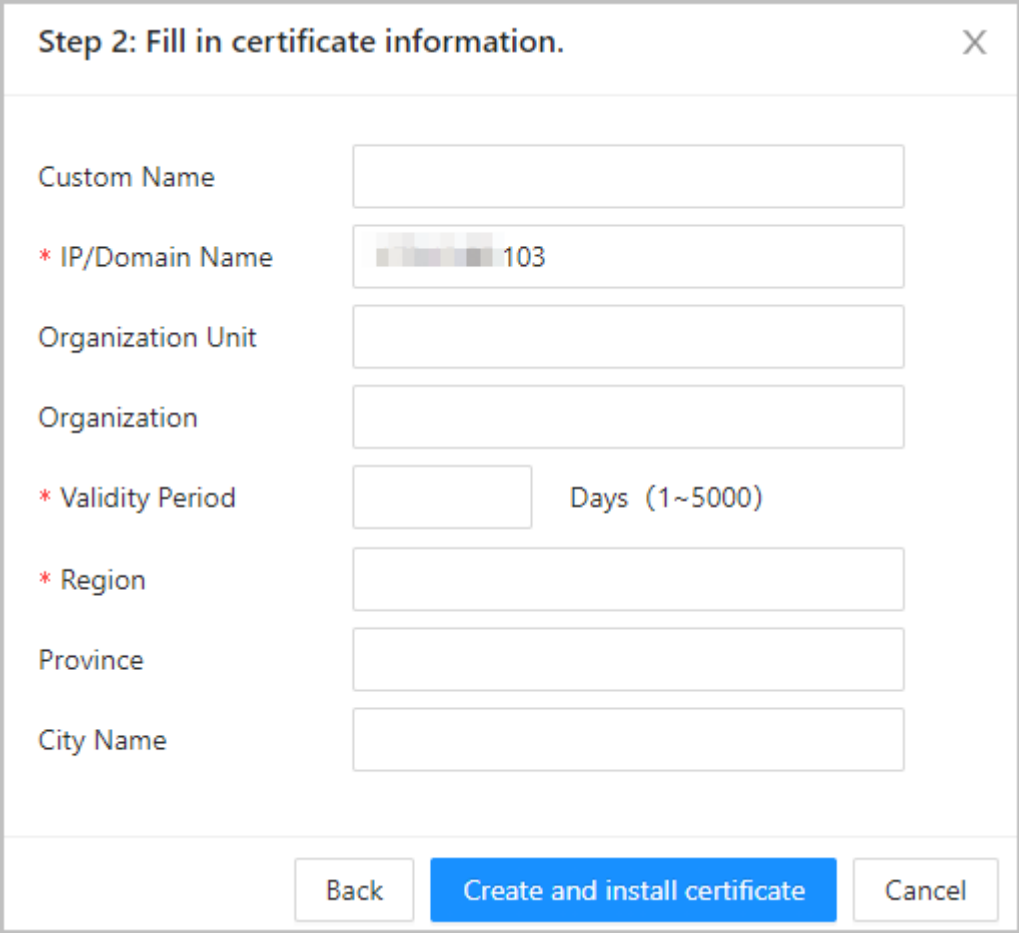
3.3.4.1 Certificaat aanmaken

Maak een certificaat voor het apparaat.

Procedure

- Stap 1 Selecteer  > **CA-certificaat** > **Apparaatcertificaat** .
- Stap 2 Selecteer **Apparaatcertificaat installeren** .
- Stap 3 Selecteer **Certificaat maken** en klik op **Volgende** .
- Stap 4 Voer de certificaatgegevens in.

Figuur 3-9 Certificaatinformatie



De naam van de regio mag niet langer zijn dan 2 tekens. Wij raden aan de afkorting van de naam van de regio in te voeren.

Stap 5 Klik op **Certificaat maken en installeren**.

Het nieuw geïnstalleerde certificaat wordt weergegeven op de pagina **Apparaatcertificaat** nadat het certificaat succesvol is geïnstalleerd.

Verwante bewerkingen

- Klik op **Bewerkingsmodus openen** op de pagina **Apparaatcertificaat** om de naam van het certificaat te bewerken.
- Klik  om het certificaat te downloaden.
- Klik  om het certificaat te verwijderen.

3.3.4.2 Aanvragen en importeren van CA-certificaat

Importeer het certificaat van de externe CA naar het apparaat.

Procedure

Stap 1 Selecteer  > **CA-certificaat** > **Apparaatcertificaat**.

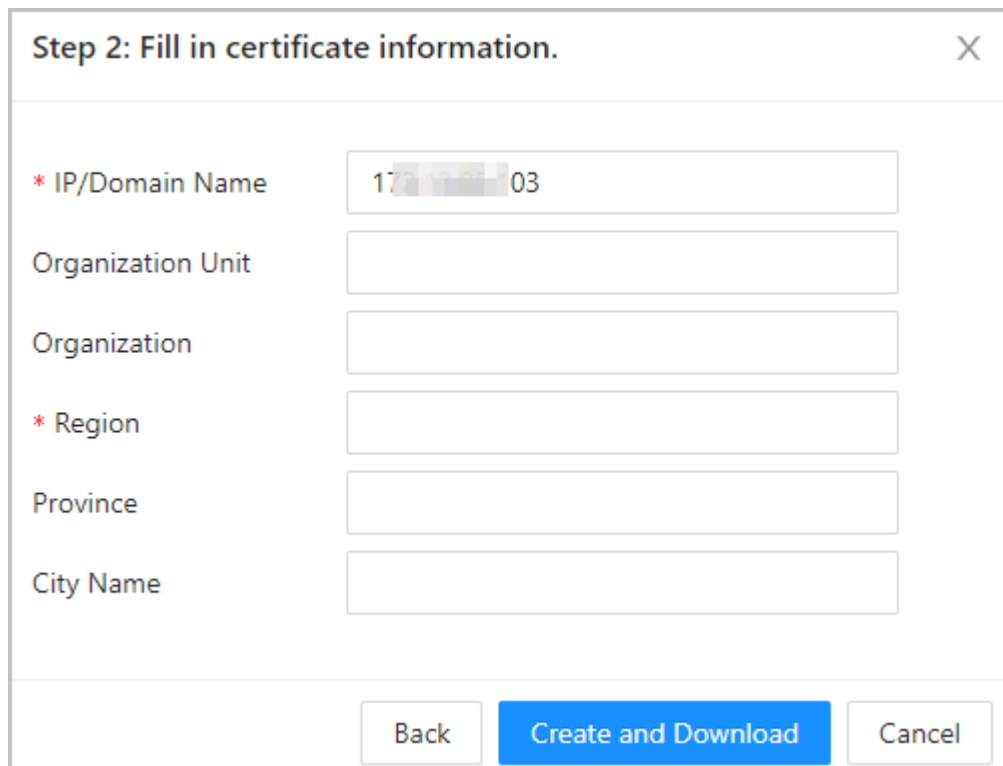
Stap 2 Klik op **Apparaatcertificaat installeren**.

Stap 3 Selecteer **CA-certificaat aanvragen en importeren (aanbevolen)** en klik op **Volgende**.

Stap 4 Voer de certificaatgegevens in.

- IP/Domeinnaam: het IP-adres of de domeinnaam van het Apparaat.
- Regio: De naam van de regio mag niet langer zijn dan 3 tekens. Wij raden u aan de afkorting van de regionaam in te voeren.

Figuur 3-10 Certificaatinformatie



Step 2: Fill in certificate information. X

* IP/Domain Name

Organization Unit

Organization

* Region

Province

City Name

Back Create and Download Cancel

Stap 5 Klik op **Maken en downloaden**.

Sla het aanvraagbestand op uw computer op.

Stap 6 Vraag het certificaat aan bij een externe CA-autoriteit met behulp van het aanvraagbestand.

Stap 7 Importeer het ondertekende CA-certificaat.

- 1) Sla het CA-certificaat op uw computer op.
- 2) Klik op **Apparaatcertificaat installeren**.
- 3) Klik op **Bladeren** om het CA-certificaat te selecteren.
- 4) Klik op **Importeren en installeren**.

Het nieuw geïnstalleerde certificaat wordt weergegeven op de pagina

Apparaatcertificaat nadat het certificaat succesvol is geïnstalleerd.

- Klik op **Opnieuw maken** om het aanvraagbestand opnieuw te maken.
- Klik op **Later importeren** om het certificaat op een ander tijdstip te importeren.

Verwante bewerkingen

- Klik op **Bewerkingsmodus openen** op de pagina **Apparaatcertificaat** om de naam van het certificaat te bewerken.
- Klik  om het certificaat te downloaden.
- Klik  om het certificaat te verwijderen.

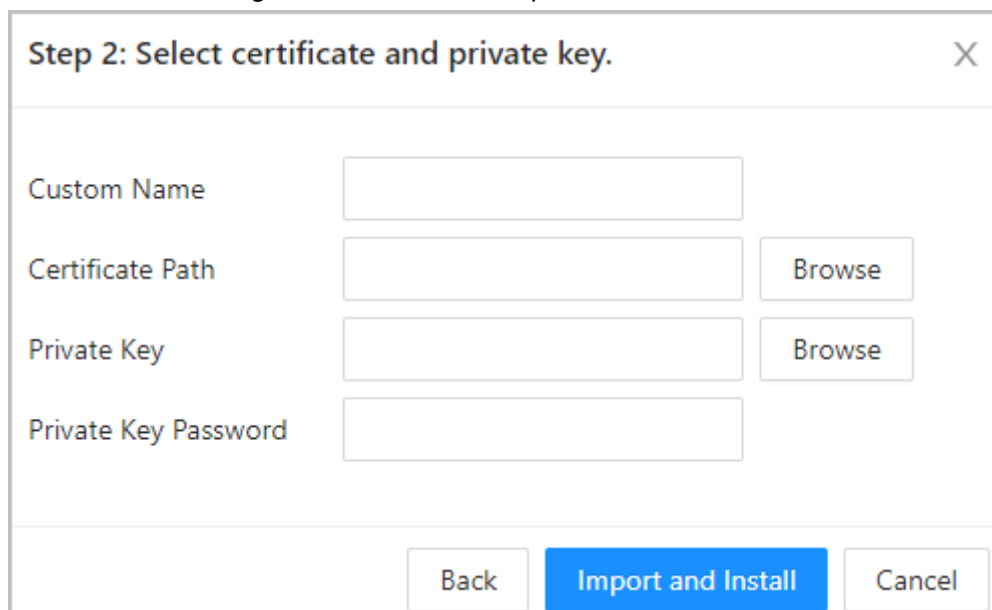
3.3.4.3 Bestaand certificaat installeren

Als u al een certificaat en een bestand met een persoonlijke sleutel hebt, importeert u het certificaat en het bestand met de persoonlijke sleutel.

Procedure

- Stap 1 Selecteer **Beveiliging > CA-certificaat > Apparaatcertificaat**.
- Stap 2 Klik **Apparaatcertificaat installeren**.
- Stap 3 Selecteer **Bestaand certificaat installeren** en klik op **Volgende**.
- Stap 4 Klik op **Bladeren** om het certificaat en het bestand met de persoonlijke sleutel te selecteren en voer het wachtwoord voor de persoonlijke sleutel in.

Figuur 3-11 Certificaat en privésleutel



- Stap 5 Klik op **Importeren en installeren**.
Het nieuw geïnstalleerde certificaat wordt weergegeven op de pagina **Apparaatcertificaat** nadat het certificaat succesvol is geïnstalleerd.

Verwante bewerkingen

- Klik op **Bewerkingsmodus openen** op de pagina **Apparaatcertificaat** om de naam van het certificaat te bewerken.
- Klik  om het certificaat te downloaden.
- Klik  om het certificaat te verwijderen.

3.3.5 Het vertrouwde CA-certificaat installeren

Een vertrouwd CA-certificaat is een digitaal certificaat dat wordt gebruikt voor het valideren van de identiteit van websites en servers. Wanneer bijvoorbeeld het 802.1X-protocol wordt gebruikt, is het CA-certificaat voor switches vereist om de identiteit ervan te verifiëren.

Achtergrondinformatie

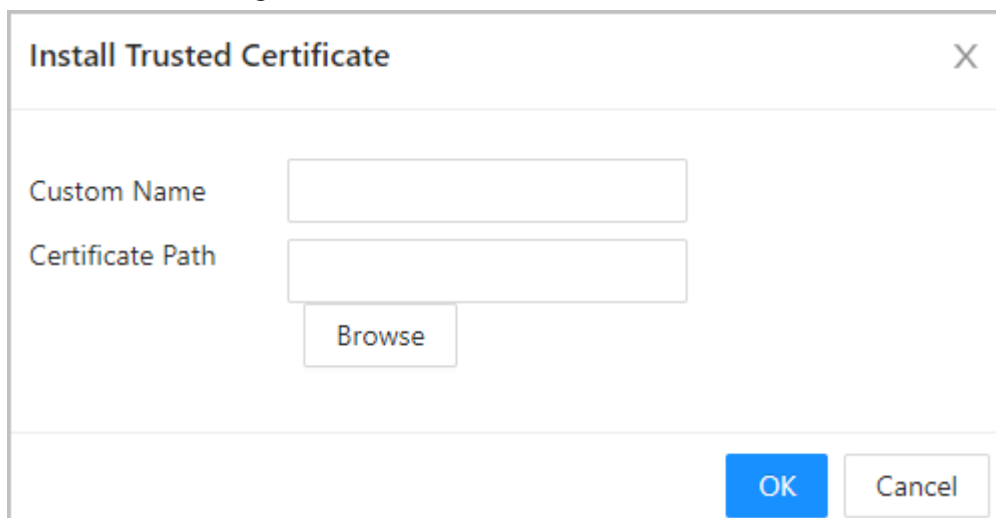
802.1X is een netwerkverificatieprotocol dat poorten opent voor netwerktoegang wanneer een

organisatie de identiteit van een gebruiker verifieert en de gebruiker toegang tot het netwerk verleent.

Procedure

- Stap 1 Selecteer  > **CA-certificaat** > **Vertrouwde CA-certificaten** .
- Stap 2 Selecteer **Vertrouwd certificaat installeren** .
- Stap 3 Klik op **Bladeren** om het vertrouwde certificaat te selecteren.

Afbeelding 3-12 Het vertrouwde certificaat installeren



- Stap 4 Klik op **OK** .
- Het nieuw geïnstalleerde certificaat wordt weergegeven op de pagina **Vertrouwde CA-certificaten** nadat het certificaat succesvol is geïnstalleerd.

Verwante bewerkingen

- Klik op **Bewerkingsmodus openen** op de pagina **Apparaatcertificaat** om de naam van het certificaat te bewerken.
- Klik  om het certificaat te downloaden.
- Klik  om het certificaat te verwijderen.

3.3.6 Beveiligingswaarschuwing

Procedure

- Stap 1 Selecteer  > **Beveiligingswaarschuwing** .
- Stap 2: Schakel de beveiligingswaarschuwingfunctie in.
- Stap 3 Klik op **Toepassen** .

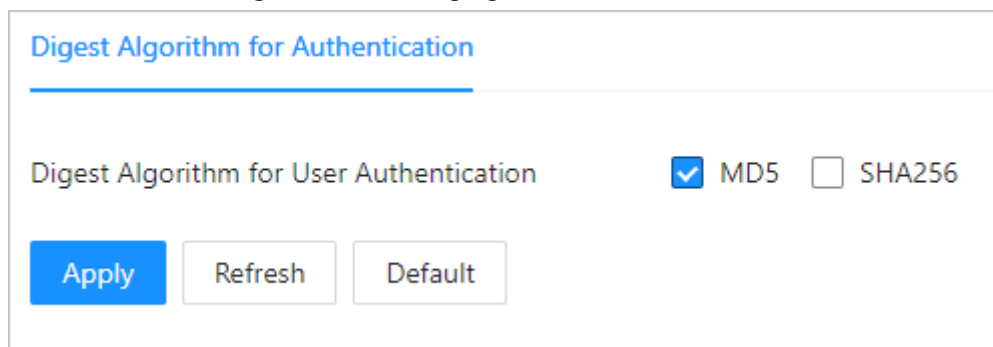
3.3.7 Beveiligingsauthenticatie

Procedure

- Stap 1 Selecteer  > **Beveiligingsverificatie** .
- Stap 2 Selecteer een algoritme voor het samenvatten van berichten.

Stap 3 Klik op **Toepassen**.

Figuur 3-13 Beveiligingsauthenticatie



3.4 VTO-configuratie

Meld u aan op de webpagina van de 2-draads controller. Het systeem geeft de VTO weer die is aangesloten op de huidige controller en de VTO die is aangesloten op cascaderende controllers.

- Klik op **Config** om de gedetailleerde configuratie van de VTO te voltooien.
- **Call Range**: Het nummerbereik dat de VTO kan bellen. U kunt geen nummers bellen die buiten dit oproepbereik vallen. Het bereik wordt gegenereerd volgens de geconfigureerde DIP op de 2-draads controller. Als het oproepbereik niet kan worden gegenereerd en rood wordt weergegeven, configureer dan de DIP op de 2-draads controller opnieuw.

Figuur 3-14 VTO



VTO ID	Call Range	Operation
2	1~256	Config
3	1~256	Config

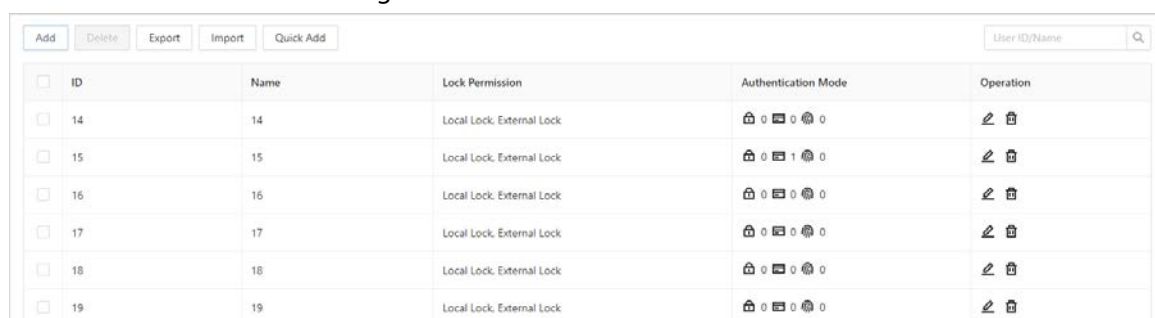
3.4.1 Personeelsbeheer

Beheer en bekijk de informatie van personen, kaarten, wachtwoorden en vingerafdrukken.

Procedure

- Stap 1 Log in op de webpagina.
- Stap 2 Klik op **Config** naast de overeenkomstige VTO.
- Stap 3 Selecteer **Personeelsbeheer**.

Figuur 3-15 Personeelsbeheer



ID	Name	Lock Permission	Authentication Mode	Operation
14	14	Local Lock; External Lock	0 0 0 0	Edit Delete
15	15	Local Lock; External Lock	0 0 1 0	Edit Delete
16	16	Local Lock; External Lock	0 0 0 0	Edit Delete
17	17	Local Lock; External Lock	0 0 0 0	Edit Delete
18	18	Local Lock; External Lock	0 0 0 0	Edit Delete
19	19	Local Lock; External Lock	0 0 0 0	Edit Delete

Stap 4 Klik op **Toevoegen**.

Stap 5 Configureer de parameters en klik vervolgens op **Toevoegen**.

Figuur 3-16 Voeg de persoon toe

Tabel 3-2 Parameterbeschrijving van het toevoegen van een persoon

Parameter	Beschrijving
Gebruikers-ID	Voer de gebruikers-ID en de naam in.
Naam	 De gebruikers-ID kan niet hetzelfde zijn als de bestaande ID.
Vergrendel toestemming	Selecteer de vergrendelingsmachtiging. - Lokale vergrendeling: Lokale vergrendeling. - Extern slot: RS-485 slot.
Ontgrendelen van meerdere deuren	Als deze optie is ingeschakeld, worden na succesvolle verificatie alle vergrendelingen waarvoor de gebruiker toestemming heeft, ingeschakeld.

Parameter	Beschrijving
Verificatiemodus	Voeg het wachtwoord, de kaart of de vingerafdruk toe. - Wachtwoord: Selecteer Wachtwoord > Toevoegen , voer het wachtwoord in, bevestig het wachtwoord en klik vervolgens op OK . - Kaart: Selecteer Kaart > Toevoegen , veeg de kaart door de kaartlezer of voer het kaartnummer in en klik vervolgens op Toevoegen .  Klik op Wijzigen om het kaartleesapparaat te wijzigen. Als u Enrollment Reader selecteert , moet u het kaarttype selecteren uit IC-kaart en ID-kaart. - Vingerafdruk: Selecteer Vingerafdruk > Toevoegen , druk uw vinger 3 keer achter elkaar op de scanner en klik vervolgens op Toevoegen .  Klik op Wijzigen om het herkenningsapparaat te wijzigen.

Verwante bewerkingen

- Voeg snel een persoon toe.
 - Klik op **Snel toevoegen** .
 - Configureer het gebruikers-ID-nummer waarmee u wilt beginnen en voer de totale hoeveelheid in.
 - Configureer de vergrendelingsmachtiging en het ontgrendelen van meerdere deuren.
 - Selecteer **Kaart > Toevoegen** , veeg de kaart door de kaartlezer of voer het kaartnummer in en klik vervolgens op **Toevoegen** .

Klik op **Wijzigen** om het kaartleesapparaat te wijzigen. Als u **Enrollment Reader selecteert** , moet u het kaarttype selecteren uit IC-kaart en ID-kaart.

- Klik op **Toevoegen** .
- Verwijder, exporteer of importeer de persoonsgegevens.

Bij het exporteren van de personeninformatie kunt u het bestandswachtwoord configureren. Voer het wachtwoord in wanneer u het informatiebestand importeert naar andere VTO's.

3.4.2 VTH-kamernummertoewijzing

U kunt het inbelnummer voor de bijbehorende VTH-ID instellen. Bel na het toewijzen de VTH alleen via het geconfigureerde nummer.



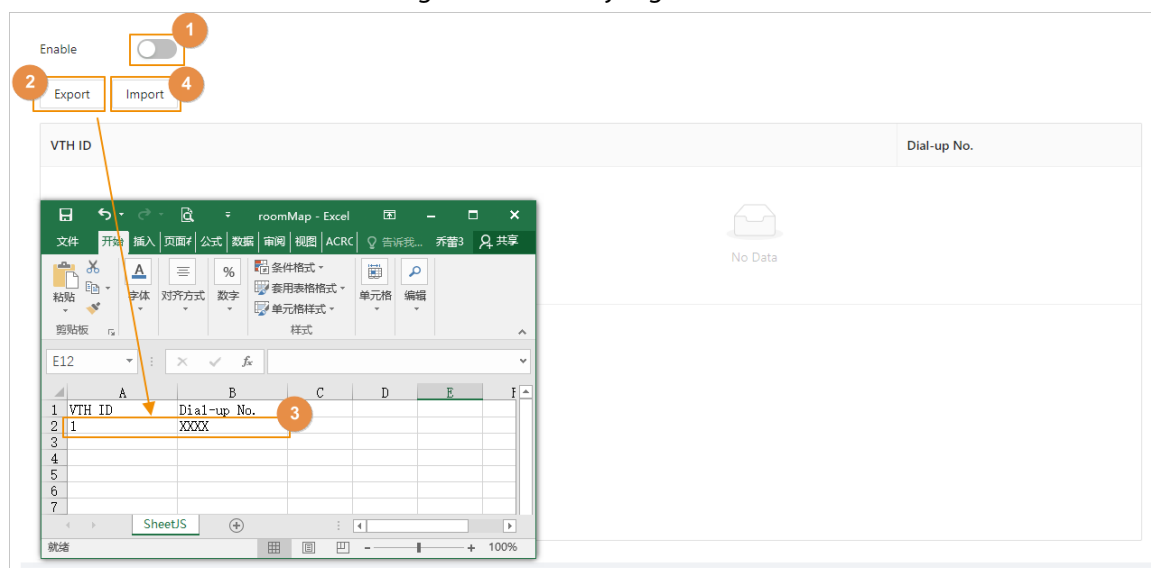
De VTH-kamernummertoewijzingsfunctie is alleen geldig wanneer de toetsenbordmodule is aangesloten

Procedure

- Stap 1** Log in op de webpagina.
- Stap 2** Klik op **Config** naast de overeenkomstige VTO.
- Stap 3** Selecteer **Kamernummertoewijzing** en configureer vervolgens de toewijzing.
- 1) Schakel de functie in.
 - 2) Klik op **Exporteren** om de sjabloon te downloaden.
 - 3) Voer de VTH-ID in, configureer het bijbehorende inbelnummer en sla de sjabloon op.
 - 4) Klik op **Importeren** om het bestand te uploaden.

De geconfigureerde inbelnummers worden op het systeem weergegeven.

Figuur 3-17 Toewijzing



3.4.3 Toegangscontrole

3.4.3.1 Configuratie

Procedure

- Stap 1** Log in op de webpagina.
- Stap 2** Klik op **Config** naast de overeenkomstige VTO.
- Stap 3** Selecteer **Toegangscontrole > Config**.
- Stap 4** Configureer de parameters.

Figuur 3-18 Toegangscontrole

Tabel 3-3 Beschrijving van de toegangscontroleparameters

Parameter	Beschrijving
Interval tussen opeenvolgende ontgrendelingen	Pas na de pauze kan de deur weer ontgrendeld worden.
Controleer het deurdetectorsignaal voordat u de deur vergrendelt	Schakel de functie in indien nodig. Indien ingeschakeld, wordt de deurdetectorstatus gedetecteerd voordat deze wordt vergrendeld om te voorkomen dat de deur wordt geopend.
IC-kaartcodering	Schakel de functie in zodat de IC-kaartcodering van kracht wordt.
Status deurdetector	• NC : Normaal gesloten. • NEE : Normaal open.

Stap 5 Klik op **Toepassen** .

3.4.3.2 RS-485

Procedure

- Stap 1 Log in op de webpagina.
- Stap 2 Klik op **Config** naast de overeenkomstige VTO.
- Stap 3 Selecteer **Toegangscontrole** > **RS-485** .
- Stap 4 Configureer de parameters van het slot dat via de RS-485-poort is aangesloten.

Afbeelding 3-19 RS-485

Tabel 3-4 RS-485-beschrijving

Parameter	Beschrijving
Poorttype	vergrendeld .

Parameter	Beschrijving
Interval tussen opeenvolgende ontgrendelingen	Pas na de pauze kan de deur weer ontgrendeld worden.

Stap 5 Klik op **Toepassen** .

3.4.4 Module

Bekijk de VTO, alle cascading modules en versie-informatie. Werk de VTO en de modules bij.

Procedure

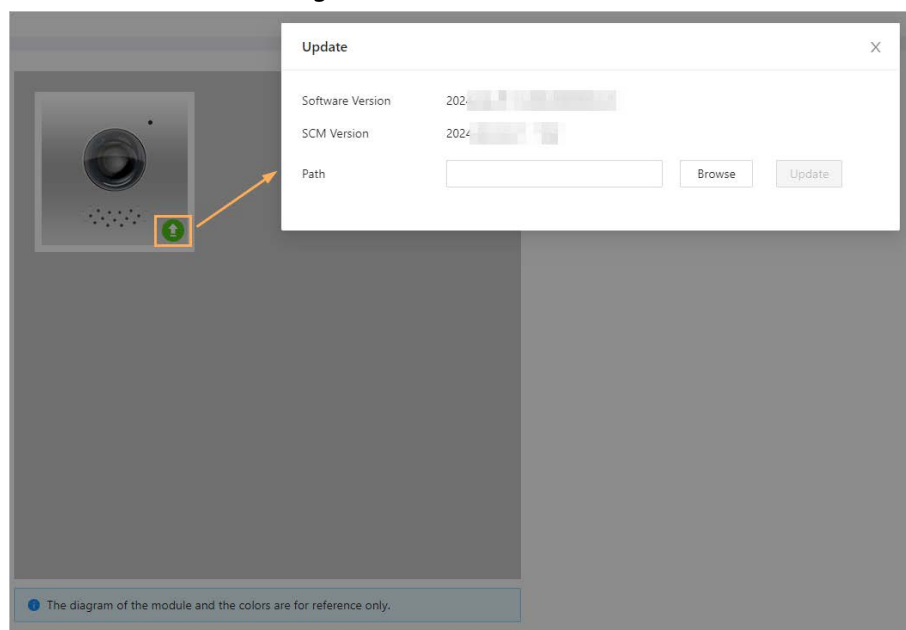
Stap 1 Log in op de webpagina.

Stap 2 Klik op **Config** naast de overeenkomstige VTO.

Stap 3 Selecteer **Module** .

- Bekijk de VTO en alle bijbehorende modules.
- Klik  om de huidige versie-informatie te bekijken.
- Klik op **Bladeren** om het updatebestand te selecteren en klik vervolgens op **Bijwerken** .

Figuur 3-20 Module



3.4.5 Onderhoud

Procedure

Stap 1 Log in op de webpagina.

Stap 2 Klik op **Config** naast de overeenkomstige VTO.

Stap 3 Selecteer **Onderhoud** .

- Klik op **Fabrieksinstellingen** om de standaardinstellingen te herstellen.
- Klik op **Opnieuw opstarten** om de controller opnieuw op te starten.

3.5 Persoon toevoegen

Voeg de persoon toe en stuur de informatie naar VTO.

Procedure

Stap 1 Log in op de webpagina.

Stap 2 Klik op **Persoon toevoegen** en configureer vervolgens de parameters.

Figuur 3-21 Persoon toevoegen

The screenshot shows a web interface for adding a person. The main window is titled 'Add Person'. It has a progress indicator with two steps: '1 Add Person' and '2 Select Device'. The 'Add Person' step is currently active. Under the 'Basic Info' section, there are two required input fields: 'User ID' and 'Name'. Below these, there are checkboxes for 'Local Lock' and 'External Lock', both of which are checked. There is also a checkbox for 'Multi-Door Unlock' with a description: 'After verification is successful, all the locks that the user has permission for will be enabled.' Under the 'Verification Mode' section, there are three expandable sections: 'Password', 'Card', and 'Fingerprint'. Each section shows 'Not Added' and has an 'Add' button. At the bottom right of the window are 'Cancel' and 'Next' buttons.

Tabel 3-5 Parameterbeschrijving van het toevoegen van een persoon

Parameter	Beschrijving
Gebruikers-ID	Voer de gebruikers-ID en de naam in.
Naam	 De gebruikers-ID mag niet hetzelfde zijn als de bestaande ID.
Vergrendel toestemming	Selecteer de vergrendelingsmachtiging. • Lokale vergrendeling: Lokale vergrendeling. • Extern slot: RS-485 slot.
Ontgrendelen van meerdere deuren	Als deze optie is ingeschakeld, worden na succesvolle verificatie alle vergrendelingen waarvoor de gebruiker toestemming heeft, ingeschakeld.

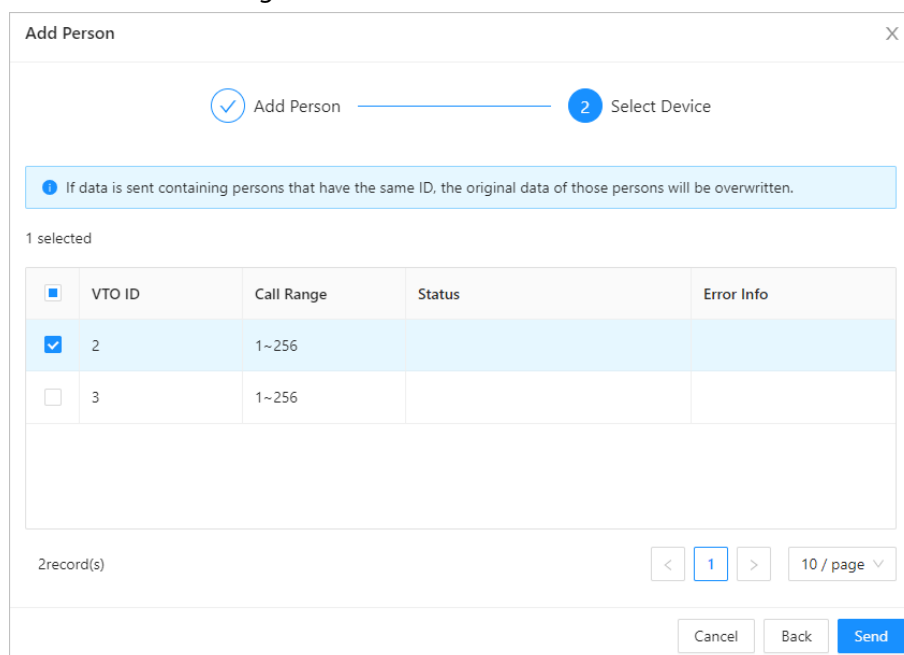
Parameter	Beschrijving
Verificatiemodus	Voeg het wachtwoord, de kaart of de vingerafdruk toe. - Wachtwoord: Selecteer Wachtwoord > Toevoegen , voer het wachtwoord in, bevestig het wachtwoord en klik vervolgens op OK . - Kaart: Selecteer Kaart > Toevoegen , veeg de kaart door de kaartlezer of voer het kaartnummer in en klik vervolgens op Toevoegen .  Klik op Wijzigen om het kaartleesapparaat en het kaarttype te wijzigen. - Vingerafdruk: Selecteer Vingerafdruk > Toevoegen , druk uw vinger 3 keer achter elkaar op de scanner en klik vervolgens op Toevoegen .  Klik op Wijzigen om het herkenningsapparaat te wijzigen.

Stap 3 Klik op **Volgende** .

Stap 4 Selecteer het apparaat en klik vervolgens op **Verzenden** .

De persoonsgegevens worden naar de door u geselecteerde VTO verzonden.

Figuur 3-22 Selecteer de VTO



Add Person

1 Add Person 2 Select Device

If data is sent containing persons that have the same ID, the original data of those persons will be overwritten.

1 selected

☐	VTO ID	Call Range	Status	Error Info
☒	2	1~256		
☐	3	1~256		

2record(s)

< 1 > 10 / page

Cancel Back Send

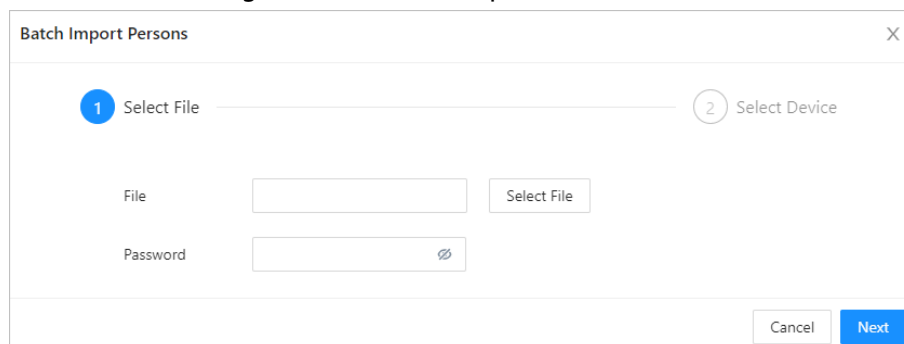
3.6 Personen in batches importeren

Nadat u de persoonsgegevens uit de VTO hebt geëxporteerd, kunt u het bestand uploaden om personen in batches naar andere VTO's te importeren.

Procedure

- Stap 1 Log in op de webpagina.
- Stap 2 Klik op **Batch Import Personen**.
- Stap 3 Selecteer het bestand, voer het wachtwoord in dat is geconfigureerd bij het exporteren van de informatie en klik vervolgens op **Volgende**.

Figuur 3-23 Mensen importeren



- Stap 4 Selecteer het apparaat en klik vervolgens op **Verzenden**.
De persoonsgegevens worden naar de door u geselecteerde VTO verzonden.

3.7 Netwerkinstellingen

3.7.1 TCP/IP configureren

U moet het IP-adres van het apparaat configureren om ervoor te zorgen dat het met andere apparaten kan communiceren.

Procedure

- Stap 1 Log in op de webpagina.
- Stap 2 Selecteer **Netwerkinstellingen > TCP/IP**.
- Stap 3 Configureer de parameters.

Figuur 3-24 TCP/IP

The screenshot displays a network configuration window. At the top, under 'Mode', there are two radio buttons: 'DHCP' and 'Static'. The 'Static' button is selected. Below this, there are several input fields: 'MAC Address', 'IP Address', 'Subnet Mask', 'Default Gateway', 'Preferred DNS', and 'Alternate DNS'. Each field is represented by a series of small boxes for individual digits. At the bottom of the window, there are three buttons: 'Apply' (highlighted in blue), 'Refresh', and 'Default'.

Tabel 3-6 Beschrijving van TCP/IP-parameters

Parameter	Beschrijving
Modus	• DHCP (Dynamic Host Configuration Protocol): Het apparaat krijgt automatisch een IP-adres, subnetmasker en gateway toegewezen. • Statisch : Voer handmatig het IP-adres, subnetmasker en de gateway in.
MAC-adres	MAC-adres van het apparaat.
IP-adres	Als u de modus instelt op Statisch , configureert u het IP-adres, subnetmasker en de gateway.
Subnetmasker	
Standaardgateway	 • Het IPv6-adres wordt weergegeven in hexadecimaal. • Voor de IPv6-versie is het niet nodig om subnetmaskers in te stellen. • Het IP-adres en de standaardgateway moeten zich in hetzelfde netwerksegment bevinden.
Voorkeurs-DNS	Stel het IP-adres van de gewenste DNS-server in.
Alternatieve DNS	Stel het IP-adres van de alternatieve DNS-server in.

Stap 4 Klik op **Toepassen** .

3.7.2 Basisservices configureren

Meld u aan op de webpagina en selecteer vervolgens **Netwerkinstellingen** > **Basisservices** .

Schakel het protocol indien nodig in en klik vervolgens op **Toepassen** .

Figuur 3-25 Basisdiensten

Tabel 3-7 Beschrijving van basisdiensten

Dienst	Beschrijving
SSH	Als deze optie is ingeschakeld, kunt u via SSH inloggen op de VTO.
CGI	Common Gateway Interface (CGI) biedt een standaardprotocol waarmee webserver programma's kunnen uitvoeren op een manier die vergelijkbaar is met consoletoepassingen die op een server worden uitgevoerd en dynamisch webpagina's genereren. Indien ingeschakeld, kunnen CGI-opdrachten worden gebruikt. CGI is standaard ingeschakeld.
Wachtwoord opnieuw instellen	Standaard ingeschakeld. Schakel de functie in en configureer vervolgens het e-mailadres. Na de configuratie kunt u op de inlogpagina op Wachtwoord vergeten? klikken om het wachtwoord opnieuw in te stellen.
Multicast/Broadcast-zoekopdracht	Als u deze functie inschakelt, kunnen meerdere gebruikers tegelijkertijd via het netwerk een voorbeeld van de videobeelden van het apparaat bekijken. Zo kunnen ze uw apparaat vinden met het multicast-/broadcastprotocol.
Authenticatiemodus	• Beveiligingsmodus (aanbevolen) : Deze modus ondersteunt geen aanmelding met Digest, DES en plattetekstverificatie. • Compatibiliteitsmodus : De modus ondersteunt inloggen met Digest, DES en plattetekstverificatie.
Noodonderhoud	Wanneer deze functie is ingeschakeld en het apparaat 5 keer achter elkaar niet opnieuw kan worden opgestart, wordt automatisch een servicepoort ingeschakeld die door de technische ondersteuning wordt gebruikt om upgrades en herstel uit te voeren.
Wachtwoord verloopt over	Selecteer de tijd waarop het wachtwoord verloopt.
Privéprotocol	Als deze optie is ingeschakeld, heeft het platform toegang tot het

Dienst	Beschrijving
TLSv1.1	apparaat met een privéprotocol.  Er bestaat een beveiligingsrisico als u TLSv1.1 inschakelt.

3.8 Onderhoudscentrum

3.8.1 Diagnose met één klik

Het systeem diagnosticeert automatisch de configuraties en de status van het apparaat om de prestaties ervan te verbeteren.

Procedure

Stap 1 Log in op de webpagina.

Stap 2 Selecteer **Onderhoudscentrum** > **Diagnose met één klik**.

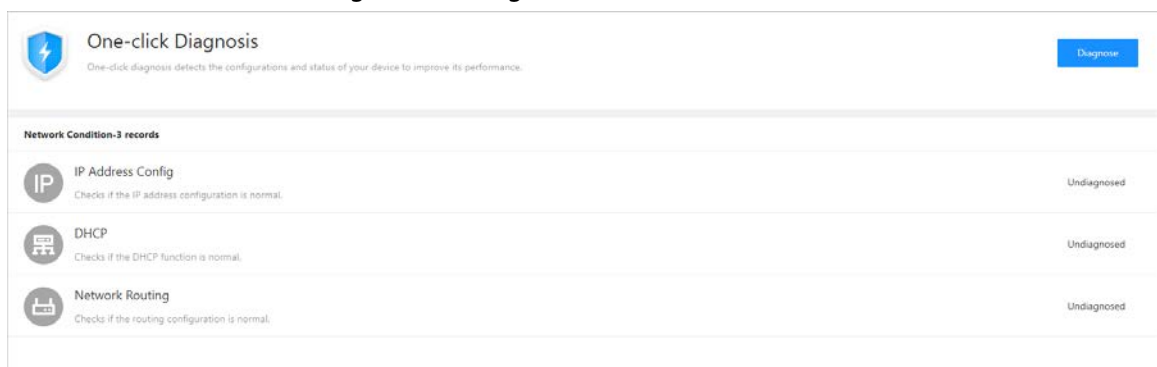
Stap 3 Klik op **Diagnose**.

Het systeem diagnosticeert automatisch de configuraties en de status van het apparaat en geeft de diagnoseresultaten weer nadat de diagnose is voltooid.

Stap 4 (Optioneel) Klik op **Details** om details van afwijkende items te bekijken.

U kunt de afwijking negeren of optimaliseren. U kunt ook op **Diagnose Again klikken** om de automatische diagnose opnieuw uit te voeren.

Figuur 3-26 Diagnose met één klik



3.8.2 Systeminformatie

Meld u aan op de webpagina, selecteer **Onderhoudscentrum** > **Systeeminfo** en bekijk de kennisgeving over de opensourcesoftware.

Selecteer **Juridische informatie** om de kennisgeving over opensourcesoftware te bekijken.

Selecteer **Systeeminfo** om de versie-informatie van de controller te bekijken.

3.8.3 Configuratiebestanden exporteren en importeren

U kunt het configuratiebestand voor het apparaat importeren en exporteren. Wanneer u dezelfde configuraties op meerdere apparaten wilt toepassen, kunt u het configuratiebestand naar hen importeren.

Procedure

Stap 1 Log in op de webpagina.

Stap 2 Selecteer **Onderhoudscentrum > Config**.

Figuur 3-27 Configuratiebeheer

Stap 3 Exporteer of importeer configuratiebestanden.

- Exporteer het configuratiebestand.

Klik op **Configuratiebestand exporteren** om het bestand naar de lokale computer te downloaden.



Het IP-adres wordt niet geëxporteerd.

- Importeer het configuratiebestand.
 1. Klik op **Bladeren** om het configuratiebestand te selecteren.
 2. Klik op **Configuratie importeren**.



Configuratiebestanden kunnen alleen worden geïmporteerd naar apparaten met hetzelfde model.

3.8.4 Het systeem updaten



- Gebruik het juiste updatebestand. Zorg ervoor dat u het juiste updatebestand van de technische ondersteuning krijgt.
- Koppel de stroomvoorziening of het netwerk niet los en start het apparaat niet opnieuw op of schakel het niet uit tijdens de update.

Procedure

Stap 1 Log in op de webpagina.

Stap 2 Selecteer **Onderhoudscentrum > Bijwerken**.

Stap 3 Klik in het gedeelte **Bestandsupdate op Bladeren** en upload vervolgens het updatebestand.



Het updatebestand moet een .bin-bestand zijn.

Stap 4 Klik op **Bijwerken**.

De 2-draadscontroller wordt opnieuw opgestart nadat de update is voltooid.

Figuur 3-28 Bestandsupdate

The screenshot shows a web interface titled 'File Update'. It contains a text input field with the placeholder text 'File'. To the right of the input field is a 'Browse' button. Further to the right is an 'Update' button.

3.8.5 Geavanceerd onderhoud

Verzamel apparaatgegevens en leg pakketten vast, zodat onderhoudspersoneel gemakkelijker problemen kan oplossen.

3.8.5.1 Exporteren

Procedure

Stap 1 Log in op de webpagina.

Stap 2 Selecteer **Onderhoudscentrum** > **Geavanceerd onderhoud** > **Exporteren**.

Stap 3 Klik op **Exporteren** om het serienummer, de firmwareversie, de apparaatwerkingslogboeken en de configuratiegegevens te exporteren.

3.8.5.2 Pakket vastleggen

Procedure

Stap 1 Log in op de webpagina.

Stap 2 Selecteer **Onderhoudscentrum** > **Geavanceerd onderhoud** > **Pakketvastlegging**.

Figuur 3-29 Pakketvastlegging

The screenshot shows a web interface titled 'Packet Capture'. It contains a table with the following columns: NIC, Device Address, IP 1: Port 1, IP 2: Port 2, Packet Sniffer Size, and Packet Sniffer Backup. There are two rows of data, one for eth0 and one for eth2. Each row has input fields for the IP addresses and a 'Packet Sniffer Size' of 0.00MB. A 'Packet Sniffer Backup' button is also present for each row.

NIC	Device Address	IP 1: Port 1	IP 2: Port 2	Packet Sniffer Size	Packet Sniffer Backup
eth0	192.168.1.155	Optional	Optional	0.00MB	▶
eth2	192.168.1.101	Optional	Optional	0.00MB	▶

Stap 3 Voer het IP-adres in en klik op ▶.

▶ verandert in ||.

Stap 4 Nadat u voldoende gegevens hebt verzameld, klikt u op ||.

Vastgelegde pakketten worden automatisch gedownload naar uw lokale computer.

Bijlage 1 Beveiligingsaanbeveling

Accountbeheer

1. Gebruik complexe wachtwoorden

Raadpleeg de volgende suggesties voor het instellen van wachtwoorden:

- De lengte mag niet korter zijn dan 8 tekens;
- Gebruik minimaal twee soorten tekens: hoofdletters en kleine letters, cijfers en symbolen;
- Gebruik niet de accountnaam of de accountnaam in omgekeerde volgorde;
- Gebruik geen doorlopende tekens, zoals 123, abc, enz.;
- Gebruik geen herhalende tekens, zoals 111, aaa, enz.

2. Wijzig wachtwoorden regelmatig

Het is raadzaam om het wachtwoord van het apparaat regelmatig te wijzigen om het risico op raden of kraken te verkleinen.

3. Wijs accounts en machtigingen op de juiste manier toe

Voeg gebruikers toe op basis van de service- en beheervereisten en wijs minimale machtigingen toe aan gebruikers.

4. Schakel de accountvergrendelingsfunctie in

De accountvergrendelingsfunctie is standaard ingeschakeld. U wordt geadviseerd deze ingeschakeld te houden om de beveiliging van uw account te beschermen. Na meerdere mislukte wachtwoordpogingen worden het bijbehorende account en bron-IP-adres vergrendeld.

5. Stel de wachtwoordherstelinformatie tijdig in en werk deze bij

Het apparaat ondersteunt de wachtwoordherstelfunctie. Om het risico te verkleinen dat deze functie door dreigingsactoren wordt gebruikt, moet u de informatie tijdig aanpassen als er een wijziging is. Bij het instellen van beveiligingsvragen wordt aanbevolen geen gemakkelijk te raden antwoorden te gebruiken.

Serviceconfiguratie

1. HTTPS inschakelen

Het wordt aanbevolen om HTTPS in te schakelen voor toegang tot webservices via beveiligde kanalen.

2. Gecodeerde transmissie van audio en video

Als de inhoud van uw audio- en videogegevens erg belangrijk of gevoelig is, raden wij u aan om de functie voor gecodeerde overdracht te gebruiken. Zo verkleint u het risico dat uw audio- en videogegevens tijdens de overdracht worden afgeluisterd.

3. Schakel niet-essentiële services uit en gebruik de veilige modus

Als het niet nodig is, is het raadzaam om een aantal services uit te schakelen, zoals SSH, SNMP, SMTP, UPnP, AP-hotspot etc., om het aanvalsoppervlak te verkleinen.

Indien nodig is het sterk aan te raden om veilige modi te kiezen, waaronder maar niet beperkt tot de volgende services:

- SNMP: Kies SNMP v3 en stel sterke encryptie- en authenticatiewachtwoorden in.
- SMTP: Kies TLS om toegang te krijgen tot de mailboxserver.
- FTP: Kies SFTP en stel complexe wachtwoorden in.
- AP-hotspot: kies de WPA2-PSK-encryptiemodus en stel complexe wachtwoorden in.

4. **Wijzig HTTP en andere standaard servicepoorten**

Het wordt aanbevolen om de standaardpoort van HTTP en andere services te wijzigen naar een poort tussen 1024 en 65535. Zo verkleint u de kans dat kwaadwillenden uw identiteit raden.

Netwerkconfiguratie

1. **Schakel de lijst Toestaan in**

Het wordt aanbevolen om de functie voor de toegestane lijst in te schakelen en alleen IP's in de toegestane lijst toegang tot het apparaat te geven. Zorg er daarom voor dat u het IP-adres van uw computer en het IP-adres van het ondersteunende apparaat toevoegt aan de toegestane lijst.

2. **MAC-adresbinding**

Het wordt aanbevolen om het IP-adres van de gateway te koppelen aan het MAC-adres op het apparaat om het risico op ARP-spoofing te verkleinen.

3. **Bouw een veilige netwerkomgeving**

Om de veiligheid van apparaten beter te waarborgen en potentiële cyberrisico's te verminderen, worden de volgende aanbevelingen gedaan:

- Schakel de poorttoewijzingsfunctie van de router uit om directe toegang tot de intranetapparaten vanaf een extern netwerk te voorkomen;
- Partitioneer het netwerk volgens de werkelijke netwerkbehoeften: als er geen communicatievraag is tussen de twee subnetten, wordt aanbevolen om VLAN, gateway en andere methoden te gebruiken om het netwerk te partitioneren om netwerkisolatie te bereiken;
- Stel een 802.1x-toegangsauthenticatiesysteem in om het risico op illegale toegang van terminals tot het privénetwerk te verkleinen.

Beveiligingscontrole

1. **Controleer online gebruikers**

Het is raadzaam om regelmatig online gebruikers te controleren om illegale gebruikers te identificeren.

2. **Controleer het apparaatlogboek**

Door logboeken te bekijken, krijgt u inzicht in de IP-adressen waarmee wordt geprobeerd in te loggen op het apparaat en de belangrijkste handelingen van de ingelogde gebruikers.

3. **Netwerklogboek configureren**

Vanwege de beperkte opslagcapaciteit van apparaten is het opgeslagen log beperkt. Als u het log voor een lange tijd moet opslaan, wordt aanbevolen om de netwerklogfunctie in te schakelen om ervoor te zorgen dat de kritieke logs worden gesynchroniseerd met de netwerklogserver voor tracering.

Softwarebeveiliging

1. **Firmware op tijd updaten**

Volgens de standaard operationele specificaties van de industrie, moet de firmware van apparaten tijdig worden bijgewerkt naar de nieuwste versie om ervoor te zorgen dat het apparaat de nieuwste functies en beveiliging heeft. Als het apparaat is aangesloten op het openbare netwerk, wordt aanbevolen om de online upgrade automatische detectiefunctie in te schakelen, om de firmware-update-informatie die door de fabrikant is vrijgegeven tijdig te verkrijgen.

2. **Werk de clientsoftware op tijd bij**

Het is raadzaam om de nieuwste clientsoftware te downloaden en te gebruiken.

Fysieke bescherming

Het is raadzaam om fysieke beveiliging toe te passen op apparaten (met name opslagapparaten). Dit kan bijvoorbeeld door het apparaat in een speciale machinekamer en kast te plaatsen en toegangscontrole en sleutelbeheer in te stellen om te voorkomen dat onbevoegden hardware en andere randapparatuur beschadigen (bijvoorbeeld een USB-stick of seriële poort).