



HIKVISION

Kamera sieciowa

Instrukcja obsługi

UD.6L0201D1919A01

Instrukcja obsługi

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

WSZELKIE PRAWA ZASTRZEŻONE.

Wszystkie informacje, w tym użyte sformułowania, zdjęcia i rysunki stanowią własność spółki Hangzhou Hikvision Digital Technology Co., Ltd. lub jej spółek zależnych (zwananych dalej „Hikvision”). Niniejszej instrukcji obsługi (zwanej dalej „Instrukcją”) nie wolno powielać, zmieniać, tłumaczyć, ani rozpowszechniać, w części ani w całości, jakimikolwiek metodami, bez uprzedniej pisemnej zgody Hikvision. Jeśli nie stwierdzono inaczej, Hikvision nie udziela żadnych gwarancji bądź rękojmi ani nie składa żadnych deklaracji, wyraźnych lub dorozumianych, dotyczących niniejszej Instrukcji.

Informacje dotyczące niniejszej instrukcji obsługi

Niniejsza Instrukcja dotyczy Kamery sieciowej (V5.3.0).

Instrukcja zawiera wskazania dotyczące użytkowania produktu i zarządzania nim. Zdjęcia, tabele, rysunki i wszelkie inne zawarte w niej informacje mają charakter wyłącznie opisowy i ilustracyjny. Informacje zawarte w niniejszej instrukcji mogą zostać zmienione bez uprzedniego powiadomienia ze względu na aktualizację oprogramowania układowego lub z innych przyczyn. Najnowszą wersję instrukcji można pobrać z witryny firmowej (<http://overseas.hikvision.com/en/>).

Prosimy o korzystanie z niniejszej instrukcji pod kontrolą specjalistów.

Uznanie znaków towarowych

HIKVISION i inne znaki towarowe oraz logo Hikvision stanowią własność Hikvision w różnych jurysdykcjach. Pozostałe znaki towarowe i logo wymienione poniżej należą do odpowiednich właścicieli.

Zastrzeżenia prawne

W MAKSYMALNYM ZAKRESIE, NA JAKI ZEZWALA PRAWO, OPISANY PRODUKT, WŁĄCZAJĄC W TO SPRZĘT FIZYCZNY, OPROGRAMOWANIE I OPROGRAMOWANIE UKŁADOWE, JEST DOSTARCZANY W STANIE

„TAKIM, W JAKIM SIĘ ZNAJDUJE”, ZE WSZELKIMI BŁĘDAMI I USTERKAMI. HIKVISION NIE SKŁADA ŻADNYCH GWARANCJI, WYRAŹNYCH LUB DOROZUMIANYCH, W TYM, ALE NIE WYŁĄCZNIE, GWARANCJI SPRZEDAWALNOŚCI, ZADOWALAJĄCEJ JAKOŚCI, PRZYDATNOŚCI DO OKREŚLONEGO CELU I NIENARUSZANIA PRAW OSÓB TRZECICH. W ŻADNYM RAZIE SPÓŁKA HIKVISION, JEJ DYREKTORZY, KIEROWNICY, PRACOWNICY ANI PRZEDSTAWICIELE NIE BĘDĄ PONOSIĆ WOBEC UŻYTKOWNIKÓW ODPOWIEDZIALNOŚCI Z TYTUŁU JAKICHKOLWIEK SZKÓD SPECJALNYCH, WTÓRNYCH, UBOCZNYCH LUB POŚREDNICH, CO OBEJMUJE MIĘDZY INNYMI ODSZKODOWANIA Z TYTUŁU UTRATY ZYSKÓW, PRZERWY W DZIAŁALNOŚCI GOSPODARCZEJ, UTRATY DANYCH LUB DOKUMENTACJI W ZWIĄZKU Z UŻYTKOWANIEM TEGO PRODUKTU, NAWET JEŚLI SPÓŁKA HIKVISION ZOSTAŁA POINFORMOWANA O MOŻLIWOŚCI WYSTĄPIENIA TAKICH SZKÓD.

UŻYTKOWANIE PRODUKTU Z DOSTĘPEM DO INTERNETU ODBYWA SIĘ NA WYŁĄCZNE RYZYKO UŻYTKOWNIKA. HIKVISION NIE PONOSI ŻADNEJ ODPOWIEDZIALNOŚCI ZA NIEPRAWIDŁOWE DZIAŁANIE, UTRATĘ PRYWATNOŚCI LUB INNE SZKODY WYNIKAJĄCE Z ATAKU CYBERNETYCZNEGO, ATAKU HAKERÓW, INFEKCJI WIRUSOWEJ LUB INNYCH ZAGROZEŃ BEZPIECZEŃSTWA INTERNETOWEGO. TYM NIEMNIEJ HIKVISION NA ŻĄDANIE BĘDZIE UDZIELAĆ W TAKICH PRZYPADKACH SZYBKIEJ POMOCY TECHNICZNEJ.

PRAWA DOTYCZĄCE MONITORINGU ZALEŻĄ OD DANEJ JURYSDYKCJI. UŻYTKOWNIK POWINIEN PRZED ROZPOCZĘCIEM KORZYSTANIA Z PRODUKTU UZYSKAĆ INFORMACJE NA TEMAT OBOWIĄZUJĄCYCH GO PRAW, ABY ZAPEWNIĆ, ŻE KORZYSTA Z PRODUKTU W SPOSÓB ZGODNY Z PRAWEM. HIKVISION NIE PONOSI ODPOWIEDZIALNOŚCI ZA UŻYTKOWANIE PRODUKTU W CELACH NIEZGODNYCH Z PRAWEM.

W RAZIE JAKICHKOLWIEK KONFLIKTÓW MIĘDZY TREŚCIĄ

PODRĘCZNIKA A OBOWIĄZUJĄCYM PRAWEM PIERWSZEŃSTWO MA TO OSTATNIE.

Informacje dotyczące przepisów prawnych

Informacje dotyczące przepisów FCC

Zgodność z wymaganiami FCC: Niniejszy sprzęt przetestowano pod kątem zgodności z ograniczeniami dla urządzeń cyfrowych, zgodnie z częścią 15 Zasad FCC. Zgodność została potwierdzona. Te ograniczenia mają na celu zapewnienie rozsądnie uzasadnionej ochrony przed szkodliwymi zakłóceniami, podczas używania sprzętu w środowisku komercyjnym. Urządzenie generuje, wykorzystuje i może emitować energię o częstotliwości radiowej. Jeśli nie jest zainstalowane i używane zgodnie z instrukcją obsługi, może powodować szkodliwe zakłócenia komunikacji radiowej. Działanie urządzenia na terenie mieszkalnym prawdopodobnie spowoduje szkodliwe zakłócenia, do których wyeliminowania będzie zobowiązany użytkownik, na własny koszt.

Warunki FCC

Urządzenie spełnia wymagania części 15 Przepisów FCC. Jego użytkowanie podlega poniższym dwóm warunkom:

1. Urządzenie nie może powodować szkodliwych zakłóceń.
2. Urządzenie musi przyjmować wszelkie otrzymane zakłócenia, w tym takie, które mogą powodować nieprawidłowe działanie.

Deklaracja zgodności UE



Ten produkt oraz – jeśli ma to zastosowanie – dostarczane z nim akcesoria są oznaczone znakiem „CE”, co oznacza spełnianie wymagań obowiązujących zharmonizowanych norm europejskich, wymienionych w dyrektywie elektromagnetycznej 2004/108/WE i dyrektywie RoHS 2011/65/UE.



2012/19/EU (dyrektywa WEEE): Produktu oznaczonego tym symbolem nie wolno w Unii Europejskiej usuwać wraz z

niesortowanymi odpadami komunalnymi. Aby umożliwić prawidłowy recykling, należy zwrócić produkt lokalnemu sprzedawcy przy zakupie nowego sprzętu lub oddać go w wyznaczonych punktach zbiórki. Więcej informacji można znaleźć w serwisie: www.recyclethis.info.



2006/66/WE (dyrektywa w sprawie baterii): Ten produkt zawiera baterię, której w Unii Europejskiej nie wolno usuwać wraz z niesortowanymi odpadami komunalnymi. Dokładne informacje o użytej baterii są podane w dokumentacji produktu. Bateria jest oznaczona tym symbolem, któremu mogą towarzyszyć litery informujące o zawartości kadmu (Cd), ołowiu (Pb) lub rtęci (Hg). W celu prawidłowego recyklingu należy zwrócić baterię odpowiedniemu sprzedawcy lub oddać ją w wyznaczonym punkcie zbiórki. Więcej informacji można znaleźć w serwisie: www.recyclethis.info.

Zgodność z kanadyjską normą branżową ICES-003

Niniejsze urządzenie spełnia wymagania norm CAN ICES-3 (A)/NMB-3(A).



Instrukcje bezpieczeństwa

Celem tych instrukcji jest zapewnienie, że użytkownik będzie używał produktu w sposób prawidłowy, aby uniknąć niebezpieczeństwa i utraty mienia.

Środki ostrożności dzielą się na „Ostrzeżenia” i „Przestrogi”:

Ostrzeżenia: Zlekceważenie któregoś z tych ostrzeżeń może spowodować poważne obrażenia lub śmierć.

Przestrogi: Zlekceważenie którejś z tych przestróg może spowodować obrażenia lub uszkodzenie sprzętu.

	
Ostrzeżenia – Postępuj zgodnie z tymi środkami ostrożności, aby zapobiec poważnym obrażeniom lub śmierci.	Przestrogi Należy stosować te środki ostrożności, aby zapobiec możliwości powstania obrażeń ciała lub szkód materialnych.



Ostrzeżenia:

- Używaj zasilacza, który spełnia normę napięcia bezpiecznego (safety extra low voltage – SELV). Źródło zasilania powinno zapewniać napięcie 12 V DC lub 24 V AC (zależnie od modelu) zgodnie z normą IEC60950-1 i normą źródła z ograniczeniem prądowym (Limited Power Source).
- Aby ograniczyć ryzyko pożaru lub porażenia prądem, nie wystawiaj produktu na deszcz lub wilgoć.
- Instalację powinien przeprowadzić wykwalifikowany monter zgodnie ze wszystkimi lokalnymi przepisami.
- Zainstaluj w obwodzie zasilania sprzęt zabezpieczający przed nagłym spadkiem napięcia, aby zapobiec uszkodzeniom w razie zaniku zasilania.
- Upewnij się, że sufit jest w stanie wytrzymać siłę oddziaływania grawitacji ponad 50 niutonów, jeśli kamera jest montowana na suficie.
- Jeśli produkt nie działa prawidłowo, skontaktuj się ze sprzedawcą lub najbliższym centrum serwisowym. Nie próbuj rozmontowywać kamery samodzielnie. (Nie ponosimy odpowiedzialności za problemy spowodowane przez nieautoryzowaną naprawę lub konserwację).



Przestrogi:

- Przed rozpoczęciem eksploatacji kamery upewnij się, że napięcie zasilania jest prawidłowe.
- Nie upuszczaj kamery na ziemię ani jej nie uderzaj.
- Nie dotykaj modułów czujników palcami. Jeśli kamerę trzeba wyczyścić, przetrzyj ją delikatnie za pomocą czystej ściereczki lekko nasączonej etanolem. Jeśli kamera nie będzie używana przez dłuższy czas, nałóż zaślepkę na obiektyw, aby chronić czujnik przed zabrudzeniem.
- Nie kieruj obiektywu kamery na silne źródło światła, takie jak słońce lub żarówka. Silne światło może poważnie uszkodzić kamerę.
- Wiązka lasera może spalić czujnik, dlatego w przypadku korzystania z jakiegokolwiek sprzętu laserowego upewnij się, że laser nie padnie na czujnik.
- Nie umieszczaj kamery w bardzo wysokich i bardzo niskich temperaturach (temperatura robocza nie powinna przekraczać $-30\text{ °C} \sim 60\text{ °C}$ lub $-40\text{ °C} \sim 60\text{ °C}$, jeśli model kamery w sufiksie nazwy zawiera literę „H”), nie instaluj jej w zapyłonym lub wilgotnym środowisku, nie wystawiaj jej na działanie silnego promieniowania elektromagnetycznego.
- Aby uniknąć przegrzania, w odpowiednim środowisku eksploatacji należy zapewnić dobrą wentylację.
- Chronić kamerę przed wodą i innymi cieczami.
- Podczas transportu kamera powinien być zapakowana w oryginalne opakowanie.
- Nieprawidłowe użytkowanie lub wymiana baterii mogą grozić wybuchem. Używaj typu baterii zalecanego przez producenta.

Uwagi:

W przypadku kamer z obsługą podczerwieni, należy zwrócić uwagę na poniższe kwestie, aby zapobiec odbiciom światła podczerwonego:

- Pył i tłuszcz na pokrywie kopułki spowoduje odbicie podczerwieni. Nie zdejmuj folii chroniącej pokrywę kopułki, dopóki instalacja kamery nie zostanie zakończona. Jeśli pokrywa kopułki jest zanieczyszczona pyłem lub tłuszczem, wyczyść ją za pomocą miękkiej ściereczki nasączonej alkoholem izopropylowym.
- Upewnij się, że w miejscu instalacji nie ma zbyt blisko kamery przedmiotów, których powierzchnie odbijają światło. Podczerwień z kamery może się odbijać i świecić w obiektyw, co spowoduje zakłócenia spowodowane odbiciem.
- Pierścień z pianki naokoło obiektywu musi być osadzony na płask z wewnętrzną powierzchnią kopułki, aby odizolować obiektyw od diod podczerwonych. Przymocuj pokrywę kopułki do korpusu kamery tak, aby pierścień z pianki i

pokrywa kopułki były połączone bez żadnych nierówności.

Spis treści

Chapter 1	<i>Połączenie sieciowe</i>	13
1.1	Konfiguracja kamery sieciowej przez LAN	13
1.1.1	Połączenie za pośrednictwem sieci WAN.....	13
1.1.2	Aktywacja kamery.....	14
1.2	Konfiguracja kamery sieciowej przez WAN	20
1.2.1	Połączenie przy użyciu statycznego adresu IP.....	20
1.2.2	Połączenie przy użyciu dynamicznego adresu IP.....	22
Chapter 2	<i>Dostęp do kamery sieciowej</i>	25
2.1	Dostęp za pomocą przeglądarki internetowej	25
2.2	Dostęp przy użyciu oprogramowania klienta	27
Chapter 3	<i>Ustawienia Wi-Fi</i>	29
3.1	Konfiguracja połączenia Wi-Fi w trybie zarządzania i Ad-hoc	29
3.2	Łatwe połączenie Wi-Fi przy użyciu funkcji WPS	34
3.3	Ustawienia właściwości IP dla połączenia z siecią bezprzewodową	36
Chapter 4	<i>Podgląd na żywo</i>	38
4.1	Strona podglądu na żywo	38
4.2	Uruchamianie podglądu na żywo	39
4.3	Ręczne nagrywanie i robienie zdjęć	40
4.4	Obsługa sterowania PTZ	40
4.4.1	Panel sterowania PTZ.....	41
4.4.2	Ustawianie/wywoływanie ustawienia wstępnego	42
4.4.3	Ustawianie/wywoływanie patrolu	43
Chapter 5	<i>Konfiguracja kamery sieciowej</i>	44
5.1	Konfiguracja lokalnych parametrów	44
5.2	Konfiguracja ustawień czasu	46
5.3	Konfiguracja ustawień sieci	48
5.3.1	Konfiguracja ustawień TCP/IP	48
5.3.2	Konfiguracja ustawień portów	50
5.3.3	Konfiguracja ustawień PPPoE.....	50
5.3.4	Konfiguracja ustawień DDNS	51
5.3.5	Konfiguracja ustawień SNMP	55
5.3.6	Konfiguracja ustawień 802.1X.....	56
5.3.7	Konfiguracja ustawień QoS	58
5.3.8	Konfiguracja ustawień UPnP™	59
5.3.9	Konfiguracja bezprzewodowego wybierania numeru.....	59

5.3.10	Wysyłanie e-maila wyzwolonego przez alarm.....	63
5.3.11	Konfiguracja ustawień NAT (Network Address Translation – translacja adresów sieciowych).....	65
5.3.12	Konfiguracja ustawień FTP	66
5.3.13	Dostęp do platformy	67
5.3.14	Ustawienia HTTPS	68
5.4	Konfiguracja ustawień wideo i audio	70
5.4.1	Konfiguracja ustawień wideo	70
5.4.2	Konfiguracja ustawień audio.....	73
5.4.3	Konfiguracja kodowania ROI	74
5.4.4	Wyświetlanie informacji na strumieniu	76
5.4.5	Konfiguracja przycinania celu	76
5.5	Konfigurowanie parametrów obrazu.....	77
5.5.1	Konfigurowanie ustawień wyświetlania	77
5.5.2	Konfiguracja ustawień OSD.....	84
5.5.3	Konfiguracja ustawień tekstu na obrazie	85
5.5.4	Konfiguracja maski prywatności	86
5.5.5	Konfiguracja nakładania obrazów	87
5.6	Konfiguracja i obsługa alarmów	88
5.6.1	Konfiguracja wykrywania ruchu.....	89
5.6.2	Konfiguracja alarmu o próbie manipulacji wideo	95
5.6.3	Konfiguracja wejścia alarmowego	97
5.6.4	Konfiguracja wyjścia alarmowego.....	98
5.6.5	Obsługa wyjątków.....	99
5.6.6	Konfiguracja innego alarmu	100
5.6.7	Konfiguracja wykrywania wyjątku audio	103
5.6.8	Konfiguracja wykrywania utraty ostrości	104
5.6.9	Konfiguracja wykrywania zmiany sceny.....	105
5.6.10	Konfiguracja wykrywania twarzy	107
5.6.11	Konfiguracja wykrywania przekroczenia linii	108
5.6.12	Konfiguracja wykrywania wtargnięcia.....	110
5.6.13	Konfiguracja wykrywania wejścia w obszar	112
5.6.14	Konfiguracja wykrywania wyjścia z obszaru.....	113
5.6.15	Konfiguracja wykrywania bagażu bez nadzoru	115
5.6.16	Konfiguracja wykrywania usunięcia obiektów	117
5.7	Konfiguracja VCA	118
5.7.1	Analiza zachowań.....	118
5.7.2	Rejestracja twarzy.....	127
5.7.3	Kolorowa mapa danych.....	131
5.7.4	Liczenie osób.....	134
Chapter 6	<i>Ustawienia pamięci masowej.....</i>	137
6.1	Konfiguracja ustawień NAS.....	137

6.2	Konfiguracja harmonogramu nagrywania	139
6.3	Konfiguracja ustawień zrzutu ekranu	144
6.4	Konfiguracja Lite Storage	146
6.5	Konfiguracja przechowywania w chmurze.....	147
<i>Chapter 7</i>	<i>Liczenie</i>	<i>149</i>
<i>Chapter 8</i>	<i>Ruch drogowy</i>	<i>153</i>
<i>Chapter 9</i>	<i>Odtwarzanie</i>	<i>157</i>
<i>Chapter 10</i>	<i>Przeszukiwanie dziennika</i>	<i>159</i>
<i>Chapter 11</i>	<i>Inne</i>	<i>161</i>
11.1	Zarządzanie kontami użytkowników	161
11.2	Autoryzacja.....	163
11.3	Anonymous Visit (Wizyta anonimowa).....	164
11.4	Filtr adresów IP.....	165
11.5	Funkcje bezpieczeństwa	167
11.6	Wyświetlanie informacji o urządzeniu.....	167
11.7	Konserwacja	168
11.7.1	Ponowne uruchamianie kamery	168
11.7.2	Przywracanie ustawień domyślnych.....	169
11.7.3	Eksport/import pliku konfiguracji	169
11.7.4	Aktualizacja systemu	170
11.8	Ustawienia RS-232	171
11.9	Ustawienia RS-485	172
11.10	Ustawienia usług.....	172
Załącznik	174
	Załącznik 1 – Wprowadzenie do oprogramowania SADP	174
	Załącznik 2 – Mapowanie portów	177

Wymagania systemowe

System operacyjny: Microsoft Windows XP SP1 i nowsze wersje / Vista / Win7 /

Server 2003 / Server 2008 32-bitowy

CPU: Intel Pentium IV 3.0 GHz lub wyższy

RAM 1 GB lub więcej

Wyświetlacz: Rozdzielczość 1024×768 lub większa

Przeglądarka internetowa: Internet Explorer 6.0 i nowsze wersje, Apple Safari 5.02 i

nowsze wersje, Mozilla Firefox 3.5 i nowsze wersje, Google Chrome 8 i nowsze wersje.

Chapter 1 Połączenie sieciowe

Uwaga:

- Użytkownik przyjmuje do wiadomości i potwierdza, że korzystanie z produktu z dostępem do Internetu może oznaczać zagrożenie dla bezpieczeństwa sieci. Aby uniknąć ataków sieciowych i wycieku informacji, użytkownik powinien wzmocnić zabezpieczenia sieci. Jeśli produkt nie działa prawidłowo, skontaktuj się ze sprzedawcą lub najbliższym centrum serwisowym.
- Aby zapewnić bezpieczeństwo sieciowe kamery sieciowej, zalecamy jej regularne sprawdzanie i konserwację. Prosimy o kontakt w razie konieczności obsługi serwisowej.

Przed rozpoczęciem pracy:

- Aby skonfigurować kamerę sieciową za pośrednictwem sieci lokalnej (LAN), zapoznaj się z *Sekcją 2.1 Konfiguracja kamery sieciowej przez LAN*.
- Aby skonfigurować kamerę sieciową za pośrednictwem sieci rozległej (WAN), zapoznaj się z *Sekcją 2.2 Konfiguracja kamery sieciowej przez WAN*.

1.1 Konfiguracja kamery sieciowej przez LAN

Cel:

Aby wyświetlać obraz z kamery sieciowej i konfigurować ją przez LAN, musisz podłączyć ją do tej samej podsieci, do której jest podłączony komputer, i zainstalować SADP lub oprogramowanie iVMS-4200 w celu wyszukiwania i zmiany IP kamery sieciowej.

Uwaga: Szczegółowe wprowadzenie do SADP znajduje się w Załączniku 1.

1.1.1 Połączenie za pośrednictwem sieci WAN

Na poniższych rysunkach przedstawiono dwa sposoby połączenia kablowego kamery sieciowej i komputera:

Cel:

- Aby przetestować kamerę sieciową, możesz bezpośrednio połączyć ją z komputerem za pomocą kabla sieciowego, jak pokazano na Ilustracji 2-1.
- Na Ilustracji 2-2 zamieszczono informacje, jak skonfigurować kamerę sieciową przez LAN przy użyciu switcha lub routera.

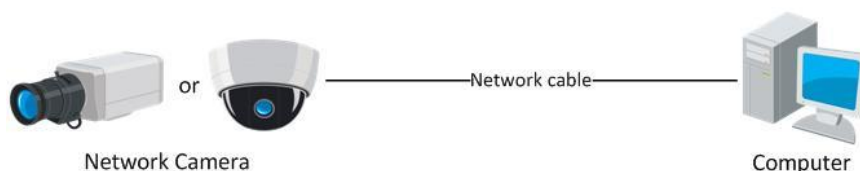


Figure 1-1 Połączenie bezpośrednie

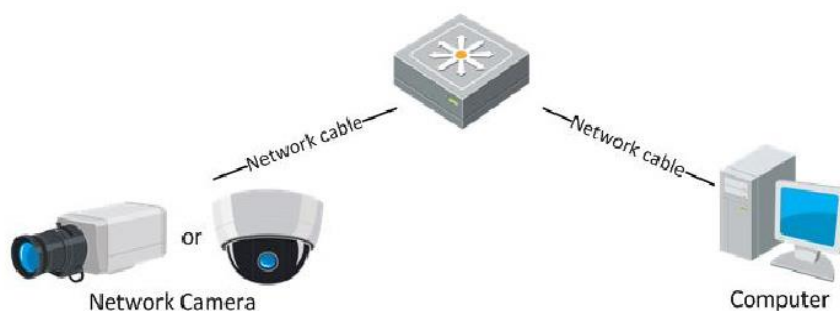


Figure 1-2 Połączenie przy użyciu switcha lub routera

1.1.2 Aktywacja kamery

Przed rozpoczęciem eksploatacji kamery trzeba ją aktywować, ustawiając dla niej silne hasło.

Możliwa jest aktywacja przez przeglądarkę internetową, SADP i oprogramowanie klienta.

❖ Aktywacja za pomocą przeglądarki internetowej

Kroki:

1. Włącz kamerę i podłącz ją do sieci.
2. Wpisz adres IP w pasku adresu przeglądarki i naciśnij Enter, aby przejść do interfejsu aktywacji.

Uwagi:

- Domyślny adres IP kamery to 192.168.1.64.
- Aby kamera domyślnie włączała DHCP, trzeba ją aktywować za pomocą

oprogramowania SADP. Zapoznaj się z kolejnym rozdziałem, aby uzyskać informacje na temat aktywacji przez SADP.

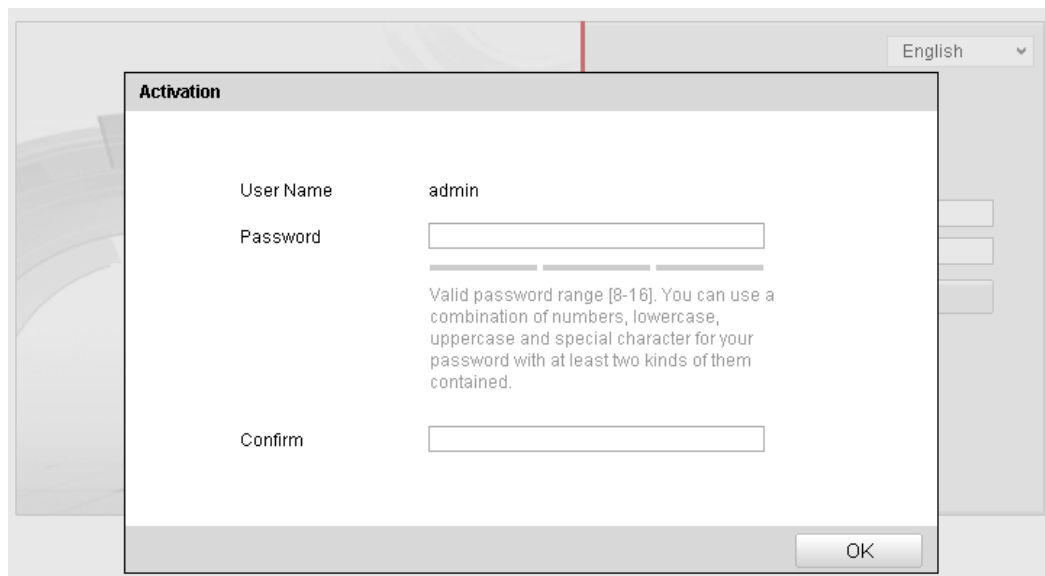


Figure 1-3 Interfejs aktywacji (WWW)

3. Stwórz hasło i wpisz je w polu Password (Hasło).



ZAŁECAMY SILNE HASŁO– Zdecydowanie zalecamy stworzenie silnego hasła wybranego przez siebie (co najmniej 8 znaków, wielkie i małe litery, cyfry i znaki specjalne), aby zwiększyć bezpieczeństwo produktu. Zalecamy również regularne zmiany hasła, szczególnie w przypadkach systemów o dużych wymaganiach w zakresie bezpieczeństwa. Zmiana hasła co miesiąc lub co tydzień umożliwia lepsze zabezpieczenie produktu.

4. Potwierdź hasło.

5. Kliknij OK, aby zapisać hasło i przejść do interfejsu podglądu na żywo.

❖ **Aktywacja za pomocą oprogramowania SADP**

Oprogramowanie SADP służy do wykrywania urządzenia online, aktywowania kamery i resetowania hasła.

Oprogramowanie SADP znajduje się na dołączonej płycie lub można je pobrać z oficjalnej witryny internetowej. Zainstaluj je zgodnie z instrukcjami wyświetlanymi na ekranie. Wykonaj kroki, aby aktywować kamerę.

Kroki:

1. Uruchom oprogramowanie SADP, aby wyszukać urządzenia online.
2. Sprawdź stan urządzenia na liście urządzeń i wybierz nieaktywne urządzenie.

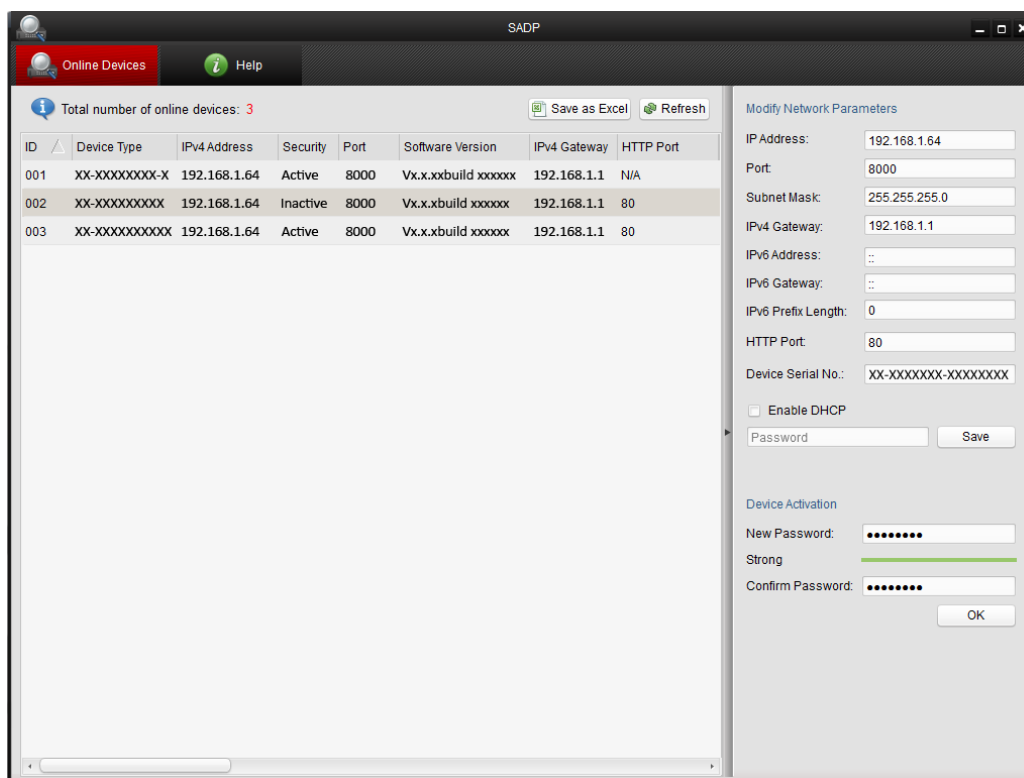


Figure 1-4 Interfejs SADP

3. Stwórz hasło, wpisz je w polu hasła i potwierdź hasło.



ZALECANE JEST SILNE HASŁO– Aby zwiększyć bezpieczeństwo produktu, zdecydowanie zalecamy stworzenie silnego własnego hasła (składającego się przynajmniej z 8 znaków, zawierającego wielkie i małe litery, cyfry i znaki specjalne). Zalecamy również regularne zmiany hasła, szczególnie w przypadkach systemów o dużych wymaganiach w zakresie bezpieczeństwa. Zmiana hasła co miesiąc lub co tydzień umożliwia lepsze zabezpieczenie produktu.

4. Kliknij **OK**, aby zapisać hasło.

Wyskakujące okno potwierdza zakończenie aktywacji. Jeśli aktywacja się nie uda, upewnij się, że hasło spełnia wymagania jego tworzenia i spróbuj jeszcze raz.

5. Zmień adres IP urządzenia na taki, który należy do tej samej podsieci, co komputer.
W tym celu wpisz adres IP ręcznie lub zaznacz pole wyboru Enable DHCP (Włącz DHCP).

Modify Network Parameters

IP Address: 192.168.1.64

Port: 8000

Subnet Mask: 255.255.255.0

IPv4 Gateway: 192.168.1.1

IPv6 Address: ::

IPv6 Gateway: ::

IPv6 Prefix Length: 0

HTTP Port: 80

Device Serial No.: XX-XXXXXXX-XXXXXXX

Enable DHCP

Password Save

Figure 1-5 Modyfikacja adresu IP

6. Wpisz hasło i kliknij przycisk **Save** (Zapisz), aby aktywować modyfikację adresu IP.

❖ Aktywacja za pomocą oprogramowania klienta

Oprogramowanie klienta to wielofunkcyjne oprogramowanie do zarządzania wideo, przeznaczone do obsługi wielu rodzajów urządzeń.

Oprogramowanie klienta znajduje się na dołączonej płycie lub można je pobrać z oficjalnej witryny internetowej. Zainstaluj je zgodnie z instrukcjami wyświetlanymi na ekranie. Wykonaj kroki, aby aktywować kamerę.

Kroki:

1. Uruchom oprogramowanie klienta. Wyświetli się panel sterowania oprogramowania, taki jak na ilustracji poniżej.

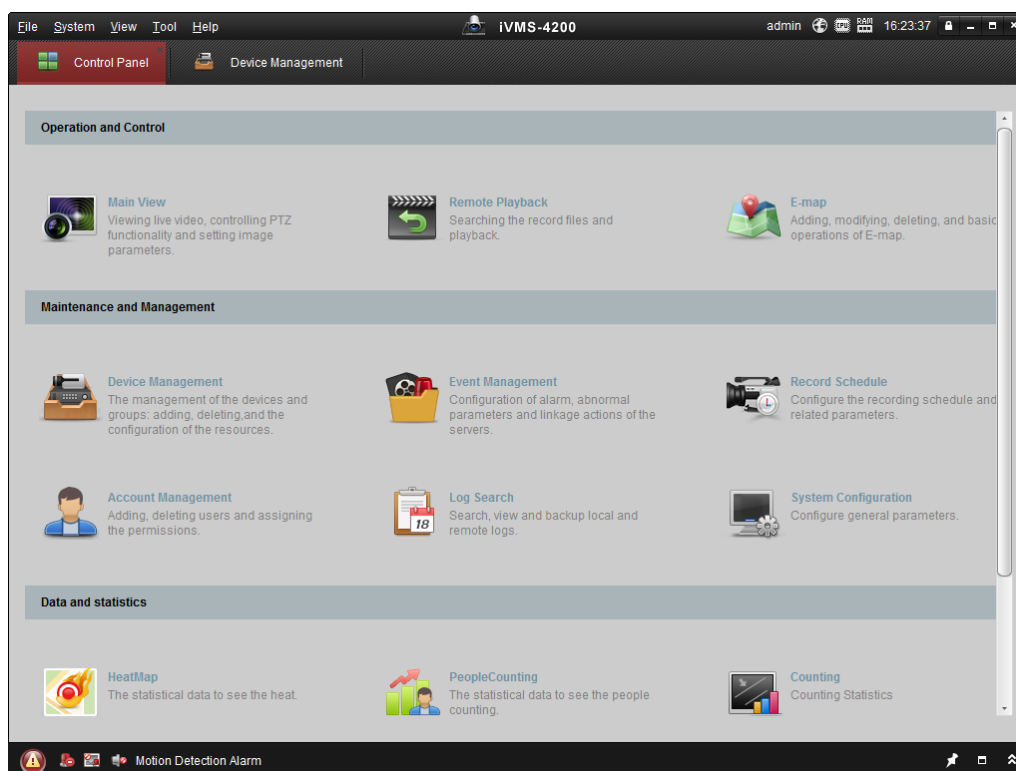


Figure 1-6 Panel sterowania

2. Kliknij ikonę **Device Management** (Zarządzanie urządzeniami), aby przejść do interfejsu zarządzania urządzeniami, jak na ilustracji poniżej.

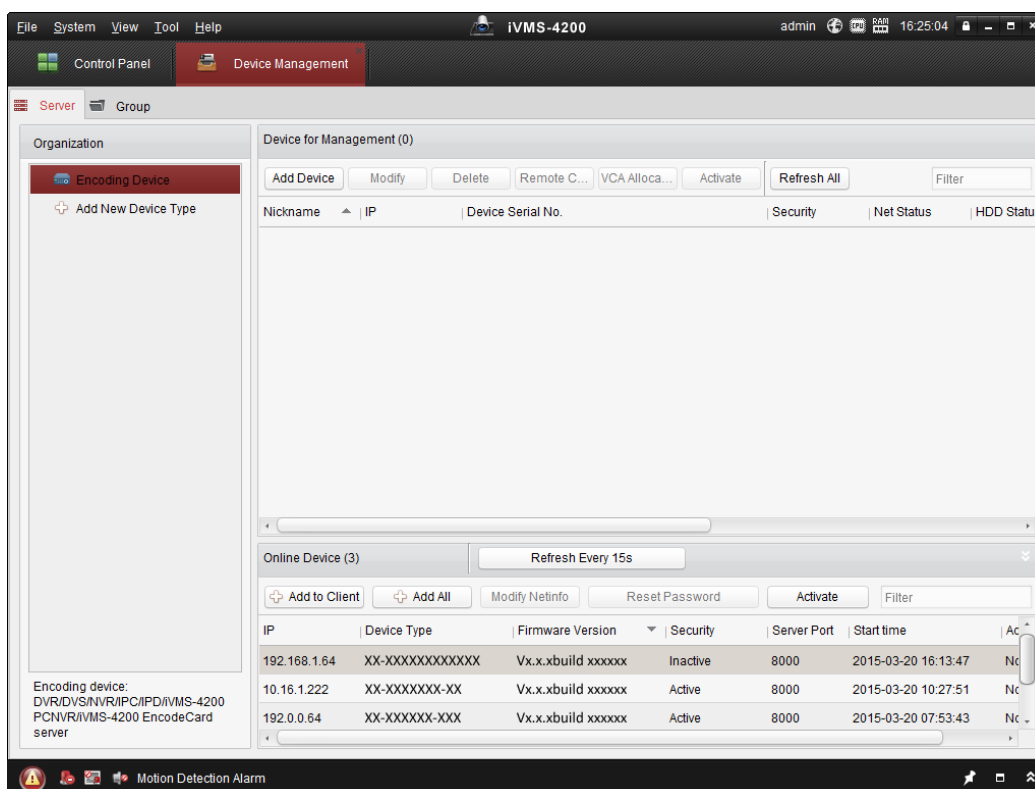


Figure 1-7 Interfejs zarządzania urządzeniami

3. Sprawdź stan urządzenia na liście urządzeń i wybierz nieaktywne urządzenie.
4. Kliknij przycisk **Activate** (Aktywuj), aby wyświetlić interfejs Activation (Aktywacja).
5. Stwórz hasło, wpisz je w polu hasła i potwierdź hasło.



ZALECANE JEST SILNE HASŁO– Aby zwiększyć bezpieczeństwo produktu, zdecydowanie zalecamy stworzenie silnego własnego hasła (składającego się przynajmniej z 8 znaków, zawierającego wielkie i małe litery, cyfry i znaki specjalne). Zalecamy regularną zmianę hasła, szczególnie w systemach o zwiększonym poziomie bezpieczeństwa. Zmiana hasła co miesiąc lub co tydzień przyczynia się do lepszego zabezpieczenia produktu.

Figure 1-8 Interfejs aktywacji (oprogramowanie klienta)

6. Kliknij przycisk **OK**, aby rozpocząć aktywację.
7. Kliknij przycisk **Modify Netinfo** (Modyfikuj informacje sieciowe), aby przejść do interfejsu modyfikacji parametrów sieci, jak na ilustracji poniżej.

1. Podłącz kamerę sieciową do routera.
2. Przypisz jej adres IP, maskę podsieci i bramę LAN. Szczegółowe informacje na temat konfiguracji adresu IP kamery sieciowej znajdują się w Sekcji 2.1.2.
3. Zapisz statyczny IP w routerze.
4. Skonfiguruj mapowanie portów, np. 80, 8000 i 554. Kroki mapowania portów różnią się w zależności od modelu routera. Skontaktuj się z producentem routera, aby uzyskać pomoc w zakresie mapowania portów.

Uwaga: Szczegółowe informacje na temat mapowania portów znajdują się w Załączniku 2.

5. Przejdź do interfejsu kamery sieciowej przez przeglądarkę internetową lub oprogramowanie klienta przez Internet.

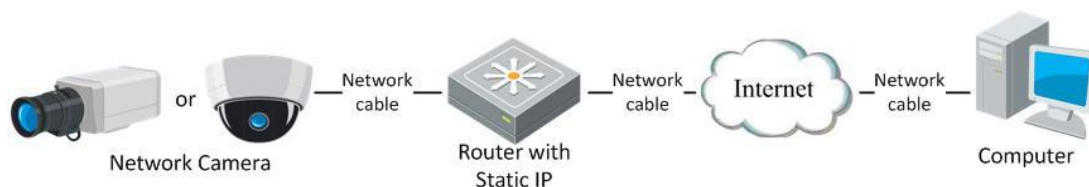


Figure 1-10 Uzyskiwanie dostępu do kamery przez router przy użyciu statycznego adresu IP

- **Bezpośrednie podłączenie kamery sieciowej przy użyciu statycznego adresu IP**

Stacyjny adres IP można też zapisać w kamerze i połączyć się z nią bezpośrednio przez Internet, bez konieczności używania routera. Szczegółowe informacje na temat konfiguracji adresu IP kamery sieciowej znajdują się w Sekcji 2.1.2.

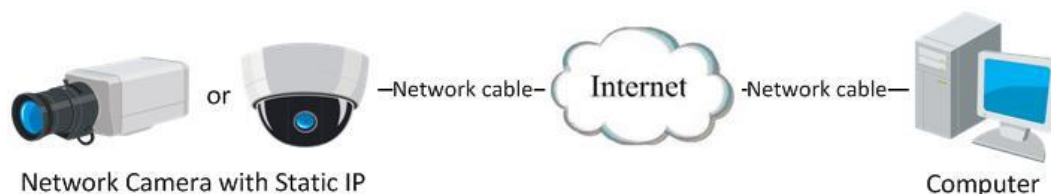


Figure 1-11 Bezpośrednie uzyskanie dostępu do kamery przy użyciu statycznego adresu IP

1.2.2 Połączenie przy użyciu dynamicznego adresu IP

Przed rozpoczęciem pracy:

Użyj dynamicznego adresu IP przyznanego przez operatora Internetu (Internet Service Provider – ISP). Przy użyciu dynamicznego adresu IP możesz podłączyć kamerę sieciową do modemu lub routera.

● **Podłączanie kamery sieciowej przez router**

Kroki:

1. Podłącz kamerę sieciową do routera.
2. W kamerze przypisz jej adres IP, maskę podsieci i bramę LAN. Szczegółowe informacje na temat konfiguracji adresu IP kamery sieciowej znajdują się w Sekcji 2.1.2.
3. W routerze ustaw nazwę użytkownika PPPoE, wpisz hasło i potwierdzenie hasła.
4. Skonfiguruj mapowanie portów. Np. 80, 8000 i 554. Kroki mapowania portów różnią się w zależności od modelu routera. Skontaktuj się z producentem routera, aby uzyskać pomoc w zakresie mapowania portów.

Uwaga: Szczegółowe informacje na temat mapowania portów znajdują się w Załączniku 2.

5. Złóż u dostawcy nazw domenowych wnioski o nazwę domenową.
6. Skonfiguruj ustawienia DDNS w interfejsie konfiguracji routera.
7. Otwórz stronę WWW kamery przy użyciu otrzymanej nazwy domenowej.

● **Podłączanie kamery sieciowej przez modem**

Cel:

Kamera obsługuje funkcję wdzwaniania automatycznego PPPoE. Kamera uzyskuje publiczny adres IP poprzez usługę wdzwaniania ADSL, gdy zostanie podłączona do modemu. Użytkownik musi skonfigurować parametry PPPoE kamery sieciowej. Szczegółowe informacje na temat konfiguracji znajdują się w *Sekcji 6.3.3*

Konfiguracja ustawień PPPoE.

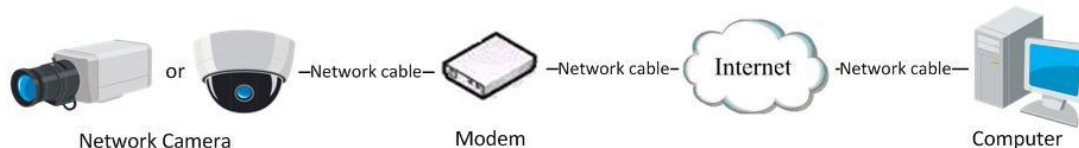


Figure 1-12 Uzyskanie dostępu do kamery przy użyciu dynamicznego adresu IP

Uwaga: Uzyskany adres IP jest dynamicznie przydzielany przez PPPoE, dlatego po ponownym uruchomieniu zawsze się zmienia. Aby rozwiązać problemy z dynamicznym adresem IP, należy uzyskać nazwę domenową od dostawcy DDNS (np. DynDns.com). Wykonaj poniższe kroki w celu rozwiązywania normalnych nazw domenowych i rozwiązywania prywatnych nazw domenowych, aby rozwiązać problem.

◆ Rozwiązywanie normalnych nazw domenowych

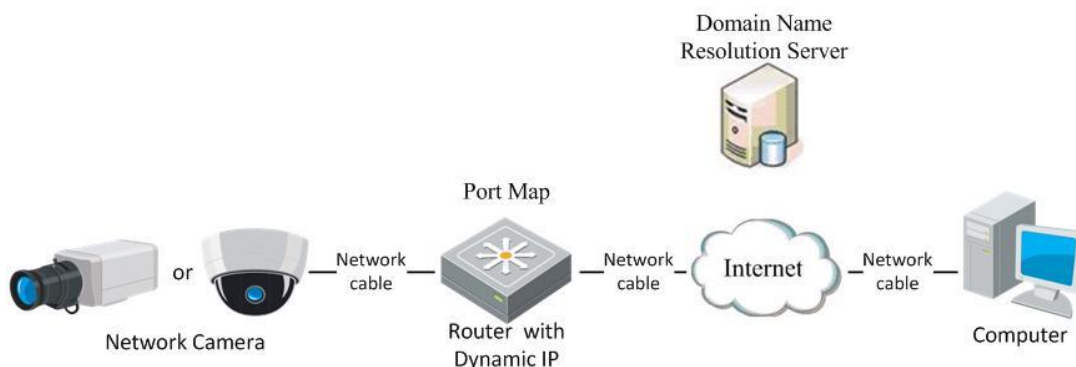


Figure 1-13 Rozwiązywanie normalnych nazw domenowych

Kroki:

1. Złóż u dostawcy nazw domenowych wnioski o nazwę domenową.
2. Skonfiguruj ustawienia DDNS w interfejsie **DDNS Settings** (Ustawienia DDNS) kamery sieciowej. Szczegółowe informacje na temat konfiguracji znajdują się w *Sekcji 6.3.4 Konfiguracja ustawień DDNS*.
3. Otwórz stronę WWW kamery przy użyciu otrzymanej nazwy domenowej.

◆ Rozwiązywanie prywatnych nazw domenowych

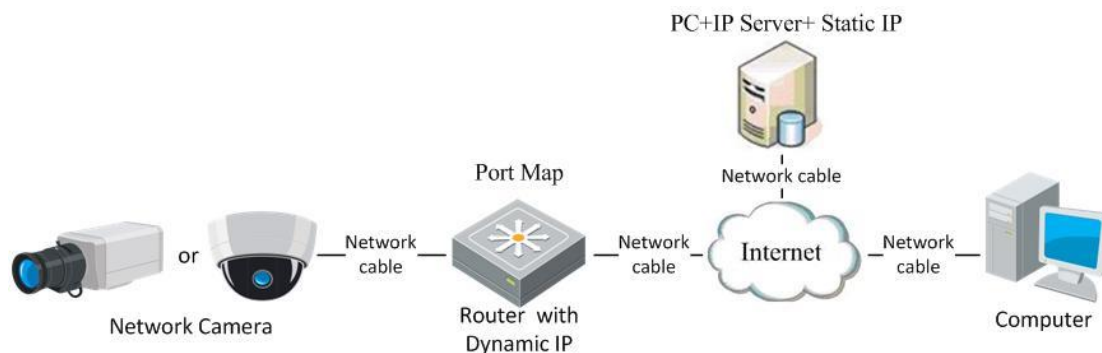


Figure 1-14 Rozwiązywanie prywatnych nazw domenowych

Kroki:

1. Zainstaluj i uruchom oprogramowanie serwera IP na komputerze ze statycznym adresem IP.
2. Otwórz interfejs kamery sieciowej przez LAN za pomocą przeglądarki internetowej lub oprogramowania klienta.
3. Włącz DDNS, a jako typ protokołu wybierz Serwer IP. Szczegółowe informacje na temat konfiguracji znajdują się w *Sekcji 6.3.4 Konfiguracja ustawień DDNS*.

Chapter 2 Dostęp do kamery sieciowej

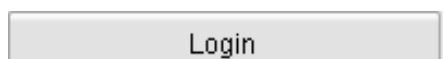
2.1 Dostęp za pomocą przeglądarki internetowej

Kroki:

1. Uruchom przeglądarkę internetową.
2. W pasku adresu przeglądarki wprowadź adres IP kamery sieciowej, a następnie naciśnij przycisk **Enter**, aby przejść do interfejsu logowania.
3. Szczegółowe informacje na temat aktywacji kamery sieciowej przed jej pierwszym użyciem znajdują się w sekcji 2.1.2.

Uwaga:

- Domyślny adres IP to 192.168.1.64.
 - Jeśli kamera nie jest aktywna, najpierw ją aktywuj, zgodnie z Rozdziałem 3.1 lub Rozdziałem 3.2.
4. Jako język interfejsu wybierz Polski (jeśli jest dostępny, w przeciwnym razie English (Angielski)) w prawym górnym rogu interfejsu logowania
 5. Wprowadź nazwę użytkownika i hasło, a następnie kliknij



Administrator powinien prawidłowo skonfigurować konta urządzeń i uprawnienia użytkowników/operatorów. Usuń niepotrzebne konta i uprawnienia użytkowników/operatorów.

Uwaga:

Adres IP urządzenia zostanie zablokowany, jeśli administrator wykona 7 nieudanych prób logowania (5 prób w przypadku użytkownika/operatora).

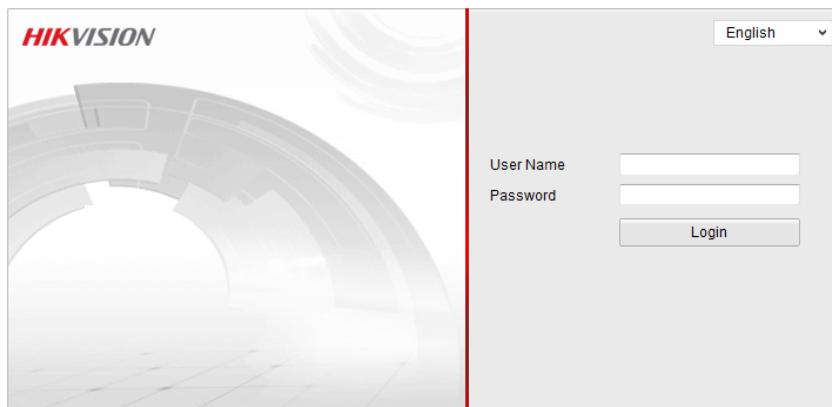


Figure 2-1 Interfejs logowania

6. Przed wyświetlaniem podglądu na żywo i obsługą kamery zainstaluj wtyczkę. Wykonaj pokazywane na ekranie instrukcje, aby zainstalować wtyczkę.

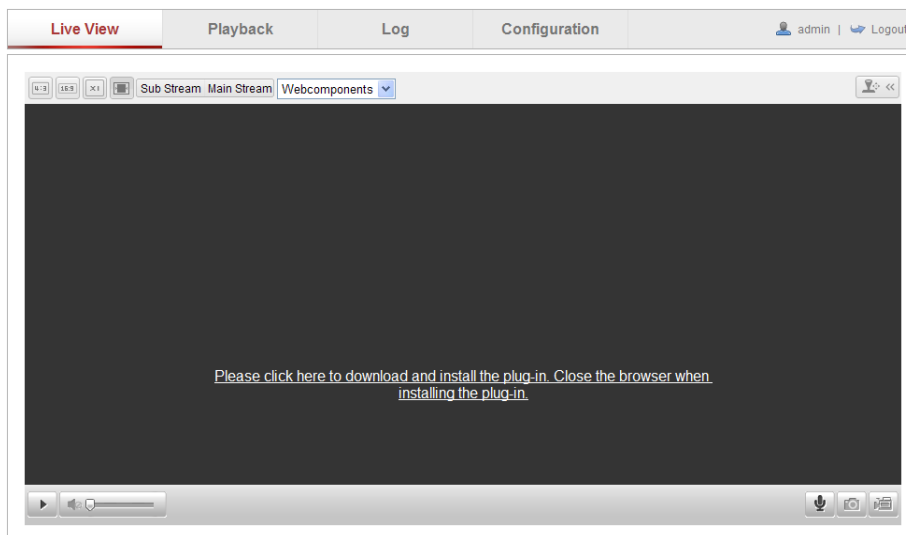


Figure 2-2 Pobierz i zainstaluj wtyczkę

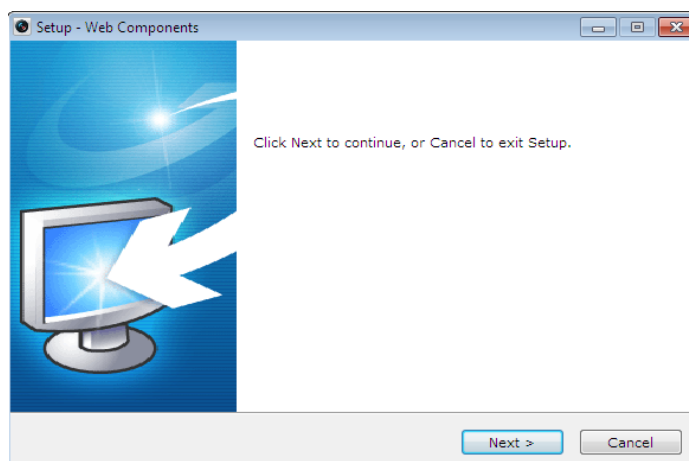


Figure 2-3 Zainstaluj wtyczkę (1)

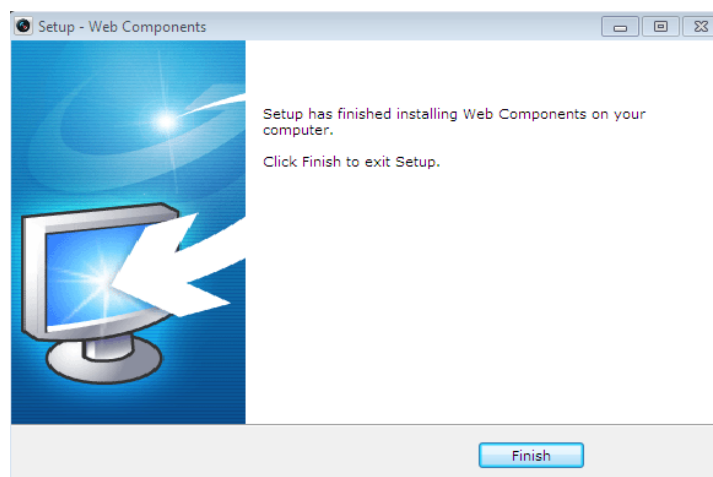


Figure 2-4 Zainstaluj wtyczkę (2)

Uwaga: Aby zainstalować wtyczkę, być może trzeba będzie zamknąć przeglądarkę. Po zainstalowaniu wtyczki otwórz przeglądarkę jeszcze raz i się zaloguj.

2.2 Dostęp przy użyciu oprogramowania klienta

Na płycie CD znajduje się oprogramowanie klienta iVMS-4200. Dzięki temu oprogramowaniu możliwe jest wyświetlanie podglądu na żywo i zarządzanie kamerą. Wykonaj pokazywane na ekranie instrukcje, aby zainstalować oprogramowanie. Poniżej pokazano panel sterowania i interfejs podglądu na żywo oprogramowania klienta iVMS-4200.

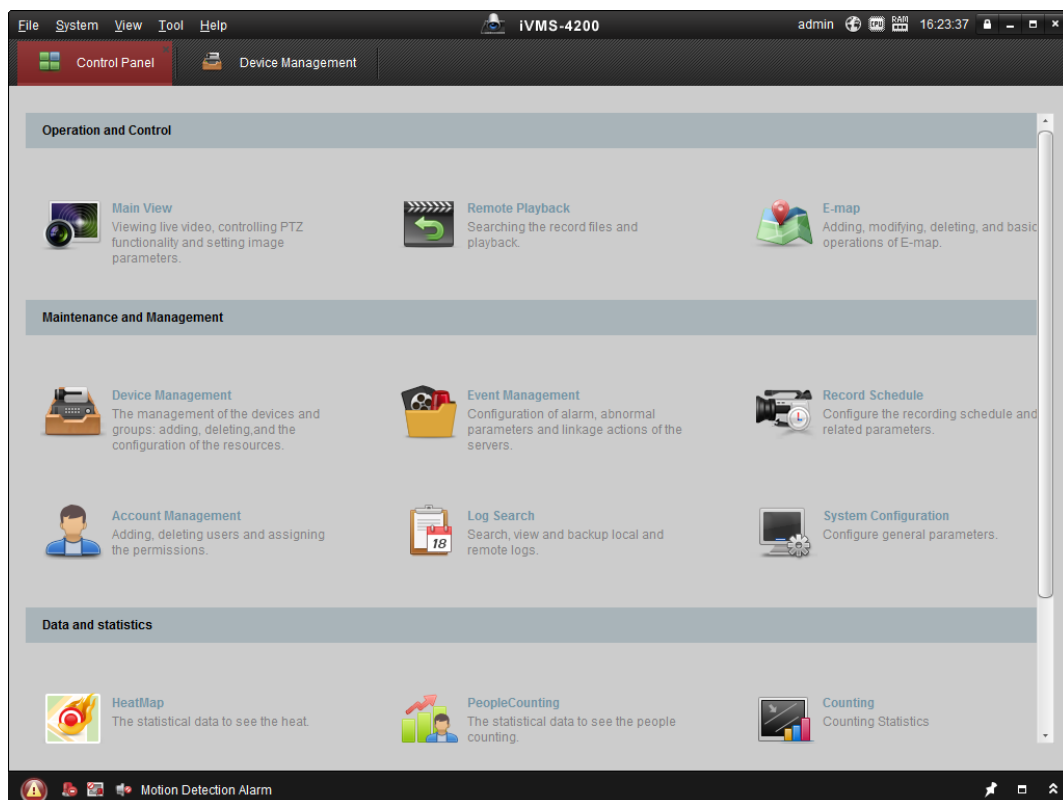


Figure 2-5 Panel sterowania iVMS-4200

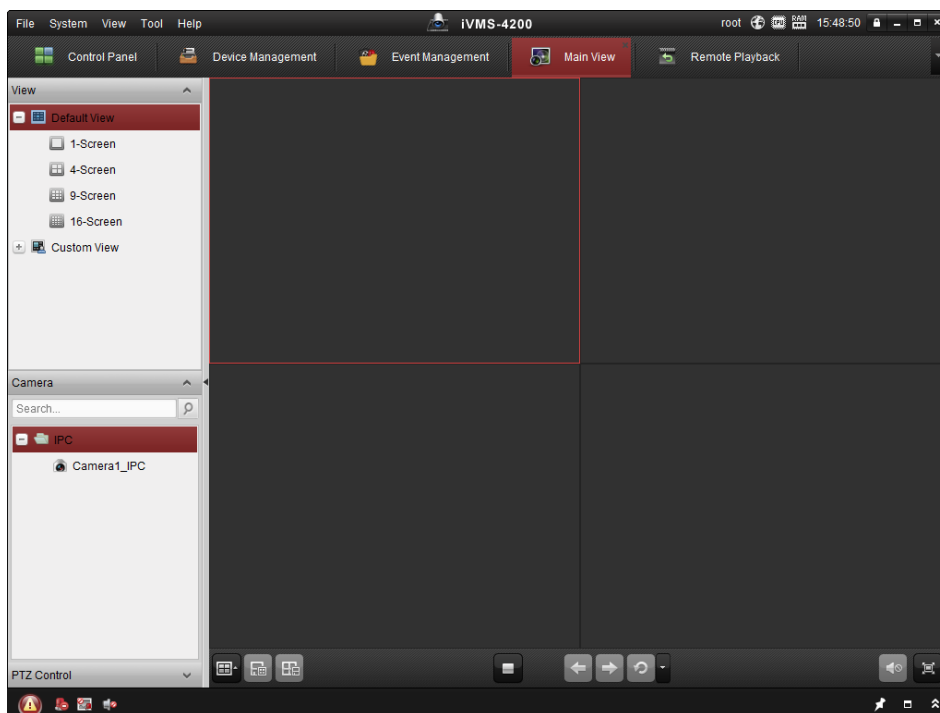


Figure 2-6 Widok główny iVMS-4200

Uwaga: Aby uzyskać szczegółowe informacje na temat oprogramowania, należy się zapoznać z instrukcją obsługi iVMS-4200.

Chapter 3 Ustawienia Wi-Fi

Cel:

Dzięki sieci bezprzewodowej nie trzeba stosować kabli, aby połączyć kamerę z siecią.

Z punktu widzenia monitoringu jest to niezwykle korzystne rozwiązanie.

Uwaga: Ten rozdział dotyczy wyłącznie kamer z wbudowanym modułem Wi-Fi.

3.1 Konfiguracja połączenia Wi-Fi w trybie zarządzania i Ad-hoc

Przed rozpoczęciem pracy:

Musi być skonfigurowana sieć bezprzewodowa.

Połączenie bezprzewodowe w trybie zarządzania

Kroki:

1. Otwórz interfejs konfiguracji Wi-Fi.

Configuration> Advanced Configuration> Network> Wi-Fi (Konfiguracja > Konfiguracja zaawansowana > Sieć > Wi-Fi)

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

Figure 3-1 Lista sieci bezprzewodowych

2. Kliknij **Search** (Wyszukaj), aby wyszukać dostępne online połączenia bezprzewodowe.
3. Kliknij, aby wybrać z listy połączenie bezprzewodowe.

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

Figure 3-2 Konfiguracja Wi-Fi – Tryb zarządzania

4. Zaznacz pole wyboru, aby wybrać *Network Mode* (Tryb sieci) jako *Manage* (Zarządzania), *Security mode* (Tryb zabezpieczeń) wyświetla się automatycznie po wybraniu sieci bezprzewodowej, nie należy go zmieniać ręcznie.

Uwaga: Te parametry są identyczne z parametrami routera.

5. Wpisz klucz, aby się połączyć z siecią bezprzewodową. Użyj klucza połączenia z siecią bezprzewodową ustawionego na routerze.

Połączenie bezprzewodowe w trybie Ad-hoc

W przypadku trybu Ad-hoc nie trzeba podłączać kamery bezprzewodowej przez router. Scenariusz jest taki sam, jak w przypadku bezpośredniego połączenia kamery i komputera kablem sieciowym.

Kroki:

1. Wybierz tryb Ad-hoc.

The screenshot shows a configuration window for Wi-Fi. The 'Wi-Fi' section is highlighted. The 'SSID' field contains 'camera6467wifi'. The 'Network Mode' section has two radio buttons: 'Manager' (unselected) and 'Ad-Hoc' (selected). The 'Security Mode' dropdown menu is open, showing 'not-encrypted' as the selected option.

Figure 3-3 Ustawienia Wi-Fi – Ad-hoc

2. Wybierz SSID dla kamery.
3. Wybierz Security Mode (Tryb zabezpieczeń) połączenia bezprzewodowego.

The screenshot shows the 'Security Mode' dropdown menu expanded. The options listed are: 'not-encrypted', 'not-encrypted', 'WEP', 'WPA-personal', 'WPA-enterprise', 'WPA2-personal', and 'WPA2-enterprise'. The 'not-encrypted' option is highlighted in blue. Below the dropdown, the 'WPS' section is visible with an unchecked checkbox for 'Enable WPS'.

Figure 3-4 Tryb zabezpieczeń – Tryb Ad-hoc

4. Włącz funkcję połączenia bezprzewodowego w komputerze.
5. Wyszukaj sieć w komputerze, na liście znalezionych sieci wyświetli się SSID kamery.



Figure 3-5 Punkt połączenia Ad-hoc

6. Wybierz SSID i połącz kamerę z komputerem.

Opis trybu zabezpieczeń:

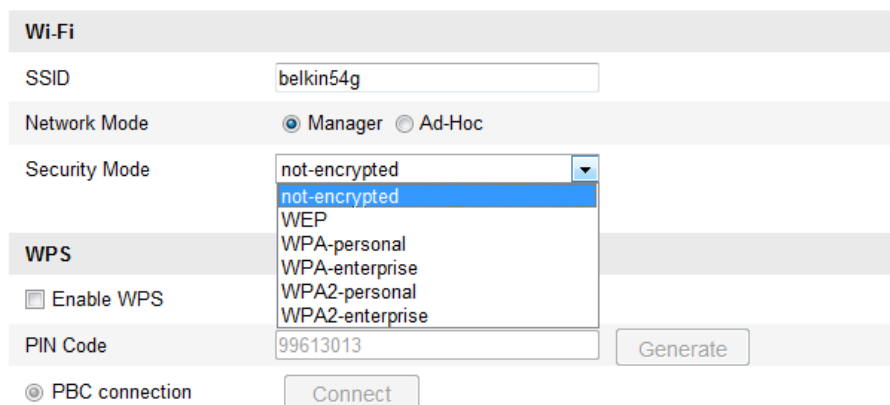


Figure 3-6 Tryb zabezpieczeń

Wybierz jeden z trybów zabezpieczeń: not-encrypted (bez szyfrowania), WEP, WPA-personal, WPA-enterprise, WPA2-personal i WPA2-enterprise.

Tryb WEP:

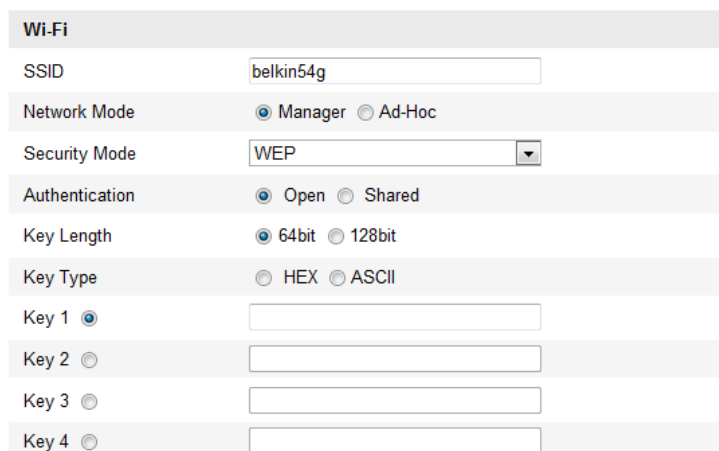


Figure 3-7 Tryb WEP

- Authentication (Uwierzytelnianie) – wybierz system uwierzytelniania Open (za

pomocą systemu otwartego) lub Shared (za pomocą klucza współdzielonego), zależnie od metody, jakiej używa punkt dostępowy. Ta opcja nie jest dostępna w każdym punkcie dostępowym. W takim przypadku prawdopodobnie korzystają z systemu otwartego, zwanego też uwierzytelnianiem otwartym lub uwierzytelnianiem SSID.

- *Key length* (Długość klucza) – Wyznacza ona długość klucza używanego do szyfrowania bezprzewodowego, może być 64-bitowa lub 128-bitowa. Długość klucza szyfrowania czasami może mieć postać 40/64 i 104/128.
- *Key type* (Typ klucza) – Typy klucza zależą od używanego punktu dostępowego. Dostępne są następujące opcje:

HEX – Pozwala na ręczne wpisanie klucza w formacie szesnastkowym.

ASCII – Ta metoda wymaga podania ciągu dokładnie 5 znaków dla 64-bitowego WEP i 13 znaków dla 128-bitowego WEP.

Tryb WPA-personal i WPA2-personal:

Wpisz wymagany klucz współdzielony punktu dostępowego, może on mieć postać numeru szesnastkowego lub hasła.

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

Figure 3-8 Tryb zabezpieczeń – WPA-personal

Tryb WPA-enterprise i WPA2-enterprise:

Wybierz typ uwierzytelniania klienta/serwera, którego używa punkt dostępowy; EAP-TLS lub EAP-PEAP.

EAP-TLS

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

Figure 3-9 EAP-TLS

- Identity (Tożsamość) – Wpisz ID użytkownika wysyłany do sieci.
- Private key password (Hasło klucza prywatnego) – Wpisz hasło dla ID użytkownika.
- EAPOL version (Wersja EAPOL) – Wybierz wersję (1 lub 2) używaną w punkcie dostępowym.
- CA Certificate (Certyfikat CA) – Wgraj certyfikat CA przedstawiany punktowi dostępowemu w celu uwierzytelnienia.

EAP-PEAP:

- User Name (Nazwa użytkownika) – Wpisz nazwę użytkownika wysyłaną do sieci.
- Password (Hasło) – Wpisz hasło sieci
- PEAP version (Wersja PEAP) – Wybierz wersję PEAP używaną w punkcie dostępowym.
- Label (Etykieta) – Wybierz etykietę używaną przez punkt dostępowy.
- EAPOL version (Wersja EAPOL) – Wybierz wersję (1 lub 2) w zależności od wersji używanej przez punkt dostępowy
- CA Certificate (Certyfikat CA) – Wgraj certyfikat CA przedstawiany punktowi dostępowemu w celu uwierzytelnienia.



- *Aby lepiej chronić prywatność i system przed ryzykami związanymi z*

bezpieczeństwem, zdecydowanie zalecamy stosowanie silnych haseł dla wszystkich funkcji i urządzeń sieciowych. Hasło powinno być wybrane przez użytkownika (i zawierać co najmniej 8 znaków, w tym wielkie i małe litery, cyfry i znaki specjalne), aby zwiększyć bezpieczeństwo produktu.

- Instalator i(lub) użytkownik końcowy ponoszą odpowiedzialność za prawidłową konfigurację wszystkich haseł i innych ustawień bezpieczeństwa.

3.2 Łatwe połączenie Wi-Fi przy użyciu funkcji WPS

Cel:

Konfiguracja połączenia z siecią bezprzewodową nigdy nie jest łatwa. Aby uniknąć skomplikowanej konfiguracji połączenia bezprzewodowego, możesz włączyć funkcję WPS.

WPS (Wi-Fi Protected Setup) odnosi się do łatwej konfiguracji szyfrowanego połączenia między urządzeniem i routerem bezprzewodowym. WPS ułatwia dodawanie nowych urządzeń do istniejącej sieci bez konieczności wpisywania długich haseł. Istnieją dwa tryby połączenia WPS: tryb PBC i tryb PIN.

Uwaga: Po włączeniu funkcji WPS nie trzeba konfigurować takich parametrów, jak typ szyfrowania, nie trzeba też znać klucza połączenia bezprzewodowego.

Kroki:

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

Figure 3-10 Ustawienia Wi-Fi – WPS

Tryb **PBC**:

W PBC (Push-Button-Configuration – konfiguracja po naciśnięciu przycisku) użytkownik po prostu naciska przycisk, rzeczywisty lub wirtualny (taki jak przycisk

w interfejsie konfiguracji przeglądarki internetowej) jednocześnie na punkcie dostępowym (i rejestratorze sieci) i na nowym bezprzewodowym urządzeniu klienckim.

1. Zaznacz pole wyboru Enable WPS , aby włączyć WPS.
2. Wybierz PBC jako tryb połączenia.

PBC connection

Uwaga: Zarówno punkty dostępowe, jak i podłączane urządzenia muszą obsługiwać tę funkcję.

3. Sprawdź, czy na routerze Wi-Fi jest przycisk WPS. Jeśli tak, naciśnij go, wskaźnik obok przycisku zacznie migać, co oznacza, że funkcja WPS routera jest włączona. Szczegółowe instrukcje znajdują się w podręczniku użytkownika routera.
4. Naciśnij przycisk WPS, aby włączyć funkcję w kamerze.

Jeśli kamera nie ma przycisku WPS, możesz też kliknąć przycisk wirtualny w interfejsie WWW, aby włączyć funkcję PBC.

5. Kliknij przycisk **Connect** (Połącz).

PBC connection

Gdy tryb PBC jest włączony jednocześnie w routerze i kamerze, kamera automatycznie łączy się z siecią bezprzewodową.

Tryb PIN:

Tryb PIN wymaga osobistego numeru identyfikacyjnego (Personal Identification Number – PIN), znajdującego się na naklejce na nowym urządzeniu bezprzewodowym lub wyświetlanego na jego ekranie. Należy wpisać ten PIN, aby połączyć urządzenie z siecią, zwykle z punktem dostępowym sieci.

Kroki:

1. Wybierz SSID połączenia bezprzewodowego z listy.

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

Wi-Fi

SSID: AP

Network Mode: Manager Ad-Hoc

Security Mode: WPA2-personal

Encryption Type: TKIP

Key 1:

WPS

Enable WPS

PIN Code: 48167581

PBC connection

Use router PIN code

SSID: AP

Router PIN code:

Figure 3-11 Ustawienia Wi-Fi – Tryb WPS PIN

- Wybierz **Use router PIN code** (Użyj kodu PIN routera).
Jeśli kod PIN jest generowany po stronie routera, w polu **Router PIN code** (Kod PIN routera) wpisz kod PIN pobrany z routera.
- Kliknij przycisk **Connect** (Połącz).

Lub

Możesz wygenerować PIN po stronie kamery. Czas ważności kodu PIN wynosi 120 sekund.

- Kliknij **Generate** (Generuj).

PIN Code: 48167581

- Wpisz kod w routerze, np. 48167581.

3.3 Ustawienia właściwości IP dla połączenia z siecią bezprzewodową

Domyślny adres IP kontrolera interfejsu sieci bezprzewodowej to 192.168.1.64. Po połączeniu się z siecią bezprzewodową można zmienić domyślny IP.

Kroki:

1. Przejdź do interfejsu konfiguracji TCP/IP.

Configuration> Advanced Configuration> Network> TCP/IP (Konfiguracja > Konfiguracja zaawansowana > Sieć > TCP/IP)

Lub

Configuration> Basic Configuration> Network> TCP/IP (Konfiguracja > Konfiguracja podstawowa > Sieć > TCP/IP)

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

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

Figure 3-12 Ustawienia TCP/IP

2. Jako NIC (Karta sieciowa) wybierz opcję WLAN.

3. Dostosuj opcje IPv4 Address (adres IPv4), IPv4 Subnet Mask (maska podsieci IPv4) i Default Gateway (brama domyślna).

Procedura konfiguracji jest taka sama jak w przypadku sieci LAN.

Jeśli chcesz, aby adres IP był przydzielany automatycznie, zaznacz pole wyboru, aby włączyć DHCP.

Chapter 4 Podgląd na żywo

4.1 Strona podglądu na żywo

Cel:

Na stronie podglądu na żywo można wyświetlać wideo w czasie rzeczywistym, robić zdjęcia, wykonywać czynności sterowania PTZ, ustawiać/wywoływać ustawienia wstępne oraz konfigurować parametry wideo.

Zaloguj się do kamery sieciowej, aby otworzyć stronę podglądu na żywo, lub kliknij **Live View** (Podgląd na żywo) na pasku menu strony głównej, aby przejść do strony podglądu na żywo.

Opisy strony podglądu na żywo:

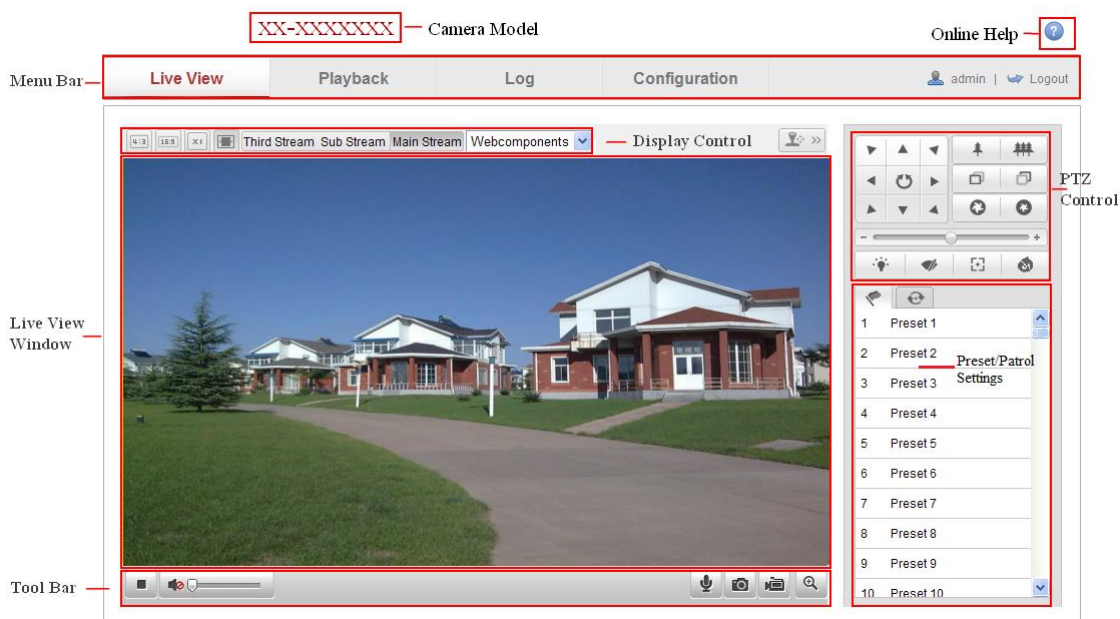



Figure 4-1 Strona podglądu na żywo

Camer Model (Model kamery):

Pokazuje model kamery, do którego się podłączasz.

Online Help (Pomoc online):

Kliknij , aby uzyskać pomoc online, która przeprowadzi cię przez podstawowe czynności obsługi dla każdej funkcji.

Menu Bar (Pasek menu):

Kliknij każdą zakładkę, aby wyświetlić odpowiednio stronę Life View (Podgląd na żywo), Playback (Odtwarzanie), Log (Dziennik) i Cofigation (Konfiguracja).

Display Control (Kontrola wyświetlania):

Kliknij każdą zakładkę, aby dopasować układ i typ strumienia podglądu na żywo. Kliknij menu rozwijane, aby wybrać wtyczkę. Dla użytkowników IE (Internet Explorer) są dostępne komponenty sieci Web i Quick Time. Dla użytkowników innych przeglądarek dostępne są komponenty sieci Web, Quick Time, VLC i MJPEG, pod warunkiem że dana przeglądarka je obsługuje.

Live View Window (Okno podglądu na żywo):

Wyświetla wideo na żywo.

Toolbar (Pasek narzędzi):

Czynności na stronie podglądu na żywo, np. wyświetlanie podglądu na żywo, rejestrowanie obrazów, nagrywanie, włączanie/wyłączanie dźwięku, dwukierunkowe audio itp.

PTZ Control (Sterowanie PTZ):

Czynności obrotu panoramicznego, pochylania i przybliżania/oddalania kamery, a także sterowanie oświetleniem i wycieraczką. (dostępne tylko dla kamer z obsługą funkcji PTZ)

Preset/Patrol Settings (Konfiguracja ustawień wstępnych/patrolu):

Ustawianie/wywoływanie/kasowanie ustawień wstępnych i patroli kamer PTZ.

4.2 Uruchamianie podglądu na żywo













W oknie podglądu na żywo, jak pokazano na Ilustracji 5-2, kliknij  na pasku narzędzi, aby uruchomić podgląd na żywo z kamery.



Figure 4-2 Pasek narzędzi podglądu na żywo



Table 4-1 Opisy paska narzędzi

Ikona	Opis
	Uruchomienie/zatrzymanie podglądu na żywo.
	Proporcje obrazu 4:3.

	Proporcje obrazu 16:9.
	Oryginalne proporcje obrazu.
	Automatycznie ustawiane proporcje obrazu.
Main Stream	Podgląd na żywo ze strumieniem głównym.
Sub Stream	Podgląd na żywo z podstrumieniem.
Third Stream	Podgląd na żywo z trzecim strumieniem.
Webcomponents ▾	Kliknij, aby wybrać wtyczkę innego producenta.
	Ręczne robienie zdjęć.
	Ręczne rozpoczynanie/kończenie nagrywania.
	Włączenie dźwięku i regulacja
	Włączenie/wyłączenie mikrofonu.
	Włączenie/wyłączenie funkcji zoomu cyfrowego.
	Włączenie/wyłączenie funkcji pozycjonowania

Uwaga: Kamera musi obsługiwać trzeci strumień i pozycjonowanie 3D.

4.3 Ręczne nagrywanie i robienie zdjęć

W interfejsie podglądu na żywo, kliknij  na pasku narzędzi, aby robić zdjęcia podglądu na żywo, lub kliknij , aby nagrywać podgląd na żywo. Ścieżki zapisu zrobionych zdjęć i klipów można ustawić na stronie **Configuration > Local Configuration** (Konfiguracja > Konfiguracja lokalna). Aby skonfigurować zdalne zaplanowane nagrywanie, zapoznaj się z *Sekcją 7.2*.

Uwaga: Zrobione zdjęcie zostanie zapisane na komputerze użytkownika jako plik JPEG lub BMP.

4.4 Obsługa sterowania PTZ

Cel:

W interfejsie podglądu na żywo możesz używać przycisków sterowania PTZ, aby sterować obracaniem, pochylaniem i przybliżaniem/oddalaniem kamery.

Uwaga: Aby wykonywać czynności sterowania PTZ, kamera podłączona do sieci

musi obsługiwać funkcję PTZ lub w kamerze musi być zainstalowany moduł obrotu/pochylenia. Prawidłowo skonfiguruj parametry PTZ na stronie ustawień RS-485, patrz *Sekcja 12.9 Ustawienia RS-485*.

4.4.1 Panel sterowania PTZ

Na stronie podglądu na żywo kliknij , aby wyświetlić panel sterowania PTZ,

lub kliknij , aby go ukryć.

Za pomocą przycisków kierunku steruj ruchami obrotu/pochylenia.



Figure 4-3 Panel sterowania PTZ

Steruj obiektywem za pomocą przycisków zoomu/przysłony/ostrości.

Uwagi:










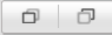






- W oknie podglądu na żywo po kliknięciu i przeciągnięciu myszą w odpowiednie pozycje jest dostępnych 8 strzałek kierunkowych (, , , , , , , ).
- W przypadku kamer, które obsługują wyłącznie ruchy obiektywu, przyciski kierunkowe nie działają.

Table 4-2 Opisy panelu sterowania PTZ

Ikona	Opis
	Przybliżenie/oddalenie
	Ostrość na blisko/daleko
	Przysłona +/-
	Oświetlenie włączone/wyłączone
	Wycieraczka włączona/wyłączona
	Pomocnicze ustawianie ostrości
	Inicjalizacja obiektywu
	Dostosowanie szybkości ruchów obrotu/pochylenia

4.4.2 Ustawianie/wywoływanie ustawienia wstępnego

● Ustawianie ustawienia wstępnego:

1. Na panelu sterowania PTZ wybierz numer Preset (ustawienie wstępne) z listy.

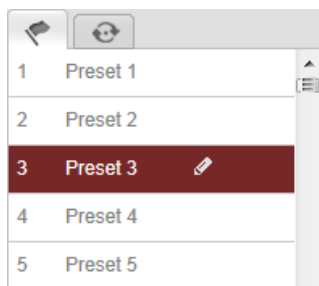




Figure 4-4 Ustawianie ustawienia wstępnego


2. Za pomocą przycisków sterowania PTZ przesuń obiektyw do żądanej pozycji.
 - Obróć kamerę w prawo lub w lewo.
 - Pochyl kamerę w górę lub w dół.
 - Przybliż lub oddal.
 - Zmień ostrość obiektywu.
3. Kliknij , aby zakończyć ustawianie bieżącego ustawienia wstępnego.
4. Możesz kliknąć , aby usunąć ustawienie wstępne.

Uwaga: Dla kamery sieciowej Mini PT można skonfigurować maks. 16 ustawień wstępnych.

● Wywoływanie ustawienia wstępnego:

Ta funkcja pozwala skierować kamerę na konkretną wstępnie zaprogramowaną scenę ręcznie lub jeśli wystąpi zdarzenie.

W przypadku zdefiniowanego ustawienia wstępnego można je wywołać w dowolnym momencie, aby skierować kamerę na żądaną zaprogramowaną scenę.

Na panelu sterowania PTZ wybierz ustawienie wstępne z listy i kliknij , aby je wywołać.

Lub umieść mysz na interfejsie ustawień wstępnych i wywołaj odpowiednie ustawienie, wpisując jego numer.

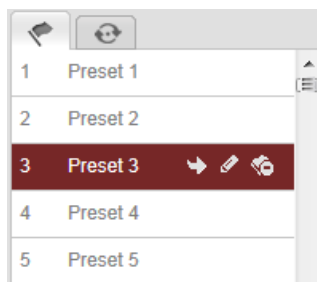




Figure 4-5 Wywoływanie ustawienia wstępnego

4.4.3 Ustawianie/wywoływanie patrolu

Uwaga:

Przed ustawieniem patrolu należy skonfigurować co najmniej 2 ustawienia wstępne.

Kroki:

1. Kliknij , aby otworzyć interfejs konfiguracji patrolu.
2. Wybierz nr ścieżki i kliknij , aby dodać skonfigurowane ustawienia wstępne.
3. Wybierz ustawienie wstępne i wpisz czas trwania oraz szybkość patrolu.
4. Kliknij OK, aby zapisać pierwsze ustawienie wstępne.
5. Wykonaj powyższe kroki jeszcze raz, aby dodać inne ustawienia wstępne.

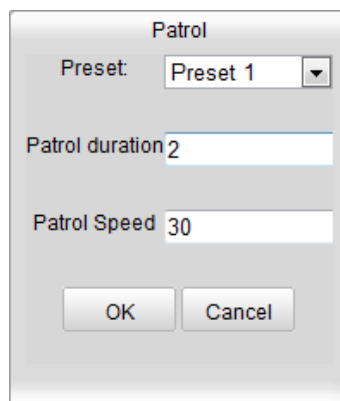






Figure 4-6 Dodawanie ścieżki patrolu

6. Kliknij , aby zapisać patrol.
7. Kliknij , aby uruchomić patrol, kliknij , aby go zatrzymać.
8. (Opcja) Kliknij , aby usunąć patrol.

Chapter 5 Konfiguracja kamery sieciowej

5.1 Konfiguracja lokalnych parametrów

Uwaga: Konfiguracja lokalna oznacza parametry podglądu na żywo, plików z nagraniami i zrobionych zdjęć. Pliki z nagraniami i zrobione zdjęcia pochodzą z nagrań i rejestracji przy użyciu przeglądarki internetowej, dlatego ich ścieżki zapisu są na komputerze, na którym jest uruchomiona przeglądarka.

Kroki:

1. Przejdź do interfejsu konfiguracji lokalnej:

Configuration > Local Configuration (Konfiguracja > Konfiguracja lokalna)

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

- Live View Parameters:** Includes 'Protocol' (radio buttons for TCP, UDP, MULTICAST, HTTP), 'Live View Performance' (radio buttons for Shortest Delay, Auto), 'Rules' (radio buttons for Enable, Disable), and 'Image Format' (radio buttons for JPEG, BMP).
- Record File Settings:** Includes 'Record File Size' (radio buttons for 256M, 512M, 1G), 'Save record files to' (text input with 'Browse' button), and 'Save downloaded files to' (text input with 'Browse' button).
- Picture and Clip Settings:** Includes 'Save snapshots in live view to' (text input with 'Browse' button), 'Save snapshots when playback to' (text input with 'Browse' button), and 'Save clips to' (text input with 'Browse' button).

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

Figure 5-1 Interfejs konfiguracji lokalnej

2. Skonfiguruj następujące ustawienia:

- **Live View Parameters (Parametry podglądu na żywo):** Wybierz typ protokołu i wydajność podglądu na żywo.
- ◆ **Protocol Type (Typ protokołu):** Do wyboru są TCP, UDP, MULTICAST i

HTTP.

TCP: Zapewnia pełne dostarczanie danych strumieniowania i lepszą jakość wideo, ale transmisja nie odbywa się w pełni w czasie rzeczywistym.

UDP: Transmisja strumieni audio i wideo w czasie rzeczywistym.

HTTP: Taka sama jakość jak TCP, ale nie trzeba ustawiać konkretnych portów dla strumieniowania w niektórych konfiguracjach sieci.

MULTICAST: Zaleca się wybrać typ MCAST w przypadku korzystania z funkcji Multicast. Szczegółowe informacje na temat Multicast znajdują się w *Sekcji 6.3.1 Konfiguracja ustawień TCP/IP*.

- ◆ **Live View Performance (Wydajność podglądu na żywo):** Ustaw wydajność podglądu na żywo na Shortest Delay (Najkrótsze opóźnienie) lub Auto.
- ◆ **Rules (Reguły):** Dotyczy reguł w lokalnej przeglądarce, wybierz opcję Enable (Włącz) lub Disable (Wyłącz), aby wyświetlać lub ukrywać kolorowe oznaczenia w sytuacji wykrycia ruchu, twarzy lub wtargnięcia. Np. gdy reguły są włączone, a jednocześnie jest włączone wykrywanie twarzy, to w momencie wykrycia twarzy zostanie ona oznaczona na ekranie podglądu na żywo zielonym prostokątem.
- ◆ **Image Format (Format obrazu):** Wybierz format obrazu dla zrobionego zdjęcia.
- **Record File Settings (Ustawienia pliku z nagraniem):** Ustaw ścieżkę zapisu nagrywanych plików wideo. Dotyczy to plików z nagraniem nagranych z poziomu przeglądarki internetowej.
- ◆ **Record File Size (Rozmiar pliku z nagraniem):** Wybierz rozmiar ręcznie nagranych i pobranych plików wideo: 256M, 512M lub 1G. Wybrana wartość decyduje o maksymalnym rozmiarze pliku z nagraniem.
- ◆ **Save record files to (Zapisz pliki z nagraniem w):** Ustaw ścieżkę zapisu ręcznie nagrywanych plików wideo.
- ◆ **Save downloaded files to (Zapisz pobrane pliki w):** Ustaw ścieżkę zapisu pobranych plików wideo w trybie odtwarzania.
- **Picture and Clip Settings (Ustawienia zdjęcia i klipu):** Ustaw ścieżkę zapisu

zrobionych zdjęć i klipów wideo. Dotyczy to zdjęć zrobionych z poziomu przeglądarki internetowej.

- ◆ **Save snapshots in live view to (Zapisz zrzuty z podglądu na żywo w):** Ustaw ścieżkę zapisu ręcznie zrobionych zdjęć w trybie podglądu na żywo.
- ◆ **Save snapshots when playback to (Zapisz zrzuty z odtwarzania w):** Ustaw ścieżkę zapisu zrobionych zdjęć w trybie odtwarzania.
- ◆ **Save clips to (Zapisz klipy w):** Ustaw ścieżkę zapisu klipów wideo w trybie odtwarzania.

Uwaga: Możesz kliknąć **Browse** (Przeglądaj), aby zmienić katalog zapisu klipów i zdjęć.

3. Kliknij **Save** (Zapisz), aby zapisać ustawienia.

5.2 Konfiguracja ustawień czasu

Cel:

Wykonaj instrukcje w tej sekcji, aby skonfigurować synchronizację czasu i ustawienia czasu letniego.

Kroki:

1. Otwórz interfejs ustawień czasu:

Configuration > Basic Configuration > System > Time Settings (Konfiguracja > Konfiguracja podstawowa > System > Ustawienia czasu)

Lub **Configuration > Advanced Configuration > System > Time Settings** (Konfiguracja > Konfiguracja zaawansowana > System > Ustawienia czasu)

Figure 5-2 Ustawienia czasu

- Wybierz Time Zone (Strefa czasowa).

Wybierz strefę czasową swojej lokalizacji z menu rozwijanego.

- ◆ Synchronizacja czasu przez serwer NTP.

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

(2) Skonfiguruj następujące ustawienia:

Server Address (Adres serwera): Adres IP serwera NTP

NTP Port (Port NTP): Port serwera NTP.


Interval (Odstęp): Odstęp czasowy między dwiema synchronizacjami z serwerem NTP.

Figure 5-3 Synchronizacja czasu przez serwer NTP

Uwaga: Jeśli kamera jest podłączona do sieci publicznej, lepiej jest użyć serwera NTP z funkcją synchronizacji czasu, takiego jak serwer National Time Center (adres IP: 210.72.145.44). Jeśli kamera jest w zmodyfikowanej sieci wewnętrznej, do założenia serwera NTP w celu synchronizacji czasu można użyć oprogramowania NTP.

- ◆ Konfiguracja ręcznej synchronizacji czasu

Włącz funkcję **Manual Time Sync** (Ręczna synchronizacja czasu), a następnie kliknij

 , aby ustawić czas systemowy z wyświetlonego podręcznego kalendarza.

Uwaga: Możesz zaznaczyć pole wyboru **Sync with computer time** (Synchronizuj z czasem komputera), aby synchronizować czas kamery z czasem komputera.

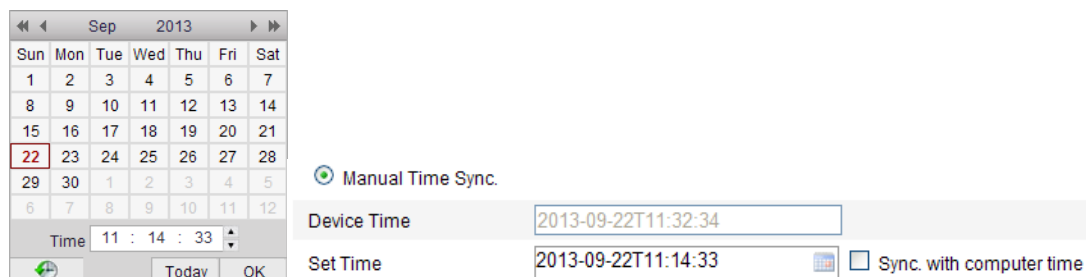


Figure 5-4 Ręczna synchronizacja czasu

- Kliknij stronę zakładki **DST** (Czas letni), aby włączyć funkcję czasu letniego, i ustaw datę okresu czasu letniego.

DST					
<input checked="" type="checkbox"/>	Enable DST				
Start Time	Apr	First	Sun	02	o'clock
End Time	Oct	Last	Sun	02	o'clock
DST Bias	30min				

Figure 5-5 Ustawienia czasu letniego

2. Kliknij **Save** (Zapisz), aby zapisać ustawienia.

5.3 Konfiguracja ustawień sieci

5.3.1 Konfiguracja ustawień TCP/IP

Cel:

Aby kamera działała w sieci, trzeba prawidłowo skonfigurować ustawienia TCP/IP. Kamera obsługuje protokoły IPv4 i IPv6. Można jednocześnie skonfigurować obie wersje, przy czym nie nastąpi między nimi konflikt, należy jednak skonfigurować co najmniej jedną wersję IP.

Kroki:

1. Otwórz interfejs ustawień TCP/IP:

Configuration > Basic Configuration > Network > TCP/IP (Konfiguracja > Konfiguracja podstawowa > Sieć > TCP/IP)

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

(Konfiguracja > Konfiguracja zaawansowana > Sieć > TCP/IP)

The screenshot displays a web-based configuration interface for TCP/IP settings. It is divided into two main sections: 'NIC Settings' and 'DNS Server'.
NIC Settings:
- **NIC Type:** A dropdown menu set to 'Auto'.
- **DHCP:** An unchecked checkbox.
- **IPv4 Address:** A text input field containing '10.11.36.159' and a 'Test' button to its right.
- **IPv4 Subnet Mask:** A text input field containing '255.255.255.0'.
- **IPv4 Default Gateway:** A text input field containing '10.11.36.254'.
- **IPv6 Mode:** A dropdown menu set to 'Route Advertisement' and a 'View Route Advertisement' button to its right.
- **IPv6 Address:** A text input field containing '::'.
- **IPv6 Subnet Mask:** A text input field containing '0'.
- **IPv6 Default Gateway:** An empty text input field.
- **Mac Address:** A text input field containing '44:19:b6:5e:16:f2'.
- **MTU:** A text input field containing '1500'.
- **Multicast Address:** An empty text input field.
- **Enable Multicast Discovery:** A checked checkbox.
DNS Server:
- **Preferred DNS Server:** A text input field containing '8.8.8.8'.
- **Alternate DNS Server:** An empty text input field.
At the bottom right of the interface is a 'Save' button.

Figure 5-6 Ustawienia TCP/IP

2. Skonfiguruj podstawowe ustawienia sieci, takie jak typ NIC, adres IPv4 lub IPv6, maska podsieci IPv4 lub IPv6, brama domyślna IPv4 lub IPv6, ustawienia MTU i adres Multicast.
3. (Opcja) Zaznacz pole wyboru **Enable Multicast Discovery** (Włącz wykrywanie Multicast), aby oprogramowanie klienta mogło za pomocą prywatnego protokołu Multicast wykryć kamerę sieciową online w sieci LAN.
4. Kliknij **Save** (Zapisz), aby zapisać powyższe ustawienia.

Uwagi:

- Zakres ważnych wartości MTU to 1280 ~ 1500.
- Multicast wysyła strumień do adresu grupy multicast i pozwala wielu klientom na jego odbiór w tym samym czasie poprzez zażądanie kopii z adresu grupy multicast. Przed użyciem tej funkcji musisz ją włączyć w routerze.
- Aby wprowadzić nowe ustawienia, trzeba zrestartować router.

5.3.2 Konfiguracja ustawień portów

Cel:

Możesz ustawić nr portu kamery, np. port HTTP, port RTSP i port HTTPS.

Kroki:

1. Otwórz interfejs ustawień portów:

Configuration > Basic Configuration > Network > Port (Konfiguracja > Konfiguracja podstawowa > Sieć > Port)

Lub **Configuration > Advanced Configuration > Network > Port** (Konfiguracja > Konfiguracja zaawansowana > Sieć > Port)

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

Figure 5-7 Ustawienia portów

2. Ustaw port HTTP, port RTSP, port HTTPS i port serwera kamery.

HTTP Port (Port HTTP): Domyślny numer portu to 80, można go zmienić na dowolny niezajęty nr portu.

RTSP Port (Port RTSP): Domyślny numer portu to 554, można go zmienić na dowolny niezajęty nr portu z zakresu od 1024 do 65535.

HTTPS Port (Port HTTPS): Domyślny numer portu to 443, można go zmienić na dowolny niezajęty nr portu.

Server Port (Port serwera): Domyślny numer portu serwera to 8000, można go zmienić na dowolny nr portu z zakresu od 2000 do 65535.

3. Kliknij **Save** (Zapisz), aby zapisać ustawienia.

Uwaga: Aby wprowadzić nowe ustawienia, trzeba zrestartować router.

5.3.3 Konfiguracja ustawień PPPoE

Kroki:

1. Przejdź do interfejsu ustawień PPPoE:

Configuration > Advanced Configuration > Network > PPPoE (Konfiguracja > Konfiguracja zaawansowana > Sieć > PPPoE)

Figure 5-8 Ustawienia PPPoE

2. Zaznacz pole wyboru **Enable PPPoE** (Włącz PPPoE), aby włączyć tę funkcję.
3. Wpisz dane w polach **User name** (Nazwa użytkownika), **Password** (Hasło) i **Confirm** (Potwierdź) hasło dostępu PPPoE.

Uwaga: Nazwę użytkownika i hasło należy uzyskać od operatora Internetu.



- *Aby lepiej chronić prywatność i system przed ryzykami związanymi z bezpieczeństwem, zdecydowanie zalecamy stosowanie silnych haseł dla wszystkich funkcji i urządzeń sieciowych. Hasło powinno być wybrane przez użytkownika (i zawierać co najmniej 8 znaków, w tym wielkie i małe litery, cyfry i znaki specjalne), aby zwiększyć bezpieczeństwo produktu.*
 - *Instalator i(lub) użytkownik końcowy ponoszą odpowiedzialność za prawidłową konfigurację wszystkich haseł i innych ustawień bezpieczeństwa.*
4. Kliknij **Save** (Zapisz), aby zapisać dane i zamknąć interfejs.

Uwaga: Aby wprowadzić nowe ustawienia, trzeba zrestartować router.

5.3.4 Konfiguracja ustawień DDNS

Cel:

Jeśli domyślne połączenie sieciowe kamery to PPPoE, do dostępu do sieci możesz użyć usługi Dynamic DNS (DDNS).

Przed rozpoczęciem pracy:

Zanim skonfigurujesz ustawienia DDNS kamery, musisz się zarejestrować w serwerze

DDNS.



- Aby lepiej chronić prywatność i system przed ryzykami związanymi z bezpieczeństwem, zdecydowanie zalecamy stosowanie silnych haseł dla wszystkich funkcji i urządzeń sieciowych. Hasło powinno być wybrane przez użytkownika (i zawierać co najmniej 8 znaków, w tym wielkie i małe litery, cyfry i znaki specjalne), aby zwiększyć bezpieczeństwo produktu.
- Instalator i(lub) użytkownik końcowy ponoszą odpowiedzialność za prawidłową konfigurację wszystkich haseł i innych ustawień bezpieczeństwa.

Kroki:

1. Otwórz interfejs ustawień DDNS:

Configuration > Advanced Configuration > Network > DDNS (Konfiguracja > Konfiguracja zaawansowana > Sieć > DDNS)

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

Figure 5-9 Ustawienia DDNS

2. Zaznacz pole wyboru **Enable DDNS** (Włącz DDNS), aby włączyć tę funkcję.
3. Wybierz **Typ DDNS**: Do wyboru są cztery typy DDNS: HiDDNS, IPServer, NO-IP i DynDNS.

- DynDNS:

Kroki:

- (1)Wpisz **Server Address** (Adres serwera) DynDNS (np. members.dyndns.org).
- (2)W polu tekstowym **Domain** (Domena) wpisz nazwę domenową otrzymaną z witryny DynDNS.
- (3)Wpisz **Port** serwera DynDNS.

(4) Wpisz dane w polach **User name** (Nazwa użytkownika) i **Password** (Hasło) zarejestrowane w witrynie DynDNS.

(5) Kliknij **Save** (Zapisz), aby zapisać ustawienia.

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

Figure 5-10 Ustawienia DynDNS

- Serwer IP:

Kroki:

(1) Wpisz adres serwera dla serwera IP.

(2) Kliknij **Save** (Zapisz), aby zapisać ustawienia.

Uwaga: W przypadku serwera IP, należy uzyskać statyczny adres IP, maskę podsieci, bramę i preferowany DNS od operatora Internetu. Należy wpisać **Server Address** (Adres serwera) będący statycznym adresem IP komputera, na którym jest uruchomione oprogramowanie serwera IP.

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

Figure 5-11 Ustawienia serwera IP

Uwaga: W przypadku USA i Kanady możesz podać adres serwera 173.200.91.74.

- NO-IP:

Kroki:

(1) Jako typ DDNS wybierz NO-IP.

The screenshot shows a web form for configuring DDNS. At the top, there is a checkbox labeled 'Enable DDNS' which is checked. Below it is a dropdown menu for 'DDNS Type' with 'NO-IP' selected. The form contains several input fields: 'Server Address', 'Domain', 'Port' (with '0' entered), 'User Name', 'Password', and 'Confirm'.

Figure 5-12 Ustawienia NO-IP

- (2) Wpisz adres serwera: www.noip.com
- (3) Wpisz zarejestrowaną nazwę domenową.
- (4) Wpisz numer portu, jeśli jest potrzebny.
- (5) Wpisz nazwę użytkownika i hasło.
- (6) Kliknij **Save** (Zapisz), obraz z kamery można wówczas wyświetlać za pomocą nazwy domenowej.

- HiDDNS

Kroki:

- (1) Jako typ DDNS wybierz HiDDNS.

The screenshot shows a web form for configuring HiDDNS. At the top, there is a checkbox labeled 'Enable DDNS' which is checked. Below it is a dropdown menu for 'DDNS Type' with 'HiDDNS' selected. The form contains several input fields: 'Server Address' (with 'www.hik-online.com' entered), 'Domain' (with '431618683' entered), 'Port' (with '0' entered), 'User Name', 'Password', and 'Confirm'.

Figure 5-13 Ustawienia HiDDNS

- (2) Wpisz adres serwera: www.hik-online.com.
- (3) Wpisz nazwę domenową kamery. Domena jest taka sama, jak alias urządzenia na serwerze HiDDNS.
- (4) Kliknij **Save** (Zapisz), aby zapisać nowe ustawienia.

Uwaga: Aby wprowadzić nowe ustawienia, trzeba zrestartować router.

5.3.5 Konfiguracja ustawień SNMP

Cel:

Można ustawić funkcję SNMP, aby uzyskiwać informacje o stanie kamery, jej parametrach i alarmach oraz aby zarządzać kamerą zdalnie, gdy jest podłączona do sieci.

Przed rozpoczęciem pracy:

Zanim ustawisz SNMP, pobierz oprogramowanie SNMP i skonfiguruj w kamerze odbieranie informacji przez port SNMP. Dzięki ustawieniu adresu sygnałów Trap (pułapek) kamera może wysyłać zdarzenia alarmowe i komunikaty o wyjątkach do centrum monitoringu.

Uwaga: Wybrana wersja SNMP powinna być taka sama, jak oprogramowanie SNMP. W zależności od wymagań poziomu zabezpieczeń może być konieczne użycie innej wersji. Protokół SNMP v1 nie ma zabezpieczeń, a SNMP v2 wymaga podania hasła dostępowego. SNMP v3 zapewnia szyfrowanie, w przypadku korzystania z trzeciej wersji musi być włączony protokół HTTPS.



- *Aby lepiej chronić prywatność i system przed ryzykami związanymi z bezpieczeństwem, zdecydowanie zalecamy stosowanie silnych haseł dla wszystkich funkcji i urządzeń sieciowych. Hasło powinno być wybrane przez użytkownika (i zawierać co najmniej 8 znaków, w tym wielkie i małe litery, cyfry i znaki specjalne), aby zwiększyć bezpieczeństwo produktu.*
- *Instalator i(lub) użytkownik końcowy ponoszą odpowiedzialność za prawidłową konfigurację wszystkich haseł i innych ustawień bezpieczeństwa.*

Kroki:

1. Otwórz interfejs ustawień SNMP:

Configuration > Advanced Configuration > Network > SNMP (Konfiguracja > Konfiguracja zaawansowana > Sieć > SNMP)

The screenshot displays the SNMP configuration interface, organized into three main sections:

- SNMP v1/v2:** Includes checkboxes for 'Enable SNMPv1' and 'Enable SNMP v2c'. Below these are text input fields for 'Write SNMP Community' (set to 'private'), 'Read SNMP Community' (set to 'public'), 'Trap Address', 'Trap Port' (set to '162'), and 'Trap Community' (set to 'public').
- SNMP v3:** Contains settings for 'Enable SNMPv3'. It features two identical sets of configuration options for Read and Write operations. Each set includes a 'Read/Write UserName' field, a 'Security Level' dropdown menu (set to 'no auth, no priv'), radio buttons for 'Authentication Algorithm' (MD5 selected, SHA unselected), an 'Authentication Password' field, radio buttons for 'Private-key Algorithm' (DES selected, AES unselected), and a 'Private-key password' field.
- SNMP Other Settings:** Includes a single 'SNMP Port' field set to '161'.

Figure 5-14 Ustawienia SNMP

2. Zaznacz pole wyboru odpowiedniej wersji (Enable SNMP SNMPv1 , Enable SNMP v2c , Enable SNMPv3), aby włączyć tę funkcję.

3. Skonfiguruj ustawienia SNMP.

Uwaga: Konfiguracja oprogramowania SNMP powinna odpowiadać ustawieniom skonfigurowanym w tym miejscu.

4. Kliknij **Save** (Zapisz), aby zapisać i zakończyć ustawienia.

Uwaga: Aby wprowadzić nowe ustawienia, trzeba zrestartować router.

5.3.6 Konfiguracja ustawień 802.1X

Cel:

Kamery sieciowe obsługują standard IEEE 802.1X, po włączeniu tej funkcji dane kamery są chronione, a podłączenie kamery do sieci chronionej przez IEEE 802.1X wymaga uwierzytelnienia użytkownika.

Przed rozpoczęciem pracy:

Musi być skonfigurowany serwer uwierzytelniania. Poproś o nazwę użytkownika i hasło 802.1X i zarejestruj je na serwerze.



- *Aby lepiej chronić prywatność i system przed ryzykami związanymi z bezpieczeństwem, zdecydowanie zalecamy stosowanie silnych haseł dla wszystkich funkcji i urządzeń sieciowych. Hasło powinno być wybrane przez użytkownika (i zawierać co najmniej 8 znaków, w tym wielkie i małe litery, cyfry i znaki specjalne), aby zwiększyć bezpieczeństwo produktu.*
- *Instalator i(lub) użytkownik końcowy ponoszą odpowiedzialność za prawidłową konfigurację wszystkich haseł i innych ustawień bezpieczeństwa.*

Kroki:

1. Przejdź do interfejsu ustawień 802.1X:

Configuration > Advanced Configuration > Network > 802.1X (Konfiguracja > Konfiguracja zaawansowana > Sieć > 802.1X)

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

Figure 5-15 Ustawienia 802.1X

2. Zaznacz pole wyboru **Enable IEEE 802.1X** (Włącz IEEE 802.1X), aby włączyć tę funkcję.
3. Skonfiguruj ustawienia 802.1X, takie jak wersja EAPOL, nazwa użytkownika i hasło.

Uwaga: Wersja EAPOL musi być identyczna jak wersja w routerze lub switchu.

4. Wpisz nazwę użytkownika i hasło, aby uzyskać dostęp do serwera.
5. Kliknij **Zapisz**, aby zakończyć ustawienia.

Uwaga: Aby wprowadzić nowe ustawienia, trzeba zrestartować router.

5.3.7 Konfiguracja ustawień QoS

Cel:

QoS (Quality of Service – jakość usługi) pomaga w rozwiązywaniu problemów z opóźnieniami i zatłoczeniami w sieci poprzez konfigurację priorytetów wysyłania danych.

Kroki:

1. Otwórz interfejs ustawień QoS:

Configuration > Advanced Configuration > Network > QoS (Konfiguracja > Konfiguracja zaawansowana > Sieć > QoS)



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

Figure 5-16 Ustawienia QoS

2. Skonfiguruj ustawienia QoS, takie jak DSCP wideo/audio, DSCP zdarzeń/alarmów i DSCP zarządzania.

Zakres ważnych wartości DSCP to 0-63. Im wyższa wartość DSCP, tym wyższy priorytet.

Uwaga: DSCP oznacza Differentiated Services Code Point; a wartości DSCP używa się w nagłówku IP w celu wskazania priorytetu danych.

3. Kliknij **Save** (Zapisz), aby zapisać ustawienia.

Uwaga: Aby wprowadzić nowe ustawienia, trzeba zrestartować router.

5.3.8 Konfiguracja ustawień UPnP™

Universal Plug and Play (UPnP™) to architektura sieciowa, która zapewnia zgodność sprzętu sieciowego, oprogramowania i innych urządzeń sprzętowych. Protokół UPnP pozwala urządzeniom na bezproblemowe łączenie i upraszcza wdrażanie sieci domowych i firmowych.

W przypadku włączenia tej funkcji nie trzeba konfigurować mapowania portów dla każdego portu, a kamera łączy się z siecią WAN przez router.

Kroki:

1. Otwórz interfejs ustawień UPnP™.

Configuration > Advanced Configuration > Network > UPnP (Konfiguracja > Konfiguracja zaawansowana > Sieć > UPnP)

2. Zaznacz pole wyboru, aby włączyć funkcję UPnP™.

Można wyedytować nazwę urządzenia wykrytego online.




Figure 5-17 Ustawienia UPnP

5.3.9 Konfiguracja bezprzewodowego wybierania numeru

Cel:

Strumień danych audio, wideo i obrazów można przesyłać przez sieć bezprzewodową 3G / 4G.

Uwaga: Funkcja bezprzewodowego wybierania numeru musi być obsługiwana przez kamerę.

1. Kliknij zakładkę **Wireless Dial** (Bezprzewodowe wybieranie numeru), aby otworzyć interfejs konfiguracji bezprzewodowego wybierania numeru.
2. Zaznacz pole wyboru **Enable** (Włącz), aby włączyć ustawienia bezprzewodowego wybierania numeru.

3. Skonfiguruj parametry wybierania numeru.

- 1) Wybierz tryb wybierania numeru z listy rozwijanej. Do wyboru są Auto i Manual (Ręczne). Po wybraniu Auto można ustawić harmonogram uzbrajania dla wybierania numeru, po wybraniu Manual (Ręczne) można ustawić czas offline i parametry ręcznego wybierania numeru.
- 2) Ustaw numer dostępowy, nazwę użytkownika, hasło, APN, MTU i protokół weryfikacji. Możesz nie wpisywać tych parametrów, urządzenie zastosuje ustawienia domyślne wybierania numeru po skonfigurowaniu innych parametrów.



- *Aby lepiej chronić prywatność i system przed ryzykami związanymi z bezpieczeństwem, zdecydowanie zalecamy stosowanie silnych haseł dla wszystkich funkcji i urządzeń sieciowych. Hasło powinno być wybrane przez użytkownika (i zawierać co najmniej 8 znaków, w tym wielkie i małe litery, cyfry i znaki specjalne), aby zwiększyć bezpieczeństwo produktu.*
 - *Instalator i(lub) użytkownik końcowy ponoszą odpowiedzialność za prawidłową konfigurację wszystkich haseł i innych ustawień bezpieczeństwa.*
- 3) Wybierz tryb sieci z listy rozwijanej. Do wyboru są Auto, 3G i 4G. Po wybraniu Auto priorytet wyboru sieci jest następujący: 4G > 3G > Sieć przewodowa.
 - 4) Jeśli jako tryb wybierania numeru wybrano Manual (Ręczne), wpisz czas offline.
 - 5) Wpisz numer UIM (numer telefonu komórkowego).
 - 6) Kliknij przycisk **Edit** (Edytuj), aby ustawić harmonogram uzbrajania, jeśli jako tryb wybierania numeru wybrano Auto.
 - 7) Kliknij **Save** (Zapisz), aby zapisać ustawienia.

^ Dial Parameters

Dial Mode

Access Number

User Name

Password

APN

MTU

Verification Protocol

Network Mode

Offline Time second

UIM Number

Figure 5-18 Parametry wybierania numeru

4. Wyświetl stan wybierania numeru.
 - 1) Kliknij przycisk **Refresh** (Odśwież), aby wyświetlić stan wybierania numeru, m.in. tryb czasu rzeczywistego, stan UIM, siła sygnału itp.
 - 2) Jeśli jako tryb wybierania numeru wybrano Manual (Ręczne), można też ręcznie łączyć/rozłączać sieć bezprzewodową.

^ Dial Status

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

Figure 5-19 Stan wybierania numeru

5. Ustaw białą listę.

- 1) Zaznacz pole wyboru **Enable SMS Alarm** (Włącz alarm SMS).

Numer telefonu komórkowego na białej liście będzie otrzymywał komunikaty alarmowe z urządzenia, będzie też możliwe resetowanie urządzenia przez SMS.

Uwaga: Do białej listy można dodać maks. 8 numerów telefonów komórkowych.

^ White List

Enable SMS Alarm

No.	Mobile Phone Number	Permission
1	1888888888	Edit
2	15968172711	
3		
4		
5		
6		
7		
8		

Figure 5-20 Ustawienia białej listy

- 2) Wybierz pozycję na białej liście i kliknij przycisk **Edit** (Edytuj), aby otworzyć interfejs ustawień alarmów SMS.

Permission

Mobile Phone Number:

Reboot via SMS

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

Figure 5-21 Ustawienia alarmów SMS

- 3) Wpisz numer telefonu komórkowego dodawany do białej listy, zaznacz pole wyboru **Reboot via SMS** (Restartuj przez SMS), wybierz alarm dla powiadomień SMS push i kliknij **OK**.

Uwaga: Aby zresetować urządzenie przez SMS, wyślij do urządzenia wiadomość „reboot” (Uruchom ponownie), urządzenie odpowie

wiadomością „reboot success” (udane ponowne uruchomienie) po udanym zresetowaniu.

- 4) (Opcja) Możesz kliknąć **Send Test SMS** (Wyślij testowy SMS), aby wysłać testową wiadomość na numer telefonu komórkowego.
- 5) Kliknij **Save** (Zapisz), aby zapisać ustawienia.

5.3.10 Wysyłanie e-maila wyzwolonego przez alarm

Cel:

Można skonfigurować system tak, aby wysyłał powiadomienie e-mailem do wszystkich wyznaczonych odbiorców w razie wykrycia zdarzenia alarmu, np. zdarzenia wykrycia ruchu, utraty sygnału wideo, manipulacji przy kamerze itp.

Przed rozpoczęciem pracy:

Aby korzystać z funkcji e-mail, najpierw skonfiguruj ustawienia serwera DNS w **Basic Configuration > Network > TCP/IP** (Konfiguracja podstawowa > Sieć > TCP/IP) lub **Advanced Configuration > Network > TCP/IP** (Konfiguracja zaawansowana > Sieć > TCP/IP).

Kroki:

1. Przejdź do ustawień TCP/IP (**Configuration > Basic Configuration > Network > TCP/IP** (Konfiguracja > Konfiguracja podstawowa > Sieć > TCP/IP) lub **Configuration > Advanced Configuration > Network > TCP/IP** (Konfiguracja > Konfiguracja zaawansowana > Sieć > TCP/IP)), aby ustawić adres IPv4, maskę podsieci IPv4, bramę domyślną IPv4 i preferowany serwer DNS.

Uwaga: Szczegółowe informacje znajdują się w *Sekcji 6.3.1 Konfiguracja ustawień TCP/IP*.

2. Przejdź do interfejsu ustawień poczty elektronicznej:

Configuration > Advanced Configuration > Network > Email (Konfiguracja > Konfiguracja zaawansowana > Sieć > E-mail)

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

Figure 5-22 Ustawienia e-mail

3. Skonfiguruj następujące ustawienia:

Sender (Nadawca): Nazwa nadawcy e-maila.

Sender's Address (Adres nadawcy): Adres e-mail nadawcy.

SMTP Server (Serwer SMTP): Adres IP lub nazwa hosta serwera SMTP (np. smtp.263xmail.com).

SMTP Port (Port SMTP): Port SMTP. Domyślny port TCP/IP dla SMTP to 25 (bez zabezpieczeń). Port SMTP z SSL to 465.

Enable SSL (Włącz SSL): Zaznacz pole wyboru, aby włączyć SSL, jeśli serwer SMTP go wymaga.

Attached Image (Załączony obraz): Zaznacz pole wyboru Załączony obraz, aby wysyłać e-maile z załączonymi obrazami alarmów.

Interval (Odstęp): Odstęp oznacza czas między dwiema czynnościami wysłania załączonych zdjęć.

Authentication (Uwierzytelnianie) (krok opcjonalny): Jeśli serwer poczty elektronicznej wymaga uwierzytelniania, zaznacz to pole wyboru, aby używać

uwierzytelniania przy logowaniu się do tego serwera, podaj nazwę użytkownika i hasło.



- *Aby lepiej chronić prywatność i system przed ryzykami związanymi z bezpieczeństwem, zdecydowanie zalecamy stosowanie silnych haseł dla wszystkich funkcji i urządzeń sieciowych. Hasło powinno być wybrane przez użytkownika (i zawierać co najmniej 8 znaków, w tym wielkie i małe litery, cyfry i znaki specjalne), aby zwiększyć bezpieczeństwo produktu.*
- *Instalator i(lub) użytkownik końcowy ponoszą odpowiedzialność za prawidłową konfigurację wszystkich haseł i innych ustawień bezpieczeństwa.*

Wybór odbiorcy: Wybierz odbiorcę e-maila. Można dodać maks. 2 odbiorców.

Receiver (Odbiorca): Nazwa powiadamianego użytkownika.

Receiver's Address (Adres odbiorcy): Adres e-mail powiadamianego użytkownika.

4. Kliknij **Save** (Zapisz), aby zapisać ustawienia.

5.3.11 Konfiguracja ustawień NAT (Network Address Translation – translacja adresów sieciowych)

Cel:

1. Przejdź do interfejsu ustawień NAT.

Configuration >Advanced Configuration > Network > NAT (Konfiguracja > Konfiguracja zaawansowana > Sieć > NAT)

2. Wybierz tryb mapowania portów.

Aby mapować porty z domyślnymi numerami portów:

Wybierz dla opcji Port Mapping Mode (Tryb mapowania portów) ustawienie **Auto**.

Aby mapować porty z własnymi numerami portów:

Wybierz dla opcji Port Mapping Mode (Tryb mapowania portów) ustawienie

Manual (Ręczne).

W przypadku ręcznego mapowania portów możesz wpisać własną wartość numeru portu.

The screenshot shows a web interface for NAT configuration. At the top, there is a checkbox labeled "Enable Port Mapping" which is checked. Below it is a dropdown menu for "Port Mapping Mode" set to "Manual". A table lists three port mappings:

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

At the bottom right of the interface is a "Save" button.

Figure 5-23 Skonfiguruj ustawienia NAT

3. Kliknij **Save (Zapisz)**, aby zapisać ustawienia.

5.3.12 Konfiguracja ustawień FTP**Cel:**

Możesz skonfigurować informacje dotyczące serwera FTP, aby włączyć wysyłanie zrobionych zdjęć na serwer FTP. Robienie zdjęć może być wyzwalane przez zdarzenia lub zaplanowane zadanie robienia zrzutu.

Kroki:

1. Otwórz interfejs ustawień FTP:
Configuration > Advanced Configuration > Network > FTP (Konfiguracja > Konfiguracja zaawansowana > Sieć > FTP)

The screenshot shows the FTP configuration interface with the following fields and options:

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

A "Test" button is located at the bottom of the form.

Figure 5-24 Ustawienia FTP

2. Skonfiguruj ustawienia FTP, do zalogowania się na serwerze FTP konieczne są

nazwa użytkownika i hasło.



- *Aby lepiej chronić prywatność i system przed ryzykami związanymi z bezpieczeństwem, zdecydowanie zalecamy stosowanie silnych haseł dla wszystkich funkcji i urządzeń sieciowych. Hasło powinno być wybrane przez użytkownika (i zawierać co najmniej 8 znaków, w tym wielkie i małe litery, cyfry i znaki specjalne), aby zwiększyć bezpieczeństwo produktu.*
- *Instalator i(lub) użytkownik końcowy ponoszą odpowiedzialność za prawidłową konfigurację wszystkich haseł i innych ustawień bezpieczeństwa.*

Katalog: W polu **Directory Structure** (Struktura katalogu) możesz wybrać katalog główny, katalog macierzysty i katalog podrzędny. Po wybraniu katalogu macierzystego możesz jako nazwę katalogu wybrać nazwę urządzenia, numer urządzenia lub IP urządzenia; po wybraniu katalogu podrzędnego możesz jako nazwę katalogu wybrać nazwę kamery lub numer kamery.

Upload Type (Typ wysyłania): Aby włączyć możliwość wysyłania zrobionych zdjęć na serwer FTP.

Anonymous Access to the FTP Server (Anonimowy dostęp do serwera FTP) (niewymagający podania nazwy użytkownika i hasła): Zaznacz pole wyboru **Anonymous** (Anonimowy), aby włączyć anonimowy dostęp do serwera FTP.

Uwaga: Serwer FTP musi obsługiwać funkcję anonimowego dostępu.

3. Kliknij **Save** (Zapisz), aby zapisać ustawienia.

Uwaga: Aby wgrywać zrobione zdjęcia na serwer FTP, musisz włączyć opcję czasowych zrzutów lub zrzutów wywołanych zdarzeniem na stronie **Snapshot** (Zrzut). Szczegółowe informacje znajdują się w *Sekcji 7.3*.

5.3.13 Dostęp do platformy

Dostęp do platformy to opcja umożliwiająca zarządzanie urządzeniami przez platformę EZVIZ Cloud P2P.

Uwaga: Funkcja dostępu do platformy różni się w zależności od modelu kamery,

kamera musi ją obsługiwać.

Zaznacz pole wyboru **Enable** (Włącz), aby włączyć EZVIZ Cloud P2P, można wówczas zarządzać urządzeniem przez witrynę EZVIZ Cloud P2P lub klienta EZVIZ Cloud P2P w postaci aplikacji na smartfony.

Jeśli ktoś nie chce zarządzać urządzeniami przez EZVIZ Cloud P2P, wystarczy zostawić niezaznaczone pole wyboru.



Figure 5-25 Dostęp do platformy

5.3.14 Ustawienia HTTPS

Cel:

HTTPS zapewnia uwierzytelnianie witryny WWW i powiązanego serwera WWW, z którym użytkownik się komunikuje, co chroni przed atakami typu Man-in-the-middle. Wykonaj następujące kroki, aby ustawić numer portu HTTPS.

Przykład: Jeśli ustawisz numer portu na 443, a adres IP to 192.168.1.64, możesz uzyskać dostęp do urządzenia, wpisując `https://192.168.1.64:443` w przeglądarce internetowej.

Kroki:

1. Przejdź do interfejsu ustawień HTTPS.

Configuration > Advanced Configuration > Network > HTTPS
(Konfiguracja > Konfiguracja zaawansowana > Sieć > HTTPS)

2. Zaznacz pole wyboru Enable HTTPS (Włącz HTTPS), aby włączyć tę funkcję.
3. Utwórz samodzielnie podpisywany certyfikat lub autoryzowany certyfikat.

TCP/IP Port DDNS PPPoE SNMP QoS FTP Wi-Fi UPnP™ Email NAT Platform Access **HTTPS**

Enable HTTPS

Create

Create Self-signed Certificate

Create Certificate Request

Install Signed Certificate

Certificate Path

Created Request

Created Request

Installed Certificate

Installed Certificate

Property Subject: C=CN, ST=ZJ, L=HZ, OU=embeddedsoftware, H/IP=192.0.0.64, EM=com.cn
 Issuer: C=CN, ST=ZJ, L=HZ, OU=embeddedsoftware, H/IP=192.0.0.64, EM=com.cn
 Validity: 2014-10-01 05:59:18 ~ 2017-09-30 05:59:18

Figure 5-26 Ustawienia HTTPS

- Utwórz samodzielnie podpisany certyfikat

1) Kliknij przycisk **Create** (Utwórz), aby otworzyć interfejs tworzenia.

Create

Create Self-signed Certificate

Create Certificate Request

Install Signed Certificate

Certificate Path

Created Request

Created Request

Installed Certificate

Installed Certificate

Figure 5-27 Tworzenie samodzielnie podpisanego certyfikatu

- 2) Wpisz kraj, nazwę/IP hosta, ważność i inne informacje.
- 3) Kliknij **OK**, aby zapisać ustawienia.

Uwaga: Jeśli masz już zainstalowany certyfikat, opcja tworzenia samodzielnie podpisanego certyfikatu będzie wyszarzona.

- **Utwórz autoryzowany certyfikat**
 - 1) Kliknij przycisk **Create** (Utwórz), aby utworzyć żądanie certyfikatu.
 - 2) Pobierz żądanie podpisania certyfikatu i złóż je w zaufanym centrum certyfikacji.
 - 3) Po otrzymaniu podpisanego ważnego certyfikatu zaimportuj certyfikat do urządzenia.
- 4. Po pomyślnym zakończeniu tworzenia i instalacji certyfikatu zostanie wyświetlona informacja o certyfikacie.

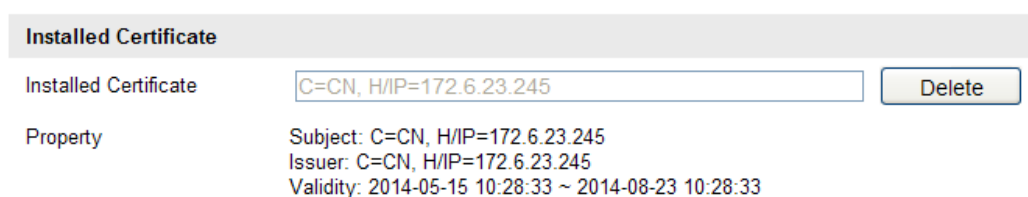


Figure 5-28 Zainstalowany certyfikat

5. Kliknij przycisk **Save** (Zapisz), aby zapisać ustawienia.

5.4 Konfiguracja ustawień wideo i audio

5.4.1 Konfiguracja ustawień wideo

Kroki:

1. Przejdź do interfejsu ustawień wideo:

Configuration > Basic Configuration > Video / Audio > Video (Konfiguracja > Konfiguracja podstawowa > Wideo / Audio > Wideo)

Lub **Configuration > Advanced Configuration > Video / Audio > Video** (Konfiguracja > Konfiguracja zaawansowana > Wideo / Audio > Wideo)

The screenshot shows a configuration window for video settings. At the top, there are tabs for 'Video', 'Audio', 'ROI', 'Display Info. on Stream', and 'Target Cropping'. The 'Video' tab is active. Below the tabs, there are several rows of settings, each with a label and a value or control:

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

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

Figure 5-29 Ustawienia wideo

- Wybierz **Stream Type** (Typ strumienia) kamery: main stream (normal) (strumień główny, ustawienie normalne), sub-stream (podstrumień) lub third stream (trzeci strumień).

Strumień główny jest zwykle używany do nagrywania i podglądu na żywo z dużą przepustowością, a podstrumienia i trzeciego strumienia można używać do podglądu na żywo, gdy przepustowość jest ograniczona.

- Możesz dopasować następujące parametry wybranego strumienia głównego lub podstrumienia:

Video Type (Typ wideo):

Wybierz typ strumienia jako strumieniowanie sygnału wideo lub kompozytowego sygnału wideo i audio. Sygnał audio będzie nagrywany tylko, jeśli jako **Video Type** (Typ wideo) zostanie wybrany **Video & Audio** (Wideo i audio).

Resolution (Rozdzielczość):

Wybierz rozdzielczość wyjścia wideo.

Bitrate Type (Typ przepływności):

Wybierz typ przepływności: constant (stała) lub variable (zmienna).

Video Quality (Jakość wideo):

Gdy jako typ przepływności zostanie wybrany **Variable** (Zmienna), dostępnych

jest 6 poziomów jakości wideo.

Frame Rate (Liczba klatek):

Ustaw liczbę klatek na 1/16~25 fps. Liczba klatek to częstotliwość, z jaką strumień wideo jest aktualizowany. Mierzy się ją w klatkach na sekundę (frames per second – fps). Wyższa liczba klatek jest zaletą, gdy w strumieniu wideo występuje ruch, ponieważ zostaje zachowana wysoka jakość obrazu w całym wideo.

Max. Bitrate (Maks. przepływność):

Ustaw maks. przepływność w zakresie 32~16384 Kb/s. Wyższa wartość odpowiada wyższej jakości wideo, ale jest dla niej wymagana wyższa przepustowość.

Uwaga: Limit maksymalnej przepływności zależy od platformy kamery. W niektórych kamerach limit to 8192 Kb/s lub 12288 Kb/s.

Video Encoding (Kodowanie wideo):

Jeśli **Stream Type** (Typ strumienia) jest ustawiony na main stream (strumień główny): Do wyboru są H.264 i MPEG4 ; jeśli typ strumienia jest ustawiony na sub-stream (podstrumień) lub third stream (trzeci strumień), do wyboru są H.264, MJPEG i MPEG4.

Uwaga: Typ kodowania wideo zależy od platformy kamery. W niektórych kamerach obsługiwany jest H.265, a nieobsługiwany MPEG4.

Profile (Profil):

Do wyboru dla kodowania są dostępne: Basic Profile (profil podstawowy), Main Profile (profil główny) i High Profile (profil wysoki).

I Frame Interval (Odstęp ramek I):

Ustaw odstęp ramek I w zakresie od 1 do 400.

SVC:

Scalable Video Coding (skalowalne kodowanie wideo) to rozszerzenie standardu H.264/AVC. Wybierz OFF/ON, aby wyłączyć/włączyć funkcję SVC. Po wybraniu Auto urządzenie będzie automatycznie wyodrębniało klatki z oryginalnego wideo, gdy przepustowość sieci jest niewystarczająca.

Smoothing (Zwiększanie płynności wideo):

Odnosi się do płynności strumienia. Im wyższa wartość płynności, tym lepiej płynnie strumień, chociaż pogorszeniu może ulec jakość wideo. Im niższa wartość płynności, tym wyższa jakość strumienia, ale nie będzie on przesyłany płynnie.

4. Kliknij **Save** (Zapisz), aby zapisać ustawienia.

5.4.2 Konfiguracja ustawień audio**Kroki:**

1. Otwórz interfejs ustawień audio:

Configuration > Basic Configuration > Video / Audio > Audio (Konfiguracja > Konfiguracja podstawowa > Wideo / Audio > Audio)

Lub **Configuration > Advanced Configuration > Video / Audio > Audio** (Konfiguracja > Konfiguracja zaawansowana > Wideo / Audio > Audio)

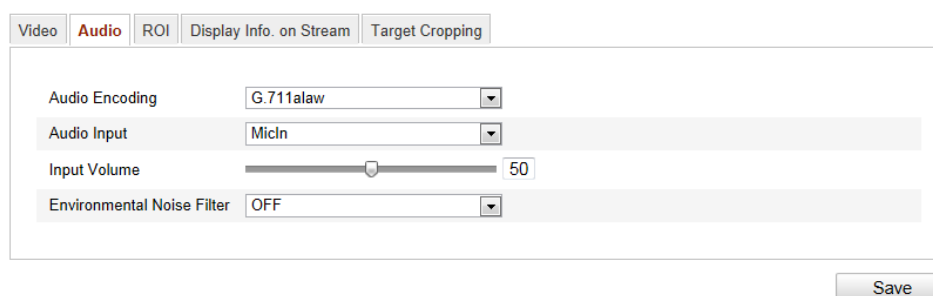


Figure 5-30 Ustawienia audio

2. Skonfiguruj następujące ustawienia.

Uwaga: Ustawienia audio zależą od modelu kamery.

Audio Encoding (Kodowanie audio): Do wyboru są G.722.1, G.711 ulaw, G.711alaw, G.726, MP2L2 i PCM. W przypadku MP2L2 można skonfigurować częstotliwość próbkowania i przepływność strumienia audio, w przypadku PCM można skonfigurować częstotliwość próbkowania.

Audio Input (Wejście audio): Do wyboru są dostępne MicIn i LineIn odpowiednio dla podłączonego mikrofonu i odbiornika.

Input Volume (Głośność wejścia): 0-100

Environmental Noise Filter (Filtr szumu otoczenia): Ustaw na OFF (Wył.) lub

ON (Wł.) Włączenie tej funkcji umożliwia częściowe filtrowanie szumu otoczenia.

3. Kliknij **Save** (Zapisz), aby zapisać ustawienia.

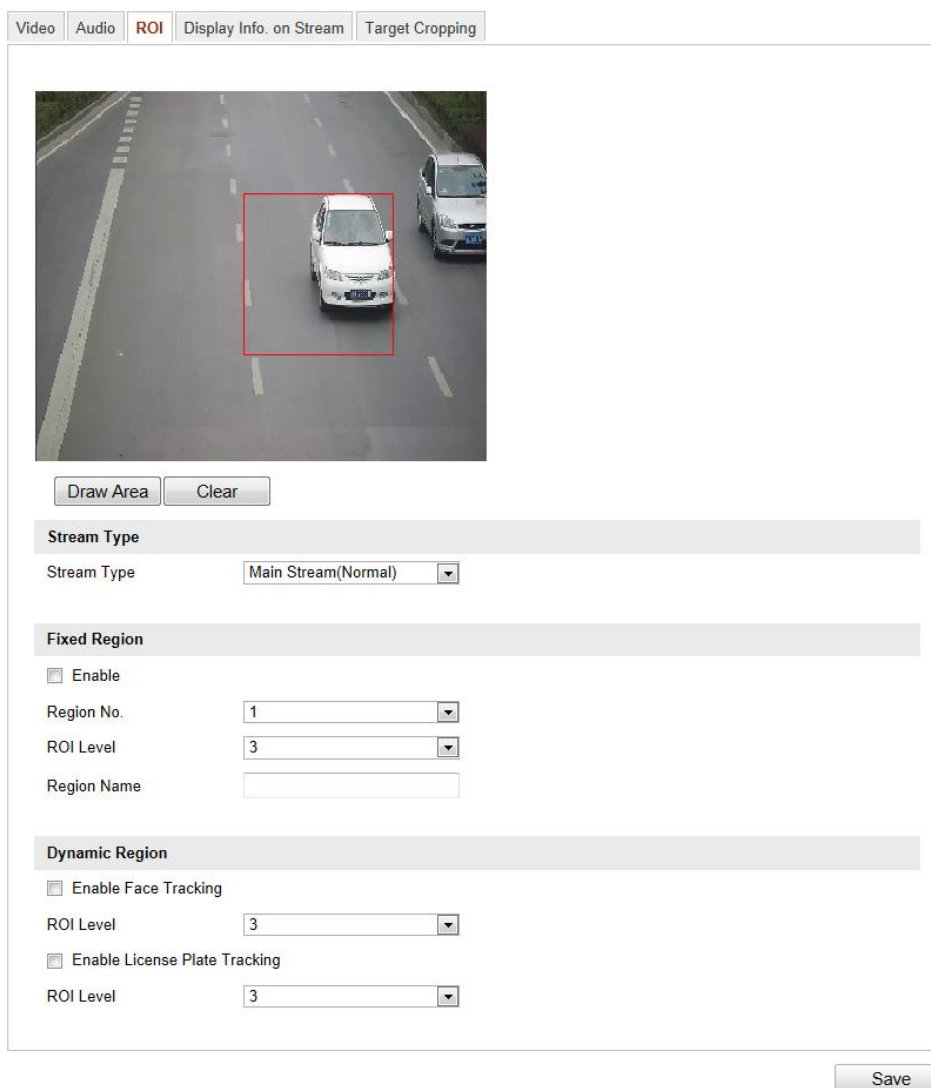
5.4.3 Konfiguracja kodowania ROI

Cel:

Kodowanie ROI (Region of Interest – obszar zainteresowania) pozwala na ustawienie różnych priorytetów dla ROI i informacji tła podczas kompresji wideo, co oznacza, że technologia przeznaczona więcej zasobów kodowania na obszar zainteresowania, aby zwiększyć jego jakość, natomiast informacje tła są traktowane drugorzędnie.

Uwaga: Funkcja ROI zależy od modelu kamery.

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



Draw Area Clear

Stream Type
Stream Type Main Stream(Normal)

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

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

Save

Figure 5-31 Ustawienia obszaru zainteresowania

Konfiguracja stałego obszaru dla ROI:

Kroki:

1. Przejdź do interfejsu ustawień ROI:
Configuration > Advanced Configuration > Video/Audio > ROI (Konfiguracja > Konfiguracja zaawansowana > Video/Audio > ROI)
2. Zaznacz pole wyboru **Enable** (Włącz) obok opcji Fixed Region (Stały obszar).
3. Wybierz typ strumienia dla kodowania ROI.
4. Wybierz obszar z listy rozwijanej ustawień ROI. Do wyboru są cztery stałe obszary.
5. Kliknij przycisk **Draw Area** (Narysuj obszar), a następnie kliknij i przeciągnij myszą, aby narysować obszar zainteresowania na wideo na żywo.
6. Wybierz poziom ROI, aby ustawić poziom wzmocnienia jakości obrazu. Im większa wartość, tym lepsza będzie jakość obrazu.
7. Wpisz nazwę obszaru dla ROI.
8. Kliknij **Save** (Zapisz), aby zapisać ustawienia.

Konfiguracja opcji Dynamic Region (Dynamiczny obszar) dla ROI:

1. Przejdź do interfejsu ustawień ROI:
Configuration > Advanced Configuration > Video/Audio > ROI (Konfiguracja > Konfiguracja zaawansowana > Video/Audio > ROI)
2. Zaznacz pole wyboru **Enable Face Tracking** (Włącz śledzenie twarzy), wówczas jako obszar zainteresowania zostanie ustawiony zarejestrowany obraz twarzy.
Uwaga: Aby włączyć funkcję śledzenia twarzy, funkcja wykrywania twarzy musi być obsługiwana i włączona.
3. Zaznacz pole wyboru **Enable License Plate Tracking** (Włącz śledzenie tablic rejestracyjnych), wówczas jako obszar zainteresowania zostanie ustawiony zarejestrowany obraz tablicy rejestracyjnej.

Uwaga: Aby włączyć funkcję śledzenia tablic rejestracyjnych, funkcja

wykrywania pojazdów musi być obsługiwana i włączona.

4. Odpowiednio należy ustawić poziom ROI. Im większa wartość, tym lepsza będzie jakość obrazu.
5. Wybierz typ strumienia dla kodowania ROI.
6. Kliknij **Save** (Zapisz), aby zapisać ustawienia.

5.4.4 Wyświetlanie informacji na strumieniu

Zaznacz pole wyboru **Enable Dual-VCA** (Włącz podwójne VCA), wówczas informacje o obiektach (ludziach, pojazdach itp.) będą oznaczane w strumieniu wideo. Można wówczas ustanowić zasady w podłączonym urządzeniu końcowym, aby wykrywać zdarzenia takie, jak przekraczanie linii, wtargnięcie itp.

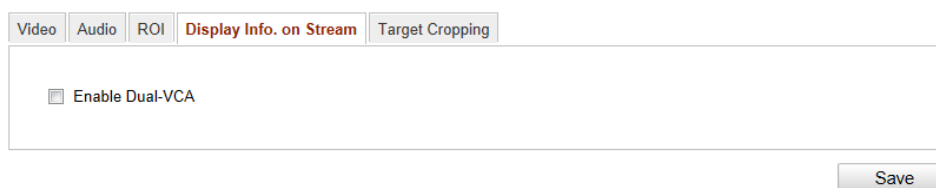


Figure 5-32 Wyświetlanie informacji na strumieniu

5.4.5 Konfiguracja przycinania celu

Cel:

Można określić obszar docelowy na wideo na żywo, a następnie wyświetlić go w trzecim strumieniu w innej rozdzielczości, aby w razie potrzeby dany obszar docelowy zawierał więcej szczegółów.

Uwaga: Funkcja przycinania celu zależy od modelu kamery.

Kroki:

1. Przejdź do interfejsu ustawień przycinania celu:

Configuration > Advanced Configuration > Video/Audio > Target Cropping

(Konfiguracja > Konfiguracja zaawansowana > Wideo/Audio > Przycinanie celu).

2. Zaznacz pole wyboru **Enable Target Cropping** (Włącz przycinanie celu), aby włączyć tę funkcję.
3. Jako Stream Type (typ strumienia) ustaw Third Stream (trzeci strumień).
4. Wybierz opcję Cropping Resolution (rozdzielczość przycinania) dla wyświetlania wideo obszaru docelowego. Na wideo na żywo wyświetla się czerwony prostokąt oznaczający obszar docelowy, można go kliknąć i przeciągnąć, aby zlokalizować na ekranie obszar docelowy.
5. Kliknij **Save** (Zapisz), aby zapisać ustawienia. Możesz przejść do strony podglądu na żywo i kliknąć zakładkę **Third Stream** (Trzeci strumień), aby wyświetlić wideo obszaru docelowego.

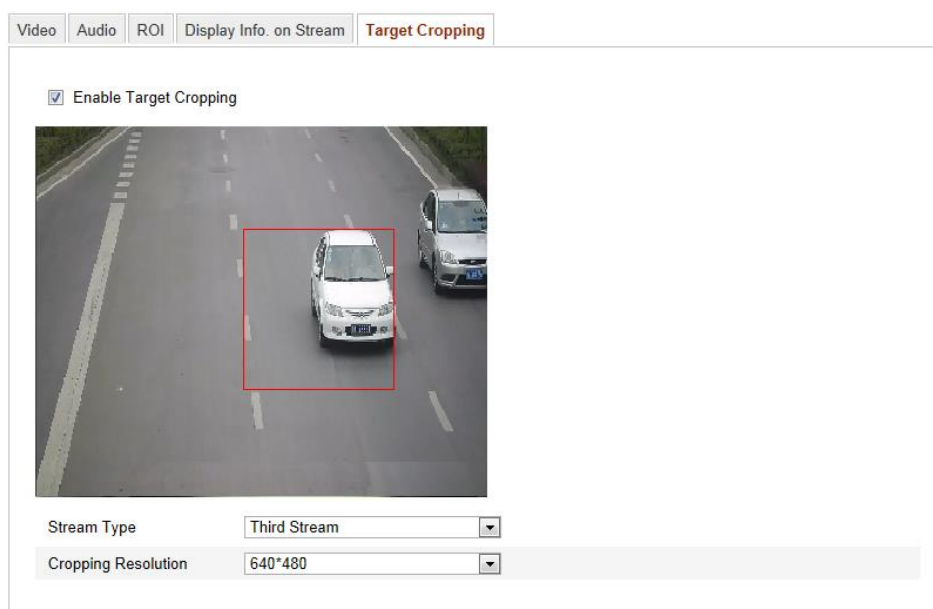


Figure 5-33 Przycinanie celu

5.5 Konfigurowanie parametrów obrazu

5.5.1 Konfigurowanie ustawień wyświetlania

Cel:

Możesz ustawić jakość obrazu z kamery, w tym jasność, kontrast, nasycenie, odcień, ostrość itp.

Uwaga: Parametry wyświetlania zależą od modelu kamery. Należy się kierować

faktycznym interfejsem, aby dowiedzieć się więcej.

Kroki:

1. Przejdź do interfejsu ustawień wyświetlania:

Configuration > Basic Configuration> Image> Display Settings
(Konfiguracja > Konfiguracja podstawowa > Obraz > Ustawienia wyświetlania)

Lub **Configuration > Advanced Configuration> Image> Display Settings**
(Konfiguracja > Konfiguracja zaawansowana > Obraz > Ustawienia wyświetlania)

2. Ustaw parametry obrazu z kamery.

Uwaga: Aby zagwarantować jakość obrazu w różnych warunkach oświetlenia, dostępne są dwa zestawy parametrów konfigurowanych przez użytkownika.

Day/Night Auto-switch (Automatyczne przełączanie Dzień/Noc)

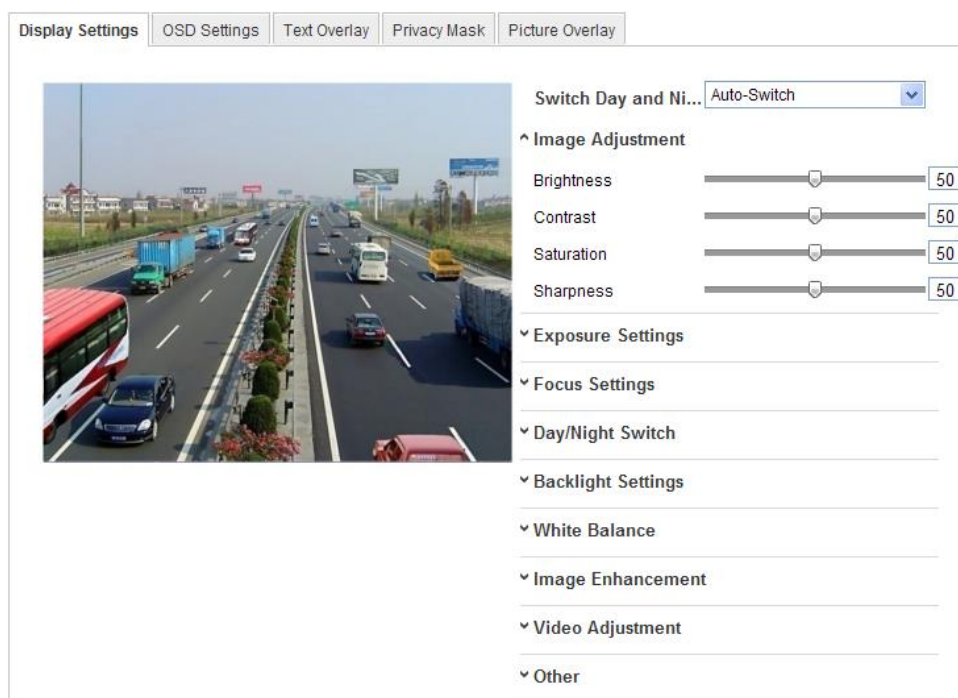


Figure 5-34 Ustawienia wyświetlania automatycznego przełączania Dzień/Noc

◆ Image Adjustment (Dostosowanie obrazu)

Brightness (Jasność) opisuje jasność obrazu w zakresie od 1 do 100, wartość domyślna to 50.

Contrast (Kontrast) opisuje kontrast obrazu w zakresie od 1 do 100, wartość domyślna to 50.

Saturation (Nasylenie) opisuje nasylenie kolorów obrazu w zakresie od 1 do 100,

wartość domyślna to 50.

Sharpness (Ostrość) opisuje kontrast krawędzi obrazu w zakresie od 1 do 100, wartość domyślna to 50.

◆ **Exposure Settings (Ustawienia ekspozycji)**

Jeśli kamera jest wyposażona w stały obiektyw, do wyboru jest tylko ustawienie **Manual** (Ręczne), nie można skonfigurować trybu przysłony.

Jeśli wybrano **Auto**, można ustawić automatyczny poziom przysłony w zakresie od 0 do 100.

Jeśli kamera obsługuje obiektyw **P-Iris**, to w przypadku zamontowania obiektywu P-Iris można wybrać typ obiektywu P-Iris, np.: Tamron 2,8-8 mm F1.2 (M13VP288-IR), jeśli natomiast jest zamontowany obiektyw DC, do wyboru są Manual (Ręczne) i Auto.

Exposure time (Czas ekspozycji) oznacza czas otwarcia elektronicznej migawki w zakresie od 1 s do 1/100 000 s. Dostosuj go zgodnie z rzeczywistymi warunkami oświetlenia.

◆ **Focus Settings (Ustawienia ostrości)**

Jeśli kamera obsługuje elektroniczny obiektyw, tryb ustawiania ostrości można ustawić na Auto, Manual (Ręczne) lub Semi-auto (Półautomatyczne). W przypadku wyboru Auto ostrość jest ustawiana automatycznie zgodnie z rzeczywistym scenariuszem monitorowania; w przypadku wyboru Manual (Ręczne) można sterować obiektywem (ustawianiem zoomu i ostrości, inicjalizacją obiektywu i wspomaganie ostrości) za pomocą interfejsu sterowania PTZ; w przypadku wyboru Semi-auto (Półautomatyczne) kamera będzie automatycznie ustawiała ostrość w momencie dopasowania parametrów zoomu.

◆ **Day/Night Switch (Przełączanie Dzień/Noc)**

Wybierz tryb przełączania Dzień/Noc i skonfiguruj w tej opcji ustawienia inteligentnej podczerwieni.

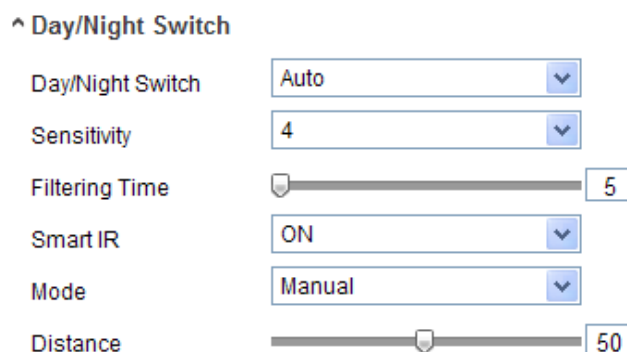


Figure 5-35 Przełączanie Dzień/Noc

Do wyboru dla przełączania Dzień/Noc są dostępne ustawienia: Day (dzień), Night (noc), Auto, Schedule (harmonogram) i Triggered by alarm input (wyzwolenie przez wejście alarmowe).

Day (Dzień): kamera pozostaje w trybie Dzień.

Night (Noc): kamera pozostaje w trybie Noc.

Auto: Kamera automatycznie przełącza się między trybami Dzień i Noc zależnie od oświetlenia. Zakres czułości wynosi od 0 do 7, im wyższa wartość, tym łatwiej przełącza się tryb. Czas filtrowania odnosi się do odstępu czasowego między przełączeniem Dzień/Noc. Można go ustawić w zakresie od 5 s do 120 s.

Schedule (Harmonogram): Ustaw czas rozpoczęcia i zakończenia, aby określić czas trwania trybu Dzień/Noc.

Triggered by alarm input (Wyzwolenie przez wejście alarmowe): Przełączenie jest wyzwalane przez wejście alarmowe, można ustawić wyzwalany tryb na Dzień i Noc.

Smart IR: Funkcja Smart IR (inteligentna podczerwień) daje użytkownikowi możliwość regulacji mocy LED podczerwieni, aby uzyskać wyraźny obraz, który nie jest ani prześwietlony, ani niedoświetlony. Wybierz ON (Wł.), aby włączyć Smart IR, wówczas do wyboru są tryby podczerwieni Auto i Manual (Ręczne).

Po wybraniu AUTO moc diody świecącej IR zmienia się automatycznie zgodnie z rzeczywistym oświetleniem. Np. jeśli aktualna scena jest wystarczająco jasna, dioda podczerwieni nastawia się sama na niższą moc, a jeśli scena nie jest wystarczająco jasna, dioda podczerwieni nastawia się sama na wyższą moc.

Po wybraniu Manual (Ręczne) można ręcznie ustawić wartość odległości między

kamerą IR i obiektem, aby dostosować moc diody podczerwieni. Mała odległość wskazuje, że obiekt jest blisko kamery IR, a urządzenie ustawia niższą moc diody podczerwieni, aby uniknąć prześwietlenia; duża odległość wskazuje, że obiekt jest daleko, a urządzenie ustawia wyższą moc diody podczerwieni, aby uniknąć niedoświetlonego obrazu.

◆ Ustawienia podświetlenia

BLC (Kompensacja podświetlenia): Gdy kamera skupia ostrość na obiekcie znajdującym się pod światło, obiekt będzie zbyt ciemny i niewyraźny. BLC kompensuje światło na obiekcie z przodu, aby był on wyraźny. Do wyboru są ustawienia OFF (Wył.), Up (Góra), Down (Dół), Left (Lewo), Right (Prawo), Center (Środek) i Customize (Własne).

WDR (Szeroki zakres dynamiki): Funkcji WDR można używać, gdy w scenie występuje wysoki kontrast między obszarami jasnymi i ciemnymi.

HLC (Kompensacja silnych źródeł światła): Funkcji HLC można używać, gdy w scenie występują silne źródła światła, pogarszające jakość obrazu.

◆ White Balance (Balans bieli)

Balans bieli to funkcja odwzorowania bieli w kamerze, służąca do dopasowania temperatury barwowej do otoczenia.

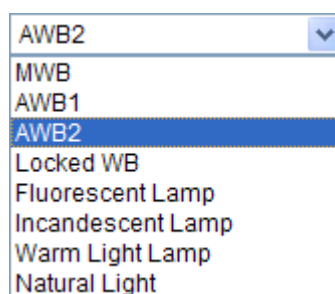


Figure 5-36 Balans bieli

◆ Image Enhancement (Ulepszanie obrazu)

DNR (Cyfrowa redukcja szumów): DNR (Digital Noise Reduction – Cyfrowa redukcja szumów) zmniejsza ilość szumów w strumieniu wideo. Do wyboru są ustawienia OFF (Wył.), Normal Mode (Tryb normalny) i Expert Mode (Tryb zaawansowany). Ustaw poziom DNR w zakresie od 0 do 100, wartość domyślna to 50

w Trybie normalnym. Ustaw poziom DNR z poziomu DNR przestrzeni [0~100] i czasu [0~100] w Trybie zaawansowanym.

Defog Mode (Tryb usuwania zamglenia): Można włączyć funkcję usuwania zamglenia, gdy w otoczeniu występuje mgła i przez to obraz jest niewyraźny. Wzmacnia to drobne szczegóły, dzięki czemu obraz jest wyraźniejszy.

Electronic Image Stabilizer (Elektroniczny stabilizator obrazu): EIS (Electronic Image Stabilizer – Elektroniczny stabilizator obrazu) zmniejsza efekty drgań na wideo.

Grey Scale (Skala szarości): Można wybrać zakres skali szarości jako [0-255] lub [16-235].

◆ **Video Adjustment (Regulacja wideo)**

Mirror (Lustro): Odbija obraz, dzięki czemu jest wyświetlany jako odwrócony. Do wyboru są ustawienia Left/Right (Lewo/Prawo), Up/Down (Góra/Dół), Center (Środek) i OFF (Wył.).

Rotate (Obróć): Aby w pełni wykorzystać proporcje obrazu 16:9, można włączyć funkcję obracania obrazu, gdy kamera jest używana w scenie o wąskim polu widoku. Podczas instalacji obróć kamerę o 90 stopni lub obróć trójosiowy obiektyw o 90 stopni i ustaw tryb obracania na włączony. Wyświetli się normalny widok sceny z proporcją obrazu 9:16, aby ignorować niepotrzebne informacje, takie jak ściana, a w scenie umieszczać bardziej istotne informacje.

Scene Mode (Tryb sceny): Wybierz scenę jako Indoor (Wnętrze) lub Outdoor (Na zewnątrz), zależnie od rzeczywistego otoczenia.

Video Standard (Standard wideo): Do wyboru są 50 Hz i 60 Hz. Wybierz wartość odpowiednią dla standardu wideo, zwykle jest to 50 Hz dla PAL i 60 Hz dla NTSC.

Capture Mode (Tryb przechwytywania): Jest to wybierany przez użytkownika tryb wejścia wideo, pasujący do różnych wymagań w zakresie pola widzenia i rozdzielczości.

Lens Distortion Correction (Korekta zniekształceń obiektywu): Wybierz ON/OFF (Wł./Wył.), aby włączyć/wyłączyć korektę zniekształceń obiektywu. Włączenie tej

funkcji powoduje korektę zniekształceń obrazu spowodowanych przez obiektyw szerokokątny.

◆ Other (Inne)

Niektóre kamery obsługują CVBS, SDI lub wyjście HDMI. Należy się kierować faktycznym modelem kamery, aby dowiedzieć się więcej.

Day/Night Scheduled-Switch (Zaplanowane przełączanie Dzień/Noc)

Interfejs konfiguracji zaplanowanego przełączania Dzień/Noc pozwala na ustawienie odrębnych parametrów kamery dla dnia i nocy, aby zagwarantować jakość obrazu przy różnym oświetleniu.



Figure 5-37 Interfejs konfiguracji zaplanowanego przełączania Dzień/Noc

Kroki:

1. Kliknij oś czasu, aby wybrać czas rozpoczęcia i czas zakończenia przełączenia.
2. Kliknij zakładkę Common (Często używane), aby skonfigurować parametry często używane w trybie Dzień i Noc.

Uwaga: Aby dowiedzieć się więcej na temat każdego parametru, należy się zapoznać z sekcją Automatyczne przełączanie Dzień/Noc.

3. Kliknij zakładkę Day (Dzień), aby skonfigurować parametry stosowane w trybie Dzień.
4. Kliknij zakładkę Night (Noc), aby skonfigurować parametry stosowane w trybie

Noc.

Uwaga: W przypadku zmiany któregoś parametru ustawienia są zapisywane automatycznie.

5.5.2 Konfiguracja ustawień OSD

Cel:

Można zmienić nazwę kamery i godzinę wyświetlaną na ekranie.

Kroki:

1. Przejdź do interfejsu ustawień OSD:

Configuration > Advanced Configuration > Image > OSD Settings

(Konfiguracja > Konfiguracja zaawansowana > Obraz > Ustawienia OSD)

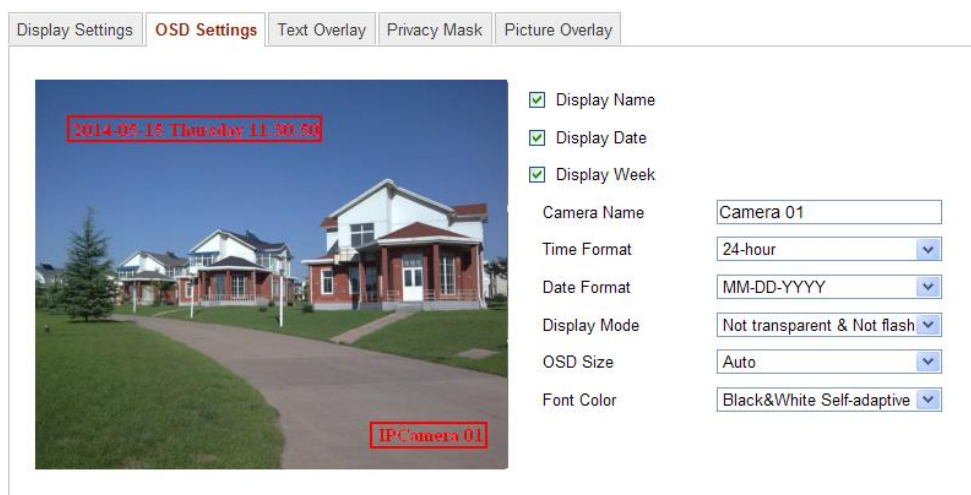


Figure 5-38 Ustawienia OSD

2. Zaznacz odpowiednie pole wyboru, aby wybrać, co ma być wyświetlane: nazwa kamery, data lub tydzień.
3. Wyedytuj nazwę kamery w polu tekstowym **Camera Name** (Nazwa kamery).
4. Wybierz z listy rozwijanej opcje ustawienia formatu godziny, formatu daty, trybu wyświetlania i rozmiaru czcionki OSD.
5. Zdefiniuj kolor czcionki OSD, klikając menu rozwijane, do wyboru są black & white self-adaptive (czarno-biały, automatycznie dopasowujący się) i custom (własny).

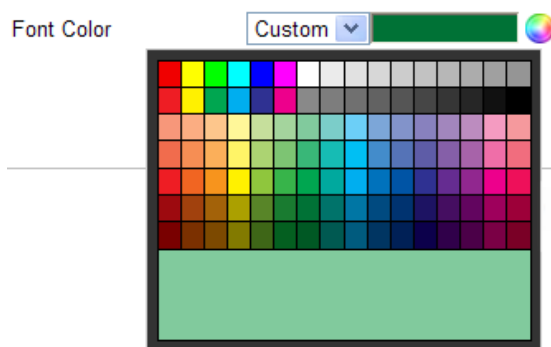


Figure 5-39 Kolor czcionki – Własny

- Kliknij i przeciągnij myszą ramkę tekstową **IPCamera 01** w oknie podglądu na żywo, aby dopasować pozycję OSD.

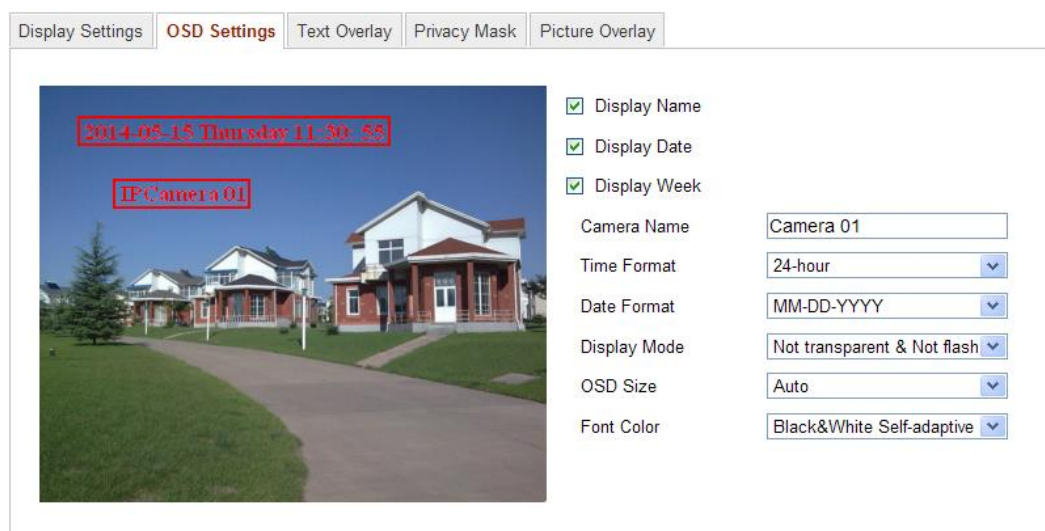


Figure 5-40 Dopasowanie położenia OSD

- Kliknij **Save** (Zapisz), aby aktywować powyższe ustawienia.

5.5.3 Konfiguracja ustawień tekstu na obrazie

Cel:

Można dostosować tekst na obrazie.

Kroki:

- Przejdź do interfejsu ustawień tekstu na obrazie:

Configuration > Advanced Configuration > Image > Text Overlay (Konfiguracja > Konfiguracja zaawansowana > Obraz > Tekst na obrazie)

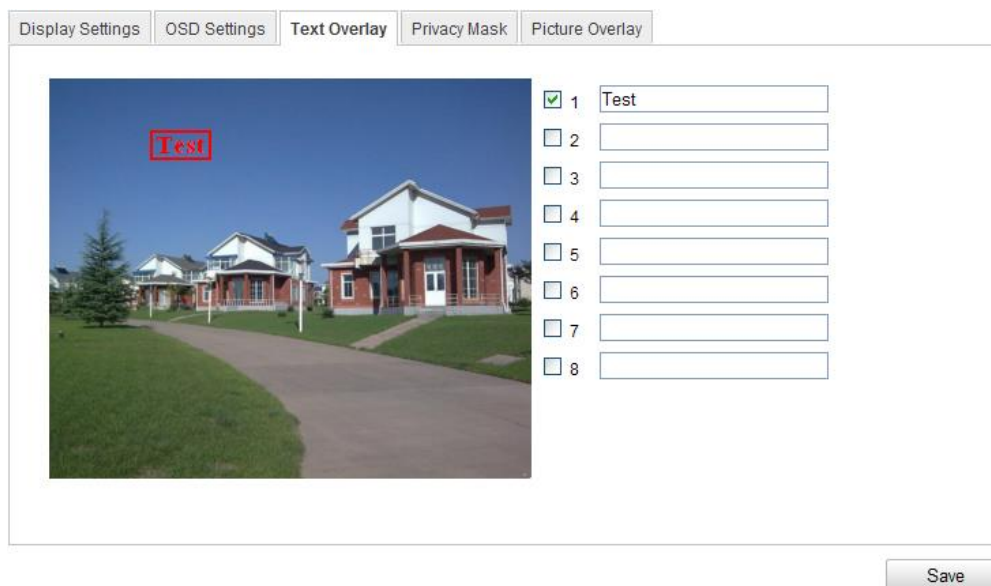


Figure 5-41 Tekst na obrazie

2. Zaznacz pole wyboru obok pola tekstowego, aby włączyć wyświetlanie ekranowe.
3. W polu tekstowym wpisz znaki.
4. (Opcja) Kliknij i przeciągnij myszą czerwoną ramkę tekstową **Test** w oknie podglądu na żywo, aby dopasować pozycję tekstu na obrazie.
5. Kliknij **Save** (Zapisz), aby zapisać ustawienia.

Uwaga: Można skonfigurować maks. 8 tekstów na obrazie.

5.5.4 Konfiguracja maski prywatności

Cel:

Maska prywatności pozwala na zasłanianie niektórych obszarów wideo na żywo, aby pewne miejsca w obszarze monitorowania nie były oglądane na żywo ani nagrywane.

Kroki:

1. Przejdź do interfejsu ustawień maski prywatności:

Configuration > Advanced Configuration > Image > Privacy Mask (Konfiguracja > Konfiguracja zaawansowana > Obraz > Maska prywatności)

2. Zaznacz pole wyboru **Enable Privacy Mask** (Włącz maskę prywatności), aby włączyć tę funkcję.

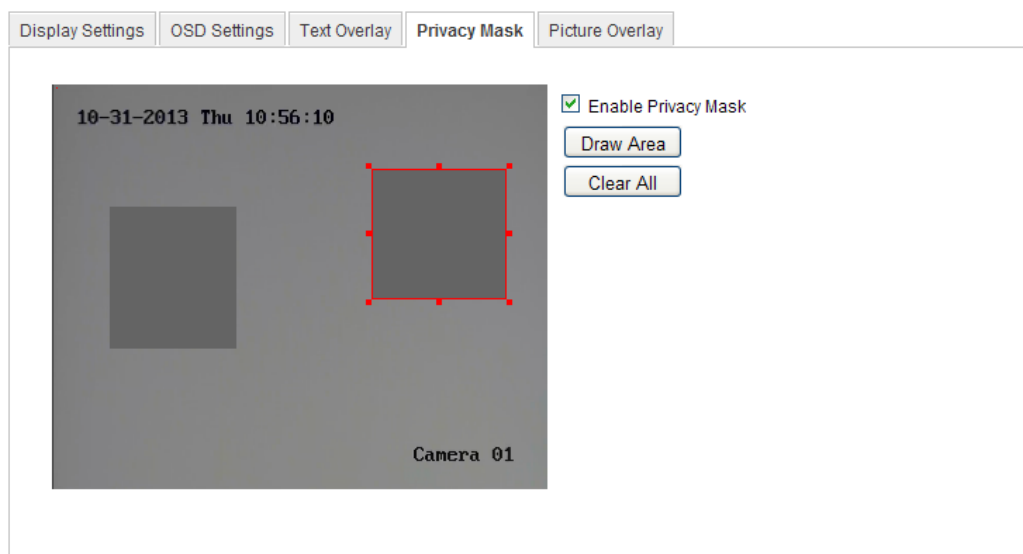
3. Kliknij **Draw Area** (Narysuj obszar).

Figure 5-42 Ustawienia maski prywatności

4. Kliknij i przeciągnij myszą w oknie wideo na żywo, aby narysować obszar maski.

Uwaga: Na tym samym obrazie można narysować maks. 4 obszary.

5. Kliknij **Stop Drawing** (Zakończ rysowanie), aby zakończyć rysowanie, lub kliknij **Clear All** (Usuń wszystko), aby usunąć wszystkie ustawiane obszary, nie zapisując ich.6. Kliknij **Save** (Zapisz), aby zapisać ustawienia.

5.5.5 Konfiguracja nakładania obrazów

Cel:

Nakładanie obrazów pozwala nałożyć jeden obraz na innym. Dzięki tej funkcji firmy lub użytkownicy mogą nałożyć swoje logo na obrazie.

Uwaga: Obraz musi być w formacie RGB24 bmp i mieć maksymalny rozmiar 128*128.

Kroki:

1. Przejdź do interfejsu ustawień nakładania obrazów:

Configuration > Advanced Configuration> Image > Picture Overlay
(Konfiguracja > Konfiguracja zaawansowana > Obraz > Nakładanie

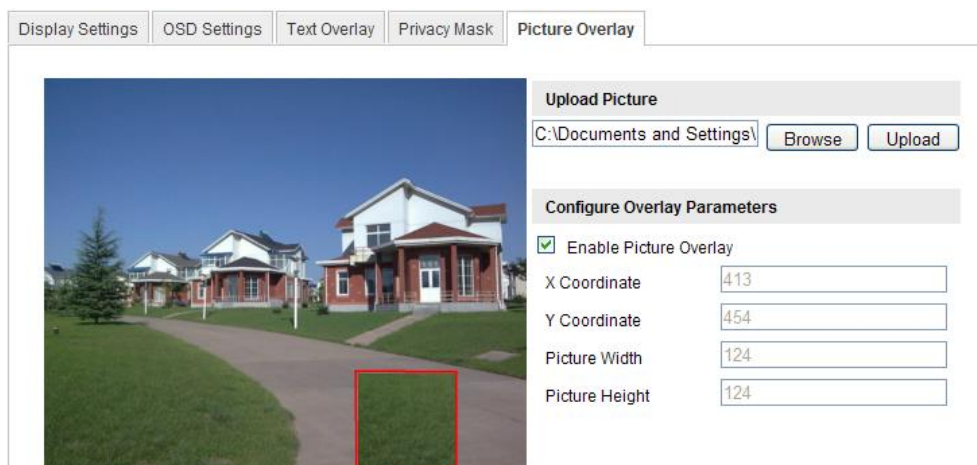
obrazów)

Figure 5-43 Nakładanie obrazów

2. Kliknij **Browse** (Przełóżaj), aby wybrać obraz.
3. Kliknij **Upload** (Wyślij), aby go wysłać.
4. Zaznacz pole wyboru **Enable Picture Overlay** (Włącz nakładanie obrazów), aby włączyć tę funkcję.

Wartości współrzędnych X Coordinate i Y Coordinate dotyczą położenia obrazu na obrazie. Picture Width (Szerokość obrazu) i Picture Height (Wysokość obrazu) pokazuje rozmiar nakładanego obrazu.


5.6 Konfiguracja i obsługa alarmów

Ta sekcja wyjaśnia, jak skonfigurować kamerę sieciową, aby reagowała na zdarzenia alarmowe, takie jak wykrycie ruchu, manipulacja wideo, wejście alarmowe, wyjście alarmowe, wyjątek, wykrywanie twarzy, wykrywanie wyjątku audio, wykrywanie wtargnięcia, wykrywanie utraty ostrości, wykrywanie zmiany sceny itp. Te zdarzenia mogą wyzwolić powiązane metody, takie jak powiadomienie centrum monitoringu, wysłanie e-maila, wyzwolenie wyjścia alarmowego itp.

Uwagi:

- Zaznacz pole wyboru **Notify Surveillance Center** (Powiadom centrum monitoringu), aby informacja o alarmie była wysyłana w trybie push do komputera lub oprogramowania klienta w smartfonie natychmiast po wyzwoleniu

alarmu.

- Kliknij , aby uzyskać pomoc podczas konfiguracji inteligentnych funkcji, takich jak wykrywanie twarzy, wykrywanie wtargnięcia, wykrywanie utraty ostrości, wykrywanie zmiany sceny itp. Dokument pomocy przeprowadzi użytkownika przez czynności konfiguracji.

5.6.1 Konfiguracja wykrywania ruchu

Cel:

Wykrywanie ruchu wykrywa obiekty poruszające się w skonfigurowanym obszarze monitoringu. Wyzwolenie alarmu może spowodować podjęcie szeregu działań.

Aby dokładnie wykrywać poruszające się obiekty i zmniejszyć częstość fałszywych alarmów, dla różnych środowisk wykrywania ruchu jest dostępna konfiguracja normalna i zaawansowana.

➤ **Normal Configuration (Konfiguracja normalna)**

W konfiguracji normalnej jest stosowany jeden i ten sam zestaw parametrów wykrywania ruchu w dzień i w nocy.

Zadania:

1. Ustaw obszar wykrywania ruchu.

Kroki:

- (1)Przejdź do interfejsu ustawień wykrywania ruchu:

Configuration > Advanced Configuration> Basic Event > Motion

Detection (Konfiguracja > Konfiguracja zaawansowana > Zdarzenie podstawowe > Wykrywanie ruchu)

- (2)Zaznacz pole wyboru **Enable Motion Detection** (Włącz wykrywanie ruchu).

- (3)Zaznacz pole wyboru **Enable Dynamic Analysis for Motion** (Włącz dynamiczną analizę ruchu), aby wykryte obiekty były oznaczane zielonymi prostokątami.

Uwaga: Wybierz Disable (Wyłącz) dla reguł, jeśli wykryte obiekty nie mają

być oznaczane prostokątami. Wybierz **Disable (Wyłącz)** w **Configuration > Local Configuration > Live View Parameters > Rules** (Konfiguracja > Konfiguracja lokalna > Parametry widoku na żywo > Reguły).

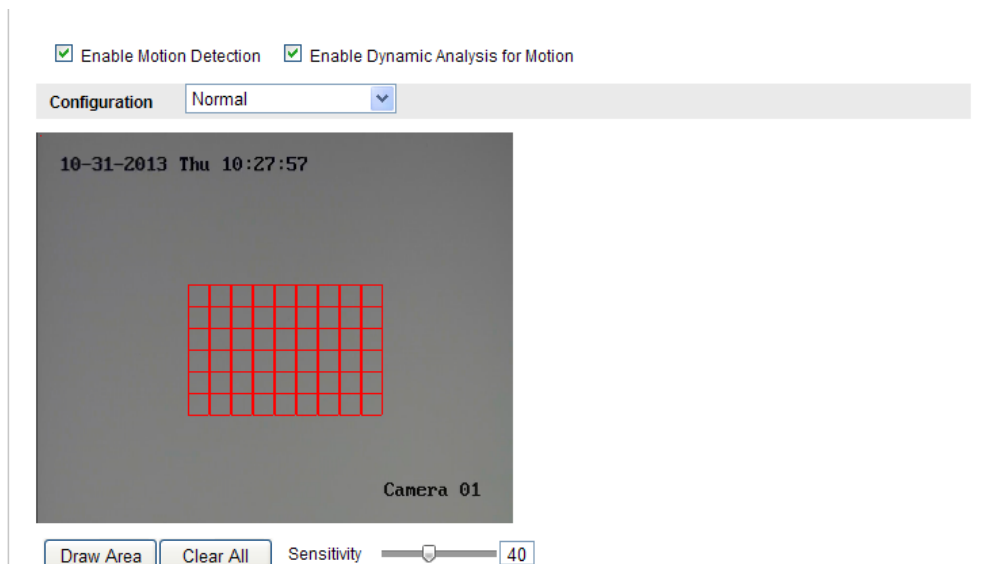


Figure 5-44 Włączanie wykrywania ruchu

- (4) Kliknij **Draw Area** (Narysuj obszar). Kliknij i przeciągnij myszą w oknie wideo na żywo, aby narysować obszar wykrywania ruchu.
- (5) Kliknij **Stop Drawing** (Zakończ rysowanie), aby zakończyć rysowanie jednego obszaru.
- (6)(Opcja) Kliknij **Clear All** (Usuń wszystko), aby wyczyścić wszystkie obszary.
- (7)(Opcja) Przesuń suwak, aby ustawić czułość wykrywania.

2. Ustaw harmonogram uzbrajania dla wykrywania ruchu.

Kroki:

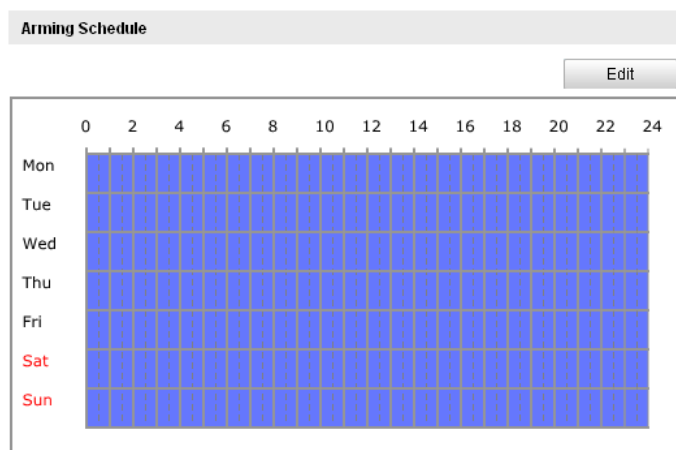

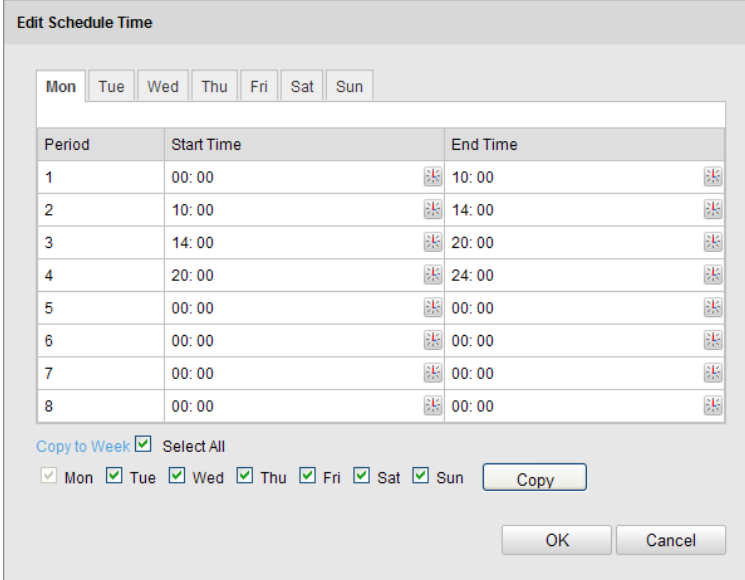


Figure 5-45 Czas uzbrajania

- (1) Kliknij **Edit** (Edytuj), aby edytować harmonogram uzbrajania. Ilustracja 6-45 przedstawia interfejs edycji harmonogramu uzbrajania.
- (2) Wybierz dzień, w którym ma zostać ustawiony harmonogram uzbrajania.
- (3) Kliknij , aby ustawić okres harmonogramu uzbrajania.
- (4) (Opcja) Po ustawieniu harmonogramu uzbrajania możesz go skopiować do innych dni.
- (5) Kliknij **OK**, aby zapisać ustawienia.

Uwaga: Okresy nie mogą się nakładać. Dla każdego dnia można skonfigurować maks. 8 okresów.



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

Copy to Week Select All

Mon Tue Wed Thu Fri Sat Sun

Figure 5-46 Harmonogram czasu uzbrajania

3. Ustaw działania alarmu dla wykrywania ruchu.

Zaznacz pole wyboru, aby wybrać powiązaną metodę. Do wyboru są: Audible Warning (Ostrzeżenie dźwiękowe), Notify surveillance center (Powiadom centrum monitoringu), Send Email (Wyślij e-mail), Upload to FTP (Wyślij do FTP), Trigger channel (Kanał wyzwiania) i Trigger alarm output (Wyzwól wyjście alarmowe). Można określić powiązaną metodę w sytuacji wystąpienia zdarzenia.

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

Figure 5-47 Powiązana metoda

- **Audible Warning (Ostrzeżenie dźwiękowe)**

Wyzwól lokalne ostrzeżenie dźwiękowe. Jest ono obsługiwane wyłącznie przez urządzenie wyposażone w wyjście audio.

- **Notify Surveillance Center (Powiadom centrum monitoringu)**

Wyślij wyjątek lub sygnał alarmu do oprogramowania do zdalnego zarządzania, gdy wystąpi zdarzenie.

- **Send Email (Wyślij e-mail)**

Wyślij e-mail z informacją o alarmie do jednego lub większej liczby użytkowników, gdy wystąpi zdarzenie.

Uwaga: Aby wysyłać e-mail, gdy wystąpi zdarzenie, zapoznaj się z *Sekcją 6.3.10 Wysyłanie e-maila wyzwolonego przez alarm*, aby ustawić powiązane parametry.

- **Upload to FTP (Wyślij do FTP)**

Po wyzwoleniu alarmu zrób zdjęcie i wyślij je do serwera FTP.

Uwagi:

- Najpierw trzeba ustawić adres FTP i zdalny serwer FTP. Szczegółowe informacje znajdują się w *Sekcji 6.3.12 Konfiguracja ustawień FTP*.
- Przejdź do strony **Advanced Configuration > Storage > Snapshot** (Konfiguracja zaawansowana > Pamięć danych > Zrzut), ustaw odstęp między zdjęciami i liczbę zdjęć.
- Zrobione zdjęcie można też zapisać na dostępnej karcie SD lub dysku sieciowym.

- **Trigger Channel (Kanał wyzwiania)**

W przypadku wykrycia ruchu zostanie nagrane wideo. Aby korzystać z tej funkcji, należy ustawić harmonogram nagrywania. Szczegółowe informacje znajdują się w *Sekcji 7.2*.

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

Gdy wystąpi zdarzenie, wyzwoł jedno lub większą liczbę wyjść alarmowych.

Uwaga: Aby ustawić powiązane parametry wyzwiania wyjścia alarmowego, gdy wystąpi zdarzenie, zapoznaj się z *Sekcją 6.6.4 Konfiguracja wyjścia alarmowego*.

➤ **Expert Configuration (Konfiguracja zaawansowana)**

Tryb zaawansowany służy głównie do konfiguracji czułości i proporcji obiektu w każdym obszarze dla różnych przełączeń Dzień/Noc.

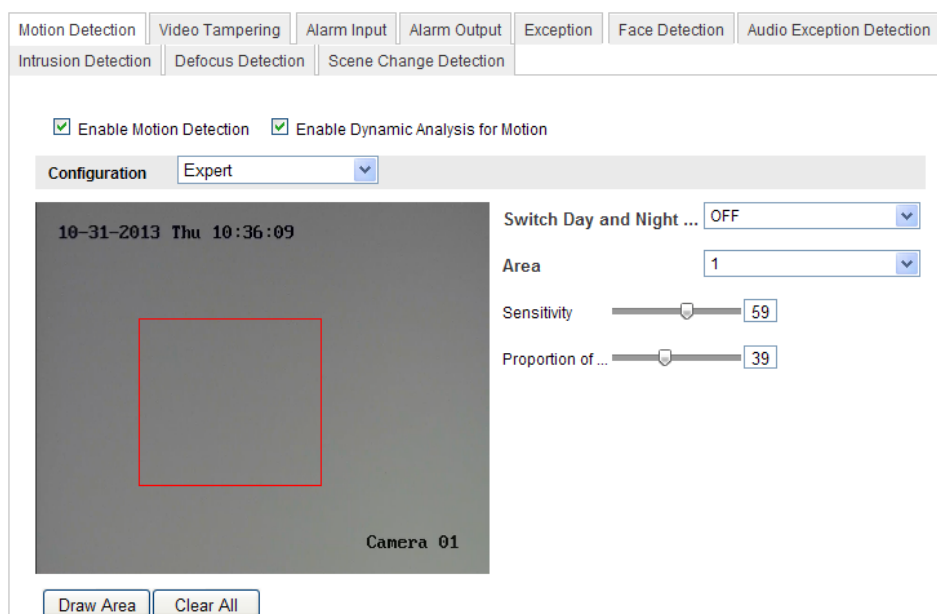


Figure 5-48 Tryb zaawansowany wykrywania ruchu

- Wyłączanie przełączania Dzień/Noc

Kroki:

(1) Narysuj obszar wykrywania jak w normalnym trybie konfiguracji.

Obsługiwanych jest maks. 8 obszarów.

(2) Wybierz **OFF** (Wył.) dla **Switch Day and Night Settings** (Ustawienia przełączania Dzień/Noc).

- (3)Wybierz obszar, klikając jego numer.
- (4)Przesuń kursor, aby dopasować czułość i proporcje obiektu na obszarze dla wybranego obszaru.
- (5)Ustaw harmonogram uzbrajania i powiązaną metodę jak w normalnym trybie konfiguracji.
- (6)Kliknij **Save (Zapisz)**, aby zapisać ustawienia.

● Autoprzełączanie Dzień/Noc

Kroki:

- (1)Narysuj obszar wykrywania jak w normalnym trybie konfiguracji.
Obsługiwanych jest maks. 8 obszarów.
- (2)Wybierz **Auto-Switch** (Autoprzełączanie) jako **Switch Day and Night Settings** (Ustawienia przełączania Dzień/Noc).

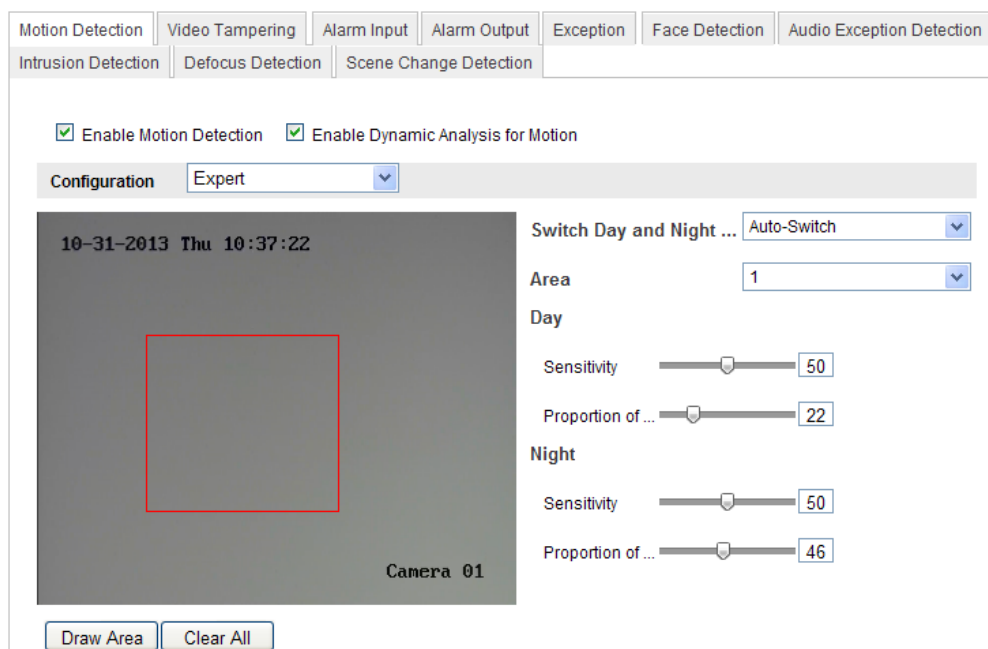


Figure 5-49 Autoprzełączanie Dzień/Noc

- (3)Wybierz obszar, klikając jego numer.
- (4)Przesuń kursor, aby dopasować czułość i proporcje obiektu na obszarze dla wybranego obszaru w dzień.
- (5)Przesuń kursor, aby dopasować czułość i proporcje obiektu na obszarze dla wybranego obszaru w nocy.

(6)Ustaw harmonogram uzbrajania i powiązaną metodę jak w normalnym trybie konfiguracji.

(7)Kliknij **Save** (Zapisz), aby zapisać ustawienia.

- Zaplanowane przełączanie Dzień/Noc

(1)Narysuj obszar wykrywania jak w normalnym trybie konfiguracji.

Obsługiwanych jest maks. 8 obszarów.

(2)Wybierz **Scheduled-Switch** (Zaplanowane przełączanie) dla **Switch Day and Night Settings** (Ustawienia przełączania Dzień/Noc).

Switch Day and Night ...	Scheduled- Switch
Start Time	06:00:00
End Time	18:00:00

Figure 5-50 Zaplanowane przełączanie Dzień/Noc

(3)Wybierz czas rozpoczęcia i czas zakończenia zaplanowanego przełączania.

(4)Wybierz obszar, klikając jego numer.

(5)Przesuń kursor, aby dopasować czułość i proporcje obiektu na obszarze dla wybranego obszaru w dzień.

(6)Przesuń kursor, aby dopasować czułość i proporcje obiektu na obszarze dla wybranego obszaru w nocy.

(7)Ustaw harmonogram uzbrajania i powiązaną metodę jak w normalnym trybie konfiguracji.

(8)Kliknij **Save** (Zapisz), aby zapisać ustawienia.

5.6.2 Konfiguracja alarmu o próbie manipulacji wideo

Cel:

Można skonfigurować kamerę tak, aby wyzwaliała alarm po zakryciu obiektywu, a także podejmowała inne działania alarmowe w reakcji na manipulację.

Kroki:

1. Przejdź do interfejsu ustawień manipulacji wideo:

Configuration > Advanced Configuration > Basic Event > Video Tampering
(**Konfiguracja > Konfiguracja zaawansowana > Zdarzenie podstawowe > Manipulacja wideo**)

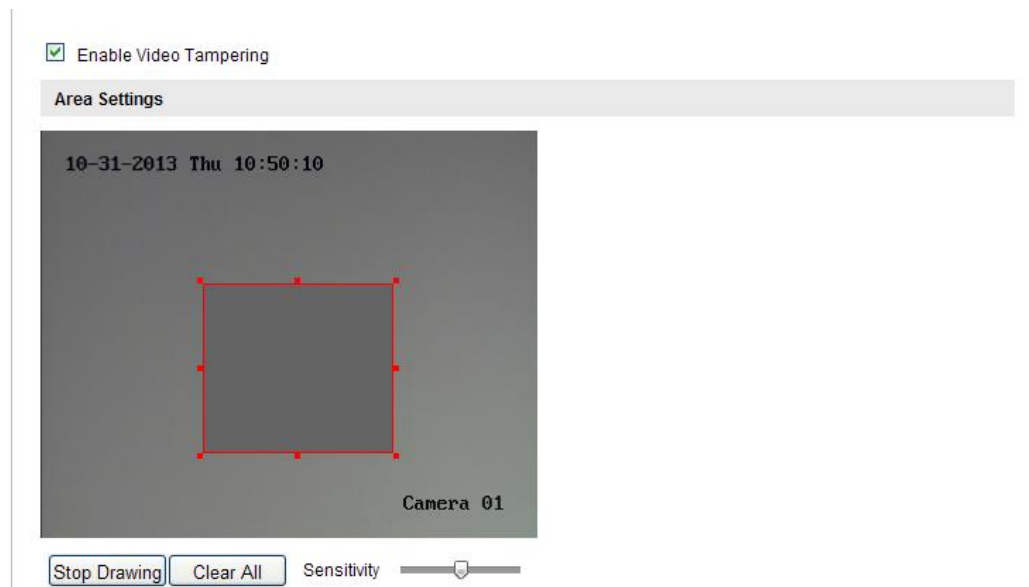


Figure 5-51 Alarm o próbie manipulacji wideo

2. Zaznacz pole wyboru **Enable Video Tampering** (Włącz manipulację wideo), aby włączyć wykrywanie manipulacji wideo.
3. Ustaw obszar wykrywania manipulacji wideo. Zapoznaj się z *Zadaniem 1 Ustaw obszar wykrywania ruchu* w *Sekcji 6.6.1*.
4. Kliknij **Edit** (Edycja), aby edytować harmonogram uzbrajania dla manipulacji wideo. Konfiguracja alarmu uzbrajania jest taka sama jak ustawianie harmonogramu uzbrajania dla wykrywania ruchu. Zapoznaj się z *Zadaniem 2 Ustaw harmonogram uzbrajania dla wykrywania ruchu* w *Sekcji 6.6.1*.
5. Zaznacz pole wyboru, aby wybrać powiązaną metodę podjętą w razie manipulacji wideo. Do wyboru są: Audible Warning (Ostrzeżenie dźwiękowe), Notify Surveillance Center (Powiadom centrum monitoringu), Send Email (Wyślij e-mail) i Trigger Alarm Output (Wyzwól wyście alarmowe). Zapoznaj się z *Zadaniem 3 Ustaw działania alarmu dla wykrywania ruchu* w *Sekcji 6.6.1*.
6. Kliknij **Save** (Zapisz), aby zapisać ustawienia.

5.6.3 Konfiguracja wejścia alarmowego

Kroki:

- Przejdź do interfejsu ustawień wejścia alarmowego:
Configuration > Advanced Configuration > Basic Event > Alarm Input
(Konfiguracja > Konfiguracja zaawansowana > Zdarzenie podstawowe > Wejście alarmowe)
- Wybierz nr wejścia alarmowego i typ alarmu. Dostępne typy alarmu: NO (Normally Open – normalnie otwarty) i NC (Normally Closed – normalnie zamknięty). Wyedytuj nazwę wejścia alarmowego (opcja).

The screenshot displays the configuration page for an alarm input. At the top, there are three main fields: 'Alarm Input No.' with a dropdown menu showing 'A<-1', 'Alarm Name' with a text input field and '(cannot copy)' to its right, and 'Alarm Type' with a dropdown menu showing 'NO'. Below these fields is a section titled 'Arming Schedule' with an 'Edit' button. The schedule is represented by a grid with 24 columns (hours) and 7 rows (days of the week: Mon, Tue, Wed, Thu, Fri, Sat, Sun). The grid cells are currently all blue, indicating that the alarm is armed 24/7.

Figure 5-52 Ustawienia wejścia alarmowego

- Kliknij **Edit** (Edytuj), aby ustawić harmonogram uzbrajania dla wejścia alarmowego. Zapoznaj się z *Zadaniem 2 Ustaw harmonogram uzbrajania dla wykrywania ruchu* w *Sekcji 6.6.1*.
- Zaznacz pole wyboru, aby wybrać powiązaną metodę podjętą dla wejścia alarmowego. Zapoznaj się z *Zadaniem 3 Ustaw działania alarmu dla wykrywania ruchu* w *Sekcji 6.6.1*.
- Możesz też wybrać powiązanie PTZ dla wejścia alarmowego, jeśli kamera jest wyposażona w moduł obrotu/pochylenia. Zaznacz odpowiednie pole wyboru i

wybierz numer, aby włączyć opcje Preset Calling (Wywoływanie ustawienia wstępne), Patrol Calling (Wywoływanie patrolu) lub Pattern Calling (Wywoływanie trasy).

6. Możesz skopiować ustawienia do innych wejść alarmowych.
7. Kliknij **Save** (Zapisz), aby zapisać ustawienia.

5.6.4 Konfiguracja wyjścia alarmowego

Kroki:

1. Przejdź do interfejsu ustawień wyjścia alarmowego:
Configuration>Advanced Configuration> Basic Event > Alarm Output
(Konfiguracja > Konfiguracja zaawansowana > Zdarzenie podstawowe > Wyjście alarmowe)
2. Wybierz jeden kanał wyjścia alarmowego na liście rozwijanej **Alarm Output** (Wyjście alarmowe). Możesz ustawić nazwę wyjścia alarmowego (opcja).
3. Dostępny czas opóźnienia: 5 s, 10 s, 30 s, 1 min, 2 min, 5 min, 10 min lub Manual (Ręczne). Czas opóźnienia odnosi się do czasu działania wyjścia alarmowego po wystąpieniu alarmu.
4. Kliknij **Edit** (Edytuj), aby przejść do interfejsu edycji czasu harmonogramu. Konfiguracja czasu harmonogramu jest taka sama jak ustawienia harmonogramu uzbrajania dla wykrywania ruchu. Zapoznaj się z *Zadaniem 2 Ustaw harmonogram uzbrajania dla wykrywania ruchu* w *Sekcji 6.6.1*.
5. Możesz skopiować ustawienia do innych wyjść alarmowych.
6. Kliknij **Save** (Zapisz), aby zapisać ustawienia.

Alarm Output: A->1

Alarm Name: (cannot copy)

Delay: Manual

Arming Schedule

Edit

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

Figure 5-53 Ustawienia wyjścia alarmowego

5.6.5 Obsługa wyjątków

Możliwe typy wyjątków: HDD Full (Dysk twardy zapelniony), HDD Error (Błąd dysku twardego), Network disconnected (Sieć rozłączona), IP address conflicted (Konflikt adresów IP), Illegal login to the cameras (Nieuprawnione logowanie do kamer).

Kroki:

1. Przejdź do interfejsu ustawień wyjątków:

Configuration > Advanced Configuration > Basic Event > Exception
(Konfiguracja > Konfiguracja zaawansowana > Zdarzenie podstawowe > Wyjątek)

2. Zaznacz pole wyboru, aby ustawić działania podjęte dla alarmu wyjątku. Zapoznaj się z *Zadaniem 3 Ustaw działania alarmu dla wykrywania ruchu* w *Sekcji 6.6.1.*

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

Figure 5-54 Ustawienia wyjątku

3. Kliknij **Save** (Zapisz), aby zapisać ustawienia.

5.6.6 Konfiguracja innego alarmu

Uwaga: Niektóre kamery obsługują alarm bezprzewodowy, alarm czujki PIR (passive infrared sensor – pasywny czujnik podczerwieni) lub alarm awaryjny.

● Alarm bezprzewodowy

Cel:

Gdy z detektora, takiego jak bezprzewodowy styk drzwiowy, jest do kamery wysyłany bezprzewodowy sygnał alarmu, zostaje wyzwolony alarm bezprzewodowy, można wówczas zareagować szeregiem działań.

Kroki:

1. Przejdź do interfejsu ustawień alarmu bezprzewodowego:
Configuration > Advanced Configuration> Basic Event> Other Alarm
(Konfiguracja > Konfiguracja zaawansowana > Zdarzenie podstawowe > Inny alarm)
2. Wybierz numer alarmu bezprzewodowego.
 Obsługiwanych jest maks. 8 kanałów zewnętrznego wejścia alarmu bezprzewodowego.
3. Zaznacz pole wyboru **Enable Wireless Alarm** (Włącz alarm bezprzewodowy), aby włączyć tę funkcję.
4. Wpisz żadaną nazwę alarmu w polu tekstowym.
5. Zaznacz pole wyboru, aby wybrać powiązaną metodę podjętą dla alarmu

bezprzewodowego.

- Kliknij **Save** (Zapisz), aby zapisać ustawienia.
- Umieść zewnętrzne urządzenie bezprzewodowe obok kamery i przejdź do **Configuration > Advanced Configuration > System > Remote Control** (Konfiguracja > Konfiguracja zaawansowana > System > Zdalne sterowanie), aby uzbroić kamerę i przeanalizować alarm bezprzewodowy.

Figure 5-55 Konfiguracja ustawień alarmu bezprzewodowego

● Alarm PIR

Cel:

Alarm PIR (Passive Infrared – pasywna podczerwień) jest wyzwalany, gdy intruz wykona ruch w polu widzenia detektora. Czujnik wykrywa energię cieplną osoby lub zwierzęcia stałocieplnego, np. psa, kota itp.

Kroki:

- Przejdź do interfejsu ustawień alarmu PIR:
Configuration > Advanced Configuration > Basic Event > Other Alarm
(Konfiguracja > Konfiguracja zaawansowana > Zdarzenie podstawowe > Inny alarm)
- Zaznacz pole wyboru **Enable PIR Alarm** (Włącz alarm PIR), aby włączyć funkcję alarmu PIR.
- Wpisz żadaną nazwę alarmu w polu tekstowym.
- Zaznacz pole wyboru, aby wybrać powiązaną metodę podjętą dla alarmu PIR.
- Kliknij przycisk **Edit** (Edytuj), aby ustawić harmonogram uzbrajania.
- Kliknij **Save** (Zapisz), aby zapisać ustawienia.

7. Przejdź do **Configuration > Advanced Configuration > System > Remote Control** (Konfiguracja > Konfiguracja zaawansowana > System > Zdalne sterowanie), aby uzbroić kamerę.

PIR Alarm

Enable PIR Alarm

Alarm Name

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

Arming Schedule

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

Figure 5-56 Konfiguracja ustawień alarmu PIR

● Alarm awaryjny

Cel:

W sytuacji awaryjnej można nacisnąć przycisk awaryjny na pilocie, aby wyzwolić alarm awaryjny.

Uwaga: Alarm awaryjny wymaga posiadania pilota. Najpierw przejdź do **Configuration > Advanced Configuration > System > Remote Control** (Konfiguracja > Konfiguracja zaawansowana > System > Zdalne sterowanie), aby sprawdzić pilota.

Kroki:

1. Przejdź do interfejsu ustawień alarmu awaryjnego:

Configuration > Advanced Configuration > Basic Event > Other Alarm

(Konfiguracja > Konfiguracja zaawansowana > Zdarzenie podstawowe > Inny alarm)

- Zaznacz pole wyboru, aby wybrać powiązane metody podjęte dla alarmu awaryjnego.
- Kliknij **Save** (Zapisz), aby zapisać ustawienia.

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

Figure 5-57 Konfiguracja ustawień alarmu awaryjnego

5.6.7 Konfiguracja wykrywania wyjątku audio

Cel:

Funkcja wykrywania wyjątku audio wykrywa nietypowe dźwięki w monitorowanej scenie, takie jak nagły wzrost/spadek natężenia dźwięku. Wyzwolenie alarmu może spowodować podjęcie szeregu działań.

Uwaga: Funkcja wykrywania wyjątku audio zależy od modelu kamery.

Kroki:

- Przejdź do interfejsu ustawień wykrywania wyjątku audio:
Configuration > Advanced Configuration > Smart Event > Audio Exception Detection (Konfiguracja > Konfiguracja zaawansowana > Zdarzenie inteligentne > Wykrywanie wyjątku audio)
- Zaznacz pole wyboru **Audio Loss Exception** (Wyjątek utraty audio), aby włączyć funkcję wykrywania utraty audio.
- Zaznacz pole wyboru **Sudden Increase of Sound Intensity Detection** (Wykrywanie nagłego wzrostu natężenia dźwięku), aby wykrywać gwałtowny wzrost głośności dźwięku w monitorowanej scenie. Można ustawić czułość wykrywania i próg gwałtownego wzrostu głośności.

- Zaznacz pole wyboru **Sudden Decrease of Sound Intensity Detection** (Wykrywanie nagłego spadku natężenia dźwięku), aby wykrywać gwałtowny spadek głośności dźwięku w monitorowanej scenie. Można ustawić czułość wykrywania i próg gwałtownego spadku głośności.

Uwagi:

- Sensitivity (Czułość): Zakres [1-100], im niższa wartość, tym gwałtowniejsza zmiana wywoła wykrywanie.
 - Sound Intensity Threshold (Próg natężenia dźwięku): Zakres [1-100], może filtrować dźwięki otoczenia, im głośniejsze dźwięki otoczenia, tym wartość powinna być wyższa. Wartość można dostosować do rzeczywistego otoczenia.
- Można usłyszeć głośność dźwięku w czasie rzeczywistym.
 - Kliknij przycisk **Edit** (Edytuj), aby ustawić harmonogram uzbrajania.
 - Wybierz powiązane metody dla wyjątku audio, takie jak Notify Surveillance Center (Powiadom centrum monitoringu), Send Email (Wyślij e-mail), Upload to FTP (Wyślij do FTP), Trigger Channel for recording (Wyzwól kanał dla nagrywania) i Trigger Alarm Output (Wyzwól wyjście alarmowe).
 - Kliknij **Save** (Zapisz), aby zapisać ustawienia.

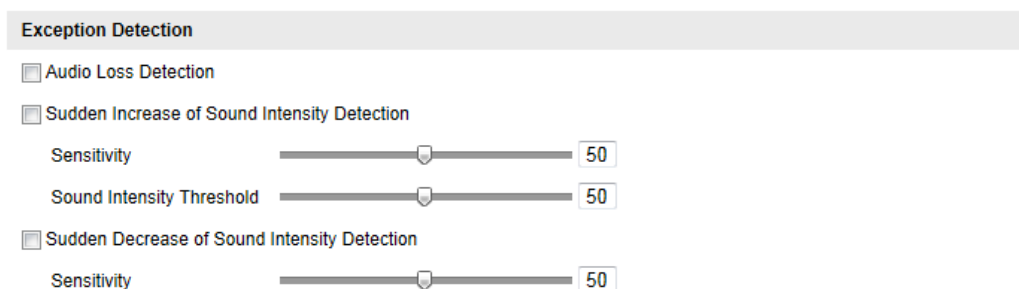


Figure 5-58 Konfiguracja wykrywania wyjątku audio

5.6.8 Konfiguracja wykrywania utraty ostrości

Cel:

Można wykrywać rozmycie obrazu spowodowane utratą ostrości przez obiektyw.

Wyzwolenie takiego alarmu może spowodować podjęcie określonych działań.

Uwaga: Funkcja wykrywania utraty ostrości zależy od modelu kamery.

Kroki:

1. Przejdź do interfejsu ustawień wykrywania utraty ostrości:
Configuration > Advanced Configuration > Smart Event > Defocus Detection
(Konfiguracja > Konfiguracja zaawansowana > Zdarzenie inteligentne > Wykrywanie utraty ostrości)
2. Zaznacz pole wyboru **Enable Defocus Detection** (Włącz wykrywanie utraty ostrości), aby włączyć tę funkcję.
3. Kliknij i przeciągnij suwak, aby ustawić czułość wykrywania. Zakres czułości wynosi od 1 do 100, im wyższa wartość, tym łatwiej rozmyty obraz wyzwoi alarm.
4. Wybierz powiązane metody dla utraty ostrości, takie jak Notify Surveillance Center (Powiadom centrum monitoringu), Send Email (Wyślij e-mail) i Trigger Alarm Output (Wyzwól wyjście alarmowe).
5. Kliknij **Save** (Zapisz), aby zapisać ustawienia.

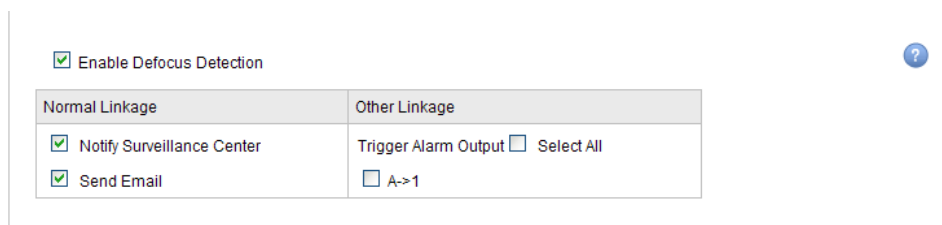


Figure 5-59 Konfiguracja wykrywania utraty ostrości

5.6.9 Konfiguracja wykrywania zmiany sceny

Cel:

Funkcja wykrywania zmiany sceny wykrywa zmianę monitorowanego otoczenia, spowodowaną przez czynniki zewnętrzne, takie jak celowe obrócenie kamery.

Wyzwolenie alarmu może spowodować podjęcie określonych działań.

Uwaga: Funkcja wykrywania zmiany sceny zależy od modelu kamery.

Kroki:

1. Przejdź do interfejsu ustawień wykrywania zmiany sceny:
Configuration > Advanced Configuration > Smart Event > Scene Change Detection (Konfiguracja > Konfiguracja zaawansowana > Zdarzenie inteligentne > Wykrywanie zmiany sceny)
2. Zaznacz pole wyboru **Enable Scene Change Detection** (Włącz wykrywanie zmiany sceny), aby włączyć tę funkcję.
3. Kliknij i przeciągnij suwak, aby ustawić czułość wykrywania. Zakres czułości wynosi od 1 do 100, im wyższa wartość, tym łatwiej zmiana sceny wywoła alarm.
4. Kliknij przycisk **Edit** (Edytuj), aby ustawić harmonogram uzbrajania.
5. Wybierz powiązane metody dla zmiany sceny, takie jak Notify Surveillance Center (Powiadom centrum monitoringu), Send Email (Wyślij e-mail), Upload to FTP (Wyślij do FTP), Trigger Channel (Kanał wyzwalany) i Trigger Alarm Output (Wyzwól wyjście alarmowe).
6. Kliknij **Save** (Zapisz), aby zapisać ustawienia.

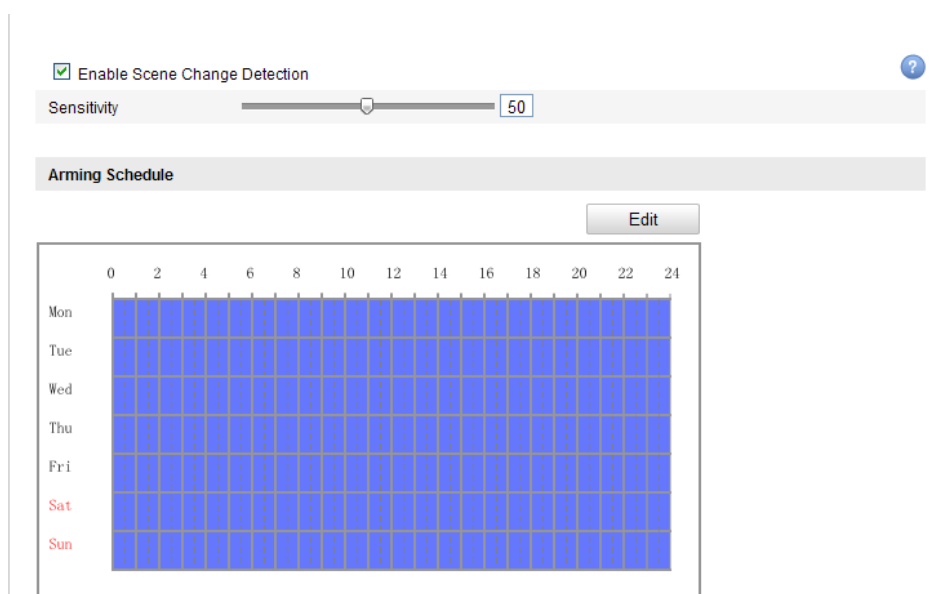


Figure 5-60 Konfiguracja wykrywania zmiany sceny

5.6.10 Konfiguracja wykrywania twarzy

Cel:

Funkcja wykrywania twarzy wykrywa, gdy w scenie monitoringu pojawia się twarz.

Wyzwolenie alarmu może spowodować podjęcie szeregu działań.

Uwaga: Funkcja wykrywania twarzy zależy od modelu kamery.

Kroki:

1. Przejdź do interfejsu ustawień wykrywania twarzy:
Configuration > Advanced Configuration > Smart Event > Face Detection
(Konfiguracja > Konfiguracja zaawansowana > Zdarzenie inteligentne > Wykrywanie twarzy)
2. Zaznacz pole wyboru **Enable Face Detection** (Włącz wykrywanie twarzy), aby włączyć tę funkcję.
3. (Opcja) Zaznacz pole wyboru **Enable Dynamic Analysis for Face Detection** (Włącz dynamiczną analizę wykrywania twarzy), wówczas wykryta twarz będzie na wideo na żywo oznaczona zielonym prostokątem.
Uwaga: Aby oznaczyć wykrytą twarz na wideo na żywo, przejdź do **Local Configuration > Live View Parameters** (Konfiguracja lokalna > Parametry widoku na żywo) i włącz **Rules** (Reguły).
4. Kliknij i przeciągnij suwak, aby ustawić czułość wykrywania.
Sensitivity (Czułość): Zakres [1-5]. Im wyższa wartość, tym łatwiej będzie wykrywana twarz.
5. Kliknij przycisk **Edit** (Edytuj), aby ustawić harmonogram uzbrajania.
6. Wybierz powiązane metody dla wykrywania twarzy, takie jak **Notify Surveillance Center** (Powiadom centrum monitoringu), **Send Email** (Wyślij e-mail), **Upload to FTP** (Wyślij do FTP), **Trigger Channel** (Kanał wyzwalany) i **Trigger Alarm Output** (Wyzwól wyjście alarmowe).
7. Kliknij **Save** (Zapisz), aby zapisać ustawienia.

Enable Face Detection
 Enable Dynamic Analysis for Face Detection
 Sensitivity 3

Arming Schedule

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

Linkage Method

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

Figure 5-61 Konfiguracja wykrywania twarzy

5.6.11 Konfiguracja wykrywania przekroczenia linii

Cel:

Funkcja wykrywania przekroczenia linii wykrywa ludzi, pojazdy i inne obiekty, które przekraczają wcześniej zdefiniowaną wirtualną linię. Wyzwolenie alarmu może spowodować podjęcie szeregu działań.

Uwaga: Funkcja wykrywania przekroczenia linii zależy od modelu kamery.

Kroki:

1. Przejdź do interfejsu ustawień wykrywania przekroczenia linii:

Configuration > Advanced Configuration > Smart Event > Line Crossing Detection (Konfiguracja > Konfiguracja zaawansowana > Zdarzenie inteligentne > Wykrywanie przekroczenia linii)

2. Zaznacz pole wyboru **Enable Line Crossing Detection** (Włącz wykrywanie przekroczenia linii), aby włączyć tę funkcję.
3. Wybierz linię z listy rozwijanej ustawień wykrywania.
4. Kliknij przycisk **Draw Area** (Narysuj obszar), na wideo na żywo wyświetli się wirtualna linia.
5. Kliknij i przeciągnij linię dożądanego położenia na wideo na żywo. Kliknij linię, na każdym końcu wyświetli się czerwony kwadrat. Kliknij i przeciągnij jeden z czerwonych kwadratów, aby zdefiniować kształt i długość linii.
6. Wybierz kierunek dla wykrywania przekroczenia linii. Można wybrać kierunki **A<->B**, **A->B** oraz **B->A**.
A<->B: Wyświetla się tylko strzałka po stronie B, gdy obiekt przechodzący przez płaszczyznę w obu kierunkach może zostać wykryty i zostanie wyzwolony alarm.
A->B: Wykrywany jest tylko obiekt przechodzący przez skonfigurowaną linię ze strony A na stronę B.
B->A: Wykrywany jest tylko obiekt przechodzący przez skonfigurowaną linię ze strony B na stronę A.
7. Kliknij i przeciągnij suwak, aby ustawić czułość wykrywania.
Sensitivity (Czułość): Zakres [1-100]. Im wyższa wartość, tym łatwiej będzie wykrywane przekroczenie linii.
8. Powtórz powyższe kroki, aby skonfigurować inne linie. Można ustawić maks. 4 linie. Możesz kliknąć przycisk **Clear** (Usuń), aby usunąć wszystkie zdefiniowane linie.
9. Kliknij przycisk **Edit** (Edytuj), aby ustawić harmonogram uzbrajania.
10. Wybierz powiązane metody dla wykrywania przekroczenia linii, takie jak Notify Surveillance Center (Powiadom centrum monitoringu), Send Email (Wyślij e-mail), Upload to FTP (Wyślij do FTP), Trigger Channel (Kanał wyzwalany) i Trigger Alarm Output (Wyzwól wyjście alarmowe).
11. Kliknij **Save** (Zapisz), aby zapisać ustawienia.

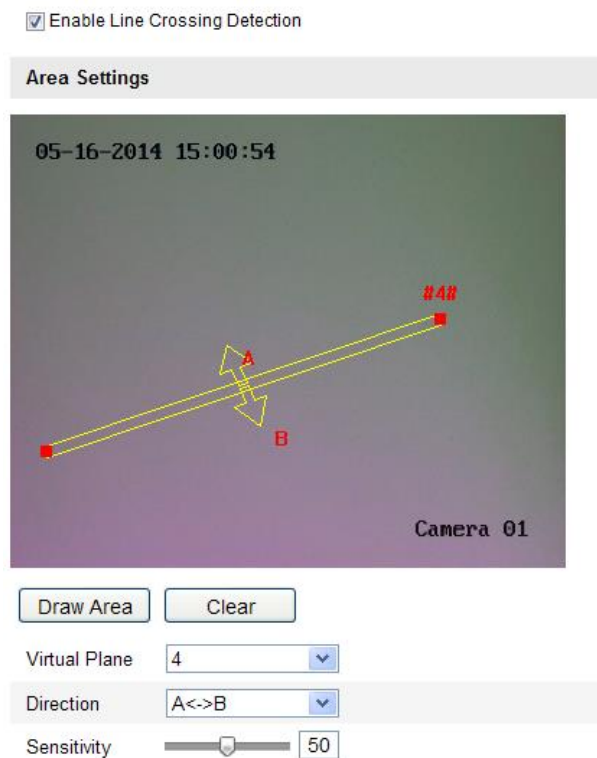


Figure 5-62 Rysowanie linii przekraczania

5.6.12 Konfiguracja wykrywania wtargnięcia

Cel:

Funkcja wykrywania wtargnięcia wykrywa ludzi, pojazdy i inne obiekty, które znalazły się we wcześniej zdefiniowanym obszarze wirtualnym i tam przebywają. Wyzwolenie alarmu może spowodować podjęcie szeregu działań.

Uwaga: Funkcja wykrywania wtargnięcia zależy od modelu kamery.

Kroki:

1. Przejdź do interfejsu ustawień wykrywania wtargnięcia:
Configuration > Advanced Configuration > Smart Event > Intrusion Detection
(Konfiguracja > Konfiguracja zaawansowana > Zdarzenie inteligentne > Wykrywanie wtargnięcia)
2. Zaznacz pole wyboru **Enable Intrusion Detection** (Włącz wykrywanie wtargnięcia), aby włączyć tę funkcję.
3. Wybierz obszar z listy rozwijanej ustawień wykrywania.

4. Kliknij przycisk **Draw Area** (Narysuj obszar), aby rozpocząć rysowanie obszaru.
5. Kliknij w wideo na żywo, aby określić cztery wierzchołki obszaru wykrywania, kliknij prawym przyciskiem, aby zakończyć rysowanie.
6. Ustaw próg czasowy, czułość wykrywania i procent zapełnienia przez obiekt dla wykrywania wtargnięcia.

Threshold (Próg): Zakres [0 s-10 s], próg czasu przebywania obiektu w obszarze. Jeśli ustawisz wartość na 0, alarm zostanie wyzwolony natychmiast, gdy obiekt znajdzie się w obszarze.

Sensitivity (Czułość): Zakres [1-100]. Wartość czułości określa rozmiar obiektu, który może wyzwolić alarm. Wysoka czułość oznacza, że alarm może być wyzwolony przez bardzo mały obiekt.

Percentage (Procent): Zakres [1-100]. Procent oznacza stosunek wielkości części obiektu przebywającej w obszarze, która może wyzwolić alarm. Na przykład, jeśli procent wynosi 50%, to gdy obiekt znajdzie się w obszarze i zajmuje 50% jego powierzchni, zostanie wyzwolony alarm.

7. Powtórz powyższe kroki, aby skonfigurować inne obszary. Można ustawić maks. 4 obszary. Możesz kliknąć przycisk **Clear** (Usuń), aby usunąć wszystkie zdefiniowane obszary.
8. Kliknij przycisk **Edit** (Edytuj), aby ustawić harmonogram uzbrajania.
9. Wybierz powiązane metody dla wykrywania wtargnięcia, takie jak Notify Surveillance Center (Powiadom centrum monitoringu), Send Email (Wyślij e-mail), Upload to FTP (Wyślij do FTP), Trigger Channel (Kanał wyzwalany) i Trigger Alarm Output (Wyzwól wyjście alarmowe).
10. Kliknij **Save** (Zapisz), aby zapisać ustawienia.

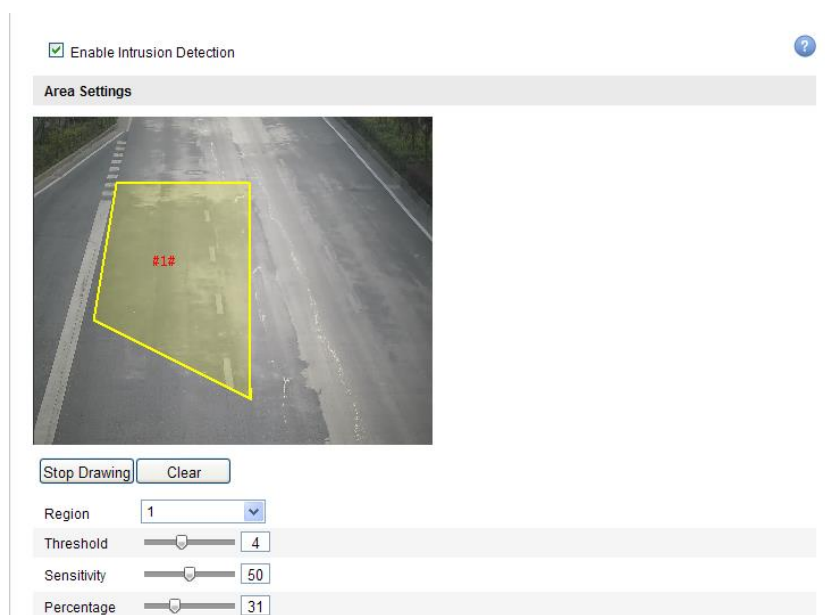


Figure 5-63 Konfiguracja obszaru wtargnięcia

5.6.13 Konfiguracja wykrywania wejścia w obszar

Cel:

Funkcja wykrywania wejścia w obszar wykrywa ludzi, pojazdy i inne obiekty, które wchodzi z zewnątrz do wcześniej zdefiniowanego obszaru. Wyzwolenie alarmu może spowodować podjęcie szeregu działań.

Uwaga: Funkcja wykrywania wejścia w obszar zależy od modelu kamery.

Kroki:

1. Przejdź do interfejsu ustawień wykrywania wejścia w obszar:
Configuration > Advanced Configuration > Smart Event > Region Entrance Detection (Konfiguracja > Konfiguracja zaawansowana > Zdarzenie inteligentne > Wykrywanie wejścia w obszar)
2. Zaznacz pole wyboru **Enable Region Entrance Detection** (Włącz wykrywanie wejścia w obszar), aby włączyć tę funkcję.
3. Wybierz obszar z listy rozwijanej ustawień wykrywania.
4. Kliknij przycisk **Draw Area** (Narysuj obszar), aby rozpocząć rysowanie obszaru.
5. Kliknij w wideo na żywo, aby określić cztery wierzchołki obszaru wykrywania, kliknij prawym przyciskiem, aby zakończyć rysowanie.

6. Kliknij i przeciągnij suwak, aby ustawić czułość wykrywania.
Sensitivity (Czułość): Zakres [1-100]. Wartość czułości określa rozmiar obiektu, który może wyzwolić alarm. Wysoka czułość oznacza, że alarm może być wyzwolony przez bardzo mały obiekt wchodzący w obszar.
7. Powtórz powyższe kroki, aby skonfigurować inne obszary. Można ustawić maks. 4 obszary. Możesz kliknąć przycisk Clear (Usuń), aby usunąć wszystkie zdefiniowane obszary.
8. Kliknij przycisk **Edit** (Edytuj), aby ustawić harmonogram uzbrajania.
9. Wybierz powiązane metody dla wykrywania wejścia w obszar, takie jak Notify Surveillance Center (Powiadom centrum monitoringu), Send Email (Wyślij e-mail), Upload to FTP (Wyślij do FTP), Trigger Channel (Kanał wyzwalany) i Trigger Alarm Output (Wyzwól wyjście alarmowe).
10. Kliknij **Save** (Zapisz), aby zapisać ustawienia.

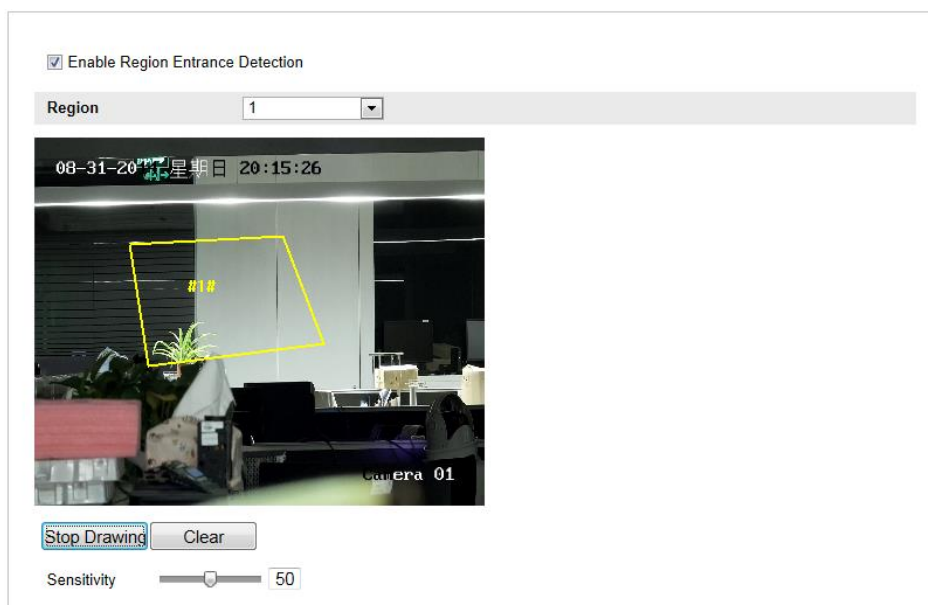


Figure 5-64 Konfiguracja wykrywania wejścia w obszar

5.6.14 Konfiguracja wykrywania wyjścia z obszaru

Cel:

Funkcja wykrywania wyjścia z obszaru wykrywa ludzi, pojazdy i inne obiekty, które opuszczają wcześniej zdefiniowany wirtualny obszar. Wyzwolenie alarmu może spowodować podjęcie szeregu działań.

Uwaga: Funkcja wykrywania wyjścia z obszaru zależy od modelu kamery.

Kroki:

1. Przejdź do interfejsu ustawień wykrywania wyjścia z obszaru:
Configuration > Advanced Configuration > Smart Event > Region Exiting Detection (Konfiguracja > Konfiguracja zaawansowana > Zdarzenie inteligentne > Wykrywanie wyjścia z obszaru)
2. Zaznacz pole wyboru **Enable Region Exiting Detection** (Włącz wykrywanie wyjścia z obszaru), aby włączyć tę funkcję.
3. Wybierz obszar z listy rozwijanej ustawień wykrywania.
4. Kliknij przycisk **Draw Area** (Narysuj obszar), aby rozpocząć rysowanie obszaru.
5. Kliknij w wideo na żywo, aby określić cztery wierzchołki obszaru wykrywania, kliknij prawym przyciskiem, aby zakończyć rysowanie.
6. Kliknij i przeciągnij suwak, aby ustawić czułość wykrywania.
Sensitivity (Czułość): Zakres [1-100]. Wartość czułości określa rozmiar obiektu, który może wyzwolić alarm. Wysoka czułość oznacza, że alarm może być wyzwolony przez bardzo mały obiekt opuszczający obszar.
7. Powtórz powyższe kroki, aby skonfigurować inne obszary. Można ustawić maks. 4 obszary. Możesz kliknąć przycisk **Clear** (Usuń), aby usunąć wszystkie zdefiniowane obszary.
8. Kliknij przycisk **Edytuj**, aby ustawić harmonogram uzbrajania.
9. Wybierz powiązane metody dla wykrywania wyjścia z obszaru, takie jak Notify Surveillance Center (Powiadom centrum monitoringu), Send Email (Wyślij e-mail), Upload to FTP (Wyślij do FTP), Trigger Channel (Kanał wyzwalań) i Trigger Alarm Output (Wyzwól wyjście alarmowe).
10. Kliknij **Save** (Zapisz), aby zapisać ustawienia.

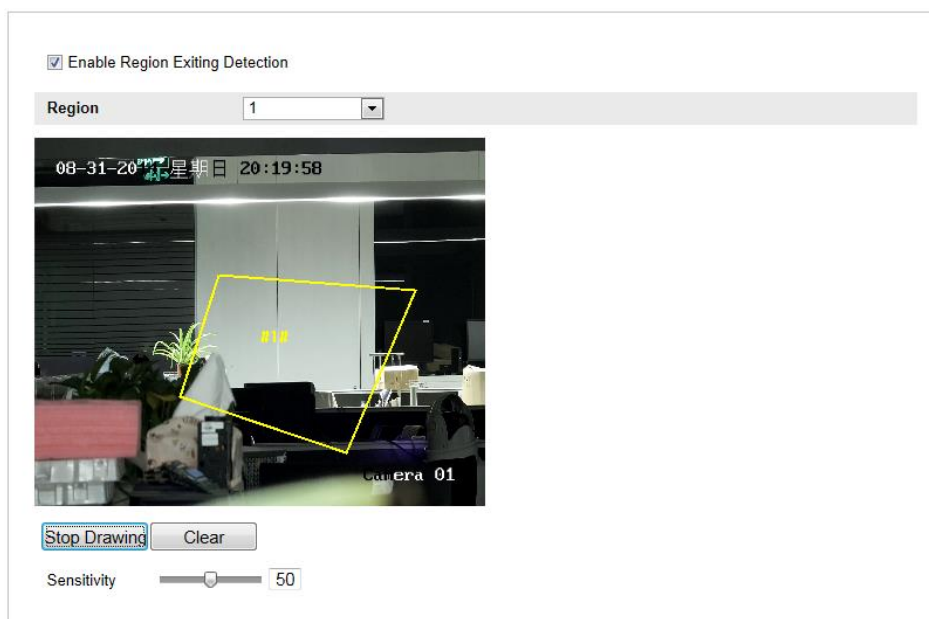


Figure 5-65 Konfiguracja wykrywania wyjścia z obszaru

5.6.15 Konfiguracja wykrywania bagażu bez nadzoru

Cel:

Funkcja wykrywania bagażu bez nadzoru wykrywa obiekty pozostawione w zdefiniowanym obszarze, takie jak bagaż, portmonetki, niebezpieczne materiały itp. Wyzwolenie alarmu może spowodować podjęcie szeregu działań.

Uwaga: Funkcja wykrywania bagażu bez nadzoru zależy od modelu kamery.

Kroki:

1. Przejdź do interfejsu ustawień wykrywania bagażu bez nadzoru:
Configuration > Advanced Configuration > Smart Event > Unattended Baggage Detection (Konfiguracja > Konfiguracja zaawansowana > Zdarzenie inteligentne > Wykrywanie bagażu bez nadzoru)
2. Zaznacz pole wyboru **Enable Unattended Baggage Detection** (Włącz wykrywanie bagażu bez nadzoru), aby włączyć tę funkcję.
3. Wybierz obszar z listy rozwijanej ustawień wykrywania.
4. Kliknij przycisk **Draw Area** (Narysuj obszar), aby rozpocząć rysowanie obszaru.
5. Kliknij w wideo na żywo, aby określić cztery wierzchołki obszaru wykrywania, kliknij prawym przyciskiem, aby zakończyć rysowanie.

6. Ustaw próg czasowy i czułość wykrywania bagażu bez nadzoru.
Threshold (Próg): Zakres [5 s-20 s], próg czasu pozostawienia obiektu bez nadzoru w obszarze. Po ustawieniu wartości na 10 alarm zostanie wywołony, gdy obiekt zostanie pozostawiony w obszarze na 10 s.
Sensitivity (Czułość): Zakres [1-100]. Wartość czułości oznacza stopień podobieństwa obrazu tła. Zwykle wysoka czułość oznacza, że alarm może być wywołony przez bardzo mały obiekt pozostawiony w obszarze.
7. Powtórz powyższe kroki, aby skonfigurować inne obszary. Można ustawić maks. 4 obszary. Możesz kliknąć przycisk **Clear** (Usuń), aby usunąć wszystkie zdefiniowane obszary.
8. Kliknij przycisk **Edit** (Edytuj), aby ustawić harmonogram uzbrajania.
9. Wybierz powiązane metody dla wykrywania bagażu bez nadzoru, takie jak Notify Surveillance Center (Powiadom centrum monitoring), Send Email (Wyślij e-mail), Upload to FTP (Wyślij do FTP), Trigger Channel (Kanał wyzwalany) i Trigger Alarm Output (Wyzwól wyjście alarmowe).
10. Kliknij **Save** (Zapisz), aby zapisać ustawienia.

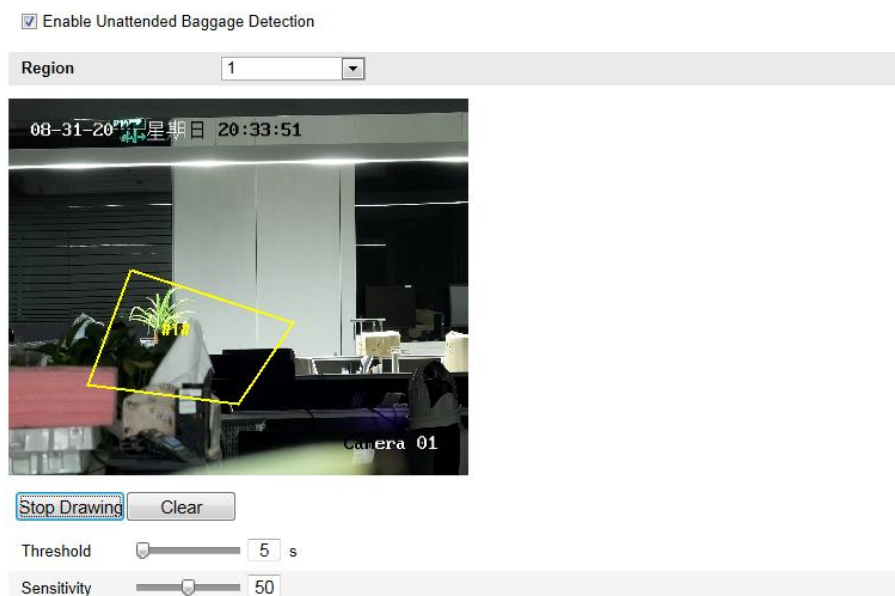


Figure 5-66 Konfiguracja bagażu bez nadzoru

5.6.16 Konfiguracja wykrywania usunięcia obiektów

Cel:

Funkcja wykrywania usunięcia obiektów wykrywa obiekty usunięte ze zdefiniowanego obszaru, np. reklamy. Wyzwolenie alarmu może spowodować podjęcie szeregu działań.

Uwaga: Funkcja wykrywania usunięcia obiektów zależy od modelu kamery.

Kroki:

1. Przejdź do interfejsu ustawień wykrywania usunięcia obiektów:
Configuration > Advanced Configuration > Smart Event > Object Removal Detection (Konfiguracja > Konfiguracja zaawansowana > Zdarzenie inteligentne > Wykrywanie usunięcia obiektów)
2. Zaznacz pole wyboru **Enable Object Removal Detection** (Włącz wykrywanie usunięcia obiektów), aby włączyć tę funkcję.
3. Wybierz obszar z listy rozwijanej ustawień wykrywania.
4. Kliknij przycisk **Draw Area** (Narysuj obszar), aby rozpocząć rysowanie obszaru.
5. Kliknij w wideo na żywo, aby określić cztery wierzchołki obszaru wykrywania, kliknij prawym przyciskiem, aby zakończyć rysowanie.
6. Ustaw próg czasowy i czułość wykrywania usunięcia obiektów.
Threshold (Próg): Zakres [5 s-20 s], próg czasu usunięcia obiektu z obszaru. Po ustawieniu wartości na 10 alarm zostanie wyzwolony, gdy obiekt zniknie z obszaru na 10 s.
Sensitivity (Czułość): Zakres [1-100]. Wartość czułości oznacza stopień podobieństwa obrazu tła. Zwykle wysoka czułość oznacza, że alarm może być wyzwolony przez bardzo mały obiekt usunięty z obszaru.
7. Powtórz powyższe kroki, aby skonfigurować inne obszary. Można ustawić maks. 4 obszary. Możesz kliknąć przycisk **Clear** (Usuń), aby usunąć wszystkie zdefiniowane obszary.
8. Kliknij przycisk **Edit** (Edytuj), aby ustawić harmonogram uzbrajania.
9. Wybierz powiązane metody dla wykrywania usunięcia obiektów, takie jak Notify

Surveillance Center (Powiadom centrum monitoringu), Send Email (Wyślij e-mail), Upload to FTP (Wyślij do FTP), Trigger Channel (Kanał wyzwalany) i Trigger Alarm Output (Wyzwól wyjście alarmowe).

10. Kliknij **Save** (Zapisz), aby zapisać ustawienia.



Figure 5-67 Konfiguracja wykrywania usunięcia obiektów

5.7 Konfiguracja VCA

5.7.1 Analiza zachowań

Analiza zachowań wykrywa serię podejrzanych zachowań. Wyzwolenie alarmu spowoduje włączenie pewnych powiązanych metod.

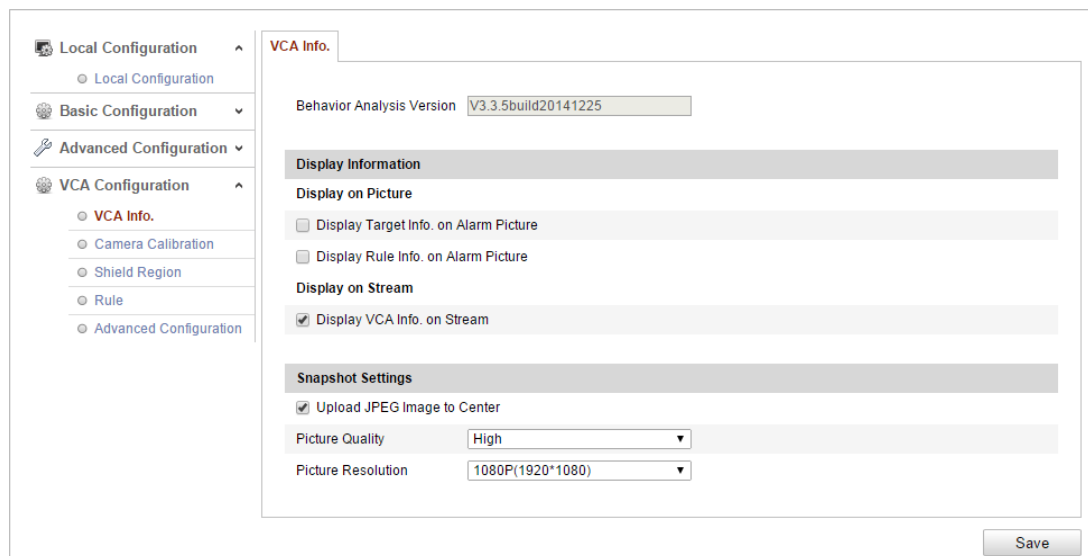


Figure 5-68 Analiza zachowań

❖ Informacje VCA

Wersja analizy zachowań: Wyświetla wersję biblioteki algorytmów.

Wyświetlane informacje obejmują wyświetlanie na zdjęciu i na strumieniu.

Display Target info. on Alarm Picture (Wyświetlanie informacji o celu na zdjęciu alarmu): Zaznaczenie tego pola wyboru spowoduje, że na wgranym zdjęciu alarmu cel zostanie oznaczony ramką.

Display Rule info. on Alarm Picture (Wyświetlanie informacji o regule na zdjęciu alarmu): Na zdjęciu alarmu przechwycony cel i skonfigurowany obszar będą otoczone ramką.

Display VCA info. on Stream (Wyświetlanie informacji VCA na strumieniu): W podglądzie na żywo lub podczas odtwarzania cel będzie oznaczony zieloną ramką.

Uwaga: Upewnij się, że reguły są włączone w ustawieniach lokalnych. Przejdź do **Configuration > Local Configuration > Rules** (Konfiguracja > Konfiguracja lokalna > Reguły), aby je włączyć.

Ustawienia zrzutu ekranu: Można ustawić jakość i rozdzielczość zrobionego zdjęcia.

Upload JPEG Image to Center (Wyślij zdjęcie JPEG do centrum): Zaznacz to pole wyboru, aby wysłać zrobione zdjęcie do centrum monitoringu, gdy wystąpi alarm VCA.

Picture Quality (Jakość obrazu): Do wyboru są High (Wysoka), Medium (Średnia) i Low (Niska).

Picture Resolution (Rozdzielczość obrazu): Do wyboru są CIF, 4CIF, 720P i 1080P.

❖ **Camera Calibration (Kalibracja kamery)**

Wykonaj następujące kroki, aby zmierzyć i wykonać próbkowanie obrazu z kamery w trzech wymiarach, a następnie obliczyć rozmiar każdego celu. Konfiguracja kalibracji kamery pozwoli uzyskać dokładniejsze wykrywanie VCA.

Kroki:

1. Zaznacz pole wyboru **Camera Calibration (Kalibracja kamery)**, aby włączyć tę funkcję.
2. Wybierz tryb kalibracji: **Input Basic Data (Wprowadź dane podstawowe)** lub **Draw on Live View Video (Rysuj na wideo na żywo)**.

Input Basic Data (Wprowadź dane podstawowe): Ręcznie wprowadź wysokość montażu, kąt widzenia i współczynnik horyzontu kamery.

Draw on Live View Video (Rysuj na wideo na żywo): Kliknij **Draw Verification Line (Horizontal) / (Vertical)** (Narysuj linię weryfikacyjną (poziomą) / (pionową)), aby na podglądzie na żywo narysować linię poziomą/pionową i wprowadzić rzeczywistą długość w polu **Real Length (Rzeczywista długość)**. Dzięki narysowaniu linii referencyjnych i podaniu ich rzeczywistej długości kamera może określić, kiedy w polu widzenia pojawiają się inne obiekty.

3. (Opcja) Zaznacz pole wyboru **Enable Verification of Camera Calibration (Włącz weryfikację kalibracji kamery)**, kliknij przycisk **Horizontal Verify / Vertical Verify (Weryfikacja pozioma/Weryfikacja pionowa)**, aby narysować na wideo na żywo poziomą/pionową linię, a następnie kliknij przycisk **Calibrate (Kalibruj)**, aby obliczyć długość linii. Porównaj obliczoną długość linii z długością rzeczywistą, aby sprawdzić ustawione informacje o kalibracji.
4. Możesz kliknąć **Delete (Usuń)**, aby usunąć narysowane linie.
5. Kliknij **Save (Zapisz)**, aby zapisać ustawienia.

Uwaga: Jeśli widok na żywo zostanie zatrzymany, kalibracja kamery będzie nieprawidłowa.

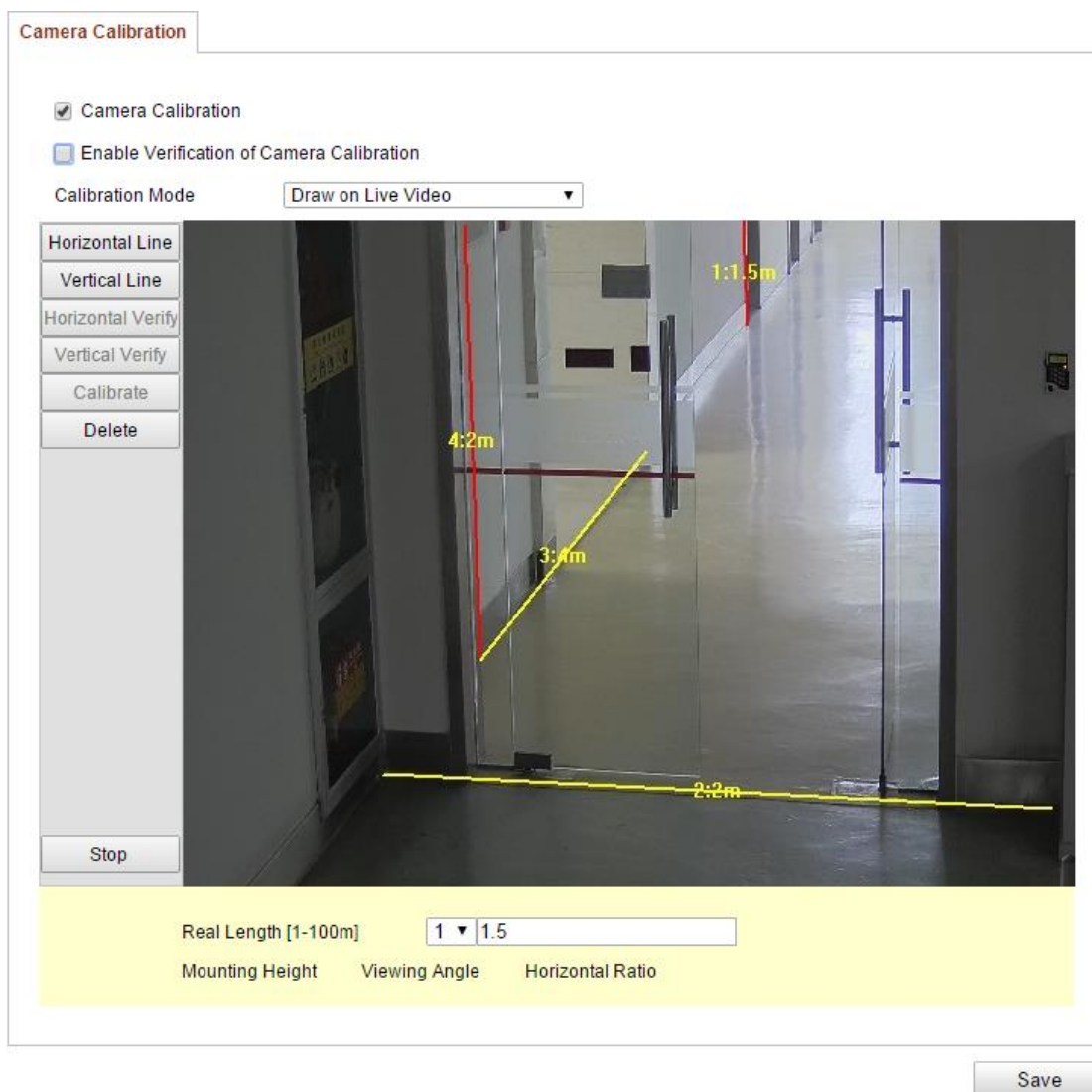


Figure 5-69 Rysowanie w oknie podglądu na żywo

❖ Shield Region (Strefa bez wykrywania)

Strefa bez wykrywania pozwala ustawić specjalną strefę, w której analiza zachowań nie będzie przeprowadzana. Obsługiwane są maks. 4 strefy bez wykrywania.

Kroki:

1. Kliknij zakładkę **Shield Region** (Strefa bez wykrywania), aby otworzyć interfejs konfiguracji strefy bez wykrywania.
2. Kliknij **Draw Area** (Narysuj obszar). Narysuj obszar, klikając lewym przyciskiem punkty końcowe w oknie podglądu na żywo, kliknij prawym przyciskiem, aby zakończyć rysowanie obszaru.

Uwagi:

- Obsługiwane są wielokąty z maks. 10 bokami.

- Kliknij **Delete** (Usuń), aby usunąć narysowane obszary.
 - Jeśli podgląd na żywo zostanie zatrzymany, nie można narysować stref bez wykrywania.
3. Kliknij **Save** (Zapisz), aby zapisać ustawienia.

❖ **Rule (Reguła)**

Analiza zachowania obsługuje szereg zachowań, takich jak wykrywanie przekroczenia linii, wtargnięcia, wejścia w obszar, wyjścia z obszaru itp.

Uwaga: Szczegółowe informacje o każdym zachowaniu znajdują się w odpowiednim rozdziale.

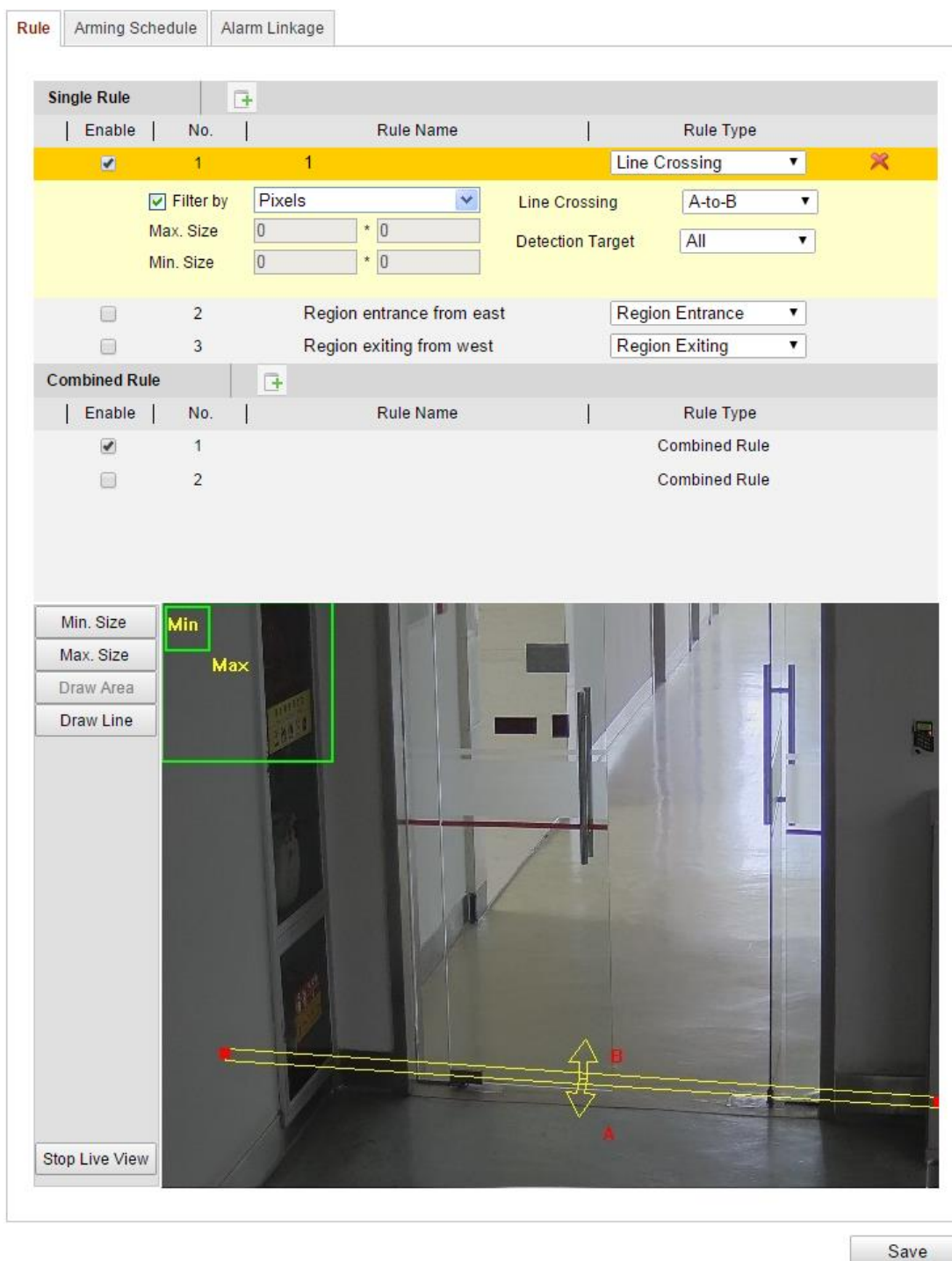


Figure 5-70 Konfiguracja reguły

Kroki:

1. Kliknij zakładkę **Rule** (Reguła), aby otworzyć interfejs konfiguracji reguły.
2. Zaznacz pole wyboru pojedynczej reguły, aby włączyć jej stosowanie w analizie zachowania.
3. Wybierz typ reguły, ustaw typ filtra, a następnie narysuj linię/obszar na wideo na żywo dla pojedynczej reguły.

Filter Type (Typ filtru): Do wyboru są Pixels (Piksele) i Actual Size (Rzeczywisty rozmiar). Po wybraniu Pikseli narysuj na wideo na żywo obszar o maksymalnym rozmiarze i minimalnym rozmiarze dla każdej reguły. Po wybraniu Rzeczywistego rozmiaru wpisz długość i szerokość maksymalnego i minimalnego rozmiaru. Alarm zostanie wyzwolony tylko przez cel o rozmiarze zawierającym się między wartością minimalną i maksymalną.

Uwaga: W przypadku Rzeczywistego rozmiaru upewnij się, że skonfigurowano kalibrację kamery.

Detection Target (Cel wykrywania): Jako cel wykrywania wybierz Human (Człowiek) lub Vehicle (Pojazd). Możesz też wybrać All (Wszystko), aby jako cele wykrywać wszystkie obiekty.

Draw line / area: (Narysuj linię/obszar): W przypadku wykrywania przekroczenia linii, narysuj linię i wybierz kierunek przekraczania: dwukierunkowy, $A > B$ lub $B > A$. W przypadku innych zdarzeń, takich jak wejście w obszar, wyjście z obszaru itp., kliknij lewym przyciskiem na wideo na żywo, aby ustawić punkty końcowe obszaru, kliknij prawym przyciskiem, aby zakończyć rysowanie obszaru.

Uwaga: Po zatrzymaniu podglądu na żywo nie można narysować obszaru/linii wykrywania i nie można ustawić reguł.

4. Zaznacz pole wyboru połączonej reguły, aby włączyć jej stosowanie w analizie zachowania.
5. Wybierz dwie skonfigurowane pojedyncze reguły jako Regułę A i Regułę B połączonej reguły, ustaw minimalny i maksymalny odstęp czasowy między obiema pojedynczymi regułami, a następnie wybierz kolejność wyzwalania pojedynczych reguł dla filtrowania alarmu.

Uwagi:

- W przypadku wybrania typu reguły None (Brak) opcja reguły nie działa i nie można skonfigurować analizy zachowania.
- Kolejność wyzwalania pojedynczych reguł dla filtrowania alarmu można ustawić na In Ascending Order (Rosnąco) lub In Ascending/Descending Order (Rosnąco/Malejąco).
- Można skonfigurować maks. 8 pojedynczych reguł i 2 połączone reguły. W przypadku połączonych reguł obsługiwane są: przekraczanie linii, wtargnięcie, wyjście z obszaru i wejście w obszar.

6. Kliknij **Save** (Zapisz), aby zapisać ustawienia.
7. Kliknij zakładkę **Arming Schedule** (Harmonogram uzbrajania), kliknij **Edit** (Edytuj), aby ustawić zaplanowany czas dla każdej reguły, a następnie kliknij **Save** (Zapisz), aby zapisać ustawienia.
8. Kliknij zakładkę **Alarm Linkage** (Powiązania alarmów), zaznacz pole wyboru odpowiedniej powiązanej metody dla każdej reguły, a następnie kliknij **Save** (Zapisz), aby zapisać ustawienia.

❖ **Advanced Configuration (Konfiguracja zaawansowana)**

- **Parameters (Parametry)**

Skonfiguruj następujące szczegółowe parametry.

Figure 5-71 Konfiguracja zaawansowana

Detection Sensitivity (Czułość rejestracji) [0~4]: Odnosi się do czułości, z jaką kamera wykrywa cel. Im wyższa wartość, tym łatwiej będzie rozpoznawany cel, ale wzrośnie również liczba fałszywych alarmów. Zaleca się pozostawienie wartości domyślnej 3.

Background Update Rate (Częstotliwość aktualizacji tła) [0~4]: Odnosi się do szybkości, z jaką nowa scena zastępuje poprzednią. Zaleca się pozostawienie wartości domyślnej 3.

Single Alarm (Pojedynczy alarm): Po wybraniu pojedynczego alarmu cel w skonfigurowanym obszarze wywoła alarm tylko raz. W przypadku niezaznaczenia tej opcji ten sam cel w tym samym skonfigurowanym obszarze będzie wywoływał ciągły alarm.

Leave Interference Suppression (Eliminacja zakłóceń powodowanych przez liście)

Zaznacz to pole wyboru, aby zniwelować zakłócenia spowodowane przez liście w skonfigurowanym obszarze.

Typ wyjścia (Output Type): Wybierz pozycję ramki. Do wyboru są Target Center (Cel w środku), Bottom Center (W środku na dole) i Top Centers (W środku na górze). Przykład: Cel będzie się znajdował w środku ramki po wybraniu opcji Target Center (Cel w środku).

Restore Default (Przywracanie ustawień domyślnych): Kliknij, aby przywrócić skonfigurowane parametry do ustawień domyślnych.

Restart VCA (Ponowne uruchomienie VCA): Ponownie uruchom bibliotekę algorytmów analizy zachowania.

- Globalny filtr rozmiaru

Uwaga: W porównaniu z filtrem rozmiaru w regule, dotyczącym odrębnej reguły, globalny filtr rozmiaru dotyczy wszystkich reguł.

Kroki:

1. Zaznacz pole wyboru **Global Size Filter** (Globalny filtr rozmiaru), aby włączyć tę funkcję.
2. Jako Filter Type (Typ filtru) wybierz Actual Size (Rozmiar rzeczywisty) lub Pixel (Piksel).

Actual Size (Rozmiar rzeczywisty): Wpisz długość i szerokość rozmiaru maksymalnego i minimalnego. Alarm zostanie wyzwolony tylko przez cel o rozmiarze zawierającym się między wartością minimalną i maksymalną.

Uwagi:

- W przypadku wyboru filtru wg rozmiaru rzeczywistego należy skonfigurować kalibrację kamery.
- Długość rozmiaru maksymalnego powinna być większa niż długość rozmiaru minimalnego, podobnie szerokość.

Pixel (Piksel): Kliknij Minimum Size (Rozmiar minimalny), aby na podglądzie na żywo narysować prostokąt rozmiaru minimalnego. Kliknij Maximum Size (Rozmiar maksymalny), aby na podglądzie na żywo narysować prostokąt rozmiaru maksymalnego. Cele mniejsze niż rozmiar minimalny i większe niż

rozmiar maksymalny będą filtrowane.

Uwagi:

- Narysowany obszar będzie konwertowany na piksele przez algorytm działający w tle.
 - Jeśli podgląd na żywo zostanie zatrzymany, nie będzie można skonfigurować globalnego filtru rozmiaru.
 - Długość rozmiaru maksymalnego powinna być większa niż długość rozmiaru minimalnego, podobnie szerokość.
3. Kliknij **Save** (Zapisz), aby zapisać ustawienia.

5.7.2 Rejestracja twarzy

Rejestracja twarzy może rejestrować twarz, która pojawi się w skonfigurowanym obszarze. Wraz ze zrobionym zdjęciem twarzy będą wysyłane informacje opisowe, takie jak wiek, płeć i czy dana osoba nosi okulary.

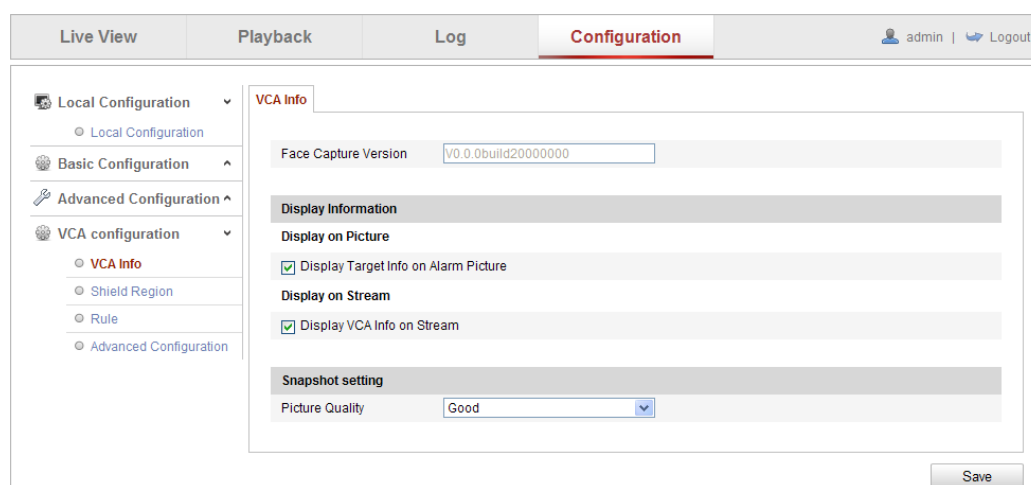


Figure 5-72 Rejestracja twarzy

❖ VCA Info (Informacje VCA)

Face Capture Version (Wersja rejestracji twarzy): Wyświetla wersję biblioteki algorytmów.

Display Information (Wyświetlane informacje) obejmują wyświetlanie na zdjęciu i na strumieniu.

Display Target info. on Alarm Picture (Wyświetlanie informacji o celu na

zdjęciu alarmu): Zaznaczenie tego pola wyboru spowoduje, że na wgranym zdjęciu alarmu cel zostanie oznaczony ramką.

Display VCA info. on Stream (Wyświetlanie informacji VCA na strumieniu): W podglądzie na żywo lub podczas odtwarzania cel będzie oznaczony zieloną ramką.

Snapshot Setting (Ustawienie zrzutu ekranu): Wybierz jakość obrazu dla zrobionego zdjęcia. Do wyboru są Good (Dobra), Better (Lepsza) i Best (Najlepsza).

❖ **Shield Region (Strefa bez wykrywania)**

Strefa bez wykrywania pozwala ustawić specjalną strefę, w której rejestracja twarzy nie będzie przeprowadzana. Obsługiwane są maks. 4 strefy bez wykrywania.

Kroki:

1. Kliknij zakładkę **Shield Region** (Strefa bez wykrywania), aby otworzyć interfejs konfiguracji strefy bez wykrywania.
2. Kliknij **Draw Area** (Narysuj obszar). Narysuj obszar, klikając lewym przyciskiem cztery punkty końcowe w oknie podglądu na żywo, kliknij prawym przyciskiem, aby zakończyć rysowanie obszaru.

Uwagi:

- Kliknij **Delete** (Usuń), aby usunąć narysowane obszary.
 - Jeśli podgląd na żywo zostanie zatrzymany, nie można narysować stref bez wykrywania.
3. Kliknij **Save** (Zapisz), aby zapisać ustawienia.

❖ **Rule (Reguła)**

Kroki:

1. Zaznacz pole wyboru **Rule** (Reguła), aby włączyć reguły rejestracji twarzy.
2. Kliknij **Minimize Pupil Distance** (Minimalna odległość między źrenicami), aby narysować minimalną odległość między źrenicami. W polu pod podglądem na żywo wyświetli się narysowana odległość między źrenicami. Minimalna odległość między źrenicami odnosi się do minimalnego rozmiaru kwadratu będącego obszarem między źrenicami, jest to podstawowy standard, według którego kamera identyfikuje cel.
3. Kliknij **Draw Area** (Narysuj obszar), aby narysować obszar, w którym ma działać rejestracja twarzy. Narysuj obszar, klikając lewym przyciskiem

punkty końcowe w oknie podglądu na żywo, kliknij prawym przyciskiem, aby zakończyć rysowanie obszaru.

Uwagi:

- Obsługiwany jest obszar wielokąta (4~10 boków).
- Jeśli podgląd na żywo zostanie zatrzymany, nie można narysować skonfigurowanego obszaru.

4. Kliknij **Save** (Zapisz), aby zapisać ustawienia.

❖ **Advanced Configuration (Konfiguracja zaawansowana)**

Skonfiguruj następujące parametry odpowiadające rzeczywistemu otoczeniu.

Detection Parameters (Parametry wykrywania):

Generation Speed (Szybkość generacji) [1~5] Szybkość identyfikacji celu. Im wyższa wartość, tym szybciej cel będzie rozpoznawany. W przypadku ustawienia dość niskiej wartości, jeśli w skonfigurowanym obszarze twarz znajdowała się od początku, nie zostanie ona zarejestrowana. Może to ograniczyć liczbę fałszywych trafień w przypadku malunków lub plakatów na ścianach. Zaleca się pozostawienie wartości domyślnej 3.

Capture Times (Czasy rejestracji) [1~10]: Odnosi się do tego, ile razy twarz będzie rejestrowana w trakcie przebywania w skonfigurowanym obszarze. Wartość domyślna to 1.

Sensitivity (Czułość) [1~5]: Czułość identyfikacji celu. Im wyższa wartość, tym łatwiej będzie rozpoznawana twarz, ale wzrośnie również liczba fałszywych alarmów. Zaleca się pozostawienie wartości domyślnej 3.

Capture Interval (Interwał rejestracji) [1~255 klatek]: Interwał klatek między kolejnymi zdjęciami. Ustawienie tej wartości na 1 (domyślnie) powoduje, że kamera rejestruje twarz w każdej klatce.

Capture Sensitivity (Czułość rejestracji) [0~20]: Próg, po którego osiągnięciu kamera traktuje cel jak twarz. Dopiero gdy punktacja twarzy generowana przez algorytm będzie równa tej wartości lub ją przekroczy, kamera potraktuje cel jak twarz. Zaleca się pozostawienie wartości domyślnej 2.

Face Capture Advanced Parameters (Zaawansowane parametry rejestracji)

twarzy):

Face Exposure (Ekspozycja twarzy): Zaznacz pole wyboru, aby włączyć ekspozycję twarzy.

Reference Brightness (Jasność odniesienia) [0~100]: Jasność odniesienia twarzy w trybie ekspozycji twarzy. Po wykryciu twarzy kamera dostosowuje jasność twarzy od ustawionej wartości. Im wyższa wartość, tym jaśniejsza twarz.

Minimum Duration (Min. czas trwania) [1~60 min]: Minimalny czas, przez który kamera wykonuje ekspozycję twarzy. Wartość domyślna to 1 minuta.

Uwaga: W przypadku włączenia ekspozycji twarzy należy się upewnić, że wyłączono funkcję WDR i wybrano ręczną przysłonę.

Enable Face ROI (Włącz ROI twarzy): Gdy kamera rejestruje twarz, obszar twarzy będzie traktowany jak obszar zainteresowania, a jakość obrazu tego obszaru zostanie wzmocniona.

Restore Default (Przywracanie ustawień domyślnych): Kliknij **Restore** (Przywróć), aby przywrócić wszystkie ustawienia w konfiguracji zaawansowanej do wartości domyślnych.

The screenshot shows a web interface titled "Parameters" with a sub-section "Parameters". Under "Detection Parameters", there are five sliders with corresponding numeric input boxes: "Generation Speed[1-5]" (value 3), "Capture Times[1-10]" (value 1), "Sensitivity[1-5]" (value 3), "Capture Interval[1-255 fra...]" (value 1), and "Capture Sensitivity[0-20]" (value 4). Under "Face Capture Advanced ...", there are three items: "Face Exposure" (checked checkbox), "Reference Brightness[0-...]" (slider with value 50), and "minimum duration[1-60...]" (slider with value 1). At the bottom, there is a "Restore Default" label and a "Restore" button.

Figure 5-73 Konfiguracja zaawansowana

5.7.3 Kolorowa mapa danych

Kolorowa mapa danych (zwana też mapą cieplną), to graficzne przedstawienie danych reprezentowanych przez kolory. Funkcja kolorowej mapy danych kamery zwykle służy do analizy czasów obecności i czasów przebywania w skonfigurowanym obszarze.

❖ Konfiguracja kolorowej mapy danych

Kroki:

1. Przejdź do interfejsu konfiguracji kolorowej mapy danych: **Configuration > Advanced Configuration > Heat Map (Konfiguracja > Konfiguracja zaawansowana > Kolorowa mapa danych)**

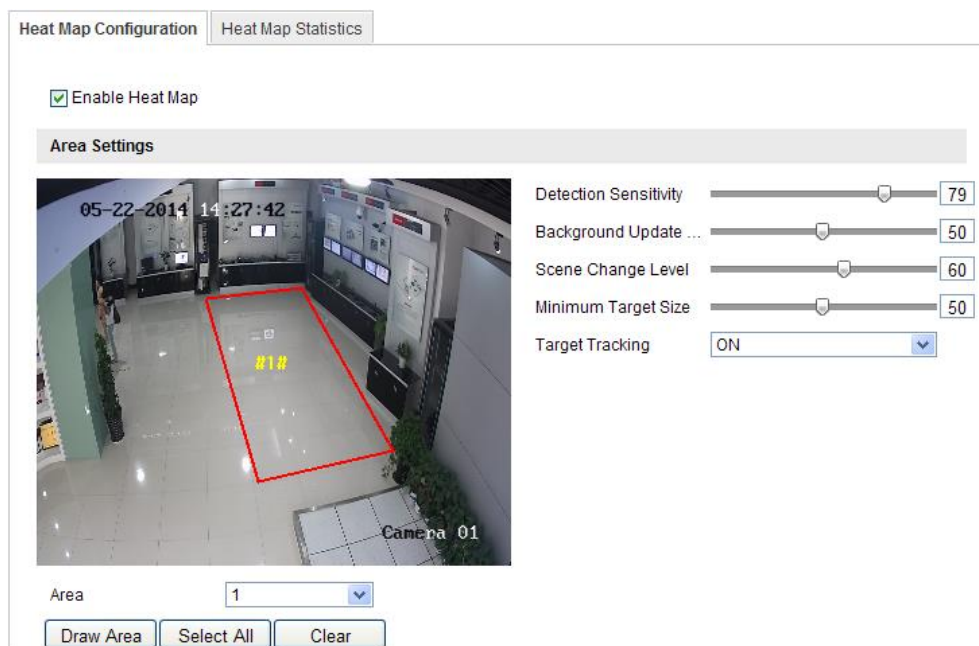


Figure 5-74 Konfiguracja kolorowej mapy danych

2. Wybierz zakładkę **Heat Map Configuration** (Konfiguracja kolorowej mapy danych), aby ustawić szczegółowe parametry.
3. Zaznacz pole wyboru **Enable Heat Map** (Włącz kolorową mapę danych), aby włączyć tę funkcję.
4. Kliknij **Draw Area** (Narysuj obszar), aby zdefiniować obszar dla statystyk wartości w postaci kolorów. Narysuj obszar, klikając lewym przyciskiem cztery punkty końcowe w oknie podglądu na żywo, kliknij prawym

przyciskiem, aby zakończyć rysowanie obszaru. Można skonfigurować maks. 8 obszarów.

Uwaga: Możesz kliknąć **Select All** (Wybierz wszystko), aby jako skonfigurowany obszar wybrać całe okno podglądu na żywo. Kliknij **Delete** (Usuń), aby usunąć aktualny narysowany obszar.

5. Skonfiguruj parametry dla narysowanego obszaru.

Detection Sensitivity (Czułość wykrywania) [0~100]: Odnosi się do czułości, z jaką kamera identyfikuje cel. Zbyt duża czułość może spowodować fałszywe trafienia. Zaleca się ustawienie domyślnej czułości 50.

Background Update Rate (Częstotliwość aktualizacji tła) [0~100]: Odnosi się do szybkości, z jaką nowa scena zastępuje poprzednią. Przykład: Jeśli kamera jest zwrócona na regał z towarami, ludzie obok regału zostaną policzeni dwukrotnie, gdy towary zostaną zdjęte z regału, a kamera potraktuje regał (opróżniony z towarów) jako nową scenę. Zaleca się pozostawienie wartości domyślnej 50.

Scene Change Level (Poziom zmiany sceny) [0~100]: Odnosi się do poziomu reakcji kamery na dynamiczne otoczenie, np. powiewającą na wietrze zasłonę. Kamera może potraktować powiewającą zasłonę jako cel. Prawidłowe ustawienie poziomu pozwoli uniknąć fałszywych trafień. Poziom domyślny to 50.

Minimum Target Size (Minimalny rozmiar celu) [0~100] Odnosi się do rozmiaru, przy którym kamera identyfikuje cel. Można ustawić rozmiar celu zgodnie z rzeczywistym otoczeniem. Rozmiar domyślny to 50.

Target Track (Śledzenie celu): Wybierz ON (Wł.) lub OFF (Wył.), aby włączyć lub wyłączyć śledzenie celu.

6. Kliknij **Edit** (Edytuj), aby ustawić harmonogram uzbrajania.
7. Wybierz powiązaną metodę, zaznaczając pole wyboru Notify the Surveillance Center (Powiadom centrum monitoringu).
8. Kliknij **Save** (Zapisz), aby zapisać ustawienia.

❖ Statystyki kolorowej mapy danych

Kroki:

1. Kliknij **Heat Map Statistics** (Statystyki kolorowej mapy danych), aby otworzyć interfejs statystyk danych.
2. Wybierz typ raportu, klikając menu rozwijane. Do wyboru są: Daily Report

(Raport dzienny), Weekly Report (Raport tygodniowy), Monthly Report (Raport miesięczny) i Annual Report (Raport roczny).

3. Kliknij **Counting** (Liczenie), aby wyeksportować dane.
4. Wybierz **Statistics Result** (Wynik statystyk) jako Space Heat Map (Kolorowa mapa danych wg miejsca) lub Time Heat Map (Kolorowa mapa danych wg czasu), zostanie wyświetlona odpowiednia mapa.

W przypadku wyboru wyświetlania statystyk jako mapy wg czasu, pojawi się przycisk **Export** (Eksport), służący do wyeksportowania danych do pliku Excel.

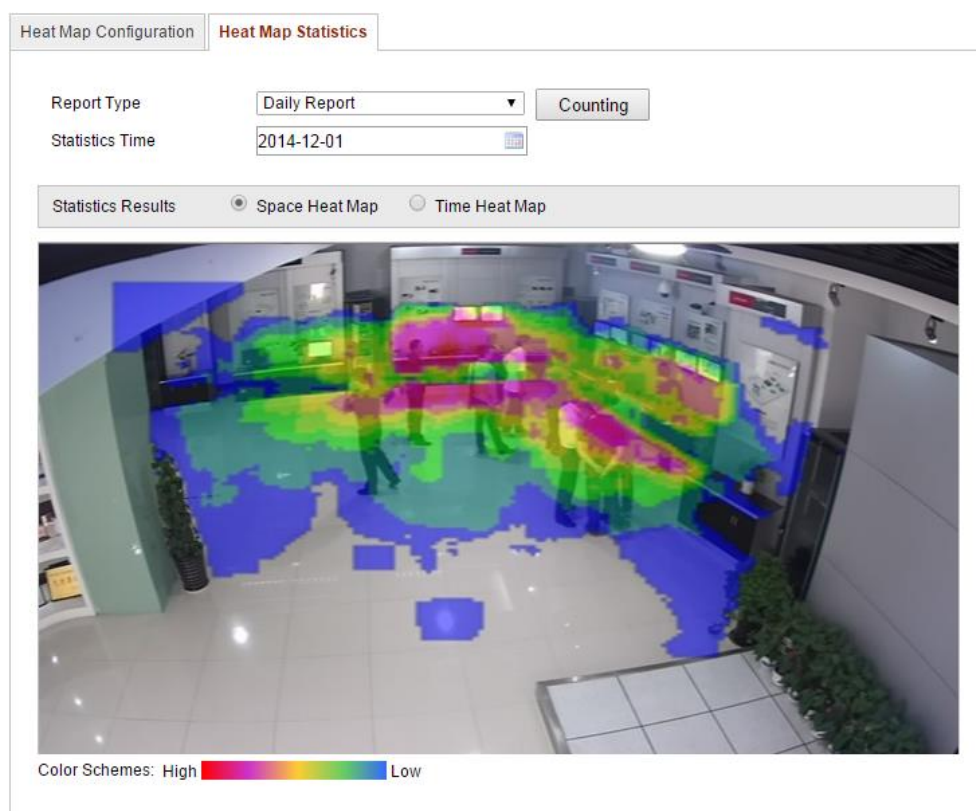


Figure 5-75 Kolorowa mapa danych wg miejsca

Uwagi:

- Jak pokazano na ilustracji powyżej, blok w kolorze czerwonym (255, 0, 0) wskazuje najczęściej odwiedzany obszar, a blok w kolorze niebieskim (0, 0, 255) wskazuje rzadziej odwiedzany obszar.
- Zaleca się, aby po instalacji nie wykonywać regulacji elektronicznego obiektywu, ponieważ może to spowodować pogorszenie dokładności danych.

5.7.4 Liczenie osób

Funkcja liczenia osób pomaga zliczyć liczbę ludzi, którzy weszli w określony skonfigurowany obszar lub z niego wyszli, często stosuje się ją przy obserwacji wejść i wyjść.

Uwagi:

- Funkcję liczenia osób obsługują niektóre modele kamer iDS.
- Zaleca się instalację kamery prostopadle względem ziemi, wówczas funkcja liczenia osób będzie dokładniejsza.

❖ **Konfiguracja liczenia osób**

Kroki:

1. Przejdź do interfejsu konfiguracji liczenia osób:
Configuration > Advanced Configuration > People Counting
(**Konfiguracja > Konfiguracja zaawansowana > Liczenie osób**)
2. Wybierz zakładkę **People Counting Configuration** (Konfiguracja liczenia osób), aby ustawić szczegółowe parametry.

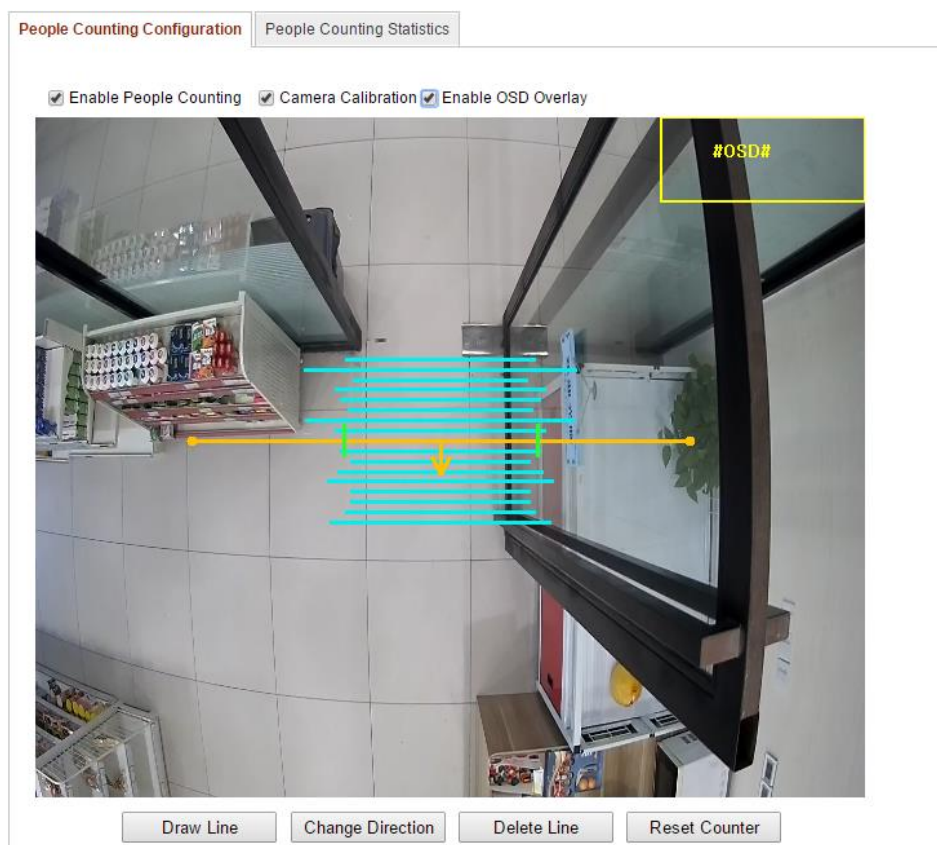


Figure 5-76 Konfiguracja liczenia os ǒb

3. Zaznacz pole wyboru **Enable People Counting** (Włącz liczenie os ǒb), aby włączyć tę funkcję.
4. (Opcja) Zaznacz pole wyboru **Enable OSD Overlay** (Włącz nakładanie OSD), wówczas na wideo na żywo będzie wyświetlana w czasie rzeczywistym liczba os ǒb wchodzących i wychodzących.
5. Ustaw linię wykrywania.
Na wideo na żywo można ustawić pomarańczową linię, tzw. linię wykrywania. Wówczas ludzie wchodzący i wychodzący, którzy przechodzą przez tę linię, będą wykrywania i liczeni.
 - 1) Kliknij **Draw Line** (Narysuj linię), na obrazie pojawi się pomarańczowa linia wykrywania.
 - 2) Kliknij i przeciągnij linię wykrywania, aby dostosować jej położenie.
 - 3) Kliknij i przeciągnij dwa punkty końcowe linii wykrywania, aby dostosować jej długość.
 - 4) Aby usunąć linię wykrywania, kliknij przycisk **Delete Line** (Usuń linię).
- Uwaga:** Linia wykrywania powinna obejmować całe wejście/wyjście.
6. Po wybraniu linii wykrywania pojawia się strzałka wskazująca kierunek przechodzenia os ǒb. Kliknij przycisk **Change Direction** (Zmień kierunek), aby zmienić kierunek strzałki na przeciwny.
7. Zaznacz pole wyboru **Camera Calibration** (Kalibracja kamery), aby włączyć tę funkcję.
8. Kliknij przycisk **Reset Counter** (Resetuj licznik), liczba os ǒb, które weszły i wyszły, zostanie wyzerowana.
9. Kliknij **Edit** (Edytuj), aby ustawić harmonogram uzbrajania.
10. Zaznacz pole wyboru **Notify Surveillance Center** (Powiadom centrum monitoringu), aby ustawić powiązane działanie.
11. Kliknij **Save** (Zapisz), aby zapisać ustawienia.

❖ Dane statystyczne liczenia os ǒb

Kroki:

1. Kliknij **People Counting Statistics** (Dane statystyczne liczenia os ǒb), aby otworzyć interfejs statystyki danych.
2. Wybierz typ raportu, klikając menu rozwijane. Do wyboru są: Daily Report

(Raport dzienny), Weekly Report (Raport tygodniowy), Monthly Report (Raport miesięczny) i Annual Report (Raport roczny).

3. Wybierz **Statistics Type** (Typ statystyki): People Entered (Liczba osób wchodzących) lub People Exited (Liczba osób wychodzących).
4. Wybierz **Statistics Time** (Czas statystyki).
Uwaga: Raport dzienny oblicza dane dla wybranej daty, raport tygodniowy oblicza dane dla tygodnia, w którym przypada wybrany dzień, raport miesięczny oblicza dane dla miesiąca, w którym przypada wybrany dzień, a raport roczny oblicza dane dla roku, w którym przypada wybrany dzień.
5. Kliknij **Counting** (Liczenie), aby obliczyć dane.
6. Wybierz postać eksportu **Statistics Result** (Wynik statystyki): Table (Tabela), Bar Chart (Wykres słupkowy), Line Chart (Wykres liniowy).

Uwaga: W przypadku wyboru wyświetlania statystyki jako tabeli pojawi się przycisk **Export** (Eksport), służący do wyeksportowania danych do pliku Excel.

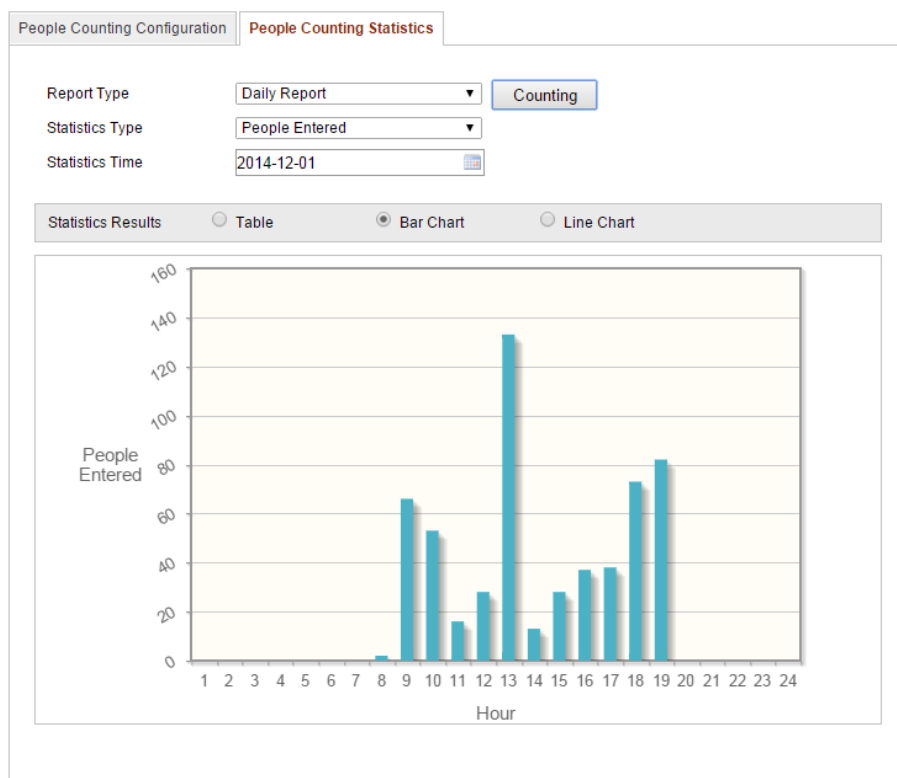


Figure 5-77 Wyniki statystyczne

Uwaga: Zaleca się, aby po instalacji nie wykonywać regulacji elektronicznego obiektywu, ponieważ może to spowodować pogorszenie dokładności danych.

Chapter 6 Ustawienia pamięci masowej

Przed rozpoczęciem pracy:

Aby skonfigurować ustawienia nagrań, upewnij się, że w sieci jest dostępne sieciowe urządzenie pamięci masowej lub do kamery jest włożona karta SD.

6.1 Konfiguracja ustawień NAS

Przed rozpoczęciem pracy:

W sieci powinien być dostępny dysk sieciowy, odpowiednio skonfigurowany, aby przechowywać nagrania, pliki dzienników itp.

Kroki:

1. Dodaj dysk sieciowy

- (1) Otwórz ustawienia interfejsu NAS (Network-Attached Storage – sieciowa pamięć masowa):

Configuration > Advanced Configuration > Storage > NAS (Konfiguracja > Konfiguracja zaawansowana > Pamięć masowa > NAS)

HDD No.	Type	Server Address	File Path
1	NAS	172.6.21.99	/dvr/test01
Mounting Type: NFS <input type="button" value="v"/> NFS <input type="button" value="v"/> SMB/CIFS			
2	NAS		
3	NAS		
4	NAS		
5	NAS		
6	NAS		
7	NAS		
8	NAS		

Figure 6-1 Dodawanie dysku sieciowego

- (2) Wpisz adres IP dysku sieciowego i ścieżkę do plików.

- (3) Wybierz Typ montowania. Do wyboru są NFS i SMB/CIFS. W przypadku wybrania SMB/CIFS możesz ustawić nazwę użytkownika i hasło, aby zapewnić bezpieczeństwo.

Uwaga: Informacje na temat tworzenia ścieżki do plików znajdują się w *Podręczniku użytkownika NAS*.



- *Aby lepiej chronić prywatność i system przed ryzykami związanymi z bezpieczeństwem, zdecydowanie zalecamy stosowanie silnych haseł dla wszystkich funkcji i urządzeń sieciowych. Hasło powinno być wybrane przez użytkownika (i zawierać co najmniej 8 znaków, w tym wielkie i małe litery, cyfry i znaki specjalne), aby zwiększyć bezpieczeństwo produktu.*
- *Instalator i(lub) użytkownik końcowy ponoszą odpowiedzialność za prawidłową konfigurację wszystkich haseł i innych ustawień bezpieczeństwa.*

- (4) Kliknij **Save** (Zapisz), aby dodać dysk sieciowy.

2. Zainicjalizuj dodany dysk sieciowy.

- (1) Przejdź do interfejsu ustawień dysku twardego (**Advanced Configuration > Storage > Storage Management** (Konfiguracja zaawansowana > Pamięć masowa > Zarządzanie pamięcią masową)), w którym znajdują się informacje o pojemności, wolnym miejscu, stanie, rodzaju i właściwościach dysku.

Record Schedule
Storage Management
NAS
Snapshot

HDD Device List
Format

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

Quota

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

Figure 6-2 Interfejs zarządzania pamięcią masową

- (2) Jeśli stan dysku to **Uninitialized** (Niezainicjalizowany), zaznacz odpowiednie pole wyboru, aby wybrać dysk, a następnie kliknij **Format**, aby rozpocząć inicjalizację dysku.

Po zakończeniu inicjalizacji stan dysku zmieni się na **Normal** (Normalny).

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

Figure 6-3 Wyświetlanie stanu dysku

3. Zdefiniuj limit miejsca na nagrania i zdjęcia.
- (1) Wpisz procent limitu miejsca na zdjęcia i nagrania.
- (2) Kliknij **Save** (Zapisz) i odśwież stronę, aby aktywować ustawienia.

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

Figure 6-4 Ustawienia limitu miejsca

Uwagi:

- Do kamery można podłączyć maks. 8 dysków NAS.
- Po włożeniu karty SD wykonaj takie same kroki jak w przypadku inicjalizacji dysku NAS, aby ją zainicjalizować i móc jej używać.

6.2 Konfiguracja harmonogramu nagrywania

Cel:

Istnieją dwa rodzaje nagrywania przez kamerę: ręczne nagrywanie i zaplanowane nagrywanie. Informacje na temat ręcznego nagrywania znajdują się w *Sekcji 5.3*

Ręczne nagrywanie i robienie zdjęć. Wykonaj instrukcje w tej sekcji, aby skonfigurować zaplanowane nagrywanie. Domyślnie pliki z nagraniami z zaplanowanego nagrywania są zapisywane na karcie SD (jeśli jest obsługiwana) lub na dysku sieciowym.

Kroki:

1. Przejdź do interfejsu ustawień harmonogramu nagrywania:

Configuration > Advanced Configuration> Storage > Record Schedule
(Konfiguracja > Konfiguracja zaawansowana > Pamięć masowa > Harmonogram nagrywania)

The screenshot displays the 'Record Schedule' configuration page. At the top, there are three dropdown menus: 'Pre-record' set to '5s', 'Post-record' set to '5s', and 'Overwrite' set to 'Yes'. Below these is a checked checkbox labeled 'Enable Record Schedule'. The main part of the interface is a 24-hour grid for each day of the week (Mon-Sun). The grid is color-coded according to a legend on the right: Continuous (blue), Motion Detection (green), Alarm (red), Motion | Alarm (orange), Motion & Alarm (light blue), and Other (purple). The grid shows that from 00:00 to 08:00, the recording mode is 'Motion Detection' (green). From 08:00 to 14:00, it is 'Motion & Alarm' (light blue). From 14:00 to 20:00, it is 'Other' (purple). From 20:00 to 24:00, it is 'Continuous' (blue). There are also 'Edit' and 'Save' buttons.

Figure 6-5 Interfejs harmonogramu nagrywania

2. Zaznacz pole wyboru **Enable Record Schedule** (Włącz harmonogram nagrywania), aby włączyć tę funkcję.
3. Ustaw parametry nagrania z kamery.

This is a close-up of the recording parameters section. It shows three dropdown menus: 'Pre-record' set to '5s', 'Post-record' set to '5s', and 'Overwrite' set to 'Yes'.

Figure 6-6 Parametry nagrania

- Pre-record (Prealarm – wyprzedzenie rozpoczęcia nagrywania): Ustaw czas rozpoczęcia nagrania przed zaplanowanym czasem lub zdarzeniem. Jeśli np. alarm wyzwała nagrywanie o 10:00, a czas prealarmu jest ustawiony na 5 sekund, kamera rozpoczyna nagrywanie o 9:59:55.

Dostępne opcje prealarmu: No Pre-record (Bez prealarmu), 5 s, 10 s, 15 s, 20 s, 25 s, 30 s lub Not limited (Nieograniczony).

- Post-record (Postalarm – opóźnienie zakończenia nagrywania): Ustaw czas zakończenia nagrania po zaplanowanym czasie lub zdarzeniu. Jeśli np. nagrywanie wyzwolone alarmem kończy się o 11:00, a czas postalarmu jest ustawiony na 5 sekund, kamera kończy nagrywanie o 11:00:05.

Dostępne opcje czasu postalarmu: 5 s, 10 s, 30 s, 1 min, 2 min, 5 min lub 10 min.

Uwaga: Opcje konfiguracji parametrów nagrywania zależą od modelu kamery.

4. Kliknij **Edit** (Edytuj), aby edytować harmonogram nagrywania.

The screenshot shows the 'Edit Schedule' dialog box. At the top, there are tabs for days of the week: Mon, Tue, Wed, Thu, Fri, Sat, Sun. Below the tabs, there are two radio buttons: 'All Day' (unselected) and 'Customize' (selected). To the right of the 'All Day' radio button is a dropdown menu showing 'Continuous'. Below this is a table with 8 rows. The table has four columns: 'Period', 'Start Time', 'End Time', and 'Record Type'. Each row has a 'Period' number from 1 to 8, 'Start Time' and 'End Time' both set to '00:00', and 'Record Type' set to 'Continuous'. Below the table, there is a 'Copy to Week' section with a 'Select All' checkbox and checkboxes for each day of the week: Mon (checked), Tue, Wed, Thu, Fri, Sat, Sun. To the right of these checkboxes is a 'Copy' button. At the bottom right of the dialog are 'OK' and 'Cancel' buttons.

Period	Start Time	End Time	Record Type
1	00:00	00:00	Continuous
2	00:00	00:00	Continuous
3	00:00	00:00	Continuous
4	00:00	00:00	Continuous
5	00:00	00:00	Continuous
6	00:00	00:00	Continuous
7	00:00	00:00	Continuous
8	00:00	00:00	Continuous

Figure 6-7 Harmonogram nagrywania

5. Wybierz dzień, w którym ma zostać ustawiony harmonogram nagrywania.

(1) Ustaw nagrywanie całego dnia lub nagrywanie segmentu:

- ◆ Aby skonfigurować nagrywanie całego dnia, zaznacz pole wyboru **All Day** (Cały dzień).
 - ◆ Aby nagrywać w różnych odcinkach czasu, zaznacz pole wyboru **Customize** (Własne). Ustaw **Start Time** (Czas rozpoczęcia) i **End Time** (Czas zakończenia).
- Uwaga:** Segmenty nie mogą się nakładać. Można skonfigurować maks. 4 segmenty.

(2) Wybierz **Record Type** (Typ nagrywania). Dostępne opcje typu nagrywania: Continuous (Ciągłe), Motion Detection (Wykrywanie ruchu), Alarm, Motion | Alarm (Ruch lub alarm), Motion & Alarm (Ruch i alarm naraz), PIR Alarm (Alarm PIR), Wireless Alarm (Alarm bezprzewodowy), Emergency Alarm (Alarm awaryjny) lub Motion | Alarm Input | PIR | Wireless | Emergency (dowolna z opcji ruch/wejście alarmowe/PIR/bezprzewodowy/awaryjny).

◆ **Continuous (Ciągłe)**

Po wybraniu **Continuous** (Ciągłe) wideo będzie nagrywane automatycznie, zgodnie z czasem w harmonogramie.

◆ **Record Triggered by Motion Detection (Nagrywanie wyzwolone przez wykrywanie ruchu)**

Po wybraniu **Motion Detection** (Wykrywanie ruchu) wideo będzie nagrywane w razie wykrycia ruchu.

Oprócz skonfigurowania harmonogramu nagrywania trzeba ustawić obszar wykrywania ruchu i zaznaczyć pole wyboru **Trigger Channel** (Kanał wyzwalania) w opcji **Linkage Method (Powiązana metoda)** w interfejsie ustawień wykrywania ruchu. Szczegółowe informacje znajdują się w *Kroku 1 Ustaw obszar wykrywania ruchu w Sekcji 6.6.1.*

◆ **Record Triggered by Alarm (Nagrywanie wyzwolone przez alarm)**

Po wybraniu **Alarm** wideo będzie nagrywane w momencie wyzwolenia alarmu za pośrednictwem kanałów wejściowych zewnętrznego alarmu.

Oprócz skonfigurowania harmonogramu nagrywania trzeba ustawić **Alarm Type** (Typ alarmu) i zaznaczyć pole wyboru **Trigger Channel** (Kanał

wyzwalania) w opcji **Linkage Method** (Powiązana metoda) interfejsu **Alarm Input Settings** (Ustawienia wejścia alarmowego). Szczegółowe informacje znajdują się w *Sekcji 6.6.3*

◆ **Record Triggered by Motion & Alarm (Nagrywanie wyzwolone przez ruch i alarm naraz)**

Po wybraniu **Motion & Alarm** (Ruch i alarm naraz) wideo będzie nagrywane, gdy ruch oraz alarm zostaną wyzwolone jednocześnie.

Oprócz konfiguracji harmonogramu nagrywania należy skonfigurować ustawienia interfejsów **Motion Detection** (Wykrywanie ruchu) i **Alarm Input Settings** (Ustawienia wejścia alarmowego). Szczegółowe informacje znajdują się w *Sekcji 6.6.1* i *Sekcji 6.6.3*.

◆ **Record Triggered by Motion | Alarm (Nagrywanie wyzwolone przez ruch lub alarm)**

Po wybraniu **Motion | Alarm** (Ruch lub alarm) wideo będzie nagrywane w momencie wyzwolenia zewnętrznego alarmu lub wykrycia ruchu.

Oprócz konfiguracji harmonogramu nagrywania należy skonfigurować ustawienia interfejsów **Motion Detection** (Wykrywanie ruchu) i **Alarm Input Settings** (Ustawienia wejścia alarmowego). Szczegółowe informacje znajdują się w *Sekcji 6.6.1* i *Sekcji 6.6.3*.

Edit Schedule

Mon | Tue | Wed | Thu | Fri | Sat | Sun

All Day Continuous

Customize

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

Copy to Week Select All

Mon Tue Wed Thu Fri Sat Sun Copy

OK Cancel

Figure 6-8 Zmień harmonogram nagrywania

- (3) Zaznacz pole wyboru **Select All** (Wybierz wszystko) i kliknij **Copy** (Kopiuj), aby skopiować ustawienia tego dnia na cały tydzień. Możesz też zaznaczyć dowolne pola wyboru obok daty i kliknąć **Copy** (Kopiuj).
- (4) Kliknij **OK**, aby zapisać ustawienia i zamknąć interfejs **Edit Record Schedule** (Edytuj harmonogram nagrywania).

6. Kliknij **Save** (Zapisz), aby zapisać ustawienia.

6.3 Konfiguracja ustawień zrzutu ekranu

Cel:

Można skonfigurować zaplanowany zrzut ekranu lub zrzut wyzwolony przez zdarzenie. Zrobione zdjęcie może zostać zapisane na karcie SD (jeśli jest obsługiwana) lub dysku sieciowym (szczegółowe informacje na temat dysku sieciowego znajdują się w *Sekcji 7.1 Konfiguracja ustawień NAS*). Możesz też wysyłać zrobione zdjęcia na serwer FTP.

Ustawienia podstawowe

Kroki:

1. Przejdź do interfejsu ustawień zrzutu ekranu:

Configuration > Advanced Configuration > Storage > Snapshot (Konfiguracja > Konfiguracja zaawansowana > Pamięć masowa > Zrzut)

2. Zaznacz pole wyboru **Enable Timing Snapshot** (Włącz czasowe zrzuty ekranu), aby włączyć ciągłe robienie zrzutów. Zaznacz pole wyboru **Enable Event-triggered Snapshot** (Włącz zrzuty ekranu wyzwalane zdarzeniem), aby włączyć robienie zrzutów, gdy wystąpi zdarzenie.
3. Wybierz jakość zrzutu.
4. Ustaw odstęp czasu między dwoma zrzutami.
5. Kliknij **Save** (Zapisz), aby zapisać ustawienia.

Wysyłanie na FTP

Wykonaj poniższe instrukcje, aby skonfigurować wysyłanie zrzutów na FTP.

- Wgrywaj ciągłe zrzuty ekranu na FTP

Kroki:

- 1) Skonfiguruj ustawienia FTP i zaznacz pole wyboru **Upload Picture** (Wyślij zdjęcie) w interfejsie ustawień FTP. Szczegółowe informacje na temat konfiguracji parametrów FTP znajdują się w *Sekcji 6.3.12 Konfiguracja ustawień FTP*.

- 2) Zaznacz pole wyboru **Enable Timing Snapshot** (Włącz czasowe zrzuty ekranu).

- Wysyłaj do FTP zrzuty ekranu wyzwolone przez zdarzenie.

Kroki:

- 1) Skonfiguruj ustawienia FTP i zaznacz pole wyboru **Upload Picture** (Wyślij zdjęcie) w interfejsie ustawień FTP. Szczegółowe informacje na temat konfiguracji parametrów FTP znajdują się w *Sekcji 6.3.12 Konfiguracja ustawień FTP*.

- 2) Zaznacz pole wyboru **Upload Picture** (Wyślij zdjęcie) w interfejsie ustawień wykrywania ruchu lub wejścia alarmowego. Zapoznaj się z *Krokiem 3 Ustaw działania alarmu podjęte dla wykrywania ruchu* w *Sekcji 6.6.1* lub *Krokiem 4 Konfiguracja zewnętrznych wejść alarmowych* w *Sekcji 6.6.4*.

- 3) Zaznacz pole wyboru **Enable Event-triggered Snapshot** (Włącz zrzut ekranu wyzwalany przez zdarzenie).

Timing

Enable Timing Snapshot

Format: JPEG

Resolution: 1920*1080

Quality: High

Interval: 0 millisecond

Event-Triggered

Enable Event-Triggered Snapshot

Format: JPEG

Resolution: 1920*1080

Quality: High

Interval: 0 millisecond

Capture Number: 4

Save

Figure 6-9 Ustawienia zrzutu ekranu

6.4 Konfiguracja Lite Storage

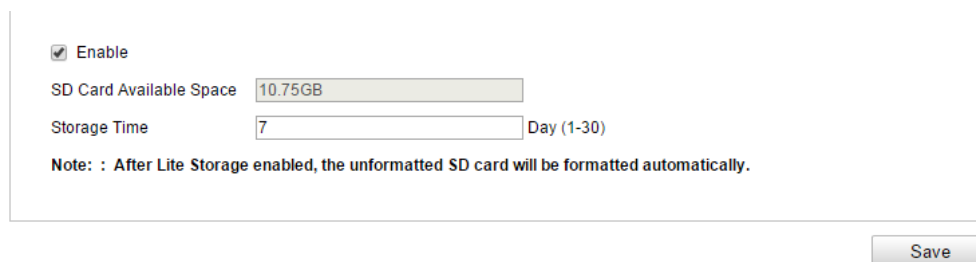
Cel:

Gdy w scenariuszu monitorowania nie ma poruszającego się obiektu, można zmniejszyć liczbę klatek i przepływność strumienia wideo, aby wydłużyć dostępny czas zapisu na karcie SD.

Uwagi:

- Funkcja Lite Storage zależy od modelu kamery.
 - Pliki wideo nagrane w trybie Lite Storage będą odtwarzane z pełną liczbą klatek (25 fps/30 fps), dlatego odtwarzanie będzie w przyspieszonym tempie.
1. Przejdź do interfejsu Lite Storage: **Configuration > Advanced Configuration > Storage > Lite Storage** (Konfiguracja > Konfiguracja zaawansowana > Pamięć masowa > Lite Storage.)
 2. Zaznacz pole wyboru **Enable** (Włącz), aby włączyć funkcję Lite Storage.
 3. W polu tekstowym wpisz czas zapisu w pamięci masowej. Na tej stronie można zobaczyć ilość miejsca dostępnego na karcie SD.

4. Kliknij **Save** (Zapisz), aby zapisać ustawienia.



Enable

SD Card Available Space

Storage Time Day (1-30)

Note: : After Lite Storage enabled, the unformatted SD card will be formatted automatically.

Save

Figure 6-10 Ustawienia Lite Storage

6.5 Konfiguracja przechowywania w chmurze

Cel:

Zrobione zdjęcia można zapisywać w rejestratorze NVR, który działa w trybie przechowywania w chmurze.

Uwaga: Funkcja przechowywania w chmurze zależy od modelu kamery.

Przed rozpoczęciem pracy:

Upewnij się, że rejestrator NVR jest przełączony w tryb przechowywania w chmurze. Szczegółowe informacje znajdują się w podręczniku użytkownika rejestratora.

Kroki:

1. Przejdź do interfejsu przechowywania w chmurze: **Configuration > Advanced Configuration > Storage > Cloud Storage** (Konfiguracja > Konfiguracja zaawansowana > Pamięć masowa > Przechowywanie w chmurze).
2. Zaznacz pole wyboru **Enable Cloud Storage** (Włącz przechowywanie w chmurze).
3. Wpisz adres IP i port serwera pamięci masowej.
4. Wpisz nazwę użytkownika, hasło i potwierdzenie hasła uwierzytelniania serwera pamięci masowej.



- Aby lepiej chronić prywatność i system przed ryzykami związanymi z bezpieczeństwem, zdecydowanie zalecamy stosowanie silnych haseł dla

wszystkich funkcji i urządzeń sieciowych. Hasło powinno być wybrane przez użytkownika (i zawierać co najmniej 8 znaków, w tym wielkie i małe litery, cyfry i znaki specjalne), aby zwiększyć bezpieczeństwo produktu.

- Instalator i(lub) użytkownik końcowy ponoszą odpowiedzialność za prawidłową konfigurację wszystkich haseł i innych ustawień bezpieczeństwa.
5. Wpisz ID puli pamięci masowej zdjęć serwera.
 6. (Opcja) Możesz kliknąć **Test**, aby przetestować ustawienia pamięci masowej.
 7. Kliknij **Save** (Zapisz), aby zapisać ustawienia.

The screenshot shows a configuration form for cloud storage. At the top, there is a checkbox labeled "Enable Cloud Storage". Below it are several input fields: "Server IP Address" with the value "0.0.0.0", "Server Port" with "6001", "User Name", "Password", "Confirm", and "Picture Storage Pool ID" with "1". A "Test" button is located below the "Picture Storage Pool ID" field. To the right of the main form area, there is a separate "Save" button.

Figure 6-11 Ustawienia przechowywania w chmurze

Chapter 7 Liczenie

Cel:

Funkcja liczenia służy do obliczania liczby obiektów, które wkroczyły w określony skonfigurowany obszar lub z niego wyszły, często stosuje się ją przy obserwacji wejść i wyjść.

Uwagi:

- Funkcję liczenia obsługują niektóre modele kamer z serii innych niż iDS.
- W porównaniu z funkcją liczenia osób obsługiwaną przez kamery iDS, funkcja liczenia w kamerach innych niż iDS nie wymaga ustawień kalibracji.
- Zaleca się instalację kamery pionowo względem ziemi, wówczas funkcja liczenia osób będzie dokładniejsza.

Kroki:

❖ **Konfiguracja liczenia**

1. Przejdź do interfejsu konfiguracji liczenia:

Configuration > Advanced Configuration > Counting (Konfiguracja > Konfiguracja zaawansowana > Liczenie)

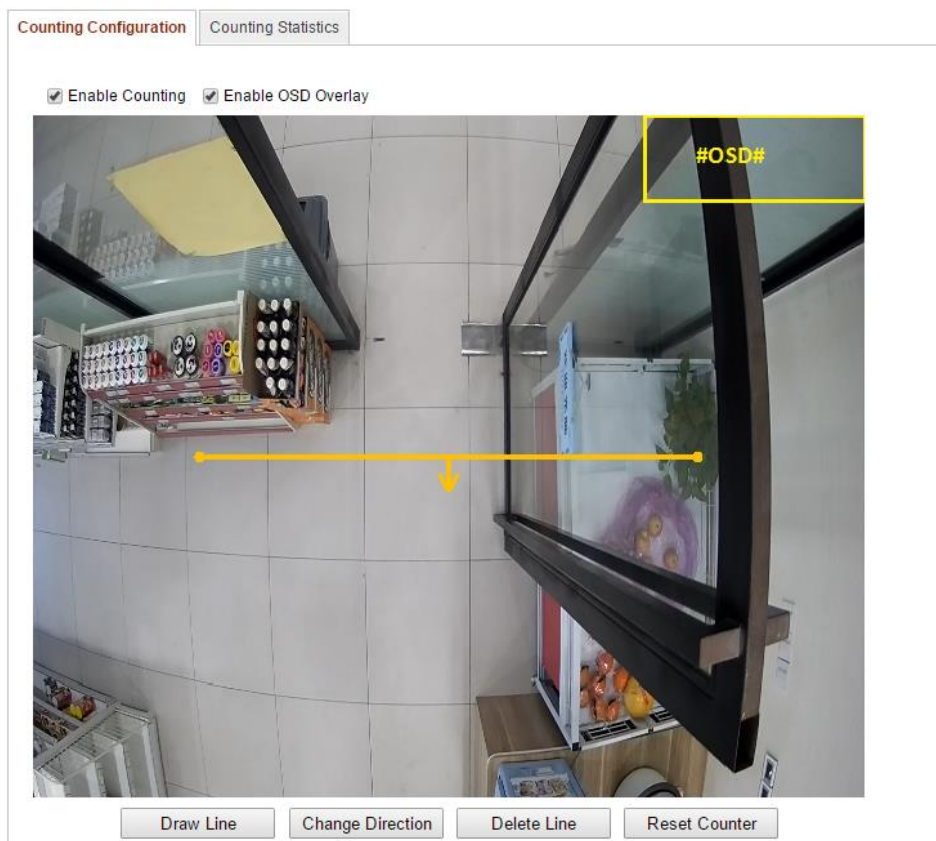


Figure 7-1 Konfiguracja liczenia

2. Wybierz zakładkę **Counting Configuration** (Konfiguracja liczenia), aby ustawić szczegółowe parametry.
3. Zaznacz pole wyboru **Enable Counting** (Włącz liczenie), aby włączyć tę funkcję.
4. (Opcja) Zaznacz pole wyboru **Enable OSD Overlay** (Włącz nakładanie OSD), wówczas na wideo na żywo będzie wyświetlana w czasie rzeczywistym liczba obiektów wkraczających w obszar i go opuszczających. Pozycję OSD można też dostosować do bieżących wymagań.
5. Ustaw linię wykrywania.

Na wideo na żywo można ustawić pomarańczową linię, tzw. linię wykrywania. Wówczas obiekty wkraczające w obszar i go opuszczające, które przechodzą przez tę linię, będą wykrywane i liczone.

- 1) Kliknij **Draw Line** (Narysuj linię), na obrazie pojawi się pomarańczowa linia wykrywania.
- 2) Kliknij i przeciągnij linię wykrywania, aby dostosować jej położenie.
- 3) Kliknij i przeciągnij dwa punkty końcowe linii wykrywania, aby dostosować jej długość.

- 4) Aby usunąć linię wykrywania, kliknij przycisk **Delete Line** (Usuń linię).
Uwaga: Linia wykrywania powinna obejmować całe wejście/wyjście.
6. Kliknij przycisk **Reset Counter** (Resetuj licznik), liczba osób, które weszły i wyszły, zostanie wyzerowana.
7. Kliknij **Edit** (Edytuj), aby ustawić harmonogram uzbrajania.
8. Zaznacz pole wyboru **Notify Surveillance Center** (Powiadom centrum monitoringu), aby ustawić powiązane działanie.
9. Kliknij **Save** (Zapisz), aby zapisać ustawienia.

❖ **Dane statystyczne liczenia**

Kroki:

1. Kliknij **Counting Statistics** (Statystyka liczenia), aby otworzyć interfejs statystyki danych.
2. Wybierz typ raportu, klikając menu rozwijane. Do wyboru są: Daily Report (Raport dzienny), Weekly Report (Raport tygodniowy), Monthly Report (Raport miesięczny) i Annual Report (Raport roczny).
3. Wybierz Statistics Type (Typ statystyki): People Entered (Liczba osób wchodzących) lub People Exited (Liczba osób wychodzących).
Uwaga: Raport dzienny oblicza dane dla wybranej daty; raport tygodniowy oblicza dane dla tygodnia, w którym przypada wybrany dzień; raport miesięczny oblicza dane dla miesiąca, w którym przypada wybrany dzień; raport roczny oblicza dane dla roku, w którym przypada wybrany dzień.
4. Wybierz Statistics Time (Czas statystyki).
5. Kliknij **Counting** (Liczenie), aby obliczyć dane.
6. Wybierz postać eksportu **Statistics Result** (Wynik statystyki): Table (Tabela), Bar Chart (Wykres słupkowy), Line Chart (Wykres liniowy).

Uwaga: W przypadku wyboru wyświetlania statystyk jako tabeli pojawi się przycisk **Export** (Eksport), służący do wyeksportowania danych do pliku Excel.

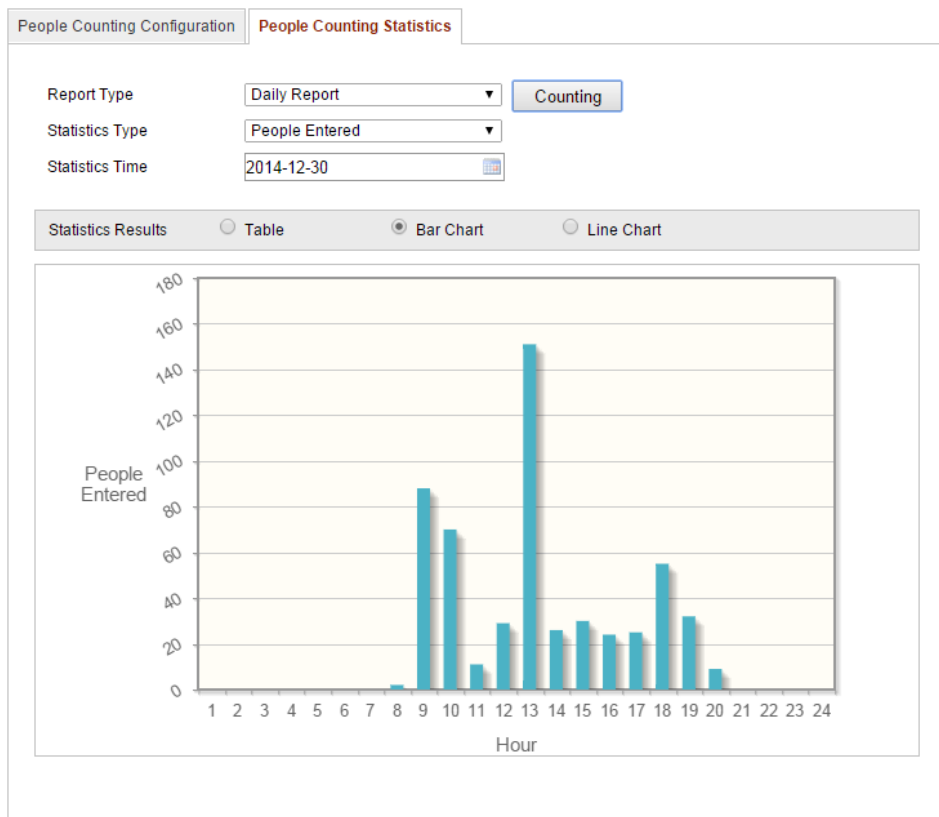


Figure 7-2 Wyniki statystyczne

Chapter 8 Ruch drogowy

Cel:

Dla monitorowania ruchu drogowego są dostępne opcje Vehicle Detection (Wykrywanie pojazdów) i Mixed-traffic Detection (Wykrywanie mieszanego ruchu). W trybie wykrywania pojazdów wykrywane są przejeżdżające pojazdy, możliwe jest zrobienie zdjęcia ich tablicy rejestracyjnej oraz automatyczne rozpoznawanie koloru, logo i innych informacji o pojeździe. W trybie wykrywania mieszanego ruchu wykrywani są piesi oraz pojazdy silnikowe i bez silników, możliwe jest zrobienie zdjęcia obiektu (w przypadku pieszego/pojazdu bez silnika/pojazdu silnikowego bez rejestracji) lub tablicy rejestracyjnej (w przypadku pojazdu silnikowego z rejestracją). Można wysłać sygnał alarmowy, aby powiadomić centrum monitoringu, a także wysłać zrobione zdjęcie do serwera FTP.

Uwaga: Funkcja ruchu drogowego zależy od modelu kamery.

Kroki:

❖ Konfiguracja ustawień wykrywania


1. Wybierz typ wykrywania z listy. Do wyboru są Vehicle Detection (Wykrywanie pojazdów) i Mixed-traffic Detection (Wykrywanie mieszanego ruchu).

Uwaga: Po zmianie rodzaju wykrywania ruchu drogowego należy zrestartować urządzenie, aby aktywować nowe ustawienia.

2. Zaznacz pole wyboru **Enable** (Włącz), aby włączyć wybraną funkcję wykrywania.
3. Wybierz numer pasa z odpowiedniej listy rozwijanej. Można wybrać maks. 4 pasy.
4. Kliknij i przesuń linię pasa, by ustawić jej pozycję, lub kliknij i przeciągnij koniec linii, aby dopasować długość i kąt nachylenia linii.
5. Wyreguluj współczynnik powiększenia kamery tak, aby wielkość pojazdu na obrazie była zbliżona do czerwonej ramki. Można ustawiać tylko położenie czerwonej ramki.

Uwaga: Dla każdego pasa można rejestrować tylko 1 tablicę rejestracyjną

jednocześnie.

6. Wybierz z listy rozwijanej skrót prowincji/stanu, jeśli nie można rozpoznać atrybutu tablicy rejestracyjnej.
7. Ustaw harmonogram uzbrajania dla wykrywania pojazdu.
 - 1) Aby wyedytować harmonogram uzbrajania, kliknij przycisk **Edit** (Edytuj).
 - 2) Wybierz dzień, w którym ma zostać ustawiony harmonogram uzbrajania.
 - 3) Kliknij , aby ustawić okres harmonogramu uzbrajania.
 - 4) (Opcja) Po ustawieniu harmonogramu uzbrajania możesz kliknąć przycisk **Copy** (Kopiuj), aby skopiować harmonogram na inne dni.
 - 5) Kliknij **OK**, aby zapisać ustawienia.

Uwaga: Okresy nie mogą się nakładać.

8. Zaznacz pole wyboru, aby wybrać powiązaną metodę. Do wyboru są: Notify surveillance center (Powiadom centrum monitoringu) i Upload to FTP (Wyślij do FTP).

Notify Surveillance Center (Powiadom centrum monitoringu): Wyślij wyjątek lub sygnał alarmu do oprogramowania do zdalnego zarządzania, gdy wystąpi zdarzenie.

Upload to FTP (Wyślij do FTP): Po wyzwoleniu alarmu zrób zdjęcie i wyślij je do serwera FTP. Zapisz też obraz na lokalnej karcie SD lub podłączonym dysku NAS.

9. Kliknij **Save** (Zapisz), aby zapisać ustawienia.

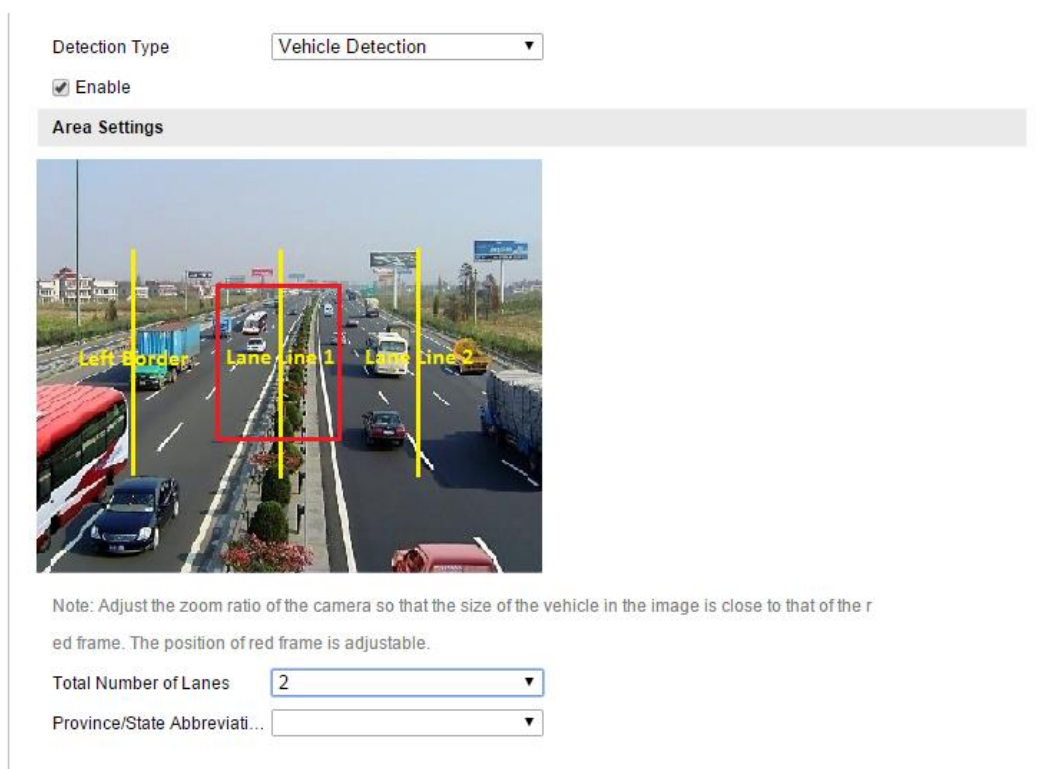



Figure 8-1 Konfiguracja wykrywania pojazdu

❖ Konfiguracja wysyłanego zdjęcia

1. Ustaw jakość zdjęcia.

Można podać Picture Quality (Jakość zdjęcia) lub Picture Size (Rozmiar zdjęcia).

2. (Opcja) Włącz i wyedytuj tekst nakładany na wysyłanym zdjęciu.

Możesz ustawić kolor czcionki i tła, klikając ikonę  i klikając żądany kolor w palecie, która się wyświetli.

3. Wybierz informacje stanowiące nakładany tekst, takie jak nr kamery, informacje o kamerze, nr urządzenia, godzina rejestracji, nr tablicy rejestracyjnej, kolor pojazdu itp. Możesz też kliknąć strzałki W górę i W dół, aby dopasować sekwencję tekstu.
4. Kliknij **Save** (Zapisz), aby aktywować ustawienia.

Picture Quality[1-100] 80
 Picture Size[64-2048k] 1024
 Enable Text Overlay
 Font Color
 Background Color
Text Overlay
 Camera No. Camera Info. Device No. Capture Time Plate No.
 Vehicle Color Type Vehicle Logo

Type		
Camera No.		↑ ↓
Camera Info.		↑ ↓
Device No.		↑ ↓
Capture Time		↑ ↓
Plate No.		↑ ↓
Vehicle Color		↑ ↓
Type		↑ ↓
Vehicle Logo		↑ ↓

Figure 8-2 Ustawienia wysyłania zdjęć

❖ **Konfiguracja treści nakładanego tekstu**

1. W odpowiednim polu tekstowym wyedytuj treść: nr kamery, informacje o kamerze, informacje o urządzeniu.
2. (Opcja) Włącz i wyedytuj tekst nakładany na wysyłanym zdjęciu.
3. Kliknij przycisk **Save** (Zapisz), aby aktywować ustawienia.

Device No.
 Camera No.
 Camera Info.

Figure 8-3 Ustawienia nakładanych treści

Chapter 9 Odtwarzanie

Cel:

W tej sekcji objaśniono, jak wyświetlać nagrane zdalnie pliki wideo zapisane na dyskach sieciowych lub kartach SD.

Kroki:

1. Kliknij **Playback** (Odtwórz) na pasku menu, aby przejść do interfejsu odtwarzania.

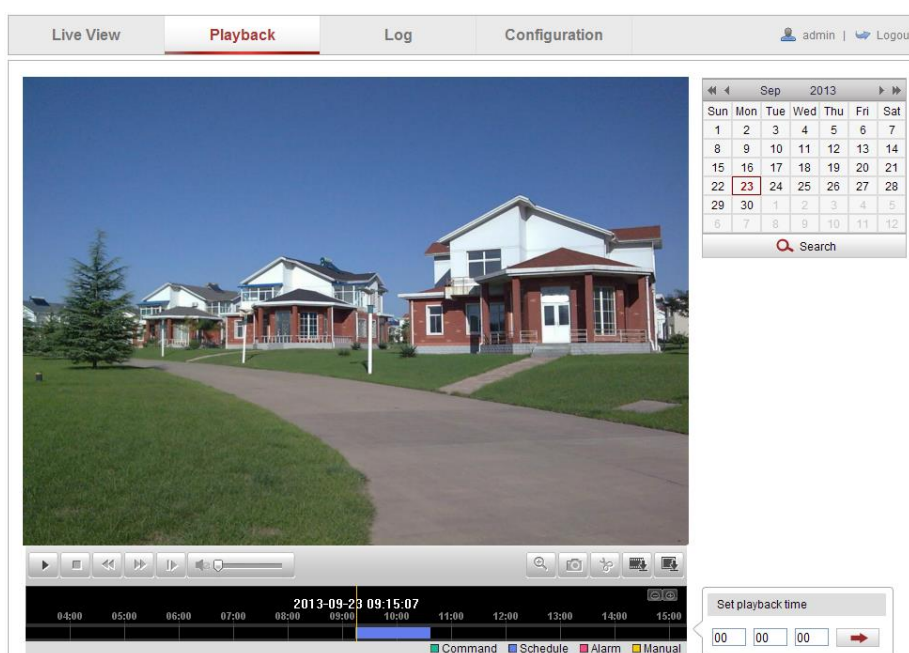


Figure 9-1 Interfejs odtwarzania

2. Wybierz datę i kliknij **Search** (Szukaj).

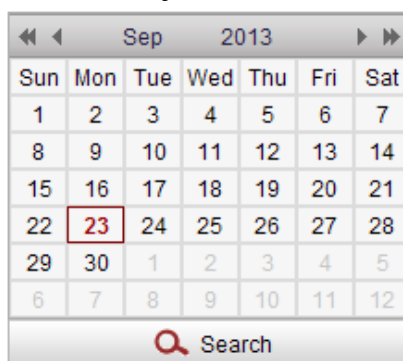



Figure 9-2 Wyszukiwanie wideo

3. Kliknij , aby odtworzyć pliki wideo znalezione pod tą datą.

Do sterowania procesem odtwarzania można użyć paska narzędzi na dole interfejsu odtwarzania.



Figure 9-3 Pasek narzędzi odtwarzania

Table 9-1 Opis przycisków

Przycisk	Działanie	Przycisk	Działanie
	Odtwarzaj		Zrób zdjęcie
	Pauza		Rozpocznij/zatrzymaj tworzenie klipów wideo
	Zatrzymaj		Włączenie dźwięku i regulacja głośności/wyciszenie
	Zwolnij		Pobierz pliki wideo
	Przyspiesz		Pobierz zrobione zdjęcia
	Odtwarzaj poklatkowo		Włącz/wyłącz zoom cyfrowy

Uwaga: W interfejsie konfiguracji lokalnej możesz wybrać lokalne ścieżki plików dla pobranych plików wideo i zdjęć. Szczegółowe informacje znajdują się w *Sekcji 6.1*. Przeciągnij pasek postępu myszą, aby ustalić dokładny punkt odtwarzania. Możesz też wpisać czas i kliknąć , aby zlokalizować punkt odtwarzania w polu **Set playback time** (Ustaw czas odtwarzania). Możesz też kliknąć , aby oddalić/przybliżyć pasek postępu.

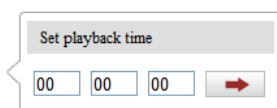


Figure 9-4 Ustawianie czasu odtwarzania



Figure 9-5 Pasek postępu

Różne kolory wideo na pasku postępu odpowiadają różnym typom wideo.

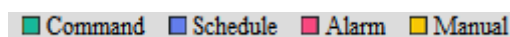


Figure 9-6 Typy wideo

Chapter 10 Przeszukiwanie dziennika

Cel:

Czynności obsługi, alarmy, wyjątki i informacje o kamerze można przechowywać w plikach dziennika. Można też w razie potrzeby eksportować pliki dziennika.

Przed rozpoczęciem pracy:

Skonfiguruj sieciową pamięć masową dla kamery lub włóż do kamery kartę SD.

Kroki:

1. Kliknij **Log** (Dziennik) na pasku menu, aby otworzyć interfejs przeszukiwania dziennika.

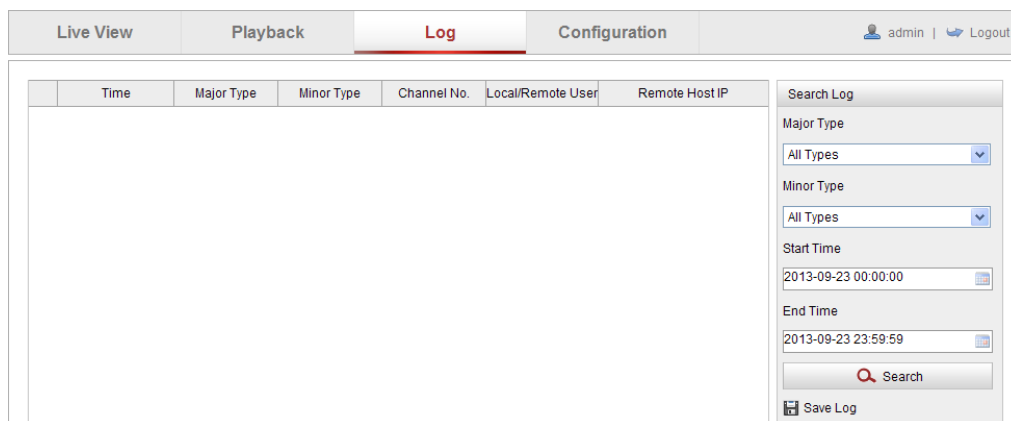
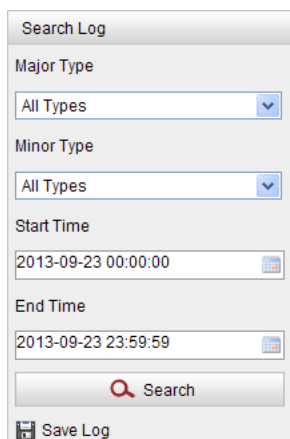


Figure 10-1 Interfejs przeszukiwania dziennika

2. Ustaw warunki przeszukiwania dziennika, aby zawęzić wyniki wyszukiwania, takie jak Major Type (typ główny), Minor Type (typ mniejszej wagi, podtyp), Start Time (czas rozpoczęcia), End Time (czas zakończenia).
3. Kliknij **Search** (Szukaj), aby przeszukiwać pliki dziennika. Pasujące pliki dziennika zostaną wyświetlone w interfejsie **Log** (Dziennik).



The screenshot shows a 'Search Log' window with the following elements:

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

Figure 10-2 Przeszukiwanie dziennika

4. Aby wyeksportować pliki dziennika, kliknij **Save log** (Zapisz dziennik) w celu zapisania plików dziennika na komputerze.

Chapter 11 Inne

11.1 Zarządzanie kontami użytkowników

Przejdź do interfejsu zarządzania użytkownikami:

Configuration > Basic Configuration > Security > User (Konfiguracja > Konfiguracja podstawowa > Bezpieczeństwo > Użytkownik)

Lub **Configuration > Advanced Configuration > Security > User (Konfiguracja > Konfiguracja zaawansowana > Bezpieczeństwo > Użytkownik)**

No.	User Name	Level
1	admin	Administrator
2	Test	Operator

Figure 11-1 Informacje o użytkowniku

- **Dodawanie użytkownika**

Użytkownik *admin* ma domyślnie wszystkie uprawnienia, może tworzyć/modyfikować/usuwać inne konta.

Użytkownika *admin* nie można usunąć, można jedynie zmienić hasło *admin*.

Kroki:

1. Kliknij **Add** (Dodaj), aby dodać użytkownika.
2. Wpisz **User Name** (Nazwa użytkownika), wybierz **Level** (Poziom) i wpisz **Password** (Hasło).

Uwagi:

- Można stworzyć maks. 31 użytkowników.
- Różne poziomy użytkownika mają różne uprawnienia. Do wyboru są operator i użytkownik.



Aby lepiej chronić prywatność i system przed ryzykami związanymi z bezpieczeństwem, zdecydowanie zalecamy stosowanie silnych haseł dla wszystkich funkcji i urządzeń sieciowych. Hasło powinno być wybrane przez

użytkownika (i zawierać co najmniej 8 znaków, w tym wielkie i małe litery, cyfry i znaki specjalne), aby zwiększyć bezpieczeństwo produktu.

- Instalator i(lub) użytkownik końcowy ponoszą odpowiedzialność za prawidłową konfigurację wszystkich haseł i innych ustawień bezpieczeństwa.
3. W polu **Basic Permission** (Podstawowe uprawnienie) i polu **Camera Configuration** (Konfiguracja kamery) zaznacz uprawnienia dla nowego użytkownika lub usuń ich zaznaczenie.
 4. Kliknij **OK**, aby zakończyć dodawanie użytkownika.

Figure 11-2 Dodawanie użytkownika

- **Modyfikacja użytkownika**

Kroki:

1. Kliknij lewym przyciskiem, aby wybrać użytkownika, i kliknij **Modify** (Modyfikuj).
2. Zmodyfikuj **User Name** (Nazwa użytkownika), **Level** (Poziom) lub **Password** (Hasło).
3. W polu **Basic Permission** (Podstawowe uprawnienie) i polu **Camera**

Configuration (Konfiguracja kamery) zaznacz uprawnienia lub usuń ich zaznaczenie.

4. Kliknij **OK**, aby zakończyć modyfikację użytkownika.

Modify user

User Name: test1

Level: Operator

Password: ●●●●●●

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

Confirm: ●●●●●●

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

OK Cancel

Figure 11-3 Modyfikacja użytkownika

- **Usuwanie użytkownika**

Kroki:

1. Kliknij, aby wybrać użytkownika do usunięcia, i kliknij **Delete** (Usuń).
2. W oknie dialogowym, które się wyświetli, kliknij **OK**, aby usunąć użytkownika.

11.2 Autoryzacja

Cel:

Można dodatkowo zabezpieczyć strumień danych podglądu na żywo.

Kroki:

1. Przejdź do interfejsu autoryzacji: Configuration> Advanced Configuration> Security > Authentication (Konfiguracja > Konfiguracja zaawansowana > Bezpieczeństwo > Autoryzacja)

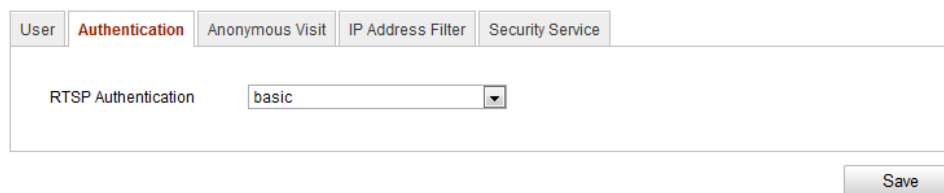


Figure 11-4 Autoryzacja RTSP

- Wybierz typ **Authentication** (Autoryzacja) RTSP: **basic** (podstawowa) lub **disable** (wyłącz) z listy rozwijanej, aby włączyć lub wyłączyć autoryzację RTSP.

Uwaga: Po wyłączeniu autoryzacji RTSP każdy będzie miał dostęp do strumienia wideo przy użyciu protokołu RTSP za pośrednictwem adresu IP.

- Kliknij **Save** (Zapisz), aby zapisać ustawienia.

11.3 Anonymous Visit (Wizyta anonimowa)

Po włączeniu tej funkcji każdy, nawet jeśli nie ma nazwy użytkownika i hasła, będzie mógł oglądać obraz z kamery.

Uwaga: Użytkownik anonimowy ma dostęp wyłącznie do podglądu na żywo.

Kroki:

- Przejdź do interfejsu wizyty anonimowej:

Configuration > Advanced Configuration > Security > Anonymous Visit
(Konfiguracja > Konfiguracja zaawansowana > Bezpieczeństwo > Wizyta anonimowa)

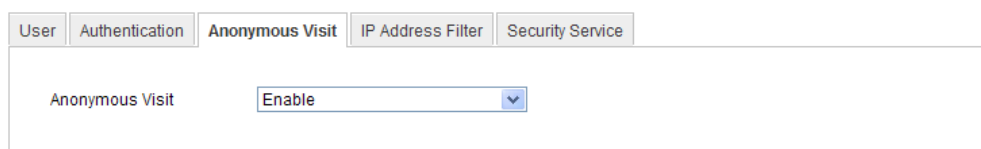


Figure 11-5 Wizyta anonimowa

- Ustaw uprawnienie do **Anonymous Visit** (Wizyta anonimowa) na **Enable** (Włącz) lub **Disable** (Wyłącz) na liście rozwijanej, aby umożliwić wizyty anonimowe lub ich nie umożliwiać.

- Kliknij **Save** (Zapisz), aby zapisać ustawienia.

Po następnym zalogowaniu będzie dostępne pole wyboru **Anonymous**

(Anonimowe).

The screenshot shows a login form with the following elements:

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

Figure 11-6 Interfejs logowania z polem wyboru Anonimowe

4. Zaznacz pole wyboru **Anonymous** (Anonimowe) i kliknij **Login** (Zaloguj się).

Dzięki zezwoleniu na anonimowy dostęp do podglądu na żywo inni użytkownicy mogą go oglądać, nie podając danych logowania. Dlatego, przy zezwoleniu na anonimowy dostęp do podglądu na żywo, niewłaściwe znaczenie ma konfiguracja pola widzenia kamery w taki sposób, aby nie naruszać prywatności osób, które mogłyby być zarejestrowane bez autoryzacji.

Ze względu na naruszający prywatność charakter monitoringu wideo, nie jest on odpowiedni w miejscach, w których do prywatności przykładana jest większą wagę.

11.4 Filtr adresów IP

Cel:

Ta funkcja rozszerza możliwości kontroli dostępu.

Kroki:

1. Przejdź do interfejsu filtra adresów IP:

Configuration > Advanced Configuration > Security > IP Address Filter
(Konfiguracja > Konfiguracja zaawansowana > Bezpieczeństwo > Filtr adresów IP)

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

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

No.	IP
1	172.6.23.2

Figure 11-7 Interfejs filtru adresów IP

2. Zaznacz pole wyboru **Enable IP Address Filter** (Włącz filtr adresów IP).
3. Wybierz typ adresów IP z listy rozwijanej, do wyboru są **Forbidden** (Zabroniony) i **Allowed** (Dopuszczony).
4. Ustaw listę filtru adresów IP.
 - Dodaj adres IP

Kroki:

- (1) Kliknij **Add** (Dodaj), aby dodać IP.
- (2) Wpisz adres IP.

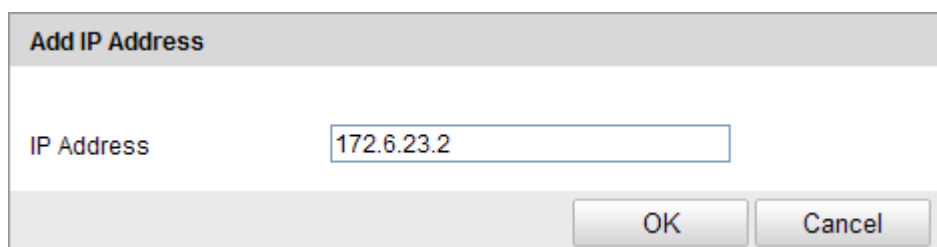


Figure 11-8 Dodawanie IP

- (3) Kliknij **OK**, aby zakończyć dodawanie.

- Zmodyfikuj adres IP

Kroki:

- (1) Kliknij lewym przyciskiem adres IP na liście filtru i kliknij **Modify** (Modyfikuj).
- (2) Zmodyfikuj adres IP w polu tekstowym.

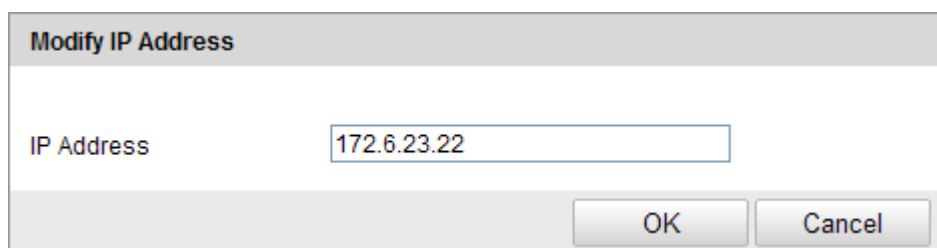


Figure 11-9 Modyfikacja IP

- (3) Kliknij **OK**, aby zakończyć modyfikację.

- Usuń adres IP

Kliknij lewym przyciskiem adres IP na liście filtru i kliknij **Delete** (Usuń).

- Skasuj wszystkie adresy IP

Kliknij **Clear** (Usuń), aby usunąć wszystkie adresy IP.

5. Kliknij **Save** (Zapisz), aby zapisać ustawienia.

11.5 Funkcje bezpieczeństwa

Aby umożliwić zdalne logowanie i zwiększyć bezpieczeństwo komunikacji danych, kamera jest wyposażona w funkcje bezpieczeństwa, ułatwiające usługę.

Kroki:

1. Przejdź do **Configuration > Advanced configuration > Security > Security Service** (Konfiguracja > Konfiguracja zaawansowana > Bezpieczeństwo > Funkcje bezpieczeństwa), aby otworzyć interfejs konfiguracji funkcji bezpieczeństwa.

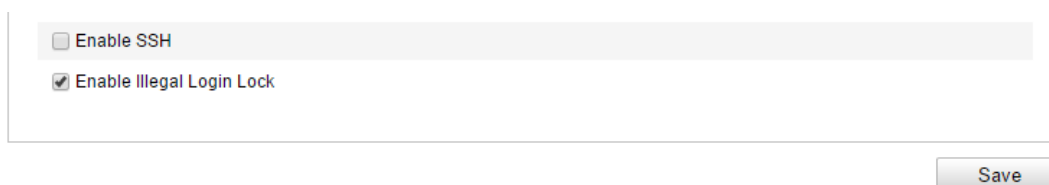


Figure 11-10 Funkcje bezpieczeństwa

2. Zaznacz pole wyboru **Enable SSH** (Włącz SSH), aby zapewnić bezpieczeństwo przesyłu danych, usuń zaznaczenie, aby wyłączyć SSH.

3. Zaznacz pole wyboru **Enable Illegal Login Lock** (Włącz blokadę nieuprawnionego logowania), wówczas w przypadku wpisania nieprawidłowej nazwy użytkownika lub hasła 5 razy pod rząd urządzenie zostanie zablokowane.

Uwaga: Jeśli urządzenie jest zablokowane, możesz spróbować się do niego zalogować po 30 minutach lub zrestartować je przed ponowną próbą.

11.6 Wyświetlanie informacji o urządzeniu

Przejdź do interfejsu informacji o urządzeniu: **Configuration > Basic Configuration > System > Device Information** (Konfiguracja > Konfiguracja podstawowa > System > Informacje o urządzeniu) lub **Configuration > Advanced Configuration > System > Device Information** (Konfiguracja > Konfiguracja zaawansowana > System > Informacje o urządzeniu).

W interfejsie **Device Information** (Informacje o urządzeniu) możesz wyedytować nazwę urządzenia.

Wyświetlane są inne informacje o kamerze sieciowej, takie jak Model (model), Serial No. (nr seryjny), Firmware Version (wersja oprogramowania układowego), Encoding Version (wersja kodowania), Number of Channels (liczba kanałów), Number of HDDs (liczba dysków twardych), Number of Alarm Input (liczba wejść alarmowych) i Number of Alarm Output (liczba wyjść alarmowych). W tym menu nie można ich zmienić. Stanowią one dane referencyjne, które w przyszłości mogą pomóc w konserwacji lub modyfikacji.

Basic Information	
Device Name	<input type="text" value="IP CAMERA"/>
Device No.	<input type="text" value="88"/>
Model	XX-XXXXXXXX
Serial No.	XXXXXXXXXXXXXXXXXXXX
Firmware Version	V5.1.0 build 131104
Encoding Version	V5.5 build 131104
Number of Channels	1
Number of HDDs	1
Number of Alarm Input	1
Number of Alarm Output	1

Figure 11-11 Informacje o urządzeniu

11.7 Konserwacja

11.7.1 Ponowne uruchamianie kamery

Kroki:

1. Przejdź do interfejsu konserwacji:

Configuration > Basic Configuration > System > Maintenance (Konfiguracja > Konfiguracja podstawowa > System > Konserwacja)

Lub **Configuration > Advanced Configuration > System > Maintenance (Konfiguracja > Konfiguracja zaawansowana > System > Konserwacja):**

2. Kliknij **Reboot** (Uruchom ponownie), aby ponownie uruchomić kamerę.

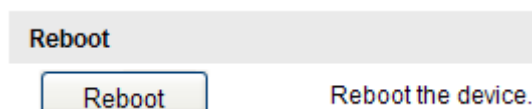


Figure 11-12 Ponowne uruchamianie urządzenia

11.7.2 Przywracanie ustawień domyślnych

Kroki:

1. Przejdź do interfejsu konserwacji:

Configuration > Basic Configuration > System > Maintenance (Konfiguracja > Konfiguracja podstawowa > System > Konserwacja)

Lub **Configuration > Advanced Configuration > System > Maintenance (Konfiguracja > Konfiguracja zaawansowana > System > Konserwacja):**

2. Kliknij **Restore** (Przywróć) lub **Default** (Domyślne), aby przywrócić ustawienia domyślne.

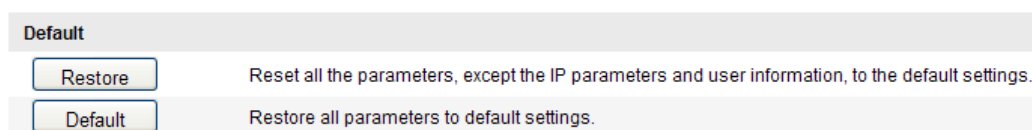


Figure 11-13 Przywracanie ustawień domyślnych

Uwaga: Po przywróceniu ustawień domyślnych przywracany jest także domyślny adres IP, należy o tym pamiętać.

11.7.3 Eksport/import pliku konfiguracji

Cel:

Pliku konfiguracji używa się do wsadowej konfiguracji kamer, co upraszcza kroki konfiguracji wielu kamer naraz.

Kroki:

1. Przejdź do interfejsu konserwacji: **Configuration > Basic Configuration > System > Maintenance (Konfiguracja > Konfiguracja podstawowa > System > Konserwacja)** lub **Configuration > Advanced Configuration > System >**

Maintenance (Konfiguracja > Konfiguracja zaawansowana> System > Konserwacja).

2. Kliknij **Export** (Eksport), aby wyeksportować bieżący plik konfiguracji i zapisać go na innym urządzeniu.
3. Kliknij **Browse** (Przeglądaj), aby wybrać zapisany plik konfiguracji, i kliknij **Import**, aby zaimportować plik konfiguracji.

Uwaga: Po zaimportowaniu pliku konfiguracji należy ponownie uruchomić kamerę.

4. Kliknij **Export** (Eksport) i ustaw ścieżkę zapisu, aby zapisać plik konfiguracji w lokalnej pamięci masowej.

The screenshot shows two sections of a web interface. The top section is titled 'Import Config. File' and contains a text input field labeled 'Config File' with the value 'F:\12', a 'Browse' button, and an 'Import' button. Below this is a 'Status' label. The bottom section is titled 'Export Config. File' and contains an 'Export' button.

Figure 11-14 Import/eksport pliku konfiguracji

11.7.4 Aktualizacja systemu

Kroki:

1. Przejdź do interfejsu konserwacji: Configuration > Basic Configuration> System > Maintenance (Konfiguracja > Konfiguracja podstawowa > System > Konserwacja) lub Configuration>Advanced Configuration> System > Maintenance (Konfiguracja > Konfiguracja zaawansowana > System > Konserwacja).
2. Wybierz oprogramowanie układowe lub katalog, który je zawiera, aby znaleźć plik aktualizacji.

Firmware (Oprogramowanie układowe): Podaj dokładną ścieżkę do pliku aktualizacji.

Firmware Directory (Katalog oprogramowania układowego): Wystarczy podać nazwę katalogu, w którym znajduje się plik aktualizacji.

3. Kliknij **Browse** (Przeglądaj), aby wybrać lokalny plik aktualizacji, i kliknij **Upgrade** (Aktualizuj), aby rozpocząć zdalną aktualizację.



Figure 11-15 Zdalna aktualizacja

Uwaga: Proces aktualizacji trwa 1~10 minut. W tym czasie nie odłączaj zasilania kamery, po aktualizacji kamera automatycznie uruchomi się ponownie.

11.8 Ustawienia RS-232

Portu RS-232 można używać na dwa sposoby:

- Konfiguracja parametrów: Podłącz komputer do kamery przez port szeregowy. Można skonfigurować parametry urządzenia przy użyciu programu takiego, jak HyperTerminal. Parametry portu szeregowego muszą być takie same jak parametry portu szeregowego kamery.
- Kanał transparentny: Podłącz urządzenie szeregowe bezpośrednio do kamery. Urządzenie szeregowe będzie sterowane zdalnie z komputera w sieci.

Kroki:

1. Przejdź do interfejsu ustawień portu RS-232:

Configuration > Advanced Configuration > System > RS232 (Konfiguracja > Konfiguracja zaawansowana > System > RS232)

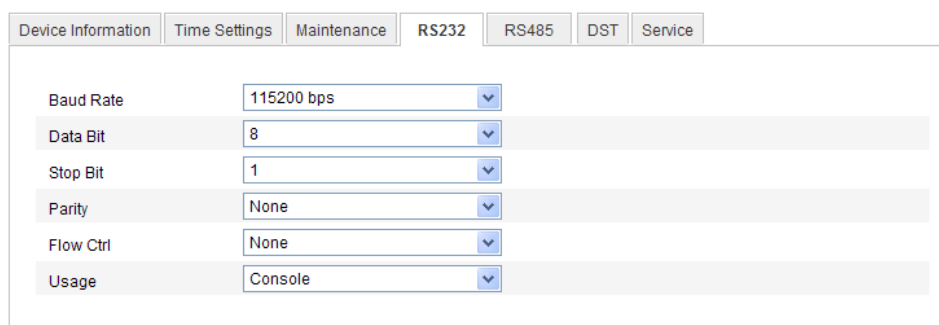


Figure 11-16 Ustawienia RS-232

Uwaga: Aby podłączyć kamerę przez port RS-232, parametry RS-232 powinny być identyczne jak parametry skonfigurowane w tym miejscu.

2. Kliknij **Save** (Zapisz), aby zapisać ustawienia.

11.9 Ustawienia RS-485

Cel:

Portu RS-485 używa się do sterowania funkcjami PTZ kamery. Aby można było sterować modulem PTZ, najpierw należy skonfigurować parametry PTZ.

Kroki:

1. Przejdź do interfejsu ustawień portu RS-485:

Configuration > Advanced Configuration > System > RS485 (Konfiguracja > Konfiguracja zaawansowana > System > RS485)

Field	Value
Baud Rate	9600 bps
Data Bit	8
Stop Bit	1
Parity	None
Flow Ctrl	None
PTZ Protocol	PELCO-D
PTZ Address	0

Figure 11-17 Ustawienia RS-485

2. Ustaw parametry RS-485 i kliknij **Save** (Zapisz), aby zapisać ustawienia.

Domyślnie Baud Rate (Szybkość transmisji) to 9600 bps, Data Bit (Bit danych) to 8, Stop Bit (Bit stopu) to 1, a Parity (Parzystość) i Flow Control (Kontrola przepływu) to None (Brak).

Uwaga: Parametry szybkości transmisji, protokołu PTZ i adresu PTZ powinny być identyczne jak parametry kamery PTZ.

11.10 Ustawienia usług

Przejdź do **Configuration > Advanced Configuration > System > Service** (Konfiguracja > Konfiguracja zaawansowana > System > Usługi, aby otworzyć interfejs ustawień usług.

Ustawienia usług odnoszą się do usług sprzętowych obsługiwanych przez kamerę i

różnią się w zależności od modelu kamery.

W przypadku kamer z obsługą diody podczerwieni, ABF (Auto Back Focus), automatycznego usuwania zamgleń lub diody stanu można wejść do menu usług sprzętowych i wybrać, czy włączyć, czy wyłączyć daną usługę, zależnie od potrzeb.

Załącznik

Załącznik 1 – Wprowadzenie do oprogramowania SADP

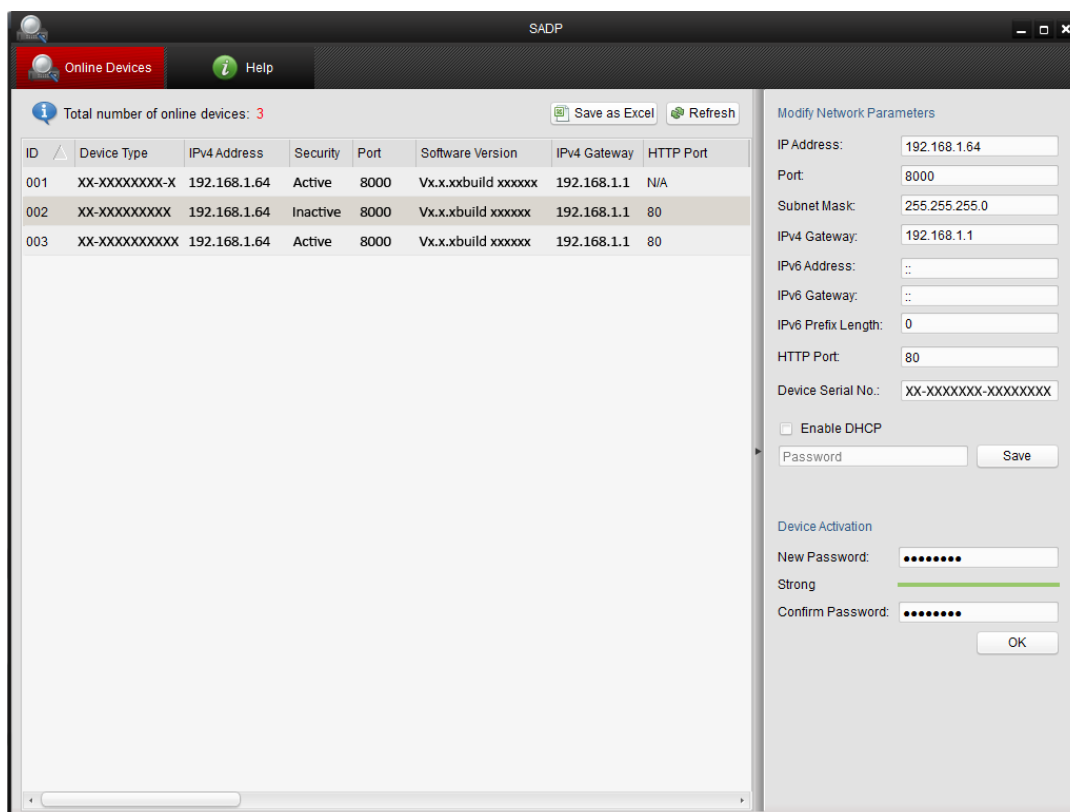
● Opis SADP

SADP (Search Active Devices Protocol – protokół wyszukiwania aktywnych urządzeń) to narzędzie wyszukiwania urządzeń online, które jest łatwe w obsłudze i nie wymaga instalacji. Wyszukuje aktywne urządzenia online w podsieci i wyświetla o nich informacje. Przy użyciu tego oprogramowania można też zmodyfikować podstawowe informacje sieciowe urządzeń.

● Wyszukiwanie aktywnych urządzeń w trybie online

◆ Automatyczne wyszukiwanie urządzeń w trybie online

Po uruchomieniu oprogramowanie SADP automatycznie, co 15 sekund, wyszukuje urządzenia dostępne w podsieci, do której jest podłączony komputer PC. Wyświetla łączną liczbę znalezionych urządzeń i informacje o nich w interfejsie urządzeń w trybie online. Zostaną wyświetlone takie informacje, jak typ urządzenia, adres IP, nr portu itp.

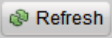


Ilustracja A.1.1 Wyszukiwanie urządzeń w trybie online





Uwaga:

Urządzenie można wyszukać i wyświetlić na liście po 15 s od przejścia w tryb online, zostanie usunięte z listy po 45 s od przejścia w tryb offline.

◆ Ręczne wyszukiwanie urządzeń w trybie online

Można też kliknąć , aby ręcznie odświeżyć listę urządzeń w trybie online. Nowo wyszukane urządzenia zostaną dodane do listy.



Możesz kliknąć  lub  na każdym nagłówku kolumny, aby uporządkować informacje; możesz kliknąć , aby rozszerzyć tabelę urządzeń i ukryć panel parametrów sieciowych z prawej strony, lub kliknąć , aby wyświetlić panel parametrów sieciowych.

● Modyfikacja parametrów sieciowych

Kroki:

1. Wybierz modyfikowane urządzenie z listy urządzeń, parametry sieciowe urządzenia wyświetlą się w panelu **Modify Network Parameters** (Zmodyfikuj parametry sieciowe) z prawej strony.

2. Zmodyfikuj parametry sieciowe, które można zmienić, np. adres IP i numer portu.
3. Wprowadź hasło konta administratora urządzenia w polu **Password** (Hasło) i kliknij , aby zapisać zmiany.



- *Aby lepiej chronić prywatność i system przed ryzykami związanymi z bezpieczeństwem, zdecydowanie zalecamy stosowanie silnych haseł dla wszystkich funkcji i urządzeń sieciowych. Hasło powinno być wybrane przez użytkownika (i zawierać co najmniej 8 znaków, w tym wielkie i małe litery, cyfry i znaki specjalne), aby zwiększyć bezpieczeństwo produktu.*
- *Instalator i(lub) użytkownik końcowy ponoszą odpowiedzialność za prawidłową konfigurację wszystkich haseł i innych ustawień bezpieczeństwa.*

Modify Network Parameters

IP Address:

Port:

Subnet Mask:

IPv4 Gateway:

IPv6 Address:

IPv6 Gateway:

IPv6 Prefix Length:

Serial No.:

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

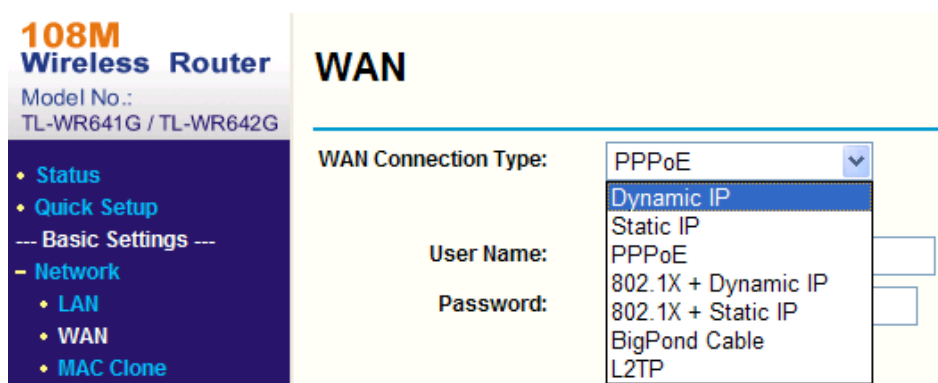
Ilustracja A.1.2 Modyfikacja parametrów sieciowych

Załącznik 2 – Mapowanie portów

Przedstawione ustawienia dotyczą routera TP-LINK (TL-WR641G). Ustawienia różnią się w zależności od modelu routera.

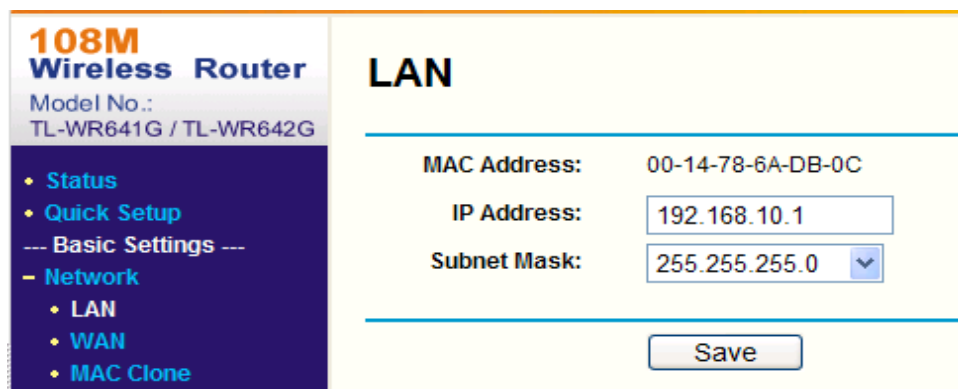
Kroki:

1. Wybierz **WAN connection type** (Typ połączenia WAN), jak pokazano poniżej:



Ilustracja A.2.1 Wybór typu połączenia WAN

2. Ustaw parametry **LAN** routera, jak na poniższej ilustracji, takie jak adres IP i maska podsieci.



Ilustracja A.2.2 Ustawienia parametrów LAN

3. Ustaw mapowanie portów w wirtualnych serwerach funkcji **Forwarding** (Przekierowywanie). Domyślnie kamera używa portów 80, 8000 i 554. Można zmienić te wartości przy użyciu przeglądarki internetowej lub oprogramowania klienta.

Przykład:

Gdy kamery są podłączone do tego samego routera, można skonfigurować porty

jednej kamery jako 80, 8000, 554, 8200 z adresem IP 192.168.1.23, a porty innej kamery jako 81, 8001, 555, 8201 z IP 192.168.1.24. Wykonaj kroki przedstawione poniżej:

Kroki:

1. Wykorzystaj powyższe ustawienia, aby zmapować porty 80, 8000, 554 i 8200 dla kamery sieciowej z adresem 192.168.1.23
2. Zmapuj porty 81, 8001, 555 i 8201 dla kamery sieciowej z adresem 192.168.1.24
3. Włącz wszystkie protokoły (**ALL**) lub tylko protokół **TCP**.
4. Zaznacz pole wyboru **Enable** (Włącz) i kliknij **Save** (Zapisz), aby zapisać ustawienia.

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

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

Virtual Servers

ID	Service Port	IP Address	Protocol	Enable
1	80	192.168.10.23	ALL	<input checked="" type="checkbox"/>
2	8000	192.168.10.23	ALL	<input checked="" type="checkbox"/>
3	554	192.168.10.23	ALL	<input checked="" type="checkbox"/>
4	8200	192.168.10.23	ALL	<input checked="" type="checkbox"/>
5	81	192.168.10.24	ALL	<input checked="" type="checkbox"/>
6	8001	192.168.10.24	ALL	<input checked="" type="checkbox"/>
7	555	192.168.10.24	ALL	<input checked="" type="checkbox"/>
8	8201	192.168.10.24	ALL	<input checked="" type="checkbox"/>

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

Previous Next Clear All Save

Ilustracja A.2.3 Mapowanie portów

Uwaga: Port kamery sieciowej nie może być w konflikcie z innymi portami. Na przykład, port 80 w niektórych routerach może służyć do zarządzania przez sieć. Zmień port kamery, jeśli jest taki sam jak port zarządzania.



First Choice for Security Professionals