



HIKVISION

Cameră termometrică de rețea, de tip bullet

Manual de utilizare

UD02330B

Manual de utilizare

COPYRIGHT ©2016 Hangzhou Hikvision Digital Technology Co., Ltd.

TOATE DREPTURILE REZERVATE.

Toate informațiile, inclusiv, printre altele, formulările, imaginile, graficele sunt proprietatea Hangzhou Hikvision Digital Technology Co., Ltd. sau a filialelor acesteia (denumite în continuare „Hikvision”). Acest manual de utilizare (denumit în continuare „Manualul”) nu poate fi reprodus, modificat, tradus sau distribuit, parțial sau în întregime, prin niciun fel de mijloc, fără permisiunea prealabilă scrisă a Hikvision. Dacă nu este stipulat contrariul, Hikvision nu face nicio asigurare, garanție sau declarație, expresă sau implicită, cu privire la manual.

Despre acest manual

Acest Manual este valabil pentru camera termometrică de rețea, de tip bullet (V5.3.7). Manualul include instrucțiunile pentru utilizarea și gestionarea produsului. Fotografiile, graficele și imaginile, precum și celelalte informații expuse în continuare sunt prezente exclusiv în scop descriptiv și explicativ. Informațiile din Manual pot fi modificate fără notificare, ca urmare a actualizărilor de firmware sau din alte motive. Vă rugăm să consultați cea mai recentă versiune pe site-ul web al firmei (<http://overseas.hikvision.com/en/>).

Vă rugăm să folosiți acest manual de utilizare sub îndrumarea unor profesioniști.

Informațiile despre mărcile comerciale

HIKVISION și alte mărci comerciale și sigle ale Hikvision reprezintă proprietatea Hikvision în diferite jurisdicții. Alte mărci comerciale și sigle menționate mai jos reprezintă proprietatea respectivilor deținători.

Declinarea răspunderii legale

ÎN MĂSURA MAXIMĂ PERMISĂ DE LEGISLAȚIA APLICABILĂ, PRODUSUL DESCRIS, ÎMPREUNĂ CU COMPONENTELE HARDWARE, SOFTWARE ȘI FIRMWARE ALE ACESTUIA, ESTE FURNIZAT „AȘA CUM ESTE”, CU TOATE DEFECTELE ȘI ERORILE, IAR HIKVISION NU GARANTEAZĂ NICI ÎN MOD EXPRES, NICI SUBÎNȚELES, INCLUSIV, DAR FĂRĂ A SE LIMITA LA, VANDABILITATEA, CALITATEA SATISFĂCĂTOARE, ADECVAREA PENTRU UN ANUMIT SCOP ȘI NEATINGEREA TERȚILOR. ÎN NICIO SITUAȚIE HIKVISION, DIRECTORII, FUNCȚIONARII, ANGAJAȚII SAU AGENȚII SĂI NU VOR RĂSPUNDE PENTRU NICIUN FEL DE DAUNE CONSECUTIVE, ACCIDENTALE SAU INDIRECTE, INCLUSIV, PRINTRE ALTELE, DAUNE PENTRU PIERDEREA PROFITULUI ACTIVITĂȚII, ÎNTRERUPEREA ACTIVITĂȚII, SAU PIERDEREA DE DATE SAU DOCUMENTE ÎN LEGĂTURĂ CU UTILIZAREA ACESTUI PRODUS, CHIAR DACĂ HIKVISION A FOST AVERTIZAT DE POSIBILITATEA UNOR ASTFEL DE DAUNE.

ÎN CEEA CE PRIVEȘTE PRODUSUL CU ACCES LA INTERNET, UTILIZAREA PRODUSULUI SE VA FACE ÎN ÎNTREGIME DOAR PE RISC PROPRIU. HIKVISION NU ÎȘI VA ASUMA RESPONSABILITATEA PENTRU FUNCȚIONAREA NECORESPUNZĂTOARE, SCURGERILE DE INFORMAȚII CONFIDENȚIALE SAU ALTE DAUNE CARE POT REZULTA DIN ATACURILE CIBERNETICE, ATACURILE HACKERILOR, INFECTAREA CU VIRUȘI SAU ALTE RISCURI DE SECURITATE PE INTERNET; CU TOATE ACESTE, HIKVISION VA OFERI ASISTENȚĂ TEHNICĂ OPORTUNĂ DACĂ ESTE NECESAR.

LEGISLAȚIA PRIVIND SUPRAVEGHEREA POATE VARIA ÎN FUNCȚIE DE JURISDICȚIE. VĂ RUGĂM SĂ VERIFICAȚI TOATE LEGILE RELEVANTE DIN JURISDICȚIA DVS. ÎNAINTE DE A UTILIZA ACEST PRODUS PENTRU A ASIGURA CĂ UTILIZAREA RESPECTĂ LEGEA APLICABILĂ. HIKVISION NU VA FI RĂSPUNZĂTOR ÎN EVENTUALITATEA ÎN CARE ACEST PRODUS ESTE UTILIZAT ÎN SCOPURI NELEGITIME.

ÎN EVENTUALITATEA UNUI CONFLICT ÎNTRE ACEST MANUAL ȘI LEGISLAȚIA APLICABILĂ, VA AVEA PRIORITATE ULTIMA DINTRE ACESTE.

Informații de reglementare

Informații FCC

Conformitatea FCC: Acest echipament a fost testat și s-a stabilit că se încadrează în limitele pentru dispozitive digitale conforme cu partea 15 a Regulamentului FCC. Aceste limite sunt concepute pentru a oferi o protecție rezonabilă împotriva interferenței dăunătoare atunci când echipamentul este operat în medii comerciale. Acest echipament generează, utilizează și poate radia energie pe frecvență radio și, dacă nu este instalat și utilizat în conformitate cu manualul de instrucțiuni, poate cauza interferențe dăunătoare comunicațiilor radio. Operarea acestui echipament într-o zonă rezidențială poate cauza interferențe dăunătoare, caz în care utilizatorul va trebui să corecteze interferența pe propria sa cheltuială.

Condiții FCC

Acest dispozitiv respectă partea 15 a Reglementărilor FCC. Funcționarea este supusă următoarelor două condiții:

1. Acest dispozitiv nu trebuie să cauzeze interferențe dăunătoare.
2. Acest dispozitiv trebuie să accepte orice interferențe primite, inclusiv interferențele care pot provoca o funcționare nedorită.

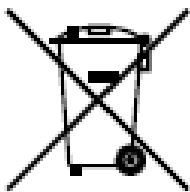
Declarația de conformitate UE



Acest produs și – dacă este cazul – accesoriile furnizate sunt însemnate cu marcajul „CE” și, prin urmare, respectă standardele europene armonizate aplicabile, enumerate în Directiva CEM 2014/30/UE și Directiva RoHS 2011/65/UE.



2012/19/UE (directiva DEEE): Produsele marcate cu acest simbol nu pot fi eliminate ca deșeu municipal nesortat în Uniunea Europeană. Pentru o reciclare adecvată, returnați acest produs furnizorului dvs. local la achiziționarea unui nou echipament echivalent sau eliminați-l în punctele de colectare indicate. Pentru mai multe informații, consultați: www.recyclethis.info.



2006/66/CE (directiva privind bateriile și acumulatorii): Acest produs conține o baterie care nu poate fi eliminată ca deșeu municipal nesortat în Uniunea Europeană. Consultați documentația produsului pentru informații specifice cu privire la baterie. Bateria este marcată cu acest simbol, care poate include litere pentru a indica substanțele cadmiu (Cd), plumb (Pb) sau mercur (Hg). Pentru o reciclare adecvată, returnați bateria furnizorului dvs. sau la un punct de colectare adecvat. Pentru mai multe informații, a se vedea: www.recyclethis.info.

Conformitate Industry Canada ICES-003

Acest dispozitiv respectă cerințele standardului CAN ICES-3 (A)/NMB-3(A).

Instrucțiuni de siguranță

Aceste instrucțiuni au fost concepute pentru a se asigura că utilizatorul poate folosi corect produsul, în scopul evitării pericolelor și a pagubelor materiale.

Măsurile de precauție sunt împărțite în „Avertismente” și „Atenționări”:

Avertismente: În cazul în care avertismentele sunt neglijate, pot surveni leziuni grave sau moartea.

Atenționări: În cazul în care atenționările sunt neglijate, pot surveni leziuni sau deteriorarea echipamentului.

	
Avertismente Urmați aceste măsuri preventive pentru a preveni rănirea gravă sau moartea.	Atenționări Urmați aceste precauții pentru a preveni potențiala rănire sau pagubele materiale.



Avertismente:

- Achiziționați un adaptor de alimentare, care poate îndeplini standardul SELV (tensiune de siguranță foarte joasă). Și sursa cu 12 V c.c. sau 24 V c.a. (în funcție de modele) conform IEC60950-1 și standardului Sursă de energie limitată.
- Pentru a reduce riscul de incendiu sau șoc electric, nu expuneți acest produs la ploaie sau umiditate.

- Această instalare trebuie să fie făcută de către o persoană autorizată și trebuie să se conformeze tuturor codurilor locale.
- Instalați echipament de protecție în caz de pene de curent în circuitul de alimentare cu energie pentru întreruperea fără probleme a alimentării.
- Asigurați-vă că plafonul poate susține mai mult de 50 newtoni (N) când camera se fixează de tavan.
- Dacă produsul nu funcționează corespunzător, vă rugăm să contactați distribuitorul sau cel mai apropiat centru de service. Nu încercați niciodată să demontați singuri camera. (Nu ne asumăm responsabilitatea pentru problemele cauzate de lucrările de reparații sau întreținere neautorizate).



Atenționări:

- Asigurați-vă că tensiunea sursei de alimentare este corectă, înainte de a utiliza camera.
- Nu scăpați camera și nu o supuneți șocurilor fizice.
- Nu atingeți modulele senzorului cu degetele. Dacă este necesară curățarea, utilizați o lavetă curată cu un pic de etanol și ștergeți ușor. În cazul în care camera nu va fi utilizată o perioadă mai lungă, înlocuiți capacul obiectivului pentru a proteja senzorul de murdărie.
- Nu îndreptați obiectivul camerei spre o lumină puternică, cum ar fi soarele sau o lampă incandescentă. Lumina puternică poate provoca distrugerea camerei.
- Senzorul poate fi ars de către un fascicul laser, de aceea, atunci când echipamentul laser este în uz, asigurați-vă că suprafața senzorului nu va fi expusă la fasciculul laser.
- Nu amplasați camera în medii cu temperaturi extrem de ridicate sau de scăzute (temperatura de funcționare trebuie să fie între -40 °C și +65 °C) sau în medii prăfoase ori umede și nu o expuneți la radiații electromagnetice puternice.
- Pentru a evita acumularea căldurii, este necesară o ventilare corespunzătoare a mediului de lucru.
- Țineți camera departe de apă și de orice alt lichid.
- În timpul livrării, camera trebuie să fie împachetată în ambalajul său original.
- Utilizarea necorespunzătoare sau înlocuirea bateriei poate genera pericol de explozie. Vă rugăm să folosiți tipul de baterie recomandat de producător.

Note:

Pentru camerele care acceptă IR, acordați atenție următoarelor precauții pentru a preveni reflexia IR:

- Praful sau grăsimea de pe carcasa cupolei va provoca reflexia IR. Nu îndepărtați pelicula de pe carcasa cupolei până când nu este finalizată instalarea. Dacă există praf sau grăsime pe carcasa cupolei, curățați-o cu o lavetă moale curată și alcool izopropilic.
- Asigurați-vă că locul instalării nu are suprafețe reflectorizante prea aproape de cameră. Lumina IR provenită de la cameră poate fi reflectată înapoi în obiectiv, cauzând reflexia.
- Inelul de spumă din jurul obiectivului trebuie să fie sprijinit complet pe suprafața interioară a bulei, pentru a izola obiectivul de LED-urile IR. Fixați carcasa cupolei de corpul camerei, astfel încât inelul de spumă și carcasa cupolei să fie prinse perfect una de alta.

Cuprins

Capitolul 1	<i>Cerințe de sistem</i>	11
Capitolul 2	<i>Conexiune rețea</i>	12
2.1	Setarea camerei de rețea prin LAN	12
2.1.1	Cablarea în LAN	12
2.1.2	Activarea camerei	13
2.2	Setarea camerei de rețea prin WAN	19
2.2.1	Conexiune cu IP static	19
2.2.2	Conexiune cu IP dinamic	20
Capitolul 3	<i>Accesul la camera de rețea</i>	23
3.1	Accesare prin browser web	23
3.2	Accesarea prin software-ul client	25
Capitolul 4	<i>Vizualizare live</i>	27
4.1	Pagina Vizualizare live	27
4.2	Inițializare Vizualizare live	28
4.3	Înregistrarea și capturarea manuală a imaginilor	29
Capitolul 5	<i>Configurarea camerei de rețea</i>	30
5.1	Configurare parametrilor locali	30
5.2	Configurarea setărilor de timp	33
5.3	Configurare Setări rețea	35
5.3.1	Configurare Setări TCP/IP	35
5.3.2	Configurare Setări Port	36
5.3.3	Configurare setări PPPoE	37
5.3.4	Configurare setări DDNS	38
5.3.5	Configurare Setări SNMP	41
5.3.6	Configurare setări 802.1X	44
5.3.7	Configurare Setări QoS	45
5.3.8	Configurarea setărilor UPnP™	46
5.3.9	Trimiterea de e-mailuri declanșată de o alarmă	46
5.3.10	Configurare Setări NAT (Network Address Translation)	48
5.3.11	Configurare setări FTP	49
5.3.12	Setări HTTPS	50
5.4	Configurare setări video și audio	53
5.4.1	Configurare setări video	53
5.4.2	Configurare Setări audio	55
5.4.3	Configurarea codificării ROI	56
5.5	Configurare parametri imagine	57

5.5.1	Configurare Setări de afișare.....	57
5.5.2	Configurarea setărilor OSD.....	60
5.5.3	Configurare Setări suprapunere text.....	61
5.5.4	Configurarea măștii de confidențialitate	62
5.5.5	Configurarea suprapunerii de imagine	63
5.5.6	Configurarea DPC (corecția pixelilor defecti)	64
5.6	Configurarea și tratarea evenimentelor de alarmă	65
5.6.1	Configurare Detecție mișcare.....	66
5.6.2	Configurare Alarmă corupere video	71
5.6.3	Configurare Intrare alarmă.....	72
5.6.4	Configurare ieșire alarmă.....	73
5.6.5	Gestionare excepție	74
5.6.6	Configurarea detectării excepțiilor audio	75
5.6.7	Detectarea schimbării scenei.....	76
5.6.8	Configurarea detectării dinamice a sursei incendiului	77
5.7	Măsurarea temperaturii	78
5.7.1	Configurarea măsurării temperaturii.....	78
5.7.2	Măsurarea temperaturii și alarma.....	79
5.8	Configurare VCA	81
5.8.1	Tipul de resursă VCA.....	81
5.8.2	Informațiile VCA	82
5.8.3	Analiza comportamentului	83
Capitolul 6	Configurări stocare.....	92
6.1	Gestionarea stocării.....	92
6.2	Configurarea setărilor NAS.....	92
6.3	Configurarea programului de înregistrare	95
6.4	Configurarea setărilor instantaneului	100
Capitolul 7	Redare.....	102
Capitolul 8	Căutare jurnal.....	105
Capitolul 9	Altele.....	106
9.1	Gestionarea conturilor de utilizator	106
9.2	Autentificare	108
9.3	Vizita anonimă	109
9.4	Filtru adresă IP.....	110
9.5	Serviciu de securitate	112
9.6	Vizualizarea informațiilor despre dispozitiv	112
9.7	Întreținere	113

9.7.1	Reinițializarea camerei.....	113
9.7.2	Restabilirea setărilor implicite	114
9.7.3	Exportarea/Importarea fișierului de configurare	114
9.7.4	Actualizare sistem.....	115
9.8	Setările RS-485	116
9.9	Setările serviciilor.....	116
Anexă.....		118
Anexa 1	Introducere software SADP.....	118
Anexa 2	Maparea portului	121

Capitolul 1 Cerințe de sistem

Sistem de operare: Microsoft Windows XP SP1 sau o versiune mai recentă / Vista / Win7 / Server 2003 / Server 2008 pe 32 biți

UCP: Intel Pentium IV de 3,0 GHz sau mai puternic

RAM: 1 GB sau mai mult

Afișaj: Rezoluție 1024×768 sau mai mare

Browser web: Internet Explorer 6.0 și versiuni mai noi, Apple Safari 5.02 și versiuni mai noi, Mozilla Firefox 3.5 și versiuni mai noi și Google Chrome 8 și versiuni mai noi.

Capitolul 2 Conexiune rețea

Notă:

- Trebuie să rețineți că utilizarea produsului cu acces la internet poate cauza riscuri de securitate în rețea. Îmbunătățiți sistemul de securitate pentru a evita atacurile în rețea și pierderile de informații. Dacă produsul nu funcționează corespunzător, contactați furnizorul sau cel mai apropiat centru de service.
- Pentru a asigura securitatea rețelei camerei de rețea, vă recomandăm să verificați și să întrețineți camera periodic. Ne puteți contacta dacă aveți nevoie de un astfel de serviciu.

Înainte de a începe:

- Dacă doriți să setați camera de rețea printr-o LAN (Local Area Network, rețea locală), consultați *Secțiunea 2.1 Setarea camerei de rețea prin LAN*.
- Dacă doriți să setați camera de rețea printr-o WAN (Wide Area Network, rețea extinsă), consultați *Secțiunea 2.2 Setarea camerei de rețea prin WAN*.

2.1 Setarea camerei de rețea prin LAN

Scopul:

Pentru a vizualiza și a configura camera prin intermediul unei rețele LAN, trebuie să conectați camera de rețea în aceeași subrețea cu computerul dvs și să instalați SADP sau software-ul iVMS-4200 pentru a căuta și a schimba IP-ul camerei de rețea.

Notă: Pentru detalii privind SADP, consultați Anexa 1.

2.1.1 Cablarea în LAN

Următoarele figuri arată cele două moduri de conectare a cablului unei camere de rețea și a unui computer:

Scopul:

- Pentru a testa camera de rețea, puteți conecta direct camera de rețea la computer cu un cablu de rețea, după cum s-a arătat în figura Figura 2-1.

- Consultați Figura 2–2 pentru a seta camera de rețea prin LAN cu ajutorul unui switch sau al unui router.

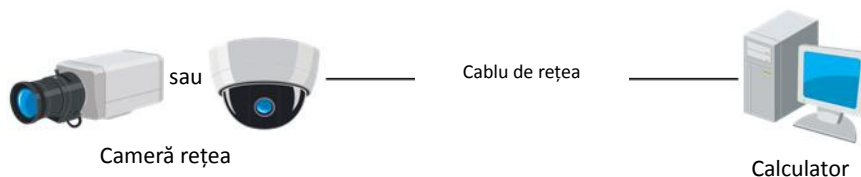


Figura 2–1 Conectarea directă

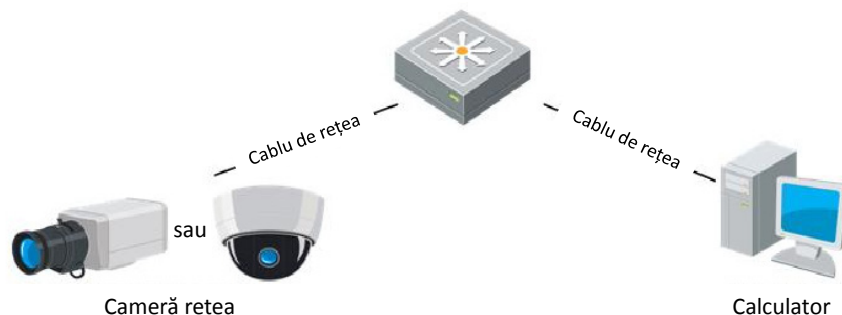


Figura 2–2 Conectarea prin switch sau router

2.1.2 Activarea camerei

Mai întâi trebuie să activați camera, prin stabilirea unei parole puternice, înainte de a putea folosi camera.

Activarea prin browserul web, activarea prin SADP și activarea printr-un software client sunt toate acceptate.

❖ Activarea prin browser web

Pași:

1. Porniți camera și conectați-o la rețea.
2. Introduceți adresa IP în bara de adrese a browserului web și apăsați Enter pentru a accesa interfața de activare.

Note:

- Adresa IP implicită a camerei este 192.168.1.64.
- Pentru ca o cameră să activeze DHCP (protocolul de configurare dinamică a gazdei) în mod implicit, trebuie să activați camera prin software-ul SADP. Consultați următorul capitol pentru activarea prin SADP.

Figura 2–3 Interfața de activare (web)

3. Creați o parolă și introduceți-o în câmpul pentru parolă.



SE RECOMANDĂ O PAROLĂ PUTERNICĂ – Vă recomandăm să creați o parolă puternică la alegerea dvs. (folosind minimum 8 caractere, printre care majuscule, minuscule, cifre și caractere speciale) pentru a crește siguranța produsului dvs. De asemenea, vă recomandăm resetarea parolei cu regularitate, în special în sistemul cu securitate sporită, resetarea lunară sau săptămânală a parolei vă poate proteja produsul mai bine.

4. Confirmați parola.
5. Faceți clic pe OK pentru a salva parola și a intra în interfața de vizualizare live.

❖ **Activarea via software-ul SADP**

Software-ul SADP este folosit pentru detectarea dispozitivului online, activarea camerei și resetarea parolei.

Obțineți software-ul SADP de pe discul inclus sau de pe site-ul web oficial și instalați SADP conform indicațiilor afișate. Urmăți pașii pentru a activa camera.

Pași:

1. Rulați software-ul SADP pentru a căuta dispozitivele online.
2. Verificați starea dispozitivului din lista de dispozitive și selectați dispozitivul inactiv.

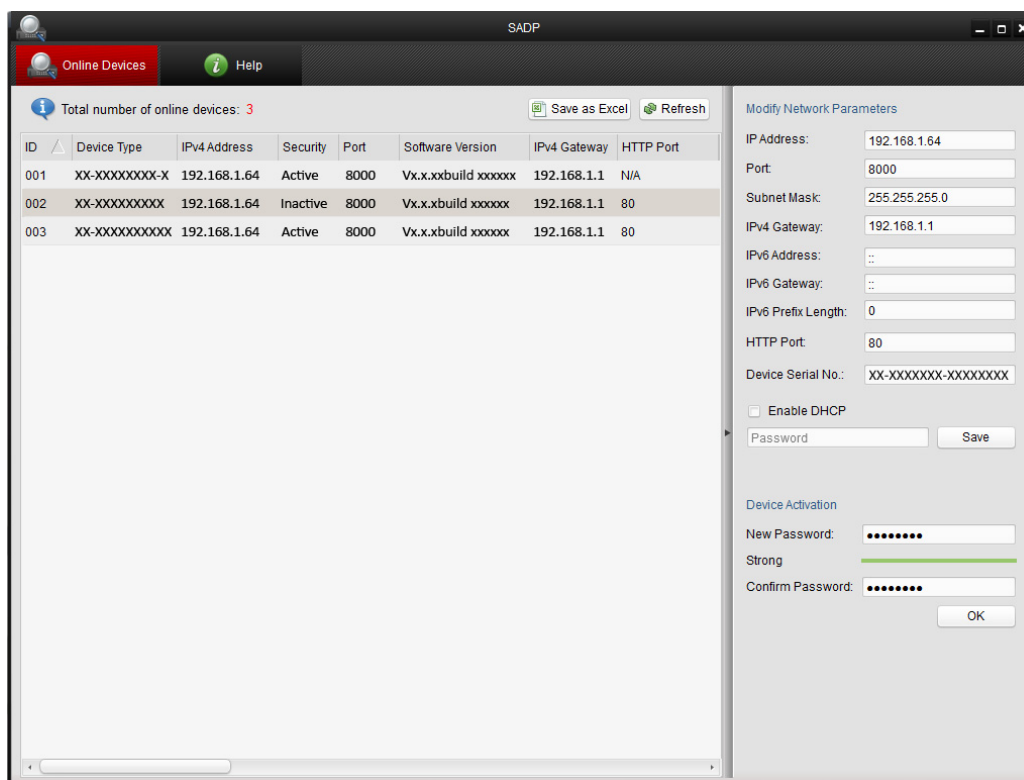


Figura 2–4 Interfață SADP

3. Creați o parolă și introduceți-o în câmpul de parolă și apoi confirmați-o.



SE RECOMANDĂ O PAROLĂ PUTERNICĂ – Vă recomandăm să creați o parolă puternică la alegerea dvs. (folosind minimum 8 caractere, printre care majuscule, minuscule, cifre și caractere speciale) pentru a crește siguranța produsului dvs. De asemenea, vă recomandăm resetarea parolei cu regularitate, în special în sistemul cu securitate sporită, resetarea lunară sau săptămânală a parolei vă poate proteja produsul mai bine.

4. Faceți clic pe **OK** pentru a salva parola.

Puteți verifica dacă activarea a fost finalizată din fereastra popup. Dacă activarea nu a reușit, vă rugăm să vă asigurați că parola îndeplinește cerințele și încercați din nou.

5. Schimbați adresa IP a dispozitivului pentru a se potrivi cu subrețeaua computerului prin modificarea manuală a adresei IP sau prin bifarea casetei de selectare Enable DHCP.

Modify Network Parameters

IP Address: 192.168.1.64

Port: 8000

Subnet Mask: 255.255.255.0

IPv4 Gateway: 192.168.1.1

IPv6 Address: ::

IPv6 Gateway: ::

IPv6 Prefix Length: 0

HTTP Port: 80

Device Serial No.: XX-XXXXXXX-XXXXXXX

☐ Enable DHCP

Password Save

Figura 2–5 Modificare adresă IP

6. Introduceți parola și faceți clic pe butonul **Save** pentru a activa modificarea adresei IP.

❖ Activarea prin software-ul clientului

Software-ul client este un software de gestionare video pentru mai multe tipuri de dispozitive.

Obțineți software-ul client de pe discul inclus sau de pe site-ul web oficial și instalați-l conform indicațiilor afișate. Urmăriți pașii pentru a activa camera.

Pași:

1. Rulați software-ul client și panoul de control al software-ului va fi afișat, așa cum este prezentat în figura de mai jos.

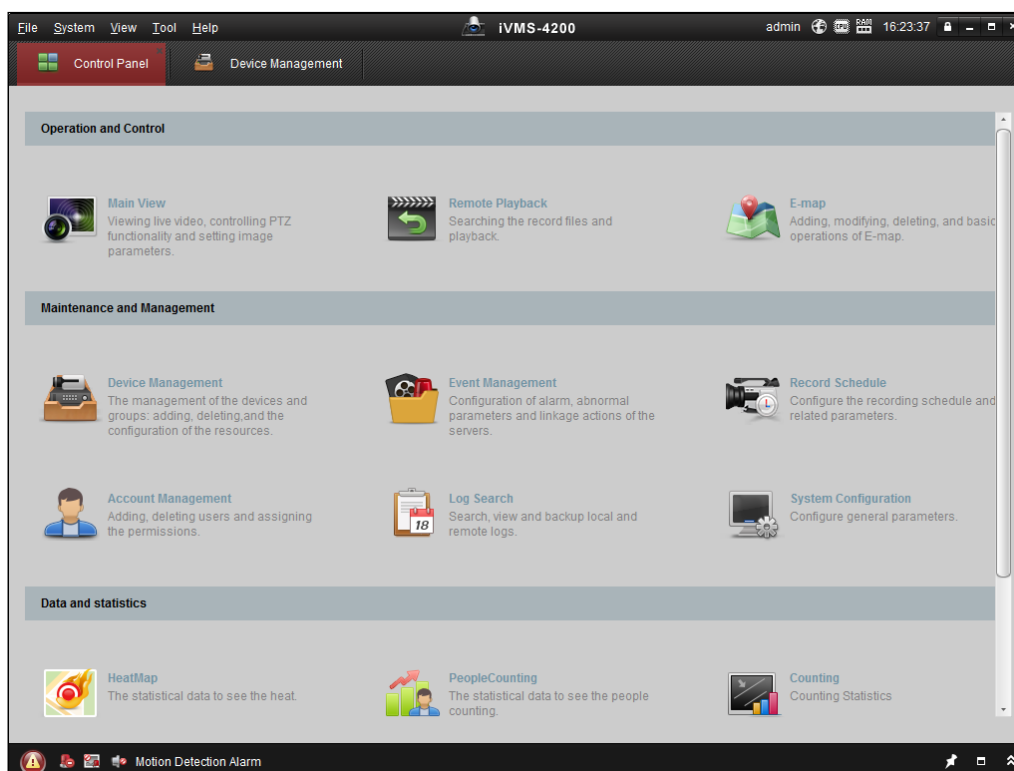


Figura 2–6 Panou de control

2. Faceți clic pe pictograma **Device Management** pentru a accesa interfața Device Management, după cum se arată în figura de mai jos.

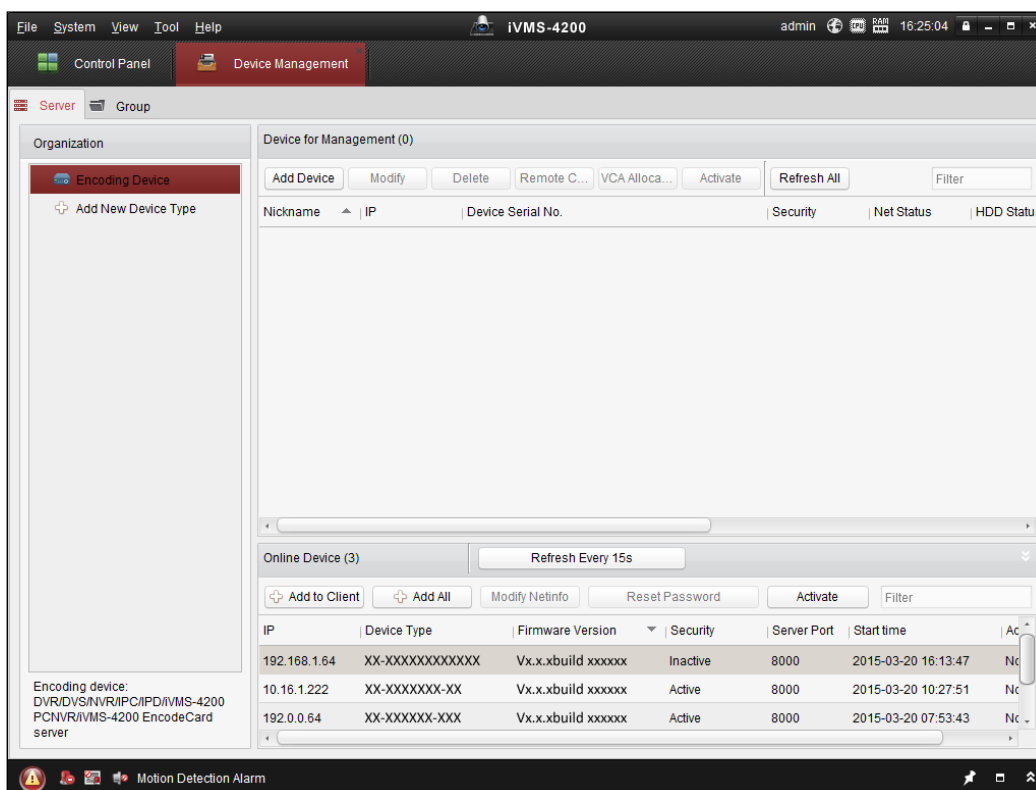


Figura 2–7 Interfața gestionare dispozitiv

3. Verificați starea dispozitivului din lista de dispozitive și selectați un dispozitiv care nu este activ.
4. Faceți clic pe butonul **Activate** pentru a afișa interfața Activare.
5. Creați o parolă și introduceți-o în câmpul de parolă și apoi confirmați-o.



SE RECOMANDĂ O PAROLĂ PUTERNICĂ – Vă recomandăm să creați o parolă puternică la alegerea dvs. (folosind minimum 8 caractere, printre care majuscule, minuscule, cifre și caractere speciale) pentru a crește siguranța produsului dvs. Vă recomandăm resetarea parolei cu regularitate, în special în sistemul cu securitate sporită, resetarea lunară sau săptămânală a parolei vă poate proteja produsul mai bine.

Figura 2–8 Interfața de activare (Software client)

6. Faceți clic pe butonul **OK** pentru a porni activarea.
7. Faceți clic pe butonul Modify Netinfo pentru a afișa interfața Modificare parametri rețea, așa cum este prezentat în figura de mai jos.

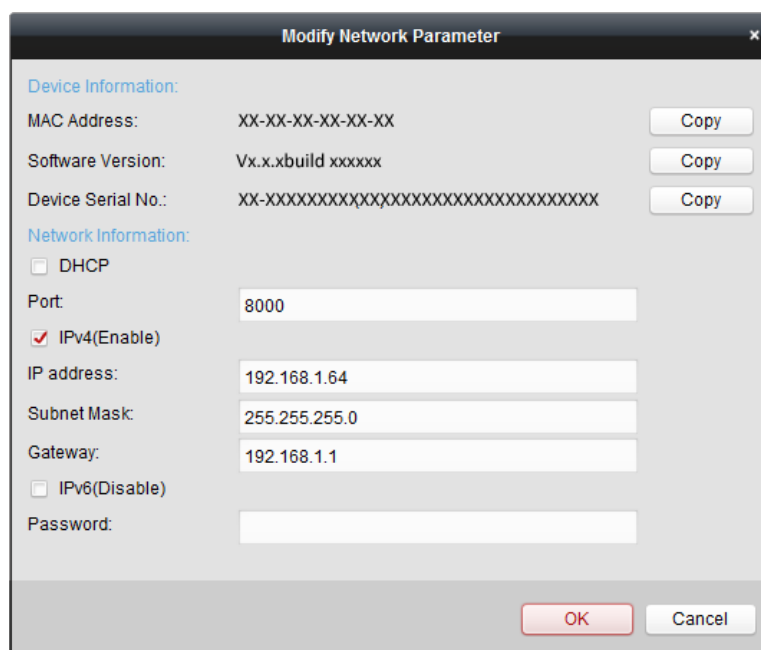


Figura 2–9 Modificare parametri rețea

8. Schimbați adresa IP a dispozitivului pentru a se potrivi cu subrețeaua computerului prin modificarea manuală a adresei IP sau prin bifarea casetei de selectare Enable DHCP.
9. Introduceți parola pentru a activa modificarea adresei IP.

2.2 Setarea camerei de rețea prin WAN

Scopul:

Această secțiune vă explică cum să conectați camera de rețea WAN cu un IP static sau un IP dinamic.

2.2.1 Conexiune cu IP static

Înainte de a începe:

Aplicați un IP static de la un ISP (Furnizor de servicii de internet). Cu adresa IP statică, puteți conecta camera de rețea prin intermediul unui router sau conectați-l direct la WAN.

- **Conectarea camerei de rețea prin intermediul unui router**

Pași:

1. Conectați camera de rețea la router.
2. Atribuiți o adresă IP LAN, masca de subrețea și gateway-ul. Consultați Secțiunea 2.1.2 pentru configurarea detaliată a adresei IP a camerei de rețea.
3. Salvați IP-ul static în router.
4. Setări maparea portului, de ex., porturile 80, 8000 și 554. Pașii pentru maparea portului variază în funcție de diversele routere. Contactați producătorul routerului pentru asistență privind maparea porturilor.

Notă: Consultați Anexa 2 pentru informații detaliate privind maparea porturilor.

5. Vizitați camera de rețea prin intermediul unui browser web sau software-ul client de pe internet.

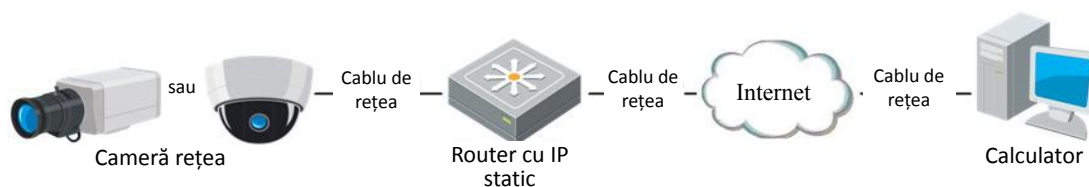


Figura 2–10 Accesarea camerei printr-un router cu IP static

● **Conectarea camerei de rețea cu IP static direct**

De asemenea, puteți salva IP-ul static în cameră și să-l conectați direct la internet fără a utiliza un router. Consultați Secțiunea 2.1.2 pentru configurarea detaliată a adresei IP a camerei de rețea.



Figura 2–11 Accesarea directă a camerei cu IP static

2.2.2 Conexiune cu IP dinamic

Înainte de a începe:

Aplicați un IP dinamic de la un ISP. Cu adresa IP dinamică, puteți conecta camera de rețea prin intermediul unui modem sau router.

● Conectarea camerei de rețea prin intermediul unui router

Pași:

1. Conectați camera de rețea la router.
2. În cameră, atribuiți o adresă IP LAN, masca de subrețea și gateway-ul. Consultați Secțiunea 2.1.2 pentru configurarea detaliată a adresei IP a camerei de rețea.
3. Din router, setați numele de utilizator, parola și confirmați parola pentru PPPoE.
4. Setați maparea porturilor. De ex. porturile 80, 8000 și 554. Pașii pentru maparea porturilor variază în funcție de router. Contactați producătorul routerului pentru asistență privind maparea porturilor.

Notă: Consultați Anexa 2 pentru informații detaliate privind maparea porturilor.

5. Aplicați un nume de domeniu de la un furnizor de nume de domeniu.
6. Configurați setările DDNS din interfața de setări a routerului.
7. Vizitați camera utilizând numele de domeniu aplicat.

● Conectarea camerei de rețea prin intermediul unui modem

Scopul:

Această cameră suportă funcția de linie comutată automată PPPoE. Camera înregistrează o adresă IP publică prin linie comutată ADSL după ce camera este conectată la un modem. Trebuie să configurați parametrii PPPoE ai camerei de rețea. Consultați *Secțiunea 5.3.3 Configurare setări PPPoE* pentru configurarea detaliată.

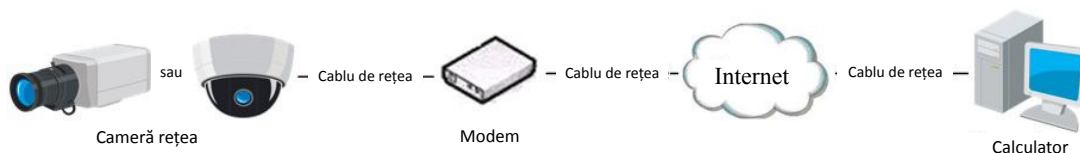


Figura 2–12 Accesarea camerei cu IP dinamic

Notă: Adresa IP obținută este atribuită dinamic prin intermediul PPPoE, astfel încât adresa IP se modifică întotdeauna după repornirea camerei. Pentru a soluționa problemele apărute din cauza unui IP dinamic trebuie să obțineți un nume de domeniu de la un furnizor DDNS (De exemplu, DynDns.com). Urmăriți pașii de mai jos pentru rezolvarea obișnuită a numelor de domenii și rezolvarea numelui de domeniu privat pentru a rezolva problema.

◆ Soluționare nume de domeniu normal

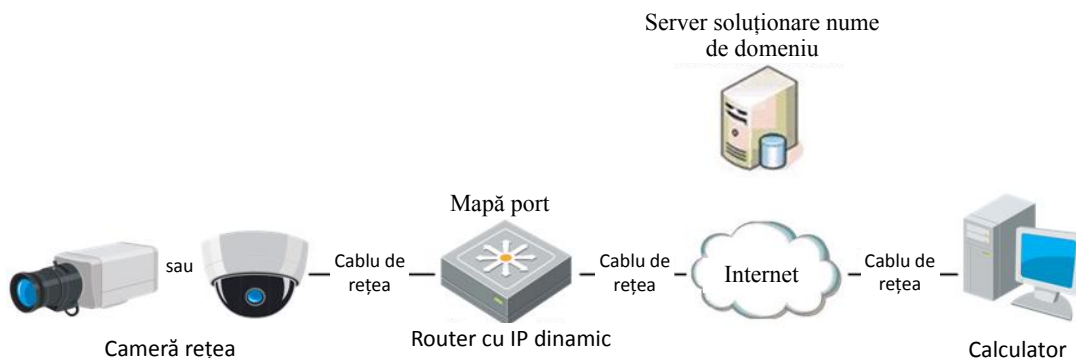


Figura 2–13 Soluționare nume de domeniu normal

Pași:

1. Aplicați un nume de domeniu de la un furnizor de nume de domeniu.
2. Configurați setările DDNS în interfața **Setări DDNS** a camerei de rețea.
Consultați *Secțiunea 5.3.4 Configurare setări DDNS* pentru configurarea detaliată.
3. Vizitați camera utilizând numele de domeniu aplicat.

◆ Rezoluția numelui domeniului privat

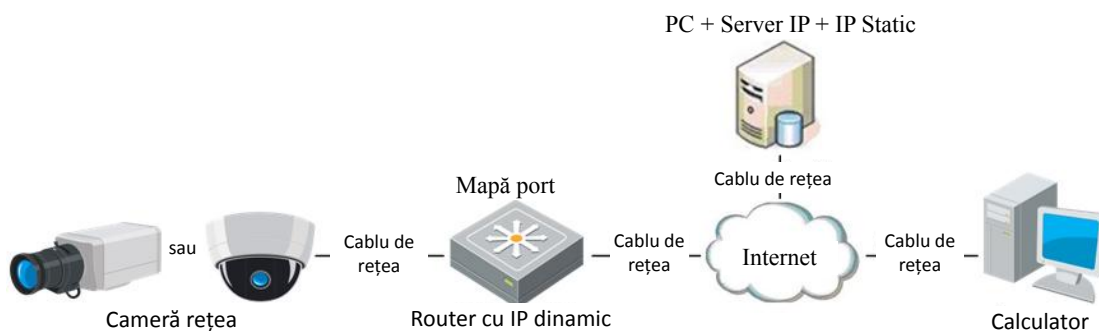


Figura 2–14 Rezolvarea numelui de domeniu privat

Pași:

1. Instalați și rulați software-ul serverului IP într-un computer cu un IP static.
2. Accesați camera de rețea prin LAN cu un browser web sau software-ul clientului.
3. Activați DDNS și selectați serverul IP ca tip de protocol. Consultați *Secțiunea 5.3.4 Configurare setări DDNS* pentru configurarea detaliată.

Capitolul 3 Accesul la camera de rețea

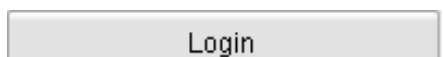
3.1 Accesare prin browser web

Pași:

1. Deschideți browserul web.
2. În bara de adrese a browserului introduceți adresa IP a camerei de rețea și apăsați tasta **Enter** pentru a intra în interfața de conectare.
3. Activați camera de rețea pentru utilizarea inițială, consultați secțiunea 2.1.2 pentru informații detaliate.

Notă:

- Adresa IP implicită este 192.168.1.64.
 - În cazul în care camera nu este activată, activați, mai întâi, camera, urmând instrucțiunile din Capitolul 3.1 sau din Capitolul 3.2.
4. Selectați engleza ca limba interfeței din partea dreaptă-sus a interfeței de conectare.
 5. Introduceți numele de utilizator și parola și faceți clic pe



Utilizatorul admin trebuie să configureze corespunzător permisiunile pentru conturile de dispozitiv și pentru utilizator/operator. Ștergeți permisiunile care nu sunt necesare pentru conturi și utilizator/operator.

Notă:

Adresa IP a dispozitivului se blochează dacă utilizatorul administrator introduce greșit parola de 7 ori (5 încercări pentru utilizator/operator).

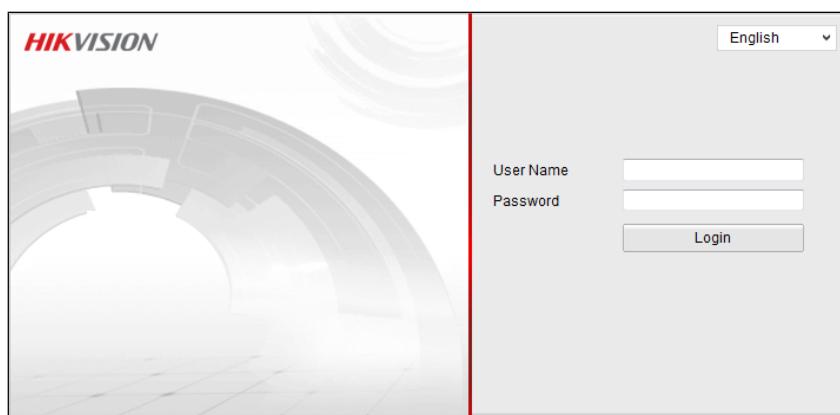


Figura 3–1 Interfața de autentificare

6. Instalați insertul înainte de a viziona conținutul video live și de a gestiona camera.
- Urmați indicațiile de instalare pentru a instala plug-in-ul.

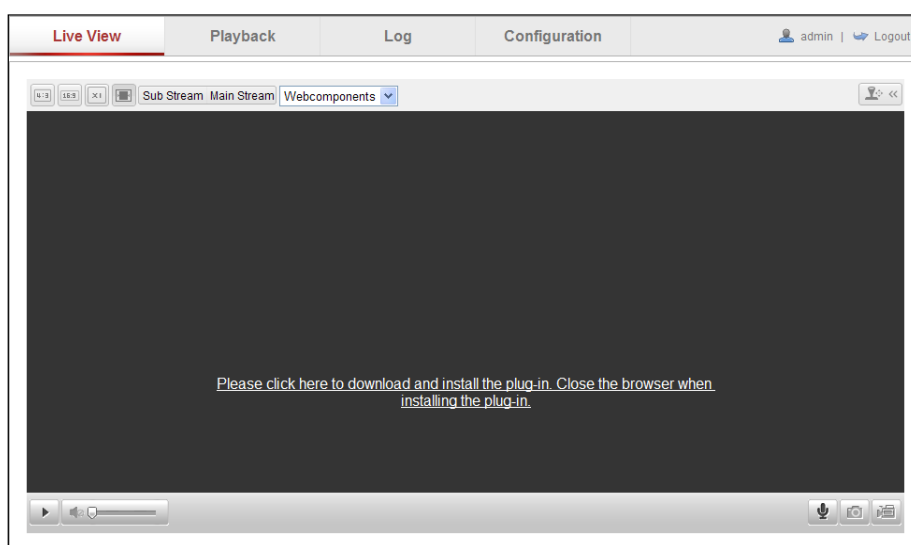


Figura 3–2 Descărcare și instalare plug-in

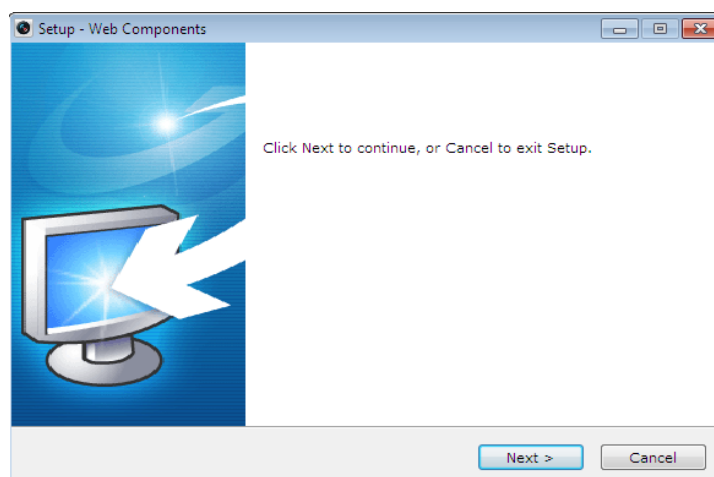


Figura 3–3 Instalarea plug-in-ului (1)

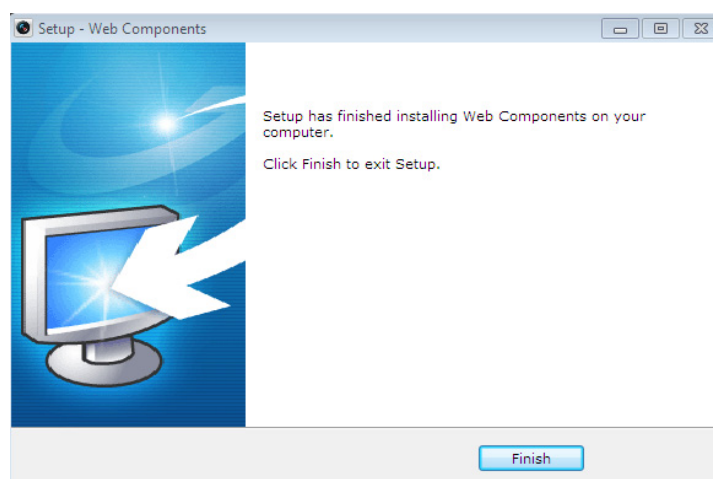


Figura 3–4 Instalarea plug-in-ului (2)

Notă: Este posibil să trebuiască să închideți browserul web pentru a instala plug-in-ul. Redeschideți browserul web și conectați-vă din nou după instalarea plug-in-ului.

3.2 Accesarea prin software-ul client

CD-ul produsului conține software-ul client iVMS-4200. Puteți vizualiza videoclipul live și puteți gestiona camera cu software-ul.

Urmați instrucțiunile de instalare de pe ecran pentru a instala software-ul. Panoul de control și interfața de vizualizare live a software-ului client iVMS-4200 sunt prezentate mai jos.

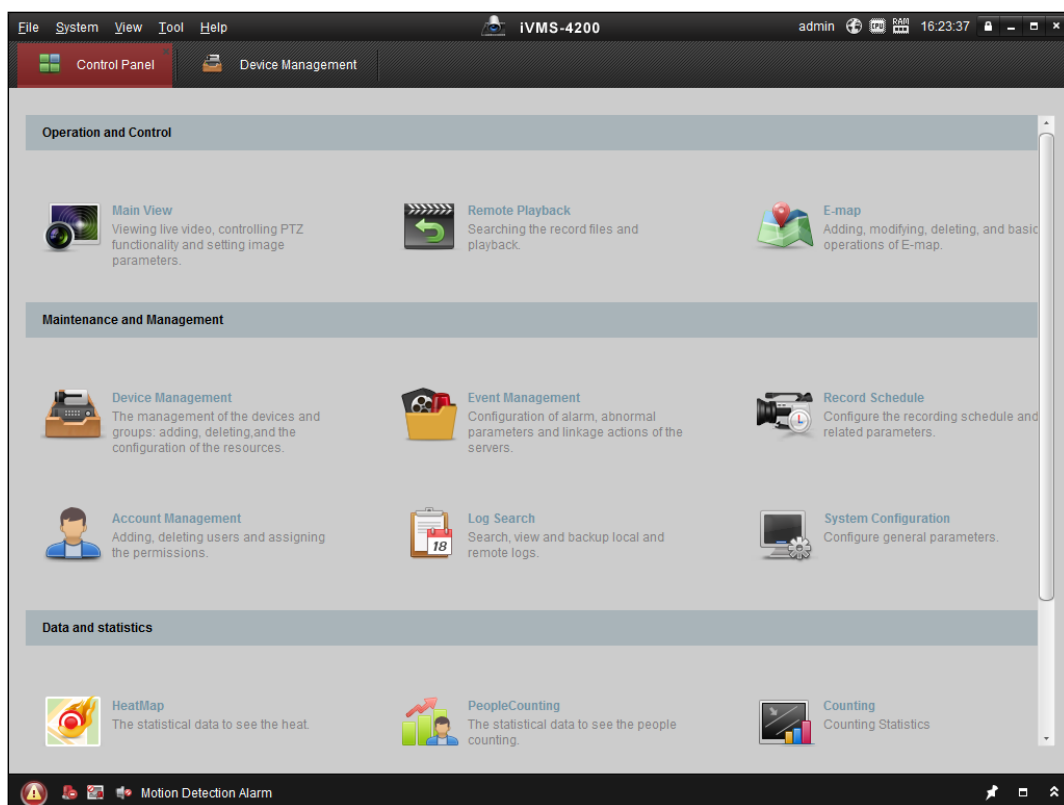


Figura 3–5 Panou de control iVMS-4200

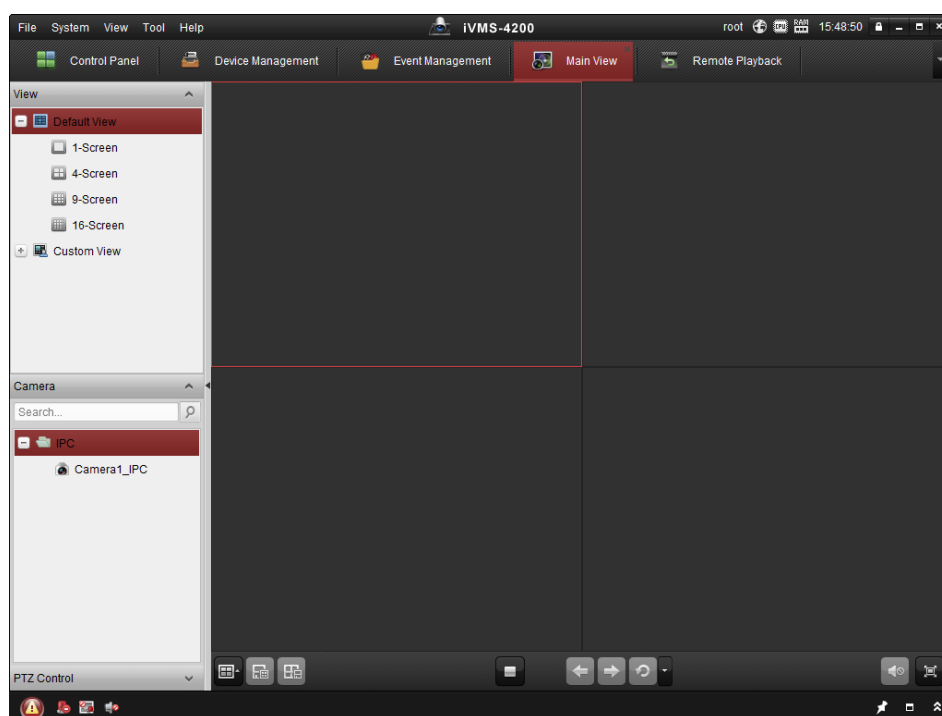


Figura 3–6 Vedere principală iVMS-4200

Notă: Pentru informații detaliate despre software, consultați manualul utilizatorului pentru iVMS-4200.

Capitolul 4 Vizualizare live

4.1 Pagina Vizualizare live

Scopul:

Pagina de vizualizare live vă permite să vizualizați video-ul în timp real, să capturați imagini, să realizați controlul PTZ, să setați/presetați apeluri și să configurați parametrii video.

Conectați camera de rețea pentru a intra în pagina de vizualizare live, sau faceți clic pe **Live View** pe bara de meniu a paginii principale pentru a intra în pagina de vizualizare live.

Descrierile paginii de vizualizare live:

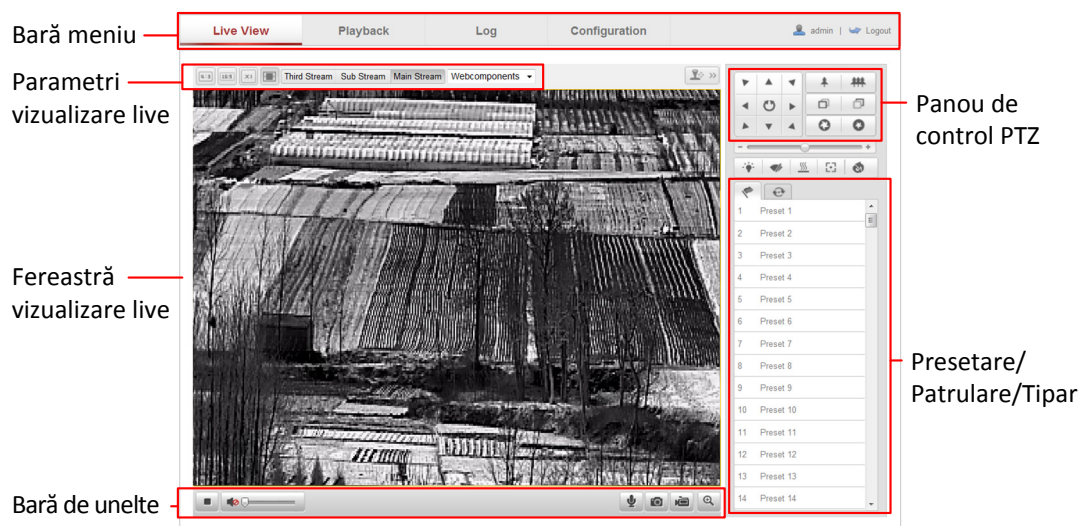


Figura 4–1 Pagina Vizualizare live

Model cameră:

Indică modelul camerei la care vă conectați.

Ajutor on-line:

Faceți clic pe  pentru a obține ajutorul on-line, care vă va ghida privind operațiunile de bază ale fiecărei funcții.

Bara de meniu:

Faceți clic pe fiecare filă pentru a accesa paginile Vizualizare live, Redare, Jurnal și Configurare.

Control afișaj:

Faceți clic pe fiecare buton pentru a regla aspectul și tipul de flux ale vizualizării live. Puteți face clic pe lista verticală pentru a selecta aspectul afișajului. Utilizatorul de IE (Internet Explorer) poate selecta componentele web și formatul quick time. Neutilizatorul de IE poate selecta componentele web, formatul quick time, VLC sau MJPEG dacă acestea sunt acceptate de către browserul web.

Fereastra Vizualizare live:

Afișează video live.

Bară de instrumente:

Operațiunile de pe pagina vizualizării live, de exemplu, pornirea/oprirea vizualizării live, capturarea, înregistrarea, pornirea/oprirea sunetului pe două căi etc.

Control PTZ:

Acțiunile de panoramare, de înclinare și de mărire/micșorare ale camerei și controlul luminii și al ștergătorului. (disponibile numai pentru camerele care acceptă funcția PTZ)

Setări patrulă/presetări:

Setați/apelați/ștergeți presetările sau patrulele pentru camerele PTZ.

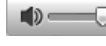
4.2 Inițializare Vizualizare live

În fereastra de vizualizare live, cum se arată în Figura 4–2, faceți clic pe  bara de instrumente pentru a porni vizualizarea live a camerei.



Figura 4–2 Bara de instrumente vizualizare live

Tabelul 4–1 Descrierea barei de control al afișajului și a barei de instrumente

Pictogramă	Descriere
	Pornire/oprire vizualizare live.
	Dimensiunea ferestrei este de 4:3.
	Dimensiunea ferestrei este de 16:9.
	Dimensiunea originală a ferestrei.
	Dimensiunea ferestrei auto-adaptive.
Main Stream	Vizualizare live cu flux principal.
Sub Stream	Vizualizare live cu flux secundar.
Webcomponents 	Faceți clic pentru a selecta insertul terței părți.
2*2 	Divizarea ferestrei
	Realizați o captură manuală a imaginii.
	Porniți/opriți înregistrarea manual.
 	Pornirea sonorului și reglarea volumului/fără sonor.
 	Pornirea/Oprirea sunetului pe două căi.
 	Activarea/Dezactivarea funcției e-PTZ.

4.3 Înregistrarea și capturarea manuală a imaginilor

În interfața de vizualizare live, faceți clic pe  din bara de instrumente pentru a captura imagini live sau faceți clic pe  pentru a înregistra vizualizarea live. Căile de salvare ale imaginilor și videoclipurilor capturate pot fi setate pe pagina **Configuration > Local Configuration**. Pentru a configura înregistrarea programată de la distanță, consultați *Secțiunea 6.3*.

Notă: Imaginea capturată va fi salvată ca fișier JPEG sau BMP în computerul dvs.

Capitolul 5 Configurarea camerei de rețea

5.1 Configurare parametrii locali

Notă: Configurarea locală se referă la parametrii vizualizării live, ai fișierelor înregistrate și ai imaginilor și videoclipurilor capturate. Fișierele înregistrate, imaginile și videoclipurile capturate sunt cele pe care le-ați înregistrat și le-ați capturat folosind browserul web și, astfel, căile de salvare ale acestora se găsesc pe PC-ul pe care rulează browserul.

Pași:

1. Accesați interfața Local Configuration:

Configuration > Local Configuration

The screenshot displays the 'Local Configuration' web interface. It is organized into three main sections: 'Live View Parameters', 'Record File Settings', and 'Picture and Clip Settings'. Each section contains various configuration options with radio buttons for selection and text input fields for file paths, accompanied by 'Browse' buttons.

Live View Parameters	
Protocol	☒ TCP ☐ UDP ☐ MULTICAST ☐ HTTP
Live View Performance	☐ Shortest Delay ☒ Auto
Rules	☐ Enable ☒ Disable
Image Format	☒ JPEG ☐ BMP
Display Temperature Info.	☐ Enable ☒ Disable
Display Temperature Info. on Capture	☐ Enable ☒ Disable

Record File Settings	
Record File Size	☐ 256M ☒ 512M ☐ 1G
Save record files to	C:\Users\yanjiamin\Web\RecordFiles Browse
Save downloaded files to	C:\Users\yanjiamin\Web\DownloadFiles Browse

Picture and Clip Settings	
Save snapshots in live view to	C:\Users\yanjiamin\Web\CaptureFiles Browse
Save snapshots when playback to	C:\Users\yanjiamin\Web\PlaybackPics Browse
Save clips to	C:\Users\yanjiamin\Web\PlaybackFiles Browse

Figura 5–1 Interfață Configurare locală

2. Configurați setările următoare:

- **Live View Parameters:** Setati tipul de protocol și performanța vizualizării live.
 - **Tip protocol:** Se pot selecta TCP, UDP, MULTICAST și HTTP.

TCP: Asigură furnizarea completă a datelor de flux și o calitate mai bună a semnalului video, dar transmisiunea în timp real va fi afectată.

UDP: Oferă fluxuri audio și video în timp real.

HTTP: Asigură aceeași calitate ca protocolul TCP fără a seta porturi specifice pentru flux, în cadrul anumitor medii de rețea.

MULTICAST: Se recomandă să selectați tipul de MCAST când folosiți funcția de distribuire multiplă. Pentru informații detaliate despre Multicast, consultați *Secțiunea 5.3.1 Configurare Setări TCP/IP*.
 - **Live View Performance:** Setati live view performance la Shortest Delay sau la Auto.
 - **Auto Start Live View:** Dacă activați această funcție, imaginile vizualizării live vor fi pornite automat atunci când activați fila **Vizualizare live**. Dacă această funcție este dezactivată, puteți, de asemenea, porni manual vizualizarea live din interfața Vizualizare live.
 - **Rules:** Se referă la regulile de pe browserul dvs. local, selectați activare sau dezactivare pentru a afișa sau nu marcasele colorate când se declanșează detectarea mișcării, detectarea feței sau detectarea intruziunilor. De exemplu, activat conform regulilor, iar detectarea feței este de asemenea activată, când o față este detectată, acesta va fi marcată cu un dreptunghi verde pe vizualizarea live.
 - **Image Format:** Alegeți formatul de imagine pentru captura imaginii.
 - **Fire Point:** Selectați Detectare sursă incendiu ca Tip de resursă VCA (analiza conținutului video). Bifați caseta pentru a activa funcțiile necesare. Puteți selecta Display Fire Point Distance, Display Highest Temperature, Locate Highest Temperature Point și Frame Fire Point.

- **Display Temperature Info. on Stream:** Selectați Măsurare temperatură ca Tip de resursă VCA. Bifați caseta pentru a afișa informațiile despre temperatură în interfața vizualizării live.
- **Display Temperature Info. on Capture:** Selectați Măsurare temperatură ca Tip de resursă VCA. Bifați caseta pentru a afișa informațiile despre temperatură pe capturi.
- **Record File Settings:** Setați calea de salvare a fișierelor video înregistrate. Valabil pentru fișierele pe care le-ați înregistrat cu browserul web.
 - **Record File Size:** Selectați dimensiunea comprimată a înregistrării manuale și fișierelor video descărcate la 256 M, 512 M sau 1 G. După selectare, dimensiunea maximă a fișierului înregistrat este valoarea pe care ați selectat-o.
 - **Save record files to:** Setare cale de salvare pentru fișierele video înregistrate manual.
 - **Save downloaded files to:** Setați calea de salvare a fișierelor video descărcate în modul redare.
- **Picture and Clip Settings:** Setare căi de salvare pentru imaginile și fișierele video tăiate capturate. Setarea este valabilă pentru imaginile capturate cu ajutorul browserului web.
 - **Save snapshots in live view to:** Setați calea de salvare a imaginilor capturate manual în modul de vizualizare live.
 - **Save snapshots when playback to:** Setați calea de salvare a imaginilor capturate în modul de redare.
 - **Save clips to:** Setați calea de salvare a fișierelor video înregistrate în modul redare.

Notă: Puteți face clic pe **Browse** pentru a schimba directorul de salvare a videoclipurilor și a imaginilor.

3. Faceți clic pe **Save** pentru a salva setările.

5.2 Configurarea setărilor de timp

Scopul:

Puteți urma instrucțiunile din această secțiune pentru a configura sincronizarea timpului și setările DST.

Pași:

1. Accesați interfața Time Settings:

Configuration > Basic Configuration > System > Time Settings

Sau **Configuration > Advanced Configuration > System > Time Settings**

Figura 5–2 Setări oră

2. Selectați Fusul orar.

Selectați fusul orar al locației dvs. din meniul vertical.

3. Setări Sincronizarea timpului.

Puteți sincroniza timpul prin intermediul NTP (protocolul timpului rețelei) sau puteți face manual acest lucru.

- Sincronizarea timpului prin intermediul serverului NTP.

(1) Bifați caseta pentru a activa funcția **NTP**.

(2) Configurați setările următoare:

Server Address: Adresa IP a serverului NTP.

NTP Port: Portul serverului NTP.

Interval: Intervalul de timp dintre două acțiuni de sincronizare cu serverul NTP.

Time Sync.	
☒ NTP	
Server Address	time.windows.com
NTP Port	123
Interval	1440 min.

Figura 5–3 Sincronizare oră prin server NTP

Notă: În cazul în care camera este conectată la o rețea publică, trebuie să utilizați un server NTP care are o funcție de sincronizare a timpului, cum ar fi serverul de la National Time Center (Centrul național de timp) (adresa IP: 210.72.145.44). În cazul în care camera este configurată într-o rețea personalizată, software-ul NTP poate fi utilizat pentru a crea un server NTP pentru sincronizarea timpului.

- Sincronizarea manuală a timpului

Activați funcția **Manual Time Sync**, după care faceți clic pe  pentru a seta timpul sistemului din calendarul pop-up.

Notă: Puteți, de asemenea, bifa caseta **Sync with computer time** pentru a sincroniza timpul camerei cu timpul computerului dvs.

Sep 2013						
Sun	Mon	Tue	Wed	Thu	Fri	Sat
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	1	2	3	4	5
6	7	8	9	10	11	12

Manual Time Sync.	
Device Time	2013-09-22T11:32:34
Set Time	2013-09-22T11:14:33 ☒ Sync with computer time

Figura 5–4 Sincronizare oră manual

4. Faceți clic pe pagina filei **DST (Configuration > Advanced Configuration > System > DST)** pentru a activa funcția DST (ora de vară) și setați data perioadei DST.

DST					
☒	Enable DST				
Start Time	Apr	First	Sun	02	o'clock
End Time	Oct	Last	Sun	02	o'clock
DST Bias	30min				

Figura 5–5 Setări DST

5. Faceți clic pe **Save** pentru a salva setările.

5.3 Configurare Setări rețea

5.3.1 Configurare Setări TCP/IP

Scopul:

Setările TCP/IP trebuie configurate în mod corespunzător înainte de a opera camera în rețea. Camera suportă atât IPv4, cât și IPv6. Puteți configura simultan ambele versiuni, fără ca acestea să intre în conflict una cu cealaltă, și trebuie să configurați cel puțin o versiune de IP.

Pași:

1. Accesați interfața Setări TCP/IP:

Configuration > Basic Configuration > Network > TCP/IP

Sau **Configuration > Advanced Configuration > Network > TCP/IP**

NIC Settings	
NIC Type	Auto
☐ DHCP	
IPv4 Address	10.11.36.159 Test
IPv4 Subnet Mask	255.255.255.0
IPv4 Default Gateway	10.11.36.254
IPv6 Mode	Route Advertisement View Route Advertisement
IPv6 Address	::
IPv6 Subnet Mask	0
IPv6 Default Gateway	
Mac Address	44:19:b6:5e:16:f2
MTU	1500
Multicast Address	
☒ Enable Multicast Discovery	
DNS Server	
Preferred DNS Server	8.8.8.8
Alternate DNS Server	

Figura 5–6 Setări TCP/IP

2. Configurați setările de bază de rețea, inclusiv tipul NIC, adresa IPv4 sau IPv6, masca de subrețea IPv4 sau IPv6, gateway implicit IPv4 sau IPv6, setări MTU și adresă distribuire multiplă.
3. (Opțional) Bifați caseta **Enable Multicast Discovery**, după care camera de rețea conectată (on-line) poate fi detectată automat de către software-ul client prin intermediul protocolului multicast privat din LAN.
4. Faceți clic pe **Save** pentru a salva setările de mai sus.

Note:

- Intervalul de valori valid al MTU este 1280 - 1500.
- Difuzarea multiplă trimite un flux adresei grupului de difuzare multiplă și permite mai multor clienți să obțină fluxul în același timp prin solicitarea unei copii de la adresa grupului de difuzare multiplă. Înainte de a utiliza această funcție, trebuie să activați funcția de distribuire multiplă a routerului dvs.
- Repornirea este necesară pentru ca setările să aibă efect.

5.3.2 Configurare Setări Port

Scopul:

Puteți seta numărul portului camerei, de exemplu, portul HTTP, portul RTSP (protocolul de streaming în timp real), portul HTTPS și portul serverului.

Pași:

1. Accesați interfața Setări Port:

Configuration > Basic Configuration > Network > Port

Sau **Configuration > Advanced Configuration > Network > Port**

HTTP Port	80
RTSP Port	554
HTTPS Port	443
Server Port	8000

Figura 5–7 Setări port

2. Setăți portul HTTP, portul RTSP, portul HTTPS și portul de server al camerei.

HTTP Port: Numărul de port implicit este 80 și poate fi schimbat cu orice nr. de port care nu este ocupat.

RTSP Port: Numărul de port implicit este 554 și poate fi schimbat cu orice nr. de port între 1024 și 65535.

HTTPS Port: Numărul de port implicit este 443 și poate fi schimbat cu orice nr. de port care nu este ocupat.

Server Port: Numărul de port implicit al serverului este 8000 și acesta poate fi schimbat cu orice nr. de port între 2000 și 65535.

3. Faceți clic pe **Save** pentru a salva setările.

Notă: Repornirea este necesară pentru ca setările să aibă efect.

5.3.3 Configurare setări PPPoE

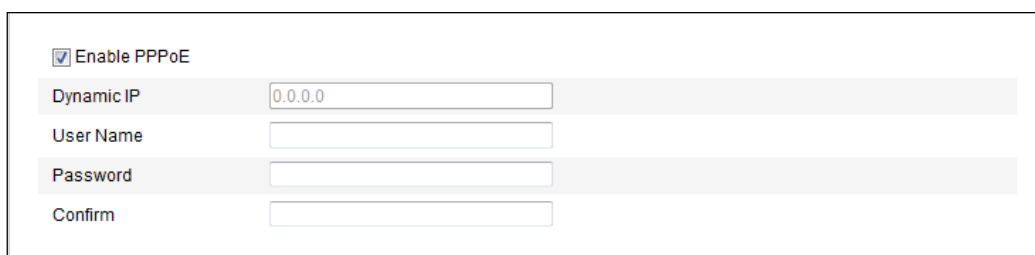
Scopul:

Dacă nu aveți un router ci doar un modem, puteți utiliza funcția Protocol Punct la Punct prin Ethernet (PPPoE).

Pași:

1. Accesați interfața Setări PPPoE:

Configuration > Advanced Configuration > Network > PPPoE



☒ Enable PPPoE	
Dynamic IP	0.0.0.0
User Name	
Password	
Confirm	

Figura 5–8 Setări PPPoE

2. Bifați caseta **Enable PPPoE** pentru a activa această funcționalitate.
3. Introduceți **Nume de utilizator**, **Parola**, și **Confirmare** parolă pentru accesul la PPPoE.

Notă: Numele de utilizator și parola trebuie să fi atribuite de către ISP-ul dvs.



- *Pentru confidențialitatea dvs. și pentru a vă proteja mai bine sistemul împotriva riscurilor de securitate, vă recomandăm să utilizați parole puternice pentru toate funcțiile și dispozitivele de rețea. Parola trebuie să fie aleasă de către dvs. (folosind minimum 8 caractere, printre care majuscule, minuscule, cifre și caractere speciale) pentru a crește siguranța produsului dvs.*
 - *Configurarea adecvată a tuturor parolelor și a altor setări de securitate este responsabilitatea instalatorului și/sau a utilizatorului final.*
4. Faceți clic pe **Save** pentru a salva și a ieși din interfață.

Notă: Repornirea este necesară pentru ca setările să aibă efect.

5.3.4 Configurare setări DDNS

Scopul:

În cazul în care camera este setată să utilizeze PPPoE drept conexiune la rețea implicită, puteți utiliza Dynamic DNS (DDNS) pentru acces la rețea.

Înainte de a începe:

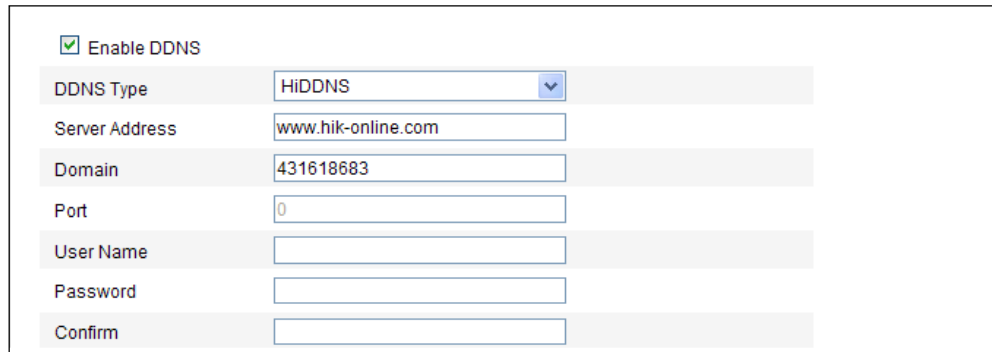
Înainte de configurarea setărilor DDNS ale camerei, este necesară înscrierea pe serverul DDNS.



- *Pentru confidențialitatea dvs. și pentru a vă proteja mai bine sistemul împotriva riscurilor de securitate, vă recomandăm să utilizați parole puternice pentru toate funcțiile și dispozitivele de rețea. Parola trebuie să fie aleasă de către dvs. (folosind minimum 8 caractere, printre care majuscule, minuscule, cifre și caractere speciale) pentru a crește siguranța produsului dvs.*
- *Configurarea adecvată a tuturor parolelor și a altor setări de securitate este responsabilitatea instalatorului și/sau a utilizatorului final.*

Pași:

1. Accesați interfața Setări DDNS:

Configuration > Advanced Configuration > Network > DDNS


The screenshot shows the DDNS configuration page. At the top, there is a checkbox labeled 'Enable DDNS' which is checked. Below it, the 'DDNS Type' is set to 'HiDDNS' in a dropdown menu. The 'Server Address' field contains 'www.hik-online.com'. The 'Domain' field contains '431618683'. The 'Port' field contains '0'. The 'User Name' and 'Password' fields are empty. The 'Confirm' field is also empty.

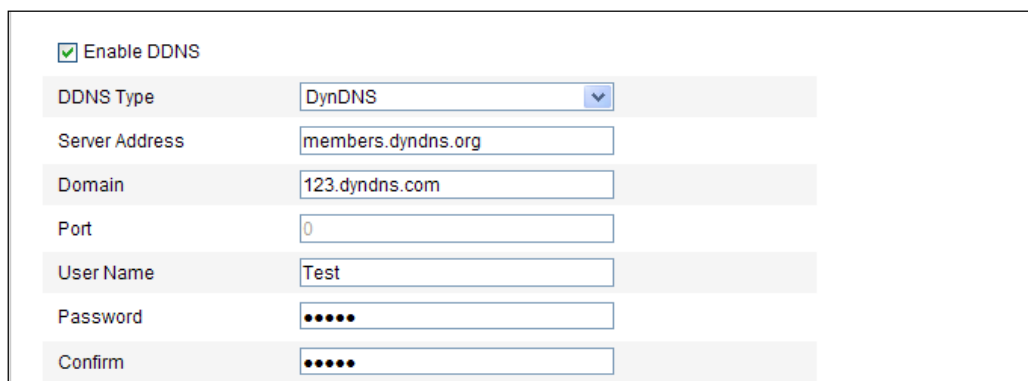
Figura 5–9 Setări DDNS

2. Bifați caseta de selectare **Enable DDNS** pentru a activa această caracteristică.
3. Selectați **Tipul de DDNS**. Puteți selecta patru tipuri de DDNS: HiDDNS, IPServer, NO-IP și DynDNS.

- DynDNS:

Pași:

- (1) Introduceți **Server Address** DynDNS (de ex. members.dyndns.org).
- (2) În câmpul de text **Domain** introduceți domeniul obținut de pe site-ul web DynDNS.
- (3) Introduceți **Portul** serverului DynDNS.
- (4) Introduceți **Numele de utilizator** și **parola** înregistrate pe site-ul web DynDNS.
- (5) Faceți clic pe **Save** pentru a salva setările.



The screenshot shows the DDNS configuration page with 'DynDNS' selected in the 'DDNS Type' dropdown. The 'Server Address' field contains 'members.dyndns.org'. The 'Domain' field contains '123.dyndns.com'. The 'Port' field contains '0'. The 'User Name' field contains 'Test'. The 'Password' and 'Confirm' fields are filled with dots, indicating masked text.

Figura 5–10 Setări DynDNS

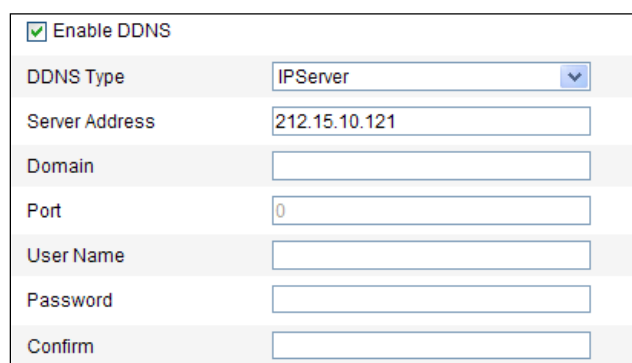
- Server IP:

Pași:

(1) Introduceți adresa de server a serverului IP.

(2) Faceți clic pe **Save** pentru a salva setările.

Notă: Pentru serverul IP, trebuie să aplicați un IP static, o mască de subrețea, gateway-ul și DNS-ul (sistemul de nume de domeniu) preferat de la ISP. **Server Address** trebuie să fie introdusă cu adresa IP-ului static al computerului pe care rulează software-ul serverului IP.



The screenshot shows a web form for configuring DDNS. At the top, there is a checkbox labeled 'Enable DDNS' which is checked. Below it, the 'DDNS Type' is set to 'IPServer' in a dropdown menu. The 'Server Address' field contains the IP address '212.15.10.121'. The 'Domain' field is empty. The 'Port' field contains the value '0'. The 'User Name' and 'Password' fields are empty. The 'Confirm' field is also empty.

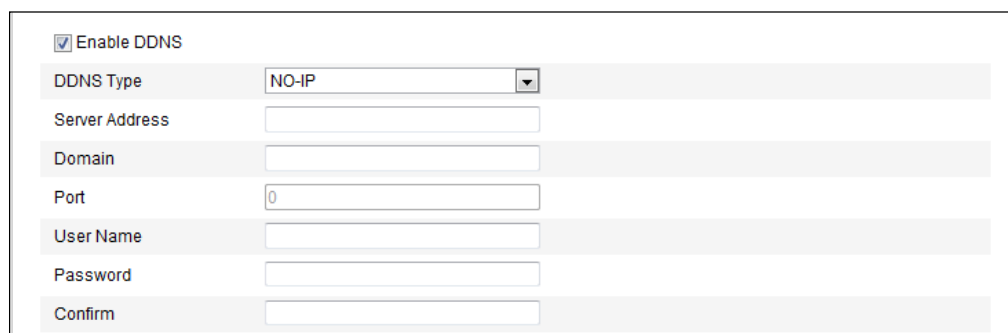
Figura 5–11 Setările serverului IP

Notă: Pentru zona Statelor Unite și a Canadei, puteți introduce 173.200.91.74 ca adresă a serverului.

- NO-IP:

Pași:

(1) Alegeți DDNS Type ca NO-IP.



The screenshot shows the same DDNS configuration form as Figure 5-11, but with 'DDNS Type' set to 'NO-IP'. The 'Server Address' field is empty. The 'Domain' field is empty. The 'Port' field contains the value '0'. The 'User Name' and 'Password' fields are empty. The 'Confirm' field is also empty.

Figura 5–12 Setările NO-IP

(2) Introduceți adresa serverului ca www.noip.com

(3) Introduceți numele domeniului pe care l-ați înregistrat.

- (4) Introduceți numărul portului, dacă este necesar.
- (5) Introduceți numele de utilizator și parola.
- (6) Faceți clic pe **Save**, după care puteți vizualiza camera cu numele domeniului.

- HiDDNS

Pași:

- (1) Alegeți DDNS Type ca HiDDNS.

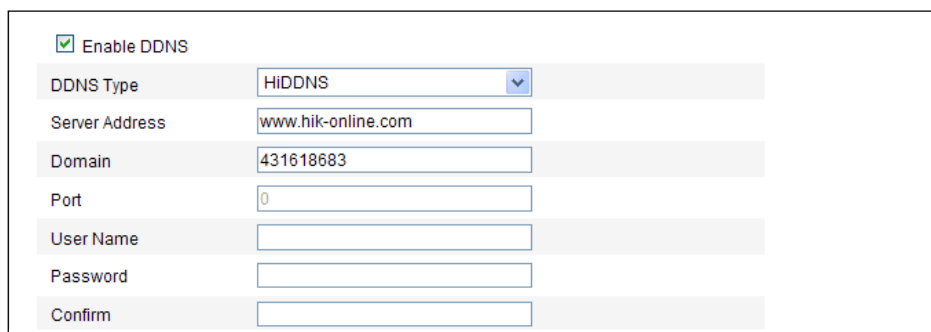


Figura 5–13 Setările HiDDNS

- (2) Introduceți adresa de server *www.hik-online.com*.
- (3) Introduceți numele domeniului camerei. Domeniul este același cu aliasul dispozitivului de pe serverul HiDDNS.
- (4) Faceți clic pe **Save** pentru a salva noile setări.

Notă: Repornirea este necesară pentru ca setările să aibă efect.

5.3.5 Configurare Setări SNMP

Scopul:

Puteți seta funcția SNMP (protocolul simplu de gestionare a rețelei) pentru a obține informații despre starea camerei, despre parametri și despre alarme și pentru a gestiona de la distanță camera atunci când aceasta este conectată la rețea.

Înainte de a începe:

Înainte de a seta SNMP, descărcați software-ul SNMP și configurați primirea informațiilor despre cameră prin portul SNMP. Dacă setați Trap Address, camera poate trimite evenimentul de alarmă și mesajele de excepție la centrul de supraveghere.

Notă: Versiunea de SNMP selectată trebuie să fie aceeași cu cea a software-ului SNMP. De asemenea, trebuie să utilizați versiunea diferită în funcție de nivelul de securitate pe care l-ați solicitat. SNMP v1 nu asigură nicio securitate. SNMP v2 necesită o parolă pentru acces. SNMP v3 asigură criptare. Și, dacă utilizați cea de-a treia versiune, trebuie să activați protocolul HTTPS.



- *Pentru confidențialitatea dvs. și pentru a vă proteja mai bine sistemul împotriva riscurilor de securitate, vă recomandăm să utilizați parole puternice pentru toate funcțiile și dispozitivele de rețea. Parola trebuie să fie aleasă de către dvs. (folosind minimum 8 caractere, printre care majuscule, minuscule, cifre și caractere speciale) pentru a crește siguranța produsului dvs.*
- *Configurarea adecvată a tuturor parolelor și a altor setări de securitate este responsabilitatea instalatorului și/sau a utilizatorului final.*

Pași:

1. Accesați interfața Setări SNMP:

Configuration > Advanced Configuration > Network > SNMP

SNMP v1/v2	
Enable SNMPv1	☐
Enable SNMP v2c	☐
Write SNMP Community	private
Read SNMP Community	public
Trap Address	
Trap Port	162
Trap Community	public
SNMP v3	
Enable SNMPv3	☐
Read UserName	
Security Level	no auth, no priv
Authentication Algorithm	☒ MD5 ☐ SHA
Authentication Password	
Private-key Algorithm	☒ DES ☐ AES
Private-key password	
Write UserName	
Security Level	no auth, no priv
Authentication Algorithm	☒ MD5 ☐ SHA
Authentication Password	
Private-key Algorithm	☒ DES ☐ AES
Private-key password	
SNMP Other Settings	
SNMP Port	161

Figura 5–14 Setări SNMP

2. Bifați caseta versiunii corespunzătoare (**Enable SNMPv1**, **Enable SNMPv2c** și **Enable SNMPv3**) pentru a activa funcționalitatea respectivă.

3. Configurare setări SNMP.

Notă: Setările software-ului SNMP trebuie să fie identice cu setările pe care le configurați aici.

4. Faceți clic pe **Save** pentru a salva și termina setările.

Notă: Repornirea este necesară pentru ca setările să aibă efect.

5.3.6 Configurare setări 802.1X

Scopul:

Standardul IEEE 802.1X este acceptat de către camerele de rețea. Atunci când funcționalitatea este activată, datele camerei sunt securizate și autentificarea utilizatorului este necesară în momentul conectării camerei la rețeaua protejată de către IEEE 802.1X.

Înainte de a începe:

Serverul de autentificare trebuie să fie configurat. Aplicați și înregistrați un nume de utilizator și o parolă pentru 802.1X în server.



- *Pentru confidențialitatea dvs. și pentru a vă proteja mai bine sistemul împotriva riscurilor de securitate, vă recomandăm să utilizați parole puternice pentru toate funcțiile și dispozitivele de rețea. Parola trebuie să fie aleasă de către dvs. (folosind minimum 8 caractere, printre care majuscule, minuscule, cifre și caractere speciale) pentru a crește siguranța produsului dvs.*
- *Configurarea adecvată a tuturor parolelor și a altor setări de securitate este responsabilitatea instalatorului și/sau a utilizatorului final.*

Pași:

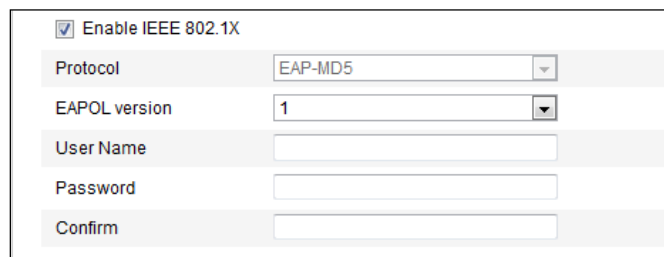
1. Accesați interfața Setări 802.1X:

Configuration > Advanced Configuration > Network > 802.1X

2. Bifați caseta de selectare **Enable IEEE 802.1X** pentru a activa caracteristica.
3. Configurați setările 802.1X, inclusiv versiunea de EAPOL (protocolul extensibil de autentificare prin rețeaua locală), numele de utilizator și parola.

Notă: Versiunea de EAPOL trebuie să fie identică cu cea a routerului sau a switchului.

4. Introduceți numele de utilizator și parola pentru accesarea serverului.



☒ Enable IEEE 802.1X
Protocol: EAP-MD5
EAPOL version: 1
User Name:
Password:
Confirm:

Figura 5–15 Setări 802.1X

5. Faceți clic pe **Save** pentru a finaliza setările.

Notă: Repornirea este necesară pentru ca setările să aibă efect.

5.3.7 Configurare Setări QoS

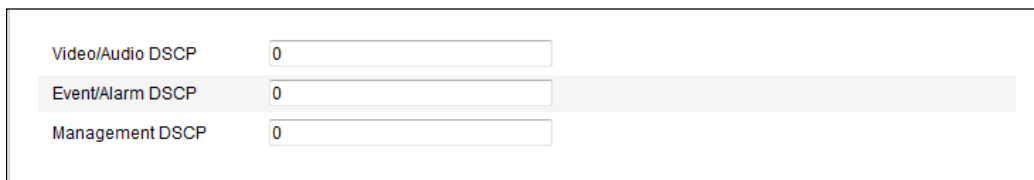
Scopul:

QoS (Quality of Service) poate ajuta în soluționarea întârzierii și a aglomerației în rețea prin configurarea priorității trimiterii de date.

Pași:

1. Accesați interfața Setări QoS:

Configuration > Advanced Configuration > Network > QoS



Video/Audio DSCP	0
Event/Alarm DSCP	0
Management DSCP	0

Figura 5–16 Setări QoS

2. Configurați setările QoS, inclusiv DSCP-ul video/audio, DSCP-ul de eveniment/de alarmă și DSCP-ul de gestionare.

Intervalul valoric valid al DSCP-ului este 0-63. Cu cât valoarea DSCP este mai mare, cu atât este mai mare prioritatea.

Notă: DSCP se referă la Punct de cod de servicii diferențiate; iar valoarea DSCP este utilizată în antetul IP pentru a indica prioritatea datelor.

3. Faceți clic pe **Save** pentru a salva setările.

Notă: Repornirea este necesară pentru ca setările să aibă efect.

5.3.8 Configurarea setărilor UPnP™

Universal Plug and Play (UPnP™) este o arhitectură de rețea care oferă compatibilitate între echipamentele de rețea, software și alte dispozitive hardware. Protocolul UPnP permite conectarea neperturbată a dispozitivelor și simplificarea implementării rețelelor în mediile private și în cele corporative.

Cu această funcție activată, nu este nevoie să configurați maparea porturilor pentru fiecare port iar camera se conectează la WAN prin intermediul routerului.

Pași:

1. Accesați interfața Setări UPnP™.

Configuration > Advanced Configuration > Network > UPnP™

2. Bifați caseta de selectare pentru a activa funcția UPnP™.

Numele dispozitivului, atunci când acesta este detectat on-line, poate fi editat.



Figura 5–17 Setările UPnP™

5.3.9 Trimiterea de e-mailuri declanșată de o alarmă

Scopul:

Sistemul poate fi configurat pentru a trimite o notificare prin e-mail către toate receptoarele desemnate dacă este detectat un eveniment de alarmă, de exemplu, eveniment de detectare mișcare, pierdere video, modificare nepermisă video etc.

Înainte de a începe:

Configurați setările serverului DNS din **Basic Configuration > Network > TCP/IP** sau din **Advanced Configuration > Network > TCP/IP** înainte de a utiliza funcția E-mail.

Pași:

1. Accesați setările TCP/IP (**Configuration > Basic Configuration > Network > TCP/IP** sau **Configuration > Advanced Configuration > Network > TCP/IP**) pentru a seta adresa IPv4, masca de subrețea IPv4, gateway-ul IPv4 implicit și serverul DNS preferat.

Notă: Consultați *Secțiunea 5.3.1 Configurare Setări TCP/IP* pentru informații detaliate.

- Accesați interfața Setări email:

Configuration > Advanced Configuration > Network > Email

The screenshot displays the 'Email' configuration page. It is divided into two main sections: 'Sender' and 'Receiver'.
Sender Section:
 - 'Sender' field: Test
 - 'Sender's Address' field: Test@gmail.com
 - 'SMTP Server' field: smtp.263xmail.com
 - 'SMTP Port' field: 25
 - 'Enable SSL' checkbox: unchecked
 - 'Interval' dropdown: 2s
 - 'Attached Image' checkbox: unchecked
 - 'Authentication' checkbox: unchecked
 - 'User Name' field: empty
 - 'Password' field: empty
 - 'Confirm' field: empty
Receiver Section:
 - 'Receiver1' field: Test1
 - 'Receiver1's Address' field: Test1@gmail.com
 - 'Receiver2' field: empty
 - 'Receiver2's Address' field: empty
 - 'Receiver3' field: empty
 - 'Receiver3's Address' field: empty
 A 'Save' button is located at the bottom right of the form.

Figura 5–18 Setări email

- Configurați setările următoare:

Sender: Numele expeditorului de email.

Sender's Address: Adresa de email a expeditorului.

SMTP Server: Numele gazdei sau adresa IP a serverului SMTP (de exemplu, smtp.263xmail.com).

SMTP Port: Portul SMTP. Portul TCP/IP implicit pentru SMTP este 25 (nesecurizat). Iar portul SSL SMTP este 465.

Enable SSL: Bifați caseta de selectare pentru a activa SSL dacă serverul SMTP solicită acest lucru.

Attached Image: Bifați caseta de selectare a Attached Image dacă doriți să trimiteți e-mailuri cu imaginile de alarmă atașate.

Interval: Intervalul se referă la timpul dintre două acțiuni de trimitere a imaginilor atașate.

Authentication (optional): Dacă serverul de e-mail necesită autentificare, bifați această casetă de selectare pentru a utiliza autentificarea să vă conectați la acest server și introduceți numele de utilizator și parola de conectare.



- *Pentru confidențialitatea dvs. și pentru a vă proteja mai bine sistemul împotriva riscurilor de securitate, vă recomandăm să utilizați parole puternice pentru toate funcțiile și dispozitivele de rețea. Parola trebuie să fie aleasă de către dvs. (folosind minimum 8 caractere, printre care majuscule, minuscule, cifre și caractere speciale) pentru a crește siguranța produsului dvs.*
- *Configurarea adecvată a tuturor parolelor și a altor setări de securitate este responsabilitatea instalatorului și/sau a utilizatorului final.*

Choose Receiver: Selectați destinatarul căruia îi expediați emailul. Pot fi configurați până la 3 destinatari.

Receiver: Numele utilizatorului ce urmează a fi notificat.

Receiver's Address: Adresa de e-mail a utilizatorului ce urmează a fi notificat.

4. Faceți clic pe **Save** pentru a salva setările.

5.3.10 Configurare Setări NAT (Network Address Translation)

Scopul:

NAT se referă la maparea portului atunci când setarea UPnP™ este activată.

Pași:

1. Deschideți interfața cu setările pentru NAT.

Configuration > Advanced Configuration > Network > NAT

2. Alegeți modul de mapare a portului.

Pentru a mapa porturile cu numerele de porturi implicite:

Alegeți Port Mapping Mode ca **Auto**.

Pentru a mapa porturile cu numerele de porturi personalizate:

Alegeți Port Mapping Mode ca **Manual**.

Iar pentru maparea manuală a portului, puteți personaliza dvs. înșivă valoarea numărului portului.

	Port Type	External Port	External IP Address	Status
☒	HTTP	80	0.0.0.0	Not Valid
☒	RTSP	554	0.0.0.0	Not Valid
☒	Server Port	8000	0.0.0.0	Not Valid

Figura 5–19 Configurarea setărilor NAT

3. Faceți clic pe **Save** pentru a salva setările.

5.3.11 Configurare setări FTP

Scopul:

Puteți configura informațiile corespunzătoare ale serverului FTP pentru a permite încărcarea imaginilor capturate pe serverul FTP. Imaginile capturate pot fi declanșate de evenimente sau de o sarcină de instantaneu sincronizare.

Pași:

1. Accesați interfața Setări FTP:

Configuration > Advanced Configuration > Network > FTP

2. Configurați setările FTP. Numele de utilizator și parola sunt necesare pentru conectarea la serverul FTP.



- Pentru confidențialitatea dvs. și pentru a vă proteja mai bine sistemul împotriva riscurilor de securitate, vă recomandăm să utilizați parole puternice pentru toate funcțiile și dispozitivele de rețea. Parola trebuie să fie aleasă de către dvs. (folosind minimum 8 caractere, printre care majuscule, minuscule, cifre și caractere speciale) pentru a crește siguranța produsului dvs.
- Configurarea adecvată a tuturor parolelor și a altor setări de securitate este responsabilitatea instalatorului și/sau a utilizatorului final.

Directory: Din câmpul **Directory Structure** puteți selecta folderul rădăcină, folderul principal și folderul secundar. Când este selectat directorul părinte, aveți opțiunea de a folosi numele dispozitivului, numărul dispozitivului sau IP-ul dispozitivului pentru numele directorului, iar când directorul copil este selectat, puteți utiliza numele camerei sau numărul camerei ca nume al directorului.

Upload type: Pentru activarea încărcării imaginilor capturate pe serverul FTP.

Acces anonim la serverul FTP (caz în care numele de utilizator și parola nu vor fi solicitate): Bifați caseta de selectare **Anonymous** pentru a permite accesul anonim la serverul FTP.

Notă: Funcția de acces anonim trebuie acceptată de serverul FTP.

Server Address	0.0.0.0
Port	21
User Name	☐ Anonymous
Password	
Confirm	
Directory Structure	Save in the root directory.
Parent Directory	Use Device Name
Child Directory	Use Camera Name
Upload Type	☐ Upload Picture
Test	

Figura 5–20 Setări FTP

3. Faceți clic pe **Save** pentru a salva setările.

Notă: Dacă doriți să încărcați imaginile capturate pe serverul FTP, trebuie să activați instantaneul de sincronizare sau instantaneul declanșat de eveniment de pe pagina **Instantaneu**. Pentru informații detaliate, consultați *Secțiunea 6.4*.

5.3.12 Setări HTTPS

Scopul:

HTTPS oferă autentificarea siteului web și a serverului web asociat cu care se comunică, protejând astfel împotriva atacurilor Man-in-the-middle. Efectuați următorii pași pentru a seta numărul portului https.

De exemplu, dacă setați numărul portului la 443 și adresa IP este 192.168.1.64, puteți accesa dispozitivul introducând https://192.168.1.64:443 în browserul web.

Pași:

1. Deschideți interfața cu setările pentru HTTPS.

Configuration > Advanced Configuration > Network > HTTPS

☐ Enable HTTPS

Create

Create Self-signed Certificate

Create Certificate Request

Install Signed Certificate

Certificate Path

Created Request

Created Request

Installed Certificate

Installed Certificate	C=CN, ST=ZJ, L=HZ, OU=embeddedsoftware, H/IP=192.	Delete
Property	Subject: C=CN, ST=ZJ, L=HZ, OU=embeddedsoftware, H/IP=192.168.1.64, EM=com.cn Issuer: C=CN, ST=ZJ, L=HZ, OU=embeddedsoftware, H/IP=192.168.1.64, EM=com.cn Validity: 2015-07-23 14:29:46 ~ 2018-07-22 14:29:46	

Figura 5–21 setările HTTPS

2. Bifați caseta Enable HTTPS pentru a activa această funcționalitate.
 3. Creați certificatul auto-semnat sau certificatul autorizat.
 - Creare certificat auto-semnat
- 1) Faceți clic pe butonul **Create** pentru a intra în interfața de creare.

Create

Create Self-signed Certificate

Create Certificate Request

Install Signed Certificate

Certificate Path

Created Request

Created Request

Installed Certificate

Installed Certificate

Figura 5–22 Creare certificat auto-semnat

2) Introduceți țara, numele gazdei/adresa IP, validitatea și alte informații.

Country	* example:CN
Hostname/IP	*
Password	
State or province	
Locality	
Organization	
Organizational Unit	
Email	
OK Cancel	

Figura 5–23 Crearea unui certificat

3) Faceți clic pe **OK** pentru a salva setările.

Notă: Dacă aveți deja un certificat instalat, zona Creare certificat autosemnat este colorată în gri deschis.

- Creați certificatul autorizat

1) Faceți clic pe butonul **Create** pentru a crea cererea de certificat.

2) Descărcați solicitarea de certificat și trimiteți-o la autoritatea de certificare de încredere pentru semnătură.

3) După ce primiți certificatul valid semnat, importați certificatul pe dispozitiv.

4. Vor exista informații despre certificat după ce creați și instalați cu succes certificatul.

Installed Certificate	
Installed Certificate	C=CN, ST=ZJ, L=HZ, OU=embeddedsoftware, H/IP=192.168.1.64, EM=com.cn Delete
Property	Subject: C=CN, ST=ZJ, L=HZ, OU=embeddedsoftware, H/IP=192.168.1.64, EM=com.cn Issuer: C=CN, ST=ZJ, L=HZ, OU=embeddedsoftware, H/IP=192.168.1.64, EM=com.cn Validity: 2015-07-23 14:29:46 ~ 2018-07-22 14:29:46

Figura 5–24 Certificat instalat

5. Faceți clic pe butonul **Save** pentru a salva setările.

5.4 Configurare setări video și audio

5.4.1 Configurare setări video

Pași:

1. Accesați interfața Setări video:

Configuration > Basic Configuration > Video/Audio > Video

Sau **Configuration > Advanced Configuration > Video/Audio > Video**

Setting	Value	Unit
Stream Type	Main Stream(Normal)	
Video Type	Video Stream	
Resolution	640*512	
Bitrate Type	Constant	
Video Quality	Medium	
Frame Rate	50	fps
Max. Bitrate	2048	Kbps
Video Encoding	H.264	
H.264+	OFF	
Profile	High Profile	
I Frame Interval	50	
SVC	OFF	
Smoothing	50	

Figura 5–25 Setări video

2. Selectați **tipul de flux** al camerei ca flux principal (normal), flux secundar sau flux terțiar. Fluxul principal este în mod normal pentru înregistrare și vizualizare live cu lungime de bandă bună și fluxul secundar poate fi utilizat pentru vizualizare live atunci când lungimea de bandă este limitată.
3. Puteți personaliza următorii parametri pentru fluxul principal sau fluxul secundar selectate:

Video Type:

Selectați tipul de flux ca flux video sau ca flux combinat audio-video. Semnalul audio poate fi înregistrat doar atunci când **Video Type** este selectat ca **Video & Audio**.

Resolution:

Selectați rezoluția pentru ieșirea video.

Bitrate Type:

Selectați tipul de rată a biților ca și constantă sau ca variabilă.

Video Quality:

Atunci când tipul de rată a biților este selectat ca **Variable**, puteți selecta 6 niveluri de calitate video.

Frame Rate:

Setați frecvența cadrelor la 1/16~25 fps. Rata de cadre descrie frecvența cu care fluxul video este actualizat și este măsurată în cadre per secundă (fps). O rată de cadre mai mare este avantajoasă în cazuri în care există mișcare în fluxul video deoarece păstrează constantă calitatea imaginii.

Max. Bitrate:

Setați rata maximă a biților la 256~16384 Kbps. Cu cât este mai mare valoarea cu atât este mai ridicată calitatea video însă, este necesară o lungime de bandă mai mare.

Notă: Limita maximă a valorii maxime de transfer variază în funcție de diversele platforme de cameră. Pentru anumite camere, limita maximă este de 8192 Kbps sau de 12288 Kbps.

Video Encoding:

Dacă **Stream Type** este setat la main stream: Puteți selecta H.264 și MPEG4; dacă stream type este setat la sub stream, puteți selecta H.264, MJPEG și MPEG4.

Notă: Tipul de codificare video variază în funcție de diversele platforme de cameră.

Profile:

Pentru codificare, puteți selecta Basic profile, Main Profile și High Profile.

I Frame Interval:

Setați intervalul Cadru I la 1~400.

SVC:

Codificarea video scalabilă este o extensie a standardului H.264/AVC. Selectați OFF/ON (OPRIT/PORNIT) pentru a dezactiva/activa funcția SVC. Selectați Auto și dispozitivul va extrage automat cadrele din transmisiunea video originală atunci când lățimea de bandă a rețelei este insuficientă.

Smoothing:

Aceasta se referă la corecția fluxului. Cu cât mai mare este valoarea de corecție, cu atât fluenta fluxului este mai bună, totuși, calitatea video poate să nu fie atât de satisfăcătoare. Cu cât mai mare este valoarea de corecție, cu atât mai înaltă este calitatea fluxului, deși, acesta ar putea să nu pară atât de fluent.

4. Faceți clic pe **Save** pentru a salva setările.

5.4.2 Configurare Setări audio

Pași:

1. Accesați interfața Setări audio

Configuration > Basic Configuration > Video/Audio > Audio

Sau **Configuration > Advanced Configuration > Video/Audio > Audio**

The screenshot shows the 'Audio' configuration page. At the top, there are three tabs: 'Video', 'Audio' (which is highlighted), and 'ROI'. Below the tabs, there are four rows of settings. The first row is 'Audio Encoding' with a dropdown menu showing 'G.711ulaw'. The second row is 'Audio Input' with a dropdown menu showing 'Lineln'. The third row is 'Input Volume' with a horizontal slider bar and a numeric input field showing '50'. The fourth row is 'Environmental Noise Filter' with a dropdown menu showing 'OFF'. At the bottom right of the form, there is a 'Save' button.

Figura 5–26 Setări audio

2. Configurați următoarele setări.

Notă: Setările audio variază în funcție de diferitele modele de cameră.

Audio Encoding: Puteți selecta G.722.1, G.711 ulaw, G.711alaw, G.726, MP2L2, AAC și PCM. Pentru MP2L2, puteți configura rata de eșantionare și rata de biți a fluxului audio; pentru PCM, puteți seta rata de eșantionare.

Audio Input: MicIn și LineIn sunt selectabile pentru microfonul conectat și respectiv preluare.

Input Volume: 0-100

Environmental Noise Filter: Setăți-l ca OFF sau ON. Atunci când această funcție este activată, zgomotul din mediu poate fi atenuat într-o anumită măsură.

3. Faceți clic pe **Save** pentru a salva setările.

5.4.3 Configurarea codificării ROI

Scopul:

Codificarea ROI (regiune de interes) contribuie la diferențierea între ROI și informațiile de fundal în timpul comprimării video, ceea ce înseamnă că tehnologia atribuie mai multe resurse de codificare regiunii de interes, pentru a crește, astfel, calitatea ROI, în timp ce informațiilor de fundal li se acordă mai puțină atenție.

Notă: Funcția ROI variază în funcție de diversele modele de cameră.

Configurarea regiunii fixe pentru ROI:

Pași:

1. Accesați interfața Setări ROI:

Configuration > Advanced Configuration > Video/Audio > ROI

2. Bifați caseta de selectare a **Enable** sub articolul Fixed Region.
3. Selectați tipul de flux pentru codificarea ROI.
4. Selectați regiunea din lista verticală Nr. regiune pentru setările ROI. Se pot selecta patru regiuni fixe.
5. Faceți clic pe butonul **Draw Area**, după care faceți clic și glisați mouse-ul pentru a desena regiunea de interes peste transmisiunea video live.
6. Selectați nivelul de ROI pentru a seta nivelul de îmbunătățire a calității imaginii. Cu cât valoarea este mai mare, cu atât este mai bună calitatea imaginii.

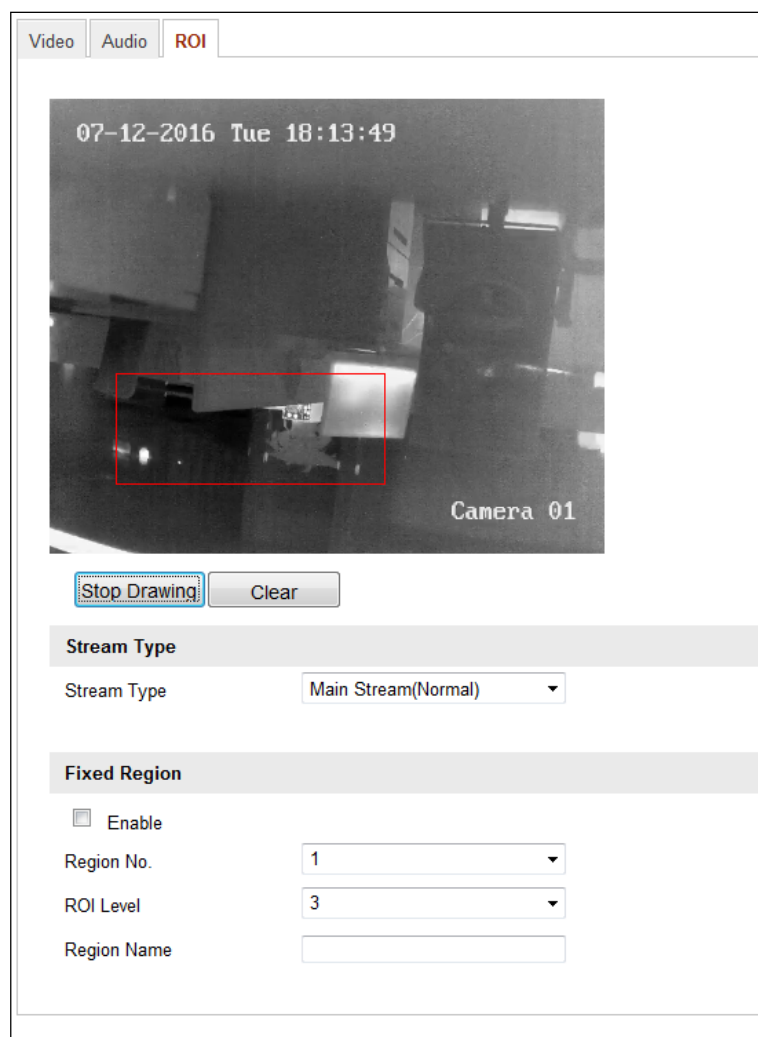


Figura 5–27 Setări regiune de interes

7. Introduceți numele regiunii pentru ROI, după preferințe.
8. Faceți clic pe **Save** pentru a salva setările.

5.5 Configurare parametri imagine

5.5.1 Configurare Setări de afișare

Scopul:

Puteți seta calitatea imaginii camerei, inclusiv luminozitatea, contrastul etc.

Notă: Parametrii de afișaj variază în funcție de diferitele modele de camere.

Consultați interfața actuală pentru detalii.

Pași:

1. Accesați interfața Display Settings:

Configuration > Basic Configuration > Image > Display Settings

Sau **Configuration > Advanced Configuration > Image > Display Settings**

2. Setați parametrii de imagine ai camerei.

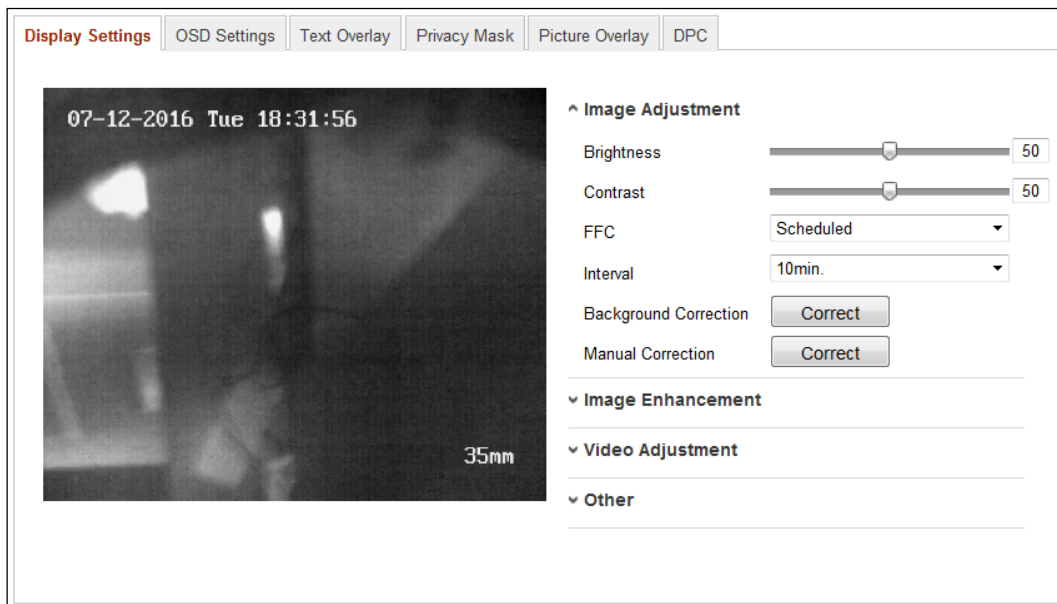


Figura 5–28 Configurarea setărilor de afișare pentru Camera 2

- **Reglare imagine**

Brightness descrie cât de luminoasă este imaginea, într-un interval de la 1 la 100, iar valoarea implicită este 50.

Contrast descrie contrastul imaginii, într-un interval de la 1 la 100, iar valoarea implicită este 50.

FFC (corecția câmpului plan) îmbunătățește calitatea imaginilor digitale. Poate elimina artefactele din imaginile 2-D provocate de variațiile de sensibilitate de la pixel la pixel ale detectorului sau de perturbările din calea optică. Puteți selecta Programare, Temperatură și OFF (OPRIT).

- **Schedule:** Puteți selecta intervalul de corecție dintre 10, 20, 30, 40, 50, 60, 120, 180 și 240 de minute.
- **Temperature:** Camera reglează imaginea în funcție de temperatură.

Manual Background Correction: Acoperiți complet obiectivul cu un obiect (se recomandă utilizarea capacului obiectivului) și faceți clic pe butonul Manual Background Correction, după care camera reglează imaginea în funcție de mediul curent.

Manual Shutter Correction: Faceți clic pe butonul Manual Shutter Correction, după care camera reglează imaginea în funcție de temperatura proprie a camerei.

- **Îmbunătățire imagine**

Digital Noise Reduction: DNR reduce zgomotul în fluxul video. Puteți selecta OFF, Normal și Expert. Setați nivelul DNR (atenuarea digitală a zgomotului) de la 0 la 100 în modul Normal. Setați nivelul DNR atât pentru nivelul DNR spațial [0-100], cât și pentru nivelul DNR temporal [0-100] în modul Expert.

Palettes: Paletele vă permit să selectați culorile dorite. Puteți selecta white hot, black hot, fusion 1, rainbow, fusion 2, ironbow 1, ironbow 2, sepia, color 1, color 2, ice fire, rain, red hot și green hot.

DDE: DDE (mărirea digitală a detaliilor) poate regla detaliile imaginii. Și o puteți seta la modul OFF sau Normal. Iar Nivel DDE poate fi reglat de la 1 la 100 în modul Normal.

- **Ajustare video**

Mirror: Reflectă imaginea pentru a o putea vedea inversată. Puteți selecta Left/Right, Up/Down, Center și OFF.

Video Standard: puteți selecta 50 Hz și 60 Hz. Alegeți în funcție de diferitele standarde video; în mod normal 50 Hz pentru standardul PAL și 60 Hz pentru standardul NTSC.

Capture Mode: Este modul de intrare video selectabil pentru a satisface cerințele diferite ale câmpului vizual și rezoluției.

Digital Zoom: Selectați panoramarea digitală ca OFF (OPRIT), 2X sau 4X pentru a afișa vizualizarea live la dimensiunea originală, ca panoramare

digitală la dimensiunea 2X sau ca panoramare digitală la dimensiunea 4X.

- **Altele**

Local Output: Activați sau dezactivați ieșirea locală a dispozitivului.

3. (Opțional) Faceți clic pe **Default** pentru a restabili setările implicite

5.5.2 Configurarea setărilor OSD

Scopul:

Puteți personaliza numele camerei și ora de pe ecran.

Pași:

1. Accesați interfața OSD Settings:

Configuration > Advanced Configuration > Image > OSD Settings

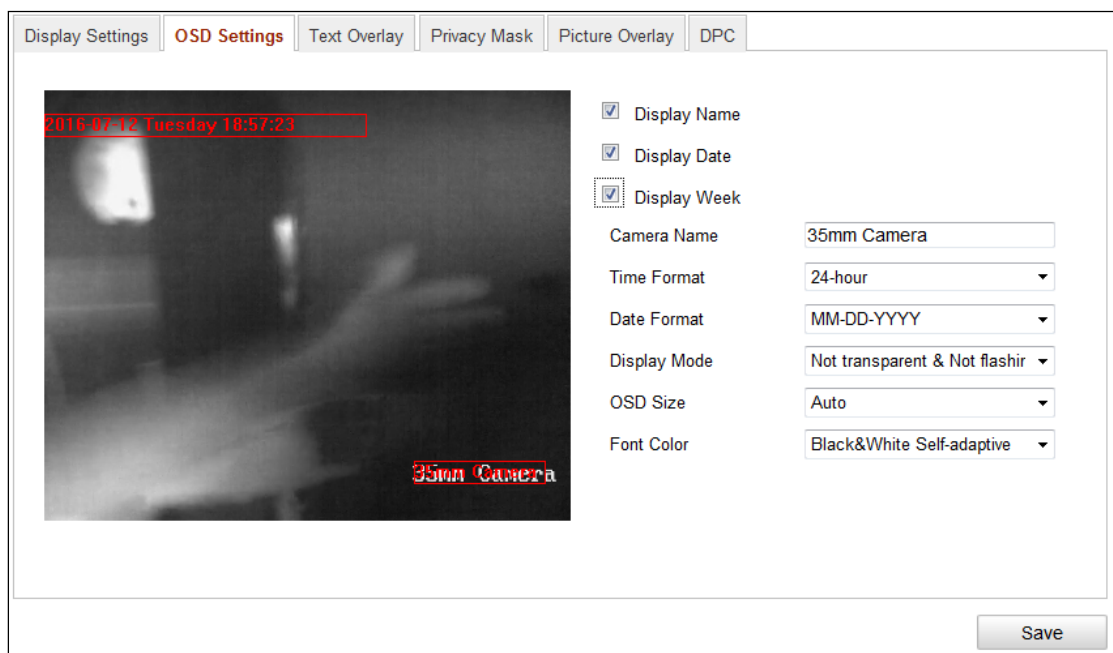


Figura 5–29 Setări OSD

2. Bifați caseta de selectare corespunzătoare pentru a selecta afișarea numelui camerei, data sau săptămâna dacă este necesar.
3. Editați numele camerei în câmpul de text **Camera Name**.
4. Selectați din lista verticală pentru a seta formatul orei, formatul datei, modul de afișare și dimensiunea fonturilor afișate pe ecran.
5. Definiți culoarea fonturilor afișate pe ecran făcând clic pe lista verticală și puteți

selecta black & white self-adaptive și custom.

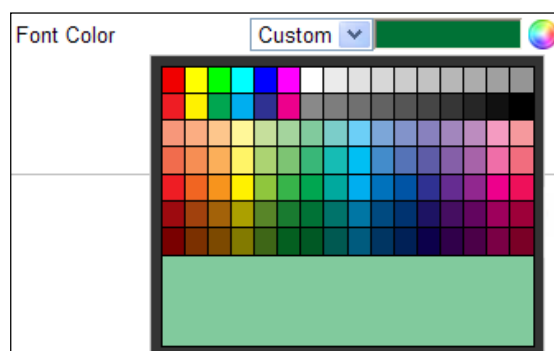


Figura 5–30 Culoarea fonturilor-Personalizare

6. Puteți utiliza mouse-ul pentru a face clic și a glisa cadrul de text **35mm Camera** în fereastra de vizualizare live pentru a regla poziția afișării pe ecran.

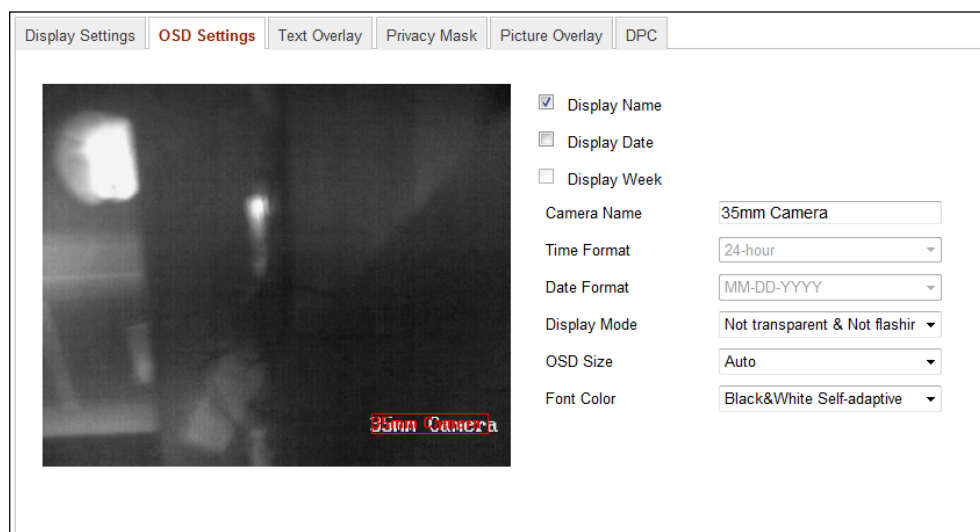


Figura 5–31 Reglarea poziționării afișării pe ecran

7. Faceți clic pe **Save** pentru a activa setările anterioare.

5.5.3 Configurare Setări suprapunere text

Scopul:

Puteți personaliza suprapunerea textului.

Pași:

1. Accesați interfața Setări suprapunere text:

Configuration > Advanced Configuration > Image > Text Overlay

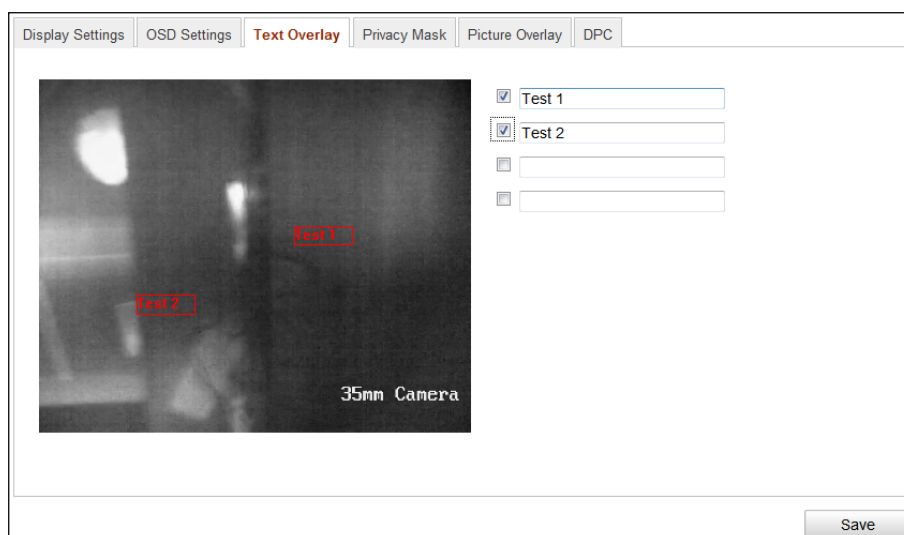


Figura 5–32 Suprapunerea textului

2. Bifați caseta de selectare din dreptul casetei de text pentru a activa afișarea pe ecran.
3. Introduceți caracterele în caseta de text.
4. (Opțional) Utilizați mouse-ul pentru a face clic și a glisa cadrul de text de culoare roșie **Test 1** în fereastra de vizualizare live pentru a regla poziția suprapunerii textului.
5. Faceți clic pe **Save** pentru a salva setările.

Notă: Sunt configurabile până la 8 suprapuneri de text.

5.5.4 Configurarea măștii de confidențialitate

Scopul:

Masca de confidențialitate vă permite să acoperiți anumite zone de pe videoul live pentru a preveni anumite vizualizări live și înregistrarea anumitor porțiuni din zona de supraveghere.

Pași:

1. Accesați interfața Setări Mască de confidențialitate:

Configuration > Advanced Configuration > Image > Privacy Mask

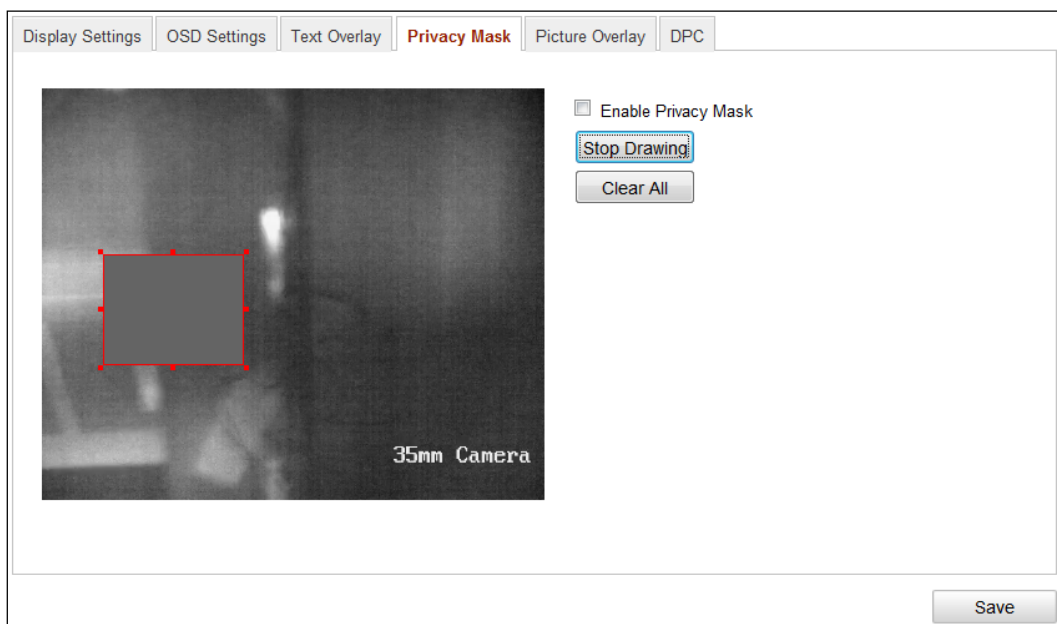


Figura 5–33 Setările mască de confidențialitate

2. Bifați caseta de selectare **Enable Privacy Mask** pentru a activa această funcționalitate.
3. Faceți clic pe **Draw Area**.
4. Faceți clic și glisați mouse-ul în fereastra video-ului live pentru a desena o zonă de mască.
Notă: Puteți desena până la 4 de zone pe aceeași imagine.
5. Faceți clic pe **Stop Drawing** pentru a termina desenul sau faceți clic pe **Clear All** pentru a șterge toate zonele pe care le-ați setat fără a le salva.
6. Faceți clic pe **Save** pentru a salva setările.

5.5.5 Configurarea suprapunerii de imagine

Scopul:

Suprapunerea de imagine vă permite să suprapuneți o imagine peste o altă imagine. Această funcție permite unei întreprinderi sau utilizatorilor să suprapună logo-ul lor pe imagine.

Notă: Desenul trebuie să fie în formatul RGB24 bmp, iar dimensiunea maximă a desenului este de 128*128.

Pași:

1. Accesați interfața Setări suprapunere imagine:

Configuration > Advanced Configuration > Image > Picture Overlay

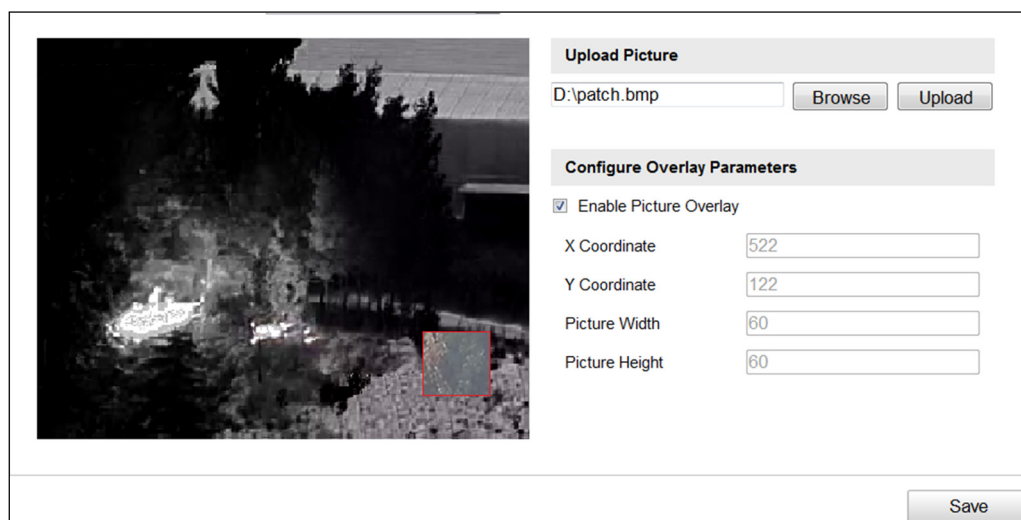


Figura 5–34 Suprapunere de imagine

2. Faceți clic pe **Browse** pentru a selecta un desen.
3. Faceți clic pe Încărcare pentru a-l încărca.
4. Bifați caseta Activare suprapunere imagine pentru a activa această funcționalitate.

Valorile Coordonatei X și Coordonatei Y sunt setate pentru amplasarea desenului pe imagine. Iar lățimea și înălțimea desenului indică dimensiunea desenului.

5. Faceți clic pe **Save** pentru a salva setările.

5.5.6 Configurarea DPC (corecția pixelilor defecti)

Scopul:

DPC (corecția pixelilor defecti) se referă la funcția prin care camera poate corecta pixelii defecti de pe LCD, a căror performanță nu este cea preconizată.

Notă: Această funcție nu este disponibilă decât pentru anumite modele de cameră.

Pași:

1. Accesați interfața Setări DPC.

Configuration > Advanced Configuration > Image > DPC

2. Faceți clic pe imagine pentru a selecta un pixel defect. Cursorul de pe imagine se va deplasa către locul în care ați făcut clic. Puteți face clic pe  pentru a regla ușor poziția cursorului.

3. Faceți clic pe  pentru a iniția corecția.



Figura 5–35 Corecția pixelilor defecti

4. (Opțional) Faceți clic pe  pentru a anula corecția.

5.6 Configurarea și tratarea evenimentelor de alarmă

În această secțiune este explicat modul de configurare a camerei de rețea astfel încât să reacționeze la evenimentele de alarmă, inclusiv la detectarea mișcării, la modificarea nepermisă video, la intrarea alarmei, la ieșirea alarmei, la excepții, la detectarea feței, la detectarea excepției audio, la detectarea intruziunii, la detectarea defocalizării, la detectarea schimbării scenei etc. Aceste evenimente pot declanșa metode de conectare sau de legare, cum ar fi Înștiințare centru de supraveghere, Trimitere e-mail, Declanșare ieșire alarmă etc.

Note:

- Bifați caseta Înștiințare centru de supraveghere dacă doriți ca informațiile despre alarme să fie transmise PC-ului sau software-ului client mobil de îndată ce alarma este declanșată.

- Faceți clic pe  pentru ajutor atunci când configurați funcțiile inteligente, inclusiv detectarea feței, detectarea excepției audio, detectarea intruziunii, detectarea defocalizării, detectarea schimbării scenei etc. Un document de ajutor vă va susține să parcurgeți pașii de configurare.

5.6.1 Configurare Detecție mișcare

Scopul:

Detectarea mișcării detectează obiectele în mișcare în zona de supraveghere configurată și o serie de măsuri pot fi luate atunci când alarma este declanșată.

Pentru a detecta obiectele în mișcare cu precizie și a reduce rata alarmelor false, configurarea normală și configurarea expert sunt selectabile pentru diferite medii de detectare a mișcării.

- **Configurarea obișnuită**

În cazul configurării obișnuite este adoptat același set de parametri de detectare a mișcării pe timpul zilei și pe timpul nopții.

Sarcina 1: Setarea zonei de detectare a mișcării.

Pași:

- (1) Accesați interfața setărilor de detectare a mișcării

Configuration > Advanced Configuration > Basic Event > Motion Detection

- (2) Bifați caseta de selectare pentru **Enable Motion Detection**.

- (3) Bifați caseta **Enable Dynamic Analysis for Motion** dacă doriți ca obiectele detectate să fie marcate cu dreptunghiuri de culoare verde în transmisiunea video live.

Notă: Pentru a activa/dezactiva marcarea obiectelor mișcării în transmisiunea video live, mergeți la Local Configuration > Live View Parameters și activați/dezactivați Regulile.

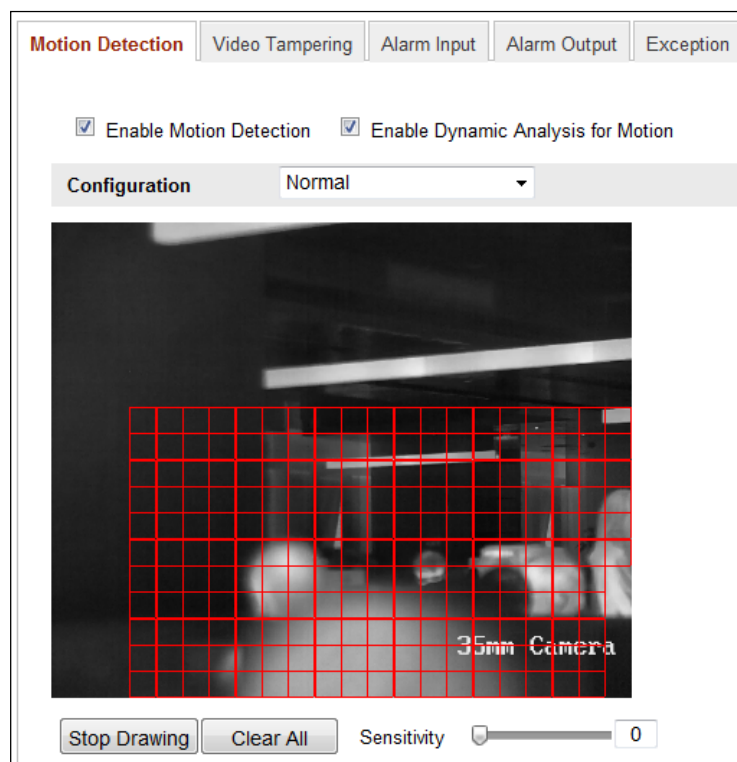


Figura 5–36 Permiteți detectarea mișcării

- (4) Faceți clic pe **Draw Area**. Faceți clic și glisați mouse-ul pe video-ul live pentru a desena o zonă de detectare a mișcării.
- (5) Faceți clic pe **Stop Drawing** pentru a termina de desenat o zonă.
- (6) (Opțional) Faceți clic pe **Clear All** pentru a șterge toate zonele.
- (7) (Opțional) Deplasați glisorul pentru a seta sensibilitatea detectării.

Sarcina 2: Setarea programării armării pentru detectarea mișcării.

Pași:

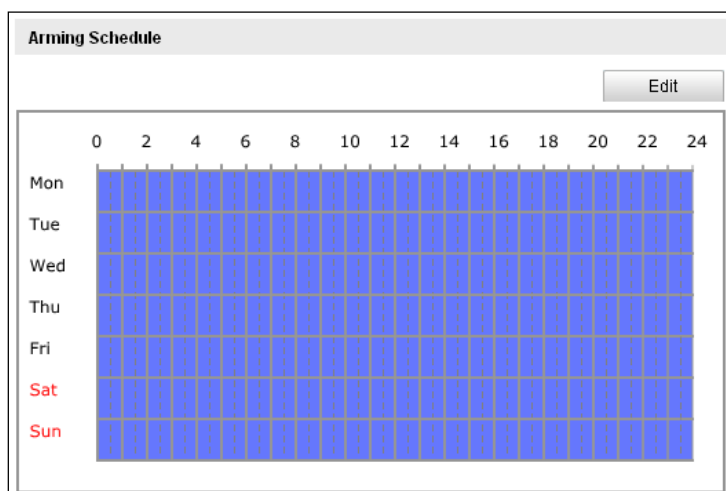
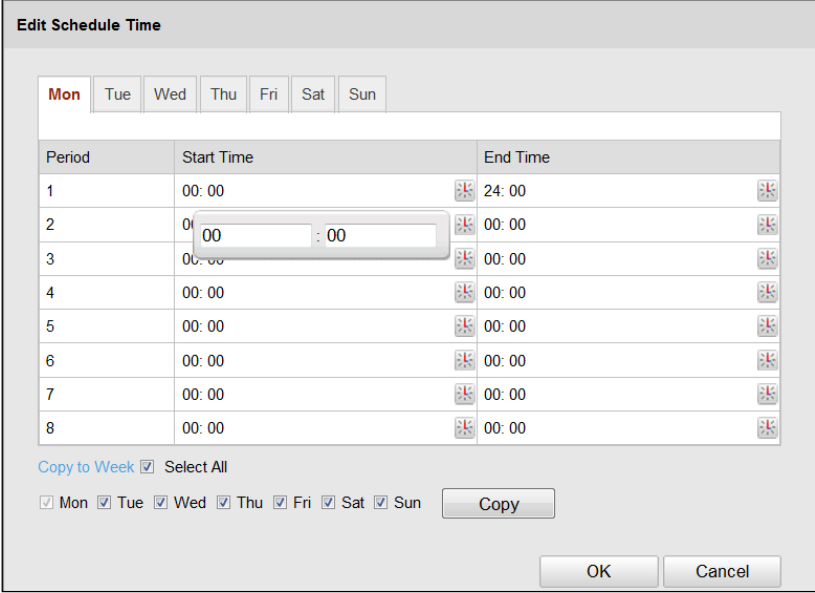


Figura 5–37 Momentul armării

- (1) Faceți clic pe **Edit** pentru a edita programarea armării. În Figura 6-34 este prezentată interfața de editare a programării armării.
- (2) Alegeți ziua pentru care doriți să setați programarea armării.
- (3) Faceți clic pe  pentru a seta intervalul temporal corespunzător programării armării.
- (4) (Opțional) După ce setați programarea armării, puteți copia programarea la alte zile.
- (5) Faceți clic pe **OK** pentru a salva setările.

Notă: Durata fiecărei perioade nu poate fi suprapusă. Pot fi configurate până la 8 perioade pentru fiecare zi.



Period	Start Time	End Time
1	00: 00	24: 00
2	00: 00	00: 00
3	00: 00	00: 00
4	00: 00	00: 00
5	00: 00	00: 00
6	00: 00	00: 00
7	00: 00	00: 00
8	00: 00	00: 00

Copy to Week ☒ Select All

☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☒ Sat ☒ Sun

Copy

OK Cancel

Figura 5–38 Program oră armare

Sarcina 3: Setare Acțiuni alarmă pentru Detecție mișcare.

Bifați caseta de selectare pentru a selecta metoda de legătură. Puteți selecta Notify Surveillance Center, Send Email, Upload to FTP, Trigger Channel și Trigger Alarm Output. Puteți specifica metoda de legătură în momentul în care apare un eveniment.

Linkage Method	
Normal Linkage	Other Linkage
☐ Notify Surveillance Center ☐ Send Email ☐ Upload to FTP Trigger Channel ☐ Select All ☐ D1 ☐ D2	Trigger Alarm Output ☐ Select All ☐ A->1

Figura 5–39 Metodă creare legătură

- **Avertisment audibil**

Declanșați local avertismentul audibil. Această funcție este acceptată numai de către dispozitivul care prezintă o ieșire audio.

- **Notificare centru de supraveghere**

Trimite un semnal de excepție sau de alarmă la un software de gestionare de la de la distanță atunci când are loc un eveniment.

- **Expediere Email**

Trimite un e-mail cu informații despre alarmă către un utilizat sau mai mulți utilizatori atunci când are loc un eveniment.

Notă: Pentru a trimite e-mailuri în momentul producerii unui eveniment, trebuie să consultați *Secțiunea 5.3.9 Trimiterea de e-mailuri declanșată de o alarmă* pentru a seta parametrul corespunzător.

- **Încărcare pe FTP**

Capturați imaginea atunci când alarma este declanșată și încărcați imaginea pe un server FTP.

Note:

- Setati mai întâi adresa FTP și serverul FTP de la distanță. Consultați *Secțiunea 5.3.11 Configurare setări FTP* pentru informații detaliate.
- Mergeți la pagina **Advanced Configuration > Storage > Snapshot**, activați instantaneul declanșat de eveniment și setați intervalul de capturare și numărul de capturi.
- Imaginea capturată poate fi de asemenea încărcată pe cardul SD disponibil sau pe discul de rețea.

● Declanșare canal

Video-ul va fi înregistrat când se detectează mișcare. Trebuie să setați programul de înregistrare pentru această funcție. Consultați *Secțiunea 6.3* pentru informații detaliate.

● Declanșare ieșire alarmă

Declanșarea uneia sau a mai multor ieșiri de alarmă externă atunci când are loc un eveniment.

Notă: Pentru a declanșa o ieșire a alarmei în momentul producerii unui eveniment, consultați *Secțiunea 5.6.4 Configurare ieșire alarmă* pentru a seta parametrii corespunzători.

● Configurare Expert

Modul Expert este utilizat în principal pentru a configura sensibilitatea și proporțiile obiectelor din fiecare zonă pentru diverse comutări zi/noapte.

Notă: Comutarea zi/noapte nu funcționează pentru canalul camerei termice. Dar puteți încă configura Zona, Sensibilitatea și Proporțiile unui obiect din zonă.

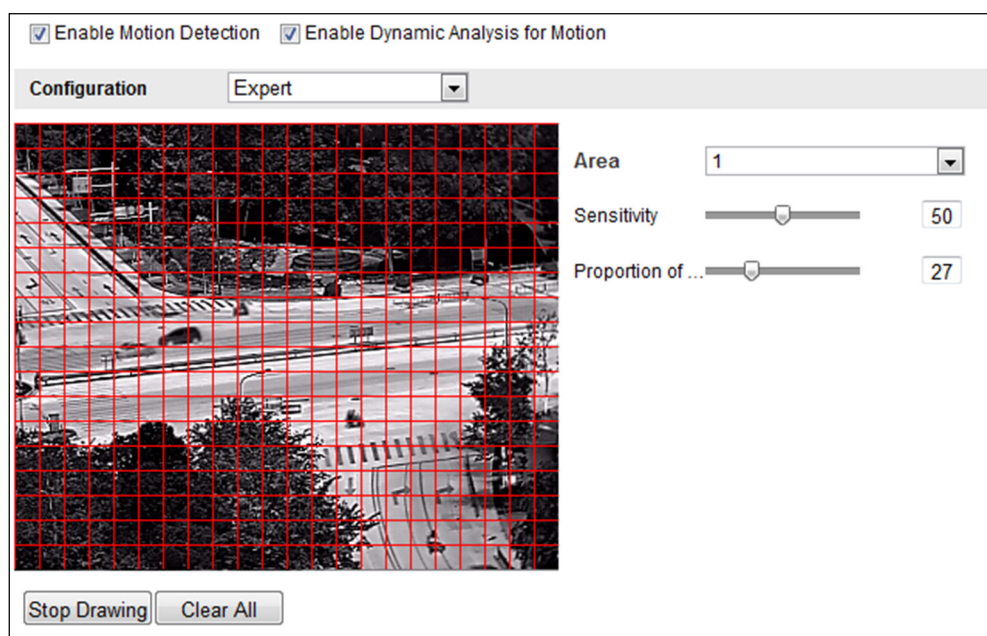


Figura 5–40 Modul expert de detectare a mișcării

5.6.2 Configurare Alarmă corupere video

Scopul:

Puteți configura camera să declanșeze alarma atunci când obiectivul este acoperit și să întreprindă anumite acțiuni ca răspuns la alarmă.

Pași:

1. Accesați interfața Setări Corupere video:

Configuration > Advanced Configuration > Basic Event > Video Tampering

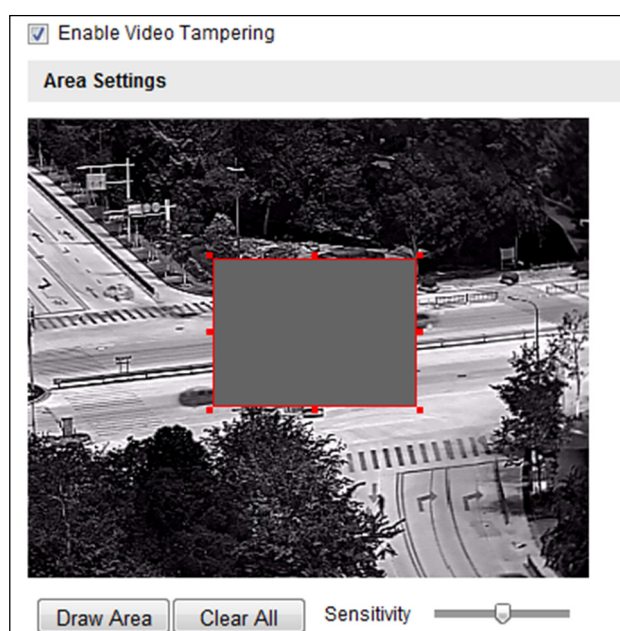


Figura 5–41 Alarma de modificare nepermisă video

2. Bifați caseta de selectare **Enable Video Tampering** pentru a activa detectarea modificare nepermisă video.
3. Setati zona de modificare nepermisă video. Consultați *Sarcina 1 Setarea zonei de detectare a mișcării* din *Secțiunea 5.6.1*.
4. Faceți clic pe **Edit** pentru a edita programul de armare pentru modificare nepermisă video. Configurarea programului de armare este aceeași ca setarea programului de armare pentru detecție mișcare. Consultați *Sarcina 2 Setarea programării armării pentru detectarea mișcării* din *Secțiunea 5.6.1*.

5. Bifați caseta de selectare pentru a selecta metoda de conectare pentru modificare nepermisă video. Puteți selecta avertismentul sonor, înștiințarea centrului de supraveghere, trimiterea de e-mailuri și declanșarea ieșirii alarmei. Consultați *Sarcina 3 Setarea acțiunilor de alarmă pentru detectarea mișcării* din *Secțiunea 5.6.1*.
6. Faceți clic pe **Save** pentru a salva setările.

5.6.3 Configurare Intrare alarmă

Scopul:

Detectează intrarea alarmei și întreprinde acțiuni de răspuns în momentul declanșării alarmei.

Pași:

1. Accesați interfața Setări intrare alarmă:

Configuration > Advanced Configuration > Basic Event > Alarm Input

2. Alegeți numărul intrării alarmei și tipul de alarmă. Tipul de alarmă poate fi NO (deschis în mod normal) și NC (închis în mod normal). Editați numele pentru a seta un nume pentru intrarea alarmei (opțional).

Alarm Input No.

Alarm Name (cannot copy)

Alarm Type

Arming Schedule

	0	2	4	6	8	10	12	14	16	18	20	22	24
Mon													
Tue													
Wed													
Thu													
Fri													
Sat													
Sun													

Figura 5–42 Setări intrare alarmă

3. Faceți clic pe **Edit** pentru a seta programarea armării pentru intrarea alarmei. Consultați *Sarcina 2 Setarea programării armării pentru detectarea mișcării* din Secțiunea 5.6.1.
4. Bifați caseta pentru a selecta metoda de conectare sau de legare aplicată intrării alarmei. Consultați *Sarcina 3 Setarea acțiunilor de alarmă pentru detectarea mișcării* din Secțiunea 5.6.1.
5. Puteți, de asemenea, alege legătura PTZ pentru intrarea alarmei în cazul în care camera dvs. este instalată cu o unitate de panoramare/înclinare. Bifați casetele de selectare corespunzătoare și selectați numărul pentru a activa Apelare presetare, Apelare patrulare sau Apelare tipar.
6. Puteți copia setările la alte intrări de alarmă.
7. Faceți clic pe **Save** pentru a salva setările.

5.6.4 Configurare ieșire alarmă

Scopul:

Detectează ieșirea alarmei și întreprinde acțiuni de răspuns în momentul declanșării alarmei.

Pași:

1. Accesați interfața Setări ieșire alarmă:
Configuration > Advanced Configuration > Basic Event > Alarm Output
2. Selectați un canal de ieșire a alarmei din lista verticală **Alarm Output**. De asemenea, puteți seta un nume pentru ieșirea alarmei (opțional).
3. Intervalul de activare poate fi setat la 5sec, 10sec, 30sec, 1min, 2min, 5min, 10min sau la Manual. Întârzierea se referă la durata în care o ieșire de alarmă rămâne activă după ce o alarmă a avut loc.
4. Faceți clic pe **Edit** pentru a accesa interfața Editare oră programare. Configurarea programării temporale este identică cu setările programării armării pentru detectarea mișcării. Consultați *Sarcina 2 Setarea programării armării pentru detectarea mișcării* din Secțiunea 5.6.1.
5. Puteți copia setările la alte ieșiri de alarmă.
6. Faceți clic pe **Save** pentru a salva setările.

Alarm Output: A->1

Alarm Name: (cannot copy)

Delay: 5s

Arming Schedule

Edit

	0	2	4	6	8	10	12	14	16	18	20	22	24
Mon													
Tue													
Wed													
Thu													
Fri													
Sat													
Sun													

Figura 5–43 Setări ieșire alarmă

5.6.5 Gestionare excepție

Tipul excepției poate fi HDD plin, eroare HDD, rețea deconectată, adresă IP în conflict și conectare ilegală la camere.

Pași:

1. Accesați interfața Setări excepție:

Configuration > Advanced Configuration > Basic Event > Exception

2. Bifați caseta de selectare pentru a seta acțiunile aplicate pentru alarma de Excepție. Consultați *Sarcina 3 Setarea acțiunilor de alarmă întreprinse pentru detectarea mișcării* din Secțiunea 5.6.1.

Exception Type: HDD Full

Normal Linkage	Other Linkage
☐ Notify Surveillance Center	Trigger Alarm Output ☐ Select All
☐ Send Email	☐ A->1

Save

Figura 5–44 Setări excepție

3. Faceți clic pe **Save** pentru a salva setările.

5.6.6 Configurarea detectării excepțiilor audio

Scopul:

Funcția de detectare excepție audio detectează sunetele anormale în scena de supraveghere, cum ar fi creșterea sau scăderea bruscă a intensității sunetului și unele acțiuni pot fi luate atunci când alarma este declanșată.

Notă: Funcția de detectare a excepțiilor audio variază în funcție de diferitele modele de camere.

Pași:

1. Accesați interfața setărilor Detectare excepție audio:
Configuration > Advanced Configuration > Smart Event > Audio Exception Detection
2. Bifați caseta de selectare a **Audio Loss Exception** pentru a activa funcția de detectare pierdere audio.
3. Bifați caseta de validare a **Sudden Increase of Sound Intensity Detection** pentru a detecta creșterea bruscă a sunetului în scena de supraveghere. Puteți seta sensibilitatea de detectare și pragul pentru creșterea bruscă a sunetului.
4. Bifați caseta de validare a **Sudden Decrease of Sound Intensity Detection** pentru a detecta scăderea bruscă a sunetului în scena de supraveghere. Puteți seta sensibilitatea de detectare și pragul pentru scăderea bruscă a sunetului.

Note:

- Sensibilitate: Intervalul [1-100], cu cât mai mică este valoarea, cu atât mai mare trebuie să fie schimbarea pentru a declanșa detectarea.
- Pragul de intensitate a sunetului: Intervalul [1-100], acesta poate filtra sunetul ambiental, cu cât mai puternic sunetul ambiental, cu atât mai mare trebuie să fie valoarea. Îl puteți regla conform mediului real.

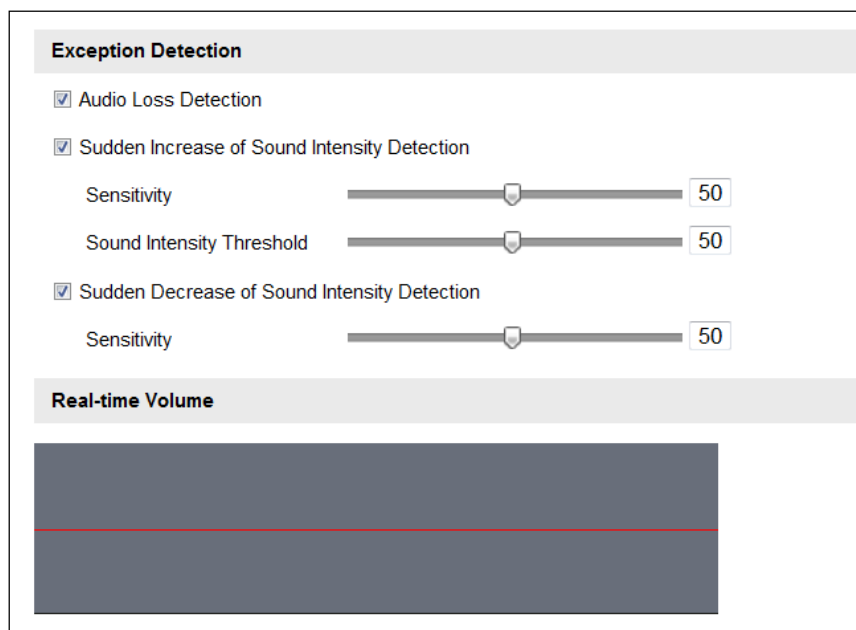


Figura 5–45 Configurarea detectării excepției audio

5. Puteți vizualiza volumul în timp real al sonorului.
6. Faceți clic pe butonul **Edit** pentru a seta programul de armare.
7. Selectați metodele de conectare sau de legare pentru excepția audio. Consultați *Sarcina 3 Setarea acțiunilor de alarmă întreprinse pentru detectarea mișcării* din Secțiunea 5.6.1.
8. Faceți clic pe **Save** pentru a salva setările.

5.6.7 Detectarea schimbării scenei

Scopul:

Funcția de detectare a schimbării scenei detectează schimbarea mediului de supraveghere afectat de factori externi; cum ar fi rotirea intenționată a camerei și pot fi efectuate anumite acțiuni când alarma este declanșată.

Pași:

1. Accesați interfața setărilor Detectare schimbare scenă: Configuration > Advanced Configuration > Smart Event > Scene Change Detection.
2. Bifați caseta **Enable Scene Change Detection** pentru a activa această funcție.

3. Faceți clic și trageți glisorul pentru a seta sensibilitatea detectării. Valoarea sensibilității variază de la 1 la 100 și, cu cât valoarea este mai mare, cu atât este mai ușor ca schimbarea scenei să declanșeze alarma.
4. Faceți clic pe butonul **Edit** pentru a seta programul de armare.
5. Selectați metodele de conectare sau de legare pentru schimbarea scenei, printre care **Înștiințare centru de supraveghere, Trimitere e-mail, Încărcare pe FTP, Declanșare canal și Declanșare ieșire alarmă.**
6. Faceți clic pe **Save** pentru a salva setările.

5.6.8 Configurarea detectării dinamice a sursei incendiului

Scopul:

În momentul în care activați această funcție și este detectată o sursă de incendiu, vor fi declanșate acțiuni de alarmă.

Pași:

1. Accesați interfața setării Detectare dinamică sursă incendiu:
Configuration > Advanced Configuration > Smart Event > Dynamic Fire Source Detection
2. Bifați caseta **Enable Dynamic Fire Source Detection** pentru a activa această funcție.

Audio Exception Detection **Dynamic Fire Source Detection**

Dynamic Fire Source Detection

☒ Enable Dynamic Fire Source Detection

☒ Display Fire Source Frame on Stream

Sensitivity 5

Linkage Method

Normal Linkage	Other Linkage
☐ Notify Surveillance Center	Trigger Alarm Output ☐ Select All
☐ Send Email	☐ A->1
☐ Upload to FTP	
Trigger Channel ☐ Select All	
☐ D1 ☐ D2	

Save

Figura 5–46 Configurarea detectării dinamice a sursei incendiului

3. Bifați caseta **Display Fire Source Frame on Stream** pentru a afișa un cadru de culoare roșie în jurul sursei de incendiu din flux în momentul producerii unui incendiu. (opțional)
4. Puteți glisa cursorul pentru a regla gradul de sensibilitate al detectării dinamice a sursei incendiului de la 1 la 10. Cu cât valoarea este mai mare, cu atât este mai sensibilă detectarea.
5. Bifați caseta pentru a selecta metoda de conectare sau de legare aplicată intrării alarmei. Consultați *Sarcina 3: Setarea acțiunilor de alarmă pentru detectarea mișcării* din Secțiunea *Detectarea mișcării*. În câmpul Altă legătură, puteți bifa caseta pentru a activa ieșirea alarmei (numărul ieșirii alarmei variază în funcție de proprietățile dispozitivului).
6. Faceți clic pe **Save** pentru a salva setările.

5.7 Măsurarea temperaturii

Scopul:

Atunci când activați această funcție, este măsurată temperatura efectivă a punctului monitorizat. Dispozitivul emite o alarmă atunci când temperatura depășește valoarea de prag a temperaturii.

Înainte de a începe:

Accesați **Configuration > Advanced Configuration > System > VCA Resource Type** pentru a selecta **Temperature Measurement + Behavior Analysis** ca Tip de resursă VCA.

5.7.1 Configurarea măsurării temperaturii

Pași:

1. Accesați **Configuration > Advanced Configuration > Temperature Measurement Configuration**.

Figura 5–47 Detectarea dinamică a sursei incendiului

2. Bifați casetele interfeței pentru a seta configurațiile de măsurare a temperaturii.
 - **Enable Temperature Measurement:** Bifați caseta pentru a activa funcția de măsurare a temperaturii.
 - **Display Temperature Info. on Stream:** Bifați caseta pentru a afișa informațiile despre temperatură în modul de vizualizare live.
 - **Add Original Data on Capture:** Bifați caseta pentru a adăuga date originale pe captură.
 - **Add Original Data on Stream:** Bifați caseta pentru a adăuga date originale pe flux.
 - **Data Refresh Interval:** Selectați intervalul de reîmprospătare a datelor de la 1 s la 5 s.
 - **Unit:** Afișați temperatura în grade Celsius (°C)/grade Fahrenheit (°F)/grade Kelvin (K).
 - **Temperature Range:** Setați intervalul de temperatură.
3. Faceți clic pe **Save** pentru a salva setările.

5.7.2 Măsurarea temperaturii și alarma

Scopul:

Această funcție este utilizată pentru a măsura temperatura punctului detectat, iar dispozitivul compară temperatura regiunilor selectate și emite o alarmă.

Pași:

1. Accesați **Configuration > Advanced Configuration > Temperature Measurement and Alarm**.
2. Setați regula de alarmă: Selectați din lista de reguli o regulă de măsurare a temperaturii și configurați parametrii.
 - **Name:** Puteți personaliza numele regulii.
 - **Type:** Selectați punctul, linia sau cadrul ca tip de regulă.
 - **Emissivity:** Setați emisivitatea țintei dvs. Notă: Fiecare obiect are o altă emisivitate.

- **Distance (m):** Distanța în linie dreaptă dintre țintă și dispozitiv.
- **Reflective Temperature:** Dacă în scenă există vreo țintă cu emisivitate ridicată, bifați caseta și setați temperatura de reflexie pentru a corecta temperatura. Dacă nu există o astfel de țintă, debifați caseta.

Temperature Measurement Configuration
Temperature Measurement and Alarm

07-12-2016 Tue 16:15:30


Region Tem...
Alarm Linkage

Enable	ID	Name	Type	Emissivity	Distance(m)	Reflective Temper...	Alarm Rule
☒	2		Frame	0.98	1	☐ 0	☐
☒	3		Line	0.96	30	☐ 0	☐
☒	4		Point	0.96	30	☐ 0	☐
☐	5		Point	0.96	30	☐ 0	☐
☐	6		Point	0.96	30	☐ 0	☐
☐	7		Point	0.96	30	☐ 0	☐
☐	8		Point	0.96	30	☐ 0	☐
☐	9		Point	0.96	30	☐ 0	☐

Save

Figura 5–48 Configurarea măsurării temperaturii

3. Faceți clic pe  din listă pentru a afișa interfața regulii de alarmă.

- **Alarm Rule:** Regula de alarmă variază în funcție de tip. Regula presupune compararea informațiilor despre temperatură pentru două regiuni selectate. Pentru țintele setate în funcție de cadru, regulile includ: **Temperatură max. mai ridicată decât**, **Temperatură max. mai scăzută decât**, **Temperatură min. mai ridicată decât**, **Temperatură min. mai scăzută decât**, **Temperatură medie mai ridicată decât**, **Temperatură medie mai scăzută decât**, **Diferență de temperatură mai ridicată decât** și **Diferență de temperatură mai scăzută decât**. Pentru țintele setate în funcție de linie, regulile includ Temperatură max., Temperatură min. și Temperatură medie. Pentru țintele setate în funcție de punct, regulile sunt diferențiate în funcție de Temperatură medie.

- **Pre-Alarm Temperature și Alarm Temperature:** Setați temperatura de pre-alarmă și temperatura de alarmă, dispozitivul emite pre-alarma atunci când temperatura sa de regulă depășește temperatura de pre-alarmă și emite alarma atunci când temperatura sa de regulă depășește temperatura de alarmă.
 - **Tolerance Temperature:** Setați temperatura de toleranță și dispozitivul apreciază dacă alarma declanșată încetează până când temperatura dispozitivului/diferența de temperatură este mai scăzută decât temperatura de regulă luându-se în considerare temperatura de toleranță. De exemplu, setați temperatura de toleranță la 3 °C, setați temperatura de alarmă la 55 °C și setați temperatura de pre-alarmă la 50 °C. Dispozitivul emite pre-alarma atunci când temperatura sa atinge 50 °C și emite alarma atunci când temperatura sa atinge 55 °C și anulează alarma numai atunci când temperatura dispozitivului este mai scăzută decât 52 °C.
4. Desenați regiunea-țintă: Selectați regula și desenați cadrul/linia/punctul corespunzător(oare). Faceți clic pe  pentru a desena punctul. Faceți clic pe  pentru a desena linia. Faceți clic pe  pentru a desena cadrul.
 5. Setați alarma de diferență de temperatură: Faceți clic pe Temperature Difference Alarm pentru a accesa interfața alarmei de diferență de temperatură, puteți seta până la patru alarme de diferență de temperatură.
-  **NOTE**
- Alarma de diferență de temperatură se aplică numai țințelor setate în funcție de cadru.
6. Setați legătura alarmei: Faceți clic pe Alarm Linkage pentru a accesa interfața de legătură a alarmei și setați metodele de legare.
 7. Faceți clic pe **Save** pentru a salva setările.

5.8 Configurare VCA

5.8.1 Tipul de resursă VCA

Înainte de a putea utiliza regulile VCA ale camerei, trebuie să selectați tipul de resursă VCA.

Pentru a utiliza Măsurare temperatură și Analiză comportament, selectați **Temperature Measurement și Behavior Analysis**. Pentru a utiliza funcția Detectare dinamică sursă incendiu, selectați **Dynamic Fire Source Detection**. Odată ce ați selectat oricare dintre resurse, nu puteți activa cealaltă regulă VCA.

5.8.2 Informațiile VCA

- **Behavior Analysis Version:**

Aceasta listează versiunea bibliotecii de algoritmi.

- **Display information**

Include afișarea în imagine și afișarea în flux. Bifați casetele pentru a activa afișările corespunzătoare.

Figura 5–49 Informațiile VCA

- **Display Target info. on Alarm Picture:** Va fi un cadru pe ținta imaginii alarmei încărcate în cazul în care caseta de validare este bifată.
- **Display Rule info. on Alarm Picture:** Ținta capturată și zona configurată vor fi încadrate pe imaginea de alarmă.
- **Display VCA info. on Stream:** Cadrele verzi vor fi afișate pe țintă pentru o vizualizare live sau redare.

Notă: Asigurați-vă că Regulile sunt activate în setările dvs. locale. Accesați **Configuration > Local Configuration > Rules** pentru activare.

- **Snapshot Setting**

Puteți seta calitatea și rezoluția pentru imaginea capturată.

- **Upload JPEG Image to Center:** Bifați caseta de validare pentru a încărca imaginea capturată în centrul de supraveghere când apare o alarmă VCA.
- **Picture Quality:** Puteți selecta Înaltă, Medie și Slabă.
- **Picture Resolution:** Puteți selecta 384*288, CIF, 4CIF, 720P și 1080P.

Notă: Opțiunile de rezoluție a imaginii ce pot fi selectate variază în funcție de diversele modele de cameră.

5.8.3 Analiza comportamentului

Scopul:

Analiza compartimentului detectează o serie de comportamente suspicioase și anumite metode de conectare vor fi activate dacă alarma este declanșată. Consultați pașii următori pentru a configura setările analizei comportamentului.

Pași:

1. Configurați informațiile afișate și setările instantaneului pe pagina **Info. VCA**.
2. Setați **calibrarea camerei**

Efectuați pașii următori pentru a măsura tridimensional și a cuantifica imaginea de la cameră și apoi pentru a calcula dimensiunea fiecărei ținte. Detectarea VCA va fi mai precisă în cazul în care calibrarea camerei este configurată.

Pași:

- 1) Accesați interfața setării Calibrare cameră:
Configuration > VCA Configuration > Camera Calibration
- 2) Bifați caseta de selectare a **Camera Calibration** pentru a activa această funcționalitate.
- 3) Selectați calibration mode ca Input Basic Data sau ca Draw on Live View Video.

Input Basic Data: Introduceți manual înălțimea de montare, unghiul de vizualizare și raportul de orizont ale camerei.

Draw on Live View Video: Faceți clic pe Desenare linie de verificare (orizontală)/(verticală) pentru a desena o linie orizontală/verticală în modul de vizualizare live și introduceți lungimea efectivă în câmpul Lungime reală. Cu liniile de referință desenate și lungimea lor reală, camera poate detecta că apar alte obiecte în vizualizarea live.

- 4) (Opțional) Bifați caseta **Enable Verification of Camera Calibration**, faceți clic pe butonul **Horizontal Verify/Vertical Verify** pentru a desena o linie orizontală/verticală în transmisiunea video live, după care faceți clic pe butonul **Calibrate** pentru a calcula lungimea liniei. Comparați lungimea liniei calculate cu lungimea reală pentru a verifica informațiile de calibrare pe care le-ați setat.
- 5) Puteți face clic pe **Delete** pentru a șterge liniile desenate.
- 6) Faceți clic pe **Save** pentru a salva setările.

Notă: Dacă vizualizarea live este oprită, calibrarea camerei este nevalidă.

Figura 5–50 Introducerea datelor de bază

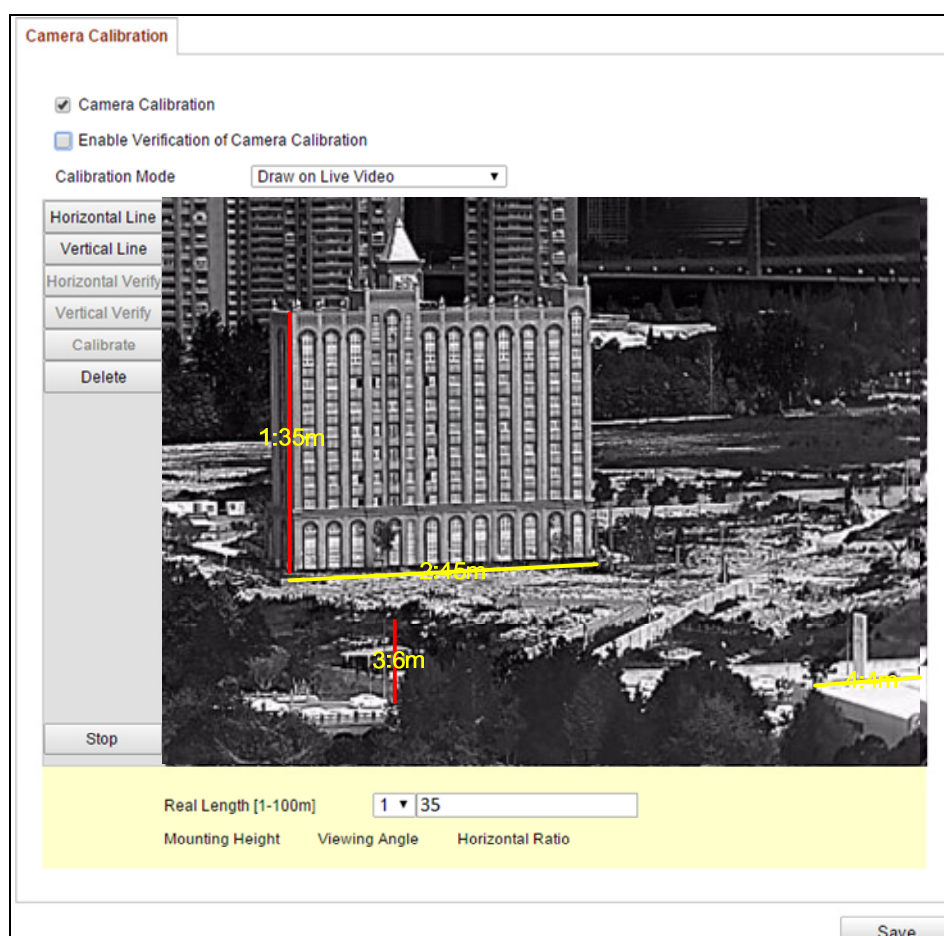


Figura 5–51 Trasați pe fereastra de vizualizare live

3. Desenați regiunea scut

Regiunea scutului vă permite să setați regiunea specifică în care analiza comportamentului nu va funcționa. Sunt acceptate până la 4 regiuni scut.

Pași:

- 1) Accesați interfața setării Regiune scut:

Configuration > VCA Configuration > Shield Region

- 2) Faceți clic pe **Draw Area**. Trasați zona cu clic stânga pe punctele finale din fereastra vizualizare live și faceți clic dreapta pentru a finaliza trasarea zonei.

Note:

- Este acceptată zona poligonală cu până la 10 laturi.
 - Faceți clic pe **Delete** pentru a șterge zonele desenate.
 - Dacă vizualizarea live este oprită, nu există niciun mod de a trasa regiunile scutului.
- 3) Faceți clic pe **Save** pentru a salva setările.

4. Configurați **Regula**

Analiza comportamentului acceptă o serie de comportamente, printre care traversarea liniei, intruziunea, intrarea în regiune, ieșirea din regiune etc.

Notă: Tipul de regulă pentru setare variază în funcție de diversele modele de cameră.

Pași:

- 1) Faceți clic pe fila **Rule** pentru a deschide interfața de configurare a regulii.
- 2) Faceți clic pe  pentru a adăuga o regulă nouă. (Opțional) Faceți clic pe  pentru a o șterge.
- 3) Bifați caseta regulii dorite pentru a activa regula pentru analiza comportamentului.
- 4) Selectați tipul de regulă, setați tipul de filtru și apoi trasați linia/zona pe video live pentru regula individuală.
 - **Line Crossing** detectează persoanele, vehiculele sau alte obiecte care traversează o linie imaginară predefinită, putând fi întreprinse anumite acțiuni în momentul declanșării alarmei.
Atunci când selectați acest tip de regulă, trebuie să selectați direcția de traversare înainte de a desena o linie. Puteți selecta Bidirecțional, De la A la B și De la B la A.
 - **Intrusion** detectează persoanele, vehiculele sau alte obiecte care pătrund și vagabondează într-o regiune imaginară predefinită, putând fi întreprinse anumite acțiuni în momentul declanșării alarmei.
Atunci când selectați acest tip de regulă, trebuie să setați durata intruziunii. Duratele disponibile variază de la 1 s la 100 s.

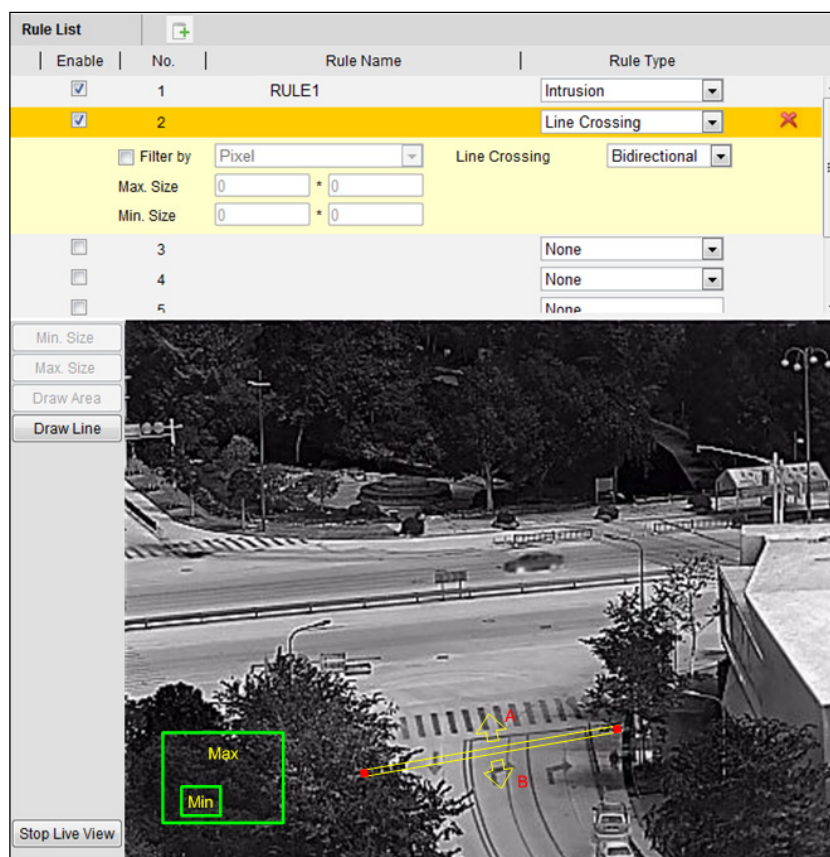


Figura 5–52 Tipul de regulă – Traversarea liniei

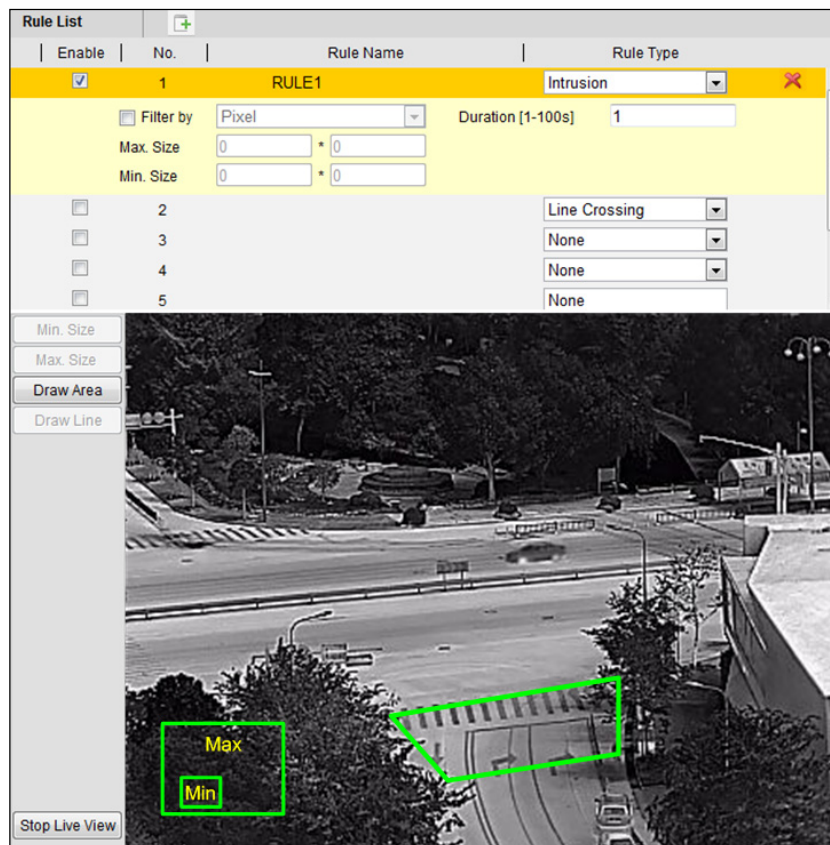


Figura 5–53 Tipul de regulă – Intruziunea

- **Region Entrance** detectează persoanele, vehiculele sau alte obiecte care pătrund din exterior într-o regiune imaginată predefinită, putând fi întreprinse anumite acțiuni în momentul declanșării alarmei.
- **Region Exiting** detectează persoanele, vehiculele sau alte obiecte care ies dintr-o regiune imaginată predefinită, putând fi întreprinse anumite acțiuni în momentul declanșării alarmei.

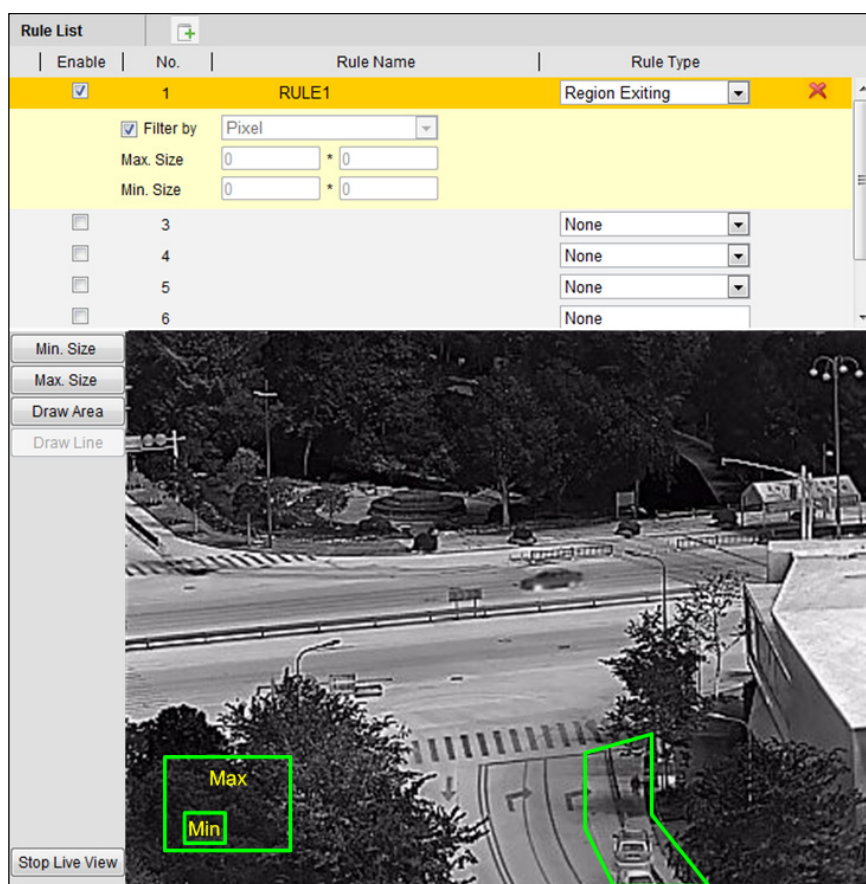


Figura 5–54 Tipul de regulă – ieșirea din regiune

- **Filter type:** Puteți selecta Pixels și Actual Size. Dacă selectați Pixels, desenați zona de dimensiune maximă și zona de dimensiune minimă în transmisiunea video live pentru fiecare regulă. Dacă Actual Size este selectat, introduceți lungimea și lățimea dimensiunii maxime și dimensiunii minime. Doar ținta a cărei dimensiune este între valoarea minimă și valoarea maximă va declanșa alarma.

Notă: Calibrarea camerei trebuie să fie configurată dacă dimensiunea reală este selectată.

- **Draw line/area:** Pentru alte evenimente, precum intruziunea, intrarea în regiune, ieșirea din regiune etc., trebuie să faceți clic stânga în transmisiunea video live pentru a seta punctele de terminare ale zonei și să faceți clic dreapta pentru a finaliza desenarea zonei.

Notă: Dacă vizualizarea live este oprită, zona/linia de detectare nu pot fi trasate și regulile nu pot fi setate.

- 5) Bifați caseta de validare a regulii combinate pentru a activa regula pentru analiza comportamentului.
- 6) Selectați două reguli individuale configurare ca Regula A și Regula B a regulii combinate, setați intervalul de timp minim și maxim pentru cele două reguli individuale, apoi selectați ordinea de declanșare a regulilor individuale pentru filtrarea alarmei.

Note:

- Dacă selectați rule type ca None, opțiunea de regulă este invalidă și nu puteți configura nicio analiză a comportamentului.
- Ordinea de declanșare a regulilor individuale pentru filtrarea alarmelor poate fi setată ca Ordine crescătoare sau ca Ordine crescătoare/Ordine descrescătoare.
- Pot fi configurate până la 8 reguli individuale și 2 reguli combinate. Iar traversarea liniei, intruziunea, ieșirea din regiune și intrarea în regiune sunt acceptate pentru regulile combinate.

- 7) Faceți clic pe **Save** pentru a salva setările.
- 8) Faceți clic pe fila **Arming Schedule**, faceți clic pe **Edit** pentru a seta momentul programării pentru fiecare regulă și faceți clic pe **Save** pentru a salva setările.
- 9) Faceți clic pe fila **Alarm Linkage**, bifați caseta metodei de legare corespunzătoare pentru fiecare regulă și faceți clic pe **Save** pentru a salva setările.

5. Setarea **configurării avansate**

- **Parametru**

Configurați următorii parametri pentru a detalia configurarea.

Figura 5–55 Configurare avansată

Detection Sensitivity [0~4]: Se referă la sensibilitatea cu care camera detectează o țintă. Cu cât mai mare este valoarea, cu atât mai ușor poate fi recunoscută o țintă și cu atât mai ridicată este informarea greșită. Valoarea implicită de 3 este recomandată.

Background Update Rate [0~4]: Aceasta se referă la viteza cu care scena nouă înlocuiește scena anterioară. Valoarea implicită de 2 este recomandată.

Single Alarm: Dacă este selectată o singură alarmă, ținta din zona configurată va declanșa alarma o singură dată. Dacă nu este verificată, aceeași țintă va cauza alarma continuă din aceeași zonă configurată.

Leave Interference Suppression: Bifați această casetă de selectare pentru a opri interferența cauzată de frunzele din zona configurată.

Output Type: Selectați poziția cadrului. Puteți selecta centrul-țintă, centrul din partea de jos și centrul din partea de sus. De exemplu: Ținta se va găsi în centrul cadrului dacă selectați centrul-țintă.

Restore Default: Faceți clic pentru a restabili parametrii configurați la valoarea implicită.

Restart VCA: Reporniți biblioteca de algoritmi a analizei comportamentului.

- Filtru dimensiune globală

Notă: În comparație cu regula filtrului de dimensiune inferioară, care vizează fiecare regulă în parte, filtrul de dimensiune globală vizează toate regulile.

Pași:

- 1) Bifați caseta de validare a **Global Size Filter** pentru a activa această funcție.
- 2) Selectați Filter Type ca Actual Size sau ca Pixel.

Actual Size: Introduceți lungimea și lățimea dimensiunii maxime și dimensiunii minime. Doar ținta a cărei dimensiune este între valoarea minimă și valoarea maximă va declanșa alarma.

Note:

- Calibrarea camerei trebuie configurată dacă selectați filtrul după dimensiunea reală.
- Lungimea dimensiunii maxime trebuie să fie mai lungă decât lungimea dimensiunii minime, la fel ca și lățimea.

Pixel: Faceți clic pe Dimensiune minimă pentru a desena dreptunghiul de dimensiune minimă în modul de vizualizare live. Și faceți clic pe Dimensiune maximă pentru a desena dreptunghiul de dimensiune maximă în modul de vizualizare live. Ținta mai mică decât dimensiunea min. sau mai mare decât dimensiunea max. va fi filtrată.

Note:

- Zona trasată va fi transformată în pixel de algoritmul din fundal.
- Filtrul dimensiunii globale nu poate fi configurat dacă vizualizarea live este oprită.
- Lungimea dimensiunii maxime trebuie să fie mai lungă decât lungimea dimensiunii minime, la fel ca și lățimea.

- 3) Faceți clic pe **Save** pentru a salva setările.

Capitolul 6 Configurări stocare

Înainte de a începe:

Pentru a configura setările înregistrării, asigurați-vă că dispozitivul de stocare de rețea se găsește în interiorul rețelei sau că ați introdus cardul SD în camera dvs.

6.1 Gestionarea stocării

Gestionarea stocării vă permite să vizualizați starea HDD-ului, inclusiv capacitatea, spațiul liber, starea, tipul, progresul etc. Puteți, de asemenea, formata HDD-ul dacă este necesar. În plus, puteți atribui cota destinată imaginilor și fișierelor înregistrate.

Notă: Înainte de a putea gestiona dispozitivele HDD, trebuie să le adăugați. Introduceți cardul SD sau consultați următoarea secțiune pentru a adăuga dispozitivele HDD.

The screenshot shows the 'Storage Management' tab in a web interface. It contains two main sections: 'HDD Device List' and 'Quota'.

HDD Device List: A table with columns: HDD No., Capacity, Free space, Status, Type, Property, and Progress. There is a 'Format' button to the right of the table.

HDD No.	Capacity	Free space	Status	Type	Property	Progress
9	20.00GB	0.00GB	Uninitialized	NAS	R/W	

Quota: A section with input fields for various storage limits and percentages.

Max. Picture Capacity	0.00GB
Free Size for Picture	0GB
Max. Record Capacity	0.00GB
Free Size for Record	0GB
Percentage of Picture	25%
Percentage of Record	75%

Figura 6–1 Interfața Gestionare stocare

6.2 Configurarea setărilor NAS

Înainte de a începe:

Discul de rețea trebuie să fie disponibil în cadrul rețelei și trebuie să fie configurat în mod corespunzător pentru a stoca fișierele înregistrate, fișierele jurnal etc.

Pași:

1. Adăugare disc de rețea

(1) Accesați interfața Setări NAS (Network-Attached Storage):

Configuration > Advanced Configuration > Storage > NAS

HDD No.	Type	Server Address	File Path
1	NAS	172.6.21.99	/dvr/test01
2	NAS		
3	NAS		
4	NAS		
5	NAS		
6	NAS		
7	NAS		
8	NAS		

Mounting Type: NFS SMB/CIFS User Name: Password:

Save

Figura 6–2 Adăugați discul de rețea

- (2) Introduceți adresa IP a discului de rețea și introduceți calea fișierului.
- (3) Selectați tipul de montare. NFS și SMB/CIFS sunt selectabile. Și puteți seta numele de utilizator și parola pentru a garanta securitatea dacă SMB/CIFS este selectat.

Notă: Consultați *Manualul utilizatorului de NAS* pentru crearea căii fișierului.

- Pentru confidențialitatea dvs. și pentru a vă proteja mai bine sistemul împotriva riscurilor de securitate, vă recomandăm să utilizați parole puternice pentru toate funcțiile și dispozitivele de rețea. Parola trebuie să fie aleasă de către dvs. (folosind minimum 8 caractere, printre care majuscule, minuscule, cifre și caractere speciale) pentru a crește siguranța produsului dvs.
- Configurarea adecvată a tuturor parolelor și a altor setări de securitate este responsabilitatea instalatorului și/sau a utilizatorului final.

- (4) Faceți clic pe **Save** pentru a adăuga discul de rețea.

2. Inițializarea discului de rețea adăugat.

(1) Accesați interfața Setări HDD

Advanced Configuration > Storage > Storage Management

The screenshot shows the 'Storage Management' tab with the 'HDD Device List' table and the 'Quota' section below it.

HDD Device List							
☐	HDD No.	Capacity	Free space	Status	Type	Property	Progress
☐	g	20.00GB	0.00GB	Uninitialized	NAS	R/W	

Format

Quota

Max. Picture Capacity	0.00GB
Free Size for Picture	0GB
Max. Record Capacity	0.00GB
Free Size for Record	0GB
Percentage of Picture	25 %
Percentage of Record	75 %

Figura 6–3 Interfața Gestionare stocare

- (2) Dacă starea discului este **Uninitialized**, bifați caseta de validare corespunzătoare pentru a selecta discul și faceți clic pe **Format** pentru a începe inițializarea discului. Când inițializarea este finalizată, starea discului va deveni **Normal**.

The screenshot shows the 'HDD Device List' table after formatting. The status has changed from 'Uninitialized' to 'Normal'.

HDD Device List							
☐	HDD No.	Capacity	Free space	Status	Type	Property	Progress
☐	g	20.00GB	19.75GB	Normal	NAS	R/W	

Format

Figura 6–4 Vizualizare stare disc

3. Definiți cota pentru înregistrări și imagini.

- (1) Introduceți procentul pentru imagini și înregistrări.
- (2) Faceți clic pe **Save** și actualizați pagina browserului pentru a activa setările.

The screenshot shows the 'Quota' section with updated values.

Max. Picture Capacity	4.94GB
Free Size for Picture	4.94GB
Max. Record Capacity	14.81GB
Free Size for Record	14.81GB
Percentage of Picture	25 %
Percentage of Record	75 %

Figura 6–5 Setare cotă

Note:

- Se pot conecta până la 8 discuri NAS la cameră.
- Pentru a inițializa și a utiliza cardul SD după introducerea acestuia în cameră, consultați pașii de inițializare a discului NAS.

6.3 Configurarea programului de înregistrare

Scopul:

Există două tipuri de înregistrare pentru camere: înregistrare manuală și înregistrare programată. Pentru înregistrarea manuală, consultați *Secțiunea 4.3 Înregistrarea și capturarea manuală a imaginilor*. În această secțiune puteți urma instrucțiunile pentru a configura înregistrarea programată. În mod implicit, fișierele de înregistrare pentru înregistrare programată sunt stocate pe cardul SD (dacă este acceptat) sau pe discul de rețea.

Pași:

1. Accesați interfața de setări Program înregistrare:

Configuration > Advanced Configuration > Storage > Record Schedule

Record Schedule | Storage Management | NAS | Snapshot

Channel No.

Pre-record

Post-record

Overwrite

Recording Stream

☒ Enable Record Schedule

	0	2	4	6	8	10	12	14	16	18	20	22	24
Mon	Other	Other	Other	Other	Other	Other	Other	Other	Other	Other	Other	Other	Other
Tue	Other	Other	Other	Other	Other	Other	Other	Other	Other	Other	Other	Other	Other
Wed	Other	Other	Other	Other	Other	Other	Other	Other	Other	Other	Other	Other	Other
Thu	Other	Other	Other	Other	Other	Other	Other	Other	Other	Other	Other	Other	Other
Fri	Other	Other	Other	Other	Other	Other	Other	Other	Other	Other	Other	Other	Other
Sat	Other	Other	Other	Other	Other	Other	Other	Other	Other	Other	Other	Other	Other
Sun	Other	Other	Other	Other	Other	Other	Other	Other	Other	Other	Other	Other	Other

Legend:

- Continuous
- Motion Detection
- Alarm
- Motion | Alarm
- Motion & Alarm
- Other

Figura 6–6 Interfață Program înregistrare

2. Bifați caseta **Enable Record Schedule** pentru a activa înregistrarea programată.
3. Setări parametrii de înregistrare ai camerei.

Pre-record	5s
Post-record	5s
Overwrite	Yes
Recording Stream	Main Stream

Figura 6–7 Parametri înregistrare

- **Pre-record:** T impuls setat pentru pornirea înregistrării înaintea orei sau evenimentului programat. De exemplu, dacă o alarmă declanșează înregistrarea la ora 10:00 și timpul de preînregistrare este setat la 5 secunde, camera începe să înregistreze la 9:59:55.

Durata de preînregistrare poate fi configurată ca Nicio preînregistrare, 5 s, 10 s, 15 s, 20 s, 25 s, 30 s sau ca nelimitată.

- **Post-record:** T impuls setat pentru a opri înregistrarea după timpul sau evenimentul programat. De exemplu, dacă o înregistrare declanșată de alarmă se termină la 11:00 și timpul post-înregistrare este setat ca 5 secunde, camera înregistrează până la 11:00:05.

Durata de postînregistrare poate fi configurată ca 5 s, 10 s, 30 s, 1 min, 2 min, 5 min sau ca 10 min.

- **Recording Stream:** Puteți selecta Flux principal și Flux secundar. Fluxul principal este utilizat, de obicei, pentru înregistrare și pentru vizualizarea live cu o bună lățime de bandă, iar fluxul secundar și fluxul terțiar pot fi utilizate pentru vizualizarea live atunci când lățimea de bandă este limitată.

Notă: Configurațiile parametrului de înregistrare variază în funcție de modelul camerei.

4. Faceți clic pe **Edit** pentru a edita programarea înregistrării.

Edit Schedule

Mon Tue Wed Thu Fri Sat Sun

☐ All Day Continuous

☒ Custom

Period	Start Time	End Time	Record Type
1	00:00	08:00	Fire Source Detec
2	08:00	14:00	Alarm
3	14:00	20:00	Continuous
4	20:00	24:00	Motion Alarm
5	00:00	00:00	Continuous
6	00:00	00:00	Continuous
7	00:00	00:00	Continuous
8	00:00	00:00	Continuous

Copy to Week ☒ Select All

☒ Mon
 ☒ Tue
 ☒ Wed
 ☒ Thu
 ☒ Fri
 ☒ Sat
 ☒ Sun
 Copy

OK Cancel

Figura 6–8 Editarea programării înregistrării

5. Alegeți ziua pentru care doriți să setați programarea înregistrării.

(1) Setați înregistrarea pe durata întregii zile sau înregistrarea pe segmente:

- Dacă doriți să configurați înregistrarea pe durata întregii zile, bifați caseta **All Day**.
- Dacă doriți să înregistrați în intervale temporale diferite, bifați caseta **Custom**. Setați **Start Time** și **End Time**.

Notă: Orele segmentelor nu se pot suprapune. Pot fi configurate până la 8 segmente.

(2) Selectați un tip de **înregistrare**.

Tipul de înregistrare poate fi Continuu, Detectare mișcare, Alarmă, Mișcare | Alarmă, Mișcare și alarmă, Detectare excepție audio, Înregistrare VCA, Detectare sursă incendiu și Toate evenimentele.

- **Continuu**

Dacă selectați **Continuous**, fișierul video va fi înregistrat automat în funcție de ora programării.

- **Înregistrare declanșată de detectarea mișcării**

Dacă selectați **Motion Detection**, fișierul video va fi înregistrat în momentul detectării mișcării.

Pe lângă configurarea programului de înregistrare, trebuie să setați zona de detectare a mișcării și să bifați caseta de selectare a **Trigger Channel** din **Linkage Method** a interfeței cu setări pentru Detectare mișcare. Pentru informații detaliate, consultați *Sarcina 1: Setarea zonei de detectare a mișcării din Secțiunea 5.6.1*.

- **Înregistrare declanșată de alarmă**

Dacă selectați **Alarm**, fișierul video va fi înregistrat atunci când alarma este declanșată prin intermediul canalelor externe de intrare a alarmei.

În afară de a configura programarea înregistrării, trebuie să setați **tipul de alarmă** și să bifați caseta **Trigger Channel** din **Linkage Method** a interfeței **Setări intrare alarmă**. Pentru informații detaliate, consultați *Secțiunea 5.6.3*.

- **Înregistrare declanșată de mișcare și alarmă**

Dacă selectați **Motion & Alarm**, conținutul video va fi înregistrat când mișcarea și alarma sunt declanșate în același timp.

Pe lângă configurarea înregistrării, trebuie să configurați setările din interfețele **Detectie mișcare** și **Setări intrare alarmă**. Consultați *Secțiunea 5.6.1* și *Secțiunea 5.6.3* pentru informații detaliate.

- **Înregistrare declanșată de mișcare | alarmă**

Dacă selectați **Motion | Alarm**, conținutul video va fi înregistrat când alarma externă este declanșată sau mișcarea este detectată.

Pe lângă configurarea înregistrării, trebuie să configurați setările din interfețele **Detectie mișcare** și **Setări intrare alarmă**. Consultați *Secțiunea 5.6.1* și *Secțiunea 5.6.3* pentru informații detaliate.

- **Înregistrarea declanșată de Detectare excepție audio**

Dacă selectați **Audio Exception Detection**, fișierul video va fi înregistrat atunci când sunt detectate sunete neobișnuite în scena de supraveghere, cum ar fi creșterea/scăderea bruscă a intensității sonorului.

Pe lângă configurarea înregistrării, trebuie să configurați setările din interfața **Detectie excepție audio**. Consultați *Secțiunea 5.6.6* pentru informații detaliate.

- **Înregistrarea declanșată de Înregistrare VCA**

Dacă selectați **VCA Recording**, fișierul video va fi înregistrat atunci când VCA detectează serii de comportamente suspecte, cum ar fi traversarea liniei, intruziunea, intrarea în regiune și ieșirea din regiune.

În afară de a configura programarea înregistrării, trebuie să configurați setarea Regulă din interfața Configurare VCA. Consultați *Secțiunea 5.7.2* pentru informații detaliate.

- **Înregistrarea declanșată de Detectare sursă incendiu**

Dacă selectați **Fire Source Detection**, fișierul video va fi înregistrat în momentul detectării unei surse de incendiu.

În afară de a configura programarea înregistrării, trebuie să configurați setările din interfața **Dynamic Fire Source Detection**. Consultați *Secțiunea 5.6.7* pentru informații detaliate.

- **Înregistrarea declanșată de Toate evenimentele**

Dacă selectați **All Events**, fișierul video va fi înregistrat în momentul producerii oricăruia dintre evenimentele menționate anterior.

În afară de a configura programarea înregistrării, trebuie să configurați setările din interfețele de eveniment corespunzătoare.

(3) (Opțional) Bifați caseta **Select All** și faceți clic pe **Copy** pentru a copia setările acestei zile la întreaga săptămână. Puteți, de asemenea, bifa oricare dintre casetele de dinaintea datei și puteți face clic pe **Copy**.

(4) Faceți clic pe **OK** pentru a salva setările și a ieși din interfața **Edit Record Schedule**.

6. Faceți clic pe **Save** pentru a salva setările.

6.4 Configurarea setărilor instantaneului

Scopul:

Puteți configura instantanee programate și instantanee declanșate de un eveniment. Imaginea capturată poate fi stocată pe cardul SD (dacă este acceptat) sau pe NAS (pentru informații detaliate, consultați *Secțiunea 6.2 Configurarea setărilor NAS*). Puteți, de asemenea, încărca imaginile capturate pe un server FTP.

Setări de bază

Pași:

1. Accesați interfața Setări instantaneu:

Configuration > Advanced Configuration > Storage > Snapshot

The screenshot displays the 'Snapshot' configuration page within the 'Storage' section. It features two main tabs: 'Timing' and 'Event-Triggered'. The 'Timing' tab is active, showing settings for enabling snapshots, format (JPEG), resolution (640*512), quality (High), and interval (0 milliseconds). Below these settings is a calendar grid for scheduling snapshots by day and time. The 'Event-Triggered' tab is also visible, showing similar settings for event-based snapshots, including a capture number of 4.

	0	2	4	6	8	10	12	14	16	18	20	22	24
Mon													
Tue													
Wed													
Thu													
Fri													
Sat													
Sun													

Figura 6–9 Interfața setării instantaneului

2. Selectați un număr de canal. Pentru modelele de cameră care prezintă mai multe canale ale camerei, trebuie să selectați, mai întâi, numărul canalului pentru configurare.
3. Bifați caseta de selectare **Enable Timing Snapshot** pentru a activa instantaneul continuu.

Editați ora programării pentru instantanee. Pentru setări detaliate, consultați ***Secțiunea 6.3 Configurarea programului de înregistrare.***
4. Bifați caseta **Enable Event-triggered Snapshot** pentru a activa instantaneul declanșat de eveniment.
5. Selectați formatul, rezoluția și calitatea instantaneului.
6. Setăți intervalul de timp dintre cele două instantanee.
7. Faceți clic pe **Save** pentru a salva setările.

Încărcare pe FTP

Puteți urma instrucțiunile de configurare de mai jos pentru a încărca instantaneele pe FTP.

- Încărcare instantanee continue pe FTP

Pași:

- 1) Configurați setările FTP și bifați caseta de selectare **Upload Picture** din interfața Setări FTP. Consultați ***Secțiunea 5.3.11 Configurare setări FTP*** pentru informații detaliate despre configurarea parametrilor FTP.
- 2) Bifați caseta de selectare **Enable Timing Snapshot**.

- Încărcare instantanee declanșate de eveniment pe FTP

Pași:

- 1) Configurați setările FTP și bifați caseta de selectare **Upload Picture** din interfața Setări FTP. Consultați ***Secțiunea 5.3.11 Configurare setări FTP*** pentru informații detaliate despre configurarea parametrilor FTP.
- 2) Bifați caseta **Upload Picture** din interfața Setări detectare mișcare sau din interfața Intrare alarmă. Consultați ***Sarcina 3: Setarea acțiunilor de alarmă întreprinse pentru detectarea mișcării din Secțiunea 5.6.1,***
- 3) Bifați caseta de selectare **Enable Event-triggered Snapshot**.

Capitolul 7 Redare

Scopul:

Această secțiune explică modul în care să vizualizați fișierele video înregistrate la distanță pe discurile de rețea sau cardurile SD.

Pași:

1. Faceți clic pe **Playback** de pe bara de meniu pentru a deschide interfața de redare.

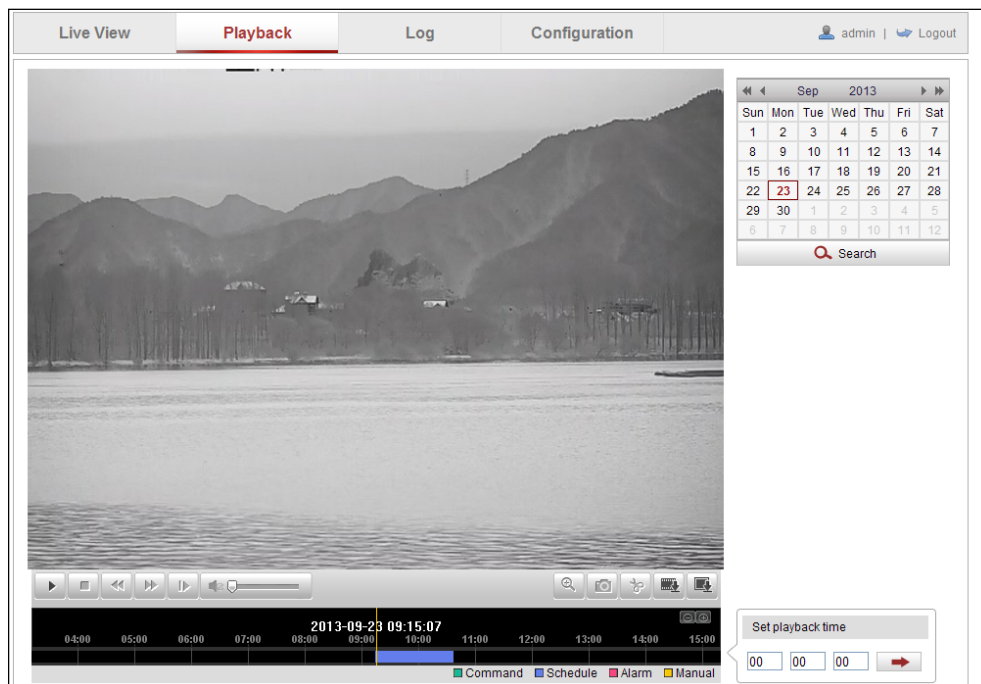


Figura 7-1 Interfață redare

2. Selectați o dată și faceți clic pe **Search** pentru a căuta fișierele înregistrate.

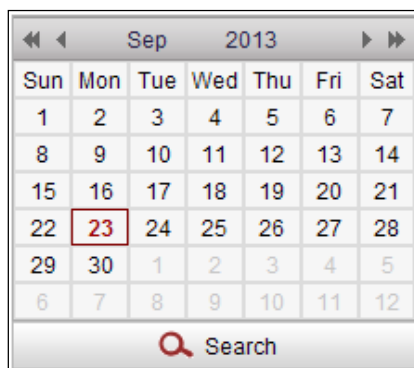


Figura 7-2 Căutare video

3. Faceți clic pe  pentru a reda fișierele video găsite la această dată. Puteți utiliza bara de instrumente din partea de jos a interfeței de Redare pentru a controla procesul de redare.

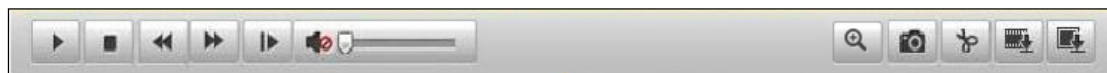


Figura 7–3 Bară de instrumente Redare

Tabelul 7–1 Descrierea butoanelor

Pictogramă	Descriere	Pictogramă	Descriere
	Redare		Capturare imagine
	Pauză		Pornire/oprire decupare fișiere video
	Oprire		Audio pornit și reglare volum/ audio oprit
	Micșorare viteză		Descărcarea fișierelor video
	Mărire viteză		Descărcarea imaginilor capturate
	Redare după cadru		Activare/Dezactivare zoom digital

Notă: Puteți alege căile de fișiere locale pentru descărcarea fișierelor video și a imaginilor din interfața Configurare locală. Consultați *Secțiunea 5.1* pentru informații detaliate.

4. Glisați bara de progres cu mouse-ul pentru a localiza punctul exact de redare.

De asemenea, puteți introduce timpul și apoi faceți clic pe pentru a localiza punctul de redare din câmpul **Set playback time**. De asemenea, puteți face clic pe zoom out/in pe bara de progres.

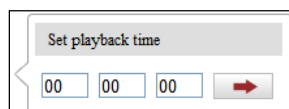


Figura 7–4 Setare T imp redare

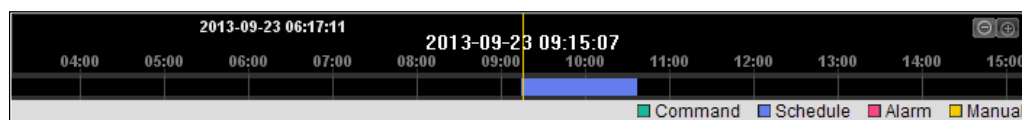


Figura 7–5 Bară de progres

Culorile diferite ale conținutului video de pe bara de progres reprezintă diferite tipuri video.

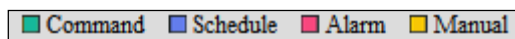


Figura 7–6 Tipuri video

Capitolul 8 Căutare jurnal

Scopul:

Funcționarea, alarma, excepția și informațiile camerei pot fi stocate în fișierele jurnal. De asemenea, puteți exporta fișierele de jurnal atunci când doriți.

Înainte de a începe:

Asigurați-vă că stocarea de rețea este configurată pentru cameră sau că stocarea locală (cardul SD) funcționează.

Pași:

1. Faceți clic pe **Log** din bara de meniu pentru a accesa interfața de căutare a jurnalelor.

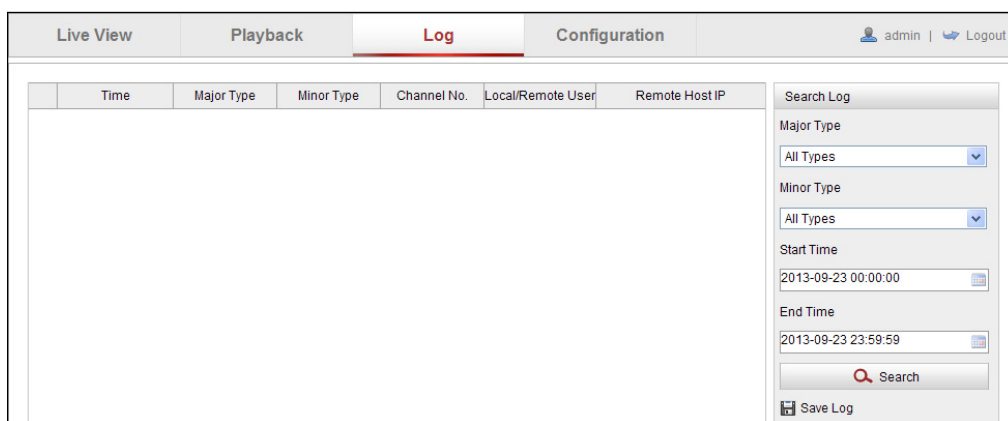


Figura 8–1 Interfață Căutare jurnal

2. Setați condițiile de căutare în jurnal pentru a specifica tipul de căutare, inclusiv tipul major, tipul minor, ora de începere și ora de terminare.
3. Faceți clic pe **Search** pentru a căuta fișierele jurnal. Fișierele de jurnal potrivite vor fi afișate în interfața **Log**.

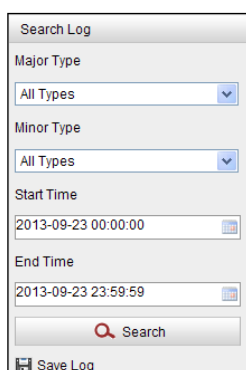


Figura 8–2 Căutare jurnal

4. Pentru a exporta fișierele-jurnal, faceți clic pe **Save log** pentru a salva fișierele-jurnal în computerul dvs.

Capitolul 9 Altele

9.1 Gestionarea conturilor de utilizator

Scopul:

Utilizatorul admin poate adăuga, șterge sau modifica conturi de utilizator și să le acorde diverse permisiuni. Vă recomandăm ca utilizatorul să gestioneze adecvat conturile dispozitivului și permisiunile de utilizator.

Accesați interfața Gestionare utilizator pentru a finaliza setările: **Configuration > Basic Configuration > Security > User** sau **Configuration > Advanced Configuration > Security > User**

User

Authentication

Anonymous Visit

IP Address Filter

Security Service

Add

Modify

Delete

No.	User Name	Level
1	admin	Administrator
2	Test	Operator

Figura 9–1 Informații utilizator

- **Adăugarea unui utilizator**

Utilizatorul *admin* are toate permisiunile în mod implicit, poate crea, modifica și șterge alte conturi.

Notă: Utilizatorul *admin* nu poate fi șters și numai dvs. puteți schimba parola *admin*.

Pași:

1. Faceți clic pe **Add** pentru a adăuga un utilizator.
2. Introduceți **numele de utilizator**, selectați **Level** și introduceți **parola**.

Note:

- Se pot crea până la 31 de conturi de utilizator.
- Diversele niveluri de utilizator dețin diverse permisiuni. Operatorul și utilizatorul pot fi selectați.



- Pentru confidențialitatea dvs. și pentru a vă proteja mai bine sistemul împotriva riscurilor de securitate, vă recomandăm să utilizați parole puternice pentru toate funcțiile și dispozitivele de rețea. Parola trebuie să fie aleasă de către dvs. (folosind minimum 8 caractere, printre care majuscule, minuscule, cifre și caractere speciale) pentru a crește siguranța produsului dvs.
 - Configurarea adecvată a tuturor parolelor și a altor setări de securitate este responsabilitatea instalatorului și/sau a utilizatorului final.
3. În câmpurile **Basic Permission** și **Camera Configuration**, puteți bifa sau debifa permisiunile pentru noul utilizator.
 4. Faceți clic pe **OK** pentru finalizarea adăugării utilizatorului.

Add user

User Name: test1

Level: Operator

Password: [masked] ✓
Strong
 Valid password range [8-16]. You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained.

Confirm: [masked]

Basic Permission	Camera Configuration
☐ Remote: Parameters Settings	Remote: Live View Select All ☒
☒ Remote: Log Search / Interrogate Working Status	☒ D1 ☒ D2
☐ Remote: Upgrade / Format	☒ Remote: PTZ Control
☒ Remote: Two-way Audio	Remote: Manual Record Select All ☒
☐ Remote: Shutdown / Reboot	☒ D1 ☒ D2
☐ Remote: Notify Surveillance Center / Trigger Alarm Output	Remote: Playback Select All ☒
☐ Remote: Video Output Control	☒ D1 ☒ D2
☐ Remote: Serial Port Control	

OK Cancel

Figura 9–2 Adăugarea unui utilizator

- **Modificarea unui utilizator**

Pași:

1. Faceți clic stânga pentru a selecta utilizatorul din listă și faceți clic pe **Modify**.
2. Modificați **User Name**, **Level** sau **Password**.

3. În câmpurile **Basic Permission** și **Camera Configuration**, puteți bifa sau debifa permisiunile.
4. Faceți clic pe **OK** pentru finalizarea modificării utilizatorului.

Figura 9–3 Modificarea unui utilizator

- **Ștergerea unui utilizator**

Pași:

1. Faceți clic pentru a selecta utilizatorul pe care doriți să îl ștergeți și faceți clic pe **Delete**.
2. Faceți clic pe **OK** din caseta de dialog pop-up pentru a șterge utilizatorul.

9.2 Autentificare

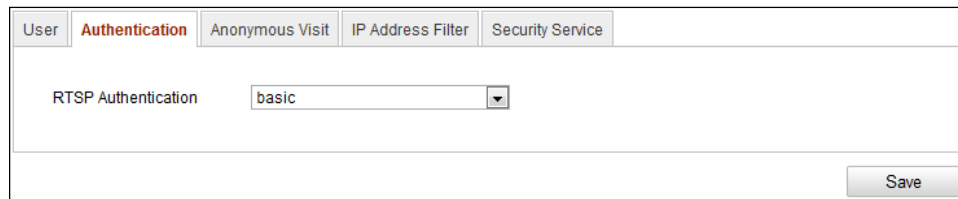
Scopul:

Puteți securiza datele de flux pentru vizualizarea live.

Pași:

1. Accesați interfața Authentication:

Configuration > Advanced Configuration > Security > Authentication



User	Authentication	Anonymous Visit	IP Address Filter	Security Service
RTSP Authentication basic				
Save				

Figura 9–4 Autentificare RTSP

2. Selectați din lista verticală tipul de **RTSP Authentication** ca **basic** sau ca **disable** pentru a activa sau a dezactiva autentificarea RTSP.

Notă: Dacă dezactivați autentificarea RTSP, oricine poate accesa fluxul video prin protocolul RTSP cu ajutorul adresei de IP.

3. Faceți clic pe **Save** pentru a salva setările.

9.3 Vizita anonimă

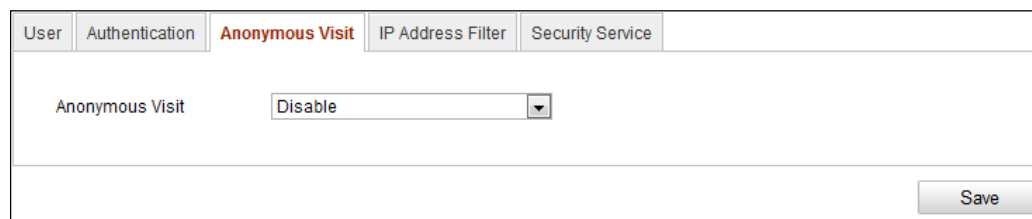
Activarea acestei funcții permite vizitarea de către vizitatori care nu dețin numele de utilizator sau parola dispozitivului.

Notă: Pentru utilizatorii anonimi nu este disponibilă decât vizualizarea live.

Pași:

1. Accesați interfața Anonymous Visit:

Configuration > Advanced Configuration > Security > Anonymous Visit

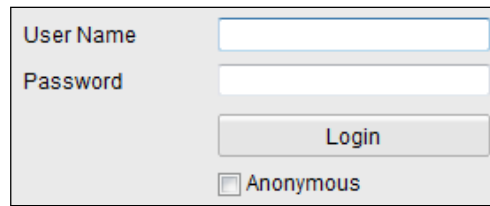


User	Authentication	Anonymous Visit	IP Address Filter	Security Service
Anonymous Visit Disable				
Save				

Figura 9–5 Vizită anonimă

2. Selectați din lista verticală permisiunea **Anonymous Visit** ca **Enable** sau ca **Disable** pentru a activa sau a dezactiva vizitarea anonimă.
3. Faceți clic pe **Save** pentru a salva setările.

Data următoare când vă conectați, va apărea o casetă Anonim.



User Name

Password

Login

☐ Anonymous

Figura 9–6 Interfață de conectare cu casetă de selectare Anonim

4. Bifați caseta **Anonymous** și faceți clic pe **Login**.

Activând funcția „Vizualizare live” anonimă, le puteți permite altora să vă acceseze camera și să vizualizeze imagini live fără să prezinte acreditări de conectare. Din acest motiv, este foarte important ca atunci când activați funcția de „V izualizare live” pentru Anonim să vă asigurați că câmpul de vizualizare a camerei nu afectează confidențialitatea persoanelor ale căror imagini pot fi capturate fără autorizare.

Datorită caracterului său invaziv inerent, supravegherea video nu este potrivită în zonele în care oamenii se așteaptă la un nivel de confidențialitate ridicat.

9.4 Filtru adresă IP

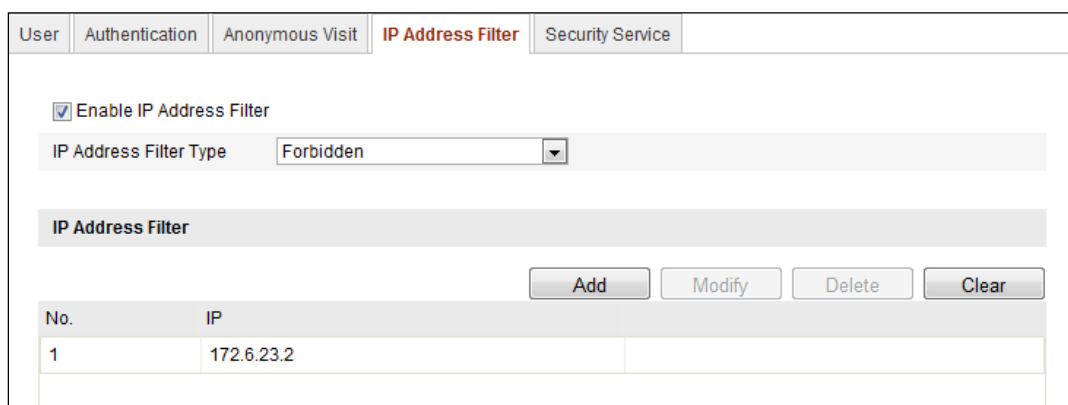
Scopul:

Această funcție permite controlul accesului.

Pași:

1. Accesați interfața IP Address Filter:

Configuration > Advanced Configuration > Security > IP Address Filter



User Authentication Anonymous Visit **IP Address Filter** Security Service

☒ Enable IP Address Filter

IP Address Filter Type Forbidden

IP Address Filter

Add Modify Delete Clear

No.	IP
1	172.6.23.2

Figura 9–7 Interfața filtru adresă IP

2. Bifați caseta de selectare **Enable IP Address Filter**.

3. Selectați din lista verticală tipul de Filtru adresă IP, puteți selecta **Forbidden** și **Allowed**.

4. Configurare listă Filtru adrese IP.

- Adăugarea unei adrese IP

Pași:

(1) Faceți clic pe **Add** pentru a adăuga un IP.

(2) Introduceți adresa IP.

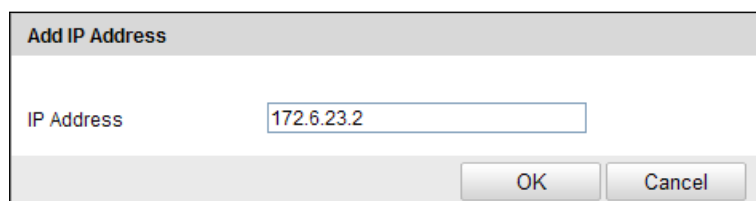


Figura 9–8 Adăugarea unei adrese IP

(3) Faceți clic pe **OK** pentru a finaliza adăugarea.

- Modificarea unei adrese IP

Pași:

(1) Faceți clic stânga pe o adresă IP din lista de filtrare și faceți clic pe **Modify**.

(2) Modificați adresa IP din câmpul de text.

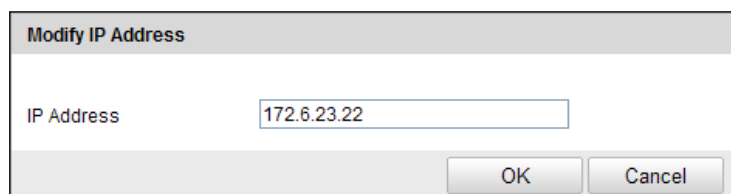


Figura 9–9 Modificare unui IP

(3) Faceți clic pe **OK** pentru a finaliza modificarea.

- Ștergerea unei adrese IP

Faceți clic stânga pe o adresă IP din lista de filtrare și faceți clic pe **Delete**.

- Ștergerea tuturor adreselor IP

Faceți clic pe **Clear** pentru a șterge toate adresele IP.

5. Faceți clic pe **Save** pentru a salva setările.

9.5 Serviciu de securitate

Pentru a activa conectarea la distanță și a îmbunătăți securitatea de comunicare a datelor, camera oferă serviciul de securitate pentru o mai bună experiență a utilizatorului.

Pași:

1. Intrați în interfața de configurare a serviciului de securitate:

Configuration > Advanced configuration > Security > Security Service



Figura 9–10 Serviciu de securitate

2. Bifați caseta **Enable SSH** pentru a activa securitatea comunicării datelor și debifați caseta pentru a dezactiva SSH.
3. Bifați caseta **Enable Illegal Login Lock**, după care dispozitivul va fi blocat dacă introduceți numele de utilizator sau parola incorect(ă) de 5 ori la rând.

Notă: Dacă dispozitivul este blocat, puteți încerca să vă conectați la dispozitiv după 30 de minute sau reinițializați dispozitivul înainte de a reîncerca.

9.6 Vizualizarea informațiilor despre dispozitiv

Accesați interfața Informații dispozitiv: **Configuration > Basic Configuration > System > Device Information** sau **Configuration > Advanced Configuration > System > Device Information**.

În interfața **Device Information**, puteți edita numele dispozitivului.

Sunt afișate alte informații despre camera de rețea, cum ar fi Model, Nr. serie, Versiune firmware, Versiune codificare, Număr de canale, Număr de HDD-uri, Număr intrare alarmă și Număr ieșire alarmă. Informațiile din acest meniu nu pot fi modificate. Acestea servesc drept referință sau modificare pe viitor.

Device Information	Time Settings	Maintenance	RS232	DST	Service	VCA Resource Type
---------------------------	---------------	-------------	-------	-----	---------	-------------------

Basic Information	
Device Name	THERMAL CAMERA
Device No.	88
Model	
Serial No.	
Firmware Version	V5.3.7 build 160711
Encoding Version	V7.3 build 160621
Number of Channels	1
Number of HDDs	0
Number of Alarm Input	2
Number of Alarm Output	2

Figura 9–11 Informații dispozitiv

9.7 Întreținere

9.7.1 Reinițializarea camerei

Pași:

1. Accesați interfața Maintenance:

Configuration > Basic Configuration > System > Maintenance

Sau **Configuration > Advanced Configuration > System > Maintenance**

2. Faceți clic pe **Reboot** pentru a reinițializa camera de rețea.

Reboot	
Reboot	Reboot the device.

Figura 9–12 Reinițializarea dispozitivului

9.7.2 Restabilirea setărilor implicite

Pași:

1. Accesați interfața Maintenance:

Configuration > Basic Configuration > System > Maintenance

Sau **Configuration > Advanced Configuration > System > Maintenance**

2. Faceți clic pe **Restore** sau pe **Default** pentru a restabili setările implicite.

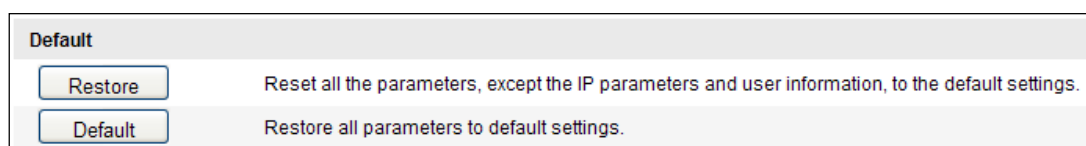


Figura 9–13 Restaurare setări implicite

Notă: După restabilirea setărilor implicite, adresa IP este, de asemenea, restabilită la adresa IP implicită, fiți atent la această acțiune.

9.7.3 Exportarea/Importarea fișierului de configurare

Scopul:

Fișierul de configurare este utilizat pentru configurarea ca lot a camerelor, ceea ce poate simplifica pașii configurării atunci când există o mulțime de camere ce necesită configurare.

Pași:

1. Accesați interfața Maintenance:

Configuration > Basic Configuration > System > Maintenance

sau **Configuration > Advanced Configuration > System > Maintenance**

2. Faceți clic pe **Export** pentru a exporta fișierul de configurare actual și salvați-l într-un loc anume.
3. Faceți clic pe **Browse** pentru a selecta fișierul de configurare salvat și apoi faceți clic pe **Import** pentru a începe să importați fișierul de configurare.

Notă: Trebuie să reporniți camera după importul fișierului de configurare.

4. Faceți clic pe **Export** și setați calea de salvare pentru a salva fișierul de configurare în stocarea locală.

The screenshot shows a web interface for configuration file management. It is divided into two main sections: 'Import Config. File' and 'Export Config. File'. In the 'Import' section, there is a text input field with the value 'F:\12', a 'Browse' button to the right, and an 'Import' button further right. Below this is a 'Status' label. The 'Export' section is below and contains a single 'Export' button.

Figura 9–14 Importarea/Exportarea fișierului de configurare

9.7.4 Actualizare sistem

Pași:

1. Accesați interfața Maintenance:

Configuration > Basic Configuration > System > Maintenance

sau **Configuration > Advanced Configuration > System > Maintenance**

2. Selectați firmware-ul sau directorul firmware pentru a localiza fișierul de upgrade.

Firmware: Localizați calea exactă a fișierului de upgrade.

Firmware Directory: Este necesar numai directorul de care aparține fișierul de upgrade.

3. Faceți clic pe **Browse** pentru a selecta fișierul de upgrade local, după care faceți clic pe **Upgrade** pentru a iniția upgrade-ul de la distanță.

The screenshot shows the 'Remote Upgrade' interface. It includes a 'Firmware' dropdown menu, a text input field, a 'Browse' button, and an 'Upgrade' button. Below these is a 'Status' section with a note: 'Note : The upgrading process will be 1 to 10 minutes, please don't disconnect power to the device during the process. The device reboots automatically after upgrading.'

Figura 9–15 Actualizare de la distanță

Notă: Procesul de actualizare durează între 1 și 10 minute. Nu întrerupeți alimentarea cu electricitate a dispozitivului în timpul acestui proces. Dispozitivul este reinițializat automat după upgrade.

9.8 Setările RS-485

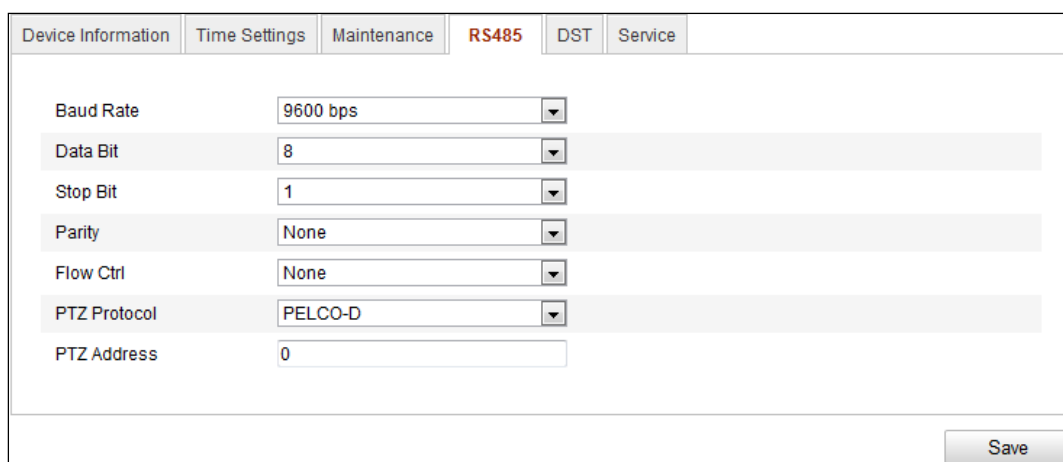
Scopul:

Portul serial RS-485 este utilizat pentru a controla PTZ-ul camerei. Configurarea parametrilor PTZ trebuie efectuată înainte de a controla unitatea PTZ.

Pași:

1. Accesați interfața Setări Port RS-485:

Configuration > Advanced Configuration > System > RS485



Device Information	Time Settings	Maintenance	RS485	DST	Service
Baud Rate: 9600 bps Data Bit: 8 Stop Bit: 1 Parity: None Flow Ctrl: None PTZ Protocol: PELCO-D PTZ Address: 0 Save					

Figura 9–16 Setări RS-485

2. Setati parametrii RS-485 și faceți clic pe **Save** pentru a salva setările.

În mod implicit, Rată transfer este setată ca 9600 bps, Bit de date, ca 8, Bit de oprire, ca 1, în timp ce Paritate și Control flux sunt setate ca Niciunul.

Notă: Parametrii Ratei de transfer, Protocolului PTZ și Adresei PTZ ar trebui să fie exact la fel ca parametrii PTZ ai camerei.

9.9 Setările serviciilor

Mergeți la **Configuration > Advanced Configuration > System > Service** pentru a accesa interfața setărilor serviciilor.

Setările serviciilor se referă la serviciile hardware acceptate de către cameră și variază în funcție de diversele camere.

Pentru camerele care acceptă LED IR, ABF (Focalizare spate automată), Dezaburire automată sau LED de stare, puteți merge la serviciul hardware și puteți selecta dacă să activați sau să dezactivați serviciul corespunzător în funcție de necesitățile actuale.

Pentru camera care acceptă încălzitorul de dezghețare, puteți bifa caseta pentru a activa dezghețarea automată.

Notă: Încălzitorul de dezghețare este acceptat numai dacă alimentarea cu electricitate se face ca POE+, 24 V c.a. sau 12 V c.c. Încălzitorul de dezghețare acceptă numai o alimentare electrică standard de tipul 802.3at, nu și alimentarea electrică standard de tipul 802.3af.

Anexă

Anexa 1 Introducere software SADP

● Descriere SADP

SADP (Search Active Devices Protocol) este un tip de instrument de căutare dispozitive, ușor de folosit și fără a fi necesară o instalare. Acesta caută dispozitivele online active din cadrul subrețelei și afișează informațiile aferente. De asemenea, cu ajutorul acestui software, puteți modifica informațiile de bază de rețea pentru aceste dispozitive.

● Căutarea dispozitivelor active online

◆ Căutarea automată a dispozitivelor online

După lansarea software-ului SADP, acesta caută automat dispozitivele online la fiecare 15 secunde din clasa subnet în care se află computerul dumneavoastră. Acesta afișează numărul total și informațiile pentru dispozitivele căutate din interfața Dispozitive online. Vor fi afișate informațiile de dispozitiv, inclusiv tipul de dispozitiv, adresa IP, numărul de port etc.

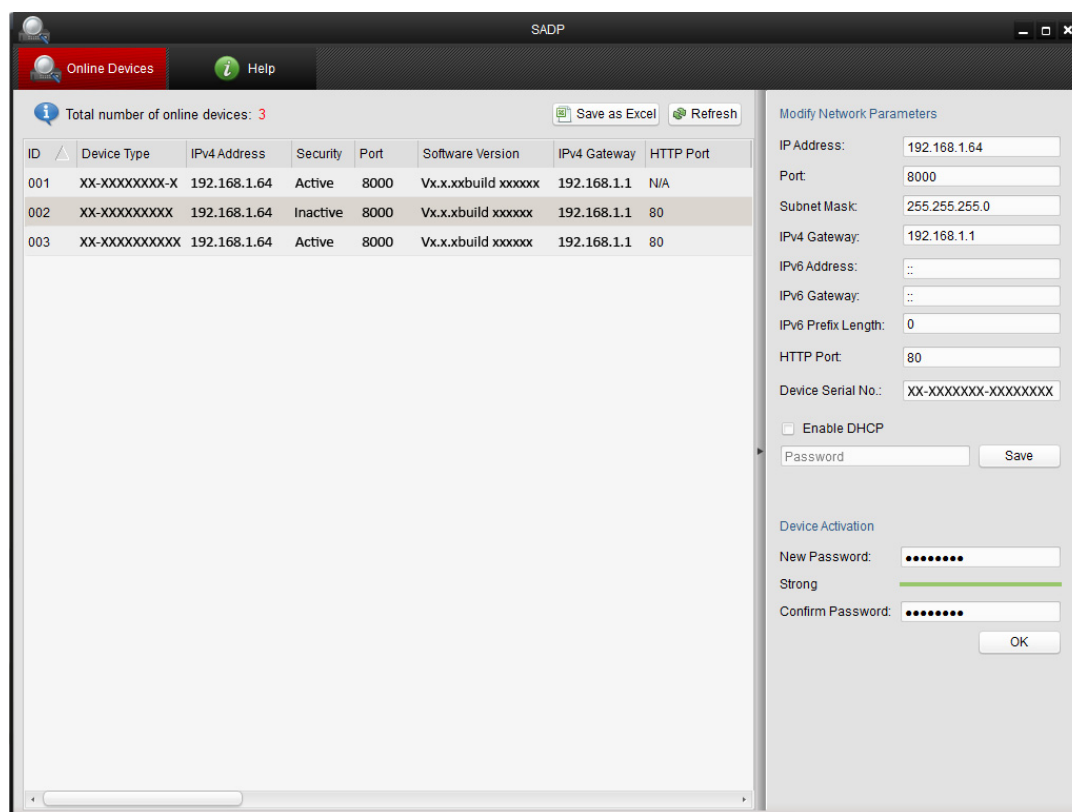
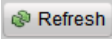


Figura A.1.1 Căutarea dispozitivelor online

Notă:

Dispozitivul poate fi căutat și afișat în listă după 15 secunde de la intrarea online; acesta va fi eliminat din listă în 45 de secunde după ce iese offline.

◆ **Căutarea manuală a dispozitivelor online**

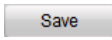
De asemenea, puteți face clic pe  pentru a reîmprospăta lista de dispozitive online manual. Noile dispozitive căutate vor fi adăugate la listă.



Puteți face clic pe  sau  din fiecare cap de coloană pentru a vizualiza informațiile; puteți face clic pe  pentru a desfășura tabelul cu dispozitive și pentru a ascunde panoul cu parametri de rețea din partea dreaptă, sau faceți clic pe  pentru a afișa panoul cu parametri de rețea.

● **Modificare parametri rețea**

Pași:

1. Selectați dispozitivul care urmează a fi modificat din lista de dispozitive și parametrii de rețea ai dispozitivului vor fi afișați în panoul **Modify Network Parameters** din partea dreaptă.
2. Editați parametrii de rețea care pot fi modificați, de exemplu, adresa IP și numărul portului.
3. Introduceți parola contului de administrare a dispozitivului în câmpul **Password** și faceți clic pe  pentru a salva modificările.



- *Pentru confidențialitatea dvs. și pentru a vă proteja mai bine sistemul împotriva riscurilor de securitate, vă recomandăm să utilizați parole puternice pentru toate funcțiile și dispozitivele de rețea. Parola trebuie să fie aleasă de către dvs. (folosind minimum 8 caractere, printre care majuscule, minuscule, cifre și caractere speciale) pentru a crește siguranța produsului dvs.*
- *Configurarea adecvată a tuturor parolelor și a altor setări de securitate este responsabilitatea instalatorului și/sau a utilizatorului final.*

Modify Network Parameters

IP Address:

192.168.1.64

Port:

8000

Subnet Mask:

255.255.255.0

IPv4 Gateway:

192.168.1.1

IPv6 Address:

3a3a::

IPv6 Gateway:

3a3a::

IPv6 Prefix Length:

64

Serial No.:

XX-XXXXXX-XXXXXX-XXXXXX

Password

Save

 Note: Enter the admin password of the device before you save the network parameters.

Figura A.1.2 Modificare parametri rețea

Anexa 2 Maparea portului

Următoarele setări sunt pentru routerul TP-LINK (TL-WR641G). Setările variază în funcție de diferite modele de routere.

Pași:

1. Selectați **WAN Connection Type**, după cum este indicat mai jos:

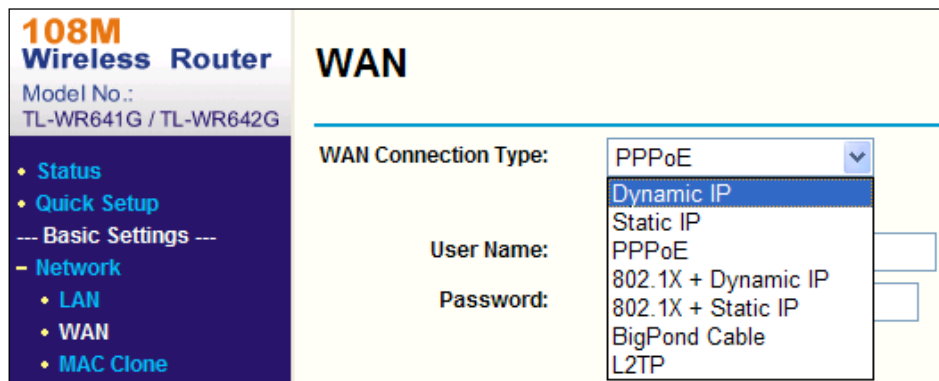


Figura A.2.1 Selectați tipul de conexiune WAN

2. Setați parametrii **LAN** ai routerului ca în figura de mai jos, inclusiv setările adresei IP și măștii de subrețea.

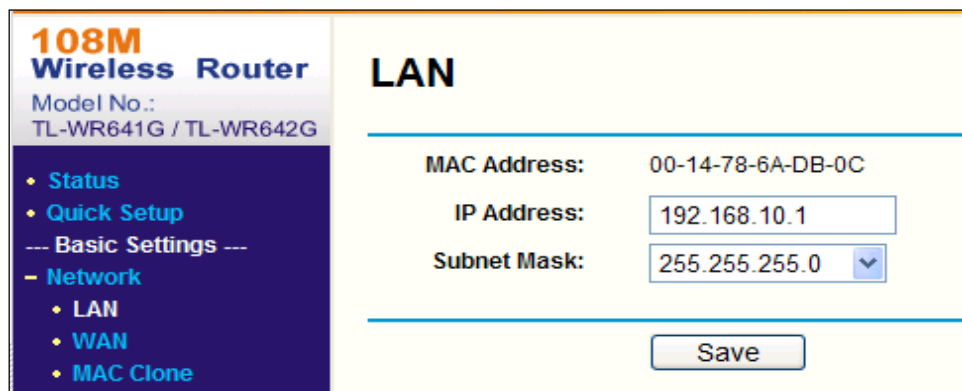


Figura A.2.2 Setați parametrii LAN

3. Setați maparea portului de pe serverele virtuale ca **Redirecționare**. Implicit, camera utilizează portul 80, 8000 și 554. Puteți schimba valoarea acestor porturi cu browserul web sau software-ul client.

Exemplu:

Când camerele sunt conectate la același router, puteți configura porturile unei camere ca 80, 8000 și 554 cu adresa IP 192.168.1.23, și porturile alte camere ca 81, 8001, 555, 8201 cu IP 192.168.1.24. Consultați etapele de mai jos:

Pași:

1. Ca setările menționate mai sus, mapați portul 80, 8000, 554 și 8200 pentru camera de rețea la 192.168.1.23
2. Mapați portul 81, 8001, 555 și 8201 pentru camera de rețea la 192.168.1.24.
3. Activați protocoalele **ALL** sau **TCP**.
4. Bifați caseta de selectare **Enable** și faceți clic pe **Save** pentru a salva setările.

108M Wireless Router
Model No.: TL-WR641G / TL-WR642G

- Status
- Quick Setup
- Basic Settings ---
- Network
- Wireless
- Advanced Settings ---
- DHCP
- Forwarding
 - Virtual Servers
 - Port Triggering
 - DMZ
 - UPnP
- Security
 - Static Routing
 - Dynamic DNS
- Maintenance ---
- System Tools

Virtual Servers

ID	Service Port	IP Address	Protocol	Enable
1	80	192.168.10.23	ALL	☒
2	8000	192.168.10.23	ALL	☒
3	554	192.168.10.23	ALL	☒
4	8200	192.168.10.23	ALL	☒
5	81	192.168.10.24	ALL	☒
6	8001	192.168.10.24	ALL	☒
7	555	192.168.10.24	ALL	☒
8	8201	192.168.10.24	ALL	☒

Common Service Port: DNS(53) Copy to ID 1

Previous Next Clear All Save

Figura A.2.3 Maparea portului

Notă: Portul camerei de rețea nu poate intra în conflict cu alte porturi. De exemplu, un port de gestionare web a routerului este 80. Schimbați portul camerei dacă acesta este același cu portul de gestionare.



First Choice for Security Professionals