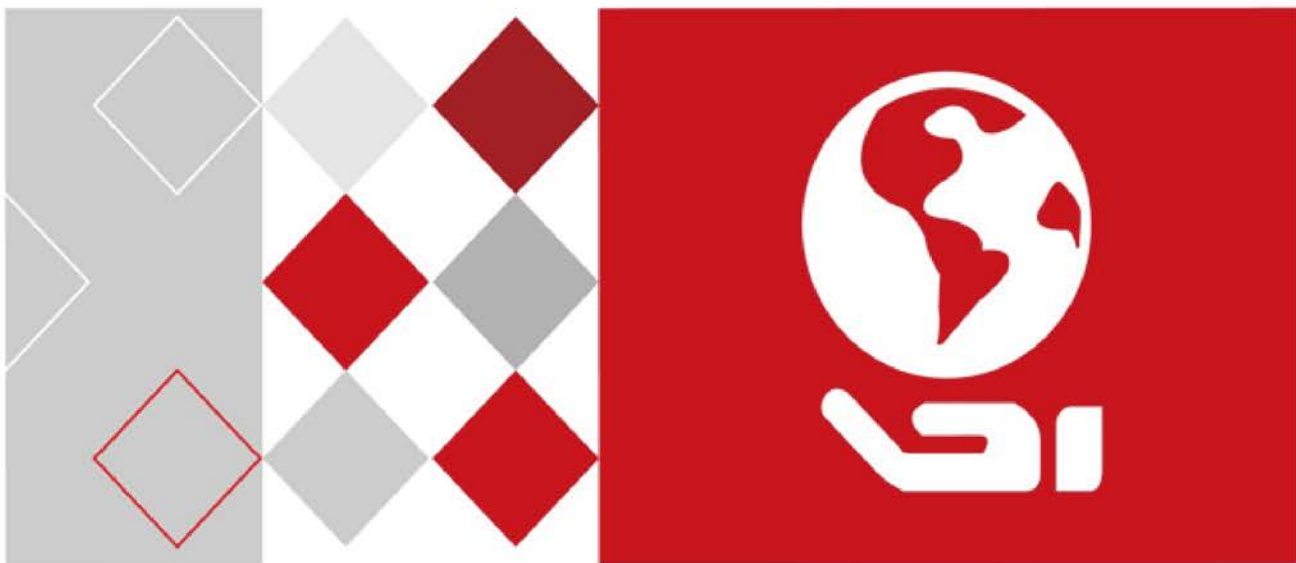


**HIKVISION**



**Termowizyjna tubowa  
kamera sieciowa**

**Podręcznik użytkownika**

UD05094B-A

## **Podręcznik użytkownika**

COPYRIGHT ©2017 Hangzhou Hikvision Digital Technology Co., Ltd.

### **WSZELKIE PRAWA ZASTRZEŻONE.**

Wszelkie zamieszczone w niniejszym podręczniku informacje, takie jak tekst, zdjęcia i grafika, są własnością firmy Hangzhou Hikvision Digital Technology Co., Ltd. lub jej podmiotów stowarzyszonych (zwanymi dalej „Hikvision”). Zabronione jest powielanie, modyfikowanie, tłumaczenie i rozpowszechnianie niniejszego podręcznika użytkownika (zwanego dalej „Podręcznikiem”), częściowo lub w całości, niezależnie od metody, bez uprzedniego uzyskania zezwolenia od firmy Hikvision. Jeżeli nie uzgodniono inaczej, firma Hikvision nie udziela żadnych gwarancji i nie składa żadnych deklaracji, jawnych lub dorozumianych, dotyczących Podręcznika.

### **Opis Podręcznika**

Ten Podręcznik dotyczy **termowizyjnej tubowej kamery sieciowej**.

Podręcznik zawiera instrukcje dotyczące użycia tego urządzenia i obchodzenia się z nim. Zdjęcia, wykresy, obrazy i inne informacje zamieszczono w Podręczniku wyłącznie dla celów informacyjnych i opisowych. Informacje zamieszczone w Podręczniku mogą ulec zmianie bez powiadomienia w związku z aktualizacjami oprogramowania układowego lub w innych okolicznościach. Najnowsza wersja jest dostępna w firmowej witrynie internetowej (<http://overseas.hikvision.com/en/>).

Podczas korzystania z niniejszego Podręcznika użytkownika należy uwzględnić zalecenia specjalistów.

### **Znaki towarowe**

**HIKVISION** oraz inne znaki towarowe i logo Hikvision są własnością firmy Hikvision w różnych jurysdykcjach. Inne znaki towarowe i logo użyte w Podręczniku należą do odpowiednich właścicieli.

## **Zastrzeżenie prawne**

W PEŁNYM ZAKRESIE DOZWOLONYM PRZEZ OBOWIĄZUJĄCE PRAWO OPISANY PRODUKT ORAZ ZWIĄZANE Z NIM WYPOSAŻENIE, OPROGRAMOWANIE APLIKACYJNE I OPROGRAMOWANIE UKŁADOWE SĄ UDOSTĘPNIANE BEZ GWARANCJI, ZE WSZYSTKIMI USTERKAMI I BŁĘDAMI, A FIRMA HIKVISION NIE UDZIELA ŻADNYCH GWARANCJI, WYRAŹNYCH ANI DOROZUMIANYCH, TAKICH JAK GWARANCJA PRZYDATNOŚCI HANDLOWEJ, DOSTATECZNEJ JAKOŚCI, PRZYDATNOŚCI DO OKREŚLONEGO CELU I OCHRONY PRAW STRON TRZECICH. NIEZALEŻNIE OD OKOLICZNOŚCI FIRMA HIKVISION, JEJ CZŁONKOWIE ZARZĄDU, KIEROWNICTWO, PRACOWNICY I AGENCI NIE PONOSZĄ ODPOWIEDZIALNOŚCI ZA STRATY SPECJALNE, WYNIKOWE, PRZYPADKOWE LUB POŚREDNIE, TAKIE JAK STRATA OCZEKIWANYCH ZYSKÓW Z DZIAŁALNOŚCI BIZNESOWEJ, PRZERWY W DZIAŁALNOŚCI BIZNESOWEJ ALBO STRATA DANYCH LUB DOKUMENTACJI, ZWIĄZANE Z UŻYCIEM TEGO PRODUKTU, NAWET JEŻELI FIRMA HIKVISION ZOSTAŁA POINFORMOWANA O MOŻLIWOŚCI WYSTĄPIENIA STRAT TEGO TYPU.

W PRZYPADKU PRODUKTU Z DOSTĘPEM DO INTERNETU UŻYTKOWNIK KORZYSTA Z PRODUKTU NA WŁASNE RYZYKO. FIRMA HIKVISION NIE PONOSI ODPOWIEDZIALNOŚCI ZA NIEPRAWIDŁOWE FUNKCJONOWANIE PRODUKTU, NIEAUTORYZOWANE UJAWNIECIE DANYCH OSOBOWYCH ALBO INNE SZKODY WYNIKAJĄCE Z ATAKU CYBERNETYCZNEGO LUB HAKERSKIEGO, DZIAŁANIA WIRUSÓW KOMPUTEROWYCH LUB INNYCH ZAGROŻEŃ WYSTĘPUJĄCYCH W INTERNECIE. FIRMA HIKVISION ZAPEWNI JEDNAK POMOC TECHNICZNĄ W ODPOWIEDNIM CZASIE, JEŻELI BĘDZIE TO WYMAGANE.

PRZEPISY DOTYCZĄCE MONITORINGU SĄ ZALEŻNE OD JURYSDYKCJI. PRZED UŻYCIEM TEGO PRODUKTU NALEŻY ZAPOZNAĆ SIĘ ZE WSZYSTKIMI ODPOWIEDNIMI PRZEPISAMI WPROWADZONYMI W DANEJ JURYSDYKCJI, ABY UPEWNIĆ SIĘ, ŻE PRODUKT JEST UŻYWANY ZGODNIE Z OBOWIĄZUJĄCYM PRAWEM. FIRMA HIKVISION NIE PONOSI ODPOWIEDZIALNOŚCI ZA UŻYCIE TEGO PRODUKTU DO CELÓW NIEZGODNYCH Z PRAWEM.

W PRZYPADKU NIEZGODNOŚCI NINIEJSZEGO PODRĘCZNIKA Z OBOWIĄZUJĄCYM PRAWEM, WYŻSZY PRIORYTET BĘDZIE MIAŁO OBOWIĄZUJĄCE PRAWO.

## Informacje dotyczące przepisów

### Komisja FCC

**Zgodność z przepisami komisji FCC:** To urządzenie było testowane i zostało uznane za zgodne z limitami dla urządzeń cyfrowych, określonymi w części 15 przepisów komisji FCC. Te limity określono w celu zapewnienia uzasadnionej ochrony przed szkodliwymi zakłóceniami w środowisku komercyjnym. To urządzenie generuje, wykorzystuje i może emitować energię o częstotliwościach radiowych i powodować zakłócenia łączności radiowej, jeżeli nie jest zainstalowane i użytkowane zgodnie z podręcznikiem użytkownika. Użycie tego urządzenia w budynkach mieszkalnych może powodować szkodliwe zakłócenia. W takich okolicznościach użytkownik jest zobowiązany do eliminacji tych zakłóceń na własny koszt.

### Warunki komisji FCC

To urządzenie jest zgodne z wymaganiami określonymi w części 15 przepisów komisji FCC. Korzystanie z tego urządzenia jest uzależnione od dwóch warunków:

1. Urządzenie nie może powodować szkodliwych zakłóceń.
2. Urządzenie musi być odporne na zakłócenia zewnętrzne, łącznie z zakłóceniami powodującymi nieprawidłowe funkcjonowanie.

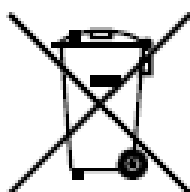
### Deklaracja zgodności z dyrektywami Unii Europejskiej



Ten produkt i ewentualnie dostarczone z nim akcesoria oznaczono symbolem „CE” potwierdzającym zgodność z odpowiednimi ujednoczonymi normami europejskimi, uwzględnionymi w dyrektywie 2004/108/WE dotyczącej kompatybilności elektromagnetycznej (EMC) i dyrektywie 2011/65/UE w sprawie ograniczenia stosowania niektórych niebezpiecznych substancji w sprzęcie elektrycznym i elektronicznym (RoHS).



Dyrektywa 2012/19/UE w sprawie zużytego sprzętu elektrycznego i elektronicznego (WEEE): Produktów oznaczonych tym symbolem nie wolno utylizować na obszarze Unii Europejskiej jako niesegregowane odpady komunalne. Aby zapewnić prawidłowy recykling, należy zwrócić ten produkt do lokalnego dostawcy przy zakupie równoważnego nowego urządzenia lub utylizować go w wyznaczonym punkcie zbiórki. Aby uzyskać więcej informacji, należy odwiedzić stronę internetową: [www.recyclethis.info](http://www.recyclethis.info).



Dyrektywa 2006/66/WE w sprawie baterii i akumulatorów: Ten produkt zawiera baterię, której nie wolno utylizować na obszarze Unii Europejskiej jako niesegregowane odpady komunalne. Szczegółowe informacje dotyczące baterii zamieszczono w dokumentacji produktu. Bateria jest oznaczona tym symbolem, który może także zawierać litery wskazujące na zawartość kadmu (Cd), ołowiu (Pb) lub rtęci (Hg). Aby zapewnić prawidłowy recykling, należy zwrócić baterię do dostawcy lub wyznaczonego punktu zbiórki. Aby uzyskać więcej informacji, należy odwiedzić stronę internetową: [www.recyclethis.info](http://www.recyclethis.info).

### **Zgodność z kanadyjską normą ICES-003**

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



### **Instrukcje dotyczące bezpieczeństwa**

Niniejsze instrukcje zostały opracowane w celu zapewnienia, iż urządzenie jest prawidłowo użytkowane oraz w celu uniknięcia zagrożeń i utraty mienia w wyniku nieprawidłowego użytkowania urządzenia.

Środki ostrożności wymienione w instrukcji zostały podzielone na „ostrzeżenia“ i „uwagi“

**Ostrzeżenia:** Niezastosowanie się do ostrzeżeń może prowadzić do poważnych obrażeń ciała lub śmierci.

**Uwagi:** Niezastosowanie się do uwag może prowadzić do obrażeń ciała lub uszkodzenia urządzenia.

	
<p><b>Ostrzeżenia:</b></p> <p>Należy przestrzegać tych środków ostrożności w celu uniknięcia poważnych obrażeń ciała lub śmierci.</p>	<p><b>Uwagi:</b></p> <p>Należy przestrzegać tych środków ostrożności w celu uniknięcia potencjalnych obrażeń ciała lub szkód materialnych.</p>



**Ostrzeżenia:**

- Należy stosować niskonapięciowe zasilacze zgodne ze standardem SELV (Safety Extra Low Voltage). Należy stosować zasilanie 12 V DC lub 24 V AC (zależnie od modelu) zgodnie z normą IEC60950-1 i źródła zasilania z własnym ograniczeniem (LPS, Limited Power Source).
- Aby ograniczyć ryzyko pożaru lub porażenia prądem elektrycznym, należy chronić ten produkt przed deszczem i wilgocią.
- Instalacja powinna zostać przeprowadzona przez wykwalifikowanego technika w zgodzie z lokalnymi normami bezpieczeństwa.
- W obwodzie zasilania należy zainstalować elementy blokujące przepływ prądu w celu przerwania dostawy prądu w dowolnym momencie.
- Należy upewnić się, że strop jest przystosowany do obciążenia ponad 50 N, jeżeli kamera jest zamocowana na stropie.
- Jeśli urządzenie nie działa prawidłowo, należy skontaktować się z lokalnym sprzedawcą lub najbliższym centrum serwisowym. Nie wolno samodzielnie demontować kamery. (Firma Hikvision nie ponosi żadnej odpowiedzialności za problemy spowodowane przez prace naprawcze lub konserwacyjne przeprowadzone przez nieautoryzowany serwis).



**Uwagi:**

- Przed użyciem kamery należy upewnić się, że napięcie sieci elektrycznej jest odpowiednie.
- Należy chronić kamerę przed upadkiem lub udarem mechanicznym.
- Nie wolno dotykać modułów czujników palcami. Jeżeli konieczne jest oczyszczenie kamery, należy przetrzeć ją czystą ściereczką z niewielką ilością etanolu. Jeżeli kamera nie będzie używana przez dłuższy czas, należy zamocować na obiektywie kołpak chroniący czujnik przed kurzem i pyłem.
- Nie wolno kierować obiektywu kamery na źródło intensywne światła, takie jak słońce lub żarówka. Intensywne światło może spowodować nieodwracalne uszkodzenie kamery.
- Jeśli czujnik zostanie porażony wiązką laserową, może ulec spaleni. Dlatego też podczas korzystania z urządzeń emitujących wiązki laserowe, należy upewnić się, że powierzchnia czujnika nie jest narażona na kontakt z wiązką laserową.
- Nie wolno umieszczać kamery w lokalizacjach, w których występują ekstremalnie wysokie lub niskie temperatury (gdy kamera jest uruchomiona temperatura powinna wynosić od  $-30^{\circ}\text{C}$  do  $+60^{\circ}\text{C}$ , a w przypadku kamer z sufiksem „H” w nazwie modelu temperatura powinna wynosić od  $-40^{\circ}\text{C}$  do  $+60^{\circ}\text{C}$ ), kurz, pył lub wilgoć. Należy chronić kamerę przed silnym promieniowaniem elektromagnetycznym.
- Aby zapobiec akumulacji ciepła, należy zapewnić prawidłową wentylację urządzenia.
- Należy chronić kamerę przed wodą i innymi cieciami.
- Przed transportem należy umieścić kamerę w oryginalnym opakowaniu lub użyć odpowiednich materiałów do pakowania. Można też użyć takiej samej tektury do pakowania.
- Nieprawidłowe użycie lub wymiana baterii może spowodować wybuch. Należy stosować rodzaj baterii zgodny z zaleceniami producenta.

**Uwagi:**

Kamera obsługuje podczerwień, dlatego należy uwzględnić następujące zalecenia, aby zapobiec odbiciu promieniowania podczerwonego:

- Kurz, pył lub tłuszcz na pokrywie kopułkowej odbijają promieniowanie podczerwone. Nie wolno usuwać folii z pokrywy kopułkowej przed zakończeniem instalacji. Jeżeli widoczny jest kurz, pył lub tłuszcz na pokrywie kopułkowej, należy oczyścić ją czystą, miękką ściereczką i alkoholem izopropylowym.
- Należy upewnić się, że w lokalizacji instalacji żadne obiekty odbijające światło nie znajdują się zbyt blisko kamery. Promieniowanie podczerwone z kamery może być odbijane wstecz do obiektywu.
- Piankowy pierścień wokół obiektywu musi być ułożony równo z wewnętrzną powierzchnią kopułki, aby chronić obiektyw przed diodami LED emitującymi podczerwień. Pokrywę kopułkową należy przymocować do korpusu kamery w taki sposób, aby piankowy pierścień prawidłowo przywierał do pokrywy.



## Spis treści

<b>Rozdział 1</b>	<b>Wymagania systemowe .....</b>	<b>11</b>
<b>Rozdział 2</b>	<b>Połączenie sieciowe.....</b>	<b>12</b>
2.1	Konfigurowanie kamery przy użyciu sieci LAN .....	12
2.1.1	Połączenie przewodowe za pośrednictwem sieci LAN.....	12
2.1.2	Aktywacja kamery.....	13
2.2	Konfigurowanie kamery przy użyciu sieci WAN .....	20
2.2.1	Podłączanie za pośrednictwem statycznego adresu IP .....	20
2.2.2	Podłączanie szybkoobrotowej kamery kopułkowej do sieci za pośrednictwem dynamicznego adresu IP .....	21
<b>Rozdział 3</b>	<b>Dostęp do kamery sieciowej.....</b>	<b>24</b>
3.1	Uzyskiwanie dostępu za pośrednictwem przeglądarki internetowej.....	24
3.2	Uzyskiwanie dostępu za pośrednictwem oprogramowania do zarządzania urządzeniami wideo.....	25
<b>Rozdział 4</b>	<b>Widok na żywo.....</b>	<b>27</b>
4.1	Interfejs podglądu na żywo.....	27
4.2	Uruchamianie podglądu na żywo.....	28
4.3	Ręczne nagrywanie i wykonywanie zdjęć .....	29
4.4	Sterowanie PTZ.....	29
4.4.1	Panel sterowania PTZ.....	30
4.4.2	Konfigurowanie/wywoływanie ustawienia wstępnego .....	31
4.4.3	Konfigurowanie/wywoływanie patrolu.....	32
<b>Rozdział 5</b>	<b>Konfiguracja kamery sieciowej.....</b>	<b>34</b>
5.1	Konfigurowanie parametrów lokalnych.....	34
5.2	Konfigurowanie ustawień systemowych .....	37
5.2.1	Konfigurowanie podstawowych informacji.....	37
5.2.2	Konfigurowanie ustawień czasu.....	39
5.2.3	Konfigurowanie ustawień RS485 .....	41
5.2.4	Konfigurowanie ustawień czasu letniego.....	42
5.2.5	Wyświetlanie licencji .....	42
5.3	Konserwacja .....	43
5.3.1	Uaktualnienie i konserwacja .....	43
5.3.2	Dziennik .....	44
5.3.3	Usługa systemowa .....	45
5.3.4	Typ zasobu VCA.....	46
5.4	Ustawienia zabezpieczeń .....	47
5.4.1	Uwierzytelniania .....	47

5.4.2	Filtr adresów IP .....	48
5.4.3	Usługa zabezpieczeń .....	49
<b>5.5</b>	<b>Zarządzanie użytkownikami .....</b>	<b>50</b>
5.5.1	Zarządzanie użytkownikami .....	50
5.5.2	Użytkownicy połączeni z urządzeniem.....	53
<b>Rozdział 6</b>	<b><i>Ustawienia sieciowe</i>.....</b>	<b>55</b>
<b>6.1</b>	<b>Konfigurowanie ustawień podstawowych .....</b>	<b>55</b>
6.1.1	Konfigurowanie ustawień protokołu TCP/IP .....	55
6.1.2	Konfigurowanie ustawień usługi DDNS.....	57
6.1.3	Konfigurowanie ustawień protokołu PPPoE.....	59
6.1.4	Konfigurowanie ustawień portów.....	60
6.1.5	Konfigurowanie ustawień translacji adresów sieciowych (NAT) .....	61
<b>6.2</b>	<b>Konfigurowanie ustawień zaawansowanych .....</b>	<b>62</b>
6.2.1	Konfigurowanie ustawień protokołu SNMP .....	62
6.2.2	Konfigurowanie ustawień serwera FTP.....	64
6.2.3	Konfigurowanie ustawień wysyłania wiadomości e-mail.....	66
6.2.4	Konfigurowanie ustawień HTTPS .....	68
6.2.5	Konfigurowanie ustawień jakości usługi (QoS) .....	70
6.2.6	Konfigurowanie ustawień standardu IEEE 802.1X .....	71
<b>Rozdział 7</b>	<b><i>Ustawienia wideo/audio</i>.....</b>	<b>73</b>
<b>7.1</b>	<b>Konfigurowanie ustawień wideo.....</b>	<b>73</b>
<b>7.2</b>	<b>Konfigurowanie ustawień audio.....</b>	<b>77</b>
<b>7.3</b>	<b>Konfigurowanie kodowania ROI.....</b>	<b>78</b>
<b>7.4</b>	<b>Ustawienia metadanych .....</b>	<b>80</b>
<b>Rozdział 8</b>	<b><i>Ustawienia obrazu</i> .....</b>	<b>82</b>
<b>8.1</b>	<b>Konfigurowanie ustawień wyświetlania .....</b>	<b>82</b>
<b>8.2</b>	<b>Konfigurowanie ustawień menu ekranowego .....</b>	<b>85</b>
<b>8.3</b>	<b>Konfigurowanie maski prywatności .....</b>	<b>86</b>
<b>8.4</b>	<b>Konfigurowanie nakładania obrazu.....</b>	<b>87</b>
<b>8.5</b>	<b>Konfigurowanie DPC (korekcji wadliwych pikseli).....</b>	<b>88</b>
<b>8.6</b>	<b>Konfigurowanie wyświetlania reguł VCA.....</b>	<b>90</b>
<b>Rozdział 9</b>	<b><i>Ustawienia zdarzeń</i> .....</b>	<b>91</b>
<b>9.1</b>	<b>Zdarzenia podstawowe .....</b>	<b>91</b>
9.1.1	Konfigurowanie detekcji ruchu .....	91
9.1.2	Konfigurowanie alarmu sabotażu sygnału wideo .....	98
9.1.3	Konfigurowanie wejścia alarmu.....	100
9.1.4	Konfigurowanie wyjścia alarmu .....	101

9.1.5	Obsługa zdarzeń nietypowych .....	102
<b>9.2</b>	<b>Zdarzenia inteligentne .....</b>	<b>103</b>
9.2.1	Konfigurowanie detekcji nietypowego dźwięku .....	103
9.2.2	Konfigurowanie detekcji zmiany sceny .....	105
9.2.3	Konfigurowanie dynamicznej detekcji źródła ognia.....	106
9.2.4	Konfigurowanie maskowania detekcji źródła ognia.....	107
<b>9.3</b>	<b>Konfiguracja VCA .....</b>	<b>109</b>
9.3.1	Konfigurowanie nakładania obrazu i wykonywania zdjęć.....	109
9.3.2	Konfiguracja analizy zachowania .....	110
9.3.3	Konfigurowanie maskowanego obszaru .....	113
9.3.4	Konfigurowanie reguły.....	114
9.3.5	Konfiguracja zaawansowana .....	116
<b>9.4</b>	<b>Pomiar temperatury .....</b>	<b>119</b>
9.4.1	Ustawienia podstawowe.....	119
9.4.2	Konfigurowanie reguły pomiaru temperatury .....	120
9.4.3	Działania powiązane .....	126
<b>Rozdział 10</b>	<b><i>Ustawienia magazynowania nagrań i zdjęć.....</i></b>	<b>127</b>
<b>10.1</b>	<b>Konfigurowanie harmonogramu nagrywania .....</b>	<b>127</b>
<b>10.2</b>	<b>Konfigurowanie harmonogramu wykonywania zdjęć .....</b>	<b>130</b>
<b>10.3</b>	<b>Konfigurowanie sieciowego dysku HDD .....</b>	<b>132</b>
<b>10.4</b>	<b>Detekcja karty pamięci .....</b>	<b>135</b>
<b>10.5</b>	<b>Konfigurowanie Magazynowania uproszczonego .....</b>	<b>137</b>
<b>Rozdział 11</b>	<b><i>Odtwarzanie .....</i></b>	<b>139</b>
<b>Rozdział 12</b>	<b><i>Zdjęcia.....</i></b>	<b>141</b>
<b>Aneks</b>	<b>.....</b>	<b>142</b>
<b>Aneks 1</b>	<b>Wprowadzenie do oprogramowania SADP .....</b>	<b>142</b>
<b>Aneks 2</b>	<b>Mapowanie portów .....</b>	<b>145</b>

# Rozdział 1 Wymagania systemowe

**System operacyjny:** Microsoft Windows XP SP1 lub nowszy

**Procesor:** 2,0 GHz lub nowszy

**Pamięć RAM:** 1 GB lub więcej

**Wyświetlacz:** Rozdzielczość 1024 x 768 lub większa

**Przeglądarka internetowa:** Internet Explorer 8.0 lub nowsza, Apple Safari 5.0.2 lub nowsza, Mozilla Firefox 5.0 lub nowsza i Google Chrome 18 lub nowsza.

## Rozdział 2 Połączenie sieciowe

### **Uwaga:**

- Użytkownik potwierdza, iż jest świadomy zagrożeń sieciowych wynikających z korzystania z urządzenia, które jest połączone z Internetem. Aby uniknąć ataków sieciowych i wycieku prywatnych informacji, należy wzmocnić ochronę urządzenia. Jeśli urządzenie nie działa prawidłowo, należy skontaktować się z lokalnym sprzedawcą lub najbliższym centrum serwisowym.
- Aby zapewnić bezpieczeństwo kamery w sieci, należy regularnie sprawdzać stan kamery sieciowej i wykonywać prace konserwacyjne. W celu skorzystania z tego typu usługi można skontaktować się z firmą Hikvision.

### **Zanim rozpoczniesz:**

- Jeżeli chcesz konfigurować kamerę przy użyciu sieci lokalnej (LAN, Local Area Network), zobacz 2.1.
- Jeżeli chcesz konfigurować kamerę przy użyciu sieci rozległej (WAN, Wide Area Network), zobacz 2.2.

## 2.1 Konfigurowanie kamery przy użyciu sieci LAN

### **Cel:**

Aby wyświetlić obraz z kamery sieciowej i skonfigurować ją przy użyciu sieci LAN, należy połączyć kamerę z tą samą podsiecią, z którą jest połączony komputer, i zainstalować oprogramowanie SADP lub iVMS-4200 umożliwiające wyszukiwanie i zmianę adresu IP kamery sieciowej.

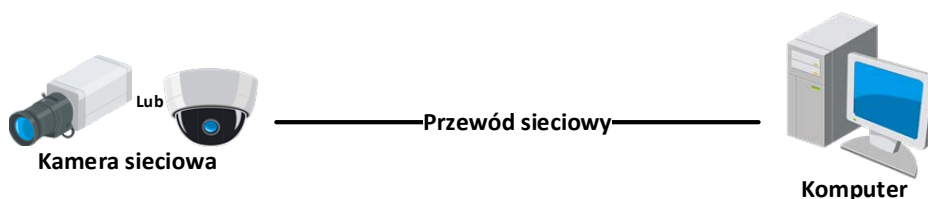
**Uwaga:** Aby uzyskać szczegółowe wprowadzenie do obsługi aplikacji SADP, należy zapoznać się z załącznikiem 1.

### 2.1.1 Połączenie przewodowe za pośrednictwem sieci LAN

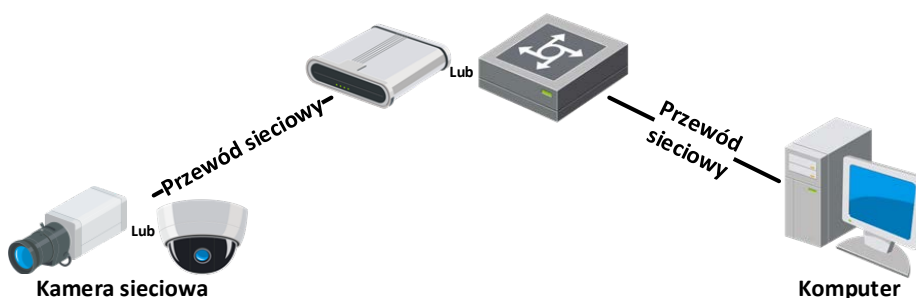
Na poniższych rysunkach przedstawiono dwie metody przewodowego połączenia kamery sieciowej z komputerem:

**Cel:**

- Aby przetestować kamerę sieciową, można podłączyć ją bezpośrednio do komputera kablem sieciowym w sposób przedstawiony na Rysunek 2–1.
- Aby ustawić kamerę sieciową przez sieć LAN przy użyciu przełącznika lub routera, patrz.



Rysunek 2–1 Połączenie bezpośrednie



Rysunek 2–2 Rysunek – Połączenie przy użyciu przełącznika lub routera

## 2.1.2 Aktywacja kamery

Przed użyciem kamery należy ją aktywować, ustawiając silne hasło dla kamery.

Obsługiwana jest aktywacja przy użyciu przeglądarki internetowej, oprogramowania SADP i oprogramowania klienckiego.

### ❖ Aktywacja za pośrednictwem przeglądarki internetowej

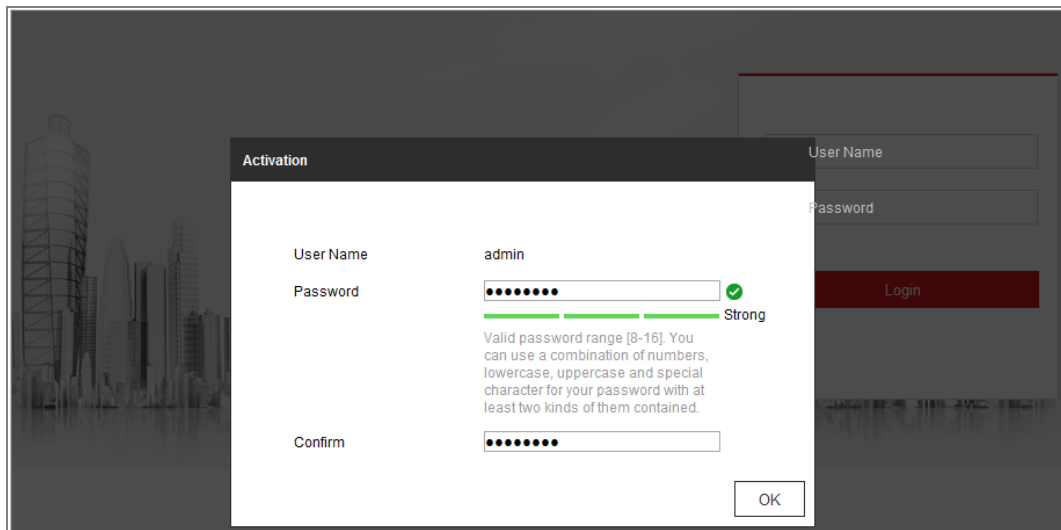
**Kroki:**

1. Włącz zasilanie kamery i połącz ją z siecią.
2. W polu adresowym przeglądarki internetowej wprowadź adres IP kamery, a następnie naciśnij klawisz „**Enter**”, aby przejść do interfejsu aktywacji.

**Uwagi:**

- Domyślny adres IP kamery to 192.168.1.64.

- Komputer i kamera powinny należeć do tej samej podsięci.
- Obsługa protokołu DHCP w kamerze jest domyślnie włączona, dlatego należy wyszukać adres IP przy użyciu oprogramowania SADP.



Rysunek 2–3 Aktywacja przy użyciu przeglądarki internetowej

3. Utwórz hasło i wprowadź je w polu hasła.



**ZALECANE JEST STOSOWANIE SILNEGO HASŁA** — zdecydowanie zalecane jest utworzenie własnego silnego hasła (co najmniej osiem znaków należących do co najmniej trzech z następujących kategorii: wielkie litery, małe litery, cyfry i znaki specjalne) w celu zapewnienia lepszej ochrony urządzenia. Zalecane jest również regularne resetowanie hasła. Zwłaszcza w systemie z restrykcyjnymi zabezpieczeniami resetowanie hasła co miesiąc lub co tydzień zapewnia lepszą ochronę urządzenia.

4. Potwierdź hasło.
5. Kliknij przycisk **OK**, aby zapisać hasło i wyświetlić podgląd na żywo.

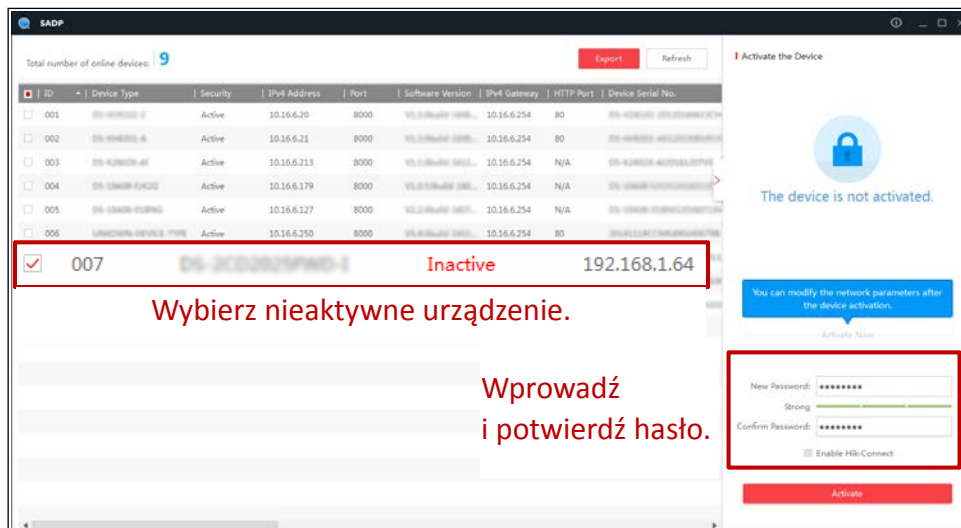
#### ❖ Aktywacja za pośrednictwem aplikacji SADP

Oprogramowanie SADP jest używane do wykrywania urządzenia w stanie online, aktywacji kamery i resetowania hasła.

Pobierz aplikację SADP z dołączonej płyty lub z oficjalnej strony internetowej, a następnie zainstaluj aplikację SADP, postępując zgodnie z komunikatami wyświetlanymi na ekranie. Wykonaj poniższe kroki, aby aktywować kamerę.

**Kroki:**

1. Uruchom aplikację SADP, aby wyszukać urządzenia połączone z siecią.
2. Sprawdź stan urządzenia na liście i wybierz nieaktywne urządzenie.



Rysunek 2–4 Oprogramowanie SADP

**Uwaga:**

Oprogramowanie SADP obsługuje zbiorczą aktywację kamer. Aby uzyskać więcej informacji, skorzystaj z podręcznika użytkownika oprogramowania SADP.

3. Utwórz hasło i wprowadź je w polu hasła, a następnie potwierdź.



**ZALECANE JEST UTWORZENIE SILNEGO HASŁA** – zdecydowanie zalecane jest utworzenie własnego silnego hasła (co najmniej osiem znaków należących do co najmniej trzech z następujących kategorii: wielkie litery, małe litery, cyfry i znaki specjalne) w celu zapewnienia lepszej ochrony urządzenia. Zalecane jest również regularne resetowanie hasła. Zwłaszcza w systemie z restrykcyjnymi zabezpieczeniami resetowanie hasła co miesiąc lub co tydzień zapewnia lepszą ochronę urządzenia.

**Uwaga:**

Podczas aktywacji można włączyć usługę Hik-Connect dla urządzenia.

4. Kliknij przycisk **Activate**, aby rozpocząć aktywację.



W wyskakującym okienku wyświetlone zostaną informacje o pomyślnym lub niepomyślnym zakończeniu aktywacji. Jeżeli aktywacja nie powiedzie się, należy upewnić się, że hasło spełnia wymagania, i spróbować ponownie.

5. Zmień ręcznie adres IP urządzenia lub zaznacz pole wyboru „Enable DHCP” (Włącz DHCP), aby upewnić się, że kamera i komputer znajdują się w tej samej podsieci.

Rysunek 2–5 Zmiana adresu IP

6. Wprowadź hasło administratora i kliknij przycisk **Modify**, aby aktywować modyfikację adresu IP.

Zbiorcza modyfikacja adresu IP jest obsługiwana przez oprogramowanie SADP. Aby uzyskać więcej informacji, skorzystaj z podręcznika użytkownika oprogramowania SADP.

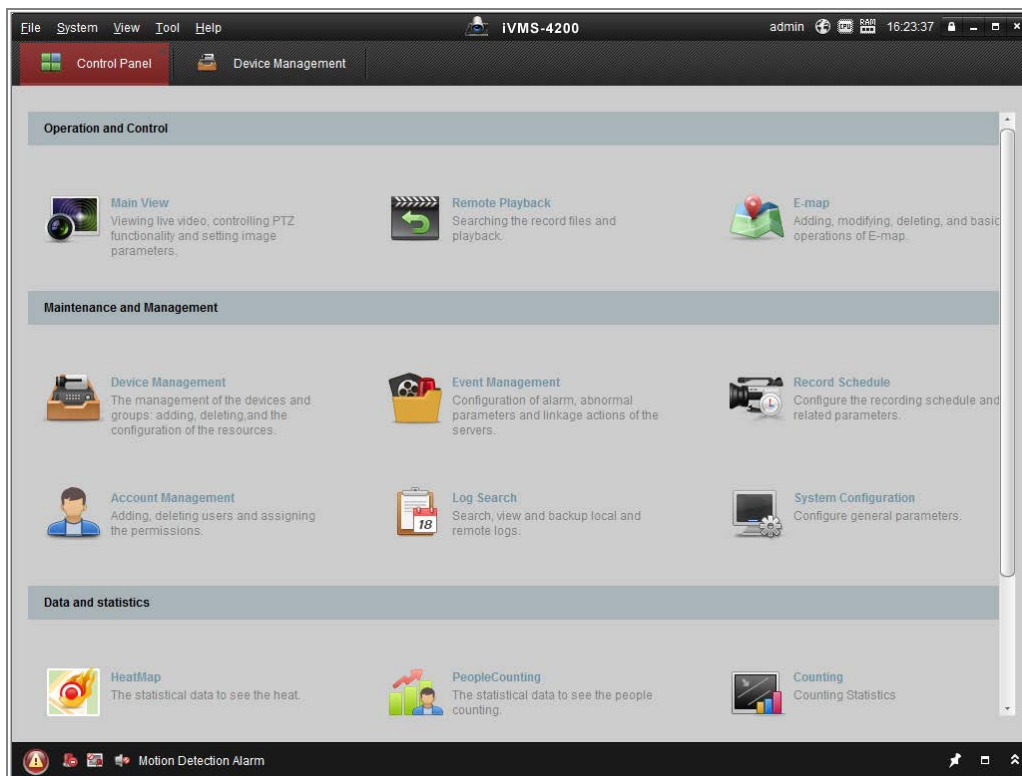
## ❖ Aktywacja za pośrednictwem oprogramowania do zarządzania urządzeniami wideo

Urządzenie można aktywować za pomocą różnych rodzajów oprogramowania do zarządzania różnymi urządzeniami wideo.

Pobierz oprogramowanie z dołączonej płyty lub z oficjalnej strony internetowej, a następnie zainstaluj, postępując zgodnie z komunikatami wyświetlanymi na ekranie. Wykonaj poniższe kroki, aby aktywować kamerę.

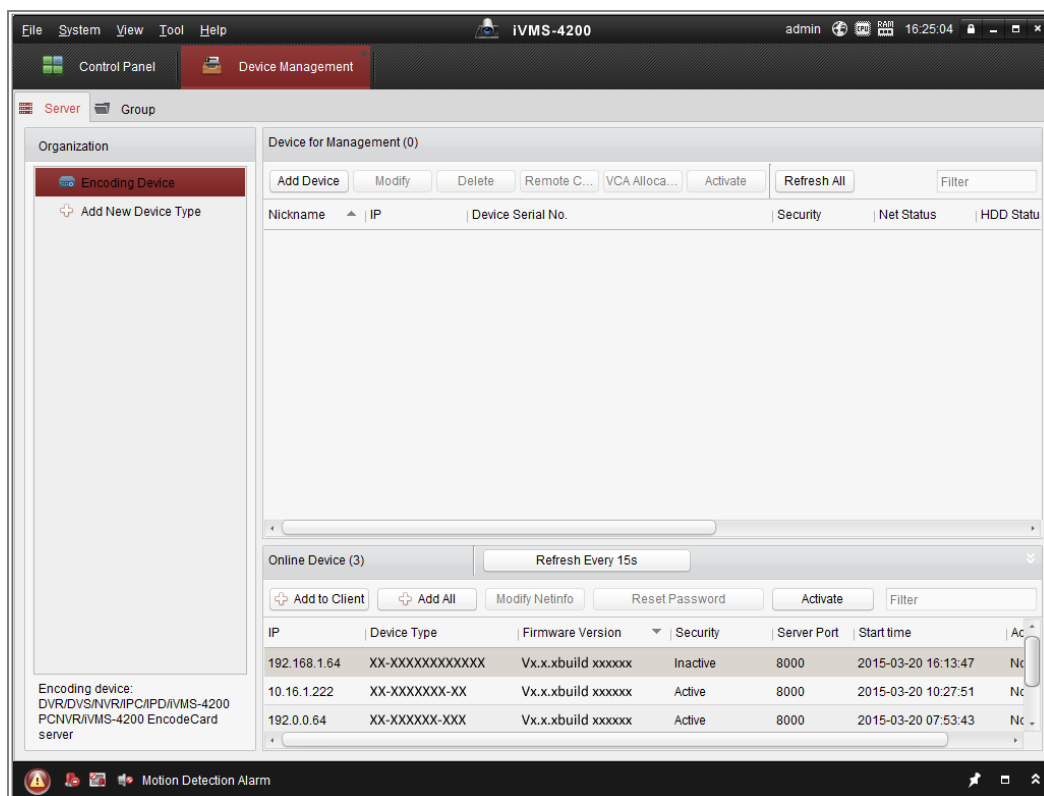
**Kroki:**

1. Uruchom oprogramowanie. Na ekranie wyświetli się okno panelu sterowania, jak przedstawiono na poniższym rysunku.



Rysunek 2–6 Panel sterowania

2. Kliknij ikonę „**Device Management**”, aby przejść do interfejsu zarządzania urządzeniami, jak przedstawiono na poniższym rysunku.

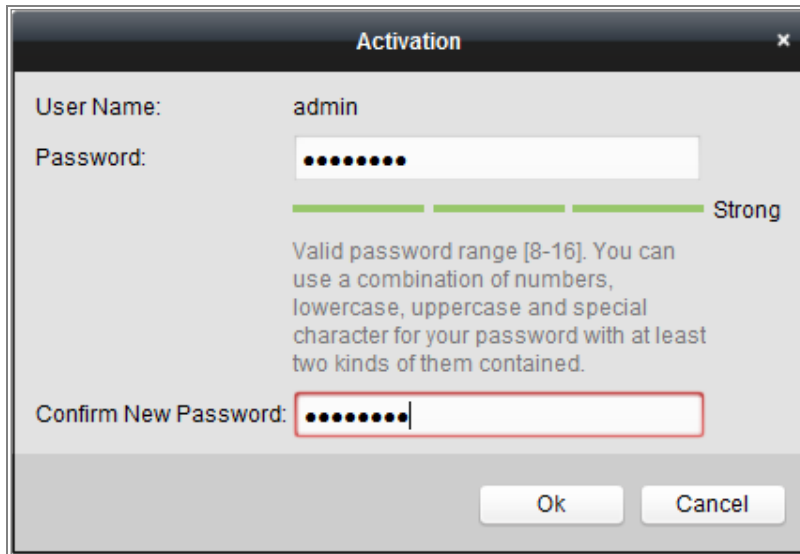


Rysunek 2–7 Zarządzanie urządzeniami

3. Sprawdź stan urządzeń na liście urządzeń i wybierz nieaktywne urządzenie.
4. Kliknij przycisk „**Activate**“, aby wyświetlić interfejs aktywowania.
5. Utwórz hasło i wprowadź je w polu hasła, a następnie potwierdź.

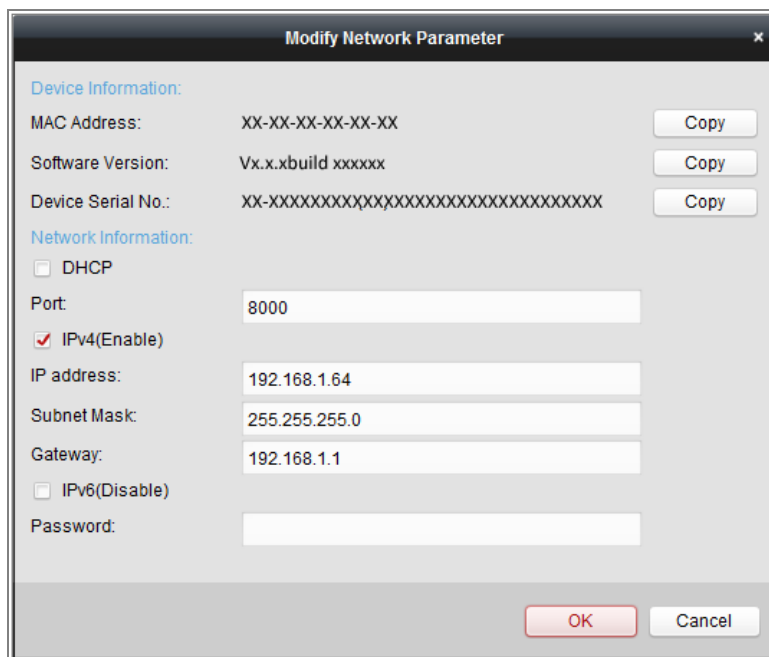


**ZALECANE JEST STOSOWANIE SILNEGO HASŁA** — zdecydowanie zalecane jest utworzenie własnego silnego hasła (co najmniej osiem znaków należących do co najmniej trzech z następujących kategorii: wielkie litery, małe litery, cyfry i znaki specjalne) w celu zapewnienia lepszej ochrony urządzenia. Zalecane jest regularne resetowanie hasła. Zwłaszcza w systemie z restrykcyjnymi zabezpieczeniami resetowanie hasła co miesiąc lub co tydzień zapewnia lepszą ochronę urządzenia.



Rysunek 2–8 Aktywacja (oprogramowanie klienckie)

6. Kliknij przycisk „OK”, aby rozpocząć aktywację.
7. Kliknij przycisk Modify Netinfo, aby wyświetlić okno Modyfikowanie parametrów sieciowych, przedstawione na rysunku poniżej.



Rysunek 2–9 Modyfikowanie parametrów sieciowych

8. Zmień ręcznie adres IP urządzenia lub zaznacz pole wyboru „Enable DHCP” (Włącz DHCP), aby upewnić się, że kamera i komputer znajdują się w tej samej podsieci.
9. Wprowadź hasło, aby aktywować zmieniony adres IP.

## 2.2 Konfigurowanie kamery przy użyciu sieci WAN

### **Cel:**

W tej sekcji wyjaśniono, jak połączyć kamerę z siecią WAN przy użyciu statycznego lub dynamicznego adresu IP.

### 2.2.1 Podłączanie za pośrednictwem statycznego adresu IP

#### **Zanim rozpoczniesz:**

Wprowadź statyczny adres IP otrzymany od usługodawcy internetowego. W przypadku statycznego adresu IP można połączyć kamerę sieciową przy użyciu routera lub połączyć ją bezpośrednio z siecią WAN.

- **Połączenie kamery sieciowej przy użyciu routera**

#### **Kroki:**

1. Podłącz kamerę sieciową do routera.
2. Wprowadź adres IP sieci LAN, maskę podsieci i bramę. Aby uzyskać więcej informacji dotyczących konfiguracji adresu IP kamery sieciowej, zobacz 2.1.2.
3. Zapisz statyczny adres IP w ustawieniach routera.
4. Skonfiguruj mapowanie portów np. 80, 8000 i 554. Kroki związane z mapowaniem portów są zależne od routera. Aby uzyskać pomoc w kwestii mapowania portów, należy skontaktować się z producentem routera.

**Uwaga:** Aby uzyskać szczegółowe informacje na temat mapowania portów, należy zapoznać się z załącznikiem 2.

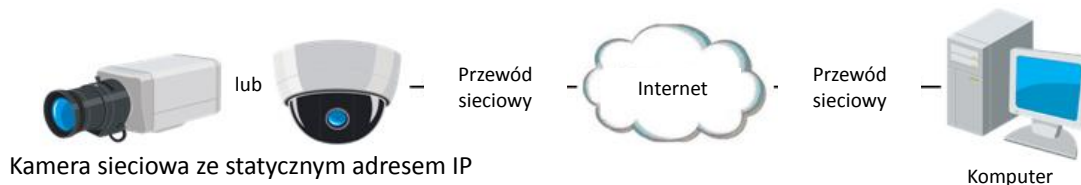
5. Uzyskaj dostęp do kamery sieciowej przy użyciu przeglądarki internetowej lub oprogramowania klienckiego za pośrednictwem Internetu.



Rysunek 2–10 Uzyskiwanie dostępu do kamery przez router ze statycznym adresem IP

- **Bezpośrednie połączenie kamery sieciowej ze statycznym adresem IP**

Można również zapisać statyczny adres IP w kamerze i połączyć ją bezpośrednio z Internetem bez użycia routera. Aby uzyskać więcej informacji dotyczących konfiguracji adresu IP kamery sieciowej, zobacz 2.1.2.



Rysunek 2–11 Bezpośredni dostęp do kamery przy użyciu statycznego adresu IP

## 2.2.2 Podłączanie szybkoobrotowej kamery kopułkowej do sieci za pośrednictwem dynamicznego adresu IP

### **Zanim rozpoczniesz:**

Wprowadź dynamiczny adres IP otrzymany od usługodawcy internetowego. W przypadku dynamicznego adresu IP można podłączyć kamerę sieciową do modemu lub routera.

- **Połączenie kamery sieciowej przy użyciu routera**

### **Kroki:**

1. Podłącz kamerę sieciową do routera.
2. Przypisz w kamerze adres IP sieci LAN, maskę podsieci i bramę. Aby uzyskać więcej informacji na temat konfiguracji adresu IP kamery sieciowej, zobacz sekcję 2.1.2.
3. W ustawieniach protokołu PPPoE routera wprowadź nazwę użytkownika, hasło i potwierdź hasło.
4. Ustaw mapowanie portów. Na przykład porty 80, 8000 i 554. Procedura mapowania portów może się różnić w zależności od modelu routera. Aby uzyskać pomoc w kwestii mapowania portów, należy skontaktować się z producentem routera.

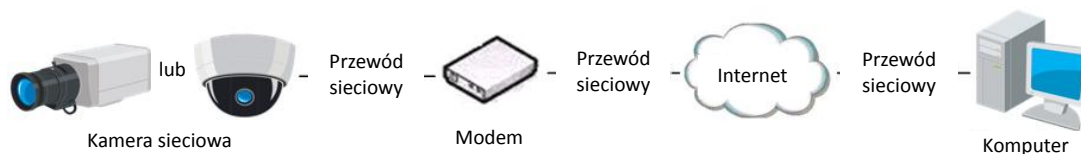
**Uwaga:** Aby uzyskać szczegółowe informacje na temat mapowania portów, należy zapoznać się z załącznikiem 2.

5. Zastosuj nazwę domeny otrzymaną od dostawcy nazwy domeny.
6. Skonfiguruj ustawienia DDNS w interfejsie ustawień routera.
7. Uzyskaj dostęp do kamery przy użyciu zastosowanej nazwy domeny.

● **Połączenie kamery sieciowej przy użyciu modemu**

**Cel:**

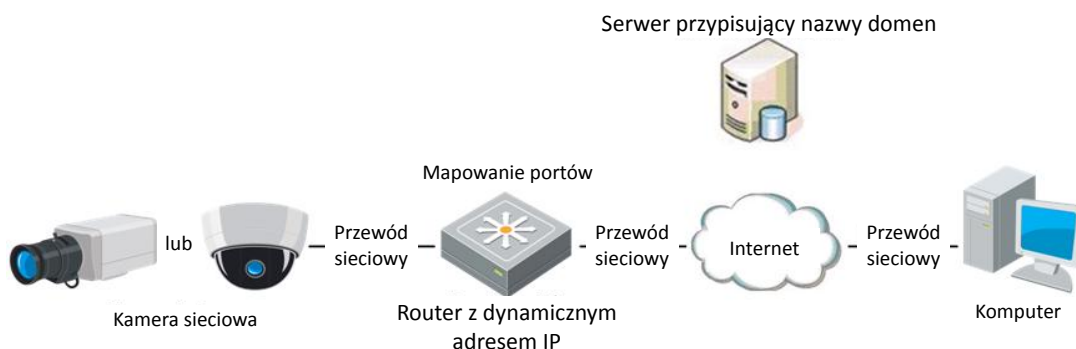
Ta kamera obsługuje automatyczne połączenia telefoniczne przy użyciu protokołu PPPoE. Kamera uzyskuje publiczny adres IP przy użyciu telefonicznego połączenia ADSL po podłączeniu jej do modemu. Należy skonfigurować parametry protokołu PPPoE kamery sieciowej. Aby uzyskać więcej informacji na temat konfiguracji, zobacz **Sekcję 6.1.3 Konfigurowanie ustawień protokołu PPPoE.**



Rysunek 2–12 Dostęp do kamery z dynamicznym adresem IP

**Uwaga:** Uzyskany adres IP jest dynamicznie przypisywany przy użyciu protokołu PPPoE, dlatego zawsze ulega zmianie po ponownym uruchomieniu kamery. Aby rozwiązać problem stale zmieniającego się dynamicznego adresu IP, należy uzyskać nazwę domeny od usługodawcy DDNS (np. DynDns.com). Aby rozwiązać ten problem, wykonaj poniższe kroki związane z rozpoznawaniem nazw domen zwykłych i prywatnych.

◆ Uzyskiwanie normalnej nazwy domeny

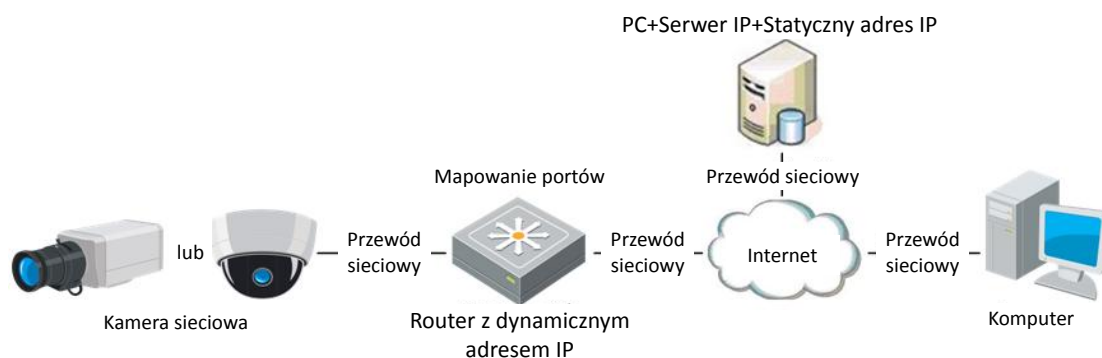


Rysunek 2–13 Uzyskiwanie normalnej nazwy domeny

**Kroki:**

1. Zastosuj nazwę domeny otrzymaną od dostawcy nazwy domeny.
2. Skonfiguruj ustawienia DDNS w interfejsie ustawień DDNS kamery sieciowej.  
Aby uzyskać więcej informacji na temat konfiguracji, zobacz *Sekcję 6.1.2 Konfigurowanie ustawień usługi DDNS*.
3. Uzyskaj dostęp do kamery przy użyciu zastosowanej nazwy domeny.

◆ Rozpoznawanie nazw domen prywatnych



Rysunek 2–14 Rozpoznawanie nazw domen prywatnych

**Kroki:**

1. Zainstaluj i uruchom Serwer IP na komputerze ze statycznym adresem IP.
2. Uzyskaj dostęp do kamery sieciowej przy użyciu sieci LAN i przeglądarki internetowej lub oprogramowania klienckiego.
3. Włącz funkcję DDNS i wybierz Serwer IP jako typ protokołu. Aby uzyskać więcej informacji na temat konfiguracji, zobacz *Sekcję 6.1.2 Konfigurowanie ustawień usługi DDNS*.



# Rozdział 3 Dostęp do kamery sieciowej

## 3.1 Uzyskiwanie dostępu za pośrednictwem przeglądarki internetowej

**Kroki:**

1. Otwórz przeglądarkę internetową.
2. Wprowadź adres IP kamery sieciowej na pasku adresu przeglądarki i naciśnij klawisz **Enter**, aby wyświetlić okno logowania.

**Uwaga:**

Domyślny adres IP to 192.168.1.64. Użytkownik powinien zmienić adres IP na adres w podsieci, w której znajduje się jego komputer.

3. Wprowadź nazwę użytkownika oraz hasło i kliknij przycisk **Login**.

Użytkownik o uprawnieniach administratora powinien odpowiednio skonfigurować konta urządzenia i uprawnienia innych użytkowników/operatorów. Usuń niepotrzebne konta i uprawnienia użytkowników/operatorów.

**Uwaga:**

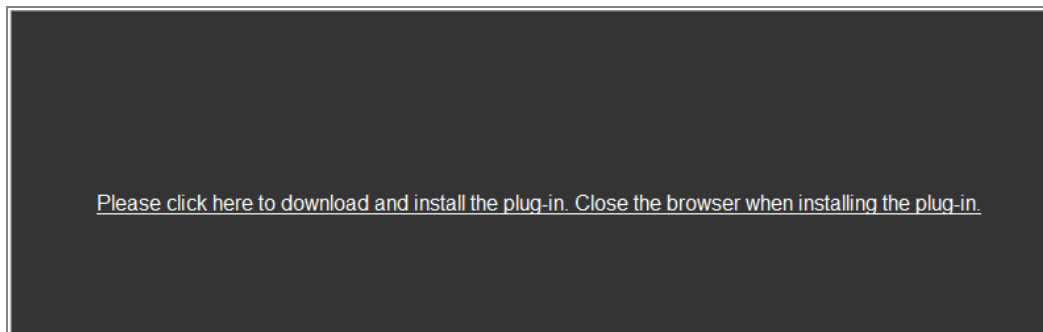
Adres IP jest blokowany, jeżeli użytkownik admin wprowadzi nieprawidłowe hasło siedem razy (pięć razy w przypadku gościa/operatora).



Rysunek 3–1 Okno logowania

4. Kliknij przycisk **Login**.

5. Przed wyświetleniem widoku na żywo obrazu wideo i skorzystaniem z kamery zainstaluj wtyczkę. Postępuj zgodnie z monitami instalacyjnymi, aby zainstalować wtyczkę.

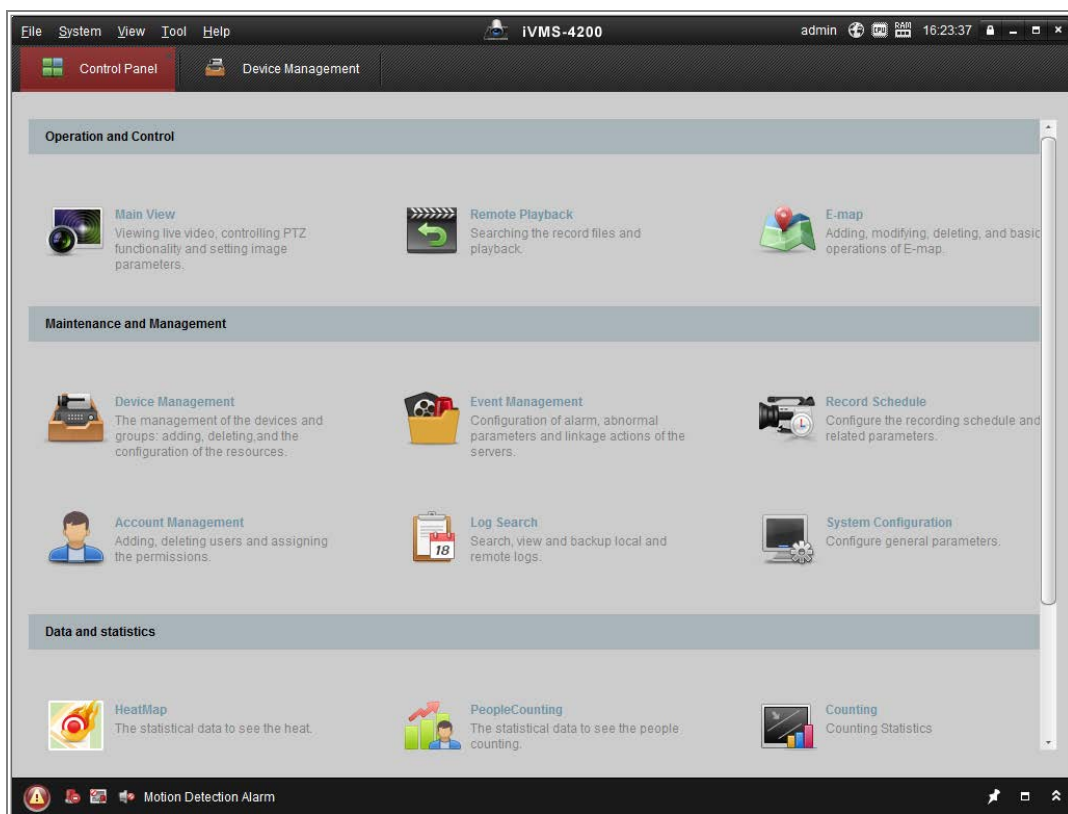


Rysunek 3–2 Pobieranie i instalacja wtyczki

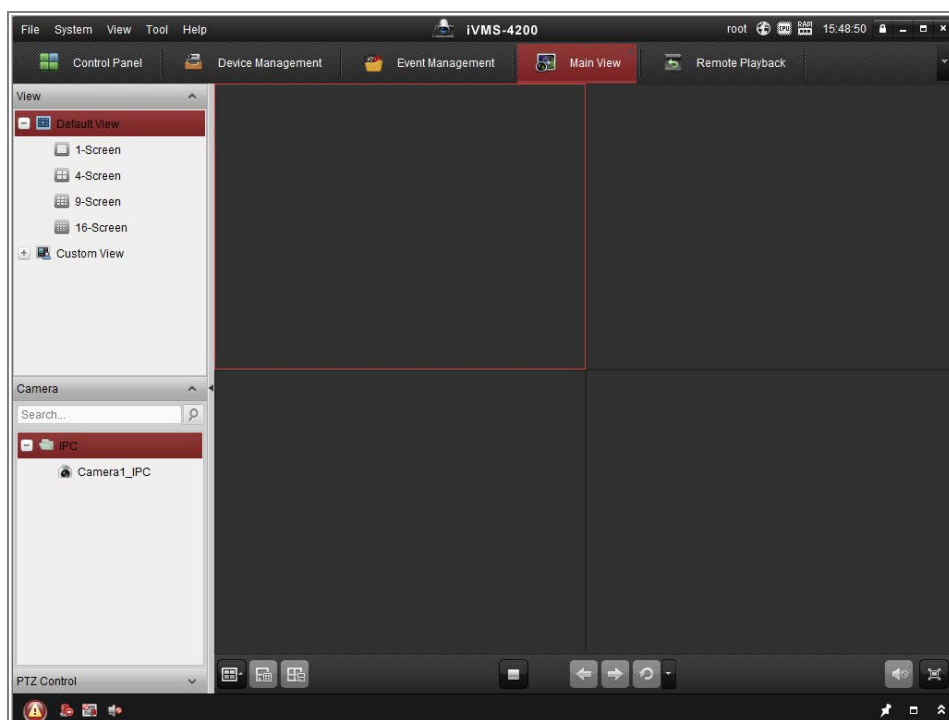
- Uwaga:** Konieczne może być zamknięcie przeglądarki internetowej w celu ukończenia instalacji wtyczki.
6. Otwórz ponownie przeglądarkę internetową po zainstalowaniu wtyczki i powtórz kroki 2–4, aby się zalogować.
- Uwaga:** Aby uzyskać szczegółowe instrukcje dotyczące dalszej konfiguracji, skorzystaj z podręcznika użytkownika kamery sieciowej.

## 3.2 Uzyskiwanie dostępu za pośrednictwem oprogramowania do zarządzania urządzeniami wideo

Dysk CD produktu zawiera oprogramowanie klienckie iVMS-4200. Korzystając z oprogramowania, można wyświetlać widok na żywo z kamery i zarządzać kamerą. Postępuj zgodnie z monitami instalacyjnymi, aby zainstalować oprogramowanie. Poniżej przedstawiono panel sterowania i okno podglądu na żywo oprogramowania klienckiego iVMS-4200.



Rysunek 3–3 Panel sterowania iVMS-4200



Rysunek 3–4 Widok główny oprogramowania iVMS-4200

## Rozdział 4 Widok na żywo

### 4.1 Interfejs podglądu na żywo

#### Cel:

Na stronie podglądu na żywo można wyświetlać w czasie rzeczywistym obraz wideo i wykonane zdjęcia, korzystać ze sterowania PTZ, ustawiać/wywoływać ustawienia wstępne i konfigurować parametry wideo.

Aby wyświetlić stronę podglądu na żywo, należy zalogować się do kamery sieciowej lub kliknąć przycisk **Live View** na pasku menu okna głównego.

#### Opis elementów interfejsu podglądu na żywo:



Rysunek 4–1 Strona podglądu na żywo

#### Pasek menu:

Kliknięcie zakładek „Live View” (Podgląd na żywo), „Playback” (Odtwarzanie), „Picture” (Zdjęcie) i „Configuration” (Konfiguracja) umożliwia przejście do odpowiednich interfejsów.

#### Okno podglądu na żywo:

Służy do wyświetlania obrazu podglądu na żywo.

**Pasek narzędzi:**

Korzystając z paska narzędzi, można dostosować rozmiar okna podglądu na żywo, typ strumienia i dodatki typu plug-in. Można wykonywać operacje na stronie podglądu na żywo, takie jak uruchamianie/zatrzymywanie podglądu na żywo, wykonywanie zdjęć, nagrywanie, włączanie/wyłączanie dźwięku, dwukierunkowe przesyłanie sygnału audio lub włączanie/wyłączanie powiększenia cyfrowego.

Użytkownicy programu Internet Explorer (IE) mogą wybierać wtyczki takie jak składniki sieci Web i Quick Time. Użytkownicy przeglądarek internetowych innych niż IE mogą wybierać składniki sieci Web, Quick Time, VLC lub MJPEG, jeżeli są one obsługiwane przez daną przeglądarkę.

**Sterowanie PTZ:**

Obracanie i pochylanie kamery oraz powiększanie obrazu z kamery. Obsługa oświetlenia i wycieraczki (tylko kamery obsługujące funkcję PTZ).

**Ustawienia wstępne/patrole:**

Konfigurowanie/wywoływanie/usuwanie ustawień wstępnych lub patroli dla kamer PTZ.

## 4.2 Uruchamianie podglądu na żywo




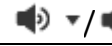


W oknie podglądu na żywo, przedstawionym na Rysunek 4–2, kliknij przycisk ► na pasku narzędzi, aby wyświetlić widok na żywo z kamery.



Rysunek 4–2 Pasek narzędzi podglądu na żywo



Tabela 4–1 Opis elementów paska narzędzi

Ikona	Opis
▶/■	Uruchamianie/zatrzymywanie podglądu na żywo.
4:3	Proporcje okna 4:3.
16:9	Proporcje okna 16:9.
1x	Oryginalny rozmiar okna.
📺	Automatyczne dostosowanie rozmiaru okna.
🔊	Podgląd na żywo strumienia głównego.
🔊	Podgląd na żywo podstrumienia.
🔊	Podgląd na żywo trzeciego strumienia.

Ikona	Opis
	Kliknij, aby wybrać wtyczkę innej firmy.
	Ręczne wykonanie zdjęcia.
	Ręczne rozpoczęcie/kończenie nagrywania.
	Włączanie dźwięku i dostosowanie głośności/wyciszenie dźwięku.
	Włączanie/wyłączanie mikrofonu.
	Włączanie/wyłączanie funkcji powiększenia cyfrowego.

**Uwaga:** Ikony są zależne od modelu kamery.

### 4.3 Ręczne nagrywanie i wykonywanie zdjęć

W oknie podglądu na żywo należy kliknąć przycisk  na pasku narzędzi, aby wykonać zdjęcia, lub kliknąć przycisk  w celu nagrania obrazu podglądu na żywo. Ścieżki zapisywania wykonanych zdjęć i klipów można ustawić na stronie **Configuration > Local**. Aby skonfigurować zdalne zaplanowane nagrywanie, zobacz sekcję 10.1.

**Uwaga:** Wykonane zdjęcie jest zapisywane jako plik JPEG lub BMP na komputerze.

### 4.4 Sterowanie PTZ



**Uwaga:** Niektóre modele kamer nie obsługują sterowania PTZ. Ta sekcja dotyczy tylko kamer obsługujących sterowania PTZ.

**Cel:**

W oknie podglądu na żywo można obracać/pochylać kamerę i powiększać obraz z kamery przy użyciu przycisków sterowania PTZ.

**Uwaga:** Sterowanie PTZ kamerą połączoną z siecią jest dostępne tylko w przypadku kamery obsługującej funkcję PTZ lub wyposażonej w moduł obracania/pochylania. Należy prawidłowo skonfigurować parametry PTZ na stronie ustawień RS485, korzystając z sekcji 5.2.3.

#### 4.4.1 Panel sterowania PTZ

Aby wyświetlić panel sterowania PTZ, należy kliknąć przycisk  po prawej stronie w oknie podglądu na żywo. Przycisk  umożliwia ukrycie tego panelu.

Użyj przycisków kierunkowych, aby sterować obrotem lub pochyleniem.



Rysunek 4–3 Panel sterowania PTZ

Aby sterować obiektywem, należy kliknąć przyciski powiększenia/ostrości/przystony.

#### **Uwagi:**























- Na panelu sterowania dostępnych jest osiem przycisków ze strzałkami (, , , , , , , ). Należy kliknąć strzałki, aby dostosować położenie względne.
- W przypadku kamer przystosowanych tylko do zmiany położenia obiektywu przyciski kierunkowe są niedostępne.

Tabela 4–2 Opis panelu sterownia PTZ

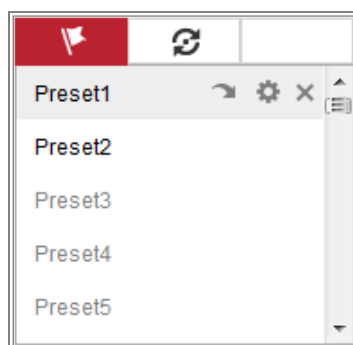
Ikona	Opis
	Powiększanie/pomniejszanie
	Wyostrowanie obiektów w bliży/dali
	Przystona +/-
	Regulacja prędkości PTZ
	Włączanie/wyłączanie oświetlenia
	Włączanie/wyłączanie wycieraczki
	Pomocnicza regulacja ostrości

Ikona	Opis
	Inicjowanie obiektywu
	Regulacja prędkości obracania/pochylania
	Rozpoczęcie śledzenia ręcznego
	Uruchomienie funkcji Zoom 3D
	Włączanie podgrzewania
	Ustawienie wstępne
	Patrol



#### 4.4.2 Konfigurowanie/wywoływanie ustawienia wstępnego

- **Konfigurowanie ustawienia wstępnego**

1. W panelu sterowania PTZ wybierz numer ustawienia wstępnego z listy ustawień wstępnych.



Rysunek 4–4 Konfigurowanie ustawienia wstępnego


2. Za pomocą przycisków sterowania PTZ przesuń obiektyw na pożądaną pozycję.
  - Obróć kamerę w prawo lub w lewo.
  - Podnieś kamerę w górę lub pochyl ją w dół?
  - Powiększ lub pomniejsz obraz.
  - Ustaw ostrość obiektywu.
3. Kliknij przycisk , aby zakończyć konfigurowanie bieżącego ustawienia wstępnego.
4. Kliknij przycisk , aby usunąć ustawienie wstępne.



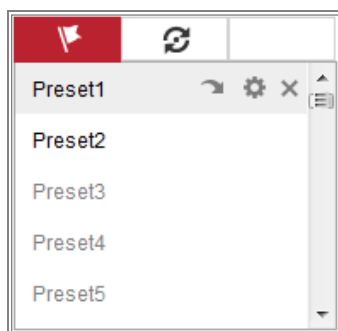
### ● Wywoływanie ustawienia wstępnego:

Ta funkcja umożliwia skierowanie kamery na wstępnie określoną scenę ręcznie lub po wystąpieniu określonego zdarzenia.

Zdefiniowane ustawienie wstępne można wywołać w dowolnej chwili, aby skierować kamerę na odpowiednią scenę.

W panelu sterowania PTZ wybierz zdefiniowane ustawienie wstępne z listy i kliknij przycisk , aby wywołać ustawienie wstępne.

Można też wybrać pozycję na liście ustawień wstępnych przy użyciu myszy komputerowej lub wpisać numer w celu wywołania odpowiedniego ustawienia wstępnego.





Rysunek 4–5 Wywoływanie ustawienia wstępnego

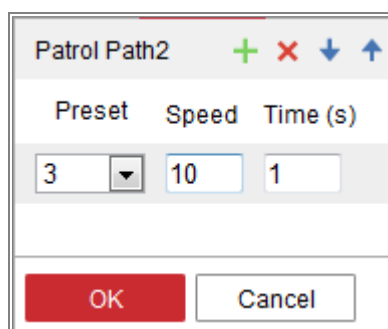
## 4.4.3 Konfigurowanie/wywoływanie patrolu

### **Uwaga:**




Patrol można ustawić pod warunkiem, że skonfigurowano co najmniej dwa ustawienia wstępne.

### **Kroki:**

1. Kliknij przycisk , aby wyświetlić okno konfiguracji patroli.
2. Wybierz numer ścieżki i kliknij przycisk , aby dodać skonfigurowane ustawienia wstępne.
3. Wybierz ustawienie wstępne i wprowadź czas trwania i szybkość patrolu.
4. Kliknij przycisk OK, aby zapisać pierwsze ustawienie wstępne.
5. Wykonaj powyższe kroki, aby dodać inne ustawienia wstępne.



Rysunek 4–6 Dodawanie ścieżki patrolu

6. Kliknij przycisk **OK**, aby zapisać patrol.
7. Kliknij przycisk , aby rozpocząć patrol, i kliknij przycisk  w celu zatrzymania patrolu.
8. (Opcjonalnie) Kliknij przycisk , aby usunąć patrol.

# Rozdział 5 Konfiguracja kamery sieciowej

## 5.1 Konfigurowanie parametrów lokalnych

### **Cel:**

Konfiguracja lokalna dotyczy parametrów podglądu na żywo, plików nagrań i wykonanych zdjęć. Pliki nagrań i wykonane zdjęcia są zapisywane i pobierane przy użyciu przeglądarki internetowej, dlatego ich ścieżki zapisu wskazują lokalizacje na komputerze, na którym jest uruchomiona przeglądarka.

### **Kroki:**

1. Przejdź do interfejsu konfiguracji lokalnej, wybierając opcje: **Configuration >**

#### **Local.**

Live View Parameters	
Protocol	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> MULTICAST <input type="radio"/> HTTP
Play Performance	<input type="radio"/> Shortest Delay <input checked="" type="radio"/> Balanced <input type="radio"/> Fluent
Rules	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Auto Start Live View	<input type="radio"/> Yes <input checked="" type="radio"/> No
Image Format	<input checked="" type="radio"/> JPEG <input type="radio"/> BMP
Fire Point	<input type="checkbox"/> Locate Highest Te... <input type="checkbox"/> Frame Fire Point

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

Picture and Clip Settings	
Save snapshots in live view to	<input type="text" value="C:\Users\yanjiamin\Web\CaptureFiles"/> <input type="button" value="Browse"/> <input type="button" value="Open"/>
Save snapshots when playback to	<input type="text" value="C:\Users\yanjiamin\Web\PlaybackPics"/> <input type="button" value="Browse"/> <input type="button" value="Open"/>
Save clips to	<input type="text" value="C:\Users\yanjiamin\Web\PlaybackFiles"/> <input type="button" value="Browse"/> <input type="button" value="Open"/>

Live View Parameters				
Protocol	<input checked="" type="radio"/> TCP	<input type="radio"/> UDP	<input type="radio"/> MULTICAST	<input type="radio"/> HTTP
Play Performance	<input type="radio"/> Shortest Delay	<input checked="" type="radio"/> Balanced	<input type="radio"/> Fluent	
Rules	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable		
Auto Start Live View	<input type="radio"/> Yes	<input checked="" type="radio"/> No		
Image Format	<input checked="" type="radio"/> JPEG	<input type="radio"/> BMP		
Display Temperature Info.	<input type="radio"/> Yes	<input checked="" type="radio"/> No		
Display Temperature Info. on Capt...	<input type="radio"/> Yes	<input checked="" type="radio"/> No		

Rysunek 5–1 Konfiguracja lokalna

## 2. Skonfiguruj następujące ustawienia:

- **Live View Parameters:** ustaw typ protokołu i wydajność podglądu na żywo.
  - ◆ **Protocol Type:** Do wyboru dostępne są opcje: TCP, UDP, MULTICAST i HTTP.
 

**TCP:** Protokół ten umożliwia bezstratne strumieniowanie danych i zapewnia wysoką jakość obrazu wideo, jednak może powodować opóźnienia podczas transmisji w czasie rzeczywistym.

**UDP:** Zapewnia przesyłanie strumieni audio i wideo w czasie rzeczywistym.

**HTTP:** Zapewnia przesyłanie sygnału o takiej samej jakości, jak podczas korzystania z protokołu TCP i nie wymaga przy tym ustawiania określonych portów do strumieniowania w pewnych środowiskach sieciowych.

**MULTICAST:** Zalecane jest wybranie typu MCAST, jeżeli używana jest funkcja Multicast. Aby uzyskać więcej informacji na temat multiemisji, zobacz *Sekcję 6.1.1*.
  - ◆ **Play Performance:** Ustaw jedną z dwóch opcji działania odtwarzania: „Shortest Delay” lub „Auto”.
  - ◆ **Rules:** To ustawienie dotyczy reguł w przeglądarce lokalnej. Włącz lub wyłącz ustawienie, aby wyświetlić lub ukryć kolorowe znaczniki po wyzwoleniu detekcji ruchu, twarzy lub wtargnięcia. Na przykład po włączeniu reguł i funkcji detekcji twarzy każda wykryta twarz będzie oznaczana zielonym prostokątem w podglądzie na żywo.
  - ◆ **Image Format:** wybierz format obrazu dla wykonywania zdjęć.

- ◆ **Fire Point:** Dostępne są ustawienia **Locate Highest Temperature Point** i **Frame Fire Point**. Obszar o najwyższej temperaturze można wyróżnić punktem lub ramką.
- ◆ **Display Temperature Info.:** włączanie lub wyłączenie funkcji wyświetlania temperatury i skonfigurowanej reguły pomiaru temperatury.
- ◆ **Display Temperature Info. on Capture:** włączanie lub wyłączenie funkcji wyświetlania temperatury na wykonanym zdjęciu.
- **Record File Settings:** Ustaw ścieżkę zapisu nagranych plików wideo. To ustawienie dotyczy plików nagranych przy użyciu przeglądarki internetowej.
- ◆ **Record File Size:** Wybierz rozmiar pakietu ręcznie nagranych i pobranych plików wideo 256 MB, 512 MB lub 1 GB. Maksymalny rozmiar pliku nagrania będzie zgodny z wybranym ustawieniem.
- ◆ **Save record files to:** Ustaw ścieżkę zapisu ręcznie nagranych plików wideo.
- ◆ **Save downloaded files to:** ustaw ścieżkę zapisu pobranych plików wideo w trybie odtwarzania.
- **Picture and Clip Settings:** Ustaw ścieżkę zapisu zarejestrowanych zdjęć i przyciętych plików wideo. To ustawienie dotyczy zdjęć wykonanych przy użyciu przeglądarki internetowej.
- ◆ **Save snapshots in live view to:** ustaw ścieżkę zapisu ręcznie wykonanych zdjęć w podglądzie na żywo.
- ◆ **Save snapshots when playback to:** ustaw ścieżkę zapisu wykonanych zdjęć w trybie odtwarzania.
- ◆ **Save clips to:** ustaw ścieżkę zapisu przyciętych plików wideo w trybie odtwarzania.

**Uwaga:** Można kliknąć przycisk **Browse**, aby zmienić katalog zapisywania klipów i zdjęć, i kliknąć przycisk **Open** w celu otwarcia ustawionego folderu do zapisu klipów i zdjęć.

3. Kliknij przycisk „**Save**“, aby zapisać ustawienia.

## 5.2 Konfigurowanie ustawień systemowych

### *Cel:*

Poniższe instrukcje dotyczą konfigurowania ustawień systemowych w oknach takich jak Ustawienia systemowe, Konserwacja, Zabezpieczenia i Zarządzanie użytkownikami.

### 5.2.1 Konfigurowanie podstawowych informacji

Przejdź do interfejsu informacji o urządzeniu, wybierając opcje: **Configuration > System > System Settings > Basic Information**.

W oknie **Informacje podstawowe** można edytować ustawienia Device Name i Device No. Wyświetlane są inne informacje o kamerze sieciowej takie jak jej model, numer seryjny, wersja oprogramowania sprzętowego, wersja kodowania, liczba kanałów, liczba dysków twardej, numer wejścia alarmowego i numer wyjścia alarmowego. Informacje wyświetlane w tej części interfejsu nie mogą zostać zmienione. Stanowią one istotny punkt odniesienia podczas przyszłych zabiegów konserwacyjnych lub podczas modyfikacji urządzenia.

Basic Information	Time Settings	RS232	RS485	DST
Device Name	<input type="text" value="IP CAMERA"/>			
Device No.	<input type="text" value="88"/>			
Model	<input type="text" value="XX-XXXXXXXXXX"/>			
Serial No.	<input type="text" value="XX-XXXXXXXXXXXXXXXXXXXXXXXXXXXX"/>			
Firmware Version	<input type="text" value="Vx.x.xbuild xxxxxx"/>			
Encoding Version	<input type="text" value="Vx.xbuild xxxxxx"/>			
Web Version	<input type="text" value="Vx.x.xbuild xxxxxx"/>			
Plugin Version	<input type="text" value="Vx.x.x.x"/>			
Number of Channels	<input type="text" value="1"/>			
Number of HDDs	<input type="text" value="0"/>			
Number of Alarm Input	<input type="text" value="0"/>			
Number of Alarm Output	<input type="text" value="0"/>			
<input type="button" value="Save"/>				

Rysunek 5–2 Informacje podstawowe

### Uaktualnienie w trybie online

W przypadku niektórych modeli kamer, gdy zainstalowana jest karta pamięci, można kliknąć przycisk **Update** po prawej stronie obok pola tekstowego **Firmware Version**, aby sprawdzić, czy dostępna jest nowa wersja. Jeżeli dostępna jest nowa wersja, numer wersji jest wyświetlany w polu tekstowym **New Version** i można kliknąć przycisk **Upgrade**, aby uaktualnić oprogramowanie układowe kamery.

<i>Firmware Version</i>	<input type="text" value="VX.X.X build XXXXXX"/>	<input type="button" value="Update"/>
<i>New Version</i>	<input type="text" value="VX.X.X build XXXXXX"/>	<input type="button" value="Upgrade"/>

Rysunek 5–3 Uaktualnienie w trybie online

**Uwaga:** Nie wolno wyłączać zasilania kamery podczas uaktualniania. Podczas uaktualniania kamera może być niedostępna. Należy poczekać 1–2 minuty na ukończenie uaktualnienia.

## 5.2.2 Konfigurowanie ustawień czasu

### Cel:

Instrukcje w tej sekcji umożliwiają skonfigurowanie synchronizacji czasu i ustawień czasu letniego.

### Kroki:

1. Wyświetl okno ustawień czasu (**Configuration > System > System Settings > Time Settings**).

Rysunek 5–4 Ustawienia czasu


2. Wybierz strefę czasową w swojej lokalizacji z menu rozwijanego.
3. Skonfiguruj ustawienia protokołu NTP.
  - (1) Kliknij, aby włączyć funkcję **NTP**.
  - (2) Skonfiguruj następujące ustawienia:
    - Server Address:** adres IP serwera NTP.
    - NTP Port:** port serwera NTP.
    - Interval:** interwał czasowy między dwiema operacjami synchronizacji z serwerem NTP.

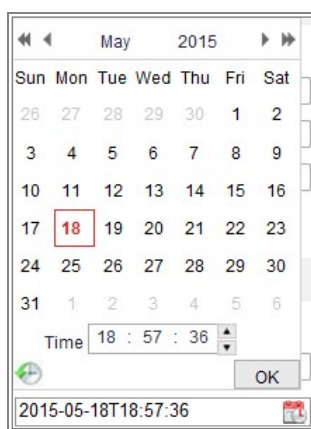


- (3) (Opcjonalnie) Można kliknąć przycisk **Test**, aby przetestować funkcję synchronizacji czasu z serwerem NTP.

Rysunek 5–5 Synchronizacja czasu z serwerem NTP

**Uwaga:** Jeżeli kamera jest połączona z siecią publiczną, należy korzystać z serwera NTP z funkcją synchronizacji czasu, takiego jak serwer National Time Center (adres IP: 210.72.145.44). Jeżeli kamera jest skonfigurowana w dostosowanej sieci, oprogramowanie NTP umożliwia ustanowienie serwera NTP używanego do synchronizacji czasu.

- Skonfiguruj ręczną synchronizację czasu.
  - (1) Zaznacz pole wyboru **Manual Time Sync**, w celu włączenia funkcji ręcznej synchronizacji czasu.
  - (2) Kliknij ikonę , aby wybrać datę i godzinę z kalendarza.
  - (3) (Opcjonalnie) Można zaznaczyć opcję **Sync. with computer time**, aby synchronizować czas urządzenia z komputerem lokalnym.



Rysunek 5–6 Ręczna synchronizacja czasu

- Kliknij przycisk „**Save**”, aby zapisać ustawienia.


### 5.2.3 Konfigurowanie ustawień RS485

**Cel:**

Port szeregowy RS485 jest używany do sterowania PTZ kamerą. Przed rozpoczęciem sterowania ruchem PTZ kamery należy najpierw skonfigurować parametry PTZ.

**Kroki:**

1. Przejdź do interfejsu ustawień portu RS-485, wybierając opcje: **Configuration > System > System Settings > RS485**.

Basic Information	Time Settings	RS232	RS485	DST
<b>RS485</b>				
Baud Rate	9600			
Data Bit	8			
Stop Bit	1			
Parity	None			
Flow Ctrl	None			
PTZ Protocol	PELCO-D			
PTZ Address	0			
				

Rysunek 5–7 Ustawienia RS-485

2. Skonfiguruj parametry RS485 i kliknij przycisk **Save**, aby zapisać ustawienia.

Domyślnie skonfigurowane są opcje Baud Rate z ustawieniem 9600 b/s, Data Bit z ustawieniem 8, Stop Bit z ustawieniem 1 oraz Parity i Flow Control z ustawieniem None.

**Uwaga:** Parametry Szybkość transmisji bitów, Protokół PTZ i Adres PTZ powinny być takie same, jak parametry kamery PTZ.

## 5.2.4 Konfigurowanie ustawień czasu letniego

### **Cel:**

Czas letni (DST, Daylight Saving Time) umożliwia lepsze wykorzystanie naturalnego światła dziennego dzięki przesunięciu zegara o jedną godzinę do przodu w miesiącach letnich i do tyłu w okresie zimowym.

Należy skonfigurować czas letni zgodnie z wymaganiami.

### **Kroki:**

1. Wyświetl okno konfiguracji czasu letniego.

**Configuration > System > System Settings > DST**

Rysunek 5–8 Ustawienia czasu letniego (DST)

2. Wybierz godzinę początkową i godzinę końcową.
3. Wybierz ustawienie DST Bias.
4. Kliknij przycisk **Save**, aby aktywować ustawienia.

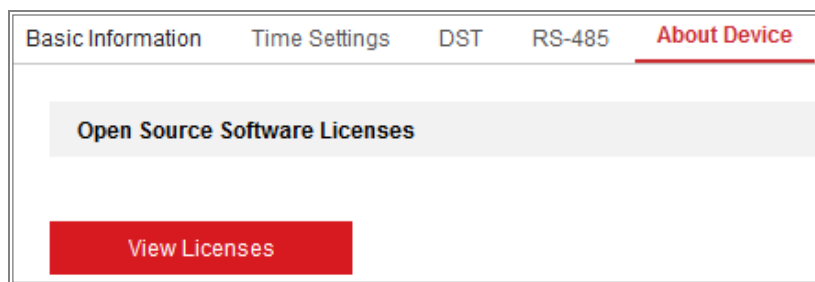
## 5.2.5 Wyświetlanie licencji

### **Cel:**

Można wyświetlić licencje oprogramowania typu Open Source, związane z kamerą internetową.

### **Kroki:**

1. Wyświetl informacje o urządzeniu: **Configuration > System > System Settings > About Device**.
2. Kliknij przycisk **View Licenses**.



Rysunek 5–9 Informacje o urządzeniu

## 5.3 Konserwacja

### 5.3.1 Uaktualnienie i konserwacja

#### **Cel:**

Korzystając z okna uaktualnienia i konserwacji, można wykonywać operacje takie jak ponowne uruchomienie, częściowe przywrócenie, przywrócenie ustawień domyślnych, eksportowanie/importowanie plików konfiguracyjnych i uaktualnienie urządzenia.

Przejdź do interfejsu konserwacji, wybierając opcje: **Configuration > System > Maintenance > Upgrade & Maintenance**.

- **Reboot:** ponowne uruchomienie urządzenia.
- **Restore:** resetowanie wszystkich parametrów z wyjątkiem parametrów IP i informacji o użytkowniku i przywrócenie ustawień domyślnych.
- **Default:** przywrócenie fabrycznych ustawień domyślnych wszystkich parametrów.

**Uwaga:** Po przywróceniu ustawień domyślnych przywracany jest również domyślny adres IP, dlatego należy zachować ostrożność podczas wykonywania tej operacji.

- **Export/Import Config. File:** plik konfiguracyjny ułatwia zbiorcze konfigurowanie wielu kamer.

#### **Kroki:**

1. Kliknij przycisk **Device Parameters**, aby wyeksportować bieżący plik konfiguracyjny i zapisać go w określonej lokalizacji.
2. Kliknij przycisk **Browse**, aby wybrać zapisany plik konfiguracyjny, a następnie kliknij przycisk **Import** w celu rozpoczęcia importowania tego pliku.

**Uwaga:** Po zaimportowaniu pliku konfiguracyjnego należy ponownie uruchomić kamerę.

- **Upgrade:** uaktualnienie urządzenia do określonej wersji.

**Kroki:**

1. Wybierz oprogramowanie układowe lub katalog oprogramowania układowego, aby zlokalizować plik uaktualnienia.

Oprogramowania: zlokalizuj dokładnie ścieżkę pliku uaktualnienia.

Katalog Oprogramowania: wymagany jest tylko katalog, w którym znajduje się plik uaktualnienia.

2. Kliknij przycisk **Browse**, aby wybrać lokalny plik uaktualnienia, a następnie kliknij przycisk Upgrade w celu rozpoczęcia zdalnego uaktualnienia.

**Uwaga:** Proces uaktualniania potrwa od 1 do 10 minut. Nie wolno odłączać zasilania kamery podczas tego procesu. Kamera jest automatycznie ponownie uruchamiana po uaktualnieniu.

## 5.3.2 Dziennik

**Cel:**

Operacje, alarmy, wyjątki i informacje dotyczące kamery można zapisywać w plikach rejestru. W razie potrzeby pliki rejestru można eksportować.

**Zanim rozpocznie:**

Skonfiguruj magazyn sieciowy dla kamery lub zainstaluj kartę SD w kamerze.

**Kroki:**

1. Wyświetl okno wyszukiwania w rejestrze: **Configuration > System > Maintenance >**

**Log.**

Upgrade & Maintenance <b>Log</b>						
Major Type	All Types	Minor Type	All Types			
Start Time	2015-06-04 00:00:00	End Time	2015-06-04 23:59:59	Search		
Log List						Export
No.	Time	Major Type	Minor Type	Channel No.	Local/Remote User	Remote Host IP

Rysunek 5–10 Okno wyszukiwania w dzienniku

2. Skonfiguruj kryteria wyszukiwania w dzienniku, takie jak typ główny, typ podrzędny, godzina początkowa i godzina końcowa.
3. Kliknij przycisk **Search**, aby rozpocząć wyszukiwanie w plikach rejestru. Pasujące pliki rejestru zostaną wyświetlone na liście.

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

Total 614 Items << < 1/7 > >>

Rysunek 5–11 Wyszukiwanie w dzienniku


4. Aby wyeksportować pliki rejestru, kliknij przycisk **Export** w celu zapisania tych plików.

### 5.3.3 Usługa systemowa

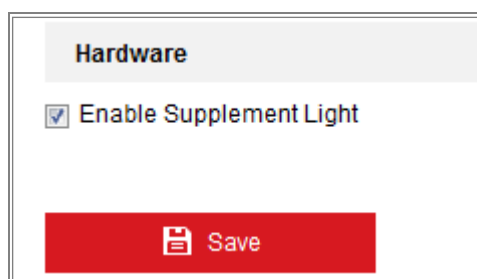
#### **Cel:**

Te ustawienia systemowe dotyczą funkcji sprzętowych obsługiwanych przez kamerę. Obsługiwane funkcje są zależne od kamery. W kamerach uwzględniono automatyczne podgrzewanie, oświetlenie LED podczerwienią, oświetlenie pomocnicze, automatyczną regulację tylnej płaszczyzny ogniskowania (ABF), automatyczne usuwanie mgły lub wskaźnik stanu, dlatego można włączyć lub wyłączyć odpowiednią funkcję zależnie od wymagań.

**Automatic De-icing:** Można zaznaczyć pole wyboru, aby włączyć funkcję automatycznego podgrzewania urządzenia. Podgrzewanie w celu usunięcia oblodzenia jest obsługiwane tylko w przypadku zastosowania zasilania POE+, 24VAC lub 12VDC.

**ABF:** gdy funkcja ABF jest włączona, można kliknąć przycisk  na panelu sterowania PTZ, aby skorzystać z pomocniczej regulacji ostrości.

**Supplement Light:** w przypadku niektórych modeli można zaznaczyć pole wyboru **Enable Supplement Light**, aby ponownie uruchomić system i włączyć oświetlenie pomocnicze.



Rysunek 5–12 Włączanie oświetlenia pomocniczego

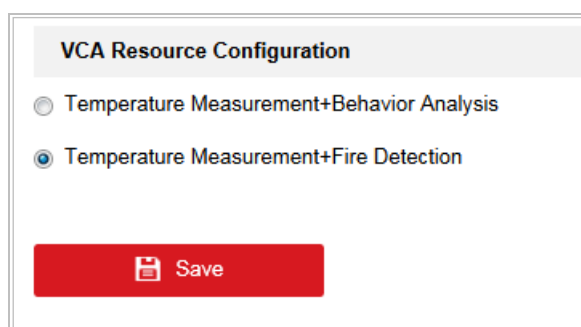
### 5.3.4 Typ zasobu VCA

**Cel:**

Zasób VCA umożliwia włączanie określonych funkcji VCA zgodnie z wymaganiami, gdy dostępnych jest kilka funkcji VCA. Ułatwia to przydzielanie większej ilości zasobów do żądanych funkcji.

**Kroki:**

1. Wyświetl okno typu zasobu VCA: **Configuration > System > Maintenance > VCA Resource Type.**



Rysunek 5–13 Typ zasobu VCA

2. Zaznacz to pole wyboru, aby włączyć typ zasobu VCA.
3. Kliknij **Save**. Ponowne uruchomienie jest wymagane po skonfigurowaniu funkcji Zasób VCA.

**Uwagi:**

- Funkcja Zasób VCA jest zależna od modelu kamery.
- Ta funkcja nie jest obsługiwana przez niektóre modele kamer.

## 5.4 Ustawienia zabezpieczeń

W oknie zabezpieczeń można skonfigurować parametry takie jak Uwierzytelnianie, Wizyta anonimowa, Filtr adresów IP i Usługa zabezpieczeń.

### 5.4.1 Uwierzytelnianie

**Cel:**

Funkcja ta służy do ochrony danych strumienia podglądu na żywo.

**Kroki:**

1. Przejdź do interfejsu uwierzytelniania, wybierając opcje: **Configuration > System > Security > Authentication**.



Rysunek 5–14 Uwierzytelnianie RTSP

2. Wybierz dla opcji **RTSP Authentication** typ **basic** lub **disable** z listy rozwijanej, aby włączyć lub wyłączyć uwierzytelnianie RTSP.

**Uwaga:** Jeżeli uwierzytelnianie RTSP zostanie wyłączone, każdy może uzyskać dostęp do strumienia wideo przy użyciu protokołu RTSP i adresu IP.

3. Kliknij przycisk „**Save**“, aby zapisać ustawienia.



## 5.4.2 Filtr adresów IP

### Cel:

Ta funkcja umożliwia kontrolę dostępu.

### Kroki:

- Wyświetl okno Filtr adresów IP: **Configuration > System > Security > IP Address**

#### Filter

The screenshot shows the 'IP Address Filter' configuration interface. At the top, there are three tabs: 'Authentication', 'IP Address Filter' (which is active and highlighted in red), and 'Security Service'. Below the tabs, there is a checkbox labeled 'Enable IP Address Filter' which is checked. Underneath, there is a label 'IP Address Filter Type' followed by a dropdown menu currently showing 'Forbidden'. Below this is a table with a header row containing 'No.' and 'IP'. To the right of the table are three buttons: 'Add', 'Modify', and 'Delete'.

Rysunek 5–15 Filtr adresów IP

- Zaznacz pole wyboru „**Enable IP Address Filter**”.
- Wybierz filtr adresów IP z listy rozwijanej IP Address Filter. Dostępne są ustawienia **Forbidden** i **Allowed**.
- Ustaw listę filtrowanych adresów IP.
  - Dodawanie adresu IP

### Kroki:

- Kliknij przycisk **Add**, aby dodać adres IP.
- Wprowadź adres IP.

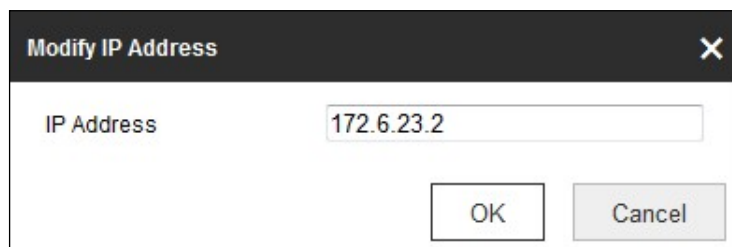
The screenshot shows a dialog box titled 'Add IP Address'. The dialog has a title bar with the text 'Add IP Address' and a close button (X). Inside the dialog, there is a label 'IP Address' followed by a text input field containing the IP address '172.6.23.2'. To the right of the input field is a green checkmark icon. At the bottom of the dialog, there are two buttons: 'OK' and 'Cancel'.

Rysunek 5–16 Dodawanie adresu IP

- Kliknij przycisk „**OK**”, aby zakończyć dodawanie.
  - Modyfikowanie adresu IP

**Kroki:**

- (1) Kliknij lewym przyciskiem myszy adres IP na liście filtrowania, a następnie kliknij przycisk „**Modify**”.
- (2) Zmień adres IP znajdujący się w polu tekstowym.



Rysunek 5–17 Modyfikowanie adresu IP

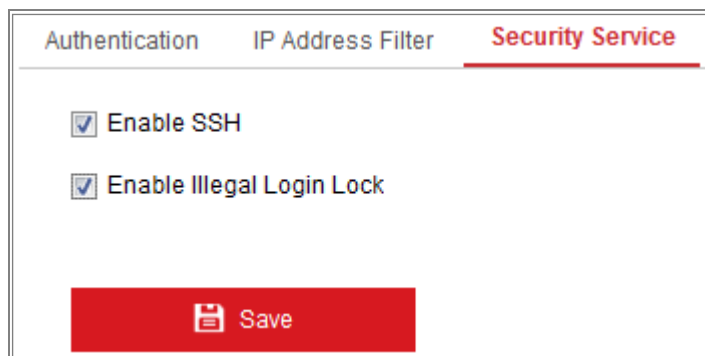
- (3) Kliknij przycisk „**OK**”, aby zakończyć modyfikowanie.
  - Usuń adres IP lub adresy IP.  
Wybierz adresy IP i kliknij przycisk **Delete**.
5. Kliknij przycisk „**Save**”, aby zapisać ustawienia.

### 5.4.3 Usługa zabezpieczeń

Aby umożliwić zdalne logowanie i zapewnić lepszą ochronę przesyłanych danych, w kamerze uwzględniono usługę zabezpieczeń.

**Kroki:**

1. Wyświetl okno konfiguracji usługi zabezpieczeń: **Configuration > System > Security > Security Service**.



Rysunek 5–18 Usługa zabezpieczeń

2. Zaznacz pole wyboru **Enable SSH**, aby włączyć zabezpieczenia przesyłanych danych, i wyczyść to pole wyboru w celu wyłączenia zabezpieczeń SSH.
3. Zaznacz pole wyboru **Enable Illegal Login Lock**, aby adres IP był blokowany, jeżeli użytkownik admin wprowadzi nieprawidłową nazwę użytkownika/hasło siedem razy (pięć razy w przypadku gościa/operatora).

**Uwaga:** Jeżeli adres IP zostanie zablokowany, próbę zalogowania się można podjąć dopiero po 30 minutach.

## 5.5 Zarządzanie użytkownikami

### 5.5.1 Zarządzanie użytkownikami

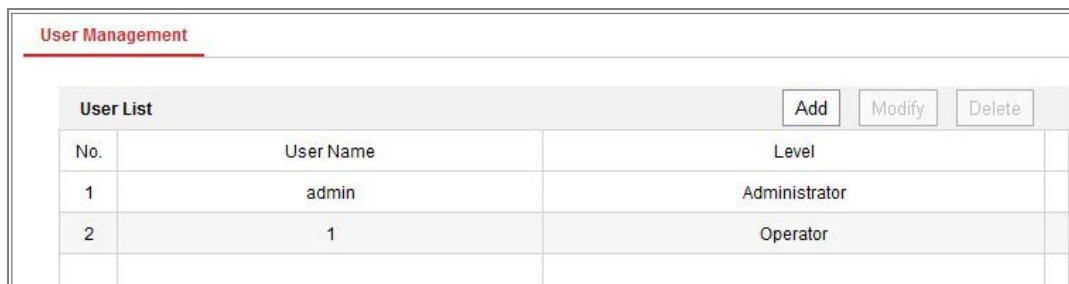
**Cel:**

Użytkownik admin może dodawać, usuwać lub modyfikować konta użytkowników i udzielać im różnych uprawnień. Zdecydowanie zalecamy prawidłowe zarządzanie kontami i uprawnieniami użytkowników.

**Kroki:**

1. Przejdź do interfejsu zarządzania użytkownikami, wybierając opcje:

**Configuration > System > User Management**



User Management		
User List		
		Add Modify Delete
No.	User Name	Level
1	admin	Administrator
2	1	Operator

Rysunek 5–19 Zarządzanie użytkownikami

- **Dodawanie użytkownika**

Domyślnie użytkownik *admin* ma wszystkie uprawnienia i może tworzyć/modyfikować/usuwać inne konta.

Nie można usunąć użytkownika *admin* i można tylko zarządzać hasłem użytkownika *admin*.

**Kroki:**

1. Kliknij przycisk **Add**, aby dodać użytkownika.
2. Wprowadź nazwę użytkownika w polu **User Name**, wybierz ustawienie **Level** i wprowadź hasło w polu **Password**.

**Uwagi:**

- Można utworzyć do 31 kont użytkowników.
- Użytkownicy na poszczególnych poziomach mają różne uprawnienia domyślne. Dostępne są ustawienia Operator i Użytkownik.



**ZALECANE JEST STOSOWANIE SILNEGO HASŁA** — zdecydowanie zalecane jest utworzenie własnego silnego hasła (co najmniej osiem znaków należących do co najmniej trzech z następujących kategorii: wielkie litery, małe litery, cyfry i znaki specjalne) w celu zapewnienia lepszej ochrony urządzenia. Zalecane jest również regularne resetowanie hasła. Zwłaszcza w systemie z restrykcyjnymi zabezpieczeniami resetowanie hasła co miesiąc lub co tydzień zapewnia lepszą ochronę urządzenia.

3. Można zaznaczyć lub wyczyścić uprawnienia dla nowego użytkownika.
4. Kliknij przycisk **OK**, aby ukończyć dodawanie użytkownika.

Rysunek 5–20 Dodawanie użytkownika


- **Modyfikowanie użytkownika**

**Kroki:**

1. Kliknij lewym przyciskiem myszy, aby wybrać użytkownika z listy, i kliknij przycisk

**Modify.**

2. Zmień ustawienia **User Name**, **Level** i **Password**.

 **ZALECANE JEST STOSOWANIE SILNEGO HASŁA** — zdecydowanie zalecane jest utworzenie własnego silnego hasła (co najmniej osiem znaków należących do co najmniej trzech z następujących kategorii: wielkie litery, małe litery, cyfry i znaki specjalne) w celu zapewnienia lepszej ochrony urządzenia. Zalecane jest również regularne resetowanie hasła. Zwłaszcza w systemie z restrykcyjnymi zabezpieczeniami resetowanie hasła co miesiąc lub co tydzień zapewnia lepszą ochronę urządzenia.

3. Można zaznaczyć lub wyczyścić uprawnienia.

4. Kliknij przycisk **OK**, aby ukończyć modyfikowanie użytkownika.

Rysunek 5–21 Modyfikowanie użytkownika

- **Usuwanie użytkownika**

**Kroki:**

1. Kliknij, aby wybrać użytkownika przeznaczonego do usunięcia, i kliknij przycisk **Delete**.
2. Kliknij przycisk **OK** w oknie dialogowym, aby potwierdzić usunięcie.

## 5.5.2 Użytkownicy połączeni z urządzeniem

**Cel:**

W interfejsie tym wyświetlane są informacje o użytkownikach, którzy aktualnie korzystają z urządzenia za pośrednictwem interfejsu sieciowego. Na liście użytkowników wyświetlane są informacje takie, jak nazwa użytkownika, poziom uprawnień, adres IP i czas obsługi urządzenia.

Kliknij przycisk „**Refresh**“, aby odświeżyć listę.

User Management		<u>Online Users</u>		
User List				Refresh
No.	User Name	Level	IP Address	User Operation Time
1	admin	Administrator	10.16.2.101	2015-11-16 10:57:55

Rysunek 5–22 Widok użytkowników w trybie online

## Rozdział 6 Ustawienia sieciowe

### ***Cel:***

Instrukcje podane w tym Rozdziale dotyczą konfigurowania ustawień podstawowych i zaawansowanych.

### **6.1 Konfigurowanie ustawień podstawowych**

#### ***Cel:***

Postępując zgodnie z instrukcjami podanymi w tej sekcji, można skonfigurować parametry takie jak TCP/IP, DDNS, PPPoE, Port i translacja NAT.

#### **6.1.1 Konfigurowanie ustawień protokołu TCP/IP**

##### ***Cel:***

Aby obsługiwać kamerę za pośrednictwem sieci, należy prawidłowo skonfigurować ustawienia protokołów TCP/IP. Kamera obsługuje zarówno protokół IPv4, jak i protokół IPv6. Obie wersje można skonfigurować równocześnie, nie powodując ich konfliktu. Należy skonfigurować co najmniej jedną wersję protokołu IP.

##### ***Kroki:***

1. Przejdź do interfejsu ustawień protokołu TCP/IP, wybierając opcje: „**Configuration**“ > „**Network**“ > „**Basic Settings**“ > „**TCP/IP**“



The screenshot shows a configuration window for TCP/IP settings. At the top, there are tabs for 'TCP/IP', 'DDNS', 'PPPoE', 'Port', and 'NAT'. The 'TCP/IP' tab is selected. The settings are as follows:

- NIC Type: Auto
- DHCP:
- IPv4 Address: 10.11.37.120 (with a Test button)
- IPv4 Subnet Mask: 255.255.255.0
- IPv4 Default Gateway: 10.11.37.254
- IPv6 Mode: Route Advertisement (with a View Route Advertisement button)
- IPv6 Address: ::
- IPv6 Subnet Mask: 0
- IPv6 Default Gateway: ::
- Mac Address: c0:56:e3:60:27:5d
- MTU: 1500
- Multicast Address: (empty)
- Enable Multicast Discovery:

Below these settings is a section for DNS Server:

- Preferred DNS Server: 8.8.8.8
- Alternate DNS Server: (empty)

At the bottom left, there is a red button labeled 'Save' with a floppy disk icon.

Rysunek 6–1 Ustawienia protokołu TCP/IP

2. Skonfiguruj podstawowe ustawienia sieciowe takie jak Typ karty sieciowej, Adres IPv4 lub IPv6, maska podsieci IPv4 lub IPv6, Brama domyślna IPv4 lub IPv6, MTU i Adres multiemisji.
3. (Opcjonalnie) Zaznacz pole wyboru **Enable Multicast Discovery**, aby umożliwić automatyczne wykrywanie kamery sieciowej w trybie online przez oprogramowanie klienckie przy użyciu protokołu multiemisji prywatnej w sieci LAN.
4. Skonfiguruj serwer DNS. Wprowadź preferowany i alternatywny serwer DNS.
5. Kliknij przycisk **Save**, aby zapisać powyższe ustawienia.

**Uwagi:**

- Prawidłowy zakres wartości MTU to 1280–1500.
- W trybie multiemisji szybkoobrotowa kamera kopułkowa prześle strumień na adres grupy multiemisji, dzięki czemu wielu klientów może jednocześnie uzyskać dostęp do strumienia, przesyłając żądanie uzyskania kopii na adres grupy multiemisji. Przed skorzystaniem z tej funkcji należy włączyć funkcję Multiemisja routera.

- Ustawienia zostaną uwzględnione po ponownym uruchomieniu.

## 6.1.2 Konfigurowanie ustawień usługi DDNS

### **Cel:**

Jeżeli w domyślnych ustawieniach sieciowych kamery uwzględniono obsługę protokołu PPPoE, można uzyskać dostęp do sieci przy użyciu usługi Dynamic DNS (DDNS).

### **Zanim rozpoczniesz:**

Przed skonfigurowaniem ustawień usługi DDNS kamery należy wykonać procedurę rejestracji na serwerze DDNS.

### **Kroki:**

1. Przejdź do interfejsu ustawień usługi DDNS, wybierając opcje: **Configuration > Network > Basic Settings > DDNS**.
2. Zaznacz pole wyboru „**Enable DDNS**” (Włącz DDNS), aby włączyć tę funkcję.
3. Wybierz ustawienie **DDNS Type**. Dostępne są dwa typy usług DDNS:  
„DynDNS” i „NO-IP”.

- DynDNS:

### **Kroki:**

- (1) Wprowadź adres serwera („**Server Address**”) usługi DynDNS (e.g. members.dyndns.org).
- (2) W polu tekstowym „**Domain**” wprowadź nazwę domeny otrzymaną ze strony DynDNS.
- (3) Wprowadź nazwę użytkownika („**User Name**”) i hasło („**Password**”) zarejestrowane na stronie DynDNS.
- (4) Kliknij przycisk **Save**, aby zapisać ustawienia.

The screenshot shows the DDNS configuration interface. At the top, there are tabs for 'TCP/IP', 'DDNS' (which is selected), 'PPPoE', 'Port', and 'NAT'. Below the tabs, there is a checkbox labeled 'Enable DDNS' which is checked. The 'DDNS Type' is set to 'DynDNS'. The 'Server Address' is 'members.dyndns.org' with a green checkmark. The 'Domain' is '123.dyndns.com' with a green checkmark. The 'User Name' is 'test' with a green checkmark. The 'Port' is '0'. The 'Password' and 'Confirm' fields are filled with dots and have green checkmarks. At the bottom, there is a red 'Save' button.

Rysunek 6–2 Ustawienia DynDNS

- NO-IP:

**Kroki:**

- (1) Wybierz ustawienie NO-IP opcji DDNS Type.

The screenshot shows the DDNS configuration interface with 'NO-IP' selected as the DDNS Type. The 'Server Address' is 'www.noip.com' with a green checkmark. The 'Domain', 'User Name', 'Password', and 'Confirm' fields are empty. At the bottom, there is a red 'Save' button.

Rysunek 6–3 Ustawienia NO-IP DNS

- (2) W polu Server Address wprowadź adres serwera [www.noip.com](http://www.noip.com)
- (3) Wprowadź zarejestrowaną nazwę w polu Nazwa domeny.
- (4) Wprowadź informacje w polach Nazwa użytkownika i Hasło.
- (5) Kliknij przycisk **Save**, aby wyświetlić kamerę z nazwą domeny.

**Uwaga:** Aby ustawienia zostały uwzględnione, należy ponownie uruchomić urządzenie.

### 6.1.3 Konfigurowanie ustawień protokołu PPPoE

#### Kroki:

1. Przejdź do interfejsu ustawień protokołu PPPoE, wybierając opcje: **Configuration > Network > Basic Settings > PPPoE**

Rysunek 6–4 Ustawienia funkcji PPPoE

2. Zaznacz pole wyboru „**Enable PPPoE**“, aby włączyć tę funkcję.
3. Wprowadź nazwę użytkownika („**User Name**“), hasło („**Password**“) i potwierdź hasło („**Confirm**“), aby uzyskać dostęp za pomocą protokołu PPPoE.

**Uwaga:** Nazwa użytkownika i Hasło powinny być przypisane przez usługodawcę internetowego.



- *W celu lepszej ochrony systemu i prywatności użytkownika przed zagrożeniami zdecydowanie zaleca się korzystanie z silnych haseł do zabezpieczenia wszystkich funkcji i urządzeń sieciowych. Należy wybrać własne hasło (co najmniej osiem znaków należących do co najmniej trzech z następujących kategorii: wielkie litery, małe litery, cyfry i znaki specjalne) w celu zapewnienia lepszej ochrony urządzenia.*
  - *Instalator i/lub użytkownik końcowy są zobowiązani do prawidłowego skonfigurowania wszystkich haseł i innych ustawień zabezpieczeń.*
4. Kliknij przycisk **Save**, aby zapisać ustawienia i zamknąć okno.

**Uwaga:** Ustawienia zostaną uwzględnione po ponownym uruchomieniu.

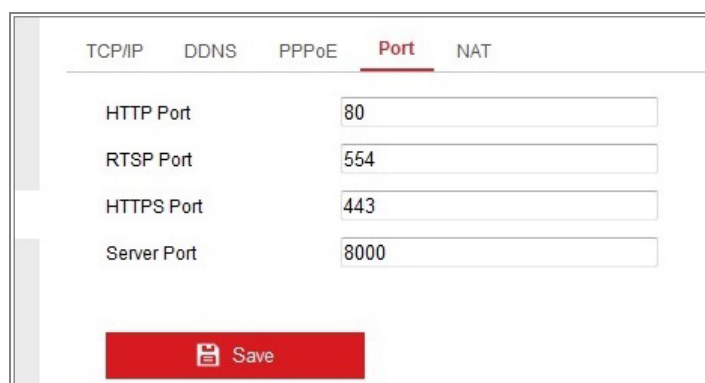
## 6.1.4 Konfigurowanie ustawień portów

### **Cel:**

Można ustawić numer portu kamery (np. portu HTTP, RTSP i HTTPS).

### **Kroki:**

1. Wyświetl okno Ustawienia portów (**Configuration > Network > Basic Settings > Port**).



	TCP/IP	DDNS	PPPoE	<b>Port</b>	NAT
HTTP Port				80	
RTSP Port				554	
HTTPS Port				443	
Server Port				8000	

Save

Rysunek 6–5 Ustawienia portów

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

**HTTP Port:** domyślny numer portu 80 można zmienić na dowolny numer, który nie jest zajęty.

**RTSP Port:** domyślny numer portu 554 można zmienić na dowolny numer z zakresu 1–65 535.

**HTTPS Port:** domyślny numer portu 443 można zmienić na dowolny numer, który nie jest zajęty.

**Server Port:** domyślny numer portu 8000 można zmienić na dowolny numer z zakresu 2000–65 535.

3. Kliknij przycisk „**Save**”, aby zapisać ustawienia.

**Uwaga:** Ustawienia zostaną uwzględnione po ponownym uruchomieniu.

## 6.1.5 Konfigurowanie ustawień translacji adresów sieciowych (NAT)

### Cel:

W oknie Translacja NAT można skonfigurować parametry funkcji UPnP™.

Universal Plug and Play (UPnP™) to architektura sieciowa zapewniająca zgodność różnego rodzaju sprzętu i oprogramowania sieciowego. Protokół UPnP ułatwia ustanawianie połączeń urządzeń oraz wdrażanie sieci w środowiskach domowych i firmowych.

Dzięki włączeniu funkcji translacji adresów sieciowych (NAT) nie ma potrzeby konfigurowania mapowania każdego portu, a kamera może zostać podłączona do sieci WAN za pośrednictwem routera.

### Kroki:

1. Wyświetl ustawienia translacji NAT. **Configuration > Network > Basic Settings > NAT.**
2. Zaznacz pole wyboru „Enable UPnP™” (Włącz UPnP™), aby włączyć funkcję UPnP.
3. Wybierz pseudonim kamery lub użyj nazwy domyślnej.
4. Wybierz tryb mapowania portów. Dostępne są ustawienia Manual i Auto.  
W przypadku ręcznego mapowania portów można dostosować wartość portu zewnętrznego.
5. Kliknij przycisk „**Save**”, aby zapisać ustawienia.

Port Type	External Port	External IP Address	Internal Port
HTTP	80	0.0.0.0	80
RTSP	554	0.0.0.0	554
Server Port	8000	0.0.0.0	8000

Rysunek 6–6 Ustawienia funkcji UPnP

## 6.2 Konfigurowanie ustawień zaawansowanych

### **Cel:**

Postępując zgodnie z instrukcjami podanymi w tej sekcji, można skonfigurować parametry takie jak SNMP, FTP, E-mail, HTTPS, QoS i 802.1x.

### 6.2.1 Konfigurowanie ustawień protokołu SNMP

#### **Cel:**

Konfigurując odpowiednio funkcję SNMP, można uzyskać informacje dotyczące stanu kamery, parametrów i alarmów oraz zdalnie zarządzać kamerą połączoną z siecią.

#### **Zanim rozpocznie:**

Przed skonfigurowaniem protokołu SNMP należy pobrać oprogramowanie SNMP i uzyskać informacje dotyczące kamery za pośrednictwem portu SNMP. Skonfigurowanie ustawienia Adres pułapki umożliwia kamerze wysłanie wiadomości dotyczących zdarzeń i wyjątków alarmowych do centrum monitoringu.

**Uwaga:** Wybrana wersja protokołu SNMP powinna odpowiadać wersji protokołu w oprogramowaniu SNMP. Należy użyć odpowiedniej wersji zależnie od wymaganego poziomu ochrony. Wersja SNMP v1 nie zapewnia zabezpieczeń, a w przypadku wersji SNMP v2 należy podać hasło, aby uzyskać dostęp. Wersja SNMP v3 zapewnia szyfrowanie. Aby korzystać z trzeciej wersji, należy włączyć obsługę protokołu HTTPS.



- *W celu lepszej ochrony systemu i prywatności użytkownika przed zagrożeniami zdecydowanie zaleca się korzystanie z silnych haseł do zabezpieczenia wszystkich funkcji i urządzeń sieciowych. Należy wybrać własne hasło (co najmniej osiem znaków należących do co najmniej trzech z następujących kategorii: wielkie litery, małe litery, cyfry i znaki specjalne) w celu zapewnienia lepszej ochrony urządzenia.*
- *Instalator i/lub użytkownik końcowy są zobowiązani do prawidłowego skonfigurowania wszystkich haseł i innych ustawień zabezpieczeń.*

**Kroki:**

1. Przejdź do interfejsu ustawień protokołu SNMP, wybierając opcje: **Configuration > Network > Advanced Settings > SNMP.**

The screenshot displays the SNMP configuration page with a navigation bar at the top containing 'SNMP', 'FTP', 'Email', 'HTTPS', 'QoS', and '802.1x'. The main content is organized into three sections:

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

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

Rysunek 6–7 Ustawienia funkcji SNMP



2. Zaznacz pole wyboru Enable SNMPv1, Enable SNMP v2c, Enable SNMPv3, aby włączyć odpowiednią funkcję.
3. Skonfiguruj ustawienia protokołu SNMP.

**Uwaga:** Ustawienia oprogramowania SNMP powinny być takie same, jak ustawienia skonfigurowane w tym oknie.

4. Kliknij przycisk **Save**, aby zapisać i potwierdzić ustawienia.

**Uwagi:**

- Ustawienia zostaną uwzględnione po ponownym uruchomieniu.
- Aby ograniczyć ryzyko nieautoryzowanego ujawnienia informacji, należy włączyć opcję SNMP v3 zamiast SNMP v1 lub v2.

## 6.2.2 Konfigurowanie ustawień serwera FTP

**Cel:**

Można skonfigurować informacje dotyczące serwera FTP, aby umożliwić przekazywanie wykonanych zdjęć do serwera FTP. Wykonywanie zdjęć może być wyzwalane przez zdarzenia lub zgodnie z harmonogramem.

**Kroki:**

1. Przejdź do interfejsu ustawień serwera FTP, wybierając opcje: **Configuration > Network > Advanced Settings > FTP**.

The screenshot displays the FTP configuration page. At the top, there are tabs for 'SNMP', 'FTP' (which is selected), 'Email', 'HTTPS', 'QoS', and '802.1x'. The main content area contains the following fields and options:

- Server Address: 0.0.0.0
- Port: 21
- User Name: (empty field)  Anonymous
- Password: (empty field)
- Confirm: (empty field)
- Directory Structure: Save in the root directory (dropdown menu)
- Picture Filing Interval: 7 (dropdown menu) Day(s)
- Picture Name: Default (dropdown menu)
- Upload Picture
- Test button
- Save button (red)

Rysunek 6–8 Ustawienia serwera FTP

2. Wprowadź adres i port serwera FTP.
3. Skonfiguruj ustawienia serwera FTP. Nazwa użytkownika i hasło są wymagane do logowania na serwerze FTP.



- *W celu lepszej ochrony systemu i prywatności użytkownika przed zagrożeniami zdecydowanie zaleca się korzystanie z silnych haseł do zabezpieczenia wszystkich funkcji i urządzeń sieciowych. Należy wybrać własne hasło (co najmniej osiem znaków należących do co najmniej trzech z następujących kategorii: wielkie litery, małe litery, cyfry i znaki specjalne) w celu zapewnienia lepszej ochrony urządzenia.*
  - *Instalator i/lub użytkownik końcowy są zobowiązani do prawidłowego skonfigurowania wszystkich haseł i innych ustawień zabezpieczeń.*
4. Skonfiguruj strukturę katalogów i interwał zapisywania zdjęć.

**Directory:** W polu „**Directory Structure**” wybierz odpowiedni katalog: „Root directory”, „Parent directory” lub „Child directory” . Po wybraniu katalogu nadrzędnego można użyć ustawienia Nazwa urządzenia, Numer urządzenia lub Adres IP urządzenia jako nazwy katalogu, a po wybraniu katalogu podrzędnego można użyć ustawienia Nazwa kamery lub Numer kamery jako nazwy katalogu.

**Picture Filing Interval:** Aby lepiej zarządzać zdjęciami, można ustawić interwał zapisywania zdjęć z zakresu 1–30 dni. Zdjęcia wykonywane w tym samym przedziale czasowym będą zapisywane w jednym folderze, którego nazwa będzie składać się z daty rozpoczęcia i daty zakończenia przedziału czasowego.

**Picture Name:** Skonfiguruj regułę nazewnictwa dla plików wykonywanych zdjęć. Można wybrać pozycję **Default** z listy rozwijanej, aby użyć następującej reguły domyślnej:

*adres IP\_numer kanału\_godzina wykonania zdjęcia\_typ zdarzenia.jpg*  
(np. 10.11.37.189\_01\_20150917094425492\_FACE\_DETECTION.jpg).

Można też dostosować ją, dodając prefiks **Custom Prefix** do domyślnej reguły nazewnictwa.

5. Zaznacz pole wyboru Upload Picture, aby włączyć tę funkcję.

**Upload Picture:** Aby włączyć przesyłanie zarejestrowanych zdjęć na serwer FTP, wybierz opcję „Upload picture“ (Prześlij zdjęcie).

**Anonymous Access to the FTP Server (nazwa użytkownika i hasło nie są wymagane):** zaznacz pole wyboru **Anonymous**, aby włączyć dostęp anonimowy do serwera FTP.

**Uwaga:** Dostęp anonimowy musi być obsługiwany przez serwer FTP.

6. Kliknij przycisk „**Save**“, aby zapisać ustawienia.

### 6.2.3 Konfigurowanie ustawień wysyłania wiadomości e-mail

#### **Cel:**

System można skonfigurować do wysyłania powiadomienia e-mail do wszystkich wyznaczonych adresatów po wykryciu zdarzenia alarmowego (np. wykrycie ruchu, zanik sygnału wideo lub sabotaż sygnału wideo).

#### **Zanim rozpocznie:**

Aby korzystać z funkcji wysyłania wiadomości e-mail należy skonfigurować ustawienia serwera DNS Server w oknie **Configuration > Network > Basic Settings > TCP/IP**.

#### **Kroki:**

1. Wyświetl okno Ustawienia protokołów TCP/IP (**Configuration > Network > Basic Settings > TCP/IP**), aby skonfigurować ustawienia Adres IPv4, Maska podsieci IPv4, Brama domyślna IPv4 i Preferowany serwer DNS.

**Uwaga:** Aby uzyskać więcej informacji, zobacz *sekcję 6.1.1*.

2. Przejdź do interfejsu ustawień wysyłania wiadomości e-mail, wybierając opcje: **Configuration > Network > Advanced Settings > Email**.
3. Skonfiguruj następujące ustawienia:  
**Sender:** Imię nadawcy wiadomości e-mail.  
**Sender's Address:** Adres e-mail nadawcy wiadomości.

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

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

**Email Encryption:** Dostępne opcje to: „None“ (Brak), „SSL“ oraz „TLS“. Po wybraniu opcji „SSL“ lub „TLS“ i wyłączeniu operacji StartTLS („Enable STARTTLS“) wiadomości e-mail będą przed wysłaniem szyfrowane za pomocą standardu SSL lub TLS. Jako port SMTP do wysyłania szyfrowanych wiadomości należy ustawić port nr 465. Po wybraniu opcji „SSL“ lub „TLS“ i włączeniu operacji StartTLS („Enable STARTTLS“) wiadomości e-mail będą wysyłane po ustanowieniu szyfrowania połączenia za pomocą operacji StartTLS. Jako port SMTP do wysyłania szyfrowanych wiadomości należy ustawić port nr 25.

**Uwaga:** Jeżeli konieczne jest korzystanie z protokołu STARTTLS, należy upewnić się, że ten protokół jest obsługiwany przez serwer e-mail. Jeżeli pole wyboru Enable STARTTLS jest zaznaczone, a serwer e-mail nie obsługuje tego protokołu, wiadomości e-mail nie będą szyfrowane.

**Attached Image:** Zaznacz pole wyboru Załącz zdjęcie, jeżeli chcesz wysłać wiadomości e-mail z załączonymi zdjęciami związanymi z alarmem.

**Interval:** odstęp czasowy między akcjami wysyłania załączonych zdjęć.

**Authentication** (opcjonalnie): jeżeli serwer e-mail wymaga uwierzytelnienia, zaznacz to pole wyboru, aby używać uwierzytelniania do logowania do tego serwera, i wprowadź nazwę użytkownika i hasło używane do logowania.



- *W celu lepszej ochrony systemu i prywatności użytkownika przed zagrożeniami zdecydowanie zaleca się korzystanie z silnych haseł do zabezpieczenia wszystkich funkcji i urządzeń sieciowych. Należy wybrać własne hasło (co najmniej osiem znaków należących do co najmniej trzech z następujących kategorii: wielkie litery, małe litery, cyfry i znaki specjalne) w celu zapewnienia lepszej ochrony urządzenia.*

- Instalator i/lub użytkownik końcowy są zobowiązani do prawidłowego skonfigurowania wszystkich haseł i innych ustawień zabezpieczeń.

Tabela **Receiver**: Wybierz odbiorcę wiadomości e-mail. Można skonfigurować maksymalnie trzech adresatów.

**Receiver**: Imię użytkownika, do którego przesyłane jest powiadomienie.

**Receiver's Address**: Adres e-mail użytkownika, do którego przesyłane jest powiadomienie.

The screenshot shows the 'Email' configuration page. At the top, there are tabs for 'SNMP', 'FTP', 'Email' (selected), 'HTTPS', 'QoS', and '802.1x'. The configuration fields include:

- Sender: test (with a green checkmark)
- Sender's Address: test@gmail.com (with a green checkmark)
- SMTP Server: (empty)
- SMTP Port: 25
- E-mail Encryption: None (dropdown menu)
- Attached Image:
- Interval: 2 (dropdown menu with 's' for seconds)
- Authentication:
- User Name: (empty)
- Password: (empty)
- Confirm: (empty)

Below these fields is a table titled 'Receiver' with the following structure:

No.	Receiver	Receiver's Address	Test
1			Test
2			
3			

At the bottom of the form is a red 'Save' button.

Rysunek 6–9 Ustawienia poczty e-mail

4. Kliknij przycisk „**Save**“, aby zapisać ustawienia.

## 6.2.4 Konfigurowanie ustawień HTTPS

### **Cel:**

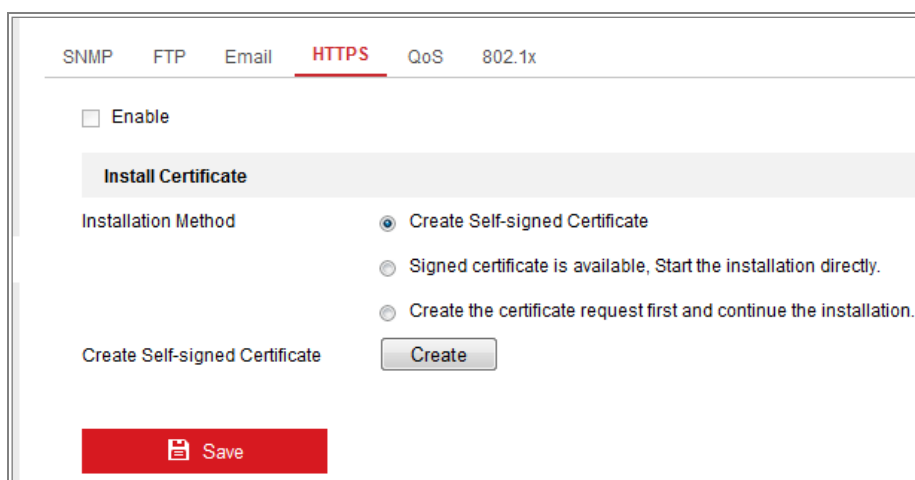
Protokół HTTPS zapewnia uwierzytelnianie użytkowników witryny internetowej i powiązanego serwera sieci Web oraz ochronę przed atakami typu Man-in-the-middle.

Aby ustawić numer portu protokołu HTTPS, należy wykonać poniższe kroki.

Jeżeli na przykład zostanie ustawiony numer portu 443 i adres IP 192.168.1.64, można uzyskać dostęp do urządzenia, wprowadzając adres `https://192.168.1.64:443` w przeglądarce internetowej.

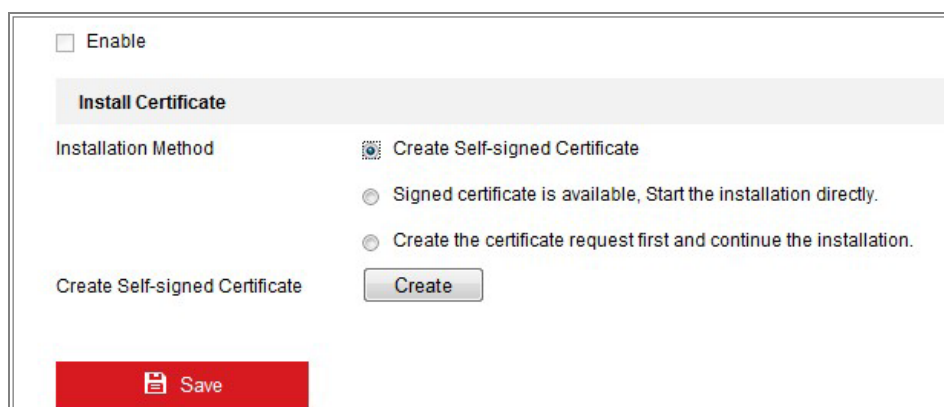
**Kroki:**

1. Wyświetl okno ustawień protokołu HTTPS. **Configuration > Network > Advanced Settings > HTTPS.**
2. Zaznacz pole wyboru Enable, aby włączyć tę funkcję.



Rysunek 6–10 Konfiguracja funkcji HTTPS

3. Utwórz certyfikat z podpisem własnym lub autoryzowany certyfikat.
  - Tworzenie certyfikatu z podpisem własnym
    - (1) Wybierz opcję **Create Self-signed Certificate** w sekcji Metoda instalacji.
    - (2) Kliknij przycisk **Create**, aby wyświetlić okno tworzenia.

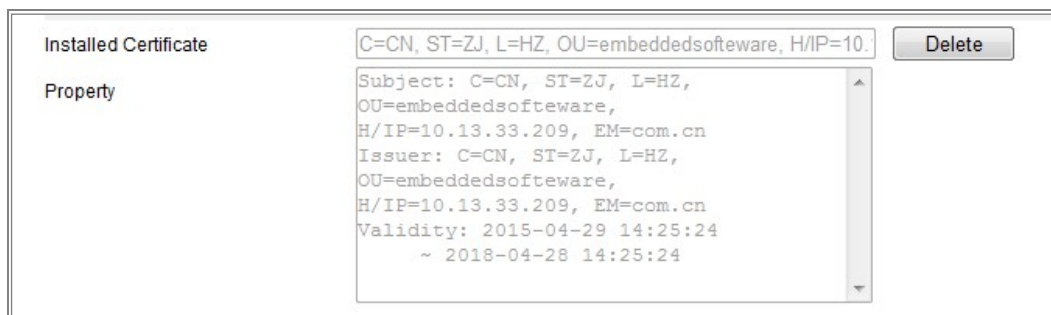


Rysunek 6–11 Tworzenie certyfikatu z podpisem własnym

- (3) Wprowadź nazwę kraju, nazwę/adres IP hosta, datę ważności i inne kraje.
- (4) Kliknij przycisk **OK**, aby zapisać ustawienia.

**Uwaga:** Jeżeli certyfikat został już zainstalowany, opcja Create Self-signed Certificate jest wyszarzona.

- Tworzenie autoryzowanego certyfikatu
- (1) Wybierz opcję **Create the certificate request first and continue the installation** w sekcji Metoda instalacji.
  - (2) Kliknij przycisk **Create**, aby utworzyć żądanie certyfikatu. Wpisz wymagane informacje w oknie podręcznym.
  - (3) Pobierz żądanie certyfikatu i prześlij je do zaufanego urzędu certyfikacji w celu uzyskania sygnatury.
  - (4) Po otrzymaniu prawidłowego sygnowanego certyfikatu zaimportuj go do urządzenia.
4. Po pomyślnym utworzeniu i zainstalowaniu certyfikatu dostępne będą informacje dotyczące certyfikatu.



Rysunek 6–12 Zainstalowany certyfikat

5. Kliknij przycisk **Save**, aby zapisać ustawienia.

## 6.2.5 Konfigurowanie ustawień jakości usługi (QoS)

### **Cel:**

Funkcja jakości usługi (Quality of Service – QoS) może pomóc rozwiązać problemy związane z opóźnieniami i przeciążeniem sieci dzięki nadaniu priorytetów przesyłanym danym.

**Kroki:**

1. Przejdź do interfejsu ustawień jakości usługi (QoS), wybierając opcje: **Configuration > Network > Advanced Settings > QoS**

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

Rysunek 6–13 Ustawienia jakości usługi (QoS)

2. Konfiguruj ustawienia jakości usługi (QoS), w tym parametry: (Wartość DSCP pakietów audio/wideo), (Wartość DSCP pakietów zdarzeń/alarmów) oraz (Wartość DSCP pakietów zarządzania).

Wartości ustawienia DSCP powinny należeć do zakresu 0–63. Im większa wartość DSCP, tym wyższy priorytet.

**Uwaga:** Skrót DSCP oznacza Differentiated Service Code Point. Wartość DSCP jest używana w nagłówku protokołu IP do sygnalizowania priorytetu danych.

3. Kliknij przycisk „**Save**”, aby zapisać ustawienia.

**Uwaga:** Ustawienia zostaną uwzględnione po ponownym uruchomieniu.

## 6.2.6 Konfigurowanie ustawień standardu IEEE 802.1X

**Cel:**

Standard IEEE 802.1X jest obsługiwany przez kamery sieciowe, a po włączeniu tej funkcji dane kamery są zabezpieczone i konieczne jest uwierzytelnienie użytkownika podczas ustanawiania połączenia kamery z siecią chronioną przez zabezpieczenia IEEE 802.1X.

**Zanim rozpoczniesz:**

Serwer uwierzytelniania musi być skonfigurowany. Złóż wniosek o przyznanie nazwy użytkownika i hasła i zarejestruj te informacje na serwerze 802.1X.





- W celu lepszej ochrony systemu i prywatności użytkownika przed zagrożeniami zdecydowanie zaleca się korzystanie z silnych haseł do zabezpieczenia wszystkich funkcji i urządzeń sieciowych. Należy wybrać własne hasło (co najmniej osiem znaków należących do co najmniej trzech z następujących kategorii: wielkie litery, małe litery, cyfry i znaki specjalne) w celu zapewnienia lepszej ochrony urządzenia.
- Instalator i/lub użytkownik końcowy są zobowiązani do prawidłowego skonfigurowania wszystkich haseł i innych ustawień zabezpieczeń.

#### Kroki:

1. Wyświetl okno Ustawienia 802.1X (**Configuration > Network > Advanced Settings > 802.1X**).

Rysunek 6–14 Ustawienia funkcji 802.1X

2. Zaznacz pole wyboru **Enable IEEE 802.1X**, aby włączyć tę funkcję.
3. Skonfiguruj ustawienia 802.1X takie jak Protokół, Wersja EAPOL, Nazwa użytkownika, Hasło i Potwierdź.

**Uwaga:** Ustawienie **EAPOL version** musi być identyczne z odpowiednim ustawieniem routera lub przełącznika.

4. Wprowadź nazwę użytkownika i hasło, aby uzyskać dostęp do serwera.
5. Kliknij przycisk **Save**, aby ukończyć konfigurowanie ustawień.

**Uwaga:** Ustawienia zostaną uwzględnione po ponownym uruchomieniu.

## Rozdział 7 Ustawienia wideo/audio

### Cel:

Poniższe instrukcje dotyczą konfigurowania ustawień wideo, ustawień audio, ROI i Wyświetlaj informacje o strumieniu.

### 7.1 Konfigurowanie ustawień wideo

#### Kroki:

1. Wyświetl okno Ustawienia wideo (**Configuration > Video/Audio > Video**).

The screenshot shows a web-based configuration interface for video settings. It has three tabs: 'Video' (selected), 'Audio', and 'Display Info. on Stream'. The settings are as follows:

Stream Type	Main Stream(Normal)
Video Type	Video&Audio
Resolution	1920*1080P
Bitrate Type	Variable
Video Quality	Medium
Frame Rate	25 fps
Max. Bitrate	4096 Kbps
Max. Average Bitrate	2048 Kbps
Video Encoding	H.264
H.264+	ON
Profile	High Profile
I Frame Interval	50
SVC	OFF
Smoothing	50 [ Clear<->Smooth ]

At the bottom, there is a red 'Save' button with a floppy disk icon.

Rysunek 7–1 Ustawienia wideo

2. W pozycji Typ strumienia kamery wybierz strumień główny (zwykły), podstrumień lub trzeci strumień.

**Uwagi:**

- W przypadku niektórych modeli, aby ponownie uruchomić system i wyłączyć trzeci strumień, należy przejść do okna System > Maintenance > System Service > Software i zaznaczyć pole wyboru Enable Third Stream.
  - Strumień główny jest zazwyczaj używany do nagrywania i wyświetlania podglądu na żywo przy odpowiedniej przepustowości, a podstrumienia można użyć do wyświetlania podglądu na żywo przy ograniczonej przepustowości.
  - Aby ponownie uruchomić system i wyłączyć trzeci strumień, należy przejść do System > Maintenance > System Service > Software i zaznaczyć pole wyboru Enable Third Stream.
3. Można dostosować następujące parametry dla wybranego typu strumienia.

**Video Type:**

Wybierz jeden z następujących typów strumienia: strumień wideo lub złożony strumień audio-wideo. Sygnał dźwiękowy będzie nagrywany tylko wówczas, gdy z wybrano ustawienie **Video & Audio** opcji **Video Type**.

**Resolution:**

Wybierz rozdzielczość wyjścia wideo.

**Bitrate Type:**

Wybierz stałą lub zmienną transmisję danych.

**Video Quality:**

Po wybraniu typu transmisji bitów Variable dostępnych jest sześć poziomów jakości obrazu wideo do wyboru.

**Frame Rate:**

Ustaw liczbę klatek na sekundę. Parametr ten służy do określenia częstotliwości odświeżania strumienia wideo i jest mierzony w postaci liczby klatek na sekundę (fps). Większa liczba klatek na sekundę umożliwia uzyskanie płynnego obrazu wideo podczas filmowania poruszających się obiektów.

**Max. Bitrate:**

Ustaw maksymalną szybkość transmisji bitów w zakresie 32–16 384 Kb/s. Większa wartość oznacza wyższą jakość wideo, jednak w takim wypadku wymagana jest lepsza przepustowość.

**Uwaga:** Górny limit maksymalnej szybkości transmisji bitów jest zależny od platformy kamery. W przypadku niektórych kamer górny limit wynosi 8192 Kb/s lub 12 288 Kb/s.

#### **Video Encoding:**

Jeżeli dla opcji Stream Type skonfigurowano ustawienie Main Stream, dostępne są ustawienia H.264 i H.265, a jeżeli wybrano typ strumienia Sub Stream lub Third Stream, dostępne są ustawienia H.264, MJPEG i H.265. Standard H.265 jest nową technologią kodowania. W porównaniu ze standardem H.264 umożliwia on zmniejszenie szybkości transmisji bitów przy tej samej rozdzielczości, liczbie klatek na sekundę i jakości obrazu.

**Uwaga:** Dostępne typy kodowania wideo są zależne od trybu kamery.

#### **H.264+ i H.265+:**

- **H.264+:** Jeżeli wybrano ustawienie Main Stream opcji Stream Type i ustawienie H.264 opcji Video Encoding, dostępne jest ustawienie H.264+. Standard H.264+ jest ulepszoną technologią kodowania opartą na standardzie H.264. Po włączeniu obsługi standardu H.264+ użytkownicy mogą oszacować użycie dysku twardego na podstawie jego maksymalnej przeciętnej szybkości transmisji bitów. W porównaniu do standardu H.264 standard H.264+ umożliwia zmniejszenie rozmiaru pliku o 50% przy tej samej maksymalnej szybkości bitów w przypadku większości scen.
- **H.265+:** Jeżeli wybrano ustawienie Main Stream opcji Stream Type i ustawienie H.265 opcji Video Encoding, dostępne jest ustawienie H.265+. Standard H.265+ jest ulepszoną technologią kodowania opartą na standardzie H.265. Po włączeniu obsługi standardu H.265+ użytkownicy mogą oszacować użycie dysku twardego na podstawie jego maksymalnej przeciętnej szybkości transmisji bitów. W porównaniu do standardu H.265 standard H.265+ umożliwia zmniejszenie rozmiaru pliku o 50% przy tej samej maksymalnej szybkości bitów w przypadku większości scen.

Aby włączyć lub wyłączyć obsługę standardu H.264+/H.265+, należy ponownie uruchomić kamerę. W przypadku bezpośredniego przełączenia ze standardu H.264+ do H.265+ lub odwrotnie ponowne uruchomienie systemu nie jest wymagane.

**Uwagi:**

- Jeśli występują problemy ze zgodnością i obraz podgląd na żywo lub odtwarzania nie jest odpowiednio wyświetlany, wówczas należy zaktualizować odtwarzacz wideo do najnowszej wersji.
- Aby korzystać ze standardu H.264+ lub H.265+, należy wybrać zmienną szybkość transmisji bitów.
- Po włączeniu obsługi standardu H.264+/H.265+ parametry takie jak profil, interwał klatki I, jakość wideo i SVC są wyszarzone, jeżeli wybrano zmienną szybkość transmisji bitów.
- Niektóre funkcje nie są dostępne po włączeniu obsługi standardu H.264+/H.265+. Okna związane z tymi funkcjami będą ukryte.
- Standardy H.264+/H.265+ umożliwiają automatyczne dostosowanie rozkładu szybkości transmisji bitów zgodnie z wymaganiami monitorowanej sceny w celu wykorzystania ustawionej maksymalnej szybkości transmisji bitów w perspektywie długoterminowej. Dostosowanie kamery do określonej monitorowanej sceny trwa co najmniej trzy dni.

**Max. Average Bitrate:**

Po ustawieniu maksymalnej szybkości transmisji bitów odpowiednia zalecana maksymalna przeciętna szybkość transmisji bitów jest wyświetlana w polu Max. Average Bitrate. Można również ręcznie ustawić maksymalną przeciętną szybkość transmisji bitów w zakresie od 32 Kb/s do wartości maksymalnej szybkości transmisji bitów.

**Profile:**

Dostępne są ustawienia kodowania Basic profile, Main Profile i High Profile.

**I Frame Interval:**

Ustaw parametr I Frame Interval w zakresie 1–400.

**SVC:**

Standard SVC (Scalable Video Coding) stanowi rozszerzenie standardu H.264/AVC. Wybierz pozycję przełącznika OFF lub ON, aby wyłączyć lub włączyć funkcję SVC. Po wybraniu ustawienia Auto urządzenie automatycznie wyodrębnia klatki z oryginalnego obrazu wideo, gdy przepustowość sieci jest niedostateczna.

**Smoothing:**

Funkcja ta odnosi się do wygładzania strumienia. Im wyższa wartość parametru wygładzania, tym bardziej płynny będzie strumień, jednak jakość wideo może być niedostateczna. Im niższa wartość parametru wygładzania, tym wyższa jakość wideo, jednak płynność strumienia może być niedostateczna.

4. Kliknij przycisk „**Save**”, aby zapisać ustawienia.

**Uwaga:**

Parametry wideo są zależne od modelu kamery. Należy skorzystać z odpowiedniej strony wyświetlania funkcji kamery.

## 7.2 Konfigurowanie ustawień audio

**Kroki:**

1. Wyświetl okno Ustawienia audio. **Configuration > Video/Audio > Audio.**

Setting	Value
Channel No.	Analog Camera1
Audio Encoding	G.711alaw
Audio Input	MicIn
Input Volume	50
Environmental Noise Filter	OFF

Rysunek 7–2 Ustawienia audio

2. Skonfiguruj poniższe ustawienia.

**Uwaga:** Ustawienia audio są zależne od modelu kamery.

**Audio Encoding:** Dostępne są ustawienia G.722.1, G.711 ulaw, G.711alaw, G.726, MP2L2 i PCM. Dla ustawienia MP2L2 można skonfigurować szybkość próbkowania i szybkość transmisji bitów audio. Dla ustawienia PCM można skonfigurować szybkość próbkowania.

**Audio Input:** Aby korzystać z podłączonego mikrofonu i przetwornika, można wybrać ustawienie odpowiednio MicIn i LineIn.

**Input Volume:** Regulacja w zakresie 0–100.

**Environmental Noise Filter:** Wybierz ustawienie OFF lub ON. Po włączeniu tej funkcji można częściowo eliminować szумы w otoczeniu.

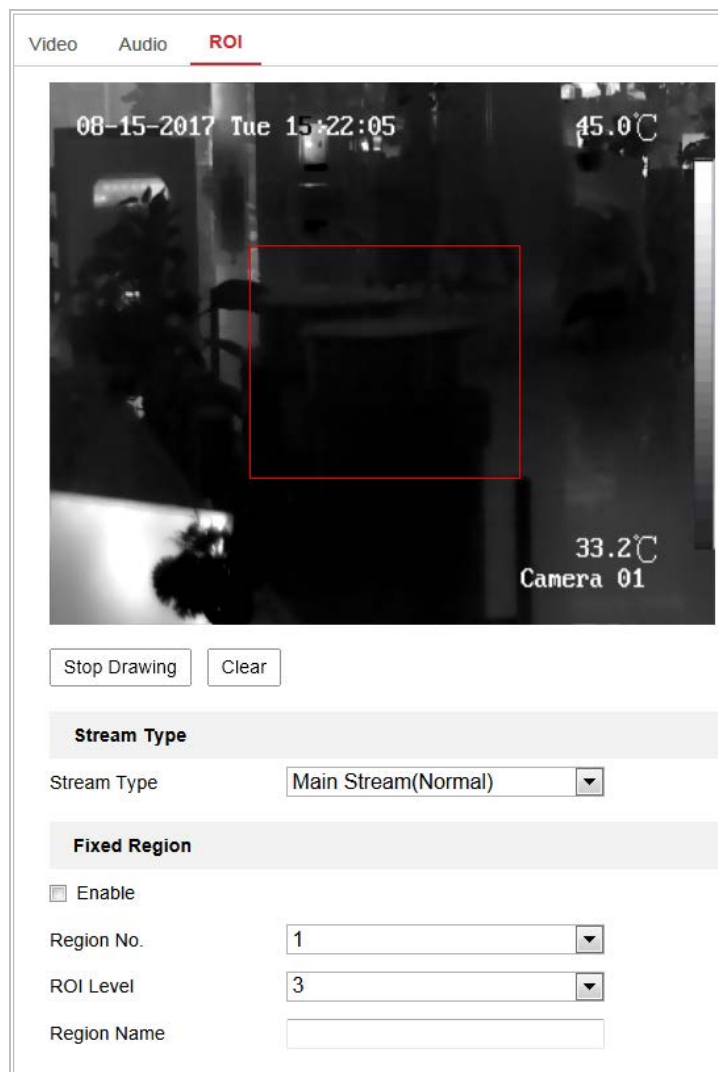
3. Kliknij przycisk „**Save**“, aby zapisać ustawienia.

## 7.3 Konfigurowanie kodowania ROI

### **Cel:**

Kodowanie obszaru zainteresowania (ROI, Region of Interest) ułatwia odróżnienie informacji ROI od tła w procesie kompresji wideo i przypisanie większej ilości zasobów związanych z kodowaniem do obszaru zainteresowania w celu podwyższenia jakości obrazu ROI i zmniejszenia ostrości obrazu tła.

**Uwaga:** Funkcja ROI jest zależna od modelu kamery.



Rysunek 7–3 Ustawienia obszaru zainteresowania

**Kroki:**

1. Przejdź do interfejsu ustawień kodowania obszaru zainteresowania (ROI), wybierając opcje: **Configuration > Video/Audio > ROI**.
2. Wybierz typ strumienia w polu Stream Type dla kodowania ROI.
3. Zaznacz pole wyboru **Enable** w obszarze Fixed Region.
4. Wybierz ustawienie **Fixed Region** ROI.
  - (1) Wybierz pozycję Region No. z listy rozwijanej.
  - (2) Zaznacz pole wyboru **Enable**, aby włączyć funkcję ROI dla wybranego obszaru.
  - (3) Kliknij przycisk **Drawing**. Kliknij myszą i przeciągnij jej wskaźnik na ekranie, aby wyznaczyć czerwony prostokątny obszar ROI. Można kliknąć przycisk **Clear**, aby anulować wyznaczony obszar. Kliknij przycisk **Stop Drawing** po zakończeniu.



- (4) Wybierz ustawienie ROI level.
  - (5) Wprowadź nazwę wybranego obszaru.
  - (6) Kliknij przycisk **Save**, aby zapisać ustawienia ROI dla wybranego obszaru.
  - (7) Powtórz kroki od (1) do (6), aby skonfigurować inne obszary.
5. Wybierz ustawienie **Dynamic Region** dla funkcji ROI.
- (1) Zaznacz pole wyboru, aby włączyć funkcję **Face Tracking**.
- Uwaga:** Aby włączyć funkcję śledzenia twarzy, należy upewnić się, że funkcja detekcji twarzy jest obsługiwana i włączona.
- (2) Wybierz ustawienie ROI level.
6. Kliknij przycisk **Save**, aby zapisać ustawienia.
- Uwaga:** Poziom ROI oznacza poziom poprawy jakości obrazu. Im większa wartość, tym lepsza jakość obrazu.

## 7.4 Ustawienia metadanych

### **Zanim rozpocznie:**

Przejdź do **5.3.4 Typ zasobu VCA**, aby ustawić typ zasobu VCA (Video Content Analysis) urządzenia.

### **Cel:**

Aby zarządzać platformą innej firmy przy użyciu metadanych, należy włączyć obsługę metadanych.

### **Kroki:**

1. Przejdź do Configuration > Video/Audio > metadata Settings.
2. Sprawdź typ VCA do obsługi metadanych.
3. Kliknij przycisk „Save”, aby zapisać ustawienia.

Video Audio ROI **metadata Settings**

Channel No. Camera2

**Enable metadata**

Temperature Measurement

Dynamic Fire Source Detection

The metadata settings only take effect when you enable the VCA function.

Save

Rysunek 7–4 Ustawienia metadanych

**Uwaga:** Ustawienia metadanych są uwzględniane tylko po włączeniu funkcji VCA. Na przykład po włączeniu opcji Temperature Measurement ta funkcja działa pod warunkiem, że skonfigurowano i zapisano reguły pomiaru temperatury.

## Rozdział 8 Ustawienia obrazu

### **Cel:**

Instrukcje podane w tym rozdziale dotyczą konfigurowania parametrów obrazu takich jak ustawienia wyświetlania, ustawienia OSD, maska prywatności i nakładanie obrazu.

### 8.1 Konfigurowanie ustawień wyświetlania

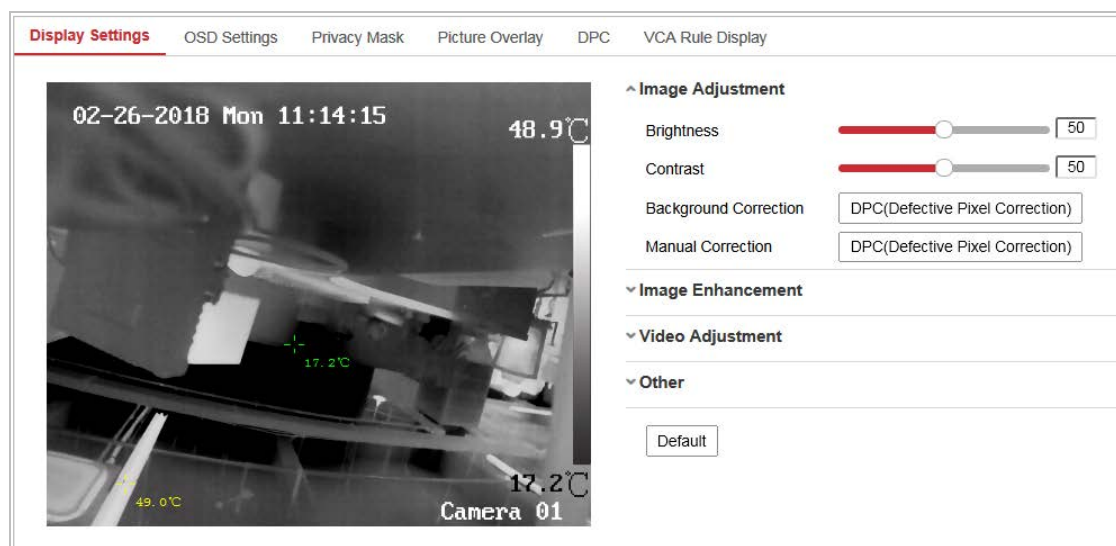
### **Cel:**

Konfigurowanie dostosowania obrazu, ustawień ekspozycji, przełącznika trybu dzień/noc, ustawienia oświetlenia, balansu bieli, poprawy jakości obrazu, dostosowania obrazu wideo i innych parametrów w ustawieniach wyświetlania.

**Uwaga:** Parametry wyświetlania są zależne od modelu kamery. Aby uzyskać więcej informacji, sprawdź ustawienia w danym oknie.

### **Kroki:**

1. Wyświetl okno Ustawienia wyświetlania (**Configuration > Image > Display Settings**).



Rysunek 8–1 Ustawienia wyświetlania informacji

2. Skonfiguruj parametry obrazu z kamery.

**Uwaga:** Aby zagwarantować jakość obrazu przy różnym oświetleniu, uwzględniono dwa zestawy parametrów konfigurowanych przez użytkowników.

- **Image Adjustment**

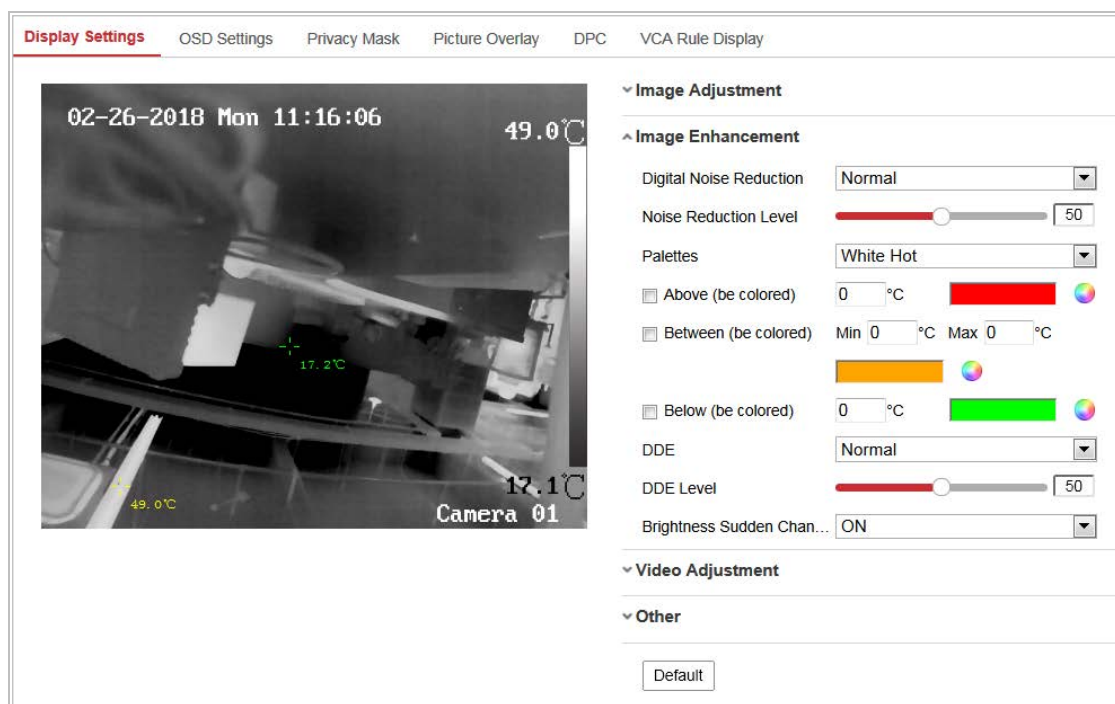
Pozycja **Brightness** opisuje jasność obrazu, która waha się od 1 do 100, a jej wartość domyślna wynosi 50.

Pozycja **Contrast** opisuje kontrast obrazu, który waha się od 1 do 100, a jej wartość domyślna wynosi 50.

**Manual Background Correction:** Zakryj całkowicie obiektyw, używając przedmiotu (zaleca się użycie osłony obiektywu) i kliknij przycisk Manual Background Correction. Następnie kamera dopasuje obraz odpowiednio do bieżącego środowiska.

**Manual Shutter Correction:** Kliknij przycisk Manual Shutter Correction, aby kamera dostosowała obraz odpowiednio do temperatury kamery.

- **Image Enhancement**



Rysunek 8–2 Ulepszanie obrazu

**Digital Noise Reduction:** Funkcja DNR ogranicza zakłócenia szumowe w strumieniu wideo. Dostępne są ustawienia OFF, Normal i Expert do wyboru. W trybie zwykłym ustaw poziom DNR w zakresie od 0 do 100.

W trybie zaawansowanym ustaw poziom DNR zarówno z poziomu DNR przestrzeni [0–100], jak i z poziomu DNR czasu [0–100].

**Palettes:** Korzystając z palet, można wybrać żądane kolory. Dostępne są ustawienia white hot, black hot, fusion 1, rainbow, fusion 2, ironbow 1, ironbow 2, sepia, color 1, color 2, ice fire, rain, red hot i green hot.

W trybie **White Hot** można dostosować różne kolory obiektów w zakresach temperatury.

- Zaznacz pole wyboru **Above (be colored)** i ustaw temperaturę. Obiekty na scenie, których temperatura jest wyższa niż ustawiona wartość, będą wyróżniane czerwonym (domślnie) kolorem.
- Zaznacz pole wyboru **Between (be colored)** i ustaw temperaturę. Obiekty na scenie, których temperatura będzie należeć do zakresu określonego przez dwie ustawione wartości, będą wyróżniane żółtym (domślnie) kolorem.
- Zaznacz pole wyboru **Below (be colored)** i ustaw temperaturę. Obiekty na scenie, których temperatura jest niższa niż ustawiona wartość, będą wyróżniane zielonym (domślnie) kolorem.

**DDE:** DDE (cyfrowa poprawa szczegółów) pozwala dostosować szczegółowość obrazu. Można wybrać opcję OFF lub Normal. W trybie zwykłym parametr DDE Level można dostosowywać w zakresie od 1 do 100.

**Brightness Sudden Change:** (Ta funkcja jest dostępna tylko w przypadku zasobu VCA Behavior Analysis) Gdy jasność obiektu różni się bardzo od jasności tła (duża różnica temperatury), system zmniejsza tę różnicę na wyświetlanym obrazie.

- **Video Adjustment**

**Mirror:** Lustrzane przekształcenie umożliwia wyświetlenie odwróconego obrazu. Dostępne są ustawienia W lewo/w prawo, W górę/W dół, Środek i WYŁĄCZONE.

**Video Standard:** Dostępne są ustawienia 50 Hz i 60 Hz. Wybierz ustawienie zgodnie ze standardami wideo (zazwyczaj 50 Hz dla standardu PAL i 60 Hz dla standardu NTSC).

**Capture Mode:** Można wybrać tryb wejścia wideo zgodnie z wymaganiami dotyczącymi pola widzenia i rozdzielczości.

**Digital Zoom:** W pozycji powiększenia cyfrowego można wybrać opcję OFF, 2X lub 4X, aby wyświetlić podgląd na żywo w oryginalnym rozmiarze, przy dwukrotnym powiększeniu cyfrowym i czterokrotnym powiększeniu cyfrowym.

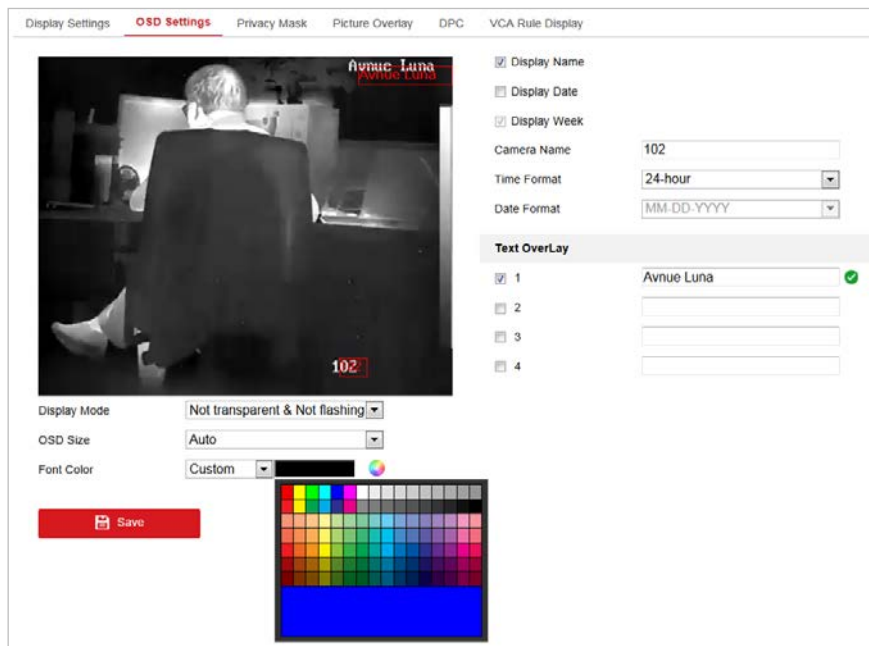
- **Inne**

**Local Output:** Włącz lub wyłącz lokalne wyjście urządzenia.

## 8.2 Konfigurowanie ustawień menu ekranowego

**Cel:**

Można dostosować nazwę kamery, format godziny/daty, tryb wyświetlania i rozmiar tekstu OSD dla podglądu na żywo.



Rysunek 8–3 Ustawienia OSD

**Kroki:**

1. Przejdź do interfejsu ustawień OSD, wybierając opcje: **Configuration > Image > OSD Settings.**

2. Zaznacz odpowiednie pole wyboru, aby wybrać opcję wyświetlania nazwy kamery, daty lub tygodnia, jeżeli jest to wymagane.
3. Edytuj nazwę kamery w polu tekstowym **Camera Name**.
4. Wybierz ustawienia formatu godziny i formatu daty z listy rozwijanej.
5. Wybierz ustawienia z listy rozwijanej ustawienia formatu godziny, formatu daty, trybu wyświetlania, rozmiaru OSD i koloru czcionki.
6. Skonfiguruj ustawienia nakładania tekstu.
  - (1) Zaznacz pole wyboru przed polem tekstowym, aby włączyć wyświetlanie na ekranie.
  - (2) Wprowadź odpowiednie informacje w polu tekstowym.

**Uwaga:** Można skonfigurować maksymalnie osiem nakładek tekstowych.
7. Dostosuj położenie i wyrównanie ramek tekstowych.

Dostępne są ustawienia wyrównania do lewej, wyrównania do prawej i niestandardowe. Jeżeli zostanie wybrane ustawienie niestandardowe, można kliknąć myszą i przeciągnąć ramki tekstowe w oknie podglądu na żywo, aby dostosować ich położenie.

**Uwaga:** Wyrównanie można dostosować tylko w przypadku elementów Nakładka tekstowa.
8. Kliknij przycisk „**Save**“, aby zapisać ustawienia.

## 8.3 Konfigurowanie maski prywatności

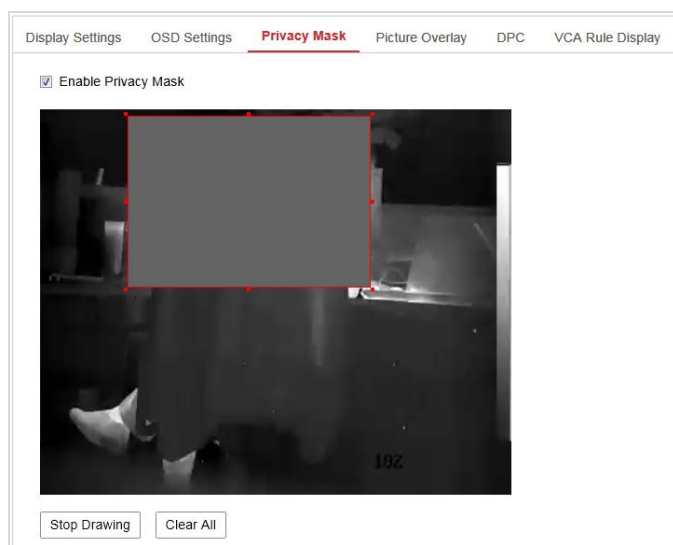
### **Cel:**

Maska prywatności umożliwia zakrycie pewnych obszarów podglądu na żywo, aby zapobiec wyświetlaniu i nagrywaniu obrazu pewnych punktów w obszarze monitorowanym.

### **Kroki:**

1. Przejdź do interfejsu ustawień maski prywatności, wybierając opcje: **Configuration > Image > Privacy Mask**.
2. Zaznacz pole wyboru „**Enable Privacy Mask**“, aby włączyć tę funkcję.

3. Kliknij przycisk **Draw Area**.



Rysunek 8–4 Ustawienia maski prywatności

4. Kliknij myszą i przeciągnij jej wskaźnik w oknie podglądu wideo na żywo, aby wyznaczyć obszar maskowania.

**Uwaga:** Na jednym obrazie można zaznaczyć do 4 obszarów maskowanych.

5. Kliknij przycisk **Stop Drawing**, aby zakończyć wyznaczanie obszaru, lub kliknij przycisk **Clear All** w celu wyczyszczenia wszystkich wyznaczonych obszarów bez zapisywania.
6. Kliknij przycisk „**Save**“, aby zapisać ustawienia.

## 8.4 Konfigurowanie nakładania obrazu

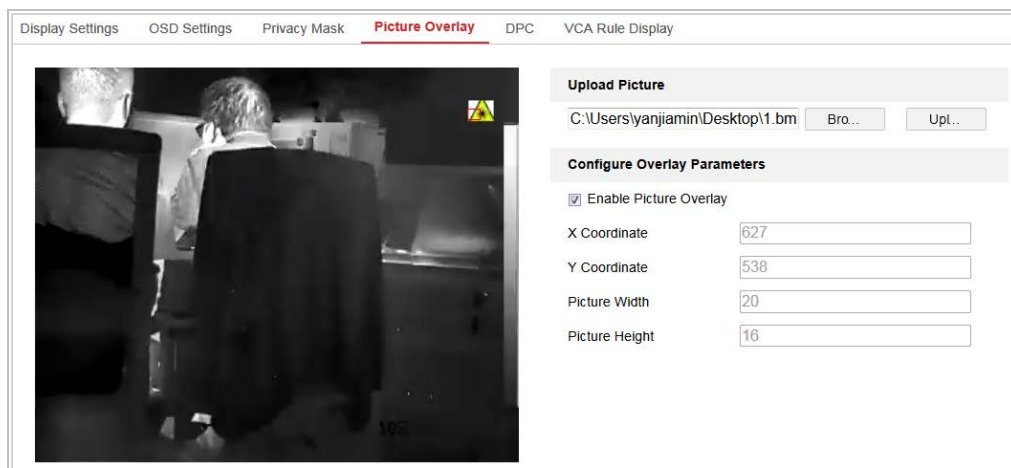
**Cel:**

Ta funkcja umożliwia nakładanie obrazu. Korzystając z tej funkcji, firmy lub użytkownicy mogą nakładać swoje logo na obraz.

**Kroki:**

1. Wyświetl okno Ustawienia nakładania obrazu (**Configuration > Image > Picture Overlay**).





Rysunek 8–5 Nakładanie obrazu

2. Kliknij przycisk **Browse**, aby wybrać obraz.
3. Kliknij przycisk **Upload**, aby przekazać ten element.
4. Zaznacz pole wyboru **Enable Picture Overlay**, aby włączyć tę funkcję.
5. Ustaw wartości Współrzędna X i Współrzędna Y, aby dostosować położenie nakładki na obrazie. Dostosuj ustawienia Szerokość obrazu i Wysokość obrazu zgodnie z wymaganym rozmiarem.
6. Kliknij przycisk **Save**, aby zapisać ustawienia.

**Uwaga:** Obraz musi być w formacie RGB24 bmp, a jego rozmiar nie powinien być większy niż 128\*128.

## 8.5 Konfigurowanie DPC (korekcji wadliwych pikseli)

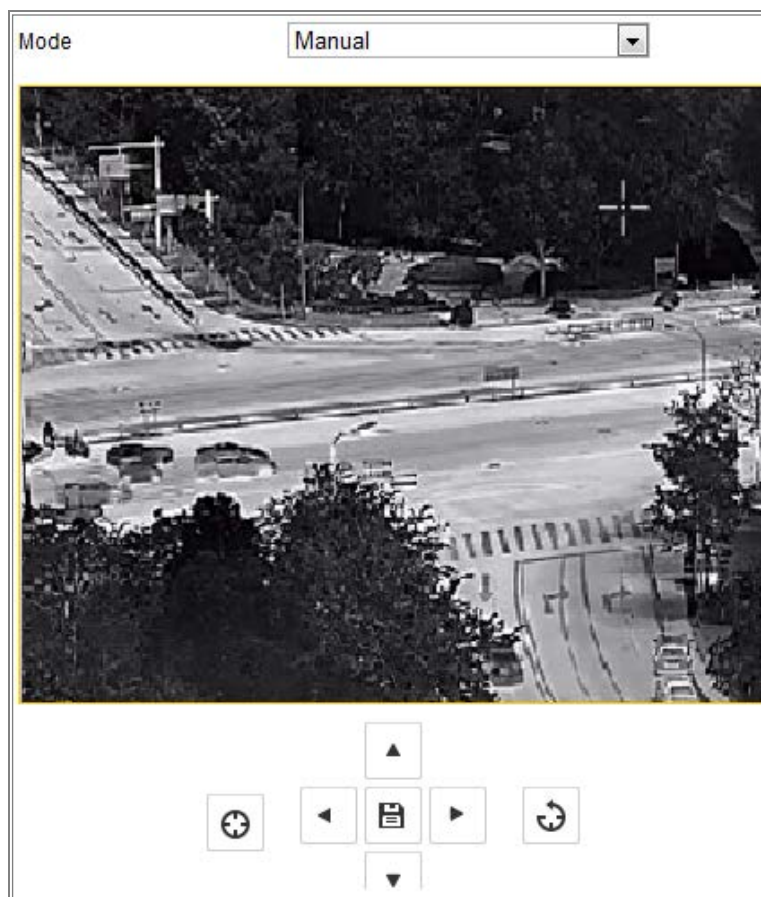
### **Cel:**

Termin DPC (korekcja wadliwych pikseli) odnosi się do funkcji kamery, dzięki której można skorygować nieodpowiednio działające, uszkodzone piksele na ekranie LCD.





**Uwaga:** Ta funkcja dostępna tylko dla niektórych modeli kamer.

### **Kroki:**

1. Przejdź do interfejsu ustawień DPC. **Configuration > Image > DPC**



Rysunek 8–6 Korekcja wadliwych pikseli

2. Wybierz tryb. Poniżej przedstawiono przykład trybu ręcznego.
3. Kliknij obraz, aby zaznaczyć uszkodzony piksel. Wskaźnik na obrazie zostanie przeniesiony do klikniętego miejsca. Można kliknąć przycisk , aby nieco dopasować położenie kursora.
4. Kliknij przycisk , aby uruchomić korekcję.
5. Kliknij przycisk , aby anulować wprowadzone korekty, lub kliknij przycisk , aby je zapisać.

## 8.6 Konfigurowanie wyświetlania reguł VCA

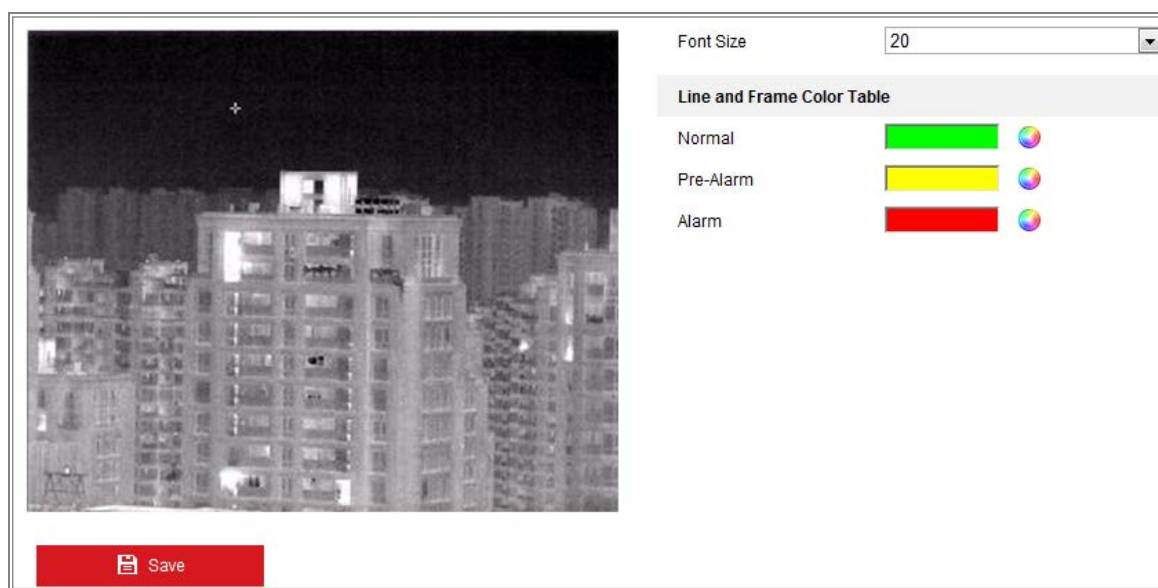
### Cel:

Korzystając z funkcji wyświetlania reguł VCA, można dostosować nakładane na obraz informacje dotyczące reguł VCA (np. pomiar temperatury), takie jak rozmiar czcionki oraz kolor linii i ramki.

**Uwaga:** Ta funkcja dostępna tylko dla niektórych modeli kamer.

### Kroki:

1. Wyświetl ustawienia wyświetlania reguł VCA: **Configuration > Image > VCA Rule Display**
2. Wybierz żądany rozmiar czcionki oraz kolor linii i ramki dla trybu zwykłego, alarmu wstępnego i alarmu właściwego.
3. Kliknij przycisk **Save**.



Rysunek 8–7 Wyświetlanie reguł VCA

## Rozdział 9 Ustawienia zdarzeń

W tej sekcji wyjaśniono, jak skonfigurować kamerę sieciową do reagowania na zdarzenia alarmowe, łącznie ze zdarzeniami podstawowymi i inteligentnymi.

### 9.1 Zdarzenia podstawowe

Instrukcje podane w tej sekcji dotyczą konfigurowania zdarzeń podstawowych, takich jak detekcja ruchu, sabotaż sygnału wideo, wejście alarmowe, wyjście alarmowe i sytuacja wyjątkowa. Te zdarzenia mogą wyzwać powiązane działania, takie jak Powiadomienie centrum monitoringu, Wysłanie wiadomości e-mail lub Wyzwolenie wyjścia alarmowego.

**Uwaga:** Zaznacz pole wyboru powiadomienia centrum monitoringu, jeśli chcesz, aby informacje o alarmie były wysyłane do oprogramowania klienta na komputerze lub urządzeniu mobilnym zaraz po wyzwoleniu alarmu.

#### 9.1.1 Konfigurowanie detekcji ruchu

**Cel:**

Ta funkcja umożliwia detekcję obiektów poruszających się w skonfigurowanym monitorowanym obszarze i wykonanie serii akcji po wyzwoleniu alarmu.

Aby precyzyjnie wykrywać poruszające się obiekty i ograniczyć liczbę fałszywych alarmów, można wybrać konfigurację zwykłą lub zaawansowaną zależnie od środowiska detekcji ruchu.

##### ● Zwykła konfiguracja

Po wybraniu zwykłej konfiguracji stosowany jest ten sam zestaw parametrów detekcji ruchu w ciągu dnia jak w nocy.

### Zadania 1: Wyznaczanie obszaru detekcji ruchu

#### Kroki:

1. Wyświetl ustawienia detekcji ruchu: **Configuration > Event > Basic Event > Motion Detection**.
2. Zaznacz pole wyboru **Enable Motion Detection**.
3. Zaznacz pole wyboru **Enable Dynamic Analysis for Motion**, jeżeli chcesz oznaczać wykrywane obiekty zielonymi prostokątami.

**Uwaga:** Jeżeli wykrywane obiekty nie powinny być wyróżniane zielonymi prostokątami, należy zaznaczyć opcję Disable. Wybierz reguły wyłączania w oknie **Configuration > Local Configuration > Live View Parameters-rules**.



Rysunek 9–1 Włączenie detekcji ruchu

4. Kliknij przycisk **Draw Area**. Kliknij myszą i przeciągnij jej wskaźnik w podglądzie wideo na żywo, aby wyznaczyć obszar detekcji ruchu. Kliknij przycisk **Stop Drawing**, aby ukończyć wyznaczanie jednego obszaru.
5. (Opcjonalnie) Kliknij przycisk **Clear All**, aby usunąć wszystkie obszary.
6. (Opcjonalnie) Przesuń suwak, aby ustawić czułość detekcji.

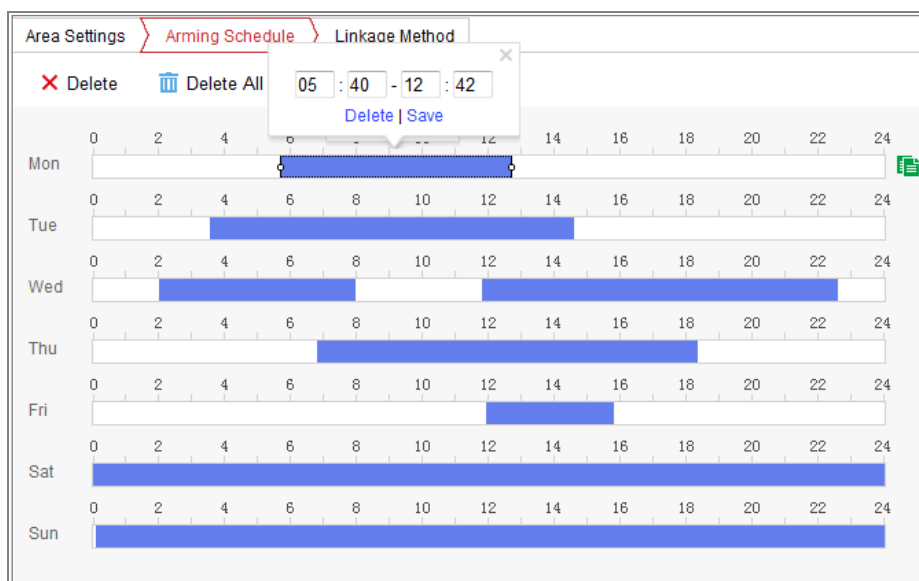
**Zadanie 2: Konfigurowanie harmonogramu zabezpieczenia dla funkcji detekcji ruchu**



Rysunek 9–2 Harmonogram uzbrajania

**Kroki:**

1. Wybierz kartę **Arming Schedule**, aby edytować harmonogram zabezpieczenia.
2. Kliknij pasek czasu i przeciągnij wskaźnik myszy, aby wybrać przedział czasowy.



Rysunek 9–3 Harmonogram uzbrajania

**Uwaga:** Po kliknięciu wybranego przedziału czasowego można go dostosować zgodnie z wymaganiami, przesuując pasek czasu lub wprowadzając dokładną wartość.

3. (Opcjonalnie) Kliknij przycisk Delete, aby usunąć bieżący harmonogram zabezpieczenia, lub kliknij przycisk Zapisz w celu zapisania ustawień.
4. Przesuń wskaźnik myszy do końca każdego dnia, aby wyświetlić okno dialogowe umożliwiające skopiowanie bieżących ustawień do innych dni.
5. Kliknij przycisk „**Save**”, aby zapisać ustawienia.

**Uwaga:** Przedziały czasowe nie powinny nakładać się. Dla każdego dnia można skonfigurować maksymalnie osiem przedziałów czasowych.

### **Zadanie 3: Konfigurowanie działania powiązanego z detekcją ruchu**

Aby wybrać określone działania powiązane, zaznacz odpowiednie pola wyboru. Dostępne są ustawienia Audible Warning, Send Email, Notify Surveillance Center, Upload to FTP/Memory Card/NAS, Trigger Channel i Trigger Alarm Output. W interfejsie tym można określić działania powiązane z wystąpieniem zdarzenia.

Area Settings > Arming Schedule > Linkage Method		
<input type="checkbox"/> Normal Linkage	<input type="checkbox"/> Trigger Alarm Output	<input type="checkbox"/> Trigger Channel
<input type="checkbox"/> Audible Warning	<input type="checkbox"/> A->1	<input type="checkbox"/> A1
<input type="checkbox"/> Send Email		
<input type="checkbox"/> Notify Surveillance Center		
<input type="checkbox"/> Full Screen Monitoring		
<input type="checkbox"/> Upload to FTP		

Rysunek 9–4 Działania powiązane

**Uwaga:** Powiązane działania są zależne od modelu kamery.

- **Audible Warning**

Wyzwalanie lokalnego ostrzeżenia dźwiękowego. Obsługiwane tylko przez urządzenie wyposażone w wyjście audio.

- **Notify Surveillance Center**

W chwili wystąpienia zdarzenia sygnał alarmowy lub nietypowy sygnał jest przesyłany do zdalnego oprogramowania do zarządzania monitoringiem.

- **Send Email**

W chwili wystąpienia zdarzenia wiadomość e-mail z informacjami alarmowymi jest przesyłana do użytkownika lub użytkowników.

**Uwaga:** Aby uzyskać informacje na temat konfigurowania wysyłania wiadomości e-mail po wystąpieniu zdarzenia, zobacz 6.2.3.

- **Upload to FTP/Memory Card/NAS**

W momencie wyzwolenia alarmu wykonywane jest zdjęcie, które jest następnie przesyłane na serwer FTP.

**Uwagi:**

- Najpierw należy skonfigurować adres FTP i zdalny serwer FTP. Aby uzyskać więcej informacji, zobacz 6.2.2.
- Przejdź do strony **Configuration > Storage > Schedule Settings > Capture > Capture Parameters**, włącz funkcję wykonywania zdjęć wyzwalanego przez zdarzenia, a następnie ustaw interwał wykonywania zdjęć i liczbę zdjęć.



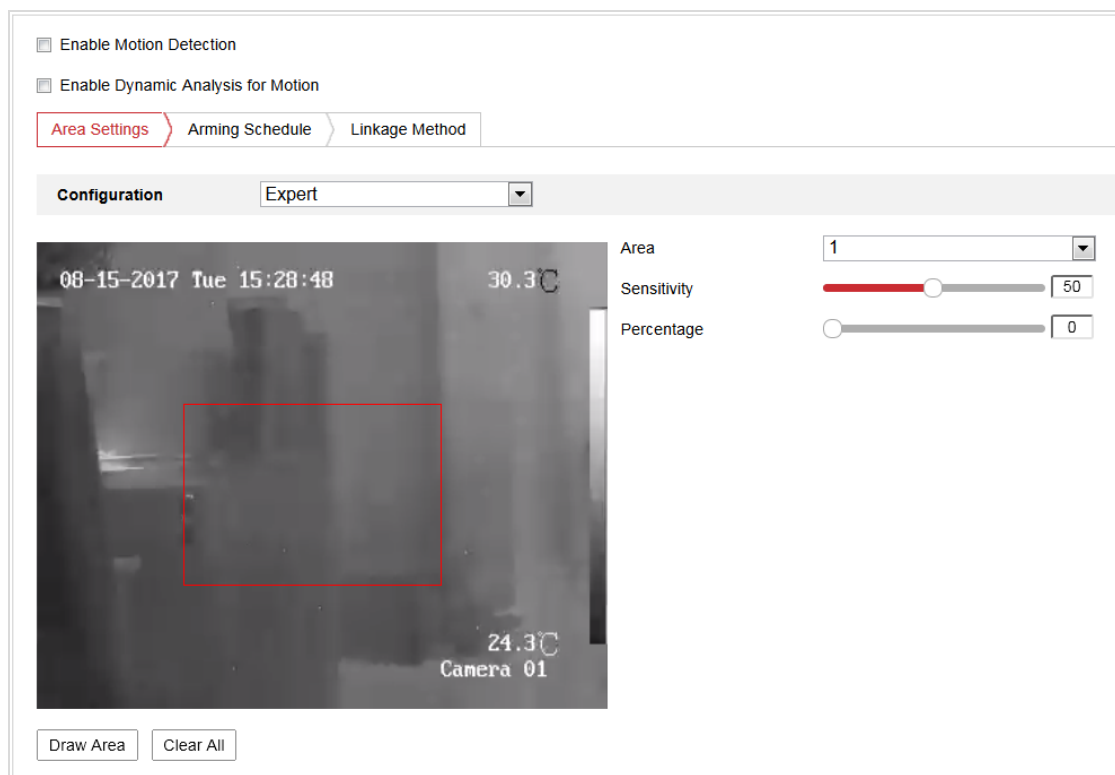
- Wykonane zdjęcie można również przekazać do dostępnej karty SD lub dysku sieciowego.
- **Trigger Channel**

Wideo może być nagrywane po wykryciu ruchu. Aby móc skorzystać z tej funkcji, należy skonfigurować harmonogram nagrywania. Aby uzyskać szczegółowe informacje, patrz 10.1.
- **Trigger Alarm Output**

Wyzwolenie jednego lub kilku wyjść alarmu zewnętrznego w chwili wystąpienia zdarzenia.

**Uwaga:** Aby skonfigurować parametry związane z wyzwalaniem wyjścia alarmowego po wystąpieniu zdarzenia, zobacz **Sekcję 9.1.4 Konfigurowanie wyjścia alarmu**.
- **Konfiguracja zaawansowana**

Tryb zaawansowany służy głównie do konfiguracji czułości i proporcji obiektu na każdym obszarze w przypadku różnego przełączania trybu dzień/noc.



Rysunek 9–5 Tryb zaawansowany detekcji ruchu

- Wyłączanie przełącznika trybu dzień/noc

**Kroki:**

1. Wyznacz obszar detekcji, tak jak w trybie konfiguracji zwykłej. Obsługiwanych jest maksymalnie osiem obszarów.
2. Wybierz ustawienie **OFF** opcji **Switch Day and Night Settings**.
3. Wybierz obszar, klikając odpowiedni numer obszaru.
4. Przesuń wskaźnik, aby dostosować czułość i proporcje obiektu dla wybranego obszaru.
5. Skonfiguruj harmonogram zabezpieczenia i powiązane działanie, tak jak w trybie konfiguracji zwykłej.
6. Kliknij przycisk „**Save**”, aby zapisać ustawienia.

- Automatyczny przełącznik trybu dzień/noc


**Kroki:**

1. Wyznacz obszar detekcji, tak jak w trybie konfiguracji zwykłej. Obsługiwanych jest maksymalnie osiem obszarów.
2. Wybierz ustawienie **Auto-Switch** opcji **Switch Day and Night Settings**.
3. Wybierz obszar, klikając odpowiedni numer obszaru.
4. Przesuń wskaźnik, aby dostosować czułość i proporcje obiektu dla wybranego obszaru w trybie dziennym.
5. Przesuń wskaźnik, aby dostosować czułość i proporcje obiektu dla wybranego obszaru w trybie nocnym.
6. Skonfiguruj harmonogram zabezpieczenia i powiązane działanie, tak jak w trybie konfiguracji zwykłej.
7. Kliknij przycisk „**Save**”, aby zapisać ustawienia.

- Przełączanie trybu dzień/noc według harmonogramu

**Kroki:**

1. Wyznacz obszar detekcji, tak jak w trybie konfiguracji zwykłej. Obsługiwanych jest maksymalnie osiem obszarów.
2. Wybierz ustawienie **Scheduled-Switch** opcji **Switch Day and Night Settings**.



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

Rysunek 9–6 Przełączanie trybu dzień/noc według harmonogramu

3. Wybierz godzinę rozpoczęcia i godzinę zakończenia przełączania.
4. Wybierz obszar, klikając odpowiedni numer obszaru.
5. Przesuń wskaźnik, aby dostosować czułość i proporcje obiektu dla wybranego obszaru w trybie dziennym.
6. Przesuń wskaźnik, aby dostosować czułość i proporcje obiektu dla wybranego obszaru w trybie nocnym.
7. Skonfiguruj harmonogram zabezpieczenia i powiązane działanie, tak jak w trybie konfiguracji zwykłej.
8. Kliknij przycisk „**Save**“, aby zapisać ustawienia.

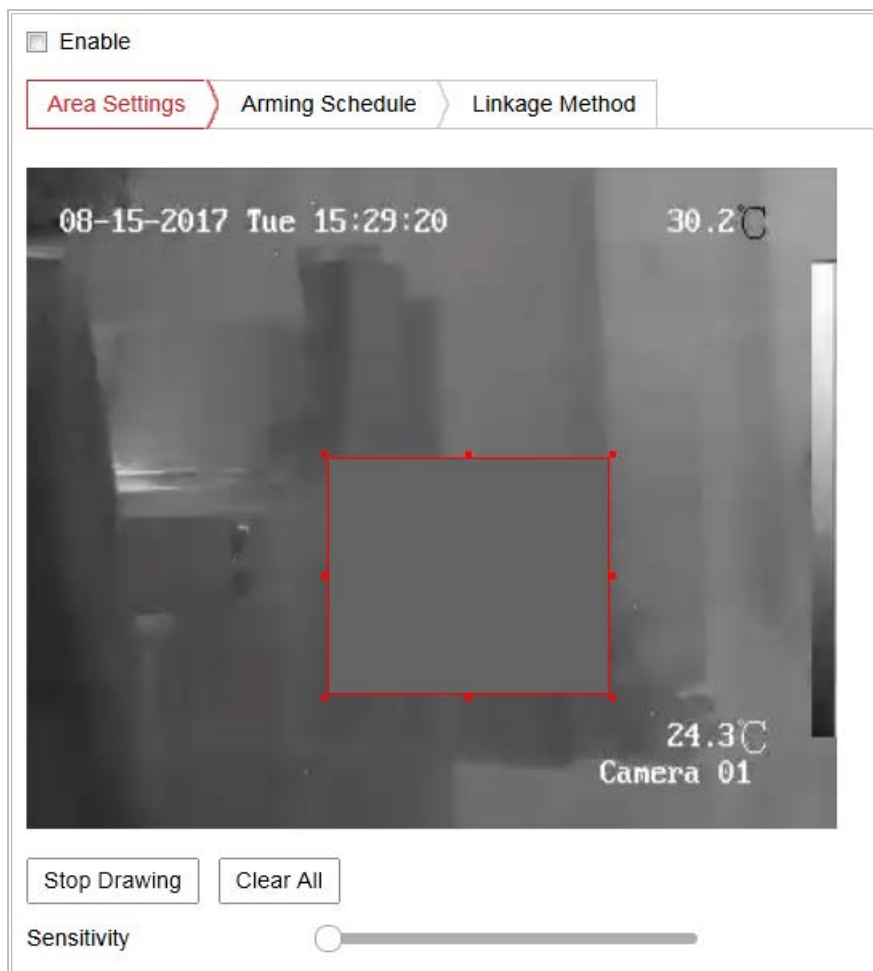
### 9.1.2 Konfigurowanie alarmu sabotażu sygnału wideo

**Cel:**

Można skonfigurować kamerę do wyzwalania alarmu w przypadku przesłonięcia obiektywu i wykonania odpowiednich akcji reagowania na alarm.

**Kroki:**

1. Wyświetl ustawienia detekcji sabotażu sygnału wideo (**Configuration > Event > Basic Event > Video Tampering.**).



Rysunek 9–7 Alarm sabotażu sygnału wideo

2. Zaznacz pole wyboru **Enable Video Tampering**, aby włączyć funkcję detekcji sabotażu sygnału wideo.
3. Wyznacz obszar detekcji sabotażu sygnału wideo. Zobacz **Zadanie 1: Wyznaczanie obszaru detekcji ruchu** w sekcji 9.1.1.
4. Kliknij przycisk **Edit**, aby edytować harmonogram zabezpieczenia dla funkcji sabotażu sygnału wideo. Konfiguracja harmonogramu uzbrojenia przebiega tak samo, jak konfiguracja harmonogramu uzbrojenia dla detekcji ruchu. Zobacz **Zadanie 2: Konfigurowanie harmonogramu zabezpieczenia dla funkcji detekcji ruchu** w sekcji 9.1.1.
5. Zaznacz pole wyboru, aby wybrać powiązane działanie wykonywane po wykryciu sabotażu sygnału wideo. Można wybrać dźwiękowy sygnał ostrzegawczy, powiadomienie centrum monitoringu, wysłanie wiadomości e-mail lub wyzwolenie wyjścia alarmu. Zobacz **Zadanie 3: Ustawianie działania powiązanego z detekcją ruchu** w sekcji 9.1.1.

6. Kliknij przycisk „**Save**“, aby zapisać ustawienia.

### 9.1.3 Konfigurowanie wejścia alarmu

#### Kroki:

1. Przejdź do interfejsu ustawień wejścia alarmu, wybierając opcje: **Configuration > Event > Basic Event > Alarm Input**.
2. Wybierz numer wejścia alarmowego i typ alarmu. Dostępne typy alarmu to: NO (normalnie otwarty) i NC (normalnie zamknięty). Edytuj nazwę wejścia alarmowego (opcjonalnie).

The screenshot shows the 'Alarm Input' configuration page with the following details:

- Navigation tabs: Motion Detection, Video Tampering, **Alarm Input**, Alarm Output, Exception.
- Alarm Input No.: A<-1 (dropdown)
- Alarm Type: NO (dropdown)
- IP Address: Local (text input)
- Alarm Name: (text input, marked as 'cannot copy')
- Enable Alarm Input Handling
- Active tabs: **Arming Schedule**, Linkage Method
- Buttons: Delete (with red X), Delete All (with trash icon)
- Schedule Grid: A 7x24 grid showing arming times for each day of the week.
 

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

Rysunek 9–8 Ustawienia wejścia alarmowego

3. Kliknij kartę **Arming Schedule**, aby skonfigurować harmonogram zabezpieczenia wejścia alarmowego. Zobacz **Zadanie 2: Konfigurowanie harmonogramu zabezpieczenia dla funkcji detekcji ruchu** w sekcji 9.1.1.
4. Kliknij przycisk **Linkage Method** i zaznacz pole wyboru, aby wybrać działanie powiązane z wejściem alarmowym. Zobacz **Zadanie 3: Ustawianie działania powiązanego z detekcją ruchu** w sekcji 9.1.1.

5. Ustawienia można skopiować i zastosować do innych wejść alarmu.
6. Kliknij przycisk „**Save**”, aby zapisać ustawienia.

### 9.1.4 Konfigurowanie wyjścia alarmu

The screenshot shows the 'Alarm Output' configuration page. It includes the following elements:

- Tabs:** Motion Detection, Video Tampering, Alarm Input, **Alarm Output**, Exception.
- Fields:**
  - Alarm Output No.: A->1
  - IP Address: Local
  - Default Status: Low Level
  - Triggering Status: Pulse
  - Delay: 5s
  - Alarm Name: (cannot copy)
  - Alarm Status: OFF (cannot copy)
- Arming Schedule:**
  - Buttons: Delete, Delete All
  - Grid showing arming schedules for Mon, Tue, Wed, Thu, Fri, Sat, Sun. Each row has a 24-hour scale from 0 to 24.
- Bottom Buttons:** Manual Alarm, Copy to..., Save

Rysunek 9–9 Ustawienia wyjścia alarmowego

#### **Kroki:**

1. Przejdź do interfejsu ustawień wyjścia alarmu, wybierając opcje: **Configuration > Event > Basic Event > Alarm Output**.
2. Wybierz jeden kanał wyjścia alarmowego z listy rozwijanej **Alarm Output**. Można też skonfigurować nazwę wyjścia alarmowego (opcjonalnie).
3. W pozycji czasu opóźnienia można wybrać jedną z wartości: 5sec, 10sec, 30sec, 1min, 2min, 5min, 10min lub Manual. Czas opóźnienia to czas wstrzymania przesyłania sygnału alarmowego do wyjścia alarmu w momencie wystąpienia alarmu

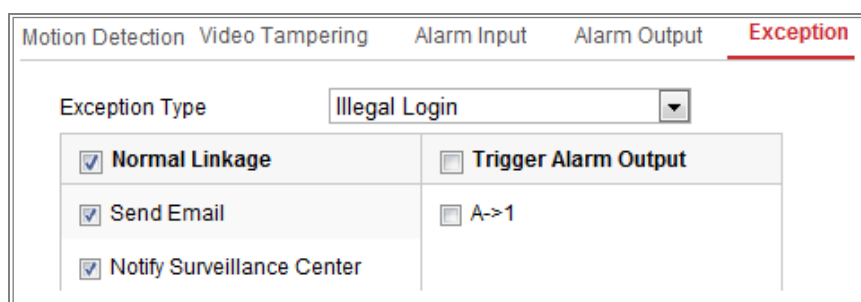
4. Kliknij kartę **Arming Schedule**, aby wyświetlić okno Edycja harmonogramu. Konfiguracja harmonogramu czasowego przebiega tak samo, jak ustawianie harmonogramu uzbrajania dla detekcji ruchu. Zobacz **Zadanie 2: Konfigurowanie harmonogramu zabezpieczenia dla funkcji detekcji ruchu** w sekcji 9.1.1.
5. Ustawienia można skopiować i zastosować do innych wyjść alarmu.
6. Kliknij przycisk „**Save**”, aby zapisać ustawienia.

### 9.1.5 Obsługa zdarzeń nietypowych

Można ustawić następujące rodzaje wyjątków: zapewnienie dysku twardego, błąd dysku twardego, rozłączenie z siecią, konflikt adresów IP i nieuprawnione logowanie do kamer.

#### **Kroki:**

1. Przejdź do interfejsu ustawień zdarzeń nietypowych, wybierając opcje: **Configuration > Event > Basic Event > Exception**.
2. Zaznacz pole wyboru, aby ustawić działania wykonywane w momencie wystąpienia alarmu zdarzenia nietypowego. Zobacz **Zadanie 3: Ustawianie działania powiązanego z detekcją ruchu** w 9.1.1, aby zapoznać się ze szczegółowym opisem procedury.



Rysunek 9–10 Ustawienia wyjątków

3. Kliknij przycisk „**Save**”, aby zapisać ustawienia.

## 9.2 Zdarzenia inteligentne

Instrukcje podane w tej sekcji dotyczą konfigurowania zdarzeń inteligentnych, takich jak detekcja nietypowego dźwięku, detekcja zmiany sceny, dynamiczna detekcja źródła ognia lub maskowanie detekcji źródła ognia.

### 9.2.1 Konfigurowanie detekcji nietypowego dźwięku

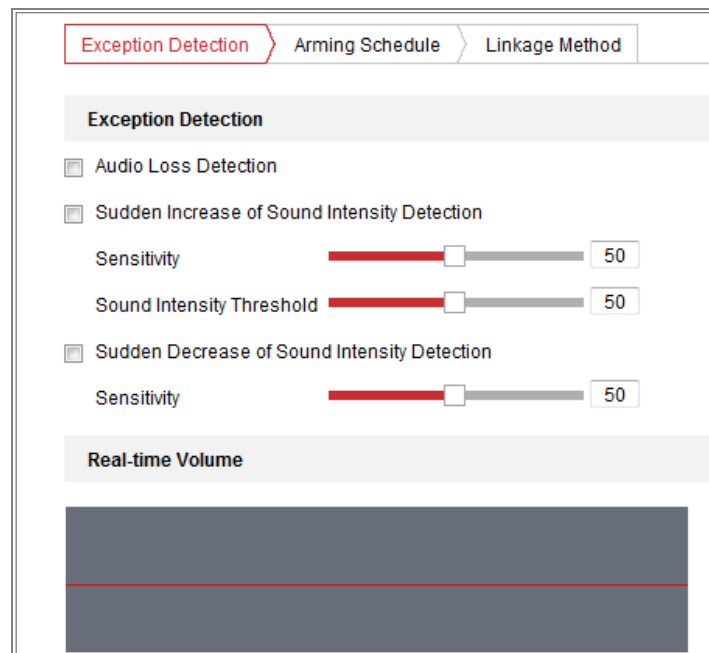
**Cel:**

Ta funkcja umożliwi detekcję nietypowych dźwięków na monitorowanej scenie, takich jak nagłe zwiększenie/zmniejszenie natężenia dźwięku, i wykonanie określonych akcji po wyzwoleniu alarmu.

**Uwaga:** Funkcja detekcji nietypowego dźwięku jest zależna od modelu kamery.

**Kroki:**

- Wyświetl ustawienia Detekcja nietypowego dźwięku (**Configuration > Event > Smart Event > Audio Exception Detection**).



Rysunek 9–11 Detekcja nietypowego sygnału audio

- Zaznacz pole wyboru **Audio Loss Exception**, aby włączyć funkcję detekcji zaniku sygnału audio.



3. Zaznacz pole wyboru **Sudden Increase of Sound Intensity Detection**, aby wykrywać nagły wzrost natężenia dźwięku na monitorowanej scenie. Można ustawić czułość detekcji i wartość progową nagłego zwiększenia natężenia dźwięku.
4. Zaznacz pole wyboru **Sudden Decrease of Sound Intensity Detection**, aby wykrywać nagły spadek natężenia dźwięku na monitorowanej scenie. Można ustawić czułość detekcji i wartość progową nagłego zmniejszenia natężenia dźwięku.

**Uwagi:**

- Czułość: Zakres 1-100. Im niższa wartość, tym większa zmiana jest wymagana do wyzwolenia funkcji detekcji.
  - Sound Intensity Threshold: Zakres 1-100. To ustawienie umożliwia filtrowanie dźwięku w otoczeniu. Im większe natężenie dźwięku w otoczeniu, tym wyższa powinna być ta wartość. Można dostosować to ustawienie zgodnie z rzeczywistym otoczeniem.
  - W tym oknie jest wyświetlana głośność dźwięku w czasie rzeczywistym.
5. Kliknij kartę **Arming Schedule**, aby skonfigurować harmonogram zabezpieczenia. Aby uzyskać szczegółowe instrukcje, zobacz **Zadanie 2 Konfigurowanie harmonogramu zabezpieczenia dla funkcji detekcji ruchu** w *Sekcji 9.1.1*.
  6. Kliknij kartę **Linkage Method** i wybierz działania powiązane z detekcją nietypowego dźwięku, takie jak Powiadomienie centrum monitoringu, Wysłanie wiadomości e-mail, Przekazanie do serwera FTP/karty pamięci/dysku NAS, Wyzwolenie nagrywania w kanale i Wyzwolenie wyjścia alarmowego.
  7. Kliknij przycisk „**Save**”, aby zapisać ustawienia.

## 9.2.2 Konfigurowanie detekcji zmiany sceny

### Cel:

Ta funkcja umożliwia detekcję zmiany sceny monitorowanego środowiska na skutek czynników zewnętrznych, takich jak celowe obrócenie kamery. Po wyzwoleniu alarmu mogą być wykonywane określone akcje.

**Uwaga:** Funkcja detekcji zmiany sceny jest zależna od modelu kamery.

### Kroki:

1. Wyświetl ustawienia Detekcja zmiany sceny (**Configuration > Event > Smart Event > Scene Change Detection**).



Rysunek 9–12 Detekcja zmiany sceny

2. Zaznacz pole wyboru **Enable**, aby włączyć tę funkcję.
3. Kliknij i przeciągnij suwak czułości detekcji dożądanego położenia. Wartość czułości można regulować w zakresie 1–100. Im wyższa wartość, tym mniejsza zmiana sceny powoduje wyzwolenie alarmu.
4. Kliknij kartę **Arming Schedule**, aby skonfigurować harmonogram zabezpieczenia. Aby uzyskać szczegółowe instrukcje, zobacz **Zadanie 2 Konfigurowanie harmonogramu zabezpieczenia dla funkcji detekcji ruchu** w sekcji 9.1.1.

- Kliknij kartę **Linkage Method**, aby wybrać działania powiązane z detekcją zmiany sceny, takie jak Powiadomienie centrum monitoringu, Wysłanie wiadomości e-mail, Przekazanie do serwera FTP/karty pamięci/dysku NAS, Wyzwolenie kanału i Wyzwolenie wyjścia alarmowego.
- Kliknij przycisk **Save**, aby zapisać ustawienia.

### 9.2.3 Konfigurowanie dynamicznej detekcji źródła ognia

#### **Cel:**

Po włączeniu tej funkcji w przypadku wykrycia źródła ognia nastąpi wyzwolenie działania alarmowego.

#### **Kroki:**

- Przejdź do interfejsu ustawiania dynamicznej detekcji źródła ognia: **Configuration > Event > Smart Event > Dynamic Fire Source Detection**
- Zaznacz pole wyboru **Enable Dynamic Fire Source Detection**, aby włączyć tę funkcję.

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

Rysunek 9–13 Konfigurowanie dynamicznej detekcji źródła ognia

- Zaznacz pole wyboru **Display Fire Source Frame on Stream**, aby w przypadku pożaru wyświetlić na strumieniu czerwoną ramkę wokół źródła ognia. (opcjonalnie)

4. Można przeciągnąć suwak, aby wyregulować czułość dynamicznej detekcji źródła ognia w zakresie od 1 do 10. Im większa liczba, tym bardziej czuła detekcja.
5. Zaznacz pole wyboru, aby wybrać metodę powiązania stosowaną dla wejścia alarmu. Zobacz **Zadanie 3: Ustawianie akcji alarmowych dla detekcji ruchu** w sekcji 9.1.1. Można zaznaczyć pole wyboru w polu Other Linkage, aby włączyć wyjście alarmu. Numer wyjścia alarmu różni się w zależności od funkcji urządzenia.
6. Kliknij przycisk „**Save**“, aby zapisać ustawienia.

## 9.2.4 Konfigurowanie maskowania detekcji źródła ognia

### **Cel:**

Maskowanie źródła ognia umożliwia wykluczenie określonych obszarów z zakresu detekcji źródła ognia.

### **Kroki:**

1. Wyświetl okno **Configuration > Event > Smart Event > Fire Source Detection Shield**.
2. Zaznacz pole wyboru, aby włączyć detekcję ognia.
3. Kliknij przycisk **Draw Area**, a następnie kliknij i przeciągnij wskaźnik myszy w oknie podglądu na żywo, aby wyznaczyć obszar.



Rysunek 9–14 Maskowanie detekcji źródła ognia

4. Można przeciągnąć narożniki czerwonego prostokątnego obszaru, aby zmienić jego kształt i rozmiar.
5. Kliknij przycisk **Stop Drawing**, aby zakończyć wyznaczanie obszaru, lub kliknij przycisk **Clear All** w celu wyczyszczenia wszystkich wyznaczonych obszarów bez zapisywania.
6. Ustaw przezroczystość maski obszaru (półprzezroczysta, nieprzezroczysta lub przezroczysta).
7. Kliknij przycisk **Add**, aby zapisać ustawienia maskowania detekcji źródła ognia. Maska zostanie zapisana na liście Fire Source Detection Shield List. Można wybrać region i kliknąć przycisk **Delete**, aby usunąć go z listy. Można też określić kolor regionów.
8. Zaznacz pole wyboru **Enable Fire Source Detection Shield**, aby włączyć tę funkcję.

**Uwaga:** Na jednym obrazie można zaznaczyć do 24 obszarów maskowanych.

## 9.3 Konfiguracja VCA

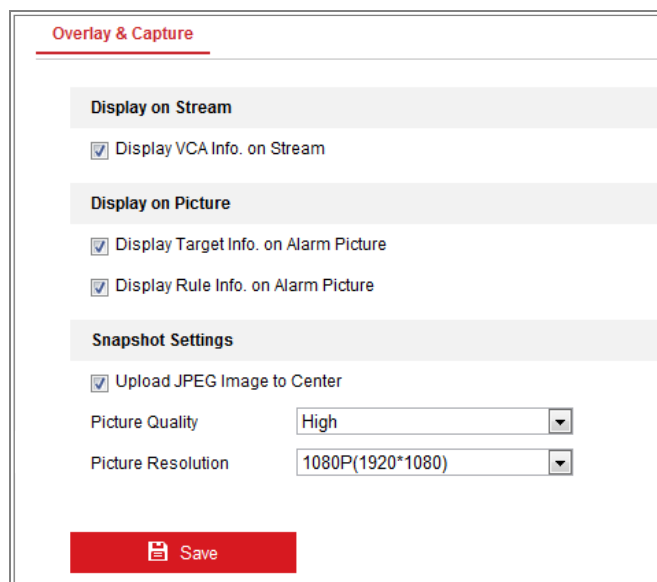
### 9.3.1 Konfigurowanie nakładania obrazu i wykonywania zdjęć

#### **Cel:**

Można włączyć funkcję wyświetlania informacji VCA na strumieniu lub informacji o obiekcie na zdjęciu oraz ustawić jakość i rozdzielczość zdjęcia.

#### **Kroki:**

1. Wyświetl okno **Configuration > VCA > Overlay & Capture**.
2. Zaznacz żądane pole wyboru ustawień wyświetlania oraz wybierz jakość i rozdzielczość zdjęć.



Rysunek 9–15 Nakładanie obrazu i wykonywanie zdjęć

Informacje mogą być wyświetlane na zdjęciach i strumieniu.

**Display VCA info. on Stream:** W podglądzie na żywo lub trybie odtwarzania zielone ramki będą wyświetlane wokół obiektów docelowych.

**Display Target info. on Alarm Picture:** Jeżeli to pole wyboru jest zaznaczone, ramka będzie wyświetlana wokół obiektu docelowego na przekazanym zdjęciu alarmowym.

**Display Rule info. on Alarm Picture:** Ramka będzie wyświetlana wokół wykrytego obiektu i skonfigurowanego obszaru na zdjęciu alarmowym.

**Uwaga:** Należy upewnić się, że reguły są włączone w ustawieniach lokalnych.

Przejdź do **Configuration > Local Configuration > Rules**, aby włączyć tę funkcję.

Konfiguracja wykonywania zdjęć: Można skonfigurować jakość i rozdzielczość wykonywanego zdjęcia.

**Upload JPEG Image to Center:** Zaznacz pole wyboru, aby przekazywać wykonane zdjęcie do centrum monitoringu, gdy zostanie zgłoszony alarm VCA.

**Picture Quality:** Do wyboru dostępna jest wysoka, średnia i niska jakość.

**Picture Resolution:** Dostępne są ustawienia CIF, 4CIF, 720P i 1080P.

### 9.3.2 Konfiguracja analizy zachowania

Poniższe kroki należy wykonać w celu trójwymiarowego pomiaru i oceny ilościowej obrazu z kamery, a następnie obliczenia rozmiaru każdego celu. Detekcja VCA będzie bardziej precyzyjna, jeżeli zostanie skonfigurowana kalibracja kamery.

#### **Zanim rozpocziesz:**

Upewnij się, że znasz rzeczywisty wzrost osoby na scenie.

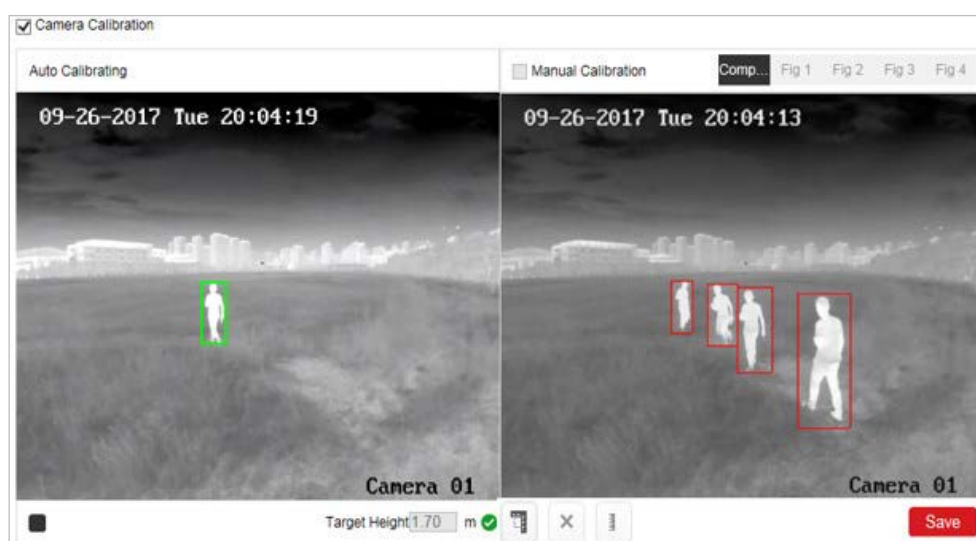
#### **Kroki:**

1. Skonfiguruj wyświetlane informacje i ustawienia wykonywania zdjęć.
2. Ustaw opcję **Auto Calibration**.
  - a) Zaznacz pole wyboru **Camera Calibration**, aby włączyć tę funkcję.
  - b) Upewnij się, że tylko jedna osoba jest widoczna na podglądzie na żywo, i wprowadź jej wzrost w polu tekstowym Target Height.
  - c) Kliknij przycisk ►, aby rozpocząć kalibrację automatyczną.

#### **Uwagi:**

- Upewnij się, że w polu widzenia nie znajdują się żadne ruchome obiekty z wyjątkiem danej osoby.
- Kalibracja automatyczna rozpocznie się, gdy cała sylwetka osoby znajdzie się w polu widzenia kamery, i zakończy się po ustawieniu osoby w punkcie końcowym (odległość punktu końcowego od kamery wyrażona w metrach jest cztery razy większa niż ogniskowa wyrażona w milimetrach). Na przykład dla ogniskowej 7 mm zalecana odległość punktu końcowego wynosi 28 m (7\*4).

- Po rozpoczęciu kalibracji osoba powinna iść zygzakiem.
  - Upewnij się, że ścieżka ruchu obejmuje lewą, środkową i prawą część obrazu.
  - Czas trwania konfiguracji automatycznej nie powinien być krótszy niż 10 sekund ani dłuższy niż 10 minut. Teoretycznie przejście ścieżką w kształcie podwójnego „Z” powinno być wystarczające.
  - W przypadku zakłóceń powodowanych przez liście/drzewa w podglądzie na żywo zalecane jest ustawienie maski.
3. Po wyjściu osoby z pola widzenia kliknij, aby zatrzymać kalibrację automatyczną.





Rysunek 9–16 Kalibracja automatyczna

### Weryfikacja:

1. Kliknij przycisk **Enable Verification** .

#### Uwagi:

- Należy zweryfikować nie tylko osobę, ale również inne obiekty w polu widzenia. Przykładem może być samochód lub lampa uliczna.
  - Weryfikacja umożliwia ustawienie tylko wysokości linii. Szerokość w poziomie nie jest mierzona.
2. Kliknij przycisk **Vertical Verify**  i przeciągnij pionową linię na obrazie.
  3. Kliknij przycisk **Calibration** , aby obliczyć długość.



4. Porównaj obliczoną długość linii z rzeczywistą długością obiektu, aby zweryfikować ustawienia kalibracji.



Rysunek 9–17 Weryfikacja kalibracji


**Uwaga:**

Jeżeli konfiguracja automatyczna nie powiedzie się lub wynik weryfikacji będzie negatywny, kliknij karty od Fig 1 do Fig 4, aby ustalić, czy prawidłowo zidentyfikowano osobę/obiekt na zdjęciach. Jeżeli tak, wykonaj kalibrację ręcznie.

5. (Opcjonalnie) Ustaw opcję **Manual Calibration**.
  - a) Zaznacz pole wyboru **Manual Calibration**.
  - b) Wybierz kartę Fig 1.



Rysunek 9–18 Kalibracja ręczna

- c) Kliknij przycisk  i przeciągnij pionową linię, aby dopasować ją do obiektu.

- d) Wprowadź rzeczywistą długość linii kalibracyjnej.
- e) (Opcjonalnie) Można kliknąć ikonę ×, aby usunąć linię kalibracyjną.
- f) Gdy pojawi się znacznik wyboru (v), wybierz karty od Fig 2 do Fig 4 i powtórz krok 3.
- g) Kliknij **Save**.

**Uwagi:**

- Należy rozdzielić cztery pionowe linie w lewej, środkowej i prawej części obrazu.
- Należy rozdzielić cztery pionowe linie na kierunku osi optycznej w bliskiej, średniej i dużej odległości.
- Na czterech zdjęciach kalibrowany obiekt nie musi być ten sam. Wybierz odpowiedni obiekt na każdym zdjęciu.
- Jeżeli wynik kalibracji ręcznej jest nieprawidłowy, zresetuj obiekt w celu ponownej kalibracji.


**Weryfikacja:**

Skorzystaj z procedury weryfikacji **Kalibracja automatyczna**.


### 9.3.3 Konfigurowanie maskowanego obszaru

Ta funkcja umożliwia wyznaczenie obszaru chronionego, w którym analiza zachowań nie jest wykonywana. Obsługiwane są maksymalnie cztery obszary chronione.

**Kroki:**

1. Wyświetl okno **Configuration > VCA > Shield Region**.
2. Kliknij kartę **Shield Region**, aby wyświetlić okno konfiguracji obszaru chronionego.
3. Kliknij symbol sześciokąta , aby wyznaczyć obszar chroniony, klikając punkty końcowe lewym przyciskiem myszy w podglądzie na żywo, i kliknij prawym przyciskiem w celu zakończenia wyznaczania obszaru.

**Uwagi:**

- Obsługiwany jest wielokątny obszar o maksymalnie dziesięciu bokach.
- Aby usunąć wyznaczone obszary, należy kliknąć przycisk .

- Jeżeli podgląd na żywo zostanie zatrzymany, nie można wyznaczyć obszarów chronionych.
4. Kliknij przycisk „**Save**”, aby zapisać ustawienia.

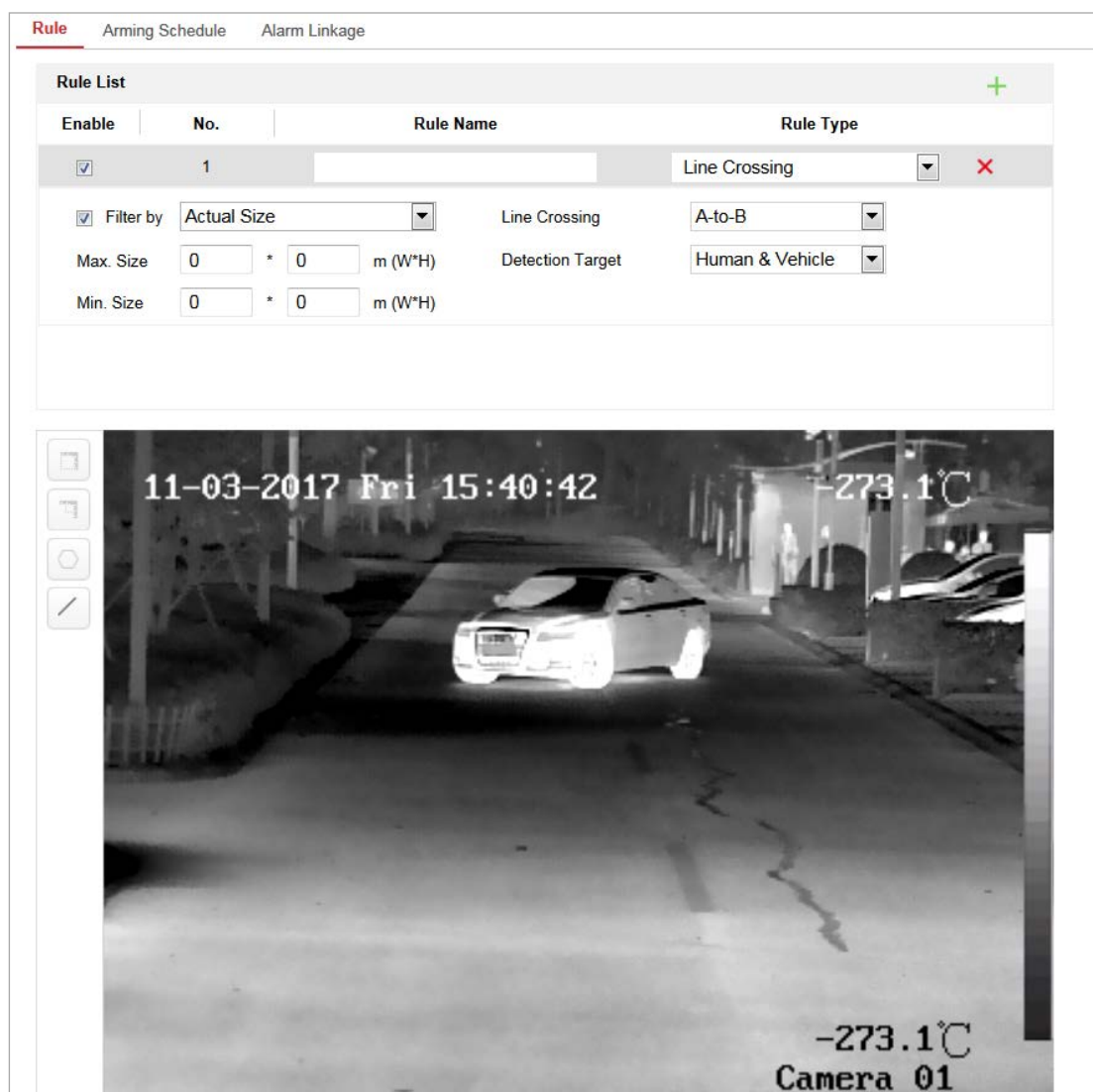
### 9.3.4 Konfigurowanie reguły

Analiza zachowań obejmuje między innymi detekcję przekroczenia linii, wtargnięcia, wejścia w obszar i opuszczenie obszaru.

**Uwaga:** Aby uzyskać więcej informacji na temat poszczególnych zachowań, zobacz odpowiednie rozdziały.

**Kroki:**

1. Wyświetl okno **Configuration > VCA > Rule**.
2. Kliknij kartę **Rule**, aby wyświetlić okno konfiguracji reguł.
3. Zaznacz pole wyboru pojedynczej reguły, aby uwzględnić ją w analizie zachowań.
4. Wybierz typ reguły, ustaw typ filtru, a następnie wyznacz linię/obszar w podglądzie wideo na żywo dla pojedynczej reguły.



Rysunek 9–19 Konfigurowanie reguły

**Przykład:**

- Wybierz typ reguły przekroczenia linii.
- Ustaw typ filtru Actual Size po skonfigurowaniu kalibracji kamery.
- Wprowadź szerokość i wysokość w polach Max. Size i Min. Size. Tylko obiekt docelowy o wymiarach, które należą do zakresu określonego przez ustawienia Max. Size i Min. Size, będzie powodować wyzwolenie alarmu.
- Ustaw obiekt detekcji Human, Vehicle lub Human & Vehicle przy użyciu listy Detection Target. Tylko obiekty wybranego typu będą wyzwalać alarm.

**Uwaga:**

Jeżeli chcesz prawidłowo wykrywać osoby, których sylwetka ma szerokość 0,5 metra i wysokość 1,8 metra, zalecane są poniższe ustawienia.

**Min. Size: 0.4\*0.8(m)**

**Max. Size: 1.5\*2.5(m)**

**Detection Target: Human.**

e) Wyznacz linię na podglądzie na żywo i wybierz kierunek przekroczenia linii.

**Uwaga:** Obsługiwanych jest maksymalnie osiem reguł.

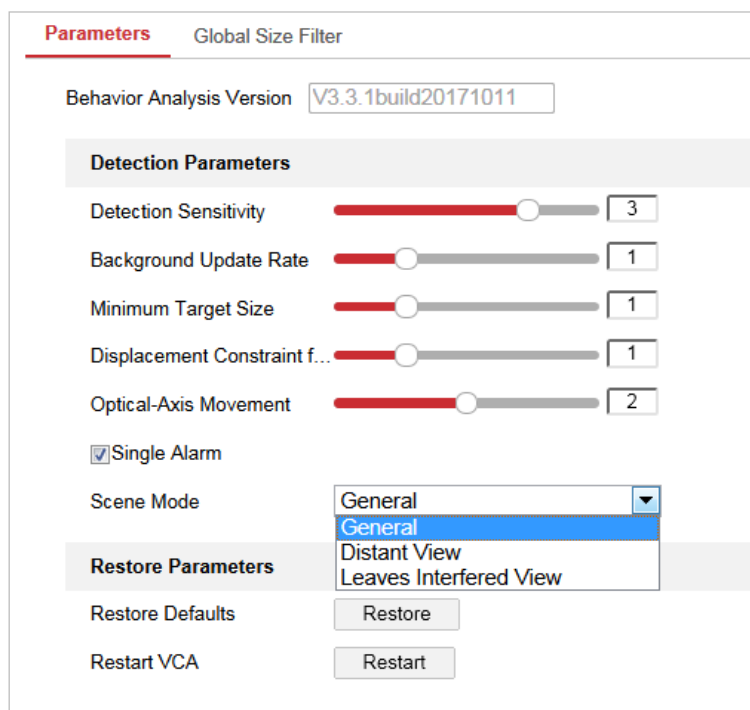
5. Kliknij przycisk „**Save**“, aby zapisać ustawienia.
6. Kliknij kartę **Arming Schedule**, aby ustawić godzinę harmonogramu dla poszczególnych reguł.
7. Kliknij kartę **Linkage Method** i zaznacz pole wyboru odpowiedniego działania powiązanego dla poszczególnych reguł.

### 9.3.5 Konfiguracja zaawansowana

Behavior Analysis Version: Wersja biblioteki algorytmów.

- **Parameter**

Skonfiguruj następujące parametry, aby szczegółowo określić konfigurację.



Rysunek 9–20 Konfiguracja zaawansowana

**Detection Sensitivity** [0 - 4]: Czulość wykrywania celu przez kamerę. Im wyższa wartość, tym łatwiej cel jest wykrywany, jednak liczba nieuzasadnionych alertów jest większa. Zalecana jest wartość domyślna 3.

**Background Update Rate** [0 - 4]: Szybkość zastępowania poprzedniej sceny nową sceną. Zalecana jest wartość domyślna 3.

**Minimum Target Size** [0~4]: Gdy rozmiar obiektu jest mniejszy niż ustawiona wartość, reguła VCA systemu nie jest uwzględniana. Zalecana jest wartość domyślna 1.

**Displacement Constraint for Target Generation** [0~4]: Dotyczy to obiektu powodującego reakcję. Im wyższa wartość, tym precyzyjniej, ale również wolniej, jest identyfikowany obiekt docelowy.

**Optical-Axis Movement**: Jeżeli obiekt porusza się na osi optycznej kamery, ustaw czulość ruchu na osi optycznej. Im niższa wartość, tym precyzyjniej, ale również wolniej, jest identyfikowany obiekt docelowy.

**Single Alarm**: Jeżeli zostanie wybrany pojedynczy alarm, cel w skonfigurowanym obszarze spowoduje wyzwolenie alarmu tylko jeden raz. Jeżeli to pole wyboru nie jest zaznaczone, ten sam cel spowoduje włączenie ciągłego alarmu w tym samym skonfigurowanym obszarze.

#### **Scene Mode:**

- **General**: W trybie General analiza zachowania działa prawidłowo.
- **Distant View**: Jeżeli kamera jest zainstalowana poza budynkami, wybierz tryb Distant View.
- **Leaves Interfered View**: Jeżeli kamera jest zainstalowana w lokalizacji, w której drzewa lub liście mogą przesłaniać widok, wybierz tryb Leaves Interfered View.

**Restore Default**: Kliknij, aby przywrócić domyślne ustawienia skonfigurowanych parametrów.

**Restart VCA**: Ponowne uruchomienie biblioteki algorytmów analizy zachowań.

- **Global Size Filter**

**Uwaga**: W przeciwieństwie do lokalnego filtra rozmiarów w regule globalny filtr rozmiarów dotyczy wszystkich reguł.

**Kroki:**

1. Wyświetl okno **Configuration > VCA > Advanced Configuration**.
2. Zaznacz pole wyboru **Global Size Filter**, aby włączyć tę funkcję.
3. Wybierz ustawienie Actual Size lub Pixel opcji Filter Type.

**Actual Size:** Długość i szerokość dla rozmiaru maksymalnego i minimalnego. Tylko obiekt docelowy o rozmiarze większym niż wartość minimalna i mniejszym niż wartość maksymalna będzie powodować wyzwolenie alarmu.

**Uwagi:**

- Należy skonfigurować kalibrację kamery, jeżeli zostanie wybrane filtrowanie według rzeczywistego rozmiaru.
- Długość/szerokość rozmiaru maksymalnego powinna być większa niż długość/szerokość rozmiaru minimalnego.

**Pixel:** Kliknij przycisk rozmiaru minimalnego, aby narysować prostokąt o minimalnym rozmiarze w podglądzie na żywo. Kliknij przycisk rozmiaru maksymalnego, aby narysować prostokąt o maksymalnym rozmiarze w trybie podglądu na żywo. Obiekt mniejszy niż rozmiar minimalny i większy niż rozmiar maksymalny zostanie odrzucony przez filtr.

**Uwagi:**

- Wyznaczony obszar zostanie skonwertowany na piksel przez algorytm tła.
  - Nie można skonfigurować globalnego filtra rozmiarów, jeżeli podgląd na żywo zostanie zatrzymany.
  - Długość/szerokość rozmiaru maksymalnego powinna być większa niż długość/szerokość rozmiaru minimalnego.
4. Kliknij **Save**, aby zapisać ustawienia.

## 9.4 Pomiar temperatury

### 9.4.1 Ustawienia podstawowe

**Cel:**

Urządzenie może mierzyć rzeczywistą temperaturę monitorowanego miejsca. Gdy temperatura przekracza wartość progową temperatury, uruchomiony zostaje alarm urządzenia.

**Uwaga:** Przed skorzystaniem z funkcji pomiaru temperatury, wyświetl okno **Configuration > System > Maintenance > VCA Resource Type**, aby wybrać ustawienie **Temperature Measurement + Behavior Analysis** z listy VCA Resource Type.

**Kroki:**

1. Wyświetl okno **Configuration > Temperature Measurement > Basic Settings**.

The screenshot shows the 'Basic Settings' configuration window for temperature measurement. The window has three tabs: 'Basic Settings' (selected), 'Advanced Settings', and 'Linkage Method'. Under 'Basic Settings', there are several options: 'Channel No.' is set to 'Camera2'; 'Enable Temperature Measurement' is checked; 'Enable Color-Temperature' is checked; 'Display Temperature Info. on Stream' is checked; 'Add Original Data on Capture' is unchecked; 'Add Original Data on Stream' is unchecked; 'Data Refresh Interval' is set to 3 seconds; 'Unit' is set to 'Degree Celsius(°C)'; 'Temperature Range' is set to '-20.0~150.0'; 'Version' is 'V1.0.7build20161221'. Below these is a section titled 'Manual Temperature Me...' with 'Emissivity' set to 0.98 and 'Distance' set to 20 meters. A red 'Save' button is at the bottom.

Rysunek 9–21 Ustawienia podstawowe

2. Zaznacz pola wyboru w interfejsie, aby ustawić konfigurację pomiaru temperatury.



- **Enable Temperature Measurement:** Zaznacz pole wyboru, aby włączyć funkcję pomiaru temperatury.
- **Enable Color-Temperature:** Zaznacz pole wyboru, aby wyświetlić paletę temperatury w podglądzie na żywo.
- **Display Temperature Info. on Stream:** Zaznacz pole wyboru, aby wyświetlić informacje o temperaturze w trybie podglądu na żywo.
- **Add Original Data on Capture:** Zaznacz pole wyboru, aby nanieść oryginalne dane na wykonane zdjęcie.
- **Add Original Data on Stream:** Zaznacz pole wyboru, aby nanieść oryginalne dane na strumień.
- **Data Refresh Interval:** Wybierz interwał odświeżania danych w przedziale czasu od 1 do 5 sekund.
- **Unit:** Wyświetlanie temperatury w stopniach Celsjusza (°C)/stopniach Fahrenheita (°F)/Kelwinach (K).
- **Temperature Range:** Ustaw zakres temperatury.
- **Emissivity:** Ustaw emisyjność obiektu docelowego. Uwaga: Emisyjność każdego obiektu jest inna.
- **Algorithm Version:** Wyświetlanie wersji bieżącego algorytmu.
- **Distance (m):** Odległość w linii prostej pomiędzy celem a urządzeniem.

3. Kliknij przycisk „Save“, aby zapisać ustawienia.

## 9.4.2 Konfigurowanie reguły pomiaru temperatury

### **Zanim rozpoczniesz:**

Zazwyczaj funkcja pomiaru temperatury jest używana razem z funkcją alarmu. Można ustawić powiązanie alarmu, tak aby każdy alarm właściwy/wstępny mógł wyzwalać powiązany alarm.

### **Cel:**

Ta funkcja służy do pomiaru temperatury wykrytego miejsca. Urządzenie porównuje temperatury wybranych obszarów i alarmów.

**Kroki:**

● (Tryb zwykły)

1. Wyświetl okno **Configuration > Temperature Measurement > Advanced Settings**.

2. Wybierz tryb konfiguracji **Normal**.
3. Skonfiguruj parametry.

**Emissivity:** Ustaw emisyjność obiektu docelowego. Uwaga: Emisyjność każdego obiektu jest inna.

**Distance (m):** Odległość w linii prostej pomiędzy celem a urządzeniem.

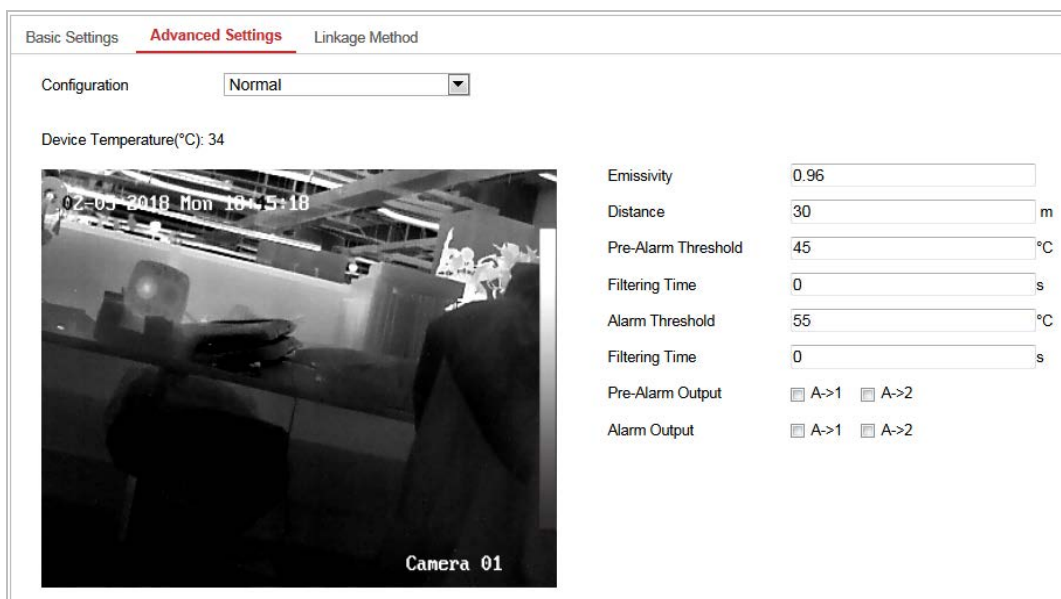
- **Pre-Alarm:** Gdy temperatura obiektu docelowego przekroczy wartość **Pre-Alarm Threshold** i ten stan będzie utrzymywać się przez czas NIE krótszy niż ustawienie **Filtering Time**, zostanie wyzwolony alarm wstępny.

Zaznacz pole wyboru **Pre-Alarm Output**, aby ustawić powiązanie alarmu wstępnego z podłączonym urządzeniem alarmowym.

- **Alarm:** Gdy temperatura obiektu docelowego przekroczy wartość **Alarm Threshold** i ten stan będzie utrzymywać się przez czas NIE krótszy niż ustawienie **Filtering Time**, zostanie wyzwolony alarm.

Zaznacz pole wyboru **Alarm Output**, aby ustawić powiązanie alarmu wstępnego z podłączonym urządzeniem alarmowym.

4. Kliknij **Save**.



Rysunek 9–22 Konfiguracja pomiaru temperatury

- (Tryb zaawansowany)
  1. Wyświetl okno **Configuration > Temperature Measurement > Advanced Settings**.
  2. Wybierz tryb konfiguracji **Expert**.
  3. Skonfiguruj parametry.
 

**Name:** Można dostosować nazwę reguły.

**Type:** Wybierz typ reguły **Point**, **Line** lub **Area**.

**Emissivity:** Ustaw emisyjność obiektu docelowego. Emisyjność każdego obiektu jest inna. Aby uzyskać więcej informacji, zobacz Dodatek.

**Distance (m):** Odległość w linii prostej pomiędzy celem a urządzeniem.

**Reflective Temperature:** Jeżeli inny obiekt (np. lustro) odbija obraz obiektu docelowego, wprowadź wartość temperatury tła / temperatury obiektu odbijającego światło. Jeżeli nie, wyczyść pole wyboru.

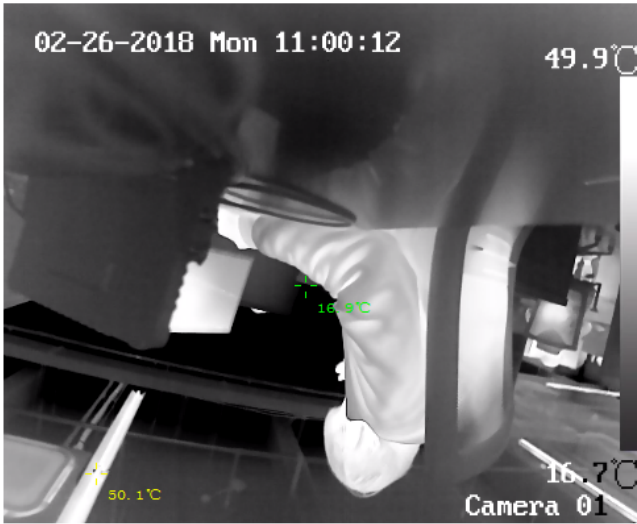
**Tolerance Temperature:** Wyzwolony alarm NIE jest wyłączany do chwili, gdy temperatura / różnica temperatur jest niższa/wyższa od temperatury reguły z uwzględnieniem tolerancji temperatury.

**Przykład:** Ustaw tolerancję 3°C i ustaw temperaturę alarmu 55°C. Alarm zostanie włączony po osiągnięciu temperatury 55°C i zostanie wyłączony tylko wówczas, gdy temperatura będzie niższa niż 52°.

Basic Settings **Advanced Settings** Linkage Method

Configuration

Device Temperature(°C): 30



02-26-2018 Mon 11:00:12

49.9°C

16.9°C

16.7°C

50.1°C

Camera 01

▼ ▲ ▼ 🔍 🔍

◀ ⏪ ▶ ⏩

▶ ▼ ◀ 🔍 🔍

4

1 Preset 1 ⚙️

2 Preset 2

3 Preset 3

4 Preset 4

5 Preset 5

6 Preset 6

7 Preset 7

8 Preset 8

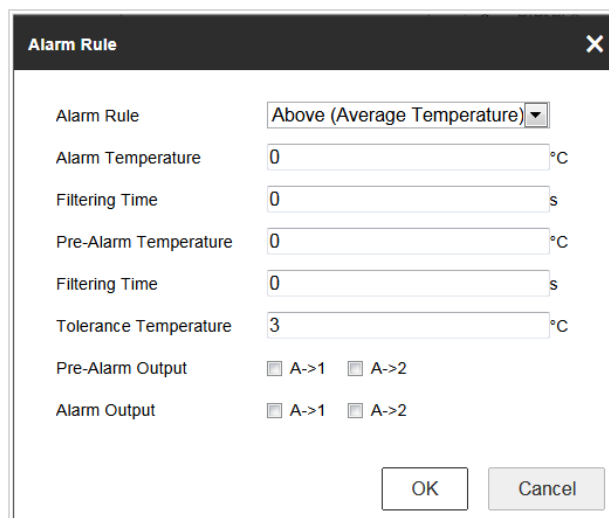
Enable	ID	Name	Type	Emissivity	Distance(...)	Reflective Temp...	Alarm Rule
<input type="checkbox"/>	1		Point ▼	0.96	30	<input type="checkbox"/> 20	<input checked="" type="checkbox"/>
<input type="checkbox"/>	2		Point ▼	0.96	30	<input type="checkbox"/> 20	<input checked="" type="checkbox"/>
<input type="checkbox"/>	3		Point ▼	0.96	30	<input type="checkbox"/> 20	<input checked="" type="checkbox"/>
<input type="checkbox"/>	4		Point ▼	0.96	30	<input type="checkbox"/> 20	<input checked="" type="checkbox"/>
<input type="checkbox"/>	5		Point ▼	0.96	30	<input type="checkbox"/> 20	<input checked="" type="checkbox"/>
<input type="checkbox"/>	6		Point ▼	0.96	30	<input type="checkbox"/> 20	<input checked="" type="checkbox"/>

Rysunek 9–23 Konfiguracja pomiaru temperatury

4. Zaznacz pole wyboru Enable, aby włączyć regułę alarmu.

**Reguła Point:**

a) Kliknij przycisk , aby wyświetlić ustawienia reguł alarmów.



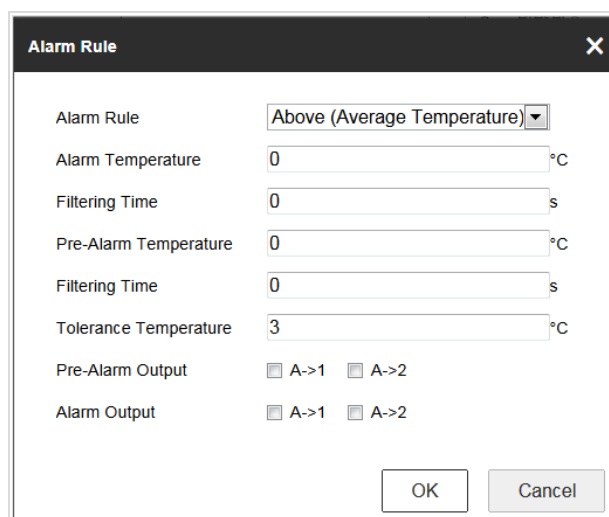
Rysunek 9–24 Ustawienia reguł alarmów (punkt)

- b) Ustaw opcję **Alarm Rule**.
- c) Ustaw opcje **Alarm Temperature**, **Pre-Alarm Temperature** i **Tolerance Temperature**.
- d) Ustaw opcję **Filtering Time**.
- e) Ustaw opcje **Pre-Alarm Output** i **Alarm Output** z podłączonym czujnikiem alarmowym i urządzeniem alarmowym.

Przykład: Wybierz ustawienie **Above (Average Temperature)** opcji **Alarm Rule** i ustaw temperaturę **Alarm Temperature** 50°C i czas filtrowania **Filtering Time** 5 sekund. W takiej konfiguracji urządzenie będzie alarmować, gdy przeciętna temperatura będzie niższa niż 50°C przez ponad 5 sekund.

#### Reguły Line i Area:

- a) Kliknij przycisk , aby wyświetlić ustawienia reguł alarmów.



Rysunek 9–25 Ustawienia reguł alarmów (linia)

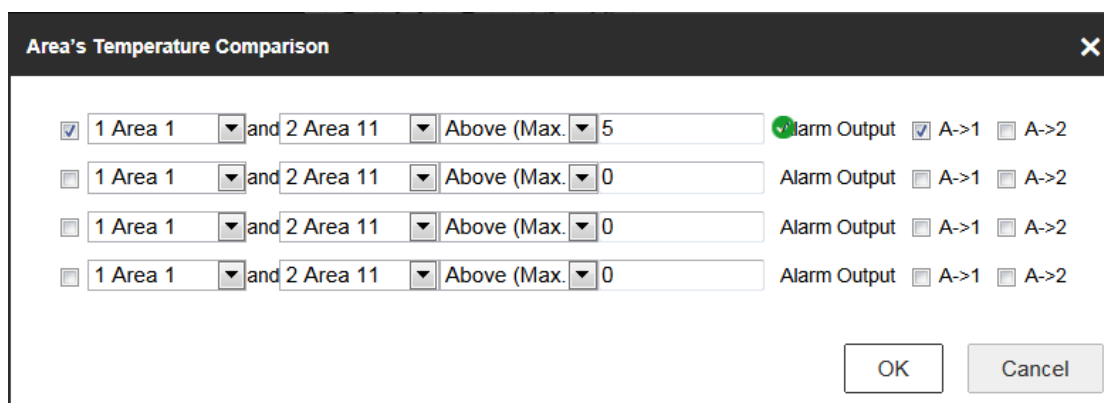
- b) Ustaw opcję **Alarm Rule**.
- c) Ustaw opcje **Alarm Temperature**, **Pre-Alarm Temperature** i **Tolerance Temperature**.
- d) Ustaw opcję **Filtering Time**.
- e) Ustaw opcje **Pre-Alarm Output** i **Alarm Output** z podłączonym czujnikiem alarmowym i urządzeniem alarmowym.

Przykład: Wybierz ustawienie Min. Temperature is Lower than opcji Alarm Rule i ustaw temperaturę Alarm Temperature 40°C. W takiej konfiguracji urządzenie będzie alarmować, gdy minimalna temperatura będzie niższa niż 40°C.

#### Porównanie temperatury obszaru:

Upewnij się, że obszary są przygotowane do porównania.

- a) Kliknij przycisk Area's Temperature Comparison, aby wyświetlić okno porównania temperatury obszaru.
- b) Wybierz obszary.



Rysunek 9–26 Alarm porównania temperatury obszaru

- c) Wybierz regułę porównania.
- d) Ustaw wartość progową różnicy temperatur.

Przykład: Wybierz obszary **Area 1** i **Area 11**, a następnie ustaw regułę porównania **Above (Max. Temperature)** i wartość progową różnicy temperatur 5°C. Urządzenie będzie alarmować, gdy różnica maksymalnych temperatur dwóch obszarów jest wyższa niż 5°C.

### 9.4.3 Działania powiązane

#### **Cel:**

Ustaw działania powiązane z alarmem.

#### **Kroki:**

1. Wyświetl okno **Configuration > Temperature Measurement > Linkage Method**.
2. Ustaw harmonogram uzbrajania i działania powiązane.
  - **Arming Schedule:** Kliknij pasek czasu i przeciągnij wskaźnik myszy, aby wybrać przedział czasowy.
  - **Linkage Method:** Kliknij przycisk Linkage Method i zaznacz pole wyboru, aby wybrać działania powiązane. Można wybrać dźwiękowy sygnał ostrzegawczy, powiadomienie centrum monitoringu, wysłanie wiadomości e-mail, przekazanie do serwera FTP lub wyzwolenie wyjścia alarmowego. W interfejsie tym można określić działania powiązane z wystąpieniem zdarzenia.
3. Kliknij przycisk „**Save**“, aby zapisać ustawienia.

Po skonfigurowaniu ustawień można wyświetlać bieżącą temperaturę i wilgotność w tym oknie.

# Rozdział 10 Ustawienia

## magazynowania nagrań i zdjęć

### Zanim rozpoczniesz:

Aby skonfigurować ustawienia nagrywania, upewnij się, że skonfigurowano sieciowe lub lokalne urządzenie magazynujące.

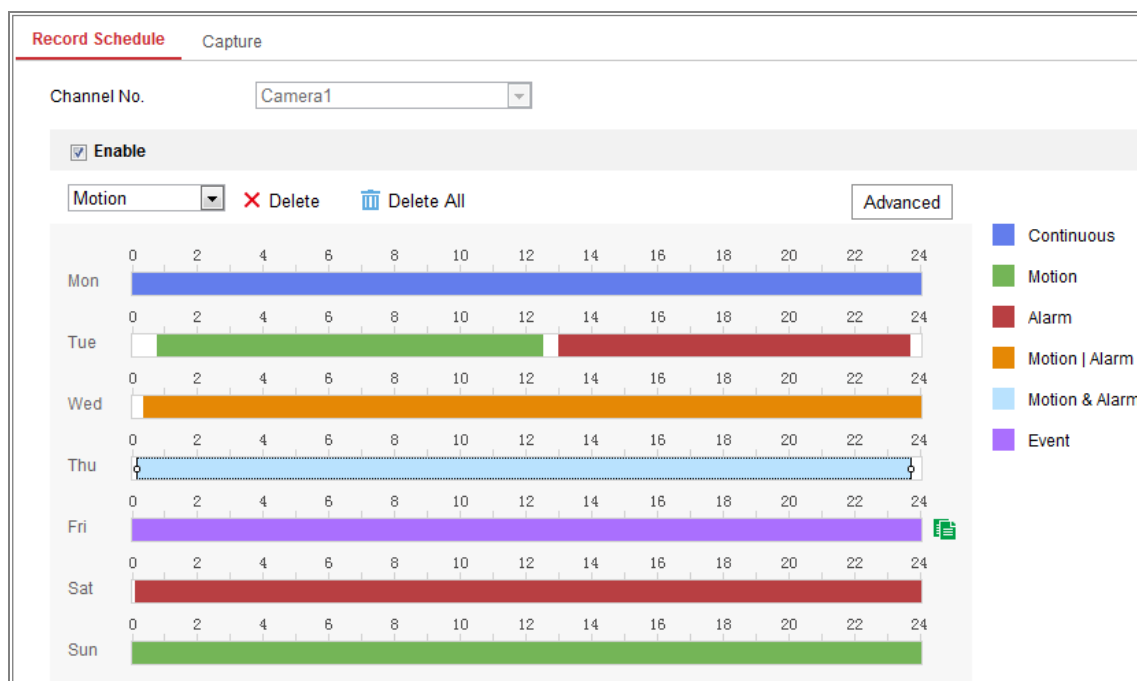
### 10.1 Konfigurowanie harmonogramu nagrywania

#### Cel:

Dostępne są dwa tryby nagrywania dla kamer: ręczne i zaplanowane. W tym rozdziale zamieszczono instrukcje dotyczące konfiguracji nagrywania według harmonogramu. Domyślnie pliki nagrań wykonanych zgodnie z harmonogramem są przechowywane w magazynie lokalnym lub na dysku sieciowym.

#### Kroki:

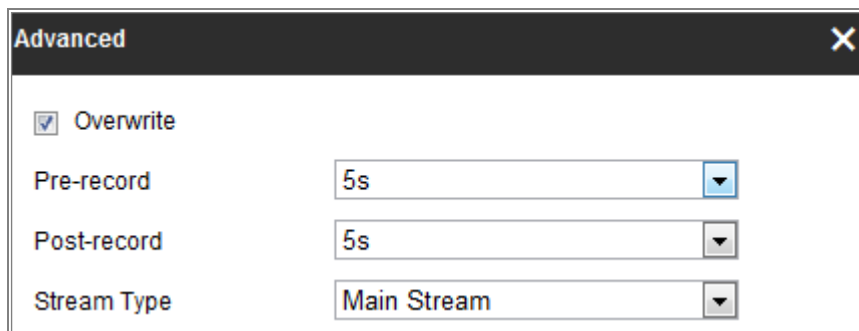
- Przejdź do interfejsu ustawień harmonogramu nagrywania, wybierając opcje: **Configuration > Storage > Schedule Settings > Record Schedule.**



Rysunek 10–1 Harmonogram nagrywania



2. Zaznacz pole wyboru „**Enable**“, aby włączyć nagrywanie według harmonogramu.
3. Kliknij przycisk **Advanced**, aby skonfigurować parametry nagrywania kamery.



Rysunek 10–2 Parametry nagrywania

- **Pre-record:** Funkcja ta służy do rozpoczęcia nagrywania przed zdarzeniem lub ustawionym za pomocą harmonogramu okresem nagrywania. Jeżeli na przykład alarm wyzwala nagrywanie o godz. 10:00 i skonfigurowano czas nagrywania z wyprzedzeniem 5 sekund, kamera rozpocznie nagrywanie o godz. 9:59:55.

Dostępne ustawienia nagrywania z wyprzedzeniem to No Pre-record, 5s, 10s, 15s, 20s, 25s, 30s lub Not limited.

- **Post-record:** Funkcja ta służy do przedłużenia nagrywania po zdarzeniu lub po zakończeniu ustawionego za pomocą harmonogramu okresu nagrywania. Jeżeli na przykład alarm wyzwolił nagrywanie o godz. 11:00 i skonfigurowano czas nagrywania z opóźnieniem 5 sekund, kamera będzie nagrywać do godz. 11:00:05.

Dostępne ustawienia nagrywania z opóźnieniem to 5s, 10s, 30s, 1 min, 2 min, 5 min lub 10 min.

- **Stream Type:** Wybierz typ strumienia do nagrywania.

**Uwaga:** Konfiguracje parametrów nagrywania są zależne od modelu kamery.

4. Wybierz **Typ Nagrywania**. Dostępne są następujące ustawienia rodzaju nagrywania: Ciągłe, Detekcja ruchu, Alarm, Ruch lub alarm, Ruch i alarm oraz Zdarzenie.

- **Nieprzerwane**

Jeśli wybrano opcję „**Continuous**“, wówczas obraz wideo będzie nagrywany automatycznie zgodnie z harmonogramem.

- **Nagrywanie wyzwalane przez funkcję detekcji ruchu.**

Jeśli wybrano opcję „**Motion Detection**“, wówczas obraz wideo zostanie nagrany w momencie wykrycia ruchu.

Oprócz konfigurowania harmonogramu nagrywania należy ustawić obszar detekcji ruchu i zaznaczyć pole wyboru Trigger Channel w pozycji Linkage Method w oknie ustawień detekcji ruchu. Aby uzyskać więcej informacji, zobacz **Zadanie 1: Ustawianie obszaru detekcji ruchu** w sekcji 9.1.1.

- **Nagrywanie wyzwalane przez alarm**

Jeśli wybrano opcję „**Alarm**“, wówczas obraz wideo zostanie nagrany w momencie wyzwolenia alarmu za pośrednictwem kanałów wejścia zewnętrznego alarmu.

Aby móc skorzystać z tej funkcji, oprócz harmonogramu nagrywania należy także ustawić parametr „**Alarm Type**“ i zaznaczyć pole „**Trigger Channel**“ w zakładce „**Linkage Method**“ w interfejsie **Alarm Input Settings**. Aby uzyskać więcej informacji, zobacz sekcję 9.1.3.

- **Nagrywanie wyzwalane przez funkcję detekcji ruchu i alarm**

Jeśli wybrano opcję „**Motion & Alarm**“, wówczas obraz wideo zostanie nagrany w momencie jednoczesnego wykrycia ruchu i wyzwolenia alarmu.

Aby móc skorzystać z tej funkcji, oprócz harmonogramu nagrywania należy także skonfigurować ustawienia w interfejsie **detekcji ruchu** i **ustawień wejścia alarmu**. Aby uzyskać szczegółowe informacje, patrz *Rozdział 9.1.1* i *Rozdział 9.1.3*.

- **Nagrywanie wyzwalane przez ruch lub alarm (Motion | Alarm)**

Jeżeli wybrano ustawienie **Motion | Alarm**, wówczas obraz wideo zostanie nagrany w momencie wyzwolenia alarmu lub wykrycia ruchu.

Aby móc skorzystać z tej funkcji, oprócz harmonogramu nagrywania należy także skonfigurować ustawienia w interfejsie **detekcji ruchu** i **ustawień wejścia alarmu**. Aby uzyskać szczegółowe informacje, patrz *Rozdział 9.1.1* i *Rozdział 9.1.3*.

- **Nagrywanie wyzwalane po wystąpieniu zdarzeń**

Jeżeli zostanie wybrane ustawienie **Event**, wideo będzie nagrywane, jeżeli wystąpią jakiegokolwiek zdarzenia. Należy skonfigurować harmonogram nagrywania i ustawienia zdarzeń.

- Wybierz rodzaj nagrywania, a następnie kliknij myszą i przeciągnij jej wskaźnik na pasku czasu, aby skonfigurować harmonogram nagrywania.
- Kliknij przycisk „Save“, aby zapisać ustawienia.

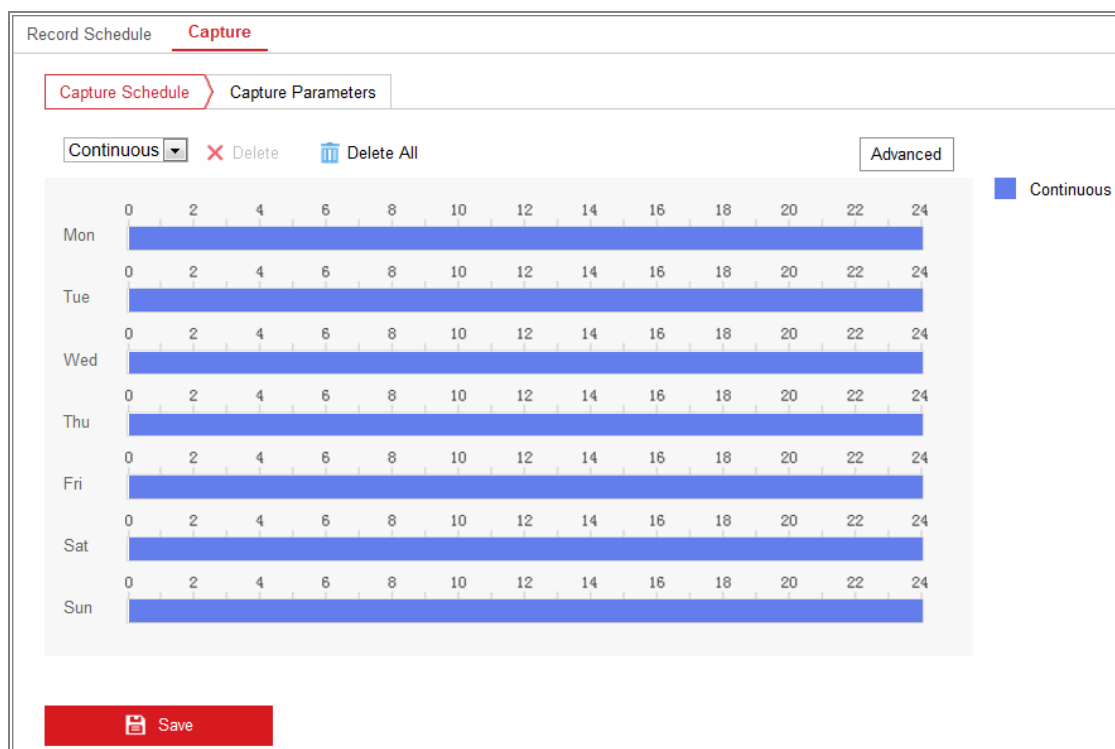
## 10.2 Konfigurowanie harmonogramu wykonywania zdjęć

### Cel:

Możesz skonfigurować wykonywanie zdjęć według harmonogramu i wykonywanie zdjęć wyzwolone przez zdarzenia. Zarejestrowane zdjęcie może zostać zapisane w lokalnym lub sieciowym magazynie.

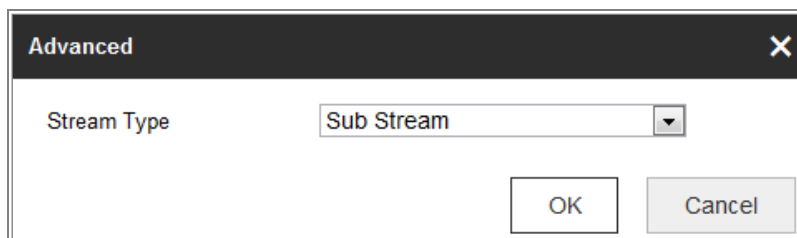
### Kroki:

- Wyświetl okno Ustawienia wykonywania zdjęć: **Configuration > Storage > Storage Settings > Capture**.



Rysunek 10–3 Konfiguracja wykonywania zdjęć

- Przejdź do karty **Capture Schedule**, aby skonfigurować harmonogram wykonywania zdjęć, klikając myszą i przeciągając jej wskaźnik na pasku czasu. Można skopiować harmonogram nagrywania do innych dni, klikając zieloną ikonę kopiowania po prawej stronie obok paska czasu.
- Kliknij przycisk **Advanced**, aby wybrać typ strumienia.



Rysunek 10–4 Zaawansowane ustawienia harmonogramu wykonywania zdjęć

- Kliknij przycisk „**Save**”, aby zapisać ustawienia.
- Przejdź do karty **Capture Parameters**, aby skonfigurować parametry wykonywania zdjęć.
  - Zaznacz pole wyboru **Enable Timing Snapshot**, aby włączyć tryb ciągłego wykonywania zdjęć.
  - Wybierz format zdjęcia, rozdzielczość, jakość i interwał wykonywania zdjęć.
  - Zaznacz pole wyboru „**Enable Event-triggered Snapshot**”, aby włączyć wykonywanie zdjęć w momencie wystąpienia zdarzenia.
  - Wybierz format zdjęcia, rozdzielczość, jakość, interwał wykonywania zdjęć i liczbę zdjęć.

Record Schedule **Capture**

Capture Schedule > Capture Parameters

**Timing**

Enable Timing Snapshot

Format: JPEG

Resolution: 704\*576

Quality: High

Interval: 500 millisecond

**Event-Triggered**

Enable Event-Triggered Snapshot

Format: JPEG

Resolution: 704\*576

Quality: High

Interval: 500 millisecond

Capture Number: 4

**Save**

Rysunek 10–5 Ustawianie parametrów wykonywania zdjęć

6. Ustaw odstęp czasowy pomiędzy wykonywaniem zdjęć.
7. Kliknij przycisk „**Save**“, aby zapisać ustawienia.

## 10.3 Konfigurowanie sieciowego dysku HDD

### **Zanim rozpoczniesz:**

Dysk sieciowy powinien być dostępny w sieci i prawidłowo skonfigurowany do przechowywania plików nagrań, plików rejestru, zdjęć itp.

### **Kroki:**

1. Dodaj dysk Net HDD.
  - (1) Wyświetl okno ustawień Net HDD (**Configuration > Storage > Storage Management > Net HDD**).

HDD No.	Server Address	File Path	Type	Delete
1	10.10.36.61	/cxy_1	NAS	✘
2	10.10.36.252	/dvr/yangjian_1	NAS	✘
3			NAS	✘

Mounting Type:  User Name:  Password:

Rysunek 10–6 Dodawanie dysku sieciowego

- (2) Wprowadź adres IP dysku sieciowego i ścieżkę plików.
- (3) Wybierz typ protokołu udostępniania. Dostępne opcje to „NFS” i „SMB/CIFS”. Jeżeli zostanie wybrane ustawienie SMB/CIFS, można skonfigurować nazwę użytkownika i hasło, aby zapewnić ochronę.

**Uwaga:** Aby uzyskać informacje o tworzeniu ścieżki zapisu plików, należy zapoznać się z *Instrukcją obsługi urządzeń magazynujących dołączonych do sieci (NAS)*.

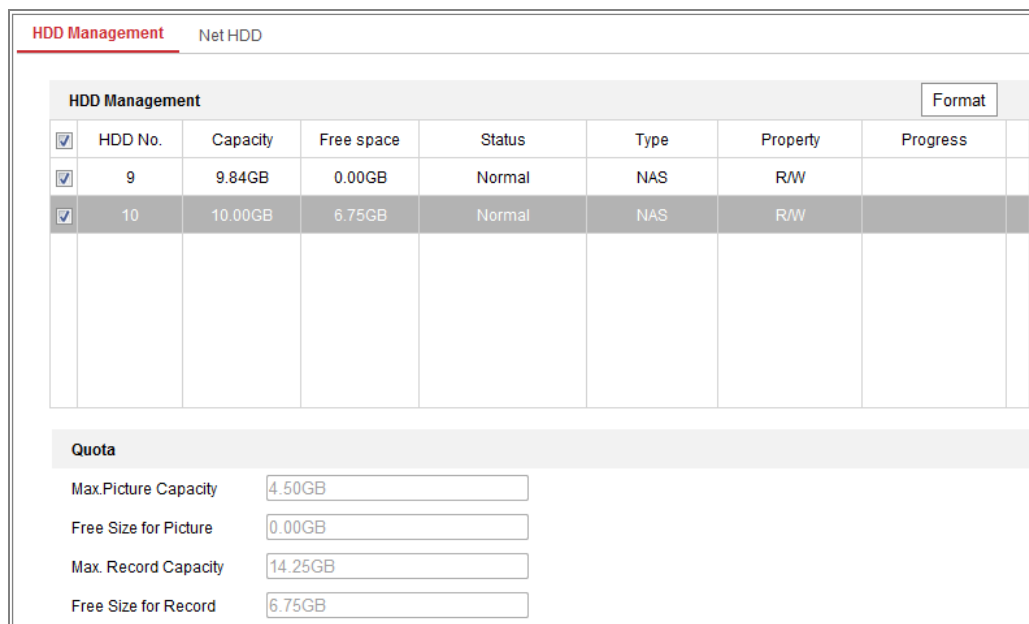


- W celu lepszej ochrony systemu i prywatności użytkownika przed zagrożeniami zdecydowanie zaleca się korzystanie z silnych haseł do zabezpieczenia wszystkich funkcji i urządzeń sieciowych. Należy wybrać własne hasło (co najmniej osiem znaków należących do co najmniej trzech z następujących kategorii: wielkie litery, małe litery, cyfry i znaki specjalne) w celu zapewnienia lepszej ochrony urządzenia.
- Instalator i/lub użytkownik końcowy są zobowiązani do prawidłowego skonfigurowania wszystkich haseł i innych ustawień zabezpieczeń.

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

## 2. Inicjowanie dodanego dysku sieciowego

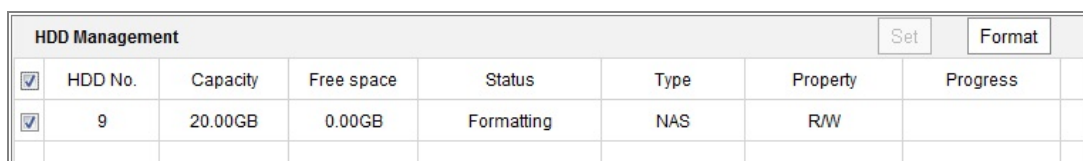
- (1) Przejdź do interfejsu ustawień dysku HDD, wybierając opcje: „**Configuration**” > „**Storage**” > „**Storage Management**” > „**HDD Management**”. W interfejsie tym wyświetlane są informacje o pojemności dysku, dostępnym wolnym miejscu, stanie, typie i właściwościach dysku.



Rysunek 10–7 Zarządzanie magazynem

- (2) Jeśli stan dysku to „**Uninitialized**”, zaznacz pole wyboru przy dysku i kliknij opcję „**Format**”, aby rozpocząć inicjowanie dysku.

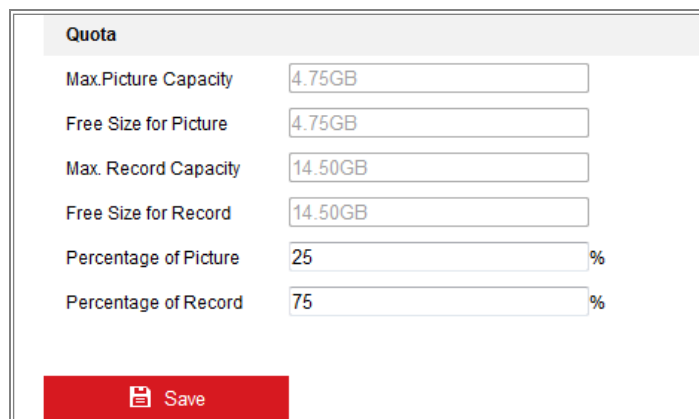
Po zakończeniu inicjowania stan dysku zmieni się na „**Normal**”.



Rysunek 10–8 Wyświetlanie stanu dysku

3. Zdefiniuj przydział dla nagrywania i wykonywania zdjęć.

- (1) Wprowadź procentową wartość przydziału magazynowania nagrań i zdjęć.  
 (2) Kliknij przycisk „**Save**” i odśwież stronę przeglądarki, aby aktywować ustawienia.



Rysunek 10–9 Ustawienia przydziału

**Uwaga:**

Do kamery można przyłączyć do 8 dysków NAS.

## 10.4 Detekcja karty pamięci

**Cel:**

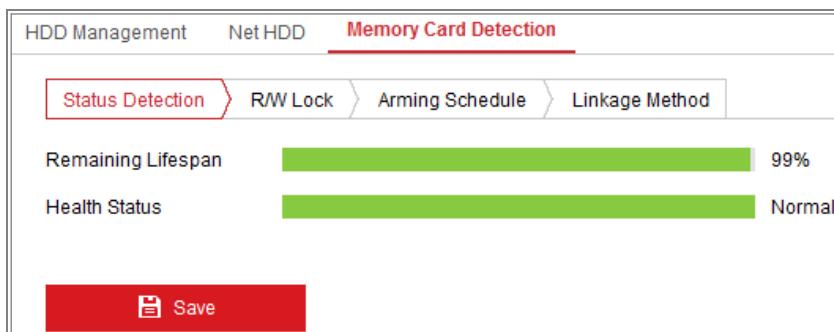
Funkcja detekcji karty pamięci umożliwia wyświetlanie informacji dotyczących stanu karty pamięci, blokowanie karty pamięci i powiadamianie o wykryciu usterki karty pamięci.

**Uwaga:** Funkcja wykrywania karty pamięci jest dostępna tylko w przypadku niektórych typów kart pamięci i modeli kamer. Jeżeli ta karta nie jest wyświetlana na odpowiedniej stronie internetowej, oznacza to, że kamera nie obsługuje tej funkcji lub zainstalowana karta pamięci nie jest obsługiwana przez tę funkcję. Aby uzyskać informacje dotyczące kart pamięci obsługiwanych przez tę funkcję, należy skontaktować się z dystrybutorem lub sprzedawcą detalicznym.

**Kroki:**

1. Wyświetl okno konfiguracji Detekcja karty pamięci:

### Configuration > Storage > Storage Management > Memory Card Detection



Rysunek 10–10 Detekcja karty pamięci

2. Wyświetl informacje dotyczące stanu karty pamięci na karcie **Status Detection**.

**Remaining Lifespan:** Procentowo wyrażony pozostały czas przydatności do użytku.

Czas przydatności karty do użytku jest zależny od czynników takich jak jej pojemność i szybkość transmisji bitów. Należy wymienić kartę pamięci, jeżeli zbliża się koniec okresu jej przydatności do użytku.

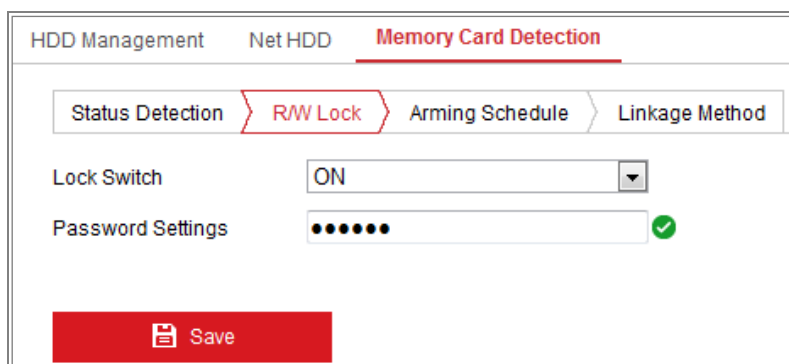


**Health Status:** Informacje dotyczące kondycji karty pamięci. Wyświetlane są trzy etykiety opisujące kondycję: „dobra”, „zła” i „uszkodzony”. Użytkownik jest powiadamiany, jeżeli kondycja jest inna niż „dobra”, po skonfigurowaniu ustawień **Arming Schedule** i **Linkage Method**.

**Uwaga:** Zalecana jest wymiana karty pamięci, gdy jej kondycja jest inna niż „dobra”.

3. Kliknij kartę **R/W Lock**, aby dodać blokadę do karty pamięci.

Jeżeli dodano blokadę odczytu/zapisu, kartę można odczytywać i zapisywać tylko po odblokowaniu.



Rysunek 10–11 Ustawianie blokady odczytu/zapisu

- Dodanie blokady
  - (1) Wybierz z listy **Lock Switch** ustawienie ON.
  - (2) Wprowadź hasło.
  - (3) Kliknij przycisk „**Save**”, aby zapisać ustawienia.
- Odblokowanie
  - (1) Jeżeli kamera zablokuje zainstalowaną w niej kartę pamięci, odblokowanie następuje automatycznie, a użytkownicy nie muszą wykonywać żadnych czynności w celu odblokowania karty.
  - (2) Jeżeli karta pamięci (z blokadą) zostanie użyta w innej kamerze, można wyświetlić okno **HDD Management**, aby ręcznie odblokować kartę. Wybierz kartę pamięci i kliknij przycisk **Unlock** wyświetlany obok przycisku **Format**. Następnie wprowadź poprawne hasło, aby usunąć blokadę.

**Uwagi:**

- Kartę można odczytywać i zapisywać tylko po odblokowaniu.
  - Jeżeli zostaną przywrócone ustawienia fabryczne kamery, która zablokowała kartę pamięci, można usunąć blokadę, korzystając z okna Zarządzanie dyskami twardymi.
- Usuwanie blokady
    - (1) Wybierz z listy **Lock Switch** ustawienie **OFF**.
    - (2) Wprowadź poprawne hasło w polu tekstowym **Password Settings**.
    - (3) Kliknij przycisk „**Save**“, aby zapisać ustawienia.
4. Skonfiguruj ustawienia **Arming Schedule** i **Linkage Method**, jeżeli chcesz otrzymać powiadomienie w przypadku zmiany stanu kondycji karty pamięci na stan inny niż „dobra”. Zobacz **Zadanie 2: Konfigurowanie harmonogramu zabezpieczenia dla funkcji detekcji ruchu** i **Zadanie 3: Ustawianie działania powiązanego z detekcją ruchu** w sekcji 9.1.1.
  5. Kliknij przycisk „**Save**“, aby zapisać ustawienia.

## 10.5 Konfigurowanie Magazynowania uproszczonego

**Cel:**

Gdy żaden poruszający się obiekt nie zostanie wykryty na monitorowanej scenie, można zmniejszyć liczbę klatek na sekundę i szybkość transmisji bitów strumienia wideo, aby zwiększyć czas trwania nagrań, które można przechowywać na karcie pamięci.

**Uwagi:**

- Funkcja magazynu uproszczonego jest zależna od modelu kamery.
  - Pliki wideo nagrywane w trybie magazynowania uproszczonego są odtwarzane z maksymalną liczbą klatek na sekundę (25/30), dlatego proces odtwarzania jest postrzegany przez użytkownika jako przyśpieszony.
1. Wyświetl okno Magazynowanie uproszczone:

**Configuration > Storage > Storage Management > Lite Storage**

2. Zaznacz pole wyboru **Enable**, aby włączyć funkcję magazynowania uproszczonego.
3. Wprowadź czas magazynowania w polu tekstowym. Na tej stronie wyświetlana jest ilość dostępnego miejsca na karcie SD.
4. Kliknij przycisk „**Save**”, aby zapisać ustawienia.

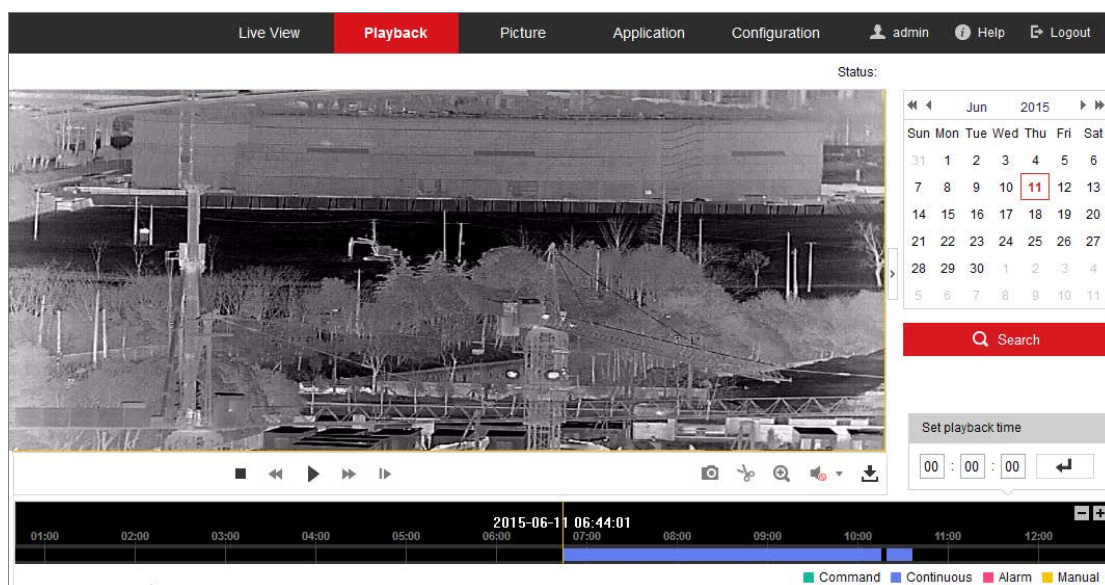
# Rozdział 11 Odtwarzanie

## Cel:

W tej sekcji wyjaśniono, jak wyświetlać zdalnie nagrywane pliki wideo, przechowywane na dyskach sieciowych lub kartach SD.

## Kroki:

1. Kliknij przycisk **Playback** na pasku menu, aby wyświetlić okno odtwarzania.



Rysunek 11–1 Okno odtwarzania

2. Wybierz datę i kliknij przycisk **Search**.



Rysunek 11–2 Wyszukiwanie pliku wideo

3. Kliknij przycisk ►, aby odtworzyć pliki wideo nagrane danego dnia.

Pasek narzędzi znajdujący się u dołu interfejsu odtwarzania może zostać użyty do sterowania procesem odtwarzania.






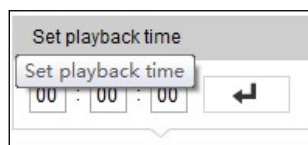
Rysunek 11–3 Pasek narzędzi odtwarzania

Tabela 11–1 Opis przycisków

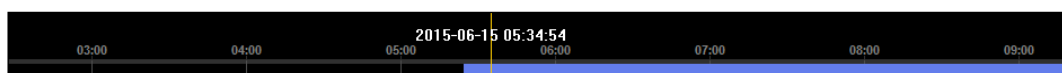
Przycisk	Opis	Przycisk	Opis
	Odtwarzanie		Rejestrowanie zdjęć
	Wstrzymanie		Rozpoczęcie/zakończenie przycinania plików wideo
	Zatrzymanie		Włączanie dźwięku i dostosowanie głośności/wyciszenie
	Zmniejszenie szybkości		Pobierz
	Zwiększenie szybkości		Odtwarzanie poklatkowe
	Włączanie/wyłączenie cyfrowego powiększenia		

**Uwaga:** Lokalne ścieżki zapisu pobranych plików wideo i zdjęć można ustawić w interfejsie konfiguracji lokalnej.

Można także wprowadzić czas i kliknąć przycisk , aby zlokalizować punkt odtwarzania ustawiony w polu „Set playback time“. Kliknij przyciski  , aby powiększyć/pomniejszyć pasek postępu.

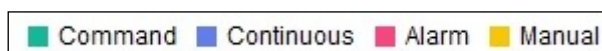


Rysunek 11–4 Ustawianie czasu odtwarzania



Rysunek 11–5 Pasek postępu

Typy wideo wyróżniono różnymi kolorami na pasku postępu.



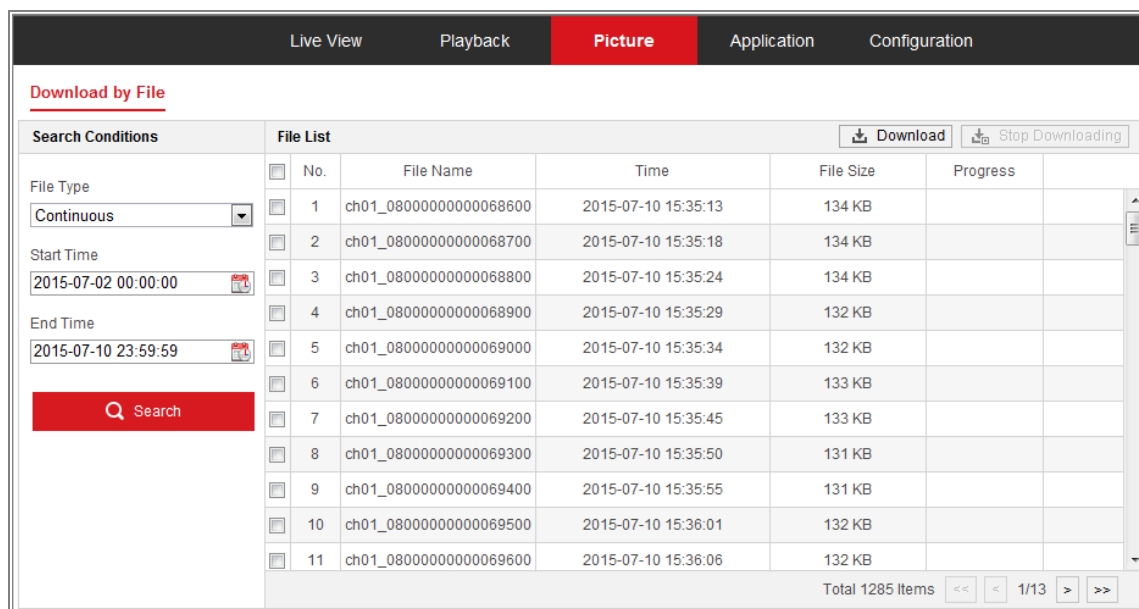
Rysunek 11–6 Typy wideo

## Rozdział 12 Zdjęcia

Kliknij przycisk Zdjęcia, aby wyświetlić okno wyszukiwania zdjęć. Można wyszukiwać, wyświetlać i pobierać zdjęcia przechowywane w magazynie lokalnym lub sieciowym.

### Uwagi:

- Aby skorzystać z funkcji wyszukiwania zdjęć, należy upewnić się, że poprawnie skonfigurowano dysk twardy, dysk NAS lub kartę pamięci.
- Należy upewnić się, że harmonogram wykonywania zdjęć został skonfigurowany. Przejdź do **Configuration > Storage > Schedule Settings > Capture**, aby skonfigurować harmonogram wykonywania zdjęć.



Rysunek 12–1 Wyszukiwanie zdjęć

### Kroki:

1. Wybierz typ pliku z listy rozwijanej. Dostępne są ustawienia Continuous, Motion, Alarm, Motion | Alarm, Motion & Alarm, Line Crossing, Intrusion Detection i Scene Change Detection.
2. Wybierz godzinę rozpoczęcia i godzinę zakończenia.
3. Kliknij przycisk **Search**, aby wyszukać pasujące zdjęcia.
4. Zaznacz pole wyboru zdjęć, a następnie kliknij przycisk **Download**, aby pobrać wybrane zdjęcia.

### Uwaga:

Za każdym razem można wyświetlić maksymalnie 4000 zdjęć.

# Aneks

## Aneks 1 Wprowadzenie do oprogramowania SADP

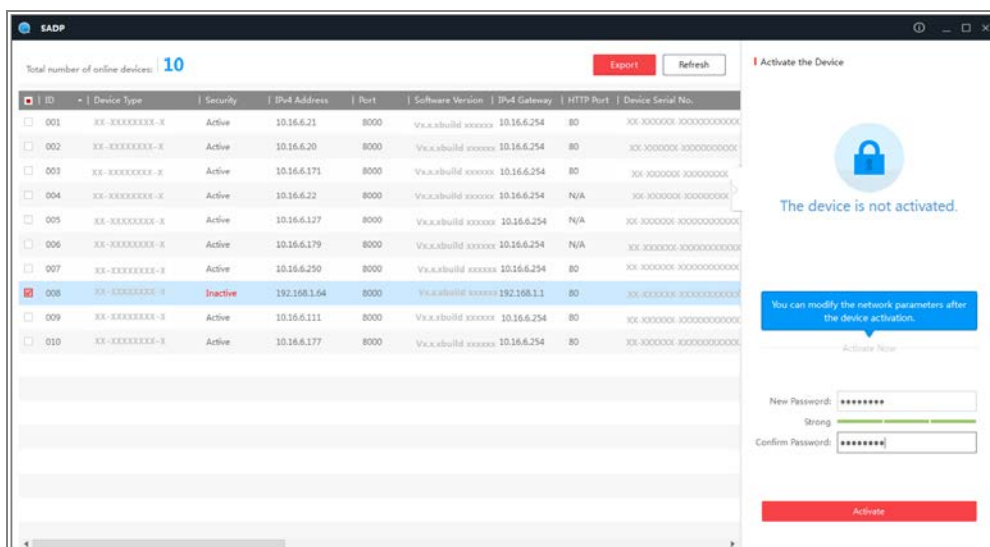
### ● Opis oprogramowania SADP

SADP (Search Active Devices Protocol) to przyjazne dla użytkownika i niewymagające instalacji narzędzie do wyszukiwania urządzeń połączonych z siecią. Oprogramowanie to wyszukuje urządzenia aktywne w podsieci użytkownika i wyświetla informacje o znalezionych urządzeniach. Za pomocą oprogramowania SADP można także zmienić podstawowe ustawienia sieciowe urządzeń.

### ● Wyszukiwanie aktywnych urządzeń połączonych z siecią

#### ◆ Automatyczne wyszukiwanie urządzeń połączonych z siecią

Po uruchomieniu oprogramowanie SADP automatycznie co 15 sekund wyszukuje urządzenia w podsieci, z którą połączony jest komputer użytkownika. W interfejsie urządzeń połączonych z siecią wyświetlana jest całkowita liczba wszystkich znalezionych urządzeń i informacje na ich temat. Wyświetlane informacje o urządzeniach obejmują typ urządzenia, adres IP, numer portu itp.

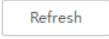


Rysunek A.1.1 Wyszukiwanie urządzeń połączonych z siecią





**Uwaga:**

Urządzenie można wyszukiwać i wyświetlać na liście 15 sekund po przełączeniu go do trybu online. Urządzenie zostanie usunięte z listy 45 sekund po przełączeniu go do trybu offline.


**◆ Ręczne wyszukiwanie urządzeń połączonych z siecią**

Kliknij przycisk , aby ręcznie odświeżyć listę urządzeń połączonych z siecią. Nowo wyszukane urządzenia zostaną dodane do listy.



Kliknij przycisk  lub  w nagłówku każdej z kolumn, aby zmienić porządek wyświetlania informacji o urządzeniach. Kliknij przycisk , aby rozwinąć tabelę urządzeń i ukryć panel parametrów sieciowych znajdujący się po prawej stronie lub kliknij przycisk , aby wyświetlić panel parametrów sieciowych.

**● Modyfikowanie parametrów sieciowych****Kroki:**

1. Wybierz z listy urządzenie, które chcesz modyfikować. Parametry sieciowe urządzenia zostaną wyświetlone w panelu „**Modify Network Parameters**“ po prawej stronie.
2. Możesz edytować te parametry sieciowe urządzeń, które są modyfikowalne, np. adres IP i numer portu.
3. Wprowadź hasło konta admin urządzenia w polu **Admin Password** i kliknij przycisk , aby zapisać zmiany.



- *W celu lepszej ochrony systemu i prywatności użytkownika przed zagrożeniami zdecydowanie zaleca się korzystanie z silnych haseł do zabezpieczenia wszystkich funkcji i urządzeń sieciowych. Należy wybrać własne hasło (co najmniej osiem znaków należących do co najmniej trzech z następujących kategorii: wielkie litery, małe litery, cyfry i znaki specjalne) w celu zapewnienia lepszej ochrony urządzenia.*



- Instalator i/lub użytkownik końcowy są zobowiązani do prawidłowego skonfigurowania wszystkich haseł i innych ustawień zabezpieczeń.

**Modify Network Parameters**

Enable DHCP

Device Serial No.:

IP Address:

Port:

Subnet Mask:

Gateway:

IPv6 Address:

IPv6 Gateway:

IPv6 Prefix Length:

HTTP Port:

Security Verification

Admin Password:

[Modify](#)

[Forgot Password](#)

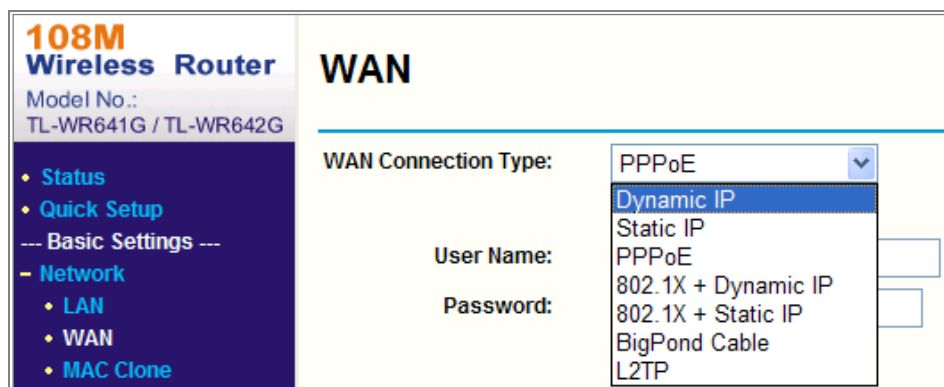
Rysunek A.1.2 Modyfikowanie parametrów sieciowych

## Aneks 2 Mapowanie portów

Następujące ustawienia dotyczą routera TP-LINK (TL-WR641G). Ustawienia są zależne od modelu routera.

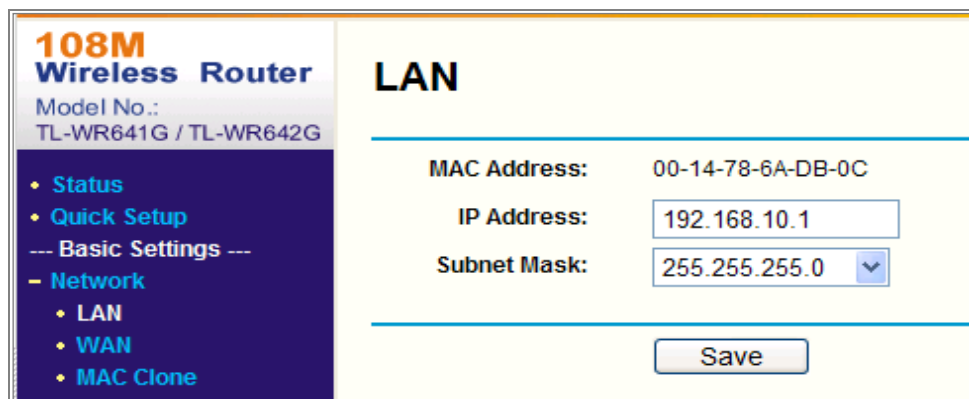
### Kroki:

- Wybierz parametr **WAN Connection Type**, jak przedstawiono poniżej:



Rysunek A.2.1 Wybór typu połączenia sieci WAN

- Skonfiguruj parametry sieci **LAN** routera, takie jak ustawienia adresu IP i maski podsieci, zgodnie z poniższym rysunkiem.



Rysunek A.2.2 Konfiguracja parametrów sieci LAN

- Ustaw mapowanie portu na serwerze wirtualnym **przekazywania**. Domyślnie kamera korzysta z portu 80, 8000 i 554. Można zmienić te wartości portów, korzystając z przeglądarki internetowej lub oprogramowania klienckiego.

**Przykład:**

Gdy kamery są podłączone do tego samego routera, można skonfigurować porty 80, 8000 i 554 jednej kamery z adresem IP 192.168.1.23 i porty 81, 8001, 555, 8201 innej kamery z adresem IP 192.168.1.24. Skorzystaj z poniższych kroków:

**Kroki:**

1. Zgodnie z powyższymi ustawieniami zmapuj port 80, 8000, 554 i 8200 dla kamery sieciowej z adresem 192.168.1.23.
2. Zmapuj port 81, 8001, 555 i 8201 dla kamery sieciowej z adresem 192.168.1.24.
3. Włącz obsługę protokołów **ALL** lub **TCP**.
4. Zaznacz pole wyboru **Enable** i kliknij przycisk **Save**, aby zapisać ustawienia.

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

Rysunek A.2.3 Mapowanie portów

**Uwaga:** Port kamery sieciowej nie powinien powodować konfliktu z innymi portami. Na przykład niektóre routery używają portu 80 do zarządzania internetowego. Zmień port kamery, jeżeli jest taki sam, jak port zarządzania.



See Far, Go Further