Kamera sieciowa

Instrukcja użytkownika

UD.6L0201D1990A01

Instrukcja użytkownika

Wszelkie niniejsze informacje, w tym pośród innych, informacje tekstowe, obrazy, wykresy, schematy stanowią własność korporacji Hangzhou Hikvision Digital Technology Co., Ltd. lub jej spółek zależnych (dalej krótko: HIKVISION). Niniejszej instrukcji użytkownika (dalej krótko: INSTRUKCJA) nie wolno powielać, zmieniać, tłumaczyć czy rozprowadzać, ani w części ani w całości, w żaden sposób, bez uzyskania uprzednio pisemnej zgody od HIKVISION. O ile nie wskazano inaczej, HIKVISION nie daje żadnych gwarancji, nie stanowi żadnej reprezentacji — ani bezpośredniej ani dorozumianej — w stosunku do niniejszej INSTRUKCJI.

Krótko o niniejszej instrukcji

INSTRUKCJA dotyczy następującego urządzenia: Kamera Sieciowa, wer. 5.3.3.

W INSTRUKCJI podano zalecany sposób użytkowania urządzenia oraz zarządzania nim. Obrazy, wykresy schematy, ilustracje, jak też wszelkie inne informacje/dane użyte dalej w tekście INSTRUKCJI, zostały zamieszczone w niej wyłącznie w celach opisowo-objaśniających. Informacje i dane, zawarte w niniejszej instrukcji, mogą na obecną chwilę być już nieaktualne z powodu nowego oprogramowania wewnętrznego (tj. firmware'u) lub z powodów innych. Najnowszą wersję tego oprogramowania można znaleźć na stronie naszej firmy (http://overseas.hikvision.com/en/).

Niniejszą INSTRUKCJĘ UŻYTKOWNIKA należy stosować pod opieką specjalisty z branży.

Znaki handlowe

Znaki towarowe i logotypy HIKVISION stanowią własność HIKVISION w różnych jurysdykcjach. Pozostałe znaki towarowe i logotypy, wzmiankowane poniżej w tekście, stanowią własność ich odnośnych właścicieli.

Zastrzeżenia

W maksymalnym zakresie dopuszczanym przez odnośne, stosujące się regulacje prawne opisywany tu produkt, wraz z jego częścią sprzętową, software'm i firmware'm, dostarcza się w stanie zastanym („jako taki"), z wszelkimi ułomnościami i błędami w funkcjonowaniu; ponadto HIKVISION nie daje żadnej gwarancji, ani wyraźnej (explicite) ani dorozumianej (implicite), w tym w szczególności gwarancji: sprzedażności rynkowej, zadowalającej jakości, zdatności do konkretnego celu, nienaruszania praw osób trzecich — jednak bez zawężania zakresu do tychże gwarancji. Ani korporacja HIKVISION, ani jej kierownictwo, ani członkowie jej zarządu, ani jej pracownicy, ani jej pośrednicy handlowi w żadnym przypadku nie ponoszą odpowiedzialności przed UŻYTKOWNIKIEM za jakiekolwiek skonkretyzowane, następcze, incydentalne czy pośrednio powstałe szkody — w tym m.in. szkody wynikłe z utraty zysków w działalności gospodarczej, nieciągłości działalności gospodarczej, ani też wynikłe z

utraty danych czy dokumentacji, zaistniałe w związku z użytkowaniem niniejszego produktu — a to nawet w przypadku poinformowania HIKVISION o potencjalnej możliwości wystąpienia tychże strat.

W zakresie produktów, posiadających dostęp do sieci Internet, UŻYTKOWNIK eksploatuje niniejszy produkt w całości na własne ryzyko. HIKVISION nie przyjmuje jakiejkolwiek odpowiedzialności za nieprawidłową pracę urządzenia, wycieki danych prywatnych czy za inne straty, powstałe wskutek: cyber-ataków, ataków hackerskich, penetrację przez wirusy komputerowe lub straty wynikłe z innych potencjalnych zagrożeń z Internetu. Mimo powyższego, w razie potrzeby, HIKVISION dostarczy na czas wsparcie techniczne.

Przepisy w zakresie nadzoru / dozoru są różne w zależności od konkretnej jurysdykcji. Prosimy sprawdzić wszelkie stosujące się przepisy prawa w jurysdykcji UŻYTKOWNIKA przed rozpoczęciem użytkowania niniejszego produktu — ażeby zagwarantować, że użytkowanie u UŻYTKOWNIKA zachodzi w zgodzie ze stosującymi się przepisami prawa. HIKVISION nie ponosi odpowiedzialności w przypadkach, w których produkt jest użytkowany do osiągania celów nielegalnych.

W każdym przypadku wystąpienia jakichkolwiek sprzeczności między niniejszą INSTRUKCJĄ a odnośnym przepisem prawa, ten ostatni uznaje się za przesądzający w sprawie.

Informacje o regulacjach prawnych

Informacje o zgodności FCC

Zgodność z wymogami komisji FCC: Po poddaniu urządzenia technicznym próbom kwalifikacyjnym stwierdzono, że spełnia ono wymogi nakreślone w rozdziale nr 15 *Przepisów Regulacyjnych* komisji FCC. Wymogi te zapewniają właściwą i dostateczną ochronę przed niepożądanymi zakłóceniami, generowanymi przez urządzenie, kiedy jest użytkowane w otoczeniu komercyjnym. Opisywane urządzenie wykorzystuje i może emitować promieniowanie z zakresu częstotliwości radiowych. Eksploatowanie niniejszego urządzenia na terenach mieszkalnych najprawdopodobniej wprowadzi zakłócenia istotnie szkodliwe — w takich to przypadkach UŻYTKOWNIK będzie zmuszony usunąć te zakłócenia na własny koszt.

- **Warunki FCC**

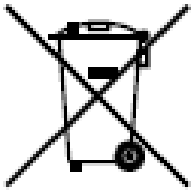
Niniejsze urządzenie jest zgodne z wymogami opisanymi w rozdziale nr 15 *Przepisów Regulacyjnych* komisji FCC. Użytkowanie urządzenia wymaga spełnienia dwóch następujących warunków:

1. Urządzenie nie może wywoływać zakłóceń istotnie szkodliwych.
2. Urządzenie musi być odporne na wszelkie zakłócenia docierające z zewnątrz, włącznie z zakłóceniami, zdolnymi wywoływać jego niepożądane funkcjonowanie.

Oświadczenie o zgodności z normami UE

Niniejszy produkt oraz, o ile przypadek ma miejsce, zastosowanie, dostarczane do niego akcesoria opatrzone są znakiem „CE”, który wykazuje ich zgodność ze stosującymi się, ujednoliconymi normami europejskimi, wymienionymi w dyrektywach EMC nr 2004/108/EC oraz RoHS nr 2011/65/EU.

Dyrektywa 2012/19/EU (tzw. dyrektywa WEEE): Produktów opatrzonych tym znakiem nie wolno nigdzie na terenie UE wyrzucać do miejskich śmieci niesegregowanych. Aby zrealizować należyty odzysk surowców z tego produktu (tzw. recykling) oddaj ten produkt do Twojego lokalnego Sprzedawcy w chwili zakupu nowego urządzenia (stanowiącego odpowiednik urządzenia usuwanego); ewentualnie usuń/oddaj to urządzenie w specjalnie do tego zorganizowanym punkcie zbierania odpadów. Więcej o tym na stronie: www.recyclethis.info.



Dyrektywa 2006/66/EC (dyrektywa dot. baterii): W niniejszym produkcie znajduje się bateria, której nie wolno wyrzucać – nigdzie na terenie UE – do miejskich śmieci niesegregowanych. W dokumentacji towarzyszącej produktowi podano informacje o konkretnie zastosowanej w nim baterii. Bateria ta nosi pokazane obok oznaczenie, do którego może być dodane literowe oznaczenie pierwiastka chemicznego: Cd (kadm), Pb (ołów) albo Hg (rtęć). W celu uzyskania optymalnego recyklingu zdaj tę baterię u Twojego Sprzedawcy lub w adekwatnie oznakowanym, wyspecjalizowanym punkcie zbierania odpadów. Więcej o tym na stronie www.recyclethis.info.

Zgodność z ICES-003 (Kanada)

Niniejsze urządzenie spełnia wymogi normy CAN ICES-3 (A)/NMB-3(A).

Zasady bezpiecznej eksploatacji

Poniższe zalecenia mają na celu zagwarantowanie, że UŻYTKOWNIK produktu będzie potrafił prawidłowo go użytkować — tj. tak, by nie mogła zaistnieć sytuacja niebezpieczna czy straty w mieniu.

Wymagane tu środki ostrożności dzielą się na 2 grupy: ‘**Ostrzeżenia**’ i ‘**Przestrogi**’.

Ostrzeżenia (Warning**)**: Zaniedbanie któregokolwiek z tych ***Ostrzeżeń*** grozi powstaniem poważnego obrażenia lub śmierci.

Przestrogi (Caution**)**: Zaniedbanie którejkolwiek z tych ***Przestróg*** może spowodować obrażenia lub uszkodzenie urządzenia/eń.

	
Ostrzeżenie: Zastosuj się do tych zaleceń ochronnych, aby nie dopuścić do poważnych obrażeń czy śmierci.	**Przestrogi:** Zastosuj się do tych środków ostrożności, aby zapobiec potencjalnym obrażeniom lub stratom

	materialnym.

Ostrzeżenia:

- Do zasilania kamery należy zastosować zasilacz, spełniający wymogi zasilania napięciem obniżonym typu SELV (Safety Extra Low-Voltage). W tym, musi być źródłem prądu 12 V DC lub 24 V AC (zależy od modelu kamery), zgodnym z normą IEC60950-1 i normą dla źródeł prądu LPS (Limited Power Source).
- Aby zmniejszyć ryzyko pożarowe / zagrożenie porażeniowe, nie wolno wystawiać tego urządzenia na działanie deszczu ani wilgoci.
- Instalacja urządzenia musi zostać wykonana przez technika-specjalistę i zgodnie ze wszelkimi przepisami technicznymi obowiązującymi w miejscu instalacji.
- W elektryczny obwód zasilającym należy włączyć urządzenia wyłączające, aby zapewnić wygodne urządzenie do odcinania dopływu prądu do instalacji.
- Jeśli kamera ma zostać zamontowana pod sufitem, to trzeba się najpierw upewnić, że sufit wytrzyma siłę ciężkości powyżej 50 N (niutonów).
- W sytuacjach, w których produkt nie działa prawidłowo, prosimy zwrócić się do Państwa Sprzedawcy lub do najbliższego Centrum Serwisowego. Nigdy nie próbuj rozbierać (demontować) kamery samemu. (Nie bierzemy, w żadnym zakresie, odpowiedzialności za problemy powstałe w następstwie nieupoważnionej naprawy lub nieupoważnionego konserwowania urządzenia.)

Przestrogi:

- Zanim rozpoczniesz użytkowanie kamery, upewnij się, że napięcie prądu dostarczanego do niej z zastosowanego źródła zasilania jest prawidłowe.
- Uważaj, by nie upuścić kamery, ani nie wystawiaj kamery na żadne udary wzgl. wstrząsy mechaniczne.
- Nie dotykaj modułu matrycy fotoczułej palcami. Gdyby wymagał oczyszczenia, użyj do tego czystej szmatki nasączonej niewielką ilością etanolu (alkoholu etylowego), którą delikatnie przetrzyj moduł czujnika. Jeśli kamera ma pozostawać przez dłuższy czas nieużywana, to zakryj jej obiektyw nasadką ochronną, aby chronić czujnik od zabrudzeń.
- Nie kieruj obiektywu kamery na źródła silnego światła, jak np. słońce, żarówki (lampy żarowe). Zadziałanie silnego światła na kamerę może być fatalne (niszczące) w skutkach.
- Padająca wiązka światła laserowego może wypalić fotoczułą matrycę kamery, dlatego podczas stosowania jakichkolwiek przyrządów laserowych bacznie uważaj, żeby nie wystawiać go na działanie światła laserowego.
- Nie umieszczaj kamery w miejscach skrajnie gorących / mroźnych (podczas pracy kamery temperatura otoczenia powinna wynosić: –30 ℃~+60 ℃, a w przypadku kamer z końcówką „H” w kodzie modelu: –40 ℃~+60 ℃), ani w otoczeniu zapylonym czy wilgotnym. Nie wystawiaj też kamery na działanie silnego promieniowania elektromagnetycznego.
- Aby nie dochodziło do gromadzenia się ciepła wzgl. przegrzania kamery, urządzenie musi mieć zapewnioną odpowiednio wydajną wentylację dla uzyskania właściwego środowiska pracy.
- Chroń kamerę od wody i innych cieczy.
- Na potrzeby transportu kamera musi być zapakowana w swoje oryginalne opakowanie od producenta.
- Niewłaściwie użyta lub niewłaściwie wymieniona bateria kamery grozi wybuchnięciem. W kamerze należy stosować baterię o typie technicznym zalecanym przez producenta kamery.

Uwagi:

W przypadku kamer zdolnych do rejestracji obrazu w świetle podczerwonym (IR), zastosuj poniższe środki ostrożności, aby nie dopuścić do powstania odbić światła IR:

- Zapylenie lub zatłuszczenie obecne na kopułce kamery spowoduje odbicia światła IR. Nie zdejmuj folii ochronnej z kopułki, aż skończysz zupełnie instalować kamerę. Pył lub zatłuszczenie, obecne na kopułce kamery, usuń przez przetarcie kopułki czystą, miękką szmatką zwilżoną alkoholem izopropylowym.

- Uważaj, żeby w bezpośrednim otoczeniu miejsca, w którym montujesz kamerę, nie było powierzchni / przedmiotów zdolnych odbijać światło, w tym IR. (Pamiętaj, że światło IR, emitowane z kamery, może ulec odbiciu i powrócić do kamery via obiektyw, wywołując przy tym niepożądane artefakty obrazowe, tzw. refleksy.)
- Pierścień gąbczasty, znajdujący się wokół obiektywu kamery, musi być swą płaszczyzną na równo z wewnętrzną powierzchnią wypukłości optyki, aby zapewnić rozdzielnie obiektywu od reflektora IR (IR-LED) w kamerze. Zamocuj obudowę kopułkową kamery do korpusu kamery tak, żeby pierścień gąbczasty i kopułka były ze sobą złączone w całość idealnie równo i niezauważalnie spasowane.

Spis treści

1. Wymagania systemowe

System operacyjny (OS): Microsoft Windows XP z poprawką SP1, lub wersja wyższa.
Procesor (CPU): 2,0 GHz, lub z szybszym taktowaniem.
Pamięć (RAM): 1GB, lub większa pojemność.
Rozdzielczość ekranowa (DISPLAY): 1024×768 px, lub wyższa.
Przeglądarka internetowa:

– *Internet Explorer*	wer. 8.0,	lub wersja wyższa,
– *Apple Safari*	wer. 5.0.2,	lub wersja wyższa,
– *Mozilla Firefox*	wer. 5.0,	lub wersja wyższa,
– *Google Chrome*	wer. 18,	lub wersja wyższa.

2. Podłączenie do sieci teleinformatycznej

Uwaga – pamiętaj:

- Przyjmujesz do wiadomości, że użytkowanie niniejszego produktu z dostępem do sieci Internet może być obarczone ryzykiem ekspozycji na zagrożenia sieciowe. Dla uniknięcia wszelkich ataków z sieci oraz zapobieżenia ewentualnym wyciekom danych należy wzmocnić swoją własną ochronę (IT). Jeśli produkt nie działałby prawidłowo, to należy zwrócić się z występującym problemem do Sprzedawcy lub najbliższego Centrum Serwisowego naszych produktów.
- Aby zapewnić bezpieczeństwo sieciowe tej kamery sieciowej, zalecamy okresowe badanie/monitorowanie stanu urządzenia i robienie przeglądów konserwacyjnych. Możesz skontaktować się z nami, jeśli potrzebujesz takiej usługi.

Przygotuj na wstępie:

- Jeśli zamierzasz skonfigurować tę kamerę sieciową poprzez sieć lokalną (LAN), to zajrzyj do *podrozdz. 2.1* ***Konfigurowanie kamery sieciowej via LAN***, str. 12.
- Jeśli zamierzasz konfigurować tę kamerę sieciową poprzez sieć WAN, to zajrzyj do *podrozdz. 2.2* ***Konfigurowanie kamery sieciowej via WAN***, str. 19.

2.1. Konfigurowanie kamery sieciowej via LAN

Cel czynności:

Aby uzyskiwać podgląd bieżący obrazu tej kamery poprzez sieć LAN lub aby skonfigurować ustawienia tej kamery poprzez sieć LAN — musisz włączyć kamerę do tej samej podsieci co Twój komputer operatorski[1] i zainstalować oprogramowanie *SADP* lub *iVMS-4200*, by móc wyszukać i zmodyfikować adres sieciowy IP tej kamery sieciowej.

Uwaga: Dokładne wiadomości wstępne o oprogramowaniu *SADP* znajdziesz w części ***Załącznik 1: Wiadomości wstępne o oprogramowaniu SADP***, od str. 162.

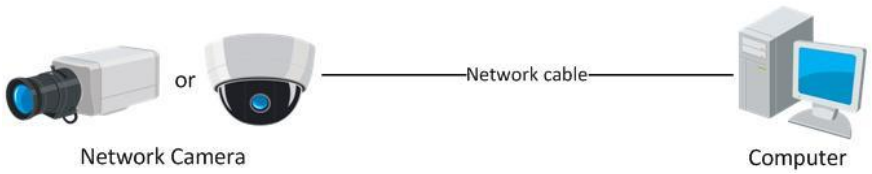
2.1.1. Podłączenie przewodowe poprzez sieć LAN

Na poniższych schematach pokazano dwa sposoby połączenia przewodowego kamery sieciowej z komputerem operatorskim:

Cel czynności:

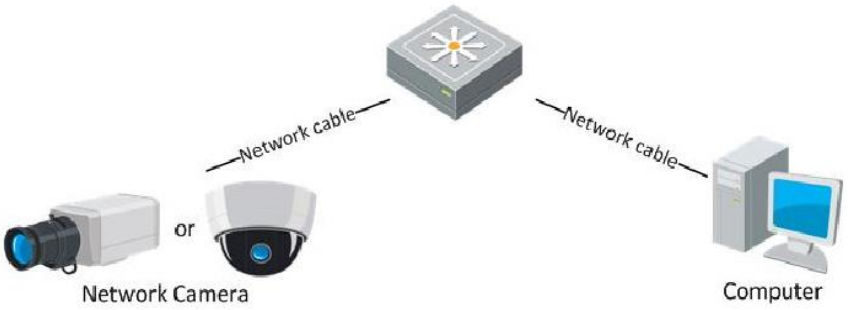
- Aby przetestować funkcjonowanie Twojej kamery sieciowej, możesz połączyć ją kablem sieciowym bezpośrednio z Twoim komputerem operatorskim, jak pokazane na schemacie:

[1] komputer sterujący, obsługiwany przez operatora kamery — przyp. red.



Rys. 2–1: Połączenie kamery ze sterującym PC — zrealizowane bezpośrednio

- Łącząc urządzenia sieciowe jak pokazane na poniższym schemacie, będziesz w stanie konfigurować ustawienia Twojej kamery sieciowej poprzez sieć lokalną (LAN) za pośrednictwem PRZEŁĄCZNIKA SIECIOWEGO / RUTERA.



Rys. 2–2: Połączenie kamery ze sterującym PC — via PRZEŁĄCZNIK SIECIOWY lub RUTER

2.1.2. Zdefiniowanie hasła dostępowego

Aby uaktywnić kamerę[2] musisz najpierw zdefiniować w niej **silne hasło dostępowe** — dopiero po utworzeniu tego HASŁA, da się normalnie używać kamerę.
Masz do dyspozycji każdą z następujących opcji:
– zdefiniowanie hasła w Twojej przeglądarce internetowej,
– zdefiniowanie hasła z poziomu oprogramowania *SADP*, a także
– zdefiniowanie hasła z poziomu oprogramowania klienckiego.

❖ Zdefiniowanie hasła z poziomu przeglądarki internetowej

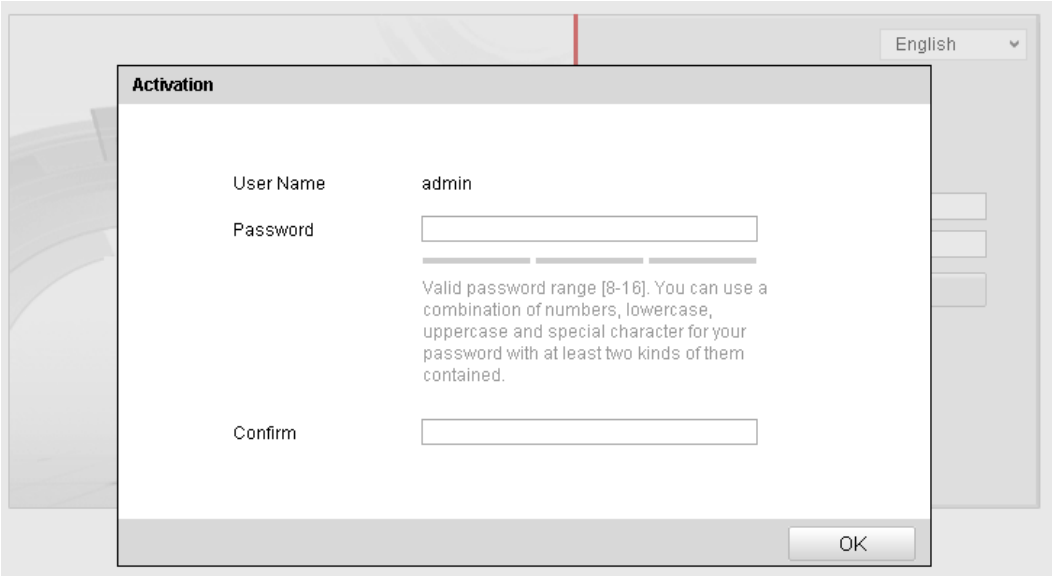
Procedura wykonania:

1. Załącz zasilanie do kamery i podłącz kamerę do sieci.
2. Wprowadź adres IP kamery (zob. ***Uwagi:*** niżej) w polu adresów sieciowych w oknie Twojej przeglądarki internetowej. Następnie naciśnij klawisz **Enter**, aby go wywołać i by uruchomił się INTERFEJS EKRANOWY do obsługi kamery, tj. w celu jej uaktywnienia.

Uwagi:

- Domyślnym adresem IP opisywanej tu kamery sieciowej jest: **192.168.1.64**.
- W kamerach, które domyślnie mają załączoną opcję DHCP, ich adresy IP są alokowane automatycznie. W takiej sytuacji musisz uaktywnić kamerę z poziomu oprogramowania *SADP* (zob. w następnym podrozdziale podano, jak to zrobić).

[2] (tj. uruchomić ją do normalnego użytkowania) — przyp. tłum.



Rys. 2–3: Zdefiniowanie hasła kamery z poziomu Twojej przeglądarki internetowej

3. Utwórz hasło i wprowadź je do pola edycji hasła.

ZALECAMY SILNE HASŁO – Stanowczo zalecamy zdefiniowanie silnego hasła własnego pomysłu. Przy czym musi ono mieć długość co najmniej 8 znaków, w tym co najmniej 3 znaki z następujących kategorii znakowych: litery wielkie, litery małe, cyfry, znaki specjalne — ażeby odpowiednio podnieść poziom zabezpieczenia kamery. Nadto, zalecamy regularne redefiniowanie tego hasła, zwłaszcza w systemach z wymogiem podwyższonej klasy bezpieczeństwa. Redefiniowanie hasła wykonywane co miesiąc / co tydzień może poprawić poziom ochrony kamery.

4. Potwierdź wprowadzone hasło (wpisując je ponownie w polu **Confirm**).
5. Kliknij **OK**, aby zachować hasło w pamięci i wejść w INTERFEJS obsługi kamery, w którym wyświetli się podgląd bieżący z kamery.

❖ Zdefiniowanie hasła kamery z poziomu oprogramowania *SADP*

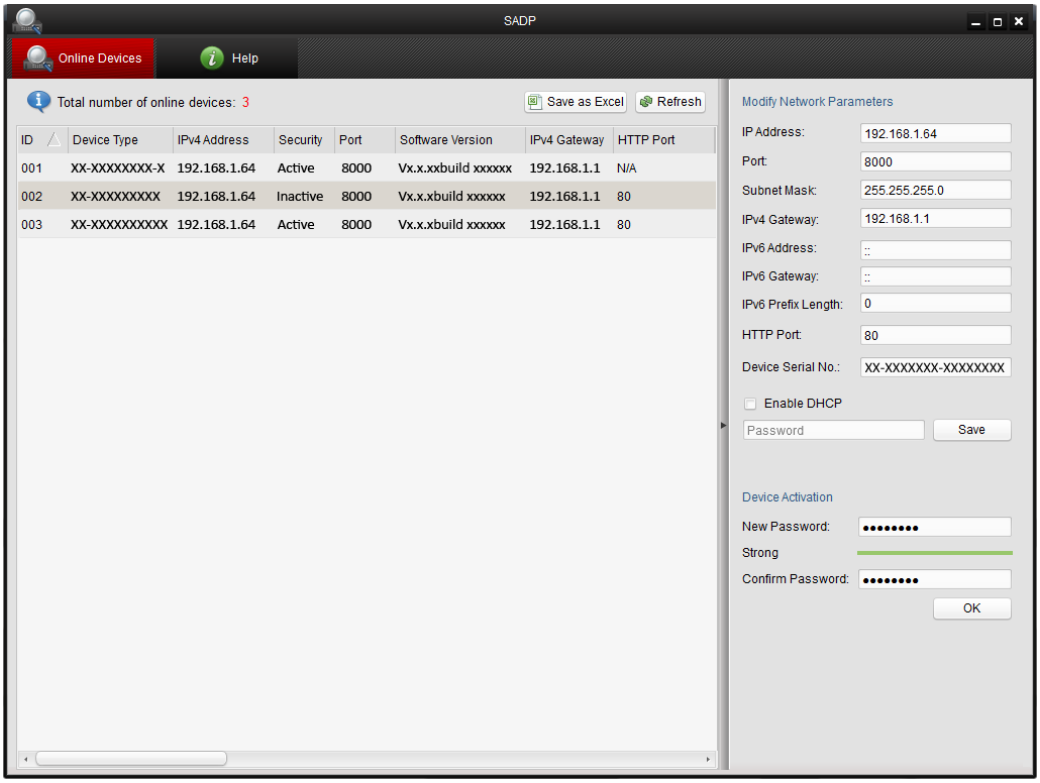
Oprogramowanie *SADP* pozwala użytkownikowi: wykrywać urządzenia znajdujące się w stanie online, aktywować kamerę, redefiniować hasło dostępu do kamery.

Oprogramowanie *SADP* znajdziesz na dołączonej płycie albo pobierz je z naszej oficjalnej witryny internetowej. Uruchom instalatora i przeprowadź instalację postępując zgodnie z instrukcjami w kolejnych okienkach dialogowych instalatora. Poz zainstalowaniu, wykonaj kroki poniższej procedury, aby pomyślnie uaktywnić kamerę.

Procedura wykonania:

1. Uruchom oprogramowanie *SADP*, aby wyszukało urządzenia online (automatycznie wyszuka i wylistuje urządzenia sieciowe, znajdujące się w stanie online).

2. W liście wykrytych urządzeń **Online Devices** przejrzyj stan aktywności obsługowej poszczególnych urządzeń i wybierz spośród nich KAMERĘ NIEAKTYWNĄ.



Rys. 2–4: Interfejs użytkownika w aplikacji *SADP*

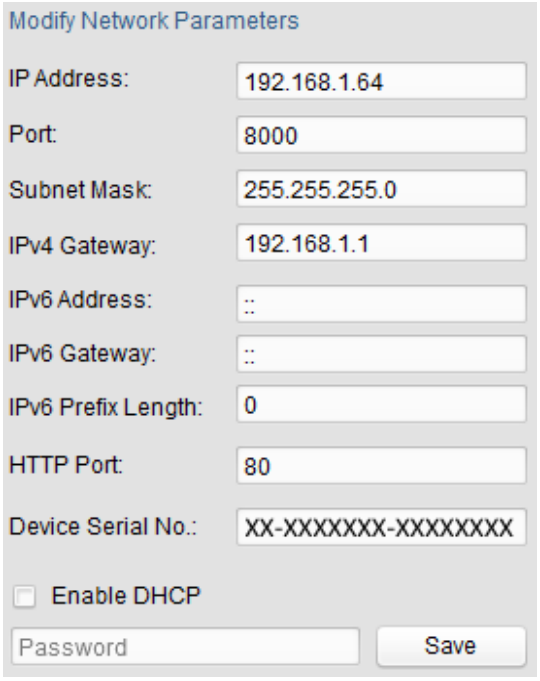
3. Utwórz hasło i wprowadź je w pole edycji hasła **New Password**, po czym potwierdź to hasło przez ponowne wpisanie go w polu **Confirm Password**.

ZALECAMY SILNE HASŁO – Stanowczo zalecamy zdefiniowanie silnego hasła własnego pomysłu. Przy czym musi mieć długość min. 8 znaków, w tym co najmniej 3 znaki z następujących kategorii znakowych: litery wielkie, litery małe, cyfry, znaki specjalne — ażeby odpowiednio podnieść poziom zabezpieczenia kamery. Nadto, zalecamy regularne redefiniowanie tego hasła, zwłaszcza w systemach z wymogiem podwyższonej klasy bezpieczeństwa. Redefiniowanie hasła wykonywane co miesiąc / co tydzień może poprawić poziom ochrony kamery.

4. Kliknij przycisk **OK**, aby zapisać hasło.

To – czy uaktywnienie kamery się powiodło czy nie – możesz sprawdzić w wyświetlającym się zaraz potem okienku wyskakującym. Jeśli uaktywnienie się nie powiodło, to najpierw dobrze sprawdź, czy hasło wprowadzone dla kamery spełnia ww. wymogi i spróbuj jeszcze raz uaktywnić kamerę.

5. Zmień adres IP kamery na tę samą podsieć co Twój komputer: zrób to albo przez ręczne wyedytowanie adresu IP (pole **IP Address**) albo przez zaznaczenie pola wyboru **Enable DHCP**:



Rys. 2–5: Panel w SADP do modyfikowania adresu IP kamery

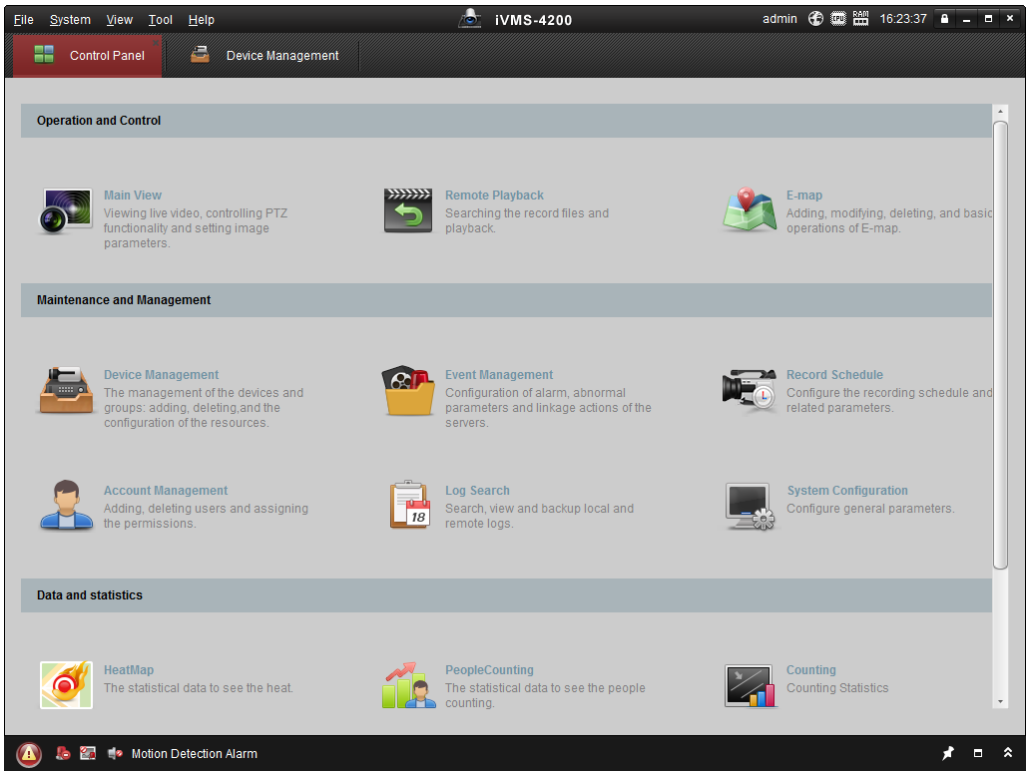
6. Wprowadź hasło, po czym kliknij przycisk **Save**, aby uaktywnić ten zmieniony adres IP kamery.

❖ Zdefiniowanie hasła kamery z poziomu oprogramowania klienckiego

Poniższe oprogramowanie klienckie *iVMS-4200* to bardzo wszechstronna aplikacja, przeznaczona do zarządzania obrazem wielu różnych rodzajów urządzeń wizyjnych.
Weź to oprogramowanie z dostarczonej płyty lub pobierz je z naszej oficjalnej witryny i zainstaluj zgodnie z instrukcjami wyświetlanymi przez instalatora w kolejnych okienkach. Wykonaj poniższe kroki, aby uaktywnić kamerę**.**

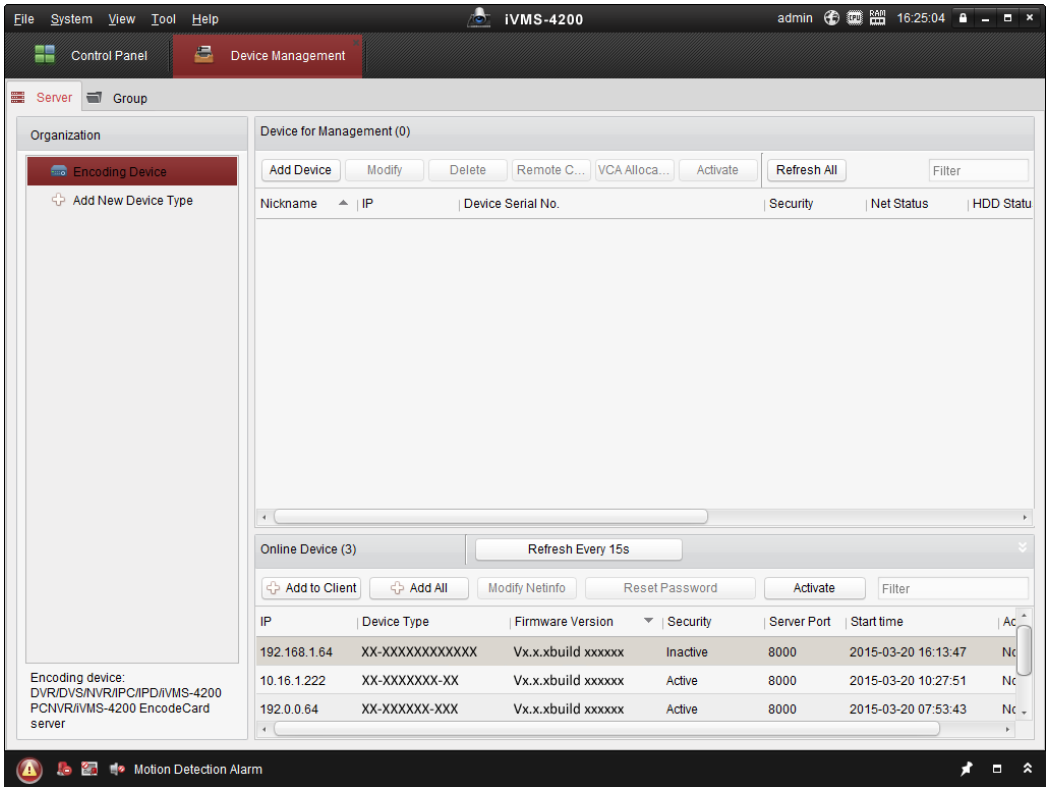
Procedura wykonania:

1. Uruchom oprogramowanie klienckie na komputerze. Pojawia się okienko panelu sterującego tego oprogramowania, jak na ilustracji poniżej:



Rys. 2–6: Panel sterujący oprogramowania klienckiego *iVMS4200* (Control Panel)

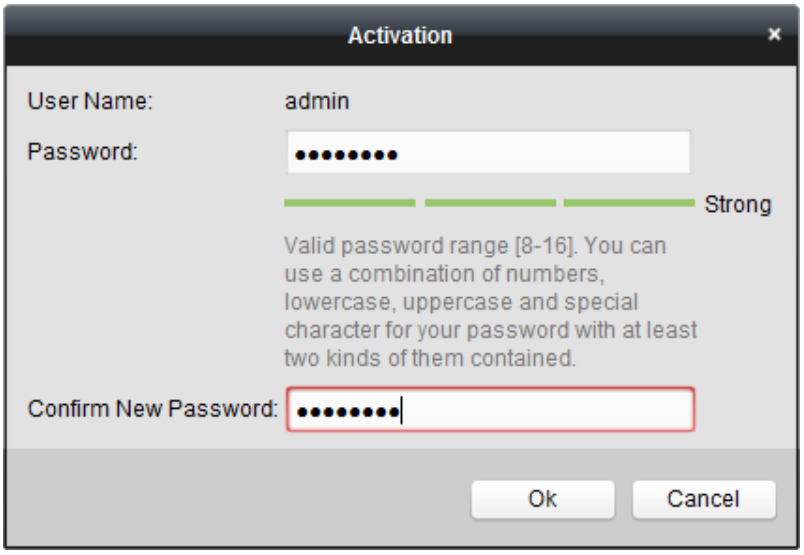
2. W listwie menu (pod belką menu aplikacji) kliknij pole z ikoną **Device Management**, aby wyświetlić INTERFEJS zarządzania urządzeniami (Device Management), jak ten pokazany na poniższej ilustracji:



Rys. 2–7: Interfejs ekranowy do zarządzania urządzeniami w aplikacji-kliencie *iVMS-4200* (Device Management)

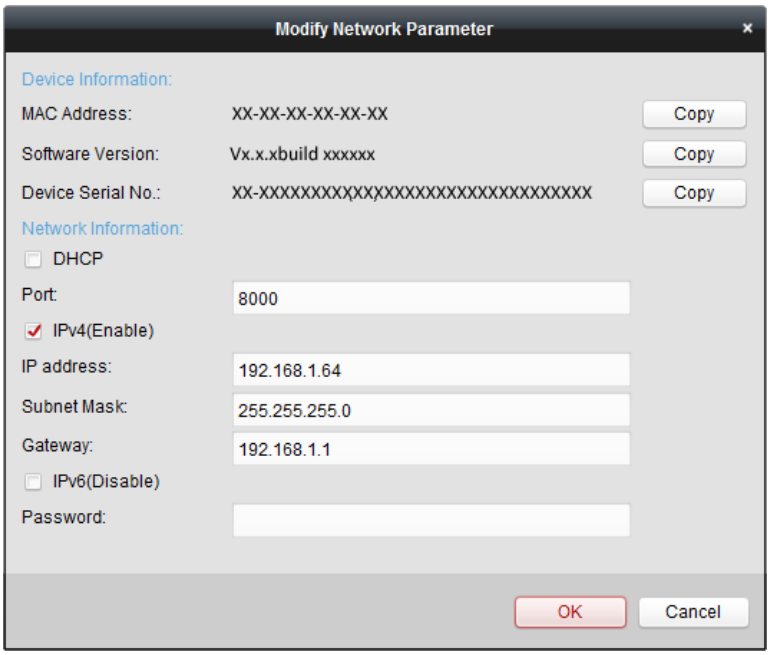
3. Sprawdź stan aktywności obsługowej kamery w liście urządzeń, po czym wybierz tę NIEAKTYWNĄ.
4. Kliknij przycisk **Activate**, aby wyświetlił się interfejs służący do uaktywnienia kamery — okienko **Activation**.
5. Utwórz hasło i wprowadź je w pole edycji hasła (**Password**), po czym potwierdź to hasło w następnym polu (**Confirm New Password**).

ZALECAMY SILNE HASŁO – Stanowczo zalecamy zdefiniowanie silnego hasła własnego pomysłu. Przy czym musi mieć długość min. 8 znaków, w tym co najmniej trzy znaki z następujących kategorii znakowych: litery wielkie, litery małe, cyfry, znaki specjalne — ażeby odpowiednio podnieść poziom zabezpieczenia kamery. Nadto, zalecamy regularne redefiniowanie tego hasła (**Reset Password**), zwłaszcza w systemach z wymogiem podwyższonej klasy bezpieczeństwa. Redefiniowanie hasła wykonywane co miesiąc / co tydzień może poprawić poziom ochrony kamery.



Rys. 2–8: Interfejs ekranowy do uaktywnienia kamery **Activation** (*iVMS-4200*)

6. Kliknij przycisk **OK**, aby uruchomić proces aktywowania kamery.
7. Kliknij przycisk **Modify Netinfo**, aby otworzyć w okno dialogowe konfigurowania parametrów sieciowych **Network Parameter Modification** — pokazane na ilustracji poniżej:



Rys. 2–9: Modyfikowanie parametrów sieciowych urządzenia w iVMS-4200 (Modify Network Parameter)

8. Zmień adres IP kamery na tę samą podsieć co Twój komputer albo przez ręczne zmodyfikowanie adresu IP albo przez zaznaczenie pola wyboru DHCP.
9. Wprowadź hasło, aby uaktywnić w systemie ten zmodyfikowany adres IP.

2.2. Konfigurowanie kamery sieciowej via WAN

Założony cel działania:

W tym podrozdziale wyjaśnimy, jak podłączyć kamerę sieciową do sieci WAN z wykorzystaniem adresu statycznego IP / adresu dynamicznego IP.

2.2.1. Podłączenie wykorzystujące statyczny adres IP

Przygotuj na wstępie:

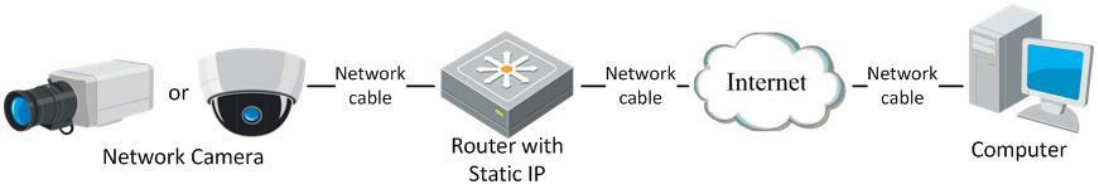
Poniżej prosimy wykorzystać adres statyczny IP, uzyskany od dostawcy internetu (ISP). Dysponując tym adresem statycznym IP, możesz podłączyć tę kamerę sieciową albo via ruter albo bezpośrednio — do sieci WAN.

- **Podłączenie kamery sieciowej (na statycznym IP) — via ruter**

Procedura wykonania:

1. Podłącz kamerę do rutera.
2. Przyporządkuj adres IP sieci LAN, maskę podsieci, bramę sieciową. Skonfigurowanie adresu IP kamery sieciowej – zob. dokładny opis w *podrozdz. 2.1.1* (od str. 12).
3. Zapisz (Save) ten adres statyczny IP w ruterze.

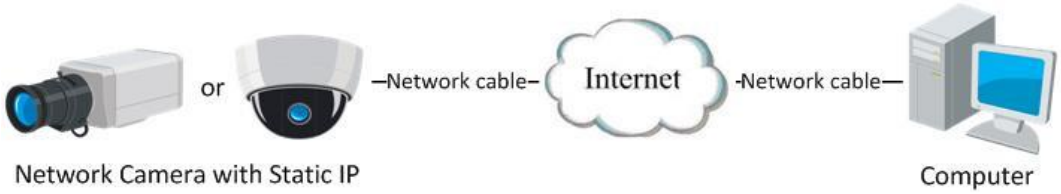
4. Wprowadź mapowanie portów kamery, np. dla portów: 80, 8000, 554. Kroki, pozwalające zmapować porty są zazwyczaj różne dla różnych ruterów (w sprawie mapowania portów należy zadzwonić po pomoc do producenta danego rutera).
   Uwaga: W rozdziale ***Załącznik 2: Mapowanie portów***, str. 165 podajemy przykładowo opis procedury mapowania portów w ruterze marki TP-LINK (model TL-WR641G).
5. Wejdź z przeglądarki internetowej (bądź oprogramowania klienckiego) na stronę Twojej kamery sieciowej.



Rys. 2–10: Uzyskanie dostępu z PC do kamery ze statycznym IP — za pośrednictwem rutera

- **Podłączenie kamery sieciowej (na statycznym IP) — bezpośrednio**

Możesz również zapisać statyczny adres IP w kamerze i podłączyć ją do Internetu bez pośrednictwa dodatkowego urządzenia (rutera), czyli bezpośrednio. Więcej szczegółów o konfigurowaniu adresu IP danej kamery sieciowej — zob. *podrozdz. 2.1.1* (od str. 12).



Rys. 2–11: Uzyskanie dostępu z PC do kamery ze statycznym IP — w sposób bezpośredni

2.2.2. Podłączenie wykorzystujące dynamiczny adres IP

Przygotuj na wstępie:

Poniżej prosimy wykorzystać adres dynamiczny IP, uzyskany od dostawcy Internetu (ISP). Dysponując dynamicznym adresem IP, możesz podłączyć tę kamerę sieciową do modemu bądź rutera.

- **Podłączenie kamery sieciowej za pośrednictwem rutera**

Procedura wykonania:

1. Podłącz Twoją kamerę sieciową do rutera.
2. W kamerze przyporządkuj: adres IP sieci LAN, maskę podsieci, bramę sieciową. Więcej o konfigurowaniu adresu IP danej kamery sieciowej – w podrozdziale 2.1.2.
3. W ruterze wprowadź dla PPPoE: nazwę użytkownika, hasło i potwierdź to hasło.
4. Skonfiguruj mapowanie portów, np. porty: 80, 8000, 554. Kroki, pozwalające zmapować porty są zazwyczaj różne dla różnych ruterów (w sprawie mapowania portów należy zadzwonić po pomoc do producenta danego rutera).

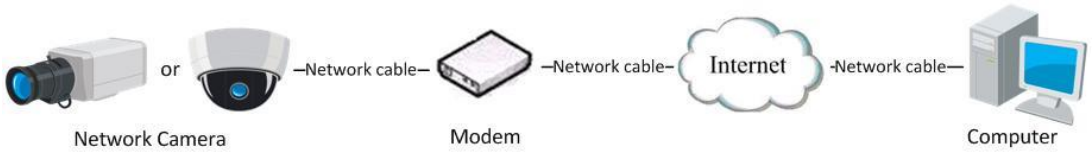
Uwaga: W rozdziale ***Załącznik 2: Mapowanie portów***, str. 165 podajemy przykładowo opis procedury mapowania portów w ruterze marki TP-LINK.

5. Zastosuj nazwę domeny, zawczasu uzyskaną od dostawcy nazw domen (DNP).
6. Odnośnie skonfiguruj ustawienia DDNS w interfejsie konfiguracyjnym rutera.
7. Wywołaj kamerę podając tę nazwę domeny.

- **Podłączenie kamery sieciowej za pośrednictwem modemu**

Cel czynności:

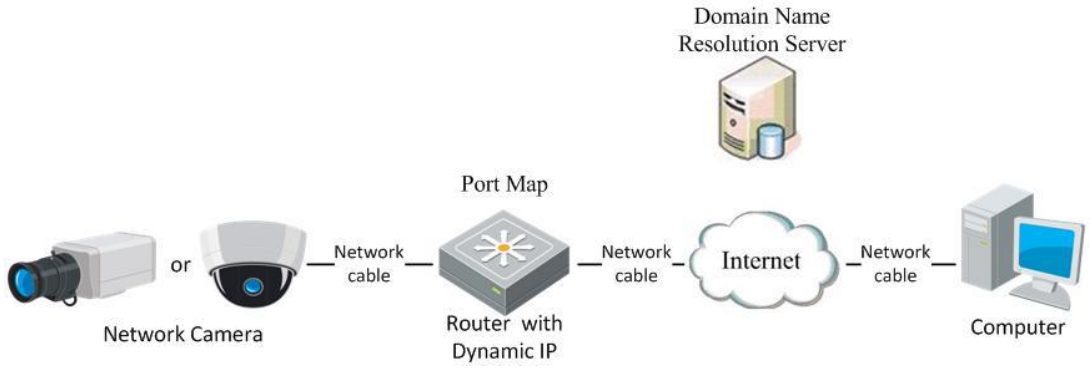
Opisywana kamera obsługuje funkcję automatycznego połączenia wdzwanianego-modemowego PPPoE. Kamera, po podłączeniu do modemu, uzyskuje ogólnodostępny adres IP przez połączenie wdzwonione ADSL. Będziesz musiał skonfigurować parametry PPPoE Twojej kamery sieciowej. Dokładniej o tym — zob. opis w *podrozdz. 6.3.3* ***Konfigurowanie ustawień protokołu PPPoE***, str. 46.



Rys. 2–12: Realizacja dostępu do kamery przy dynamicznym adresie IP

Uwaga: Uzyskany adres IP zostaje dynamicznie przyporządkowany via PPPoE, dlatego adres ten zmienia się na inny, ilekroć nastąpi przeładowanie systemu kamery (reboot). Aby usunąć tę niedogodność z tym zmiennym (dynamicznym) IP, musisz pozyskać nazwę domeny od dostawcy DDNS (np. DynDns.com). Aby pozbyć się problemu, wykonaj poniższe kroki dla uzyskania rozróżnialności bazującej na normalnej nazwie domeny oraz bazującej na prywatnej nazwie domeny.

♦ Sieciowa rozróżnialność z wykorzystaniem NORMALNEJ NAZWY DOMENY

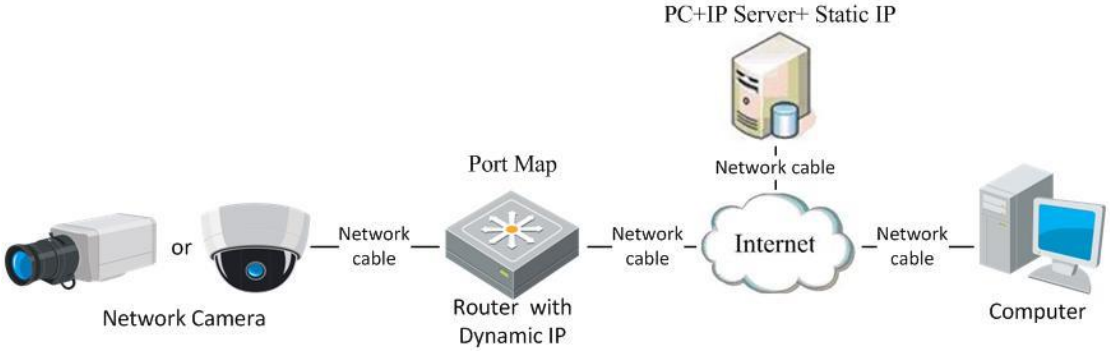


Rys. 2–13: Uzyskanie rozróżnialności sieciowej przez użycie normalnej nazwy domeny

Procedura wykonania:

1. Zastosuj tu nazwę domeny, którą uzyskałeś od dostawcy nazw domen.
2. Wprowadź ustawienia DDNS w interfejsie ustawień **DDNS Settings** należących do tej kamery sieciowej — szczegółowy opis wprowadzania tych ustawień podajemy w *podrozdz. 6.3.4* ***Konfigurowanie ustawień DDNS***, str. 47.
3. Wywołaj kamerę używając zastosowanej nazwy domeny.

♦ Sieciowa rozróżnialność urządzeń z wykorzystaniem PRYWATNEJ NAZWY DOMENY



Rys. 2–14: Uzyskanie rozróżnialności sieciowej przez użycie prywatnej nazwy domeny

Procedura wykonania:

1. Zainstaluj oprogramowanie IP-serwera na komputerze, mającym statyczny adres sieciowy IP. I uruchom je.
2. Wywołaj kamerę sieciową przez sieć LAN z przeglądarki internetowej lub oprogramowania klienckiego.
3. Załącz w ustawieniach kamery pole wyboru **Enable DDNS** oraz wybierz **IP Server** jako rodzaj protokołu komunikacyjnego.[3] Szczegółowy opis konfigurowania tych ustawień znajdziesz w *podrozdz. 6.3.4* ***Konfigurowanie ustawień DDNS***, str. 47.

[3] (tzn. DDNS Type = IP Server) — przyp. tłum.

3. Uzyskanie dostępu do kamery sieciowej

3.1. Dostęp z poziomu przeglądarki internetowej

Procedura wykonania:

1. Uruchom Twoją przeglądarkę internetową.
2. W polu adresów sieciowych tej przeglądarki wprowadź adres IP Twojej kamery sieciowej, następnie naciśnij klawisz **Enter**, aby wejść w interfejs logowania.
3. Uaktywnij tę kamerę sieciową (tylko przy pierwszym użyciu). Szczegółowy opis uaktywniania — zob. w *podrozdz. 2.1.2* ***Zdefiniowanie hasła dostępowego***, str. 13.

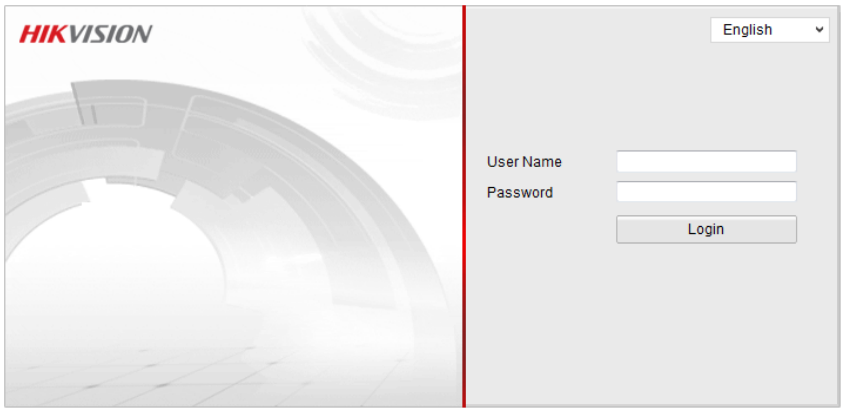
   Uwagi:

   - Domyślnym adresem IP tej kamery sieciowej jest: **192.168.1.64**.
   - Jeśli potrzebna kamera nie została jeszcze uaktywniona, to należy ją najpierw uaktywnić, jak podane w *podrozdz. 3.1* (str. 23) lub *podrozdz. 3.2* (str. 25).
4. Z listy rozwijalnej u góry po prawej stronie okna logowania wybierz opcję **English** jako język interfejsu użytkownika.
5. Wpisz nazwę użytkownika (w polu **User Name**) i hasło (w polu **Password**) Login.

Użytkownik z uprawnieniami poziomu *admin* powinien zawczasu założyć i skonfigurować konta użytkowników kamery poziomu *user* lub *operator*, przydzielając im odpowiednie zezwolenia. (Skasuj niepotrzebne konta użytkowników, odłącz niepotrzebne zezwolenia dostępowe użytkownikom *user/operator*.)

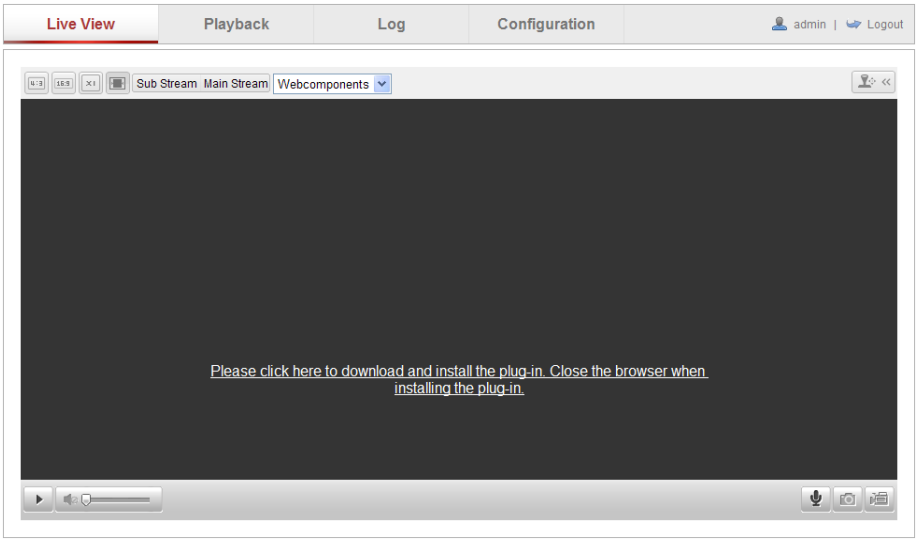
Uwaga – pamiętaj:

Dostęp do wywoływanego adresu IP ulegnie zablokowaniu (locked), jeśli użytkownik o randze *admin* wykona **7** (siedem) nieudanych prób wprowadzenia hasła dostępowego [to samo po **5** (pięciu) nieudanych próbach użytkownika rangi *user/operator*].

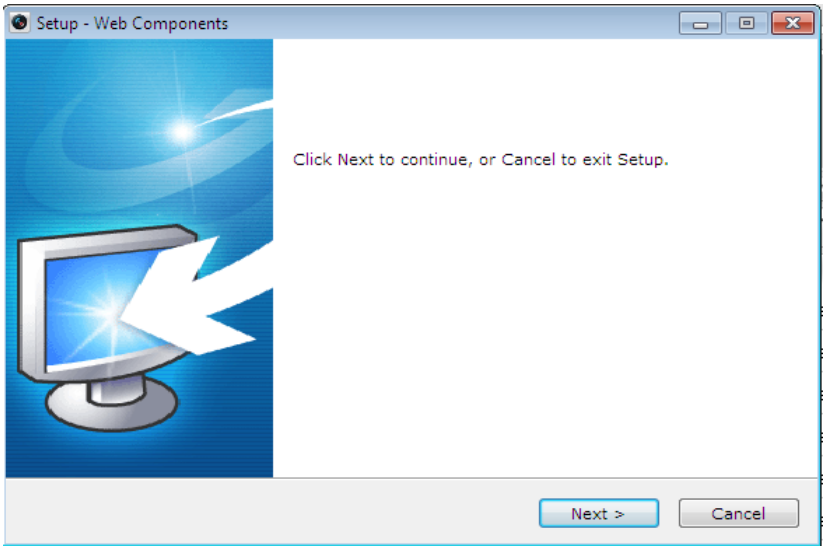


Rys. 3–1: Interfejs logowania do obsługi tej kamery sieciowej

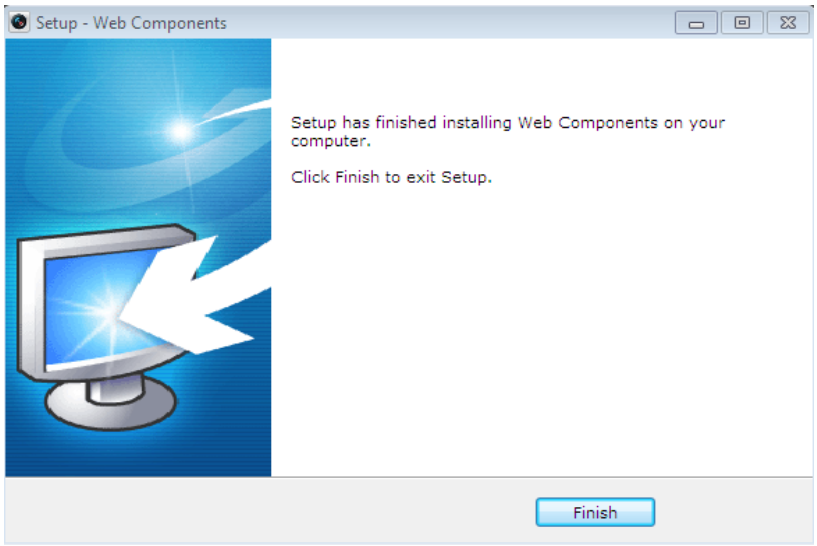
6. Zainstaluj odpowiedni moduł funkcjonalności (dalej krótko: *plug-in*), aby można było uzyskać podgląd bieżący z kamery oraz aby można było kamerą sterować. Aby zainstalować plug-in, postępuj zgodnie z instrukcjami wyświetlanymi kolejno w interfejsie ekranowym.



Rys. 3–2: Pobierz plug-in z sieci i zainstaluj go (aby umożliwić podgląd/obsługę kamery) Kliknij w link „**Please click here to download and install the plug-in…**” na tle ekranu.



Rys. 3–3: Instalacja plug-inu (krok nr **1**)

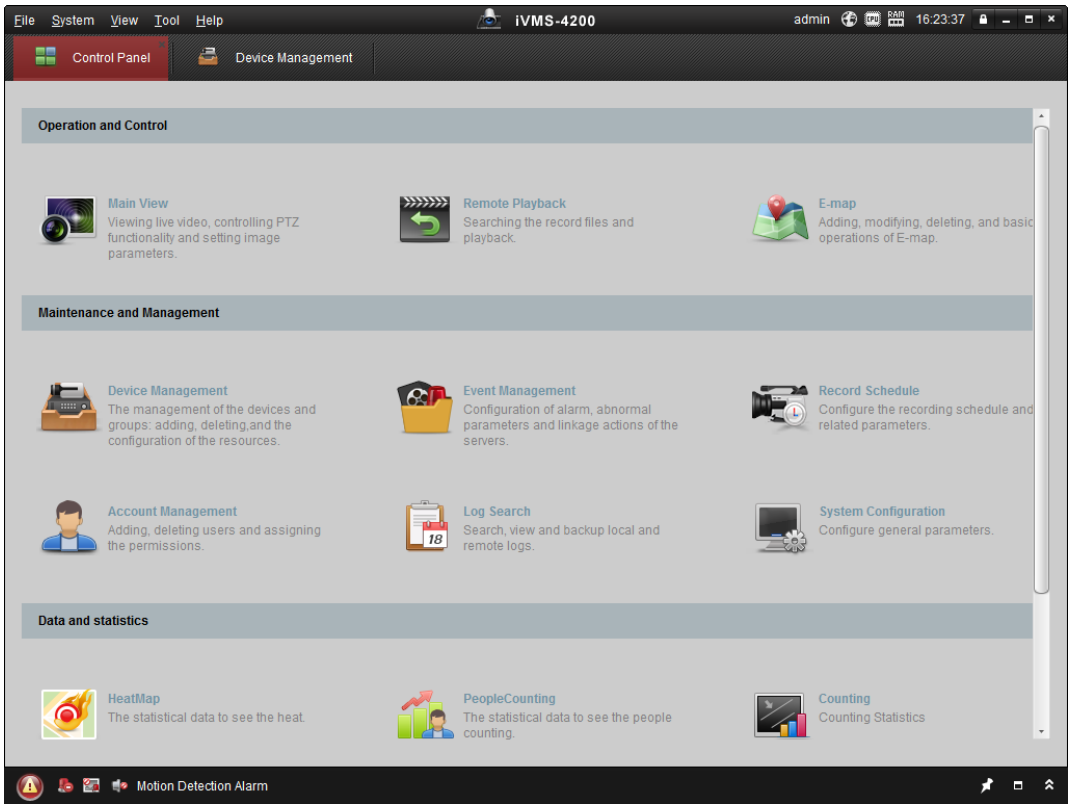


Rys. 3–4: Instalowanie plug-inu (krok nr **2**)

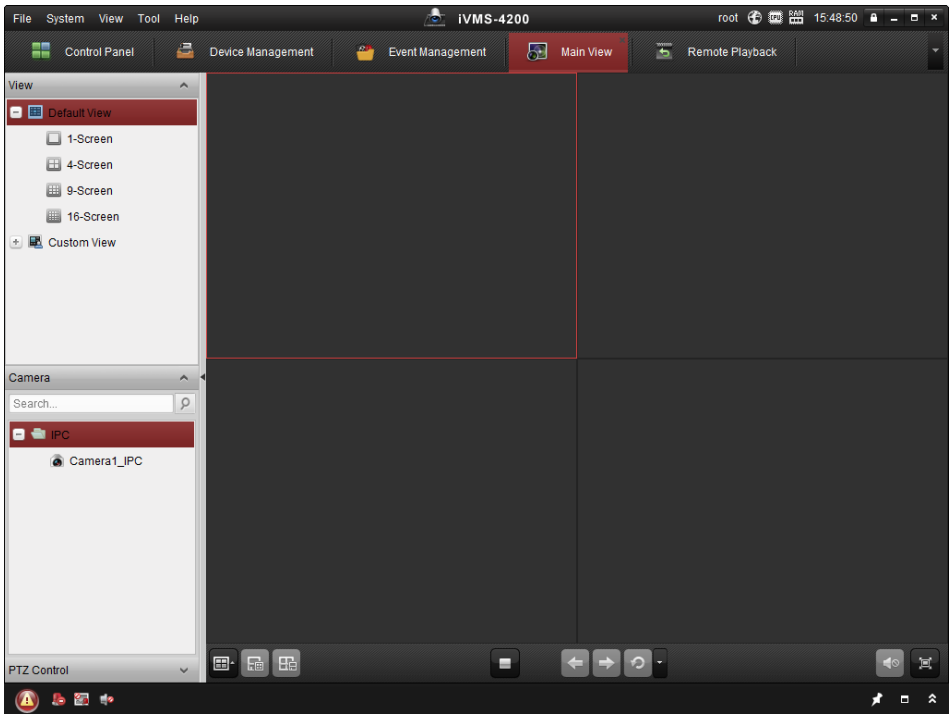
Uwaga: Być może będziesz musiał zamknąć swoją przeglądarkę internetową, aby dało się zainstalować plug-in. Dlatego po zainstalowaniu plug-inu zamknij i ponownie uruchom swoją przeglądarkę i ponownie zaloguj się w systemie kamery.

3.2. Dostęp z poziomu oprogramowania klienckiego

Na płycie CD, towarzyszącej produktowi/kamerze, jest wersja instalacyjna oprogramowania klienckiego *iVMS-4200*. Za pomocą tej aplikacji operator może wyświetlać podgląd bieżący kamery oraz może zarządzać kamerą.
W celu zainstalowania tego oprogramowania postępuj zgodnie z instrukcjami kolejno pojawiającymi się na ekranie podczas instalacji.
W tym oprogramowaniu dostępny jest m.in. główny panel sterujący oraz interfejs wyświetlający podgląd z kamery — prezentujemy je na kolejnych ilustracjach poniżej:



Rys. 3–5: Panel sterujący oprogramowania iVMS-4200



Rys. 3–6: Podstawowy ekran oprogramowania iVMS-4200

Uwaga: Szczegółowe informacje o tym oprogramowaniu znajdują się w *instrukcji użytkownika* od pakietu ***iVMS-4200***.

4. Ustawienia komunikacji Wi-Fi

Cel czynności:

Dzięki przyłączeniu urządzenia do sieci bezprzewodowej nie musisz używać żadnych przewodów elektrycznych, aby utworzyć połączenie kamery z siecią — jest to bardzo praktyczne w zadaniach nadzorczych realizowanych w rzeczywistości.

Uwaga: Niniejszy rozdział ma zastosowanie wyłącznie do kamer z wbudowanym modułem do komunikacji Wi-Fi.

4.1. Konfigurowanie połączenia Wi-Fi w trybach „Manager” i „Ad-hoc”

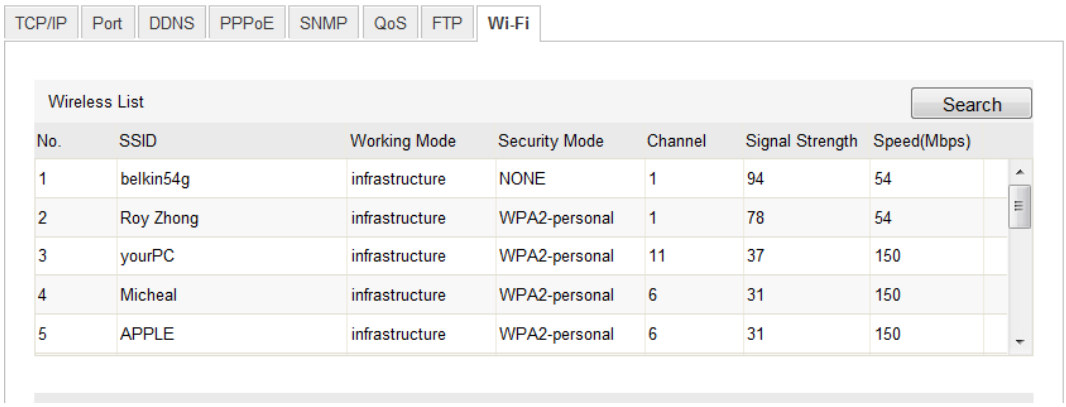
Przygotuj na wstępie:

Musisz mieć skonfigurowana Twoją sieć łączności bezprzewodowej (Wi-Fi).

Połączenie sieciowe bezprzewodowe — w trybie *Manager*

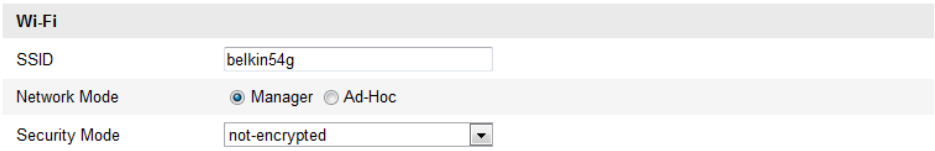
Procedura wykonania:

1. Wyświetl interfejs ekranowy kamery do konfigurowania komunikacji Wi-Fi (zakładka Wi-Fi), przejdź w tym celu kolejno po ścieżce:
   Configuration > Advanced Configuration > Network > Wi-Fi



Rys. 4–1: Lista dostępnych sieci bezprzewodowych — interfejs ustawień Wi-Fi w kamerze

2. Kliknij przycisk **Search**, aby wyszukać dostępne (=stan online) możliwości uzyskania połączenia bezprzewodowego.
3. W wyświetlonej w ten sposób liście połączeń Wireless List kliknij żądane połączenie bezprzewodowe (aby je wybrać do dalszego konfigurowania).



Rys. 4–2: Ustawienia wybranego połączenia bezprzewodowego Wi-Fi

4. Zaznacz w polu Network Mode radio-przycisk wyboru opcji Manager — wtedy w polu listy rozwijalnej Security Mode automatycznie wyświetli się tryb zabezpieczenia tej sieci (kiedy zostaje wybierana sieć bezprzewodowa). Prosimy nie edytować tego ustawienia ręcznie.

Uwaga: Te parametry są dokładnie takie same jak te od pośredniczącego rutera.

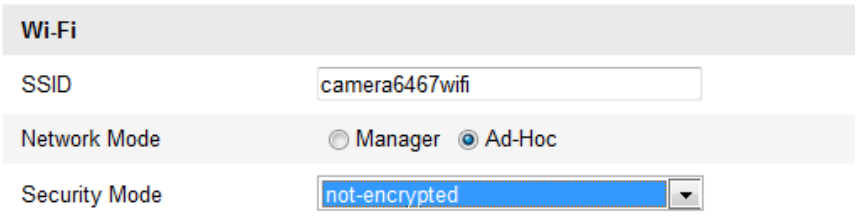
5. Wprowadź klucz (key) dla zrealizowania połączenia z tą wybraną siecią bezprzewodową. Kluczem powinien być ten key od bezprzewodowego połączenia sieciowego, które skonfigurowałeś w ruterze.

Połączenie sieciowe bezprzewodowe — w trybie ‘Ad-Hoc’

Jeśli powyżej wybierzesz opcję Ad-Hoc jako tryb sieciowy, to nie będziesz musiał łączyć się z kamerą bezprzewodową z przejściem przez ruter.
Scenariusz postępowania jest identyczny z tym, gdy łączysz kamerę z komputerem za pomocą przewodów, bezpośrednio.

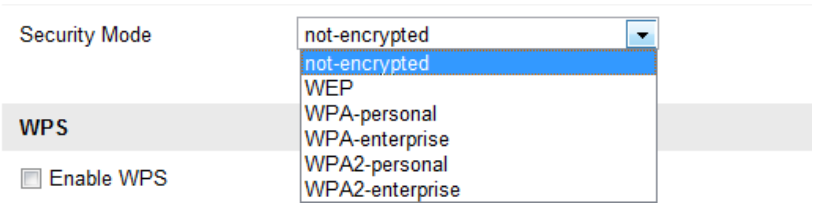
Procedura wykonania:

1. W Network Mode kliknij radio-przycisk wyboru opcji Ad-Hoc:



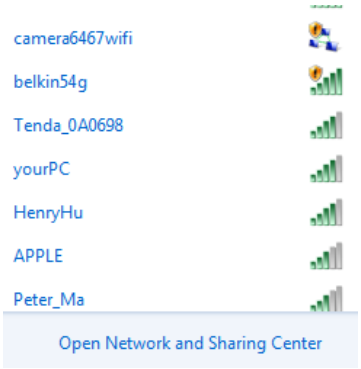
Rys. 4–3: Ustawienia łączności bezprzewodowej Wi-Fi — wybranie trybu sieci: ‘Ad-hoc’

2. Wprowadź jakiś własny SSID jako identyfikator tej kamery bezprzewodowej.
3. Z listy rozwijalnej Security Mode wybierz żądany tryb zabezpieczenia (dla tego połączenia bezprzewodowego).



Rys. 4–4: Wybór zabezpieczenia łączności bezprzewodowej — tryb sieci Ad-hoc

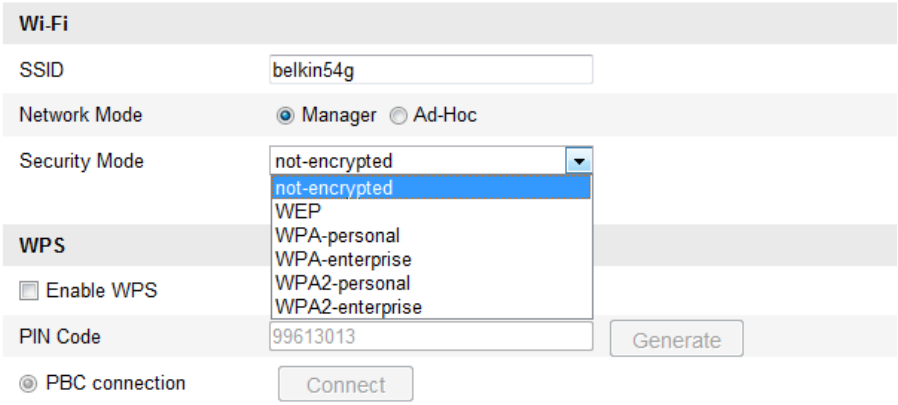
4. Uaktywnij funkcjonowanie łączności bezprzewodowej w Twoim PC.
5. Po stronie tego PC: Przeszukaj sieci i zobaczysz w jednej z pozycji (zob. lista na ilustracji poniżej) wcześniej wpisane SSID kamery:



Rys. 4–5: Punkt łączności dla trybu sieciowego Ad-Hoc

6. Wybierz to SSID i połącz się (z nim).

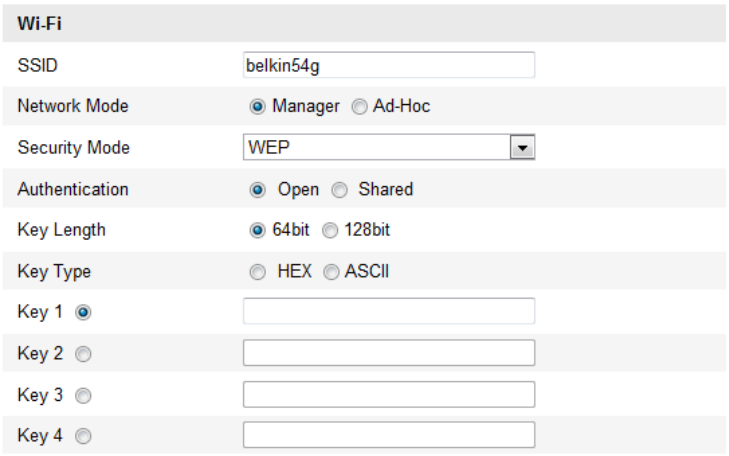
Opis dostępnych trybów zabezpieczenia ('Security Mode'):



Rys. 4–6: Dostępne opcje wybierające tryb zabezpieczenia łączności (**Security Mode**)

Jako tryb zabezpieczenia łączności możesz wybrać jeden z następujących: **not-encrypted** (bez szyfrowania), **WEP**, **WPA-personal**, **WPA-enterprise**, **WPA2-personal**, **WPA2-enterprise**.

♦Tryb zabezpieczenia: **WEP**:



Rys. 4–7: Tryb zabezpieczenia łączności WEP

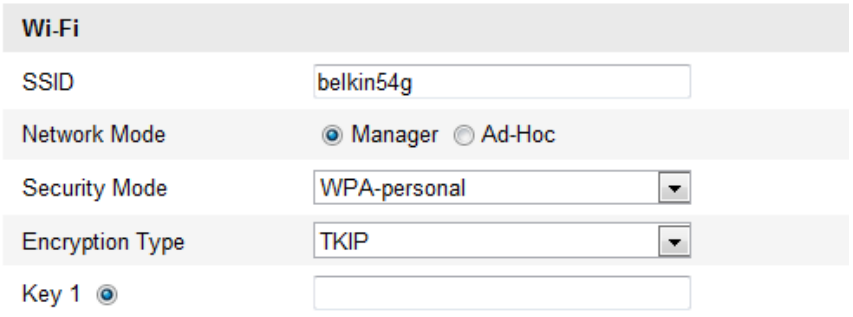
- **Authentication** (metoda uwierzytelnienia użytkownika) — Wybierz opcję **Open** lub opcję **Shared Key System Authentication** w zależności od metody stosowanej przez Twój sieciowy punkt dostępowy. Nie wszystkie punkty dostępowe mają tę opcję i w takich przypadkach najprawdopodobniej wykorzystują technikę Systemu Otwartego (Open System), która czasem nazywana jest uwierzytelnieniem SSID.
- **Key length** (długość klucza) — Tą opcją ustawiasz długość klucza zastosowanego do szyfrowania łączności bezprzewodowej: **64** bity lub **128** bitów. Możesz napotkać zapis długości klucza szyfrującego w postaci: 40/64 oraz 104/128.
- **Key type** (rodzaj klucza) — Rodzaje dostępnych kluczy zależą od konkretnie wykorzystywanego punktu dostępowego. W tym polu możliwe są następujące ustawienia:

  HEX – ta opcja pozwoli ręcznie wprowadzić klucz w zapisie szesnastkowym.

  ASCII – używając tej metody, musisz wprowadzić ciąg znakowy o długości dokładnie 5 znaków dla 64-bitowego WEP bądź 13 znaków dla 128-bitowego WEP.

♦Tryby zabezpieczenia: **WPA-personal** i **WPA2-personal**:

Wprowadź wymagany dla tego punku dostępowego **Pre-shared Key**, którym może być liczba w notacji szesnastkowej (hex) albo ciąg znaków hasła (tzw. *fraza hasłowa*).

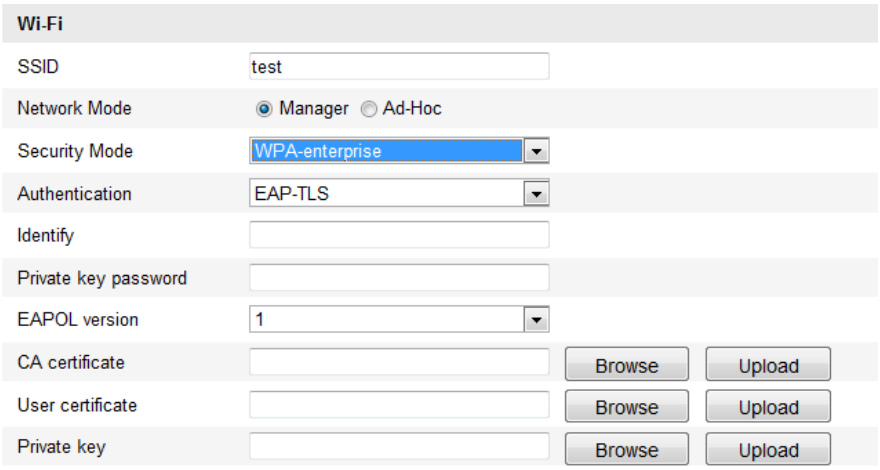


Rys. 4–8: Tryb zabezpieczenia łączności: **WPA-personal**

♦Tryby zabezpieczenia: **WPA-enterprise** i **WPA2-enterprise**:

Wybierz rodzaj uwierzytelniania klient/serwer, wykorzystywany w tym punkcie dostępowym: **EAP-TLS** lub **EAP-PEAP**.

– *Uwierzytelnianie metodą* **EAP-TLS**:



Rys. 4–9: Wybranie metody uwierzytelniania (**Authentication**): EAP-TLS

- **Identify** – Wpisz tu ID użytkownika, które ma być przedstawiane sieci.
- **Private key password** – Wpisz tu hasło pasujące do ID użytkownika.
- **EAPOL version** – Wybierz nr wersji (**1** lub **2**), wykorzystywanej w Twoim punkcie dostępowym.
- **CA Certificate** – Wyślij przez upload certyfikat CA, który ma być przedstawiany w punkcie dostępowym w celu uwierzytelnienia użytkownika.
- – *Uwierzytelnianie metodą* EAP-PEAP:
- **User Name** – Wpisz tu nazwę użytkownika, która ma być przedstawiana sieci.
- **Password** – Wpisz tu hasło sieci.
- **PEAP Version** – Wybierz wersję PEAP, która jest wykorzystywana w tym punkcie dostępowym.
- **Label** – Wybierz etykietę, wykorzystywaną przez ten punkt dostępowy.
- **EAPOL version** – Wybierz nr wersji (**1** lub **2**) wykorzystywany w Twoim punkcie dostępowym.
- **CA Certificate** – Wyślij (upload) certyfikat CA, który ma być przedstawiany w punkcie dostępowym w celu uwierzytelnienia użytkownika.

- *Dla ochrony Twojej własnej prywatności oraz dla lepszej ochrony Twojego systemu od źródeł zagrożeń sieciowych zdecydowanie zalecamy zastosowanie* ***silnych haseł*** *do wszystkich funkcji i urządzeń sieciowych. Hasło takie powinno być czymś, co samemu sobie wybierzesz, (powinno być w nim minimum 8 znaków, w tym co najmniej trzy z następujących kategorii znakowych: litery wielkie, litery małe, cyfry, znaki specjalne), aby podnieść poziom zabezpieczenia Twojego produktu (kamery).*

- *Odpowiedzialność za właściwe skonfigurowanie wszystkich haseł i innych nastaw zabezpieczających spoczywa na instalatorze oraz/lub użytkowniku końcowym (tj. konsumencie/odbiorcy) instalowanego rozwiązania.*

4.2. Łatwa łączność Wi-Fi dzięki funkcji WPS

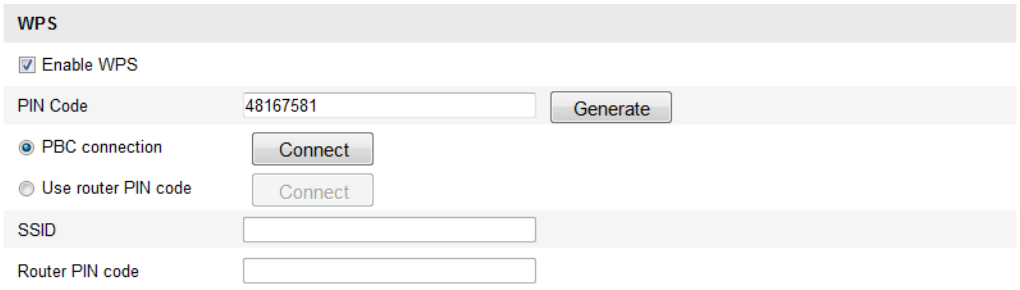
Cel czynności:

Wprowadzenie ustawień konfigurujących łączność przez sieć bezprzewodową nigdy nie jest czymś łatwym. Aby uniknąć dużej złożoności konfigurowania łączności bezprzewodowej, możesz załączyć w ustawieniach urządzenia funkcję WPS.

Termin **WPS**[4] oznacza zasadniczo funkcję łatwego konfigurowania łączności szyfrowanej, pomiędzy interesującym urządzeniem a ruterem bezprzewodowym. Funkcja WPS ułatwia dodawanie nowych urządzeń do istniejącej sieci bez potrzeby wprowadzania długich fraz hasłowych. Istnieją dwa opisane niżej tryby realizowania połączeń WPS – są to: tryb **PBC** oraz tryb **PIN**.

Uwaga: Kiedy załączysz w ustawieniach kamery funkcję WPS (pole wyboru **Enable WPS**), nie będziesz musiał konfigurować parametrów takich jak np. rodzaj szyfrowania, a ponadto nie potrzebujesz znać klucza do połączeń bezprzewodowych.

Procedura wykonania:



Rys. 4–10: Ustawienia łączności bezprzewodowej **Wi-Fi**: załączenie funkcji WPS

♦ Tryb **PBC**:

Skrót ‘**PBC**’ (Push-Button-Configuration) = *Konfiguracja-za-Naciśnięciem-Przycisku*. Ten tryb konfigurowania polega na tym, że użytkownik po prostu musi nacisnąć przycisk, rzeczywisty lub wirtualny (jak np. przycisk Connect w interfejsie konfiguracyjnym przeglądarki internetowej IE), zarówno w Punkcie Dostępowym (i u Rejestratora sieci), jak i w nowym urządzeniu-kliencie sieci bezprzewodowej.

1. Zaznacz pole wyboru Enable WPS, aby załączyć funkcję WPS.
2. Wybierz **PBC connection** jako tryb połączenia:

[4] WPS = **W**i-Fi **P**rotected **S**etup (chronione konfigurowanie łączności Wi-Fi) — przyp. tłum.

Uwaga: Ten tryb musi być obsługiwany zarówno przez Punkty Dostępowe, jak i urządzenia łącznikowe.

3. Zobacz w ruterze Wi-Fi, czy ma może przycisk opisany '**WPS**'. Jeśli ma, to naciśnij go teraz — wtedy zobaczysz, że kontrolka wskaźnikowa obok przycisku zaczęła migać, co wskazuje, że załączyłeś w ruterze funkcję WPS. Więcej o obsłudze rutera (w kontekście tej funkcji) znajdziesz w jego instrukcji użytkownika.
4. Naciśnij przycisk funkcji **WPS**, aby załączyć funkcję WPS w kamerze.
   Gdyby w kamerze nie było przycisku **WPS**, to możesz równie dobrze kliknąć przycisk wirtualny w interfejsie przeglądarki, aby uruchomić funkcję PBC:
5. Kliknij więc przycisk **Connect**:

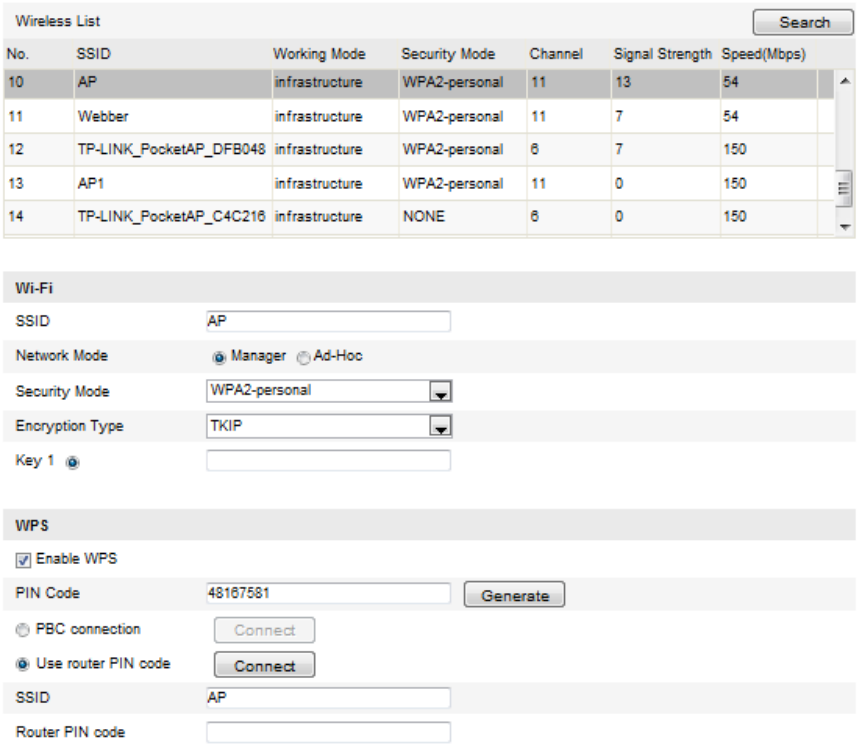
Gdy tryb PBC zostanie uaktywniony i w ruterze, i w kamerze, to nastąpi automatyczne nawiązanie połączenia kamery bezprzewodowej z siecią bezprzewodową.

♦ Tryb **PIN**:

Tryb PIN wymaga odczytania numeru PIN (***P**ersonal **I**dentification **N**umber*) albo z nalepki albo z wyświetlacza w nowym urządzeniu bezprzewodowym. Numer ten (PIN) trzeba następnie wprowadzić w ustawieniach (zob. niżej), aby połączyć to urządzenie z siecią, zwykle z Punktem Dostępowym tej sieci.

Procedura wykonania:

1. Z listy Wireless List wybierz żądane połączenie bezprzewodowe; widać SSID.



Rys. 4–11: Ustawienia łączności bezprzewodowej Wi-Fi: użycie trybu dla funkcji WPS

2. Zaznacz pole wyboru **Use router PIN code**.
   Jeśli kod PIN zostaje wygenerowany po stronie rutera, to w polu **Router PIN code** musisz wprowadzić ten kod PIN, który uzyskasz po stronie rutera.
3. Kliknij przycisk **Connect**.
   albo ewentualnie:
   Możesz też wygenerować kod PIN po stronie kamery. Czas przeterminowania ważności takiego kodu PIN wynosi: 120 s. W celu wygenerowania tego kodu:
   A) Kliknij przycisk **Generate**.

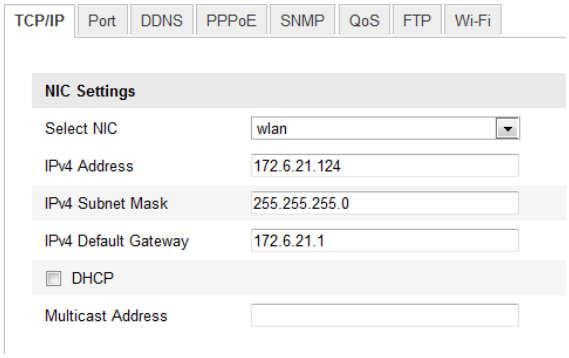
   B) Kod zwrócony w odpowiedzi (w polu **PIN Code**) wprowadź do rutera. W tym przykładzie musisz wprowadzić do rutera kod: **48167581**.

4.3. Ustawienia własności adresu IP dla połączeń przez sieci bezprzewodowe

Domyślnym adresem IP sterownika NIC (sieć bezprzewodowa) jest: **192.168.1.64**.
Gdy podłączysz sieć bezprzewodową, możesz zmienić ten domyślny adres IP.

Procedura wykonania:

1. Wyświetl interfejs ekranowy, służący do konfigurowania ustawień TCP/IP.
   Configuration > Advanced Configuration > Network > TCP/IP
   albo też:
   Configuration > Basic Configuration > Network > TCP/IP



Rys. 4–12: Ustawienia TCP/IP

2. Z listy rozwijalnej **Select NIC** wybierz ‘**wlan**’ jako NIC.
3. Wprowadź wg własnych potrzeb: adres IPv4 (**IPv4 Address**), maskę podsieci IPv4 (**IPv4 Subnet Mask**) oraz domyślną bramę IPv4 (**IPv4 Default Gateway**).

Procedura konfigurowania ustawień jest identyczna jak dla sieci LAN.
Jeśli chcesz uzyskać przyporządkowany adres IP, to możesz zaznaczyć pole wyboru **DHCP**, aby włączyć funkcjonalność DHCP.

5. Podgląd bieżący kamery

5.1. Strona podglądu bieżącego

Cel czynności:

Na stronie podglądu bieżącego możesz:

• wyświetlać obraz z kamery w czasie rzeczywistym (tj. podgląd bieżący),

• zapisywać klatki i obraz kamery,

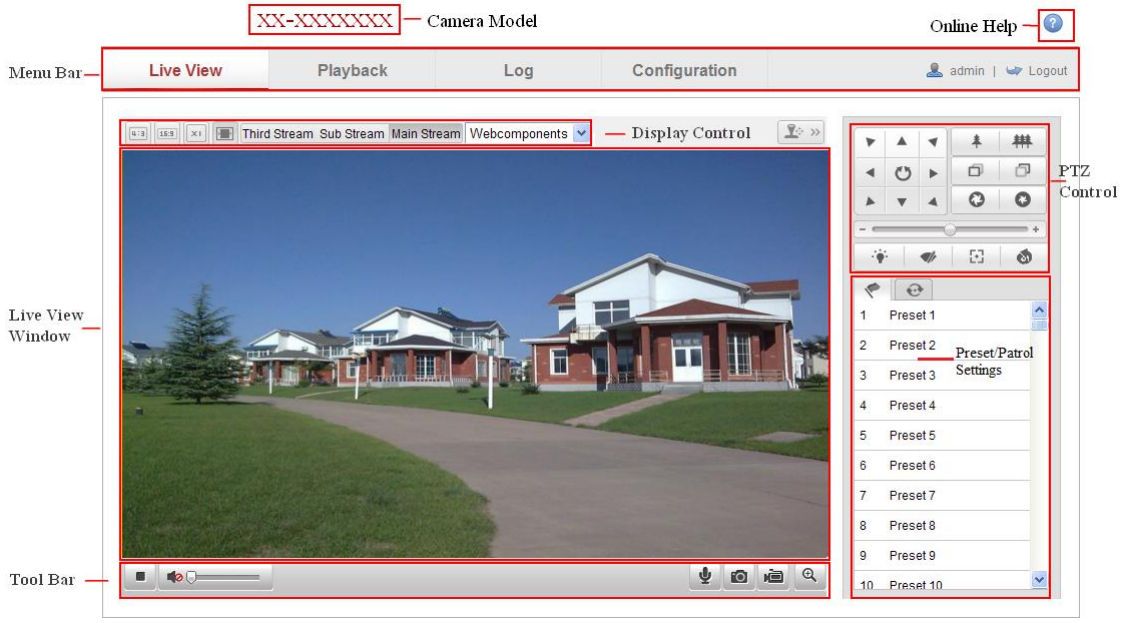
• sterować kamerą (akcje PTZ),

• programować i wywoływać presety obserwacyjne kamery, oraz

• ustawiać parametry obrazu.

Aby wejść na stronę podglądu bieżącego, zaloguj się w Twojej kamerze sieciowej, albo — jeśli masz już wyświetloną stronę główną interfejsu kamery — kliknij przycisk **Live View** na głównej listwie menu.

♦ **Opis elementów widocznych na stronie podglądu bieżącego:**



Rys. 5–1: Strona podglądu bieżącego kamery

Model kamery (Camera Model**):**

W tym polu wyświetla się model kamery sieciowej, z którą się łączysz.

Pomoc dostępna online (Online Help**):**

Kliknij , aby wejść w pomoc dostępną z sieci (=online), która przeprowadzi Cię przez podstawowe czynności dla każdej dostępnej funkcji.

Główna listwa menu (Menu Bar**):**

Kliknij daną zakładkę w tej listwie, aby wejść odpowiednio na stronę: podglądu bieżącego (**Live View**), odtwarzania obrazu zarejestrowanego (**Playback**), logu (**Log**) oraz konfigurowania (**Configuration**).

Regulatory wyświetlania (Display Control**):**

Kliknij daną zakładkę, aby dobrać żądane: layout wyświetlania i rodzaj strumienia źródłowego dla podglądu bieżącego. Możesz też kliknąć przycisk rozwijający listę rozwijalną, aby wybrać żądaną wtyczkę (=plug-in). Jeśli korzystasz z przeglądarki Internet Explorer (IE), to możesz z listy wybrać: różne web-komponenty oraz wtyczkę Quick-Time'u. Jeśli używasz jakiejś innej przeglądarki niż IE, to w liście są do wyboru: różne web-Komponenty, wtyczka Quick-Time'u, a także wtyczka VLC / MJPEG (o ile są obsługiwane przez tę konkretną przeglądarkę).

Okno podglądu bieżącego (Live View Window**)**:

Na powierzchni tego panelu wyświetla się podgląd bieżący z kamery.

Pasek narzędziowy (Toolbar**)**:

Znajdujące się tu elementy sterujące służą do operowania na podglądzie bieżącym kamery, np. uruchom podgląd bieżący z kamery, zapisz fotozrzut[5], nagrywaj obraz, włącz/wyłącz dźwięk, uruchom transmisję dźwięku w obu kierunkach, itd.

Regulatory akcji sterujących PTZ (PTZ Control**)**:

Te elementy pozwalają sterować kamerą: obracaj poziomo (=panoramuj), obracaj pionowo (=pochylaj/odchylaj), zbliżaj scenę (=zoom), a także przełącz IR-reflektor i włącz/wyłącz wycieraczkę. (Opcje te dostępne są jednak tylko w kamerach wyposażonych technicznie w funkcjonalność PTZ.)

Ustawienia presetów/patroli (Preset/Patrol Settings**)**:

Tu możesz: zdefiniować/wywołać/skasować presety lub patrole (dotyczy tylko kamer obrotowo-zoomujących PTZ).

5.2. Uruchomienie podglądu bieżącego

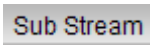
W oknie podglądu obrazu bieżącego z kamery kliknij na pasku narzędzi przycisk , aby uruchomić wyświetlanie podglądu bieżącego z kamery:

Rys. 5–2: Pasek narzędzi sterujących podglądem bieżącym

Tabela 1: Objaśnienia elementów pasku narzędziowym

Ikonka	Funkcja
/	Uruchom/Zatrzymaj wyświetlanie podglądu bieżącego.
	Proporcje wymiarów okna: 4:3.
	Proporcje wymiarów okna: 16:9.

[5] fotozrzut = klatka obrazu wychwycona/zarejestrowana z podglądu kamery — przyp. tłum.

	Przywróć pierwotne wymiary okna.
	Dobierz wymiary okna automatycznie (adaptacyjnie).
	Podgląd bieżący ze strumienia głównego.
	Podgląd bieżący z pod-strumienia.
	Podgląd bieżący ze strumienia trzeciego.
	Kliknij tu, aby wybrać wtyczkę od innego/obcego dostawcy.
	Ręcznie zapisz klatkę obrazu kamery (=fotozrzut).
	Ręcznie uruchom/zatrzymaj nagrywanie obrazu kamery.
	Włącz fonię kamery & wyreguluj głośność / wycisz fonię do zera.
	Włącz mikrofon / wyłącz mikrofon.
	Włącz / wyłącz funkcję cyfrowego zbliżenia sceny.
	Włącz / wyłącz funkcję pozycjonowania w 3 wymiarach (3D).

Uwaga: Użycie ww. funkcji [wyświetlaj Third Stream] oraz [pozycjonowanie 3D] wymaga ich technicznej dostępności w kamerze.

5.3. Ręczne nagrywanie ciągłe | ręczny fotozrzut klatek

W interfejsie ekranowym podglądu bieżącego kliknij przycisk  , aby ręcznie zapisać klatkę z podglądu bieżącego kamery (tworzy plik fotozrzutu) albo kliknij stamtąd przycisk  , aby ręcznie rozpocząć nagrywanie ciągłe podglądu bieżącego kamery (tworzy plik wideonagrania).
Ścieżkę zapisu ww. plików fotozrzutu i ww. plików wideonagrań możesz zadać na stronie otwieranej ciągiem poleceń: **Configuration > Local Configuration**.
***Uwaga*:** Klatka obrazu uzyskana przez ręczny fotozrzut zostaje zapisana w pliku JPEG / BMP na Twoim komputerze.

Jeśli potrzebujesz zdalnego rejestrowania obrazu sterowanego czasem (harmonogram), to opis jego konfigurowania znajdziesz w *podrozdz. 7.2*, str. 132.

5.4. Obsługa akcji sterujących PTZ

Cel czynności:
W interfejsie podglądu bieżącego kamery za pomocą przycisków z panelu akcji sterujących PTZ możesz uruchomić różne operacje sterujące kamerą – panoramowanie / pochylanie / zbliżenia.

Pamiętaj: Aby wykonać ww. akcje sterujące PTZ, kamera (podłączona do sieci) musi umieć obsłużyć wywoływaną funkcję sterowania PTZ wzgl. musi mieć zainstalowaną jednostkę obrotową P/T. Pamiętaj też, by prawidłowo ustawić parametry PTZ kamery na stronie ustawień RS-485 — zob. *podrozdz. 11.9* ***Ustawienia portu RS-485***, str. 160.

5.4.1. Panel akcji sterujących PTZ

Na stronie podglądu bieżącego kliknij przycisk  , aby wyświetlić panel sterujący PTZ, albo kliknij przycisk  , aby panel ten zgasić.
Klikając przyciski kierunkowe w ww. panelu PTZ sterujesz obrotami P/T kamery:

Rys. 5–3: Panel sterujący PTZ

Klikając w panelu sterującym PTZ przyciski zbliżania / regulacji otworu przysłony / przestawiania ostrości możesz sterować funkcjami obiektywu.

Uwagi:

- W oknie podglądu bieżącego jest w sumie możliwych 8 różnych strzałek, wskazujących kierunek ruchu kamery (△,▽,◁, ▷,▽,◁,△,◁) — są wyświetlane, gdy klikniesz-i-pociągniesz myszką po podglądzie w danym kierunku.
- W kamerach, które potrafią obsługiwać tylko regulacje obiektywu kamery, ww. przyciski kierunkowe nie zadziałają.

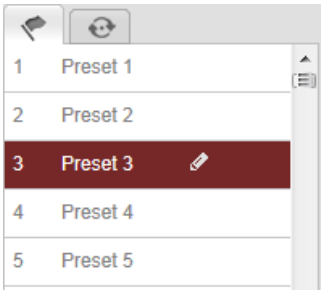
Tabela **2**: Objaśnienia elementów Panelu Sterowania PTZ

Ikonka	Funkcja
	Przybliż / Oddal scenę
	Przestaw ostrość Bliżej / Dalej w scenie
	Rozewrzyj / przymknij przysłonę
	Reflektor włącz / wyłącz
	Wycieraczkę włącz / wyłącz
	Ostrzenie pomocnicze (na żądanie)
	Zainicjalizuj obiektyw
	Wyreguluj szybkość obracania P/T

5.4.2. Definiowanie / wywoływanie presetów

- **Zdefiniowanie presetu obserwacyjnego (=widoku stałego):**

1. W panelu sterującym PTZ wybierz z listy presetów preset o żądanym numerze:



Rys. 5–4: Definiowanie presetu obserwacyjnego dla kamery

2. Przyciskami sterującymi z panelu PTZ przestaw obiektyw na żądaną pozycję obserwacji otoczenia.
   • Obróć kamerę w prawo / w lewo.
   • Pochyl kamerę w dół / odchyl ją do góry.
   • Zbliż / oddal widok sceny.
   • Zmień plan ostry w scenie na bliższy / dalszy.
3. Kliknij przycisk , aby zakończyć definiowanie aktualnego presetu.
4. Ewentualnie możesz też kliknąć przycisk , aby skasować zdefiniowany preset.

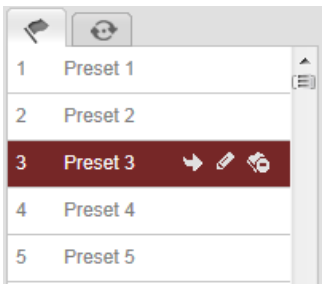
***Uwaga*:** W kamerach sieciowych *Network Mini PT Camera* możesz skonfigurować maks. 16 presetów.

- **Wywołanie presetu obserwacyjnego:**

Dzięki tej funkcji kamera może zostać skierowana na zdefiniowaną wcześniej scenę (widok) za pomocą akcji ręcznej operatora albo w reakcji na wystąpienie określonego zdarzenia.

Jeśli masz zdefiniowany preset obserwacyjny, to możesz w dowolnej chwili zażądać od kamery (=wywołanie), żeby zrealizowała nakierowanie na ten preset i pokazała jego obraz. W tym celu w panelu sterującym PTZ wybierz z listy presetów zdefiniowanych preset żądany, po czym kliknij przycisk , aby go wywołać.

Ewentualnie umieść kursor myszy gdzieś w obrębie interfejsu presetów i wywołaj żądany preset przez wpisanie jego numeru z klawiatury.



Rys. 5–5: Wywołanie presetu obserwacyjnego kamery

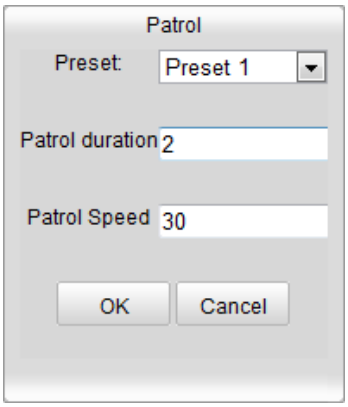
5.4.3. Zdefiniowanie / wywołanie patrolu

Uwaga:

Aby móc zdefiniować patrol presetów, musisz mieć najpierw zdefiniowane w kamerze **co najmniej 2 presety**.

Procedura wykonania:

1. Kliknij przycisk , aby wejść w interfejs konfigurowania patroli.
2. Wybierz tam numer ścieżki patrolu, po czym kliknij przycisk , aby dodać do niej Twoje wcześniej zdefiniowane presety.
3. Wybierz z listy żądany preset i wprowadź czas patrolowania (**Patrol duration**) oraz szybkość patrolu (**Patrol Speed**).
4. Kliknij przycisk **OK**, aby zachować ten pierwszy preset (w tym patrolu).
5. Powtórz powyższe kroki, aby dodać kolejne presety składające się na ten patrol presetów.



Rys. 5–6: Dodanie presetu do (ścieżki) patrolu

6. Na koniec kliknij przycisk , aby zapisać zdefiniowany patrol.
7. Możesz kliknąć przycisk , aby uruchomić patrol albo możesz kliknąć przycisk , aby zatrzymać wykonywanie patrolu już uruchomionego.
8. *(Ewentualnie):* Kliknij przycisk , aby skasować patrol.

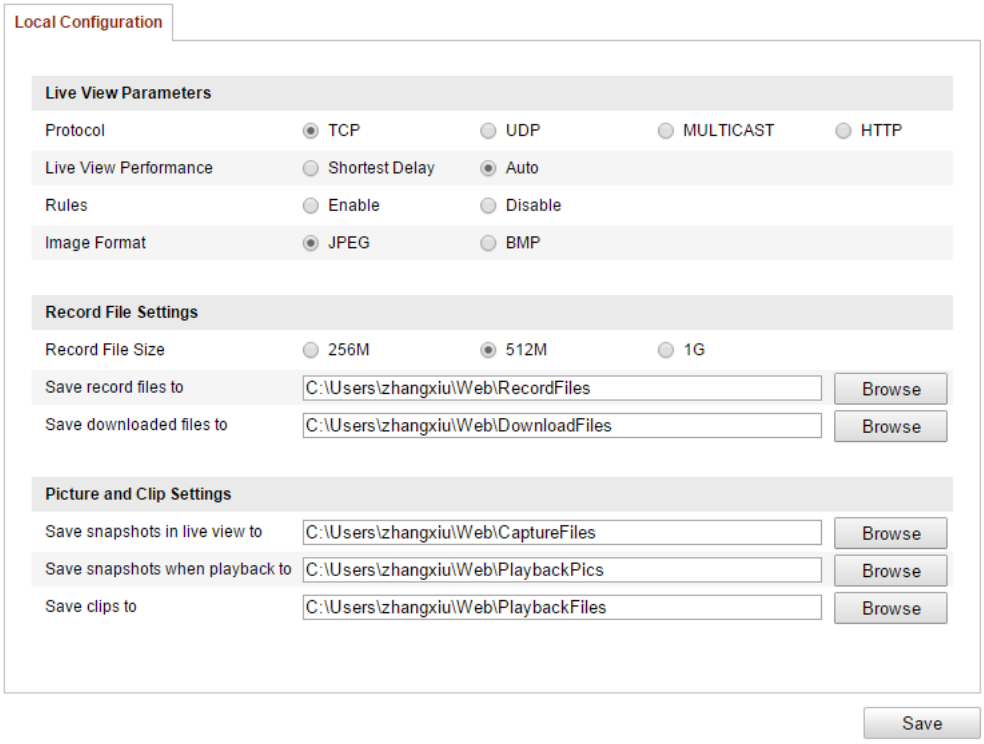
6. Konfigurowanie kamery sieciowej

6.1. Konfigurowanie parametrów lokalnych

Uwaga: Konfiguracja lokalna obejmuje sparametryzowanie: podglądu bieżącego, plików wideo-nagrań wycinkowych, plików fotozrzutów. Pliki wideo-nagrań wycinkowych i fotozrzutów to te nagrywane i wychwytywane samodzielnie przez Ciebie w Twojej przeglądarce internetowej — dlatego ich ścieżki zapisu odnoszą się do Twojego komputera PC (na którym działa Twoja przeglądarka).

Procedura wykonania:

1. Wyświetl interfejs ustawień konfiguracji lokalnej:
   Configuration > Local Configuration



Rys. 6–1: Interfejs z opcjami do ustawiania konfiguracji lokalnej (Local Configuration)

2. Skonfiguruj następujące ustawienia:

- **Parametry podglądu bieżącego (Live View Parameters):** Skonfiguruj rodzaj protokołu (Protocol) oraz parametry realizowania podglądu bieżącego (Live View Performance).
  - **Rodzaj protokołu (Protocol):** Do wyboru są protokoły: TCP, UDP, MULTICAST, HTTP.
    TCP: Zapewnia kompletne dostarczanie danych strumieniowanych oraz lepszą jakość obrazu, jednak utrudnia osiągnięcie transmisji w czasie rzeczywistym.
    UDP: Zapewnia dosył strumienia fonii i wizji w czasie rzeczywistym.

HTTP: Zapewnia tę samą jakość co ww. protokół **TCP** jednak bez konfigurowania konkretnych portów na potrzeby strumieniowania w niektórych środowiskach sieciowych.

MULTICAST: Zaleca się wybranie protokołu MCAST, jeśli wykorzystujesz funkcję Multicast. Więcej o funkcji Multicast – zob. *podrozdz. 6.3.1 **Konfigurowanie ustawień TCP/IP***, str. 45.

- **Szybkość podglądu bieżącego (Live View Performance):** Możesz ustawić szybkość realizowania podglądu bieżącego albo na **Shortest Delay** (najmniejsze opóźnienie) albo na **Auto** (dobierana automatycznie).
- **Reguły (Rules):** Ta opcja oznacza reguły, obowiązujące w Twojej lokalnej przeglądarce internetowej. Do wyboru masz dwie opcje: reguły załączone (**Enable**) / reguły odłączone (**Disable**), aby odpowiednio wyświetlać / nie wyświetlać na podglądzie kamery kolorowych znaczników, gdy kamera wykryje w swoim obrazie: ruch, twarz, wtargnięcię. Przykład: jeśli dla **Rules** zaznaczona jest opcja **Enabled**, a ponadto załączona jest również funkcja wykrywania twarzy w obrazie, to z chwilą wykrycia twarzy, na wyświetlanym podglądzie bieżącym twarz ta zostaje wyraźnie zaznaczona zielonym prostokątem.
- **Format obrazów (Image Format):** Wybierz komputerowy format, w jakim mają być zapisywane fotozrzuty robione z bieżącego obrazu kamery.

- **Ustawienia plików wideonagrań (Record File Settings):** Ustaw w tej sekcji ustawień m.in. ścieżkę zapisu dla plików wideonagrań z kamery. Odnosi się do plików wideo-nagrań, które Ty nagrasz ręcznie za pomocą Twojej przeglądarki internetowej.
  - **Długość pliku nagrania (Record File Size):** Wybierz tu długość spakowaną dla ręcznie nagrywanych oraz dla pobieranych (download) plików wideo-nagrań: **256M**, **512M** lub **1G**. Po dokonaniu tego wyboru, maksymalną dozwoloną wielkością pliku wideo-nagrania staje się właśnie ta wartość, którą tu zaznaczyłeś.
  - **Zapisz pliki nagrań w... (Save record files to):** Wprowadź tu ścieżkę zapisu plików wideo-nagrań, nagrywanych ręcznie przez Ciebie.
  - **Zapisz pliki pobrane w... (Save downloaded files to):** Wprowadź tu ścieżkę zapisu dla plików wideo-nagrań pobieranych (download) podczas trybu odtwarzania nagrań.
- **Ustawienia obrazów i klipów wideo (Picture and Clip Settings):** Wprowadź tu ścieżkę zapisu dla ręcznie robionych fotozrzutów / wideo-nagrań wycinkowych (=klipów wideo). Dotyczy tylko obrazów, które Ty sam ręcznie rejestrujesz za pomocą Twej przeglądarki internetowej.
  - **Zapisz fotozrzuty podczas podglądu bieżącego w... (Save snapshots in live view to):** Wprowadź tu ścieżkę zapisu dla ręcznie wychwytywanych klatek obrazowych w trakcie podglądu bieżącego.

- **Zapisz fotozrzuty podczas odtwarzania w... (Save snapshots when playback to):** Wprowadź tu ścieżkę zapisu dla ręcznie wychwytywanych klatek obrazowych podczas realizowanego odtwarzania.
- **Zapisz wideonagrania wycinkowe w (Save clips to):** Wprowadź tu ścieżkę zapisu dla wideo-nagrań ręcznie „wyciętych" z materiału odtwarzanego, podczas jego odtwarzania.

***Uwaga*:** Aby określić wybierany katalog docelowy dla wideonagrań wycinkowych i fotozrzutów, możesz kliknąć przycisk przeglądania katalogów **Browse**.

3. Kliknij przycisk **Save**, aby zachować wprowadzone ustawienia.

6.2. Konfigurowanie ustawień czasu

Cel czynności:

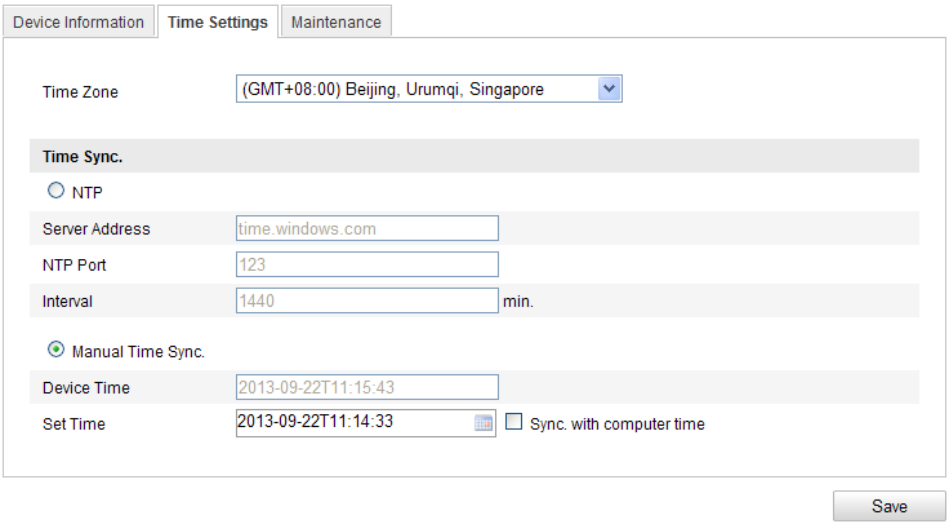
Możesz wykonać kroki z niniejszego podrozdziału, jeśli potrzebujesz skonfigurować ustawienia funkcji synchronizacji czasu i funkcji DST.

Procedura wykonania:

1. Wyświetl interfejs ustawień czasu (karta Time Settings):

   Configuration > Basic Configuration > System > Time Settings

   albo też: **Configuration > Advanced Configuration > System > Time Settings**



Rys. 6–2: Opcje do skonfigurowania ustawień czasu (Time Settings)

- Wybierz żądaną strefę czasową.

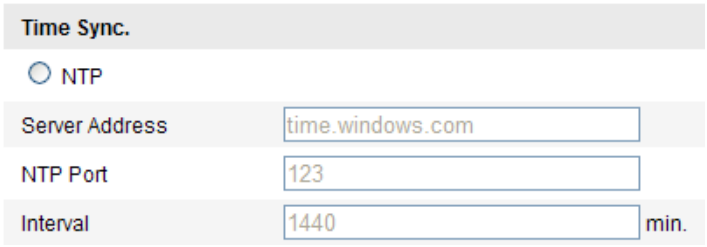
  Z listy rozwijalnej Time Zone wybierz strefę czasową geograficznie zgodną z Twoją lokalizacją.

- Synchronizacja wskazań czasu — automatycznie z serwera NTP

(1) Zaznacz pole wyboru NTP, aby załączyć funkcję **NTP**.

(2) Skonfiguruj następujące ustawienia:
Adres serwera (Server Address): adres IP serwera NTP.
Port NTP (NTP Port): port dla serwera NTP.

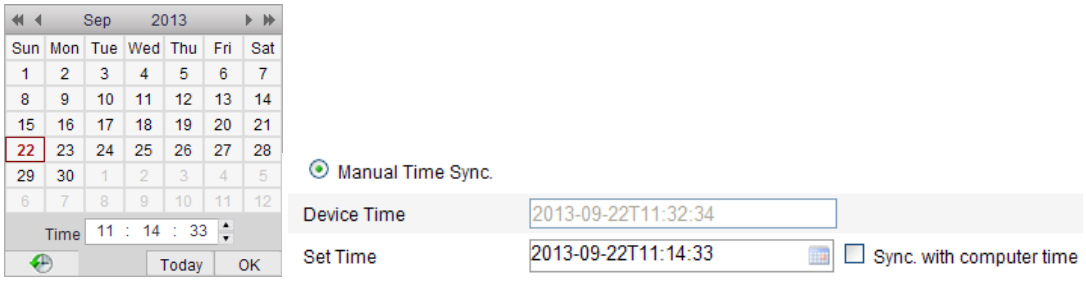
Przedział czasu (Interval): odstęp czasu pomiędzy dwiema kolejnymi akcjami synchronizacji czasu z serwera NTP.



Rys. 6–3: Opcje do skonfigurowania synchronizacji czasu z serwera NTP

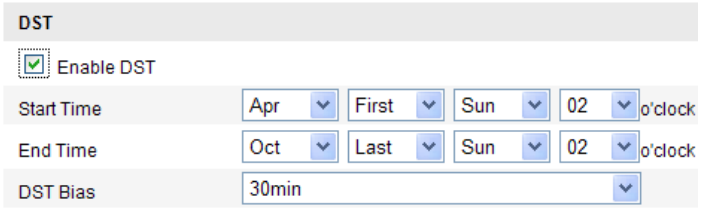
***Uwaga*:** Jeżeli kamera zostaje podłączona do ogólnodostępnej sieci teleinformatycznej, to powinieneś wykorzystać serwer NTP wyposażony w funkcję synchronizacji czasu, np. serwer w Ogólnokrajowym Centrum Regulacji Czasu (tj. *National Time Center* pod adresem IP: 210.72.145.44). Jeśli natomiast konfigurujesz kamerę do pracy w sieci teleinformatycznej przygotowanej indywidualnie dla Klienta, to używając oprogramowania NTP możesz założyć serwer NTP, aby zrealizować funkcję synchronizacji czasu.

- Synchronizacja czasu — wykonywana ręcznie
  Kliknij w radio-przycisk ręcznej synchronizacji czasu Manual Time Sync., po czym kliknij przycisk , aby wyświetlić podręczne okienko kalendarza i ręcznie wprowadzić z niego czas systemowy dla kamery.
  Uwaga: Ewentualnie możesz zaznaczyć pole wyboru Sync with computer time (zsynchronizuj ze wskazaniem czasu w komputerze), aby nastąpiło zsynchronizowanie czasu/zegara kamery z czasem/zegarem systemowym Twojego komputera.



Rys. 6–4: Synchronizacja czasu wykonywana ręcznie (Manual Time Sync.)

- Kliknij w zakładkę strony **DST**, aby załączyć na niej funkcję DST (pole Enable DST) i wprowadzić dane, specyfikujące okres panowania czasu letniego DST (początek Start Time, koniec End Time oraz przesunięcie DST Bias).



Rys. 6–5: Konfigurowanie ustawień funkcji DST

2. Kliknij przycisk **Save**, aby zachować wszystkie wprowadzone ustawienia.

6.3. Konfigurowanie ustawień sieciowych

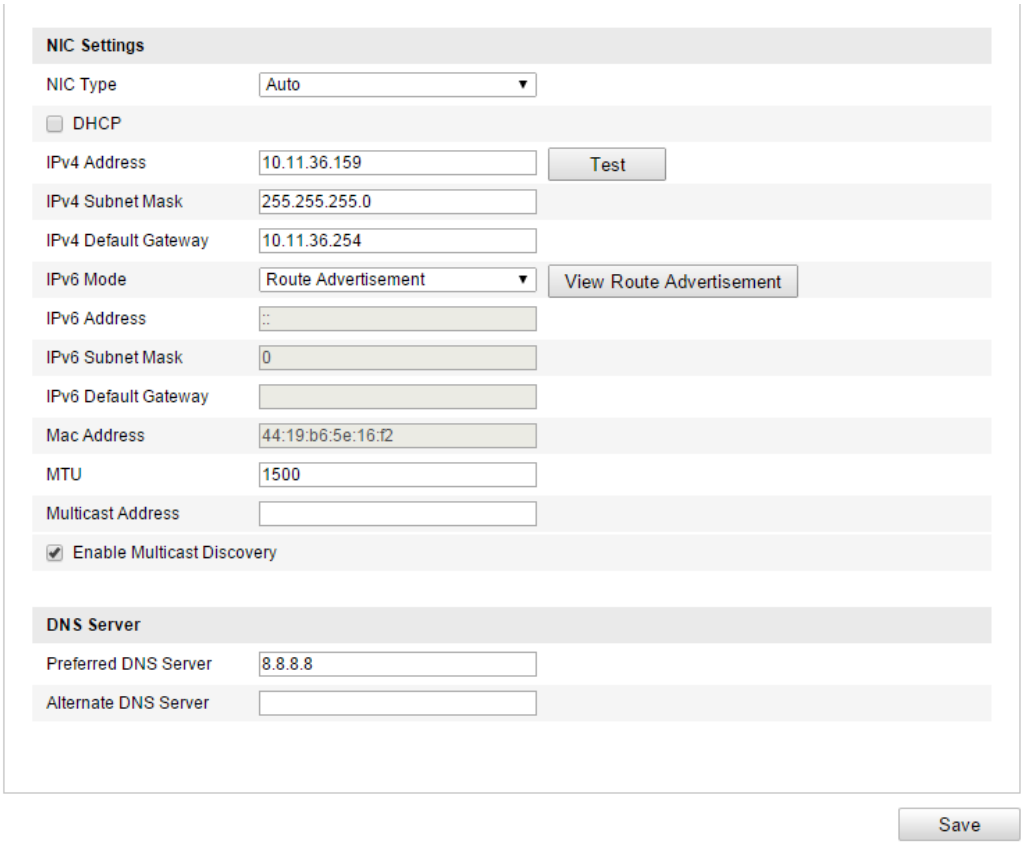
6.3.1. Konfigurowanie ustawień TCP/IP

Cel czynności:

Musisz właściwie skonfigurować ustawienia TCP/IP, zanim zaczniesz użytkować kamerę przez sieć. Ta kamera sieciowa obsługuje zarówno IPv4, jak i IPv6. Obie wersje protokołu możesz mieć skonfigurowane równocześnie bez obawy o konflikt między nimi — pamiętaj jednak, że chociaż jedna z nich musi zostać należycie skonfigurowana.

Procedura wykonania:

1. Wyświetl interfejs ekranowy ustawień TCP/IP:
   Configuration > Basic Configuration > Network > TCP/IP
   albo też: **Configuration > Advanced Configuration > Network > TCP/IP**



Rys. 6–6: Konfigurowane ustawienia protokołu TCP/IP

2. Skonfiguruj podstawowe ustawienia sieci, w tym: **NIC Type**, adres IPv4 / adres IPv6, maskę podsieci IPv4 / IPv6, bramę sieciową IPv4 / IPv6, wielkość jednostki MTU oraz adres dla selektywnej transmisji grupowej **Multicast Address**.

3. (*Ewentualnie*): Zaznacz pole wyboru **Enable Multicast Discovery**, a wtedy kamera sieciowa, w stanie online, będzie mogła być automatycznie wykrywana przez oprogramowanie klienckie via prywatny protokół *multicast* w sieci LAN.

4. Kliknij przycisk **Save**, aby zachować powyższe ustawienia.

***Uwagi*:**

- Zakres regulacyjny dla MTU obowiązujący (valid) w systemie: **1280~1500**.
- Definiowana tu funkcja *multicast* wysyła dany strumień danych na adres rozsyłu grupowego **Multicast Address** oraz pozwala wielu klientom pobrać ten strumień równocześnie przez zażądanie kopii z ww. adresu rozsyłu grupowego. Przed skorzystaniem z tej funkcjonalności, musisz załączyć funkcję *multicast* w Twoim ruterze.
- Wymagane jest przeładowanie systemu kamery (reboot), aby wprowadzone tu ustawienia zaczęły działać.

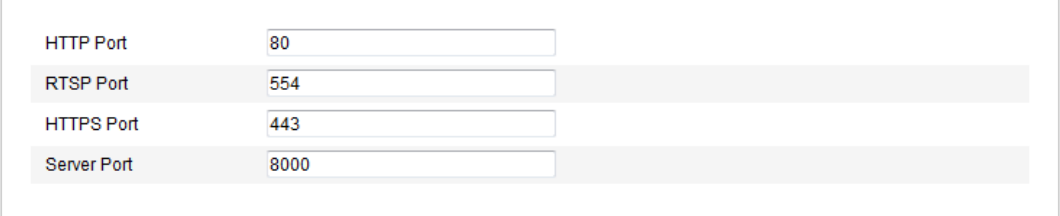
6.3.2. Konfigurowanie ustawień portów

Cel czynności:

W ustawieniach kamery możesz wprowadzić numer portu kamery, np. dla HTTP, RTSP, HTTPS.

Procedura wykonania:

1. Wyświetl interfejs ekranowy ustawień portów:
   Configuration > Basic Configuration > Network > Port
   albo też: **Configuration > Advanced Configuration > Network > Port**



Rys. 6–7: Konfigurowane ustawienia portów kamery

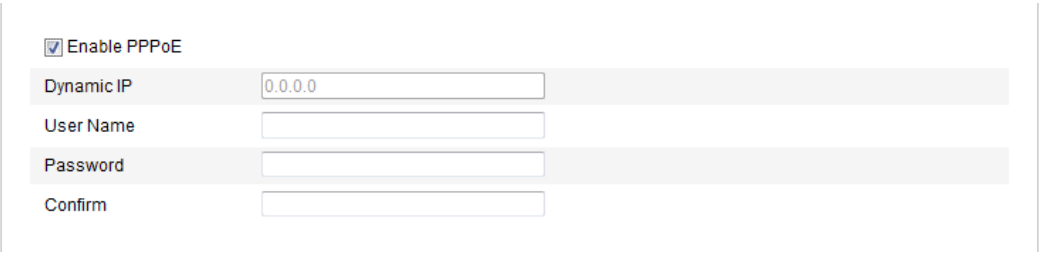
2. Wpisz numer portu: HTTP, RTSP, HTTPS i portu serwera.
   HTTP Port: Domyślnym numerem tego portu jest **80**. Można go zmienić na dowolny inny wolny (niezajęty) numer portu.
   RTSP Port: Domyślnym numerem tego portu jest **554**. Można go zmienić na dowolny inny port z zakresu **1024~65535**.
   HTTPS Port: Domyślnym numerem tego portu jest **443**. Można go zmienić na dowolny inny wolny (=niezajęty) numer portu.
   Server Port: Domyślnym numerem tego portu jest **8000**. Można go zmienić na dowolny inny port z zakresu **2000~65535**.
3. Kliknij przycisk **Save**, zapisać wprowadzone zmiany ustawień.

***Uwaga*:** Uaktywnienie tych ustawień wymaga przeładowania systemu (reboot).

6.3.3. Konfigurowanie ustawień protokołu PPPoE

Procedura wykonania:

1. Wyświetl interfejs ekranowy ustawień PPPoE:
   Configuration >Advanced Configuration > Network > PPPoE



Rys. 6–8: Konfigurowane ustawienia protokołu PPPoE

2. Zaznacz pole wyboru **Enable PPPoE**, aby załączyć tę funkcję.
3. Wpisz nazwę użytkownika (**User Name**), jego hasło (**Password**), a w polu **Confirm** potwierdź to hasło dostępu przez PPPoE.

Uwaga: Powyższe: nazwę użytkownika i hasło musisz mieć przydzielone przez Twojego dostawcę Internetu (ISP).

- *Dla ochrony Twojej własnej prywatności oraz dla lepszej ochrony Twojego systemu od źródeł zagrożeń sieciowych zdecydowanie zalecamy zastosowanie **silnych haseł** do wszystkich funkcji i urządzeń sieciowych. Hasło takie powinno być czymś, co samemu sobie wybierzesz, (powinno być w nim minimum 8 znaków, w tym co najmniej trzy z następujących kategorii znakowych: litery wielkie, litery małe, cyfry, znaki specjalne), aby podnieść poziom zabezpieczenia Twojego produktu (kamery).*
- *Odpowiedzialność za właściwe skonfigurowanie wszystkich haseł i innych nastaw zabezpieczających spoczywa na instalatorze oraz/lub użytkowniku końcowym (tj. konsumencie/odbiorcy) instalowanego rozwiązania.*

4. Kliknij przycisk **Save**, aby zachować zmiany ustawień i wyjść z interfejsu konfiguracyjnego.

***Uwaga*:** Uaktywnienie tych ustawień wymaga przeładowania kamery (reboot).

6.3.4. Konfigurowanie ustawień DDNS

Cel czynności:

Jeśli skonfigurowałeś kamerę, żeby używała PPPoE jako domyślnego połączenia sieciowego, to dla dostępów sieciowych możesz wykorzystać funkcjonalność Dynamicznego-DNS (tj. DDNS).

Przygotuj na wstępie:

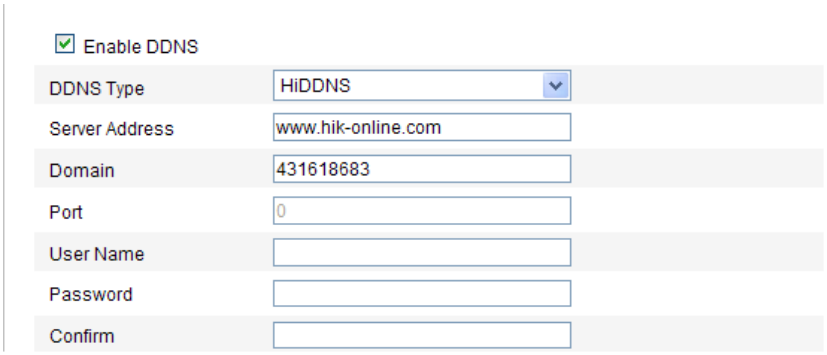
Zanim zaczniesz konfigurować ustawienia DDNS kamery, musisz zarejestrować używany serwer DDNS.

- *Dla ochrony Twojej własnej prywatności oraz dla lepszej ochrony Twojego systemu od źródeł zagrożeń sieciowych zdecydowanie zalecamy zastosowanie **silnych haseł** do wszystkich funkcji i urządzeń sieciowych. Hasło takie powinno być czymś, co samemu sobie wybierzesz, (powinno być w nim minimum 8 znaków, w tym co najmniej trzy z następujących kategorii znakowych: litery wielkie, litery małe, cyfry, znaki specjalne), aby podnieść poziom zabezpieczenia Twojego produktu (kamery).*
- *Odpowiedzialność za właściwe skonfigurowanie wszystkich haseł i innych nastaw zabezpieczających spoczywa na instalatorze oraz/lub użytkowniku końcowym (tj. konsumencie/odbiorcy) instalowanego rozwiązania.*

Procedura wykonania:

1. Wyświetl interfejs ekranowy ustawień DDNS:

   Configuration > Advanced Configuration > Network > DDNS



Rys. 6–9: Konfigurowane ustawienia serwera DDNS

2. Zaznacz pole wyboru **Enable DDNS**, aby załączyć tę funkcję.
3. Z listy rozwijalnej **DDNS Type** wybierz rodzaj żądanego DDNS-u — do wyboru są cztery rodzaje DDNS: **HiDDNS**, **IPServer**, **NO-IP**, a także **DynDNS**.

   - Wariant z opcją **DynDNS**:

Procedura wykonania:

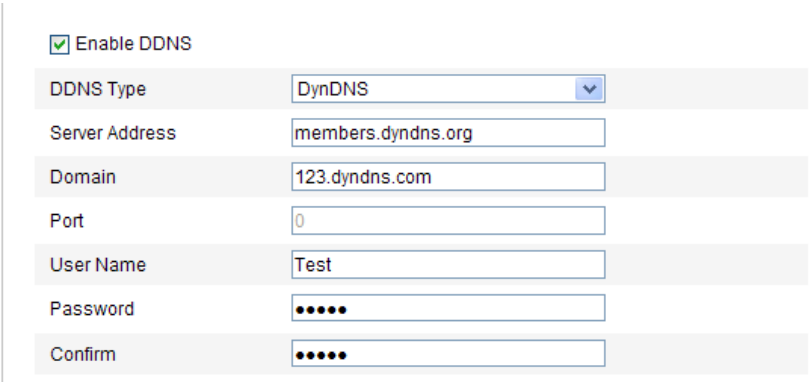
(1)W polu **Server Address** wpisz adres serwera DynDNS (np. members.dyndns.org).

(2)W polu tekstowym domeny (**Domain**) wpisz nazwę domeny uzyskanej z wybranej wyżej witryny DynDNS.

(3)Wpisz numer portu (pole **Port**) dla serwera DynDNS.

(4)Wpisz nazwę użytkownika (pole **User Name**) i jego hasło (pole **Password**), jak masz je zarejestrowane na witrynie DynDNS.

(5)Kliknij przycisk **Save**, aby zachować wprowadzone ustawienia.



Rys. 6–10: Konfigurowane ustawienia funkcji DDNS — w wariancie **DynDNS**

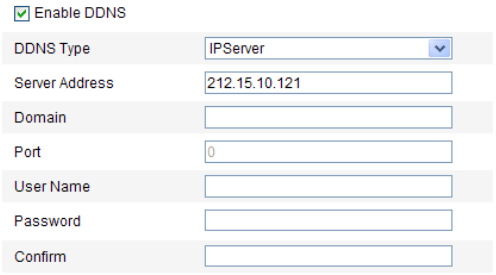
- Wariant z opcją **IP Server**:

Procedura wykonania:

(1) Wpisz adres serwera IP (pole **Server Address**).

(2) Kliknij przycisk **Save**, aby zachować wprowadzone ustawienia.

Uwaga: W przypadku DDNS w wariancie **IP Server** musisz zastosować statyczny adres IP, maskę podsieci, bramę sieciową oraz preferowany DNS — od Twojego dostawcy Internetu. Do pola **Server Address** trzeba wprowadzić ten statyczny adres IP komputera, na którym pracuje oprogramowanie realizujące IP-serwer.



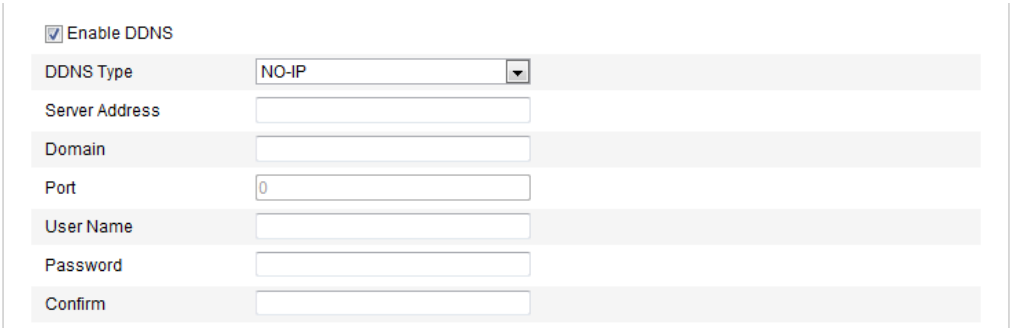
Rys. 6–11: Konfigurowane ustawienia funkcji DDNS — w wariancie **IP Server**

Uwaga: W przypadku terytorium USA i Kanady jako adres serwera możesz wprowadzić 173.200.91.74.

- Wariant z opcją **NO-IP**:

Procedura wykonania:

(1) W liście rozwijalnej **DDNS Type** wybierz **NO-IP** jako żądany rodzaj DDNS.



Rys. 6–12: Konfigurowane ustawienia funkcji DDNS w wariancie **NO-IP**

(2) W polu **Server Address** wpisz www.noip.com jako adres serwera.

(3) W polu **Domain** wpisz nazwę domeny, którą masz zarejestrowaną.

(4) Jeśli potrzeba, wpisz numer portu (pole **Port**).

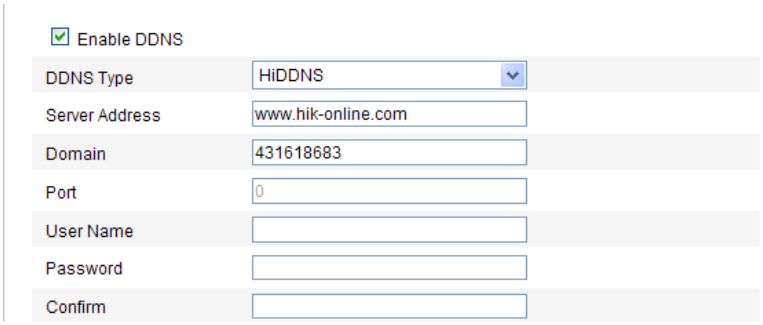
(5) Wpisz nazwę użytkownika (**User Name**) i jego hasło (**Password**).

(6) Kliknij **Save**. Po tym, możesz uzyskiwać wgląd w obraz kamery przez zastosowanie ww. nazwy domeny.

- Wariant z opcją **HiDDNS**:

Procedura wykonania:

(1) W liści rozwijalnej **DDNS Type** wybierz **HiDDNS** jako żądany rodzaj DDNS.



Rys. 6–13: Konfigurowane ustawienia funkcji DDNS w wariancie **HiDDNS**

(2) W polu **Server Address** wpisz *www.hik-online.com* jako adres serwera.

(3) Wpisz nazwę domeny od tej kamery. Ta domena jest tożsama z aliasem urządzenia na serwerze HiDDNS.

(4) Kliknij przycisk **Save**, aby zachować nowo wprowadzone ustawienia.

Uwaga: Uaktywnienie tych ustawień wymaga przeładowania kamery (reboot).

6.3.5. Konfigurowanie ustawień protokołu SNMP

Cel czynności:

Możesz skonfigurować funkcję obsługi protokołu SNMP, aby móc odczytywać aktualny status systemowy kamery, parametry i dane dot. alarmów, a także zdalnie zarządzać kamerą — gdy kamera jest podłączona do sieci.

Przygotuj na wstępie:

Zanim przystąpisz do konfigurowania SNMP, pobierz oprogramowanie realizująco-zarządzające SNMP, aby móc pobierać dane kamery przez port SNMP. Przez wprowadzenie w ustawieniach adresu pułapkowego **Trap Address** umożliwisz kamerze transmisję powiadomień o zdarzeniach alarmowych i wyjątkach systemowych (exceptions) do żądanego centrum monitoringowego.

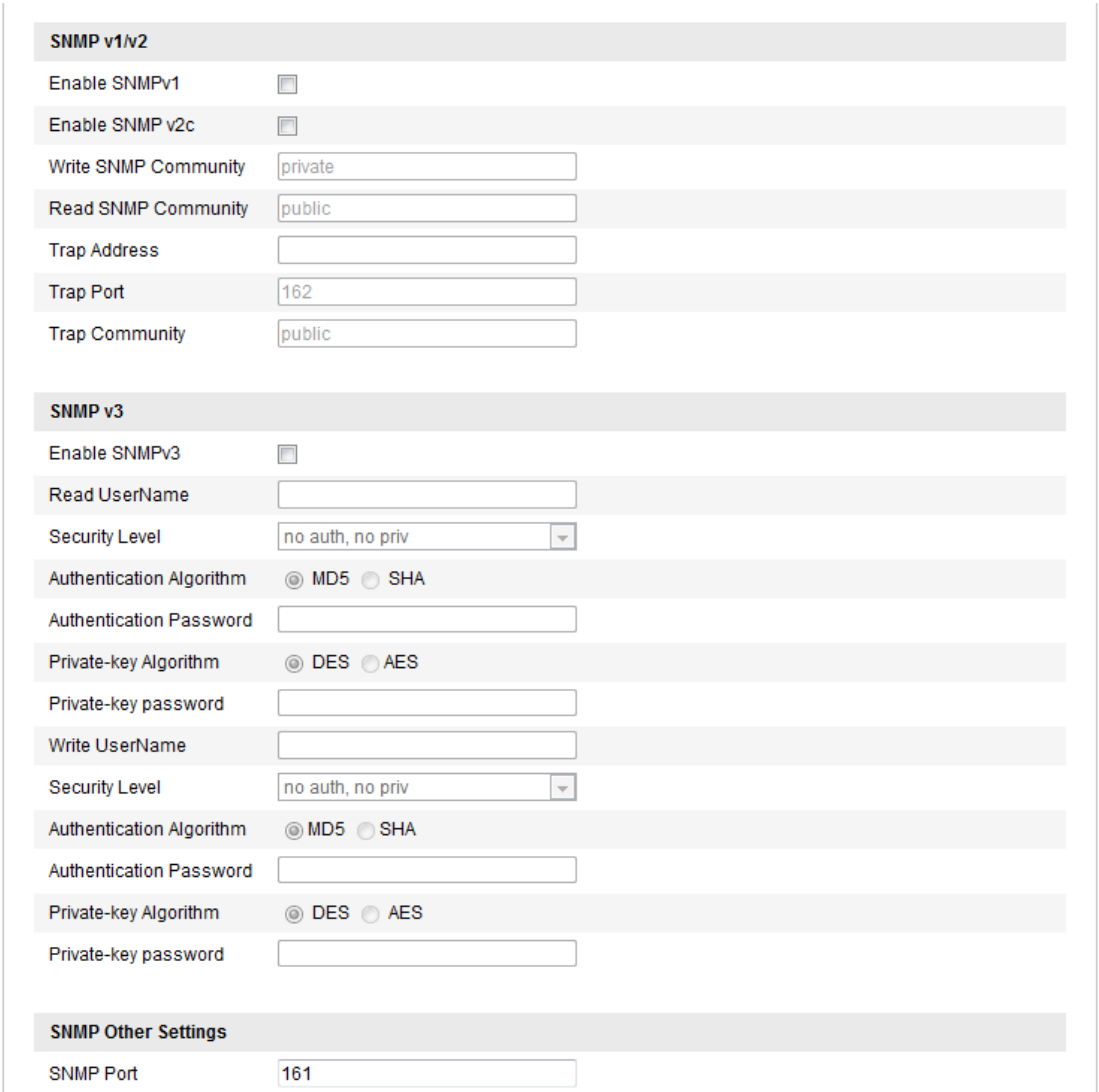
Uwaga: Wersja protokołu SNMP, którą tu wybierzesz jako używaną, musi być identyczna z wersją obsługiwaną przez wykorzystywane oprogramowanie SNMP. Ogólnie, możesz stosować różne wersje SNMP, zależnie od konkretnego, pożądanego poziomu zabezpieczenia. SNMP wer.**1** nie zapewnia żadnego zabezpieczenia,

SNMP wer.**2** zabezpiecza przez wymóg podania hasła dla zrealizowania dostępów, a SNMP wer.**3** zapewnia szyfrowanie. Jeśli jednak zastosujesz SNMP wer.3, to musi być do tego załączony także protokół HTTPS.

- *Dla ochrony Twojej własnej prywatności oraz dla lepszej ochrony Twojego systemu od źródeł zagrożeń sieciowych zdecydowanie zalecamy zastosowanie **silnych haseł** do wszystkich funkcji i urządzeń sieciowych. Hasło takie powinno być czymś, co samemu sobie wybierzesz, (powinno być w nim minimum 8 znaków, w tym co najmniej trzy z następujących kategorii znakowych: litery wielkie, litery małe, cyfry, znaki specjalne), aby podnieść poziom zabezpieczenia Twojego produktu (kamery).*
- *Odpowiedzialność za właściwe skonfigurowanie wszystkich haseł i innych nastaw zabezpieczających spoczywa na instalatorze oraz/lub użytkowniku końcowym (tj. konsumencie/odbiorcy) instalowanego rozwiązania.*

Procedura wykonania:

1. Wyświetl interfejs ekranowy ustawień SNMP:
   Configuration > Advanced Configuration > Network > SNMP



Rys. 6–14: Konfigurowane ustawienia protokołu SNMP

2. Zaznacz pole wyboru, stosownie do żądanej wersji SNMP (Enable SNMP SNMPv1 , Enable SNMP v2c , Enable SNMPv3), aby załączyć w kamerze żądaną funkcjonalność SNMP (v1/v2/v3).
3. Skonfiguruj ustawienia SNMP pod wersją protokołu wybraną w kroku 2.

   Uwaga: Pamiętaj, że wprowadzone tu ustawienia muszą być takie same jak te w używanym oprogramowaniu do realizacji SNMP.
4. Kliknij przycisk **Save**, to zachować ustawienia i skończyć to konfigurowanie.

***Uwaga*:** Uaktywnienie tych ustawień w kamerze wymaga jej przeładowania (reboot).

6.3.6. Konfigurowanie ustawień 802.1X

Cel czynności:

Opisywana kamera sieciowa obsługuje standard sieciowy IEEE 802.1X. Gdy funkcja ta zostanie załączona w ustawieniach, dane kamery są chronione — i podczas podłączania kamery do sieci teleinformatycznej (chronionej przez IEEE 802.1X) wymagane jest uwierzytelnianie użytkownika.

Przygotuj na wstępie:

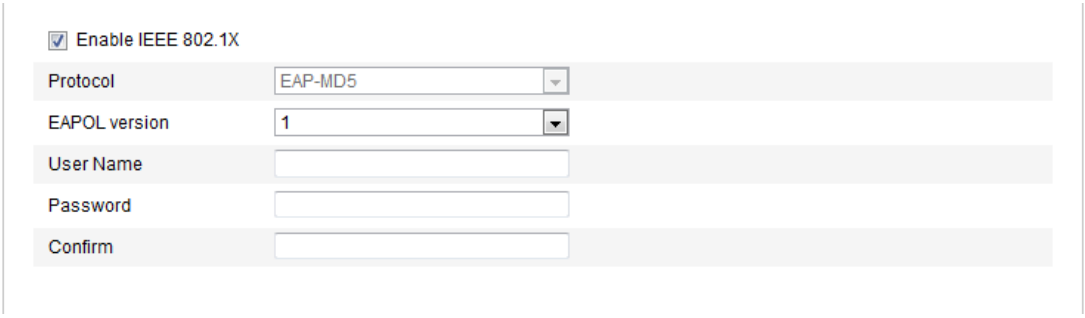
Do poniższych ustawień trzeba dysponować odpowiednio skonfigurowanym serwerem uwierzytelnień (authetication server). Prosimy zaaplikować o zarejestrowanie nazwy użytkownika i jego hasła, aby móc skorzystać z funkcji 802.1X serwera.

- *Dla ochrony Twojej własnej prywatności oraz dla lepszej ochrony Twojego systemu od źródeł zagrożeń sieciowych zdecydowanie zalecamy zastosowanie **silnych haseł** do wszystkich funkcji i urządzeń sieciowych. Hasło takie powinno być czymś, co samemu sobie wybierzesz, (powinno być w nim minimum 8 znaków, w tym co najmniej trzy z następujących kategorii znakowych: litery wielkie, litery małe, cyfry, znaki specjalne), aby podnieść poziom zabezpieczenia Twojego produktu (kamery).*
- *Odpowiedzialność za właściwe skonfigurowanie wszystkich haseł i innych nastaw zabezpieczających spoczywa na instalatorze oraz/lub użytkowniku końcowym (tj. konsumencie/odbiorcy) instalowanego rozwiązania.*

Procedura wykonania:

1. Wyświetl interfejs ekranowy ustawień 802.1X:

   Configuration > Advanced Configuration > Network > 802.1X



Rys. 6–15: Konfigurowane ustawienia standardu sieci 802.1X

2. Zaznacz pole wyboru **Enable IEEE 802.1X**, aby załączyć w kamerze funkcjonalność 802.1X.
3. Skonfiguruj widoczne ustawienia funkcjonalności 802.1X, w tym: wersję EAPOL (**EAPOL version**), nazwę użytkownika (**User name**) oraz hasło użytkownika (**Password** | **Confirm**).
   Uwaga: Wersja EAPOL, wybrana w tych ustawieniach, musi być identyczna z obecną we współpracującym ruterze lub hubie przełączającym.
4. Wpisz nazwę użytkownika (pole **User name**) i hasło użytkownika (pole **Password**), dające dostęp do ww. serwera.
5. Kliknij przycisk **Save**, aby zakończyć wprowadzanie tych ustawień.

Uwaga: Uaktywnienie tych ustawień w kamerze wymaga jej przeładowania (reboot).

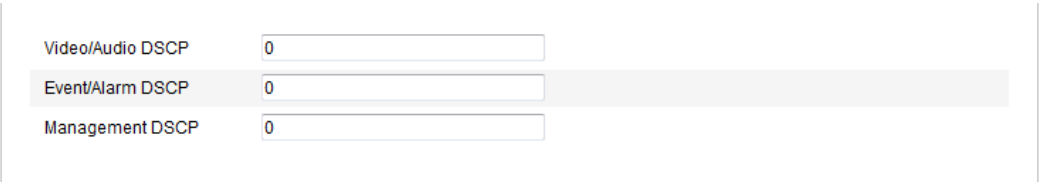
6.3.7. Konfigurowanie ustawień QoS

Cel czynności:

Funkcja QoS (Jakość Funkcjonowania) ułatwia rozwiązanie problemu opóźnień i przeciążeń sieci — wykorzystując w tym celu (odpowiednio skonfigurowany przez Ciebie) priorytet przesyłu danych.

Procedura wykonania:

1. Wyświetl interfejs ekranowy ustawień funkcji QoS:
   Configuration >Advanced Configuration > Network > QoS



Rys. 6–16: Konfigurowane ustawienia QoS

2. Skonfiguruj następujące ustawienia funkcji QoS: DSCP wizji/fonii (pole **Video/Audio DSCP***)), DSCP zdarzeń/alarmów (pole **Event/Alarm DSCP**), DSCP akcji zarządzających (pole **Management DSCP**).
   Dostępnym zakresem wartości dla DSCP jest: **0~63**. Im wyższa wartość DSCP, tym wyższy jest priorytet danych.

***) Uwaga:** DSCP = ***D**ifferentiated **S**ervice **C**ode **P**oint*. Podawana przez Ciebie w tych ustawieniach wartość DSCP zostaje umieszczona w header-rze IP i poprzez to wskazuje poziom priorytetu transmisji danych.

3. Kliknij **Save**, zapisać wprowadzone ustawienia.

***Uwaga*:** Uaktywnienie tych ustawień w kamerze wymaga jej przeładowania (reboot).

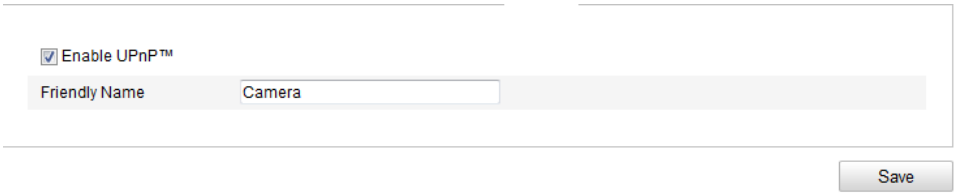
6.3.8. Konfigurowanie ustawień UpnP ™

Universal Plug and Play (UPnP™) to architektura tworzenia sieci, która zapewnia zgodność różnych sieciowych: urządzeń, programów czy pozostałego osprzętu (hardware'u). Dzięki protokołowi UPnP wzajemne łączenie urządzeń może odbywać się gładko i płynnie. UPnP upraszcza też implementację sieci w środowiskach domowym i korporacyjnym.

Po załączeniu funkcji UpnP nie musisz już konfigurować mapowania poszczególnych portów, a kamera podłącza się do sieci WAN za pośrednictwem rutera.

Procedura wykonania:

1. Wyświetl interfejs ekranowy ustawień funkcji UPnP™.
   Configuration > Advanced Configuration > Network > UPnP
2. Zaznacz pole wyboru **Enable UPnP™**, aby załączyć w kamerze protokół UPnP.
   Nazwę urządzenia (pole **Friendly Name**) – gdy tylko zostanie wykryte jako dostępne online – możesz przez edycję tego pola zmienić na inną, bardziej zrozumiałą.



Rys. 6–17: Konfigurowane ustawienia UPnP

6.3.9. Konfigurowanie wdzwanianych/modemowych połączeń bezprzewodowych

Cel czynności:

Napływające z kamery strumienie danych: audio, video, obrazkowych można transmitować via sieć bezprzewodowa technologii 3G / 4G.

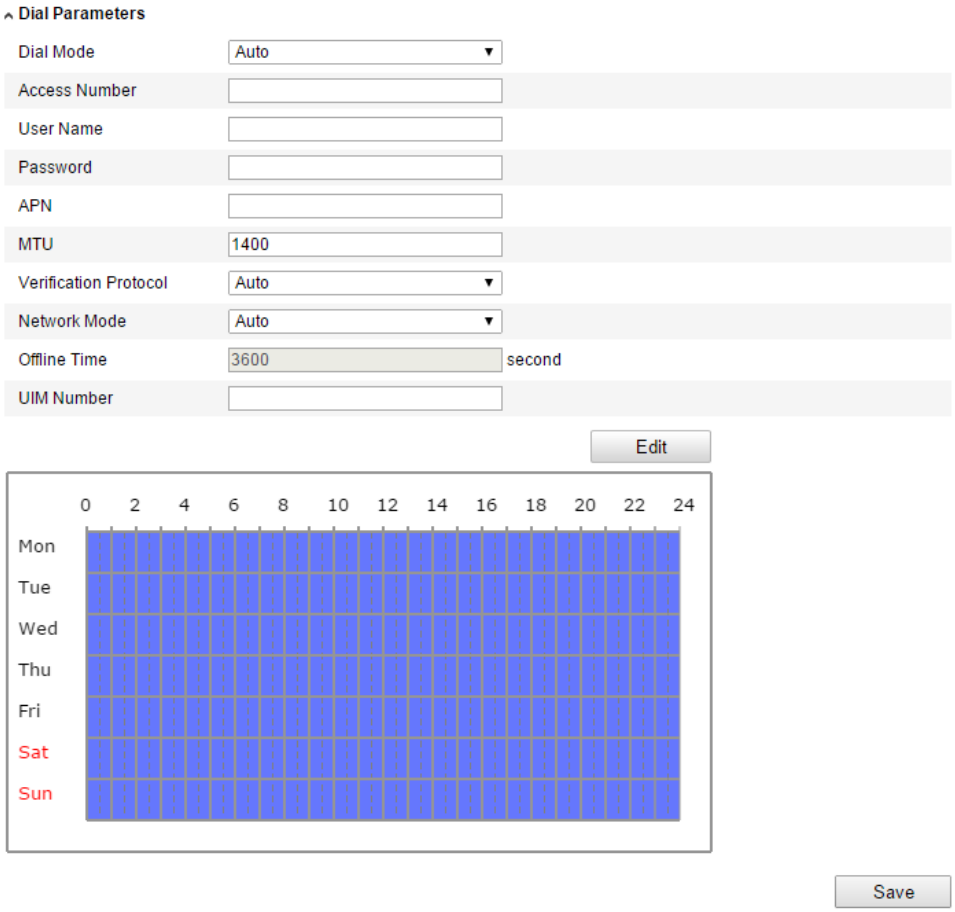
Uwaga: Funkcja wdzwanianych połączeń bezprzewodowych musi być obsługiwana przez zainstalowaną kamerę.

1. Kliknij w zakładkę **Wireless Dial**, aby wyświetlić interfejs ekranowy, służący do konfigurowania ustawień wdzwanianych połączeń bezprzewodowych.
2. W interfejsie tym zaznacz pole wyboru **Enable**, aby załączyć w kamerze ustawienia bezprzewodowych połączeń wdzwanianych.

3. Skonfiguruj ustawienia tworzenia bezprzewodowych połączeń wdzwanianych (zob. rys. na str. 56):
   1) Z listy rozwijalnej **Dial Mode** wybierz żądany tryb wdzwaniania — do wyboru są 2 tryby: **Auto**, **Manual**. W razie wybrania **Auto** możesz skonfigurować harmonogram uzbrajania funkcji wdzwaniania. W razie wybrania **Manual** możesz wprowadzić czas stanu offline oraz parametry ręcznego nawiązywania połączeń wdzwanianych.
   2) Wpisz dostępowy numer telefoniczny (**Access Number**), nazwę użytkownika (**User Name**), hasło użytkownika (**Password**), APN (**APN**), wartość MTU (**MTU**) oraz protokół weryfikacji użytkownika (**Verification Protocol**). Możesz też pozostawić pola tych ustawień puste — wtedy urządzenie przyjmie domyślne wartości wdzwaniania połączenia (z siecią), kiedy już skonfigurujesz parametry pozostałe.

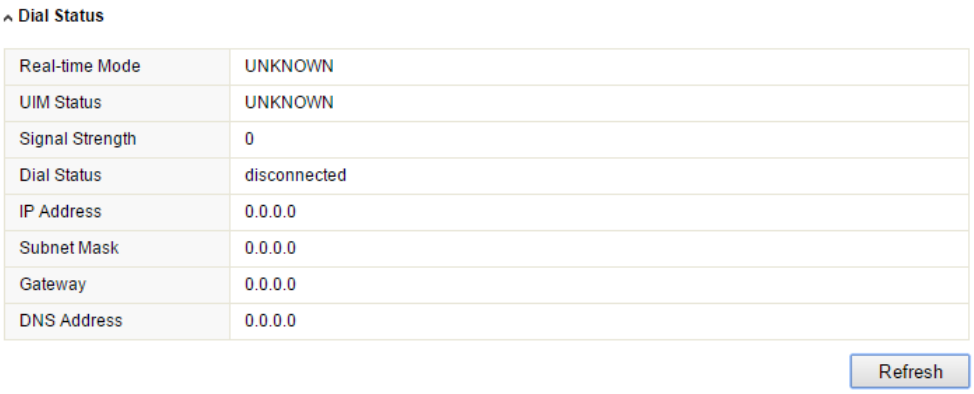
      

      - *Dla ochrony Twojej własnej prywatności oraz dla lepszej ochrony Twojego systemu od źródeł zagrożeń sieciowych zdecydowanie zalecamy zastosowanie **silnych haseł** do wszystkich funkcji i urządzeń sieciowych. Hasło takie powinno być czymś, co samemu sobie wybierzesz, (powinno być w nim minimum 8 znaków, w tym co najmniej trzy z następujących kategorii znakowych: litery wielkie, litery małe, cyfry, znaki specjalne), aby podnieść poziom zabezpieczenia Twojego produktu (kamery).*
      - *Odpowiedzialność za właściwe skonfigurowanie wszystkich haseł i innych nastaw zabezpieczających spoczywa na instalatorze oraz/lub użytkowniku końcowym (tj. konsumencie/odbiorcy) instalowanego rozwiązania.*
   3) Z listy rozwijalnej **Network Mode** wybierz żądany tryb sieci — do wyboru są 3 tryby: **Auto**, **3G**, **4G**. Jeśli wybierzesz **Auto**, to kamera przyjmie priorytet auto-wyboru sieci uszeregowany następująco: 4G > 3G > SIEĆ PRZEWODOWA.
   4) Wpisz czas stanu offline (**Offline Time**), o ile w kroku **1**) wybrałeś ręczny tryb wdzwaniania (tj. opcja **Manual** z listy rozwijalnej **Dial Mode**).
   5) Wpisz numer UIM (numer komórkowy).
   6) Kliknij przycisk **Edit**, aby zdefiniować harmonogram uzbrajania, o ile w kroku **1)** wybrałeś automatyczny tryb wdzwaniania (tj. opcja **Auto** z listy rozwijalnej **Dial Mode**).
   7) Kliknij przycisk **Save**, aby zachować wprowadzone ustawienia.



Rys. 6–18: Parametry wdzwanianych połączeń bezprzewodowych z siecią

4. Zobacz stan tworzenia połączenia wdzwanianego.
   1) Kliknij przycisk odświeżenia **Refresh**, aby zobaczyć parametry opisujące stan połączenia wdzwanianego (**Dial Status**) — a w nim: tryb real-time (**Real-time Mode**), status UIM (**UIM Status**), siłę sygnału (**Signal Strength**) i inne (np. jak na ilustr. poniżej).
   2) Jeśli wybrałeś **Manual** jako **Dial Mode**, to możesz także ręcznie nawiązywać / kończyć połączenia z siecią bezprzewodową.

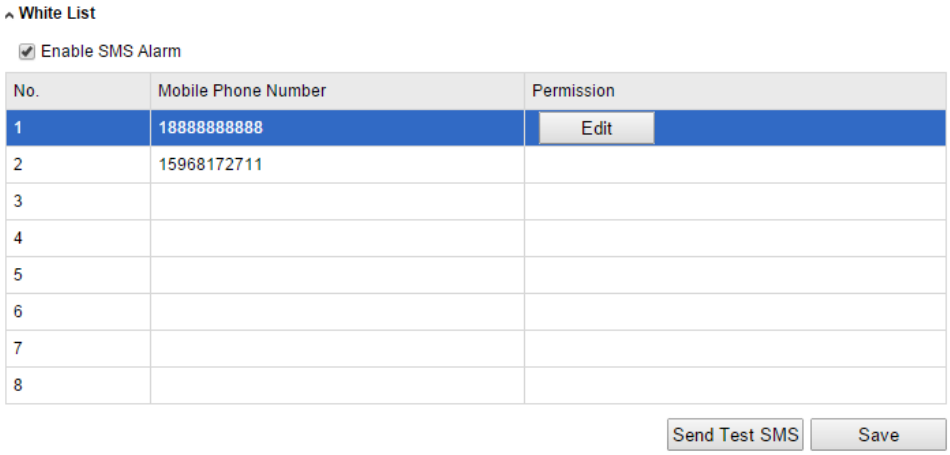


Rys. 6–19: Interfejs ekranowy do odczytu stanu wdzwanianego połączenia z siecią

5. Wypełnij białą listę (**White List**) żądanymi numerami telefonów komórkowych.
   1) Zaznacz pole wyboru: **Enable SMS Alarm** (tj. alarmowanie via SMS).

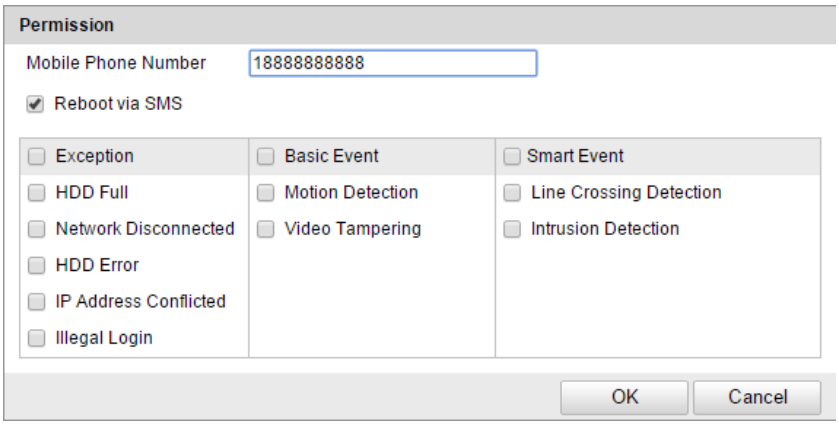
Na numer telefonu komórkowego umieszczony na tej białej liście mogą nadchodzić SMS-owe powiadomienia o alarmach wysyłane z urządzenia. Z tego numeru – przez wysłanie wiadomości SMS o odpowiedniej treści – można również przeładować urządzenie (reboot) — w tym celu zob. pkt **3**) poniżej.

Uwaga: Na tej białej liście można umieścić maks. 8 numerów telefonicznych.



Rys. 6–20: Tabela do skonfigurowania białej listy numerów komórkowych

2) Wybierz (tj. podświetl) pozycję na białej liście, po czym kliknij przycisk **Edit**, aby wejść do interfejsu konfigurowania ustawień alarmów SMS-owych:



Rys. 6–21: Konfigurowane ustawienia alarmowania za pomocą SMS-ów

3) W polu **Mobile Phone Number** wpisz numer telefonu komórkowego wprowadzany do białej listy. Zaznacz pole wyboru **Reboot via SMS**. Zaznacz też pola wyboru przy tych alarmach, które mają wyzwalać alarmowy SMS. Na koniec kliknij przycisk **OK**.

   Uwaga: Aby przeładować urządzenie za pomocą SMS-a, wyślij do urządzenia wiadomość o treści „**reboot**”; urządzenie w odpowiedzi przyśle wiadomość zwrotną „**reboot success**”, jak tylko wykona przeładowanie swojego systemu.

4) (*Krok opcjonalny*) Możesz kliknąć przycisk **Send Test SMS**, aby do tego definiowanego w białej liście telefonu komórkowego wysłać, na próbę, testową wiadomość SMS.

5) Kliknij przycisk **Save**, aby zachować wprowadzone ustawienia.

6.3.10. Powiadamianie e-mailowe o alarmach

Cel czynności:

Możesz skonfigurować system, żeby w razie wykrycia zdarzenia alarmowego (np. sytuacja wykrycia ruchu, zaniku wizji, usiłowania sabotowania wizji) wysłał stosowne powiadomienie alarmowe w liście e-mail.

Przygotuj na wstępie:

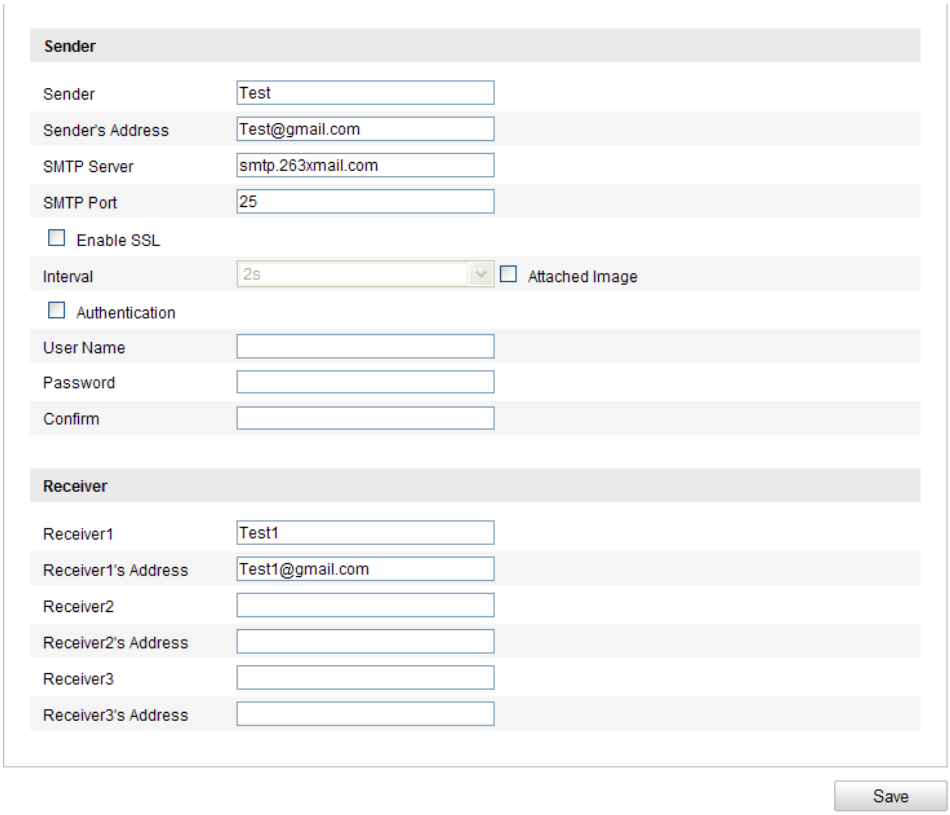
Przed wykorzystaniem funkcji powiadomień e-mailowych trzeba najpierw wprowadzić ustawienia, konfigurujące serwer DNS (ścieżka: **Basic Configuration > Network > TCP/IP** lub **Advanced Configuration > Network > TCP/IP**).

Procedura wykonania:

1. Wyświetl interfejs do konfigurowania ustawień TCP/IP (ścieżka: **Configuration > Basic Configuration > Network > TCP/IP** lub **Configuration > Advanced Configuration > Network > TCP/IP),** aby wprowadzić tam adres IPv4 (**IPv4 Address**), maskę podsieci IPv4 (**IPv4 Subnet Mask**), domyślną bramę IPv4 (**IPv4 Default Gateway**) oraz preferowany serwer DNS.

   Uwaga: Więcej o konfigurowaniu powyższych ustawień — zob. *podrozdz. 6.3.1* ***Konfigurowanie ustawień TCP/IP***, str. 45.

2. Wyświetl interfejs ekranowy z ustawieniami e-mailowymi: **Configuration > Advanced Configuration > Network > Email**



Rys. 6–22: Konfigurowane ustawienia alarmowych powiadomień e-mailowych

3. Skonfiguruj następujące ustawienia:

Nadawca powiadomień (Sender): Etykieta opisująca nadawcę powiadomień e-mailowych.

Adres e-mailowy nadawcy (Sender's Address): Adres e-mailowy nadawcy powiadomień e-mailowych.

Serwer SMTP (SMTP Server): Adres IP serwera e-pocztowego SMTP lub nazwa hosta poczty (np. **smtp.263xmail.com**).

Port SMPT (SMTP Port): Port usługi SMTP. Domyślnym portem TCP/IP dla SMTP jest: 25 (port bez ochrony transmisji). Natomiast port z ochroną SSL dla SMTP to: 465.

Załącz ochronę techniką SSL (Enable SSL): Zaznacz to pole wyboru, aby załączyć ochronę transmisji przez protokół SSL, o ile jest on wymagany przez serwer SMTP, wprowadzony wyżej w ustawieniach **(SMTP Server)**.

Załącznik graficzny (Attached Image): Zaznacz to pole wyboru, jeśli potrzebujesz wysyłać e-maile z obrazami alarmowymi dodawanymi jako załącznik.

Odstęp czasu (Interval): W tym ustawieniu należy podać odstęp czasu pomiędzy dwiema kolejnymi akcjami wysyłania e-mailu z załącznikiem graficznym.

Uwierzytelnienie (Authentication) (*opcjonalne*): Jeśli Twój serwer e-pocztowy wymaga uwierzytelniania użytkownika, to zaznacz to pole wyboru, aby podczas logowania się na ten serwer następowało uwierzytelnianie za pomocą nazwy użytkownika i hasła użytkownika, które wpiszesz w polach **User Name** i **Password** | **Confirm** w tym interfejsie ekranowym.

- *Dla ochrony Twojej własnej prywatności oraz dla lepszej ochrony Twojego systemu od źródeł zagrożeń sieciowych zdecydowanie zalecamy zastosowanie **silnych haseł** do wszystkich funkcji i urządzeń sieciowych. Hasło takie powinno być czymś, co samemu sobie wybierzesz, (powinno być w nim minimum 8 znaków, w tym co najmniej trzy z następujących kategorii znakowych: litery wielkie, litery małe, cyfry, znaki specjalne), aby podnieść poziom zabezpieczenia Twojego produktu (kamery).*
- *Odpowiedzialność za właściwe skonfigurowanie wszystkich haseł i innych nastaw zabezpieczających spoczywa na instalatorze oraz/lub użytkowniku końcowym (tj. konsumencie/odbiorcy) instalowanego rozwiązania.*

Odbiorcy powiadomień (Receiver): W polach tej grupy ustawień wybierz żądanego odbiorcę/ów powiadomień rozsyłanych via e-mail. Możesz skonfigurować co najwyżej **2** takich odbiorców.

Odbiorca1/2/3 (Receiver1/2/3): Nazwa użytkownika, który ma być powiadamiany.

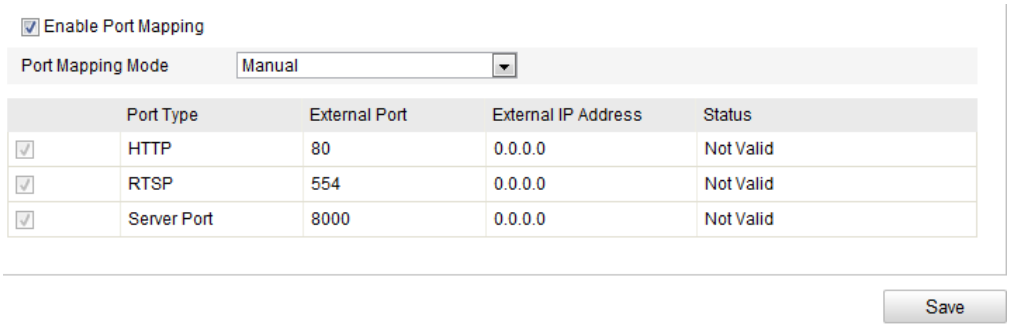
Adres odbiorcy1/2/3 (Receiver(1/2/3)'s Address): Adres e-mailowy użytkownika, który ma otrzymywać powiadomienia via e-mail.

4. Kliknij **Save**, aby zachować wprowadzone ustawienia.

6.3.11. Konfigurowanie ustawień funkcji NAT

Procedura wykonania:

1. Wyświetl interfejs ekranowy dla ustawień konfigurujących NAT.[6]
   Configuration >Advanced Configuration > Network > NAT
2. Wybierz tryb mapowania portów.
   • Aby zastosować mapowanie portów oparte na domyślnych numerach portów:
   Z listy rozwijalnej **Port Mapping Mode** wybierz opcję: **Auto**.
   • Aby zastosować mapowanie portów oparte na numerach portów określonych samemu:
   Z listy rozwijalnej **Port Mapping Mode** wybierz opcję: **Manual**.
   W ustawieniu **Manual** możesz wprowadzić własny żądany numer portu.



Rys. 6–23: Konfigurowane ustawienia dla funkcji NAT (tłumaczenie adresów)

3. Kliknij **Save**, aby zachować wprowadzone ustawienia.

6.3.12. Konfigurowanie ustawień protokołu FTP

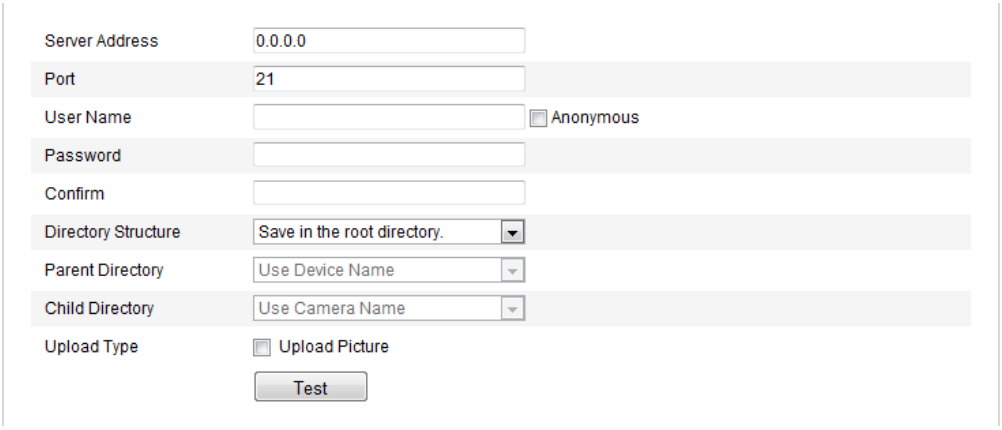
Cel czynności:

Możesz w ustawieniach kamery wprowadzić dane konfiguracyjne serwera FTP, aby umożliwić wysyłanie na ten serwer (upload) klatek wideo wychwytywanych z obrazu kamery. Wychwyt klatek wideo z kamery może być wyzwalany przez zdarzenie albo przez zadanie okresowe (task), zrzucające pojedyncze klatki.

Procedura wykonania:

1. Wyświetl interfejs ekranowy ustawień FTP:
   Configuration > Advanced Configuration > Network > FTP

[6] NAT = tłumaczenie adresów sieciowych



Rys. 6–24: Ustawienia do skonfigurowania serwera FTP

2. Skonfiguruj te ustawienia FTP — nazwa użytkownika **User Name** oraz hasło użytkownika **Password** będą wymagane do zalogowania się na serwerze FTP.

- *Dla ochrony Twojej własnej prywatności oraz dla lepszej ochrony Twojego systemu od źródeł zagrożeń sieciowych zdecydowanie zalecamy zastosowanie **silnych haseł** do wszystkich funkcji i urządzeń sieciowych. Hasło takie powinno być czymś, co samemu sobie wybierzesz, (powinno być w nim minimum 8 znaków, w tym co najmniej trzy z następujących kategorii znakowych: litery wielkie, litery małe, cyfry, znaki specjalne), aby podnieść poziom zabezpieczenia Twojego produktu (kamery).*
- *Odpowiedzialność za właściwe skonfigurowanie wszystkich haseł i innych nastaw zabezpieczających spoczywa na instalatorze oraz/lub użytkowniku końcowym (tj. konsumencie/odbiorcy) instalowanego rozwiązania.*

Katalog dla uploadu plików: Z listy rozwijalnej **Directory Structure**, możesz wybrać docelowe miejsce dla plików (**Save to the...**): w katalogu głównym (...**root directory**), w katalogu nadrzędnym (...**parent directory**), w katalogu potomnym (...**child directory**). Jeśli wybierzesz z tej listy opcję ...**parent directory**, to będziesz mógł ponadto określić, co system ma przyjąć za nazwę katalogu nadrzędnego: nazwę urządzenia (**Use Device Name**), numer urządzenia (**Use Device Number**), IP urządzenia (**Use Device IP**). Jeśli natomiast wybierzesz opcję ...**child directory**, to będziesz mógł określić, że system ma przyjąć za nazwę katalogu potomnego: nazwę/etykietę kamery (**Camera Name**) lub numer kamery (**Camera No.**).

Treść uploadu (Upload type): Zaznacz to pole, aby załączyć uploadowanie wychwyconych klatek na ten wyspecyfikowany serwer FTP.

Dostęp do serwera FTP jak użytkownik anonimowy: po zaznaczeniu pola wyboru **Anonymous** nie jest wymagane wprowadzenie nazwy użytkownika, ani hasła użytkownika. Zaznacz pole **Anonymous**, aby włączyć logowanie się na serwer FTP jako użytkownik typu anonimowego (tj. bez wymogu podawania danych uwierzytelniających).

Uwaga: Aby opcja dostępów realizowanych anonimowo zadziałała, konfigurowany tu serwer FTP musi ją obsługiwać.

3. Kliknij **Save**, aby zachować wprowadzone ustawienia.

   Uwaga: Jeśli chcesz wysyłać wychwycone klatki wideo na serwer FTP, to na stronie **Snapshot** musisz załączyć w kamerze funkcję wychwytu okresowego lub funkcję wychwytu inicjowanego przez zdarzenie. Dokładniejszy opis tych ustawień — zob. *podrozdz. 7.3* (str. 136).

6.3.13. Dostęp poprzez chmurę sieciową

Funkcja dostępu **EZVIZ Cloud P2P** zapewnia możliwość zarządzania urządzeniami na platformie łączności via chmura sieciowa EZVIZ P2P.

Uwaga: Opisywana tu funkcja dostępu ma różne własności/działanie w różnych modelach kamery. Żeby można było z niej skorzystać, kamera musi ją obsługiwać.

Zaznacz pole wyboru **Enable**, aby załączyć funkcję chmury P2P EZVIZ — wtedy będziesz w stanie zarządzać urządzeniem przez witrynę chmury EZVIZ P2P albo też za pomocą klienta chmury EZVIZ P2P w postaci aplikacji na telefony komórkowe.

Niektórzy użytkownicy mogą nie chcieć zarządzania urządzeniami poprzez chmurę EZVIZ P2P — wtedy możesz zostawić to pole wyboru w stanie niezaznaczonym.

Rys. 6–25: Ustawienia do skonfigurowania dostępu przez chmurę

6.3.14. Ustawienia HTTPS

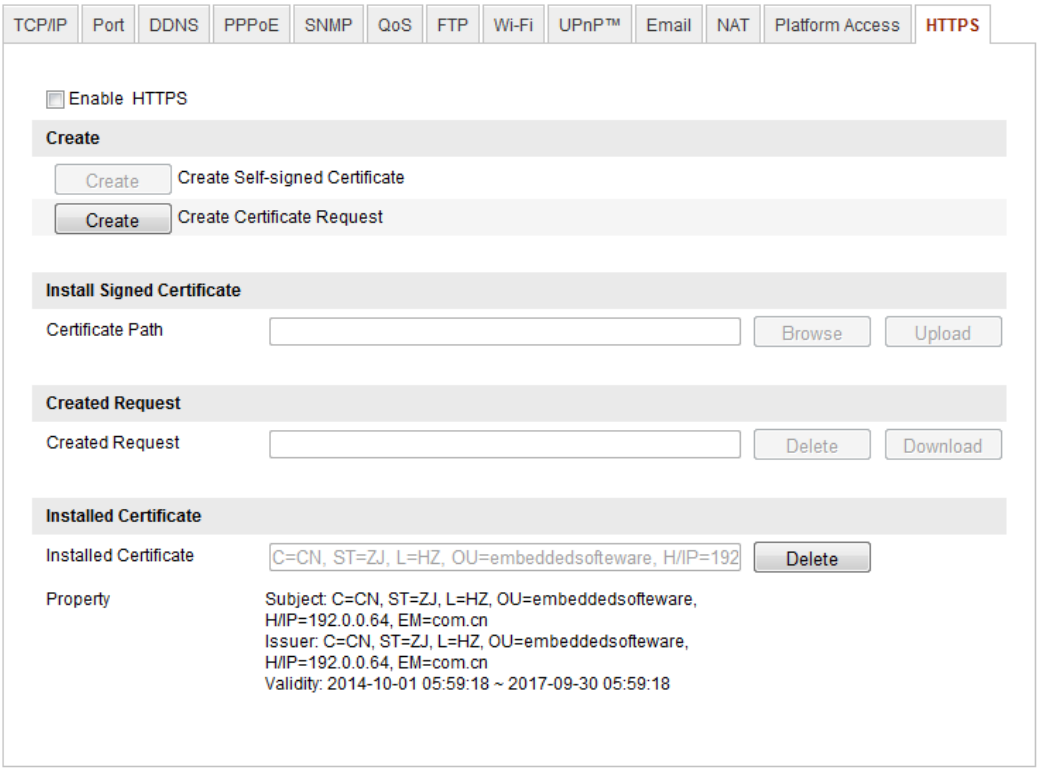
Cel czynności:

Protokół HTTPS zapewnia uwierzytelnianie witryny i związanego z nią web-serwera (z którym ktoś się komunikuje), co zabezpiecza przed atakami MITM (*man-in-the-middle*). Wykonaj poniższe kroki, aby skonfigurować numer portu dla HTTPS.

Przykład: Jeśli jako numer portu wprowadzisz 443, a adresem IP urządzenia jest 192.168.1.64, to uzyskasz dostęp do tego urządzenia z przeglądarki internetowej przez wpisanie w niej ciągu adresowego następującej treści: **https://192.168.1.64:443**.

Procedura wykonania:

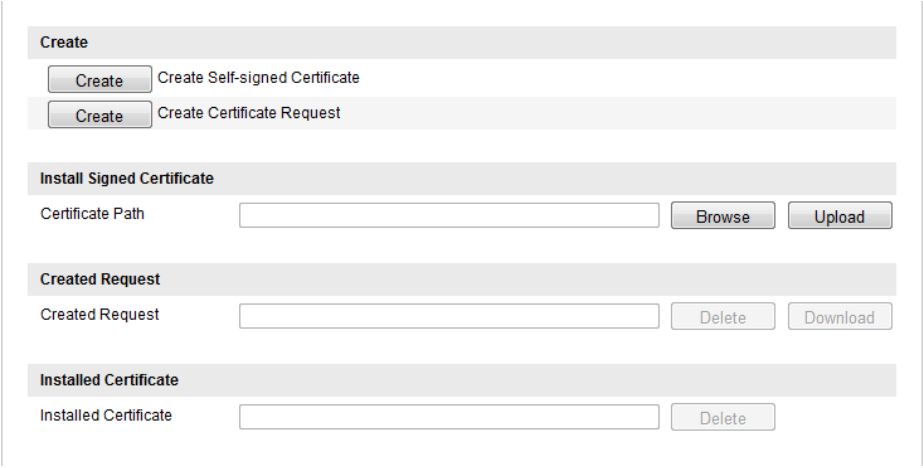
1. Wyświetl interfejs ekranowy ustawień HTTPS.
   Configuration > Advanced Configuration > Network > HTTPS
2. Zaznacz pole wyboru **Enable HTTPS**, aby załączyć funkcjonalność HTTPS.
3. Utwórz certyfikat z własnym podpisem albo certyfikat zewnętrznie uwierzytelniony.



Rys. 6–26: Ustawienia do skonfigurowania protokołu HTTPS

- Utwórz certyfikat z własnym podpisem

1) Kliknij przycisk **Create** (Create self-signed certificate), aby wyświetlić interfejs tworzenia certyfikatu.



Rys. 6–27: Interfejs z ustawieniami do tworzenia certyfikatu z własnym podpisem

2) Wprowadź kraj, nazwę/IP hosta, termin ważności i dane pozostałe.
3) Kliknij przycisk **OK**, aby zachować wprowadzone ustawienia.

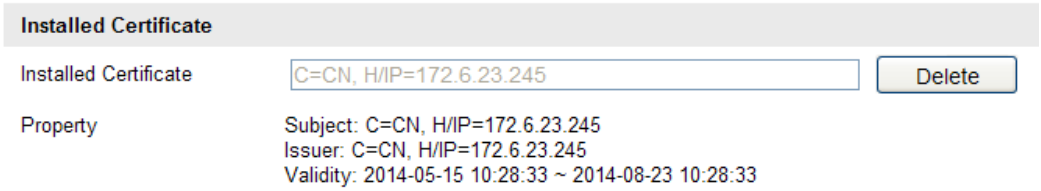
Uwaga: Jeśli już wcześniej zainstalowałeś jakiś certyfikat, to przycisk **Create Self-signed Certificate** będzie przygaszony (=stan nieaktywny).

- Utwórz certyfikat zewnętrznie uwierzytelniany

1) Kliknij przycisk **Create** (Create Certificate Request), aby wygenerować zamówienie certyfikatu.

2) Pobierz to zamówienie certyfikatu i przedłóż je do podpisu w renomowanym urzędzie, wydającym certyfikaty.
3) Po otrzymaniu podpisanego, ważnego certyfikatu, zaimportuj go do urządzenia.

4. Po pomyślnym utworzeniu i zainstalowaniu certyfikatu będzie się wyświetlała stosowna „metryczka” opisująca go (zob. pole **Property**):



Rys. 6–28: Treść pól interfejsu, gdy w urządzeniu zainstalowano certyfikat HTTPS

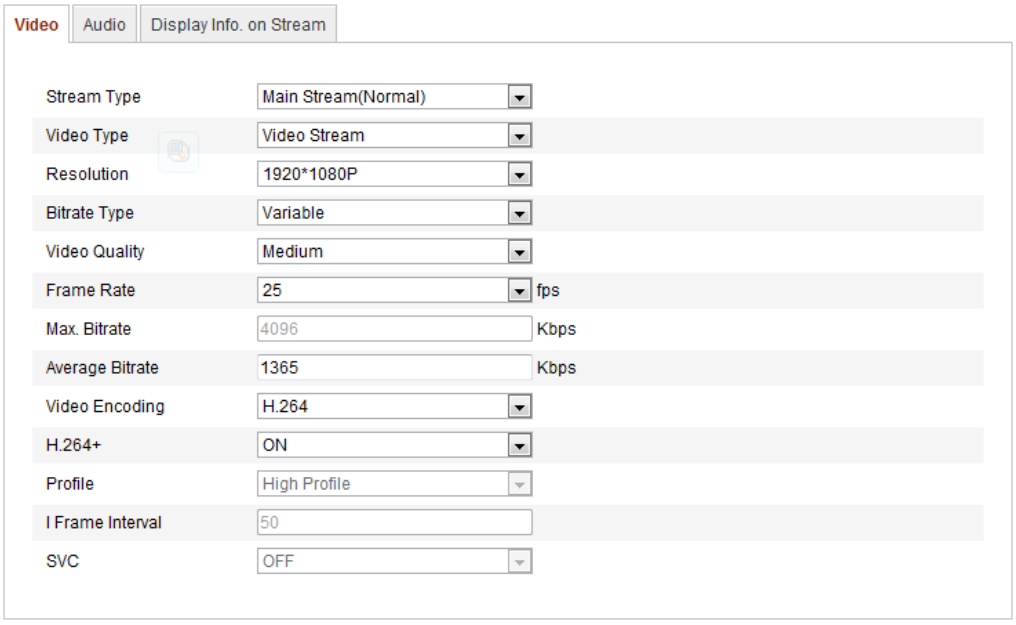
5. Kliknij przycisk **Save**, aby zachować wprowadzone ustawienia.

6.4. Skonfiguruj ustawienia definiujące obraz i dźwięk

6.4.1. Ustawienia transmisji obrazu kamery

Procedura wykonania:

1. Wyświetl interfejs ekranowy ustawień obrazu:
   Configuration > Basic Configuration > Video / Audio > Video
   albo też: **Configuration > Advanced Configuration > Video / Audio > Video**



Rys. 6–29: Ustawienia do skonfigurowania transmisji obrazu

2. Wybierz z listy **Stream Type** rodzaju strumienia dla kamery: **Main Stream(Normal)**, **Sub-stream** lub **Third stream**.

   Strumień główny (**Main Stream**) służy zwykle do rejestrowania obrazu i przesyłu podglądu bieżącego przy odpowiednio dobrym dostępnym paśmie transmisyjnym. Natomiast pod-strumień (**Sub-stream**) czy strumień trzeci

(Third Stream) można wykorzystać do przesyłu podglądu bieżącego, gdy wielkość dostępnego pasma daje ograniczone możliwości transmisyjne.

3. Możesz dopasować do własnych potrzeb następujące parametry wybranego strumienia głównego (Main Stream) lub podstrumienia (Sub-stream):

Rodzaj treści wideo (Video Type):

Z listy Video Type możesz wybrać jako rodzaj wideo następujące opcje: strumień wideo (Video Stream), strumień zespolony audio-wideo (Video&Audio Composite Stream). Uzyskasz w materiał wideo zarejestrowany z sygnałem fonii (dźwiękiem) tylko wtedy, gdy wybierzesz opcję Video&Audio.

Rozdzielczość obrazu (Resolution):

Wybierz rozdzielczość dla obrazu podawanego z kamery.

Szybkość bitowa transmisji (Bitrate Type):

Wybierz z tej listy rozwijalnej żądaną szybkość transmisji strumienia: utrzymywaną na stałym poziomie (constant) lub zmienną (variable).

Jakość obrazu (Video Quality):

Jeżeli z listy Bitrate Type wybrałeś szybkość Variable, to w tej liście rozwijalnej masz 6 poziomów jakości obrazu do wyboru (np. Medium).

Szybkość odświeżania obrazu (Frame Rate):

Wybierz dla szybkości obrazu wartość z przedziału 1/16~25 fps. Parametr Frame Rate określa częstotliwość, z którą strumień wideo kamery jest na bieżąco odświeżany i jest ona tu wyrażana w klatkach na sekundę (kl/s=fps). Wyższe wartości Frame Rate okazują się pożądane w przypadkach, gdy w strumieniowanym obrazie kamery widać ruch, gdyż są w stanie zapewnić w każdej dowolnej chwili przesyłu odpowiednią jakość obrazu.

Maks. szybkość bitowa transmisji (Max. Bitrate):

Określ maks. szybkość transmisji Max.Bitrate wartością z przedziału 32~16384 Kbps. Wyższe wartości odpowiadają wyższej jakości obrazowej wideo, ale wymagają większej części dostępnego pasma.

Uwaga: Górna granica maksymalnej szybkości strumienia Max. Bitrate jest różna dla różnych platform kamer. W pewnych określonych kamerach może wynosić 8192Kbps albo 12288Kbps.

Kodowanie obrazu (Video Encoding):

Jeżeli z listy Stream Type wybrałeś strumień główny Main Stream, to w tej liście rozwijalnej masz do wyboru następujące opcje (kodeki): H.264, MPEG4. Jeśli natomiast wybrałeś tam Sub-stream lub Third stream, to do wyboru masz kodeki: H.264, MJPEG, MPEG4.

Uwaga: Napotkasz różne enkodowanie obrazu na różnych platformach kamer. W pewnych określonych kamerach kodek **H.264** będzie obsługiwany, a kodek **MPEG4** – już nie.

H.264+:

Jeśli jako rodzaj strumienia (**Stream Type**) wybrałeś strumień główny (**Main Stream**), a jako kodowanie obrazu kamery (**Video Encoding**) wybrałeś kodek **H.264**, to zobaczysz w interfejsie parametr **H.264+** otwarty do skonfigurowania. H.264+ to nowoczesna technologia enkodująco-kompresująca. Dzięki załączeniu w ustawieniach opcji H.264+ (**ON**) operator może obliczyć stopień zużycia wolnego miejsca na HDD na podst. przeciętnej szybkości transmisji strumienia, w tym może oszczędzić to miejsce przez obniżenie tej szybkości. Załączenie (**ON**) lub odłączenie (**OFF**) funkcji H.264+ wymaga przeładowania kamery (reboot), żeby zmiana zaczęła obowiązywać w systemie.

Po załączeniu funkcji H.264+ (=**ON**): jeśli wybierzesz dla **Bitrate Type** szybkość zmienną (**Variable**), to możesz też wprowadzić żądaną przeciętną szybkość transmisji strumienia — **Average Bitrate**. Wtedy, na jej podstawie, możesz obliczać zużycie wolnego miejsca na HDD; ewentualnie możesz zmienić wartość **Average Bitrate** ręcznie, pamiętając jednak, że musi być mniejsza niż wartość maks. szybkości transmisji, widoczna w polu **Max. Bitrate**.

Uwagi:

- Przy załączonej funkcji H.264+ parametry: profil (**Profile**), odstęp klatek typu I (**I frame interval**), SVC (**SVC**) i maks. szybkość bitowa strumienia (**Max. Bitrate**) są przygaszone, o ile w **Bitrate Type** wybrano **Variable**. Jeśli natomiast w **Bitrate Type** wybierzesz **Constant**, to wtedy przygaszone będą parametry: **Video Quality**, **Profile**, **I frame interval** oraz **SVC**.

Przy załączonej opcji H.264+ wiele funkcji, w tym: **ROI**, **Clipping**, **Third stream**, **Smart event**, **Display info. on stream**, **Counting** oraz **Rotate** nie będzie obsługiwanych.

Profil (Profile):

Do wyboru w tej liście rozwijalnej są następujące profile operacji kodowania: podstawowy (**Basic profile**), główny (**Main Profile**), wysoki (**High Profile**).

Odstęp klatek typu I (I Frame Interval):

Wprowadź tu odstęp dla klatek typu I-Frame jako wartość z zakresu: **1~400**.

Kodowanie skalowane (SVC):

Kodowanie skalowane (SVC) jest rozszerzeniem standardu H.264/AVC. Wybierz z tej listy rozwijalnej opcję **OFF/ON**, aby odpowiednio odłączyć/załączyć funkcję SVC. Możesz też wybrać tu opcję **Auto**, a wtedy — w sytuacjach nie wystarczającego pasma transmisyjnego w sieci — urządzenie automatycznie wydobędzie potrzebne klatki z pierwotnego strumienia video.

Wygładzanie (Smoothing):

Chodzi tu o tzw. wygładzanie strumienia. Im wyższa wprowadzona tu wartość regulacyjna (Smoothing), tym lepsza płynność strumienia, choć jednocześnie jakość obrazu może być niezbyt zadowalająca. I odwrotnie: im niższa wartość Smoothing, tym wyższa jakość strumienia, lecz przy tym strumień może wydawać się nie wystarczająco płynny.

4. Kliknij przycisk **Save**, aby zachować wprowadzone tu ustawienia.

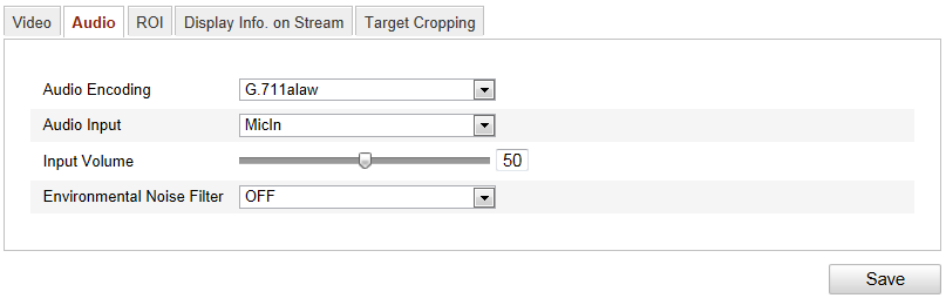
Uwaga:

Dostępne parametry wideo mogą być różne dla różnych modeli kamer — faktycznie dostępne funkcje kamer należy odczytywać ze stron faktycznie przez nie wyświetlanych.

6.4.2. Ustawienia transmisji dźwięku

Procedura wykonania:

1. Wyświetl interfejs ekranowy ustawień dźwięku:
   Configuration > Basic Configuration > Video / Audio > Audio
   albo: **Configuration > Advanced Configuration > Video / Audio > Audio**



Rys. 6–30: Ustawienia do skonfigurowania transmisji dźwięku

2. Skonfiguruj następujące ustawienia.
   Uwaga: Ustawienia dźwięku są różne w różnych modelach kamer.

Kodowanie dźwięku (Audio Encoding): W tej liście rozwijalnej do wyboru są następujące kodowania: G.722.1, G.711 ulaw, G.711alaw, G.726, MP2L2, PCM. W razie wybrania MP2L2 możesz dodatkowo skonfigurować częstotliwość próbkowania dźwięku i szybkość strumienia, a w przypadku PCM możesz dodatkowo skonfigurować tylko częstotliwość próbkowania dźwięku.

Źródło wejściowe dźwięku (Audio Input): Z tej listy rozwijalnej możesz wybrać MicIn, LineIn oznaczające odpowiednio podłączony mikrofon, przetwornik elektroakustyczny (z poziomem sygnału Line).

Poziom głośności sygn. wejściowego (Input Volume): Regulacja suwakiem w zakresie 0~100.

Filtr szumów otoczenia (Environmental Noise Filter): Wybierz z tej listy rozwijalnej ON, żeby filtr ten załączyć bądź wybierz OFF, żeby go odłączyć. Gdy

funkcja ta jest załączona, system odfiltruje z dźwięku kamery pewną część przeszkadzających dźwięków, tzw. szumów otoczenia.

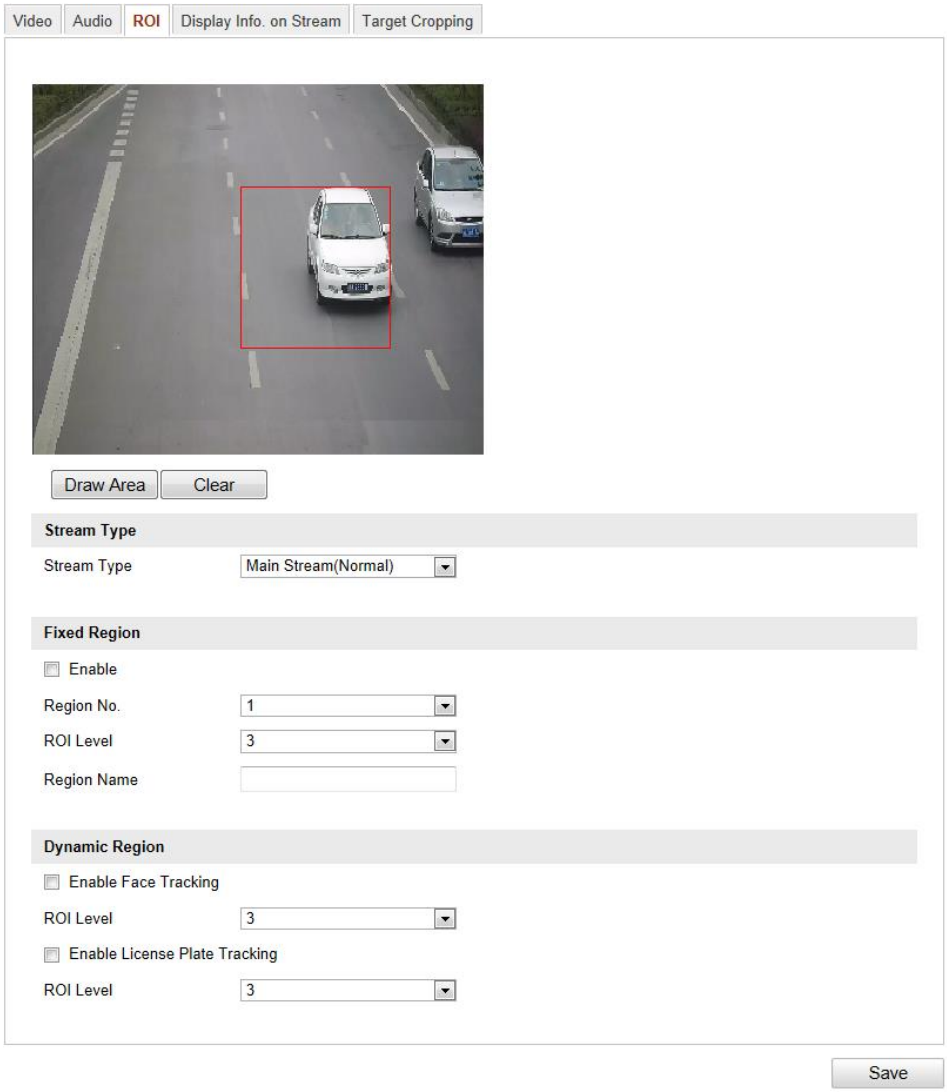
3. Kliknij przycisk **Save**, aby zachować wprowadzone ustawienia.

6.4.3. Konfigurowanie kodowania obszarów ROI

Cel czynności:

Zakodowanie obszarów interesujących ROI[7] w strumieniu kamery pomaga, dla kompresowania obrazu kamery, odróżnić wideo-informację obszarów istotnych (tj. ROI) od wideo-informacji tła sceny. W efekcie, algorytm kodujący alokuje więcej zasobów enkodujących dla obszarów ROI (niż do obszaru tła), dzięki czemu podnosi jakość/szczegółowość obrazu w obrębie ROI w stosunku do jakości obszarów pozostałych (tło), na które kładzie mniejszy nacisk.

Uwaga: Zakres/dostępność funkcji ROI jest różna w różnych modelach kamer.



Rys. 6–31: Ustawienia służące do konfigurowania obszarów ROI

[7] ROI = **R**egion **O**f **I**nterest (wydzielony obszar w kadrze, szczególnie istotny/cenny z punktu widzenia monitoringu sceny) — przyp. tłum.

Skonfigurowanie obszaru stałego ROI (Fixed Region):

Procedura wykonania:

1. Wyświetl interfejs ekranowy z ustawieniami obszarów ROI:
   Configuration > Advanced Configuration > Video/Audio > ROI
2. W grupie ustawień **Fixed Region** zaznacz pole wyboru **Enable**, aby załączyć funkcję obszarów stałych ROI.
3. Z listy rozwijalnej **Stream Type** wybierz rodzaj strumienia, w którym mają być enkodowane obszary ROI kamery.
4. Z listy rozwijalnej **Region No.** wybierz żądany obszar ROI do skonfigurowania jego ustawień. Są tu do wyboru 4 (cztery) obszary stałe.
5. Kliknij przycisk **Draw Area** (wejście w tryb rysowania obszaru), a następnie kliknij–i–przeciągnij myszą po obrazie bieżącym sceny, aby zakreślić ten interesujący obszar ROI.
6. Z listy rozwijalnej **ROI Level** wybierz poziom poprawy jakości obrazu dla tego obszaru. Im większa wartość, tym lepsza jakość obrazu (w obszarze).
7. Wprowadź swoją, żądaną etykietę dla tego obszaru ROI.
8. Kliknij przycisk **Save**, aby zachować wprowadzone ustawienia.

Skonfigurowanie obszarów dynamicznych ROI (Dynamic Region):

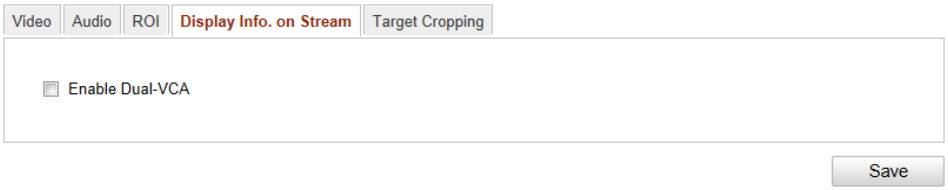
1. Wyświetl interfejs ekranowy z ustawieniami obszarów ROI:
   Configuration > Advanced Configuration > Video/Audio > ROI
2. W grupie ustawień **Dynamic Region** zaznacz pole wyboru **Enable Face Tracking** (załącz śledzenie twarzy), a wówczas obszar obrazu, zawierający jakąś wykrytą twarz, zostaje dynamicznie przyjęty/zdefiniowany przez system jako obszar ROI.

   Uwaga: Aby można było tu załączyć ww. funkcję śledzenia twarzy, Twoja kamera musi obsługiwać funkcję wykrywania twarzy (face detection function) i musi mieć ją uaktywnioną.
3. Zaznacz pole wyboru **Enable License Plate Tracking** (śledzenie tablic rejestracyjnych), wówczas obszar obrazu, zawierający jakąś wykrytą tablicę rejestracyjną, zostaje dynamicznie przyjęty/zdefiniowany przez system jako obszar ROI.

   Uwaga: Aby można było załączyć tę funkcję śledzenia tablic rejestracyjnych, Twoja kamera musi obsługiwać funkcję wykrywania pojazdów (vehicle detection function) i musi mieć ją uaktywnioną.
4. Wybierz poziom poprawy jakości obrazu **ROI Level** dla powyższych ewentualnie załączonych obszarów dynamicznych. Im większa wartość, tym lepsza jakość obrazu (w obrębie danego obszaru).
5. Z listy rozwijalnej **Stream Type** wybierz rodzaj strumienia, w którym mają być enkodowane obszary ROI kamery.
6. Kliknij przycisk **Save**, aby zachować wprowadzone ustawienia.

6.4.4. Wyświetlenie danych o strumieniu

Na karcie **Display Info. on Stream**, zaznacz pole wyboru **Enable Dual-VCA**, aby do strumienia kamery były wstawiane znaczniki z informacjami o obiektach (np. osoby, pojazdy, itd.). Po zaznaczeniu tego pola, możesz zdefiniować żądane reguły (**Rule**) w podłączonym urządzeniu końcowym (rear-end device), które mają wykrywać interesujące zdarzenia — w tym: przekroczenia linii detekcyjnej, wtargnięcia / naruszenia obszaru, itp.



Rys. 6–32: Ustawienie **Display Info. on Stream** zapewniające wstawienie do strumienia specjalnych informacji detekcyjnych

6.4.5. Przycięcie powierzchni obrazu do wykrytego celu

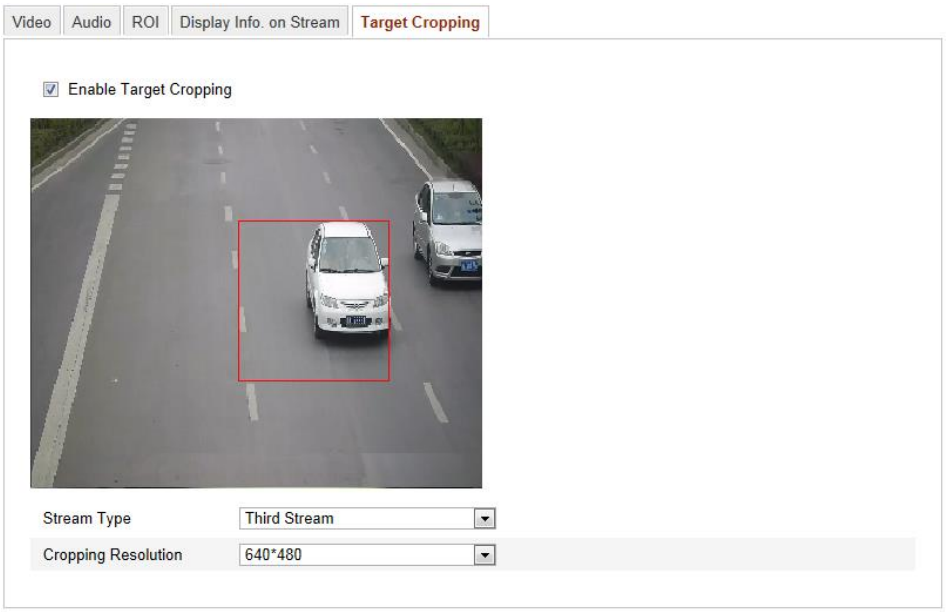
Cel czynności:

Na podglądzie bieżącym kamery możesz zdefiniować myszą pewien ważny, prostokątny fragment sceny jako cel monitoringowy, aby móc go wyświetlać w trzecim strumieniu (Third Stream) w odpowiednio podwyższonej rozdzielczości obrazowej (Cropping Resolution), którą sam zadasz w ustawieniach. Dzięki temu w ważnym miejscu sceny będziesz w razie potrzeby dysponować większą liczbą szczegółów do analizy.

Uwaga: Zakres/dostępność funkcji przycinania obrazu do celu jest różna w różnych modelach kamer.

Procedura wykonania:

1. Wyświetl interfejs ekranowy do konfigurowania przycięcia obrazu do celu: **Configuration > Advanced Configuration > Video/Audio > Target Cropping.**
2. Zaznacz pole wyboru **Enable Target Cropping** (zob. następna ilustracja), aby załączyć funkcję przycięcia.
3. Z listy **Stream Type**, jako rodzaj docelowego strumienia, wybierz strumień trzeci (**Third Stream**).
4. Z listy **Cropping Resolution** wybierz rozdzielczość obrazową dla wycinka obrazu stanowiącego Twój cel monitoringowy w scenie. Na podglądzie bieżącym kamery widać teraz nałożoną czerwoną ramkę, która pokazuje aktualny obszar Twojego celu monitoringowego — przez kliniecie-i-przeciągnięcie myszą możesz tę ramkę umieścić w żądanym miejscu sceny.
5. Kliknij przycisk **Save**, aby zachować wprowadzone ustawienia. Po tym możesz przejść do strony **Live View** (zob. str. 35) i kliknąć na niej zakładkę **Third Stream**, aby wyświetlić na niej obraz z obszaru wyżej zdefiniowanego celu.



Rys. 6–33: Ustawienia pozwalające skonfigurować funkcję przycięcia sceny do celu monitoringowego (Target Cropping)

6.5. Konfigurowanie parametrów obrazu

6.5.1. Konfigurowanie ustawień wyświetlania obrazu

Cel czynności:

W tych ustawieniach możesz wyregulować parametry, wpływające na jakość i wygląd obrazu kamery — w tym poziom: jaskrawości, kontrastu, nasycenia koloru, przechyłu odcienia koloru, wyostrzenia i tak dalej.

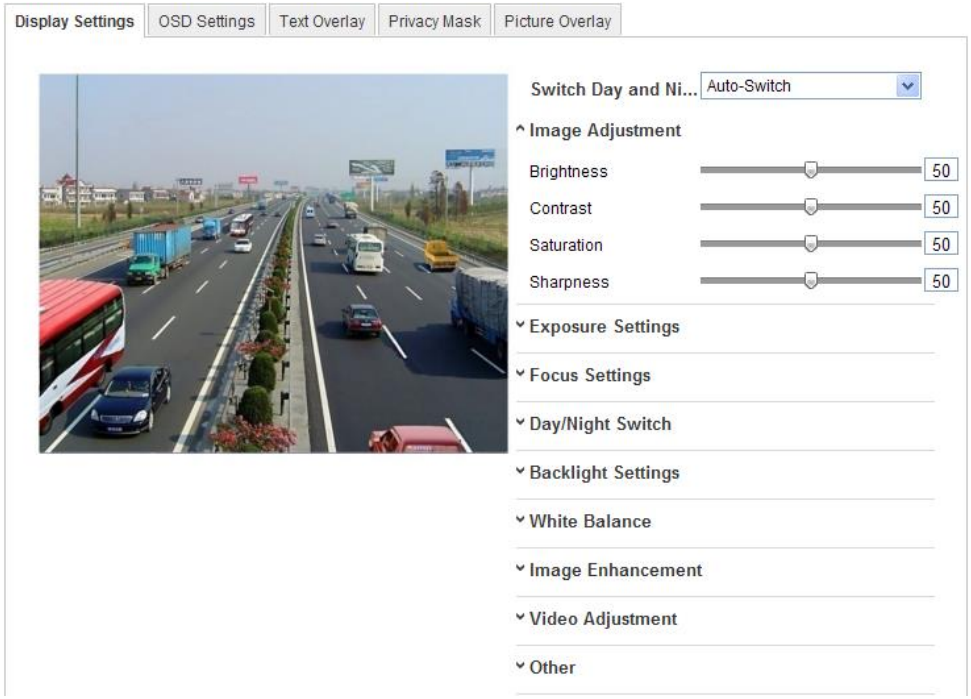
Uwaga: Dostępność parametrów wyświetlania obrazu jest różna w różnych modelach kamery. Odszukaj faktycznie dostępne parametry na interfejsie ekranowym tej konkretnej kamery.

Procedura wykonania:

1. Wyświetl interfejs ekranowy z ustawieniami wyświetlania obrazu:
   Configuration > Basic Configuration> Image> Display Settings
   albo też: **Configuration > Advanced Configuration> Image> Display Settings**
2. Wyreguluj parametry obrazu kamery.

Uwaga: Aby zagwarantować odpowiednio wysoką jakość obrazu kamery w różnych warunkach oświetleniowych, użytkownik może skonfigurować dwa różne zestawy parametrów obrazu.

Tryb Dzień/Noc – przełączanie automatyczne (Auto-Switch)



Rys. 6–34: Ustawienia konfigurujące wyświetlanie podglądu kamery (automatyka D/N)

♦ **Regulatory obrazu –** Image Adjustment

Poziom jaskrawości (**Brightness**) – tym suwak pozwala wyregulować żądaną jaskrawość obrazu, w zakresie **1~100**; nastawą domyślną jest: **50**.

Poziom kontrastu (**Contrast**) – ten suwak pozwala wyregulować żądaną kontrastowość obrazu, w zakresie **1~100**; nastawą domyślną jest: **50**.

Poziom nasycenia koloru (**Saturation**) – ten suwak pozwala wyregulować żądane natężenie/siłę koloru w obrazie, w zakresie **1~100**; nastawą domyślną jest: **50**.

Poziom wyostrzenia (**Sharpness**) – ten suwak pozwala wyregulować żądaną siłę wyostrzenia krawędzi/konturów w treści obrazowej, w zakresie **1~100**; nastawą domyślną jest: **50**.

♦ **Regulatory naświetlania –** Exposure Settings

W przypadku kamer, mających obiektyw nieautomatyczny (fixed), daje się wybrać tylko opcję **Manual**, a metody pracy przysłony obiektywu (**Iris Mode**) nie daje się konfigurować.

Jeśli masz możliwość i wybierzesz tu opcję **Auto**, to możesz wyregulować poziom przysłony w zakresie **0~100**.

W przypadku kamer obsługujących przysłonę **P-Iris** i przy założeniu, że w kamerze zainstalowano obiektyw z przysłoną P-Iris [np.: Tamron 2,8-8 mm F/1,2 (M13VP288-IR)], można tu wybrać opcję **P-Iris**. A jeśli w kamerze zainstalowano obiektyw typu DC, to można tu wybrać opcję **Manual** bądź opcję **Auto**.

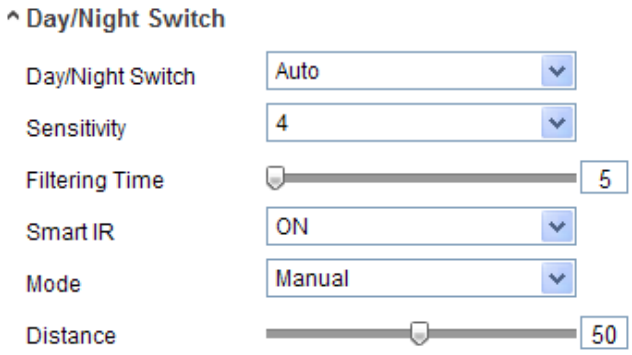
Czas naświetlania (**Exposure Time**) oznacza czas otwarcia migawki elektronicznej, dostępny do regulacji w zakresie wartości **1~1/100000 s**. Wyreguluj ten czas zgodnie z faktycznymi warunkami oświetleniowymi panującymi w scenie.

♦ **Ustawienia nastawiania ostrości –** Focus Settings

W przypadku kamer obsługujących obiektywy elektroniczne, możesz wybrać z listy trybu ostrzenia[8] **Focus Mode** trzy opcje: **Auto** (automat), **Manual** (nastawianie ręczne), **Semi-auto** (nastawianie półautomatyczne). Jeżeli wybierzesz opcję **Auto**, ostrość obrazu jest regulowana w pełni automatycznie przez kamerę zgodnie z konkretną sytuacją w scenie. Jeśli wybierzesz **Manual**, to możesz (odpowiednią akcją ręczną w interfejsie ekranowym PTZ) wyregulować w obiektywie: wielkość zbliżenia (zoom+/–), plan ostrości (focus+/–), inicjalizację obiektywu, ostrzenie pomocnicze (na żądanie). Jeśli wybierzesz opcję **Semi-auto**, to kamera będzie nastawiała ostrość automatycznie, ilekroć zmienisz ręcznie wielkość zbliżenia (zoom).

♦ **Przełączanie trybu rejestracji Dzień⇔Noc –** Day/Night Switch

Wybierz tryb sterowania przełączaniem Dzień/Noc oraz skonfiguruj tu inteligentnie regulowany reflektor IR (**Smart IR**).



Rys. 6–35: Ustawienia do skonfigurowania funkcji przełączania Dzień/Noc

Z listy rozwijalnej **Day/Night Switch** możesz wybrać następujące opcje: **Day**, **Night**, **Auto**, **Schedule**, **Triggered By Alarm Input**, definiujące warunek przełączenia trybu rejestracji *Dzienna*/*Nocna*:

• **Dzień (Day):** brak przełączania — kamera stale utrzymuje tryb rejestracji *Dziennej*.

• **Noc (Night):** brak przełączania — kamera stale utrzymuje tryb rejestracji *Nocnej*.

• **Automatyczne (Auto):** kamera automatycznie przełącza tryb rejestracji, między *Dziennym* a *Nocnym*, na podstawie aktualnie panujących warunków oświetleniowych.

Czułość automatyki przełączania (**Sensitivity**) można wyregulować w zakresie: **0~7** (im wyższa wartość, tym łatwiej następuje przełączenie trybu rejestracji).

Czas przeciwzakłóceniowy (**Filtering Time**) oznacza opóźnienie czasowe operacji przełączenia trybu rejestracji. Można go zadać w zakresie: **5s~120s**.

• **Czasowe (Schedule):** wprowadź czas rozpoczęcia **Start Time** oraz czas zakończenia **End Time**, specyfikujące okres trwania danego trybu rejestracji (*Dzienny*/*Nocny*).

• **Wyzwalane przez wej. sygnał alarmowy (Triggered By Alarm Input):** przełączenie trybu rejestracji *Dzienny*/*Nocny* następuje wskutek pojawienia się na wejściu sygnału alarmowego. Możesz tu także wybrać tryb rejestracji (**Triggered Mode**) wyzwalany przez odebrany sygnał alarmowy: **Day** (*Dzienny*) bądź **Night** (*Nocny*).

[8] dokł. nastawianie na ostrość — przyp. tłum.

Dobór siły oświetlenia IR (Smart IR): Funkcja *Smart IR* daje użytkownikowi możliwość wyregulowania siły światła rzucanego z diod reflektora LED–IR na scenę, zapewniającą czytelny obraz — który nie jest ani prześwietlony (zbyt jasny) ani niedoświetlony (zbyt ciemny). Gdy z tej listy rozwijalnej wybierzesz opcję **ON**, aby załączyć *Smart IR*, w liście rozwijalnej **Mode** możesz wybrać 2 opcje: **Auto** i **Manual**.

- W opcji **AUTO** kamera będzie automatycznie dobierać siłę świecenia swoich diod IR–LED, stosownie do bieżących warunków oświetleniowych.

  Przykład: Jeśli dana scena jest aktualnie wystarczająco jasna, to kamera samoczynnie przełączy swoje IR–LED-y na *niższą* intensywność świecenia; jeśli natomiast aktualnie scena jest niewystarczająco jasna, to kamera samoczynnie przełączy LED-y IR na intensywność świecenia *wyższą*.
- Natomiast w opcji **Manual** możesz sam ustawić wartość odległości od kamery do obiektu obserwowanego (suwakiem **Distance**), aby wyregulować intensywność świecenia diod LED–IR kamery. Mała wartość odległości oznacza, że obiekt znajduje się blisko kamery/IR, więc kamera świeci swoimi IR–LED-ami z mniejszą siłą, aby uniknąć prześwietlenia sceny (tj. zbyt jasnego obrazu). I odwrotnie, duża wartość odległości oznacza, że obiekt znajduje się daleko od kamery/IR, więc kamera przełącza swoje LED–IR na wyższą siłę świecenia, aby uniknąć niedoświetlenia sceny (tj. zbyt ciemnego obrazu).

♦ **Korekcja dla obserwacji podświetlnej –** Backlight Settings

Funkcja BLC: Jeśli usiłujesz nastawić ostrość na obiekt ustawiony pod światło, to obiekt ten będzie zbyt ciemny i przez to niewystarczająco czytelny. Funkcja BLC kompensuje to tylne oświetlenie, rozświetlając obiekt obecny przed nim, aby stał się jaśniejszy i czytelniejszy. Dla tej funkcji dostępne są następujące opcje regulacyjne: **OFF**, **Up**, **Down**, **Left**, **Right**, **Center**, **Customize**.

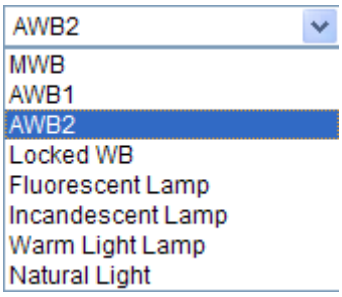
Funkcja WDR: Funkcję rozszerzonej rozpiętości tonalnej WDR (***W**ide **D**ynamic **R**ange*) możesz zastosować do obserwowania scen, w których panuje zbyt duży kontrast między partiami jasnymi a partiami ciemnymi (tj. zbyt duża dynamika).

Funkcja HLC: Funkcję korekcji wysokich świateł HLC (***H**igh **L**ight **C**ompression*) możesz zastosować wtedy, gdy w scenie są obecne mocne światła,[9] które pogarszają widoczność innych elementów/obszarów sceny.

♦ **Balans bieli –** White Balance

Balans bieli[10] to funkcja prawidłowej/wiernej reprodukcji bieli przez kamerę, umożliwiająca dobór najlepszej kompensacji zafałszowań koloru do aktualnej temperatury barwowej oświetlenia sceny.

[9] (np. reflektory lub ultra-jasne połyskliwe przedmioty, odbijające światło) — przyp. tłum.
[10] (dokł. korekcja punktu bieli) — przyp. tłum.



Rys. 6–36: Dostępne ustawienia do skonfigurowania balansu bieli

♦ **Poprawa obrazu –** Image Enhancement

Cyfrowa redukcja szumu (Digital Noise Reduction): Funkcja DNR redukuje szum obecny w strumieniu wideo. Do wyboru są opcje: **OFF**, **Normal Mode**, **Expert Mode**. Ustaw dla poziomu odszumiania DNR (**DNR level**) wartość z zakresu **0~100**. Wartość domyślna dla ww. trybu **Normal Mode** to: **50**. Natomiast po wybraniu ww. trybu **Expert Mode** możesz ustawić dwa poziomy DNR: przestrzenny **Space DNR level** [0~100] oraz czasowy **Time DNR level** [0~100].

Odmgławianie (Defog Mode): Możesz załączyć funkcję odmgławiania w sytuacjach, gdy obserwowane otoczenie wypełnia mgła, a podgląd z kamery jest zbyt mglisty. Funkcja wzmacnia widoczność delikatnych detali w obrazie, dzięki czemu obraz staje się czytelniejszy w odbiorze.

Stabilizator obrazu EIS (Electrical Image Stabilizer): Funkcja EIS osłabia wpływ ewentualnego drżenia kamery na jakość rejestrowanego przez nią obrazu.

Odcienie szarości (Grey Scale): Możesz wybrać nastawę regulacyjną odcieni szarości jako liczbę [**0~255**] lub [**16~235**].

♦ **Regulatory wizji –** Video Adjustment

Odbicie lustrzane (Mirror): Ta funkcja wykonuje odbicie lustrzane obrazu, aby operator mógł obserwować go w zażądanym układzie odwróconym. Do wyboru masz następuję opcje przekształceń lustrzanych: **Left/Right** (lewa po prawej, prawa po lewej), **Up/Down** (góra na dole, dół na górze), **Center** (lewy dolny w prawym górnym, prawy górny w lewym dolnym), **OFF** (brak przekształcenia).

Obrót (Rotate): Aby maksymalnie wykorzystać zalety obrazu o proporcjach 16:9, możesz załączyć funkcję **Rotate**, jeśli kamera musi obserwować scenę, ale ma zbyt wąskie pole widzenia.

Na etapie instalowania kamery obrócić ją o 90° bądź obróć jej obiektyw (3D) na 90°, po czym wybierz dla **Rotate** załączenie **ON**. Będziesz mieć wtedy na podglądzie normalny widok sceny z obrazem użytecznym o proporcjach 9:16, aby pominąć elementy niepotrzebne (np. ściany) i uzyskać pełniejszy informacyjnie widok sceny.

Typ sceny (Scene Mode): Wybierz tu rodzaj sceny: **indoor** (z wnętrza obiektu) bądź **outdoor** (na zewnątrz obiektu) zgodnie z charakterem faktycznie obserwowanego otoczenia.

Standard wizyjny (**Video Standard**): Są tu dwie opcje do wyboru: **50 Hz** i **60 Hz**. Wybierz opcję zgodnie z danym standardem wizji stosowanym u Ciebie; normalnie jest

to **50 Hz** dla systemu kodowania wizji PAL oraz **60 Hz** dla systemu kodowania wizji NTSC.

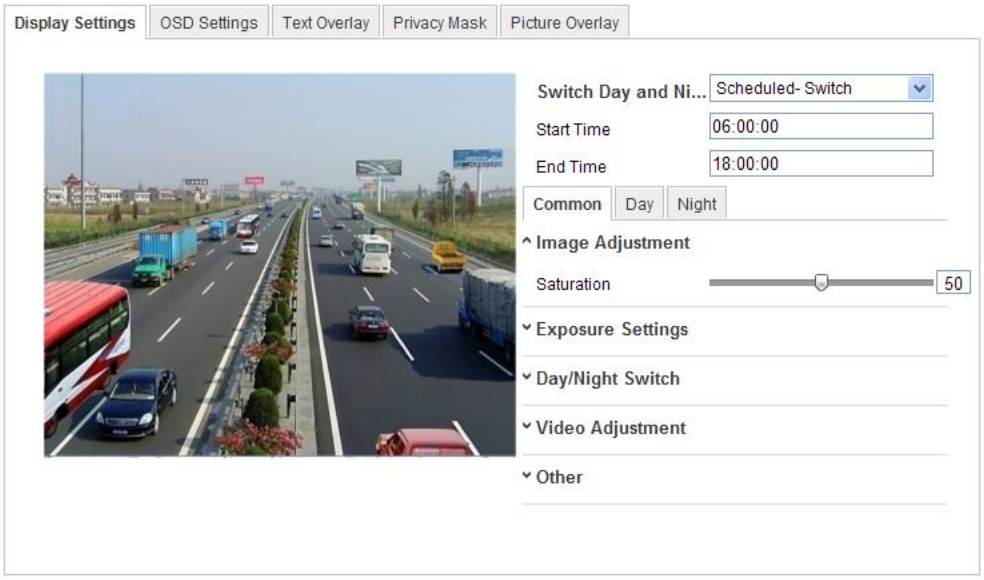
Tryb rejestracji (**Capture Mode**): Jest to wybieralny tryb wejściowego sygnału wizji, aby sprostać różnym wymogom, co do pola widzenia i rozdzielczości.

Korekcja optycznej dystorsji obiektywu (Lens Distortion Correction): Wybierz tu opcję **ON** / **OFF**, aby odpowiednio załączyć / odłączyć funkcję elektronicznego korygowania zniekształceń optycznych obiektywu kamery. Jeżeli załączysz w kamerze tę funkcję, to geometrycznie zniekształcony obraz kamery z obiektywem szerokokątnym będzie wyświetlany bez zniekształceń.

- **Inne ewentualnie dostępne ustawienia**
  Niektóre kamery obsługują sygnały wyjściowe: CVBS, SDI, HDMI — szczegóły jak w konkretnym modelu kamery.

Tryb Dzień/Noc – auto-przełączanie sterowane czasem (Scheduled-Switch)

W interfejsie ustawień dla przełączania trybu rejestracji Dzień/Noc na podst. czasu[11] możesz skonfigurować dwa oddzielne zestawy parametrów kamery — jeden dla okresu Dnia (**Day**) i jeden dla okresu Nocy (**Night**) — ażeby uzyskać zagwarantowaną, odpowiednią jakość obrazu z kamery w różnych warunkach oświetleniowych.



Rys. 6–37: Interfejs ustawień funkcji PRZEŁĄCZANIA TRYBU REJESTRACJI DZIEŃ/NOC — wariant z przełączaniem sterowanym za pomocą czasu (**Scheduled Switch**)

Procedura wykonania:

1. Kliknij oś czasu, aby wprowadzić czas rozpoczęcia (**Start Time**) i zakończenia (**End Time**), specyfikujące okres przełączania trybu Dzień/Noc.
2. Kliknij zakładkę **Common**, aby skonfigurować na jej karcie parametry wspólne, które mają być stosowane zarówno do trybu rejestracji Dziennej, jak i do trybu rejestracji Nocnej.

[11] tzn. gdy w liście rozwijalnej „Switch Day and Ni…" wybrano opcję „Scheduled-Switch" — przyp. tłum.

Uwaga: Dokładny opis poszczególnych parametrów podano w podrozdz. ***Tryb Dzień/Noc – przełączanie automatyczne (****Auto-Switch****)***, str. 72.

3. Kliknij zakładkę **Day**, aby skonfigurować na jej karcie parametry, stosujące się do trybu rejestracji *Dziennej*.
4. Kliknij zakładkę **Night**, aby skonfigurować na jej karcie parametry, stosujące się do trybu rejestracji *Nocnej*.

   Uwaga: Powyższe ustawienia zostają zachowane automatycznie, gdy tylko zmienisz wartość któregoś z parametrów.

6.5.2. Konfigurowanie danych wyświetlanych na podglądzie kamery

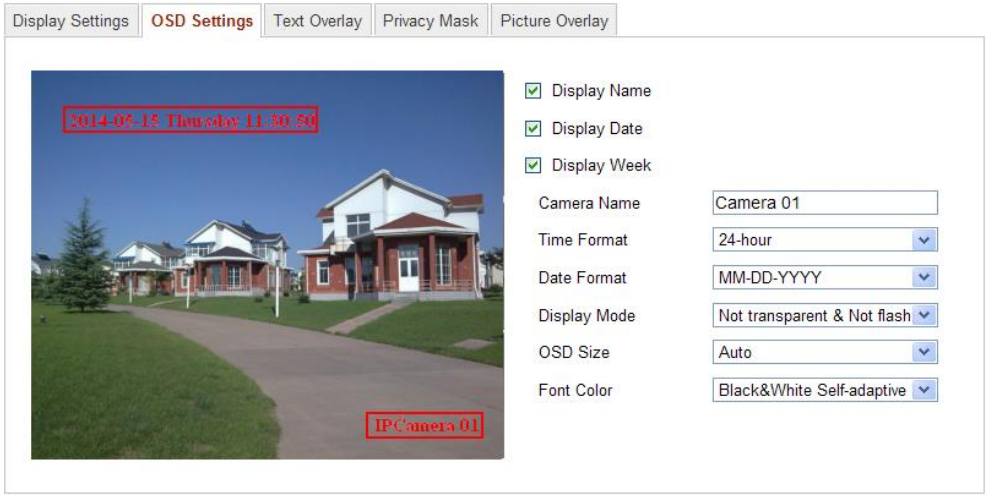
Cel czynności:

Możesz wybrać i sformatować wg własnych potrzeb dane wyświetlane jako nakładka ekranowa OSD (etykietę kamery, czas, datę) na podgląd bieżący kamery.

Procedura wykonania:

1. Wyświetl interfejs ekranowy ustawień wyświetlania danych OSD:

   Configuration > Advanced Configuration > Image > OSD Settings



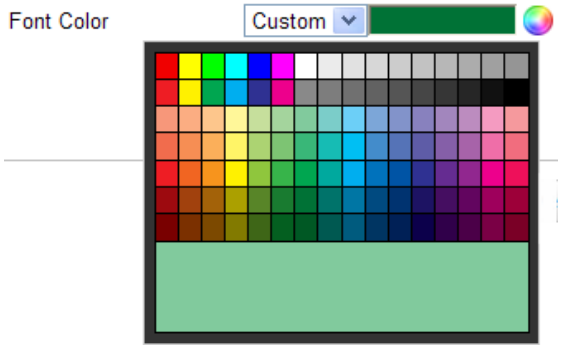
Rys. 6–38: Ustawienia do skonfigurowania wyświetlania nakładki ekranowej OSD

2. Zaznacz pole wyboru, odnoszące się do wyświetlania danych OSD,[12] które potrzebujesz widzieć na podglądzie kamery: etykieta kamery (**Display Name**), data (**Display Date**), tydzień (**Display Week**).
3. W polu tekstowym **Camera Name** wpisz etykietę dla tej kamery.
4. Z listy rozwijalnej **Time Format** wybierz format wyświetlania czasu.
   Z listy rozwijalnej **Date Format** wybierz format wyświetlania daty kalendarzowej.
   Z listy rozwijalnej **Display Mode** wybierz metodę wyświetlania danych OSD na podglądzie kamery (np. **Not transparent & Not flashing** = nieprzezorczyste i nie-migające).

[12] dane OSD (**O**n-**S**creen **D**isplay) to zestaw danych (czas, data, etykieta kamery), nakładanych na podgląd kamery w UI operatora — przyp. tłum.

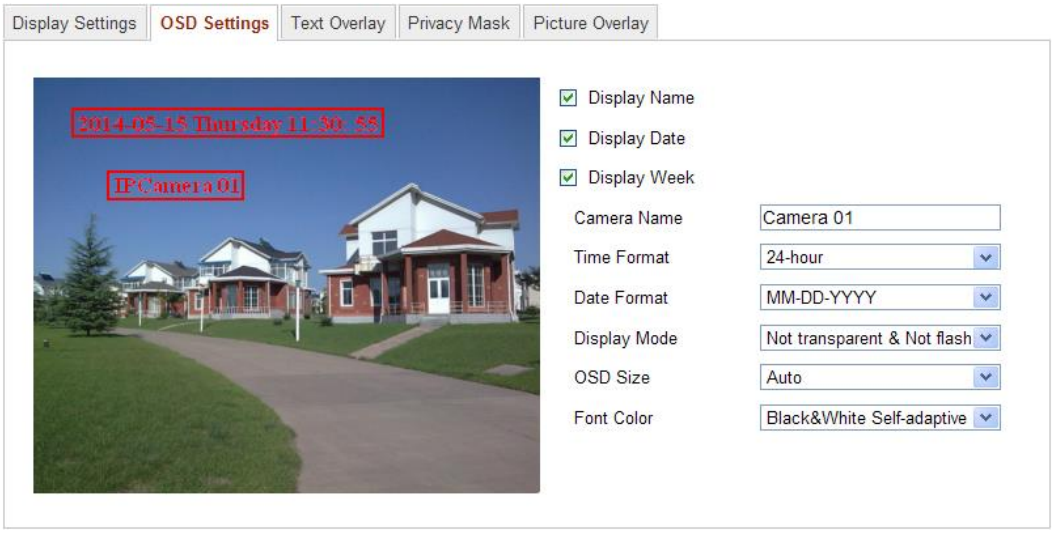
Z listy rozwijalnej **OSD Size** wybierz wielkość czcionki dla wyświetlanych danych.

5. Określ kolor czcionki dla całego zestawu danych OSD przez kliknięcie listy rozwijalnej **Font Color** — są tam do wyboru opcje: czarno-białe (**Black&White**), kolor dopasowywany automatycznie (**Self-adaptive**), kolor własny (**Custom**).



Rys. 6–39: Wybranie z palety własnego koloru czcionki (**Custom**) dla danych OSD

6. (*Ewentualnie*): W oknie podglądu bieżącego kamery kliknij kursorem myszy widoczną tam ramkę tekstową IPCamera 01 i przeciągnij ją po podglądzie, jeśli potrzebujesz przesunąć tę daną w inne lepsze miejsce sceny.



Rys. 6–40: Przesuwanie elementów danych nakładki OSD w żądane miejsce sceny

7. Kliknij przycisk **Save**, aby uaktywnić wprowadzone powyżej ustawienia.

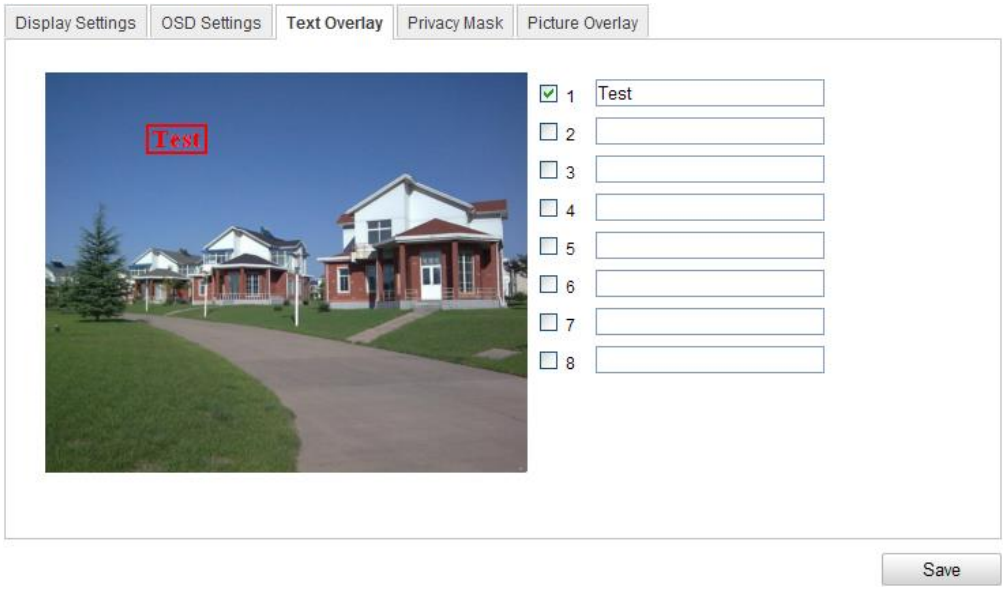
6.5.3. Konfigurowanie nakładek tekstowych użytkownika

Cel czynności:

Na podgląd kamery możesz też nakładać napisy o dowolnej treści własnego pomysłu.

Procedura wykonania:

1. Wyświetl interfejs ekranowy ustawień nakładek tekstowych użytkownika:
   Configuration > Advanced Configuration > Image > Text Overlay



Rys. 6–41: Interfejs do zdefiniowania własnych nakładek testowych

2. Zaznacz pole wyboru (np. 1) sprzed danego pola edycji, aby załączyć wyświetlanie tej nakładki tekstowej na podglądzie kamery (razem z innymi danymi OSD).
3. Do ww. pola edycji tekstu wpisz żądaną etykietę tekstową (np. tekst „Test").
4. (*I ewentualnie*) w oknie podglądu bieżącego kamery kliknij myszą widoczną tam czerwoną ramkę z wpisanym tekstem (p. Krok **3** powyżej) Test i przeciągnij ją, żeby wybrać nowe miejsce wyświetlania tej nakładki tekstowej.
5. Kliknij przycisk **Save**, aby zachować wprowadzone ustawienia.

Uwaga: Może skonfigurować maksymalnie **8** własnych nakładek tekstowych OSD.

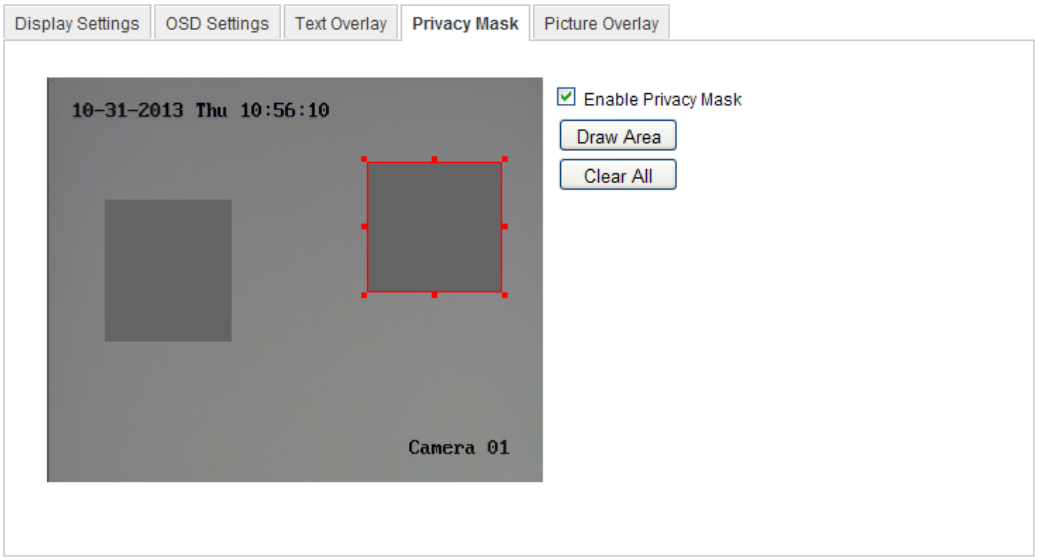
6.5.4. Konfigurowanie masek prywatności

Cel czynności:

Korzystając z masek ochrony prywatności możesz zasłonić pewne obszary w bieżącym obrazie kamery, aby uniemożliwić oglądanie i rejestrowanie wybranych miejsc monitorowanej sceny.

Procedura wykonania:

1. Wyświetl interfejs ekranowy ustawień masek prywatności (Privacy Mask): **Configuration > Advanced Configuration > Image > Privacy Mask**
2. Zaznacz pole wyboru Enable Privacy Mask, aby załączyć w kamerze funkcję masek.
3. Kliknij przycisk **Draw Area**, aby rozpocząć rysowanie prostokątnej maski.



Rys. 6–42: Interfejs umożliwiający zdefiniowanie własnych masek prywatności

4. Kliknij myszą w żądanym miejscu panelu, wyświetlającego podgląd bieżący, i przeciągnij nią tak daleko, jak daleko ma sięgać ten definiowany obszar maskujący.

Uwaga: Na jednym i tym samym obrazie wolno narysować maks. **4** obszary maskujące.

5. Kliknij przycisk **Stop Drawing**, aby zakończyć rysowanie obszarów masek lub ewentualnie kliknij przycisk **Clear All**, aby skasować z obrazu wszystkie dotychczas zdefiniowane obszary maskujące.
6. Kliknij przycisk **Save**, aby zachować wprowadzone ustawienia.

6.5.5. Konfigurowanie nakładki graficznej

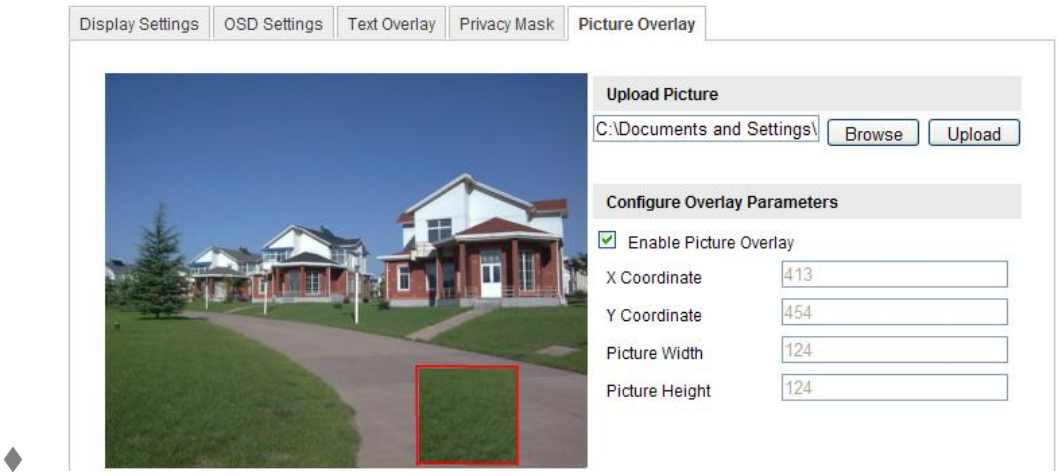
Cel czynności:

Funkcja nakładki graficznej pozwala nałożyć żądany obrazek na obraz kamery. Pewne firmy / użytkownicy mogą w ten sposób umieścić swoje logo na wyświetlanym obrazie monitoringowym.

Uwaga: Nakładany obrazek musi być w formacie BMP 24-bit RGB i nie może być większy niż 128x128 pikseli.

Procedura wykonania:

1. Wyświetl interfejs ekranowy ustawień nakładek obrazkowych:
   Configuration > Advanced Configuration > Image > Picture Overlay



Rys. 6–43: Interfejs z ustawieniami do skonfigurowania nakładki graficznej

2. Kliknij przycisk przeglądania **Browse**, aby wybrać obrazek do nałożenia.
3. Kliknij przycisk **Upload**, aby wysłać ten obrazek przez sieć do kamery.
4. Zaznacz pole wyboru **Enable Picture Overlay**, aby załączyć wyświetlanie nakładki.

Wartości w polach **X Coordinate** (współrzędna odcięta) i **Y Coordinate** (współrzędna rzędna) specyfikują punkt wyświetlania obrazka na obrazie kamery. Wartości w polach **Picture Width** (szerokość obrazka) i **Picture Height** (wysokość obrazka) podają wymiary własne obrazka w pikselach.

6.6. Konfigurowanie i obsługa zdarzeń podstawowych

W tym podrozdziale wyjaśnimy, jak skonfigurować kamerę sieciową, żeby mogła reagować na podstawowe zdarzenia monitoringowe, w tym na: wykrywanie ruchu, sabotowanie podglądu z kamery, odebranie wejściowego sygnału alarmowego, wystawienie wyjściowego sygnału alarmowego, a także wyjątki systemowe. Wymienione zdarzenia mogą też wyzwalać określone operacje alarmowe — jak np. zdalne powiadomienie centrum monitoringu, wysłanie powiadomienia w e-mailu, rozpoczęcie nagrywania kanału, wzbudzenie wyjścia alarmowego, etc.

Uwaga:

Możesz zaznaczyć pole wyboru **Notify Surveillance Center**, aby wyzwolenie danego alarmu wysłało informację o nim, z wymuszeniem odbioru (push), do stacji PC / do oprogramowania-klienckiego dla urządzeń mobilnych.

6.6.1. Konfigurowanie wykrywania ruchu

Cel czynności:

Funkcja wykrywania ruchu potrafi wykryć w obrazie kamery obiekty, które poruszają się w obszarze monitorowanym, skonfigurowanym przez użytkownika. Wyzwolony w ten sposób alarm detekcyjny może zainicjować określone akcje alarmowe, które wskazujesz w ustawieniach (jako powiązane z tym alarmem).

Aby zapewnić dokładne wykrywanie poruszających się obiektów i zmniejszyć częstotliwość alarmów mylnych/fałszywych, w interfejsie funkcji wykrywania ruchu masz do wyboru konfigurację normalną i konfigurację ekspercką.

➢ Konfiguracja normalna

Konfiguracja normalna wykorzystuje jeden i ten sam zestaw ustawień wykrywania ruchu zarówno dla okresu Dnia, jak i dla okresu Nocy.

Zadania:

1. [***Zadanie 1***]: Skonfiguruj obszar wykrywania ruchu.

Procedura wykonania:

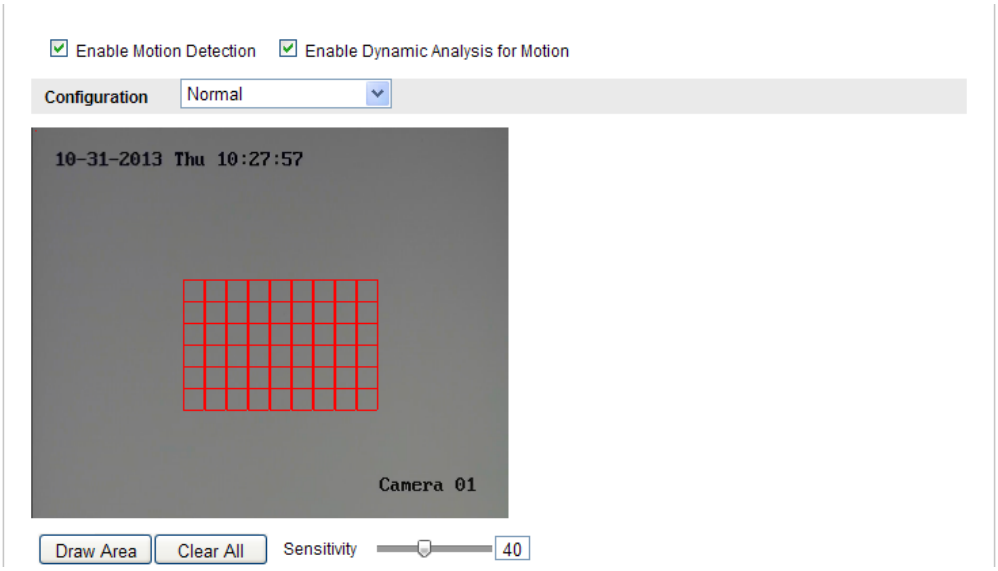
(1)Wyświetl interfejs funkcji wykrywania ruchu:

Configuration > Advanced Configuration > Basic Event > Motion Detection

(2)Zaznacz pole wyboru **Enable Motion Detection**, aby załączyć funkcję wykrywania ruchu w obrazie kamerze.

(3)Zaznacz pole wyboru **Enable Dynamic Analysis for Motion**, jeżeli wykryte obiekty ruchome mają zostać otoczone na obrazie zielonymi prostokątami.

Uwaga: Jeśli nie chcesz, żeby wykryty obiekt był wyświetlany z użyciem ww. ramek znacznikowych, to wybierz w regułach parametrów podglądu bieżącego opcję **Disable**. Przejdź w tym celu do odnośnych reguł po ścieżce: **Configuration > Local Configuration > Live View Parameters – Rules**.



Rys. 6–44: Interfejsie, w którym załączono funkcję wykrywania ruchu w obrazie kamery (pole wyboru **Enable Motion Detection**)

(4)Kliknij przycisk **Draw Area**. Na podglądzie bieżącym kamery kliknij-i-pociągnij myszą, aby narysować prostokątny obszar wykrywania ruchu (tzw. obszar detekcyjny).

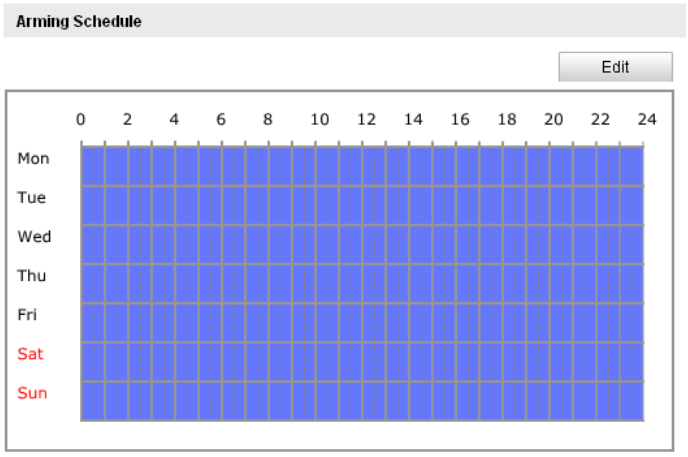
(5)Kliknij przycisk **Stop Drawing**, aby zakończyć rysowanie tego obszaru.

(6)(*Ewentualnie*): Kliknij przycisk **Clear All**, aby wykasować wszystkie dotychczas zdefiniowane obszary wykrywania ruchu.

(7)(*Ewentualnie*): Przesuń rączkę suwaka ekranowego **Sensitivity** w żądane położenie, aby wyregulować żądaną czułość wykrywania ruchu.

2. [***Zadanie 2***]: Skonfiguruj harmonogram uzbrajania funkcji wykrywania ruchu.

Procedura wykonania:



Rys. 6–45: Plan czasowy uzbrojenia funkcji – definiowanie okresów aktywności funkcji

(1)Kliknij przycisk **Edit**, aby rozpocząć edycję planu czasowego uzbrojenia funkcji. Na następnej ilustracji (str. 84) pokazano interfejs, służący do edycji tego harmonogramu.

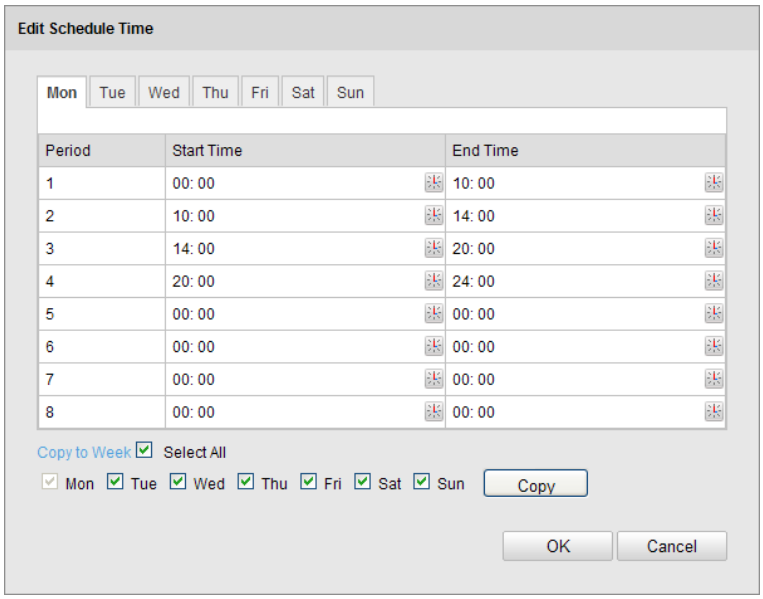
(2)Wybierz dzień, dla którego potrzebujesz skonfigurować okres uzbrojenia funkcji.

(3)Kliknij przyciski , aby wprowadzić okres czasu, w którym funkcja ma być uzbrojona (tj. załączona/aktywna).

(4)(*Ewentualnie*): Po wprowadzeniu w harmonogramie żądanych okresów uzbrojenia (dla danego dnia), możesz je przekopiować na inne dni (zob. przycisk **Copy**).

(5)Kliknij **OK**, aby zapisać wprowadzone ustawienia.

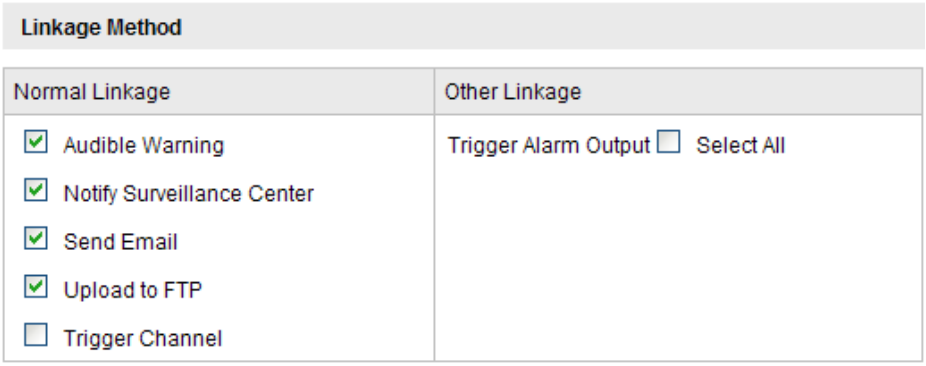
Uwaga: W harmonogramie, przedział czasu jednego okresu nie może nakładać się z przedziałem czasu jakiegokolwiek innego okresu. Dla jednego dnia można zdefiniować maks. **8** okresów uzbrojenia.



Rys. 6–46: Harmonogram ze zdefiniowanymi okresami uzbrojenia (tj. załączenia) funkcji wykrywania ruchu

3. [***Zadanie 3***]: Skonfiguruj akcje alarmowe powiązane z funkcją wykrywania ruchu.

   W grupie ustawień **Linkage Method** zaznacz żądane pole wyboru, aby wybrać odnośną akcję alarmową. Do wyboru są następujące akcje: **Audible Warning** (wyprowadź sygnał akustyczny), **Notify Surveillance Center** (wyślij powiadomienie do centrum monitoringu), **Send Email** (wyślij powiadomienie na adres e-mail), **Upload to FTP** (wyślij obrazek/ki na serwer FTP), **Trigger Channel** (wyzwól rejestrowanie kanału), a także **Trigger Alarm Output** (pobudź wyjście alarmowe). Wybierz tu akcję alarmową powiązaną, która ma zostać wyzwolona, gdy wystąpi zdarzenie wykrycia ruchu:



Rys. 6–47: Zaznaczanie akcji inicjowanych przez wykrycie ruchu

- **Wyprowadź sygnał akustyczny (Audible Warning)**

Zdarzenie uruchomi lokalnie słyszalne ostrzeżenie. Opcja jest obsługiwana tylko przez urządzenia, które są wyposażone w wyjście audio.

- **Powiadom Centrum Monitoringu (Notify Surveillance Center)**

Jeśli zaznaczysz tę opcję, to z chwilą wystąpienia zdarzenia zostanie wysłany sygnał wyjątku lub sygnał alarmowy do zdalnego oprogramowania zarządzającego.

- **Wyślij wiadomość e-mail (Send Email)**

Ta opcja spowoduje, że z chwilą wystąpienia zdarzenia zostanie/ą wysłany/e e-mail/e do użytkownika/ów z informacją o alarmie.

Uwaga: Aby mogło działać wysyłanie e-maili alarmowych w reakcji na zdarzenia, musisz skonfigurować odnośne parametry — w tym celu zob. *podrozdz. 6.3.10* ***Powiadamianie e-mailowe o alarmach***, str. 58.

- **Wyślij na serwer FTP (Upload to FTP)**

Jeśli zaznaczysz tę opcję, to wystąpienie zdarzenia spowoduje pobranie klatki z obrazu kamery i wysłanie jej (jako obrazek) na odnośny serwer FTP.

Uwagi:

- Najpierw, w ustawieniach kamery, musisz wprowadzić adres FTP serwera i skonfigurować ten serwer — zob. opis w *podrozdz. 6.3.12* ***Konfigurowanie ustawień protokołu FTP***, str. 60.
- Przejdź na stronę funkcji fotozrzutów klatek **Advanced Configuration** > **Storage** > **Snapshot** (zob. str. 132) i załącz tam opcję **Enable Event-triggered Snapshot** (fotozrzucanie wyzwalane przez zdarzenia). Skonfiguruj też parametr **Capture Interval** (czas między kolejnymi fotozrzutami) oraz **Capture Number** (numer fotozrzutu).
- Zarejestrowana klatka obrazu może zostać wysłana również na udostępnioną kartę pamięci SD albo na dysk sieciowy.

- **Wyzwól rejestrowanie kanału (Trigger Channel)**

Jeśli zaznaczysz tę opcję, to wykrycie ruchu w obrazie kamery uruchomi nagranie klipu z jej obrazu. Jednak aby zrealizować tę funkcję, musisz skonfigurować harmonogram nagrywania — zob. dokładny opis w *podrozdz. 7.2* (str. 132).

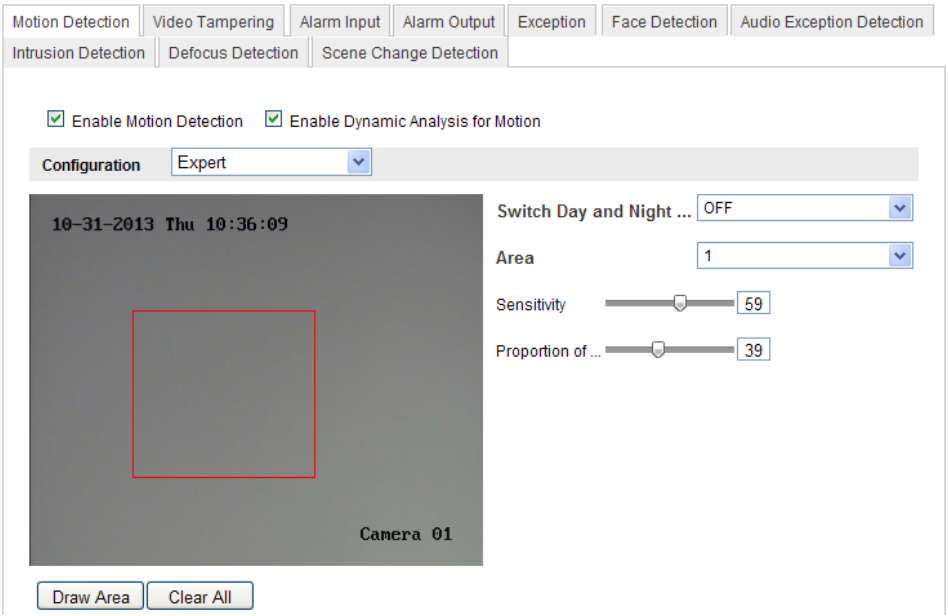
- **Pobudź wyjście alarmowe (Trigger Alarm Output)**

Jeśli zaznaczysz tę opcję, to wystąpienie zdarzenia przestawi jedno / więcej zewnętrznych wyjść alarmowych kamery w stan aktywny (=pobudzony).

Uwaga: Aby zrealizować pobudzenie wyjścia alarmowego przez zdarzenie, musisz najpierw skonfigurować odnośne parametry — zob. opis w *podrozdz. 6.6.4* ***Konfigurowanie wyjść alarmowych***, str. 90.

➢ Konfiguracja ekspercka

Tryb ekspercki (**Configuration: Expert**) służy głównie do zadania żądanej czułości obszaru (**Sensitivity**) oraz stosunku wielkości obiektu-celu do obszaru (**Proportion of...**) dla każdego definiowanego obszaru detekcji ruchu — obowiązujących w poszczególnych trybach przełączania Dzień/Noc.



Rys. 6–48: Konfigurowanie wykrywania ruchu — tryb ekspercki (**Expert**)

- Przełączanie Dzień/Noc — wyłączone

Procedura wykonania:

(1)Narysuj obszar czuły na ruch, jak podano dla trybu konfiguracji normalnej. Możesz zdefiniować maks. 8 takich obszarów.

(2)Z listy rozwijalnej **Switch Day and Night...**, definiującej sposób działania przełączania Dzień/Noc, wybierz opcję **OFF**.

(3)Wybierz żądany obszar (tj. jego numer) z listy rozwijalnej **Area**.

(4)Ustaw suwak tak, by wyregulować dla tego wybranego obszaru: czułość na ruch (suwak **Sensitivity**), względną wielkość obiektu w stos. do obszaru (suwak **Proportion of...**).

(5)Skonfiguruj harmonogram okresów uzbrajania (**Edit Schedule Time**) oraz akcje powiązane z wykryciem ruchu (**Linkage Method**) — jak podano dla konfiguracji normalnej.

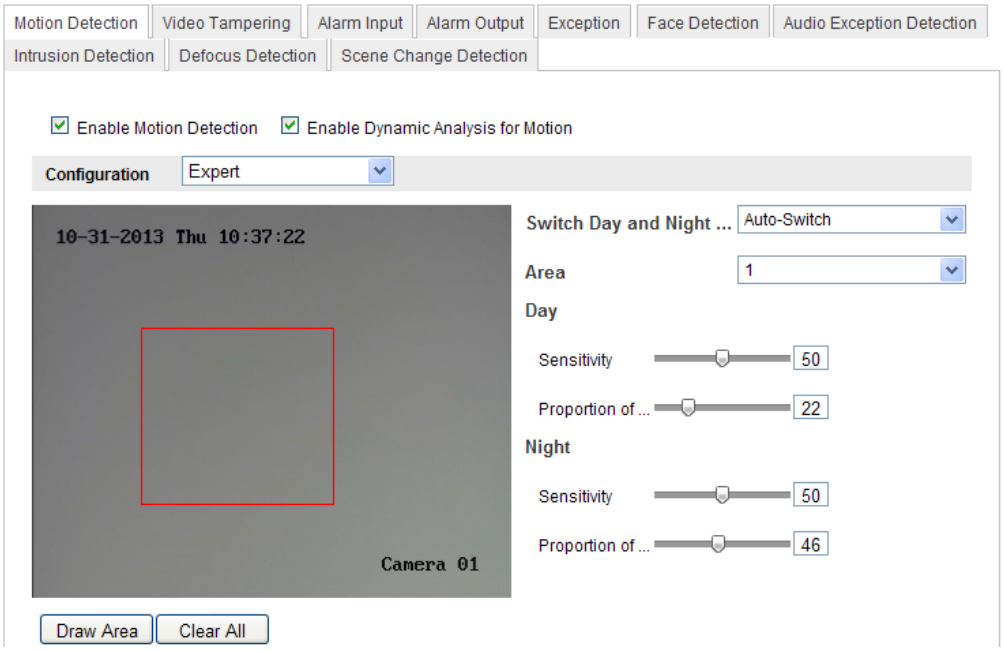
(6)Kliknij przycisk **Save**, aby zachować wprowadzone ustawienia.

- Przełączanie Dzień/Noc — automatyczne

Procedura wykonania:

(1)Narysuj obszar czuły na ruch, jak podano dla trybu konfiguracji normalnej. Możesz zdefiniować maks. 8 takich obszarów.

(2)Z listy rozwijalnej **Switch Day and Night...**, definiującej tryb przełączania Dzień/Noc, wybierz opcję **Auto-Switch**.



Rys. 6–49: Ustawienia wykrywania ruchu dla trybu automatycznego przełączania Dzień/Noc (**Auto-Switch**)

(3)Wybierz żądany obszar (numer) z listy rozwijalnej **Area**.

(4)Wyreguluj odnośnym suwakiem: czułość na ruch (suwak **Sensitivity**), względną wielkość obiektu w stosunku do wielkości obszaru (suwak **Proportion of...**) — które mają obowiązywać dla tego wybranego obszaru w okresie *Dnia*.

(5)Wyreguluj odnośnym suwakiem: czułość na ruch (suwak **Sensitivity**), względną wielkość obiektu w stos. do wielkości obszaru (suwak **Proportion of...**) — które mają obowiązywać dla tego wybranego obszaru w okresie *Nocy*.

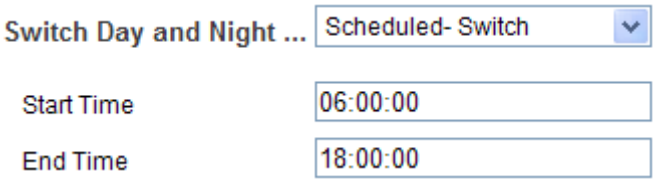
(6)Skonfiguruj harmonogram okresów uzbrajania (**Edit Schedule Time**) oraz akcje powiązane z wykryciem ruchu (**Linkage Method**) — jak podano dla konfiguracji normalnej.

(7)Kliknij przycisk **Save**, aby zachować wprowadzone ustawienia.

- Przełączanie Dzień/Noc — sterowane z harmonogramu

(1)Narysuj obszar czuły na ruch, jak podano dla trybu konfiguracji normalnej. Możesz zdefiniować maks. 8 takich obszarów.

(2)Z listy rozwijalnej **Switch Day and Night...**, definiującej sposób działania przełączania Dzień/Noc, wybierz opcję **Scheduled-Switch**.



Rys. 6–50: Ustawienia wykrywania ruchu dla trybu przełączania Dzień/Noc sterowanego czasem (**Scheduled-Switch**)

(3)Wprowadź czas rozpoczęcia (**Start Time**) i czas zakończenia (**End Time**), wyznaczające punkty czasowe auto-przełączania trybów Dzień<>Noc.

(4)Wybierz żądany obszar (numer) z listy rozwijalnej **Area**.

(5)Wyreguluj odnośnym suwakiem: czułość na ruch (suwak **Sensitivity**), względną wielkość obiektu w stosunku do wielkości obszaru (suwak **Proportion of...**) — które mają obowiązywać dla tego wybranego obszaru w okresie *Dnia*.

(6)Wyreguluj odnośnym suwakiem: czułość na ruch (suwak **Sensitivity**), względną wielkość obiektu w stos. do wielkości obszaru (suwak **Proportion of...**) — które mają obowiązywać dla tego wybranego obszaru w okresie *Nocy*.

(7)Skonfiguruj harmonogram okresów uzbrajania (**Edit Schedule Time**) oraz akcje powiązane z wykryciem ruchu (**Linkage Method**) — jak podano dla konfiguracji normalnej.

(8)Kliknij przycisk **Save**, aby zachować wprowadzone ustawienia.

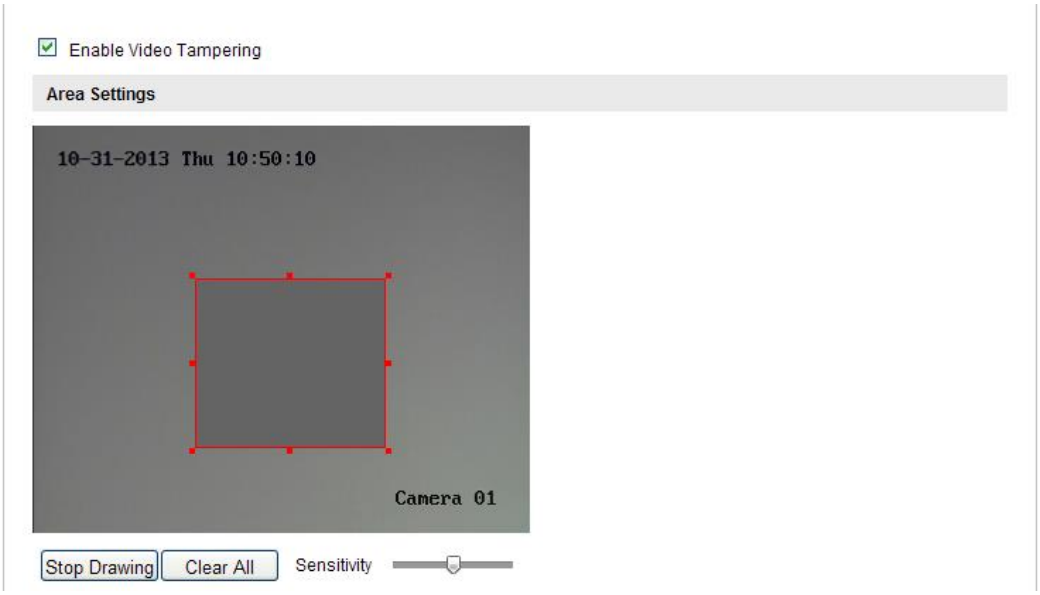
6.6.2. Konfigurowanie alarmu dla sabotażu podglądu z kamery

Cel czynności:

Możesz skonfigurować kamerę, żeby wyzwalała alarm, gdyby jej obiektyw został zasłonięty/zakryty. Możesz przy tym zadać, żeby ten alarm automatyczne wyzwolił określone akcje alarmowe.

Procedura wykonania:

1. Wyświetl interfejs ekranowy ustawień dot. sabotowania podglądu z kamery:
   Configuration > Advanced Configuration > Basic Event > Video Tampering



Rys. 6–51: Ustawienia alarmu dla sabotażu podglądu z kamery

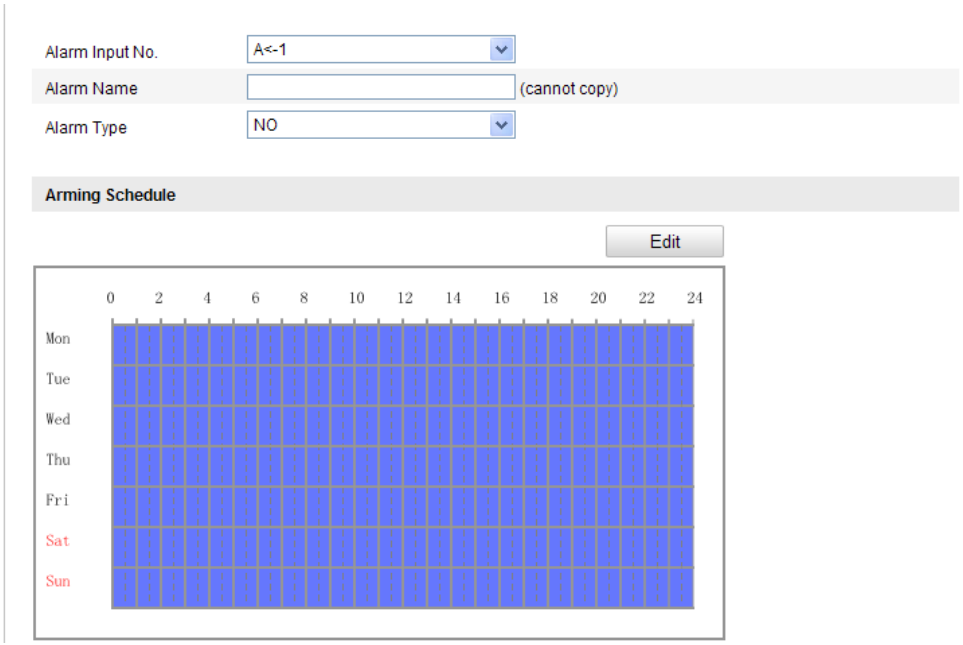
2. Zaznacz pole wyboru **Enable Video Tampering**, aby załączyć funkcję wykrywania sabotażu podglądu z kamery.

3. Skonfiguruj obszar wykrywania sabotażu. Więcej o tym — zob. ***Zadanie 1*** w *podrozdz. 6.6.1* ***Konfigurowanie wykrywania ruchu***, str. 82.
4. Kliknij przycisk **Edit**, aby wyedytować harmonogram uzbrajania dla funkcji wykrywania sabotażu na podglądzie kamery. Konfigurowanie tego harmonogramu wykonuje się tak samo jak konfigurowanie harmonogramu uzbrojenia dla funkcji wykrywania ruchu w obrazie — zob. ***Zadanie 2*** w *podrozdz. 6.6.1*, str. 83.
5. Zaznacz żądane pola wyboru, aby wybrać odnośne akcje alarmowe, wyzwalane w przypadku wykrycia sabotażu podglądu z kamery. Do wyboru są następujące akcje: **Audible Warning** (słyszalne ostrzeżenie), **Notify Surveillance Center** (wyślij powiadomienie do centrum monitoringu), **Send Email** (wyślij powiadomienie na adres email), **Upload to FTP** (wyślij obrazek/ki na serwer FTP), a także **Trigger Alarm Output** (pobudź wyjście alarmowe). Dokładniejsze wskazówki — zob. ***Zadanie 3*** w *podrozdz. 6.6.1*, str. 84.
6. Kliknij przycisk **Save**, aby zachować wprowadzone ustawienia.

6.6.3. Konfigurowanie wejść alarmowych

Procedura wykonania:

1. Wyświetl interfejs ekranowy ustawień wejść alarmowych kamery:
   Configuration > Advanced Configuration > Basic Event > Alarm Input:
2. Z listy rozwijalnej **Alarm Input No.** wybierz numer konfigurowanego wejścia alarmowego. Z listy rozwijalnej **Alarm Type** wybierz rodzaj testowania stanu alarmowego — możesz wybrać: **NO** (czuły na zwarcie obwodu) lub **NC** (czuły na rozwarcie obwodu). (*Ewentualnie*): W polu **Alarm Name** wpisz etykietę dla tego wejścia alarmowego.



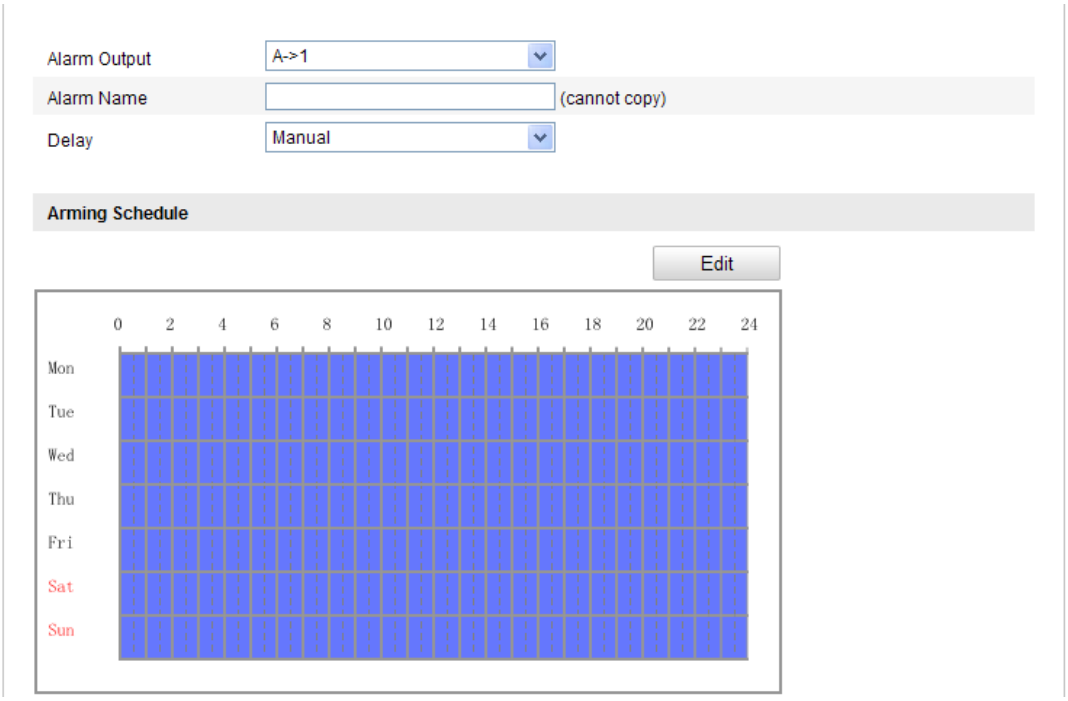
Rys. 6–52: Interfejs ustawień do konfigurowania wejść alarmowych kamery

3. Kliknij przycisk **Edit**, aby skonfigurować harmonogram uzbrajania tego wejścia alarmowego. Dokładniejsze wskazówki — zob. ***Zadanie 2*** w *podrozdz. 6.6.1*, str. 83.
4. Zaznacz żądane pola wyboru, aby wybrać odnośne akcje alarmowe, które chcesz powiązać z wystąpieniem sygnału aktywnego na tym wejściu alarmowym. Dokładniejsze wskazówki — zob. ***Zadanie 3*** w *podrozdz. 6.6.1*, str. 84.
5. Jako ww. akcję powiązaną możesz również wybrać tu akcję **PTZ**, o ile Twoja kamera ma zainstalowaną jednostkę siłownika P/T. Jeżeli ma, to zaznacz odnośne pole wyboru i wybierz żądany numer (**No.**), aby jako akcja **PTZ** nastąpiło wywołanie: presetu (**Preset**) / patrolu (**Patrol**) / trasy (**Pattern**), o tym numerze.
6. Możesz przekopiować ustawienia tego wejścia alarmowego do innych wejść alarmowych kamery.
7. Kliknij przycisk **Save**, aby zachować wprowadzone ustawienia.

6.6.4. Konfigurowanie wyjść alarmowych

Procedura wykonania:

1. Wyświetl interfejs ekranowy ustawień wyjść alarmowych kamery:
   Configuration > Advanced Configuration > Basic Event > Alarm Output
2. Z listy rozwijalnej **Alarm Output** wybierz jedno żądane wyjście alarmowe. (*Ewentualnie*): Nadaj etykietę temu wyjściu alarmowemu (zob. pole **Alarm Name**).
3. Dla czasu opóźnienia, wybieranego z listy rozwijalnej **Delay**, możesz zadać wartości: **5sec**, **10sec**, **30sec**, **1min**, **2min**, **5min**, **10min** lub opcję **Manual**. **Delay** to okres, przez który wyjście alarmowe jest podtrzymywane w stanie aktywnym, licząc od chwili wzbudzenia go przez zaistniały alarm.
4. Kliknij **Edit**, aby wyświetlił się interfejs ekranowy edycji harmonogramu **Edit Schedule Time**. Konfigurowanie tego harmonogramu wykonuje się tak samo jak konfigurowanie harmonogramu uzbrajania funkcji wykrywania ruchu w obrazie; odnośne wskazówki — zob. ***Zadanie 2*** w *podrozdz. 6.6.1*, str. 83.
5. Możesz przekopiować ustawienia tego wyjścia alarmowego do innych wyjść alarmowych kamery.
6. Kliknij przycisk **Save**, aby zachować wprowadzone ustawienia.



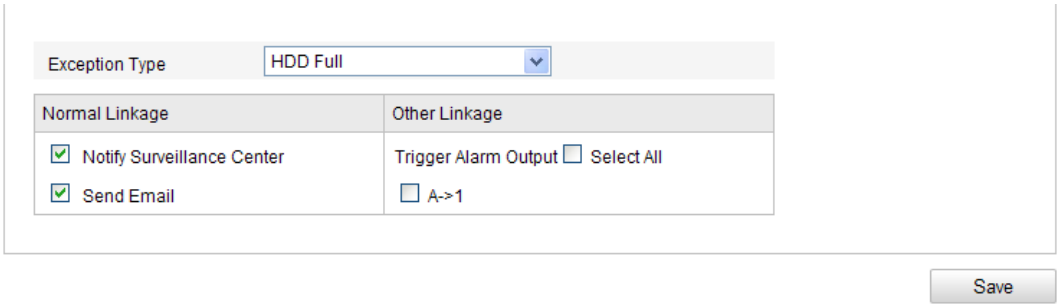
Rys. 6–53: Interfejs ustawień do konfigurowania wyjść alarmowych kamery

6.6.5. Konfigurowanie obsługi wyjątków systemu

Wyjątkami systemu, których obsługę możesz skonfigurować w tej kamerze, mogą być: **HDD Full** (przepełnienie dysku), **HDD Error** (błąd dysku), **Network Disconnected** (odłączenie sieci), **IP Address Conflicted** (konflikt w adresie IP) oraz **Illegal Login to the Cameras** (logowanie z użyciem nielegalnych danych, do użytkowania kamer).

Procedura wykonania:

1. Wyświetl interfejs ekranowy ustawień wyjątków systemu:
   Configuration > Advanced Configuration > Basic Event > Exception
2. Zaznacz żądane pola wyboru, aby wybrać nimi odnośne akcje alarmowe wykonywane, gdy wystąpi alarm wyjątku (wybrany przez Ciebie z listy rozwijalnej **Exception Type**). Dokładniejsze wskazówki — zob. ***Zadanie 3*** w *podrozdz. 6.6.1*, str. 84.



Rys. 6–54: Interfejs ustawień do konfigurowania wyjątków systemowych

3. Kliknij przycisk **Save**, aby zachować wprowadzone ustawienia.

6.6.6. Konfigurowanie innych alarmów

Uwaga: Niektóre kamery obsługują alarmy ze źródeł bezprzewodowych, alarmy z czujek PIR, a także alarmy napadowe/sytuacyjne.

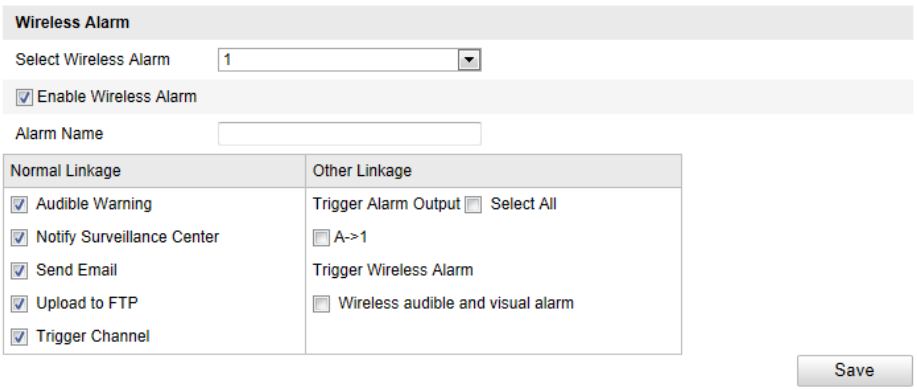
- **Alarmy ze źródeł bezprzewodowych**

Cel czynności:

Kiedy sygnał alarmu bezprzewodowego zostaje wysłany do kamery z czujnika (np. bezprzewodowego kontaktu monitorującego drzwi), to zostaje wyzwolony alarm bezprzewodowy i w odpowiedzi może zostać wykonanych szereg akcji alarmowych.

Procedura wykonania:

1. Wyświetl interfejs ekranowy ustawień alarmów bezprzewodowych:
   Configuration > Advanced Configuration > Basic Event > Other Alarm
2. Z listy rozwijalnej Select Wireless Alarm wybierz numer żądanego alarmu bezprzewodowego. Kamera dysponuje maks. 8 kanałami do obsługi zewnętrznych wejściowych sygnałów alarmowych.
3. Zaznacz pole wyboru Enable Wireless Alarm, aby uaktywnić obsługę tego konfigurowanego alarmu bezprzewodowego.
4. W polu Alarm Name wpisz etykietę nadawaną temu alarmowi.
5. Zaznacz żądane pola wyboru, aby wybrać nimi odnośne akcje alarmowe, wykonywane w odpowiedzi na ten alarm bezprzewodowy.
6. Kliknij przycisk **Save**, aby zachować wprowadzone ustawienia.
7. Odszukaj współpracujące źródłowe urządzenie bezprzewodowe gdzieś w pobliżu kamery, po czym przejdź do **Configuration > Advanced Configuration > System > Remote Control**, aby uzbroić kamerę i „przestudiować” alarm bezprzewodowy.



Rys. 6–55: Konfigurowanie ustawień alarmu bezprzewodowego

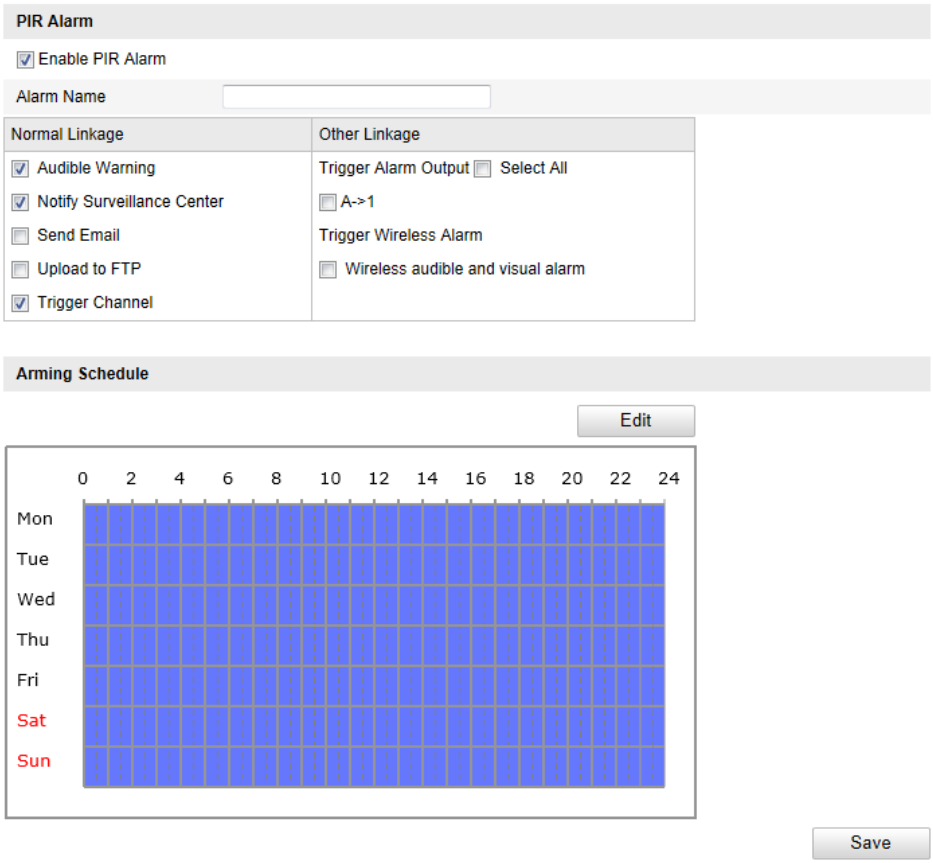
- **Alarmy z czujek PIR**

Cel czynności:

Alarm PIR zostaje wyzwolony, gdy intruz poruszy się w polu widzenia/detekcji danej czujki PIR. Czujka może wykryć ciepło rozpraszane przez osobę czy każde inne stworzenie ciepłokrwiste (np. psa, kota, etc.).

Procedura wykonania:

1. Wyświetl interfejs ekranowy ustawień alarmów PIR:
   Configuration > Advanced Configuration > Basic Event > Other Alarm
2. Zaznacz pole wyboru Enable PIR Alarm, aby uaktywnić obsługę alarmów nadsyłanych do kamery z czujek PIR.
3. W polu Alarm Name wpisz etykietę dla tego konfigurowanego alarmu PIR.
4. Zaznacz żądane pola wyboru, aby wybrać nimi odnośne akcje, wykonywane w odpowiedzi na ten alarm PIR.
5. Kliknij przycisk **Edit**, aby skonfigurować harmonogram uzbrajania tego alarmu.
6. Kliknij przycisk **Save**, aby zachować wprowadzone ustawienia.
7. Przejdź do opcji **Configuration > Advanced Configuration > System > Remote Control**, aby uzbroić kamerę.



Rys. 6–56: Konfigurowanie ustawień dla alarmów z czujek PIR

● Alarmy napadowo/sytuacyjne

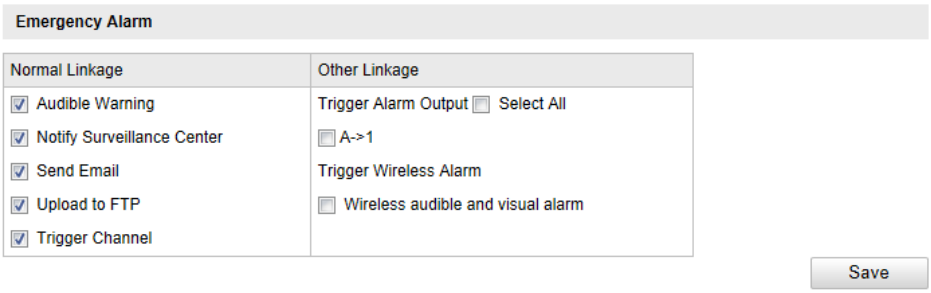
Cel czynności:

W sytuacji zagrożenia użytkownik kamery może nacisnąć na pilocie od kamery przycisk „napadowy” (Emergency) — aby wyzwolić nim alarm napadowy.

Uwaga: Do zrealizowania alarmu napadowego trzeba posiadać pilota zdalnego sterowania od kamery. Przejdź do opcji **Configuration > Advanced Configuration > System > Remote Control**, aby najpierw zapoznać się z takim pilotem.

Procedura wykonania:

1. Wyświetl interfejs ekranowy ustawień alarmów napadowych:
   Configuration > Advanced Configuration > Basic Event > Other Alarm
2. W sekcji ustawień Emergency Alarm zaznacz żądane pola wyboru, aby wybrać nimi odnośne akcje alarmowe, wykonywane w odpowiedzi na alarm napadowy zgłoszony z pilota.
3. Kliknij przycisk **Save**, aby zachować wprowadzone ustawienia.



Rys. 6–57: Konfigurowanie ustawień alarmu napadowego/sytuacyjnego

6.7. Konfigurowanie i obsługa zdarzeń inteligentnych

W tym podrozdziale wyjaśnimy, jak skonfigurować tę kamerę sieciową, aby reagowała na tzw. *zdarzenia inteligentne* — w tym na: wykrycie twarzy, wykrycie wyjątku w kanale audio, wykrycie utraty ostrości podglądu, wykrycie zmiany sceny obserwowanej, wykrycie przekroczenia linii granicznej, wykrycie wtargnięć, wykrycie wejścia do obszaru, wykrycie bagażu-bez-opieki, a także wykrycie usunięcia obiektu ze sceny. Zdarzenia te możesz skonfigurować, żeby wyzwalały wskazane przez Ciebie akcje alarmowe, np.: wysłanie powiadomienia do centrum monitoringu, wysłanie powiadomienia via e-mail, pobudzenie wyjścia alarmowego kamery, itd.

Uwaga:

Zaznacz pole wyboru akcji alarmowej Notify Surveillance Center, jeżeli chcesz, żeby z chwilą wyzwolenia alarmu informacja o nim została podana z wymuszeniem odbioru (technika *push*) do stacji PC albo do oprogramowania klienckiego dla urządzeń mobilnych.

6.7.1. Konfigurowanie wykrywania wyjątków w kanale audio

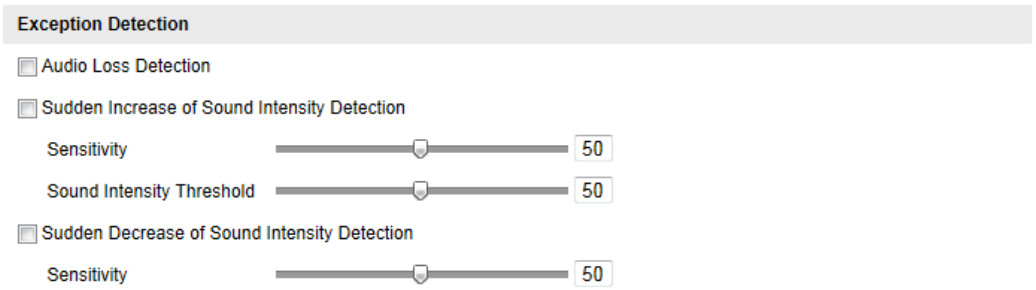
Cel czynności:

Funkcja wykrywania audio-wyjątków wykrywa nieprawidłowości w dźwięku z monitorowanej sceny (np. nagły wzrost/spadek poziomu dźwięku) oraz pozwala wybrać pewne akcje alarmowe, które mają zostać wykonane w chwili, gdy zostanie wyzwolony alarm wykrycia audio-wyjątku.

Uwaga: Zakres/dostępność funkcji wykrywania audio-wyjątków zależy od danego modelu kamery.

Procedura wykonania:

1. Wyświetl interfejs ekranowy ustawień, konfigurujących działanie funkcji wykrywania audio-wyjątków:
   Configuration > Advanced Configuration > Smart Event > Audio Exception Detection
2. Zaznacz pole wyboru **Audio Loss Exception**, aby załączyć wykrywanie zupełnych zaników dźwięku (fonii).
3. Zaznacz pole wyboru **Sudden Increase of Sound Intensity Detection** (wykrywanie nagłych wzrostów siły dźwięku), aby wykrywać strome narastanie poziomu dźwięku ze sceny monitorowanej. Aby prawidłowo wykrywać te szybkie wzrosty dźwięku, możesz skonfigurować tu ponadto: czułość wykrywania (**Sensitivity**), próg siły dźwięku (**Sound Intensity Threshold**).
   Zaznacz pole wyboru **Sudden Decrease of Sound Intensity Detection** (wykrywanie nagłych spadków siły dźwięku), aby wykrywać szybko-strome spadki poziomu dźwięku ze sceny monitorowanej. Aby prawidłowo wykrywać te szybkie spadki dźwięku, możesz skonfigurować tu ponadto: czułość wykrywania (**Sensitivity**), próg siły dźwięku (**Sound Intensity Threshold**).
   Uwagi:
   - **Sensitivity**: zakres regulacyjny [**1~100**]. Im mniejszą wartość wyregulowano, tym większa musi być zmiana siły dźwięku, żeby nastąpiło wykrycie.
   - **Sound Intensity Threshold**: zakres regulacyjny [**1~100**]. Ten regulator pozwala odfiltrować dźwięki otoczenia, przy czym im głośniejsze otoczenie, tym wyższą wartość trzeba tu wyregulować. Odpowiednią sytuacyjnie wartość możesz wyregulować w warunkach autentycznego otoczenia.
4. Masz podgląd głośności dźwięku, aktualizowany w czasie rzeczywistym.
5. Kliknij przycisk **Edit**, aby skonfigurować harmonogram uzbrajania tego zdarzenia (tj. wykrywania audio-wyjątków).
6. Zaznacz żądane pola wyboru od odnośnych akcji alarmowych, aby powiązać je z wystąpieniem audio-wyjątku — akcje dostępne to: **Notify Surveillance Center** (wyślij powiadomienie do centrum monitoringu), **Send Email** (wyślij powiadomienie na adres e-mail), **Upload to FTP** (wyślij obrazek/ki na serwer FTP), **Trigger Channel for Recording** (wyzwól nagrywanie kanału), a także **Trigger Alarm Output** (pobudź wyjście alarmowe).
7. Kliknij przycisk **Save**, aby zachować wprowadzone ustawienia.



Rys. 6–58: Ustawienia, pozwalające skonfigurować wykrywanie audio-wyjątków

6.7.2. Konfigurowanie wykrywania utraty ostrości podglądu

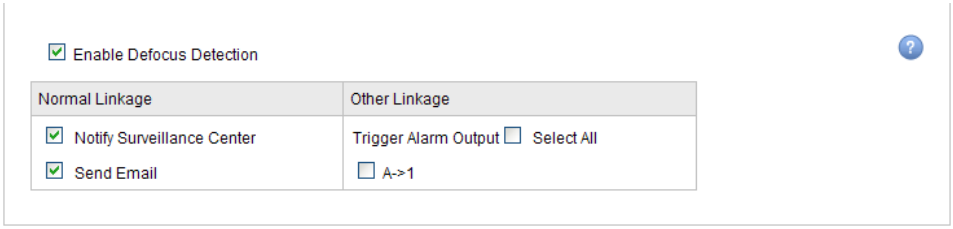
Cel czynności:

Kamera potrafi wykrywać rozmycie podglądu, spowodowane złym ustawieniem ostrości w scenie przez obiektyw. Może też automatycznie wykonać pewne żądane akcje alarmowe w odpowiedzi na wykrycie rozmycia (tj. alarm wykrycia rozmycia).

Uwaga: Zakres/dostępność funkcji wykrywania utraty ostrości podglądu zależy od danego modelu kamery.

Procedura wykonania:

1. Wyświetl interfejs ekranowy ustawień, konfigurujących funkcję wykrywania utraty ostrości podglądu:
   Configuration > Advanced Configuration > Smart Event > Defocus Detection
2. Zaznacz pole wyboru **Enable Defocus Detection**, aby załączyć w kamerze funkcję wykrywania utraty ostrości podglądu.
3. Wyreguluj suwakiem ekranowym (kliknij-i-pociągnij) poziom czułości wykrywania (**Sensitivity**). Zakres regulacyjny czułości to [**1~100**] — im wyższą wartość tu zadasz, tym mniejsze rozmycie obrazu zdoła wyzwolić alarm.
4. Zaznacz żądane pola wyboru od odnośnych akcji alarmowych, aby powiązać je z wykryciem utraty ostrości podglądu — akcje dostępne to: **Notify Surveillance Center** (wyślij powiadomienie do centrum monitoringu), **Send Email** (wyślij powiadomienie na adres e-mail), **Trigger Alarm Output** (pobudź wyjście alarmowe kamery).
5. Kliknij przycisk **Save**, aby zachować wprowadzone ustawienia.



Rys. 6–59: Ustawienia, pozwalające skonfigurować wykrywanie utraty ostrości podglądu

6.7.3. Konfigurowanie wykrywania zmiany sceny

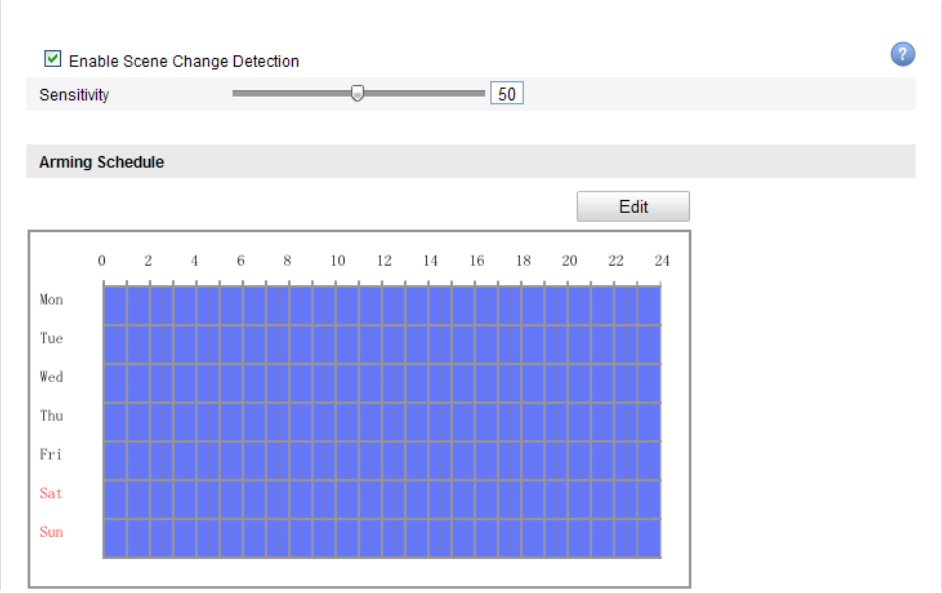
Cel czynności:

Funkcja wykrywania zmiany sceny wykrywa zmianę monitorowanego otoczenia, wywołaną czynnikami zewnętrznymi (np. umyślne obrócenie kamery), oraz pozwala wybrać pewne akcje alarmowe, które mają zostać wykonane w chwili, gdy zostanie wyzwolony alarm (w związku z tym zdarzeniem).

Uwaga: Zakres/dostępność funkcji wykrywania zmiany sceny zależy od danego modelu kamery.

Procedura wykonania:

1. Wyświetl interfejs ekranowy ustawień, konfigurujących funkcję wykrywania zmiany sceny:
   Configuration > Advanced Configuration > Smart Event > Scene Change Detection
2. Zaznacz pole wyboru **Enable Scene Change Detection**, aby załączyć w kamerze funkcję wykrywania zmiany sceny.
3. Wyreguluj suwakiem ekranowym (kliknij i pociągnij) poziom czułości wykrywania (**Sensitivity**). Zakres regulacyjny czułości to [**1~100**] — im wyższą wartość tu zadasz, tym mniejsza zmiana sceny zdoła wyzwolić alarm.
4. Kliknij przycisk **Edit**, aby wyedytować harmonogram uzbrajania tej funkcji.
5. Zaznacz żądane pola wyboru od odnośnych akcji alarmowych, aby powiązać je z wykryciem zmiany sceny — w tym akcje: **Notify Surveillance Center** (wyślij powiadomienie do centrum monitoringu), **Send Email** (wyślij powiadomienie na adres e-mail), **Upload to FTP** (wyślij obrazek/ki na serwer FTP), **Trigger Alarm Output** (pobudź wyjście alarmowe kamery).
6. Kliknij przycisk **Save**, aby zachować wprowadzone ustawienia.



Rys. 6–60: Ustawienia, pozwalające skonfigurować wykrywanie zmiany sceny

6.7.4. Konfigurowanie wykrywania twarzy

Cel czynności:

Funkcja wykrywania twarzy wykrywa twarze, pojawiające się w monitorowanej scenie, oraz pozwala wybrać pewne akcje alarmowe, które mają zostać wykonane w chwili, gdy zostanie wyzwolony alarm (w związku z tym zdarzeniem).

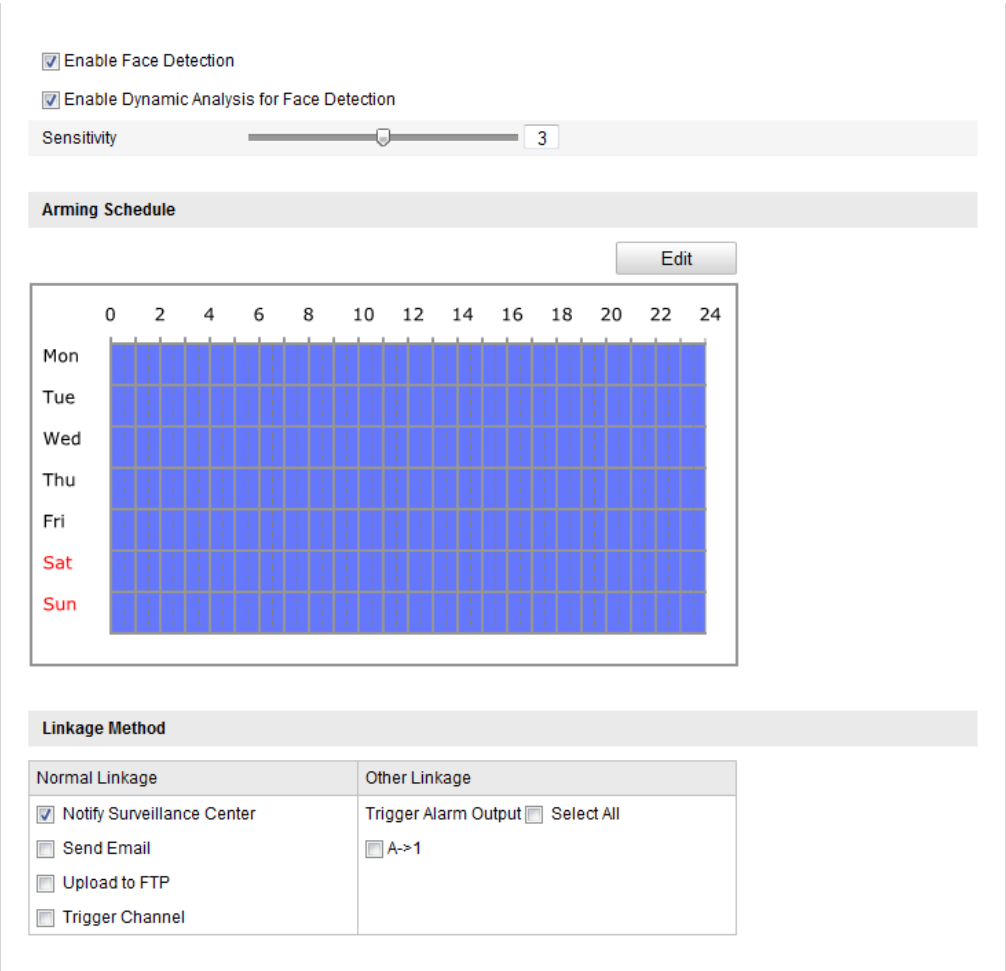
Uwaga: Zakres/dostępność funkcji wykrywania twarzy zależy od danego modelu kamery.

Procedura wykonania:

1. Wyświetl interfejs ekranowy ustawień, konfigurujących funkcję wykrywania twarzy:
   Configuration> Advanced Configuration> Smart Event> Face Detection
2. Zaznacz pole wyboru **Enable Face Detection**, aby załączyć w kamerze funkcję wykrywania twarzy.
3. (*Ewentualnie*): Zaznacz pole wyboru **Enable Dynamic Analysis for Face Detection** — wtedy wykryta twarz zostanie otoczona zieloną (prostokątną) ramką na podglądzie bieżącym z kamery.

   Uwaga: Aby wprowadzić ww. zaznaczanie wykrytych twarzy na podglądzie bieżącym, przejdź do: **Local Configuration > Live View Parameters** i załącz tam odnośne reguły (**Rules**).
4. Wyreguluj suwakiem ekranowym (kliknij i pociągnij) poziom czułości wykrywania.

   Sensitivity: Zakres regulacyjny [1~5]. Im wyższą wartość tu zadasz, tym łatwiej będą wykrywane twarze w obrazie.
5. Kliknij przycisk **Edit**, aby wyedytować harmonogram uzbrajania tej funkcji.
6. Zaznacz żądane pola wyboru od odnośnych akcji alarmowych, aby powiązać je z wykryciem twarzy — w tym akcje: **Notify Surveillance Center** (wyślij powiadomienie do centrum monitoringu), **Send Email** (wyślij powiadomienie na adres e-mail), **Upload to FTP** (wyślij obrazek/ki na serwer FTP), **Trigger Channel** (wyzwól nagrywanie kanału), **Trigger Alarm Output** (pobudź wyjście alarmowe kamery).
7. Kliknij przycisk **Save**, aby zachować wprowadzone ustawienia.



Rys. 6–61: Ustawienia, pozwalające skonfigurować wykrywanie zmiany sceny

6.7.5. Konfigurowanie wykrywania przekroczenia linii

Cel czynności:

Funkcja wykrywania przekroczenia linii wykrywa: osoby, pojazdy / inne obiekty, gdy te przekraczają zdefiniowaną (przez użytkownika) wirtualną linię. Pozwala też wybrać pewne akcje alarmowe, które mają zostać wykonane w chwili, gdy zostanie wyzwolony alarm (w związku z tym zdarzeniem).

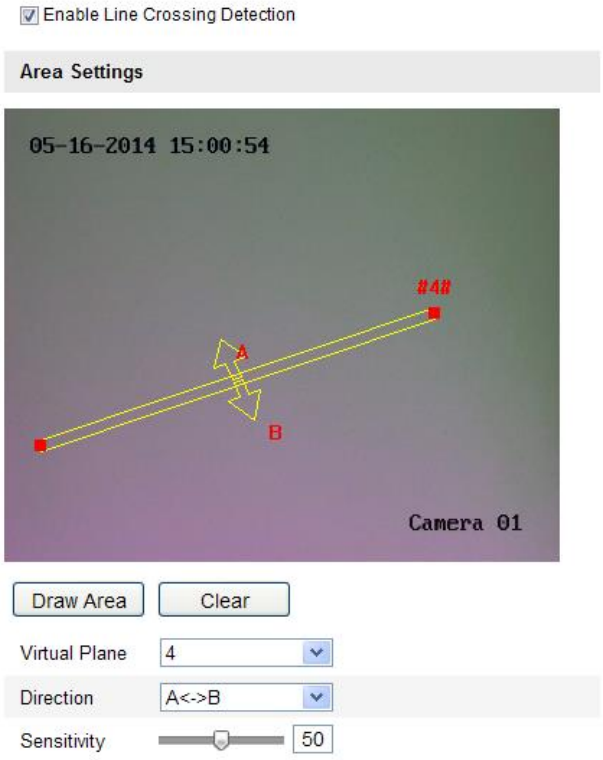
Uwaga: Zakres/dostępność funkcji wykrywania przekroczenia linii zależy od danego modelu kamery.

Procedura wykonania:

1. Wyświetl interfejs ekranowy ustawień, konfigurujących funkcję przekroczenia linii: **Configuration > Advanced Configuration > Smart Event > Line Crossing Detection**
2. Zaznacz pole wyboru **Enable Line Crossing Detection**, aby załączyć w kamerze funkcję wykrywania przekroczenia linii.
3. Z listy rozwijalnej **Virtual Plane** (płaszczyzna wirtualna)[13] wybierz żądaną linię (tj. jej numer identyfikacyjny), aby ją skonfigurować w następnych krokach procedury.

[13] Linia symbolizuje na obrazie sceny płaszczyznę wirtualną. — przyp. tłum.

4. Kliknij przycisk **Draw Area** — wtedy na podglądzie bieżącym kamery pojawia się ta wybrana wirtualna linia. (Jest to tzw. linia detekcyjna.)
5. Kliknij-i-przeciągnij tę wyświetloną linię, aby umieścić ją w żądanym miejscu sceny (podgląd na żywo). Kliknij w linię — wyświetlają się dwa kwadraciki na obu końcach linii i jeśli klikniesz-i-pociągniesz jeden z nich, to możesz określić kształt i długość linii.
6. Z listy rozwijalnej **Direction** wybierz kierunek przekroczenia tej linii (przez obiekt-cel), rozpoznawany jako przekroczenie linii.
   Kierunki do wyboru: **A<–>B**, **A–>B**, **B–>A**:
   A<–>B: Gdy dany obiekt porusza się po podglądzie i przekracza linię w obu kierunkach, zostaje wykryty i stosowne alarmy zostają wyzwolone.
   A–>B: Gdy dany obiekt przekracza tę konfigurowaną linię ze strony A na stronę B, może zostać wykryty.
   B–>A: Gdy dany obiekt przekracza tę konfigurowaną linię ze strony B na stronę A, może zostać wykryty.
7. Wyreguluj suwakiem ekranowym (kliknij-i-pociągnij) poziom czułości wykrywania przekroczenia konfigurowanej linii detekcyjnej.
   Sensitivity: Zakres regulacyjny [**1~100**]. Im wyższą wartość tu wyregulujesz, tym łatwiej operacja przekroczenia linii będzie mogła zostać wykryta.
8. Powtórz powyższe kroki, aby skonfigurować pozostałe, ewentualnie potrzebne linie — może być ich w sumie maks. **4** (cztery). Możesz ewentualnie kliknąć przycisk **Clear**, jeśli potrzebujesz skasować wszystkie dotychczas zdefiniowane linie.
9. Kliknij przycisk **Edit**, aby skonfigurować harmonogram uzbrajania funkcji wykrywania przekroczenia linii.
10. Zaznacz żądane pola wyboru od odnośnych akcji alarmowych, aby powiązać je z wykryciem przekroczenia linii — do wyboru są akcje: **Notify Surveillance Center** (wyślij powiadomienie do centrum monitoringu), **Send Email** (wyślij powiadomienie na adres e-mail), **Upload to FTP** (wyślij obrazek/ki na serwer FTP), **Trigger Channel** (wyzwól nagrywanie kanału), **Trigger Alarm Output** (pobudź wyjście alarmowe kamery).
11. Kliknij przycisk **Save**, aby zachować wprowadzone ustawienia.



Rys. 6–62: Definiowanie długości / położenia linii czułej na przekroczenia

6.7.6. Konfigurowanie wykrywania wtargnięć

Cel czynności:

Funkcja wykrywania wtargnięć wykrywa: osoby, pojazdy / inne obiekty, gdy te wejdą do zdefiniowanego (przez użytkownika) obszaru detekcyjnego i „kręcą się" w jego obrębie. Pozwala też wybrać pewne akcje alarmowe, które mają zostać wykonane w chwili, gdy zostanie wyzwolony alarm (w związku z tym zdarzeniem).

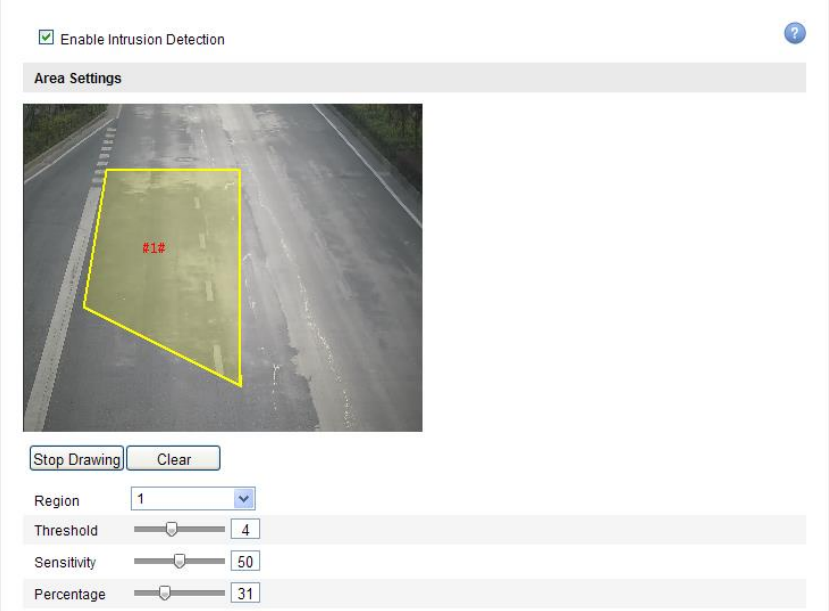
Uwaga: Zakres/dostępność funkcji wykrywania wtargnięć zależy od danego modelu kamery.

Procedura wykonania:

1. Wyświetl interfejs ekranowy ustawień, konfigurujących funkcję wtargnięcia: **Configuration > Advanced Configuration > Smart Event > Intrusion Detection**
2. Zaznacz pole wyboru **Enable Intrusion Detection**, aby załączyć w kamerze funkcję wykrywania wtargnięć.
3. Z listy rozwijalnej **Region** wybierz obszar detekcyjny (tj. jego numer identyfikacyjny) do skonfigurowania w następnych krokach procedury.
4. Kliknij przycisk **Draw Area**, aby wejść w procedurę „rysowania" obszaru.[14]
5. Kolejnymi kliknięciami na podglądzie bieżącym kamery określ położenie czterech narożników tego obszaru detekcyjnego. Następnie kliknij prawym klawiszem myszy, aby zakończyć tę procedurę „rysowania".

[14] tj. definiowania narożników obszaru — przyp. tłum.

6. Wyreguluj suwakami ekranowymi: próg czasu przebywania (**Threshold**), czułość wykrywania (**Sensitivity**), procent wypełnienia obszaru (**Percentage**) — charakteryzujące działanie funkcji wykrywania wtargnięć.
   Threshold: Zakres regulacyjny [**0s~10s**]. Jest to czasowy próg zadziałania, tj. minimalny czas, przez który obiekt musi się poruszać („kręcić się") w obrębie obszaru, aby zostało to wykryte jako wtargnięcie do obszaru. Jeśli zadasz tu wartość **0**, to alarm zostanie wyzwolony natychmiast, jak tylko obiekt wejdzie do tego obszaru.
   Sensitivity: Zakres regulacyjny [**1~100**]. Wartość czułości określa wielkość obiektu, który jest w stanie wyzwolić alarm detektora. Jeśli wartość ta jest duża, to nawet bardzo mały obiekt wyzwoli ten alarm wtargnięcia.
   Percentage: Zakres regulacyjny [**1~100**]. Wartość w tym parametrze definiuje procent wypełnienia całego obszaru przez obiekt znajdujący się wewnątrz obszaru, który jest w stanie wyzwolić alarm wtargnięcia. Jeśli, przykładowo, zadasz ten procent jako równy **50%** — to z chwilą, gdy dany obiekt wejdzie w obszar i zajmie co najmniej połowę całego obszaru, wyzwolony zostanie alarm wtargnięcia.
7. Powtórz czynności z powyższych kroków, aby skonfigurować pozostałe obszary tego detektora — może być ich w sumie maks. **4** (cztery). Możesz też ewentualnie kliknąć przycisk **Clear**, jeśli potrzebujesz skasować wszystkie dotychczas zdefiniowane obszary.
8. Kliknij przycisk **Edit**, aby skonfigurować harmonogram uzbrajania funkcji wykrywania wtargnięć.
9. Zaznacz żądane pola wyboru od odnośnych akcji alarmowych, aby powiązać je z wykryciem wtargnięć — do wyboru są akcje: **Notify Surveillance Center** (wyślij powiadomienie do centrum monitoringu), **Send Email** (wyślij powiadomienie na adres email), **Upload to FTP** (wyślij obrazek/ki na serwer FTP), **Trigger Channel** (wyzwól nagrywanie kanału), **Trigger Alarm Output** (pobudź wyjście alarmowe kamery).
10. Kliknij przycisk **Save**, aby zachować wprowadzone ustawienia.



Rys. 6–63: Konfigurowanie obszaru czułego na wtargnięcia (naruszenia obszaru)

6.7.7. Konfigurowanie wykrywania wejść do obszaru

Cel czynności:

Funkcja wykrywania wejść do obszaru wykrywa: osoby, pojazdy / inne obiekty, gdy te wejdą z zewnątrz do zdefiniowanego (przez użytkownika) obszaru detekcyjnego. Pozwala też wybrać pewne akcje alarmowe, które mają zostać wykonane w chwili, gdy zostanie wyzwolony alarm (w związku z tym zdarzeniem).

Uwaga: Zakres/dostępność funkcji wykrywania wejść do obszaru zależy od danego modelu kamery.

Procedura wykonania:

1. Wyświetl interfejs ekranowy ustawień, konfigurujących funkcję wykrywania wejść do obszaru:
   Configuration > Advanced Configuration > Smart Event > Region Entrance Detection
2. Zaznacz pole wyboru **Enable Region Entrance Detection**, aby załączyć w kamerze funkcję wykrywania wejść do obszaru.
3. Z listy rozwijalnej **Region** wybierz żądany obszar detekcyjny (tj. jego numer identyfikacyjny) do skonfigurowania w następnych krokach procedury.
4. Kliknij przycisk **Draw Area**, aby wejść w procedurę „rysowania” obszaru.
5. Kolejnymi kliknięciami na podglądzie bieżącym kamery określ położenie czterech narożników tego obszaru detekcyjnego. Następnie kliknij prawym klawiszem myszy, aby zakończyć tę procedurę „rysowania”.
6. Wyreguluj suwakiem ekranowym (kliknij-i-pociągnij) czułość wykrywania.
   Sensitivity: Zakres regulacyjny [1~100]. Wartość czułości określa wielkość obiektu, który jest w stanie wyzwolić alarm detektora. Jeśli wartość ta jest duża, to nawet bardzo mały obiekt, wchodzący do obszaru, wyzwoli ten alarm.

7. Powtórz powyższe kroki, aby skonfigurować pozostałe obszary tego detektora — może być ich w sumie maks. **4** (cztery). Możesz też ewentualnie kliknąć przycisk **Clear**, jeśli potrzebujesz skasować wszystkie dotychczas zdefiniowane obszary.
8. Kliknij przycisk **Edit**, aby skonfigurować harmonogram uzbrajania funkcji wykrywania wejść do obszaru.
9. Zaznacz żądane pola wyboru od odnośnych akcji alarmowych, aby powiązać je z wykryciem wejść do obszaru — do wyboru są akcje: **Notify Surveillance Center** (wyślij powiadomienie do centrum monitoringu), **Send Email** (wyślij powiadomienie na adres e-mail), **Upload to FTP** (wyślij obrazek/ki na serwer FTP), **Trigger Channel** (wyzwól nagrywanie kanału), **Trigger Alarm Output** (pobudź wyjście alarmowe kamery).
10. Kliknij przycisk **Save**, aby zachować wprowadzone ustawienia.

Rys. 6–64: Konfigurowanie wykrywania wejść do obszaru detekcyjnego

6.7.8. Konfigurowanie wykrywania wyjść z obszaru

Cel czynności:

Funkcja wykrywania wyjść z obszaru wykrywa: osoby, pojazdy / inne obiekty, gdy te opuszczają zdefiniowany (przez użytkownika) obszar detekcyjny. Pozwala też wybrać pewne akcje alarmowe, które mają zostać wykonane w chwili, gdy zostanie wyzwolony alarm (w związku z tym zdarzeniem).

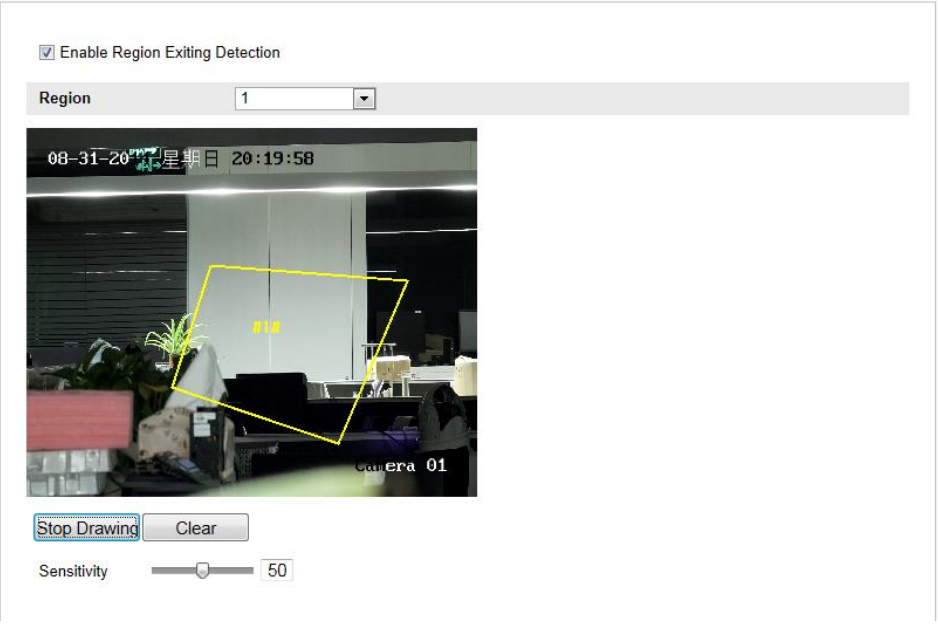
Uwaga: Zakres/dostępność funkcji wykrywania wyjść z obszaru zależy od danego modelu kamery.

Procedura wykonania:

1. Wyświetl interfejs ekranowy ustawień, konfigurujących funkcję wykrywania wyjść z obszaru:

   Configuration > Advanced Configuration > Smart Event > Region Exiting Detection

2. Zaznacz pole wyboru **Enable Region Exiting Detection**, aby załączyć w kamerze funkcję wykrywania wyjść z obszaru.
3. Z listy rozwijalnej **Region** wybierz żądany obszar detekcyjny (tj. jego numer identyfikacyjny) do skonfigurowania w następnych krokach procedury.
4. Kliknij przycisk **Draw Area**, aby wejść w procedurę „rysowania” obszaru.
5. Kolejnymi kliknięciami na podglądzie bieżącym kamery wprowadź położenie czterech narożników tego obszaru detekcyjnego. Następnie kliknij prawym klawiszem myszy, aby zakończyć tę procedurę „rysowania”.
6. Wyreguluj suwakiem ekranowym (kliknij-i-pociągnij) czułość wykrywania.
   Sensitivity: Zakres regulacyjny [**1~100**]. Wartość czułości określa wielkość obiektu, który jest w stanie wyzwolić alarm detektora. Jeśli wartość ta jest duża, to nawet bardzo mały obiekt, opuszczający obszar, wyzwoli ten alarm.
7. Powtórz powyższe kroki, aby skonfigurować pozostałe obszary tego detektora — może być ich w sumie maks. **4** (cztery). Możesz też ewentualnie kliknąć przycisk **Clear**, jeśli potrzebujesz skasować wszystkie dotychczas zdefiniowane obszary.
8. Kliknij przycisk **Edit**, aby skonfigurować harmonogram uzbrajania funkcji wykrywania wyjść z obszaru.
9. Zaznacz żądane pola wyboru od odnośnych akcji alarmowych, aby powiązać je z wykryciem wyjść z obszaru — do wyboru są akcje: **Notify Surveillance Center** (wyślij powiadomienie do centrum monitoringu), **Send Email** (wyślij powiadomienie na adres e-mail), **Upload to FTP** (wyślij obrazek/ki na serwer FTP), **Trigger Channel** (wyzwól nagrywanie kanału), **Trigger Alarm Output** (pobudź wyjście alarmowe kamery).
10. Kliknij przycisk **Save**, aby zachować wprowadzone ustawienia.



Rys. 6–65: Konfigurowanie wykrywania wyjść z obszaru detekcyjnego

6.7.9. Konfigurowanie wykrywania bagażu-bez-opieki

Cel czynności:

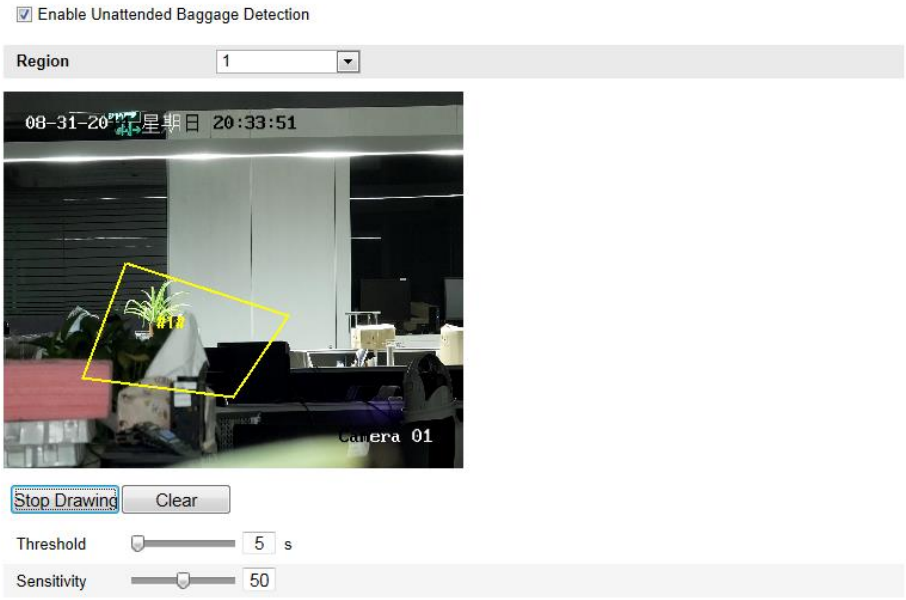
Funkcja wykrywania bagażu-bez-opieki wykrywa obiekty/przedmioty, gdy te są pozostawione same sobie w zdefiniowanym (przez użytkownika) obszarze detekcyjnym, jak np. sztuki bagażu, torebki, niebezpieczne materiały, itd. Pozwala też wybrać pewne akcje alarmowe, które mają zostać wykonane w chwili, gdy zostanie wyzwolony alarm (wskutek tego zdarzenia).

Uwaga: Zakres/dostępność funkcji wykrywania bagażu-bez-opieki zależy od danego modelu kamery.

Procedura wykonania:

1. Wyświetl interfejs ekranowy ustawień, konfigurujących funkcję wykrywania bagażu-bez-opieki:
   Configuration> Advanced Configuration> Smart Event> Unattended Baggage Detection
2. Zaznacz pole wyboru **Enable Unattended Baggage Detection**, aby załączyć w kamerze funkcję wykrywania bagażu pozostawionego bez opieki.
3. Z listy rozwijalnej **Region** wybierz żądany obszar detekcyjny (tj. jego numer identyfikacyjny) do skonfigurowania w następnych krokach procedury.
4. Kliknij przycisk **Draw Area**, aby wejść w procedurę „rysowania" obszaru.
5. Kolejnymi kliknięciami na podglądzie bieżącym kamery określ położenie czterech narożników tego obszaru detekcyjnego. Następnie kliknij prawym klawiszem myszy, aby zakończyć tę procedurę „rysowania".
6. Wyreguluj suwakami ekranowymi: próg czasu przebywania (**Threshold**), czułość wykrywania (**Sensitivity**) , aby doprecyzować warunki zadziałania wykrywania bagażu-bez-opieki.
   Threshold: Zakres regulacyjny [**5s~20s**]. Jest to czasowy próg zadziałania, tj. minimalny czas, przez który podejrzany obiekt musi pozostawać w obrębie obszaru detekcyjnego, aby został wykryty jako bagaż-bez-opieki. Jeśli zadasz tu, przykładowo, wartość **10**, to alarm zostanie wyzwolony po tym, jak obiekt pozostawiono w obszarze i pozostaje tam przez minimum 10 sekund.
   Sensitivity: Zakres regulacyjny [**1~100**]. Wartość czułości określa stopień podobieństwa tła sceny, analizowanego komparatywnie w skali czasu. W większości przypadków, gdy ta czułość ma dużą wartość, to nawet bardzo mały obiekt wyzwoli alarm detekcyjny.
7. Powtórz powyższe kroki, aby skonfigurować pozostałe obszary tego detektora — może być ich w sumie maks. **4** (cztery). Możesz też ewentualnie kliknąć przycisk **Clear**, jeśli potrzebujesz skasować wszystkie dotychczas zdefiniowane obszary.
8. Kliknij przycisk **Edit**, aby skonfigurować harmonogram uzbrajania funkcji wykrywania bagażu-bez-opieki.

9. Zaznacz żądane pola wyboru od odnośnych akcji alarmowych, aby powiązać je z wykryciem wtargnięć — do wyboru są akcje: **Notify Surveillance Center** (wyślij powiadomienie do centrum monitoringu), **Send Email** (wyślij powiadomienie na adres e-mail), **Upload to FTP** (wyślij obrazek/ki na serwer FTP), **Trigger Channel** (wyzwól nagrywanie kanału), **Trigger Alarm Output** (pobudź wyjście alarmowe kamery).
10. Kliknij przycisk **Save**, aby zachować wprowadzone ustawienia.



Rys. 6–66: Konfigurowanie wykrywania bagażu-bez-opieki

6.7.10. Konfigurowanie wykrywania usunięcia obiektu

Cel czynności:

Funkcja wykrywania usunięcia obiektu wykrywa obiekty/przedmioty – np. eksponaty wystawowe – które były, ale znikły ze zdefiniowanego (przez użytkownika) obszaru detekcyjnego. Pozwala też wybrać pewne akcje alarmowe, które mają zostać wykonane w chwili, gdy zostanie wyzwolony alarm (w związku z tym zdarzeniem).

Uwaga: Zakres/dostępność funkcji wykrywania usunięcia obiektu zależy od danego modelu kamery.

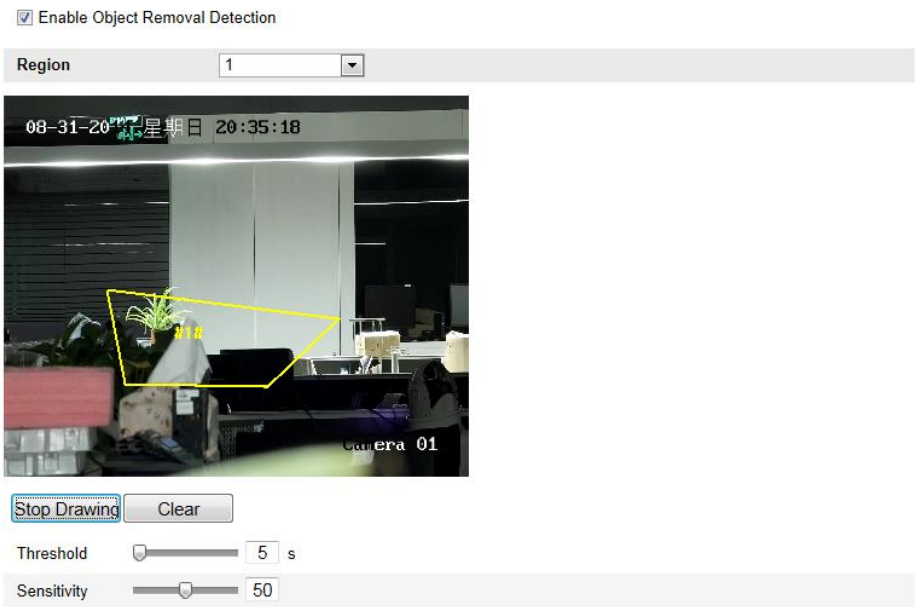
Procedura wykonania:

1. Wyświetl interfejs ekranowy ustawień, konfigurujących funkcję wykrywania usunięcia obiektu:
   Configuration > Advanced Configuration > Smart Event > Object Removal Detection
2. Zaznacz pole wyboru **Enable Object Removal Detection**, aby załączyć w kamerze funkcję wykrywania usunięcia obiektu.
3. Z listy rozwijalnej **Region** wybierz żądany obszar detekcyjny (tj. jego numer identyfikacyjny) do skonfigurowania w następnych krokach procedury.
4. Kliknij przycisk **Draw Area**, aby wejść w procedurę „rysowania” obszaru.

5. Kolejnymi kliknięciami na podglądzie bieżącym kamery określ położenie czterech narożników tego obszaru detekcyjnego. Następnie kliknij prawym klawiszem myszy, aby zakończyć tę procedurę „rysowania”.
6. Wyreguluj suwakami ekranowymi: próg czasu przebywania (**Threshold**), czułość wykrywania (**Sensitivity**), aby doprecyzować warunki zadziałania wykrywania usunięcia obiektu.

   Threshold: Zakres regulacyjny [**5s~20s**]. Jest to czasowy próg zadziałania, tj. minimalny czas, przez który obiektu musi nie być w obrębie obszaru detekcyjnego, aby zostało to wykryte jako jego usunięcie/zabranie. Jeśli zadasz tu wartość **10**, to alarm zostanie wyzwolony po tym, jak obiekt zniknie na co najmniej 10 s.

   Sensitivity: Zakres regulacyjny [**1~100**]. Wartość czułości określa stopień podobieństwa (mierzonego w czasie) tła sceny, analizowanego komparatywnie (z postępem czasu). W większości przypadków, gdy ta czułość ma dużą wartość, to nawet bardzo mały obiekt usunięty/zabrany z obszaru detekcyjnego wyzwoli alarm detekcyjny.
7. Powtórz powyższe kroki, aby skonfigurować pozostałe obszary tego detektora — może być ich w sumie maks. **4** (cztery). Możesz też ewentualnie kliknąć przycisk **Clear**, jeśli potrzebujesz skasować wszystkie dotychczas zdefiniowane obszary.
8. Kliknij przycisk **Edit**, aby skonfigurować harmonogram uzbrajania funkcji wykrywania usunięcia obiektu.
9. Zaznacz żądane pola wyboru od odnośnych akcji alarmowych, aby powiązać je z wykryciem usunięcia obiektu — do wyboru są akcje: **Notify Surveillance Center** (wyślij powiadomienie do centrum monitoringu), **Send Email** (wyślij powiadomienie na adres email), **Upload to FTP** (wyślij obrazek/ki na serwer FTP), **Trigger Channel** (wyzwól nagrywanie kanału), **Trigger Alarm Output** (pobudź wyjście alarmowe kamery).
10. Kliknij przycisk **Save**, aby zachować wprowadzone ustawienia.

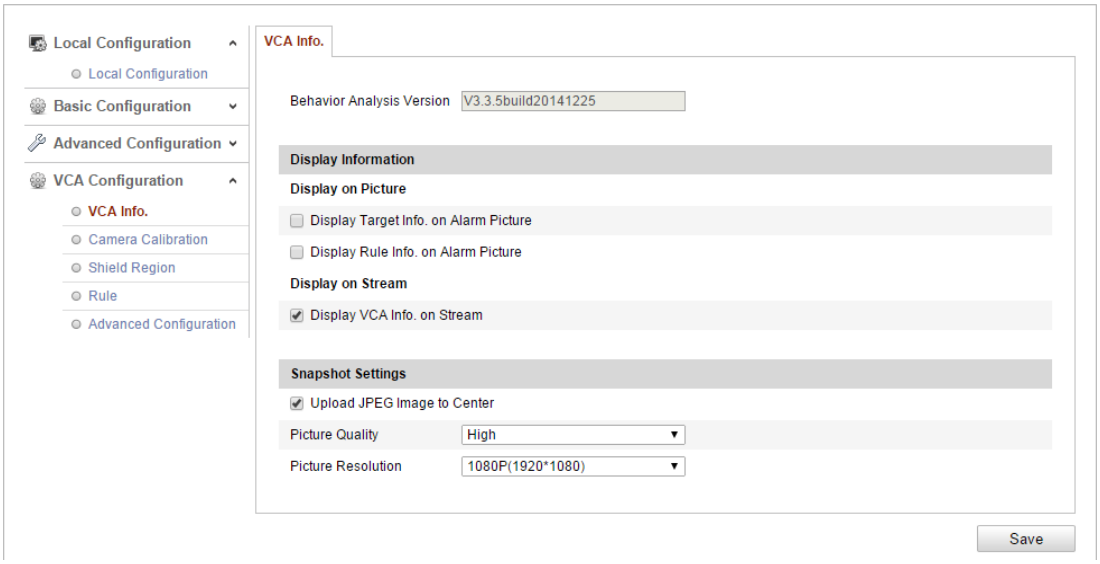


Rys. 6–67: Konfigurowanie wykrywania usunięcia obiektu (z obszaru detekcyjnego)

6.8. Konfigurowanie VCA

6.8.1. Analiza Zachowań

Tzw. *Analiza Zachowań* (**Behavior Analysis**) pozwala wykrywać ciągi podejrzanych zachowań obiektów oraz inicjować określone (powiązane z tym wykryciem) akcje alarmowe, wykonywane natychmiast w chwili wyzwolenia danego alarmu detekcyjnego.



Rys. 6–68: Pierwsza karta ustawień konfiguracyjnych *Analizy Zachowań VCA* – **VCA Info.**

❖ **Karta VCA Info**

Pole **Behavior Analysis Version**: Podaje wersję stosowanej biblioteki algorytmów.

Sekcja ustawień **Display Information** obejmuje ustawienia dot. wyświetlania na fotozrzutach (**Display on Picture**) oraz na wideo-strumieniu (**Display on Stream**).

Display Target info. on Alarm Picture — Jeśli zaznaczysz to pole wyboru, to na przysłanym via upload fotozrzucie alarmowym wokół wykrytego obiektu-celu alarmowego będzie wyświetlana ramka (w celu zaznaczenia go).

Display Rule info. on Alarm Picture — Jeśli zaznaczysz to pole wyboru, to na fotozrzucie alarmowym, wykryty obiekt-cel alarmowy i skonfigurowany obszar alarmowy będą ujęte w ramki, dla zaznaczenia ich.

Display VCA info. on Stream — Jeśli zaznaczysz to pole wyboru, to na wyświetlanym [podglądzie bieżącym z kamery] lub [obrazie odtwarzanym z nagrania] wykryty obiekt-cel alarmowy będzie otoczony zieloną ramką.

Uwaga: Upewnij się, że potrzebne reguły masz załączone w Twoich lokalnych ustawieniach — przejdź do **Configuration > Local Configuration > Rules**, aby załączyć te reguły.

Sekcja ustawień **Snapshot Settings**: Tu możesz wprowadzić dla fotozrzutów[15], wychwytywanych z obrazu kamery, żądaną jakość i rozdzielczość rejestracyjną.

[15] (tj. klatek wydzielonych z wideo kamery) — przyp. tłum.

Upload JPEG Image to Center — Zaznacz to pole wyboru, aby w chwili wystąpienia alarmu VCA zapisany fotozrzut alarmowy (plik obrazkowy JPEG) został wysłany z kamery przez sieć do centrum monitoringu.

Picture Quality — Wybierz z tej listy rozwijalnej żądaną jakość obrazową dla ww. fotozrzutów spośród opcji: **High** (wysoka), **Medium** (średnia), **Low** (niska).

Picture Resolution — Wybierz z tej listy rozwijalnej żądaną rozdzielczość obrazową dla ww. fotozrzutów spośród opcji: **CIF**, **4CIF**, **720P**, **1080P**.

❖ **Karta Camera Calibration**

Wykonaj poniższe kroki kalibracyjne, aby 3-wymiarowo zmierzyć i „posegmentować" podgląd z kamery, a następnie obliczyć wielkość każdego celu. Wykrywanie zachowań VCA będzie działało dokładniej, jeżeli przeprowadzisz kalibrację kamery.

Procedura wykonania:

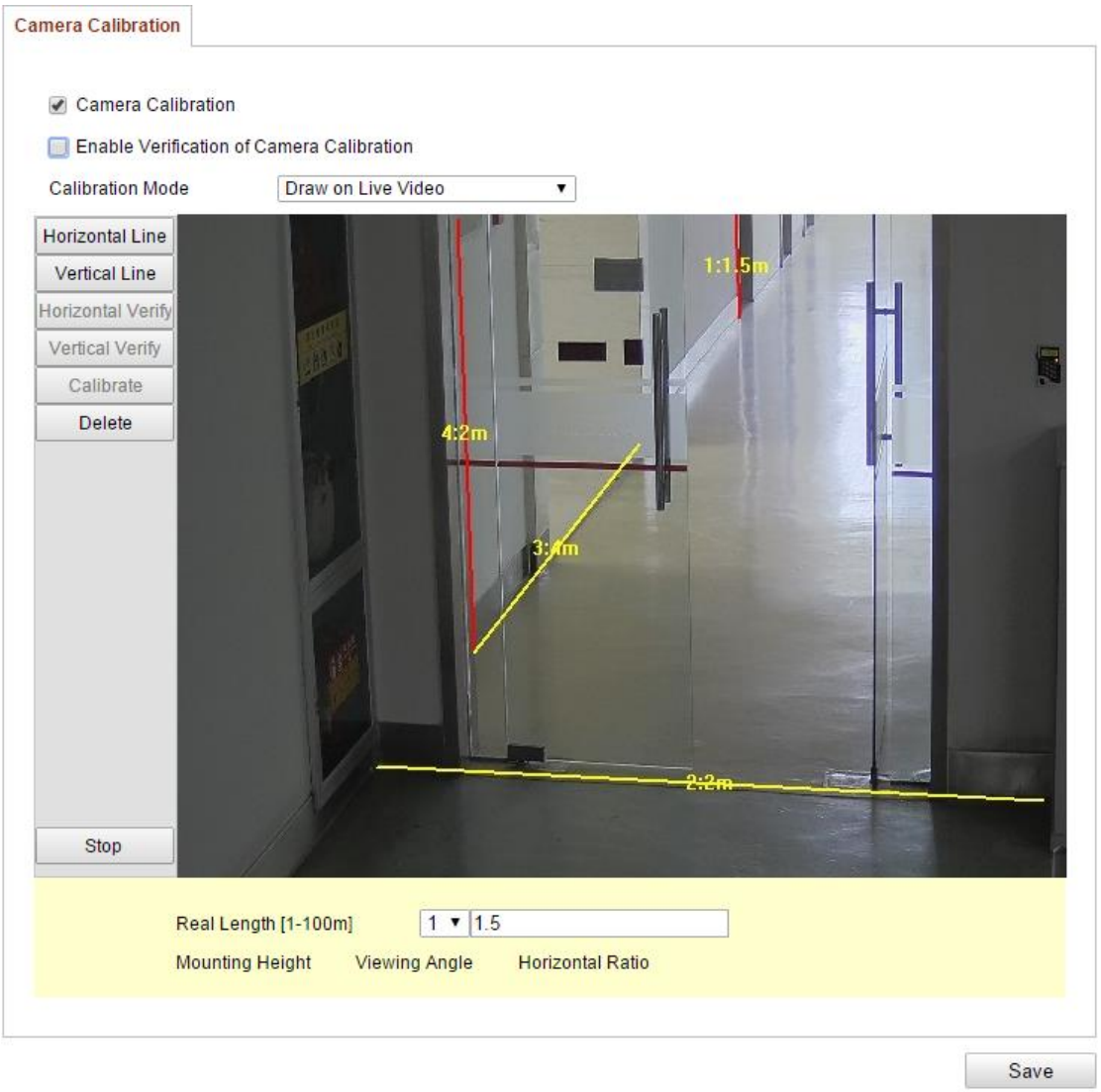
1. Zaznacz pole wyboru **Camera Calibration**, aby załączyć funkcję kalibracji.
2. Z listy rozwijalnej **Calibration Mode** wybierz żądany tryb kalibracji: **Input Basic Data** bądź **Draw on Live Video**.

   Input Basic Data (wprowadź dane podstawowe) — Wprowadź ręcznie: wysokość montażową kamery (**Mounting Height**), kąt skierowania kamery na scenę (**Viewing Angle**) oraz stosunek poziomy (**Horizontal Ratio**).

   Draw on Live View Video (rysuj na powierzchni podglądu bieżącego kamery) — Kliknij przycisk **Draw Verification Line (Horizontal) / (Vertical)**, aby na widoku z podglądem bieżącym narysować kalibracyjną linię poziomą / pionową i by wprowadzić w polu **Real Length** jej faktyczną długość.[16] Na podstawie tych narysowanych linii kalibracyjnych i ich faktycznej długości kamera potrafi wyciągać prawidłowe wnioski oceniające obiekty, pojawiające się w jej podglądzie bieżącym.
3. (*Ewentualnie*): Zaznacz pole wyboru **Enable Verification of Camera Calibration**. Po czym kliknij przycisk **Horizontal Verify** / **Vertical Verify**, aby narysować linię poziomą / linię pionową na podglądzie bieżącym kamery. Następnie kliknij przycisk **Calibrate**, aby kamera obliczyła długość odcinka, reprezentowanego przez tę linię, w rzeczywistości. Porównaj tę wyliczoną długość z długością w rzeczywistości, aby zweryfikować prawidłowość wprowadzonych danych kalibracyjnych.
4. W razie potrzeby możesz kliknąć przycisk **Delete**, aby skasować nim narysowane linie.
5. Kliknij przycisk **Save**, aby zachować wprowadzone ustawienia.

   Uwaga: Jeśli wyświetlanie podglądu bieżącego kamery zostanie zatrzymane[17], to wykonana kalibracja kamery traci ważność (invalid).

[16] długość odcinka w rzeczywistości, który reprezentuje ta narysowana linia — przyp. tłum.
[17] (zob. przycisk **Stop**) — przyp. tłum.



Rys. 6–69: Rysowanie linii kalibracyjnych w oknie z podglądem bieżącym kamery

❖ Karta Shield Region

Za pomocą opcji wykluczania obszarów **Shield Region** możesz wykluczyć z *Analizy Zachowań* pewien wskazany (tj. narysowany) przez Ciebie obszar. Możesz zadać w sumie **4** takie obszary chronione.

Procedura wykonania:

1. Kliknij zakładkę **Shield Region**, aby wyświetlić interfejs konfiguracyjny dla obszarów chronionych.
2. Kliknij przycisk **Draw Area**. Zdefiniuj żądany obszar chroniony przez kliknięcie lewym przyciskiem myszy w miejscach, które mają być narożnikami tego obszaru. Kliknij 1 raz prawym przyciskiem myszy, aby zakończyć procedurę rysowania.

   Uwagi:

   - Funkcja **Shield Region** obsługuje wieloboki z maks. 10 bokami.
   - W razie potrzeby kliknij przycisk **Delete**, aby skasować nim już narysowane obszary chronione.

- Jeśli wyświetlanie podglądu bieżącego kamery zostanie zatrzymane,[18] to nie da się w żaden sposób narysować obszarów chronionych.

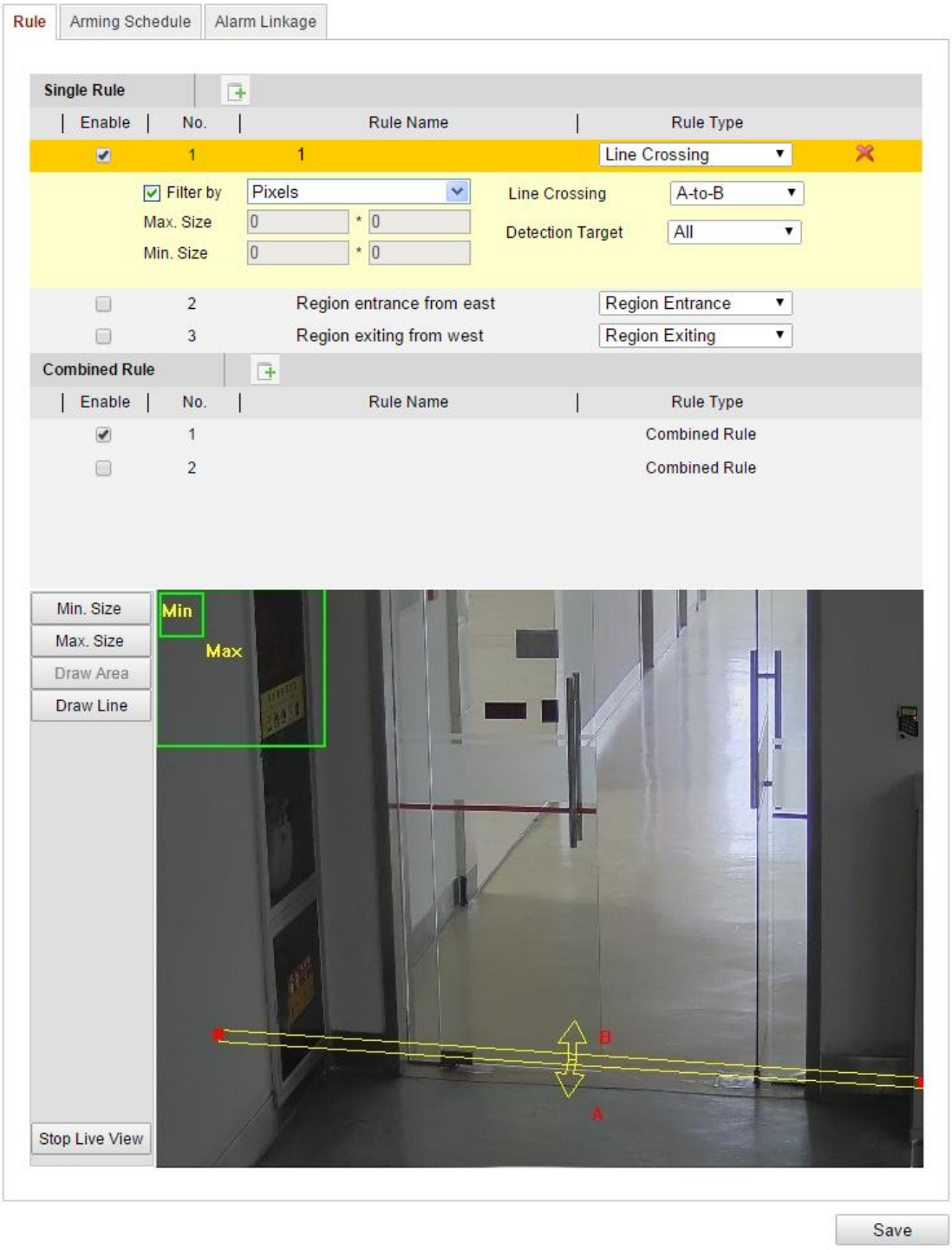
3. Kliknij przycisk **Save**, aby zachować wprowadzone ustawienia.

❖ **Karta Rule**

Analiza Zachowań (**Behavior Analysis**) potrafi analizować cały szereg różnych zachowań, m.in. potrafi wykrywać: przekraczanie linii, wtargnięcia-naruszenia obszaru, wejścia w obszar, wyjścia z obszaru, i inne.

Uwaga: Dokładny opis poszczególnych „zachowań" znajdziesz w odnośnych podrozdziałach (np. przekraczanie linii — *podrozdz. 6.7.5* od str. 99).

[18] (zob. przycisk **Stop**) — przyp. tłum.



Rys. 6–70: Konfigurowanie reguł detekcji alarmów dla *Analizy Zachowań*

Procedura wykonania:

1. Kliknij zakładkę **Rule**, aby wyświetlić interfejs z ustawieniami do skonfigurowania reguł detekcyjnych, wykorzystywanych przez *Analizę Zachowań*.
2. W sekcji **Single Rule**, definiującej pojedyncze reguły detekcyjne, zaznacz pole wyboru w kolumnie **Enable**, aby załączyć uwzględnianie tej reguły detekcyjnej w *Analizie Zachowań*, stosowanej przez kamerę.

3. W kolumnie **Rule Type** wybierz z listy rozwijalnej rodzaj żądanej reguły detekcyjnej (np. **Line Crossing**). Dalej, z listy rozwijalnej **Filter by** wybierz rodzaj filtrowania (np. **Pixels**). Po tym, na podglądzie bieżącym kamery narysuj linię detekcyjną / obszar detekcyjny, stanowiącą/y tę regułę pojedynczą.

   Filter by... (odfiltruj zdarzenia wg...) — W tej liście rozwijalnej dostępne są opcje: **Pixels** (wg pikseli) i **Actual Size** (wg wymiarów rzeczywistych).

   • Jeśli wybierzesz opcję **Pixels**, to narysuj na podglądzie bieżącym – dla każdej definiowanej reguły detekcyjnej – obszar wyznaczający rozmiary maksymalne (obiektu-celu) oraz obszar wyznaczający rozmiary minimalne (obiektu-celu).

   • Jeśli wybierzesz opcję **Actual Size**, to (zamiast rysować) wpisz ręcznie długość i szerokość, tj. rzeczywiste rozmiary minimalne i rozmiary maksymalne dla obiektu-celu. Alarm wyzwoli tylko ten obiekt-cel, którego wymiary będą pomiędzy **Min. Size** i **Max. Size**.

   Uwaga: Aby użyć opcji **Actual Size**, musisz mieć wykonaną kalibrację kamery (zob. str. 110).

   Detection Target (obiekt-cel dla wykrywania) — Wybierz z tej listy rozwijalnej rodzaj obiektu-celu do wykrycia: **Human** (człowiek), **Vehicle** (pojazd). Możesz też wybrać opcję **All**, aby wszelkie obiekty spełniające regułę były wykrywane jako cele alarmowe.

   Draw Line (rysuj linię) / **Draw Area** (rysuj obszar) — W przypadku wykrywania przekraczania linii detekcyjnej (zob. wyżej **Rule Type**), musisz narysować tę linię i wybrać dla niej kierunek przekraczania (zob. lista rozwijalna **Line Crossing**), którym może być: **Bidirectional** (w obie strony) lub **A-to-B** (ze strony A na stronę B) lub **B-to-A** (ze strony B na stronę A). Natomiast dla pozostałych zdarzeń detekcyjnych (jak np.: wtargnięcia-naruszenia obszaru, wejścia do obszaru, wyjścia z obszaru, itd.) musisz kolejnymi kliknięciami lewym przyciskiem myszy na podglądzie bieżącym kamery zdefiniować kolejne wierzchołki żądanego obszaru detekcyjnego, a na koniec musisz kliknąć prawym przyciskiem myszy, aby zakończyć to „rysowanie” obszaru.

   Uwaga: Jeśli wyświetlanie podglądu bieżącego kamery jest zatrzymane,[19] to nie da się rysować ani linii detekcyjnych ani obszarów detekcyjnych, a także nie da się konfigurować reguł detekcyjnych.

4. W sekcji **Combined Rule**, definiującej kombinowane reguły detekcyjne, zaznacz pole wyboru w kolumnie **Enable** aby załączyć uwzględnianie takiej reguły detekcyjnej w *Analizie Zachowań*, stosowanej przez kamerę.
5. Wybierz dwie wcześniej skonfigurowane reguły pojedyncze, regułę A (**Rule A**) i regułę B (**Rule B**), które mają tworzyć Twoją regułę kombinowaną. Ustaw minimalny i maksymalny odstęp czasu dla tych dwóch pojedynczych reguł, a

[19] (zob. przycisk **Stop Live View**) — przyp. tłum.

następnie wybierz kolejność wyzwalania (**Trigger Order**) używaną do filtrowania zdarzeń alarmowych.

Uwagi:

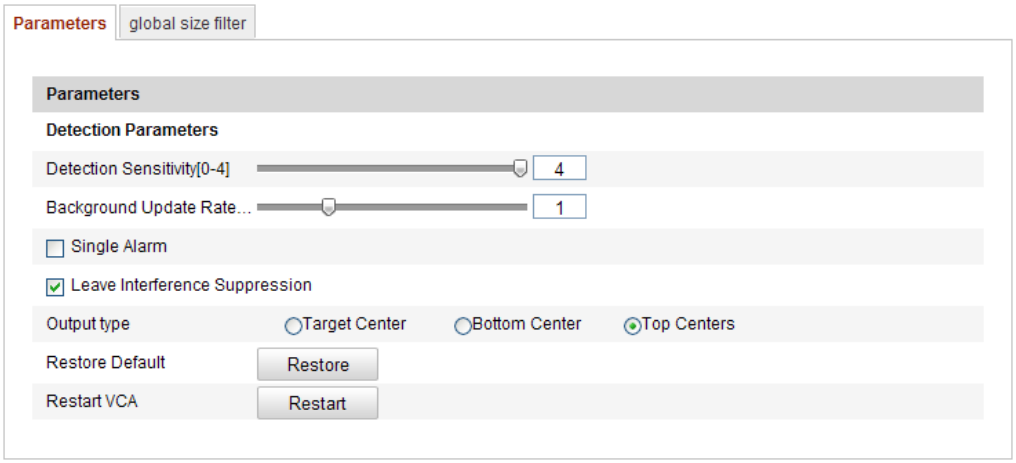
- Jeśli jako **Rule Type** wybierzesz opcję **None**, to ta reguła jest systemowo nieważna (invalid), czyli nie ma skonfigurowanej żadnej *Analizy Zachowań*.
- Kolejność wyzwalania (**Trigger Order**) reguł pojedynczych, zapewniającą osiągnięcia żądane filtrowanie zdarzeń alarmowych, możesz zdefiniować albo jako **In Ascending Order** (w porządku rosnącym) albo jako **In Ascending/Descending Order** (w porządku rosnącym / malejącym).
- Możesz skonfigurować maks. **8** (osiem) reguł pojedynczych i **2** (dwie) reguły kombinowane. Reguły kombinowane obsługują: przekraczanie linii, wtargnięcia-naruszenia, wejścia do obszaru, wyjścia z obszaru.

6. Kliknij przycisk **Save**, aby zachować wprowadzone ustawienia.
7. Kliknij zakładkę **Arming Schedule**, po czym kliknij przycisk **Edit**, aby skonfigurować harmonogram uzbrajania każdej poszczególnej reguły detekcyjnej. Następnie kliknij przycisk **Save**, aby zachować wprowadzone ustawienia.
8. Kliknij zakładkę **Alarm Linkage**, po czym zaznacz pola wyboru od akcji alarmowych, które mają być powiązane z każdą poszczególną regułą detekcyjną. Następnie kliknij przycisk **Save**, aby zachować wprowadzone ustawienia.

❖ **Karta Advanced Configuration**

- Karta **Parameters**

Skonfiguruj opisane niżej parametry (konfiguracji zaawansowanej), aby doprecyzować ustawienia konfiguracyjne kamery.



Rys. 6–71: Interfejs ustawień zaawansowanych VCA – karta zakładki **Advanced Configuration**

Detection Sensitivity [0~4] (czułość wykrywania): Ten parametr jest czułością, z jaką kamera ma wykrywać obiekt-cel. Im wyższa jest ta wartość, tym łatwiej obiekt-cel zostanie rozpoznany, ale także tym wyższa szansa omylności detektora. Zalecamy użycie wartości domyślnej: **3.**

Background Update Rate [0~4] (szybkość odświeżania tła): Ten parametr jest tempem, z jakim nowa scena zastępuje scenę poprzednią. Zalecamy użycie wartości domyślnej: **3.**

Single Alarm (alarm jednorazowy): Jeśli zaznaczysz to pole wyboru, to obiekt-cel w konfigurowanym obszarze detekcyjnym wyzwoli alarm tylko jeden raz. Jeśli go nie zaznaczysz, to tenże sam obiekt-cel wyzwoli alarm ciągły, z tegoż samego obszaru detekcyjnego.

Leave Interference Suppression (filtr zakłóceń pochodzących od liści/listowia): Zaznacz to pole wyboru, aby zredukować zakłócenia detekcyjne, wywoływane przez liście widoczne w konfigurowanym obszarze detekcyjnym.

Output Type (orientacja wyjścia): Wybierz żądane położenie ramki spośród dostępnych opcji: **Target Center** (środek obiektu-celu), **Bottom Center** (środek części dolnej), **Top Centers** (środki części górnej). Jeśli, przykładowo, wybierzesz **Target Center**, to obiekt-cel będzie znajdować się w środku ramki.

Restore Default: Kliknij przycisk **Restore**, aby przywrócić konfigurowane parametry do ich wartości domyślnych.

Restart VCA: Kliknij przycisk **Restart**, aby zrestartować bibliotekę algorytmów wykorzystywaną przez moduł *Analizy Zachowań*.

- Funkcja **Global Size Filter**

  Uwaga: W porównaniu z filtrem analizy rozmiarów w ramach danej reguły detekcyjnej (który działa na poszczególne reguły z osobna), globalny filtr analizy rozmiarów (tj. **Global Size Filter**) działa na *wszystkie* reguły.

Procedura wykonania:

1. Zaznacz pole wyboru **Global Size Filter**, aby załączyć funkcję filtru globalnego.
2. Z listy rozwijalnej **Filter Type** (rodzaj filtru) wybierz: **Actual Size** bądź **Pixel**.

   Opcja **Actual Size**: Wprowadź długość i szerokość zarówno w polach rozmiaru minimalnego **Min. Size**, jak i rozmiaru maksymalnego **Max. Size**. Alarm wyzwoli tylko ten obiekt-cel, którego wymiary będą się zawierały pomiędzy **Min. Size** a **Max. Size**.

   Uwagi:

   - Aby użyć opcji **Actual Size**, musisz mieć wykonaną kalibrację kamery (zob. str. 110).
   - Wartość długości zadana w rozmiarze maksymalnym (**Max. Size**) musi być dłuższa niż wartość długości zadana w rozmiarze minimalnym (**Min. Size**); i to samo ograniczenie obowiązuje dla szerokości.

   Opcja **Pixel**: Kliknij przycisk **Minimum Size**, aby na podglądzie bieżącym narysować prostokąt, specyfikujący rozmiary minimalne obiektu-celu. Kliknij też przycisk **Maximum Size**, aby na podglądzie bieżącym narysować prostokąt, specyfikujący rozmiary maksymalne obiektu-celu. Obiekt-cel mniejszy niż ten zdefiniowany prostokąt **Min. Size** lub większy niż ten zdefiniowany prostokąt **Max. Size** zostanie każdorazowo odfiltrowany.

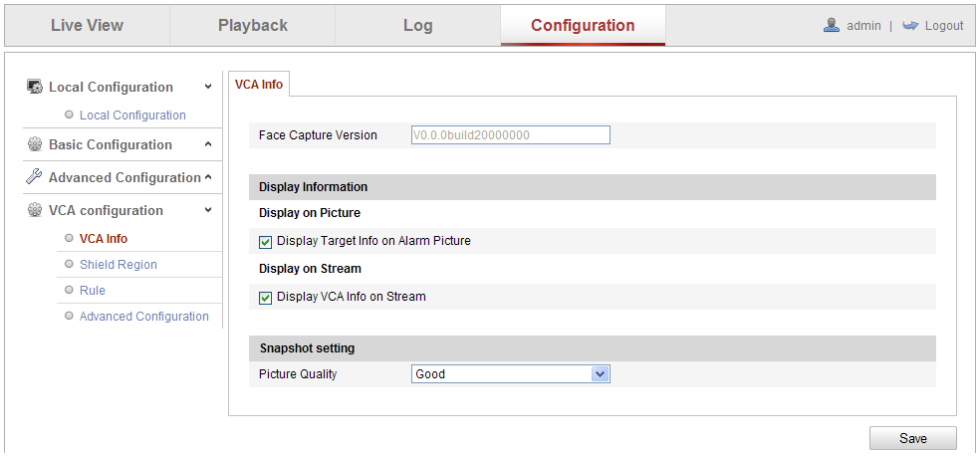
Uwagi:

- Narysowany obszar zostanie automatycznie w tle przeliczony na piksele (algorytm przetwarzający w tle).
- Nie da się skonfigurować globalnego filtru analizy rozmiarów (tj. **Global Size Filter**), jeśli wyświetlanie podglądu bieżącego kamery jest zatrzymane (**Stop**).
- Wartość długości zadana w rozmiarze maksymalnym (**Max. Size**) musi być dłuższa niż wartość długości zadana w rozmiarze minimalnym (**Min. Size**); to samo ograniczenie obowiązuje dla szerokości.

3. Kliknij przycisk **Save**, aby zachować wprowadzone ustawienia.

6.8.2. Rejestrowanie twarzy

Funkcja rejestrowania twarzy (**Face Capture**) potrafi zarejestrować obraz twarzy, gdy ta pojawi się w odpowiednio skonfigurowanym obszarze detekcyjnym. Ponadto, wraz z tym obrazem, funkcja ta wyśle przez via upload szereg cech charakterystycznych wykrytej twarzy, *w tym:* wiek, płeć, obecność / brak okularów na twarzy.



Rys. 6–72: Funkcja wykrywania twarzy (**Face Capture**)

❖ **Karta VCA Info**

Pole danych **Face Capture Version**: Tu podawana jest wersja używanej biblioteki algorytmów.

Sekcja ustawień **Display Information** obejmuje ustawienia wyświetlania na fotozrzutach alarmowych (**Display on Picture**) oraz wyświetlania na wideo-strumieniu (**Display on Stream**).

Display Target info. on Alarm Picture — Jeśli zaznaczysz to pole wyboru, to na przysłanym via upload fotozrzucie alarmowym dookoła obiektu-celu alarmowego będzie wyświetlana ramka, zaznaczająca go.

Display VCA info. on Stream — Jeśli zaznaczysz to pole wyboru, to na wyświetlanym [podglądzie bieżącym z kamery] czy na [obrazie kamery odtwarzanym z nagrania] wykryty obiekt-cel alarmowy będzie widać otoczony zieloną ramką.

Sekcja ustawień **Snapshot Settings**: Tu możesz wybrać żądaną jakość rejestracyjną dla fotozrzutów detekcyjnych wychwytywanych z wideo kamery.

Picture Quality (jakość obrazowa) — Z tej listy rozwijalnej wybierz żądaną jakość obrazu spośród dostępnych opcji: **Good** (dobra), **Better** (lepsza), **Best** (najlepsza).

❖ Karta Shield Region

Za pomocą funkcji wykluczania obszarów (**Shield Region**) możesz przez narysowanie zadać obszar, w którym rejestrowanie twarzy ma nie działać. Możesz zadać w sumie **4** takie obszary chronione.

Procedura wykonania:

1. Kliknij zakładkę **Shield Region**, aby wyświetlić interfejs konfiguracyjny dla obszarów chronionych.
2. Kliknij przycisk **Draw Area**. Zdefiniuj żądany obszar chroniony klikając lewym przyciskiem myszy w 4 miejscach, które mają być 4 narożnikami tego obszaru. Kliknij 1 raz prawym przyciskiem myszy, aby zakończyć procedurę rysowania.

   Uwagi:

   - Kliknij przycisk **Delete**, aby ewentualnie skasować już narysowane obszary chronione.
   - Jeśli wyświetlanie podglądu bieżącego kamery jest zatrzymane (**Stop**), to nie da się w żaden sposób narysować obszarów chronionych.
3. Kliknij przycisk **Save**, aby zachować wprowadzone ustawienia.

❖ Karta Rule

Procedura wykonania:

1. Zaznacz pole wyboru **Rule**, aby załączyć funkcję rejestrowania twarzy.
2. Kliknij przycisk **Minimize Pupil Distance**, aby przez narysowanie zadać minimalny odstęp źrenic oczu (dla wykrywanych twarzy). Narysowana odległość zostanie wyświetlona jako liczba w polu pod panelem podglądu bieżącego kamery.

   Wartość **Minimize Pupil Distance** to rozmiar najmniejszego kwadratowego obszaru, istniejącego pomiędzy dwiema źrenicami. Jest to podstawowy wzorzec detekcyjny stosowany przez kamerę do rozpoznania celu.[20]
3. Kliknij przycisk **Draw Area**, aby „narysować” obszar, w którym ma zachodzić wykrywanie/rejestrowanie twarzy. Narysuj go kolejnymi kliknięciami lewego przycisku myszy na wyświetlającym się podglądzie bieżącym kamery, i zakończ to „rysowanie” przez kliknięcie prawym przyciskiem myszy.

   Uwagi:

   - Funkcja obsługuje obszary wieloboczne o liczbie boków: **4~10**.

[20] (tj. twarzy w scenie) — przyp. tłum.

- Jeśli wyświetlanie podglądu bieżącego kamery jest zatrzymane (**Stop**), to nie da się w żaden sposób narysować konfigurowanego obszaru detekcyjnego.

4. Kliknij przycisk **Save**, aby zachować wprowadzone ustawienia.

❖ **Karta Advanced Configuration**

Skonfiguruj poniższe parametry zgodnie z rzeczywistymi warunkami, panującymi w Twoim otoczeniu monitorowanym.

Sekcja **Parameters >> podsekcja Detection Parameters**:

Suwaki ekranowe:

Generation Speed [**1~5**]: Jest to szybkość rozpoznawania obiektu-celu detekcji. Im wyższa jest ta wartość, tym szybciej wykrywany cel zostanie rozpoznany. Jeśli zadasz w tym parametrze bardzo małą wartość, to — o ile dana twarz od początku była obecna w konfigurowanym obszarze detekcyjnym — twarz ta nie zostanie zarejestrowana. Ten parametr pomaga obniżyć omylność funkcji rejestrowania twarzy w przypadku twarzy widocznych na muralach (wzgl. malowidłach ściennych) czy na plakatach/afiszach reklamowych. Zalecamy użycie wartości domyślnej: **3.**

Capture Times [**1~10**]: Parametr podaje, ile razy kamera zarejestruje daną twarz, pozostającą w konfigurowanym obszarze detekcyjnym. Wartość domyślna: **1.**

Sensitivity [**1~5**]: Jest to czułość rozpoznawania celu detekcji. Im wyższa jest ta wartość, tym łatwiej twarze będą rozpoznawane, ale także tym bardziej wzrasta poziom omylności takiego rozpoznawania. Zalecamy użycie domyślnej wartości: **3.**

Capture Interval [**1~255 frame**]: Jest to odstęp międzyklatkowy dla operacji rejestrowania twarzy. Jeśli ustawisz tu 1 (tj. wartość domyślną), to znaczy, że kamera ma rejestrować twarz w każdej klatce obrazu.

Capture Sensitivity [**0~20**]: Jest to próg zadziałania detekcji, na podstawie którego kamera może potraktować potencjalny cel jako twarz. Tylko wtedy — gdy wynik rozpoznawania twarzy (tzw. *face score*), obliczony przez algorytm klasyfikatora analizy, jest równy lub większy od tej wartości — kamera uzna i potraktuje cel jako twarz. Zalecamy użycie wartości domyślnej: **2.**

Sekcja **Parameters >> podsekcja Face Capture Advanced... Parameters**:

Pole wyboru **Face Exposure** (naświetlenie twarzy)**:** Zaznacz to pole, aby załączyć funkcję korekcji naświetlenia twarzy (ekspozycji twarzy).

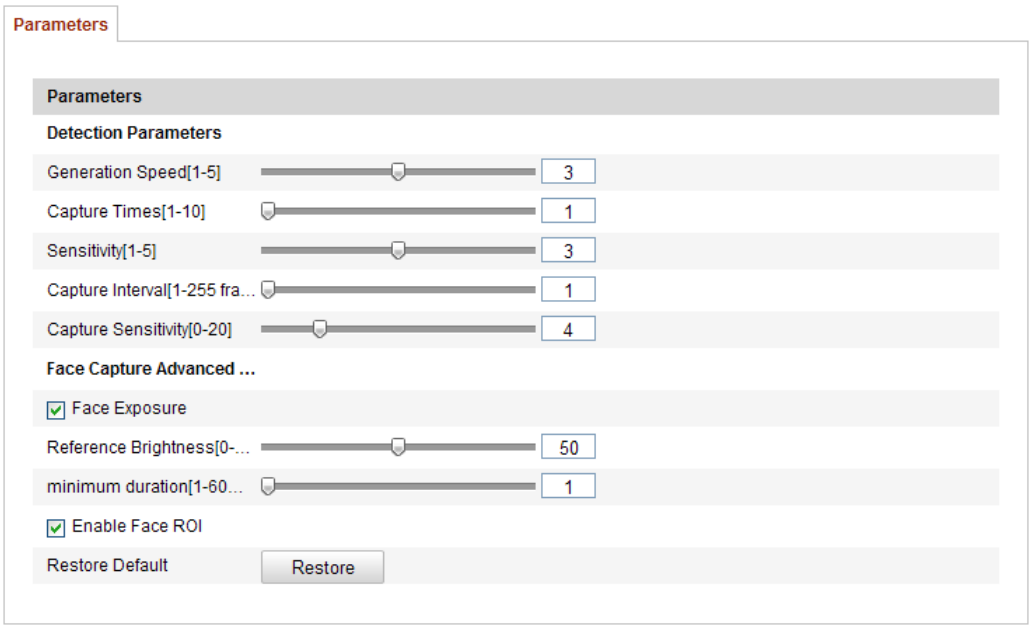
Suwaki ekranowe:

Reference Brightness [**0~100**]: Jest to jaskrawość odniesienia (dokł. poziom odniesienia dla jaskrawości) w trybie korekcji naświetlenia twarzy. Jeśli twarz zostanie wykryta, to kamera nałoży korekcję jasności twarzy zgodnie z wartością, którą zadasz tym suwakiem. Im wyższa będzie zadana tu wartość, tym jaśniejsza będzie twarz.

minimum duration [**1~60min**]: Minimalny czas trwania, przez który kamera naświetla twarz. Wartością domyślną jest: **1** minuta.

Uwaga: Jeśli załączysz korekcję naświetlania twarzy (**Face Exposure**), to upewnij się, że masz odłączoną w ustawieniach funkcję WDR oraz że wybrałeś przysłonę ręcznie sterowaną (manual iris).

Pole wyboru **Enable Face ROI**: Po zaznaczeniu tego pola wyboru, jeśli kamera zarejestruje daną twarz, to obszar tej twarzy będzie traktowany jako obszar ROI i w konsekwencji jakość obrazu w obrębie tego obszaru odpowiednio wzrośnie.
Etykieta **Restore Default**: Kliknij przycisk **Restore**, aby przywrócić wszystkie ustawienia tej konfiguracji zaawansowanej do fabrycznych wartości domyślnych.



Rys. 6–73: Funkcja wykrywania twarzy (**Face Capture**) – ustawienia zaawansowane (**Advanced Configuration**)

6.8.3. Zliczanie osób

Cel czynności:

Funkcja zliczania osób (**People Counting**) służy do obliczenia liczby obiektów, które weszły lub wyszły do/z pewnego skonfigurowanego obszaru detekcyjnego i jest powszechnie stosowana w monitoringu wejść lub wyjść (na chronionym obiekcie).

Uwagi:

- W porównaniu z funkcją zliczania obsługiwaną przez kamery typu Non-iDS — niniejsza funkcja zliczania osób (**People Counting**) wymaga wprowadzenia ustawień kalibracyjnych kamery, aby zapewnić większą dokładność wyników.
- Aby podnieść dokładność zliczania przez tę funkcję, zalecamy zamontować kamerę możliwe dokładnie nad samym monitorowanym wejściem/wyjściem; należy też upewnić się, że kamera jest poziomo.

Procedura wykonania:

❖ **Zakładka People Counting — funkcja zliczania osób**

1. Wyświetl interfejs ekranowy, służący do konfigurowania funkcji zliczania osób:

Configuration > Advanced Configuration > People Counting

Rys. 6–74: Konfigurowanie funkcji zliczania ludzi (People Counting Configuration)

2. Kliknij w zakładkę People Counting Configuration, aby na jej karcie skonfigurować parametry szczegółowe funkcji zliczania osób.
3. Zaznacz pole wyboru Enable Counting, aby załączyć w kamerze tę funkcję.
4. (*Ewentualnie*): Zaznacz pole wyboru Enable OSD Overlay (załącz nakładanie danych na ekran), aby na podglądzie bieżącym kamery wyświetlała się liczba obiektów wchodzących (napis Enter:) i wychodzących (napis Leave:), aktualizowana w czasie rzeczywistym.

   Możesz również przesunąć miejsce wyświetlania ww. nakładki danych (OSD), aby uzyskać lepsze dopasowanie do faktycznych potrzeb monitoringu.
5. Skonfiguruj linię detekcyjną dla realizacji funkcji zliczania osób:

   Na podglądzie bieżącym kamery możesz wprowadzić pomarańczową linię – zwaną linią detekcyjną – aby funkcja zliczała obiekty/osoby wchodzące lub wychodzące przez tę linię (zob. ilustracja powyżej). W tym celu:

   1) Kliknij przycisk **Draw Line**, wtedy na obrazie pojawi się ww. pomarańczowa linia.

      Uwaga:

      - Linię detekcyjną musisz narysować na obrazie w punkcie, który jest położony dokładnie pod kamerą. Linia ta powinna być ponadto na tyle długa, żeby obejmowała cały obszar/prześwit wejścia/wyjścia.
      - Linię detekcyjną narysuj w takim miejscu, w którym mało kto dłużej przestaje, ociągając się z wejściem/wyjściem.

2) Kliknij-i-przeciągnij linię detekcyjną po obrazie myszką, aby wybrać dla niej optymalne położenie w scenie.
3) Kliknij-i-pociągnij za któryś z dwóch końców narysowanej linii detekcyjnej (po jednym na raz), aby optymalnie wyregulować jej długość.
4) Aby ewentualnie usunąć aktualną linię detekcyjną, kliknij przycisk **Delete Line**.

6. Zaznacz pole wyboru **Enable Calibration**, aby załączyć kalibrowanie kamery.
   Po załączeniu ww. kalibrowania kamery w oknie konfiguracyjnym pojawia się pionowa linia. Ponadto, jeśli jeden cel przekroczy pomarańczową linię detekcyjną, pojawia się linia pozioma (niebieska). Po jednej stronie linii detekcyjnej może wyświetlić się maks. 8 linii poziomych.
   Ww. linia pozioma zostaje wyliczona zgodnie z szerokością ramion (barków) wykrytego obiektu-celu. I wtedy – na podstawie szerokości różnych kolejnych przemieszczających się obiektów – możesz wybrać najbardziej optymalne położenie linii kalibracyjnej. Aby przesunąć linię kalibracyjną w to żądane miejsce, kliknij-i-przeciągnij ją po obrazie.
7. Kliknij przycisk **Reset Counter** (zeruj licznik), a wtedy licznik osób wchodzących (**Enter:**) oraz licznik osób wychodzących (**Leave:**) zostają przestawione na 0 (zero).
8. Kliknij przycisk **Edit**, aby skonfigurować harmonogram uzbrajania dla funkcji zliczania osób.
9. Zaznacz pole wyboru **Notify Surveillance Center** (powiadom centrum monitoringowe), aby powiązać do funkcji zliczania tę akcję alarmową.
10. Kliknij przycisk **Save**, aby zachować wprowadzone ustawienia.

❖ Zakładka People Counting Statistics — opracowanie statystyczne zliczeń osób

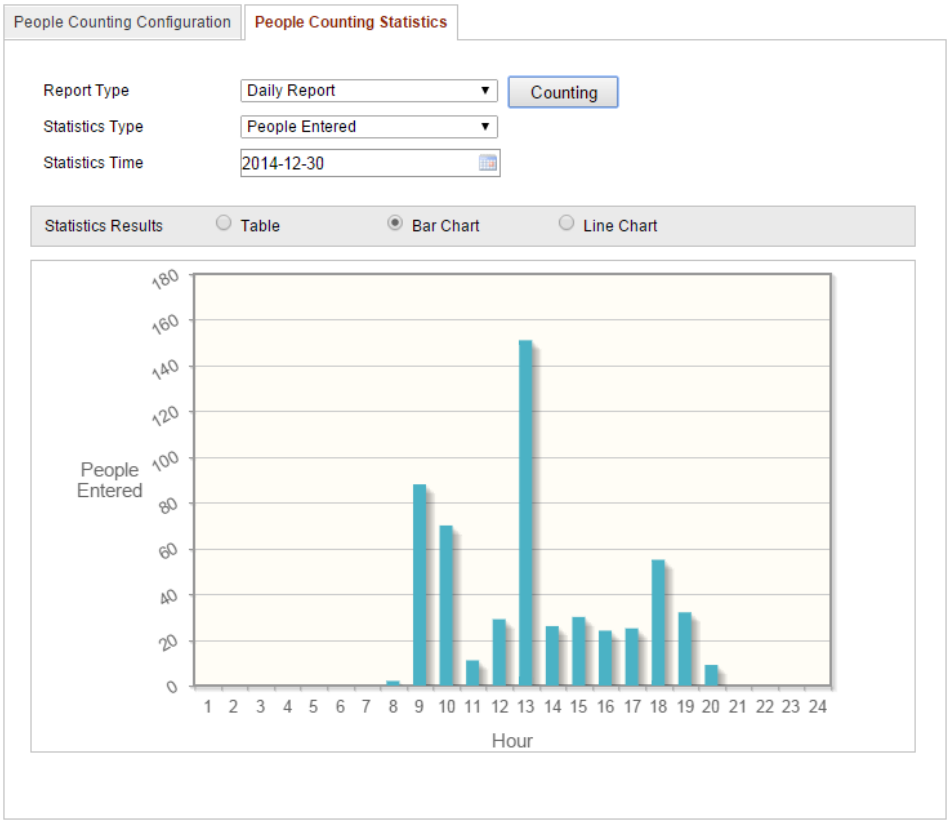
Procedura wykonania:

1. Kliknij zakładkę **People Counting Statistics**, aby wyświetlić na jej karcie interfejs, pozwalający zaprezentować zliczenia osób w raportach statystycznych.
2. Z listy rozwijalnej **Report Type** wybierz żądany rodzaj raportu z danych — do wyboru są: **Daily Report** (dobowy), **Weekly Report** (tygodniowy), **Monthly Report** (miesięczny), **Annual Report** (całoroczny).
3. Z listy rozwijalnej **Statistics Type** wybierz żądany przedmiot opracowania statystycznego w tym raporcie spośród dostępnych: **People Entered** (osoby, które weszły) bądź **People Exited** (osoby, które wyszły).
   Uwaga: Raport typu dobowego (**Daily Report**) oblicza swoje dane dla dnia, który aktualnie wybrałeś.[21] Raport tygodniowy oblicza je dla tygodnia, który obejmuje Twój dzień wybrany. Raport miesięczny oblicza je dla miesiąca, który obejmuje Twój dzień wybrany. A raport całoroczny oblicza je dla roku, który obejmuje Twój dzień wybrany.

[21] (zob. dzień wybrany w liście rozwijalnej **Statistics Time**) — przyp. tłum.

4. Z listy rozwijalnej **Statistics Time** wybierz punkt czasu dla przygotowania raportu z odpowiedniego okresu.
5. Kliknij przycisk **Counting**, aby obliczyć i pokazać rozkład statystyczny osób w zależności od czasu dla raportu.
6. Przyciskami wyboru opcji (**Statistics Result**) wybierz żądaną formę eksportu/prezentacji raportu: **Table** (tabela), **Bar Chart** (wykres słupkowy), **Line Chart** (wykres liniowy).

   Uwaga: Jeśli do wyświetlenia danych wybierzesz tu opcję prezentacji stabelaryzowanej (**Table**), to w interfejsie pojawi się dodatkowo przycisk **Export**, który umożliwi Ci wyeksportowanie tych danych w formacie arkusza kalkulacyjnego Excel.



Rys. 6–75: Wyniki zliczeń osób w opracowaniu statystycznym (na wykresie słupkowym – **Bar Chart**)

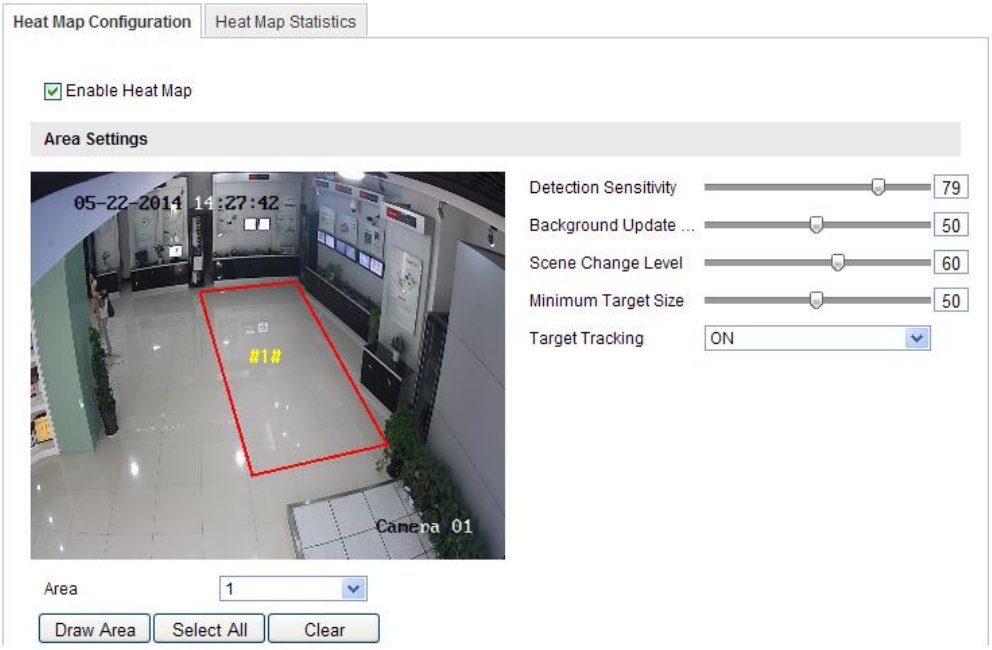
6.8.4. Mapa cieplna

Mapa cieplna (**Heat Map**) to graficzne przedstawienie zbioru danych za pomocą różnych kolorów. Funkcję mapy cieplnej w kamerze zwykle wykorzystuje się do przeanalizowania liczby odwiedzin i czasu przebywania klientów w skonfigurowanym obszarze detekcyjnym.

❖ **Zakładka Heat Map Configuration** — konfigurowanie mapy cieplnej

Procedura wykonania:

1. Wyświetl interfejs ustawień do skonfigurowania funkcji mapy cieplnej: **Configuration > Advanced Configuration > Heat Map**



Rys. 6–76: Interfejs ustawień do konfigurowania funkcji mapy cieplnej

2. Kliknij zakładkę **Heat Map Configuration**, aby wprowadzić szczegółowe parametry konfiguracyjne.
3. Zaznacz pole wyboru **Enable Heat Map**, aby załączyć w kamerze funkcję mapy cieplnej.
4. Kliknij przycisk **Draw Area**, aby na podglądzie kamery narysować obszar, który będzie zbierał „cieplne" dane statystyczne, przeznaczone do mapy cieplnej. Narysuj go kolejnymi kliknięciami lewego przycisku myszy w oknie z podglądem bieżącym kamery. Zakończ to rysowanie przez kliknięcie prawym przyciskiem myszy. Możesz skonfigurować maks. **8** takich obszarów.
   Uwaga: Możesz też kliknąć przycisk **Select All**, aby jako obszar skonfigurowany wybrać całą powierzchnię podglądu bieżącego. Ewentualnie możesz kliknąć przycisk **Delete**, aby skasować aktualnie narysowany obszar.
5. Ustaw parametry konfigurujące narysowany obszar.

Suwaki ekranowe:

Detection Sensitivity [**0~100**]: Ten parametr to czułość używana w kamerze do rozpoznawania celu. Nadmiernie wysoka czułość może prowadzić do mylnych wskazań / rozpoznań / dezinformacji. Zalecamy ustawienie tym suwakiem wartości domyślnej, tj. **50.**

Background Update Rate (tempo odświeżania tła**)** [**0~100**]: Parametr ten określa szybkość, z jaką nowa scena zastępuje scenę poprzednią, aby zapewnić prawidłowe zliczanie. Przykład: W obszarze przed regałem, osoby znajdujące się przy tym regale zostaną policzone aż dwa razy, jeśli towary są zdejmowane z regału, a kamera potraktuje regał (z którego zabrano towary) jako nową scenę. Zalecamy użycie domyślnej wartości: **50.**

Scene Change Level (poziom zmienności sceny) [**0~100**]**:** Parametr ten opisuje poziom reakcji kamery na zajścia w zmiennym otoczeniu, np. kołysanie się zasłony. Kamera mogłaby potraktować kołyszącą się / poruszoną zasłonę jako cel, ale ustawienie tego parametru na właściwą wartość pozwala zapobiec mylnym rozpoznaniom celu. Domyślnym poziomem jest: 50.

Minimum Target Size (minimalna wielkość celu) [**0~100**]: Parametr ten określa wielkość obiektu, który kamera potraktuje jako cel. Możesz ustawić tę wielkość zgodnie z rzeczywistymi warunkami monitorowanej sceny. Domyślną wielkością jest: 50.

Lista rozwijalna **Target Track** (śledzenie celu)**:** Wybierz z tej listy opcję załączenia (**ON**) bądź odłączenia (**OFF**) funkcji śledzenia celu.

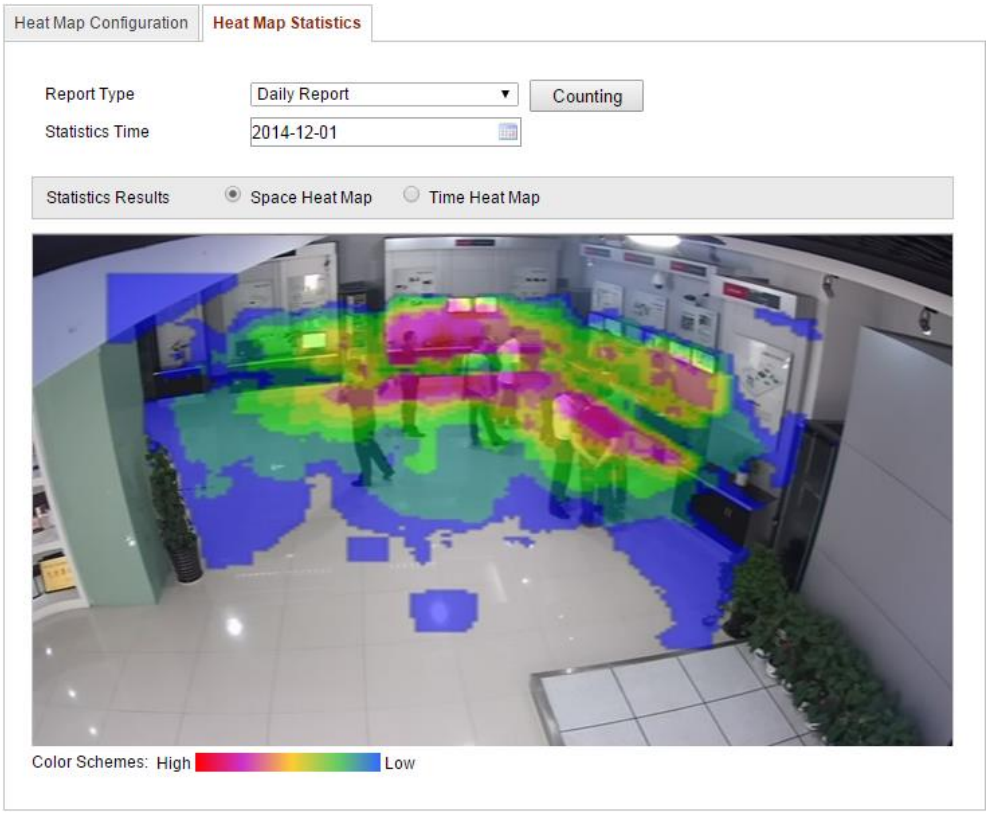
6. Kliknij przycisk **Edit**, aby skonfigurować harmonogram uzbrajania dla konfigurowanej tu funkcji mapy cieplnej.
7. Wybierz żądaną akcję powiązaną. W tym celu zaznacz pole wyboru przy akcji **Notify Surveillance Center** (powiadom centrum monitoringowe).
8. Kliknij przycisk **Save**, aby zachować wprowadzone ustawienia.

❖ **Zakładka Heat Map Statistics — dane statystyczne mapy cieplnej**

Procedura wykonania:

1. Kliknij przycisk **Heat Map Statistics**, aby wyświetlić interfejs analizy statystycznej dla zbioru danych do mapy cieplnej.
2. Z listy rozwijalnej **Report Type** wybierz żądany rodzaj raportu z danych — do wyboru są: **Daily Report** (dobowy), **Weekly Report** (tygodniowy), **Monthly Report** (miesięczny), **Annual Report** (całoroczny).
3. Kliknij przycisk **Counting**, aby obliczyć rozkład statystyczny w zbiorze danych.
4. Przyciskami wyboru opcji (**Statistics Result**) wybierz żądaną formę eksportu/prezentacji raportu: **Space Heat Map** (mapa cieplna dla rozkładu przestrzennego) lub **Time Heat Map** (mapa cieplna dla rozkładu cieplnego), a wtedy poniżej na tej karcie zostanie wyświetlona stosowna mapa cieplna.

Jeśli do wyświetlenia danych wybierzesz opcję prezentacji rozkładu czasowego (Time Heat Map), to w interfejsie pojawi się dodatkowo przycisk **Export** do wyeksportowania tych danych w formacie arkusza kalkulacyjnego Excel.



Rys. 6–77: Przykładowa mapa cieplna z rozkładem przestrzennym (Space Heat Map)

Uwagi:

- Na ilustracji powyżej: obszary mapy w kolorze czerwonym (255, 0, 0) wskazują miejsca najczęściej odwiedzane przez klientów, zaś obszary w kolorze niebieskim (0, 0, 255) wskazują miejsca najmniej popularne.
- Zalecamy, żeby nie regulować obiektywu elektronicznego po zainstalowaniu kamery, gdyż w przeciwnym wypadku dane zbierane przez funkcję mapy cieplnej mogą okazać się do pewnego stopnia niedokładne.

6.8.5. Zliczanie

Funkcja zliczania (Counting) pomaga wyznaczyć liczbę osób, które weszły lub wyszły do/z pewnego skonfigurowanego obszaru detekcyjnego i jest powszechnie stosowana w monitoringu wejść lub wyjść (na chronionym obiekcie).

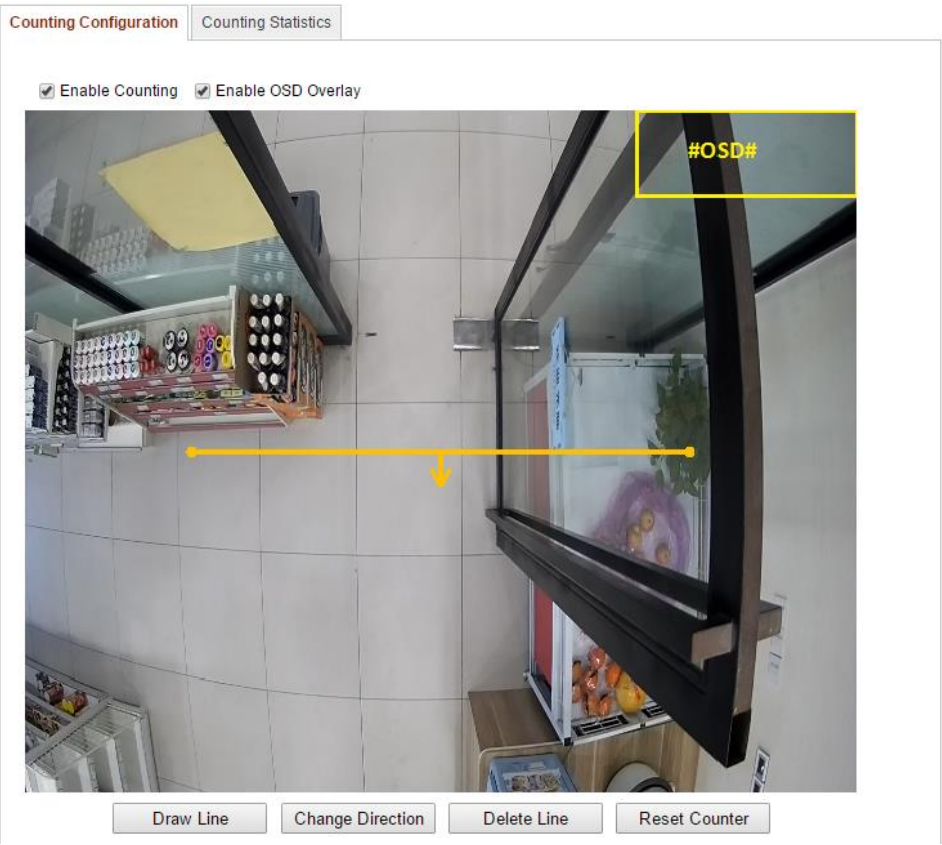
Uwagi:

Aby podnieść dokładność zliczania przez tę funkcję — zalecamy zamontować kamerę możliwe dokładnie nad samym monitorowanym wejściem/wyjściem; należy też upewnić się, że kamera jest poziomo.

❖ **Zakładka Counting Configuration** — konfiguracja funkcji zliczania

Procedura wykonania:

1. Wyświetl interfejs ekranowy, służący do konfigurowania funkcji zliczania: **Configuration > Advanced Configuration > Counting**
2. Kliknij w zakładkę **Counting Configuration**, aby na jej karcie skonfigurować parametry szczegółowe funkcji zliczania.



Rys. 6–78: Konfigurowanie funkcji zliczania (**Counting Configuration**)

3. Zaznacz pole wyboru **Enable Counting**, aby załączyć w kamerze tę funkcję.
4. (*Ewentualnie*): Zaznacz pole wyboru **Enable OSD Overlay** (załącz nakładanie danych na ekran), aby na podglądzie bieżącym kamery wyświetlała się liczba obiektów wchodzących i wychodzących, aktualizowana w czasie rzeczywistym.
5. Skonfiguruj linię detekcyjną dla realizacji zliczania:

   Na podglądzie bieżącym kamery możesz wprowadzić pomarańczową linię – zwaną linią detekcyjną – aby funkcja wykrywała i zliczała osoby wchodzące lub wychodzące przez tę linię (zob. ilustracja powyżej).

   1) Kliknij przycisk **Draw Line**, wtedy na obrazie pojawi się ww. pomarańczowa linia.

      Uwagi:

      - Linię detekcyjną musisz narysować na obrazie w punkcie, który jest położony dokładnie pod kamerą. Linia ta powinna być ponadto na tyle długa, żeby obejmowała cały obszar/prześwit wejścia/wyjścia.

- Linię detekcyjną narysuj w takim miejscu, w którym mało kto dłużej przestaje, ociągając się z wejściem/wyjściem.

2) Kliknij-i-przeciągnij linię detekcyjną po obrazie myszką, aby wybrać dla niej optymalne położenie w scenie.
3) Kliknij-i-pociągnij za któryś z dwóch końców narysowanej linii detekcyjnej (po jednym na raz), aby optymalnie wyregulować jej długość.
4) Aby ewentualnie usunąć aktualną linię detekcyjną, kliknij przycisk **Delete Line**.

6. Po wybraniu konfigurowanej linii detekcyjnej, pojawia się na niej strzałka wskazująca wykrywany kierunek ruchu osób tj. wchodzenie osób (Entering). Możesz teraz kliknąć przycisk **Change Direction**, aby przestawić kierunek strzałki na wykrywanie ruchu w drugą stronę, tj. wychodzenie osób (Leaving).
7. Kliknij przycisk **Reset Counter** (zeruj licznik), a wtedy licznik osób wchodzących (**Enter:**) oraz licznik osób wychodzących (**Leave:**) zostają przestawione na 0 (zero).
8. Kliknij przycisk **Edit**, aby skonfigurować harmonogram uzbrajania dla funkcji zliczania.
9. Zaznacz pole wyboru **Notify Surveillance Center** (wyślij powiadomienie do centrum monitoringowego), aby powiązać funkcję z tą akcją.
10. Kliknij przycisk **Save**, aby zachować wprowadzone ustawienia.

❖ **Zakładka Counting Statistics — opracowanie statystyczne zliczeń**

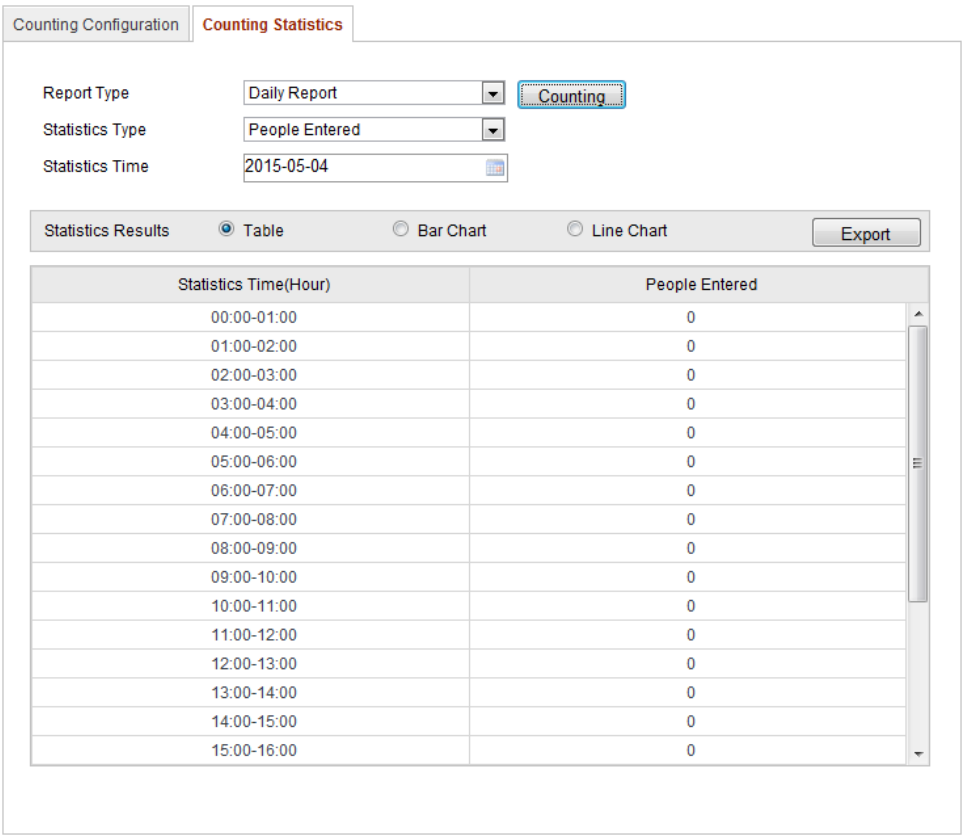
Procedura wykonania:

1. Kliknij zakładkę **People Counting Statistics**, aby wyświetlić na jej karcie interfejs, pozwalający zaprezentować zliczenia w raportach statystycznych.
2. Z listy rozwijalnej **Report Type** wybierz żądany rodzaj raportu z danych — do wyboru są: **Daily Report** (dobowy), **Weekly Report** (tygodniowy), **Monthly Report** (miesięczny), **Annual Report** (całoroczny).
3. Z listy rozwijalnej **Statistics Type** wybierz żądany przedmiot opracowania statystycznego w tym raporcie spośród dostępnych: **People Entered** (osoby wchodzące) bądź **People Exited** (osoby wychodzące).
4. Z listy rozwijalnej **Statistics Time** wybierz punkt czasu dla przygotowania raportu z odpowiedniego okresu.

   Uwaga: Raport typu dobowego (**Daily Report**) oblicza swoje dane dla dnia, który aktualnie wybrałeś. Raport tygodniowy oblicza je dla tygodnia, który obejmuje Twój dzień wybrany. Raport miesięczny oblicza je dla miesiąca, który obejmuje Twój dzień wybrany. A raport całoroczny oblicza je dla roku, który obejmuje Twój dzień wybrany.
5. Kliknij przycisk **Counting**, aby obliczyć i pokazać rozkład statystyczny zliczeń.

6. Przyciskami wyboru opcji (**Statistics Result**) wybierz żądaną formę eksportu/prezentacji raportu: **Table** (tabela), **Bar Chart** (wykres słupkowy), **Line Chart** (wykres liniowy).

   Uwaga: Jeśli do wyświetlenia danych wybierzesz tu opcję prezentacji stabelaryzowanej (**Table**), to w interfejsie pojawi się dodatkowo przycisk **Export**, który umożliwi Ci wyeksportowanie tych danych w formacie arkusza kalkulacyjnego Excel.



Rys. 6–79: Wyniki zliczeń osób w ujęciu statystycznym (postać stabelaryzowana – opcja **Table**)

Uwaga: Zalecamy nie regulować obiektywu elektronicznego po zainstalowaniu kamery, gdyż w przeciwnym wypadku dane zbierane przez tę funkcję mogą okazać się do pewnego stopnia niedokładne.

7. Ustawienia rejestrowania obrazu

Przygotuj na wstępie:

Aby skonfigurować ustawienia nagrywania/rejestracji obrazu, najpierw upewnij się, że w Twojej sieci teleinformatycznej (tj. sieci IT) masz zainstalowany sieciowy magazyn danych albo że w kamerze masz zainstalowaną kartę pamięci SD.

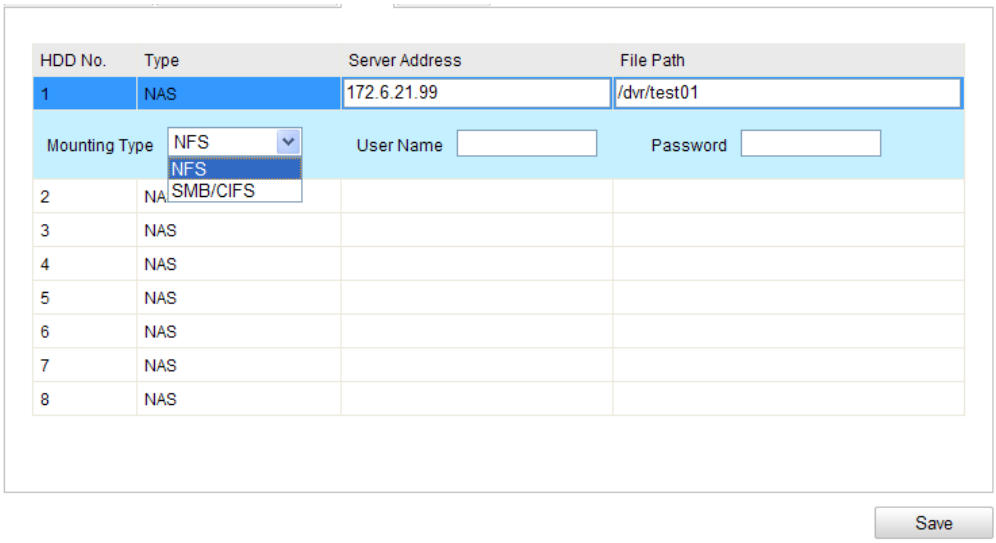
7.1. Konfigurowanie ustawień dysków sieciowych NAS

Przygotuj na wstępie:

Aby możliwe było zachowywanie w pamięci: nagranych plików monitoringowych, plików dziennikowych (tj. logów) oraz innych danych — musisz mieć, zainstalowany i dostępny z sieci, dysk sieciowy NAS.

Procedura wykonania:

1. Dodaj podłączony dysk sieciowy do systemu kamery.
   (1) Wyświetl interfejs z ustawieniami do konfigurowania magazynów NAS (*Network-Attached Storage*):
   Configuration > Advanced Configuration > Storage > NAS



Rys. 7–1: Dodanie dysku sieciowego do systemu kamery

(2) Do pola **Server Address** wprowadź adres IP żądanego dysku sieciowego, a do pola **File Path** wprowadź żądaną ścieżkę plików.

(3) Z listy rozwijalnej **Mounting Type** wybierz żądany sposób „zamontowania" dysku: **NFS** bądź **SMB/CIFS**. Jeśli wybierzesz montowanie **SMB/CIFS**, to możesz zdefiniować nazwę użytkownika (pole **User Name**) oraz jego hasło dostępowe (pole **Password**), aby zrealizować ochronę dostępów.

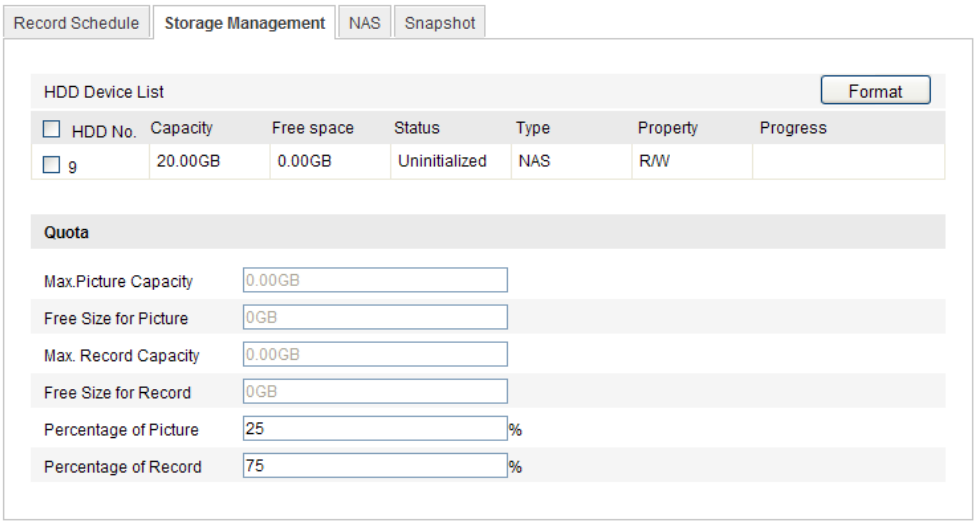
Uwaga: Opisu tworzenia ścieżki plików (**File Path**) należy szukać w *Instrukcji użytkownika do magazynów danych NAS* (ang. *User Manual of NAS*).

- *Dla ochrony Twojej własnej prywatności oraz dla lepszej ochrony Twojego systemu od źródeł zagrożeń sieciowych zdecydowanie zalecamy zastosowanie **silnych haseł** do wszystkich funkcji i urządzeń sieciowych. Hasło takie powinno być czymś, co samemu sobie wybierzesz, (powinno być w nim minimum 8 znaków, w tym co najmniej trzy z następujących kategorii znakowych: litery wielkie, litery małe, cyfry, znaki specjalne), aby podnieść poziom zabezpieczenia Twojego produktu (kamery).*
- *Odpowiedzialność za właściwe skonfigurowanie wszystkich haseł i innych nastaw zabezpieczających spoczywa na instalatorze oraz/lub użytkowniku ostatecznym (tj. konsumencie/odbiorcy) instalowanego rozwiązania.*

(4) Kliknij przycisk **Save**, aby dodać ten dysk sieciowy do systemu kamery.

2. Zainicjalizuj dodany dysk sieciowy.

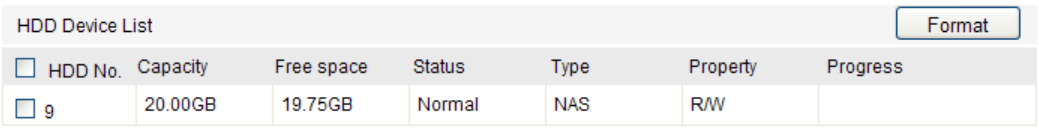
(1) Wyświetl interfejs z ustawieniami do konfigurowania HDD (**Advanced Configuration** > **Storage** > **Storage Management**), w którym możesz przejrzeć: pojemność HDD (**Capacity**), wolne miejsce na HDD (**Free space**), status eksploatacyjny HDD (**Status**), Typ HDD (**Type**) oraz flagę zapisu (**Property**).



Rys. 7–2: Interfejs do konfigurowania sieciowych magazynów danych (karta **Storage Management**)

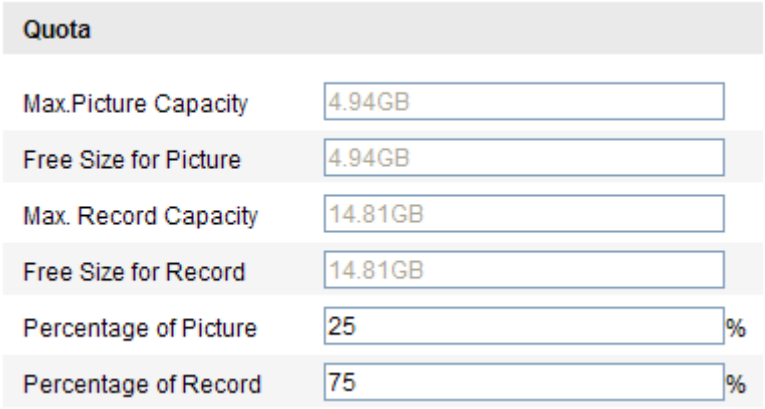
(2) Jeżeli w kolumnie **Status** Twojego dysku widzisz napis **Uninitialized** (niezainicjalizowany), to aby zainicjalizować ten dysk, zaznacz pole wyboru tego dysku, po czym kliknij przycisk **Format**, aby wejść w inicjalizowanie.

Po pełnym ukończeniu operacji inicjalizowania, wpis w polu **Status** tego dysku zmieni się z **Uninitialized** na **Normal**.



Rys. 7–3: Skontrolowanie statusu eksploatacyjnego dysku (kolumna **Status**)

3. Wprowadź miejsce na dysku przydzielane na wideo-nagrania i fotozrzuty monitoringowe.
   (1) Wprowadź procent miejsca dla fotozrzutów (pole **Percentage of Picture**) oraz procent miejsca dla wideo-nagrań (pole **Percentage of Record**).
   (2) Kliknij przycisk **Save** i odśwież tę wyświetlaną stronę w przeglądarce, aby uaktywnić wprowadzone ustawienia.



Rys. 7–4: Ustawienia do skonfigurowania podziału miejsca na dysku NAS (**Quota**)

Uwagi:

- Do kamery możesz podłączyć przez sieć maks. **8** dysków sieciowych NAS.
- Aby zainicjalizować i móc wykorzystywać kartę pamięci SD, włóż ją najpierw do kamery i postępuj, jak podane wyżej w procedurze inicjalizowania dysków NAS.

7.2. Konfigurowanie harmonogramu nagrywania

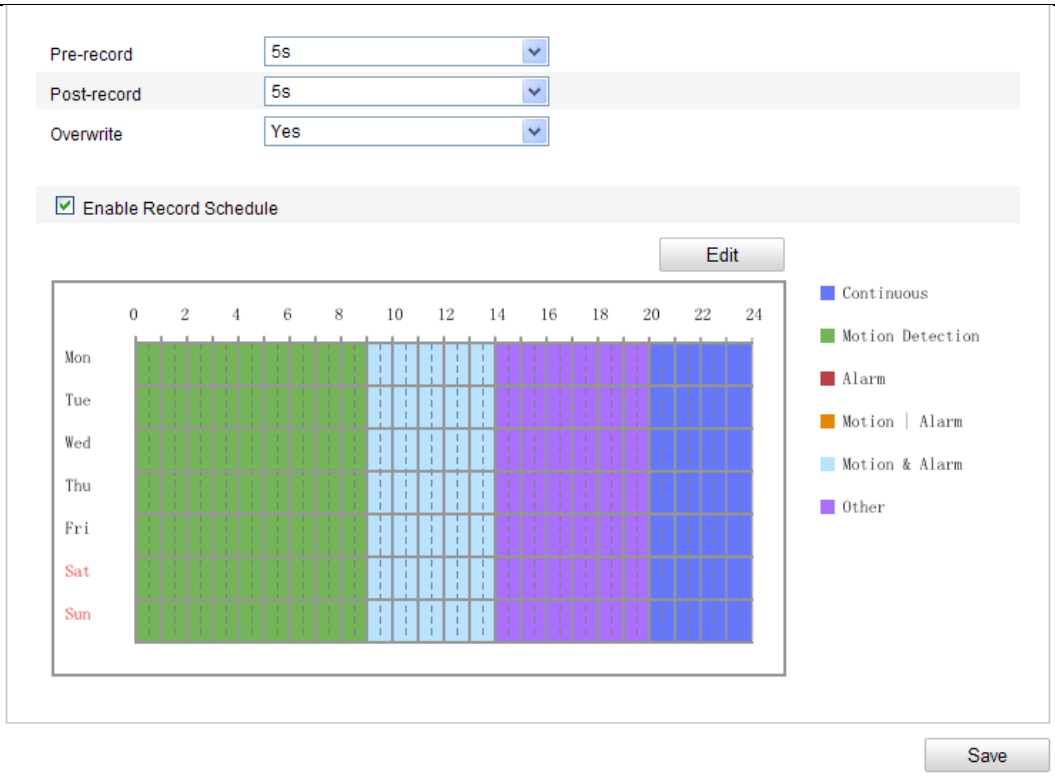
Cel czynności:

Dla opisywanych tu kamer istnieją 2 rodzaje rejestrowania: rejestrowanie ręczne i rejestrowanie harmonogramowane. [Opis rejestrowania ręcznego znajdziesz w *podrozdz. 5.3* ***Ręczne nagrywanie ciągłe | ręczny fotozrzut*** klatek (str. 37).]

W niniejszym podrozdziale podajemy procedurę konfigurującą rejestrowanie czasowe wg harmonogramu. W ustawieniu domyślnym, pliki wideonagrań z rejestracji harmonogramowanych zostają zapisane na: karcie pamięci SD obecnej w kamerze (o ile ta dysponuje obsługą kart SD) lub na dodanym dysku sieciowym.

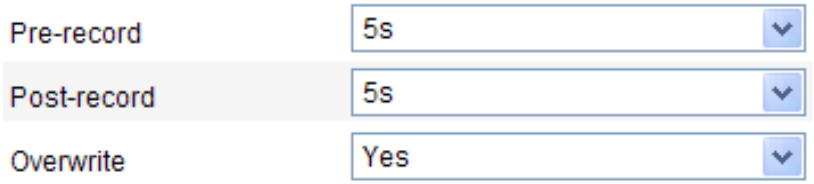
Procedura wykonania:

1. Wyświetl interfejs z ustawieniami do konfigurowania rejestrowania czasowego wg harmonogramu:
   Configuration > Advanced Configuration > Storage > Record Schedule



Rys. 7–5: Interfejs z ustawieniami do skonfigurowania harmonogramu nagrywania (**Record Schedule**)

2. Zaznacz pole wyboru **Enable Record Schedule**, aby załączyć w kamerze funkcję rejestrowania harmonogramowanego.
3. Wybierz wartości dla parametrów rejestrowania w kamerze:



Rys. 7–6: Zespół parametrów konfigurujących rejestrowanie w kamerze

- **Pre-record**: To czas pre-rejestracji, który ustawiasz, żeby podać, na ile wcześniej przed [czasem naznaczonym w harmonogramie] lub przed [zdarzeniem alarmowym] kamera ma zacząć rejestrowanie go. Przykład: Jeśli alarm wyzwolił rejestrowanie o godzinie 10:00, a czas **Pre-record** masz ustawiony na **5s** (5 sekund), to kamera rozpocznie nagrywanie obrazu już o 9:59:55.

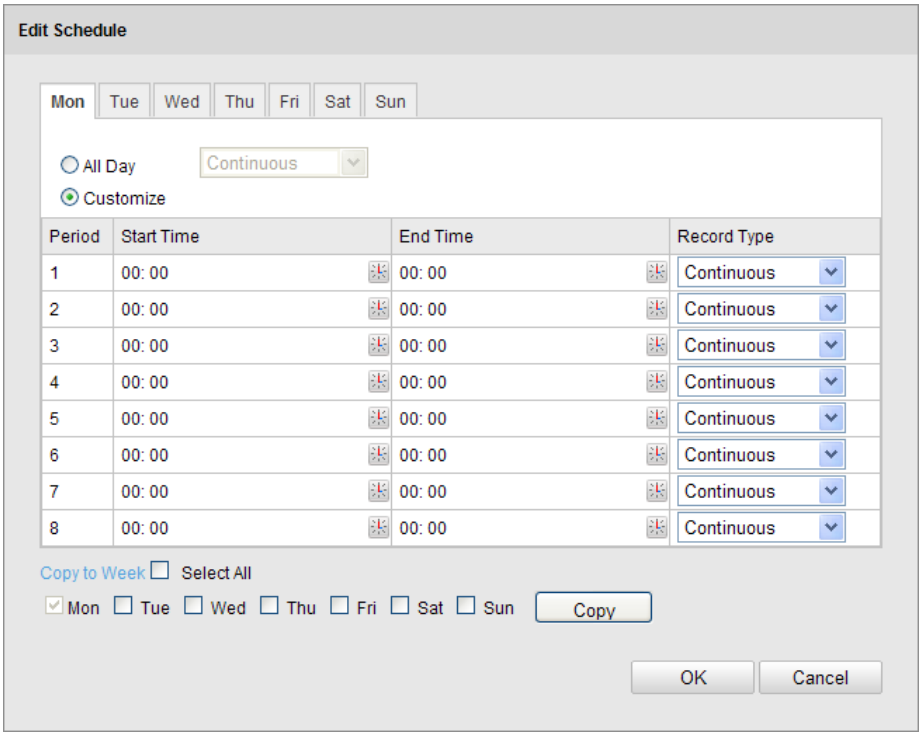
  Dla czasu pre-rejestracji możesz z tej listy rozwijalnej wybrać następujące opcje: **No Pre-record** (brak pre-rejestracji) **5s**, **10s**, **15s**, **20s**, **25s**, **30s** lub **Not Limited** (czas nieograniczony).
- **Post-record**: To czas post-rejestracji, który ustawiasz, żeby podać, z jak dużym opóźnieniem po [czasie wyznaczonym wg harmonogramu] lub po [zdarzeniu alarmowym] kamera ma zakończyć rejestrowanie go. Przykład: jeśli rejestracja wyzwolona alarmem kończy się o 11:00, a czas **Post-record** masz

ustawiony na **5s**, to kamera będzie kontynuowała nagrywanie obrazu aż do 11:00:05.

Dla czasu post-rejestracji możesz z tej listy rozwijalnej wybrać następujące opcje: **5s**, **10s**, **30s**, **1min**, **2min**, **5min** lub **10min**.

Uwaga: Zestaw dostępnych parametrów rejestrowania zależy od konkretnego modelu kamery.

4. Kliknij przycisk **Edit**, aby wyedytować harmonogram nagrywania:



Rys. 7–7: Harmonogram rejestrowania obrazu kamery — dostępne ustawienia konfiguracyjne (**Edit Schedule**)

5. Klikając odnośną zakładkę (**Mon–Sun**), wybierz dzień, dla którego zamierzasz skonfigurować rejestrowanie harmonogramowane.

   (1)Wybierz dla nagrywania w tym dniu opcję: **All-day** (całodobowe) lub **Customize** (segmentowe, wg własnej definicji):

   ♦ Aby uzyskać nagrywanie trwające ciągle przez całą dobę, zaznacz pole wyboru **All Day**.

   ♦ Aby uzyskać nagrywanie odbywające się tylko w pewnych wybranych okresach dnia, zaznacz pole wyboru **Customize** i wprowadź w wierszu każdego żądanego okresu (**Period**): czas rozpoczęcia okresu (kolumna **Start Time**) i czas zakończeniu okresu (kolumna **End Time**).

   Uwaga: Pamiętaj, że definiowane okresy nie mogą się wzajemnie nakładać. Ponadto, można skonfigurować maks. **4** okresy rejestracyjne.

   (2)Z odnośnej listy rozwijalnej **Record Type**[22] wybierz żądany sposób rejestracji, spośród dostępnych opcji: **Continuous**, **Motion Detection**, **Alarm**, **Motion |**

[22] Do rejestracji całodobowych odnosi się lista rozwijalna u samej góry interfejsu (tuż pod zakładkami dni tygodnia), a do okresów rejestracyjnych w obrębie danego dnia odnoszą się listy rozwijalne w kolumnie **Record Type**. — przyp. tłum.

Alarm, **Motion&Alarm**, **PIR Alarm**, **Wireless Alarm**, **Emergency Alarm** lub **Motion | Alarm Input | PIR | Wireless | Emergency**.

♦ **Nagrywanie ciągłe — opcja Continuous**

Jeśli wybierzesz opcję **Continuous**, to obraz kamery zacznie być nagrywany automatycznie zgodnie z czasem wyznaczonym w tym harmonogramie.

♦ **Nagrywanie wyzwalane przez wykrycie ruchu — opcja Motion Detection**

Jeśli wybierzesz opcję **Motion Detection**, to obraz kamery zacznie być nagrywany od chwili, gdy kamera wykryje ruch w obrazie.

W tej opcji, oprócz skonfigurowania harmonogramu rejestracyjnego kamery, musisz jeszcze narysować/zdefiniować obszar detekcji ruchu. Ponadto, w interfejsie ustawień wykrywania ruchu (grupa ustawień **Linkage Method**) musisz zaznaczyć pole wyboru akcji alarmowej **Trigger Channel**. Dokładny opis wprowadzania wymaganych ustawień — znajdziesz w *Kroku 1* w *podrozdz. 6.6.1* ***Konfigurowanie wykrywania ruchu***, str. 81.

♦ **Nagrywanie wyzwalane przez zewn. sygnał alarmowy — opcja Alarm**

Jeśli wybierzesz opcję **Alarm**, to obraz kamery zacznie być nagrywany od chwili, gdy wystąpi alarm inicjowany przez nadejście do kamery sygnału via zewnętrzny kanał sygnałów alarmowych.

W tej opcji, oprócz skonfigurowania harmonogramu rejestracyjnego kamery, musisz jeszcze ustawić rodzaj alarmu (**Alarm Type**). Ponadto – w interfejsie ustawień wejść alarmowych (**Alarm Input**) – musisz zaznaczyć pole wyboru opcji **Trigger Channel** w grupie **Linkage Method**. Dokładny opis wymaganych ustawień — znajdziesz w podrozdziale *6.6.3*, str. 89.

♦ **Nagrywanie wyzwalane przez ruch i alarm — opcja Motion & Alarm**

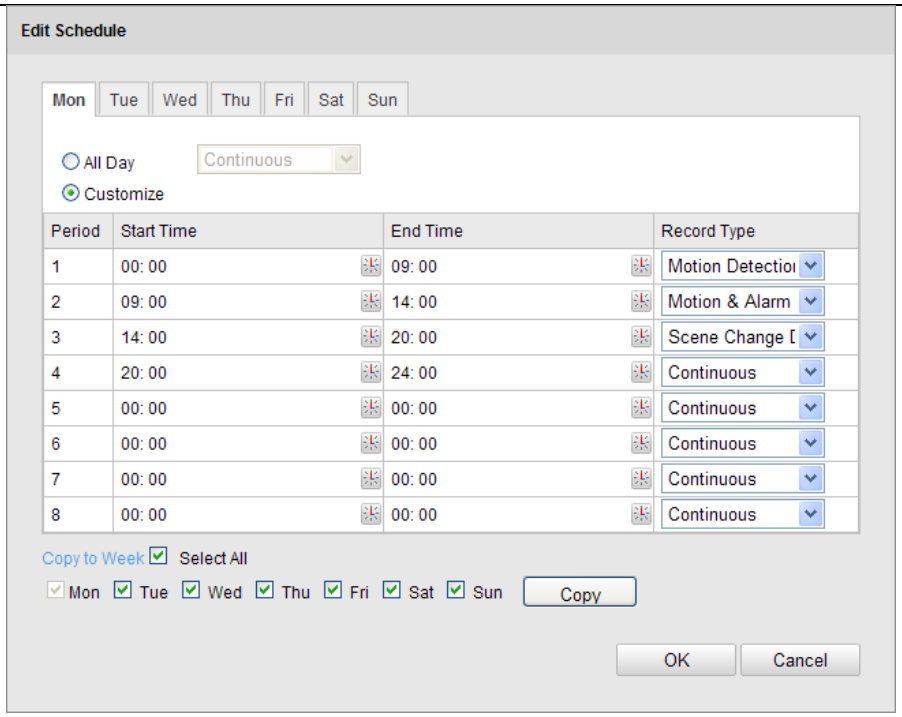
Jeśli wybierzesz opcję **Motion & Alarm**, to obraz kamery zacznie być nagrywany od chwili, gdy – jednocześnie – zostanie wykryty ruch i wyzwolony alarm.

W tej opcji, oprócz skonfigurowania harmonogramu rejestracyjnego kamery, musisz jeszcze skonfigurować ustawienia w interfejsie konfiguracyjnym wykrywania ruchu (**Motion Detection**) i interfejsie konfiguracyjnym wejść alarmowych (**Alarm Input**). Dokładny opis wymaganych ustawień — znajdziesz w podrozdz.: *6.6.1* (str. 81) i *6.6.3* (str. 89).

♦ **Nagrywanie wyzwalane przez ruch | alarm — opcja Motion | Alarm**

Jeśli wybierzesz opcję **Motion | Alarm**, to obraz kamery zacznie być nagrywany od chwili, gdy zostanie wykryty ruch *lub* wyzwolony alarm.

W tej opcji, oprócz skonfigurowania harmonogramu rejestracyjnego kamery, musisz jeszcze skonfigurować ustawienia w interfejsie konfiguracyjnym wykrywania ruchu (**Motion Detection**) i interfejsie konfiguracyjnym wejść alarmowych (**Alarm Input**). Dokładny opis wymaganych ustawień — znajdziesz w podrozdz.: *6.6.1* (str. 81) i *6.6.3* (str. 89).



Rys. 7–8: Harmonogram rejestrowania z częściowo skonfigurowanymi ustawieniami

(3)Zaznacz pole wyboru **Select All** (obok etykiety **Copy to Week**) i kliknij przycisk **Copy**, aby przekopiować ustawienia z tego dnia do wszystkich pozostałych dni tygodnia. Jeśli potrzebujesz skopiować je tylko do wybranych dni, to możesz zaznaczyć pola wyboru tych docelowych dni i kliknąć przycisk **Copy**.

(4)Kliknij przycisk **OK.**, aby zachować wprowadzone ustawienia i wyjść z interfejsu edycji harmonogramu rejestracyjnego **Edit Schedule**.

6. Kliknij przycisk **Save**, aby zachować wprowadzone ustawienia.

7.3. Konfigurowanie fotozrzutów z obrazu kamery

Cel czynności:

W kamerze możesz skonfigurować fotozrzuty sterowane czasem oraz fotozrzuty wyzwalane przez zdarzenia, a zarejestrowane klatki obrazu mogą być zapisywane na karcie SD (o ile kamera ją obsługuje) lub na sieciowym HDD. (Dokładniej o sieciowych HDD — zob. *podrozdz. 7.1* ***Konfigurowanie ustawień dysków sieciowych NAS***, str. 130.) Ponadto, kamera może też przesłać zarejestrowaną klatkę obrazu przez sieć na odpowiednio skonfigurowany serwer FTP (upload).

♦ **Ustawienia podstawowe**

Procedura wykonania:

1. Wyświetl ekranowy interfejs ustawień do konfigurowania fotozrzutów:
   Configuration > Advanced Configuration > Storage > Snapshot

2. Zaznacz pole wyboru **Enable Timing Snapshot**, aby załączyć funkcję ciągłego fotozrzutu poklatkowego.[23] Zaznacz pole wyboru **Enable Event-triggered Snapshot**, aby załączyć funkcję fotozrzutu zdarzeniowego.[24]
3. Z list rozwijalnych (**Format**, **Resolution**, **Quality**) wybierz parametry, określające żądaną jakość fotozrzutu.
4. Z listy rozwijalnej **Interval** wybierz odstęp ciągłej serii poklatkowej pomiędzy dwoma kolejnymi fotozrzutami.
5. Kliknij przycisk **Save**, aby zachować wprowadzone ustawienia.

Wysyłanie na serwer FTP

Aby wysyłać pliki fotozrzutów na serwer FTP, wykonaj kroki poniższej procedury.

- Wysyłaj pliki ciągłego fotozrzutu poklatkowego na serwer FTP

Procedura wykonania:

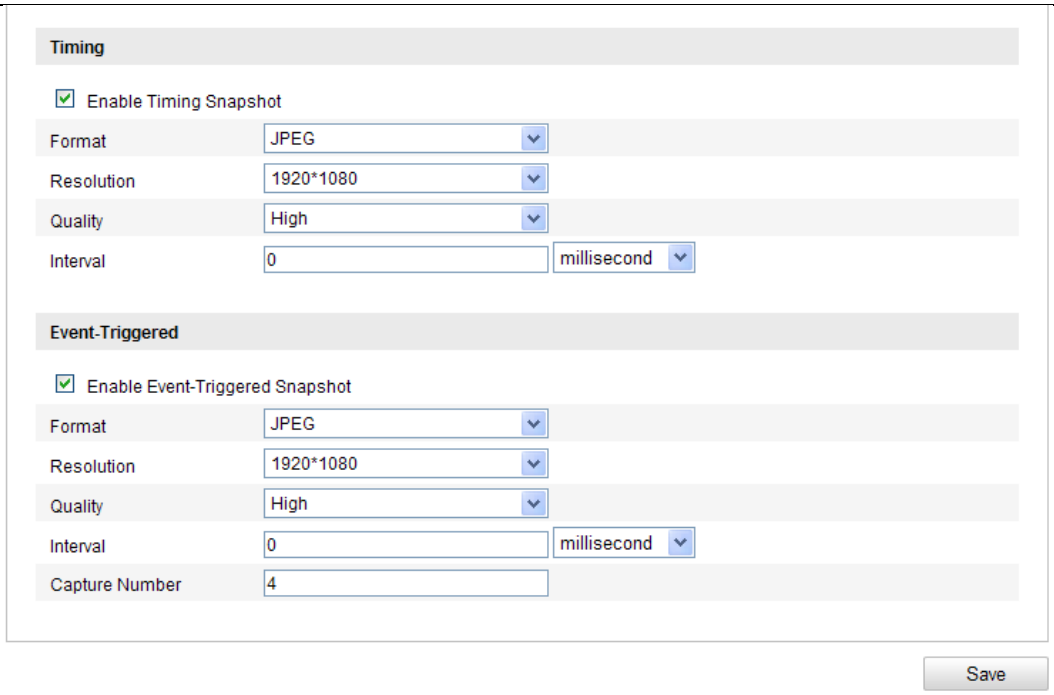
1) Skonfiguruj ustawienia serwera FTP i zaznacz pole wyboru **Upload Picture** w interfejsie ustawień FTP — zob. dokładniejszy opis tych ustawień w *podrozdz. 6.3.12* ***Konfigurowanie ustawień protokołu FTP***, str. 60.
2) Zaznacz pole wyboru **Enable Timing Snapshot**.

- Wysyłaj pliki fotozrzutu zdarzeniowego na serwer FTP

Procedura wykonania:

1) Skonfiguruj ustawienia serwera FTP i zaznacz pole wyboru **Upload Picture** w interfejsie ustawień FTP — zob. dokładniejszy opis tych ustawień w *podrozdz. 6.3.12* ***Konfigurowanie ustawień protokołu FTP***, str. 60.
2) Zaznacz pole wyboru akcji **Upload Picture** w interfejsie ustawień wykrywania ruchu (**Motion Detection**) lub w interfejsie ustawień wejść alarmowych (**Alarm Input**). Dokładniejszy opis tych ustawień — zob. *Krok 3):* ***Skonfiguruj akcje alarmowe powiązane z funkcją wykrywania ruchu*** (*podrozdz. 6.6.1*, str. 84) albo też *Krok 4)* w ***Konfigurowanie wejść alarmowych*** (*podrozdz. 6.6.3*, str. 89).
3) Zaznacz pole wyboru **Enable Event-triggered Snapshot**.

[23] (zapis klatek obrazu, zachodzący ciągle, w stałym tempie, określonym przez użytkownika w parametrze **Interval**) — przyp. tłum.
[24] (zapis klatek wyzwalany przez wystąpienie zdarzenia alarmowego) — przyp. tłum.



Rys. 7–9: Ustawienia do konfigurowania fotozrzutu klatek z wideo kamery

7.4. Konfigurowanie funkcji oszczędnego zapisu

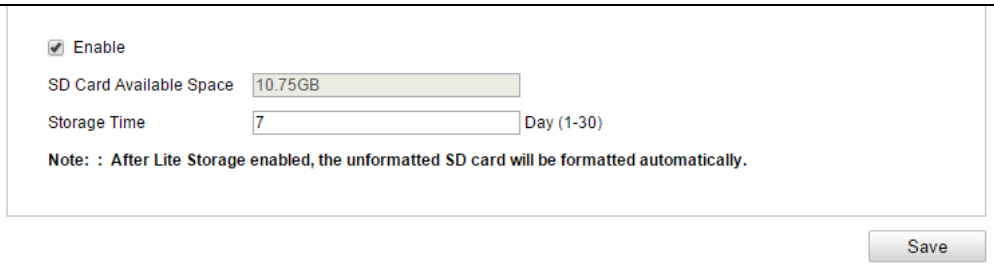
Cel czynności:

W przypadkach, gdy w obrazie monitorowanej sceny nie ma poruszających się obiektów, kamera może obniżać szybkość rejestracji obrazu i szybkość transmisji strumienia obrazu, aby w ten sposób wydłużyć maksymalny okres rejestracji dostępny (do zrealizowania) na karcie SD w kamerze.

Uwagi:

- Funkcja oszczędnego zapisu (*Lite Storage*) jest różna w różnych modelach kamery.
- Pliki wideo nagrane w trybie Lite Storage będą odtwarzane z pełną szybkością poklatkową (25 kl/s lub 30 kl/s), stąd obraz podczas odtwarzania będzie się wydawał szybszy niż normalnie.

1. Wyświetl interfejs do konfiguracji funkcji *Lite Storage*:
   Configuration > Advanced Configuration > Storage > Lite Storage.
2. Zaznacz pole wyboru **Enable**, aby załączyć w kamerze funkcję *Lite Storage*.
3. W polu **Storage Time** wpisz potrzebny okres rejestracji. Miejsce dostępne dla rejestracji na karcie SD możesz skontrolować w polu **SD Card Available Space**.
4. Kliknij przycisk **Save**, aby zachować wprowadzone ustawienia.



Rys. 7–10: Ustawienia do skonfigurowania fotozrzutu klatek z wideo kamery
(**Uwaga: gdy załączysz funkcję Lite Storage, niesformatowana karta SD kamery zostanie automatycznie w niej sformatowana.**)

7.5. Konfigurowanie magazynowania danych w chmurze

Cel czynności:

Klatki pobierane z obrazu kamery mogą być zapisywane na rejestratorze sieciowym (NVR), ustawionym na pracę w trybie chmury (*cloud storage*).

Uwaga: Funkcja magazynowania danych w chmurze sieciowej jest różna w różnych modelach kamery.

Przygotuj na wstępie:

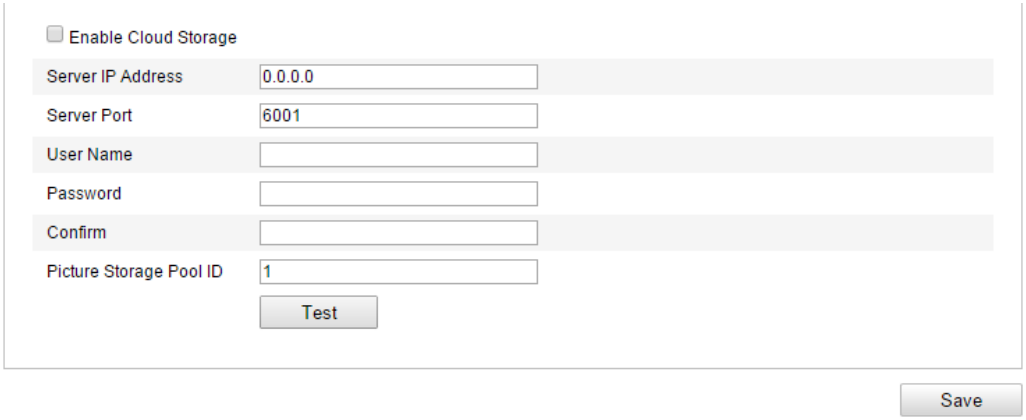
Upewnij się, że wykorzystywany rejestrator NVR został przełączony w tryb pracy w chmurze sieciowej — zob. opis w *Instrukcji użytkownika* od tego NVR.

Procedura wykonania:

1. Wyświetl interfejs ustawień funkcji magazynowania chmurowego:
   Configuration > Advanced Configuration > Storage > Cloud Storage
2. Zaznacz pole wyboru **Enable Cloud Storage**, aby załączyć w kamerze funkcję magazynu chmurowego.
3. Do pola **Server IP Address** wprowadź adres IP serwera pamięci, a do pola **Server Port** — jego port.
4. Aby zapewnić uwierzytelnianie dostępów do tego serwera pamięci — wprowadź dostępowe: nazwę użytkownika (**User Name**), hasło użytkownika (**Password**) i potwierdź wprowadzone hasło w polu **Confirm**.

- *Dla ochrony Twojej własnej prywatności oraz dla lepszej ochrony Twojego systemu od źródeł zagrożeń sieciowych zdecydowanie zalecamy zastosowanie **silnych haseł** do wszystkich funkcji i urządzeń sieciowych. Hasło takie powinno być czymś, co samemu sobie wybierzesz, (powinno być w nim minimum 8 znaków, w tym co najmniej trzy z następujących kategorii znakowych: litery wielkie, litery małe, cyfry, znaki specjalne), aby podnieść poziom zabezpieczenia Twojego produktu (kamery).*
- *Odpowiedzialność za właściwe skonfigurowanie wszystkich haseł i innych nastaw zabezpieczających spoczywa na instalatorze oraz/lub użytkowniku ostatecznym (tj. konsumencie/odbiorcy) instalowanego rozwiązania.*

5. W polu **Picture Storage Pool ID** wpisz ID (numer) żądanej Grupy magazynującej pliki graficzne na tym serwerze.
6. (*Ewentualnie*): Jeśli potrzeba, kliknij przycisk **Test**, żeby przetestować poprawność ustawień wprowadzonych dla funkcji magazynowania danych w chmurze (*cloud storage*).
7. Kliknij przycisk **Save**, aby zachować wprowadzone ustawienia.



Rys. 7–11: Ustawienia do skonfigurowania funkcji magazynowania danych w chmurze (**Cloud Storage**)

8. Monitorowanie ruchu drogowego

Cel czynności:

Na potrzeby monitoringu ruchu drogowego dostępne 2 rodzaje detekcji: wykrywanie pojazdów oraz wykrywanie uczestników ruchu mieszanego.

Podczas WYKRYWANIA POJAZDÓW kamera potrafi wykryć przejeżdżający pojazd oraz może zapisać klatkę obrazu, zawierającą jego tablicę rejestracyjną. Oprócz tego automatycznie mogą zostać rozpoznane: kolor karoserii i logo tego pojazdu, a także inne jego cechy charakterystyczne.

Podczas WYKRYWANIA UCZESTNIKÓW RUCHU MIESZANEGO kamera potrafi wykrywać: pieszych, pojazdy silnikowe, pojazdy bezsilnikowe i może zapisać klatkę obrazu, utrwalającą te obiekty w całości (dotyczy: pieszych / poj. bezsilnikowych / poj. silnikowych bez tablicy rejestracyjnej) albo klatkę obrazu, zawierającą tablicę rejestracyjną pojazdu (dotyczy: p. silnikowych wyposażonych w tablicę rejestracyjną).

Można też skonfigurować, żeby w razie wykrycia kamera wysłała: powiadamiający sygnał alarmowy do centrum monitoringu oraz archiwalną klatkę obrazu przez upload na serwer FTP.

Uwaga: Zakres/dostępność funkcji monitorowania ruchu drogowego jest różna w różnych modelach kamer.

Procedura wykonania:

❖ **Konfigurowanie ustawień wykrywania — Detection Settings**

1. Z listy **Detection Type** wybierz żądany tryb wykrywania — spośród dostępnych: **Vehicle Detection** i **Mixed-traffic Detection**.

   Uwaga: Zmieniając tryb wykrywania (**Detection Type**) na inny, pamiętaj, żeby przeładować system kamery (reboot), aby nowe ustawienia mogły zacząć działać.
2. Zaznacz pole wyboru **Enable**, aby załączyć wybrany tryb wykrywania.
3. Z listy **Total Number of Lanes** wybierz liczbę pasów ruchu w monitorowanej trasie. Funkcja obsługuje maks. **4** pasy drogowe.
4. Kliknij-i-przeciągnij linię detekcyjną żądanego pasa (**Lane line x**) na żądane miejsce w scenie. *Albo też:* kliknij-i-pociągnij za zakończenie tej linii, aby dobrać jej żądaną długość i kąt nachylenia.
5. Wyreguluj wielkość zbliżenia (tj. zoom) w kamerze do takiego poziomu, żeby wielkość pojazdów rozpoznawanych w scenie była bliska wielkości czerwonej ramki na obrazie. Tylko położenie tej czerwonej ramki daje się zmieniać.[25]

Uwaga: Kamera potrafi na raz rejestrować tylko po 1 tablicy rejestracyjnej na każdym monitorowanym pasie drogi.

[25] (tzn. nie można wyregulować wielkości tej czerwonej ramki.) — przyp. tłum.

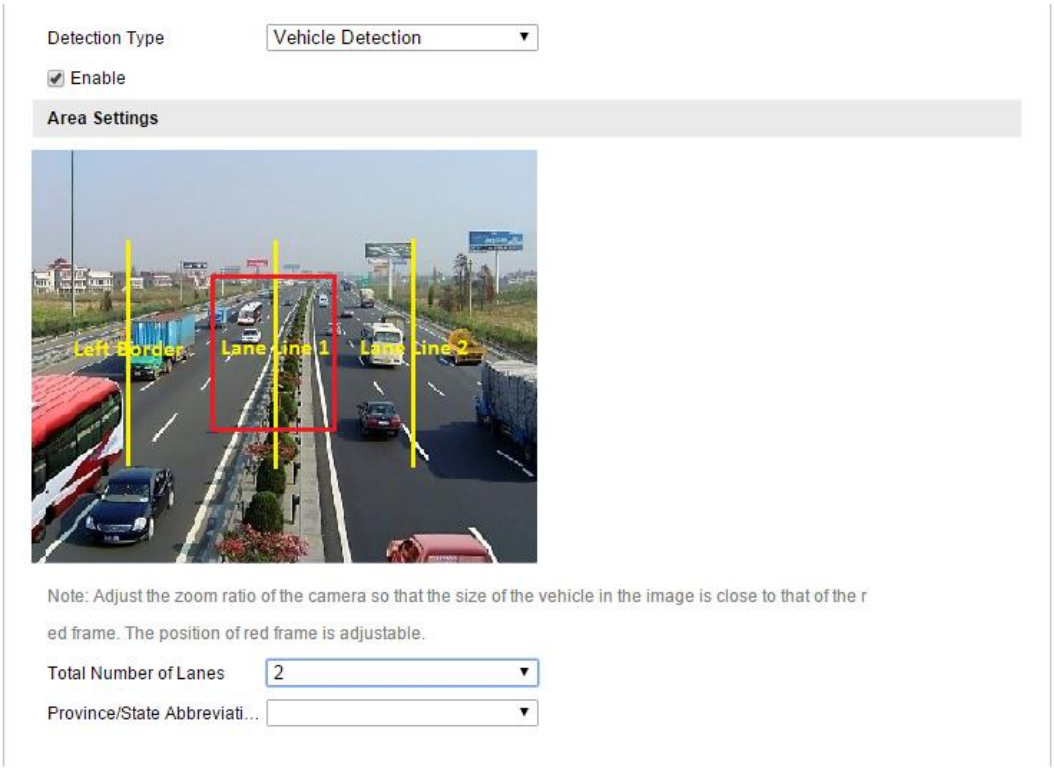
6. Z listy rozwijalnej **Province/State Abbreviati...** wybierz żądany skrót/kod regionu/okręgu/stanu na wypadek, gdyby nie udawało się rozpoznać pochodzenia pojazdu.
7. Skonfiguruj harmonogram uzbrajania dla funkcji wykrywania pojazdów.
   1) Aby wejść w edycję harmonogramu uzbrajania, kliknij przycisk **Edit**.
   2) Wybierz dzień, dla którego chcesz określić uzbrajanie tej funkcji.
   3) Kliknij przycisk , aby zdefiniować okres uzbrajania.
   4) (*Ewentualnie*): Po skonfigurowaniu harmonogramu uzbrajania możesz kliknąć przycisk **Copy**, aby przekopiować ustawienia tego dnia na inne dni harmonogramu.
   5) Kliknij przycisk **OK**, aby zachować wprowadzone ustawienia.

   Uwaga: Przedział czasu jednego okresu nie może nakładać się z przedziałem czasu jakiegokolwiek innego okresu.
8. Zaznacz żądane pola wyboru od odnośnych akcji alarmowych, aby powiązać te akcje ze zdarzeniem wykrycia pojazdu. Do wyboru dostępne są akcje: **Notify Surveillance Center** (wyślij powiadomienie do centrum monitoringu) oraz **Upload to FTP** (wyślij obrazek/ki na serwer FTP).

   Notify Surveillance Center: W chwili, gdy zostanie wykryty pojazd, do zdalnego oprogramowania zarządzającego zostanie wysłany sygnał wyjątku lub sygnał alarmowy.

   Upload to FTP: Gdy zostanie wyzwolony alarm wykrycia, zostanie zarejestrowana klatka z podglądu kamery i wysłana przez sieć na serwer FTP. Ponadto, klatka ta zostanie zapisana na lokalnej karcie SD[26] lub na podłączonym dysku sieciowym NAS.
9. Kliknij przycisk **Save**, aby zachować wprowadzone ustawienia.

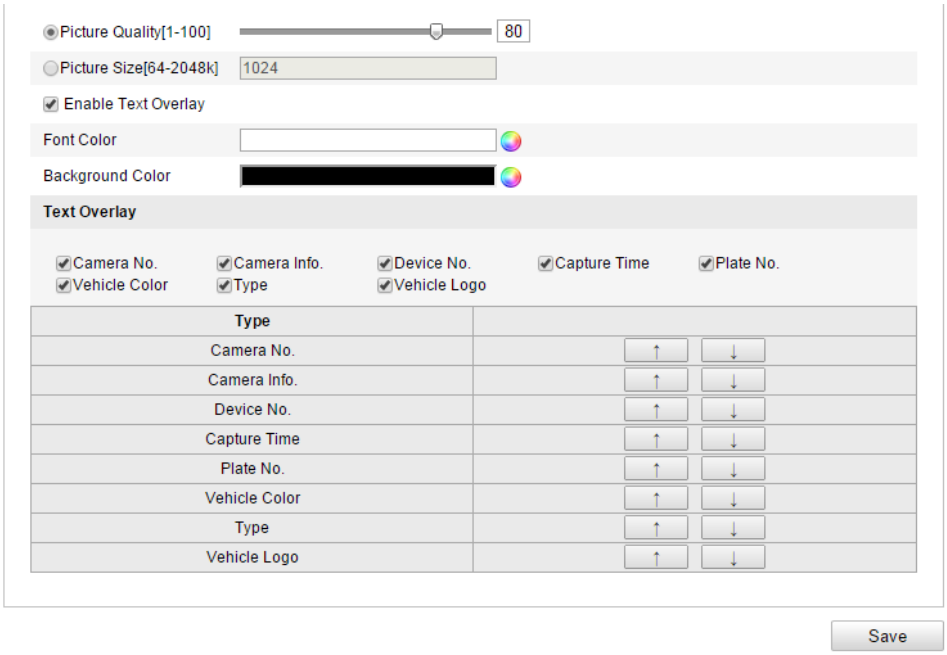
[26] (tj. karcie w kamerze) — przyp. tłum.



Rys. 8–1: Ustawienia do konfigurowania funkcji wykrywania pojazdów w ruchu drogowym (tryb **Vehicle Detection**)

❖ **Konfigurowanie wysyłania klatki na serwer — Upload Picture**

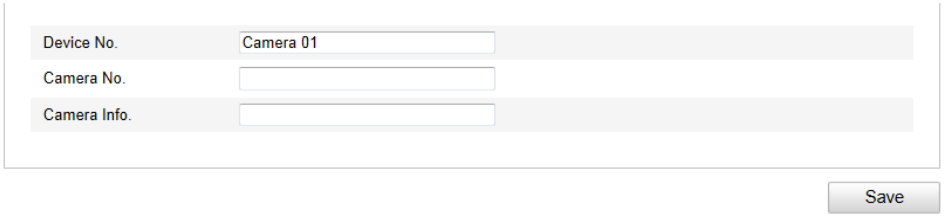
1. Suwakiem ekranowym **Picture Quality** ustaw żądaną jakość obrazu.
   Jakość obrazu możesz wyspecyfikować tylko zamiennie: albo suwakiem **Picture Quality** albo wartością wpisaną w polu **Picture Size**.
2. (*Ewentualnie*): Zaznaczając pole wyboru **Enable Text Overlay** załącz funkcję nakładania danych na wysyłaną klatkę obrazu, po czym zaznaczając odnośne pola wyboru (zob. krok **3** poniżej) zgłoś elementy danych wstawiane w tej nakładce.
   Dla nakładki możesz także wybrać kolor czcionki (**Font Color**) i kolor tła (**Background Color**) — kliknij w tym celu przycisk i z otwartej w ten sposób, podręcznej palety kolorów wybierz żądane kolory.
3. Zaznacz pola wyboru w grupie **Text Overlay**, aby wybrać żądane elementy danych wstawiane do nakładki — a w tym: **Camera No.** (nr kamery), **Camera Info** (dane kamery), **Device No.** (nr urządzenia), **Capture Time** (czas pozyskania klatki), **Plate No.** (numery na tablicy rejestracyjnej), **Vehicle Color** (kolor pojazdu) i inne. Kliknij przycisk ze strzałką (w dół / w górę), aby zmienić pozycję danego elementu danych w uszeregowaniu tych elementów dla nakładki.
4. Kliknij przycisk **Save**, aby uaktywnić wprowadzone ustawienia.



Rys. 8–2: Ustawienia do konfigurowania obrazków wysyłanych na serwer (**Upload Picture**)

❖ **Konfigurowanie treści elementów w nakładce — Overlay Content**

1. Wprowadź/zmień treść następujących elementów przeznaczonych do nakładki: nr kamery (pole **Camera No.**), dane kamery (pole **Camera Info**), nr urządzenia (pole **Device No.**).
2. (*Ewentualnie*): Załącz i wyedytuj inny zestaw elementów, które mają być wstawione do nakładki na klatkę wysyłaną na serwer FTP.
3. Kliknij przycisk **Save**, aby uaktywnić wprowadzone ustawienia.



Rys. 8–3: Ustawienia do konfigurowania treści tekstowej niektórych elementów wstawianych do nakładki (**Overlay Content**)

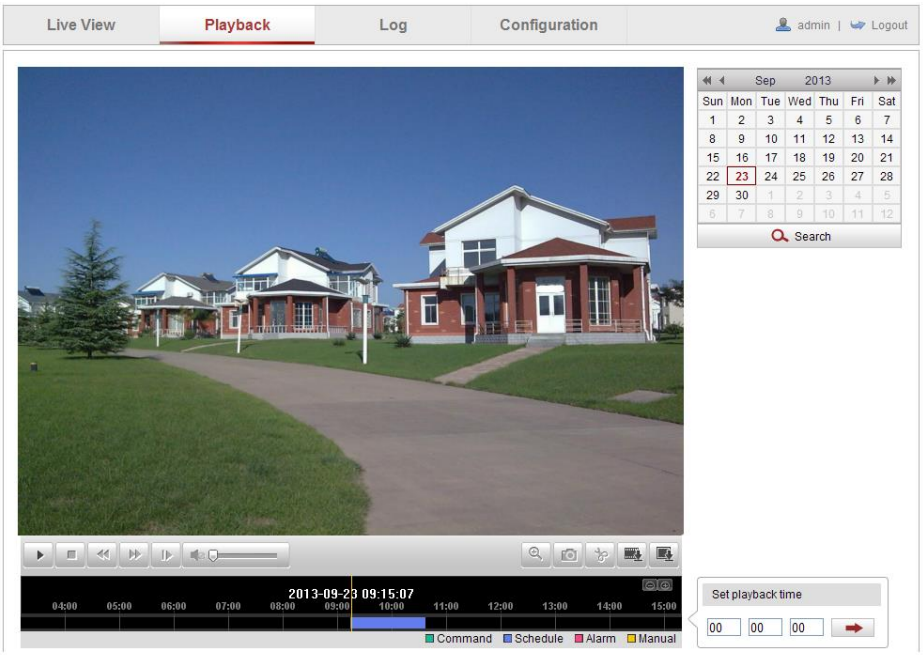
9. Odtwarzanie obrazu nagranego

Cel czynności:

W niniejszym rozdziale podajemy, jak obejrzeć obraz z plików wideo, zapisanych w stacji oddalonej, na dysku sieciowym lub karcie SD.

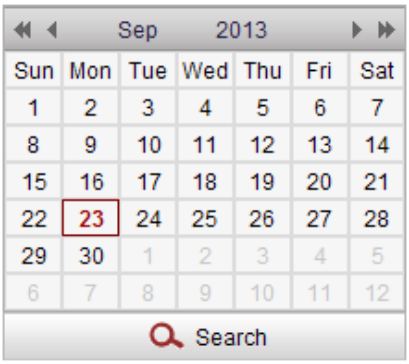
Procedura wykonania:

1. W pasku menu kliknij przycisk **Playback**, aby wyświetlić interfejs odtwarzania wideo-nagrań.



Rys. 9–1: Interfejs ekranowy do odtwarzania wideonagrań kamery (Playback)

2. W kalendarzu wybierz datę wideo-nagrania, które chcesz obejrzeć, po czym kliknij przycisk **Search**.



Rys. 9–2: Kalendarz z wybraną datą i przyciskiem **Search** do wyszukiwania wideonagrań

3. Po wyszukaniu, kliknij przycisk  , aby kolejno odtworzyć pliki wideo-nagrań znalezione pod tą datą.

Do sterowania odtwarzaniem wideonagrań używasz elementów, zebranych w pasku narzędziowym (tzw. *pasku odtwarzania*), znajdującym się u dołu tego interfejsu:

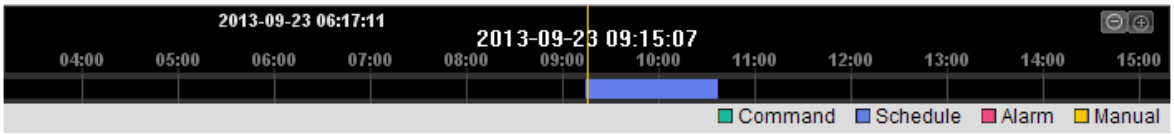
Rys. 9–3: Pasek odtwarzania

Tabela 3: PASEK ODTWARZANIA — funkcje przycisków

Przycisk	Funkcja	Przycisk	Funkcja
	odtwarzaj		zrób 1-klatkowy fotozrzut z wideo
	pauza		start/stop podczas wycinania klipu wideo
	stop		włącz i wyreguluj siłę dźwięku / wycisz kompletnie
	zwolnij		pobierz plik wideonagrania do siebie na swój PC
	przyspiesz		pobierz plik fotozrzutu do siebie na swój PC
	odtwarzaj poklatkowo		załącz/odłącz zbliżenie cyfrowe

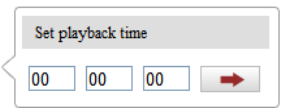
Uwaga: Ścieżki zapisu pobieranych plików wideonagrań i fotozrzutów możesz wskazać lokalnie[27] za pomocą interfejsu ustawień lokalnych kamery (**Local Configuration**), dokładniejszy opis — zob. *podrozdz. 6.1*, str. 41.

Jeżeli w wyszukanym wideo-nagraniu chcesz przesunąć bieżący punkt odtwarzania na inny interesujący Cię, to w panelu odczytu wideo-nagrań przeciągnij myszą pasek lokalizatora odczytu na ten inny czas:



Rys. 9–4: Panel odczytu/lokalizacji wideo-nagrań kamery

Żądany czas odczytu możesz też wprowadzić precyzyjniej, z klawiatury (zob. trzy pola **Set playback time** na następnej ilustracji). Potem musisz jeszcze kliknąć przycisk  , aby nastąpiło przestawienie bieżącego punktu odtwarzania na ten wpisany czas:



Rys. 9–5: Pola do wpisania żądanego czasu odtwarzania

[27] (w urządzeniu sterowanym, tj. kamerze) — przyp. tłum.

Klikając przyciski  możesz zmniejszyć/powiększyć paskowy lokalizator odczytu.

Po kolorze paska odczytu nagrania — w panelu odczytu wideo-nagrań — poznasz rodzaj danego nagrania:

Rys. 9–6: Każdy rodzaj wideonagrania ma swój kolor

10. Wyszukiwanie w treści logu

Cel czynności:

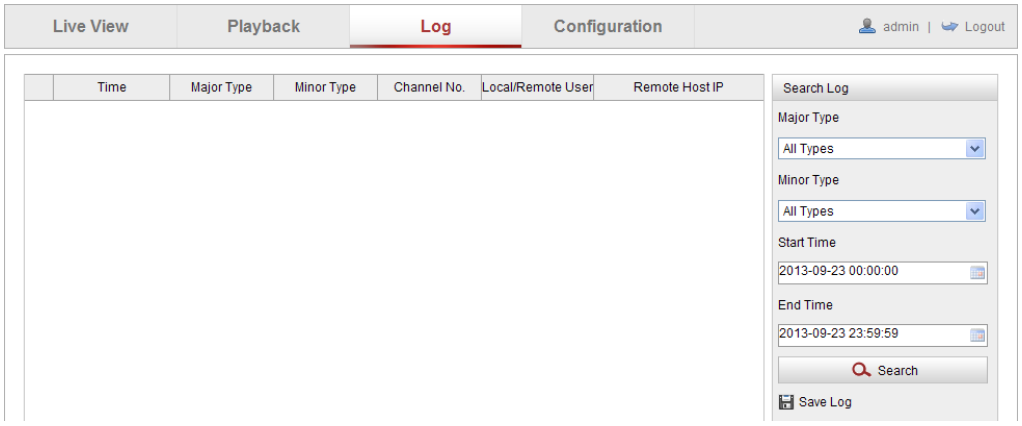
Kamera może zapisywać: swój stan funkcjonowania, występujące alarmy, wyjątki systemowe oraz informacje o kamerze — w plikach dziennikowych (=logach). Jeśli trzeba, treść logu możesz wyczytać do pliku zewnętrznego.[28]

Przygotuj na wstępie:

Należy skonfigurować sieciowy magazyn danych do użycia przez kamerę albo włożyć kartę pamięci SD do kamery.

Procedura wykonania:

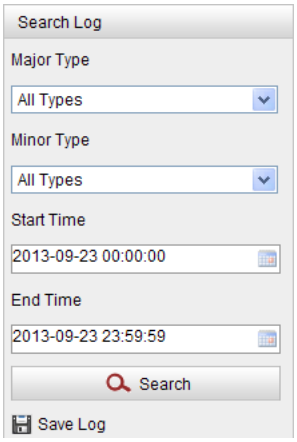
1. W pasku menu kliknij przycisk **Log**, aby wyświetlić interfejs ekranowy funkcji wyszukiwania:



Rys. 10–1: Interfejs funkcji wyszukiwania w logu (Search Log)

2. W panelu ustawień Search Log wybierz kryteria, specyfikujące rodzaj/typ poszukiwanych — a w tym: te typu ważniejszego (Major Type), te typu pomniejszego (Minor Type), czas rozpoczęcia (Start Time), czas zakończenia się (End Time).
3. Kliknij przycisk **Search**, aby przeszukać pliki dziennikowe kamery (=logi). Logi pasujące do kryteriów wyszukiwania (zadanych w kroku **2**.) wyświetlą się w tym interfejsie, zebrane w tabeli.

[28] zob. przycisk **Save Log** — przyp. tłum.



Rys. 10–2: Panel wyszukiwania w logach

4. Pliki logów możesz wyeksportować przez kliknięcie przycisku **Save Log**, aby zachować je na swoim komputerze.

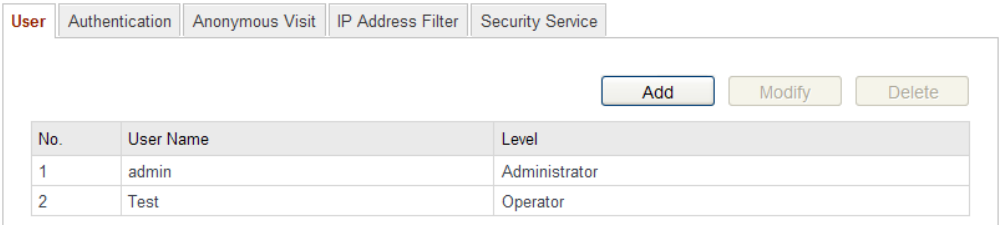
11. Pozostałe funkcje

11.1. Zarządzanie kontami użytkowników

Wyświetl interfejs ekranowy do zarządzania użytkownikami (User):

Configuration > Basic Configuration > Security > User

albo też: **Configuration > Advanced Configuration > Security > User**



Rys. 11–1: Dane o użytkownikach

- **Dodanie użytkownika — przycisk Add**

Użytkownik *admin* ma domyślnie do dyspozycji wszystkie możliwe uprawnienia — może: dodawać nowe konta / modyfikować inne konta / kasować inne konta.

Użytkownika *admin* nie można skasować, a ponadto spośród jego parametrów możesz mu zmienić tylko jego hasło dostępowe.

Procedura wykonania:

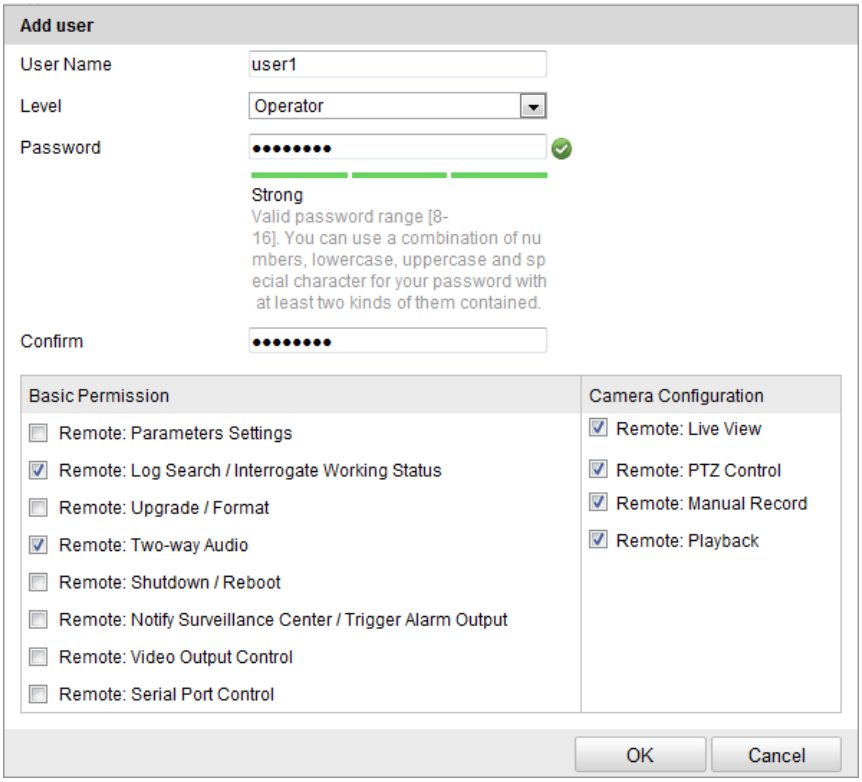
1. Kliknij przycisk **Add**, aby dodać nowego użytkownika systemu kamery.
2. W polu User Name wpisz nazwę nowego użytkownika. Z listy rozwijalnej Level wybierz rangę dla tego użytkownika, a w polu Password wpisz jego hasło dostępowe.

Uwagi:

- Można utworzyć maks. **31** kont użytkownika.
- Użytkownicy mający różną rangę (Level) mają też różne uprawnienia. System pozwala nadać danemu użytkownikowi dwie rangi (Level): Operator, User.

- *Dla ochrony Twojej własnej prywatności oraz dla lepszej ochrony Twojego systemu od źródeł zagrożeń sieciowych zdecydowanie zalecamy zastosowanie **silnych haseł** do wszystkich funkcji i urządzeń sieciowych. Hasło takie powinno być czymś, co samemu sobie wybierzesz, (powinno być w nim minimum 8 znaków, w tym co najmniej trzy z następujących kategorii znakowych: litery wielkie, litery małe, cyfry, znaki specjalne), aby podnieść poziom zabezpieczenia Twojego produktu (kamery).*
- *Odpowiedzialność za właściwe skonfigurowanie wszystkich haseł i innych nastaw zabezpieczających spoczywa na instalatorze oraz/lub użytkowniku ostatecznym (tj. konsumencie/odbiorcy) instalowanego rozwiązania.*

3. W grupach ustawień **Basic Permission** (uprawnienia podstawowe) i **Camera Configuration** (konfigurowanie ustawień kamery) zaznacz/odznacz pola wyboru od tych uprawnień, które przydzielasz/zabierasz temu nowemu użytkownikowi.
4. Kliknij przycisk **OK**, aby zakończyć dodawanie tego użytkownika.

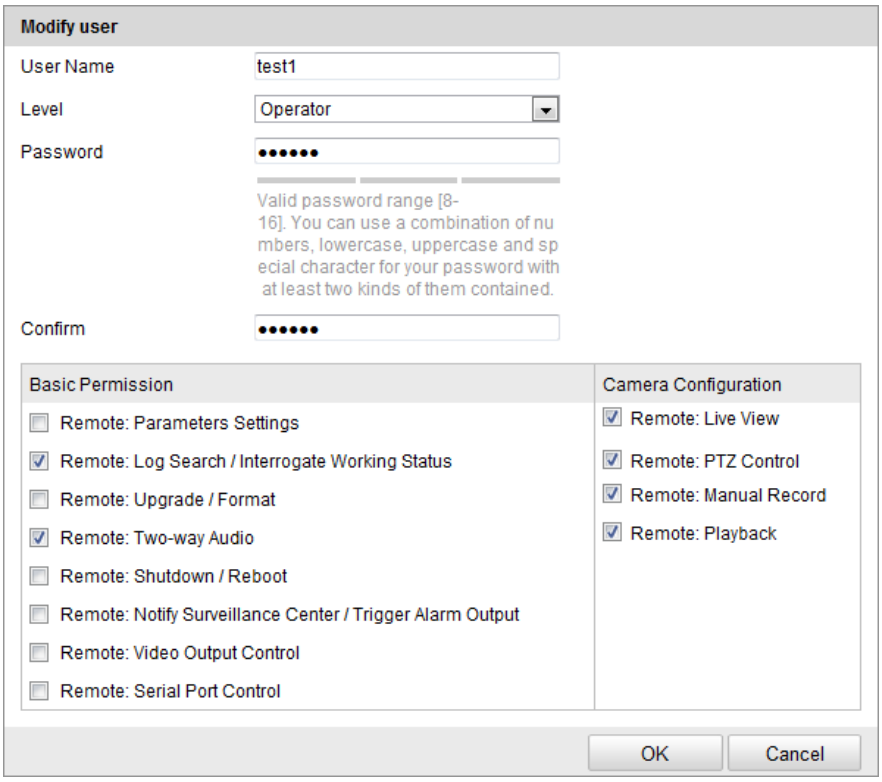


Rys. 11–2: Interfejs służący do dodania użytkownika (**Add User**)

- **Zmodyfikowanie użytkownika — przycisk Modify**

Procedura wykonania:

1. Kliknij lewym przyciskiem myszy, aby z listy użytkowników (p. rys. na str. 150) wybrać użytkownika do zmodyfikowania, po czym kliknij przycisk **Modify**.
2. Jeśli trzeba — zmodyfikuj w koncie tego użytkownika jego: nazwę systemową (**User Name**) lub rangę (**Level**) lub hasło dostępowe (**Password**).
3. Jeśli trzeba — w grupach **Basic Permission** i **Camera Configuration** zaznacz/odznacz pola wyboru od uprawnień, aby je przydzielić/zabrać temu modyfikowanemu użytkownikowi.
4. Kliknij przycisk **OK**, aby zakończyć modyfikowanie tego użytkownika.



Rys. 11–3: Interfejs służący do zmodyfikowania użytkownika (Modify User)

- **Skasowanie użytkownika — przycisk** Delete

Procedura wykonania:

1. Kliknij w liście użytkowników, aby wybrać użytkownika, którego konto potrzebujesz skasować z systemu. Następnie kliknij przycisk **Delete**.
2. W wyświetlonym okienku dialogowym kliknij przycisk **OK**, aby potwierdzić chęć skasowania użytkownika i usunąć go z systemu.

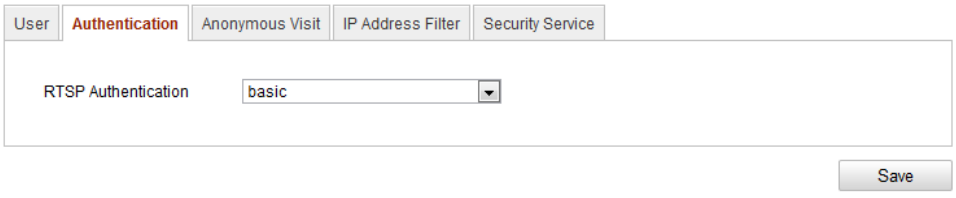
11.2. Uwierzytelnianie

Cel czynności:

Kamera umożliwia skonkretyzowaną ochronę strumienia danych, w którym przesyłany jest podgląd bieżący kamery.

Procedura wykonania:

1. Wyświetl interfejs konfigurowania funkcji uwierzytelniania:
   Configuration > Advanced Configuration > Security > Authentication



Rys. 11–4: Uwierzytelnianie RTSP (Authentication)

2. Z listy rozwijalnej **RTSP Authentication** wybierz rodzaj uwierzytelnienia: **basic** (podstawowy) / **disable** (wyłączony), aby załączyć / odłączyć funkcję uwierzytelniania RTSP.

Uwaga: Jeżeli odłączysz w systemie uwierzytelnianie RTSP, to każdy będzie mógł uzyskać dostęp do strumienia obrazu kamery poprzez protokół RTSP przez adres IP.

3. Kliknij przycisk **Save**, aby zachować wprowadzone ustawienia.

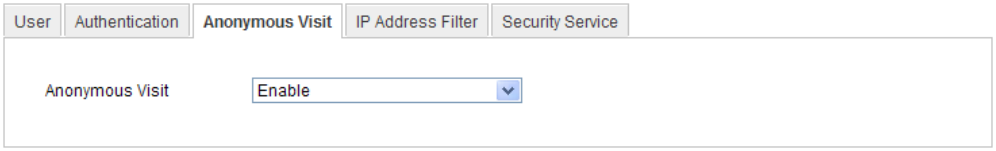
11.3. Odwiedziny przez użytkowników anonimowych

Załączenie tej funkcji pozwala wywoływać kamerę wszystkim tym, którzy nie posiadają nazwy użytkownika i hasła dostępowego do tego urządzenia.

Uwaga: Kamera udostępnia takim użytkownikom anonimowym tylko samo wyświetlanie podglądu bieżącego z kamery.

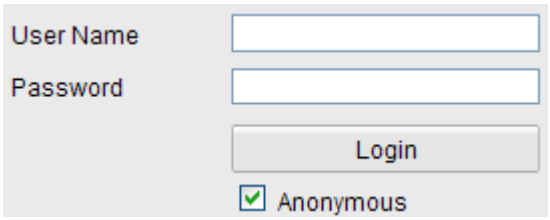
Procedura wykonania:

1. Wyświetl interfejs ekranowy dla konfigurowania odwiedzin anonimowych:
   Configuration > Advanced Configuration > Security > Anonymous Visit



Rys. 11–5: Interfejs do konfigurowania odwiedzin anonimowych (**Anonymous Visit**)

2. Z listy rozwijalnej **Anonymous Visit** wybierz opcję: **Enable** / **Disable**, aby załączyć / odłączyć zezwolenie dostępów anonimowych do kamery.
3. Kliknij przycisk **Save**, aby zachować wprowadzone ustawienia.
   Przy następnym logowaniu się do kamery, w interfejsie logowania zobaczysz dodatkowo pole wyboru **Anonymous**, jak na poniższej ilustracji:



Rys. 11–6: Interfejs logowania umożliwiający odwiedziny anonimowe (**Anonymous**)

4. Zaznacz pole wyboru **Anonymous** i kliknij przycisk **Login**.

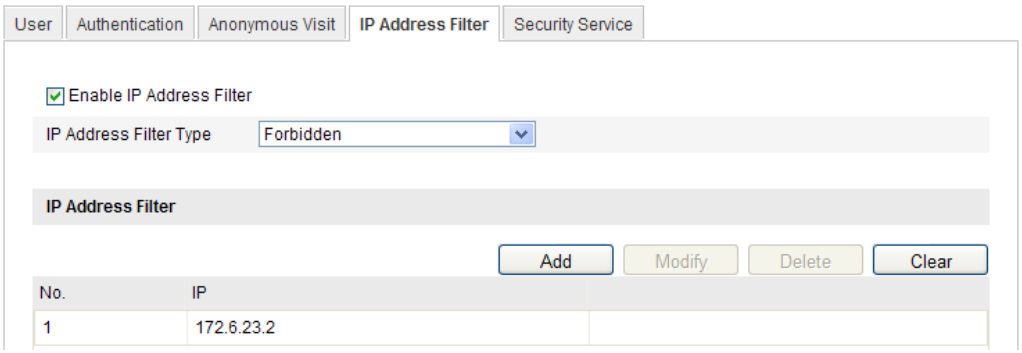
Przez zezwolenie na anonimowe korzystanie z funkcji podglądu bieżącego kamery (*Live View*) umożliwiasz innym osobom sieciowy dostęp do Twojej kamery i do jej obrazu bieżącego, bez nakładania na nie wymogu „okazywania” danych uwierzytelniających. Stąd — przy zezwalaniu na anonimowe korzystanie z funkcji podglądu bieżącego — sprawą wagi krytycznej staje się zagwarantowanie, że (dostępny

bez uwierzytelnienia) widok w polu widzenia Twojej kamery nie narusza prywatności osób ewentualnie pojawiających się na obrazie kamery.
Uwzględniając immanentną natarczywość i „wścibskość" wideo-monitoringu należy uznać go za rozwiązanie niewłaściwe w miejscach, w których przebywają ludzie o wyższych wymaganiach co do poszanowania ich prywatności.

11.4. Filtr adresu IP

Cel czynności:
Ta funkcja otwiera możliwość zrealizowania kontroli dostępów.

Procedura wykonania:
1. Wyświetl interfejs ekranowy do konfigurowania funkcji filtru IP:
   Configuration > Advanced Configuration > Security > IP Address Filter



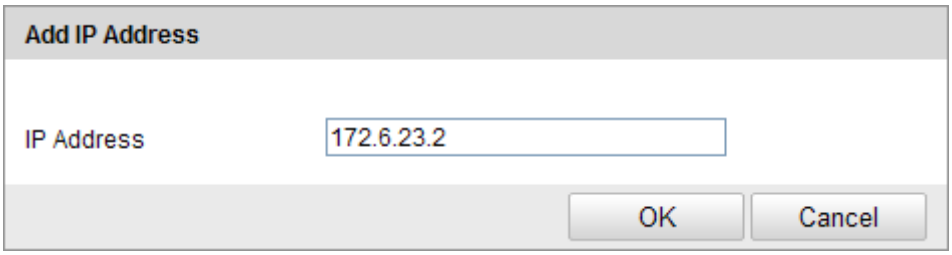
Rys. 11–7: Interfejs z ustawieniami do konfigurowania filtrowania adresu IP (**IP Address Filter**)

2. Zaznacz pole wyboru **Enable IP Address Filter**, aby załączyć w kamerze funkcję filtrowania adresów IP.
3. Z listy rozwijalnej **IP Address Filter Type** wybierz żądany rodzaj odfiltrowania — dostępne są dwa: **Forbidden** i **Allowed**.
4. W sekcji ustawień **IP Address Filter** utwórz przyciskami listę filtrowanych adresów IP.

   - Dodaj nowy adres IP do listy adresów filtrowanych — przycisk **Add**

Procedura wykonania:

(1) Kliknij przycisk **Add**, aby dodać nowy adres IP do listy adresów filtrowanych.
(2) W polu **IP Address** wpisz ten żądany adres IP do dodania.



Rys. 11–8: Interfejs do dodania nowego adresu IP do listy adresów filtrowanych (Add IP Address)

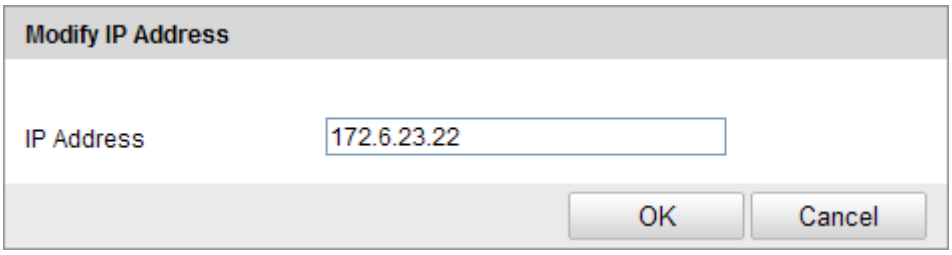
(3) Kliknij przycisk **OK**, aby zakończyć dodawanie adresu.

- Zmodyfikuj adres IP w liście adresów filtrowanych — przycisk **Modify**

Procedura wykonania:

(1) Kliknij lewym przyciskiem myszy w żądany adres IP widoczny na liście adresów filtrowanych — aby go wybrać, po czym kliknij przycisk **Modify**.

(2) Wyedytuj treść adresu w polu IP Address, aby uzyskać żądaną modyfikację.



Rys. 11–9: Interfejs do zmodyfikowania adresu IP, wybranego z listy adresów filtrowanych (Modify IP Address)

(3) Kliknij przycisk **OK**, aby zakończyć modyfikowanie adresu.

- Wykasuj adres IP z listy adresów filtrowanych — przycisk **Delete**
  Kliknij lewym przyciskiem myszy w żądany adres IP widoczny na liście adresów filtrowanych, aby go wybrać, po czym kliknij przycisk **Delete**.

- Wykasuj wszystkie adresy IP z listy adresów filtrowanych — przycisk **Clear**
  Kliknij przycisk **Clear**, aby usunąć wszystkie adresy z listy adresów filtrowanych (czyści całą listę).

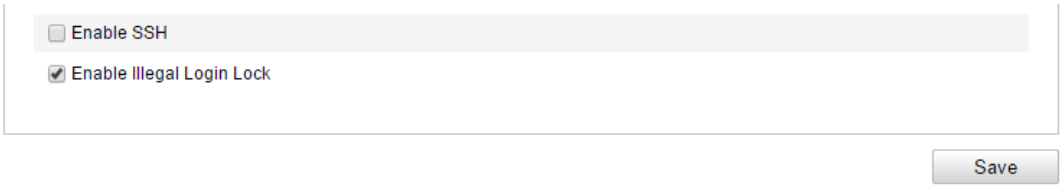
5. Kliknij przycisk **Save**, aby zachować wprowadzone ustawienia.

11.5. Usługa zabezpieczania (Security Service)

Aby umożliwić zdalne logowanie użytkowników i by poprawić bezpieczeństwo transmisji danych, kamera zapewnia usługę zabezpieczania pomyślaną dla poprawy komfortu użytkowego.

Procedura wykonania:

1. Przejdź do **Configuration** > **Advanced Configuration** > **Security** > **Security Service**, aby wyświetlić interfejs ustawień do konfigurowania usługi zabezpieczania.



Rys. 11–10: Interfejs do konfigurowania usługi zabezpieczania (**Security Service**)

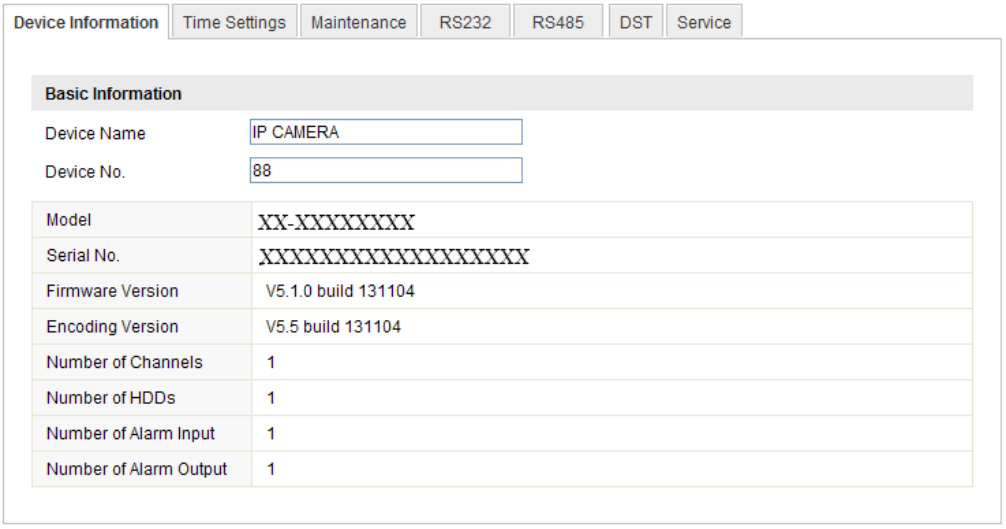
2. Zaznacz pole wyboru **Enable SSH**, aby załączyć w kamerze funkcję zabezpieczania transmisji danych bądź też odznacz je, aby ją odłączyć.
3. Zaznacz pole wyboru **Enable Illegal Login Lock**, aby adres IP ulegał zablokowaniu po **7** (siedmiu) nieudanych próbach uwierzytelnienia (nazwa/hasło) przez użytkownika o randze *admin* [**5** (pięć) razy dla użytkowników o randze *operator*/*user*].

   Uwaga: Jeśli adres IP ulegnie zablokowaniu, to możesz podjąć kolejną próbę logowania do kamery po 30 minutach.

11.6. Dane urządzenia

1. Wyświetl interfejs danych urządzenia:
   Configuration > Basic Configuration > System > Device Information
   albo: **Configuration > Advanced Configuration > System > Device Information**

W otwartym już interfejsie w sekcji **Basic Information** możesz wyedytować etykietę urządzenia (pole **Device Name**). Natomiast pozostałe widoczne tu dane tej kamery sieciowej, tj. **Model** (model), **Serial No.** (nr seryjny/produkcyjny), **Firmware Version** (wersja oprogramowania sprzętowego), **Encoding Version** (wersja enkodera), **Number of Channels** (liczba kanałów), **Number of HDDs** (liczba jednostek HDD), **Number of Alarm Input** (liczba wejść alarmowych) oraz **Number of Alarm Output** (liczba wyjść alarmowych) — wyświetlane są jedynie do wglądu. Nie można tych danych zmienić w tym menu, służą tylko jako informacja dla konserwatorów-serwisantów lub do zmiany w przyszłości.



Rys. 11–11: Interfejs do wglądu w dane urządzenia/kamery (Device Information)

11.7. Konserwacja i naprawy

11.7.1. Przeładowanie kamery (reboot)

Procedura wykonania:

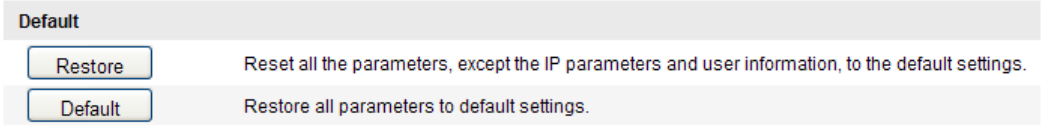
1. Wyświetl interfejs z opcjami konserwacji i napraw:
   Configuration > Basic Configuration > System > Maintenance
   albo też: **Configuration > Advanced Configuration> System > Maintenance**
2. Kliknij przycisk **Reboot**, aby przeładować system tej kamery sieciowej:

Rys. 11–12: Interfejs służący do przeładowania urządzenia (Reboot)

11.7.2. Przywrócenie ustawień domyślnych

Procedura wykonania:

1. Wyświetl interfejs z opcjami konserwacji i napraw:
   Configuration > Basic Configuration > System > Maintenance
   albo też: **Configuration > Advanced Configuration> System > Maintenance**
2. Kliknij przycisk **Restore** lub przycisk **Default**, aby przywrócić ustawienia konfiguracyjne kamery do ich stanu domyślnego.



Rys. 11–13: Interfejs służący do przywrócenia ustawień domyślnych w kamerze (Default)

Restore Przestaw wszystkie parametry – oprócz określających IP i danych użytkownika – do ich wartości domyślnych.
Default: Przywróć wszystkie parametry do ich wartości domyślnych.

Uwaga: Przywrócenie ustawień domyślnych – wykonane przyciskiem **Default** – przywraca również adres IP do jego stanu domyślnego — z funkcji przywrócenia ustawień należy więc korzystać *ostrożnie*.

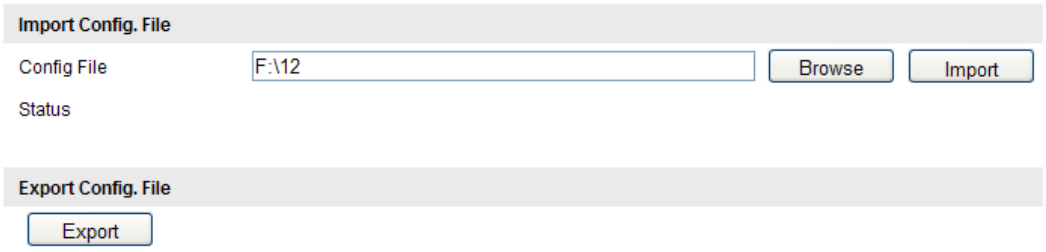
11.7.3. Eksportowanie / importowanie pliku konfiguracyjnego

Cel czynności:

Plik konfiguracyjny służy do seryjnego skonfigurowania większej liczby kamer pod rząd tym samym zestawem danych, co może uprościć proces konfigurowania w instalacjach z wieloma kamerami (wymagającymi skonfigurowania).

Procedura wykonania:

1. Wyświetl interfejs z opcjami konserwacji i napraw:
   Configuration > Basic Configuration > System > Maintenance
   albo też: **Configuration > Advanced Configuration > System > Maintenance**
2. Kliknij przycisk **Export**, aby wyeksportować aktualną konfigurację do pliku konfiguracyjnego i by wyczytać go w pewne wybrane miejsce.
3. Kliknij przycisk **Browse**, aby ręcznie odszukać/wskazać wcześniej zachowany plik konfiguracyjny. Następnie kliknij przycisk **Import**, aby uruchomić importowanie danych konfiguracyjnych z tego pliku.
   Uwaga: Po zaimportowaniu pliku konfiguracyjnego musisz przeładować kamerę (reboot).
4. Kliknij przycisk **Export** i ustaw ścieżkę zapisu, aby zachować plik konfiguracyjny w pamięci lokalnej**.**



Rys. 11–14: Interfejs służący do zaimportowania/wyeksportowania pliku konfiguracyjnego

11.7.4. Załadowanie nowocześniejszego systemu do kamery

Procedura wykonania:

1. Wyświetl interfejs z opcjami konserwacji i napraw:
   Configuration > Basic Configuration > System > Maintenance
   albo też: **Configuration > Advanced Configuration > System > Maintenance**
2. Z listy rozwijalnej Remote Upgrade wybierz Firmware lub Firmware Directory, aby wskazać położenie pliku unowocześnienia (tj. upgrade'u):
   Firmware: Wskaż dokładną ścieżkę wraz z plikiem upgrade'u.

Firmware Directory: Ta opcja wymaga podanie jedynie samego katalogu, w którym znajduje się plik upgrade'u.

3. Kliknij przycisk **Browse**, aby wybrać lokalny plik upgrade'u, po czym kliknij przycisk **Upgrade**, aby uruchomić aktualizację przez sieć w zdalnej lokalizacji.

Rys. 11–15: Interfejs służący do unowocześnienia firmware'u tej kamery sieciowej

Uwaga: Ładowanie unowocześnienia firmware'u do kamery może zająć nawet **1~10 minut**. W tym czasie nie wolno odłączać zasilania od kamery. Ponadto, z chwilą zakończenia ładowania unowocześnienia kamera samoczynnie wykona przeładowanie (reboot), aby dopełnić aktualizacji.

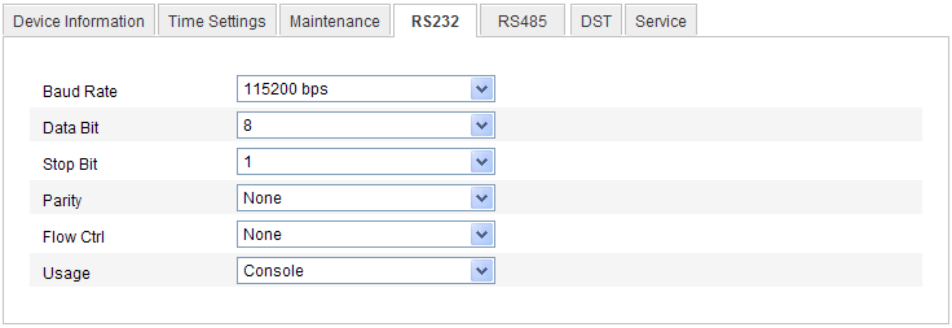
11.8. Ustawienia portu RS-232

Z portu komunikacyjnego RS-232 w kamerze możesz wykorzystać dwojako:

- **Konfigurowanie parametrów**: Podłącz do kamery komputer przez jego port szeregowy. Parametry urządzenia (tj. kamery) będzie można wtedy skonfigurować za pomocą aplikacji typu *HyperTerminal* uruchomionej na tym komputerze. Pamiętaj, że parametry pracy portu szeregowego w komputerze muszą być identyczne z tymi od portu szeregowego kamery.
- **Kanał przezroczysty**: Podłącz urządzenie szeregowe bezpośrednio do kamery. Tym urządzeniem szeregowym będziesz sterować zdalnie przez sieć z poziomu Twojego komputera.

Procedura wykonania:

1. Wyświetl interfejs z ustawieniami służącymi do konfigurowania portu RS-232: **Configuration > Advanced Configuration > System > RS232**



Rys. 11–16: Interfejs z ustawieniami do konfigurowania portu RS-232

Uwaga: Jeśli chcesz podłączyć się do kamery przez jej port RS-232, to pamiętaj, że parametry transmisji RS-232 (w urządzeniu podłączanym do kamery) muszą być dokładnie takie same jak parametry, które skonfigurujesz w tym interfejsie.

2. Po wybraniu żądanych ustawień kliknij przycisk **Save**, aby je zachować.

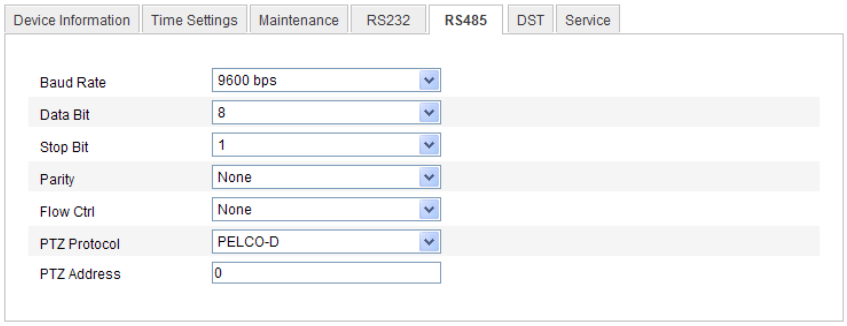
11.9. Ustawienia portu RS-485

Cel czynności:

Port szeregowy RS-485 kamery jest wykorzystywany do sterowania głowicą PTZ kamery. Jednak zanim zaczniesz nią sterować, musisz mieć skonfigurowane parametry PTZ.

Procedura wykonania:

1. Wyświetl interfejs z ustawieniami służącymi do konfigurowania portu RS-485:
   Configuration > Advanced Configuration > System > RS485



Rys. 11–17: Interfejs z ustawieniami do konfigurowania portu RS-485

2. Wybierz żądane wartości dla poszczególnych parametrów transmisji po RS-485 i kliknij przycisk **Save**, aby zachować wprowadzone ustawienia.

   Ustawienia parametrów w stanie domyślnym: szybkość bitowa **Baud Rate** = **9600 bps**, liczba bitów danych **Data Bit** = **8**, liczba bitów zakończenia transmisji **Stop Bit** = **1**, kontrola parzystości **Parity** = **None** (brak), sterowanie przepływem **Flow Control** = **None** (brak).

   Uwaga: Dla parametrów, określanych w listach rozwijalnych: **Baud Rate**, **PTZ Protocol** i **PTZ Address**, musisz wybrać dokładnie takie same wartości jak te w parametrach PTZ kamery.

11.10. Ustawienia usług dla podzespołów sprzętowych

Przejdź do: **Configuration > Advanced Configuration > System > Service**, aby wyświetlić interfejs udostępniający ustawienia serwisowe do obsługi podzespołów sprzętowych.

Ustawienia serwisowe (**Service**) odnoszą się do serwisowania podzespołów sprzętowych, którymi dana kamera dysponuje / ma na wyposażeniu. Zakres tych ustawień będzie różny w różnych modelach kamer.

W przypadku kamer — wyposażonych w: oświetlenie/reflektor IR–LED, automatyczny układ regulacji ABF (*Auto Back Focus*), automat odmgławiania (*Auto Defog*) czy wskaźnik stanu LED — możesz wejść do tych ustawień serwisowych (**Service**) i

wybrać dla tych poszczególnych jednostek, czy mają być załączone (**Enable**) czy odłączone (**Disable**) w tej kamerze (w zależności od aktualnych/faktycznych potrzeb).

Załączniki

Załącznik 1: Wiadomości wstępne o oprogramowaniu SADP

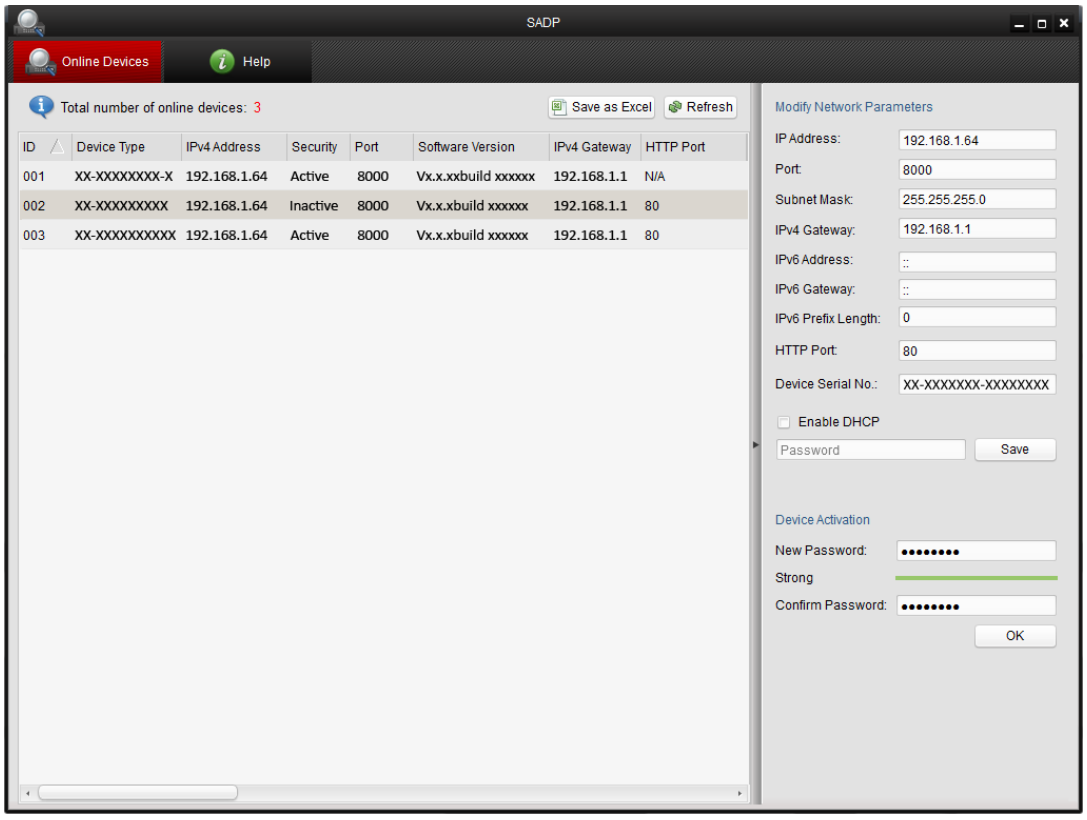
- **Opis oprogramowania SADP**

SADP (***S**earch **A**ctive **D**evices **P**rotocol*) to przyjazne w użyciu i nie wymagające instalowania narzędzie software'owe do online-wyszukiwania urządzeń. Wyszukuje ono aktywne urządzenia online w Twojej podsieci i wyświetla informacje o tych urządzeniach. Za pomocą tego oprogramowania możesz też zmodyfikować podstawowe parametry sieciowe tych urządzeń.

- **Wyszukiwanie aktywnych urządzeń online**

♦ **AUTOMATYCZNIE wyszukuj urządzenia w stanie online**

Po uruchomieniu oprogramowania SADP, wyszukuje ono automatycznie urządzenia sieciowe w stanie online dla systemu — i robi to co 15 s z podsieci, w której ulokowany jest Twój komputer. Wyświetla przy tym — w interfejsie **Online Devices** (zob. ilustracja poniżej) — całkowitą liczbę urządzeń wyszukanych oraz ich dane. Wśród tych danych wyświetlane są: rodzaj urządzenia (kol. **Device Type**), jego adres IP (kol. **IPv4 Address**), jego nr portu (kol. **Port**) i inne.



Rys. A.1.1: Wyszukiwanie urządzeń sieciowych, znajdujących się w stanie online

Uwaga:

Urządzenie może zostać wyszukane i wyświetlone w ww. liście już w **15 s** od jego przejścia (ze stanu offline) w stan online. Zostanie natomiast z listy usunięte po upływie **45 s** od przejścia w stan offline.

♦ **RĘCZNIE wyszukaj urządzenia w stanie online**

Możesz też ewentualnie kliknąć przycisk Refresh, aby ręcznie odświeżyć listę urządzeń, znajdujących się w stanie online — świeżo wyszukane urządzenia online zostaną wtedy dodane do listy.

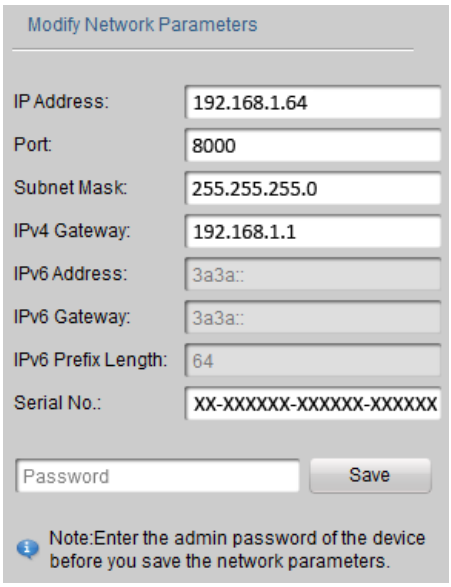
NOTE W nagłówkach kolumn tej listy znajdują się przyciski / — klikając je możesz uporządkować sobie wyświetlone w liście urządzenia w kolejności rosnącej / malejącej (wg treści w tej kliknięte kolumnie). Ponadto kliknięciem przycisku możesz rozwinąć tabelę urządzeń na całą szerokość (chowa panel parametrów sieciowych, który jest po prawej od tabeli nierozwiniętej). Albo kliknij znowu , aby z powrotem wyświetliła się tabela z panelem parametrów sieciowych.

● Edytowanie ustawień sieciowych — grupa Modify network parameters

Procedura wykonania:

1. Z listy urządzeń kliknięciem wybierz żądane urządzenie, którego parametry sieciowe zamierzasz zmienić — wyświetlą się one w panelu **Modify Network Parameters** po prawej stronie od listy/tabeli.
2. Przez edycję zmodyfikuj te parametry sieciowe urządzenia, które dają się zmienić, np. adres IP (pole **IP Address**) i numer portu (pole **Port**).
3. W polu **Password** wpisz hasło użytkownika *admin* dla tego modyfikowanego urządzenia. Następnie kliknij przycisk Save, aby zapisać zmiany w urządzeniu.

- *Dla ochrony Twojej własnej prywatności oraz dla lepszej ochrony Twojego systemu od źródeł zagrożeń sieciowych zdecydowanie zalecamy zastosowanie **silnych haseł** do wszystkich funkcji i urządzeń sieciowych. Hasło takie powinno być czymś, co samemu sobie wybierzesz, (powinno być w nim minimum 8 znaków, w tym co najmniej trzy z następujących kategorii znakowych: litery wielkie, litery małe, cyfry, znaki specjalne), aby podnieść poziom zabezpieczenia Twojego produktu (kamery).*
- *Odpowiedzialność za właściwe skonfigurowanie wszystkich haseł i innych nastaw zabezpieczających spoczywa na instalatorze oraz/lub użytkowniku ostatecznym (tj. konsumencie/odbiorcy) instalowanego rozwiązania.*



Rys. A.1.2: Panel umożliwiający modyfikowanie parametrów sieciowych urządzenia aktualnie zaznaczonego w liście

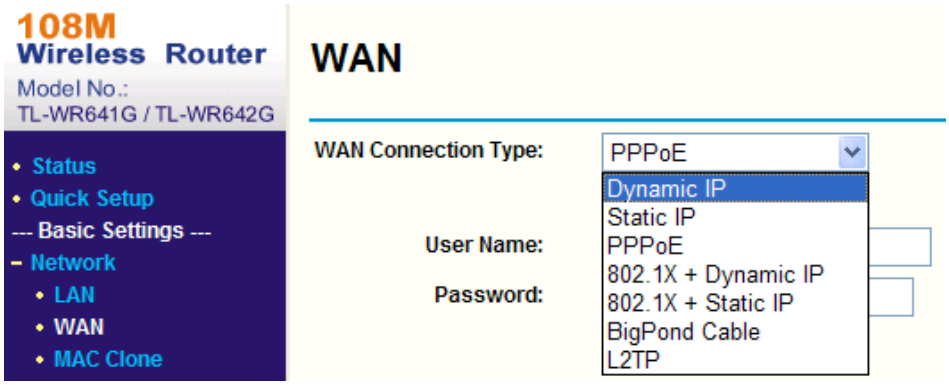
Nota: Zanim będziesz mógł zapisać wprowadzone parametry sieciowe, musisz wprowadzić hasło *admina*-a tego urządzenia.

Załącznik 2: Mapowanie portów

Konfigurowanie poniższych ustawień odnosi się do rutera TP-LINK (model TL-WR641G). Zakres tych ustawień będzie różny w innych/różnych modelach ruterów.

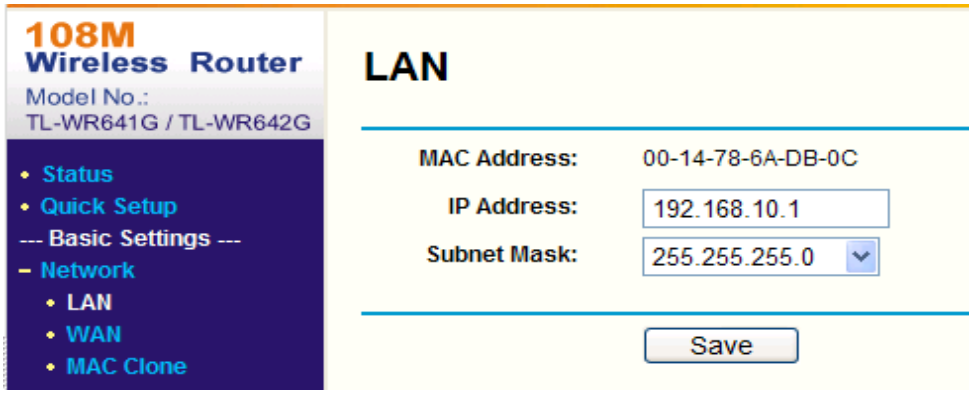
Procedura wykonania:

1. Z listy rozwijalnej **WAN Connection Type** wybierz żądane połączenie WAN, jak pokazane poniżej:



Rys. A.2.1: Interfejs ekranowy rutera — wybierz w ruterze prawidłowy rodzaj połączenia WAN

2. Wprowadź ustawienia **LAN** rutera, jak pokazane na poniższej ilustracji — adres IP (w polu **IP Address**) oraz maskę podsieci (lista rozwijalna **Subnet Mask**).



Rys. A.2.2: Interfejs ekranowy rutera — wprowadź prawidłowe ustawienia dla sieci LAN

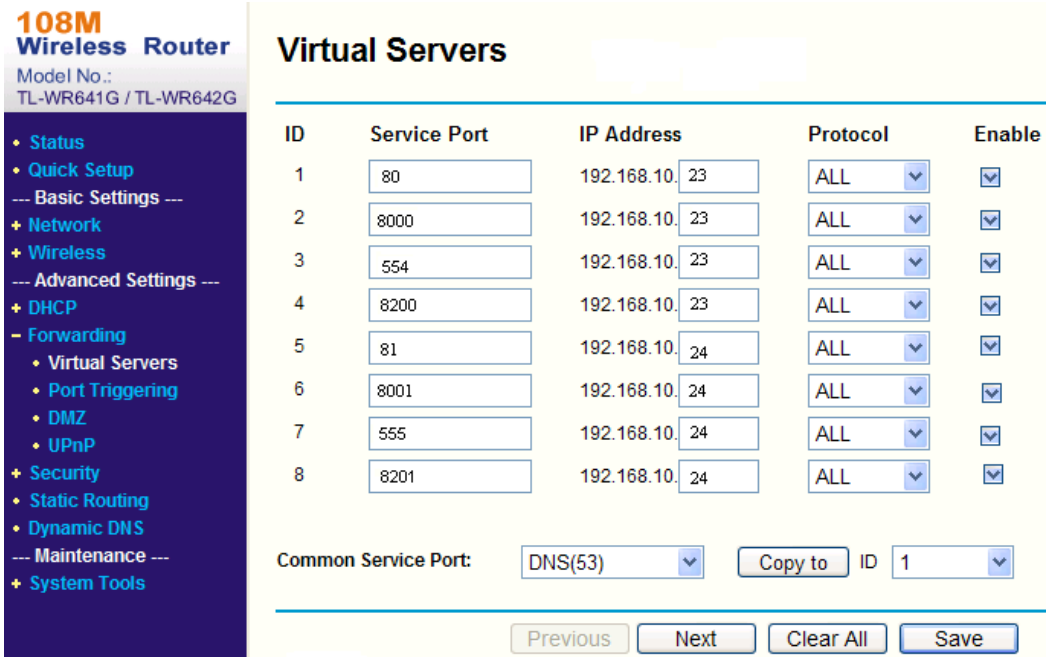
3. W ustawieniach funkcji **Forwarding** (zob. następna ilustracja poniżej) wprowadź w części **Virtual Severs** żądane mapowania portów. W swym ustawieniu domyślnym, kamera wykorzystuje porty nr: **80**, **8000** oraz **554**. Możesz zmienić te wartości z poziomu przeglądarki internetowej lub oprogramowania klienckiego.

   Przykład:

   Załóżmy, że masz 2 kamery sieciowe podłączone do tego samego rutera. Możesz wtedy skonfigurować w ruterze porty (**Service Port**) jednej z tych kamery jako: **80**, **8000**, **554** i **8200** z adresem IP 192.168.10.**23**, a porty drugiej z tych kamer jako: **81**, **8001**, **555** i **8201** z adresem IP 192.168.10.**24**. Opis wprowadzenia tych ustawień — zob. poniższe kroki:

Procedura wykonania:

1. Zgodnie z ustawieniami przyjętymi wyżej w naszym przykładzie, wykonaj mapowanie portów: 80, 8000, 554 i 8200 dla pierwszej kamery sieciowej, obecnej pod adresem: 192.168.1.23
2. Wykonaj też mapowanie portów: 81, 8001, 555 i 8201 dla drugiej kamery sieciowej, obecnej pod adresem: 192.168.1.24.
3. W listach rozwijalnych kolumny **Protocol** wybierz jako protokół: **ALL** lub **TCP**.
4. W kolumnie **Enable** zaznacz odnośne pola wyboru, aby załączyć te mapowania, po czym kliknij przycisk **Save**, aby zachować wprowadzone ustawienia



Rys. A.2.3: Interfejs ekranowy rutera — wprowadź prawidłowe mapowanie portów kamer

Uwaga: Pamiętaj, że konfigurowany tu port kamery sieciowej nie może powodować konfliktu z innymi portami. Przykładowo, port pewnych funkcji zarządzania w ruterze ma nr 80. Zmień więc port kamery, jeśli jest taki sam jak ww. port zarządzania.

0503001050121


First Choice for Security Professionals