



HIKVISION

Termowizyjna kamera sieciowa typu bullet

Podręcznik użytkownika

UD02330B

Podręcznik użytkownika

COPYRIGHT ©2016 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

Ta instrukcja dotyczy termowizyjnej kamery sieciowej typu bullet (V5.3.7).

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 witrynie internetowej firmy (<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 OBOWIAZUJĄCE 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, WYRAŻNYCH 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.

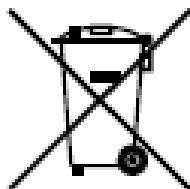
Deklaracja zgodności z dyrektywami Unii Europejskiej



Produkt i jego akcesoria (jeśli występują) są oznaczone znakiem „CE” i zgodne z obowiązującymi przepisami zharmonizowanych norm europejskich wymienionych w Dyrektywie 2014/30/UE w sprawie kompatybilności elektromagnetycznej oraz Dyrektywie 2011/65/UE w sprawie ograniczenia stosowania niektórych niebezpiecznych substancji w sprzęcie elektrycznym i elektronicznym.



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. Więcej informacji zamieszczono w następującej witrynie internetowej: 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.

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>Ostrzeżenia Należy przestrzegać tych środków ostrożności w celu uniknięcia poważnych obrażeń ciała lub śmierci.</p>	<p>Uwagi 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.
- Należy zainstalować w obwodzie zasilania wyłącznik ułatwiający odłączenie zasilania.
- 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).



Przestrogi:

- Przed użyciem kamery należy upewnić się, że napięcie sieci elektrycznej jest odpowiednie.
- Należy chronić kamerę przed upadkiem lub uderzeniem 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 intensywnego światła, takie jak słońce lub żarówka. Intensywne światło może spowodować nieodwracalne uszkodzenie kamery.
- Jeśli czujnik zostanie porażony wiązką laserową, może ulec spaleniu. Dlatego też podczas korzystania z urządzeń emitujących wiązki laserowe, należy upewnić się, że powierzchnia czujnika nie jest narażona na kontakt z wiązką laserową.
- Nie umieszczać kamery w bardzo wysokich lub niskich temperaturach (temperatura powinna mieścić się w zakresie $-40^{\circ}\text{C} \sim 65^{\circ}\text{C}$), zakurzonym lub wilgotnym otoczeniu i nie narażać jej na wysokie promieniowanie elektromagnetyczne.
- Aby uniknąć akumulacji ciepła, urządzeniu należy zapewnić odpowiednią wentylację w środowisku obsługi.
- Kamerę należy trzymać z dala od wody i płynów.
- W transporcie kamera powinna znajdować się w oryginalnym opakowaniu.
- 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

Rozdział 1	Wymagania systemowe.....	11
Rozdział 2	Połączenie sieciowe.....	12
2.1	Konfigurowanie kamery przy użyciu sieci LAN.....	12
2.1.1	Połączenie przewodowe za pośrednictwem sieci LAN	13
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
Rozdział 3	Dostęp do kamery sieciowej.....	24
3.1	Uzyskiwanie dostępu za pośrednictwem przeglądarki internetowej	24
3.2	Uzyskiwanie dostępu za pośrednictwem oprogramowania do zarządzania urządzeniami wideo	26
Rozdział 4	Widok na żywo.....	28
4.1	Interfejs podglądu na żywo	28
4.2	Uruchamianie podglądu na żywo.....	29
4.3	Ręczne nagrywanie i wykonywanie zdjęć.....	30
Rozdział 5	Konfiguracja kamery sieciowej	31
5.1	Konfigurowanie parametrów lokalnych.....	31
5.2	Konfigurowanie ustawień czasu	34
5.3	Konfigurowanie ustawień sieciowych	36
5.3.1	Konfigurowanie ustawień protokołu TCP/IP	36
5.3.2	Konfigurowanie ustawień portów	37
5.3.3	Konfigurowanie ustawień protokołu PPPoE	38
5.3.4	Konfigurowanie ustawień usługi DDNS	39
5.3.5	Konfigurowanie ustawień protokołu SNMP	42
5.3.6	Konfigurowanie ustawień standardu IEEE 802.1X.....	44
5.3.7	Konfigurowanie ustawień jakości usługi (QoS).....	45
5.3.8	Konfigurowanie ustawień UPnP™.....	46
5.3.9	Wysyłka wiadomości e-mail wyzwalana przez alarm	46
5.3.10	Konfiguracja ustawień translacji adresów sieciowych (NAT)	49
5.3.11	Konfigurowanie ustawień serwera FTP	49
5.3.12	Ustawienia protokołu HTTPS	51
5.4	Konfigurowanie ustawień audio i wideo.....	53
5.4.1	Konfigurowanie ustawień wideo	53
5.4.2	Konfigurowanie ustawień audio.....	55

5.4.3	Konfigurowanie kodowania ROI.....	56
5.5	Konfigurowanie parametrów obrazu	58
5.5.1	Konfigurowanie ustawień wyświetlania.....	58
5.5.2	Konfigurowanie ustawień menu ekranowego	60
5.5.3	Konfigurowanie ustawień nakładek tekstowych	62
5.5.4	Konfigurowanie maski prywatności	63
5.5.5	Konfigurowanie nakładania obrazu.....	64
5.5.6	Konfigurowanie DPC (korekcji wadliwych pikseli)	64
5.6	Konfigurowanie i obsługa zdarzeń alarmowych.....	65
5.6.1	Konfigurowanie detekcji ruchu	66
5.6.2	Konfigurowanie alarmu sabotażu sygnału wideo	71
5.6.3	Konfigurowanie wejścia alarmu.....	72
5.6.4	Konfigurowanie wyjścia alarmu.....	73
5.6.5	Obsługa zdarzeń nietypowych.....	74
5.6.6	Konfigurowanie detekcji nietypowego dźwięku	75
5.6.7	Detekcja zmiany sceny	76
5.6.8	Konfigurowanie dynamicznej detekcji źródła ognia	77
5.7	Pomiar temperatury.....	78
5.7.1	Konfiguracja pomiaru temperatury	78
5.7.2	Pomiar i alarm temperatury	79
5.8	Konfiguracja VCA	82
5.8.1	Typ zasobu VCA	82
5.8.2	Informacje VCA	82
5.8.3	Analiza zachowania.....	83
Rozdział 6	<i>Ustawienia magazynowania nagrań i zdjęć.....</i>	93
6.1	Zarządzanie magazynem	93
6.2	Konfigurowanie ustawień NAS	93
6.3	Konfigurowanie harmonogramu nagrywania	96
6.4	Konfigurowanie ustawień wykonywania zdjęć.....	102
Rozdział 7	<i>Odtwarzanie.....</i>	104
Rozdział 8	<i>Wyszukiwanie w rejestrze.....</i>	106
Rozdział 9	<i>Inne ustawienia.....</i>	108
9.1	Zarządzanie kontami użytkowników.....	108
9.2	Uwierzytelnianie	111
9.3	Użytkownik anonimowy.....	111
9.4	Filtr adresów IP	112
9.5	Usługa zabezpieczeń	114

9.6	Wyświetlanie informacji o urządzeniu	115
9.7	Konserwacja	116
9.7.1	Ponowne uruchamianie kamery.....	116
9.7.2	Przywracanie ustawień domyślnych.....	116
9.7.3	Eksportowanie/importowanie pliku konfiguracji	117
9.7.4	Uaktualnienie systemu.....	117
9.8	Ustawienia RS-485.....	118
9.9	Ustawienia usługi.....	119
<i>Załącznik</i>		<i>120</i>
Dodatek 1 Wprowadzenie do oprogramowania SADP		120
Dodatek 2 Mapowanie portów		123

Rozdział 1 Wymagania systemowe

System operacyjny: Microsoft Windows XP SP1 lub późniejsze wersje/Vista/Win7/Server 2003/Server 2008 32-bitowy

Procesor: Intel Pentium IV 3.0 GHz lub nowszy

Pamięć RAM: 1 GB lub więcej

Wyświetlacz: Rozdzielczość 1024 x 768 lub większa

Przeglądarka internetowa: Internet Explorer 6.0 lub nowsza wersja, Apple Safari 5.02 lub nowsza wersja, Mozilla Firefox 3.5 lub nowsza wersja oraz Google Chrome 8 lub nowsza wersja.

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:

- Jeśli chcesz ustawić kamerę sieciową przy użyciu sieci LAN (sieci lokalnej), zajrzyj do *rozdziału 2.1 Konfigurowanie kamery przy użyciu sieci LAN*.
- Jeśli chcesz ustawić kamerę sieciową przy użyciu sieci WAN (bezprzewodowej sieci rozległej), zajrzyj do *rozdziału 2.2 Konfigurowanie kamery przy użyciu sieci WAN*.

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.

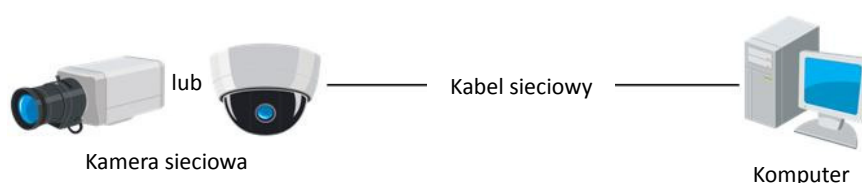
Uwaga: Aby uzyskać szczegółowe wprowadzenie do obsługi aplikacji SADP, należy zapoznać się z załącznikiem 1.

2.1.1 Połączenie przewodowe za pośrednictwem sieci LAN

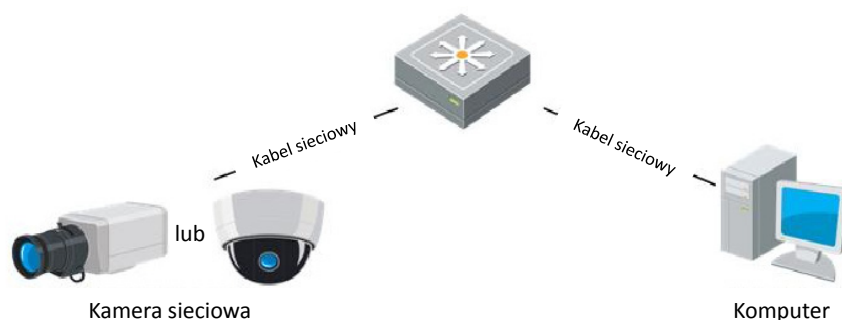
Na poniższych rysunkach przedstawiono dwie metody przewodowego połączenia kamery sieciowej z komputerem:

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 2–2.



Rysunek 2–1 Podłączenie bezpośrednie



Rysunek 2–2 Podłączenie przez przełącznik lub router

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.

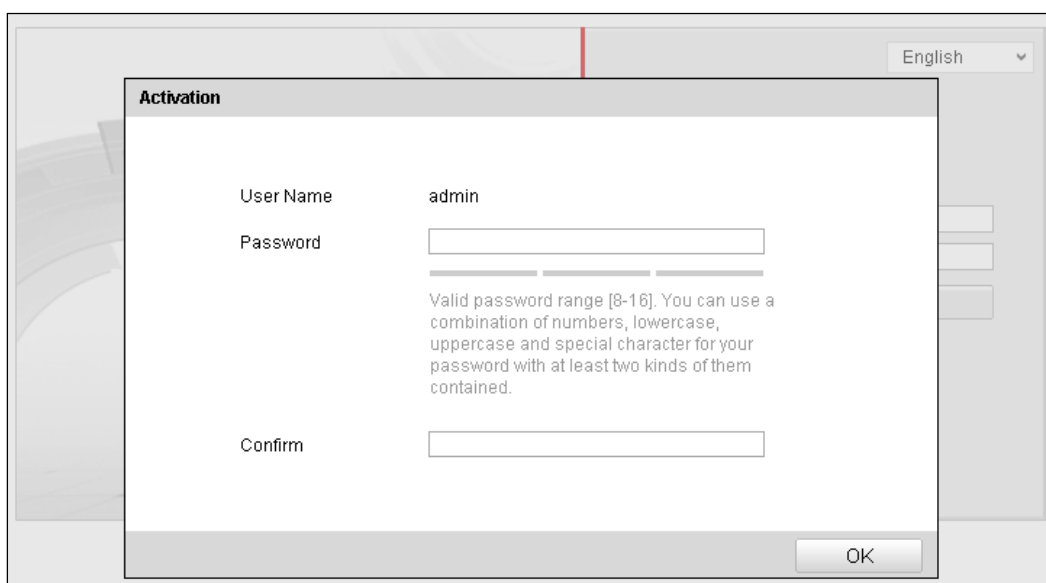
❖ Aktywacja za pośrednictwem przeglądarki internetowej

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.
- Aby kamera domyślnie korzystała z protokołu DHCP, należy aktywować ją za pomocą oprogramowania SADP. Zapoznaj się następującym Rozdziałem, aby uzyskać informacje na temat aktywacji za pomocą SADP.



Rysunek 2–3 Interfejs aktywacji (interfejs sieciowy)

3. Utwórz hasło i wprowadź je w polu hasła.



ZALECANE JEST STOSOWANIE SILNEGO HASŁA – Zdecydowanie zalecamy utworzenie silnego własnego hasła (minimum 8 znaków z uwzględnieniem wielkich i małych liter, cyfr i znaków specjalnych) w celu zapewnienia lepszej ochrony produktu. 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.

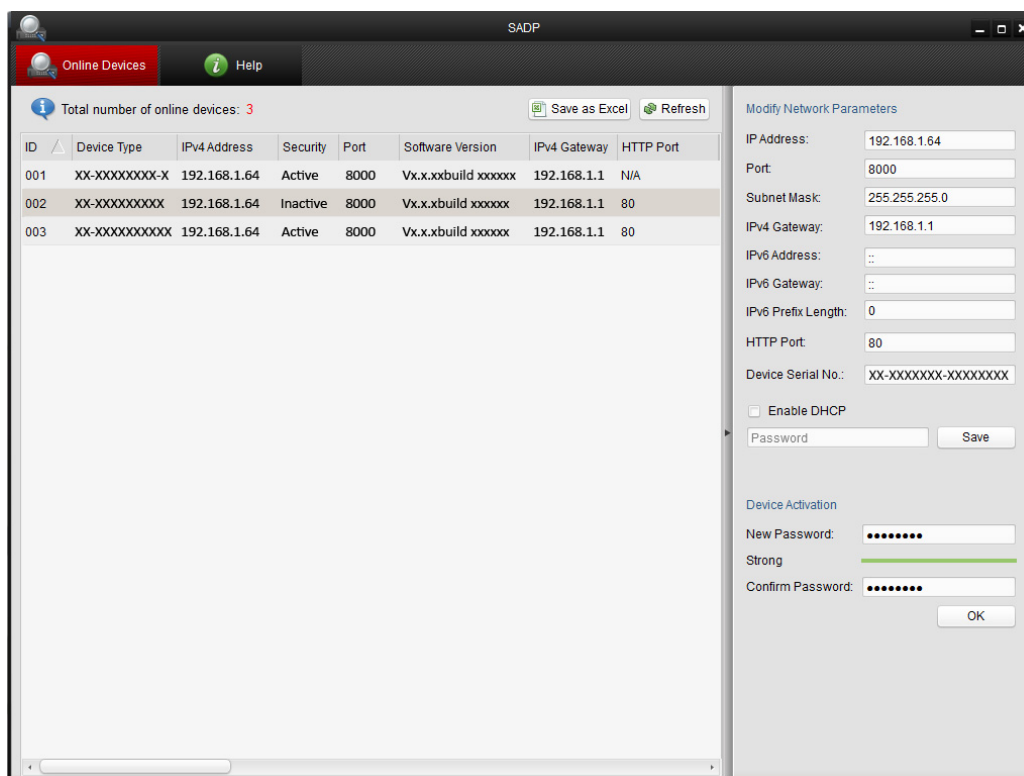
❖ **Aktywacja za pośrednictwem aplikacji SADP**

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 Interfejs SADP

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

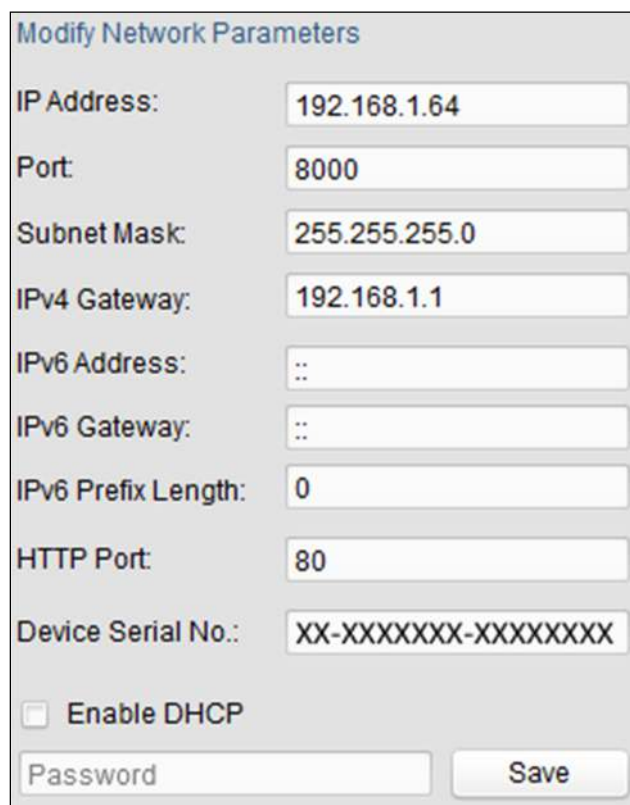


ZAŁECANE JEST STOSOWANIE SILNEGO HASŁA – Zdecydowanie zalecamy utworzenie silnego własnego hasła (minimum 8 znaków z uwzględnieniem wielkich i małych liter, cyfr i znaków specjalnych) w celu zapewnienia lepszej ochrony produktu. Zalecane jest również regularne resetowanie hasła. Zwłaszcza w systemie z restrykcyjnymi zabezpieczeniami resetowanie hasła co miesiąc lub co tydzień zapewnia lepszą ochronę urządzenia.

4. Kliknij przycisk „OK“, aby zapisać hasło.

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“, aby upewnić się, że kamera i komputer znajdują się w tej samej podsieci.



Modify Network Parameters

IP Address: 192.168.1.64

Port: 8000

Subnet Mask: 255.255.255.0

IPv4 Gateway: 192.168.1.1

IPv6 Address: ::

IPv6 Gateway: ::

IPv6 Prefix Length: 0

HTTP Port: 80

Device Serial No.: XX-XXXXXXX-XXXXXXX

☐ Enable DHCP

Password Save

Rysunek 2–5 Zmiana adresu IP

6. Wprowadź hasło i kliknij przycisk „Save“, aby aktywować zmieniony adres IP.

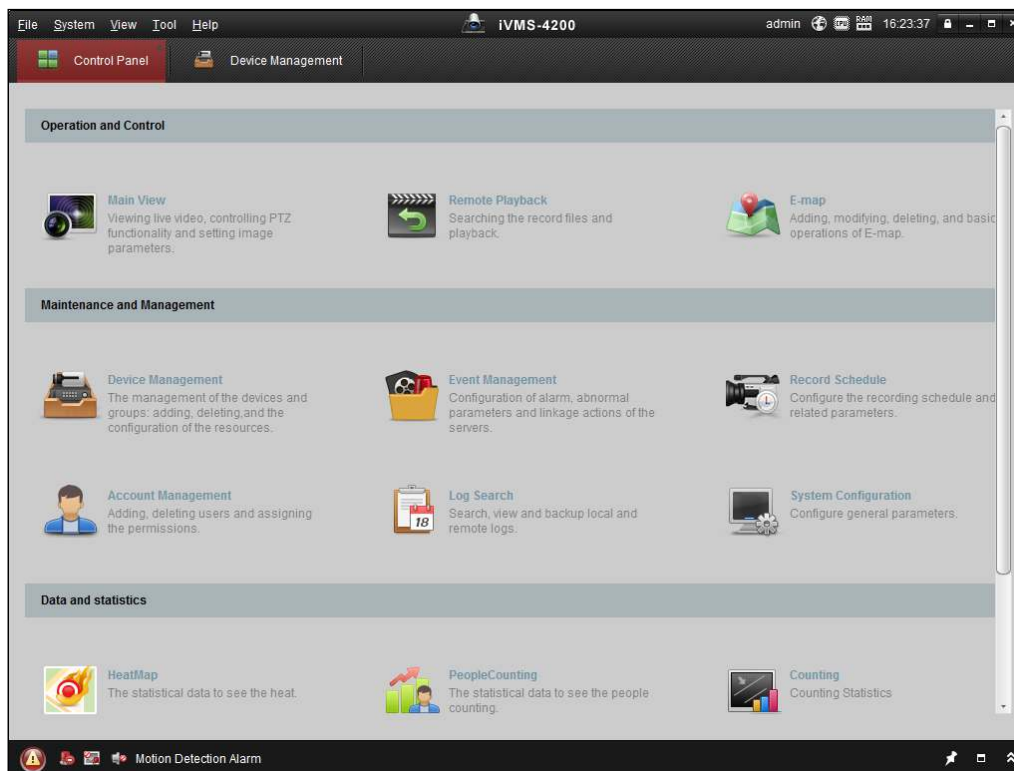
❖ Aktywacja za pośrednictwem oprogramowania do zarządzania urządzeniami wideo

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.

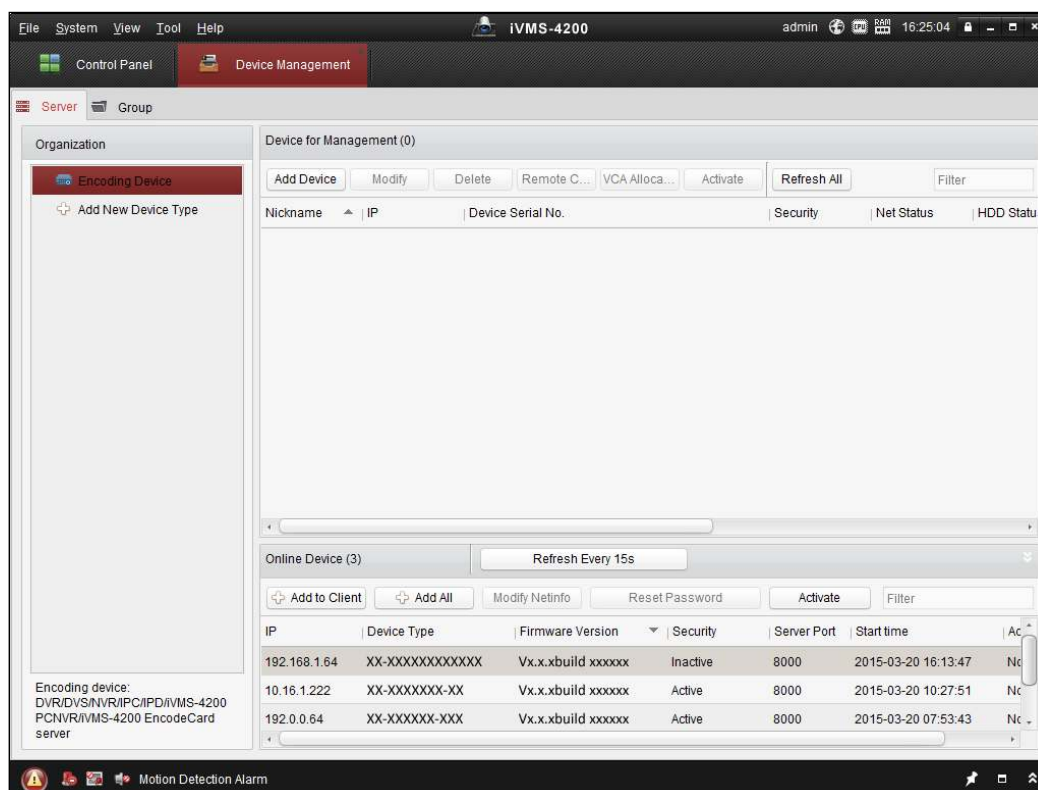
Kroki:

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 Device Management, jak pokazano na rysunku poniżej.

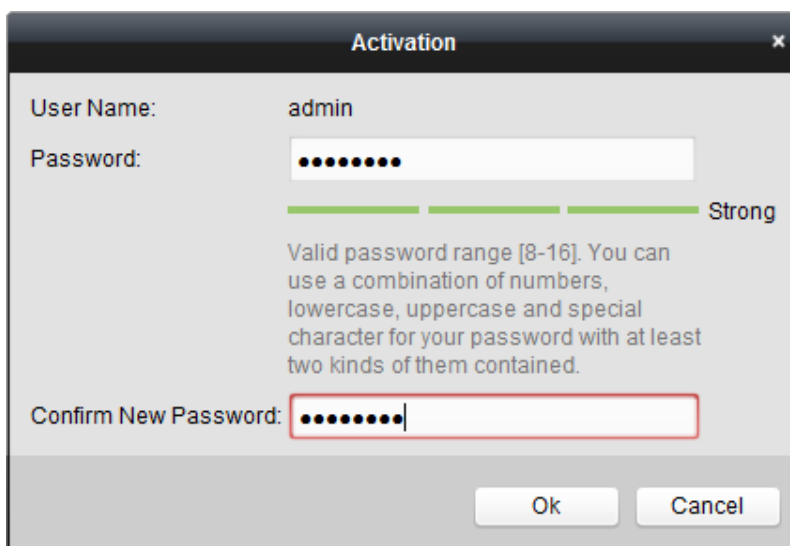


Rysunek 2–7 Interfejs zarządzania urządzeniami

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

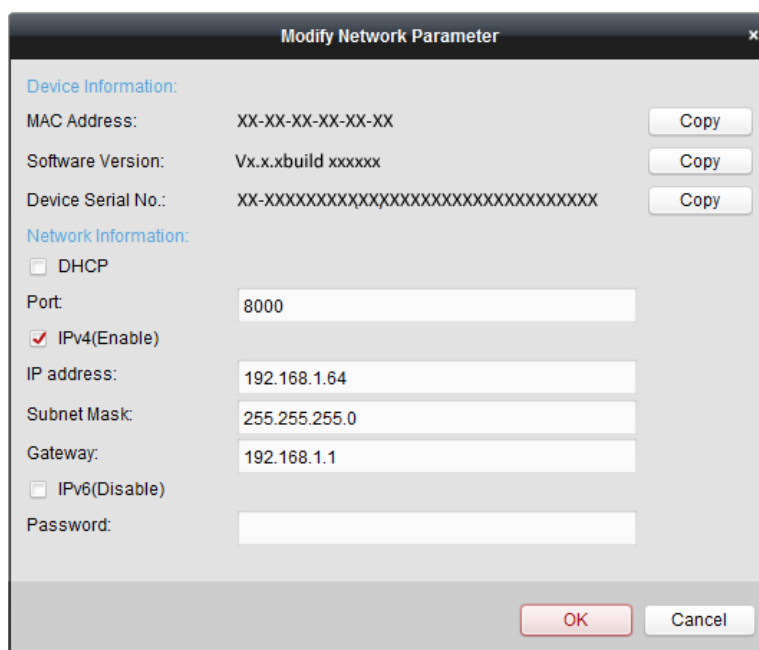


ZAŁECANE JEST STOSOWANIE SILNEGO HASŁA – Zdecydowanie zalecamy utworzenie silnego własnego hasła (minimum 8 znaków z uwzględnieniem wielkich i małych liter, cyfr i znaków specjalnych) w celu zapewnienia lepszej ochrony produktu. Zalecane jest regularne resetowanie hasła. Zwłaszcza w systemie z restrykcyjnymi 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 interfejs modyfikacji parametrów sieciowych, jak przedstawiono na poniższym rysunku.



Rysunek 2–9 Modyfikowanie parametrów sieciowych

8. Zmień ręcznie adres IP urządzenia lub zaznacz pole wyboru „Enable DHCP“, aby upewnić się, że kamera i komputer znajdują się w tej samej podsięci.
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. Patrz Rozdział 2.1.2, aby uzyskać szczegółowe informacje na temat konfiguracji adresu IP kamery sieciowej.
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.

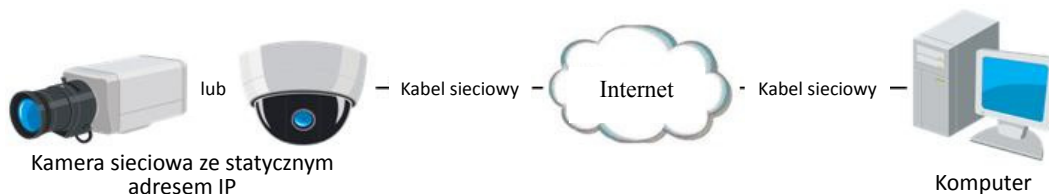
5. Uzyskaj dostęp do kamery sieciowej przy użyciu przeglądarki internetowej lub oprogramowania klienckiego za pośrednictwem Internetu.



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. Patrz Rozdział 2.1.2, aby uzyskać szczegółowe informacje na temat konfiguracji adresu IP kamery sieciowej.



Rysunek 2–11 Bezpośredni dostęp do kamery ze statycznym adresem 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. Patrz Rozdział 2.1.2, aby uzyskać szczegółowe informacje na temat konfiguracji adresu IP kamery sieciowej.
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.

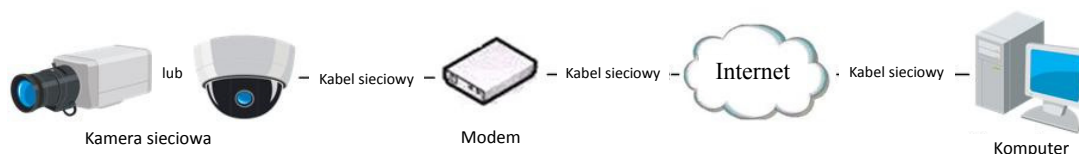
Uwaga: Aby uzyskać szczegółowe informacje na temat mapowania portów, należy zapoznać się z załącznikiem 2.

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:

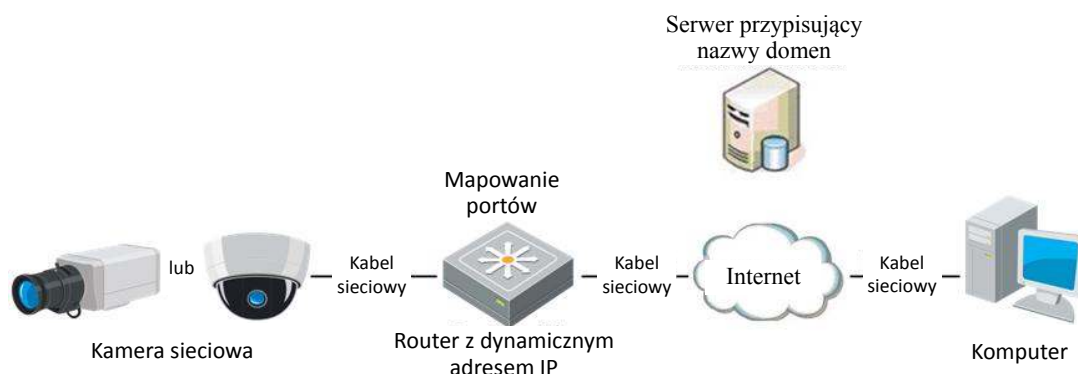
Ta kamera obsługuje automatyczne połączenia telefoniczne przy użyciu protokołu PPPoE. Kamera uzyskuje publiczny adres IP przy użyciu telefonicznego połączenia ADSL po podłączeniu jej do modemu. Należy skonfigurować parametry protokołu PPPoE kamery sieciowej. Patrz *Rozdział 5.3.3 Konfigurowanie ustawień protokołu PPPoE*, aby uzyskać szczegółowe informacje na temat konfiguracji.



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

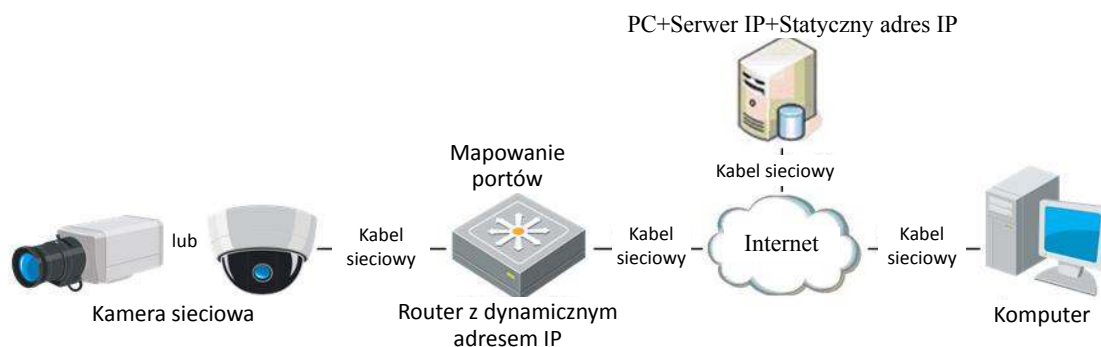


Rysunek 2–13 Uzyskiwanie normalnej nazwy domeny

Kroki:

1. Zastosuj nazwę domeny otrzymaną od dostawcy nazwy domeny.
2. Skonfiguruj ustawienia DDNS w interfejsie **ustawień DDNS** kamery sieciowej.
Patrz **Rozdział 5.3.4 Konfigurowanie ustawień usługi DDNS**, aby uzyskać szczegółowe informacje na temat konfiguracji.
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. Patrz **Rozdział 5.3.4 Konfigurowanie ustawień usługi DDNS**, aby uzyskać szczegółowe informacje na temat konfiguracji.

Rozdział 3 Dostęp do kamery sieciowej

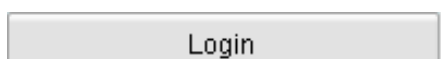
3.1 Uzyskiwanie dostępu za pośrednictwem przeglądarki internetowej

Kroki:

1. Otwórz przeglądarkę internetową.
2. Wprowadź adres IP kamery sieciowej na pasku adresu przeglądarki i naciśnij klawisz **Enter**, aby wyświetlić okno logowania.
3. Aktywuj kamerę sieciową do użycia po raz pierwszy. Aby uzyskać szczegółowe informacje, patrz Rozdział 2.1.2.

Uwaga:

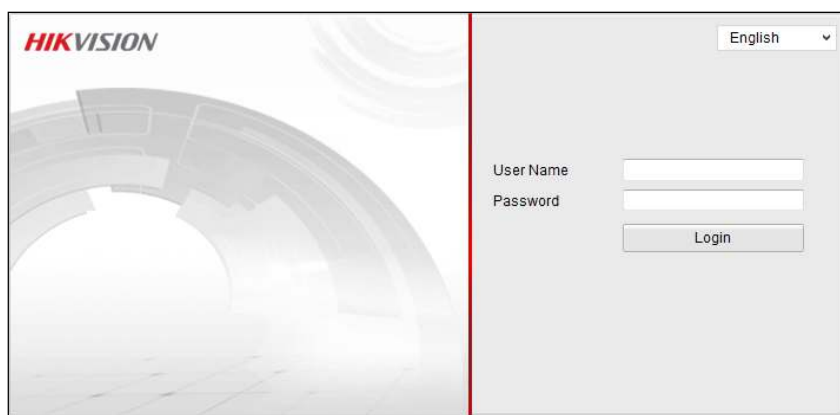
- Domyślny adres IP to 192.168.1.64.
 - Jeśli kamera nie jest aktywowana, aktywuj najpierw kamerę zgodnie z instrukcjami podanymi w Rozdziale 3.1 lub Rozdziale 3.2.
4. W prawym górnym rogu interfejsu logowania wybierz „English“ (Język angielski) jako język interfejsu.
 5. Wprowadź nazwę użytkownika i hasło, a następnie kliknij przycisk



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

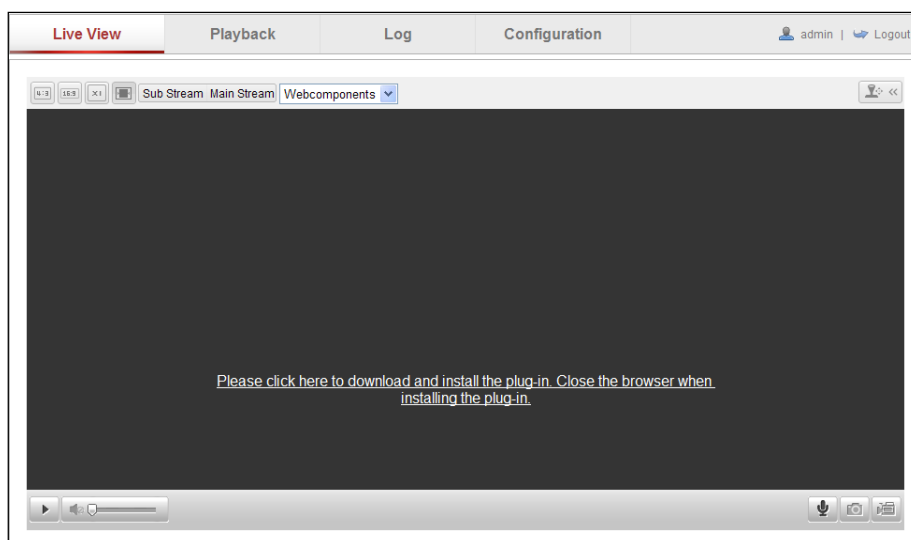
Uwaga:

Adres IP urządzenia zostanie zablokowany po 7 nieudanych próbach wprowadzenia hasła przez użytkownika o uprawnieniach administratora (w przypadku innych użytkowników/operatorów jest to 5 prób).

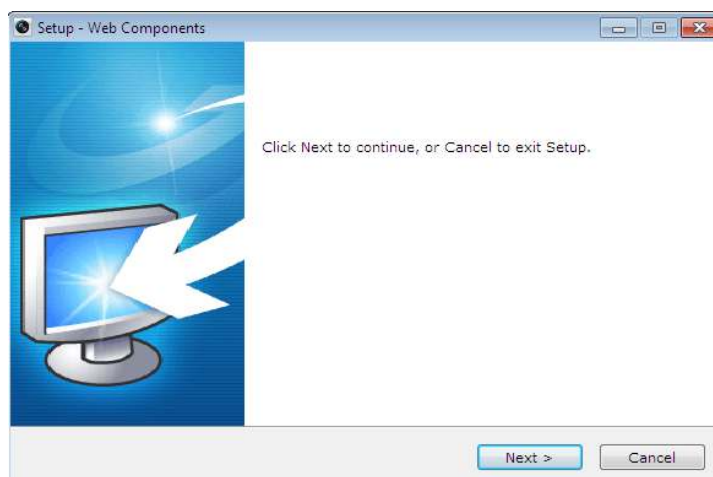


Rysunek 3–1 Okno logowania

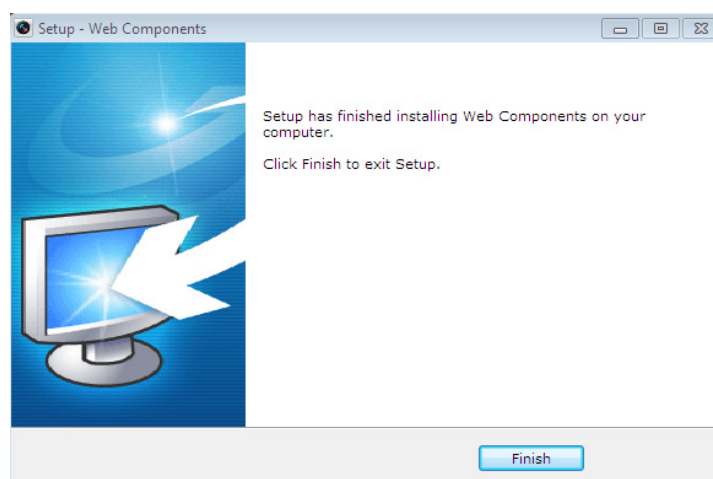
6. Przed wyświetleniem widoku na żywo obrazu wideo i skorzystaniem z kamery zainstaluj wtyczkę. Aby zainstalować wtyczkę, postępuj zgodnie z wyświetlanymi komunikatami instalacyjnymi.



Rysunek 3–2 Pobieranie i instalacja wtyczki



Rysunek 3–3 Instalacja wtyczki (1)

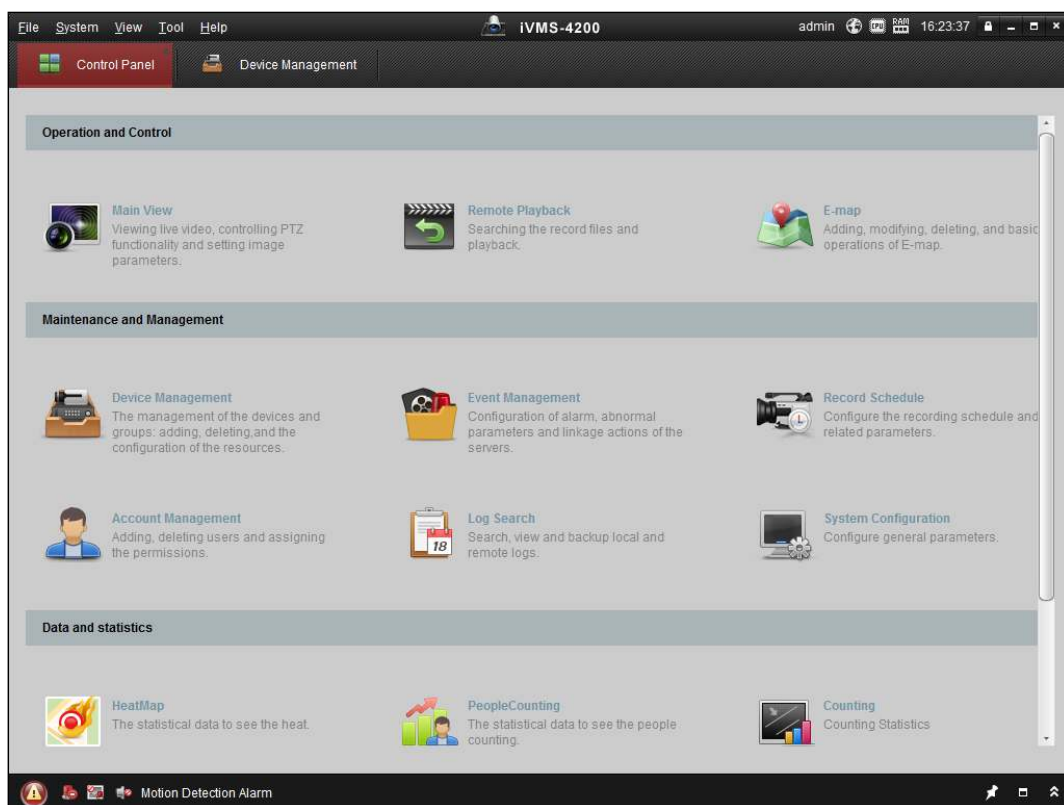


Rysunek 3–4 Instalacja wtyczki (2)

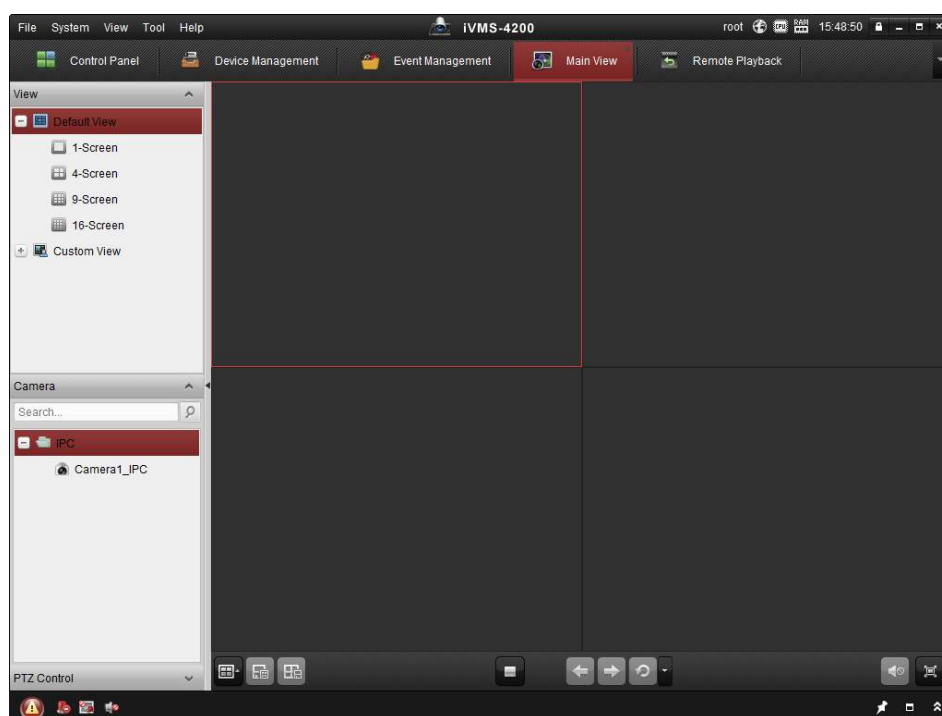
Uwaga: Do zakończenia instalacji wtyczki konieczne może być zamknięcie i ponowne uruchomienie przeglądarki internetowej. Po zainstalowaniu wtyczki i ponownym uruchomieniu przeglądarki zaloguj się.

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 3–5 Panel sterowania iVMS-4200



Rysunek 3–6 Widok główny oprogramowania iVMS-4200

Uwaga: Szczegółowe informacje na temat oprogramowania znajdują się w instrukcji użytkownika oprogramowania iVMS-4200.

Rozdział 4 Widok na żywo

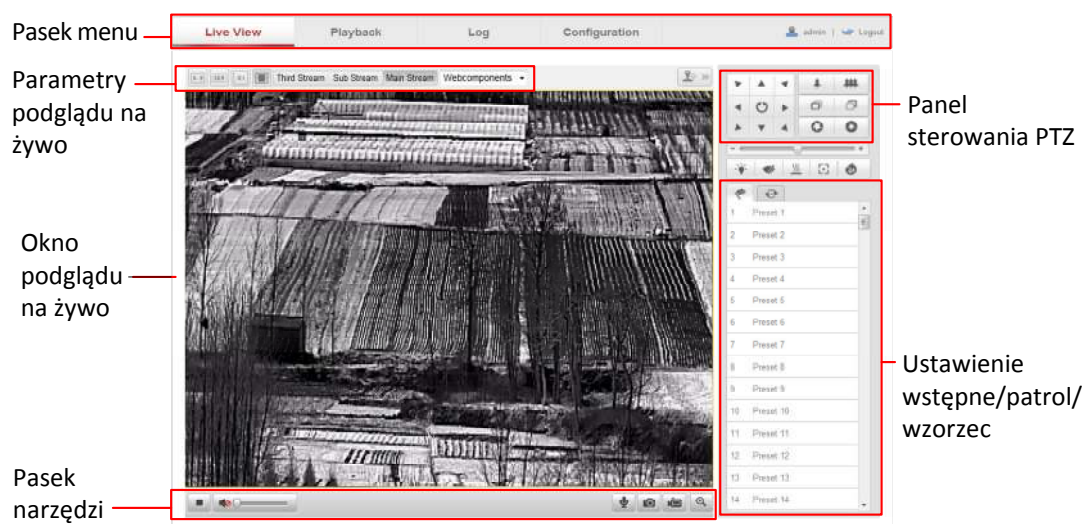
4.1 Interfejs podglądu na żywo

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 Interfejs podglądu na żywo

Model kamery:

Wyświetla model kamery, z którą się łączysz.

Pomoc online:

Kliknij przycisk , aby uzyskać pomoc online, dzięki której poznasz podstawowe operacje każdej funkcji.

Pasek menu:

Kliknij odpowiednią kartę, aby przejść na stronę podglądu na żywo, odtwarzania, rejestru lub konfiguracji.

Sterowanie wyświetlaniem:

Kliknij odpowiedni przycisk, aby dostosować układ i typ strumienia podglądu na żywo. Można kliknąć listę rozwijaną, aby wybrać odpowiedni układ wyświetlania. Użytkownicy przeglądarki Internet Explorer mogą wybrać składniki sieci Web i Quick Time. Użytkownicy niekorzystający z przeglądarki Internet Explorer mogą wybrać składniki sieci Web, Quick Time, VLC lub MJPEG, jeśli są one obsługiwane przez przeglądarkę sieci Web.

Okno podglądu na żywo:

Służy do wyświetlania obrazu podglądu na żywo.

Pasek narzędzi:

Operacje na stronie podglądu na żywo takie jak uruchamianie/zatrzymywanie podglądu na żywo, wykonywanie zdjęć, nagrywanie, uruchamianie/zatrzymywanie dwukierunkowego przesyłania sygnału audio.


Sterowanie PTZ:

Obrót, pochylenie i powiększenie obrazu kamery oraz sterowanie światłem i wycieraczką. (dostępne tylko w przypadku kamer z obsługą funkcji 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 Opisy paska sterowania wyświetlania oraz paska narzędzi

Ikona	Opis
	Uruchamianie/zatrzymywanie podglądu na żywo.
	Proporcje okna 4:3.
	Proporcje okna 16:9.
	Oryginalny rozmiar okna.
	Automatyczne dostosowanie rozmiaru okna.
Main Stream	Podgląd na żywo strumienia głównego.
Sub Stream	Podgląd na żywo podstrumienia.
Webcomponents	Kliknij, aby wybrać wtyczkę innej firmy.
2*2	Podział okna
	Ręczne wykonanie zdjęcia.
	Ręczne rozpoczynanie/kończenie nagrywania.
	Włączanie dźwięku i regulacja głośności/wyciszenie.
	Uruchomienie/zatrzymanie dwukierunkowego przesyłania sygnału audio.
	Włączanie/wyłączanie funkcji e-PTZ.

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 zapisu wykonanych zdjęć i klipów wideo można ustawić na stronie **Configuration > Local Configuration**. Aby skonfigurować zaplanowane nagrywanie zdalne, patrz *Rozdział 6.3*.

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

Rozdział 5 Konfiguracja kamery sieciowej

5.1 Konfigurowanie parametrów lokalnych

Uwaga: Konfiguracja lokalna odnosi się do parametrów podglądu na żywo, nagrywania plików i wykonanych zdjęć i klipów wideo. Pliki nagrań, wykonane zdjęcia i klipy wideo są nagrywane i wykonywane za pomocą przeglądarki sieci Web i z tego względu ich ścieżki zapisu znajdują się na komputerze, na którym uruchomiona jest przeglądarka.

Kroki:

1. Przejdź do interfejsu Local Configuration:

Configuration > Local Configuration

The screenshot displays the 'Local Configuration' web interface. It features three main sections: 'Live View Parameters', 'Record File Settings', and 'Picture and Clip Settings'. Each section contains various configuration options with radio buttons for selection and text input fields for file paths, accompanied by 'Browse' buttons. A 'Save' button is located at the bottom right of the interface.

Live View Parameters				
Protocol	<input checked="" type="radio"/> TCP	<input type="radio"/> UDP	<input type="radio"/> MULTICAST	<input type="radio"/> HTTP
Live View Performance	<input type="radio"/> Shortest Delay	<input checked="" type="radio"/> Auto		
Rules	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable		
Image Format	<input checked="" type="radio"/> JPEG	<input type="radio"/> BMP		
Display Temperature Info.	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable		
Display Temperature Info. on Capture	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable		

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"/>
Save downloaded files to	<input type="text" value="C:\Users\yanjiamin\Web\DownloadFiles"/>			<input type="button" value="Browse"/>

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

Rysunek 5–1 Interfejs konfiguracji lokalnej

2. Skonfiguruj następujące ustawienia:

- **Live View Parameters:** ustaw typ protokołu i wydajność podglądu na żywo.
 - **Typ protokołu:** Dostępne opcje to: 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. Szczegółowe informacje na temat funkcji Multicast można znaleźć w *Rozdziale 5.3.1 Konfigurowanie ustawień protokołu TCP/IP*.
 - **Live View Performance:** Ustawianie wydajności podglądu na żywo live view performance na najkrótsze opóźnienie Shortest Delay lub tryb automatyczny Auto.
 - **Auto Start Live View:** Jeśli włączysz tę funkcję, obrazy podglądu na żywo zostaną automatycznie uruchomione po aktywowaniu karty **podglądu na żywo**. Jeśli funkcja jest wyłączona, można ręcznie uruchomić podgląd na żywo w interfejsie podglądu na żywo.
 - **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:** Wybór detekcji źródła ognia jako typu zasobu VCA. Zaznacz to pole wyboru, aby włączyć wymagane funkcje. Można wybrać opcje Display Fire Point Distance, Display Highest Temperature, Locate Highest Temperature Point i Frame Fire Point.

- **Display Temperature Info. on Stream:** Wybór pomiaru temperatury jako typu zasobu VCA. Zaznacz to pole wyboru, aby wyświetlić informacje o temperaturze w interfejsie podglądu na żywo.
- **Display Temperature Info. on Capture:** Wybór pomiaru temperatury jako typu zasobu VCA. Zaznacz to pole wyboru, aby wyświetlić informacje o temperaturze w wykonanych zdjęciach.
- **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. Ważne dla zdjęć wykonanych za pomocą przeglądarki sieci Web.
 - **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: Kliknij przycisk **Browse**, aby zmienić katalog zapisu klipów i zdjęć.

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

5.2 Konfigurowanie ustawień czasu

Cel:

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

Kroki:

1. Przejdź do interfejsu Time Settings:

Configuration > Basic Configuration > System > Time Settings

Lub **Configuration > Advanced Configuration > System > Time Settings**

Rysunek 5–2 Ustawienia czasu

2. Wybierz strefę czasową.

Wybierz strefę czasową w swojej lokalizacji z menu rozwijanego.

3. Ustaw synchronizację czasu.

Można synchronizować czas za pomocą protokołu synchronizacji czasu NTP lub ręcznie.

- Synchronizacja czasu przez serwer NTP.
 - (1) Zaznacz to pole wyboru, 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.

Time Sync.	
<input type="radio"/> NTP	
Server Address	time.windows.com
NTP Port	123
Interval	1440 min.

Rysunek 5–3 Synchronizacja czasu za pośrednictwem serwera 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.

- Ręczne synchronizowanie czasu

Włącz funkcję **Manual Time Sync**, a następnie kliknij przycisk , aby ustawić czas systemowy z wyświetlonego kalendarza.

Uwaga: Można również zaznaczyć pole wyboru **Sync with computer time**, aby zsynchronizować czas kamery z czasem komputera.

Sep 2013						
Sun	Mon	Tue	Wed	Thu	Fri	Sat
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	1	2	3	4	5
6	7	8	9	10	11	12

Manual Time Sync.	
Device Time	2013-09-22T11:32:34
Set Time	2013-09-22T11:14:33 
<input type="checkbox"/> Sync with computer time	

Rysunek 5–4 Ręczna synchronizacja czasu

- Kliknij stronę karty **DST (Configuration > Advanced Configuration > System > DST)**, aby włączyć funkcję DST i ustawić datę okresu DST.

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

Rysunek 5–5 Ustawienia czasu letniego (DST)

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

5.3 Konfigurowanie ustawień sieciowych

5.3.1 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 jednocześnie bez powodowania konfliktów oraz należy skonfigurować co najmniej jedną wersję IP.

Kroki:

1. Przejdź do interfejsu ustawień protokołu TCP/IP, wybierając opcje:

Configuration > Basic Configuration > Network > TCP/IP

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

Rysunek 5–6 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 wykrycie kamery sieciowej w trybie online przez oprogramowanie klienckie za pośrednictwem prywatnego protokołu multicast w sieci LAN.

4. 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.

5.3.2 Konfigurowanie ustawień portów

Cel:

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

Kroki:

1. Przejdź do interfejsu ustawień portów, wybierając opcje:

Configuration > Basic Configuration > Network > Port

Lub **Configuration > Advanced Configuration > Network > Port**

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

Rysunek 5–7 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 1024–65 535.

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.

5.3.3 Konfigurowanie ustawień protokołu PPPoE

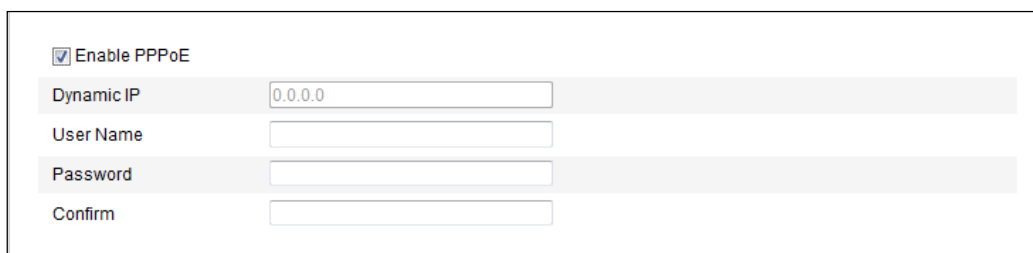
Cel:

Jeśli posiadasz jedynie modem bez routera, możesz skorzystać z protokołu Point-to-Point Protocol over Ethernet (PPPoE).

Kroki:

1. Przejdź do interfejsu ustawień protokołu PPPoE, wybierając opcje:

Configuration > Advanced Configuration > Network > PPPoE



Rysunek 5–8 Ustawienia protokołu PPPoE

2. Zaznacz pole wyboru **Enable PPPoE**, aby włączyć tę funkcję.
3. Aby umożliwić dostęp przy użyciu protokołu PPPoE, wprowadź informacje w polach **User Name**, **Password** i **Confirm**.

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



- Aby zapewnić ochronę prywatności i systemu przed zagrożeniami bezpieczeństwa, zdecydowanie zalecamy używanie silnych haseł dla wszystkich funkcji i urządzeń sieciowych. Aby zwiększyć bezpieczeństwo urządzenia, należy ustawić własne hasło (składającego się z minimum 8 znaków, w tym wielkich liter, małych liter, cyfr i znaków specjalnych).
- 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.

5.3.4 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.



- Aby zapewnić ochronę prywatności i systemu przed zagrożeniami bezpieczeństwa, zdecydowanie zalecamy używanie silnych haseł dla wszystkich funkcji i urządzeń sieciowych. Aby zwiększyć bezpieczeństwo urządzenia, należy ustawić własne hasło (składającego się z minimum 8 znaków, w tym wielkich liter, małych liter, cyfr i znaków specjalnych).
- Instalator i/lub użytkownik końcowy są zobowiązani do prawidłowego skonfigurowania wszystkich haseł i innych ustawień zabezpieczeń.

Kroki:

1. Przejdź do interfejsu ustawień usługi DDNS, wybierając opcje:

Configuration > Advanced Configuration > Network > DDNS

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

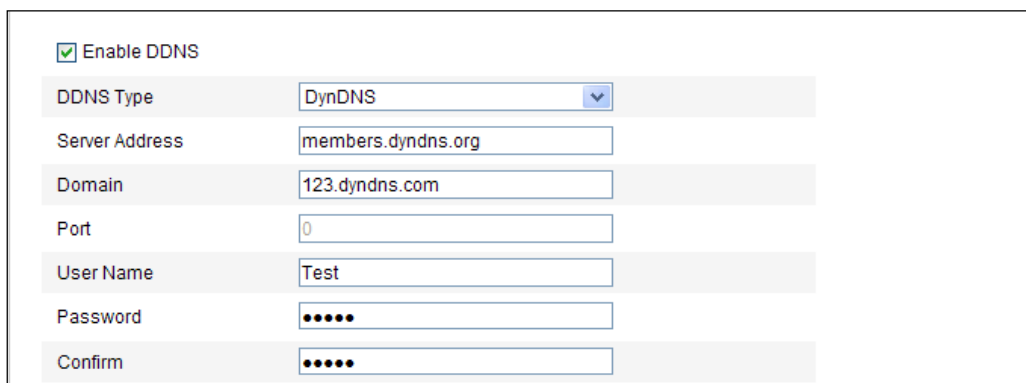
Rysunek 5–9 Ustawienia usługi DDNS

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

- DynDNS:

Kroki:

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



The screenshot shows a web form for configuring DynDNS. At the top, there is a checkbox labeled "Enable DDNS" which is checked. Below it, there are several input fields: "DDNS Type" is a dropdown menu set to "DynDNS"; "Server Address" is a text box containing "members.dyndns.org"; "Domain" is a text box containing "123.dyndns.com"; "Port" is a text box containing "0"; "User Name" is a text box containing "Test"; "Password" and "Confirm" are password fields, both masked with dots.

Rysunek 5–10 Ustawienia DynDNS

- Serwer IP:

Kroki:

- (1) Wprowadź adres serwera IP.
- (2) Kliknij przycisk **Save**, aby zapisać ustawienia.

Uwaga: W przypadku serwera IP należy zastosować statyczny adres IP, maskę podsieci, bramę oraz preferowany DNS od usługodawcy internetowego. W polu **Server Address** należy wpisać statyczny adres IP komputera, na którym uruchomione jest oprogramowanie serwera IP.

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

Rysunek 5–11 Ustawienia serwera IP

Uwaga: Na obszarze USA i Kanady w polu adresu serwera można wprowadzić numer 173.200.91.74.

- NO-IP:

Kroki:

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

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

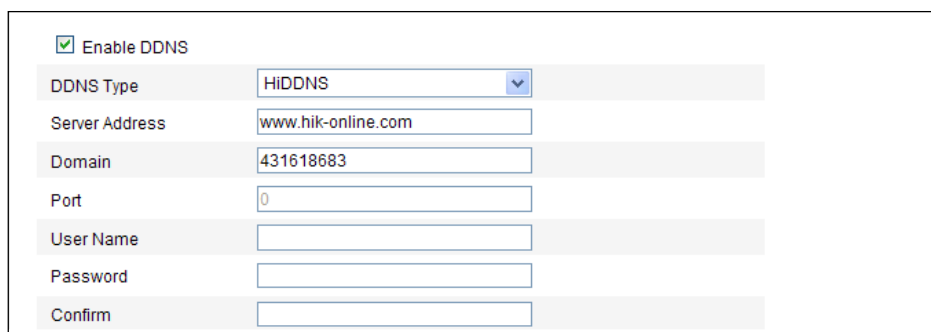
Rysunek 5–12 Ustawienia NO-IP

- (2) Wprowadź Adres serwera www.noip.com
- (3) Wprowadź zarejestrowaną nazwę w polu Nazwa domeny.
- (4) W razie potrzeby wprowadź numer portu.
- (5) Wprowadź informacje w polach Nazwa użytkownika i Hasło.
- (6) Kliknij przycisk **Save**, aby móc wyświetlić obraz kamery z nazwą domeny.

- HiDDNS

Kroki:

- (1) W polu DDNS Type wybierz HiDDNS.



Rysunek 5–13 Ustawienia HiDDNS

- (2) Wprowadź adres serwera *www.hik-online.com*.
- (3) Wprowadź nazwę domeny kamery. Domena jest taka sama co domena aliasu urządzenia na serwerze HiDDNS.
- (4) Kliknij **Save**, aby zapisać nowe ustawienia.

Uwaga: Ustawienia zostaną uwzględnione po ponownym uruchomieniu.

5.3.5 Konfigurowanie ustawień protokołu SNMP

Cel:

Można ustawić funkcję SNMP, aby uzyskać informacje na temat stanu, parametrów i alarmu kamery oraz zdalnie zarządzać kamerą, gdy jest podłączona do sieci.

Zanim rozpoczniesz:

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. SNMP v1 nie zapewnia żadnego zabezpieczenia. SNMP v2 wymaga hasła dostępu w celu uzyskania dostępu. SNMP v3 zapewnia szyfrowanie. Jeśli używasz trzeciej wersji, należy włączyć protokół HTTPS.



- Aby zapewnić ochronę prywatności i systemu przed zagrożeniami bezpieczeństwa, zdecydowanie zalecamy używanie silnych haseł dla wszystkich funkcji i urządzeń sieciowych. Aby zwiększyć bezpieczeństwo urządzenia, należy ustawić własne hasło (składającego się z minimum 8 znaków, w tym wielkich liter, małych liter, cyfr i znaków specjalnych).
- 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 > Advanced Configuration > Network > SNMP

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

Rysunek 5–14 Ustawienia protokołu SNMP

2. Zaznacz pole wyboru odpowiedniej wersji (**Enable SNMPv1**, **Enable SNMPv2c**, lub **Enable SNMPv3**), aby włączyć tę 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.

Uwaga: Ustawienia zostaną uwzględnione po ponownym uruchomieniu.

5.3.6 Konfigurowanie ustawień standardu IEEE 802.1X

Cel:

Standard IEEE 802.1X jest obsługiwany przez kamery sieciowe. Kiedy ta funkcja jest włączona, dane kamery są zabezpieczone i podczas podłączania kamery do sieci chronionej standardem IEEE 802.1X wymagane jest uwierzytelnianie użytkownika.

Zanim rozpoczniesz:

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



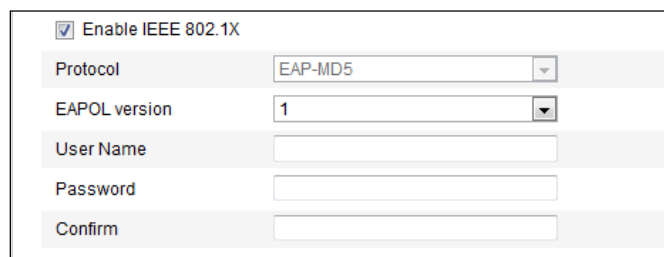
- Aby zapewnić ochronę prywatności i systemu przed zagrożeniami bezpieczeństwa, zdecydowanie zalecamy używanie silnych haseł dla wszystkich funkcji i urządzeń sieciowych. Aby zwiększyć bezpieczeństwo urządzenia, należy ustawić własne hasło (składającego się z minimum 8 znaków, w tym wielkich liter, małych liter, cyfr i znaków specjalnych).
- Instalator i/lub użytkownik końcowy są zobowiązani do prawidłowego skonfigurowania wszystkich haseł i innych ustawień zabezpieczeń.

Kroki:

1. Przejdź do interfejsu ustawień standardu IEEE 802.1X, wybierając opcje:
Configuration > Advanced Configuration > Network > 802.1X
2. Zaznacz pole wyboru **Enable IEEE 802.1X**, aby włączyć tę funkcję.
3. Konfigurowanie ustawień 802.1X, w tym wersji EAPOL, nazwy użytkownika i hasła.

Uwaga: Wersja protokołu EAPOL musi zgadzać się z wersją routera lub przełącznika.

4. Wprowadź nazwę użytkownika i hasło, aby uzyskać dostęp do serwera.



Rysunek 5–15 Ustawienia standardu 802.1X

5. Kliknij przycisk **Save**, aby ukończyć konfigurowanie ustawień.

Uwaga: Ustawienia zostaną uwzględnione po ponownym uruchomieniu.

5.3.7 Konfigurowanie ustawień jakości usługi (QoS)

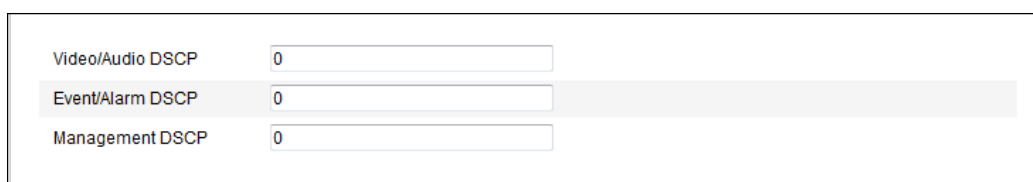
Cel:

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 > Advanced Configuration > Network > QoS



Rysunek 5–16 Ustawienia jakości usługi (QoS)

2. Skonfiguruj ustawienia QoS, w tym DSCP wideo/audio, DSCP zdarzenia/alarmu i DSCP zarządzania.

Prawidłowy zakres wartości DSCP wynosi od 0 do 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.

5.3.8 Konfigurowanie ustawień UPnP™

Universal Plug and Play (UPnP™) to architektura sieciowa zapewniająca zgodność różnego rodzaju sprzętu i oprogramowania sieciowego. Protokół UPnP pozwala urządzeniom bezproblemowo łączyć się ze sobą i upraszcza wdrażanie sieci w domu i w środowisku firmowym.

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. Przejdź do interfejsu ustawień protokołu UPnP™, wybierając opcję:
Configuration > Advanced Configuration > Network > UPnP™
2. Zaznacz pole wyboru „Enable UPnP™“ (Włącz UPnP™), aby włączyć funkcję UPnP.

Można edytować nazwę urządzenia po jego wykryciu w sieci.



Rysunek 5–17 Ustawienia UPnP™

5.3.9 Wysyłka wiadomości e-mail wyzwalana przez alarm

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 rozpocznieś:

Przed skorzystaniem z funkcji poczty e-mail skonfiguruj ustawienia serwera DNS w obszarze **Basic Configuration > Network > TCP/IP** lub **Advanced Configuration > Network > TCP/IP**.

Kroki:

1. Przejdź do ustawień protokołu TCP/IP (**Configuration > Basic Configuration > Network > TCP/IP** lub **Configuration > Advanced Configuration > Network > TCP/IP**), aby ustawić parametry adresu IPv4, maski podsieci IPv4, bramy domyślnej IPv4 oraz preferowanego serwera DNS.

Uwaga: Aby uzyskać szczegółowe informacje, patrz *Rozdział 5.3.1*

Konfigurowanie ustawień protokołu TCP/IP.

2. Przejdź do interfejsu ustawień wysyłania wiadomości e-mail, wybierając opcje:

Configuration > Advanced Configuration > Network > Email

The screenshot displays the 'Email' configuration page. It is divided into two main sections: 'Sender' and 'Receiver'.
Sender Section:
 - 'Sender' text box: Test
 - 'Sender's Address' text box: Test@gmail.com
 - 'SMTP Server' text box: smtp.263xmail.com
 - 'SMTP Port' text box: 25
 - 'Enable SSL' checkbox: unchecked
 - 'Interval' dropdown: 2s
 - 'Attached Image' checkbox: unchecked
 - 'Authentication' checkbox: unchecked
 - 'User Name' text box: (empty)
 - 'Password' text box: (empty)
 - 'Confirm' text box: (empty)
Receiver Section:
 - 'Receiver1' text box: Test1
 - 'Receiver1's Address' text box: Test1@gmail.com
 - 'Receiver2' text box: (empty)
 - 'Receiver2's Address' text box: (empty)
 - 'Receiver3' text box: (empty)
 - 'Receiver3's Address' text box: (empty)
 At the bottom right, there is a 'Save' button.

Rysunek 5–18 Ustawienia wysyłania wiadomości e-mail

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 serwera SMTP (np. smtp.263xmail.com).

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

Enable SSL: Zaznacz to pole wyboru, aby włączyć szyfrowanie SSL, jeśli jest ono wymagane przez serwer SMTP.

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 (optional): Jeśli serwer e-mail wymaga uwierzytelnienia, zaznacz to pole wyboru, aby używać uwierzytelniania podczas logowania się do serwera oraz wprowadź nazwę użytkownika i hasło.



- *Aby zapewnić ochronę prywatności i systemu przed zagrożeniami bezpieczeństwa, zdecydowanie zalecamy używanie silnych haseł dla wszystkich funkcji i urządzeń sieciowych. Aby zwiększyć bezpieczeństwo urządzenia, należy ustawić własne hasło (składającego się z minimum 8 znaków, w tym wielkich liter, małych liter, cyfr i znaków specjalnych).*
- *Instalator i/lub użytkownik końcowy są zobowiązani do prawidłowego skonfigurowania wszystkich haseł i innych ustawień zabezpieczeń.*

Choose 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.

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

5.3.10 Konfiguracja ustawień translacji adresów sieciowych (NAT)

Cel:

Termin NAT odnosi się do mapowania portu, gdy włączona jest funkcja UPnP™.

Kroki:

- Wyświetl ustawienia translacji NAT.

Configuration > Advanced Configuration > Network > NAT

- Wybierz tryb mapowania portu.

Aby mapować porty przy użyciu domyślnych numerów portów:

W pozycji Port Mapping Mode wybierz opcję **Auto**.

Aby mapować porty przy użyciu niestandardowych numerów portów:

W pozycji Port Mapping Mode wybierz opcję **Manual**.

W przypadku ręcznego mapowania portu można samemu dostosować wartość numeru portu.

The screenshot shows the NAT configuration page. At the top, there is a checkbox labeled 'Enable Port Mapping' which is checked. Below it is a dropdown menu for 'Port Mapping Mode' with 'Manual' selected. Below the dropdown is a table with the following data:

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

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

Rysunek 5–19 Konfiguracja ustawień NAT

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

5.3.11 Konfigurowanie ustawień serwera FTP

Cel:

Można skonfigurować informacje serwera FTP, aby umożliwić wysyłanie wykonanych zdjęć na serwer FTP. Wykonywanie zdjęć może być wyzwalane przez zdarzenia lub zgodnie z harmonogramem.

Kroki:

- Przejdź do interfejsu ustawień serwera FTP, wybierając opcje:

Configuration > Advanced Configuration > Network > FTP

2. Skonfiguruj ustawienia FTP; nazwa użytkownika i hasło są wymagane do zalogowania się do serwera FTP.



- Aby zapewnić ochronę prywatności i systemu przed zagrożeniami bezpieczeństwa, zdecydowanie zalecamy używanie silnych haseł dla wszystkich funkcji i urządzeń sieciowych. Aby zwiększyć bezpieczeństwo urządzenia, należy ustawić własne hasło (składającego się z minimum 8 znaków, w tym wielkich liter, małych liter, cyfr i znaków specjalnych).
- Instalator i/lub użytkownik końcowy są zobowiązani do prawidłowego skonfigurowania wszystkich haseł i innych ustawień zabezpieczeń.

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.

Upload type: Aby włączyć przysyłanie zarejestrowanych zdjęć na serwer FTP, wybierz opcję „Upload picture” (Prześlij zdjęcie).

Dostęp anonimowy do serwera FTP (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.

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

Rysunek 5–20 Ustawienia serwera FTP

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

Uwaga: Aby przesyłać wykonane zdjęcia na serwer FTP, na stronie wykonywania zdjęć należy włączyć funkcję wykonywania zdjęć w odstępach czasu lub

wykonywania zdjęć wyzwalanego zdarzeniem. Aby uzyskać szczegółowe informacje, patrz *Rozdział 6.4*.

5.3.12 Ustawienia protokołu 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 > Advanced Configuration > Network > HTTPS

☐ Enable HTTPS

Create

Create Self-signed Certificate

Create Certificate Request

Install Signed Certificate

Certificate Path

Created Request

Created Request

Installed Certificate

Installed Certificate

Property
Subject: C=CN, ST=ZJ, L=HZ, OU=embeddedsoftware, H/IP=192.168.1.64, EM=com.cn
Issuer: C=CN, ST=ZJ, L=HZ, OU=embeddedsoftware, H/IP=192.168.1.64, EM=com.cn
Validity: 2015-07-23 14:29:46 ~ 2018-07-22 14:29:46

Rysunek 5–21 Ustawienia protokołu HTTPS

2. Zaznacz pole wyboru Enable HTTPS, aby włączyć tę funkcję.
3. Utwórz certyfikat z podpisem własnym lub autoryzowany certyfikat.
 - Tworzenie certyfikatu z podpisem własnym
 - 1) Kliknij przycisk **Create**, aby wyświetlić okno tworzenia.

The screenshot shows a web interface with two main sections:

- Create**: Contains two buttons labeled 'Create'. The first button is for 'Create Self-signed Certificate' and the second is for 'Create Certificate Request'.
- Install Signed Certificate**: Contains a text input field for 'Certificate Path', a 'Browse' button, and an 'Upload' button.
- Created Request**: Contains a text input field for 'Created Request', a 'Delete' button, and a 'Download' button.
- Installed Certificate**: Contains a text input field for 'Installed Certificate' and a 'Delete' button.

Rysunek 5–22 Tworzenie certyfikatu z podpisem własnym

- 2) Wprowadź nazwę kraju, nazwę/adres IP hosta, datę ważności i inne kraje.

The screenshot shows a form for creating a certificate with the following fields:

- Country: Text input field with a hint '* example: CN'.
- Hostname/IP: Text input field with a hint '*'.
- Password: Text input field.
- State or province: Text input field.
- Locality: Text input field.
- Organization: Text input field.
- Organizational Unit: Text input field.
- Email: Text input field.

At the bottom right, there are 'OK' and 'Cancel' buttons.

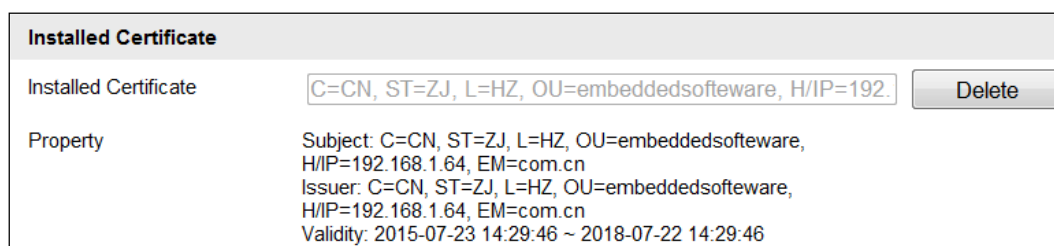
Rysunek 5–23 Tworzenie certyfikatu

- 3) Kliknij przycisk **OK**, aby zapisać ustawienia.

Uwaga: Jeśli masz już zainstalowany certyfikat, opcja tworzenia certyfikatu z podpisem własnym jest wygaszona.

- Tworzenie autoryzowanego certyfikatu

- 1) Kliknij przycisk **Create**, aby utworzyć żądanie certyfikatu.
- 2) Pobierz żądanie certyfikatu i prześlij je do zaufanego urzędu certyfikacji w celu uzyskania sygnatury.
- 3) Po otrzymaniu prawidłowego sygnowanego certyfikatu zaimportuj go do urządzenia.
4. Po pomyślnym utworzeniu i zainstalowaniu certyfikatu dostępne będą informacje dotyczące certyfikatu.



Rysunek 5–24 Zainstalowany certyfikat

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

5.4 Konfigurowanie ustawień audio i wideo

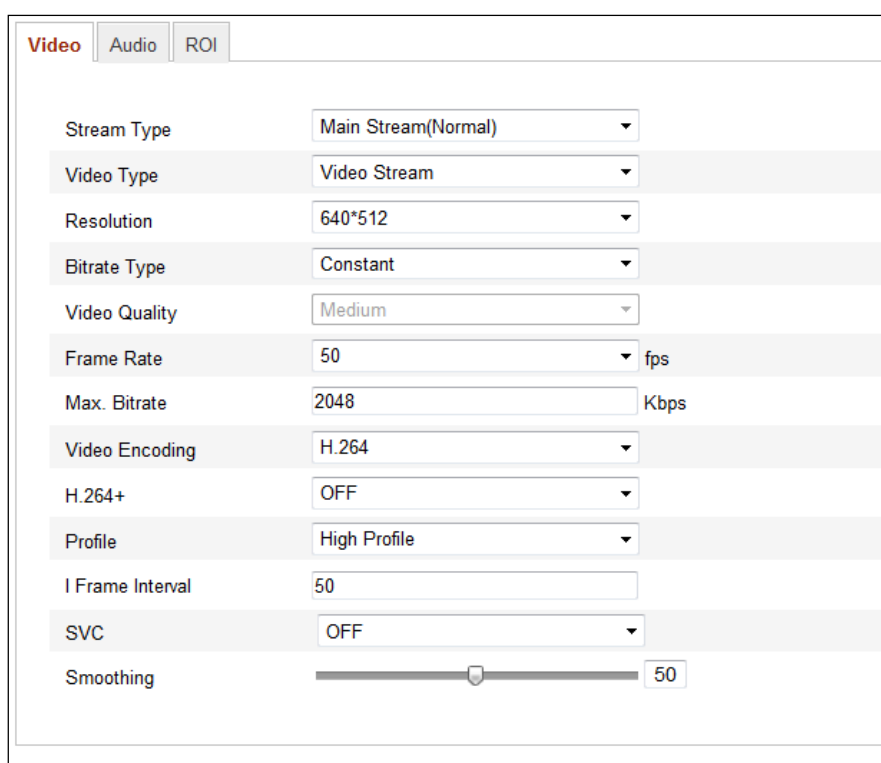
5.4.1 Konfigurowanie ustawień wideo

Kroki:

1. Przejdź do interfejsu ustawień wideo, wybierając opcje:

Configuration > Basic Configuration > Video/Audio > Video

Lub **Configuration > Advanced Configuration > Video/Audio > Video**



Rysunek 5–25 Ustawienia wideo

2. W pozycji **Typ strumienia** kamery wybierz strumień główny (zwykły), podstrumień lub trzeci strumień. Strumień główny jest zazwyczaj wykorzystywany do nagrywania i podglądu na żywo wówczas, gdy użytkownik dysponuje połączeniem sieciowym o dużej przepustowości. W przypadku, gdy przepustowość jest mniejsza, do wyświetlania podglądu na żywo można wykorzystać podstrumień.
3. Po wybraniu strumienia głównego lub podstrumienia można skonfigurować następujące parametry:

Video Type:

Wybierz jeden z następujących typów strumienia: strumień wideo lub złożony strumień audio-wideo. Sygnał audio może być nagrywany tylko wtedy, gdy w pozycji **Video Type** wybrano opcję **Video & Audio**.

Resolution:

Wybierz rozdzielczość wyjścia wideo.

Bitrate Type:

Wybierz stałą lub zmienną transmisję danych.

Video Quality:

Po wybraniu typu transmisji danych **Variable** do wyboru dostępne jest 6 poziomów jakości obrazu wideo.

Frame Rate:

Ustaw liczbę klatek na sekundę na poziomie 1/16~25 fps. 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 maks. transmisję danych na poziomie 256~16384 Kbps. Im wyższa wartość tego parametru, tym większa jakość obrazu wideo, ale zarazem tym większa przepustowość jest wymagana podczas przesyłania sygnału wideo.

Uwaga: Górny limit maksymalnej szybkości transmisji bitów jest zależny od platformy kamery. W przypadku niektórych kamer stosowane jest maksymalne ograniczenie wynoszące 8192Kbps lub 12288Kbps.

Video Encoding:

Jeśli w pozycji **Stream Type** wybrano opcję **Main Stream**: Do wyboru dostępne są opcje: H.264 i MPEG4. Jeśli w pozycji stream type wybrano opcję sub stream, do wyboru dostępne będą opcje: H.264, MJPEG i MPEG4.

Uwaga: Typ kodowania wideo różni się w zależności od danej platformy kamery.

Profile:

Można wybrać opcje kodowania: Basic profile, Main Profile lub High Profile.

I Frame Interval:

Ustaw interwał klatki I 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. Wybierz opcję Auto, aby urządzenie automatycznie wyodrębniało klatki z oryginalnego obrazu wideo, gdy przepustowość sieci jest niewystarczająca.

Smoothing:

Funkcja ta odnosi się do wygładzania strumienia. Im wyższa wartość parametru wygładzania, tym większa płynność strumieniowania, jednak jakość obrazu wideo może nie być satysfakcjonująca. Im niższa wartość parametru wygładzania, tym wyższa jakość obrazu wideo, choć strumieniowanie może wydawać się niezbyt płynne.

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

5.4.2 Konfigurowanie ustawień audio

Kroki:

1. Przejdź do interfejsu ustawień audio, wybierając opcje:

Configuration > Basic Configuration > Video/Audio > Audio

Lub **Configuration > Advanced Configuration > Video/Audio > Audio**

Rysunek 5–26 Ustawienia audio

2. Skonfiguruj poniższe ustawienia.

Uwaga: Ustawienia audio są zależne od modelu kamery.

Audio Encoding: Do wyboru dostępne są opcje: G.722.1, G.711 ulaw, G.711alaw, G.726, MP2L2, AAC i PCM. W przypadku MP2L2 można skonfigurować częstotliwość próbkowania i szybkość transmisji strumienia audio; w przypadku PCM można ustawić częstotliwość próbkowania.

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

Input Volume: 0-100

Environmental Noise Filter: Wybierz ustawienie OFF lub ON. Gdy funkcja jest włączona, można do pewnego stopnia pozbyć się panującego w środowisku hałasu.

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

5.4.3 Konfigurowanie kodowania ROI

Cel:

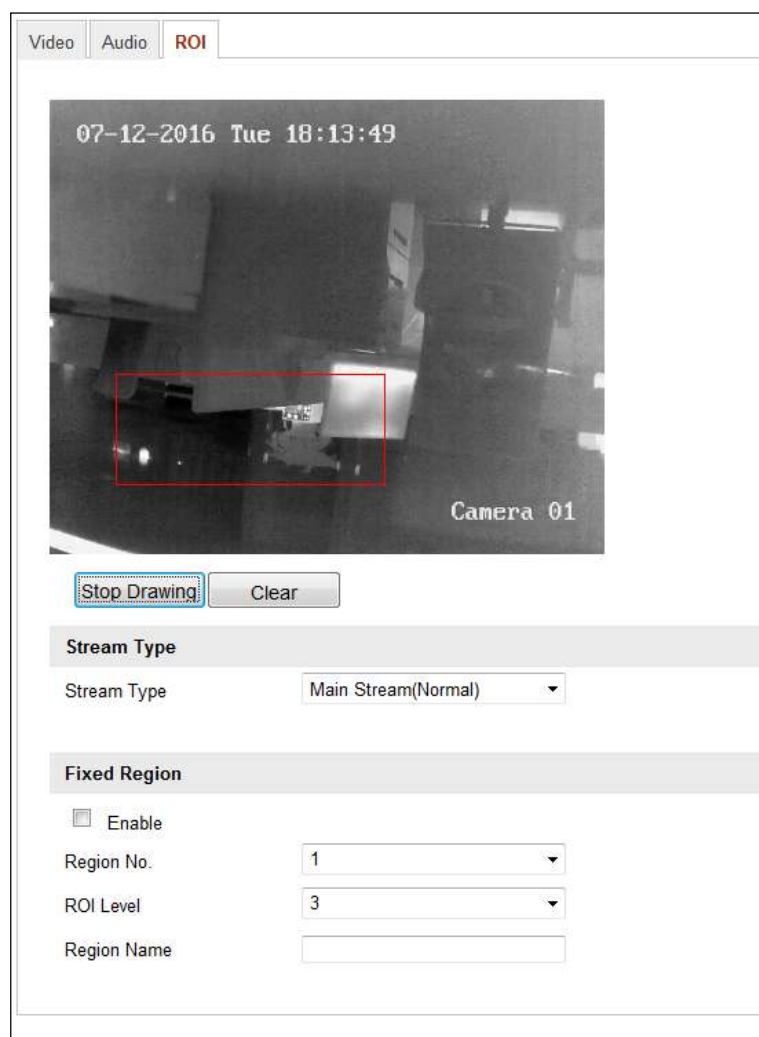
ROI (obszar zainteresowania) pomaga odróżnić informacje obszaru zainteresowania od informacji tła w trakcie kompresji wideo. Oznacza to, że oprogramowanie przydziela więcej zasobów kodowania w obszarze zainteresowania, tym samym zwiększając jakość obrazu w obszarze zainteresowania przy obniżeniu jakości informacji tła.

Uwaga: Funkcja ROI jest zależna od modelu kamery.

Konfigurowanie stałego obszaru dla funkcji ROI:

Kroki:

1. Przejdź do interfejsu ustawień kodowania obszaru zainteresowania (ROI), wybierając opcje:
Configuration > Advanced Configuration > Video/Audio > ROI
2. Zaznacz pole wyboru **Enable** w obszarze Fixed Region.
3. Wybierz typ strumienia dla kodowania ROI.
4. Wybierz obszar z listy rozwijanej numerów obszarów do skonfigurowania w ustawieniach ROI. Do wyboru są cztery stałe obszary.
5. Kliknij przycisk **Draw Area**, a następnie kliknij i przeciągnij wskaźnik myszy, aby narysować obszar zainteresowania na obrazie wideo na żywo.
6. Wybierz poziom ROI, aby ustawić poziom poprawy jakości obrazu. Im większa wartość, tym lepsza jakość obrazu.



Rysunek 5–27 Ustawienia obszaru zainteresowania

7. Wprowadź nazwę obszaru ROI.
8. Kliknij przycisk **Save**, aby zapisać ustawienia.

5.5 Konfigurowanie parametrów obrazu

5.5.1 Konfigurowanie ustawień wyświetlania

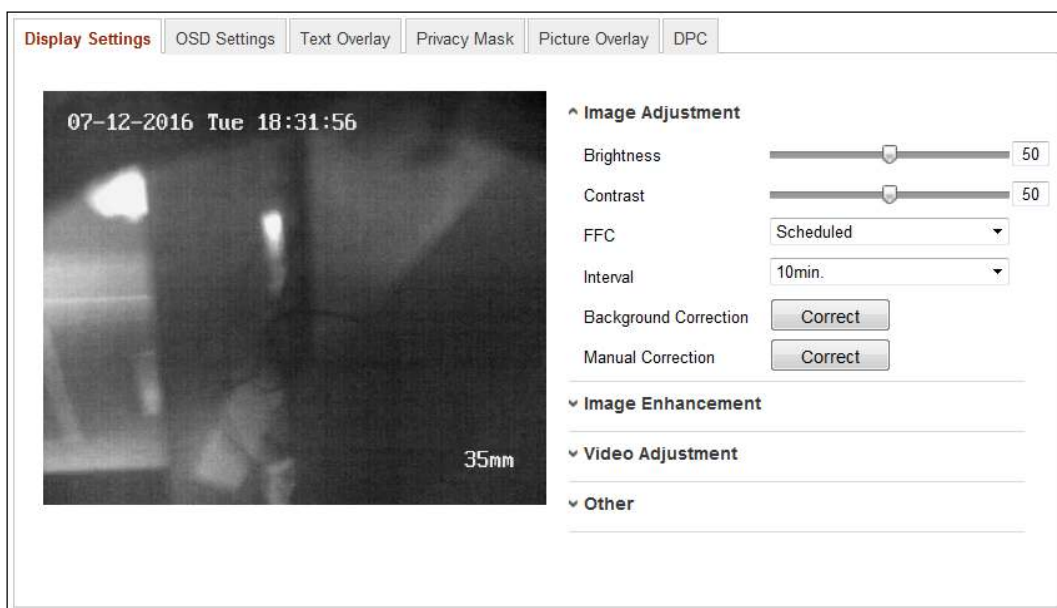
Cel:

Można ustawić parametry jakości obrazu kamery takie jak jasność i kontrast.

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

Kroki:

1. Przejdź do interfejsu Display Settings:
Configuration > Basic Configuration > Image > Display Settings
 Lub **Configuration > Advanced Configuration > Image > Display Settings**
2. Skonfiguruj parametry obrazu z kamery.



Rysunek 5–28 Konfigurowanie ustawień wyświetlania dla kamery 2

- **Dostosowanie obrazu**

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.

FFC (korekcja płaskiego pola) poprawia jakość obrazowania cyfrowego. Pozwala usunąć artefakty z obrazów dwuwymiarowych, które są spowodowane różnicą czułości pikseli w urządzeniu wykrywającym lub zakłóceń występujących w ścieżce optycznej. Do wyboru dostępne są opcje: harmonogram, temperatura i wyłączenie.

- **Schedule:** Można wybrać interwał korekcji o wartości: 10, 20, 30, 40, 50, 60, 120, 180 lub 240 minut.
- **Temperature:** Kamera dostosowuje obraz w zależności od temperatury.

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.

- **Poprawa obrazu**

Digital Noise Reduction: Funkcja DNR ogranicza zakłócenia szumowe w strumieniu wideo. Dostępne do wyboru są opcje: OFF, Normal i Expert. W trybie zwykłym ustaw poziom DNR w zakresie od 0 do 100. W trybie eksperta ustaw poziom DNR zarówno z poziomu DNR przestrzeni [0-100], jak i z poziomu DNR czasu [0-100].

Palettes: Palety pozwalają wybrać pożądane kolory. Do wyboru dostępne są następujące opcje: 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.

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

- **Dostosowane obrazu wideo**

Mirror: Lustrzane przekształcenie umożliwia wyświetlenie odwróconego obrazu. Do wyboru dostępne są opcje: Left/Right, Up/Down, Center, i OFF.

Video Standard: Do wyboru dostępne są opcje 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 funkcje**

Local Output: Włącz lub wyłącz lokalne wyjście urządzenia.

3. (Opcjonalnie) Kliknij przycisk **Default**, aby przywrócić ustawienia domyślne

5.5.2 Konfigurowanie ustawień menu ekranowego

Cel:

Można dostosować nazwę kamery i czas na ekranie.

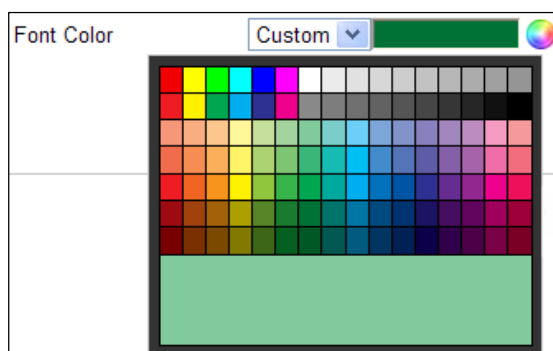
Kroki:

1. Przejdź do interfejsu OSD Settings:

Configuration > Advanced Configuration > Image > OSD Settings

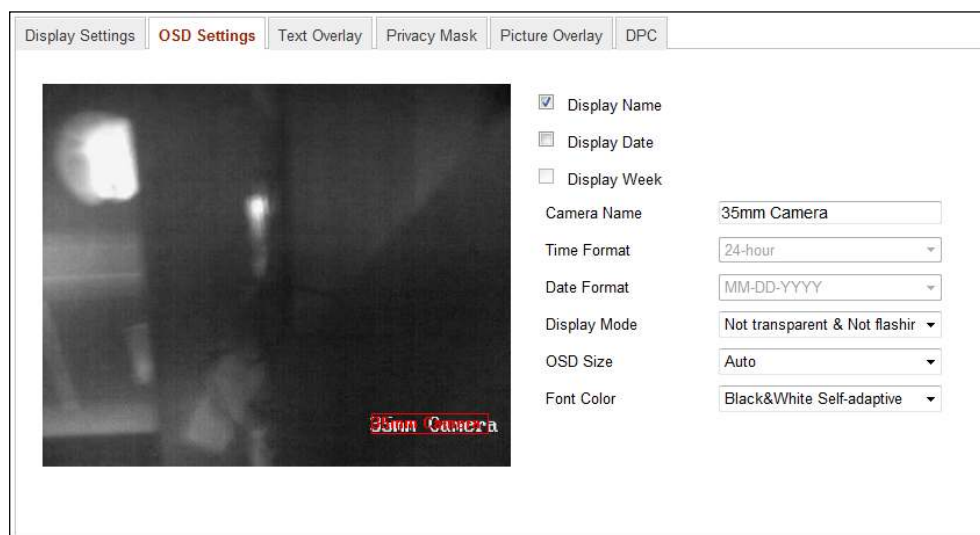
Rysunek 5–29 Ustawienia OSD

2. Zaznacz odpowiednie pole wyboru, aby wybrać opcję wyświetlania nazwy kamery, daty lub tygodnia, jeżeli jest to wymagane.
3. Edytuj nazwę kamery w polu **Camera Name**.
4. Z listy rozwijanej wybierz format czasu, formatu daty, tryb wyświetlania i rozmiar czcionki OSD.
5. Zdefiniuj kolor czcionki OSD, klikając menu rozwijane. Do wyboru dostępne są opcje: black & white self-adaptive oraz custom.



Rysunek 5–30 Niestandardowy kolor czcionki

6. (Opcjonalnie) Można użyć wskaźnika myszy, aby kliknąć i przeciągnąć ramkę tekstową **35mm Camera** w oknie podglądu na żywo w celu dostosowania położenia OSD.



Rysunek 5–31 Dostosowywanie położenia OSD

7. Kliknij **Save**, aby aktywować powyższe ustawienia.

5.5.3 Konfigurowanie ustawień nakładek tekstowych

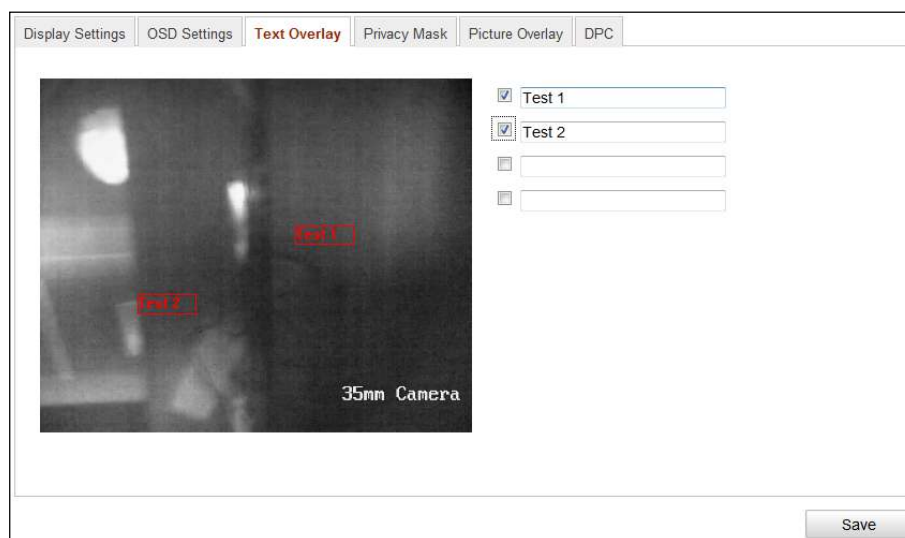
Cel:

W interfejsie tym można wprowadzić niestandardowe ustawienia wyświetlania nakładek tekstowych.

Kroki:

1. Przejdź do interfejsu ustawień nakładek tekstowych, wybierając opcje:

Configuration > Advanced Configuration > Image > Text Overlay



Rysunek 5–32 Nakładanie tekstu

2. Zaznacz pole wyboru z lewej strony pola tekstowego, które chcesz wyświetlić na ekranie.
3. Wprowadź odpowiednie informacje w polu tekstowym.
4. (Opcjonalnie) Użyj wskaźnika myszy, aby kliknąć i przeciągnąć czerwoną ramkę tekstową **Test 1** w oknie podglądu na żywo w celu dostosowania położenia nakładania tekstu.
5. Kliknij przycisk **Save**, aby zapisać ustawienia.

Uwaga: Można skonfigurować maksymalnie osiem nakładek tekstowych.

5.5.4 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 > Advanced Configuration > Image > Privacy Mask



Rysunek 5–33 Ustawienia maski prywatności

2. Zaznacz pole wyboru „**Enable Privacy Mask**“, aby włączyć tę funkcję.
3. Kliknij przycisk **Draw Area**.
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.

5.5.5 Konfigurowanie nakładania obrazu

Cel:

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

Uwaga: Obraz musi mieć format .bmp RGB24 oraz maksymalny rozmiar 128*128.

Kroki:

1. Przejdź do interfejsu ustawień nakładania obrazu:

Configuration > Advanced Configuration > Image > Picture Overlay



Rysunek 5–34 Nakładanie obrazu

2. Kliknij przycisk **Browse**, aby wybrać zdjęcie.
3. Kliknij przycisk przesyłania, aby je przesłać.
4. Zaznacz pole wyboru włączenia nakładania obrazu, aby włączyć tę funkcję.
Wartości współrzędnych X i Y służą do lokalizacji zdjęcia na obrazie. Z kolei szerokość i wysokość zdjęcia określają rozmiar obrazu.
5. Kliknij przycisk **Save**, aby zapisać ustawienia.

5.5.6 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 > Advanced Configuration > Image > DPC

2. Kliknij obraz, aby zaznaczyć uszkodzony piksel. Wskaźnik na obrazie zostanie przeniesiony do klikniętego miejsca. Można kliknąć przycisk , aby nieco dopasować położenie kursora.

3. Kliknij przycisk , aby uruchomić korekcję.




Rysunek 5–35 Korekcja wadliwych pikseli

4. (Opcjonalnie) Kliknij przycisk , aby anulować korekcję.

5.6 Konfigurowanie i obsługa zdarzeń alarmowych

W tym Rozdziale wyjaśniono, jak należy konfigurować kamerę sieciową, aby reagowała na zdarzenia alarmowe, takie jak detekcja ruchu, alarm sabotażu sygnału wideo, wejście alarmu, wyjście alarmu, wyjątek, detekcja twarzy, detekcja nietypowego dźwięku, detekcja wtargnięcia, detekcja braku ostrości i detekcja zmiany sceny. Te zdarzenia mogą wywołać metody powiązania takie jak powiadomienie centrum monitoringu, wysłanie wiadomości e-mail czy wyzwolenie wyjścia alarmu.

Uwagi:

- 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.
- Kliknij przycisk , aby uzyskać pomoc podczas konfigurowania funkcji inteligentnych takich jak detekcja twarzy, detekcja nietypowego dźwięku, detekcja wtargnięcia, detekcja braku ostrości, detekcja zmiany sceny. W dokumencie pomocy znajdują się instrukcje dotyczące konfiguracji.

5.6.1 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: Ustawianie obszaru detekcji ruchu.

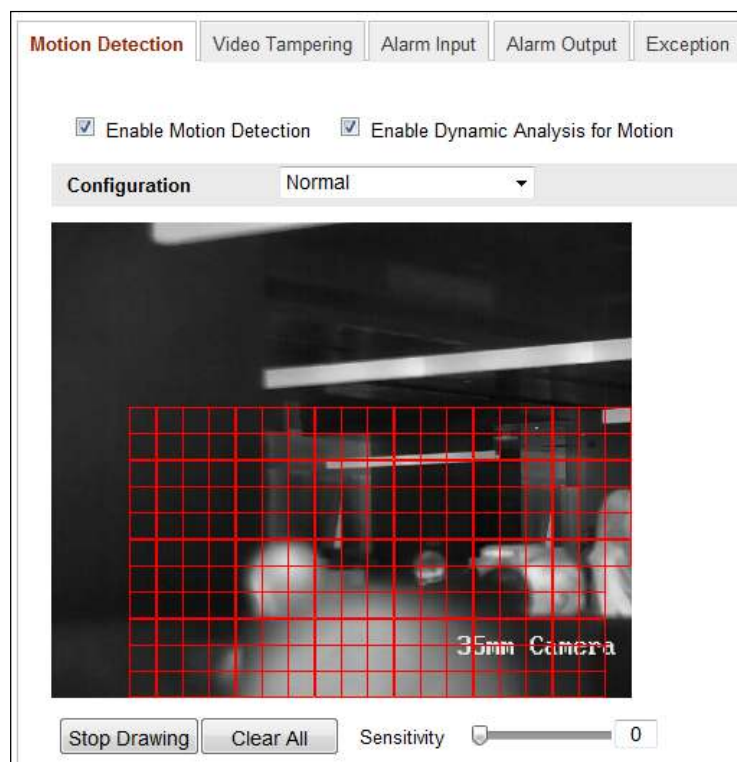
Kroki:

- (1) Przejdź do interfejsu ustawień detekcji ruchu

Configuration > Advanced Configuration > Basic Event > Motion Detection

- (2) Zaznacz pole wyboru **Enable Motion Detection**.
- (3) Zaznacz pole wyboru **Enable Dynamic Analysis for Motion**, jeśli chcesz oznaczyć wykryte obiekty przy użyciu zielonych prostokątów na obrazie wideo na żywo.

Uwaga: Aby włączyć/wyłączyć oznaczenie obiektów ruchu na obrazie wideo na żywo, przejdź do obszaru Local Configuration > Live View Parameters i włącz/wyłącz reguły.

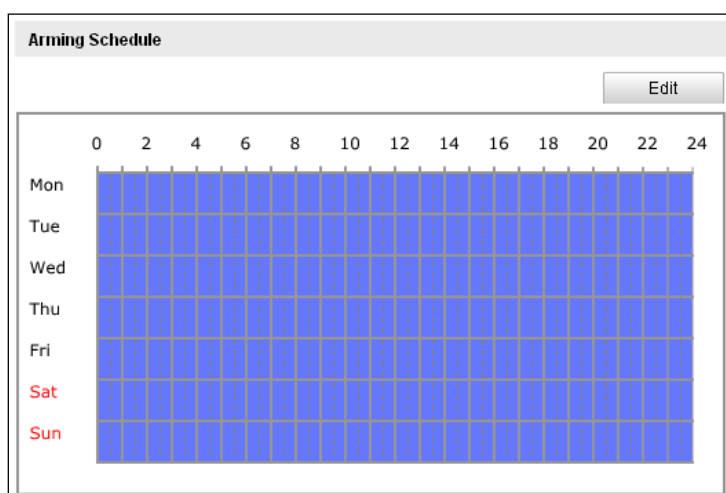


Rysunek 5–36 Włączanie detekcji ruchu


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

Zadanie 2: Ustawianie harmonogramu uzbrajania pod kątem detekcji ruchu.

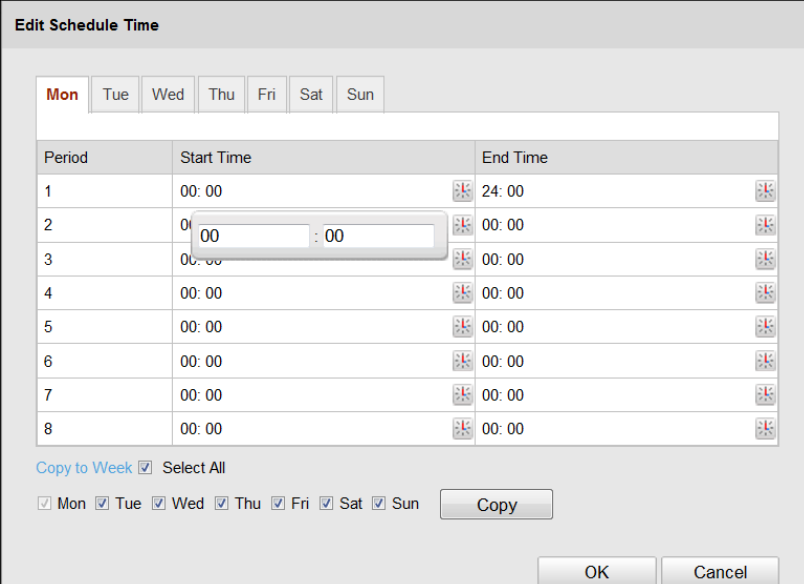
Kroki:



Rysunek 5–37 Czas uzbrojenia

- (1) Kliknij przycisk **Edit**, aby edytować harmonogram uzbrajania. Na rysunku 6-34 pokazano interfejs edycji harmonogramu uzbrajania.
- (2) Wybierz dzień, na który chcesz ustawić harmonogram uzbrajania.
- (3) Kliknij przycisk , aby ustawić przedział czasu harmonogramu uzbrajania.
- (4) (Opcjonalnie) Po ustawieniu harmonogramu uzbrajania można skopiować harmonogram na inne dni.
- (5) Kliknij przycisk **OK**, aby zapisać ustawienia.

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



Edit Schedule Time

Mon Tue Wed Thu Fri Sat Sun

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

Copy to Week ☒ Select All

☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☒ Sat ☒ Sun

Copy

OK Cancel

Rysunek 5–38 Harmonogram czasu uzbrojenia

Zadanie 3: Ustawianie działań alarmowych detekcji ruchu.

Aby wybrać określone działania powiązane, zaznacz odpowiednie pola wyboru. Do wyboru dostępne są opcje: Notify surveillance center, send email, upload to FTP, trigger channel i Trigger alarm output. W interfejsie tym można określić działania powiązane z wystąpieniem zdarzenia.

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

Rysunek 5–39 Działania powiązane

- **Ostrzeżenie dźwiękowe**

Wyzwalanie lokalnego ostrzeżenia dźwiękowego. Funkcja ta jest obsługiwana tylko przez urządzenia wyposażone w wyjście audio.

- **Powiadomienie centrum monitoringu**

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

- **Prześlij wiadomość e-mail**

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

Uwaga: Aby wysłać wiadomość e-mail w chwili zajścia zdarzenia, patrz *Rozdział 5.3.9 Wysyłka wiadomości e-mail wyzwalana przez alarm*, aby ustawić odpowiednie parametry.

- **Przesyłanie zdjęć na serwer FTP**

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 szczegółowe informacje, patrz *Rozdział 5.3.11 Konfigurowanie ustawień serwera FTP*.
- Przejdź do strony **Advanced Configuration > Storage > Snapshot**, aby włączyć wykonywanie zdjęć wyzwalane zdarzeniem, a następnie ustaw interwał wykonywania zdjęć i liczbę wykonywanych zdjęć.
- Wykonane zdjęcie można również przekazać do dostępnej karty SD lub dysku sieciowego.

- **Wyzwalany Kanał**

Video może być nagrywane po wykryciu ruchu. Aby móc skorzystać z tej funkcji, należy skonfigurować harmonogram nagrywania. Aby uzyskać szczegółowe informacje, patrz *Rozdział 6.3*.

- **Wyzwolenie wyjścia alarmowego**

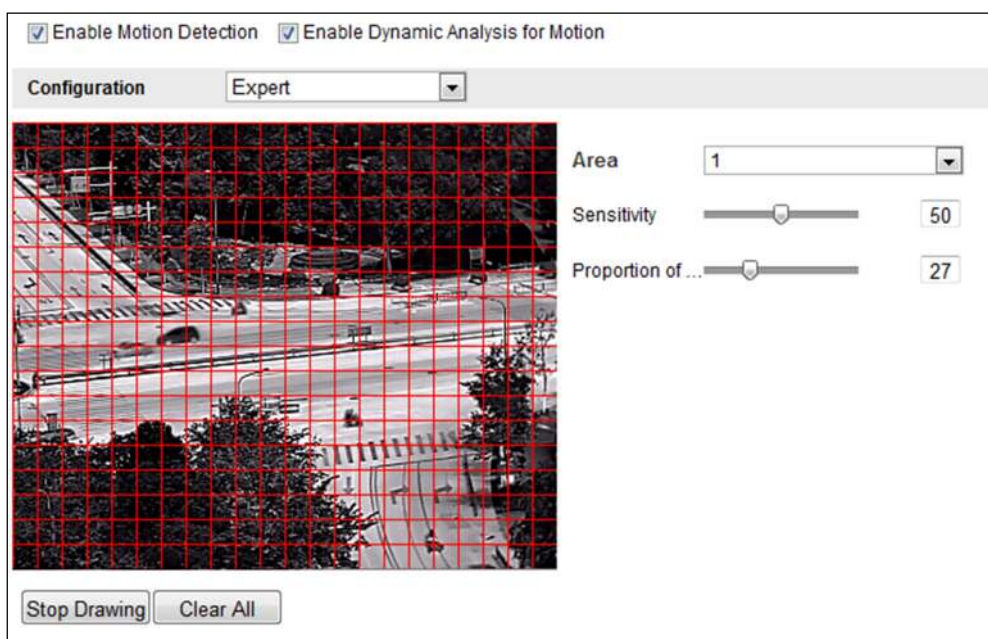
Wyzwolenie jednego lub kilku wyjść alarmu zewnętrznego w chwili wystąpienia zdarzenia.

Uwaga: Aby wyzwolić wyjście alarmu w chwili zajścia zdarzenia, patrz *Rozdział 5.6.4 Konfigurowanie wyjścia alarmu*, aby ustawić odpowiednie parametry.

- **Konfiguracja zaawansowana**

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

Uwaga: Przełączanie trybu dzień/noc jest niemożliwe w przypadku kanału kamery termowizyjnej. Jednak można wciąż konfigurować obszar, czułość i proporcje obiektu na obszarze.



Rysunek 5–40 Tryb zaawansowany detekcji ruchu

5.6.2 Konfigurowanie alarmu sabotażu sygnału wideo

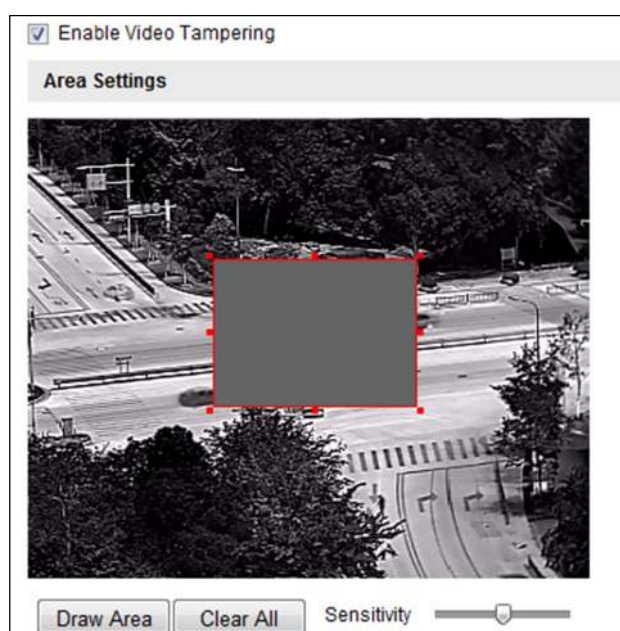
Cel:

Można skonfigurować kamerę, aby wyzwała alarm w przypadku zakrycia obiektywu oraz wykonywała pewne działania alarmowe.

Kroki:

1. Przejdź do interfejsu ustawień sabotażu sygnału wideo, wybierając opcję:

Configuration > Advanced Configuration > Basic Event > Video Tampering



Rysunek 5–41 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. Patrz *Zadanie 1 Ustawianie obszaru detekcji ruchu* w Rozdziale 5.6.1.
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. Patrz *Zadanie 2 Ustawianie harmonogramu uzbrajania pod kątem detekcji ruchu* w Rozdziale 5.6.1.

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. Patrz *Zadanie 3 Ustawianie działań alarmowych pod kątem detekcji ruchu* w Rozdziale 5.6.1.
6. Kliknij przycisk **Save**, aby zapisać ustawienia.

5.6.3 Konfigurowanie wejścia alarmu

Cel:

Wykrywa wejście alarmu i podejmuje działania w przypadku wyzwolenia alarmu.

Kroki:

1. Przejdź do interfejsu ustawień wejścia alarmu, wybierając opcje:

Configuration > Advanced Configuration > Basic Event > Alarm Input

2. Wybierz numer wejścia alarmu i typ alarmu. Dostępne typy alarmu to: NO (normalnie otwarty) i NC (normalnie zamknięty). Edytuj nazwę wejścia alarmowego (opcjonalnie).

Alarm Input No.

Alarm Name (cannot copy)

Alarm Type

Arming Schedule

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

Rysunek 5–42 Ustawienia wejścia alarmu

3. Kliknij przycisk **Edit**, aby ustawić harmonogram uzbrajania dla wejścia alarmu. Patrz *Zadanie 2 Ustawianie harmonogramu uzbrajania pod kątem detekcji ruchu* w Rozdziale 5.6.1.
4. Zaznacz pole wyboru, aby wybrać metodę powiązania stosowaną dla wejścia alarmu. Patrz *Zadanie 3 Ustawianie działań alarmowych pod kątem detekcji ruchu* w Rozdziale 5.6.1.
5. Można również wybrać powiązanie PTZ dla wejścia alarmu, jeśli kamera jest zainstalowana z jednostką umożliwiającą obrót/pochylenie. Zaznacz odpowiednie pole wyboru i wybierz numer ustawienia wstępnego, patrolu lub wzorca, aby je wywołać w momencie wystąpienia alarmu.
6. Ustawienia można skopiować i zastosować do innych wejść alarmu.
7. Kliknij przycisk **Save**, aby zapisać ustawienia.

5.6.4 Konfigurowanie wyjścia alarmu

Cel:

Wykrywa wyjście alarmu i podejmuje działania w przypadku wyzwolenia alarmu.

Kroki:

1. Przejdź do interfejsu ustawień wyjścia alarmu, wybierając opcje:
Configuration > Advanced Configuration > 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 przycisk **Edit**, aby przejść do interfejsu edycji czasu harmonogramu. Konfiguracja harmonogramu czasu jest taka sama jak dla ustawień harmonogramu uzbrajania dotyczących detekcji ruchu. Patrz *Zadanie 2 Ustawianie harmonogramu uzbrajania pod kątem detekcji ruchu* w Rozdziale 5.6.1.
5. Ustawienia można skopiować i zastosować do innych wyjść alarmu.
6. Kliknij przycisk **Save**, aby zapisać ustawienia.

Alarm Output: A->1

Alarm Name: (cannot copy)

Delay: 5s

Arming Schedule

Edit

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

Rysunek 5–43 Ustawienia wyjścia alarmu

5.6.5 Obsługa zdarzeń nietypowych

Można ustawić następujące rodzaje wyjątków: zapelnienie 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 > Advanced Configuration > Basic Event > Exception
2. Zaznacz pole wyboru, aby ustawić działania wykonywane w momencie wystąpienia alarmu zdarzenia nietypowego. Patrz *Zadanie 3 Ustawianie działań alarmowych wykonywanych pod kątem detekcji ruchu* w Rozdziale 5.6.1.

Exception Type: HDD Full

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

Save

Rysunek 5–44 Ustawienia zdarzeń nietypowych

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

5.6.6 Konfigurowanie detekcji nietypowego dźwięku

Cel:

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

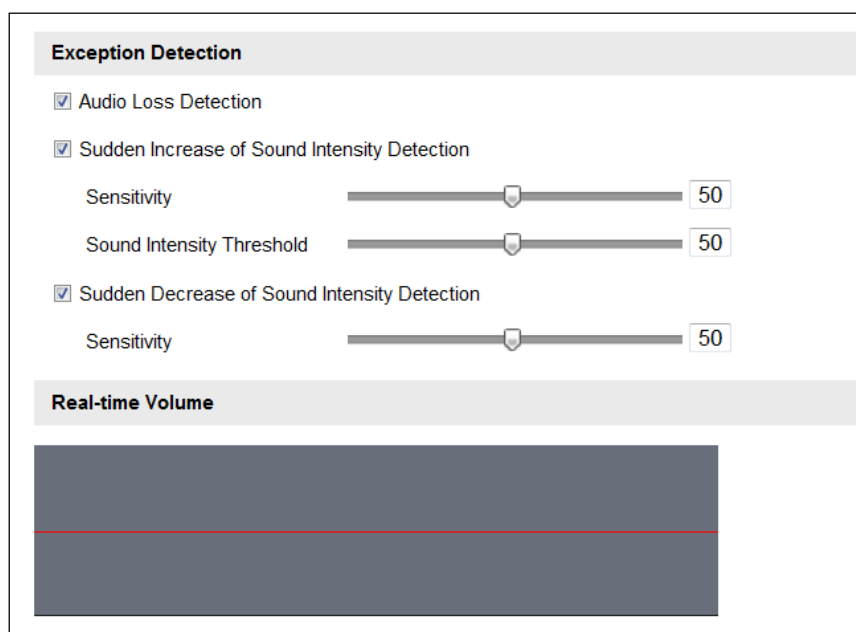
Uwaga: Funkcja detekcji nietypowego dźwięku jest zależna od modelu kamery.

Kroki:

1. Przejdź do interfejsu ustawień detekcji nietypowego dźwięku:
Configuration > Advanced Configuration > Smart Event > Audio Exception Detection
2. 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.



Rysunek 5–45 Konfigurowanie detekcji nietypowego dźwięku

5. Można wyświetlić głośność dźwięku w czasie rzeczywistym.
6. Kliknij przycisk **Edit**, aby skonfigurować harmonogram zabezpieczenia.
7. Wybierz metody powiązania nietypowego dźwięku. Patrz **Zadanie 3 Ustawianie działań alarmowych wykonywanych pod kątem detekcji ruchu** w Rozdziale 5.6.1.
8. Kliknij przycisk **Save**, aby zapisać ustawienia.

5.6.7 Detekcja zmiany sceny

Cel:

Ta funkcja umożliwia detekcję zmiany sceny monitorowanego środowiska na skutek czynników zewnętrznych, takich jak celowe obrócenie kamery, i wykonanie określonych akcji po wyzwoleniu alarmu.

Kroki:

1. Przejdź do interfejsu ustawień detekcji zmiany sceny: Configuration > Advanced Configuration > Smart Event > Scene Change Detection.
2. Zaznacz pole wyboru **Enable Scene Change Detection**, aby włączyć tę funkcję.
3. Kliknij i przeciągnij suwak czułości detekcji dożądanego położenia. Zakres wartości czułości wynosi od 1 do 100. Im wyższa jest wartość, tym łatwiej zmiana sceny może wywołać alarm.

4. Kliknij przycisk **Edit**, aby skonfigurować harmonogram zabezpieczenia.
5. Wybierz metody powiązania dla zmiany sceny, w tym: **Powiadomienie centrum monitoringu, Wyślij e-mail, Przekaż do serwera FTP, wyzwany kanał i Wyzwolenie wyjścia alarmu.**
6. Kliknij przycisk **Save**, aby zapisać ustawienia.

5.6.8 Konfigurowanie dynamicznej detekcji źródła ognia

Cel:

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

Kroki:

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

Audio Exception Detection **Dynamic Fire Source Detection**

Dynamic Fire Source Detection

☒ Enable Dynamic Fire Source Detection

☒ Display Fire Source Frame on Stream

Sensitivity 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	

Save

Rysunek 5–46 Konfigurowanie dynamicznej detekcji źródła ognia

3. Zaznacz pole wyboru **Display Fire Source Frame on Stream**, aby w przypadku pożaru wyświetlić na strumieniu czerwoną ramkę wokół źródła ognia. (Opcjonalnie)
4. Można przesunąć wskaźnik, aby dostosować stopień czułości 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 działań alarmowych pod kątem detekcji ruchu** w Rozdziale **Detekcja ruchu**. Można zaznaczyć pole wyboru w polu innych powiązań, aby włączyć wyjście alarmu (numer wyjścia alarmu różni się w zależności od funkcji urządzenia).
6. Kliknij przycisk **Save**, aby zapisać ustawienia.

5.7 Pomiar temperatury

Cel:

Po włączeniu funkcja ta mierzy rzeczywistą temperaturę monitorowanego miejsca. Gdy temperatura przekracza wartość progową temperatury, uruchomiony zostaje alarm urządzenia.

Zanim zaczniesz:

Przejdź do obszaru **Configuration > Advanced Configuration > System > VCA Resource Type**, aby wybrać opcję **Temperature Measurement + Behavior Analysis** jako typ zasobu VCA.

5.7.1 Konfiguracja pomiaru temperatury

Kroki:

1. Otwórz obszar **Configuration > Advanced Configuration > Temperature Measurement Configuration**.

Rysunek 5–47 Dynamiczna detekcja źródła ognia

2. Zaznacz pola wyboru w interfejsie, aby ustawić konfigurację pomiaru temperatury.
 - **Enable Temperature Measurement:** Zaznacz pole wyboru, aby włączyć funkcję pomiaru temperatury.
 - **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.
3. Kliknij przycisk **Save**, aby zapisać ustawienia.

5.7.2 Pomiar i alarm temperatury

Cel:



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

Kroki:

1. Przejdź do obszaru **Configuration > Advanced Configuration > Temperature Measurement and Alarm**.
2. Ustaw regułę alarmu: Z listy reguł wybierz regułę pomiaru temperatury i skonfiguruj parametry.

- **Name:** Można dostosować nazwę reguły.
- **Type:** Wybierz jeden z typów reguły: punkt, linię lub ramkę.
- **Emissivity:** Ustaw emisyjność obiektu docelowego. Uwaga: Emisyjność każdego obiektu jest inna.
- **Distance (m):** Odległość w linii prostej pomiędzy celem a urządzeniem.
- **Reflective Temperature:** W przypadku występowania na scenie celu o wysokiej emisyjności zaznacz to pole wyboru i ustaw temperaturę odbitą, aby skorygować temperaturę. W przypadku braku takiego celu odznacz to pole wyboru.

Temperature Measurement Configuration **Temperature Measurement and Alarm**


07-12-2016 Tue 16:15:30






Region Tem...
Alarm Linkage

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

Save

Rysunek 5-48 Konfiguracja pomiaru temperatury

3. Kliknij przycisk  na liście, aby wyświetlić interfejs reguł alarmowych.

- **Alarm Rule:** Reguła alarmu różni się w zależności od typu. Reguła ma za zadanie porównanie informacji o temperaturze z dwóch wybranych obszarów. W przypadku celów wyznaczonych za pomocą ramki można użyć następujących reguł: **Temperatura maksymalna jest wyższa niż, Temperatura maksymalna jest niższa niż, Temperatura minimalna jest wyższa niż, Temperatura minimalna jest niższa niż, Średnia temperatura jest wyższa niż, Średnia temperatura jest niższa niż, Różnica temperatur jest wyższa niż i Różnica temperatur jest niższa niż.** W przypadku celów wyznaczonych za pomocą linii można użyć reguł: Max. Temperature, Min. Temperature i Average Temperature. W przypadku celów wyznaczonych za pomocą punktu można użyć reguły Average Temperature.
 - **Pre-Alarm Temperature i Alarm Temperature:** Ustaw temperaturę alarmu wstępnego i temperaturę alarmu. Urządzenie wysyła alarm wstępny w przypadku, gdy temperatura reguły przekroczy temperaturę alarmu wstępnego oraz wysyła alarm w przypadku, gdy temperatura reguły przekroczy temperaturę alarmu.
 - **Tolerance Temperature:** Ustaw dopuszczalne odchylenie temperatury, aby umożliwić urządzeniu określenie, czy wyzwolony alarm powinien zostać zatrzymywany, gdy temperatura/różnica temperatur urządzenia jest niższa od temperatury reguły o wartość dopuszczalnego odchylenia temperatury. Na przykład można ustawić dopuszczalne odchylenie temperatury na poziomie 3° C, temperaturę alarmu na 55°C, a temperaturę alarmu wstępnego na 50°C. Urządzenie wysyła alarm wstępny, gdy jego temperatura osiągnie 50°C, natomiast gdy jego temperatura osiągnie 55°C następuje uruchomienie alarmu. Alarm zostanie anulowany dopiero, gdy temperatura urządzenia spadnie poniżej 52°C.
4. Narysuj obszar docelowy: Wybierz regułę i narysuj odpowiednią ramkę/linię/punkt. Kliknij przycisk , aby narysować punkt. Kliknij przycisk , aby narysować linię. Kliknij przycisk , aby narysować ramkę.
 5. Ustaw alarm różnicy temperatur: Kliknij przycisk Temperature Difference Alarm, aby przejść do interfejsu alarmu różnicy temperatur. Można ustawić maks. cztery alarmy różnicy temperatur.
-
- Alarm różnicy temperatury dotyczy tylko celów wytyczonych ramką.
6. Ustaw powiązanie alarmu: Kliknij przycisk Alarm Linkage, aby przejść do interfejsu powiązania alarmowego i ustawić metody powiązania.
 7. Kliknij przycisk **Save**, aby zapisać ustawienia.

5.8 Konfiguracja VCA

5.8.1 Typ zasobu VCA

Przed użyciem reguł VCA kamery należy wybrać typ zasobu VCA.

Aby używać pomiaru temperatury i analizy zachowania, wybierz **Temperature Measurement** i **Behavior Analysis**. Aby użyć funkcji dynamicznej detekcji źródła ognia, wybierz opcję **Dynamic Fire Source Detection**. Po wybraniu któregoś z tych zasobów nie można włączyć innej reguły VCA.

5.8.2 Informacje VCA

- **Behavior Analysis Version:**

Wersja biblioteki algorytmów.

- **Display information**

Zawiera wyświetlanie na obrazie i wyświetlanie na strumieniu. Zaznacz pola wyboru, aby włączyć odpowiednie wyświetlacze.

VCA Info.

Behavior Analysis Version: V3.2.2build20140904

Display Information

Display on Picture

☐ Display Target Info. on Alarm Picture

☐ Display Rule Info. on Alarm Picture

Display on Stream

☐ Display VCA Info. on Stream

Snapshot Settings

☒ Upload JPEG Image to Center

Picture Quality: High

Picture Resolution: 384*288

Save

Rysunek 5–49 Informacje VCA

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

Uwaga: Upewnij się, że reguły są włączone w ustawieniach lokalnych. Przejdź do **Configuration > Local Configuration > Rules**, aby włączyć tę funkcję.

- **Snapshot Setting**

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:** Można wybrać 384*288, CIF, 4CIF, 720P lub 1080P.

Uwaga: Dostępne do wyboru opcje rozdzielczości zdjęć różnią się w zależności od modelu.

5.8.3 Analiza zachowania

Cel:

Analiza zachowania umożliwia detekcję serii podejrzanych zachowań i wykonanie powiązanych działań po wyzwoleniu alarmu. Zapoznaj się z następującymi czynnościami, aby skonfigurować ustawienia analizy zachowania.

Kroki:

1. Skonfiguruj informacje wyświetlania i ustawienia wykonywania zdjęć na stronie **VCA Info**.

2. Ustaw **kalibrację kamery**

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.

Kroki:

- 1) Przejdź do interfejsu ustawiania kalibracji kamery:

Configuration > VCA Configuration > Camera Calibration

- 2) Zaznacz pole wyboru **Camera Calibration**, aby włączyć tę funkcję.
- 3) W pozycji calibration mode wybierz Input Basic Data lub Draw on Live View Video.

Input Basic Data: Wprowadź ręcznie wysokość mocowania, kąt widzenia i współczynnik horyzontu kamery.

Draw on Live View Video: Kliknij przycisk rysowania linii weryfikacji (poziomej)/(pionowej), aby narysować linię poziomą/pionową w podglądzie na żywo, a następnie wprowadź długość rzeczywistą w polu długości rzeczywistej. Korzystając z wyznaczonych linii referencyjnych i ich rzeczywistej długości, kamera może analizować inne obiekty w podglądzie na żywo.

- 4) (Opcjonalnie) Zaznacz pole wyboru **Enable Verification of Camera Calibration**, kliknij przycisk **Horizontal Verify/Vertical Verify**, aby narysować linię poziomą/pionową w trybie podglądu na żywo, a następnie kliknij przycisk **Calibrate**, aby obliczyć długość linii. Porównaj obliczoną długość linii z rzeczywistą długością, aby zweryfikować skonfigurowane informacje kalibracyjne.
- 5) Kliknij przycisk **Delete**, aby usunąć narysowane linie.
- 6) Kliknij przycisk **Save**, aby zapisać ustawienia.

Uwaga: Jeżeli widok na żywo zostanie zatrzymany, kamera nie zostanie prawidłowo skalibrowana.

Camera Calibration

☒ Camera Calibration
☐ Enable Verification of Camera Calibration

Calibration Mode

Input Basic Data

H: Mounting Height [2-50m]

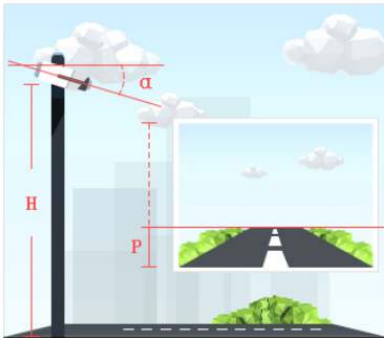

0

α: Viewing Angle [1-89°]

0

P: Horizontal Ratio [0-10000%]

0

Save

Rysunek 5–50 Wprowadzanie danych podstawowych

Camera Calibration

☒ Camera Calibration
☐ Enable Verification of Camera Calibration

Calibration Mode

Draw on Live Video

Horizontal Line

Vertical Line

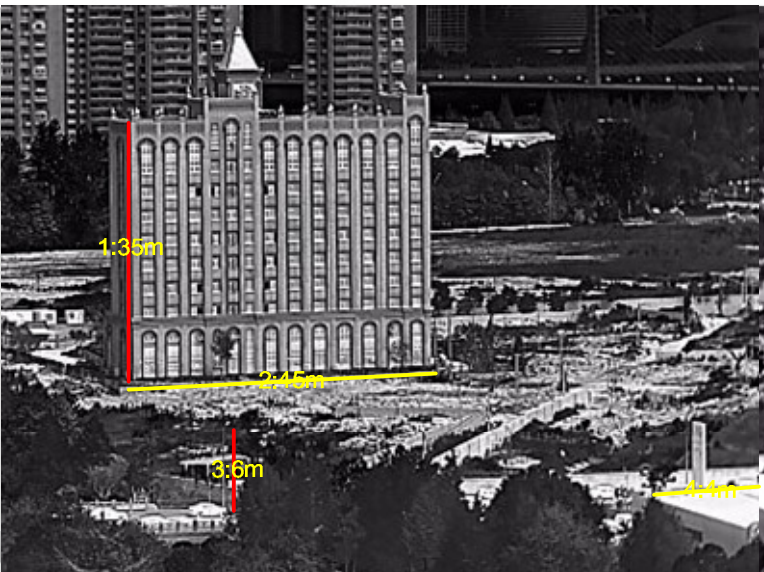
Horizontal Verify

Vertical Verify

Calibrate

Delete

Stop



Real Length [1-100m]

1

35

Mounting Height

Viewing Angle

Horizontal Ratio

Save

Rysunek 5–51 Wyznaczanie linii w podglądzie na żywo

3. Narysuj **chroniony obszar**

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

Kroki:

- 1) Przejdź do interfejsu ustawiania chronionego obszaru:

Configuration > VCA Configuration > Shield Region

- 2) Kliknij przycisk **Draw Area**. Wyznacz obszar, 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.
- Kliknij przycisk **Delete**, aby usunąć narysowane obszary.
- Jeżeli podgląd na żywo zostanie zatrzymany, nie można wyznaczyć obszarów chronionych.



- 3) Kliknij przycisk **Save**, aby zapisać ustawienia.

4. Skonfiguruj **regułę**

Analiza zachowania obsługuje szereg zachowań, w tym przekraczanie linii, wtargnięcie, wejście w obszar i wyjście z obszaru.

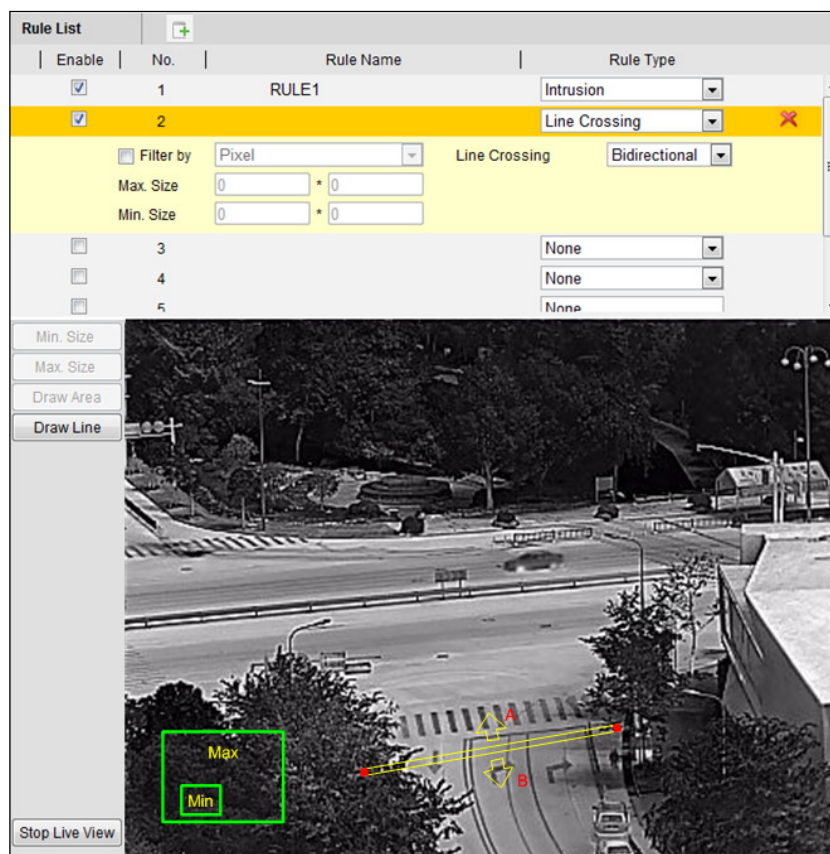
Uwaga: Typ reguły dla ustawienia różni się w zależności od modelu kamery.

Kroki:

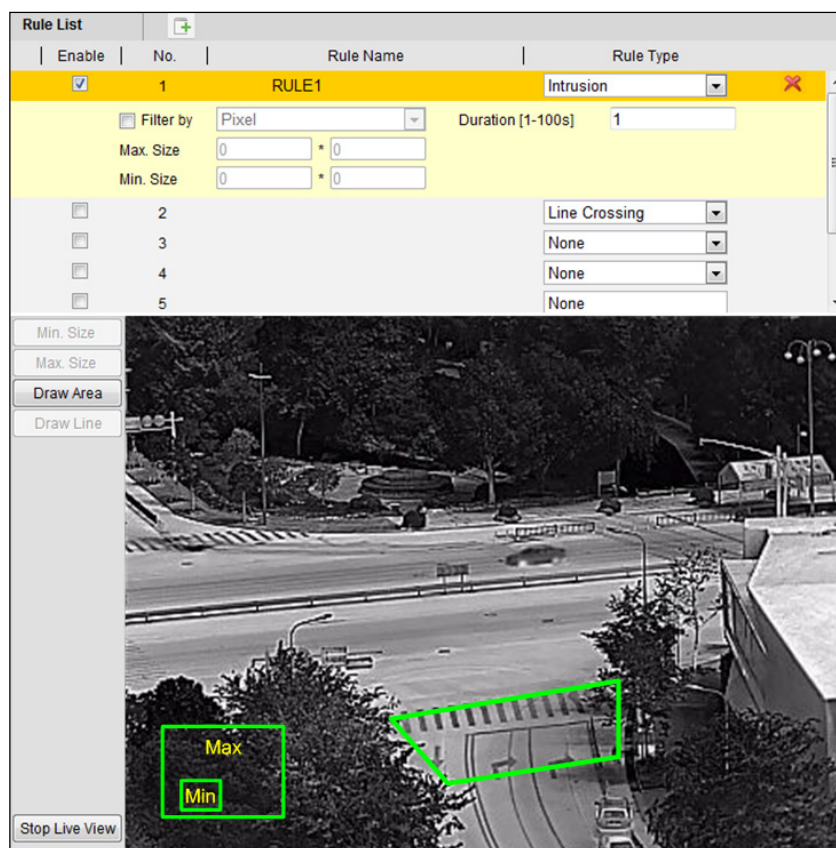
- 1) Kliknij kartę **Rule**, aby wyświetlić okno konfiguracji reguł.
- 2) Kliknij przycisk , aby dodać nową regułę. (Opcjonalnie) Kliknij przycisk , aby ją usunąć.
- 3) Zaznacz pole wyboru pożądanej reguły, aby włączyć regułę dla analizy zachowania.
- 4) Wybierz typ reguły, ustaw typ filtru, a następnie wyznacz linię/obszar w podglądzie wideo na żywo dla pojedynczej reguły.
 - Funkcja **Line Crossing** wykrywa osoby, pojazdy lub inne obiekty przekraczające wstępnie zdefiniowaną linię wirtualną, a po wyzwoleniu alarmu mogą być wykonywane różne działania.

Po wybraniu tego typu reguły należy wybrać kierunek przekroczenia linii przed jej narysowaniem. Do wyboru dostępne jest przekroczenie w dwóch kierunkach, w kierunku od A do B i od B do A.

- Funkcja **Intrusion** wykrywa osoby, pojazdy lub inne obiekty, które wkraczają na wstępnie zdefiniowany obszar wirtualny i pozostają na nim. Po wyzwoleniu alarmu mogą być wykonywane różne działania. Po wybraniu tego typu reguły należy ustawić czas trwania wtargnięcia. Dostępny zakres czasu trwania wynosi od 1 do 100 sekund.

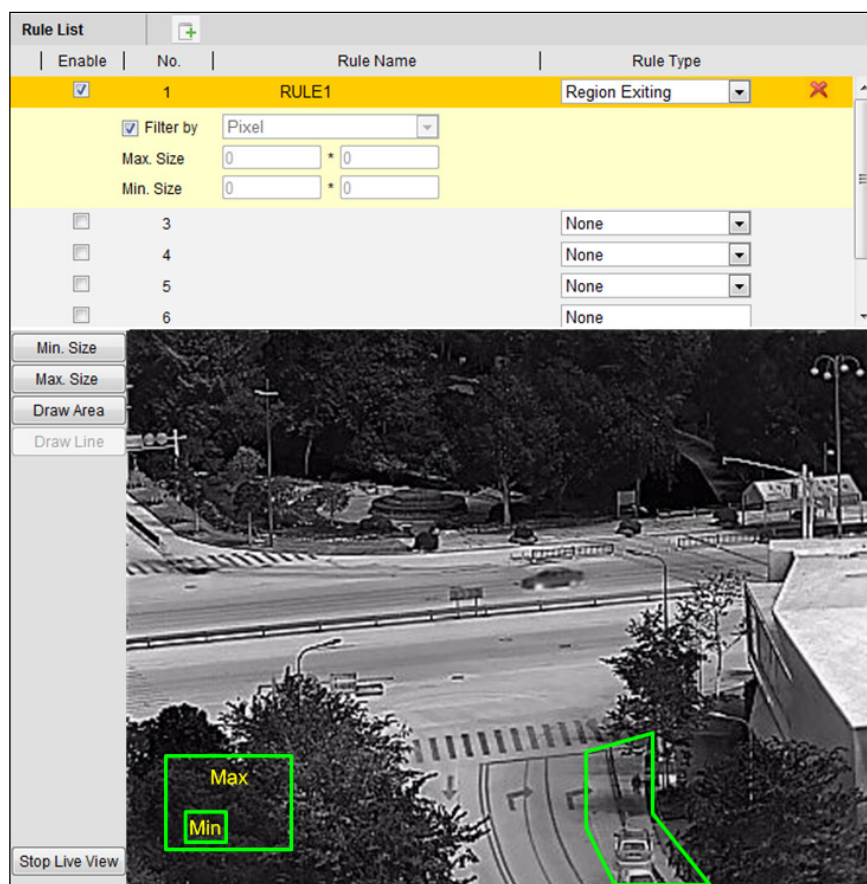


Rysunek 5–52 typ reguły - przekroczenie linii



Rysunek 5–53 typ reguły - wtargnięcie

- Funkcja **Region Entrance** wykrywa osoby, pojazdy lub inne obiekty, które wkraczą na wstępnie zdefiniowany obszar wirtualny z lokalizacji zewnętrznej. Po wyzwoleniu alarmu mogą być wykonywane różne działania.
- Funkcja **Region Exiting** wykrywa osoby, pojazdy lub inne obiekty, które opuszczają wstępnie zdefiniowany obszar wirtualny. Po wyzwoleniu alarmu mogą być wykonywane różne działania.



Rysunek 5–54 Typ reguły - wyjście z obszaru

- **Filter type:** Do wyboru dostępne są opcje Pixels i Actual Size. Jeśli wybrana została opcja Pixels, narysuj obszar o rozmiarze maksymalnym i rozmiarze minimalnym na obrazie wideo na żywo dla każdej reguły. Jeżeli wybrano ustawienie Actual Size, wprowadź 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.

Uwaga: Należy upewnić się, że kalibracja kamery została skonfigurowana, jeżeli wybrano rozmiar rzeczywisty.

- **Draw line/area:** W przypadku innych zdarzeń takich jak wtargnięcie, wejście w obszar, wyjście z obszaru należy kliknąć lewym przyciskiem myszy obraz wideo na żywo, aby ustawić punkty końcowe obszaru, a następnie kliknąć prawym przyciskiem myszy, aby zakończyć rysowanie obszaru.

Uwaga: Jeżeli podgląd na żywo zostanie zatrzymany, nie można wyznaczyć obszaru/linii detekcji i nie można konfigurować reguł.

- 5) Zaznacz pole wyboru połączonej reguły, aby uwzględnić ją w analizie zachowań.
- 6) Wybierz dwie skonfigurowane pojedyncze reguły jako Regułę A i Regułę B reguły połączonej, ustaw minimalny i maksymalny przedział czasowy dla tych dwóch pojedynczych reguł, a następnie wybierz kolejność ich wyzwalania dla funkcji filtrowania alarmów.

Uwagi:

- Jeśli w pozycji rule type wybierzesz opcję None, reguła będzie nieważna i nie będzie można skonfigurować analizy zachowania.
 - Kolejność wyzwalania pojedynczej reguły dla filtrowania alarmów można ustawić rosnąco lub rosnąco/malejąco.
 - Można skonfigurować maksymalnie osiem pojedynczych reguł i dwie reguły połączone. W przypadku reguł połączonych obsługiwana jest detekcja przekroczenia linii, wtargnięcia, opuszczenia obszaru i wejścia w obszar.
- 7) Kliknij przycisk **Save**, aby zapisać ustawienia.
 - 8) Kliknij kartę **Arming Schedule**, kliknij przycisk **Edit**, aby ustawić czas harmonogramu dla każdej reguły, a następnie kliknij przycisk **Save**, aby zapisać ustawienia.
 - 9) Kliknij kartę **Alarm Linkage**, a następnie dla każdej reguły zaznacz pole wyboru odpowiedniej metody powiązania i kliknij przycisk **Save**, aby zapisać ustawienia.

5. Ustaw konfigurację zaawansowaną

• Parametry

Skonfiguruj następujące parametry, aby szczegółowo określić konfigurację.

Rysunek 5–55 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 2.

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.

Leave Interference Suppression: Zaznacz to pole wyboru, aby wyeliminować zakłócenia powodowane przez liście w skonfigurowanym obszarze.

Output Type: Wybierz położenie ramki. Do wyboru dostępne są następujące opcje: środek celu, dolna część celu i górna część celu. Np.: Po wybraniu opcji środek celu, cel będzie znajdować się w środku ramki.

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

Restart VCA: Ponowne uruchomienie biblioteki algorytmów analizy zachowań.

- Globalny filtr rozmiarów

Uwaga: W porównaniu z filtrem rozmiaru dla reguły, który ma zastosowanie dla każdej reguły z osobna, globalny filtr rozmiarów ma zastosowanie dla wszystkich reguł.

Kroki:

- 1) Zaznacz pole wyboru **Global Size Filter**, aby włączyć tę funkcję.
- 2) W pozycji Filter Type wybierz opcję Actual Size lub Pixel.

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.
- 3) Kliknij przycisk **Save**, aby zapisać ustawienia.

Rozdział 6 Ustawienia magazynowania nagrań i zdjęć

Zanim rozpoczniesz:

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

6.1 Zarządzanie magazynem

Zarządzanie magazynem umożliwia wyświetlanie stanu dysku twardego, w tym pojemności, miejsca wolnego, stanu, typu i postępu. Jeśli jest to konieczne, można również sformatować dysk twardy. Ponadto można przypisać plikom zdjęć i nagrań limit przydziału.

Uwaga: Zanim będzie można zarządzać dyskami twardymi należy najpierw je dodać.

Aby dodać twardy dysk, włóż kartę SD lub patrz następny Rozdział.

The screenshot shows the 'Storage Management' tab in a web interface. It contains two main sections: 'HDD Device List' and 'Quota'.

HDD Device List: A table with columns: HDD No., Capacity, Free space, Status, Type, Property, and Progress. There is a 'Format' button to the right of the table.

HDD No.	Capacity	Free space	Status	Type	Property	Progress
9	20.00GB	0.00GB	Uninitialized	NAS	R/W	

Quota: A section with input fields for various capacity and percentage settings.

Max. Picture Capacity	0.00GB
Free Size for Picture	0GB
Max. Record Capacity	0.00GB
Free Size for Record	0GB
Percentage of Picture	25%
Percentage of Record	75%

Rysunek 6–1 Interfejs zarządzania magazynem

6.2 Konfigurowanie ustawień NAS

Zanim rozpoczniesz:

Aby móc zapisywać pliki nagrań, rejestru itp. na sieciowym dysku twardym, musi on

być podłączony do sieci i odpowiednio skonfigurowany.

Kroki:

1. Dodawanie dysku sieciowego

- (1) Przejdź do interfejsu ustawień urządzeń magazynujących dołączonych do sieci (Network-Attached Storage – NAS), wybierając opcje:

Configuration > Advanced Configuration > Storage > NAS

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

User Name: Password:

Rysunek 6–2 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: Szczegółowe informacje na temat tworzenia ścieżki pliku znajdują się w instrukcji użytkownika dysku NAS.



- Aby zapewnić ochronę prywatności i systemu przed zagrożeniami bezpieczeństwa, zdecydowanie zalecamy używanie silnych haseł dla wszystkich funkcji i urządzeń sieciowych. Aby zwiększyć bezpieczeństwo urządzenia, należy ustawić własne hasło (składającego się z minimum 8 znaków, w tym wielkich liter, małych liter, cyfr i znaków specjalnych).
- 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 dysków twardych

Advanced Configuration > Storage > Storage Management

The screenshot shows the 'Storage Management' tab in the 'Advanced Configuration > Storage' section. It features a 'HDD Device List' table and a 'Quota' section with various input fields.

HDD Device List							Format
<input type="checkbox"/>	HDD No.	Capacity	Free space	Status	Type	Property	Progress
<input type="checkbox"/>	9	20.00GB	0.00GB	Uninitialized	NAS	R/W	

Quota

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

Rysunek 6–3 Interfejs zarządzania 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**“.

This screenshot shows the 'HDD Device List' table after the disk has been formatted. The status is now 'Normal' and the free space is 19.75GB.

HDD Device List							Format
<input type="checkbox"/>	HDD No.	Capacity	Free space	Status	Type	Property	Progress
<input type="checkbox"/>	9	20.00GB	19.75GB	Normal	NAS	R/W	

Rysunek 6–4 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.

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

Rysunek 6–5 Ustawienia przydziału

Uwagi:

- Do kamery można przyłączyć do 8 dysków NAS.
- Aby zainicjować kartę SD i korzystać z niej, po jej włożeniu do kamery, należy zapoznać się z krokami inicjowania dysku NAS.

6.3 Konfigurowanie harmonogramu nagrywania

Cel:

Dostępne są dwa tryby nagrywania dla kamer: ręczne i zaplanowane. Informacje na temat nagrywania ręcznego znajdują się w *Rozdziale 4.3 Ręczne nagrywanie i wykonywanie zdjęć*. W tym rozdziale zamieszczono instrukcje dotyczące konfiguracji nagrywania według harmonogramu. Pliki zarejestrowane w trybie nagrywania według harmonogramu są domyślnie zapisywane na karcie SD (jeśli jest ona obsługiwana) lub na dysku sieciowym.

Kroki:

1. Przejdź do interfejsu ustawień harmonogramu nagrywania, wybierając opcje:

Configuration > Advanced Configuration > Storage > Record Schedule

Record Schedule | Storage Management | NAS | Snapshot

Channel No.

Pre-record

Post-record

Overwrite

Recording Stream

☒ Enable Record Schedule

	0	2	4	6	8	10	12	14	16	18	20	22	24
Mon	[Grid with colored cells]												
Tue	[Grid with colored cells]												
Wed	[Grid with colored cells]												
Thu	[Grid with colored cells]												
Fri	[Grid with colored cells]												
Sat	[Grid with colored cells]												
Sun	[Grid with colored cells]												

☐ Continuous
☐ Motion Detection
☐ Alarm
☐ Motion | Alarm
☐ Motion & Alarm
☐ Other

Rysunek 6–6 Harmonogram nagrywania

- Zaznacz pole wyboru **Enable Record Schedule**, aby włączyć planowane nagrywanie.
- Ustaw parametry nagrywania kamery.

Pre-record

Post-record

Overwrite

Recording Stream

Rysunek 6–7 Parametry nagrywania

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

Można skonfigurować czas poprzedzający nagrywanie, wybierając jedną z następujących opcji: brak nagrywania wstępnego, 5 s, 10 s, 15 s, 20 s, 25 s, 30 s lub bez ograniczeń.

- **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.

W pozycji czasu po rozpoczęciu nagrania można wybrać jedną z wartości: 5 s, 10 s, 30 s, 1 min, 2 min, 5 min lub 10 min.

- **Recording Stream:** Można wybrać strumień główny lub podstrumień. Strumień główny jest zwykle używany do nagrywania i wyświetlania na żywo przy dobrej przepustowości sieci, a podstrumienia i trzeciego strumienia można używać do wyświetlania na żywo, gdy przepustowość sieci jest ograniczona.

Uwaga: Konfiguracje parametrów nagrywania są zależne od modelu kamery.

4. Kliknij przycisk **Edit**, aby edytować harmonogram nagrywania.

Edit Schedule

☒ All Day ☐ Custom

Continuous

Period	Start Time	End Time	Record Type
1	00:00	08:00	Fire Source Detec
2	08:00	14:00	Alarm
3	14:00	20:00	Continuous
4	20:00	24:00	Motion Alarm
5	00:00	00:00	Continuous
6	00:00	00:00	Continuous
7	00:00	00:00	Continuous
8	00:00	00:00	Continuous

Copy to Week ☒ Select All

☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☒ Sat ☒ Sun

Copy

OK Cancel

Rysunek 6–8 Edytowanie harmonogramu nagrywania

5. Wybierz dzień, aby ustawić harmonogram nagrywania.

(1) Ustaw nagrywanie całonocne lub nagrywanie segmentu:

- Jeśli chcesz skonfigurować nagrywanie całonocne, zaznacz pole wyboru **All Day**.
- Jeśli chcesz nagrywać o różnych porach, zaznacz pole wyboru **Custom**.
Ustaw parametry **Start Time** i **End Time**.

Uwaga: Czasy odpowiednich segmentów nie mogą na siebie nachodzić.

Można skonfigurować maks. 8 segmentów.

(2) Wybierz **Typ Nagrywania**.

W pozycji typu nagrania można wybrać następujące opcje: nagrywanie ciągłe, detekcja ruchu, alarm, ruch lub alarm, ruchu i alarm, detekcja nietypowego dźwięku, nagrywanie VCA, detekcja źródła ognia i wszystkie zdarzenia.

- **Nieprzerwane**

Jeśli wybierzesz opcję nagrywania ciągłego **Continuous**, obraz wideo będzie nagrywany automatycznie według czasu ustawionego w harmonogramie.

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

Jeśli wybierzesz opcję **Motion Detection**, obraz wideo będzie nagrywany po detekcji ruchu.

Aby móc skorzystać z tej funkcji, oprócz harmonogramu nagrywania należy także ustawić obszar detekcji ruchu i zaznaczyć pole „**Trigger Channel**” w zakładce „**Linkage Method**” w interfejsie ustawień detekcji ruchu. Aby uzyskać więcej informacji, zobacz ***Zadanie 1: Ustawianie obszaru detekcji ruchu*** w *Rozdziale 5.6.1*.

- **Nagrywanie wyzwalane przez alarm**

Jeśli wybierzesz opcję alarmu **Alarm**, obraz wideo będzie nagrywany po wyzwoleniu alarmu przez zewnętrzne kanały wejścia alarmu.

Oprócz konfigurowania harmonogramu nagrywania, należy ustawić typ alarmu w pozycji **Typ Alarmu** i zaznaczyć pole wyboru **Trigger Channel** w pozycji **Linkage Method** na interfejsie **Ustawienia wejścia alarmu**. Aby uzyskać szczegółowe informacje, patrz *Rozdział 5.6.3*.

- **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 5.6.1* i *Rozdział 5.6.3*.

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

Jeśli wybrano opcję „**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 5.6.1* i *Rozdział 5.6.3*.

- **Nagranie wywołane detekcją nietypowego dźwięku**

Jeśli wybierzesz opcję **Audio Exception Detection**, obraz wideo będzie nagrywany po wykryciu na monitorowanej scenie nietypowych dźwięków takich jak nagłe zwiększenie/zmniejszenie natężenia dźwięku.

Aby móc skorzystać z tej funkcji, oprócz harmonogramu nagrywania należy także skonfigurować ustawienia w interfejsie **Detekcji Nietypowego Sygnału Audio**. Aby uzyskać szczegółowe informacje, patrz *Rozdział 5.6.6*.

- **Nagranie wywołane nagraniem VCA**

Jeśli wybierzesz opcję **VCA Recording**, obraz wideo będzie nagrywany po wykryciu przez VCA podejrzanych zachowań takich jak przekroczenie linii, wtargnięcie, wejście w obszar czy wyjście z obszaru.

Oprócz konfigurowania harmonogramu nagrywania należy skonfigurować ustawienie reguły na interfejsie konfiguracji VCA. Aby uzyskać szczegółowe informacje, patrz *Rozdział 5.7.2*.

- **Nagranie wywołane przez detekcję źródła ognia**

Jeśli wybierzesz opcję **Fire Source Detection**, obraz wideo będzie nagrywany po wykryciu źródła ognia.

Oprócz konfigurowania harmonogramu nagrywania należy skonfigurować ustawienia w interfejsie **Dynamic Fire Source Detection**. Aby uzyskać szczegółowe informacje, patrz *Rozdział 5.6.7*.

- **Nagranie wywołane wszystkimi zdarzeniami**

Jeśli wybierzesz opcję **All Events**, obraz wideo będzie nagrywany po zajściu któregośkolwiek z wymienionych zdarzeń.

Oprócz konfigurowania harmonogramu nagrywania należy skonfigurować ustawienia w interfejsach odpowiednich zdarzeń.

(3) (Opcjonalnie) Zaznacz pole wyboru **Select All** i kliknij przycisk **Copy**, aby skopiować ustawienia tego dnia na cały tydzień. Można również zaznaczyć pola wyboru przed tą datą, a następnie kliknąć przycisk **Copy**.

(4) Kliknij przycisk **OK**, aby zapisać ustawienia i wyjść z interfejsu **Edit Record Schedule**.

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

6.4 Konfigurowanie ustawień wykonywania zdjęć

Cel:

Możesz skonfigurować wykonywanie zdjęć według harmonogramu i wykonywanie zdjęć wyzwolone przez zdarzenia. Wykonane zdjęcie może być przechowywane na karcie SD (jeśli jest obsługiwana) lub na serwerze NAS (szczegółowe informacje znajdują się w *Rozdziale 6.2 Konfigurowanie ustawień NAS*). Można również przesyłać wykonane zdjęcia na serwer FTP.

Ustawienia podstawowe

Kroki:

1. Przejdź do interfejsu ustawień wykonywania zdjęć, wybierając opcje:

Configuration > Advanced Configuration > Storage > Snapshot

The screenshot shows the 'Snapshot' configuration page. At the top, there are tabs: 'Record Schedule', 'Storage Management', 'NAS', and 'Snapshot' (which is active). The 'Timing' section includes a checked 'Enable Timing Snapshot' checkbox. Below it are dropdown menus for 'Format' (set to JPEG), 'Resolution' (set to 640*512), and 'Quality' (set to High). An 'Interval' field is set to 0 with a unit dropdown set to 'millisecond'. An 'Edit' button is located to the right of the interval field. Below the timing settings is a 7x24 grid for scheduling snapshots by day of the week (Mon to Sun) and hour (0 to 24). The 'Event-Triggered' section includes an unchecked 'Enable Event-Triggered Snapshot' checkbox. Below it are dropdown menus for 'Format' (set to JPEG), 'Resolution' (set to 640*512), and 'Quality' (set to High). An 'Interval' field is set to 0 with a unit dropdown set to 'millisecond'. A 'Capture Number' field is set to 4.

Rysunek 6–9 Interfejs ustawiania wykonywania zdjęć

2. Wybierz numer kanału. W przypadku modeli kamer, które mają więcej niż jeden kanał kamery, należy najpierw wybrać numer kanału do skonfigurowania.
3. Zaznacz pole wyboru **Enable Timing Snapshot**, aby włączyć tryb ciągłego wykonywania zdjęć.
Edytuj czas harmonogramu dla wykonywania zdjęć. Szczegółowe instrukcje dotyczące ustawiania można znaleźć w **Rozdziale 6.3 Konfigurowanie harmonogramu nagrywania**.
4. Zaznacz pole wyboru „**Enable Event-triggered Snapshot**“, aby włączyć wykonywanie zdjęć w momencie wystąpienia zdarzenia.
5. Wybierz format, rozdzielczość i jakość wykonywanych zdjęć.
6. Ustaw odstęp czasowy pomiędzy wykonywaniem zdjęć.
7. Kliknij przycisk **Save**, aby zapisać ustawienia.

Przesyłanie zdjęć na serwer FTP

Aby przesłać zdjęcia na serwer FTP, należy postępować zgodnie z poniższymi instrukcjami dotyczącymi konfiguracji.

- Nieprzerwane przesyłanie zdjęć na serwer FTP

Kroki:

- 1) Skonfiguruj serwer FTP w interfejsie ustawień serwera FTP oraz zaznacz pole wyboru „**Upload Picture**“. Aby uzyskać szczegółowe informacje na temat konfigurowania parametrów FTP, patrz **Rozdział 5.3.11 Konfigurowanie ustawień serwera FTP**.
- 2) Zaznacz pole wyboru „**Enable Timing Snapshot**“.

- Przesyłanie na serwer FTP zdjęć wyzwolonych przez zdarzenie

Kroki:

- 1) Skonfiguruj serwer FTP w interfejsie ustawień serwera FTP oraz zaznacz pole wyboru „**Upload Picture**“. Aby uzyskać szczegółowe informacje na temat konfigurowania parametrów FTP, patrz **Rozdział 5.3.11 Konfigurowanie ustawień serwera FTP**.
- 2) Sprawdź pole wyboru **Upload Picture** w interfejsie ustawień detekcji ruchu lub wejścia alarmu. Zobacz **Zadanie 3: Ustawianie działań alarmowych podejmowanych w celu detekcji ruchu** w **Rozdziale 5.6.1**,
- 3) Zaznacz pole wyboru „**Enable Event-triggered Snapshot**“.

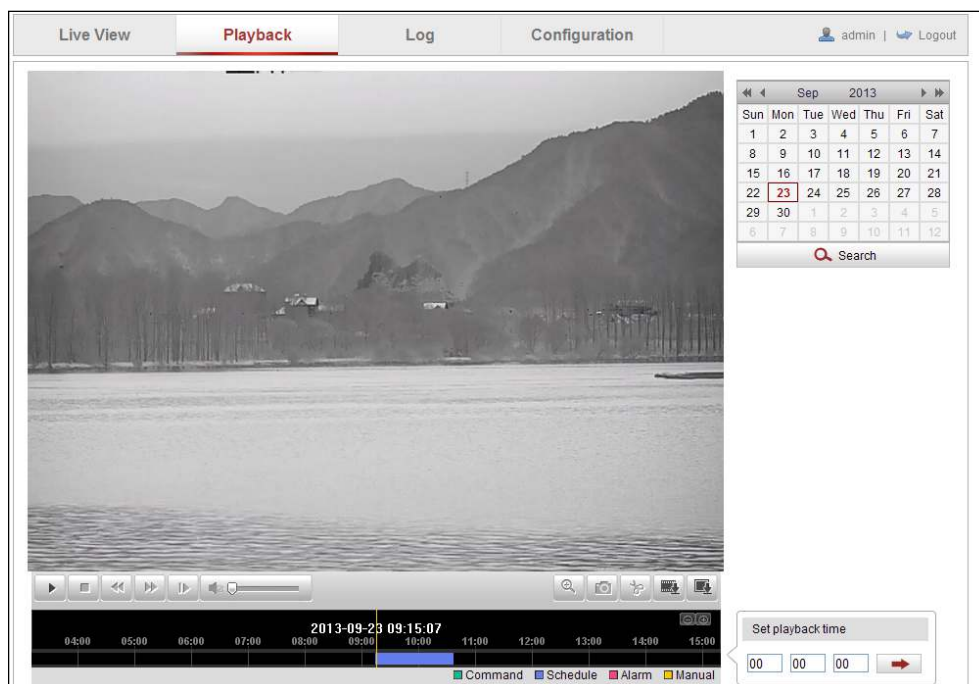
Rozdział 7 Odtwarzanie

Cel:

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

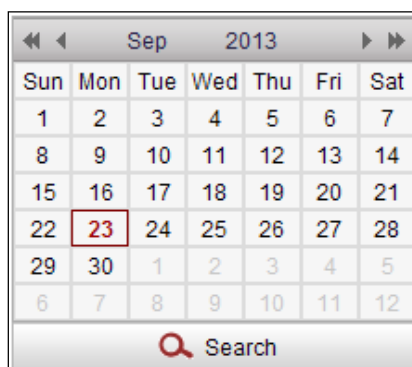
Kroki:

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




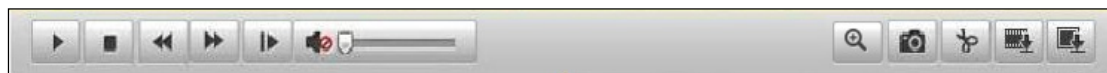
Rysunek 7–1 Interfejs odtwarzania

2. Wybierz datę i kliknij przycisk **Search**, aby wyszukać pliki nagrań.



Rysunek 7–2 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 7-3 Pasek narzędzi odtwarzania

Tabela 7-1 Opis przycisków

Ikona	Opis	Ikona	Opis
	Odtwarzanie		Rejestrowanie zdjęć
	Wstrzymanie		Rozpoczęcie/zakończenie przycinania plików wideo
	Zatrzymanie		Włączanie dźwięku i regulacja głośności/wyciszenie.
	Zmniejszenie szybkości		Pobieranie plików wideo
	Zwiększenie szybkości		Pobieranie wykonanych zdjęć
	Odtwarzanie poklatkowe		Włączanie/wyłączanie powiększenia cyfrowego

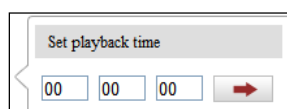
Uwaga: Lokalne ścieżki zapisu pobranych plików wideo i zdjęć można ustawić w interfejsie konfiguracji lokalnej. Aby uzyskać szczegółowe informacje, patrz *Rozdział 5.1*.

- Aby wybrać punkt, od którego ma się rozpocząć odtwarzanie, przeciągnij za pomocą myszy suwak na pasku postępu. Można także wprowadzić czas i kliknąć przycisk

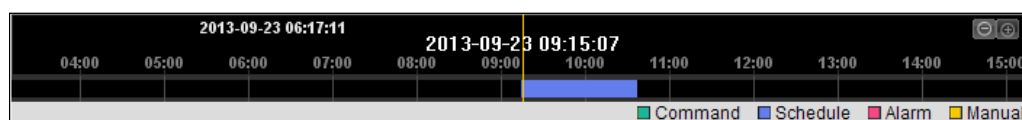


, aby zlokalizować punkt odtwarzania ustawiony w polu „**Set playback time**“.

Kliknij przyciski , aby powiększyć/pomniejszyć pasek postępu.

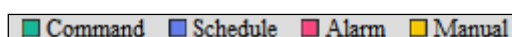


Rysunek 7-4 Ustawianie czasu odtwarzania



Rysunek 7-5 Pasek postępu

Typy wideo wyróżniono różnymi kolorami na pasku postępu.



Rysunek 7-6 Typy wideo

Rozdział 8 Wyszukiwanie w rejestrze

Cel:

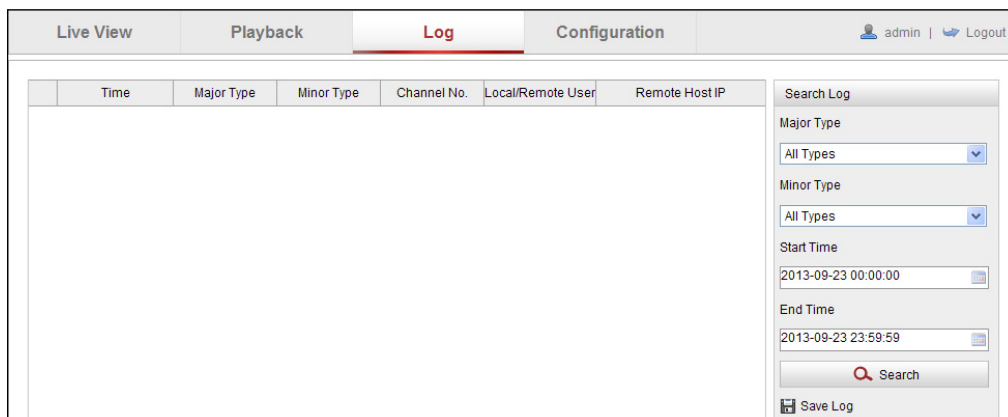
Operacje, alarmy, wyjątki i informacje dotyczące kamery można zapisywać w plikach rejestru. W razie potrzeby pliki rejestru można eksportować.

Zanim rozpoczniesz:

Upewnij się, że skonfigurowany jest magazyn sieciowy kamery lub uruchomiony jest magazyn lokalny (karta SD).

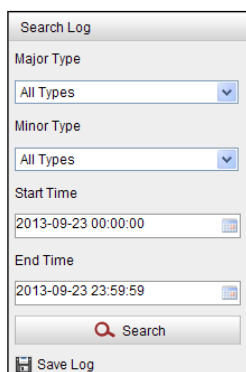
Kroki:

1. Kliknij przycisk **Log** na pasku menu, aby przejść do interfejsu wyszukiwania rejestru.



Rysunek 8–1 Interfejs wyszukiwania w rejestrze

2. Skonfiguruj kryteria wyszukiwania w rejestrze, takie jak Typ główny, Typ podrzędny, Godzina rozpoczęcia i Godzina zakończenia.
3. Kliknij przycisk **Search**, aby rozpocząć wyszukiwanie w plikach rejestru. Pliki rejestru odpowiadające kryteriom wyszukiwania zostaną wyświetlone w interfejsie rejestru („Log“).



Search Log

Major Type
All Types

Minor Type
All Types

Start Time
2013-09-23 00:00:00

End Time
2013-09-23 23:59:59

Search

Save Log

Rysunek 8–2 Wyszukiwanie w rejestrze

4. Aby wyeksportować pliki rejestrów, kliknij przycisk **Save log**, aby zapisać pliki rejestrów na komputerze.

Rozdział 9 Inne ustawienia

9.1 Zarządzanie kontami użytkowników

Cel:

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

Przejdź do interfejsu zarządzania użytkownikami, aby zapisać ustawienia:

Configuration > Basic Configuration > Security > User lub **Configuration > Advanced Configuration > Security > User**

User

Authentication

Anonymous Visit

IP Address Filter

Security Service

Add

Modify

Delete

No.	User Name	Level
1	admin	Administrator
2	Test	Operator

Rysunek 9–1 Informacje o użytkowniku

- **Dodawanie użytkownika**

Administrator ma domyślnie wszelkie uprawnienia do tworzenia, modyfikowania i usuwania innych kont.

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

Kroki:

1. Kliknij przycisk **Add**, aby dodać użytkownika.
2. Wprowadź **nazwę użytkownika**, wybierz poziom **Level** i wprowadź **hasło**.

Uwagi:

- Można utworzyć do 31 kont użytkowników.
- Użytkownicy na różnym poziomie mają różne uprawnienia. Dostępne są ustawienia Operator i Użytkownik.



- W celu zapewnienia prywatności użytkownika i lepszej ochrony systemu przed zagrożeniami bezpieczeństwa zalecamy używanie silnych haseł w przypadku wszystkich funkcji i urządzeń sieciowych. Aby zapewnić lepszą ochronę produktu, hasło powinno zawierać unikatowy ciąg znaków (minimum 8 znaków z uwzględnieniem wielkich i małych liter, cyfr oraz znaków specjalnych).
 - Prawidłowa konfiguracja wszystkich haseł i innych ustawień bezpieczeństwa należy do obowiązków osoby instalującej lub użytkownika końcowego.
3. W polu „**Basic Permission**“ oraz w polu „**Camera Configuration**“ można zaznaczyć lub odznaczyć uprawnienia nowego użytkownika.
 4. Kliknij przycisk **OK**, aby ukończyć dodawanie użytkownika.

Add user

User Name: test1

Level: Operator

Password: [masked]

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

Confirm: [masked]

Basic Permission	Camera Configuration
<input type="checkbox"/> Remote: Parameters Settings	Remote: Live View Select All <input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Remote: Log Search / Interrogate Working Status	<input checked="" type="checkbox"/> D1 <input checked="" type="checkbox"/> D2
<input type="checkbox"/> Remote: Upgrade / Format	<input checked="" type="checkbox"/> Remote: PTZ Control
<input checked="" type="checkbox"/> Remote: Two-way Audio	Remote: Manual Record Select All <input checked="" type="checkbox"/>
<input type="checkbox"/> Remote: Shutdown / Reboot	<input checked="" type="checkbox"/> D1 <input checked="" type="checkbox"/> D2
<input type="checkbox"/> Remote: Notify Surveillance Center / Trigger Alarm Output	Remote: Playback Select All <input checked="" type="checkbox"/>
<input type="checkbox"/> Remote: Video Output Control	<input checked="" type="checkbox"/> D1 <input checked="" type="checkbox"/> D2
<input type="checkbox"/> Remote: Serial Port Control	

OK Cancel

Rysunek 9–2 Dodawanie użytkownika

- **Modyfikowanie użytkownika**

Kroki:

1. Kliknij lewym przyciskiem myszy, aby wybrać użytkownika z listy, a następnie kliknij przycisk **Modify**.
2. Zmodyfikuj pozycję **User Name**, **Level** lub **Password**.
3. W polu (**Uprawnienia podstawowe**) oraz w polu (**Konfiguracja kamery**) można zaznaczyć lub odznaczyć uprawnienia.
4. Kliknij przycisk **OK**, aby ukończyć modyfikowanie użytkownika.

Modify user

User Name: test1

Level: Operator

Password: •••••

Confirm: •••••

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

Basic Permission	Camera Configuration
<input type="checkbox"/> Remote: Parameters Settings	Remote: Live View Select All <input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Remote: Log Search / Interrogate Working Status	<input checked="" type="checkbox"/> D1 <input checked="" type="checkbox"/> D2
<input type="checkbox"/> Remote: Upgrade / Format	<input checked="" type="checkbox"/> Remote: PTZ Control
<input checked="" type="checkbox"/> Remote: Two-way Audio	Remote: Manual Record Select All <input checked="" type="checkbox"/>
<input type="checkbox"/> Remote: Shutdown / Reboot	<input checked="" type="checkbox"/> D1 <input checked="" type="checkbox"/> D2
<input type="checkbox"/> Remote: Notify Surveillance Center / Trigger Alarm Output	Remote: Playback Select All <input checked="" type="checkbox"/>
<input type="checkbox"/> Remote: Video Output Control	<input checked="" type="checkbox"/> D1 <input checked="" type="checkbox"/> D2
<input type="checkbox"/> Remote: Serial Port Control	

OK Cancel

Rysunek 9–3 Modyfikowanie użytkownika

- **Usuwanie użytkownika**

Kroki:

1. Wybierz użytkownika, którego chcesz usunąć, a następnie kliknij przycisk **Delete**.
2. Kliknij przycisk **OK** w wyświetlonym oknie dialogowym, aby usunąć użytkownika.

9.2 Uwierzytelnianie

Cel:

Funkcja ta służy do ochrony danych strumienia podglądu na żywo.

Kroki:

1. Przejdź do interfejsu Authentication:

Configuration > Advanced Configuration > Security > Authentication



The screenshot shows a web interface for configuring security settings. At the top, there are five tabs: 'User', 'Authentication' (highlighted in red), 'Anonymous Visit', 'IP Address Filter', and 'Security Service'. Below the tabs, there is a section for 'RTSP Authentication' with a dropdown menu currently showing 'basic'. At the bottom right of the configuration area, there is a 'Save' button.

Rysunek 9–4 Uwierzytelnianie RTSP

2. W pozycji **RTSP Authentication** wybierz typ podstawowy **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.

9.3 Użytkownik anonimowy

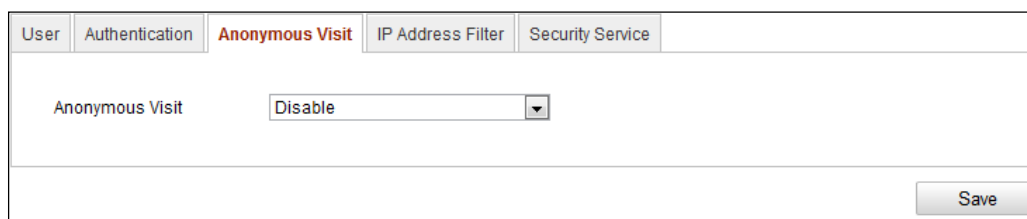
Włączenie tej funkcji umożliwia wizyty gości, którzy nie mają nazwy użytkownika lub hasła urządzenia.

Uwaga: Użytkownicy anonimowi mają dostęp tylko do podglądu na żywo.

Kroki:

1. Przejdź do interfejsu Anonymous Visit:

Configuration > Advanced Configuration > Security > Anonymous Visit

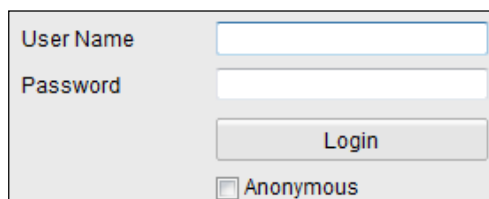


The screenshot shows a web interface for configuring security settings. At the top, there are five tabs: 'User', 'Authentication', 'Anonymous Visit' (highlighted in red), 'IP Address Filter', and 'Security Service'. Below the tabs, there is a section for 'Anonymous Visit' with a dropdown menu currently showing 'Disable'. At the bottom right of the configuration area, there is a 'Save' button.

Rysunek 9–5 Użytkownik anonimowy

2. W pozycji **Anonymous Visit** wybierz opcję **Enable** lub **Disable** z listy rozwijanej, aby włączyć lub wyłączyć dostęp dla użytkownika anonimowego.
3. Kliknij przycisk **Save**, aby zapisać ustawienia.

Podczas następnego logowania pojawi się pole wyboru użytkownika anonimowego.



The image shows a login form with a light gray background. It contains two text input fields: the first is labeled 'User Name' and the second is labeled 'Password'. Below these fields is a button labeled 'Login'. At the bottom of the form is a checkbox labeled 'Anonymous'.

Rysunek 9–6 Interfejs logowania z opcją logowania anonimowego

4. Zaznacz pole wyboru **Anonymous** i kliknij przycisk **Login**.

Udostępnianie funkcji anonimowego podglądu na żywo może dać innym osobom dostęp do kamery i obrazu podglądu na żywo bez potwierdzenia danych logowania. Dlatego przed włączeniem opcji anonimowego dostępu do podglądu na żywo jest niezwykle istotne, aby upewnić się, iż pole widzenia kamery nie obejmuje przestrzeni prywatnej osób, które nie wyraziły zgody na filmowanie.

Ponieważ monitoring wideo może naruszać prywatność, nie należy stosować go w obszarach o zwiększonych wymaganiach dotyczących ochrony prywatności.

9.4 Filtr adresów IP

Cel:

Ta funkcja umożliwia kontrolę dostępu.

Kroki:

1. Przejdź do interfejsu IP Address Filter:

Configuration > Advanced Configuration > Security > IP Address Filter

Rysunek 9–7 Filtr adresów IP

2. Zaznacz pole wyboru „**Enable IP Address Filter**“.
3. Wybierz typ filtru adresu IP z listy rozwijanej. Do wyboru dostępne są opcje **Forbidden** i **Allowed**.
4. Ustaw listę filtrowanych adresów IP.
 - Dodawanie adresu IP

Kroki:

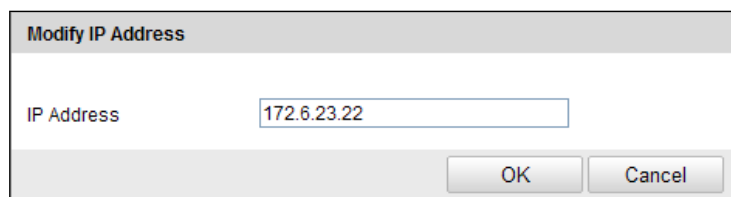
- (1) Kliknij przycisk **Add**, aby dodać adres IP.
- (2) Wprowadź adres IP.

Rysunek 9–8 Dodawanie adresu IP

- (3) Kliknij przycisk „**OK**“, aby zakończyć dodawanie.
- Modyfikowanie adresu IP

Kroki:

 - (1) Kliknij lewym przyciskiem myszy adres IP z listy filtrów, a następnie kliknij przycisk **Modify**.
 - (2) Zmień adres IP znajdujący się w polu tekstowym.



Rysunek 9–9 Modyfikowanie adresu IP

(3) Kliknij przycisk „**OK**“, aby zakończyć modyfikowanie.

- Usuwanie adresu IP

Kliknij lewym przyciskiem myszy adres IP z listy filtrów, a następnie kliknij przycisk **Delete**.

- Usuwanie wszystkich adresów IP

Kliknij przycisk **Clear**, aby usunąć wszystkie adresy IP.

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


9.5 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 > Advanced configuration > Security > Security Service



Rysunek 9–10 Usługa zabezpieczeń

2. Zaznacz pole wyboru **Enable SSH**, aby włączyć zabezpieczenia komunikacji danych, lub odznacz pole wyboru, aby wyłączyć SSH.
3. Zaznacz pole wyboru **Enable Illegal Login Lock**, a następnie urządzenie zostanie zablokowane, jeśli nazwa użytkownika lub hasło zostanie wprowadzone niepoprawnie 5 razy pod rząd.

Uwaga: Jeśli urządzenie jest zablokowane, można spróbować zalogować się po upływie 30 minut lub uruchomić urządzenie ponownie przed kolejną próbą.

9.6 Wyświetlanie informacji o urządzeniu

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

W interfejsie **Device Information** można edytować nazwę urządzenia.

Wyświetlane są inne informacje o kamerze sieciowej takie jak jej model, numer seryjny, wersja oprogramowania sprzętowego, wersji kodowania, liczba kanałów, liczba dysków twardych, numer wejścia alarmu i numer wyjścia alarmu. 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	
Device Name	THERMAL CAMERA
Device No.	88
Model	
Serial No.	
Firmware Version	V5.3.7 build 160711
Encoding Version	V7.3 build 160621
Number of Channels	1
Number of HDDs	0
Number of Alarm Input	2
Number of Alarm Output	2

Rysunek 9–11 Informacje o urządzeniu

9.7 Konserwacja

9.7.1 Ponowne uruchamianie kamery

Kroki:

1. Przejdź do interfejsu Maintenance:

Configuration > Basic Configuration > System > Maintenance

Lub **Configuration > Advanced Configuration > System > Maintenance**

2. Kliknij przycisk **Reboot**, aby uruchomić ponownie kamerę sieciową.



Rysunek 9–12 Ponowne uruchomienie urządzenia

9.7.2 Przywracanie ustawień domyślnych

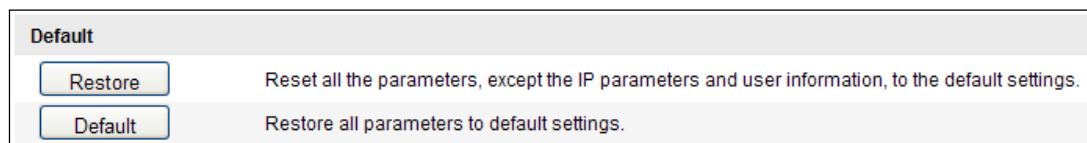
Kroki:

1. Przejdź do interfejsu Maintenance:

Configuration > Basic Configuration > System > Maintenance

Lub **Configuration > Advanced Configuration > System > Maintenance**

2. Kliknij przycisk **Restore** lub **Default**, aby przywrócić ustawienia domyślne.



Rysunek 9–13 Przywracanie ustawień domyślnych

Uwaga: Po przywróceniu ustawień domyślnych, adres IP jest również przywracany do wartości domyślnej, w związku z czym należy korzystać z tej funkcji w sposób rozważny.

9.7.3 Eksportowanie/importowanie pliku konfiguracji

Cel:

Plik konfiguracji jest używany do zbiorczego konfigurowania kamer, co może uprościć procedurę konfiguracji, w przypadku gdy konieczne jest skonfigurowanie wielu kamer.

Kroki:

1. Przejdź do interfejsu Maintenance:

Configuration > Basic Configuration > System > Maintenance

lub **Configuration > Advanced Configuration > System > Maintenance**

2. Kliknij przycisk **Export**, aby wyeksportować bieżący plik konfiguracji, a następnie zapisz go w odpowiednim miejscu.
3. Kliknij przycisk **Browse**, aby wybrać zapisany plik konfiguracji, a następnie kliknij przycisk **Import**, aby uruchomić importowanie pliku konfiguracji.

Uwaga: Po zaimportowaniu pliku konfiguracyjnego należy ponownie uruchomić kamerę.

4. Kliknij przycisk **Export** i ustaw ścieżkę zapisu, aby zapisać plik konfiguracji w magazynie lokalnym.

The screenshot shows a web interface for configuration management. It is divided into two main sections: 'Import Config. File' and 'Export Config. File'. In the 'Import' section, there is a text input field labeled 'Config File' containing the path 'F:\12'. To the right of this field are two buttons: 'Browse' and 'Import'. Below the input field is a 'Status' label. The 'Export Config. File' section is below the import section and contains a single 'Export' button.

Rysunek 9–14 Importowanie/eksportowanie pliku konfiguracji

9.7.4 Uaktualnienie systemu

Kroki:

1. Przejdź do interfejsu Maintenance:

Configuration > Basic Configuration > System > Maintenance

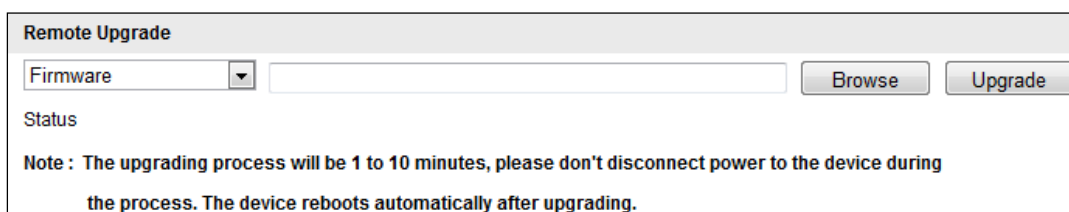
lub **Configuration > Advanced Configuration > System > Maintenance**

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

Firmware: zlokalizuj dokładnie ścieżkę pliku uaktualnienia.

Firmware Directory: wymagany jest tylko katalog, w którym znajduje się plik uaktualnienia.

- Kliknij przycisk **Browse**, aby wybrać lokalny plik aktualizacji, a następnie kliknij przycisk **Upgrade**, aby rozpocząć uaktualnienie zdalne.



Remote Upgrade

Firmware

Status

Note : The upgrading process will be 1 to 10 minutes, please don't disconnect power to the device during the process. The device reboots automatically after upgrading.

Rysunek 9–15 Zdalne uaktualnianie

Uwaga: Proces uaktualniania potrwa od 1 do 10 minut. Nie odłączaj zasilania urządzenia w trakcie trwania tego procesu. Urządzenie automatycznie uruchomi się ponownie po uaktualnieniu.

9.8 Ustawienia RS-485

Cel:

Port szeregowy RS-485 jest wykorzystywany do sterowania ruchem PTZ kamery. Przed rozpoczęciem sterowania ruchem PTZ kamery należy najpierw skonfigurować parametry PTZ.

Kroki:

- Przejdź do interfejsu ustawień portu RS-485, wybierając opcje:

Configuration > Advanced Configuration > System > RS485

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

Rysunek 9–16 Ustawienia portu RS-485

2. Ustaw parametry RS-485 i kliknij przycisk **Save**, aby zapisać ustawienia.

Domyślnie szybkość transmisji jest ustawiona na poziomie 9600 bps, wartość bitów danych wynosi 8, bit zatrzymania wynosi 1, a w pozycjach parzystości i sterowania przepływu podano wartość „brak”.

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

9.9 Ustawienia usługi

Przejdź do obszaru **Configuration > Advanced Configuration > System > Service**, aby otworzyć interfejs ustawień usługi.

Ustawienia usługi odnoszą się do usługi sprzętowej obsługiwanej przez kamerę, która różni się w zależności od kamery.

W przypadku gdy kamera obsługuje funkcję IR LED, ABF (automatyczna regulacja tylnej płaszczyzny ogniskowania), automatyczne usuwanie mgły lub diody LED stanu, można przejść do usługi sprzętowej i włączyć lub wyłączyć usługę w zależności od potrzeb.

W przypadku kamery obsługującej podgrzewanie w celu usunięcia oblodzenia można zaznaczyć pole wyboru, aby włączyć automatyczne usuwanie oblodzenia.

Uwaga: Podgrzewanie w celu usunięcia oblodzenia jest obsługiwane tylko w przypadku zastosowania zasilania POE+, 24VAC lub 12VDC. Podgrzewanie w celu usunięcia oblodzenia obsługuje tylko zasilanie standardowe 802.3at i nie obsługuje zasilania standardowego 802.3af.

Załącznik

Dodatek 1 Wprowadzenie do oprogramowania SADP

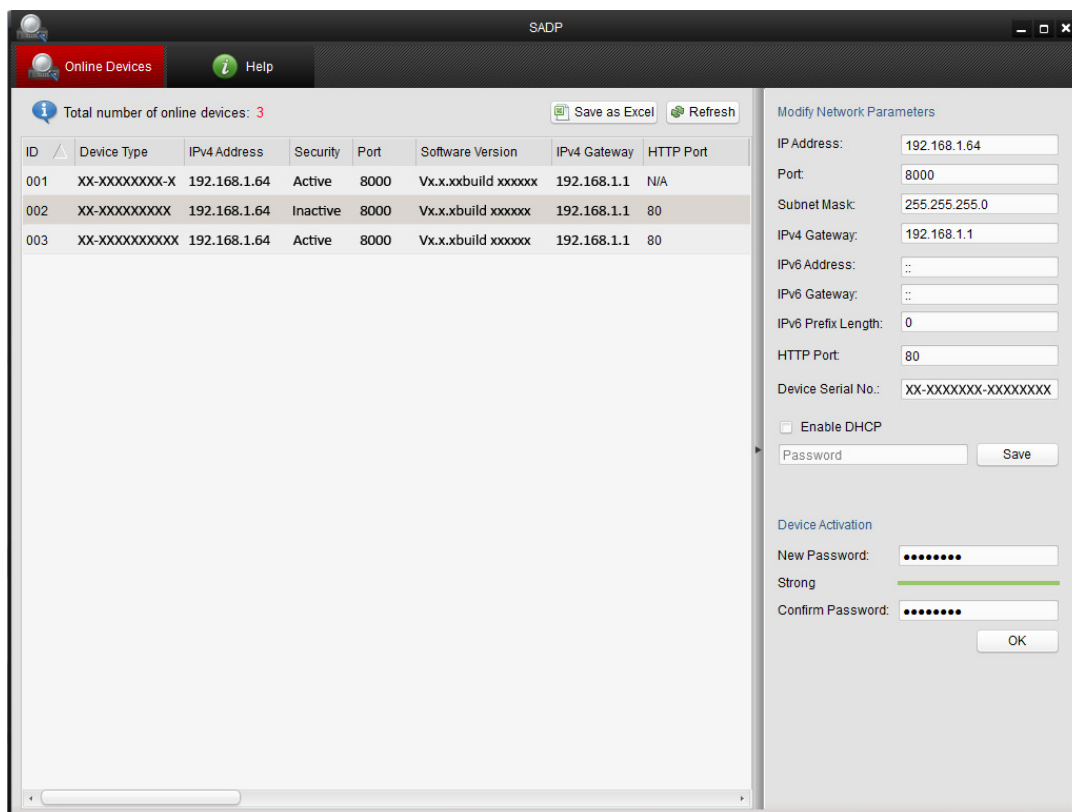
● Opis oprogramowania SADP

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.

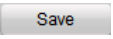
◆ Ręczne wyszukiwanie urządzeń połączonych z siecią

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. W polu „**Password**“ wprowadź hasło dostępu do konta administratora urządzenia i kliknij przycisk , aby zapisać zmiany.



- Aby zapewnić ochronę prywatności i systemu przed zagrożeniami bezpieczeństwa, zdecydowanie zalecamy używanie silnych haseł dla wszystkich funkcji i urządzeń sieciowych. Aby zwiększyć bezpieczeństwo urządzenia, należy ustawić własne hasło (składającego się z minimum 8 znaków, w tym wielkich liter, małych liter, cyfr i znaków specjalnych).
- Instalator i/lub użytkownik końcowy są zobowiązani do prawidłowego skonfigurowania wszystkich haseł i innych ustawień zabezpieczeń.

Modify Network Parameters

IP Address:

192.168.1.64

Port:

8000

Subnet Mask:

255.255.255.0

IPv4 Gateway:

192.168.1.1

IPv6 Address:

3a3a::

IPv6 Gateway:

3a3a::

IPv6 Prefix Length:


64

Serial No.:

XX-XXXXXX-XXXXXX-XXXXXX

Password

Save

 Note: Enter the admin password of the device before you save the network parameters.

Rysunek A.1.2 Modyfikowanie parametrów sieciowych

Dodatek 2 Mapowanie portów

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

Kroki:

- Wybierz ustawienie **WAN Connection Type** przedstawione na poniższym rysunku:

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.

108M Wireless Router
Model No.: TL-WR641G / TL-WR642G

- Status
- Quick Setup
- Basic Settings
- Network
- Wireless
- Advanced Settings
- DHCP
- Forwarding
 - Virtual Servers
 - Port Triggering
 - DMZ
 - UPnP
- Security
 - Static Routing
 - Dynamic DNS
- Maintenance
- System Tools

Virtual Servers

ID	Service Port	IP Address	Protocol	Enable
1	80	192.168.10.23	ALL	<input checked="" type="checkbox"/>
2	8000	192.168.10.23	ALL	<input checked="" type="checkbox"/>
3	554	192.168.10.23	ALL	<input checked="" type="checkbox"/>
4	8200	192.168.10.23	ALL	<input checked="" type="checkbox"/>
5	81	192.168.10.24	ALL	<input checked="" type="checkbox"/>
6	8001	192.168.10.24	ALL	<input checked="" type="checkbox"/>
7	555	192.168.10.24	ALL	<input checked="" type="checkbox"/>
8	8201	192.168.10.24	ALL	<input checked="" type="checkbox"/>

Common Service Port: DNS(53) Copy to ID 1

Previous Next Clear All Save

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.



First Choice for Security Professionals