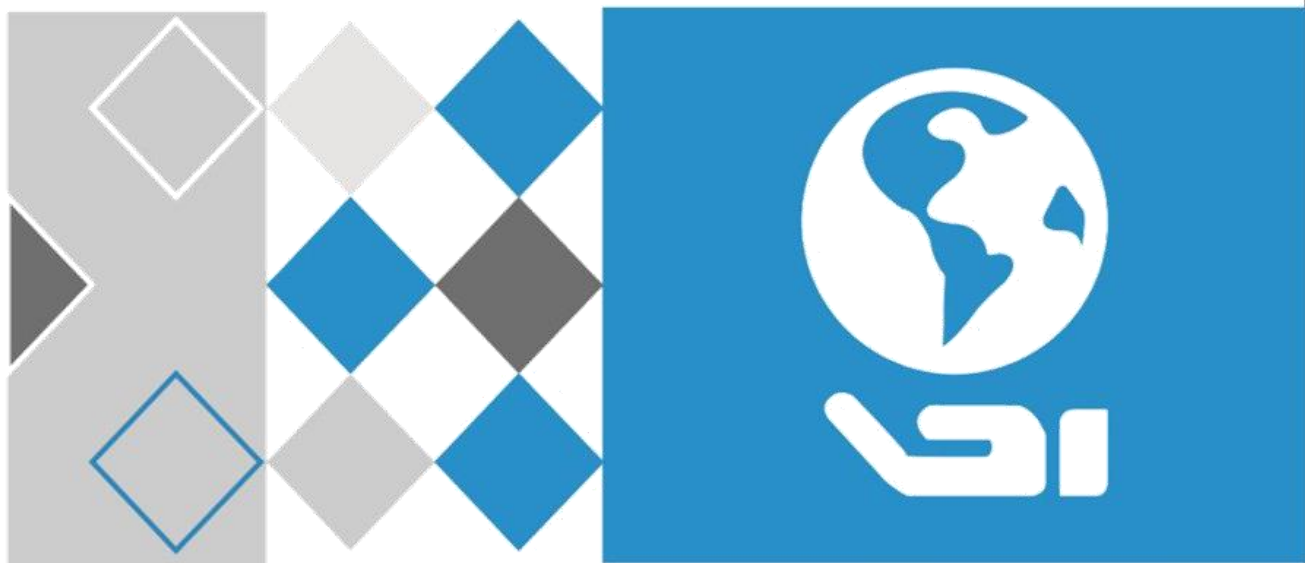


HiLook



Popis aplikace a funkcí pro síťové kamery HIKVISION

Uživatelský manuál
(UD11278)

Děkujeme, že jste si vybrali produkt Hikvision.

Technologie ovlivňuje každý aspekt našeho života. Jako high-tech společnost si stále více uvědomujeme roli, kterou technologie hraje při zlepšování obchodní efektivity a kvality života, ale zároveň si uvědomujeme potenciální škody způsobené jejich nesprávným používáním. Video produkty jsou například schopny zaznamenávat skutečný, úplný a jasný obraz. To poskytuje vysokou hodnotu při zpětném pohledu a zachování skutečností v reálném čase. Může však také vést k porušení osobních práv a zájmů třetí strany, pokud dojde k neoprávněné distribuci, použití a/nebo zpracování video dat. S filozofií „Technologie pro dobro“ požaduje Hikvision, aby každý koncový uživatel videotechnologie a produktů Hikvision dodržoval všechny platné zákony a předpisy, stejně jako etické zvyky, s cílem společně vytvořit lepší komunitu.

Přečtěte si prosím pozorně následující:

- Každý má rozumné očekávání ohledně soukromí a instalace video produktů by neměla být v rozporu s tímto rozumným očekáváním. Při instalaci video produktů ve veřejných prostorách by proto mělo být přiměřeným a účinným způsobem uvedeno varování a mělo by být objasněn rozsah monitorování. U neveřejných oblastí budou při instalaci video produktů vyhodnocena práva a zájmy třetích stran, včetně, ale nikoli výhradně, instalace video produktů pouze po získání souhlasu zúčastněných stran a nikoli instalace vysoce neviditelných video produktů.
- Účelem video produktů je zaznamenat skutečné aktivity v konkrétním čase a prostoru a za specifických podmínek. Každý uživatel si proto nejprve přiměřeně vymezí svá práva v takovém konkrétním rozsahu, aby se vyhnul zásahu do soukromí či jiných zákonných práv třetí osoby.
- Během používání video produktů budou nadále generována obrazová data odvozená ze skutečných scén, včetně velkého množství biologických dat (jako jsou snímky obličeje), a data by mohla být dále aplikována nebo znovu zpracována. Video produkty samy o sobě nedokáží rozlišit dobré od špatného, pokud jde o to, jak používat data založená pouze na snímcích zachycených video produkty. Výsledek použití údajů závisí na způsobu a účelu použití správci údajů. Správci údajů proto nejen dodržují všechny platné zákony a předpisy a další normativní požadavky, ale také respektují mezinárodní normy, společenskou morálku, dobré mravy, běžné postupy a další nezávazné požadavky a respektují soukromí, portrét a další práva a zájmy.
- Práva, hodnoty a další požadavky různých zúčastněných stran by měly být vždy brány v úvahu při zpracování video dat, která jsou nepřetržitě generována video produkty. V tomto ohledu je mimořádně zásadní bezpečnost produktu a zabezpečení dat. Každý koncový uživatel a správce údajů proto přijme veškerá přiměřená a nezbytná opatření, aby zajistil bezpečnost údajů a zabránil úniku údajů, nesprávnému zveřejnění a nesprávnému použití, mimo jiné včetně nastavení řízení přístupu, výběru vhodného síťového prostředí (internetu nebo intranet), kde jsou připojeny video produkty, čímž se vytváří a neustále optimalizuje zabezpečení sítě.
- Video produkty významně přispěly ke zlepšení sociálního zabezpečení po celém světě a věříme, že tyto produkty budou hrát aktivní roli i ve více aspektech společenského života. Jakékoli zneužití video produktů v rozporu s lidskými právy nebo vedoucí k trestné činnosti je v rozporu s původním záměrem technologických inovací a vývoje produktů. Každý uživatel si proto musí vytvořit mechanismus hodnocení a sledování své aplikace produktu, aby zajistil, že každý produkt bude používán správným a přiměřeným způsobem a v dobré víře.

O této příručce

Manuál obsahuje pokyny pro používání a správu produktu. Obrázky, grafy a všechny další informace níže slouží pouze pro popis a vysvětlení. Informace obsažené v příručce se mohou bez upozornění změnit v důsledku aktualizací firmwaru nebo z jiných důvodů. Nejnovější verzi této příručky naleznete na webových stránkách Hikvision (<https://www.hikvision.com/>).

Používejte prosím tuto příručku s vedením a pomocí profesionálů vyškolených v podpoře produktu.

ochranné známky

HiLook a další ochranné známky a loga společnosti Hikvision jsou majetkem společnosti Hikvision v různých jurisdikcích. Ostatní ochranné známky a loga uvedená níže jsou majetkem příslušných vlastníků.

Ostatní uvedené ochranné známky a loga jsou majetkem příslušných vlastníků.

Zřeknutí se odpovědnosti

V MAXIMÁLNÍM ROZSAHU POVOLENÉM PLATNÝM ZÁKONEM JSOU TENTO NÁVOD A POPISOVANÝ PRODUKT S HARDWAREM, SOFTWAREM A FIRMWAREM POSKYTOVÁNY „TAK JAK JSOU“ A „SE VŠEMI CHYBAMI A CHYBAMI“. HIKVISION NEPOSKYTUJE ŽÁDNÉ ZÁRUKY, VÝSLOVNÉ ANI PŘEDPOKLÁDANÉ, VČETNĚ, BEZ OMEZENÍ, OBCHODOVATELNOSTI, USPOKOJIVÉ KVALITY NEBO VHODNOSTI PRO KONKRÉTNÍ ÚČEL. POUŽÍVÁNÍ PRODUKTU JE NA VLASTNÍ RIZIKO. V ŽÁDNÉM PŘÍPADĚ VÁM NEBUDE HIKVISION ODPOVĚDNÁ ZA JAKÉKOLI ZVLÁŠTNÍ, NÁSLEDNÉ, NÁHODNÉ NEBO NEPŘÍMÉ ŠKODY, VČETNĚ, MIMO JINÉ, ŠKOD ZA ZTRÁTU ZISKŮ Z OBCHODNÍHO ZIMU, PŘERUŠENÍ OBCHODNÍ ČINNOSTI NEBO ZTRÁTU DAT, PORUŠENÍ SYSTÉMU AŽ NA ZÁKLADĚ PORUŠENÍ SMLOUVY, deliktu (VČETNĚ NEDBALOSTI), ODPOVĚDNOSTI ZA PRODUKT NEBO JINAK V SOUVISLOSTI S POUŽÍVÁNÍM PRODUKTU, I KDYŽ BYLA HIKVISION UPOZORNĚNA NA MOŽNOST TAKOVÝCH ŠKOD NEBO ZTRÁTY.

BERETE NA VĚDOMÍ, ŽE POVAHA INTERNETU POSKYTUJE PŘIROZENÁ BEZPEČNOSTNÍ RIZIKA, A HIKVISION NEPŘEBERE ŽÁDNOU ODPOVĚDNOST ZA ABNORMÁLNÍ PROVOZ, ÚNIK OCHRANY SOUKROMÍ NEBO JINÉ ŠKODY VYPLÝVAJÍCÍ V NÁSLEDUJÍCÍCH KYBERNETICKÝCH ÚTOKŮ, JINÝCH BEZPEČNOSTNÍCH ÚTOKŮ, INTERNETHACKERKS; V PŘÍPADĚ POŽADAVKY VŠAK HIKVISION POSKYTNE VČASNOU TECHNICKOU PODPORU.

SOUHLASÍTE S POUŽÍVÁNÍM TENTO PRODUKT V SOULADU SE VŠEMI PŘÍSLUŠNÝMI ZÁKONY A JSTE VÝHRADNĚ ODPOVĚDNÍ ZA ZAJIŠTĚNÍ, ŽE VAŠE POUŽÍVÁNÍ JE V SOULADU S PŘÍSLUŠNÝMI ZÁKONY. ZVLÁŠTNĚ JSTE ODPOVĚDNÍ ZA POUŽÍVÁNÍ TOHOTO PRODUKTU ZPŮSOBEM, KTERÝ NEPORUŠUJE PRÁVA TŘETÍCH STRAN, VČETNĚ, BEZ OMEZENÍ, PRÁVA NA PUBLICITA, PRÁVA DUŠEVNÍHO VLASTNICTVÍ NEBO OCHRANA DAT A JINÁ PRÁVA SOUKROMÍ. NESMÍTE TENTO PRODUKT POUŽÍVAT K ŽÁDNÉMU ZAKÁZANÉMU KONCOVÉMU POUŽITÍ, VČETNĚ

VÝVOJ NEBO VÝROBA ZBRANÍ HROMADNÉHO NIČENÍ, VÝVOJ NEBO VÝROBA CHEMICKÝCH NEBO BIOLOGICKÝCH ZBRANÍ, JAKÉKOLI ČINNOSTI V SOUVISLOSTI S JAKÝKOLI JADERNÝM VÝBUŠNÝM NEBO NEBEZPEČNÝM CYKLUSEM JADERNÉHO PALIVA NEBO PŘI SUPĚNÍ RHUMAN




V PŘÍPADĚ JAKÝCHKOLI KONFLIKTŮ MEZI TÍMTO NÁVODEM A PLATNÝM ZÁKONEM, PŘEVLÁDÁ POZDĚJŠÍ.

Aktualizujte firmware

Pro lepší uživatelský zážitek vám doporučujeme co nejdříve aktualizovat vaše zařízení na nejnovější firmware. Získejte nejnovější balíček firmwaru z oficiálních webových stránek nebo od místního technického odborníka. Další informace naleznete na oficiálních stránkách: <https://www.hikvision.com/en/support/download/firmware/>. Nastavení upgradu viz [Upgrade](#).

Symbolové konvence

Symbole, které lze nalézt v tomto dokumentu, jsou definovány následovně.

Symbol	Popis
Nebezpečí 	Označuje nebezpečnou situaci, která, pokud se jí nevyhnete, nastane nebo může způsobit smrt nebo vážné zranění.
Pozor 	Označuje potenciálně nebezpečnou situaci, která, pokud se jí nevyhnete, může vést k poškození zařízení, ztrátě dat, výkonu degradace nebo neočekávané výsledky.
Poznámka 	Poskytuje další informace ke zdůraznění nebo doplnění důležité body hlavního textu.

Bezpečnostní instrukce

Účelem těchto pokynů je zajistit, aby uživatel mohl výrobek správně používat, aby se zabránilo nebezpečí nebo ztrátě majetku.

Zákony a předpisy

- Zařízení by mělo být používáno v souladu s místními zákony, předpisy o elektrické bezpečnosti a předpisy o prevenci požárů.

Přeprava

- Při přepravě uchovávejte zařízení v originálním nebo podobném obalu.

Zdroj napájení

- Vstupní napětí by mělo odpovídat normě IEC60950-1: SELV (Safety Extra Low Voltage) a omezený zdroj napájení. Podrobné informace naleznete v příslušné dokumentaci.
- Ujistěte se, že je zástrčka správně zapojena do elektrické zásuvky.
- **NEPŘIPOJUJTE** více zařízení k jednomu napájecímu adaptéru, aby nedošlo k přehřátí nebo požáru způsobenému přetížením.

Zabezpečení systému

- Instalační technik a uživatel jsou odpovědní za konfiguraci hesla a zabezpečení a jeho nastavení.

Baterie

- Nesprávné použití nebo výměna baterie může způsobit nebezpečí výbuchu.
- Vyměňte pouze za stejný nebo ekvivalentní typ. Použité baterie zlikvidujte v souladu s místními předpisy.

Údržba

- Pokud výrobek nefunguje správně, kontaktujte svého prodejce nebo nejbližší servisní středisko. Nepřebíráme žádnou odpovědnost za problémy způsobené neoprávněnou opravou nebo údržbou.

- Několik součástí zařízení (např. elektrolytický kondenzátor) vyžaduje pravidelnou výměnu. Průměrná životnost se liší, proto se doporučuje pravidelná kontrola. Podrobnosti vám sdělí prodejce.

Použití prostředí

- Ujistěte se, že běžící prostředí splňuje požadavky zařízení. Provozní teplota musí být -30 °C až 60 °C (-22 °F až 140 °F) a provozní vlhkost musí být 95 % nebo méně, bez kondenzace.
- Při používání jakéhokoli laserového zařízení se ujistěte, že čočka zařízení není vystavena laserovému paprsku, jinak by se mohla spálit.
- Nevystavujte zařízení silnému elektromagnetickému záření nebo prašnému prostředí.
- Zařízení určené pouze pro vnitřní použití umístěte do suchého a dobře větraného prostředí.
- Nemiřte objektivem do slunce nebo jiného jasného světla.

Nouze

- Pokud ze zařízení vychází kouř, zápach nebo hluk, okamžitě vypněte napájení, odpojte napájecí kabel a kontaktujte servisní středisko.

Synchronizace času

- Pokud není místní čas synchronizován s časem sítě, nastavte čas kamery pro první přístup ručně. Navštivte kameru prostřednictvím webového prohlížeče/klientského softwaru a přejděte do rozhraní nastavení času.

Obsah

[Kapitola 1](#) Požadavky na systém

[Kapitola 2](#) Síťové připojení

- 2.1 Nastavení síťové kamery přes síť LAN
 - 2.1.1 Zapojení přes síť LAN
 - 2.1.2 Aktivace kamery
- 2.2 Nastavení síťové kamery přes síť WAN
 - 2.2.1 Statické připojení IP
 - 2.2.2 Dynamické připojení IP

[Kapitola 3](#) Přístup k síťové kameře

- 3.1 Přístup pomocí webových prohlížečů
- 3.2 Přístup pomocí klientského softwaru

[Kapitola 4](#) Nastavení Wi-Fi

- 4.1 Konfigurace připojení Wi-Fi v režimech Správa a Ad-hoc
- 4.2 Snadné připojení Wi-Fi pomocí funkce WPS
- 4.3 Nastavení vlastností IP pro připojení k bezdrátové síti

[Kapitola 5](#) Živé zobrazení

- 5.1 Stránka živého náhledu
- 5.2 Spuštění živého náhledu
- 5.3 Ruční nahrávání a pořizování snímků
- 5.4 Ovládání PTZ
 - 5.4.1 Ovládací panel PTZ
 - 5.4.2 Nastavení/vyvolání předvolby
 - 5.4.3 Nastavení/svolání hlídky

[Kapitola 6](#) Konfigurace síťové kamery

- 6.1 Konfigurace místních parametrů
- 6.2 Konfigurace nastavení systému
 - 6.2.1 Konfigurace základních informací
 - 6.2.2 Konfigurace nastavení času
 - 6.2.3 Konfigurace nastavení letního času
 - 6.2.4 Konfigurace nastavení RS232
 - 6.2.5 Zobrazení licence
- 6.3 Údržba
 - 6.3.1 Upgrade a údržba
 - 6.3.2 Přihlásit se
 - 6.3.3 Systémová služba
- 6.4 Nastavení zabezpečení
 - 6.4.1 Ověřování
 - 6.4.2 Filtr IP adres
 - 6.4.3 Bezpečnostní služba
- 6.5 Správa uživatelů
 - 6.5.1 Správa uživatelů
 - 6.5.2 Online uživatelé

[Kapitola 7 Nastavení sítě](#)

- 7.1 Konfigurace základních nastavení
 - 7.1.1 Konfigurace nastavení TCP/IP
 - 7.1.2 Konfigurace nastavení DDNS
 - 7.1.3 Konfigurace nastavení PPPoE
 - 7.1.4 Konfigurace nastavení portu
 - 7.1.5 Konfigurace nastavení překladu síťových adres (NAT)
- 7.2 Konfigurace pokročilých nastavení
 - 7.2.1 Konfigurace nastavení SNMP
 - 7.2.2 Konfigurace nastavení FTP
 - 7.2.3 Konfigurace nastavení e-mailu
 - 7.2.4 Přístup k platformě
 - 7.2.5 Nastavení HTTPS
 - 7.2.6 Konfigurace nastavení QoS
 - 7.2.7 Konfigurace nastavení 802.1X
 - 7.2.8 Protokol o integraci

[Kapitola 8 Nastavení videa a zvuku](#)

- 8.1 Konfigurace nastavení videa
- 8.2 Konfigurace nastavení zvuku
- 8.3 Konfigurace kódování ROI
- 8.4 Zobrazení informací na streamu

[Kapitola 9 Nastavení obrazu](#)

- 9.1 Konfigurace nastavení displeje
 - 9.1.1 Automatické přepínání den/noc
 - 9.1.2 Denní/noční plánovaný přepínač
- 9.2 Konfigurace nastavení OSD
- 9.3 Konfigurace masky soukromí

[Kapitola 10 Nastavení událostí](#)

- 10.1 Základní události
 - 10.1.1 Konfigurace detekce pohybu
 - 10.1.2 Konfigurace alarmu proti neoprávněné manipulaci s videem
 - 10.1.3 Konfigurace vstupu alarmu
 - 10.1.4 Konfigurace výstupu alarmu
 - 10.1.5 Konfigurace alarmu PIR
 - 10.1.6 Zpracování výjimky
- 10.2 Chytré události
 - 10.2.7 Konfigurace detekce narušení
 - 10.2.8 Konfigurace detekce křížení vedení

[Kapitola 11 Nastavení úložiště](#)

- 11.1 Konfigurace plánu záznamů
- 11.2 Konfigurace plánu snímání
- 11.3 Konfigurace pevného disku Net HDD

[Kapitola 12 Přehrávání](#)

[Kapitola 13 Snímek](#)

Kapitola 1 Požadavky na systém

Operační systém: Microsoft Windows XP a vyšší verze

CPU: 3,0 GHz nebo vyšší

Paměť RAM: 1G nebo více

Zobrazení: Rozlišení: 1024×768 nebo vyšší

Webový prohlížeč: Internet Explorer 8.0 a vyšší verze, Apple Safari 8.0 a vyšší verze, Mozilla Firefox 30.0-51 a Google Chrome 31.0-44.

Kapitola 2 Připojení k síti

● Berete na vědomí, že používání produktu s přístupem na internet může být ohroženo bezpečnostními riziky sítě. Abyste předešli případným síťovým útokům a úniku informací, posilte prosím svou vlastní ochranu. Pokud výrobek nefunguje správně, obraťte se na svého prodejce nebo nejbližší servisní středisko.

● Pro zajištění bezpečnosti síťové kamery doporučujeme nechat síťovou kameru pravidelně vyhodnocovat a udržovat. Pokud takovou službu potřebujete, můžete se na nás obrátit.

Než začnete:

● Pokud chcete síťovou kameru nastavit prostřednictvím sítě LAN (Local Area Network), přečtěte si část 2.1 Nastavení síťové kamery prostřednictvím sítě LAN.

● Pokud chcete síťovou kameru nastavit prostřednictvím sítě WAN (Wide Area Network), přečtěte si část 2.2 Nastavení síťové kamery prostřednictvím sítě WAN.

2.1 Nastavení síťové kamery přes síť LAN

Účel:

Chcete-li zobrazit a konfigurovat kameru prostřednictvím sítě LAN, musíte síťovou kameru připojit do stejné podsítě s počítačem a nainstalovat software SADP nebo HiLookVision pro vyhledání a změnu IP adresy síťové kamery.

Poznámka: Podrobné představení SADP naleznete v příloze 1.

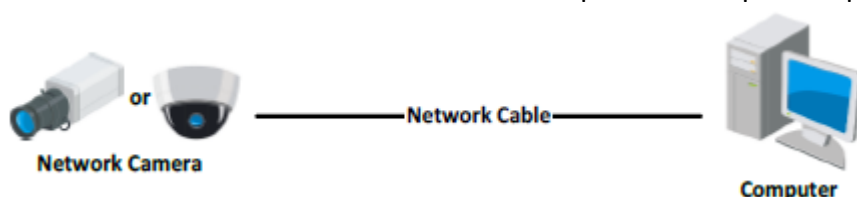
2.1.1 Zapojení přes síť LAN

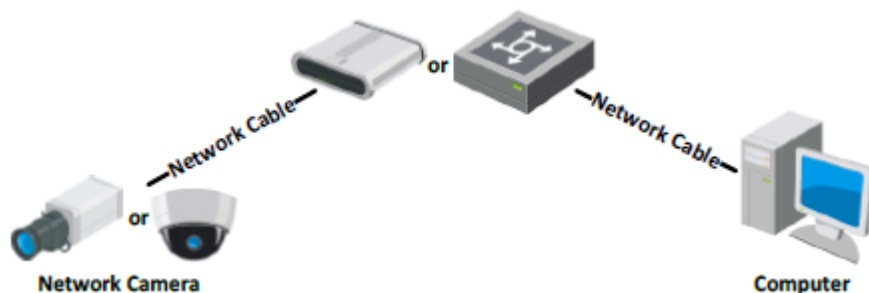
Následující obrázky ukazují dva způsoby kabelového propojení síťové kamery a počítače:

Účel:

● Chcete-li otestovat síťovou kameru, můžete ji přímo připojit k počítači pomocí síťového kabelu, jak je znázorněno na obrázku 2-1.

● Podle obrázku 2-2 nastavte síťovou kameru přes síť LAN pomocí přepínače nebo směrovače.





Obrázek 2-2

2.1.2 Aktivace kamery

Před použitím kamery je nutné je nejprve aktivovat nastavením silného hesla. Podporována je aktivace prostřednictvím webového prohlížeče, aktivace prostřednictvím SADP a aktivace prostřednictvím klientského softwaru.

◆Aktivace prostřednictvím webového prohlížeče

Kroky:

1. Zapněte kameru a připojte je k síti.
2. Zadejte IP adresu do adresního řádku webového prohlížeče a kliknutím na tlačítko Enter vstupte do aktivačního rozhraní.

Poznámky:

- Výchozí IP adresa kamery je 192.168.1.64.
- Ve výchozím nastavení je u kamery zapnuto DHCP, IP adresa je přidělena automaticky. A je třeba ji aktivovat prostřednictvím softwaru SADP. Viz v následující kapitole Aktivace prostřednictvím SADP.

Obrázek 2-3 Aktivace prostřednictvím webového prohlížeče

3. Vytvořte heslo a zadejte je do pole pro zadání hesla.
4. Potvrďte heslo.
5. Kliknutím na tlačítko OK uložte heslo a vstupte do rozhraní živého náhledu.

◆Aktivace prostřednictvím softwaru SADP

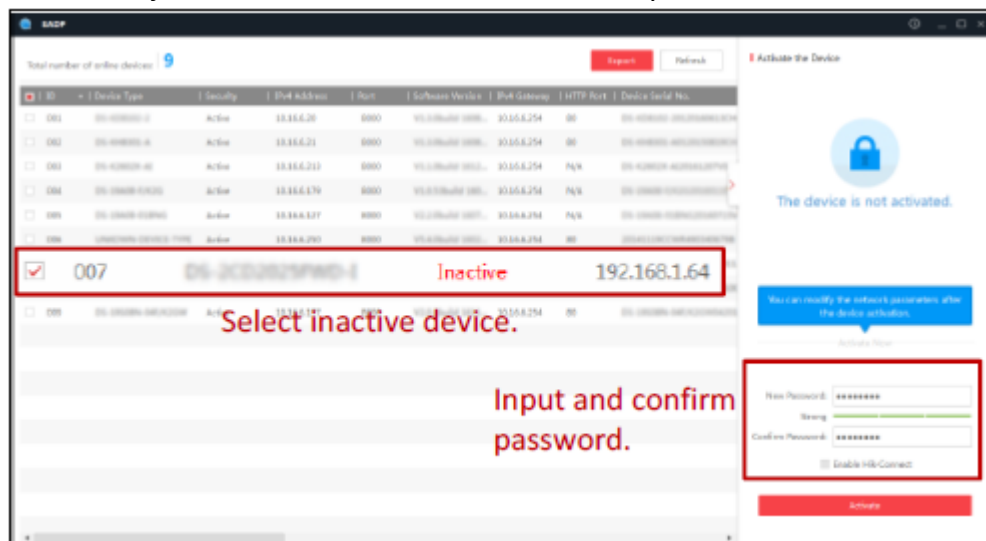
Software SADP slouží k detekci online zařízení, aktivaci kamery a resetování hesla.

Získejte software SADP z dodaného disku nebo z oficiálních webových stránek a nainstalujte jej podle pokynů. Postupujte podle pokynů pro aktivaci kamery.

DOPORUČUJEME SILNÉ HESLO - v zájmu zvýšení bezpečnosti vašeho produktu doporučujeme vytvořit silné heslo podle vlastního výběru (s použitím minimálně 8 znaků, včetně alespoň tří z následujících kategorií: velká písmena, malá písmena, číslice a speciální znaky). A doporučujeme vám pravidelně obnovovat heslo, zejména v systému s vysokým zabezpečením, a obnovovat heslo každý měsíc nebo každý týden může lépe chránit váš produkt.

Kroky:

1. Spusťte software SADP a vyhledejte zařízení online.
2. Zkontrolujte stav zařízení v seznamu zařízení a vyberte neaktivní zařízení.



Obrázek 2-4 Rozhraní SADP

3. Vytvořte heslo, zadejte je do pole pro zadání hesla a potvrďte je.

4. Heslo uložíte kliknutím na tlačítko OK.

Ve vyskakovacím okně můžete zkontrolovat, zda byla aktivace dokončena. Pokud se aktivace nezdařila, zkontrolujte, zda heslo splňuje požadavky, a zkuste to znovu.

5. Změňte IP adresu zařízení na stejnou podsíť s počítačem buď ruční úpravou IP adresy, nebo zaškrtnutím políčka Povolit DHCP.

Vyberte neaktivní zařízení. Zadejte a potvrďte heslo.

Modify Network Parameters

Enable DHCP
 Enable Hik-Connect

Device Serial No.: XXX-XXXXXXXX-XXXXXXXXXXXXXXXXXX

IP Address: 192.168.1.64

Port: 8000

Subnet Mask: 255.255.255.0

Gateway: 192.168.1.1

IPv6 Address: ::

IPv6 Gateway: ::

IPv6 Prefix Length: 0

HTTP Port: 80

Security Verification

Admin Password:

Modify

[Forgot Password](#)

Obrázek 2-5 Úprava IP adresy

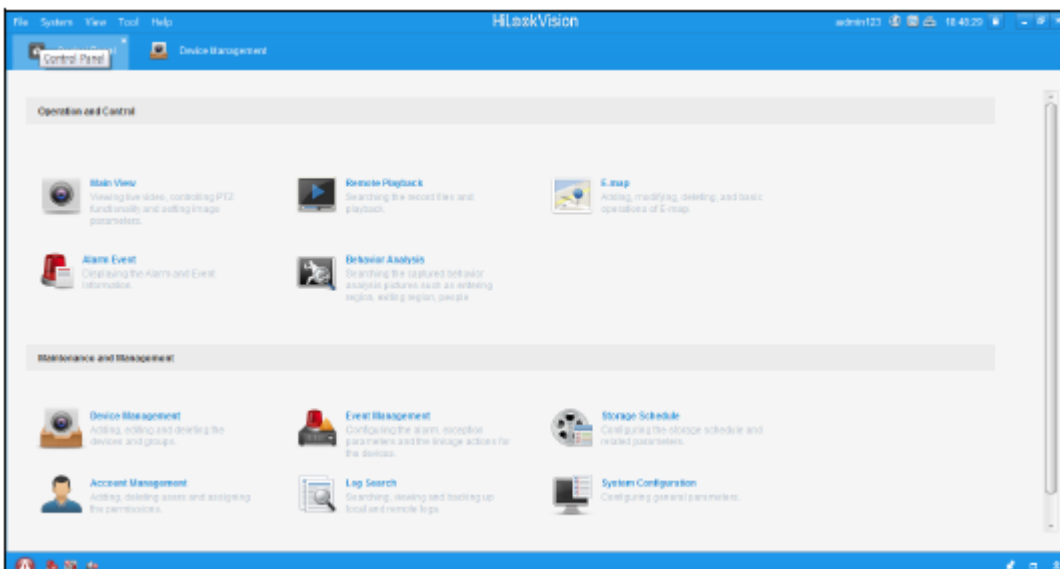
6. Zadejte heslo a kliknutím na tlačítko Upravit aktivujete úpravu IP adresy.

❖ Aktivace prostřednictvím klientského softwaru

Klientský software je univerzální software pro správu videa pro různé druhy zařízení. Získejte klientský software z dodaného disku nebo z oficiálních webových stránek a nainstalujte jej podle pokynů. Postupujte podle pokynů pro aktivaci kamery.

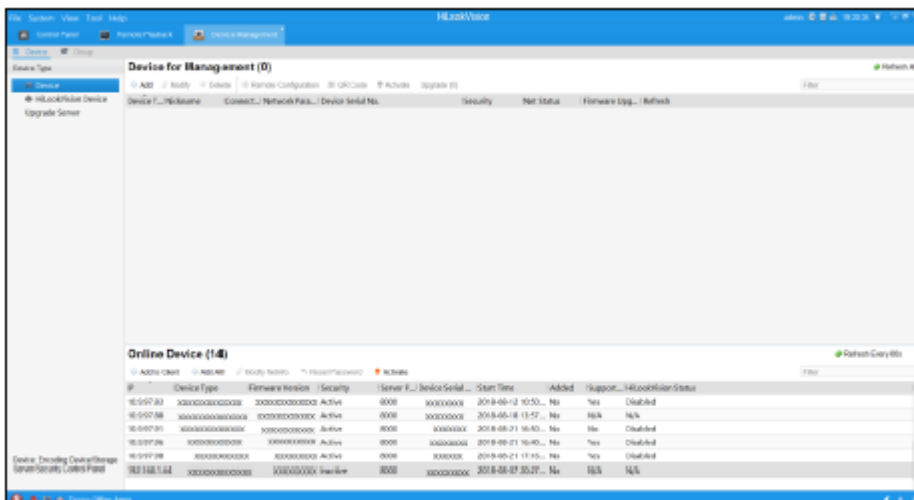
Kroky:

1. Spusťte klientský software a zobrazí se ovládací panel softwaru, jak je znázorněno na obrázku níže.



Obrázek 2-6 Ovládací panel

2. Kliknutím na ikonu Správa zařízení vstoupíte do rozhraní Správa zařízení, jak je znázorněno na obrázku níže.

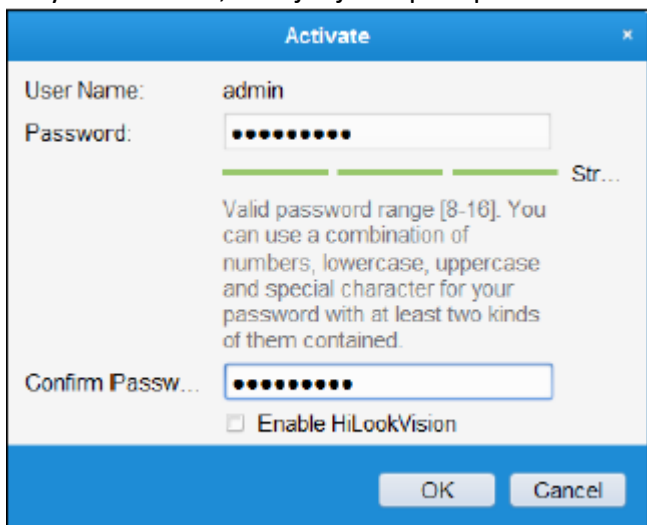


Obrázek 2-7 Rozhraní pro správu zařízení

3. Zkontrolujte stav zařízení v seznamu zařízení a vyberte neaktivní zařízení.

4. Kliknutím na tlačítko Aktivovat zobrazíte aktivační rozhraní.

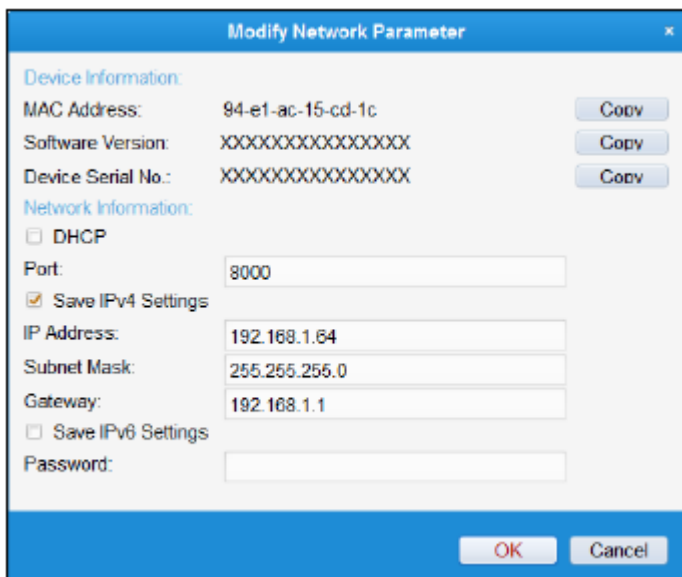
5. Vytvořte heslo, zadejte je do pole pro zadání hesla a potvrďte je.



Obrázek 2-8 Aktivační rozhraní (klientský software)

6. Kliknutím na tlačítko OK zahájíte aktivaci.

7. Kliknutím na tlačítko Modifikace Netinfo se zobrazí rozhraní pro úpravu síťových parametrů, jak je znázorněno na obrázku níže.



Obrázek 2-9 Úprava parametrů sítě

8. Změňte IP adresu zařízení na stejnou podsít s počítačem buď ruční úpravou IP adresy, nebo zaškrtnutím políčka Povolit DHCP.

9. Zadáním hesla aktivujete změnu IP adresy.

2.2 Nastavení síťové kamery přes síť WAN

Účel:

Tato část vysvětluje, jak připojit síťovou kameru k síti WAN pomocí statické nebo dynamické IP adresy.

2.2.1 Statické připojení IP

Než začnete:

Použijte statickou IP adresu od poskytovatele internetových služeb (ISP). Se statickou IP adresou můžete síťovou kameru připojit přes směrovač nebo ji připojit přímo k síti WAN.

● Připojení síťové kamery přes směrovač

Kroky:

1. Připojte síťovou kameru ke směrovači.

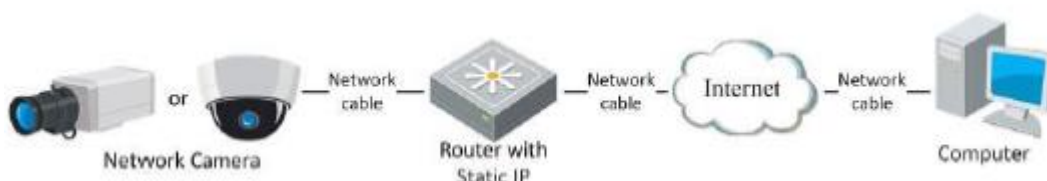
2. Přiřadte adresu IP sítě LAN, masku podsítě a bránu. Podrobnou konfiguraci IP adresy síťové kamery naleznete v části 2.1.2.

3. Uložte statickou adresu IP do směrovače.

4. Nastavte mapování portů, např. porty 80, 8000 a 554. Kroky pro mapování portů se liší podle různých směrovačů. O pomoc s mapováním portů požádejte výrobce směrovače.

Poznámka: Podrobné informace o mapování portů najdete v dodatku 2.

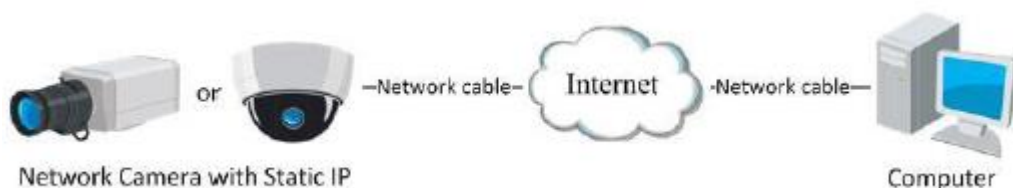
5. Navštivte síťovou kameru prostřednictvím webového prohlížeče nebo klientského softwaru přes internet.



Obrázek 2-10 Přístup ke kameře přes směrovač se statickou IP adresou

- Přímé připojení síťové kamery se statickou IP adresou

Statickou IP adresu můžete také uložit do kamery a připojit ji přímo k internetu bez použití směrovače. Podrobnou konfiguraci IP adresy síťové kamery naleznete v části 2.1.2.



Obrázek 2-11 Přímý přístup ke kameře se statickou IP adresou

2.2.2 Dynamické připojení IP

Než začnete:

Použijte dynamickou IP od poskytovatele internetových služeb. S dynamickou IP adresou můžete síťovou kameru připojit k modemu nebo směrovači.

- Připojení síťové kamery přes směrovač

Kroky:

21

1.Připojte síťovou kameru ke směrovači.

2.Kameře přiřadte IP adresu sítě LAN, masku podsítě a bránu. Podrobnou konfiguraci IP adresy síťové kamery naleznete v části 2.1.2.

3.Ve směrovači nastavte uživatelské jméno PPPoE, heslo a potvrďte je.

4.Nastavení mapování portů. Např. porty 80, 8000 a 554. Kroky pro mapování portů se liší v závislosti na různých směrovačích. O pomoc s mapováním portů požádejte výrobce směrovače.

Poznámka: Podrobné informace o mapování portů najdete v dodatku 2.

5.Použijte název domény od poskytovatele doménových jmen.

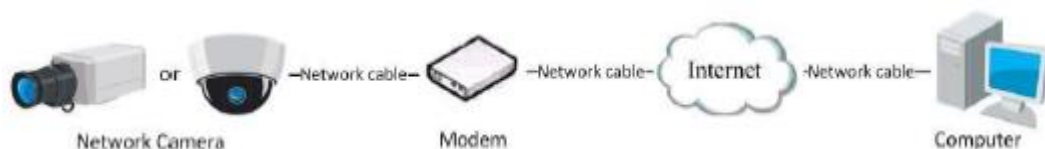
6.Konfigurace nastavení DDNS v rozhraní nastavení směrovače.

7.Navštivte kameru prostřednictvím použitého názvu domény.

- Připojení síťové kamery přes modem

Účel:

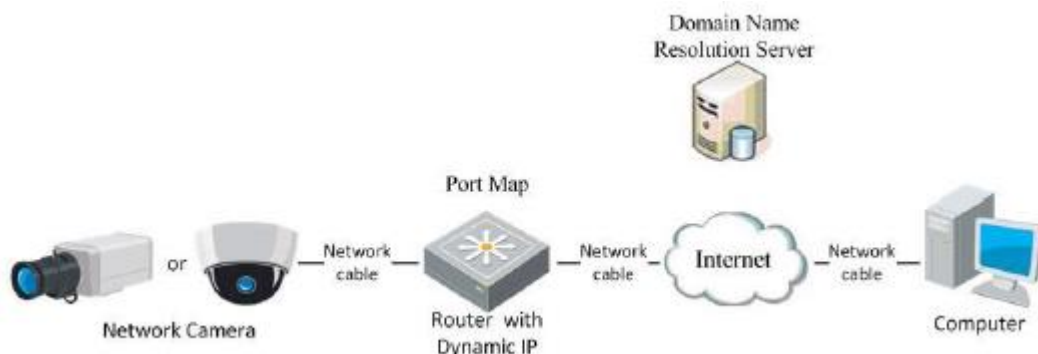
Tato kamera podporuje funkci automatického vytáčení PPPoE. Kamera získá veřejnou IP adresu pomocí vytáčeného připojení ADSL po připojení kamery k modemu. Je třeba nakonfigurovat parametry PPPoE síťové kamery.



Obrázek 2-12 Přístup ke kameře pomocí dynamické IP adresy

Poznámka: Získaná IP adresa je dynamicky přidělována prostřednictvím PPPoE, takže se IP adresa po restartu kamery vždy změní. Chcete-li vyřešit nepříjemnosti spojené s dynamickou IP adresou, musíte získat název domény od poskytovatele DDNS (např. DynDns.com). Pro vyřešení problému postupujte podle níže uvedených kroků pro normální překlad názvu domény a překlad názvu soukromé domény.

- ◆Normální rozlišení doménových jmen

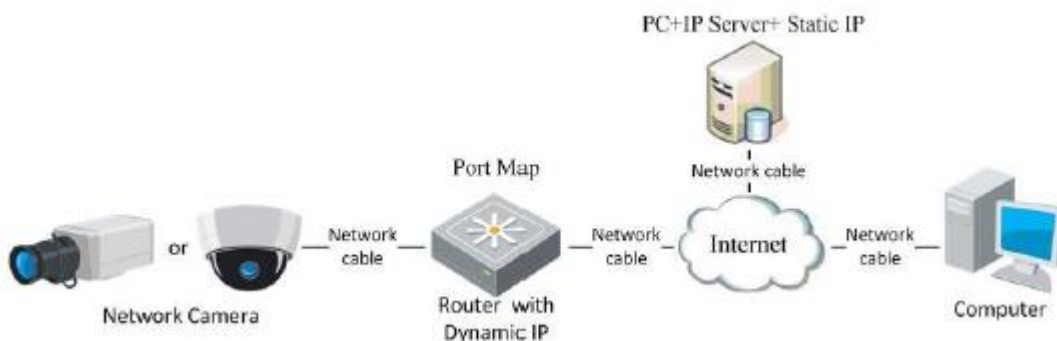


Obrázek 2-13 Normální rozlišení doménových jmen

Kroky:

1. Použijte název domény od poskytovatele doménových jmen.
2. Konfigurace nastavení DDNS v rozhraní DDNS Settings síťové kamery. Podrobnou konfiguraci naleznete v části 7.1.2 Konfigurace nastavení DDNS.
3. Přistupte ke kameře prostřednictvím použitého názvu domény.

◆ Soukromé řešení doménových jmen



Obrázek 2-14 Rozlišení názvů soukromých domén

Kroky:

1. Nainstalujte a spusťte software IP Server v počítači se statickou IP adresou.
2. Přístup k síťové kameře prostřednictvím sítě LAN pomocí webového prohlížeče nebo klientského softwaru.
3. Povolte DDNS a jako typ protokolu vyberte IP server. Viz část 7.1.2 Konfigurace nastavení DDNS pro podrobnou konfiguraci.

Kapitola 3 Přístup k síti kamery

3.1 Přístup pomocí webových prohlížečů

Kroky:

1. Otevřete webový prohlížeč.
2. Do adresního řádku prohlížeče zadejte IP adresu síťové kamery a stisknutím klávesy Enter vstupte do přihlašovacího rozhraní.
3. Poprvé aktivujte síťovou kameru pomocí, viz část 2.1.2. podrobnosti.

Poznámka:

- Výchozí IP adresa je 192.168.1.64.
- Pokud kamera není aktivována, nejprve ji aktivujte podle kapitoly 2.1.2.

4. V pravém horním rohu přihlašovacího rozhraní vyberte jako jazyk rozhraní angličtinu.

5. Zadejte uživatelské jméno a heslo a klikněte na tlačítko Přihlásit.

Uživatel správce by měl správně nakonfigurovat účty zařízení a oprávnění uživatelů/operátorů. Odstraňte nepotřebné účty a uživatelská/operátorská oprávnění.

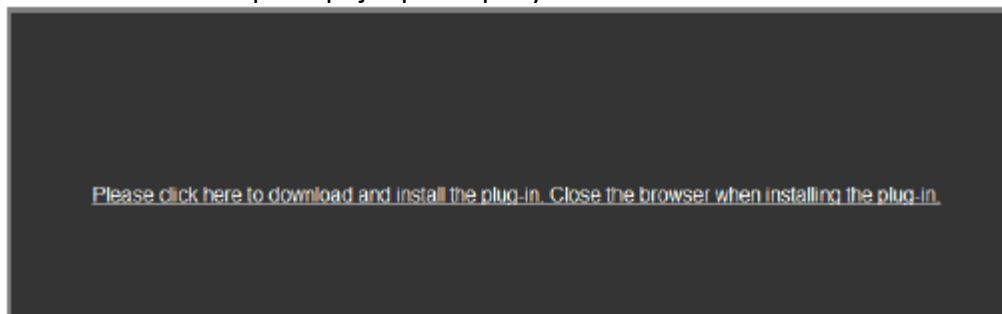
Poznámka:

IP adresa se zablokuje, pokud uživatel administrátor provede 7 neúspěšných pokusů o zadání hesla (5 pokusů pro uživatele/operátora).



Obrázek 3-1 Přihlašovací rozhraní

6. Před sledováním živého videa a obsluhou kamery nainstalujte zásuvný modul. Při instalaci zásuvného modulu postupujte podle pokynů k instalaci.



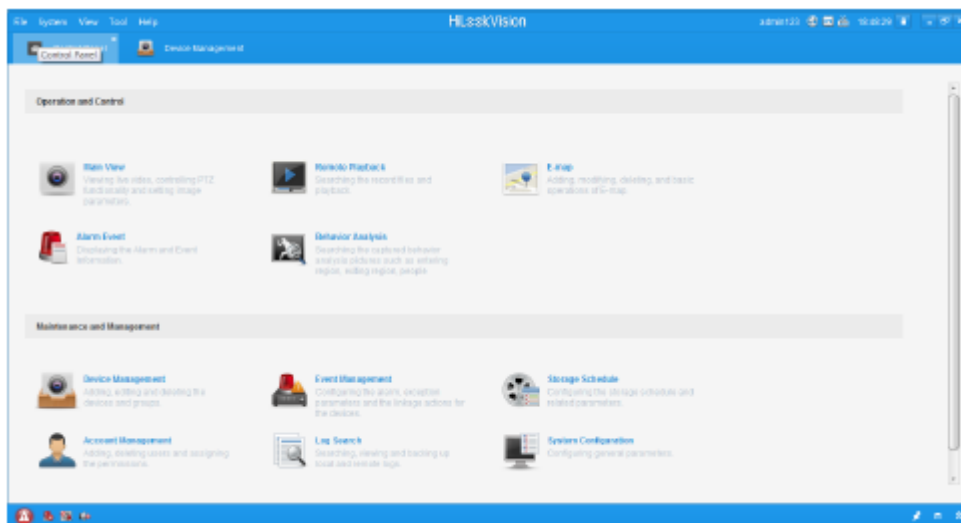
Obrázek 3-2 Stažení a instalace modulu plug-in

Poznámka: Pro instalaci zásuvného modulu může být nutné zavřít webový prohlížeč. Po instalaci zásuvného modulu znovu otevřete webový prohlížeč a znovu se přihlaste.

3.2 Přístup pomocí klientského softwaru

CD s produktem obsahuje klientský software HiLookVision. Pomocí tohoto softwaru můžete sledovat živý obraz a spravovat kameru.

Při instalaci softwaru postupujte podle pokynů k instalaci. Ovládací panel a rozhraní živého náhledu klientského softwaru HiLookVision jsou zobrazeny níže.



Obrázek 3-3 Ovládací panel HiLookVision

Poznámka: Podrobné informace o softwaru naleznete v uživatelské příručce klientského softwaru HiLookVision.

Kapitola 4 Nastavení Wi-Fi

Díky připojení k bezdrátové síti nemusíte pro připojení k síti používat žádný kabel, což je velmi výhodné pro vlastní dohledové aplikace. Poznámka: Tato kapitola platí pouze pro kamery s vestavěným modulem Wi-Fi.

4.1 Konfigurace připojení Wi-Fi v režimech Správa a Ad-hoc

Účel:

Podporovány jsou dva režimy připojení. Vyberte požadovaný režim a proveďte kroky pro konfiguraci Wi-Fi.

Bezdrátové připojení v režimu správy

Kroky:

1. Vstupte do konfiguračního rozhraní Wi-Fi.

Konfigurace > Síť > Rozšířená nastavení > Wi-Fi

2. Kliknutím na tlačítko Hledat vyhledáte bezdrátová připojení online.

FTP Email Platform Access HTTPS QoS **Wi-Fi**

Enable

Wireless List Search

No.	SSID	Working Mode	Security Mode	Channel	Signal Strength	Speed(Mbps)	Connection Status
1	XXXXXXXXXXXXXX	Manage	WPA2-personal	1	92	150	Disconnected
2	SSID	Manage	WPA2-personal	9	88	150	Disconnected
3	XXXXXXXXXXXXXX	Manage	WPA2-personal	6	88	150	Disconnected
4	TP-LINK_cdtest	Manage	WPA2-personal	1	79	150	Disconnected
5	XXXXXXXXXXXXXX	Manage	WPA2-personal	1	75	150	Disconnected
6	@PHICOMM_90	Manage	WPA2-personal	1	72	150	Disconnected
7	XXXXXXXXXXXXXX	Manage	WPA2-personal	1	70	150	Disconnected
8	TP-LINK_57CC	Manage	WPA2-personal	1	67	150	Disconnected
9	doyoulove	Manage	WPA2-personal	1	64	150	Disconnected
10	Manage	WPA2-personal	1	64	150	Disconnected

Obrázek 4-1 Seznam Wi-Fi

3. Kliknutím vyberte bezdrátové připojení v seznamu.

Obrázek 4-2 Nastavení Wi-Fi - režim správy

4. Zaškrtnutím přepínače vyberte režim sítě jako Spravovat a režim zabezpečení sítě se automaticky zobrazí při výběru bezdrátové sítě, neměňte jej ručně.

Poznámka: Tyto parametry jsou zcela shodné s parametry směrovače.

5. Zadejte klíč pro připojení k bezdrátové síti. Klíč by měl odpovídat klíči bezdrátového síťového připojení, který jste nastavili na směrovači.

Bezdrátové připojení v režimu Ad-hoc

Pokud zvolíte režim Ad-hoc, nemusíte bezdrátovou kameru připojovat přes směrovač. Scénář je stejný, jako když propojíte kameru a počítač přímo síťovým kabelem.

Kroky:

1. Vyberte režim Ad-hoc.

Wi-Fi

SSID

Network Mode Manage Ad-Hoc

Security Mode

Encryption Type

Key 1

Obrázek 4-3 Nastavení Wi-Fi - Ad-hoc

2. Přizpůsobení identifikátoru SSID pro kameru.

3. Zvolte režim zabezpečení bezdrátového připojení.

4. Povolte funkci bezdrátového připojení počítače.

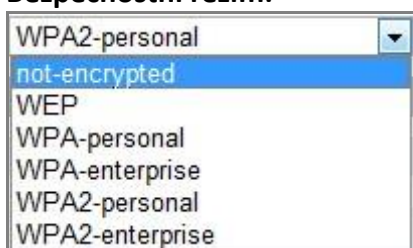
5. Na straně PC vyhledejte síť a uvidíte SSID kamery v seznamu.



Obrázek 4-4 Bod připojení Ad-hoc

6. Vyberte SSID a připojte se.

Bezpečnostní režim:



Obrázek 4-5 Režim zabezpečení

Režim zabezpečení můžete zvolit jako nešifrovaný, WEP, WPA-personal, WPA-enterprise, WPA2-personal a WPA2-enterprise.

Režim WEP:

Security Mode	WEP
Authentication	<input checked="" type="radio"/> Open <input type="radio"/> Shared
Key Length	<input checked="" type="radio"/> 64bit <input type="radio"/> 128bit
Key Type	<input checked="" type="radio"/> HEX <input type="radio"/> ASCII
Key 1	<input type="text"/>
Key 2	<input type="text"/>
Key 3	<input type="text"/>
Key 4	<input type="text"/>

Obrázek 4-6 Režim WEP

- **Ověřování** - v závislosti na metodě používané přístupovým bodem vyberte možnost **Ověřování systémem otevřeného klíče** nebo **Ověřování systémem sdíleného klíče**. Ne všechny přístupové body mají tuto možnost, v takovém případě pravděpodobně používají otevřený systém, který je někdy známý jako **ověřování SSID**.

- **Délka klíče** - Nastavuje délku klíče použitého pro bezdrátové šifrování, 64 nebo 128 bitů. Délka šifrovacího klíče se někdy uvádí jako 40/64 a 104/128.

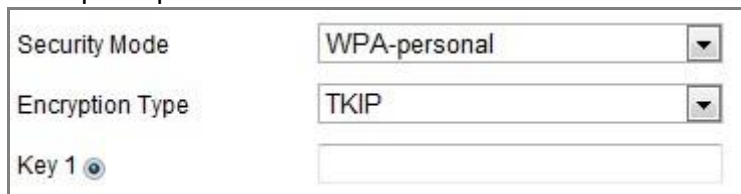
- **Typ klíče** - dostupné typy klíčů závisí na použitém přístupovém bodu. K dispozici jsou následující možnosti:

HEX - Umožňuje ručně zadat hexadecimální klíč.

ASCII - Při této metodě musí mít řetězec přesně 5 znaků pro 64bitový WEP a 13 znaků pro 128bitový WEP.

Osobní režim WPA a osobní režim WPA2:

Zadejte požadovaný předsdílený klíč pro přístupový bod, kterým může být hexadecimální číslo nebo přístupová fráze.



The screenshot shows a configuration window for WPA personal security. It includes a 'Security Mode' dropdown menu set to 'WPA-personal', an 'Encryption Type' dropdown menu set to 'TKIP', and a 'Key 1' text input field with a radio button next to it.

Obrázek 4-7 Režim zabezpečení - WPA - osobní WPA - podnikový a WPA2 - podnikový režim:

Vyberte typ ověřování klient/server, který přístupový bod používá: EAP-TLS nebo EAP-PEAP.

EAP - TLS



The screenshot shows a configuration window for EAP-TLS security. It includes a 'Security Mode' dropdown menu set to 'WPA-enterprise', an 'Authentication' dropdown menu set to 'EAP-TTLS', a 'User Name' text input field, a 'Password' text input field with masked characters, an 'Inner authentication' dropdown menu set to 'PAP', an 'Anonymous identity' text input field, an 'EAPOL version' dropdown menu set to '1', and a 'CA certificate' text input field with 'Browse' and 'Upload' buttons next to it.

Obrázek 4-8 EAP-TLS

- Identita - Zadejte ID uživatele, které chcete předložit síti.
- Heslo soukromého klíče - zadejte heslo pro své ID uživatele.
- Verze EAPOL - Vyberte verzi používanou v přístupovém bodě (1 nebo 2).
- Certifikáty certifikační autority - Nahrajte certifikát certifikační autority, který předložíte přístupovému bodu k ověření.

EAP-PEAP:

- Uživatelské jméno - zadejte uživatelské jméno, které chcete prezentovat v síti.
- Heslo - zadejte heslo sítě
- Verze PEAP - Vyberte verzi PEAP používanou v přístupovém bodě.
- Štítek - vyberte štítek používaný přístupovým bodem.
- Verze EAPOL - Vyberte verzi (1 nebo 2) v závislosti na verzi používané v přístupovém bodě.
- Certifikáty certifikační autority - Nahrajte certifikát certifikační autority, který předložíte přístupovému bodu k ověření.
- V zájmu ochrany vašeho soukromí a lepší ochrany vašeho systému před bezpečnostními riziky.

Pozor: důrazně doporučujeme používat silná hesla pro všechny funkce a síťová zařízení. Heslo by mělo být podle vašeho vlastního výběru (s použitím minimálně 8 znaků, včetně alespoň tří z následujících kategorií: velká písmena, malá písmena, číslice a speciální znaky), aby se zvýšila bezpečnost vašeho produktu.

- Za správnou konfiguraci všech hesel a dalších bezpečnostních nastavení je zodpovědný instalátor a/nebo koncový uživatel.

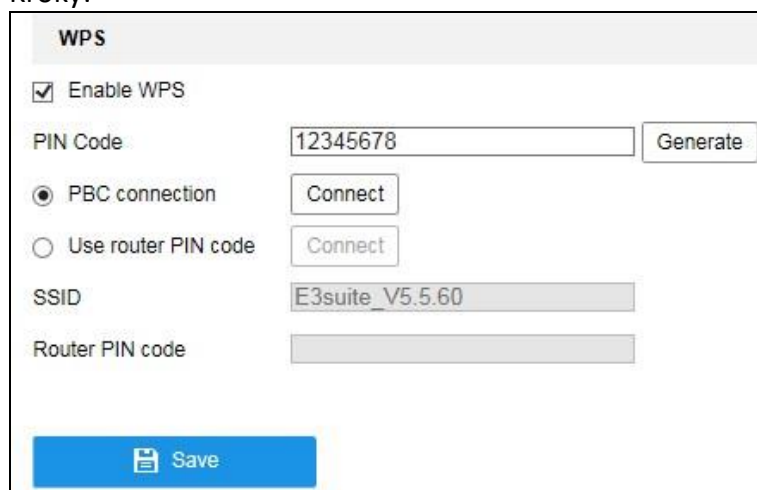
4.2 Snadné připojení Wi-Fi pomocí funkce WPS

Nastavení bezdrátového síťového připojení není nikdy snadné. Chcete-li se vyhnout složitému nastavování bezdrátového připojení, můžete povolit funkci WPS.

WPS (Wi-Fi Protected Setup) znamená snadnou konfiguraci šifrovaného připojení mezi zařízením a bezdrátovým směrovačem. WPS usnadňuje přidávání nových zařízení do stávající sítě bez nutnosti zadávat dlouhé přístupové fráze. Existují dva režimy připojení WPS, režim PBC a režim PIN.

Poznámka: Pokud povolíte funkci WPS, nemusíte konfigurovat parametry, jako je typ šifrování, a nemusíte znát klíč bezdrátového připojení.

Kroky:



Obrázek 4-9 Nastavení Wi-Fi – WPS

Režim PBC:

PBC označuje Push-Button-Configuration, kdy uživatel jednoduše stiskne tlačítko, ať už skutečné, nebo virtuální (jako tlačítko na konfiguračním rozhraní prohlížeče IE), jak na přístupovém bodu (a registrátoru sítě), tak na novém bezdrátovém klientském zařízení.

1. Zaškrtnutím políčka povolte funkci WPS.

2. Zvolte režim připojení jako PBC.

Poznámka: Podpora tohoto režimu je povinná jak pro přístupové body, tak pro připojená zařízení.

3. Zkontrolujte, zda je na routeru Wi-Fi tlačítko WPS. Pokud ano, stiskněte tlačítko a uvidíte, že indikátor v blízkosti tlačítka začne blikat, což znamená, že je funkce WPS směrovače povolena. Podrobné informace o ovládání naleznete v uživatelské příručce směrovače.

4. Stisknutím tlačítka WPS povolte funkci na kameře.

Pokud na kameře není tlačítko WPS, můžete také kliknutím na virtuální tlačítko povolit funkci PBC na webovém rozhraní.

5. Klikněte na tlačítko Připojit.

Pokud je režim PBC povolen ve směrovači i v kameře, dojde k automatickému připojení kamery a bezdrátové sítě.

Režim PIN:

Režim PIN vyžaduje osobní identifikační číslo (PIN), které lze přečíst buď z nálepky, nebo z displeje nového bezdrátového zařízení. Tento kód PIN je pak třeba zadat pro připojení k síti, obvykle k přístupovému bodu sítě.

Kroky:

1. Vyberte bezdrátové připojení v seznamu a SSID se načte automaticky.
2. Vyberte možnost Použití kód PIN trasy.

WPS	
<input checked="" type="checkbox"/> Enable WPS	
PIN Code	12345678 <input type="button" value="Generate"/>
<input type="radio"/> PBC connection	<input type="button" value="Connect"/>
<input checked="" type="radio"/> Use router PIN code	<input type="button" value="Connect"/>
SSID	C-WPA2-Personal
Router PIN code	

Obrázek 4-10 Použití kódu PIN

Pokud je kód PIN generován ze strany směrovače, měli byste do pole PIN kód směrovače zadat kód PIN, který jste získali ze strany směrovače.

3. Klikněte na tlačítko Připojit.

Kód PIN můžete vygenerovat na straně kamery. Doba platnosti kódu PIN je 120 sekund.

1. Klikněte na tlačítko Generovat.

PIN Code	12345678 <input type="button" value="Generate"/>
----------	--

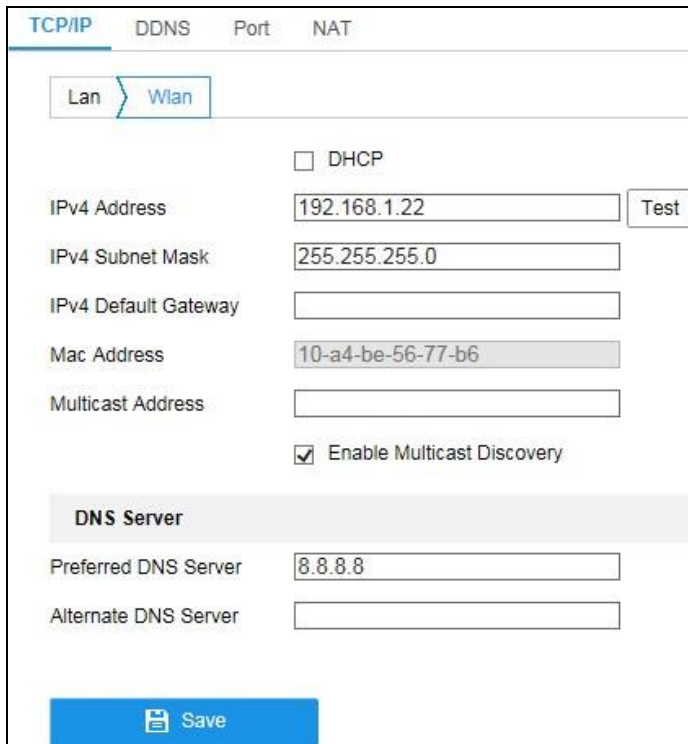
2. Zadejte kód směrovače, v příkladu zadejte 48167581.

4.3 Nastavení vlastností IP pro připojení k bezdrátové síti

Výchozí IP adresa řadiče bezdrátového síťového rozhraní je 192.168.1.64. Po připojení bezdrátové sítě můžete výchozí IP adresu změnit.

Kroky:

1. Vstupte do konfiguračního rozhraní TCP/IP. Konfigurace > Síť > Základní nastavení > TCP/IP
2. Vyberte kartu Wlan.



Obrázek 4-11 Nastavení parametrů sítě WLAN

3. Přizpůsobte adresu IPv4, masku podsítě IPv4 a výchozí bránu. Postup nastavení je stejný jako u sítě LAN.

Pokud chcete, aby vám byla přidělena IP adresa, můžete zaškrtnutím políčka povolit DHCP.

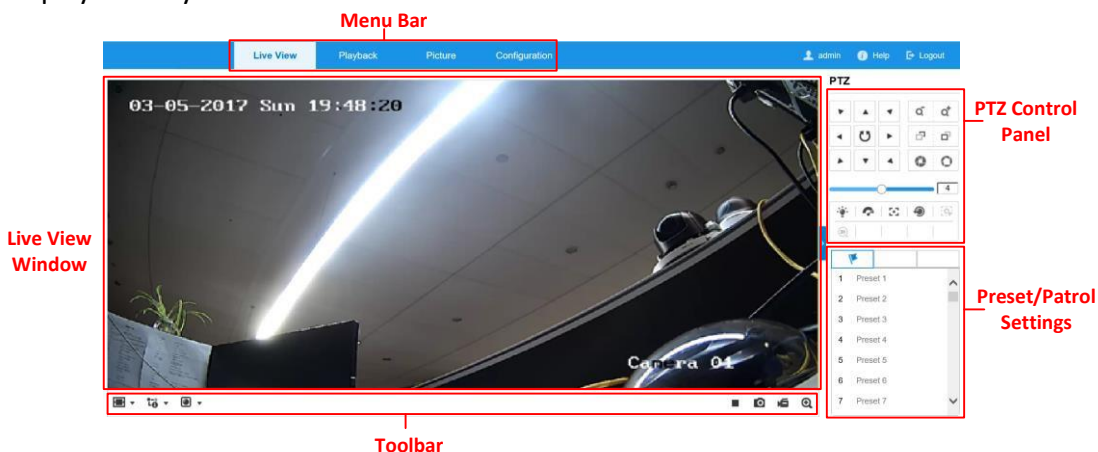
Kapitola 5 Živé zobrazení

5.1 Stránka živého náhledu

Stránka živého náhledu umožňuje prohlížet video v reálném čase, pořizovat snímky, ovládat PTZ, nastavovat/vyvolávat předvolby a konfigurovat parametry videa.

Přihlášením k síťové kameře vstoupíte na stránku živého náhledu nebo můžete kliknout na možnost Živý náhled na obrazovce na liště nabídek hlavní stránky, abyste vstoupili na stránku živého náhledu.

Popisy stránky živého náhledu:



Obrázek 5-1 Stránka živého náhledu

Kliknutím na jednotlivé karty vstoupíte na stránky živého náhledu, přehrávání, obrázku a konfigurace.

Okno živého náhledu:

Zobrazení živého videa.

Panel nástrojů:

Panel nástrojů umožňuje nastavit velikost okna živého zobrazení, typ streamu a zásuvné moduly. Umožňuje také zpracovávat operace na stránce živého náhledu, např. spuštění/zastavení živého náhledu, snímání, nahrávání, zapnutí/vypnutí zvuku, obousměrný zvuk, spuštění/zastavení digitálního zoomu atd.

Uživatelé prohlížeče IE (Internet Explorer) mohou zvolit pluginy jako webové komponenty a quick time. A pro uživatele jiných prohlížečů než IE je možné použít webové komponenty, quick time, VLC nebo MJPEG.

Ovládání PTZ:

Provádějte otáčení, naklápění a přibližování kamery. Ovládejte světlo a stěrač. (K dispozici pouze u kamer podporujících funkci PTZ)

Přednastavená nastavení / nastavení hlídání:

Nastavení/vyvolání/odstranění předvoleb nebo hlídek pro kamery PTZ.

5.2 Spuštění živého náhledu

V okně živého náhledu, jak je znázorněno na obrázku 4-2, klikněte na panel nástrojů a spusťte živý náhled kamery.





Obrázek 5-2 Panel nástrojů živého náhledu Tabulka 5-1 Popisy panelu nástrojů

Poznámka: Ikony se liší podle různých modelů kamer.

Ikona / Popis

- ▶/■ Spuštění/zastavení živého náhledu.
- 4:3 Velikost okna je 4:3.
- 16:9 Velikost okna je 16:9.
- 1x Původní velikost vdovy.
- 🖥️ Samočinná adaptivní velikost okna.
- 📺 Živý náhled s hlavním proudem.
- 📺 Živé zobrazení s dílčím streamem.
- 📺 Živý náhled s třetím streamem.
- 🖥️ Kliknutím vyberte zásuvný modul třetí strany.
- 📷 Ruční pořízení snímku.
- 🎥 Ruční spuštění/zastavení nahrávání.
- 🔊 Zapnutí zvuku a nastavení hlasitosti / ztlumení zvuku.
- 🎤 Zapnutí/vypnutí mikrofonu.
- 🔍 Spuštění/zastavení funkce digitálního zoomu.

5.3 Ruční nahrávání a pořizování snímků

V rozhraní živého náhledu klikněte na  pro zachycení živých snímků nebo klikněte na  pro záznam živého náhledu. Cesty k uložení zachycených snímků a klipů mohou být nastavené na stránce Konfigurace > Místní. Konfigurace vzdáleného plánovaného nahrávání, viz oddíl 11.1

Poznámka: Pořízený snímek se uloží do počítače jako soubor JPEG nebo BMP.

5.4 Ovládání PTZ

V rozhraní živého náhledu můžete pomocí tlačítek PTZ ovládat otáčení/naklápění/zvětšování kamery.

Poznámka: Pro ovládání PTZ musí kamera připojená k síti podporovat funkci PTZ nebo musí být na kameře nainstalována jednotka pro otáčení/naklápění.

5.4.1 Ovládací panel PTZ









Na stránce živého náhledu kliknutím vedle pravé strany okna živého náhledu zobrazíte ovládací panel PTZ a kliknutím jej skryjete.

Kliknutím na směrová tlačítka ovládejte pohyby otáčení/naklápění.
















Obrázek 5-3 Ovládací panel PTZ Klepnutím na tlačítka zoomu/ostření/iris můžete ovládat objektiv.

Poznámky:

- K dispozici je osm směrových šipek ( ,  ,  ,  ) na ovládacím panelu. Kliknutím na šipky realizujete nastavení v relativních polohách.
- U kamer, které podporují pouze pohyb objektivu, jsou směrová tlačítka neplatná.

Tabulka 5-2 Popis ovládacího panelu PTZ

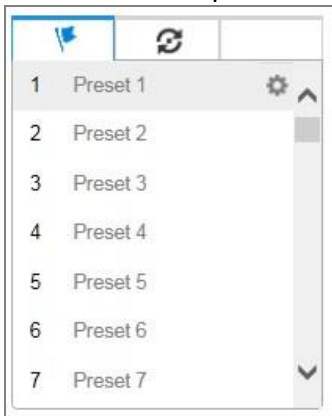
Ikona / Popis

		Zvětšení/zmenšení
		Zaostření na blízko/dálku
		Iris +/-
		Nastavení rychlosti PTZ
	Zapnutí/vypnutí světla	
	Zapnutí/vypnutí stěračů	
	Pomocné zaměření	
	Inicializace objektivu	
	Spuštění ručního sledování	
	Spuštění 3D zoomu	

5.4.2 Nastavení/vyvolání předvolby

●Nastavení předvolby:

1.Na ovládacím panelu PTZ vyberte číslo předvolby ze seznamu předvoleb.



Obrázek 5-4 Nastavení předvolby

2.Pomocí ovládacích tlačítek PTZ přesuňte objektiv do požadované polohy.

- Posuňte kameru doprava nebo doleva.
- Nakloňte kameru nahoru nebo dolů.
- Přiblížení nebo oddálení.
- Přeostřete objektiv.

3.Kliknutím dokončíte nastavení aktuální předvolby.

4.Předvolbu můžete kliknutím odstranit.

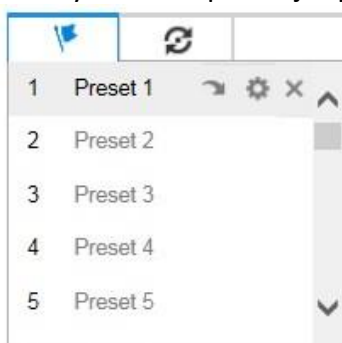
●Vyvolání předvolby:

Tato funkce umožňuje, aby kamera zamířila na zadanou přednastavenou scénu ručně nebo v případě, že dojde k nějaké události.

U definované předvolby můžete kdykoli vyvolat požadovanou přednastavenou scénu.

Na ovládacím panelu PTZ vyberte ze seznamu definovanou předvolbu a klikněte na ni.

Nebo můžete umístit myš na rozhraní předvoleb a vyvolat předvolbu zadáním čísla předvolby, čímž vyvoláte odpovídající předvolbu.



Obrázek 5-5 Vyvolání předvolby

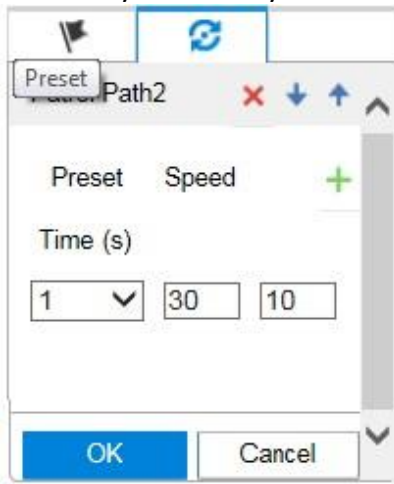
5.4.3 Nastavení/svolání hlídky

Poznámka: Před nastavením hlídky musí být nakonfigurovány nejméně 2 předvolby.

Kroky:

- 1.Kliknutím vstoupíte do konfiguračního rozhraní hlídky.
- 2.Vyberte číslo cesty a kliknutím přidejte nakonfigurované předvolby.
- 3.Vyberte předvolbu a zadejte délku obchůzky a rychlost obchůzky.
- 4.Kliknutím na tlačítko OK uložte první předvolbu.

5. Podle výše uvedených kroků přidejte další předvolby.



Obrázek 5-6 Přidat trasu hlídky

6. Kliknutím na tlačítko OK hlídku uložíte.

7. Kliknutím na tlačítko hlídku spustíte a kliknutím na tlačítko ji zastavíte.

8. (Nepovinné) Kliknutím na tlačítko hlídku odstraníte

Kapitola 6 Konfigurace síťové kamery

6.1 Konfigurace místních parametrů

Účel: Místní konfigurace se týká parametrů živého náhledu, souborů záznamu a pořízených snímků. Záznamové soubory a zachycené obrázky jsou ty, které nahráváte a zachycujete pomocí webového prohlížeče, a proto jsou cesty k jejich uložení na počítači, na kterém běží prohlížeč.

Kroky:

1. Vstupte do rozhraní místní konfigurace: Konfigurace > Místní.

Live View Parameters								
Protocol	<input checked="" type="radio"/>	TCP	<input type="radio"/>	UDP	<input type="radio"/>	MULTICAST	<input type="radio"/>	HTTP
Play Performance	<input type="radio"/>	Shortest Delay	<input checked="" type="radio"/>	Balanced	<input type="radio"/>	Fluent		
Rules	<input type="radio"/>	Enable	<input checked="" type="radio"/>	Disable				
Display POS Information	<input type="radio"/>	Enable	<input checked="" type="radio"/>	Disable				
Image Format	<input checked="" type="radio"/>	JPEG	<input type="radio"/>	BMP				

Record File Settings						
Record File Size	<input type="radio"/>	256M	<input checked="" type="radio"/>	512M	<input type="radio"/>	1G
Save record files to	<input type="text" value="C:\Users\zhubingqing\Web\Reco"/>	<input type="button" value="Browse"/>	<input type="button" value="Open"/>			
Save downloaded files to	<input type="text" value="C:\Users\zhubingqing\Web\Down"/>	<input type="button" value="Browse"/>	<input type="button" value="Open"/>			

Picture and Clip Settings					
Save snapshots in live vi...	<input type="text" value="C:\Users\zhubingqing\Web\Captu"/>	<input type="button" value="Browse"/>	<input type="button" value="Open"/>		
Save snapshots when pla...	<input type="text" value="C:\Users\zhubingqing\Web\Playb"/>	<input type="button" value="Browse"/>	<input type="button" value="Open"/>		
Save clips to	<input type="text" value="C:\Users\zhubingqing\Web\Playb"/>	<input type="button" value="Browse"/>	<input type="button" value="Open"/>		

Obrázek 6-1 Místní konfigurační rozhraní

2. Nakonfigurujte následující nastavení:

- Parametry živého náhledu: Nastavte typ protokolu a výkon živého náhledu.
- ◆ Typ protokolu: Protokoly: TCP, UDP, MULTICAST a HTTP jsou na výběr.

TCP: Zajišťuje kompletní doručení streamovaných dat a lepší kvalitu videa, ale přenos v reálném čase bude ovlivněn.

UDP: Poskytuje audio a video toky v reálném čase.

HTTP: V některých síťových prostředích umožňuje stejnou kvalitu jako protokol TCP bez nastavení konkrétních portů pro streamování.

MULTICAST: Při použití funkce Multicast se doporučuje zvolit typ MCAST. Podrobné informace o funkci Multicast naleznete v části

7.1.1 Konfigurace nastavení TCP/IP.

◆ Přehrát představení: Nastavte výkon přehrávání na možnost Nejkratší zpoždění nebo Automaticky.

◆ Pravidla: Zvolte možnost povolit nebo zakázat zobrazení nebo nezobrazení barevných značek, když se spustí detekce pohybu, detekce obličeje nebo detekce narušení. Např. pokud je povoleno, jak jsou nastavena pravidla, a je povolena i detekce obličeje, bude při detekci obličeje v živém náhledu označen zeleným obdélníkem.

◆ Zobrazení informací o pokladně: Při zapnutí funkce se v živém obraze dynamicky zobrazují informace o vlastnostech detekovaného cíle v jeho blízkosti. Informace o funkci se u různých funkcí liší. Například ID a čekací doba pro řízení fronty, výška pro počítání osob atd.

Poznámka:

Zobrazení informací POS je k dispozici pouze u některých modelů kamer.

◆ Formát obrázku: Zvolte formát snímku pro zachycení obrázku.

● Nastavení souboru záznamu: Nastavte cestu pro ukládání nahraných videosouborů. Platí pro soubory záznamu, které jste nahráli pomocí webového prohlížeče.

◆ Velikost souboru záznamu: Zvolte balenou velikost ručně nahrávaných a stahovaných video souborů na 256M, 512M nebo 1G. Po výběru je maximální velikost souboru záznamu zvolená hodnota.

◆ Uložení souborů se záznamy do: Nastavte cestu pro ukládání ručně nahraných videosouborů.

◆ Stažené soubory uložte do: Nastavte cestu pro uložení stažených video souborů v režimu přehrávání.

● Nastavení obrázků a klipů: Nastavte cesty ukládání pořízených obrázků a vystřižených videosouborů. Platí pro obrázky zachycené pomocí webového prohlížeče.

◆ Ukládání snímků v živém náhledu do: Nastavte cestu ukládání ručně pořízených snímků v režimu živého náhledu.

◆ Uložení snímků při přehrávání do: Nastavte cestu ukládání pořízených snímků v režimu přehrávání.

◆ Uložte klipy do: Nastavte cestu pro ukládání vystřižených videosouborů v režimu přehrávání.

Poznámka: Kliknutím na tlačítko Browse (Procházet) můžete změnit adresář pro ukládání klipů a obrázků a kliknutím na tlačítko Open (Otevřít) otevřete nastavenou složku pro ukládání klipů a obrázků.

3. Nastavení uložíte kliknutím na tlačítko Uložit.

6.2 Konfigurace nastavení systému

Podle níže uvedených pokynů nakonfigurujte nastavení systému, včetně nastavení systému, údržby, zabezpečení a správy uživatelů atd.


6.2.1 Konfigurace základních informací

Vstupte do rozhraní Informace o zařízení: Základní informace: Konfigurace > Systém > Nastavení systému > Základní informace.

V rozhraní Základní informace můžete upravit Název zařízení a Číslo zařízení.

Zobrazí se další informace o síťové kameře, například model, sériové číslo, verze firmwaru, verze kódování, počet kanálů, počet HDD, počet alarmových vstupů, počet alarmových výstupů a vlastnost verze firmwaru. Tyto informace nelze v této nabídce měnit. Jedná se o odkaz pro budoucí údržbu nebo úpravy.

Basic Information	Time Settings	DST	RS-232	About
Device Name	<input type="text" value="IP CAMERA"/>			
Device No.	<input type="text" value="88"/>			
Model	<input type="text" value="XX-XXXXXXXXXX"/>			
Serial No.	<input type="text" value="XX-XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX"/>			
Firmware Version	<input type="text" value="Vx.x.xbuild xxxxxxx"/>			
Encoding Version	<input type="text" value="Vx.xbuild xxxxxxx"/>			
Web Version	<input type="text" value="Vx.x.xbuild xxxxxxx"/>			
Plugin Version	<input type="text" value="Vx.x.x.x"/>			
Number of Channels	<input type="text" value="1"/>			
Number of HDDs	<input type="text" value="0"/>			
Number of Alarm Input	<input type="text" value="0"/>			
Number of Alarm Output	<input type="text" value="0"/>			
Firmware Version Property	<input type="text" value="XX-XX"/>			

 Save

Obrázek 6-2 Základní informace

6.2.2 Konfigurace nastavení času

Podle pokynů v této části můžete nakonfigurovat nastavení synchronizace času a letního času.

Kroky:

1. Vstupte do rozhraní Nastavení času, Konfigurace > Systém > Nastavení systému > Nastavení času.

Basic Information **Time Settings** DST RS-232 About

Time Zone (GMT+08:00) Beijing, Urumqi, Singapore

NTP

NTP

Server Address time.windows.com

NTP Port 123

Interval 1440 minute(s)

Test

Manual Time Sync.

Manual Time Sync.

Device Time 1970-01-07T06:41:17

Set Time 1970-01-07T06:40:31 Sync. with computer time

Save

Obrázek 6-3 Nastavení času

2.V rozevírací nabídce vyberte časové pásmo vaší polohy.

3.Konfigurace nastavení NTP.

(1)Kliknutím povolíte funkci NTP.

(2)Nakonfigurujte následující nastavení:

Adresa serveru: IP adresa serveru NTP.

Port NTP: Port serveru NTP.

Interval: Časový interval mezi dvěma synchronizacemi se serverem NTP.

(3)(Volitelné) Kliknutím na tlačítko Test můžete otestovat funkci synchronizace času prostřednictvím serveru NTP.

NTP

NTP

Server Address time.windows.com

NTP Port 123

Interval 1440 minute(s)

Test

Obrázek 6-4 Synchronizace času pomocí serveru NTP

Poznámka: Pokud je kamera připojena k veřejné síti, měli byste použít server NTP s funkcí synchronizace času, například server Národního časového centra (IP adresa: 210.72.145.44). Pokud je kamera nastavena ve vlastní síti, lze k vytvoření serveru NTP pro synchronizaci času použít software NTP.

Konfigurace ruční synchronizace času.

(1)Zaškrtnutím položky Manual Time Sync. povolíte funkci ruční synchronizace času.

(2)Kliknutím na ikonu vyberte datum a čas z vyskakovacího kalendáře.

(3)(Volitelné) Můžete zaškrtnout položku Synchronizovat s časem počítače, aby se čas zařízení synchronizoval s časem místního počítače.



Obrázek 6-5 Ruční synchronizace času Kliknutím na tlačítko Uložit uložíte nastavení.

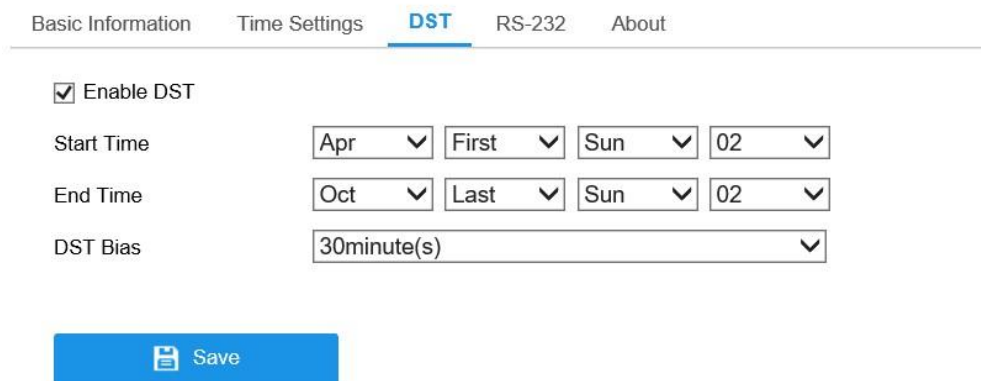
6.2.3 Konfigurace nastavení letního času

Letní čas (DST) je způsob, jak lépe využívat přirozené denní světlo tím, že se v letních měsících posunou hodiny o hodinu dopředu a na podzim zase zpět. Konfigurace DST podle aktuální potřeby.

Kroky:

1. Vstupte do konfiguračního rozhraní DST.

Konfigurace > Systém > Nastavení systému > Letní čas



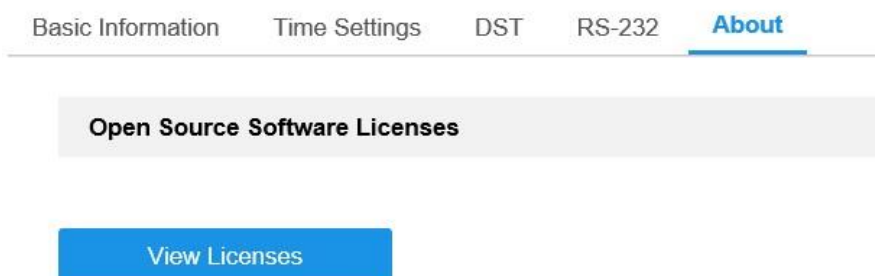
6.2.5 Prohlížení licence

Můžete zobrazit licence k softwaru s otevřeným zdrojovým kódem, které se vztahují na IP kameru.

Kroky:

1. Zadejte informace o rozhraní zařízení: O rozhraní: Konfigurace > Systém > Systémová nastavení > O zařízení.

2. Klikněte na možnost Zobrazit licence.



Obrázek 6-8 O rozhraní

6.3 Údržba

6.3.1 Aktualizace a údržba

Rozhraní pro upgrade a údržbu umožňuje provádět operace, včetně restartu, částečného obnovení, obnovení výchozího nastavení, exportu/importu konfiguračních souborů a upgradu zařízení.

Vstupte do rozhraní údržby:

Konfigurace > Systém > Údržba > Aktualizace a údržba Restart: Restartujte zařízení.

- **Obnovení:** Obnovení výchozího nastavení: Obnovte všechny parametry kromě parametrů IP a uživatelských informací.

- **Výchozí nastavení:** Obnoví všechny parametry na výchozí nastavení z výroby.

Poznámka: Po obnovení výchozího nastavení se také obnoví výchozí IP adresa, buďte proto při této akci opatrní.

- **Export/import konfigurace.** Soubor: Konfigurační soubor slouží k dávkové konfiguraci kamery, což může zjednodušit konfiguraci v případě, že je třeba konfigurovat velké množství kamer.

Kroky:

1. Klikněte na položku Parametry zařízení a zadejte šifrovací heslo, exportujte aktuální konfigurační soubor a uložte jej na určité místo.

2. Kliknutím na tlačítko Procházet vyberte uložený konfigurační soubor a poté kliknutím na tlačítko Importovat spusťte import konfiguračního souboru.

Poznámka: Po importu konfiguračního souboru je třeba kameru restartovat.

- **Upgrade:** Upgrade zařízení na určitou verzi.

Kroky:

1. Vyberte firmware nebo adresář firmwaru pro vyhledání aktualizacího souboru.

Firmware: Vyhledejte přesnou cestu k aktualizacímu souboru.

Adresář firmwaru: Je vyžadován pouze adresář, do kterého patří soubor aktualizace.

2. Kliknutím na tlačítko Procházet vyberte místní aktualizací soubor a poté kliknutím na tlačítko Aktualizovat spusťte vzdálenou aktualizaci.

Poznámka: Proces aktualizace trvá 1 až 10 minut. Během procesu neodpojujte napájení kamery a kamera se po aktualizaci automaticky restartuje.

6.3.2 Protokol

Provoz, alarmy, výjimky a informace o kameře lze ukládat do souborů protokolu. Soubory protokolu můžete na požádání také exportovat.

Než začnete:

Nakonfigurujte pro kameru síťové úložiště nebo do něj vložte kartu SD.

Kroky:

1. Vstupte do rozhraní pro vyhledávání protokolů: Záznamy: Konfigurace > Systém > Údržba > Záznamy.

Major Type: Minor Type:
 Start Time: End Time:

Log List							<input type="button" value="Export"/>
No.	Time	Major Type	Minor Type	Channel No.	Local/Remote User	Remote Host IP	

Obrázek 6-9 Rozhraní pro vyhledávání protokolů

2. Nastavte podmínky vyhledávání v protokolu, abyste specifikovali vyhledávání, včetně hlavního typu, vedlejšího typu, času zahájení a času ukončení.

3. Kliknutím na tlačítko Hledat prohledáte soubory protokolu. Vyhledané soubory protokolů se zobrazí v rozhraní seznamu protokolů.

Start Time: End Time:

Log List							<input type="button" value="Export"/>
No.	Time	Major Type	Minor Type	Channel No.	Local/Remote User	Remote Host IP	
1	2015-05-25 19:12:34	Operation	Remote: Get Working Sta...		admin	10.16.1.107	
2	2015-05-25 19:12:12	Operation	Remote: Get Working Sta...		admin	10.16.1.107	
3	2015-05-25 19:12:12	Operation	Remote: Get Working Sta...		admin	10.16.1.107	
4	2015-05-25 19:12:12	Operation	Remote: Get Working Sta...		admin	10.16.1.107	
5	2015-05-25 19:12:11	Operation	Remote: Get Working Sta...		admin	10.16.1.107	
6	2015-05-25 19:12:11	Operation	Remote: Get Working Sta...		admin	10.16.1.107	
7	2015-05-25 19:12:11	Operation	Remote: Get Working Sta...		admin	10.16.1.107	
8	2015-05-25 19:12:10	Operation	Remote: Get Working Sta...		admin	10.16.1.107	
9	2015-05-25 19:09:28	Operation	Remote: Get Parameters		admin	10.16.1.107	
10	2015-05-25 19:09:25	Operation	Remote: Get Parameters		admin	10.16.1.107	
11	2015-05-25 19:09:25	Operation	Remote: Get Parameters		admin	10.16.1.107	
12	2015-05-25 19:09:24	Operation	Remote: Get Parameters		admin	10.16.1.107	

Total 614 Items << 1/7 >>

Obrázek 6-10 Vyhledávání v protokolu

4. Chcete-li exportovat soubory protokolu, klikněte na tlačítko Exportovat a uložte soubory protokolu.

6.3.3 Systémová služba

Nastavení systémové služby se týká hardwarové služby, kterou kamera podporuje. Podporované funkce se liší podle různých kamer. U kamer podporujících IR LED, ABF (Auto Back Focus), Auto Defog nebo Status LED můžete zvolit povolení nebo zakázání příslušné služby podle aktuálních požadavků.

6.4 Nastavení zabezpečení

Konfigurace parametrů včetně ověřování, filtru IP adres a služby zabezpečení z rozhraní zabezpečení.

6.4.1 Ověřování

Můžete speciálně zabezpečit data živého náhledu.

Kroky:

1. Vstupte do rozhraní Ověřování: Vstupte do rozhraní Authentication: Configuration > System > Security > Authentication.

Authentication IP Address Filter Security Service

RTSP Authentication

WEB Authentication

 Save

Obrázek 6-12 Ověřování

2.Nastavení metody ověřování pro ověřování RTSP a ověřování WEB.

Upozornění:

Doporučenou metodou ověřování pro lepší zabezpečení dat je Digest. Pokud jako metodu ověřování použijete základní, musíte si být vědomi rizika.

3.Nastavení uložíte kliknutím na tlačítko Uložit.

6.4.2 Filtr IP adres

Tato funkce umožňuje kontrolu přístupu.

Kroky:

1.Zadejte rozhraní filtru IP adres: Vstupte do rozhraní Konfigurace > Systém > Zabezpečení > Filtr IP adres.

Authentication IP Address Filter Security Service

Enable IP Address Filter

IP Address Filter Type

IP Address Filter

<input type="checkbox"/>	No.	IP
<input type="checkbox"/>		

Obrázek 6-13 Rozhraní filtru IP adres

2.Zaškrtněte políčko Povolit filtr IP adres.

3.V rozevíracím seznamu vyberte typ filtru IP adres, lze vybrat položky Zakázáno a Povoleno.

4.Nastavení seznamu Filtr IP adres. Přidání IP adresy Kroky:

(1)Klepnutím na tlačítko Přidat přidáte IP adresu.

(2)Zadejte adresu IP.

(3)Kliknutím na tlačítko OK přidání dokončíte.

●Úprava IP adresy Kroky:

(1)Klikněte levým tlačítkem myši na IP adresu ze seznamu filtrů a klikněte na tlačítko Upravit.

(2)Upravte IP adresu v textovém souboru.

Modify IP Address

IP Address

Obrázek 6-15 Úprava IP

(3)Kliknutím na tlačítko OK dokončete úpravy.

●Odstranění IP adresy nebo IP adres.

Vyberte IP adresy a klikněte na tlačítko Odstranit.

5.Nastavení uložíte kliknutím na tlačítko Uložit.

6.4.3 Bezpečnostní služba

Pro umožnění vzdáleného přihlášení a zlepšení zabezpečení datové komunikace poskytuje kamera bezpečnostní službu pro lepší uživatelský komfort.

Kroky:

1.Vstupte do konfiguračního rozhraní služby zabezpečení: Konfigurace > Systém > Zabezpečení > Bezpečnostní služba.



Obrázek 6-16 Bezpečnostní služba

2.Zaškrtněte políčko Povolit zámek nepovoleného přihlášení a IP adresa bude uzamčena, pokud uživatel správce provede 7 neúspěšných pokusů o zadání uživatelského jména/hesla (5krát pro operátora/uživatele).

Poznámka: Pokud je IP adresa uzamčena, můžete se k zařízení zkusit přihlásit po 30 minutách.

6.5 Správa uživatelů

6.5.1 Správa uživatelů

Uživatel správce může přidávat, odstraňovat nebo upravovat uživatelské účty a přidělovat jim různá oprávnění. Důrazně doporučujeme uživatelské účty a oprávnění správně spravovat.

Kroky:

1. Vstupte do rozhraní správy uživatelů: Uživatelská správa: Konfigurace > Systém > Uživatelská správa.

Přidání uživatele

Uživatel admin má ve výchozím nastavení všechna oprávnění a může vytvářet/upravovat/mazat ostatní účty.

Uživatele admin nelze smazat a lze pouze změnit heslo administrátora.

Kroky:

1.Kliknutím na tlačítko Přidat přidáte uživatele.

2.Zadejte uživatelské jméno, vyberte úroveň, zadejte heslo správce a heslo.

Poznámky:

- Lze vytvořit až 31 uživatelských účtů.
- Uživatelé různých úrovní mají různá výchozí oprávnění. Operátor a uživatel jsou volitelní.
- DOPORUČUJEME SILNÉ HESLO - v zájmu zvýšení bezpečnosti vašeho

produktu doporučujeme vytvořit silné heslo podle vlastního výběru (s použitím minimálně 8 znaků, včetně alespoň tří z následujících kategorií: velká písmena, malá písmena, číslice a speciální znaky). A doporučujeme pravidelně obnovovat heslo, zejména v systému s vysokým zabezpečením může obnovení hesla každý měsíc nebo každý týden lépe ochránit váš produkt.

3. Můžete zaškrtnout nebo zrušit zaškrtnutí oprávnění nového uživatele.

4. Kliknutím na tlačítko OK dokončete přidávání uživatelů.

Úprava uživatele

1. Kliknutím vyberte uživatele, kterého chcete odstranit, a klikněte na tlačítko Odstranit.
2. Kliknutím na tlačítko OK ve vyskakovacím dialogovém okně potvrďte odstranění.

6.5.2 Uživatelé online

Prostřednictvím tohoto rozhraní můžete zobrazit aktuální uživatele, kteří navštěvují zařízení. V seznamu uživatelů se zobrazují informace o uživateli, jako je uživatelské jméno, úroveň, IP adresa a doba provozu.

Klikněte na Obnovit - obnovit seznam.

Click **Refresh** to refresh the list.



User Management		Online Users			
User List					Refresh
No.	User Name	Level	IP Address	User Operation Time	
1	admin	Administrator	10.16.5.16	2017-03-18 20:15:40	

Figure 6 -20 View the Online Users

Kapitola 7 Nastavení sítě

Podle pokynů v této kapitole nakonfigurujte základní a pokročilá nastavení.

7.1 Konfigurace základních nastavení

Parametry, včetně TCP/IP, DDNS, PPPoE, portu, NAT atd., můžete konfigurovat podle pokynů v této části.

7.1.1 Konfigurace nastavení TCP/IP

Nastavení TCP/IP musí být správně nakonfigurováno před provozem kamery po síti. Kamera podporuje protokoly IPv4 i IPv6. Obě verze lze konfigurovat současně, aniž by si vzájemně odporovaly, a měla by být nakonfigurována alespoň jedna verze IP.

Kroky:

1. Vstupte do rozhraní TCP/IP Settings: Konfigurace > Síť > Základní Nastavení > TCP/IP

TCP/IP		DDNS	PPPoE	Port	NAT
NIC Type	Auto				
	<input type="checkbox"/> DHCP				
IPv4 Address	10.65.96.42	Test			
IPv4 Subnet Mask	255.255.255.0				
IPv4 Default Gateway	10.65.96.254				
IPv6 Mode	Route Advertisement	View Route Advertisement			
IPv6 Address					
IPv6 Subnet Mask					
IPv6 Default Gateway	::				
Mac Address	94:e1:ac:6b:29:03				
MTU	1500				
Multicast Address					
	<input checked="" type="checkbox"/> Enable Multicast Discovery				
DNS Server					
Preferred DNS Server	8.8.8.8				
Alternate DNS Server					

Obrázek 7-1 Nastavení TCP/IP

2. Nakonfigurujte základní nastavení sítě, včetně typu síťové karty, adresy IPv4 nebo IPv6, masky podsítě IPv4 nebo IPv6, výchozí brány IPv4 nebo IPv6, nastavení MTU a adresy vícesměrového vysílání.

3. (Nepovinné) Zaškrtněte políčko Enable Multicast Discovery (Povolit zjišťování vícesměrového vysílání), a pak může být online síťová kamera automaticky detekována klientským softwarem prostřednictvím soukromého vícesměrového protokolu v síti LAN.

4. Konfigurace serveru DNS. Zadejte preferovaný server DNS a alternativní server DNS.

5. Kliknutím na tlačítko Uložit uložíte výše uvedená nastavení.

Poznámky:

- Platný rozsah hodnot MTU je 1280 až 1500.
- Multicast odesílá stream na adresu skupiny multicast a umožňuje více klientům získat stream současně tím, že si vyžádají kopii z adresy skupiny multicast. Před využitím této funkce je nutné povolit funkci Multicast směrovače.
- Aby se nastavení projevilo, je nutné restartovat počítač.

7.1.2 Konfigurace nastavení DDNS

Pokud je kamera nastavena tak, že jako výchozí síťové připojení používá PPPoE, můžete pro přístup k síti použít dynamický systém DNS (DDNS).

Než začnete:

Před konfigurací nastavení DDNS kamery je nutná registrace na serveru DDNS.


Kroky:

1. Vstupte do rozhraní Nastavení DDNS: Vstupte do rozhraní DDNS: Konfigurace > Síť > Základní nastavení > DDNS.
2. Zaškrtnutím políčka Povolit DDNS tuto funkci povolíte.
3. Vyberte typ DDNS. Je možné vybrat dva typy DDNS: DynDNS a NO-IP.

DynDNS:

Kroky:

- (1) Zadejte adresu serveru DynDNS (např. members.dyndns.org).
- (2) Do textového pole Doména zadejte název domény získaný z webu DynDNS.
- (3) Zadejte uživatelské jméno a heslo registrované na webové stránce DynDNS.
- (4) Klikněte na tlačítko Uložit.

TCP/IP	DDNS	PPPoE	Port	NAT
<input checked="" type="checkbox"/> Enable DDNS				
DDNS Type	DynDNS			
Server Address	members.dyndns.org			
Domain	123.dyndns.com			✓
User Name	test			✓
Port	0			
Password	••••			✓
Confirm	••••			✓
				

Obrázek 7-2 Nastavení služby DynDNS

NO-IP:

- (1) Zvolte typ DDNS jako NO-IP.

TCP/IP **DDNS** PPPoE Port NAT

Enable DDNS

DDNS Type

Server Address ✓


Domain

User Name

Port

Password

Confirm ✓

 Save

Obrázek 7-3 Nastavení DNS protokolu NO-IP

- (2) Zadejte adresu serveru jako `www.noip.com`
- (3) Zadejte název domény, který jste zaregistrovali.
- (4) Zadejte uživatelské jméno a heslo.
- (5) Klikněte na tlačítko Uložit a poté můžete zobrazit kameru s názvem domény.

7.1.3 Konfigurace nastavení PPPoE

Kroky:

1. Vstupte do rozhraní PPPoE Settings: Konfigurace > Síť > Základní nastavení > PPPoE.

TCP/IP DDNS **PPPoE** Port NAT


Enable PPPoE

Dynamic IP

User Name

Password

Confirm

 Save

Obrázek 7-4 Nastavení PPPoE

2. Zaškrtnutím políčka Povolit PPPoE tuto funkci povolíte.
 3. Zadejte Uživatelské jméno, Heslo a Potvrzení hesla pro přístup PPPoE.
- Poznámka: Uživatelské jméno a heslo by měl přidělit váš poskytovatel internetových služeb.

● V zájmu ochrany vašeho soukromí a lepší ochrany systému před bezpečnostními riziky důrazně doporučujeme používat silná hesla pro všechny funkce a síťová zařízení. Heslo by mělo být něco, co si sami zvolíte (s použitím minimálně 8 znaků, včetně alespoň tří z následujících kategorií: velká písmena, malá písmena, číslice a speciální znaky), aby se zvýšila bezpečnost vašeho produktu.

● Za správnou konfiguraci všech hesel a dalších bezpečnostních nastavení je zodpovědný instalátor a/nebo koncový uživatel.

4. Kliknutím na tlačítko Uložit uložte a ukončete rozhraní.

7.1.5 Konfigurace nastavení překladačů síťových adres (NAT)

Rozhraní NAT umožňuje konfigurovat parametry UPnP™.

Universal Plug and Play (UPnP™) je síťová architektura, která zajišťuje kompatibilitu mezi síťovými zařízeními, softwarem a dalšími hardwarovými zařízeními. Protokol UPnP umožňuje bezproblémové připojení zařízení a zjednodušuje implementaci sítí v domácím i firemním prostředí.

Pokud je funkce povolena, není třeba konfigurovat mapování portů pro jednotlivé porty a kamera je připojena k rozsáhlé síti prostřednictvím směrovače.

Kroky:

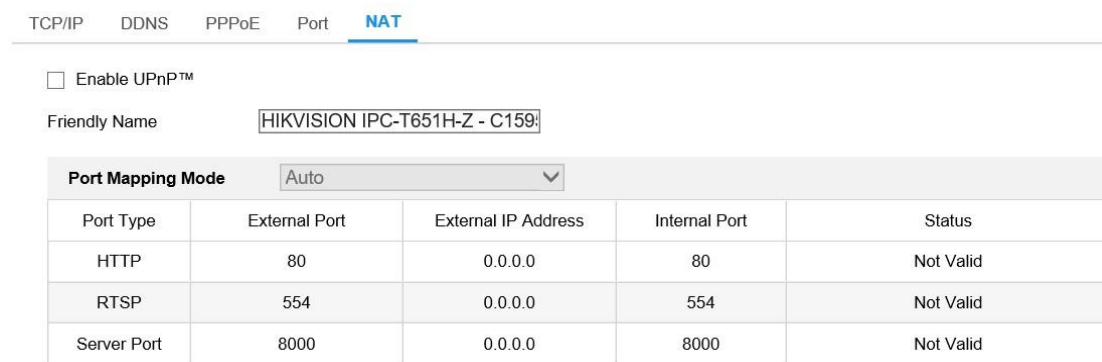
1. Vstupte do rozhraní nastavení NAT. Konfigurace > Síť > Základní nastavení > NAT.

2. Zaškrtnutím políčka povolíte funkci UPnP™.

3. Vyberte přezdívku kamera nebo můžete použít výchozí název.

4. Vyberte režim mapování portů. Lze zvolit manuální a automatický režim. V případě ručního mapování portů můžete hodnotu externího portu přizpůsobit.

5. Nastavení uložíte kliknutím na tlačítko Uložit.



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

Obrázek 7-6 Nastavení UPnP

7.2 Konfigurace pokročilých nastavení

Parametry, včetně SNMP, FTP, e-mailu, HTTPS, QoS, 802.1x atd., můžete konfigurovat podle pokynů v této části.

7.2.1 Konfigurace nastavení SNMP

Můžete nastavit funkci SNMP, abyste získali informace o stavu kamery, parametrech a alarmech a mohli kameru vzdáleně spravovat, když je připojena k síti.

Než začnete:

Před nastavením protokolu SNMP si stáhněte software SNMP a spravujte příjem informací z kamery prostřednictvím portu SNMP. Nastavením adresy Trap může kamera odesílat zprávy o poplachových událostech a výjimkách do dohledového centra.

Poznámka: Vybraná verze protokolu SNMP by měla být stejná jako verze softwaru SNMP. A také musíte použít jinou verzi podle požadované úrovně zabezpečení. SNMP v1 neposkytuje žádné zabezpečení a SNMP v2 vyžaduje pro přístup heslo. A SNMP v3 poskytuje šifrování, a pokud použijete třetí verzi, musí být povolen protokol HTTPS.

- V zájmu ochrany vašeho soukromí a lepší ochrany systému před bezpečnostními riziky důrazně doporučujeme používat silná hesla pro všechny funkce a síťová zařízení. Heslo by mělo být něco, co si sami zvolíte (s použitím minimálně 8 znaků, včetně alespoň tří z následujících kategorií: velká písmena, malá písmena, číslice a speciální znaky), aby se zvýšila bezpečnost vašeho produktu.
- Za správnou konfiguraci všech hesel a dalších bezpečnostních nastavení je zodpovědný instalátor a/nebo koncový uživatel.

Kroky:

1. Vstupte do rozhraní SNMP Settings: SNMP: Konfigurace > Síť > Rozšířená nastavení > SNMP.
2. Překontrolujte nastavení a zatrhněte checkboxy pro Enable SNMPv1, Enable SNMP v2c, Enable SNMPv3

3. Nakonfigurujte nastavení SNMP.

Poznámka: Nastavení softwaru SNMP by měla být stejná jako nastavení, která zde konfigurujete.

4. Klepnutím na tlačítko Uložit uložte a dokončete nastavení.

Poznámky:

- Aby se nastavení projevila, je třeba restartovat počítač.
- Chcete-li snížit riziko úniku informací, doporučujeme povolit SNMP v3 namísto SNMP v1 nebo v2.

7.2.2 Konfigurace nastavení FTP

Informace související se serverem FTP můžete nakonfigurovat tak, aby bylo možné odesílat pořízené snímky na server FTP. Zachycené obrázky mohou být spuštěny událostmi nebo úkolem načasování snímku.

kroky:

1. Vstupte do rozhraní Nastavení FTP: Konfigurace > Síť > Pokročilá nastavení > FTP.

SNMP	FTP	Email	Platform Access	HTTPS	QoS	802.1x	Integration Protocol
Server Address	<input type="text" value="0.0.0.0"/>						
Port	<input type="text" value="21"/>						
User Name	<input type="text"/>	<input type="checkbox"/>	Anonymous				
Password	<input type="password"/>						
Confirm	<input type="password"/>						
Directory Structure	<input type="text" value="Save in the root directory"/>						
Picture Filing Interval	<input type="text" value="7"/>						Day(s)
Picture Name	<input type="text" value="Default"/>						
	<input checked="" type="checkbox"/>						Upload Picture
	<input type="button" value="Test"/>						

Obrázek 7-8

Nastavení FTP

2. Zadejte FTP adresu a port.

3. Nakonfigurujte nastavení FTP; a uživatelské jméno a heslo jsou vyžadovány pro přihlášení k serveru FTP.

- Pro vaše soukromí a lepší ochranu vašeho systému před bezpečnostními riziky důrazně doporučujeme používat silná hesla pro všechny funkce a síťová zařízení. Heslo by mělo být podle vašeho vlastního výběru (s použitím minimálně 8 znaků, včetně alespoň tří z následujících kategorií: velká písmena, malá písmena, čísla a speciální znaky), aby se zvýšila bezpečnost vašeho produktu.

- Za správnou konfiguraci všech hesel a dalších nastavení zabezpečení odpovídá instalační technik a/nebo koncový uživatel.

4. Nastavte strukturu adresářů a interval ukládání obrázků.

Adresář: V poli Struktura adresáře můžete vybrat kořenový adresář, nadřazený adresář a podřízený adresář. Když je vybrán nadřazený adresář, máte možnost použít jako název adresáře Název zařízení, Číslo zařízení nebo IP zařízení; a když je vybrán Podřízený adresář, můžete jako název adresáře použít Název kamery nebo Číslo kamery.

Interval ukládání obrázků: Pro lepší správu obrázků můžete nastavit interval ukládání obrázků od 1 dne do 30 dní. Snímky pořízené ve stejném časovém intervalu budou uloženy do jedné složky pojmenované podle počátečního a koncového data časového intervalu.

Název obrázku: Nastavte pravidlo pro pojmenování souborů zachycených obrázků. Můžeš si vybrat:

Výchozí v rozevíracím seznamu pro použití výchozího pravidla, tj.

IP adresa_ číslo kanálu_ zachycení času_ typ události.jpg

(např. 10.11.37.189_01_20150917094425492_FACE_DETECTION.jpg).

Nebo jej můžete přizpůsobit přidáním vlastní předpony do výchozího pravidla pro pojmenování.

5. Zaškrtnutím políčka Odeslat obrázek funkci povolíte.

Upload Picture (Nahrát obrázek): Chcete-li povolit odeslání zachyceného obrázku na server FTP.

Anonymní přístup k FTP serveru (v takovém případě nebude vyžadováno uživatelské jméno a heslo.): Zaškrtnutím políčka Anonymní povolíte anonymní přístup k FTP serveru.

Poznámka: Funkce anonymního přístupu musí být podporována serverem FTP.

6. Klepnutím na tlačítko Uložit uložíte nastavení.

7.2.3 Konfigurace nastavení e-mailu

Systém lze nakonfigurovat tak, aby odeslal e-mailové upozornění všem určeným příjemcům, pokud je detekována událost alarmu, např. detekce pohybu, ztráta videa, manipulace s videem atd.

Než začneš:

Před použitím funkce E-mail nakonfigurujte nastavení serveru DNS v části Konfigurace > Síť > Základní nastavení > TCP/IP.

kroky:

1. Vstupte do Nastavení TCP/IP (Konfigurace > Síť > Základní nastavení > TCP/IP) pro nastavení adresy IPv4, masky podsítě IPv4, výchozí brány IPv4 a preferovaného serveru DNS.

Poznámka: Podrobné informace naleznete v části 7.1.1 Konfigurace nastavení TCP/IP.

2. Vstupte do rozhraní Nastavení e-mailu: Konfigurace > Síť > Pokročilá nastavení > E-mail.

3. Nakonfigurujte následující nastavení:

Odesílatel: Jméno odesílatele e-mailu.

Sender's Address: E-mailová adresa odesílatele.

Server SMTP: IP adresa nebo název hostitele (např. smtp.263xmail.com) serveru SMTP.
SMTP Port: Port SMTP. Výchozí port TCP/IP pro SMTP je 25 (nezabezpečeno). A port SSL SMTP je 465.

Šifrování e-mailů: Šifrování: Žádné, SSL a TLS je možné zvolit. Když vyberete možnost SSL nebo TLS a zakážete STARTTLS, budou e-maily odesílány po zašifrování pomocí SSL nebo TLS. Port SMTP by měl být pro tuto metodu šifrování nastaven na hodnotu 465. Když vyberete SSL nebo TLS a povolíte STARTTLS, e-maily budou odesílány po zašifrování pomocí STARTTLS a port SMTP by měl být nastaven na 25.

Poznámka: Pokud chcete použít protokol STARTTLS, ujistěte se, že je tento protokol podporován vaším e-mailovým serverem. Pokud zaškrtnete políčko Povolit STARTTLS, i když váš e-mailový server tento protokol nepodporuje, vaše e-maily nebudou šifrovány.

Přiložený obrázek: Pokud chcete odesílat e-maily s přiloženými obrázky budíků, zaškrtněte políčko Přiložený obrázek.

Interval: Interval označuje dobu mezi dvěma akcemi odeslání přiložených obrázků.

Ověřování (volitelné): Pokud váš e-mailový server vyžaduje ověření, zaškrtněte toto políčko, abyste použili ověření pro přihlášení k tomuto serveru a zadali přihlašovací uživatelské jméno a heslo.

- V zájmu ochrany vašeho soukromí a lepší ochrany systému před bezpečnostními riziky důrazně doporučujeme používat silná hesla pro všechny funkce a síťová zařízení. Heslo by mělo být něco, co si sami zvolíte (s použitím minimálně 8 znaků, včetně alespoň tří z následujících kategorií: velká písmena, malá písmena, číslice a speciální znaky), aby se zvýšila bezpečnost vašeho produktu.

- Za správnou konfiguraci všech hesel a dalších bezpečnostních nastavení je zodpovědný instalátor a/nebo koncový uživatel.

Tabulka příjemce: Zvolte příjemce, kterému je e-mail odeslán. Lze nakonfigurovat až 3 příjemce.

Příjemce: Jméno uživatele, který má být upozorněn.

Adresa příjemce: E-mailová adresa uživatele, který má být informován.

4. Nastavení uložíte kliknutím na tlačítko Uložit.

7.2.4 Přístup k platformě

Přístup k platformě vám poskytuje možnost spravovat zařízení prostřednictvím platformy.

kroky:

1. Vstupte do rozhraní konfigurace přístupu k platformě: Konfigurace > Síť > Pokročilá nastavení > Přístup k platformě.

SNMP FTP Email **Platform Access** HTTPS QoS 802.1x Integration Protocol

Platform Access Mode:


Enable


Server IP: Custom

Register Status:

Verification Code:

6 to 12 letters (a to z, A to Z) or numbers (0 to 9), case sensitive. You are recommended to use a combination of no less than 8 letters or numbers.

 Create a verification code.

 Save

Obrázek 7-10 Konfigurace přístupu k platformě

2. Zaškrtnutím políčka Povolit povolíte funkci přístupu k platformě zařízení. Poté se zobrazí vyskakovací okno.
 3. Klikněte a přečtěte si Podmínky služby a Zásady ochrany osobních údajů ve vyskakovacím okně.
 4. Vytvořte ověřovací kód nebo změňte ověřovací kód pro kameru a poté zadejte potvrzený ověřovací kód.
- Poznámka: Při přidávání kamer do aplikace Hik-Connect je vyžadován ověřovací kód.
5. Klepněte na tlačítko OK.
 6. Vyberte Režim přístupu k platformě jako Hik-Connect.
 7. Můžete použít výchozí adresu serveru. Nebo můžete zaškrtnout políčko Vlastní napravo a zadat požadovanou adresu serveru.
 8. Klepnutím na tlačítko Uložit uložíte nastavení.

7.2.5 Nastavení HTTPS

HTTPS poskytuje autentizaci webové stránky a jejího přidruženého webového serveru, který chrání před útoky typu Man-in-the-middle. Chcete-li nastavit číslo portu https, proveďte následující kroky.

Pokud například nastavíte číslo portu na 443 a IP adresa je 192.168.1.64, můžete k zařízení přistupovat zadáním `https://192.168.1.64:443` přes webový prohlížeč.

kroky:

1. Vstupte do rozhraní nastavení HTTPS. Konfigurace > Síť > Pokročilá nastavení > HTTPS.
2. Zaškrtnutím políčka Povolit funkci povolíte.

Enable**Install Certificate**

Installation Method

Create Self-signed Certificate

Signed certificate is available, start the installation directly.

Create the certificate request first and continue the installation.

Create Self-signed Certificate

Obrázek 7-11 Konfigurační rozhraní HTTPS

3. Vytvořte certifikát podepsaný svým držitelem nebo autorizovaný certifikát.

Vytvořte certifikát podepsaný svým držitelem

(1) Jako metodu instalace vyberte Vytvořit certifikát s vlastním podpisem.

(2) Klepnutím na tlačítko Vytvořit vstoupíte do rozhraní pro vytváření.

Create
✕

Public Key Length	<input type="text" value="1024"/>	▼	
Country	<input type="text"/>		*
Hostname/IP	<input type="text"/>		*
Validity	<input type="text"/>		Day(s)*
Password	<input type="text"/>		
State or province	<input type="text"/>		
Locality	<input type="text"/>		
Organization	<input type="text"/>		
Organizational Unit	<input type="text"/>		
Email	<input type="text"/>		

Obrázek 7-12 Create Self-signed Certificate (3)

Zadejte zemi, název hostitele/IP, platnost a další informace.

(4) Klepnutím na OK uložte nastavení.

Poznámka: Pokud jste již měli certifikát nainstalovaný, je možnost Vytvořit certifikát podepsaný svým držitelem zašedlá.

Vytvořte autorizovaný certifikát

(1) Nejprve vyberte Vytvořit žádost o certifikát a pokračujte v instalaci jako způsob instalace.

(2) Klepnutím na tlačítko Vytvořit vytvořte žádost o certifikát. Ve vyskakovacím okně vyplňte požadované informace.

- (3) Stáhněte si žádost o certifikát a odešlete ji k podpisu důvěryhodné certifikační autoritě.
 (4) Po obdržení podepsaného platného certifikátu importujte certifikát do zařízení.
 4. Po úspěšném vytvoření a instalaci certifikátu se zobrazí informace o certifikátu.



Obrázek 7-13 Instalovaný certifikát

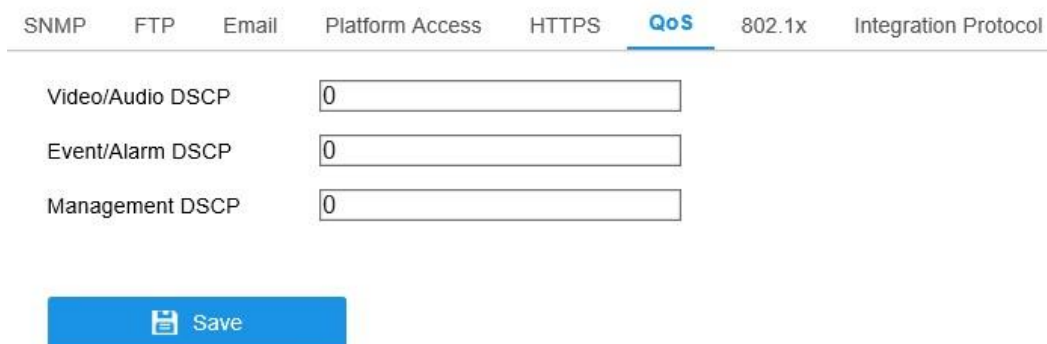
5. Klepnutím na tlačítko Uložit nastavení uložíte.

7.2.6 Konfigurace nastavení QoS

QoS (Quality of Service) může pomoci vyřešit zpoždění a přetížení sítě nastavením priority odesílání dat.

Kroky:

1. Vstupte do rozhraní Nastavení QoS: Konfigurace > Síť > Rozšířená nastavení > QoS.



Obrázek 7-14 Nastavení QoS

2. Nakonfigurujte nastavení QoS, včetně Video/Audio DSCP, Event/Alarm DSCP a Management DSCP.

Platný rozsah hodnot DSCP je 0 až 63. Čím vyšší je hodnota DSCP, tím vyšší je priorita.

7.2.7 Konfigurace nastavení 802.1X

Síťové kamery podporují standard IEEE 802.1X, a když je tato funkce povolena, data kamery jsou zabezpečena a při připojení kamery k síti chráněné standardem IEEE 802.1X je vyžadováno ověření uživatele.

Než začneš:

Ověřovací server musí být nakonfigurován. Použijte a zaregistrujte uživatelské jméno a heslo pro 802.1X na serveru.

Pro vaše soukromí a lepší ochranu vašeho systému před bezpečnostními riziky důrazně doporučujeme používat silná hesla pro všechny funkce a síťová zařízení. Heslo by mělo být podle vašeho vlastního výběru (s použitím minimálně 8 znaků, včetně alespoň tří z následujících kategorií: velká písmena, malá písmena, čísla a speciální znaky), aby se zvýšila bezpečnost vašeho produktu.

Za správnou konfiguraci všech hesel a dalších nastavení zabezpečení odpovídá instalační technik a/nebo koncový uživatel.

kroky:

1. Vstupte do rozhraní Nastavení 802.1X, Konfigurace > Síť > Upřesnit Nastavení > 802.1X

SNMP FTP Email Platform Access HTTPS QoS **802.1x** Integration Protocol

Enable IEEE 802.1X

Protocol

EAPOL version

User Name

Password

Confirm

Save

Obrázek 7-15 Nastavení 802.1X

2. Zaškrtnutím políčka Povolit IEEE 802.1X tuto funkci povolíte.

3. Nakonfigurujete nastavení 802.1X, včetně protokolu, verze EAPOL, uživatelského jména, hesla a potvrzení.

Poznámka: Verze EAPOLu musí být shodná s verzí routeru nebo switche.

4. Zadejte uživatelské jméno a heslo pro přístup k serveru.

5. Klepnutím na tlačítko Uložit dokončete nastavení.

Poznámka: Aby se nastavení projevila, je třeba restartovat počítač.

7.2.8 Integrovaný protokol

Pokud potřebujete ke kameře přistupovat prostřednictvím platformy třetí strany, můžete povolit funkci CGI. A pokud potřebujete k zařízení přistupovat prostřednictvím protokolu ONVIF, můžete v tomto rozhraní nakonfigurovat uživatele ONVIF. Podrobná pravidla konfigurace naleznete ve standardu ONVIF.

● CGI

Zaškrtněte políčko Povolit Hikvision_CGI a poté vyberte ověření z rozevíracího seznamu.

Poznámka: Digest je doporučená metoda ověřování.

●ONVIF

Kroky:

1.Zaškrtnutím políčka Povolit ONVIF funkci povolíte.

2.Přidání uživatelů ONVIF. Povoleno je až 32 uživatelů.

Nastavte uživatelské jméno a heslo a potvrďte heslo. Uživatele můžete nastavit jako uživatele médií, operátora a správce.

Poznámka: Uživatelský účet ONVIF se liší od uživatelského účtu kamery. Uživatelský účet ONVIF musíte nastavit nezávisle.

3.Uložte nastavení.

Poznámka: Uživatelská nastavení ONVIF se při obnovení kamery vymažou.

Kapitola 8 Nastavení videa a zvuku

Podle níže uvedených pokynů nakonfigurujte nastavení videa, nastavení zvuku, ROI a informace o zobrazení v aplikaci Stream.

8.1 Konfigurace nastavení videa

Kroky:

1.Vstupte do rozhraní Nastavení videa, Konfigurace > Video/Audio > Video.

The screenshot shows the 'Video' configuration page in the Stream application. The page has a header with 'Video' and 'ROI' tabs. Below the header is a list of settings:

Stream Type	Main Stream(Normal)	▼
Video Type	Video Stream	▼
Resolution	2560*1920	▼
Bitrate Type	Variable	▼
Video Quality	Medium	▼
Frame Rate	12.5	▼ fps
Max. Bitrate	5530	Kbps
Video Encoding	H.264	▼
H.264+	OFF	▼
Profile	Main Profile	▼
I Frame Interval	50	
Smoothing	<input type="range" value="50"/>	50 [Clear<->Smooth]

At the bottom of the settings list is a blue 'Save' button with a floppy disk icon.

Obrázek 8-1 Nastavení videa

2.Vyberte typ streamu kamery na hlavní stream (normální), vedlejší stream nebo třetí stream.

Poznámka: Hlavní proud je obvykle určen pro nahrávání a živé zobrazení při dobré šířce pásma a vedlejší proud lze použít pro živé zobrazení, pokud je šířka pásma omezená.

3.Pro vybraný typ streamu můžete upravit následující parametry.

Typ videa:

Vyberte typ streamu na video stream nebo video a audio kompozitní stream. Zvukový signál bude zaznamenán pouze v případě, že je nastaven typ videa Video & Audio.

Rozlišení:

Vyberte rozlišení výstupu videa.

Typ datového toku:

Vyberte typ datového toku na konstantní nebo proměnný.

Kvalita videa:

Pokud je vybrán typ datového toku Variabilní, lze zvolit 6 úrovní kvality videa.

Snímková frekvence:

Nastavení snímkové frekvence. Snímková frekvence popisuje frekvenci, s jakou se aktualizuje datový tok videa, a měří se pomocí snímků za sekundu (fps). Vyšší snímková frekvence je výhodná, pokud je ve videoproudu pohyb, protože zachovává kvalitu obrazu po celou dobu.

Max. Datový tok:

Nastavte maximální datový tok od 32 do 16384 Kb/s. Vyšší hodnota odpovídá vyšší kvalitě videa, ale vyžaduje větší šířku pásma.

Poznámka: Maximální hranice hodnoty maximálního datového toku se liší podle různých platforem kamer. U některých kamer je maximální limit 8192 Kb/s nebo 12288 Kb/s.

Kódování videa:

Kamera podporuje více typů kódování videa, například H.264, H.265, MJPEG a MPEG4.

Podporované typy kódování pro různé typy datových toků se mohou lišit. H.265 je nová technologie kódování. Ve srovnání s H.264 snižuje přenosový datový tok při stejném rozlišení, snímkové frekvenci a kvalitě obrazu. Poznámka: Vybrané typy kódování videa se mohou lišit podle různých režimů kamery.

H.264+ a H.265+:

- H.264+: Pokud nastavíte hlavní proud jako typ proudu a H.264 jako kódování videa, uvidíte, že je k dispozici H.264+. H.264+ je vylepšená technologie kódování komprese založená na H.264. Povolením H.264+ mohou uživatelé odhadnout spotřebu pevného disku podle jeho maximálního průměrného datového toku. Ve srovnání s H.264 snižuje H.264+ u většiny scén úložný prostor až o 50 % při stejném maximálním datovém toku.

- H.265+: Pokud nastavíte hlavní proud jako typ proudu a H.265 jako kódování videa, zobrazí se dostupný H.265+. H.265+ je vylepšená technologie kódování komprese založená na H.265. Povolením H.265+ mohou uživatelé odhadnout spotřebu pevného disku podle jeho maximálního průměrného datového toku. V porovnání s H.265+ snižuje H.265+ u většiny scén úložný prostor až o 50 % při stejném maximálním datovém toku.

Pokud chcete zapnout nebo vypnout H.264+/H.265+, je třeba kameru restartovat. Pokud přepnete z H.264+ na H.265+ přímo a naopak, systém restart nevyžaduje.

Poznámky:

- Pokud živé zobrazení nebo přehrávání nefunguje správně kvůli kompatibilitě, aktualizujte přehrávač videa na nejnovější verzi.

- Při zapnutém H.264+/H.265+ jsou parametry, jako je profil, interval I snímků, kvalita videa a SVC, šedé.

- Při zapnuté funkci H.264+/H.265+ nejsou některé funkce podporovány. U těchto funkcí budou příslušná rozhraní skryta.

- H.264+/H.265+ dokáže samočinně upravit rozložení datového toku podle požadavků aktuální scény, aby bylo možné dlouhodobě realizovat nastavený maximální průměrný datový tok. Kamera potřebuje alespoň 24 hodin, aby se přizpůsobila pevné monitorovací scéně.

•**Max. Průměrný datový tok:**

Pokud nastavíte maximální datový tok, zobrazí se v poli Max. maximální průměrný datový tok odpovídající doporučenému maximálnímu datovému toku. Průměrný datový tok. Maximální průměrný datový tok můžete také nastavit ručně v rozsahu od 32 Kb/s do hodnoty nastaveného maximálního datového toku.

•**Profil:**

Pokud jako kódování videa vyberete H.264 nebo H.265, můžete nastavit profil. Vybrané profily se liší podle modelů kamer.

•**I Interval snímků:**

Nastavení intervalu I Frame Interval od 1 do 400.

•**SVC:**

Škálovatelné kódování videa je rozšířením standardů H.264/AVC a H.265. Výběrem možnosti OFF/ON vypnete/zapnete funkci SVC. Vyberte možnost Automaticky a zařízení bude automaticky extrahovat snímky z původního videa, pokud je šířka pásma sítě nedostatečná.

Vyhlazování:

Odkazuje na hladkost proudu. Čím vyšší je hodnota vyhlazení, tím lepší je plynulost toku, i když kvalita videa nemusí být tak uspokojivá. Čím nižší je hodnota vyhlazování, tím kvalitnější bude proud, i když se může zdát, že není plynulý.

4. Nastavení uložíte kliknutím na tlačítko Uložit.

Poznámka:

Parametry videa se liší podle různých modelů kamer. Informace o funkcích kamery naleznete na stránce aktuálního zobrazení.

8.2 Konfigurace nastavení zvuku

Kroky:

1. Vstupte do rozhraní Nastavení zvuku: Nastavení > Video/Audio > Audio.
2. Nakonfigurujte následující nastavení.

Poznámka: Nastavení zvuku se liší podle různých modelů kamer.

Kódování zvuku: Lze vybrat G.722.1, G.711 ulaw, G.711alaw, G.726, MP2L2 a PCM. U MP2L2 lze konfigurovat vzorkovací rychlost a bitovou rychlost audio streamu. U PCM lze nastavit vzorkovací frekvenci.

Audio vstup: MicIn a LineIn jsou volitelné pro připojený mikrofon a snímač.

Vstupní hlasitost: nastavitelná 0-100.

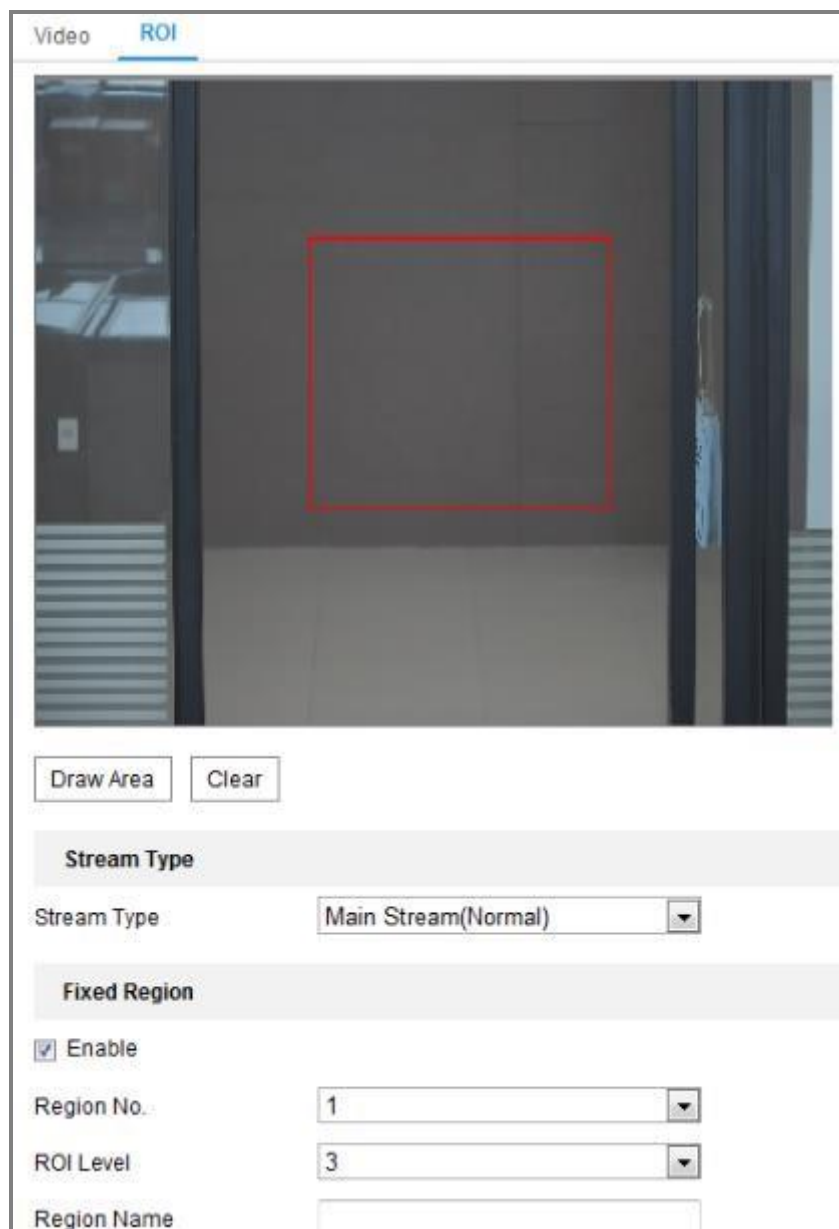
Environmental Noise Filter: Nastavte jej na VYPNUTO nebo ZAPNUTO. Když je funkce povolena, lze do určité míry filtrovat hluk v okolí.

3. Klepnutím na tlačítko Uložit uložíte nastavení.

8.3 Konfigurace kódování ROI

Kódování ROI (Region of Interest) pomáhá rozlišovat ROI a informace na pozadí při kompresi videa, což znamená, že technologie přiřazuje oblasti zájmu více zdrojů kódování, čímž se zvyšuje kvalita ROI, zatímco informace na pozadí jsou méně zaměřené.

Poznámka: Funkce ROI se liší podle různých modelů kamer.



Obrázek 8-3 Kroky nastavení oblasti zájmu:

1. Vstupte do rozhraní nastavení ROI: Configuration > Video/Audio > ROI.
2. Vyberte typ toku pro kódování ROI.
3. Zaškrtněte políčko Povolit v položce Pevná oblast.
4. Nastavte Fixed Region pro ROI.
 - (1) Vyberte Region No. z rozevíracího seznamu.
 - (2) Zaškrtnutím políčka Enable povolte funkci ROI pro vybranou oblast.

(3) Klepněte na tlačítko Kreslení. Kliknutím a přetažením myši na obrazovce zobrazení nakreslete červený obdélník jako oblast ROI. Kliknutím na tlačítko Clear (Vymazat) zrušíte předchozí kreslení. Po dokončení klikněte na tlačítko Zastavit kreslení.

(4) Vyberte úroveň ROI.

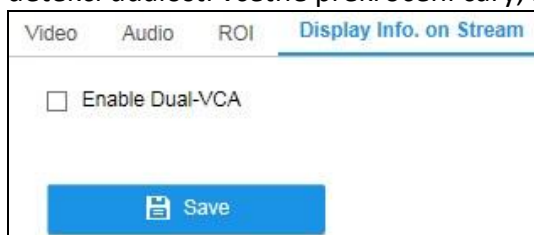
(5) Zadejte název vybrané oblasti.

(6) Kliknutím na tlačítko Uložit uložte nastavení ROI pro vybranou pevnou oblast.

(7) Opakováním kroků (1) až (6) nastavte další pevné oblasti.

8.4 Zobrazení informací na streamu

Zaškrtněte políčko Enable Dual-VCA a informace o objektech (např. člověk, vozidlo atd.) budou označeny ve videoproudu. Poté můžete na připojeném zadním zařízení nastavit pravidla pro detekci událostí včetně překročení čáry, narušení atd.



Obrázek 8-4 Zobrazení informací o streamu

Kapitola 9 Nastavení obrazu

Podle pokynů v této kapitole nakonfigurujte parametry obrazu, včetně nastavení zobrazení, nastavení OSD, masky ochrany soukromí a překrytí obrazu.

9.1 Konfigurace nastavení zobrazení

Nakonfigurujte nastavení obrazu, nastavení expozice, přepínání den/noc, nastavení podsvícení, vyvážení bílé, vylepšení obrazu, nastavení videa a další parametry v nastavení zobrazení.

Poznámka: Tuto funkci podporují pouze některé modely kamer. Parametry zobrazení se liší podle různých modelů kamer. Podrobnosti najdete ve skutečném rozhraní.

9.1.1 Automatické přepínání den/noc

kroky:

1. Vstupte do rozhraní Nastavení zobrazení, Konfigurace > Obrázek > Nastavení zobrazení.



Obrázek 9-1 Nastavení zobrazení automatického přepínání den/noc

2. Vyberte montážní scénář pro kameru. Normální a Silniční jsou volitelné pro scénář montáže. Každý scénář montáže má sadu parametrů obrazu. Výběr vhodného scénáře může pomoci upravit obraz pohodlněji.

3. Nastavte parametry obrazu kamery.

Poznámka: Aby byla zaručena kvalita obrazu při různém osvětlení, poskytuje uživatelům ke konfiguraci dvě sady parametrů.

Úprava obrazu

Jas popisuje jas obrazu, který se pohybuje od 1 do 100.

Kontrast popisuje kontrast obrazu, který se pohybuje od 1 do 100. Sytost popisuje barevnost barvy obrazu, která se pohybuje od 1 do 100.

Ostrost popisuje okrajový kontrast obrazu, který se pohybuje od 1 do 100.

Nastavení expozice

Pokud je kamera vybavena pevným objektivem, lze vybrat pouze manuální a režim clony nelze konfigurovat.

Pokud je vybrána možnost Auto, můžete nastavit úroveň automatické clony od 0 do 100.

Doba expozice se vztahuje k času elektronické závěrky, který se pohybuje od 1 do 1/100 000 s.

Upravte jej podle aktuálních podmínek jasu.

Zesílení obrazu lze také ručně konfigurovat od 0 do 100. Čím větší hodnota, tím jasnější bude obraz a ve větší míře bude zesílen i šum.

Přepínání den/noc

Vyberte režim přepínání den/noc podle různých požadavků na sledování. Den, Noc, Auto, Plánované přepínání a Spouštění alarmovým vstupem jsou volitelné pro přepínání den/noc.

Den: Kamera zůstane v denním režimu.

Noc: Kamera zůstane v nočním režimu.

Auto: Kamera se automaticky přepíná mezi denním a nočním režimem podle osvětlení. Citlivost se pohybuje od 0 do 7, čím vyšší je hodnota, tím snazší je přepínání režimu. Doba filtrování se vztahuje k časovému intervalu mezi přepnutím den/noc. Můžete ji nastavit od 5s do 120s.

Scheduled-Switch: Nastavte čas začátku a čas konce a definujte dobu trvání denního/nočního režimu.

Spouštěno poplachovým vstupem: Spínač se spouští poplachovým vstupem. Spouštěný režim můžete nastavit na den nebo noc.

Spouštěno videem: Kamera přepíná mezi denním a nočním režimem analýzou výkonu obrazu.

Inteligentní doplňkové světlo: Nastavte doplňkové světlo na ZAPNUTO a pro režim osvětlení lze vybrat Auto a Manual.

Vyberte Auto a doplňkové světlo se změní podle skutečného jasu. Pokud je například aktuální scéna dostatečně jasná, doplňkové světlo se samo upraví na nižší výkon; a pokud scéna není dostatečně jasná, světlo se samo upraví na vyšší výkon.

Vyberte možnost Manual a můžete upravit doplněk úpravou vzdálenosti. Pokud je například objekt blízko kamery, zařízení nastaví doplňkové světlo na nižší výkon a světlo má vyšší výkon, pokud je objekt daleko.

Nastavení podsvícení

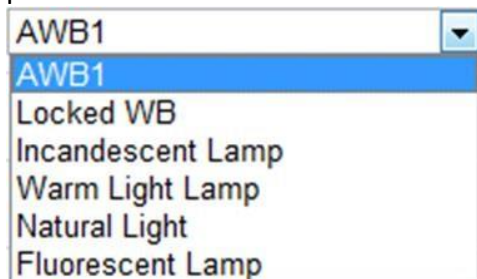
Oblast BLC: Pokud zaostříte na objekt proti silnému protisvětlu, objekt bude příliš tmavý na to, aby byl jasně vidět. BLC kompenzuje světlo do objektu vpředu, aby bylo jasné. Lze vybrat OFF, Up, Down, Left, Right, Center, Auto a Custom.

Poznámka: Pokud je režim BLC nastaven jako Vlastní, můžete na obraz živého náhledu nakreslit červený obdélník jako oblast BLC. **WDR:** Široký dynamický rozsah lze použít v případě, že je na scéně vysoký kontrast světlé a tmavé oblasti.

HLC: Funkci High Light Compression lze použít v případě, že se ve scéně vyskytuje silné světlo, které ovlivňuje kvalitu obrazu.

●Vyvážení bílé

Vyvážení bílé je funkce podání bílé barvy kamery, která slouží k nastavení teploty barev podle prostředí.



Obrázek 9-4 Vyvážení bílé

●Vylepšení obrazu

Digitální redukce šumu: DNR snižuje šum ve videoproudu. Lze vybrat možnosti OFF, Normal a Expert. V režimu Normal nastavte úroveň DNR od 0 do 100. V režimu Expert nastavte úroveň DNR jak z úrovně prostorové DNR [0-100], tak z úrovně časové DNR [0-100].

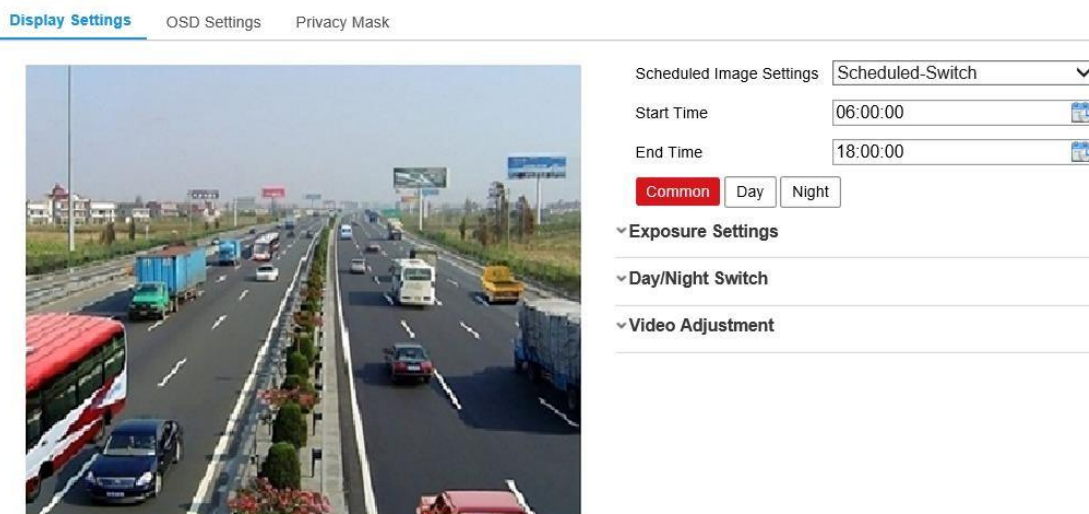
Režim odmlžování: V případě, že je prostředí zamížené a obraz je mlhavý, můžete zapnout funkci odmlžování. Vylepšuje jemné detaily, takže obraz vypadá jasněji.

EIS (elektrický stabilizátor obrazu): EIS snižuje účinky vibrací ve videu.

Šedá škála: Můžete zvolit rozsah stupnice šedi [0-255] nebo [16-235].

9.1.2 Plánované přepínání den/noc

Konfigurační rozhraní pro plánované přepínání den/noc umožňuje nastavit parametry kamery pro den a noc odděleně, čímž je zaručena kvalita obrazu při různém osvětlení.



Obrázek 9-5 Kroky konfigurace rozhraní pro plánované přepínání den/noc:

1. Klepnutím na ikonu kalendáře vyberte čas zahájení a čas ukončení přepnutí.

Poznámky:

- Čas začátku a čas konce se vztahují k platnému času pro denní režim.
- Časové období může začínat a končit dva dny po sobě. Pokud například nastavíte čas začátku na 10:00 a čas konce na 1:00, denní režim se aktivuje v 10 hodin ráno a zastaví se v 1 hodinu časně následujícího rána.

2. Klepnutím na kartu Společné nakonfigurujte společné parametry platné pro denní a noční režim.

Poznámka: Podrobné informace o každém parametru naleznete v části 0 Automatické přepínání den/noc.

3. Klepnutím na kartu Den nakonfigurujte parametry použitelné pro denní režim.
4. Klepnutím na záložku Noc nakonfigurujte parametry použitelné pro noční režim.

Poznámka: Při změně jakéhokoli parametru se nastavení automaticky uloží.

9.2 Konfigurace nastavení OSD

Můžete si přizpůsobit název kamery, formát času/data, režim zobrazení a velikost OSD zobrazené v živém náhledu.

kroky:

1. Vstupte do rozhraní Nastavení OSD: Konfigurace > Obrázek > Nastavení OSD.
2. Zaškrtnutím příslušného políčka vyberte zobrazení názvu kamery, data nebo týdne, pokud je to nutné.
3. Upravte název kamery v textovém poli Název kamery.
4. Vyberte z rozevíracího seznamu a nastavte formát času a formátu data.
5. Nakonfigurujte nastavení překrývání textu.
 - (1) Chcete-li povolit zobrazení na obrazovce, zaškrtněte políčko před textovým polem.
 - (2) Zadejte znaky do textového pole.

Poznámka: Lze konfigurovat až 8 překrývných textů.

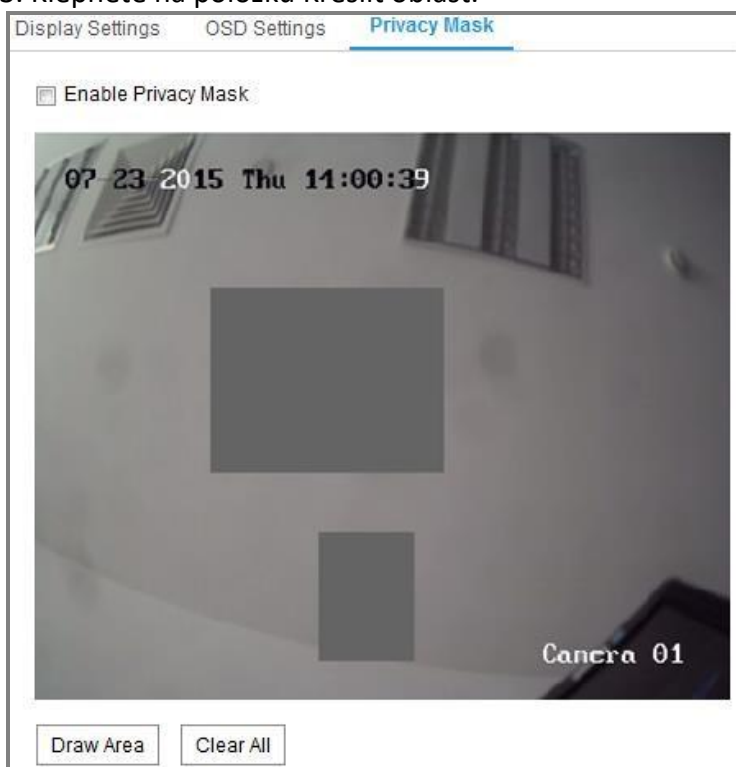
6. Vyberte z rozevíracího seznamu a nastavte režim zobrazení, velikost OSD a barvu písma.
7. Upravte polohu a zarovnání textových rámečků.
Lze vybrat Zarovnat doleva, Zarovnat doprava a Vlastní. Pokud vyberete vlastní, můžete pomocí myši klikat a přetahovat textové rámečky v okně živého náhledu a upravit jejich polohu.
Poznámka: Úprava zarovnání je použitelná pouze pro položky Text Overlay.
8. Klepnutím na tlačítko Uložit uložíte nastavení.

9.3 Konfigurace masky soukromí

Soukromá maska vám umožňuje pokrýt určité oblasti živého videa, abyste zabránili živému sledování a nahrávání určitých míst v oblasti sledování.

kroky:

1. Vstupte do rozhraní Nastavení masky soukromí: Konfigurace > Obrázek > Maska soukromí.
2. Chcete-li tuto funkci aktivovat, zaškrtněte políčko Enable Privacy Mask.
3. Klepněte na položku Kreslit oblast.



Obrázek 9-7 Nastavení privátní masky

4. Klepnutím a tažením myši v okně živého videa nakreslete oblast masky.
Poznámka: Na jeden obrázek můžete nakreslit až 4 oblasti.
5. Klepnutím na Zastavit kreslení dokončíte kreslení nebo klepnutím na Vymazat vše vymažete všechny oblasti, které jste nastavili, aniž byste je uložili.
6. Klepnutím na tlačítko Uložit uložíte nastavení.

Kapitola 10 Nastavení událostí

Tato část vysvětluje, jak nakonfigurovat síťovou kameru tak, aby reagovala na události alarmu, včetně základní události a inteligentní události.

10.1 Základní události

Podle pokynů v této části můžete nakonfigurovat základní události, včetně detekce pohybu, narušení videa, vstupu alarmu, výstupu alarmu a výjimky atd. Tyto události mohou spouštět metody propojení, jako je Upozornit dohledové centrum, Odeslat e-mail, Spustit alarmový výstup atd.

Poznámka: Zaškrtněte políčko Notify Surveillance Center, pokud chcete, aby se informace o alarmu odeslaly do PC nebo mobilního klientského softwaru, jakmile je alarm spuštěn.

10.1.1 Konfigurace detekce pohybu

Detekce pohybu detekuje pohybující se objekty v nakonfigurované sledované oblasti a po spuštění alarmu lze provést řadu akcí.

Aby bylo možné přesně detekovat pohybující se objekty a snížit míru falešných poplachů, lze pro různá prostředí detekce pohybu zvolit normální konfiguraci a expertní konfiguraci.

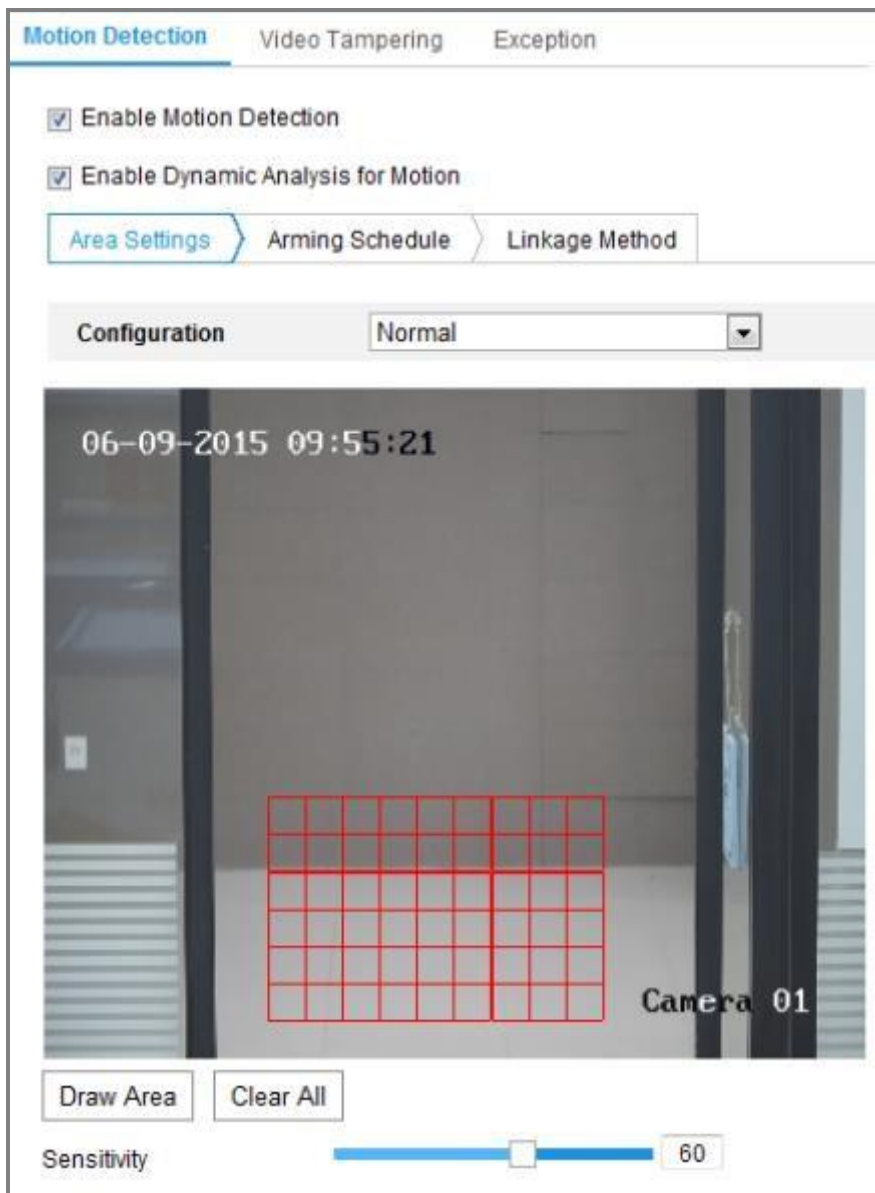
Normální konfigurace

Normální konfigurace používá stejnou sadu parametrů detekce pohybu ve dne i v noci.

Úkol 1: Nastavení oblasti detekce pohybu Kroky:

1. Vstupte do rozhraní pro nastavení detekce pohybu: Detektor pohybu: Konfigurace > Událost > Základní událost > Detekce pohybu.
2. Zaškrtněte políčko Povolit detekci pohybu.
3. Chcete-li detekované objekty označit zelenými obdélníky, zaškrtněte políčko Povolit dynamickou analýzu pohybu.

Poznámka: Pokud nechcete, aby se detekovaný objekt zobrazoval se zelenými obdélníky, vyberte možnost Zakázat pro pravidla. Vyberte zakázání pravidel z Konfigurace > Místní konfigurace > Parametry živého zobrazení-pravidla.



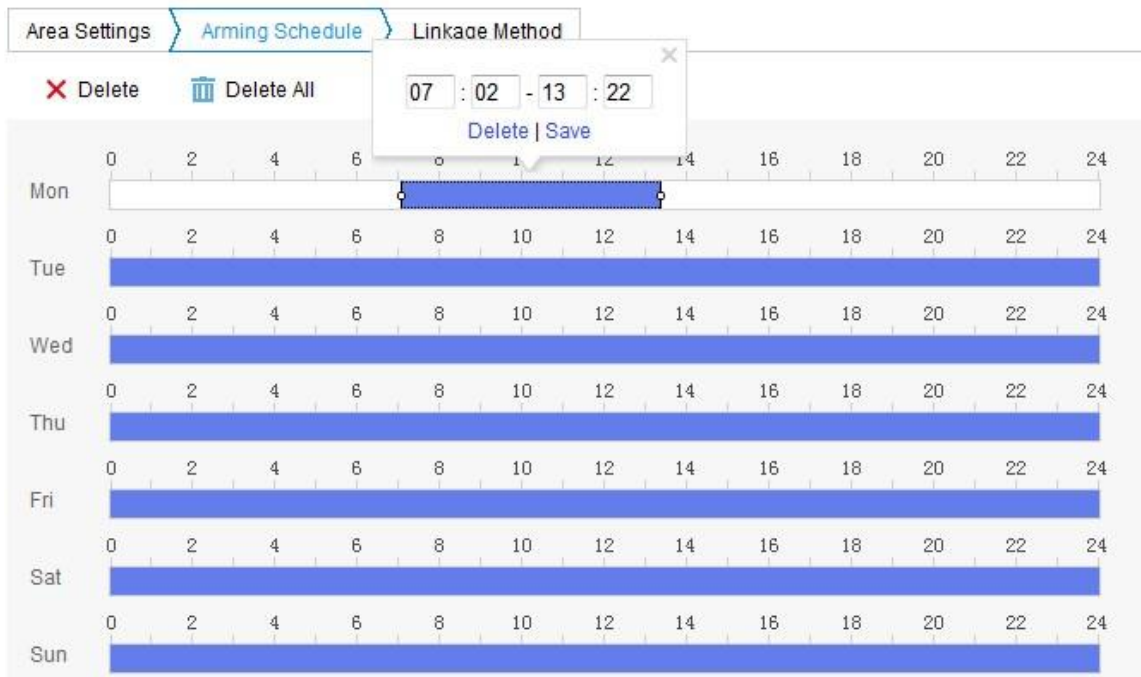
Obrázek 10-1 Povolit detekci pohybu

4. Klepněte na položku Kreslit oblast. Kliknutím a tažením myši na živém videu nakreslíte oblast detekce pohybu. Klepnutím na Zastavit kreslení dokončíte kreslení jedné oblasti.
5. (Volitelně) Klepnutím na Vymazat vše vymažete všechny oblasti.
6. (Volitelně) Posunutím posuvníku nastavte citlivost detekce.

Úkol 2: Nastavte plán aktivace pro detekci pohybu

kroky:

1. Klikněte na Plán zapnutí pro úpravu plánu zapnutí.
2. Klikněte na časovou lištu a tažením myši vyberte časové období.



Obrázek 10-3

Poznámka: Klikněte na vybraný časový úsek, časový úsek můžete upravit na požadovaný čas buď posunutím časové lišty, nebo zadáním přesného časového úseku.

3.(Volitelné) Kliknutím na tlačítko Odstranit smažete aktuální plán strážní služby nebo kliknutím na tlačítko Uložit uložíte nastavení.

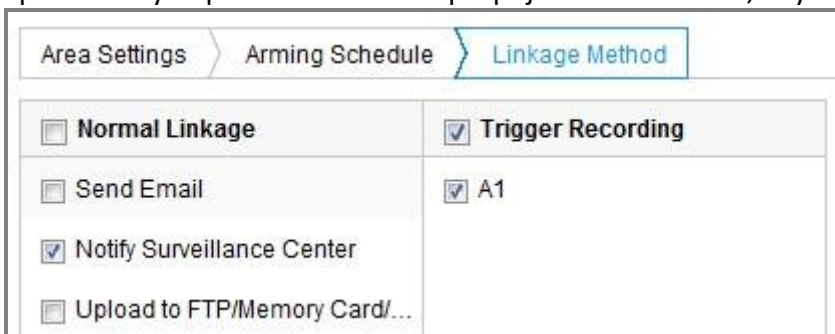
4.Když najedete myší na konec každého dne, zobrazí se dialogové okno pro kopírování a aktuální nastavení můžete zkopírovat do dalších dnů.

5.Nastavení uložíte kliknutím na tlačítko Uložit.

Poznámka: Čas jednotlivých období se nesmí překrývat. Pro každý den lze nakonfigurovat až 8 období.

Úkol 3: Nastavení metody propojení pro detekci pohybu

Zaškrtnutím políčka vyberte metodu propojení. Lze zvolit možnost Zvukové varování, Odeslat e-mail, Upozornit dohledové centrum, Nahrát na FTP/paměťovou kartu/NAS, Spouštěcí kanál a Spouštěcí výstup alarmu. Metodu propojení můžete určit, když dojde k události.



Obrázek 10-4 Metoda propojení

Poznámka: Způsoby propojení se liší podle různých modelů kamer.

●Zvukové varování

Spusťte zvukovou výstrahu na místě. Podporuje to pouze zařízení, které má zvukový výstup.

●Upozornit dozorové středisko

Odeslání signálu výjimky nebo alarmu do softwaru pro vzdálenou správu, když dojde k události.

●Odeslat e-mail

Odeslání e-mailu s informacemi o alarmu uživateli nebo uživatelům, když dojde k události.

Poznámka: Chcete-li odeslat e-mail při výskytu události, přečtěte si část 7.2.3 a předem dokončete nastavení e-mailu.

- Nahrávání na FTP/paměťovou kartu/NAS

Po spuštění alarmu zachytí obrázky a nahraje je na server FTP.

Poznámky:

- Nejprve nastavte adresu FTP a vzdálený server FTP. Podrobné informace naleznete v části 7.2.2 Konfigurace nastavení FTP.

- Přejděte na stránku Konfigurace > Úložiště > Nastavení plánu> Snímání > Parametry snímání, povolte snímání spouštěné událostí a nastavte interval snímání a počet snímání.

- Pořízený snímek lze také nahrát na dostupnou kartu SD nebo síťový disk.

- Spouštěcí kanál

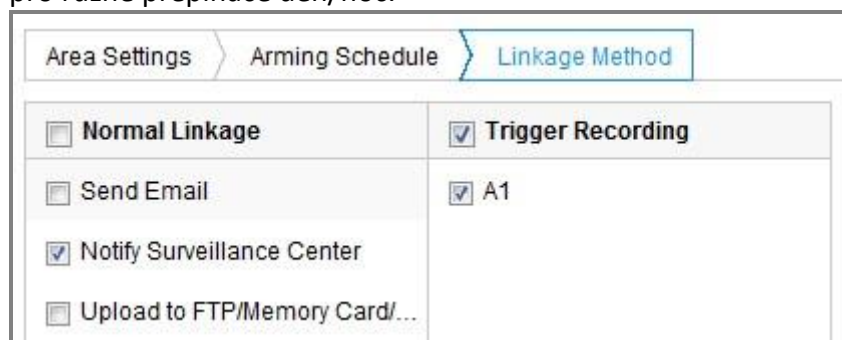
Video se nahraje, jakmile je detekován pohyb. Pro realizaci této funkce je třeba nastavit plán nahrávání. Podrobné informace naleznete v části 11.1.

- Výstup spouštěcího alarmu

Spuštění jednoho nebo více externích alarmových výstupů při výskytu události.

Expertní konfigurace

Expertní režim slouží především k nastavení citlivosti a podílu objektů na jednotlivých plochách pro různé přepínače den/noc.



Obrázek 10-5 Expertní režim detekce pohybu

Přepínač den/noc OFF

Kroky:

- 1.Nakreslete oblast detekce jako v běžném režimu konfigurace. Podporováno je až 8 oblastí.
- 2.Pro možnost Plánovaná nastavení obrázků vyberte možnost VYPNUTO.
- 3.Oblast vyberte kliknutím na oblast č.
- 4.Posunutím kurzoru nastavte citlivost a podíl objektu na ploše pro vybranou oblast.
- 5.Nastavte plán strážní služby a způsob propojení jako v běžném režimu konfigurace.
- 6.Nastavení uložíte kliknutím na tlačítko Uložit.

Kroky automatického přepínání den/noc:

- 1.Nakreslete oblast detekce jako v běžném režimu konfigurace. Podporováno je až 8 oblastí.
- 2.Vyberte možnost Automatické přepínání pro naplánované nastavení obrázků.
- 3.Oblast vyberte kliknutím na oblast č.
- 4.Posunutím kurzoru nastavte citlivost a podíl objektu na ploše pro vybranou oblast ve dne.
- 5.Posunutím kurzoru nastavte citlivost a podíl objektu na ploše pro vybranou oblast v noci.
- 6.Nastavte plán strážní služby a způsob propojení jako v běžném režimu konfigurace.
- 7.Nastavení uložíte kliknutím na tlačítko Uložit.

Kroky plánovaného přepínání den/noc:

- 1.Nakreslete oblast detekce jako v běžném režimu konfigurace. Podporováno je až 8 oblastí.
- 2.Vyberte možnost Plánované - přepínač pro plánované nastavení obrázků.

Scheduled Image Settings	Scheduled-Switch	▼
Start Time	06:00:00	
End Time	18:00:00	

Obrázek 10-6 Plánovaný přepínač den/noc

3. Zvolte čas začátku a čas konce časování spínače.
4. Oblast vyberte kliknutím na oblast č.
5. Posunutím kurzoru nastavte citlivost a podíl objektu na ploše pro vybranou oblast ve dne.
6. Posunutím kurzoru nastavte citlivost a podíl objektu na ploše pro vybranou oblast v noci.
7. Nastavte plán strážní služby a způsob propojení jako v běžném režimu konfigurace.
8. Nastavení uložte kliknutím na tlačítko Uložit.

23

10.1.2 Konfigurace alarmu proti neoprávněnému vniknutí do videa

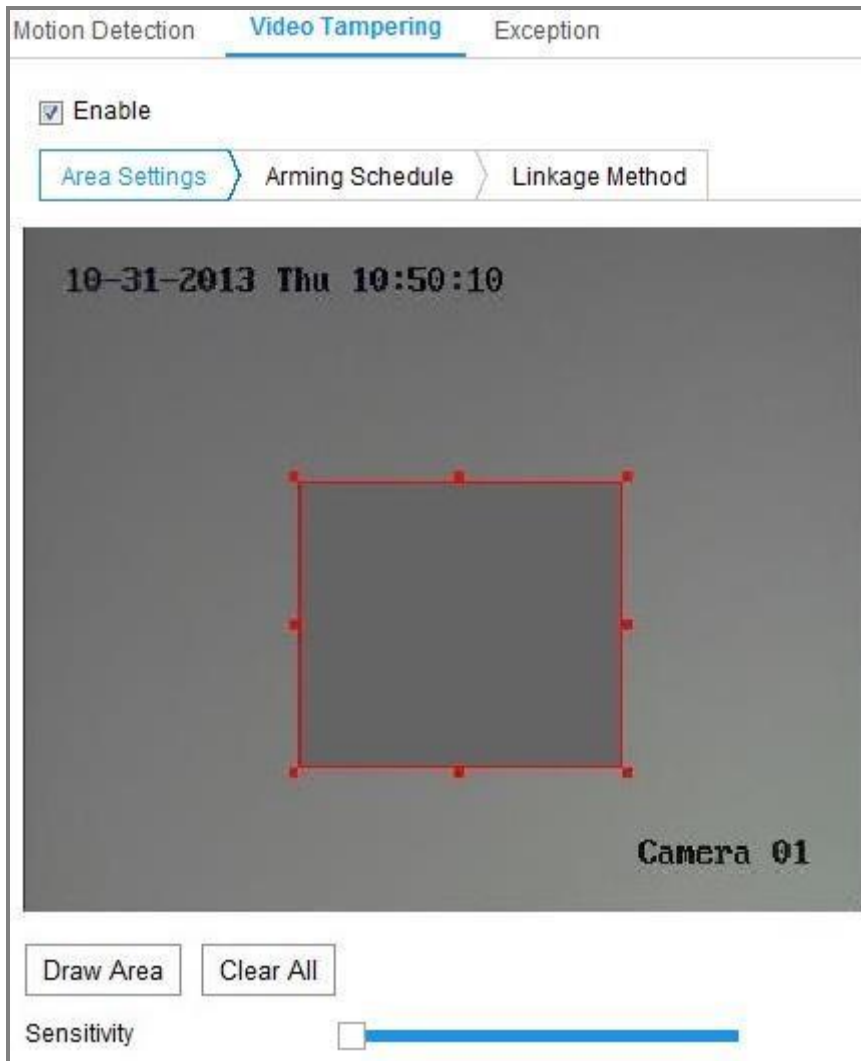
Kameru můžete nakonfigurovat tak, aby spustil alarm při zakrytí objektivu a provedl určité akce reakce na alarm.

Kroky:

1. Vstupte do rozhraní Nastavení narušení videa, Konfigurace > Událost > Základní událost > Narušení videa.

Obrázek 10-7 Poplach při neoprávněné manipulaci s videem

2. Zaškrtnutím políčka Enable Video Tampering (Povolit manipulaci s videem) povolíte detekci manipulace s videem.



Obrázek 10-8 Nastavení alarmových vstupů

3. Kliknutím na Plán zastřežení nastavíte plán zastřežení pro vstup alarmu. Viz Úkol 2: Nastavení plánu zastřežení pro detekci pohybu v části 10.1.1.
4. Klikněte na možnost Metoda propojení a zaškrtnutím políčka vyberte metodu propojení použitou pro vstup alarmu. Viz Úkol 3: Nastavení metody propojení pro detekci pohybu v části 10.1.1.
5. Nastavení můžete zkopírovat do jiných alarmových vstupů.
6. Nastavení uložíte kliknutím na tlačítko Uložit.

10.1.3 Konfigurace poplachového vstupu

kroky:

1. Vstupte do rozhraní Nastavení poplachového vstupu: Konfigurace > Událost > Základní událost > Poplachový vstup.
2. Vyberte číslo vstupu alarmu a Typ alarmu. Typ alarmu může být NO (normálně otevřený) a NC (normálně zavřený). Upravte název a nastavte název pro poplachový vstup (volitelné).

Motion Detection Video Tampering **Alarm Input** Alarm Output Exception PIR Alarm

Alarm Input No. A<-1 IP Address Local

Alarm Type NO Alarm Name (cannot copy)

Enable Alarm Input Handling

Arming Schedule Linkage Method

	0	2	4	6	8	10	12	14	16	18	20	22	24
Mon	[Bar chart showing active period from 6:00 to 14:00]												
Tue	[Bar chart showing active period from 6:00 to 12:00]												
Wed	[Bar chart showing active period from 6:00 to 10:00]												
Thu	[Bar chart showing active period from 6:00 to 12:00]												
Fri	[Bar chart showing active period from 6:00 to 14:00]												
Sat	[Bar chart showing active period from 6:00 to 14:00]												
Sun	[Bar chart showing active period from 6:00 to 14:00]												

Obrázek 10-8 Nastavení poplachového vstupu

3. Klikněte na Plán zapnutí pro nastavení plánu zapnutí pro poplachový vstup. Viz Úkol 2: Nastavte plán aktivace pro detekci pohybu v části 10.1.1.
4. Klikněte na Linkage Method a zaškrtnutím políčka vyberte metodu propojení použitou pro alarmový vstup. Viz Úloha 3: Nastavení metody propojení pro detekci pohybu v části 10.1.1.
5. Svá nastavení můžete zkopírovat do jiných poplachových vstupů.
6. Klepnutím na tlačítko Uložit uložíte nastavení.

10.1.4 Konfigurace výstupu alarmu

Kroky:

1. Vstupte do rozhraní Nastavení alarmových výstupů: Výstup alarmu: Konfigurace > Událost > Základní událost > Výstup alarmu.
2. V rozevíracím seznamu Alarm Output vyberte jeden výstupní kanál alarmu. Můžete také nastavit název alarmového výstupu (volitelné).
3. Doba zpoždění lze nastavit na 5 s, 10 s, 30 s, 1 min, 2 min, 5 min, 10 min nebo ručně. Doba zpoždění označuje dobu, po kterou zůstane výstup alarmu v platnosti po vzniku alarmu.
4. Kliknutím na Plán strážní služby vstoupíte do rozhraní Upravit časový plán. Konfigurace časového plánu je stejná jako nastavení plánu zastřežení pro detekci pohybu Viz Úkol 2: Nastavení plánu zastřežení pro detekci pohybu v části 10.1.1.
5. Nastavení můžete zkopírovat do jiných výstupů alarmu.
6. Nastavení uložíte kliknutím na tlačítko Uložit.

10.1.5 Konfigurace PIR alarmu

Účel:

PIR (pasivní infračervený) poplach se spustí, když se v zorném poli detektoru pohybuje narušitel. Tepelnou energii rozptýlenou osobou nebo jakýmkoli jiným teplokrevným tvorem, jako jsou psi, kočky atd., lze detekovat.

kroky:

1. Vstupte do rozhraní PIR Alarm: Konfigurace > Událost > Základní událost > PIR Alarm.
2. Zaškrtnutím políčka Povolit aktivujete funkci alarmu PIR.
3. Do textového pole zadejte požadovaný název alarmu.
4. Klikněte na Plán zapnutí pro vstup do rozhraní Edit Schedule Time. Konfigurace časového plánu je stejná jako nastavení plánu zapnutí pro detekci pohybu Viz Úkol 2: Nastavte plán zapnutí pro detekci pohybu v části 10.1.1.
5. Zaškrtnutím políčka vyberte metodu propojení použitou pro manipulaci s videem. Na výběr je zvuková výstraha, upozornění na dohledové centrum, odeslání e-mailu a spuštění poplachového výstupu. Viz Úkol 3: Nastavení metody propojení pro detekci pohybu v části 10.1.1.
6. Nastavení můžete zkopírovat do jiných poplachových výstupů.
7. Klepnutím na tlačítko Uložit uložíte nastavení.

10.1.6 Zpracování výjimky

Typem výjimky může být plný HDD, chyba HDD, odpojení od sítě, konflikt IP adres a nelegální přihlášení ke kamerám.

Poznámka: Tuto funkci podporují pouze některé modely kamer. Parametry zobrazení se liší podle různých modelů kamer. Podrobnosti naleznete v aktuálním rozhraní.

Kroky:

1. Vstupte do rozhraní Nastavení výjimek: Výjimka: Konfigurace > Událost > Základní událost > Výjimka.
2. Zaškrtnutím políčka nastavíte akce prováděné pro alarm výjimky. Viz Úkol 3: Nastavení metody propojení pro detekci pohybu v části 10.1.1.



Obrázek 10-11 Nastavení výjimek

3. Nastavení uložíte kliknutím na tlačítko Uložit.

10.2 Chytré události

Podle pokynů v této části můžete nakonfigurovat inteligentní události, včetně detekce zvukových výjimek, detekce rozostření, detekce změny scény, detekce narušení a detekce překročení čáry

atd. Tyto události mohou spouštět metody propojení, jako je Upozornit dohledové centrum, Odeslat e-mail, Spustit alarmový výstup atd.

10.2.1 Konfigurace detekce narušení

Funkce detekce narušení detekuje osoby, vozidla nebo jiné objekty, které vstoupí a pohybují se v předem definované virtuální oblasti, a po spuštění alarmu lze provést určité akce.

Poznámka: Funkce detekce narušení se liší podle různých modelů kamer.

Kroky:

1. Vstupte do rozhraní nastavení detekce narušení, Konfigurace > Událost > Inteligentní událost > Detekce narušení.



Obrázek 10-12 Detekce narušení

2. Zaškrtnutím políčka Povolit funkci povolíte.

3. Vyberte číslo regionu z rozevíracího seznamu Region.

Region: Oblast: Předdefinovaná oblast vrcholů na obraze živého náhledu. Cíle, jako jsou osoby, vozidla nebo jiné objekty, které vstoupí do této oblasti a zdržují se v ní, budou detekovány a spustí nastavený alarm.

4. Klikněte na kartu Nastavení oblasti a kliknutím na tlačítko Nakreslit oblast spustíte kreslení oblasti.

5. Kliknutím na živé video určete čtyři vrcholy detekční oblasti a kliknutím pravým tlačítkem myši dokončete kreslení.

6. Nastavte hodnotu Max. Velikost a min. Size pro platné cíle. Cíle menší nebo větší, než je platná velikost cíle, nejsou schopny spustit detekci.

Max. Velikost: Maximální velikost platného cíle. Cíle s většími rozměry by detekci nevyvolaly.

Min. Velikost: Minimální velikost platného cíle. Cíle s menší velikostí by detekci nevyvolaly.

7. Po dokončení kreslení klikněte na tlačítko Zastavit kreslení.

8. Nastavení časového prahu pro detekci narušení.

Prahová hodnota: Práh: Rozsah [0s-10s], práh pro dobu, po kterou se objekt zdržuje v oblasti.

Pokud nastavíte hodnotu 0, alarm se spustí okamžitě po vstupu objektu do oblasti.

9. Přetažením posuvníku nastavte hodnotu citlivosti.

Citlivost: Rozsah [1-100]. Citlivost znamená procento části těla přijatelného cíle, které zasahuje do předem definované oblasti.

Citlivost = $100 - S1/S T * 100$

S1 znamená cílovou část těla, která prochází předem definovanou oblastí. S1 označuje celé cílové těleso.

Příklad: Pokud nastavíte hodnotu 60, může být akce započítána jako narušení pouze tehdy, když do oblasti vstoupí 40 % těla.

Poznámka: Citlivost detekce podporují jen některé modely. Podrobnosti naleznete na aktuálním displeji.

10. Pro konfiguraci dalších oblastí zopakujte výše uvedené kroky. Lze nastavit až 4 regiony.

Kliknutím na tlačítko Vymazat vymažete všechny předdefinované regiony.

11. Kliknutím na Plán zastřežení nastavíte plán zastřežení.

12. Kliknutím na možnost Metoda propojení vyberte metody propojení pro detekci narušení, včetně možností Upozornit dohledové centrum, Odeslat e-mail, Nahrát na FTP/paměťovou kartu/NAS, Spouštěcí kanál a Spouštěcí výstup alarmu.

13. Nastavení uložíte kliknutím na tlačítko Uložit.

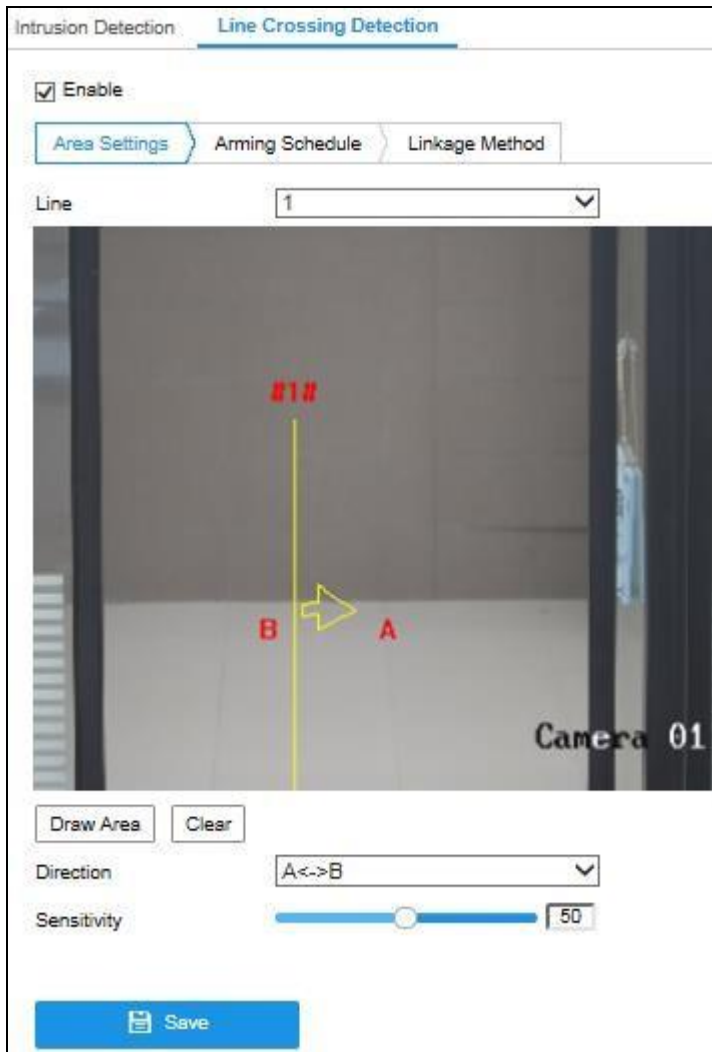
10.2.2 Konfigurace detekce překročení čáry

Funkce detekce překročení čáry detekuje osoby, vozidla nebo jiné objekty, které překročí předem definovanou virtuální čáru, a po spuštění alarmu lze provést určité akce.

Poznámka: Funkce detekce křížení čar se liší podle různých modelů kamer.

Kroky:

1. Vstupte do rozhraní nastavení detekce křížení vedení, Konfigurace > Událost > Inteligentní událost > Detekce překročení čáry.



Obrázek 10-13 Detekce překročení čáry

2. Zaškrtnutím políčka Povolit funkci povolíte.

3. Vyberte řádek z rozevíracího seznamu.

4. Klikněte na kartu Nastavení oblasti a na tlačítko Nakreslit oblast a na živém videu se zobrazí virtuální čára.

5. Přetáhněte čáru a můžete ji umístit na živé video podle potřeby. Klikněte na čáru, na každém konci se zobrazí dva červené čtverce a kliknutím a přetažením jednoho z červených čtverců můžete definovat tvar a délku čáry.

6. Nastavte hodnotu Max. Velikost a min. Size pro platné cíle. Cíle menší nebo větší, než je platná velikost cíle, nejsou schopny spustit detekci.

Max. Velikost: Maximální velikost platného cíle. Cíle s většími rozměry by detekci nevyvolaly.

Min. Velikost: Minimální velikost platného cíle. Cíle s menší velikostí by detekci nevyvolaly.

7. Zvolte směr detekce křížení čar. Můžete vybrat směry A<->B, A->B a B->A.

A<->B: Objekt procházející rovinou oběma směry může být detekován a jsou spuštěny alarmy.

A->B: lze detekovat pouze objekt, který přechází přes nakonfigurovanou linii ze strany A na stranu B.

B->A: lze detekovat pouze objekt, který přechází přes nakonfigurovanou linii ze strany B na stranu A.

8. Po dokončení kreslení klikněte na tlačítko Zastavit kreslení.

9. Přetažením posuvníku nastavte hodnotu citlivosti.

Citlivost: Rozsah [1-100]. Označuje procento části těla přijatelného cíle, které překračuje předem definovanou čáru.

Citlivost = $100 - S / S T * 100$

S1 znamená cílovou část těla, která prochází přes předem definovanou čáru. ST označuje celé cílové těleso.

Příklad: Pokud nastavíte hodnotu 60, může být akce započítána jako akce překročení čáry pouze tehdy, když 40 % nebo více částí těla překročí čáru. Poznámka: Citlivost detekce je podporována jen u některých modelů. Podrobnosti naleznete na aktuálním displeji.

Kapitola 11 Nastavení úložiště

Než začnete:

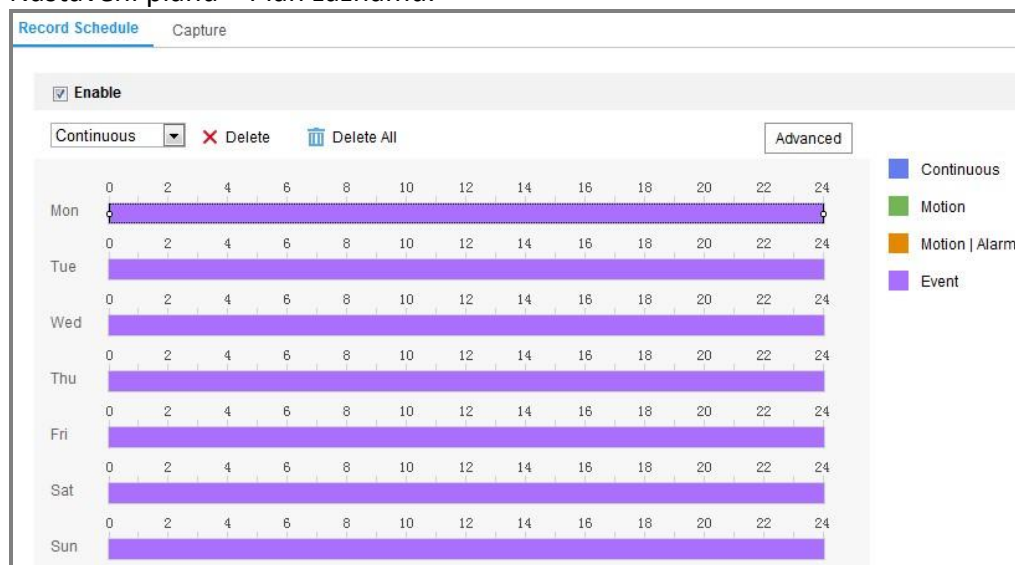
Chcete-li nakonfigurovat nastavení záznamu, ujistěte se, že máte nakonfigurované síťové nebo místní úložné zařízení.

11.1 Konfigurace plánu záznamů

Kamery mají dva druhy nahrávání: ruční nahrávání a plánované nahrávání. V této části můžete podle pokynů nakonfigurovat plánované nahrávání. Ve výchozím nastavení se soubory záznamu plánovaného nahrávání ukládají do místního úložiště nebo na síťový disk.

Kroky:

1. Vstupte do rozhraní Nastavení plánu záznamů: Nastavení záznamu: Konfigurace > Úložiště > Nastavení plánu > Plán záznamu.



Obrázek 11-1 Rozhraní plánu nahrávání 2. Zaškrtnutím políčka Povolit povolíte plánované nahrávání.

3. Kliknutím na tlačítko Advanced (Pokročilý) nastavte parametry záznamu z kamery.

Advanced
✕

Overwrite

Pre-record ▼

Post-record ▼

Stream Type ▼

Obrázek 11-2 Parametry záznamu

- **Předběžný záznam:** Čas, který jste nastavili pro zahájení nahrávání před plánovaným časem nebo událostí. Pokud například alarm spustí nahrávání v 10:00 a čas před nahráváním je nastaven na 5 sekund, kamera začne nahrávat v 9:59:55. Dobu předběžného záznamu lze nastavit jako Žádný předběžný záznam, 5 s, 10 s, 15 s, 20 s, 25 s, 30 s nebo neomezeně.

- **Pořízení záznamu:** Čas, který jste nastavili pro ukončení nahrávání po uplynutí naplánovaného času nebo události. Pokud například záznam spuštěný alarmem skončí v 11:00 a čas po ukončení záznamu je nastaven na 5 sekund, kamera bude nahrávat až do 11:00:05. Čas po záznamu lze nastavit jako 5 s, 10 s, 30 s, 1 min, 2 min, 5 min nebo 10 min.

- **Typ toku:** Zvolte typ proudu pro nahrávání.

Poznámka: Konfigurace parametrů záznamu se liší v závislosti na modelu kamery.

4. Vyberte typ záznamu. Typ záznamu může být kontinuální, detekce pohybu, alarm, pohyb | alarm, pohyb a alarm a událost.

- **Průběžné**

Pokud vyberete možnost Nepřetržitý, bude se video nahrávat automaticky podle časového plánu.

- **Záznam spuštěný detekcí pohybu**

Pokud vyberete možnost Detekce pohybu, bude video zaznamenáno při detekci pohybu.

Kromě konfigurace plánu nahrávání je třeba nastavit oblast detekce pohybu a zaškrtnout políčko Trigger Channel v rozhraní Linkage Method of Motion Detection

37

Settings. Podrobné informace naleznete v části Úkol 1: Nastavení oblasti detekce pohybu v části 10.1.1.

- **Záznam spuštěný alarmem**

Pokud vyberete možnost Alarm, bude se video nahrávat, když se alarm spustí prostřednictvím externích vstupních kanálů alarmu.

Kromě konfigurace plánu nahrávání je třeba nastavit typ alarmu a zaškrtnout políčko Trigger Channel (Spouštěcí kanál) v rozhraní Alarm Input Settings (Nastavení vstupů alarmu). Podrobné informace naleznete v části 10.1.2.

- **Záznam spuštěný pohybem a alarmem**

Pokud vyberete možnost Pohyb a alarm, bude video zaznamenáno při současném spuštění pohybu a alarmu.

Kromě konfigurace plánu nahrávání je třeba nakonfigurovat nastavení v rozhraních Detekce pohybu a Nastavení alarmových vstupů. Podrobné informace naleznete v části 10.1.1 a 10.1.2.

- **Záznam spuštěný pohybem | Alarm**

Pokud vyberete možnost Pohyb | Alarm, video se bude nahrávat při spuštění externího alarmu nebo při detekci pohybu.

Kromě konfigurace plánu nahrávání je třeba nakonfigurovat nastavení v rozhraních Detekce pohybu a Nastavení alarmových vstupů. Podrobné informace naleznete v části 10.1.1 a 10.1.3.

- **Záznam spuštěný událostmi**

Pokud vyberete možnost Událost, bude video zaznamenáno, pokud dojde ke spuštění některé z událostí. Kromě konfigurace plánu nahrávání musíte nakonfigurovat i nastavení událostí.

5. Vyberte typ záznamu a kliknutím a tažením myši na časový pruh nastavte plán záznamu.

6. Nastavení uložíte kliknutím na tlačítko Uložit.

11.2 Konfigurace plánu snímání

Můžete nakonfigurovat naplánovaný snímek a snímek spouštěný událostí. Pořízený snímek lze uložit do místního nebo síťového úložiště.

Kroky:

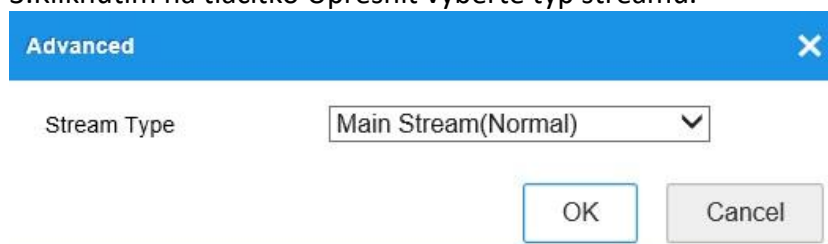
1. Vstupte do rozhraní Capture Settings: Nastavení úložiště > Capture: Konfigurace > Úložiště > Nastavení úložiště > Capture.



Obrázek 11-3 Konfigurace snímání

2. Přejděte na kartu Plán snímání a nakonfigurujte plán snímání kliknutím myši na časový pruh. Plán záznamu můžete zkopírovat do dalších dnů kliknutím na zelenou ikonu kopírování vpravo na každém časovém pruhu.

3. Kliknutím na tlačítko Upřesnit vyberte typ streamu.



Obrázek 11-4 Pokročilé nastavení plánu snímání

4. Nastavení uložíte kliknutím na tlačítko Uložit.

5. Přejděte na kartu Parametry snímání a nakonfigurujte parametry snímání.

(1) Zaškrtnutím políčka Povolit časový snímek povolíte průběžné snímání.

(2) Vyberte formát obrazu, rozlišení, kvalitu a interval snímání.

(3) Zaškrtnutím políčka Enable Event-triggered Snapshot povolíte událostmi spouštěný snímek.

(4) Vyberte formát obrázku, rozlišení, kvalitu, interval snímání a číslo snímání.

Capture Schedule > Capture Parameters

Timing

Enable Timing Snapshot

Format: JPEG

Resolution: 2560*1920

Quality: High

Interval: 1000 millisecond

Event-Triggered

Enable Event-Triggered Snapshot

Format: JPEG

Resolution: 2560*1920

Quality: High

Interval: 1000 millisecond

Capture Number: 4

Obrázek 11-5 Nastavení parametrů zachycení

- Nastavte časový interval mezi dvěma snímky.
- Klepnutím na tlačítko Uložit uložíte nastavení.

11.3 Konfigurace síťového HDD

Než začneš:

Síťový disk by měl být dostupný v síti a správně nakonfigurován pro ukládání nahraných souborů, souborů protokolu, obrázků atd.

kroky:

- Přidejte Net HDD.

(1) Vstupte do rozhraní nastavení Net HDD, Configuration > Storage > Storage Management > Net HDD.

HDD Management **Net HDD**

HDD No.	Server Address	File Path	Type	Delete
1	10.16.5.33	/cxy_1	NAS	✖

Mounting Type: SMB/CIFS User Name: cxy1 Password: ●●●●●● Test

(2) Zadejte IP adresu síťového disku a zadejte cestu k souboru.

(3) Vyberte typ montáže. Lze vybrat NFS a SMB/CIFS. Pokud je vybrána možnost SMB/CIFS, můžete nastavit uživatelské jméno a heslo pro zajištění bezpečnosti.

Poznámka: Informace o vytvoření cesty k souboru naleznete v uživatelské příručce NAS.

● V zájmu ochrany vašeho soukromí a lepší ochrany systému před bezpečnostními riziky důrazně doporučujeme používat silná hesla pro všechny funkce a síťová zařízení. Heslo by mělo být něco,

co si sami zvolíte (s použitím minimálně 8 znaků, včetně alespoň tří z následujících kategorií: velká písmena, malá písmena, číslice a speciální znaky), aby se zvýšila bezpečnost vašeho produktu.

● Za správnou konfiguraci všech hesel a dalších bezpečnostních nastavení je zodpovědný instalátor a/nebo koncový uživatel.

(4) Kliknutím na tlačítko Uložit přidejte síťový disk.

2. Inicializujte přidaný síťový disk.

(1) Vstupte do rozhraní HDD Settings, Configuration > Storage > Storage Management > HDD Management, ve kterém můžete zobrazit kapacitu, volné místo, stav, typ a vlastnosti disku.

HDD Management								Format
<input checked="" type="checkbox"/>	HDD No.	Capacity	Free space	Status	Type	Property	Progress	
<input checked="" type="checkbox"/>	9	9.84GB	0.00GB	Normal	NAS	R/W		
<input checked="" type="checkbox"/>	10	10.00GB	6.75GB	Normal	NAS	R/W		
<input type="checkbox"/>								

Quota	
Max. Picture Capacity	<input type="text" value="4.50GB"/>
Free Size for Picture	<input type="text" value="0.00GB"/>
Max. Record Capacity	<input type="text" value="14.25GB"/>
Free Size for Record	<input type="text" value="6.75GB"/>

Obrázek 11-7 Rozhraní pro správu úložiště

(2) Pokud je stav disku Neinicializovaný, zaškrtnutím příslušného políčka vyberte disk a kliknutím na tlačítko Formátovat spusťte inicializaci disku.

Po dokončení inicializace bude disk ve stavu Normal.

HDD Management								Set	Format
<input checked="" type="checkbox"/>	HDD No.	Capacity	Free space	Status	Type	Property	Progress		
<input checked="" type="checkbox"/>	9	20.00GB	0.00GB	Formatting	NAS	R/W			
<input type="checkbox"/>									

Obrázek 11-8 Zobrazení stavu disku

3. Definujte kvótu pro záznamy a obrázky.

(1) Zadejte procentní podíl kvóty pro obrázek a pro záznam.

(2) Klikněte na tlačítko Uložit a obnovte stránku prohlížeče, aby se nastavení aktivovalo.

Quota	
Max. Picture Capacity	<input type="text" value="4.75GB"/>
Free Size for Picture	<input type="text" value="4.75GB"/>
Max. Record Capacity	<input type="text" value="14.50GB"/>
Free Size for Record	<input type="text" value="14.50GB"/>
Percentage of Picture	<input type="text" value="25"/> %
Percentage of Record	<input type="text" value="75"/> %

Obrázek 11-9 Nastavení kvóty Poznámka:

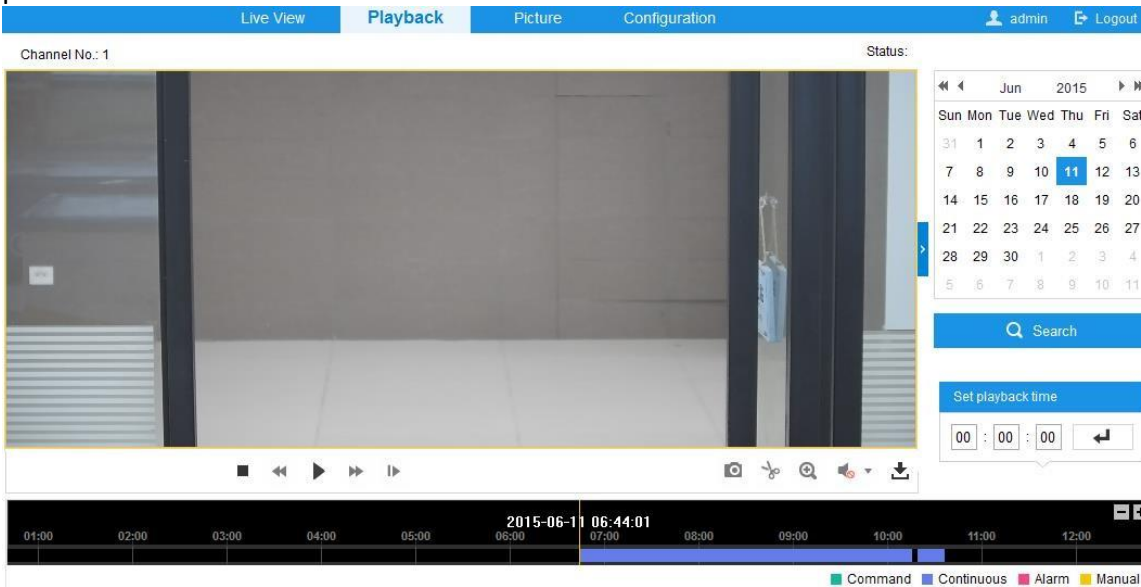
Ke kameře lze připojit až 8 disků NAS.

Kapitola 12 Přehrávání

Tato část vysvětluje, jak zobrazit vzdáleně nahrané videosoubory uložené na síťových discích nebo paměťových kartách.

Kroky:

1. Klepnutím na tlačítko Playback (Přehrávání) na panelu nabídek vstoupíte do rozhraní pro přehrávání.



2. Vyberte datum a klikněte na tlačítko Hledat.



Obrázek 12-2 Vyhledávání videa

3. Kliknutím přehrajete videosoubory nalezené k tomuto datu.

Rozhraní pro přehrávání

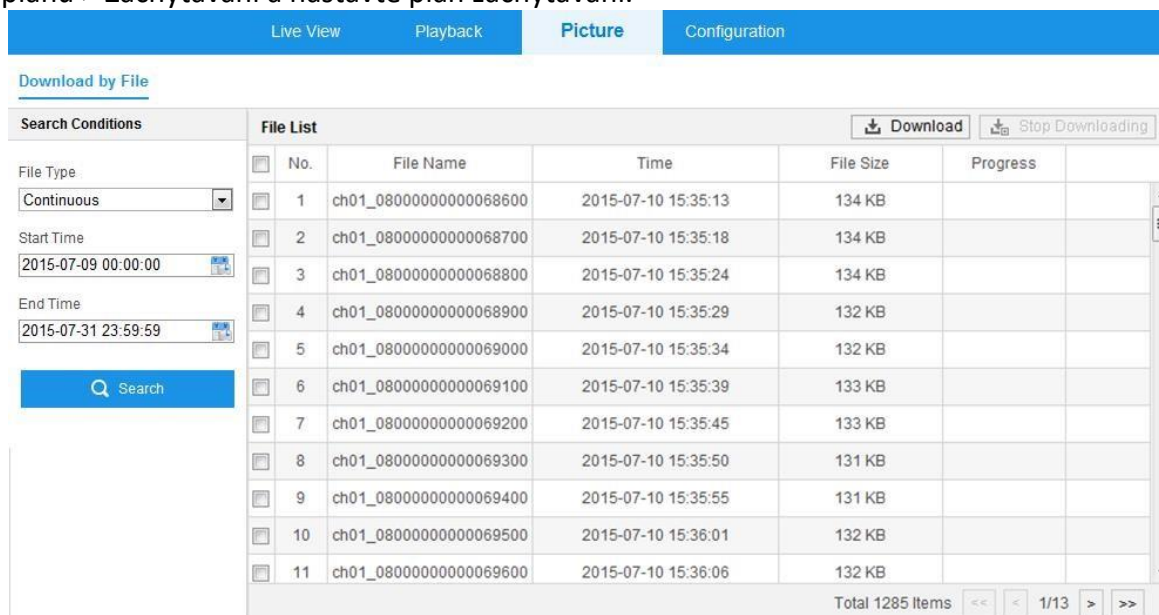


Kapitola 13 Snímek

Klepnutím na Snímek vstoupíte do rozhraní pro vyhledávání obrázků. Můžete vyhledávat, prohlížet a stahovat obrázky uložené v místním úložišti nebo v síťovém úložišti.

Poznámky:

- Před zpracováním vyhledávání obrázků se ujistěte, že jsou HDD, NAS nebo paměťová karta správně nakonfigurovány.
- Ujistěte se, že je nakonfigurován plán zachycení. Přejděte do Konfigurace > Úložiště > Nastavení plánu > Zachytávání a nastavte plán zachytávání.



The screenshot shows a web interface for image search. At the top, there are four tabs: 'Live View', 'Playback', 'Picture' (selected), and 'Configuration'. Below the tabs, there is a 'Download by File' link. The main area is divided into 'Search Conditions' on the left and 'File List' on the right. The 'Search Conditions' section includes a 'File Type' dropdown set to 'Continuous', 'Start Time' (2015-07-09 00:00:00), and 'End Time' (2015-07-31 23:59:59). A 'Search' button is located below these fields. The 'File List' section is a table with columns: No., File Name, Time, File Size, and Progress. It contains 11 rows of data. At the bottom right of the table, it says 'Total 1285 Items' and has navigation buttons for page 1/13.

No.	File Name	Time	File Size	Progress
1	ch01_08000000000068600	2015-07-10 15:35:13	134 KB	
2	ch01_08000000000068700	2015-07-10 15:35:18	134 KB	
3	ch01_08000000000068800	2015-07-10 15:35:24	134 KB	
4	ch01_08000000000068900	2015-07-10 15:35:29	132 KB	
5	ch01_08000000000069000	2015-07-10 15:35:34	132 KB	
6	ch01_08000000000069100	2015-07-10 15:35:39	133 KB	
7	ch01_08000000000069200	2015-07-10 15:35:45	133 KB	
8	ch01_08000000000069300	2015-07-10 15:35:50	131 KB	
9	ch01_08000000000069400	2015-07-10 15:35:55	131 KB	
10	ch01_08000000000069500	2015-07-10 15:36:01	132 KB	
11	ch01_08000000000069600	2015-07-10 15:36:06	132 KB	

Obrázek 13-1 Kroky rozhraní pro vyhledávání obrázků:

- Vyberte Typ souboru jako Nepřetržitý, Pohyb nebo Výstraha.
 - (1) Vyberte typ souboru, čas zahájení a čas ukončení.
 - (2) Klepněte na Hledat. Výsledky budou uvedeny v oblasti seznamu obrázků.
 - (3) Vyberte jeden obrázek a kliknutím na Náhled zobrazíte náhled obrázku.
 - (4) Zaškrtněte políčko u každého obrázku a kliknutím na Stáhnout stáhněte vybrané obrázky.
- Vyberte Typ souboru jako Detekce vozidla.
 - (1) Vyberte typ souboru, čas zahájení a čas ukončení. Pro zúžení vyhledávání můžete také zadat SPZ.

Poznámka:

Fuzzy vyhledávání je podporováno pro SPZ. Pro vyhledávání podle SPZ jsou potřeba pouze čísla a písmena.

- (2) Klepněte na Hledat. Výsledky budou uvedeny v oblasti seznamu obrázků.
- (3) Chcete-li stáhnout obrázky, zaškrtněte políčko u požadovaných obrázků a klikněte na Stáhnout v pravém horním rohu stránky.
- (4) Chcete-li exportovat informace o vozidle z výsledků vyhledávání, klikněte na Export.

Poznámka:

- Nakonfigurujte cestu uložení z Konfigurace > Místní > Nastavení obrázků a klipů > Uložit snímky v živém zobrazení do.
- Najednou lze zobrazit až 4000 snímků.

Dodatek 1 Úvod do softwaru SADP

SADP (Search Active Devices Protocol) je druh uživatelsky přívětivého online nástroje pro vyhledávání zařízení bez nutnosti instalace. Prohledává aktivní online zařízení ve vaší podsíti a zobrazuje informace o zařízeních. Pomocí tohoto softwaru můžete také upravit základní síťové informace zařízení.

- Hledat aktivní zařízení online
- Automaticky vyhledávat online zařízení

Po spuštění softwaru SADP automaticky každých 15 sekund prohledá online zařízení z podsítě, kde se nachází váš počítač. Zobrazuje celkový počet a informace o hledaných zařízeních v rozhraní Online zařízení. Zobrazí se informace o zařízení včetně typu zařízení, IP adresy a čísla portu atd.

Zařízení lze vyhledat a zobrazit v seznamu do 15 sekund po připojení; bude odstraněn ze seznamu do 45 sekund po přechodu do režimu offline.

- Vyhledejte online zařízení ručně

Můžete také kliknout a aktualizovat online seznam zařízení ručně. Nově vyhledaná zařízení budou přidána do seznamu.

Kliknutím na záhlaví každého sloupce můžete informace seřadit; můžete kliknutím rozbalit tabulku zařízení a skrýt panel síťových parametrů na pravé straně nebo kliknutím zobrazit panel síťových parametrů.

- Upravte parametry sítě

kroky:

1. Vyberte zařízení, které chcete upravit, v seznamu zařízení a síťové parametry zařízení se zobrazí v panelu Upravit parametry sítě na pravé straně.
2. Upravte upravitelné parametry sítě, např. IP adresa a číslo portu.
3. Do pole Heslo správce zadejte heslo účtu správce zařízení pole a kliknutím uložte změny.

- Pro vaše soukromí a lepší ochranu vašeho systému před bezpečnostními riziky důrazně doporučujeme používat silná hesla pro všechny funkce a síťová zařízení. Heslo by mělo být podle vašeho vlastního výběru (s použitím minimálně 8 znaků, včetně alespoň tří z následujících kategorií: velká písmena, malá písmena, čísla a speciální znaky), aby se zvýšila bezpečnost vašeho produktu.

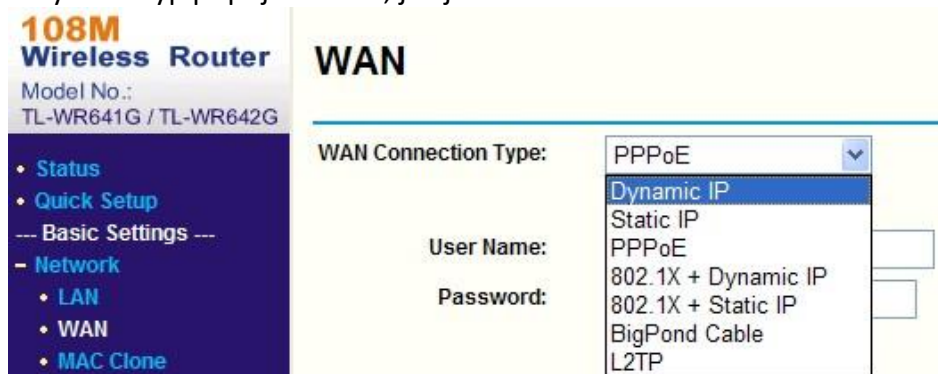
- Za správnou konfiguraci všech hesel a dalších nastavení zabezpečení odpovídá instalační technik a/nebo koncový uživatel.

Dodatek 2 Mapování portů

Následující nastavení platí pro router TP-LINK (TL-WR641G). Nastavení se liší v závislosti na různých modelech routerů.

kroky:

1. Vyberte typ připojení WAN, jak je znázorněno níže:



Obrázek A.2.1 Vyberte typ připojení WAN

2. Nastavte parametry LAN routeru jako na následujícím obrázku, včetně nastavení IP adresy a masky podsítě.

3. Nastavte mapování portů na virtuálních serverech Forwarding. Ve výchozím nastavení kamera používá porty 80, 8000 a 554. Hodnotu těchto portů můžete změnit pomocí webového prohlížeče nebo klientského softwaru.

Příklad:

Když jsou kamery připojeny ke stejnému routeru, můžete nakonfigurovat porty kamery jako 80, 8000 a 554 s IP adresou 192.168.1.23 a porty jiné kamery jako 81, 8001, 555, 8201 s IP 192.168.1.24. Postupujte podle níže uvedených kroků:

kroky:

1. Jak je uvedeno výše, namapujte port 80, 8000, 554 a 8200 pro síťovou kameru na 192.168.1.23
2. Namapujte port 81, 8001, 555 a 8201 pro síťovou kameru na 192.168.1.24.
3. Povolte VŠECHNY nebo TCP protokoly.
4. Zaškrtněte políčko Povolit a kliknutím na Uložit uložte nastavení.

Poznámka: Port síťové kamery nemůže být v konfliktu s jinými porty. Například některý port pro webovou správu routeru je 80. Změňte port kamery, pokud je stejný jako port pro správu.



First Choice for Security Professionals