Camera de rețea

Manual de utilizare

Inițiative privind utilizarea produselor video

Vă mulțumim că ați ales produsele Hikvision.

Tehnologia afectează fiecare aspect al vieții noastre. În calitate de companie de înaltă tehnologie, suntem din ce în ce mai conștienți de rolul pe care îl joacă tehnologia în îmbunătățirea eficienței afacerii și a calității vieții, dar, în același timp, de potențialul prejudiciu al utilizării necorespunzătoare. De exemplu, produsele video sunt capabile să înregistreze imagini reale, complete și clare. Acest lucru oferă o valoare ridicată retrospectiv și păstrând faptele în timp real. Cu toate acestea, poate duce, de asemenea, la încălcarea drepturilor și intereselor legitime ale unei terțe părți dacă are loc distribuirea, utilizarea și/sau prelucrarea necorespunzătoare a datelor video. Cu filozofia „Tehnologie pentru bine", Hikvision solicită ca fiecare utilizator final al tehnologiei video și al produselor video să respecte toate legile și reglementările aplicabile, precum și obiceiurile etice, cu scopul de a crea împreună o comunitate mai bună.

Vă rugăm să citiți cu atenție următoarele inițiative:

- Toată lumea are o așteptare rezonabilă de confidențialitate, iar instalarea produselor video nu ar trebui să intre în conflict cu această așteptare rezonabilă. Prin urmare, la instalarea produselor video în zone publice, se va da o notificare de avertizare într-o manieră rezonabilă și eficientă și va clarifica domeniul de monitorizare. Pentru zonele non-publice, drepturile și interesele unei terțe părți vor fi evaluate atunci când se instalează produse video, inclusiv, dar fără a se limita la, instalarea de produse video numai după obținerea consimțământului părților interesate și nu instalarea de produse video extrem de invizibile.

- Scopul produselor video este de a înregistra activități reale într-un anumit timp și spațiu și în condiții specifice. Prin urmare, fiecare utilizator trebuie să-și definească în mod rezonabil propriile drepturi într-un astfel de domeniu specific, pentru a evita încălcarea portretelor, a vieții private sau a altor drepturi legitime ale unei terțe părți.
- În timpul utilizării produselor video, datele de imagine video derivate din scene reale vor continua să fie generate, inclusiv o cantitate mare de date biologice (cum ar fi imaginile faciale), iar datele ar putea fi aplicate sau reprocesate în continuare. Produsele video în sine nu au putut distinge binele de rău în ceea ce privește modul de utilizare a datelor bazate exclusiv pe imaginile capturate de produsele video. Rezultatul utilizării datelor depinde de metoda și scopul utilizării operatorilor de date. Prin urmare, operatorii de date nu numai că trebuie să respecte toate legile și reglementările aplicabile și alte cerințe normative, ci și normele internaționale, morala socială, bunele moravuri, practicile obișnuite și alte cerințe neobligatorii și să respecte viața privată individuală, portretul și alte drepturi. si interese.

- Drepturile, valorile și alte cerințe ale diferitelor părți interesate ar trebui să fie întotdeauna luate în considerare atunci când se prelucrează date video care sunt generate continuu de produsele video. În acest sens, securitatea produsului și securitatea datelor sunt extrem de cruciale. Prin urmare, fiecare utilizator final și controlor de date trebuie să ia toate măsurile rezonabile și necesare pentru a asigura securitatea datelor și pentru a evita scurgerea datelor, dezvăluirea necorespunzătoare și utilizarea necorespunzătoare, inclusiv, dar fără a se limita la, configurarea accesului.

control, selectând un mediu de rețea adecvat (Internet sau Intranet) unde sunt conectate produsele video, stabilirea și optimizarea constantă a securității rețelei.

- Produsele video au adus o contribuție deosebită la îmbunătățirea securității sociale în întreaga lume și credem că aceste produse vor juca, de asemenea, un rol activ în mai multe aspecte ale vieții sociale. Orice abuz de produse video cu încălcarea drepturilor omului sau care duce la activități criminale este contrar intenției inițiale de inovare tehnologică și dezvoltare de produse. Prin urmare, fiecare utilizator trebuie să stabilească un mecanism de evaluare și urmărire a aplicației produsului pentru a se asigura că fiecare produs este utilizat într-o manieră adecvată și rezonabilă și cu bună-credință.

Informații legale

Despre acest manual

Manualul include instrucțiuni pentru utilizarea și gestionarea produsului. Imaginile, diagramele, imaginile și toate celelalte informații de mai jos sunt doar pentru descriere și explicație. Informațiile conținute în Manual pot fi modificate, fără notificare, din cauza actualizărilor de firmware sau din alte motive. Vă rugăm să găsiți cea mai recentă versiune a acestui manual pe site-ul web Hikvision (***https:// www.hikvision.com/***).

Vă rugăm să utilizați acest manual cu îndrumarea și asistența profesioniștilor instruiți în sprijinirea Produsului.

Mărci comerciale

HIKVISION și alte mărci comerciale și logo-uri Hikvision sunt proprietatea Hikvision în diferite jurisdicții.
Alte mărci comerciale și logo-uri menționate sunt proprietățile deținătorilor respectivi.

Disclaimer

ÎN MĂSURA MAXIMĂ PERMISĂ DE LEGEA APLICABILĂ, ACEST MANUAL ȘI PRODUSUL DESCRIS, CU HARDWARE-UL, SOFTWARE-UL ȘI FIRMWARE-UL SUNT FURNIZATE „CA ATIE” ȘI „CU TOATE DEFECTELE ȘI ERORIILE”. HIKVISION NU OFERĂ GARANȚII, EXPRESE SAU IMPLICITE, INCLUSIV FĂRĂ LIMITĂRI, VANTABILITATE, CALITATE SATISFĂCĂTORĂ SAU ADECVENȚĂ PENTRU UN ANUMIT SCOP. UTILIZAREA PRODUSULUI DE CĂTRE DVS. ESTE PE PROPRIU RISC. HIKVISION NU VA FI RESPONSABIL ÎN NICIO CAZ PENTRU ORICE DAUNE SPECIALE, CONSECUȚIALE, INCIDENTALE SAU INDIRECTE, INCLUSIV, PRIN ALTE, DAUNE PENTRU PIERDEREA PROFITURILOR AFACERII, ÎNTRERUPEREA AFACERII SAU PIERDEREA DATELOR, CORUPEREA SISTEMELOR SAU PIERDEREA DOCUMENTEI FĂCĂ PE BAZĂ DE ÎNCĂLCAREA CONTRACTULUI, DELICIT (INCLUSUL NEGLIGENȚEI), RĂSPUNDEREA PRODUSULUI SAU ALTELE, ÎN LEGAȚIE CU UTILIZAREA PRODUSULUI, CHIAR DACĂ HIKVISION A FOST Anunțat despre POSIBILITATEA ASTELOR DAUNE SAU PIERDERI.
RECUNOSCĂȚI CĂ NATURA INTERNETULUI PREVĂRĂ RISCURI INERENTE DE SECURITATE, ȘI HIKVISION NU ÎȘI VA ASUMA NICIO RESPONSABILITATE PENTRU FUNCȚIONARE ANORMALĂ, SCURTARE DE CONFIDENTIALITATE SAU ALTE DAUNE REZULTATE DIN ATAC CIBERNICE, ATAC DE HACKER, ALTĂ INFRACȚIE DE SECURITATE, VIRUS; CU toate acestea, HIKVISION VA FURNIZA SISTEMUL TEHNIC LA TEMPORUL DACĂ ESTE NECESAR.
SUNTEȚI DE ACORD SĂ UTILIZAȚI ACEST PRODUS ÎN CONFORMITATE CU TOATE LEGILE APLICABILE ȘI SUNTEȚI UNCUL RESPONSABIL PENTRU A ASIGURA CĂ UTILIZAREA DVS. CONFORM LEGEA APLICABĂ. În special, ești RESPONSABIL PENTRU UTILIZAREA ACESTUI PRODUS ÎN MANIERĂ CARE NU ÎNCĂLCĂ DREPTURILE TERȚILOR, INCLUSIV FĂRĂ LIMITARE, DREPTURILE DE PUBLICITATE, DREPTURILE DE PROPRIETATE INTELECTUALĂ SAU PROTECȚIA DATELOR ȘI ALTE DREPTURI ȘI ALTE DREPTURI. NU UTILIZAȚI ACEST PRODUS PENTRU UTILIZĂRI FINALE INTERZISE, INCLUSIV

DEZVOLTAREA SAU PRODUCȚIA ARMELOR DE DISTRUCȚIE ÎN MASĂ, DEZVOLTAREA SAU PRODUCȚIA DE ARME CHIMICE SAU BIOLOGICE, ORICE ACTIVITĂȚI ÎN CONTEXT LEGATE DE ORICE EXPLOZIV NUCLEAR SAU PERICOL CICLU DE COMBUSTIBIL NUCLEAR, SAU ÎN SUPORTUL UMANILOR.
ÎN CAZUL ORICE CONFLICTE ÎNTRE ACEST MANUAL ȘI LEGEA APLICABILĂ, CEEA DIN URME PREVALEAZA.

Convenții de simbol

Simbolurile care pot fi găsite în acest document sunt definite după cum urmează.

Simbol	Descriere
Pericol	Indică o situație periculoasă care, dacă nu este evitată, va sau ar putea duce la moarte sau vătămări grave.
Prudență	Indică o situație potențial periculoasă care, dacă nu este evitată, ar putea duce la deteriorarea echipamentului, pierderea datelor, degradarea performanței sau rezultate neașteptate.
Notă	Oferă informații suplimentare pentru a sublinia sau completa punctele importante ale textului principal.

Instrucțiuni de siguranță

Aceste instrucțiuni au scopul de a se asigura că utilizatorul poate folosi produsul corect pentru a evita pericolul sau pierderea proprietății.

Legi și reglementări

- Dispozitivul trebuie utilizat în conformitate cu legile locale, reglementările de siguranță electrică și reglementările de prevenire a incendiilor.

Electricitate

- În utilizarea produsului, trebuie să respectați strict reglementările de siguranță electrică ale națiunii și regiunii.
- Echipamentul nu trebuie expus la picurare sau stropire și nu trebuie plasate pe echipament obiecte umplute cu lichide, cum ar fi vaze.
- Asigurați un supresor de supratensiune la deschiderea de admisie a echipamentului în condiții speciale, cum ar fi vârful muntelui, turnul de fier și pădure.
- ATENȚIE: Pentru a reduce riscul de incendiu, înlocuiți numai cu siguranță de același tip și de același tip.
- Echipamentul trebuie conectat la o priză cu împământare.
- Un dispozitiv de deconectare adecvat, ușor accesibil, trebuie încorporat în exteriorul echipamentului.
- Un dispozitiv adecvat de protecție împotriva supracurentului trebuie încorporat în exteriorul echipamentului, care să nu depășească specificațiile clădirii.
- În instalația electrică a clădirii va fi încorporat un întrerupător de rețea pe toți polii.
- Asigurați-vă cablarea corectă a bornelor pentru conectarea la o sursă de alimentare de curent alternativ.
- Echipamentul a fost proiectat, atunci când este necesar, modificat pentru conectarea la un sistem IT de distribuție a energiei.

Baterie

- Nu ingerati bateria. Pericol de arsuri chimice!
- Acest produs conține o baterie tip monedă/buton. Dacă bateria monedă/buton este înghițită, poate provoca arsuri interne severe în doar 2 ore și poate duce la moarte.
- Păstrați bateriile noi și uzate departe de copii.
- Dacă compartimentul bateriei nu se închide bine, nu mai utilizați produsul și țineți-l departe de copii.
- Dacă credeți că bateriile ar fi putut fi înghițite sau plasate în orice parte a corpului, solicitați imediat asistență medicală.
- ATENȚIE: Risc de explozie dacă bateria este înlocuită cu una de tip incorect. Aruncați bateriile uzate conform instrucțiunilor.
- ATENTIE: IL YA RISQUE D'EXPLOSION SI LA BATTERIE EST REMPLACÉE PAR UNE BATTERIE DE TYPE INCORRECT. METTRE AU REBUT LES BATTERIES USAGEES CONFORMÉMENT AUX INSTRUCTIONS.

- Înlocuirea necorespunzătoare a bateriei cu un tip incorect poate înlătura o protecție (de exemplu, în cazul unor tipuri de baterii cu litiu).
- Nu aruncați bateria în foc sau într-un cuptor încins și nu zdrobiți sau tăiați mecanic bateria, ceea ce poate duce la o explozie.
- Nu lăsați bateria într-un mediu înconjurător cu temperatură extrem de ridicată, ceea ce poate duce la o explozie sau la scurgerea de lichid sau gaz inflamabil.
- Nu supuneți bateria la o presiune extrem de scăzută a aerului, ceea ce poate duce la o explozie sau la scurgerea de lichid sau gaz inflamabil.
- + identifică bornele pozitive ale echipamentului care este utilizat cu sau generează curent continuu.
  - identifică bornele negative ale echipamentului care este utilizat cu sau generează curent continuu.

De prevenire a incendiilor

- Pe echipament nu trebuie amplasate surse de flacără liberă, cum ar fi lumânările aprinse.
- Portul serial al echipamentului este folosit doar pentru depanare.

Prevenirea suprafețelor fierbinți

- 

ATENȚIE: Piese fierbinți! Degete arse la manipularea pieselor. Așteptați o jumătate de oră după oprire înainte de manipularea pieselor. Acest autocolant indică faptul că elementul marcat poate fi fierbinte și nu trebuie atins fără grijă. Pentru dispozitivul cu acest autocolant, acest dispozitiv este destinat instalării într-o locație cu acces restricționat, accesul poate fi obținut numai de către persoanele de service sau de către utilizatorii care au fost instruiți despre motivele restricțiilor aplicate locației și despre orice precauții care trebuie să fie Luat.

Instalare

- Instalați echipamentul conform instrucțiunilor din acest manual.
- Pentru a preveni rănirea, acest echipament trebuie să fie atașat ferm de podea/perete în conformitate cu instrucțiunile de instalare.
- Nu așezați niciodată echipamentul într-un loc instabil. Echipamentul poate cădea, provocând vătămări corporale grave sau deces.

Alimentare electrică

- Tensiunea de intrare trebuie să fie în conformitate cu standardul IEC60950-1: SELV (Tensiune foarte joasă de siguranță) și sursa de alimentare limitată. Consultați documentația corespunzătoare pentru informații detaliate.
- Sursa de alimentare trebuie să îndeplinească cerințele sursei de alimentare limitate sau PS2 conform standardului IEC 60950-1 sau IEC 62368-1.
- NU conectați mai multe dispozitive la un singur adaptor de alimentare, pentru a evita supraîncălzirea sau pericolele de incendiu cauzate de suprasarcină.
- Asigurați-vă că ștecherul este conectat corect la priza de alimentare.

Iluminator cu lumină albă (dacă este acceptat)

- Radiații optice posibil periculoase emise de acest produs.
- NU priviți la sursa de lumină care funcționează. Poate fi dăunător pentru ochi.
- Purtați protecție adecvată pentru ochi sau NU aprindeți lumina albă când asamblați, instalați sau întrețineți camera.

Transport

- Păstrați dispozitivul în ambalajul original sau similar în timpul transportului.

Securitatea sistemului

- Instalatorul și utilizatorul sunt responsabili pentru configurarea parolei și a securității.

întreținere

- Dacă produsul nu funcționează corect, vă rugăm să contactați dealerul sau cel mai apropiat centru de service.
- Nu ne asumăm nicio responsabilitate pentru problemele cauzate de reparații sau întreținere neautorizate.
- Câteva componente ale dispozitivului (de exemplu, condensatorul electrolitic) necesită înlocuire regulată. Durata medie de viață variază, așa că se recomandă verificarea periodică. Contactați dealerul dumneavoastră pentru detalii.

Curatenie

- Vă rugăm să utilizați o cârpă moale și uscată când curățați suprafețele interioare și exterioare ale capacului produsului. Nu utilizați detergenți alcalini.

Utilizarea Mediului

- Atunci când este utilizat orice echipament laser, asigurați-vă că lentila dispozitivului nu este expusă la raza laser, altfel se poate arde.
- NU expuneți dispozitivul la radiații electromagnetice ridicate sau la medii cu praf.
- Pentru dispozitivul de interior, plasați-l într-un mediu uscat și bine ventilat.
- NU îndreptați obiectivul spre soare sau spre orice altă lumină puternică.
- Asigurați-vă că mediul de rulare îndeplinește cerințele dispozitivului. Temperatura de funcționare trebuie să fie de la -30 °C la 60 °C (de la -22 °F la 140 °F), iar umiditatea de funcționare trebuie să fie de 95% sau mai puțin (fără condensare).
- NU așezați camera în locuri extrem de calde, reci, cu praf sau umede și nu o expuneți la radiații electromagnetice puternice.

De urgență

- Dacă de la dispozitiv apar fum, miros sau zgomot, opriți imediat alimentarea, deconectați cablul de alimentare și contactați centrul de service.

Sincronizarea timpului

- Configurați manual ora dispozitivului pentru primul acces dacă ora locală nu este sincronizată cu cea a rețelei. Vizitați dispozitivul prin intermediul software-ului de navigare web/client și accesați interfața de setări de timp.

Reflecţie

- Asigurați-vă că nicio suprafață reflectorizantă nu este prea aproape de lentila dispozitivului. Lumina IR de la dispozitiv se poate reflecta înapoi în obiectiv cauzând reflexie.

Cuprins

Capitolul 1 Activarea și accesarea dispozitivului

Pentru a proteja securitatea și confidențialitatea contului de utilizator și a datelor, ar trebui să setați o parolă de conectare pentru a activa dispozitivul atunci când accesați dispozitivul prin rețea.

Notă

Consultați manualul de utilizare al clientului software pentru informații detaliate despre activarea software-ului client.

1.1 Activați dispozitivul

Dispozitivul trebuie activat prin setarea unei parole puternice înainte de utilizare. Această parte introduce activarea folosind diferite instrumente client.

1.1.1 Activați prin SADP

SADP este un instrument pentru detectarea, activarea și modificarea adresei IP a dispozitivului prin LAN.

Inainte sa incepi

- Obțineți software-ul SADP de pe discul furnizat sau de pe site-ul web oficial ***http:// www.hikvision.com/*** ,și instalați SADP conform instrucțiunilor.
- Dispozitivul și computerul care rulează instrumentul SADP ar trebui să aparțină aceleiași subrețele.

Următorii pași arată cum să activați un dispozitiv și să modificați adresa IP a acestuia. Pentru activarea lotului și modificarea adresei IP, consultați*Manual de utilizare al SADP*pentru detalii.

Pași

1.Rulați software-ul SADP și căutați dispozitivele online.

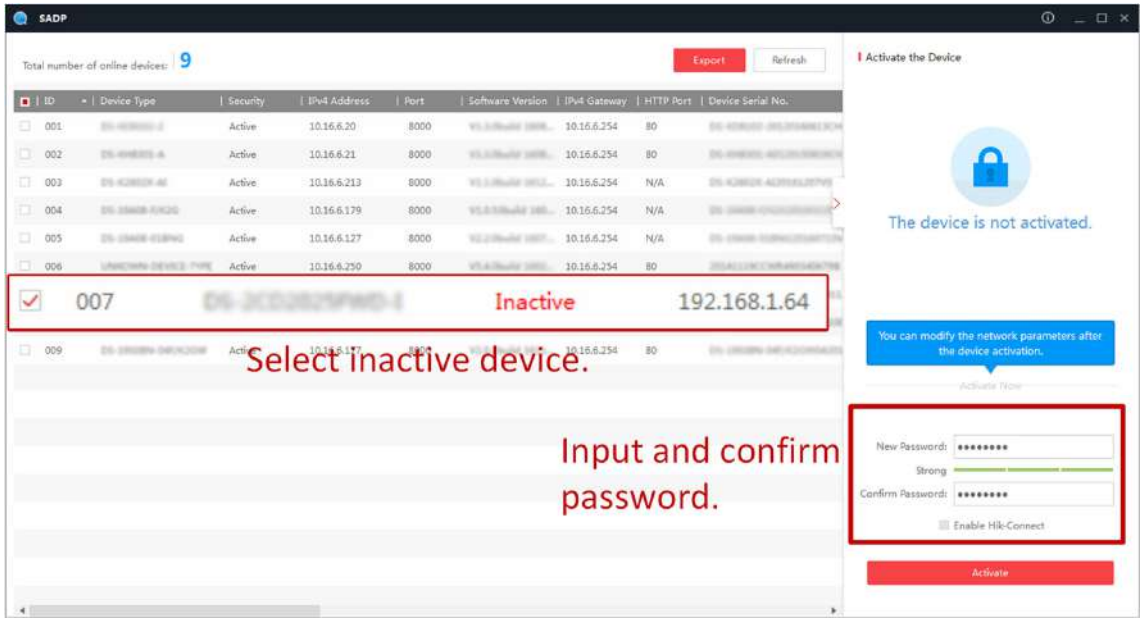
2.Găsiți și selectați dispozitivul dvs. în lista de dispozitive online.

3.Introduceți o nouă parolă (parolă de administrator) și confirmați parola.

Prudență

RECOMANDĂ PAROLĂ SURBA-Vă recomandăm să creați o parolă puternică, la alegerea dvs. (folosind minim 8 caractere, inclusiv litere mari, litere mici, cifre și caractere speciale) pentru a crește securitatea produsului dumneavoastră. Și vă recomandăm să vă resetați parola în mod regulat, mai ales în sistemul de înaltă securitate, resetarea parolei lunar sau săptămânal vă poate proteja mai bine produsul.

4.Clic**Activati**pentru a începe activarea.



Starea dispozitivului devine**Activ**după activarea cu succes.

5.Modificați adresa IP a dispozitivului.

1) Selectați dispozitivul.

2) Schimbați adresa IP a dispozitivului la aceeași subrețea ca și computerul dvs. fie modificând adresa IP manual, fie verificând**Activați DHCP**.

3) Introduceți parola de administrator și faceți clic**Modifica**pentru a activa modificarea adresei IP.

1.1.2 Activați camera prin iVMS-4200

iVMS-4200 este un client PC pentru a gestiona și opera dispozitivele dumneavoastră. Activarea camerei este acceptată de software.

Inainte sa incepi

- Obțineți software-ul client de pe discul furnizat sau de pe site-ul web oficial***http://www.hikvision.com/en/*** .Instalați software-ul urmând instrucțiunile.
- Camera și PC-ul care rulează software-ul ar trebui să fie în aceeași subrețea.

Pași

1.Rulați software-ul client.

2.introduce**Managementul dispozitivelor**sau**Dispozitiv online**.

3.Verificați starea dispozitivului din lista de dispozitive și selectați o cameră inactivă.

4.Apasă pe**Activati**.

5.Creați și confirmați parola de administrator a camerei.

Prudență

RECOMANDĂ PAROLĂ SURBA-Vă recomandăm să creați o parolă puternică, la alegerea dvs. (folosind minim 8 caractere, inclusiv litere mari, litere mici, cifre și caractere speciale) pentru a crește securitatea produsului dumneavoastră. Și vă recomandăm să vă resetați parola în mod regulat, mai ales în sistemul de înaltă securitate, resetarea parolei lunar sau săptămânal vă poate proteja mai bine produsul.

6.Clic**Bine**pentru a începe activarea.

Starea dispozitivului se schimbă în**Activ**după activarea cu succes.

7.Modificați adresa IP a dispozitivului.

1) Selectați dispozitivul și faceți clic**Modificați Netinfo**la**Dispozitiv online**.

2) Schimbați adresa IP a dispozitivului la aceeași subrețea cu computerul dvs. fie modificând adresa IP manual, fie verificând**DHCP**.

3) Introduceți parola de administrator a dispozitivului și faceți clic**Bine**pentru a finaliza modificarea.

1.1.3 Activați dispozitivul prin browser web

Utilizați browserul web pentru a activa dispozitivul. Pentru dispozitivul cu DHCP activat în mod implicit, utilizați software-ul SADP sau clientul PC pentru a activa dispozitivul.

Inainte sa incepi

Asigurați-vă că dispozitivul și computerul dvs. se conectează la aceeași rețea LAN.

Pași

1.Schimbați adresa IP a computerului dvs. la aceeași subrețea ca și dispozitivul.

Adresa IP implicită a dispozitivului este 192.168.1.64.

2.Deschideți un browser web și introduceți adresa IP implicită.

3.Creați și confirmați parola de administrator.

Prudență

RECOMANDĂ PAROLĂ SURBA-Vă recomandăm să creați o parolă puternică, la alegerea dvs. (folosind minim 8 caractere, inclusiv litere mari, litere mici, cifre și caractere speciale) pentru a crește securitatea produsului dumneavoastră. Și vă recomandăm să vă resetați parola în mod regulat, mai ales în sistemul de înaltă securitate, resetarea parolei lunar sau săptămânal vă poate proteja mai bine produsul.

4.Clic**Bine**pentru a finaliza activarea și pentru a intra**Vizualizare live**pagină.

5.Modificați adresa IP a camerei.

1) Accesați pagina de modificare a adresei IP.**Configurare → Rețea → TCP/IP**

2) Schimbați adresa IP.

3) Salvați setările.

1.2 Acces Camera

Această parte prezintă modul de accesare a camerei prin browser web sau software client.

1.2.1 Accesați camera prin browser web

Inainte sa incepi

Verificați cerințele de sistem pentru a confirma că computerul de operare și browserul web îndeplinesc cerințele.

Tabelul 1-1 Cerințe de sistem

Sistem de operare	Microsoft Windows XP și versiunea superioară, Mac OS X 10.8 și versiunea superioară
CPU	3,0 GHz sau mai mare
RAM	1 GB sau mai mare
Afişa	Rezoluție 1024 × 768 sau mai mare
Browser web	Internet Explorer 8.0 și versiunea superioară, Mozilla Firefox 30.0-51, Google Chrome 31.0-44, Safari 8.0+

Pași

1.Deschideți browserul web.

Notă

Pentru unele browsere web, este necesar un plug-in. Pentru cerințe detaliate, vezi***Instalare plug-in*** .

2.Introdu adresa IP a camerei pentru a intra în interfața de conectare.

3.Introduceți numele de utilizator și parola.

Notă

Blocarea de conectare ilegală este activată implicit. Dacă utilizatorul admin efectuează șapte încercări eșuate de parolă (cinci încercări pentru utilizator/operator), adresa IP este blocată timp de 30 de minute.

Dacă blocarea ilegală de conectare nu este necesară, accesați**Configurare → Sistem → Securitate → Serviciu de securitate** pentru a-l opri.

4.Clic**Log in**.

5.Descărcați și instalați pluginul corespunzător pentru browserul dvs. web.

Pentru browser web bazat pe IE, componente web și™sunt optionale. Pentru browser web non-IE, componente web,™, VLC și MJEPG sunt opționale.

Ce e de facut in continuare

- Puteți recupera parola de administrator. Pentru setări detaliate, vezi***Recuperarea parolei de administrator*** .
- Puteți seta blocarea de conectare ilegală pentru a îmbunătăți securitatea. Pentru setări detaliate, vezi***Blocare ilegală de conectare*** .

Instalare plug-in

Anumite sisteme de operare și browser web pot restricționa afișarea și funcționarea funcției camerei. Ar trebui să instalați plug-in-ul sau să finalizați anumite setări pentru a asigura afișarea și funcționarea normale. Pentru funcția restricționată detaliată, consultați dispozitivul real.

Sistem de operare	Browser web	Operațiune
Windows	• Internet Explorer 8+ • Google Chrome 57 și versiunea anterioară • Mozilla Firefox 52 și versiunea anterioară	Urmați instrucțiunile pop-up pentru a finaliza instalarea plug-in-ului.
	• Google Chrome 57+ • Mozilla Firefox 52+	Clic Download Plug-in la descărcați și instalați pluginul.
Mac OS	• Google Chrome 57+ • Mozilla Firefox 52+ • Mac Safari 16+	Instalarea plug-in nu este necesară. Mergi la**Configurare → Rețea → Setări avansate → Serviciu de rețea**pentru a activa WebSocket sau Websockets pentru vizualizarea normală. Afișarea și operarea anumitor funcții sunt restricționate. De exemplu, Redare și Imagine nu sunt disponibile. Pentru detalii funcție restricționată, referiți-vă la dispozitivul real.

Notă

Camera acceptă numai sistemele Windows și Mac OS și nu acceptă sistemul Linux.

Recuperarea parolei de administrator

Dacă uitați parola de administrator, puteți reseta parola făcând clic**Parola uitata**pe pagina de conectare după finalizarea setărilor de securitate a contului.

Puteți reseta parola setând întrebarea de securitate sau e-mailul.

Notă

Când trebuie să resetați parola, asigurați-vă că dispozitivul și computerul sunt pe același segment de rețea.

Întrebare de securitate

Puteți seta securitatea contului în timpul activării. Sau poți merge la**Configurare → Sistem → Gestionare utilizatori**,clic**Setări de securitate a contului**, selectați întrebarea de securitate și introduceți răspunsul.

Puteți da clic**Parola uitata**și răspundeți la întrebarea de securitate pentru a reseta parola de administrator când accesați dispozitivul prin browser.

E-mail

Puteți seta securitatea contului în timpul activării. Sau poți merge la**Configurare → Sistem → Gestionare utilizatori**,clic**Setări de securitate a contului**, introduceți adresa dvs. de e-mail pentru a primi codul de verificare în timpul procesului de operare de recuperare.

Blocare ilegală de conectare

Ajută la îmbunătățirea securității atunci când accesați dispozitivul prin Internet.

Mergi la**Configurare → Sistem → Securitate → Serviciu de securitate**,și activați**Activați blocarea autentificărilor ilegale**.**Încercări ilegale de conectare**și**Durata de blocare**sunt configurabile.

Încercări ilegale de conectare

Când încercările dvs. de conectare cu parola greșită ating orele setate, dispozitivul este blocat. **Durata de blocare**

Dispozitivul eliberează blocarea după durata setării.

1.2.2 Accesați camera prin iVMS-4200

Adăugați camera la software-ul client înainte de operare ulterioară.

Consultați*Manual de utilizare software client iVMS-4200*pentru pași de setare detaliați.

1.2.3 Accesați camera prin Hik-Connect

Hik-Connect este o aplicație pentru dispozitive mobile. Folosind aplicația, puteți vizualiza imagini live, primi notificări de alarmă și așa mai departe.

Inainte sa incepi

Conectați camera la rețea cu cabluri de rețea.

Pași

1.Obțineți și instalați aplicația Hik-Connect prin următoarele moduri.

- Vizita***https://appstore.hikvision.com*** pentru a descărca aplicația conform sistemului dvs. de telefonie mobilă.
- Vizitați site-ul oficial al companiei noastre. Apoi du-te la**Asistență → Instrumente → Magazin de aplicații Hikvision**.
- Scanați codul QR de mai jos pentru a descărca aplicația.

Notă

Dacă în timpul instalării apar erori precum „Aplicație necunoscută”, rezolvați problema în două moduri.

- Vizita***https://appstore.hikvision.com/static/help/index.html*** pentru a face referire la depanare.
- Vizita***https://appstore.hikvision.com/*** ,și faceți clic**Ajutor pentru instalare**în colțul din dreapta sus al interfeței pentru a face referire la depanare.

2.Porniți aplicația și înregistrați-vă pentru un cont de utilizator Hik-Connect.

3.Conectați-vă după înregistrare.

4.În aplicație, atingeți „+” în colțul din dreapta sus și apoi scanați codul QR al camerei pentru a adăuga camera. Codul QR îl găsiți pe cameră sau pe coperta Ghidului de pornire rapidă al camerei din pachet.

5.Urmați instrucțiunile pentru a seta conexiunea la rețea și adăugați camera la contul dvs. Hik-Connect.

Pentru informații detaliate, consultați manualul de utilizare al aplicației Hik-Connect.

Activați serviciul Hik-Connect pe cameră

Serviciul Hik-Connect ar trebui să fie activat pe camera dvs. înainte de a utiliza serviciul.

Puteți activa serviciul prin software-ul SADP sau browser web.

Activați serviciul Hik-Connect prin browser web

Urmați următorii pași pentru a activa serviciul Hik-Connect prin browser web.

Inainte sa incepi

Trebuie să activați camera înainte de a activa serviciul.

Pași

1.Accesați camera prin browser web.

2.Accesați interfața de configurare a accesului la platformă.**Configurare → Rețea → Setări avansate → Acces platformă**

3.Selectați Hik-Connect ca**Modul de acces la platformă**.

4.Verifica**Permite**.

5.Faceți clic și citiți „Termeni și condiții” și „Politica de confidențialitate” în fereastra pop-up.

6.Creați un cod de verificare sau modificați vechiul cod de verificare pentru cameră.

Notă

Codul de verificare este necesar când adăugați camera la serviciul Hik-Connect.

7.Salvați setările.

Activați serviciul Hik-Connect prin software-ul SADP

Această parte prezintă cum să activați serviciul Hik-Connect prin intermediul software-ului SADP al unei camere activate.

Pași

1.Rulați software-ul SADP.

2.Selectați o cameră și intrați**Modificați parametrii rețelei**pagină.

3.Verifica**Activați Hik-Connect**.

4.Creați un cod de verificare sau modificați vechiul cod de verificare.

Notă

Codul de verificare este necesar când adăugați camera la serviciul Hik-Connect.

5.Faceți clic și citiți „Termeni și condiții” și „Politica de confidențialitate”.

6.Confirmați setările.

Configurați Hik-Connect

Pași

1.Obțineți și instalați aplicația Hik-Connect prin următoarele moduri.

- Vizita***https://appstore.hikvision.com*** pentru a descărca aplicația conform sistemului dvs. de telefonie mobilă.
- Vizitați site-ul oficial al companiei noastre. Apoi du-te la**Asistență → Instrumente → Magazin de aplicații Hikvision**.
- Scanați codul QR de mai jos pentru a descărca aplicația.

Notă

Dacă în timpul instalării apar erori precum „Aplicație necunoscută”, rezolvați problema în două moduri.

- Vizita***https://appstore.hikvision.com/static/help/index.html*** pentru a face referire la depanare.
- Vizita***https://appstore.hikvision.com/*** ,și faceți clic**Ajutor pentru instalare**în colțul din dreapta sus al interfeței pentru a face referire la depanare.

2.Porniți aplicația și înregistrați-vă pentru un cont de utilizator Hik-Connect.

3.Conectați-vă după înregistrare.

Adăugați o cameră la Hik-Connect

Pași

1.Conectați-vă dispozitivul mobil la o rețea Wi-Fi.

2.Conectați-vă la aplicația Hik-Connect.

3.În pagina de pornire, atingeți „+” în colțul din dreapta sus pentru a adăuga o cameră.

4.Scanați codul QR pe corpul camerei sau pe*Ghid de inițiere rapidă*acoperi.

Notă

Dacă codul QR lipsește sau este prea neclar pentru a fi recunoscut, puteți adăuga și camera prin introducerea numărului de serie al camerei.

5.Introduceți codul de verificare al camerei dvs.

Notă

- Codul de verificare necesar este codul pe care îl creați sau îl modificați atunci când activați serviciul Hik-Connect pe cameră.
- Dacă uitați codul de verificare, puteți verifica codul de verificare curent**Acces la platformă** pagina de configurare prin browser web.

6.Atingeți**Conectați-vă la o rețea**butonul din interfața pop-up.

7.Alege**Conexiune prin cablu**sau**Conexiune fără fir**în funcție de funcția dvs. de cameră.

Fără fir Conexiune	Introduceți parola Wi-Fi la care s-a conectat telefonul mobil și atingeți **Următorul**pentru a începe procesul de conectare Wi-Fi. (Găsiți camera la 3 metri de router atunci când configurați Wi-Fi.)
Cablat Conexiune	Conectați camera la router cu un cablu de rețea și atingeți**Conectat** în interfața de rezultate.

Notă

Routerul ar trebui să fie același la care s-a conectat telefonul mobil.

8.Atingeți**Adăuga**în următoarea interfață pentru a termina adăugarea.

Pentru informații detaliate, consultați manualul de utilizare al aplicației Hik-Connect.

Inițializați cardul de memorie prin Hik-Connect

Cardul de memorie necesită inițializare înainte de a salva înregistrările și imaginile camerei.

Pași

1.Verificați starea cardului de memorie atingând pe**Starea stocării**în interfața de setări a dispozitivului.

2.Dacă starea cardului de memorie se afișează ca Neinițializat, atingeți pentru a o inițializa.

Starea se va schimba în Normal după inițializarea cu succes.

Rezultat

Puteți începe apoi înregistrarea oricărui eveniment video declanșat în cameră, cum ar fi detectarea mișcării.

Capitolul 2 Configurarea camerei de rețea

2.1 Actualizare firmware

Pentru o experiență mai bună a utilizatorului, vă recomandăm să vă actualizați dispozitivul la cel mai recent firmware cât mai curând posibil.

Vă rugăm să obțineți cel mai recent pachet de firmware de pe site-ul oficial sau de la expertul tehnic local. Pentru mai multe informații, vă rugăm să vizitați site-ul oficial:***https://www.hikvision.com/en/support/download/firmware/*** .

Pentru setările de actualizare, consultați***Actualizare*** .

2.2 Cerințe de sistem

Computerul dvs. trebuie să îndeplinească cerințele pentru vizitarea și operarea corectă a produsului.

Sistem de operare	Microsoft Windows XP SP1 și versiunea superioară de 2,0
CPU	GHz sau mai mare
RAM	1G sau mai mare
Afişa	Rezoluție 1024×768 sau mai mare
Browser web	Pentru detalii, vezi***Instalare plug-in***

2.3 Vizualizare live

Introduce parametrii de vizualizare live, pictogramele funcțiilor și setările parametrilor de transmisie.

2.3.1 Parametrii Live View

Funcțiile acceptate variază în funcție de model.

Activați și dezactivați vizualizarea live

Această funcție este utilizată pentru a activa sau dezactiva rapid vizualizarea în direct a canalului.

- Clic ▶ pentru a începe vizualizarea live.
- Clic ■ pentru a opri vizualizarea live.

Ajustați raportul de aspect

Pași

1.Clic**Vizualizare live**.

2.Clic  pentru a selecta raportul de aspect.

-  se referă la dimensiunea ferestrei 4:3.
-  se referă la dimensiunea ferestrei 16:9.
-  se referă la dimensiunea originală a ferestrei.
-  se referă la dimensiunea ferestrei auto-adaptabile.
-  se referă la dimensiunea originală a ferestrei raportului.

Tip de flux Live View

Selectați tipul de flux de vizualizare live în funcție de nevoile dvs. Pentru informații detaliate despre selecția tipului de flux, consultați ***Tipul fluxului*** .

Selectați plug-in-ul terță parte

Când vizualizarea live nu poate fi afișată prin anumite browsere, puteți modifica pluginul pentru vizualizarea live în funcție de browser.

Pași

1.Clic**Vizualizare live**.

2.Faceți clic  pentru a selecta plug-in-ul.

- Când accesați dispozitivul prin Internet Explorer, puteți selecta Webcomponents sau QuickTime.
- Când accesați dispozitivul prin alte browsere, puteți selecta Webcomponents, QuickTime, VLC sau MJPEG.

Divizia ferestre

-  se referă la împărțirea ferestrei 1 × 1.
-  se referă la împărțirea ferestrei 2 × 2. se
-  referă la împărțirea ferestrelor 3 × 3.
-  se referă la împărțirea ferestrelor 4 × 4.

Ușoară

Clic  pentru a porni sau opri iluminatorul.

Numără pixeli

Ajută la obținerea pixelului de înălțime și lățime a regiunii selectate în imaginea de vizualizare live.

Pași

1.Faceți clic pentru a activa funcția.

2.Trageți mouse-ul pe imagine pentru a selecta zona dreptunghiulară dorită.

Pixelul de lățime și pixelul de înălțime sunt afișate în partea de jos a imaginii de vizualizare live.

Porniți Zoom digital

Vă ajută să vedeți informații detaliate despre orice regiune din imagine.

Pași

1.Faceți clic pentru a activa zoom-ul digital.

2.În imaginea de vizualizare live, trageți mouse-ul pentru a selecta regiunea dorită.

3.Faceți clic pe imaginea de vizualizare live pentru a reveni la imaginea originală.

Focalizare auxiliară

Este folosit pentru dispozitive motorizate. Poate îmbunătăți imaginea dacă dispozitivul nu poate focaliza clar.

Pentru dispozitivul care acceptă ABF, ajustați unghiul obiectivului, apoi focalizați și faceți clic pe butonul ABF de pe dispozitiv. Dispozitivul poate focaliza clar.

Faceți clic pentru a focaliza automat.

Notă

- Dacă dispozitivul nu poate focaliza cu focalizare auxiliară, puteți utiliza ***Inițializarea lentilelor*** ,apoi utilizați din nou focalizarea auxiliară pentru a clarifica imaginea.
- Dacă focalizarea auxiliară nu poate ajuta dispozitivul să se concentreze clar, puteți utiliza focalizarea manuală.

Inițializarea lentilelor

Inițializarea obiectivului este utilizată pe dispozitivul echipat cu lentilă motorizată. Funcția poate reseta obiectivul atunci când zoomul sau focalizarea de lungă durată au ca rezultat o imagine încețoșată. Această funcție variază în funcție de diferite modele.

Inițializare manuală a obiectivului

Faceți clic pentru a opera inițializarea obiectivului.

Inițializare automată a obiectivului

Mergi la**Configurare → Sistem → Întreținere → Corecție lentile**pentru a activa această funcție. Puteți seta programul de armare, iar dispozitivul va corecta automat obiectivul în perioadele de timp configurate.

Setare rapidă Live View

Oferă o configurare rapidă a PTZ, setări de afișare, OSD, setări video/audio pe pagina de vizualizare live.

Pași

1.Faceți clic pentru a afișa pagina de configurare rapidă.

2.Setați PTZ, setările de afișare, OSD, parametrii video/audio.

- Pentru setările PTZ, consultați***Reglarea parametrilor obiectivului*** .
- Pentru setările de afișare, vezi***Setări de afișare*** .
- Pentru setările OSD, vezi***OSD*** .
- Pentru setările audio și video, consultați***Video și audio*** .

Notă

Funcția este acceptată doar de anumite modele.

Reglarea parametrilor obiectivului

Este folosit pentru a regla focalizarea obiectivului, zoomul și irisul.

Zoom

- Clic , iar obiectivul mărește.
- Clic , iar obiectivul micșorează.

Concentrează-te

- Clic , apoi obiectivul focalizează departe și obiectul îndepărtat devine clar.
- Clic , apoi obiectivul focalizează aproape și obiectul din apropiere devine clar.

Viteza PTZ

- Slide pentru a regla viteza mișcării pan/tilt.

Iris

- Când imaginea este prea întunecată, faceți clic pentru a mări irisul.
- Când imaginea este prea luminoasă, faceți clic pentru a opri irisul.

Blocare PTZ

Blocarea PTZ înseamnă dezactivarea funcțiilor de zoom, focalizare și rotație PTZ ale canalului corespunzător, astfel încât să reducă lipsa țintei cauzată de ajustarea PTZ.

Mergi la**Configurare → PTZ**,Verifica**Activați blocarea PTZ**, și faceți clic**Salvați**.

Efectuați poziționarea 3D

Poziționarea 3D este de a muta zona selectată în centrul imaginii.

Pași

1.Faceți clic pentru a activa funcția.

2.Selectați o zonă țintă în imaginea live.

- Faceți clic stânga pe un punct din imaginea live: punctul este mutat în centrul imaginii live. Fără efect de mărire sau micșorare.
- Țineți apăsat și trageți mouse-ul într-o poziție din dreapta jos pentru a încadra o zonă din live: zona încadrată este mărită și mutată în centrul imaginii live.
- Țineți apăsat și trageți mouse-ul într-o poziție din stânga sus pentru a încadra o zonă din live: zona încadrată este micșorat și mutată în centrul imaginii live.

3.Faceți clic din nou pe butonul pentru a dezactiva funcția.

2.3.2 Setați parametrii de transmisie

Imaginea live view poate fi afișată anormal în funcție de condițiile rețelei. În diferite medii de rețea, puteți ajusta parametrii de transmisie pentru a rezolva problema.

Pași

1.Mergi la**Configurare → Local**.

2.Setați parametrii de transmisie după cum este necesar.

Protocol

TCP

TCP asigură livrarea completă a datelor în flux și o calitate video mai bună, dar transmisia în timp real va fi afectată. Este potrivit pentru mediul de rețea stabil.

UDP

UDP este potrivit pentru mediul de rețea instabil care nu necesită o fluență video ridicată.

MULTICAST

MULTICAST este potrivit pentru situația în care există mai mulți clienți. Ar trebui să setați adresa de multicast pentru ele înainte de selectare.

Notă

Pentru informații detaliate despre multicast, consultați***Multicast*** .

HTTP

HTTP este potrivit pentru situația în care terțul trebuie să obțină fluxul de pe dispozitiv.

Performanță de redare

Cea mai scurtă întârziere

Dispozitivul ia imaginea video în timp real ca prioritate față de fluența video.

Echilibrat

Dispozitivul asigură atât imaginea video în timp real, cât și fluența.

Fluent

Dispozitivul are ca prioritate fluența video față de timpul de lucru. Într-un mediu de rețea slab, dispozitivul nu poate asigura fluența video, chiar dacă fluența este activată.

Personalizat

Puteți seta manual rata cadrelor. În mediul de rețea sărac, puteți reduce rata de cadre pentru a obține o vizualizare live fluentă. Dar este posibil ca informațiile despre reguli să nu fie afișate.

3.Clic**Bine**.

2.3.3 Setați fluxul fluid

Este o funcție pentru a aborda latența și congestionarea rețelei cauzate de starea instabilă a rețelei și pentru a menține fluidul fluxului de vizualizare live pe browserul web sau software-ul client.

Inainte sa incepi

Adăugați dispozitivul la software-ul client și selectați protocolul NPQ în software-ul client înainte de a configura funcția de streaming fluid.

Asigurați-vă că**Tip rata de biți**este selectat ca**Constant**si**SVC**este selectat ca**OFF**înainte de a activa funcția. Mergi la**Configurare → Video/Audio → Video**pentru a seta parametrii.

Pași

1.Accesați pagina de setări:**Configurare → Rețea → Setări avansate → Streaming fluid**.

2.Verifica**Activați Smooth Streaming**.

3.Selectați modul pentru streaming fluid.

Auto Rezoluția și rata de biți sunt ajustate automat, iar rezoluția are prioritate. Limitele superioare ale acestor doi parametri nu vor depăși valorile pe care le-ați setat **Video**pagină. Mergi la**Configurare → Video/Audio → Video**,Seteaza **Rezoluţie**și **Max. Rata de biți**înainte de a activa funcția de streaming fluid. În acest mod, rata de cadre va fi ajustată automat la valoarea maximă.

Rezoluţie Prioritate Rezoluția rămâne aceeași cu valoarea setată**Video**pagina, iar rata de biți va fi ajustată automat. Mergi la**Configurare → Video/Audio → Video**, Seteaza **Max. Rata de biți**înainte de a activa funcția de streaming fluid. În acest mod, framerate va fi ajustat automat la valoarea maximă.

Frame Rate Prioritate Imaginea este încă netedă chiar și sub o rețea slabă, în timp ce calitatea imaginii poate să nu fie bună.

Eroare Corecţie Rezoluția și rata de biți rămân aceleași cu valorile setate**Video**pagină. Modul este utilizat pentru a corecta eroarea datelor în timpul transmisiei pentru a asigura calitatea imaginii. Puteți seta**Proporția de corectare a erorilor**în intervalul 0-100.

Când proporția este 0, eroarea datelor va fi corectată prin retransmiterea datelor. Când proporția este mai mare de 0, datele de eroare vor fi corectate prin date redundante care sunt adăugate fluxului și retransmiterii datelor. Cu cât valoarea este mai mare, cu atât va fi generată o dată mai redundantă, cu atât mai multe erori de date ar fi corectate, dar cu atât ar fi necesară o lățime de bandă mai mare. Când proporția este 100, datele redundante vor fi la fel de mari ca datele originale, iar lățimea de bandă este necesară de două ori.

Notă

Asigurați-vă că lățimea de bandă este suficientă în modul de corectare a erorilor.

4.Salvați setările.

2.4 Video și audio

Această parte prezintă configurația parametrilor video și audio.

2.4.1 Setări video

Această parte prezintă setările parametrilor video, cum ar fi tipul fluxului, codificarea video și rezoluția.

Accesați pagina de setări:**Configurare → Video/Audio → Video**.

Tipul fluxului

Pentru dispozitivul care acceptă mai mult de un flux, puteți specifica parametrii pentru fiecare tip de flux.

Fluxul principal

Fluxul reprezintă cea mai bună performanță de flux pe care o acceptă dispozitivul. De obicei, oferă cea mai bună rezoluție și cea mai bună rată a cadrelor pe care dispozitivul le poate face. Dar rezoluția ridicată și rata de cadre înseamnă de obicei spațiu de stocare mai mare și cerințe mai mari de lățime de bandă în transmisie.

Flux secundar

Fluxul oferă de obicei opțiuni de rezoluție relativ scăzută, care consumă mai puțină lățime de bandă și spațiu de stocare.

Alte fluxuri

Steam-uri, altele decât fluxul principal și fluxul secundar, pot fi, de asemenea, oferite pentru utilizare personalizată.

Setați videoclipul personalizat

Puteți configura fluxuri video suplimentare, dacă este necesar. Pentru fluxurile video personalizate, le puteți previzualiza, dar nu le puteți înregistra sau reda.

Pași

Notă

- Funcția este acceptată numai de anumite modele de cameră.
- După restaurarea dispozitivului (nu restaurarea la setările implicite), cantitatea de fluxuri video personalizate și numele acestora sunt păstrate, dar parametrii aferenti sunt restaurați.

1.Faceți clic pentru a adăuga un flux.

2.Schimbați numele fluxului după cum este necesar.

Notă

Pentru numele fluxului sunt permise până la 32 de litere și simboluri (cu excepția &, <, >, ' sau ").

3.Personalizați parametrii fluxului (rezoluție, frame rate, bitrate max., codificare video).

4. Opțional: Adăugați descrierea fluxului după cum este necesar.

5. Opțional: Dacă nu este necesar un flux personalizat, faceți clic pentru a-l șterge.

6.Clic**Salvați**.

Tip video

Selectați conținutul (video și audio) care ar trebui să fie conținut în flux.

Video

Numai conținutul video este conținut în flux.

Video și audio

Conținutul video și conținutul audio sunt conținute în fluxul compus.

Rezoluţie

Selectați rezoluția video în funcție de nevoile reale. O rezoluție mai mare necesită lățime de bandă și stocare mai mare.

Bitrate Tip și Max. Rata de biți

Bitrate constantă

Înseamnă că fluxul este comprimat și transmis la o rată de biți relativ fixă. Viteza de compresie este rapidă, dar pe imagine poate apărea mozaic.

Rată de biți variabilă

Înseamnă că dispozitivul ajustează automat rata de biți sub set**Max. Rata de biți**. Viteza de compresie este mai mică decât viteza de biți constantă. Dar garantează calitatea imaginii scenelor complexe.

Calitate video

Când**Tip rata de biți**este setată ca Variabilă, calitatea video este configurabilă. Selectați o calitate video în funcție de nevoile reale. Rețineți că o calitate video mai mare necesită o lățime de bandă mai mare.

Frame Rate

Rata de cadre este pentru a descrie frecvența la care fluxul video este actualizat și este măsurată prin cadre pe secundă (fps).

O rată de cadre mai mare este avantajoasă atunci când există mișcare în fluxul video, deoarece menține calitatea imaginii pe tot parcursul. Rețineți că o rată de cadre mai mare necesită lățime de bandă mai mare și spațiu de stocare mai mare.

Codificare video

Reprezintă standardul de compresie pe care dispozitivul îl adoptă pentru codificarea video.

Notă

Standardele de compresie disponibile variază în funcție de modelele de dispozitiv.

H.264

H.264, cunoscut și ca MPEG-4 Part 10, Advanced Video Coding, este un standard de compresie. Fără a comprima calitatea imaginii, crește raportul de compresie și reduce dimensiunea fișierului video decât MJPEG sau MPEG-4 Partea 2.

H.264+

H.264+ este o tehnologie de codare de compresie îmbunătățită bazată pe H.264. Prin activarea H.264+, puteți estima consumul HDD după rata de biți medie maximă. În comparație cu H.264, H.264+ reduce stocarea cu până la 50% cu același bitrate maxim în majoritatea scenelor.

Când H.264+ este activat,**Max. Rata medie de biți**este configurabil. Aparatul oferă un max. rata medie de biți în mod implicit. Puteți ajusta parametrul la o valoare mai mare dacă calitatea video este mai puțin satisfăcătoare. Max. rata medie de biți nu trebuie să fie mai mare decât max. rata de biți.

Notă

Când H.264+ este activat,**Calitate video**,**I Frame Interval**,**Profil**,**SVC**,**Netezirea fluxului principal** și**ROI**nu sunt suportate.

H.265

H.265, cunoscut și ca High Efficiency Video Coding (HEVC) și MPEG-H Part 2, este un standard de compresie. În comparație cu H.264, oferă o compresie video mai bună la aceeași rezoluție, rata de cadre și calitate a imaginii.

H.265+

H.265+ este o tehnologie de codare de compresie îmbunătățită bazată pe H.265. Prin activarea H.265+, puteți estima consumul HDD după rata de biți medie maximă. În comparație cu H.265, H.265+ reduce stocarea cu până la 50%, cu același bitrate maxim în majoritatea scenelor.

Când H.265+ este activat,**Max. Rata medie de biți**este configurabil. Aparatul oferă un max. rata medie de biți în mod implicit. Puteți ajusta parametrul la o valoare mai mare dacă calitatea video este mai puțin satisfăcătoare. Max. rata medie de biți nu trebuie să fie mai mare decât max. rata de biți.

Notă

Când H.265+ este activat,**Calitate video**,**I Frame Interval**,**Profil**și**SVC**nu sunt configurabile.

Intervalul I-Frame

Intervalul I-cadre definește numărul de cadre dintre 2 I-cadre.

În H.264 și H.265, un cadru I, sau intra cadru, este un cadru autonom care poate fi decodat independent, fără nicio referire la alte imagini. Un cadru I consumă mai mulți biți decât alte cadre. Astfel, videoclipurile cu mai multe cadre I, cu alte cuvinte, un interval I-cadre mai mic, generează biți de date mai stabili și mai fiabili, în timp ce necesită mai mult spațiu de stocare.

SVC

Scalable Video Coding (SVC) este numele pentru extensia Anexa G a standardului de compresie video H.264 sau H.265.

Obiectivul standardizării SVC a fost acela de a permite codificarea unui flux de biți video de înaltă calitate care conține unul sau mai multe subseturi de biți care pot fi ele însele decodificate cu o complexitate și o calitate de reconstrucție similară cu cea obținută folosind H.264 sau H. existente. 265 design cu aceeași cantitate de date ca și în subsetul de biți. Fluxul de biți subsetul este derivat prin eliminarea pachetelor din fluxul de biți mai mare.

SVC permite compatibilitatea înainte pentru hardware-ul mai vechi: același flux de biți poate fi consumat de hardware-ul de bază care poate decoda doar un subset de rezoluție scăzută, în timp ce hardware-ul mai avansat va putea decoda fluxul video de înaltă calitate.

MPEG4

MPEG4, referitor la MPEG-4 Partea 2, este un format de compresie video dezvoltat de Moving Picture Experts Group (MPEG).

MJPEG

Motion JPEG (M-JPEG sau MJPEG) este un format de compresie video în care este utilizată tehnologia de codare intraframe. Imaginile în format MJPEG sunt comprimate ca imagini JPEG individuale.

Profil

Această funcție înseamnă că sub aceeași rată de biți, cu cât profilul este mai complex, cu atât calitatea imaginii este mai ridicată, iar cerința pentru lățimea de bandă a rețelei este, de asemenea, mai mare.

Netezire

Se referă la netezimea fluxului. Cu cât valoarea netezirii este mai mare, cu atât fluența fluxului va fi mai bună, totuși, calitatea video poate să nu fie atât de satisfăcătoare. Cu cât valoarea mai mică a netezirii este, cu atât va fi mai mare calitatea fluxului, deși poate părea că nu este fluent.

2.4.2 ROI

Codarea ROI (regiune de interes) ajută la discriminarea rentabilității investiției și a informațiilor de fundal în compresia video. Tehnologia atribuie mai multe resurse de codare regiunii de interes, astfel pentru a crește calitatea ROI, în timp ce informațiile de fundal sunt mai puțin concentrate.

Setați rentabilitatea investiției

Codificarea ROI (Region of Interest) ajută la alocarea mai multor resurse de codare regiunii de interes, astfel încât să mărească calitatea ROI, în timp ce informațiile de fundal sunt mai puțin concentrate.

Inainte sa incepi

Vă rugăm să verificați tipul de codare video. ROI este acceptat atunci când tipul de codare video este H.264 sau H. 265.

Pași

1.Mergi la**Configurare → Video/Audio → ROI**.

2.Verifica**Permite**.

3.Selectați**Tipul fluxului**.

4.Selectați**Regiunea nr.**în**Regiunea fixă**pentru a desena regiunea ROI.

1) Faceți clic**Zona de desenare**.

2) Faceți clic și trageți mouse-ul pe ecranul de vizualizare pentru a desena regiunea fixă.

3) Faceți clic**Opriți desenul**.

Notă

Selectați regiunea fixă care trebuie ajustată și trageți mouse-ul pentru a-și ajusta poziția.

5.Introduceți**Numele regiunii**și**Nivelul ROI**.

6.Clic**Salvați**.

Notă

Cu cât nivelul ROI este mai mare, cu atât imaginea regiunii detectate este mai clară.

7. Opțional: Selectați alt număr de regiune și repetați pașii de mai sus dacă trebuie să desenați mai multe regiuni fixe.

2.4.3 Afișare informații. pe Stream

Informațiile obiectelor (de exemplu, om, vehicul etc.) sunt marcate în fluxul video. Puteți seta reguli pe dispozitivul din spate conectat sau pe software-ul client pentru a detecta evenimentele, inclusiv trecerea liniei, intruziunea etc.

Pași

1.Accesați pagina de setări:**Configurare → Video/Audio → Afișare informații. pe Stream**.

2.Verifica**Activați Dual-VCA**.

3.Clic**Salvați**.

2.4.4 Setări audio

Este o funcție de setare a parametrilor audio, cum ar fi codificarea audio, filtrarea zgomotului din mediu.

Accesați pagina de setări audio:**Configurare → Video/Audio → Audio**.

Codificare audio

Selectați compresia de codificare audio a sunetului.

Intrare audio

Notă

- Conectați dispozitivul de intrare audio după cum este necesar.
- Afișajul de intrare audio variază în funcție de modelele de dispozitiv.

LineIn	A stabilit**Intrare audio**la**LineIn**atunci când dispozitivul se conectează la dispozitivul de intrare audio cu putere mare de ieșire, cum ar fi MP3, sintetizator sau pickup activ.
Microfon cuplat	A stabilit**Intrare audio**la**Microfon cuplat**atunci când dispozitivul se conectează la dispozitivul de intrare audio cu putere de ieșire scăzută, cum ar fi microfonul sau pickup-ul pasiv.

Iesire audio

Notă

Conectați dispozitivul de ieșire audio după cum este necesar.

Este un comutator al ieșirii audio a dispozitivului. Când este dezactivat, tot sunetul dispozitivului nu poate ieși.
Afișajul ieșirii audio variază în funcție de modurile dispozitivului.

Filtru de zgomot de mediu

Setați-l ca OFF sau ON. Când funcția este activată, zgomotul din mediu poate fi filtrat într-o oarecare măsură.

2.4.5 Audio bidirecțional

Este folosit pentru a realiza funcția audio bidirecțională între centrul de monitorizare și țintă din ecranul de monitorizare.

Inainte sa incepi

- Asigurați-vă că dispozitivul de intrare audio (pick-up sau microfon) și dispozitivul de ieșire audio (difuzor) conectat la dispozitiv funcționează corect. Consultați specificațiile dispozitivelor de intrare și ieșire audio pentru conectarea dispozitivului.
- Dacă dispozitivul are microfon și difuzor încorporate, funcția audio bidirecțională poate fi activată direct.

Pași

1.Clic**Vizualizare live**.

2.Clic pe bara de instrumente pentru a activa funcția audio bidirecțională a

3.Clic camerei. , dezactivați funcția audio bidirecțională.

2.4.6 Setări de afișare

Oferă setările parametrilor pentru a ajusta caracteristicile imaginii.

Mergi la**Configurare → Imagine → Setări afișare**. Clic**Mod implicit**pentru a restabili setările.

Modul scena

Există mai multe seturi de parametri de imagine predefiniti pentru diferite medii de instalare. Selectați o scenă în funcție de mediul real de instalare pentru a accelera setările de afișare.

Ajustarea imaginii

Prin ajustarea**Luminozitate**,**Saturare**,**Nuanţă**,**Contrast**și**Claritate**, imaginea poate fi afișată cel mai bine.

Figura 2-1 Saturație

Setări de expunere

Expunerea este controlată de combinația irisului, obturatorului și sensibilității foto. Puteți regla efectul imaginii setând parametrii de expunere.

În modul manual, trebuie să setați**Timp de expunere**,**Câştig**și**Obturator lent**.

Concentrează-te

Oferă opțiuni pentru reglarea modului de focalizare.

Modul de focalizare

Auto

Dispozitivul focalizează automat pe măsură ce scena se schimbă. Dacă nu puteți obține o imagine bine focalizată în modul automat, reduceți sursele de lumină din imagine și evitați luminile intermitente.

Semi auto

Dispozitivul focalizează o dată după PTZ și zoomul obiectivului. Dacă imaginea este clară, focalizarea nu se schimbă atunci când scena se schimbă.

Manual

Puteți regla manual focalizarea pe pagina de vizualizare live.

Comutator zi/noapte

Funcția de comutare zi/noapte poate oferi imagini color în modul de zi și poate activa lumina de umplere în modul de noapte. Modul comutator este configurabil.

Zi

Imaginea este întotdeauna colorată.

Noapte

Imaginea este alb/negru sau colorată, iar lumina suplimentară va fi activată pentru a asigura o imagine clară cu vizualizare live pe timp de noapte.

Notă

Doar anumite modele de dispozitive acceptă imaginea suplimentară luminoasă și colorată.

Auto

Camera comută automat între modul zi și modul noapte în funcție de iluminare.

Comutator programat

Seteaza**Timpul de începere**si**Sfârșitul timpului**pentru a defini durata pentru modul de zi.

Notă

Funcția de comutare zi/noapte variază în funcție de model.

Scară de gri

Puteți alege gama de**Scară de gri**ca [0-255] sau [16-235].

Roti

Când este activată, vizualizarea live se va roti la 90 ° în sens invers acelor de ceasornic. De exemplu, 1280 × 720 este rotit la 720 × 1280.

Activarea acestei funcții poate modifica intervalul efectiv de monitorizare în direcția verticală.

Corectarea distorsiunii lentilei

Pentru dispozitivele echipate cu lentile motorizate, imaginea poate apărea distorsionată într-o oarecare măsură. Activați această funcție pentru a corecta distorsiunea.

Notă

- Această funcție este acceptată numai de anumite dispozitive echipate cu lentile motorizate.
- Marginea imaginii se va pierde dacă această funcție este activată.

BLC

Dacă focalizați asupra unui obiect în condiții de lumină de fundal puternică, obiectul va fi prea întunecat pentru a fi văzut clar. BLC (compensarea luminii de fundal) compensează lumina pentru obiectul din față pentru a-l clarifica. Dacă modul BLC este setat ca**Personalizat**, puteți desena un dreptunghi roșu pe imaginea de vizualizare live ca zonă BLC.

WDR

Funcția WDR (Wide Dynamic Range) ajută camera să ofere imagini clare în mediul înconjurător, cu diferențe puternice de iluminare.

Când în câmpul vizual există simultan zone foarte luminoase și foarte întunecate, puteți activa funcția WDR și puteți seta nivelul. WDR echilibrează automat nivelul de luminozitate al întregii imagini și oferă imagini clare cu mai multe detalii.

Notă

Când WDR este activat, este posibil ca unele alte funcții să nu fie acceptate. Consultați interfața reală pentru detalii.

Figura 2-2 WDR

HLC

Când zona luminoasă a imaginii este supraexpusă și zona întunecată este subexpusă, funcția HLC (High Light Compression) poate fi activată pentru a slăbi zona luminoasă și a lumina zona întunecată, astfel încât să se obțină echilibrul luminii imaginea de ansamblu.

Echilibru alb

Balanța de alb este funcția de redare a albului a camerei. Este folosit pentru a regla temperatura culorii în funcție de mediu.

Figura 2-3 Balanța de alb

DNR

Digital Noise Reduction este utilizat pentru a reduce zgomotul imaginii și pentru a îmbunătăți calitatea imaginii. **Normal** și**Expert**modurile sunt selectabile.

Normal

Setați nivelul DNR pentru a controla gradul de reducere a zgomotului. Nivelul superior înseamnă un grad de reducere mai puternic.

Expert

Setați nivelul DNR atât pentru DNR spațial, cât și pentru DNR temporal pentru a controla gradul de reducere a zgomotului. Nivelul superior înseamnă un grad de reducere mai puternic.

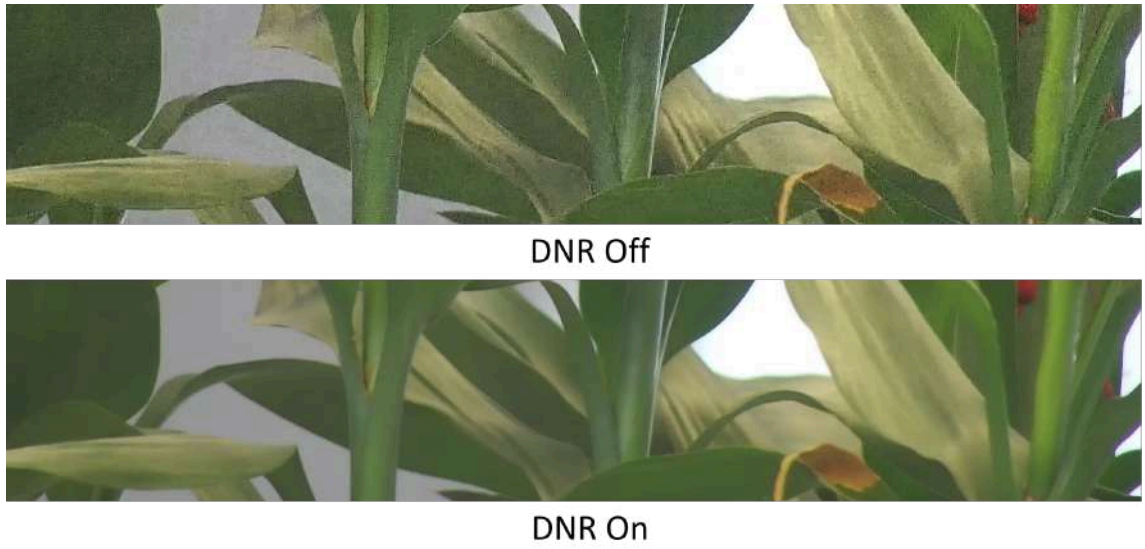


Figura 2-4 DNR

Dezaburire

Puteți activa funcția de dezaburire când mediul este în ceață și imaginea este ceață. Îmbunătățește detaliile subtile, astfel încât imaginea să pară mai clară.

Figura 2-5 Dezaburire

EIS

Creșteți stabilitatea imaginii video utilizând tehnologia de compensare a jitterului.

Oglindă

Când imaginea live view este inversul scenei reale, această funcție ajută la afișarea normală a imaginii.

Selectați modul oglindă după cum este necesar.

Notă

Înregistrarea video va fi întreruptă la scurt timp când funcția este activată.

Comutarea parametrilor imaginii

Dispozitivul comută automat parametrii imaginii în perioade de timp stabilite.

Accesați pagina de setare a comutatorului parametrilor imaginii:**Configurare → Imagine → Comutare parametri imagine**, și setați parametrii după cum este necesar.

Setați comutatorul

Comutați automat parametrii imaginii la scenă în anumite perioade de timp.

Pași

1.Verifica**Permite**.

2.Selectați și configurați perioada de timp corespunzătoare și scena.

Notă

Pentru configurarea scenei, consultați***Modul scena*** .

3.Clic**Salvați**.

Standard video

Standardul video este o capacitate a unei plăci video sau a unui dispozitiv de afișare video care definește cantitatea de culori afișate și rezoluția. Cele mai frecvente două standarde video utilizate sunt NTSC și PAL. În NTSC, 30 de cadre sunt transmise în fiecare secundă. Fiecare cadru este alcătuit din 525 de linii de scanare individuale. În PAL, 25 de cadre sunt transmise în fiecare secundă. Fiecare cadru este alcătuit din 625 de linii de scanare individuale. Selectați standardul de semnal video în funcție de sistemul video din țara/regiunea dvs.

Ieșire video locală

Dacă dispozitivul este echipat cu interfețe de ieșire video, cum ar fi BNC, CVBS, HDMI și SDI, puteți previzualiza imaginea live direct conectând dispozitivul la un ecran de monitor.

Selectați modul de ieșire ca ON/OFF pentru a controla ieșirea.

2.4.7 OSD

Puteți personaliza informațiile OSD (Afișare pe ecran), cum ar fi numele dispozitivului, ora/data, fontul, culoarea și suprapunerea textului afișate în fluxul video.

Accesați pagina de setări OSD:**Configurare → Imagine → Setări OSD**.Setați parametrii corespunzători și faceți clic**Salvați**pentru a intra în vigoare.

Set de caractere

Selectați setul de caractere pentru informațiile afișate. Dacă coreeană trebuie să fie afișată pe ecran, selectați **EUC-KR**. În caz contrar, selectați**GBK**.

Informații afișate

Setați numele camerei, data, săptămâna și formatul de afișare aferent acestora.

Suprapunere text

Setați text suprapus personalizat pe imagine.

Parametrii OSD

Setați parametrii OSD, cum ar fi**Modul de afișare**,**Dimensiune OSD**,**Culoare font**, și**Aliniere**.

2.4.8 Setați mască de confidențialitate

Funcția blochează anumite zone din vizualizarea live pentru a proteja confidențialitatea. Indiferent de modul în care se mișcă dispozitivul, scena blocată nu va fi văzută niciodată.

Pași

1.Accesați pagina de setare a măștii de confidențialitate:**Configurare → Imagine → Mască de confidențialitate**.

2.Verifica**Activați Masca de confidențialitate**.

3.Clic**Zona de desenare**. Trageți mouse-ul în vizualizarea live pentru a desena o zonă închisă.

Trageți colțurile zonei Reglați dimensiunea zonei. Reglați

Trageți zona poziția zonei. Ștergeți toate

Faceți clic pe Clear All zonele pe care le-ați setat.

4.Clic**Opriți desenul**.

5.Clic**Salvați**.

2.4.9 Imagine suprapusă

Suprapuneți o imagine personalizată pe vizualizarea live.

Inainte sa incepi

Imaginea de suprapus trebuie să fie în format BMP cu 24 de biți, iar dimensiunea maximă a imaginii este de 128 × 128 pixeli.

Pași

1.Accesați pagina de setare a suprapunerii imaginii:**Configurare → Imagine → Suprapunere imagine**.

2.Clic**Naviga**pentru a selecta o imagine și faceți clic**Încărcați**.

Imaginea cu un dreptunghi roșu va apărea în vizualizare live după încărcarea cu succes.

3.Verifica**Activați Suprapunerea imaginii**.

4.Trageți imaginea pentru a-i ajusta poziția.

5.Clic**Salvați**.

2.4.10 Setați decuparea țintă

Puteți decupa imaginea, transmite și salva doar imaginile din zona țintă pentru a economisi lățimea de bandă de transmisie și stocarea.

Pași

1.Mergi la**Configurare → Video/Audio → Decupare țintă**.

2.Verifica**Activați decuparea țintă**și setați**Al treilea flux**dupa cum**Tipul fluxului**.

Notă

După activarea decupării țintei, a treia rezoluție a fluxului nu poate fi configurată.

3.Alege o**Rezoluție de decupare**.

Un cadru roșu apare în vizualizarea live.

4.Trageți cadrul în zona țintă.

5.Clic**Salvați**.

Notă

- Doar anumite modele acceptă decuparea țintei, iar funcția variază în funcție de diferitele modele de cameră.
- Unele funcții pot fi dezactivate după activarea decupării țintei.

2.5 Înregistrare video și captură de imagini

Această parte prezintă operațiunile de captare a clipurilor video și instantanee, redare și descărcare a fișierelor capturate.

2.5.1 Setări de stocare

Această parte prezintă configurația mai multor căi de stocare comune.

Setați cardul de memorie

Dacă alegeți să stocați fișierele pe cardul de memorie, asigurați-vă că introduceți și formatați cardul de memorie în avans.

Inainte sa incepi

Introduceți cardul de memorie în cameră. Pentru instalare detaliată, consultați*Ghid de inițiere rapidă*a camerei.

Pași

1. Accesați pagina de setări de gestionare a spațiului de stocare:**Configurare → Stocare → Gestionare stocare → Gestionare HDD**.
2. Selectați cardul de memorie și faceți clic**Format**pentru a începe inițializarea cardului de memorie.

   The**stare**a cardului de memorie se transformă în**Normal**din**Neinițializat**, ceea ce înseamnă că cardul de memorie poate fi utilizat în mod normal.
3. **Opțional:**Definiți**Cotă**a cardului de memorie. Introduceți procentul de cotă pentru diferite conținuturi în funcție de nevoile dvs.
4. Clic**Salvați**.

Detectați starea cardului de memorie

Dispozitivul detectează starea cardului de memorie Hikvision. Primiți notificări când cardul de memorie este detectat anormal.

Inainte sa incepi

Pagina de configurare apare numai când un card de memorie Hikvision este instalat pe dispozitiv.

Pași

1. Mergi la**Configurare → Stocare → Gestionare stocare → Detectare card de memorie**.
2. Clic**Detectarea stării**pentru a verifica**Durata de viață rămasă**și**Stare de sănătate**a cardului dvs. de memorie.

   Durata de viață rămasă

   Arată procentul din durata de viață rămasă. Durata de viață a unui card de memorie poate fi influențată de factori precum capacitatea sa și rata de biți. Trebuie să schimbați cardul de memorie dacă durata de viață rămasă nu este suficientă.

   Stare de sănătate

   Acesta arată starea cardului de memorie. Există trei descrieri de stare: bun, rău și deteriorat. Veți primi o notificare dacă starea de sănătate este altceva decât bună atunci când**Program de armare**și**Metoda de legare**sunt aranjate.

   Notă

   Este recomandat să schimbați cardul de memorie atunci când starea de sănătate nu este „bună”.
3. Clic**Blocare R/W**pentru a seta permisiunea de citire și scriere pe cardul de memorie.
   - Adăugați o blocare

A. Selectează**Comutator de blocare**un fiu.

b. Introduceți parola.

c. Clic**Salvați**

- Deblocați
  - Dacă utilizați cardul de memorie pe dispozitivul care îl blochează, deblocarea se va face automat și nu sunt necesare proceduri de deblocare din partea utilizatorilor.
  - Dacă utilizați cardul de memorie (cu blocare) pe un alt dispozitiv, puteți accesa**Management HDD** pentru a debloca manual cardul de memorie. Selectați cardul de memorie și faceți clic **Deblocați**. Introduceți parola corectă pentru a o debloca.
- Scoateți încuietoarea

A. Selectează**Comutator de blocare**ca OFF.

b. Introduceți parola în**Setări parole**.

c. Clic**Salvați**.

Notă

- Numai utilizatorul administrator poate seta**Blocare R/W**.
- Cardul de memorie poate fi citit și scris numai atunci când este deblocat.
- Dacă dispozitivul, care adaugă o blocare la un card de memorie, este restabilit la setările din fabrică, puteți accesa**Management HDD**pentru a debloca cardul de memorie.

4.A stabilit**Program de armare**și**Metoda de legare**. Vedea***Setați programul de armare*** și***Setări pentru metoda de conectare*** pentru detalii.

5.Clic**Salvați**.

Setați FTP

Puteți configura serverul FTP pentru a salva imaginile care sunt capturate de evenimente sau de o sarcină de instantanee cronometrată.

Inainte sa incepi

Obțineți mai întâi adresa serverului FTP.

Pași

1.Mergi la**Configurare → Rețea → Setări avansate → FTP**.

2.Configurați setările FTP.

Protocolul FTP

FTP și SFTP sunt selectabile. Încărcarea fișierelor este criptată utilizând protocolul SFTP.

Adresa și portul serverului

Adresa serverului FTP și portul corespunzător.

Nume de utilizator și parolă

Utilizatorul FTP ar trebui să aibă permisiunea de a încărca imagini.

Dacă serverul FTP acceptă încărcarea imaginilor de către utilizatori anonimi, puteți verifica**Anonim** pentru a ascunde informațiile despre dispozitiv în timpul încărcării.

Structura directorului

Calea de salvare a instantaneelor pe serverul FTP. **Interval de**

înregistrare a imaginii

Pentru o gestionare mai bună a imaginii, puteți seta intervalul de înregistrare a imaginilor de la 1 zi la 30 de zile. Imaginile capturate în același interval de timp vor fi salvate într-un folder numit după data de început și data de încheiere a intervalului de timp.

Nume imagine

Setați regula de denumire pentru imaginile capturate. Tu poti alege**Mod implicit**în lista derulantă pentru a utiliza regula implicită, adică IP address_channel number_capture time_event type.jpg (de exemplu, 10.11.37.189_01_20150917094425492_FACE_DETECTION.jpg). Sau îl puteți personaliza adăugând un **Prefix personalizat**la regula implicită de denumire.

3.Verifica**Încarcă imagine**pentru a activa încărcarea instantaneelor pe serverul FTP.

4.Verifica**Activați reaprovizionarea automată a rețelei**.

Notă

Încărcați pe FTP/Card de memorie/NASîn**Metoda de legare**și**Activați reaprovizionarea automată a rețelei**ar trebui să fie ambele activate simultan.

5.Clic**Test**pentru a verifica serverul FTP.

6.Clic**Salvați**.

Setați NAS

Luați serverul de rețea ca disc de rețea pentru a stoca fișierele de înregistrare, imaginile capturate etc.

Inainte sa incepi

Obțineți mai întâi adresa IP a discului de rețea.

Pași

1.Accesați pagina de setări NAS:**Configurare → Stocare → Gestionare stocare → HDD net**.

2.Clic**HDD nr.**. Introduceți adresa serverului și calea fișierului pentru disc.

Adresa serverului

Adresa IP a discului de rețea. **Calea**

fișierului

Calea de salvare a fișierelor de pe disc de rețea.

Tip de montare

Selectați protocolul sistemului de fișiere în funcție de sistemul de operare.

Introduceți numele de utilizator și parola HDD-ului net pentru a garanta securitatea dacă**SMB/CIFS**este selectat.

3.Clic**Test**pentru a verifica dacă discul de rețea este disponibil.
4.Clic**Salvați**.

Protecție eMMC

Este de a opri automat utilizarea eMMC ca mediu de stocare atunci când starea sa de sănătate este slabă.

Notă

Protecția eMMC este acceptată numai de anumite modele de dispozitive cu hardware eMMC.

Mergi la**Configurare → Sistem → Întreținere → Serviciu sistem**pentru setari.

eMMC, prescurtare pentru card multimedia încorporat, este un sistem de memorie nevolatilă încorporat. Este capabil să stocheze imaginile sau videoclipurile capturate ale dispozitivului.

Dispozitivul monitorizează starea de sănătate a eMMC și oprește eMMC atunci când starea acestuia este slabă. În caz contrar, utilizarea unui eMMC uzat poate duce la eșecul de pornire a dispozitivului.

Setați stocarea în cloud

Ajută la încărcarea imaginilor și datelor capturate în cloud. Platforma solicită imagini direct din cloud pentru imagine și analiză. Funcția este acceptată doar de anumite modele.

Pași

Prudență

Dacă stocarea în cloud este activată, imaginile sunt stocate în primul rând în managerul video cloud.

1.Mergi la**Configurare → Stocare → Gestionare stocare → Stocare în cloud**.
2.Verifica**Activați stocarea în cloud**.
3.Setați parametrii de bază.

Versiunea protocolului	Versiunea de protocol a managerului video cloud.
IP server	Adresa IP a managerului video cloud. Suportă adresa IPv4.
Servire Port	Portul managerului video cloud. Vi se recomandă să utilizați portul implicit.
Cheie de acces	Cheia pentru a vă conecta la managerul video cloud.
Cheie secreta	Cheia pentru criptarea datelor stocate în managerul video cloud.
Nume de utilizator și Parola	Numele de utilizator și parola managerului video cloud.
Depozitarea imaginilor ID-ul piscinei	ID-ul regiunii de stocare a imaginilor în managerul video cloud. Asigurați-vă că ID-ul pool-ului de stocare și ID-ul regiunii de stocare sunt identice.

4.Clic**Test**pentru a testa setările configurate.

5.Clic**Salvați**.

2.5.2 Înregistrare video

Această parte prezintă operațiunile de înregistrare manuală și programată, redare și descărcare a fișierelor înregistrate.

Înregistrează automat

Această funcție poate înregistra video automat în perioadele de timp configurate.

Inainte sa incepi

Selectați**Declanșează înregistrarea**în setările de eveniment pentru fiecare tip de înregistrare, cu excepția**Continuu**. Vedea***Eveniment și alarmă*** pentru detalii.

Pași

1.Mergi la**Configurare → Stocare → Setări de programare → Program de înregistrare**.

2.Verifica**Permite**.

3.Selectați un tip de înregistrare.

Notă

Tipul de înregistrare variază în funcție de diferite modele.

Continuu

Videoclipul va fi înregistrat continuu conform programului.

Mişcare

Când detectarea mișcării este activată și înregistrarea declanșării este selectată ca metodă de conectare, mișcarea obiectului este înregistrată.

Alarma

Când intrarea alarmei este activată și înregistrarea declanșării este selectată ca metodă de conectare, videoclipul este înregistrat după primirea semnalului de alarmă de la dispozitivul extern de intrare de alarmă.

Mișcare | Alarma

Videoclipul este înregistrat atunci când este detectată mișcare sau este primit semnal de alarmă de la dispozitivul extern de intrare de alarmă.

Mișcare și alarmă

Videoclipul este înregistrat numai atunci când este detectată mișcare și semnalul de alarmă este primit de la dispozitivul extern de intrare de alarmă.

Eveniment

Videoclipul este înregistrat când este detectat evenimentul configurat.

4.Setați programul pentru tipul de înregistrare selectat. A se referi la***Setați programul de armare*** pentru operatia de setare.

5. Click **Advanced** to set the advanced settings.

Overwrite

Enable **Overwrite** to overwrite the video records when the storage space is full. Otherwise the camera cannot record new videos.

Pre-record

The time period you set to record before the scheduled time.

Post-record

The time period you set to stop recording after the scheduled time.

Stream Type

Select the stream type for recording.

Note

When you select the stream type with higher bitrate, the actual time of the pre-record and post-record may be less than the set value.

Recording Expiration

The recordings are deleted when they exceed the expired time. The expired time is configurable. Note that once the recordings are deleted, they can not be recovered.

6. Click **Save**.

Record Manually

Steps

1. Go to **Configuration → Local** .
2. Set the **Record File Size** and saving path to for recorded files.
3. Click **Save**.
4. Click in the live view interface to start recording. Click to stop recording.

Set Lite Storage

After the lite storage is enabled, the frame rate and bitrate of the video stream can be reduced to lengthen the storage time of the memory card when there is no moving object in the monitoring scenario.

Steps

1. Go to **Configuration → Storage → Storage Management → Lite Storage** .
2. Check **Enable** and set the level. The higher the level is, the larger the frame rate and bitrate are, and the shorter the recommended storage time is.
3. Set the storage time. The device automatically calculates the bitrate and offers the recommended storage time according to the memory card space and level. You are recommended to set the storage time to the device recommended time.

Note

- If the lite storage is enabled, unformatted memory card will be formatted automatically.
- The displayed available space of the memory card is assigned by default according to **Percentage of Record** in **Storage → Storage Management → Quota** . You can adjust it as required.
- Only certain device models support the function.

Playback and Download Video

You can search, playback and download the videos stored in the local storage or network storage.

Steps

1. Click **Playback**.
2. Set search condition and click **Search**.

   The matched video files showed on the timing bar.
3. Click ▶ to play the video files.
   - Click ✂ to clip video files.
   - Double click the live view image to play video files in full screen. Press **ESC** to exit full screen.

   Note

   Go to **Configuration → Local** , click **Save clips to** to change the saving path of clipped video files.
4. Click ⬇ on the playback interface to download files.
   1) Set search condition and click **Search**.
   2) Select the video files and then click **Download**.

      Note

      Go to **Configuration → Local** , click **Save downloaded files to** to change the saving path of downloaded video files.

2.5.3 Capture Configuration

The device can capture the pictures manually or automatically and save them in configured saving path. You can view and download the snapshots.

Capture Automatically

This function can capture pictures automatically during configured time periods.

Before You Start

If event-triggered capture is required, you should configure related linkage methods in event settings. Refer to ***Event and Alarm*** for event settings.

Steps

1. Go to **Configuration → Storage → Schedule Settings → Capture → Capture Parameters** .
2. Set the capture type.

   Timing

   Capture a picture at the configured time interval.

   Event-Triggered

   Capture a picture when an event is triggered.
3. Set the **Format**, **Resolution**, **Quality**, **Interval**, and **Capture Number**.
4. Refer to ***Set Arming Schedule*** for configuring schedule time.
5. Click **Save**.

Capture Manually

Steps

1. Go to **Configuration → Local** .
2. Set the **Image Format** and saving path to for snapshots.

   JPEG

   The picture size of this format is comparatively small, which is better for network transmission.

   BMP

   The picture is compressed with good quality.
3. Click **Save**.
4. Click near the live view or play back window to capture a picture manually.

Set Timing Wake

When the device is sleeping, it will wake up at the set time interval, and capture pictures and upload them.

Steps

Note

The function is only supported by certain device models.

1. Go to **Configuration → System → System Settings → Power Consumption Mode** , under **Sleep Schedule**, click the time schedule to set **Sleep Capture Interval**.
2. Enter **Configuration → Event → Basic Event → Timing Wake** .
3. Check **Enable**.
4. Select **Capture Types**.
5. For the linkage method settings, see ***Linkage Method Settings*** .
6. Click **Save**.

Result

The device will wake up at the set sleep capture interval, and capture pictures and upload them.

View and Download Picture

You can search, view and download the pictures stored in the local storage or network storage.

Steps

1. Click **Picture**.
2. Set search condition and click **Search**.
   The matched pictures showed in the file list.
3. Select the pictures then click **Download** to download them.

Note

Go to **Configuration → Local** , click **Save snapshots when playback** to change the saving path of pictures.

2.6 Event and Alarm

This part introduces the configuration of events. The device takes certain response to triggered alarm. Certain events may not be supported by certain device models.

2.6.1 Basic Event

Set Motion Detection

It helps to detect the moving objects in the detection region and trigger the linkage actions.

Steps

1. Go to **Configuration → Event → Basic Event → Motion Detection** .
2. Check **Enable Motion Detection**.
3. **Optional:** Highlight to display the moving object in the image in green.
   1) Check **Enable Dynamic Analysis for Motion**.
   2) Go to **Configuration → Local** .
   3) Set **Rules** to **Enable**.
4. Select **Configuration Mode**, and set rule region and rule parameters.
   - For the information about normal mode, see ***Normal Mode*** .
   - For the information about expert mode, see ***Expert Mode*** .
5. Set the arming schedule and linkage methods. For the information about arming schedule settings, see ***Set Arming Schedule*** . For the information about linkage methods, see ***Linkage Method Settings*** .

6. Click **Save**.

Expert Mode

You can configure different motion detection parameters for day and night according to the actual needs.

Steps

1. Select **Expert Mode** in **Configuration**.
2. Set parameters of expert mode.

   Scheduled Image Settings

   OFF

   Image switch is disabled.

   Auto-Switch

   The system switches day/night mode automatically according to environment. It displays colored image at day and black and white image at night.

   Scheduled-Switch

   The system switches day/night mode according to the schedule. It switches to day mode during the set periods and switches to night mode during the other periods.

   Sensitivity

   The higher the value of sensitivity is, the more sensitive the motion detection is. If scheduled image settings is enabled, the sensitivity of day and night can be set separately.
3. Select an **Area** and click **Draw Area**. Click and drag the mouse on the live image and then release the mouse to finish drawing one area.

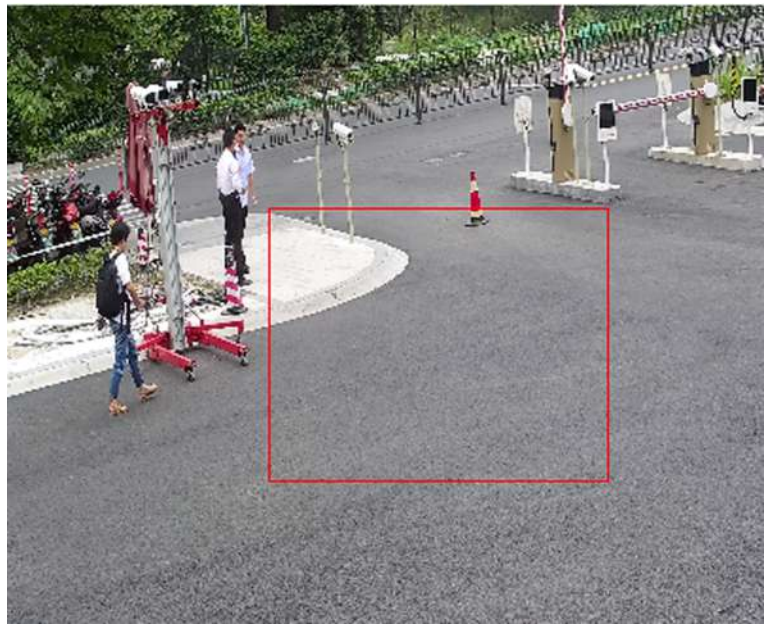


Figure 2-6 Set Rules

Stop Drawing Finish drawing one area.

Clear All Delete all the areas.

4. Click **Save**.
5. **Optional:** Repeat above steps to set multiple areas.

Normal Mode

You can set motion detection parameters according to the device default parameters.

Steps

1. Select normal mode in **Configuration**.
2. Set the sensitivity of normal mode. The higher the value of sensitivity is, the more sensitive the motion detection is. If the sensitivity is set to ***0***, motion detection and dynamic analysis do not take effect.
3. Set **Detection Target**. Human and vehicle are available. If the detection target is not selected, all the detected targets will be reported, including the human and vehicle.
4. Click **Draw Area**. Click and drag the mouse on the live video, and then release the mouse to finish drawing one area.

Stop Drawing Stop drawing one area.

Clear All Clear all the areas.

5. **Optional:** You can set the parameters of multiple areas by repeating the above steps.

Set Video Tampering Alarm

When the configured area is covered and cannot be monitored normally, the alarm is triggered and the device takes certain alarm response actions.

Steps

1. Go to **Configuration → Event → Basic Event → Video Tampering** .
2. Check **Enable**.
3. Set the **Sensitivity**. The higher the value is, the easier to detect the area covering.
4. Click **Draw Area** and drag the mouse in the live view to draw the area.

Stop Drawing	Finish drawing.
Clear All	Delete all the drawn areas.

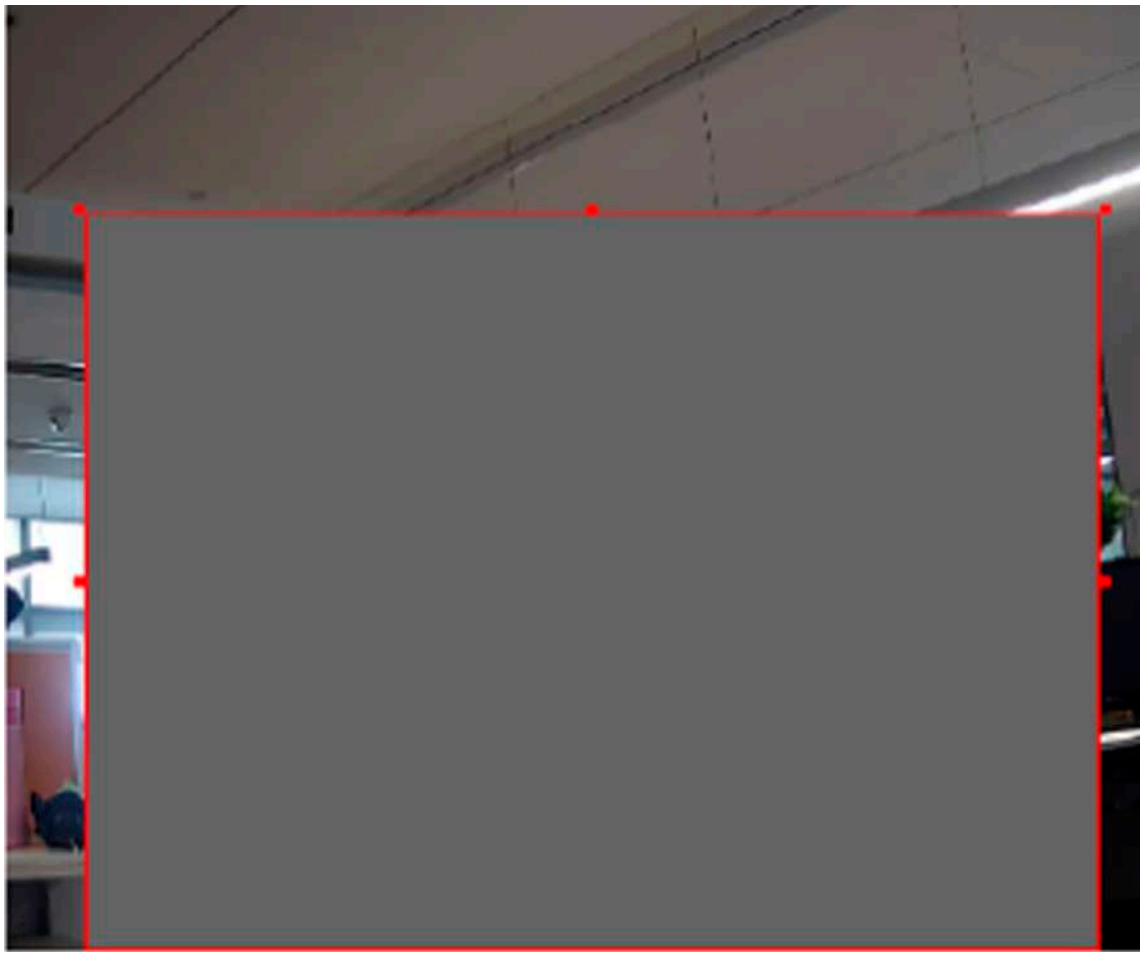


Figure 2-7 Set Video Tampering Area

5. Refer to ***Set Arming Schedule*** for setting scheduled time. Refer to ***Linkage Method Settings*** for setting linkage method.
6. Click **Save**.

Set PIR Alarm

A PIR (Passive Infrared) alarm is triggered when an intruder moves within the detector's field of view. The heat energy dissipated by a person, or any other warm blooded creature such as dogs, cats, etc., can be detected.

Steps

Note

Only certain models support PIR alarm.

1. Go to **Configuration → Advanced Configuration → Basic Event → PIR Alarm** .
2. Check **Enable PIR Alarm**.
3. Refer to ***Set Arming Schedule*** for setting scheduled time. Refer to ***Linkage Method Settings*** for setting linkage method.
4. Click **Save**.

Set Exception Alarm

Exception such as network disconnection can trigger the device to take corresponding action.

Steps

1. Go to **Configuration → Event → Basic Event → Exception** .
2. Select **Exception Type**.

HDD Full	The HDD storage is full.
HDD Error	Error occurs in HDD.
Network Disconnected	The device is offline.
IP Address Conflicted	The IP address of current device is same as that of other device in the network.
Illegal Login	Incorrect user name or password is entered.

3. Refer to ***Linkage Method Settings*** for setting linkage method.
4. Click **Save**.

Set Alarm Input

Alarm signal from the external device triggers the corresponding actions of the current device.

Before You Start

Make sure the external alarm device is connected. See *Quick Start Guide* for cable connection.

Steps

1. Go to **Configuration → Event → Basic Event → Alarm Input** .

2. Check **Enable Alarm Input Handling**.
3. Select **Alarm Input NO.** and **Alarm Type** from the dropdown list. Edit the **Alarm Name**.
4. Refer to ***Set Arming Schedule*** for setting scheduled time. Refer to ***Linkage Method Settings*** for setting linkage method.
5. Click **Copy to...** to copy the settings to other alarm input channels.
6. Click **Save**.

Set Video Quality Diagnosis

When the video quality of the device is abnormal and the alarm linkage is set, the alarm will be triggered automatically.

Steps

1. Go to **Configuration → Event → Basic Event → Video Quality Diagnosis** .
2. Select **Diagnosis Type**.
3. Set the corresponding parameters.

   Alarm Detection Interval

   The time interval to detect the exception.

   Sensitivity

   The higher the value is, the more easily the exception will be detected, and the higher possibility of misinformation would be.

   Alarm Delay Times

   The device uploads the alarm when the alarm reaches the set number of times.
4. Check **Enable**, and the selected diagnosis type will be detected.
5. Set arming schedule. See ***Set Arming Schedule*** .
6. Set linkage method. See ***Linkage Method Settings*** .
7. Click **Save**.

Note

The function is only supported by certain models. The actual display varies with models.

Set Vibration Detection

It is used to detect whether the device is vibrating. The device reports an alarm and triggers linkage actions if the function is enabled.

Steps

1. Go to **Configuration → Event → Basic Event → Vibration Detection** .
2. Check **Enable**.
3. Drag the slider to set the detection sensitivity. You can also enter number to set the sensitivity.
4. Set the arming schedule. See ***Set Arming Schedule*** .

5. Set the linkage method. See ***Linkage Method Settings*** .
6. Click **Save**.

Note

The function is only supported by certain models. The actual display varies with models.

2.6.2 Smart Event

Set smart events by the following instructions.

Note

- For certain device models, you need to enable the smart event function on **VCA Resource** page first to show the function configuration page.
- The function varies according to different models.

Detect Audio Exception

Audio exception detection function detects the abnormal sound in the scene, such as the sudden increase/decrease of the sound intensity, and some certain actions can be taken as response.

Steps

1. Go to **Configuration → Event → Smart Event → Audio Exception Detection** .
2. Select one or several audio exception detection types.

   Audio Loss Detection

   Detect sudden loss of audio track.

   Sudden Increase of Sound Intensity Detection

   Detect sudden increase of sound intensity. **Sensitivity** and **Sound Intensity Threshold** are configurable.

   Note

   - The lower the sensitivity is, the more significant the change should be to trigger the detection.
   - The sound intensity threshold refers to the sound intensity reference for the detection. It is recommended to set as the average sound intensity in the environment. The louder the environment sound, the higher the value should be. You can adjust it according to the real environment.

   Sudden Decrease of Sound Intensity Detection

   Detect sudden decrease of sound intensity. **Sensitivity** is configurable.
3. Refer to ***Set Arming Schedule*** for setting scheduled time. Refer to ***Linkage Method Settings*** for setting linkage methods.

4. Click **Save**.

Note

The function is only supported by certain models. The actual function varies according to different models.

Set Defocus Detection

The blurred image caused by lens defocus can be detected. If it occurs, the device can take linkage actions.

Steps

1. Go to **Configuration → Event → Smart Event → Defocus Detection** .
2. Check **Enable**.
3. Set **Sensitivity**. The higher the value is, the more easily the defocus image can trigger the alarm. You can adjust the value according to the actual environment.
4. For the linkage method settings, refer to ***Linkage Method Settings*** .
5. Click **Save**.

Note

The function is only supported by certain models. The actual display varies with models.

Detect Scene Change

Scene change detection function detects the change of the scene. Some certain actions can be taken when the alarm is triggered.

Steps

1. Go to **Configuration → Event → Smart Event → Scene Change Detection** .
2. Click **Enable**.
3. Set the **Sensitivity**. The higher the value is, the more easily the change of scene can be detected. But the detection accuracy is reduced.
4. Refer to ***Set Arming Schedule*** for setting scheduled time. Refer to ***Linkage Method Settings*** for setting linkage method.
5. Click **Save**.

Note

The function varies according to different models.

Set Face Detection

It helps to detect the face in the detection region. If a face is detected, the device triggers the linkage actions.

Steps

1. Go to **Configuration → Event → Smart Event → Face Detection** .
2. Check **Enable Face Detection**.
3. **Optional:** Highlight to display the face in the image.
   1) Check **Enable Dynamic Analysis For Face Detection**.
   2) Go to **Configuration → Local** , set **Rules** to **Enable**.
4. Set **Sensitivity**. The lower the sensitivity is, the profile of the face or unclear face is more difficult to detect.
5. Set the arming schedule and linkage methods. For the information about arming schedule settings, see ***Set Arming Schedule*** . For the information about linkage methods, see ***Linkage Method Settings*** .
6. Click **Save**.

Set Video Loss

This function can detect the video signal loss in time and trigger the linkage action.

Steps

1. Go to **Configuration → Event → Basic Event → Video Loss** .
2. Check **Enable**.
3. Refer to ***Set Arming Schedule*** for setting scheduled time. Refer to ***Linkage Method Settings*** for setting linkage method.
4. Click **Save**.

Set Intrusion Detection

It is used to detect objects entering and loitering in a predefined virtual region. If it occurs, the device can take linkage actions.

Before You Start

- For certain device models, you need to enable the smart event function on VCA Resource page first.
- For the device supporting HEOP, go to **VCA → APP** to import and enable **Smart Event**.

Steps

1. Go to **VCA → Smart Event → Intrusion Detection** . For certain device models, you should go to **Configuration → Event → Smart Event → Intrusion Detection** .
2. Check **Enable**.

3. Select a **Region**. For the detection region settings, refer to ***Draw Area*** .
4. Set the minimum size and the maximum size for the target to improve detection accuracy. Only targets whose size are between the maximum size and the minimum size trigger the detection. For the detail settings, refer to ***Set Size Filter*** .
5. Set rules.

   Sensitivity

   Sensitivity stands for the percentage of the body part of an acceptable target that enters the predefined region. Sensitivity = 100 - S1/ST × 100. S1 stands for the target body part that goes across the predefined region. ST stands for the complete target body. The higher the value of sensitivity is, the more easily the alarm can be triggered.

   Threshold

   Threshold stands for the threshold for the time of the object loitering in the region. If the time that one object stays exceeds the threshold, the alarm is triggered. The larger the value of the threshold is, the longer the alarm triggering time is.

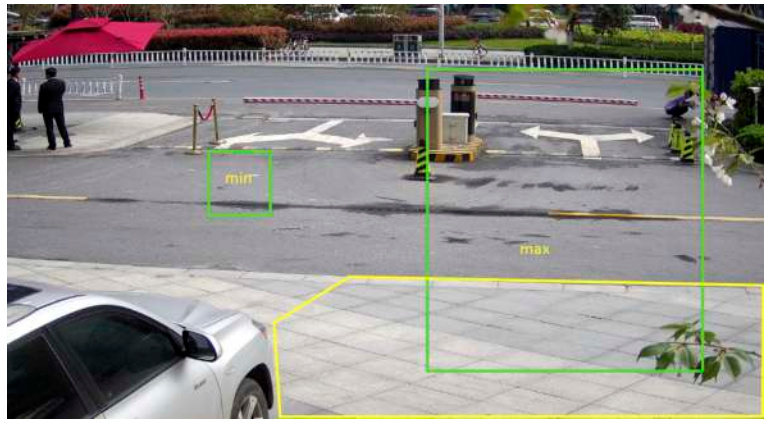


Figure 2-8 Set Rule

6. **Optional:** You can set the parameters of multiple areas by repeating the above steps.
7. For the arming schedule settings, refer to ***Set Arming Schedule*** . For the linkage method settings, refer to ***Linkage Method Settings*** .
8. Click **Save**.

Set Line Crossing Detection

It is used to detect objects crossing a predefined virtual line. If it occurs, the device can take linkage actions.

Before You Start

- For certain device models, you need to enable the smart event function on VCA Resource page first.
- For the device supporting HEOP, go to **VCA → APP** to import and enable **Smart Event**.

Steps

1. Go to **VCA → Smart Event → Line Crossing Detection** . For certain device models, you should go to **Configuration → Event → Smart Event → Line Crossing Detection** .
2. Check **Enable**.
3. Select one **Line** and set the size filter. For the size filter settings, refer to ***Set Size Filter*** .
4. Click **Draw Area** and a line with an arrow appears in the live video. Drag the line to the location on the live video as desired.
5. Set rules.

Direction

It stands for the direction from which the object goes across the line.

A<->B: The object going across the line from both directions can be detected and alarms are triggered.

A->B: Only the object crossing the configured line from the A side to the B side can be detected.

B->A: Only the object crossing the configured line from the B side to the A side can be detected.

Sensitivity

It stands for the percentage of the body part of an acceptable target that goes across the pre-defined line. Sensitivity = 100 - S1/ST × 100. S1 stands for the target body part that goes across the pre-defined line. ST stands for the complete target body. The higher the value of sensitivity is, the more easily the alarm can be triggered.

Detection Target

Human and vehicle are available. If the detection target is not selected, all the detected targets will be reported, including the human and vehicle.

Target Validity

If you set a higher validity, the required target features should be more obvious, and the alarm accuracy would be higher. The target with less obvious features would be missing.

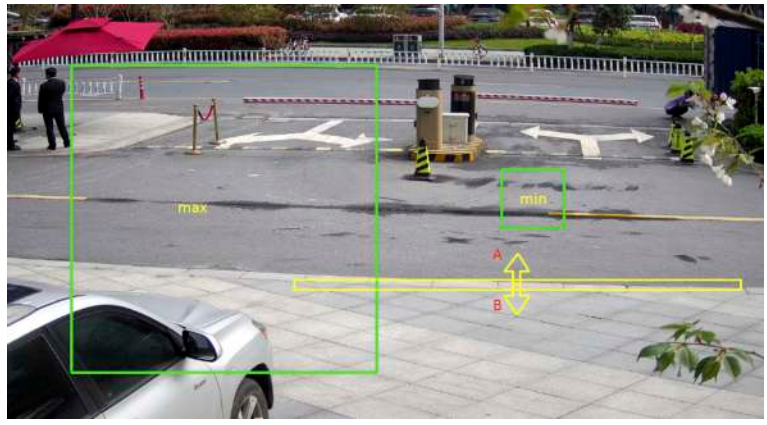


Figure 2-9 Set Rule

6. **Optional:** You can set the parameters of multiple areas by repeating the above steps.
7. For the arming schedule settings, refer to ***Set Arming Schedule*** . For the linkage method settings, refer to ***Linkage Method Settings*** .
8. Click **Save**.

Set Region Entrance Detection

It is used to detect objects entering a predefined virtual region from the outside place. If it occurs, the device can take linkage actions.

Before You Start

- For certain device models, you need to enable the smart event function on VCA Resource page first.
- For the device supporting HEOP, go to **VCA → APP** to import and enable **Smart Event**.

Steps

1. Go to **VCA → Smart Event → Region Entrance Detection** . For certain device models, you should go to **Configuration → Event → Smart Event → Region Entrance Detection** .
2. Check **Enable**.
3. Select a **Region**. For the detection region settings, refer to ***Draw Area*** .
4. Set the minimum size and the maximum size for the target to improve detection accuracy. Only targets whose size are between the maximum size and the minimum size trigger the detection. For the detail settings, refer to ***Set Size Filter*** .
5. Set the detection target, sensitivity and the target validity.

   Sensitivity

   It stands for the percentage of the body part of an acceptable target that goes across the predefined region. Sensitivity = 100 - S1/ST × 100. S1 stands for the target body part that goes across the predefined region. ST stands for the complete target body. The higher the value of sensitivity is, the more easily the alarm can be triggered.

   Detection Target

   Human and vehicle are available. If the detection target is not selected, all the detected targets will be reported, including the human and vehicle.

   Target Validity

   If you set a higher validity, the required target features should be more obvious, and the alarm accuracy would be higher. The target with less obvious features would be missing.

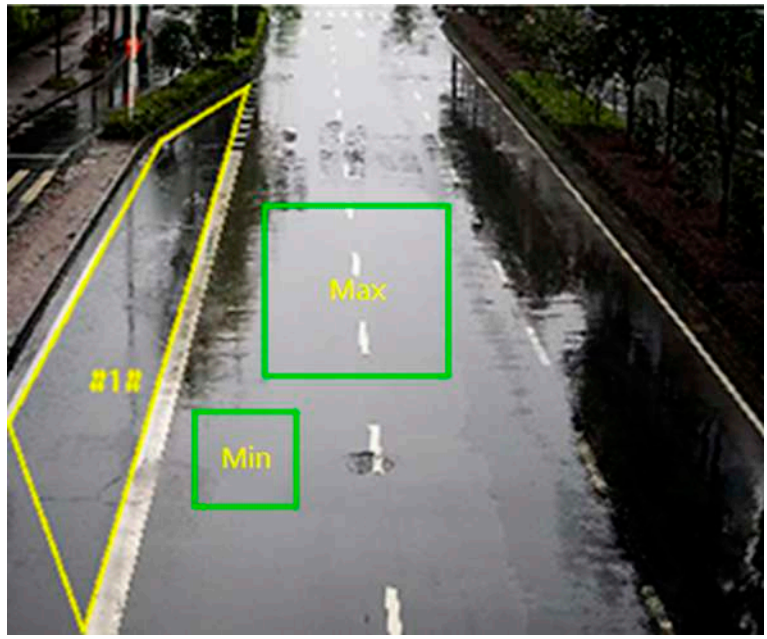


Figure 2-10 Set Rule

6. **Optional:** You can set the parameters of multiple areas by repeating the above steps.
7. For the arming schedule settings, refer to ***Set Arming Schedule*** . For the linkage method settings, refer to ***Linkage Method Settings*** .
8. Click **Save**.

Set Region Exiting Detection

It is used to detect objects exiting from a predefined virtual region. If it occurs, the device can take linkage actions.

Before You Start

- For certain device models, you need to enable the smart event function on VCA Resource page first.
- For the device supporting HEOP, go to **VCA → APP** to import and enable **Smart Event**.

Steps

1. Go to **VCA → Smart Event → Region Exiting Detection** . For certain device models, you should go to **Configuration → Event → Smart Event → Region Exiting Detection** .
2. Check **Enable**.
3. Select a **Region**. For the detection region settings, refer to ***Draw Area*** .
4. Set the minimum size and the maximum size for the target to improve detection accuracy. Only targets whose size are between the maximum size and the minimum size trigger the detection. For the detail settings, refer to ***Set Size Filter*** .
5. Set the detection target, sensitivity and the target validity.

Sensitivity

It stands for the percentage of the body part of an acceptable target that goes across the predefined region. Sensitivity = 100 - S1/ST × 100. S1 stands for the target body part that goes across the predefined region. ST stands for the complete target body. The higher the value of sensitivity is, the more easily the alarm can be triggered.

Detection Target

Human and vehicle are available. If the detection target is not selected, all the detected targets will be reported, including the human and vehicle.

Target Validity

If you set a higher validity, the required target features should be more obvious, and the alarm accuracy would be higher. The target with less obvious features would be missing.

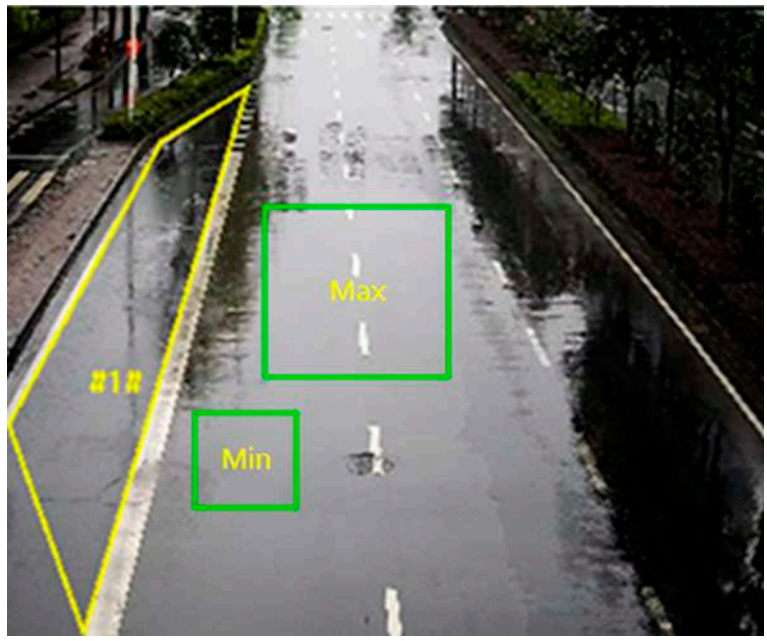


Figure 2-11 Set Rule

6. **Optional:** You can set the parameters of multiple areas by repeating the above steps.
7. For the arming schedule settings, refer to ***Set Arming Schedule*** . For the linkage method settings, refer to ***Linkage Method Settings*** .
8. Click **Save**.

Set Unattended Baggage Detection

It is used to detect the objects left over in the pre-defined region. Linkage methods can be triggered after the object is left and stays in the region for a set time period.

Steps

1. Go to **Configuration → Event → Smart Event → Unattended Baggage Detection** .

2. Check **Enable**.
3. Select one **Region**. For the detection region settings, refer to ***Draw Area*** .
4. Set rules.

Sensitivity Sensitivity stands for the percentage of the body part of an acceptable target that enters the pre-defined region. Sensitivity = 100 - S1/ST × 100. S1 stands for the target body part that goes across the pre-defined region. ST stands for the complete target body. The higher the value of sensitivity is, the more easily the alarm can be triggered.

Threshold It stands for the time of the objects left in the region. Alarm is triggered after the object is left and stays in the region for the set time period.

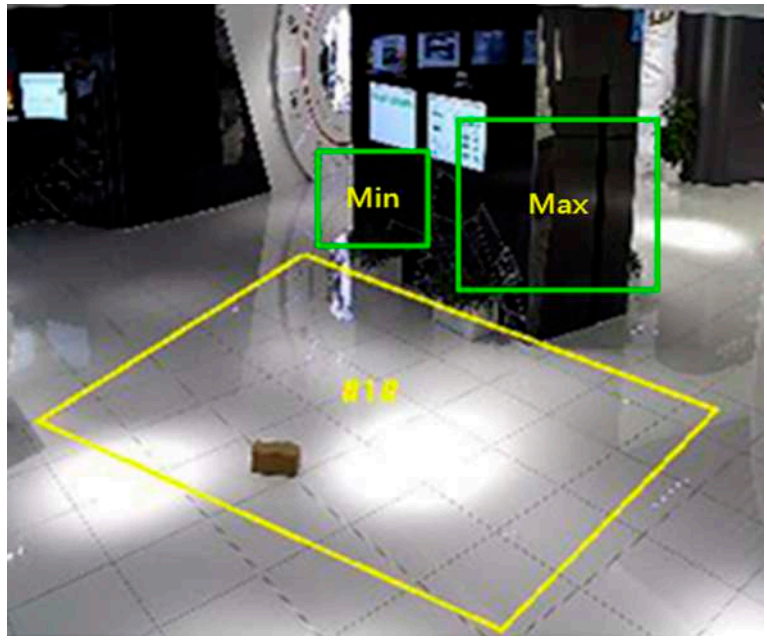


Figure 2-12 Set Rule

5. **Optional:** You can set the parameters of multiple areas by repeating the above steps.
6. For the arming schedule settings, refer to ***Set Arming Schedule*** . For the linkage method settings, refer to ***Linkage Method Settings*** .
7. Click **Save**.

Set Object Removal Detection

It detects whether the objects are removed from the pre-defined detection region, such as the exhibits on display. If it occurs, the device can take linkage actions and the staff can take measures to reduce property loss.

Steps

1. Go to **Configuration → Event → Smart Event → Object Removal Detection** .

2. Check **Enable**.
3. Select a **Region**. For the region settings, see ***Draw Area*** .
4. Set the rule.

Sensitivity It stands for the percentage of the body part of an acceptable target that leaves the pre-defined region.

Sensitivity = 100 – S1/ST*100

S1 stands for the target body part that leaves the pre-defined region. ST stands for the complete target body.

Example: If you set the value as 60, a target is possible to be counted as a removed object only when 40 percent body part of the target leaves the region.

Threshold The threshold for the time of the objects removed from the region. If you set the value as 10, alarm is triggered after the object disappears from the region for 10s.

5. **Optional:** Repeat the above steps to set more regions.
6. For the arming schedule settings, see ***Set Arming Schedule*** . For the linkage method settings, see ***Linkage Method Settings*** .
7. Click **Save**.

Note

The function is only supported by certain models. The actual display varies with the models.

Draw Area

This section introduces the configuration of area.

Steps

1. Click **Detection Area**.
2. Click on the live view to draw the boundaries of the detection region, and right click to complete drawing.
3. Click **Save**.

Note

- Click **Clear** to clear the selected area.
- Click **Clear All** to clear all pre-defined areas.

Set Size Filter

This part introduces the setting of size filter. Only the target whose size is between the minimum value and maximum value is detected and triggers alarm.

Steps

1. Click **Max. Size**, and drag the mouse in the live view to draw the maximum target size.
2. Click **Min. Size**, and drag the mouse in the live view to draw the minimum target size.
3. Click **Save**.

2.7 Network Settings

2.7.1 TCP/IP

TCP/IP settings must be properly configured before you operate the device over network. IPv4 and IPv6 are both supported. Both versions can be configured simultaneously without conflicting to each other.

Go to **Configuration → Network → Basic Settings → TCP/IP** for parameter settings.

NIC Type

Select a NIC (Network Interface Card) type according to your network condition.

IPv4

Two IPv4 modes are available.

DHCP

The device automatically gets the IPv4 parameters from the network if you check **DHCP**. The device IP address is changed after enabling the function. You can use SADP to get the device IP address.

Note

The network that the device is connected to should support DHCP (Dynamic Host Configuration Protocol).

Manual

You can set the device IPv4 parameters manually. Input **IPv4 Address**, **IPv4 Subnet Mask**, and **IPv4 Default Gateway**, and click **Test** to see if the IP address is available.

IPv6

Three IPv6 modes are available.

Route Advertisement

The IPv6 address is generated by combining the route advertisement and the device Mac address.

Note

Route advertisement mode requires the support from the router that the device is connected to.

DHCP

The IPv6 address is assigned by the server, router, or gateway.

Manual

Input **IPv6 Address**, **IPv6 Subnet**, **IPv6 Default Gateway**. Consult the network administrator for required information.

MTU

It stands for maximum transmission unit. It is the size of the largest protocol data unit that can be communicated in a single network layer transaction.

The valid value range of MTU is 1280 to 1500.

DNS

It stands for domain name server. It is required if you need to visit the device with domain name. And it is also required for some applications (e.g., sending email). Set **Preferred DNS Server** and **Alternate DNS server** properly if needed.

Dynamic Domain Name

Check **Enable Dynamic Domain Name** and input **Register Domain Name**. The device is registered under the register domain name for easier management within the local area network.

Note

DHCP should be enabled for the dynamic domain name to take effect.

Multicast

Multicast is group communication where data transmission is addressed to a group of destination devices simultaneously.

Go to **Configuration → Network → Basic Settings → Multicast** for the multicast settings.

IP Address

It stands for the address of multicast host.

Stream Type

The stream type as the multicast source.

Video Port

The video port of the selected stream.

Audio Port

The audio port of the selected stream.

Multicast Discovery

Check the **Enable Multicast Discovery**, and then the online network camera can be automatically detected by client software via private multicast protocol in the LAN.

2.7.2 SNMP

You can set the SNMP network management protocol to get the alarm event and exception messages in network transmission.

Before You Start
Before setting the SNMP, you should download the SNMP software and manage to receive the device information via SNMP port.

Steps
1. Go to the settings page: **Configuration → Network → Advanced Settings → SNMP** .
2. Check **Enable SNMPv1**, **Enable SNMP v2c** or **Enable SNMPv3**.

Note

The SNMP version you select should be the same as that of the SNMP software.
And you also need to use the different version according to the security level required. SNMP v1 is not secure and SNMP v2 requires password for access. And SNMP v3 provides encryption and if you use the third version, HTTPS protocol must be enabled.

3. Configure the SNMP settings.
4. Click **Save**.

2.7.3 Set SRTP

The Secure Real-time Transport Protocol (SRTP) is a Real-time Transport Protocol (RTP) internet protocol, intended to provide encryption, message authentication and integrity, and replay attack protection to the RTP data in both unicast and multicast applications.

Steps
1. Go to **Configuration → Network → Advanced Settings → SRTP** .
2. Select **Server Certificate**.
3. Select **Encrypted Algorithm**.
4. Click **Save**.

Note

- Only certain device models support this function.
- If the function is abnormal, check if the selected certificate is abnormal in certificate management.

2.7.4 Port Mapping

By setting port mapping, you can access devices through the specified port.

Before You Start
When the ports in the device are the same as those of other devices in the network, refer to ***Port*** to modify the device ports.

Steps
1. Go to **Configuration → Network → Basic Settings → NAT** .
2. Select the port mapping mode.

Auto Port Mapping	Refer to ***Set Auto Port Mapping*** for detailed information.
Manual Port Mapping	Refer to ***Set Manual Port Mapping*** for detailed information.

3. Click **Save**.

Set Auto Port Mapping

Steps
1. Check **Enable UPnP™**, and choose a friendly name for the camera, or you can use the default name.
2. Select the port mapping mode to **Auto**.
3. Click **Save**.

Note
UPnP™ function on the router should be enabled at the same time.

Set Manual Port Mapping

Steps
1. Check **Enable UPnP™**, and choose a friendly name for the device, or you can use the default name.
2. Select the port mapping mode to **Manual**, and set the external port to be the same as the internal port.
3. Click **Save**.

What to do next
Go to the router port mapping settings interface and set the port number and IP address to be the same as those on the device. For more information, refer to the router user manual.

Set Port Mapping on Router

The following settings are for a certain router. The settings vary depending on different models of routers.

Steps

1. Select the **WAN Connection Type**.
2. Set the **IP Address**, **Subnet Mask** and other network parameters of the router.
3. Go to **Forwarding → Virtual Severs** , and input the **Port Number** and **IP Address**.
4. Click **Save**.

Example

When the cameras are connected to the same router, you can configure the ports of a camera as 80, 8000, and 554 with IP address 192.168.1.23, and the ports of another camera as 81, 8001, 555, 8201 with IP 192.168.1.24.

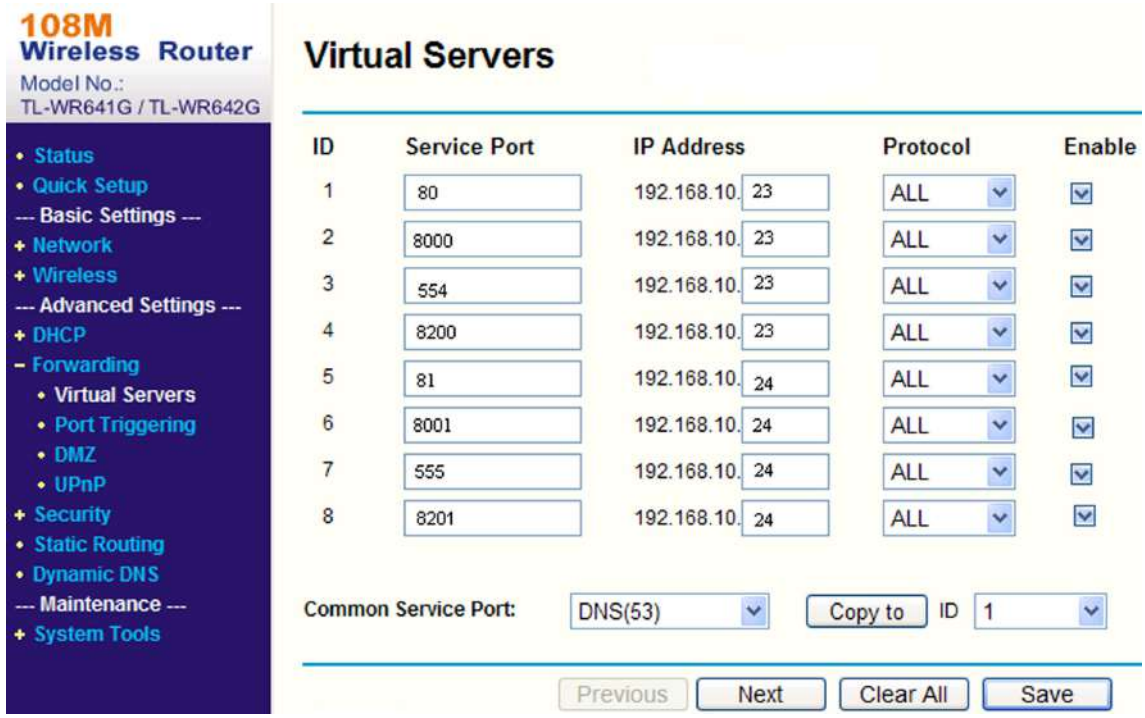


Figure 2-13 Port Mapping on Router

Note

The port of the network camera cannot conflict with other ports. For example, some web management port of the router is 80. Change the camera port if it is the same as the management port.

2.7.5 Port

The device port can be modified when the device cannot access the network due to port conflicts.

Caution

Do not modify the default port parameters at will, otherwise the device may be inaccessible.

Go to **Configuration → Network → Basic Settings → Port** for port settings.

HTTP Port

It refers to the port through which the browser accesses the device. For example, when the **HTTP Port** is modified to 81, you need to enter ***http://192.168.1.64:81*** in the browser for login.

HTTPS Port

It refers to the port through which the browser accesses the device with certificate. Certificate verification is required to ensure the secure access.

RTSP Port

It refers to the port of real-time streaming protocol.

SRTP Port

It refers to the port of secure real-time transport protocol.

Server Port

It refers to the port through which the client adds the device.

Enhanced SDK Service Port

It refers to the port through which the client adds the device. Certificate verification is required to ensure the secure access.

WebSocket Port

TCP-based full-duplex communication protocol port for plug-in free preview.

WebSockets Port

TCP-based full-duplex communication protocol port for plug-in free preview. Certificate verification is required to ensure the secure access.

Note

- Enhanced SDK Service Port, WebSocket Port, and WebSockets Port are only supported by certain models.
- For device models that support that function, go to **Configuration → Network → Advanced Settings → Network Service** to enable it.

2.7.6 Access to Device via Domain Name

You can use the Dynamic DNS (DDNS) for network access. The dynamic IP address of the device can be mapped to a domain name resolution server to realize the network access via domain name.

Before You Start
Registration on the DDNS server is required before configuring the DDNS settings of the device.

Steps
1. Refer to ***TCP/IP*** to set DNS parameters.
2. Go to the DDNS settings page: **Configuration → Network → Basic Settings → DDNS** .
3. Check **Enable DDNS** and select **DDNS type**.

   DynDNS

   Dynamic DNS server is used for domain name resolution.

   NO-IP

   NO-IP server is used for domain name resolution.
4. Input the domain name information, and click **Save**.
5. Check the device ports and complete port mapping. Refer to ***Port*** to check the device port , and refer to ***Port Mapping*** for port mapping settings.
6. Access the device.

By Browsers	Enter the domain name in the browser address bar to access the device.
By Client Software	Add domain name to the client software. Refer to the client manual for specific adding methods.

2.7.7 Access to Device via PPPoE Dial Up Connection

This device supports the PPPoE auto dial-up function. The device gets a public IP address by ADSL dial-up after the device is connected to a modem. You need to configure the PPPoE parameters of the device.

Steps
1. Go to **Configuration → Network → Basic Settings → PPPoE** .
2. Check **Enable PPPoE**.
3. Set the PPPoE parameters.

   Dynamic IP

   After successful dial-up, the dynamic IP address of the WAN is displayed.

   User Name

   User name for dial-up network access.

   Password

   Password for dial-up network access.

Confirm

Input your dial-up password again.

4. Click **Save**.
5. Access the device.

By Browsers	Enter the WAN dynamic IP address in the browser address bar to access the device.
By Client Software	Add the WAN dynamic IP address to the client software. Refer to the client manual for details.

Note

The obtained IP address is dynamically assigned via PPPoE, so the IP address always changes after rebooting the camera. To solve the inconvenience of the dynamic IP, you need to get a domain name from the DDNS provider (e.g. DynDns.com). Refer to ***Access to Device via Domain Name*** for detail information.

2.7.8 Wireless Dial

Data of audio, video and image can be transferred via 3G/4G wireless network.

Note

The function is only supported by certain device models.

Set Wireless Dial

The built-in wireless module offers dial-up access to the Internet for the device.

Before You Start

Get a SIM card, and activate 3G/4G services. Insert the SIM card to the corresponding slot.

Steps

1. Go to **Configuration → Network → Advanced Settings → Wireless Dial** .
2. Check to enable the function.
3. Click **Dial Parameters** to configure and save the parameters.
4. Click **Dial Plan**. See ***Set Arming Schedule*** for detailed information.
5. **Optional:** Set **Allowlist**. See for detailed information.
6. Click **Dial Status**.

Click Refresh	Refresh the dial status.
Click Disconnect	Disconnect the 3G/4G wireless network.

When the **Dial Status** turns to **Connected**, it means a successful dial.

7. Access the device via the **IP Address** of the computer in the network.
   - Input the IP address in the browser to access the device.

- Add the device in client application. Select **IP/Domain**, and input IP address and other parameters to access the device.

2.7.9 Wi-Fi

Connect the device to wireless network by setting Wi-Fi parameters.

Note

This function is only supported by certain device models.

Connect Device to Wi-Fi

Before You Start

Refer to the user manual of wireless router or AP to set SSID, key, and other parameters.

Steps

1. Go to TCP/IP settings page: **Configuration → Network → Basic Configuration → TCP/IP** .
2. Select **Wlan** to set the parameters. Refer to ***TCP/IP*** for detailed configuration.

   Note

   For stable use of Wi-Fi, it is not recommended to use DHCP.
3. Go to Wi-Fi settings page: **Configuration → Network → Advanced Configuration → Wi-Fi** .
4. Set and save the parameters.
   1) Click **Search**.
   2) Select a **SSID**, which should be the same as that of wireless router or AP.

      The parameters of the network is automatically shown in **Wi-Fi**.
   3) Select the **Network Mode** as **Manage**.
   4) Input the key to connect the wireless network. The key should be that of the wireless network connection you set on the router.

What to do next

Go to TCP/IP settings page: **Configuration → Network → Basic Configuration → TCP/IP** , and click **Wlan** to check the **IPv4 Address** and log in the device.

2.7.10 Set Network Service

You can control the ON/OFF status of certain protocol as desired.

Steps

Note

This function varies according to different models.

1. Go to **Configuration → Network → Advanced Settings → Network Service** .
2. Set network service.

WebSocket & WebSockets

WebSocket or WebSockets protocol should be enabled if you use Google Chrome 57 and its above version or Mozilla Firefox 52 and its above version to visit the device. Otherwise, live view, image capture, digital zoom, etc. cannot be used.

If the device uses HTTP, enable WebSocket.

If the device uses HTTPS, enable WebSockets.

When you use WebSockets, select the **Server Certificate**.

Note

Complete certificate management before selecting server certificate. Refer to ***Certificate Management*** for detailed information.

SDK Service & Enhanced SDK Service

Check **Enable SDK Service** to add the device to the client software with SDK protocol.

Check **Enable Enhanced SDK Service** to add the device to the client software with SDK over TLS protocol.

When you use Enhanced SDK Service, select the **Server Certificate**.

Note

- Complete certificate management before selecting server certificate. Refer to ***Certificate Management*** for detailed information.
- When set up connection between the device and the client software, it is recommended to use Enhanced SDK Service and set the communication in Arming Mode to encrypt the data transmission. See the user manual of the client software for the arming mode settings.

TLS (Transport Layer Security)

The device offers TLS1.1, TLS1.2 and TLS1.3. Enable one or more protocol versions according to your need.

Bonjour

Uncheck to disable the protocol.

3. Click **Save**.

2.7.11 Set Open Network Video Interface

If you need to access the device through Open Network Video Interface protocol, you can configure the user settings to enhance the network security.

Steps

1. Go to **Configuration → Network → Advanced Settings → Integration Protocol** .

2. Check **Enable Open Network Video Interface**.
3. Click **Add** to configure the Open Network Video Interface user.

   Delete Delete the selected Open Network Video Interface user.

   Modify Modify the selected Open Network Video Interface user.
4. Click **Save**.
5. **Optional:** Repeat the steps above to add more Open Network Video Interface users.

2.7.12 Set ISUP

When the device is registered on ISUP platform (formerly called Ehome), you can visit and manage the device, transmit data, and forward alarm information over public network.

Steps

1. Go to **Configuration → Network → Advanced Settings → Platform Access** .
2. Select **ISUP** as the platform access mode.
3. Select **Enable**.
4. Select a protocol version and input related parameters.
5. Click **Save**.

   Register status turns to **Online** when the function is correctly set.

2.7.13 Set Alarm Server

The device can send alarms to destination IP address or host name through HTTP, HTTPS, or ISUP protocol. The destination IP address or host name should support HTTP, HTTP, or ISUP data transmission.

Steps

1. Go to **Configuration → Network → Advanced Settings → Alarm Server** .
2. Enter **Destination IP or Host Name**, **URL**, and **Port**.
3. **Optional:** Check **Enable** to enable ANR.
4. Select **Protocol**.

   Note

   HTTP, HTTPS, and ISUP are selectable. It is recommended to use HTTPS, as it encrypts the data transmission during communication.
5. Click **Test** to check if the IP or host is available.
6. Click **Save**.

2.8 Arming Schedule and Alarm Linkage

Arming schedule is a customized time period in which the device performs certain tasks. Alarm linkage is the response to the detected certain incident or target during the scheduled time.

2.8.1 Set Arming Schedule

Set the valid time of the device tasks.

Steps

1. Click **Arming Schedule**.
2. Drag the time bar to draw desired valid time.

   Note

   Up to 8 periods can be configured for one day.
3. Adjust the time period.
   - Click on the selected time period, and enter the desired value. Click **Save**.
   - Click on the selected time period. Drag the both ends to adjust the time period.
   - Click on the selected time period, and drag it on the time bar.
4. **Optional:** Click **Copy to...** to copy the same settings to other days.
5. Click **Save**.

2.8.2 Linkage Method Settings

You can enable the linkage functions when an event or alarm occurs.

Trigger Alarm Output

If the device has been connected to an alarm output device, and the alarm output No. has been configured, the device sends alarm information to the connected alarm output device when an alarm is triggered.

Steps

Note

This function is only supported by certain models.

1. Go to **Configuration → Event → Basic Event → Alarm Output** .
2. Set alarm output parameters.

   Automatic Alarm For the information about the configuration, see ***Automatic Alarm*** .

   Manual Alarm For the information about the configuration, see ***Manual Alarm*** .

3. Click **Save**.

Manual Alarm

You can trigger an alarm output manually.

Steps

1. Set the manual alarm parameters.

   Alarm Output No.

   Select the alarm output No. according to the alarm interface connected to the external alarm device.

   Alarm Name

   Edit a name for the alarm output.

   Delay

   Select **Manual**.

2. Click **Manual Alarm** to enable manual alarm output.
3. **Optional:** Click **Clear Alarm** to disable manual alarm output.

Automatic Alarm

Set the automatic alarm parameters, then the device triggers an alarm output automatically in the set arming schedule.

Steps

1. Set automatic alarm parameters.

   Alarm Output No.

   Select the alarm output No. according to the alarm interface connected to the external alarm device.

   Alarm Name

   Custom a name for the alarm output.

   Delay

   It refers to the time duration that the alarm output remains after an alarm occurs.

2. Set the alarming schedule. For the information about the settings, see ***Set Arming Schedule*** .
3. Click **Copy to...** to copy the parameters to other alarm output channels.
4. Click **Save**.

FTP/NAS/Memory Card Uploading

If you have enabled and configured the FTP/NAS/memory card uploading, the device sends the alarm information to the FTP server, network attached storage and memory card when an alarm is triggered.

Refer to ***Set FTP*** to set the FTP server.

Refer to ***Set NAS*** for NAS configuration.

Refer to ***Set Memory Card*** for memory card storage configuration.

Send Email

Check **Send Email**, and the device sends an email to the designated addresses with alarm information when an alarm event is detected.

For email settings, refer to ***Set Email*** .

Set Email

When the email is configured and **Send Email** is enabled as a linkage method, the device sends an email notification to all designated receivers if an alarm event is detected.

Before You Start

Set the DNS server before using the Email function. Go to **Configuration → Network → Basic Settings → TCP/IP** for DNS settings.

Steps

1. Go to email settings page: **Configuration → Network → Advanced Settings → Email** .
2. Set email parameters.
   1) Input the sender's email information, including the **Sender's Address**, **SMTP Server**, and **SMTP Port**.
   2) **Optional:** If your email server requires authentication, check **Authentication** and input your user name and password to log in to the server.
   3) Set the **E-mail Encryption**.
      - When you select **SSL** or **TLS**, and disable STARTTLS, emails are sent after encrypted by SSL or TLS. The SMTP port should be set as 465.
      - When you select **SSL** or **TLS** and **Enable STARTTLS**, emails are sent after encrypted by STARTTLS, and the SMTP port should be set as 25.

      Note

      If you want to use STARTTLS, make sure that the protocol is supported by your email server. If you check the **Enable STARTTLS** while the protocol is not supported by your email sever, your email is sent with no encryption.

4) **Optional:** If you want to receive notification with alarm pictures, check **Attached Image**. The notification email has 3 attached alarm pictures about the event with configurable image capturing interval.
5) Input the receiver's information, including the receiver's name and address.
6) Click **Test** to see if the function is well configured.

3. Click **Save**.

Notify Surveillance Center

Check **Notify Surveillance Center**, the alarm information is uploaded to the surveillance center when an alarm event is detected.

Trigger Recording

Check **Trigger Recording**, and the device records the video about the detected alarm event.

For recording settings, refer to ***Video Recording and Picture Capture*** .

Flashing Light

After enabling **Flashing Light** and setting the **Flashing Light Alarm Output**, the light flashes when an alarm event is detected.

Set Flashing Alarm Light Output

Steps

1. Go to **Configuration → Event → Basic Event → Flashing Alarm Light Output** .
2. Set **Flashing Duration**, **Flashing Frequency** and **Brightness**.

   Flashing Duration

   The time period the flashing lasts when one alarm happens.

   Flashing Frequency

   The flashing speed of the light. High, Medium, and Low are selectable.

   Brightness

   The brightness of the light.
3. Edit the arming schedule.
4. Click **Save**.

Note

Only certain camera models support the function.

Audible Warning

After enabling **Audible Warning** and setting **Audible Alarm Output**, the built-in speaker of the device or connected external speaker plays warning sounds when an alarm happens.

For audible alarm output settings, refer to ***Set Audible Alarm Output*** .

Note

The function is only supported by certain camera models.

Set Audible Alarm Output

When the device detects targets in the detection area, audible alarm can be triggered as a warning.

Steps

1. Go to **Configuration → Event → Basic Event → Audible Alarm Output** .
2. Select **Sound Type** and set related parameters.
   - Select **Prompt** and set the alarm times you need.
   - Select **Warning** and its contents. Set the alarm times you need.
   - Select **Custom Audio**. You can select a custom audio file from the drop-down list. If no file is available, you can click **Add** to upload an audio file that meets the requirement. Up to three audio files can be uploaded.
3. **Optional:** Click **Test** to play the selected audio file on the device.
4. Set arming schedule for audible alarm. See ***Set Arming Schedule*** for details.
5. Click **Save**.

Note

The function is only supported by certain device models.

2.9 System and Security

It introduces system maintenance, system settings and security management, and explains how to configure relevant parameters.

2.9.1 View Device Information

You can view device information, such as Device No., Model, Serial No. and Firmware Version.

Enter **Configuration → System → System Settings → Basic Information** to view the device information.

2.9.2 Search and Manage Log

Log helps locate and troubleshoot problems.

Steps

1. Go to **Configuration → System → Maintenance → Log** .
2. Set search conditions **Major Type**, **Minor Type**, **Start Time**, and **End Time**.
3. Click **Search**.

   The matched log files will be displayed on the log list.
4. **Optional:** Click **Export** to save the log files in your computer.

2.9.3 Simultaneous Login

The administrator can set the maximum number of users logging into the system through web browser simultaneously.

Go to **Configuration → System → User Management** , click **General** and set **Simultaneous Login**.

2.9.4 Import and Export Configuration File

It helps speed up batch configuration on other devices with the same parameters.

Enter **Configuration → System → Maintenance → Upgrade & Maintenance** . Choose device parameters that need to be imported or exported and follow the instructions on the interface to import or export configuration file.

2.9.5 Export Diagnose Information

Diagnose information includes running log, system information, hardware information.

Go to **Configuration → System → Maintenance → Upgrade & Maintenance** , and click **Diagnose Information** to export diagnose information of the device.

2.9.6 Reboot

You can reboot the device via browser.

Go to **Configuration → System → Maintenance → Upgrade & Maintenance** , and click **Reboot**.

2.9.7 Restore and Default

Restore and Default helps restore the device parameters to the default settings.

Steps

1. Go to **Configuration → System → Maintenance → Upgrade & Maintenance** .
2. Click **Restore** or **Default** according to your needs.

Restore Reset device parameters, except user information, IP parameters and video format to the default settings.

Default Reset all the parameters to the factory default.

Note

Be careful when using this function. After resetting to the factory default, all the parameters are reset to the default settings.

2.9.8 Upgrade

Before You Start

You need to obtain the correct upgrade package.

Caution

DO NOT disconnect power during the process, and the device reboots automatically after upgrade.

Steps

1. Go to **Configuration → System → Maintenance → Upgrade & Maintenance** .
2. Choose one method to upgrade.

Firmware Locate the exact path of the upgrade file.

Firmware Directory Locate the directory which the upgrade file belongs to.

3. Click **Browse** to select the upgrade file.
4. Click **Upgrade**.

2.9.9 Device Auto Maintenance

Steps

1. Check **Enable Auto Maintenance**.
2. Read the prompt information and click **OK**.
3. Select the date and time you want to restart the device.
4. Click **Save**.

Note

This function is only available for Administrator.

Warning

After enabling auto maintenance, the device will automatically restart according to the maintenance plan. The device cannot record video during the restarting process.

2.9.10 View Open Source Software License

Go to **Configuration → System → System Settings → About Device** , and click **View Licenses**.

2.9.11 Wiegand

Note

This function is only supported by certain camera models.

Check **Enable** and select the protocol. The default protocol is SHA-1 26bit.

If enabled, the recognized license plate number will be output via the selected Wiegand protocol.

2.9.12 Metadata

Metadata is the raw data that the camera collects before algorithm processing. It provide the option to users to explore various data usages.

Note

The function is only supported by certain device models.

Go to **Configuration → System → Metadata Settings** to enable metadata uploading of the desired function.

Smart Event

The metadata of the smart event includes the target ID, target coordinate, time, etc.

2.9.13 Time and Date

You can configure time and date of the device by configuring time zone, time synchronization and Daylight Saving Time (DST).

Synchronize Time Manually

Steps

1. Go to **Configuration → System → System Settings → Time Settings** .
2. Select **Time Zone**.

3. Click **Manual Time Sync.**.
4. Choose one time synchronization method.
   - Select **Set Time**, and manually input or select date and time from the pop-up calendar.
   - Check **Sync. with computer time** to synchronize the time of the device with that of the local PC.
5. Click **Save**.

Set NTP Server

You can use NTP server when accurate and reliable time source is required.

Before You Start
Set up a NTP server or obtain NTP server information.

Steps
1. Go to **Configuration → System → System Settings → Time Settings** .
2. Select **Time Zone**.
3. Click **NTP**.
4. Set **Server Address**, **NTP Port** and **Interval**.

Note
Server Address is NTP server IP address.

5. Click **Test** to test server connection.
6. Click **Save**.

Synchronize Time by Satellite

Note
This function varies depending on different devices.

Steps
1. Enter **Configuration → System → System Settings → Time Settings** .
2. Select **Satellite Time Sync.**.
3. Set **Interval**.
4. Click **Save**.

Set DST

If the region where the device is located adopts Daylight Saving Time (DST), you can set this function.

Steps

1. Go to **Configuration → System → System Settings → DST** .
2. Check **Enable DST**.
3. Select **Start Time**, **End Time** and **DST Bias**.
4. Click **Save**.

2.9.14 Set RS-485

RS-485 is used to connect the device to external device. You can use RS-485 to transmit the data between the device and the computer or terminal when the communication distance is too long.

Before You Start

Connect the device and computer or terminal with RS-485 cable.

Steps

1. Go to **Configuration → System → System Settings → RS-485** .
2. Set the RS-485 parameters.

   Note

   You should keep the parameters of the device and the computer or terminal all the same.
3. Click **Save**.

2.9.15 Set RS-232

RS-232 can be used to debug device or access peripheral device. RS-232 can realize communication between the device and computer or terminal when the communication distance is short.

Before You Start

Connect the device to computer or terminal with RS-232 cable.

Steps

1. Go to **Configuration → System → System Settings → RS-232** .
2. Set RS-232 parameters to match the device with computer or terminal.
3. Click **Save**.

2.9.16 Power Consumption Mode

It is used to switch the power consumption when the device is working.

Note

The function is only supported by certain camera models.

Go to **Configuration → Proactive Mode → Power Consumption Mode** , select the desired power consumption mode.

Performance Mode

The device works with all the functions enabled.

Proactive Mode

The device DSP works normally. It records the videos with the main stream at the half frame rate, and supports the remote login, preview and the configuration.

Low Power Sleep

When the device power is lower than **Threshold of Low Power Sleep Mode**, the device enters sleep mode.

When the device power is recovered to 10% above the threshold, the device enters the user configuration mode.

Scheduled Sleep

If the device is during **Scheduled Sleep Time**, it enters the sleep mode, otherwise it enters the user configuration mode.

Note

For the scheduled sleep schedule settings, see ***Set Arming Schedule*** .
The device supports the timing wake. For the details, see ***Set Timing Wake*** .

2.9.17 External Device

For the device supporting external devices, including the supplement light, wiper on the housing, the LED light, and heater, you can control them via the Web browser when it is used with the housing. External devices vary with models.

Supplement Light Settings

You can set supplement light and refer to the actual device for relevant parameters.

Smart Supplement Light

Smart supplement light avoids over exposure when the supplement light is on.

Supplement Light Mode

When the device supports supplement light, you can select supplement light mode.

IR Mode

IR light is enabled.

White Light Mode

White light is enabled.

Mix Mode

Both IR light and white light are enabled.

Off

Supplement light is disabled.

Brightness Adjustment Mode

Auto

The brightness adjusts according to the actual environment automatically.

Manual

You can drag the slider or set value to adjust the brightness.

Heater

You can enable heater to remove fog around the lens of the device.

Go to **Configuration → System → System Settings → External Device** and select the mode as required.

2.9.18 Security

You can improve system security by setting security parameters.

Authentication

You can improve network access security by setting RTSP and WEB authentication.

Go to **Configuration → System → Security → Authentication** to choose authentication protocol and method according to your needs.

RTSP Authentication

Digest and digest/basic are supported, which means authentication information is needed when RTSP request is sent to the device. If you select **digest/basic**, it means the device supports digest or basic authentication. If you select **digest**, the device only supports digest authentication.

RTSP Digest Algorithm

MD5, SHA256 and MD5/SHA256 encrypted algorithm in RTSP authentication. If you enable the digest algorithm except for MD5, the third-party platform might not be able to log in to the device or enable live view because of compatibility. The encrypted algorithm with high strength is recommended.

WEB Authentication

Digest and digest/basic are supported, which means authentication information is needed when WEB request is sent to the device. If you select **digest/basic**, it means the device supports digest or basic authentication. If you select **digest**, the device only supports digest authentication.

WEB Digest Algorithm

MD5, SHA256 and MD5/SHA256 encrypted algorithm in WEB authentication. If you enable the digest algorithm except for MD5, the third-party platform might not be able to log in to the device or enable live view because of compatibility. The encrypted algorithm with high strength is recommended.

Note

Refer to the specific content of protocol to view authentication requirements.

Set IP Address Filter

IP address filter is a tool for access control. You can enable the IP address filter to allow or forbid the visits from the certain IP addresses.

IP address refers to IPv4.

Steps

1. Go to **Configuration → System → Security → IP Address Filter** .
2. Check **Enable IP Address Filter**.
3. Select the type of IP address filter.

   Forbidden IP addresses in the list cannot access the device.

   Allowed Only IP addresses in the list can access the device.
4. Edit the IP address filter list.

   Add Add a new IP address or IP address range to the list.

   Modify Modify the selected IP address or IP address range in the list.

   Delete Delete the selected IP address or IP address range in the list.
5. Click **Save**.

Set HTTPS

HTTPS is a network protocol that enables encrypted transmission and identity authentication, which improves the security of remote access.

Steps

1. Go to **Configuration → Network → Advanced Settings → HTTPS** .
2. Check **Enable** to access the camera via HTTP or HTTPS protocol.
3. Check **Enable HTTPS Browsing** to access the camera only via HTTPS protocol.
4. Select the **Server Certificate**.
5. Click **Save**.

Note

If the function is abnormal, check if the selected certificate is abnormal in **Certificate Management**.

Set QoS

QoS (Quality of Service) can help improve the network delay and network congestion by setting the priority of data sending.

Note

QoS needs support from network device such as router and switch.

Steps

1. Go to **Configuration → Network → Advanced Configuration → QoS** .
2. Set **Video/Audio DSCP**, **Alarm DSCP** and **Management DSCP**.

   Note

   Network can identify the priority of data transmission. The bigger the DSCP value is, the higher the priority is. You need to set the same value in router while configuration.
3. Click **Save**.

Set IEEE 802.1X

IEEE 802.1x is a port-based network access control. It enhances the security level of the LAN/ WLAN. When devices connect to the network with IEEE 802.1x standard, the authentication is needed.

Go to **Configuration → Network → Advanced Settings → 802.1X** , and enable the function.

Set **Protocol** and **EAPOL Version** according to router information.

Protocol

EAP-LEAP, EAP-TLS, and EAP-MD5 are selectable

EAP-LEAP and EAP-MD5

If you use EAP-LEAP or EAP-MD5, the authentication server must be configured. Register a user name and password for 802.1X in the server in advance. Input the user name and password for authentication.

EAP-TLS

If you use EAP-TLS, input Identify, Private Key Password, and upload CA Certificate, User Certificate and Private Key.

EAPOL Version

The EAPOL version must be identical with that of the router or the switch.

Control Timeout Settings

If this function is enabled, you will be logged out when you make no operation (not including viewing live image) to the device via web browser within the set timeout period.

Go to **Configuration → System → Security → Advanced Security** to complete settings.

Search Security Audit Logs

You can search and analyze the security log files of the device so as to find out the illegal intrusion and troubleshoot the security events.

Steps

Note

This function is only supported by certain camera models.

1. Go to **Configuration → System → Maintenance → Security Audit Log** .
2. Select log types, **Start Time**, and **End Time**.
3. Click **Search**.

   The log files that match the search conditions will be displayed on the Log List.
4. **Optional:** Click **Export** to save the log files to your computer.

Security Reinforcement

Security reinforce is a solution to enhance network security. With the function enabled, risky functions, protocols, ports of the device are disabled and more secured alternative functions, protocols and ports are enabled.

Go to **Configuration → System → Security → Advanced Security** . Check **Security Reinforcement**, and click **Save**.

SSH

Secure Shell (SSH) is a cryptographic network protocol for operating network services over an unsecured network.

Go to **Configuration → System → Security → Security Service** , and check **Enable SSH**.

The SSH function is disabled by default.

Caution

Use the function with caution. The security risk of device internal information leakage exists when the function is enabled.

2.9.19 Certificate Management

It helps to manage the server/client certificates and CA certificate, and to send an alarm if the certificates are close to expiry date, or are expired/abnormal.

Note

The function is only supported by certain device models.

Create Self-signed Certificate

Steps

1. Click **Create Self-signed Certificate**.
2. Follow the prompt to enter **Certificate ID**, **Country/Region**, **Hostname/IP**, **Validity** and other parameters.

   Note

   The certificate ID should be digits or letters and be no more than 64 characters.
3. Click **OK**.
4. **Optional:** Click **Export** to export the certificate, or click **Delete** to delete the certificate to recreate a certificate, or click **Certificate Properties** to view the certificate details.

Create Certificate Request

Before You Start

Select a self-signed certificate.

Steps

1. Click **Create Certificate Request**.
2. Enter the related information.
3. Click **OK**.

Import Certificate

Steps

1. Click **Import**.
2. Click **Create Certificate Request**.
3. Enter the **Certificate ID**.
4. Click **Browser** to select the desired server/client certificate.
5. Select the desired import method and enter the required information.
6. Click **OK**.

7. **Optional:** Click **Export** to export the certificate, or click **Delete** to delete the certificate to recreate a certificate, or click **Certificate Properties** to view the certificate details.

Note

- Up to 16 certificates are allowed.
- If certain functions are using the certificate, it cannot be deleted.
- You can view the functions that are using the certificate in the functions column.
- You cannot create a certificate that has the same ID with that of the existing certificate and import a certificate that has the same content with that of the existing certificate.

Install Server/Client Certificate

Steps

1. Go to **Configuration → System → Security → Certificate Management** .
2. Click **Create Self-signed Certificate**, **Create Certificate Request** and **Import** to install server/client certificate.

Create self-signed certificate	Refer to ***Create Self-signed Certificate***
Create certificate request	Refer to ***Create Certificate Request***
Import Certificate	Refer to ***Import Certificate***

Install CA Certificate

Steps

1. Click **Import**.
2. Enter the **Certificate ID**.
3. Click **Browser** to select the desired server/client certificate.
4. Select the desired import method and enter the required information.
5. Click **OK**.

Note

Up to 16 certificates are allowed.

Enable Certificate Expiration Alarm

Steps

1. Check **Enable Certificate Expiration Alarm**. If enabled, you will receive an email or the camera links to the surveillance center that the certificate will expire soon, or is expired or abnormal.
2. Set the **Remind Me Before Expiration (day)**, **Alarm Frequency (day)** and **Detection Time (hour)**.

Note

- If you set the reminding day before expiration to 1, then the camera will remind you the day before the expiration day. 1 to 30 days are available. Seven days is the default reminding days.
- If you set the reminding day before expiration to 1, and the detection time to 10:00, and the certificate will expire in 9:00 the next day, the camera will remind you in 10:00 the first day.

3. Click **Save**.

2.9.20 User and Account

Set User Account and Permission

The administrator can add, modify, or delete other accounts, and grant different permission to different user levels.

Caution

To increase security of using the device on the network, please change the password of your account regularly. Changing the password every 3 months is recommended. If the device is used in high-risk environment, it is recommended that the password should be changed every month or week.

Steps

1. Go to **Configuration → System → User Management → User Management** .
2. Click **Add**. Enter **User Name**, select **Level**, and enter **Password**. Assign remote permission to users based on needs.

   Administrator

   The administrator has the authority to all operations and can add users and operators and assign permission.

   User

   Users can be assigned permission of viewing live video, setting PTZ parameters, and changing their own passwords, but no permission for other operations.

   Operator

   Operators can be assigned all permission except for operations on the administrator and creating accounts.

   Modify Select a user and click **Modify** to change the password and permission.

   Delete Select a user and click **Delete**.

Note

The administrator can add up to 31 user accounts.

3. Click **OK**.

Simultaneous Login

The administrator can set the maximum number of users logging into the system through web browser simultaneously.

Go to **Configuration → System → User Management** , click **General** and set **Simultaneous Login**.

Online Users

The information of users logging into the device is shown.

Go to **Configuration → System → User Management → Online Users** to view the list of online users.

2.10 VCA Resource

VCA resource is a collection of smart functions supported by the device.

2.10.1 Allocate VCA Resource

VCA resource offers you options to enable certain VCA functions according to actual needs. It helps allocate more resources to the desired functions.

Steps

1. Go to **VCA → VCA Resource** . For certain device models, you should go to **Configuration → System → System Settings → VCA Resource** .
2. Select desired VCA functions.
3. Save the settings.

Note

Certain VCA functions are mutually exclusive.

2.10.2 Set Open Platform

HEOP (Hikvision Embedded Open Platform) allows you to install the application for the third-party to develop and run its function and service. For the device supporting HEOP, you can follow the steps to import and run smart applications.

Steps

1. Go to **VCA → APP** .

Note

Before installing the application, make sure that the application you want to install fit the following conditions.

- Each application has its own exclusive name.
- The FLASH memory space that the application takes up is less than the available FLASH memory space of the device.
- The memory and computing power of the application is less than that available memory and computing power of the device.

2. In **Apps**, click **Import Application**.
3. Click **Browse** to select an application package.
4. Click **Import** to import the package. You can click the APP to view relevant details.
5. **Optional:** Set application.

Click	Enable or disable the application.
Click	Delete the application.
Click **Download Logs**	Export log.
Click **Update**	Browse a local path and import an application package to update the application.

Figure 2-14 Set VCA Resource

2.10.3 Road Traffic

Vehicle Detection and Mixed-traffic Detection are available for the road traffic monitoring. The device captures the passing motor vehicles and non-motor vehicles and uploads the relevant information together with the captured pictures.

Note

- For certain device models, you need to select **Road Traffic** on **VCA Resource** page first.
- This function is only supported by certain device models.

Set Vehicle Detection

The vehicles that enter the set lane can be detected and the picture of the vehicle and its license plate can be captured and stored. Alarms will be triggered and captures can be uploaded.

Before You Start
Go to **VCA → VCA Resources** , and select **Road Traffic**.

Steps
1. Go to **VCA → Road Traffic → Detection Configuration** , and select **Vehicle Detection** as detection type.
2. Check **Enable**.
3. Select the total number of lanes.
4. Click and drag the lane line to set its position, or click and drag the line end to adjust the length and angle of the line.
5. Adjust the zoom ratio of the camera so that the size of the vehicle in the image is close to that of the red frame. Only the position of red frame is adjustable.

Note

Only 1 license plate can be captured at one time for each lane.

6. Select **Region** and **Country/Region**.
7. Select the license plate information upload mode.

Entrance/Exit	The license plate information of the detected vehicle will be uploaded when the vehicle passes the detection area and triggers the detection in entrance/exit.
City Street	The license plate information of the detected vehicle will be uploaded when the vehicle passes the detection area and triggers the detection in city streets.
Alarm Input	It means the input alarm will trigger a license plate capture and recognition action.

Note

- When Alarm Input is selected, the alarm input A<-1 will automatically be assigned to trigger vehicle detection and its alarm type is always NO.
- If the A<-1 alarm input is used to trigger vehicle detection, it can not be used for other basic events.
- When Alarm Input is selected and saved, previously configured linkage method for A<-1 will be canceled.

8. Select the **Detection mode**.
9. Check **Remove Duplicated License Plates** ans set the **Time Interval**. The default time interval is 4 minutes.

Note

Up to 8 license plates are supported.

10. Set arming schedule and linkage method. For the arming schedule settings, refer to ***Set Arming Schedule*** . For the linkage method settings, refer to ***Linkage Method Settings*** .
11. Click **Save**.

Set Mixed-Traffic Detection Rule

The motor vehicles and non-motor vehicles that enter the set lane can be detected, and the picture of targets can be captured and stored. Alarms will be triggered and captures can be uploaded.

Before You Start

Go to **VCA → VCA Resources** , and select **Road Traffic**.

Steps

1. Go to **VCA → Road Traffic → Detection Configuration** , and select **Mixed-traffic Detection** as detection type.
2. Check **Enable**.
3. Select the total number of lanes.
4. Click and drag the lane line to set its position, or click and drag the line end to adjust the length and angle of the line.
5. Adjust the zoom ratio of the camera so that the size of the vehicle in the image is close to that of the red frame. Only the position of red frame is adjustable.

Note

Only 1 license plate can be captured at one time for each lane.

6. Select **Region** and **Country/Region**.
7. Check **Remove Duplicated License Plates** ans set **Time Interval**. The default time interval is 4 minutes.

Note

Up to 8 license plates are supported.

8. Set arming schedule and linkage method. For the arming schedule settings, refer to ***Set Arming Schedule*** . For the linkage method settings, refer to ***Linkage Method Settings*** .
9. Click **Save**.

Uploading Pictures Settings

You can set the image parameters of the captured images in vehicle detection and mixed-traffic detection.

Go to **VCA → Road Traffic → Picture** .

Picture Quality

The larger the value is, the clearer the picture is, but larger storage space is also required.

Picture Size

The larger the value is, the larger the storage space is needed. And the level of network transmission requirement is also higher.

License Plate Enhancement

The larger the value is, the clearer the license plate is, but larger storage space is also required.

Check **License Plate Enhancement** and set the level. The default level is 50.

Note

Only certain device models support this function.

Overlay

You can overlay camera, device or vehicle information on the captured image and click ↑ ↓ to adjust the order of overlay texts.

Camera Settings

You can set the parameters of each camera for better management.

Go to **Configuration → Road Traffic → Camera** to set relevant parameters and click **Save**.

Import or Export Blocklist & Allowlist

You can import and export the blocklist and allowlist as desired, and check the list content in this interface.

Steps

1. Click **Browse** to open the PC local directory.
2. Find the blocklist & allowlist file and click to select it. Click **Open** to confirm.

Note

- The file to import should corresponds with the file template that is required by the camera. You are recommended to export an empty blocklist & allowlist file from the camera as the template and fill in the content.
- The file should be in the .xls format and the cell format should be Text.

3. Click **Import** to import the selected file.
4. Click **Export** to open the PC local directory.
5. Select a directory in your PC local directory.
6. Name the file in the file name text filed.
7. Click **Save**.

2.10.4 Face Capture

The device can capture the face that appears in the configured area, and the face information will be uploaded with the captured picture as well.

Note

Face capture is only supported by certain models.

Set Face Capture

The face that appears in the configured area can be captured.

Before You Start

To enable the function, go to **VCA → VCA Resource** and select **Face Capture**.
For the device supporting HEOP, go to **VCA → APP** to import and enable **Face Capture**.

Steps

1. Go to **VCA → Face Capture** .
2. For shield region settings, refer to ***Set Shield Region*** .
3. Select **Rule** and check **Rule** to enable the rule.
4. Input the min. pupil distance in the text field, or click to draw the min. pupil distance.

   Min. Pupil Distance

   The min. pupil distance refers to the minimum area between two pupils, and it is basic for the device to recognize a face.
5. Input the max. pupil distance in the text field, or click to draw the max. pupil distance.
6. Click to draw the detection area you want the face capture to take effect. Draw area by left-clicking end-points in the live view window, and right-clicking to finish the area drawing. It is recommended that the drawn area occupies 1/2 to 2/3 of the live view image.
7. For the arming schedule settings, refer to ***Set Arming Schedule*** . For the linkage method settings, refer to ***Linkage Method Settings*** .
8. Click **Save**.
9. For overlay and capture settings, refer to ***Overlay and Capture*** . For advanced parameters settings, refer to ***Face Capture Algorithms Parameters*** .

Result

You can view and download captured face images in **Picture**. Refer to ***View and Download Picture*** for details.

Overlay and Capture

Choose to configure capture parameters and the information you want to display on stream and picture.

Display VCA info. on Stream

Display smart information on stream, including the target and rules information.

Display Target info. on Alarm Picture

Overlay the alarm picture with target information.

Target Picture Settings

Custom, Head Shot, Half-Body Shot and Full-Body Shot are selectable.

Note

If you select **Custom**, you can customize **width**, **head height** and **body height** as required.

You can check **Fixed Value** to set the picture height.

Background Picture Settings

Comparing to target picture, background picture is the scene image offers extra environmental information. You can set the background picture quality and resolution. If the background image need to be uploaded to surveillance center, check **Background Upload**.

People Counting Overlay

Select flow overlay type.

Select the daily reset time. Click **Manual Reset** if you want to reset right now.

Camera

You can set **Device No.** and **Camera Info.** for the camera, which can be overlaid on captured picture.

Text Overlay

You can check desired items and adjust their order to display on captured pictures by .

The content of **Device No.** and **Camera Info** should be on the same page.

Face Capture Algorithms Parameters

It is used to set and optimize the parameters of the algorithm library for face capture.

Face Capture Version

It lists the version of the algorithms library.

Detection Parameters

Generation Speed

The speed to identify a target. The higher the value, the faster the target will be recognized. Setting the value quite low, and if there was a face in the configured area from the start, this face will not be captured. It can reduce the misinformation of the faces in the wall painting or posters. The default value of 3 is recommended.

Sensitivity

The sensitivity to identify a target. The higher the value is, the easier a face will be recognized, and the higher possibility of misinformation would be. The default value of 3 is recommended.

Capture Parameters

Best Shot

The best shot after target leave the detection area.

Capture Times

It refers to the capture times a face will be captured during its stay in the configured area. The default value is 1.

Capture Threshold

It stands for the quality of face to trigger capture and alarm. Higher value means better quality should be met to trigger capture and alarm.

Quick Shot

You can define quick shot threshold and max. capture interval.

Quick Shot Threshold

It stands for the quality of face to trigger quick shot.

Face Exposure

Check the checkbox to enable the face exposure.

Reference Brightness

The reference brightness of a face in the face exposure mode. If a face is detected, the camera adjusts the face brightness according to the value you set. The higher the value, the brighter the face is.

Minimum Duration

The minimum duration of the camera exposures the face.

Note

If the face exposure is enabled, please make sure the WDR function is disabled, and the manual iris is selected.

Face Filtering Time

It means the time interval between the camera detecting a face and taking a capture action. If the detected face stays in the scene for less than the set filtering time, capture will not be triggered. For example, if the face filtering time is set as 5 seconds, the camera will capture the detected face when the face keeps staying in the scene for 5 seconds.

Note

The face filtering time (longer than 0s) may increase the possibility of the actual capture times less than the set value above.

Restore Default

Click **Restore** to restore all the settings in advanced configuration to the factory default.

Set Shield Region

The shield region allows you to set the specific region in which the set smart function rule is invalid.

Steps

1. Select **Shield Region**.
2. Click to draw shield area. Repeat this step above to set more shield regions.
3. **Optional:** Click to delete the drawn areas.
4. Click **Save**.

2.11 Smart Display

This function displays real time pictures captured by smart functions and analyzes the target in real time.

Note

The function is only supported when certain smart functions are enabled.

Live View Parameter

Icon	Function
	Capture a picture.
	Start or stop recording.
	Adjust the volume of live view. Move the slider to right to turn up the volume and left to turn down the volume. Move to the left end to mute the live view.

Download Display Pictures

Click and the device stores captured pictures to the browser cache. Hover the pointer over the icon to see the number of pictures in the cache. Click again to download the pictures in a package.

Note

The browser cache has a limited size. The recommended number of pictures to download is no more than 200.

Layout

Click and choose **Layout**. Check the display content you need to add it to the smart display page. When real-time analyze is selected, you can choose the contents you want to display.

Detect Feature

Click and choose **Detect Feature**. Check the corresponding checkbox to display the features of the detection target.

2.12 EPTZ

EPTZ (Electronic PTZ) is a high-resolution function that digitally zooms and pans into portions of the image, with no physical camera movement. If you want to use the EPTZ function, make sure you have select the **Fourth Stream** in the live view. Fourth stream and EPTZ should be both enabled simultaneously.

Note

The function is only supported by certain device models.

2.12.1 Patrol

Steps

1. Go to **Configuration → EPTZ** .
2. Check **Enable EPTZ**.
3. Check **Fourth Stream**.
4. Select **Patrol** in **Application**.
5. Click **Save**.

What to do next

For the detailed information about the patrol settings, see the PTZ operations on live view page.

2.12.2 Auto-Tracking

Steps

1. Go to **Configuration → EPTZ** .
2. Check **Enable EPTZ**.
3. Check **Fourth Stream**.
4. Select **Auto-tracking** in **Application**.
5. Click **Detection Area** to start drawing.
6. Click on the live video to specify the four vertexes of the detection area, and right click to complete drawing.
7. Set rules.

Detection Target	Human and vehicle are available. If the detection target is not selected, all the detected targets will be tracked, including the human and vehicle.
	Note Only certain camera models support this function.
Sensitivity	It stands for the percentage of the body part of an acceptable target that is tracked. Sensitivity = 100 - S1/ST × 100. S1 stands for the target body part that enters the pre-defined area. ST stands for the complete target body. The higher the value of sensitivity is, the more easily the target can be tracked.

8. Click **Save**.

2.13 Image Stitching

You can switch the video output mode for the camera according to your actual demand.

Steps

Note

- The function is only supported by certain device models.
- The actual video output mode varies according to different models. The actual model prevails.

1. Go to **Configuration → System → System Settings → Image Stitching** .
2. Select the desired video output mode.

Panorama + ePTZ	One stitched panoramic image (8 MP) and multiple channels ePTZ images. Channel 01 is the 8 MP panoramic image, and channel 02 and the subsequent channels are ePTZ images. You can set the number of the channels for the ePTZ image. Ten channels are available. For example, if you set the number of the ePTZ channels as 6, then the live view is seven channels: one 8 MP panoramic image and six ePTZ images.

Panorama	One stitched panoramic image (32 MP) and the panoramic image output from 1 or 3 encoder track.
Original	Four independent original images (8 MP). Take the pendent mounting as an example, when facing the camera lens, the channel order is 01 ~ 04 from right to left.
Divided Panorama	The stitched 32 MP panoramic image is divided into four 8 MP images.
Encoder Track	Stream can be divided into several tracks in order to make up for the deficiency of decoder. 1 track and 3 tracks are selectable, and it is recommended to select 3, when the decoder is in poor performance.

Note

- The ePTZ channels support patrol function. You can click on the live view image to enable or disable the patrol function for ePTZ channels.
- You can set the image settings for each channel in the original mode.
- Only the main stream of 24 MP and 16 MP panorama camera support the encoder track.

3. Enter the best stitching distance.

Best Stitching Distance

The distance between the lens and the stitching surface you set for the best stitching image quality. The further the distance is, the worse the stitching image quality is.

Example

For example, if you set the best stitching distance to 30 meters, the stitching image of 30 meters far from the lens is the best quality. The stitching image of 20 or 40 meters far from the lens is not good and the image of 10 or 50 meters far from the lens is the worst.

4. Click **Save**.

Note

For **Original** mode, **Best Stitching Distance** are not supported.

Appendix A. FAQ

Scan the following QR code to find the frequently asked questions of the device.

Note that some frequently asked questions only apply to certain models.

Appendix B. Device Command

Scan the following QR code to get device common serial port commands.

Note that the command list contains the commonly used serial port commands for all Hikvision network cameras.

Appendix C. Device Communication Matrix

Scan the following QR code to get device communication matrix.

Note that the matrix contains all communication ports of Hikvision network cameras.


See Far, Go Further