Trådlöst relä

Bruksanvisning



ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD. V1.0.0

Innehållsförteckning

1 Inledning 1
1.1 Översikt 1
1.2 Tekniska specifikationer 1
2 Checklista 3
3 Utseende 4
4 Lägga till det trådlösa reläet till hubben 5
5 Installation 6
5.1 Kabeldragning 6
5.2 Installera det trådlösa reläet 7
6 Konfiguration 8
6.1 Se status 8
6.2 Konfigurera reläet 8
Bilaga 1 Rekommendationer beträffande cybersäkerhet 11

1 Inledning

1.1 Översikt

Ett trådlöst relä är en torr kontaktenhet som används för att fjärrstyra 0–36 VDC ström. Reläets torra kontakt är elektriskt isolerad från enhetens strömförsörjningskrets. Relä kan användas vid lågspänning för att styra strömförsörjningen till andra enheter. Enheten levereras med ett överspännings- och överhettningsskydd.

1.2 Tekniska specifikationer

Det här avsnittet innehåller tekniska specifikationer för reläet. Se de som motsvarar din modell.

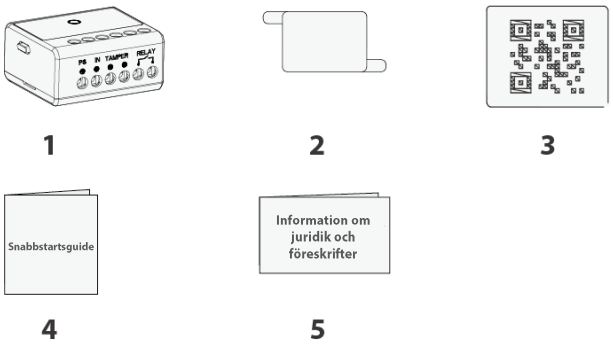
Tabell 1-1 Tekniska specifikationer

Typ	Parameter	Beskrivning	
Funktion	Indikatorlampa	1 för flera statusar (parkoppling, strömstatus och larm)	
	Knapp	1	
	Uppdatering på distans	Uppdatering via molnet	
	Signalstyrka	Detekterar signalstyrka	
Trådlöst	Bärvågsfrekvens	DHI-ARM7011-W2(868): 868–868,6 MHz	DHI-ARM7011-W2: 433,1–434,6 MHz
	Kommunikationsavstånd	DHI-ARM7011-W2(868): Upp till 1200 m (3937,01 fot) i öppet utrymme	DHI-ARM7011-W2: Upp till 800 m (2624,67 fot) i öppet utrymme
	Sändareffekt	DHI-ARM7011-W2(868): Gränsvärde på 25 mW	DHI-ARM7011-W2: Gränsvärde på 15,8 mW
	Kommunikationsmekanism	Tvåvägs	
	Krypteringsläge	AES128	
	Frekvenshopp	Ja	
Allmänt	Arbetstemperatur	-10–55 °C (14–131 °F) (inomhus)	
	Förvaringstemperatur	-10–55 °C (14–131 °F)	
	Luftfuktighet vid drift	10–90 % (RH)	
	Luftfuktighet vid förvaring	10–90 % (RH)	
	Nätaggregat	DHI-ARM7011-W2(868) och DHI-ARM7011-W2: 7–24 VDC	
	Produktens mått	39 x 33 x 19 mm (1,54 x 1,30 x 0,75 tum)	
	Förpackningens mått	95 x 59,5 x 30,5 mm (3,74 x 2,34 x 1,20 tum)	
	Installation	Väggfäste	

Typ	Parameter	Beskrivning	
	Nettovikt	45 g (0,10 lb)	
	Bruttovikt	60 g (0,13 lb)	
	Certifieringar	DHI-ARM7011-W2(868): CE	DHI-ARM7011-W2: CE, FCC
	Höljets material	PC + ABS	
Teknik	Testläget	Ja	
Port	Larmingång	1 för sabotage, NO/NC	
	Reläutgång	1, NO/NC (0–36 VAC, Max 5A）	

2 Checklista

Figur 2-1 Checklista

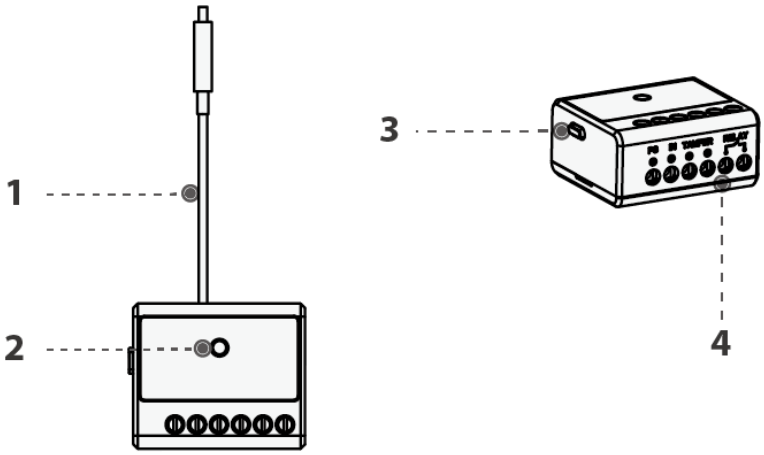


Tabell 2-1 Checklista

Nr.	Artikelnamn	Kvantitet	Nr.	Artikelnamn	Kvantitet
1	Relä	1	4	Snabbstartsguide	1
2	Dubbelsidig tejp	1	5	Information om juridik och föreskrifter	1
3	QR-kod	1	–	–	–

3 Utseende

Figur 3-1 Utseende



Tabell 3-1 Struktur

Nr.	Namn	Beskrivning
1	Antenn	Skickar och tar emot signaler.
2	Indikering	• Tryck på och håll knappen nedtryckt i två sekunder för att aktivera systemets parkopplingsläge. ◊ Lyser fast under 1 sekund, släcks sedan under 0,5 sekunder och lyser sedan fast: Sammankopplingen lyckades. ◊ Blinkar långsamt i 3 sekunder och släcks sedan: Sammankopplingen misslyckades. • Efter att enheten är påslagen kan du trycka på och håll knappen nedtryckt i två sekunder för att stänga av den.
3	Strömknapp	
4	Ledningsterminal	Reläet kan anslutas till en 6,5–36,5 VDC strömförsörjning. • PS IN: Matningsanslutning. Är den ansluten direkt till strömkabeln? • RAMP: Ingångsterminal för extern enhet. Den är ansluten till den externa enheten för att utlösa sabotagelarm. • RELÄ: Anslutningen mellan utgångsterminalen och matningsanslutningen styrs genom att öppna och stänga det inbyggda reläet.

4 Lägga till det trådlösa reläet till hubben

Installera DMSS-appen på din telefon innan du ansluter reläet till hubben. Den här bruksanvisningen använder iOS som exempel.

- Se till att versionen av DMSS-appen är 1.99.200 eller senare och hubben är version V1.001.0000004.0.R.221104 eller senare.
- Se till att du redan har skapat ett konto och lagt till hubben i DMSS.
- Se till att hubben har en stabil internetanslutning.
- Se till att hubben är inaktiverad.

Steg 1: Gå till hubbens skärm och tryck på **Kringutrustning** (Peripheral) för att lägga till reläet.

Steg 2: Tryck på **+** för att skanna QR-koden längst ned på reläet och tryck sedan på **Nästa** (Next).

Steg 3: Tryck på **Nästa** (Next) när reläet har hittats.

Steg 4: Följ instruktionerna på skärmen och slå på reläet. Tryck sedan på **Nästa** (Next).

Steg 5: Vänta på parkopplingen.

Steg 6: Anpassa namnet på reläet och välj området. Tryck sedan på **Slutförd** (Completed).

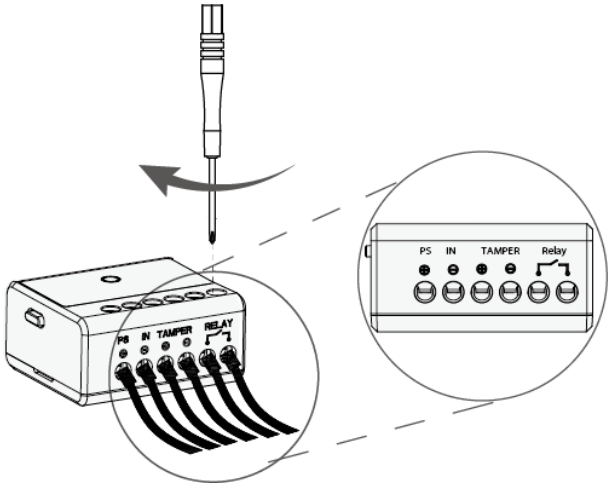
5 Installation

Innan installationen ska du lägga till reläet till hubben och kontrollera signalstyrkan vid installationsplatsen. Vi rekommenderar att du installerar reläet på en plats med en signalstyrka på minst 2 staplar.

5.1 Kabeldragning

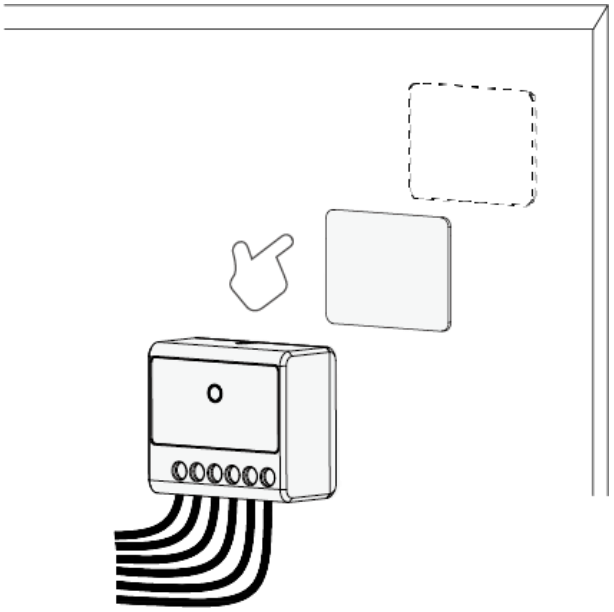
- Reläet kan anslutas till en 6,5–36,5 VDC strömförsörjning.
- Baserat på dess mått kan du installera reläet i kopplingsdosan, inuti den elektriska apparatens höljet eller på distributionskortet.

Figur 5-1 Ledning



5.2 Installera det trådlösa reläet

Figur 5-2 Fästa reläet



6 Konfiguration

Du kan se och redigera allmän information om reläet.

6.1 Se status

Välj ett relä från tillbehörslistan på hubbens skärm. Sedan kan du se statusen för reläet.

Tabell 6-1 Status

Parameter	Värde
Tillfälligt inaktivering	Status för om uppreparens funktioner är aktiverade eller avaktiverade. ● : Aktivera. ● : Avaktivera.
Signalstyrka	Signalstyrkan mellan hubben och reläet. ● : Låg. ● : Svag. ● : God. ● : Utmärkt. ● : Nr.
Ingångspänning	Spänningsvärde för inmatningen.
Utgångsstatus	Reläets utgångsstatus.
Online-status	Online- och offline-status för reläet. ● : Online. ● : Offline.
Skicka via upprepare	Status för om reläet vidarebefordrar tillbehörsmeddelanden till hubben via uppreparen.
Programversion	Reläets programversion.

6.2 Konfigurera reläet

Välj ett relä från kringutrustningslistan på hubbens skärm. Tryck sedan på för att konfigurera reläets parametrar.

Tabell 6-2 Parameterbeskrivning

Parameter	Beskrivning
Enhetskonfiguration	● Se reläets namn, typ, serienummer och modell. ● Redigera reläets namn och tryck sedan på **Spara** (Save) för att spara konfigurationen.
Område	Välj det område som reläet är tilldelat.

Parameter	Beskrivning
Tillfälligt inaktivering	Om sensorinformation skickas till larmhubben. • Tryck på **Aktivera** (Enable). Reläet skickar sedan larmmeddelanden till hubben. **Aktivera** (Enable) är satt som standard. • Tryck på **Inaktivera** (Disable). Reläet upphör sedan att skicka larmmeddelanden till hubben.
Utgångstyp	Välj mellan **Vanligtvis öppet** (Normally Open) eller **Vanligtvis stängt** (Normally Closed). **Vanligtvis öppet** (Normally Closed) är satt som standard.
Utgångsläge	Välj mellan (**Stabilt läge**) (Steady State) eller (**Puls**) (Pulse). **Puls** (Pulse) är satt som standard. När du väljer som Pulse (**Puls**) kan du ställa in pulslängden.
Lysdiodindikator	Lysdiodindikatorn (LED Indicator) är aktiverad som standard.  Om lysdiodindikatorn är inaktiverad förblir den släckt oavsett om reläet fungerar normalt eller inte.
Scenarioinställning	Konfigurera scenarier som låter dig associera reläet för att utföra motsvarande åtgärd. Klicka på **Skapa scenario** (Create Scenario). Sedan kan du välja mellan, **Aktivering/inaktivering av länkningsscenario, Larm för länkningsscenario** (Arming/Disarming Linkage Scenario, Alarm Linkage Scenario) eller **Schemalagt länkningsscenario** (Scheduled Linkage Scenario). • **Aktivera/inaktivera länkningsscenario:** Efter att du har valt anpassat namn på scenariot och länkområde kan du aktivera eller inaktivera ,**Aktivera länkningsutgångsmodul, Inaktivera länkningsutgångsmodul** (Arming Linkage Output Module, Disarming Linkage Output Module) eller **Hemlägets länkningsutgångsmodul** (Home Mode Linkage Output Module). • **Larm för länkningsscenario** • **Schemalagt länkningsscenario:** Efter att du har valt anpassat namn på scenariot och aktiverat **Modul för länkningsutgångsmodul** (Scheduled Linkage Output Module) kan du ställa in tid och upprepade perioder.
Externt sabotage	Efter att **Externt sabotage** (External Tamper) har aktiverats utlöses larm för externa sabotage.
Detektering av signalstyrka	Testa den aktuella signalstyrkan.

Parameter	Beskrivning
Övergångseffekt	• Välj mellan hög, låg och automatisk. • Ju högre effektnivån på överföringen är, desto längre kan överföringar färdas. Effektförbrukningen ökar dock. • Om du väljer **Låg** (Low) aktiverar reläet läget reducerad känslighet. • Vi rekommenderar att du väljer **Låg** (Low) när du installerar enheten för att testa signalstyrkan på installationsplatsen och sedan justerar till **Hög** (High) eller **Automatisk** (Automatic). • Indikatorn blinkar när du ställer in den till **Låg** (Low).
Ta bort	Ta bort reläet. Öppna hubbens skärm och välj reläet från listan. Svep sedan åt vänster för att ta bort den.

Bilaga 1 Rekommendationer beträffande cybersäkerhet

Cybersäkerhet är mer än bara ett modeord. Det är något som kan tillämpas på alla enheter som är anslutna till internet. IP-videoövervakning är inte immun mot cyberattacker. Att ta grundläggande steg för att skydda och stärka nätverk samt nätverksanslutna enheter göra dem dock mindre mottagliga för attacker. Nedan följer några tips och rekommendationer från Dahua om hur du kan skapa ett säkrare system.

Obligatoriska åtgärder som ska vidtas för grundläggande enhetssäkerhet i nätverket:

1. **Använd starka lösenord**
   Se följande förslag när lösenord skapas:
   - Längden bör inte vara mindre än 8 tecken.
   - Inkludera minst två typer av tecken. Olika typer av tecken inkluderar stora och små bokstäver, siffror och symboler.
   - Låt inte kontonamnet vara en del av lösenordet och använd inte kontonamnet i omvänd ordning.
   - Använd inte kontinuerliga tecken såsom 123 eller abc osv.
   - Använd inte överlappande tecken såsom 111 eller aaa osv.
2. **Uppdatera inbyggd programvara och klientprogramvara vid rätt tidpunkt**
   - Enligt bästa praxis inom teknikindustrin rekommenderar vi att hålla din enhets (såsom NVR, DVR, IP-kamera osv.) inbyggda programvara uppdaterad för att säkerställa att systemet är utrustat med de senaste säkerhetskorrigeringarna och uppdateringarna. När enheten är ansluten till det offentliga nätverket rekommenderas att funktionen "Automatisk kontroll av uppdateringar" aktiveras för att få aktuell information om uppdateringar av inbyggd programvara som har släppts av tillverkaren.
   - Vi föreslår att du laddar ned och använder den senaste versionen av klientprogramvaran.

Rekommendationer som är bra att använda för att förbättra enhetssäkerheten i nätverket:

1. **Fysiskt skydd**
   Vi rekommenderar att du skapar fysiskt skydd för enheten, särskilt på lagringsenheter. Placera enheten i till exempel ett speciellt datorrum och -skåp samt implementera behörigheter för åtkomstkontroll och nyckelhantering. Detta för att förhindra obehörig personal från att ha fysisk kontakt och kunna skada hårdvara, skapa otillåten anslutning av flyttbara enheter (såsom USB-minnen, seriella portar) osv.
2. **Byt lösenord regelbundet**
   Vi föreslår att du byter lösenord regelbundet för att reducera risken att det knäcks.
3. **Konfigurera och uppdatera information om återställning av lösenord**
   Enheten har stöd för funktionen att återställa lösenord. Uppdatera relevant information om lösenordsåterställning i tid, inklusive slutanvändarens e-postadress och skyddsfrågor för lösenord. Om informationen ändras ska den uppdateras i tid. När skyddsfrågor för lösenord skapas rekommenderar vi att du inte använder de som är lätta att gissa.

4. **Aktivera kontolåsning**
   Funktionen kontolåsning är aktiverad som standard och vi rekommenderar att den förblir aktiv för att garantera kontosäkerheten. Om en angripare försöker logga in med fel lösenord flera gånger blockeras motsvarande konto och källans IP-adress.
5. **Ändra de HTTP-portar och andra tjänsteportar som är standard**
   Vi rekommenderar att du ändrar de HTTP-portar och andra tjänsteportar som är standard till valfria portar mellan 1024–65535. Detta reducerar risken för att utomstående ska kunna gissa vilka portar som används.
6. **Aktivera HTTPS**
   Vi föreslår att du aktiverar HTTPS för att kunna besöka webbtjänster via en säker kommunikationskanal.
7. **MAC-adressbindning**
   Vi rekommenderar att du binder IP- och MAC-adresser för din gateway till enheten. Detta reducerar risken för ARP-spoofing.
8. **Tilldela konton och privilegier inom rimliga gränser**
   Lägg till användare enligt krav från verksamheten och ledningen samt tilldela endast den minsta uppsättning behörigheter som behövs.
9. **Inaktivera onödiga tjänster och välj säkra lägen**
   Om det inte behövs rekommenderas att vissa tjänster såsom SNMP, SMTP, UPnP osv. inaktiveras för att reducera riskerna.
   Vid behov rekommenderas starkt att du använder säkra lägen, inklusive men inte begränsade till, följande tjänster:
   - SNMP: Välj SNMP v3 och konfigurera starka krypterings- och autentiseringslösenord.
   - SMTP: Välj TLS för att komma åt e-postservern.
   - FTP: Välj SFTP och konfigurera starka lösenord.
   - AP-hotspot: Välj WPA2-PSK-krypteringsläget och konfigurera starka lösenord.
10. **Krypterad ljud- och videoöverföring**
    Om ljud- och videodata är mycket viktiga eller känsliga rekommenderar vi att du använder krypterad överföring för att reducera risken för att ljud- och videodata stjäls under överföringen.
    Påminnelse: krypterad överföring orsakar viss förlust av överföringseffektiviteten.
11. **Säker granskning**
    - Kontrollera online-användare: vi föreslår att du kontrollerar online-användare regelbundet för att se om enheten är inloggad utan tillstånd.
    - Kontrollera enhetsloggen: Att läsa loggarna ger information om IP-adresserna som användes för att logga in på dina enheter och deras nyckelfunktioner.
12. **Nätverkslogg**
    På grund av enhetens begränsade lagringskapacitet är den lagrade loggen begränsad. Om du behöver spara loggen under en längre tidsperiod rekommenderas att du aktiverar funktionen nätverkslogg för att garantera att de kritiska loggarna synkroniseras med nätverkets loggserver för spårning.
13. **Skapa en säker nätverksmiljö**
    För att bättre säkerställa enhetens säkerhet och reducera potentiella cyberrisker rekommenderar vi:
    - Inaktivera funktionen portmappning på routern för att undvika extern direktåtkomst till enheterna i det interna nätverket.

- Nätverket bör vara uppdelat och isolerat enligt de faktiska nätverksbehoven. Om det inte finns några kommunikationskrav mellan två undernätverk rekommenderas att VLAN, nätverks-GAP och andra tekniker används för att partitionera nätverket. Detta skapar en isolering av nätverket.
- Etablera system med 802.1x-åtkomstautentisering för att reducera risken för obehörig åtkomst till privata nätverk.
- Aktivera funktionen IP/MAC-adressfiltrering för att begränsa antalet värdar som får åtkomst till enheten.

Mer information

Besök Dahuas officiella webbplats med vår säkerhetscentral för nödsituationer som erbjuder säkerhetsmeddelanden och de senaste säkerhetsrekommendationerna.

MÖJLIGGÖR ETT SÄKERT SAMHÄLLE OCH SMARTARE LIVSSTANDARD

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.
Adress: No.1199 Bin'an Road, Binjiang District, Hangzhou, P. R. Kina | Webbplats: www.dahuasecurity.com | Postnummer: 310053
E-post: overseas@dahuatech.com | Fax: +86-571-87688815 | Tel: +86-571-87688883