



HIKVISION

Sít'ová kamera

Uživatelská příručka

UD.6L0201D1919A01

Uživatelská příručka

COPYRIGHT ©2015 Hangzhou Hikvision Digital Technology Co., Ltd.

VŠECHNA PRÁVA VYHRAZENA.

Veškeré informace, mj. včetně formulací, obrázků, grafů, jsou majetkem společnosti Hangzhou Hikvision Digital Technology Co., Ltd. nebo jejích dceřiných společností (dále označováno jako "Hikvision"). Tuto uživatelskou příručku (dále označovanou jako "příručka") ani žádnou její část nelze žádným způsobem reprodukovat, měnit, překládat ani šířit bez předchozího písemného souhlasu společnosti Hikvision. Pokud není určeno jinak, společnost Hikvision neposkytuje žádné záruky, garance ani vyjádření, jak výslovné, tak mlčky předpokládané, ohledně této příručky.

O této příručce

Tato příručka se vztahuje k síťové videokameře (V5.3.0).

Tato příručka obsahuje pokyny k používání a ovládání výrobku. Obrázky, grafy, snímky a veškeré další dále uvedené informace slouží pouze k popisu a vysvětlení. Informace obsažené v příručce mohou být bez předchozího oznámení změněny z důvodu aktualizací firmwaru nebo jiných důvodů. Nejnovější verzi získáte na webových stránkách společnosti (<http://overseas.hikvision.com/en/>).

Tuto příručku používejte pod dohledem odborníků.

Uznání ochranných známek

HIKVISION a další ochranné známky a loga společnosti Hikvision jsou majetkem společnosti Hikvision v různých jurisdikcích. Ostatní dále zmíněné ochranné známky a loga jsou majetkem příslušných vlastníků.

Odmítnutí právní odpovědnosti

V MAXIMÁLNÍ MÍŘE PŘÍPUSTNÉ PLATNÝMI ZÁKONY JE POPISOVANÝ VÝROBEK, VČETNĚ HARDWARU, SOFTWARE A FIRMWARU, POSKYTOVÁN "TAK, JAK JE", SE VŠEMI VADAMI A CHYBAMI, A SPOLEČNOST HIKVISION NEPOSKYTUJE ŽÁDNÉ VÝSLOVNÉ ANI MLČKY PŘEDPOKLÁDANÉ ZÁRUKY MJ. NA OBCHODOVATELNOST,

USPOKOJIVOU KVALITU, VHODNOST KE KONKRÉTNÍMU ÚČELU A NEZASAHOVÁNÍ DO PRÁV TŘETÍ STRANY. SPOLEČNOST HIKVISION, JEJÍ ŘEDITELÉ, VEDOUcí PRACOVNÍCI, ZAMĚSTNANCI ANI ZÁSTUPCI NEJSOU V ŽÁDNÉM PŘÍPADĚ ODPOVĚDNÍ ZA JAKÉKOLI ZVLÁŠNÍ, NÁSLEDNÉ, NÁHODNÉ NEBO NEPŘÍMÉ ŠKODY, VČETNĚ MJ. ŠKOD Z DŮVODU UŠLÉHO ZISKU, PŘERUŠENÍ OBCHODNÍ ČINNOSTI NEBO ZTRÁTY DAT ČI DOKUMENTACE, VE SPOJENÍ S POUŽITÍM TOHOTO VÝROBKU, I V PŘÍPADĚ, ŽE BYLA SPOLEČNOST HIKVISION NA MOŽNOST TAKOVÝCH ŠKOD UPOZORNĚNA.

S OHLEDEM NA VÝROBEK S PŘÍSTUPEM K INTERNETU JE JEHO POUŽITÍ VÝHRADNĚ NA VAŠE VLASTNÍ RIZIKO. SPOLEČNOST HIKVISION NEPŘIJÍMÁ JAKOUKOLI ODPOVĚDNOST ZA NENORMÁLNÍ ČINNOST, ÚNIK SOUKROMÝCH INFORMACÍ NEBO JINÉ ŠKODY V DŮSLEDKU KYBERNETICKÉHO ÚTOKU, ÚTOKU POČÍTAČOVÝCH PIRÁTŮ, NAKAŽENÍ VIREM NEBO JINÁ BEZPEČNOSTNÍ RIZIKA INTERNETU; V PŘÍPADĚ POTŘEBY VŠAK SPOLEČNOST HIKVISION POSKYTNE VČASNOU TECHNICKOU PODPORU.

ZÁKONY SOUVISEJÍCÍ S KAMEROVÝMI SYSTÉMU SE V RŮZNÝCH JURISDIKCÍCH LIŠÍ. PŘED POUŽITÍM TOHOTO VÝROBKU PROVĚŘTE VŠECHNY SOUVISEJÍCÍ ZÁKONY, ABY BYLO ZAJIŠTĚNO, ŽE POUŽITÍ SPLŇUJE ZÁKONNÉ POŽADAVKY. SPOLEČNOST HIKVISION NEPŘIJÍMÁ JAKOUKOLI ODPOVĚDNOST V PŘÍPADĚ, ŽE JE VÝROBEK POUŽÍVÁN PRO NEZÁKONNÉ ÚČELY.

V PŘÍPADĚ KONFLIKTŮ MEZI TOUTO PŘÍRUČKOU A PLATNÝMI ZÁKONY MAJÍ PŘEDNOST ZÁKONY.

Informace o právních předpisech

Informace úřadu FCC

Shoda FCC: Toto zařízení bylo testováno a shledáno vyhovujícím omezením platným pro digitální zařízení, na základě části 15 směrnic FCC. Tato omezení jsou

navržena tak, aby poskytovala přiměřenou ochranu vůči škodlivému rušení, pokud je zařízení provozováno v komerčním prostředí. Zařízení generuje, používá a může vyzařovat rádiové frekvence, a pokud není instalováno v souladu s uživatelskou příručkou, může způsobovat škodlivé rušení rádiové komunikace. Provozování tohoto zařízení v obytné oblasti může způsobovat škodlivé rušení; pokud je tomu tak, je nutné, aby uživatel toto rušení odstranil na vlastní náklady.

Podmínky FCC

Toto zařízení vyhovuje části 15 směrnic FCC. Provozování podléhá následujícím dvěma podmínkám:

1. Toto zařízení nesmí způsobovat škodlivé rušení.
2. Toto zařízení musí akceptovat jakékoli rušení, včetně rušení, které může způsobovat nežádoucí činnost.

Prohlášení o shodě - EU



Tento produkt a případně dodávané příslušenství jsou také označeny logem „CE“ a splňují tak příslušné evropské normy uvedené ve směrnici pro elektromagnetickou kompatibilitu EMC 2004/108/ES, směrnici pro omezení používání určitých nebezpečných látek v elektrických a elektronických přístrojích RoHS 2011/65/EU.



Směrnice Evropského parlamentu a rady 2012/19/EU o odpadních elektrických a elektronických zařízeních (OEEZ): Výrobky označené tímto symbolem nesmí být v Evropské unii likvidovány jako netříděný komunální odpad. Za účelem správné likvidace výrobku, při koupi nového ekvivalentního zařízení, vraťte tento výrobek svému prodejci nebo jej odevzdejte na určených sběrných místech. Více informací naleznete na: www.recyclethis.info.



Směrnice Evropského parlamentu a rady 2006/66/ES o bateriích a akumulátorech: Tento výrobek obsahuje baterii, která nesmí být v Evropské unii likvidována jako netříděný komunální odpad. Konkrétní informace o baterii naleznete v dokumentaci k výrobku.

Baterie je označena tímto symbolem, který může obsahovat písmena označující kadmium (Cd), olovo (Pb) nebo rtuť (Hg). Za účelem správné likvidace výrobku vraťte baterii svému prodejci nebo ji odevzdejte na určených sběrných místech. Více informací naleznete na: www.recyclethis.info.

Shoda Industry Canada ICES-003

Toto zařízení splňuje požadavky norem CAN ICES-3 (A)/NMB-3(A).



Bezpečnostní pokyny

Účelem těchto pokynů je zajistit, aby uživatel mohl používat výrobek správným způsobem bez rizika ohrožení nebo ztráty majetku.

Preventivní opatření jsou rozdělena na „výstrahy“ a „upozornění“:

Výstrahy: Pokud není některé výstrahy dbáno, může dojít k závažnému zranění nebo usmrcení.

Upozornění: Pokud není některé výstrahy dbáno, může dojít ke zranění nebo poškození zařízení.

	
Výstrahy Abyste předešli závažnému zranění nebo usmrcení, dodržujte tato bezpečnostní opatření.	Upozornění Aby nedošlo k případnému zranění nebo materiálním škodám, dodržujte tato preventivní opatření.



Výstrahy:

- Používejte napájecí adaptér, který splňuje požadavky normy SELV (bezpečné malé napětí), a zdroj s napětím 12 VDC nebo 24 VAC (dle modelu) v souladu s normou IEC60950-1 a normou pro napájecí zdroje s omezeným výkonem.
- Abyste předešli nebezpečí požáru nebo úrazu elektrickým proudem, nevystavujte tento výrobek dešti ani vlhkosti.
- Instalaci by měl provést kvalifikovaný pracovník a měla by splňovat všechny místní předpisy.
- Pro případ výpadku napájení instalujte do napájecího obvodu záložní napájecí zdroj.
- Pokud je kamera připevněna ke stropu, ujistěte se, že strop udrží sílu 50 N.
- Pokud výrobek nefunguje správně, obraťte se na prodejce nebo nejbližší servisní středisko. Nikdy se nesnažte kameru rozebrat sami. (Nepřijímáme žádnou

odpovědnost za problémy způsobené neschválenými opravami nebo údržbou.)



Upozornění:

- Před použitím kamery se ujistěte, že napětí zdroje je správné.
- Předcházejte upuštění kamery a vystavení fyzickým nárazům.
- Nedotýkejte se modulů senzoru prsty. Pokud je nutné čištění, použijte čistý hadřík s malým množstvím etanolu a jemně přístroj otřete. Pokud kamera nebude delší dobu používána, nasad'te krytku objektivu pro ochranu senzoru před nečistotami.
- Nemiřte objektivem kamery na silné zdroje světla, jako slunce nebo žárovky. Silné světlo může způsobit nevratné poškození kamery.
- Senzor může být vypálen laserovým paprskem, takže v případě použití laserových zařízení se ujistěte, že povrch senzoru není vystaven laserovému paprsku.
- Neumist'ujte kameru do prostředí s velmi vysokou nebo nízkou teplotou (provozní teplota by měla být v rozmezí -30 °C ~ 60 °C, nebo -40 °C ~ 60 °C v případě modelů kamer s písmenem H na konci označení), prašného nebo vlhkého prostředí a nevystavujte ji silnému elektromagnetickému záření.
- Aby nedocházelo k hromadění tepla, je vyžadováno řádné větrání provozního prostředí.
- Uchovejte kameru z dosahu vody a jiných tekutin.
- Při přepravě by kamera měla být zabalena v původním obalu.
- Nesprávné použití nebo výměna baterie může vést k nebezpečí výbuchu. Používejte typ baterie doporučený výrobcem.

Poznámky:

Pokud kamera podporuje infračervené snímání, je třeba věnovat pozornost následujícím upozorněním ohledně prevence odrazů infračerveného světla:

- Prach nebo mastnota na krytu kopule způsobí odrazy infračerveného světla. Neodstraňujte fólii z krytu kopule před dokončením instalace. Pokud se na krytu kopule nachází prach nebo mastnota, očistěte ho čistým měkkým hadříkem a isopropylalkoholem.
- Ujistěte se, že v místě instalace se v těsné blízkosti kamery nenacházejí povrchy odrážející světlo. Infračervené světlo z kamery se může odrazit zpět do objektivu a způsobit odraz.
- Pěnový kroužek kolem objektivu musí být nasazen v rovině s vnitřním povrchem kopule, aby izoloval objektiv od infračervených diod. Upevněte kryt kopule k tělu kamery tak, aby pěnový kroužek a kryt kopule byly nasazeny beze spár.

Obsah

Chapter 1	<i>Síťové připojení</i>	11
1.1	Nastavení síťové kamery přes síť LAN	11
1.1.1	Zapojení přes síť LAN	11
1.1.2	Aktivace kamery.....	12
1.2	Nastavení síťové kamery přes síť WAN	18
1.2.1	Připojení se statickou IP adresou	18
1.2.2	Připojení s dynamickou IP adresou	19
Chapter 2	<i>Přístup k síťové kameře</i>	22
2.1	Přístup přes webové prohlížeče	22
2.2	Přístup prostřednictvím klientského softwaru	24
Chapter 3	<i>Nastavení Wi-Fi</i>	26
3.1	Konfigurace připojení Wi-Fi ve režimech Manage a Ad-hoc	26
3.2	Jednoduché připojení k síti Wi-Fi pomocí funkce WPS	31
3.3	Nastavení vlastností IP adresy pro připojení k bezdrátové síti	33
Chapter 4	<i>Živý náhled</i>	35
4.1	Stránka živého náhledu	35
4.2	Spuštění živého náhledu	36
4.3	Manuální záznam a pořizování snímků	37
4.4	Obsluha ovládání PTZ	37
4.4.1	Ovládací panel PTZ.....	38
4.4.2	Nastavení/vyvolání předvolby	38
4.4.3	Nastavení/vyvolání kontroly	40
Chapter 5	<i>Konfigurace síťové kamery</i>	41
5.1	Konfigurace místních parametrů	41
5.2	Konfigurace nastavení času	43
5.3	Konfigurace nastavení sítě	45
5.3.1	Konfigurace nastavení TCP/IP	45
5.3.2	Konfigurace nastavení portů	47
5.3.3	Konfigurace nastavení PPPoE	48
5.3.4	Konfigurace nastavení DDNS.....	48
5.3.5	Konfigurace nastavení SNMP	52
5.3.6	Konfigurace nastavení 802.1X.....	53
5.3.7	Konfigurace nastavení QoS	55
5.3.8	Konfigurace nastavení UPnP™	55
5.3.9	Konfigurace nastavení bezdrátového komunikačního spojení	56

5.3.10	Odeslání e-mailu aktivované alarmem.....	60
5.3.11	Konfigurace nastavení NAT (Network Address Translation)	62
5.3.12	Konfigurace nastavení FTP	63
5.3.13	Přístup k platformě	64
5.3.14	Nastavení HTTPS	65
5.4	Konfigurace nastavení videa a audia	67
5.4.1	Konfigurace nastavení videa	67
5.4.2	Konfigurace nastavení audia	70
5.4.3	Konfigurace kódování ROI	71
5.4.4	Zobrazení informací o streamu	73
5.4.5	Konfigurace oříznutí cíle	73
5.5	Konfigurace místních obrazu.....	74
5.5.1	Konfigurace nastavení zobrazení.....	74
5.5.2	Konfigurace nastavení OSD	80
5.5.3	Konfigurace nastavení překrytí textem	82
5.5.4	Konfigurace funkce Privacy Mask (místa zakrytá kvůli ochraně soukromí)	83
5.5.5	Konfigurace překrytí obrázkem.....	84
5.6	Konfigurace a zpracování alarmů	85
5.6.1	Konfigurace detekce pohybu	86
5.6.2	Konfigurace alarmu manipulace s videem	92
5.6.3	Konfigurace vstupu alarmu	93
5.6.4	Konfigurace výstupu alarmu	95
5.6.5	Zpracování výjimky	96
5.6.6	Konfigurace jiného alarmu.....	96
5.6.7	Konfigurace detekce výjimky audia	99
5.6.8	Konfigurace detekce rozostření	101
5.6.9	Konfigurace detekce změny scény	101
5.6.10	Konfigurace detekce obličeje	103
5.6.11	Konfigurace detekce překročení čáry.....	104
5.6.12	Konfigurace detekce narušení.....	106
5.6.13	Konfigurace detekce vstupu do oblasti	108
5.6.14	Konfigurace detekce opuštění oblasti	109
5.6.15	Konfigurace detekce opuštěného zavazadla	111
5.6.16	Konfigurace detekce odstranění předmětu.....	113
5.7	Konfigurace VCA	114
5.7.1	Analýza chování	114
5.7.2	Zachycení obličeje.....	123
5.7.3	Tepelná mapa.....	126
5.7.4	Počítání lidí	129
Chapter 6	<i>Nastavení úložiště.....</i>	133
6.1	Konfigurace nastavení NAS	133
6.2	Konfigurace rozvrhu nahrávání	135

6.3	Konfigurace nastavení snímků	139
6.4	Konfigurace funkce Lite Storage	141
6.5	Konfigurace cloudového úložiště	142
<i>Chapter 7</i>	<i>Počítání</i>	<i>144</i>
<i>Chapter 8</i>	<i>Silniční provoz</i>	<i>147</i>
<i>Chapter 9</i>	<i>Přehrávání</i>	<i>151</i>
<i>Chapter 10</i>	<i>Vyhledávání protokolů</i>	<i>154</i>
<i>Chapter 11</i>	<i>Ostatní</i>	<i>156</i>
11.1	Správa uživatelských účtů	156
11.2	Ověřování	158
11.3	Anonymní návštěva.....	159
11.4	Filtr IP adres	160
11.5	Služba zabezpečení	162
11.6	Prohlížení informací o zařízení	162
11.7	Údržba.....	163
11.7.1	Restartování kamery	163
11.7.2	Obnovení výchozích nastavení	164
11.7.3	Import/export souboru konfigurace	164
11.7.4	Upgrade systému.....	165
11.8	Nastavení rozhraní RS-232	166
11.9	Nastavení RS-485	166
11.10	Nastavení služeb	167
<i>Příloha</i>	<i>168</i>
Příloha 1	Představení softwaru SADP	168
Příloha 2	Mapování portů	171

Požadavky na systém

Operační systém: Microsoft Windows XP SP1 a novější verze / Vista / Win7 / Server 2003 / Server 2008, 32bitový systém

Procesor: Intel Pentium IV 3,0 GHz nebo rychlejší

RAM: 1 GB nebo více

Zobrazení: Rozlišení 1024×768 nebo vyšší

Webový prohlížeč: Internet Explorer 6.0 a novější verze, Apple Safari 5.02 a novější verze, Mozilla Firefox 3.5 a novější verze a Google Chrome 8 a novější verze.

Chapter 1 Síťové připojení

Poznámka:

- Vezměte prosím na vědomí, že použití tohoto výrobku s přístupem k internetu může představovat rizika pro zabezpečení sítě. Aby nedocházelo k síťovým útokům a úniku informací, zvyšte svou vlastní ochranu. Pokud výrobek nefunguje správně, obraťte se na prodejce nebo nejbližší servisní středisko.
- Aby bylo zajištěno zabezpečení sítě síťové kamery, doporučujeme každého čtvrt roku provádět vyhodnocení a údržbu síťové kamery. Pokud takové služby vyžadujete, můžete nás kontaktovat.

Než začnete:

- Pokud chcete nastavit síťovou kameru prostřednictvím sítě LAN (Local Area Network), postupujte podle *kapitoly 2.1 Nastavení síťové kamery přes síť LAN*.
- Pokud chcete nastavit síťovou kameru prostřednictvím sítě WAN (Wide Area Network), postupujte podle *kapitoly 2.2 Nastavení síťové kamery přes síť WAN*.

1.1 Nastavení síťové kamery přes síť LAN

Účel:

Pro zobrazení a konfiguraci kamery přes síť LAN je zapotřebí připojit kameru do stejné podsítě s vaším počítačem a nainstalovat software SADP nebo iVMS-4200 k vyhledání a změně IP adresy síťové kamery.

Poznámka: Podrobné informace o softwaru SADP jsou uvedeny v Příloze 1.

1.1.1 Zapojení přes síť LAN

Následující obrázky znázorňují dva způsoby propojení síťové kamery a počítače pomocí kabelu:

Účel:

- Při testování kamery můžete přímo připojit síťovou kameru k počítači pomocí síťového kabelu dle obrázku 2-1.

- Obrázek 2-2 znázorňuje nastavení kamery přes síť LAN prostřednictvím přepínače nebo směrovače.

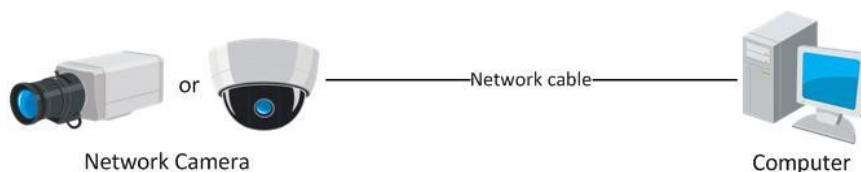


Figure 1-1 Přímé připojení

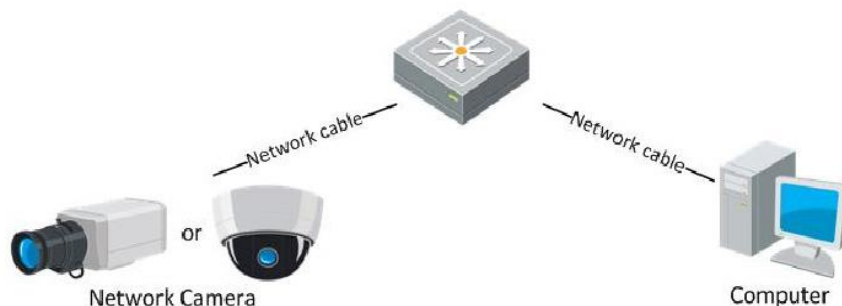


Figure 1-2 Připojení prostřednictvím přepínače nebo směrovače

1.1.2 Aktivace kamery

Nejprve je třeba kameru aktivovat nastavením silného hesla, abyste ji mohli používat. Je podporovaná aktivace pomocí webového prohlížeče, aktivace pomocí softwaru SADP a aktivace pomocí klientského softwaru.

❖ Aktivace pomocí webového prohlížeče

Postup:

1. Zapněte kameru a připojte ji do sítě.
2. Zadejte IP adresu do panelu adresy webového prohlížeče a stisknutím klávesy Enter přejděte do rozhraní pro aktivaci.

Poznámky:

- Výchozí IP adresa kamery je 192.168.1.64.
- V případě kamery s povoleným protokolem DHCP ve výchozím stavu je třeba provést aktivaci pomocí softwaru SADP. Aktivaci prostřednictvím softwaru SADP popisuje následující kapitola.

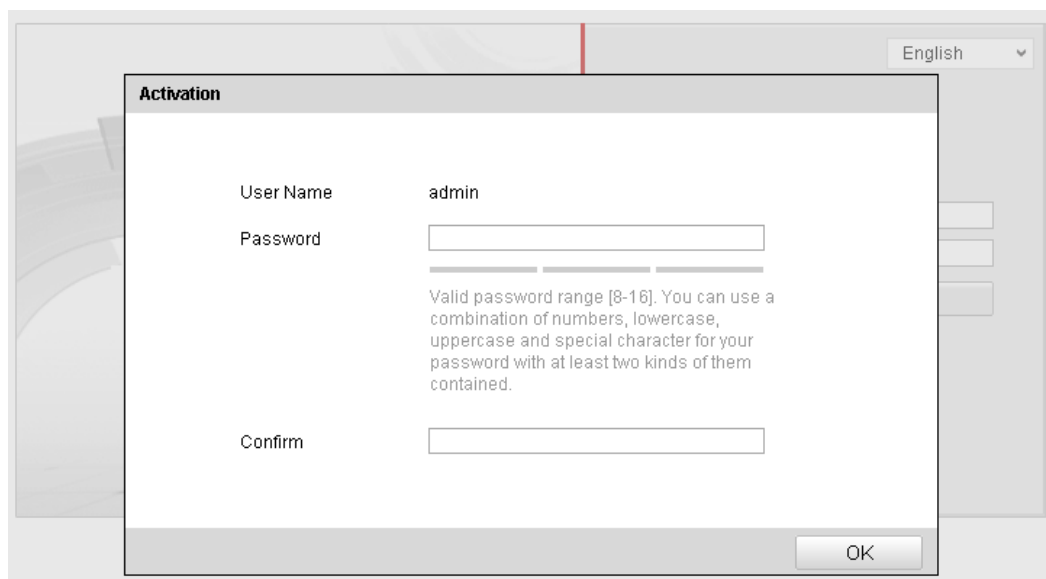


Figure 1-3 Rozhraní pro aktivaci (web)

3. Vytvořte heslo a zadejte ho do pole hesla.

! DOPORUČUJEME POUŽÍT SILNÉ HESLO – důrazně doporučujeme, abyste vytvořili silné heslo dle vlastního výběru (o délce alespoň 8 znaků, s velkými písmeny, malými písmeny, čísly a speciálními znaky), abyste zvýšili zabezpečení výrobku. Rovněž doporučujeme heslo pravidelně obnovovat, obzvláště v systému s vysokým zabezpečením může měsíční nebo týdenní obnovování hesla lépe chránit váš výrobek.

4. Potvrďte heslo.

5. Kliknutím na tlačítko OK uložíte heslo a vstoupíte do rozhraní živého náhledu.

❖ Aktivace prostřednictvím softwaru SADP

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

Software SADP vyhledejte na dodávaném disku nebo oficiálních webových stránkách a proveďte jeho instalaci dle pokynů. Aktivujte kameru podle následujícího postupu.

Postup:

1. Spustěte software SADP pro vyhledání zařízení online.
2. Zkontrolujte stav zařízení v seznamu zařízení a vyberte neaktivní zařízení.

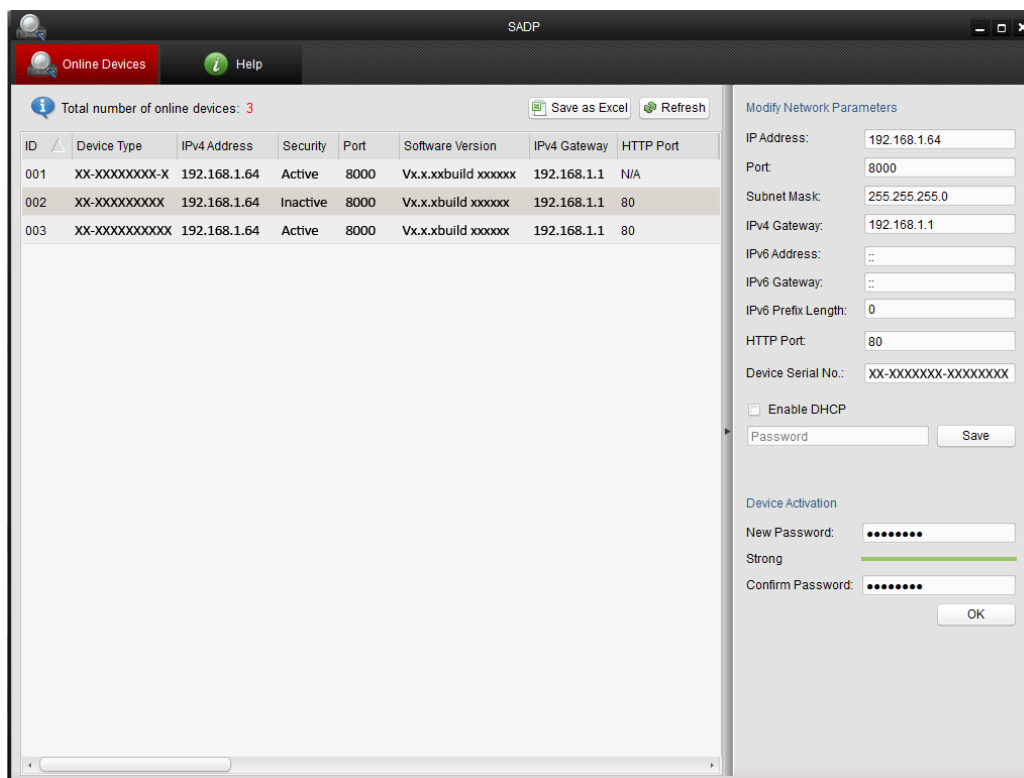


Figure 1-4 Rozhraní softwaru SADP

3. Vytvořte heslo, zadejte ho do pole hesla a potvrďte ho.



DOPORUČUJEME POUŽÍT SILNÉ HESLO – důrazně

doporučujeme, abyste vytvořili silné heslo dle vlastního výběru (o délce alespoň 8 znaků, s velkými písmeny, malými písmeny, čísly a speciálními znaky), abyste zvýšili zabezpečení výrobku. Rovněž doporučujeme heslo pravidelně obnovovat, obzvláště v systému s vysokým zabezpečením může měsíční nebo týdenní obnovování hesla lépe chránit váš výrobek.

4. Kliknutím na tlačítko OK uložte heslo.

Dokončení aktivace můžete zkontrolovat v místním okně. Pokud se aktivace nezdařila, ujistěte se, že heslo splňuje požadavky, a zkuste to znovu.

5. Změňte IP adresu zařízení na stejnou podsíť jako váš počítač buď ruční změnou IP adresy, nebo zaškrtnutím políčka Enable DHCP (Povolit DHCP).

Modify Network Parameters

IP Address: 192.168.1.64

Port: 8000

Subnet Mask: 255.255.255.0

IPv4 Gateway: 192.168.1.1

IPv6 Address: ::

IPv6 Gateway: ::

IPv6 Prefix Length: 0

HTTP Port: 80

Device Serial No.: XX-XXXXXXXX-XXXXXXXX

Enable DHCP

Password Save

Figure 1-5 Změna IP adresy

6. Zadejte heslo a kliknutím na tlačítko **Save** (Uložit) aktivujte změnu IP adresy.

❖ Aktivace prostřednictvím klientského softwaru

Klientský software je všestranný software pro správu videa pro různé druhy zařízení. Klientský software vyhledejte na dodávaném disku nebo oficiálních webových stránkách a proveďte jeho instalaci dle pokynů. Aktivujte kameru podle následujícího postupu.

Postup:

1. Spusťte klientský software a zobrazí se ovládací panel softwaru, viz obrázek níže.

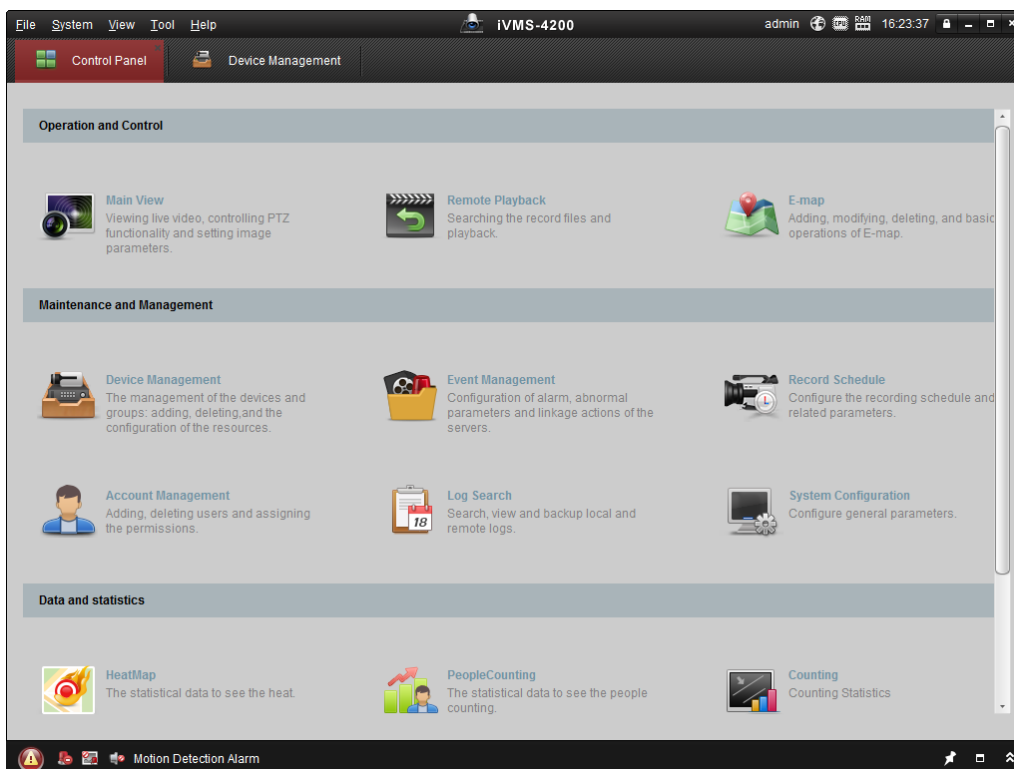


Figure 1-6 Ovládací panel

2. Kliknutím na ikonu **Device Management** (Správa zařízení) vstoupíte do rozhraní správy zařízení, viz obrázek níže.

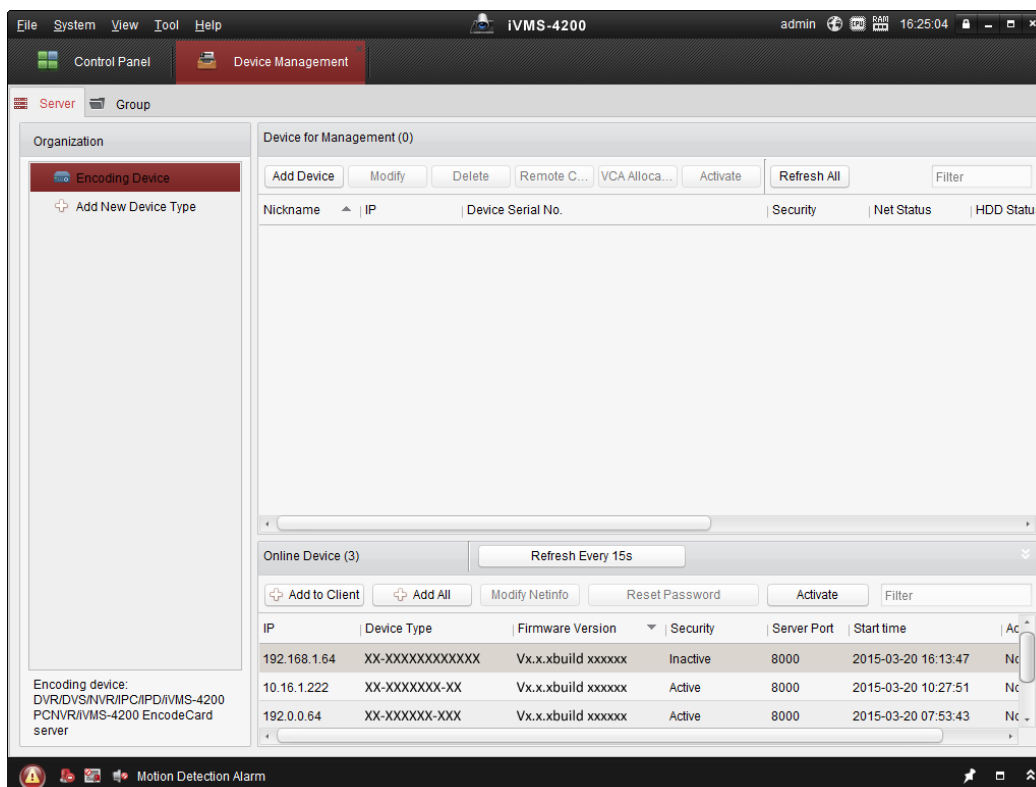


Figure 1-7 Rozhraní správy zařízení

3. Zkontrolujte stav zařízení v seznamu zařízení a vyberte neaktivní zařízení.
4. Klikněte na tlačítko **Activate** (Aktivovat) a zobrazí se rozhraní pro aktivaci.
5. Vytvořte heslo, zadejte ho do pole hesla a potvrďte ho.



DOPORUČUJEME POUŽÍT SILNÉ HESLO – důrazně doporučujeme, abyste vytvořili silné heslo dle vlastního výběru (o délce alespoň 8 znaků, s velkými písmeny, malými písmeny, čísly a speciálními znaky), abyste zvýšili zabezpečení výrobku. Doporučujeme heslo pravidelně obnovovat, obzvláště v systému s vysokým zabezpečením může měsíční nebo týdenní obnovování hesla lépe chránit váš výrobek.

Figure 1-8 Rozhraní pro aktivaci (klientský software)

6. Kliknutím na tlačítko **OK** zahajte aktivaci.
7. Klikněte na tlačítko **Modify Netinfo** (Upravit informace o síti) a zobrazí se rozhraní úpravy parametrů sítě, viz obrázek níže.

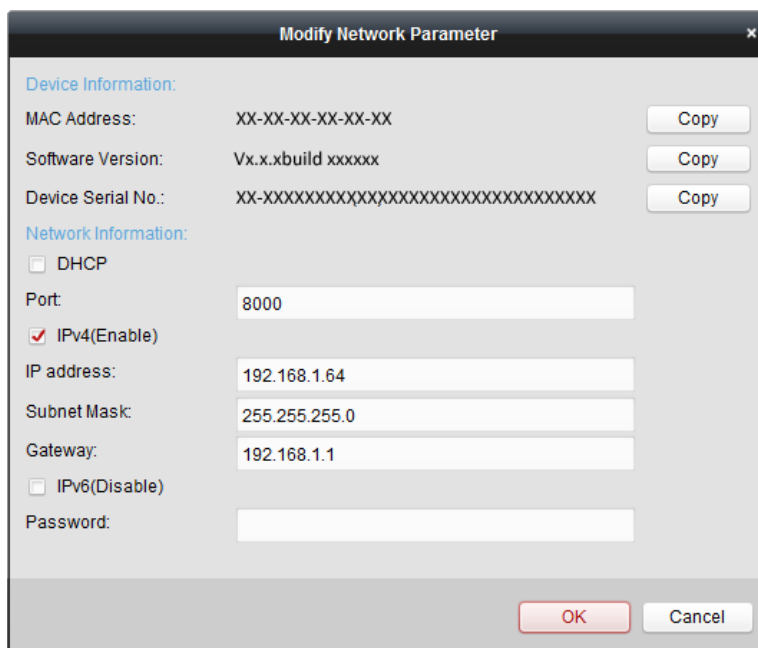


Figure 1-9 Úpravy parametrů sítě

8. Změňte IP adresu zařízení na stejnou podsíť jako váš počítač buď ruční změnou IP adresy, nebo zaškrtnutím políčka Enable DHCP (Povolit DHCP).
9. Zadejte heslo, aby se úprava IP adresy aktivovala.

1.2 Nastavení síťové kamery přes síť WAN

Účel:

Tato část popisuje, jak připojit síťovou kameru k síti WAN se statickou nebo dynamickou IP adresou.

1.2.1 Připojení se statickou IP adresou

Než začnete:

Použijte statickou IP adresu od poskytovatele připojení k internetu. Se statickou IP adresou můžete připojit síťovou kameru prostřednictvím směrovače, nebo přímo k síti WAN.

- **Připojení síťové kamery prostřednictvím směrovače**

Postup:

1. Připojte síťovou kameru ke směrovači.

2. Přiřaďte IP adresu v síti LAN, masku podsítě a bránu. Podrobný popis konfigurace IP adresy síťové kamery je uveden v části 2.1.2.
3. Uložte statickou IP adresu ve směrovači.
4. Nastavte mapování portů, např. porty 80, 8000 a 554. Postup mapování portů se u různých směrovačů liší. O pomoc s mapováním portů požádejte výrobce směrovače.

Poznámka: Podrobné informace o mapování portů jsou uvedeny v Příloze 2.

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

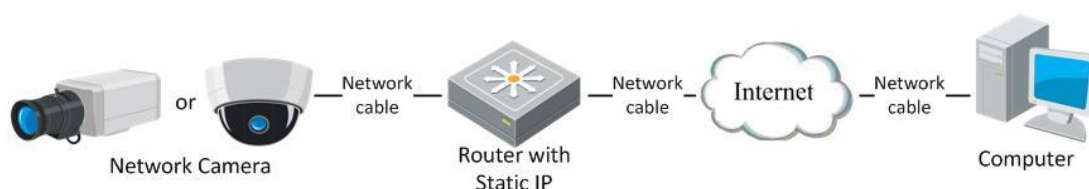


Figure 1-10 Přístup ke kameře prostřednictvím směrovače se statickou IP adresou

- **Přímé připojení síťové kamery se statickou IP adresou**

Můžete také uložit statickou IP adresu do kamery a přímo ji připojit k internetu bez použití směrovače. Podrobný popis konfigurace IP adresy síťové kamery je uveden v části 2.1.2.

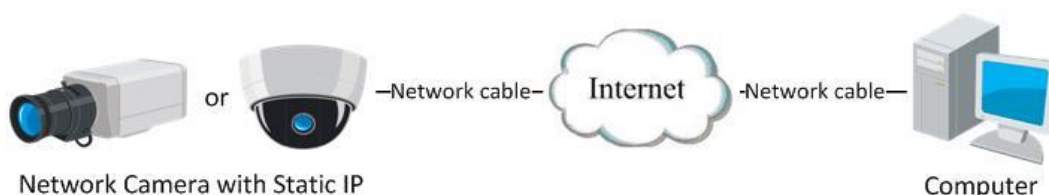


Figure 1-11 Přímý přístup ke kameře se statickou IP adresou

1.2.2 Připojení s dynamickou IP adresou

Než začnete:

Použijte dynamickou IP adresu od poskytovatele připojení k internetu. S dynamickou IP adresou můžete připojit síťovou kameru k modemu nebo směrovači.

- **Připojení síťové kamery prostřednictvím směrovače**

Postup:

1. Připojte síťovou kameru ke směrovači.
2. V kameře přiřaďte IP adresu v síti LAN, masku podsítě a bránu. Podrobný popis konfigurace IP adresy síťové kamery je uveden v části 2.1.2.
3. Ve směrovači nastavte uživatelské jméno PPPoE, heslo a potvrzené heslo.
4. Nastavte mapování portů. Např. porty 80, 8000 a 554. Postup mapování portů se u různých směrovačů liší. O pomoc s mapováním portů požádejte výrobce směrovače.

Poznámka: Podrobné informace o mapování portů jsou uvedeny v Příloze 2.

5. Použijte název domény od poskytovatele názvů domén.
6. Nakonfigurujte nastavení DDNS v nastavení směrovače.
7. Navštivte kameru pomocí použitého názvu domény.

● Připojení síťové kamery prostřednictvím modemu

Účel:

Tato kamera podporuje funkci automatického vytáčení PPPoE. Kamera obdrží veřejnou IP adresu prostřednictvím vytáčeného připojení ADSL po jejím připojení k modemu. Je třeba nakonfigurovat parametry PPPoE síťové kamery. Podrobnosti o konfiguraci jsou uvedeny v části 6.3.3 **Konfigurace nastavení PPPoE**.

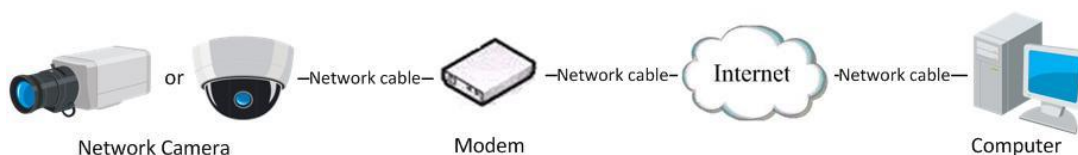


Figure 1-12 Přístup ke kameře s dynamickou IP adresou

Poznámka: Obdržená IP adresa je dynamicky přidělena prostřednictvím PPPoE, takže IP adresa se po restartování kamery vždy změní. Pro vyřešení nepohodlí dynamické IP adresy je třeba obdržet název domény od poskytovatele DDNS (např. DynDns.com). Pokud chcete problém vyřešit, použijte následující postup pro rozlišení normálního a privátního názvu domény

- ◆ Rozlišení normálního názvu domény

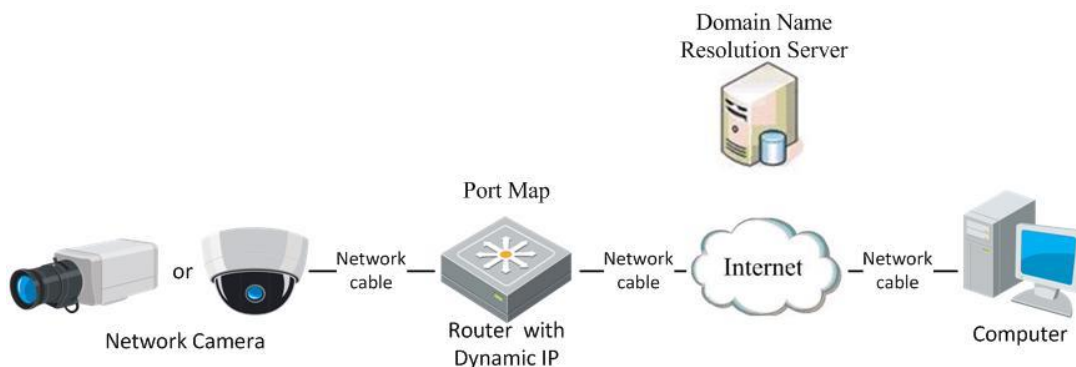


Figure 1-13 Rozlišení normálního názvu domény

Postup:

1. Použijte název domény od poskytovatele názvů domén.
2. Nakonfigurujte nastavení DDNS v rozhraní **DDNS Settings** (Nastavení DDNS) síťové kamery. Podrobnosti o konfiguraci jsou uvedeny v části **6.3.4 Konfigurace nastavení DDNS**.
3. Navštivte kameru pomocí použitého názvu domény.

◆ Rozlišení privátního názvu domény

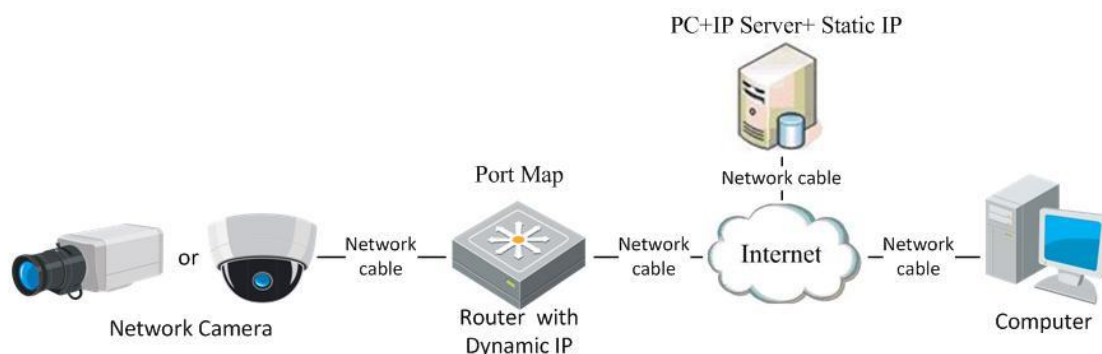


Figure 1-14 Rozlišení privátního názvu domény

Postup:

1. Nainstalujte a spusťte software IP server do počítače se statickou IP adresou.
2. Připojte se k síťové kameře přes síť LAN pomocí webového prohlížeče nebo klientského softwaru.
3. Povolte funkci DDNS a jako typ protokolu vyberte IP Server. Podrobnosti o konfiguraci jsou uvedeny v části **6.3.4 Konfigurace nastavení DDNS**.

Chapter 2 Přístup k síťové kameře

2.1 Přístup přes webové prohlížeče

Postup:

1. Otevřete webový prohlížeč.
2. Chcete-li zobrazit přihlašovací obrazovku, do adresního řádku prohlížeče zadejte IP adresu síťové kamery a pak stiskněte klávesu **Enter**.
3. Aktivujte síťovou kameru pro první použití, podrobnosti najdete v části 2.1.2.

Poznámka:

- Výchozí IP adresa je 192.168.1.64.
 - Pokud kamera není aktivovaná, aktivujte ji dle kapitoly 3.1 nebo kapitoly 3.2.
4. V pravém horním rohu rozhraní pro přihlášení vyberte jako jazyk rozhraní možnost English (Angličtina).

5. Zadejte uživatelské jméno a heslo a klikněte na .

Administrátor by měl řádně nakonfigurovat účty zařízení a oprávnění uživatelů/operátorů. Odstraňte zbytečné účty a oprávnění uživatelů/operátorů.

Poznámka:

Pokud administrátor provede 7 chybných pokusů o zadání hesla (5 pokusů v případě hosta/operátora), IP adresa zařízení se uzamkne.

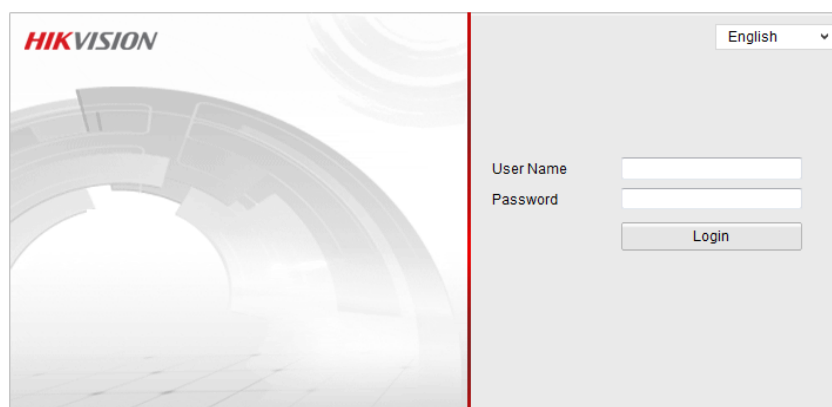


Figure 2-1 Přihlašovací obrazovka

6. Před zobrazením živého videa a ovládáním kamery nainstalujte modul plug-in.

Postup instalace modulu proveďte podle pokynů pro instalaci.

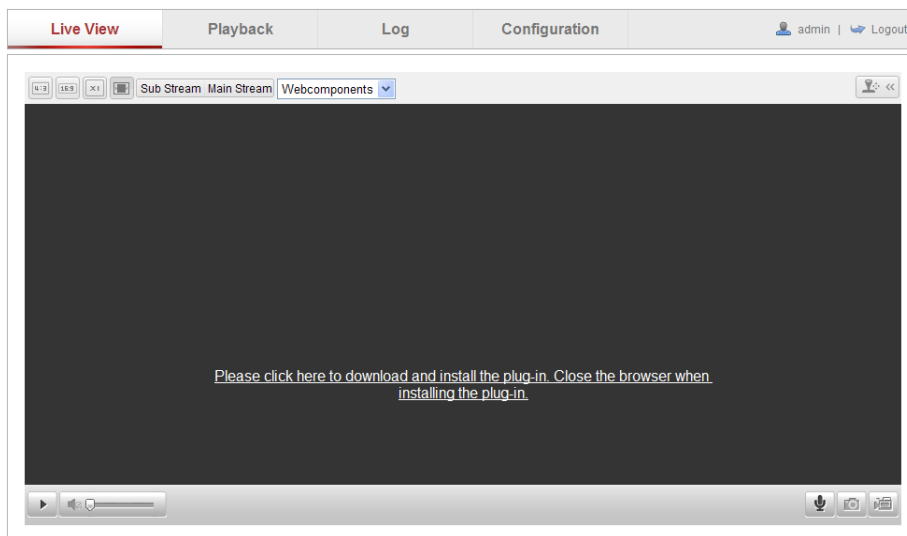


Figure 2-2 Stažení a instalace modulu plug-in

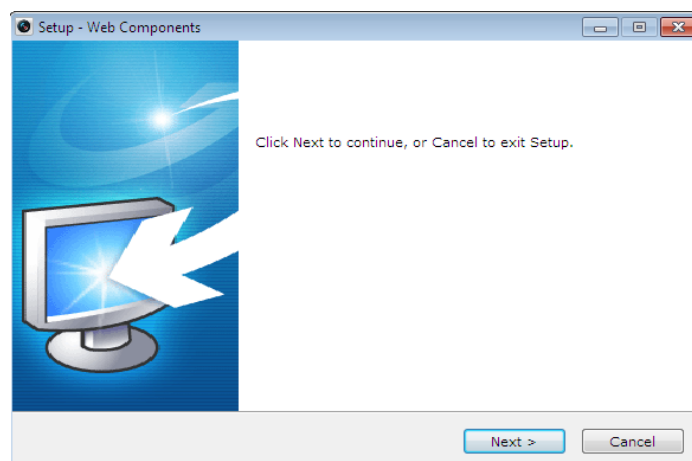


Figure 2-3 Instalace modulu plug-in (1)

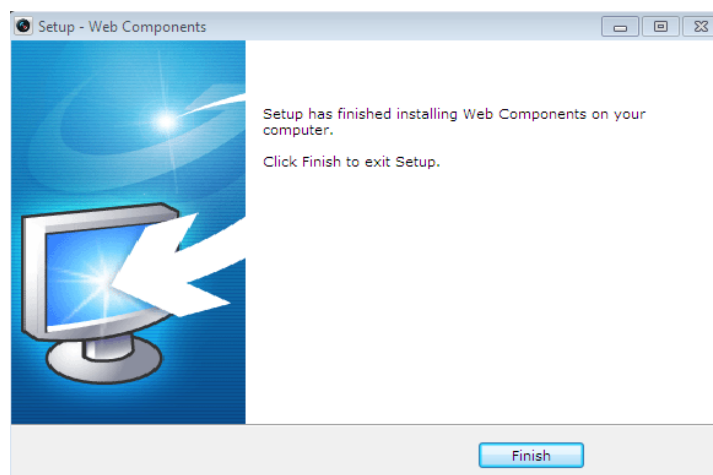


Figure 2-4 Instalace modulu plug-in (2)

Poznámka: Před instalací modulu plug-in může být nutné ukončit webový prohlížeč.

Po instalaci webový prohlížeč znovu spustíte a opět se přihlaste.

2.2 Přístup prostřednictvím klientského softwaru

Disk CD k výrobku obsahuje klientský software iVMS-4200. S pomocí tohoto softwaru můžete sledovat živé video a spravovat kameru.

Software nainstalujte podle pokynů pro instalaci. Ovládací panel a rozhraní živého náhledu klientského softwaru iVMS-4200 vypadá následovně.

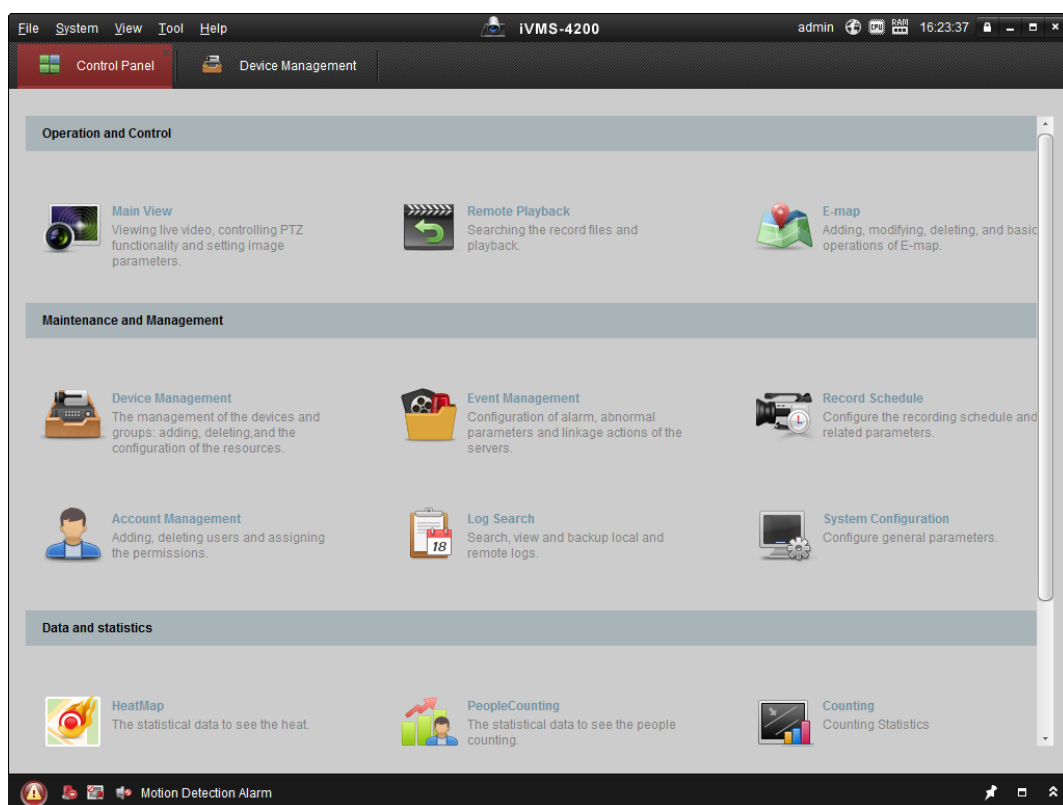


Figure 2-5 Ovládací panel softwaru iVMS-4200

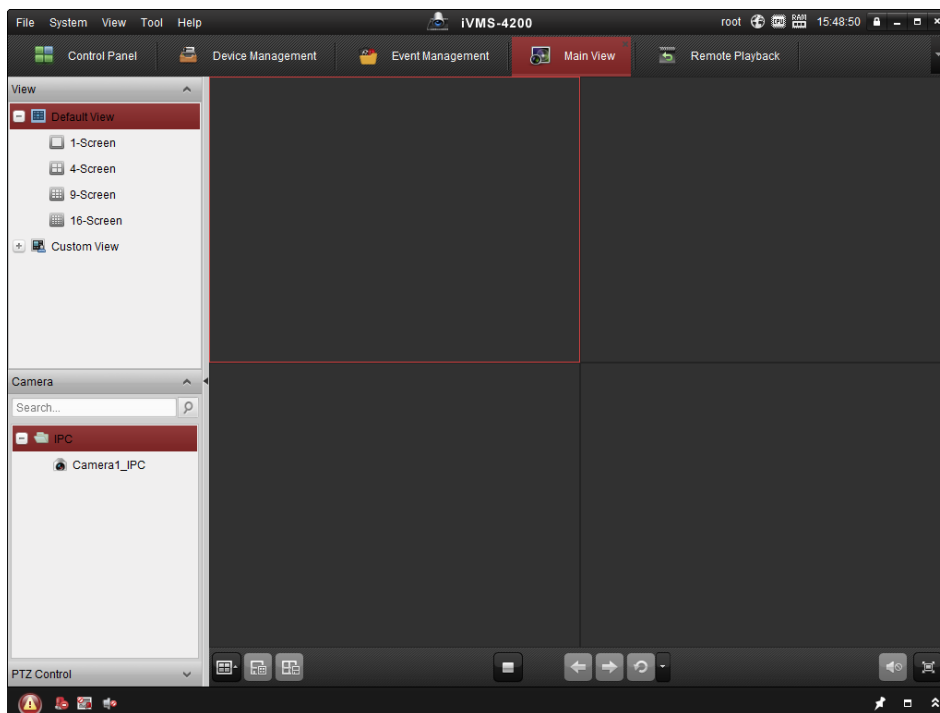


Figure 2-6 Hlavní zobrazení softwaru iVMS-4200

Poznámka: Podrobné informace o softwaru jsou uvedeny v uživatelské příručce softwaru iVMS-4200.

Chapter 3 Nastavení Wi-Fi

Účel:

V případě připojení k bezdrátové síti není pro připojení k síti zapotřebí použít jakýkoli druh kabelů, což je pro reálné využití kamerového systému velmi praktické.

Poznámka: Tato kapitola se vztahuje pouze ke kamerám s vestavěným modulem Wi-Fi.

3.1 Konfigurace připojení Wi-Fi ve režimech Manage a Ad-hoc

Než začnete:

Musí být nakonfigurovaná bezdrátová síť.

Bezdrátové připojení v režimu Manage

Postup:

1. Vstupte do rozhraní konfigurace Wi-Fi.

Configuration (Konfigurace) > Advanced Configuration (Rozšířená konfigurace) > Network (Síť) > Wi-Fi

Wireless List							Search
No.	SSID	Working Mode	Security Mode	Channel	Signal Strength	Speed(Mbps)	
1	belkin54g	infrastructure	NONE	1	94	54	▲
2	Roy Zhong	infrastructure	WPA2-personal	1	78	54	☰
3	yourPC	infrastructure	WPA2-personal	11	37	150	
4	Micheal	infrastructure	WPA2-personal	6	31	150	
5	APPLE	infrastructure	WPA2-personal	6	31	150	▼

Figure 3-1 Seznam bezdrátových sítí

2. Kliknutím na tlačítko **Search** (Hledat) vyhledejte bezdrátová připojení online.
3. Kliknutím vyberte bezdrátové připojení v seznamu.

Wi-Fi	
SSID	<input type="text" value="belkin54g"/>
Network Mode	<input checked="" type="radio"/> Manager <input type="radio"/> Ad-Hoc
Security Mode	<input type="text" value="not-encrypted"/>

Figure 3-2 Nastavení Wi-Fi - režim Manage

4. Zaškrtnutím políčka vyberte *Network mode* (Režim sítě) *Manage* a po výběru bezdrátové sítě se automaticky zobrazí *Security mode* (Režim zabezpečení) sítě. Neměňte ho ručně.

Poznámka: Tyto parametry jsou přesně shodné s parametry směrovače.

5. Zadejte klíč pro připojení k bezdrátové síti. Mělo by se jednat o klíč bezdrátového připojení k síti, který jste nastavili na směrovači.

Bezdrátové připojení v režimu Ad-hoc

Pokud zvolíte režim Ad-hoc, nemusíte připojovat bezdrátovou kameru pomocí směrovače. Situace je stejná jako v případě připojení kamery k počítači přímo pomocí síťového kabelu.

Postup:

1. Vyberte režim Ad-hoc.

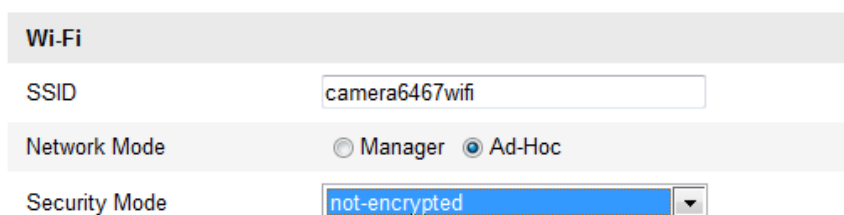


Figure 3-3 Nastavení Wi-Fi - režim Ad-hoc

2. Upravte název SSID pro kameru.
3. Vyberte režim zabezpečení bezdrátového připojení.

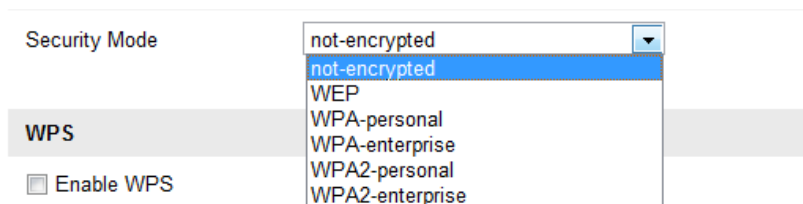


Figure 3-4 Režim zabezpečení - režim Ad-hoc

4. Povolte funkci bezdrátového připojení pro váš počítač.
5. Na straně počítače vyhledejte síť a v seznamu uvidíte název SSID kamery.



Figure 3-5 Bod připojení Ad-hoc

6. Vyberte název SSID a připojte se.

Popis režimu zabezpečení:

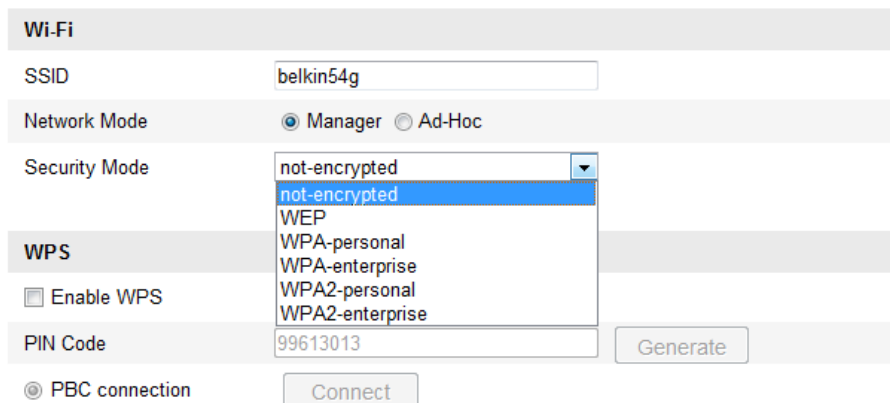


Figure 3-6 Režim zabezpečení:

Můžete zvolit z následujících režimů zabezpečení: nešifrované, WEP, WPA-personal, WPA-enterprise, WPA2-personal, a WPA2-enterprise.

Režim WEP:

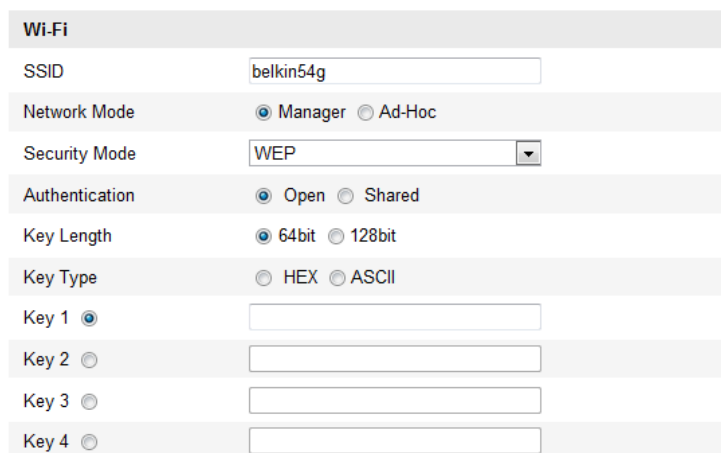


Figure 3-7 Režim WEP

- Authentication (*Ověření*) - vyberte z možností Open (Otevřené) nebo Shared Key

(Sdílený klíč), v závislosti na metodě používané vaším přístupovým bodem. Ne všechny přístupové body mají tuto možnost; v takovém případě pravděpodobně používají otevřený systém, který je někdy označován jako ověřování SSID.

- *Key length (Délka klíče)* - nastavuje délku klíče použitého k šifrování bezdrátové komunikace, 64 nebo 128 bitů. Délka šifrovacího klíče může být někdy zobrazena jako 40/64 a 104/128.
- *Key type (Druh klíče)* - dostupné druhy klíčů závisí na používaném přístupovém bodu. K dispozici jsou následující možnosti:

HEX - umožňuje ručně zadat hexadecimální klíč.

ASCII - při této metodě musí mít řetězec délku přesně 5 znaků v případě 64bitového šifrování WEP a 13 znaků v případě 128bitového šifrování WEP.

Režimy WPA-personal a WPA2-personal:

Zadejte požadovaný předsdílený klíč pro přístupový bod, což může být hexadecimální číslo nebo heslo.

Wi-Fi	
SSID	<input type="text" value="belkin54g"/>
Network Mode	<input checked="" type="radio"/> Manager <input type="radio"/> Ad-Hoc
Security Mode	<input type="text" value="WPA-personal"/>
Encryption Type	<input type="text" value="TKIP"/>
Key 1 <input checked="" type="radio"/>	<input type="text"/>

Figure 3-8 Režim zabezpečení - WPA-personal

Režimy WPA-enterprise a WPA2-enterprise :

Vyberte typ ověřování klient/server používaný přístupovým bodem; EAP-TLS nebo EAP-PEAP.

EAP-TLS

Wi-Fi	
SSID	<input type="text" value="test"/>
Network Mode	<input checked="" type="radio"/> Manager <input type="radio"/> Ad-Hoc
Security Mode	<input type="text" value="WPA-enterprise"/>
Authentication	<input type="text" value="EAP-TLS"/>
Identify	<input type="text"/>
Private key password	<input type="text"/>
EAPOL version	<input type="text" value="1"/>
CA certificate	<input type="text"/> <input type="button" value="Browse"/> <input type="button" value="Upload"/>
User certificate	<input type="text"/> <input type="button" value="Browse"/> <input type="button" value="Upload"/>
Private key	<input type="text"/> <input type="button" value="Browse"/> <input type="button" value="Upload"/>

Figure 3-9 EAP-TLS

- Identity (Identita) – zadejte ID uživatele, které bude předloženo síti.
- Private key password (Heslo privátního klíče) – zadejte heslo pro vaše ID uživatele.
- EAPOL version (Verze EAPOL) – vyberte verzi (1 nebo 2) používanou ve vašem přístupovém bodě.
- CA Certificates (Certifikáty CA) – odešlete certifikát CA, který bude předložen přístupovému bodu k ověření.

EAP-PEAP:

- User Name (Uživatelské jméno) – zadejte uživatelské jméno, které bude předloženo síti
- Password (Heslo) – zadejte heslo sítě
- PEAP Version (Verze PEAP) – vyberte verzi PEAP používanou v přístupovém bodě.
- Label (Štítek) – vyberte štítek používaný přístupovým bodem.
- EAPOL version (Verze EAPOL) – vyberte verzi (1 nebo 2) používanou ve vašem přístupovém bodě
- CA Certificates (Certifikáty CA) – odešlete certifikát CA, který bude předložen přístupovému bodu k ověření.



- *Pro vaše soukromí a lepší ochranu vašeho systému před bezpečnostními riziky důrazně doporučujeme používat pro všechny funkce a síťová zařízení silná hesla. Heslo by mělo být vytvořeno dle vašeho vlastního výběru (o délce alespoň 8 znaků, s velkými písmeny, malými písmeny, čísly a speciálními znaky), abyste zvýšili zabezpečení výrobku.*
- *Za řádnou konfiguraci veškerých hesel a dalších nastavení zabezpečí ručí osoba provádějící instalaci a/nebo koncový uživatel.*

3.2 Jednoduché připojení k sítí Wi-Fi pomocí funkce WPS

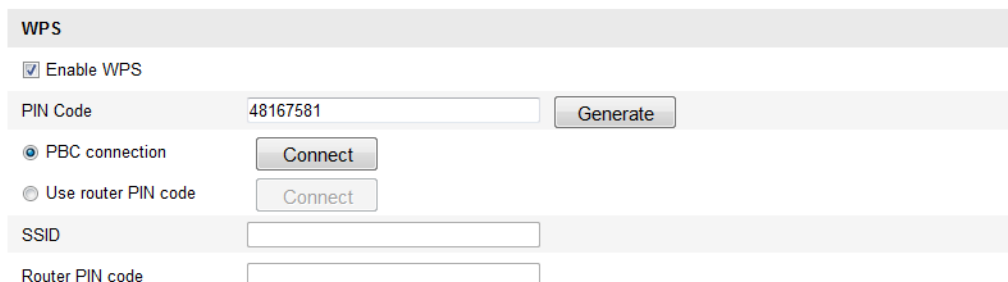
Účel:

Nastavení připojení k bezdrátové síti nikdy není snadné. Abyste se vyhnuli složitému nastavení bezdrátového připojení, můžete povolit funkci WPS.

WPS (Wi-Fi Protected Setup) označuje jednoduchou konfiguraci šifrovaného spojení mezi zařízením a bezdrátovým směrovačem. Funkce WPS umožňuje snadné přidávání nových zařízení do stávající sítě bez zadávání dlouhých hesel. Připojení WPS funguje ve dvou režimech, v režimu PBC a v režimu PIN.

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

Postup:

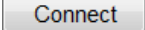


WPS	
<input checked="" type="checkbox"/> Enable WPS	
PIN Code	48167581 <input type="button" value="Generate"/>
<input checked="" type="radio"/> PBC connection	<input type="button" value="Connect"/>
<input type="radio"/> Use router PIN code	<input type="button" value="Connect"/>
SSID	<input type="text"/>
Router PIN code	<input type="text"/>

Figure 3-10 Nastavení Wi-Fi – WPS

Režim PBC:

PBC označuje funkci Push-Button-Configuration (Konfigurace stiskem tlačítka), při které stačí jen stisknout tlačítko, buď skutečné, nebo virtuální (jako tlačítko

 v rozhraní konfigurace prohlížeče IE), jak na přístupovém bodě (a registrátoru sítě), tak na novém bezdrátovém klientském zařízení.

1. Funkci WPS povolíte zaškrtnutím políčka Enable WPS .
2. Vyberte režim připojení PBC.



Poznámka: Podpora tohoto režimu je povinná na přístupovém bodě i na připojících se zařízeních.

3. Prohlédněte váš Wi-Fi směrovač, zda se na něm nachází tlačítko WPS. Pokud ano, stiskněte ho a indikátor v blízkosti tlačítka začne blikat, což znamená, že funkce WPS na směrovači je aktivovaná. Podrobný popis obsluhy najdete v uživatelské příručce ke směrovači.

4. Stisknutím tlačítka WPS aktivujte funkci na kameře.

Pokud na kameře tlačítko WPS není, můžete rovněž kliknout na virtuální tlačítko a aktivovat funkci PBC ve webovém rozhraní

5. Klikněte na tlačítko **Connect** (Připojit).



Když je režim PBC aktivovaný na směrovači i na kameře, kamera a bezdrátová síť se propojí automaticky.

Režim PIN:

Režim PIN vyžaduje přečtení osobního identifikačního čísla PIN (Personal Identification Number) buď ze štítku nebo z displeje na bezdrátovém zařízení. Tento kód PIN je poté třeba zadat pro připojení k síti, obvykle k přístupovému bodu sítě.

Postup:

1. Vyberte bezdrátové připojení v seznamu a zobrazí se název SSID.

The screenshot shows a 'Wireless List' table with the following data:

No.	SSID	Working Mode	Security Mode	Channel	Signal Strength	Speed(Mbps)
10	AP	infrastructure	WPA2-personal	11	13	54
11	Webber	infrastructure	WPA2-personal	11	7	54
12	TP-LINK_PocketAP_DFB048	infrastructure	WPA2-personal	6	7	150
13	AP1	infrastructure	WPA2-personal	11	0	150
14	TP-LINK_PocketAP_C4C218	infrastructure	NONE	6	0	150

Below the table are configuration sections for Wi-Fi and WPS. The Wi-Fi section includes fields for SSID (AP), Network Mode (Manager selected), Security Mode (WPA2-personal), Encryption Type (TKIP), and Key 1. The WPS section includes a checked 'Enable WPS' checkbox, a PIN Code field (48167581) with a 'Generate' button, and radio buttons for 'PBC connection' and 'Use router PIN code' (selected), each with a 'Connect' button. There is also an SSID field (AP) and a Router PIN code field.

Figure 3-11 Nastavení Wi-Fi – WPS, režim PIN

2. Vyberte možnost **Use router PIN code** (Použití kódu PIN směrovače). Pokud je kód PIN vygenerovaný ze strany směrovače, měli byste zadat kód ze směrovače do pole **Router PIN code** (Kód PIN směrovače).
3. Klikněte na tlačítko **Connect** (Připojit).
nebo
Můžete vygenerovat kód PIN na straně kamery. Doba vypršení kódu PIN je 120 sekund.
1. Klikněte na tlačítko **Generate** (Vygenerovat).

A close-up of the WPS configuration section showing the 'PIN Code' field containing '48167581' and a 'Generate' button.

2. Zadejte kód PIN do směrovače, v uvedeném příkladu byste do směrovače zadali kód 48167581.

3.3 Nastavení vlastnosti IP adresy pro připojení k bezdrátové síti

Výchozí adresa řadiče rozhraní bezdrátové sítě je 192.168.1.64. Když se připojíte k bezdrátové síti, výchozí IP adresu můžete změnit.

Postup:

1. Vstupte do rozhraní konfigurace TCP/IP.

Configuration (Konfigurace) > Advanced Configuration (Rozšířená konfigurace) >

Network (Síť) > TCP/IP

nebo

Configuration (Konfigurace) > Basic Configuration (Základní konfigurace) >

Network (Síť) > TCP/IP

The screenshot shows a web-based configuration interface for TCP/IP settings. At the top, there are several tabs: TCP/IP (selected), Port, DDNS, PPPoE, SNMP, QoS, FTP, and Wi-Fi. Below the tabs is a section titled "NIC Settings". It contains the following fields:

- Select NIC: wlan (dropdown menu)
- IPv4 Address: 172.6.21.124
- IPv4 Subnet Mask: 255.255.255.0
- IPv4 Default Gateway: 172.6.21.1
- DHCP: (unchecked)
- Multicast Address: (empty text box)

Figure 3-12 Nastavení TCP/IP

2. Vyberte kartu síťového rozhraní wlan.
3. Upravte adresu IPv4, masku podsítě IPv4 a výchozí bránu.

Postup nastavení je stejný jako v případě sítě LAN.

Pokud chcete nechat přiřadit IP adresu, můžete zaškrtnout políčko pro povolení

DHCP.

Chapter 4 Živý náhled

4.1 Stránka živého náhledu

Účel:

Stránka živého náhledu umožňuje sledovat video v reálném čase, zachytávat snímky, provádět ovládání PTZ, nastavovat/vyvolávat předvolby a konfigurovat parametry videa.

Přihlaste se k síťové kameře a vstupte na stránku živého náhledu nebo klikněte na tlačítko **Live View** (Živý náhled) v panelu nabídky hlavní stránky a vstupte na stránku živého náhledu.

Popis stránky živého náhledu:

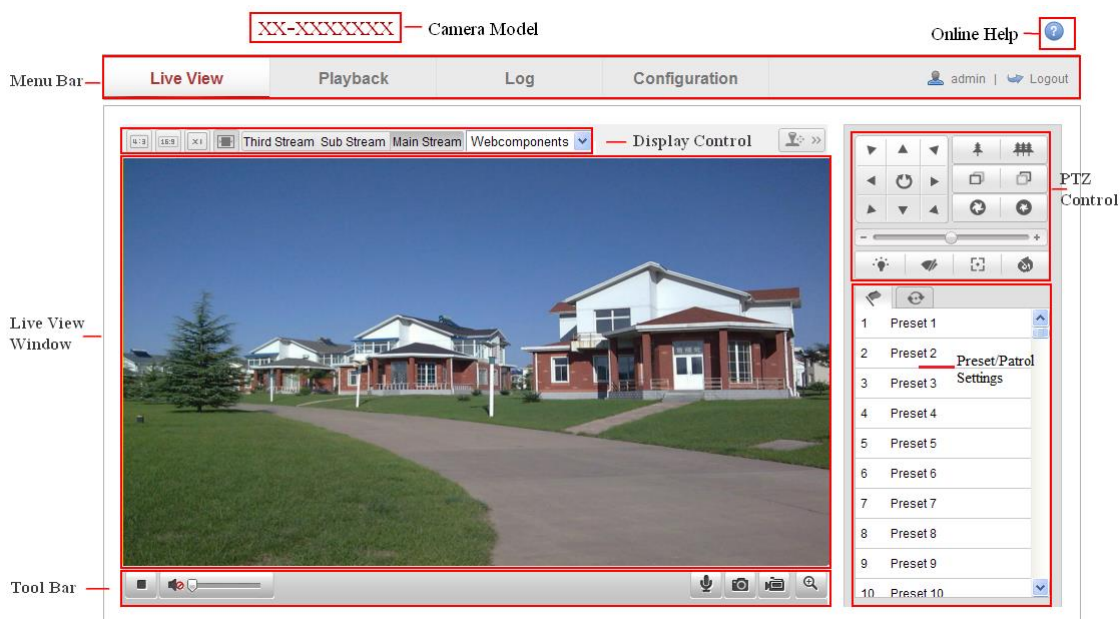



Figure 4-1 Stránka živého náhledu

Model kamery:

Uvádí model kamery, ke které jste připojeni.

Nápověda online:

Kliknutím na ikonu  získáte nápovědu online, která vás provede základní obsluhou jednotlivých funkcí

Panel nabídky:

Kliknutím na jednotlivé karty přejdete na stránku živého náhledu, přehrávání, protokolu a konfigurace.

Ovládní izobrazení

Po kliknutí na jednotlivé stránky můžete upravit rozvržení a typ streamu živého zobrazení. Po kliknutí na rozevírací nabídku můžete vybrat modul plug-in pro uživatele aplikace Internet Explorer, vybírat lze z možností Webcomponents a QuickTime. Pro uživatele jiných prohlížečů lze vybrat z možností Webcomponents, QuickTime, VLC nebo MJPEG, pokud jsou webovým prohlížečem podporovány.

Okno živého náhledu:

Zobrazení živého videa.

Panel nástrojů:

Ovládní na stránce živého náhledu, např. živý náhled, snímání, záznam, zapnutí/vypnutí zvuku, obousměrný zvuk atd.

Ovládní IPTZ:

Funkce posunu, nánklonu a zoomu kameru a ovládní světla a stěračce (k dispozici pouze u kamer s podporou funkce PTZ).

Nastavení předvolby/kontroly:

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

4.2 Spuštění živého náhledu














V okně živého náhledu, viz obr. 5-2, klikněte na ikonu  na panelu nástrojů a zobrazí se živý náhled kamery.



Figure 4-2 Panel nástrojů živého náhledu



Table 4-1 Popis panelu nástrojů

Ikona	Popis
	Spustit/zastavit živý náhled.
	Formát okna je 4:3.
	Formát okna je 16:9.
	Původní formát okna.

	Automatické přizpůsobení formátu okna.
Main Stream	Živý náhled s hlavním streamem.
Sub Stream	Živý náhled s vedlejším streamem.
Third Stream	Živý náhled s třetím streamem.
Webcomponents 	Kliknutím vyberte modul plug-in třetí strany.
	Manuální pořízení snímku.
	Manuální spuštění/zastavení záznamu.
	Zapnutí zvuku a nastavení hlasitosti / vypnutí
	Zapnutí/vypnutí mikrofону.
	Zapnutí/vypnutí funkce digitálního zoomu.
	Zapnutí/vypnutí funkce 3D nastavení polohy.

Poznámka: Funkce třetího streamu a 3D nastavení polohy vyžadují podporu kamery.

4.3 Manuální záznam a pořízování snímků

V rozhraní živého náhledu kliknutím na ikonu  na panelu nástrojů pořídíte snímek z živého videa a kliknutím na ikonu  spustíte záznam živého náhledu. Cesty ukládání pořízených snímků a klipů lze nastavit na stránce **Configuration (Konfigurace) > Local Configuration (Místní konfigurace)**. Pokud chcete nakonfigurovat vzdáleně plánovanou nahrávku postupujte podle *části 7.2*.

Poznámka: Pořízený snímek bude do počítače uložen ve formátu JPEG nebo BMP.



4.4 Obsluha ovládaní PTZ

Účel:

V rozhraní živého náhledu můžete použít tlačítka ovládaní PTZ k provádění funkcí posunu/náklonu/zoomu kamery.

Poznámka: K provádění ovládaní PTZ musí kamera připojená do sítě podporovat funkci PTZ nebo k ní musí být instalovaná jednotka pro posun/náklon. Řádně nastavte parametry PTZ na stránce nastavení rozhraní RS-485 dle *části 12.9 Nastavení rozhraní RS-485*.

4.4.1 Ovládací panel PTZ

Na stránce živého náhledu kliknutím na ikonu  zobrazíte ovládací panel PTZ nebo ho kliknutím na ikonu  skryjete.

Kliknutím na směrová tlačítka ovládejte pohyb posunu/náklonu.



Figure 4-3 Ovládací panel PTZ

Kliknutím na tlačítka zoomu/clony/ostření provádějte ovládání objektivu.

Poznámky:










- V okně živého náhledu se nachází 8 směrových šipek () , které umožňují pohyb v příslušném směru kliknutím a tažením myši.
- U kamer, které podporují pouze pohyb objektivu, jsou směrová tlačítka nefunkční.

Table 4-2 Popis ovládacího panelu PTZ

Ikona	Popis
	Přiblížení/oddálení
	Zaostření blíž/dál
	Clona +/-
	Zapnutí/vypnutí světla
	Zapnutí/vypnutí stěrače
	Pomocné zaostřování
	Inicializace objektivu
	Nastavení rychlosti pohybu posunu/náklonu

4.4.2 Nastavení/vyvolání předvolby

- **Nastavení předvolby:**

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

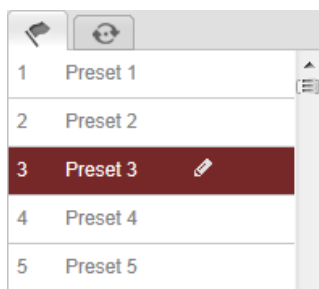




Figure 4-4 Nastavení předvolby


2. Pomocí ovládacích tlačítek PTZ přesuňte objektiv na požadovanou pozici.
 - Posouvejte kamerou doprava nebo doleva.
 - Nakloňte kameru nahoru nebo dolů.
 - Použijte přiblížení nebo oddálení.
 - Změňte zaostření objektivu.
3. Kliknutím na tlačítko  dokončete nastavení aktuální předvolby.
4. Můžete kliknout na tlačítko  a předvolbu odstranit.

Poznámka: Pro síťovou kameru Mini PT lze nakonfigurovat až 16 předvoleb.

● **Vyvolání předvolby:**

Tato funkce umožňuje ručně namířit kameru na specifikovaný záběr, když nastane nějaká událost.

Nadefinovanou předvolbu můžete kdykoli vyvolat a zabrat tak předem nastavenou scénu.

Na ovládacím panelu PTZ vyberte nadefinovanou předvolbu ze seznamu a kliknutím na tlačítko  ji vyvolejte.

Nebo můžete umístit myš do rozhraní předvoleb a vyvolat příslušnou předvolbu napsáním jejího čísla.

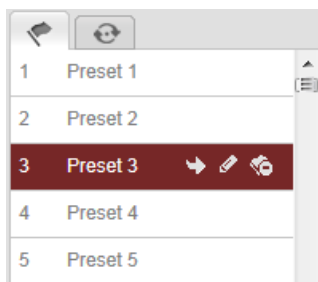




Figure 4-5 Vyvolání předvolby

4.4.3 Nastavení vyvolání kontroly

Poznámka:

Abyste mohli nastavit kontrolu, musí být nastaveny nejméně dvě předvolby.

Postup:

1. Kliknutím na ikonu  vstupte do rozhraní konfigurace kontroly.
2. Vyberte číslo trasy a kliknutím na tlačítko  přidejte nakonfigurované předvolby.
3. Vyberte předvolbu a zadejte dobu a rychlost kontroly.
4. Kliknutím na tlačítko OK uložte první předvolbu.
5. Pomocí výše uvedeného postupu přidejte další předvolby.

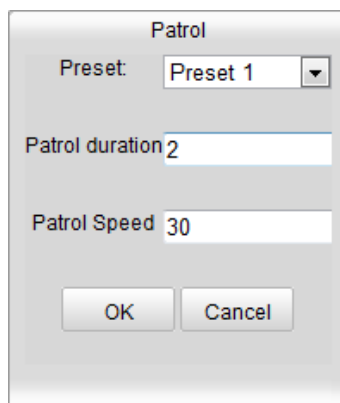






Figure 4-6 Přidání trasy kontroly

6. Kliknutím na tlačítko  kontrolu uložte.
7. Kliknutím na tlačítko  spustíte kontrolu a tlačítkem  ji zastavíte.
8. (Volitelné) Kliknutím na tlačítko  kontrolu odstraní.

Chapter 5 Konfigurace síťové kamery

5.1 Konfigurace místních parametrů

Poznámka: Místní konfigurace se vztahuje k parametrům živého náhledu, souborů záznamu a pořízených snímků. Soubory záznamu a pořízené snímky jsou soubory, které nahrajete nebo pořídíte pomocí webového prohlížeče, takže cesty k jejich uložení se nacházejí na počítači, na kterém je prohlížeč spuštěný.

Postup:

1. Vstupte do rozhraní místní konfigurace:

Configuration (Konfigurace) > Local Configuration (Místní konfigurace)

The screenshot shows the 'Local Configuration' web interface. It is divided into three main sections:

- Live View Parameters:**
 - Protocol: TCP, UDP, MULTICAST, HTTP
 - Live View Performance: Shortest Delay, Auto
 - Rules: Enable, Disable
 - Image Format: JPEG, BMP
- Record File Settings:**
 - Record File Size: 256M, 512M, 1G
 - Save record files to:
 - Save downloaded files to:
- Picture and Clip Settings:**
 - Save snapshots in live view to:
 - Save snapshots when playback to:
 - Save clips to:

A 'Save' button is located at the bottom right of the configuration area.

Figure 5-1 Rozhraní místní konfigurace

2. Nakonfigurujte následující nastavení
 - **Live View Parameters (Parametry živého náhledu):** Nastavte typ protokolu a výkon živého náhledu.
 - ◆ **Protocol Type (Typ protokolu):** Lze vybírat z možností TCP, UDP, MULTICAST a HTTP.

TCP: Zaručuje úplnou dodávku streamovaných dat a lepší kvalitu videa, bude však ovlivněn přenos v reálném čase.

UDP: Poskytuje audio a video streamy v reálném čase.

HTTP: Umožňuje stejnou kvalitu jako TCP bez nastavování konkrétních portů pro streaming v některých síťových prostředích.

MULTICAST (Vícesměrové vysílání): Při použití funkce vícesměrového vysílání je doporučeno vybrat typ MCAST. Podrobné informace o vícesměrovém vysílání jsou uvedeny v *části 6.3.1 Konfigurace nastavení TCP/IP*.

- ◆ **Live View Performance (Výkon živého náhledu):** Nastavte výkon živého náhledu Shortest Delay (Nejkratší zpoždění) nebo Auto (Automaticky).
- ◆ **Rules (Pravidla):** Označuje pravidla ve vašem místním prohlížeči. Výběrem možnosti Enable (Povolit) nebo Disable (Zakázat) zapnete nebo vypnete zobrazení barevných značek, když je aktivována detekce pohybu, detekce obličeje nebo detekce narušení. Např. pokud jsou pravidla povolena a rovněž je povolena detekce obličeje, v případě detekce bude obličej v živém náhledu označen zeleným obdélníkem.
- ◆ **Image Format (Formát obrázků):** Vyberte formát pořízených snímků.
- **Record File Settings (Nastavení souborů záznamu):** Nastavte cestu pro ukládání nahraných souborů videa. Platí pro soubory záznamů, které jste nahráli pomocí webového prohlížeče.
- ◆ **Record File Size (Velikost souborů záznamu):** Vyberte komprimovanou velikost manuálně nahrávaných a stahovaných souborů videa z možností 256M, 512M nebo 1G. Po výběru bude vybraná hodnota použita jako maximální velikost souborů záznamu.
- ◆ **Save record files to (Umístění uložených souborů záznamu):** Nastavte cestu pro ukládání manuálně nahraných souborů videa.
- ◆ **Save downloaded files to (Umístění stažených souborů):** Nastavte cestu pro ukládání stažených souborů videa v režimu přehrávání.
- **Picture and Clip Settings (Nastavení obrázků a klipů):** Nastavte cesty pro

ukládání pořízených snímků a oříznutých souborů videa. Platí pro obrázky, které jste pořídili pomocí webového prohlížeče.

- ◆ **Save snapshots in live view to (Umístění uložených snímků pořízených v živém náhledu):** Nastavte cestu pro ukládání snímků manuálně pořízených v režimu živého náhledu.
- ◆ **Save snapshots when playback to (Umístění uložených snímků pořízených při přehrávání):** Nastavte cestu pro ukládání snímků pořízených v režimu přehrávání.
- ◆ **Save clips to (Umístění uložených klipů):** Nastavte cestu pro ukládání oříznutých souborů videa v režimu přehrávání.

Poznámka: Můžete kliknout na tlačítko **Browse** (Procházet) a změnit adresář pro ukládání klipů a obrázků.

3. Uložte nastavení kliknutím na tlačítko Uložit.

5.2 Konfigurace nastavení času

Účel:

Pomocí pokynů v této části můžete nakonfigurovat nastavení synchronizace času a DTS.

Postup:

1. Vstupte do rozhraní nastavení času:

Configuration (Konfigurace) > Basic Configuration (Základní konfigurace)
> System (Systém) > Time Settings (Nastavení času)
nebo **Configuration (Konfigurace) > Advanced Configuration (Rozšířená konfigurace) > System (Systém) > Time Settings (Nastavení času)**

Figure 5-2 Nastavení času

- Vyberte časové pásmo.

Vyberte časové pásmo vaší lokality v rozevírací nabídce.

- ◆ Synchronizace času pomocí serveru NTP.

(1) Chcete-li zapnout funkci **NTP**, zaškrtněte příslušné políčko.

(2) Nakonfigurujte následující nastavení

Server Address (Adresa serveru): IP adresa serveru NTP.

NTP Port (Port NTP): Port serveru NTP.

Interval: Časový interval mezi dvěma synchronizacemi se serverem NTP.

Figure 5-3 Synchronizace času ze serveru NTP

Poznámka: Pokud je kamera připojená k veřejné síti, měli byste použít server NTP, který má funkci synchronizace času, jako je server organizace National Time Center (IP adresa: 210.72.145.44). Pokud je kamera instalovaná v přizpůsobené síti, lze použít software NTP k vytvoření serveru NTP pro synchronizaci času.

- ◆ Manuální synchronizace času

Povolte funkci **Manual Time Sync** (Manuální synchronizace času) a poté kliknutím

na tlačítko  nastavte systémový čas v zobrazeném kalendáři.

Poznámka: Rovněž můžete zaškrtnout políčko **Sync with computer time**

(Synchronizovat s časem počítače) a synchronizovat čas kamery s časem vašeho počítače.

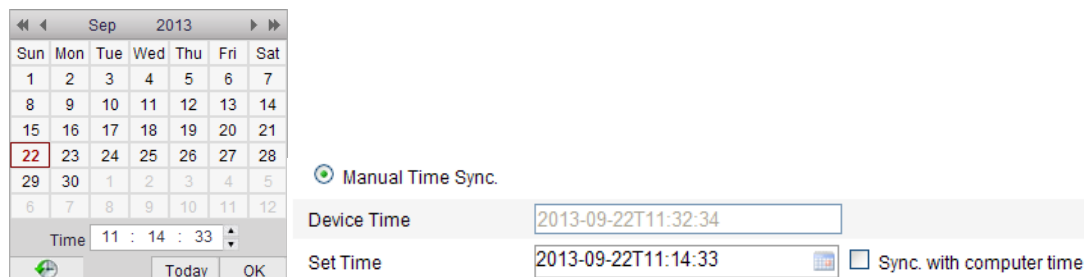


Figure 5-4 Manuální synchronizace času

- Klikněte na kartu **DST** a povolte funkci DST a nastavte čas pro období DST.

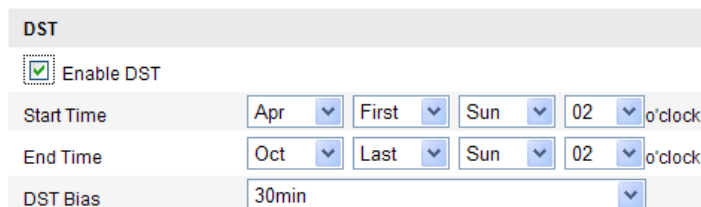


Figure 5-5 Nastavení DST

2. Uložte nastavení kliknutím na tlačítko **Uložit**.

5.3 Konfigurace nastavení sítě

5.3.1 Konfigurace nastavení TCP/IP

Účel:

Abyste mohli kameru ovládat po síti, musí být správně nakonfigurována nastavení TCP/IP. Kamera podporuje protokoly IPv4 i IPv6. Obě verze mohou být nakonfigurovány současně, aniž by tím došlo ke konfliktu, a měla by být nakonfigurována alespoň jedna verze protokolu IP.

Postup:

1. Vstupte do rozhraní nastavení TCP/IP.

Configuration (Konfigurace) > Basic Configuration (Základní konfigurace) > Network (Síť) > TCP/IP

nebo **Configuration (Konfigurace) > Advanced Configuration (Rozšířená konfigurace) > Network (Síť) > TCP/IP**

Figure 5-6 Nastavení TCP/IP

2. Nakonfigurujte základní nastavení sítě, jako typ karty síťového rozhraní, adresa IPv4 nebo IPv6, maska podsítě IPv4 nebo IPv6, výchozí brána IPv4 nebo IPv6, nastavení MTU a adresa vícesměrového vysílání.
3. (Volitelné) Pokud zaškrtnete políčko **Enable Multicast Discovery** (Povolit zjišťování vícesměrového vysílání) a síťovou kameru online bude možné automaticky detekovat v klientském softwaru prostřednictvím privátního protokolu vícesměrového vysílání v síti LAN.
4. Kliknutím na tlačítko **Save** (Uložit) uložíte výše uvedená nastavení.

Poznámky:

- Platný rozsah hodnot MTU je 1280 ~ 1500.
- Vícesměrové vysílání odesílá stream na skupinovou adresu vícesměrového vysílání a umožňuje více klientům přijímat stream ve stejném okamžiku požadavkem o kopii ze skupinové adresy vícesměrového vysílání. Před použitím této funkce je třeba povolit funkci vícesměrového vysílání vašeho směrovače.

- Aby se nastavení projevilo, je nutné provést restart.

5.3.2 Konfigurace nastavení portů

Účel:

Můžete nastavit číslo portu kamery, např. port HTTP, port RTSP a port HTTPS.

Postup:

1. Vstupte do rozhraní nastavení portů:

Configuration (Konfigurace) > Basic Configuration (Základní konfigurace) > Network (Síť) > Port

nebo **Configuration (Konfigurace) > Advanced Configuration (Rozšířená konfigurace) > Network (Síť) > Port**

HTTP Port	<input type="text" value="80"/>
RTSP Port	<input type="text" value="554"/>
HTTPS Port	<input type="text" value="443"/>
Server Port	<input type="text" value="8000"/>

Figure 5-7 Nastavení portů

2. Nastavte port HTTP, port RTSP, port HTTPS a port serveru kamery.

HTTP Port (Port HTTP): Výchozí číslo portu je 80 a lze je změnit na libovolné číslo portu, které není obsazené.

RTSP Port (Port RTSP): Výchozí číslo portu je 554 a lze je změnit na libovolné číslo portu, v rozmezí 1024 až 65 535.

HTTPS Port (Port HTTPS): Výchozí číslo portu je 443 a lze je změnit na libovolné číslo portu, které není obsazené.

Server Port (Port serveru): Výchozí číslo portu je 8 000 a lze je změnit na libovolné číslo portu, v rozmezí 2 000 až 65 535.

3. Uložte nastavení kliknutím na tlačítko **Uložit**.

Poznámka: Aby se nastavení projevilo, je nutné provést restart.

5.3.3 Konfigurace nastavení PPPoE

Postup:

1. Vstupte do rozhraní nastavení PPPoE:

Configuration (Konfigurace) > Advanced Configuration (Rozšířená konfigurace) > Network (Síť) > PPPoE

Figure 5-8 Nastavení PPPoE

2. Zaškrtnutím políčka **Enable PPPoE** (Povolit PPPoE) povolte tuto funkci.
3. Zadejte parametry **User Name** (Uživatelské jméno), **Password** (Heslo) a **Confirm** password (Potvrďte heslo) pro přístup pomocí PPPoE.

Poznámka: Uživatelské jméno a heslo by vám měl přidělit váš poskytovatel připojení k internetu.



- Pro vaše soukromí a lepší ochranu vašeho systému před bezpečnostními riziky důrazně doporučujeme používat pro všechny funkce a síťová zařízení silná hesla. Heslo by mělo být vytvořeno dle vašeho vlastního výběru (o délce alespoň 8 znaků, s velkými písmeny, malými písmeny, čísly a speciálními znaky), abyste zvýšili zabezpečení výrobku.
 - Za řádnou konfiguraci veškerých hesel a dalších nastavení zabezpečí ručí osoba provádějící instalaci a/nebo koncový uživatel.
4. Kliknutím na tlačítko **Save** (Uložit) uložíte nastavení a opustíte rozhraní.

Poznámka: Aby se nastavení projevilo, je nutné provést restart.

5.3.4 Konfigurace nastavení DDNS

Účel:

Pokud je vaše kamera nastavená na použití PPPoE jakožto výchozího síťového připojení, můžete pro přístup k síti použít službu DDNS (Dynamic DNS).

Než začnete:

Než nakonfigurujete nastavení DDNS kamery, je nutná registrace na serveru DDNS.



- *Pro vaše soukromí a lepší ochranu vašeho systému před bezpečnostními riziky důrazně doporučujeme používat pro všechny funkce a síťová zařízení silná hesla. Heslo by mělo být vytvořeno dle vašeho vlastního výběru (o délce alespoň 8 znaků, s velkými písmeny, malými písmeny, čísly a speciálními znaky), abyste zvýšili zabezpečení výrobku.*
- *Za řádnou konfiguraci veškerých hesel a dalších nastavení zabezpečí ručí osoba provádějící instalaci a/nebo koncový uživatel.*

Postup:

1. Vstupte do rozhraní nastavení DDNS:

Configuration (Konfigurace) > Advanced Configuration (Rozšířená konfigurace) > Network (Síť) > DDNS

<input checked="" type="checkbox"/>	Enable DDNS
DDNS Type	HiDDNS
Server Address	www.hik-online.com
Domain	431618683
Port	0
User Name	
Password	
Confirm	

Figure 5-9 Nastavení DDNS

2. Zaškrtnutím políčka **Enable DDNS** (Povolit DDNS) povolte tuto funkci.
3. Vyberte možnost **DDNS Type** (Typ DDNS). Lze vybírat ze čtyř typů DDNS: HiDDNS, IPServer, NO-IP a DynDNS.

- DynDNS:

Postup:

- (1) Zadejte **adresu serveru** DynDNS (např. members.dyndns.org).

- (2) Do textového pole Domain (Doména) zadejte název domény získané z webových stránek DynDNS.
- (3) Zadejte **port** serveru DynDNS.
- (4) Zadejte položky **User Name** (Uživatelské jméno) a **Password** (Heslo) zaregistrované na webových stránkách DynDNS.
- (5) Uložte nastavení kliknutím na tlačítko **Uložit**.

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

Figure 5-10 Nastavení DynDNS

- IP Server:

Postup:

- (1) Zadejte adresu IP serveru.
- (2) Uložte nastavení kliknutím na tlačítko **Uložit**.

Poznámka: V případě IP serveru je třeba použít statickou IP adresu, masku podsítě, bránu a upřednostňovaný server DNS od poskytovatele připojení k internetu. Jako **adresa serveru** by měla být zadána statická IP adresa počítače, na kterém je spuštěn software IP Server.

<input checked="" type="checkbox"/> Enable DDNS	
DDNS Type	IPServer
Server Address	212.15.10.121
Domain	
Port	0
User Name	
Password	
Confirm	

Figure 5-11 Nastavení IP Server

Poznámka: V oblasti USA a Kanady můžete jako adresu serveru zadat adresu 173.200.91.74.

- NO-IP:

Postup:

(1) Vyberte typ DDNS NO-IP.

<input checked="" type="checkbox"/> Enable DDNS	
DDNS Type	NO-IP
Server Address	
Domain	
Port	0
User Name	
Password	
Confirm	

Figure 5-12 Nastavení NO-IP

(2) Zadejte adresu serveru www.noip.com

(3) Zadejte název domény, který jste zaregistrovali.

(4) V případě potřeby zadejte číslo portu.

(5) Zadejte uživatelské jméno a heslo.

(6) Klikněte na tlačítko **Save** (Uložit) a poté můžete zobrazit kameru s pomocí názvu domény.

- HiDDNS

Postup:

(1) Vyberte typ DDNS HiDDNS.

<input checked="" type="checkbox"/> Enable DDNS	
DDNS Type	HiDDNS
Server Address	www.hik-online.com
Domain	431618683
Port	0
User Name	
Password	
Confirm	

Figure 5-13 Nastavení HiDDNS

(2) Zadejte adresu serveru www.hik-online.com.

(3) Zadejte název domény kamery. Doména je shodná s aliasem zařízení na serveru HiDDNS.

(4) Kliknutím na tlačítko **Save** (Uložit) uložte nová nastavení.

Poznámka: Aby se nastavení projevila, je nutné provést restart.

5.3.5 Konfigurace nastavení SNMP

Účel:

Můžete nastavit funkci SNMP, abyste mohli zjišťovat stav kamery, parametry a informace související s alarmy a vzdáleně spravovat kameru, když je připojena k síti.

Než začnete:

Před nastavením SNMP stáhněte software SNMP a nastavte příjem informací o kameře prostřednictvím portu SNMP. Nastavením adresy zachycení umožníte kameře odesílat události alarmu a zprávy o výjimkách do monitorovacího centra.

Poznámka: Vybraná verze SNMP by se měla shodovat s verzí softwaru SNMP. Rovněž je třeba použít jinou verzi dle požadované úrovně zabezpečení. SNMP v1 neposkytuje žádné zabezpečení a SNMP v2 vyžaduje pro přístup heslo. SNMP v3 poskytuje šifrování, a pokud použijete třetí verzi, musí být povolený protokol HTTPS.



- *Pro vaše soukromí a lepší ochranu vašeho systému před bezpečnostními riziky důrazně doporučujeme používat pro všechny funkce a síťová zařízení silná hesla. Heslo by mělo být vytvořeno dle vašeho vlastního výběru (o délce alespoň 8 znaků, s velkými písmeny, malými písmeny, čísly a speciálními znaky), abyste zvýšili zabezpečení výrobku.*
- *Za řádnou konfiguraci veškerých hesel a dalších nastavení zabezpečí ručí osoba provádějící instalaci a/nebo koncový uživatel.*

Postup:

1. Vstupte do rozhraní nastavení SNMP:

Configuration (Konfigurace) > Advanced Configuration (Rozšířená konfigurace) > Network (Síť) > SNMP

SNMP v1/v2	
Enable SNMPv1	<input type="checkbox"/>
Enable SNMP v2c	<input type="checkbox"/>
Write SNMP Community	<input type="text" value="private"/>
Read SNMP Community	<input type="text" value="public"/>
Trap Address	<input type="text"/>
Trap Port	<input type="text" value="162"/>
Trap Community	<input type="text" value="public"/>
SNMP v3	
Enable SNMPv3	<input type="checkbox"/>
Read UserName	<input type="text"/>
Security Level	<input type="text" value="no auth, no priv"/>
Authentication Algorithm	<input checked="" type="radio"/> MD5 <input type="radio"/> SHA
Authentication Password	<input type="text"/>
Private-key Algorithm	<input checked="" type="radio"/> DES <input type="radio"/> AES
Private-key password	<input type="text"/>
Write UserName	<input type="text"/>
Security Level	<input type="text" value="no auth, no priv"/>
Authentication Algorithm	<input checked="" type="radio"/> MD5 <input type="radio"/> SHA
Authentication Password	<input type="text"/>
Private-key Algorithm	<input checked="" type="radio"/> DES <input type="radio"/> AES
Private-key password	<input type="text"/>
SNMP Other Settings	
SNMP Port	<input type="text" value="161"/>

Figure 5-14 Nastavení SNMP

2. Zaškrtnutím políčka u příslušné verze (Enable SNMP SNMPv1 , Enable SNMP v2c , Enable SNMPv3) povolte tuto funkci.
3. Nakonfigurujte nastavení SNMP.
Poznámka: Nastavení softwaru SNMP by měla být stejná jako nastavení, která nakonfigurujete zde.
4. Kliknutím na tlačítko **Save** (Uložit) uložte a dokončete nastavení.

Poznámka: Aby se nastavení projevilo, je nutné provést restart.

5.3.6 Konfigurace nastavení 802.1X

Účel:

Norma IEEE 802.1X je podporovaná síťovými kamerami, a pokud je tato funkce povolena, při připojení kamery k síti chráněné zabezpečením IEEE 802.1X jsou data kamery jsou zabezpečena a je nutné ověření uživatele.

Než začnete:

Musí být nakonfigurovaný ověřovací server. Použijte a zaregistrujte uživatelské jméno pro zabezpečení 802.1X na serveru.



- *Pro vaše soukromí a lepší ochranu vašeho systému před bezpečnostními riziky důrazně doporučujeme používat pro všechny funkce a síťová zařízení silná hesla. Heslo by mělo být vytvořeno dle vašeho vlastního výběru (o délce alespoň 8 znaků, s velkými písmeny, malými písmeny, čísly a speciálními znaky), abyste zvýšili zabezpečení výrobku.*
- *Za řádnou konfiguraci veškerých hesel a dalších nastavení zabezpečí ručí osoba provádějící instalaci a/nebo koncový uživatel.*

Postup:

1. Vstupte do rozhraní nastavení zabezpečení 802.1X:

Configuration (Konfigurace) > Advanced Configuration (Rozšířená konfigurace) > Network (Síť) > 802.1X

<input checked="" type="checkbox"/> Enable IEEE 802.1X
Protocol: EAP-MD5
EAPOL version: 1
User Name: []
Password: []
Confirm: []

Figure 5-15 Nastavení zabezpečení 802.1X

2. Zaškrtnutím políčka **Enable IEEE 802.1X** (Povolit IEEE 802.1X) povolte tuto funkci.
3. Nakonfigurujte nastavení 802.1X, včetně verze EAPOL, uživatelského jména a hesla.

Poznámka: Verze EAPOL musí být shodná s verzí ve směrovači nebo prepínači.

4. Zadejte uživatelské jméno a heslo pro přístup k serveru.
5. Nastavení dokončete kliknutím na tlačítko **Save** (Uložit).

Poznámka: Aby se nastavení projevilo, je nutné provést restart.

5.3.7 Konfigurace nastavení QoS

Účel:

Funkce QoS (Quality of Service) může pomoci řešit prodlevu sítě a zahlcení sítě prostřednictvím konfigurace priority odesílání dat.

Postup:

1. Vstupte do rozhraní nastavení QoS:

Configuration (Konfigurace) > Advanced Configuration (Rozšířená konfigurace) > Network (Síť) > QoS

Video/Audio DSCP	<input type="text" value="0"/>
Event/Alarm DSCP	<input type="text" value="0"/>
Management DSCP	<input type="text" value="0"/>

Figure 5-16 Nastavení QoS

2. Nakonfigurujte nastavení QoS, včetně DSCP videa/audia, DSCP události/alarmu a DSCP pro správu.

Platný rozsah hodnot DSCP je 0 ~ 63. Čím vyšší je hodnota DSCP? tím vyšší je priorita.

Poznámka: DSCP znamená Differentiated Service Code Point; a hodnota DSCP použitá v hlavičce IP indikuje prioritu dat.

3. Uložte nastavení kliknutím na tlačítko **Uložit**.

Poznámka: Aby se nastavení projevilo, je nutné provést restart.

5.3.8 Konfigurace nastavení UPnP™

Universal Plug and Play (UPnP™) je síťová architektura, které zajišťuje kompatibilitu

síťových zařízení, softwaru a jiných hardwarových zařízení. Protokol UPnP umožňuje zařízením připojit se bez problémů a zjednodušit implementaci sítí v domácím i firemním prostředí.

V případě povolení této funkce není nutné konfigurovat mapování portů pro jednotlivé porty a kamera se připojí k síti WAN prostřednictvím směrovače.

Postup:

1. Vstupte do rozhraní nastavení UPnP™.

Configuration (Konfigurace) > Advanced Configuration (Rozšířená konfigurace) > Network (Síť) > UPnP

2. Chcete-li zapnout funkci UPnP™, zaškrtněte příslušné políčko.

Název zařízení v případě detekce online lze upravit.



Figure 5-17 Nastavení UPnP

5.3.9 Konfigurace nastavení bezdrátového komunikačního spojení

Účel:

Datový audio stream video stream a stream obrázků lze přenášet prostřednictvím bezdrátové sítě 3G/4G.

Poznámka: Funkce bezdrátového komunikačního spojení vyžaduje podporu kamery.

1. Klikněte na kartu **Wireless Dial** (Bezdrátové komunikační spojení) a vstupte do rozhraní konfigurace bezdrátového komunikačního spojení.
2. Zaškrtnutím políčka **Enable** (Povolit) povolte nastavení bezdrátového komunikačního spojení.
3. Nakonfigurujte parametry komunikačního spojení.
 - 1) Vyberte režim vytáčení z rozevíracího seznamu. Lze zvolit z možností Auto

(Automatické) a Manual (Manuální). Pokud je vybrána možnost Auto, můžete nastavit rozvrh zapnutí ochrany pro vytáčení; pokud je vybrána možnost Manual, můžete nastavit čas offline a parametry manuálního vytáčení.

- 2) Nastavte přístupové číslo, uživatelské jméno, heslo, APN, MTU a ověřovací protokol. Tyto parametry také můžete nechat nevyplněné a zařízení použije výchozí nastavení pro vytáčení po nakonfigurování ostatních parametrů.



- *Pro vaše soukromí a lepší ochranu vašeho systému před bezpečnostními riziky důrazně doporučujeme používat pro všechny funkce a síťová zařízení silná hesla. Heslo by mělo být vytvořeno dle vašeho vlastního výběru (o délce alespoň 8 znaků, s velkými písmeny, malými písmeny, čísly a speciálními znaky), abyste zvýšili zabezpečení výrobku.*
 - *Za řádnou konfiguraci veškerých hesel a dalších nastavení zabezpečí ručí osoba provádějící instalaci a/nebo koncový uživatel.*
- 3) Vyberte režim sítě z rozevíracího seznamu. Lze zvolit z možností Auto (Automatický), 3G a 4G. Pokud je vybrána možnost Auto, priorita výběru sítě je následující: 4G > 3G > kabelová síť.
 - 4) Zadejte čas offline, pokud je vybraný režim vytáčení Manual.
 - 5) Zadejte číslo UIM (číslo mobilního telefonu).
 - 6) Klikněte na tlačítko **Edit** (Upravit) a nastavte rozvrh zapnutí ochrany, pokud je nastavený režim vytáčení Auto.
 - 7) Uložte nastavení kliknutím na tlačítko **Uložit**.

^ Dial Parameters

Dial Mode

Access Number

User Name

Password

APN

MTU

Verification Protocol

Network Mode

Offline Time second

UIM Number

Figure 5-18 Parametry vytáčení

4. Podívejte se na stav vytáčení.
 - 1) Kliknutím na tlačítko **Refresh** (Obnovit) zobrazíte stav vytáčení, včetně režimu v reálném čase, stavu UIM, intenzity signálu atd.
 - 2) Pokud je vybraný režim vytáčení Manual, můžete se rovněž manuálně připojit/odpojit od bezdrátové sítě.

^ Dial Status

Real-time Mode	UNKNOWN
UIM Status	UNKNOWN
Signal Strength	0
Dial Status	disconnected
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Gateway	0.0.0.0
DNS Address	0.0.0.0

Figure 5-19 Stav vytáčení

5. Nastavte seznam povolených.

- 1) Zaškrtněte políčko **Enable SMS Alarm** (Povolit SMS alarm).

Mobilní telefonní číslo ze seznamu povolených může obdržet zprávu o alarmu od zařízení a restartovat zařízení prostřednictvím zprávy SMS.

Poznámka: Do seznamu povolených lze přidat až 8 mobilních telefonních čísel.

^ White List

Enable SMS Alarm

No.	Mobile Phone Number	Permission
1	18888888888	<input type="button" value="Edit"/>
2	15968172711	
3		
4		
5		
6		
7		
8		

Figure 5-20 Nastavení seznamu povolených

- 2) Vyberte položku v seznamu povolených a kliknutím na tlačítko **Edit** (Upravit) vstupte do rozhraní nastavení SMS alarmu.

Permission

Mobile Phone Number:

Reboot via SMS

<input type="checkbox"/> Exception	<input type="checkbox"/> Basic Event	<input type="checkbox"/> Smart Event
<input type="checkbox"/> HDD Full	<input type="checkbox"/> Motion Detection	<input type="checkbox"/> Line Crossing Detection
<input type="checkbox"/> Network Disconnected	<input type="checkbox"/> Video Tampering	<input type="checkbox"/> Intrusion Detection
<input type="checkbox"/> HDD Error		
<input type="checkbox"/> IP Address Conflicted		
<input type="checkbox"/> Illegal Login		

Figure 5-21 Nastavení SMS alarmu

- 3) Zadejte telefonní číslo pro seznam povolených, zaškrtněte políčko **Reboot via SMS** (Restartovat přes SMS), vyberte alarm pro zasílané zprávy SMS a klikněte na tlačítko **OK**.

Poznámka: Pokud chcete restartovat zařízení pomocí SMS, odešlete do něj zprávu „reboot“ a zařízení po úspěšném restartu odpoví zprávu „reboot success“ (úspěšný restart).

- 4) (Volitelné) Kliknutím na tlačítko **Send Test SMS** (Odeslat testovací SMS) odešlete zprávu do telefonu pro otestování.
- 5) Uložte nastavení kliknutím na tlačítko **Uložit**.

5.3.10 Odeslání e-mailu aktivovaným alarmem

Účel:

Systém lze nakonfigurovat, aby odesílal e-mailová oznámení všem určeným uživatelům, pokud je detekována událost alarmu, např. událost detekce pohybu, ztráty videa, manipulace s videem atd.

Než začnete:

Před použitím funkce e-mailu nakonfigurujte nastavení serveru DNS v nabídce **Basic Configuration (Základní konfigurace) > Network (Síť) > TCP/IP** nebo **Advanced Configuration (Rozšířená konfigurace) > Network (Síť) > TCP/IP**.

Postup:

1. Vstupte do nastavení TCP/IP (**Configuration > Basic Configuration > Network > TCP/IP** nebo **Configuration > Advanced Configuration > Network > TCP/IP**) a nastavte parametry IPv4 Address (Adresa IPv4), IPv4 Subnet Mask (Maska podsítě IPv4), IPv4 Default Gateway (Výchozí brána IPv4) a Preferred DNS Server (Upřednostňovaný server DNS).

Poznámka: Podrobné informace jsou uvedeny v *části 6.3.1 Konfigurace nastavení TCP/IP*.

2. Vstupte do rozhraní nastavení e-mailu: **Configuration (Konfigurace) > Advanced Configuration (Rozšířená konfigurace) > Network (Síť) > Email (E-mail)**

The screenshot shows a web-based configuration interface for email settings. It is divided into two main sections: 'Sender' and 'Receiver'.
Sender Section:
 - Sender: Text input field containing 'Test'.
 - Sender's Address: Text input field containing 'Test@gmail.com'.
 - SMTP Server: Text input field containing 'smtp.263xmail.com'.
 - SMTP Port: Text input field containing '25'.
 - Enable SSL: A checkbox that is currently unchecked.
 - Interval: A dropdown menu set to '2s'.
 - Attached Image: A checkbox that is currently unchecked.
 - Authentication: A checkbox that is currently unchecked.
 - User Name: Text input field (empty).
 - Password: Text input field (empty).
 - Confirm: Text input field (empty).
Receiver Section:
 - Receiver1: Text input field containing 'Test1'.
 - Receiver1's Address: Text input field containing 'Test1@gmail.com'.
 - Receiver2: Text input field (empty).
 - Receiver2's Address: Text input field (empty).
 - Receiver3: Text input field (empty).
 - Receiver3's Address: Text input field (empty).
 At the bottom right of the form is a 'Save' button.

Figure 5-22 Nastavení e-mailu

3. Nakonfigurujte následující nastavení

Sender (Odesílatel): Jméno odesílatele e-mailu.

Sender's Address (Adresa odesílatele): E-mailová adresa odesílatele.

SMTP Server (Server SMTP): IP adresa nebo název hostitele (např. smtp.263xmail.com) serveru SMTP.

SMTP Port (Port SMTP): Port SMTP. Východí port TCP/IP pro SMTP je 25 (nezabezpečený). Port SMTP SSL je 465.

Enable SSL (Povolit SSL): Zaškrtnutím tohoto políčka povolíte SSL, pokud je serverem SMTP vyžadováno.

Attached Image (Přiložený obrázek): Pokud chcete posílat e-maily s přiloženými obrázky alarmů, zaškrtněte políčko Attached Picture.

Interval: Interval představuje čas mezi dvěma úkony odeslání obrázkových příloh.

Authentication (Ověřování) (volitelné): Pokud váš e-mailový server vyžaduje ověření, zaškrtněte toto políčko pro použití ověření při přihlášení k tomuto

serveru a zadejte přihlašovací uživatelské jméno a heslo.



- *Pro vaše soukromí a lepší ochranu vašeho systému před bezpečnostními riziky důrazně doporučujeme používat pro všechny funkce a síťová zařízení silná hesla. Heslo by mělo být vytvořeno dle vašeho vlastního výběru (o délce alespoň 8 znaků, s velkými písmeny, malými písmeny, čísly a speciálními znaky), abyste zvýšili zabezpečení výrobku.*
- *Za řádnou konfiguraci veškerých hesel a dalších nastavení zabezpečí ručí osoba provádějící instalaci a/nebo koncový uživatel.*

Vyberte příjemce: Vyberte příjemce, kterému bude e-mail odeslán. Lze nakonfigurovat až 2 příjemce.

Receiver (Příjemce): Jméno uživatele, který bude informován.

Receiver's Address (Adresa příjemce): E-mailová adresa uživatele, který bude informován.

4. Uložte nastavení kliknutím na tlačítko **Uložit**.

5.3.11 Konfigurace nastavení NAT (Network Address Translation)

Účel:

1. Vstupte do rozhraní nastavení NAT.

Configuration (Konfigurace) > Advanced Configuration (Rozšířená konfigurace) > Network (Síť) > NAT

2. Vyberte režim mapování portů.

Pro mapování portů s výchozími čísly portů:

Vyberte Port Mapping Mode (Režim mapování portů) **Auto** (Automatický).

Pro mapování portů s upravenými čísly portů:

Vyberte Port Mapping Mode (Režim mapování portů) **Manual** (Manuální).

V případě manuálního mapování portů můžete upravit hodnotu čísla portu sami.

Enable Port Mapping

Port Mapping Mode

	Port Type	External Port	External IP Address	Status
<input checked="" type="checkbox"/>	HTTP	80	0.0.0.0	Not Valid
<input checked="" type="checkbox"/>	RTSP	554	0.0.0.0	Not Valid
<input checked="" type="checkbox"/>	Server Port	8000	0.0.0.0	Not Valid

Figure 5-23 Konfigurace nastavení NAT

- Uložte nastavení kliknutím na tlačítko **Uložit**.

5.3.12 Konfigurace nastavení FTP

Účel:

Můžete nakonfigurovat informace související se serverem FTP pro odesílání pořízených snímků na server FTP. Pořízené snímky mohou být aktivovány událostí nebo úlohou načasované snímky.

Postup:

- Vstupte do rozhraní nastavení FTP:
Configuration (Konfigurace) > Advanced Configuration (Rozšířená konfigurace) > Network (Síť) > FTP

Server Address

Port

User Name Anonymous

Password

Confirm

Directory Structure

Parent Directory

Child Directory

Upload Type Upload Picture

Figure 5-24 Nastavení FTP

- Nakonfigurujte nastavení FTP; pro přihlášení k serveru FTP je vyžadováno uživatelské jméno a heslo.



- Pro vaše soukromí a lepší ochranu vašeho systému před bezpečnostními

riziky důrazně doporučujeme používat pro všechny funkce a síťová zařízení silná hesla. Heslo by mělo být vytvořeno dle vašeho vlastního výběru (o délce alespoň 8 znaků, s velkými písmeny, malými písmeny, čísly a speciálními znaky), abyste zvýšili zabezpečení výrobku.

- *Za řádnou konfiguraci veškerých hesel a dalších nastavení zabezpečí ručí osoba provádějící instalaci a/nebo koncový uživatel.*

Adresář: V poli **Directory Structure** (Adresářová struktura) můžete vybrat kořenový adresář, nadřazený adresář a podřízený adresář. Pokud je vybrán nadřazený adresář, máte možnost použít jako název adresáře název zařízení, číslo zařízení nebo IP adresu zařízení; pokud je vybrán podřízený adresář, můžete jako název adresáře použít název kamery nebo číslo kamery.

Upload type (Typ odeslání): Slouží k povolení odeslání pořízeného snímku na server FTP.

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

Poznámka: Funkci anonymního přístupu musí podporovat server FTP.

3. Uložte nastavení kliknutím na tlačítko **Uložit**.

Poznámka: Pokud chcete odeslat pořízené snímky na server FTP, je třeba povolit načasovaný snímek nebo událostí aktivovaný snímek na stránce **Snapshot** (Snímek). Podrobné informace jsou uvedeny v *části 7.3*.

5.3.13 Přístup k platformě

Přístup k platformě vám poskytuje možnost spravovat zařízení prostřednictvím platformy EZVIZ Cloud P2P.

Poznámka: Funkce přístupu k platformě se liší dle modelu kamery a vyžaduje podporu kamery.

Zaškrtnutím políčka **Enable** (Povolit) povolte funkci EZVIZ Cloud P2P a budete moci spravovat zařízení prostřednictvím webové stránky EZVIZ Cloud P2P nebo

klienta EZVIZ Cloud P2P, což je aplikace pro mobilní telefony.

Protože někteří uživatelé nechtějí spravovat zařízení pomocí funkce EZVIZ Cloud P2P, můžete nechat toto políčko nezaškrtnuté.



Figure 5-25 Přístup k platformě

5.3.14 Nastavení HTTPS

Účel:

Protokol HTTPS nabízí ověřování webových stránek a souvisejícího webového serveru, se kterým probíhá komunikace, což slouží k ochraně před útoky typu Man-in-the-middle. Pro nastavení čísla portu https použijte následující postup.

Např.: Pokud nastavíte číslo portu 443 a IP adresa je 192.168.1.64, získáte přístup k zařízení zadáním adresy `https://192.168.1.64:443` pomocí webového prohlížeče.

Postup:

1. Vstupte do rozhraní nastavení HTTPS.
Configuration (Konfigurace) > Advanced Configuration (Rozšířená konfigurace) > Network (Síť) > HTTPS
2. Chcete-li tuto funkci aktivovat, zaškrtněte políčko Enable HTTPS (Povolit HTTPS).
3. Vytvořte certifikát podepsaný svým držitelem nebo autorizovaný certifikát.

Figure 5-26 Nastavení HTTPS

- Vytvořte certifikát podepsaný svým držitelem
- 1) Kliknutím na tlačítko **Create** (Vytvořit) vstupte do rozhraní vytváření.

Figure 5-27 Vytvoření certifikátu podepsaného svým držitelem

- 2) Zadejte zemi, název hostitele / IP adresu, platnost a další informace.
- 3) Kliknutím na tlačítko **OK** uložte nastavení.

Poznámka: Pokud již certifikát máte nainstalovaný, tlačítko Create Self-signed Certificate (Vytvořit certifikát podepsaný svým držitelem) je

neaktivní

- Vytvořte autorizovaný certifikát
 - 1) Kliknutím na tlačítko **Create** (Vytvořit) vytvořte žádost o certifikát.
 - 2) Stáhněte si žádost o certifikaci a odešlete ji k podpisu důvěryhodnému certifikačnímu úřadu.
 - 3) Po přijetí podepsaného platného certifikátu importujte certifikát do zařízení.
- 4. Po úspěšném vytvoření a instalaci certifikátu budou k dispozici informace o certifikátu.

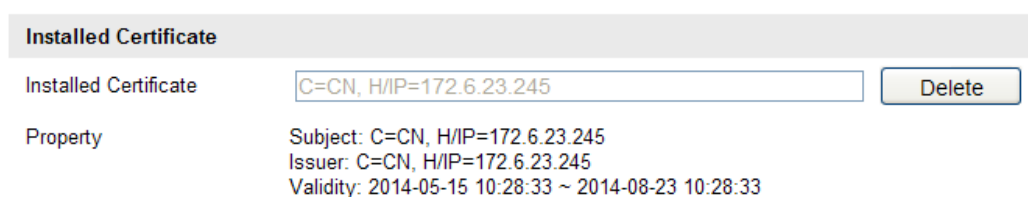


Figure 5-28 Nainstalovaný certifikát

5. Uložte nastavení kliknutím na tlačítko **Save** (Uložit).

5.4 Konfigurace nastavení videa a audia

5.4.1 Konfigurace nastavení videa

Postup:

1. Vstupte do rozhraní nastavení videa:

Configuration (Konfigurace) > Basic Configuration (Základní konfigurace) >

Video / Audio > Video

nebo **Configuration (Konfigurace) > Advanced Configuration (Rozšířená konfigurace) > Video / Audio > Video**

The screenshot shows a configuration window with several tabs: Video (selected), Audio, ROI, Display Info. on Stream, and Target Cropping. The Video tab contains the following settings:

- Stream Type: Main Stream(Normal)
- Video Type: Video&Audio
- Resolution: 1920*1080P
- Bitrate Type: Variable
- Video Quality: Higher
- Frame Rate: 25 fps
- Max. Bitrate: 4096 Kbps
- Video Encoding: H.264
- Profile: High Profile
- I Frame Interval: 50
- SVC: OFF
- Smoothing: 50 [Clear<->Smooth]

A Save button is located at the bottom right of the configuration area.

Figure 5-29 Nastavení videa

2. Vyberte **Stream Type** (Typ streamu) kamery z možností Main Stream (Normal) (Hlavní stream (normální)), sub-stream (Vedlejší stream) nebo third stream (Třetí stream).

Hlavní stream obvykle slouží pro záznam a živý náhled s vysokou přenosovou rychlostí, vedlejší stream a třetí stream lze použít k živému náhledu v případě omezené přenosové rychlosti.

3. Pro vybraný hlavní stream nebo vedlejší stream můžete přizpůsobit následující parametry:

Video Type (Typ videa):

Vyberte typ streamu z možností video nebo složený video a audio stream. Audio signál bude nahráván, pouze pokud je pod položkou **Video Type** vybrána možnost **Video & Audio**.

Resolution (Rozlišení):

Vyberte rozlišení video výstupu.

Bitrate Type (Typ datového toku):

Vyberte konstantní nebo variabilní typ datového toku.

Video Quality (Kvalita videa):

Pokud je vybrán **variabilní** typ datového toku, lze volit z 6 úrovní kvality videa.

Frame Rate (Snímková frekvence):

Nastavte snímkovou frekvenci v rozmezí 1/16 ~ 25 sn./s. Snímková frekvence je frekvence, kterou je video stream aktualizován a měří se ve snímcích za sekundu (sn./s). Vyšší snímková frekvence je výhodná, pokud ve video streamu dochází k rychlému pohybu, protože udržuje kvalitu obrazu.

Max. Bitrate (Max. datový tok):

Nastavte maximální datový tok v rozmezí 32 ~ 16 384 kbit/s. Vyšší hodnota odpovídá vyšší kvalitě videa, ale vyžaduje vyšší přenosovou rychlost.

Poznámka: Maximální limit maximálního datového toku se liší dle různých platform kamer. U některých konkrétních kamer je maximální limit 8192 kbit/s nebo 12288 kbit/s.

Video Encoding (Kódování videa):

Pokud je položka **Stream Type** nastavena na hlavní stream: Lze vybírat z možností H.264 a MPEG4 ; pokud je typ streamu nastavený na vedlejší nebo třetí stream, lze vybírat z možností H.264, MJPEG a MPEG4.

Poznámka: Typ kódování videa se liší dle různých platform kamer. U některých konkrétních kamer je podporováno kódování H.265 a není podporováno kódování MPEG4.

Profile (Profil):

Lze volit z profilů Basic, Main a High pro kódování.

I Frame Interval (Interval I-Frame):

Nastavte interval snímků I-Frame v rozmezí 1 ~ 400.

SVC:

Technologie Scalable Video Coding je rozšířením standardu H.264/AVC. Výběrem možnosti OFF (Vypnuto) / ON (Zapnuto) vypnete nebo zapnete funkci SVC. V případě výběru možnosti Auto (Automaticky) zařízení automaticky vynechává snímky z původního videa, pokud je přenosová rychlost sítě nedostatečná.

Smoothing (Vyhlazování):

Označuje vyhlazování streamu. Čím vyšší hodnota vyhlazování je použita, tím plynulejší je stream, ale kvalita videa nemusí být uspokojující. Čím nižší hodnota

vyhlazování je použita, tím vyšší je kvalita streamu, ale může působit neplynule.

4. Uložte nastavení kliknutím na tlačítko **Uložit**.

5.4.2 Konfigurace nastavení audia

Postup:

1. Vstupte do rozhraní nastavení audia:

**Configuration (Konfigurace) > Basic Configuration (Základní konfigurace)
> Video / Audio > Audio**

nebo **Configuration (Konfigurace) > Advanced Configuration (Rozšířená konfigurace) > Video / Audio > Audio**

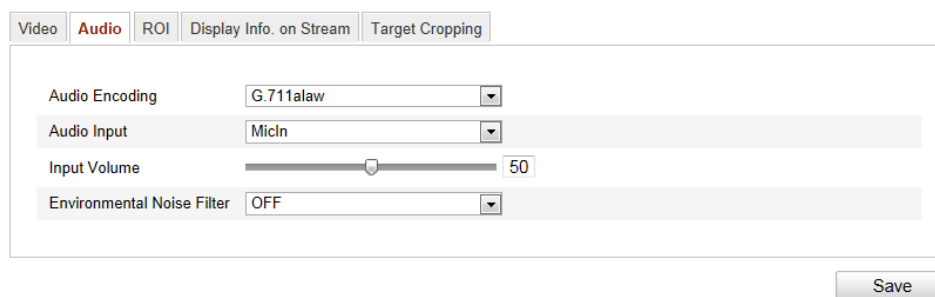


Figure 5-30 Nastavení audia

2. Nakonfigurujte následující nastavení

Poznámka: Nastavení audia se liší dle různých modelů kamer.

Audio Encoding (Kódování audia): Lze vybírat z možností G.722.1, G.711 ulaw, G.711alaw, G.726, MP2L2 a PCM. V případě kódování MP2L2, jsou vzorkovací frekvence a datový tok audio streamu konfigurovatelné; v případě kódování PCM lze nastavit vzorkovací frekvenci.

Audio Input (Audio vstup): Lze vybírat z možností MicIn a LineIn dle připojení mikrofону.

Input Volume (Hlasitost vstupu): 0-100

Environmental Noise Filter (Filtr hluku okolního prostředí): Nastavte na možnost OFF (Vypnuto) nebo ON (Zapnuto). Když je tato funkce povolena, hluk okolního prostředí lze do určité míry filtrovat.

3. Uložte nastavení kliknutím na tlačítko **Uložit**.

5.4.3 Konfigurace kódování ROI

Účel:

Kódování ROI (Region of Interest, oblast zájmu) pomáhá rozlišit oblast zájmu a okolí při komprimaci videa, což znamená, že technologie přidělí více prostředků kódování oblasti zájmu, čímž zvýší kvalitu oblasti zájmu, zatímco okolí je méně ostré.

Poznámka: Funkce ROI se liší dle různých modelů kamer.

Video Audio **ROI** Display Info. on Stream Target Cropping

Draw Area Clear

Stream Type
Stream Type Main Stream(Normal)

Fixed Region
 Enable
Region No. 1
ROI Level 3
Region Name

Dynamic Region
 Enable Face Tracking
ROI Level 3
 Enable License Plate Tracking
ROI Level 3

Save

Figure 5-31 Nastavení oblasti zájmu

Konfigurace pevné oblasti pro funkci ROI:

Postup:

1. Vstupte do rozhraní nastavení funkce ROI.

Configuration (Konfigurace) >Advanced Configuration (Rozšířená konfigurace) > Video / Audio > ROI

2. Zaškrtněte políčko **Enable** (Povolit) pod položkou Fixed Region (Pevná oblast).
3. Vyberte typ streamu pro kódování ROI.
4. Vyberte oblast z rozevíracího seznamu pro nastavení ROI. Vybírat lze ze čtyř pevných oblastí
5. Klikněte na tlačítko **Draw Area** (Nakreslit oblast) a poté tažením myši nakreslete oblast zájmu v živém videu.
6. Vyberte úroveň ROI pro nastavení úrovně vylepšení kvality obrazu. Čím vyšší je hodnota, tím vyšší je kvalita obrazu.
7. Zadejte název oblasti pro ROI dle potřeby.
8. Uložte nastavení kliknutím na tlačítko **Uložit**.

Konfigurace dynamické oblasti pro funkci ROI:

1. Vstupte do rozhraní nastavení funkce ROI.

Configuration (Konfigurace) >Advanced Configuration (Rozšířená konfigurace) > Video / Audio > ROI

2. Zaškrtněte políčko **Enable Face Tracking** (Povolit sledování obličeje) a poté bude jako oblast zájmu nastaven obrázek zachyceného obličeje.

Poznámka: Abyste mohli povolit funkci sledování obličeje, funkce by měla být podporovaná a povolena

3. Zaškrtněte políčko **Enable License Tracking** (Povolit sledování registrační značky) a poté bude jako oblast zájmu nastaven obrázek zachycené registrační značky.

Poznámka: Abyste mohli povolit funkci sledování registrační značky, funkce by měla být podporovaná a povolena.

4. Nastavte příslušným způsobem úroveň ROI. Čím vyšší je hodnota, tím vyšší je kvalita obrazu.
5. Vyberte typ streamu pro kódování ROI.

6. Uložte nastavení kliknutím na tlačítko **Uložit**.

5.4.4 Zobrazen informací o streamu

Zaškrtněte políčko **Enable Dual-VCA** (Povolit duální VCA) a informace o objektech (např. osobě, vozidle) budou vyznačeny ve video streamu. Poté můžete nastavit pravidla pro připojené koncové zařízení pro detekci událostí, jako překročení čáry, narušení atd.

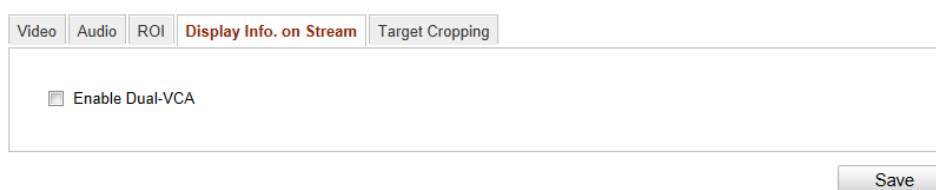


Figure 5-32 Zobrazen informací o streamu

5.4.5 Konfigurace oříznutí cíle

Účel:

Můžete specifikovat cílovou oblast živého videa, která poté může být zobrazena prostřednictvím třetího streamu v určitém rozlišení a v případě potřeby poskytovat více detailů cílové oblasti.

Poznámka: Funkce oříznutí cíle se liší dle různých modelů kamer.

Postup:

1. Vstupte do rozhraní nastavení funkce oříznutí cíle:
Configuration (Konfigurace) > Advanced Configuration (Rozšířená konfigurace)
> Video / Audio > Target Cropping (Oříznutí cíle)
2. Chcete-li tuto funkci aktivovat, zaškrtněte políčko **Enable Target Cropping** (Povolit oříznutí cíle).
3. Nastavte jako typ streamu třetí stream.
4. Vyberte rozlišení ořezu pro zobrazení videa cílové oblasti. V živém videu se zobrazí červený obdélník označující cílovou oblast; obdélník můžete přetáhnout

na cílovou oblast dle potřeby.

- Uložte nastavení kliknutím na tlačítko **Uložit**. Můžete přejít na stránku živého náhledu a po kliknutí na kartu **Third Stream** (Třetí stream) zobrazit video cílové oblasti.

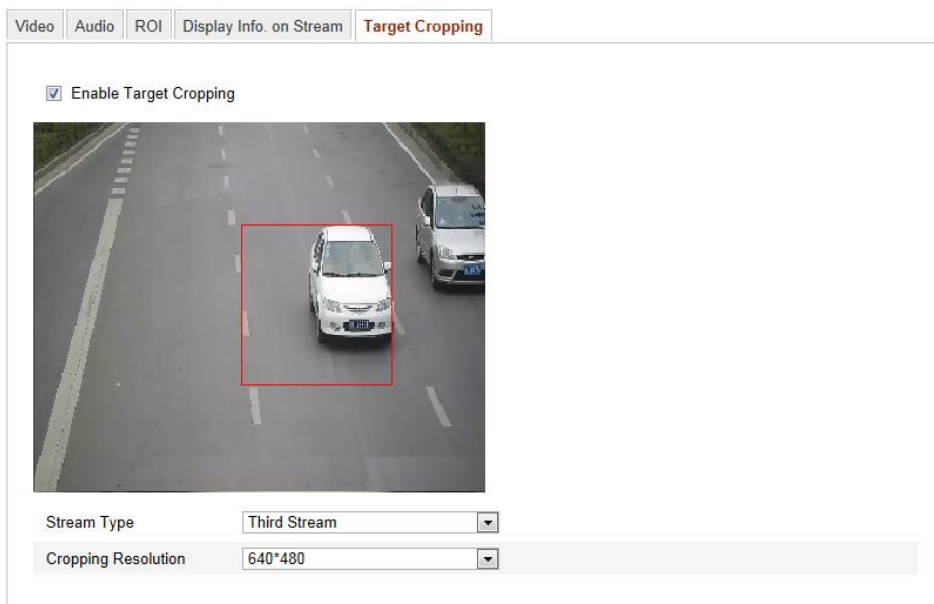


Figure 5-33 Oříznutí cíle

5.5 Konfigurace místního obrazu

5.5.1 Konfigurace nastavení zobrazení

Účel:

Můžete nastavit kvalitu obrazu kamery, jako jas, kontrast, sytost, odstín, ostrost atd.

Poznámka: Parametry zobrazení se liší dle různých modelů kamer. Podrobnosti lze vidět v samotném rozhraní.

Postup:

- Vstupte do rozhraní nastavení zobrazení

Configuration (Konfigurace) > Basic Configuration (Základní konfigurace)
> Image (Obraz) > Display Settings (Nastavení zobrazení)
 nebo **Configuration (Konfigurace) > Advanced Configuration (Rozšířená konfigurace) > Image (Obraz) > Display Settings (Nastavení zobrazení)**

2. Nastavte parametry obrazu kamery.

Poznámka: Aby byla zaručena kvalita obrazu při různém osvětlení, k dispozici jsou dvě sady parametrů, které může uživatel nakonfigurovat.

Automatické přepínání dne/noci

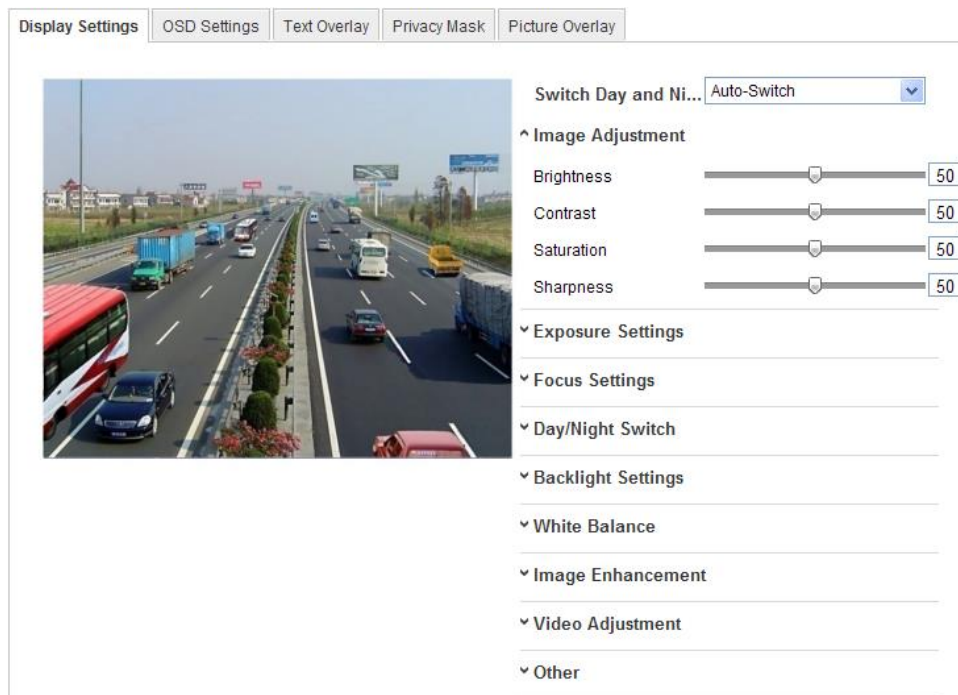


Figure 5-34 Nastavení zobrazení automatického přepínání dne/noci

◆ Nastavení obrazu

Brightness (Jas) popisuje jas obrazu v rozmezí 1~100 s výchozí hodnotou 50.

Contrast (Kontrast) popisuje kontrast obrazu v rozmezí 1~100 s výchozí hodnotou 50.

Saturation (Sytost) popisuje barevnost obrazu v rozmezí 1~100 s výchozí hodnotou 50.

Sharpness (Ostrost) popisuje kontrast hran v obrazu v rozmezí 1~100 s výchozí hodnotou 50.

◆ Nastavení expozice

Pokud je kamera vybavená pevným objektivem, lze vybrat pouze možnost **Manual** (Manuální) a režim clony není konfigurovatelný.

Pokud je vybrána možnost **Auto** (Automatické), můžete nastavit automatickou úroveň clony v rozmezí 10 ~ 100.

Pokud kamera podporuje objektivy **P-Iris** a je použitý objektiv P-Iris, lze zvolit typ objektivu P-Iris, např.: Tamron 2.8-8mm F1.2 (M13VP288-IR), nebo pokud je použitý objektiv DC, lze vybírat z možností Manual a Auto.

Délka expozice představuje čas elektronické závěrky v rozmezí od 1 do 1/100 000 s. Nastavte ji dle aktuálních světelných podmínek.

◆ Nastavení ostření

Pokud kamera podporuje elektronický objektiv, můžete nastavit režim ostření Auto (Automatický), Manual (Manuální) nebo Semi-auto (Poloautomatický). Pokud je vybrán automatický režim, ostření se upravuje automaticky dle reálné situace sledování; pokud je vybrán manuální režim, můžete ovládat objektiv nastavením zoomu, ostření, inicializace objektivu a pomocného ostření prostřednictvím ovládacího rozhraní PTZ; pokud je vybrán poloautomatický režim, kamera zaostří automaticky, když upravíte parametry zoomu.

◆ Přepnutí režimu den/noc

Vyberte režim přepínání dne/noci a nakonfigurujte nastavení inteligentního infračerveného osvětlení pomocí této možnosti.

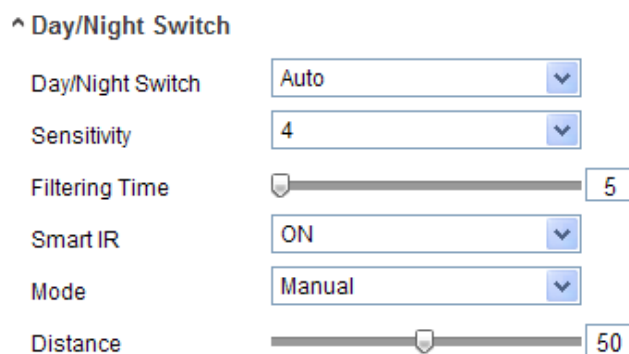


Figure 5-35 Přepnutí režimu den/noc

Pro přepnutí dne/noci lze vybírat z možností Day (Den), Night (Noc), Auto (Automaticky), Schedule (Rozvrh) a Triggered by alarm input (Aktivováno vstupem alarmu).

Day: kamera zůstane v denním režimu.

Night: kamera zůstane v nočním režimu.

Auto: kamera automaticky přepíná mezi denním a nočním režimem dle osvětlení.

Citlivost lze nastavit v rozmezí 0 ~ 7; čím vyšší je, tím snáze se režim přepne. Čas filtrování označuje interval mezi přepnutími dne/noci. Můžete ho nastavit v rozmezí od 5 s do 120 s.

Schedule: Nastavením času začátku a konce definujete dobu denního/nočního režimu.

Triggered by alarm input: Přepnutí je aktivováno vstupem alarmu a můžete nastavit aktivovaný režim na den nebo noc.

Smart IR (Inteligentní infračervené osvětlení): Funkce Smart IR poskytuje uživateli možnost upravit výkon infračervené diody pro zajištění čistého obrazu, který není přexponovaný ani příliš tmavý. Výběrem možnosti ON (Zapnuto) povolíte funkci Smart IR a pro režim IR lze vybírat z možností Auto (Automatický) a Manual (Manuální).

Vyberte možnost AUTO a výkon infračervené diody se změní automaticky dle aktuálního osvětlení. Např. pokud je aktuální scéna dostatečně jasná, infračervená dioda se nastaví na nižší výkon; pokud scéna není dostatečně jasná, infračervená dioda se nastaví na vyšší výkon.

Vyberte možnost Manual a můžete manuálně nastavit hodnotu vzdálenosti mezi infračervenou kamerou a objektem pro úpravu výkonu infračervené diody. Hodnota malé vzdálenosti indikuje, že objekt je blízko infračervené kamery, a zařízení nastaví nižší výkon infračervené diody, aby nedošlo k přexpozici; hodnot velké vzdálenosti indikuje, že objekt je daleko a zařízení nastaví vyšší výkon infračervené diody, aby obraz nebyl příliš tmavý.

◆ Nastavení protisvětla

BLC: Pokud ostříte na objekt v silném protisvětle, bude příliš tmavý a nebude zřetelně vidět. Funkce BLC kompenzuje osvětlení objektu v popředí, aby byl jasný. Lze vybírat z možností OFF (Vypnuto), Up (Nahore), Down (Dole), Left (Vlevo), Right (Vpravo), Center (Uprostřed) a Customize (Přizpůsobit).

WDR: Široký dynamický rozsah lze použít, pokud je mezi jasnou oblastí a tmavou oblastí záběru vysoký kontrast.

HLC: Funkci potlačení silného světla lze použít, pokud se v záběru nacházejí silná

světla ovlivňující kvalitu obrazu.

◆ Vyvážení bílé

Vyvážení bílé je funkce vykreslení bílé barvy kamery, sloužící k úpravě teploty barev dle prostředí.

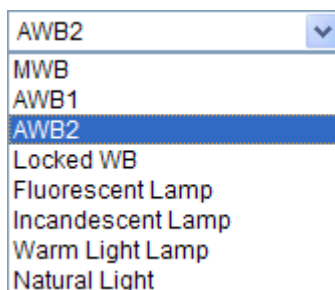


Figure 5-36 Vyvážení bílé

◆ Vylepšení obrazu

Digital Noise Reduction (Digitální redukce šumu): Funkce DNR snižuje šum ve video streamu. Lze vybírat z možností OFF (Vypnuto), Normal Mode (Normální režim) a Expert Mode (Režim pro odborníky). Vyberte úroveň DNR v rozmezí 0~100, s výchozí hodnotou 50 v normálním režimu. V režimu pro odborníky nastavte úroveň DNR jak pro prostorovou úroveň DNR [0~100], tak pro časovou úroveň DNR [0~100].

Defog Mode (Režim odmlžení): Můžete povolit funkci odmlžení, pokud je prostředí mlhavé a obraz je zamlžený. Zdůrazňuje jemné detaily, takže obraz vypadá zřetelnější.

Electrical Image Stabilizer (Elektronická stabilizace obrazu): Funkce EIS snižuje vlivy vibrací ve videu.

Grey Scale (Odstíny šedi): Můžete vybrat rozmezí odstínů šedi z možností [0-255] nebo [16-235].

◆ Nastavení videa

Mirror (Převrátit): Převrátí obraz. Lze vybírat z možností Left/Right (Podle svislé osy), Up/Down (Podle vodorovné osy), Center (Podle středu) a OFF (Vypnuto).

Rotate (Otočit): Abyste plně využili poměru stran 16:9, můžete povolit funkci otáčení, pokud kameru používáte ve scéně s úzkým záběrem.

Při instalaci otočte kameru o 90° nebo otočte 3osý objektiv o 90° a zapněte režim otočení. Dosáhnete tak normálního zobrazení scény s poměrem stran 9:16, abyste mohli ignorovat nepotřebné informace, jako zeď, a získali smysluplnější informace o scéně.

Scene Mode (Režim scény): Vyberte scénu jako interiér nebo exteriér dle skutečného prostředí.

Video Standard (Norma videa): Lze vybírat z možností 50 Hz a 60 Hz. Vyberte dle různých norem videa, obvykle 50 Hz pro normu PAL a 60 Hz pro normu NTSC.

Capture Mode (Režim snímání): Jde o volitelný režim video vstupu tak, aby splnil různé požadavky na úhel záběru a rozlišení.

Lens Distortion Correction (Korekce zkreslení objektivu): Výběrem možnosti ON (Zapnuto) / OFF (Vypnuto) povolte/zakažte korekci zkreslení objektivu. Pokud je tato funkce povolena, lze korigovat zkreslený obraz způsobený širokoúhlým objektivem.

◆ Ostatní

Některé kamery podporují výstupy CVBS, SDI nebo HDMI. Podrobnosti zjistíte ze samotné kamery.

Plánované přepínání dne/noci

Rozhraní konfigurace plánovaného přepínání dne/noci vám umožňuje nastavit samostatné parametry kamery pro den a noc, aby byla zaručena kvalita obrazu při různém osvětlení.



Figure 5-37 Rozhraní konfigurace plánovaného přepínání dne/noci

Postup:

1. Klikněte na časovou osu a vyberte čas začátku a čas konce přepnutí.
2. Klikněte na kartu Common (Obecné) a nakonfigurujte obecné parametry platné pro denní režim a noční režim.

Poznámka: Podrobné informace o jednotlivých parametrech jsou uvedeny v části o automatickém přepínání dne/noci.

3. Klikněte na kartu Day (Den) a nakonfigurujte parametry platné pro denní režim.
4. Klikněte na kartu Night (Noc) a nakonfigurujte parametry platné pro noční režim.

Poznámka: V případě změny parametru se nastavení uloží automaticky.

5.5.2 Konfigurace nastavení OSD

Účel:

Můžete přizpůsobit název kamery a čas na obrazovce.

Postup:

1. Vstupte do rozhraní nastavení OSD:

Configuration (Konfigurace) > Advanced Configuration (Rozšířená konfigurace) > Image (Obraz) > OSD Settings (Nastavení OSD)

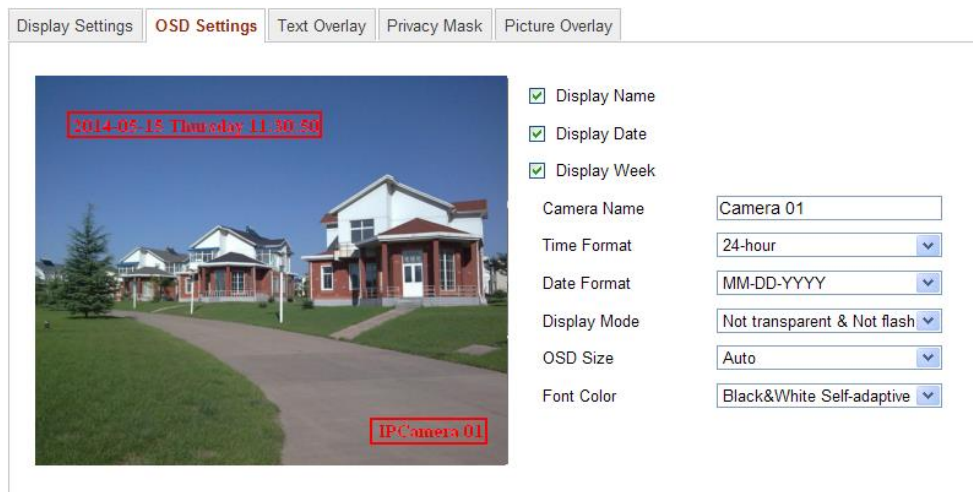


Figure 5-38 Nastavení OSD

2. Zaškrtnutím příslušného políčka zvolte zobrazení názvu kamery, dne nebo týdne dle potřeby.
3. Upravte název kamery v textovém poli **Camera Name** (Název kamery).
4. Vyberte v rozevřacím seznamu formát času, formát data, režim zobrazení a velikost písma OSD.
5. Definujte barvu písma OSD kliknutím na rozevřací seznam. Lze vybrat z možností Black&White Self-adaptive (Černobílé s automatickým přizpůsobením) a Custom (Vlastní).

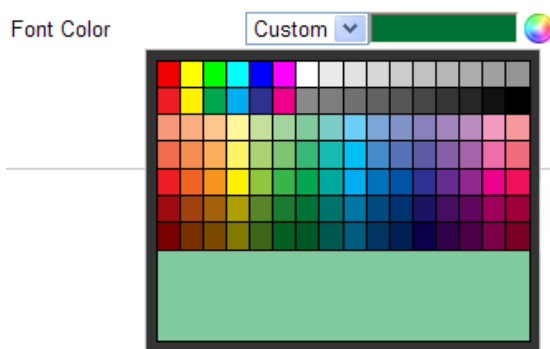


Figure 5-39 Barva písma – vlastní

6. Pomocí myši můžete přetáhnout textový rámeček **IPCamera 01** v okně živého náhledu a nastavit pozici OSD.

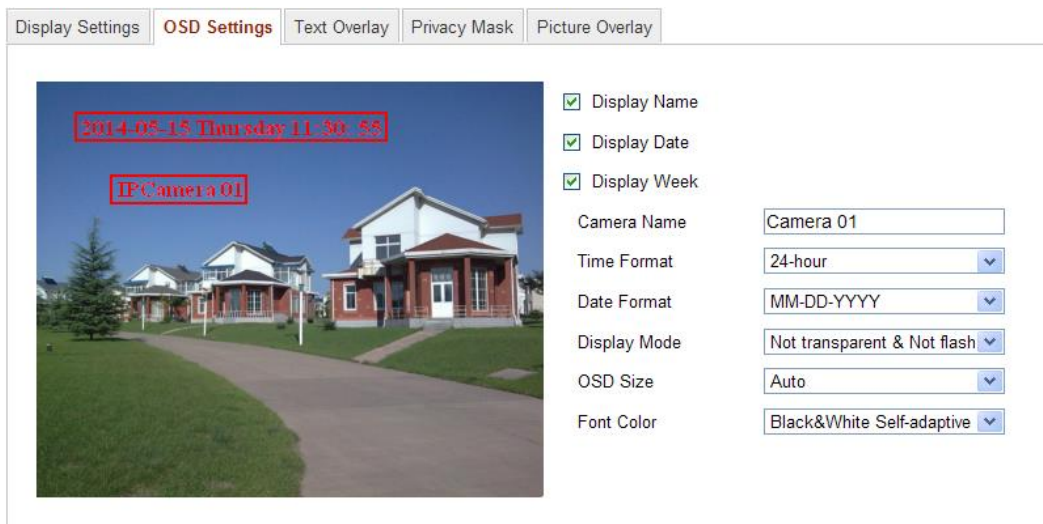


Figure 5-40 Nastavení pozice OSD

7. Kliknutím na tlačítko **Save** (Uložit) aktivujete výše uvedená nastavení.

5.5.3 Konfigurace nastavení překrytí itextem

Účel:

Překrytí textem můžete přizpůsobit.

Postup:

1. Vstupte do rozhraní nastavení překrytí textem:

Configuration (Konfigurace) > Advanced Configuration (Rozšířená konfigurace) > Image (Obraz) > Text Overlay (Překrytí textem)

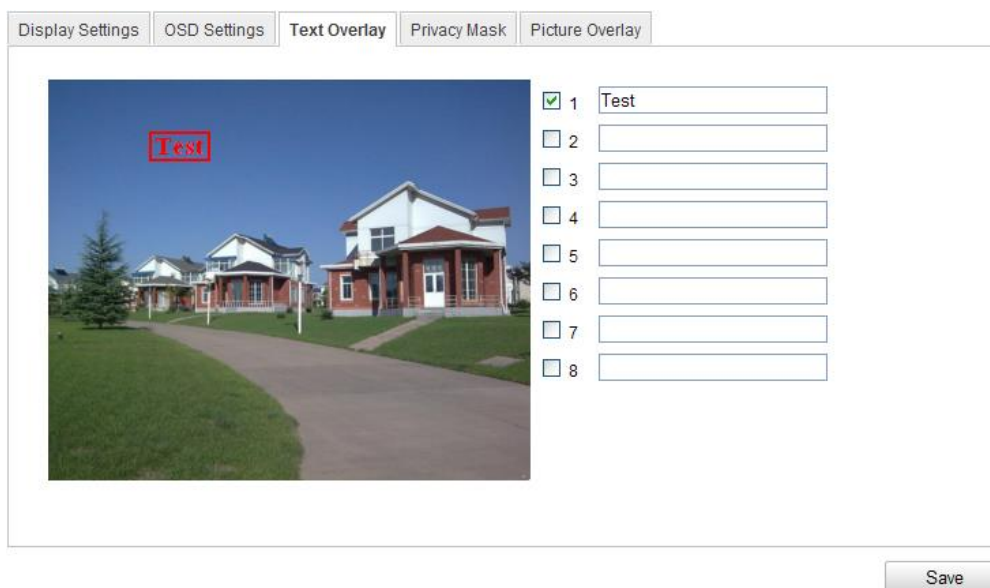



Figure 5-41 Překrytí textem

2. Zaškrtnutím políčka před textovým polem povolte zobrazení na obrazovce.
3. Zadejte znaky do textového pole.
4. (Volitelné) Pomocí myši můžete přetáhnout červený textový rámeček  v okně živého náhledu a nastavit pozici překrytí textem.
5. Uložte nastavení kliknutím na tlačítko **Uložit**.

Poznámka: Lze nakonfigurovat až 8 překrytí textem.

5.5.4 Konfigurace funkce Privacy Mask (místa zakrytá kvůli ochraně soukromí)

Účel:

Funkce Privacy Mask vám umožňuje zakrýt určité oblasti v živém videu, aby určitá místa ve sledované oblasti nemohla být sledována a nahrávána.

Postup:

1. Vstupte do rozhraní nastavení funkce Privacy Mask:
Configuration (Konfigurace) > Advanced Configuration (Rozšířená konfigurace) > Image (Obraz) > Privacy Mask
2. Zaškrtnutím políčka **Enable Privacy Mask** (Povolit funkci Privacy Mask) povolte tuto funkci.
3. Klikněte na tlačítko **Draw Area** (Nakreslit oblast).

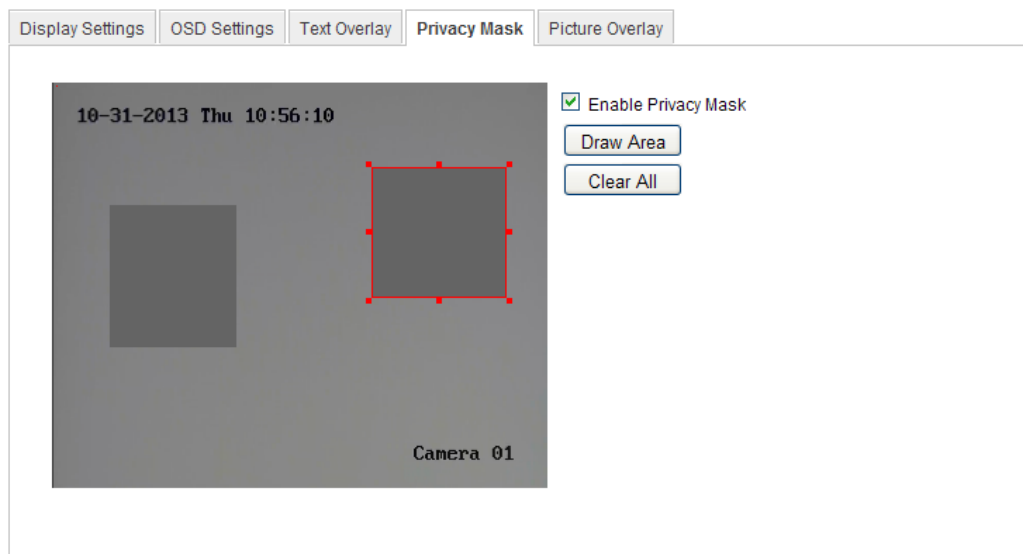


Figure 5-42 Nastavení funkce Privacy Mask

4. Kliknutím a tažením myši v okně živého videa nakreslete maskovanou oblast.

Poznámka: Do stejného obrázku můžete nakreslit až 4 oblasti.

5. Kliknutím na tlačítko **Stop Drawing** (Přestat kreslit) dokončete kreslení nebo klikněte na tlačítko **Clear All** (Smazat vše) a smažte všechny oblasti, které jste nastavili, aniž by byly uloženy.

6. Uložte nastavení kliknutím na tlačítko **Uložit**.

5.5.5 Konfigurace překrytí obrázkem

Účel:

Překrytí obrázkem umožňuje překrytí obrazu obrázkem. Tato funkce umožňuje určitým podnikům nebo uživatelům vložit do obrazu své logo.

Poznámka: Obrázek musí být ve formátu BMP RGB24 a maximální velikost obrázku je 128×128.

Postup:

1. Vstupte do rozhraní nastavení překrytí obrázkem:

Configuration (Konfigurace) > Advanced Configuration (Rozšířená konfigurace) > Image (Obraz) > Picture Overlay (Překrytí obrázkem)

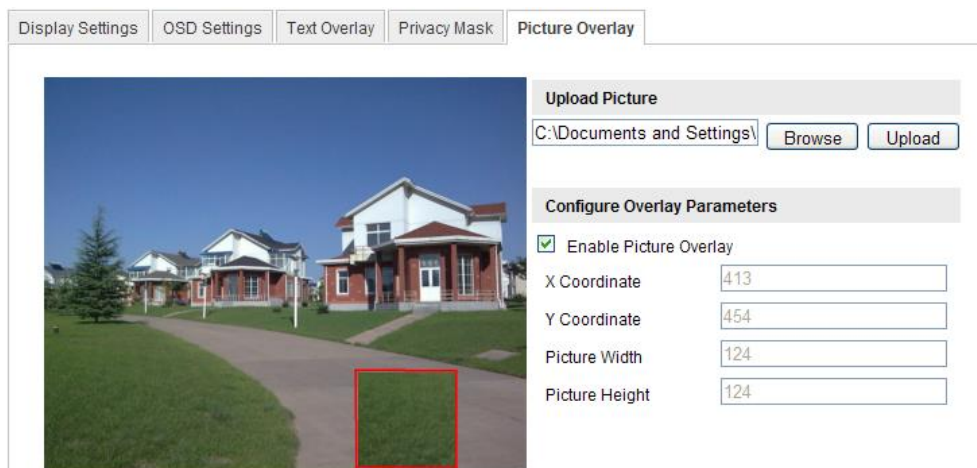


Figure 5-43 Překrytí obrázkem


2. Klikněte na tlačítko **Browse** (Procházet) a vyberte obrázek.
3. Kliknutím na tlačítko **Upload** (Odeslat) ho odešlete.
4. Zaškrtnutím políčka **Enable Picture Overlay** (Povolit překrytí obrázkem) funkci povolte.

Hodnoty X Coordinate (Souřadnice X) a Y Coordinate (Souřadnice Y) určují pozici obrázku v obraze. Parametry Picture Width (Šířka obrázku) a Picture Height (Výška obrázku) zobrazují velikost obrázku.

5.6 Konfigurace a zpracování alarmů

Tato část popisuje, jak nakonfigurovat síťovou kameru na reakci na události alarmu, jako detekce pohybu, manipulace s videem, vstup alarmu, výstup alarmu, výjimka, detekce obličeje, detekce výjimky audia, detekce narušení, detekce rozostření, detekce změny scény atd. Tyto události mohou aktivovat metody propojení, jako informování monitorovacího centra, odeslání e-mailu, aktivace výstupu alarmu atd.

Poznámky:

- Pokud chcete zaslat informaci o alarmu do počítače nebo mobilního klientského softwaru, jakmile dojde k aktivaci alarmu, zaškrtněte políčko Notify Surveillance Center (Informovat monitorovací centrum).
- Kliknutím na ikonu  získáte nápovědu při konfiguraci inteligentních funkcí, jako detekce obličeje, detekce výjimky audia, detekce narušení, detekce

rozostření, detekce změny scény atd. Dokument nápovědy vás provede postupem konfigurace.

5.6.1 Konfigurace detekce pohybu

Účel:

Detekce pohybu detekuje pohybující se objekty v nakonfigurované oblasti sledování a když se aktivuje tento alarm, může být provedena řada činností.

Aby byla detekce pohybujících se objektů přesná a omezila se četnost falešných poplachů, lze volit z normální konfigurace a konfigurace pro odborníky pro různá prostředí detekce pohybu.

➤ **Normální konfigurace**

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

Činnosti:

1. Nastavte oblast detekce pohybu.

Postup:

- (1) Vstupte do rozhraní nastavení detekce pohybu.

Configuration (Konfigurace) > Advanced Configuration (Rozšířená konfigurace) > Basic Event (Základní událost) > Motion Detection (Detekce pohybu)

- (2) Zaškrtněte políčko **Enable Motion Detection** (Povolit detekci pohybu).

- (3) Pokud chcete označit detekované objekty zelenými obdélníky, zaškrtněte políčko **Enable Dynamic Analysis for Motion** (Povolit dynamickou analýzu pro pohyb).

Poznámka: Pokud nechcete zobrazovat detekované objekty s obdélníky, vyberte u příslušných pravidel možnost Disable (Zakázat). Vyberte možnost Disable (Zakázat) pod položkou **Configuration (Konfigurace) > Local Configuration > (Místní konfigurace) > Live View Parameters (Parametry živého náhledu) > Rules (Pravidla)**.

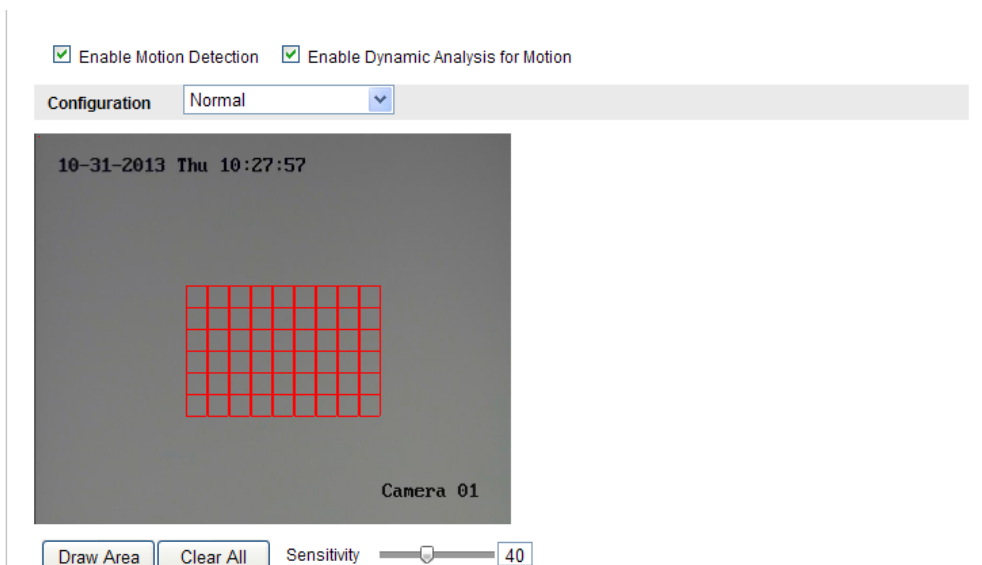


Figure 5-44 Zapnout detekci pohybu

- (4) Klikněte na tlačítko **Draw Area** (Nakreslit oblast). Kliknutím a tažením myší v okně živého videa nakreslete oblast detekce pohybu.
- (5) Kliknutím na tlačítko **Stop Drawing** (Zastavit kreslení) dokončete kreslení jedné oblasti.
- (6) (Volitelné) Kliknutím na tlačítko **Clear All** (Smazat vše) smažete všechny oblasti.
- (7) (Volitelné) Posunutím posuvníku nastavte citlivost detekce.

2. Nastavte rozvrh zapnutí ochrany pro detekci pohybu.

Postup:

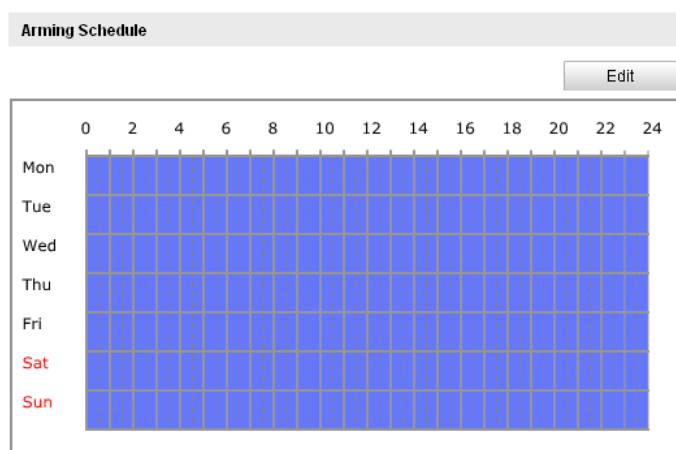

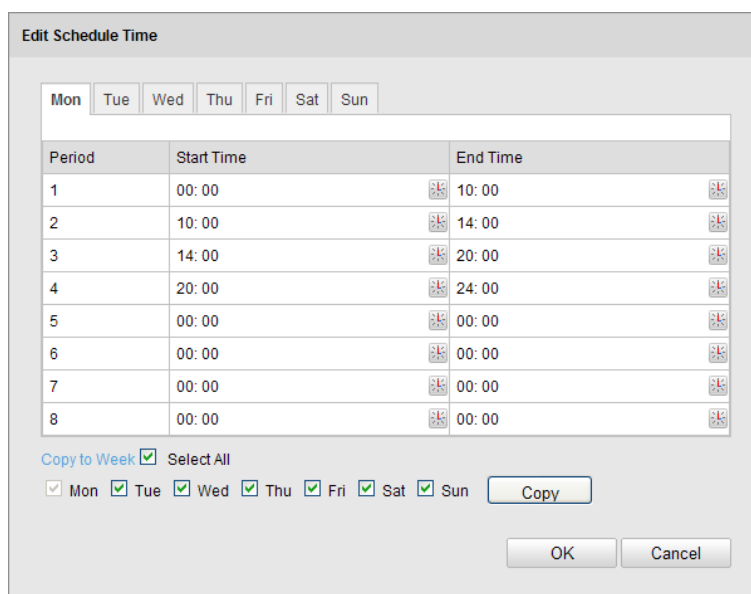


Figure 5-45 Čas zapnutí ochrany

- (1) Kliknutím na tlačítko **Edit** (Upravit) upravte rozvrh zapnutí ochrany. Obrázek 6-34 znázorňuje rozhraní úprav rozvrhu zapnutí ochrany.

- (2) Vyberte den, pro který chcete nastavit rozvrh zapnutí ochrany.
- (3) Klikněte na tlačítko  a nastavte časové období pro rozvrh zapnutí ochrany.
- (4) (Volitelné) Po nastavení rozvrhu zapnutí ochrany můžete zkopírovat rozvrh do dalších dní.
- (5) Kliknutím na tlačítko **OK** uložíte nastavení.

Poznámka: Časy jednotlivých období se nesmějí překrývat. Pro každý den lze nastavit až 8 intervalů.



Period	Start Time	End Time
1	00: 00	10: 00
2	10: 00	14: 00
3	14: 00	20: 00
4	20: 00	24: 00
5	00: 00	00: 00
6	00: 00	00: 00
7	00: 00	00: 00
8	00: 00	00: 00

Copy to Week Select All
 Mon Tue Wed Thu Fri Sat Sun

Figure 5-46 Časový rozvrh zapnutí ochrany

3. Nastavte akce alarmů pro detekci pohybu.

Zaškrtnutím políčka vyberte metodu propojení. Vybírat lze z možností informovat monitorovací centrum, odeslat e-mail, nahrát na server FTP, aktivovat kanál a aktivovat výstup alarmu. Můžete specifikovat metodu propojení při výskytu události.

Linkage Method	
Normal Linkage	Other Linkage
<input checked="" type="checkbox"/> Audible Warning <input checked="" type="checkbox"/> Notify Surveillance Center <input checked="" type="checkbox"/> Send Email <input checked="" type="checkbox"/> Upload to FTP <input type="checkbox"/> Trigger Channel	Trigger Alarm Output <input type="checkbox"/> Select All

Figure 5-47 Metoda propojení

- **Audible Warning (Zvukové upozornění)**

Aktivace imšního zvukového upozornění. Podporují pouze zařízení s audio výstupem.

- **Notify Surveillance Center (Informovat monitorovací centrum)**

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

- **Send Email (Odeslat e-mail)**

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

Poznámka: Abyste mohli odeslat e-mail, když nastane událost, je třeba nastavit příslušné parametry podle části 6.3.10 *Odeslání e-mailu aktivovaným alarmem*.

- **Upload to FTP (Nahrát na server FTP)**

Pořízení snímku při aktivaci alarmu a jeho odeslání na server FTP.

Poznámky:

- Nejprve nastavte adresu serveru FTP a vzdálený server FTP. Podrobnosti jsou uvedeny v části 6.3.12 *Konfigurace nastavení FTP*.
- Přejděte na stránku **Advanced Configuration (Rozšířená konfigurace)** > **Storage (Úložiště)** > **Snapshot (Snímek)**, povolte snímek aktivovaný událostí a nastavte interval a počet snímání.
- Pořízený snímek lze nahrát také na dostupnou kartu SD nebo síťový disk.

- **Trigger Channel (Aktivovat kanál)**

V případě detekce pohybu bude nahráno video. K provedení této funkce je třeba nastavit rozvrh směrování. Podrobné informace jsou uvedeny v části 7.2.

- **Trigger Alarm Output (Aktivovat výstup alarmu)**

Aktivace jednoho nebo více externích výstupů alarmu, když dojde k události.

Poznámka: Postup nastavení příslušných parametrů aktivace výstupu alarmu při výskytu události je uveden v části 6.6.4 *Konfigurace výstupu alarmu*.

- **Konfigurace pro odborníky**

Režim pro odborníky slouží hlavně ke konfiguraci citlivosti a proporce objektu v jednotlivých oblastech pro různá nastavení dne/noci.

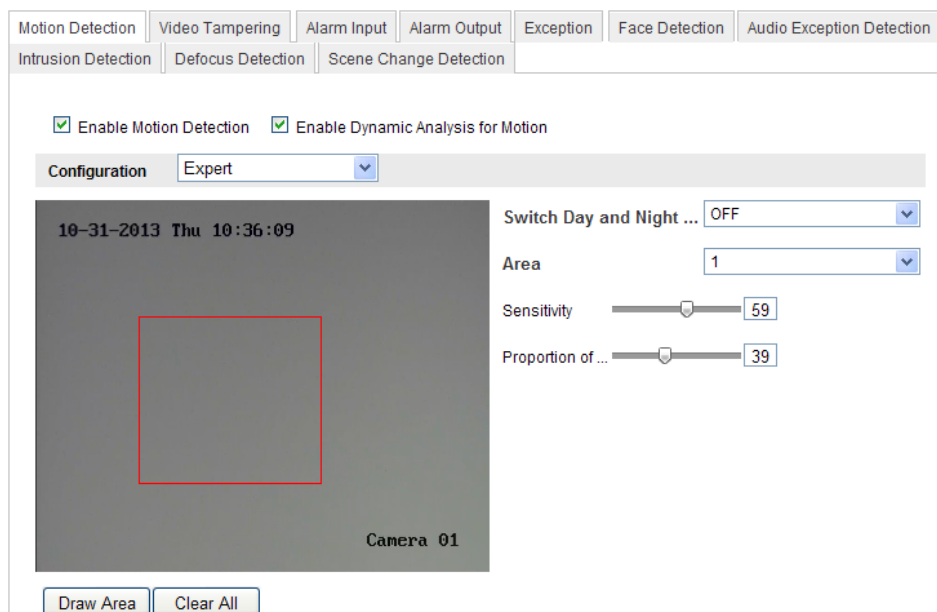


Figure 5-48 Režim detekce pohybu pro odborníky

- Vypnutí přepínání dne/noci

Postup:

- (1) Nakreslete oblast detekce jako v normálním režimu konfigurace. Podporováno je až 8 oblastí.
- (2) Vyberte možnost **OFF** (Vypnuto) u položky **Switch Day and Night Settings** (Přepínat nastavení dne a noci).
- (3) Vyberte oblast kliknutím na číslo oblasti.
- (4) Posunutím kurzoru nastavte citlivost a proporce objektu ve vybrané oblasti.
- (5) Nastavte rozvrh zapnutí ochrany a metodu propojení jako v normálním režimu konfigurace.
- (6) Uložte nastavení kliknutím na tlačítko **Uložit**.

- Automatické přepínání dne/noci

Postup:

- (1) Nakreslete oblast detekce jako v normálním režimu konfigurace. Podporováno je až 8 oblastí.
- (2) Vyberte možnost **Auto-Switch** (Automatické přepínání) u položky **Switch**

Day and Night Settings (Přepínat nastavení dne a noci).

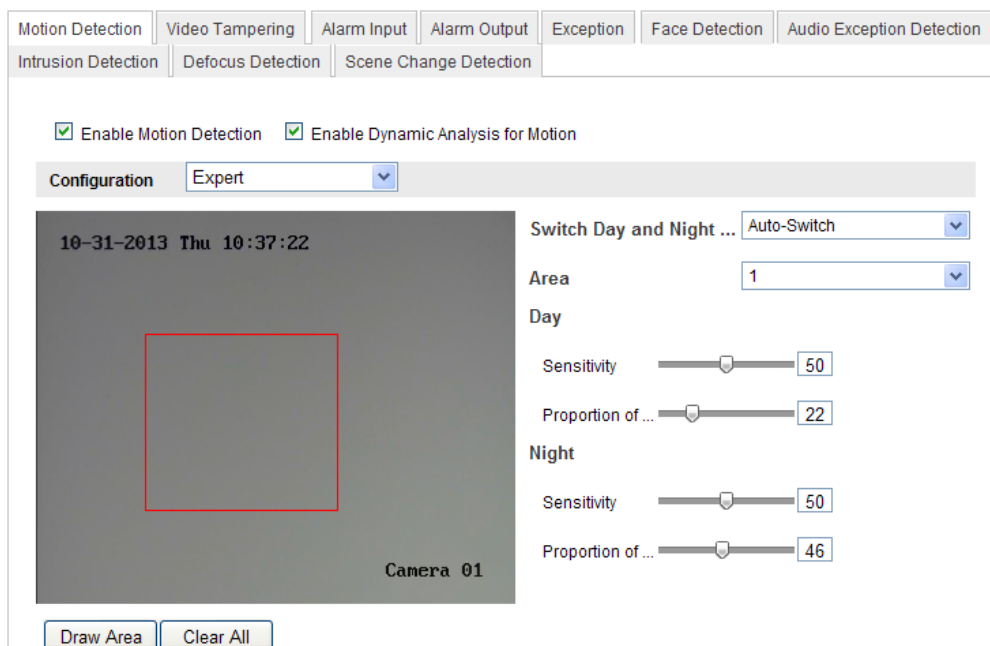


Figure 5-49 Automatické přepínání dne/noci

(3) Vyberte oblast kliknutím na číslo oblasti.

(4) Posunutím kurzoru nastavte citlivost a proporce objektu ve vybrané oblasti v denní době.

(5) Posunutím kurzoru nastavte citlivost a proporce objektu ve vybrané oblasti v noci.

(6) Nastavte rozvrh zapnutí ochrany a metodu propojení jako v normálním režimu konfigurace.

(7) Uložte nastavení kliknutím na tlačítko **Uložit**.

- Plánované přepínání dne/noci

(1) Nakreslete oblast detekce jako v normálním režimu konfigurace. Podporováno je až 8 oblastí.

(2) Vyberte možnost **Scheduled-Switch** (Plánované přepínání) u položky **Switch Day and Night Settings** (Přepínat nastavení dne a noci).

Switch Day and Night ...	Scheduled- Switch <input type="button" value="v"/>
Start Time	<input type="text" value="06:00:00"/>
End Time	<input type="text" value="18:00:00"/>

Figure 5-50 Plánované přepínání dne/noci

- (3) Vyberte čas začátku a čas konce pro načasování přepínání.
- (4) Vyberte oblast kliknutím na číslo oblasti.
- (5) Posunutím kurzoru nastavte citlivost a proporce objektu ve vybrané oblasti v denní době.
- (6) Posunutím kurzoru nastavte citlivost a proporce objektu ve vybrané oblasti v noci.
- (7) Nastavte rozvrh zapnutí ochrany a metodu propojení jako v normálním režimu konfigurace.
- (8) Uložte nastavení kliknutím na tlačítko **Uložit**.

5.6.2 Konfigurace alarmu manipulace s videem

Účel:

Můžete nakonfigurovat kameru, aby aktivovala alarm, když dojde k zakrytí objektivu, a provedla určité činnosti reakce.

Postup:

1. Vstupte do rozhraní nastavení manipulace s videem:

Configuration (Konfigurace) > Advanced Configuration (Rozšířená konfigurace) > Basic Event (Základní událost) > Video Tampering (Manipulace s videem)

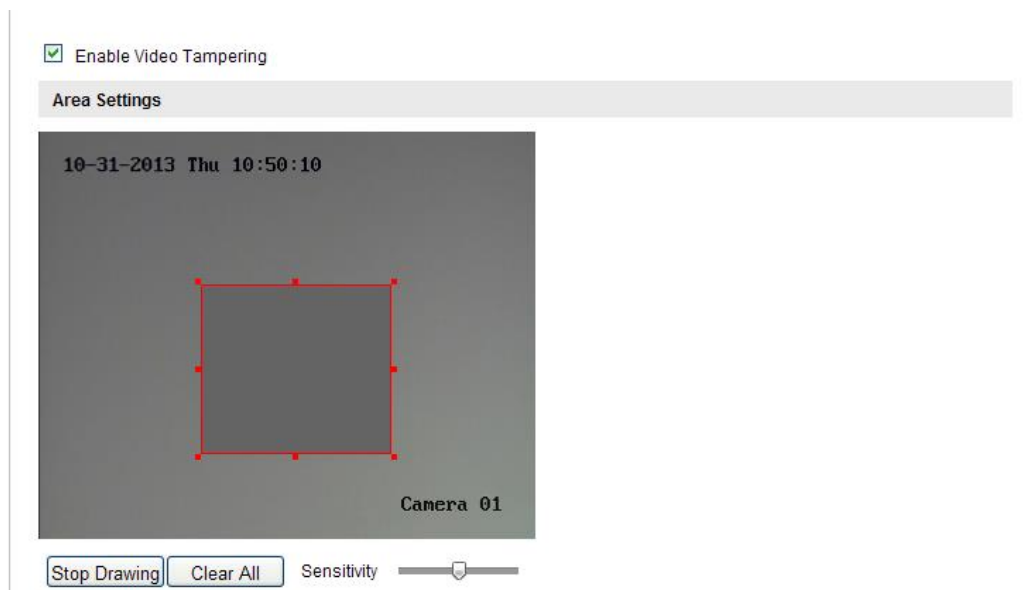


Figure 5-51 Alarm manipulace s videem

2. Zaškrtnutím políčka **Enable Video Tampering** (Povolit manipulaci s videem) povolte detekci manipulace s videem.
3. Nastavte oblast manipulace s videem. Postupujte podle 1. ikonu *Nastavení oblasti detekce pohybu* v části 6.6.1.
4. Kliknutím na tlačítko **Edit** (Upravit) upravte rozvrh zapnutí ochrany pro manipulaci s videem. Konfigurace rozvrhu zapnutí ochrany je stejná jako nastavení rozvrhu zapnutí ochrany pro detekci pohybu. Postupujte podle 2. ikonu *Nastavení rozvrhu zapnutí ochrany pro detekci pohybu* v části 6.6.1.
5. Zaškrtnutím políčka vyberte metodu propojení použitou pro manipulaci s videem. Lze vybrat z možností zvukové upozornění, informování monitorovacího centra, odeslání e-mailu a aktivace výstupu alarmu. Postupujte podle 3. ikonu *Nastavení akce alarmu pro detekci pohybu* v části 6.6.1.
6. Uložte nastavení kliknutím na tlačítko **Uložit**.

5.6.3 Konfigurace vstupu alarmu

Postup:

1. Vstupte do rozhraní nastavení vstupu alarmu:

Configuration (Konfigurace) > Advanced Configuration (Rozšířená

konfigurace) > Basic Event (Základní událost) > Alarm Input (Vstup alarmu)

2. Vyberte číslo vstupu alarmu a druh alarmu. Druh alarmu může být NO (V klidu rozpojeno) a NC (V klidu sepnuto). Upravte název vstupu alarmu (volitelné).

The screenshot shows the configuration interface for an Alarm Input. It includes the following elements:

- Alarm Input No.:** A dropdown menu with the value "A<-1".
- Alarm Name:** A text input field with the placeholder "(cannot copy)".
- Alarm Type:** A dropdown menu with the value "NO".
- Arming Schedule:** A section with a header "Arming Schedule" and an "Edit" button. Below the header is a grid representing the arming schedule. The grid has columns for hours from 0 to 24 in increments of 2, and rows for days of the week: Mon, Tue, Wed, Thu, Fri, Sat, and Sun. The grid cells are currently all blue, indicating that the alarm is armed 24/7.

Figure 5-52 Nastavení vstupu alarmu

3. Kliknutím na tlačítko **Edit** (Upravit) nastavte rozvrh zapnutí ochrany pro vstup alarmu. Postupujte podle 2. ikonu *Nastavení rozvrhu zapnutí ochrany pro detekci pohybu* v části 6.6.1.
4. Zaškrtnutím políčka vyberte metodu propojení použitou pro vstup alarmu. Postupujte podle 3. ikonu *Nastavení akce alarmu pro detekci pohybu* v části 6.6.1.
5. Rovněž můžete zvolit propojení PTZ pro vstup alarmu, pokud je kamera instalovaná s jednotkou pro posun/náklon. Zaškrtněte příslušné políčko a výběrem čísla povolte možnosti Preset Calling (Vyvolání předvolby), Patrol Calling (Vyvolání kontroly) nebo Pattern Calling (Vyvolání vzoru).
6. Nastavení můžete zkopírovat do jiných vstupů alarmu.
7. Uložte nastavení kliknutím na tlačítko **Uložit**.

5.6.4 Konfigurace v ýstupu alarmu

Postup:

1. Vstupte do rozhraní nastavení v ýstupu alarmu:
Configuration (Konfigurace) > Advanced Configuration (Rozšířená konfigurace) > Basic Event (Základní událost) > Alarm Output (V ýstup alarmu)
2. Vyberte jeden kanál v ýstupu alarmu z rozsváceno seznamu **Alarm Output** (V ýstup alarmu). Rovněž můžete nastavit název v ýstupu alarmu (volitelné).
3. Čas prodlevy může být 5 sekund, 10 sekund, 30 sekund, 1 minuta, 2 minuty, 5 minut, 10 minut nebo manuální. Čas prodleva označuje dobu, po kterou v ýstup alarmu zůstane aktivní po výskytu alarmu.
4. Kliknutím na tlačítko **Edit** (Upravit) vstupte do rozhraní úpravy času rozvrhu. Konfigurace časového rozvrhu je stejná jako nastavení rozvrhu zapnutí ochrany pro detekci pohybu. Postupujte podle 2. ikonu *Nastavení rozvrhu zapnutí ochrany pro detekci pohybu* v části 6.6.1.
5. Nastavení můžete zkopírovat do jiných výstupů alarmu.
6. Uložte nastavení kliknutím na tlačítko **Uložit**.

Alarm Output

Alarm Name (cannot copy)

Delay

Arming Schedule

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

Figure 5-53 Nastavení výstupu alarmu

5.6.5 Zpracování výjimky

Dostupné typy výjimek jsou plný pevný disk, chyba pevného disku, odpojení sítě, konflikt IP adres a neoprávněné přihlášení ke kamerám.

Postup:

1. Vstupte do rozhraní nastavení výjimek:
Configuration (Konfigurace) > Advanced Configuration (Rozšířená konfigurace) > Basic Event (Základní událost) > Exception (Výjimka)
2. Zaškrtnutím políčka nastavte akce provedené v případě alarmu v výjimce. Postupujte podle 3. úkonu *Nastavení akcí alarmu pro detekci pohybu* v části 6.6.1.

Exception Type: HDD Full	
Normal Linkage	Other Linkage
<input checked="" type="checkbox"/> Notify Surveillance Center	Trigger Alarm Output <input type="checkbox"/> Select All
<input checked="" type="checkbox"/> Send Email	<input type="checkbox"/> A->1

Save

Figure 5-54 Nastavení výjimek

3. Uložte nastavení kliknutím na tlačítko **Uložit**.

5.6.6 Konfigurace jiného alarmu

Poznámka: Některé kamery podporují bezdrátový alarm, PIR (pasivní infračervený senzor) alarm nebo nouzový alarm.

● Bezdrátový alarm

Účel:

Když je do kamery odeslán bezdrátový alarm z detektoru, např. detektoru dveřního kontaktu, aktivuje se bezdrátový alarm a může být provedena řada činností reakce.

Postup:

1. Vstupte do rozhraní nastavení bezdrátového alarmu:
Configuration (Konfigurace) > Advanced Configuration (Rozšířená konfigurace) > Basic Event (Základní událost) > Other Alarm (Jiný alarm)
2. Nastavte číslo bezdrátového alarmu.
 Podporováno je až 8 kanálů externího vstupu bezdrátového alarmu.
3. Zaškrtnutím políčka **Enable Wireless Alarm** (Povolit bezdrátový alarm) aktivujte bezdrátový alarm.
4. Zadejte název alarmu do textového pole dle potřeby.
5. Zaškrtnutím políčka vyberte metody propojení použitou pro bezdrátový alarm.
6. Uložte nastavení kliknutím na tlačítko **Uložit**.
7. Vyhledejte externí bezdrátové zařízení v blízkosti kamery a v nabídce **Configuration (Konfigurace) > Advanced Configuration (Rozšířená konfigurace) > System (Systém) > Remote Control (Dálkové ovládní)** zapněte ochranu kamery a sledování bezdrátového alarmu.

Wireless Alarm	
Select Wireless Alarm	1
<input checked="" type="checkbox"/> Enable Wireless Alarm	
Alarm Name	
Normal Linkage	Other Linkage
<input checked="" type="checkbox"/> Audible Warning	Trigger Alarm Output <input type="checkbox"/> Select All
<input checked="" type="checkbox"/> Notify Surveillance Center	<input type="checkbox"/> A->1
<input checked="" type="checkbox"/> Send Email	Trigger Wireless Alarm
<input checked="" type="checkbox"/> Upload to FTP	<input type="checkbox"/> Wireless audible and visual alarm
<input checked="" type="checkbox"/> Trigger Channel	
<input type="button" value="Save"/>	

Figure 5-55 Konfigurace nastavení bezdrátového alarmu

● PIR alarm

Účel:

PIR (Passive Infrared) alarm se aktivuje, když se narušitel pohybuje v zorném poli detektoru. Tepelná energie vyzařovaná osobou nebo jiným teplokrevným živočichem, jako psi, kočky atd., může být detekována.

Postup:

1. Vstupte do rozhraní nastavení PIR alarmu:
Configuration (Konfigurace) > Advanced Configuration (Rozšířená

konfigurace) > Basic Event (Základní událost) > Other Alarm (Jiný alarm)

2. Zaškrtnutím políčka **Enable PIR Alarm** (Povolit PIR alarm) aktivujete funkci PIR alarmu.
3. Zadejte název alarmu do textového pole dle potřeby.
4. Zaškrtnutím políčka vyberte metody propojení použité pro PIR alarm.
5. Kliknutím na tlačítko **Edit** (Upravit) nastavte rozvrh zapnutí ochrany.
6. Uložte nastavení kliknutím na tlačítko **Uložit**.
7. Přejděte do nabídky **Configuration (Konfigurace) > Advanced Configuration (Rozšířená konfigurace) > System (Systém) > Remote Control (Dálkové ovládání)** a zapněte ochranu kamery.

PIR Alarm

Enable PIR Alarm

Alarm Name

Normal Linkage	Other Linkage
<input checked="" type="checkbox"/> Audible Warning	Trigger Alarm Output <input type="checkbox"/> Select All
<input checked="" type="checkbox"/> Notify Surveillance Center	<input type="checkbox"/> A->1
<input type="checkbox"/> Send Email	Trigger Wireless Alarm
<input type="checkbox"/> Upload to FTP	<input type="checkbox"/> Wireless audible and visual alarm
<input checked="" type="checkbox"/> Trigger Channel	

Arming Schedule

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

Figure 5-56 Konfigurace nastavení PIR alarmu

● **Nouzový alarm**

Účel:

Stisknutím tlačítka Emergency na dálkovém ovladači můžete aktivovat nouzový alarm v případě nouze.

Poznámka: Pro nouzový alarm je zapotřebí dálkový ovladač. Nejprve přejděte do nabídky **Configuration (Konfigurace) > Advanced Configuration (Rozšířená konfigurace) > System (Systém) > Remote Control (Dálkové ovládání)**, abyste se na dálkový ovladač podívali.

Postup:

1. Vstupte do rozhraní nastavení nouzového alarmu:
Configuration (Konfigurace) > Advanced Configuration (Rozšířená konfigurace) > Basic Event (Základní událost) > Other Alarm (Jiný alarm)
2. Zaškrtnutím políčka vyberte metody propojení použité pro nouzový alarm.
3. Uložte nastavení kliknutím na tlačítko **Uložit**.

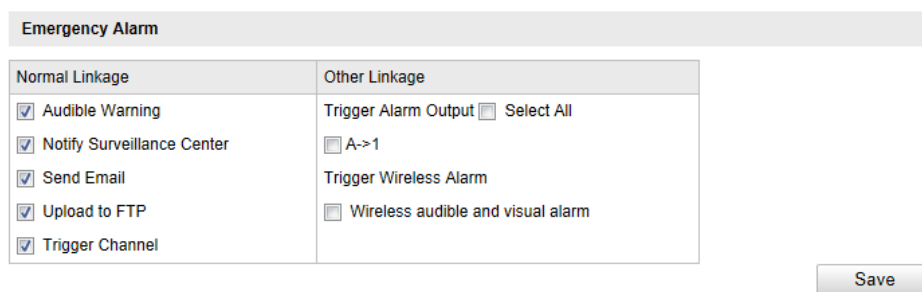


Figure 5-57 Konfigurace nastavení nouzového alarmu

5.6.7 Konfigurace detekce výjimky audia

Účel:

Funkce detekce výjimky zvuku detekuje neobvyklé zvuky ve sledované scéně, jako náhlé zvýšení/snížení intenzity zvuku, a po aktivaci alarmu mohou být provedeny určité činnosti.

Poznámka: Funkce detekce výjimky audia se liší dle různých modelů kamer.

Postup:

1. Vstupte do rozhraní nastavení detekce výjimky audia:
Configuration (Konfigurace) > Advanced Configuration (Rozšířená konfigurace) > Smart Event (Inteligentní událost) > Audio Exception Detection (Detekce výjimky audia)
2. Zaškrtnutím políčka **Audio Loss Exception (Výjimka ztráty zvuku)** povolíte

funkci detekce ztráty zvuku.

3. Zaškrtnutím políčka **Sudden Increase of Sound Intensity Detection** (Detekce náhlého zvýšení intenzity zvuku) povolíte detekci rychlého nárůstu hlasitosti zvuku ve sledované scéně. Můžete nastavit citlivost detekce a práh pro rychlý nárůst hlasitosti zvuku.
4. Zaškrtnutím políčka **Sudden Decrease of Sound Intensity Detection** (Detekce náhlého snížení intenzity zvuku) povolíte detekci rychlého poklesu hlasitosti zvuku ve sledované scéně. Můžete nastavit citlivost detekce a práh pro rychlý pokles hlasitosti zvuku.

Poznámky:

- Citlivost: Rozsah [1-100], čím nižší je hodnota, tím závažnější změna aktivuje detekci.
 - Sound Intensity Threshold (Prah intenzity zvuku): Rozsah [1-100], umožňuje filtrovat zvuk v prostředí; čím vyšší je hluk prostředí, tím vyšší by hodnota měla být. Můžete ho nastavit dle skutečného prostředí.
5. Můžete sledovat hlasitost zvuku v reálném čase.
 6. Kliknutím na tlačítko **Edit** (Upravit) nastavte rozvrh zapnutí ochrany.
 7. Vyberte metody propojení pro výjimku audia, jako informování monitorovacího centra, odeslání e-mailu, nahrání na server FTP, aktivace kanálu pro nahrávání a aktivace výstupu alarmu.
 8. Uložte nastavení kliknutím na tlačítko **Uložit**.

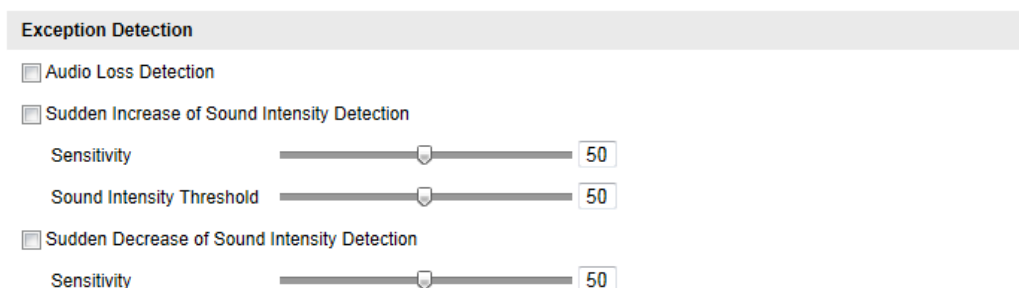


Figure 5-58 Konfigurace detekce v výjimky audia

5.6.8 Konfigurace detekce rozostření

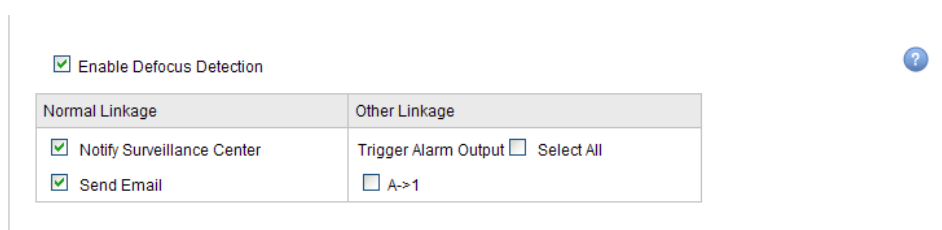
Účel:

Rozostření obrazu způsobené rozostřením objektivu může být detekováno a po aktivaci alarmu mohou být provedeny určité činnosti.

Poznámka: Funkce detekce rozostření se liší dle různých modelů kamer.

Postup:

1. Vstupte do rozhraní nastavení detekce rozostření:
Configuration (Konfigurace) > Advanced Configuration (Rozšířená konfigurace) > Smart Event (Inteligentní událost) > Defocus Detection (Detekce rozostření)
2. Povolte funkci zaškrtnutím políčka **Enable Defocus Detection** (Povolit detekci rozostření).
3. Kliknutím a posunutím posuvníku můžete nastavit citlivost detekce. Hodnota Sensitivity (Citlivost) má rozmezí od 1 do 100 a čím vyšší je, tím snáze může rozostření obrazu aktivovat alarm.
4. Vyberte metody propojení pro rozostření, jako informování monitorovacího centra, odeslání e-mailu a aktivace výstupu alarmu.
5. Uložte nastavení kliknutím na tlačítko **Uložit**.



Normal Linkage	Other Linkage
<input checked="" type="checkbox"/> Notify Surveillance Center	Trigger Alarm Output <input type="checkbox"/> Select All
<input checked="" type="checkbox"/> Send Email	<input type="checkbox"/> A->1

Figure 5-59 Konfigurace detekce rozostření

5.6.9 Konfigurace detekce změny scény

Účel:

Funkce detekce změny scény detekuje změnu sledovaného prostředí ovlivněnou vnějšími faktory, jako záměrné otočení kamery, a po aktivaci alarmu mohou být provedeny určité činnosti.

Poznámka: Funkce detekce změny scény se liší dle různých modelů kamer.

Postup:

1. Vstupte do rozhraní nastavení detekce změny scény:
Configuration (Konfigurace) > Advanced Configuration (Rozšířená konfigurace) > Smart Event (Inteligentní událost) > Scene Change Detection (Detekce změny scény)
2. Povolte funkci zaškrtnutím políčka **Enable Scene Change Detection** (Povolit detekci změny scény).
3. Kliknutím a posunutím posuvníku můžete nastavit citlivost detekce. Hodnota Sensitivity (Citlivost) má rozmezí od 1 do 100 a čím vyšší je, tím snáze může změna scény aktivovat alarm.
4. Kliknutím na tlačítko **Edit** (Upravit) nastavte rozvrh zapnutí ochrany.
5. Vyberte metody propojení pro změnu scény, jako informování monitorovacího centra, odeslání e-mailu, nahrání na server FTP, aktivace kanálu a aktivace výstupu alarmu.
6. Uložte nastavení kliknutím na tlačítko **Uložit**.



Figure 5-60 Konfigurace detekce změny scény

5.6.10 Konfigurace detekce obličeje

Účel:

Funkce detekce obličeje detekuje obličeje, které se objeví ve sledovaném záběru, a když se aktivuje tento alarm, mohou být provedeny určité činnosti.

Poznámka: Funkce detekce obličeje se liší dle různých modelů kamer.

Postup:

1. Vstupte do rozhraní nastavení detekce obličeje:
Configuration (Konfigurace) > Advanced Configuration (Rozšířená konfigurace) > Smart Event (Inteligentní událost) > Face Detection (Detekce obličeje)
2. Povolte funkci zaškrtnutím políčka **Enable Face Detection** (Povolit detekci obličeje).
3. (Volitelné) Zaškrtněte políčko **Enable Dynamic Analysis for Face Detection** (Povolit dynamickou analýzu pro detekci obličeje) a detekované obličeje budou v živém videu označeny zeleným obdélníkem.
Poznámka: Pro označení detekovaného obličeje v živém videu přejděte do nabídky **Local Configuration (Místní konfigurace) > Live View Parameters (Parametry živého náhledu)** a povolte příslušná pravidla.
4. Kliknutím a posunutím posuvníku můžete nastavit citlivost detekce.
Citlivost: Rozsah [1~5]. Čím vyšší je hodnota, tím snáze může být obličej detekován.
5. Kliknutím na tlačítko **Edit** (Upravit) nastavte rozvrh zapnutí ochrany.
6. Vyberte metody propojení pro detekci obličeje, jako informování monitorovacího centra, odeslání e-mailu, nahrání na server FTP, aktivace kanálu a aktivace výstupu alarmu.
7. Uložte nastavení kliknutím na tlačítko **Uložit**.



Figure 5-61 Konfigurace detekce obličeje

5.6.11 Konfigurace detekce překročení čáry

Účel:

Funkce detekce překročení čáry detekuje osoby, vozidla nebo jiné objekty, které překročí předem definovanou virtuální čáru, a pokud je tento alarm aktivován, mohou být provedeny určité činnosti.

Poznámka: Funkce detekce překročení čáry se liší dle různých modelů kamer.

Postup:

1. Vstupte do rozhraní nastavení detekce překročení čáry:

Configuration (Konfigurace) > Advanced Configuration (Rozšířená konfigurace) > Smart Event (Inteligentní událost) > Line Crossing Detection (Detekce překročení čáry)

2. Povolte funkci zaškrtnutím políčka **Enable Line Crossing Detection** (Povolit detekci překročení čáry).
3. Vyberte čáru z rozevřacího seznamu pro nastavení detekce.
4. Klikněte na tlačítko **Draw Area** (Nakreslit oblast) a v živém videu se zobrazí virtuální čára.
5. Tažením můžete čáru umístit do živého videa dle potřeby. Klikněte na čáru se zobrazenými červenými čtverečky na obou koncích a tažením červených čtverečků definujte tvar a délku čáry.
6. Vyberte směr detekce překročení čáry. Můžete vybrat směry **A<->B**, **A->B** a **B->A**.
A<->B: Pouze šipka na straně B ukazuje, kdy může být detekován objekt překračující rovinu oběma směry a aktivují se alarmy.
A->B: Detekován může být pouze objekt překračující nakonfigurovanou čáru ze strany A na stranu B.
B->A: Detekován může být pouze objekt překračující nakonfigurovanou čáru ze strany B na stranu A.
7. Kliknutím a posunutím posuvníku můžete nastavit citlivost detekce.
Citlivost: Rozsah [1~100]. Čím vyšší je hodnota, tím snáze může být akce překročení čáry detekována.
8. Opakováním výše uvedeného postupu nakonfigurujte další čáry. Lze nakonfigurovat až 4 čáry. Můžete kliknout na tlačítko **Clear** (Smazat) a vymazat všechny předem definované čáry.
9. Kliknutím na tlačítko **Edit** (Upravit) nastavte rozvrh zapnutí ochrany.
10. Vyberte metody propojení pro detekci překročení čáry, jako informování monitorovacího centra, odeslání e-mailu, nahrání na server FTP, aktivace kanálu a aktivace vstupu alarmu.
11. Uložte nastavení kliknutím na tlačítko **Uložit**.

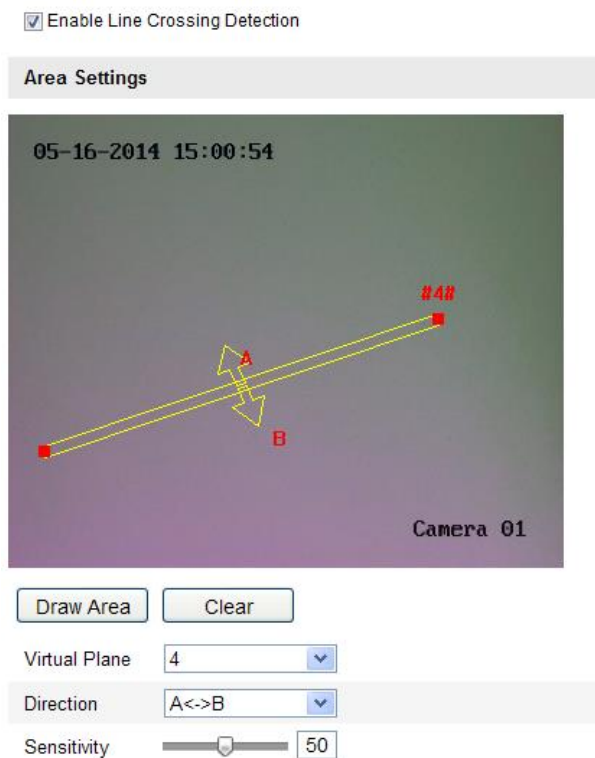


Figure 5-62 Nakreslení čáry překročení

5.6.12 Konfigurace detekce narušení

Účel:

Funkce detekce narušení detekuje osoby, vozidla nebo jiné objekty, které vstoupí do předem definované virtuální oblasti a pohybují se v ní a pokud je tento alarm aktivován, mohou být provedeny určité činnosti.

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

Postup:

1. Vstupte do rozhraní nastavení detekce narušení:
Configuration (Konfigurace) > Advanced Configuration (Rozšířená konfigurace) > Smart Event (Inteligentní událost) > Intrusion Detection (Detekce narušení)
2. Povolte funkci zaškrtnutím políčka **Enable Intrusion Detection** (Povolit detekci narušení).
3. Vyberte oblast z rozevřacího seznamu pro nastavení detekce.

4. Klikněte na tlačítko **Draw Area** (Nakreslit oblast) a začněte kreslit oblast.
5. Klikněte na živé video a určete čtyři body pro oblast detekce. Kreslení dokončete kliknutím pravým tlačítkem.
6. Nastavte práh času, citlivost detekce a procentuální podíl objektu pro detekci narušení.

Threshold (Prah): Rozsah [0s-10s], práh času, po který se objekt pohybuje v oblasti. Pokud nastavíte hodnotu 0, alarm se aktivuje ihned poté co objekt vstoupí do oblasti.

Citlivost: Rozsah [1--100]. Hodnota citlivosti určuje velikost objektu, který může alarm aktivovat. Když je citlivost vysoká, může alarm aktivovat i velmi malý objekt.

Percentage (Procentní podíl): Rozsah [1--100]. Procentuální podíl určuje poměr části objektu v oblasti, který může aktivovat alarm. Například pokud je procentuální podíl nastavený na 50 %, když objekt vstoupí do oblasti a obsadí polovinu celé oblasti, alarm se aktivuje.

7. Opakováním výše uvedeného postupu nakonfigurujte další oblasti. Lze nakonfigurovat až 4 oblasti. Můžete kliknout na tlačítko **Clear** (Smazat) a vymazat všechny předem definované oblasti.
8. Kliknutím na tlačítko **Edit** (Upravit) nastavte rozvrh zapnutí ochrany.
9. Vyberte metody propojení pro detekci narušení, jako informování monitorovacího centra, odeslání e-mailu, nahrání na server FTP, aktivace kanálu a aktivace výstupu alarmu.
10. Uložte nastavení kliknutím na tlačítko **Uložit**.

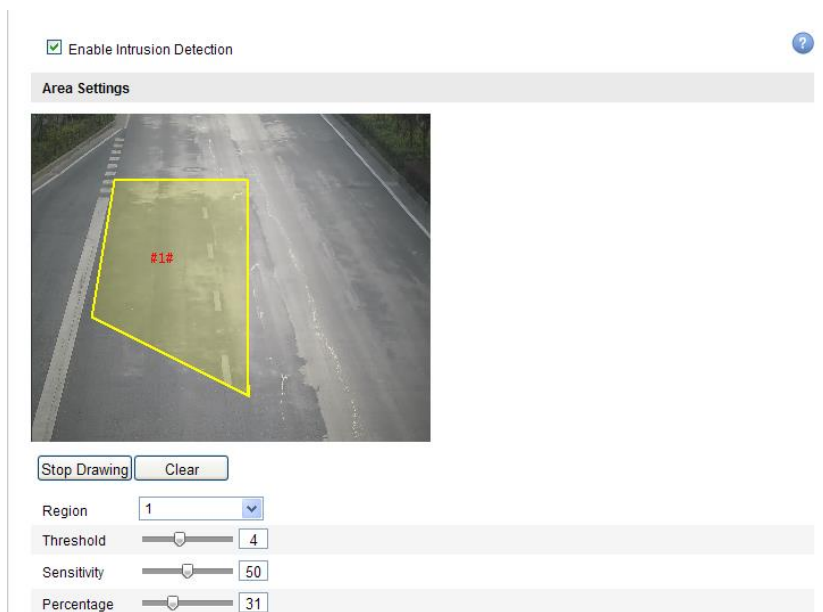


Figure 5-63 Konfigurace oblasti narušení

5.6.13 Konfigurace detekce vstupu do oblasti

Účel:

Funkce vstupu do oblasti detekuje osoby, vozidla nebo jiné objekty, které vstoupí zvnějšku do předem definované virtuální oblasti, a pokud je tento alarm aktivován, mohou být provedeny určité činnosti.

Poznámka: Funkce detekce vstupu do oblasti se liší dle různých modelů kamer.

Postup:

1. Vstupte do rozhraní nastavení detekce vstupu do oblasti:
Configuration (Konfigurace) > Advanced Configuration (Rozšířená konfigurace) > Smart Event (Inteligentní událost) > Region Entrance Detection (Detekce vstupu do oblasti)
2. Povolte funkci zaškrtnutím políčka **Enable Region Entrance Detection** (Povolit detekci vstupu do oblasti).
3. Vyberte oblast z rozevřacího seznamu pro nastavení detekce.
4. Klikněte na tlačítko **Draw Area** (Nakreslit oblast) a začněte kreslit oblast.
5. Klikněte na živé video a určete čtyři body pro oblast detekce. Kreslení dokončete kliknutím pravým tlačítkem.

6. Kliknutím a posunutím posuvníku můžete nastavit citlivost detekce.
Citlivost: Rozsah [1~100]. Hodnota citlivosti určuje velikost objektu, který může alarm aktivovat. Když je citlivost vysoká, může alarm aktivovat i velmi malý objekt, který vstoupí do oblasti.
7. Opakováním výše uvedeného postupu nakonfigurujte další oblasti. Lze nakonfigurovat až 4 oblasti. Můžete kliknout na tlačítko Clear (Smazat) a vymazat všechny předem definované oblasti.
8. Kliknutím na tlačítko **Edit** (Upravit) nastavte rozvrh zapnutí ochrany.
9. Vyberte metody propojení pro detekci vstupu do oblasti, jako informování monitorovacího centra, odeslání e-mailu, nahrání na server FTP, aktivace kanálu a aktivace výstupu alarmu.
10. Uložte nastavení kliknutím na tlačítko **Uložit**.

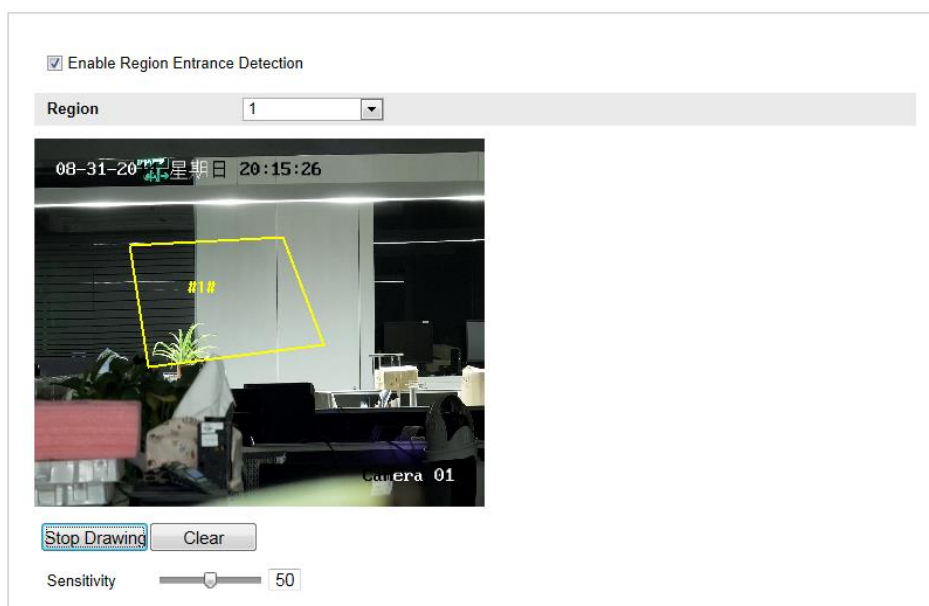


Figure 5-64 Konfigurace detekce vstupu do oblasti

5.6.14 Konfigurace detekce opuštění oblasti

Účel:

Funkce detekce opuštění oblasti detekuje osoby, vozidla nebo jiné objekty, které opustí předem definovanou virtuální oblast, a pokud je tento alarm aktivován, mohou být provedeny určité činnosti.

Poznámka: Funkce detekce opuštění oblasti se liší dle různých modelů kamer.

Postup:

1. Vstupte do rozhraní nastavení detekce opuštění oblasti:
Configuration (Konfigurace) > Advanced Configuration (Rozšířená konfigurace) > Smart Event (Inteligentní událost) > Region Exiting Detection (Detekce opuštění oblasti)
2. Povolte funkci zaškrtnutím políčka **Enable Region Exiting Detection** (Povolit detekci opuštění oblasti).
3. Vyberte oblast z rozevřacích seznamů pro nastavení detekce.
4. Klikněte na tlačítko **Draw Area** (Nakreslit oblast) a začněte kreslit oblast.
5. Klikněte na živé video a určete čtyři body pro oblast detekce. Kreslení dokončete kliknutím pravým tlačítkem.
6. Kliknutím a posunutím posuvníku můžete nastavit citlivost detekce.
Citlivost: Rozsah [1~100]. Hodnota citlivosti určuje velikost objektu, který může alarm aktivovat. Když je citlivost vysoká, může alarm aktivovat i velmi malý objekt, který opustí oblast.
7. Opakováním výše uvedeného postupu nakonfigurujte další oblasti. Lze nakonfigurovat až 4 oblasti. Můžete kliknout na tlačítko **Clear** (Smazat) a vymazat všechny předem definované oblasti.
8. Kliknutím na tlačítko **Edit** (Upravit) nastavte rozvrh zapnutí ochrany.
9. Vyberte metody propojení pro detekci opuštění oblasti, jako informování monitorovacího centra, odeslání e-mailu, nahrání na server FTP, aktivace kanálu a aktivace výstupu alarmu.
10. Uložte nastavení kliknutím na tlačítko **Uložit**.

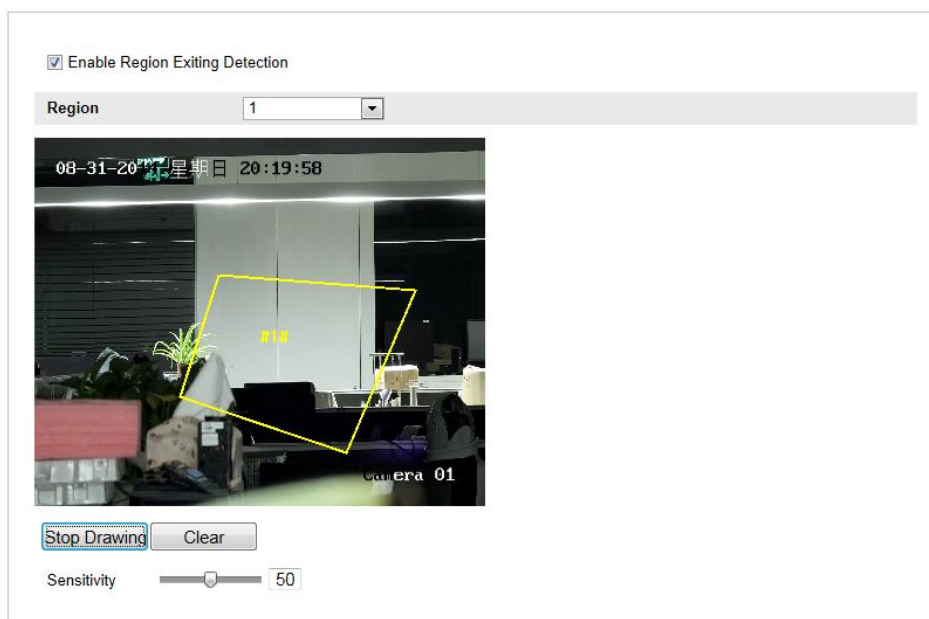


Figure 5-65 Konfigurace detekce opuštění oblasti

5.6.15 Konfigurace detekce opuštěného zavazadla

Účel:

Funkce detekce opuštěného zavazadla detekuje objekty ponechané v předem definované oblasti, jako zavazadla, kabelky, nebezpečné materiály atd., a po aktivaci alarmu může být provedena řada činností.

Poznámka: Funkce detekce opuštěného zavazadla se liší dle různých modelů kamer.

Postup:

1. Vstupte do rozhraní nastavení detekce opuštěného zavazadla:
Configuration (Konfigurace) > Advanced Configuration (Rozšířená konfigurace) > Smart Event (Inteligentní událost) > Unattended Baggage Detection (Detekce opuštěného zavazadla)
2. Povolte funkci zaškrtnutím políčka **Enable Unattended Baggage Detection** (Povolit detekci opuštěného zavazadla).
3. Vyberte oblast z rozevřacího seznamu pro nastavení detekce.
4. Klikněte na tlačítko **Draw Area** (Nakreslit oblast) a začněte kreslit oblast.
5. Klikněte na živé video a určete čtyři body pro oblast detekce. Kreslení dokončete kliknutím pravým tlačítkem.

6. Nastavte práh času a citlivost detekce pro detekci opuštěného zavazadla.

Threshold (Práh): Rozsah [5s-20s], práh času, po který je objekt ponechán v oblasti. Pokud nastavíte hodnotu 10, alarm se aktivuje, když objekt je ponechán a zůstane v oblasti po dobu 10 sekund.

Citlivost: Rozsah [1~100]. Hodnota Sensitivity (Citlivost) určuje stupeň podobnosti obrazu na pozadí. Když je citlivost vysoká, může alarm aktivovat i velmi malý objekt ponechaný v oblasti.
7. Opakováním výše uvedeného postupu nakonfigurujte další oblasti. Lze nakonfigurovat až 4 oblasti. Můžete kliknout na tlačítko Clear (Smazat) a vymazat všechny předem definované oblasti.
8. Kliknutím na tlačítko **Edit** (Upravit) nastavte rozvrh zapnutí ochrany.
9. Vyberte metody propojení pro detekci opuštěného zavazadla, jako informování monitorovacího centra, odeslání e-mailu, nahrání na server FTP, aktivace kanálu a aktivace výstupu alarmu.
10. Uložte nastavení kliknutím na tlačítko **Uložit**.

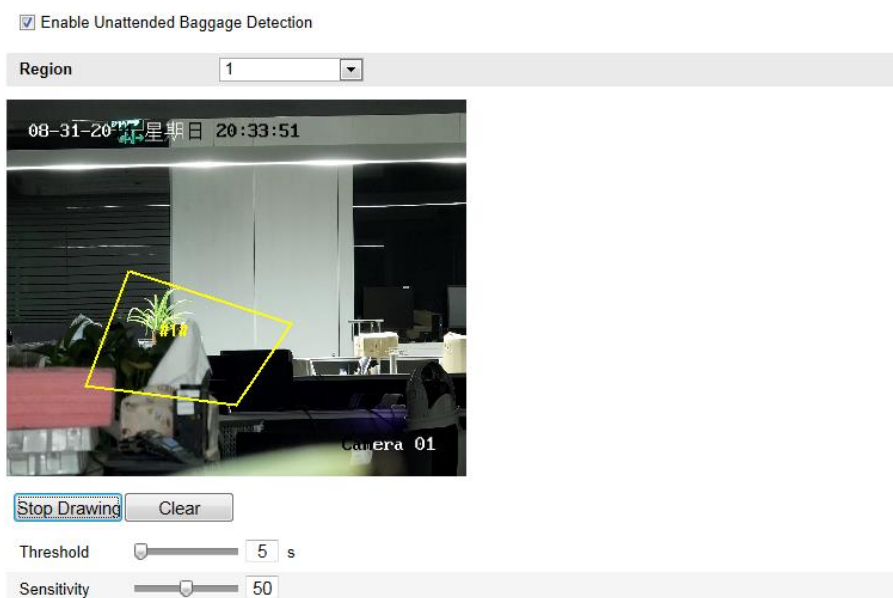


Figure 5-66 Konfigurace opuštěného zavazadla

5.6.16 Konfigurace detekce odstranění předmětu

Účel:

Funkce detekce odstranění předmětu detekuje objekty odstraněné z předem definované oblasti, jako vystavené exponáty, a po aktivaci alarmu může být provedena řada činností.

Poznámka: Funkce detekce odstranění předmětu se liší dle různých modelů kamer.

Postup:

1. Vstupte do rozhraní nastavení detekce odstranění předmětu:
Configuration (Konfigurace) > Advanced Configuration (Rozšířená konfigurace) > Smart Event (Inteligentní událost) > Object Removal Detection (Detekce odstranění předmětu)
2. Povolte funkci zaškrtnutím políčka **Enable Object Removal Detection** (Povolit detekci odstranění předmětu).
3. Vyberte oblast z rozevřacího seznamu pro nastavení detekce.
4. Klikněte na tlačítko **Draw Area** (Nakreslit oblast) a začněte kreslit oblast.
5. Klikněte na živé video a určete čtyři body pro oblast detekce. Kreslení dokončete kliknutím pravým tlačítkem.
6. Nastavte práh času a citlivost detekce pro detekci odstranění předmětu.
Threshold (Prah): Rozsah [5s-20s], práh času, po který je objekt odstraněn z oblasti. Pokud nastavíte hodnotu 10, alarm se aktivuje, když objekt zmizí z oblasti na 10 sekund.
Citlivost: Rozsah [1~100]. Hodnota Sensitivity (Citlivost) určuje stupeň podobnosti obrazu na pozadí. Když je citlivost vysoká, může alarm aktivovat i velmi malý objekt odstraněný z oblasti.
7. Opakováním výše uvedeného postupu nakonfigurujte další oblasti. Lze nakonfigurovat až 4 oblasti. Můžete kliknout na tlačítko Clear (Smazat) a vymazat všechny předem definované oblasti.
8. Kliknutím na tlačítko **Edit** (Upravit) nastavte rozvrh zapnutí ochrany.
9. Vyberte metody propojení pro detekci odstranění předmětu, jako informování

monitorovacího centra, odeslání e-mailu, nahrání na server FTP, aktivace kanálu a aktivace výstupu alarmu.

10. Uložte nastavení kliknutím na tlačítko **Uložit**.

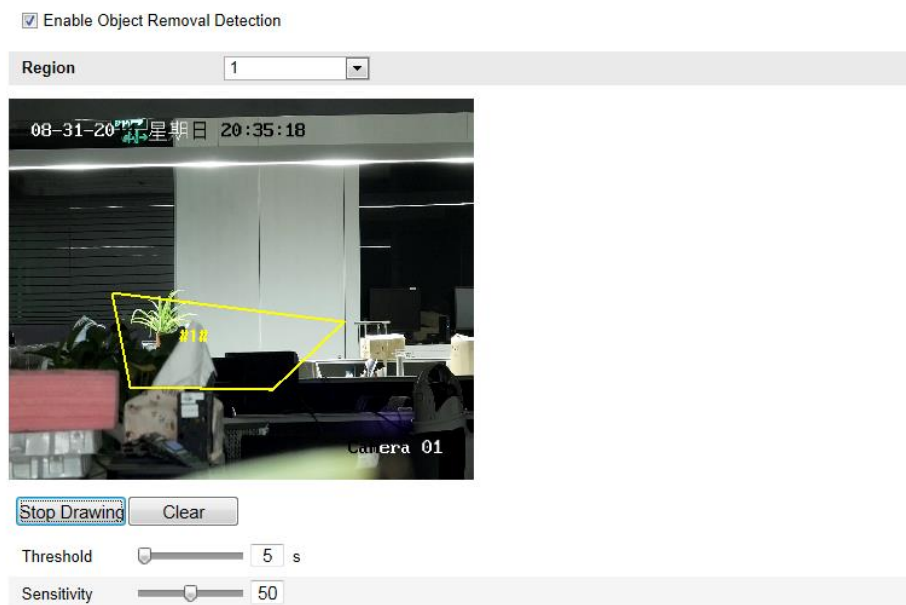


Figure 5-67 Konfigurace detekce odstranění předmětu

5.7 Konfigurace VCA

5.7.1 Analýza chování

Analýza chování detekuje podezřelé chování a po aktivaci alarmu budou povoleny určité metody propojení.

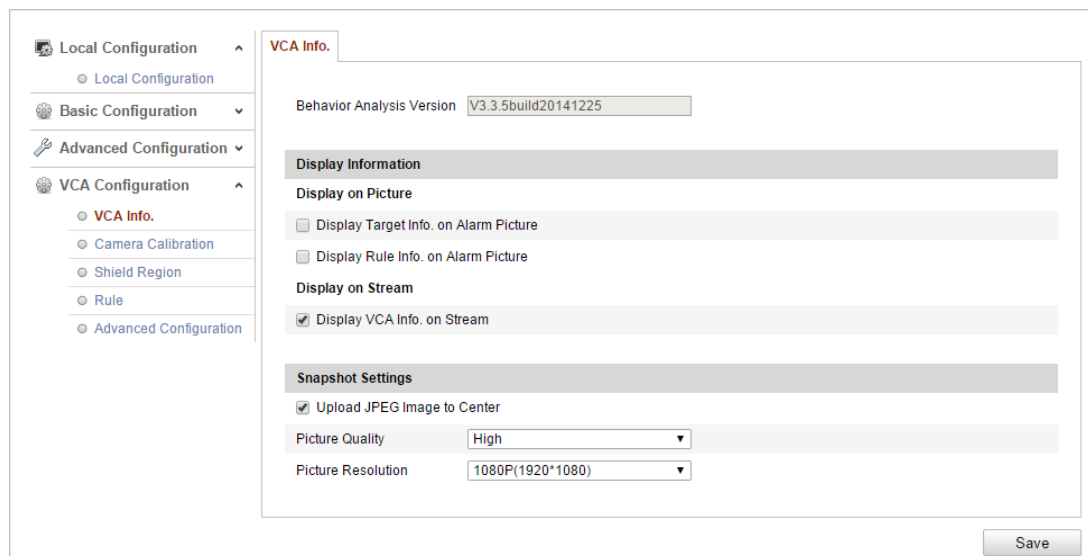


Figure 5-68 Analýza chování

❖ VCA info

Behavior Analysis Version (Verze analýzy chování): Uvádí verzi knihovny algoritmů. Zobrazené informace zahrnují zobrazenív obrázku a zobrazeníve streamu.

Display Target info. on Alarm Picture (Zobrazit info o cíli na obrázku alarmu): Pokud je toto políčko zaškrtnuté, kolem cíle na nahraném obrázku alarmu bude rámeček.

Display Rule info. on Alarm Picture (Zobrazit info o pravidlu na snímku alarmu): Zachycený cíl a nakonfigurovaná oblast na obrázku alarmu budou označeny rámečkem.

Display VCA info. on Stream (Zobrazit info o VCA ve streamu): Při živém náhledu nebo přehrávání budou na cíli zobrazeny zelené rámečky.

Poznámka: Ujistěte se, že jsou v místních nastaveních povolena pravidla. Přejděte do nabídky **Configuration** (Konfigurace) > **Local Configuration** (Místní konfigurace) > **Rules** (Pravidla) a povolte je.

Snapshot Setting (Nastavení snímku): Můžete nastavit kvalitu a rozlišení pořízeného snímku.

Upload JPEG Image to Center (Odeslat obrázek JPEG do centra): Pokud zaškrtnete toto políčko, pořízený snímek bude odeslán do monitorovacího centra, když nastane alarm VCA.

Picture Quality (Kvalita obrázku): Lze vybrat z možností High (Vysoká), Medium (Střední) a Low (Nízká).

Picture Resolution (Rozlišení obrázku): Lze vybrat z možností CIF, 4CIF, 720P a 1080P.

❖ **Kalibrace kamery**

Proveďte následující postup pro trojrozměrné měření a kvantizaci obrazu z kamery a následný výpočet velikosti všech cílů. Detekce VCA bude přesnější, pokud je nakonfigurovaná kalibrace kamery.

Postup:

1. Zaškrtnutím políčka **Camera Calibration** (Kalibrace kamery) povolte tuto funkci.
2. Vyberte režim kalibrace Input Basic Data (Zadat základní data) nebo Draw on Live View Video (Nakreslit ve videu živého náhledu).

Input Basic Data (Zadat základní data): Zadejte výšku upevnění, úhel pohledu a poměr horizontu kamery ručně.

Draw on Live View Video (Nakreslit ve videu živého náhledu): Klikněte na tlačítko **Draw Verification Line (Horizontal) / (Vertical)** (Nakreslit ověřovací čáru (vodorovnou) / (svislou)), nakreslete vodorovnou/svislou čáru v živém náhledu a zadejte skutečnou délku do pole Real Length (Skutečná délka). S nakreslenými referenčními čarami a jejich skutečnou délkou může kamera odhalit jiné objekty, které se objeví v živém náhledu.

3. (Volitelné) Zaškrtněte políčko **Enable Verification of Camera Calibration** (Povolit ověření kalibrace kamery), klikněte na tlačítko **Horizontal Verify / Vertical Verify** (Vodorovné ověření / Svislé ověření) a nakreslete vodorovnou/svislou čáru v živém videu; poté klikněte na tlačítko **Calibrate** (Kalibrovat) pro výpočet délky čáry. Porovnáním vypočítané délky čáry se skutečnou délkou ověřte nastavené kalibrační informace.
4. Můžete kliknout na tlačítko **Delete** (Odstranit) a odstranit nakreslené čáry.
5. Uložte nastavení kliknutím na tlačítko **Uložit**.

Poznámka: Pokud je živý náhled zastavený, kalibrace kamery je neplatná

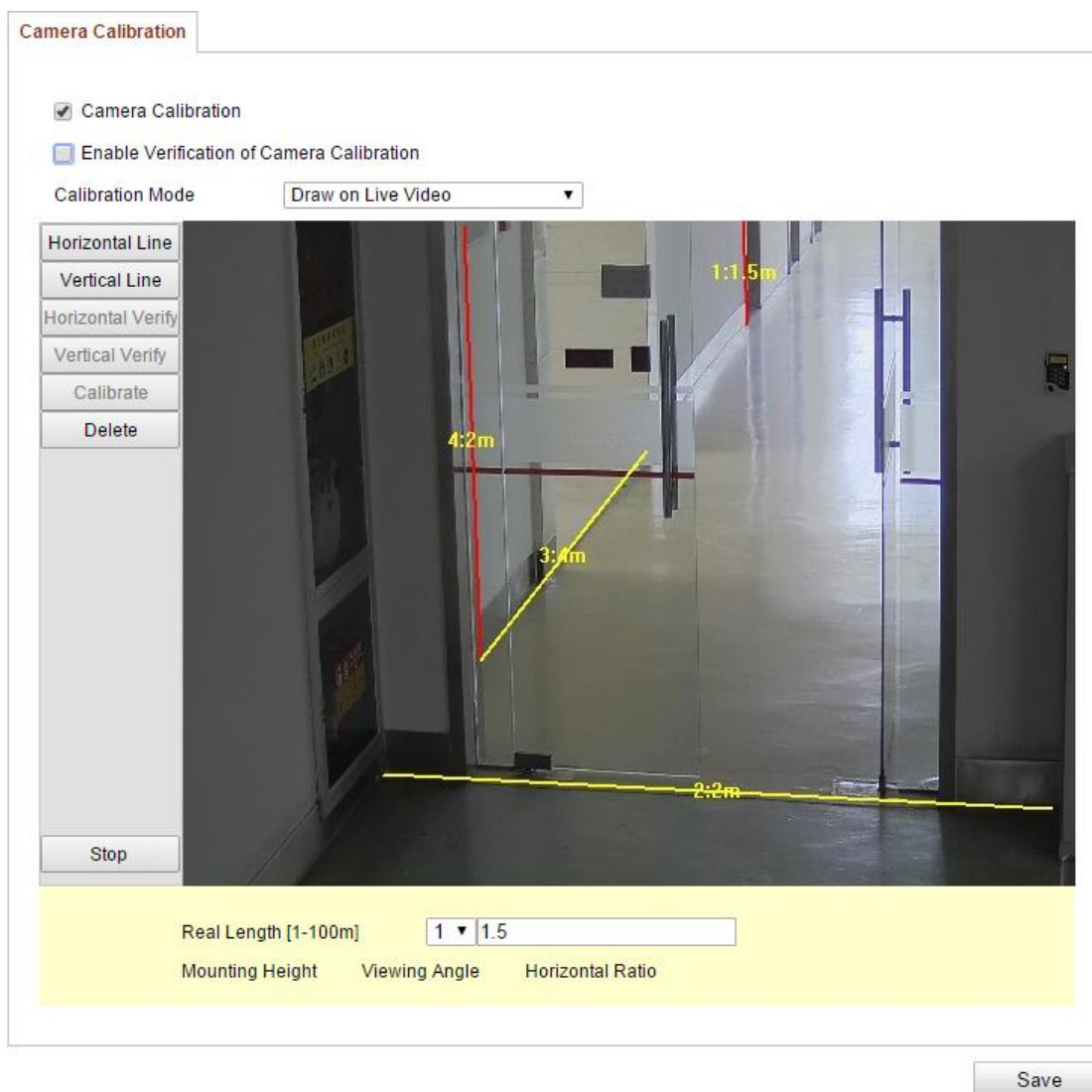


Figure 5-69 Nakreslení ve videu živého náhledu

❖ Oblast mimo detekci

Oblast mimo detekci vám umožňuje nastavit konkrétní oblast, ve které analýza chování nebude fungovat. Podporovány jsou až 4 oblasti mimo detekci.

Postup:

1. Klikněte na kartu **Shield Region** (Oblast mimo detekci) a vstupte do rozhraní konfigurace oblasti mimo detekci.
2. Klikněte na tlačítko **Draw Area** (Nakreslit oblast). Nakreslete oblast zanesením koncových bodů levým tlačítkem do okna živého náhledu a kliknutím pravým tlačítkem kreslení oblasti dokončete.

Poznámky:

- Podporované jsou mnohoúhelníkové oblasti s až 10 stranami.

- Kliknutím na tlačítko **Delete** (Odstranit) odstraní nakreslenou oblast.
- Pokud je živý náhled zastavený, nelze oblast mimo detekci nakreslit.

3. Uložte nastavení kliknutím na tlačítko **Uložit**.

❖ **Pravidlo**

Analýza chování podporuje různá chování, včetně detekce překročení čáry, narušení, vstupu do oblasti a opuštění oblasti atd.

Poznámka: Podrobné informace o jednotlivých detekcích jsou uvedeny v příslušných kapitolách.

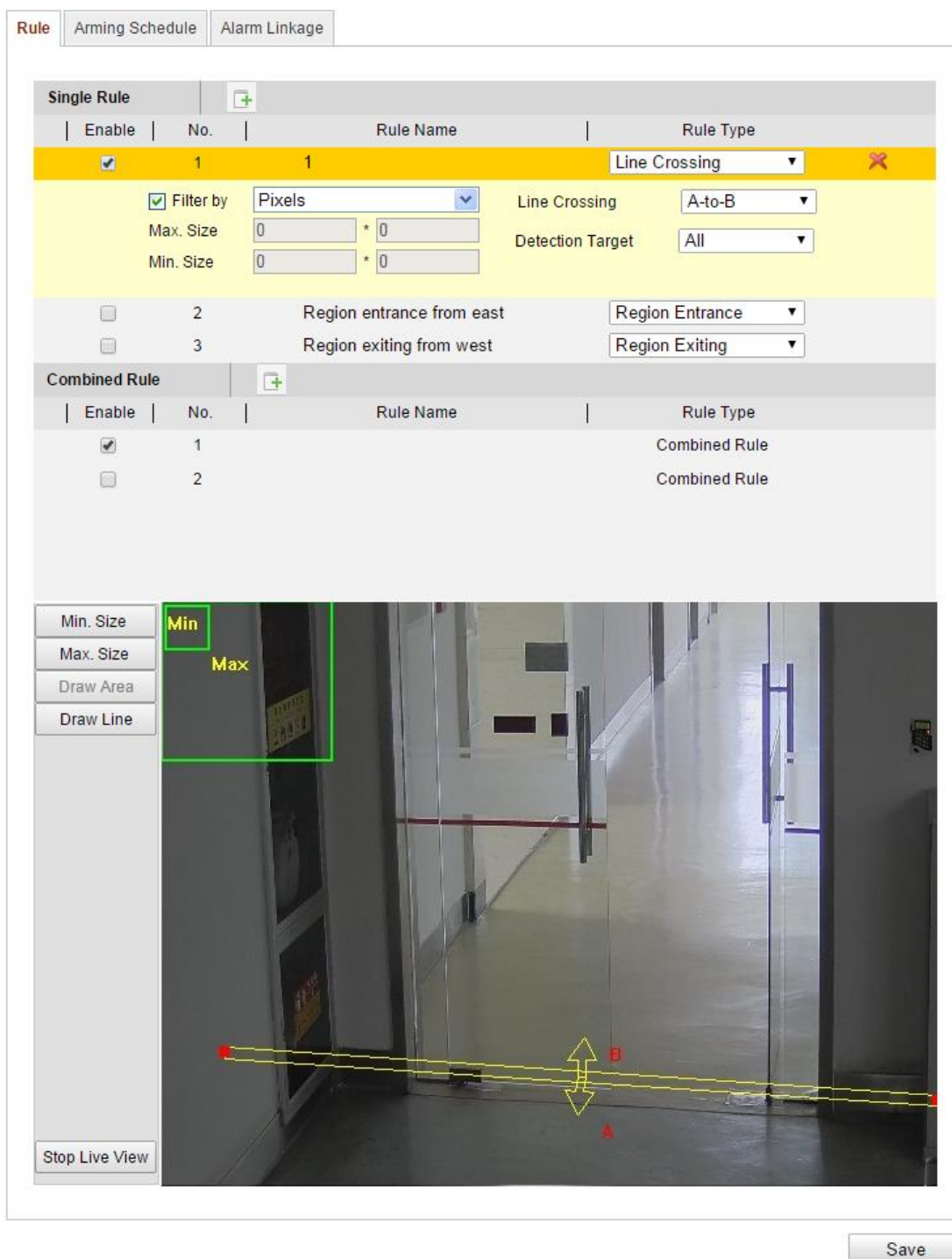


Figure 5-70 Konfigurace pravidla

Postup:

1. Klikněte na kartu **Rule** (Pravidlo) a vstupte do rozhraní konfigurace pravidel.
2. Zaškrtnutím políčka jednotlivého pravidla povolíte příslušné pravidlo pro analýzu chování.
3. Vyberte typ pravidla, nastavte typ filtru a poté nakreslete čáru/oblast v živém náhledu pro jednotlivé pravidlo.

Filter type (Typ filtru): Lze vybrat z možností Pixels (Pixely) a Actual Size (Skutečná velikost). Pokud je vybraná možnost Pixels, nakreslete oblast maximální velikosti a minimální velikosti pro každé pravidlo do živého videa. Pokud je vybraná možnost Actual Size, zadejte délku a šířku maximální a minimální velikosti. Alarm aktivují pouze cíle, jejichž velikost je mezi minimální a maximální hodnotou.

Poznámka: Pokud je vybraná skutečná velikost, ujistěte se, že je nakonfigurovaná kalibrace kamery.

Detection Target (Cíl detekce): Jako cíl detekce vyberte možnost Human (Člověk) nebo Vehicle (Vozidlo). Můžete také vybrat možnost All (Vše) a jako cíl budou detekovány všechny objekty.

Draw line / area (Nakreslit čáru / oblast): Pro detekci překročení čáry je třeba nakreslit čáru a vybrat směr překročení z možností obousměrné, A-do-B nebo B-do-A. V případě jiných událostí, jako narušení, vstup do oblasti, opuštění oblasti atd. je třeba kliknout levým tlačítkem do živého videa a nastavit koncové body oblasti a kliknutím pravým tlačítkem kreslení oblasti dokončit.

Poznámka: Pokud je živý náhled zastavený, oblast/čáru detekce nelze nakreslit a pravidla nelze nastavit.

4. Zaškrtnutím políčka kombinovaného pravidla povolíte příslušné pravidlo pro analýzu chování
5. Vyberte dvě nakonfigurovaná jednotlivá pravidla jako pravidlo A a pravidlo B kombinovaného pravidla, nastavte minimální a maximální časový interval pro obě jednotlivá pravidla a poté vyberte pořadí aktivace jednotlivých pravidel pro filtrování alarmů.

Poznámky:

- Pokud vyberte typ pravidla None (Žádné), volba pravidla je neplaná a analýza chování nelze nakonfigurovat.
- Pořadí aktivace jednotlivých pravidel pro filtrování alarmů lze nastavit z možností In Ascending Order (Ve vzestupném pořadí) nebo In Ascending/Descending Order (Ve vzestupném/sestupném pořadí).
- Lze nakonfigurovat až 8 jednotlivých pravidel a 2 kombinovaná pravidla. V případě kombinovaných pravidel je podporováno překročení čáry, narušení, opuštění oblasti a vstup do oblasti.

6. Uložte nastavení kliknutím na tlačítko **Uložit**.
7. Klikněte na kartu **Arming Schedule** (Rozvrh zapnutí ochrany), klikněte na tlačítko **Edit** (Upravit) a nastavte čas pro jednotlivá pravidla. Nastavení uložte kliknutím na tlačítko **Save** (Uložit).
8. Klikněte na kartu **Alarm linkage** (Propojení alarmu), zaškrtněte políčko příslušné metody propojení pro jednotlivá pravidla a uložte nastavení kliknutím na tlačítko **Save** (Uložit).

❖ Rozšířená konfigurace

- **Parametr**

Nakonfigurujte následující parametry podrobné konfigurace.

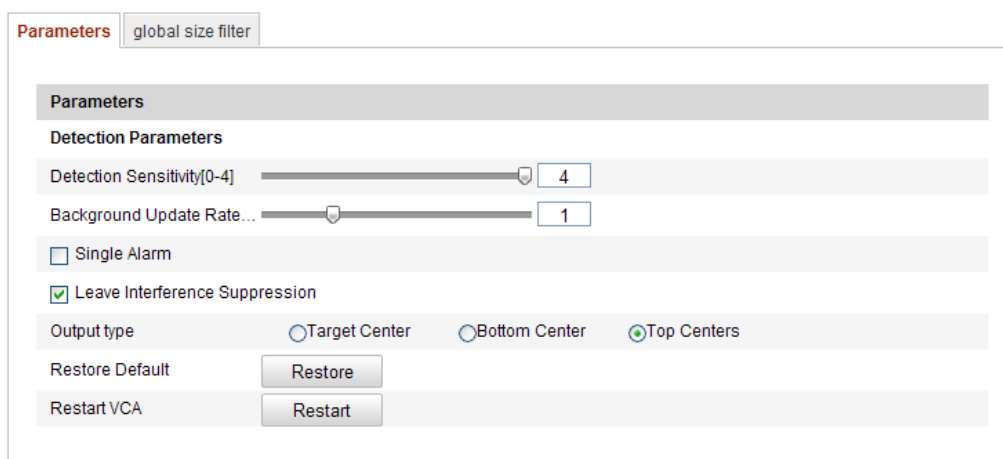


Figure 5-71 Rozšířená konfigurace

Detection Sensitivity (Citlivost detekce) [0~4]: Označuje citlivost detekce cíle kamerou. Čím vyšší je hodnota, tím snáze bude cíl rozpoznán a tím vyšší je pravděpodobnost chybné informace. Doporučujeme použít výchozí hodnotu 3.

Background Update Rate (Frekvence aktualizace pozadí) [0~4]: Označuje rychlost, jakou nová scéna nahradí předchozí scénu. Doporučujeme použít výchozí hodnotu 3.

Jediný alarm: Pokud je vybrán jediný alarm, cíl v nakonfigurované oblasti aktivuje alarm pouze jednou. Pokud není zaškrtnuto, stejný cíl v téže nakonfigurované oblasti způsobí neustálý alarm.

Leave Interference Suppression (Potlačení rušení listy): Zaškrtnutím tohoto políčka potlačíte rušení způsobované listy v nakonfigurované oblasti.

Output Type (Druh výstupu): Vyberte pozici rámečku. Lze vybrat z možností Target Center (Střed cíle), Bottom Center (Dole uprostřed) a Top Center (Nahore uprostřed).

Např.: Pokud je vybraná možnost Target Center, cíl bude uprostřed záběru.

Restore Default (Obnovit výchozí): Kliknutím obnovíte nakonfigurované parametry na výchozí hodnoty.

Restart VCA (Restartovat VCA): Restartování knihovny algoritmů analýzy chování.

- Global Size Filter (Globální filtr rozměrů)

Poznámka: Ve srovnání s filtrem velikosti pod pravidlem, který je zaměřený na jednotlivá pravidla, globální filtr rozměrů je zaměřený na všechna pravidla.

Postup:

1. Povolte funkci zaškrtnutím políčka **Global Size Filter** (Globální filtr rozměrů).
2. Vyberte typ filtru z možností Actual Size (Skutečná velikost) nebo Pixel.

Actual Size (Skutečná velikost): Zadejte délku a šířku maximální i minimální velikosti. Alarm aktivují pouze cíle, jejichž velikost je mezi minimální a maximální hodnotou.

Poznámky:

- Pokud vyberete filtr podle skutečné velikosti, musí být nastavená kalibrace kamery.
- Délka maximální velikosti by měla být delší než délka minimální velikosti, a stejně tak šířka.

Pixel: Klikněte na položku Minimum Size (Minimální velikost) a nakreslete obdélník minimální velikosti v živém náhledu. Poté klikněte na položku Maximum Size (Maximální velikost) a nakreslete obdélník maximální velikosti v živém náhledu. Cíle menší než minimální velikost nebo větší než maximální velikost budou filtrovány.

Poznámky:

- Nakreslená oblast bude algoritmem pozadí převedena na pixely.
- Globální filtr rozměrů nelze nakonfigurovat, pokud je živý náhled zastavený.
- Délka maximální velikosti by měla být delší než délka minimální velikosti,

a stejně tak šířka.

3. Uložte nastavení kliknutím na tlačítko **Uložit**.

5.7.2 Zachycení obličeje

Zachycení obličeje může zachytit obličej, který se objeví v nakonfigurované oblasti, a se zachyceným snímkem budou odeslány také informace o charakteru obličeje, jako věk, pohlaví a nošení či nenošení brýlí.

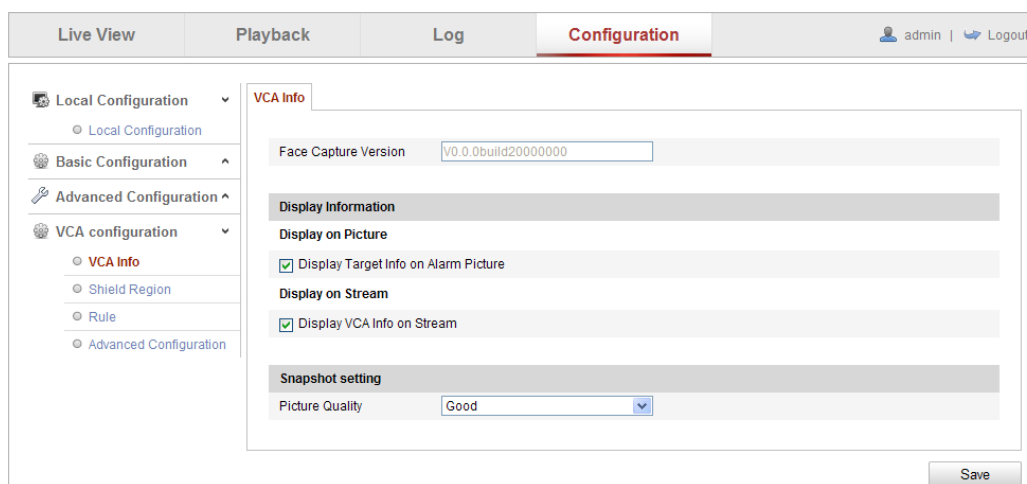


Figure 5-72 Zachycení obličeje

❖ VCA info

Face Capture Version (Verze zachycení obličeje): Uvádí verzi knihovny algoritmů.

Zobrazené informace zahrnují zobrazenív obrázku a zobrazeníve streamu.

Display Target info. on Alarm Picture (Zobrazit info o cíli na obrázku alarmu):

Pokud je toto políčko zaškrtnuté, kolem cíle na nahraném obrázku alarmu bude rámeček.

Display VCA info. on Stream (Zobrazit info o VCA ve streamu): Při živém náhledu nebo přehrávání budou na cíli zobrazeny zelené rámečky.

Snapshot Setting (Nastavení snímku): Vyberte kvalitu obrazu zachyceného snímku.

Lze vybrat z možností Good (Dobrá), Better (Lepší) a Best (Nejlepší).

❖ Oblast mimo detekci

Oblast mimo detekci vám umožňuje nastavit konkrétní oblast, ve které zachycení obličeje nebude fungovat. Podporovány jsou až 4 oblasti mimo detekci.

Postup:

1. Klikněte na kartu **Shield Region** (Oblast mimo detekci) a vstupte do rozhraní konfigurace oblasti mimo detekci.
2. Klikněte na tlačítko **Draw Area** (Nakreslit oblast). Nakreslete oblast zanesením čtyř koncových bodů levým tlačítkem do okna živého náhledu a kliknutím pravým tlačítkem kreslení oblasti dokončete.

Poznámky:

- Kliknutím na tlačítko **Delete** (Odstranit) odstraní nakreslené oblasti.
 - Pokud je živý náhled zastavený, nelze oblasti mimo detekci nakreslit.
3. Uložte nastavení kliknutím na tlačítko **Uložit**.

❖ **Pravidlo**

Postup:

1. Zaškrtnutím políčka **Rule** (Pravidlo) povolte pravidla zachycení obličeje.
2. Klikněte na tlačítko **Minimize Pupil Distance** (Minimalizovat vzdálenost zornic) a nakreslete minimální vzdálenost zornic. Vzdálenost nakreslených zornic bude zobrazena v poli pod živým náhledem.

Minimální vzdálenost zornic označuje minimální velikost čtverce tvořeného oblastí mezi oběma zornicemi a jde o základní standard pro identifikaci cíle kamerou.

3. Kliknutím na tlačítko **Draw Area** (Nakreslit) oblast nakreslete oblast, ve které se má zachycení obličeje použít. Nakreslete oblast zanesením koncových bodů levým tlačítkem do okna živého náhledu a kliknutím pravým tlačítkem kreslení oblasti dokončete.

Poznámky:

- Podporovaná je mnohoúhelníková oblast (4 až 10 stran).
 - Pokud je živý náhled zastavený, nelze nakonfigurovanou oblast nakreslit.
4. Uložte nastavení kliknutím na tlačítko **Uložit**.

❖ **Rozšířená konfigurace**

Nakonfigurujte následující parametry dle skutečného prostředí.

Parametry detekce:

Generation Speed (Rychlost generování) [1~5]: Rychlost identifikace cíle. Čím je

hodnota vyšší, tím rychleji bude cíl rozpoznán. Pokud je hodnota nastavená relativně nízko a obličej byl v nakonfigurované oblasti od začátku, nebude zachycen. Umožňuje omezit chybné informace o obličejích na obrazech nebo plakátech. Doporučujeme použít výchozí hodnotu 3.

Capture Times (Časy zachytávání) [1~10]: Označuje čas, po kterém bude obličej zachycen při setrvání v nakonfigurované oblasti. Výchozí hodnota je 1.

Sensitivity (Citlivost) [1~5]: Citlivost identifikace cíle. Čím vyšší je hodnota, tím snáze bude obličej rozpoznán a tím vyšší je pravděpodobnost chybné informace. Doporučujeme použít výchozí hodnotu 3.

Capture Interval (Interval zachytávání) [1~255 snímků]: Interval snímků pro zachycení obrázku. Pokud nastavíte hodnotu 1 což, je výchozí hodnota, znamená to, že kamera zachytí obličej v každém snímku.

Capture Sensitivity (Citlivost zachytávání) [0~20]: Prahová hodnota, při které kamera považuje cíl za obličej. Kamera bude cíl považovat za obličej, pouze pokud je skóre obličeje vygenerované algoritmem rovno nebo vyšší než nastavená hodnota. Doporučujeme použít výchozí hodnotu 2.

Face Capture Advanced Parameters (Pokročilé parametry zachytávání obličeje):

Face Exposure (Odhalení obličeje): Zaškrtnutím tohoto políčka povolíte expozici obličeje.

Reference Brightness (Referenční jas) [0~100]: Referenční jas obličeje v režimu odhalení obličeje. Pokud je detekován obličej, kamera upraví jeho jas dle nastavené hodnoty. Čím vyšší je hodnota, tím světlejší je obličej.

Minimum Duration (Min. doba trvání) [1~60min]: Minimální doba, po které kamera odhalí obličej. Výchozí hodnota je 1 minuta.

Poznámka: Pokud je odhalení obličeje povoleno, ujistěte se, že je vypnutá funkce WDR a vybrán manuální íclona.

Enable Face ROI (Povolit oblast zájmu (ROI) obličeje): Pokud kamera zachytí obličej, oblast obličeje bude považována za oblast zájmu a kvalita obrazu této oblasti bude vylepšená.

Restore Default (Obnovit výchozí): Kliknutím na tlačítko **Restore** (Obnovit)

obnovíte všechna nastavení v rozšířené konfiguraci na výchozí tovární hodnoty.

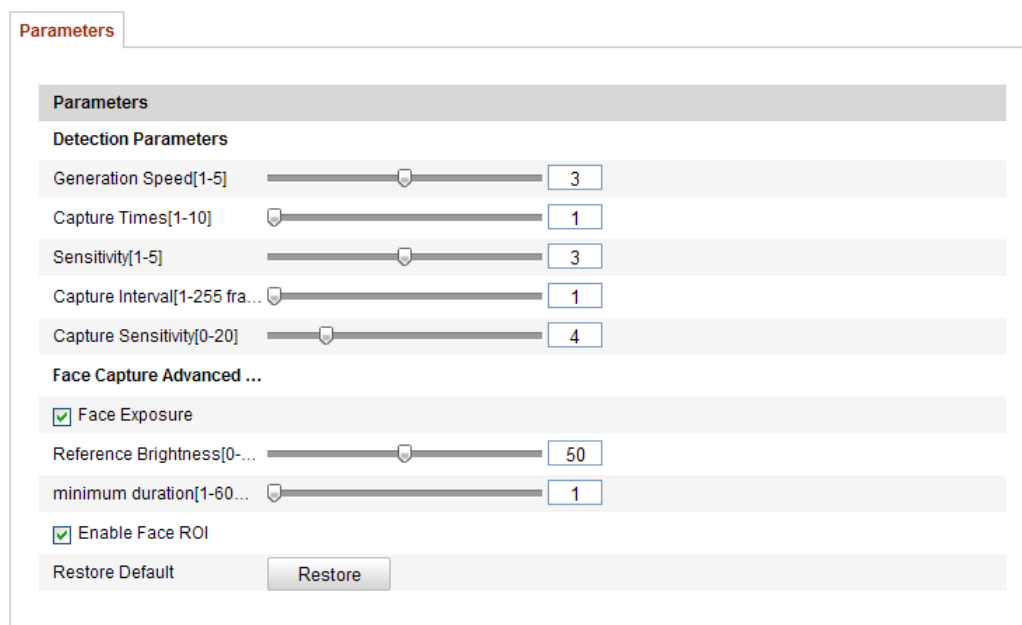


Figure 5-73 Rozšířená konfigurace

5.7.3 Tepelná mapa

Tepelná mapa je grafické znázornění dat reprezentovaných barvami. Funkce tepelné mapy kamery se obvykle používá k analýze časů návštěvy a času setrvání zákazníků v nakonfigurované oblasti.

❖ Konfigurace tepelné mapy

Postup:

1. Vstupte do rozhraní konfigurace tepelné mapy: **Configuration (Konfigurace) > Advanced Configuration (Rozšířená konfigurace) > Heat Map (Tepelná mapa)**

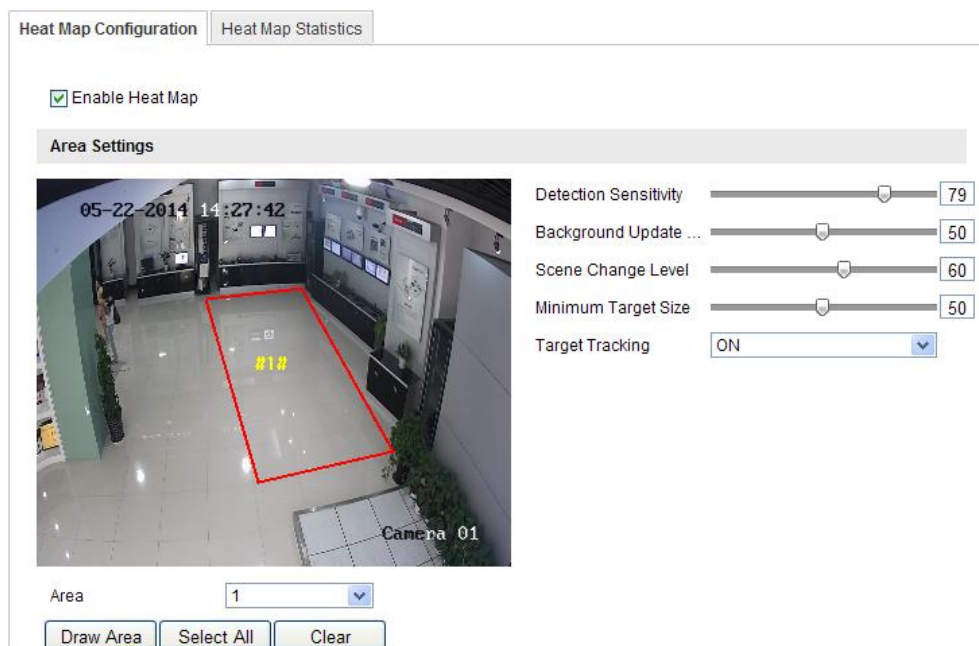


Figure 5-74 Konfigurace tepelné mapy

2. Vyberte kartu **Heat Map Configuration** (Konfigurace tepelné mapy) a nastavte podrobné parametry.
3. Povolte funkci zaškrtnutím políčka **Enable Heat Map** (Povolit tepelnou mapu).
4. Klikněte na tlačítko **Draw Area** (Nakreslit) a definujte oblast pro statistiku hodnot teploty. Nakreslete oblast zanesením čtyř koncových bodů levým tlačítkem do okna živého náhledu a kliknutím pravým tlačítkem kreslení oblasti dokončete. Lze nakonfigurovat je až 8 oblastí.

Poznámka: Můžete kliknout na tlačítko **Select All** (Vybrat vše) a vybrat jako nakonfigurovanou oblast celé okno živého náhledu. Kliknutím na tlačítko **Delete** (Odstranit) odstraníte aktuálně nakreslenou oblast.

5. Nakonfigurujte parametry pro nakreslenou oblast.

Detection Sensitivity (Citlivost detekce) [0~100]: Označuje citlivost identifikace cíle kamerou. Příliš vysoká citlivost může způsobit chybné informace. Doporučujeme nastavit citlivost na výchozí hodnotu 50.

Background Update Rate (Frekvence aktualizace pozadí) [0~100]: Označuje rychlost, jakou nová scéna nahradí předchozí scénu. Např.: Před regálem budou osoby mimo regál počítány dvakrát, pokud je z regálu odebráno zboží, a kamera považuje regál (z něhož bylo odebráno zboží) za novou

scénu. Doporučujeme použít výchozí hodnotu 50.

Scene Change Level (Úroveň změny scény) [0~100]: Označuje úroveň, jakou kamera reaguje na dynamické prostředí, např. vlnící se závěs. Kamera může pohybující se závěs považovat za cíl. Správným nastavením úrovně předejdete chybným informacím. Výchozí úroveň je 50.

Minimum Target Size (Minimální velikost cíle) [0~100]: Označuje velikost cíle identifikovaného kamerou. Velikost cíle můžete nastavit dle skutečného prostředí. Výchozí velikost je 50.

Target Track (Sledování cíle): Výběrem možnosti ON (Zapnuto) nebo OFF (Vypnuto) povolte/zakažte sledování cíle.

6. Kliknutím na tlačítko **Edit** (Upravit) nastavte rozvrh zapnutí ochrany.
7. Vyberte metodu propojení zaškrtnutím políčka informování monitorovacího centra.
8. Uložte nastavení kliknutím na tlačítko **Uložit**.

❖ **Statistika tepelné mapy**

Postup:

1. Kliknutím na tlačítko **Heat Map Statistics** (Statistika tepelné mapy) vstupte do rozhraní datové statistiky.
2. Vyberte typ zprávy kliknutím na rozsvícený nabídku. Lze vybrat z denní zprávy, týdenní zprávy, měsíční zprávy a roční zprávy.
3. Kliknutím na tlačítko **Counting** (Výpočet) vyexportujte data.
4. Vyberte **Statistics Result** (Výsledek statistiky) z možností Space Heat Map (Prostorová tepelná mapa) nebo Time Heat Map (Časová tepelná mapa) a zobrazí se příslušná tepelná mapa.

Pokud pro výpis statistiky vyberete časovou tepelnou mapu, k dispozici je tlačítko **Export** pro export dat do souboru aplikace Excel.

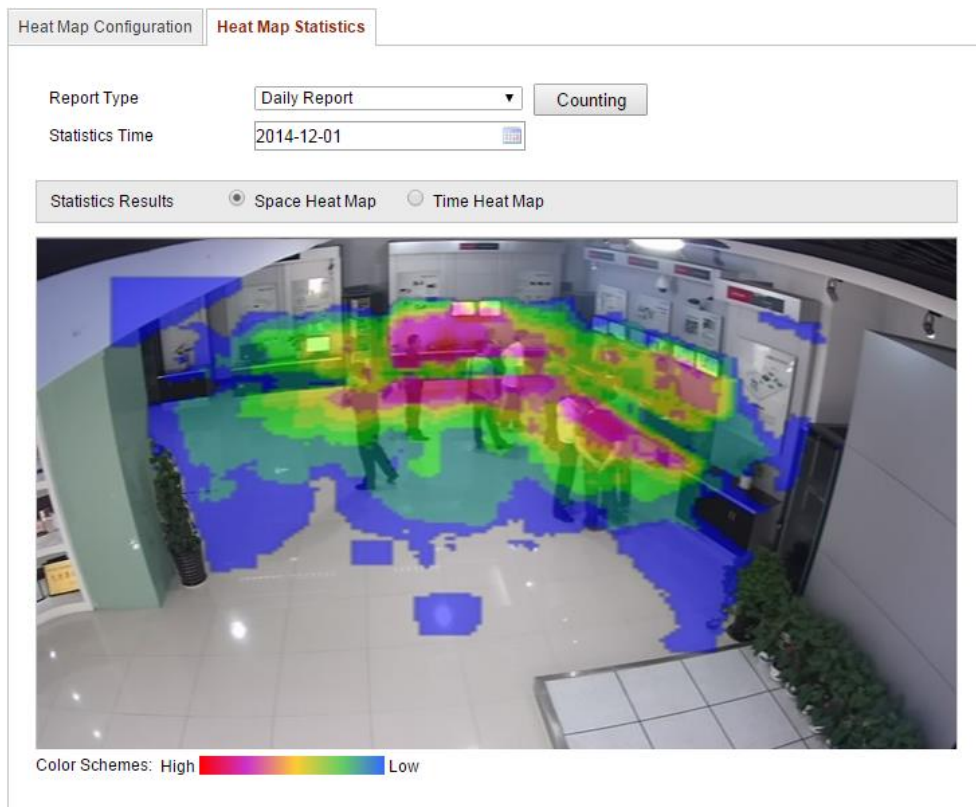


Figure 5-75 Prostorov átepeln ámapa

Pozn áanky:

- Jak znázorňuje obrázek výše, červený blok (255, 0, 0) indikuje nejnavštěvovanější oblast a modrý blok (0, 0, 255) indikuje méně oblíbenou oblast.
- Doporučujeme nenastavovat po dokončení instalace elektronický objektiv. Mohlo by to do jisté míry způsobit nepřesnost dat.

5.7.4 Počítání lidí

Funkce počítání lidí pomáhá počítat osoby, které vstoupí do určité nakonfigurované oblasti nebo ji opustí, a často se používá pro vchody a východy.

Pozn áanky:

- Funkci počítání lidí podporují některé modely kamer iDS.
- Doporučujeme instalovat kameru svisle vůči zemi, aby funkce počítání byla přesnější.

❖ **Konfigurace počítání lidí**

Postup:

1. Vstupte do rozhraní konfigurace počítání lidí
Configuration (Konfigurace) > Advanced Configuration (Rozšířená konfigurace) > People Counting (Počítání lidí)
2. Vyberte kartu **People Counting Configuration** (Konfigurace počítání lidí) a nastavte podrobné parametry.

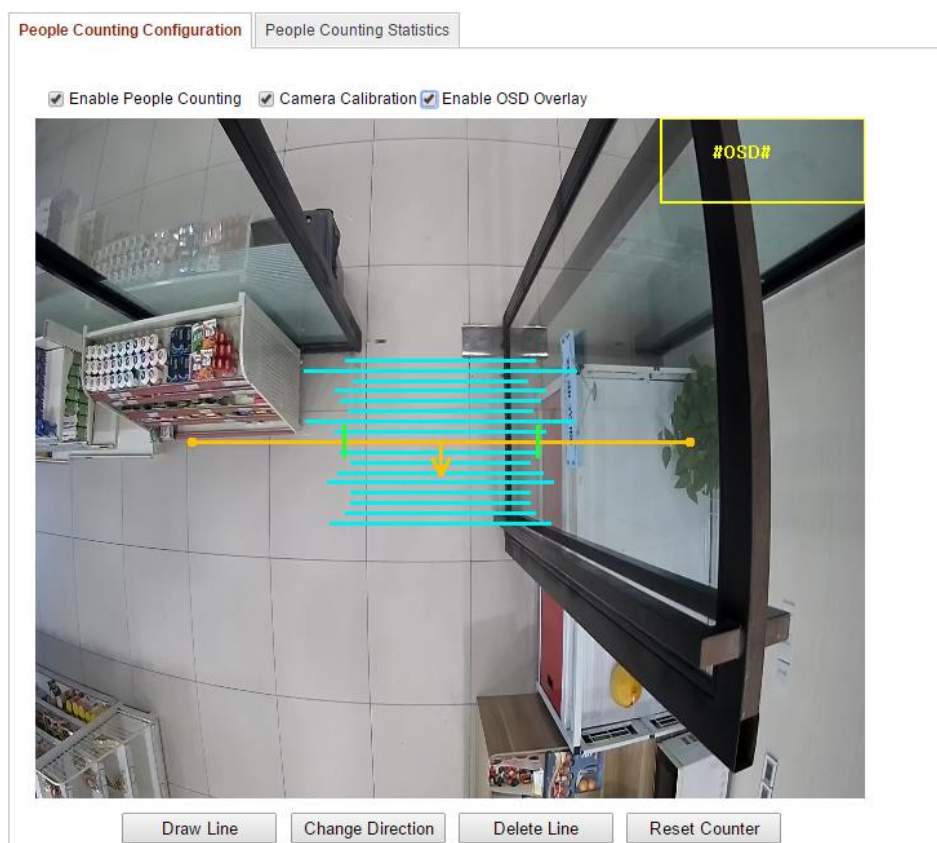


Figure 5-76 Konfigurace počítání lidí

3. Povolte funkci zaškrtnutím políčka **Enable People Counting** (Povolit počítání lidí).
4. (Volitelné) Zaškrtněte políčko **Enable OSD Overlay** (Povolit překrytí textem) a v živém videu se bude zobrazovat počet osob, které vstoupily nebo odešly, v reálném čase.
5. Nastavte čáru detekce.
 Oranžovou čáru, nazývanou čára detekce, lze nastavit v živém videu, a detekovány a počítány budou osoby, které vstoupí nebo odejdou přes tuto čáru.
 - 1) Klikněte na tlačítko **Draw Line** (Nakreslit čáru) a v obraze se zobrazí

oranžová čára detekce.

- 2) Tažením čáry detekce upravte její pozici.
- 3) Tažením za koncové body upravte délku čáry.
- 4) Pokud chcete čáru detekce odstranit, klikněte na tlačítko **Delete Line** (Odstranit čáru).

Poznámka: Čára detekce by měla pokrývat celý vchod/východ.

6. Po výběru čáry detekce se zobrazí šipka indikující směr vstupu osob. Můžete kliknout na tlačítko **Change Direction** (Změnit směr) a upravit směr šipky na opačnou stranu.
7. Zaškrtnutím políčka **Camera Calibration** (Kalibrace kamery) povolte tuto funkci.
8. Klikněte na tlačítko **Reset Counter** (Vynulovat počítadlo) a počet osob, které vstoupily nebo odešly, bude vynulován.
9. Kliknutím na tlačítko **Edit** (Upravit) nastavte rozvrh zapnutí ochrany.
10. Zaškrtnutím políčka **Notify Surveillance Center** (Informovat monitorovací centrum) nastavte akci propojení.
11. Uložte nastavení kliknutím na tlačítko **Uložit**.

❖ **Statistika počítání lidí**

Postup:

1. Kliknutím na tlačítko **People Counting Statistics** (Statistika počítání lidí) vstupte do rozhraní datové statistiky.
2. Vyberte typ zprávy kliknutím na rozevřací nabídku. Lze vybrat z denní zprávy, týdenní zprávy, měsíční zprávy a roční zprávy.
3. Vyberte **Statistics Type** (Typ statistiky) z možností People Entered (Příchozí osoby) nebo People Exited (Odchozí osoby).
4. Vyberte položku **Statistics Time** (Čas statistiky).

Poznámka: Denní zpráva vypočítá data pro vybrané datum, týdenní zpráva vypočítá data pro týden, do kterého patří vámi vybrané datum, měsíční zpráva vypočítá data pro měsíc, do kterého patří vámi vybrané datum, a roční zpráva vypočítá data pro rok, do kterého patří vámi vybrané datum.

5. Kliknutím na tlačítko **Counting** (Výpočet) vypočítejte data.
6. Vyberte export **výsledků statistiky** ve formě tabulky, sloupcového grafu nebo čárového grafu.

Poznámka: Pokud pro výpis statistiky vyberete tabulku, k dispozici je tlačítko **Export** pro export dat do souboru aplikace Excel.

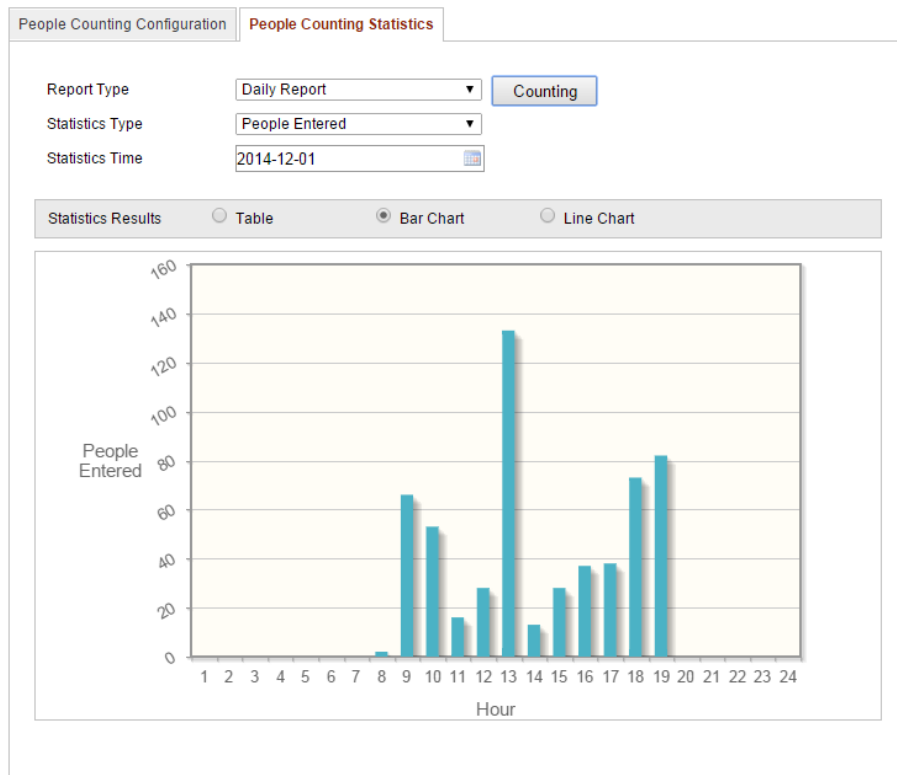


Figure 5-77 Výsledky statistiky

Poznámka: Doporučujeme nenastavovat po dokončení instalace elektronický objektiv. Mohlo by to do jisté míry způsobit nepřesnost dat.

Chapter 6 Nastavení úložiště

Než začnete:

Pro konfiguraci nastavení nahrávání se ujistěte, že se v síti nachází síťové úložiště nebo je v kameře vložena karta SD.

6.1 Konfigurace nastavení NAS

Než začnete:

Pro ukládání nahraných souborů, souborů protokolu atd. by měl být k dispozici síťový disk připojený do sítě a řádně nakonfigurovaný.

Postup:

1. Přidání síťového disku

(1) Vstupte do rozhraní nastavení úložiště NAS (Network-Attached Storage):

Configuration (Konfigurace) > Advanced Configuration (Rozšířená konfigurace)
> Storage (Úložiště) > NAS

HDD No.	Type	Server Address	File Path
1	NAS	172.6.21.99	/dvr/test01
	Mounting Type	User Name	Password
	NFS		
	SMB/CIFS		
2	NAS		
3	NAS		
4	NAS		
5	NAS		
6	NAS		
7	NAS		
8	NAS		

Save

Figure 6-1 Přidání síťového disku

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

(3) Vyberte typ připojení. Lze vybrat z možností NFS a SMB/CIFS. Pokud je vybrán typ SMB/CIFS, můžete nastavit uživatelské jméno a heslo pro

zajištění zabezpečení.

Poznámka: Popis vytvoření cesty k souborům najdete v *uživatelské příručce k úložišti NAS*.



- Pro vaše soukromí a lepší ochranu vašeho systému před bezpečnostními riziky důrazně doporučujeme používat pro všechny funkce a síťová zařízení silná hesla. Heslo by mělo být vytvořeno dle vašeho vlastního výběru (o délce alespoň 8 znaků, s velkými písmeny, malými písmeny, čísly a speciálními znaky), abyste zvýšili zabezpečení výrobku.
- Za řádnou konfiguraci veškerých hesel a dalších nastavení zabezpečí ručí osoba provádějící instalaci a/nebo koncový uživatel.

(4) Kliknutím na tlačítko **Save** (Uložit) přidejte síťový disk.

2. Inicializujte přidaný síťový disk.

(1) Vstupte do rozhraní nastavení pevných disků (**Advanced Configuration (Rozšířená konfigurace) > Storage (Úložiště) > Storage Management (Správa úložiště)**), ve kterém můžete zobrazit kapacitu, volné místo, stav, typ a vlastnosti disku.

The screenshot shows the 'Storage Management' tab in a web interface. It features a 'HDD Device List' table and a 'Quota' section with several input fields.

HDD Device List							Format
<input type="checkbox"/>	HDD No.	Capacity	Free space	Status	Type	Property	Progress
<input type="checkbox"/>	g	20.00GB	0.00GB	Uninitialized	NAS	R/W	

Quota

Max. Picture Capacity	<input type="text" value="0.00GB"/>
Free Size for Picture	<input type="text" value="0GB"/>
Max. Record Capacity	<input type="text" value="0.00GB"/>
Free Size for Record	<input type="text" value="0GB"/>
Percentage of Picture	<input type="text" value="25"/> %
Percentage of Record	<input type="text" value="75"/> %

Figure 6-2 Rozhraní správy úložiště

(2) Pokud je stav disku **Uninitialized** (Neinicializovaný) zaškrtnutím příslušného políčka disk vyberte a kliknutím na tlačítko **Format** (Formátovat) spusťte

inicializaci disku.

Po dokončení inicializace se stav disku změní na **Normal** (Normální).

HDD Device List							Format
<input type="checkbox"/>	HDD No.	Capacity	Free space	Status	Type	Property	Progress
<input type="checkbox"/>	g	20.00GB	19.75GB	Normal	NAS	R/W	

Figure 6-3 Zobrazení stavu disku

3. Definujte kvótu pro nahrávky a obrázky.

- (1) Zadejte procentuální kvótu pro obrázky a nahrávky.
- (2) Klikněte na tlačítko **Save** (Uložit) a obnovte stránku prohlížeče, aby se nastavení aktivovala.

Quota	
Max. Picture Capacity	<input type="text" value="4.94GB"/>
Free Size for Picture	<input type="text" value="4.94GB"/>
Max. Record Capacity	<input type="text" value="14.81GB"/>
Free Size for Record	<input type="text" value="14.81GB"/>
Percentage of Picture	<input type="text" value="25"/> %
Percentage of Record	<input type="text" value="75"/> %

Figure 6-4 Nastavení kvóty

Poznámky:

- Ke kameře lze připojit až 8 disků NAS.
- Pro inicializaci a použití karty SD po jejím vložení do kamery použijte postup uvedený u inicializace disku NAS.

6.2 Konfigurace rozvrhu nahrávání

Účel:

Pro kamery jsou k dispozici dva druhy nahrávání: manuální nahrávání a plánované nahrávání. V případě manuálního nahrávání postupujte podle části 5.3 **Manuální nahrávání a pořizování snímků**. V této části můžete pomocí uvedeného postupu nakonfigurovat plánované nahrávání. Ve výchozím stav se soubory záznamu

plánovaného nahrávání ukládají na kartu SD (pokud je podporovaná) nebo na síťový disk.

Postup:

1. Vstupte do rozhraní rozvrhu nahrávání

Configuration (Konfigurace) > Advanced Configuration (Rozšířená konfigurace) > Storage (Úložiště) > Record Schedule (Rozvrh nahrávání)

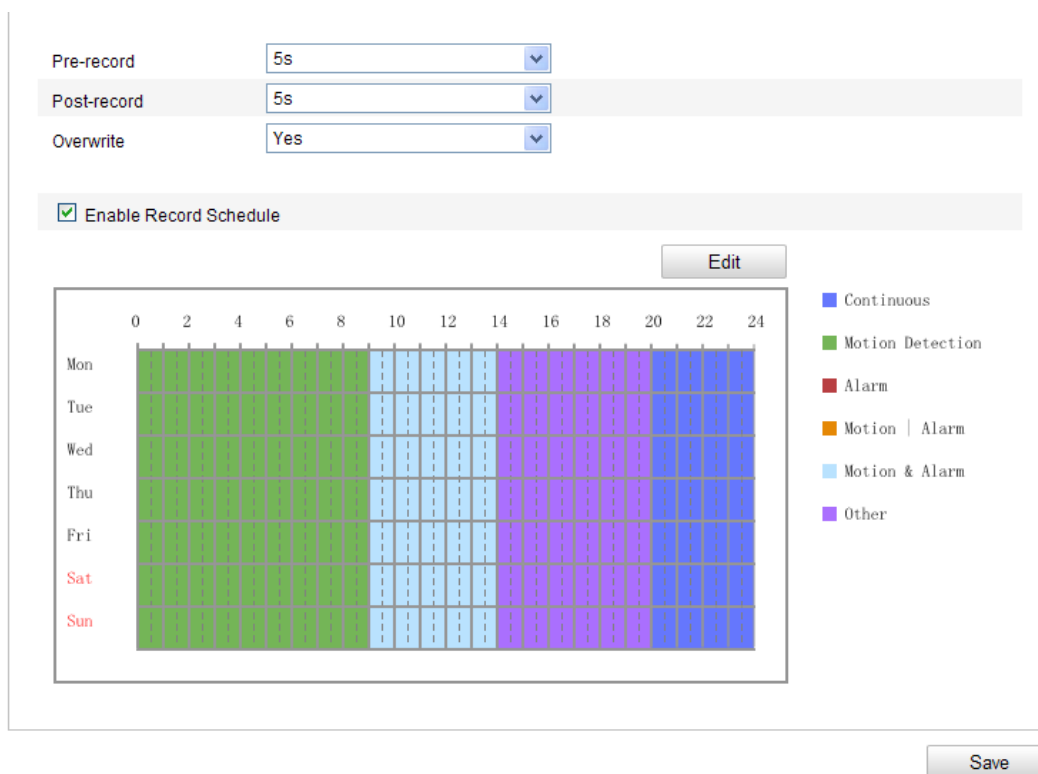


Figure 6-5 Rozhraní rozvrhu nahrávání

2. Povolte funkci zaškrtnutím políčka **Enable Record Schedule** (Povolit rozvrh nahrávání).
3. Nastavte parametry záznamu kamery.

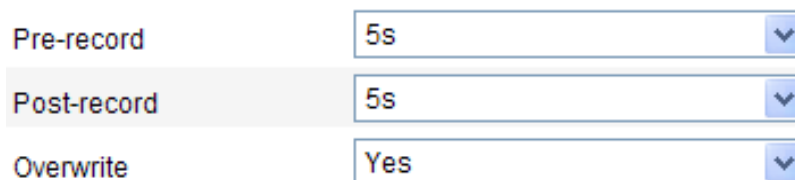


Figure 6-6 Parametry záznamu

- Pre-record (Předběžný záznam): Nastavení doby spuštění záznamu před naplánovaným časem nebo událostí. Například pokud alarm spustí záznam v

10:00 a nastavíte předběžný záznam na 5 sekund, kamera začne nahrávat od času 9:59:55.

Dobu předběžného záznamu lze nakonfigurovat z možností No Pre-record (Bez předběžného záznamu), 5 s, 10 s, 15 s, 20 s, 25 s, 30 s nebo neomezená.

- **Post-record (Následný záznam):** Nastavení doby zastavení záznamu po naplánovaném čase nebo události. Například pokud záznam aktivovaný alarmem skončí v 11:00 a nastavíte následný záznam na 5 sekund, kamera nahrává do času 11:00:05.

Dobu následného záznamu lze nakonfigurovat z možností 5 s, 10 s, 30 s, 1 min, 2 min, 5 min nebo 10 min.

Poznámka: Konfigurace parametrů záznamu se liší dle modelu kamery.

4. Kliknutím na tlačítko **Edit** (Upravit) upravte rozvrh nahrávání

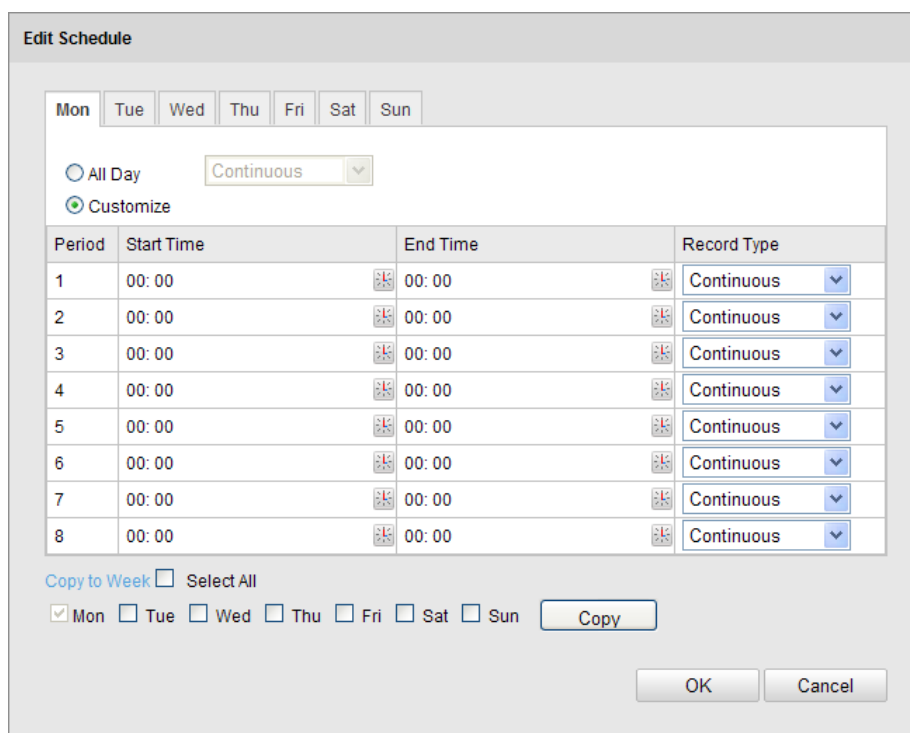


Figure 6-7 Rozvrh nahrávání

5. Vyberte den, pro který chcete nastavit rozvrh nahrávání

(1) Vyberte celodenní nahrávání nebo nahrávání úseku.

- ◆ Pokud chcete nakonfigurovat celodenní nahrávání, zaškrtněte políčko **All Day** (Celý den).
- ◆ Pokud chcete nahrávat v různých časových úsecích, zaškrtněte políčko

Customize (Přizpůsobit). Nastavte parametry **Start Time** (Čas začátku) a **End Time** (Čas konce).

Poznámka: Časy jednotlivých úseků se nesmějí překrývat. Lze nakonfigurovat až 4 úseky.

- (2) Vyberte položku **Record Type** (Druh záznamu). Druh záznamu může být nepřetržitý, detekce pohybu, alarm, pohyb | alarm, pohyb a alarm, PIR alarm, bezdrátový alarm, nouzový alarm nebo pohyb | vstup alarmu | PIR | bezdrátový | nouzový.

◆ **Nepřetržitý**

Pokud vyberete možnost **Continuous** (Nepřetržitý), video bude nahráváno automaticky dle času rozvrhu.

◆ **Nahrávání iaktivované detekce pohybu**

Pokud vyberete možnost **Motion Detection** (Detekce pohybu) video bude nahráváno, když bude detekován pohyb.

Kromě konfigurace rozvrhu nahrávání je třeba nastavit oblast detekce pohybu a zaškrtnout políčko **Trigger Channel** (Aktivovat kanál) pod položkou **Linkage Method** (Metoda propojení) rozhraní nastavení detekce pohybu. Podrobné informace jsou uvedeny v *1. kroku Nastavte oblast detekce pohybu v části 6.6.1.*

◆ **Nahrávání iaktivované alarmem**

Pokud vyberete možnost **Alarm**, video se bude nahrávat, když se aktivuje alarm prostřednictvím externích kanálů vstupu alarmu.

Kromě konfigurace rozvrhu nahrávání je třeba nastavit položku **Alarm Type** (Druh alarmu) a zaškrtnout políčko **Trigger Channel** (Aktivovat kanál) pod položkou **Linkage Method** (Metoda propojení) rozhraní nastavení vstupu alarmu. Podrobné informace jsou uvedeny v *části 6.6.3.*

◆ **Nahrávání iaktivované pohybem a alarmem**

Pokud vyberete možnost **Motion & Alarm** (Pohyb a alarm), video se bude nahrávat, když je současně aktivován pohyb i alarm.

Kromě konfigurace rozvrhu nahrávání je třeba nakonfigurovat nastavení v

rozhraní **detekce pohybu** a **vstupu alarmu**. Podrobné informace jsou uvedeny v *části 6.6.1* a *části 6.6.3*.

◆ **Nahrávání iaktivovaným pohybem nebo alarmem**

Pokud vyberete možnost **Motion | Alarm** (Pohyb nebo alarm), video se bude nahrávat, když je aktivován externí alarm nebo je detekován pohyb.

Kromě konfigurace rozvrhu nahrávání je třeba nakonfigurovat nastavení v rozhraní **detekce pohybu** a **vstupu alarmu**. Podrobné informace jsou uvedeny v *části 6.6.1* a *části 6.6.3*.

The screenshot shows the 'Edit Schedule' dialog box. At the top, there are tabs for days of the week (Mon, Tue, Wed, Thu, Fri, Sat, Sun). Below that, there are radio buttons for 'All Day' and 'Customize', and a dropdown menu set to 'Continuous'. The main part of the dialog is a table with the following structure:

Period	Start Time	End Time	Record Type
1	00:00	09:00	Motion Detection
2	09:00	14:00	Motion & Alarm
3	14:00	20:00	Scene Change
4	20:00	24:00	Continuous
5	00:00	00:00	Continuous
6	00:00	00:00	Continuous
7	00:00	00:00	Continuous
8	00:00	00:00	Continuous

Below the table, there are checkboxes for 'Copy to Week' (checked) and 'Select All'. Underneath, there are checkboxes for each day of the week (Mon, Tue, Wed, Thu, Fri, Sat, Sun), all of which are checked. A 'Copy' button is located to the right of these checkboxes. At the bottom right of the dialog are 'OK' and 'Cancel' buttons.

Figure 6-8 Úprava rozvrhu nahrávání

- (3) Zaškrtněte políčko **Select All** (Vybrat vše) a kliknutím na tlačítko **Copy** (Kopírovat) zkopírujte nastavení tohoto dne do celého týdne. Můžete rovněž zaškrtnout políčka před konkrétními dny a kliknout na tlačítko **Copy**.
- (4) Kliknutím na tlačítko **OK** uložíte nastavení a opustíte rozhraní pro úpravy rozvrhu nahrávání.

6. Uložte nastavení kliknutím na tlačítko **Uložit**.

6.3 Konfigurace nastavení snímků

Účel:

Můžete nakonfigurovat naplánovaný snímek a snímek aktivovaný událostí. Pořízený snímek bude uložen na kartu SD (pokud je podporovaná) nebo síťový pevný disk (podrobné informace o síťovém pevném disku jsou uvedeny v *části 7.1 Konfigurace nastavení NAS*). Pořízené snímky můžete také nahrávat na server FTP.

Základní nastavení

Postup:

1. Vstupte do rozhraní nastavení snímků:

Configuration (Konfigurace) > Advanced Configuration (Rozšířená konfigurace) > Storage (Úložiště) > Snapshot (Snímek)

2. Zaškrtnutím políčka **Enable Timing Snapshot** (Povolit načasovaný snímek) povolte průběžné pořizování snímků. Zaškrtnutím políčka **Enable Event-triggered Snapshot** (Povolit snímek aktivovaný událostí) povolte snímky aktivované událostí.
3. Nastavte kvalitu snímku.
4. Nastavte časový interval mezi dvěma snímky.
5. Uložte nastavení kliknutím na tlačítko **Uložit**.

Nahrávání na server FTP

Pomocí následujících pokynů pro konfiguraci můžete nahrávat snímky na server FTP.

- Nahrávání průběžných snímků na server FTP

Postup:

- 1) Nakonfigurujte server FTP a zaškrtněte políčko **Upload Picture** (Nahrát snímek) v rozhraní nastavení serveru FTP. Další podrobnosti o konfiguraci parametrů FTP jsou uvedeny v *části 6.3.12 Konfigurace nastavení FTP*.
- 2) Zaškrtněte políčko **Enable Timing Snapshot** (Povolit načasovaný snímek).

- Nahrávání snímků aktivovaných událostí na server FTP

Postup:

- 1) Nakonfigurujte server FTP a zaškrtněte políčko **Upload Picture** (Nahrát snímek) v rozhraní nastavení serveru FTP. Další podrobnosti o konfiguraci parametrů FTP jsou uvedeny v *části 6.3.12 Konfigurace nastavení FTP*.
- 2) Zaškrtněte políčko **Upload Picture** (Nahrát snímek) v rozhraní nastavení detekce

pohybu nebo vstupu alarmu. Postupujte podle *3. kroku Nastavení akce í alarmu pro detekci pohybu* v části 6.6.1 nebo *4. kroku Konfigurace externího vstupu alarmu* v části 6.6.4.

- 3) Zaškrtněte políčko **Enable Event-triggered Snapshot** (Povolit snímek aktivovaný událostí).

The screenshot shows a configuration window with two sections: 'Timing' and 'Event-Triggered'. Both sections have a checked checkbox for enabling snapshots. The 'Timing' section has dropdowns for Format (JPEG), Resolution (1920*1080), and Quality (High), and a text input for Interval (0) with a unit dropdown (millisecond). The 'Event-Triggered' section has similar dropdowns for Format (JPEG), Resolution (1920*1080), and Quality (High), a text input for Interval (0) with a unit dropdown (millisecond), and a text input for Capture Number (4). A 'Save' button is located at the bottom right.

Figure 6-9 Nastavení snímku

6.4 Konfigurace funkce Lite Storage

Účel:

Pokud se v monitorovaném záběru nepohybuje žádný objekt, snímkovou frekvenci a datový tok video streamu lze omezit, aby se prodloužila doba záznamu na kartě SD.

Poznámky:

- Funkce Lite Storage se liší dle různých modelů kamer.
- Soubory videa uložené v režimu Lite Storage se budou přehrávat plnou snímkovou frekvencí (25 sn./s / 30 sn./s), takže průběh přehrávání bude zrychlený.

1. Vstupte do rozhraní funkce Lite Storage: **Configuration (Konfigurace)** >

Advanced Configuration (Rozšířená konfigurace) > Storage (Úložiště) > Lite Storage

2. Zaškrtnutím políčka **Enable** (Povolit) povolte funkci Lite Storage.
3. Zadejte čas ukládání do textového pole. Na stránce můžete zjistit dostupné místo na kartě SD.
4. Uložte nastavení kliknutím na tlačítko **Uložit**.

Enable
 SD Card Available Space
 Storage Time Day (1-30)
 Note: : After Lite Storage enabled, the unformatted SD card will be formatted automatically.

Save

Figure 6-10 Nastavení funkce Lite Storage

6.5 Konfigurace cloudového úložiště

Účel:

Pořízené snímky mohou být uloženy v NVR, který pracuje v režimu cloudového úložiště.

Poznámka: Funkce cloudového úložiště se liší dle různých modelů kamer.

Než začnete:

Ujistěte se, že NVR je přepnutý do pracovního režimu cloudového úložiště; podrobnosti najdete v uživatelské příručce k NVR.

Postup:

1. Vstupte do rozhraní cloudového úložiště: **Configuration (Konfigurace) > Advanced Configuration (Rozšířená konfigurace) > Storage (Úložiště) > Cloud Storage (Cloudové úložiště)**
2. Zaškrtněte políčko **Enable Cloud Storage** (Povolit Cloudové úložiště).
3. Zadejte IP adresu a port serveru úložiště.
4. Zadejte uživatelské jméno, heslo a potvrďte heslo pro ověření serveru úložiště.



- *Pro vaše soukromí a lepší ochranu vašeho systému před bezpečnostními riziky důrazně doporučujeme používat pro všechny funkce a síťová zařízení silná hesla. Heslo by mělo být vytvořeno dle vašeho vlastního výběru (o délce alespoň 8 znaků, s velkými písmeny, malými písmeny, čísly a speciálními znaky), abyste zvýšili zabezpečení výrobku.*
 - *Za řádnou konfiguraci veškerých hesel a dalších nastavení zabezpečí ručí osoba provádějící instalaci a/nebo koncový uživatel.*
5. Zadejte ID fondu ukládání snímků serveru.
 6. (Volitelné) Kliknutím na tlačítko **Test** můžete otestovat nastavení cloudového úložiště.
 7. Uložte nastavení kliknutím na tlačítko **Uložit**.

<input type="checkbox"/> Enable Cloud Storage	
Server IP Address	0.0.0.0
Server Port	6001
User Name	
Password	
Confirm	
Picture Storage Pool ID	1
	<input type="button" value="Test"/>
	<input type="button" value="Save"/>

Figure 6-11 Nastavení cloudového úložiště

Chapter 7 Počítání

Účel:

Funkce počítání slouží k počítání objektů, které vstoupily do určité nakonfigurované oblasti nebo ji opustily, a často se používá pro vchody a východy.

Poznámky:

- Funkci počítání podporují některé kamery mimo modely iDS.
- Ve srovnání s funkcí počítání lidí podporovanou kamerami iDS funkce počítání jiných kamer nevyžaduje nastavení kalibrace.
- Doporučujeme instalovat kameru svisle vůči zemi, aby funkce počítání byla přesnější.

Postup:

❖ Konfigurace počítání

1. Vstupte do rozhraní konfigurace počítání:

Configuration (Konfigurace) > Advanced Configuration (Rozšířená konfigurace) > Counting (Počítání)

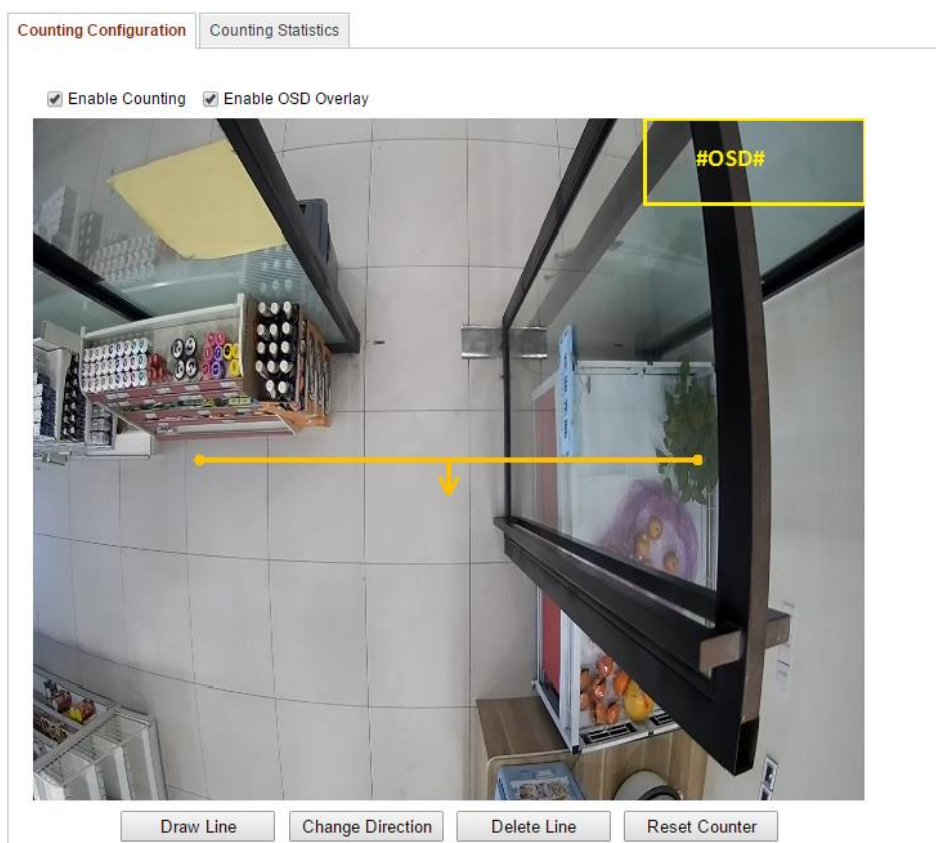


Figure 7-1 Konfigurace počítání

2. Vyberte kartu **Counting Configuration** (Konfigurace počítání) a nastavte podrobné parametry.
3. Povolte funkci zaškrtnutím políčka **Enable Counting** (Povolit počítání).
4. (Volitelné) Zaškrtněte políčko **Enable OSD Overlay** (Povolit překrytí textem) a v živém videu se bude zobrazovat počet objektů, které vstoupily nebo odešly, v reálném čase.
Můžete také upravit pozici OSD dle aktuálních potřeb.
5. Nastavte čáru detekce.
Oranžovou čáru, nazývanou čára detekce, lze nastavit v živém videu, a detekovány a počítány budou objekty, které vstoupí nebo odejdou přes tuto čáru.
 - 1) Klikněte na tlačítko **Draw Line** (Nakreslit čáru) a v obraze se zobrazí oranžová čára detekce.
 - 2) Tažením čáry detekce upravte její pozici.
 - 3) Tažením za koncové body upravte délku čáry.
 - 4) Pokud chcete čáru detekce odstranit, klikněte na tlačítko **Delete Line** (Odstranit čáru).

Poznámka: Čára detekce by měla pokrývat celý vchod/východ.
6. Klikněte na tlačítko **Reset Counter** (Vynulovat počítadlo) a počet osob, které vstoupily nebo odešly, bude vynulován.
7. Kliknutím na tlačítko **Edit** (Upravit) nastavte rozvrh zapnutí ochrany.
8. Zaškrtnutím políčka **Notify Surveillance Center** (Informovat monitorovací centrum) nastavte akci propojení.
9. Uložte nastavení kliknutím na tlačítko **Uložit**.

❖ Statistika počítání

Postup:

1. Kliknutím na tlačítko **Counting Statistics** (Statistika počítání) vstupte do rozhraní datové statistiky.
2. Vyberte typ zprávy kliknutím na rozevřací nabídku. Lze vybrat z denní zprávy, týdenní zprávy, měsíční zprávy a roční zprávy.
3. Vyberte Statistics Type (Typ statistiky) z možností People Entered (Příchozí osoby) nebo People Exited (Odchozí osoby).

Poznámka: Denní zpráva vypočítá data pro vybrané datum, týdenní zpráva vypočítá data pro týden, do kterého patří vámi vybrané datum, měsíční zpráva vypočítá data pro měsíc, do kterého patří vámi vybrané datum, a roční zpráva vypočítá data pro rok, do kterého patří vámi vybrané datum.

4. Vyberte položku Statistics Time (Čas statistiky).
5. Kliknutím na tlačítko **Counting** (Výpočet) vypočítejte data.
6. Vyberte export **výsledků statistiky** ve formě tabulky, sloupcového grafu nebo čárového grafu.

Poznámka: Pokud pro zobrazení statistiky vyberete tabulku, k dispozici je tlačítko **Export** pro export dat do souboru aplikace Excel.

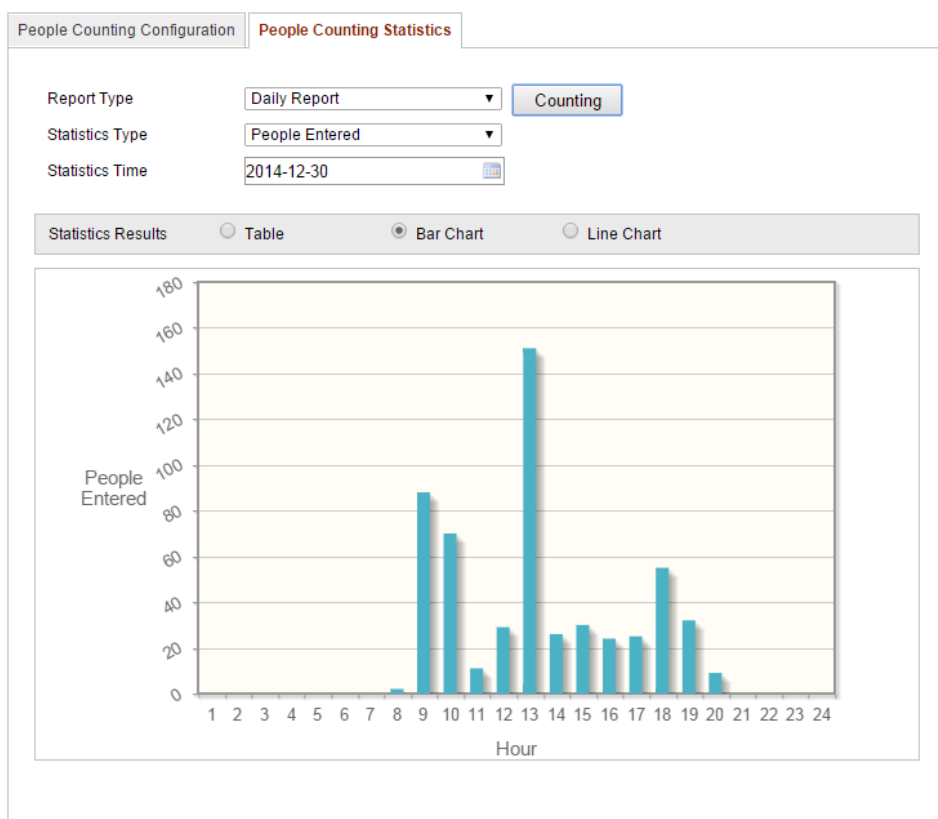


Figure 7-2 Výsledky statistiky

Chapter 8 Silniční provoz

Účel:

Pro sledování silničního provozu jsou k dispozici funkce detekce vozidel a detekce smíšeného provozu. Při detekci vozidel mohou být detekována projíždějící vozidla a lze pořídit snímek registrační značky; navíc lze automaticky rozpoznat barvu, logo vozidla a další informace. Při detekci smíšeného provozu lze detekovat chodce, motorová vozidla a nemotorová vozidla a může být pořízen snímek objektu (v případě chodce / nemotorového vozidla / motorového vozidla bez registrační značky) nebo registrační značky (v případě motorového vozidla s registrační značkou). Můžete odeslat signál alarmu pro upozornění monitorovacího centra a odeslat pořízený snímek na server FTP.

Poznámka: Funkce silničního provozu se liší dle různých modelů kamer.

Postup:

❖ Konfigurace nastavení detekce


1. Vyberte druh detekce ze seznamu. Lze vybrat z možností Vehicle Detection (Detekce vozidla) a Mixed-traffic Detection (Detekce smíšeného provozu).

Poznámka: Při přepnutí druhu detekce silničního provozu restartujte zařízení, aby se nově nastavení aktivovala.

2. Zaškrtnutím políčka **Enable** (Povolit) povolte vybranou funkci detekce.
3. Vyberte počet jízdních pruhů v příslušném rozevíracím seznamu. Lze zvolit až 4 jízdní pruhy.
4. Tažením čáry pruhu nastavte její pozici nebo tažením za konec čáry upravte její délku a úhel.
5. Nastavte poměr přiblížení kamery tak, aby velikost vozidla v obraze byla blízko pozice červeného rámečku. Nastavitelná je pouze pozice červeného rámečku.

Poznámka: V jednom okamžiku lze pro každý jízdní pruh zachytit pouze jednu registrační značku.

6. Vyberte zkratku oblasti/státu v rozevíracím seznamu, pokud nelze určení registrační značky rozpoznat.

7. Nastavte rozvrh zapnutí ochrany pro detekci vozidla.
 - 1) Pokud chcete rozvrh zapnutí ochrany upravit, klikněte na tlačítko **Edit** (Upravit).
 - 2) Vyberte den, pro který chcete nastavit rozvrh zapnutí ochrany.
 - 3) Klikněte na tlačítko  a nastavte časové období pro rozvrh zapnutí ochrany.
 - 4) (Volitelné) Po nastavení rozvrhu zapnutí ochrany můžete kliknout na tlačítko **Copy** (Kopírovat) a zkopírovat rozvrh do dalších dní.
 - 5) Kliknutím na tlačítko **OK** uložíte nastavení.

Poznámka: Časy jednotlivých období se nesmějí překrývat.

8. Zaškrtnutím políčka vyberte metodu propojení. Lze vybrat z možností informování monitorovacího centra nebo nahrání na server FTP.

Informovat monitorovací centrum: Odeslání signálu v ýjimky nebo alarmu softwaru pro vzdálenou správu, když dojde k události.

Nahrát na FTP: Pořízení snímku při aktivaci alarmu a jeho odeslání na server FTP. Soubor uložte na místní kartu SD nebo připojené úložiště NAS.

9. Uložte nastavení kliknutím na tlačítko **Uložit**.

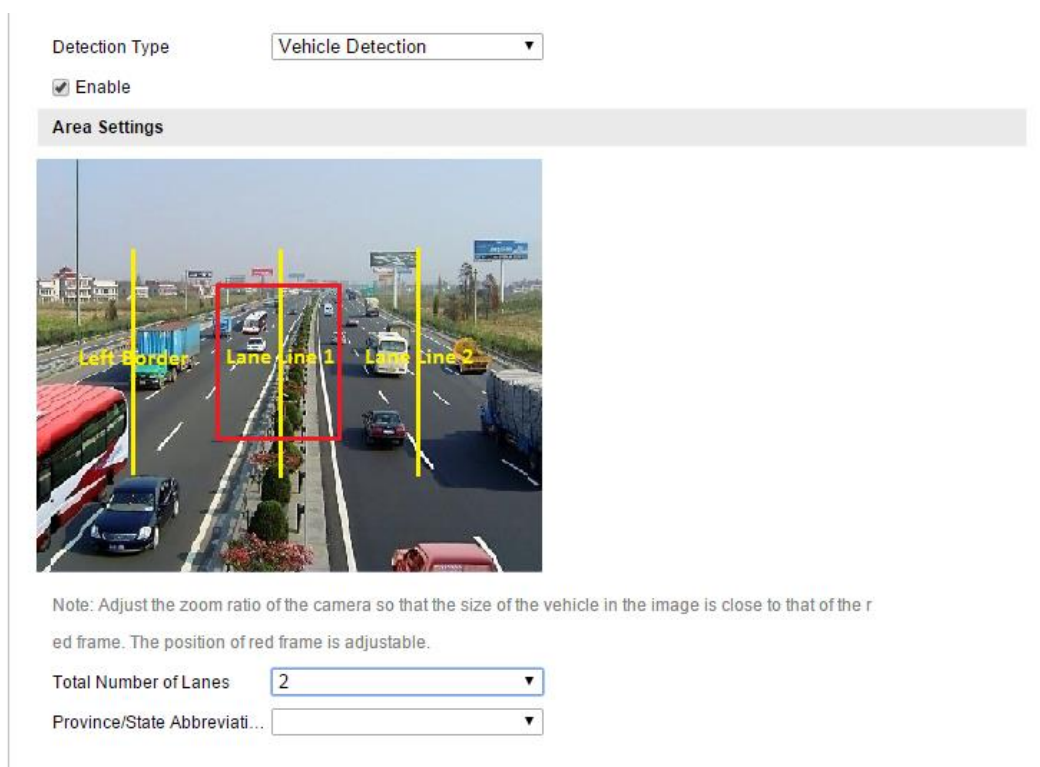



Figure 8-1 Konfigurace detekce vozidla

❖ Konfigurace nahrávání snímku

1. Nastavte kvalitu snímku.

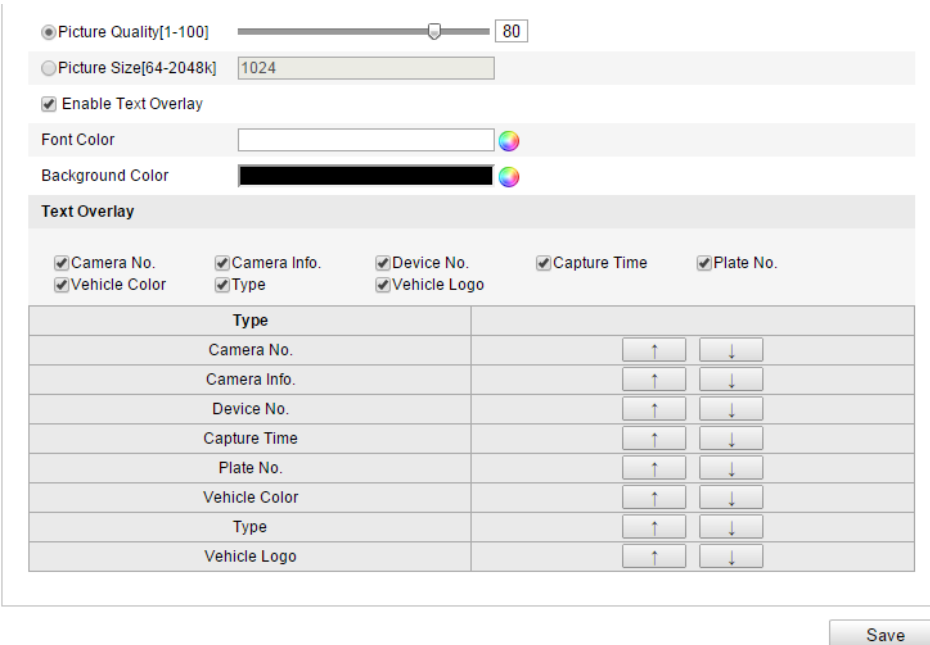
Při určení kvality snímku lze nastavit buď parametr Picture Quality (Kvalita snímku), nebo parametr Picture Size (Velikost snímku).

2. (Volitelné) Povolte a upravte překrytí textem v nahraném snímku.

Po kliknutí na ikonu  a výběru požadované barvy v zobrazené paletě můžete nastavit barvu písma a pozadí

3. Vyberte informace pro překrytí textem, jako číslo kamery, informace o kameře, číslo zařízení, čas pořízení, číslo registrační značky, barva vozidla atd. Můžete také kliknout na směrová tlačítka nahoru a dolů pro změnu pořadí textu.

4. Kliknutím na tlačítko **Save** (Uložit) aktivujete nastavení.



The screenshot shows a configuration window with the following elements:

- Picture Quality**: A slider set to 80.
- Picture Size**: A dropdown menu set to 1024.
- Enable Text Overlay**: A checked checkbox.
- Font Color**: A text input field with a color selection icon.
- Background Color**: A color selection icon.
- Text Overlay**: A section with several checked checkboxes:
 - Camera No.
 - Camera Info.
 - Device No.
 - Capture Time
 - Plate No.
 - Vehicle Color
 - Type
 - Vehicle Logo
- Ordering Table**: A table with 8 rows, each representing a text overlay type. Each row has a 'Type' column and two arrow buttons (up and down) for reordering.

Type		
Camera No.	↑	↓
Camera Info.	↑	↓
Device No.	↑	↓
Capture Time	↑	↓
Plate No.	↑	↓
Vehicle Color	↑	↓
Type	↑	↓
Vehicle Logo	↑	↓
- Save**: A button at the bottom right of the window.

Figure 8-2 Nastavení nahrávání snímků

❖ Konfigurace obsahu překrytí

1. Upravte obsah čísla kamery, informací o kameře a informací o zařízení v příslušných textových polích.
2. (Volitelné) Povolte a upravte překrytí textem v nahrávaném snímku.
3. Kliknutím na tlačítko **Save** (Uložit) aktivujete nastavení.

Device No.	<input type="text" value="Camera 01"/>
Camera No.	<input type="text"/>
Camera Info.	<input type="text"/>

Figure 8-3 Nastavení obsahu překrytí

Chapter 9 Přehrávání

Účel:

Tato část popisuje, jak prohlížet vzdáleně nahrané soubory videa uložené na síťových discích nebo kartách SD.

Postup:

1. Kliknutím na tlačítko **Playback** (Přehrávání) v panelu nabídky vstupte do rozhraní přehrávání.

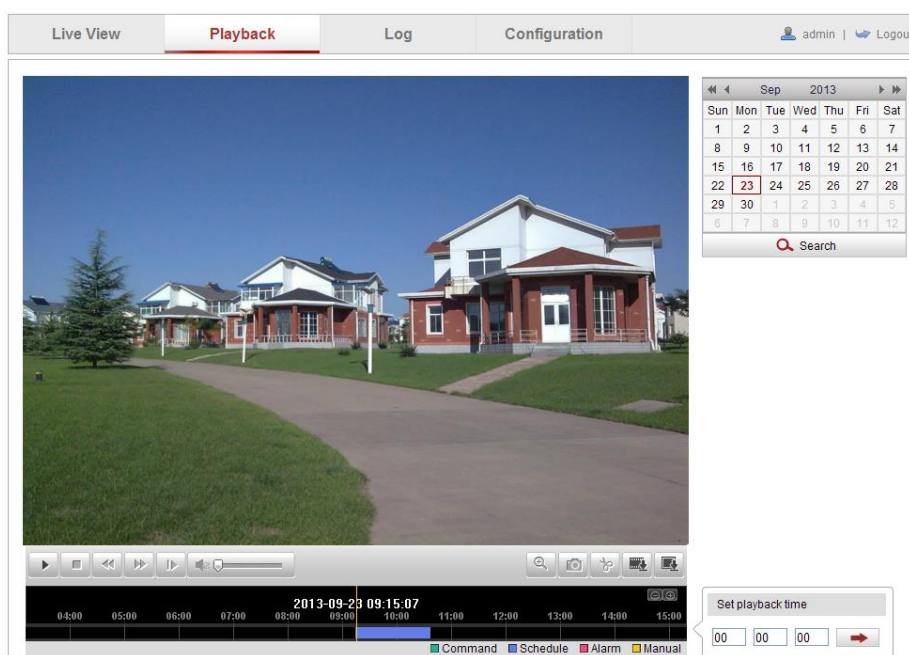


Figure 9-1 Rozhraní přehrávání

2. Vyberte datum a klikněte na tlačítko **Search** (Hledat).

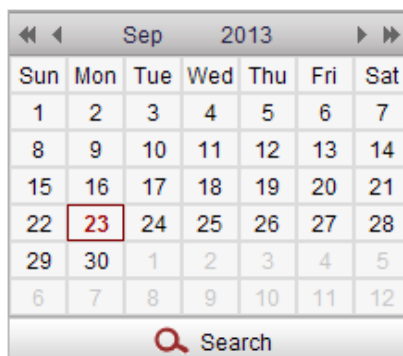



Figure 9-2 Vzhled kalendáře videa

3. Kliknutím na tlačítko  přehrajete soubory videa nalezené pro toto datum. Panel nástrojů ve spodní části rozhraní přehrávání lze použít k ovládní průběhu

přehrávání.



Figure 9-3 Panel nástrojů přehrávání

Table 9-1 Popis tlačítek

Tlačítko	Ovládní	Tlačítko	Ovládní
	Přehrát		Pořídít snímek
	Pozastavit		Spustit/zastavit ořezávání souborů videa
	Zastavit		Zapnutí izvuku a nastavení hlasitosti / vypnutí izvuku
	Zpomalit		Stáhnout soubory videa
	Zrychlit		Stáhnout pořízené snímky
	Přehrávání po snímcech		Povolit/zakázat digitální zoom

Poznámka: Místní cesty k souborům pro stažené soubory přehrávaného videa a snímky lze vybrat v rozhraní nastavení konfigurace. Podrobnosti jsou uvedeny v části 6.1.

Tažením indikátoru průběhu určete přesné místo přehrávání. Můžete také zadat čas a kliknout na tlačítko pro vyhledání místa přehrávání v poli **Set playback time** (Nastavit čas přehrávání). Rovněž můžete kliknout na tlačítko pro přiblížení/oddálení indikátoru průběhu.

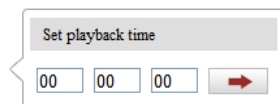


Figure 9-4 Nastavení času přehrávání

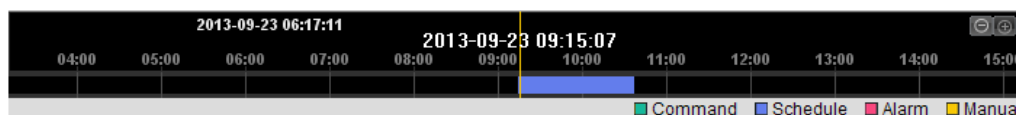


Figure 9-5 Indikátor průběhu

Různé barvy videa na indikátoru průběhu představují různé druhy videa.

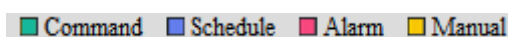


Figure 9-6 Druhy videa

Chapter 10 Vyhledávání protokolů

Účel:

Ovládání alarmy, výjimky a informace o kameře mohou být ukládány do souborů protokolu. Soubory protokoly můžete také dle potřeby exportovat.

Než začnete:

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

Postup:

1. Kliknutím na tlačítko **Log** (Protokol) v panelu nabídky vstupte do rozhraní vyhledávání protokolů.

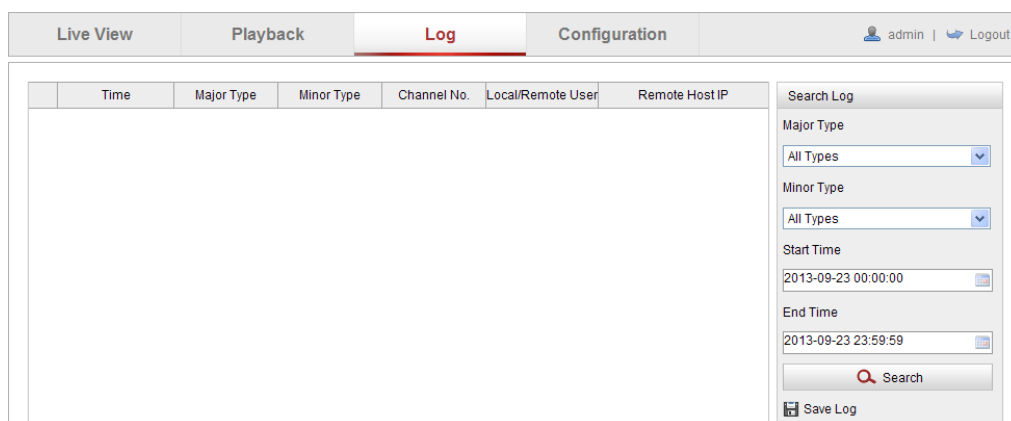
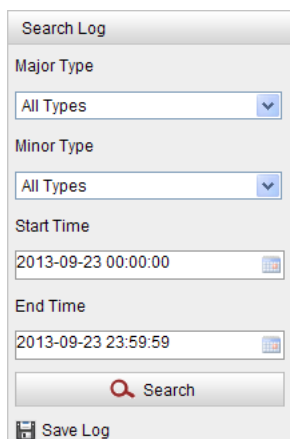


Figure 10-1 Rozhraní vyhledávání protokolů

2. Nastavte podmínky vyhledávání protokolů pro vymezení vyhledávání, jako Major Type (Hlavní typ), Minor Type (Vedlejší typ), Start Time (Čas začátku) a End Time (Čas konce).
3. Kliknutím na tlačítko **Search** (Hledat) spusťte vyhledávání souborů protokolu. Odpovídající soubory protokolu se zobrazí v rozhraní protokolu.



The image shows a 'Search Log' dialog box with the following fields and controls:

- Major Type:** A dropdown menu currently set to 'All Types'.
- Minor Type:** A dropdown menu currently set to 'All Types'.
- Start Time:** A text field containing '2013-09-23 00:00:00' with a calendar icon to its right.
- End Time:** A text field containing '2013-09-23 23:59:59' with a calendar icon to its right.
- Search:** A button with a magnifying glass icon and the text 'Search'.
- Save Log:** A button with a floppy disk icon and the text 'Save Log'.

Figure 10-2 Vyhledávání protokolů

4. Pokud chcete soubory protokolu vyexportovat, klikněte na tlačítko **Save log** (Uložit protokol) a uložte soubory protokolu do vašeho počítače.

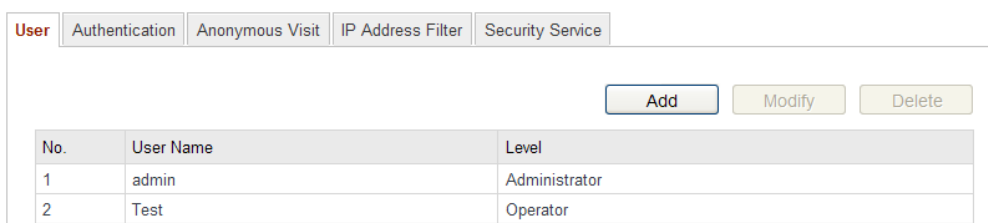
Chapter 11 Ostatní

11.1 Správa uživatelských účtů

Vstupte do rozhraní správy uživatelů:

Configuration (Konfigurace) > Basic Configuration (Základní konfigurace) > Security (Zabezpečení) > User (Uživatel)

nebo **Configuration (Konfigurace) > Advanced Configuration (Rozšířená konfigurace) > Security (Zabezpečení) > User (Uživatel)**



No.	User Name	Level
1	admin	Administrator
2	Test	Operator

Figure 11-1 Informace o uživateli

- **Přidání uživatele**

Administrátor má ve výchozím stavu všechna oprávnění a může vytvářet/upravovat/odstraňovat jiné účty.

Administrátora nelze odstranit a můžete jen změnit heslo *administrátora*.

Postup:

1. Kliknutím na tlačítko **Add** (Přidat) přidejte uživatele.
2. Zadejte parametr **User Name** (Uživatelské jméno), vyberte **Level** (Úroveň) a zadejte **Password** (Heslo).

Poznámky:

- Lze vytvořit až 31 uživatelských účtů
- Různé uživatelské účty vlastní různá oprávnění. Lze vybrat operátora nebo uživatele.



Pro vaše soukromí a lepší ochranu vašeho systému před bezpečnostními riziky důrazně doporučujeme používat pro všechny funkce a síťová zařízení silná hesla. Heslo by mělo být vytvořeno dle vašeho vlastního výběru (o délce

alespoň 8 znaků, s velkými písmeny, malými písmeny, čísly a speciálními znaky), abyste zvýšili zabezpečení výrobku.

- Za řádnou konfiguraci veškerých hesel a dalších nastavení zabezpečí ručí osoba provádějící instalaci a/nebo koncový uživatel.
3. V polích **Basic Permission** (Základní oprávnění) a **Camera Configuration** (Konfigurace kamery) můžete zaškrtnout nebo zrušit zaškrtnutí oprávnění pro nového uživatele.
 4. Kliknutím na tlačítko **OK** dokončete přidávání uživatele.

Add user

User Name: user1

Level: Operator

Password: [masked] ✔

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

Confirm: [masked]

Basic Permission	Camera Configuration
<input type="checkbox"/> Remote: Parameters Settings	<input checked="" type="checkbox"/> Remote: Live View
<input checked="" type="checkbox"/> Remote: Log Search / Interrogate Working Status	<input checked="" type="checkbox"/> Remote: PTZ Control
<input type="checkbox"/> Remote: Upgrade / Format	<input checked="" type="checkbox"/> Remote: Manual Record
<input checked="" type="checkbox"/> Remote: Two-way Audio	<input checked="" type="checkbox"/> Remote: Playback
<input type="checkbox"/> Remote: Shutdown / Reboot	
<input type="checkbox"/> Remote: Notify Surveillance Center / Trigger Alarm Output	
<input type="checkbox"/> Remote: Video Output Control	
<input type="checkbox"/> Remote: Serial Port Control	

OK Cancel

Figure 11-2 Přidání uživatele

- **Úprava uživatele**

Postup:

1. Kliknutím levým tlačítkem vyberte uživatele ze seznamu a klikněte na tlačítko **Modify** (Změnit).
2. Změňte parametry **User Name** (Uživatelské jméno), **Level** (Úroveň) nebo **Password** (Heslo).
3. V polích **Basic Permission** (Základní oprávnění) a **Camera Configuration**

(Konfigurace kamery) můžete zaškrtnout nebo zrušit zaškrtnutí oprávnění.

4. Kliknutím na tlačítko **OK** dokončete úprava uživatele.

Figure 11-3 Úprava uživatele

- **Odstranění uživatele**

Postup:

1. Kliknutím vyberte uživatele, kterého chcete odstranit, a klikněte na tlačítko **Delete** (Odstranit).
2. Kliknutím na tlačítko **OK** v místním dialogovém okně uživatele odstraníte.

11.2 Ověřování

Účel:

Streamovaná data živého náhledu můžete zabezpečit.

Postup:

1. Vstupte do rozhraní ověřování. Configuration (Konfigurace) > Advanced Configuration (Rozšířená konfigurace) > Security (Zabezpečení) > Authentication (Ověřování)

Figure 11-4 RTSP Authentication (Ověřování RTSP)

2. Výběrem typu ověřování **basic** (základní) nebo **disable** (zakázat) v rozevíracím seznamu povolte nebo zakažte ověřování RTSP.

Poznámka: Pokud zakážete ověřování RTSP, kdokoli bude mít přístup k video streamu pomocí protokolu RTSP prostřednictvím IP adresy.

3. Uložte nastavení kliknutím na tlačítko **Uložit**.

11.3 Anonymní návštěva

Povolení této funkce umožňuje návštěvu, která nemá uživatelské jméno a heslo k zařízení.

Poznámka: Pro anonymního uživatele je k dispozici pouze živý náhled.

Postup:

1. Vstupte do rozhraní anonymní návštěvy:

Configuration (Konfigurace) > Advanced Configuration (Rozšířená konfigurace) > Security (Zabezpečení) > Anonymous Visit (Anonymní návštěva)

Figure 11-5 Anonymní návštěva

2. Nastavte oprávnění **anonymní návštěvy** v rozevíracím seznamu z možností **Enable** (Povolit) nebo **Disable** (Zakázat) a povolte nebo zakažte anonymní návštěvu.

3. Uložte nastavení kliknutím na tlačítko **Uložit**.

Při vašem příštím přihlášení se zobrazí zaškrťovací políčko **Anonymous** (Anonymní).

The screenshot shows a login form with the following elements:

- A text input field labeled "User Name".
- A text input field labeled "Password".
- A button labeled "Login".
- A checked checkbox labeled "Anonymous".

Figure 11-6 Rozhraní pro přihlášení se zaškrťávacím políčkem Anonymous

4. Zaškrtněte políčko **Anonymous** a klikněte na tlačítko **Login** (Přihlásit se).

Povolením anonymního „živého náhledu“ můžete ostatním umožnit přístup ke kameře a sledování živého obrazu bez poskytnutí přihlašovacích údajů. Proto je v případě povolení funkce anonymního „živého náhledu“ kriticky důležité zajistit, že úhel záběru kamery neovlivňuje soukromí osob, jejichž obraz může být zachycen bez oprávnění.

Vzhledem k neodmyslitelné přítomnosti kamerové sledování je nevhodné v oblastech, kde lidé předpokládají vyšší úroveň soukromí.

11.4 Filtr IP adres

Účel:

Tato funkce umožňuje řízení přístupu.

Postup:

1. Vstupte do rozhraní filtrování IP adres:

Configuration (Konfigurace) > Advanced Configuration (Rozšířená konfigurace) > Security (Zabezpečení) > IP Address Filter (Filtrování IP adres)

The screenshot shows the configuration page for IP Address Filter. It includes the following elements:

- Navigation tabs: User, Authentication, Anonymous Visit, **IP Address Filter**, Security Service.
- Checkbox: Enable IP Address Filter.
- Dropdown menu: IP Address Filter Type (Forbiden).
- Buttons: Add, Modify, Delete, Clear.
- Table:

No.	IP
1	172.6.23.2

Figure 11-7 Rozhraní filtrování IP adres

2. Zaškrtněte políčko **Enable IP Address Filter** (Povolit filtrování IP adres).
3. Zvolte druh filtrování IP adres v rozevíracím seznamu; lze vybrat z možností **Forbidden** (Zakázané) a **Allowed** (Povolené).
4. Nastavte seznam filtrování IP adres.

- Přidání IP adresy

Postup:

(1) Kliknutím na tlačítko **Add** (Přidat) přidejte IP adresu.

(2) Zadejte IP adresu.

Figure 11-8 Přidání IP adresy

(3) Kliknutím na tlačítko **OK** dokončete přidávání.

- Změna IP adresy

Postup:

(1) Kliknutím levým tlačítkem vyberte IP adresu ze seznamu filtrování a klikněte na tlačítko **Modify** (Změnit).

(2) Změňte IP adresu v textovém poli.

Figure 11-9 Změna IP adresy

(3) Kliknutím na tlačítko **OK** dokončete změnu.

- Odstranění IP adresy

Kliknutím levým tlačítkem vyberte IP adresu ze seznamu filtrování a klikněte na tlačítko **Delete** (Odstranit).

- Odstranění všech IP adres

Kliknutím na tlačítko **Clear** (Smazat) odstráňte všechny IP adresy.

5. Uložte nastavení kliknutím na tlačítko **Uložit**.

11.5 Služba zabezpečení

Aby bylo možné vzdálené přihlášení a pro zlepšení zabezpečení datové komunikace, podporuje kamera službu zabezpečení pro lepší pohodlí uživatele.

Postup:

1. Přejděte do nabídky **Configuration (Konfigurace)** > **Advanced Configuration** (Rozšířená konfigurace) > **Security** (Zabezpečení) > **Security Service** (Služba zabezpečení) a vstupte do rozhraní konfigurace služby zabezpečení.

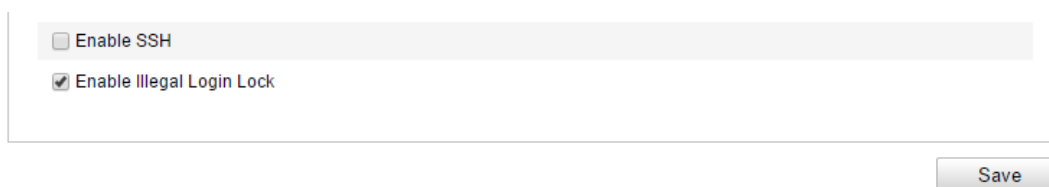


Figure 11-10 Služba zabezpečení

2. Zaškrtnutím políčka **Enable SSH** (Povolit SSH) povolte zabezpečení datové komunikace; zrušením zaškrtnutí políčka funkci SSH vypnete.
3. Zaškrtněte políčko **Enable Illegal Login Lock** (Povolit zámek neoprávněného přihlášení), a pokud 5krát po sobě zadáte nesprávné uživatelské jméno nebo heslo, zařízení se uzamkne.

Poznámka: Pokud je zařízení uzamčené, můžete se k němu pokusit přihlásit po 30 minutách nebo je zařízení nutné před dalším pokusem restartovat.

11.6 Prohlížení informací o zařízení

Vstupte do rozhraní informací o zařízení. **Configuration** (Konfigurace) > **Basic Configuration** (Základní konfigurace) > **System** (Systém) > **Device Information** (Informace o zařízení) nebo **Configuration** (Konfigurace) > **Advanced Configuration** (Rozšířená konfigurace) > **System** (Systém) > **Device Information** (Informace o zařízení).

V rozhraní **Device Information** (Informace o zařízení) lze upravit název zařízení.

Zobrazí se další informace o síťové kameře, jako model, sériové číslo, verze firmwaru, verze kódování, počet kanálů, počet pevných disků, počet vstupů alarmů a počet výstupů alarmu. Informace nelze v této nabídce měnit. Slouží k referenci pro údržbu nebo budoucí změny.

Basic Information	
Device Name	IP CAMERA
Device No.	88
Model	XX-XXXXXXXX
Serial No.	XXXXXXXXXXXXXXXXXXXX
Firmware Version	V5.1.0 build 131104
Encoding Version	V5.5 build 131104
Number of Channels	1
Number of HDDs	1
Number of Alarm Input	1
Number of Alarm Output	1

Figure 11-11 Informace o zařízení

11.7 Údržba

11.7.1 Restartování kamery

Postup:

1. Vstupte do rozhraní údržby.

Configuration (Konfigurace) > Basic Configuration (Základní konfigurace) > System (Systém) > Maintenance (Údržba)

nebo **Configuration (Konfigurace) > Advanced Configuration (Rozšířená konfigurace) > System (Systém) > Maintenance (Údržba):**

2. Kliknutím na tlačítko **Reboot** (Restartovat) restartujte síťovou kameru.

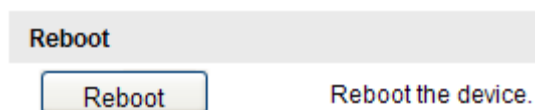


Figure 11-12 Restartování zařízení

11.7.2 Obnovení výchozích nastavení

Postup:

1. Vstupte do rozhraní údržby.

Configuration (Konfigurace) > Basic Configuration (Základní konfigurace) > System (Systém) > Maintenance (Údržba)

nebo **Configuration (Konfigurace) > Advanced Configuration (Rozšířená konfigurace) > System (Systém) > Maintenance (Údržba)**

2. Kliknutím na tlačítko **Restore** (Obnovit) nebo **Default** (Výchozí) obnovíte výchozí nastavení

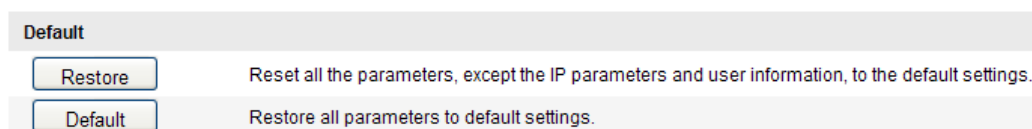


Figure 11-13 Obnovit výchozí nastavení

Poznámka: Po obnovení výchozích nastavení se obnoví také IP adresa na výchozí, takže v případě tohoto úkonu buďte opatrní.

11.7.3 Import/export souboru konfigurace

Účel:

Soubor konfigurace slouží k dávkové konfiguraci kamery, což může zjednodušit postup konfigurace, pokud je třeba nakonfigurovat velké množství kamer.

Postup:

1. Vstupte do rozhraní údržby. **Configuration (Konfigurace) > Basic Configuration (Základní konfigurace) > System (Systém) > Maintenance (Údržba)** nebo **Configuration (Konfigurace) > Advanced Configuration (Rozšířená konfigurace) > System (Systém) > Maintenance (Údržba)**
2. Kliknutím na tlačítko **Export** vyexportujete aktuální soubor konfigurace a uložíte ho na určité místo.
3. Klikněte na tlačítko **Browse** (Procházet) a vyberte uložený soubor konfigurace a

poté kliknutím na tlačítko **Import** spustíte import souboru konfigurace.

Poznámka: Po importu souboru konfigurace je třeba kameru restartovat.

4. Klikněte na tlačítko **Export** a nastavte cestu pro uložení souboru konfigurace do místního úložiště.

The screenshot shows two sections: 'Import Config. File' and 'Export Config. File'. In the 'Import' section, there is a text input field labeled 'Config File' containing the text 'F:\12'. To the right of this field are two buttons: 'Browse' and 'Import'. Below this is a 'Status' label. The 'Export' section is below and contains a single 'Export' button.

Figure 11-14 Import/export souboru konfigurace

11.7.4 Upgrade systému

Postup:

1. Vstupte do rozhraní údržby. Configuration (Konfigurace) > Basic Configuration (Základní konfigurace) > System (Systém) > Maintenance (Údržba) nebo Configuration (Konfigurace) > Advanced Configuration (Rozšířená konfigurace) > System (Systém) > Maintenance (Údržba)
2. Vyberte soubor firmwaru nebo adresář firmwaru, kde se nachází soubor upgradu.
Firmware: Určete přesnou cestu souboru upgradu.
Firmware Directory (Adresář firmwaru): Je vyžadován pouze adresář, ve kterém se nachází soubor upgradu.
3. Klikněte na tlačítko **Browse** (Procházet) a vyberte místní soubor upgradu a poté kliknutím na tlačítko **Upgrade** (Upgradovat) spustíte vzdálený upgrade.

The screenshot shows a 'Remote Upgrade' section. It features a dropdown menu currently set to 'Firmware'. Below the dropdown is a text input field. To the right of the input field are two buttons: 'Browse' and 'Upgrade'. The dropdown menu is open, showing 'Firmware' and 'Firmware Directory' as options.

Figure 11-15 Vzdálený upgrade

Poznámka: Průběh upgradu trvá 1 ~ 10 minut. V jeho průběhu neodpojujte napájení kamery; po upgradu se kamera automaticky restartuje.

11.8 Nastavení rozhraní RS-232

Port RS-232 lze použít dvěma způsoby:

- Konfigurace parametrů: Připojte počítač ke kameře prostřednictvím sériového portu. Parametry zařízení lze konfigurovat pomocí softwaru, jako HyperTerminal. Parametry sériového portu musí být stejné jako parametry sériového portu kamery.
- Transparentní kanál: Připojte sériové zařízení přímo ke kameře. Sériové zařízení bude ovládáno vzdáleně počítačem prostřednictvím sítě.

Postup:

1. Vstupte do rozhraní nastavení portu RS-232:

nebo Configuration (Konfigurace) > Advanced Configuration (Rozšířená konfigurace) > System (Systém) > RS232

Device Information	Time Settings	Maintenance	RS232	RS485	DST	Service
Baud Rate	115200 bps					
Data Bit	8					
Stop Bit	1					
Parity	None					
Flow Ctrl	None					
Usage	Console					

Figure 11-16 Nastavení rozhraní RS-232

Poznámka: Pokud chcete připojit kameru k portu RS-232, parametry portu RS-232 by se měly přesně shodovat se zde nakonfigurovanými parametry.

2. Uložte nastavení kliknutím na tlačítko **Uložit**.

11.9 Nastavení RS-485

Účel:

Sériový port RS-485 se používá k ovládání funkcí PTZ kamery. Konfigurace parametrů PTZ by měla být provedena předtím, než budete ovládat PTZ jednotku.

Postup:

1. Vstupte do rozhraní nastavení portu RS-485:

**Configuration (Konfigurace) > Advanced Configuration (Rozšířená konfigurace)
> System (Systém) > RS485**

Field	Value
Baud Rate	9600 bps
Data Bit	8
Stop Bit	1
Parity	None
Flow Ctrl	None
PTZ Protocol	PELCO-D
PTZ Address	0

Figure 11-17 Nastavení RS-485

2. Nastavte parametry rozhraní RS-485 a uložte nastavení kliknutím na tlačítko **Save (Uložit)**.

Ve výchozím stavu jsou nastaveny parametry Baud Rate (Rychlost v baudech) na hodnotu 9 600 baudů/s, Data Bit (Datové bity) na hodnotu 8, Stop Bit na hodnotu 1 a parametry Parity (Parita) a Flow Control (Řízení toku) na možnost None (Žádné).

Poznámka: Parametry Baud Rate, PTZ Protocol (Protokol PTZ) a PTZ Address (Adresa PTZ) by se měly přesně shodovat s parametry PTZ kamery.

11.10 Nastavení služeb

Přejděte do nabídky **Configuration (Konfigurace) > Advanced Configuration (Rozšířená konfigurace) > System (Systém) > Service (Služba)** vstupte do rozhraní nastavení služeb.

Nastavení služeb označují hardwarové služby, které kamera podporuje, a liší se dle různých kamer.

V případě kamer s podporou funkcí IR LED, ABF (Auto Back Focus), Auto Defog nebo Status LED můžete přejít do hardwarových služeb a povolit nebo zakázat příslušné služby dle aktuálních požadavků.

Příloha

Příloha 1 Představení softwaru SADP

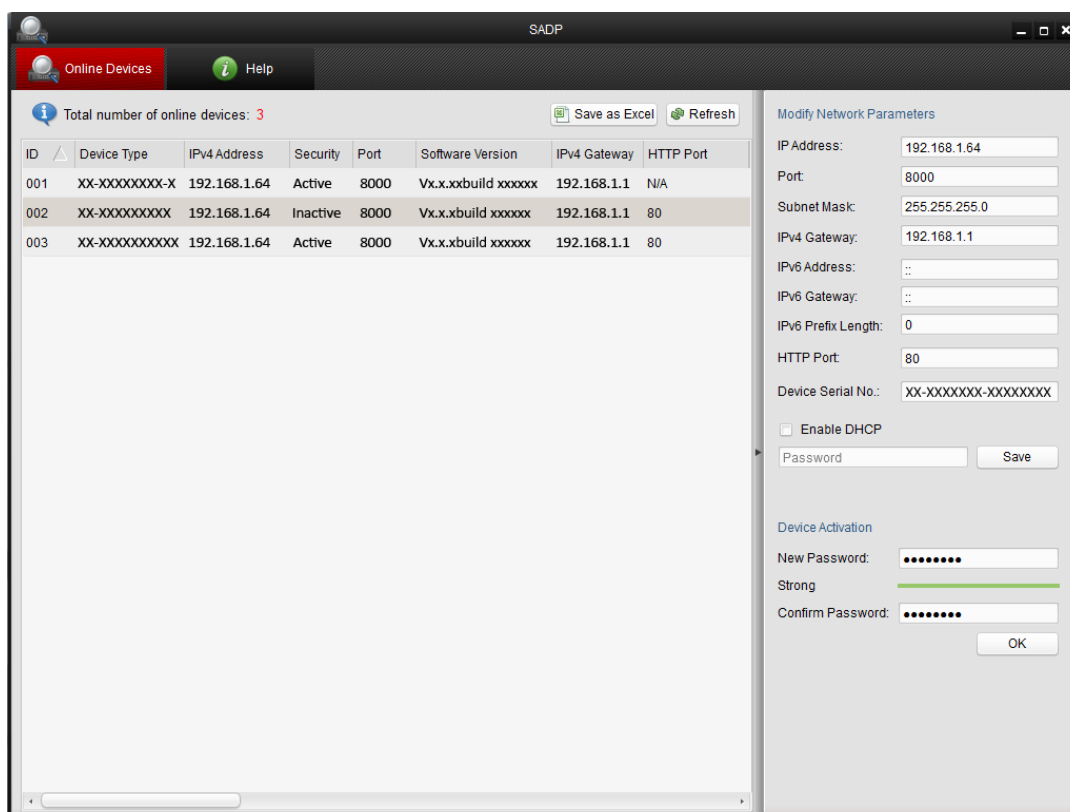
● Popis softwaru SADP

SADP (Search Active Devices Protocol) je druh nástroje pro uživatelsky přívětivé vyhledávání zařízení online bez instalace. Vyhledává aktivní zařízení online v rámci vaší podsítě a zobrazuje informace o zařízeních. Pomocí tohoto softwaru také můžete změnit základní informace o síti zařízení.

● Vyhledávání aktivních zařízení online

◆ Automatické vyhledávání zařízení online

Software SADP po spuštění automaticky každých 15 sekund vyhledává online zařízení v podsíti, v jaké je váš počítač. Zobrazuje celkový počet a informace o vyhledaných zařízeních v rozhraní Online Devices (Zařízení online). Zobrazí se informace o zařízení, jako typ zařízení, IP adresa a číslo portu atd.



Obr. A.1.1 Vyhledávání zařízení online





Poznámka:

Zařízení mohou být vyhledána a zobrazena v seznamu 15 sekund poté, co přešla do stavu online; 45 sekund poté, co přešla do stavu offline, budou odstraněna.

◆ Manuální vyhledávání zařízení online

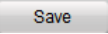
Můžete také kliknout na tlačítko  a obnovit seznam zařízení online ručně. Nově nalezená zařízení se přidají do seznamu.



Kliknutím na tlačítka  nebo  v záhlavích jednotlivých sloupců seřadíte informace; kliknutím na tlačítko  rozbalíte tabulku zařízení a skryjete panel parametrů sítě na pravé straně; kliknutím na tlačítko  zobrazíte panel parametrů sítě.

● Úprava parametrů sítě

Postup:

1. Vyberte zařízení, které chcete upravit, v seznamu zařízení, a parametry sítě zařízení se zobrazí v panelu **Modify Network Parameters** (Upravit parametry sítě) napravo.
2. Upravte modifikovatelné parametry sítě, např. IP adresu a číslo portu.
3. Chcete-li uložit změny, zadejte heslo účtu správce zařízení do pole **Password** (Heslo) a kliknutím na tlačítko  uložte změny.



- *Pro vaše soukromí a lepší ochranu vašeho systému před bezpečnostními riziky důrazně doporučujeme používat pro všechny funkce a síťová zařízení silná hesla. Heslo by mělo být vytvořeno dle vašeho vlastního výběru (o dříve alespoň 8 znaků, s velkými písmeny, malými písmeny, čísly a speciálními znaky), abyste zvýšili zabezpečení výrobku.*
- *Za řádnou konfiguraci veškerých hesel a dalších nastavení zabezpečí ručí osoba provádějící instalaci a/nebo koncový uživatel.*

Modify Network Parameters

IP Address:

Port:

Subnet Mask:


IPv4 Gateway:

IPv6 Address:

IPv6 Gateway:

IPv6 Prefix Length:

Serial No.:

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

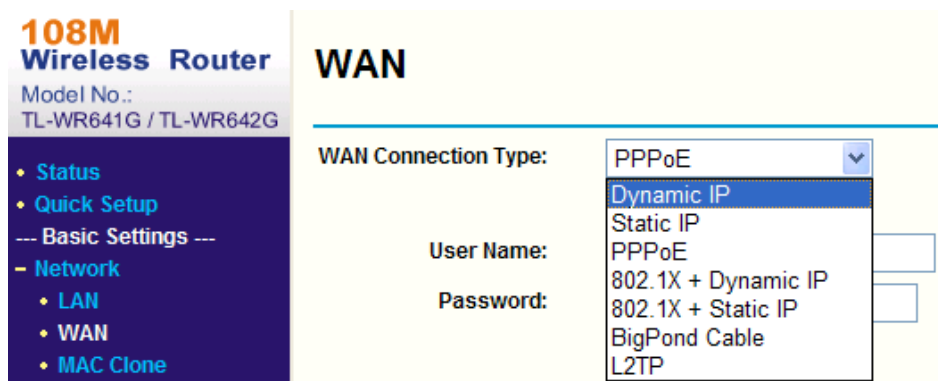
Obr. A.1.2 Úprava parametrů sítě

Příloha 2 Mapování portů

Následující nastavení jsou určena pro směrovač TP-LINK (TL-WR641G). Nastavení se liší dle modelu směrovače.

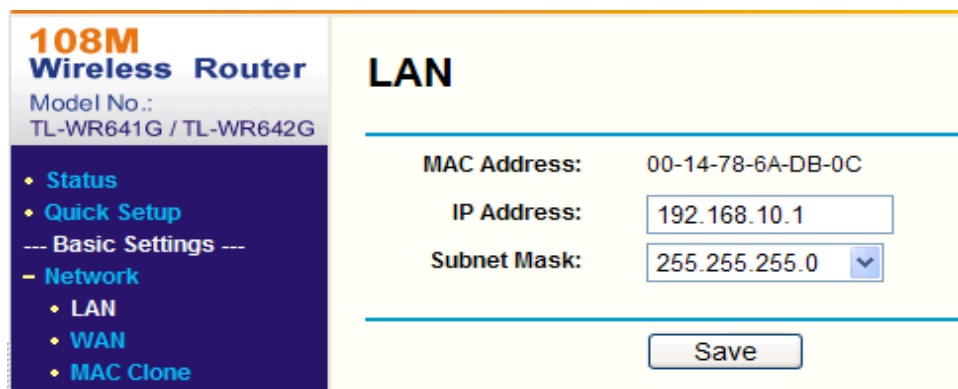
Postup:

1. Vyberte parametr **WAN Connection Type** (Typ připojení k síti WAN) dle vyobrazení



Obr. A 2.1 Výběr typu připojení k síti WAN

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



Obr. A.2.2 Nastavení parametrů sítě LAN

3. Nastavte mapování portů ve virtuálních serverech v části **Forwarding** (Předávání). Ve výchozím stavu kamera používá porty 80, 8000 a 554. Hodnoty těchto portů můžete změnit pomocí webového prohlížeče nebo klientského softwaru.

Příklad:

Když jsou kamery připojené ke stejnému směrovači, můžete nakonfigurovat porty kamery 80, 8000 a 554 s IP adresou 192.168.1.23 a porty další kamery 81, 8001, 555, 8201 s IP adresou IP 192.168.1.24. Použijte následující postupu:

Postup:

1. V případě výše uvedených nastavení namapujte porty 80, 8000, 554 a 8200 pro síťovou kameru s IP adresou 192.168.1.23
2. Namapujte porty 81, 8001, 555 a 8201 pro síťovou kameru s IP adresou 192.168.1.24
3. Povolte protokoly **ALL** (Všechny) nebo **TCP**.
4. Zaškrtněte políčko **Enable** (Povolit) a kliknutím na tlačítko **Save** (Uložit) uložte nastavení.

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

Virtual Servers


ID	Service Port	IP Address	Protocol	Enable
1	80	192.168.10.23	ALL	<input checked="" type="checkbox"/>
2	8000	192.168.10.23	ALL	<input checked="" type="checkbox"/>
3	554	192.168.10.23	ALL	<input checked="" type="checkbox"/>
4	8200	192.168.10.23	ALL	<input checked="" type="checkbox"/>
5	81	192.168.10.24	ALL	<input checked="" type="checkbox"/>
6	8001	192.168.10.24	ALL	<input checked="" type="checkbox"/>
7	555	192.168.10.24	ALL	<input checked="" type="checkbox"/>
8	8201	192.168.10.24	ALL	<input checked="" type="checkbox"/>

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

Previous Next Clear All Save

Obr. A.2.3 Mapování portů

Poznámka: Port síťové kamery nesmí být v konfliktu s jinými porty. Například jeden z portů pro webovou správu směrovače je 80. Změňte port kamery, pokud je stejný jako port pro správu.



First Choice for Security Professionals