



HIKVISION

Síťová termokamera v provedení bullet

Návod k obsluze

UD02330B

Návod k obsluze

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

VŠECHNA PRÁVA VYHRAZENA.

Jakékoli a veškeré informace, včetně, mimo jiné, textů, obrázků a grafů jsou vlastnictvím společnosti Hangzhou Hikvision Digital Technology Co., Ltd. nebo jejích poboček (dále uváděno jako „Hikvision“). Žádnou část tohoto návodu k obsluze (dále uváděného jako „návod“) ani návod jako celek nelze bez předchozího písemného souhlasu společnosti Hikvision jakýmkoli způsobem reprodukovat, měnit, překládat ani šířit. Pokud není jinak výslovně uvedeno, společnost Hikvision neposkytuje ve vztahu k návodu žádné záruky ani ujištění, a to ani výslovné, ani vyplývající.

Informace o tomto návodu

Toto je příručka k síťové termokameře v provedení bullet (V5.3.7).

V návodu jsou obsaženy pokyny k používání a obsluze výrobku. Obrázky, schémata, snímky a veškeré ostatní zde uvedené informace slouží pouze jako popis a vysvětlení. Informace obsažené v tomto návodu podléhají vzhledem k aktualizacím firmwaru nebo z jiných důvodů změnám bez upozornění. Nejnovější verzi naleznete na webových stránkách společnosti (<http://overseas.hikvision.com/en/>).

Používejte tento návod k obsluze pod dohledem profesionálních odborníků.

Potvrzení o ochranných známkách

HIKVISION a ostatní ochranné známky a loga společnosti Hikvision jsou vlastnictvím společnosti Hikvision v různých jurisdikcích. Ostatní níže uvedené ochranné známky a loga jsou vlastnictvím příslušných vlastníků.

Prohlášení o vyloučení odpovědnosti

POPISOVANÝ VÝROBEK JE DO MAXIMÁLNÍHO ROZSAHU POVOLENÉHO PŘÍSLUŠNÝMI ZÁKONY SPOLU SE SVÝM HARDWAREM, SOFTWAREM A FIRMWAREM POSKYTOVÁN „TAK, JAK JE“ SE VŠEMI SVÝMI ZÁVADAMI A CHYBAMI A SPOLEČNOST HIKVISION NEPOSKYTUJE ŽÁDNÉ ZÁRUKY, VÝSLOVNĚ VYJÁDŘENÉ ANI VYPLÝVAJÍCÍ, VČETNĚ, ALE NIKOLI VÝHRADNĚ, PRODEJNOSTI, USPOKOJIVÉ KVALITY, VHODNOSTI PRO URČITÝ ÚČEL A BEZ NEOPRÁVNĚNÉHO ZÁSAHU DO PRÁV TŘETÍ STRANY. V ŽÁDNÉM PŘÍPADĚ NEBUDE SPOLEČNOST HIKVISION, JEJÍ ŘEDITELÉ, MANAŽEŘI, ZAMĚSTNANCI ANI ZÁSTUPCI ZODPOVĚDNÍ ZA JAKÉKOLI ZVLÁŠTNÍ, NÁSLEDNÉ, NÁHODNÉ NEBO NEPŘÍMÉ ŠKODY, VČETNĚ, MIMO JINÉ, ŠKOD ZE ZTRÁTY OBCHODNÍHO ZISKU, PŘERUŠENÍ OBCHODNÍ ČINNOSTI NEBO ZE ZTRÁTY DAT NEBO DOKUMENTACE VE SPOJENÍ S POUŽÍVÁNÍM TOHOTO VÝROBKU, A TO ANI V PŘÍPADĚ, ŽE SPOLEČNOST HIKVISION BYLA NA MOŽNOST TAKOVÝCHTO ŠKOD UPOZORNĚNA.

POUŽÍVÁNÍ VÝROBKŮ S PŘÍSTUPEM NA INTERNET JE ZCELA NA VAŠE VLASTNÍ RIZIKO. SPOLEČNOST HIKVISION NENESE ŽÁDNOU ZODPOVĚDNOST ZA NEOBVYKLÉ FUNGOVÁNÍ, ÚNIK OSOBNÍCH ÚDAJŮ ANI JINÉ ŠKODY VYPLÝVAJÍCÍ Z KYBERÚTOKU, ÚTOKU HACKERŮ, NAPADENÍ VIRY NEBO JINÝCH BEZPEČNOSTNÍCH RIZIK INTERNETU. SPOLEČNOST HIKVISION VŠAK V PŘÍPADĚ POTŘEBY POSKYTNE OKAMŽITOU TECHNICKOU PODPORU.

PRÁVO VZTAHUJÍCÍ SE KE SLEDOVÁNÍ SE LIŠÍ DLE JURISDIKCE. PŘED POUŽÍVÁNÍM TOHOTO VÝROBKU SI PŘEČTĚTE VŠECHNY PŘÍSLUŠNÉ ZÁKONY VAŠÍ JURISDIKCE, ABYSTE ZAJISTILI, ŽE POUŽÍVÁNÍ JE V SOULADU S PŘÍSLUŠNÝMI ZÁKONY. SPOLEČNOST HIKVISION NEPONESE ŽÁDNOU ZODPOVĚDNOST V PŘÍPADĚ, ŽE SE TENTO VÝROBEK POUŽÍVÁ K NELEGÁLNÍM ÚČELŮM.

V PŘÍPADĚ JAKÉHOKOLI KONFLIKTU MEZI TÍMTO NÁVODEM A PŘÍSLUŠNÝMI ZÁKONY PLATÍ DRUHÉ ZMÍNĚNÉ.

Právní informace

Informace o směrnících FCC

Soulad se směrnici FCC: Toto zařízení bylo testováno a shledáno vyhovujícím v souladu s omezeními pro digitální zařízení podle části 15 směrnic FCC. Tyto limity jsou navrženy tak, aby poskytovaly náležitou ochranu před škodlivým rušením, když je zařízení používáno v komerčním prostředí. Toto zařízení generuje, využívá a může vyzařovat radiofrekvenční energii, a pokud není instalováno a používáno v souladu s návodem k obsluze, může způsobit škodlivé rušení rádiové komunikace. Provoz tohoto zařízení v obytných oblastech bude pravděpodobně způsobovat škodlivé rušení a v takovém případě bude po uživateli požadováno, aby rušení odstranil na své vlastní náklady.

Podmínky směrnic FCC

Toto zařízení splňuje požadavky části 15 směrnic FCC. Provoz je podmíněn následujícími dvěma podmínkami:

1. Toto zařízení nesmí způsobovat škodlivé rušení.
2. Toto zařízení musí přijmout libovolné přijaté rušení, včetně rušení, které může způsobit nežádoucí činnost.

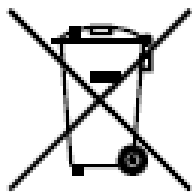
Prohlášení o shodě s předpisy EU



Tento produkt a případné dodávané příslušenství jsou označeny jako „CE“, což znamená, že jsou v souladu s platnými harmonizovanými evropskými normami uvedenými v směrnici EMC 2014/30/ES, směrnicí RoHS 2011/65/ES.



Směrnice 2012/19/ES (WEEE): Výrobky označené tímto symbolem nelze v Evropské unii likvidovat společně s netříděným domovním odpadem. Tento výrobek řádně recyklujte při zakoupení nového ekvivalentního výrobku vrácením svému místnímu dodavateli, nebo jej zlikvidujte odevzdáním v určených sběrných místech. Více informací naleznete na webu: www.recyclethis.info.



Směrnice 2006/66/ES (týkající se baterií): Tento výrobek obsahuje baterii, kterou nelze v Evropské unii likvidovat společně s netříděným domovním odpadem. Konkrétní informace o baterii naleznete v dokumentaci výrobku. Baterie je označena tímto symbolem, který může obsahovat písmena značící kadmium (Cd), olovo (Pb) nebo měď (Hg). Baterii řádně zlikvidujte odevzdáním svému dodavateli nebo na určeném sběrném místě. Další informace naleznete na adrese: www.recyclethis.info.

Soulad se směrnicí ICES-003 kanadského Ministerstva průmyslu

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

Bezpečnostní pokyny

Účelem těchto pokynů je to, aby uživatel používal tento produkt správně a nedošlo k žádným nebezpečím ani ztrátě majetku.

Toto opatření se dělí na „Upozornění“ a „Výstrahy“:

Výstrahy: Nebude-li některá z těchto výstrah respektována, může dojít k vážnému zranění nebo smrti.

Upozornění: Nebude-li některé z těchto upozornění respektováno, může dojít ke zranění nebo poškození zařízení.

Výstrahy Dodržujte tyto bezpečnostní pokyny, abyste předešli vážnému zranění nebo smrti.	Upozornění Aby se zabránilo možnému zranění nebo věcným škodám, respektujte tato opatření.



Výstrahy:

- Používejte napájecí adaptér, který splňuje standard SELV (velmi nízké bezpečnostní napětí). A zdroj 12 V stejnosm. nebo 24 V stř. (v závislosti na modelu) odpovídá normě IEC60950-1 a standardu pro omezený zdroj napájení.
- Nevystavujte zařízení dešti ani vlhkosti, aby se snížilo nebezpečí vzniku požáru nebo úrazu elektrickým proudem.
- Tato montáž by měla být provedena kvalifikovanou servisní osobou a musí vyhovovat všem místním předpisům.

- Namontujte do napájecího obvodu zařízení proti výpadkům elektřiny pro pohodlné napájení při výpadku dodávek elektřiny.
- Pokud připevňujete kameru ke stropu, zkontrolujte, zda strop unese zatížení gravitační silou vyšší než 50 N.
- V případě, že produkt nefunguje správně, obraťte se na prodejce nebo na nejbližší servisní středisko. Nikdy se nepokoušejte sami rozebírat kameru. (Neneseme žádnou odpovědnost za problémy způsobené neoprávněnými opravami nebo údržbou).



Upozornění:

- Než kameru použijete, zkontrolujte, zda je napájecí napětí správné.
- Neupusťte kameru a nevystavujte ji ani jiným fyzickým nárazům.
- Nedotýkejte se prsty modulů senzoru. Pokud je třeba provést čištění, použijte čistý hadřík s malým množstvím etanolu a jemně otírejte. Pokud nebudete kameru po delší dobu používat, nasad'te kryt objektivu, abyste ochránili senzor před nečistotami.
- Nemiřte objektivem kamery na silný zdroj světla, jako je slunce nebo klasická žárovka. Silné světlo může způsobit nevratné poškození kamery.
- Laserový paprsek může vypálit snímač. Při použití jakékoliv laserové zařízení proto zajistěte, aby povrch snímače nebyl vystaven laserovému paprsku.
- Kameru neinstalujte v místech s extrémně vysokými nebo nízkými teplotami (provozní teplota by měla být mezi -40 °C a 65 °C), v prašném nebo vlhkém prostředí, a nevystavujte ji vysokému elektromagnetickému záření.
- Aby nedošlo k hromadění tepla, je nutná pro správné provozní prostředí dobrá ventilace.
- Kameru nevystavujte působení vody ani jiných kapalin.
- Během přepravy musí být kamera zabalena v původním obalu.
- Nesprávné používání nebo výměna baterie by mohly vést k nebezpečí výbuchu. Používejte typ baterie doporučený výrobcem.

Poznámky:

U kamer podporujících infračervené osvětlení je nutné dbát následujících bezpečnostních opatření, aby nedocházelo k odrazům infračerveného záření:

- Prach nebo mastnota na kopulovitém krytu způsobí odrazy infračerveného záření. Fólii kopulovitého krytu sejměte až po dokončení montáže. Pokud se na kopulovitém krytu nachází prach nebo mastnota, vyčistěte kopulovitý kryt měkkým čistým hadříkem a izopropylalkoholem.

- Zajistěte, aby místo montáže nemělo odrazný povrch, na kterém by docházelo v těsné blízkosti kamery k odrazům objektů. Infračervené osvětlení z kamery se může odrážet zpět do objektivu, a způsobovat tak odrazy.
- Pěnový prstenec okolo objektivu musí být usazen v jedné rovině s vnitřním povrchem kopule, aby byl objektiv izolován od infračervených diod LED. Připevněte kopulovitý kryt k tělu kamery tak, aby k sobě pěnový prstenec a kopulovitý kryt těsně přiléhaly.

Obsah

Kapitola 1 Systémové požadavky	11
Kapitola 2 Síťové připojení.....	12
2.1 Nastavení síťové kamery pomocí sítě LAN.....	12
2.1.1 Připojení kabeláže přes LAN	12
2.1.2 Aktivace kamery	13
2.2 Nastavení síťové kamery pomocí sítě WAN.....	19
2.2.1 Připojení se statickou IP adresou	19
2.2.2 Připojení s dynamickou IP adresou.....	20
Kapitola 3 Přístup k síťové kamerě.....	23
3.1 Přístup přes webové prohlížeče.....	23
3.2 Přístup pomocí klientského softwaru.....	25
Kapitola 4 Živé zobrazení.....	27
4.1 Stránka živého zobrazení	27
4.2 Spuštění živého zobrazení	28
4.3 Ruční nahrávání a zachycování snímků	29
Kapitola 5 Konfigurace síťové kamery	30
5.1 Konfigurace místních parametrů	30
5.2 Konfigurace nastavení času.....	32
5.3 Konfigurace nastavení sítě	35
5.3.1 Konfigurace nastavení protokolu TCP/IP	35
5.3.2 Konfigurace nastavení portu	36
5.3.3 Konfigurace nastavení PPPoE	37
5.3.4 Konfigurace nastavení DDNS	38
5.3.5 Konfigurace nastavení SNMP	41
5.3.6 Konfigurace nastavení 802.1X	43
5.3.7 Konfigurace nastavení QoS	44
5.3.8 Konfigurace nastavení UPnP™	45
5.3.9 Alarmem spuštěné odeslání e-mailu	45
5.3.10 Konfigurace nastavení NAT (Network Address Translation).....	47
5.3.11 Konfigurace nastavení FTP	48
5.3.12 Nastavení protokolu HTTPS.....	49
5.4 Konfigurace nastavení videa a zvuku.....	52
5.4.1 Konfigurace nastavení videa.....	52
5.4.2 Konfigurace nastavení zvuku.....	54
5.4.3 Konfigurace kódování oblasti ROI.....	55
5.5 Konfigurace parametrů obrazu	57

5.5.1	Konfigurace nastavení displeje.....	57
5.5.2	Konfigurace nastavení nabídky OSD.....	59
5.5.3	Konfigurace nastavení překrytí textem.....	61
5.5.4	Konfigurace masky privátních zón.....	61
5.5.5	Konfigurace překrytí obrazu.....	62
5.5.6	Konfigurace DPC (korekce chybných pixelů).....	63
5.6	Konfigurace a správa událostí alarmu.....	64
5.6.1	Konfigurace detekce pohybu.....	65
5.6.2	Konfigurace alarmu na neoprávněnou manipulaci s videem.....	69
5.6.3	Konfigurace vstupu alarmu.....	71
5.6.4	Konfigurace výstupu alarmu.....	72
5.6.5	Ošetření výjimky.....	73
5.6.6	Konfigurace detekce výjimky zvuku.....	74
5.6.7	Detekce změny scény.....	75
5.6.8	Konfigurace dynamické detekce zdroje požáru.....	76
5.7	Měření teploty.....	77
5.7.1	Konfigurace měření teploty.....	77
5.7.2	Měření teploty a alarm.....	78
5.8	Konfigurace VCA.....	80
5.8.1	Typ zdroje VCA.....	80
5.8.2	Informace VCA.....	81
5.8.3	Analýza chování.....	82
Kapitola 6 Nastavení úložiště.....		91
6.1	Správa úložiště.....	91
6.2	Konfigurace nastavení NAS.....	91
6.3	Konfigurace harmonogramu nahrávání.....	94
6.4	Konfigurace nastavení snímku.....	99
Kapitola 7 Přehrávání.....		101
Kapitola 8 Vyhledávání v protokolu.....		103
Kapitola 9 Jiné.....		104
9.1	Správa uživatelských účtů.....	104
9.2	Ověřování.....	106
9.3	Anonymní návštěva.....	107
9.4	Filtr adres IP.....	108
9.5	Služba zabezpečení.....	110
9.6	Zobrazení informací o zařízení.....	110
9.7	Údržba.....	111

9.7.1	Restartování kamery	111
9.7.2	Obnovení výchozích nastavení	112
9.7.3	Export/import konfiguračního souboru.....	112
9.7.4	Upgrade systému	113
9.8	Nastavení RS-485	113
9.9	Nastavení služby	114
<i>Dodatek</i>	<i>.....</i>	<i>115</i>
Dodatek 1	Úvod k softwaru SADP	115
Dodatek 2	Mapování portů	118

Kapitola 1 Systémové požadavky

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

Procesor: Intel Pentium IV 3,0 GHz nebo vyšší

RAM: 1 GB nebo více

Displej: Rozlišení 1024 × 768 nebo vyšší

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

Kapitola 2 Síťové připojení

Poznámka:

- Upozorňujeme, že používání produktu s přístupem k internetu může podléhat síťovým bezpečnostním rizikům. V rámci prevence síťových útoků a úniků informací doporučujeme posílit vaši vlastní ochranu. V případě, že produkt nefunguje správně, obraťte se na prodejce nebo na nejbližší servisní středisko.
- K zajištění zabezpečení sítě síťové kamery doporučujeme, abyste k síťové kameře pravidelně přistupovali a udržovali ji. Potřebujete-li takovou službu, můžete nás kontaktovat.

Než začnete:

- Chcete-li síťovou kameru nastavit prostřednictvím sítě LAN (Local Area Network), postupujte podle instrukcí v *Části 2.1 Nastavení síťové kamery pomocí sítě LAN*.
- Chcete-li síťovou kameru nastavit prostřednictvím sítě WAN (Wide Area Network), postupujte podle instrukcí v *Části 2.2 Nastavení síťové kamery pomocí sítě WAN*.

2.1 Nastavení síťové kamery pomocí sítě LAN

Účel:

Chcete-li kameru zobrazit a nakonfigurovat pomocí sítě LAN, je nutné síťovou kameru připojit do stejné podsítě, jako je počítač. K vyhledání a změně IP adresy síťové kamery je také nutné nainstalovat software SADP nebo iVMS-4200.

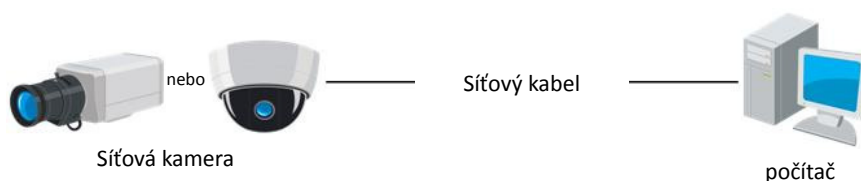
Poznámka: Podrobné pokyny k SADP najdete v dodatku 1.

2.1.1 Připojení kabeláže přes LAN

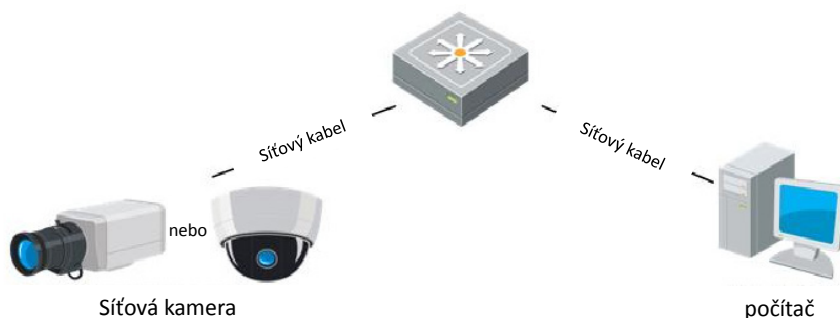
Na následujících obrázcích jsou uvedeny dva způsoby propojení síťové kamery a počítače kabelem:

Účel:

- Chcete-li síťovou kameru otestovat, můžete ji připojit pomocí síťového kabelu přímo k počítači, viz Obrázek 2–1.
- Pro nastavení síťové kamery prostřednictvím sítě LAN a přepínače nebo směrovače postupujte podle Obrázek 2–2.



Obrázek 2–1 Přímé připojení



Obrázek 2–2 Připojení prostřednictvím přepínače nebo směrovače

2.1.2 Aktivace kamery

Než budete moci kameru používat, je nutné ji nejdříve aktivovat nastavením silného hesla.

Podporována je aktivace prostřednictvím webového prohlížeče, aktivace prostřednictvím softwaru SADP i aktivace prostřednictvím klientského softwaru.

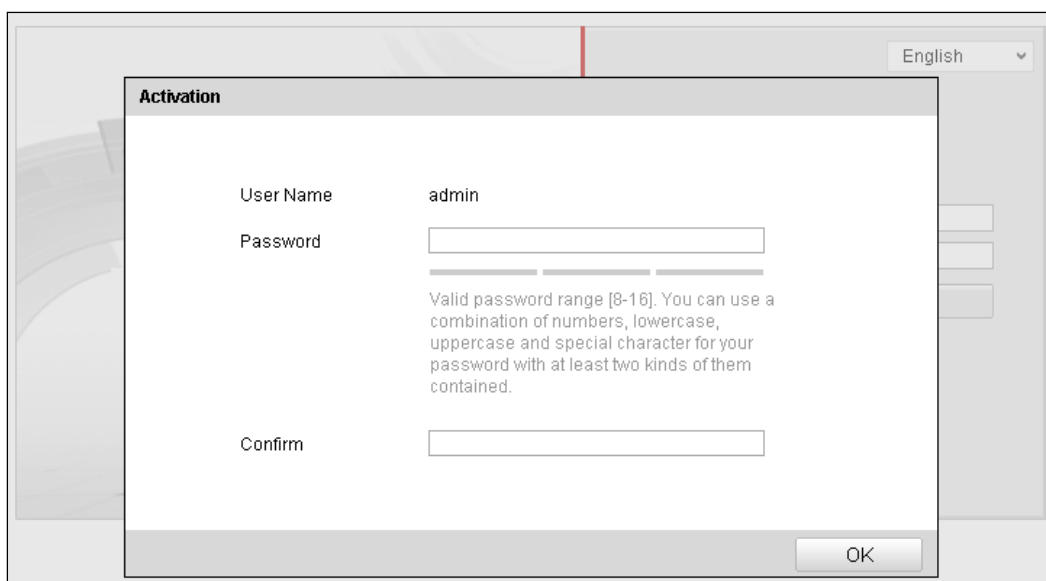
❖ Aktivace přes webový prohlížeč

Kroky:

1. Zapněte kameru a připojte ji k síti.
2. Do adresního řádku zadejte IP adresu a po kliknutí na Enter vstoupíte do aktivačního rozhraní.

Poznámky:

- Výchozí IP adresa kamery je 192.168.1.64.
- Pokud kamera ve výchozím nastavení povoluje protokol DHCP, musíte ji aktivovat prostřednictvím softwaru SADP. Další informace o aktivaci prostřednictvím softwaru SADP naleznete v následující kapitole.



Obrázek 2–3 Aktivační rozhraní (web)

3. Vytvořte heslo a zadejte je do pole s heslem.



DOPORUČUJEME SILNÉ HESLO – Pro zvýšení zabezpečení vašeho produktu důrazně doporučujeme vytvoření silného hesla, které vyberete sami (s použitím minimálně 8 znaků, včetně velkých a malých písmen, čísel a speciálních znaků). Doporučujeme také, abyste heslo pravidelně měnili, zvláště v systémech s vysokým zabezpečením. Změna hesla jednou za měsíc nebo za týden lépe ochrání váš výrobek.

4. Potvrďte heslo.
5. Kliknutím na tlačítko OK uložte heslo a přejděte k oknu živého zobrazení.

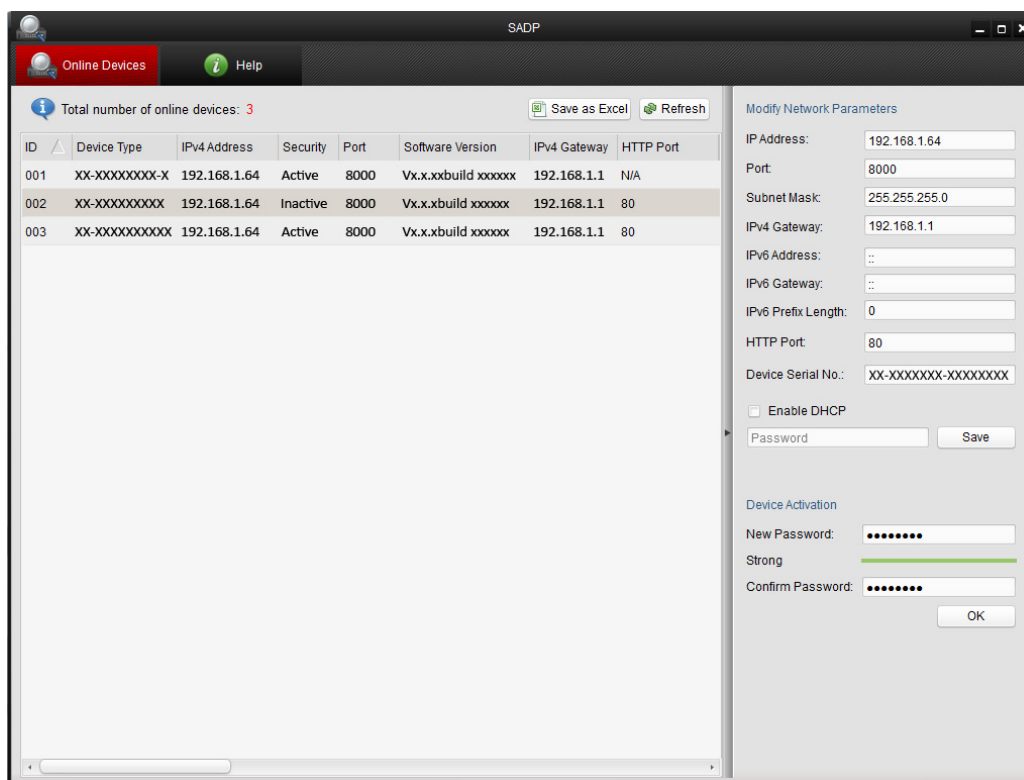
❖ **Aktivace přes software SADP**

Software SADP se používá k rozpoznávání zařízení online, aktivaci kamery a obnovení hesla.

Software SADP získáte z dodaného disku nebo na oficiálních internetových stránkách. Nainstalujte SADP podle pokynů. Postupujte podle pokynů k aktivaci kamery.

Kroky:

1. Spusťte software SADP pro vyhledávání zařízení online.
2. V seznamu zařízení zkontrolujte stav zařízení a vyberte neaktivní zařízení.



Obrázek 2–4 Rozhraní SADP

3. Vytvořte heslo a zadejte je do pole hesla a heslo potvrďte.



DOPORUČUJEME SILNÉ HESLO – Pro zvýšení zabezpečení vašeho produktu důrazně doporučujeme vytvoření silného hesla, které vyberete sami (s použitím minimálně 8 znaků, včetně velkých a malých písmen, čísel a speciálních znaků). Doporučujeme také, abyste heslo pravidelně měnili, zvláště v systémech s vysokým zabezpečením. Změna hesla jednou za měsíc nebo za týden lépe ochrání váš výrobek.

4. Uložte heslo kliknutím na **OK**.

V automatické otevřeném okně můžete zkontrolovat, zda byla aktivace dokončena. Pokud se aktivace nezdaří, zkontrolujte, zda heslo splňuje požadavky, a opakujte akci.

5. Ruční změnou IP adresy nebo zaškrtnutím políčka Enable DHCP změňte IP adresu zařízení na stejnou podsíť s počítačem.

Modify Network Parameters

IP Address: 192.168.1.64

Port: 8000

Subnet Mask: 255.255.255.0

IPv4 Gateway: 192.168.1.1

IPv6 Address: ::

IPv6 Gateway: ::

IPv6 Prefix Length: 0

HTTP Port: 80

Device Serial No.: XX-XXXXXXX-XXXXXXX

Enable DHCP

Password

Obrázek 2–5 Úprava IP adresy

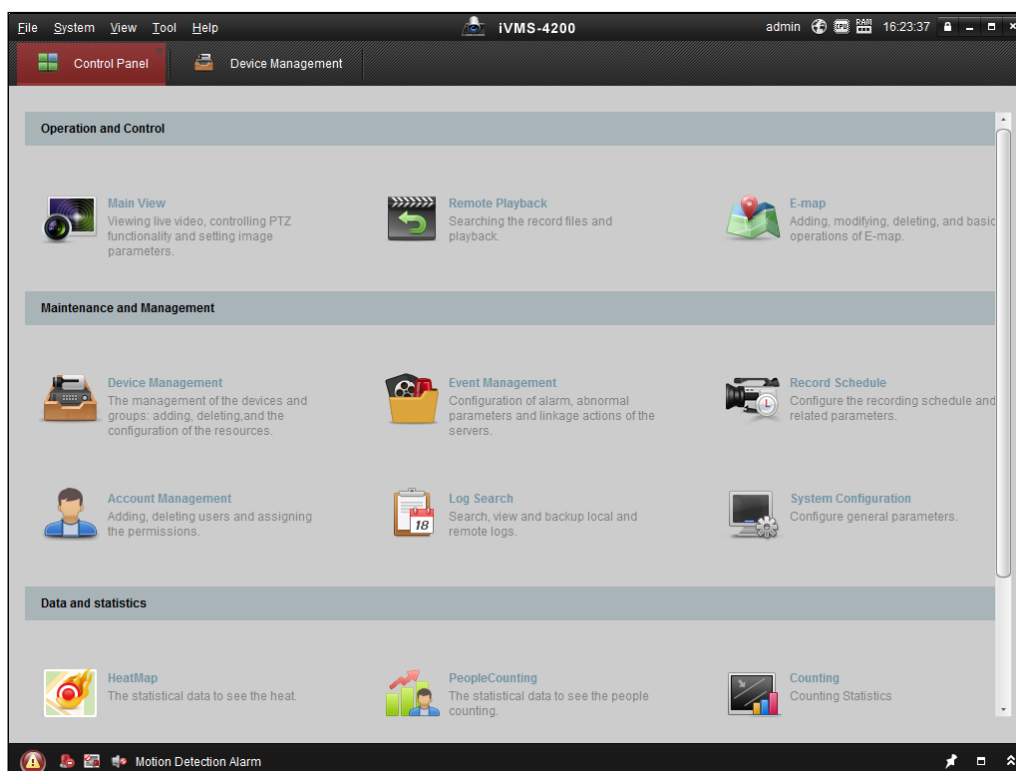
6. Zadejte heslo a klikněte na tlačítko **Save** k aktivaci upravené IP adresy.

❖ **Aktivace pomocí klientského softwaru**

Klientský software je univerzální software pro správu videa pro více druhů zařízení. Klientský software získáte z dodaného disku nebo na oficiálních internetových stránkách. Nainstalujte software podle pokynů. Postupujte podle pokynů k aktivaci kamery.

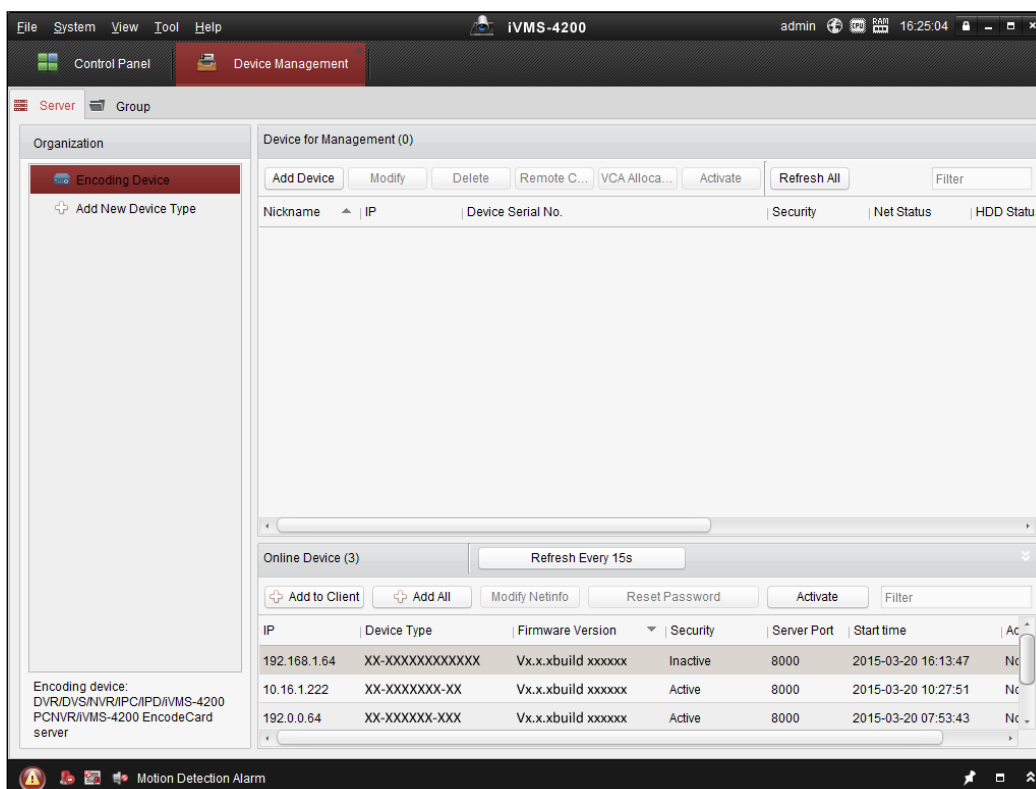
Kroky:

1. Spustěte klientský software – zobrazí se ovládací panel softwaru, viz obrázek níže.



Obrázek 2–6 Ovládací panel

2. Pro vstup do rozhraní Device Management klikněte na ikonu **Device Management**, jak je zobrazeno na následujícím obrázku.



Obrázek 2–7 Rozhraní správy zařízení

3. Zkontrolujte stav zařízení v seznamu zařízení a vyberte neaktivní zařízení.
4. Kliknutím na tlačítko **Activate** otevřete aktivační rozhraní.
5. Vytvořte heslo a zadejte je do pole hesla a heslo potvrďte.



DOPORUČUJEME SILNÉ HESLO – Pro zvýšení zabezpečení vašeho produktu důrazně doporučujeme vytvoření silného hesla, které vyberete sami (s použitím minimálně 8 znaků, včetně velkých a malých písmen, čísel a speciálních znaků). Doporučujeme, abyste heslo pravidelně měnili, zvláště v systémech s vysokým zabezpečením. Změna hesla jednou za měsíc nebo za týden lépe ochrání váš výrobek.

Activation

User Name: admin

Password: ●●●●●●

Strong

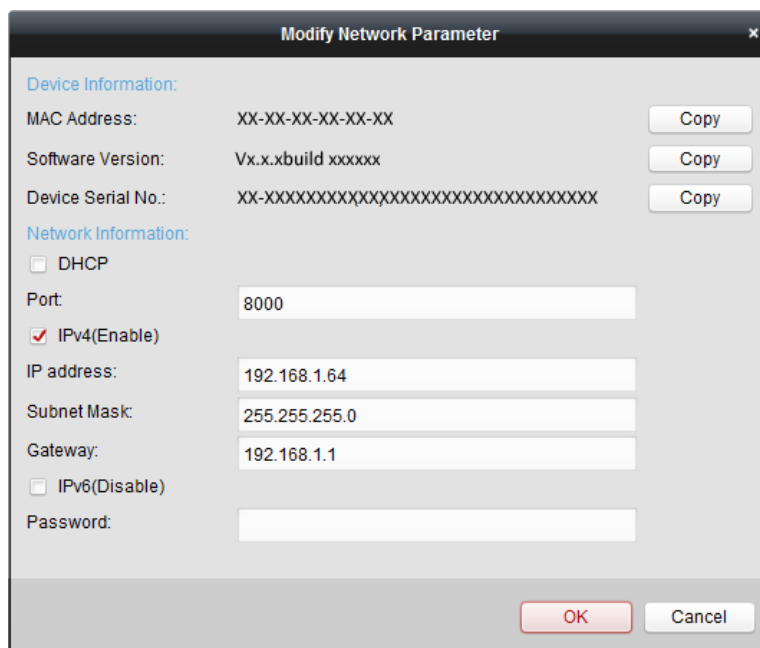
Valid password range [8-16]. You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained.

Confirm New Password: ●●●●●●

Ok Cancel

Obrázek 2–8 Okno aktivace (klientský software)

6. Kliknutím na tlačítko **OK** zahájíte aktivaci.
7. Kliknutím na tlačítko **Modify Netinfo** otevřete rozhraní síťových parametrů, viz obr. níže.



Obrázek 2–9 Úprava síťových parametrů

8. Ruční změnou IP adresy nebo zaškrtnutím políčka Enable DHCP změňte IP adresu zařízení na stejnou podsíť s počítačem.
9. Zadejte heslo pro aktivaci změny IP adresy.

2.2 Nastavení síťové kamery pomocí sítě WAN

Účel:

V této části je vysvětleno, jak síťovou kameru připojit do sítě WAN pomocí statické nebo dynamické IP adresy.

2.2.1 Připojení se statickou IP adresou

Než začnete:

Použijte statickou IP adresu od poskytovatele připojení k internetu. Pomocí statické IP adresy lze síťovou kameru připojit prostřednictvím směrovače nebo ji připojit do sítě WAN přímo.

- **Připojení síťové kamery prostřednictvím směrovače**

Kroky:

1. Připojte síťovou kameru ke směrovači.
2. Přiřaďte LAN IP adresu, masku podsítě a bránu. Podrobnosti o konfiguraci adresy IP síťové kamery naleznete v části 2.1.2.
3. Uložte statickou IP adresu do směrovače.
4. Nastavte mapování portů, například portů 80, 8000 a 554. Postup mapování portů se liší v závislosti na různých směrovačích. Při mapování portů se obraťte na výrobce směrovače, který vám poskytne další informace.

Poznámka: Viz dodatek 2, kde najdete podrobné informace k mapování portů.

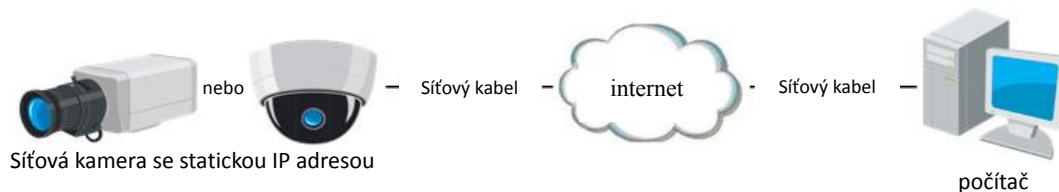
5. Přistupte k síťové kameře přes internet prostřednictvím webového prohlížeče nebo klientského softwaru.



Obrázek 2–10 Přístup ke kameře prostřednictvím směrovače se statickou IP adresou

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

Statickou IP adresu lze také uložit v kameře a připojit ji k internetu přímo bez použití směrovače. Podrobnosti o konfiguraci adresy IP síťové kamery naleznete v Části 2.1.2.



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

2.2.2 Připojení s dynamickou IP adresou

Než začnete:

Použijte dynamickou IP adresu od poskytovatele připojení k internetu. Pomocí dynamické IP adresy lze síťovou kameru připojit k modemu nebo směrovači.

● Připojení síťové kamery prostřednictvím směrovače

Kroky:

1. Připojte síťovou kameru ke směrovači.
2. Přiřaďte v kameře IP adresu LAN, masku podsítě a bránu. Podrobnosti o konfiguraci adresy IP síťové kamery naleznete v části 2.1.2.
3. Ve směrovači nastavte uživatelské jméno PPPoE, heslo a potvrzení hesla.
4. Nastavte mapování portů. Například portů 80, 8000 a 554. Tyto kroky se při mapování portů liší v závislosti na různých směrovačích. Při mapování portů se obraťte na výrobce směrovače, který vám poskytne další informace.

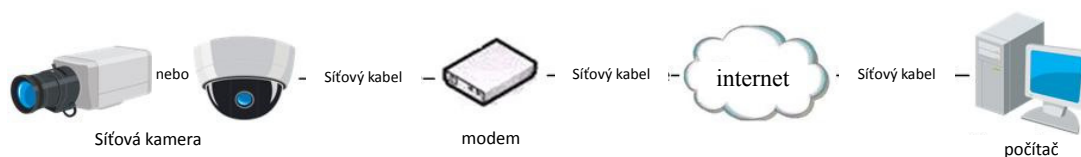
Poznámka: Viz dodatek 2, kde najdete podrobné informace k mapování portů.

5. Použijte název domény od poskytovatele názvu domény.
6. Konfigurujte nastavení DDNS v nastavení rozhraní směrovače.
7. Přistupte ke kameře prostřednictvím použitého názvu domény.

● Připojení síťové kamery prostřednictvím modemu

Účel:

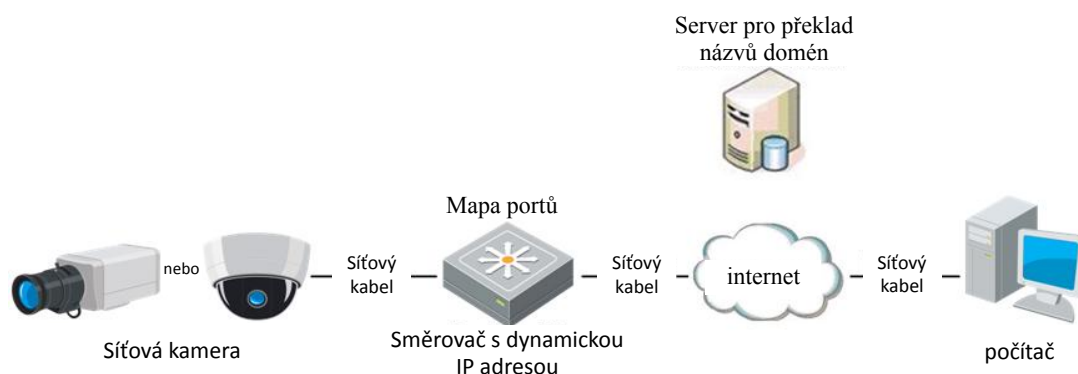
Tato kamera podporuje funkci automatického vytáčení PPPoE. Jakmile se kamera připojí k modemu, získá veřejnou IP adresu díky vytáčení ADSL. Je třeba nakonfigurovat parametry funkce PPPoE síťové kamery. Pro podrobnou konfiguraci se řiďte pokyny v *Části 5.3.3 Konfigurace nastavení PPPoE*.



Obrázek 2–12 Přístup ke kameře s dynamickou IP adresou

Poznámka: Získaná IP adresa se přiřazuje dynamicky pomocí funkce PPPoE, po restartování kamery proto vždy dojde ke změně IP adresy. Chcete-li vyřešit nepříjemnosti dynamické IP adresy, je nutné získat doménový název od poskytovatele DDNS (např. DynDns.com). Problém s překladem názvu normální domény a s překladem názvu privátní domény vyřešíte postupováním podle níže uvedených kroků.

◆ Překlad normálního doménového názvu

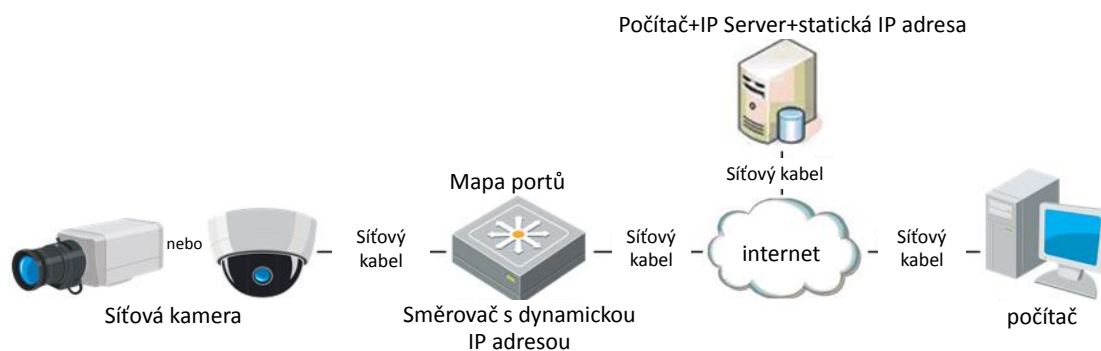


Obrázek 2–13 Překlad normálních doménových názvů

Kroky:

1. Použijte název domény od poskytovatele názvu domény.
2. Nastavení DDNS nakonfigurujte v rozhraní **Nastavení DDNS** síťové kamery.
Pro podrobnou konfiguraci se řiďte pokyny v
Části 5.4.3 Konfigurace nastavení DDNS.
3. Přistupte ke kameře prostřednictvím použitého názvu domény.

◆ Rozlišení privátního názvu domény



Obrázek 2–14 Překlad názvu privátní domény

Kroky:

1. V počítači se statickou IP adresou nainstalujte a spusťte software IP Server.
2. Přistupte k síťové kameře přes síť LAN prostřednictvím webového prohlížeče nebo klientského softwaru.
3. Povolte službu DDNS a jako typ protokolu zvolte možnost IP Server. Pro podrobnou konfiguraci se řiďte pokyny v
Části 5.4.3 Konfigurace nastavení DDNS.


Kapitola 3 Přístup k síťové kameře

3.1 Přístup přes webové prohlížeče

Kroky:

1. Otevřete webový prohlížeč.
2. Do adresního řádku prohlížeče zadejte IP adresu síťové kamery. Stisknutím tlačítka **Enter** přejděte k oknu pro přihlášení.
3. Při první aktivaci síťové kamery postupujte podle pokynů uvedených v Části 2.1.2.

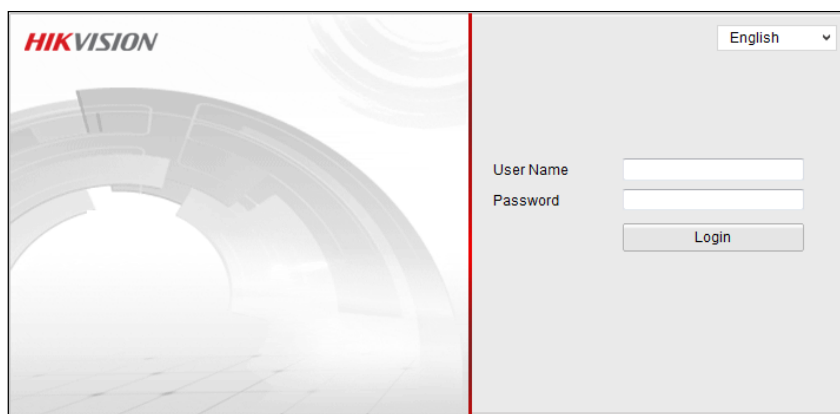
Poznámka:

- Výchozí adresa IP je 192.168.1.64.
 - Není-li kamera aktivována, nejprve ji aktivujte podle postupu v Kapitole 3.1 nebo 3.2.
4. V pravém horním rohu přihlašovacího rozhraní zvolte angličtinu jako jazyk rozhraní.
 5. Zadejte uživatelské jméno a heslo a klikněte na .

Uživatel s oprávněním správce by měl řádně konfigurovat účty zařízení a oprávnění uživatelů/operátorů. Odstraňte nepotřebné účty a oprávnění uživatelů/operátorů.

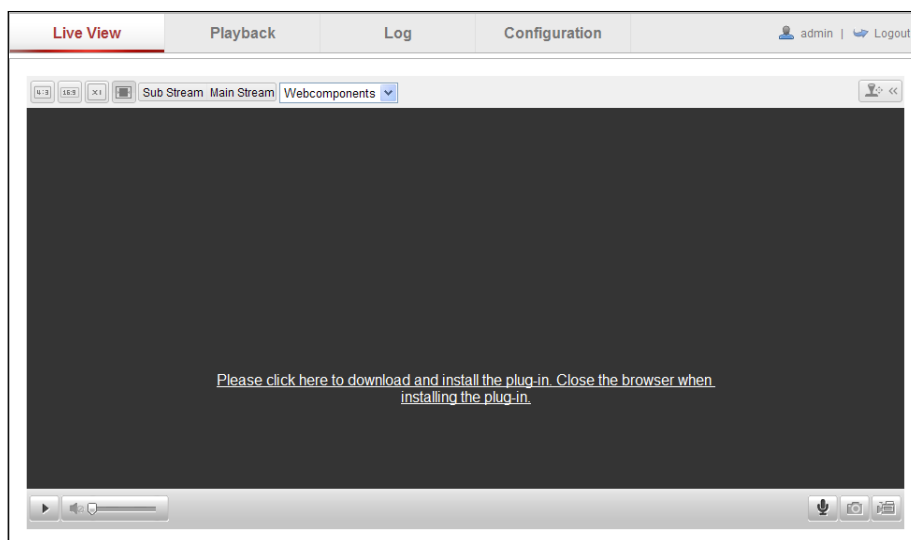
Poznámka:

IP adresa zařízení bude zablokována v případě, že uživatel s oprávněním správce provede 7 neúspěšných pokusů k zadání hesla (5 pokusů pro uživatele/operátora).

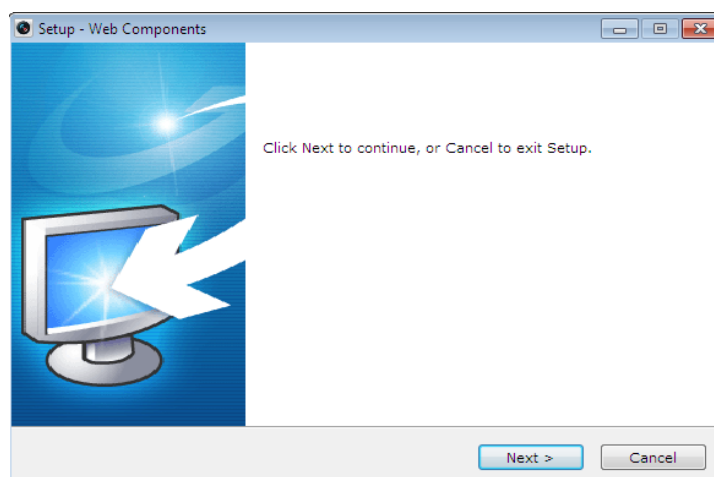


Obrázek 3–1 Okno pro přihlášení

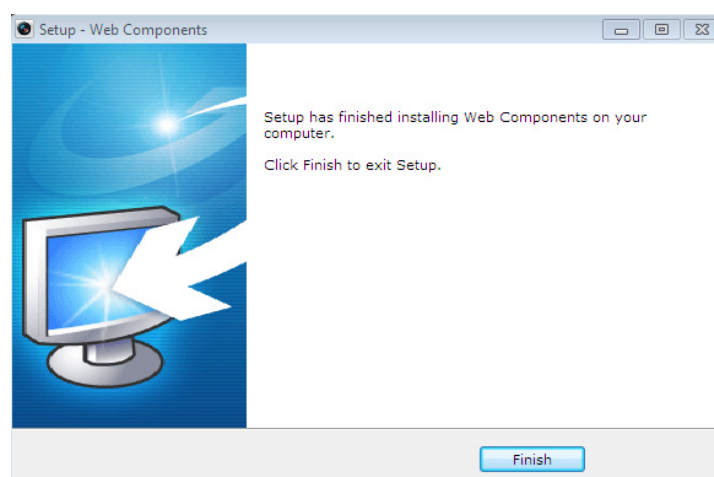
6. Než budete moci zobrazit živé video a obsluhovat kameru, nainstalujte modul plug-in. Postupujte podle pokynů k instalaci modulu plug-in.



Obrázek 3–2 Stažení a instalace modulu plug-in



Obrázek 3–3 Instalace modulu plug-in (1)



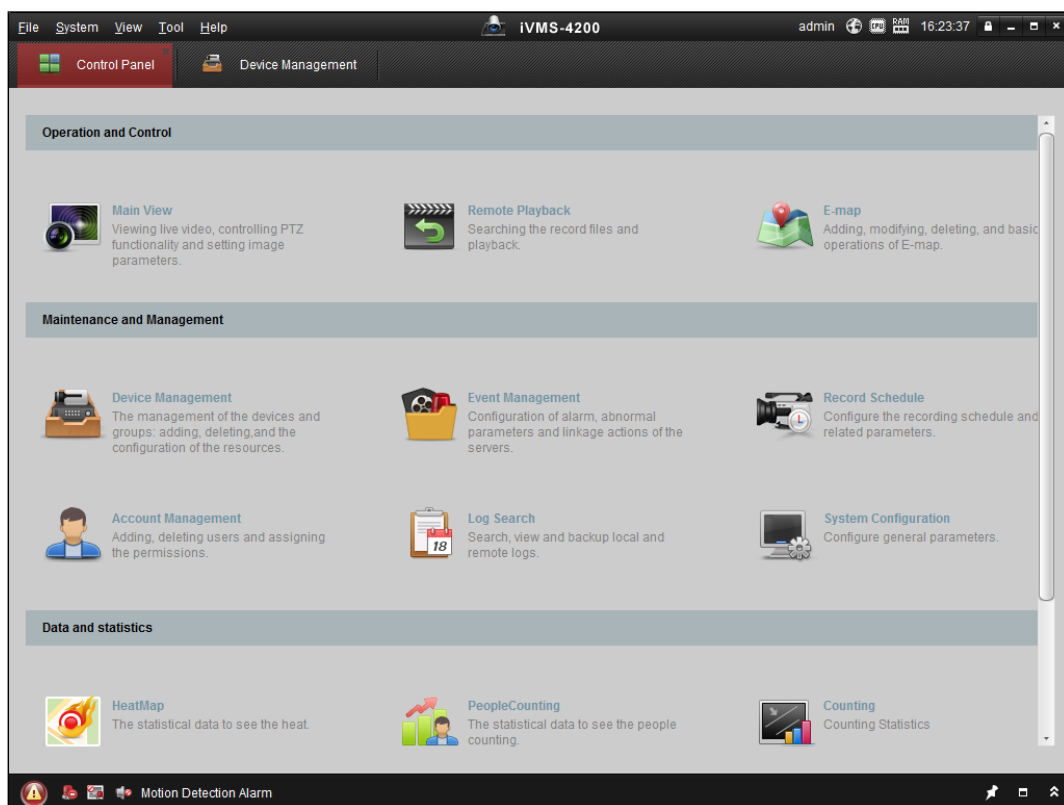
Obrázek 3–4 Instalace modulu plug-in (2)

Poznámka: Před nainstalováním modulu plug-in bude případně nutné zavřít webový prohlížeč. Po instalaci modulu plug-in znovu otevřete webový prohlížeč a přihlaste se znovu.

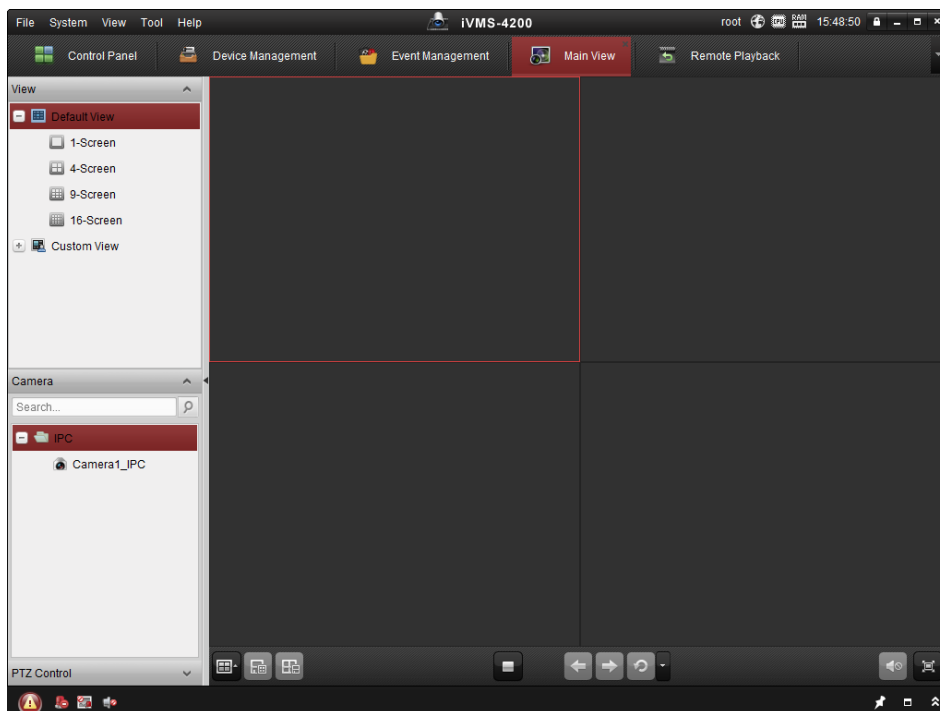
3.2 Přístup pomocí klientského softwaru

Klientský software iVMS-4200 je obsažen na disku CD výrobku. Pomocí softwaru lze zobrazovat živé video a spravovat kameru.

Software nainstalujete postupováním podle výzev k instalaci. Níže je zobrazen ovládací panel a okno živého zobrazení klientského softwaru iVMS-4200.



Obrázek 3–5 Ovládací panel iVMS-4200



Obrázek 3–6 Hlavní okno softwaru iVMS-4200

Poznámka: Podrobné informace o softwaru naleznete v uživatelské příručce zařízení iVMS-4200.

Kapitola 4 Živé zobrazení

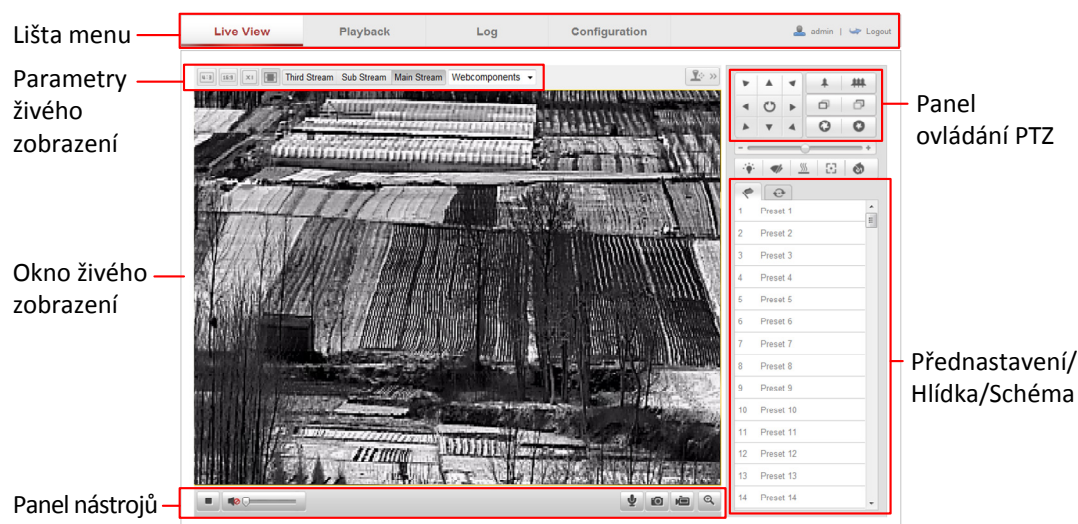
4.1 Stránka živého zobrazení

Účel:

Stránka živého zobrazení umožňuje zobrazovat video ve skutečném čase, zachycovat snímky, uskutečňovat ovládání PTZ, nastavovat a vyvolávat předvolby a konfigurovat parametry videa.

Přihlášením k síťové kameře přejděte na stránku živého zobrazení. Na stránku živého zobrazení lze také přejít kliknutím na možnost **Live View** v řádku nabídek hlavní stránky.

Popis stránky živého zobrazení:




Obrázek 4–1 Stránka živého zobrazení

Model kamery:

Zobrazuje model kamery, k níž se připojujete.

Nápověda online:

Pro získání nápovědy online, která vás provede základními operacemi každé funkce, klikněte na  .

Panel nabídek:

Po kliknutí na jednotlivé karty vstoupíte na příslušné stránky Živé zobrazení, Přehrávání, Protokol a Konfigurace.

Ovládání displeje:

Klikněte na jednotlivá tlačítka a upravte rozvržení a typ streamu živého zobrazení. Rozvržení zobrazení vyberte kliknutím na rozbalovací nabídku. Uživatelé IE (Internet Explorer) mohou volit webové komponenty a Quick Time. Pro uživatele, kteří IE nepoužívají, mohou být webové komponenty, Quick Time, VLC nebo MJPEG volitelné, pokud tyto funkce podporuje webový prohlížeč.

Okno živého zobrazení:

Zobrazení živého videa.

Panel nástrojů:

Operace na stránce živého zobrazení, např. spuštění/zastavení živého zobrazení, snímání, záznam, spuštění/zastavení obousměrného zvuku atd.


Ovládání PTZ:

Otáčení, naklánění a přiblížení kamery a ovládání světla a stěrače. (Dostupné jen pro kamery s podporou funkce PTZ)

Nastavení předvoleb/hlídky:

Slouží k nastavení, vyvolání nebo odstranění předvoleb nebo hlídek u kamer PTZ.






4.2 Spuštění živého zobrazení

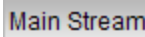
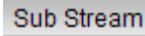







V okně živého zobrazení, viz Obrázek 4–2, spust'íte živé zobrazení kamery kliknutím na tlačítko  v panelu nástrojů.





Obrázek 4–2 Panel nástrojů živého zobrazení

Tabulka 4–1 Popisy ovládacího panelu displeje a panelu nástrojů

Ikona	Popis
	Spuštění a zastavení živého zobrazení.
	Nastavení velikosti okna na formát 4:3
	Nastavení velikosti okna na formát 16:9
	Nastavení původní velikosti okna
	Nastavení automaticky se přizpůsobující velikosti okna

Ikona	Popis
	Živé zobrazení s hlavním streamem
	Živé zobrazení s dílčím streamem
	Volba modulu plug-in jiného výrobce
	Rozdělení okna
	Ruční snímání obrazu
	Ruční spuštění a zastavení nahrávání
	Zapnout zvuk a nastavit/ztlumit hlasitost.
	Spustit/zastavit obousměrný zvuk.
	Povolit/zakázat funkci e-PTZ.

4.3 Ruční nahrávání a zachycování snímků

Snímek živého zobrazení zachytíte v okně živého zobrazení kliknutím na tlačítko  v panelu nástrojů. Kliknutím na tlačítko  živé zobrazení nahrajete. Cesty k ukládání zachycených snímků a klipů je možno nastavit na stránce **Configuration > Local Configuration**. Pro konfiguraci vzdáleného naplánovaného nahrávání postupujte podle pokynů uvedených v *Části 6.3*.

Poznámka: Zachycený snímek se v počítači uloží ve formátu souboru JPEG nebo BMP.

Kapitola 5 Konfigurace síťové kamery

5.1 Konfigurace místních parametrů

Poznámka: Místní konfigurace odkazuje na parametry živého zobrazení, souborů nahrávek a zachycených snímků a klipů. Zaznamenané soubory, zachycené obrázky a klipy jsou ty, které zaznamenáváte a zachytíte prostřednictvím webového prohlížeče, a cesty pro jejich ukládání se tedy nachází v počítači, v němž je prohlížeč spuštěn.

Kroky:

1. Pro vstup do rozhraní Local Configuration:

Configuration > Local Configuration

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

- Live View Parameters:** Includes radio buttons for Protocol (TCP selected, UDP, MULTICAST, HTTP), Live View Performance (Shortest Delay, Auto selected), Rules (Enable, Disable selected), Image Format (JPEG selected, BMP), Display Temperature Info. (Enable, Disable selected), and Display Temperature Info. on Capture (Enable, Disable selected).
- Record File Settings:** Includes radio buttons for Record File Size (256M, 512M selected, 1G), a text input for 'Save record files to' (C:\Users\yanjiamin\Web\RecordFiles) with a 'Browse' button, and a text input for 'Save downloaded files to' (C:\Users\yanjiamin\Web\DownloadFiles) with a 'Browse' button.
- Picture and Clip Settings:** Includes text inputs for 'Save snapshots in live view to' (C:\Users\yanjiamin\Web\CaptureFiles), 'Save snapshots when playback to' (C:\Users\yanjiamin\Web\PlaybackPics), and 'Save clips to' (C:\Users\yanjiamin\Web\PlaybackFiles), each with a 'Browse' button.

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

Obrázek 5–1 Rozhraní místní komunikace

2. Nakonfigurujte následující nastavení:

- **Live View Parameters:** Nastavte typ protokolu a výkon živého zobrazení.
 - **Typ protokolu:** Lze zvolit položky TCP, UDP, MULTICAST a HTTP.

TCP: Zajišťuje kompletní přenos streamovaných dat a lepší kvalitu obrazu, avšak bude ovlivněn přenos v reálném čase.

UDP: Poskytuje zvukový a obrazový stream v reálném čase.

HTTP: Umožňuje stejnou kvalitu jako TCP bez stanovení specifických portů pro streamování v některých síťových prostředích.

MULTICAST: Používáte-li funkci vícesměrového vysílání, doporučujeme vybrat typ MCAST. Podrobné informace o vícesměrovém vysílání naleznete v *Části 5.3.1 Konfigurace nastavení protokolu TCP/IP.*
 - **Live View Performance:** Položku live view performance nastavte na Shortest Delay nebo Auto.
 - **Auto Start Live View:** Pokud tuto funkci povolíte, živé zobrazení se při aktivaci funkce **Živé zobrazení** spustí automaticky. Je-li tato funkce vypnuta, můžete živé zobrazení spustit v rozhraní živého zobrazení také ručně.
 - **Rules:** Tato možnost se vztahuje k pravidlům místního prohlížeče. Povoláním nebo zakázáním této možnosti zobrazíte nebo zrušíte zobrazení barevných značek při spuštění detekce pohybu, detekce obličeje nebo detekce narušení. Pokud jsou například pravidla povolena a je povolena také detekce obličeje, označí se v živém zobrazení rozpoznáný obličej zeleným obdélníkem.
 - **Image Format:** Vyberte formát snímku pro zachycený obraz.
 - **Fire Point:** Detekci zdroje požáru vyberte jako Typ prostředku VCA. Pokud chcete požadované funkce povolit, zaškrtněte políčko. Volit můžete z možností Display Fire Point Distance, Display Highest Temperature, Locate Highest Temperature Point a Frame Fire Point.
 - **Display Temperature Info. on Stream:** Jako VCA Resource Type vyberte Temperature Measurement. Toto políčko zaškrtněte pro zobrazení informací o teplotě v rozhraní živého zobrazení.

- **Display Temperature Info. on Capture:** Jako VCA Resource Type vyberte Temperature Measurement. Toto políčko zaškrtněte pro zobrazení informací o teplotě na snímcích.
- **Record File Settings:** Nastavte cestu uložení pro nahrané videosoubory. Možnost platí pro soubory záznamů nahrané pomocí webového prohlížeče.
 - **Record File Size:** Vyberte zkomprimovanou velikost ručně nahraných a stažených videosouborů 256 MB, 512 MB nebo 1 GB. Vybrané možnosti bude odpovídat maximální velikost souboru záznamu.
 - **Save record files to:** Nastavení cesty pro uložení ručně nahraných video souborů.
 - **Save downloaded files to:** Nastavte cestu uložení pro videosoubory stažené v režimu přehrávání.
- **Picture and Clip Settings:** Nastavení cest pro uložení zaznamenaných snímků a oříznutých video souborů. Platí pro snímky zachycené prostřednictvím webového prohlížeče.
 - **Save snapshots in live view to:** Nastavte cestu uložení pro ručně zachycené snímky v režimu živého zobrazení.
 - **Save snapshots when playback to:** Nastavte cestu uložení pro snímky zachycené v režimu přehrávání.
 - **Save clips to:** Nastavte cestu uložení pro videosoubory ořezané v režimu přehrávání.

Poznámka: Pokud chcete změnit adresář pro ukládání klipů a snímků, klikněte na tlačítko **Browse**.

3. Kliknutím na tlačítko **Save** uložte nastavení.

5.2 Konfigurace nastavení času

Účel:

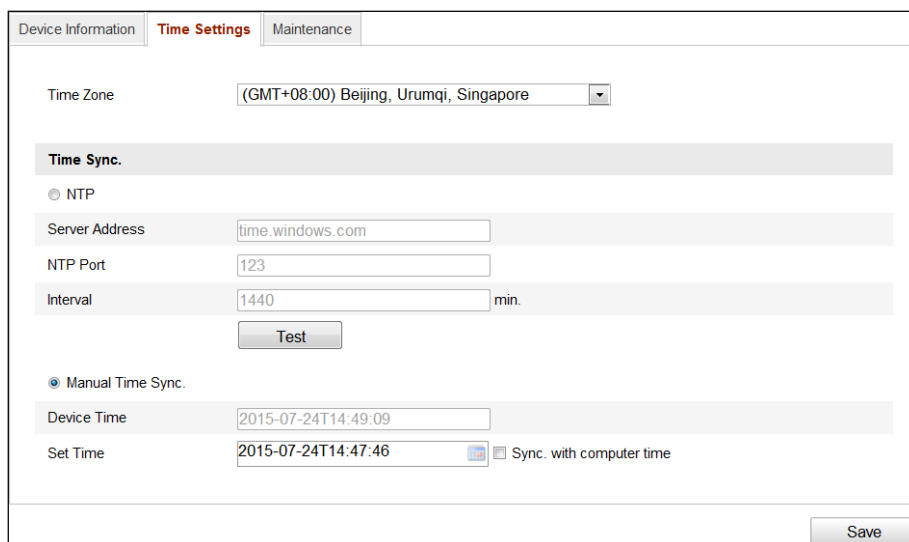
Pomocí pokynů uvedených v této části lze nakonfigurovat synchronizaci času a nastavení letního času.

Kroky:

1. Vstupte do rozhraní Time Settings:

Configuration > Basic Configuration > System > Time Settings

Nebo **Configuration > Advanced Configuration > System > Time Settings**



Obrázek 5–2 Nastavení času

2. Vyberte časové pásmo.

V rozevřacím seznamu vyberte časové pásmo svého umístění.

3. Nastavte synchronizaci času.

Čas můžete synchronizovat prostřednictvím NTP nebo to můžete provést ručně.

- Synchronizace času prostřednictvím serveru NTP.

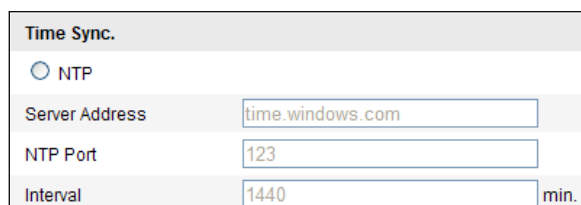
(1) Funkci NTP povolíte zaškrtnutím políčka.

(2) Nakonfigurujte následující nastavení:

Server Address: Jedná se o IP adresu serveru NTP.

NTP Port: Jedná se o port serveru NTP.


Interval: Jedná se o časový interval mezi dvěma akcemi synchronizace se serverem NTP.



Obrázek 5–3 Synchronizace času podle serveru NTP

Poznámka: Pokud je kamera připojena k veřejné síti, měli byste používat server NTP s funkcí synchronizace času, jako je například server organizace National Time Center (IP adresa: 210.72.145.44). Pokud se kamera nastavuje v přizpůsobené síti, lze k navázání serveru NTP využitého k synchronizaci času použít software NTP.

- Ruční synchronizace času

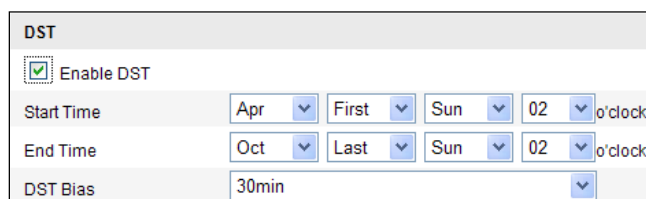
Povolte funkci **Manual Time Sync** a potom pro nastavení systémového času v rozevřacím kalendáři klikněte na tlačítko .

Poznámka: Pro synchronizaci času kamery s časem v počítači můžete také zaškrtnout políčko **Sync with computer time**.



Obrázek 5–4 Ruční synchronizace času

4. Pro povolení funkce DST a nastavení data období DST klikněte na záložku stránky **DST (Configuration > Advanced Configuration > System > DST)**.



Obrázek 5–5 Nastavení DST

5. Kliknutím na tlačítko **Save** uložte nastavení.

5.3 Konfigurace nastavení sítě

5.3.1 Konfigurace nastavení protokolu TCP/IP

Účel:

Nastavení TCP/IP je nutné řádně nakonfigurovat, než kameru připojíte k síti. Kamera podporuje protokol IPv4 i IPv6. Obě verze mohou být konfigurovány současně bez vzájemného konfliktu, měla by být nakonfigurována nejméně jedna verze IP.

Kroky:

1. Otevřete rozhraní pro nastavení protokolu TCP/IP:

Configuration > Basic Configuration > Network > TCP/IP

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

The screenshot displays the 'NIC Settings' configuration page. It includes the following fields and options:

- NIC Type:** Auto (dropdown menu)
- DHCP:** Unchecked checkbox
- IPv4 Address:** 10.11.36.159 (text input) with a 'Test' button
- IPv4 Subnet Mask:** 255.255.255.0 (text input)
- IPv4 Default Gateway:** 10.11.36.254 (text input)
- IPv6 Mode:** Route Advertisement (dropdown menu) with a 'View Route Advertisement' button
- IPv6 Address:** :: (text input)
- IPv6 Subnet Mask:** 0 (text input)
- IPv6 Default Gateway:** (text input)
- Mac Address:** 44:19:b6:5e:16:f2 (text input)
- MTU:** 1500 (text input)
- Multicast Address:** (text input)
- Enable Multicast Discovery:** Checked checkbox
- DNS Server:**
 - Preferred DNS Server: 8.8.8.8 (text input)
 - Alternate DNS Server: (text input)

Obrázek 5–6 Nastavení protokolu TCP/IP

2. Nakonfigurujte základní nastavení sítě, jako jsou typ NIC, adresa IPv4 nebo IPv6, maska podsítě IPv4 nebo IPv6, výchozí brána IPv4 nebo IPv6, nastavení MTU a adresa vícesměrového vysílání.
3. (Volitelné) Zaškrtněte políčko **Enable Multicast Discovery**, následně je možno online síťovou kameru automaticky detekovat klientským softwarem prostřednictvím soukromého protokolu vícesměrového vysílání v síti LAN.
4. Kliknutím na tlačítko **Save** výše uvedená nastavení uložte.

Poznámky:

- Platný rozsah hodnot MTU je 1280–1500.
- Multicast odesílá stream na multicastovou skupinovou adresu, takže více klientů může získat stream současně vyžádáním kopie z multicastové skupinové adresy. Než tuto funkci využijete, je nutné funkci vícesměrového vysílání povolit na směrovači.
- Nastavení se projeví až po restartování.

5.3.2 Konfigurace nastavení portu

Účel:

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

Kroky:

1. Otevřete rozhraní pro nastavení portu:

Configuration > Basic Configuration > Network > Port

Nebo **Configuration > Advanced Configuration > Network > 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"/>

Obrázek 5–7 Nastavení portu

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

HTTP Port: Výchozí číslo portu je 80 a lze jej změnit na jakékoli číslo portu, které není použito.

RTSP Port: Výchozí číslo portu je 554 a lze jej změnit na jakékoli číslo portu v rozsahu od 1024 do 65535.

HTTPS Port: Výchozí číslo portu je 443 a lze jej změnit na jakékoli číslo portu, které není použito.

Server Port: Výchozí číslo portu serveru je 8000 a lze jej změnit na jakékoli číslo portu v rozsahu od 2000 do 65535.

3. Kliknutím na tlačítko **Save** uložte nastavení.

Poznámka: Nastavení se projeví až po restartování.

5.3.3 Konfigurace nastavení PPPoE

Účel:

Pokud nemáte směrovač, ale jen modem, můžete použít funkci „Point-to-Point Protocol over Ethernet“ (PPPoE).

Kroky:

1. Otevřete rozhraní pro nastavení PPPoE:

Configuration > Advanced Configuration > Network > PPPoE

Obrázek 5–8 Nastavení PPPoE

2. Pro povolení této funkce zaškrtněte políčko **Enable PPPoE**.
3. Pro přístup PPPoE zadejte **User Name**, **Password** a **Confirm Password**.

Poznámka: Uživatelské jméno a heslo by vám měl přiřadit váš poskytovatel služeb internetu.



- *Kvůli vašim osobním údajům a lepší ochraně před bezpečnostními riziky důrazně doporučujeme použít silná hesla pro všechny funkce a síťová zařízení. Pro zvýšení zabezpečení vašeho produktu by heslo mělo být takové, které jste vybrali sami (s použitím minimálně 8 znaků, včetně velkých a malých písmen, čísel a zvláštních znaků).*
 - *Zodpovědnost za správnou konfiguraci všech hesel a ostatních bezpečnostních opatření nese montážní pracovník nebo konečný uživatel.*
4. Kliknutím na tlačítko **Save** uložte nastavení a zavřete okno.

Poznámka: Nastavení se projeví až po restartování.

5.3.4 Konfigurace nastavení DDNS

Účel:

Pokud je v kameře jako výchozí síťové připojení nastavena funkce PPPoE, lze k síťovému přístupu použít službu Dynamic DNS (DDNS).

Než začnete:

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



- *Kvůli vašim osobním údajům a lepší ochraně před bezpečnostními riziky důrazně doporučujeme použít silná hesla pro všechny funkce a síťová zařízení. Pro zvýšení zabezpečení vašeho produktu by heslo mělo být takové, které jste vybrali sami (s použitím minimálně 8 znaků, včetně velkých a malých písmen, čísel a zvláštních znaků).*
- *Zodpovědnost za správnou konfiguraci všech hesel a ostatních bezpečnostních opatření nese montážní pracovník nebo konečný uživatel.*

Kroky:

1. Otevřete rozhraní pro nastavení DDNS:

Configuration > Advanced Configuration > Network > DDNS

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

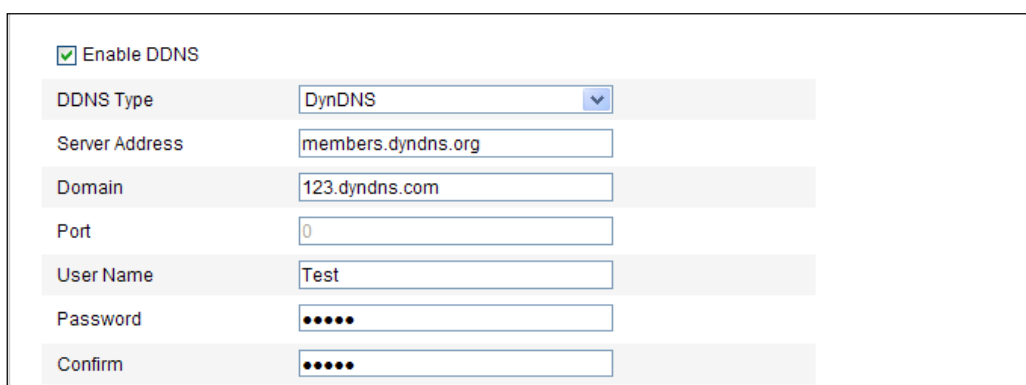
Obrázek 5–9 Nastavení DDNS

2. Zaškrtnutím políčka **Enable DDNS** tuto funkci povolíte.
3. U možnosti **DDNS Type** vyberte typ. Je možno volit ze čtyř typů DDNS: HiDDNS, IPServer, NO-IP a DynDNS.

- DynDNS:

Kroky:

- (1) Zadejte **Server Address** DynDNS (např. members.dyndns.org).
- (2) V textovém poli **Domain** zadejte název domény získaný z webových stránek DynDNS.
- (3) Zadejte **Port** serveru DynDNS.
- (4) Zadejte **User Name** a **Password** zaregistrované na webu DynDNS.
- (5) Kliknutím na tlačítko **Save** uložte nastavení.



<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	•••••

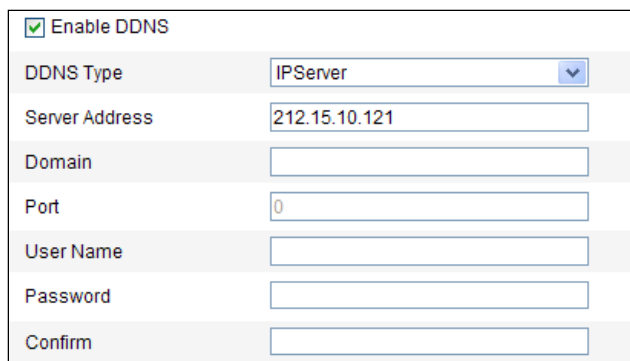
Obrázek 5–10 Nastavení DynDNS

- Server IP:

Kroky:

- (1) Zadejte adresu serveru IP serveru.
- (2) Kliknutím na tlačítko **Save** uložte nastavení.

Poznámka: V případě IP serveru budete muset použít IP statické adresy, masku podsítě, bránu a upřednostňovaný server DNS ISP. **Server Address** je třeba zadat se statickou adresou IP počítače, v němž běží software serveru IP.



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

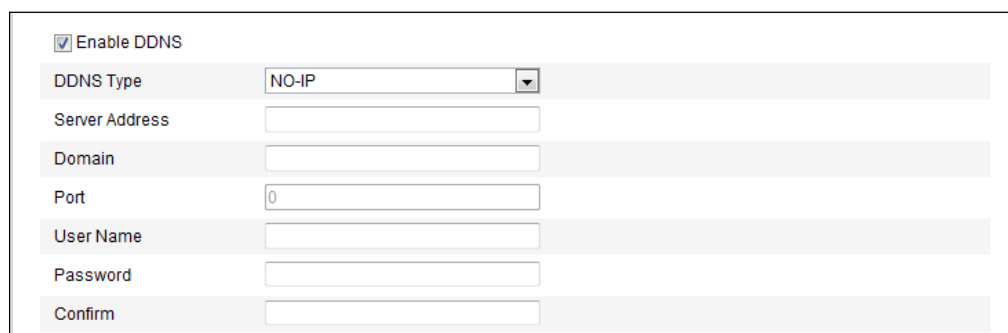
Obrázek 5–11 Nastavení serveru IP

Poznámka: Pro oblast USA a Kanady můžete jako adresu serveru zadat 173.200.91.74.

- NO-IP:

Kroky:

- (1) U možnosti DDNS Type vyberte nastavení NO-IP.



The screenshot shows a configuration form for DDNS. At the top, there is a checkbox labeled 'Enable DDNS' which is checked. Below it, the 'DDNS Type' dropdown menu is set to 'NO-IP'. The other fields are empty: 'Server Address', 'Domain', 'Port' (set to 0), 'User Name', 'Password', and 'Confirm'.

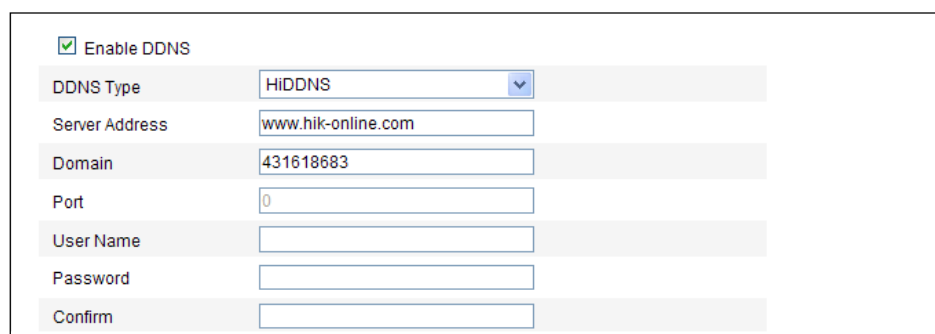
Obrázek 5–12 Nastavení serveru NO-IP

- (2) Zadejte adresu serveru jako 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**, následně si můžete prohlédnout kameru s názvem domény.

- HiDDNS

Kroky:

- (1) Typ DDNS Type vyberte jako HiDDNS.



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

Obrázek 5–13 Nastavení HiDDNS

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

(3) Zadejte název domény kamery. Doména je stejná jako alias zařízení na serveru HiDDNS.

(4) Nová nastavení uložíte kliknutím na tlačítko **Save**.

Poznámka: Nastavení se projeví až po restartování.

5.3.5 Konfigurace nastavení SNMP

Účel:

Pro získání stavu kamery můžete nastavit funkci SNMP, s alarmem související parametry a informace a vzdáleně spravovat kameru, je-li připojena k síti.

Než začnete:

Než protokol SNMP nastavíte, stáhněte si software SNMP a nastavte příjem informací kamery prostřednictvím portu SNMP. Nastavíte-li adresu pro depeše, má kamera povoleno odesílat zprávy o událostech alarmu a výjimkách do monitorovacího centra.

Poznámka: Vámi zvolená verze SNMP by měla být stejná jako v softwaru SNMP. Je třeba také použít různé verze v závislosti na požadované úrovni zabezpečení. SNMP v1 neposkytuje žádné zabezpečení. SNMP v2 vyžaduje přístupové heslo. SNMP v3 nabízí šifrování. Pokud používáte třetí verzi, musí být povolen protokol HTTPS.



- *Kvůli vašim osobním údajům a lepší ochraně před bezpečnostními riziky důrazně doporučujeme použít silná hesla pro všechny funkce a síťová zařízení. Pro zvýšení zabezpečení vašeho produktu by heslo mělo být takové, které jste vybrali sami (s použitím minimálně 8 znaků, včetně velkých a malých písmen, čísel a zvláštních znaků).*
- *Zodpovědnost za správnou konfiguraci všech hesel a ostatních bezpečnostních opatření nese montážní pracovník nebo konečný uživatel.*

Kroky:

1. Otevřete rozhraní pro nastavení SNMP:

Configuration > Advanced Configuration > Network > 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"/>

Obrázek 5–14 Nastavení SNMP

- Pro povolení této funkce zaškrtněte políčko odpovídající verze (**Enable SNMPv1**, **Enable SNMPv2c**, a **Enable SNMPv3**).

- Konfigurujte nastavení SNMP.

Poznámka: Nastavení softwaru SNMP by mělo být shodné s nastaveními, která konfiguruje zde.

- Kliknutím na tlačítko **Save** nastavení uložte a dokončete.

Poznámka: Nastavení se projeví až po restartování.

5.3.6 Konfigurace nastavení 802.1X

Účel:

Síťovými kamerami je podporován standard IEEE 802.1. Je-li tato funkce povolena, data z kamery jsou zabezpečena a při připojení kamery k síti chráněné prostřednictvím standardu IEEE 802.1 X je vyžadováno ověření uživatele.

Než začnete:

Server ověřování musí být náležitě nakonfigurován. Použijte a zaregistrujte pro protokol 802.1X na serveru uživatelské jméno a heslo.



- *Kvůli vašim osobním údajům a lepší ochraně před bezpečnostními riziky důrazně doporučujeme použít silná hesla pro všechny funkce a síťová zařízení. Pro zvýšení zabezpečení vašeho produktu by heslo mělo být takové, které jste vybrali sami (s použitím minimálně 8 znaků, včetně velkých a malých písmen, čísel a zvláštních znaků).*
- *Zodpovědnost za správnou konfiguraci všech hesel a ostatních bezpečnostních opatření nese montážní pracovník nebo konečný uživatel.*

Kroky:

1. Otevřete rozhraní pro nastavení 802.1X:
Configuration > Advanced Configuration > Network > 802.1X
2. Zaškrtnutím zaškrtačovacího políčka **Enable IEEE 802.1X** tuto funkci povolte.
3. Nakonfigurujte nastavení 802.1X, včetně nastavení verze EAPOL, uživatelského jména a hesla.
Poznámka: Nastavení možnosti EAPOL version musí být shodné s nastavením směrovače nebo přepínače.
4. Zadejte uživatelské jméno a heslo k přístupu k síti.

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

Obrázek 5–15 Nastavení 802.1X

5. Kliknutím na tlačítko **Save** dokončete nastavení.

Poznámka: Nastavení se projeví až po restartování.

5.3.7 Konfigurace nastavení QoS

Účel:

QoS (Quality of Service) může pomoci při řešení prodlevy sítě a překážce provozu tím, že dojde k nastavení priority odesílání dat.

Kroky:

1. Otevřete rozhraní pro nastavení QoS:

Configuration > Advanced Configuration > Network > QoS

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

Obrázek 5–16 Nastavení QoS

2. Nakonfigurujte nastavení technologie QoS, včetně DSCP videa/audia, DSCP události/alarmu a správy DSCP.

Platný rozsah hodnoty DSCP je 0–63. Čím vyšší je hodnota DSCP, tím vyšší je priorita.

Poznámka: DSCP znamená „Differentiated Service Code Point“ (klíč diferencovaných služeb). Hodnota DSCP se používá v IP hlavičce k označení priority dat.

3. Kliknutím na tlačítko **Save** uložte nastavení.

Poznámka: Nastavení se projeví až po restartování.

5.3.8 Konfigurace nastavení UPnP™

Universal Plug and Play (UPnP™) je síťová architektura, která zajišťuje kompatibilitu mezi síťovými zařízeními, softwarem a dalšími hardwarovými zařízeními. Protokol UPnP umožňuje bezproblémové připojení a zjednodušenou implementaci sítí doma a v podnikových prostředích.

Je-li tato funkce povolena, není nutné konfigurovat mapování portů pro každý port a kamera je připojena k síti Wide Area Network pomocí směrovače.

Kroky:

1. Otevřete rozhraní pro nastavení UPnP™:

Configuration > Advanced Configuration > Network > UPnP™

2. Zaškrtněte políčko pro aktivaci funkce UPnP™.

Při detekci online je možno název zařízení upravit.



Obrázek 5–17 Nastavení UPnP™

5.3.9 Alarmem spuštěné odeslání e-mailu

Účel:

Lze nakonfigurovat, aby systém odesílal upozornění na e-mail všem určeným příjemcům v případě, že dojde k detekci události alarmu, např. k události detekce pohybu, ztráty videa, neoprávněné manipulace s videem atd.

Než začnete:

Před použitím funkce e-mailu nakonfigurujte nastavení serveru DNS v nabídce **Basic Configuration > Network > TCP/IP** nebo **Advanced Configuration > Network > TCP/IP**.

Kroky:

1. Zadejte nastavení TCP/IP (**Configuration > Basic Configuration > Network > TCP/IP** nebo **Configuration > Advanced Configuration > Network > TCP/IP**) pro adresu IPv4, masku podsítě IPv4, výchozí bránu IPv4 a upřednostňovaný Server DNS.

Poznámka: Pro podrobné informace se řiďte pokyny v *Části 5.3.1 Konfigurace nastavení protokolu TCP/IP.*

2. Otevřete rozhraní pro nastavení e-mailu:

Configuration > Advanced Configuration > Network > Email

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.

Obrázek 5–18 Nastavení e-mailu

3. Nakonfigurujte následující nastavení:

Sender: Název odesílatele e-mailu.

Sender's Address: E-mailová adresa odesílatele.

SMTP Server: Jedná se o IP adresu serveru SMTP nebo název hostitele (např. smtp.263xmail.com).

SMTP Port: Jedná se o port SMTP. Výchozí port TCP/IP pro protokol SMTP je 25 (bez zabezpečení). Port SSL SMTP je 465.

Enable SSL: Zaškrtněte políčko pro povolení protokolu SSL, pokud je vyžadován serverem SMTP.

Attached Image: Zaškrtněte políčko Attached Image, pokud chcete posílat e-maily s připojenými snímky alarmu.

Interval: Interval představuje dobu mezi dvěma akcemi odesílání přiložených snímků.

Authentication (volitelné): Pokud e-mailový server vyžaduje ověření, zaškrtněte toto políčko pro použití ověřování k přihlášení k tomuto serveru a zadejte přihlašovací uživatelské jméno a heslo.



- *Kvůli vašim osobním údajům a lepší ochraně před bezpečnostními riziky důrazně doporučujeme použít silná hesla pro všechny funkce a síťová zařízení. Pro zvýšení zabezpečení vašeho produktu by heslo mělo být takové, které jste vybrali sami (s použitím minimálně 8 znaků, včetně velkých a malých písmen, čísel a zvláštních znaků).*
- *Zodpovědnost za správnou konfiguraci všech hesel a ostatních bezpečnostních opatření nese montážní pracovník nebo konečný uživatel.*

Choose Receiver: Vyberte příjemce, jemuž bude e-mail odeslán. Lze nakonfigurovat až 3 příjemce.

Receiver: Jméno uživatele, jemuž má být odesláno upozornění.

Receiver's Address: E-mailová adresa uživatele, jemuž má být odesláno upozornění.

4. Kliknutím na tlačítko **Save** uložte nastavení.

5.3.10 Konfigurace nastavení NAT (Network Address Translation)

Účel:

NAT odkazuje na mapování portů při povoleném UPnP™.

Kroky:

1. Přejděte do okna nastavení protokolu NAT:

Configuration > Advanced Configuration > Network > NAT

2. Vyberte režim mapování portů.

Pro mapování portů pomocí výchozích čísel portů:

Port Mapping Mode vyberte jako **Auto**.

Pro mapování portů pomocí přizpůsobených čísel portů:

Port Mapping Mode vyberte jako **Manual**.

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

<input checked="" type="checkbox"/> Enable Port Mapping				
Port Mapping Mode <input type="text" value="Manual"/>				
	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
<input type="button" value="Save"/>				

Obrázek 5–19 Konfigurace nastavení NAT

3. Kliknutím na tlačítko **Save** uložíte nastavení.

5.3.11 Konfigurace nastavení FTP

Účel:

Můžete nakonfigurovat související informace o serveru FTP a povolit odesílání pořízených snímků na server FTP. Zachycování snímků lze spustit událostmi nebo úlohou časovaného snímku.

Kroky:

1. Otevřete rozhraní pro nastavení FTP:

Configuration > Advanced Configuration > Network > FTP

2. Nakonfigurujte nastavení FTP. Pro přihlášení k serveru FTP jsou vyžadovány uživatelské jméno a heslo.



- *Kvůli vašim osobním údajům a lepší ochraně před bezpečnostními riziky důrazně doporučujeme použít silná hesla pro všechny funkce a síťová zařízení. Pro zvýšení zabezpečení vašeho produktu by heslo mělo být takové, které jste vybrali sami (s použitím minimálně 8 znaků, včetně velkých a malých písmen, čísel a zvláštních znaků).*

- *Zodpovědnost za správnou konfiguraci všech hesel a ostatních bezpečnostních opatření nese montážní pracovník nebo konečný uživatel.*

Directory: V poli **Directory Structure** můžete vybrat kořenový adresář, nadřazený adresář a podřízený adresář. Vyberete-li možnost nadřazeného adresáře, lze pro název adresáře použít název zařízení, číslo zařízení nebo IP zařízení. Vyberete-li možnost podřízeného adresáře, můžete jako název adresáře použít název kamery nebo číslo kamery.

Upload type: Chcete-li povolit nahrávání uloženého obrázku do serveru FTP.

Anonymní přístup k serveru FTP (v takovém případě není vyžadováno uživatelské jméno ani heslo): Zaškrtnutím zaškrtačacího políčka **Anonymous** povolíte anonymní přístup k serveru FTP.

Poznámka: Server FTP musí funkci anonymního přístupu podporovat.

Server Address	<input type="text" value="0.0.0.0"/>
Port	<input type="text" value="21"/>
User Name	<input type="text"/> <input type="checkbox"/> Anonymous
Password	<input type="text"/>
Confirm	<input type="text"/>
Directory Structure	<input type="text" value="Save in the root directory."/> ▼
Parent Directory	<input type="text" value="Use Device Name"/> ▼
Child Directory	<input type="text" value="Use Camera Name"/> ▼
Upload Type	<input type="checkbox"/> Upload Picture
<input type="button" value="Test"/>	

Obrázek 5–20 Nastavení FTP

3. Kliknutím na tlačítko **Save** uložte nastavení.

Poznámka: Chcete-li pořízené snímky nahrát na server FTP, musíte na stránce **Snímek** povolit časovaný snímek nebo snímek spuštěný událostí. Podrobné informace naleznete v *Části 6.4*.

5.3.12 Nastavení protokolu HTTPS

Účel:

Protokol HTTPS poskytuje ověření webové stránky a souvisejícího webového serveru, se kterým zařízení komunikuje. Je tak zajištěna ochrana proti narušení přenosu (útoky man-in-the-middle). Číslo portu HTTPS nastavíte provedením následujících kroků.

Pokud například nastavíte číslo portu 443 a IP adresa je 192.168.1.64, můžete k zařízení přistoupit prostřednictvím webového prohlížeče zadáním adresy <https://192.168.1.64:443>.

Kroky:

1. Přejděte do okna nastavení protokolu HTTPS.

Configuration > Advanced Configuration > Network > HTTPS

Obrázek 5–21 Okno nastavení protokolu HTTPS

2. Pro povolení této funkce zaškrtněte políčko Enable HTTPS.
3. Vytvořte certifikát podepsaný svým držitelem nebo ověřený certifikát.
 - Vytvoření certifikátu podepsaného svým držitelem
 - 1) Klikněte na tlačítko **Create**, a přejděte tak do okna pro vytvoření.

Obrázek 5–22 Vytvoření certifikátu podepsaného svým držitelem

2) Zadejte zemi, název a IP adresu hostitele, platnost a jiné údaje.

Obrázek 5–23 Vytvoření certifikátu

3) Kliknutím na tlačítko **OK** uložte nastavení.

Poznámka: Pokud již máte certifikát nainstalovaný, bude možnost Vytvořit certifikát podepsaný svým držitelem zašedlá.

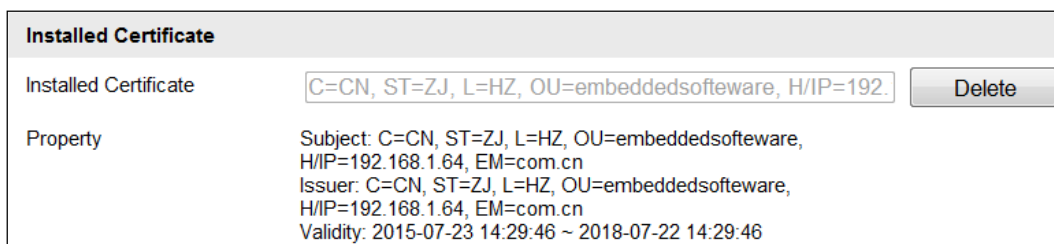
- Vytvoření ověřeného certifikátu

1) Kliknutím na tlačítko **Create** vytvořte požadavek na certifikát.

2) Stáhněte si požadavek na certifikát a odešlete jej důvěryhodné certifikační autoritě k podpisu.

3) Jakmile obdržíte platný podepsaný certifikát, importujte certifikát do zařízení.

4. Po úspěšném vytvoření a instalaci certifikátu se zobrazí informace o certifikátu.



Obrázek 5–24 Nainstalovaný certifikát

5. Kliknutím na tlačítko **Save** uložíte nastavení.

5.4 Konfigurace nastavení videa a zvuku

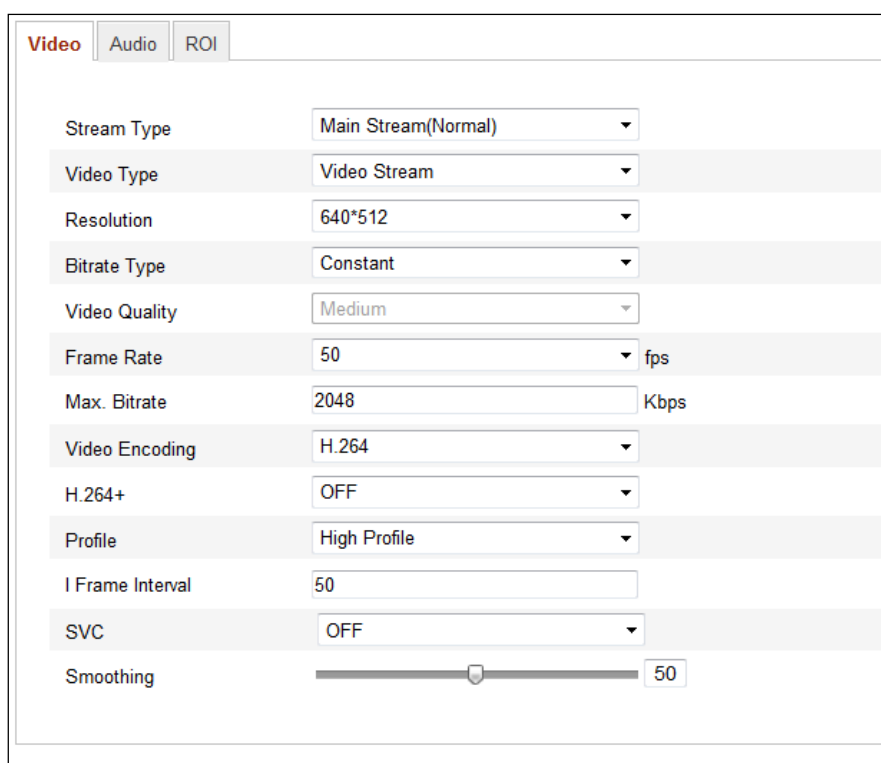
5.4.1 Konfigurace nastavení videa

Kroky:

1. Otevřete rozhraní pro nastavení videa:

Configuration > Basic Configuration > Video/Audio > Video

Nebo **Configuration > Advanced Configuration > Video/Audio > Video**



Obrázek 5–25 Nastavení videa

2. Vyberte **Typ streamu** kamery do hlavního streamu (normální), dílčího streamu nebo třetího streamu. Hlavní stream je obvykle určen pro nahrávání a sledování živého obrazu s dobrou šířku pásma. Dílčí stream může být použit ke sledování živého zobrazení, když je šířka pásma omezena.
3. Následující parametry můžete přizpůsobit pro vybraný hlavní stream nebo dílčí stream:

Video Type:

Vyberte typ streamu do videostreamu nebo kompozitního streamu videa a audia. Audiosignál je možno zaznamenat pouze v případě, že je jako **Video Type** nastaveno **Video & Audio**.

Resolution:

Zvolte rozlišení obrazového výstupu.

Bitrate Type:

Typ datového toku vyberte jako konstantní nebo variabilní.

Video Quality:

Je-li jako typ datového toku vybrán **Variable**, je možno volit 6 úrovní kvality videa.

Frame Rate:

Kmitočet snímků nastavte v intervalu 1/16 až 25 sn./s. Snímkový kmitočet popisuje frekvenci, při které je videostream aktualizován a je měřen počtem snímků za sekundu (fps). Vyšší počet snímků za sekundu je výhodný, když je ve videostreamu pohyb, protože udržuje kvalitu obrazu po celou dobu.

Max. Bitrate:

Maximální datový tok vyberte v intervalu 256 až 16384 Kbps. Vyšší hodnota odpovídá vyšší kvalitě videa, avšak je nutná také vyšší šířka pásma.

Poznámka: Maximální mez maximální přenosové rychlosti se liší v závislosti na různých platformách kamery. U některých kamer, je maximální limit 8192 Kbps nebo 12288 Kbps.

Video Encoding:

Je-li jako **Stream Type** nastaven main stream: Možnosti jsou H.264 a MPEG4. Je-li stream type nastaven na sub stream, je možno volit H.264, MJPEG, a MPEG4.

Poznámka: Typ kódování videa se liší v závislosti na různých platformách kamer.

Profile:

Pro kódování je možno zvolit Basic profile, Main Profile a High Profile.

I Frame Interval:

Interval snímku I nastavte na 1 až 400.

SVC:

Škálovatelné kódování videa je rozšířením standardu H.264/AVC. Pro povolení/zakázání funkce SVC vyberte možnosti VYP/ZAP. Při volbě Auto bude zařízení v případě nedostatečné šířky pásma sítě automaticky extrahovat snímky z původního videa.

Smoothing:

To souvisí s plynulostí streamu. Čím vyšší hodnota vyhlazování, tím lepší plynulost proudu, avšak kvalita videa nemusí být tak uspokojivá. Čím nižší hodnota vyhlazování, tím vyšší kvalita proudu, avšak nemusí se jevit tak plynulý.

4. Kliknutím na tlačítko **Save** uložte nastavení.

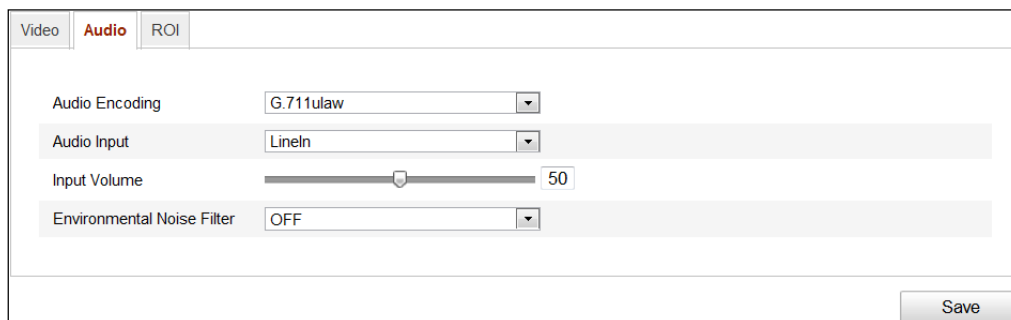
5.4.2 Konfigurace nastavení zvuku

Kroky:

1. Otevřete rozhraní pro nastavení zvuku:

Configuration > Basic Configuration > Video/Audio > Audio

Nebo **Configuration > Advanced Configuration > Video/Audio > Audio**



Obrázek 5–26 Nastavení zvuku

2. Konfigurujte následující nastavení.

Poznámka: Nastavení zvuku se liší v závislosti na různých modelech kamer.

Audio Encoding: Můžete volit možnosti G.722.1, G.711 ulaw, G.711alaw, G.726, MP2L2, AAC a PCM. U MP2L2 je možno konfigurovat vzorkovací kmitočet a přenosovou rychlost audiostreamu. U PCM je možno nastavit vzorkovací kmitočet.

Audio Input: Pro připojený mikrofon a snímací zařízení lze příslušně zvolit mezi možnostmi MicIn a LineIn.

Input Volume: 0–100

Environmental Noise Filter: Nastavte hodnotu OFF nebo ON. Je-li tato funkce povolena, je do jisté míry možno filtrovat okolní hluk.

3. Kliknutím na tlačítko **Save** uložte nastavení.

5.4.3 Konfigurace kódování oblasti ROI

Účel:

Kódování oblasti zájmu pomáhá při kompresi videa rozlišit oblast zájmu a informace v pozadí, což znamená, že technologie přiřadí k oblasti zájmu další zdroje kódování, čímž se zvýší kvalita oblasti zájmu, zatímco informace z pozadí nejsou tak zřetelné.

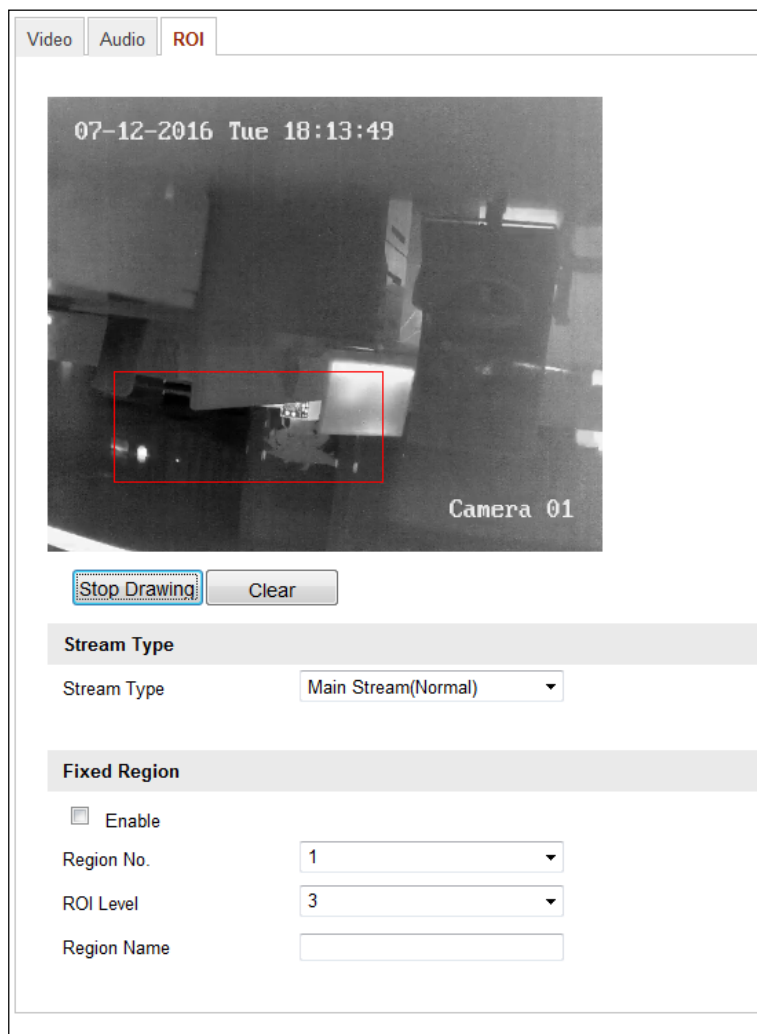
Poznámka: Funkce oblasti ROI se liší v závislosti na různých modelech kamer.

Konfigurace pevného regionu pro ROI:

Kroky:

1. Otevřete rozhraní pro nastavení ROI:
Configuration > Advanced Configuration > Video/Audio > ROI
2. Zaškrtněte zaškrťovací políčko **Enable** pod možností Fixed Region.
3. Vyberte typ datového proudu pro kódování ROI.
4. Pro nastavení oblasti zájmu vyberte region z rozevíracího seznamu čísel regionů.
Lze vybrat čtyři pevné oblasti.
5. Klikněte na tlačítko **Draw Area** a kliknutím a přetažením myši nakreslete oblast zájmu na živé video.

6. Pro nastavení úrovně vylepšení kvality obrazu vyberte úroveň oblasti zájmu. Čím je hodnota vyšší, tím lepší je kvalita obrazu.



Obrázek 5–27 Nastavení oblasti zájmu

7. Podle potřeby zadejte název oblasti pro oblast zájmu.
8. Kliknutím na tlačítko **Save** uložte nastavení.

5.5 Konfigurace parametrů obrazu

5.5.1 Konfigurace nastavení displeje

Účel:

Můžete nastavit kvalitu obrazu kamery včetně jasu, kontrastu atd.

Poznámka: Parametry zobrazení se liší v závislosti na různých modelech kamer.

Podrobné informace naleznete ve skutečných oknech.

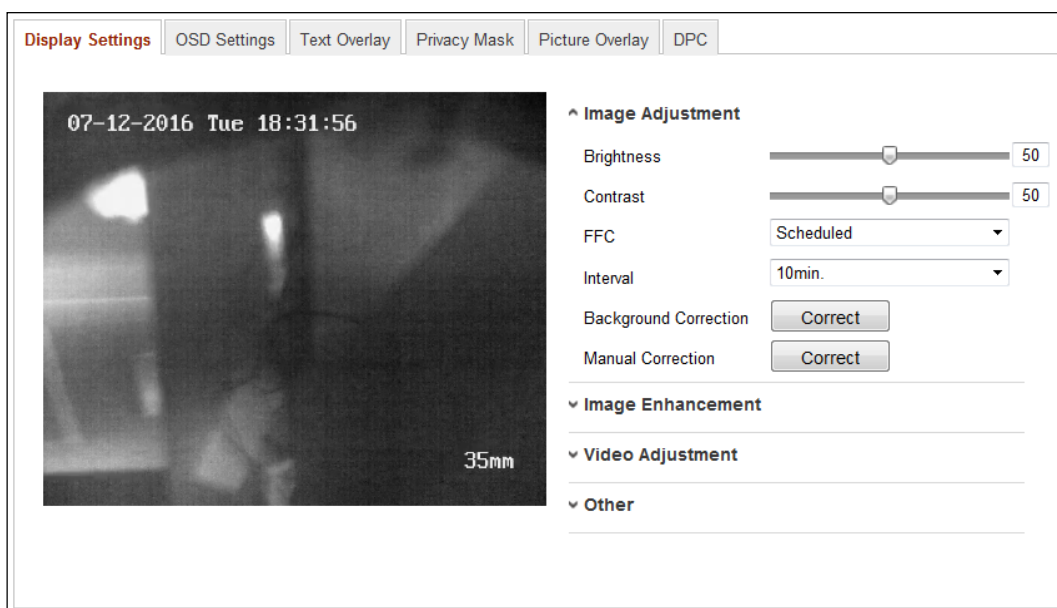
Kroky:

1. Vstupte do rozhraní Display Settings:

Configuration > Basic Configuration > Image > Display Settings

Nebo **Configuration > Advanced Configuration > Image > Display Settings**

2. Nastavte parametry obrazu kamery.



Obrázek 5–28 Konfigurace nastavení zobrazení pro kameru 2

- **Nastavení obrazu**

Brightness popisuje jas obrazu, který se pohybuje v rozmezí 1–100, výchozí hodnota je 50.

Contrast popisuje kontrast obrazu, který se pohybuje v rozmezí 1–100, výchozí hodnota je 50.

FFC (Korekce rovného pole) zlepšuje kvalitu digitálního zobrazování. Dokáže odstranit artefakty z 2D snímků, které způsobily rozdíly v citlivosti pixel na pixel detektoru nebo deformace v optické dráze. Volitelné jsou možnosti Plán, Teplota a OFF.

- **Schedule:** Korekci intervalu můžete vybrat v rozmezí 10, 20, 30, 40, 50, 60, 120, 180 a 240 minut.
- **Temperature:** Kamera snímek přizpůsobí podle teploty.

Manual Background Correction: Objektiv zcela zakryjte nějakým předmětem (doporučujeme kryt objektivu) a klikněte na tlačítko Manual Background Correction, kamera následně snímek upraví podle aktuálního prostředí.

Manual Shutter Correction: Klikněte na tlačítko Manual Shutter Correction, kamera následně snímek nastaví podle teploty samotné kamery.

- **Vylepšení obrazu**

Digital Noise Reduction: Funkce DNR snižuje ve videostreamu šum.

Volitelné jsou možnosti OFF, Normal a Expert. Úroveň DNR nastavte v intervalu 0 až 100 v normálním režimu. Úroveň DNR nastavte z obou rozsahů úrovně DNR [0–100] a úrovně DNR [0–100] v režimu Expert.

Palettes: Palety vám umožňují vybírat požadované barvy. Volitelné jsou možnosti white hot, black hot, fusion 1, rainbow, fusion 2, ironbow 1, ironbow 2, sepia, color 1, color 2, ice fire, rain, red hot a green hot.

DDE: Funkce DDE (digitální vylepšení detailů) dokáže upravit detaily snímku. Vy ji můžete nastavit do režimu OFF nebo Normal. V normálním režimu je možno úroveň DDE nastavit v rozmezí od 1 do 100.

- **Nastavení videa**

Mirror: Funkce zrcadlí obraz, takže se zobrazuje převráceně. Volitelné jsou možnosti Left/Right, Up/Down, Center a OFF.

Video Standard: Volitelné možnosti jsou 50 Hz a 60 Hz. Možnost zvolte v závislosti na různých videostandardech. Obvykle se používá hodnota 50 Hz pro standard PAL a hodnota 60 Hz pro standard NTSC.

Capture Mode: Možnost představuje volitelný režim vstupu videa ke splnění různých požadavků na zorné pole a rozlišení.

Digital Zoom: Pro zobrazení živého zobrazení v původní velikosti, ve dvojnásobném digitálním přiblížení nebo ve čtyřnásobném digitálním přiblížení vyberte digitální zoom jako VYP, 2X nebo 4X.

- **Jiné**

Local Output: Zapnutí nebo vypnutí místního výstupního zařízení.

3. (Volitelné) Výchozí nastavení obnovíte kliknutím na tlačítko **Default**.

5.5.2 Konfigurace nastavení nabídky OSD

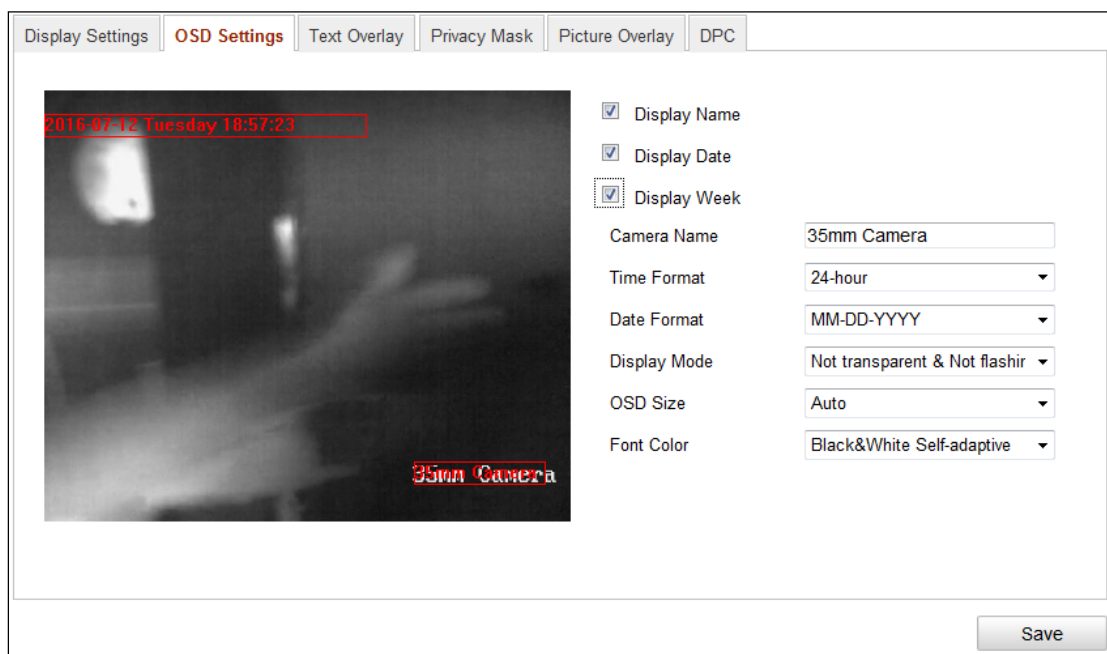
Účel:

Na obrazovce můžete upravit název kamery a čas.

Kroky:

1. Vstupte do rozhraní OSD Settings:

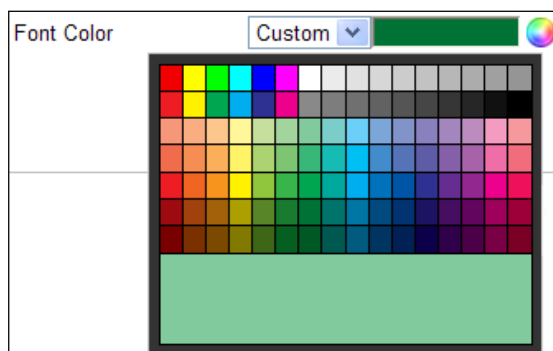
Configuration > Advanced Configuration > Image > OSD Settings



Obrázek 5–29 Nastavení OSD

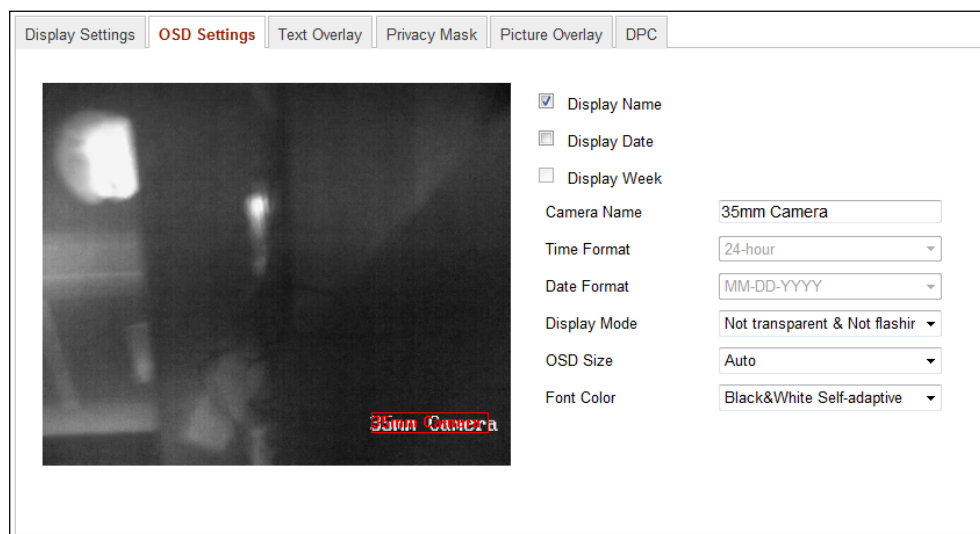
2. Zaškrtnutím odpovídajícího zaškrťovacího políčka vyberte v případě potřeby zobrazení názvu kamery, data nebo týdne.
3. V textovém poli **Camera Name** upravte název kamery.

4. V rozevřacím seznamu vyberte nastavení formátu času, formátu data, režimu zobrazení a velikosti písma OSD.
5. Barvu písma OSD definujete kliknutím na rozevřací seznam, volitelné možnosti jsou black & white self-adaptive a custom.



Obrázek 5–30 Barva písma-vlastní

6. Pro úpravu pozice OSD můžete v okně živého zobrazení kliknout a myší přetáhnout textový rámeček **35mm kamera**.



Obrázek 5–31 Úprava lokace OSD

7. Výše uvedená nastavení aktivujete kliknutím na tlačítko **Save**.

5.5.3 Konfigurace nastavení překrytí textem

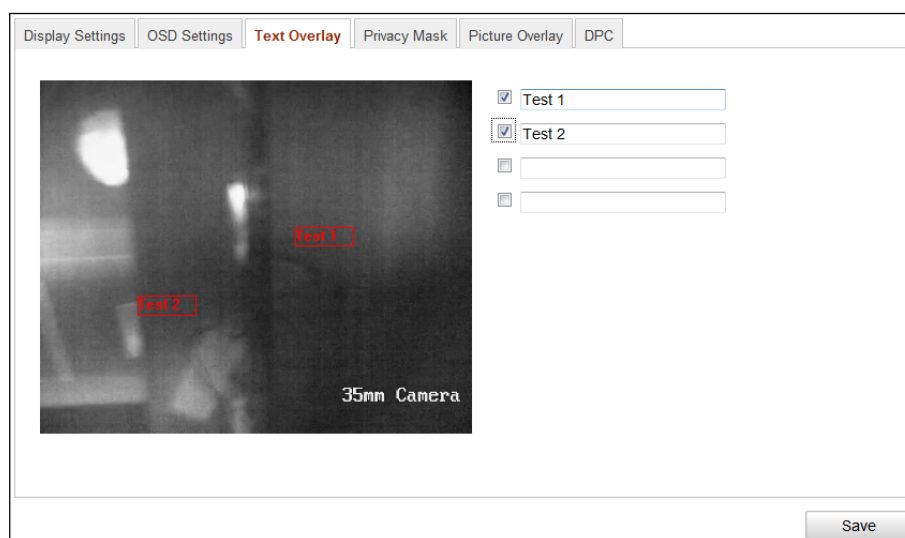
Účel:

Můžete upravit překrytí textem.

Kroky:

1. Otevřete rozhraní pro nastavení překrytí textem:

Configuration > Advanced Configuration > Image > Text Overlay



Obrázek 5–32 Překrytí textem

2. Zobrazení na obrazovce povolíte zaškrtnutím políčka před textovým polem.
3. V textovém poli zadejte znaky.
4. (Volitelné) Pro úpravu pozice překrytí textem můžete v okně živého zobrazení kliknout a myší přetáhnout červený textový rámeček **Test 1**.
5. Kliknutím na tlačítko **Save** uložíte nastavení.

Poznámka: Nakonfigurovat lze až 8 překrytí textem.

5.5.4 Konfigurace masky privátních zón

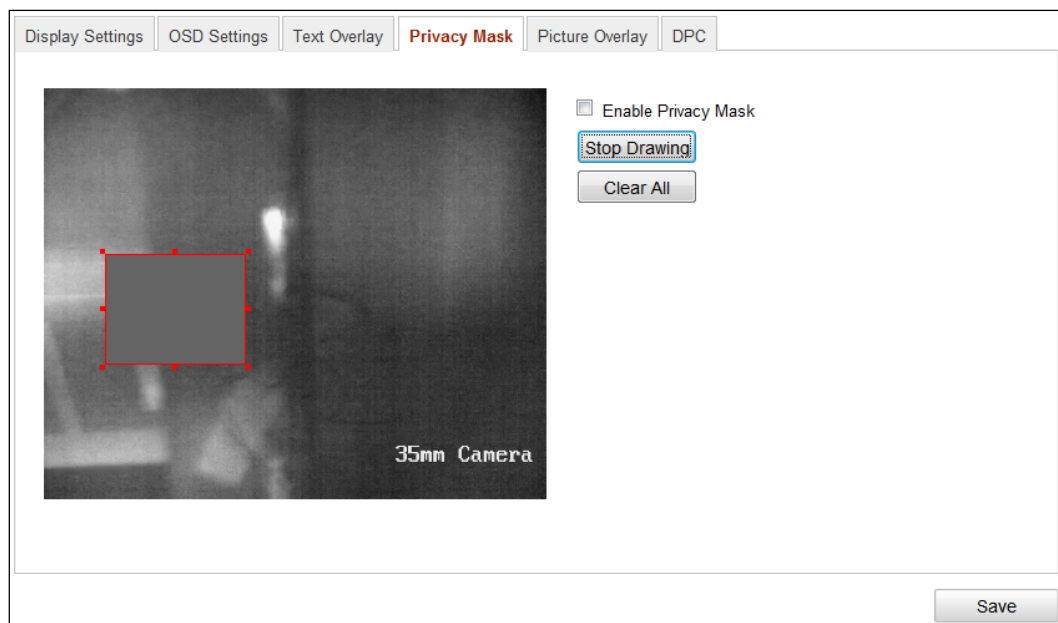
Účel:

Maska privátní zóny umožňuje zakrýt určité oblasti živého video, aby nebylo možno živě zobrazovat a zaznamenávat určitá místa v oblasti sledování.

Kroky:

1. Otevřete rozhraní pro nastavení masky privátní zóny:

Configuration > Advanced Configuration > Image > Privacy Mask



Obrázek 5–33 Nastavení masky privátní zóny

2. Tuto funkci aktivujete zaškrtnutím políčka **Enable Privacy Mask**.
3. Klikněte na možnost **Draw Area**.
4. Kliknutím myši a jejím přetažením nakreslíte v okně živého zobrazení oblast masky.
Poznámka: Na stejném snímku můžete nakreslit až 4 oblastí.
5. Kliknutím na tlačítko **Stop Drawing** dokončete kreslení nebo kliknutím na tlačítko **Clear All** odstraňte všechny nastavené oblasti bez jejich uložení.
6. Kliknutím na tlačítko **Save** uložte nastavení.

5.5.5 Konfigurace překrytí obrazu

Účel:

Překrytí obrazu umožňuje překrýt snímaný obraz. Tato funkce umožňuje určitým podnikům nebo uživatelům překrýt svým logem obraz.

Poznámka: Snímek musí být ve formátu RGB24 bmp, maximální velikost snímku je 128x128.

Kroky:

1. Otevřete rozhraní Nastavení překrytí snímků:

Configuration > Advanced Configuration > Image > Picture Overlay



Obrázek 5–34 Překrytí obrazu

2. Kliknutím na tlačítko **Browse** vyberte obrázek.
3. Kliknutím na tlačítko Upload jej načtěte.
4. Zaškrtnutím zaškrtačacího políčka Enable Picture Overlay tuto funkci povolte. Hodnoty souřadnic X a Y odkazují na umístění obrázku na snímku. Výška a šířka snímku zobrazují velikost snímku.
5. Kliknutím na tlačítko **Save** uložte nastavení.

5.5.6 Konfigurace DPC (korekce chybných pixelů)

Účel:



DPC (korekce chybných pixelů) odkazuje na funkci, kdy kamera může opravit chybné pixely na LCD, které se nechovají podle očekávání.

Poznámka: Tato funkce je dostupná pouze u některých modelů kamer.

Kroky:


1. Vstupte do rozhraní nastavení OSD.

Configuration > Advanced Configuration > Image > DPC

2. Klikněte na snímek a vyberte chybný pixel. Kurzor na snímku se přesune na pozici kliknutí. Pro jemnou úpravu pozice kurzoru můžete kliknout na .
3. Pro zahájení korekce klikněte na .



Obrázek 5–35 Oprava chybných pixelů


4. (Volitelné) Pro zrušení korekce klepněte na .

5.6 Konfigurace a správa událostí alarmu

Tato část vysvětluje, jak síťovou kameru nakonfigurovat tak, aby reagovala na události alarmu, včetně detekce pohybu, neoprávněné manipulace s videem, vstupu alarmu, výstupu alarmu, výjimky, detekce obličeje, detekce výjimky zvuku, detekce narušení, detekce rozostření, detekce změny scény atd. Tyto události mohou spustit metody propojení, jako je upozornění monitorovacího centra, odesílání e-mailu, spuštění výstupu alarmu atd.

Poznámky:

- Pokud chcete v případě spuštění alarmu odeslat push oznámení s informacemi o alarmu na počítač nebo do mobilního klientského softwaru, zaškrtněte zaškrťovací políčko Notify Surveillance Center.

- Klikněte na  pro nápovědu při konfiguraci inteligentních funkcí, včetně detekce obličeje, detekce výjimky zvuku, detekce narušení, detekce rozostření, detekce změny scény atd. Nápověda vás provede kroky konfigurace.

5.6.1 Konfigurace detekce pohybu

Účel:

Funkce detekce pohybu detekuje v nakonfigurované oblasti sledování pohybující se objekty. Při spuštění alarmu může dojít k provedení řady akcí.

K přesné detekci pohybujících se objektů a snížení četnosti falešných alarmů lze pro různý prostředí detekce pohybu zvolit z možností normální konfigurace a odborné konfigurace.

- **Běžná konfigurace**

Běžná konfigurace přijímá stejnou sadu parametrů detekce pohybu ve dne i v noci.

Úloha 1: Nastavit oblast detekce pohybu.

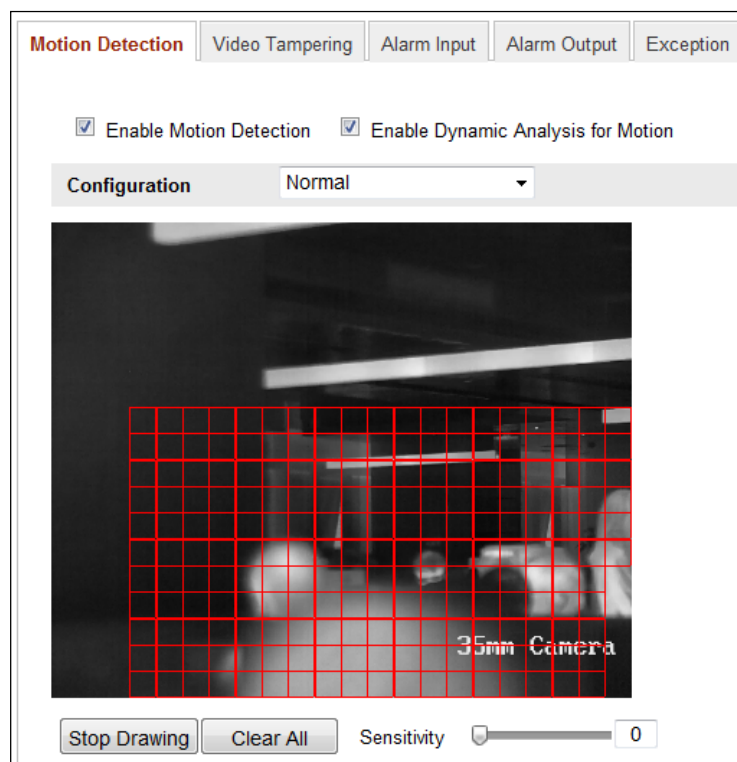
Kroky:

- (1) Vstupte do rozhraní nastavení detekce pohybu

Configuration > Advanced Configuration > Basic Event > Motion Detection

- (2) Zaškrtněte zaškrťovací políčko **Enable Motion Detection**.
- (3) Chcete-li detekované objekty v živém videu označit zelenými obdélníky , zaškrtněte políčko **Enable Dynamic Analysis for Motion**.

Poznámka: Pro povolení nebo zakázání označení pohybujících se objektů v živém videu přejděte na položky Local Configuration > Live View Parameters a povolte/zakažte pravidla.

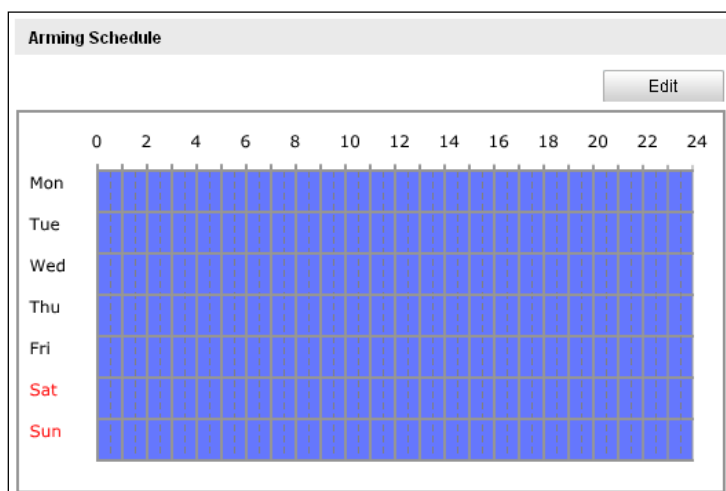


Obrázek 5–36 Povolení detekce pohybu


- (4) Klikněte na možnost **Draw Area**. Kliknutím myši a jejím přetažením nakreslíte v živém zobrazení oblast detekce pohybu.
- (5) Kliknutím na tlačítko **Stop Drawing** dokončíte nakreslení jedné oblasti.
- (6) (Volitelné:) Kliknutím na tlačítko **Clear All** odstraníte všechny oblasti.
- (7) (Volitelné:) Posunutím posuvníku nastavíte citlivost detekce.

Úloha 2: Nastavte plán střezení pro detekci pohybu.

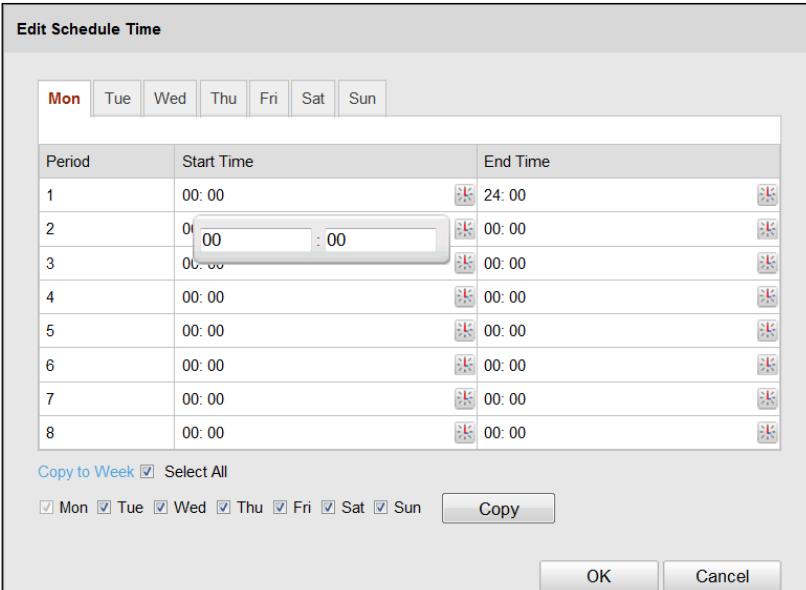
Kroky:



Obrázek 5–37 Čas střezení

- (1) Pro úpravu plánu střežení klikněte na možnost **Edit**. Obrázek 6-34 zobrazuje rozhraní úprav plánu střežení.
- (2) Vyberte den, pro který chcete nastavit plán střežení.
- (3) Pro nastavení časového období plánu střežení klikněte na .
- (4) (Volitelné) Po nastavení plánu střežení můžete tento plán kopírovat na další dny.
- (5) Kliknutím na tlačítko **OK** uložíte nastavení.

Poznámka: Čas jednotlivých období se nemůže překrývat. Pro jednotlivé dny lze nakonfigurovat až 8 období.



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

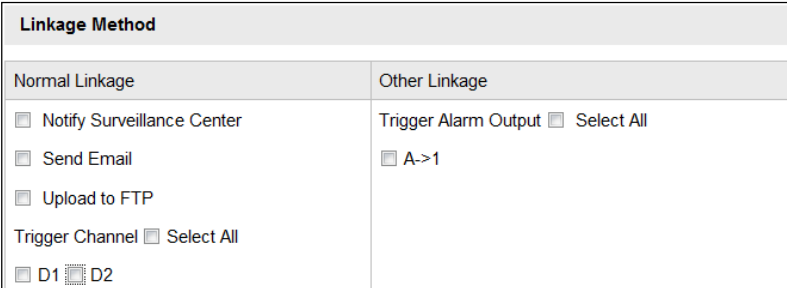
Copy to Week Select All

Mon Tue Wed Thu Fri Sat Sun

Obrázek 5–38 Časový harmonogram aktivace

Úloha 3: Nastavte akce alarmu pro detekci pohybu.

Zaškrtnutím políčka vyberte metodu propojení. Volitelné možnosti jsou Notify Surveillance Center, Send Email, Upload to FTP, Trigger Channel a Trigger Alarm Output. Můžete specifikovat metodu propojení při výskytu alarmu.



Normal Linkage	Other Linkage
<input type="checkbox"/> Notify Surveillance Center	Trigger Alarm Output <input type="checkbox"/> Select All
<input type="checkbox"/> Send Email	<input type="checkbox"/> A->1
<input type="checkbox"/> Upload to FTP	
Trigger Channel <input type="checkbox"/> Select All	
<input type="checkbox"/> D1 <input type="checkbox"/> D2	

Obrázek 5–39 Metoda propojení

- **Slyšitelné varování**

Jedná se o místní spuštění slyšitelného varování. Podporována je pouze zařízením se zvukovým výstupem.

- **Upozornění monitorovacího centra**

Při výskytu události odeslat výjimku nebo signál alarmu do vzdáleného softwaru pro správu.

- **Odeslat e-mail**

Při výskytu události odeslat e-mail s informacemi o alarmu uživateli nebo uživatelům.

Poznámka: Pro odeslání e-mailu v případě vzniku události se řiďte pokyny v *Části 5.3.9 Alarmem spuštěné odeslání e-mailu* a nastavte odpovídající parametry.

- **Nahrání na FTP**

Při aktivaci alarmu zachytit snímek a nahrát obrázek na server FTP.

Poznámky:

- Nejprve nastavte adresu serveru FTP a vzdáleného serveru FTP. Pro podrobné informace se řiďte pokyny v *Části 5.3.11 Konfigurace nastavení FTP*.
- Přejděte na stránku **Advanced Configuration > Storage > Snapshot**, povolte snímek při spuštění události a nastavte interval snímání a počet snímků.
- Zachycený snímek lze také načíst na dostupnou kartu SD nebo síťový disk.

- **Spuštění kanálu**

V případě detekce pohybu dojde k nahrávání videa. Pro realizaci této funkce je nutné nastavit harmonogram nahrávání. Pro podrobné informace se řiďte pokyny v *Části 6.3*.

- **Spuštění výstupu alarmu**

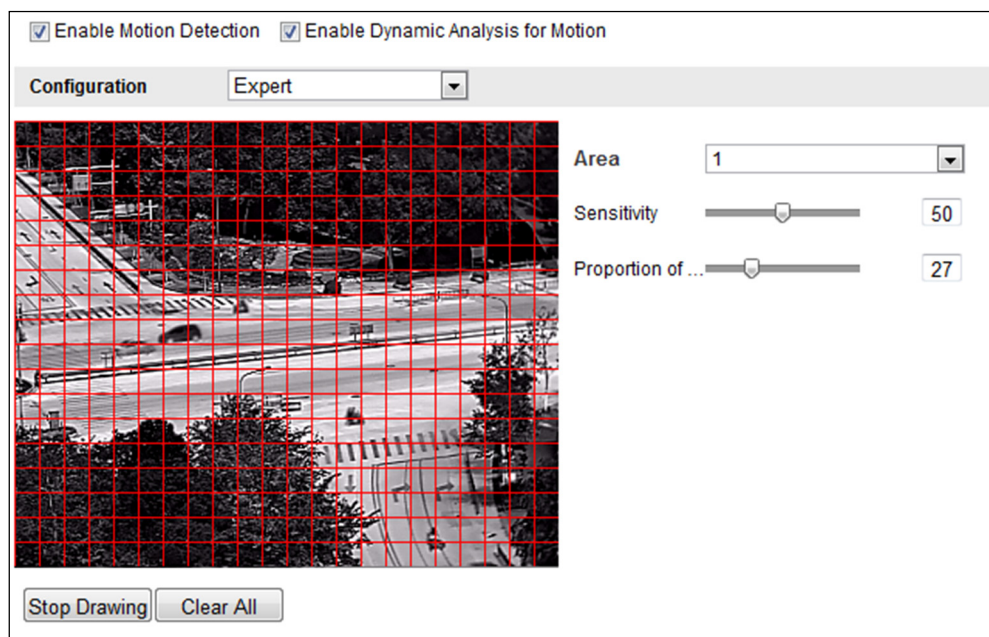
Při výskytu události aktivovat jeden nebo více externích výstupů alarmu.

Poznámka: Pro spuštění výstupu alarmu v případě vzniku události se řiďte pokyny v *Části 5.6.4 Konfigurace výstupu alarmu* a nastavte odpovídající parametry.

● Odborná konfigurace

Režim Expert se používá především ke konfiguraci citlivosti a proporcí objektu u jednotlivých oblastí pro různé přepínání režimů den/noc.

Poznámka: Přepínání režimů den/noc není možno realizovat pro kanál termovizní kamery. Položky Oblast, Citlivost a Proporce objektu v oblasti jsou stále konfigurovatelné.



Obrázek 5–40 Odborný režim detekce pohybu

5.6.2 Konfigurace alarmu na neoprávněnou manipulaci s videem

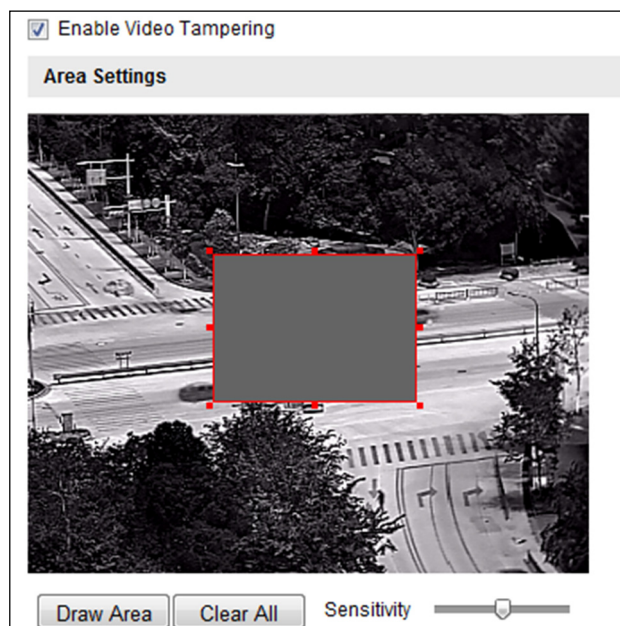
Účel:

Kameru můžete nakonfigurovat tak, aby spustila alarm v okamžiku, kdy je objektiv zakryt a aby v reakci na alarm provedla určité akce.

Kroky:

1. Otevřete rozhraní pro nastavení neoprávněné manipulace s videem:

Configuration > Advanced Configuration > Basic Event > Video Tampering



Obrázek 5–41 Alarm neoprávněné manipulace s videem

2. Zaškrtnutím zaškrťovacího políčka **Enable Video Tampering** povolte funkci detekce neoprávněné manipulace s videem.
3. Nastavte oblast neoprávněné manipulace s videem. Řiďte se podle *Úlohy 1, Nastavení oblasti detekce pohybu v Části 5.6.1.*
4. Kliknutím na tlačítko **Edit** upravte plán střežení pro neoprávněnou manipulaci s videem. Konfigurace harmonogramu aktivace je stejná jako nastavení harmonogramu aktivace pro detekci pohybu. Řiďte se podle *Úlohy 2, Nastavení plánu střežení pro detekci pohybu v Části 5.6.1.*
5. Zaškrtnutím zaškrťovacího políčka vyberte způsob propojení pro neoprávněnou manipulaci s videem. Lze zvolit z možností Audible Warning, Notify Surveillance Center, Send Email a Trigger Alarm Output. Řiďte se podle *Úlohy 3, Nastavení plánu akcí pro detekci pohybu v Části 5.6.1.*
6. Kliknutím na tlačítko **Save** uložte nastavení.

5.6.3 Konfigurace vstupu alarmu

Účel:

Detekuje vstup alarmu a provádí kroky reakce při spuštění alarmu.

Kroky:

1. Otevřete rozhraní pro nastavení vstupu alarmu:

Configuration > Advanced Configuration > Basic Event > Alarm Input

2. Vyberte číslo vstupu alarmu a typ alarmu. V nabídce Alarm Type lze zvolit z možností NO (normálně rozpojený) nebo NC (normálně sepnutý). Úpravou názvu nastavte název vstupu alarmu (volitelné).

The screenshot displays the configuration page for an alarm input. At the top, there are three input fields: 'Alarm Input No.' with a dropdown menu showing 'A<-1', 'Alarm Name' with a text box and '(cannot copy)' label, and 'Alarm Type' with a dropdown menu showing 'NO'. Below these fields is a section titled 'Arming Schedule' with an 'Edit' button. The schedule is represented by a grid with days of the week (Mon, Tue, Wed, Thu, Fri, Sat, Sun) on the vertical axis and a 24-hour clock (0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24) on the horizontal axis. The grid cells are currently empty.

Obrázek 5–42 Nastavení vstupu alarmu

3. Pro nastavení plánu střežení vstupu alarmu klikněte na tlačítko **Edit**. Řiďte se podle *Úlohy 2, Nastavení plánu střežení pro detekci pohybu* v *Části 5.6.1*.
4. Zaškrtněte políčko pro volbu metody propojení vstupu alarmu. Řiďte se podle *Úlohy 3, Nastavení plánu akcí pro detekci pohybu* v *Části 5.6.1*.
5. Je-li vaše kamera nainstalována s jednotkou pro otáčení/náklon, můžete také zvolit propojení PTZ pro vstup alarmu. Zaškrtněte příslušné zaškrťovací políčko a vyberte číslo – tím aktivujete volání předvolby, volání hlídky nebo volání vzoru.

6. Můžete zkopírovat nastavení do ostatních vstupů alarmu.
7. Kliknutím na tlačítko **Save** uložíte nastavení.

5.6.4 Konfigurace výstupu alarmu

Účel:

Detekuje výstup alarmu a provádí kroky reakce při spuštění alarmu.

Kroky:

1. Otevřete rozhraní pro nastavení výstupu alarmu:
Configuration >Advanced Configuration > Basic Event > Alarm Output
2. Vyberte některý výstupní kanál alarmu v rozevíracím seznamu **Alarm Output**.
Pro výstup alarmu lze také upravit název (volitelné).
3. Doba prodlevy může být nastavena na 5sec, 10sec, 30sec, 1min, 2min, 5min, 10min nebo Manual. Doba prodlevy platí pro dobu trvání, kdy výstup alarmu zůstává v platnosti po výskytu alarmu.
4. Pro vstup do rozhraní pro úpravu časového plánu klikněte na položku **Edit**.
Konfigurace časového plánu je stejná jako nastavení plánu střežení pro detekci pohybu. Řiďte se podle *Úlohy 2, Plán střežení pro detekci pohybu* v *Části 5.6.1*.
5. Můžete zkopírovat nastavení do ostatních výstupů alarmu.
6. Kliknutím na tlačítko **Save** uložíte nastavení.

Alarm Output: A->1

Alarm Name: (cannot copy)

Delay: 5s

Arming Schedule

Edit

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

Obrázek 5–43 Nastavení výstupu alarmu

5.6.5 Ošetření výjimky

Typ výjimky může představovat plný pevný disk, chyba pevného disku, odpojení sítě, konflikt IP adres a nepovolené přihlášení ke kamerám.

Kroky:

1. Otevřete rozhraní pro nastavení výjimky:

Configuration > Advanced Configuration > Basic Event > Exception

2. Zaškrtněte políčko pro nastavení akcí prováděných při alarmu výjimky. Řiďte se podle *Úlohy 3, Nastavení plánu akcí podniknutých při detekci pohybu v Části 5.6.1.*

Exception Type: HDD Full

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

Save

Obrázek 5–44 Nastavení vyjímky

3. Kliknutím na tlačítko **Save** uložíte nastavení.

5.6.6 Konfigurace detekce výjimky zvuku

Účel:

Funkce detekce výjimky zvuku rozpoznává ve scéně sledování abnormální zvuky, jako je náhlé zvýšení nebo snížení zvukové intenzity. Při spuštění alarmu lze provést určité akce.

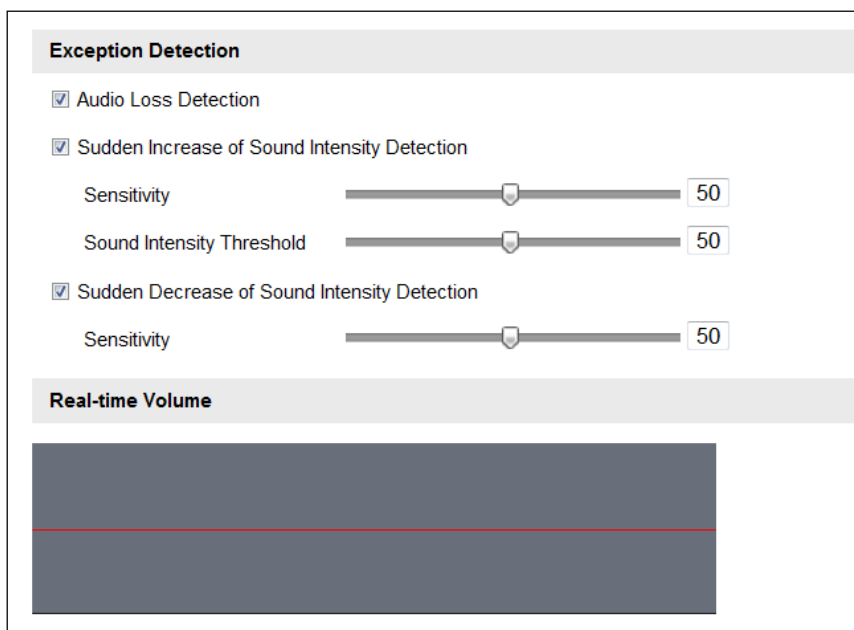
Poznámka: Funkce detekce výjimky zvuku se liší v závislosti na různých modelech kamer.

Kroky:

1. Vstupte do rozhraní nastavení detekce výjimky zvuku:
Configuration > Advanced Configuration > Smart Event > Audio Exception Detection
2. Funkci detekce ztráty zvuku povolíte zaškrtnutím zaškrťovacího políčka **Audio Loss Exception**.
3. Náhlé zesílení zvuku ve scéně sledování rozpoznáte zaškrtnutím zaškrťovacího políčka u možnosti **Sudden Increase of Sound Intensity Detection**. Pro náhlé zesílení zvuku lze nastavit citlivost a práh detekce.
4. Náhlé zeslabení zvuku ve scéně sledování rozpoznáte zaškrtnutím zaškrťovacího políčka u možnosti **Sudden Decrease of Sound Intensity Detection**. Pro náhlé zeslabení zvuku lze nastavit citlivost a práh detekce.

Poznámky:

- Citlivost: Rozsah [1–100] – čím nižší je hodnota, tím silnější musí být změna ke spuštění detekce.
- Práh intenzity zvuku: Rozsah [1–100] – pomocí této možnosti lze filtrovat zvuk prostředí. Čím je zvuk prostředí hlasitější, tím vyšší by měla být hodnota. Možnost lze nastavit dle skutečného prostředí.



Obrázek 5–45 Konfigurace detekce výjimky zvuku

5. Můžete zobrazit hlasitost zvuku v reálném čase.
6. Kliknutím na tlačítko **Edit** nastavte plán střežení.
7. Vyberte metodu propojení pro výjimku zvuku. Řiďte se podle *Úlohy 3, Nastavení plánu akcí podniknutých při detekci pohybu* v Části 5.6.1.
8. Kliknutím na tlačítko **Save** uložte nastavení.

5.6.7 Detekce změny scény

Účel:

Funkce detekce změny scény slouží k detekci změny sledovaného prostředí ovlivněné externími faktory, jako je úmyslné otočení kamery. Při spuštění alarmu lze provést určité akce.

Kroky:

1. Vstupte do rozhraní nastavení detekce změny scény: Configuration > Advanced Configuration > Smart Event > Scene Change Detection.
2. Pro povolení této funkce zaškrtněte políčko **Enable Scene Change Detection**.
3. Kliknutím a přetažením posuvníku nastavte citlivost detekce. Hodnota citlivosti se pohybuje na stupnici od 1 do 100, čím vyšší je hodnota, tím snadněji může změna scény spustit alarm.

4. Kliknutím na tlačítko **Edit** nastavte plán střežení.
5. Vyberte metodu propojení pro změnu scény, včetně **Upozornění monitorovacího centra, odeslání e-mailu, nahrání na FTP, spuštění kanálu a spuštění výstupu alarmu.**
6. Kliknutím na tlačítko **Save** uložte nastavení.

5.6.8 Konfigurace dynamické detekce zdroje požáru

Účel:

Když tuto funkci povolíte a je zjištěn zdroj požáru, spustí se akce alarmu.

Kroky:

1. Vstupte do rozhraní dynamické detekce zdroje požáru:
Configuration > Advanced Configuration > Smart Event > Dynamic Fire Source Detection
2. Pro povolení této funkce zaškrtněte políčko **Enable Dynamic Fire Source Detection**.

Dynamic Fire Source Detection	
<input checked="" type="checkbox"/>	Enable Dynamic Fire Source Detection
<input checked="" type="checkbox"/>	Display Fire Source Frame on Stream
Sensitivity	<input type="range" value="5"/>
Linkage Method	
Normal Linkage	Other Linkage
<input type="checkbox"/> Notify Surveillance Center	Trigger Alarm Output <input type="checkbox"/> Select All
<input type="checkbox"/> Send Email	<input type="checkbox"/> A->1
<input type="checkbox"/> Upload to FTP	
Trigger Channel <input type="checkbox"/> Select All	
<input type="checkbox"/> D1 <input type="checkbox"/> D2	
<input type="button" value="Save"/>	

Obrázek 5–46 Konfigurace dynamické detekce zdroje požáru

3. Pro zobrazení červeného rámečku kolem zdroje požáru ve streamu v případě požáru zaškrtněte políčko **Display Fire Source Frame on Stream**. (volitelné)

4. Stupeň citlivosti dynamické detekce zdroje požáru můžete posunutím kurzoru upravit na stupnici od 1 do 10. Čím vyšší bude číslo, tím citlivější bude detekce.
5. Zaškrtněte políčko pro volbu metody propojení vstupu alarmu. Viz **Úloha 3: V části *Detekce pohybu nastavte akce alarmu pro detekci pohybu***. V poli Other Linkage můžete zaškrtnout políčko pro povolení výstupu alarmu (počet alarmů se liší podle možností zařízení).
6. Kliknutím na tlačítko **Save** uložte nastavení.

5.7 Měření teploty

Účel:

Když tuto funkci povolíte, měří skutečnou teplotu monitorovaného místa. Zařízení spustí alarm, pokud teplota překročí prahovou hodnotu teploty.

Dříve než začnete:

Pro volbu **Temperature Measurement + Behavior Analysis** jako VCA Resource Type zadejte **Configuration > Advanced Configuration > System > VCA Resource Type**.

5.7.1 Konfigurace měření teploty

Kroky:

1. Vstupte do nabídky konfigurace **Configuration > Advanced Configuration > Temperature Measurement**.

Obrázek 5–47 Dynamická detekce zdroje požáru

2. Zaškrtněte políčka rozhraní pro nastavení konfigurace měření teploty.
 - **Enable Temperature Measurement:** Toto políčko zaškrtněte pro povolení funkce měření teploty.
 - **Display Temperature Info. on Stream:** Toto políčko zaškrtněte pro zobrazení informací o teplotě v živém zobrazení.
 - **Add Original Data on Capture:** Toto políčko zaškrtněte pro přidání originálních dat na nahrávku.
 - **Add Original Data on Stream:** Toto políčko zaškrtněte pro přidání originálních dat na stream.
 - **Data Refresh Interval:** Interval aktualizace dat vyberte v intervalu od 1 do 5 sekund.
 - **Unit:** Zobrazení teploty ve stupních Celsia (°C) / stupních Fahrenheita (°F) / stupních Kelvina (K).
 - **Temperature Range:** Nastavte teplotní rozsah.
3. Nastavení uložíte kliknutím na tlačítko **Save**.

5.7.2 Měření teploty a alarm

Účel:

Tato funkce je používána pro měření teploty zjištěné na místě, zařízení porovnává teploty vybraných regionů a alarmy.


Kroky:





1. Vstupte do nabídky **Configuration > Advanced Configuration > Temperature Measurement and Alarm**.
2. Nastavte pravidlo alarmu: Ze seznamu pravidel vyberte pravidlo pro měření teploty a nakonfigurujte parametry.
 - **Name:** Můžete přizpůsobit název pravidla.
 - **Type:** Jako typ pravidla vyberte bod, linii nebo snímek.
 - **Emissivity:** Nastavte emisivitu cíle. Poznámka: Emisivita každého objektu je jiná.
 - **Distance (m):** Lineární vzdálenost mezi cílem a zařízením.

- **Reflective Temperature:** Pokud na scéně existuje nějaký cíl s vysokou emisivitou, zaškrtněte políčko a nastavte reflexivní teplotu pro úpravu teploty. Pokud žádný takový cíl neexistuje, zaškrtnutí políčka zrušte.

Enable	ID	Name	Type	Emissivity	Distance(m)	Reflective Temper...	Alarm Rule
<input checked="" type="checkbox"/>	2		Frame	0.98	1	<input type="checkbox"/> 0	<input type="checkbox"/>
<input checked="" type="checkbox"/>	3		Line	0.96	30	<input type="checkbox"/> 0	<input type="checkbox"/>
<input checked="" type="checkbox"/>	4		Point	0.96	30	<input type="checkbox"/> 0	<input type="checkbox"/>
<input type="checkbox"/>	5		Point	0.96	30	<input type="checkbox"/> 0	<input type="checkbox"/>
<input type="checkbox"/>	6		Point	0.96	30	<input type="checkbox"/> 0	<input type="checkbox"/>
<input type="checkbox"/>	7		Point	0.96	30	<input type="checkbox"/> 0	<input type="checkbox"/>
<input type="checkbox"/>	8		Point	0.96	30	<input type="checkbox"/> 0	<input type="checkbox"/>
<input type="checkbox"/>	9		Point	0.96	30	<input type="checkbox"/> 0	<input type="checkbox"/>

Obrázek 5–48 Konfigurace měření teploty

3. Pro zobrazení rozhraní pravidla alarmu klikněte v seznamu na .
 - **Alarm Rule:** Pravidlo alarmu se liší podle různých typů. Toto pravidlo je určeno pro porovnávání informací o teplotě dvou vybraných oblastí. U cílů stanovených snímkem pravidla zahrnují: **Max. teplota je vyšší než, Max. teplota je nižší než, Min teplota je vyšší než, Min. teplota je nižší než, Průměrná teplota je vyšší než, Průměrná teplota je nižší než, Teplotní rozdíl je vyšší než a Teplotní rozdíl je nižší než.** U cílů stanovených linií pravidla zahrnují Max. teplotu, Min. teplotu a Průměrnou teplotu. U cílů stanovených bodem se pravidla liší podle průměrné teploty.

- **Pre-Alarm Temperature a Alarm Temperature:** Nastavte teplotu předpoplachu a teplotu alarmu. Zařízení vyšle předpoplach, pokud teplota pravidla přesáhne teplotu předpoplachu, alarm bude odeslán, pokud teplota pravidla překročí teplotu alarmu.
 - **Tolerance Temperature:** Nastavte toleranci teploty a zařízení posoudí, zda se spuštěný alarm zastaví, dokud teplota/teplotní rozdíl zařízení nebude nižší než pravidlo teploty tolerance teploty. Můžete například nastavit toleranci teploty na 3 °C, teplotu alarmu na 55 °C a teplotu předpoplachu na 50 °C. Zařízení vyšle předpoplach v okamžiku, kdy teplota dosáhne 50 °C a spustí alarm ve chvíli, kdy teplota dosáhne 55 °C, alarm bude zrušen pouze v případě, že teplota zařízení bude nižší než 52 °C.
4. Vykreslete cílovou oblast: Vyberte pravidlo a vykreslete odpovídající snímek/čáru/bod. Pro vykreslení bodu klikněte na . Pro vykreslení linie klikněte na . Pro vykreslení snímku klikněte na .
 5. Nastavte alarm teplotního rozdílu: Pro vstup do rozhraní teplotního rozdílu klikněte na tlačítko Temperature Difference Alarm, nastavit lze až čtyři alarmy teplotního rozdílu.


Alarm teplotního rozdílu se vztahuje pouze na cíle stanovené snímkem.
 6. Nastavte propojení alarmu: Pro vstup do rozhraní propojení alarmu klikněte na Alarm Linkage a nastavte metodu propojení.
 7. Kliknutím na tlačítko **Save** uložte nastavení.

5.8 Konfigurace VCA

5.8.1 Typ zdroje VCA

Před použitím pravidel VCA kamery musíte nejprve vybrat typ prostředku VCA.

Pro použití měření teploty a analýzy chování vyberte **Temperature Measurement a Behavior Analysis**. Pro použití dynamické detekce zdroje požáru vyberte možnost **Dynamic Fire Source Detection**. Jakmile některý ze zdrojů vyberete, druhé pravidlo VCA nelze povolit.

5.8.2 Informace VCA

- **Behavior Analysis Version:**

Slouží k zobrazení seznamu verzí knihovny algoritmů.

- **Display information**

Zahrnuje zobrazení na snímku obrázku a zobrazení ve streamu. Odpovídající zobrazení povolíte zaškrtnutím políček.

Obrázek 5–49 Informace VCA

- **Display Target info. on Alarm Picture:** Pokud je toto políčko zaškrtnuto, zobrazí se v načteném snímku alarmu na cíli rámeček.
- **Display Rule info. on Alarm Picture:** Zachycený cíl a nakonfigurovaná oblast budou na snímku alarmu označeny rámečkem.
- **Display VCA info. on Stream:** V živém zobrazení nebo přehrávání se na cíli zobrazí zelené rámečky.

Poznámka: Zkontrolujte, zda jsou v místních nastaveních pravidla povolena. Přejděte na nabídku **Configuration > Local Configuration > Rules** a povolte je.

- **Snapshot Setting**

Pro zachycený snímek lze nastavit kvalitu a rozlišení.

- **Upload JPEG Image to Center:** Zaškrtnete-li toto políčko, dojde v případě alarmu VCA k načtení zachyceného snímku do monitorovacího centra.
- **Picture Quality:** Lze zvolit z možností High, Medium a Low.
- **Picture Resolution:** Volitelné možnosti jsou 384x288, CIF, 4CIF, 720 P a 1080 P.

Poznámka: Možnosti volitelného rozlišení snímku se liší v závislosti na různých modelech kamer.

5.8.3 Analýza chování

Účel:

Analýza chování provádí detekci řady podezřelých chování. Pokud se spustí alarm, budou povoleny určité způsoby propojení. Pro nastavení konfigurace analýzy chování postupujte podle následujících kroků.

Kroky:

1. Zobrazení informací a nastavení snímku nakonfigurujte na stránce **Informace VCA**.
2. Nastavení **kalibrace kamery**

Provedením následujících kroků nastavíte trojrozměrné měření a výpočty snímku z kamery, a tím kalkulaci velikosti všech cílů. Detekce VCA bude v případě nakonfigurované kalibrace kamery přesnější.

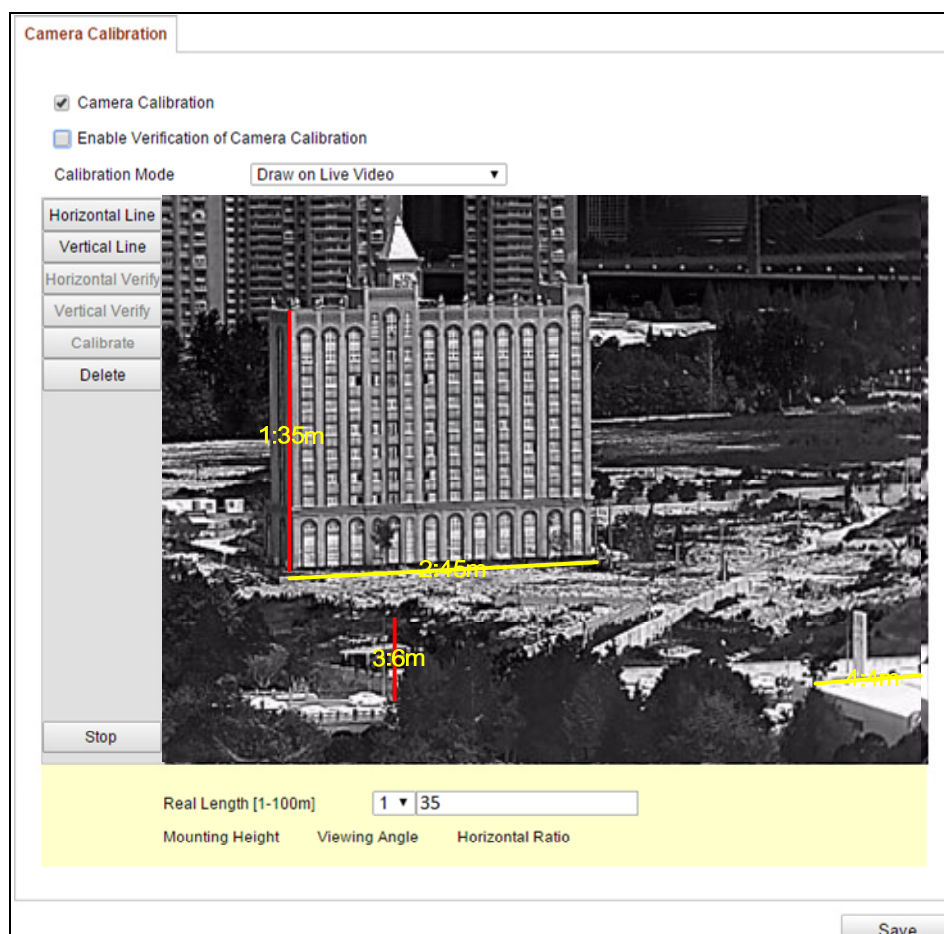
Kroky:

- 1) Vstupte do rozhraní nastavení kalibrace kamery:
Configuration > VCA Configuration > Camera Calibration
- 2) Zaškrtnutím zaškrťovacího políčka **Camera Calibration** tuto funkci povolte.
- 3) Calibration mode vyberte jako Input Basic Data nebo Draw on Live View Video.
Input Basic Data: Ručně zadejte montážní výšku, zorný úhel a poměr horizontu kamery.
Draw on Live View Video: Kliknutím na možnost Nakreslit ověřovací linii (horizontální)/(vertikální) nakreslete v živém zobrazení horizontální nebo vertikální linii a do pole reálné délky zadejte skutečnou délku. Kamera může pomocí nakreslených referenčních linií a jejich skutečných délek vyhodnotit jiné objekty, které se v živém zobrazení objeví.

- 4) (Volitelné) Zaškrtněte políčko **Enable Verification of Camera Calibration**, pro vykreslení vodorovné/svislé čáry v živém zobrazení klikněte na tlačítko **Horizontal Verify/Vertical Verify**, následně pro výpočet délky linie klikněte na tlačítko **Calibrate**. Porovnáním vypočítané délky linie a skutečné délky ověřte nastavené kalibrační údaje.
- 5) Vykreslené linie můžete odstranit kliknutím na tlačítko **Delete**.
- 6) Kliknutím na tlačítko **Save** uložte nastavení.

Poznámka: Pokud dojde k zastavení živého zobrazení, není kalibrace kamery platná.

Obrázek 5–50 Zadání základních dat



Obrázek 5–51 Kreslení v okně živého zobrazení

3. Vykreslete **region stínění**

Funkce regionu stínění umožňuje nastavit konkrétní region, pro který se nebude analýza chování provádět. Jsou podporovány až 4 regiony stínění.

Kroky:

1) Vstupte do rozhraní nastavení regionu stínění:

Configuration > VCA Configuration > Shield Region

2) Klikněte na možnost **Draw Area**. Nakreslete oblast – kliknutím levým tlačítkem myši nakreslete v okně živého zobrazení koncové body. Kliknutím pravým tlačítkem myši kreslení oblasti dokončete.

Poznámky:

- Podporována je mnohoúhelníková oblast až o 10 stranách.
- Vykreslené linie odstraní kliknutím na tlačítko **Delete**.
- Pokud dojde k zastavení živého zobrazení, nelze regiony stínění žádným způsobem nakreslit.



3) Kliknutím na tlačítko **Save** uložte nastavení.

4. Nakonfigurujte **Pravidlo**

Analýza chování podporuje sérii chování, včetně překročení linie, narušení, vstupu do oblasti, výstupu z oblasti atd.

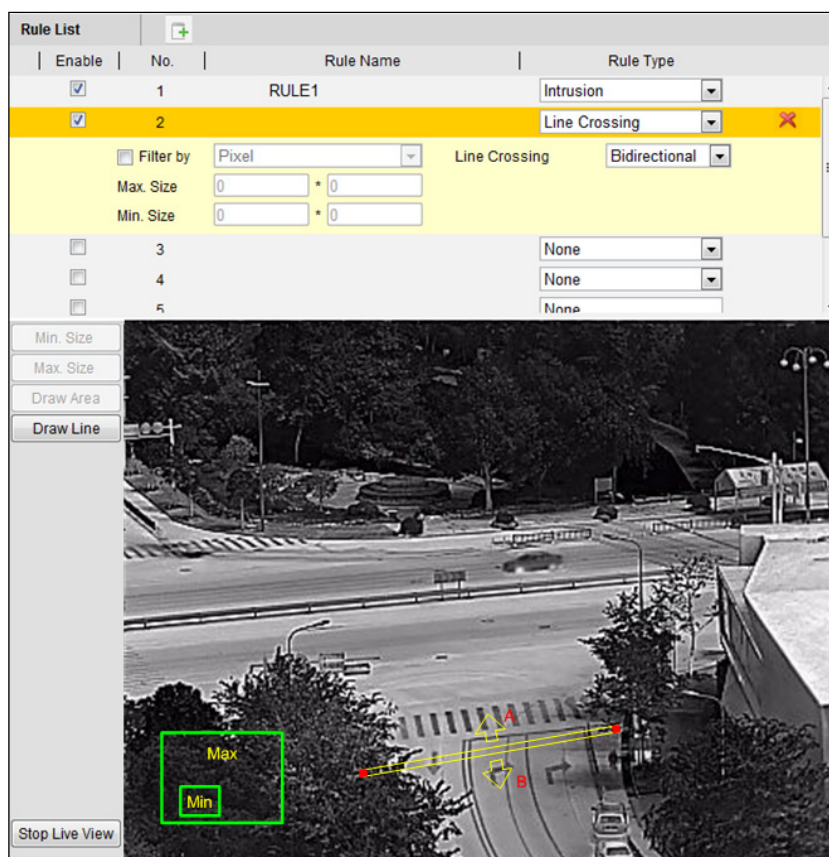
Poznámka: Typ pravidla pro nastavení se liší v závislosti na různých kamerách.

Kroky:

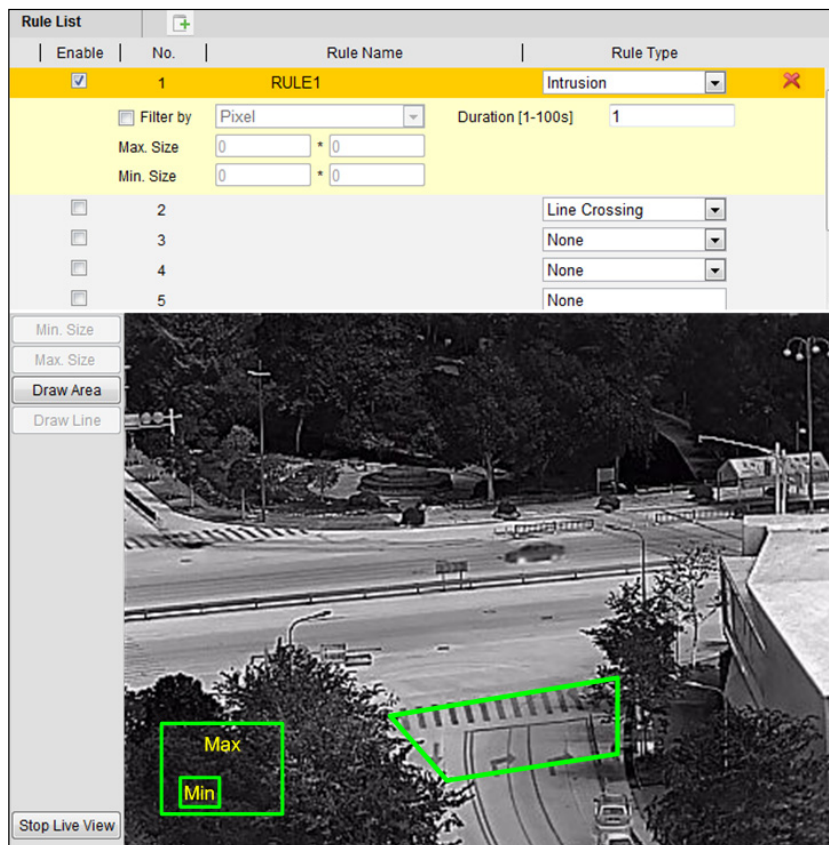
- 1) Klikněte na kartu **Rule**, a přejděte tak do okna konfigurace pravidel.
- 2) Nové pravidlo přidejte kliknutím na . (Volitelné) Odstraňte je kliknutím na .
- 3) Pro povolení pravidla analýzy chování zaškrtněte políčko požadovaného pravidla.
- 4) Vyberte typ pravidla, nastavte typ filtru a poté v živém videu nakreslete pro jednotlivá pravidla linii nebo oblast.
 - **Line Crossing** detekuje osoby, vozidla nebo jiné objekty, které překročí předem definovanou virtuální linii, při spuštění alarmu mohou být podniknuty určité kroky.

Při výběru tohoto typu pravidla musíte před vykreslením linie vybrat směr překročení. Volitelné možnosti jsou Obousměrný, A do B a B do A.
 - **Intrusion** detekuje osoby, vozidla nebo jiné objekty, které vstoupí a zdržují se v předem definované virtuální oblasti, při spuštění alarmu mohou být podniknuty určité kroky.

Při výběru tohoto typu pravidla musíte nastavit dobu trvání narušení. Dostupná doba trvání je od 1 do 100 sekund.

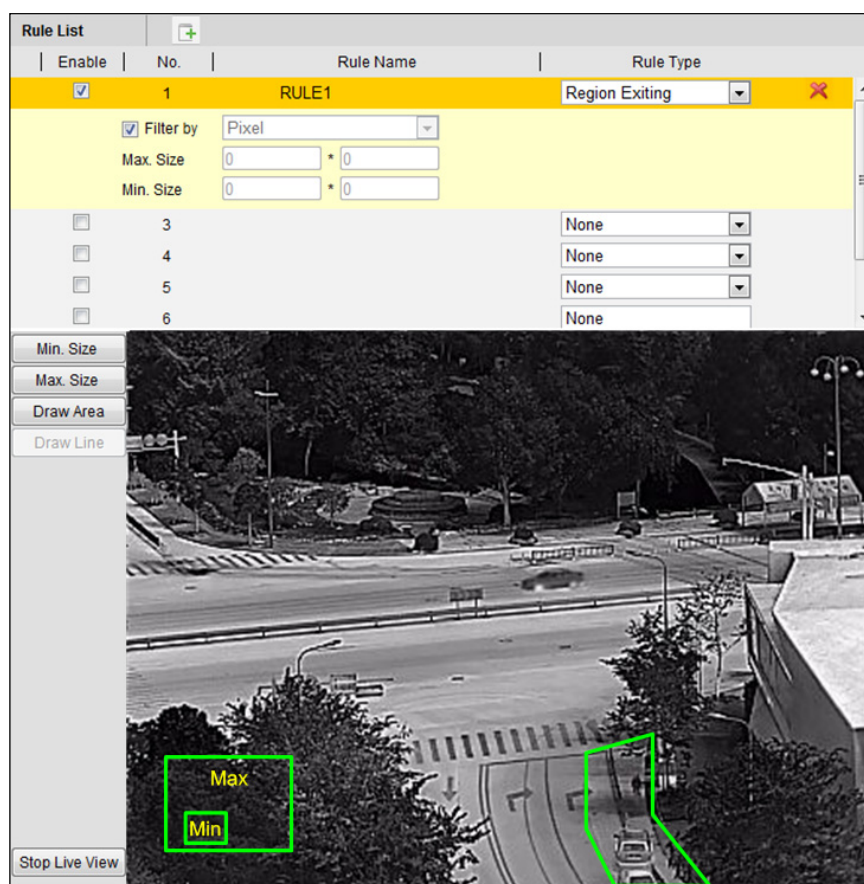


Obrázek 5–52 Typ pravidla – Překročení linie



Obrázek 5–53 Typ pravidla – Narušení

- **Region Entrance** detekuje osoby, vozidla nebo jiné objekty, které do předem definované virtuální oblasti vstoupí zvenčí, při spuštění alarmu mohou být podniknuty určité kroky.
- **Region Exiting** detekuje osoby, vozidla nebo jiné objekty, které opouští předem definovanou virtuální oblast, při spuštění alarmu mohou být podniknuty určité kroky.



Obrázek 5–54 Typ pravidla – opuštění oblasti

- **Filter type:** Volitelné možnosti jsou Pixels a Actual Size. Je-li vybrána možnost Pixels, vykreslete pro každé pravidlo na živém videu oblast maximální a minimální velikosti. Pokud je vybrána možnost Actual Size, zadejte délku a šířku maximální a minimální velikosti. Alarm spustí pouze ty cíle, jejichž velikost je mezi minimální a maximální hodnotou.
Poznámka: Pokud je vybrána skutečná velikost, zkontrolujte, zda je nakonfigurována kalibrace kamery.
- **Draw line/area:** Pro ostatní události, jako je narušení, vstup do oblasti, opuštění oblasti atd. musíte kliknutím levého tlačítka myši na živé video nastavit koncové body oblasti, kliknutím pravým tlačítkem myši na oblast vykreslování dokončíte.

Poznámka: Pokud dojde k zastavení živého zobrazení, nelze oblast nebo linii detekce nakreslit a nastavit pravidla.

- 5) Zaškrtnutím zaškrťovacího políčka kombinovaného pravidla povolíte pravidlo pro analýzu chování.
- 6) Jako pravidlo A a pravidlo B kombinovaného pravidla vyberte dvě jednotlivá nakonfigurovaná pravidla. Nastavte pro tato dvě jednotlivá pravidla minimální a maximální časový interval. Poté vyberte pro filtrování alarmů pořadí spuštění jednotlivých pravidel.

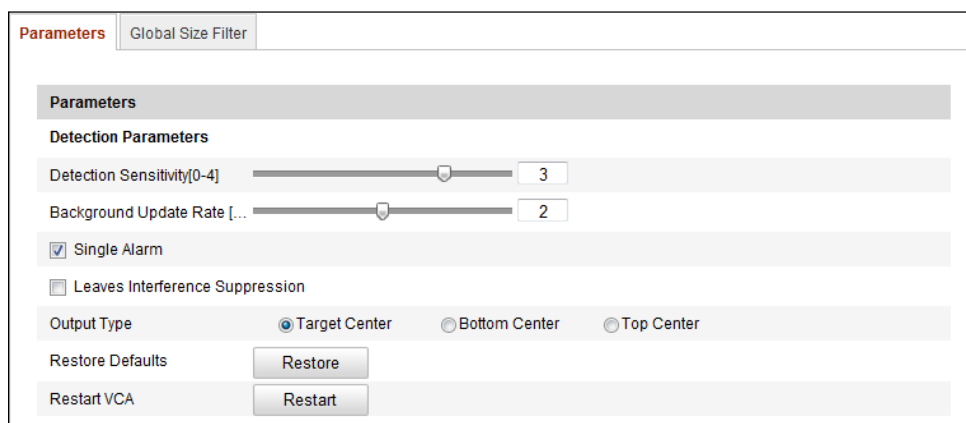
Poznámky:

- Pokud v nabídce Rule Type vyberete možnost None, nebude pravidlo platné a nebude možné nakonfigurovat analýzu chování.
 - Pořadí aktivace samostatných pravidel pro filtrování alarmů lze nastavit ve vzestupném nebo vzestupném/sestupném pořadí.
 - Nakonfigurovat lze až 8 jednotlivých pravidel a 2 kombinovaná pravidla. Pro kombinovaná pravidla je podporováno překročení linie, narušení, vystupování z oblasti a vstupování do oblasti.
- 7) Kliknutím na tlačítko **Save** uložíte nastavení.
 - 8) Klikněte na kartu **Arming Schedule**, pro nastavení časového plánu pro každé pravidlo klikněte na možnost **Edit**, nastavení uložíte kliknutím na tlačítko **Save**.
 - 9) Klikněte na kartu **Alarm Linkage**, zaškrtněte políčko odpovídajících metody propojení pro každé pravidlo, nastavení uložíte kliknutím na tlačítko **Save**.

5. Nastavení **Rozšířené konfigurace**

- **Parametr**

Nakonfigurováním následujících parametrů nastavte podrobnější konfiguraci.



Obrázek 5–55 Pokročilá konfigurace

Detection Sensitivity [0–4]: Vztahuje se k citlivosti kamery při rozpoznávání cíle. Čím vyšší je hodnota, tím snadněji dojde k rozpoznání cíle a tím více je obsaženo mylných informací. Jako výchozí je doporučena hodnota 3.

Background Update Rate [0–4]: Vztahuje se k rychlosti, s jakou nová scéna nahrazuje předchozí scénu. Jako výchozí je doporučena hodnota 2.

Single Alarm: Je-li zvolena možnost jednotlivého alarmu, spustí cíl v nakonfigurované oblasti alarm pouze jednou. Pokud není tato možnost zaškrtnuta, bude stejný cíl ve stejné nakonfigurované oblasti spouštět nepřetržitý alarm.

Leave Interference Suppression: Zaškrtnutím tohoto zaškrťovacího políčka zastavíte v nakonfigurované oblasti rušení způsobené listy.

Output Type: Zvolte umístění rámečku. Volitelné možnosti jsou střed cíle, dole uprostřed a nahoře uprostřed. Např.: Je-li vybrán střed cíle, bude cíl uprostřed snímku.

Restore Default: Kliknutím obnovíte nastavení nakonfigurovaných parametrů na výchozí hodnoty.

Restart VCA: Slouží k restartování knihovny algoritmů analýzy chování.

- Filtr celkové velikosti

Poznámka: Oproti velikosti filtru podle pravidla, které je zaměřeno na každé pravidlo, je filtr celkové velikosti zaměřen na všechna pravidla.

Kroky:

- 1) Zaškrtnutím zaškrťovacího políčka **Global Size Filter** tuto funkci povolte.
- 2) Filter Type vyberte jako Actual Size nebo Pixel.

Actual Size: Zadejte délku a šířku jako pro maximální, tak pro minimální velikost. Alarm spustí pouze ty cíle, jejichž velikost je mezi minimální a maximální hodnotou.

Poznámky:

- Pokud vyberete možnost filtru dle skutečné velikosti, je nutné nakonfigurovat kalibraci kamery.

- Délka u maximální velikosti musí být větší než délka u minimální velikosti. Stejné pravidlo platí pro šířku.

Pixel: Pro vykreslení čtyřúhelníku o minimální velikosti v živém zobrazení klikněte na možnost Minimální velikost. Pro vykreslení čtyřúhelníku o maximální velikosti v živém zobrazení klikněte na možnost Maximální velikost. Cíle menší, než je minimální velikost, nebo větší, než je maximální velikost, budou vyfiltrovány.

Poznámky:

- Algoritmus na pozadí převede nakreslenou oblast na pixely.
 - Pokud dojde k zastavení živého zobrazení, nelze filtr celkové velikosti nakonfigurovat.
 - Délka u maximální velikosti musí být větší než délka u minimální velikosti. Stejné pravidlo platí pro šířku.
- 3) Nastavení uložíte kliknutím na tlačítko **Save**.

Kapitola 6 Nastavení úložiště

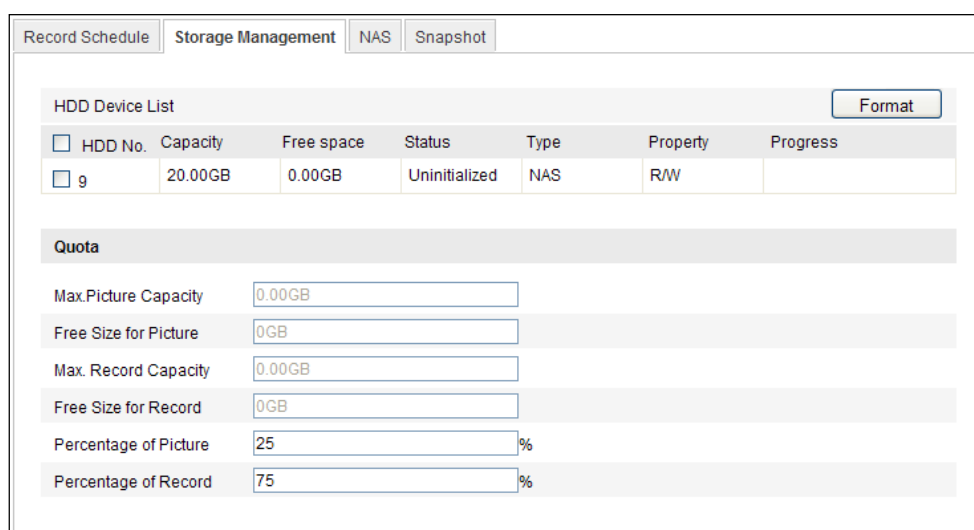
Než začnete:

Pro konfiguraci nastavení záznamů se ujistěte, zda máte síťové paměťové zařízení v rámci sítě, nebo zda je v kameře vložena karta SD.

6.1 Správa úložiště

Správa úložiště vám umožňuje zobrazit stav HDD, včetně kapacity, volného místa, stavu, typu, pokroku atd. V případě potřeby můžete pevný disk také formátovat. Kromě toho můžete přiřadit kvóty pro snímky a soubory záznamů.

Poznámka: Předtím, než budete moci zařízení HDD spravovat, musí být napřed přidána. Vložte kartu SD nebo podle následující části přidejte zařízení HDD.



Obrázek 6–1 Rozhraní správy úložiště

6.2 Konfigurace nastavení NAS

Než začnete:

Síťový disk by měl být k dispozici v dané síti a být řádně nakonfigurován pro ukládání nahraných souborů, souborů protokolu atd.

Kroky:

1. Přidání síťového disku

(1) Otevřete rozhraní pro nastavení NAS (Network-Attached Storage):

Configuration > Advanced Configuration > Storage > NAS

HDD No.	Type	Server Address	File Path
1	NAS	172.6.21.99	/dvr/test01
Mounting Type: <input type="text" value="NFS"/> User Name: <input type="text"/> Password: <input type="text"/>			
2	NAS		
3	NAS		
4	NAS		
5	NAS		
6	NAS		
7	NAS		
8	NAS		

Obrázek 6–2 Přidání síťového disku

- (2) Zadejte IP adresu síťového disku a cestu souboru.
- (3) Vyberte typ připojení. Lze vybrat možnosti NFS a SMB/CIFS. Pokud je vybrána možnost SMB/CIFS, lze k zajištění zabezpečení nastavit uživatelské jméno a heslo.

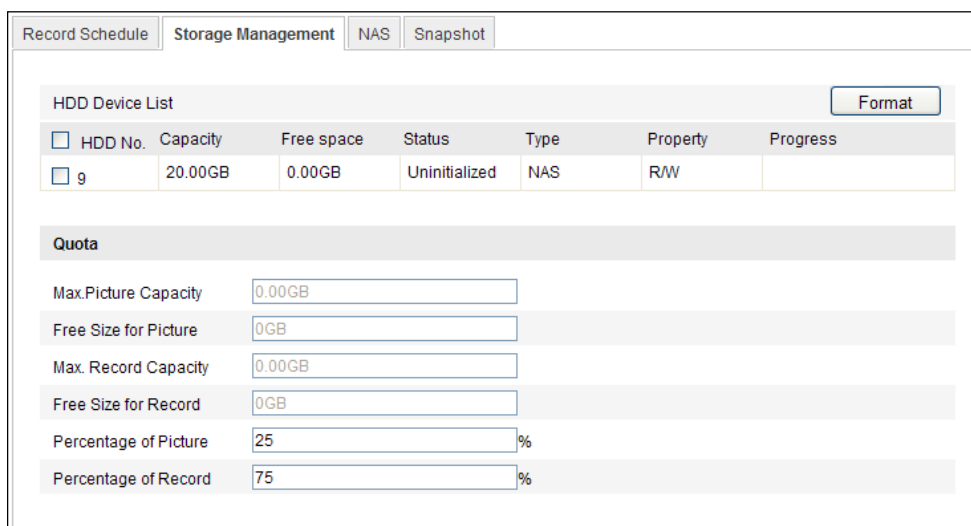
Poznámka: Pro vytvoření souboru cesty se řiďte pokyny v *Uživatelské příručce NAS*.



- *Kvůli vašim osobním údajům a lepší ochraně před bezpečnostními riziky důrazně doporučujeme použít silná hesla pro všechny funkce a síťová zařízení. Pro zvýšení zabezpečení vašeho produktu by heslo mělo být takové, které jste vybrali sami (s použitím minimálně 8 znaků, včetně velkých a malých písmen, čísel a zvláštních znaků).*
- *Zodpovědnost za správnou konfiguraci všech hesel a ostatních bezpečnostních opatření nese montážní pracovník nebo konečný uživatel.*

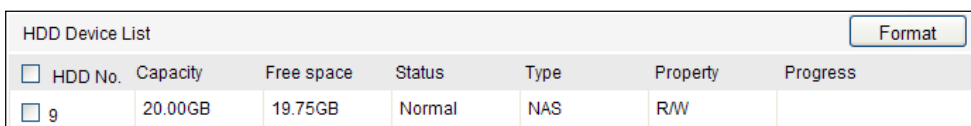
- (4) Kliknutím na tlačítko **Save** přidejte síťový disk.
2. Inicializujte přidaný síťový disk.
 - (1) Vstupte do rozhraní nastavení HDD

Rozšířené konfigurace > Úložiště > Správa úložiště



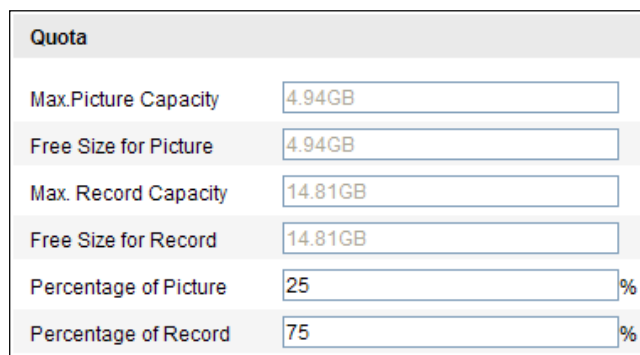
Obrázek 6–3 Rozhraní správy úložiště

- (2) Pokud je stav disku **Uninitialized**, zaškrtnutím odpovídajícího políčka vyberte disk a kliknutím na tlačítko **Format** a provedte inicializaci disku. Po dokončení inicializace bude stav disku **Normal**.



Obrázek 6–4 Zobrazení stavu disku

3. Pro záznamy a snímky definujte kvótu.
- (1) Zadejte procentní kvótu pro obrázky a záznam.
- (2) Kliknutím na tlačítko **Save** aktualizujete stránku v prohlížeči a aktivujete nastavení.



Obrázek 6–5 Nastavení kvóty

Poznámky:

- Ke kameře lze připojit až osm disků NAS.
- Pro inicializaci a použití karty SD po vložení do kamery postupujte podle kroků inicializace disku NAS.

6.3 Konfigurace harmonogramu nahrávání

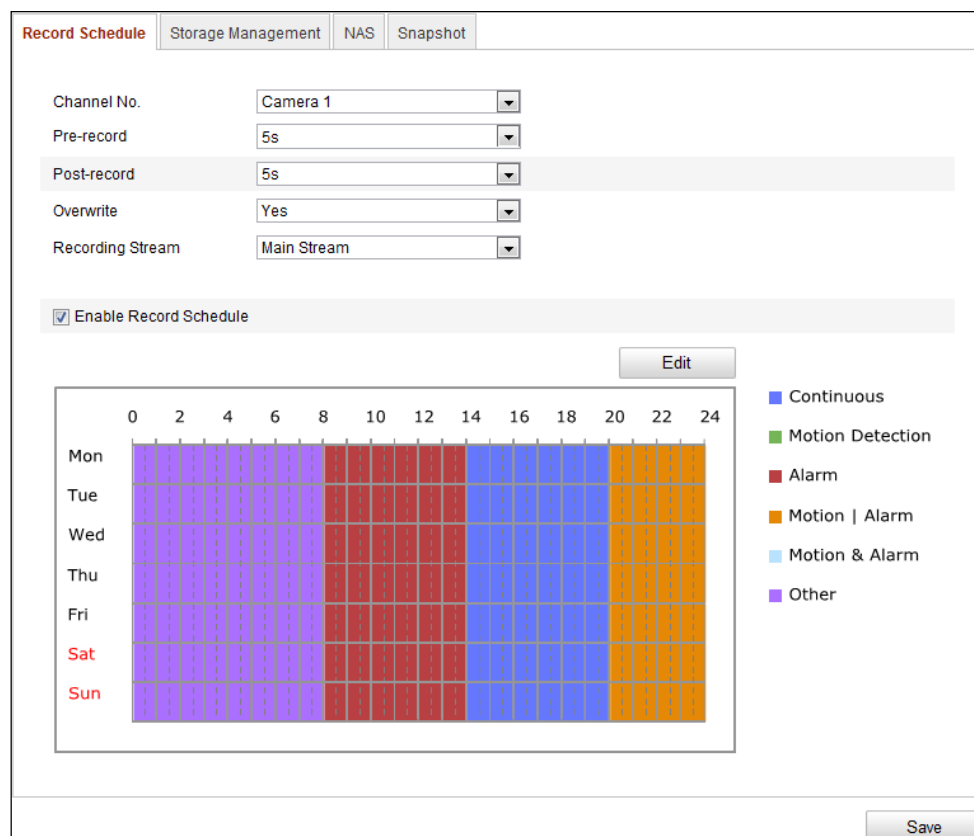
Účel:

K dispozici jsou dva způsoby nahrávání kamer: ruční nahrávání a plánované nahrávání. Informace o ručním nahrávání naleznete v *Části 4.3 Ruční nahrávání a zachycování snímků*. V této části můžete postupovat podle pokynů pro konfiguraci plánovaného nahrávání. Ve výchozím nastavení jsou zaznamenané soubory plánovaného nahrávání ukládány na kartu SD (je-li podporována) nebo na síťový disk.

Kroky:

1. Otevřete rozhraní pro nastavení harmonogramu nahrávání:

Configuration > Advanced Configuration > Storage > Record Schedule



Obrázek 6–6 Okno plánu nahrávání

2. Pro povolení plánovaného nahrávání zaškrtněte políčko **Enable Record Schedule**.
3. Nastavte parametry nahrávání kamery.

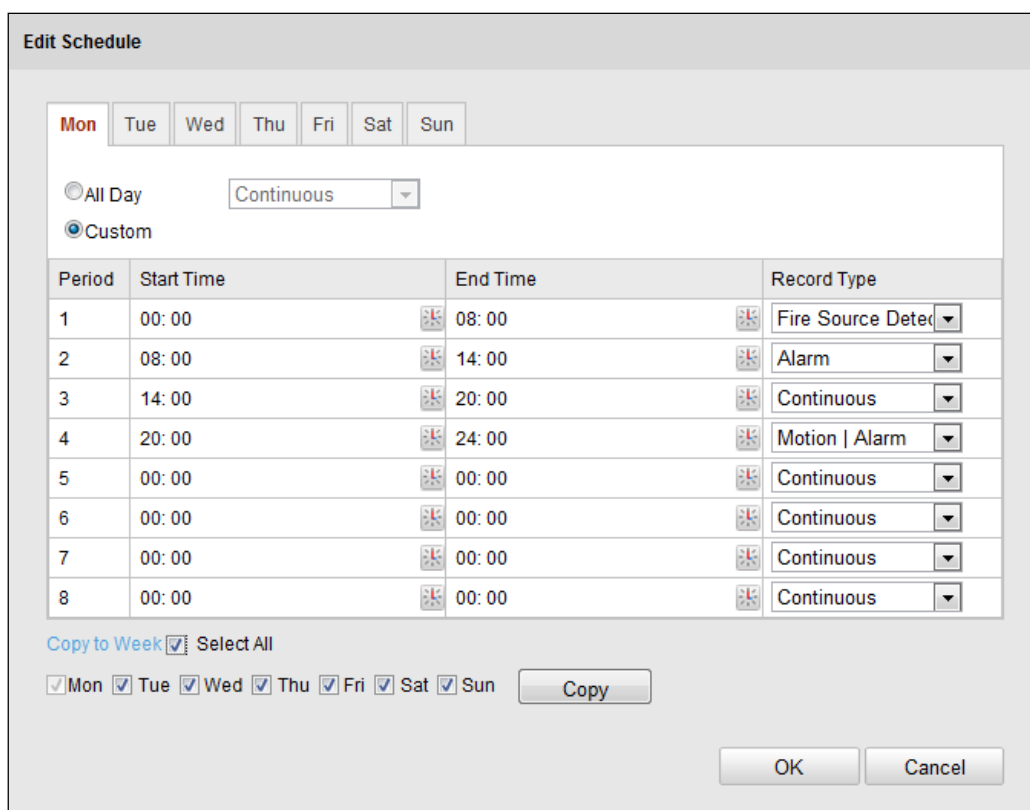
Pre-record	5s
Post-record	5s
Overwrite	Yes
Recording Stream	Main Stream

Obrázek 6–7 Parametry nahrávání

- **Pre-record:** Čas, který nastavíte pro zahájení nahrávání před naplánovaným časem nebo událostí. Pokud například alarm spustí nahrávání v 10:00 a nastavili jste dobu před nahráváním na 5 sekund, začne kamera nahrávat v 9:59:55.
Čas před záznamem je možno nakonfigurovat jako Bez času před záznamem, 5 s, 10 s, 15 s, 20 s, 25 s, 30 s nebo bez omezení.
- **Post-record:** Čas, který nastavíte pro zastavení nahrávání po naplánovaném čase nebo události. Pokud například alarm skončí nahrávání v 11:00 a nastavili jste dobu po nahrávání na 5 sekund, bude kamera nahrávat do 11:00:05.
Čas po záznamu může být nakonfigurován jako 5 s, 10 s, 30 s, 1 min, 2 min, 5 min nebo 10 min.
- **Recording Stream:** Volitelné možnosti jsou Hlavní stream a Dílčí stream. Hlavní stream se obvykle používá pro záznam a živé sledování s dobrou šířku pásma, dílčí a třetí stream je možno použít pro živé sledování při omezené šířce pásma.

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

4. Pro úpravu plánu nahrávání klikněte na možnost **Edit**.



Obrázek 6–8 Upravit plán nahrávání

5. Vyberte den pro nastavení plánu nahrávání.

(1) Nastavte celodenní nahrávání nebo segmentové nahrávání:

- Chcete-li nakonfigurovat celodenní nahrávání, zaškrtněte políčko **All Day**.
- Pro nastavení nahrávání v různých časových obdobích zaškrtněte políčko **Custom**. Nastavte **Start Time** a **End Time**.

Poznámka: Časy segmentů se nemohou překrývat. Nakonfigurovat je možno až 8 segmentů.

(2) Vyberte **Typ záznamu**.

Typ záznamu může být Kontinuální, Detekce pohybu, Alarm, Pohyb | Alarm, Pohyb a alarm, Detekce výjimky zvuku, Nahrávání VCA, Detekce zdroje požáru a Všechny události.

- **Nepřetržité**

Pokud vyberete možnost **Continuous**, video se automaticky nahraje podle naplánovaného času.

- **Nahrávání aktivované pomocí Motion Detection**

Pokud vyberete možnost **Motion Detection**, video bude nahrávat, bude-li detekován pohyb.

Kromě konfigurace harmonogramu nahrávání je nutné nastavit oblast detekce pohybu a zaškrtnout políčko **Trigger Channel** v **Linkage Method** rozhraní Nastavení detekce pohybu. Podrobné informace viz *Úloha 1: Nastavení oblasti detekce pohybu* v *Části 5.6.1*.

- **Nahrávání aktivované přes Alarm**

Pokud vyberete možnost **Alarm**, video bude po spuštění alarmu nahrávat prostřednictvím externích kanálů vstupu alarmu.

Kromě konfigurace plánu nahrávání musíte nastavit **Typ alarmu** a v nabídce **Linkage Method** rozhraní **Nastavení vstupu alarmu** zaškrtnout políčko **Trigger Channel**. Podrobné informace naleznete v *Části 5.6.3*.

- **Nahrávání aktivované pomocí Motion & Alarm**

Zvolíte-li možnost **Motion & Alarm**, video bude nahráváno při pohybu a současné aktivaci alarmu.

Kromě konfigurace harmonogramu nahrávání je nutné nakonfigurovat také nastavení rozhraní **Detekce pohybu** a **Nastavení vstupu alarmu**. Podrobné informace naleznete v *Části 5.6.1* a v *Části 5.6.3*.

- **Nahrávání aktivované pomocí Motion | Alarm**

Zvolíte-li možnost **Motion | Alarm**, video bude nahráváno při aktivaci externího alarmu nebo při zjištění pohybu.

Kromě konfigurace harmonogramu nahrávání je nutné nakonfigurovat také nastavení rozhraní **Detekce pohybu** a **Nastavení vstupu alarmu**. Podrobné informace naleznete v *Části 5.6.1* a v *Části 5.6.3*.

- **Záznam spuštěný detekcí výjimky zvuku**

Pokud vyberete **Audio Exception Detection**, video bude nahrávat, budou-li na místě sledování detekovány abnormální zvuky, například náhlé zvýšení/snížení intenzity zvuku.

Kromě konfigurace harmonogramu nahrávání je nutné nakonfigurovat také nastavení rozhraní **Detekce výjimky zvuku**. Podrobné informace naleznete v *Části 5.6.6*.

- **Nahrávání, spuštěné nahráváním VCA**

Pokud vyberete **VCA Recording**, video bude nahrávat, když VCA detekuje sérii podezřelých chování, například překročení linie, narušení, vstup do oblasti a odchod z oblasti.

Kromě konfigurace plánu nahrávání musíte v rozhraní konfigurace VCA nakonfigurovat nastavení pravidla. Podrobné informace naleznete v *Části 5.7.2*.

- **Záznam spuštěný detekcí zdroje požáru**

Pokud vyberete možnost **Fire Source Detection**, video bude nahrávat, bude-li detekován zdroj požáru.

Kromě konfigurace plánu nahrávání musíte v rozhraní **Dynamic Fire Source Detection** nakonfigurovat nastavení. Podrobné informace naleznete v *Části 5.7.6*.

- **Záznam spuštěný všemi událostmi**

Při výběru možnosti **All Events** bude video nahrávat, kdykoli nastane kterákoli z výše uvedených událostí.

Kromě konfigurace plánu nahrávání musíte nastavení konfigurovat v rozhraní odpovídajících událostí.

- (3) (Volitelné) Zaškrtněte políčko **Select All** a klikněte na tlačítko **Copy** pro kopírování nastavení tohoto dne na celý týden. Můžete také zaškrtnout políčka před datem a kliknout na tlačítko **Copy**.
- (4) Pro uložení nastavení a ukončení rozhraní **Edit Record Schedule** klikněte na tlačítko **OK**.

6. Kliknutím na tlačítko **Save** uložte nastavení.

6.4 Konfigurace nastavení snímku

Účel:

Můžete konfigurovat naplánovaný snímek a snímek aktivovaný určitou událostí. Zachycený snímek může být uložen na kartě SD (je-li podporována) nebo v NAS (podrobné informace naleznete v *Části 6.2 Konfigurace nastavení NAS*). Pořízené snímky můžete také nahrát na server FTP.

Základní nastavení

Kroky:

1. Otevřete rozhraní pro nastavení snímků:

Configuration > Advanced Configuration > Storage > Snapshot

Record Schedule | Storage Management | NAS | **Snapshot**

Timing

Enable Timing Snapshot

Format: JPEG

Resolution: 640*512

Quality: High

Interval: 0 millisecond

Edit

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

Event-Triggered

Enable Event-Triggered Snapshot

Format: JPEG

Resolution: 640*512

Quality: High

Interval: 0 millisecond

Capture Number: 4

Obrázek 6–9 Rozhraní nastavení snímku

2. Vyberte číslo kanálu. U modelů kamer s více než jedním kanálem kamery nejprve vyberete číslo kanálu pro konfiguraci.
3. Zaškrtnutím zaškrtačacího políčka **Enable Timing Snapshot** povolte nepřetržité zachycování snímků.
Upravte naplánovaný čas pro snímky. Podrobné informace týkající se nastavení naleznete v *Části 6.3 Konfigurace harmonogramu nahrávání*.
4. Zaškrtnutím políčka **Enable Event-triggered Snapshot** povolíte snímek aktivovaný událostí.
5. Vyberte formát, rozlišení a kvalitu snímku.
6. Nastavte časový interval mezi dvěma snímky.
7. Kliknutím na tlačítko **Save** uložte nastavení.

Nahrávání na FTP

Postupem podle následujících pokynů můžete nahrávat na server FTP.

- Nahrávání nepřetržitých snímků na FTP

Kroky:

- 1) Nakonfigurujte nastavení FTP a zaškrtněte políčko **Upload Picture** v rozhraní pro nastavení FTP. Podrobné informace o konfiguraci parametrů FTP naleznete v *Části 5.3.11 Konfigurace nastavení FTP*.
- 2) Zaškrtněte políčko **Enable Timing Snapshot**.

- Nahrávání snímků aktivovaných na základě události na FTP

Kroky:

- 1) Nakonfigurujte nastavení FTP a zaškrtněte políčko **Upload Picture** v rozhraní pro nastavení FTP. Podrobné informace o konfiguraci parametrů FTP naleznete v *Části 5.3.11 Konfigurace nastavení FTP*.
- 2) V rozhraní nastavení detekce pohybu nebo vstupu alarmu zaškrtněte políčko **Upload Picture**. Viz *Úloha 3: Nastavení plánu akcí podniknutých při detekci pohybu* v *Části 5.6.1*.
- 3) Zaškrtněte políčko **Enable Event-triggered Snapshot**.

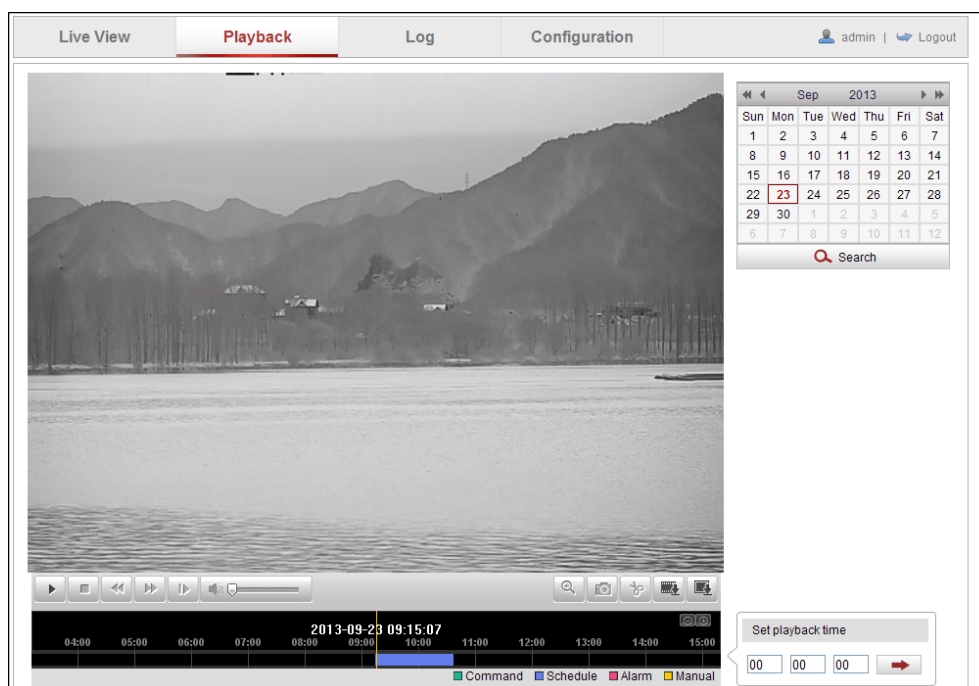
Kapitola 7 Přehrávání

Účel:

V této části je vysvětleno, jak vzdáleně zobrazit nahrané videosoubory uložené na síťových discích nebo kartách SD.

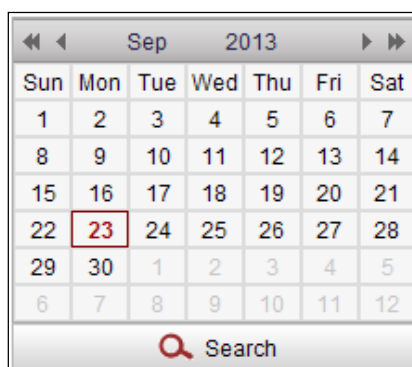
Kroky:

1. Klikněte v řádku nabídek na možnost **Playback**, a přejděte tak do okna přehrávání.




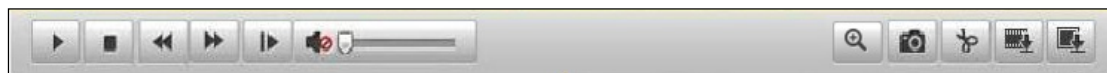
Obrázek 7–1 Rozhraní pro přehrávání

2. Vyberte datum a pro vyhledávání souborů záznamů klikněte na tlačítko **Search**.



Obrázek 7–2 Prohledávání videa

3. Kliknutím na  přehrávejte video soubory nalezené k tomuto datu. Panel nástrojů v dolní části rozhraní pro přehrávání lze použít k ovládání přehrávání.



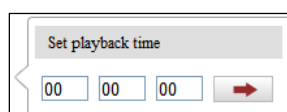
Obrázek 7-3 Panel nástrojů pro přehrávání

Tabulka 7-1 Popis tlačítek

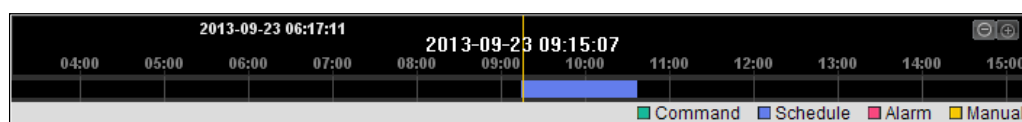
Ikona	Popis	Ikona	Popis
	Přehrávání		Zachytit obrázek
	Pozastavit		Spustit/zastavit ořez video souborů
	Zastavení		Zapnout zvuk a upravit hlasitost/ztlumením
	Zpomalit		Stahování videosouborů
	Zrychlit		Stahování zachycených snímků
	Přehrávat po snímku		Povolit/zakázat digitální zoom

Poznámka: U stažených videosouborů pro přehrávání můžete vybrat místní cestu k video souborům a obrázkům v rozhraní místní konfigurace. Podrobnosti naleznete v *Části 5.1*.

4. Přetáhněte ukazatel průběhu myši pro vyhledání přesného místa pro přehrávání. Můžete také zadat čas a kliknutím na tlačítko vyhledat místo přehrávání v poli **Set playback time**. Můžete také kliknout na pro oddálení/přiblížení ukazatele průběhu.

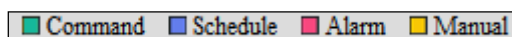


Obrázek 7-4 Nastavení času přehrávání



Obrázek 7-5 Ukazatel průběhu

Různé barvy videa na indikátoru průběhu značí různé typy videí.



Obrázek 7-6 Typy videa

Kapitola 8 Vyhledávání v protokolu

Účel:

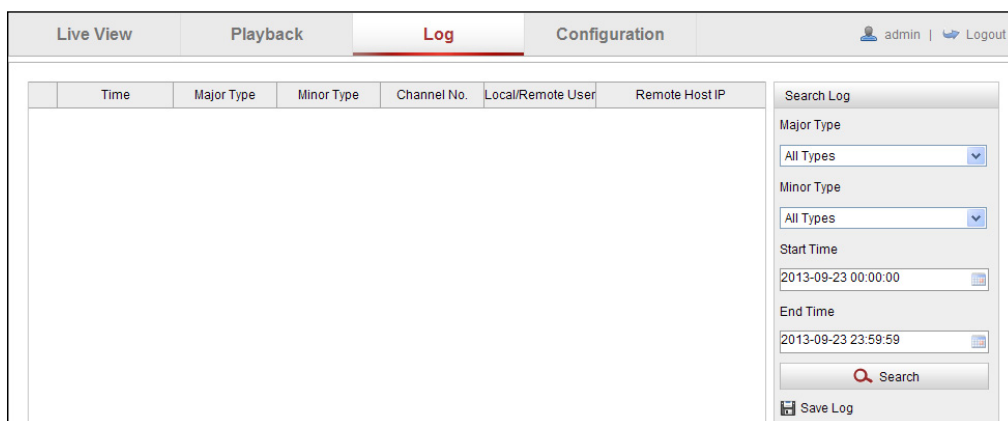
Informace o chodu, alarmech, výjimkách a informace o kameře lze ukládat do souborů protokolů. Soubory protokolu můžete také podle potřeby exportovat.

Než začnete:

Zkontrolujte, zda je síťové úložiště pro kameru nakonfigurováno, nebo zda funguje místní úložiště (karta SD).

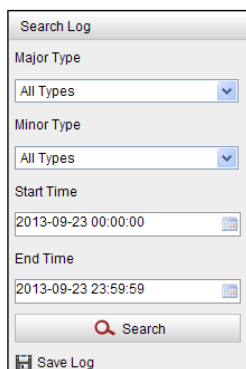
Kroky:

1. Pro vstup protokolu hledání rozhraní klikněte na tlačítko **Log** v panelu nabídek.



Obrázek 8–1 Rozhraní vyhledávání v protokolu

2. Upřesněte své vyhledávání nastavením podmínek vyhledávání, včetně hlavního typu, vedlejšího typu, počátečního času a koncového času.
3. Kliknutím na tlačítko **Search** spustíte vyhledávání souborů protokolů. V rozhraní **Log** se zobrazí odpovídající soubory protokolu.



Obrázek 8–2 Vyhledávání v protokolu

4. Chcete-li exportovat soubory protokolu, klikněte na tlačítko **Save log** a uložte soubory protokolů do počítače.

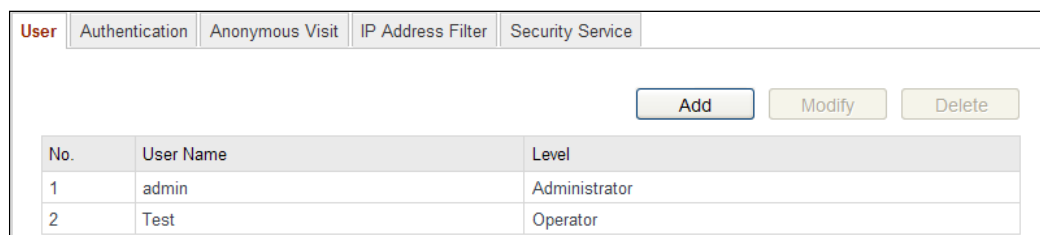
Kapitola 9 Jiné

9.1 Správa uživatelských účtů

Účel:

Uživatel s rolí správce může přidávat, odstraňovat nebo upravovat uživatelské účty a udělovat jim různá oprávnění. Uživateli důrazně doporučujeme náležité spravování účtů zařízení a uživatelských oprávnění.

Pro dokončení nastavení vstupte do rozhraní pro správu uživatelů: **Configuration > Basic Configuration > Security > User** nebo **Configuration > Advanced Configuration > Security > User**



No.	User Name	Level
1	admin	Administrator
2	Test	Operator

Obrázek 9–1 Informace o uživateli

- **Přidání uživatele**

Uživatel *správce* má ve výchozím nastavení všechna oprávnění pro vytváření, úpravu a odstraňování jiných účtů.

Poznámka: Účet uživatele s rolí *správce* nelze odstranit a lze pouze změnit heslo *správce*.

Kroky:

1. Kliknutím na tlačítko **Add** přidejte uživatele.
2. Zadejte **Uživatelské jméno**, vyberte **Level** a zadejte **heslo**.

Poznámky:

- Lze vytvořit až 31 uživatelských účtů.
- Různé úrovně uživatelů mají různá oprávnění. Lze zvolit úroveň Operator nebo User.



- *K lepší ochraně soukromí a ochraně systému proti bezpečnostním rizikům důrazně doporučujeme používat ke všem funkcím a síťovým zařízením silná hesla. Pro zvýšení zabezpečení vašeho produktu by heslo mělo být takové, které jste vybrali sami (s použitím minimálně 8 znaků, včetně velkých a malých písmen, čísel a zvláštních znaků).*
 - *Za správnou konfiguraci všech hesel a dalších nastavení zabezpečení zodpovídá osoba provádějící instalaci nebo koncový uživatel.*
3. V poli **Basic Permission** a **Camera Configuration** můžete zkontrolovat nebo zrušit oprávnění pro nového uživatele.
 4. Kliknutím na tlačítko **OK** přidání uživatele dokončete.

Obrázek 9–2 Přidání uživatele

- **Úprava uživatele**

Kroky:

1. Uživatele ze seznamu vyberte levým tlačítkem myši a klikněte na tlačítko **Modify**.

2. Upravte **User Name**, **Level** nebo **Password**.
3. V poli **Basic Permission** a **Camera Configuration** můžete zaškrtnout nebo zrušit zaškrtnutí daných oprávnění.
4. Kliknutím na tlačítko **OK** úpravu uživatele dokončete.

Obrázek 9–3 Úprava uživatele

- **Odstranění uživatele**

Kroky:

1. Kliknutím vyberte uživatele, jehož chcete odstranit a klikněte na možnost **Delete**.
2. Pro odstranění uživatele klikněte na tlačítko **OK** v místním dialogovém okně.

9.2 Ověřování

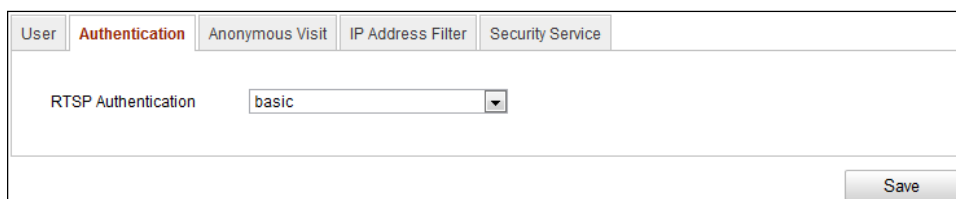
Účel:

Data streamu živého zobrazení lze specificky zabezpečit.

Kroky:

1. Vstupte do rozhraní Authentication:

Configuration > Advanced Configuration > Security > Authentication



Obrázek 9–4 Ověřování pomocí protokolu RTSP

2. V rozevíracím seznamu u možnosti **RTSP Authentication** vyberte typ **basic** nebo **disable**, a povolte tak nebo zakažte ověřování pomocí protokolu RTSP.

Poznámka: Pokud ověřování pomocí protokolu RTSP zakážete, může k videostreamu získat prostřednictvím protokolu RTSP přístup kdokoli.

3. Kliknutím na tlačítko **Save** uložte nastavení.

9.3 Anonymní návštěva

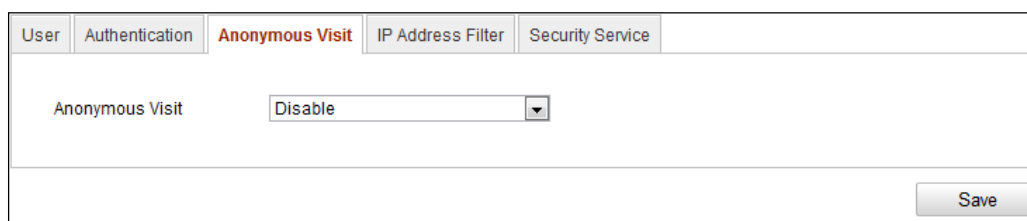
Povolení této funkce umožňuje návštěvy návštěvníků, kteří nemají uživatelské jméno nebo heslo k zařízení.

Poznámka: Pro anonymní uživatele je dostupné jen živé zobrazení.

Kroky:

1. Vstupte do rozhraní **Anonymous Visit**:

Configuration > Advanced Configuration > Security > Anonymous Visit



Obrázek 9–5 Anonymní návštěva

2. Pro povolení nebo zakázání anonymních návštěv nastavte oprávnění pro **Anonymous Visit** v rozevíracím seznamu na **Enable** nebo **Disable**.
3. Kliknutím na tlačítko **Save** uložte nastavení.

Při příštím přihlášení uvidíte zaškrtačací políčko **Anonymní**.

The image 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 checkbox labeled "Anonymus" which is currently unchecked.

Obrázek 9–6 Rozhraní pro přihlášení se zaškrtnávacím políčkem Anonymus.

4. Zaškrtněte políčko **Anonymus** a klikněte na tlačítko **Login**.

Povolením anonymní funkce „Živé zobrazení“ můžete ostatním povolit přístup ke své kameře a zobrazovat živé obrazy bez zadání přihlašovacích údajů. Při povolení anonymní funkce „živého zobrazení“ je proto velmi důležité, abyste zajistili, že zorné pole kamery nebude mít vliv na soukromí osob, jejichž obraz by mohl být zachycen bez oprávnění.

Vzhledem k vlastnímu narušení soukromí je video sledování nevhodné v oblastech, kde lidé více očekávají soukromí.

9.4 Filtr adres IP

Účel:

Tato funkce umožňuje řízení přístupu.

Kroky:

1. Přejděte do okna filtru adres IP:

Configuration > Advanced Configuration > Security > IP Address Filter

The image shows the configuration window for the IP Address Filter. It includes the following details:

- Navigation tabs: User, Authentication, Anonymous Visit, **IP Address Filter**, Security Service.
- Checkbox: Enable IP Address Filter.
- Dropdown menu: IP Address Filter Type set to "Forbidden".
- Section header: IP Address Filter.
- Buttons: Add, Modify, Delete, Clear.
- Table:

No.	IP
1	172.6.23.2

Obrázek 9–7 Okno filtru adres IP

2. Zaškrtněte políčko **Enable IP Address Filter**.

3. Z rozevíracího seznamu vyberte typ filtru adres IP, volitelné možnosti jsou **Forbidden** a **Allowed**.

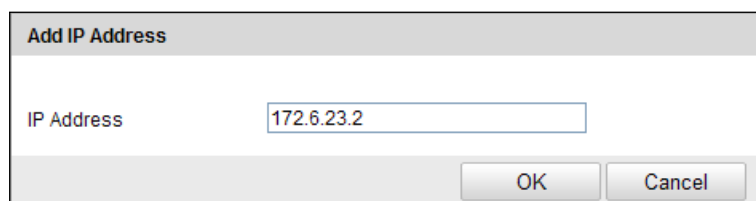
4. Nastavte seznam filtrů adres IP.

- Přidání adresy IP

Kroky:

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

(2) Zadejte adresu IP.



Obrázek 9–8 Přidání adresy IP

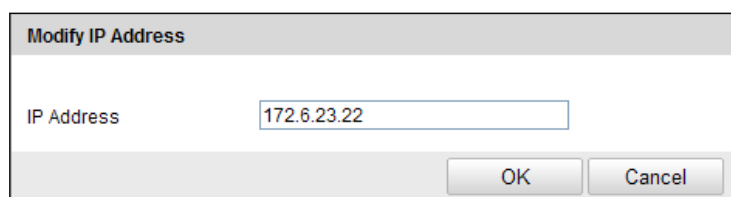
(3) Kliknutím na **OK** dokončíte přidání.

- Úprava adresy IP

Kroky:

(1) V seznamu filtrů klikněte levým tlačítkem na adresu IP a klikněte na možnost **Modify**.

(2) Upravte adresu IP v textovém poli.



Obrázek 9–9 Úprava adresy IP

(3) Kliknutím na **OK** dokončíte úpravy.

- Odstranění adresy IP

V seznamu filtrů klikněte levým tlačítkem na adresu IP a klikněte na možnost **Delete**.

- Odstranění všech adres

Pro odstranění všech adres IP klikněte na možnost **Clear**.

5. Kliknutím na tlačítko **Save** uložte nastavení.

9.5 Služba zabezpečení

Kamera poskytuje službu zabezpečení a tím větší uživatelské pohodlí v případě, že chcete povolit vzdálené přihlašování a vylepšit zabezpečení datové komunikace.

Kroky:

1. Přejděte do okna konfigurace služby zabezpečení:

Configuration > Advanced configuration > Security > Security Service



Obrázek 9–10 Služba zabezpečení

2. Pro povolení bezpečnosti datové komunikace zaškrtněte políčko **Enable SSH**, pro zakázání SSH zaškrtnutí políčka zrušte.
3. Zaškrtněte políčko **Enable Illegal Login Lock**, pokud pětkrát po sobě zadáte nesprávné uživatelské jméno nebo heslo, zařízení se uzamkne.

Poznámka: Je-li zařízení uzamčeno, můžete se k němu zkusit přihlásit po 30 minutách, nebo zařízení před opakováním pokusu restartujte.

9.6 Zobrazení informací o zařízení

Otevřete rozhraní informací o zařízení: **Configuration > Basic Configuration > System > Device Information** nebo **Configuration > Advanced Configuration > System > Device Information**.

V rozhraní **Device Information** můžete upravovat název zařízení.

Zobrazují se i další údaje síťové kamery, jako je Model, Serial No., Firmware Version, Encoding Version, Number of Channels, Number of HDDs, Number of Alarm Input a Number of Alarm Output. Tyto informace nelze změnit v této nabídce. Jde o referenční informace pro údržbu nebo změny v budoucnosti.

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

Obrázek 9–11 Informace o zařízení

9.7 Údržba

9.7.1 Restartování kamery

Kroky:

1. Otevřete rozhraní pro údržbu:

Configuration > Basic Configuration > System > Maintenance

nebo **Configuration > Advanced Configuration > System > Maintenance**

2. Pro restartování síťové kamery klikněte na tlačítko **Reboot**.

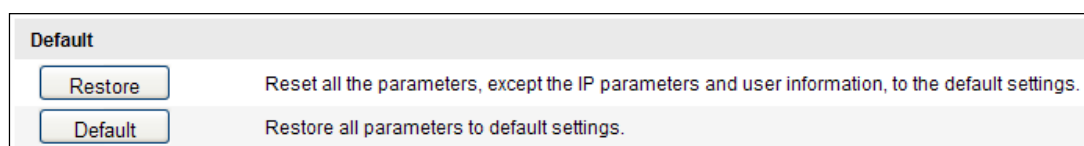


Obrázek 9–12 Restartování zařízení

9.7.2 Obnovení výchozích nastavení

Kroky:

- Otevřete rozhraní pro údržbu:
Configuration > Basic Configuration > System > Maintenance
nebo **Configuration > Advanced Configuration > System > Maintenance**
- Pro obnovení výchozího nastavení klikněte na tlačítko **Restore** nebo **Default**.



Obrázek 9–13 Obnovení výchozího nastavení

Poznámka: Po obnovení výchozího nastavení je obnovena i adresa IP na výchozí adresu IP, proto buďte při provádění této akce opatrní.

9.7.3 Export/import konfiguračního souboru

Účel:

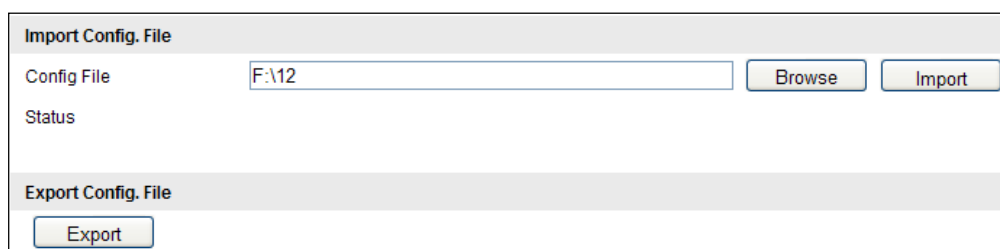
Konfigurační soubor je používán pro dávkovou konfiguraci kamer a může zjednodušit kroky konfigurace v případech, kdy je nutno nakonfigurovat hodně kamer.

Kroky:

- Otevřete rozhraní pro údržbu:
Configuration > Basic Configuration > System > Maintenance
nebo **Configuration > Advanced Configuration > System > Maintenance**
- Pro export aktuálního konfiguračního souboru klikněte na tlačítko **Export** a uložte jej na konkrétním místě.
- Pro výběr uloženého konfiguračního souboru klikněte na tlačítko **Browse** a potom pro zahájení importu konfiguračního souboru klikněte na tlačítko **Import**.

Poznámka: Po importu konfiguračního souboru je třeba kameru restartovat.

- Klikněte na tlačítko **Export** a nastavte cestu pro uložení konfiguračního souboru v místním úložišti.

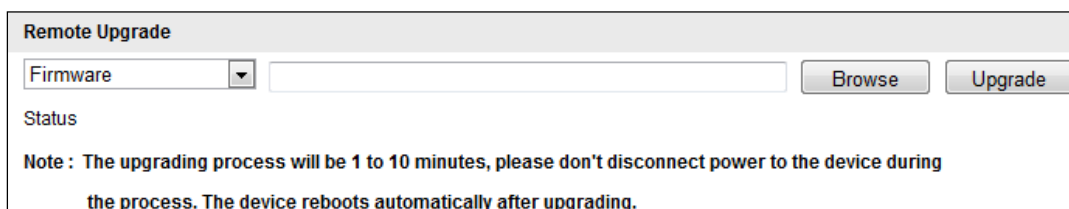


Obrázek 9–14 Export/import konfiguračního souboru

9.7.4 Upgrade systému

Kroky:

- Otevřete rozhraní pro údržbu:
Configuration > Basic Configuration > System > Maintenance
 nebo **Configuration > Advanced Configuration > System > Maintenance**
- Vyhledejte soubor upgradu výběrem firmwaru nebo adresáře firmwaru.
 Firmware: Slouží k vyhledání přesné cesty souboru upgradu.
 Firmware Directory: Je požadováno zadání pouze adresáře, ve kterém je soubor upgradu umístěn.
- Pro výběr místního souboru aktualizace klikněte na tlačítko **Browse** a potom pro zahájení vzdálené aktualizace klikněte na tlačítko **Upgrade**.



Obrázek 9–15 Vzdálený upgrade

Poznámka: Proces upgradu trvá 1 až 10 min. Během procesu neodpojujte zařízení od napájení. Po aktualizaci se zařízení automaticky restartuje.

9.8 Nastavení RS-485

Účel:

Sériový port RS-485 se používá k ovládní PTZ kamery. Parametry PTZ je vhodné konfigurovat předtím, než budete ovládat jednotku PTZ.

Kroky:

1. Otevřete rozhraní pro nastavení portu RS-485:

Configuration > Advanced Configuration > System > RS485

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

Obrázek 9–16 Nastavení rozhraní RS-485

2. Nastavte parametry RS-485 a pro uložení nastavení klikněte na tlačítko **Save**.

Ve výchozím nastavení je přenosová rychlost nastavena na hodnotu 9600 bps, datového bitu na 8, stop bit je 1 a parita a řízení toku mají hodnotu Žádný.

Poznámka: Parametry přenosové rychlosti, protokolu PTZ a adresy PTZ by měly být naprosto shodné s parametry kamery PTZ.

9.9 Nastavení služby

Pro vstup do rozhraní nastavení služby přejděte do nabídky **Configuration > Advanced Configuration > System > Service**.

Nastavení služby označuje hardwarovou službu, kterou kamera podporuje a liší se v závislosti na různých kamerách.

U kamer s podporou IR LED, ABF (automatické zpětné zaostření), automatické odmlžení nebo LED stavu můžete přejít do hardwarové služby a v závislosti na aktuálních požadavcích vybrat možnost povolení nebo zakázání odpovídající služby.

U kamer s podporou topného tělesa pro odmrazování můžete pro povolení automatického odmrazování zaškrtnout odpovídající políčko.

Poznámka: Topné těleso pro odmrazování je podporováno pouze se zdrojem napájení POE+, 24 V AC nebo 12 V DC. U topného tělesa pro odmrazování je podporován pouze zdroj napájení 802.3af, standardní napájení 802.3af topné těleso pro odmrazování nepodporuje.

Dodatek

Dodatek 1 Úvod k softwaru SADP

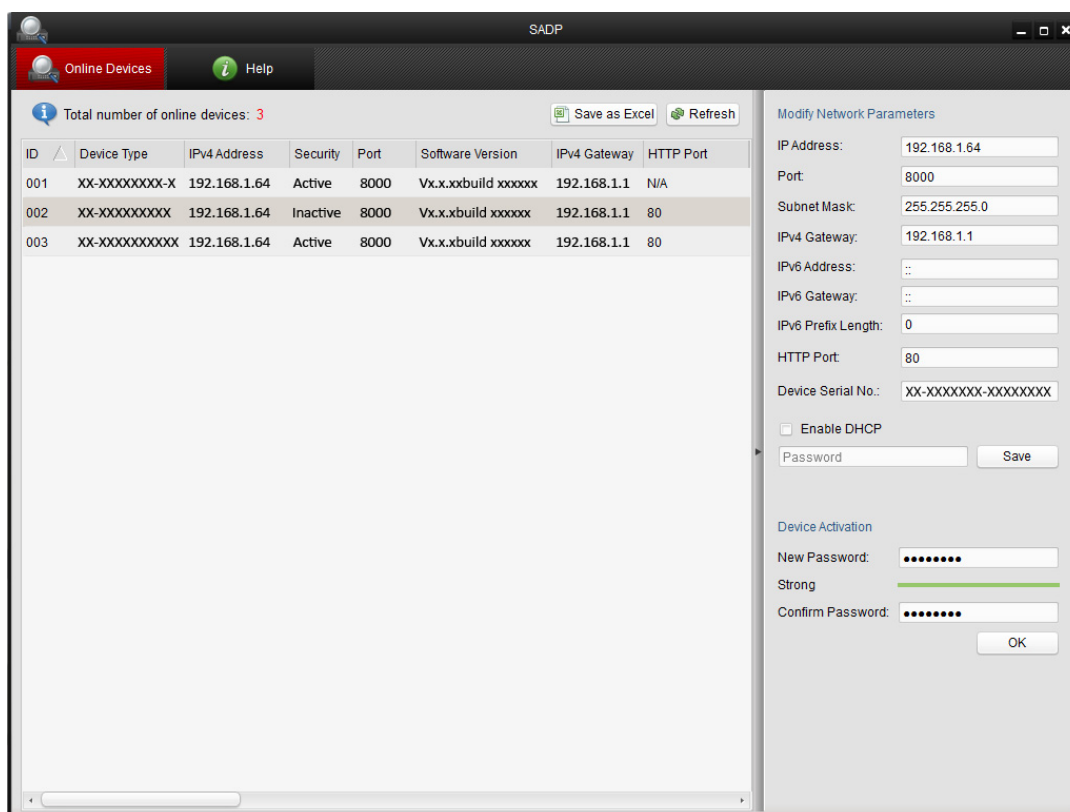
● Popis SADP

SADP (Search Active Devices Protocol) je uživatelsky přívětivý a bezinstalační nástroj pro vyhledávání zařízení on-line. Nástroj vyhledává aktivní internetová zařízení v podsíti a zobrazí informace o zařízeních. Můžete také upravit základní síťové informace zařízení využívajících tento software.

● Vyhledávání aktivních zařízení on-line

◆ Automatické vyhledávání zařízení on-line

Po spuštění softwaru SADP se automaticky prohledávají internetové zařízení každých 15 sekund v podsíti, kde počítač nachází. Zobrazí se celkový počet a informace o vyhledávání v zařízeních v rozhraní zařízení on-line. Zobrazí se informace o zařízení včetně typu zařízení, adresy IP a čísla portu atd.

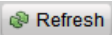


Obrázek A.1.1 Vyhledávání zařízení on-line





Poznámka:

Zařízení lze vyhledat a zobrazit v seznamu 15 sekund poté, co dojde ke změně jeho stavu na online. Zařízení bude ze seznamu odebráno 45 sekund poté, co dojde ke změně jeho stavu na offline.

◆ **Ruční vyhledávání zařízení on-line**

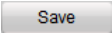
Můžete také kliknout na  pro ruční aktualizaci seznam zařízení on-line. Nově vyhledaná zařízení budou přidána do seznamu.



Kliknutím na  nebo  v každém záhlaví sloupce seřadíte příslušné informace. Kliknutím na  rozšíříte tabulku zařízení a skryjete panel parametrů sítě na pravé straně, kliknutím na tlačítko  jej opět zobrazíte.

● **Úprava síťových parametrů**

Kroky:

1. V seznamu zařízení vyberte zařízení, která chcete upravit, a síťové parametry zařízení se zobrazí na panelu **Modify Network Parameters** vpravo.
2. Upravte nastavitelné síťové parametry, např. adresu IP a číslo portu.
3. Zadejte heslo účtu správce zařízení v poli **Password** a kliknutím na  uložte změny.



- *Kvůli vašim osobním údajům a lepší ochraně před bezpečnostními riziky důrazně doporučujeme použít silná hesla pro všechny funkce a síťová zařízení. Pro zvýšení zabezpečení vašeho produktu by heslo mělo být takové, které jste vybrali sami (s použitím minimálně 8 znaků, včetně velkých a malých písmen, čísel a zvláštních znaků).*
- *Zodpovědnost za správnou konfiguraci všech hesel a ostatních bezpečnostních opatření nese montážní pracovník nebo konečný 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.

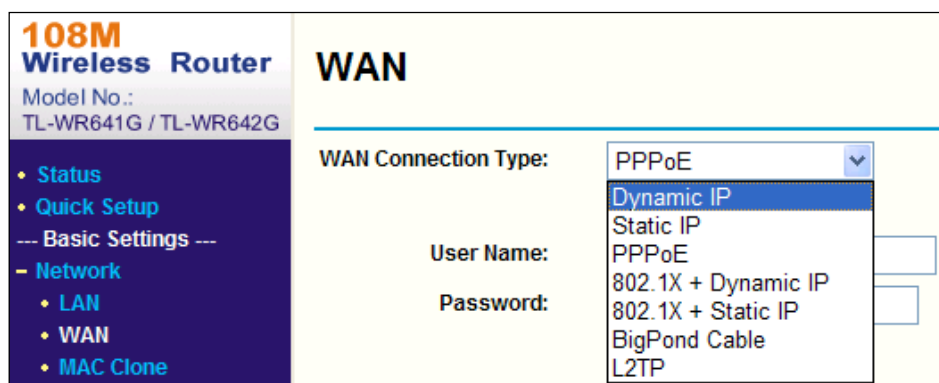
Obrázek A.1.2 Úprava síťových parametrů

Dodatek 2 Mapování portů

Následující nastavení se vztahují ke směrovači TP-LINK (TL-WR641G). Nastavení se liší v závislosti na různých modelech směrovačů.

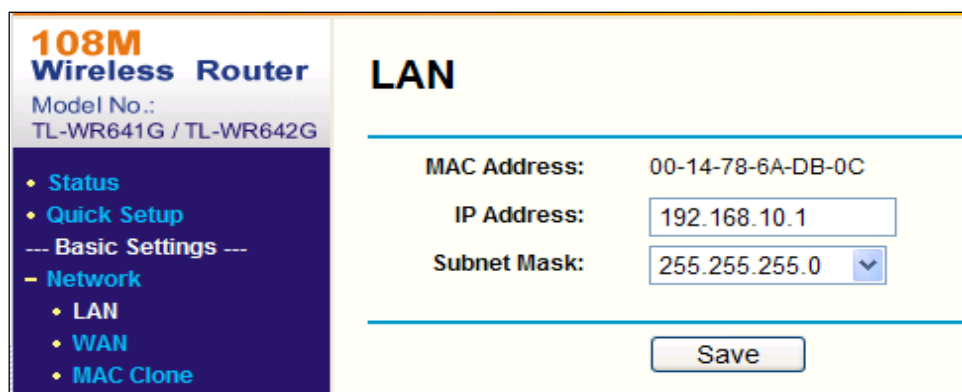
Kroky:

1. Vyberte nastavení možnosti **WAN Connection Type**, viz níže:



Obrázek A.2.1 Výběr typu připojení WAN

2. Nastavte parametry sítě **LAN** směrovače dle následujícího obrázku, včetně nastavení IP adresy a masky podsítě.



Obrázek A.2.2 Nastavení parametrů sítě LAN

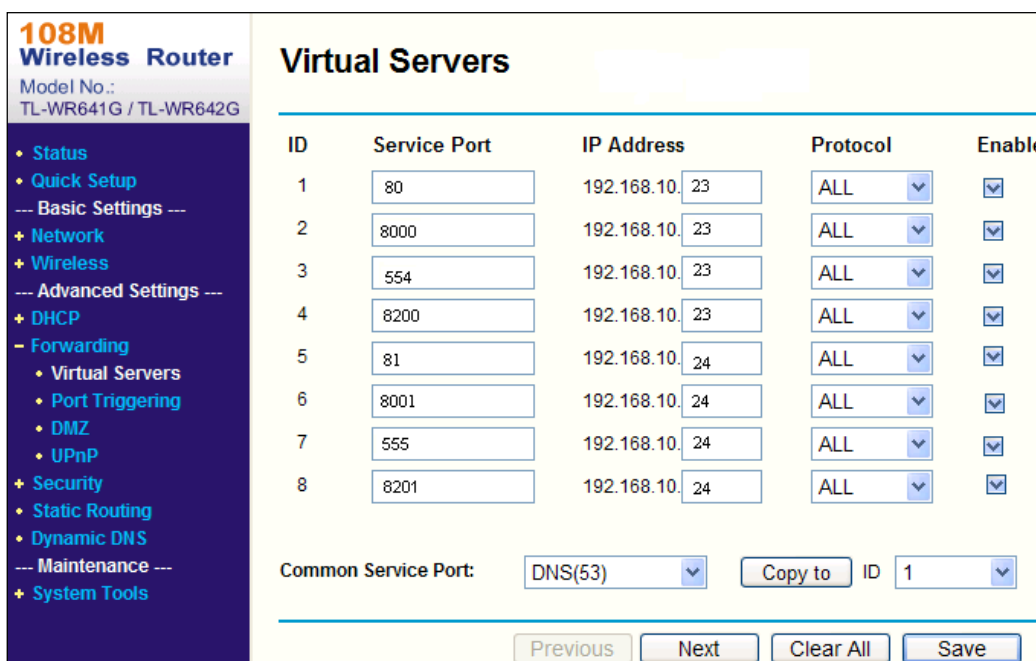
3. Nastavte mapování portů virtuálních serverů **Předávání**. Ve výchozím nastavení používá kamera port 80, 8000 a 554. Pomocí webového prohlížeče nebo klientského softwaru lze hodnoty těchto portů změnit.

Příklad:

Pokud jsou kamery připojeny ke stejnému směrovači, lze nakonfigurovat porty jedné kamery s IP adresou 192.168.1.23 na 80, 8000 a 554 a porty druhé kamery s IP adresou 192.168.1.24 na 81, 8001, 555, 8201. Viz kroky níže:

Kroky:

1. Jak je uvedeno v nastavení výše, namapujte na IP adrese 192.168.1.23 porty síťové kamery 80, 8000, 554 a 8200.
2. Na IP adrese 192.168.1.24. namapujte porty 81, 8001, 555 a 8201 druhé síťové kamery.
3. Pro protokoly povolte možnost **ALL** nebo **TCP**.
4. Zaškrtněte zaškrťovací políčko **Enable** a kliknutím na tlačítko **Save** nastavení uložte.



Obrázek A.2.3 Mapování portů

Poznámka: Port síťové kamery nemůže být v konfliktu s jinými porty. Někjaký port pro webovou správu směrovače je například nastaven na 80. Změňte port kamery, pokud jde o stejný port pro správu.



First Choice for Security Professionals